暗号化されたベンダー固有属性

暗号化されたベンダー固有属性の機能により、ユーザはRADIUS サーバでフィルタを一元的に管理することができます。また、この機能は次の種類の文字列のベンダー固有属性（VSA）をサポートしています。

- タグ付きの文字列 VSA （2 ページ）（この新しい VSA がタグ付きであることを除き、Cisco VSA Type 1（Cisco:AVPair (1)）に類似）
- 暗号化された文字列 VSA （2 ページ）（この新しい VSA が暗号化されていることを除き、Cisco VSA Type 1 に類似）
- タグ付きおよび暗号化された文字列 VSA （2 ページ）（この新しい VSA がタグ付きで、暗号化されていることを除き、Cisco VSA Type 1 に類似）

Cisco:AVPairs では、属性と値のペア（AVP）の文字列の形式で追加の認証情報および認可情報を指定します。Internet Engineering Task Force（IETF）の RADIUS 属性 26（Vendor-Specific）が、ベンダー ID 番号「9」およびベンダータイプ値「1」で転送された場合（Cisco AVPair であることを意味します）、Cisco AVPair の RADIUS ユーザ プロファイルは「Cisco:AVPair = "protocol:attribute=value"」というような形式になります。

暗号化されたベンダー固有属性の前提条件

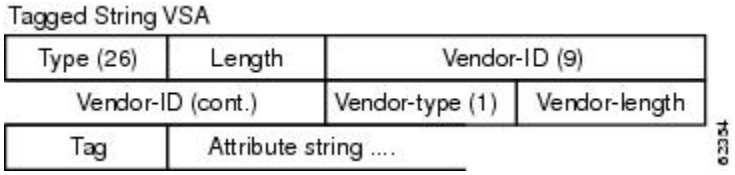
タグ付きで暗号化された VSA を RADIUS サーバが受け付けるようにするためには、AAA 認証および AAA 認可用にサーバを設定し、PPP コールを受け付けるように設定する必要があります。

暗号化されたベンダー固有属性に関する情報

タグ付きの文字列 VSA

次の図は、タグ付きの文字列 VSA のパケット形式を示します。

図 *1:* タグ付きの文字列 *VSA* の形式

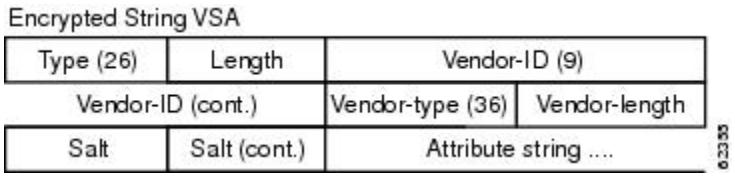


正しい値を取り出すために、Tag フィールドが正しく解析される必要があります。このフィールドの値の範囲はわずか 0x01 ～ 0x1F です。値が指定範囲内にない場合、RADIUS サーバはその値を無視し、Tag フィールドが Attribute String フィールドの一部であると見なします。

暗号化された文字列 VSA

次の図は、暗号化された文字列 VSA のパケット形式を示します。

図 *2:* 暗号化された文字列 *VSA* の形式



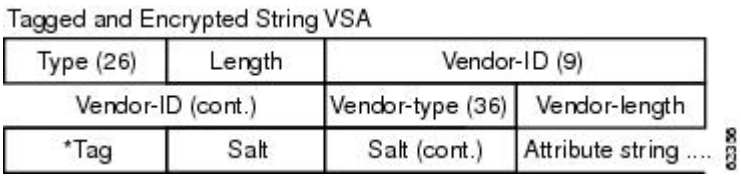
Saltフィールドは、VSAの各インスタンスの暗号化に使用される暗号キーの一意性を保証します。Salt フィールドの先頭の最上位ビットは 1 に設定する必要があります。

（注） Vendor-type (36) は、属性が暗号化された文字列 VSA であることを示しています。

タグ付きおよび暗号化された文字列 VSA

次の図は、新しくサポートされた各 VSA のパケットの形式を示しています。

図 *3:* タグ付きおよび暗号化された文字列 ***VSA*** の形式



この VSA は、Tag フィールドが追加されていることを除き、暗号化された文字列 VSA とほぼ同じです。Tag フィールドは、値が有効な範囲内（0x01 ～ 0x1F）にない場合、Salt フィールドの一部と見なされます。

暗号化されたベンダー固有属性の確認方法

暗号化されたベンダー固有属性の機能では、設定は必要ありません。RADIUS のタグ付きおよび暗号化 VSA が RADIUS サーバから送信されていることを検証するために、次のコマンドを特権 EXEC モードで実行します。

コマンド	目的
`Router# debug radius`	RADIUS 関連の情報を表示します。このコマンドの出力は、タグ付きおよび暗号化 VSA が RADIUS サーバから送信されているかどうかを示しています。

暗号化されたベンダー固有属性の設定例

NAS の設定例

次の例は、タグ付きおよび暗号化 VSA を使用して、基本的な設定のネットワーク アクセス サーバ（NAS）を設定する方法を示しています（この例では、PPP コールの確立に必要な設定がすでにイネーブルになっていると想定されています）。

```
aaa new-model
aaa authentication ppp default group radius
aaa authorization network default group radius
!
radius-server host 10.2.2.2 auth-port 1645 acct-port 1646
radius-server key cisco
```

タグ付きおよび暗号化 VSA がある RADIUS ユーザ プロファイルの例

次の例は、タグ付きおよび暗号化された文字列 VSA をサポートする RADIUS サーバのユーザ プロファイルの例です。

```
mascot   Password = "password1"
```

```
Service-Type = NAS-Prompt,
Framed-Protocol = PPP,
Cisco:Cisco-Enc = "ip:route=10.0.0.0 255.0.0.0"
Cisco.attr Cisco-Enc 36 tag-encstr(*,*)
```

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	『*Cisco IOS Master Commands List, All Releases*』
RADIUS 属性	『*Cisco IOS XE Security Configuration Guide: Securing User Services*, Release 2』
メディア独立型 PPP およびマルチリンク PPP	「メディア独立型 PPP およびマルチリンク PPP の設定」機能モジュール
認証	「認証の設定」機能モジュール
許可	「認可の設定」機能モジュール

標準

標準	タイトル
なし。	--

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)*』
RFC 2868	『*RADIUS Attributes for Tunnel Protocol Support*』

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

暗号化されたベンダー固有属性の機能情報

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 *1*：暗号化されたベンダー固有属性の機能情報

機能名	リリース	機能情報
暗号化されたベンダー固有属性	Cisco IOS XE Release 2.3	暗号化されたベンダー固有属性の機能により、ユーザは RADIUS サーバでフィルタを一元的に管理できます。また、この機能はタグ付き、暗号化、タグ付きおよび暗号化の各文字列ベンダー固有属性（VSA）をサポートしています。 Cisco IOS XE Release 2.3 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。

暗号化されたベンダー固有属性の機能情報

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。