CHAPTER 34

AAA の RADIUS サーバの設定

この章では、RADIUS AAA を設定する方法について説明します。次の項目を取り上げます。

RADIUS サーバに関する情報

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

この項では、次のトピックについて取り上げます。

サポートされている認証方式

ASA は、RADIUS サーバで次の認証方法をサポートします。

- 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 に接続の場合、

（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。パスワード管理をイネーブルにすると、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 接続のユーザ許可

ASA では 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な 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 によって ACL が削除されます。

ACL に加え、ASA は、その他多数の許可属性、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 セッションに対する許可の設定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
- Cisco VSA（Cisco-Priv-Level）。特権の標準ランキングである 0 ～ 15 の数値を指定します。1 が最低レベルを示し、15 が最高レベルを示します。0 レベルは特権がないことを示します。第 1 レベル（login）では、このレベルで使用可能なコマンドに対する特権 EXEC アクセスが許可されます。第 2 レベル（enable）では CLI コンフィギュレーション特権が許可されます。

サポートされる RADIUS 認証属性

許可では、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。

表 34-1 に、ユーザ許可に使用でき、がサポートしている使用可能な 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 によって RADIUS 属性が適用されるときは、属性名ではなく数値の属性 ID に基づいて適用されます。

表 34-1 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、認証および許可の要求の場合に 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。

Cisco ACS 5x および Cisco ISE は、バージョン 9.0（1）の RADIUS 認証を使用する IP アドレスの割り当ての IPv6 Framed IP アドレスはサポートされません。

表 34-1　サポートされる RADIUS 認証属性

属性名	ASA	属性 No.	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 = ディセーブル 1 = イネーブル
Authenticated-User-Idle-Timeout	Y	50	Integer	シングル	1 ～ 35791394 分
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	Integer	シングル	0 = しない 1 = する

表 34-1　サポートされる RADIUS 認証属性 （続き）

属性名	ASA	属性 No.	構文 / タイプ	シングルまたはマルチ値	説明または値
Authorization-Type	Y	65	Integer	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	Integer	シングル	0 = ディセーブル 1 = イネーブル
Cisco-LEAP-Bypass	Y	75	Integer	シングル	0 = ディセーブル 1 = イネーブル
Client Type	Y	150	Integer	シングル	1 = Cisco VPN クライアント（IKEv1） 2 = AnyConnect クライアント SSL VPN 3 = クライアントレス SSL VPN 4 = カットスルー プロキシ 5 = L2TP/IPsec SSL VPN 6 = AnyConnect クライアント 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 Address
Extended-Authentication-On-Rekey	Y	122	Integer	シングル	0 = ディセーブル 1 = イネーブル
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	Integer	シングル	0 = なし 1 = ローカル

表 34-1　サポートされる RADIUS 認証属性 （続き）

属性名	ASA	属性 No.	構文 / タイプ	シングルまたはマルチ値	説明または値
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	Integer	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	Integer	シングル	10 ～ 300 秒
IKE-Keepalive-Retry-Interval	Y	84	Integer	シングル	2 ～ 10 秒
IKE-Keep-Alives	Y	41	ブール	シングル	0 = ディセーブル 1 = イネーブル
Intercept-DHCP-Configure-Msg	Y	62	ブール	シングル	0 = ディセーブル 1 = イネーブル
IPsec-Allow-Passwd-Store	Y	16	ブール	シングル	0 = ディセーブル 1 = イネーブル
IPsec-Authentication		13	Integer	シングル	0 = なし 1 = RADIUS 2 = LDAP（許可のみ） 3 = NT ドメイン 4 = SDI 5 = 内部 6 = RADIUS での Expiry 7 = Kerberos/Active Directory
IPsec-Auth-On-Rekey	Y	42	ブール	シングル	0 = ディセーブル 1 = イネーブル
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	Integer	シングル	0 = 必須 1 = オプション

表 34-1　サポートされる RADIUS 認証属性 （続き）

属性名	ASA	属性 No.	構文 / タイプ	シングルまたはマルチ値	説明または値
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）。
IPsec-IKE-Peer-ID-Check	Y	40	Integer	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	Integer	シングル	0 = ディセーブル 1 = イネーブル
IPsec-Mode-Config	Y	31	ブール	シングル	0 = ディセーブル 1 = イネーブル
IPsec-Over-UDP	Y	34	ブール	シングル	0 = ディセーブル 1 = イネーブル
IPsec-Over-UDP-Port	Y	35	Integer	シングル	4001 ～ 49151。デフォルト値は 10000 です。
IPsec-Required-Client-Firewall-Capability	Y	56	Integer	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	Integer	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
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	Integer	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 = ディセーブル 1 = イネーブル
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

表 34-1　サポートされる RADIUS 認証属性 （続き）

属性名	ASA	属性 No.	構文 / タイプ	シングルまたはマルチ値	説明または値
L2TP-Encryption		21	Integer	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
L2TP-MPPC-Compression		38	Integer	シングル	0 = ディセーブル 1 = イネーブル
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
NAC-Enable		89	Integer	シングル	0 = しない 1 = する
NAC-Revalidation-Timer		91	Integer	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	Integer	シングル	30 ～ 1800 秒
Perfect-Forward-Secrecy-Enable	Y	88	ブール	シングル	0 = しない 1 = する
PPTP-Encryption		20	Integer	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	Integer	シングル	0 = ディセーブル 1 = イネーブル
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

表 34-1　サポートされる RADIUS 認証属性 （続き）

属性名	ASA	属性 No.	構文 / タイプ	シングルまたはマルチ値	説明または値
Privilege-Level	Y	220	Integer	シングル	0 ～ 15 の整数。
Required-Client- Firewall-Vendor-Code	Y	45	Integer	シングル	1 = シスコ（Cisco Integrated Client を使用） 2 = Zone Labs 3 = NetworkICE 4 = Sygate 5 = シスコ（Cisco Intrusion Prevention Security Agent を使用）
Required-Client-Firewall-Description	Y	47	文字列	シングル	文字列
Required-Client-Firewall-Product-Code	Y	46	Integer	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	Integer	シングル	0 = ディセーブル 1 = イネーブル
Require-HW-Client-Auth	Y	48	ブール	シングル	0 = ディセーブル 1 = イネーブル
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	Integer	シングル	未使用
Session Subtype	Y	152	Integer	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。

表 34-1　サポートされる RADIUS 認証属性 （続き）

属性名	ASA	属性 No.	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	Integer	シングル	0 = なし 1 = AnyConnect クライアント SSL VPN 2 = AnyConnect クライアント IPSec VPN（IKEv2） 3 = クライアントレス SSL VPN 4 = クライアントレス電子メール プロキシ 5 = Cisco VPN クライアント（IKEv1） 6 = IKEv1 LAN-LAN 7 = IKEv2 LAN-LAN 8 = VPN ロード バランシング
Simultaneous-Logins	Y	2	Integer	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	Integer	シングル	0 = ディセーブル 1 = イネーブル 2 = 自動スタート
Smart-Tunnel-Auto-Signon-Enable	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 = ディセーブル 1 = イネーブル
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	Integer	シングル	5 ～ 120 秒
SVC-DPD-Interval-Client	Y	108	Integer	シングル	0 = オフ 5 ～ 3600 秒
SVC-DPD-Interval-Gateway	Y	109	Integer	シングル	0 = オフ 5 ～ 3600 秒
SVC-DTLS	Y	123	Integer	シングル	0 = False 1 = True
SVC-Keepalive	Y	107	Integer	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	Integer	シングル	MTU 値 256 ～ 1406 バイト

表 34-1　サポートされる RADIUS 認証属性 （続き）

属性名	ASA	属性 No.	構文 / タイプ	シングルまたはマルチ値	説明または値
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	Integer	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	Integer	シングル	1 = PPTP 2 = L2TP 4 = IPSec（IKEv1） 8 = L2TP/IPSec 16 = WebVPN. 32 = SVC 64 = IPsec（IKEv2） 8 および 4 は相互排他値。 0 ～ 11、16 ～ 27、32 ～ 43、48 ～ 59 は有効値。
Use-Client-Address		17	ブール	シングル	0 = ディセーブル 1 = イネーブル
[VLAN]	Y	140	Integer	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
WebVPN-ActiveX-Relay	Y	137	Integer	シングル	0 = ディセーブル Otherwise = イネーブル
WebVPN-Apply-ACL	Y	102	Integer	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-Auto-HTTP-Signon	Y	124	文字列	シングル	Reserved
WebVPN-Citrix-Metaframe-Enable	Y	101	Integer	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-Content-Filter-Parameters	Y	69	Integer	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）

表 34-1　サポートされる RADIUS 認証属性 （続き）

属性名	ASA	属性 No.	構文 / タイプ	シングルまたはマルチ値	説明または値
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	Integer	シングル	0x7fffffff
WebVPN-File-Access-Enable	Y	94	Integer	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-File-Server-Browsing-Enable	Y	96	Integer	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-File-Server-Entry-Enable	Y	95	Integer	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-Group-based-HTTP/HTTPS-Proxy-Exception-List	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	Integer	シングル	0 = なし 1 = 表示
WebVPN-Home-Page-Use-Smart-Tunnel	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	Integer	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	Integer	シングル	0 ～ 30。0 = ディセーブル。
WebVPN-Keepalive-Ignore	Y	121	Integer	シングル	0 ～ 900
WebVPN-Macro-Substitution	Y	223	文字列	シングル	無制限。例については、次の URL にある『*SSL VPN Deployment Guide*』を参照してください。 http://supportwiki.cisco.com/ViewWiki/index.php/Cisco_ASA_5500_SSL_VPN_Deployment_Guide%2C_Version_8.x

表 34-1　サポートされる RADIUS 認証属性 （続き）

属性名	ASA	属性 No.	構文 / タイプ	シングルまたはマルチ値	説明または値
WebVPN-Macro-Substitution	Y	224	文字列	シングル	無制限。例については、次の URL にある『*SSL VPN Deployment Guide*』を参照してください。 http://supportwiki.cisco.com/ViewWiki/index.php/Cisco_ASA_5500_SSL_VPN_Deployment_Guide%2C_Version_8.x
WebVPN-Port-Forwarding-Enable	Y	97	Integer	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-Port-Forwarding-Exchange-Proxy-Enable	Y	98	Integer	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-Port-Forwarding-HTTP-Proxy	Y	99	Integer	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-Port-Forwarding-List	Y	72	文字列	シングル	ポート転送リスト名
WebVPN-Port-Forwarding-Name	Y	79	文字列	シングル	文字列の名前（「Corporate-Apps」など） 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	Integer	シングル	0x7fffffff
WebVPN-Session-Timeout-Alert-Interval	Y	149	Integer	シングル	0 ～ 30。0 = ディセーブル。
WebVPN Smart-Card-Removal-Disconnect	Y	225	ブール	シングル	0 = ディセーブル 1 = イネーブル
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	Integer	シングル	0 = ディセーブル 1 = イネーブル 2 = 自動開始
WebVPN-Smart-Tunnel-Tunnel-Policy	Y	227	文字列	シングル	「e networkname」、「i networkname」、「a networkname」のうちの 1 つが Smart Tunnel ネットワークのリストの名前です。「e」は除外されたトンネルを、「i」は指定されたトンネルを、「a」はすべてのトンネルを示します。
WebVPN-SSL-VPN-Client-Enable	Y	103	Integer	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-SSL-VPN-Client-Keep- Installation	Y	105	Integer	シングル	0 = ディセーブル 1 = イネーブル

表 34-1　サポートされる RADIUS 認証属性 （続き）

属性名	ASA	属性 No.	構文 / タイプ	シングルまたはマルチ値	説明または値
WebVPN-SSL-VPN-Client-Required	Y	104	Integer	シングル	0 = ディセーブル 1 = イネーブル
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	Integer	シングル	15 ～ 600 秒、0= オフ
WebVPN-SVC-Client-DPD-Frequency	Y	108	Integer	シングル	5 ～ 3600 秒、0= オフ
WebVPN-SVC-DTLS-Enable	Y	123	Integer	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-SVC-DTLS-MTU	Y	125	Integer	シングル	MTU 値は 256 ～ 1406 バイトです。
WebVPN-SVC-Gateway-DPD-Frequency	Y	109	Integer	シングル	5 ～ 3600 秒、0= オフ
WebVPN-SVC-Rekey-Time	Y	110	Integer	シングル	4 ～ 10080 分、0= オフ
WebVPN-SVC-Rekey-Method	Y	111	Integer	シングル	0（オフ）、1（SSL）、2（新しいトンネル）
WebVPN-SVC-Compression	Y	112	Integer	シングル	0（オフ）、1（デフォルトの圧縮）
WebVPN-UNIX-Group-ID (GID)	Y	222	Integer	シングル	UNIX での有効なグループ ID
WebVPN-UNIX-User-ID (UIDs)	Y	221	Integer	シングル	UNIX での有効なユーザ ID
WebVPN-Upload-Max-Size	Y	158	Integer	シングル	0x7fffffff
WebVPN-URL-Entry-Enable	Y	93	Integer	シングル	0 = ディセーブル 1 = イネーブル
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

表 34-2 に、サポートされている IETF RADIUS 属性を示します。

表 34-2　サポートされる IETF RADIUS 属性

属性名	ASA	属性 No.	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 以降の場合は、表 34-1 で説明している Group-Policy 属性（VSA 3076、#25）を使用することを推奨します。 • *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	Integer	シングル	Seconds
IETF-Radius-Service-Type	Y	6	Integer	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	Integer	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
ACCT_DISC_ADMIN_REBOOT = 7
ACCT_DISC_PORT_ERROR = 8

切断の理由コード （続き）
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

RADIUS サーバのライセンス要件

モデル	ライセンス要件
すべてのモデル	基本ライセンス

注意事項と制約事項

この項では、この機能のガイドラインと制限事項について説明します。

コンテキスト モードのガイドライン

シングル コンテキスト モードとマルチ コンテキスト モードでサポートされています。

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードとトランスペアレント ファイアウォール モードでサポートされています。

IPv6 のガイドライン

IPv6 をサポートします。

その他のガイドライン

- 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。

- ローカル データベースを使用してフォール バック サポートを設定する場合は、「フォールバック サポート」（P.33-2）と「グループ内の複数のサーバを使用したフォールバックの仕組み」（P.33-2）を参照してください。
- RADIUS 認証を使用する場合に、ASA からのロック アウトを防止するためは、「ロックアウトからの回復」（P.45-35）を参照してください。

RADIUS サーバの設定

この項では、次のトピックについて取り上げます。

- 「RADIUS サーバを設定するためのタスク フロー」（P.34-16）
- 「RADIUS サーバ グループの設定」（P.34-16）
- 「グループへの RADIUS サーバの追加」（P.34-18）
- 「認証プロンプトの追加」（P.34-20）

RADIUS サーバを設定するためのタスク フロー

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、使用する 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 グループを追加します。「RADIUS サーバ グループの設定」（P.34-16）を参照してください。

ステップ 3　サーバ グループの場合は、グループにサーバを追加します。「グループへの RADIUS サーバの追加」（P.34-18）を参照してください。

ステップ 4　（任意）AAA 認証チャレンジ プロセスの実行中にユーザに表示するテキストを指定します。「認証プロンプトの追加」（P.34-20）を参照してください。

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 RADIUS プロトコルあたり少なくとも 1 つの AAA 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。AAA サーバ グループは名前で識別されます。

RADIUS サーバ グループを追加するには、次の手順を実行します。

手順の詳細

ステップ 1　[Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups] を選択します。

ステップ 2　[AAA Server Groups] 領域で、[Add] をクリックします。

[Add AAA Server Group] ダイアログボックスが表示されます。

ステップ 3　[Server Group] フィールドで、グループの名前を入力します。

ステップ 4　[Protocol] ドロップダウン リストから、RADIUS サーバ タイプを選択します。

ステップ 5　[Accounting Mode] フィールドで、[Simultaneous] または [Single] をクリックします。

[Single] モードの場合、ASA ではアカウンティング データが 1 つのサーバにだけ送信されます。

[Simultaneous] モードの場合、ASA ではアカウンティング データがグループ内のすべてのサーバに送信されます。

ステップ 6　[Reactivation Mode] フィールドで、[Depletion] または [Timed] をクリックします。

[Depletion] モードの場合、障害が発生したサーバは、グループ内のサーバがすべて非アクティブになったときに限り、再アクティブ化されます。

Timed モードでは、障害が発生したサーバは 30 秒の停止時間の後で再アクティブ化されます。

ステップ 7　[Depletion] 再アクティブ化モードを選択した場合は、[Dead Time] フィールドに時間間隔を入力します。

[Dead Time] には、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、すべてのサーバが再びイネーブルになるまでの時間間隔を分単位で指定します。

ステップ 8　[Max Failed Attempts] フィールドに、許容される試行の失敗回数を指定します。

このオプションで設定するのは、応答のないサーバを非アクティブと宣言するまでに許可される接続試行の失敗回数です。

ステップ 9　（任意）RADIUS サーバのタイプを追加する場合には、次の手順を実行します。

a. クライアントレス SSL セッションおよび AnyConnect セッションに対して、マルチセッション アカウンティングをイネーブルにする場合は、[Enable interim accounting update] チェックボックスをオンにします。

b. [Enable Active Directory Agent Mode] チェックボックスをオンにして ASA と AD エージェント間の共有秘密を指定し、RADIUS サーバ グループにフル機能の RADIUS サーバではない AD エージェントを含めるよう指示します。ユーザ アイデンティティに関連付けることができるのは、このオプションを使用して設定された RADIUS サーバ グループのみです。

c. [VPN3K Compatibility Option] 下矢印をクリックしてリストを展開し、さらに次のいずれかのボタンをクリックして、RADIUS パケットから受け取ったダウンロード可能な ACL を、Cisco AV ペア ACL とマージするかどうかを指定します。

- **Do not merge**
- **Place the downloadable ACL after Cisco AV-pair ACL**
- **Place the downloadable ACL before Cisco AV-pair ACL**

ステップ 10　[OK] をクリックします。

[Add AAA Server Group] ダイアログボックスが閉じ、新しいサーバ グループが [AAA Server Groups] テーブルに追加されます。

ステップ 11　[AAA Server Groups] ダイアログボックスの [Apply] をクリックして、変更内容を実行コンフィギュレーションに保存します。

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。

手順の詳細

ステップ 1　[Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups] を選択し、[AAA Server Groups] 領域で、サーバを追加するサーバ グループをクリックします。

テーブル内の該当する行が選択されます。

ステップ 2　[Selected Group] 領域の [Servers]（下部ペイン）で、[Add] をクリックします。

サーバ グループに対応する [Add AAA Server Group] ダイアログボックスが表示されます。

ステップ 3　[Interface Name] ドロップダウン リストから、認証サーバが常駐するインターフェイスの名前を選択します。

ステップ 4　[Server Name] フィールドまたは [IP Address] フィールドに、グループに追加するサーバの名前または IP アドレスを入力します。

ステップ 5　[Timeout] フィールドで、タイムアウト値を入力します。デフォルト値をそのまま使用することもできます。[Timeout] フィールドには、バックアップ サーバへ要求を送信した ASA が、プライマリ サーバからの応答を待機する時間を秒単位で指定します。

ステップ 6　[Convert ACL Netmask] フィールドに、ASA がダウンロード可能 ACL に受信したネットマスクを処理する方法を指定します。次のオプションから選択します。

- [Detect automatically] : ASA で、使用されているネットマスク表現のタイプが判定されます。ASA でワイルドカード ネットマスク表現が検出された場合は、ASA により標準ネットマスク表現に変換されます。

（注）　一部のワイルドカード表現は明確な検出が困難なため、この設定を選択した場合には、ワイルドカード ネットマスク表現が誤って標準ネットマスク表現として検出されることもあります。

- [Standard] : ASA は、RADIUS サーバから受信したダウンロード可能な ACL に標準ネットマスク表現のみが含まれていると見なします。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] : ASA は、RADIUS サーバから受信したダウンロード可能な ACL にワイルドカード ネットマスク表現のみが含まれていると見なし、ACL のダウンロード時にそれらのすべてを標準ネットマスク表現に変換します。

ステップ 7　[Common Password] フィールドで、この ASA によって RADIUS 許可サーバにアクセスするユーザ間で共通の大文字と小文字が区別されるパスワードを指定します。この情報は、RADIUS サーバ管理者に伝えてください。

（注）　RADIUS 認証サーバ（許可サーバではない）に対しては、共通のパスワードは設定しないでください。

このフィールドをブランクのままにした場合は、RADIUS 許可サーバにアクセスする際のパスワードには、各ユーザ名が使用されます。

RADIUS 許可サーバを認証に使用することは避けてください。共通パスワードやユーザ名を転用したパスワードは、ユーザごとに一意のパスワードに比べ、安全性が低くなります。

このパスワードは、RADIUS プロトコルや RADIUS サーバによって要求されますが、ユーザが知っている必要はありません。

ステップ 8　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 をサポートしていない場合、このチェックボックスをオンにすれば、そのサーバから非 MS-CHAPv2 認証要求が送信されるようにできます。

ステップ 9　[Retry Interval] フィールドで、ASA のサーバへのアクセス試行待機時間間隔を 1 ～ 10 秒から指定します。

ステップ 10　[Accounting Mode] フィールドで、[Simultaneous] または [Single] をクリックします。

[Single] モードの場合、ASA ではアカウンティング データが 1 つのサーバにだけ送信されます。

[Simultaneous] モードの場合、ASA ではアカウンティング データがグループ内のすべてのサーバに送信されます。

ステップ 11　[Server Accounting Port] フィールドに、ユーザ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。デフォルトのポートは 1646 です。

ステップ 12　[Server Authentication Port] フィールドに、ユーザの認証に使用するサーバ ポートを指定します。デフォルトのポートは 1645 です。

ステップ 13　[Server Secret Key] フィールドに、ASA に対する RADIUS サーバの認証に使用される共有秘密キーを指定します。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。最大フィールド長は、64 文字です。

ステップ 14　[OK] をクリックします。

[Add AAA Server Group] ダイアログボックスが閉じ、AAA サーバが AAA サーバ グループに追加されます。

ステップ 15　[AAA Server Groups] ペインで [Apply] をクリックし、変更内容を実行コンフィギュレーションに保存します。

認証プロンプトの追加

RADIUS サーバからのユーザ認証が必要な場合に、ASA 経由の HTTP、FTP、Telnet アクセス用の AAA チャレンジ テキストを指定できます。このテキストは飾りのようなもので、ユーザのログイン時に、ユーザ名プロンプトとパスワード プロンプトの上に表示されます。認証プロンプトを指定しない場合、RADIUS サーバでの認証時にユーザに対して表示される内容は次のようになります。

接続タイプ	デフォルトのプロンプト
FTP	FTP authentication
HTTP	HTTP 認証
Telnet	なし

認証プロンプトを追加するには、次の手順を実行します。

ステップ 1　[Configuration] > [Device Management] > [Users/AAA] > [Authentication Prompt] ペインの [Prompt] フィールドに、ログイン時にユーザに対して表示されるユーザ名およびパスワードのプロンプトの上部にメッセージとして表示されるテキストを入力します。

次の表に、認証プロンプトの文字数制限を示します。

アプリケーション	文字制限
Microsoft Internet Explorer	37
Telnet	235
FTP	235

ステップ 2　[Messages] 領域の [User accepted message] フィールドおよび [User rejected message] フィールドにそれぞれメッセージを入力します。

Telnet からのユーザ認証を実行する場合、[User accepted message] オプションおよび [User rejected message] オプションを使用すれば、認証試行が RADIUS サーバにより受け入れられた、または拒否されたことを示すさまざまな状態のプロンプトを表示できます。

これらのメッセージ テキストをそれぞれ指定した場合、ASA では、RADIUS サーバにより認証されたユーザに対してはユーザ承認メッセージ テキストが表示され、認証されなかったユーザに対しては ASA によりユーザ拒否メッセージ テキストが表示されます。HTTP セッションおよび FTP セッションの認証では、プロンプトにチャレンジ テキストのみが表示されます。ユーザ承認メッセージ テキストおよびユーザ拒否メッセージ テキストは表示されません。

ステップ 3　[Apply] をクリックして変更内容を実行コンフィギュレーションに保存します。

RADIUS サーバによる認証および許可のテスト

ASA において RADIUS サーバへのアクセスやユーザの認証および許可が実行できるかどうかを判定するには、次の手順を実行します。

ステップ 1　[Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups] > [AAA Server Groups] テーブルで、サーバが含まれるサーバ グループをクリックします。

テーブル内の該当する行が選択されます。

ステップ 2　[Selected Group] テーブルの [Servers] から、テストするサーバをクリックします。

テーブル内の該当する行が選択されます。

ステップ 3　[Test] をクリックします。

選択したサーバに対応する [Test AAA Server] ダイアログボックスが表示されます。

ステップ 4　実行するテストのタイプ（[Authentication] または [Authorization]）をクリックします。

ステップ 5　[Username] フィールドにユーザ名を入力します。

ステップ 6　認証をテストする場合は、そのユーザ名に対応するパスワードを [Password] フィールドに入力します。

ステップ 7　[OK] をクリックします。

認証または許可のテスト メッセージが ASA からサーバへ送信されます。テストが失敗した場合は、ASDM によりエラー メッセージが表示されます。

RADIUS サーバのモニタリング

RADIUS サーバをモニタするには、次のペインを参照してください。

パス	目的
[Monitoring] > [Properties] > [AAA Servers]	設定済みの RADIUS サーバの統計情報を表示します。
[Monitoring] > [Properties] > [AAA Servers]	RADIUS サーバ実行コンフィギュレーションを表示します。

その他の関連資料

RADIUS サーバを使用した AAA の実装に関する詳細については、「RFC」（P.34-22）を参照してください。

RFC

RFC	タイトル
2138	*『Remote Authentication Dial In User Service (RADIUS)』*
2139	*『RADIUS Accounting』*
2548	*『Microsoft Vendor-specific RADIUS Attributes』*
2868	*『RADIUS Attributes for Tunnel Protocol Support』*

RADIUS サーバの機能履歴

表 34-3 に、各機能変更と、それが実装されたプラットフォーム リリースを示します。ASDM は、複数のプラットフォーム リリースとの下位互換性があるため、サポートが追加された特定の ASDM リリースは一覧には含まれていません。

表 34-3　RADIUS サーバの機能履歴

機能名	プラットフォーム リリース	機能情報
AAA の RADIUS サーバ	7.0(1)	AAA 用に RADIUS サーバを設定する方法について説明します。 次の画面が導入されました。 [Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups] [Configuration] > [Device Management] > [Users/AAA] > [Authentication Prompt]。
ASA からの RADIUS アクセス要求パケットおよび RADIUS アカウンティング要求パケットで送信された主なベンダー固有属性（VSA）	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、許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。