AAA の RADIUS サーバ

この章では、AAA 用に RADIUS サーバを設定する方法について説明します。

AAA 用の RADIUS サーバについて

Cisco ASA は AAA について、次の RFC 準拠 RADIUS サーバをサポートしています。

- Cisco Secure ACS 3.2、4.0、4.1、4.2、および 5.x
- Cisco Identity Services Engine（ISE）
- RSA 認証マネージャ 5.2、6.1 および 7.x の RSA Radius
- Microsoft

サポートされている認証方式

ASA は、RADIUS サーバでの次の認証方式をサポートします。

- PAP：すべての接続タイプの場合。
- CHAP および MS-CHAPv1：L2TP-over-IPsec 接続の場合。
- MS-CHAPv2：L2TP-over-IPsec 接続の場合。また、パスワード管理機能がイネーブルで、通常の IPsec リモート アクセス接続の場合。MS-CHAPv2 は、クライアントレス接続でも使用できます。
- 認証プロキシ モード：RADIUS から Active Directory、RADIUS から RSA/SDI、Radius からトークン サーバ、RSA/SDI から RADIUS の各接続。

（注） MS-CHAPv2 を、ASA と RADIUS サーバの間の VPN 接続で使用されるプロトコルとしてイネーブルにするには、トンネル グループ一般属性でパスワード管理をイネーブルにする必要があります。パスワード管理を有効にすると、ASA から RADIUS サーバへの MS-CHAPv2 認証要求が生成されます。詳細については、**password-management** コマンドの説明を参照してください。

二重認証を使用し、トンネル グループでパスワード管理をイネーブルにした場合は、プライマリ認証要求とセカンダリ認証要求に MS-CHAPv2 要求属性が含まれます。RADIUS サーバが MS-CHAPv2 をサポートしない場合は、**no mschapv2-capable** コマンドを使用して、そのサーバが MS-CHAPv2 以外の認証要求を送信するように設定できます。

VPN 接続のユーザ認証

ASA は、RADIUS サーバを使用して、ダイナミック ACL またはユーザごとの ACL 名を使用する VPN リモート アクセスおよびファイアウォール カットスルー プロキシ セッションのユーザ許可を実行できます。ダイナミック ACL を実装するには、これをサポートするように RADIUS サーバを設定する必要があります。ユーザを認証する場合、RADIUS サーバによってダウンロード可能 ACL、または ACL 名が ASA に送信されます。所定のサービスへのアクセスが ACL によって許可または拒否されます。認証セッションの有効期限が切れると、ASA は ACL を削除します。

ACL に加えて、ASA は、VPN リモート アクセスおよびファイアウォール カットスルー プロキシセッションの認証およびアクセス許可の設定を行うための多くの属性をサポートしています。

RADIUS 属性のサポートされるセット

ASA は次の RADIUS 属性のセットをサポートしています。

- RFC 2138 に定義されている認証属性
- RFC 2139 に定義されているアカウンティング属性
- RFC 2868 に定義されているトンネル プロトコル サポート用の RADIUS 属性
- Cisco IOS ベンダー固有属性（VSA）は、RADIUS ベンダー ID 9 で識別されます。
- RADIUS ベンダー ID 3076 によって識別される Cisco VPN 関連 VSA
- RFC 2548 に定義されている Microsoft VSA

サポートされる RADIUS 認証属性

認可では、権限または属性を使用するプロセスを参照します。認証サーバとして定義されているRADIUSサーバは、権限または属性が設定されている場合はこれらを使用します。これらの属性のベンダー ID は 3076 です。

次の表に、ユーザ認可に使用可能な、サポートされている RADIUS 属性の一覧を示します。

（注） RADIUS 属性名には、cVPN3000 プレフィックスは含まれていません。Cisco Secure ACS 4.x は、この新しい名前をサポートしますが、4.0 以前の ACS の属性名にはまだ cVPN3000 プレフィックスが含まれています。ASA は、属性名ではなく数値の属性 ID に基づいて RADIUS 属性を使用します。

次の表に示した属性はすべてダウンストリーム属性であり、RADIUS サーバから ASA に送信されます。ただし、属性番号146、150、151、および152を除きます。これらの属性番号はアップストリーム属性であり、ASA から RADIUS サーバに送信されます。RADIUS 属性 146 および 150 は、認証および認可の要求の場合に ASA から RADIUS サーバに送信されます。前述の 4 つの属性はすべて、アカウンティング開始、中間アップデート、および終了の要求の場合に ASA から RADIUS サーバに送信されます。アップストリーム RADIUS 属性 146、150、151、152 は、バージョン 8.4(3) で導入されました。

表 *1*：サポートされる *RADIUS* 認証属性

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
Access-Hours	Y	1	文字列	シングル	時間範囲の名前（Business-hours など）
Access-List-Inbound	Y	86	文字列	シングル	ACL ID
Access-List-Outbound	Y	87	文字列	シングル	ACL ID
Address-Pools	Y	217	文字列	シングル	IP ローカルプールの名前
Allow-Network-Extension-Mode	Y	64	ブール	シングル	0 = 無効1 = 有効
Authenticated-User-Idle-Timeout	Y	50	整数	シングル	1 ～ 35791394 分

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
Authorization-DN-Field	Y	67	文字列	シングル	有効な値：UID、OU、O、CN、L、SP、C、EA、T、N、GN、SN、I、GENQ、DNQ、SER、use-entire-name
Authorization-Required		66	整数	シングル	0 = いいえ 1 = はい
Authorization-Type	Y	65	整数	シングル	0 = なし 1 = RADIUS 2 = LDAP
Banner1	Y	15	文字列	シングル	Cisco VPN リモート アクセス セッション（IPsec IKEv1、AnyConnect SSL-TLS/DTLS/IKEv2、およびクライアントレス SSL）に対して表示されるバナー文字列
Banner2	Y	36	文字列	シングル	Cisco VPN リモート アクセス セッション（IPsec IKEv1、AnyConnect SSL-TLS/DTLS/IKEv2、およびクライアントレス SSL）に対して表示されるバナー文字列。Banner2 文字列は Banner1 文字列に連結されます（設定されている場合）。
Cisco-IP-Phone-Bypass	Y	51	整数	シングル	0 = 無効1 = 有効
Cisco-LEAP-Bypass	Y	75	整数	シングル	0 = 無効1 = 有効

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
クライアントタイプ	Y	150	整数	シングル	1 = Cisco VPN Client（IKEv1） 2 = AnyConnect Client SSL VPN 3 = Clientless SSL VPN 4 = Cut-Through-Proxy 5 = L2TP/IPsec SSL VPN 6 = AnyConnect Client IPsec VPN（IKEv2）
Client-Type-Version-Limiting	Y	77	文字列	シングル	IPsec VPN のバージョン番号を示す文字列
DHCP-Network-Scope	Y	61	文字列	シングル	IP アドレス
Extended-Authentication-On-Rekey	Y	122	整数	シングル	0 = 無効1 = 有効
Framed-Interface-Id	Y	96	文字列	シングル	割り当てられた IPv6 インターフェイス ID。完全に割り当てられた IPv6 アドレスを作成するために、Framed-IPv6-Prefix と組み合わせます。例：Framed-Interface-ID=1:1:1:1 と Framed-IPv6-Prefix=2001:0db8::/64 を組み合わせると、IP アドレス 2001:0db8::1:1:1:1 が得られます。

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
Framed-IPv6-Prefix	Y	97	文字列	シングル	割り当てられた IPv6 プレフィックスと長さ。完全に割り当てられた IPv6 アドレスを作成するために、Framed-Interface-Id と組み合わせます。例：プレフィックス 2001:0db8::/64 と Framed-Interface-Id=1:1:1:1 を組み合わせると、IP アドレス 2001:0db8::1:1:1:1 が得られます。この属性を使用し、プレフィックス長 /128 の完全な IPv6 アドレスを割り当てて、Framed-Interface-Id を使用せずに IP アドレスを割り当てることができます。例：Framed-IPv6-Prefix=2001:db8::1/128。

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
Group-Policy	Y	25	文字列	シングル	リモートアクセス VPN セッションのグループポリシーを設定します。バージョン 8.2.x 以降では、IETF-Radius-Class の代わりにこの属性を使用します。次の形式のいずれかを使用できます。 • グループポリシー名 • OU=グループポリシー名 • OU=グループポリシー名;
IE-Proxy-Bypass-Local		83	整数	シングル	0 = なし 1 = ローカル
IE-Proxy-Exception-List		82	文字列	シングル	改行（\n）区切りの DNS ドメインのリスト
IE-Proxy-PAC-URL	Y	133	文字列	シングル	PAC アドレス文字列
IE-Proxy-Server		80	文字列	シングル	IP アドレス
IE-Proxy-Server-Policy		81	整数	シングル	1 = 変更なし 2 = プロキシなし 3 = 自動検出 4 = コンセントレータ設定を使用する
IKE-KeepAlive-Confidence-Interval	Y	68	整数	シングル	10 ～ 300 秒
IKE-Keepalive-Retry-Interval	Y	84	整数	シングル	2 ～ 10 秒
IKE-Keep-Alives	Y	41	ブール	シングル	0 = 無効1 = 有効

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
Intercept-DHCP-Configure-Msg	Y	62	ブール	シングル	0 = 無効1 = 有効
IPsec-Allow-Passwd-Store	Y	16	ブール	シングル	0 = 無効1 = 有効
IPsec-Authentication		13	整数	シングル	0 = なし 1 = RADIUS 2 = LDAP（認可のみ） 3 = NT ドメイン 4 = SDI 5 = 内部 6 = RADIUS での Expiry 認証 7 = Kerberos/Active Directory
IPsec-Auth-On-Rekey	Y	42	ブール	シングル	0 = 無効1 = 有効
IPsec-Backup-Server-List	Y	60	文字列	シングル	サーバ アドレス（スペース区切り）
IPsec-Backup-Servers	Y	59	文字列	シングル	1=クライアントが設定したリストを使用する 2 = クライアントリストをディセーブルにして消去する 3 = バックアップ サーバ リストを使用する
IPsec-Client-Firewall-Filter-Name		57	文字列	シングル	クライアントにファイアウォール ポリシーとして配信するフィルタの名前を指定します。
IPsec-Client-Firewall-Filter-Optional	Y	58	整数	シングル	0 = 必須 1 = オプション
IPsec-Default-Domain	Y	28	文字列	シングル	クライアントに送信するデフォルト ドメイン名を 1 つだけ指定します（1 ～ 255 文字）。

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
IPsec-IKE-Peer-ID-Check	Y	40	整数	シングル	1 = 必須 2 = ピア証明書でサポートされる場合 3 = チェックしない
IPsec-IP-Compression	Y	39	整数	シングル	0 = 無効1 = 有効
IPsec-Mode-Config	Y	31	ブール	シングル	0 = 無効1 = 有効
IPsec-Over-UDP	Y	34	ブール	シングル	0 = 無効1 = 有効
IPsec-Over-UDP-Port	Y	35	整数	シングル	4001 ～ 49151。デフォルトは 10000 です。
IPsec-Required-Client-Firewall-Capability	Y	56	整数	シングル	0 = なし 1 = リモート FW Are-You-There（AYT）で定義されているポリシー 2 = Policy pushed CPP 4 = サーバからのポリシー
IPsec-Sec-Association		12	文字列	シングル	セキュリティアソシエーションの名前
IPsec-Split-DNS-Names	Y	29	文字列	シングル	クライアントに送信するセカンダリドメイン名のリストを指定します（1 ～ 255 文字）。
IPsec-Split-Tunneling-Policy	Y	55	整数	シングル	0 = スプリット トンネリングなし 1 = スプリット トンネリング 2 = ローカル LAN を許可

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
IPsec-Split-Tunnel-List	Y	27	文字列	シングル	スプリットトンネルの包含リストを記述したネットワークまたはACLの名前を指定します。
IPsec-Tunnel-Type	Y	30	整数	シングル	1 = LAN-to-LAN 2 = リモート アクセス
IPsec-User-Group-Lock		33	ブール	シングル	0 = 無効1 = 有効
IPv6-Address-Pools	Y	218	文字列	シングル	IP ローカル プール IPv6 の名前
IPv6-VPN-Filter	Y	219	文字列	シングル	ACL 値
L2TP-Encryption		21	整数	シングル	ビットマップ： 1 = 暗号化が必要 2 = 40 ビット 4 = 128 ビット 8 = ステートレスが必要 15 = 40/128 ビットで暗号化/ステートレスが必要
L2IP-MPPC-Compression		38	整数	シングル	0 = 無効1 = 有効
Member-Of	Y	145	文字列	シングル	カンマ区切りの文字列。例： `Engineering, Sales` ダイナミック アクセス ポリシーで使用できる管理属性。グループ ポリシーは設定されません。
MS-Client-Subnet-Mask	Y	63	ブール	シングル	IP アドレス
NAC-Default-ACL		92	文字列		ACL

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
NAC-Enable		89	整数	シングル	0 = いいえ 1 = はい
NAC-Revalidation-Timer		91	整数	シングル	300 ～ 86400 秒
NAC-Settings	Y	141	文字列	シングル	NAC ポリシーの名前
NAC-Status-Query-Timer		90	整数	シングル	30 ～ 1800 秒
Perfect-Forward-Secrecy-Enable	Y	88	ブール	シングル	0 = いいえ 1 = はい
PPTP-Encryption		20	整数	シングル	ビットマップ： 1 = 暗号化が必要 2 = 40 ビット 4 = 128 ビット 8 = ステートレスが必要 15 = 40/128 ビットで暗号化/ステートレスが必要
PPTP-MPPC-Compression		37	整数	シングル	0 = 無効1 = 有効
Primary-DNS	Y	5	文字列	シングル	IP アドレス
Primary-WINS	Y	7	文字列	シングル	IP アドレス
Privilege-Level	Y	220	整数	シングル	0 ～ 15 の整数。
Required-Client-Firewall-Vendor-Code	Y	45	整数	シングル	1 = Cisco Systems （Cisco Integrated Client を使用） 2 = Zone Labs 3 = NetworkICE 4 = Sygate 5 = Cisco Systems （Cisco Intrusion Prevention Security Agent を使用）
Required-Client-Firewall-Description	Y	47	文字列	シングル	文字列

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
Required-Client-Firewall-Product-Code	Y	46	整数	シングル	シスコ製品： 1 = Cisco Intrusion Prevention Security Agent または Cisco Integrated Client（CIC） Zone Labs 製品： 1 = Zone Alarm 2 = Zone AlarmPro 3 = Zone Labs Integrity NetworkICE 製品： 1 = BlackIce Defender/Agent Sygate 製品： 1 = Personal Firewall 2 = Personal Firewall Pro 3 = Security Agent
Required-Individual-User-Auth	Y	49	整数	シングル	0 = 無効1 = 有効
Require-HW-Client-Auth	Y	48	ブール	シングル	0 = 無効1 = 有効
Secondary-DNS	Y	6	文字列	シングル	IP アドレス
Secondary-WINS	Y	8	文字列	シングル	IP アドレス
SEP-Card-Assignment		9	整数	シングル	未使用
Session Subtype	Y	152	整数	シングル	0 = なし 1 =クライアントレス 2=クライアント 3=クライアントのみ Session Subtype が適用されるのは、Session Type（151）属性の値が 1、2、3、または 4 の場合のみです。

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
Session Type	Y	151	整数	シングル	0 = なし 1 = AnyConnect Client SSL VPN 2 = AnyConnect Client IPSec VPN（IKEv2） 3 = クライアントレス SSL VPN 4 = クライントレス電子メールプロキシ 5 = Cisco VPN Client（IKEv1） 6 = IKEv1 LAN-LAN 7 = IKEv2 LAN-LAN 8 = VPN ロードバランシング
Simultaneous-Logins	Y	2	整数	シングル	0-2147483647
Smart-Tunnel	Y	136	文字列	シングル	スマートトンネルの名前
Smart-Tunnel-Auto	Y	138	整数	シングル	0 = ディセーブル 1 = イネーブル 2 = 自動スタート
SmartTunnelAutoSignonEnable	Y	139	文字列	シングル	ドメイン名が付加された Smart Tunnel Auto Signon リストの名前
Strip-Realm	Y	135	ブール	シングル	0 = 無効1 = 有効
SVC-Ask	Y	131	文字列	シングル	0 = ディセーブル 1 = イネーブル 3 = デフォルトサービスをイネーブルにする 5 = デフォルトクライアントレスをイネーブルにする （2 と 4 は使用しない）
SVC-Ask-Timeout	Y	132	整数	シングル	5 ～ 120 秒

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
SVC-DPD-Interval-Client	Y	108	整数	シングル	0 = オフ 5 ～ 3600 秒
SVC-DPD-Interval-Gateway	Y	109	整数	シングル	0 = オフ 5 ～ 3600 秒
SVC-DTLS	Y	123	整数	シングル	0 = False 1 = True
SVC-Keepalive	Y	107	整数	シングル	0 = オフ 15 ～ 600 秒
SVC-Modules	Y	127	文字列	シングル	文字列（モジュールの名前）
SVC-MTU	Y	125	整数	シングル	MTU 値 256 ～ 1406 バイト
SVC-Profiles	Y	128	文字列	シングル	文字列（プロファイルの名前）
SVC-Rekey-Time	Y	110	整数	シングル	0 = ディセーブル 1 ～ 10080 分
Tunnel Group Name	Y	146	文字列	シングル	1 ～ 253 文字
Tunnel-Group-Lock	Y	85	文字列	シングル	トンネル グループの名前または「none」
Tunneling-Protocols	Y	11	整数	シングル	1 = PPTP 2 = L2TP 4 = IPSec (IKEv1) 8 = L2TP/IPSec 16 = WebVPN 32 = SVC 64 = IPsec (IKEv2) 8 と 4 は相互排他。0 ～ 11、16 ～ 27、32 ～ 43、48 ～ 59 は有効な値。
Use-Client-Address		17	ブール	シングル	0 = 無効1 = 有効
VLAN	Y	140	整数	シングル	0 ～ 4094
WebVPN-Access-List	Y	73	文字列	シングル	アクセス リスト名
WebVPN ACL	Y	73	文字列	シングル	デバイスの WebVPN ACL 名

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
WebVPN-ActiveX-Relay	Y	137	整数	シングル	0 = 無効 その他 = 有効
WebVPN-Apply-ACL	Y	102	整数	シングル	0 = 無効1 = 有効
WebVPN-Auto-HTTP-Signon	Y	124	文字列	シングル	予約済み
WebVPN-Citrix-MetaFrame-Enable	Y	101	整数	シングル	0 = 無効1 = 有効
WebVPN-Content-Filter-Parameters	Y	69	整数	シングル	1 = Java ActiveX 2 = Java スクリプト 4 = イメージ 8 = イメージに含まれるクッキー
WebVPN-Customization	Y	113	文字列	シングル	カスタマイゼーションの名前
WebVPN-Default-Homepage	Y	76	文字列	シングル	URL（たとえば http://example.example.com）
WebVPN-Deny-Message	Y	116	文字列	シングル	有効な文字列（500 文字以内）
WebVPN-Download_Max-Size	Y	157	整数	シングル	0x7fffffff
WebVPN-File-Access-Enable	Y	94	整数	シングル	0 = 無効1 = 有効
WebVPN-File-Server-Browsing-Enable	Y	96	整数	シングル	0 = 無効1 = 有効
WebVPN-File-Server-Entry-Enable	Y	95	整数	シングル	0 = 無効1 = 有効
WebVPN-Group-based-HTTP/HTTPS-Proxy-Exceptions	Y	78	文字列	シングル	オプションのワイルドカード（*）を使用したカンマ区切りの DNS/IP（たとえば、*.cisco.com、192.168.1.*、wwwin.cisco.com）
WebVPN-Hidden-Shares	Y	126	整数	シングル	0 = なし 1 = 表示される

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
WebVPN-HomePageUseSmartTunnel	Y	228	ブール	シングル	クライアントレスホームページをスマートトンネル経由で表示する場合にイネーブルにします。
WebVPN-HTML-Filter	Y	69	Bitmap	シングル	1 = Java ActiveX 2 = スクリプト 4 = イメージ 8 = クッキー
WebVPN-HTTP-Compression	Y	120	整数	シングル	0 = オフ 1 = デフレート圧縮
WebVPN-HTTP-Proxy-IP-Address	Y	74	文字列	シングル	http= または https= プレフィックス付きの、カンマ区切りの DNS/IP:ポート（例：http=10.10.10.10:80、https=11.11.11.11:443）
WebVPN-Idle-Timeout-Alert-Interval	Y	148	整数	シングル	0 ～ 30。0 = ディセーブル。
WebVPN-Keepalive-Ignore	Y	121	整数	シングル	0 ～ 900
WebVPN-Macro-Substitution	Y	223	文字列	シングル	無制限。
WebVPN-Macro-Substitution	Y	224	文字列	シングル	無制限。
WebVPN-Port-Forwarding-Enable	Y	97	整数	シングル	0 = 無効1 = 有効
WebVPN-Port-Forwarding-Exchange-Proxy-Enable	Y	98	整数	シングル	0 = 無効1 = 有効
WebVPN-Port-Forwarding-HTTP-Proxy	Y	99	整数	シングル	0 = 無効1 = 有効
WebVPN-Port-Forwarding-List	Y	72	文字列	シングル	ポート転送リスト名

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
WebVPN-Port-Forwarding-Name	Y	79	文字列	シングル	名前の文字列（例、「Corporate-Apps」）。 このテキストでクライアントレスポータル ホームページのデフォルト文字列「Application Access」が置き換えられます。
WebVPN-Post-Max-Size	Y	159	整数	シングル	0x7fffffff
WebVPN-Session-Timeout-Alert-Interval	Y	149	整数	シングル	0 ～ 30。0 = ディセーブル。
WebVPN SmartCard-Removal-Disconnect	Y	225	ブール	シングル	0 = 無効1 = 有効
WebVPN-Smart-Tunnel	Y	136	文字列	シングル	スマート トンネルの名前
WebVPN-Smart-Tunnel-Auto-Sign-On	Y	139	文字列	シングル	ドメイン名が付加されたスマート トンネル自動サインオン リストの名前
WebVPN-Smart-Tunnel-Auto-Start	Y	138	整数	シングル	0 = 無効1 = 有効2 = 自動スタート

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
WebVPN-Smart-Tunnel-Policy	Y	227	文字列	シングル	「e ネットワーク名」、「i ネットワーク名」、「a」のいずれか。ここで、ネットワーク名は、スマートトンネル ネットワークのリストの名前です。e はトンネルが除外されることを示し、i はトンネルが指定されることを示し、a はすべてのトンネルを示します。
WebVPN-SSL-VPN-Client-Enable	Y	103	整数	シングル	0 = 無効1 = 有効
WebVPN-SSL-VPN-Client-Keep-Installation	Y	105	整数	シングル	0 = 無効1 = 有効
WebVPN-SSL-VPN-Client-Required	Y	104	整数	シングル	0 = 無効1 = 有効
WebVPN-SSO-Server-Name	Y	114	文字列	シングル	有効な文字列
WebVPN-Storage-Key	Y	162	文字列	シングル	
WebVPN-Storage-Objects	Y	161	文字列	シングル	
WebVPN-SVC-Keepalive-Frequency	Y	107	整数	シングル	15 ～ 600 秒、0=オフ
WebVPN-SVC-Client-DPD-Frequency	Y	108	整数	シングル	5 ～ 3600 秒、0=オフ
WebVPN-SVC-DTLS-Enable	Y	123	整数	シングル	0 = 無効1 = 有効
WebVPN-SVC-DTLS-MTU	Y	125	整数	シングル	MTU 値は 256 ～ 1406 バイトです。
WebVPN-SVC-Gateway-DPD-Frequency	Y	109	整数	シングル	5 ～ 3600 秒、0=オフ
WebVPN-SVC-Rekey-Time	Y	110	整数	シングル	4 ～ 10080 分、0=オフ

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
WebVPN-SVC-Rekey-Method	Y	111	整数	シングル	0（オフ）、1（SSL）、2（新しいトンネル）
WebVPN-SVC-Compression	Y	112	整数	シングル	0（オフ）、1（デフォルトの圧縮）
WebVPN-UNIX-Group-ID (GID)	Y	222	整数	シングル	UNIX での有効なグループ ID
WebVPN-UNIX-User-ID (UIDs)	Y	221	整数	シングル	UNIX での有効なユーザ ID
WebVPN-Upload-Max-Size	Y	158	整数	シングル	0x7fffffff
WebVPN-URL-Entry-Enable	Y	93	整数	シングル	0 = 無効1 = 有効
WebVPN-URL-List	Y	71	文字列	シングル	URL リスト名
WebVPN-User-Storage	Y	160	文字列	シングル	
WebVPN-VDI	Y	163	文字列	シングル	設定のリスト

サポートされる IETF RADIUS 認証属性

次の表に、サポートされる IETF RADIUS 属性の一覧を示します。

表 *2 :* サポートされる *IETF RADIUS* 属性

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
IETF-Radius-Class	Y	25		シングル	バージョン 8.2.x 以降では、Group-Policy 属性（VSA 3076、#25）を使用することをお勧めします。 • グループ ポリシー名 • OU=グループ ポリシー名 • OU=グループ ポリシー名
IETF-Radius-Filter-Id	Y	11	文字列	シングル	フル トンネルの IPsec クライアントと SSL VPN クライアントのみに適用される、ASA で定義された ACL 名。
IETF-Radius-Framed-IP-Address	Y	n/a	文字列	シングル	IP アドレス
IETF-Radius-Framed-IP-Netmask	Y	n/a	文字列	シングル	IP アドレス マスク
IETF-Radius-Idle-Timeout	Y	28	整数	シングル	Seconds

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
IETF-Radius-Service-Type	Y	6	整数	シングル	秒。使用可能なサービス タイプの値： • .Administrative：ユーザは configure プロンプトへのアクセスを許可されています。 • .NAS-Prompt：ユーザは exec プロンプトへのアクセスを許可されています。 • .remote-access：ユーザはネットワーク アクセスを許可されています。
IETF-Radius-Session-Timeout	Y	27	整数	シングル	Seconds

RADIUS アカウンティング切断の理由コード

これらのコードは、パケットを送信するときに ASA が切断された場合に返されます。

切断の理由コード
ACCT_DISC_USER_REQ = 1
ACCT_DISC_LOST_CARRIER = 2
ACCT_DISC_LOST_SERVICE = 3
ACCT_DISC_IDLE_TIMEOUT = 4
ACCT_DISC_SESS_TIMEOUT = 5
ACCT_DISC_ADMIN_RESET = 6

切断の理由コード
ACCT_DISC_ADMIN_REBOOT = 7
ACCT_DISC_PORT_ERROR = 8
ACCT_DISC_NAS_ERROR = 9
ACCT_DISC_NAS_REQUEST = 10
ACCT_DISC_NAS_REBOOT = 11
ACCT_DISC_PORT_UNNEEDED = 12
ACCT_DISC_PORT_PREEMPTED = 13
ACCT_DISC_PORT_SUSPENDED = 14
ACCT_DISC_SERV_UNAVAIL = 15
ACCT_DISC_CALLBACK = 16
ACCT_DISC_USER_ERROR = 17
ACCT_DISC_HOST_REQUEST = 18
ACCT_DISC_ADMIN_SHUTDOWN = 19
ACCT_DISC_SA_EXPIRED = 21
ACCT_DISC_MAX_REASONS = 22

AAA の RADIUS サーバのガイドライン

ここでは、AAA 用の RADIUS サーバを設定する前に確認する必要のあるガイドラインおよび制限事項について説明します。

- シングル モードで最大 100 個のサーバ グループ、またはマルチ モードでコンテキストごとに 4 つのサーバ グループを持つことができます。
- 各グループには、シングル モードで最大 16 台、マルチ モードで最大 4 台のサーバを含めることができます。

IPv6

AAA サーバは IPv4 アドレスを使用する必要がありますが、エンドポイントは IPv6 を使用できます。

AAA 用の RADIUS サーバの設定

ここでは、AAA 用に RADIUS サーバを設定する方法について説明します。

手順

ステップ 1 ASA の属性を RADIUS サーバにロードします。属性をロードするために使用する方法は、使用している RADIUS サーバのタイプによって異なります。

- Cisco ACS を使用している場合：サーバには、これらの属性がすでに統合されています。したがって、この手順をスキップできます。
- 他のベンダーの RADIUS サーバ（たとえば Microsoft Internet Authentication Service）の場合：ASA の各属性を手動で定義する必要があります。属性を定義するには、属性名または番号、タイプ、値、ベンダー コード（3076）を使用します。

ステップ 2 RADIUS サーバ グループの設定 （23 ページ）。

ステップ 3 グループへの RADIUS サーバの追加 （27 ページ）。

RADIUS サーバ グループの設定

認証、許可、またはアカウンティングに外部 RADIUS サーバを使用する場合は、まず AAA プロトコルあたり少なくとも 1 つの RADIUS サーバ グループを作成して、各グループに 1 つ以上のサーバを追加する必要があります。

手順

ステップ 1 RADIUS AAA サーバ グループを作成します。

aaa-server *group_name* **protocol radius**

例：

```
ciscoasa(config)# aaa-server servergroup1 protocol radius
ciscoasa(config-aaa-server-group)#
```

aaa-server protocol コマンドを入力すると、aaa-server グループ コンフィギュレーション モードが開始します。

ステップ 2 （任意）次のサーバを試す前にグループ内の RADIUS サーバでの AAA トランザクションの失敗の最大数を指定します。

max-failed-attempts *number*

範囲は、1 ～ 5 です。デフォルトは 3 です。

ローカルデータベースを使用してフォールバック方式（管理アクセス専用）を設定している場合で、グループ内のすべてのサーバが応答しないとき、グループは応答なしと見なされ、フォールバック方式が試行されます。サーバ グループで、追加の AAA 要求によるアクセスがない、非応答と見なされる時間が 10 分間（デフォルト）続くと、ただちにフォールバック方式が使用されます。非応答時間をデフォルトから変更するには、次のステップの **reactivation-mode** コマンドを参照してください。

フォールバック方式として設定されていない場合、ASA は引き続きグループ内のサーバにアクセスしようとします。

例：

```
ciscoasa(config-aaa-server-group)# max-failed-attempts 2
```

ステップ 3 （任意）グループ内で障害の発生したサーバを再度アクティブ化する方法（再アクティブ化ポリシー）を指定します。

reactivation-mode {**depletion** [**deadtime** *minutes*] | **timed**}

それぞれの説明は次のとおりです。

- **depletion** [**deadtime** *minutes*] は、グループ内のすべてのサーバが非アクティブになった後でのみ、障害が発生したサーバを再アクティブ化します。これがデフォルトの再アクティブ化モードです。グループ内の最後のサーバがディセーブルになってから、その後すべてのサーバを再度イネーブルにするまでの時間を 0 ～ 1440 分の範囲で指定できます。デフォルトは 10 分です。
- **timed** 30 秒のダウン時間の後、障害が発生したサーバを再アクティブ化します。

例：

```
ciscoasa(config-aaa-server-group)# reactivation-mode deadtime 20
```

ステップ 4 （任意）グループ内のすべてのサーバにアカウンティング メッセージを送信します。

accounting-mode simultaneous

アクティブ サーバだけ送信メッセージをデフォルトに戻すには、**accounting-mode single** コマンドを入力します。

例：

```
ciscoasa(config-aaa-server-group)# accounting-mode simultaneous
```

ステップ 5 （任意）RADIUS 中間アカウンティング アップデート メッセージの定期的な生成をイネーブルにします。

interim-accounting-update [**periodic** [*hours*]]

ISE は、ASA などの NAS デバイスから受信するアカウンティング レコードに基づいて、アクティブ セッションのディレクトリを保持します。ただし、セッションがアクティブであるという通知（アカウンティング メッセージまたはポスチャ トランザクション）を 5 日間受信しなかった場合、ISE はデータベースからそのセッションのレコードを削除します。存続時間の長い VPN 接続が削除されないようにするには、すべてのアクティブ セッションについて ISE に定期的に中間アカウンティング更新メッセージを送信するように、グループを設定します。

- **periodic**[*hours*] は、対象のサーバ グループにアカウンティング レコードを送信するように設定されたすべての VPN セッションのアカウンティング レコードの定期的な生成と伝送をイネーブルにします。オプションで、これらの更新の送信間隔（時間単位）を含めることができます。デフォルトは 24 時間で、指定できる範囲は 1 ～ 120 時間です。
- （パラメータなし）。**periodic** キーワードなしでこのコマンドを使用すると、ASA は、VPN トンネル接続がクライアントレス VPN セッションに追加されたときにのみ中間アカウンティング更新メッセージを送信します。これが発生した場合、新たに割り当てられた IP アドレスを RADIUS に通知するためのアカウンティング アップデートが生成されます。

例：

```
hostname(config-aaa-server-group)# interim-accounting-update periodic 12
```

ステップ 6 （任意）AAA サーバ グループの RADIUS の動的認可（ISE 許可変更、CoA）サービスをイネーブルにします。

dynamic-authorization [**port** *number*]

ポートの指定は任意です。デフォルトは 1700 です。指定できる範囲は 1024 ～ 65535 です。

VPN トンネルでサーバ グループを使用すると、対応する RADIUS サーバ グループが CoA 通知用に登録され、ASA は ISE からの CoA ポリシー更新用ポートをリッスンします。このサーバ グループを ISE と併せてリモート アクセス VPN で使用する場合にのみ動的認可をイネーブルにします。

例：

```
ciscoasa(config-aaa-server-group)# dynamic-authorization
```

ステップ 7 （任意）認証に ISE を使用しない場合は、RADIUS サーバ グループに対し認可専用モードを有効にします。（このサーバ グループを ISE と併せてリモート アクセス VPN で使用する場合にのみ認可専用モードをイネーブルにします）。

authorize-only

これは、サーバ グループを認可に使用するときに、RADIUS アクセス要求メッセージが、AAA サーバ用に設定されているパスワード方式に反して、「認可専用」要求として構築されることを示しています。**radius-common-pw** コマンドを使用して RADIUS サーバの共通パスワードを設定すると、そのパスワードは無視されます。

たとえば、認証にこのサーバ グループではなく証明書を使用する場合には、認可専用モードを使用します。VPN トンネルでの認可とアカウンティングにこのサーバ グループを使用する可能性があるからです。

例：

```
ciscoasa(config-aaa-server-group)# authorize-only
```

ステップ 8 （任意）ダウンロード可能 ACL と、RADIUS パケットから Cisco AV ペアで受信した ACL を結合します。

merge-dacl {**before-avpair** | **after-avpair**}

例：

```
ciscoasa(config-aaa-server-group)# merge-dacl before-avpair
```

このオプションは、VPN 接続にのみ適用されます。VPN ユーザの場合は、ACL は Cisco AV ペア ACL、ダウンロード可能 ACL、および ASA で設定される ACL の形式になります。このオプションでは、ダウンロード可能 ACL と AV ペア ACL を結合するかどうかを決定します。ASA で設定されている ACL には適用されません。

デフォルト設定は **no merge dacl** で、ダウンロード可能な ACL は Cisco AV ペア ACL と結合されません。AV ペアおよびダウンロード可能 ACL の両方を受信した場合は、AV ペアが優先し、使用されます。

before-avpair オプションは、ダウンロード可能 ACL エントリが Cisco-AV-Pair エントリの前に配置されるように指定します。

after-avpair オプションは、ダウンロード可能 ACL エントリが Cisco-AV-Pair エントリの後に配置されるように指定します。

例

次に、単一サーバで 1 つの RADIUS グループを追加する例を示します。

```
ciscoasa(config)# aaa-server AuthOutbound protocol radius
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server AuthOutbound (inside) host 10.1.1.3
ciscoasa(config-aaa-server-host)# key RadUauthKey
ciscoasa(config-aaa-server-host)# exit
```

次の例は、ISE サーバ グループに、動的認可（CoA）のアップデートと時間ごとの定期的なアカウンティングを設定する方法を示しています。ISE によるパスワード認証を設定するトンネル グループ設定が含まれています。

```
ciscoasa(config)# aaa-server ise protocol radius
ciscoasa(config-aaa-server-group)# interim-accounting-update periodic 1
ciscoasa(config-aaa-server-group)# dynamic-authorization
```

```
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server ise (inside) host 10.1.1.3
ciscoasa(config-aaa-server-host)# key sharedsecret
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# tunnel-group aaa-coa general-attributes
ciscoasa(config-tunnel-general)# address-pool vpn
ciscoasa(config-tunnel-general)# authentication-server-group ise
ciscoasa(config-tunnel-general)# accounting-server-group ise
ciscoasa(config-tunnel-general)# exit
```

次に、ISE でローカル証明書の検証と認可用のトンネル グループを設定する例を示します。サーバ グループは認証用に使用されないため、authorize-only コマンドをサーバ グループ コンフィギュレーションに組み込みます。

```
ciscoasa(config)# aaa-server ise protocol radius
ciscoasa(config-aaa-server-group)# authorize-only
ciscoasa(config-aaa-server-group)# interim-accounting-update periodic 1
ciscoasa(config-aaa-server-group)# dynamic-authorization
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server ise (inside) host 10.1.1.3
ciscoasa(config-aaa-server-host)# key sharedsecret
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# tunnel-group aaa-coa general-attributes
ciscoasa(config-tunnel-general)# address-pool vpn
ciscoasa(config-tunnel-general)# authentication certificate
ciscoasa(config-tunnel-general)# authorization-server-group ise
ciscoasa(config-tunnel-general)# accounting-server-group ise
ciscoasa(config-tunnel-general)# exit
```

グループへの RADIUS サーバの追加

RADIUS サーバをグループに追加するには、次の手順を実行します。

手順

ステップ 1 RADIUS サーバと、そのサーバが属する AAA サーバ グループを識別します。

aaa-server *server_group* [**(***interface_name***)**] **host** *server_ip*

例：

```
ciscoasa(config-aaa-server-group)# aaa-server servergroup1 outside host 10.10.1.1
```

(*interface_name***)** を指定していない場合、ASA はデフォルトで**内部**インターフェイスを使用します。

ステップ 2 RADIUS サーバからダウンロード可能な ACL で受信したネットマスクを ASA が処理する方法を指定します。

acl-netmask-convert {**auto-detect** | **standard** | **wildcard**}

例：

```
ciscoasa(config-aaa-server-host)# acl-netmask-convert standard
```

auto-detect キーワードは、使用されているネットマスク表現のタイプの判別を ASA が試みる必要があることを指定します。ASA によってワイルドカード ネットマスク表現が検出された場合は、標準ネットマスク表現に変換されます。

standard キーワードは、RADIUS サーバから受信したダウンロード可能 ACL には、標準ネットマスク表現のみが含まれていると ASA が見なすように指定します。ワイルドカード ネットマスク表現からの変換は実行されません。

wildcard キーワードは、RADIUS サーバから受信したダウンロード可能 ACL には、ワイルドカード ネットマスク表現のみが含まれていると ASA が見なし、ACL をダウンロードしたときにそれらすべてを標準ネットマスク表現に変換するように指定します。

ステップ 3 ASA を介して RADIUS 認可サーバにアクセスするすべてのユーザが使用する共通パスワードを指定します。

radius-common-pw *string*

例：

```
ciscoasa(config-aaa-server-host)# radius-common-pw examplepassword123abc
```

string 引数は、大文字と小文字が区別される最大 127 文字の英数字キーワードです。RADIUS サーバとのすべての認可トランザクションで共通パスワードとして使用されます。

ステップ 4 RADIUS サーバへの MS-CHAPv2 認証要求をイネーブルにします。

mschapv2-capable

例：

```
ciscoasa(config-aaa-server-host)# mschapv2-capable
```

ステップ 5 サーバへの接続試行のタイムアウト値を指定します。

timeout *seconds*

サーバのタイムアウト間隔（1 ～ 300 秒）を指定します。デフォルトは 10 秒です。各 AAA トランザクションに対して、タイムアウトに達するまで（**retry-interval** コマンドで定義された間隔に基づいて）ASA による接続の再試行が行われます。連続して失敗したトランザクションの数が AAA サーバ グループ内の max-failed-attempts コマンドで指定された制限に達すると、AAA サーバは非アクティブ化され、ASA は（設定されている場合は）別の AAA サーバへの要求の送信を開始します。

例：

```
ciscoasa(config-aaa-server-host)# timeout 15
```

ステップ 6 前のコマンドで指定した特定の AAA サーバに対して、再試行間隔を設定します。

retry-interval *seconds*

例：

```
ciscoasa(config-aaa-server-host)# retry-interval 8
```

seconds 引数に要求の再試行間隔（1 ～ 10 秒）を指定します。これは、接続要求を再試行するまでに ASA が待機する時間です。

（注） RADIUS プロトコルの場合、サーバが ICMP ポート到達不能メッセージで応答すると、再試行間隔の設定が無視され、AAA サーバはただちに障害状態になります。このサーバが AAA グループ内の唯一のサーバである場合は、サーバが再アクティブ化され、別の要求がサーバに送信されます。これは意図された動作です。

ステップ 7 グループ内のすべてのサーバにアカウンティング メッセージを送信します。

accounting-mode simultaneous

例：

```
ciscoasa(config-aaa-server-group)# accounting-mode simultaneous
```

アクティブ サーバにのみメッセージを送信するデフォルトに戻すには、**accounting-mode single** コマンドを入力します。

ステップ 8 認証ポートをポート番号 1645 に指定するか、またはユーザ認証に使用するサーバ ポートを指定します。

authentication-port *port*

例：

```
ciscoasa(config-aaa-server-host)# authentication-port 1646
```

ステップ 9 アカウンティング ポートをポート番号 1646 に指定するか、またはこのホストのアカウンティングに使用するサーバ ポートを指定します。

accounting-port *port*

例：

```
ciscoasa(config-aaa-server-host)# accounting-port 1646
```

ステップ 10 ASA に対する RADIUS サーバの認証に使用されるサーバ秘密値を指定します。設定したサーバ秘密キーは、RADIUS サーバで設定されたサーバ秘密キーと一致する必要があります。サーバ秘密キーの値が不明の場合は、RADIUS サーバの管理者に問い合わせてください。最大長は、64 文字です。

key

例：

```
ciscoasa(config-aaa-host)# key myexamplekey1
```

設定したサーバ秘密キーは、RADIUS サーバで設定されたサーバ秘密キーと一致する必要があります。サーバ秘密キーの値が不明の場合は、RADIUS サーバの管理者に問い合わせてください。最大長は、64 文字です。

例

次に、既存の RADIUS サーバ グループに RADIUS サーバを追加する例を示します。

```
ciscoasa(config)# aaa-server svrgrp1 protocol radius
ciscoasa(config-aaa-server-group)# aaa-server svrgrp1 host 192.168.3.4
ciscoasa(config-aaa-server-host)# acl-netmask-convert wildcard
ciscoasa(config-aaa-server-host)# radius-common-pw myexaplepasswordabc123
ciscoasa(config-aaa-server-host)# mschapv2-capable
ciscoasa(config-aaa-server-host)# timeout 9
ciscoasa(config-aaa-server-host)# retry-interval 7
ciscoasa(config-aaa-server-host)# accounting-mode simultaneous
ciscoasa(config-aaa-server-host)# authentication-port 1650
ciscoasa(config-aaa-server-host)# authorization-port 1645
ciscoasa(config-aaa-server-host)# key mysecretkeyexampleiceage2
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)#
```

AAA 用の RADIUS サーバのモニタリング

AAA 用の RADIUS サーバのステータスのモニタリングについては、次のコマンドを参照してください。

- **show aaa-server**

  このコマンドは、設定された RADIUS サーバの統計情報を表示します。**clear aaa-server statistics** コマンドを使用して、カウンタをゼロにリセットできます。

- **show running-config aaa-server**

  このコマンドは、RADIUS サーバの実行コンフィギュレーションを表示します。

AAA 用の RADIUS サーバの履歴

表 *3 : AAA* 用の *RADIUS* サーバの履歴

機能名	プラットフォーム リリース	説明
AAA の RADIUS サーバ	7.0(1)	AAA 用の RADIUS サーバを設定する方法について説明します。 次のコマンドを導入しました。 **aaa-server protocol**、**max-failed-attempts**、**reactivation-mode**、**accounting-mode simultaneous**、**aaa-server host**、**show aaa-server**、**show running-config aaa-server**、**clear aaa-server statistics**、**authentication-port**、**accounting-port**、**retry-interval**、**acl-netmask-convert**、**clear configure aaa-server**、**merge-dacl**、**radius-common-pw**、**key**。
ASA からの RADIUS アクセス要求パケットおよびアカウンティング要求パケットでの主なベンダー固有属性（VSA）の送信	8.4(3)	4 つの新しい VSA：Tunnel Group Name（146）および Client Type（150）は、ASA からの RADIUS アクセス要求パケットで送信されます。Session Type（151）および Session Subtype（152）は、ASA からの RADIUS アカウンティング要求パケットで送信されます。4 つのすべての属性が、すべてのアカウンティング要求パケット タイプ（開始、中間アップデート、および終了）に送信されます。RADIUS サーバ（ACS や ISE など）は、認可属性やポリシー属性を強制適用したり、アカウンティングや課金のためにそれらの属性を使用したりできます。