# 外部ワイヤレスLANコントローラのWeb認証の 設定

内容	
<u>はじめに</u>	
<u>前提条件</u>	
<u>要件</u>	
<u>使用するコンポーネント</u>	
表記法	
web 認証	
<u>······ was</u> Web 認証プロセス	
<u>内部 Web 認証用の WLC の設定</u>	
<u>WLAN インスタンスの追加</u>	
Web 認証でユーザを認証する 3 とおりの方法	
<u>NOS の設定</u> Cisco WLC への RADIUS サーバ情報の入力	
 RADIUSサーバを使用したWLANの設定	
<u>ACS の確認</u>	
<u>LDAP サーバ</u>	
<u>Web 認証を使用するための WLAN クライアントの設定</u>	
<u>クライアントの設定</u>	
<u>クライアントログイン</u>	
Web 認証のトラブルシューティング	
ACS のトラブルシューティング	
<u>IPv6 ブリッジングでの Web 認証</u>	
<u>関連情報</u>	

# はじめに

このドキュメントでは、内部Web認証をサポートするようにCisco 4400シリーズワイヤレス LAN(WLAN)コントローラ(WLC)を設定する方法について説明します。

# 前提条件

#### 要件

4400 WLCを初期設定することをお勧めします。

#### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- ・ バージョン 7.0.116.0 が稼働している 4400 シリーズ WLC
- Microsoft® Windows 2003 Server にインストールされている Cisco Secure Access Control Server (ACS) バージョン 4.2
- ・ Cisco Aironet 1131AG シリーズ Lightweight アクセス ポイント
- バージョン 4.0 が稼働する Cisco Aironet 802.11 a/b/g CardBus ワイヤレス アダプタ

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始していま す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認して ください。

#### 表記法

ドキュメント表記の詳細は、『<u>テクニカルティップスのフォーマット表記法の使用とその他のコ</u> <u>ンテンツ</u>』を参照してください。

### Web 認証

Web認証は、有効なユーザ名とパスワードが正しく入力されるまで、特定のクライアントからの IPトラフィック(DHCPおよびDNS関連のパケットを除く)をコントローラで許可しないように するレイヤ3セキュリティ機能です。これは、サプリカントやクライアント ユーティリティを必 要としない簡単な認証方式です。一般に、Web 認証はゲスト アクセス ネットワークを展開する 場合に使用されます。一般的な導入には、T-Mobile®やStarbucks®が提供するような「ホットス ポット」の場所が含まれます。

Web 認証はデータ暗号化を提供しないことを注意してください。Web認証は、接続性だけが問題 となるホットスポットまたはキャンパス環境での単純なゲストアクセスとして使用されます。

Web認証は次のコマンドを使用して実行できます。

- WLCのデフォルトログインウィンドウ
- WLCのデフォルトログインウィンドウの変更バージョン
- 外部Webサーバで設定するカスタマイズされたログインウィンドウ(外部Web認証)
- コントローラにダウンロードするカスタマイズされたログインウィンドウ

このマニュアルでは、内部 Web 認証用のワイヤレス LAN コントローラが設定されています。

# Web 認証プロセス

ユーザが Web 認証用に設定された WLAN に接続する場合は、次のようになります。

- ユーザは、Web ブラウザを開き、URL として、たとえば、http://www.cisco.com を入力します。クライアントは、宛先の IP を取得するため、この URL の DNS 要求を送信します。WLC は DNS サーバに DNS 要求をバイパスし、DNS サーバは宛先 www.cisco.com の IP アドレスを含む DNS 応答で返答します。次にこれがワイヤレス クライアントに転送されます。
- 続いて、クライアントは宛先 IP アドレスを使用して TCP 接続を開始しようとします。
   www.cisco.com の IP アドレスを宛先とする TCP SYN パケットが送信されます。
- WLC にはクライアント用に設定されたルールがあるため、www.cisco.com のプロキシとし て機能します。WLC は、www.cisco.com の IP アドレスを送信元とする TCP SYN-ACK パ ケットをクライアントに戻します。クライアントは、3 ウェイ TCP ハンドシェイクを完了 するために、TCP ACK パケットを返し、TCP 接続が完全に確立されます。
- クライアントは、宛先が www.cisco.com である HTTP GET パケットを送信します。WLC はこのパケットをインターセプトして、リダイレクト処理用に送信します。HTTP アプリケ ーション ゲートウェイは、HTML 本文を準備し、クライアントから要求された HTTP GET への応答として返します。この HTML により、クライアントは WLC のデフォルト Web ペ ージの URL(たとえば、http://<Virtual-Server-IP>/login.html.)に転送されます。
- ・ クライアントは、たとえば、www.cisco.com などの IP アドレスとの TCP 接続を閉じます。
- ここで、クライアントが http://10.1.1.1/login.html に移動したいとします。そのため、クラ イアントは WLC の仮想 IP アドレスとの TCP 接続を開こうとします。WLC に 10.1.1.1 の TCP SYN パケットを送信します。
- WLC は TCP SYN-ACK で返答し、クライアントはハンドシェイクを完了するために、TCP ACK を WLC に戻します。
- クライアントは、ログインページを要求するために、10.1.1.1を宛先とする、/login.htmlの HTTP GETを送信します。
- この要求はWLCのWebサーバで許可され、サーバはデフォルトログインページで応答します。クライアントは、ユーザがログインできるログインページをブラウザウィンドウで受け取ります。

Web認証プロセスの説明については、『<u>CiscoワイヤレスLANコントローラ(WLC)でのWeb認証</u>』 を参照してください。

### ネットワーク構成

このドキュメントでは、次のネットワーク セットアップを使用します。



ネットワーク構成

Web 認証用のコントローラの設定

このドキュメントでは、WLAN は Web 認証用に設定され、専用 VLAN にマップされています。 以下に示すのは、Web 認証用の WLAN の設定に関係した手順です。

- 1. <u>VLAN インターフェイスの作成</u>
- 2. <u>内部 Web 認証用の WLC の設定</u>
- 3. WLAN インスタンスの追加
- 4. <u>認証タイプの設定(Web 認証でユーザを認証する 3 とおりの方法)</u>

この項では、Web認証用にコントローラを設定する方法を中心に説明します。

このドキュメントで使用する IP アドレスは次のとおりです。

• WLC の IP アドレスは 10.77.244.204 です。

• ACS サーバの IP アドレスは 10.77.244.196 です。

VLAN インターフェイスの作成

次のステップを実行します。

1. ワイヤレス LAN コントローラ GUI で、上部のメニューから [Controller] を選択し、左側の メニューから [Interfaces] を選択し、ウィンドウの右上の [New] をクリックして、新しい動 的インターフェイスを作成します。

[Interfaces] > [New] ウィンドウが表示されます。この例では、[Interface Name] には vlan90 を、[VLAN ID] には 90 をそれぞれ使用しています。

cisco	MONITOR WL	ANs		WIRELESS	SECURITY
Controller	Interfaces > N	lew			
General Inventory Interfaces Interface Groups	Interface Name	e 🔽	lan90 0		
Multicast Network Routes					
Internal DHCP Server 「インタフェース」>「新担ウィント	ミウトの順に聞く				

2. VLAN インターフェイスを作成するには、[Apply] をクリックします。

[Interfaces] > [Edit] ウィンドウが表示され、インターフェイス固有の情報を入力することが 求められます。

- 3. このドキュメントでは、次のパラメータを使用します。
  - IP アドレス: 10.10.10.2
  - ネットマスク:255.255.255.0(24 ビット)
  - ゲートウェイ: 10.10.10.1
  - ポート番号:2
  - プライマリ DHCP サーバ: 10.77.244.204

◆ 注:このパラメータは、RADIUSサーバまたはDHCPサーバのIPアドレスである 必要があります。この例では、内部 DHCP スコープが WLC 上で設定されてい 💊 るため、WLC の管理アドレスは DHCP サーバとして使用されます。

- セカンダリ DHCP サーバ: 0.0.0.0
  - 注:この例ではセカンダリDHCPサーバがないため、0.0.0.0を使用しています。 設定にセカンダリ DHCP サーバがあれば、そのサーバ IP アドレスをこのフィー ルドに追加します。
- ACL 名:なし

ululu cisco	MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT		
Controller	Interfaces > Edit	ing a descent of the second of					
General Inventory	General Informati						
Interfaces Interface Groups	Interface Name MAC Address						
Network Routes	Configuration						
<ul> <li>Internal DHCP Server</li> <li>Mobility Management Ports</li> <li>NTD</li> </ul>	Guest Lan  Quarantine Quarantine Vlan Id						
▶ CDP	Physical Information						
Advanced	Port Number Backup Port Active Port Enable Dynamic AP	2 0 Management					
	Interface Address						
	VLAN Identifier	90					
	IP Address	10.	10.10.2	1			
	Netrnask Gateway	10.	10.10.1				
	DHCP Information						
	Primary DHCP Serv Secondary DHCP Se	er 1 erver [	0.77.244.204				
	Access Control Lis	st					
	ACI: Name		006				

4. Apply をクリックして変更を保存します。

内部 Web 認証用の WLC の設定

次の手順では、内部 Web 認証用の WLC を設定します。内部 Web 認証は、WLC 上でのデフォル トの Web 認証タイプです。このパラメータが変更されていなければ、内部 Web 認証を有効にす るための設定は必要ありません。Web 認証パラメータが以前に変更されている場合には、内部 Web 認証用に WLC を設定するために、次の手順を実行します。

- 1. コントローラのGUIから、Security > Web Auth > Web Login Page の順に選択して、Web Login Pageにアクセスします。
- 2. [Web Authentication Type] ドロップダウン ボックスから、[Internal Web Authentication] を 選択します。
- 3. Redirect URL after loginフィールドに、認証が成功した後にエンドユーザがリダイレクトさ れるページのURLを入力します。

،، ،،، ،، cısco	MONITOR WLANS	CONTROLLER V	VIRELESS	SECURITY	MANAGEMENT	COMMANDS
Security	Web Login Page			- *	-	
<ul> <li>AAA</li> <li>General</li> <li>RADIUS</li> <li>Authentication</li> <li>Accounting</li> <li>Fallback</li> <li>TACACS+</li> </ul>	Web Authentication Redirect URL after In This page allows you to page. The Login page i WLAN if 'Web Authentic	Type ogin s customize the conte s presented to web us sation' is turned on (u	Inter www nt end eppe sers the first nder WLAN	mal (Default) .cisco.com orance of the time they acc Security Polici	Login cess the es),	
LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Password Policies	Cisco Logo Headline Message	€ Show	C Hide			<u>*</u>
<ul> <li>Local EAP</li> <li>Priority Order</li> <li>Certificate</li> <li>Access Control Lists</li> <li>Wireless Protection Policies</li> <li>Web Auth Web Login Page Certificate</li> <li>Advanced</li> </ul>						¥.

ログイン後のリダイレクトURL

Ջ 注:WLCバージョン5.0以降では、Web認証用のログアウトページもカスタマイズできます。

#### WLAN インスタンスの追加

内部 Web 認証が有効になっており、Web 認証専用の VLAN があるので、Web 認証ユーザをサポ

ートするために新しい WLAN/SSID を提供する必要があります。

新しい WLAN/SSID を作成するには、次の手順を実行します。

1. WLC GUI から、最上部のメニューで [WLAN] をクリックし、右上にある [New] をクリック します。

[Type] で [WLAN] を選択します。Web 認証用のプロファイル名と WLAN SSID を選択しま す。この例では、Profile NameとWLAN SSIDの両方にGuestを使用しています。

cisco	MONITOR WLANS		WIRELESS	SECURITY	MANAGEMENT	COMMANDS
WLANS WLANS Advanced	WLANs > New Type Profile Name SSID ID	WLAM Guest 1				
プロファイル名とWLAN	ISSID					

2. [APPLY] をクリックします。

新しい [WLANs] > [Edit] ウィンドウが表示されます。

MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

WLANS > Edit Gues	/LANs > I	Edit '	Guest'
-------------------	-----------	--------	--------

Profile Name	Guest
Туре	WLAN
SSID	Guest
Status	✓ Enabled
Security Policies	None (Modifications done under security tab will appear after applying the chang
Radio Policy	All
Interface/Interface Group(G)	vlan90 💌
Multicast Vlan Feature	Enabled
Broadcast SSID	Enabled

WLANs > Editウィンドウが表示されます

3. WLAN のステータス ボックスをオンにして、WLAN を有効にします。[Interface] メニュー で、以前に作成した VLAN インターフェイスの名前を選択します。この例では、インター フェイス名は vlan90 です。

💊 注:この画面の他のパラメータは、デフォルト値のままにします。

4. [Security] タブをクリックします。

次の手順を実行して、Web 認証を設定します。

- a. [Layer 2] タブをクリックして、セキュリティを [None] に設定します。
  - ◆ 注:WLANでは、Webパススルーをレイヤ3セキュリティとして802.1xを使用する ように設定したり、WPA/WPA2をレイヤ2セキュリティとして設定したりするこ とはできません。ワイヤレスLANコントローラレイヤ2およびレイヤ3セキュリテ ィの互換性については、『<u>ワイヤレスLANコントローラレイヤ2レイヤ3セキュリ</u> <u>ティの互換性マトリクス</u>』を参照してください
- b. [レイヤ3(Layer 2)] タブをクリックします[Web Policy] ボックスをオンにして、次に 示す [Authentication] オプションを選択します。

cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT
WLANS WLANS Advanced	WLANs > Edit 'Guest'  General Security QoS Advanced  Layer 2 Layer 3 AAA Servers  Layer 3 Security None  Web Policy 4  Authentication  Passthrough  Conditional Web Redirect  Splash Page Web Redirect  On MAC Filter failure44  Preauthentication ACL None  Over-ride Global Config Enable

Layer 3」タブをクリックし、Web Policyボックスにチェックマークを付けます

- c. [Apply] をクリックして、WLAN を保存します。
- d. WLAN 概要ウィンドウに戻ります。SSID ゲストの WLAN テーブルの [Security Policies] 列の下で、Web 認証が有効になっていることを確認します。

Web 認証でユーザを認証する 3 とおりの方法

Web 認証を使用する場合には、ユーザを認証する 3 とおりの方法があります。ローカル認証によって、Cisco WLC のユーザを認証することができます。さらに、外部 RADIUS サーバまたは LDAP サーバをバックエンド データベースとして使用してユーザを認証することもできます。

このドキュメントでは、3 つすべての方法での設定例を示しています。

ローカル認証

ゲストユーザのユーザデータベースは、WLCのローカルデータベースに保存されます。ユーザは 、次のデータベースに対してWLCによって認証されます。

- 1. WLC GUI で [Security] を選択します。
- 2. 左側の [AAA] メニューから [Local Net Users] をクリックします。

cisco		<u>W</u> LANs		WIRELESS	<u>SECURITY</u>	MANAGEMENT	C <u>O</u> MMANDS
Security	Local Net	Users					
<ul> <li>AAA</li> <li>General</li> <li>RADIUS</li> <li>Authentication</li> <li>Accounting</li> <li>Fallback</li> <li>TACACS+</li> <li>LOAP</li> <li>Local Net Users</li> <li>MAC Filtering</li> <li>Disabled Clients</li> <li>User Login Policies</li> <li>AP Policies</li> <li>Password Policies</li> </ul>	User Nam	e WLAN I	Profile Guest U	ser Role De	scription		
▶ Local EAP							
Priority Order							
▶ Certificate							
► Access Control Lists							
Wireless Protection     Policies							
Web Auth							
Advanced							

左側のメニューからローカルネットユーザをクリックします

3. Newをクリックして新しいユーザを作成します。

新しいウィンドウが表示され、ユーザ名とパスワード情報の入力が求められます。

4. 新しいユーザを作成するためにユーザ名とパスワードを入力し、使用するパスワードを確認 します。

この例では、User1というユーザを作成します。

5. 説明を追加します。

この例では、Guest User1 を使用します。

6. Applyをクリックして、新しいユーザ設定を保存します。

CISCO	MONITOR WLANS C	ONTROLLER WIRELESS SECURITY	MANAGEMENT	
Security	Local Net Users > Ne	ēW		
AAA     General     RADIUS     Authentication     Accounting     Fallback     TACACS+     LDAP     Local Net Users	User Name Password Confirm Password Guest User Lifetime (seconds)	User1 •••••• •••••• Ø 86400	1	<b>1</b>
MAC Filtering Disabled Clients User Login Policies AP Policies Password Policies	Guest User Role WLAN Profile Description	Guest GuestUser1	Ĩ	
Local EAP	4			
<ul> <li>Priority Order</li> <li>Certificate</li> </ul>				
Access Control Lists     Wireless Protection     Policies				
Web Auth				

cisco	MONITOR WLAN		WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	EEEDBACK
Security	Local Net User	s						
<ul> <li>▼ AAA</li> <li>General</li> <li>▼ RADIUS</li> <li>Authentication</li> <li>Accounting</li> <li>Fallback</li> <li>▼ TACACE+</li> <li>LDAP</li> </ul>	User Name			WLAN Profile	Guest User Yes	Role	Desc	ription
Local Net Users MAC filtering Disabled Clients					375			

7. データベースにさらにユーザーを追加するには、手順3-6を繰り返します。

Web 認証用の RADIUS サーバ

このドキュメントは、RADIUS サーバとして Windows Server 2003 上のワイヤレス ACS を使用 します。ネットワークで現在展開されている使用可能な任意の RADIUS サーバを使用できます。

◆ 注:ACSはWindows NTまたはWindows 2000 Serverで設定できます。Cisco.comからACSを ダウンロードするには、『Software Center(ダウンロード) – Cisco Secure Software』を 参照してください。ソフトウェアをダウンロードするには、Cisco Web アカウントが必要 です。 「ACS の設定」のセクションでは、RADIUS 用に ACS を設定する方法を示しています。ドメイン ネーム システム(DNS)および RADIUS サーバがある、完全に機能するネットワークが必要です。

ACS の設定

このセクションでは、RADIUS 用に ACS を設定するための情報を提供します。

サーバ上で ACS を設定し、認証用のユーザを作成するために次の手順を実行します。

1. ACS によりブラウザ ウィンドウで ACS を開いて設定するかどうかが尋ねられた場合は、 [yes] をクリックします。

💊 注:ACSをセットアップすると、デスクトップにもアイコンが表示されます。

2. 左側のメニューで、[User Setup] をクリックします。

このアクションにより、次に示す [User Setup] 画面が表示されます。

CiscoSecure ACS -	Microsoft Internet Explorer	
Ele Edit Yew Fi	gvantes Iools Help	Links 🎌 🌋
Address http://127	.0.0.1:1065/	💌 🔁 😡
Cinco Systems	User Setup	×
	User:       webuser1         Find       Add/Edit         List users beginning with letter/number:       A B C B K F G H I J K L H         M D F G B S T U Y S X Y Z       D I Z J J S S Z D Y         List all users       List all users         Remove Dynamic Users       D Back te Help	<text><list-item><list-item><list-item><list-item><list-item><ul> <li>Help</li> <li>Mare Salone and External User Databases</li> <li>Hondra &amp; Specific User in the ACS Internal Database</li> <li>Hondra &amp; Specific User in the ACS Internal Database</li> <li>Linina User to the ACS Internal Database</li> <li>Linina Userames that Deepin with a Particular Characters</li> <li>Linina Userames in the ACS Internal Database</li> <li>Linina Userames in the ACS Internal Database</li> <li>Linina Userames in the ACS Internal Database</li> <li>Tenna Userames in the ACS Internal User Database</li> <li>Remore Dynamic Usera</li> <li>Der Satur and Database User Society and Future Database</li> <li>Annoral Database and External User Database</li> <li>Ber Satur and Database User Society and Future Information, and users, and other action and user of actions Database</li> <li>Annoral Database are used to configure individual user information, and users, and other actions are used and the ACS internal User Database</li> <li>Annoral property configured:</li> <li>Annoral database section:</li> <li>Moral and the Uninnoon User Policy in the External User Database for users defined in an external user database in the ACS internal database for users defined in a external user database intell, for added security, entherization, and accounting and a database intellecture database users and the locate and accounting and action the ACS internal database for users defined in a external user database intellecture database intellecture and actions and accounting and actionation and active action in the action action action database in the ACS internal database for users defined in an external user database intellecture in the ACS internal database. The action action action action action action action action actin action action actin action action action action action</li></ul></list-item></list-item></list-item></list-item></list-item></text>

User Setup画面

3. Web 認証に使用するユーザを入力して、[Add/Edit] をクリックします。

ユーザの作成後に、次に示す2番目のウィンドウが表示されます。

CiscoSecure ACS - M	icrosoft Internet Explorer	X
Ele Edt Yew Fgr	antes Iools Help	Links » 🦓
Address D http://127.0	0.1:1066/	- <b>D</b>
CIECO STATEMA	User Setup	×
alls.	Edit	Holp 🗠
Setup	User: webuser1 (New User)	Account Disabled     Orleting a Unersame
Shared Profile Components	C Account Disabled	Soundementary User Jate     Passered Authentication     Group to which the user is assigned     Calback
Network Configuration	Supplementary User Info 🔶	Cleant IP: Address Assignment     Advanced Settings
Configuration	Real Name Web Auth Description	Sixtmark Access Bestictions     Max Sessions     Unser Questes
Configuration		Occuminadable ACLs     Advanced IACACs - Settings
Administration Control		TACACS - Enable Control     TACACS - Enable Parament
Dia External User Databases	User Setup	TACACS - Duthound Password     TACACS - Shell Command Anthonization
Postere Validation	Password Authentication	Command Antherization for Network Device Nanagement Applications     TACACS - Unknown Services     IETE RADIUS Attributes
Profiles	CiscoSecure PAP (Also used for CHAP/MS- CHAP/ARAP, if the Separate field is not	BADIUS Yeader Specific Attributes
Activity	Password ••••••	Account Disabled Status
Contine Documentation	Confirm Password	Select the Account Disabled check box to disable this account; clear the check box to enable the account.
<b>HILLIGHTER</b>	Separate (CHAP/M5-CHAP/ARAP)	(Back to Yeal)
	Password	
	Confirm	Determine The Delate between a set of the se
	When a token server is used for authentication, supplying a constate CHAP paceword for a token	Account, not when you are adding a new user account. To delete the current user account from the database, click <b>Delete</b> . When asked to confirm your action, click <b>OK</b> .
	Submit Cancel	(Rack to Tas)
Done		🕥 Internet

ユーザが作成されると、2番目のウィンドウが開きます

- 4. 上部の [Account Disabled] ボックスがオンになっていないことを確認します。
- 5. [Password Authentication] オプションに [ACS Internal Database] を選択します。
- 6. パスワードを入力します。管理者には、PAP/CHAPまたはMD5-CHAP認証を設定して、 ACS内部データベースにユーザを追加するオプションがあります。PAP は、コントローラ 上の Web 認証ユーザのための、デフォルトの認証タイプです。管理者は、次のCLIコマン ドを使用して、認証方式をchap/md5-chapに柔軟に変更できます。

config custom-web radiusauth <auth method>

7. 「発行」をクリックします。

Cisco WLC への RADIUS サーバ情報の入力

次のステップを実行します。

- 1. 上部のメニューで [Security] をクリックします。
- 2. 左側のメニューで [RADIUS Authentication] をクリックします。
- 3. Newをクリックして、ACS/RADIUSサーバのIPアドレスを入力します。この例では、ACS サーバの IP アドレスは 10.77.244.196 です。
- 4. RADIUS サーバの共有秘密を入力します。この秘密鍵が、WLC の RADIUS サーバで入力した秘密鍵と同じであることを確認します。
- 5. ポート番号はデフォルトの 1812 のままにしておきます。
- 6. [Server Status] オプションが [Enabled] であることを確認します。
- 7. このRADIUSサーバをワイヤレスネットワークユーザの認証に使用するために、Network User Enableボックスにチェックマークを付けます。
- 8. [適用(Apply)] をクリックします。

cisco	MONITOR WLANS		WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	EEEOBAC
Security	RADIUS Authentic	ation Server:	s > New					
<ul> <li>AAA General</li> <li>RADUUS Authentication Accounting Fallback</li> <li>TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Password Policies</li> </ul>	Server Index (Priorit Server IP Address Shared Secret Forma Shared Secret Confirm Shared Secr Key Wrap Port Number Server Status	y) nt eet [	1 × 10.77.244.196 ASCII × (Designed fi 1012 Enabled ×	6 or FIPS custon	ners and requires	a key wrap comp	iliant RAD	)IUS server)
Local EAP	Support for RFC 3576	5	Enabled -					
Priority Order	Server Timeout		2 seconds	ε				
Certificate	Network User		Enable					
Access Control Lists	Management		Enable					
<ul> <li>Wireless Protection</li> <li>Policies</li> </ul>	IPSec		□ Enable					
▶ Web Auth								
Advanced								

Network User Enableボックス

Network User ボックスにチェックマークが付いていて、Admin Status がEnabledになっていることを確認します。

cisco	MONITOR	WLANS Q	ONTROLLER	WIRELESS 2	ECURITY	MANAGEMENT	COMMANDS	HELP	EEEDBACK
Security	RADIUS	Authenticat	ion Serve	rs					
<ul> <li>AAA</li> <li>General</li> <li>RADIUS</li> <li>Authenboation</li> <li>Accounting</li> <li>Fallback</li> <li>TACACS+</li> <li>LDAP</li> <li>Local Net Users</li> <li>MAC Filtering</li> <li>Disabled Clients</li> <li>User Login Folicies</li> <li>AF Policies</li> <li>Password Policies</li> </ul>	Call Sta Use AES MAC De Network User	tion ID Type 4 S Key Wrap dimiter Management	IP Addre (Design Hyphen Server Index I	ss  ied for FIPS custom Server Address 10.77.244 196	ers and requ Port 1812	ires a key wrap o IPSec Disabled	ompliant RADJU Adm Enab	S server) in Statu- led	5
<ul> <li>Local EAP</li> <li>Priority Order</li> <li>Certificate</li> <li>Access Control Lists</li> </ul>	1. Gew Stat	xon:10:7ype=will マークを入れて	be applicable	e only for non 802.1 Statusを有効に	x authentica	tian anly,			

RADIUSサーバを使用したWLANの設定

RADIUS サーバが WLC 上で設定されたので、この RADIUS サーバを Web 認証に使用するよう に WLAN を設定する必要があります。RADIUS サーバで WLAN を設定するには、次の手順を実 行します。

- 1. WLC ブラウザを開き、[WLANs] をクリックします。これにより、WLC 上で設定されてい るすべての WLAN のリストが表示されます。Web 認証用に作成された WLAN のゲストを クリックします。
- 2. WLANs > Editページで、Securityタブをクリックします。[Security] の下の [AAA Servers] タブをクリックします。次に、RADIUS サーバを選択します。この例では 10.77.244.196 で す。

ı. cısco	MONETOR <u>W</u> LANS <u>C</u> ONTRO	LLER WIRELESS SECURITY MON	IAGEMENT C <u>o</u> mman	DS HE∐P	EEEDBACK
WLANs	WLANs > Edit 'Guest'				
WLANS WLANS	General Security Q	oS Advanced			
▶ Advanced	Layer 2 Layer 3 A	AA Servers			
	Radius Server Overwrite i	Authentication Servers	Accounting Servers	Server 1	None •
		🗹 Enabled	Enabled	Server 3	None 💌
	Server 1	IP:10.77.244.195, Port:1812 💌	None •		
	Server 2	None	None \star		
	Server 3	None	None •		
	Local EAP Authentication				
	Local EAP Authentication	D Enabled			

Securityタブをクリックしてから、AAA Serversタブをクリックします

3. [APPLY] をクリックします。

ACS の確認

ACS を設定するときには、最新のパッチと最新のコードをすべて必ずダウンロードしてください 。これにより、差し迫った問題を解決できます。RADIUS認証を使用する場合は、WLCがAAAク ライアントの1つとしてリストされていることを確認します。これを確認するには、左側の [Network Configuration] メニューをクリックします。[AAA Client] をクリックし、設定されている パスワードと認証タイプを確認します。

CiscoSecure ACS - N	ticrosoft Internet Explorer			IS NOT THE REAL PROPERTY IN THE REAL PROPERTY INTERNAL
Ble Edit Yew Fg	varites Iooks Help			an a
🔾 Back + 🔿 - 📄	😰 🐔 🔎 Search 対 Favorites 🕴	e 💁 🖏 🖬		Links <sup>30</sup>
Address Attp://127.0	0.0.1:1065/			دې 🛃 💌
Cisco Systems	Network Configurat	ion		×
and the and then.	Select			A Help
User Setup				Network Device Groups
Group Setup	<b>%</b> Q	AAA Clients	?	Adding a Nationalk Device Group     Editing a Nationalk Device Group     Delating a Nationalk Device Group
Shared Profile Components	AAA Client Hostname	AAA Client IP Address	Authenticate Using	Searching for Network Devices
Pinel Network	(WLC)	10.77.244.204	RADIUS (Cisco Airespace)	Adding a AAA Climat
Configuration	wic210	10.77.244.210	RADIUS (Cisco Airespace)	Editing a AAA Client     Deleting a AAA Client
Configuration		Add Entry Course		AAA Servers     Adding a AAA Server
Configuration		Add Entry Search		Editing a AAA Server     Deleting a AAA Server
Administration Control	<b>%</b> 0	AAA Servers	?	Preasy Distribution Table     Adding a Preasy Distribution Table Entry     Sorting Preasy Distribution Table Entries
Databases	AAA Server Name	AAA Server IP Address	AAA Server Type	Editing a Proxy Distribution Table Entry     Deleting a Proxy Distribution Table Entry
Posture Validation	ts-web	10.77.244.196	CiscoSecure ACS	
Network Access		Add Entry Search		Note: This page changes
Co L Basarts and				depending your interface configuration. If you are using
Activity		Beoug Distribution Table	9	after you click Network Configuration in the havigation
Documentation	Character String	AAA Servers	1	bar, only the Network Device Groups table and Proxy
	(Default)	ts-web	No Local	Distribution Table information appear. If you are not using bDCs, she Abb. Clinets Table and
	L			the AAA Servers table appear in place of the Network Device
		Add Entry Sort Entries		Groups table.
				Network Device Groups
		Back to Help		피
æ]				🔮 Internet

WLCがAAAクライアントとしてリストされる

[User Setup] を選択したら、ユーザが実際に存在していることを再度確認します。[List All Users] をクリックします。次に示すウィンドウが表示されます。作成したユーザがリスト内にあること を確認します。

ale ale	User Setup				
illine addition.	Select	User List			
User Setup		User	Status	Group	Network Access Profile
Setup Shared Profile	User: Find Add/Edit	User1	Enabled	Default Group (3 users)	(Default)
Components Net work		User2	Enabled	Default Group (3 users)	(Default)
Configuration	List users beginning with letter/number: <u>A B C D E F C H I J E L B</u>	Webuser	Enabled	Default Group (3 users)	(Default)
Postuse Validation Network Access Profiles Reports and Activity Dolline Evolumentation	Back, to Help				

すべてのユーザーを一覧表示

LDAP サーバ

この項では、Lightweight Directory Access Protocol(LDAP)サーバを、RADIUS データベースや ローカル ユーザ データベースに類似したバックエンド データベースとして設定する方法につい て説明します。LDAP バックエンド データベースでは、コントローラは、特定のユーザのクレデ ンシャル(ユーザ名とパスワード)について LDAP サーバに照会することができます。このクレ デンシャルはユーザの認証に使用されます。

コントローラのGUIを使用してLDAPを設定するには、次の手順を実行します。

1. [Security] > [AAA] > [LDAP] をクリックして、LDAP サーバを開きます。

このページでは、これまでに設定されたすべての LDAP サーバが表示されます。

- 現在のLDAPサーバを削除する場合は、そのサーバの青いドロップダウン矢印の上に カーソルを移動し、Removeを選択します。
- コントローラが特定のサーバに到達できることを確認するには、そのサーバの青いドロップダウンの矢印の上にカーソルを置いて、[Ping]を選択します。

- 2. 次のいずれかのオプションを実行します。
  - 現在のLDAPサーバを編集するには、そのサーバのインデックス番号をクリックします。[LDAP Servers > Edit] ページが表示されます。
  - LDAP サーバを追加するには、[New] をクリックします。[LDAP Servers > New] ページが表示されます。

cisco		<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP
Security	LDAP Se	rvers > N	lew.					
<ul> <li>AAA</li> <li>General</li> <li>RADIUS</li> <li>Authentication</li> <li>Accounting</li> <li>Fallback</li> <li>TACACS+</li> <li>LDAP</li> <li>Local Net Users</li> <li>MAC Filtering</li> <li>Disabled Clients</li> <li>User Login Policies</li> <li>AP Policies</li> <li>Password Policies</li> <li>Local EAP</li> <li>Priority Order</li> <li>Certificate</li> <li>Access Control Lists</li> <li>Wireless Protection</li> <li>Policies</li> <li>Web Auth</li> </ul>	Server In Server IP Port Num Simple Bi Bind User Bind Pass Confirm B User Attri User Attri User Obje Server Ti Enable Se	ndex (Priori Address ber ind mame word Bind Passw e DN ibute ect Type meaut srver Statu	ty) ord	1  1 10.77.244.194 369 Authenticated user2  000-active.ou uid person 2 seconds Enabled	6 -employees,o	u=people,c=cisco	com	
LDAPサーバの追加								

- 3. 新しいサーバを追加する場合は、Server Index (Priority)ドロップダウンボックスから番号を 選択して、他の設定済みLDAPサーバに対するこのサーバの優先順位を指定します。サーバ は最大 17 個まで設定できます。コントローラが最初のサーバに接続できない場合、リスト の 2 番目のサーバへの接続を試行する、というようになります。
- 4. 新しいサーバを追加する場合は、Server IP AddressフィールドにLDAPサーバのIPアドレス を入力します。
- 5. 新しいサーバを追加する場合は、LDAPサーバのTCPポート番号をポート番号フィールドに 入力します。有効な範囲は 1 ~ 65535 で、デフォルト値は 389 です。
- Enable Server Statusチェックボックスにチェックマークを入れてこのLDAPサーバを有効に するか、チェックマークを外して無効にします。デフォルト値は無効です。
- [Simple Bind] ドロップダウン ボックスから、[Anonymous] または [Authenticated] を選択して、LDAP サーバ用のローカル認証バインド方式を指定します。匿名方式では LDAP サーバへの匿名アクセスが可能です。一方、認可方式ではユーザ名とパスワードを入力してアクセスをセキュリティで保護する必要があります。デフォルトでは [Anonymous] になっています。
- 8. 手順7で [Authenticated] を選択した場合は、次の手順に従ってください。

- a. [Bind Username] フィールドに、LDAP サーバに対するローカル認証に使用されるユ ーザ名を入力します。
- b. [Bind Password] フィールドおよび [Confirm Bind Password] フィールドには、LDAP サーバに対するローカル認証で使用されるパスワードを入力します。
- 9. [User Base DN] フィールドに、すべてのユーザのリストを含む LDAP サーバ内のサブツリ ーの識別名(DN)を入力します。たとえば、ou=organizational unit、ou=next organizational unit、o=corporation.exampleのようになります。ユーザを含むツリーがベー スDNである場合は、「o=corporation.example」または「dc=corporation, dc=com」と入力 します。
- 10. [User Attribute] フィールドに、ユーザ名を含むユーザ レコード内の属性の名前を入力しま す。この属性はディレクトリ サーバから取得できます。
- 11. [User Object Type] フィールドに、対象のレコードをユーザとして特定する LDAP objectType 属性の値を入力します。多くの場合、ユーザ レコードには objectType 属性の値 が複数あり、そのうちのいくつかはユーザに固有であり、また、いくつかは他のオブジェク ト タイプと共有されています。
- 12. [Server Timeout] フィールドに、再送信の間隔(秒数)を入力します。有効な範囲は2~
   30 秒であり、デフォルト値は2秒です。
- 13. [Apply] をクリックして、変更を確定します。
- 14. [Save Configuration] をクリックして変更を保存します。
- 15. 特定の LDAP サーバを WLAN に割り当てるには、次の手順を実行します。
  - a. ClickWLANsをクリックして、WLANsページを開きます。
  - b. 必要な WLAN の ID 番号をクリックします。
  - c. [WLANs] > [Edit] ページが表示されたら [Security] > [AAA Servers] タブをクリックし 、[WLANs] > [Edit] ([Security] > [AAA Servers])ページを開きます。

ANs > Edit 'Guest'				
eneral Security QoS	Advanced			
Laver 2 Laver 3 AAA Ser	vers			
EXT. 2 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	1620.1			
Select 444 covers below to over	والمتحدث والمتحدث والمتحدث	- above and way		
THE PARTY ACTIVELY DELOW TO OVER	ride use of default servers t	OD TRUS WLAN		
nation was servers below to over	rue use of default servers t	OD UNIS WEARS		
Radius Servers	rue use of nerault servers t	In this wears	LDAP Serve	rs
Radius Servers Radius Server Overwrite interface	Enabled	In this weaks	LDAP Serve Server 1	rs TPSIDD7R24031958PD7t83891
Radius Servers Radius Server Overwrite interface	Enabled     Authentication Servers	Accounting Servers	LDAP Serve Server 1 Server 2	rs IPS10274201.1954 Port-889 - Nona
Radius Servers Radius Server Overwrite interface	Enabled      Enabled      Enabled      Enabled	Accounting Servers	LDAP Serve Server 1 Server 2 Server 3	rs 19:10.27.244.195. Port 389 None
Radius Servers Radius Server Overwrite interface Server 1	Enabled Authentication Servers Enabled None	Accounting Servers	LDAP Server Server 1 Server 2 Server 3	rs (19-10.77.244.195, Port 389) None None
Radius Servers Radius Server Overwrite interface Server 1 Server 2	Enabled     Authentication Servers     Enabled     None     None	Accounting Servers	LDAP Server 1 Server 2 Server 3	rs 19:10.27.214.195. Part 389 None -
Radius Servers Radius Server Overwrite interface Server 1 Server 2 Server 3	Enabled     Authentication Servers     None     None	Accounting Servers	LDAP Server Server 1 Server 2 Server 3	PS 19:10.27.244.195. Port-389. None  None

- Security > AAA Servers Tabsをクリックします
- d. [LDAP Servers] ドロップダウン ボックスから、この WLAN に使用する LDAP サーバ を選択します。最大 3 台の LDAP サーバを選択できます。これらのサーバは優先順位 に従って試行されます。
- e. [Apply] をクリックして、変更を確定します。
- f. [Save Configuration] をクリックして変更を保存します。

### Web 認証を使用するための WLAN クライアントの設定

WLC を設定したら、クライアントは Web 認証用に正しく設定される必要があります。このセク ションでは、Web 認証用に Windows システムを設定するための情報を提供します。

#### クライアントの設定

Microsoft ワイヤレス クライアントの設定は、このサブスクライバの場合はほとんど変更されま せん。適切な WLAN/SSID 設定情報を追加するだけで済みます。次のステップを実行します。

- 1. Windows の [Start] メニューから、[Settings] > [Control Panel] > [Network and Internet Connections] を選択します。
- 2. [Network Connections] アイコンをクリックします。
- 3. [LAN Connection] アイコンを右クリックして、[Disable] を選択します。
- 4. [Wireless Connection] アイコンを右クリックして、[Enable] を選択します。
- 5. [Wireless Connection] アイコンを再度右クリックして、[Properties] を選択します。
- 6. [Wireless Network Connection Properties] ウィンドウから、[Wireless Networks] をクリック します。

- 7. 推奨されるネットワーク エリアの下で、[Add] をクリックして、Web 認証 SSID を設定します。
- 8. [Association] タブの下で、Web 認証に使用するネットワーク名(WLAN/SSID)の値を入力 します。

Wireless network properties	? ×
Association Authentication C	onnection
Network <u>n</u> ame (SSID):	uest
Wireless network key	
This network requires a key f	or the following:
Network Authentication:	Open 💌
Data encryption:	Disabled
Network key:	
Confirm network key:	
Key inde <u>x</u> (advanced):	3
The key is provided for m	e automatically
This is a <u>computer-to-comp</u> access points are not used	uter (ad hoc) network; wireless
	OK Cancel

Associationタブでネットワーク名を入力します。

◆ 注:デフォルトでは、Data EncryptionはWired Equivalent Privacy(WEP)です。Web認 証が機能するように、データ暗号化を無効にします。

9. ウィンドウの下部にある [OK] をクリックして、設定を保存します。

WLAN と通信する場合は、[Preferred Network] ボックスにビーコン アイコンが表示されます。

これは Web 認証とのワイヤレス接続が正常であることを示します。WLC は、ワイヤレス Windows クライアントに IP アドレスを提供済みです。

<b>*</b> Wireless Network Conne	ction 3 Status 🛛 🕜 🔀
General Support	
Internet Protocol (TCP/IP)	
Address Type:	Assigned by DHCP
IP Address:	10.10.10.7
Subnet Mask:	255.255.255.0
Default Gateway:	10.10.10.1
	Details
Regain	
	Çlose

WLCが提供するIPアドレス



◆ 注:ログインに成功した後、ワイヤレスクライアントがアイドル状態で他のデバイスと通信 しない場合、クライアントはアイドルタイムアウト期間の後に認証を解除されます。タイム アウト時間はデフォルトで300秒であり、CLIコマンドconfig network usertimeout ◆ <seconds>で変更できます。タイムアウトになると、クライアント エントリはコントローラ から削除されます。クライアントは、再度関連付けられると、Webauth\_Reqd状態に戻るこ とができます。

注:ログインに成功した後、クライアントがアクティブである場合は、そのWLANに設定されたセッションタイムアウト期間(たとえば、デフォルトでは1800秒ですが、CLIコマンド config wlan session-timeout <WLAN ID> <seconds>を使用して変更できます)が経過した後でも、クライアントは認証を解除してコントローラからエントリを削除できます。タイムアウトになると、クライアント エントリはコントローラから削除されます。クライアントは、再度関連付けられると、Webauth\_Reqd状態に戻ります。

クライアントがWebauth\_Reqd状態の場合、クライアントがアクティブかアイドルかに関係なく 、web-auth required timeout期間(たとえば、300秒で、この時間はユーザが設定できないなど )の後にクライアントの認証が解除される場合があります。クライアントからのすべてのトラフ ィック(事前認証ACLを介して許可される)が中断されます。クライアントは、再度関連付けら れると、Webauth\_Reqd状態に戻ります。

クライアントログイン

次のステップを実行します。

ブラウザ ウィンドウを開き、URL または IP アドレスを入力します。こうするとクライアントに Web 認証ページが表示されます。

コントローラが3.0より前のリリースを実行している場合、ユーザはWeb認証ページを表示 するためにhttps://10.1.1.1/login.htmlを入力する必要があります。

セキュリティ アラート ウィンドウが表示されます。

2. [Yes]をクリックして次に進みます。

[Login] ウィンドウが表示されたら、作成したローカル ネット ユーザのユーザ名とパスワードを入力します。

Login		
Welcome to	the Cisco wireless network	
Cisco is please your network. Pl solution to work	d to provide the Wireless LAN infrastructure for ease login and put your unified wireless	
User Name	Useri	
Password	•••••	
	Submit	

ログインウィンドウ

ログインに成功すると、2つのブラウザウィンドウが表示されます。大きい方のウィンドウ はログインに成功したことを示し、このウィンドウを使用してインターネットをブラウズで きます。小さいほうのウィンドウは、ゲスト ネットワークの使用が完了したときのログア ウトに使用します。

上の図は、Web認証のリダイレクトが成功した状態を示しています。

次の図は、認証が発生すると表示されるLogin Successfulウィンドウを示しています。



ログイン成功!

Cisco 4404/WiSMコントローラは、125の同時Web認証ユーザログインをサポートし、最大 5000のWeb認証クライアントまで拡張できます。

Cisco 5500コントローラは、150の同時Web Authユーザログインをサポートできます。

Web 認証のトラブルシューティング

パスワード認証で問題が発生する場合は、ACS の 左下にある [Reports and Activity] をクリック して、使用可能なすべてのレポートを開きます。レポートウィンドウを開いた後で、RADIUS Accounting、Failed Attempts for log in、Passed Authentications、Logged-in Users、およびその 他のレポートを開くオプションがあります。これらのレポートは .csv ファイルであり、ご使用の マシン上でローカルに開くことができます。レポートは、認証の問題(ユーザ名やパスワードの 誤りなど)を検出するために役立ちます。ACS には、オンライン ドキュメントが付属していま す。ライブ ネットワークに接続しておらず、サービス ポートを定義していない場合、ACS はサ ービス ポートにイーサネット ポートの IP アドレスを使用します。ネットワークに接続していな い場合、たいていは Windows 169.254.x.x のデフォルト IP アドレスを使用することになります。

CiscoSecure ACS - M	Scrosoft Internet Explorer		lΧ
the tot your for	vankes Iaals Help	(res *	tr.
Address Thetp://127.0	0.0.1:1065/	- 0	60
Cinco Statema	Reports and Activity		×
with a differ	Select	Help	-
Extrap Setup S	Reports  TACACS+ Accounting  TACACS+ Accounting  ACACS+ Administration  ACS Backup And Restore  Catabase Replication  Administration Audit  Stor Password Changes  ACS Service Monitoring  ACS Service Monitoring  Entitlement Reports	Hair         Previous         This page is used to select the ACS reports.         Previous Reports         Consolutions and Disactions Reports         Previous Reports         Reports         Reports         Previous Reports         Reports Reports         Reports Reports         Versing Reports         Previous Reports and previous reports reports from the ACS web intenefi	<b>4</b>
		criteria includes a regular expression, a time range, or both: • Regular expression-based filtering chacks that at least one of each column's value, per row.	
	1	mutches the neucled constar surveysize, when you use resultar surveysize Greeks ACS	-

レポートとアクティビティウィンドウ

◆ 注:外部URLを入力すると、WLCによって内部Web認証ページに自動的に接続されます。 自動接続が機能しない場合には、URL バーで WLC の管理 IP アドレスを入力するとトラブ ルシューティングができます。ブラウザの上部で Web 認証のリダイレクトについて通知す るメッセージを確認します。

Web認証のトラブルシューティングの詳細については、『ワイヤレスLANコントローラ(WLC)で

<u>のWeb認証のトラブルシューティング</u>』を参照してください。

# IPv6 ブリッジングでの Web 認証

WLAN を IPv6 ブリッジング用に設定するには、コントローラ GUI から [WLANs] に移動します。 次に、目的の WLAN を選択し、[WLANs] > [Edit] ページから [Advanced] を選択します。

このWLANに接続するクライアントがIPv6パケットを受け入れることができるようにするには、 IPv6 Enableチェックボックスをオンにします。それ以外の場合、このチェックボックスはオフ (デフォルト値)のままにしておきます。IPv6チェックボックスを無効にする(またはオフにす る)と、IPv6は認証後にのみ許可されます。IPv6 を有効にすると、コントローラはクライアント 認証なしで IPv6 トラフィックを渡せるようになります。

General Security	QoS Adv	vanced		
Aironet IE Enablad		Management Frame Protection (MFP)		
Diagnostic Charnel	Enabled		the second second second	
1Pv6 Enable 7			MFP Client Protection \$	Optional 💌
Override Interface ACL None 🗙		DTIM Period (in beacon intervals)		
P2P Blocking Action Disabled				
Client Exclusion 2		60	802.11a/n (1 - 255)	1
	El chabled	Timeout Value (cecc)	802.11h/g/n (1 - 255)	1
Off Channel Scanning	Defer		NAC	
Scan Defer Priority	0 1 2 3 4 5 6 7		State Enabled	
			Load Balancing and Band Select	
Scan Defer Time (msecs)			Client Load Balancing	
	100		Client Band Select	

目的のWLANを選択し、Advancedを選択します

# 関連情報

- WLCを使用した外部Web認証の設定
- ・ <u>ワイヤレスLANコントローラ(WLC)でのWeb認証のトラブルシューティング</u>
- <u>Cisco ワイヤレス LAN</u>
- Cisco WLANコントローラを使用した有線ゲストアクセスの設定例
- CiscoワイヤレスLANコントローラの廃止に関する通知
- RADIUSサーバを介したワイヤレスLANコントローラのロビー管理者の認証
- シスコのテクニカルサポートとダウンロード

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。