



付録：FlexVPN の RADIUS 属性

この章では、FlexVPN サーバーでサポートされる RADIUS 属性について説明します。

- [FlexVPN RADIUS 属性 \(1 ページ\)](#)

FlexVPN RADIUS 属性

次に、FlexVPN サーバーによって使用される RADIUS 属性カテゴリを示します。

- インバウンドおよび双方向 IETF RADIUS 属性
- アウトバウンド ローカル
- アウトバウンド リモート



(注) 次のリストに含まれていない FlexVPN サーバーによって RADIUS に送信されるインバウンド属性では、値は AAA システムによって設定されます。

属性	User-Name
タイプ	IETF
書式	文字列
属性 ID	1

説明	<p>この属性は、FlexVPN サーバーによって RADIUS に送信され、次のように取得されます。</p> <ul style="list-style-type: none"> • AAA ベースの事前共有キー：ピア IKEv2 ID • EAP 認証：ピア EAP ID • ユーザー認証またはグループ認証：name mangler の出力または IKEv2 プロファイル認証コマンドで指定された文字列。 • アカウンティング：ピア EAP ID または IKEv2 ID。 <p>この属性は、正常な EAP 認証後に Access-Accept で RADIUS から受信されることもあります。また、認証済みのピア EAP ID を指定します。</p>
属性	User-Password
タイプ	IETF
書式	文字列
属性 ID	2
説明	<p>この属性は、FlexVPN サーバーによって RADIUS に送信され、次のように取得されます。</p> <ul style="list-style-type: none"> • AAA ベースの事前共有キー：「cisco」 • ユーザー/グループ認証：「cisco」
属性	Calling-Station-ID
タイプ	IETF
書式	文字列
属性 ID	31
説明	<p>この属性は、FlexVPN サーバーによって RADIUS に送信され、次のように取得されます。</p> <ul style="list-style-type: none"> • AAA ベースの事前共有キー：IKEv2 発信側アドレス • EAP 認証：IKEv2 発信側アドレス • ユーザー/グループ認証：IKEv2 発信側アドレス
属性	Service-Type
タイプ	IETF

書式	文字列
属性 ID	6
説明	この属性は、FlexVPN サーバーによって EAP 認証に使用されており、この属性の値は「Login」に設定されています。

属性	EAP-Message
タイプ	IETF
書式	文字列
属性 ID	79
説明	この属性は、FlexVPN サーバーによって EAP 認証に使用されており、EAP サーバーとリモート アクセス クライアントの間で EAP パケットをリレーします。

属性	Message-Authenticator
タイプ	IETF
書式	文字列
属性 ID	80
説明	この属性は、FlexVPN サーバーによって EAP 認証用に送信されます。この属性の値は、AAA サブシステムによって設定されます。

属性	Framed-Pool
タイプ	IETF
書式	文字列
属性 ID	88
ローカル設定	pool name
RADIUS 設定	Framed-Pool= <i>pool-name</i>
説明	FlexVPN サーバーが IPv4 アドレスの割り当てに使用する IPv4 アドレスプールの名前を指定して、クライアントに割り当てます。割り当てられたアドレスは、IKEv2 標準設定属性の INTERNAL_IP4_ADDRESS を介してクライアントにプッシュされます。

属性	ipsec:group-dhcp-server
タイプ	Cisco AV ペア

書式	文字列
ローカル設定	dhcp server { <i>ipaddr</i> <i>host</i> }
RADIUS 設定	cisco-avpair="ipsec: group-dhcp-server= <i>ipaddr</i> "
説明	FlexVPN サーバーが IPv4 アドレスのリースに使用する IPv4 DHCP サーバーを指定して、クライアントに割り当てます。リースされたアドレスは、IKEv2 標準設定属性の INTERNAL_IP4_ADDRESS を介してクライアントにプッシュされます。

属性	ipsec:dhcp-giaddr
タイプ	Cisco AV ペア
書式	IPAddr
ローカル設定	dhcp giaddr <i>ipaddr</i>
RADIUS 設定	cisco-avpair="psec: dhcp-giaddr= <i>ipaddr</i> "
説明	FlexVPN サーバーが DHCP サーバーへの接続に使用する IPv4 DHCP ゲートウェイ IP アドレスを指定します。

属性	ipsec:dhcp-timeout
タイプ	Cisco AV ペア
書式	整数
ローカル設定	dhcp timeout <i>seconds</i>
RADIUS 設定	cisco-avpair="ipsec:dhcp-timeout= <i>seconds</i> "
説明	FlexVPN サーバーが DHCP サーバーからの応答をタイムアウトするのに使用する、IPv4 DHCP サーバーからの応答の待機時間を指定します。

属性	ipsec:ipv6-addr-pool
タイプ	Cisco AV ペア
書式	文字列
ローカル設定	ipv6 <i>pool name</i>
RADIUS 設定	cisco-avpair="ipsec:ipv6-addr-pool= <i>pool-name</i> "

説明	FlexVPN サーバーが IPv6 アドレスの割り当てに使用する IPv6 アドレス プールの名前を指定して、クライアントに割り当てます。割り当てられたアドレスは、IKEv2 標準設定属性の INTERNAL_IP6_ADDRESS を介してクライアントにプッシュされます。
属性	ipsec:route-set=prefix
タイプ	Cisco AV ペア
書式	文字列
ローカル設定	該当なし
RADIUS 設定	cisco-avpair="ipsec:route-set=prefix <i>prefix/length</i> "
例	ipsec:route-set=prefix 192.168.1.0/24
説明	FlexVPN サーバーによって保護されるサブネットを指定します。これは、IKEv2 標準設定属性の INTERNAL_IP4_SUBNET を介してクライアントにプッシュされます。 (注) この AV ペアは、Cisco IOS リリース 15.2(2)T で導入されました。
属性	ipsec:route-set=interface
タイプ	Cisco AV ペア
書式	文字列
ローカル設定	route set interface
RADIUS 設定	cisco-avpair="ipsec:route-set=interface"
説明	この属性はローカルに使用され、IKEv2 標準設定属性の INTERNAL_IP4_SUBNET を介したピアへの VPN インターフェイス IP アドレスの送信を有効にします。これによって、BGP over VPN などのルーティングプロトコルが実行されます。 (注) Cisco IOS リリース 15.2(2)T で、「ipsec:route-set-interface」 AV ペアからこの AV ペアに置き換えられました。
属性	ipsec:route-accept
タイプ	Cisco AV ペア
書式	文字列
ローカル設定	route accept any [tag <i>tag-id</i>] [distance <i>distance</i>]

RADIUS 設定	cisco-avpair="ipsec:route-accept=any [tag:tag] [distance:distance]"
例	ipsec:route-accept=any tag=100
説明	<p>この属性はローカルに使用され、IKEv2 標準設定属性の INTERNAL_IP4_SUBNET を介してピアから受信されるサブネットのフィルタを指定します。この属性は、フィルタ処理されたサブネット用に IKEv2 よって追加されるルートのタグと距離も指定します。</p> <p>(注) Cisco IOS リリース 15.2(2)T で、AV ペア「ipsec:route-accept=accept acl:any」から「ipsec:route-accept=any」に置き換えられ、AV ペア「ipsec:route-accept=deny」から「ipsec:route-accept=none」に置き換えられました。</p>
属性	ipsec:ipsec-flow-limit
タイプ	Cisco AV ペア
書式	整数
ローカル設定	ipsec flow-limit <i>limit</i>
RADIUS 設定	cisco-avpair="ipsec:ipsec-flow-limit= <i>limit</i> "
説明	<p>この属性は FlexVPN サーバーによって使用され、IPSec dVTI セッションが使用可能な IPSec SA の最大数を指定します。デフォルトでは制限はありません。このパラメータは crypto ipsec profile コマンドおよび set security-policy limit コマンドと同様です。</p>
属性	ip:interface-config
タイプ	Cisco AV ペア
書式	文字列
ローカル設定	aaa attribute list <i>list</i> attribute type interface-config <i>string</i>
RADIUS 設定	cisco-avpair="ip:interface-config=interface cmd string"
例	ip:interface-config=ip vrf forwarding red
説明	<p>この属性はローカルに使用され、セッションの仮想アクセス インターフェイスに適用される インターフェイス コンフィギュレーション モードのコマンド文字列を指定します。ローカル設定の場合、IKEv2 認証ポリシーは、interface-config 属性が必要な AAA 属性リストを示します。</p>
属性	Tunnel-Type

タイプ	IETF
書式	整数
属性 ID	64
RADIUS 設定	Tunnel-Type=type
説明	この属性は、トンネルタイプ（ESP、AH、GRE など）を指定し、FlexVPN サーバーが RADIUS サーバーからセッションの事前共有キーを取得するときに受信されます。

属性	Tunnel-Medium-Type
タイプ	IETF
書式	整数
属性 ID	65、
RADIUS 設定	Tunnel-Medium-Type=type
説明	この属性は、トンネル転送タイプ（IPv4、IPv6 など）を指定し、FlexVPN サーバーが RADIUS サーバーからセッションの事前共有キーを取得するときに受信されます。

属性	Tunnel-Password
タイプ	IETF
書式	文字列
属性 ID	69
RADIUS 設定	Tunnel-Password=string
説明	この属性は、対称の事前共有キーを指定し、FlexVPN サーバーが RADIUS サーバーからセッションの事前共有キーを取得するときに受信されます。

属性	ipsec:ikev2-password-local
タイプ	Cisco AV ペア
書式	文字列
RADIUS 設定	cisco-avpair="ipsec:ikev2-password-local=string"
説明	この属性は、ローカルの事前共有キーを指定し、FlexVPN サーバーが RADIUS サーバーからセッションの事前共有キーを取得するときに受信されます。

属性	ipsec:ikev2-password-remote
タイプ	Cisco AV ペア
書式	文字列
RADIUS 設定	cisco-avpair="ipsec:ikev2-password-remote= <i>string</i> "
説明	この属性は、リモートの事前共有キーを指定し、FlexVPN サーバーが RADIUS サーバーからセッションの事前共有キーを取得するときに受信されます。
属性	Framed-IP-Address
タイプ	IETF
書式	IPAddr
属性 ID	8
RADIUS 設定	Framed-IP-Address= <i>ipaddr</i>
説明	クライアントに割り当てられる IPv4 アドレスを指定します。これは、IKEv2 標準設定属性の INTERNAL_IP4_ADDRESS を介してクライアントにプッシュされます。
属性	Framed-IP-Netmask
タイプ	IETF
書式	IPAddr
属性 ID	9
ローカル設定	netmask <i>mask</i>
RADIUS 設定	Framed-IP-Netmask= <i>mask</i>
説明	クライアントに割り当てられる IPv4 アドレスのサブネット マスクを指定します。これは、IKEv2 標準設定属性の INTERNAL_IP4_NETMASK を介してクライアントにプッシュされます。
属性	ipsec:dns-servers
タイプ	Cisco AV ペア
書式	文字列
ローカル設定	dns <i>primary</i> [<i>secondary</i>]
RADIUS 設定	cisco-avpair="ipsec:dns-servers= <i>primary secondary</i> "

説明	クライアントのプライマリ IPv4 DNS サーバーおよびセカンダリ IPv4 DNS サーバーを指定します。これは、IKEv2 標準設定属性の INTERNAL_IP4_DNS を介してクライアントにプッシュされます。
属性	ipsec:wins-servers
タイプ	Cisco AV ペア
書式	文字列
ローカル設定	wins <i>primary</i> [<i>secondary</i>]
RADIUS 設定	cisco-avpair="ipsec:wins-servers= <i>primary secondary</i> "
説明	クライアントのプライマリ IPv4 WINS サーバーおよびセカンダリ IPv4 WINS サーバーを指定します。これは、IKEv2 標準設定属性の INTERNAL_IP4_NBNS を介してクライアントにプッシュされます。
属性	ipsec:route-set=access-list
タイプ	Cisco AV ペア
書式	文字列
ローカル設定	route set access-list { <i>acl-name</i> <i>acl-number</i> }
RADIUS 設定	cisco-avpair="ipsec:route-set=access-list { <i>acl-name</i> <i>acl-number</i> }"
説明	FlexVPN サーバーによって保護される IPv4 サブネットを指定します。これは、IKEv2 標準設定属性の INTERNAL_IP4_SUBNET を介してクライアントにプッシュされます。 (注) Cisco IOS リリース 15.2(2)T で、「ipsec:inacl」AV ペアからこの AV ペアに置き換えられました。
属性	ipsec:addrv6
タイプ	Cisco AV ペア
書式	文字列
RADIUS 設定	cisco-avpair="ipsec:addrv6= <i>ipv6-addr</i> "
説明	クライアントに割り当てられる IPv6 アドレスを指定します。これは、最初の 16 バイトで IKEv2 標準設定属性の INTERNAL_IP6_ADDRESS を介してクライアントにプッシュされます。
属性	ipsec:prefix-len

タイプ	Cisco AV ペア
書式	整数
ローカル設定	該当なし
RADIUS 設定	cisco-avpair="ipsec:prefix-len= <i>value</i> "
例	ipsec:prefix-len=24
説明	クライアントに割り当てられる IPv6 アドレスのプレフィックス長を指定します。これは、最後（17 番目）のバイトで IKEv2 標準設定属性の INTERNAL_IP6_ADDRESS を介してクライアントにプッシュされます。

属性	ipsec:ipv6-dns-servers-addr
タイプ	Cisco AV ペア
書式	文字列
ローカル設定	ipv6 dns <i>primary</i> [<i>secondary</i>]
RADIUS 設定	cisco-avpair="ipsec: ipv6-dns-servers-addr= <i>ipaddr1</i> * <i>ipaddr2</i> "
説明	クライアントのプライマリ IPv6 DNS サーバーおよびセカンダリ IPv6 DNS サーバーを指定します。これは、IKEv2 標準設定属性の INTERNAL_IP6_DNS を介してクライアントにプッシュされます。

属性	ipsec:route-set=access-list ipv6
タイプ	Cisco AV ペア
書式	文字列
ローカル設定	route set access-list ipv6 <i>acl-name</i>
RADIUS 設定	cisco-avpair="ipsec:route-set=access-list ipv6 <i>acl-name</i> "
説明	FlexVPN サーバーによって保護される IPv6 サブネットを指定します。これは、IKEv2 標準設定属性の INTERNAL_IP6_SUBNET を介してクライアントにプッシュされます。 (注) Cisco IOS リリース 15.2(2)T で、「ipsec:ipv6-subnet-acl」AV ペアからこの AV ペアに置き換えられました。

属性	ipsec:banner
タイプ	Cisco AV ペア
書式	文字列

ローカル設定	<code>banner text</code>
RADIUS 設定	<code>cisco-avpair="ipsec:banner=text"</code>
説明	バナーテキストを指定します。これは、Cisco Unity 属性の MODECFG_BANNER を介してクライアントにプッシュされます。
属性	<code>ipsec:default-domain</code>
タイプ	Cisco AV ペア
書式	文字列
ローカル設定	<code>def-domain name</code>
RADIUS 設定	<code>cisco-avpair="ipsec:default-domain=name"</code>
説明	デフォルト ドメインを指定します。これは、Cisco Unity 属性の MODECFG_DEFDOMAIN を介してクライアントにプッシュされます。
属性	<code>ipsec:split-dns</code>
タイプ	Cisco AV ペア
書式	文字列
ローカル設定	<code>split-dns name</code>
RADIUS 設定	<code>cisco-avpair="ipsec:split-dns=name"</code>
説明	スプリット DNS 名を指定します。これは、Cisco Unity 属性の MODECFG_SPLITDNS_NAME を介してクライアントにプッシュされます。最大 10 個のスプリット DNS 名を設定できます。
属性	<code>ipsec:ipsec-backup-gateway</code>
タイプ	Cisco AV ペア
書式	文字列
ローカル設定	<code>backup-gateway name</code>
RADIUS 設定	<code>cisco-avpair="ipsec:ipsec-backup-gateway=name"</code>
説明	バックアップ ゲートウェイを指定します。これは、Cisco Unity 属性の MODECFG_BACKUPSERVERS を介してクライアントにプッシュされます。最大 10 のバックアップ ゲートウェイを設定できます。
属性	<code>ipsec:pfs</code>

タイプ	Cisco AV ペア
書式	整数
ローカル設定	pfs
RADIUS 設定	cisco-avpair="ipsec:pfs= <i>value</i> "
説明	IPsec PFS (Perfect Forward Secrecy) の有効/無効を指定します。これは、Cisco Unity 属性の MODECFG_PFS を介してクライアントにプッシュされます。値は、無効の場合は 0、有効の場合は 1 にする必要があります。

属性	ipsec:include-local-lan
タイプ	Cisco AV ペア
書式	整数
ローカル設定	include-local-lan
RADIUS 設定	cisco-avpair="ipsec:include-local-lan= <i>value</i> "
説明	ローカル LAN の包含を有効または無効にします。これは、Cisco Unity 属性の MODECFG_INCLUDE_LOCAL_LAN を介してクライアントにプッシュされます。値は、無効の場合は 0、有効の場合は 1 にする必要があります。

属性	ipsec:smartcard-removal-disconnect
タイプ	Cisco AV ペア
書式	整数
ローカル設定	smartcard-removal-disconnect
RADIUS 設定	cisco-avpair="ipsec:smartcard-removal-disconnect= <i>value</i> "
説明	スマートカードが取り外されたときの切断を有効または無効にします。これは、Cisco Unity 属性の MODECFG_SMARTCARD_REMOVAL_DISCONNECT を介してクライアントにプッシュされます。値は、無効の場合は 0、有効の場合は 1 にする必要があります。

属性	ipsec:configuration-url
タイプ	Cisco AV ペア
書式	文字列
ローカル設定	configuration url <i>url</i>
RADIUS 設定	cisco-avpair="ipsec:configuration-url= <i>url</i> "

説明	設定ダウンロードの URL を指定します。これは、Cisco FlexVPN 属性の MODECFG_CONFIG_URL を介してクライアントにプッシュされます。
属性	ipsec:configuration-version
タイプ	Cisco AV ペア
書式	整数
ローカル設定	configuration version <i>version</i>
RADIUS 設定	cisco-avpair="ipsec:configuration-version= <i>version</i> "
説明	ダウンロードする設定のバージョンを指定します。これは、Cisco FlexVPN 属性の MODECFG_CONFIG_VERSION を介してクライアントにプッシュされます。
属性	Route-set remote
タイプ	Cisco AV ペア
書式	文字列
ローカル設定	route set remote {ipv4 ip-address mask ipv6 ip-address/mask}
RADIUS 設定	cisco-avpair="ipsec:route-set=remote {ipv4 network subnet_mask ipv6 network/subnet_mask}"
説明	FlexVPN サーバーによって保護されるサブネットを指定します。これは、IKEv2 標準設定属性の INTERNAL_IP4_SUBNET を介してクライアントにプッシュされます。ルートセットプレフィックスは 10 進数形式で表されたサブネットマスク（例：/24）で機能しますが、ルートセットリモートには標準のサブネットマスク表現（例：255.255.255.0）が必要です。 (注) この AV ペアは、Cisco IOS リリース 3.10.0S で導入されました。
属性	Route-set local
タイプ	Cisco AV ペア
書式	文字列
ローカル設定	route set local {ipv4 ip-address mask ipv6 ip-address/mask}
RADIUS 設定	cisco-avpair="ipsec:route-set=local {ipv4 network subnet_mask ipv6 network/subnet_mask}"

説明	<p>この属性は、リモートデバイスから受信したルーティング情報を信頼する必要がないエクストラネットのシナリオで役立ちます。言い換えると、この AV ペアを使用して、リモートルートを拒否し、ルートの追加をローカルに制御できます。</p> <p>(注) この AV ペアは、Cisco IOS リリース 3.10.0S で導入されました。</p>
----	---

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。