Session Aware Networking コマンド リファレンス、Cisco IOS XE Release 3SE（Catalyst 3850 スイッチ）

初版：2013 年 01 月 29 日

最終更新：2013 年 01 月 29 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次

A ～ Z

aaa accounting identity

アカウンティングをイネーブルにし、Session Aware Networking 加入者サービスのアカウンティング方式リストを作成するには、グローバル コンフィギュレーション モードで **aaa accounting identity** コマンドを使用します。 Session Aware Networking のアカウンティングをディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa accounting identity {*method-list-name*| **default**} **start-stop [broadcast] group** {*server-group-name*| **radius**| **tacacs+**} [**group**{*server-group-name*| **radius**| **tacacs+**}]

no aaa accounting identity {*method-list-name*| **default**}

構文の説明

method-list-name	この名前に続くアカウンティング方式を指定して、アカウンティング サービスを作成するための方式リストの名前。
default	このキーワードに続くアカウンティング方式を使用してアカウンティング サービスのデフォルト方式リストを作成します。
start-stop	プロセスの開始時に「start」アカウンティング通知を送信し、プロセスの終了時に「stop」アカウンティング通知を送信します。「start」アカウンティング レコードはバックグラウンドで送信されます。要求されたユーザ プロセスは、「start」アカウンティング通知をアカウンティング サーバから受信したかどうかにかかわらず開始されます。
broadcast	（任意）複数の認証、許可、およびアカウンティング（AAA）サーバにアカウンティング レコードを送信します。 各グループの最初のサーバに対し、アカウンティング レコードを同時に送信します。最初のサーバを使用できない場合、デバイスはそのグループ内に定義されているバックアップ サーバを使用します。
group	アカウンティング サービスに使用する 1 つ以上のサーバ グループを指定します。サーバ グループは、指定された順序で適用されます。

server-group-name	**aaa group server radius** コマンドまたは **aaa group server tacacs+** コマンドによって定義された RADIUS サーバまたは TACACS+ サーバの名前付きサブセット。
radius	**radius-server host** コマンドで設定されたすべての RADIUS サーバのリストを使用します。
tacacs+	**tacacs-server host** コマンドで設定されたすべての TACACS+ サーバのリストを使用します。

コマンド デフォルト

アカウンティングはディセーブルです。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

aaa accounting identity コマンドは、アカウンティング サービスをイネーブルにし、Session Aware Networking 加入者サービスの特定のアカウンティング方式を定義する方式リストを作成します。方式リストによって、ネットワーク アクセス サーバがアカウンティング レコードを送信する送信先となるセキュリティ サーバのリストが特定されます。

Cisco IOS ソフトウェアは、Session Aware Networking のアカウンティングについて、次の 2 つの方式をサポートしています。

- RADIUS：ネットワーク アクセス サーバは、アカウンティング レコードの形式で RADIUS セキュリティ サーバに対してユーザ アクティビティを報告します。 各アカウンティング レコードにはアカウンティングの Attribute-Value（AV）ペアが含まれ、レコードはセキュリティ サーバに格納されます。
- TACACS+：ネットワーク アクセス サーバは、アカウンティング レコードの形式で TACACS+ セキュリティ サーバに対してユーザ アクティビティを報告します。 各アカウンティング レコードは、アカウンティング AV ペアが含まれ、セキュリティ サーバ上で保管されます。

デフォルトの方式リストは、明示的に定義された名前付きの方式リストを持つ加入者セッションを除くすべてのセッションに自動的に適用されます。 名前付きの方式リストは、デフォルトの方式リストよりも優先されます。

AAA アカウンティングがアクティブにされると、ネットワーク アクセス サーバは、ユーザが実装したセキュリティ方式に応じて、接続に関係するRADIUSアカウンティング属性またはTACACS+ AV ペアをモニタします。 ネットワーク アクセス サーバはこれらの属性をアカウンティング レコードとしてレポートし、アカウンティング レコードはその後セキュリティ サーバのアカウンティング ログに保存されます。

aaa accounting identity コマンドを入力するには、事前に **aaa new-model** コマンドで AAA をイネーブルにしておく必要があります。

例

次の例は、アカウンティング サービスが TACACS+ サーバによって提供される場合に、デフォルトのアカウンティング方式リストを設定する方法を示しています。

```
aaa new-model
aaa accounting identity default start-stop group tacacs+
```

次の例は、アカウンティング サービスが RADIUS サーバによって提供される場合に、名前付きのアカウンティング方式リストを設定する方法を示しています。

```
aaa new model
aaa accounting identity LIST_1 start-stop group radius
```

関連コマンド

コマンド	説明
aaa group server radius	各種の RADIUS サーバ ホストを別個のリストにグループ化します。
aaa group server tacacs+	各種の TACACS+ サーバ ホストを別個のリストにグループ化します。
aaa new-model	AAA アクセス コントロール モデルをイネーブルにします。
radius-server host	RADIUS サーバ ホストを指定します。
tacacs-server host	TACACS+ サーバ ホストを指定します。

aaa local authentication

Lightweight Directory Access Protocol（LDAP）サーバからのローカル認証と許可に使用する方式リストを指定するには、グローバル コンフィギュレーション モードで **aaa local authentication** コマンドを使用します。 デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

aaa local authentication {*method-list-name*| **default**} **authorization** {*method-list-name*| **default**}

no aaa local authentication {*method-list-name*| **default**} **authorization** {*method-list-name*| **default**}

構文の説明

method-list-name	AAA 方式リストの名前。
default	デフォルト AAA 方式リストを使用します。

コマンド デフォルト

ローカル LDAP ベースの認証はディセーブルです。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
15.3(1)S	このコマンドが導入されました。
15.3(1)T	このコマンドが Cisco IOS Release 15.3(1)T に統合されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

aaa local authentication コマンドを使用して、ローカルまたはリモートの LDAP サーバから拡張認証プロトコル（EAP）資格情報を取得します。

例

次に、EAP_LIST という名前の方式リストを使用するようにローカル認証を設定する例を示します。

```
aaa new-model
aaa local authentication EAP_LIST authorization EAP_LIST
```

関連コマンド

aaa new-model	AAA アクセス コントロール モデルをイネーブルにします。
ldap server	LDAP サーバを定義します。

absolute-timer

加入者セッションに対して絶対タイムアウトをイネーブルにするには、サービステンプレートコンフィギュレーション モードで **absolute-timer** コマンドを使用します。 このタイマーをディセーブルにするには、このコマンドの **no** 形式を使用します。

absolute-timer *minutes*

no absolute-timer

構文の説明

minutes	分単位の最大セッション時間。 範囲：1 ～ 65535。 デフォルトは 0 で、タイマーは無効になっています。

コマンド デフォルト

ディセーブル（絶対タイムアウトは 0）。

コマンド モード

サービス テンプレート コンフィギュレーション（config-service-template）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

absolute-timer コマンドを使用して、加入者セッションがアクティブな状態を維持できる分数を制限します。 このタイマーが満了すると、セッションは新しい要求と同じように接続を確立するプロセスを繰り返す必要があります。

例

次に、SVC_3 という名前のサービステンプレートで、15 分に絶対タイムアウトを設定する例を示します。

```
service-template SVC_3
 description sample
 access-group ACL_2
 vlan 113
 inactivity-timer 15
 absolute-timer 15
```

関連コマンド

コマンド	説明
event absolute-timeout	条件が満たされる場合に、制御ポリシーでアクションをトリガーするイベントのタイプを指定します。
inactivity-timer	加入者セッションの非アクティブ タイムアウトをイネーブルにします。
show service-template	サービス テンプレートの設定情報を表示します。

access-group（サービス テンプレート）

サービス テンプレートを使用してセッションにアクセス リストを適用するには、サービス テンプレート コンフィギュレーション モードで**access-group** コマンドを使用します。アクセス グループを削除するには、このコマンドの **no** 形式を使用します。

access-group *access-list-name*

no access-group *access-list-name*

構文の説明

access-list-name	適用するアクセス コントロール リスト（ACL）の名前。

コマンド デフォルト

アクセス リストは適用されていません。

コマンド モード

サービス テンプレート コンフィギュレーション（config-service-template）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

access-group コマンドを使用して、サービス テンプレートがアクティブ化されているセッションにローカルで設定された ACL を適用します。

例

次に、セッションに ACL_in という名前のアクセス リストを適用する、SVC_2 という名前のサービス テンプレートを設定する例を示します。

```
service-template SVC_2
 description label for SVC_2
 access-group ACL_in
 redirect url http://cisco.com match URL_ACL
 tag TAG_1
```

関連コマンド

コマンド	説明
activate（ポリシー マップ アクション）	加入者セッションで、制御ポリシーまたはサービス テンプレートをアクティブ化します。
ip access-list	IP アクセス コントロール リスト（ACL）を定義します。

access-session closed

ポートでの事前認証アクセスを回避するには、インターフェイス コンフィギュレーション モードで **access-session closed** コマンドを使用します。 デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

access-session closed

no access-session closed

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

ディセーブル（ポートでアクセスは開いています）。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

access-session closed コマンドはポートへのアクセスを閉じ、認証が実行される前にクライアントまたはデバイスがネットワーク アクセスを得ることを回避します。

例

次に、ポート 1/0/2 を閉じられたアクセスに設定する方法を示します。

```
interface GigabitEthernet 1/0/2
 access-session host-mode single-host
 access-session closed
 access-session port-control auto
 access-session control-direction in
```

関連コマンド

access-session control-direction	ポートでの認証制御の方向を設定します。
access-session host-mode	ホストが制御ポートへのアクセス権を取得できるようにします。
access-session port-control	ポートの許可ステートを設定します。

access-session control-direction

ポートでの認証制御の方向を設定するには、インターフェイス コンフィギュレーション モードで **access-session control-direction** コマンドを使用します。 デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

access-session control-direction {**both**| **in**}

no access-session control-direction

構文の説明

both	ポートで双方向制御をイネーブルにします。 768 ビットは、デフォルト値です。
in	ポートで単方向制御をイネーブルにします。

コマンド デフォルト

ポートは双方向モードに設定されています。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

access-session control-direction コマンドを使用して、ポートの制御を一方向または双方向のいずれかに設定します。

in キーワードはポートを一方向として設定することで、ネットワーク上のデバイスがクライアントを「ウェイクアップ」し、再認証するように強制できます。 ポートは、ホストにパケットを送信できますが、受信はできません。

both キーワードはポートを双方向として設定することで、ポートへのアクセスが両方向で制御されるようにします。 ポートは、パケットを送信または受信できません。

show access-session interface コマンドを使用して、ポート設定を検証できます。

例

次に、ポート 1/0/2 で単一方向制御をイネーブルにする例を示します。

```
interface GigabitEthernet 1/0/2
 access-session host-mode single-host
 access-session closed
 access-session port-control auto
 access-session control-direction in
```

関連コマンド

access-session closed	ポートでの事前認証アクセスを回避します。
access-session host-mode	ホストが制御ポートへのアクセス権を取得できるようにします。
access-session port-control	ポートの許可ステートを設定します。
show access-session	認証セッションに関する情報を表示します。

access-session host-mode

ホストが制御されたポートへのアクセスを取得できるようにするには、インターフェイス コンフィギュレーション モードで **access-session host-mode** コマンドを使用します。 デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

access-session host-mode {**multi-auth**| **multi-domain**| **multi-host**| **single-host**}

no access-session host-mode

構文の説明

multi-auth	複数のクライアントをポートで常時認証できるように指定します。 768 ビットは、デフォルト値です。
multi-domain	ドメイン（DATA または VOICE）ごとに、1 つのクライアントしか同時に認証できないように指定します。
multi-host	最初のクライアントが認証された後、後続のすべてのクライアントのアクセスが許可されるように指定します。
single-host	ポート上で、常時 1 つのクライアントしか認証できないように指定します。 複数のクライアントが検出されると、セキュリティ違反が発生します。

コマンド デフォルト

ポートへのアクセスは multi-auth です。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用する前に、**access-session port-control auto** コマンドをイネーブルにする必要があります。

multi-host モードでは、接続されたホストのうち 1 つのみが正常に許可されれば、すべてのホストのネットワーク アクセスが許可されます。 ポートが無許可ステートになった場合（再認証が失敗

した場合、または Extensible Authentication Protocol over LAN（EAPOL）-Logoff メッセージを受信した場合）には、接続されたすべてのクライアントがネットワーク アクセスを拒否されます。

show access-session interface コマンドを使用して、ポート設定を検証できます。

例

次に、ポート 1/0/2 で単一のクライアントを同時に認証する例を示します。

```
interface GigabitEthernet 1/0/2
 access-session host-mode single-host
 access-session closed
 access-session port-control auto
 access-session control-direction in
```

関連コマンド

access-session closed	ポートでの事前認証アクセスを回避します。
access-session control-direction	ポートでの認証制御の方向を設定します。
access-session port-control	ポートの許可ステートを設定します。
show access-session	認証セッションに関する情報を表示します。

access-session port-control

ポートの許可ステートを設定するには、インターフェイス コンフィギュレーション モードで **access-session port-control** コマンドを使用します。 デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

access-session port-control {**auto**| **force-authorized**| **force-unauthorized**}

no access-session port-control

構文の説明

auto	ポートベースの認証をイネーブルにします。ポートは無許可ステートで開始し、ポート経由で送受信できるのは Extensible Authentication Protocol over LAN（EAPOL）フレームのみです。
force-authorized	インターフェイスの IEEE 802.1X をディセーブルにし、認証情報を交換しなくても、ポートを許可ステートに変更します。 ポートはクライアントとの 802.1x ベース認証を行わずに、通常のトラフィックを送受信します。 768 ビットは、デフォルト値です。
force-unauthorized	クライアントからの認証試行をすべて無視し、ポートを強制的に無許可ステートに変更して、このインターフェイス経由のすべてのアクセスを拒否します。

コマンド デフォルト

ポートは force-authorized ステートに設定されています。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

ポートのリンク ステートがダウンからアップに移行するか、または EAPOL-Start フレームを受信すると、認証プロセスが開始されます。 システムはクライアントの識別情報を要求して、クライアントと認証サーバ間で認証メッセージのリレーを開始します。

例

次に、ポート 1/0/2 で認証ステートを自動に設定する例を示します。

```
interface GigabitEthernet 1/0/2
 access-session host-mode single-host
 access-session closed
 access-session port-control auto
 access-session control-direction in
```

関連コマンド

access-session closed	ポートでの事前認証アクセスを回避します。
access-session host-mode	ホストが制御ポートへのアクセス権を取得できるようにします。
access-session port-control	ポートの許可ステートを設定します。

activate（ポリシー マップ アクション）

加入者セッションで、制御ポリシーまたはサービス テンプレートをアクティブ化するには、コントロール ポリシー マップ アクション コンフィギュレーション モードで **activate** コマンドを使用します。 制御ポリシーからこのアクションを削除するには、このコマンドの **no** 形式を使用します。

action-number **activate** {**policy type control subscriber** *control-policy-name* | **service-template** *template-name* [**aaa-list** *list-name*] [**precedence** *number*] **[replace-all]**}

no *action-number*

構文の説明

action-number	アクション数。 アクションは、ポリシー ルール内で順番に実行されます。
policy type control subscriber *control-policy-name*	**policy-map type control subscriber** コマンドによって定義されているように、セッションに適用する制御ポリシーの名前を指定します。
service-template *template-name*	セッションに適用するサービステンプレートの名前を指定します。 このテンプレートは、**service-template** コマンドでローカルに定義することも、認証、許可、アカウンティング（AAA）サーバからダウンロードすることもできます。
aaa-list *list-name*	（任意）サービステンプレートをダウンロードするAAAサーバを識別するAAA方式リストの名前を指定します。 これを指定しない場合、テンプレートはローカルに定義する必要があります。
precedence *number*	（任意）サービス テンプレートのプライオリティ レベルを指定します。 範囲：1 ～ 254。プライオリティは 1 が最も高く、254 が最も低くなります。
replace-all	（任意）新しいデータおよびサービスで、すべての既存の許可データとサービスを置き換えます。

コマンド デフォルト

制御ポリシーまたはサービス テンプレートは、加入者セッションに対してアクティブ化されていません。

コマンド モード

コントロール ポリシーマップ アクション コンフィギュレーション（config-action-control-policymap）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

activate コマンドは制御ポリシーにアクションを定義します。

制御ポリシーによって、指定されたイベントと条件に応じて実行されるアクションが決定されます。 制御クラスによって、アクションを実行するために満たす必要がある条件が定義されます。アクションは、ポリシー ルール内で番号が付けられ、順番に実行されます。

class コマンドは、制御クラスを 1 つ以上のアクションに関連付けることでポリシー ルールを作成します。

例

次に、SEQ_AUTH_WITH_AUTH_FAIL_VLAN という名前の制御ポリシーを設定する例を示します。 認証が失敗し、制御クラス DOT1X_FAILED のすべての条件が true であると評価された場合、システムは VLAN4 上という名前のサービス テンプレートをアクティブ化します。

```
class-map type control subscriber DOT1X_FAILED match-any
  match result-type method dot1x authoritative
  match result-type method dot1x agent-not-found
!
class-map type control subscriber MAB_FAILED match-all
  match method mab
  match result-type authoritative
!
policy-map type control subscriber SEQ_AUTH_WITH_AUTH_FAIL_VLAN
  event session-started match-all
   10 class always do-all
    10 authenticate using mab priority 20
  event authentication-failure match-all
   10 class MAB_FAILED do-all
    10 terminate mab
    20 authenticate using dot1x priority 10
   20 class DOT1X_FAILED do-all
    10 activate service-template VLAN4
```

関連コマンド

コマンド	説明
class	制御ポリシーの 1 つ以上のアクションに制御クラスを関連付けます。
deactivate	加入者セッションで制御ポリシーまたはサービス テンプレートを非アクティブ化します。
event	制御クラスの評価を開始するイベントのタイプを指定します。
service-template	加入者セッションに適用する一連の属性を含むサービス テンプレートを定義します。

authenticate using

指定した方式を使用して加入者セッションの認証を開始するには、コントロールポリシーマップ アクション コンフィギュレーション モードで **authenticate using** コマンドを使用します。 制御ポリシーからこのアクションを削除するには、このコマンドの **no** 形式を使用します。

action-number **authenticate using** {**dot1x**| **mab**| **webauth**}[**aaa** {**authc-list** *authc-list-name*| **authz-list** *authz-list-name*}] **[merge]** [**parameter-map** *parameter-map-name*] [**priority** *priority-number*] [**replace**| **replace-all**] [**retries** *number* {**retry-time** *seconds*}]

no *action-number*

構文の説明

action-number	アクション数。 アクションは、ポリシー ルール内で順番に実行されます。
dot1x	IEEE 802.1X 認証方式を指定します。
mab	MAC認証バイパス（MAB）方式を指定します。
webauth	Web 認証方式を指定します。
aaa	（任意）認証、許可、およびアカウンティング（AAA）方式リストを使用して認証が実行されることを示します。
authc-list *authc-list-name*	認証要求に使用する AAA 方式リストの名前を指定します。
authz-list *authz-list-name*	許可要求に使用する AAA 方式リストの名前を指定します。
merge	（任意）新しいデータとサービスを既存の許可データとサービスに統合します。
parameter-map *parameter-map-name*	（任意）**parameter map type webauth** コマンドで定義されているように、Web認証に使用するパラメータ マップの名前を指定します。

priority *priority-number*	（任意）選択した認証方式のプライオリティを指定します。プライオリティの高い方式を、プライオリティの低い方式で進行中の認証方式に割り込ませることができます。範囲：1～254。プライオリティは 1 が最も高く、254 が最も低くなります。デフォルトのプライオリティの順序は dot1x、mab、webauth です。
replace	（任意）新しい許可データに既存の許可データを置換します。
replace-all	（任意）新しいデータおよびサービスで、すべての既存の許可データとサービスを置き換えます。 これはデフォルトの動作です。
retries *number*	（任意）初期の試行が失敗した場合に、認証方式を再試行する回数。 有効な範囲は、1 ～ 5 です。 デフォルト：2。
retry-time *seconds*	認証間隔の秒数。 範囲は 0 ～ 65535 です。 デフォルトは 30 です。

コマンド デフォルト

認証は開始されません。

コマンド モード

コントロール ポリシーマップ アクション コンフィギュレーション（config-action-control-policymap）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

authenticate using コマンドは、制御ポリシーにアクションを定義します。

制御ポリシーによって、指定されたイベントと条件に応じて実行されるアクションが決定されます。 制御クラスによって、アクションを実行するために満たす必要がある条件が定義されます。アクションは、ポリシー ルール内で番号が付けられ、順番に実行されます。

class コマンドは、制御クラスを 1 つ以上のアクションに関連付けることでポリシー ルールを作成します。

AAA 方式のリストが設定されている場合、RADIUS または TACACS+ の AAA サーバはユーザ名とパスワードを確認して、アカウントが有効かどうかを確認します。 通常、認証リストと許可リストは同じAAA方式リストを共有します。リストは異なるデータベースを使用できますが、推奨されません。

例

次に、CONC_AUTH という名前の制御ポリシーの一部の設定例を示します。セッションが開始されると、デフォルト制御クラスでは、802.1X と MAB 認証がともに動作するよう指定されます。802.1X のプライオリティ（10）のほうが、MAB のプライオリティ（20）よりも高いため、失敗しない限り、802.1X がセッションの認証に使用され、その後に MAB 認証が使用されます。

```
policy-map type control subscriber CONC_AUTH
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x priority 10
   20 authenticate using mab priority 20
```

関連コマンド

コマンド	説明
class	制御ポリシーの 1 つ以上のアクションに制御クラスを関連付けます。
class-map type control subscriber	制御クラスを作成します。これは、制御ポリシーのアクションが実行される条件を定義します。
parameter-map type webauth	Web 認証用のパラメータ マップを定義します。

authentication-restart

認証または許可が失敗した後、認証プロセスを再開するには、コントロール ポリシー マップ アクション コンフィギュレーション モードで **authentication-restart** コマンドを使用します。 制御ポリシーからこのアクションを削除するには、このコマンドの **no** 形式を使用します。

action-number **authentication-restart** *seconds*

no *action-number*

構文の説明

action-number	アクション数。 アクションは、ポリシー ルール内で順番に実行されます。
seconds	障害発生後に認証プロセスを再開するまでに待機する秒数。 範囲：1 ～ 65535。

コマンド デフォルト

認証は再開されません。

コマンド モード

コントロール ポリシーマップ アクション コンフィギュレーション（config-action-control-policymap）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

authentication-restart コマンドは、制御ポリシーにアクションを設定します。

制御ポリシーによって、指定されたイベントと条件に応じて実行されるアクションが決定されます。 制御クラスによって、アクションを実行するために満たす必要がある条件が定義されます。アクションは、ポリシー ルール内で番号が付けられ、順番に実行されます。

class コマンドは、制御クラスを 1 つ以上のアクションに関連付けることでポリシー ルールを作成します。 ポリシー ルールに定義できるアクションは、**event** コマンドによって指定されるイベントのタイプによって異なります。

例

次に、認証失敗イベント用に設定されている **authentication-restart** コマンドを使用した、制御ポリシーの一部の設定例を示します。

```
class-map type control subscriber match-all DOT1X_TIMEOUT_FAIL
 match result-type method dot1x method-timeout
!
class-map type control subscriber match-all DOT1X_AUTH_FAIL
 match result-type method dot1x authoritative
!
policy-map type control subscriber POLICY
 event session-started match-first
  10 class always do-all
   10 authenticate using dot1x
 event authentication-failure match-all
    .
    .
    .
  50 class DOT1X_AUTH_FAIL do-all
   50 authentication-restart 60
```

関連コマンド

コマンド	説明
class	制御ポリシーの 1 つ以上のアクションに制御クラスを関連付けます。
event	条件が満たされる場合に、制御ポリシーでアクションをトリガーするイベントのタイプを指定します。
resume reauthentication	認証の失敗後に再認証を再開します。

authentication display

Session Aware Networking のコンフィギュレーション表示モードを設定するには、特権 EXEC モードで **authentication display** コマンドを使用します。

authentication display {**legacy**| **new-style**}

構文の説明

legacy	従来の Authentication Manager 形式で設定を表示します。 これは、デフォルトのモードです。
new-style	Session Aware Networking をサポートする Cisco Common Classification Policy Language（C3PL）スタイルを使用して設定を表示します。

コマンド デフォルト

レガシー モードがイネーブルです。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

authentication display コマンドを使用して、セッション認証ネットワーキングをサポートするコンフィギュレーション表示モードをイネーブルにします。 このコマンドを使用して、Session Aware Networking の設定を入力するまで、2 種類の異なる表示モード間を切替えることができます。 Session Aware Networking に固有の設定を入力すると、このコマンドは無効になり、使用できなくなります。

new-style キーワードによって、関連するすべてのレガシー認証コマンドがそれらの新しいコマンドの同等物に変換されます。 new-style モードがイネーブルな場合に設定を保存すると、システムによって設定が新しいスタイルで作成されます。 リロードを実行すると、レガシーモードに戻すことはできなくなります。

例

次に、Session Aware Networking で使用するスタイルに表示モードを設定する例を示します。

```
Device# authentication display new-style
```

関連コマンド

コマンド	説明
policy-map type control subscriber	加入者セッションの制御ポリシーを定義します。

authorize

加入者セッションの認証を開始するには、コントロールポリシーマップアクション コンフィギュレーション モードで、**authorize** コマンドを使用します。 制御ポリシーからこのアクションを削除するには、このコマンドの **no** 形式を使用します。

action-number **authorize**

no *action-number*

構文の説明

action-number	アクション数。 アクションは、ポリシー ルール内で順番に実行されます。

コマンド デフォルト

許可は開始されません。

コマンド モード

コントロールポリシーマップアクション コンフィギュレーション（config-action-control-policymap）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

authorize コマンドは制御ポリシーにアクションを定義します。

制御ポリシーによって、指定されたイベントと条件に応じて実行されるアクションが決定されます。 制御クラスによって、アクションを実行するために満たす必要がある条件が定義されます。アクションは、ポリシー ルール内で番号が付けられ、順番に実行されます。

class コマンドは、制御クラスを 1 つ以上のアクションに関連付けることでポリシー ルールを作成します。

例

次に、認証失敗イベントに設定されている許可アクションと制御ポリシーを設定する方法を示します。

```
class-map type control subscriber match-all DOT1X
 match method dot1x
!
class-map type control subscriber match-all MAB
 match method mab
!
```

```
class-map type control subscriber match-any SERVER_DOWN
 match result-type aaa-timeout
!
policy-map type control subscriber POLICY_4
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using mab priority 20
 event authentication-failure match-first
  10 class SERVER_DOWN do-all
   10 authorize
  20 class MAB do-all
   10 authenticate using dot1x priority 10
  30 class DOT1X do-all
   10 activate service-template VLAN4
   20 authentication-restart 60
```

関連コマンド

コマンド	説明
class	制御ポリシーの 1 つ以上のアクションに制御クラスを関連付けます。
class-map type control subscriber	制御クラスを作成します。これは、制御ポリシーのアクションが実行される条件を定義します。
policy-map type control subscriber	加入者セッションの制御ポリシーを定義します。
unauthorize	加入者セッションから、すべての認証データを削除します。

banner（パラメータ マップ Web 認証）

Web認証ログインページにバナーを表示するには、パラメータマップWeb認証コンフィギュレーション モードで **banner** コマンドを使用します。 バナー表示をディセーブルにするには、このコマンドの **no** 形式を使用します。

banner [**file** *location*:*filename*| **text** *banner-text*]

no banner [**file** *location*:*filename*| **text** *banner-text*]

構文の説明

file *location*:*filename*	（任意）Web 認証ログイン ページに表示するバナーを含むファイルを指定します。
text *banner-text*	（認証）バナーとして使用するテキスト文字列を指定します。 バナー テキストの前後に区切り文字を入力する必要があります。 区切り文字は、「c」や「@」など、任意の文字を使用できます。

コマンド デフォルト

Web 認証ログイン Web ページにバナーは表示されません。

コマンド モード

パラメータ マップ Web 認証コンフィギュレーション（config-params-parameter-map）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

banner コマンドを使用して、考えられる次の 3 つのシナリオのいずれかを設定できます。

- キーワードまたは引数を設定せずに **banner** コマンドを使用する：デバイスの名前「シスコ <デバイスのホスト名> 認証」を使用して、デフォルトのバナーを表示します。
- **file** *filename* のキーワードと引数のペアを指定して **banner** コマンドを使用する：指定したカスタム HTML ファイルからバナーを表示します。 カスタム HTML ファイルは、デバイスのディスクまたはフラッシュ メモリに保存する必要があります。

- **text** *banner-text* のキーワードと引数のペアを指定して **banner** コマンドを使用する：指定したテキストが表示されます。 このテキストには、必要なすべての HTML タグを含める必要があります。

（注） **banner** コマンドがイネーブルではない場合、ユーザ名とパスワードを入力するテキスト ボックスを除き、ログイン ページには何も表示されません。

例

次に、webauth_banner.html という名前のフラッシュ ファイルがバナーに指定されている例を示します。

```
parameter-map type webauth MAP_1
 type webauth
 banner file flash:webauth_banner.html
```

次に、区切り文字として「c」を使用して「login page banner」というメッセージを設定する方法と、その結果として表示される設定出力の例を示します。

```
Device(config-params-parameter-map)# banner text c login page banner c
parameter-map type webauth MAP_2
 type webauth
 banner text ^c login page banner ^c
```

（注） 設定出力には、入力した区切り文字の前にキャレット記号（^）が自動的に表示されます。

関連コマンド

コマンド	説明
consent email	Web 認証ログイン Web ページで、ユーザの電子メール アドレスを要求します。
redirect（パラメータ マップ Web 認証）	Web ベースの認証中に、ユーザを特定の URL にリダイレクトします。
show ip admission status banner	Web認証用に設定されているバナーに関する情報を表示します。

class

制御ポリシー内の 1 つ以上のアクションに制御クラスを関連付けるには、コントロール ポリシー マップ クラス コンフィギュレーション モードで **class** コマンドを使用します。 制御ポリシーから制御クラスを削除するには、このコマンドの **no** 形式を使用します。

priority-number **class** {*control-class-name*| **always**} [**do-all**| **do-until-failure**| **do-until-success**]

no *priority-number*

構文の説明

priority-number	ポリシー ルール内の制御クラスの相対優先度。このプライオリティによって、制御ポリシーをセッションに適用する順序が決定されます。範囲：1 ～ 254。プライオリティは 1 が最も高く、254 が最も低くなります。
control-class-name	**class-map type control subscriber** コマンドによって定義された、以前に設定された制御クラスの名前。
always	常に true と評価されるデフォルト制御クラスを作成します。
do-all	（任意）アクションをすべて実行します。
do-until-failure	（任意）アクションの 1 つが失敗するまで、アクションを順に実行します。 これはデフォルトの動作です。
do-until-success	（任意）アクションの 1 つが成功するまで、アクションを順に実行します。

コマンド デフォルト

制御クラスは制御ポリシーに関連付けられません。

コマンド モード

コントロール ポリシー マップ クラス コンフィギュレーション（config-class-control-policymap）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

class コマンドは、制御クラス内の条件を制御ポリシー内の 1 つ以上のアクションに関連付けます。制御クラスは、一連のアクションを実行するために満たす必要がある条件を定義します。制御クラスと一連のアクションのアソシエーションは、制御ポリシー ルールと呼ばれます。

control-class-name 引数を使用して、**class-map type control subscriber** コマンドを使用して作成された名前付きの制御クラスを指定します。

always キーワードを使用して、指定されたイベントに対して常に true と評価されるデフォルトの制御クラスを作成します。

例

次に、DOT1X_NO_AGENT という名前の制御クラスを設定する例を示します。 **class** コマンドは DOT1X_NO_AGENT を POLICY_1 という名前の制御ポリシーに関連付けます。 DOT1X_NO_AGENT で true と評価されると、そのクラスに関連付けられたアクションが実行されます。

```
class-map type control subscriber match-first DOT1X_NO_AGENT
 match result-type method dot1x agent-not-found
!
policy-map type control subscriber POLICY_1
 event session-started match-all
  10 class always do-all
   10 authenticate using dot1x priority 10
 event authentication-failure match-first
  10 class DOT1X_NO_AGENT do-all
   10 authenticate using mab priority 20
  20 class DOT1X_TIMEOUT do-all
   10 authenticate using mab priority 20
  30 class DOT1X_FAILED do-all
   10 authenticate using mab priority 20
```

関連コマンド

コマンド	説明
class-map type control subscriber	制御クラスを作成します。これは、制御ポリシーのアクションが実行される条件を定義します。
event	条件が満たされる場合に、制御ポリシーでアクションをトリガーするイベントのタイプを指定します。
policy-map type control subscriber	加入者セッションの制御ポリシーを定義します。

class-map type control subscriber

制御ポリシーのアクションが実行される条件を定義する制御クラスを作成するには、グローバル コンフィギュレーション モードで **class-map type control subscriber** コマンドを使用します。 制御クラスを削除するには、このコマンドの **no** 形式を使用します。

class-map type control subscriber {**match-all| match-any| match-none**} *control-class-name*

no class-map type control subscriber {**match-all| match-any| match-none**} *control-class-name*

構文の説明

match-all	制御クラスのすべての条件が true と評価される必要があることを指定します。
match-any	制御クラスの少なくとも 1 つの条件が true と評価される必要があることを指定します。
match-none	制御クラスのすべての条件が false と評価される必要があることを指定します。
control-class-name	制御クラスの名前。

コマンド デフォルト

制御クラスは作成されません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

制御クラスは、制御ポリシーのアクションを実行するために満たす必要のある条件を定義します。制御クラスには複数の条件を含めることができます。 **match-any**、**match-all**、または **match-none** キーワードを使用して、アクションが実行されるために加入者セッションが満たす必要のある条件を指定します (条件がある場合)。

policy-map type control subscriber コマンドで設定される制御ポリシーには、**event** コマンドで指定されるイベントに基づいて評価される 1 つ以上の制御クラスが含まれます。 **class** コマンドを使用して、制御クラスを 1 つ以上のアクションに関連付けることでポリシー ルールを作成します。

例

次に、DOT1X_MAB_WEBAUTH という名前の制御ポリシーに関連付けられた、DOT1X_AUTHORITATIVE という名前の制御クラスの一部の設定例を示します。 認証失敗イベントが発生し、セッションが DOT1X_AUTHORITATIVE のすべての条件に一致する場合、ポリシーは認証処理を実行し、MAC認証バイパス（MAB）を使用してセッションを認証しようとします。

```
class-map type control subscriber match-all DOT1X_AUTHORITATIVE
  match method dot1x
  match result-type authoritative
!
policy-map type control subscriber DOT1X_MAB_WEBAUTH
  event session-started match-all
   10 class always do-until-failure
    10 authenticate using dot1x retries 3 retry-time 15
  event authentication-failure match-all
   10 class DOT1X_AUTHORITATIVE
    10 authenticate using mab
   .
   .
   .
```

関連コマンド

コマンド	説明
class	制御ポリシーの 1 つ以上のアクションに制御クラスを関連付けます。
event	条件が満たされる場合に、制御ポリシーでアクションをトリガーするイベントのタイプを指定します。
policy-map type control subscriber	加入者セッションの制御ポリシーを定義します。

clear-authenticated-data-hosts-on-port

認証が失敗した後に、ポート上の認証済みのデータホストをクリアするには、コントロールポリシー マップ アクション コンフィギュレーション モードで **clear-authenticated-data-hosts-on-port** コマンドを使用します。 制御ポリシーからこのアクションを削除するには、このコマンドの **no** 形式を使用します。

action-number **clear-authenticated-data-hosts-on-port**

no *action-number*

構文の説明

action-number	アクション数。 アクションは、ポリシー ルール内で順番に実行されます。

コマンド デフォルト

ポート上のホストは消去されません。

コマンド モード

コントロールポリシーマップアクション コンフィギュレーション（config-action-control-policymap）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

clear-authenticated-data-hosts-on-port コマンドは、制御ポリシーにアクションを定義します。

制御ポリシーによって、指定されたイベントと条件に応じて実行されるアクションが決定されます。 制御クラスによって、アクションを実行するために満たす必要がある条件が定義されます。 アクションは、ポリシー ルール内で番号が付けられ、順番に実行されます。

class コマンドは、制御クラスを 1 つ以上のアクションに関連付けることでポリシー ルールを作成します。 ポリシー ルールに定義できるアクションは、**event** コマンドによって指定されるイベントのタイプによって異なります。

例

次に、認証失敗イベントに設定されている clear-authenticated-data-hosts-on-port アクションと制御ポリシーを設定する方法を示します。

```
policy-map type control subscriber POLICY_Et0/0
 event session-started match-all
  10 class always do-until-failure
```

```
  10 authenticate using dot1x priority 10
event authentication-failure match-first
 10 class AAA_SVR_DOWN_UNAUTHD_HOST do-until-failure
  10 activate service-template VLAN123
  20 authorize
  30 pause reauthentication
  40 clear-authenticated-data-hosts-on-port
 20 class AAA_SVR_DOWN_AUTHD_HOST do-until-failure
  10 pause reauthentication
  20 authorize
 30 class always do-until-failure
  10 terminate dot1x
  20 authentication-restart 60
event agent-found match-all
 10 class always do-until-failure
  10 authenticate using dot1x priority 10
```

関連コマンド

コマンド	説明
class	制御ポリシーの 1 つ以上のアクションに制御クラスを関連付けます。
clear-session	アクティブな加入者セッションをクリアします。
event	条件が満たされる場合に、制御ポリシーでアクションをトリガーするイベントのタイプを指定します。

clear-session

アクティブな加入者セッションをクリアするには、コントロール ポリシー マップ アクション コンフィギュレーション モードで **clear-session** コマンドを使用します。 制御ポリシーからこのアクションを削除するには、このコマンドの **no** 形式を使用します。

action-number **clear-session**

no *action-number*

構文の説明

action-number	アクション数。 アクションは、ポリシー ルール内で順番に実行されます。

コマンド デフォルト

セッションは、クリアされません。

コマンド モード

コントロール ポリシーマップ アクション コンフィギュレーション（config-action-control-policymap）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

clear-session コマンドは、制御ポリシーにアクションを定義します。

制御ポリシーによって、指定されたイベントと条件に応じて実行されるアクションが決定されます。 制御クラスによって、アクションを実行するために満たす必要がある条件が定義されます。 アクションは、ポリシー ルール内で番号が付けられ、順番に実行されます。

class コマンドは、制御クラスを 1 つ以上のアクションに関連付けることでポリシー ルールを作成します。 ポリシー ルールに定義できるアクションは、**event** コマンドによって指定されるイベントのタイプによって異なります。

例

次に、非アクティブ タイムアウト イベントに設定された clear-session アクションと制御ポリシーを設定する方法を示します。

```
policy-map type control subscriber POLICY
 event session-started match-all
  10 class always do-all
   10 authenticate using dot1x
```

```
event authentication-failure match-all
 10 class DOT1X_NO_AGENT do-all
  10 activate fallback template VLAN510
event inactivity-timeout match-all
 10 class always do-all
  10 clear-session
```

関連コマンド

コマンド	説明
class	制御ポリシーの 1 つ以上のアクションに制御クラスを関連付けます。
event	条件が満たされる場合に、制御ポリシーでアクションをトリガーするイベントのタイプを指定します。

consent email

承諾ログイン Web ページでユーザの電子メールアドレスを要求するには、パラメータ マップ Web 認証コンフィギュレーション モードで **consent email** コマンドを使用します。 マップから承諾パラメータ ファイルを削除するには、このコマンドの **no** 形式を使用します。

consent email

no consent email

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

承諾ログイン ページで、電子メール アドレスは要求されません。

コマンド モード

パラメータ マップ Web 認証コンフィギュレーション（config-params-parameter-map）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

consent email コマンドを使用して、承諾ログイン ページにテキスト ボックスを表示し、識別用にユーザの電子メールアドレスを入力するように求めます。デバイスは認証、許可、およびアカウンティング（AAA）サーバに、クライアントの MAC アドレスではなく、この電子メール アドレスを送信します。

承諾機能を使用して、承諾 Web ページを表示することで、有線および無線ネットワークを使用した一時的なインターネットおよび企業内アクセスをエンドユーザに提供できます。 この Web ページには、組織がエンド ユーザにアクセス権を付与するための条項と条件が記載されています。 ユーザは、承諾 Web ページの利用条件を承諾しなければネットワークに接続できません。

type コマンドを consent に設定してパラメータ マップを作成すると、デバイスはユーザのユーザ名とパスワードの各資格情報をユーザに要求しません。 代わりに、ユーザは同意するか同意しないことを示す 2 つのオプション ボタンを選択できます。 ユーザ名を使用できない場合 (同意がイネーブルになっているため)、アカウンティング用にデバイスはクライアントの MAC アドレスを AAA サーバに送信します。

このコマンドは、名前付きパラメータ マップでのみサポートされます。

例

次に、承諾電子メール機能をイネーブルにしてパラメータ マップを設定する例を示します。

```
parameter-map type webauth PMAP_1
 type consent
 consent email
 banner file flash:consent_page.htm
```

関連コマンド

コマンド	説明
banner（パラメータ マップ Web 認証）	Web 認証ログイン Web ページにバナーを表示します。
custom-page	Web 認証ログイン時にカスタム Web ページが表示されます。
type（パラメータ マップ Web 認証）	パラメータ マップでサポートされる方式を定義します。

custom-page

Web認証ログイン中にカスタムWebページを表示するには、パラメータマップWeb認証コンフィギュレーション モードで **custom-page** コマンドを使用します。 カスタム Web ページをディセーブルにするには、このコマンドの **no** 形式を使用します。

custom-page {**failure**| **login [expired]**| **success**} **device** *location*:*filename*

no custom-page {**failure**| **login [expired]**| **success**} **device** *location*:*filename*

構文の説明

failure	ログインが失敗した場合に、カスタムWebページを表示します。
login	ログイン時に、カスタム Web ページを表示します。
expired	（任意）ログインの期限が切れたときに、カスタム Web ページを表示します。
success	ログインが成功した場合に、カスタムWebページを表示します。
location **:***filename*	指定された条件に応じて、デフォルトのHTMLファイルの代わりに使用する、ローカル側に保存された HTML ファイルの場所および名前。

コマンド デフォルト

内部デフォルト Web ページが表示されます。

コマンド モード

パラメータ マップ Web 認証コンフィギュレーション（config-params-parameter-map）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

custom-page コマンドを使用して、Web 認証ログイン中にカスタム Web ページを表示します。 カスタム Web ページをイネーブルにするには：

- 4 つのカスタム HTML ファイルをすべて指定する必要があります。 4 つ未満のファイルが指定されている場合は、内部デフォルト HTML ページが使用されます。
- 4 つのカスタム HTML ファイルとカスタム ページ内のすべてのイメージは、スイッチのディスクまたはフラッシュ メモリに保存する必要があります。 各 HTML ファイルの最大サイズは 256 KB です。
- ファイル名は web_auth で開始する必要があります。
- 外部サーバからカスタム ページとイメージを提供するには、ローカル カスタム ページを使用するのではなく、**redirect**（パラメータ マップ Web 認証）コマンドを使用して、リダイレクト ポータル IP アドレスを設定する必要があります。
- カスタム ページからの外部リンクはすべて、インターセプト ACL の設定が必要です。
- 外部リンクまたはイメージに必要なすべての名前解決では、インターセプト ACL の設定が必要です。
- カスタム Web ページ機能がイネーブルである場合、成功ログイン機能のリダイレクション URL は利用不可能です。
- カスタム ログイン ページはパブリック Web 形式であるため、このページについて次の注意事項に留意してください。
  - ログイン形式では、ユーザ名およびパスワードのユーザ入力を受け入れて、そのデータを uname および pwd として POST する必要があります。
  - カスタム ログイン ページは、ページ タイムアウト、暗号化されたパスワード、冗長送信の防止など、Web フォームに対するベスト プラクティスに従う必要があります。

例

次に、カスタムページをイネーブルにして、Web認証用の名前付きパラメータ マップを設定する例を示します。

```
parameter-map type webauth PMAP_WEBAUTH
 type webauth
 custom-page login device flash:webauth_login.html
 custom-page success device flash:webauth_success.html
 custom-page failure device flash:webauth_fail.html
 custom-page login expired device flash:webauth_expire.html
```

関連コマンド

コマンド	説明
banner（パラメータ マップ Web 認証）	Web 認証ログイン Web ページにバナーを表示します。
consent email	承諾ログイン Web ページでユーザの電子メール アドレスを要求します。

コマンド	説明
redirect（パラメータ マップ Web 認証）	Webベースの認証中に、クライアントを特定のURL にリダイレクトします。

deactivate

加入者セッションで、制御ポリシーまたはサービス テンプレートを非アクティブ化するには、コントロール ポリシー マップ アクション コンフィギュレーション モードで **deactivate** コマンドを使用します。 制御ポリシーからこのアクションを削除するには、このコマンドの **no** 形式を使用します。

action-number **deactivate** {**policy type control subscriber** *control-policy-name*| **service-template** *template-name*}

no *action-number*

構文の説明

action-number	アクション数。 アクションは、ポリシー ルール内で順番に実行されます。
policy type control subscriber *control-policy-name*	**policy-map type control subscriber** コマンドによって定義されているように、セッションで非アクティブ化する制御ポリシーの名前を指定します。
service-template *template-name*	**service-template** コマンドによって定義されているように、セッションで非アクティブ化するサービス テンプレートの名前を指定します。

コマンド デフォルト

制御ポリシーまたはサービス テンプレートは非アクティブ化されません。

コマンド モード

コントロール ポリシー マップ アクション コンフィギュレーション（config-action-control-policymap）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

deactivate コマンドは、制御ポリシーにアクションを定義します。 このコマンドは、セッションに適用されたすべての制御ポリシーとポリシー属性をアンインストールします。

制御ポリシーによって、指定されたイベントと条件に応じて実行されるアクションが決定されます。 制御クラスによって、アクションを実行するために満たす必要がある条件が定義されます。アクションは、ポリシー ルール内で番号が付けられ、順番に実行されます。

class コマンドは、制御クラスを 1 つ以上のアクションに関連付けることでポリシー ルールを作成します。

例

次に、認証が失敗した場合でも、すべてのホストへの限定されたアクセスを提供する制御ポリシーを設定する方法を示します。 認証が成功すると、ポリシーマネージャはLOW_IMPACT_TEMPLATEという名前のサービス テンプレートを非アクティブ化し、RADIUS サーバによってダウンロードされたポリシーに基づいてアクセス権を付与します。

```
class-map type control subscriber match-all DOT1X_MAB_FAILED
 no-match result-type method dot1x success
 no-match result-type method mab success
!
policy-map type control subscriber CONCURRENT_DOT1X_MAB_LOW_IMP_MODE
 event session-started match-all
  10 class always do-until-failure
   10 authorize
   20 activate service-template LOW_IMPACT_TEMPLATE
   30 authenticate using mab
   40 authenticate using dot1x
 event authentication-success match-all
  10 class always do-until-failure
   10 deactivate service-template LOW_IMPACT_TEMPLATE
 event authentication-failure match-first
  10 class DOT1X_MAB_FAILED do-until-failure
   10 authorize
   20 terminate dot1x
   30 terminate mab
 event agent-found match-all
  10 class always do-until-failure
   10 authenticate using dot1x
 event inactivity-timeout match-all
  10 class always do-until-failure
   10 clear-session
```

関連コマンド

コマンド	説明
activate（ポリシー マップ アクション）	加入者セッションで、制御ポリシーまたはサービス テンプレートをアクティブ化します。
class	制御ポリシーの 1 つ以上のアクションに制御クラスを関連付けます。
policy-map type control subscriber	加入者セッションの制御ポリシーを定義します。
service-template	加入者セッションに適用する一連のポリシー属性を含むサービステンプレートを定義します。

debug access-session

Session Aware Networking セッションに関するデバッグ情報を表示するには、特権 EXEC モードで **debug access-session** コマンドを使用します。 デバッグ出力をディセーブルにするには、このコマンドの **no** 形式を使用します。

debug access-session [**feature** *feature-name*] {**all**| **detail**| **errors**| **events**| **sync**}

no debug access-session [**feature** *feature-name*] {**all**| **detail**| **errors**| **events**| **sync**}

構文の説明

feature *feature-name*	（任意）特定の機能に関するデバッグ情報を表示します。有効な機能名を表示するには、疑問符（**?**）オンライン ヘルプ機能を使用します。
all	Session Aware Networking のすべてのデバッグ情報を表示します。
detail	詳細なデバッグ情報を表示します。
errors	エラーに関するデバッグ情報を表示します。
events	イベントに関するデバッグ情報を表示します。
sync	ステートフル スイッチオーバー（SSO）または、In Service Software Upgrade（ISSU）に関するデバッグ情報を表示します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

debug access-session コマンドを使用して、Session Aware Networking セッションのトラブルシューティングを行います。

関連コマンド

コマンド	説明
debug authentication	Authentication Manager に関するデバッグ情報を表示します。
debug dot1x	802.1X デバッグ情報を表示します。
show access-session	Session Aware Networking セッションに関する情報を表示します。

debug ip admission

Web 認証のデバッグ情報を表示するには、特権 EXEC モードで **debug ip admission** コマンドを使用します。 デバッグ出力をディセーブルにするには、このコマンドの **no** 形式を使用します。

Cisco IOS XE Release 3SE and Later Releases

debug ip admission {**aaa**| **acl**| **all**| **dos**| **eapoudp**| **error**| **ha**| **httpd**| **idle**| **input-feature**| **io**| **page**| **qualify**| **session**| **sm**| **state**| **timer**}

no debug ip admission {**aaa**| **acl**| **all**| **dos**| **eapoudp**| **error**| **ha**| **httpd**| **idle**| **input-feature**| **io**| **page**| **qualify**| **session**| **sm**| **state**| **timer**}

All Other Releases

debug ip admission {**api**| **consent**| **detailed**| **dos**| **eapoudp**| **error**| **ezvpn**| **fallback**| **function-trace**| **httpd**| **object-creation**| **object-deletion**| **timers**}

no debug ip admission {**api**| **consent**| **detailed**| **dos**| **eapoudp**| **error**| **ezvpn**| **fallback**| **function-trace**| **httpd**| **object-creation**| **object-deletion**| **timers**}

構文の説明

aaa	IPアドミッションの認証、許可、およびアカウンティング（AAA）イベントを表示します。
acl	IP アドミッションのアクセス コントロール リスト（ACL）イベントを表示します。
all	すべての IP アドミッションのデバッグ情報を表示します。
dos	認証プロキシの DOS 防止イベントを表示します。
eapoudp	User Datagram Protocol（UDP）（EAPoUDP）ネットワーク アドミッション制御イベントを介した拡張認証プロトコルに関する情報を表示します。
error	Web 認証エラー メッセージを表示します。
ha	ハイ アベイラビリティ（HA）イベントを表示します。
httpd	Web認証HTTPデーモンの情報を表示します。
idle	レイヤ 3（L3）アイドル タイマー イベントを表示します。

input-feature	IPアドミッション入力機能イベントを表示します。
io	IP アドミッション HTTP プロキシ デーモン入出力イベントを表示します。
page	IPアドミッションHTTPページのイベントを表示します。
qualify	IP アドミッション パケットの資格情報を表示します。
session	IP アドミッション セッション イベントを表示します。
sm	IP アドミッション セッション マネージャ イベントを表示します。
state	IP アドミッションの状態遷移を表示します。
timers	認証プロキシのタイマー関連のイベントを表示します。
api	IPアドミッションAPIイベントを表示します。
consent	Web 認証の承諾ページの情報を表示します。
detailed	認証プロキシの処理中に TCP イベントの詳細を表示します。詳細は、すべてのFTP、HTTP、およびTelnetプロトコルに対して汎用的です。
ezvpn	認証プロキシ Easy VPN（EzVPN）関連イベントを表示します。
fallback	IP アドミッション フォールバック イベントを表示します。
function-trace	認証プロキシ機能を表示します。
object-creation	認証プロキシのキャッシュへの追加エントリを表示します。
object-deletion	認証プロキシのキャッシュエントリの削除を表示します。

コマンド デフォルト　特権 EXEC（#）セーブルです。

コマンド履歴

リリース	変更内容
12.3(8)T	このコマンドが導入されました。
12.2(33)SXI	このコマンドが、Cisco IOS Release 12.2(33)SXI に統合されました。
Cisco IOS XE Release 3.2SE	このコマンドが変更されました。**aaa**、**acl**、**all**、**dos**、**ha**、**idle**、**input-feature**、**io**、**page**、**qualify**、**session**、**sm**、および **state** キーワードが追加されました。

使用上のガイドライン

debug ip admission コマンドを使用して、Web 認証のトラブルシューティングを行います。

例

次に、**debug ip admission eapoudp** コマンドの出力例を示します。

```
Device# debug ip admission eapoudp

Posture validation session created for client mac= 0001.027c.f364 ip= 10.0.0.1
Total Posture sessions= 1 Total Posture Init sessions= 1
*Apr  9 19:39:45.684: %AP-6-POSTURE_START_VALIDATION: IP=10.0.0.1|
Interface=FastEthernet0/0.420
*Apr  9 19:40:42.292: %AP-6-POSTURE_STATE_CHANGE: IP=10.0.0.1| STATE=POSTURE ESTAB
*Apr  9 19:40:42.292: auth_proxy_posture_parse_aaa_attributes:
CiscoDefined-ACL name= #ACSACL#-IP-HealthyACL-40921e54
Apr  9 19:40:42.957: %AP-6-POSTURE_POLICY: Apply access control list
(xACSACLx-IP-HealthyACL-40921e54) policy for host (10.0.0.1)
```

関連コマンド

debug access-session	Session Aware Networking セッションに関するデバッグ情報を表示します。
show ip admission	ネットワーク アドミッション制御（NAC）のキャッシュ エントリまたは NAC 設定を表示します。

description（サービス テンプレート）

サービス テンプレートに説明を追加するには、サービス テンプレート コンフィギュレーション モードで **description** コマンドを使用します。 説明を削除するには、このコマンドの **no** 形式を使用します。

description *description*

no description *description*

構文の説明

description	サービス テンプレートの説明。

コマンド デフォルト

説明は、サービス テンプレートでは表示されません。

コマンド モード

サービス テンプレート コンフィギュレーション（config-service-template）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

description コマンドを使用して、サービス テンプレート コンフィギュレーションを表示するときに、サービス テンプレートに関する追加情報を提供します。

例

次に、説明付きでサービス テンプレートを設定する例を示します。

```
service-template SVC_2
 description label for SVC_2
 access-group ACL_2
 redirect url http://www.cisco.com
 inactivity-timer 15
 tag TAG_2
```

関連コマンド

コマンド	説明
show service-template	サービス テンプレートに関する情報を表示します。

err-disable

セキュリティ違反が発生した後、ポートをディセーブルにするには、コントロールポリシーマップアクション コンフィギュレーション モードで **err-disable** コマンドを使用します。 制御ポリシーからこのアクションを削除するには、このコマンドの **no** 形式を使用します。

action-number **err-disable**

no *action-number*

構文の説明

action-number	アクション数。 アクションは、ポリシー ルール内で順番に実行されます。

コマンド デフォルト

ポートはディセーブルではありません。

コマンド モード

コントロールポリシーマップアクション コンフィギュレーション（config-action-control-policymap）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

err-disable コマンドは、制御ポリシーにアクションを定義します。

制御ポリシーによって、指定されたイベントと条件に応じて実行されるアクションが決定されます。 制御クラスはポリシーがアクションを実行ために満たす必要がある条件を定義します。 アクションは、ポリシー ルール内で番号が付けられ、順番に実行されます。

class コマンドは、制御クラスを 1 つ以上のアクションに関連付けることでポリシー ルールを作成します。 ポリシーに定義できるアクションは、**event** コマンドで指定するイベントのタイプによって異なります。

ポリシーでこのアクションを実行した後、**error recovery interval** コマンドで設定された時間が経過するまで（デフォルトは 300 秒）、ポートはディセーブルのままになります。 **errdisable recovery cause security-violation** コマンドを使用してエラー リカバリをイネーブルにしていなかった場合、ポートは無期限にディセーブルのままになります。

例

次に、err-disable アクションを設定して制御ポリシーを設定する例を示します。

```
policy-map type control subscriber POLICY_1
 event violation match-all
  10 class always do-until-failure
   10 err-disable
```

関連コマンド

コマンド	説明
errdisable recovery	リカバリ メカニズムの変数を設定します。
event	条件が満たされる場合に、制御ポリシーでアクションをトリガーするイベントのタイプを指定します。
restrict	ポートでセキュリティ違反が発生した後に、違反パケットをドロップし、syslog メッセージを生成します。

event

条件が満たされる場合に、制御ポリシーでアクションをトリガーするイベントのタイプを指定するには、コントロール ポリシー マップ イベント コンフィギュレーション モードで **event** コマンドを使用します。 イベント条件を削除するには、このコマンドの **no** 形式を使用します。

event *event-name* [**match-all**| **match-first**]

no event *event-name* [**match-all**| **match-first**]

構文の説明

event-name	制御クラスの条件が満たされた後にアクションをトリガーするイベントのタイプ。 有効なキーワードは次のとおりです。 • **aaa-available**：以前は到達不能であった認証、許可、およびアカウンティング（AAA）サーバを使用できるようになりました。 • **absolute-timeout**：セッションで期限切れになった絶対タイマー。 このタイマーは、**absolute-timer** コマンドで設定されます。 • **agent-found**：認証方式用のエージェントが正常に検出されました。 • **authentication-failure**：セッション認証が失敗しました。 • **authentication-success**：セッションは正常に認証されました。 • **authorization-failure**：ポートへの許可の適用に失敗しました。 • **inactivity-timeout**：セッションの非アクティブタイマーが期限切れになりました。このタイマーは、**inactivity-timer** コマンドで設定されます。 • **session-started**：ポップアップ イベントにより、セッションが作成されました。 これは、新しいMACアドレスが関連するインターフェイス上で検出された場合にトリガーされます。

	• **tag-added**：サービス テンプレート タグが追加されました。 このタグは、**tag** (service-template) コマンドで指定されます。 • **tag-removed**：サービス テンプレート タグが削除されました。 • **template-activated**：サービス テンプレートがセッションでアクティブ化されました。 • **template-activation-failed**：セッションでのサービス テンプレートのアクティブ化に失敗しました。 • **template-deactivated**：セッションでサービス テンプレートが非アクティブ化されました。 • **template-deactivation-failed**：セッションでのサービス テンプレートの非アクティブ化に失敗しました。 • **timer-expiry**：セッションで開始されたタイマーが期限切れになりました。 これは、**set-timer**（ポリシー マップ アクション）コマンドで開始されたタイマーです。 • **violation**：セッション違反が検出されました。
match-all	（任意）すべての制御クラスを評価します。 これはデフォルトの動作です。
match-first	（任意）最初の制御クラスのみを評価します。

コマンド デフォルト　イベントは、制御ポリシーに設定されません。

コマンド モード　コントロール ポリシーマップ イベント コンフィギュレーション（config-event-control-policymap）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

event コマンドは、制御ポリシーにイベント条件を設定します。 指定されたイベントが発生すると、システムは制御クラスを評価します。 制御クラスは制御ポリシーのアクションを実行するための条件を指定します。 **class** コマンドは、制御クラスを 1 つ以上のアクションに関連付けることでポリシー ルールを作成します。

event コマンドは、ポリシー ルールに定義できるアクションを判別します。 たとえば、**err-disable** コマンドを使用して定義されたアクションを違反イベントに対してのみ設定できます。

次の表に、デフォルト アクションがあるイベントを示します。

表 *1*：デフォルト アクションを含むイベント

Event	デフォルト アクション
authentication-failure	Session Manager は違反があるかどうかをチェックし、制御ポリシーによって明示的に許可が指定されている場合を除き、他の方式がまだ実行されていない場合はセッションを無許可に設定します。
authentication-success	Session Manager は、制御ポリシーによって明示的に無許可が指定されている場合を除き、セッションを許可します。
authorization-failure	Session Manager は、制御ポリシーによって明示的に許可が指定されている場合を除き、セッションを無許可にします。
violation	Session Manager は、制御ポリシーによって明示的に別のアクションが指定されている場合を除き、ポートに制限違反を生成します。

例

次に、POLICY_3 という名前の制御ポリシーを設定する方法を示します。 この制御ポリシーには、関連付けられた 2 つのイベントがあります。1 つはセッションの作成用であり、もう 1 つは認証失敗用です。 認証失敗イベントには、関連付けられた 2 つの制御クラスがあります。

```
class-map type control subscriber match-all MAB_FAILED
 match method mab
 match result-type authoritative
!
policy-map type control subscriber POLICY_3
 event session-started match-all
  10 class always do-all
   10 authenticate using mab priority 20
 event authentication-failure match-all
  10 class MAB_FAILED do-all
   10 authenticate using dot1x priority 10
  20 class DOT1X_FAILED do-all
   10 terminate dot1x
   20 activate service-template VLAN4
```

関連コマンド

コマンド	説明
class-map type control subscriber	制御ポリシーのアクションを実行するために満たす必要のある条件を指定する制御クラスを定義します。
policy-map type control subscriber	加入者セッションの制御ポリシーを定義します。

inactivity-timer

加入者セッションの非アクティブタイムアウトをイネーブルにするには、サービステンプレートコンフィギュレーション モードで **inactivity-timer** コマンドを使用します。 このタイマーをディセーブルにするには、このコマンドの **no** 形式を使用します。

inactivity-timer *minutes* **[probe]**

no inactivity-timer

構文の説明

minutes	セッションを非アクティブにできる最大時間（分）。 範囲は 0 ～ 65535 です。 デフォルトは 0 で、タイマーは無効になっています。
probe	（任意）アドレス解決プロトコル(ARP)プローブをイネーブルにします。 これらのプローブはセッションを終了する前に送信されます。

コマンド デフォルト

ディセーブル（非アクティブ タイムアウトは 0）。

コマンド モード

サービス テンプレート コンフィギュレーション（config-service-template）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

inactivity-timer コマンドを使用して、エンド クライアントからのアクティビティやデータがない状態で加入者セッションが存在できる最大時間を設定します。 アクティビティまたはデータが得られる前にこのタイマーが切れると、セッションはクリアされます。

probe キーワードにより、ARP プローブがイネーブルになります。 IP デバイス トラッキング テーブルには、既知のホスト デバイスのリストが保持され、それらデバイスがアクティブな状態を保っていることを確認するために、定期的にデバイスをプローブします。 すべてのプローブが無応答になると、セッションがクリアされます。 ホストは非アクティブ タイムアウト後に IP デバイス トラッキング テーブルから削除されるため、それ以上のプローブは送信されず、非アクティ

ブなエンド ホストはセッションを再起動するために ARP トラフィックを送信する必要があります。

ARP プローブの回数および間隔を設定するには、**ip device tracking probe** コマンドを使用します。

例

次に、アクティビティ タイマーを 15 分に設定してサービス テンプレートを設定する例を示します。

```
service-template SVC_2
 description label for SVC_2
 access-group ACL_2
 redirect url http://www.cisco.com
 inactivity-timer 15
```

関連コマンド

コマンド	説明
absolute-timer	加入者セッションに対して絶対タイムアウトをイネーブルにします。
authenticate using	指定した方式を使用して、加入者セッションを認証します。
ip device tracking probe	デバイスのプローブのトラッキングをイネーブルにします。
show service-template	サービス テンプレートに関する情報を表示します。

key-wrap enable

RADIUS サーバで Advanced Encryption Standard（AES）キー ラップをイネーブルにするには、サーバ グループ コンフィギュレーション モードで **key-wrap enable** コマンドを使用します。 キー ラップをディセーブルにするには、このコマンドの **no** 形式を使用します。

key-wrap enable

no key-wrap enable

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

キー ラップ機能はディセーブルです。

コマンド モード

サーバ グループ コンフィギュレーション（config-sg-radius）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

key-wrap enable コマンドを使用して、AES キー ラップ機能をイネーブルにします。 AES キー ラップ機能により、コントローラと RADIUS サーバ間の共有秘密の安全性が高まります。 AES キー ラップは、Federal Information Processing Standards（FIPS）を使用するユーザのために設計されており、キー ラップ準拠の RADIUS 認証サーバを必要とします。

例

次に、キー ラップ サポートをイネーブルにして、LAB_RAD という名前の RADIUS サーバ グループを設定する例を示します。

```
aaa group server radius LAB_RAD
 key-wrap enable
 subscriber mac-filtering security-mode mac
 mac-delimiter colon
```

関連コマンド

コマンド	説明
mac-delimiter	RADIUS の互換モード用の MAC デリミタを指定します。

コマンド	説明
radius-server host	RADIUS サーバ ホストを指定します。
subscriber mac-filtering security-mode	MAC フィルタリング用の RADIUS 互換モードを指定します。

mac-delimiter

RADIUS 互換性モード用の MAC デリミタを指定するには、サーバ グループ コンフィギュレーション モードで **mac-delimiter** コマンドを使用します。 デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

mac-delimiter {**colon**| **hyphen**| **none**| **single-hyphen**}

no mac-delimiter {**colon**| **hyphen**| **none**| **single-hyphen**}

構文の説明

colon	xx:xx:xx:xx:xx:xx の形式で、デリミタをコロンに設定します。
hyphen	xx-xx-xx-xx-xx-xx の形式で、デリミタをハイフン（-）に設定します。
none	xxxxxxxxxxxx の形式で、デリミタを設定しません。 768 ビットは、デフォルト値です。
single-hyphen	xxxxxx-xxxxxx の形式で、デリミタを単一ハイフンに設定します。

コマンド デフォルト

MAC デリミタは設定されません。

コマンド モード

サーバ グループ コンフィギュレーション（config-sg-radius）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

mac-delimiter コマンドを使用して、RADIUS 認証サーバに送信される MAC アドレスに使用されるデリミタを設定します。

例

次に、コロンに設定された MAC デリミタを使用して、RADIUS サーバ グループを設定する例を示します。

```
aaa group server radius LAB_RAD
 key-wrap enable
 subscriber mac-filtering security-mode mac
 mac-delimiter colon
```

関連コマンド

コマンド	説明
key-wrap enable	AES キー ラップをイネーブルにします。
subscriber mac-filtering security-mode	MAC フィルタリング用の RADIUS 互換モードを指定します。

match activated-service-template

セッションでアクティブ化されているサービス テンプレートに基づいて true と評価される条件を作成するには、コントロール クラス マップ フィルタ コンフィギュレーション モードで **match activated-service-template** コマンドを使用します。 セッションでアクティブ化されているサービス テンプレートと指定されたテンプレートが一致しない場合に true と評価される条件を作成するには、コントロール クラス マップ フィルタ コンフィギュレーション モードで **no-match activated-service-template** コマンドを使用します。 条件を削除するには、このコマンドの **no** 形式を使用します。

match activated-service-template *template-name*

no-match activated-service-template *template-name*

no {**match**| **no-match**} **activated-service-template** *template-name*

構文の説明

template-name	**service-template** コマンドによって定義された、設定済みのサービス テンプレートの名前。

コマンド デフォルト

制御クラスには、サービス テンプレートに基づいた条件は含まれません。

コマンド モード

コントロール クラス マップ フィルタ コンフィギュレーション（config-filter-control-classmap）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

match activated-service-template コマンドは、セッションに適用されているサービス テンプレートに基づいて、一致条件を制御クラスに設定します。 制御クラスには、複数の条件を含めることができ、それぞれの条件が true または false に評価されます。 制御クラスは、制御ポリシーのアクションが実行されるために、すべての条件または一部の条件が true と評価される必要があるか、あるいはいずれの条件も true と評価されない必要があるかを定義します。

このコマンドの **no-match** 形式は、一致の失敗と見なされる値を指定します。 指定された一致条件以外の他のすべての値は、一致の成功と見なされます。 たとえば、**no-match activated-service-template SVC_1** コマンドを設定すると、SVC_1 以外のすべてのテンプレート値が成功した一致として受け入れられます。

class コマンドは、制御クラスを制御ポリシーに関連付けます。

例

次に、VLAN_1 という名前のサービス テンプレートがセッションでアクティブ化されると true と評価される制御クラスを設定する例を示します。

```
class-map type control subscriber match-all CLASS_1
 match activated-service-template VLAN_1
```

関連コマンド

コマンド	説明
activate（ポリシー マップ アクション）	加入者セッションで、制御ポリシーまたはサービス テンプレートをアクティブ化します。
class	制御ポリシーの 1 つ以上のアクションに制御クラスを関連付けます。
match service-template	イベント サービス テンプレートに基づいて、true と評価される条件を作成します。
service-template	加入者セッションに適用する一連のポリシー属性を含むテンプレートを定義します。

match authorization-status

セッションの許可ステータスに基づいて true と評価される条件を作成するには、コントロール クラス マップ フィルタ コンフィギュレーション モードで **match authorization-status** コマンドを使用します。 セッションの許可ステータスが指定されたステータスと一致しない場合に true と評価される条件を作成するには、コントロール クラス マップ フィルタ コンフィギュレーション モードで **no-match authorization-status** コマンドを使用します。 条件を削除するには、このコマンドの **no** 形式を使用します。

match authorization-status {**authorized**| **unauthorized**}

no-match authorization-status {**authorized**| **unauthorized**}

no {**match**| **no-match**} **authorization-status** {**authorized**| **unauthorized**}

構文の説明

authorized	加入者が認証されたことを指定します。
unauthorized	加入者が認証されていないことを指定します。

コマンド デフォルト

制御クラスには、許可ステータスに基づいた条件は含まれません。

コマンド モード

コントロール クラス マップ フィルタ コンフィギュレーション（config-filter-control-classmap）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

match authorization-status コマンドは、セッションの許可ステータスに基づいて、一致条件を制御クラスに設定します。 制御クラスには、複数の条件を含めることができ、それぞれの条件が true または false に評価されます。 制御クラスは、制御ポリシーのアクションを実行するために、すべての条件または一部の条件が true と評価される必要があるか、あるいはいずれの条件も true と評価されない必要があるかを定義します。

このコマンドの **no-match** 形式は、一致の失敗と見なされる値を指定します。 指定された一致条件以外の他のすべての値は、一致の成功と見なされます。 たとえば、**no-match authorization-status authorized** コマンドを設定すると、無許可のステータス値が成功した一致として受け入れられます。

class コマンドは、制御クラスを制御ポリシーに関連付けます。

例

次に、セッションの状態が許可されている場合に true と評価される制御クラスを設定する例を示します。

```
class-map type control subscriber match-all CLASS_1
 match authorization-status authorized
```

関連コマンド

コマンド	説明
class	制御ポリシーの 1 つ以上のアクションに制御クラスを関連付けます。
class-map type control subscriber	制御ポリシーのアクションを実行するために満たす必要のある条件を指定する制御クラスを定義します。
policy-map type control subscriber	加入者セッションの制御ポリシーを定義します。

match authorizing-method-priority

結果的に許可になった許可方式のプライオリティに基づいて true と評価される条件を作成するには、コントロール クラス マップ フィルタ コンフィギュレーション モードで **match authorizing-method-priority** コマンドを使用します。 結果的に許可になった許可方式のプライオリティが指定されたプライオリティと一致しない場合に true と評価される条件を作成するには、コントロール クラス マップ フィルタ コンフィギュレーション モードで **no-match authorizing-method-priority** コマンドを使用します。 条件を削除するには、このコマンドの **no** 形式を使用します。

match authorizing-method-priority {**eq**| **gt**| **lt**} *priority-value*

no-match authorizing-method-priority {**eq**| **gt**| **lt**} *priority-value*

no {**match**| **no-match**} **authorizing-method-priority** {**eq**| **gt**| **lt**} *priority-value*

構文の説明

eq	現在のプライオリティの値が *priority-value* と等しいことを指定します。
gt	現在のプライオリティの値が *priority-value* よりも大きいことを指定します。 （注） 数字が大きいほど、プライオリティは低くなります。
lt	現在のプライオリティの値が *priority-value* よりも小さいことを指定します。 （注） 値が小さいほど、プライオリティが高くなります。
priority-value	照合するプライオリティ値。 範囲：1 ～ 254。プライオリティは 1 が最も高く、254 が最も低くなります。

コマンド デフォルト

制御クラスには、認証方式のプライオリティに基づいた条件は含まれません。

コマンド モード

コントロール クラス マップ フィルタ コンフィギュレーション（config-filter-control-classmap）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

match authorizing-method-priority コマンドは、結果的に許可になった認証方式のプライオリティに基づいて、制御クラスに一致条件を設定します。 制御クラスには、複数の条件を含めることができ、それぞれの条件が true または false に評価されます。 制御クラスは、制御ポリシーのアクションを実行するために、すべての条件または一部の条件が true と評価される必要があるか、あるいはいずれの条件も true と評価されない必要があるかを定義します。

このコマンドの **no-match** 形式は、一致の失敗と見なされる値を指定します。 指定された一致条件以外の他のすべての値は、一致の成功と見なされます。 たとえば、**no-match authorizing-method-priority eq 10** コマンドを設定すると、10 以外のすべてのプライオリティ値は成功した一致として受け入れられます。

class コマンドは、制御クラスをポリシー制御に関連付けます。

例

次に、許可方式のプライオリティ番号が 20 未満の場合に true と評価される制御クラスを設定する例を示します。

```
class-map type control subscriber match-all CLASS_1
 match authorizing-method-priority lt 20
```

関連コマンド

コマンド	説明
authenticate using	指定した方式を使用して加入者セッションの認証を開始します。
class	制御ポリシーの 1 つ以上のアクションに制御クラスを関連付けます。
match current-method-priority	現在の認証方式のプライオリティに基づいて true と評価される条件を作成します。
policy-map type control subscriber	加入者セッションの制御ポリシーを定義します。

match client-type

イベントのデバイス タイプに基づいて true と評価される条件を作成するには、コントロール クラス マップ フィルタ コンフィギュレーション モードで **match client-type** コマンドを使用します。指定されたデバイス タイプにイベントのデバイス タイプが一致しない場合に true と評価される条件を作成するには、コントロール クラス マップ フィルタ コンフィギュレーション モードで **no-match client-type** コマンドを使用します。 条件を削除するには、このコマンドの **no** 形式を使用します。

match client-type {**data**| **switch**| **video**| **voice**}

no-match client-type {**data**| **switch**| **video**| **voice**}

no{**match**| **no-match**} **client-type** {**data**| **switch**| **video**| **voice**}

構文の説明

data	データ デバイスを指定します。
switch	スイッチ デバイスを指定します。
video	ビデオ デバイスを指定します。
voice	音声デバイスを指定します。

コマンド デフォルト

制御クラスには、デバイス タイプに基づいた条件は含まれません。

コマンド モード

コントロール クラス マップ フィルタ コンフィギュレーション（config-filter-control-classmap）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

match client-type コマンドは、イベントのデバイス タイプに基づいて、一致条件を制御クラスに設定します。 制御クラスには、複数の条件を含めることができ、それぞれの条件が true または false に評価されます。 制御クラスは、制御ポリシーのアクションを実行するために、すべての条件または一部の条件が true と評価される必要があるか、あるいはいずれの条件も true と評価されない必要があるかを定義します。

このコマンドの **no-match** 形式は、一致の失敗と見なされる値を指定します。 指定された一致条件以外の他のすべての値は、一致の成功と見なされます。 たとえば、**no-match client-type voice** コマンドを設定すると、音声以外のすべてのデバイス値は成功した一致として受け入れられます。

class コマンドは、制御クラスを制御ポリシーに関連付けます。

例

次に、クライアント タイプがデータである場合に true と評価される制御クラスを設定する例を示します。

```
class-map type control subscriber match-all CLASS_1
 match client-type data
```

関連コマンド

コマンド	説明
class	制御ポリシーの 1 つ以上のアクションに制御クラスを関連付けます。
policy-map type control subscriber	加入者セッションの制御ポリシーを定義します。

match current-method-priority

現在の認証方式のプライオリティに基づいて true と評価される条件を作成するには、コントロール クラス マップ フィルタ コンフィギュレーション モードで **match current-method-priority** コマンドを使用します。 現在の認証方式のプライオリティが指定された方式と一致しない場合に true と評価される条件を作成するには、コントロール クラス マップ フィルタ コンフィギュレーション モードで **no-match current-method-priority** コマンドを使用します。条件を削除するには、このコマンドの **no** 形式を使用します。

match current-method-priority {**eq**| **gt**| **lt**} *priority-value*

no-match current-method-priority {**eq**| **gt**| **lt**} *priority-value*

no {**match**| **no-match**}**current-method-priority** {**eq**| **gt**| **lt**} *priority-value*

構文の説明

eq	現在のプライオリティの値が *priority-value* と等しいことを指定します。
gt	現在のプライオリティの値が *priority-value* よりも大きいことを指定します。 値が大きいほど、プライオリティは低くなります。 （注） 数字が大きいほど、プライオリティは低くなります。
lt	現在のプライオリティの値が *priority-value* よりも小さいことを指定します。 値が小さいほどプライオリティが高くなります。 （注） 値が小さいほど、プライオリティが高くなります。
priority-value	照合するプライオリティ値。 範囲：1 ～ 254。 プライオリティは 1 が最も高く、254 が最も低くなります。

コマンド デフォルト

制御クラスには、認証方式のプライオリティに基づいた条件は含まれません。

コマンド モード

コントロール クラス マップ フィルタ コンフィギュレーション（config-filter-control-classmap）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

match current-method-priority コマンドは、認証方式のプライオリティに基づいて、制御クラスに一致条件を設定します。 制御クラスには、複数の条件を含めることができ、それぞれの条件が true または false に評価されます。 制御クラスは、制御ポリシーのアクションを実行するために、すべての条件または一部の条件が true と評価される必要があるか、あるいはいずれの条件も true と評価されない必要があるかを定義します。

このコマンドの **no-match** 形式は、一致の失敗と見なされる値を指定します。 指定された一致条件以外の他のすべての値は、一致の成功と見なされます。 たとえば、**no-match current-method-priority eq 10** コマンドを設定すると、制御クラスは 10 以外のすべてのプライオリティ値を成功した一致として受け入れます。

class コマンドは、制御クラスをポリシー制御に関連付けます。

例

次に、現在の認証方式のプライオリティ番号が 20 よりも大きい場合に true と評価される制御クラスを設定する例を示します。

```
class-map type control subscriber match-all CLASS_1
 match current-method-priority gt 20
```

関連コマンド

コマンド	説明
class	制御ポリシーの 1 つ以上のアクションに制御クラスを関連付けます。
match authorizing-method-priority	許可方式のプライオリティに基づいて true と評価される条件を作成します。
policy-map type control subscriber	加入者セッションの制御ポリシーを定義します。

match ip-address

イベントのソース IPv4 アドレスに基づいて true と評価される条件を作成するには、コントロール クラス マップ フィルタ コンフィギュレーション モードで **match ip-address** コマンドを使用します。 指定した IP アドレスとイベントのソース IP アドレスが一致しない場合に true と評価される条件を作成するには、コントロール クラス マップ フィルタ コンフィギュレーション モードで **no-match ip-address** コマンドを使用します。 条件を削除するには、このコマンドの **no** 形式を使用します。

match ip-address *ip-address*

no-match ip-address *ip-address*

no {**match| no-match**} **ip-address** *ip-address*

構文の説明

ip-address	照合する IPv4 アドレス。

コマンド デフォルト

制御クラスには、ソース IPv4 アドレスに基づいた条件は含まれません。

コマンド モード

コントロール クラス マップ フィルタ コンフィギュレーション（config-filter-control-classmap）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

match ip-address コマンドは、イベントの IP アドレスに基づいて、一致条件を制御クラスに設定します。 制御クラスには、複数の条件を含めることができ、それぞれの条件が true または false に評価されます。 制御クラスは、制御ポリシーのアクションを実行するために、すべての条件または一部の条件が true と評価される必要があるか、あるいはいずれの条件も true と評価されない必要があるかを定義します。

このコマンドの **no-match** 形式は、一致の失敗と見なされる値を指定します。 指定された一致条件以外の他のすべての値は、一致の成功と見なされます。 たとえば、**no-match ip-address 10.10.10.1** コマンドを設定すると、10.10.10.1 を除くすべての IPv4 アドレスが成功した一致として受け入れられます。

class コマンドは、制御クラスを制御ポリシーに関連付けます。

例

次に、IP アドレスが 10.10.10.1 である場合に true と評価される制御クラスを設定する例を示します。

```
class-map type control subscriber match-all CLASS_1
 match ip-address 10.10.10.1
```

関連コマンド

コマンド	説明
class	制御ポリシーの 1 つ以上のアクションに制御クラスを関連付けます。
match ipv6-address	イベントのソース IPv6 アドレスに基づいて true と評価される条件を作成します。
policy-map type control subscriber	加入者セッションの制御ポリシーを定義します。

match ipv6-address

イベントのソース IPv6 アドレスに基づいて true と評価される条件を作成するには、コントロール クラス マップ フィルタ コンフィギュレーション モードで **match ipv6-address** コマンドを使用します。 指定した IP アドレスとイベントのソース IP アドレスが一致しない場合に true と評価される条件を作成するには、コントロール クラス マップ フィルタ コンフィギュレーション モードで **no-match ipv6-address** コマンドを使用します。 条件を削除するには、このコマンドの **no** 形式を使用します。

match ipv6-address *ipv6-address subnet-mask*

no-match ipv6-address *ipv6-address subnet-mask*

no {**match| no-match**} **ipv6-address** *ipv6-address subnet-mask*

構文の説明

ipv6-address	照合する IPv6 アドレス。
subnet-mask	サブネット マスク。

コマンド デフォルト

制御クラスには、ソース IPv6 アドレスに基づいた条件は含まれません。

コマンド モード

コントロール クラス マップ フィルタ コンフィギュレーション（config-filter-control-classmap）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

match ipv6-address コマンドは、加入者の IPv6 アドレスに基づいて、一致条件を制御クラスに設定します。 制御クラスには、複数の条件を含めることができ、それぞれの条件が true または false に評価されます。 制御クラスは、制御ポリシーのアクションを実行するために、すべての条件または一部の条件が true と評価される必要があるか、あるいはいずれの条件も true と評価されない必要があるかを定義します。

このコマンドの **no-match** 形式は、一致の失敗と見なされる値を指定します。 指定された一致条件以外の他のすべての値は、一致の成功と見なされます。 たとえば、**no-match ipv6-address FE80::1** コマンドを設定すると、制御クラスは FE80::1 以外の IPv6 アドレスを成功した一致として受け入れます。

class コマンドは、制御クラスを制御ポリシーに関連付けます。

例

次に、IPアドレスがFE80::1である場合にtrueと評価される制御クラスを設定する例を示します。

```
class-map type control subscriber match-all CLASS_1
 match ipv6-address FE80::1
```

関連コマンド

コマンド	説明
class	制御ポリシーの1つ以上のアクションに制御クラスを関連付けます。
match ip-address	イベントのソースIPv4アドレスに基づいてtrueと評価される条件を作成します。
policy-map type control subscriber	加入者セッションの制御ポリシーを定義します。

match mac-address

イベントの MAC アドレスに基づいて true と評価される条件を作成するには、コントロール クラス マップ フィルタ コンフィギュレーション モードで **match mac-address** コマンドを使用します。指定した MAC アドレスとイベントの MAC アドレスが一致しない場合に true と評価される条件を作成するには、コントロール クラス マップ フィルタ コンフィギュレーション モードで **no-match mac-address** コマンドを使用します。 条件を削除するには、このコマンドの **no** 形式を使用します。

match mac-address *mac-address*

no-match mac-address *mac-address*

no {**match| no-match**}**mac-address** *mac-address*

構文の説明

mac-address	照合する MAC アドレス。

コマンド デフォルト

制御クラスには、MAC アドレスに基づいた条件は含まれません。

コマンド モード

コントロール クラス マップ フィルタ コンフィギュレーション（config-filter-control-classmap）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

match mac-address コマンドは、イベントの MAC アドレスに基づいて、一致条件を制御クラスに設定します。 制御クラスには、複数の条件を含めることができ、それぞれの条件が true または false に評価されます。 制御クラスは、制御ポリシーのアクションを実行するために、すべての条件または一部の条件が true と評価される必要があるか、あるいはいずれの条件も true と評価されない必要があるかを定義します。

このコマンドの **no-match** 形式は、一致の失敗と見なされる値を指定します。 指定された一致条件以外の他のすべての値は、一致の成功と見なされます。 たとえば、**no-match mac-address 0030.94C2.D5CA** コマンドを設定すると、制御クラスは 0030.94C2.D5CA 以外の MAC アドレスを成功した一致として受け入れます。

class コマンドは、制御クラスを制御ポリシーに関連付けます。

例

次に、MAC アドレスが 0030.94C2.D5CA である場合に true と評価される制御クラスを設定する例を示します。

```
class-map type control subscriber match-all CLASS_1
 match mac-address 0030.94C2.D5CA
```

関連コマンド

コマンド	説明
class	制御ポリシーの 1 つ以上のアクションに制御クラスを関連付けます。
policy-map type control subscriber	加入者セッションの制御ポリシーを定義します。

match method

イベントの認証方式に基づいてtrueと評価される条件を作成するには、コントロール クラス マップ フィルタ コンフィギュレーション モードで **match method** コマンドを使用します。 指定した方式とイベントの認証方式が一致しない場合に true と評価される条件を作成するには、コントロール クラス マップ フィルタ コンフィギュレーション モードで **no-match method** コマンドを使用します。 条件を削除するには、このコマンドの **no** 形式を使用します。

match method {**dot1x**| **mab**| **webauth**}

no-match method {**dot1x**| **mab**| **webauth**}

no {**match**| **no-match**} **method** {**dot1x**| **mab**| **webauth**}

構文の説明

dot1x	IEEE 802.1X 認証方式を指定します。
mab	MAC認証バイパス（MAB）方式を指定します。
webauth	Web 認証方式を指定します。

コマンド デフォルト

制御クラスには、認証方式に基づいた条件は含まれません。

コマンド モード

コントロール クラス マップ フィルタ コンフィギュレーション（config-filter-control-classmap）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

match method コマンドは、認証方式に基づいて、制御クラスに一致条件を設定します。 制御クラスには、複数の条件を含めることができ、それぞれの条件がtrueまたはfalseに評価されます。 制御クラスは、制御ポリシーのアクションを実行するために、すべての条件または一部の条件がtrueと評価される必要があるか、あるいはいずれの条件も true と評価されない必要があるかを定義します。

このコマンドの **no-match** 形式は、一致の失敗と見なされる値を指定します。 指定された一致条件以外の他のすべての値は、一致の成功と見なされます。 たとえば、**no-match method dot1x** コマ

ンドを設定すると、制御クラスは dot1x 以外のすべての認証方式を成功した一致として受け入れます。

class コマンドは、制御クラスを制御ポリシーに関連付けます。

例

次に、認証方式が 802.1X である場合と、方式がタイムアウトになる場合に true と評価されるという 2 つの条件を持つ制御クラスを設定する例を示します。

```
class-map type control subscriber match-all DOT1X_TIMEOUT
  match method dot1x
  match result-type method-timeout
```

関連コマンド

コマンド	説明
authenticate using	指定した方式を使用して加入者セッションの認証を開始します。
class	制御ポリシーの 1 つ以上のアクションに制御クラスを関連付けます。
policy-map type control subscriber	加入者セッションの制御ポリシーを定義します。

match port-type（クラス マップ フィルタ）

イベントのインターフェイス タイプに基づいて true と評価される条件を作成するには、コントロール クラス マップ フィルタ コンフィギュレーション モードで **match port-type** コマンドを使用します。 指定されたタイプとイベントのインターフェイス タイプが一致しない場合に true と評価される条件を作成するには、コントロール クラス マップ フィルタ コンフィギュレーション モードで **no-match ip-address** コマンドを使用します。 条件を削除するには、このコマンドの **no** 形式を使用します。

match port-type {**l2-port| l3-port| dot11-port**}

no-match port-type {**l2-port| l3-port| dot11-port**}

no {**match| no-match**} **port-type** {**l2-port| l3-port| dot11-port**}

構文の説明

dot11-port	802.11 インターフェイスを指定します。
l2-port	レイヤ 2 インターフェイスを指定します。
l3-port	レイヤ 3 インターフェイスを指定します。

コマンド デフォルト

制御クラスには、インターフェイス タイプに基づいた条件は含まれません。

コマンド モード

コントロール クラス マップ フィルタ コンフィギュレーション（config-filter-control-classmap）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

match port-type コマンドは、インターフェイス タイプに基づいて、制御クラスに一致条件を設定します。 制御クラスには、複数の条件を含めることができ、それぞれの条件が true または false に評価されます。 制御クラスは、制御ポリシーのアクションを実行するために、すべての条件または一部の条件が true と評価される必要があるか、あるいはいずれの条件も true と評価されない必要があるかを定義します。

このコマンドの **no-match** 形式は、一致の失敗と見なされる値を指定します。 指定された一致条件以外の他のすべての値は、一致の成功と見なされます。 たとえば、**no-match port-type l2-port**

コマンドを設定すると、制御クラスは l2-port 以外のすべてのインターフェイス値を成功した一致として受け入れます。

class コマンドは、制御クラスを制御ポリシーに関連付けます。

例

次に、ポート タイプがレイヤ 2 である場合に true と評価される制御クラスを設定する例を示します。

```
class-map type control subscriber match-all CLASS_1
 match port-type l2-port
```

関連コマンド

コマンド	説明
class	制御ポリシーの 1 つ以上のアクションに制御クラスを関連付けます。
policy-map type control subscriber	加入者セッションの制御ポリシーを定義します。

match result-type

指定した認証結果に基づいてtrueと評価される条件を作成するには、コントロール クラス マップ フィルタ コンフィギュレーション モードで **match result-type** コマンドを使用します。 指定した結果と認証結果が一致しない場合にtrueと評価される条件を作成するには、コントロール クラス マップ フィルタ コンフィギュレーション モードで **no-match result-type** コマンドを使用します。 条件を削除するには、このコマンドの **no** 形式を使用します。

match result-type [**method** {**dot1x**| **mab**| **webauth**}] *result-type*

no-match result-type [**method** {**dot1x**| **mab**| **webauth**}] *result-type*

no {**match**| **no-match**} **result-type** [**method** {**dot1x**| **mab**| **webauth**}] *result-type*

構文の説明

method	（任意）指定した認証方式に対してのみ、結果を照合します。 方式を指定しなければ、ポリシーは現在のイベントに関連付けられた方式を照合します。
dot1x	IEEE 802.1X 認証方式を指定します。
mab	MAC認証バイパス（MAB）方式を指定します。
webauth	Web 認証方式を指定します。
result-type	認証結果のタイプ。 *result-type* の有効なキーワードは次のとおりです。 • **aaa-timeout**：AAA サーバがタイムアウトしました。 • **agent-not-found**：認証方式用のエージェントが検出されませんでした。 • **authoritative**：許可に失敗しました。 • **method-timeout**：認証方式がタイムアウトになりました。 • **none**：結果がありません。 • **success**：認証が成功しました。

コマンド モード

制御クラスには、結果タイプに基づいた条件は含まれません（config-filter-control-classmap）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

match result-type コマンドは、認証要求の結果に基づいて、制御クラスに一致条件を設定します。制御クラスには、複数の条件を含めることができ、それぞれの条件が true または false に評価されます。 制御クラスは、制御ポリシーのアクションを実行するために、すべての条件または一部の条件が true と評価される必要があるか、あるいはいずれの条件も true と評価されない必要があるかを定義します。

このコマンドの **no-match** 形式は、一致の失敗と見なされる値を指定します。 指定された一致条件以外の他のすべての値は、一致の成功と見なされます。 たとえば、**no-match result-type method dot1x method-timeout** コマンドを設定すると、制御クラスは dot1x method-timeout 以外の結果値を成功した一致として受け入れます。

class コマンドは、制御クラスを制御ポリシーに関連付けます。

例

次に、認証結果に基づいた不一致条件を含む、ALL_FAILED という名前の制御クラスを設定する例を示します。

```
class-map type subscriber control match-all ALL_FAILED
 no-match result-type method dot1x none
 no-match result-type method dot1x success
 no-match result-type method mab none
 no-match result-type method mab success
 no-match result-type method webauth none
 no-match result-type method webauth success
```

関連コマンド

コマンド	説明
class	制御ポリシーの 1 つ以上のアクションに制御クラスを関連付けます。
class-map type control subscriber	制御ポリシーのアクションを実行するために満たす必要のある条件を指定する制御クラスを定義します。
policy-map type control subscriber	加入者セッションの制御ポリシーを定義します。

match service-template

イベント サービス テンプレートに基づいて true と評価される条件を作成するには、コントロール クラス マップ フィルタ コンフィギュレーション モードで **match service-template** コマンドを使用します。 イベント サービス テンプレートが指定されたテンプレートと一致しない場合に true と評価される条件を作成するには、コントロール クラス マップ フィルタ コンフィギュレーション モードで **no-match service-template** コマンドを使用します。 条件を削除するには、このコマンドの **no** 形式を使用します。

match service-template *template-name*

no-match service-template *template-name*

no {**match| no-match**} **service-template** *template-name*

構文の説明

template-name	**service-template** コマンドによって定義された、設定済みのサービス テンプレートの名前。

コマンド デフォルト

制御クラスには、サービス テンプレートに基づいた条件は含まれません。

コマンド モード

コントロール クラス マップ フィルタ コンフィギュレーション（config-filter-control-classmap）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

match service-template コマンドは、イベントのサービス テンプレートに基づいて、制御クラスに一致条件を設定します。 制御クラスには、複数の条件を含めることができ、それぞれの条件が true または false に評価されます。 制御クラスは、制御ポリシーのアクションを実行するために、すべての条件または一部の条件が true と評価される必要があるか、あるいはいずれの条件も true と評価されない必要があるかを定義します。

このコマンドの **no-match** 形式は、一致の失敗と見なされる値を指定します。 指定された一致条件以外の他のすべての値は、一致の成功と見なされます。 たとえば、**no-match service-template VLAN_1** コマンドを設定すると、制御クラスは VLAN_1 以外のすべてのサービス テンプレート値を成功した一致として受け入れます。

class コマンドは、制御クラスを制御ポリシーに関連付けます。

例

次に、使用するサービス テンプレートが VLAN_1 という名前である場合に true と評価される制御クラスを設定する例を示します。

```
class-map type control subscriber match-all CLASS_1
 match service-template VLAN_1
```

関連コマンド

コマンド	説明
class	制御ポリシーの 1 つ以上のアクションに制御クラスを関連付けます。
event	条件が満たされる場合に、制御ポリシーでアクションをトリガーするイベントのタイプを指定します。
match activated-service-template	セッションでアクティブ化されているサービス テンプレートに基づいて true と評価される条件を作成します。
service-template	加入者セッションに適用する一連のポリシー属性を含むテンプレートを定義します。

match tag（クラス マップ フィルタ）

イベントに関連付けられたタグに基づいて true と評価される条件を作成するには、コントロール クラス マップ フィルタ コンフィギュレーション モードで **match tag** コマンドを使用します。 指定されたタグとイベント タグが一致していない場合に true と評価される条件を作成するには、コントロール クラス マップ フィルタ コンフィギュレーション モードで **no-match tag** コマンドを使用します。 条件を削除するには、このコマンドの **no** 形式を使用します。

match tag *tag-name*

no-match tag *tag-name*

no {**match| no-match**} **tag** *tag-name*

構文の説明

tag-name	サービス テンプレートで **tag** コマンドによって定義されたタグ名。

コマンド デフォルト

制御クラスには、イベント タグに基づいた条件は含まれません。

コマンド モード

コントロール クラス マップ フィルタ コンフィギュレーション（config-filter-control-classmap）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

match tag コマンドは、イベントのタグに基づいて、制御クラスに一致条件を設定します。 制御クラスには、複数の条件を含めることができ、それぞれの条件が true または false に評価されます。 制御クラスは、制御ポリシーのアクションを実行するために、すべての条件または一部の条件が true と評価される必要があるか、あるいはいずれの条件も true と評価されない必要があるかを定義します。

このコマンドの **no-match** 形式は、一致の失敗と見なされる値を指定します。 指定された一致条件以外の他のすべての値は、一致の成功と見なされます。 たとえば、**no-match tag TAG_1** コマンドを設定すると、制御クラスは TAG_1 以外のすべてのタグ値を成功した一致として受け入れます。

class コマンドは、制御クラスを制御ポリシーに関連付けます。

例

次に、イベントからのタグが TAG_1 という名前である場合に true と評価される制御クラスを設定する例を示します。

```
class-map type control subscriber match-all CLASS_1
 match tag TAG_1
```

関連コマンド

コマンド	説明
class	制御ポリシーの 1 つ以上のアクションに制御クラスを関連付けます。
policy-map type control subscriber	加入者セッションの制御ポリシーを定義します。
tag（サービス テンプレート）	サービステンプレートとユーザ定義のタグを関連付けます。

match timer（クラス マップ フィルタ）

イベント タイマーに基づいて true と評価される条件を作成するには、コントロール クラス マップ フィルタ コンフィギュレーション モードで **match timer** コマンドを使用します。 指定されたタイマーとイベント タイマーが一致していない場合に true と評価される条件を作成するには、コントロール クラス マップ フィルタ コンフィギュレーション モードで **no-match timer** コマンドを使用します。 条件を削除するには、このコマンドの **no** 形式を使用します。

match timer *timer-name*

no-match timer *timer-name*

no {**match**| **no-match**} **timer** *timer-name*

構文の説明

timer-name	**set-timer** コマンドで制御ポリシーに定義されているポリシー タイマーの名前。

コマンド デフォルト

制御クラスには、イベント タイマーに基づいた条件は含まれません。

コマンド モード

コントロール クラス マップ フィルタ コンフィギュレーション（config-filter-control-classmap）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

match timer コマンドは、イベントのタイマー名に基づいて、制御クラスに一致条件を設定します。 制御クラスには、複数の条件を含めることができ、それぞれの条件が true または false に評価されます。 制御クラスは、制御ポリシーのアクションを実行するために、すべての条件または一部の条件が true と評価される必要があるか、あるいはいずれの条件も true と評価されない必要があるかを定義します。

このコマンドの **no-match** 形式は、一致の失敗と見なされる値を指定します。 指定された一致条件以外の他のすべての値は、一致の成功と見なされます。 たとえば、**no-match timer TIMER_A** コマンドを設定すると、制御クラスは TIMER_A 以外のすべてのタイマー値を成功した一致として受け入れます。

class コマンドは、制御クラスを制御ポリシーに関連付けます。

例

次に、イベント タイマーが TIMER_A という名前である場合に true と評価される制御クラスを設定する例を示します。

```
class-map type control subscriber match-all CLASS_1
 match timer TIMER_A
!
policy-map type control subscriber RULE_A
 event session-start match-all
  1 class always do-until-failure
   1 set-timer TIMER_A 60
 event timer-expiry match-all
  2 class CLASS_1 do-all
   1 clear-session
```

関連コマンド

コマンド	説明
class	制御ポリシーの 1 つ以上のアクションに制御クラスを関連付けます。
policy-map type control subscriber	加入者セッションの制御ポリシーを定義します。
set-timer	加入者セッションに対して名前付きポリシー タイマーを開始します。

match username

イベントのユーザ名に基づいてtrueと評価される条件を作成するには、コントロール クラス マップ フィルタ コンフィギュレーション モードで **match username** コマンドを使用します。 指定されたユーザ名とイベント ユーザ名が一致していない場合にtrueと評価される条件を作成するには、コントロール クラス マップ フィルタ コンフィギュレーション モードで **no-match username** コマンドを使用します。 条件を削除するには、このコマンドの **no** 形式を使用します。

match username *username*

no-match username *username*

no {**match**| **no-match**} **username** *username*

構文の説明

username	ユーザ名。

コマンド デフォルト

制御クラスには、イベント ユーザ名に基づいた条件は含まれません。

コマンド モード

コントロール クラス マップ フィルタ コンフィギュレーション（config-filter-control-classmap）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

match username コマンドは、ユーザ名に基づいて、制御クラスに一致条件を設定します。 制御クラスには、複数の条件を含めることができ、それぞれの条件がtrueまたはfalseに評価されます。制御クラスは、制御ポリシーのアクションを実行するために、すべての条件または一部の条件がtrueと評価される必要があるか、あるいはいずれの条件もtrueと評価されない必要があるかを定義します。

このコマンドの **no-match** 形式は、一致の失敗と見なされる値を指定します。 指定された一致条件以外の他のすべての値は、一致の成功と見なされます。 たとえば、**no-match username josmithe** コマンドを設定すると、制御クラスはjosmithe以外のすべてのユーザ名値を成功した一致として受け入れます。

class コマンドは、制御クラスを制御ポリシーに関連付けます。

例

次に、ユーザ名が josmithe である場合に true と評価される制御クラスを設定する例を示します。

```
class-map type control subscriber match-all CLASS_1
 match username josmithe
```

関連コマンド

コマンド	説明
class	制御ポリシーの 1 つ以上のアクションに制御クラスを関連付けます。
policy-map type control subscriber	加入者セッションの制御ポリシーを定義します。

max-http-conns

Web 認証クライアントごとの HTTP 接続数を制限するには、パラメータ マップ コンフィギュレーション モードで **max-http-conns** コマンドを使用します。 デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

max-http-conns *number*

no max-http-conns *number*

構文の説明

number	許可される HTTP 同時クライアント接続の最大数。 有効な範囲は、1 ～ 200 です。 デフォルトは 30 です。

コマンド デフォルト

同時 HTTP 接続の最大数は 30 です。

コマンド モード

パラメータ マップ コンフィギュレーション（consent-parameter-map）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

max-http-conns コマンドを使用して、Web 認証クライアントごとに許可される HTTP 接続の最大数を設定します。

以前に設定された値よりも小さい値に新しい値が設定されており、現在の接続数が新しい最大値を超えると、HTTP サーバは現在のどの接続も強制終了しません。 ただし、サーバは現在の接続数が新しい設定値未満になるまで、新しい接続を受け入れません。

例

次に、Web 認証のグローバル パラメータ マップで、同時 HTTP 接続の最大数を 100 に設定する例を示します。

```
parameter-map type webauth global
 timeout init-state min 15
 max-http-conns 100
 banner file flash:webauth_banner1.html
```

関連コマンド

コマンド	説明
timeout init-state min	Web 認証セッションに Init ステート タイムアウトを設定します。

parameter-map type webauth

Web 認証用のパラメータ マップを定義するには、グローバル コンフィギュレーション モードで **parameter-map type webauth** コマンドを使用します。 パラメータ マップを削除するには、このコマンドの **no** 形式を使用します。

parameter-map type webauth {*parameter-map-name*| **global**}

no parameter-map type webauth {*parameter-map-name*| **global**}

構文の説明

parameter-map-name	Web 認証用の名前付きパラメータ マップを定義します。
global	Web 認証用のグローバル パラメータを定義します。

コマンド デフォルト

Web 認証用のパラメータ マップは定義されていません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

parameter-map type webauth コマンドを使用して、Web 認証用のパラメータ マップを定義します。 パラメータ マップを使用して、**authenticate using webauth** コマンドでポリシー マップに設定したアクションの動作を制御するパラメータを指定できます。

グローバル パラメータ マップには、システム全体のパラメータが含まれます。 このパラメータ マップは Web 認証アクションに追加されず、Web 認証と承諾の両方のパラメータがあります。 グローバル パラメータ マップは、認証アクションに自動的に適用されます。 明示的に名前付きパラメータ マップを適用し、グローバルと名前付きパラメータ マップの両方に共通なパラメータが設定されている場合、グローバル パラメータ マップ コンフィギュレーションが優先されます。

global キーワードで定義されたグローバル パラメータ マップに対してサポートされるコンフィギュレーション パラメータは、*parameter-map-name* 引数で定義される名前付きパラメータ マップに対してサポートされるパラメータとは異なります。

例

次に、POLICY_1 という名前の制御ポリシーで使用される PMAP_2 という名前のパラメータ マップを設定して、ユーザを認証する例を示します。

```
parameter-map type webauth PMAP_2
 type webconsent
 max-login-attempts 5
 banner file flash:consent_page.htm

policy-map type control subscriber match-all POLICY_1
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using webauth parameter-map PMAP_2
```

関連コマンド

コマンド	説明
authenticate using	指定した方式を使用して、加入者セッションを認証します。
policy-map type control subscriber	加入者セッションの制御ポリシーを定義します。
show ip-admission status parameter-map	指定したパラメータ マップの設定情報を表示します。
type	パラメータ マップでサポートされる認証方式を定義します。

pause reauthentication

認証の失敗後に再認証プロセスを停止するには、コントロール ポリシー マップ アクション コンフィギュレーション モードで **pause reauthentication** コマンドを使用します。 制御ポリシーからこのアクションを削除するには、このコマンドの **no** 形式を使用します。

action-number **pause reauthentication**

no *action-number*

構文の説明

action-number	アクション数。 アクションは、ポリシー ルール内で順番に実行されます。

コマンド デフォルト

再認証は停止されません。

コマンド モード

コントロール ポリシーマップ アクション コンフィギュレーション（config-action-control-policymap）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

pause reauthentication コマンドは、制御ポリシーにアクションを定義します。

制御ポリシーによって、指定されたイベントと条件に応じて実行されるアクションが決定されます。 制御クラスによって、アクションを実行するために満たす必要がある条件が定義されます。アクションは、ポリシー ルール内で番号が付けられ、順番に実行されます。

class コマンドは、制御クラスを 1 つ以上のアクションに関連付けることでポリシー ルールを作成します。 ポリシー ルールに定義できるアクションは、**event** コマンドによって指定されるイベントのタイプによって異なります。

例

次に、認証失敗イベントに設定されている認証停止アクションと制御ポリシーを設定する方法を示します。

```
policy-map type control subscriber POLICY
 event authentication-failure match-all
  1 class SERVER_DEAD_UNAUTHD_HOST do-all
   1 activate template VLAN
```

```
  2 authorized
  3 pause reauthentication
2 class SERVER_DEAD_AUTHD_HOST do-all
  1 pause reauthentication
```

関連コマンド

コマンド	説明
authentication-restart	認証または許可が失敗した後、認証プロセスを再開します。
class	制御ポリシーの 1 つ以上のアクションに制御クラスを関連付けます。
event	条件が満たされる場合に、制御ポリシーでアクションをトリガーするイベントのタイプを指定します。
resume reauthentication	認証の失敗後に再認証プロセスを再開します。

policy-map type control subscriber

加入者セッションに対して制御ポリシーを定義するには、グローバル コンフィギュレーション モードで **policy-map type control subscriber** コマンドを使用します。 制御ポリシーを削除するには、このコマンドの **no** 形式を使用します。

policy-map type control subscriber *control-policy-name*

no policy-map type control subscriber *control-policy-name*

構文の説明

control-policy-name	制御ポリシー名。

コマンド デフォルト

制御ポリシーは作成されません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

制御ポリシーによって、指定されたイベントと条件に応じて実行されるアクションが定義されます。

制御ポリシーは 1 つ以上の制御ポリシー ルールで作成されています。 制御ポリシー ルールは、制御クラスを 1 つ以上のアクションに関連付けます。 制御クラスによって、アクションを実行するために満たす必要がある条件が定義されます。 アクションに番号が付けられ、順に実行されます。

制御ポリシーの定義には、3 つの手順があります。

1. **class-map type control subscriber** コマンドを使用して、1 つ以上の制御クラスを作成します。
2. **policy-map type control subscriber** コマンドを使用して、制御ポリシーを作成します。
3. **service-policy type control subscriber** コマンドを使用して、制御ポリシーをコンテキストに適用します。

例

次に、DOT1X_MAB_WEBAUTH という名前の制御ポリシーを設定する方法を示します。 認証失敗イベントが発生し、セッションが DOT1X_AUTHORITATIVE という名前の制御クラスにあるすべての条件に一致する場合、ポリシーは、認証処理を実行し、MAC 認証バイパス（MAB）を使用してセッションを認証しようとします。

```
class-map type control subscriber match-all DOT1X_AUTHORITATIVE
 match method dot1x
 match result-type authoritative
!
policy-map type control subscriber DOT1X_MAB_WEBAUTH
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x retries 3 retry-time 15
 event authentication-failure match-first
  10 class DOT1X_AUTHORITATIVE do-all
   10 authenticate using mab
  20 class DOT1X_METHOD_TIMEOUT_3 do-all
   10 authenticate using mab
  30 class MAB_AUTHORITATIVE do-all
   10 authenticate using webauth retries 3 retry-time 15
  40 class AAA_TIMEOUT do-all
   10 activate service-template FALLBACK
 event aaa-available match-all
  10 class always do-until-failure
   10 authenticate using dot1x
```

関連コマンド

コマンド	説明
class	制御ポリシーの 1 つ以上のアクションに制御クラスを関連付けます。
class-map type control subscriber	制御ポリシーのアクションを実行するために満たす必要のある条件を指定する制御クラスを定義します。
event	制御クラスの評価を開始するイベントのタイプを指定します。
service-policy type control subscriber	インターフェイスに制御ポリシーを適用します。

protect（ポリシー マップ アクション）

ポートでセキュリティ違反が発生した後に、違反パケットをサイレントにドロップするには、コントロール ポリシー マップ アクション コンフィギュレーション モードで **protect** コマンドを使用します。 制御ポリシーからこのアクションを削除するには、このコマンドの **no** 形式を使用します。

action-number **protect**

no *action-number*

構文の説明

action-number	アクション数。 アクションは、ポリシー ルール内で順番に実行されます。

コマンド デフォルト

違反イベントに対して保護アクションは設定されません。

コマンド モード

コントロール ポリシーマップ アクション コンフィギュレーション（config-action-control-policymap）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

protect コマンドは、制御ポリシーにアクションを定義します。

制御ポリシーによって、指定されたイベントと条件に応じて実行されるアクションが決定されます。 制御クラスによって、アクションを実行するために満たす必要がある条件が定義されます。アクションは、ポリシー ルール内で番号が付けられ、順番に実行されます。

class コマンドは、制御クラスを 1 つ以上のアクションに関連付けることでポリシー ルールを作成します。 ポリシー ルールに定義できるアクションは、**event** コマンドによって指定されるイベントのタイプによって異なります。

例

次に、違反イベントに設定された保護アクションと制御ポリシーを設定する方法を示します。

```
policy-map type control subscriber POLICY_1
 event violation match-all
  1 class always do-until-failure
   10 protect
```

関連コマンド

コマンド	説明
class	制御ポリシーの 1 つ以上のアクションに制御クラスを関連付けます。
err-disable	セキュリティ違反が発生した後、ポートを一時的にディセーブルにします。
event	条件が満たされる場合に、制御ポリシーでアクションをトリガーするイベントのタイプを指定します。

radius-server host

RADIUSサーバホストを指定するには、グローバル コンフィギュレーションモードで**radius-server host** コマンドを使用します。 指定した RADIUS ホストを削除するには、このコマンドの **no** 形式を使用します。

Cisco IOS Release 12.4T and Later Releases

radius-server host {*hostname*| *ip-address*} [**alias**{*hostname*| *ip-address*}| [**acct-port** *port-number*] [**auth-port** *port-number*] **[non-standard]** [**timeout** *seconds*] [**retransmit** *retries*] [**backoff exponential** [**max-delay** *minutes*] [**backoff-retry** *number-of-retransmits*]] [**key** *encryption-key*]]

no radius-server host {*hostname*| *ip-address*}

All Other Releases

radius-server host {*hostname*| *ip-address*} [**alias**{*hostname*| *ip-address*}| [**acct-port** *port-number*] [**auth-port** *port-number*] **[non-standard]** [**timeout** *seconds*] [**retransmit** *retries*] [**test username** *user-name* **[ignore-acct-port] [ignore-auth-port]** [**idle-time** *minutes*]] [**backoff exponential** [**max-delay** *minutes*] [**backoff-retry** *number-of-retransmits*]] [**key-wrap encryption-key** *encryption-key* **message-auth-code-key** *encryption-key* [**format** {**ascii**| **hex**}]| **pac**] [**key** *encryption-key*]]

no radius-server host {*hostname*| *ip-address*}

構文の説明

hostname	RADIUS サーバ ホストのドメイン ネーム システム（DNS）名です。
ip-address	RADIUS サーバ ホストの IP アドレスです。
alias	（任意）指定した RADIUS サーバについて、1 行につき最大 8 つのエイリアスを許可します。
acct-port *port-number*	（任意）アカウンティング要求に対する UDP 宛先ポート。 • ポート番号が 0 に設定されている場合、認証にホストは使用されません。 ポート番号が指定されていない場合に割り当てられるデフォルトのポート番号は 1646 です。
auth-port *port-number*	（任意）認証要求に対する UDP 宛先ポート。 • ポート番号が 0 に設定されている場合、認証にホストは使用されません。 ポート番号が指定されていない場合に割り当てられるデフォルトのポート番号は 1645 です。

non-standard	RADIUS 標準に違反する属性を解析します。
timeout *seconds*	（任意）デバイスがRADIUSサーバの応答を待機し、再送信するまでの時間間隔（秒単位）です。 • タイムアウトのキーワードによって、**radius-server timeout** コマンドのグローバル値が上書きされます。 • タイムアウト値が指定されていない場合は、グローバル値が使用されます。値の範囲は 1～1000 です。
retransmit *retries*	（任意）サーバが応答しないか、応答に遅延がある場合に、RADIUS要求がサーバに再送信される回数。 • 再送信のキーワードによって、**radius-server retransmit** コマンドのグローバル設定は上書きされます。 • 再送信値が指定されていない場合は、グローバル値が使用されます。値の範囲は1～100 です。
test username *user-name*	（任意）RADIUS サーバ ロード バランシングの自動テスト機能用のテストユーザ名を設定します。
ignore-acct-port	（任意）アカウンティング ポートで、RADIUS サーバ ロード バランシング用の自動テスト機能をディセーブルにします。
ignore-auth-port	（任意）認証ポートで、RADIUSサーバ ロード バランシング用の自動テスト機能をディセーブルにします。
idle-time *minutes*	（任意）サーバが隔離され、テストパケットが送信されるまで、サーバがアイドル状態になる時間の長さ (分単位)。 指定できる範囲は 1 ～ 35791 です。 デフォルトは 60 です。
backoff exponential	（任意）指数再送信バックアップ モードを設定します。

max-delay *minutes*	（任意）再送信間の最大遅延を秒単位で設定します。 • **max-delay** *minutes* *minutes*：範囲は 1 ～ 120 です。 デフォルト値は 3 です。
key-wrap encryption-key	（任意）キーラップの暗号キーを指定します。
message-auth-code-key	キー ラップのメッセージ認証コード キーを指定します。
format	（任意）メッセージ オーセンティケータ コード キーの形式を指定します。 • 次の値が有効です。 ◦ **ascii**：ASCII 形式でキーを設定します。 ◦ **hex**：16 進数表記でキーを設定します。
backoff-retry *number-of-retransmits*	（任意）指数バック オフの再試行回数を指定します。 • *number-of-retransmits*：バック オフ再試行の回数。 指定できる範囲は 1 ～ 50 です。 デフォルト値は 8 です。
pac	（任意）サーバごとに Protected Access Credential（PAC）キーを生成します。

key	（任意）このRADIUSサーバ上で実行しているデバイスとRADIUSデーモンの間に使用される暗号キー。 • **key** キーワードによって、**radius-server key** コマンドのグローバル設定は上書きされます。 キー文字列を指定しない場合、グローバル値が使用されます。 （注） **key** キーワードは、RADIUS サーバで使用される暗号化キーと一致する必要があるテキスト文字列です。 キーの先頭にあるスペースは無視されますが、キー内のスペースとキー末尾のスペースは使用されるため、キーは常に **radius-server host** コマンド構文の最後のアイテムとして設定してください。 キーにスペースを使用する場合は、引用符自体がキーの一部でない限り、そのキーを引用符で囲まないでください。
encryption-key	暗号キーを指定します。 • *encryption-key* の有効な値は、次のとおりです。 ◦ **0**：暗号化されていないキーが続くことを示します。 ◦ **7**：非表示キーが後に続くことを示します。 ◦暗号化されていない（クリア テキスト）サーバ キーを指定する文字列。

コマンド デフォルト

RADIUSホストは指定されておらず、RADIUSサーバ ロード バランシングの自動テストはデフォルトでディセーブルです。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
11.1	このコマンドが導入されました。
12.0(5)T	このコマンドは、RADIUSサーバごとに、タイムアウト、再送信、およびキー値を設定するためのオプションを追加するために変更されました。
12.1(3)T	このコマンドが変更されました。 **alias** キーワードが追加されました。
12.2(15)B	このコマンドが、Cisco IOS Release 12.2(15)B に統合されました。 **backoff exponential**、**backoff-retry**、**key**、および **max-delay** キーワードと、*number-of-retransmits*、*encryption-key*、および *minutes* 引数が追加されました。
12.2(28)SB	このコマンドが、Cisco リリース 12.2(28)SB に統合されました。 **test username** *user-name*、**ignore-auth-port**、**ignore-acct-port**、および **idle-time** *seconds* キーワードと引数が、RADIUS サーバのロード バランシング自動化テスト機能用に追加されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。 Cisco IOS リリース 12.2(28)SB に追加されたキーワードと引数は、Cisco IOS リリース 12.2(33)SRA と後続の 12.2SR リリースに適用されます。
12.4(11)T	このコマンドが変更されました。 （注） Cisco IOS リリース 12.2(28)SB に追加されたキーワードと引数は、Cisco IOS リリース 12.4(11)T または後続の 12.4T リリースに適用されません。
12.2 SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。このトレインの特定の 12.2SX リリースにおけるサポートは、フィーチャ セット、プラットフォーム、およびプラットフォーム ハードウェアによって異なります。 （注） Cisco IOS リリース 12.2(28)SB に追加されたキーワードと引数は、Cisco IOS リリース 12.2SX に適用されません。
Cisco IOS XE Release 2.5	このコマンドが、Cisco IOS XE Release 2.5 に統合されました。
15.3(1)S	このコマンドが変更されました。 **key-wrap encryption-key**、**message-auth-code-key**、**format**、**ascii**、および **hex** キーワードが追加されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

複数の **radius-server host** コマンドを使用して、複数のホストを指定できます。 ソフトウェアは、指定された順序でホストを検索します。

ホスト固有のタイムアウト値、再送信値、またはキー値が指定されていない場合は、グローバル値が各ホストに適用されます。

RADIUS サーバの自動テスト用に RADIUS サーバで定義されていないテスト ユーザを使用することを推奨します。 これはテストユーザが正しく設定されていない場合に発生する可能性のあるセキュリティ上の問題から保護するためです。

非標準のオプションを使用して RADIUS サーバを設定し、非標準のオプションを使用せずに別の RADIUS サーバを設定すると、非標準のオプションを使用する RADIUS サーバ ホストでは事前定義されたホストが受け入れられません。 ただし、異なる UDP 宛先ポートに対して同じ RADIUS サーバのホスト IP アドレスを設定する場合に、1 つの UDP 宛先ポート（アカウンティング要求用）が **acct-port** キーワードを使用して設定され、もう 1 つの UDP 宛先ポート（認証要求用）が **auth-port** キーワードを使用して、非標準オプションを使用するか、使用しないで設定されているときは、RADIUS サーバは非標準オプションを受け入れません。 これにより、すべてのポート番号がリセットされます。 ホストを指定し、1 つの回線にアカウンティング ポートと認証ポートを設定する必要があります。

アカウンティングと認証に別個のサーバを使用するには、適宜 0 ポート値を使用します。

RADIUS サーバ自動テスト

radius-server host コマンドを使用して、RADIUS サーバ ロード バランシングの自動テストをイネーブルにすると、次のようになります。

- 認証ポートはデフォルトでイネーブルです。 ポート番号が指定されていない場合、デフォルトのポート番号は 1645 です。 認証ポートをディセーブルにするには、**ignore-auth-port** キーワードを指定します。
- アカウンティング ポートはデフォルトでイネーブルです。 ポート番号が指定されていない場合、デフォルトのポート番号は 1645 です。 アカウンティング ポートをディセーブルにするには、**ignore-acct-port** キーワードを指定します。

例

次に、使用しているシスコ リリースに応じて、host1 を RADIUS サーバとして設定し、アカウンティングと認証の両方にデフォルト ポートを使用する例を示します。

```
radius-server host host1
```

次に、host1 という RADIUS ホストで認証要求の宛先ポートとしてポート 1612 を指定し、アカウンティング要求の宛先ポートとしてポート 1616 を設定する例を示します。

```
radius-server host host1 auth-port 1612 acct-port 1616
```

回線を入力するとすべてのポート番号がリセットされるため、ホストを指定し、1 つの回線のアカウンティング ポートと認証ポートを設定する必要があります。

次に、RADIUS サーバとして IP アドレス 192.0.2.46 のホストを指定し、許可ポートおよびアカウンティング ポートとしてポート 1612 と 1616 を使用し、タイムアウト値を 6、再送信値を 5 にそ

れぞれ設定して、さらに RADIUS サーバのキーと一致する暗号キーとして「rad123」を設定する例を示します。

```
radius-server host 192.0.2.46 auth-port 1612 acct-port 1616 timeout 6 retransmit 5 key
rad123
```

アカウンティングと認証に別個のサーバを使用するには、適宜 0 ポート値を使用します。

次に、認証ではなくアカウンティングに RADIUS サーバ host1 を指定し、アカウントではなく認証に RADIUS サーバ host2 を指定する例を示します。

```
radius-server host host1.example.com auth-port 0
radius-server host host2.example.com acct-port 0
```

次に、IP アドレス 192.0.2.1 を使用して RADIUS サーバに 4 つのエイリアスを指定する例を示します。

```
radius-server host 192.0.2.1 auth-port 1646 acct-port 1645
radius-server host 192.0.2.1 alias 192.0.2.2 192.0.2.3 192.0.2.4
```

次に、サーバごとに指数バック オフ再送信をイネーブルにする例を示します。この例では、再送信は 3 回に設定され、タイムアウトは 5 秒に設定されていると仮定します。つまり、RADIUS 要求が 5 秒の遅延で、3 回送信されます。 その後、デバイスは再試行が 32 回行われるまで、毎回 2 倍になる遅延間隔を設けて RADIUS 要求の再送信を続けます。 デバイスは、再試行の間隔が 60 分の設定値を超えると再試行の間隔を 2 倍にするのを止め、60 分ごとに送信します。

pac キーワードを設定すると、可変長フィールドの PAC-Opaque をトランスポート層セキュリティ（TLS）トンネルの確立フェーズでサーバに送信できるようになります。 PAC-Opaque は、ピアの識別と認証を検証するために必要なサーバの情報を回復するために、サーバによってのみ解釈できます。 たとえば、PAC-Opaque には PAC キーと PAC のピアの ID が含まれる場合があります。PAC Opaque の形式と内容は発行する PAC サーバに固有のものです。

次に、デバイスで自動 PAC プロビジョニングを設定する例を示します。 シード デバイスでは、使用するサーバの自動 PAC プロビジョニングをイネーブルにするには、すべての RADIUS 交換がこの PAC Opaque を使用できるように PAC-Opaque がプロビジョニングされなければなりません。すべての非シード デバイスは、リンク初期化の認証フェーズ中に PAC-Opaque を取得します。

```
enable
configure terminal
radius-server host 10.0.0.1 auth-port 1812 acct-port 1813 pac
```

例

次に、使用している Cisco リリースに応じて指定されている許可およびアカウンティング ポートを使用したロードバランシングに対して RADIUS サーバ自動テストをイネーブルにする例を示します。

```
radius-server host 192.0.2.176 test username test1 auth-port 1645 acct-port 1646
```

関連コマンド

コマンド	説明
aaa accounting	課金またはセキュリティ目的のために、要求されたサービスの AAA アカウンティングをイネーブルにします。

コマンド	説明
aaa authentication ppp	PPP を実行するシリアル インターフェイス上で使用する 1 つ以上の AAA 認証方式を指定します。
aaa authorization	ネットワーク アクセスをユーザに制限するパラメータを設定します。
debug aaa test	アイドル タイマーまたはデッド タイマーが RADIUS サーバのロード バランシングについて期限切れになったときに表示されます。
load-balance	名前付き RADIUS サーバ グループに対する RADIUS サーバのロード バランシングをイネーブルにします。
ppp	PPP を使用して非同期接続を開始します。
ppp authentication	CHAP または PAP、あるいはその両方をイネーブルにし、インターフェイスで CHAP および PAP 認証が選択される順番を指定します。
radius-server key	デバイスおよびRADIUSデーモン間のすべての RADIUS コミュニケーションの認証キーおよび暗号キーを指定します。
radius-server load-balance	グローバル RADIUS サーバ グループに対して RADIUS サーバ ロード バランシングを有効にします。
radius-server retransmit	Cisco ソフトウェアが RADIUS サーバ ホストのリストを検索する回数の最大値を指定します。
radius-server timeout	サーバホストが応答するまでデバイスが待機する間隔を設定します。
test aaa group	RADIUS ロード バランシング サーバの応答を手動でテストします。
username	PPP CHAP および PAP などのユーザ名ベースの認証システムを確立します。

redirect（パラメータ マップ Web 認証）

Web 認証ログイン中に、ユーザを特定の URL にリダイレクトするには、パラメータ マップ Web 認証コンフィギュレーション モードで **redirect** コマンドを使用します。 URL を削除するには、このコマンドの **no** 形式を使用します。

redirect {{**for-login**| **on-failure**| **on-success**} *url* | **portal** {**ipv4** *ipv4-address*| **ipv6** *ipv6-address*}}

no redirect {**for-login**| **on-failure**| **on-success**| **portal** {**ipv4**| **ipv6**}}

構文の説明

for-login	ログイン用に、この URL にユーザを移動します。
on-failure	ログインが失敗すると、この URL にユーザを移動します。
on-success	ログインに成功すると、この URL にユーザを移動します。
url	有効な URL。
portal	カスタマイズされたログイン Web ページにアクセスするために、ユーザをこの外部 Web サーバに移動します。
ipv4 *ipv4-address*	ポータルの IPv4 アドレスを指定します。
ipv6 *ipv6-address*	ポータルの IPv6 アドレスを指定します。

コマンド デフォルト

ユーザはリダイレクトされません。

コマンド モード

パラメータ マップ Web 認証コンフィギュレーション（config-params-parameter-map）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

redirect コマンドを使用して、認証プロセス中に外部サーバに保存されているカスタム Web ページにユーザをリダイレクトします。

デバイスは最初の HTTP 要求をインターセプトした後、指定したポータル IP アドレスにクライアントをリダイレクトします。また、デバイスはクライアントから送信されたログインフォームをインターセプトし、ユーザ名およびパスワードを抽出して、ユーザを認証できます。

ローカルに保存されたカスタム Web ページを表示するには、**custom-page** コマンドを使用します。

redirect portal コマンドを設定すると、リダイレクト ポータル アドレスを拒否する（インターセプトしない）エントリを含むインターセプト ACL が Web 認証によって作成されます。 コマンド **redirect portal ipv4 10.51.3.34** を設定すると、**show ipv4 access-list** コマンドによって次の出力が表示されます。

```
Extended IP access list WA-v4-int-acl-pmap-PA
    10 deny tcp any host 10.51.3.34 eq www
    20 deny tcp any host 10.51.3.34 eq 443
    30 permit tcp any any eq www
    40 permit tcp any any eq 443
```

例

次に、カスタム Web ページにユーザをリダイレクトする名前付きパラメータ マップを設定する例を示します。

```
parameter-map type webauth PMAP_WEBAUTH
 type webauth
 redirect for-login http://10.10.3.34/~sample/login.html
 redirect on-success http://10.10.3.34/~sample/success.html
 redirect on-failure http://10.10.3.34/~sample/failure.html
 redirect portal ipv4 10.10.3.34
```

関連コマンド

コマンド	説明
custom-page	Web 認証ログイン時にカスタム Web ページが表示されます。
show ip admission	Web 認証セッションに関するネットワーク アドミッション キャッシュ エントリと情報を表示します。
type（パラメータ マップ Web 認証）	パラメータ マップでサポートされる認証方式を定義します。

redirect url

特定の URL にクライアントをリダイレクトするには、サービス テンプレート コンフィギュレーション モードで **redirect url** コマンドを使用します。 URL を削除するには、このコマンドの **no** 形式を使用します。

redirect url *url* [**match** *access-list-name* [**one-time-redirect**| **redirect-on-no-match**]]

no redirect url *url* [**match** *access-list-name* [**one-time-redirect**| **redirect-on-no-match**]]

構文の説明

url	有効な URL。
match *access-list-name*	（任意）一致するアクセス コントロール リストの名前を指定します。
one-time-redirect	（任意）アクセス リストと一致するトラフィックを一度のみリダイレクトします。
redirect-on-no-match	（任意）アクセス リストと一致しないトラフィックをリダイレクトします。

コマンド デフォルト

クライアントはリダイレクトされません。

コマンド モード

サービス テンプレート コンフィギュレーション（config-service-template）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

redirect url コマンドを使用して、加入者セッションでサービス テンプレートがアクティブ化されるときに、特定の URL にクライアントをリダイレクトします。

例

次に、IPアドレスがURL_ACLで定義されたアクセスリストと一致する場合に、認証後にCisco.comにクライアントをリダイレクトするSVC_2という名前のサービステンプレートを設定する例を示します。

```
ip access-list extended URL_ACL
 permit tcp any host 10.10.10.1 eq www
!
service-template SVC_2
 access-group ACL_in
 redirect url http://cisco.com match URL_ACL
 tag TAG_1
!
policy-map type control subscriber POLICY_WEBAUTH
 event authentication-success match-all
  10 class always do-until-failure
   10 activate service-template SVC_2 precedence 20
```

関連コマンド

コマンド	説明
access-group（サービス テンプレート）	サービステンプレートがセッションに適用するアクセス グループを指定します。
activate（ポリシー マップ アクション）	加入者セッションで、制御ポリシーまたはサービス テンプレートをアクティブ化します。

replace

ポートでセキュリティ違反が発生した後に、既存のセッションをクリアし、新しいセッションを作成するには、コントロールポリシーマップアクションコンフィギュレーションモードで**replace**コマンドを使用します。 制御ポリシーからこのアクションを削除するには、このコマンドの **no** 形式を使用します。

action-number **replace**

no *action-number*

構文の説明

action-number	アクション数。 アクションは、ポリシー ルール内で順番に実行されます。

コマンド デフォルト

既存のセッションはクリアされず、新しいセッションは作成されません。

コマンド モード

コントロールポリシーマップアクションコンフィギュレーション（config-action-control-policymap）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

replace コマンドは、制御ポリシーにアクションを定義します。

制御ポリシーによって、指定されたイベントと条件に応じて実行されるアクションが決定されます。 制御クラスによって、アクションを実行するために満たす必要がある条件が定義されます。アクションは、ポリシー ルール内で番号が付けられ、順番に実行されます。

class コマンドは、制御クラスを 1 つ以上のアクションに関連付けることでポリシー ルールを作成します。 ポリシー ルールに定義できるアクションは、**event** コマンドによって指定されるイベントのタイプによって異なります。

例

次に、違反イベントに設定された置換アクションと制御ポリシーを設定する方法を示します。

```
policy-map type control subscriber POLICY_1
 event violation match-all
  1 class always do-until-failure
   10 replace
```

関連コマンド

コマンド	説明
class	制御ポリシーの 1 つ以上のアクションに制御クラスを関連付けます。
event	条件が満たされる場合に、制御ポリシーでアクションをトリガーするイベントのタイプを指定します。
restrict	ポートでセキュリティ違反が発生した後に、違反パケットをドロップし、syslog メッセージを生成します。

restrict

ポートでセキュリティ違反が発生した後に、違反パケットをドロップし、syslog メッセージを生成するには、コントロール ポリシー マップ アクション コンフィギュレーション モードで **restrict** コマンドを使用します。 制御ポリシーからこのアクションを削除するには、このコマンドの **no** 形式を使用します。

action-number **restrict**

no *action-number*

構文の説明

action-number	アクション数。 アクションは、ポリシー ルール内で順番に実行されます。

コマンド デフォルト

違反パケットはドロップされず、syslog メッセージは生成されません。

コマンド モード

コントロール ポリシー マップ アクション コンフィギュレーション（config-action-control-policymap）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

restrict コマンドは、制御ポリシーにアクションを定義します。

制御ポリシーによって、指定されたイベントと条件に応じて実行されるアクションが決定されます。 制御クラスによって、アクションを実行するために満たす必要がある条件が定義されます。 アクションは、ポリシー ルール内で番号が付けられ、順番に実行されます。

class コマンドは、制御クラスを 1 つ以上のアクションに関連付けることでポリシー ルールを作成します。 ポリシー ルールに定義できるアクションは、**event** コマンドによって指定されるイベントのタイプによって異なります。

例

次に、違反イベントに設定された制限アクションと制御ポリシーを設定する方法を示します。

```
policy-map type control subscriber POLICY_1
 event violation match-all
  10 class always do-until-failure
   10 restrict
```

関連コマンド

コマンド	説明
class	制御ポリシーの 1 つ以上のアクションに制御クラスを関連付けます。
event	条件が満たされる場合に、制御ポリシーでアクションをトリガーするイベントのタイプを指定します。
replace	ポートでセキュリティ違反が発生した後に、既存のセッションをクリアし、新しいセッションを作成します。

resume reauthentication

認証の失敗後に再認証プロセスを再開するには、コントロール ポリシー マップ アクション コンフィギュレーション モードで **resume reauthentication** コマンドを使用します。 制御ポリシーからこのアクションを削除するには、このコマンドの **no** 形式を使用します。

action-number **resume reauthentication**

no *action-number*

構文の説明

action-number	アクション数。 アクションは、ポリシー ルール内で順番に実行されます。

コマンド デフォルト

再認証は再開されません。

コマンド モード

コントロール ポリシーマップ アクション コンフィギュレーション（config-action-control-policymap）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

resume reauthentication コマンドは、制御ポリシーにアクションを定義します。

制御ポリシーによって、指定されたイベントと条件に応じて実行されるアクションが決定されます。 制御クラスによって、アクションを実行するために満たす必要がある条件が定義されます。アクションは、ポリシー ルール内で番号が付けられ、順番に実行されます。

class コマンドは、制御クラスを 1 つ以上のアクションに関連付けることでポリシー ルールを作成します。 ポリシー ルールに定義できるアクションは、**event** コマンドによって指定されるイベントのタイプによって異なります。

例

次に、aaa使用可能イベントに設定されている認証再開アクションと制御ポリシーを設定する方法を示します。

```
policy-map type control subscriber POLICY
 event aaa-available match-all
  10 class CRITICAL_VLAN do-all
   10 clear-session
```

```
20 class NOT_CRITICAL_VLAN do-all
 10 resume reauthentication
```

関連コマンド

コマンド	説明
authentication-restart	認証または許可が失敗した後、認証プロセスを再開します。
class	制御ポリシーの 1 つ以上のアクションに制御クラスを関連付けます。
event	条件が満たされる場合に、制御ポリシーでアクションをトリガーするイベントのタイプを指定します。
pause reauthentication	認証の失敗後に再認証プロセスを停止します。

service-policy type control subscriber

インターフェイスに制御ポリシーを適用するには、インターフェイス コンフィギュレーション モードで **service-policy type control subscriber** コマンドを使用します。 制御ポリシーを削除するには、このコマンドの **no** 形式を使用します。

service-policy type control subscriber *control-policy-name*

no service-policy type control subscriber *control-policy-name*

構文の説明

control-policy-name	**policy-map type control subscriber** コマンドによって定義された、以前に設定された制御ポリシーの名前。設定済みのすべての制御ポリシーのリストを表示するには、疑問符（?）オンライン ヘルプ機能を使用します。

コマンド デフォルト

コントロール ポリシーは、コンテキストには適用されません。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

制御ポリシーは、1つ以上のインターフェイスに適用するとアクティブ化されます。インターフェイスでホストされるすべてのセッションに制御ポリシーが適用されます。 特定のインターフェイスに適用できる制御ポリシー マップは 1 つだけです。

例

次に、POLICY_1 という名前の制御ポリシーをインターフェイスに適用する例を示します。

```
interface TenGigabitEthernet 1/0/1
 access-session host-mode single-host
 access-session closed
 access-session port-control auto
 service-policy type control subscriber POLICY_1
```

関連コマンド

コマンド	説明
class-map type control subscriber	制御ポリシーのアクションを実行するために満たす必要のある条件を指定する制御クラスを定義します。
policy-map type control subscriber	加入者セッションの制御ポリシーを定義します。

service-template

加入者セッションに適用するサービス ポリシー属性のセットを含むテンプレートを定義するには、グローバル コンフィギュレーション モードで **service-template** コマンドを使用します。 テンプレートを削除するには、このコマンドの **no** 形式を使用します。

service-template *template-name*

no service-template *template-name*

構文の説明

template-name	サービス テンプレートを識別する英数字の名前。

コマンド デフォルト

サービス テンプレートは定義されていません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

service-template コマンドを使用して、同じ特徴を共有する加入者セッションに適用できる属性とともにグループ化します。

複数のテンプレートを定義できますが、1 回の加入者セッションに関連付けられるのは 1 つのテンプレートのみです。

例

次に、アクセス グループ ACL_2 をセッションに適用し、クライアントを www.cisco.com にリダイレクトする SVC_2 という名前のサービス テンプレートを設定する例を示します。

```
service-template SVC_2
 description label for SVC_2
 access-group ACL_2
 redirect url http://www.cisco.com
 inactivity-timer 15
 tag TAG_2
```

関連コマンド

コマンド	説明
activate（ポリシー マップ アクション）	加入者セッションで、制御ポリシーまたはサービス テンプレートをアクティブ化します。
match activated-service-template	セッションでアクティブ化されたサービステンプレートが指定されたテンプレートと一致する場合に true と評価される条件を作成します。
match service-template	イベントのサービステンプレートが指定されたテンプレートと一致する場合に true と評価される条件を作成します。

set-timer（ポリシー マップ アクション）

加入者セッションに対して名前付きポリシー タイマーを開始するには、コントロール ポリシー マップ アクション コンフィギュレーション モードで **set-timer** コマンドを使用します。 制御ポリシーからこのアクションを削除するには、このコマンドの **no** 形式を使用します。

action-number **set-timer** *timer-name seconds*

no *action-number*

構文の説明

action-number	アクション数。 アクションは、ポリシー ルール内で順番に実行されます。
timer-name	ポリシー タイマーの名前（最大 15 文字）。 これは、このアクションに対して定義されている任意の名前です。
seconds	秒単位のタイマー間隔。 範囲：1 ～ 65535。

コマンド デフォルト

名前付きポリシー タイマーは開始されません。

コマンド モード

コントロール ポリシーマップ アクション コンフィギュレーション（config-action-control-policymap）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

set-timer コマンドは、制御ポリシーにアクションを設定します。 このコマンドは、名前付きポリシー タイマーを開始します。 名前付きタイマーの期限が切れた後、システムは timer-expiry イベントを生成します。

制御ポリシーによって、指定されたイベントと条件に応じて実行されるアクションが決定されます。 制御クラスによって、アクションを実行するために満たす必要がある条件が定義されます。 アクションは、ポリシー ルール内で番号が付けられ、順番に実行されます。

class コマンドは、制御クラスを 1 つ以上のアクションに関連付けることでポリシー ルールを作成します。 ポリシー ルールに定義できるアクションは、**event** コマンドによって指定されるイベントのタイプによって異なります。

例

次に、session-start イベントに設定された set-timer アクションと制御ポリシーを設定する方法を示します。

```
class-map type control subscriber match-all CLASS_1
 match timer TIMER_A
!
policy-map type control subscriber RULE_A
 event session-start match-all
  10 class always do-until-failure
   10 set-timer TIMER_A 60
 event timer-expiry match-all
  20 class CLASS_1 do-all
   10 clear-session
```

関連コマンド

コマンド	説明
class	制御ポリシーの 1 つ以上のアクションに制御クラスを関連付けます。
event	条件が満たされる場合に、制御ポリシーでアクションをトリガーするイベントのタイプを指定します。
match timer（クラス マップ フィルタ）	イベント タイマーに基づいて true と評価される条件を作成します。

show access-session

Session Aware Networking セッションに関する情報を表示するには、特権 EXEC モードで **show access-session** コマンドを使用します。

show access-session [**[database]** [**handle** *handle-number*| [**method** *method*] [**interface** *interface-type interface-number*]| **mac** *mac-address*| **session-id** *session-id*] | **history** [**min-uptime** *seconds*]| **registrations**| **statistics**] **[details]**

構文の説明

database	（任意）セッション データベースに保存されるセッション データを表示します。 これにより、内部的にキャッシュされない VLAN ID などの情報を表示できます。 セッション データベースに格納されているデータが内部でキャッシュされているデータと一致しない場合、警告メッセージが表示されます。
handle *handle-number*	（任意）指定されたコンテキスト処理番号に関する情報を表示します。 範囲は 1 ～ 4294967295 です。
method *method*	（任意）次の認証方式の 1 つを使用する加入者セッションの情報を表示します。 • **dot1x**：IEEE 802.1X 認証方式。 • **mab**：MAC 認証バイパス（MAB）方式。 • **webauth**：Web 認証方式。 方式を指定する場合は、インターフェイスも指定できます。
interface *interface-type interface-number*	（任意）指定したクライアント インターフェイス タイプと一致する加入者セッションに関する情報を表示します。 インターフェイスの有効なキーワードと引数を表示するには、疑問符（**?**）オンライン ヘルプ機能を使用します。
mac *mac-address*	（任意）指定されたクライアントの MAC アドレスを持つ加入者セッションに関する情報を表示します。
session-id *session-id*	（任意）指定されたクライアントのセッション ID を持つ加入者セッションに関する情報を表示します。
history	（任意）セッション履歴を表示します。
min-uptime *seconds*	（任意）指定された秒数実行していたセッションのセッション履歴を表示します。 範囲は 1 ～ 4294967295 です。

registrations	（任意）登録済み認証方式を含むすべての登録済み Session Manager クライアントに関する情報を表示します。
statistics	（任意）認証セッション統計に関する情報を表示します。
details	（任意）1行のサマリーを表示する代わりに、各セッションに関する詳細情報を表示します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

キーワードまたは引数を指定せずに **show access-session** コマンドを入力すると、スイッチでのすべてのセッションに関する情報が表示されます。 ID を指定すると、その ID と一致するセッションの情報のみが表示されます。

例

次に、**show access-session** コマンドの出力例を示します。

```
Device# show access-session

Interface MAC Address Method Domain Status Fg Session ID
Gi1/0/17 0010.189c.19e8 webauth DATA Auth AC14F969000010B13CB02250

Session count = 1

Key to Session Events Blocked Status Flags:

A - Applying Policy (multi-line status for details)
D - Awaiting Deletion
F - Final Removal in progress
I - Awaiting IIF ID allocation
P - Pushed Session
R - Removing User Profile (multi-line status for details)
U - Applying User Profile (multi-line status for details)
X - Unknown Blocker
```

次に、**interface** キーワードを設定して **show access-session** コマンドを実行した場合のサンプル出力を示します。

```
Device# show access-session interface g1/0/17 details

Interface: GigabitEthernet1/0/17
IIF-ID: 0x1040E00000001DA
MAC Address: 0010.189c.19e8
IPv6 Address: Unknown
IPv4 Address: 9.9.2.5
User-Name: web
```

```
Status: Authorized
Domain: DATA
Oper host mode: multi-auth
Oper control dir: both
Session timeout: N/A
Common Session ID: AC14F969000010B13CB02250
Acct Session ID: Unknown
Handle: 0x180000C6
Current Policy: DEFAULT_WEBAUTH

Server Policies:

Method status list:
Method State
webauth Authc Success
```

次に、**registrations** キーワードを指定して **show access-session** コマンドを実行した場合のサンプル出力を示します。

```
Device# show access-session registrations

Clients registered with the Session Manager:
Handle Priority Name
1 0 Session Mgr IPDT Shim
2 0 Switch PI (IOU)
3 0 SVM
5 0 dct
6 0 iaf
7 0 Tag
8 0 SM Reauth Plugin
9 0 SM Accounting Feature
12 0 AIM
11 10 mab
10 5 dot1x
4 15 webauth
```

次の表は、この出力で表示される重要なフィールドについて説明しています。

表 *2*：*show access-session Field Descriptions*

フィールド	説明
Interface	認証インターフェイスのタイプと数。
MAC Address	クライアントの MAC アドレス。
Domain	ドメイン名。DATA または VOICE のいずれかです。

フィールド	説明
Status	認証セッションのステータス。 次の値が可能です。 • Authc Failed：このセッションに対して認証方式が実行され、認証が失敗しました。 • Authc Success：このセッションに対して認証方式が実行され、認証が成功しました。 • Authz Failed：フィーチャが失敗し、セッションは終了されました。 • Authz Success：すべてのフィーチャがセッションに適用され、セッションはアクティブです。 • Idle：このセッションは初期化されましたが、認証方式は実行されていません。 これは中間の状態です。 • No methods：このセッションの結果を出した認証方式はありません。 • Running：このセッションで認証方式が実行中です。

フィールド	説明
Fg	

フィールド	説明
	これらのステータス フラグは、多くの場合、非同期アクションが進行中であるため、セッションでイベントの処理が一時的にブロックされることを示します。 一時的なブロックは、1 秒未満から最大で数秒間実行されます。数秒以上ブロックされたままのセッションは何らかの問題を示しています。 他のフラグで表示できる P を除き、すべてのフラグは同時には使用されません。 セッション イベント ブロック ステータスフラグのキーは、以下のとおりです。 • A（ポリシーの適用中）（詳細はマルチラインのステータスを参照）：ポリシー アクション（イベント）が実行されており、進行中の非同期処理が含まれています。処理されているイベントの名前を表示するには、**details** キーワードを使用します。 • D（削除の待機中）：セッションの削除が開始されました。1 つ以上の非同期操作が現在進行中です（プラットフォームからアカウンティング データを取得するか、IF ID を削除します）。 • F（最終削除が進行中）：D 段階は終了しましたが、セッションはまだ削除されていません。 • I（IIF ID 割り当ての待機中）：IIF ID はセッション用のシステム全体の ID、またはプラットフォームが認識する必要のある他のオブジェクトです。 処理を進める前に、プラットフォームが IIF ID を取得する必要があります。 • P（プッシュされたセッション）：セッションが以前に認証され、無線コントローラ モジュール（WCM）からプッシュされたことを示します。 Session Manager は認証を実行するのではなく、セッションの追跡のみを行います。 これは無線セッション専用です。 また、セッションの永続的なフラグで、他のフラグで表示できます。

フィールド	説明
	• R（ユーザ プロファイルの削除中）（詳細についてはマルチライン ステータスを参照）：ユーザ プロファイルは Enforcement Policy Module（EPM）によって非同期的に排除されます。 • U（ユーザプロファイルを適用中）（詳細についてはマルチライン ステータスを参照）：ユーザプロファイルは、EPMによって非同期的に適用されます。 • X（不明なブロッカー）：不明な理由でイベントがブロックされています。
Handle	コンテキストのハンドル。
State	報告された認証セッションの動作状態。次の値が可能です。 • Not run：このセッションに対して方式は実行されませんでした。 • Running：このセッションに対して方式が実行中です。 • Failed over：方式は失敗し、次の方式によって結果が出される予定です。 • Success：方式によって、セッションの認証成功の結果が提供されました。 • Authc Failed：メソッドによって、セッションに関する失敗した認証結果が提供されます。

関連コマンド

コマンド	説明
policy-map type control subscriber	加入者セッションの制御ポリシーを定義します。
service-policy type control subscriber	インターフェイスに制御ポリシーを適用します。

show class-map type control subscriber

Session Aware Networking の制御クラスに関する情報を表示するには、ユーザ EXEC または特権 EXEC モードで **show class-map type control subscriber** コマンドを使用します。

show class-map type control subscriber {**all**| **name** *control-class-name*}

構文の説明

all	すべての制御クラスの出力を表示します。
name *control-class-name*	名前付き制御クラスの出力を表示します。

コマンド モード

ユーザ EXEC (>)

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

制御ポリシーによって、指定されたイベントと条件に応じて実行されるアクションが定義されます。 **show class-map type control subscriber** コマンドを使用して、クラス内の各一致条件が実行された回数など、設定された制御クラスに関する情報を表示します。

例

次に、**name** キーワードを使用した **show class-map type control subscriber** コマンドの出力例を示します。

```
Device# show class-map type control subscriber name DOT1X_AUTH

Class-map                 Action                        Exec  Hit  Miss  Comp
---------                 ------                        ----  ---  ----  ----
match-all DOT1X_AUTH      match method dot1x               0    0     0     0
match-all DOT1X_AUTH      match result-type authoritati    0    0     0     0

Key:
  "Exec" - The number of times this line was executed
  "Hit"  - The number of times this line evaluated to TRUE
  "Miss" - The number of times this line evaluated to FALSE
  "Comp" - The number of times this line completed the execution of its
           condition without a need to continue on to the end
```

出力にはフィールドの説明も表示されます。

関連コマンド

コマンド	説明
class-map type control subscriber	制御クラスを作成します。これは、制御ポリシーのアクションが実行される条件を定義します。
policy-map type control subscriber	加入者セッションの制御ポリシーを定義します。
show policy-map type control subscriber	Session Aware Networking の制御ポリシーに関する情報を表示します。

show ip admission

ネットワーク アドミッション キャッシュ エントリと Web 認証セッションに関する情報を表示するには、ユーザ EXEC または特権 EXEC モードで **show ip admission** コマンドを使用します。

Cisco IOS XE Release 3SE and Later Releases

show ip admission {**cache**| **statistics** [**brief**| **details**| **httpd**| **input-feature**]| **status** [**banners**| **custom-pages**| **httpd**| **parameter-map** [*parameter-map-name*]]| **watch-list**}

All Other Releases

show ip admission {**cache** [**consent**| **eapoudp**| **ip-addr** *ip-address*| **username** *username*]| **configuration**| **httpd**| **statistics**| [**brief**| **details**| **httpd**]| **status [httpd]**| **watch-list**}

構文の説明

cache	ネットワーク アドミッション エントリの現在のリストを表示します。
statistics	Web 認証の統計情報を表示します。
brief	（任意）Web認証の統計情報の要約を表示します。
details	（任意）Web認証の統計情報の詳細を表示します。
httpd	（任意）Web 認証 HTTP プロセスに関する情報を表示します。
input-feature	Web認証パケットに関する統計情報を表示します。
status	バナー、カスタム ページ、HTTP プロセス、およびパラメータ マップなど、設定済みの Web 認証機能に関するステータス情報を表示します。
banners	Web認証用に設定されているバナーに関する情報を表示します。

custom-pages	Web 認証用に設定されているカスタム ページに関する情報を表示します。 カスタム ファイルはローカル キャッシュに読み込まれ、キャッシュから実行されます。バックグラウンドプロセスは定期的にファイルを再キャッシュする必要があるかどうかを確認します。
parameter-map *parameter-map-name*	すべてのパラメータ マップについて、あるいは指定したパラメータ マップのみについて、設定されたバナーおよびカスタム ページに関する情報を表示します。
watch-list	ウォッチ リストに IP アドレスのリストを表示します。
consent	（任意）承諾 Web ページのキャッシュ エントリを表示します。
eapoudp	（任意）UDP（EAPoUDP）ネットワーク アドミッション キャッシュ エントリを介した拡張認証プロトコルを表示します。 ホストの IP アドレス、セッション タイムアウト、ポスチャの状態が含まれます。
ip-addr *ip-address*	（任意）クライアント IP アドレスに関する情報を表示します。
username *username*	（任意）クライアントのユーザ名に関する情報を表示します。
configuration	（任意）NAC 設定を表示します。 （注） このキーワードは、Cisco IOS XE Release 3.2SE 以降のリリースではサポートされません。 **show running-config all** コマンドを使用して、実行中の Web 認証設定と、デフォルト パラメータで設定されたコマンドを表示します。

コマンド モード

ユーザ EXEC (>)

特権 EXEC（#）

コマンド履歴

リリース	変更内容
12.3(8)T	このコマンドが導入されました。
12.4(11)T	このコマンドが変更されました。 このコマンドの出力が拡張され、AAA タイムアウト ポリシーが設定されているかどうかが表示されるようになりました。
12.4(15)T	このコマンドが変更されました。 **consent** キーワードが追加されました。
12.2(33)SXI	このコマンドが、Cisco IOS Release 12.2(33)SXI に統合されました。
15.3(1)T	このコマンドが変更されました。 **statistics**、**brief**、**details**、**httpd**、および **status** キーワードが追加されました。
Cisco IOS XE Release 3.2SE	このコマンドが変更されました。 **input-feature**、**banners**、**custom-pages**、および **parameter-map** キーワードが追加されました。**configuration** キーワードが削除されました。

使用上のガイドライン

ネットワーク アドミッション エントリと、Web 認証セッションに関する情報を表示するには、**show ip admission** コマンドを使用します。

例

次に、**show ip admission cache** コマンドの出力例を示します。

```
Device# show ip admission cache

Authentication Proxy Cache
Total Sessions: 1 Init Sessions: 1
 Client MAC 5cf3.fc25.7e3d Client IP 1.150.128.2 IPv6 :: Port 0, State INIT, Method Webauth
```

次に、**show ip admission statistics** コマンドの出力例を示します。

```
Device# show ip admission statistics

Webauth input-feature statistics:
                                                        IPv4          IPv6
  Total packets received                                46            0
    Delivered to TCP                                    46            0
    Forwarded                                           0             0
    Dropped                                             0             0
    TCP new connection limit reached                    0             0

Webauth HTTPd statistics:

  HTTPd process 1
    Intercepted HTTP requests:                          8
    IO Read events:                                     9
    Received HTTP messages:                             7
    IO write events:                                    11
    Sent HTTP replies:                                  7
```

```
    IO AAA messages:                                4
    SSL OK:                                         0
    SSL Read would block:                           0
    SSL Write would block:                          0
    HTTPd process scheduled count:                  23
```

次に、**show ip admission status** コマンドの出力例を示します。

```
Device# show ip admission status

IP admission status:
  Enabled interfaces            1
  Total sessions                1
  Init sessions                 1     Max init sessions allowed     100
    Limit reached               0     Hi watermark                  1
  TCP half-open connections     0     Hi watermark                  0
  TCP new connections           0     Hi watermark                  0
  TCP half-open + new           0     Hi watermark                  0
  HTTPD1 Contexts               0     Hi watermark                  1

  Parameter Map: Global
    Custom Pages
      Custom pages not configured
    Banner
      Banner not configured

  Parameter Map: PMAP_WEBAUTH
    Custom Pages
      Custom pages not configured
    Banner
      Type: text
        Banner                  " <H2>Login Page Banner</H2> "
        Html                    " <H2>Login Page Banner</H2> "
        Length                  48

  Parameter Map: PMAP_CONSENT
    Custom Pages
      Custom pages not configured
    Banner
      Banner not configured

  Parameter Map: PMAP_WEBCONSENT
    Custom Pages
      Custom pages not configured
    Banner
      Banner not configured

  Parameter Map: PMAP_WEBAUTH_CUSTOM_FLASH
    Custom Pages
      Type: "login"
        File                    flash:webauth_login.html
        File status             Ok - File cached
        File mod time           2012-07-20T02:29:36.000Z
        File needs re-cached    No
        Cache                   0x3AEE1E1C
        Cache len               246582
        Cache time              2012-09-18T13:56:57.000Z
        Cache access            0 reads, 1 write
      Type: "success"
        File                    flash:webauth_success.html
        File status             Ok - File cached
        File mod time           2012-02-21T06:57:28.000Z
        File needs re-cached    No
        Cache                   0x3A529B3C
        Cache len               70
        Cache time              2012-09-18T13:56:57.000Z
        Cache access            0 reads, 1 write
      Type: "failure"
        File                    flash:webauth_fail.html
        File status             Ok - File cached
        File mod time           2012-02-21T06:55:49.000Z
        File needs re-cached    No
        Cache                   0x3A5BEBC4
        Cache len               67
```

```
        Cache time              2012-09-18T13:56:57.000Z
        Cache access            0 reads, 1 write
      Type: "login expired"
        File                    flash:webauth_expire.html
        File status             Ok - File cached
        File mod time           2012-02-21T06:55:25.000Z
        File needs re-cached    No
        Cache                   0x3AA20090
        Cache len               69
        Cache time              2012-09-18T13:56:57.000Z
        Cache access            0 reads, 1 write
    Banner
      Banner not configured

  Parameter Map: PMAP_WEBAUTH_CUSTOM_EXTERNAL
    Custom Pages
      Custom pages not configured
    Banner
      Banner not configured
```

次に、**banner text** コマンドを使用して設定されたバナーに対する **show ip admission status banners** コマンドの出力例を示します。

```
Device# show ip admission status banners

IP admission status:
  Parameter Map: Global
    Banner not configured

  Parameter Map: PMAP_WEBAUTH
    Type: text
      Banner                    " <H2>Login Page Banner</H2> "
      Html                      " <H2>Login Page Banner</H2> "
      Length                    48
```

次に、**banner file** コマンドを使用して設定されたバナーに対する **show ip admission status banners** コマンドの出力例を示します。

```
Device# show ip admission status banners

IP admission status:
  Parameter Map: Global
    Banner not configured

  Parameter Map: PMAP_WEBAUTH
    Type: file
      Banner                    <h2>Cisco Systems</h2>
<h3>Webauth Banner from file</h3>

      Length                    60
      File                      flash:webauth_banner1.html
      File status               Ok - File cached
      File mod time             2012-07-24T07:07:09.000Z
      File needs re-cached      No
      Cache                     0x3AF6CEE4
      Cache len                 60
      Cache time                2012-09-19T10:13:59.000Z
      Cache access              0 reads, 1 write
```

次に、**show ip admission status custom pages** コマンドの出力例を示します。

```
Device# show ip admission status custom pages

IP admission status:
  Parameter Map:  Global
    Custom pages not configured
  Parameter Map:  PMAP_WEBAUTH
    Type: "login"
      File                      flash:webauth_login.html
      File status               Ok - File cached
      File mod time             2012-07-20T02:29:36.000Z
      File needs re-cached      No
      Cache                     0x3B0DCEB4
      Cache len                 246582
```

```
    Cache time                2012-09-18T16:26:13.000Z
    Cache access              0 reads, 1 write
  Type: "success"
    File                      flash:webauth_success.html
    File status               Ok - File cached
    File mod time             2012-02-21T06:57:28.000Z
    File needs re-cached      No
    Cache                     0x3A2E9090
    Cache len                 70
    Cache time                2012-09-18T16:26:13.000Z
    Cache access              0 reads, 1 write
  Type: "failure"
    File                      flash:webauth_fail.html
    File status               Ok - File cached
    File mod time             2012-02-21T06:55:49.000Z
    File needs re-cached      No
    Cache                     0x3AF6D1A4
    Cache len                 67
    Cache time                2012-09-18T16:26:13.000Z
    Cache access              0 reads, 1 write
  Type: "login expired"
    File                      flash:webauth_expire.html
    File status               Ok - File cached
    File mod time             2012-02-21T06:55:25.000Z
    File needs re-cached      No
    Cache                     0x3A2E8284
    Cache len                 69
    Cache time                2012-09-18T16:26:13.000Z
    Cache access              0 reads, 1 write
Parameter Map:  PMAP_CONSENT
  Custom pages not configured
```

次の表に、上記の出力で表示される重要なフィールドについて説明します。

表 *3*：*show ip admission* フィールドの説明

File mod time	ファイルがファイルシステムに変更されたときのタイムスタンプ。
Cache time	ファイルが最後にキャッシュに読み込まれたときのタイムスタンプ。

次の出力では、ルータに設定されているすべての IP アドミッション制御ルールを示します。

```
Device# show ip admission configuration

Authentication Proxy Banner not configured
Consent Banner is not configured
Authentication Proxy webpage
        Login page              : flash:test1.htm
        Success page            : flash:test1.htm
        Fail page               : flash:test1.htm
        Login Expire page       : flash:test1.htm
Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication global init state time is 5 minutes
Authentication Proxy Watch-list is disabled

Authentication Proxy Max HTTP process is 7
Authentication Proxy Auditing is disabled
Max Login attempts per user is 5
```

次の出力では、ホスト IP アドレス、セッション タイムアウト、およびポスチャの状態を示します。 ポスチャの状態が POSTURE ESTAB である場合、ホスト検証は成功しました。

```
Device# show ip admission cache eapoudp

Posture Validation Proxy Cache
Total Sessions: 3 Init Sessions: 1
 Client IP 10.0.0.112, timeout 60, posture state POSTURE ESTAB
 Client IP 10.0.0.142, timeout 60, posture state POSTURE INIT
 Client IP 10.0.0.205, timeout 60, posture state POSTURE ESTAB
```

出力にはフィールドの説明も表示されます。

関連コマンド

コマンド	説明
banner（パラメータ マップ Web 認証）	Web 認証ログイン Web ページにバナーを表示します。
clear ip admission cache	ルータからの IP アドミッション キャッシュ エントリをクリアします。
custom-page	Web 認証ログイン時にカスタム Web ページが表示されます。
ip admission name	レイヤ3ネットワーク アドミッション制御ルールを作成します。

show policy-map type control subscriber

Session Aware Networking の制御ポリシーに関する情報を表示するには、ユーザ EXEC または特権 EXEC モードで **show policy-map type control subscriber** コマンドを使用します。

show policy-map type control subscriber {**all**| **name** *control-policy-name*}

構文の説明

all	すべての制御ポリシーの出力を表示します。
name *control-policy-name*	名前付き制御ポリシーの出力を表示します。

コマンド モード

ユーザ EXEC (>)

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

制御ポリシーによって、指定されたイベントと条件に応じて実行されるアクションが定義されます。 **show policy-map type control subscriber** コマンドを使用して、ポリシーマップ内の各ポリシールールが実行された回数など、設定された制御ポリシーに関する情報を表示します。

例

次に、**name** キーワードを使用した **show policy-map type control subscriber** コマンドの出力例を示します。

```
Device# show policy-map type control subscriber name POLICY_1

Control_Policy: POLICY_1
  Event:      event session-started match-all
    Class-map:  10 class always do-until-failure
      Action: 10 authenticate using dot1x retries 3 retry-time 15
      Executed: 0

  Event:      event authentication-failure match-all
    Class-map:  10 class DOT1X_AUTH do-until-failure
      Action: 10 authenticate using mab
      Executed: 0

    Class-map:  20 class DOT1X_METHOD_TIMEOUT do-until-failure
      Action: 10 authenticate using mab
      Executed: 0
```

```
    Class-map:  30 class MAB_AUTH do-until-failure
      Action: 10 authenticate using webauth retries 3 retry-time 15
      Executed: 0

    Class-map:  40 class AAA_TIMEOUT do-until-failure
      Action: 10 activate service-template FALLBACK
      Executed: 0

  Event:      event aaa-available match-all
    Class-map:  10 class always do-until-failure
      Action: 10 authenticate using dot1x
      Executed: 0


Key:
  "Executed" - The number of times this rule action line was executed
```

出力にはフィールドの説明も表示されます。

関連コマンド

コマンド	説明
class-map type control subscriber	制御ポリシーのアクションを実行するために満たす必要のある条件を指定する制御クラスを定義します。
event	制御クラスの評価を開始するイベントのタイプを指定します。
policy-map type control subscriber	加入者セッションの制御ポリシーを定義します。
show class-map type control subscriber	Session Aware Networking の制御クラスに関する情報を表示します。

show service-template

設定されたサービス テンプレートに関する情報を表示するには、特権 EXEC モードで **show service-template** コマンドを使用します。

show service-template [*template-name*]

構文の説明

template-name	（任意）サービス テンプレートの名前。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

サービステンプレートは、加入者セッションに適用できるサービスポリシー属性を定義します。**show service-template** コマンドを使用して、設定されたサービス テンプレートに関する情報を表示します。 *service-template* 引数を設定せずにこのコマンドを使用すると、設定されたすべてのサービス テンプレートの要約が表示されます。

例

次に、設定されたサービス テンプレートのリストを表示する **show service-template** コマンドの出力例を示します。

```
Device# show service-template

  Policy Name     Description
================================================
    L3_default_acce NONE
    SVC_2           label for SVC_2
```

次に、SVC_2 という名前のテンプレートの設定情報を表示する、*template-name* 引数を使用した **show service-template** コマンドの出力例を示します。

```
Device# show service-template SVC_2

    Name                      :  SVC_2
    Description               :  label for SVC_2
    VLAN                      :  NONE
    URL_Redirect URL          :  www.cisco.com
    URL-Redirect Match ACL    :  NONE
```

関連コマンド

コマンド	説明
match service-template	イベントのサービステンプレートが指定されたテンプレートと一致する場合に true と評価される条件を作成します。
service-template	サービス テンプレートを定義します。

subscriber aging

加入者セッションの非アクティブタイマーをイネーブルにするには、インターフェイスコンフィギュレーション モードで **subscriber aging** コマンドを使用します。 デフォルトに戻るには、**no** 形式のコマンドを使用します。

subscriber aging {[**inactivity-timer** *seconds*] **[probe]**}

no subscriber aging

構文の説明

inactivity-timer *seconds*	セッションを非アクティブにできる最大時間（秒）。 範囲：1 ～ 65535。デフォルトは0で、タイマーはディセーブルになっています。
probe	アドレス解決プロトコル(ARP)プローブをイネーブルにします。

コマンド デフォルト

非アクティビティ タイマーはディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

subscriber aging コマンドを使用して、エンドクライアントからのアクティビティやデータがない状態で加入者セッションが存在できる最大時間を設定します。 アクティビティまたはデータが得られる前にこのタイマーが切れると、セッションはクリアされます。

例

次に、10 ギガビット イーサネット インターフェイス 1/0/2 上で非アクティビティ タイマーを 60 秒に設定する例を示します。

```
interface TenGigabitEthernet 1/0/2
 subscriber aging inactivity-timer 60 probe
 service-policy type control subscriber POLICY_1
```

関連コマンド

inactivity-timer	加入者セッションの非アクティブタイムアウトをイネーブルにします。
ip device tracking probe	デバイスのプローブのトラッキングをイネーブルにします。
service-policy type control subscriber	インターフェイスに制御ポリシーを適用します。

subscriber mac-filtering security-mode

MAC フィルタリング用の RADIUS 互換モードを指定するには、サーバ グループ コンフィギュレーション モードで **subscriber mac-filtering security-mode** コマンドを使用します。 デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

subscriber mac-filtering security-mode {**mac**| **none**| **shared-secret**}

no subscriber mac-filtering security-mode {**mac**| **none**| **shared-secret**}

構文の説明

mac	パスワードとして MAC アドレスを送信します。
none	パスワード属性を送信しません。 768 ビットは、デフォルト値です。
shared-secret	パスワードとして共有秘密を送信します。

コマンド デフォルト

セキュリティ モードは none に設定されます。

コマンド モード

サーバ グループ コンフィギュレーション（config-sg-radius）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

subscriber mac-filtering security-mode コマンドを使用して、RADIUS 互換性もーとで MAC フィルタリングに使用されるセキュリティのタイプを設定します。

例

次に、パスワードとして MAC アドレスを送信するように、MAC フィルタリングを指定してサーバ グループを設定する例を示します。

```
aaa group server radius LAB_RAD
 key-wrap enable
 subscriber mac-filtering security-mode mac
 mac-delimiter colon
```

関連コマンド

コマンド	説明
key-wrap enable	AES キー ラップをイネーブルにします。
mac-delimiter	RADIUS の互換モード用の MAC デリミタを指定します。
radius-server host	RADIUS サーバ ホストを指定します。

tag（サービス テンプレート）

サービス テンプレートとユーザ定義のタグを関連付けるには、サービス テンプレート コンフィギュレーション モードで **tag** コマンドを使用します。 タグを削除するには、このコマンドの **no** 形式を使用します。

tag *tag-name*

no tag *tag-name*

構文の説明

tag-name	タグ名として割り当てられた任意のテキスト文字列。

コマンド デフォルト

タグは、サービス テンプレートに関連付けられません。

コマンド モード

サービス テンプレート コンフィギュレーション（config-service-template）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

tag コマンドを使用して、ID タグとサービス テンプレートを関連付けます。 セッションで制御ポリシーによってサービス テンプレートがアクティブ化されると、タグがセッションに適用されます。

ポリシーのセットをタグに関連付けることができます。また、認証、許可、およびアカウンティング（AAA）サーバが認証応答への応答で同じタグを送信すると、そのタグに関連付けられたポリシーがホストで適用されます。

例

次に、SVC_1 という名前のサービステンプレートを TAG_1 に関連付ける例を示します。これは、CLASS_1 という名前の制御クラスで一致条件として使用されます。

```
service-template SVC_1
 description label for SVC_1
 redirect url www.cisco.com match ACL_1
 inactivity-timer 30
 tag TAG_1
!
```

```
class-map type control subscriber match-all CLASS_1
  match tag TAG_1
```

関連コマンド

コマンド	説明
activate（ポリシー マップ アクション）	加入者セッションで、制御ポリシーまたはサービス テンプレートをアクティブ化します。
event	制御クラスの評価を開始するイベントのタイプを指定します。
match tag	イベントのタグが指定されたタグと一致する場合に true と評価される条件を作成します。

terminate

加入者セッションで認証方式を終了するには、コントロールポリシーマップアクションコンフィギュレーション モードで **terminate** コマンドを使用します。 制御ポリシーからこのアクションを削除するには、このコマンドの **no** 形式を使用します。

action-number **terminate**{**dot1x**| **mab**| **webauth**}

no *action-number*

構文の説明

action-number	アクション数。 アクションは、ポリシー ルール内で順番に実行されます。
dot1x	IEEE 802.1X 認証方式を指定します。
mab	MAC認証バイパス（MAB）方式を指定します。
webauth	Web 認証方式を指定します。

コマンド デフォルト

認証方式は終了されません。

コマンド モード

コントロールポリシーマップアクションコンフィギュレーション（config-action-control-policymap）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

terminate コマンドは、制御ポリシーにアクションを定義します。

制御ポリシーによって、指定されたイベントと条件に応じて実行されるアクションが決定されます。 制御クラスによって、アクションを実行するために満たす必要がある条件が定義されます。 アクションは、ポリシー ルール内で番号が付けられ、順番に実行されます。

class コマンドは、制御クラスを 1 つ以上のアクションに関連付けることでポリシー ルールを作成します。

制御ポリシーを設定する場合は、ある認証方式を終了してから、別の認証方式を開始する必要があります。 Session Aware Networking は、次の方式を試みる前に自動的に現在の方式を終了しませ

ん。 このため、並列認証の場合、ある方式を明示的に終了する前に、よりプライオリティの高い別のメソッドが受け継ぐポリシー ルールを設定する必要があります。

例

次に、終結アクションを含む制御ポリシーを設定する例を示します。

```
policy-map type control subscriber POLICY_3
 event session-start
  10 class always
   10 authenticate using dot1x
 event agent-not-found
  10 class DOT1X
   10 terminate dot1x
   20 authenticate using mab
 event authentication-success
  10 class DOT1X
   10 terminate mab
   20 terminate web-auth
  20 class MAB
   10 terminate web-auth
```

関連コマンド

コマンド	説明
authenticate using	指定した方式を使用して加入者セッションの認証を開始します。
class	制御ポリシーの 1 つ以上のアクションに制御クラスを関連付けます。
event	制御クラスの評価を開始するイベントのタイプを指定します。

timeout init-state min

Web 認証セッションの開始（Init）ステート タイムアウトを設定するには、パラメータ マップ タイプ Web 認証コンフィギュレーション モードで **timeout init-state min** コマンドを使用します。 タイムアウトをデフォルト値にリセットするには、このコマンドの **no** 形式を使用します。

timeout init-state min *minutes*

no timeout init-state min *minutes*

構文の説明

minutes	分単位の Init ステートの最大遅延時間。 範囲：1 ～ 65535。 デフォルト：2。

コマンド デフォルト

Init ステートのタイムアウトは 2 分です。

コマンド モード

パラメータ マップ タイプ Web 認証コンフィギュレーション（config-params-parameter-map）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

timeout init-state min コマンドを使用して、Web 認証セッションが Init ステートを維持できる分数を制限します。 セッションは、ユーザが自分のユーザ名とパスワードの資格情報を入力するまで、Init ステートのままになります。 ユーザが自分の資格情報を入力する前にタイマーが期限切れになると、セッションはクリアされます。

例

次に、MAP_2 という名前のパラメータ マップで Init タイムアウトを 15 分に設定する例を示します。

```
parameter-map type webauth MAP_2
 type webauth
 timeout absolute min 30
 timeout init-state min 15
 max-login-attempts 5
```

関連コマンド

コマンド	説明
max-login-attempts	Web 認証セッションに対するログイン試行の回数を制限します。
timeout absolute min	Web 認証セッションに対して絶対タイムアウトを設定します。

type（パラメータ マップ Web 認証）

パラメータ マップでサポートされる認証方式を定義するには、パラメータ マップ Web 認証コンフィギュレーション モードで **type** コマンドを使用します。 デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

type {**authbypass**| **consent**| **webauth**| **webconsent**}

no type {**authbypass**| **consent**| **webauth**| **webconsent**}

構文の説明

authbypass	認証バイパスを指定します。応答のないホストの（NRH）認証を使用してアクセスできます。
consent	承諾のみを指定します。ユーザ名とパスワードの資格情報の入力を求めるプロンプトを表示せずにデフォルトのアクセスを許可します。代わりに、ユーザは同意するか同意しないことを示す 2 つのオプション ボタンを選択できます。アカウンティングの目的で、デバイスは認証、許可、およびアカウンティング（AAA）サーバにクライアントの MAC アドレスを渡します。
webauth	Web 認証のみを指定します。 ユーザの権限に基づいてアクセスを許可します。デバイスは、認証とアカウンティング用にAAAサーバにユーザ名とパスワードを送信します。 768 ビットは、デフォルト値です。
webconsent	Web 認証と承諾を指定します。

コマンド デフォルト

タイプは Web 認証（webauth）です。

コマンド モード

パラメータ マップ Web 認証コンフィギュレーション（config-params-parameter-map）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

type コマンドを使用して、マップ内のパラメータが適用される認証方式を指定します。 パラメータ マップはポリシーマップで指定されたアクションの動作を制御するパラメータを定義します。

このコマンドは、名前付きパラメータ マップでのみサポートされます。

例

次に、Web 認証のデフォルトにタイプを指定して、パラメータ マップを設定する例を示します。

```
parameter-map type webauth PMAP_3
 type webauth
 timeout init-state min 15
 banner file flash:webauth_banner.html
```

関連コマンド

コマンド	説明
banner（パラメータ マップ Web 認証）	Web 認証 Web ページにバナーを表示します。
consent email	承諾ログイン Web ページでユーザの電子メール アドレスを要求します。
custom-page	Web 認証ログイン時にカスタム Web ページが表示されます。
redirect（パラメータ マップ Web 認証）	Web 認証中に、ユーザを特定の URL にリダイレクトします。

unauthorize

ポートを無許可にして、以前の許可データに基づいて付与されたすべてのアクセス権限を削除するには、コントロール ポリシーマップ アクション コンフィギュレーション モードで **unauthorize** コマンドを使用します。 制御ポリシーからこのアクションを削除するには、このコマンドの **no** 形式を使用します。

action-number **unauthorize**

no *action-number*

構文の説明

action-number	アクション数。 アクションは、ポリシー ルール内で順番に実行されます。

コマンド デフォルト

許可データは削除されません。

コマンド モード

コントロール ポリシーマップ アクション コンフィギュレーション（config-action-control-policymap）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

unauthorize コマンドは、制御ポリシーにアクションを定義します。 このコマンドは、ユーザ プロファイルやアクティブ化されたサービス テンプレートなど、以前の許可データに基づいて付与されたすべてのアクセス権限を削除します。

制御ポリシーによって、指定されたイベントと条件に応じて実行されるアクションが決定されます。 制御クラスによって、アクションを実行するために満たす必要がある条件が定義されます。 アクションは、ポリシー ルール内で番号が付けられ、順番に実行されます。

class コマンドは、制御クラスを 1 つ以上のアクションに関連付けることでポリシー ルールを作成します。

例

次に、非アクティブタイムアウトイベントに設定された無許可アクションとともに制御ポリシーを設定する方法を示します。

```
policy-map type control subscriber POLICY
 event inactivity-timeout match-all
  10 class always
   10 unauthorize
```

関連コマンド

コマンド	説明
authorize	加入者セッションの認証を開始します。
class	制御ポリシーの 1 つ以上のアクションに制御クラスを関連付けます。
class-map type control subscriber	制御クラスを作成します。これは、制御ポリシーのアクションが実行される条件を定義します。
policy-map type control subscriber	加入者セッションの制御ポリシーを定義します。

virtual-ip

Web 認証クライアントの仮想 IP アドレスを指定するには、パラメータ マップ Web 認証コンフィギュレーション モードで **virtual-ip** コマンドを使用します。 アドレスを削除するには、このコマンドの **no** 形式を使用します。

virtual-ip {**ipv4** *ipv4-address*| **ipv6** *ipv6-address*}

no virtual-ip {**ipv4**| **ipv6**}

構文の説明

ipv4 *ipv4-address*	IPv4 アドレスを仮想 IP アドレスとして使用するように指定します。
ipv6 *ipv6-address*	IPv6 アドレスを仮想 IP アドレスとして使用するように指定します。

コマンド デフォルト

仮想 IP アドレスは設定されていません。

コマンド モード

パラメータ マップ Web 認証コンフィギュレーション（config-params-parameter-map）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

仮想 IP アドレスを Web 認証クライアントに使用するには、**virtual-ip** コマンドを使用します。

デフォルトまたはローカル カスタム ページを使用する場合、仮想 IP アドレスを設定すると、クライアントが正常に認証された後にログアウト Web ページが表示されます。 これにより、ユーザはログアウトページのリンクをクリックしてログアウトすることができます。ログアウト要求は仮想 IP アドレスに送信され、デバイスによってインターセプトされます（ログアウト要求がインターセプトされるように、ACL は自動的に作成されます）。

外部サーバからカスタムページやその他のファイルを処理するには、仮想IPアドレスを設定する必要があります。 ユーザがログインフォームに自分の資格情報を入力すると、クライアントを認証できるように、そのフォームが仮想 IP アドレスに送信され、デバイスによってインターセプトされます。

仮想IPアドレスは、ネットワーク上のアドレスまたはデバイスのアドレス以外にする必要があります。

このコマンドは、グローバル パラメータ マップでのみサポートされます。

例

次に、Web 認証用にグローバル パラメータ マップで仮想 IP アドレスを FE80::1 に設定する例を示します。

```
parameter-map type webauth global
 timeout init-state min 15
 watch-list enabled
 virtual-ip ipv6 FE80::1
```

関連コマンド

コマンド	説明
authenticate using	指定した方式を使用して加入者セッションの認証を開始します。

vlan（サービス テンプレート）

加入者セッションに VLAN を割り当てるには、サービス テンプレート コンフィギュレーション モードで **vlan** コマンドを使用します。 VLAN をディセーブルにするには、このコマンドの **no** 形式を使用します。

vlan *vlan-id*

no vlan *vlan-id*

構文の説明

vlan-id	VLAN 識別番号。 範囲は 1 ～ 4094 です。

コマンド デフォルト

サービス テンプレートは VLAN を割り当てません。

コマンド モード

サービス テンプレート コンフィギュレーション（config-service-template）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

vlan コマンドを使用して、サービステンプレートがアクティブ化されるセッションに VLAN を割り当てます。

例

次に、VLAN を適用するサービス テンプレートを設定する例を示します。

```
service-template SVC_2
 description label for SVC_2
 redirect url www.google.com
 vlan 215
 inactivity-timer 30
```

関連コマンド

コマンド	説明
activate（ポリシー マップ アクション）	加入者セッションで、制御ポリシーまたはサービス テンプレートをアクティブ化します。

コマンド	説明
tag	サービステンプレートとユーザ定義のタグを関連付けます。

watch-list

Web 認証クライアントのウォッチ リストをイネーブルにするには、パラメータ マップ Web 認証コンフィギュレーション モードで **watch-list** コマンドを使用します。 デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

watch-list {**add-item** {**ipv4** *ipv4-address*| **ipv6** *ipv6-address*}| **dynamic-expiry-timeout** *minutes*| **enabled**}

no watch-list {**add-item** {**ipv4** *ipv4-address*| **ipv6** *ipv6-address*}| **dynamic-expiry-timeout** *minutes*| **enabled**}

構文の説明

add-item	ウォッチ リストに IP アドレスを追加します。
ipv4 *ipv4-address*	クライアントの IPv4 アドレスをウォッチ リストに追加することを指定します。
ipv6 *ipv6-address*	クライアントの IPv6 アドレスをウォッチ リストに追加することを指定します。
dynamic-expiry-timeout *minutes*	エントリがウォッチリストに残る時間を分単位で設定します。 有効な範囲：0 ～ 2147483647。デフォルトは 30 です。 0（ゼロ）を指定すると、エントリはリストに永続的に保持されます。
enabled	ウォッチ リストをイネーブルにします。

コマンド デフォルト

ウォッチ リストはディセーブルです。

コマンド モード

パラメータ マップ Web 認証コンフィギュレーション（config-params-parameter-map）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

watch-list コマンドを使用して、特定の Web 認証クライアントの接続をモニタします。 ウォッチ リストをイネーブルにすると、次のいずれかのイベントが発生した後に、Web 認証によってクライアントがウォッチ リストに動的に追加されます。

- **ip admission max-login-attempts** コマンドで設定された許可されるログイン最大試行回数をクライアントが超過した場合。
- **max-http-conns** コマンドで指定された許可されるオープン TCP セッションの最大数（デフォルトは 30）をクライアントが超過した場合。

IP アドレスがウォッチ リストに追加されると、**dynamic-expiry-timeout** キーワードで設定したタイマーが期限切れになるまで、この IP アドレス（ポート 80）から新しい接続は受け入れられません。

add-item キーワードを使用して、IP アドレスをウォッチ リストに手動で追加できます。

ウォッチリストをディセーブルにすると、新しいエントリはウォッチ リストに追加されなくなり、セッションは SERVICE_DENIED ステートになります。

このコマンドは、グローバル パラメータ マップでのみサポートされます。

例

次に、ウォッチ リストがイネーブルに設定され、タイムアウトが 20 分に設定されているグローバル パラメータ マップを設定する例を示します。

```
parameter-map type webauth global
 watch-list enabled
 watch-list dynamic-expiry-timeout 20
```

（注） **add-item** キーワードを使用してウォッチ リストに追加するエントリは実行中の設定には表示されません。 これらのエントリを表示するには、**show ip admission watch-list** コマンドを使用します。

関連コマンド

コマンド	説明
ip admission max-login-attempts	ログイン試行の回数を制限します。
show ip-admission watch-list	ウォッチ リストに IP アドレスのリストを表示します。