RADIUS 許可の変更

RADIUS 認可変更（CoA）機能は、認証、許可、アカウンティング（AAA）セッションの属性を、セッション認証後に変更するためのメカニズムを提供します。AAA でユーザ、またはユーザ グループのポリシーに変更がある場合、管理者は Cisco Secure Access Control Server（ACS）などの AAA サーバから RADIUS CoA パケットを送信して認証を再初期化し、新しいポリシーを適用することができます。

- RADIUS 認可変更に関する情報 （1 ページ）
- RADIUS 認可変更の設定方法 （6 ページ）
- RADIUS 認可変更の設定例 （11 ページ）
- RADIUS 認可変更に関する追加情報 （12 ページ）
- RADIUS 認可変更の機能情報 （14 ページ）

RADIUS 認可変更に関する情報

RADIUS 認可変更について

標準RADIUSインターフェイスは通常、ネットワークに接続しているデバイスから要求が送信され、クエリーが送信されたサーバが応答するプル モデルで使用されます。シスコのソフトウェアは、プッシュ モデルで使用される RFC 5176 で定義された RADIUS CoA 要求をサポートしています。このモデルでは、要求は外部サーバからネットワークに接続されたデバイスへ発信され、外部の認証、許可、アカウンティング（AAA）またはポリシー サーバからの動的なセッション再設定が可能になります。

次のセッション単位の CoA 要求を使用します。

- セッション再認証
- セッションの終了
- ポート シャットダウンでのセッション終了
- ポート バウンスでのセッション終了
- セキュリティとパスワード

- アカウンティング

CoA 要求

CoA 要求は、RFC 5176 に記載されているように、プッシュ モデルで使用することによって、セッション識別、ホスト再認証、およびセッション終了を行うことができます。モデルは、次のように、1 つの要求（CoA-Request）と 2 つの考えられる応答コードで構成されます。

- CoA acknowledgment（ACK）[CoA-ACK]
- CoA non-acknowledgment（NAK）[CoA-NAK]

要求は CoA クライアント（通常は RADIUS またはポリシー サーバ）から開始されて、リスナーとして動作するデバイスに転送されます。

RFC 5176 規定

Disconnect Request メッセージは Packet of Disconnect（POD）とも呼ばれますが、セッション終了に対してデバイスでサポートされています。

次の表に、RADIUS 認可変更（CoA）機能でサポートされている IETF 属性を示します。

表 *1 :* サポートされている *IETF* 属性

属性番号	属性名
24	状態
31	Calling-Station-ID
44	Acct-Session-ID
80	Message-Authenticator
101	Error-Cause

次の表に、Error-Cause 属性で取ることができる値を示します。

表 *2 : Error-Cause* の値

値	説明
201	削除された残留セッション コンテキスト
202	無効な EAP パケット（無視）
401	サポートされていない属性
402	見つからない属性
403	NAS 識別情報のミスマッチ

値	説明
404	無効な要求
405	サポートされていないサービス
406	サポートされていない拡張機能
407	無効な属性値
501	管理上の禁止
502	ルート不可能な要求（プロキシ）
503	セッション コンテキストが検出されない
504	セッション コンテキストが削除できない
505	その他のプロキシ処理エラー
506	リソースが使用不可能
507	要求が発信された
508	マルチ セッションの選択がサポートされてない

CoA 要求応答コード

CoA 要求の応答コードは、デバイスへコマンドを発行するために使用されます。サポートされているコマンドを「CoA 要求コマンド」に示します。

RFC 5176 で定義されている CoA 要求応答コードのパケットの形式は、コード、ID、長さ、オーセンティケータ、およびタイプ、長さ、値（TLV）形式の属性から構成されます。

属性フィールドは、Cisco ベンダー固有属性（VSA）を送信するために使用します。

セッションの識別

特定のセッションに対する接続解除および CoA 要求の場合、デバイスは次の 1 つまたは複数の属性に基づいてセッションを検出します。

- Acct-Session-Id（IETF 属性 #44）
- Audit-Session-Id（シスコのベンダー固有属性（VSA））
- Calling-Station-Id（ホスト MAC アドレスを含む IETF 属性 #31）

CoA メッセージに含まれるすべてのセッション ID 属性がそのセッションと一致しない限り、デバイスは「Invalid Attribute Value」エラー コード属性を含む Disconnect-NAK または CoA-NAK を返します。

（注） CoA NAK メッセージは、キーの不一致があるすべての CoA 要求に送信されるわけではありません。メッセージは、クライアントの最初の 3 つの要求にのみ送信されます。その後、そのクライアントからのすべてのパケットがドロップされます。キーの不一致が見つかると、CoA NAK メッセージで送信される応答オーセンティケータはダミーのキー値から計算されます。

CoA ACK 応答コード

許可ステートの変更に成功した場合は、肯定確認応答（ACK）が送信されます。CoA ACK 内で返される属性は CoA 要求によって異なります。

CoA NAK 応答コード

否定応答（NAK）は許可ステートの変更に失敗したことを示し、エラーの理由を示す属性を含めることができます。

CoA 要求コマンド

デバイスでサポートされているコマンドを次の表に示します。すべての CoA コマンドには、デバイスと CoA クライアント間のセッション ID が含まれている必要があります。

表 *3:* デバイスでサポートされる *CoA* 要求コマンド

コマンド	シスコの VSA
Bounce host port	Cisco:Avpair="subscriber:command=bounce-host-port"
Disable host port	Cisco:Avpair="subscriber:command=disable-host-port"
Reauthenticate host	Cisco:Avpair="subscriber:command=reauthenticate"
Terminate session	VSA を必要としない標準の接続解除要求です

セッション再認証

セッション認証を開始するために、認証、許可、アカウンティング（AAA）サーバは、Cisco VSA と 1 つ以上のセッション ID 属性を含む標準 CoA 要求メッセージを送信します。Cisco VSA は、Cisco:Avpair=“subscriber:command=reauthenticate” の形式です。

次のシナリオでは、現在のセッション状態によって、メッセージに対するデバイスの応答が決まります。

- セッションが現在、IEEE 802.1*x* によって認証されている場合、デバイスは Extensible Authentication Protocol over LAN（EAPoL）-RequestId メッセージをサーバに送信することで応答します。
- セッションが現在 MAC 認証バイパス（MAB）によって認証されている場合、デバイスはアクセス要求をサーバに送信し、最初に成功した認証で使用したのと同じ ID 属性を渡します。

- デバイスがコマンドを受信した際にセッション認証が実行中である場合は、デバイスはプロセスを終了し、認証シーケンスを再開し、最初に試行されるように設定された方式で開始します。

セッションの終了

CoA 接続解除要求は、ホスト ポートをディセーブルにせずにセッションを終了します。CoA 接続解除要求終了によって、指定したホストのオーセンティケータ ステート マシンが再初期化されますが、ホストのネットワークへのアクセスは制限されません。セッションが見つからない場合、デバイスは「Session Context Not Found」エラー コード属性を使用して Disconnect-NAK メッセージを返します。セッションが見つかった場合、デバイスはセッションを終了します。セッションが完全に削除されると、デバイスは Disconnect-ACK メッセージを返します。

ホストのネットワークへのアクセスを制限するには、Cisco:Avpair="subscriber:command=disable-host-port" VSA を含む CoA 要求を使用します。このコマンドは、ホストがネットワーク上で問題を起こしていることを把握し、ホストのネットワーク アクセスを即座にブロックする必要がある場合に便利です。ポートのネットワーク アクセスを復元する場合は、非 RADIUS メカニズムを使用して再びイネーブルにします。

CoA 要求の disable host port

RADIUS サーバーの CoA disable port コマンドを実行すると、セッションをホストしている認証ポートが管理的にシャットダウンされます。その結果、セッションは終了します。このコマンドは、ホストがネットワーク上で問題を起こしていることを把握し、ホストのネットワーク アクセスを即座にブロックする必要がある場合に便利です。ポートのネットワーク アクセスを復元する場合は、非 RADIUS メカニズムを使用して再びイネーブルにします。このコマンドは、次の VSA を含む標準の CoA-Request メッセージで伝達されます。

Cisco:Avpair="subscriber:command=disable-host-port"

このコマンドはセッション指向であるため、「セッション ID」セクションに示されている 1 つ以上のセッション ID 属性とともに使用する必要があります。セッションを検出できない場合、デバイスは「Session Context Not Found」エラー コード属性を含む CoA-NAK メッセージを返します。デバイスは、セッションを検出すると、ホスティング ポートを無効にし、CoA-ACK メッセージを返します。

デバイスが CoA-ACK をクライアントに返す前にデバイスに障害が発生した場合、クライアントから要求が再送信されると、新しいアクティブ デバイス上でそのプロセスが繰り返されます。デバイスが CoA-ACK メッセージをクライアントに返した後でデバイスに障害が発生したが、操作が完了していない場合、その操作は新しいアクティブ デバイスで再開されます。

RADIUS サーバの CoA disable port コマンドを無視するには、「bounce および disable RADIUS CoA 要求を無視するためのデバイスの設定」を参照してください。

CoA 要求の bounce port

RADIUS サーバーの CoA bounce port が RADIUS サーバーから送信されると、認証ポートでリンクのフラップが発生します。その結果、このポートに接続している 1 つまたは複数のホストから、DHCP の再ネゴシエーションが開始されます。この状況は、VLAN の変更があり、この認証ポートに関する変化を検出するメカニズムがないデバイス（プリンタなど）がエンドポイ

ントの場合に発生する可能性があります。CoA bounce port は、次の新しい VSA を含む標準の CoA-Request メッセージで伝達されます。

Cisco:Avpair="subscriber:command=bounce-host-port"

このコマンドはセッション指向であるため、「セッション ID」に示されている 1 つ以上のセッション ID 属性とともに使用する必要があります。セッションが見つからない場合、デバイスは「Session Context Not Found」エラー コード属性を使用して CoA-NAK メッセージを返します。このセッションがある場合は、デバイスはホスト ポートを 10 秒間ディセーブルし、再びイネーブルにし（ポート バウンス）、CoA-ACK を返します。

RADIUS サーバの CoA bounce port を無視するには、「bounce および disable RADIUS CoA 要求を無視するためのデバイスの設定」を参照してください。

RADIUS 認可変更の設定方法

RADIUS 認可変更の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa server radius dynamic-author**
5. **client** {*ip-address* | *name* [**vrf** *vrf-name*]} **server-key** [**0** | **7**] *string*
6. **port** *port-number*
7. **auth-type** {**any** | **all** | **session-key**}
8. **ignore session-key**
9. **ignore server-key**
10. **exit**

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： `Device> 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： `Device# 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。
ステップ 3	**aaa new-model** 例：	認証、認可、アカウンティング（AAA）をグローバルに有効化します。

	コマンドまたはアクション	目的
	`Device(config)# aaa new-model`	
ステップ 4	**aaa server radius dynamic-author** 例： `Device(config)# aaa server radius dynamic-author`	ダイナミック認可ローカル サーバー コンフィギュレーション モードを開始し、デバイスが認可変更（CoA）を受け入れ、要求を取り外す RADIUS クライアントを指定します。デバイスを AAA サーバーとして設定し、外部ポリシー サーバーとの連携を可能にする。
ステップ 5	**client** {*ip-address* | *name* [**vrf** *vrf-name*]} **server-key** [**0** | **7**] *string* 例： `Device(config-locsvr-da-radius)# client 10.0.0.1`	RADIUS キーをデバイスと RADIUS クライアントとの間で共有されるように設定します。
ステップ 6	**port** *port-number* 例： `Device(config-locsvr-da-radius)# port 3799`	設定された RADIUS クライアントから RADIUS 要求をデバイスが受信するポートを指定します。 （注） パケットオブディスコネクトのデフォルト ポートは 1700 です。ACS 5.1 と相互運用するためには、ポート 3799 が必要です。
ステップ 7	**auth-type** {**any** | **all** | **session-key**} 例： `Device(config-locsvr-da-radius)# auth-type all`	デバイスが RADIUS クライアントに使用する認可のタイプを指定します。クライアントは、認可用に設定された属性と一致していなければなりません。
ステップ 8	**ignore session-key** 例： `Device(config-locsvr-da-radius)# ignore session-key`	（オプション）セッション キーを無視するようにデバイスを設定します。
ステップ 9	**ignore server-key** 例： `Device(config-locsvr-da-radius)# ignore server-key`	（オプション）サーバー キーを無視するようにデバイスを設定します。
ステップ 10	**exit** 例： `Device(config-locsvr-da-radius)# exit`	グローバル コンフィギュレーション モードに戻ります。

bounce および disable RADIUS CoA 要求を無視するためのデバイスの設定

複数のホストを使用して認証ポートを認証していて、このポートで 1 つのホストに対してフラップする認可変更（CoA）要求があるか、このポートで終了するホストセッションがある場合、このポート上のその他のホストにも影響があります。したがって、複数のホストを使用して認証されたポートは、フラップの場合に 1 つまたは複数のホストから DHCP の再ネゴシエーションをトリガーします。または、1 つまたは複数のホストについて、セッションをホストする認証ポートを管理的にシャットダウンします。

次の手順を使用して、bounce port コマンドまたは disable port コマンドの形式で RADIUS サーバの認可変更（CoA）要求を無視するようにデバイスを設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **authentication command bounce-port ignore**
5. **authentication command disable-port ignore**
6. **end**

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： `Device> 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： `Device# 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。
ステップ 3	**aaa new-model** 例： `Device(config)# aaa new-model`	認証、認可、アカウンティング（AAA）をグローバルに有効化します。
ステップ 4	**authentication command bounce-port ignore** 例： `Device(config)# authentication command bounce-port ignore`	（任意）RADIUS サーバの bounce port コマンドを無視するようにデバイスを設定します。無視しない場合、認証ポート上でホストがフラップをリンクし、結果として、そのポートに接続する 1 つまたは複数のホストから DHCP 再ネゴシエーションが発生します。

	コマンドまたはアクション	目的
ステップ 5	**authentication command disable-port ignore** 例： `Device(config)# authentication command disable-port ignore`	（任意）RADIUS サーバの CoA disable port コマンドを無視するようにデバイスを設定します。無視しない場合、1 または複数のホスト セッションをホストする認証ポートが管理的にシャットダウンされます。 • ポートがシャットダウンされると、セッションも終了します。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

RADIUS CoA 用の動的認可サービスの設定

次の手順を実行して、動的許可サービスの認証、許可、アカウンティング（AAA）サーバとしてデバイスを有効にします。このサービスは、入力方向と出力方向でポリシー マップをプッシュする認可変更（CoA）機能をサポートします。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa server radius dynamic-author**
5. **client** {*ip-addr* | *hostname*} [**server-key** [**0** | **7**] *string*]
6. **domain** {**delimiter** *character* | **stripping** | [**right-to-left**]}
7. **port** *port-num*
8. **end**

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： `Device> 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： `Device# 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	**aaa new-model** 例： `Device(config)# aaa new-model`	AAA をグローバルに有効にします。
ステップ 4	**aaa server radius dynamic-author** 例： `Device(config)# aaa server radius dynamic-author`	ローカル AAA サーバを動的認可サービス用にセットアップして、動的認可ローカル サーバ コンフィギュレーション モードに入ります。このサービスは、ポリシー マップを入力方向と出力方向にプッシュする CoA 機能をサポートするように有効にする必要があります。 • このモードでは、RADIUS アプリケーション コマンドが設定されます。
ステップ 5	**client** {*ip-addr* | *hostname*} [**server-key** [**0** | **7**] *string*] 例： `Device(config-locsvr-da-radius)# client 192.168.0.5 server-key cisco1`	AAA サーバー クライアントの IP アドレスまたはホスト名を設定します。 • オプションの **server-key** キーワードと *string* 引数を使用して、クライアントレベルのサーバー キーを設定します。 （注） クライアント レベルでサーバー キーを設定すると、グローバル レベルで設定されたサーバー キーが上書きされます。
ステップ 6	**domain** {**delimiter** *character* | **stripping** | [**right-to-left**]} 例： `Device(config-locsvr-da-radius)# domain stripping right-to-left`	（任意）RADIUS アプリケーションについてユーザ名のドメイン オプションを設定します。 • **delimiter** キーワードで、ドメインデリミタを指定します。次のいずれかのオプションを *character* 引数に指定できます。**@**、**/**、**$**、**%**、****、**#**、または **-**。 • **stripping** キーワードは、着信のユーザー名と、**@** ドメインデリミタの左側にある名前を比較します。 • The **right-to-left** キーワードは、右から左方向に見て最初のデリミタで文字列を終了します。
ステップ 7	**port** *port-num* 例： `Device(config-locsvr-da-radius)# port 3799`	CoA 要求に UDP ポートを設定します。

	コマンドまたはアクション	目的
ステップ 8	**end** 例： `Device(config-locsvr-da-radius)# end`	特権 EXEC モードに戻ります。

RADIUS 認可変更のモニタリングとトラブルシューティング

RADIUS認可変更機能のモニタリングおよび問題を解決するために、次のコマンドを使用できます。

表 *4 : RADIUS* 認可変更のモニタリングとトラブルシューティング

コマンド	目的
debug aaa coa	CoA 処理のデバッグ情報を表示します。
debug aaa pod	パケットオブディスコネクト（POD）パケットに関連するデバッグ メッセージを表示します。
debug radius	RADIUS 関連の情報を表示します。
show aaa attributes protocol radius	認証、許可、アカウンティング（AAA）属性番号と対応するAAA属性名のマッピングを表示します。

RADIUS 認可変更の設定例

例：RADIUS 認可変更の設定

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa server radius dynamic-author
Device(config-locsvr-da-radius)# client 10.0.0.1
Device(config-locsvr-da-radius)# server-key cisco123
Device(config-locsvr-da-radius)# port 3799
Device(config-locsvr-da-radius)# auth-type all
Device(config-locsvr-da-radius)# ignore session-key
Device(config-locsvr-da-radius)# ignore server-key
Device(config-locsvr-da-radius)# end
```

例：bounce および disable RADIUS 要求を無視するためのデバイスの設定

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# authentication command bounce-port ignore
Device(config)# authentication command disable-port ignore
Device(config)# end
```

例：RADIUS CoA 用の動的認可サービスの設定

次に、認証、許可、アカウンティング（AAA）サーバとしてのデバイスが、入力方向と出力方向でポリシー マップをプッシュする認可変更（CoA）機能をサポートするように設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa server radius dynamic-author
Device(config-locsvr-da-radius)# client 192.168.0.5 server-key cisco1
Device(config-locsvr-da-radius)# domain delimiter @
Device(config-locsvr-da-radius)# port 3799
Device(config-locsvr-da-radius)# end
```

RADIUS 認可変更に関する追加情報

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 Command 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』
AAA の設定	『*Authentication, Authorization, and Accounting Configuration Guide*』

標準および RFC

標準/RFC	タイトル
RFC 2903	「*Generic AAA Architecture*」
RFC 5176	「*Dynamic Authorization Extensions to 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
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 認可変更の機能情報

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 *5 : RADIUS* 認可変更の機能情報

機能名	リリース	機能情報
RADIUS 許可の変更		RADIUS 認可変更（CoA）機能は、AAA セッションの属性をセッション認証後に変更するためのメカニズムを提供します。AAA でユーザ、またはユーザ グループのポリシーに変更がある場合、管理者は Cisco Secure Access Control Server（ACS）などの AAA サーバから RADIUS CoA パケットを送信して認証を再初期化し、新しいポリシーを適用することができます。 次のコマンドが導入または変更されました。**aaa server radius dynamic-author**、**authentication command bounce-port ignore**、**authentication command disable-port ignore**

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。