



MAC 認証バイパス

MAC 認証バイパス機能とは、クライアントの MAC アドレスを使用してネットワークのクライアントを Cisco Identity Based Networking Services (IBNS) およびネットワーク アドミッションコントロール (NAC) の戦略と統合できる、MAC アドレスベースの認証メカニズムです。MAC 認証バイパス機能は、次のネットワーク環境に適用できます。

- 特定のクライアント プラットフォームにサブリカント コードを使用できないネットワーク環境。
- エンドクライアント設定が管理コントロールを受けていないネットワーク環境、つまり IEEE 802.1X 要求がサポートされていないネットワーク環境。
- [機能情報の確認 \(1 ページ\)](#)
- [MAC 認証バイパス設定の前提条件 \(2 ページ\)](#)
- [MAC 認証バイパスに関する情報 \(2 ページ\)](#)
- [MAC 認証バイパスの設定方法 \(4 ページ\)](#)
- [MAC 認証バイパスの設定例 \(9 ページ\)](#)
- [MAC 認証バイパスに関するその他の参考資料 \(10 ページ\)](#)
- [MAC 認証バイパスの機能情報 \(11 ページ\)](#)

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、使用するプラットフォームおよびソフトウェア リリースの [Bug Search Tool](#) およびリリース 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検索し、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場合は、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](#) には、<http://www.cisco.com/go/cfn> からアクセスします。[Cisco.com](#) のアカウントは必要ありません。

MAC 認証バイパス設定の前提条件

IEEE 802.1x : ポートベースのネットワーク アクセス コントロール

ポートベースのネットワーク アクセス コントロールの概念とシスコのプラットフォーム上のポートベースのネットワーク アクセス コントロールの設定方法を理解しておく必要があります。

RADIUS および ACL

RADIUS プロトコルの概念とアクセス コントロール リスト (ACL) の作成および適用方法を理解しておく必要があります。詳細については、シスコのプラットフォームのマニュアル、および『*Securing User Services Configuration Guide Library*』を参照してください。

デバイスが RADIUS 設定されていること、および Cisco Secure アクセス コントロール サーバ (ACS) に接続されていることが必要です。詳細については、『*User Guide for Secure ACS Appliance 3.2*』を参照してください。

MAC 認証バイパスに関する情報

Cisco IOS Auth Manager の概要

指定されたネットワークに接続するデバイスの機能は異なっている可能性があるため、ネットワークはさまざまな認証方式および認証ポリシーをサポートする必要があります。Cisco IOS Auth Manager は、認証方法に関係なく、ネットワーク認証要求を処理し、認可ポリシーを強制します。Auth Manager は、すべてのポートベースのネットワーク接続試行、認証、認可、および接続解除に対する運用データを維持することで、セッションマネージャとして機能します。

Auth Manager セッションには、次のような状態が考えられます。

- Idle : idle 状態では、認証セッションは初期化されていますが、実行されている方式はありません。これは中間の状態です。
- Running : 現在、方式が実行されています。これは中間の状態です。
- Authc Success : 認証方式の実行に成功しました。これは中間の状態です。
- Authc Failed : 認証方式が失敗しました。これは中間の状態です。
- Authz Success : このセッションに対するすべての機能の適用に成功しました。これは最終的な状態です。
- Authz Failed : このセッションに対して、少なくとも1つの機能の適用に失敗しました。これは最終的な状態です。
- 方法なし : このセッションに関する結果はありませんでした。これは最終的な状態です。

設定可能 MAB ユーザ名およびパスワードの概要

MAC 認証バイパス (MAB) 動作には、ユーザ名とパスワードの両方の属性を持つ RADIUS Access-Request パケットを使用した認証が含まれます。デフォルトでは、ユーザ名とパスワードの値は同じであり、MAC アドレスを含んでいます。設定可能 MAB ユーザ名およびパスワード機能により、次のシナリオで、ユーザ名とパスワードの両方の属性を設定することができます。

- フォーマットされたユーザ名属性を使用する既存の大規模データベース向けに MAB を有効化するには、クライアント MAC のユーザ名形式を設定する必要があります。ユーザ名の形式を設定するには `mab request format attribute 1 mab request format attribute 1` コマンドを使用します。
- 一部のデータベースは、ユーザ名とパスワードの値が同じである場合には、認証を受け入れません。そのような場合は、ユーザ名とは確実に異なる値になるようパスワードを設定する必要があります。パスワードを設定するには `mab request format attribute 2 mab request format attribute 2` コマンドを使用します。

設定可能 MAB ユーザ名およびパスワード機能では、Cisco IOS 認証マネージャと既存の MAC データベースおよび RADIUS サーバ間での相互運用が可能です。パスワードはグローバルパスワードなので、すべての MAB 認証およびインターフェイスで共通です。また、このパスワードはすべてのスーパーバイザデバイス間で同期され、それにより高可用性を実現します。

パスワードが提供または設定されていない場合、パスワードはユーザ名と同じ値になります。次の表に、ユーザ名とパスワードの形式を示します。

MAC アドレス	ユーザ名の形式 (グループのサイズ、区切り記号)	ユーザ名	設定されたパスワード	作成されたパスワード
08002b8619de	(1, :)	0:8:0:0:2:b:8:6:1:9:d:e	なし	08:0:0:2:b:8:6:1:9:de
	(1, -)	0-8-0-0-2-b-8-6-1-9-d-e		08-00-2b-86-19-de
	(1, .)	0.8.0.0.2.b.8.6.1.9.d.e		08.0.0.2.b.8.6.1.9.de
08002b8619de	(1, :)	0:8:0:0:2:b:8:6:1:9:d:e	Password	Password
	(1, -)	0-8-0-0-2-b-8-6-1-9-d-e		
	(1, .)	0.8.0.0.2.b.8.6.1.9.d.e		
08002b8619de	(2, :)	08:00:2b:86:19:de	なし	08:00:2b:86:19:de
	(2, -)	08-00-2b-86-19-de		08-00-2b-86-19-de
	(2, .)	08.00.2b.86.19.de		08.00.2b.86.19.de

MAC アドレス	ユーザ名の形式 (グループのサイズ、区切り記号)	ユーザ名	設定されたパスワード	作成されたパスワード
08002b8619de	(2, :) (2, -) (2, .)	08:00:2b:86:19:de 08-00-2b-86-19-de 08.00.2b.86.19.de	Password	Password
08002b8619de	(4, :) (4, -) (4, .)	0800:2b86:19de 0800-2b86-19de 0800.2b86.19de	なし	0800:2b86:19de 0800-2b86-19de 0800.2b86.19de
08002b8619de	(4, :) (4, -) (4, .)	0800:2b86:19de 0800-2b86-19de 0800.2b86.19de	Password	Password
08002b8619de	(12, <該当なし >)	08002b8619de	なし	08002b8619de
08002b8619de	(12, <該当なし >)	08002b8619de	Password	Password

MAC 認証バイパスの設定方法

MAC 認証バイパスのイネーブル化

802.1X ポートで MAC 認証バイパス機能を有効にするには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface type slot / port**
4. **mab**
5. **end**
6. **show authentication sessions interface type slot / port 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 slot / port 例： Device(config)# interface Gigabitethernet 1/2/1	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	mab 例： Device(config-if)# mab	MAB をイネーブルにします。
ステップ 5	end 例： Device(config-if)# end	特権 EXEC モードに戻ります。
ステップ 6	show authentication sessions interface type slot / port details 例： Device# show authentication session interface Gigabitethernet 1/2/1 details	インターフェイスの設定と、インターフェイス上のオーセンティケータ インスタンスを表示します。

ポート上の再認証の有効化

デフォルトでは、ポートは自動的に再認証されません。自動再認証をイネーブルにし、再認証の頻度を指定できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface type slot / port**
4. **switchport**
5. **switchport mode access**

6. **authenticationport-control auto**
7. **mab [cap]**
8. **authentication periodic**
9. **authenticationtimerreauthenticate{seconds | server}**
10. **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	interface type slot / port 例： Device(config)# interface Gigabitethernet 1/2/1	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	switchport 例： Device(config-if)# switchport	インターフェイスをレイヤ 2 スイッチド モードに設定します。
ステップ 5	switchport mode access 例： Device(config-if)# switchport mode access	インターフェイスのタイプを、非ランキング、タグなし、シングル VLAN レイヤ 2 インターフェイスに設定します。
ステップ 6	authenticationport-control auto 例： Device(config-if)# authentication port-control auto	ポートの認証ステータスを設定します。
ステップ 7	mab [cap] 例： Device(config-if)# mab	MAB をイネーブルにします。
ステップ 8	authentication periodic 例：	再認証をイネーブルにします。

	コマンドまたはアクション	目的
	Device(config-if)# authentication periodic	
ステップ 9	authenticationtimerreauthenticate {seconds server} 例 : Device(config-if)# authentication timer reauthenticate 900	再認証の間隔（秒単位）を設定します。
ステップ 10	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。

セキュリティ違反モードの指定

ポート上でセキュリティ違反がある場合、ポートをシャットダウンするか、トラフィックを制限できます。デフォルトでは、ポートはシャットダウンされます。ポートをシャットダウンする一定の時間を設定できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type slot / port*
4. **switchport**
5. **switchport mode access**
6. **authenticationport-control auto**
7. **mab** [eap]
8. **authenticationviolation** {restrict | shutdown}
9. **authenticationtimerrestart** *seconds*
10. **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。 <ul style="list-style-type: none"> • 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	interface type slot / port 例： Device(config)# interface Gigabitethernet 1/2/1	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	switchport 例： Device(config-if)# switchport	インターフェイスをレイヤ 2 スイッチド モードに設定します。
ステップ 5	switchport mode access 例： Device(config-if)# switchport mode access	インターフェイスのタイプを、非トランキング、タグなし、シングル VLAN レイヤ 2 インターフェイスに設定します。
ステップ 6	authenticationport-control auto 例： Device(config-if)# authentication port-control auto	ポートの認証ステータスを設定します。
ステップ 7	mab [cap] 例： Device(config-if)# mab	MAB をイネーブルにします。
ステップ 8	authenticationviolation {restrict shutdown} 例： Device(config-if)# authentication violation shutdown	ポート上でセキュリティ違反が生じた場合に取りうるアクションを設定します。
ステップ 9	authenticationtimerrestart seconds 例： Device(config-if)# authentication timer restart 30	未認証のポートの認証の間隔 (秒単位) を設定します。
ステップ 10	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。

設定可能 MAB ユーザ名およびパスワードの有効化

手順の概要

1. `enable`
2. `configure terminal`
3. `mab request format attribute 1 groupsize {1 | 2 | 4 | 12} separator {- | : | .} [lowercase | uppercase]`
4. `mab request format attribute 2 [0 | 7] password`
5. `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	<code>enable</code> 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	<code>configure terminal</code> 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	<code>mab request format attribute 1 groupsize {1 2 4 12} separator {- : .} [lowercase uppercase]</code> 例： Device(config)# mab request format attribute 1 groupsize 2 separator :	MAB 要求のユーザ名形式を設定します。
ステップ 4	<code>mab request format attribute 2 [0 7] password</code> 例： Device(config)# mab request format attribute 2 password1	すべての MAB 要求に適用されるグローバル パスワードを設定します。
ステップ 5	<code>end</code> 例： Device(config)# end	特権 EXEC モードに戻ります。

MAC 認証バイパスの設定例

例：MAC 認証バイパスの設定

次の例では、指定したインターフェイスで MAC 認証バイパス（MAB）機能を有効にするために、`mab` コマンドが設定されています。オプションとして、インターフェイス コンフィギュ

レーションおよびインターフェイス上の認証インスタンスを表示するための **show authentication sessions** コマンドが有効化されています。

```
Device> enable
Device# configure terminal
Device(config)# interface GigabitEthernet2/1
Device(config-if)# mab
Device(config-if)# end
Device# show authentication sessions interface GigabitEthernet2/1 details
```

例：設定可能 MAB ユーザ名およびパスワードの有効化

次の例は、MAC 認証バイパス (MAB) のユーザ名形式とパスワードを設定する方法を示しています。この例では、ユーザ名形式は区切り記号のない 12 桁の 16 進数として設定され、グローバルパスワードは **password1** と設定されます。

```
Device> enable
Device# configure terminal
Device(config)# mab request format attribute 1 groupsize 2 separator :
Device(config)# mab request format attribute 2 password1
Device(config)# end
```

MAC 認証バイパスに関するその他の参考資料

関連資料

関連項目	マニュアルタイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
認証コマンド	<ul style="list-style-type: none"> • 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』

MIB

MIB	MIB のリンク
<ul style="list-style-type: none"> • CISCO-AUTH-FRAMEWORK-MIB • CISCO-MAC-AUTH-BYPASS-MIB • CISCO-PAE-MIB • IEEE8021-PAE-MIB 	選択したプラットフォーム、Cisco IOS ソフトウェアリリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	Title
RFC 3580	「IEEE 802.1x Remote Authentication Dial In User Service (RADIUS)」

シスコのテクニカル 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

MAC 認証バイパスの機能情報

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、ソフトウェア リリース トレーンで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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

表 1: MAC 認証バイパスの機能情報

機能名	リリース	機能情報
MAC 認証バイパス (MAB)	Cisco IOS XE 3.2SE Cisco IOS XE 3.3SE Cisco IOS XE 3.5E Cisco IOS 15.2(1)E	MAC 認証バイパス機能とは、クライアントの MAC アドレスを使用してネットワークのクライアントを Cisco IBNS および NAC の戦略と統合できる、MAC アドレスベースの認証メカニズムです。 次のコマンドが導入または変更されました。 dot1xmac-auth-bypass 、 showdot1xinterface
設定可能 MAB ユーザ名 およびパスワード	Cisco IOS 15.2(1)E	設定可能 MAB ユーザ名およびパスワード機能では、MAC 認証バイパス (MAB) のユーザ名形式とパスワードを設定することにより、Cisco IOS 認証マネージャと既存の MAC データベースおよび RADIUS サーバ間での相互運用性を実現できます。 次のコマンドが導入または変更されました。 mab request format attribute 1 、 mab request format attribute 2