APPENDIX **B**

認可と認証のため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、VPN 3000、および PIX ユーザを認証および認可できるように外部 LDAP または RADIUS サーバを設定する方法について説明します。認証はユーザを確認し、認可はユーザが実行できる範囲を決定します。セキュリティ アプライアンスに外部サーバの使用を設定する前に、まずサーバにセキュリティ アプライアンスの認可アトリビュートを正しく設定し、そのアトリビュートのサブセットから特定の権限を個々のユーザに割り当てる必要があります。

この付録には、次の項があります。

LDAP、RADIUS、またはローカルの認証および認可の選択

使用するプラットフォームに適した認証または認可の方式を判別できるように、この項では、セキュリティ アプライアンス（ASA）、PIX、および VPN 3000 の各プラットフォームに提供されている LDAP および RADIUS のサポートについて説明します。

- LDAP 認証

  PIX 7.1.x およびセキュリティ アプライアンスだけでサポートされます。VPN 3000 ではネイティブの LDAP 認証をサポートしません。LDAP サーバはユーザ名を取得および検索し、定義されているアトリビュートがあれば認可機能の一部として適用します。

- LDAP 認可

  PIX、VPN 3000、およびセキュリティ アプライアンスでサポートされます。LDAP サーバはユーザ名を取得および検索し、定義されているアトリビュートがあれば適用します。

- RADIUS 認証

  PIX、VPN 3000、およびセキュリティ アプライアンスでサポートされます。RADIUS サーバはユーザ名を取得して検索し、定義されているアトリビュートがあれば認可機能の実行時に適用します。

- RADIUS 認可

  PIX、VPN 3000、およびセキュリティ アプライアンスでサポートされます。RADIUS サーバはユーザ名を取得および検索し、定義されているアトリビュートがあれば適用します。

- ローカル認証

  PIX、VPN 3000、およびセキュリティ アプライアンスでサポートされます。ローカル / 内部サーバはユーザ名を取得および検索し、定義されているアトリビュートがあれば認可機能の一部として適用します。

- ローカル認可

  PIX 7.1.x およびセキュリティ アプライアンスだけでサポートされます。ローカル / 内部サーバはユーザ名を取得および検索し、定義されているアトリビュートがあれば適用します。

権限とアトリビュートのポリシー適用について

ローカル / 内部データベース、RADIUS/LDAP 認証サーバ、または RADIUS/LDAP 認可サーバのいずれかからユーザ アトリビュートを受信するようにセキュリティ アプライアンスを設定できます。異なるアトリビュートを持つグループ ポリシーをユーザに設定することもできますが、常にユーザ アトリビュートが優先されます。デバイスがユーザとグループを認証すると、セキュリティ アプライアンスはユーザ アトリビュート セットとグループ アトリビュート セットを組み合せて 1 つの集約アトリビュート セットにします。セキュリティ アプライアンスは次の順序でアトリビュートを使用し、認証されたユーザに次の集約アトリビュート セットを適用します。

1. ユーザ　アトリビュート：サーバは、ユーザ認証または認可が正常に終了するとこのアトリビュートを返します。このアトリビュートは他のすべてのアトリビュートよりも優先されます。
2. グループ　ポリシー　アトリビュート：ユーザに関連付けられたグループ　ポリシーのアトリビュートです。ローカル データベース内のユーザ グループ ポリシー名は「vpn-group-policy」アトリビュートで識別します。外部 RADIUS/LDAP サーバの場合は、「OU=GroupName;」形式の RADIUS CLASS アトリビュートの値（25）で識別します。グループ ポリシーは、ユーザ アトリビュートに不足しているアトリビュートを提供します。両方に値がある場合は、ユーザ アトリビュートがグループ ポリシー アトリビュートを上書きします。
3. トンネル グループ default-group-policy アトリビュート：これは、トンネル グループに関連付けられている default-group-policy（Base グループ）のアトリビュートです。グループ ポリシーを検索した後、トンネル グループの default-group-policy は、ユーザ アトリビュートまたはグループ アトリビュートに不足しているアトリビュートを提供します。両方に値がある場合は、ユーザ アトリビュートがグループ ポリシー アトリビュートを上書きします。
4. システム デフォルト アトリビュート：システム デフォルト アトリビュートは、ユーザ、グループ、トンネル グループのアトリビュートに不足しているアトリビュートを提供します。

外部 LDAP サーバの設定

（注）　LDAP プロトコルの詳細については、RFC1777、RFC2251、および RFC2849 を参照してください。

この項では、LDAP サーバの構造、スキーマ、およびアトリビュートについて説明します。次の項目を取り上げます。

- LDAP ディレクトリ構造と設定手順の確認
- セキュリティ アプライアンスの LDAP スキーマの構造
- セキュリティ アプライアンスの LDAP スキーマの定義
- LDAP サーバへのスキーマのロード
- ユーザ権限の定義

LDAP ディレクトリ構造と設定手順の確認

LDAP サーバには、情報をディレクトリ内のエントリとして保存します。LDAP スキーマには、このようなエントリに保存される情報のタイプを定義します。スキーマには、クラスと、各クラスのオブジェクトに含めることができる必須およびオプションのアトリビュートのセットをリストします。

LDAP サーバにセキュリティ アプライアンスとの相互運用を設定するには、セキュリティ アプライアンス認可スキーマを定義します。セキュリティ アプライアンス認可スキーマには、セキュリティ アプライアンスがサポートするクラスとそのクラスのアトリビュートを定義します。具体的には、セキュリティ アプライアンス ユーザの認可に使用される可能性があるオブジェクト クラス（cVPN3000-User-Authorization）と、そのクラスで有効なアトリビュートすべて（アクセス時間、プライマリ DNS など）が含まれます。各アトリビュートは、アトリビュート名、番号（オブジェクト ID または OID と呼ばれる）、タイプ、および有効な値で構成されます。

セキュリティ アプライアンス認可スキーマを定義してサーバにロードしたら、セキュリティ アプライアンスのアトリビュートと権限、およびサーバの使用を認可するユーザごとの値を定義します。

LDAP サーバのセットアップ手順を要約すると、次のようになります。

- セキュリティ アプライアンス LDAP 認可スキーマを組織の階層構成に基づいて設計する。
- セキュリティ アプライアンス認可スキーマを定義する。
- LDAP サーバにスキーマをロードする 。
- 各ユーザの権限を LDAP サーバに定義する。

上記プロセスの具体的な手順は、使用する LDAP サーバのタイプによって異なります。

セキュリティ アプライアンスの LDAP スキーマの構造

この項では、LDAP 階層内の検索を行う方法と、セキュリティ アプライアンス上で LDAP サーバへの認証バインディングを行う方法について説明します。次の項目を取り上げます。

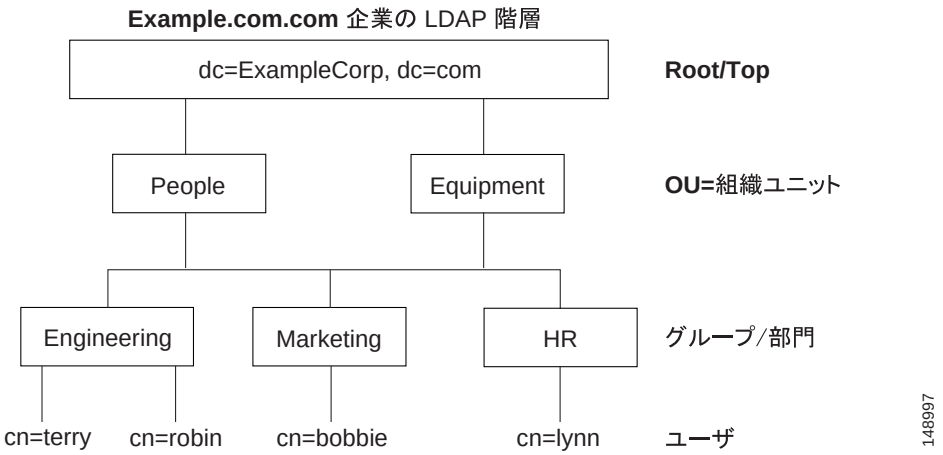
- 階層の検索
- LDAP サーバへのセキュリティ アプライアンスのバインディング

スキーマを実際に作成する前に、組織がどのような構造になっているかを検討します。LDAP スキーマには組織の論理構造を反映する必要があります。

たとえば、Example Corporation という会社に Terry という名前の従業員がいるとします。Terry は、Engineering グループに所属しています。この会社の LDAP 階層のレベルは、1 つの場合と複数の場合があります。Terry を Example Corporation のメンバーと見なして、浅いシングルレベル階層の構造にすることができます。または、マルチレベル階層の構造にすることもできます。この場合、Terry を Engineering 部門のメンバーであると見なし、Engineering 部門は People という組織ユニットのメンバーであり、People は Example Corporation のメンバーとなります。マルチレベル階層の例については、図 B-1 を参照してください。

マルチレベル階層の方が詳細に設定できますが、シングルレベル階層の方が迅速に検索できます。

図 B-1　マルチレベル 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 つのフィールドを設定すると、LDAP 階層内で検索を行うときの開始位置、範囲、および対象となる情報のタイプを定義できます。3 つのフィールドを組み合せることで、階層内の検索を、ツリー内のユーザの権限が含まれる部分だけで行うように制限できます。

- LDAP Base DN は、サーバがセキュリティ アプライアンスから認可要求を受信したときに、LDAP 階層のどこからユーザ情報の検索を開始するかを定義します。
- Search Scope は、LDAP 階層内の検索の範囲を定義します。検索は、LDAP Base DN から階層の下位に向かってここで指定したレベル数だけ行われます。サーバが検索する範囲を、直下のレベルだけに限定することも、サブツリー全体にすることもできます。シングルレベル検索はより高速ですが、サブツリー検索ではより広範囲を検索できます。
- Naming Attribute(s) は、LDAP サーバのエントリを一意に識別する RDN（Relative Distinguished Name; 相対識別名）を定義します。一般的な名前アトリビュートは、cn（共通名）と ui（ユーザ ID）です。

図 B-1 に、Example Corporation で検索可能な LDAP 階層を示します。この階層を前提とすると、複数の方法で検索を定義できます。表 B-1 に、可能な 2 つの検索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 認可を受けて IPSec トンネルを確立すると、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て、Engineering グループの Terry を検索するように指示します。この検索は短時間で行われます。

2 つ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、サーバに Example Corporation 内で Terry を検索するように指示します。この検索はより時間がかかります。

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	アトリビュートの名前	結果
1	group= Engineering,ou=People,dc=ExampleCorporation, dc=com	1 レベル	cn=Terry	検索が速い
2	dc=ExampleCorporation,dc=com	サブツリー	cn=Terry	検索が遅い

LDAP サーバへのセキュリティ アプライアンスのバインディング

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、ユーザの認証要求に Login DN フィールドを付加することにより、自身が認証バインディングされていることを示します。Login DN フィールドは、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、管理者権限を持つユーザの特性に対応する必要があります。たとえば、Login DN フィールドは cn=Administrator, cn=users, ou=people, dc=example, dc=com のように定義できます。

セキュリティ アプライアンスの LDAP スキーマの定義

この項では、LDAP スキーマの定義方法と AV ペア アトリビュート構文について説明します。次の項目を取り上げます。

- Cisco-AV-Pair アトリビュート構文
- セキュリティ アプライアンスの認可スキーマの例

LDAP 階層にどのようにユーザ情報を構造化するか決まったら、この組織をスキーマに定義します。スキーマを定義するには、最初にオブジェクト クラス名を定義します。セキュリティ アプライアンス ディレクトリのクラス名は、cVPN3000-User-Authorization です。このクラスのオブジェクト ID（OID）は、1.2.840.113556.1.8000.795.1.1 です。ディレクトリ内のすべてのエントリまたはユーザはこのクラスのオブジェクトになります。

一部の LDAP サーバ（Microsoft Active Directory LDAP サーバなど）では、一度 OID を定義したらその OID を再度使用できません。この場合は、次に大きい OID を使用してください。たとえば、誤ったクラス名 cVPN3000-Usr-Authorization を OID 1.2.840.113556.1.8000.795.1.1 で定義した場合、正しいクラス名 cVPN3000-User-Authorization を次の OID（1.2.840.113556.1.8000.795.1.2 など）で入力できます。

Microsoft Active Directory LDAP サーバの場合、LDAP Data Interchange Format（LDIF）を使用してファイルにテキスト形式でスキーマを定義します。このファイルの拡張子は、`.ldif` です（例：`schema.ldif`）。その他の LDAP サーバでは、グラフィカル ユーザ インターフェイスまたはスクリプト ファイルを使用してオブジェクト クラスとそのアトリビュートを定義します。LDIF の詳細については、RFC-2849 を参照してください。

（注）　3 種類のアプライアンスすべてで、LDAP アトリビュートはどれも文字列 cVPN3000 で開始します（例：cVPN3000-Access-Hours）。

アプライアンスは、数値の ID ではなくアトリビュート名に基づいて LDAP アトリビュートを適用します。一方、RADIUS アトリビュートは、名前ではなく数値の ID で適用されます。

認可とは、権限またはアトリビュートを適用するプロセスのことです。認証サーバまたは認可サーバとして定義されている LDAP サーバは、権限またはアトリビュートが設定されていれば、それを適用します。

PIX 500 シリーズ セキュリティ アプライアンスおよび VPN 3000 の全アトリビュートのリストについては、表 B-2 を参照してください。

すべての文字列で大文字と小文字が区別されます。また、用語の一般的な記述方式と異なる場合でも、表内のアトリビュート名と同様に表記する必要があります。たとえば、cVPN3000-IETF-RADIUS-Class ではなく cVPN3000-IETF-Radius-Class を使用します。

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 Cisco スキーマのアトリビュート

アトリビュート名 / OID（オブジェクト ID）	VPN 3000	ASA	PIX	アトリビュート OID[1]	構文 / タイプ	シングルまたはマルチ値	有効な値
cVPN3000-Access-Hours	Y	Y	Y	1	文字列	シングル	time-range の名前（Business-Hours など）
cVPN3000-Simultaneous-Logins	Y	Y	Y	2	整数	シングル	0-2147483647
cVPN3000-Primary-DNS	Y	Y	Y	3	文字列	シングル	IP アドレス
cVPN3000-Secondary-DNS	Y	Y	Y	4	文字列	シングル	IP アドレス
cVPN3000-Primary-WINS	Y	Y	Y	5	文字列	シングル	IP アドレス
cVPN3000-Secondary-WINS	Y	Y	Y	6	文字列	シングル	IP アドレス
cVPN3000-SEP-Card-Assignment				7	整数	シングル	使用しない
cVPN3000-Tunneling-Protocols	Y	Y	Y	8	整数	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）
cVPN3000-IPSec-Sec-Association	Y			9	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 Cisco スキーマのアトリビュート （続き）

アトリビュート名 / OID（オブジェクト ID）	VPN 3000	ASA	PIX	アトリビュート OID[1]	構文 / タイプ	シングルまたはマルチ値	有効な値
cVPN3000-IPSec-Authentication	Y			10	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
cVPN3000-IPSec-Banner1	Y	Y	Y	11	文字列	シングル	バナー文字列
cVPN3000-IPSec-Allow-Passwd-Store	Y	Y	Y	12	ブーリアン	シングル	0 = ディセーブル 1 = イネーブル
cVPN3000-Use-Client-Address	Y			13	ブーリアン	シングル	0 = ディセーブル 1 = イネーブル
cVPN3000-PPTP-Encryption	Y			14	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 例 : 15 = 40/128 ビットで暗号化 / ステートレスが必要
cVPN3000-L2TP-Encryption	Y			15	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
cVPN3000-IPSec-Split-Tunnel-List	Y	Y	Y	16	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。
cVPN3000-IPSec-Default-Domain	Y	Y	Y	17	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）。

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 Cisco スキーマのアトリビュート （続き）

アトリビュート名 / OID（オブジェクト ID）	VPN 3000	ASA	PIX	アトリビュート OID[1]	構文 / タイプ	シングルまたはマルチ値	有効な値
cVPN3000-IPSec-Split-DNS-Name	Y	Y	Y	18	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）。
cVPN3000-IPSec-Tunnel-Type	Y	Y	Y	19	整数	シングル	1 = LAN-to-LAN 2 = リモート アクセス
cVPN3000-IPSec-Mode-Config	Y	Y	Y	20	ブーリアン	シングル	0 = ディセーブル 1 = イネーブル
cVPN3000-IPSec-User-Group-Lock	Y			21	ブーリアン	シングル	0 = ディセーブル 1 = イネーブル
cVPN3000-IPSec-Over-UDP	Y	Y	Y	22	ブーリアン	シングル	0 = ディセーブル 1 = イネーブル
cVPN3000-IPSec-Over-UDP-Port	Y	Y	Y	23	整数	シングル	4001 ～ 49151、デフォルトは 10000
cVPN3000-IPSec-Banner2	Y	Y	Y	24	文字列	シングル	バナー文字列
cVPN3000-PPTP-MPPC-Compression	Y			25	整数	シングル	0 = ディセーブル 1 = イネーブル
cVPN3000-L2TP-MPPC-Compression	Y			26	整数	シングル	0 = ディセーブル 1 = イネーブル
cVPN3000-IPSec-IP-Compression	Y	Y	Y	27	整数	シングル	0 = ディセーブル 1 = イネーブル
cVPN3000-IPSec-IKE-Peer-ID-Check	Y	Y	Y	28	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
cVPN3000-IKE-Keep-Alives	Y	Y	Y	29	ブーリアン	シングル	0 = ディセーブル 1 = イネーブル
cVPN3000-IPSec-Auth-On-Rekey	Y	Y	Y	30	ブーリアン	シングル	0 = ディセーブル 1 = イネーブル
cVPN3000-Required-Client-Firewall-Vendor-Code	Y	Y	Y	31	整数	シングル	1 = シスコシステムズ（Cisco Integrated Client を使用） 2 = Zone Labs 3 = NetworkICE 4 = Sygate 5 = シスコシステムズ（Cisco Intrusion Prevention Security Agent を使用）

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 Cisco スキーマのアトリビュート （続き）

アトリビュート名 / OID（オブジェクト ID）	VPN 3000	ASA	PIX	アトリビュート OID[1]	構文 / タイプ	シングルまたはマルチ値	有効な値
cVPN3000-Required-Client-Firewall-Product-Code	Y	Y	Y	32	整数	シングル	シスコシステムズ製品： 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
cVPN3000-Required-Client-Firewall-Description	Y	Y	Y	33	文字列	シングル	文字列
cVPN3000-Require-Individual-User-Auth	Y	Y	Y	34	整数	シングル	0 = ディセーブル 1 = イネーブル
cVPN3000-Require-HW-Client-Auth	Y	Y	Y	35	ブーリアン	シングル	0 = ディセーブル 1 = イネーブル
cVPN3000-Authenticated-User-Idle-Timeout	Y	Y	Y	36	整数	シングル	1 ～ 35791394 分
cVPN3000-Cisco-IP-Phone-Bypass	Y	Y	Y	37	整数	シングル	0 = ディセーブル 1 = イネーブル
cVPN3000-IPSec-Split-Tunneling-Policy	Y	Y	Y	38	整数	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
cVPN3000-IPSec-Required-Client-Firewall-Capability	Y	Y	Y	39	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
cVPN3000-IPSec-Client-Firewall-Filter-Name	Y			40	文字列	シングル	クライアントにファイア ウォール ポリシーとしてプッシュするフィルタの名前を指定します。

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 Cisco スキーマのアトリビュート （続き）

アトリビュート名 / OID（オブジェクト ID）	VPN 3000	ASA	PIX	アトリビュート OID[1]	構文 / タイプ	シングルまたはマルチ値	有効な値
cVPN3000-IPSec-Client-Firewall-Filter-Optional	Y	Y	Y	41	整数	シングル	0 = 必須 1 = オプション
cVPN3000-IPSec-Backup-Servers	Y	Y	Y	42	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クリアする 3 = バックアップ サーバ リストを使用する
cVPN3000-IPSec-Backup-Server-List	Y	Y	Y	43	文字列	シングル	サーバ アドレス（スペース区切り）
cVPN3000-Client-Intercept-DHCP-Configure-Msg	Y	Y	Y	44	ブーリアン	シングル	0 = ディセーブル 1 = イネーブル
cVPN3000-MS-Client-Subnet-Mask	Y	Y	Y	45	文字列	シングル	IP アドレス
cVPN3000-Allow-Network-Extension-Mode	Y	Y	Y	46	ブーリアン	シングル	0 = ディセーブル 1 = イネーブル
cVPN3000-Strip-Realm	Y	Y	Y	47	ブーリアン	シングル	0 = ディセーブル 1 = イネーブル
cVPN3000-Cisco-AV-Pair	Y	Y	Y	48	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 アトリビュート構文」を参照してください。
cVPN3000-User-Auth-Server-Name	Y			49	文字列	シングル	IP アドレスまたはホスト名
cVPN3000-User-Auth-Server-Port	Y			50	整数	シングル	サーバ プロトコルのポート番号
cVPN3000-User-Auth-Server-Secret	Y			51	文字列	シングル	サーバのパスワード
cVPN3000-Confidence-Interval	Y	Y	Y	52	整数	シングル	10 ～ 300 秒
cVPN3000-Cisco-LEAP-Bypass	Y	Y	Y	53	整数	シングル	0 = ディセーブル 1 = イネーブル
cVPN3000-DHCP-Network-Scope	Y	Y	Y	54	文字列	シングル	IP アドレス
cVPN3000-Client-Type-Version-Limiting	Y	Y	Y	55	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

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 Cisco スキーマのアトリビュート （続き）

アトリビュート名 / OID（オブジェクト ID）	VPN 3000	ASA	PIX	アトリビュート OID[1]	構文 / タイプ	シングルまたはマルチ値	有効な値
cVPN3000-WebVPN-Content-Filter-Parameters	Y	Y		56	整数	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)
cVPN3000-WebVPN-Enable-functions				57	整数	シングル	使用しない（廃止）
cVPN3000-WebVPN-Exchange-Server-Address				58	文字列	シングル	使用しない（廃止）
cVPN3000-WebVPN-Exchange-Server-NETBIOS-Name				59	文字列	シングル	使用しない（廃止）
cVPN3000-Port-Forwarding-Name	Y	Y		60	文字列	シングル	名前の文字列（「Corporate-Apps」など）
cVPN3000-IETF-Radius-Framed-IP-Address	Y	Y	Y	61	文字列	シングル	IP アドレス
cVPN3000-IETF-Radius-Framed-IP-Netmask	Y	Y	Y	62	文字列	シングル	IP アドレス
cVPN3000-IETF-Radius-Session-Timeout	Y	Y	Y	63	整数	シングル	1 ～ 35791394 分 0 = 無制限
cVPN3000-IETF-Radius-Idle-Timeout	Y	Y	Y	64	整数	シングル	1 ～ 35791394 分 0 = 無制限
cVPN3000-IETF-Radius-Class	Y	Y	Y	65	文字列	シングル	グループ名を示す文字列。次の 3 つの形式のいずれかを使用します。 OU=Engineering OU=Engineering; Engineering
cVPN3000-IETF-Radius-Filter-Id	Y	Y	Y	66	文字列	シングル	アクセスリスト
cVPN3000-Authorization-Required	Y			67	整数	シングル	0 = No 1 = Yes
cVPN3000-Authorization-Type	Y			68	整数	シングル	0 = なし 1 = RADIUS 2 = LDAP

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 Cisco スキーマのアトリビュート （続き）

アトリビュート名 / OID（オブジェクト ID）	VPN 3000	ASA	PIX	アトリビュート OID[1]	構文 / タイプ	シングルまたはマルチ値	有効な値
cVPN3000-DN-Field	Y	Y	Y	69	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
cVPN3000-WebVPN-URL-List		Y		70	文字列	シングル	URL リスト名
cVPN3000-WebVPN-Forwarded-Ports		Y		71	文字列	シングル	ポート転送リスト名
cVPN3000-WebVPN-ACL-Filters		Y		72	文字列	シングル	アクセスリスト名
cVPN3000-WebVPN-Homepage	Y	Y		73	文字列	シングル	URL（http://example-portal.com など）
cVPN3000-WebVPN-Single-Sign-On-Server-Name		Y		74	文字列	シングル	SSO サーバの名前（1 ～ 31 文字）
cVPN3000-WebVPN-URL-Entry-Enable	Y	Y		75	整数	シングル	0 = ディセーブル 1 = イネーブル
cVPN3000-WebVPN-File-Access-Enable	Y	Y		76	整数	シングル	0 = ディセーブル 1 = イネーブル
cVPN3000-WebVPN-File-Server-Entry-Enable	Y	Y		77	整数	シングル	0 = ディセーブル 1 = イネーブル
cVPN3000-WebVPN-File-Server-Browsing-Enable	Y	Y		78	整数	シングル	0 = ディセーブル 1 = イネーブル
cVPN3000-WebVPN-Port-Forwarding-Enable	Y	Y		79	整数	シングル	0 = ディセーブル 1 = イネーブル
cVPN3000-WebVPN-Port-Forwarding-Exchange-Proxy-Enable	Y	Y		80	整数	シングル	0 = ディセーブル 1 = イネーブル
cVPN3000-WebVPN-Port-Forwarding-HTTP-Proxy-Enable	Y	Y		81	整数	シングル	0 = ディセーブル 1 = イネーブル
cVPN3000-WebVPN-Port-Forwarding-Auto-Download-Enable	Y	Y		82	整数	シングル	0 = ディセーブル 1 = イネーブル
cVPN3000-WebVPN-Citrix-Support-Enable	Y	Y		83	整数	シングル	0 = ディセーブル 1 = イネーブル
cVPN3000-WebVPN-Apply-ACL-Enable	Y	Y		84	整数	シングル	0 = ディセーブル 1 = イネーブル
cVPN3000-WebVPN-SVC-Enable	Y	Y		85	整数	シングル	0 = ディセーブル 1 = イネーブル
cVPN3000-WebVPN-SVC-Required-Enable	Y	Y		86	整数	シングル	0 = ディセーブル 1 = イネーブル
cVPN3000-WebVPN-SVC-Keep-Enable	Y	Y		87	整数	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 Cisco スキーマのアトリビュート （続き）

アトリビュート名 / OID（オブジェクト ID）	VPN 3000	ASA	PIX	アトリビュート OID[1]	構文 / タイプ	シングルまたはマルチ値	有効な値
cVPN3000-IE-Proxy-Server	Y			88	文字列	シングル	IP アドレス
cVPN3000-IE-Proxy-Method	Y			89	整数	シングル	1 = 変更なし 2 = プロキシなし 3 = 自動検出 4 = その他
cVPN3000-IE-Proxy-Exception-List	Y			90	文字列	シングル	改行（\n）区切りの DNS ドメインのリスト
cVPN3000-IE-Proxy-Bypass-Local	Y			91	整数	シングル	0 = なし 1 = ローカル
cVPN3000-Tunnel-Group-Lock		Y	Y	92	文字列	シングル	トンネル グループの名前または「none」
cVPN3000-Firewall-ACL-In		Y	Y	93	文字列	シングル	アクセスリスト ID
cVPN3000-Firewall-ACL-Out		Y	Y	94	文字列	シングル	アクセスリスト ID
cVPN3000-PFS-Required	Y	Y	Y	95	ブーリアン	シングル	0 = No 1 = Yes
cVPN3000-WebVPN-SVC-Keepalive	Y	Y		96	整数	シングル	0 = ディセーブル n = キープアライブ値（15 ～ 600 秒）
cVPN3000-WebVPN-SVC-Client-DPD	Y	Y		97	整数	シングル	0 = ディセーブル n = デッド ピア検出値（30 ～ 3600 秒）
cVPN3000-WebVPN-SVC-Gateway-DPD	Y	Y		98	整数	シングル	0 = ディセーブル n = デッド ピア検出値（30 ～ 3600 秒）
cVPN3000-WebVPN-SVC-Rekey-Period	Y	Y		99	整数	シングル	0 = ディセーブル n = 分単位の再試行間隔 (4 - 10080)
cVPN3000-WebVPN-SVC-Rekey-Method	Y	Y		100	整数	シングル	0 = なし 1 = SSL 2 = 新規トンネル 3 = 任意（SSL に設定）
cVPN3000-WebVPN-SVC-Compression	Y	Y		101	整数	シングル	0 = なし 1 = デフレート圧縮

1. 各アトリビュートの完全なオブジェクト ID を取得するには、このカラム内の番号を 1.2.840.113556.8000.795.2. の末尾に追加してください。つまり、表内の最初のアトリビュートである cVPN3000-Access-Hours の OID は 1.2.840.113556.8000.795.2.1 になります。同様に、テーブル内にある最後のアトリビュート cVPN3000-WebVPN-SVC-Compression の OID は 1.2.840.113556.8000.795.2.115 になります。

Cisco-AV-Pair アトリビュート構文

各 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 で構文ルールについて説明します。

表 B-3　AV ペア アトリビュート構文ルール

フィールド	説明
Prefix	AV ペアの一意の識別子。たとえば、`ip:inacl#1=`（標準 ACL に使用）または `webvpn:inacl#`（WebVPN ACL に使用）などです。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	ルールが一致した場合に実行するアクション：deny または permit。
Protocol	IP プロトコルの番号または名前。0 ～ 255 の整数値か、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 アドレスで指定する場合、続けて 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 アドレスで指定する場合、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）。

次の例を参考にしてください。

```
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 クライアント（SVC）トンネルに ACL 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。

WebVPN クライアントレス（ブラウザモード）トンネルに ACL 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 アトリビュートのトークン一覧を示します。

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	構文フィールド	説明
ip:inacl#*Num*=	該当なし（識別子）	(*Num* は一意の整数)。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 トンネルおよび SSL VPN（SVC）トンネルに ACL を適用します。
webvpn:inacl#*Num*=	該当なし（識別子）	(*Num* は一意の整数)。WebVPN 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。WebVPN クライアントレス（ブラウザモード）トンネルに ACL 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	Protocol	Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）。
1	Protocol	Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）。
IP	Protocol	Internet Protocol（IP; インターネット プロトコル）。
0	Protocol	Internet Protocol（IP; インターネット プロトコル）。
TCP	Protocol	Transmission Control Protocol（TCP; 伝送制御プロトコル）。
6	Protocol	Transmission Control Protocol（TCP; 伝送制御プロトコル）。
UDP	Protocol	User Datagram Protocol（UDP; ユーザ データグラム プロトコル）。
17	Protocol	User Datagram Protocol（UDP; ユーザ データグラム プロトコル）。
any	Hostname	すべてのホストにルールを適用します。
host	Hostname	ホスト名を示す任意の英数字文字列。
log	Log	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	Operator	値より小さい。
gt	Operator	値より大きい。
eq	Operator	値と等しい。
neq	Operator	値と等しくない。
range	Operator	この範囲に含まれる。range の後に 2 つの値を続けます。

セキュリティ アプライアンスの認可スキーマの例

この項では、LDAP スキーマのサンプルを示します。このスキーマはセキュリティ アプライアンスのクラスとアトリビュートをサポートしています。このスキーマは、Microsoft Active Directory LDAP サーバにだけ使用します。LDAP サーバのスキーマを定義するためのモデルとして、表 B-2 と合せて使用してください。

Schema 3k_schema.ldif

```
dn:
CN=cVPN3000-Access-Hours,CN=Schema,CN=Configuration,OU=People,DC=ExampleCorporation,DC
=com
changetype: add
adminDisplayName: cVPN3000-Access-Hours
attributeID: 1.2.840.113556.1.8000.795.2.1
attributeSyntax: 2.5.5.3
cn: cVPN3000-Access-Hours
instanceType: 4
isSingleValued: TRUE
lDAPDisplayName: cVPN3000-Access-Hours
distinguishedName:

CN=cVPN3000-Access-Hours,CN=Schema,CN=Configuration,OU=People,DC=ExampleCorporation,DC
=com
objectCategory:
 CN=Attribute-Schema,CN=Schema,CN=Configuration,OU=People,DC=ExampleCorporation,DC=com
objectClass: attributeSchema
oMSyntax: 27
name: cVPN3000-Access-Hours
showInAdvancedViewOnly: TRUE

.....
.... (define subsequent security appliance authorization attributes here)
....


dn:
CN=cVPN3000-Primary-DNS,CN=Schema,CN=Configuration,OU=People,DC=ExampleCorporation,DC=
com
changetype: add
adminDisplayName: cVPN3000-Primary-DNS
attributeID: 1.2.840.113556.1.8000.795.2.3
attributeSyntax: 2.5.5.3
cn: cVPN3000-Primary-DNS
instanceType: 4
isSingleValued: TRUE
lDAPDisplayName: cVPN3000-Primary-DNS
distinguishedName:

CN=cVPN3000-Primary-DNS,CN=Schema,CN=Configuration,OU=People,DC=ExampleCorporation,DC=
com
objectCategory:
 CN=Attribute-Schema,CN=Schema,CN=Configuration,OU=People,DC=ExampleCorporation,DC=com
objectClass: attributeSchema
oMSyntax: 27
name: cVPN3000-Primary-DNS
showInAdvancedViewOnly: TRUE

.....
.... (define subsequent security appliance authorization attributes here)
....

dn:
CN=cVPN3000-Confidence-Interval,CN=Schema,CN=Configuration,OU=People,DC=ExampleCorpora
tion,DC=com
changetype: add
adminDisplayName: cVPN3000-Confidence-Interval
attributeID: 1.2.840.113556.1.8000.795.2.52
attributeSyntax: 2.5.5.9
cn: cVPN3000-Confidence-Interval
instanceType: 4
isSingleValued: TRUE
lDAPDisplayName: cVPN3000-Confidence-Interval
distinguishedName:

CN=cVPN3000-Confidence-Interval,CN=Schema,CN=Configuration,OU=People,DC=ExampleCorpora
```

```
tion,DC=com
objectCategory:

DN:
changetype: modify
add: schemaUpdateNow
schemaUpdateNow: 1
-

dn:
CN=cVPN3000-User-Authorization,CN=Schema,CN=Configuration,OU=People,DC=ExampleCorporat
ion,DC=com
changetype: add
adminDisplayName: cVPN3000-User-Authorization
adminDescription: Cisco Class Schema
cn: cVPN3000-User-Authorization
defaultObjectCategory:

CN=cVPN3000-User-Authorization,CN=Schema,CN=Configuration,OU=People,DC=ExampleCorporat
ion,DC=com
defaultSecurityDescriptor:
 D:(A;;RPWPCRCCDCLCLOLORCWOWDSDDTDTSW;;;DA)(A;;RPWPCRCCDCLCLORCWOWDSDDTSW;;;SY)
 (A;;RPLCLORC;;;AU)
governsID: 1.2.840.113556.1.8000.795.1.1
instanceType: 4
lDAPDisplayName: cVPN3000-User-Authorization

mustContain: cn
mayContain: cVPN3000-Access-Hours
mayContain: cVPN3000-Simultaneous-Logins
mayContain: cVPN3000-Primary-DNS
...
mayContain: cVPN3000-Confidence-Interval
mayContain: cVPN3000-Cisco-LEAP-Bypass

distinguishedName:

CN=cVPN3000-User-Authorization,CN=Schema,CN=Configuration,OU=People,DC=ExampleCorporat
ion,DC=com
objectCategory:
 CN=Class-Schema,CN=Schema,CN=Configuration,OU=People,DC=ExampleCorporation,DC=com
objectClass: classSchema
objectClassCategory: 1
possSuperiors: organizationalUnit
name: cVPN3000-User-Authorization
rDNAttID: cn
showInAdvancedViewOnly: TRUE
subClassOf: top
systemOnly: FALSE

DN:
changetype: modify
add: schemaUpdateNow
schemaUpdateNow: 1
-
systemOnly: FALSE

DN:
changetype: modify
add: schemaUpdateNow
schemaUpdateNow: 1
-
```

LDAP サーバへのスキーマのロード

（注）　この項の説明は、Microsoft Active Directory LDAP サーバだけを対象としています。他のタイプのサーバを使用する場合、スキーマをロードする方法については、サーバのマニュアルを参照してください。

LDAP サーバにスキーマをロードするには、スキーマ ファイルが存在するディレクトリから次のコマンドを入力します。

```
ldifde -i -f Schema Name
```

次の例を参考にしてください。

```
ldifde -i -f 3k_schema.ldif
```

ユーザ権限の定義

（注）　この項の説明は、Microsoft Active Directory LDAP サーバだけを対象としています。他のタイプのサーバを使用する場合、ユーザ アトリビュートの定義とロードの詳細については、サーバのマニュアルを参照してください。

LDAP サーバで認可するユーザごとに、ユーザ ファイルを 1 つ定義します。ユーザ ファイルには、特定のユーザに関連付けられたセキュリティ アプライアンスのアトリビュートと値をすべて定義します。各ユーザは、クラス cVPN3000-User-Authorization のオブジェクトです。ユーザ ファイルを定義するには、テキスト エディタを使用します。ファイルの拡張子は .ldif にします（ユーザ ファイルの例については、「Robin.ldif」を参照）。

LDAP サーバにユーザ ファイルをロードするには、作成した *ldap_user*.ldif ファイルが存在するディレクトリから、コマンド ldifde -i -f ldap_user.ldif を入力します。例：ldifde -i -f Robin.ldif

スキーマとユーザ ファイルの両方を作成してロードしたら、LDAP サーバはセキュリティ アプライアンスの認可要求を処理できる状態になります。

ユーザ ファイルの例

この項では、ユーザ Robin のユーザ ファイルのサンプルを示します。

Robin.ldif

```
dn: cn=Robin,OU=People,DC=ExampleCorporation,DC=com
changetype: add
cn: Robin
CVPN3000-Access-Hours: Corporate_time
cVPN3000-Simultaneous-Logins: 2
cVPN3000-IPSec-Over-UDP: TRUE
CVPN3000-IPSec-Over-UDP-Port: 12125
cVPN3000-IPSec-Banner1: Welcome to the Example Corporation!!!
cVPN3000-IPSec-Banner2: Unauthorized access is prohibited!!!!!
cVPN3000-Primary-DNS: 10.10.4.5
CVPN3000-Secondary-DNS: 10.11.12.7
CVPN3000-Primary-WINS: 10.20.1.44
CVPN3000-SEP-Card-Assignment: 1
CVPN3000-IPSec-Tunnel-Type: 2
CVPN3000-Tunneling-Protocols: 7
cVPN3000-Confidence-Interval: 300
cVPN3000-IPSec-Allow-Passwd-Store: TRUE
objectClass: cVPN3000-User-Authorization
```

外部 RADIUS サーバの設定

この項では、RADIUS 設定手順の概要を説明し、Cisco RADIUS アトリビュートを定義します。次の項目を取り上げます。

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 ユーザの認証と認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。RADIUS サーバとセキュリティ アプライアンスの相互運用をセットアップするには、次の手順に従います。

ステップ 1　セキュリティ アプライアンスのアトリビュートを RADIUS サーバにロードします。アトリビュートをロードする方法は、使用する RADIUS サーバのタイプによって異なります。

- CiscoACS を使用する場合、サーバにはすでにこれらのアトリビュートが統合されています。この手順は省略できます。
- FUNK RADIUS サーバを使用する場合、シスコではセキュリティ アプライアンスのすべてのアトリビュートを含むディクショナリ 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 Software Center 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）の場合、セキュリティ アプライアンスの各アトリビュートを手動で定義する必要があります。アトリビュートを定義するには、アトリビュート名または番号、タイプ、値、およびベンダー コード（3076）を使用します。セキュリティ アプライアンスの RADIUS 認可アトリビュートと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　ユーザまたはグループに、IPSec/WebVPN　トンネルの確立時に送信する権限とアトリビュートをセットアップします。権限またはアトリビュートに、アクセス時間、プライマリ DNS、バナーなどが含まれる場合があります。

セキュリティ アプライアンスの RADIUS 認可アトリビュート

（注）　認可とは、権限またはアトリビュートを適用するプロセスのことです。認証サーバとして定義されている RADIUS サーバは、権限またはアトリビュートが設定されていれば、それを適用します。

表 B-5 に、セキュリティ アプライアンスがサポートする、ユーザ認可に使用できる有効なアトリビュートの一覧を示します。

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 アトリビュートと値

アトリビュート名	VPN 3000	ASA	PIX	アトリビュート #	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	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	シングル	使用しない
Tunneling-Protocols	Y	Y	Y	11	整数	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	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
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	ブーリアン	シングル	0 = ディセーブル 1 = イネーブル
Use-Client-Address	Y			17	ブーリアン	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 アトリビュートと値 （続き）

アトリビュート名	VPN 3000	ASA	PIX	アトリビュート #	構文 / タイプ	シングルまたはマルチ値	説明または値
PPTP-Encryption	Y			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
L2TP-Encryption	Y			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
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	シングル	1 = LAN-to-LAN 2 = リモート アクセス
IPSec-Mode-Config	Y	Y	Y	31	ブーリアン	シングル	0 = ディセーブル 1 = イネーブル
IPSec-User-Group-Lock	Y			33	ブーリアン	シングル	0 = ディセーブル 1 = イネーブル
IPSec-Over-UDP	Y	Y	Y	34	ブーリアン	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	シングル	4001 ～ 49151、デフォルトは 10000
Banner2	Y	Y	Y	36	文字列	シングル	バナー文字列。Banner2 文字列は Banner1 文字列に結合されます（設定されている場合）。

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 アトリビュートと値 （続き）

アトリビュート名	VPN 3000	ASA	PIX	アトリビュート #	構文 / タイプ	シングルまたはマルチ値	説明または値
PPTP-MPPC-Compression	Y			37	整数	シングル	0 = ディセーブル 1 = イネーブル
L2TP-MPPC-Compression	Y			38	整数	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	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	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	ブーリアン	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	ブーリアン	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	シングル	1 = シスコシステムズ（Cisco Integrated Client を使用） 2 = Zone Labs 3 = NetworkICE 4 = Sygate 5 = シスコシステムズ（Cisco Intrusion Prevention Security Agent を使用）
Required-Client-Firewall-Product-Code	Y	Y	Y	46	整数	シングル	シスコシステムズ製品： 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

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 アトリビュートと値 （続き）

アトリビュート名	VPN 3000	ASA	PIX	アトリビュート #	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-Description	Y	Y	Y	47	文字列	シングル	文字列
Require-HW-Client-Auth	Y	Y	Y	48	ブーリアン	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	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	シングル	1 ～ 35791394 分
Cisco-IP-Phone-Bypass	Y	Y	Y	51	整数	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	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	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-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 ポリシーとしてプッシュ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	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クリアする 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	ブーリアン	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	ブーリアン	シングル	IP アドレス

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 アトリビュートと値 （続き）

アトリビュート名	VPN 3000	ASA	PIX	アトリビュート #	構文 / タイプ	シングルまたはマルチ値	説明または値
Allow-Network-Extension-Mode	Y	Y	Y	64	ブーリアン	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	シングル	0 = なし 1 = RADIUS 2 = LDAP
Authorization-Required	Y			66	整数	シングル	0 = No 1 = Yes
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	シングル	10 ～ 300 秒
WebVPN-Content-Filter-Parameters	Y	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-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	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	名前を示す文字列（「Corporate-Apps」など）。 このテキストで WebVPN 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	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

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 アトリビュートと値 （続き）

アトリビュート名	VPN 3000	ASA	PIX	アトリビュート #	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	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	シングル	0 = なし 1 = ローカル
IKE-Keepalive-Retry-Interval	Y	Y	Y	84	整数	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
Perfect-Forward-Secrecy-Enable	Y	Y	Y	88	ブーリアン	シングル	0 = No 1 = Yes
NAC-Enable	Y			89	整数		0 = No 1 = Yes
NAC-Status-Query-Timer	Y			90	整数		30 ～ 1800 秒
NAC-Revalidation-Timer	Y			91	整数		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	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	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	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	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	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	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	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	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	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	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 アトリビュートと値 （続き）

アトリビュート名	VPN 3000	ASA	PIX	アトリビュート #	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-Enable	Y	Y		103	整数	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	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	シングル	0 = ディセーブル 1 = イネーブル
Strip-Realm	Y	Y	Y	135	ブーリアン	シングル	0 = ディセーブル 1 = イネーブル

（注）　RADIUS アトリビュート名にはプレフィックス cVPN3000 が追加されていません。これは、3 種類のセキュリティ アプライアンス（VPN 3000、PIX、ASA）すべてがサポートされていることをわかりやすく反映したためです。Cisco Secure ACS 4.x ではこの新しい命名基準がサポートされていますが、バージョン 4.0 より前にリリースされた ACS ではまだプレフィックス cVPN3000 が付いています。アプライアンスは、アトリビュートの名前ではなく数値 ID に基づいて RADIUS アトリビュートを適用します。LDAP アトリビュートは、ID ではなく名前で適用されます。

外部 RADIUS サーバの設定

この項では、RADIUS 設定手順の概要を説明し、Cisco RADIUS アトリビュートと TACACS+ アトリビュートを定義します。次の項目を取り上げます。

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 ユーザの認証と認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。RADIUS サーバとセキュリティ アプライアンスの相互運用をセットアップするには、次の手順に従います。

ステップ 1　セキュリティ アプライアンスのアトリビュートを RADIUS サーバにロードします。アトリビュートをロードする方法は、使用する RADIUS サーバのタイプによって異なります。

- CiscoACS を使用する場合、サーバにはすでにこれらのアトリビュートが統合されています。この手順は省略できます。
- FUNK RADIUS サーバを使用する場合、シスコではセキュリティ アプライアンスのすべてのアトリビュートを含むディクショナリ 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 Software Center 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）の場合、セキュリティ アプライアンスの各アトリビュートを手動で定義する必要があります。アトリビュートを定義するには、アトリビュート名または番号、タイプ、値、およびベンダー コード（3076）を使用します。セキュリティ アプライアンスの RADIUS 認可アトリビュートと値のリストについては、表 B-6 を参照してください。

ステップ 2　ユーザまたはグループに、IPSec/WebVPN　トンネルの確立時に送信する権限とアトリビュートをセットアップします。

セキュリティ アプライアンスの RADIUS 認可アトリビュート

（注）　認可とは、権限またはアトリビュートを適用するプロセスのことです。認証サーバとして定義されている RADIUS サーバは、権限またはアトリビュートが設定されていれば、それを適用します。

表 B-6 に、セキュリティ アプライアンスがサポートする、ユーザ認可に使用できる有効な RADIUS アトリビュートの一覧を示します。

表 B-6　セキュリティ アプライアンスでサポートされる RADIUS アトリビュートと値

アトリビュート名	VPN 3000	ASA	PIX	アトリビュート #	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	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	シングル	使用しない
Tunneling-Protocols	Y	Y	Y	11	整数	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	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
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	ブーリアン	シングル	0 = ディセーブル 1 = イネーブル
Use-Client-Address	Y			17	ブーリアン	シングル	0 = ディセーブル 1 = イネーブル

表 B-6　セキュリティ アプライアンスでサポートされる RADIUS アトリビュートと値（続き）

アトリビュート名	VPN 3000	ASA	PIX	アトリビュート #	構文 / タイプ	シングルまたはマルチ値	説明または値
PPTP-Encryption	Y			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
L2TP-Encryption	Y			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
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	シングル	1 = LAN-to-LAN 2 = リモート アクセス
IPSec-Mode-Config	Y	Y	Y	31	ブーリアン	シングル	0 = ディセーブル 1 = イネーブル
IPSec-User-Group-Lock	Y			33	ブーリアン	シングル	0 = ディセーブル 1 = イネーブル
IPSec-Over-UDP	Y	Y	Y	34	ブーリアン	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	シングル	4001 ～ 49151、デフォルトは 10000
Banner2	Y	Y	Y	36	文字列	シングル	バナー文字列。Banner2 文字列は Banner1 文字列に結合されます（設定されている場合）。

表 B-6　セキュリティ アプライアンスでサポートされる RADIUS アトリビュートと値（続き）

アトリビュート名	VPN 3000	ASA	PIX	アトリビュート #	構文 / タイプ	シングルまたはマルチ値	説明または値
PPTP-MPPC-Compression	Y			37	整数	シングル	0 = ディセーブル 1 = イネーブル
L2TP-MPPC-Compression	Y			38	整数	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	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	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	ブーリアン	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	ブーリアン	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	シングル	1 = シスコシステムズ（Cisco Integrated Client を使用） 2 = Zone Labs 3 = NetworkICE 4 = Sygate 5 = シスコシステムズ（Cisco Intrusion Prevention Security Agent を使用）
Required-Client-Firewall-Product-Code	Y	Y	Y	46	整数	シングル	シスコシステムズ製品： 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

表 B-6　セキュリティ アプライアンスでサポートされる RADIUS アトリビュートと値（続き）

アトリビュート名	VPN 3000	ASA	PIX	アトリビュート #	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-Description	Y	Y	Y	47	文字列	シングル	文字列
Require-HW-Client-Auth	Y	Y	Y	48	ブーリアン	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	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	シングル	1 ～ 35791394 分
Cisco-IP-Phone-Bypass	Y	Y	Y	51	整数	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	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	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-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 ポリシーとしてプッシュ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	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クリアする 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	ブーリアン	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	ブーリアン	シングル	IP アドレス

表 B-6　セキュリティ アプライアンスでサポートされる RADIUS アトリビュートと値（続き）

アトリビュート名	VPN 3000	ASA	PIX	アトリビュート #	構文 / タイプ	シングルまたはマルチ値	説明または値
Allow-Network-Extension-Mode	Y	Y	Y	64	ブーリアン	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	シングル	0 = なし 1 = RADIUS 2 = LDAP
Authorization-Required	Y			66	整数	シングル	0 = No 1 = Yes
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	シングル	10 ～ 300 秒
WebVPN-Content-Filter-Parameters	Y	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-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	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	名前を示す文字列（「Corporate-Apps」など）。 このテキストで WebVPN 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	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

表 B-6　セキュリティ アプライアンスでサポートされる RADIUS アトリビュートと値（続き）

アトリビュート名	VPN 3000	ASA	PIX	アトリビュート #	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	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	シングル	0 = なし 1 = ローカル
IKE-Keepalive-Retry-Interval	Y	Y	Y	84	整数	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
Perfect-Forward-Secrecy-Enable	Y	Y	Y	88	ブーリアン	シングル	0 = No 1 = Yes
NAC-Enable	Y			89	整数		0 = No 1 = Yes
NAC-Status-Query-Timer	Y			90	整数		30 ～ 1800 秒
NAC-Revalidation-Timer	Y			91	整数		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	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	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	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	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	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	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	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	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	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	シングル	0 = ディセーブル 1 = イネーブル

表 B-6　セキュリティ アプライアンスでサポートされる RADIUS アトリビュートと値（続き）

アトリビュート名	VPN 3000	ASA	PIX	アトリビュート #	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-Enable	Y	Y		103	整数	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	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	シングル	0 = ディセーブル 1 = イネーブル
Strip-Realm	Y	Y	Y	135	ブーリアン	シングル	0 = ディセーブル 1 = イネーブル

（注）　RADIUS アトリビュート名にはプレフィックス cVPN3000 が追加されていません。これは、3 種類のセキュリティ アプライアンス（VPN 3000、PIX、ASA）すべてがサポートされていることをわかりやすく反映したためです。Cisco Secure ACS 4.x ではこの新しい命名基準がサポートされていますが、バージョン 4.0 より前にリリースされた ACS ではまだプレフィックス cVPN3000 が付いています。アプライアンスは、アトリビュートの名前ではなく数値 ID に基づいて RADIUS アトリビュートを適用します。LDAP アトリビュートは、ID ではなく名前で適用されます。

セキュリティ アプライアンスの TACACS+ アトリビュート

セキュリティ アプライアンスは、TACACS+ アトリビュートをサポートします。TACACS+ によって、認証、認可、アカウンティングの機能が分離されます。このプロトコルでは、2 つのタイプのアトリビュート（必須とオプション）をサポートします。必須アトリビュートは、サーバとクライアントの両方で認識でき、ユーザに適用する必要があります。オプション アトリビュートの認識や使用は必須ではありません。

（注）　TACACS+ アトリビュートを使用するには、NAS 上で AAA サービスがイネーブルになっていることを確認します。

表 B-7 には、カットスルー プロキシ接続でサポートされる TACACS+ 認可応答アトリビュートの一覧を示します。表 B-8 には、サポートされる TACACS+ アカウンティング アトリビュートの一覧を示します。

表 B-7　サポートされる TACACS+ 認可応答アトリビュート

アトリビュート	説明
acl	接続に適用する、ローカルに設定されたアクセスリストを指定します。
idletime	許容される非アクティブ時間を分単位で指定します。ここに指定した時間の非アクティブ状態が経過すると、認証されたユーザ セッションは終了します。
timeout	認証クレデンシャルがアクティブである絶対時間を分単位で指定します。ここに指定した時間が経過すると、認証されたユーザセッションは終了します。

表 B-8　サポートされる TACACS+ アカウンティング アトリビュート

アトリビュート	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（Stop 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（Stop レコードのみ）。
cmd	実行され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	切断の理由を示す数値コードを指定します（Stop レコードのみ）。
elapsed_time	接続の経過時間を秒単位で定義します（Stop 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。カットスルー プロキシ接続の場合は、最もセキュリティの低いインターフェイス上のアドレスを定義します。
local_ip	トンネル接続でクライアントが接続する IP アドレスを指定します。カットスルー プロキシ接続の場合は、最もセキュリティの高いインターフェイス上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の場合はユーザの特権レベルに、それ以外の場合は 1 に設定します。
rem_iddr	クライアントの IP アドレスを指定します。
service	使用するサービスを指定します。コマンド アカウンティングの場合のみ、常に「shell」に設定します。
task_id	アカウンティング トランザクションの一意のタスク ID を指定します。
username	ユーザの名前を示します。