DNS ベースのアクセス コントロール リスト

DNS ベースのアクセス コントロール リストについて

DNS ベースの ACL は、ワイヤレス クライアント デバイスに使用されます。これらのデバイスを使用する場合は、許可またはブロックするデータ要求を決定するために、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ で認証前 ACL を設定できます。

コントローラ で DNS ベースの ACL を有効にするには、ACL の許可 URL または拒否 URL を設定する必要があります。URL は、ACL で事前設定しておく必要があります。

DNS ベースの ACL によって、登録フェーズ中のクライアントは、設定された URL への接続を許可されます。コントローラ は ACL 名で設定され、AAA サーバから返されます。ACL 名が AAA サーバによって返されると、ACL は Web リダイレクト用にクライアントに適用されます。

クライアント認証フェーズで、AAA サーバは事前認証 ACL（url-redirect-acl）を返します。DNS スヌーピングは、登録が完了してクライアントが SUPPLICANT PROVISIONING 状態になるまで、各クライアントの AP で実行されます。URL で設定された ACL がコントローラ で受信されると、CAPWAP ペイロードが AP に送信され、クライアントの DNS スヌーピングが有効になり、URL がスヌーピングされます。

適切な URL スヌーピングにより、AP は DNS 応答の解決済みドメイン名の IP アドレスを学習します。設定された URL にドメイン名が一致した場合は、IP アドレスを求めるために DNS 応答が解析され、IP アドレスが CAPWAP ペイロードとしてコントローラ に送信されます。コントローラ によって IP アドレスの許可リストに IP アドレスが追加されるため、クライアントは設定された URL にアクセスできます。

事前認証または事後認証中に、DNS ACL がアクセスポイントのクライアントに適用されます。クライアントが、ある AP から別の AP にローミングした場合、古い AP で DNS により学習された IP アドレスは新しい AP でも有効になります。

DNS ベースのアクセス コントロール リストの制約事項

DNS ベースの ACL には次の制約があります。

- 認証前フィルタと認証後フィルタはローカルモードでサポートされています。Flex（ファブリック）モードでは認証前フィルタのみがサポートされています。
- ISE からプッシュされる ACL オーバーライドはサポートされていません。

フレックス モード

URL フィルタ リストの定義

手順

	コマンドまたはアクション	目的
ステップ 1	**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 2	**urlfilter list** *list-name* 例： `Device(config)# urlfilter list urllist_flex_preauth`	URL フィルタ リストを設定します。 ここで、*list-name* は URL フィルタ リスト名を指します。リスト名は 32 文字以内の英数字にする必要があります。

	コマンドまたはアクション	目的
ステップ 3	**action permit** 例： `Device(config-urlfilter-params)# action permit`	アクションとして、permit（ホワイトリスト）または deny（ブラックリスト）を設定します。
ステップ 4	**redirect-server-ip4** *IPv4-address* 例： `Device(config-urlfilter-params)# redirect-server-ipv4 8.8.8.8`	URL リストの IPv4 リダイレクト サーバを設定します。 ここで、*IPv4-address* は IPv4 アドレスを指します。
ステップ 5	**redirect-server-ip6** *IPv6-address* 例： `Device(config-urlfilter-params)# redirect-server-ipv6 2001:300:8::81`	URL リストの IPv6 リダイレクト サーバを設定します。 ここで、*IPv6-address* は IPv6 アドレスを指します。
ステップ 6	**url** *url* 例： `Device(config-urlfilter-params)# url url1.dns.com`	URL を設定します。 ここで、*url*は URL の名前を指します。
ステップ 7	**end** 例： `Device(config-urlfilter-params)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

Flex プロファイルへの URL フィルタ リストの適用

手順

	コマンドまたはアクション	目的
ステップ 1	**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 2	**wireless profile flex** *default-flex-profile* 例： `Device(config)# wireless profile flex default-flex-profile`	新しい flex ポリシーを作成します。 デフォルトの flex プロファイル名は *default-flex-profile* です。
ステップ 3	**acl-policy** *acl policy name* 例：	ACL ポリシーを設定します。

	コマンドまたはアクション	目的
	`Device(config-wireless-flex-profile)# acl-policy acl_name`	
ステップ 4	**urlfilter list** *name* 例： `Device(config-wireless-flex-profile-acl)# urlfilter list urllist_flex_preauth`	Flex プロファイルに URL リストを適用します。
ステップ 5	**end** 例： `Device(config-wireless-flex-profile-acl)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

中央 Web 認証用の ISE の設定（GUI）

中央 Web 認証用に ISE を設定するには、次の手順に従います。

手順

ステップ 1 Cisco Identity Services Engine（ISE）にログインします。

ステップ 2 [Policy] をクリックし、[Policy Elements] をクリックします。

ステップ 3 [Results] をクリックします。

ステップ 4 [Authorization] を展開し、[Authorization Profiles] をクリックします。

ステップ 5 [Add] をクリックして、URL フィルタ用の新しい許可プロファイルを作成します。

ステップ 6 [Name] フィールドにプロファイルの名前を入力します。たとえば、CentralWebauth と入力します。

ステップ 7 [Access Type] ドロップダウン リストから [ACCESS_ACCEPT] オプションを選択します。

ステップ 8 [Advanced Attributes Setting] セクションで、ドロップダウン リストから [Cisco:cisco-av-pair] を選択します。

ステップ 9 それぞれのペアの後にある（[+]）アイコンをクリックして 1 つずつ入力します。

- url-redirect-acl=<sample_name>
- url-redirect=<sample_redirect_URL>

次に例を示します。

```
Cisco:cisco-av-pair = priv-lvl=15
Cisco:cisco-av-pair = url-redirect-acl=ACL-REDIRECTTTTTTTTTTTTTTTTTTT2
Cisco:cisco-av-pair = url-redirect=
https://9.10.8.247:port/portal/gateway?sessionId=SessionIdValue&portal=0ce17ad0-6d90-11e5-978e-00505bf2f0a&daysToExpiry=value&action=cwa
```

ステップ 10 [Attributes Details] セクションの内容を確認し、[Save] をクリックします。

中央 Web 認証用の ISE の設定

手順

ステップ 1 Cisco Identity Services Engine（ISE）にログインします。

ステップ 2 [Policy] をクリックし、[Policy Elements] をクリックします。

ステップ 3 [Results] をクリックします。

ステップ 4 [Authorization] を展開し、[Authorization Profiles] をクリックします。

ステップ 5 [Add] をクリックして、URL フィルタ用の新しい許可プロファイルを作成します。

ステップ 6 [Name] フィールドに、プロファイルの名前を入力します。たとえば、CentralWebauth と入力します。

ステップ 7 [Access Type] ドロップダウン リストから [ACCESS_ACCEPT] を選択します。

ステップ 8 [Advanced Attributes Setting] セクションで、ドロップダウン リストから [Cisco:cisco-av-pair] を選択します。

ステップ 9 それぞれのペアの後にある（[+]）アイコンをクリックして 1 つずつ入力します。

- url-redirect-acl=<sample_name>
- url-redirect=<sample_redirect_URL>

次に例を示します。

```
Cisco:cisco-av-pair = priv-lvl=15
Cisco:cisco-av-pair = url-redirect-acl=ACL-REDIRECTTTTTTTTTTTTTTTTTTT2
Cisco:cisco-av-pair = url-redirect=
https://9.10.8.247:port/portal/gateway?sessionId=SessionIdValue&portal=0ce17ad0-6d90-11e5-978e-005056bf2f0a&daysToExpiry=value&action=cwa
```

ステップ 10 [Attributes Details] セクションの内容を確認し、[Save] をクリックします。

ローカル モード

URL フィルタ リストの定義

手順

	コマンドまたはアクション	目的
ステップ 1	**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 2	**urlfilter list** *list-name* 例： `Device(config)# urlfilter list urllist_local_preauth`	URL フィルタ リストを設定します。 ここで、*list-name* は URL フィルタ リスト名を指します。リスト名は 32 文字以内の英数字にする必要があります。
ステップ 3	**action permit** 例： `Device(config-urlfilter-params)# action permit`	アクションとして、permit（ホワイトリスト）または deny（ブラックリスト）を設定します。
ステップ 4	**filter-type post-authentication** 例： `Device(config-urlfilter-params)# filter-type post-authentication`	（注） このステップは、認証後 URL フィルタを設定するときにのみ適用されます。 URL リストを認証後フィルタとして設定します。
ステップ 5	**redirect-server-ip4** *IPv4-address* 例： `Device(config-urlfilter-params)# redirect-server-ipv4 9.1.0.101`	URL リストの IPv4 リダイレクト サーバを設定します。 ここで、*IPv4-address* は IPv4 アドレスを指します。
ステップ 6	**redirect-server-ip6** *IPv6-address* 例： `Device(config-urlfilter-params)# redirect-server-ipv6 2001:300:8::82`	URL リストの IPv6 リダイレクト サーバを設定します。 ここで、*IPv6-address* は IPv6 アドレスを指します。
ステップ 7	**url** *url* 例： `Device(config-urlfilter-params)# url url1.dns.com`	URL を設定します。 ここで、*url*は URL の名前を指します。
ステップ 8	**end** 例： `Device(config-urlfilter-params)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

ポリシー プロファイルへの URL フィルタ リストの適用

手順

	コマンドまたはアクション	目的
ステップ 1	**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 2	**wireless profile policy** *profile-policy* 例： `Device(config)# wireless profile policy default-policy-profile`	ワイヤレス ポリシー プロファイルを設定します。 ここで、*profile-policy* は WLAN ポリシー プロファイルの名前を指します。

ステップ 3	**urlfilter list** {**pre-auth-filter** *name* | **post-auth-filter** *name*}
	例：
	`Device(config-wireless-policy)# urlfilter list pre-auth-filter urllist_local_preauth`
	`Device(config-wireless-policy)# urlfilter list post-auth-filter urllist_local_postauth`
		ポリシー プロファイルに URL リストを適用します。
		ここで、*name* は、以前に設定された認証前または認証後 URL フィルタ リストの名前を指します。
		（注） クライアントの join 中に、ポリシーで設定された URL フィルタが適用されます。

ステップ 4	**end** 例： `Device(config-wireless-policy)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

中央 Web 認証用の ISE の設定

許可プロファイルの作成

手順

ステップ 1 Cisco Identity Services Engine（ISE）にログインします。
ステップ 2 [Policy] をクリックし、[Policy Elements] をクリックします。
ステップ 3 [Results] をクリックします。
ステップ 4 [Authorization] を展開し、[Authorization Profiles] をクリックします。
ステップ 5 [Add] をクリックして、URL フィルタ用の新しい許可プロファイルを作成します。

ステップ 6 [Name] フィールドに、プロファイルの名前を入力します。たとえば、CentralWebauth と入力します。

ステップ 7 [Access Type] ドロップダウン リストから [ACCESS_ACCEPT] を選択します。

ステップ 8 [Advanced Attributes Setting] セクションで、ドロップダウン リストから [Cisco:cisco-av-pair] を選択します。

ステップ 9 それぞれのペアの後にある（[+]）アイコンをクリックして 1 つずつ入力します。

- url-filter-preauth=<preauth_filter_name>
- url-filter-postauth=<postauth_filter_name>

次に例を示します。

```
Cisco:cisco-av-pair = url-filter-preauth=urllist_pre_cwa
Cisco:cisco-av-pair = url-filter-postauth=urllist_post_cwa
```

ステップ 10 [Attributes Details] セクションの内容を確認し、[Save] をクリックします。

認証ルールへの許可プロファイルのマッピング

手順

ステップ 1 [Policy] > [Authentication] ページで、[Authentication] をクリックします。

ステップ 2 認証ルールの名前を入力します。

たとえば、「MAB」と入力します。

ステップ 3 [If] 条件フィールドで、プラス（[+]）アイコンをクリックします。

ステップ 4 [Compound condition] を選択し、[WLC_Web_Authentication] を選択します。

ステップ 5 [and ...] の横にある矢印をクリックして、ルールをさらに展開します。

ステップ 6 [Identity Source] フィールドの [+] アイコンをクリックし、[Internal endpoints] を選択します。

ステップ 7 [If user not found] ドロップダウン リストから [Continue] を選択します。

このオプションを使用すると、MAC アドレスが不明な場合でもデバイスを認証できます。

ステップ 8 [Save] をクリックします。

許可ルールへの許可プロファイルのマッピング

手順

ステップ 1 [Policy] > [Authorization] をクリックします。

ステップ 2 [Rule Name] フィールドに、名前を入力します。

たとえば、「CWA Post Auth」などと入力します。

ステップ 3 [Conditions] フィールドで、プラス（[+]）アイコンを選択します。

ステップ 4 ドロップダウン リストをクリックして、[Identity Groups] 領域を表示します。

ステップ 5 [User Identity Groups] > [user_group] を選択します。

ステップ 6 [and ...] の横にあるプラス記号（[+]）をクリックして、ルールをさらに展開します。

ステップ 7 [Conditions] フィールドで、プラス（[+]）アイコンを選択します。

ステップ 8 [Compound Conditions] を選択し、新しい条件の作成を選択します。

ステップ 9 設定アイコンで、オプションから [Add Attribute/Value] を選択します。

ステップ 10 [Description] フィールドで、ドロップダウン リストから属性として [Network Access] > [UseCase] を選択します。

ステップ 11 [Equals] 演算子を選択します。

ステップ 12 右側のフィールドから、[GuestFlow] を選択します。

ステップ 13 [Permissions] フィールドで、プラス（[+]）アイコンを選択してルールの結果を選択します。

[Standard] > [PermitAccess] オプションを選択するか、または必要な属性を返すカスタム プロファイルを作成できます。

DNS ベースのアクセス コントロール リストの表示

指定されたワイヤレス URL フィルタの詳細を表示するには、次のコマンドを使用します。

```
Device# show wireless urlfilter details <urllist_flex_preauth>
```

すべてのワイヤレス URL フィルタのサマリーを表示するには、次のコマンドを使用します。

```
Device# show wireless urlfilter summary
```

結果のポリシー セクションでクライアントに適用された URL フィルタを表示するには、次のコマンドを使用します。

```
Device# show wireless client mac-address <MAC_addr> detail
```

DNS ベースのアクセス コントロール リストの設定例

フレックスモード

例：*URL* フィルタ リストの定義

次に、Flex モードで URL リストを定義する例を示します。

```
Device# configure terminal
Device(config)# urlfilter list urllist_flex_pre
```

```
Device(config-urlfilter-params)# action permit
Device(config-urlfilter-params)# redirect-server-ipv4 8.8.8.8
Device(config-urlfilter-params)# redirect-server-ipv6 2001:300:8::81
Device(config-urlfilter-params)# url url1.dns.com
Device(config-urlfilter-params)# end
```

例：*Flex* プロファイルへの *URL* フィルタ リストの適用

次に、Flex モードで Flex プロファイルに URL リストを適用する例を示します。

```
Device# configure terminal
Device(config)# wireless profile flex default-flex-profile
Device(config-wireless-flex-profile)# acl-policy acl_name
Device(config-wireless-flex-profile-acl)# urlfilter list urllist_flex_preauth
Device(config-wireless-flex-profile-acl)# end
```

ローカル モード

例：認証前 *URL* フィルタ リストの定義

次に、URL フィルタ リスト（認証前）を定義する例を示します。

```
Device# configure terminal
Device(config)# urlfilter list urllist_local_preauth
Device(config-urlfilter-params)# action permit
Device(config-urlfilter-params)# redirect-server-ipv4 9.1.0.101
Device(config-urlfilter-params)# redirect-server-ipv6 2001:300:8::82
Device(config-urlfilter-params)# url url1.dns.com
Device(config-urlfilter-params)# end
```

例*:*：認証後 *URL* フィルタ リストの定義

次に、URL フィルタ リスト（認証後）を定義する例を示します。

```
Device# configure terminal
Device(config)# urlfilter list urllist_local_postauth
Device(config-urlfilter-params)# action permit
Device(config-urlfilter-params)# filter-type post-authentication
Device(config-urlfilter-params)# redirect-server-ipv4 9.1.0.101
Device(config-urlfilter-params)# redirect-server-ipv6 2001:300:8::82
Device(config-urlfilter-params)# url url1.dns.com
Device(config-urlfilter-params)# end
```

例：ポリシー プロファイルへの *URL* フィルタ リストの適用

次に、ローカル モードでポリシー プロファイルに URL リストを適用する例を示します。

```
Device# configure terminal
Device(config)# wireless profile policy default-policy-profile
Device(config-wireless-policy)# urlfilter list pre-auth-filter urllist_local_preauth
Device(config-wireless-policy)# urlfilter list post-auth-filter urllist_local_postauth
Device(config-wireless-policy)# end
```

DNS スヌーピング エージェント（DSA）の確認

DNS スヌーピング エージェント クライアントの詳細を表示するには、次のコマンドを使用します。

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent client
```

DSA が有効になっているインターフェイスの詳細を表示するには、次のコマンドを使用します。

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent client
enabled-intf
```

uCode メモリ内のパターン リストを表示するには、次のコマンドを使用します。

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent client
hw-pattern-list
```

パターン リストの OpenDNS 文字列を表示するには、次のコマンドを使用します。

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent client
hw-pattern-list odns_string
```

パターン リストの FQDN フィルタを表示するには、次のコマンドを使用します。

```
Device#
show platform hardware chassis active qfp feature dns-snoop-agent client hw-pattern-list
 fqdn-filter <fqdn_filter_ID>
```

（注） *fqdn_filter_ID* の有効な範囲は 1 ～ 16 です。

DSA クライアントの詳細を表示するには、次のコマンドを使用します。

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent client info
```

CPP クライアントのパターン リストを表示するには、次のコマンドを使用します。

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent client
pattern-list
```

パターン リストの OpenDNS 文字列を表示するには、次のコマンドを使用します。

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent client
pattern-list odns_string
```

パターン リストの FQDN フィルタを表示するには、次のコマンドを使用します。

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent client
pattern-list fqdn-filter <fqdn_filter_ID>
```

（注） *fqdn_filter_ID* の有効な範囲は 1 ～ 16 です。

DSA データパスの詳細を表示するには、次のコマンドを使用します。

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent datapath
```

DSA IP キャッシュ テーブルの詳細を表示するには、次のコマンドを使用します。

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent datapath
ip-cache
```

DSA アドレス エントリの詳細を表示するには、次のコマンドを使用します。

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent datapath
ip-cache address {ipv4 <IPv4_addr> | ipv6 <IPv6_addr>}
```

すべての DSA IP キャッシュ アドレスの詳細を表示するには、次のコマンドを使用します。

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent datapath
ip-cache all
```

DSA IP キャッシュ パターンの詳細を表示するには、次のコマンドを使用します。

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent datapath
ip-cache pattern <pattern>
```

DSA データパス メモリの詳細を表示するには、次のコマンドを使用します。

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent datapath memory
```

DSA 正規表現テーブルを表示するには、次のコマンドを使用します。

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent datapath
regexp-table
```

DSA の統計情報を表示するには、次のコマンドを使用します。

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent datapath stats
```

WebAuth 認証前および認証後 ACL による Flex クライアントの IPv6 サポートについて

IOS IPv6 ACL は、webauth ACL を AP に送信するために使用されます。

ACL 定義は次のイベントで AP にプッシュされます。

- AP の join。
- flex プロファイルでの新しい ACL マッピング。
- デフォルトの External WebAuth（EWA）セキュリティ ACL がプッシュされたとき。
- Flex プロファイルでの IPv6 ACL 定義の設定。

（注） カスタム ACL はすべて、Flex プロファイルでマッピングする必要があります。カスタム ACL の定義のみ、生成されるデフォルト ACL とは別の AP にプッシュされます。

カスタムの認証前 ACL は、WLAN プロファイルの配下にマッピングされます。一方、カスタムの認証後 ACL は、デフォルト ポリシー プロファイルの配下にマッピングされます。認証後 ACL はすべて、デフォルトの Flex プロファイルの配下で設定されます。

デフォルトのローカル Web 認証 ACL

事前定義されたデフォルトの LWA IPv6 ACL は、AP にプッシュされ、データ プレーンに組み込まれます。

デフォルトの外部 Web 認証 ACL

デフォルトの EWA ACL は、パラメータ マップで設定されたリダイレクト ポータル アドレスから生成されます。

次のリストでは、デフォルトの EWA ACL のタイプについて説明します。

- セキュリティ ACL：AP にプッシュされます。
- インターセプト ACL：データ プレーンに組み込まれます。

FQDN ACL

- FQDN ACL は、IPv6 ACL とともにエンコードされ、AP に送信されます。
- FQDN ACL は常にカスタム ACL です。
- AP は、DNS スヌーピングを行い、IPv4 および IPv6 アドレスをコントローラに送信します。
- コントローラは、AP からのスヌーピング済み IP をデータベースに保存し、AP 間の内部 wncd ローミング中にメッセージを送信します。

Flex モードでサポートされている IPv6 機能

表 *1 : Flex* モードでサポートされている *IPv6* 機能

Flex モードの IPv6 機能	機能パリティのサポート
Flex クライアントの IPv6 ラーニング	○
認証前 IPv6 ACL	○
認証後 IPv6 ACL	○
認証前 DNS ACL	○
認証後 DNS ACL	対応

LWA および EWA の認証前 ACL の有効化

手順

	コマンドまたはアクション	目的
ステップ 1	**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 2	**wlan** *wlan-name wlan-id SSID-name* 例： `Device(config)# wlan wlan-demo 1 ssid-demo`	WLAN コンフィギュレーション サブモードを開始します。 • *wlan-name*：プロファイル名を入力します。入力できる範囲は英数字で 1 ～ 32 文字です。 • *wlan-id*：WLAN ID を入力します。範囲は 1 ～ 512 です。 • *SSID-name*：この WLAN に対する Service Set Identifier（SSID）を入力します。SSID を指定しない場合、WLAN プロファイル名は SSID として設定されます。 （注） すでに WLAN を設定している場合は、**wlan wlan-name** コマンドを入力します。
ステップ 3	**ipv6 traffic-filter web** *acl_name-preauth* 例： `Device(config-wlan)# ipv6 traffic-filter web preauth_v6_acl`	Web 認証の事前認証 ACL を作成します。
ステップ 4	**no security wpa** 例： `Device(config-wlan)# no security wpa`	WPA セキュリティを無効にします。
ステップ 5	**no security wpa wpa2 ciphers aes** 例： `Device(config-wlan)#no security wpa wpa2 ciphers aes`	AES の WPA2 暗号化を無効にします。

	コマンドまたはアクション	目的
ステップ 6	**no security wpa akm dot1x** 例： `Device(config-wlan)#no security wpa akm dot1x`	dot1x に対するセキュリティの AKM をディセーブルにします。
ステップ 7	**security dot1x authentication-list** *auth-list-name* 例： `Device(config-wlan)# security dot1x authentication-list default`	dot1x セキュリティ用のセキュリティ認証リストを有効にします。
ステップ 8	**security web-auth authentication-list** *authenticate-list-name* 例： `Device(config-wlan)# security web-auth authentication-list wcm_dot1x`	WLAN の認証リストを有効にします。
ステップ 9	**security web-auth parameter-map** *parameter-map-name* 例： `Device(config-wlan)# security web-auth parameter-map param-custom-webconsent`	パラメータ マップをマッピングします。
ステップ 10	**no shutdown** 例： `Device(config-wlan)# no shutdown`	WLAN を停止します。

LWA および EWA の認証後 ACL の有効化

手順

	コマンドまたはアクション	目的
ステップ 1	**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 2	**wireless profile policy** *profile-name* 例： `Device(config)# wireless profile policy test1`	WLAN のポリシー プロファイルを作成します。 *profile-name* はポリシー プロファイルのプロファイル名です。

	コマンドまたはアクション	目的
ステップ 3	**ipv6 acl** *acl_name* 例： `Device(config-wireless-policy)# ipv6 acl testacl`	名前付き WLAN ACL を作成します。
ステップ 4	**end** 例： `Device(config-wireless-policy)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

LWA および EWA の DNS ACL の有効化

（注） 認証後 DNS ACL はサポートされていません。

手順

	コマンドまたはアクション	目的
ステップ 1	**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 2	**wireless profile policy** *profile-name* 例： `Device(config)# wireless profile policy test1`	WLAN のポリシー プロファイルを作成します。 *profile-name* はポリシー プロファイルのプロファイル名です。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

WebAuth 認証前および認証後 ACL による Flex クライアントの IPv6 サポートの確認

L2 認証後のクライアントの状態を確認するには、次のコマンドを使用します。

```
Device# show wireless client summary
Number of Local Clients: 1
```

```
MAC Address    AP Name                           WLAN  State             Protocol Method
     Role
------------------------------------------------------------------------------------------
1491.82b8.f8c1 AP4001.7A03.544C                  4      Webauth Pending   11n(5)   None
      Local

Number of Excluded Clients: 0
```

IP の状態、ディスカバリ、および MAC を確認するには、次のコマンドを使用します。

```
Device# show wireless dev da ip
  IP                                        STATE       DISCOVERY   MAC
  ------------------------------------------------------------------------------------
  15.30.0.4                                 Reachable   ARP         1491.82b8.f8c1
  2001:15:30:0:d1d7:ecf3:7940:af60          Reachable   IPv6 Packet 1491.82b8.f8c1
  fe80::595e:7c29:d7c:3c84                  Reachable   IPv6 Packet 1491.82b8.f8c1
```