RADIUS 属性値スクリーニング

RADIUS 属性値スクリーニング機能を使用すれば、認可やアカウンティングなどの目的で、ネットワーク アクセス サーバ（NAS）上の「許可」または「拒否」RADIUS 属性のリストを設定できます。

NAS が Access-Accept パケットで受信したすべての RADIUS 属性を受け入れて処理する場合は、不必要な属性を処理する可能性があり、顧客の認証、認可、およびアカウンティング（AAA）サーバを制御しないホールセール プロバイダーの場合に問題が発生します。たとえば、顧客が加入していないサービスを指定する属性が存在したり、他のホールセール ダイヤルユーザ向けのサービスを低下させる属性が存在したりする場合です。そのため、特定の属性の使用を制限するように NAS を設定できることが、多くのユーザの要件になります。

RADIUS 属性値スクリーニング機能を実装するには、次の方法のいずれかを使用する必要があります。

- NAS が、特定の目的で、設定された拒否リストに登録されたものを除く、すべての標準 RADIUS 属性を受け入れて、処理できるようにする
- NAS が、特定の目的で、設定された許可リストに登録されたものを除く、すべての標準 RADIUS 属性を拒否（除外）できるようにする

RADIUS 属性値スクリーニングの前提条件

RADIUS の許可リストおよび拒否リストを設定する前に、AAA を有効にする必要があります。

RADIUS 属性値スクリーニングの制約事項

NAS の要件

この機能を有効にするには、RADIUS グループを使用して認可するように NAS を設定する必要があります。

許可リストまたは拒否リストの制約事項

許可リストまたは拒否リストの設定に使用される 2 つのフィルタは相互排他的です。そのため、ユーザはサーバ グループの目的ごとに、1 つのアクセス リストか、1 つの拒否リストしか設定できません。

ベンダー固有属性

この機能は、ベンダー固有属性（VSA）スクリーニングをサポートしていません。ただし、ユーザは、すべての VSA を許可または拒否する許可リストまたは拒否リスト内で属性 26（Vendor-Specific）を指定できます。

必須属性スクリーニングの推奨事項

次の必須属性は、拒否しないことを推奨します。

- 認可用：
  - 6（Service-Type）
  - 7（Framed-Protocol）
- アカウンティング用：
  - 4（NAS-IP-Address）
  - 40（Acct-Status-Type）
  - 41（Acct-Delay-Time）
  - 44（Acct-Session-ID）

属性が必須の場合は、拒否が無視され、属性のパススルーが許可されます。

（注） 必須属性の拒否リストを設定してもエラーにはなりません。これは、リストでは目的（認可またはアカウンティング）が指定されないためです。サーバが、属性の使用目的を認識したときに、その属性が必須かどうかを判断します。

RADIUS 属性値スクリーニングに関する情報

RADIUS 属性値スクリーニング機能は、次のようなメリットを提供します。

- ユーザは、NAS 上で特定の目的の属性を選択して許可リストまたは拒否リストを設定できるため、不必要な属性が受け入れられ、処理されることがなくなります。
- 関連するアカウンティング属性だけの許可リストを設定することによって、不必要なトラフィックを削減し、アカウンティング データのカスタマイズを可能にすることができます。

RADIUS 属性のスクリーン方法

RADIUS 属性値スクリーニングの設定

RADIUS 属性の許可リストまたは拒否リストを認可またはアカウンティング用に設定するには、次のコマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. Router(config)# **aaa authentication ppp default**
4. Router(config)# **aaa authorization network default group** *group-name*
5. Router(config)# **aaa group server radius** *group-name*
6. Router(config-sg-radius)# **server** *ip-address*
7. Router(config-sg-radius)# **authorization** [**accept** | **reject**] *listname*
8. Router(config-sg-radius)# **exit**
9. Router(config)# **radius-server host** {*hostname* | *ip-address*} [**key** *string*
10. Router(config)# **radius-server attribute list** *listname*
11. Router(config-sg-radius)# **attribute** *value1* [*value2* [*value3...*]]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	Router(config)# **aaa authentication ppp default** 例： **group** *group-name*	PPP を実行しているシリアル インターフェイス上で使用する 1 つまたは複数の AAA 認証方式を指定します。
ステップ 4	Router(config)# **aaa authorization network default group** *group-name*	ユーザのネットワーク アクセスを制限するパラメータを設定します。
ステップ 5	Router(config)# **aaa group server radius** *group-name*	複数の RADIUS サーバ ホストを別々のリストと別々の方式にグループ分けします。
ステップ 6	Router(config-sg-radius)# **server** *ip-address*	グループ サーバ用の RADIUS サーバの IP アドレスを設定します。
ステップ 7	Router(config-sg-radius)# **authorization** [**accept** | **reject**] *listname* 例： and/or 例： Router(config-sg-radius)# **accounting** [**accept** | **reject**] *listname*	RADIUS サーバから Access-Accept パケット内で返す属性用のフィルタを指定します。 および/または アカウンティング要求内で RADIUS サーバに送信すべき属性用のフィルタを指定します。 （注） **accept** キーワードは、*listname* で指定された属性を除く、すべての属性が拒否されることを意味します。**reject** キーワードは、*listname* で指定された属性とすべての標準属性を除く、すべての属性が許可されることを意味します。
ステップ 8	Router(config-sg-radius)# **exit**	server-group コンフィギュレーション モードを終了します。
ステップ 9	Router(config)# **radius-server host** {*hostname* | *ip-address*} [**key** *string*	RADIUS サーバ ホストを指定します。
ステップ 10	Router(config)# **radius-server attribute list** *listname*	**attribute** コマンドで定義された一連の属性に指定されたリスト名を定義します。 （注） *listname* はステップ 5 で定義した *listname* と同じにする必要があります。
ステップ 11	Router(config-sg-radius)# **attribute** *value1* [*value2* [*value3...*]]	設定した許可リストまたは拒否リストに属性を追加します。

	コマンドまたはアクション	目的
		（注） このコマンドは、許可リストまたは拒否リストに属性を追加するために何回も使用できます。

RADIUS 属性値スクリーニングの確認

許可リストまたは拒否リストを確認するには、特権EXECモードで次のコマンドのいずれかを使用します。

コマンド	目的
`Router# debug aaa accounting`	説明の義務があるイベントが発生したときに、その情報を表示します。
`Router# debug aaa authentication`	AAA 認証に関する情報を表示します。
`Router# show radius statistics`	アカウンティングパケットと認証パケットについてのRADIUS 統計情報を示します。

RADIUS 属性値スクリーニングの設定例

認可許可の例

次の例は、属性 6（Service-Type）と属性 7（Framed-Protocol）用の許可リストの設定方法を示しています。他のすべての属性（VSA を含む）は RADIUS 認可に対して拒否されます。

```
aaa new-model
aaa authentication ppp default group radius-sg
aaa authorization network default group radius-sg
aaa group server radius radius-sg
server 10.1.1.1
authorization accept min-author
!
radius-server host 10.1.1.1 key mykey1
radius-server attribute list min-author
attribute 6-7
```

アカウンティング拒否の例

次の例は、属性 66（Tunnel-Client-Endpoint）と属性 67（Tunnel-Server-Endpoint）用の拒否リストの設定方法を示しています。他のすべての属性（VSA を含む）は RADIUS アカウンティングに対して受け入れられます。

```
aaa new-model
aaa authentication ppp default group radius-sg
aaa authorization network default group radius-sg
aaa group server radius radius-sg
server 10.1.1.1
accounting reject tnl-x-endpoint
!
radius-server host 10.1.1.1 key mykey1
radius-server attribute list tnl-x-endpoint
attribute 66-67
```

認可拒否とアカウンティング許可の例

次の例は、RADIUS 認可用の拒否リストと RADIUS アカウンティング用の許可リストの設定方法を示しています。認可またはアカウンティングのサーバグループごとに複数の許可リストまたは拒否リストを設定できませんが、サーバグループごとに認可用のリストとアカウンティング用のリストを 1 つずつ設定できます。

```
aaa new-model
aaa authentication ppp default group radius-sg
aaa authorization network default group radius-sg
aaa group server radius radius-sg
server 10.1.1.1
authorization reject bad-author
accounting accept usage-only
!
radius-server host 10.1.1.1 key mykey1
radius-server attribute list usage-only
attribute 1,40,42-43,46
!
radius-server attribute list bad-author
attribute 22,27-28,56-59
```

必須属性の拒否の例

次に、**debug aaa accounting** コマンドを使用した場合のデバッグ出力の例を示します。この例では、必須属性の 44、40、および 41 が拒否リストの「standard」に追加されています。

```
Router# debug aaa authorization
AAA/ACCT(6): Accounting method=radius-sg (radius)
RADIUS: attribute 44 cannot be rejected
RADIUS: attribute 61 rejected
RADIUS: attribute 31 rejected
RADIUS: attribute 40 cannot be rejected
RADIUS: attribute 41 cannot be rejected
```

その他の参考資料

次の項で、RADIUS 属性値スクリーニング機能に関する参考資料を紹介します。

関連資料

関連項目	マニュアル タイトル
RADIUS	「RADIUS の設定」機能モジュール。
その他のセキュリティ機能	『*Cisco IOS XE Security Configuration Guide: Securing User Services*, Release 2』
セキュリティ コマンド	『*Cisco IOS Security Command Reference*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

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
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

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 属性値スクリーニングの機能情報

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 : RADIUS* 属性値スクリーニングの機能情報

機能名	リリース	機能情報
RADIUS 属性値スクリーニング	Cisco IOS XE Release 2.1	RADIUS 属性値スクリーニング機能を使用すれば、認可やアカウンティングなどの目的で、ネットワーク アクセス サーバ（NAS）上の「許可」または「拒否」RADIUS 属性のリストを設定できます。 この機能は、Cisco IOS XE リリース 2.1 で Cisco ASR 1000 シリーズアグリゲーション サービス ルータに導入されました。 この機能により、次のコマンドが導入または変更されました。**accounting (server-group), authorization (server-group), attribute (server-group), radius-server attribute list**

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。