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 （1 ページ）
- DNS ベースのアクセス コントロール リストの制約事項 （3 ページ）
- フレックス モード （4 ページ）
- DNS ベースのアクセス コントロール リストの表示 （8 ページ）

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、組み込みワイヤレスコントローラで認証前 ACL を設定できます。

組み込みワイヤレスコントローラで 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。 組み込みワイヤレスコントローラは ACL 名で設定され、AAA サーバーから返されます。ACL 名が AAA サーバー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 サーバーは事前認証 ACL（url-redirect-acl：AAA サーバーに与えられた属性名）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 組み込みワイヤレス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 応答が解析されます。AP 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。

この機能は次のように URL リストをサポートします。

- 最大 32 個の URL リスト。
- URL リストごとに最大 32 個の URL。
- URL ごとに最大 30 個の IP アドレス。
- ワイルドカードを含む最大 16 個の URL リスト。
- ワイルドカードの URL ごとに最大 10 個の URL。

（注） ワイルドカードベースの URL を設定する場合、一般的なワイルドカード URL は使用できません。ドメイン名の間にワイルドカードを使用することはできません。1 つの URL に複数のワイルドカードを使用することはできません。URL でのワイルドカードの指定は、第 3 レベル以上のレベルでのみ使用できます。

（注） 競合する設定や無効な設定は使用できません。同じ URL に異なるアクションを設定することはできません。たとえば、拒否（Deny）許可（Allow）を www.yahoo.com で設定することはできません。

（注） ローカルモードの場合は、ポリシープロファイルに URL フィルタをアタッチする必要があります。フレックスモードでは、URL フィルタはフレックスプロファイルにアタッチされるため、ポリシープロファイルにアタッチする必要はありません。

（注） DNS ベースの URL は、クライアントからのアクティブな DNS クエリで機能します。したがって、URL フィルタリングでは、DNS を正しく設定する必要があります。

（注） URL フィルタは、パントまたはリダイレクト ACL、およびカスタムまたは静的事前認証 ACL よりも優先されます。

組み込みワイヤレスコントローラの FlexConnect

FlexConnect は、ブランチ オフィスとリモート オフィスに導入されるワイヤレス ソリューションです。このソリューションを使用することで、各ブランチオフィスで組み込みワイヤレスコントローラを展開することなく、企業オフィスからワイドエリアネットワーク（WAN）リンク経由で、ブランチまたはリモートオフィスのアクセスポイントを設定および制御できます。

FlexConnect アクセスポイントは、クライアント データ トラフィックをローカルに切り替え、認証を中央で実行できます。また、FlexConnect AP は、コントローラへの接続を失った場合にクライアント認証をローカルで実行できます。コントローラへの接続が回復した場合、認証とポリシーの詳細を組み込みワイヤレスコントローラに送り返すこともできます。

組み込みワイヤレス コントローラ ネットワークは、少なくとも 1 つの 802.11ax Wave 2 Cisco Aironet シリーズアクセスポイント（AP）と、ネットワーク内の他の AP を管理するソフトウェアベースの組み込みワイヤレスコントローラで構成されます。組み込みワイヤレスコントローラとして機能している AP をプライマリ AP といい、そのプライマリ AP によって管理されるネットワーク内の他の AP を下位 AP といいます。プライマリ AP は、組み込みワイヤレスコントローラとして機能するのに加え、下位 AP と連動してクライアントにサービスを提供する AP としても動作します。

事前認証 DNS ACL 機能は、ウォールドガーデン機能とも呼ばれます。ウォールドガーデンは、認証なしでアクセスできる Web サイトまたはドメインのリストです。DNS スヌーピングは各クライアントの AP で実行され、設定されたルールは送信元または宛先 IP と一致した後にクライアントトラフィックに適用されます。

ローミング

ローミング中、サポートクライアントは既存のローミングサポートを使用して AP 間をローミングします。DNS ACL は、ローミング後もターゲット AP で保持されます。DNS 事前認証 ACL および事後認証 ACL を使用したローミングの場合、ターゲット AP は、サービスを提供する AP からクライアントが解決した IP を学習します。

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。

- 中央認証を使用した FlexConnect ローカルスイッチング AP でのみサポートされています。
- AP が FlexConnect ローカル スイッチング モードにある場合、ローカル認証を使用した FlexConnect では認証後の DNS ベースの ACL はサポートされません。
- 完全修飾ドメイン名（FQDN）または DNS ベースの ACL は、Cisco Wave 1 アクセスポイントではサポートされていません。
- URL フィルタでは最初の 20 個の URL のみ考慮されますが、追加もできます。

- URL フィルタでは通常の正規表現パターンが採用され、ワイルドカード文字は URL の先頭または末尾でのみ使用できます。
- URL ACL が定義され、WLAN に関連付けられる FlexConnect ポリシープロファイルに追加されます。URL ACL は、ローカルモードの URL ACL と同様の方法で作成されます。
- FlexConnect モードでは、URL ドメイン ACL は、FlexConnect ポリシープロファイルに接続されている場合にのみ機能します。
- ポリシープロファイルを WLAN またはローカル ポリシーに関連付けることにより、ACL を WLAN に適用できます。ただし、「url-redirect-acl」を使用してオーバーライドできます。
- ISE から受信した Cisco AV ペアの場合、特定のクライアントに適用する必要があるポリシーは、ADD MOBILE の一部としてプッシュされます。

  message.
- AP が接続するか、既存の URL ACL が変更されて FlexConnect プロファイルに適用されると、マッピングされた URL フィルタリストとともに ACL 定義が AP にプッシュされます。
- AP は、マッピングされた ACL 名を使用して URL ACL 定義を保存し、DNS パケットをスヌープして、ACL の各 URL の最初の IP アドレスを学習します。AP は、IP アドレスを学習すると、URL および IP バインディングのコントローラを更新します。コントローラは、将来使用するためにこの情報をクライアントデータベースに記録します。
- 事前認証状態の間にクライアントが別の AP にローミングすると、学習した IP アドレスが新しい AP にプッシュされます。それ以外の場合、学習した IP アドレスは、クライアントが認証後の状態に移行したとき、または学習した IP アドレスの TTL が期限切れになったときに消去されます。

フレックス モード

URL フィルタリストの設定（CLI）

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** *custom-flex-profile* **例：** `Device(config)# wireless profile flex custom-flex-profile`	ワイヤレス flex プロファイルを設定し、ワイヤレス flex プロファイル 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	**acl-policy** *acl-policy-name* 例： `Device(config-wireless-flex-profile)#acl-policy acl-policy-name`	ACL ポリシーの説明を設定します。
ステップ 4	**urlfilter list** *url-filterlist-name* 例： `Device(config-wireless-flex-profile-acl)# urlfilter list url-filterlist-name`	URL フィルタリストの名前を設定して Flex プロファイルに適用します。 これは、ACL バインディング用の Flex URL フィルタ コンフィギュレーション コマンドです。

URL フィルタリストの設定（GUI）

手順

ステップ 1 [Configuration] > [Security] > [URL Filters] を選択します。
[URL Filters] ページが表示されます。

ステップ 2 [Add] ボタンをクリックします。
[Add URL Filters] ウィンドウが表示されます。

ステップ 3 [Type] ドロップダウンリストから、[PRE-AUTH] または [POST-AUTH] を選択します。

a) [POST-AUTH]：[IPv4] および [IPv6] の [Redirect Servers] を指定します。

ステップ 4 スライダを使用して、[Action] を [Permit] または [Deny] にします。

ステップ 5 [URLs] フィールドで URL を指定します。すべての URL を新しい行に入力します。

ステップ 6 [Apply to Device] をクリックします。

WLAN でのカスタム事前認証 DNS ACL の適用

事前認証の場合、この設定は Web 認証 WLAN 上にある必要があります。

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	**wlan***wlan-name wlan-id ssid-name* 例： `Device(config)# wlan wlan-name wlan-id ssid-name`	WLAN コンフィギュレーション サブモードを開始します。 1. 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。 2. wlan-id：WLAN ID を入力します。範囲は 1 ～ 512 です。 3. 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。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	**ip access-group web** *access-list-name* 例： `Device(config-wlan)#ip access-group web preauth-acl-wlan`	ACL を Web 認証 WLAN にマッピングします。 access-list-name は、IPv4 ACL の名前または ID です。

ポリシープロファイルでのカスタム事後認証 DNS ACL 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-name* 例： `Device(config)# wireless profile policy custom-policy-profile`	WLAN のポリシー プロファイルを作成します。
ステップ 3	{**ipv4** | **ipv6**} **acl** *post-acl-name* 例： `Device(config-wireless-policy)#ipv4 acl post-acl`	ワイヤレス IPv4 または IPv6 設定の ACL 設定を作成します。

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 または、[Common Tasks] セクションで、[Web Redirection] をオンにします。

ステップ 9 ドロップダウンリストから [Centralized Web Auth] オプションを選択します。

ステップ 10 ACL を指定し、ドロップダウンリストから ACL 値を選択します。

ステップ 11 [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。

（注） 優先順位に基づいて、複数の ACL をコントローラに適用できます。L2 認証 + WebAuth マルチ認証のシナリオでは、ISE が L2 認証中に ACL を返す場合、ISE ACL はデフォルトの WebAuth リダイレクト ACL よりも優先されるため、ISE ACL に許可ルールがある場合、トラフィックは WebAuth 保留状態で実行されます。このシナリオを回避するには、L2 認証 ISE から返される ACL の優先順位を設定する必要があります。デフォルトの WebAuth リダイレクト ACL の優先順位は 100 です。トラフィックの問題を回避するには、ISE によって返される ACL のリダイレクト ACL 優先順位を 100 より上の値に設定する必要があります。

ステップ 12 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-REDIRECT2
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 13 [Attributes Details] セクションの内容を確認し、[Save] をクリックします。

DNS ベースのアクセス コントロール リストの表示

URL リストを表示するには、次のコマンドを使用します。

```
Device #show wireless urlacl-enhanced summary
URL-List
--------------------------------
urllist_ut
urllist_max1
urllist_max2
urllist_max3
urllist_max4
urllist_max5
```

特定の URL リス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 wireless urlacl-enhanced details urllist_ut
List Name..................... : urllist_ut
Configured List of URLs
URL                  Preference Action Validity Invalidated URL
-------------------------------------------------------------------------------
url1.dns.com         1                 PERMIT         VALID 0
url2.dns.com         2                 DENY           VALID 0
url3.dns.com         3                 PERMIT         VALID 0
url4.dns.com         4                 DENY           VALID 0
url11.dns.com        6                 DENY           VALID 0
url12.dns.com        7                 PERMIT         VALID 0
url13.dns.com        8                 DENY           VALID 0
www.example.com      14                PERMIT         VALID 0
```

Flex プロファイルの詳細を表示するには、次のコマンドを使用します。

```
Device# sh wireless profile flex detailed custom-flex-profile
Flex Profile Name : custom-flex-profile
Description : custom flex profile
Local Auth :
        AP:
                Radius Enable            : ENABLED
                PEAP                     : DISABLED
                LEAP                     : DISABLED
                TLS                      : DISABLED
                EAP fast profile         : Not Configured
                User List                : Not Configured
        RADIUS:
                RADIUS server group name : Not Configured
        Fallback Radio shut              : DISABLED
        ARP caching                      : ENABLED
        Efficient Image Upgrade          : ENABLED
        OfficeExtend AP                  : DISABLED
        Join min latency                 : DISABLED
        Policy ACL :
                ACL Name                          URL Filter List
        Name                 Central Webauth
        ---------------------------------------------------------------
        post-acl                urllist_ut        DISABLED
        pre_v4              urllist_pre_cwa   DISABLED
        ACL-REDIRECTTTTTTT2     urllist_ut        DISABLED
        VLAN Name - VLAN ID mapping       : Not Configured
```

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#sh wireless client mac-address <Mac-address> detail
```

アクセスポイントの確認

AP の ACL の設定を表示するには、次のコマンドを使用します。

```
Device# show ip access-lists
Extended IP access list pre_v4
        1 permit udp any range 0 65535 any eq 53
        2 permit tcp any range 0 65535 any eq 53
        3 permit udp any dhcp_server any range 0 65535
        4 permit udp any range 0 65535 any eq 68
        5 permit udp any dhcp_client any range 0 65535
        6 deny ip any any
```

URL リストの設定を表示するには、次のコマンドを使用します。

```
Device#show flexconnect url-acl
ACL-NAME         ACTION         URL-LIST
pre_v4
                 allow          test.dns.com
                 allow          url2.dns.com
                 allow          url3.dns.com
                 allow          url10.dns.com
                 allow          url11.dns.com
                 allow          www.cwapre.com
                 allow          www.google.com
                 allow          oldconfig.dns.com
                 allow          *.cisco.com
```

事前認証クライアントの設定を表示するには、次のコマンドを使用します。

```
Device# show client access-lists pre-auth all C0:C1:C0:70:58:2F
Pre-Auth URL ACLs for Client: C0:C1:C0:70:58:2F
IPv4 ACL: pre_v4
IPv6 ACL:
ACTION         URL-LIST
allow          url1.dns.com
deny           url2.dns.com
allow          url3.dns.com
deny           url4.dns.com
allow          www.example.com
deny           url11.dns.com
allow          url12.dns.com
deny           url13.dns.com

Resolved IPs for Client: C0:C1:C0:70:58:2F
HIT-COUNT         URL         ACTION         IP-LIST
post-acl
        rule 0:   allow true
No IPv6 ACL found
```

事後認証クライアントの設定を表示するには、次のコマンドを使用します。

```
Device# show client access-lists post-auth all C0:C1:C0:70:58:2F
Post-Auth URL ACLs for Client: C0:C1:C0:70:58:2F
IPv4 ACL: post-acl
IPv6 ACL:
ACTION         URL-LIST
allow          url1.dns.com
deny           url2.dns.com
allow          url3.dns.com
deny           url4.dns.com
allow          www.example.com
deny           url11.dns.com
allow          url12.dns.com
deny           url13.dns.com
```

```
Resolved IPs for Client: C0:C1:C0:70:58:2F
HIT-COUNT         URL         ACTION         IP-LIST
post-acl
        rule 0: allow true
No IPv6 ACL found
```

事前認証で学習した IP を表示するには、次のコマンドを使用します。

```
Device#show client access-lists pre-auth all 60:14:B3:AA:C6:FB
Pre-Auth URL ACLs for Client: 60:14:B3:AA:C6:FB
IPv4 ACL: acl_1
IPv6 ACL:
ACTION         URL-LIST
allow          url1.dns.com
deny           url2.dns.com

Resolved IPs for Client: 60:14:B3:AA:C5:FB
HIT-COUNT         URL                 ACTION         IP-LIST
10                url1.dns.com        allow          9.10.8.1
```

事後認証で学習した IP を表示するには、次のコマンドを使用します。

```
Device#show client access-lists post-auth all 60:14:B3:AA:C6:FB
Post-Auth URL ACLs for Client: 60:14:B3:AA:C5:FB
IPv4 ACL: post_acl
IPv6 ACL:
ACTION         URL-LIST
deny           url1.dns.com
allow          url2.dns.com

Resolved IPs for Client: 60:14:B3:AA:C5:FB
HIT-COUNT         URL                 ACTION         IP-LIST
16                url2.dns.com        allow          9.10.9.1
postauth_acl
          rule 0: allow true
```

翻訳について
このドキュメントは、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。