Identity-Based Networking Services コンフィギュレーション ガイド Cisco IOS XE Release 3SE（Catalyst 3650 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。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。 このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。 このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。 添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。 シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。 マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。 説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2013 Cisco Systems, Inc. All rights reserved.

目 次

Identity-Based Networking Services の概要 1

機能情報の確認 1

Identity-Based Networking Services に関する情報 1

Identity-Based Networking Services の理解 1

Identity-Based Networking Services の機能 2

Identity-Based Networking Services のメリット 3

コモン セッション ID に対する Web 認証のサポート 3

IPv6 の Web 認証のサポート 3

その他の関連資料 4

Identity-Based Networking Services の機能情報の概要 5

アイデンティティ制御ポリシーの設定 7

機能情報の確認 7

アイデンティティ制御ポリシーに関する情報 8

並列認証方式 8

表示モードの設定 8

Identity-Based Networking Services の制御ポリシー 9

制御ポリシーの設定の概要 10

Identity-Based Networking Services 用のパラメータ マップ 11

複数の方式に対するユーザごとの非アクティブ化処理 11

アイデンティティ制御ポリシーの設定方法 11

Identity-Based Networking Services の表示モードのイネーブル化 11

制御クラスの設定 12

制御ポリシーの設定 17

インターフェイスへの制御ポリシーの適用 22

ポートでの認証機能の設定 23

Web ベース認証のパラメータ マップの設定 25

アイデンティティ制御ポリシーの設定例 29

例：並列認証方式の制御ポリシーの設定 29
例：連続認証方式の制御ポリシーの設定 30
例：パラメータ マップの設定 31
その他の関連資料 33
アイデンティティ制御ポリシーの機能情報 34
アイデンティティ サービス テンプレートの設定 37
機能情報の確認 37
アイデンティティ サービス テンプレートの前提条件 38
アイデンティティ サービス テンプレートに関する情報 38
Identity-Based Networking Services 用のサービス テンプレート 38
ダウンロード可能なサービス テンプレート 38
ローカルで設定されたサービス テンプレート 39
アイデンティティ サービス テンプレートの設定方法 39
ローカル サービス テンプレートの設定 39
アイデンティティ サービス テンプレートの設定例 42
例：サービス テンプレートのアクティブ化とすべての置き換え 42
例：フォールバック サービスのサービス テンプレートのアクティブ化 42
例：サービス テンプレートの非アクティブ化 43
その他の関連資料 44
アイデンティティ サービス テンプレートの機能に関する情報 45
認可変更のサポート 47
機能情報の確認 47
CoA のサポートに関する情報 48
RADIUS 認可変更のサポート 48
セッションの識別 49
CoA サービスのアクティブ化コマンド 49
CoA サービスの非アクティブ化コマンド 50
CoA ホスト ポートのバウンス コマンド 50
CoA ホスト ポートのディセーブル化コマンド 51
CoA セッション クエリー コマンド 51
CoA セッションの再認証コマンド 51
CoA セッションの終了コマンド 52

その他の関連資料 53
CoA サポートの機能情報 54
LDAP を使用したローカル認証の設定 55
機能情報の確認 55
LDAP を使用したローカル認証に関する情報 56
LDAP を使用したローカル認証 56
AES キー ラップ 56
LDAP を使用したローカル認証の設定方法 56
LDAP を使用したローカル認証の設定 56
MAC フィルタリング サポートの設定 57
AES キー ラップのイネーブル化 59
LDAP を使用したローカル認証の設定例 60
例：LDAP を使用したローカル認証の設定 60
例：MAC フィルタリング サポートの設定 60
例：AES キー ラップの設定 60
その他の関連資料 61
LDAP を使用したローカル認証の機能情報 62
クリティカル音声 VLAN のサポート 63
機能情報の確認 63
クリティカル音声 VLAN のサポートに関する制限 64
クリティカル音声 VLAN サポートに関する情報 64
マルチドメイン認証モードでのクリティカル音声 VLAN のサポート 64
マルチ認証モードでのクリティカル音声 VLAN のサポート 64
サービス テンプレートでのクリティカル音声 VLAN のサポート 65
クリティカル音声 VLAN サポートの設定方法 65
サービス テンプレートでの音声 VLAN の設定 65
クリティカル音声 VLAN のアクティブ化 68
クリティカル音声 VLAN サポートの設定例 71
例：サービス テンプレートでの音声 VLAN の設定 71
例：サービス テンプレートでのクリティカル音声 VLAN のアクティブ化 71
クリティカル音声 VLAN のサポートに関するその他の関連資料 72
クリティカル音声 VLAN サポートの機能情報 72

有線ゲスト アクセス 75
機能情報の確認 76
有線ゲスト アクセスに関する制限 76
有線ゲスト アクセスについて 76
有線ゲスト アクセスの概要 76
統合されたゲスト アクセス ソリューション 77
CAPWAP トンネリング 78
有線ゲスト アクセスの設定方法 79
ゲスト LAN の設定 79
サービス テンプレートでの CAPWAP トンネルの設定 80
CAPWAP フォワーディングの設定 83
有線ゲスト アクセスの設定例 84
例：サービス テンプレートでの CAPWAP トンネルの設定 84
例：モビリティ エージェントの設定 85
例：モビリティ コントローラの設定 86
例：ゲスト コントローラの設定 86
例：CAPWAP フォワーディングの設定 87
有線ゲスト アクセスに関するその他の関連資料 87
有線ゲスト アクセスの機能情報 88

第 1 章

Identity-Based Networking Services の概要

Identity-Based Networking Services は、エッジデバイスが加入者に対して柔軟かつスケーラブルなサービスを提供できる、ポリシーとアイデンティティ ベースのフレームワークを提供します。このモジュールでは、Identity-Based Networking Services の内容と、このサービスの機能とメリットについての情報を提供します。

- 機能情報の確認，1 ページ
- Identity-Based Networking Services に関する情報，1 ページ
- その他の関連資料，4 ページ
- Identity-Based Networking Services の機能情報の概要，5 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を確認し、各機能がサポートされているリリースのリストを確認するには、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

Identity-Based Networking Services に関する情報

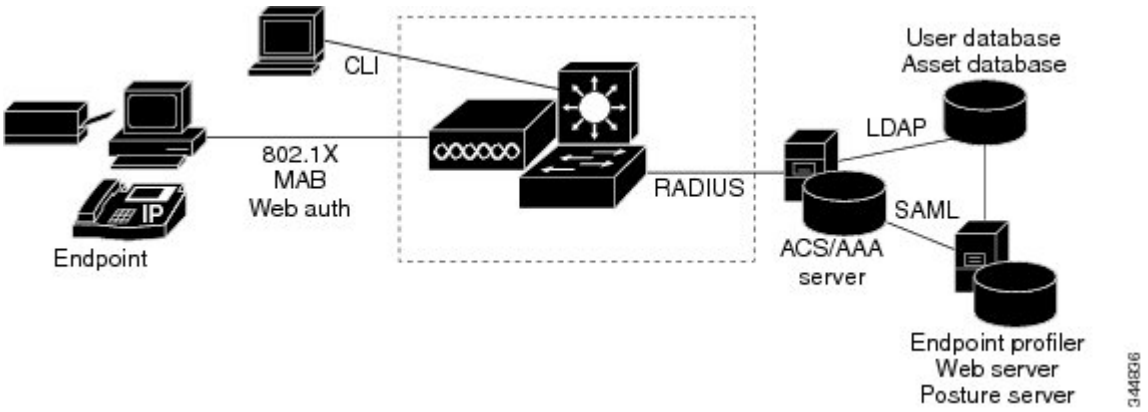
Identity-Based Networking Services の理解

Identity-Based Networking Services は、アクセス管理、および加入者管理に対するアイデンティティ ベースのアプローチを実現します。 また、複数のテクノロジーの機能に対して一貫した設定を行

う手段である、コマンド インターフェイスが用意されています。これにより、機能の容易な導入とカスタマイズが可能になります。さらに、ネットワークにおけるポリシーの施行のために、ローカルで定義したポリシーや外部サーバから受信したポリシーを適用できる、堅牢なポリシー制御エンジンも用意されています。

この図は、物理的に分散されたエンタープライズ（キャンパス、ブランチ オフィス、およびリモート ワーカーが存在する）における、Identity-Based Networking Services の一般的な導入例を示します。

図 *1*：導入例



Identity-Based Networking Services の機能

Identity-Based Networking Services には、次の機能が含まれます。

- Cisco Common Classification Policy Language（C3PL）ベースのアイデンティティの設定
- IEEE 802.1x（dot1x）、MAC 認証バイパス（MAB）、および Web 認証を含む、単一セッションでの並列認証方式。
- ダウンロード可能なアイデンティティ サービス テンプレート
- セッションのクエリー、再認証、および終了、ポートのシャットダウンとポートバウンス、およびアイデンティティ サービス テンプレートのアクティブ化と非アクティブ化に対する拡張 RADIUS Change-of-Authorization（CoA）のサポート。
- Lightweight Directory Access Protocol（LDAP）を使用したローカル認証
- ローカルで定義されたアイデンティティ制御ポリシー
- ローカルで定義されたアイデンティティ サービス テンプレート
- 複数の方式に対するユーザごとの非アクティブ化処理
- コモン セッション ID の Web 認証のサポート
- IPv6 の Web 認証のサポート

Identity-Based Networking Services のメリット

アイデンティティベースのソリューションは、低い運用コストを維持しながら、従業員、請負業者、パートナーなど、別個のグループに対するアクセス制御を行うために必要不可欠です。Identity-Based Networking Services は、ポリシーおよびアイデンティティベースのインフラストラクチャにより運用管理に対する一貫したアプローチを実現して、新機能の迅速な導入を推進し、スイッチの管理を簡単にします。

Identity-Based Networking Services には、次のメリットがあります。

- セッション管理に対するアイデンティティ ベースのフレームワーク。
- ローカルで定義したポリシーまたは外部 AAA サーバから受信したポリシーを適用する、堅牢なポリシー制御エンジン。
- 複数のアクセス テクノロジーの機能の迅速な導入およびカスタマイズ。
- 複数のアクセス方式、プラットフォーム、およびアプリケーション ドメインの機能を設定するための、簡単で一貫した方法。

コモン セッション ID に対する Web 認証のサポート

Identity-Based Networking Services により、クライアントのすべての 802.1X および MAB で認証されたセッションに加え、Web 認証セッションで単一のセッション ID を使用できるようになります。 このセッション ID は、表示コマンド、MIB、および RADIUS メッセージなどあらゆるレポート目的で使用され、ユーザが、あるセッションのメッセージと別のセッションのメッセージとを区別できるようにします。 このコモン セッション ID は、セッションに適用されるすべての認証方式と機能で一貫して使用されます。

IPv6 の Web 認証のサポート

Identity-Based Networking Services により、Web 認証に対する IPv6 サポートが導入されます。 IPv6 が Web 認証でサポートされるのは、Identity-Based Networking Services が明示的に設定されている場合のみです。 これは、**policy-map type control subscriber** コマンドなどの Identity-Based Networking Services のコマンドを明示的に設定することにより、設定を Cisco Common Classification Policy Language（C3PL）表示モードに永続的に変換する必要があることを意味します。

その他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
Identity-Based Networking Services コマンド	『Cisco IOS Identity-Based Networking Services Command Reference』
アドレス解決プロトコル（ARP）コマンド	『Cisco IOS IP Addressing Services Command Reference』
ARP 設定作業	『*IP Addressing - ARP Configuration Guide*』
認証、許可、およびアカウンティング（AAA）の設定作業	『*Authentication Authorization and Accounting Configuration Guide*』
AAA コマンド	『*Cisco IOS Security Command Reference*』

標準および RFC

標準/RFC	Title
RFC 5176	『*Dynamic Authorization Extensions to RADIUS*』

テクニカル サポート

説明	Link
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

Identity-Based Networking Services の機能情報の概要

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。 その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *1*：*Identity-Based Networking Services* の機能情報の概要

機能名	リリース	機能情報
コモン セッション ID の Web 認証のサポート	Cisco IOS XE Release 3.2SE	802.1X および MAB で認証されたセッションに加え、すべての Web 認証セッションで単一のセッション ID を使用できるようになります。

第 2 章

アイデンティティ制御ポリシーの設定

アイデンティティ制御ポリシーは、Identity-Based Networking Services が、特定の条件およびサブスクライバのイベントに対応して実行するアクションを定義します。 一貫したポリシー言語を使用して、各種のシステムアクション、条件、およびイベントを組み合わせることができます。このモジュールでは、Identity-Based Networking Services のアイデンティティ制御ポリシーの設定方法に関する情報を提供します。

- 機能情報の確認，7 ページ
- アイデンティティ制御ポリシーに関する情報，8 ページ
- アイデンティティ制御ポリシーの設定方法，11 ページ
- アイデンティティ制御ポリシーの設定例，29 ページ
- その他の関連資料，33 ページ
- アイデンティティ制御ポリシーの機能情報，34 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を確認し、各機能がサポートされているリリースのリストを確認するには、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

アイデンティティ制御ポリシーに関する情報

並列認証方式

Identity-Based Networking Services では、IEEE 802.1x（dot1x）、MAC 認証バイパス（MAB）、および Web 認証方式を同時に実行することができます。これにより、1 つの加入者セッションに対して複数の認証方式を同時に呼び出すことができるようになります。 これにより、クライアントでサポートされている方式を、シリアル化に伴う遅延なしに極力早く完了できます。

通常、ホストの承認に使用されるアクセス制御方法は、エンドポイントまで残されます。 たとえば、802.1x サプリカントのないネットワーク プリンタは MAB のみで承認され、従業員のデスクトップは 802.1x のみで、そしてゲストは Web 認証のみで承認されます。 デフォルトの優先順序は 802.1x の次に MAB、そして Web 認証です。 複数の方式の優先度が同じ場合は、最初にセッションを正常に認証した方式が優先されます。

セッションのライフタイム中に複数の方式が成功する可能性がある例として、802.1x の成功の保留中に、MAB が暫定アクセスの提供に使用される場合があります。 ホストも、クレデンシャルを更新できるように Web サーバへの暫定アクセスを許可されている場合があります。そのため、認証が失敗した後に 802.1x が成功する場合があります。

表示モードの設定

Identity-Based Networking Services により、以前サポートされていた認証コマンドおよびポリシーコマンドの多くに代わる新しい Cisco IOS コマンドが導入されています。 これらのコマンドは、Identity-Based Networking Services をサポートする Cisco Common Classification Policy Language（C3PL）表示モードをイネーブルにした後でのみ使用できます。 並列認証および IPv6 を使用した Web 認証などの Identity-Based Networking Services 機能は、レガシー モードではサポートされません。

次のいずれかを行わないかぎり、デバイスはデフォルトでレガシー設定モードを使用します。

- **authentication display new-style** コマンドを入力する。このコマンドは C3PL 表示モードへと切り替えを行い、レガシー設定を一時的に Identity-Based Networking Services の設定へと変換して、永続的な変換を行う前にこの設定を確認できるようにします。 **authentication display legacy** コマンドを使用して、レガシー モードに切り替えることができます。 「Identity-Based Networking Services の表示モードのイネーブル化, （11 ページ）」のセクションを参照してください。
- Identity-Based Networking Services 設定コマンドを入力する。最初に明示的な Identity-Based Networking Services コマンドが入力されると、設定は C3PL 表示モードへと永続的に変更され、レガシー コマンドが抑制されます。 **authentication display** コマンドはディセーブルになり、レガシーの設定モードに戻すことはできません。

Identity-Based Networking Services の制御ポリシー

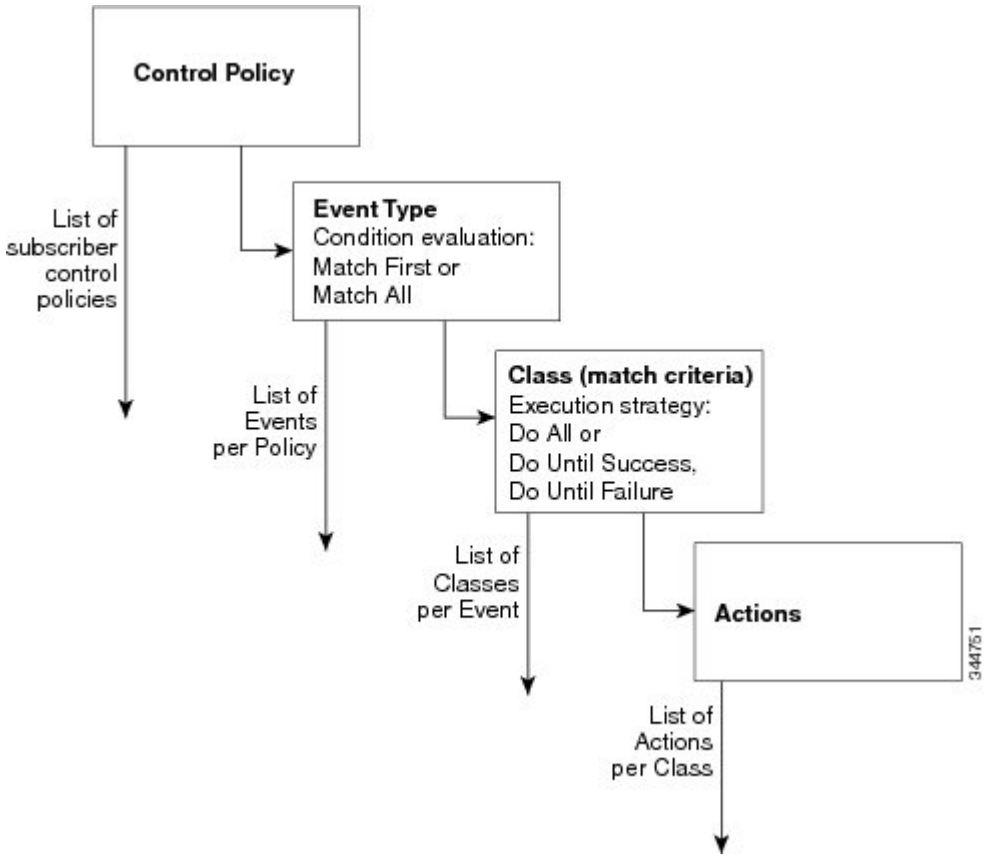
制御ポリシーは、各種の加入者ライフサイクルイベントの処理を定義します。セッションの開始やセッション障害などの各種イベントに対して、制御ポリシーでアクションを指定できます。 これらのアクションは、さまざまな一致基準に基づき、異なる加入者に対して条件付きで実行できます。 制御ポリシーは、インターフェイス上でアクティブ化され、一般に、加入者 ID の認証、およびセッションにおけるサービスのアクティベーションを制御します。 たとえば、特定の加入者を認証し、それらの加入者に特定のサービスへのアクセス権を付与するように制御ポリシーを設定できます。

制御ポリシーは、1 つ以上の制御ポリシー ルールと、そのポリシー ルールの評価方法を制御する決定戦略から構成されます。制御ポリシールールは、制御クラス（柔軟な条件句）、条件が評価されるイベント、および、1つ以上のアクションで構成されます。アクションとは「認証」や「アクティブ化」などの一般的なシステム機能です。イベントがトリガーする特定のアクションを定義します。また、一部のイベントにはデフォルトのアクションがあります。

次の図は、各制御ポリシーに、加入者のライフ サイクルに適用可能と見なされるイベントのリストがどのように含まれているのかを説明しています。 各イベント タイプ内には、加入者 ID に対

する各種の一致基準が設定された制御クラスがあり、各クラスには、実行されるアクションのリストがあります。

図 *2*：制御ポリシーの構造



制御ポリシーの設定の概要

制御ポリシーは、イベント、条件、およびアクションに関するシステム機能を表します。 制御ポリシーの定義には次の 3 つの手順があります。

1. 1 つ以上の制御クラスを作成する。制御クラスは、制御ポリシーがアクティブ化されるために満たす必要のある基準を指定します。 制御クラスには複数の条件を含めることができ、各条件は true または false の評価を行います。 Match ディレクティブは、クラスが true と評価されるためには、各条件のすべてが true と評価されるか、いずれかが true と評価されるか、あるいはいずれも true と評価されてはならないかを指定します。 または、いずれの条件も含まず、常に true と評価するデフォルトの制御クラスを指定することもできます。
2. 制御ポリシーを作成する。制御ポリシーには 1 つ以上の制御ポリシー ルールが含まれます。制御ポリシー ルールは制御クラス、クラスが評価される原因となる 1 つのイベント、および 1 つ以上のアクションから構成されます。 アクションに番号が付けられ、順に実行されます。

3 制御ポリシーを適用する。制御ポリシーは、インターフェイスに適用することによってアクティブ化されます。

Identity-Based Networking Services 用のパラメータ マップ

パラメータ マップを使用して、制御ポリシー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指定することができます。 Identity-Based Networking Services の場合、認証パラメータ マップは、**authenticate using webauth** コマンドを使用して指定されたアクションに使用するパラメータを定義します。 次のパラメータ マップのタイプを設定できます。

- 認証バイパス（これは、非応答ホスト（NRH）認証とも呼ばれます）
- 合意
- Web 認証
- Web 認証（合意あり）

パラメータ マップはオプションです。 名前付きパラメータ マップを設定しない場合は、グローバル パラメータ マップで指定されたデフォルトのパラメータが使用されます。

複数の方式に対するユーザごとの非アクティブ化処理

共通の非アクティブ化エージング機能は、Web 認証セッションに対する RADIUS 属性 28（Idle-Timeout）および 29（Termination-Action）のサポートを拡張し、802.1X、MAC 認証バイパス（MAB）、Web認証などのすべての認証方式で、一貫した非アクティブ化処理を実現します。 AAA サーバは、ユーザ認証の一環としてこれらの属性を送信します。 セッションが、属性 28 で指定された期間アイドルのままの場合、または属性29で設定されているタイムアウトの時間に到達した場合、そのセッションは終了します。

ローカルで定義したサービステンプレートを使用して、非アクティブタイムアウトと絶対タイムアウトをセッションに適用することもできます。非アクティブタイムアウトをイネーブルにする場合は、セッションが終了する前に送信されるアドレス解決プロトコル（ARP）プローブもイネーブルにできます。 設定の詳細については、「アイデンティティ サービス テンプレートの設定, （37 ページ）」モジュールを参照してください。

アイデンティティ制御ポリシーの設定方法

Identity-Based Networking Services の表示モードのイネーブル化

Identity-Based Networking Services 機能は、Cisco Common Classification Policy Language（C3PL）表示モードで設定されています。 レガシーの認証マネージャ モードはデフォルトでイネーブルです。 C3PL 表示モードに切り替えて、レガシーのコンフィギュレーション コマンドをすべて一時的に C3PL の同等のコマンドに変換するには、次の手順に従います。 これにより、永続的な変換

を行う前に、レガシーの設定を Identity-Based Networking Services 設定としてプレビューすることができます。 Identity-Based Networking Services コマンドを明示的に入力すると、変換は永続的になり、レガシー モードに戻ることはできません。

手順の概要

1. **enable**
2. **authentication display** {**legacy** | **new-style**}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**authentication display** {**legacy**	**new-style**} 例： `Device# authentication display new-style`	認証およびポリシー設定の表示モードを設定します。 • デフォルトの表示モードはレガシーです。 • 最初に Identity-Based Networking Services コマンドを明示的に実行するまでは、このコマンドを使用して、レガシーと C3PL の間で表示モードを切り替えることができます。 最初に Identity-Based Networking Services コマンドを明示的に入力すると（たとえば、制御クラスや制御ポリシーの設定時）、このコマンドはディセーブルになり、レガシー モードに戻すことはできないため、続行するかどうかを確認するプロンプトが表示されます。 （注） new-style モードがイネーブルにして設定を保存し、リロードを実行すると、表示モードは永続的に new-style に設定されます。 **authentication display** コマンドはディセーブルになり、レガシー モードに戻すことはできません。 new-style モードでスタンバイ デバイスを起動すると、そのスタンバイ デバイスは new-style モードになり、スイッチオーバーの後も、デバイスは new-style モードのままになります。 レガシー モードにスイッチバックするには、**authentication display legacy** コマンドを使用して、スダンバイ スイッチをリロードする必要があります。

制御クラスの設定

制御クラスは、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。 制御ポリシーのアクションを実行するためには、条件のすべてまたはいずれかが true と評価されるか、あるいはいず

れも true と評価されてはならないかを定義します。 制御クラスは、制御ポリシーで指定されたイベントに基づいて評価されます。

（注） この手順では、制御クラスで設定できる一致条件をすべて示します。 制御クラスを有効にするためには、制御クラスで少なくとも 1 つの条件を有効にする必要があります。 他のすべての条件および対応するステップはオプションです（下記のステップ 4～18）。

手順の概要

1. **enable**
2. **configure terminal**
3. **class-map type control subscriber** {**match-all** | **match-any** | **match-none**} *control-class-name*
4. {**match** | **no-match**} **activated-service-template** *template-name*
5. {**match** | **no-match**} **authorization-status** {**authorized** | **unauthorized**}
6. {**match** | **no-match**} **authorizing-method-priority** {**eq** | **gt** | **lt**} *priority-value*
7. {**match** | **no-match**} **client-type** {**data** | **switch** | **video** | **voice**}
8. {**match** | **no-match**} **current-method-priority** {**eq** | **gt** | **lt**} *priority-value*
9. {**match** | **no-match**} **ip-address** *ip-address*
10. {**match** | **no-match**} **ipv6-address** *ipv6-address*
11. {**match** | **no-match**} **mac-address** *mac-address*
12. {**match** | **no-match**} **method** {**dot1x** | **mab** | **webauth**}
13. {**match** | **no-match**} **port-type** {**l2-port** | **l3-port** | **dot11-port**}
14. {**match** | **no-match**} **result-type** [**method** {**dot1x** | **mab** | **webauth**}] *result-type*
15. {**match** | **no-match**} **service-template** *template-name*
16. {**match** | **no-match**} **tag** *tag-name*
17. {**match** | **no-match**} **timer** *timer-name*
18. {**match** | **no-match**} **username** *username*
19. **end**
20. **show class-map type control subscriber** {**all** | **name** *control-class-name*}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**class-map type control subscriber** {**match-all** | **match-any** | **match-none**} *control-class-name* 例： `Device(config)# class-map type control subscriber match-all DOT1X_NO_AGENT`	制御クラスを作成し、制御クラスマップ フィルタ モードを開始します。 • **m□tch-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ります。 • **match-any**：制御クラスの条件の少なくとも 1 つが true と評価される必要があります。 • **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ります。
ステップ 4	{**match** | **no-match**} **activated-service-template** *template-name* 例： `Device(config-filter-control-classmap)# match activated-service-template SVC_1`	（任意）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。
ステップ 5	{**match** | **no-match**} **authorization-status** {**authorized** | **unauthorized**} 例： `Device(config-filter-control-classmap)# match authorization-status authorized`	（任意）セッションの認可ステータスに基づいて true と評価される条件を作成します。
ステップ 6	{**match** | **no-match**} **authorizing-method-priority** {**eq** | **gt** | **lt**} *priority-value* 例： `Device(config-filter-control-classmap)# match authorizing-method-priority eq 10`	（任意）認可方式の優先度に基づいて true と評価される条件を作成します。 • **eq**：現在の優先度は *priority-value* 同じです。 • **gt**：現在の優先度は *priority-value* より大きくなります。 • **lt**：現在の優先度は *priority-value* より小さくなります。 • *priority-value*：照合される優先値。 範囲：1 ～ 254。1 の優先度が最も高く、 254 は最も低くなります。

	コマンドまたはアクション	目的
ステップ 7	{**match** | **no-match**} **client-type** {**data** | **switch** | **video** | **voice**} 例： `Device(config-filter-control-classmap)# match client-type data`	（任意）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します。
ステップ 8	{**match** | **no-match**} **current-method-priority** {**eq** | **gt** | **lt**} *priority-value* 例： `Device(config-filter-control-classmap)# match current-method-priority eq 10`	（任意）現在の認証方式の優先度に基づいて true と評価される条件を作成します。
ステップ 9	{**match** | **no-match**} **ip-address** *ip-address* 例： `Device(config-filter-control-classmap)# match ip-address 10.10.10.1`	（任意）イベント ソースの 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。
ステップ 10	{**match** | **no-match**} **ipv6-address** *ipv6-address* 例： `Device(config-filter-control-classmap)# match ipv6-address FE80::1`	（任意）イベント ソースの 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。
ステップ 11	{**match** | **no-match**} **mac-address** *mac-address* 例： `Device(config-filter-control-classmap)# match mac-address aabb.cc00.6500`	（任意）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します。
ステップ 12	{**match** | **no-match**} **method** {**dot1x** | **mab** | **webauth**} 例： `Device(config-filter-control-classmap)# match method dot1x`	（任意）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します。
ステップ 13	{**match** | **no-match**} **port-type** {**l2-port** | **l3-port** | **dot11-port**} 例： `Device(config-filter-control-classmap)# match port-type l2-port`	（任意）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します。

	コマンドまたはアクション	目的
ステップ 14	{**match** | **no-match**} **result-type** [**method** {**dot1x** | **mab** | **webauth**}] *result-type* 例： `Device(config-filter-control-classmap)# match result-type agent-not-found`	（任意）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します。 • 使用可能な結果タイプを表示するには、疑問符（**?**）のオンライン ヘルプ機能を使用します。
ステップ 15	{**match** | **no-match**} **service-template** *template-name* 例： `Device(config-filter-control-classmap)# match service-template svc_1`	（任意）イベントのサービス 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。
ステップ 16	{**match** | **no-match**} **tag** *tag-name* 例： `Device(config-filter-control-classmap)# match tag tag_1`	（任意）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します。
ステップ 17	{**match** | **no-match**} **timer** *timer-name* 例： `Device(config-filter-control-classmap)# match timer restart`	（任意）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。
ステップ 18	{**match** | **no-match**} **username** *username* 例： `Device(config-filter-control-classmap)# match username josmiths`	（任意）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します。
ステップ 19	**end** 例： `Device(config-filter-control-classmap)# end`	（任意）制御クラスマップ フィルタのコンフィギュレーション モードを終了し、特権 EXEC モードへ戻ります。
ステップ 20	**show class-map type control subscriber** {**all** | **name** *control-class-name*} 例： `Device# show class-map type control subscriber all`	（任意）Identity-Based Networking Services の制御クラスに関する情報を表示します。

例：制御クラス

次の例は、2 つの一致条件が設定された制御クラスを示しています。

```
class-map type control subscriber match-all DOT1X_NO_AGENT
 match method dot1x
 match result-type agent-not-found
```

制御ポリシーの設定

制御ポリシーは、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を決定します。 制御ポリシーには、制御クラスを 1 つ以上のアクションに関連付ける 1 つ以上の制御ポリシー ルールが含まれます。 ポリシールールで設定できるアクションは、指定するイベントのタイプに応じて異なります。

（注） この作業には、イベントにかかわらず、制御ポリシーで設定できるすべてのアクションが含まれます。 これらのすべてのアクションおよび対応するステップはオプションです（下記のステップ6～21）。特定のイベントに対してサポートされるアクションを表示するには、疑問符（**?**）のオンライン ヘルプ機能を使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map type control subscriber** *control-policy-name*
4. **event** *event-name* [**match-all** | **match-first**]
5. *priority-number* **class** {*control-class-name* | **always**} [**do-all** | **do-until-failure** | **do-until-success**]
6. *action-number* **activate** {**policy type control subscriber** *control-policy-name* [**child** [**no-propagation** | **concurrent**] | **service-template** *template-name* [**aaa-list** *list-name*] [**precedence** *number*] [**replace-all**]}
7. *action-number* **authenticate using** {**dot1x** | **mab** | **webauth**} [**aaa** {**authc-list** *authc-list-name* | **authz-list** *authz-list-name*]} [**merge**] [**parameter-map** *map-name*] [**priority** *priority-number*] [**replace** | **replace-all**] [**retries** *number* {**retry-time** *seconds*}]
8. *action-number* **authentication-restart** *seconds*
9. *action-number* **authorize**
10. *action-number* **clear-authenticated-data-hosts-on-port**
11. *action-number* **clear-session**
12. *action-number* **deactivate** {**policy type control subscriber** *control-policy-name* | **service-template** *template-name*}
13. *action-number* **err-disable**
14. *action-number* **pause reauthentication**
15. *action-number* **protect**
16. *action-number* **replace**
17. *action-number* **restrict**
18. *action-number* **resume reauthentication**
19. *action-number* **set-timer** *timer-name seconds*
20. *action-number* **terminate** {**dot1x** | **mab** | **webauth**}
21. *action-number* **unauthorize**
22. **end**
23. **show policy-map type control subscriber** {**all** | **name** *control-policy-name*}

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**policy-map type control subscriber** *control-policy-name* 例： `Device(config)# policy-map type control POLICY_1`	加入者セッションに対する制御ポリシーを定義します。
ステップ 4	**event** *event-name* [**match-all** | **match-first**] 例： `Device(config-event-control-policymap)# event session-started`	条件が満たされた場合に制御ポリシーの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-all** がデフォルトの動作です。 • 使用可能なイベントタイプを表示するには、（**?**）のオンライン ヘルプ機能を使用します。 イベント タイプの完全な説明については、**event** コマンドについて参照してください。
ステップ 5	*priority-number* **class** {*control-class-name* | **always**} [**do-all** | **do-until-failure** | **do-until-success**] 例： `Device(config-class-control-policymap)# 10 class always`	制御ポリシーを制御クラスの 1 つ以上のアクションに関連付けます。 • 名前付き制御クラスを最初に設定してから、このクラスを *control-class-name* 引数を使用して指定する必要があります。 • **do-until-failure** がデフォルトの動作です。
ステップ 6	*action-number* **activate** {**policy type control subscriber** *control-policy-name* [**child** [**no-propagation** | **concurrent**] | **service-template** *template-name* [**aaa-list** *list-name*] [**precedence** *number*] [**replace-all**]} 例： `Device(config-action-control-policymap)# 10 activate service-template FALLBACK`	（任意）加入者セッションの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。
ステップ 7	*action-number* **authenticate using** {**dot1x** | **mab** | **webauth**} [**aaa** {**authc-list** *authc-list-name* | **authz-list** *authz-list-name*]} [**merge**] [**parameter-map** *map-name*] [**priority** *priority-number*] [**replace** | **replace-all**] [**retries** *number* {**retry-time** *seconds*}] 例： `Device(config-action-control-policymap)# 10 authenticate using dot1x priority 10`	（任意）指定されたメソッドを使用して加入者セッションの認証を開始します。

	コマンドまたはアクション	目的
ステップ 8	*action-number* **authentication-restart** *seconds* 例： `Device(config-action-control-policymap)# 20 authentication-restart 60`	（任意）認証または認可の失敗後、認証プロセスを再起動するようにタイマーを設定します。
ステップ 9	*action-number* **authorize** 例： `Device(config-action-control-policymap)# 10 authorize`	（任意）加入者セッションの認可を開始します。
ステップ 10	*action-number* **clear-authenticated-data-hosts-on-port** 例： `Device(config-action-control-policymap)# 20 clear-authenticated-data-hosts-on-port`	（任意）認証失敗後にポートの認証済みデータ ホストをクリアします。
ステップ 11	*action-number* **clear-session** 例： `Device(config-action-control-policymap)# 30 clear-session`	（任意）アクティブな加入者セッションをクリアします。
ステップ 12	*action-number* **deactivate** {**policy type control subscriber** *control-policy-name* | **service-template** *template-name*} 例： `Device(config-action-control-policymap)# 20 deactivate service-template`	（任意）加入者セッションの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。
ステップ 13	*action-number* **err-disable** 例： `Device(config-action-control-policymap)# 10 err-disable`	（任意）セッション違反イベント後に一時的にポートをディセーブルにします。
ステップ 14	*action-number* **pause reauthentication** 例： `Device(config-action-control-policymap)# 20 pause reauthentication`	（任意）認証の失敗後に再認証を一時停止します。
ステップ 15	*action-number* **protect** 例： `Device(config-action-control-policymap)# 10 protect`	（任意）セッション違反イベント後に違反パケットを暗黙的にドロップします。

	コマンドまたはアクション	目的
ステップ 16	*action-number* **replace** 例： `Device(config-action-control-policymap)# 10 replace`	（任意）違反イベント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。
ステップ 17	*action-number* **restrict** 例： `Device(config-action-control-policymap)# 10 restrict`	（任意）セッションの違反イベント後に違反パケットをドロップし、syslog エントリを生成します。
ステップ 18	*action-number* **resume reauthentication** 例： `Device(config-action-control-policymap)# 20 resume reauthentication`	（任意）認証失敗後に再認証プロセスを再開します。
ステップ 19	*action-number* **set-timer** *timer-name seconds* 例： `Device(config-action-control-policymap)# 20 set-timer RESTART 60`	（任意）名前付きのポリシータイマーを開始します。
ステップ 20	*action-number* **terminate** {**dot1x** | **mab** | **webauth**} 例： `Device(config-action-control-policymap)# 20 terminate webauth`	（任意）加入者セッションの認証方式を終了します。
ステップ 21	*action-number* **unauthorize** 例： `Device(config-action-control-policymap)# 20 unauthorize`	（任意）加入者セッションからすべての認可データを削除します。
ステップ 22	**end** 例： `Device(config-action-control-policymap)# end`	（任意）制御ポリシーマップ アクションのコンフィギュレーション モードを終了し、選択特権 EXEC モードへ戻ります。
ステップ 23	**show policy-map type control subscriber** {**all** | **name** *control-policy-name*} 例： `Device# show policy-map type control subscriber name POLICY_1`	（任意）アイデンティティ制御ポリシーに関する情報を表示します。

例：制御ポリシー

次の例は、認証を開始するために必要な最小限の設定を使用した、簡単な制御ポリシーを示します。

```
policy-map type control subscriber POLICY_1
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x
```

並列認証および連続認証に対する制御ポリシーの詳細な例については、「アイデンティティ制御ポリシーの設定例, （29 ページ）」のセクションを参照してください。

インターフェイスへの制御ポリシーの適用

制御ポリシーは、一般に、加入者 ID の認証およびセッションでのサービスのアクティブ化を制御します。 インターフェイスに制御ポリシーを適用するには、この作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **service-policy type control subscriber** *control-policy-name*
5. **subscriber aging** {**inactivity-timer** *seconds* [**probe**] | **probe**}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Device(config)# interface tengigabitethernet 1/0/1`	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**service-policy type control subscriber** *control-policy-name*	以前に設定した制御ポリシーを適用します。

	コマンドまたはアクション	目的
	例： `Device(config-if)# service-policy type control subscriber POLICY_1`	• 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（**?**）のオンライン ヘルプ機能を使用します。
ステップ 5	**subscriber aging** {**inactivity-timer** *seconds* [**probe**] | **probe**} 例： `Device(config-if)# subscriber aging inactivity-timer 60 probe`	加入者セッションに対する非アクティブ タイマーをイネーブルにします。

例：インターフェイスへの制御ポリシーの適用

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

ポートでの認証機能の設定

ポートの許可状態、ホストのアクセス モード、事前認証アクセス、および認証の方向など、ポートへのアクセスを制御するには、この作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **access-session port-control** {**auto** | **force-authorized** | **force-unauthorized**}
5. **access-session host-mode** {**multi-auth** | **multi-domain** | **multi-host** | **single-host**}
6. **access-session closed**
7. **access-session control-direction** {**both** | **in**}
8. **end**
9. **show access-session interface** *interface-type interface-number* [**details**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Device(config)# interface gigabitethernet 1/0/2`	選択したインターフェイスのインターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**access-session port-control** {**auto** | **force-authorized** | **force-unauthorized**} 例： `Device(config-if)# access-session port-control auto`	ポートの認可状態を設定します。 • デフォルト値は **force-authorized** です。
ステップ 5	**access-session host-mode** {**multi-auth** | **multi-domain** | **multi-host** | **single-host**} 例： `Device(config-if)# access-session host-mode single-host`	ホストの制御ポートへのアクセスを許可します。 • このコマンドを使用するには、最初に **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。 • デフォルト値は **multi-auth** です。
ステップ 6	**access-session closed** 例： `Device(config-if)# access-session closed`	このポートへの事前認証アクセスを防止します。 • ポートはデフォルトでにオープン アクセスに設定されています。
ステップ 7	**access-session control-direction** {**both** | **in**} 例： `Device(config-if)# access-session control-direction in`	ポートでの認証制御の方向を設定します。 • デフォルト値は **both** です。
ステップ 8	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 9	**show access-session interface** *interface-type interface-number* [**details**] 例： `Device# show access-session interface gigabitethernet 1/0/2 details`	指定されたクライアントインターフェイスに一致する加入者セッションに関する情報を表示します。

例:ポート認証

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

Web ベース認証のパラメータ マップの設定

パラメータ マップを使用して、制御ポリシーで設定されたアクションの動作を制御するパラメータを変更することができます。 Webベース認証のパラメータマップは、認証中に加入者セッションに適用できるパラメータを設定します。 パラメータマップを作成しない場合、ポリシーではデフォルトのパラメータが使用されます。

Web ベース認証に対してグローバルまたは名前付きパラメータ マップのいずれかを定義するには、次の手順に従います。

（注） グローバル パラメータ マップで使用できる設定コマンドは、名前付きパラメータ マップで使用できるコマンドとは異なります。

手順の概要

1. **enable**
2. **configure terminal**
3. **parameter-map type webauth** {*parameter-map-name* | **global**}
4. **banner** {**file** *location*:*filename* | **text** *banner-text*}
5. **consent email**
6. **custom-page** {**failure** | **login [expired]** | **success**} **device** *location*:*filename*
7. **max-http-conns** *number*
8. **ratelimit init-state-sessions** *rate-limit*
9. **redirect** {{**for-login** | **on-failure** | **on-success**} *url* | **portal** {**ipv4** *ipv4-address* | **ipv6** *ipv6-address*}}
10. **timeout init-state min** *minutes*
11. **type** {**authbypass** | **consent** | **webauth** | **webconsent**}
12. **virtual-ip** {**ipv4** *ipv4-address* | **ipv6** *ipv6-address*}
13. **watch-list** {**add-item** {**ipv4** *ipv4-address* | **ipv6** *ipv6-address*} | **dynamic-expiry-timeout** *minutes* | **enabled**}
14. **end**
15. **show ip admission status** [**banners** | **custom-pages** | **parameter-map** [*parameter-map*]]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**parameter-map type webauth** {*parameter-map-name*	**global**} 例： `Device(config)# parameter-map type webauth MAP_2`	パラメータ マップを作成し、parameter-map webauth コンフィギュレーション モードを開始します。 • **global** キーワードを使用して定義されたグローバル パラメータに対してサポートされる特定のコンフィギュレーション コマンドは、*parameter-map-name* 引数を使用して指定された名前付きパラメータ マップでサポートされるコマンドとは異なります。

	コマンドまたはアクション	目的
ステップ 4	**banner** {**file** *location*:*filename* | **text** *banner-text*} 例： `Device(config-params-parameter-map)# banner file flash:webauth_banner.html`	（任意）Web 認証ログイン Web ページにバナーを表示します。
ステップ 5	**consent email** 例： `Device(config-params-parameter-map)# consent email`	（任意）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。 • 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。

ステップ 6	**custom-page** {**failure** | **login [expired]** | **success**} **device** *location*:*filename*
	
	例：
	`Device(config-params-parameter-map)# custom-page login device flash:webauth_login.html`
	`Device(config-params-parameter-map)# custom-page login expired device flash:webauth_expire.html`
	`Device(config-params-parameter-map)# custom-page success device flash:webauth_success.html`
	`Device(config-params-parameter-map)# custom-page failure device flash:webauth_fail.html`
		（任意）Web ベースの認証中に、カスタムの認証プロキシ Web ページを表示します。
		• 4 つのカスタム HTML ファイルをすべて設定する必要があります。 指定されているファイルが 4 つ未満の場合は、内部のデフォルト HTML ページが使用されます。

ステップ 7	**max-http-conns** *number* 例： `Device(config-params-parameter-map)# max-http-conns 5`	（任意）各 Web 認証クライアントの HTTP 接続の数を制限します。
ステップ 8	**ratelimit init-state-sessions** *rate-limit* 例： `Device(config-params-parameter-map)# ratelimit init-state-sessions 500`	（任意）Init 状態の Web ベース認証セッションの数を制限します。 • 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。

ステップ 9	**redirect** {{**for-login** | **on-failure** | **on-success**} *url* | **portal** {**ipv4** *ipv4-address* | **ipv6** *ipv6-address*}}
	
	例：
	`Device(config-params-parameter-map)# redirect portal ipv6 FE80::1`
	`Device(config-params-parameter-map)# redirect on-failure`
	`http://10.10.3.34/~sample/failure.html`
		（任意）Web ベースの認証時に特定の URL にユーザを転送します。

	コマンドまたはアクション	目的
ステップ 10	**timeout init-state min** *minutes* 例： `Device(config-params-parameter-map)# timeout init-state min 15`	（任意）Web ベースの認証セッションに対して Init 状態タイムアウトを設定します。
ステップ 11	**type** {**authbypass** | **consent** | **webauth** | **webconsent**} 例： `Device(config-params-parameter-map)# type consent`	（任意）Web ベースの認証パラメータ マップでサポートされる方式を定義します。 • 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。
ステップ 12	**virtual-ip** {**ipv4** *ipv4-address* | **ipv6** *ipv6-address*} 例： `Device(config-params-parameter-map)# virtual-ip ipv6 FE80::1`	（任意）Web ベース認証クライアントの仮想 IP アドレスを指定します。 • 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。

ステップ 13	**watch-list** {**add-item** {**ipv4** *ipv4-address* | **ipv6** *ipv6-address*} | **dynamic-expiry-timeout** *minutes* | **enabled**}
	
	例：
	`Device(config-params-parameter-map)# watch-list enabled`
	`Device(config-params-parameter-map)# watch-list dynamic-expiry-timeout 20`
	`Device(config-params-parameter-map)# watch-list add-item ipv6 FE80::1`
		（任意）Web ベース認証クライアントのウォッチ リストをイネーブルにします。
		• 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。

ステップ 14	**end** 例： `Device(config-params-parameter-map)# end`	（任意）parameter-map コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 15	**show ip admission status** [**banners** | **custom-pages** | **parameter-map** [*parameter-map*]] 例： `Device# show ip admission status custom-pages`	（任意）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。

例：Web ベース認証のパラメータ マップ

```
parameter-map type webauth PMAP_2
 type webconsent
 timeout init-state min 15
 max-http-conns 5
 consent email
 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
```

次の作業

制御ポリシーの設定時に **authenticate using** コマンドでパラメータ マップを指定することにより、そのパラメータ マップをセッションに適用します。 「制御ポリシーの設定, （17 ページ）」のセクションを参照してください。

アイデンティティ制御ポリシーの設定例

例：並列認証方式の制御ポリシーの設定

次の例は、並行認証を許可するように設定されている制御ポリシーを示しています。 セッションの開始時に、3 種類の方式のすべて（dot1x、MAB、Web 認証）が同時に実行されます。 dot1x 方式の優先度が最高に設定され、Web 認証の優先度が最低に設定されます。つまり、複数のメソッドが成功した場合は、プライオリティの高い方式が優先されます。

認証が失敗すると、セッション マネージャはすべての方式が失敗しているかどうかを確認します。すべてが失敗している場合は、再起動タイマーが 60 秒に設定され、60 秒が経過すると、3 種類すべての方式の再開が試行されます。 認証が正常に行われると、セッションマネージャは優先度が低い方式（dot1x の場合は MAB および Web 認証、MAB の場合は Web 認証）をすべて終了します。 最後に、セッションマネージャが、dot1x クライアント（agent-found）を検出した場合は、dot1x のみがトリガーされます。

ALL-FAILED という名前のクラス マップが、3 つの方式がすべて実行されて完了し（その時点で結果タイプが none）、それらのいずれも成功しなかったことを確認します。 つまり、3 つの方式はすべて完了しましたが、失敗しました。

（注） 並列認証のための制御ポリシーを設定する場合は、優先度の高いメソッドが成功した場合は次のメソッドを明示的に終了するポリシー規則を含める必要があります。

```
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
!
class-map type control subscriber match-all DOT1X
 match method dot1x
!
class-map type control subscriber match-all MAB
 match method mab
!
policy-map type control subscriber CONCURRENT_DOT1X_MAB_WEBAUTH
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using mab priority 20
```

```
   20 authenticate using dot1x priority 10
   30 authenticate using webauth parameter-map WEBAUTH_DEFAULT priority 30
 event authentication-failure match-first
  10 class ALL_FAILED
   10 authentication-restart 60
 event authentication-success match-all
  10 class DOT1X
   10 terminate MAB
   20 terminate webauth
  20 class MAB
   10 terminate webauth
 event agent-found match-all
  10 class always do-until-failure
   10 authenticate using dot1x priority 10
```

例：連続認証方式の制御ポリシーの設定

次の例は、802.1X（dot1x）、MAB、および Web 認証を使用する連続認証方式を許可するように設定されている制御ポリシーを示しています。

```
parameter-map type webauth WEBAUTH_FALLBACK
 type webauth
!
class-map type control subscriber match-all DOT1X_NO_RESP
 match method dot1x
 match result-type method dot1x agent-not-found
!
class-map type control subscriber match-all MAB_FAILED
 match method mab
 match result-type method mab authoritative
!
policy-map type control subscriber POLICY_Gi3/0/10
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x priority 10
 event authentication-failure match-first
  10 class DOT1X_NO_RESP do-until-failure
   10 terminate dot1x
   20 authenticate using mab priority 20
  20 class MAB_FAILED do-until-failure
   10 terminate mab
   20 authenticate using webauth parameter-map WEBAUTH_FALLBACK priority 30
  30 class always do-until-failure
   10 terminate dot1x
   20 terminate mab
   30 terminate webauth
   40 authentication-restart 60
 event agent-found match-all
  10 class always do-until-failure
   10 terminate mab
   20 terminate webauth
   30 authenticate using dot1x priority 10
```

次の例は、802.1X および MAB を使用する連続認証方式を許可するように設定されている制御ポリシーを示しています。 認証が失敗した場合は、VLAN のサービステンプレートがアクティブ化されます。

```
service-template VLAN210
 vlan 210
!
class-map type control subscriber match-all DOT1X_FAILED
 match method dot1x
 match result-type method dot1x authoritative
!
class-map type control subscriber match-all DOT1X_NO_RESP
 match method dot1x
 match result-type method dot1x agent-not-found
!
```

```
class-map type control subscriber match-all MAB_FAILED
 match method mab
 match result-type method mab authoritative
!
policy-map type control subscriber POLICY_Gi3/0/14
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x retries 2 retry-time 0 priority 10
 event authentication-failure match-first
  10 class DOT1X_NO_RESP do-until-failure
   10 terminate dot1x
   20 authenticate using mab priority 20
  20 class MAB_FAILED do-until-failure
   10 terminate mab
   20 activate service-template VLAN210
   30 authorize
  30 class DOT1X_FAILED do-until-failure
   10 terminate dot1x
   20 authenticate using mab priority 20
  40 class always do-until-failure
   10 terminate dot1x
   20 terminate mab
   30 authentication-restart 60
 event agent-found match-all
  10 class always do-until-failure
   10 terminate mab
   20 authenticate using dot1x retries 2 retry-time 0 priority 10
```

例：パラメータ マップの設定

グローバル パラメータ マップ

次の例は、グローバル パラメータ マップの設定を示しています。

```
parameter-map type webauth global
 timeout init-state min 15
 logging enabled
 watch-list enabled
 virtual-ip ipv6 FE80::1
 redirect on-failure http://10.10.3.34/~sample/failure.html
 ratelimit init-state-sessions 500
 max-http-conns 100
 watch-list dynamic-expiry-timeout 5000
 banner file flash:webauth_banner.html
```

Web 認証および認証バイパス（非応答ホスト（NRH））の名前付きパラメータ マップ

次の例は、2 つの名前付きパラメータ マップ（Web 認証用と認証バイパス用）の設定を示しています。 この例には、対応する制御ポリシーの設定も表示されています。

```
parameter-map type webauth WEBAUTH_BANNER
 type webauth
 banner
!
parameter-map type webauth WEBAUTH_NRH
 type authbypass
!
class-map type control subscriber match-all NRH_FAIL
 match method webauth
 match current-method-priority eq 254
!
policy-map type control subscriber WEBAUTH_NRH
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using webauth parameter-map WEBAUTH_NRH priority 254
 event authentication-failure match-all
```

```
  10 class NRH_FAIL do-until-failure
   10 terminate webauth
   20 authenticate using webauth parameter-map WEBAUTH_BANNER priority 30
```

カスタム ページを使用する Web 認証用の名前付きパラメータ マップ

次の例は、ログイン プロセス用のカスタム ページを定義する Web 認証用の名前付きパラメータ マップの設定を、そのパラメータ マップを使用する制御ポリシーとともに示しています。

```
parameter-map type webauth CUSTOM_WEBAUTH
 type webauth
 custom-page login device flash:login_page.htm
 custom-page success device flash:success_page.htm
 custom-page failure device flash:fail_page.htm
 custom-page login expired device flash:expire_page.htm
!
policy-map type control subscriber CUSTOM_WEBAUTH
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using webauth parameter-map CUSTOM_WEB retries 2 retry-time 0
```

同意のための名前付きパラメータ マップ

次にの例は、同意のための名前付きパラメータ マップの設定を、そのパラメータ マップを使用する対応する制御ポリシーとともに示しています。

```
parameter-map type webauth CONSENT
 type consent
!
ip access-list extended GUEST_ACL
 permit ip any 172.30.30.0 0.0.0.255
 permit ip any host 172.20.249.252
!
service-template GUEST_POLICY
 access-group GUEST_ACL
!
policy-map type control subscriber CONSENT
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using webauth parameter-map CONSENT
 event authentication-success match-all
  10 class always do-until-failure
   10 activate service-template GUEST_POLICY
```

同意を伴なう Web 認証用の名前付きパラメータ マップ

次の例は、同意を伴う Web 認証用の名前付きパラメータ マップの設定を、そのパラメータ マップを使用する対応する制御ポリシーとともに示しています。

```
parameter-map type webauth WEBAUTH_CONSENT
 type webconsent
!
ip access-list extended GUEST_ACL
 permit ip any 172.30.30.0 0.0.0.255
 permit ip any host 172.20.249.252
!
service-template GUEST_POLICY
 access-group GUEST_ACL
!
policy-map type control subscriber WEBAUTH_CONSENT
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using webauth parameter-map CONSENT
 event authentication-success match-all
  10 class always do-until-failure
   10 activate service-template GUEST_POLICY
```

その他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
Identity-Based Networking Services コマンド	『Cisco IOS Identity-Based Networking Services Command Reference』
アドレス解決プロトコル（ARP）コマンド	『Cisco IOS IP Addressing Services Command Reference』
ARP 設定作業	『*IP Addressing - ARP Configuration Guide*』
認証、許可、およびアカウンティング（AAA）の設定作業	『*Authentication Authorization and Accounting Configuration Guide*』
AAA コマンド	『*Cisco IOS Security Command Reference*』

標準および RFC

標準/RFC	Title
RFC 5176	『*Dynamic Authorization Extensions to RADIUS*』

テクニカル サポート

説明	Link
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

アイデンティティ制御ポリシーの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。 その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *2*：アイデンティティ制御ポリシーの機能情報

機能名	リリース	機能情報
Cisco Common Classification Policy Language ベースのアイデンティティの設定	Cisco IOS XE Release 3.2SE	アイデンティティ制御ポリシーは、指定されたイベントと条件に対応して実行されるアクションを定義します。 導入されたコマンド：**activate**（policy-map action）、**authenticate using**、**authentication display**、**authentication-restart**、**authorize**、**banner**（parameter-map webauth）、**class**、**class-map type control subscriber**、**clear-authenticated-data-hosts-on-port**、**clear session**、**consent email custom-page**、**deactivate**、**err-disable**、**event**、**logging enabled**（parameter-map webauth）、**match**、**max-http-conns**、**parameter-map type webauth**、**pause reauthentication**、**policy-map type control subscriber**、**protect**（policy-map action）、**ratelimit init-state-sessions**、**redirect**（parameter-map webauth）、**replace**、**restrict**、**resume reauthentication**、**service-policy type control subscriber**、**set-timer**、**show access-session**、**show class-map type control subscriber**、**show policy-map type control subscriber**、**terminate**、**type**（parameter-map webauth）、**unauthorize**、**virtual-ip**、**watch-list**。

機能名	リリース	機能情報
並列認証	Cisco IOS XE Release 3.2SE	802.1x、MAB、および Web 認証方式の並列処理を許可し、1 つのセッションで複数の認証方式を並行して呼び出すことができるようにします。
複数の方式に対するユーザごとの非アクティブ化処理	Cisco IOS XE Release 3.2SE	RADIUS 属性 28（Idle-Timeout）および 29（Termination-Action）をサポートします。

第 3 章

アイデンティティ サービス テンプレートの設定

アイデンティティ サービス テンプレートには、制御ポリシーにより 1 つ以上の加入者セッションに適用できる一連のポリシー属性や機能、RADIUS Change of Authorization（CoA）要求、またはユーザプロファイルやサービスプロファイルが含まれます。 このモジュールでは、Identity-Based Networking Services のローカル サービス テンプレートの設定方法に関する情報を提供します。

- 機能情報の確認，37 ページ
- アイデンティティ サービス テンプレートの前提条件，38 ページ
- アイデンティティ サービス テンプレートに関する情報，38 ページ
- アイデンティティ サービス テンプレートの設定方法，39 ページ
- アイデンティティ サービス テンプレートの設定例，42 ページ
- その他の関連資料，44 ページ
- アイデンティティ サービス テンプレートの機能に関する情報，45 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を確認し、各機能がサポートされているリリースのリストを確認するには、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

アイデンティティ サービス テンプレートの前提条件

ダウンロード可能なサービス テンプレートの場合、スイッチは、認証、許可、およびアカウンティング（AAA）サーバ、Cisco Secure Access Control Server（ACS）、Cisco Identity Services Engine（ISE）からサービステンプレートをダウンロードする際にデフォルト パスワード「cisco123」を使用します。 AAA、ACS および ISE サーバのサービス テンプレート設定には、パスワード「cisco123」が含まれている必要があります。

アイデンティティ サービス テンプレートに関する情報

Identity-Based Networking Services 用のサービス テンプレート

サービス テンプレートには、アクセス コントロール リスト（ACL）や VLAN 割り当てなど、一連のサービス関連の属性や機能が含まれています。これらの属性や機能は、セッション ライフサイクル イベントに対応して、1 つ以上の加入者セッションでアクティブ化することができます。テンプレートにより、ネットワーク セッション ポリシー（ポリシーが別個のグループに分類されているか、ロール ベースである）のプロビジョニングとメンテナンスが簡略化されます。

サービス テンプレートは、制御ポリシーの参照、RADIUS Change of Authorization（CoA）要求、またはユーザ プロファイルあるいはサービス プロファイルによってセッションに適用されます。ユーザ プロファイルは加入者ごとに定義され、サービス プロファイルは複数の加入者に適用できます。

Identity-Based Networking Services は、次の 2 種類のサービス テンプレートをサポートします。

- ダウンロード可能なサービス テンプレート：サービス テンプレートは外部 ACS または AAA サーバに一元的に設定され、オンデマンドでダウンロードされます。
- ローカルで設定されたサービス テンプレート：サービス テンプレートは、Cisco IOS Command-Line Interface（CLI）を使用して、デバイスでローカルに設定されます。

ダウンロード可能なサービス テンプレート

Identity-Based Networking Services は、外部 AAA サーバで定義されたサービス テンプレートをダウンロードできます。 このテンプレートは、AAA 属性の集合を定義します。 これらのテンプレートは、外部 AAA サーバまたは ACS から受信した RADIUS CoA メッセージに含まれるベンダー固有属性（VSA）によってセッションに適用されます。テンプレート名は、処理中にサービステンプレートのダウンロードをトリガーするユーザ プロファイルまたは制御ポリシーで参照されます。

ダウンロード可能なテンプレートはデバイスにキャッシュされ、後続のダウンロードの要求は、使用可能なキャッシュ テンプレートを参照します。ただし、テンプレートがキャッシュされるのは、そのテンプレートがアクティブに使用されている間のみです。 デバイスにキャッシュされた

ダウンロード済みのテンプレートは保護され、コマンドライン インターフェイスやその他のアプリケーションからは削除できません。 これにより、テンプレートが削除されるのは、そのテンプレートに対するアクティブな参照がない場合にのみになります。

ローカルで設定されたサービス テンプレート

サービステンプレートはCLIを使用してローカルで設定できます。 これらのサービステンプレートは、制御ポリシーの参照により、加入者セッションに適用できます。

アクティブなローカル テンプレートが更新されると、そのローカル テンプレートに対する変更は、そのテンプレートがアクティブになっているすべてのセッションに対して反映されます。 テンプレートが削除されると、セッションに対して適用されているそのテンプレートのすべてのコンテンツが削除されます。

アイデンティティ サービス テンプレートの設定方法

ローカル サービス テンプレートの設定

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ローカル ポリシーを定義します。 該当のローカル ポリシーを適用する必要があるセッションで、このサービス テンプレートをアクティブ化します。

手順の概要

1. **enable**
2. **configure terminal**
3. **service-template** *template-name*
4. **absolute-timer** *minutes*
5. **access-group** *access-list-name*
6. **description** *description*
7. **inactivity-timer** *minutes* **[probe]**
8. **redirect url** *url*
9. **tag** *tag-name*
10. **vlan** *vlan-id*
11. **end**
12. **show service-template** [*template-name*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**service-template** *template-name* 例： `Device(config)# service-template SVC_2`	サービス テンプレートを作成し、サービス テンプレート コンフィギュレーション モードを開始します。
ステップ 4	**absolute-timer** *minutes* 例： `Device(config-service-template)# absolute-timer 15`	（任意）加入者セッションに対する絶対タイムアウトをイネーブルにします。
ステップ 5	**access-group** *access-list-name* 例： `Device(config-service-template)# access-group ACL_2`	（任意）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 リストを適用します。
ステップ 6	**description** *description* 例： `Device(config-service-template)# description label for SVC_2`	（任意）サービス テンプレートの説明を追加します。
ステップ 7	**inactivity-timer** *minutes* **[probe]** 例： `Device(config-service-template)# inactivity-timer 15`	（任意）加入者セッションに対して、非アクティブ タイムアウトをイネーブルにします。
ステップ 8	**redirect url** *url* 例： `Device(config-service-template)# redirect url www.cisco.com`	（任意）特定のURLにクライアントを転送します。

	コマンドまたはアクション	目的
ステップ 9	**tag** *tag-name* 例： `Device(config-service-template)# tag TAG_2`	（任意）ユーザ定義のタグをサービス テンプレートに関連付けます。
ステップ 10	**vlan** *vlan-id* 例： `Device(config-service-template)# vlan 215`	（任意）サービス テンプレートを使用して、セッションに VLAN を適用します。
ステップ 11	**end** 例： `Device(config-service-template)# end`	サービス テンプレートのコンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 12	**show service-template** [*template-name*] 例： `Device# show service-template SVC_2`	設定したサービス・テンプレートに関する情報を表示します。

例：サービス テンプレート

```
service-template SVC_2
 description label for SVC_2
 access-group ACL_2
 redirect url www.cisco.com
 vlan 215
 inactivity-timer 15
 absolute-timer 15
 tag TAG_2
```

次の作業

加入者セッションでサービステンプレートをアクティブ化するには、制御ポリシーでサービステンプレートを指定します。「制御ポリシーの設定, （17 ページ）」を参照してください。

アイデンティティ サービス テンプレートの設定例

例：サービス テンプレートのアクティブ化とすべての置き換え

ローカル サービス テンプレートの設定

次の例は、デバイスでローカルに定義されたサービステンプレートの設定を示しています。このテンプレートにはPOSTURE_VALIDATIONという名前の制御ポリシーを使用するセッションに適用される属性が含まれています（以下を参照）。

```
service-template DOT1X
 access-group SVC1_ACL
 redirect url www.cisco.com match URL_REDIRECT_ACL
 inactivity-timer 60
 absolute-timer 300
!
ip access-list extended URL_REDIRECT_ACL
 permit tcp any host 5.5.5.5 eq www
```

制御ポリシーの設定

次の例は、replace-allがイネーブルになったDOT1Xという名前のサービス テンプレートをアクティブ化する制御ポリシーを示します。 正常にアクティブ化されたテンプレートは、セッションに以前に適用された、既存の認可データとすべてのサービス テンプレートを置き換えます。

```
policy-map type control subscriber POSTURE_VALIDATION
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x priority 10
   20 authenticate using webauth priority 20
 event authentication-success match-all
  10 class DOT1X do-all
   10 terminate webauth
   20 activate service-template DOT1X replace-all
```

例：フォールバック サービスのサービス テンプレートのアクティブ化

ローカル サービス テンプレートの設定

次の例は、デバイスでローカルに定義されたサービステンプレートの設定を示しています。このテンプレートにはPOSTURE_VALIDATIONという名前の制御ポリシーを使用するセッションに適用される属性が含まれています（以下を参照）。

```
service-template FALLBACK
 description fallback service
 access-group ACL_2
 redirect url www.cisco.com
 inactivity-timer 15
 absolute-timer 15
 tag TAG_2
```

制御ポリシーの設定

次の例は、認証方式 dot1x および MAB を実行する制御ポリシーを示しています。 dot1x 認証が失敗すると、MAB 認証が試行されます。 MAB が失敗すると、FALLBACK テンプレートを使用するデフォルトの許可プロファイルが提供されます。

```
policy-map type control subscriber POSTURE_VALIDATION
 event session-started match-all
  10 class always do-all
   10 authenticate using dot1x
 event authentication-failure match-all
  10 class DOT1X do-all
   10 authenticate using mab
  20 class MAB do-all
   10 activate service-template FALLBACK
```

例：サービス テンプレートの非アクティブ化

アクセス コントロール リストの設定

次の例は、以下の LOW_IMPACT_TEMPLATE という名前のローカル サービス テンプレートで使用されるアクセス コントロール リスト（ACL）の設定を示しています。

```
ip access-list extended LOW_IMPACT_ACL
 permit udp any any eq bootps
 permit tcp any any eq www
 permit tcp any any eq 443
 permit ip any 172.30.0.0 0.0.255.255
```

ローカル サービス テンプレートの設定

次の例は、認証が失敗した場合でも、すべてのホストに対する限定されたアクセスを提供するローカル サービス テンプレートの設定を示しています。

```
service-template LOW_IMPACT_TEMPLATE
 description Service template for Low impact mode
 access-group LOW_IMPACT_ACL
 inactivity-timer 60
 tag LOW_IMPACT_TEMPLATE
```

制御ポリシーの設定

次の例は、LOW_IMPACT_TEMPLATE という名前のテンプレートを使用して、認証が失敗した場合でも、すべてのホストに対する限定されたアクセスを提供する制御ポリシーの設定を示しています。 認証が成功すると、ポリシー マネージャはこのサービス テンプレートを削除し、RADIUS サーバからダウンロードされたポリシーに基づいてアクセスを提供します。

```
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
```

その他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
Identity-Based Networking Services コマンド	『Cisco IOS Identity-Based Networking Services Command Reference』
アドレス解決プロトコル（ARP）コマンド	『Cisco IOS IP Addressing Services Command Reference』
ARP 設定作業	『*IP Addressing - ARP Configuration Guide*』
認証、許可、およびアカウンティング（AAA）の設定作業	『*Authentication Authorization and Accounting Configuration Guide*』
AAA コマンド	『*Cisco IOS Security Command Reference*』

標準および RFC

標準/RFC	Title
RFC 5176	『*Dynamic Authorization Extensions to RADIUS*』

テクニカル サポート

説明	Link
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

アイデンティティサービステンプレートの機能に関する情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。 その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *3*：アイデンティティ サービス テンプレートの機能に関する情報

機能名	リリース	機能情報
ダウンロード可能なアイデンティティ サービス テンプレート	Cisco IOS XE Release 3.2SE	ACS からダウンロードサービス テンプレートと、セッションに対して適用するそのサービス テンプレートの属性をイネーブルにします。

機能名	リリース	機能情報
アイデンティティ サービス テンプレート	Cisco IOS XE Release 3.2SE	アイデンティティ サービス テンプレートのローカルでの設定と、常時利用をイネーブルにします。 導入されたコマンド：**absolute-timer**、**access-group** (service template)、**description** (service template)、**inactivity-timer**、**redirect url**、**service-template**、**show service-template**、**tag** (service template)、**vlan** (service template)。

第 4 章

認可変更のサポート

Identity-Based Networking Services は、セッションのクエリー、再認証、および終了、ポート バウンスとポートのシャットダウン、およびサービス テンプレートのアクティブ化と非アクティブ化のための RADIUS Change of Authorization（CoA）コマンドをサポートします。 このモジュールでは、Identity-Based Networking Services 用にサポートされる CoA コマンドに関する情報を提供します。

- 機能情報の確認，47 ページ
- CoA のサポートに関する情報，48 ページ
- その他の関連資料，53 ページ
- CoA サポートの機能情報，54 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を確認し、各機能がサポートされているリリースのリストを確認するには、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

CoA のサポートに関する情報

RADIUS 認可変更のサポート

Cisco IOS ソフトウェアは、RFC 5176 で定義されている RADIUS CoA の拡張をサポートします。この拡張は、一般に、外部 AAA またはポリシー サーバからのセッションのダイナミックな再構成を可能にするプッシュモデルで使用されます。セッションの特定、セッションの終了、ホストの再認証、ポートのシャットダウン、およびポートバウンスでは、セッションごとのCoA要求がサポートされます。 このモデルは、次のように、1 つの要求（CoA-Request）と 2 つの考えられる応答コードで構成されます。

- CoA acknowledgement（ACK）[CoA-ACK]
- CoA nonacknowledgement（NAK）[CoA-NAK]

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

次の表は、Identity-Based Networking Services でサポートされている RADIUS CoA コマンドとベンダー固有属性（VSA）を示します。 すべての CoA コマンドには、デバイスと CoA クライアント間のセッション ID が含まれている必要があります。

表 *4*：***Identity-Based Networking Services*** でサポートされている ***RADIUS CoA*** コマンド

CoA コマンド	シスコの **VSA**
サービスのアクティブ化	Cisco:Avpair=“subscriber:command=activate-service” Cisco:Avpair=“subscriber:service-name=<*service-name*>” Cisco:Avpair=“subscriber:precedence=<*precedence-number*>” Cisco:Avpair=“subscriber:activation-mode=replace-all”
サービスの非アクティブ化	Cisco:Avpair=“subscriber:command=deactivate-service” Cisco:Avpair=“subscriber:service-name=<*service-name*>”
Bounce host port	Cisco:Avpair=“subscriber:command=bounce-host-port”
Disable host port	Cisco:Avpair=“subscriber:command=disable-host-port”
セッション クエリー	Cisco:Avpair=“subscriber:command=session-query”
セッションの再認証	Cisco:Avpair=“subscriber:command=reauthenticate” Cisco:Avpair=“subscriber:reauthenticate-type=last” または Cisco:Avpair=“subscriber:reauthenticate-type=rerun”
セッションの終了	これは、VSA を必要としない、標準の接続解除要求です。

セッションの識別

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

- Acct-Session-Id（IETF 属性 #44）
- Audit-Session-Id VSA（シスコの VSA）
- Calling-Station-Id（ホスト MAC アドレスを含む IETF 属性 #31）
- 次のいずれかの IPv6 属性。
  - Framed-IPv6-Prefix（IETF 属性 #97）および Framed-Interface-Id（IETF 属性 #96）。ともに RFC 3162 に従った完全な IPv6 アドレスを作成する
  - Framed-IPv6-Address
- プレーン IP アドレス（IETF 属性 #8）

メッセージに複数のセッションID属性が含まれる場合は、すべての属性がセッションと一致する必要があります。一致しない場合、デバイスは、エラー コードが「Invalid Attribute Value」のDisconnect-NAK または CoA-NAK を返します。

特定の適用ポリシーを対象とする CoA 要求の場合、上記のセッション ID 属性のいずれかがメッセージに含まれていると、デバイスはエラー コードが「Invalid Attribute Value」のCoA-NAK を返します。

CoA サービスのアクティブ化コマンド

CoA サービスのアクティブ化コマンドを使用して、セッションでサービス テンプレートをアクティブ化することができます。 AAA サーバは次の VSA を使用して、標準の CoA 要求メッセージで要求を送信します。

Cisco:Avpair="subscriber:command=activate-service"

Cisco:Avpair="subscriber:service-name=<*service-name*>"

Cisco:Avpair="subscriber:precedence=<*precedence-number*>"

Cisco:Avpair="subscriber:activation-mode=replace-all"

このコマンドはセッション指向であるため、「セッションの識別, （49 ページ）」セクションに示されている 1 つ以上のセッション ID 属性とともに使用する必要があります。 デバイスがセッションを検出できない場合、デバイスは「Session Context Not Found」エラー コード属性を含むCoA-NAK メッセージを返します。 デバイスは、セッションを検出すると、ホスティング ポートに対するテンプレートのアクティブ化の操作を開始し、CoA-ACK が返されます。 テンプレートのアクティブ化が失敗すると、エラーコード属性が適切なメッセージに設定されたCoA-NAKメッセージが返されます。

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

CoA サービスの非アクティブ化コマンド

CoA サービスの非アクティブ化コマンドを使用して、セッションでサービス テンプレートを非アクティブ化することができます。 AAA サーバは次の VSA を使用して、標準の CoA 要求メッセージで要求を送信します。

Cisco:Avpair="subscriber:command=deactivate-service"

Cisco:Avpair="subscriber:service-name=<*service-name*>"

このコマンドはセッション指向であるため、「セッションの識別, （49 ページ）」セクションに示されている 1 つ以上のセッション ID 属性とともに使用する必要があります。 デバイスがセッションを検出できない場合、デバイスは「Session Context Not Found」エラー コード属性を含む CoA-NAK メッセージを返します。 デバイスは、セッションを検出すると、ホスティング ポートに対するテンプレートの非アクティブ化操作を開始し、CoA-ACK が返されます。 テンプレートの非アクティブ化が失敗すると、エラー コード属性が該当するメッセージに設定された CoA-NAK メッセージが返されます。

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

CoA ホスト ポートのバウンス コマンド

CoA ホスト ポートのバウンス コマンドはセッションを終了し、ポート をバウンスします（リンク ダウン イベントに続いてリンク アップ イベントを開始します）。 AAA サーバは、次の VSA を含む標準の CoA 要求メッセージで要求を送信します。

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

このコマンドはセッション指向であるため、「セッションの識別, （49 ページ）」セクションに示されている 1 つ以上のセッション ID 属性とともに使用する必要があります。 セッションが見つからない場合、デバイスは「Session Context Not Found」エラー コード属性を使用して CoA-NAK メッセージを返します。 セッションが見つかった場合、デバイスはホスティング ポートを 10 秒間ディセーブルにし、再びイネーブルにして（ポート バウンス）、CoA-ACK を返します。

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

CoA ポートのバウンス コマンドは、エンドポイントが承認の変更後に新しい IP アドレスを取得する必要があり、これが DHCP プロセスを再開するようエンドポイントに示す唯一の手段である

場合の最後の手段として役立ちます。 この状況は、VLAN が変更されており、この認証ポートに関する変化を検出するメカニズムがないデバイス（プリンタなど）がエンドポイントの場合に発生する可能性があります。このコマンドによって、認証ポートでリンク フラップが発生する場合があり、これにより、このポートに接続されている 1 つ以上のホストから DHCP 再ネゴシエーションがトリガされます。

CoA ホスト ポートのディセーブル化コマンド

CoA ホスト ポートのディセーブル化コマンドは、セッションをホスティングしている認証ポートを管理上の理由でシャット ダウンします。これにより、セッションは終了します。 AAA サーバは、次の VSA を含む標準の CoA 要求メッセージで要求を送信します。

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

このコマンドはセッション指向であるため、「セッションの識別, （49 ページ）」セクションに示されている 1 つ以上のセッション ID 属性とともに使用する必要があります。 セッションを検出できない場合、デバイスは「Session Context Not Found」エラー コード属性を含む CoA-NAK メッセージを返します。 デバイスは、セッションを検出すると、ホスティング ポートを無効にし、CoA-ACK メッセージを返します。

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

CoA セッション クエリー コマンド

CoA セッション クエリー コマンドは、加入者セッションに関するサービス情報を要求します。AAA サーバは次の VSA を含む標準の CoA 要求メッセージで要求を送信します。

Cisco:Avpair="subscriber:command=session-query"

このコマンドはセッション指向であるため、「セッションの識別, （49 ページ）」セクションに示されている 1 つ以上のセッション ID 属性とともに使用する必要があります。 デバイスがセッションを検出できない場合、デバイスは「Session Context Not Found」エラー コード属性を含む CoA-NAK メッセージを返します。 デバイスは、セッションを検出すると、セッションに対してセッション クエリー操作を実行し、CoA-ACK メッセージを返します。

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

CoA セッションの再認証コマンド

セッションの認証を開始するために、AAA サーバは次の VSA を含む標準の CoA 要求メッセージを送信します。

Cisco:Avpair="subscriber:command=reauthenticate"

Cisco:Avpair="subscriber:reauthenticate-type=<last | rerun>"

「reauthenticate-type」は、CoA 再認証要求が、該当のセッションで最後に成功した認証方式を使用するか、認証プロセス全体を再実行するかどうかを指定します。

次のルールが適用されます。

- 「subscriber:command=reauthenticate」は、再認証をトリガーするために必要です。
- 「subscriber:reauthenticate-type」が指定されていない場合、デフォルトの動作は該当のセッションで最後に成功した認証方式の再実行です。この方式での再認証が成功すると、すべての古い承認データが、再認証された承認データで置き換えられます。
- 「subscriber:reauthenticate-type」が有効なのは、「subscriber:command=reauthenticate」とともに使用されている場合のみです。別の CoA コマンドに含まれている場合、この VSA は暗黙的に無視されます。

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

CoA セッションの終了コマンド

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

デバイスが CoA-ACK をクライアントに返す前にデバイスに障害が発生した場合、クライアントから要求が再送信されると、新しいアクティブ デバイス上でそのプロセスが繰り返されます。

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

その他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
Identity-Based Networking Services コマンド	『Cisco IOS Identity-Based Networking Services Command Reference』
アドレス解決プロトコル（ARP）コマンド	『Cisco IOS IP Addressing Services Command Reference』
ARP 設定作業	『*IP Addressing - ARP Configuration Guide*』
認証、許可、およびアカウンティング（AAA）の設定作業	『*Authentication Authorization and Accounting Configuration Guide*』
AAA コマンド	『*Cisco IOS Security Command Reference*』

標準および RFC

標準/RFC	Title
RFC 5176	『*Dynamic Authorization Extensions to RADIUS*』

テクニカル サポート

説明	Link
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

CoA サポートの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。 その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *5* : *CoA* サポートの機能情報

機能名	リリース	機能情報
『Change of Authorization』	Cisco IOS XE Release 3.2SE	次を開始する CoA 要求がサポートされています。 • セッションでのサービス テンプレートのアクティブ化および非アクティブ化 • ポート バウンス • ポートのシャットダウン • セッションのクエリー • セッション再認証 • セッションの終了 これらの VSA は、AAA サーバからの標準 CoA 要求メッセージで送信されます。

第 5 章

LDAP を使用したローカル認証の設定

Lightweight Directory Access Protocol（LDAP）を使用したローカル認証を使用すると、LDAP をバックエンドとした Web 認証、802.1X、MAC 認証バイパス（MAB）を使用して、エンドポイントを認証することができます。 Identity-Based Networking Services のローカル認証でも、認証、許可、およびアカウンティング（AAA）属性リストとローカル ユーザ名のリストの関連付けがサポートされます。 このモジュールでは、Identity-Based Networking Services のローカル認証の設定に関する情報を提供します。

- 機能情報の確認，55 ページ
- LDAP を使用したローカル認証に関する情報，56 ページ
- LDAP を使用したローカル認証の設定方法，56 ページ
- LDAP を使用したローカル認証の設定例，60 ページ
- その他の関連資料，61 ページ
- LDAP を使用したローカル認証の機能情報，62 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を確認し、各機能がサポートされているリリースのリストを確認するには、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

LDAP を使用したローカル認証に関する情報

LDAP を使用したローカル認証

LDAP を使用したローカル認証を使用すると、LDAP をバックエンドとした Web 認証、802.1X、MAB を使用して、エンドポイントを認証することができます。ローカル認証は、ワイヤレスセッションのローカル ユーザ名と属性リストを関連付けることで、追加の AAA 属性をサポートします。

AES キー ラップ

Advanced Encryption Standards（AES）キー ラップ機能は、コントローラと RADIUS サーバ間の共有秘密の安全性を強化します。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。

LDAP を使用したローカル認証の設定方法

LDAP を使用したローカル認証の設定

ローカル認証に対して AAA 方式のリストを指定し、属性リストをローカル ユーザ名に関連付けるには、この作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa local authentication** {*method-list-name* | **default**} **authorization** {*method-list-name* | **default**}
4. **username** *name* **aaa attribute list** *aaa-attribute-list* [**password** *password*]
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa local authentication** {*method-list-name* | **default**} **authorization** {*method-list-name* | **default**} 例： `Device(config)# aaa local authentication default authorization default`	LDAP サーバからのローカル認証および認可に使用する方式のリストを指定します。
ステップ 4	**username** *name* **aaa attribute list** *aaa-attribute-list* [**password** *password*] 例： `Device(config)# username USER_1 aaa attribute list LOCAL_LIST password CISCO`	ローカル ユーザ名と AAA 属性リストを関連付けます。
ステップ 5	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

MAC フィルタリング サポートの設定

MAC フィルタリングをサポートするには、RADIUS 互換モード、MAC デリミタ、および MAC アドレスをユーザ名として設定し、この作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa group server radius** *group-name*
4. **subscriber mac-filtering security-mode** {**mac** | **none** | **shared-secret**}
5. **mac-delimiter** {**colon** | **hyphen** | **none** | **single-hyphen**}
6. **exit**
7. **username** *mac-address* **mac** [**aaa attribute list** *aaa-attribute-list*]
8. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa group server radius** *group-name* 例： `Device(config)# aaa group server radius RAD_GROUP1`	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。
ステップ 4	**subscriber mac-filtering security-mode** {**mac** | **none** | **shared-secret**} 例： `Device(config-sg-radius)# subscriber mac-filtering security-mode mac`	MAC フィルタリングの RADIUS 互換モードを指定します。 • デフォルト値は **none** です。
ステップ 5	**mac-delimiter** {**colon** | **hyphen** | **none** | **single-hyphen**} 例： `Device(config-sg-radius)# mac-delimiter hyphen`	RADIUS 互換モードの MAC デリミタを指定します。 • デフォルト値は **none** です。
ステップ 6	**exit** 例： `Device(config-sg-radius)# exit`	サーバ グループ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**username** *mac-address* **mac** [**aaa attribute list** *aaa-attribute-list*] 例： `Device(config)# username 00-22-WP-EC-23-3C mac aaa attribute list AAA_list1`	ローカルで実行される MAC フィルタリングのユーザ名として MAC アドレスを使用できるようにします。
ステップ 8	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

AES キー ラップのイネーブル化

Advanced Encryption Standards（AES）キー ラップは、コントローラと RADIUS サーバ間の共有秘密の安全性を強化します。 AES キー ラップでは、キー ラップ準拠の RADIUS 認証サーバが必要です。

手順の概要

1. **enable**
2. **configure terminal**
3. **radius-server host** {*hostname* | *ip-address*} **key-wrap encryption-key** *encryption-key* **message-auth-code-key** *encryption-key* [**format** {**ascii** | **hex**}]
4. **aaa group server radius** *group-name*
5. **server** *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*]
6. **key-wrap enable**
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**radius-server host** {*hostname* | *ip-address*} **key-wrap encryption-key** *encryption-key* **message-auth-code-key** *encryption-key* [**format** {**ascii** | **hex**}] 例： `Device(config)# radius-server host 10.10.1.2 key-wrap encryption-key testkey99 message-auth-code-key testkey123`	RADIUS サーバ ホストを定義します。
ステップ 4	**aaa group server radius** *group-name* 例： `Device(config)# aaa group server radius RAD_GROUP1`	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。

	コマンドまたはアクション	目的
ステップ 5	**server** *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*] 例： `Device(config-sg-radius)# server 10.10.1.2`	サーバ グループの RADIUS サーバの IP アドレスを指定します。
ステップ 6	**key-wrap enable** 例： `Device(config-sg-radius)# key-wrap enable`	この RADIUS サーバの AES キー ラップをイネーブルにします。
ステップ 7	**end** 例： `Device(config-sg-radius)# end`	サーバ グループ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

LDAP を使用したローカル認証の設定例

例：LDAP を使用したローカル認証の設定

次の例は、ローカル認証の設定を示しています。

```
!
username USER_1 password 0 CISCO
username USER_1 aaa attribute list LOCAL_LIST
aaa new-model
aaa local authentication EAP_LIST authorization EAP_LIST
!
```

例：MAC フィルタリング サポートの設定

次の例は、MAC フィルタリングの設定を示しています。

```
username 00-22-WP-EC-23-3C mac aaa attribute list AAA_list1
!
aaa group server radius RAD_GROUP1
 subscriber mac-filtering security-mode mac
 mac-delimiter hyphen
```

例：AES キー ラップの設定

次の例は、RADIUS サーバに対してイネーブル化されたキー ラップの設定を示しています。

```
aaa group server radius RAD_GROUP1
 server 10.10.1.2
 key-wrap enable
```

```
!
radius-server host 10.10.1.2
!
```

その他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
Identity-Based Networking Services コマンド	『Cisco IOS Identity-Based Networking Services Command Reference』
アドレス解決プロトコル（ARP）コマンド	『Cisco IOS IP Addressing Services Command Reference』
ARP 設定作業	『*IP Addressing - ARP Configuration Guide*』
認証、許可、およびアカウンティング（AAA）の設定作業	『*Authentication Authorization and Accounting Configuration Guide*』
AAA コマンド	『*Cisco IOS Security Command Reference*』

標準および RFC

標準/RFC	Title
RFC 5176	『*Dynamic Authorization Extensions to RADIUS*』

テクニカル サポート

説明	Link
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

LDAP を使用したローカル認証の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *6*：*LDAP* を使用したローカル認証の機能情報

機能名	リリース	機能情報
LDAP を使用したローカル認証	Cisco IOS XE Release 3.2SE	Lightweight Directory Access Protocol（LDAP）を使用してローカル認証のサポートを導入します。 導入または変更されたコマンド：**aaa local authentication**、**key-wrap enable**、**mac-delimiter**、**radius-server host**、**subscriber mac-filtering security-mode**、**username**。

第 6 章

クリティカル音声 VLAN のサポート

クリティカル音声 VLAN のサポート機能は、認証サーバが到達不能になると、電話のトラフィックをポートの設定済みの音声 VLAN に転送します。

通常のネットワーク接続では、IP フォンがポートで正常に認証されると、認証サーバは、電話トラフィックをポートの音声ドメインに転送します。 認証サーバが到達不能になると、IP フォンは電話トラフィックを認証できません。 マルチドメイン認証（MDA）モードまたはマルチ認証モードでは、電話トラフィックをポートの設定済みの音声 VLAN ポートに送信するように、クリティカル音声 VLAN サポート機能を設定できます。 電話は不明なドメインとして認可されます。 データおよび音声の両方が、電話に対してイネーブルになります。

- 機能情報の確認，63 ページ
- クリティカル音声 VLAN のサポートに関する制限，64 ページ
- クリティカル音声 VLAN サポートに関する情報，64 ページ
- クリティカル音声 VLAN サポートの設定方法，65 ページ
- クリティカル音声 VLAN サポートの設定例，71 ページ
- クリティカル音声 VLAN のサポートに関するその他の関連資料，72 ページ
- クリティカル音声 VLAN サポートの機能情報，72 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を確認し、各機能がサポートされているリリースのリストを確認するには、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

クリティカル音声 VLAN のサポートに関する制限

- 音声およびデータに対して、各種の VLAN を設定する必要があります。
- デバイスで音声 VLAN を設定する必要があります。
- クリティカル音声 VLAN のサポート機能は、スイッチ ポートでの標準アクセス コントロール リスト（ACL）をサポートしません。

クリティカル音声 VLAN サポートに関する情報

マルチドメイン認証モードでのクリティカル音声 VLAN のサポート

クリティカル音声 VLAN がマルチドメイン認証（MDA）モードのインターフェイスを使用して展開されている場合、ホスト モードはマルチホストに変更され、最初の電話デバイスがスタティックな転送エントリとしてインストールされます。 追加の電話デバイスは、ホスト アクセス テーブル（HAT）にダイナミックな転送エントリとしてインストールされます。

ホスト モードの詳細については、『*802.1X Authentication Services Configuration Guid*（*802.1X* 認証サービスの設定ガイド）』を参照してください。

（注） クリティカル ポートが認可済みで、再認証が行われた場合、スイッチは現在の VLAN（事前に RADIUS サーバにより割り当てられた）でそのポートをクリティカル認証状態にします。

（注） アクセス不能認証バイパスは、ゲスト VLAN と互換性があります。 ゲスト VLAN が 802.1X ポートでイネーブルの場合、この機能は次のように相互作用します。すべての RADIUS サーバが使用できず、クライアントがクリティカル ポートに接続されていて、かつ以前にゲスト VLAN に割り当てられていた場合、スイッチはそのポートをゲスト VLAN に保持します。

マルチ認証モードでのクリティカル音声 VLAN のサポート

クリティカル認証機能がマルチ認証モードで展開されている場合、1 つの電話デバイスのみが許可され、2 つ目の電話が認可を試行すると、違反が発生します。

show authentication sessions コマンドは、クリティカル音声クライアント データを表示します。マルチ認証ホスト モードでクリティカルに認可された音声クライアントは、「authz success」および「authz fail」状態になります。

（注） クリティカル音声が必要な場合は、クリティカル データも設定する必要があります。 これを行わない場合、音声 VLAN が開いたとき、クリティカル音声クライアントは「authz fail」状態と表示されます。

サービス テンプレートでのクリティカル音声 VLAN のサポート

エンタープライズエッジ（eEdge）デバイスでは、認証サーバが到達不能な場合、電話のクリティカル アクセスは、クリティカル サービス テンプレートをアクティブにすることによって設定されます。 音声機能のプラグインは、認証、許可、およびアカウンティング（AAA）の音声属性を使用して Enterprise Policy Manager（EPM）に登録され、この AAA サービスが使用できない間、音声 VLAN への無条件のアクセスを可能にします。

クリティカル音声 VLAN のサポートをイネーブルにするには、電話のクリティカル認証が、制御ポリシー ルールとサービス テンプレートの組み合わせを使用して設定されている必要があります。

認証サーバが使用できないことに加えてホストが認可されていない場合、AAA 属性 device-traffic-type は自動的に入力されません。 電話は不明なドメインとして認可され、データおよび音声 VLAN の両方がこのデバイスに対してイネーブルになり、デバイスが音声トラフィックを処理できるようになります。

クリティカル音声 VLAN サポートの設定方法

サービス テンプレートでの音声 VLAN の設定

サービステンプレートを使用してクリティカル音声 VLAN のサポートを設定するには、ポートでこの作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **service-template** *template-name*
4. **vlan** *vlan-id*
5. **exit**
6. **service-template** *template-name*
7. **voice vlan**
8. **exit**
9. **class-map type control subscriber** {**match-all** | **match-any** | **match-none**} *control-class-name*
10. **match result-type** [**method** {**dot1x** | **mab** | **webauth**}] *result-type*
11. **match authorization-status** {**authorized** | **unauthorized**}
12. **exit**
13. **class-map type control subscriber** {**match-all** | **match-any** | **match-none**} *control-class-name*
14. **match result-type** [**method** {**dot1x** | **mab** | **webauth**}] *result-type*
15. **match authorization-status** {**authorized** | **unauthorized**}
16. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**service-template** *template-name* 例： `Device(config)# service-template SERVICE-TEMPLATE`	加入者セッションに適用する一連のサービス ポリシー属性が含まれるテンプレートを定義して、サービス テンプレート コンフィギュレーション モードを開始します。
ステップ 4	**vlan** *vlan-id* 例： `Device(config-service-template)# vlan 116`	加入者セッションに VLAN を割り当てます。

	コマンドまたはアクション	目的
ステップ 5	**exit** 例： `Device(config-service-template)# exit`	サービス テンプレート コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**service-template** *template-name* 例： `Device(config)# service-template CRITICAL-VOICE`	加入者セッションに適用する一連のサービス ポリシー属性が含まれるテンプレートを定義して、サービス テンプレート コンフィギュレーション モードを開始します。
ステップ 7	**voice vlan** 例： `Device(config-service-template)# voice vlan`	加入者セッションにクリティカル音声 VLAN を割り当てます。
ステップ 8	**exit** 例： `Device(config-service-template)# exit`	サービス テンプレート コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 9	**class-map type control subscriber** {**match-all** | **match-any** | **match-none**} *control-class-name* 例： `Device(config)# class-map type control subscriber match-all AAA-SVR-DOWN-UNAUTHD-HOST`	制御ポリシーのアクションが実行され、制御クラス マップ フィルタ コンフィギュレーション モードを開始する条件を定義する制御クラスを作成します。
ステップ 10	**match result-type** [**method** {**dot1x** | **mab** | **webauth**}] *result-type* 例： `Device(config-filter-control-classmap)# match result-type aaa-timeout`	指定した認証結果に基づいて true を返す条件を作成します。
ステップ 11	**match authorization-status** {**authorized** | **unauthorized**} 例： `Device(config-filter-control-classmap)# match authorization-status unauthorized`	セッションの認可状態に基づいて true を返す条件を作成します。
ステップ 12	**exit** 例： `Device(config-filter-control-classmap)# exit`	制御クラスマップ フィルタ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
ステップ 13	**class-map type control subscriber** {**match-all** | **match-any** | **match-none**} *control-class-name* 例： `Device(config)# class-map type control subscriber match-all AAA-SVR-DOWN-AUTHD-HOST`	制御ポリシーのアクションが実行され、制御クラスマップ フィルタ コンフィギュレーション モードを開始する条件を定義する制御クラスを作成します。
ステップ 14	**match result-type** [**method** {**dot1x** | **mab** | **webauth**}] *result-type* 例： `Device(config-filter-control-classmap)# match result-type aaa-timeout`	指定した認証結果に基づいて true を返す条件を作成します。
ステップ 15	**match authorization-status** {**authorized** | **unauthorized**} 例： `Device(config-filter-control-classmap)# match authorization-status authorized`	セッションの認可状態に基づいて true を返す条件を作成します。
ステップ 16	**end** 例： `Device(config-filter-control-classmap)# end`	制御クラスマップ フィルタ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

クリティカル音声 VLAN のアクティブ化

サービス テンプレートで設定されているクリティカル音声 VLAN をアクティブ化するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map type control subscriber** *control-policy-name*
4. **event authentication-failure** [**match-all** | **match-first**]
5. *priority-number* **class** {*control-class-name* | **always**} [**do-all** | **do-until-failure** | **do-until-success**]
6. *action-number* **activate** {**policy type control subscriber** *control-policy-name* | **service-template** *template-name* [**aaa-list** *list-name*] [**precedence** [**replace-all**]]}
7. *action-number* **activate** {**policy type control subscriber** *control-policy-name* | **service-template** *template-name* [**aaa-list** *list-name*] [**precedence** [**replace-all**]]}
8. *action-number* **authorize**
9. *action-number* **pause reauthentication**
10. **exit**
11. *priority-number* **class** {*control-class-name* | **always**} [**do-all** | **do-until-failure** | **do-until-success**]
12. *action-number* **pause reauthentication**
13. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**policy-map type control subscriber** *control-policy-name* 例： `Device(config)# policy-map type control subscriber cisco-subscriber`	加入者セッションに対して制御ポリシーを定義し、制御ポリシーマップ イベントのコンフィギュレーション モードを開始します。
ステップ 4	**event authentication-failure** [**match-all**	**match-first**] 例： `Device(config-event-control-policymap)# event authentication-failure match-first`	すべての認証イベントが match であり、制御ポリシーマップ クラスのコンフィギュレーション モードが開始された場合に、制御ポリシーの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。

	コマンドまたはアクション	目的
ステップ 5	*priority-number* **class** {*control-class-name* | **always**} [**do-all** | **do-until-failure** | **do-until-success**] 例： `Device(config-class-control-policymap)# 10 class AAA-SVR-DOWN-UNAUTHD-HOST do-until-failure`	アクションの 1 つが失敗し、制御ポリシーマップアクションのコンフィギュレーションモードが開始されるまで、制御クラスが制御ポリシー内のアクションを指定された順序で実行するように指定します。
ステップ 6	*action-number* **activate** {**policy type control subscriber** *control-policy-name* | **service-template** *template-name* [**aaa-list** *list-name*] [**precedence** [**replace-all**]]} 例： `Device(config-action-control-policymap)# 10 activate service-template foo-DATA`	加入者セッションの VLAN に関連付けられている制御ポリシーをアクティブ化します。
ステップ 7	*action-number* **activate** {**policy type control subscriber** *control-policy-name* | **service-template** *template-name* [**aaa-list** *list-name*] [**precedence** [**replace-all**]]} 例： `Device(config-action-control-policymap)# 10 activate service-template CRITICAL-VOICE`	加入者セッションの音声 VLAN に関連付けられている制御ポリシーをアクティブ化します。
ステップ 8	*action-number* **authorize** 例： `Device(config-action-control-policymap)# 30 authorize`	加入者セッションの認可を開始します。
ステップ 9	*action-number* **pause reauthentication** 例： `Device(config-action-control-policymap)# 40 pause reauthentication`	認証の失敗後に再認証プロセスを停止します。
ステップ 10	**exit** 例： `Device(config-action-control-policymap)# exit`	制御ポリシーマップアクションのコンフィギュレーション モードを終了し、制御ポリシーマップ クラスのコンフィギュレーション モードを開始します。
ステップ 11	*priority-number* **class** {*control-class-name* | **always**} [**do-all** | **do-until-failure** | **do-until-success**] 例： `Device(config-class-control-policymap)# 20 class AAA-SVR-DOWN-AUTHD-HOST`	アクションの 1 つが失敗し、制御ポリシーマップアクションのコンフィギュレーションモードが開始されるまで、制御クラスが制御ポリシー内のアクションを指定された順序で実行するように指定します。

	コマンドまたはアクション	目的
ステップ 12	*action-number* **pause reauthentication** 例： `Device(config-action-control-policymap)# 10 pause reauthentication`	認証の失敗後に再認証プロセスを停止します。
ステップ 13	**end** 例： `Device(config-action-control-policymap)# exit`	制御ポリシーマップアクションのコンフィギュレーションモードを終了し、特権EXECモードを開始します。

クリティカル音声 VLAN サポートの設定例

例：サービス テンプレートでの音声 VLAN の設定

```
Device> enable
Device# configure terminal
Device(config)# service-template SERVICE-TEMPLATE
Device(config-service-template)# vlan 116
Device(config-service-template)# exit
Device(config)# service-template CRITICAL-VOICE
Device(config-service-template)# voice vlan
Device(config-service-template)# exit
Device(config)# class-map type control subscriber match-all AAA-SVR-DOWN-UNAUTHD-HOST
Device(config-filter-control-classmap)# match result-type aaa-timeout
Device(config-filter-control-classmap)# match authorization-status unauthorized
Device(config-filter-control-classmap)# exit
Device(config)# class-map type control subscriber match-all AAA-SVR-DOWN-AUTHD-HOST
Device(config-filter-control-classmap)# match result-type aaa-timeout
Device(config-filter-control-classmap)# match authorization-status authorized
Device(config-filter-control-classmap)# end
```

例：サービス テンプレートでのクリティカル音声 VLAN のアクティブ化

```
Device> enable
Device# configure terminal
Device(config)# policy-map type control subscriber cisco-subscriber
Device(config-event-control-policymap)# event authentication-failure match-first
Device(config-class-control-policymap)# 10 class AAA-SVR-DOWN-UNAUTHD-HOST do-until-failure
Device(config-action-control-policymap)# 10 activate service-template SERVICE-TEMPLATE
Device(config-action-control-policymap)# 10 activate service-template CRITICAL-VOICE
Device(config-action-control-policymap)# 30 authorize
Device(config-action-control-policymap)# 40 pause reauthentication
Device(config-action-control-policymap)# exit
Device(config-class-control-policymap)# 20 class AAA-SVR-DOWN-AUTHD-HOST
Device(config-action-control-policymap)# 10 pause reauthentication
Device(config-action-control-policymap)# end
```

クリティカル音声 VLAN のサポートに関するその他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
Cisco Identity-Based Networking Services コマンド	『Cisco IOS Identity-Based Networking Services Command Reference』

標準および RFC

標準/RFC	Title
IEEE 802.1X	『*Port Based Network Access Control*』

テクニカル サポート

説明	Link
★枠で囲まれた Technical Assistance の場合★右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

クリティカル音声 VLAN サポートの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 7：クリティカル音声 *VLAN* サポートの機能情報

機能名	リリース	機能情報
クリティカル音声 VLAN のサポート	15.2(1)E Cisco IOS XE Release 3.3SE	この機能は、認証サーバが到達不能になった場合に電話トラフィックをポートの設定済み音声 VLAN に送信する、クリティカル音声 VLAN のサポートをイネーブルにします。 追加または変更されたコマンド：**voice vlan**

第 7 章

有線ゲスト アクセス

有線ゲスト アクセス機能は、有線およびワイヤレスの両方のアクセスをサポートしている企業ネットワークのゲスト ユーザに対して、有線のイーサネット接続からのゲスト アクセス ネットワークへの接続を可能にします。 有線のイーサネット接続はゲスト アクセスに対して指定および設定されます。 モビリティ エージェントの有線セッションのゲストは、Control And Provisioning of Wireless Access Points（CAPWAP）トンネル経由で、非武装地帯（DMZ）のワイヤレス ゲスト コントローラに誘導されます。

有線ゲスト アクセスは、スタンドアロン設定または、アンカー コントローラと外部コントローラの両方を使用するデュアル コントローラ設定で設定できます。 デュアル コントローラ構成は、有線ゲスト アクセス トラフィックを分離しますが、有線ゲスト アクセスの導入は必要ありません。

有線ゲスト アクセス ポートは、まず、レイヤ 2 アクセス スイッチか、有線ゲストのアクセス トラフィック用 VLAN インターフェイスで設定されたスイッチ ポートで終端します。 有線ゲスト トラフィックはその後、アクセス スイッチからコントローラへトランクされます。 このコントローラは、アクセス スイッチの有線ゲスト アクセス VLAN にマップされているインターフェイスを使用して設定されます。

- 機能情報の確認，76 ページ
- 有線ゲスト アクセスに関する制限，76 ページ
- 有線ゲスト アクセスについて，76 ページ
- 有線ゲスト アクセスの設定方法，79 ページ
- 有線ゲスト アクセスの設定例，84 ページ
- 有線ゲスト アクセスに関するその他の関連資料，87 ページ
- 有線ゲスト アクセスの機能情報，88 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を確認し、各機能がサポートされているリリースのリストを確認するには、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

有線ゲスト アクセスに関する制限

- 有線クライアントのトンネリングは、クライアントが、オープンモード用に設定された Cisco Next Generation Wiring Closet（NGWC）デバイスのポートに接続されている場合にはサポートされません。
- 有線クライアントのトンネリングは NGWC デバイスの Web 認証が成功した後はサポートされません。これは、Web 認証の後では、自動での IP アドレスの再割り当てがサポートされないためです。
- NGWC デバイスは、コントローラで行われる Web 認証に基づくトンネルのみを経由したネットワーク アクセスをサポートします。
- Network Advertisement and Selection Protocol（NASP）は有線クライアントではサポートされません。
- ハイ アベイラビリティは、ワイヤレス セッションではサポートされていません。 有線クライアントに対してトンネル化されたゲスト アクセスが提供されている間にワイヤレス コントローラが失敗した場合、この状態が自動的にリカバリされることはありません。
- 非アクティブ化エージングは、ワイヤレス コントローラに対してプロビジョニングされた有線クライアント（たとえば、コントローラで Web 認証が実行された後で受信された RADIUS のアクセス受け入れ要求内）ではサポートされません。

有線ゲスト アクセスについて

有線ゲスト アクセスの概要

有線およびワイヤレスのアクセス両方をサポートするエンタープライズ ネットワークは、2 つのアクセス メディアでクライアント エクスペリエンスと管理性の両方の面で一貫したゲスト サービスを提供する必要があります。 ワイヤレス ネットワークの場合、モビリティ アンカー デバイ

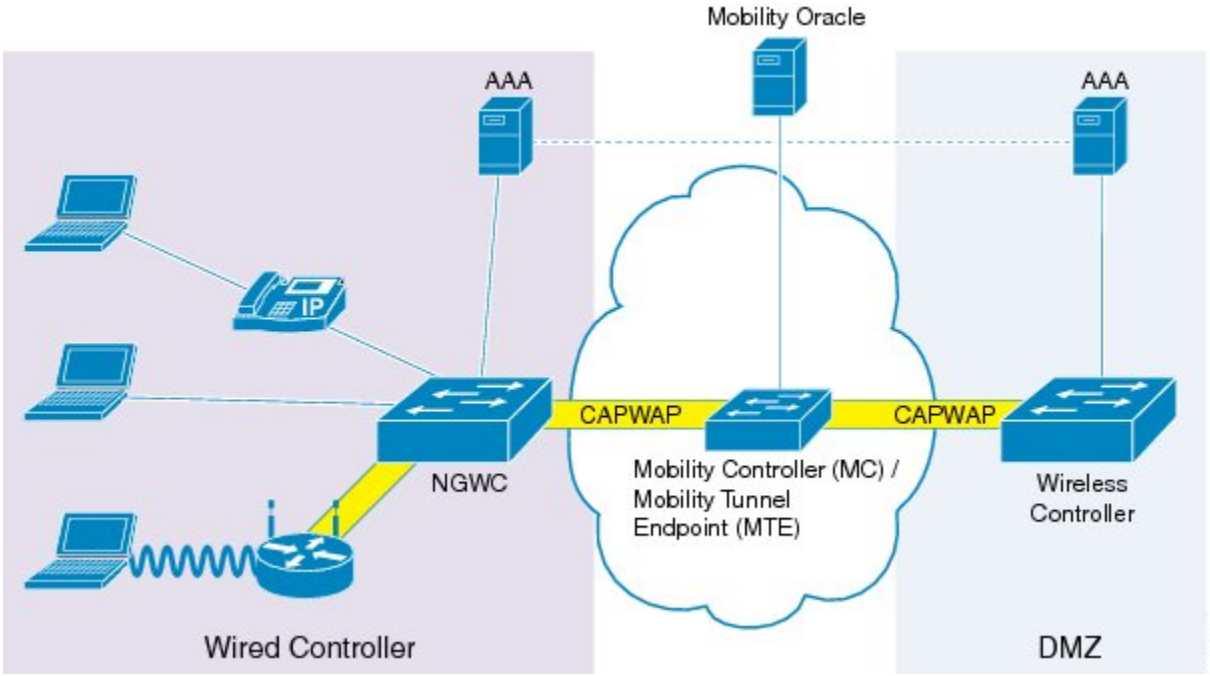
スからのゲスト トラフィックは、一般に Control And Provisioning of Wireless Access Points（CAPWAP）トンネルを経由して、非武装地帯（DMZ）にある一連のコントローラに転送されます。ここでは、Web認証アクセスまたはオープン アクセスのいずれかが提供されます。 有線のゲストトラフィックも、総称ルーティング カプセル化（GRE）のような従来からあるトンネリング メカニズムを使用して、DMZ にバックホールすることができます。 有線およびワイヤレスのアクセスが統合化された Cisco Next Generation Wiring Closet（NGWC）プラットフォームは、CAPWAP トンネリングを有線ゲストに拡張することもできます。これにより、コントローラ プラットフォーム（DMZ 内の）におけるほぼ同様の処理が可能になり、プロビジョニング オーバーヘッドを軽減することができます。

ただし、認証前に有線クライアントがゲストなのか、社内ネットワークへのアクセス権が必要なのかを判断できないため、セキュリティは引き続き問題となります。 したがって、クライアントがゲストであることが分かっている場合、DMZに有線クライアントのトラフィックをトンネリングするという決定はできません。

有線クライアントはネットワーク選択の余地がないため、ゲスト トンネリングではオープン モードはサポートされません。 オープン モードでは、クライアントがアクセス スイッチに接続すると即座に IP アドレスが割り当てられます。 クライアントがトンネル経由で接続されると、Web認証を試行するには、クライアントに DMZ でプロビジョニングされたサブネットから IP アドレスが再割り当てされている必要があります。

統合されたゲスト アクセス ソリューション

図 *3* : 統合されたゲスト アクセス ソリューション



上の図では、Cisco Next Generation Wiring Closet（NGWC）デバイスが、有線、ワイヤレスの両方のセッションの接続ポイントを形成し、適用可能な場合はレイヤ 2 認証を提供します。 モビリティ エージェント（外部デバイス）の有線セッションのゲストはControl And Provisioning of Wireless Access Points（CAPWAP）トンネルを経由して、非武装地帯（DMZ）内のワイヤレス コントローラ（アンカーデバイス）に誘導されます。 有線セッションのゲストには、ワイヤレス コントローラからオープン アクセスまたは Web 認証アクセスが提供されます。 この方法では、HTTP トラフィックを管理し、Web ページを提供するためにプロビジョニングされるネットワーク デバイスが 1 つのみであるため、ゲスト アクセスの管理が簡単になります。

有線ゲスト トラフィックから DMZ へのトンネルを使用することにより、同じコントローラ プラットフォームが Web 認証またはオープン アクセスを有線ゲストにも提供できるため、ゲスト アクセスの管理がさらに簡単になり、エンド ユーザの一貫したエクスペリエンスが保証されます。 CAPWAP トンネルをアクティブ化するには、外部デバイスとアンカー デバイスで一致するゲスト LAN プロファイルが設定されている必要があります。

認証、許可、およびアカウンティング（AAA）サービスは、レイヤ 2 認証のアクセス レイヤで必要です。また、このサービスは、オプションで有線クライアントに対するトンネルを開くようデバイスを誘導するためにも必要です。 DMZ は、クライアントのゲスト認証に AAA を使用します。 モビリティ コントローラ/モビリティ トンネル エンドポイント（MC/MTE）を使用すると、DMZ への CAPWAP トンネルを、一連のワイヤレス コントローラ間で負荷分散することができます。

CAPWAP トンネリング

有線ゲスト アクセスのエンタープライズ エッジ（eEdge）の実装では、Control And Provisioning of Wireless Access Points（CAPWAP）トンネルが Enterprise Policy Manager（EPM）プラグインとして実装されます。

トンネルがユーザ プロファイルまたはサービス テンプレート内で指定されている場合は、EPM が CAPWAP トンネルを呼び出します。 EPM は、ワイヤレス コントローラ モジュール（WCM）が、EPMがインストールされているセッションのCAPWAPトンネルを確立するよう要求します。WCMが、エラーを返すか、任意の後続のポイントでの非請求のトンネルの終了を示すと、CAPWAP トンネルは EPM の失敗を通知します。 この障害はセッション マネージャでの認証の失敗イベントが原因であり、制御ポリシー ルールを指定して、障害処理の方法を決定することができます。

セッション マネージャは eEdge フレームワークでの有線セッションの作成と管理について責任を負います。 セッション マネージャは、セッション作成で audit-session-id を割り当て、データベースのセッション エントリにクライアント ID データを保存します。 また、接続エンドポイントの認証（認証が制御ポリシーで指定されている）も管理します。

要件に基づき、WCM は、NGWC スイッチでの有線クライアントの CAPWAP トンネリングの責任を負います。 WCM も、コントローラで、トンネリングされたワイヤレスおよび有線のゲスト セッションを同様に処理します。

（注） 新しいトンネルは、アクセス スイッチと関連コントローラの間にトンネルがない場合にのみ確立されます。 トンネルがある場合、クライアントはそのトンネルに追加されます。

（注） ユーザ プロファイルを使用して CAPWAP トンネリングをアクティブ化するベンダー固有属性（VSA）は、「subscriber:capwap-tunnel-profile-name= name」です。

有線ゲスト アクセスの設定方法

ゲスト LAN の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **guest-lan** *profile-name* [*lan-id*]
4. シャットダウン
5. **client** {**association limit** [*max-connections*] | **vlan** [*vlan-id*]}
6. **security web-auth** [**parameter-map** *parameter-name*]
7. **mobility anchor** [*ip-address* | *mac-address*]
8. **no shutdown**
9. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**guest-lan** *profile-name* [*lan-id*] 例： `Device(config)# guest-lan guest-lan-name 1`	ワイヤレス ゲスト LAN ネットワークを設定し、ゲスト LAN のコンフィギュレーション モードを開始します。
ステップ 4	シャットダウン 例： `Device(config-guest-lan)# shutdown`	ゲスト LAN をディセーブルにします。

	コマンドまたはアクション	目的
ステップ 5	**client** {**association limit** [*max-connections*] | **vlan** [*vlan-id*]} 例： `Device(config-guest-lan)# client vlan VLAN100`	クライアントに対してゲスト LAN をイネーブルにします。
ステップ 6	**security web-auth** [**parameter-map** *parameter-name*] 例： `Device(config-guest-lan)# security web-auth`	ゲスト LAN のセキュリティ ポリシーを設定します。
ステップ 7	**mobility anchor** [*ip-address* | *mac-address*] 例： `Device(config-guest-lan)# mobility anchor`	ゲスト LAN のモビリティを設定します。
ステップ 8	**no shutdown** 例： `Device(config-guest-lan)# no shutdown`	ゲスト LAN をイネーブルにします。
ステップ 9	**end** 例： `Device(config-guest-lan)# end`	ゲスト LAN のコンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

サービス テンプレートでの CAPWAP トンネルの設定

サービス テンプレートで Control And Provisioning of Wireless Access Points（CAPWAP）トンネルを設定するには、次の作業を実行します。 レイヤ 2 認証の失敗が発生した場合にトンネル サービスをアクティブ化するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **service-template** *template-name*
4. **tunnel type capwap name** *tunnel-name*
5. **exit**
6. **policy-map type control subscriber** *control-policy-name*
7. **event session-started** [**match-all** | **match-any**]
8. *priority-number* **class** {*control-class-name* | **always**} [**do-all** | **do-until-failure** | **do-until-success**]
9. *action-number* **authenticate using** {**dot1x** | **mab** | **webauth**}
10. **exit**
11. **exit**
12. **event authentication-failure** [**match-all** | **match-any**]
13. *priority-number* **class** {*control-class-name* | **always**} [**do-all** | **do-until-failure** | **do-until-success**]
14. *action-number* **activate** {**policy type control subscriber** *control-policy-name* | **service-template** *template-name* [**aaa-list** *list-name*] [**precedence** [**replace-all**]]}
15. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**service-template** *template-name* 例： `Device(config)# service-template GUEST-TUNNEL`	加入者セッションに適用する一連のサービス ポリシー属性が含まれるテンプレートを定義して、サービステンプレート コンフィギュレーション モードを開始します。
ステップ 4	**tunnel type capwap name** *tunnel-name* 例： `Device(config-service-template)# tunnel type capwap name TUNNEL-CAPWAP`	サービス テンプレートで CAPWAP トンネルを設定します。

	コマンドまたはアクション	目的
ステップ 5	**exit** 例： `Device(config-service-template)# exit`	サービス テンプレート コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 6	**policy-map type control subscriber** *control-policy-name* 例： `Device(config)# policy-map type control subscriber TUNNELLED-GUEST`	加入者セッションに対して制御ポリシーを定義し、制御ポリシーマップイベントのコンフィギュレーションモードを開始します。
ステップ 7	**event session-started** [**match-all** | **match-any**] 例： `Device(config-event-control-policymap)# event seesion-started`	すべての認証イベントが match であり、制御ポリシーマップ クラスのコンフィギュレーション モードが開始された場合に、制御ポリシーの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。
ステップ 8	*priority-number* **class** {*control-class-name* | **always**} [**do-all** | **do-until-failure** | **do-until-success**] 例： `Device(config-class-control-policymap)# 1 class always`	アクションの 1 つが失敗し、制御ポリシーマップ アクションのコンフィギュレーションモードが開始されるまで、制御クラスが制御ポリシー内のアクションを指定された順序で実行するように指定します。
ステップ 9	*action-number* **authenticate using** {**dot1x** | **mab** | **webauth**} 例： `Device(config-action-control-policymap)# 1 authenticate using dot1x`	加入者セッションの制御ポリシーを認証します。
ステップ 10	**exit** 例： `Device(config-action-control-policymap)# exit`	制御ポリシーマップアクションのコンフィギュレーション モードを終了し、制御ポリシーマップ クラスのコンフィギュレーション モードを開始します。
ステップ 11	**exit** 例： `Device(config-class-control-policymap)# exit`	制御ポリシーマップ クラスのコンフィギュレーション モードを終了し、制御ポリシーマップ イベントのコンフィギュレーション モードを開始します。
ステップ 12	**event authentication-failure** [**match-all** | **match-any**] 例： `Device(config-event-control-policymap)# event authentication-failure`	すべての認証イベントが match であり、制御ポリシーマップ クラスのコンフィギュレーション モードが開始された場合に、制御ポリシーの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。

	コマンドまたはアクション	目的
ステップ 13	*priority-number* **class** {*control-class-name* | **always**} [**do-all** | **do-until-failure** | **do-until-success**] 例： `Device(config-class-control-policymap)# 1 class DOT1X-NO-RESP`	アクションの 1 つが失敗し、制御ポリシーマップ アクションのコンフィギュレーション モードが開始されるまで、制御クラスが制御ポリシー内のアクションを指定された順序で実行するように指定します。
ステップ 14	*action-number* **activate** {**policy type control subscriber** *control-policy-name* | **service-template** *template-name* [**aaa-list** *list-name*] [**precedence** [**replace-all**]]} 例： `Device(config-action-control-policymap)# 1 activate service-template GUEST-TUNNEL`	加入者セッションのコントロールポリシーをアクティブ化します。
ステップ 15	**end** 例： `Device(config-action-control-policymap)# end`	制御ポリシーマップアクションのコンフィギュレーション モードを終了し、特権 EXEC モードへ戻ります。

CAPWAP フォワーディングの設定

CAPWAP フォワーディング用に特定の VLAN を設定するには、次の作業を実行します。 設定すると、この VLAN は CAPWAP フォワーディングのみに使用できるようになります。

手順の概要

1. **enable**
2. **configure terminal**
3. **vlan** *vlan-id*
4. **exit**
5. **access-session tunnel vlan** *vlan-id*
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vlan** *vlan-id* 例： `Device(config)# vlan 1755`	VLAN を設定し、VLAN コンフィギュレーション モードを開始します。
ステップ 4	**exit** 例： `Device(config-vlan)# exit`	VLAN コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 5	**access-session tunnel vlan** *vlan-id* 例： `Device(config)# access-session tunnel vlan 1755`	指定されたトンネルに対して VLAN アクセス セッションを設定します。 （注） このコマンドを使用する前に、**vlan** *vlan-id* コマンドを使用して VLAN を設定します。
ステップ 6	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

有線ゲスト アクセスの設定例

例：サービス テンプレートでの CAPWAP トンネルの設定

次の例は、有線ゲスト アクセスをイネーブルにするサービス テンプレートで CAPWAP トンネルを設定する方法を示しています。

```
Device> enable
Device# configure terminal
Device(config)# service-template GUEST-TUNNEL
Device(config-service-template)# tunnel type capwap name TUNNEL-CAPWAP
Device(config-service-template)# exit
Device(config)# policy-map type control subscriber TUNNELLED-GUEST
Device(config-event-control-policymap)# event seesion-started
Device(config-class-control-policymap)# 1 class always
```

```
Device(config-action-control-policymap)# 1 authenticate using dot1x
Device(config-action-control-policymap)# exit
Device(config-class-control-policymap)# 1 class DOT1X-NO-RESP
Device(config-action-control-policymap)# 1 activate service-template GUEST-TUNNEL
Device(config-action-control-policymap)# end
```

例：モビリティ エージェントの設定

次の例は、モビリティエージェント（アンカー）のインターフェイスポートを設定する方法を示します。

有線ゲスト アクセス ポートはまず、レイヤ 2 アクセス スイッチ上で、または有線ゲスト アクセス トラフィック用のVLANインターフェイスで設定されているスイッチポート上で終端します。有線ゲスト トラフィックはその後、アクセス スイッチからコントローラへトランクされます。このコントローラは、アクセス スイッチ上で有線ゲスト アクセス VLAN にマップされているインターフェイスを使用して設定されます。

```
!
interface GigabitEthernet1/0/44
 description Connected to Client_Laptop
 switchport access vlan 10
 switchport mode access
 access-session host-mode single-host
 access-session closed
 access-session port-control auto
 access-session control-direction in
 mab
 dot1x pae authenticator
 dot1x timeout tx-period 5
 service-policy type control subscriber Guest-Access
!
interface GigabitEthernet1/0/1
 description Connected_to_MobilityController
 switchport mode trunk
!
interface Vlan10
 description CLIENT-VLAN
 ip address 172.16.10.201 255.255.255.0
 ip helper-address 172.16.10.200
!
interface Vlan80
 description MANAGEMENT-VLAN
 ip address 10.20.1.1 255.255.255.0
!
wireless management interface Vlan80
wireless mobility controller ip 10.20.1.2 public-ip 10.20.1.2 << Mobility Controller IP >>
!
guest-lan glan-1 1
 shutdown
 client vlan Vlan10
 no security web-auth << Use "security webauth" for webauth access & "no security webauth"
 for open access. >>
 mobility anchor 10.20.1.3 << Guest Controller IP >>
 no shutdown
!
```

例：モビリティ コントローラの設定

次の例は、有線ゲストアクセスをイネーブルにするモビリティコントローラで、インターフェイス ポートおよびワイヤレス モビリティを設定する方法を示しています。

```
!
interface TenGigabitEthernet1/0/2
 description Connected-to-MobilityAgent
 switchport mode trunk
!
interface TenGigabitEthernet1/0/1
 description Connected-to-GuestController
 switchport mode trunk
!
interface Vlan80
 description MANAGEMENT-VLAN
 ip address 10.20.1.2 255.255.255.0
!
wireless management interface Vlan80
!
wireless mobility controller peer-group pg-name
wireless mobility controller peer-group pg-name member ip 10.20.1.1 public-ip 10.20.1.1 <<
 Mobility Agent IP >>
!
wireless mobility group member ip 10.20.1.3 public-ip 10.20.1.3 << Guest Controller IP >>
wireless mobility group name mcg-name
!
```

例：ゲスト コントローラの設定

次の例は、ゲストコントローラ（アンカー）でインターフェイスポートを設定する方法と、DHCP スヌーピングをセットアップする方法について示しています。

ゲスト（ローカルWLAN）コントローラは、有線およびワイヤレスのゲストアクセス用に設定された、非武装地帯（DMZ）のアンカー WLAN コントローラにクライアントをアンカーします。クライアントから DMZ アンカー コントローラへのハンドオフが成功すると、DHCP IP アドレスの割り当て、クライアント認証などが、DMZ Cisco ワイヤレス LAN コントローラ（WLC）で処理されます。 WLC が認証を完了すると、クライアントはトラフィックの送受信を行うことができるようになります。

```
!
interface TenGigabitEthernet1/0/1
 description Connected_to_MC
 switchport mode trunk
!
interface Vlan10
 description CLIENT-VLAN
 ip address 172.16.10.200 255.255.255.0
!
interface Vlan80
 description MANAGEMENT-VLAN
 ip address 10.20.1.3 255.255.255.0
!
ip dhcp snooping vlan 10
ip dhcp snooping
ip dhcp excluded-address 172.16.10.100 172.16.10.255
ip dhcp pool vlan10
 network 172.16.10.0 255.255.255.0
 default-router 172.16.10.200
!
wireless management interface Vlan80
!
```

```
wireless mobility group name mcg-name
wireless mobility group member ip 10.20.1.2 public-ip 10.20.1.2 << Mobility Controller IP
>>
!
guest-lan glan-1 1
 shutdown
 client vlan Vlan10
 no security web-auth << Use "security web-auth" for web-auth access & "no security web-auth"
 for open access. >>
 mobility anchor
 no shutdown
!
```

例：CAPWAP フォワーディングの設定

```
Device> enable
Device# configure terminal
Device(config)# vlan 1755
Device(config-vlan)# exit
Device(config)# access-session tunnel vlan 1775
Device(config)# end
```

有線ゲスト アクセスに関するその他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
Cisco Identity-Based Networking Services コマンド	『Cisco IOS Identity-Based Networking Services Command Reference』

標準および RFC

RFC	Title
IEEE 802.1X	『*Port Based Network Access Control*』

テクニカル サポート

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

有線ゲスト アクセスの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェアリリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *8*：有線ゲスト アクセスの機能情報

機能名	リリース	機能情報
有線ゲスト アクセス	Cisco IOS XE Release 3.3SE	有線ゲスト アクセス機能は、有線およびワイヤレスの両方のアクセスをサポートしている企業ネットワークのゲスト ユーザに対して、有線のイーサネット接続からのゲストアクセスネットワークへの接続を可能にします。有線のイーサネット接続はゲスト アクセスに対して指定および設定されます。 モビリティ エージェントの有線セッションのゲストは、Control And Provisioning of Wireless Access Points（CAPWAP）トンネル経由で、非武装地帯（DMZ）のワイヤレス ゲスト コントローラに誘導されます。 導入または変更されたコマンド：**access-session tunnel vlan**、**event**、**match authorization-failure**、 **tunnel type capwap**。