APPENDIX B

許可および認証用の外部サーバの設定

この付録では、セキュリティ アプライアンスで AAA をサポートするための外部 LDAP、RADIUS、または TACACS+ サーバの設定方法について説明します。外部サーバを使用するようにセキュリティ アプライアンスを設定する前に、正しいセキュリティ アプライアンス認証属性でサーバを設定し、それらの属性のサブセットから個々のユーザに対する個別の許可を割り当てる必要があります。

この付録は、次の項で構成されています。

権限および属性のポリシー実施の概要

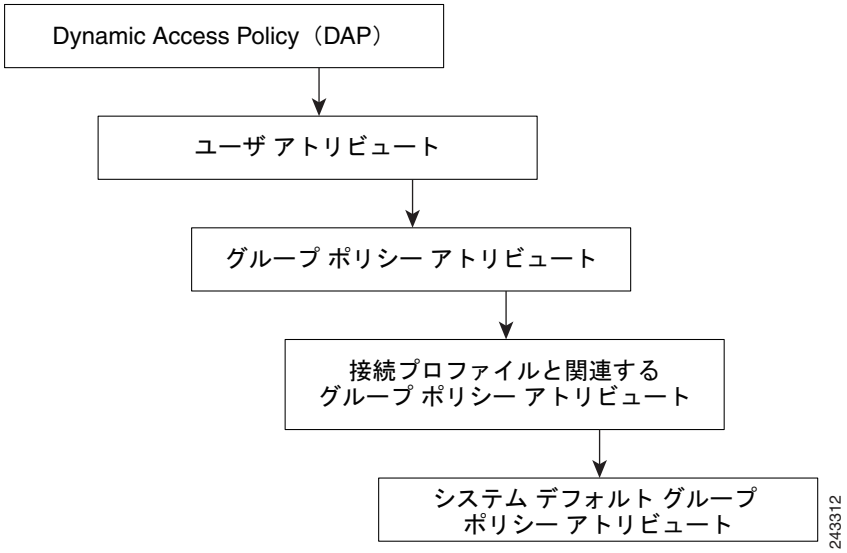
セキュリティ アプライアンスは、ユーザ許可属性（ユーザ権利またはユーザ権限とも呼ばれる）を VPN 接続に適用するためのいくつかの方法をサポートしています。ユーザ属性を、セキュリティ アプライアンスの Dynamic Access Policy（DAP; ダイナミック アクセス ポリシー）から、外部認証サーバや許可 AAA サーバ（RADIUS または LDAP）から、セキュリティ アプライアンスのグループ ポリシーから、またはこれら 3 つのすべてから取得できるようにセキュリティ アプライアンスを設定できます。

セキュリティ アプライアンスがすべてのソースから属性を受信すると、それらの属性は評価および集約され、ユーザ ポリシーに適用されます。DAP、AAA サーバ、またはグループ ポリシーから取得した属性の間で衝突がある場合、DAP から取得した属性が常に優先されます。

セキュリティ アプライアンスは、次の順序で属性を適用します（図 B-1 も参照してください）。

1. セキュリティ アプライアンスの DAP 属性：バージョン 8.0 に導入され、最も優先されます。DAP にブックマーク /URL リストを設定した場合、そのリストはグループ ポリシーのブックマーク /URL リスト セットよりも優先されます。
2. AAA サーバのユーザ属性：ユーザ認証または許可が成功すると、AAA サーバはこれらの属性を返します。これらの属性を、セキュリティ アプライアンスのローカル AAA データベースの個々のユーザに設定されている属性（ASDM のユーザ アカウント）と混同しないでください。
3. セキュリティ アプライアンスで設定されたグループ ポリシー：RADIUS サーバがユーザに対して RADIUS CLASS 属性 IETF-Class-25（OU=<group-policy>）の値を返す場合、セキュリティ アプライアンスは、ユーザを同じ名前のグループ ポリシーに配置し、サーバから返されないすべての属性をそのグループ ポリシーで適用します。LDAP サーバでは、任意の属性名を使用してセッションのグループ ポリシーを設定できます。セキュリティ アプライアンスで設定した LDAP 属性マップは、LDAP 属性を Cisco 属性 IETF-Radius-Class にマッピングします。
4. 接続プロファイル（CLI では *トンネル グループ*と呼ばれます）により割り当てられるグループ ポリシー：接続プロファイルは、接続の暫定的な設定を含み、認証前のユーザに適用されるデフォルトのグループ ポリシーが設定されています。セキュリティ アプライアンスに接続するすべてのユーザは、最初にこのグループに所属します。このグループでは、DAP、サーバから返されるユーザ属性、またはユーザに割り当てられるグループ ポリシーで不足しているすべての属性が提供されます。
5. セキュリティ アプライアンスで割り当てられたデフォルトのグループ ポリシー（DfltGrpPolicy）：システムのデフォルト属性は、DAP、ユーザ属性、グループ ポリシー、または接続プロファイルで不足している値を提供します。

図 B-1　ポリシー実施フロー



外部 LDAP サーバの設定

VPN 3000 コンセントレータと ASA/PIX 7.0 では、認証作業に Cisco LDAP スキーマが必要でした。バージョン 7.1.x 以降では、セキュリティ アプライアンスは、ネイティブ LDAP スキーマを使用して認証および許可を行うため、Cisco スキーマは必要とされません。

許可（権限ポリシー）の設定は、LDAP 属性マップを使用して行います。例については、次を参照してください。
「許可および認証用の外部サーバの設定」（P.B-1）。

この項では、LDAP サーバの構造、スキーマ、および属性について説明します。説明する項目は次のとおりです。

- 「LDAP 操作のためのセキュリティ アプライアンスの構成」（P.B-3）
- 「セキュリティ アプライアンスの LDAP コンフィギュレーションの定義」（P.B-5）
- 「ASDM を使用して LDAP を設定する場合の追加情報」（P.B-14）

上記のプロセスは、使用する LDAP サーバのタイプによって異なります。

（注）　LDAP プロトコルの詳細については、RFC 1777、2251、および 2849 を参照してください。

LDAP 操作のためのセキュリティ アプライアンスの構成

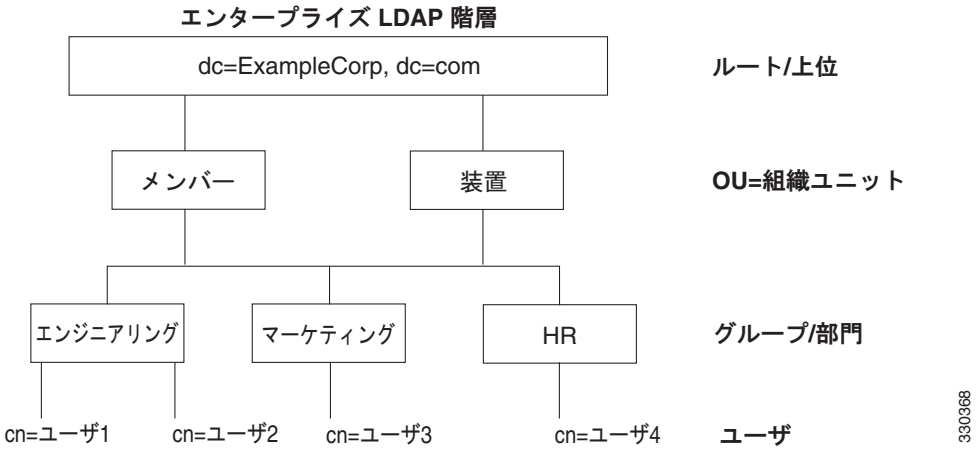
この項では、LDAP 階層、およびセキュリティ アプライアンスの LDAP サーバへの認証済みバインディング内で検索を実行する方法について説明します。説明する項目は次のとおりです。

- 「階層の検索」（P.B-4）
- 「セキュリティ アプライアンスと LDAP サーバのバインディング」（P.B-5）
- 「Active Directory の Login DN の例」（P.B-5）

LDAP コンフィギュレーションは、組織の論理階層が反映されたものにする必要があります。たとえば、Example Corporation という企業の従業員 Terry を例に考えてみます。Terry はエンジニアリンググループに従事しています。この企業の LDAP 階層は 1 つ以上のレベルを持つことができます。Terry を Example Corporation のメンバーと想定して、浅いシングルレベルの階層をセットアップすることを決定できます。あるいは、マルチレベルの階層をセットアップすることもできます。この場合、Terry は Engineering 部門のメンバーであると想定され、この部門は People と呼ばれる組織ユニットのメンバーであり、Example Corporation のメンバーです。マルチレベルの階層の例については、図 B-2 を参照してください。

マルチレベル階層はより細かく設定できますが、シングルレベル階層の方が迅速に検索できます。

図 B-2　マルチレベルの LDAP 階層



階層の検索

セキュリティ アプライアンスでは、LDAP 階層内での検索を調整できます。セキュリティ アプライアンスに次の 3 種類のフィールドを設定すると、LDAP 階層での検索開始場所とその範囲、および検索する情報のタイプを定義できます。これらのフィールドを組み合わせて使用することにより、ユーザの権限が含まれているツリーの部分だけを検索するように階層の検索を限定できます。

- LDAP Base DN は、サーバがセキュリティ アプライアンスから許可要求を受信したときにユーザ情報の検索を開始する LDAP 階層を定義します。
- Search Scope では、LDAP 階層の検索範囲を定義します。この指定では、LDAP Base DN よりもかなり下位のレベルまで検索します。サーバが行う検索を直下の 1 レベルだけにするか、サブツリー全体を検索するかを選択できます。シングルレベルの検索の方が高速ですが、サブツリー検索の方が広範囲に検索できます。
- Naming Attribute では、LDAP サーバのエントリを一意に識別する RDN を定義します。一般的な名前属性には、cn（一般名）、sAMAccountName、および userPrincipalName を含めることができます。

図 B-2 では、Example Corporation で可能な LDAP 階層の例を示します。この階層が指定されると、複数の方法で検索を定義できます。表 B-1 は、使用可能な 2 種類の検索のコンフィギュレーションを示します。

最初のコンフィギュレーションの例では、Terry が必要な LDAP 許可を得て自身の IPSec トンネル接続を確立すると、セキュリティ アプライアンスは LDAP サーバに検索要求を送信します。この要求では、サーバが Terry を代行して Engineering グループの検索を実行することを指定します。この検索は短時間でできます。

2 番目のコンフィギュレーションの例では、セキュリティ アプライアンスは、Terry を代行してサーバが Example Corporation 全体を検索するよう指示する検索要求を送信します。この検索には時間がかかります。

表 B-1　検索コンフィギュレーションの例

#	LDAP Base DN	検索範囲	名前属性	結果
1	group= Engineering,ou=People,dc=ExampleCorporation, dc=com	1 レベル	cn=Terry	検索が高速
2	dc=ExampleCorporation,dc=com	サブツリー	cn=Terry	検索に時間がかかる

セキュリティ アプライアンスと LDAP サーバのバインディング

一部の LDAP サーバ（Microsoft Active Directory サーバなど）は、セキュリティ アプライアンスに対し、他のあらゆる LDAP 操作の要求を受け入れる前に、認証済みバインディングを介してハンドシェイクを確立することを要求します。セキュリティ アプライアンスは、ログイン DN フィールドをユーザ認証要求にアタッチして、認証済みバインディングに対して識別情報を示します。Login DN フィールドでは、セキュリティ アプライアンスの認証特性を定義します。これらの特性は、管理特権を持つユーザの特性に対応している必要があります。たとえば、Login DN フィールドを cn=Administrator、cn=users、ou=people、dc=example、dc=com のように定義できます。

（注） LDAP クライアントとして、セキュリティ アプライアンスは、匿名のバインドまたは要求の送信をサポートしていません。

Active Directory の Login DN の例

Login DN は、ユーザ検索が行われる前に、セキュリティ アプライアンスがバインドの交換中に LDAP クライアントと LDAP サーバ間の信頼性を確立するために使用する LDAP サーバ上のユーザ名です。

VPN の認証/許可の操作、および、バージョン 8.0.4 以降の AD グループの取得（password-management の変更が不要なときの読み取り専用操作）では、特権の低い Login DN を使用できます。たとえば、Login DN には、Domain Users グループの memberOf で指定されているユーザを指定できます。

VPN の password-management の変更では、Login DN にはアカウント オペレータの特権が必要となります。

これらのいずれの場合でも、Login/Bind DN には、スーパーユーザ レベルの特権は必要ありません。特定の Login DN 要件については、LDAP アドミニストレータ ガイドを参照してください。

セキュリティ アプライアンスの LDAP コンフィギュレーションの定義

この項では、LDAP AV-pair 属性の構文の定義方法について説明します。説明する項目は次のとおりです。

- 「LDAP 許可でサポートされている Cisco 属性」（P.B-6）
- 「Cisco-AV-Pair 属性構文」（P.B-12）

（注）　セキュリティ アプライアンスは、数値の ID ではなく属性名に基づいて LDAP 属性を使用します。一方、RADIUS 属性には、名前ではなく数値の ID が使用されます。

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。認証サーバまたは許可サーバとして定義されている LDAP 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。

ソフトウェア バージョン 7.0 の LDAP 属性には、cVPN3000 プレフィックスが含まれています。バージョン 7.1 以降では、このプレフィックスは削除されています。

LDAP 許可でサポートされている Cisco 属性

この項では、ASA 5500、VPN 3000、および PIX 500 シリーズのセキュリティ アプライアンスで使用される属性の詳細なリスト（表 B-2）を示します。この表には、これらのセキュリティ アプライアンスを組み合わせたネットワーク構成に役立つ VPN 3000 と PIX 500 シリーズの属性サポート情報が含まれています。

表 B-2　セキュリティ アプライアンスでサポートされる LDAP 許可用の Cisco 属性

属性名 /	VPN 3000	ASA	PIX	構文 / タイプ	シングルまたはマルチ値	有効な値
Access-Hours	Y	Y	Y	文字列	シングル	time-range の名前 （Business-Hours など）
Allow-Network-Extension- Mode	Y	Y	Y	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	Y	Y	整数型	シングル	1 ～ 35791394 分
Authorization-Required	Y			整数型	シングル	0 = しない 1 = する
Authorization-Type	Y			整数型	シングル	0 = なし 1 = RADIUS 2 = LDAP
Auth-Service-Type						
Banner1	Y	Y	Y	文字列	シングル	バナー文字列
Banner2	Y	Y	Y	文字列	シングル	バナー文字列
Cisco-AV-Pair	Y	Y	Y	文字列	マルチ	次の形式のオクテット文字列： [Prefix] [Action] [Protocol] [Source] [Source Wildcard Mask] [Destination] [Destination Wildcard Mask] [Established] [Log] [Operator] [Port] 詳細については、Cisco-AV-Pair 属性構文を参照してください。
Cisco-IP-Phone-Bypass	Y	Y	Y	整数型	シングル	0 = ディセーブル 1 = イネーブル
Cisco-LEAP-Bypass	Y	Y	Y	整数型	シングル	0 = ディセーブル 1 = イネーブル

表 B-2　セキュリティ アプライアンスでサポートされる LDAP 許可用の Cisco 属性 （続き）

属性名 /	VPN 3000	ASA	PIX	構文 / タイプ	シングルまたはマルチ値	有効な値
Client-Intercept-DHCP-Configure-Msg	Y	Y	Y	ブール	シングル	0 = ディセーブル 1 = イネーブル
Client-Type-Version-Limiting	Y	Y	Y	文字列	シングル	IPSec VPN クライアントのバージョン番号を示す文字列
Confidence-Interval	Y	Y	Y	整数型	シングル	10 ～ 300 秒
DHCP-Network-Scope	Y	Y	Y	文字列	シングル	IP アドレス
DN-Field	Y	Y	Y	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
Firewall-ACL-In		Y	Y	文字列	シングル	アクセス リスト ID
Firewall-ACL-Out		Y	Y	文字列	シングル	アクセス リスト ID
IE-Proxy-Bypass-Local				ブール	シングル	0=ディセーブル 1=イネーブル
IE-Proxy-Exception-List				文字列	シングル	DNS ドメインのリスト。エントリは改行文字シーケンス（\n）で区切る必要があります。
IE-Proxy-Method	Y	Y	Y	整数型	シングル	1 = プロキシ設定を変更しない 2 = プロキシを使用しない 3 = 自動検出 4 = セキュリティ アプライアンス設定を使用する
IE-Proxy-Server	Y	Y	Y	整数型	シングル	IP アドレス
IETF-Radius-Class	Y	Y	Y		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。
IETF-Radius-Filter-Id	Y	Y	Y	文字列	シングル	セキュリティ アプライアンスで定義されたアクセス リスト名
IETF-Radius-Framed-IP-Address	Y	Y	Y	文字列	シングル	IP アドレス
IETF-Radius-Framed-IP-Netmask	Y	Y	Y	文字列	シングル	IP アドレス マスク
IETF-Radius-Idle-Timeout	Y	Y	Y	整数型	シングル	分
IETF-Radius-Service-Type	Y	Y	Y	整数型	シングル	
IETF-Radius-Session-Timeout	Y	Y	Y	整数型	シングル	
IKE-Keep-Alives	Y	Y	Y	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	Y	Y	ブール	シングル	0 = ディセーブル 1 = イネーブル

表 B-2　セキュリティ アプライアンスでサポートされる LDAP 許可用の Cisco 属性 （続き）

属性名 /	VPN 3000	ASA	PIX	構文 / タイプ	シングルまたはマルチ値	有効な値
IPSec-Authentication	Y	Y	Y	整数型	シングル	0 = なし 1 = RADIUS 2 = LDAP（許可のみ） 3 = NT ドメイン 4 = SDI（RSA） 5 = 内部 6 = RADIUS での Expiry 7 = Kerberos/Active Directory
IPSec-Auth-On-Rekey	Y	Y	Y	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	Y	Y	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	Y	Y	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	Y			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	Y	Y	整数型	シングル	0 = 必須 1 = オプション
IPSec-Default-Domain	Y	Y	Y	文字列	シングル	クライアントに送信する 1 つのデフォルト ドメイン名を指定します（1 ～ 255 文字）。
IPSec-IKE-Peer-ID-Check	Y	Y	Y	整数型	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	Y	Y	整数型	シングル	0 = ディセーブル 1 = イネーブル
IPSec-Mode-Config	Y	Y	Y	ブール	シングル	0 = ディセーブル 1 = イネーブル
IPSec-Over-UDP	Y	Y	Y	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	Y	Y	整数型	シングル	4001 ～ 49151、デフォルトは 10000
IPSec-Required-Client-Firewall-Capability	Y	Y	Y	整数型	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	Y			文字列	シングル	セキュリティ アソシエーションの名前

表 B-2　セキュリティ アプライアンスでサポートされる LDAP 許可用の Cisco 属性 （続き）

属性名 /	VPN 3000	ASA	PIX	構文 / タイプ	シングルまたはマルチ値	有効な値
IPSec-Split-DNS-Names	Y	Y	Y	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	Y	Y	整数型	シングル	0 = すべてをトンネリング 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	Y	Y	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アクセス リストの名前を指定します。
IPSec-Tunnel-Type	Y	Y	Y	整数型	シングル	1 = LAN-to-LAN 2 = リモート アクセス
IPSec-User-Group-Lock	Y			ブール	シングル	0 = ディセーブル 1 = イネーブル
L2TP-Encryption	Y			整数型	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	Y			整数型	シングル	0 = ディセーブル 1 = イネーブル
MS-Client-Subnet-Mask	Y	Y	Y	文字列	シングル	IP アドレス
PFS-Required	Y	Y	Y	ブール	シングル	0 = しない 1 = する
Port-Forwarding-Name	Y	Y		文字列	シングル	名前の文字列（「Corporate-Apps」など）
PPTP-Encryption	Y			整数型	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 例： 15 = 40/128 ビットで暗号化 / ステートレスが必要
PPTP-MPPC-Compression	Y			整数型	シングル	0 = ディセーブル 1 = イネーブル
Primary-DNS	Y	Y	Y	文字列	シングル	IP アドレス
Primary-WINS	Y	Y	Y	文字列	シングル	IP アドレス
Privilege-Level						

表 B-2　セキュリティ アプライアンスでサポートされる LDAP 許可用の Cisco 属性 （続き）

属性名 /	VPN 3000	ASA	PIX	構文 / タイプ	シングルまたはマルチ値	有効な値
Required-Client-Firewall-Vendor-Code	Y	Y	Y	整数型	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	Y	Y	文字列	シングル	文字列
Required-Client-Firewall-Product-Code	Y	Y	Y	整数型	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
Require-HW-Client-Auth	Y	Y	Y	ブール	シングル	0 = ディセーブル 1 = イネーブル
Require-Individual-User-Auth	Y	Y	Y	整数型	シングル	0 = ディセーブル 1 = イネーブル
Secondary-DNS	Y	Y	Y	文字列	シングル	IP アドレス
Secondary-WINS	Y	Y	Y	文字列	シングル	IP アドレス
SEP-Card-Assignment				整数型	シングル	未使用
Simultaneous-Logins	Y	Y	Y	整数型	シングル	0-2147483647
Strip-Realm	Y	Y	Y	ブール	シングル	0 = ディセーブル 1 = イネーブル
TACACS-Authtype	Y	Y	Y	整数	シングル	
TACACS-Privilege-Level	Y	Y	Y	整数	シングル	
Tunnel-Group-Lock		Y	Y	文字列	シングル	トンネル グループの名前または「none」

表 B-2　セキュリティ アプライアンスでサポートされる LDAP 許可用の Cisco 属性 （続き）

属性名 /	VPN 3000	ASA	PIX	構文 / タイプ	シングルまたはマルチ値	有効な値
Tunneling-Protocols	Y	Y	Y	整数型	シングル	1 = PPTP 2 = L2TP 4 = IPSec 8 = L2TP/IPSec 16 = WebVPN. 8 および 4 は相互排他値 （0 ～ 11、16 ～ 27 は有効値）
Use-Client-Address	Y			ブール	シングル	0 = ディセーブル 1 = イネーブル
User-Auth-Server-Name	Y			文字列	シングル	IP アドレスまたはホスト名
User-Auth-Server-Port	Y			整数型	シングル	サーバ プロトコルのポート番号
User-Auth-Server-Secret	Y			文字列	シングル	サーバのパスワード
WebVPN-ACL-Filters		Y		文字列	シングル	アクセス リスト名
WebVPN-Apply-ACL-Enable	Y	Y		整数型	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-Citrix-Support-Enable	Y	Y		整数型	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-Content-Filter-Parameters	Y	Y		整数型	シングル	1 = Java および 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 複数のパラメータをフィルタリングするには値を加算します。たとえば、Java スクリプトとクッキーの両方をフィルタリングするには 10 を入力します。（10 = 2 + 8）
WebVPN-Enable-functions				整数型	シングル	使用しない（廃止）
WebVPN-Exchange-Server-Address				文字列	シングル	使用しない（廃止）
WebVPN-Exchange-Server-NETBIOS-Name				文字列	シングル	使用しない（廃止）
WebVPN-File-Access-Enable	Y	Y		整数型	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-File-Server-Browsing-Enable	Y	Y		整数型	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-File-Server-Entry- Enable	Y	Y		整数型	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-Forwarded-Ports		Y		文字列	シングル	ポート転送リスト名
WebVPN-Homepage	Y	Y		文字列	シングル	URL（http://example-portal.com など）
WebVPN-Macro-Substitution-Value1	Y	Y		文字列	シングル	

表 B-2　セキュリティ アプライアンスでサポートされる LDAP 許可用の Cisco 属性 （続き）

属性名 /	VPN 3000	ASA	PIX	構文 / タイプ	シングルまたはマルチ値	有効な値
WebVPN-Macro-Substitution-Value2	Y	Y		文字列	シングル	
WebVPN-Port-Forwarding-Auto-Download-Enable	Y	Y		整数型	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-Port-Forwarding- Enable	Y	Y		整数型	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-Port-Forwarding-Exchange-Proxy-Enable	Y	Y		整数型	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-Port-Forwarding-HTTP-Proxy-Enable	Y	Y		整数型	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-Single-Sign-On-Server-Name		Y		文字列	シングル	SSO サーバの名前（1 ～ 31 文字）
WebVPN-SVC-Client-DPD	Y	Y		整数型	シングル	0 = ディセーブル n = デッドピア検出値（30 ～ 3600 秒）
WebVPN-SVC-Compression	Y	Y		整数型	シングル	0 = なし 1 = デフレート圧縮
WebVPN-SVC-Enable	Y	Y		整数型	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-SVC-Gateway-DPD	Y	Y		整数型	シングル	0 = ディセーブル n = デッドピア検出値（30 ～ 3600 秒）
WebVPN-SVC-Keepalive	Y	Y		整数型	シングル	0 = ディセーブル n = キープアライブ値（15 ～ 600 秒）
WebVPN-SVC-Keep-Enable	Y	Y		整数型	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-SVC-Rekey-Method	Y	Y		整数型	シングル	0 = なし 1 = SSL 2 = 新規トンネル 3 = 任意（SSL に設定）
WebVPN-SVC-Rekey-Period	Y	Y		整数型	シングル	0 = ディセーブル n = 分単位の再試行間隔 （4 ～ 10080 分）
WebVPN-SVC-Required-Enable	Y	Y		整数型	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-URL-Entry-Enable	Y	Y		整数型	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-URL-List		Y		文字列	シングル	URL リスト名

Cisco-AV-Pair 属性構文

Cisco-AV-Pair ルールの構文は次のとおりです。

[Prefix] [Action] [Protocol] [Source] [Source Wildcard Mask] [Destination] [Destination Wildcard Mask] [Established] [Log] [Operator] [Port]

表 B-3 で構文のルールについて説明します。

表 B-3　AV-Pair 属性の構文ルール

フィールド	説明
Prefix	AV ペアの固有の識別子。例：ip:inacl#1=（標準アクセス リスト用）または webvpn:inacl#（クライアントレス SSL VPN アクセス リスト用）。このフィールドは、フィルタが AV ペアとして送信された場合にだけ表示されます。
Action	deny、permit など、ルールが一致した場合に実行するアクション。
Protocol	IP プロトコルの番号または名前。0 ～ 255 の整数値、または icmp、igmp、ip、tcp、udp のいずれかのキーワード。
Source	パケットを送信するネットワークまたはホスト。IP アドレス、ホスト名、またはキーワード「any」で指定します。IP アドレスを使用する場合、続いて Source Wildcard Mask を指定する必要があります。
Source Wildcard Mask	送信元アドレスに適用されるワイルドカード マスク。
Destination	パケットを受信するネットワークまたはホスト。IP アドレス、ホスト名、またはキーワード「any」で指定します。IP アドレスを使用する場合、続いて Source Wildcard Mask を指定する必要があります。
Destination Wildcard Mask	宛先アドレスに適用されるワイルドカード マスク。
Log	FILTER ログ メッセージを生成します。重大度レベル 9 のイベントを生成するには、このキーワードを使用する必要があります。
Operator	論理演算子：greater than、less than、equal to、not equal to。
Port	TCP または UDP ポートの番号（0 ～ 65535）。

次に例を示します。

```
ip:inacl#1=deny ip 10.155.10.0 0.0.0.255 10.159.2.0 0.0.0.255 log
ip:inacl#2=permit TCP any host 10.160.0.1 eq 80 log

webvpn:inacl#1=permit url http://www.website.com
webvpn:inacl#2=deny smtp any host 10.1.3.5
webvpn:inacl#3=permit url cifs://mar_server/peopleshare1
```

（注） リモート IPSec トンネルおよび SSL VPN Client（SVC）トンネルにアクセス リストを適用するには、Cisco-AV-Pair エントリにプレフィックス ip:inacl# を追加して使用してください。

SSL VPN クライアントレス（ブラウザモード）トンネルにアクセス リストを適用するには、Cisco-AV-Pair エントリにプレフィックス webvpn:inacl# を追加して使用してください。

表 B-4 に、Cisco-AV-Pair 属性のトークンの一覧を示します。

表 B-4　セキュリティ アプライアンスでサポートされるトークン

トークン	構文のフィールド	説明
ip:inacl#*Num*=	該当なし（識別子）	(*Num* は固有の整数)。AV ペアのアクセス コントロール リストをすべて開始します。リモート IPSec トンネルと SSL VPN（SVC）トンネルにアクセス リストを適用します。
webvpn:inacl#*Num*=	該当なし（識別子）	(*Num* は固有の整数)。クライアントレス SSL AV ペアのアクセス コントロール リストをすべて開始します。クライアントレス（ブラウザモード）トンネルにアクセス リストを適用します。
deny	アクション	アクションを拒否します。(デフォルト)
permit	アクション	アクションを許可します。
icmp	プロトコル	インターネット制御メッセージ プロトコル（ICMP）
1	プロトコル	インターネット制御メッセージ プロトコル（ICMP）
IP	プロトコル	インターネット プロトコル（IP）
0	プロトコル	インターネット プロトコル（IP）
TCP	プロトコル	伝送制御プロトコル（TCP）
6	プロトコル	伝送制御プロトコル（TCP）
UDP	プロトコル	ユーザ データグラム プロトコル（UDP）
17	プロトコル	ユーザ データグラム プロトコル（UDP）
any	ホスト名	すべてのホストにルールを適用します。
host	ホスト名	ホスト名を示す任意の英数字文字列。
log	ログ	イベントが一致すると、フィルタ ログ メッセージが表示されます （permit and log または deny and log の場合と同様)。
lt	演算子	値より小さい
gt	演算子	値より大きい
eq	演算子	値と等しい
neq	演算子	値と等しくない
range	演算子	この範囲に含まれる。range の後に 2 つの値を続けます。

ASDM を使用して LDAP を設定する場合の追加情報

ASDM を使用して LDAP を設定する場合の追加情報は、次の URL の Cisco.com のセキュリティ アプライアンスに関するマニュアル領域で入手できます。

http://www.cisco.com/en/US/products/ps6121/products_installation_and_configuration_guides_list.html

カテゴリ「*Selected ASDM Configuration Topics for ASA*」には、Microsoft Active Directory サーバを使用してセキュリティ アプライアンス上で認証および許可を設定する手順の例が含まれています。

- ユーザベースの属性ポリシーの適用
- 特定のグループ ポリシーへの LDAP ユーザの配置
- AnyConnect トンネルへのスタティック IP アドレスの割り当て
- ダイヤルインの許可または拒否アクセスの適用

- ログイン時間と Time-of-Day ルールの適用

その他の設定例については、Cisco.com にある次のテクニカル ノートを参照してください。

- 『*ASA/PIX: Mapping VPN Clients to VPN Group Policies Through LDAP Configuration Example*』
  http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a008089149d.shtml
- 『*PIX/ASA 8.0: Use LDAP Authentication to Assign a Group Policy at Login*』
  http://www.cisco.com/en/US/partner/products/ps6120/products_configuration_example09186a00808d1a7c.shtml

外部 RADIUS サーバの設定

この項では、RADIUS の設定手順の概要を示し、Cisco RADIUS 属性を定義します。説明する項目は次のとおりです。

RADIUS 設定手順の確認

この項では、セキュリティ アプライアンスのユーザ認証および許可をサポートするために必要な RADIUS 設定手順について説明します。次の手順に従って、セキュリティ アプライアンスと相互作用する RADIUS サーバをセットアップします。

ステップ 1　セキュリティ アプライアンスの属性を 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。
- FUNK RADIUS サーバを使用している場合：シスコは、セキュリティ アプライアンスの属性がすべて含まれるディクショナリ ファイルを提供しています。このディクショナリ ファイル `cisco3k.dct` は、CCO のソフトウェア センターまたはセキュリティ アプライアンスの CD-ROM から入手してください。ディクショナリ ファイルをサーバにロードします。
- 他のベンダーの RADIUS サーバ（Microsoft Internet Authentication Service など）：セキュリティ アプライアンス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。セキュリティ アプライアンス RADIUS 許可属性および値のリストについては、表 B-5 を参照してください。

ステップ 2　権限および属性を持つユーザまたはグループをセットアップし、IPSec または SSL トンネルの確立時に送信します。

セキュリティ アプライアンスの RADIUS 許可属性

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。

表 B-5 に、ユーザ許可に使用でき、セキュリティ アプライアンスがサポートしている使用可能なすべての 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。アプライアンスは、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。LDAP 属性は、ID ではなく属性名で使用します。

表 B-5　セキュリティ アプライアンスでサポートされる RADIUS 属性と値

属性名	VPN 3000	ASA	PIX	属性 #	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	Y	Y	1	文字列	シングル	時間範囲の名前（Business-hours など）
Simultaneous-Logins	Y	Y	Y	2	整数型	シングル	0 ～ 2147483647 の整数
Primary-DNS	Y	Y	Y	5	文字列	シングル	IP アドレス
Secondary-DNS	Y	Y	Y	6	文字列	シングル	IP アドレス
Primary-WINS	Y	Y	Y	7	文字列	シングル	IP アドレス
Secondary-WINS	Y	Y	Y	8	文字列	シングル	IP アドレス
SEP-Card-Assignment				9	整数型	シングル	未使用
Tunneling-Protocols	Y	Y	Y	11	整数型	シングル	1 = PPTP 2 = L2TP 4 = IPSec 8 = L2TP/IPSec 16 = WebVPN. 4 および 8 は相互排他値、0 ～ 11 および 16 ～ 27 は有効値
IPSec-Sec-Association	Y			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-Authentication	Y			13	整数型	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
Banner1	Y	Y	Y	15	文字列	シングル	バナー文字列
IPSec-Allow-Passwd-Store	Y	Y	Y	16	ブール	シングル	0 = ディセーブル 1 = イネーブル

表 B-5　セキュリティ アプライアンスでサポートされる RADIUS 属性と値 （続き）

属性名	VPN 3000	ASA	PIX	属性 #	構文 / タイプ	シングルまたはマルチ値	説明または値
Use-Client-Address	Y			17	ブール	シングル	0 = ディセーブル 1 = イネーブル
PPTP-Encryption	Y			20	整数型	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-Encryption	Y			21	整数型	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
IPSec-Split-Tunnel-List	Y	Y	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アクセス リストの名前を指定します。
IPSec-Default-Domain	Y	Y	Y	28	文字列	シングル	クライアントに送信する 1 つのデフォルト ドメイン名を指定します（1 ～ 255 文字）。
IPSec-Split-DNS-Names	Y	Y	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-Tunnel-Type	Y	Y	Y	30	整数型	シングル	1 = LAN-to-LAN 2 = リモート アクセス
IPSec-Mode-Config	Y	Y	Y	31	ブール	シングル	0 = ディセーブル 1 = イネーブル
IPSec-User-Group-Lock	Y			33	ブール	シングル	0 = ディセーブル 1 = イネーブル
IPSec-Over-UDP	Y	Y	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	Y	Y	35	整数型	シングル	4001 ～ 49151、デフォルトは 10000

表 B-5　セキュリティ アプライアンスでサポートされる RADIUS 属性と値 （続き）

属性名	VPN 3000	ASA	PIX	属性 #	構文 / タイプ	シングルまたはマルチ値	説明または値
Banner2	Y	Y	Y	36	文字列	シングル	Banner1 文字列に連結されているバナー文字列（設定されている場合）。
PPTP-MPPC-Compression	Y			37	整数型	シングル	0 = ディセーブル 1 = イネーブル
L2TP-MPPC-Compression	Y			38	整数型	シングル	0 = ディセーブル 1 = イネーブル
IPSec-IP-Compression	Y	Y	Y	39	整数型	シングル	0 = ディセーブル 1 = イネーブル
IPSec-IKE-Peer-ID-Check	Y	Y	Y	40	整数型	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
IKE-Keep-Alives	Y	Y	Y	41	ブール	シングル	0 = ディセーブル 1 = イネーブル
IPSec-Auth-On-Rekey	Y	Y	Y	42	ブール	シングル	0 = ディセーブル 1 = イネーブル
Required-Client- Firewall-Vendor-Code	Y	Y	Y	45	整数型	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）

表 B-5　セキュリティ アプライアンスでサポートされる RADIUS 属性と値 （続き）

属性名	VPN 3000	ASA	PIX	属性 #	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	Y	Y	46	整数型	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-Client-Firewall-Description	Y	Y	Y	47	文字列	シングル	文字列
Require-HW-Client-Auth	Y	Y	Y	48	ブール	シングル	0 = ディセーブル 1 = イネーブル
Required-Individual-User-Auth	Y	Y	Y	49	整数型	シングル	0 = ディセーブル 1 = イネーブル
Authenticated-User-Idle-Timeout	Y	Y	Y	50	整数型	シングル	1 ～ 35791394 分
Cisco-IP-Phone-Bypass	Y	Y	Y	51	整数型	シングル	0 = ディセーブル 1 = イネーブル
IPSec-Split-Tunneling-Policy	Y	Y	Y	55	整数型	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-Required-Client-Firewall-Capability	Y	Y	Y	56	整数型	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

表 B-5　セキュリティ アプライアンスでサポートされる RADIUS 属性と値 （続き）

属性名	VPN 3000	ASA	PIX	属性 #	構文 / タイプ	シングルまたはマルチ値	説明または値
IPSec-Client-Firewall-Filter-Name	Y			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	Y	Y	58	整数型	シングル	0 = 必須 1 = オプション
IPSec-Backup-Servers	Y	Y	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-Backup-Server-List	Y	Y	Y	60	文字列	シングル	サーバ アドレス（スペース区切り）
DHCP-Network-Scope	Y	Y	Y	61	文字列	シングル	IP アドレス
Intercept-DHCP-Configure-Msg	Y	Y	Y	62	ブール	シングル	0 = ディセーブル 1 = イネーブル
MS-Client-Subnet-Mask	Y	Y	Y	63	ブール	シングル	IP アドレス
Allow-Network-Extension-Mode	Y	Y	Y	64	ブール	シングル	0 = ディセーブル 1 = イネーブル
Authorization-Type	Y	Y	Y	65	整数型	シングル	0 = なし 1 = RADIUS 2 = LDAP
Authorization-Required	Y			66	整数型	シングル	0 = しない 1 = する
Authorization-DN-Field	Y	Y	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
IKE-KeepAlive-Confidence-Interval	Y	Y	Y	68	整数型	シングル	10 ～ 300 秒
WebVPN-Content-Filter-Parameters	Y	Y		69	整数型	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

表 B-5　セキュリティ アプライアンスでサポートされる RADIUS 属性と値 （続き）

属性名	VPN 3000	ASA	PIX	属性 #	構文 / タイプ	シングルまたはマルチ値	説明または値
WebVPN-URL-List		Y		71	文字列	シングル	URL リスト名
WebVPN-Port-Forward-List		Y		72	文字列	シングル	ポート転送リスト名
WebVPN-Access-List		Y		73	文字列	シングル	アクセス リスト名
Cisco-LEAP-Bypass	Y	Y	Y	75	整数型	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-Homepage	Y	Y		76	文字列	シングル	URL（http://example-portal.com など）
Client-Type-Version-Limiting	Y	Y	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
WebVPN-Port-Forwarding-Name	Y	Y		79	文字列	シングル	名前の文字列（「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。
IE-Proxy-Server	Y			80	文字列	シングル	IP アドレス
IE-Proxy-Server-Policy	Y			81	整数型	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
IE-Proxy-Exception-List	Y			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-Bypass-Local	Y			83	整数型	シングル	0 = なし 1 = ローカル
IKE-Keepalive-Retry-Interval	Y	Y	Y	84	整数型	シングル	2 ～ 10 秒
Tunnel-Group-Lock		Y	Y	85	文字列	シングル	トンネル グループの名前または「none」
Access-List-Inbound		Y	Y	86	文字列	シングル	アクセス リスト ID
Access-List-Outbound		Y	Y	87	文字列	シングル	アクセス リスト ID

表 B-5　セキュリティ アプライアンスでサポートされる RADIUS 属性と値 （続き）

属性名	VPN 3000	ASA	PIX	属性 #	構文 / タイプ	シングルまたはマルチ値	説明または値
Perfect-Forward-Secrecy-Enable	Y	Y	Y	88	ブール	シングル	0 = しない 1 = する
NAC-Enable	Y			89	整数型	シングル	0 = しない 1 = する
NAC-Status-Query-Timer	Y			90	整数型	シングル	30 ～ 1800 秒
NAC-Revalidation-Timer	Y			91	整数型	シングル	300 ～ 86400 秒
NAC-Default-ACL	Y			92	文字列		アクセス リスト
WebVPN-URL-Entry-Enable	Y	Y		93	整数型	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-File-Access-Enable	Y	Y		94	整数型	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-File-Server-Entry-Enable	Y	Y		95	整数型	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-File-Server-Browsing-Enable	Y	Y		96	整数型	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-Port-Forwarding-Enable	Y	Y		97	整数型	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-Outlook-Exchange-Proxy-Enable	Y	Y		98	整数型	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-Port-Forwarding-HTTP-Proxy	Y	Y		99	整数型	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-Auto-Applet-Download-Enable	Y	Y		100	整数型	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-Citrix-Metaframe-Enable	Y	Y		101	整数型	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-Apply-ACL	Y	Y		102	整数型	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-SSL-VPN-Client-Enable	Y	Y		103	整数型	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-SSL-VPN-Client-Required	Y	Y		104	整数型	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-SSL-VPN-Client-Keep-Installation	Y	Y		105	整数型	シングル	0 = ディセーブル 1 = イネーブル

表 B-5　セキュリティ アプライアンスでサポートされる RADIUS 属性と値 （続き）

属性名	VPN 3000	ASA	PIX	属性 #	構文 / タイプ	シングルまたはマルチ値	説明または値
SVC-Keepalive	Y	Y		107	整数型	シングル	0 = オフ 15 ～ 600 秒
SVC-DPD-Interval-Client	Y	Y		108	整数型	シングル	0 = オフ 5 ～ 3600 秒
SVC-DPD-Interval-Gateway	Y	Y		109	整数型	シングル	0 = オフ 5 ～ 3600 秒
SVC-Rekey-Time		Y		110	整数型	シングル	0 = ディセーブル 1 ～ 10080 分
WebVPN-Deny-Message		Y		116	文字列	シングル	有効な文字列（500 文字以内）
SVC-DTLS		Y		123	整数型	シングル	0 = False 1 = True
SVC-MTU		Y		125	整数型	シングル	MTU 値 256 ～ 1406 バイト
SVC-Modules		Y		127	文字列	シングル	文字列（モジュールの名前）
SVC-Profiles		Y		128	文字列	シングル	文字列（プロファイルの名前）
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	整数型	シングル	5 ～ 120 秒
IE-Proxy-PAC-URL		Y		133	文字列	シングル	PAC アドレス文字列
Strip-Realm	Y	Y	Y	135	ブール	シングル	0 = ディセーブル 1 = イネーブル
Smart-Tunnel		Y		136	文字列	シングル	スマート トンネルの名前

表 B-5　セキュリティ アプライアンスでサポートされる RADIUS 属性と値 （続き）

属性名	VPN 3000	ASA	PIX	属性 #	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	整数型	シングル	0 = ディセーブル Otherwise = イネーブル
Smart-Tunnel-Auto		Y		138	整数型	シングル	0 = ディセーブル 1 = イネーブル 2 = 自動スタート
VLAN		Y		140	整数型	シングル	0 ～ 4094
NAC-Settings		Y		141	文字列	シングル	NAC ポリシーの名前
Member-Of		Y	Y	145	文字列	シングル	カンマ区切りの文字列。例： エンジニアリング、営業
Address-Pools		Y	Y	217	文字列	シングル	IP ローカル プールの名前
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
Privilege-Level		Y	Y	220	整数型	シングル	0 ～ 15 の整数。
WebVPN-Macro-Value1		Y		223	文字列	シングル	無制限
WebVPN-Macro-Value2		Y		224	文字列	シングル	無制限

外部 TACACS+ サーバの設定

セキュリティ アプライアンス は、TACACS+ 属性をサポートします。TACACS+ は、認証、許可、アカウンティングの機能を分離します。プロトコルでは、必須とオプションの 2 種類の属性をサポートします。サーバとクライアントの両方で必須属性を解釈できる必要があり、また、必須属性はユーザに適用する必要があります。オプションの属性は、解釈または使用できることも、できないこともあります。

（注）　TACACS+ 属性を使用するには、NAS で AAA サービスをイネーブルにしておいてください。

表 B-6 に、カットスルー プロキシ接続に対してサポートされている TACACS+ 許可応答属性の一覧を示します。表 B-7 に、サポートされている TACACS+ アカウンティング属性の一覧を示します。

表 B-6　サポートされる TACACS+ 許可応答属性

属性	説明
acl	接続に適用する、ローカルで設定済みのアクセス リストを識別します。
idletime	認証済みユーザ セッションが終了する前に許可される非アクティブ時間（分）を示します。
timeout	認証済みユーザ セッションが終了する前に認証クレデンシャルがアクティブな状態でいる絶対時間（分）を指定します。

表 B-7　サポートされる TACACS+ アカウンティング属性

属性	説明
bytes_in	この接続中に転送される入力バイト数を指定します（ストップ レコードのみ）。
bytes_out	この接続中に転送される出力バイト数を指定します（ストップ レコードのみ）。
cmd	実行するコマンドを定義します（コマンド アカウンティングのみ）。
disc-cause	切断理由を特定する数字コードを示します（ストップ レコードのみ）。
elapsed_time	接続の経過時間（秒）を定義します（ストップ レコードのみ）。
foreign_ip	トンネル接続のクライアントの IP アドレスを指定します。最下位のセキュリティ インターフェイスでカットスルー プロキシ接続のアドレスを定義します。
local_ip	トンネル接続したクライアントの IP アドレスを指定します。最上位のセキュリティ インターフェイスでカットスルー プロキシ接続のアドレスを定義します。
NAS port	接続のセッション ID が含まれます。
packs_in	この接続中に転送される入力パケット数を指定します。
packs_out	この接続中に転送される出力パケット数を指定します。
priv-level	コマンド アカウンティング要求に対するユーザの権限レベル、または 1 に設定されます。
rem_iddr	クライアントの IP アドレスを示します。
service	使用するサービスを指定します。コマンド アカウンティングだけは、常に「シェル」に設定されます。
task_id	アカウンティング トランザクションに固有のタスク ID を指定します。
username	ユーザの名前を示します。