CHAPTER 18

管理アクセス用の AAA の設定

この章では、管理アクセスのためにユーザを認証および認可する方法について説明します。この章は、次の項目を取り上げます。

（注） Telnet、SSH、または ASDM アクセスの場合、最初に第 17 章「管理アクセスの設定」の手順を実行します。

管理アクセス用の AAA に関する情報

AAA によって、ASA 1000V が、ユーザが誰か（認証）、ユーザが何を実行できるか（認可）、およびユーザが何を実行したか（アカウンティング）を判別することが可能になります。

認証だけで使用することも、認可およびアカウンティングとともに使用することもできます。認可では必ず、ユーザの認証が最初に済んでいる必要があります。アカウンティングだけで使用することも、認証および認可とともに使用することもできます。

この項は、次の内容で構成されています。

認証について

認証では、有効なユーザ クレデンシャルを要求してアクセスを制御します。このクレデンシャルは通常、ユーザ名とパスワードです。次の項目を認証するように、ASA 1000V を設定できます。

- ASA 1000V へのすべての管理接続（この接続には、次のセッションが含まれます）
  - Telnet
  - SSH
  - シリアル コンソール
  - ASDM（HTTPS を使用）
- **enable** コマンド

認可に関する情報

ユーザの認証後、認可によってユーザごとにアクセスが制御されます。

認可によって、各認証済みユーザが使用できるサービスおよびコマンドが制御されます。認可をイネーブルにしていない場合は、認証だけで、すべての認証済みユーザがサービスに同じようにアクセスできます。

認可で提供される制御を必要とする場合は、広範な認証ルールを設定してから、詳細な認可を設定できます。

ASA 1000V はユーザあたり最初の 16 件の認可要求をキャッシュするため、ユーザが現在の認証セッション中に同じサービスにアクセスした場合、ASA 1000V は認可サーバに要求を再送信しません。

アカウンティングに関する情報

アカウンティングは、ASA 1000V を通過するトラフィックを追跡して、ユーザ アクティビティを記録できるようにします。トラフィックの認証をイネーブルにすると、ユーザごとにトラフィックをアカウンティングできます。トラフィックを認証しない場合は、IP アドレスごとにトラフィックをアカウンティングできます。ASA 1000V アカウンティング情報には、セッションの開始時刻と終了時刻、ユーザ名、そのセッションでを経由したバイト数、使用されたサービス、各セッションの継続時間が含まれます。

管理認証に関する情報

この項では、管理アクセスの認証について説明します。次の項目を取り上げます。

認証がある場合とない場合の CLI アクセスの比較

ASA 1000V へのログイン方法は、認証をイネーブルにしているかどうかによって異なります。

- Telnet の認証をイネーブルにしていない場合は、ユーザ名を入力しません。ログイン パスワード（**password** コマンドで設定）を入力します。SSH の場合は、ユーザ名とログイン パスワードを入力します。ユーザ EXEC モードにアクセスします。
- この項の説明に従って Telnet または SSH 認証をイネーブルにした場合は、AAA サーバまたはローカル ユーザ データベースで定義されているユーザ名とパスワードを入力します。ユーザ EXEC モードにアクセスします。

ログイン後に特権 EXEC モードに入るには、**enable** コマンドを入力します。**enable** コマンドの動作は、認証がイネーブルかどうかによって異なります。

- enable 認証を設定していない場合は、**enable** コマンドを入力するときにシステム イネーブル パスワード（**enable password** コマンドで設定）を入力します。ただし、enable 認証を使用しない場合、**enable** コマンドを入力した後は、特定のユーザとしてログインしていません。ユーザ名を維持するには、enable 認証を使用してください。
- enable 認証を設定する場合（「特権 EXEC モードにアクセスするための認証の設定（enable コマンド）」（P.18-21）を参照）は、ASA 1000V によってユーザ名とパスワードの入力を求めるプロンプトが再度表示されます。この機能は、ユーザが入力できるコマンドを判別するためにユーザ名が重要な役割を果たすコマンド許可を実行する場合に特に役立ちます。

ローカル データベースを使用する enable 認証の場合は、**enable** コマンドの代わりに **login** コマンドを使用できます。**login** によりユーザ名が維持されますが、認証をオンにするための設定は必要ありません。詳細については、「login コマンドによるユーザの認証」（P.18-22）を参照してください。

認証がある場合とない場合の ASDM アクセスの比較

デフォルトでは、ブランクのユーザ名と **enable password** コマンドによって設定されたイネーブル パスワードを使用して ASDM にログインできます。ログイン画面で（ユーザ名をブランクのままにしないで）ユーザ名とパスワードを入力した場合は、ASDM によってローカル データベースで一致がチェックされることに注意してください。

HTTP 認証を設定した場合は、ユーザ名をブランクのままにし、イネーブル パスワードを指定して ASDM を使用することはできなくなります。

コマンド許可に関する情報

この項では、コマンド許可について説明します。次の項目を取り上げます。

- 「サポートされるコマンド許可方式」（P.18-3）
- 「ユーザ クレデンシャルの維持について」（P.18-4）

サポートされるコマンド許可方式

次の 2 つのコマンド許可方式のいずれかを使用できます。

- ローカル特権レベル：ASA 1000V でコマンド特権レベルを設定します。ローカル ユーザ、RADIUS ユーザ、または LDAP ユーザ（LDAP 属性を RADIUS 属性にマッピングする場合）を CLI アクセスについて認証する場合、ASA 1000V はそのユーザをローカル データベース、RADIUS、または LDAP サーバで定義されている特権レベルに所属させます。ユーザは、割り当てられた特権レベル以下のコマンドにアクセスできます。すべてのユーザは、初めてログインする

ときに、ユーザ EXEC モード（レベル 0 または 1 のコマンド）にアクセスします。ユーザは、特権 EXEC モード（レベル 2 以上のコマンド）にアクセスするために再び **enable** コマンドで認証するか、**login** コマンドでログイン（ローカル データベースに限る）できます。

（注） ローカル データベース内にユーザが存在しなくても、また CLI 認証や **enable** 認証がない場合でも、ローカル コマンド許可を使用できます。代わりに、**enable** コマンドを入力するときにシステム イネーブル パスワードを入力すると、ASA 1000V によってレベル 15 に置かれます。次に、すべてのレベルのイネーブル パスワードを作成します。これにより、**enable** *n*（2 ～ 15）を入力したときに、ASA 1000V によってレベル *n* に置かれるようになります。これらのレベルは、ローカル コマンド許可をイネーブルにした場合に限り、使用されます（「ローカル コマンド許可の設定」（P.18-25）を参照）。**enable** コマンドの詳細については、コマンド リファレンスを参照してください。

- TACACS+ サーバ特権レベル：TACACS+ サーバで、ユーザまたはグループが CLI アクセスについて認証した後で使用できるコマンドを設定します。CLI でユーザが入力するすべてのコマンドは、TACACS+ サーバで検証されます。

ユーザ クレデンシャルの維持について

ユーザが ASA 1000V にログインする場合、ユーザ名とパスワードを入力して認証される必要があります。ASA 1000V は、同じセッションで後ほど認証が再び必要になる場合に備えて、これらのセッション クレデンシャルを保持します。

次の設定が行われている場合、ユーザはログイン時にローカル サーバだけで認証されればよいことになります。その後に続く認可では、保存されたクレデンシャルが使用されます。また、特権レベル 15 のパスワードの入力を求めるプロンプトが表示されます。特権モードを出るときに、ユーザは再び認証されます。ユーザのクレデンシャルは特権モードでは保持されません。

- ローカル サーバは、ユーザ アクセスの認証を行うように設定されます。
- 特権レベル 15 のコマンド アクセスは、パスワードを要求するように設定されます。
- ユーザのアカウントは、シリアル認可専用（コンソールまたは ASDM へのアクセスなし）として設定されます。
- ユーザのアカウントは、特権レベル 15 のコマンド アクセス用に設定されます。

次の表に、ASA 1000V でのクレデンシャルの使用方法を示します。

必要なクレデンシャル	ユーザ名とパスワードによる認証	シリアル認可	特権モード コマンド許可	特権モード終了認可
ユーザ名	Yes	No	No	Yes
パスワード	Yes	No	No	Yes
特権モードのパスワード	No	No	Yes	No

サーバ サポートの要約

表 18-1 に、各 AAA サービスのサポート状況の要約を AAA サーバ タイプ（ローカル データベースを含む）別に示します。特定の AAA サーバ タイプのサポートの詳細については、表に続く項目を参照してください。

表 18-1　AAA サポートの要約

	データベース タイプ						
AAA サービス	**ローカル**	**RADIUS**	**TACACS+**	**SDI（RSA）**	**NT**	**Kerberos**	**LDAP**
認証	Yes	Yes	Yes	Yes	Yes	Yes	Yes
認可	Yes[1]	No	Yes	No	No	No	No
アカウンティング	No	Yes[2]	Yes	No	No	No	No

1. ローカル コマンド認可は、特権レベルに限りサポートされます。
2. コマンド アカウンティングは、TACACS+ でのみ使用できます。

（注） 表 18-1 に記載されているネイティブ プロトコル認証のほか、ASA 1000V ではプロキシ認証がサポートされています。たとえば、ASA 1000V は RADIUS サーバ経由で RSA/SDI または Lightweight Directory Access Protocol（LDAP）サーバ、あるいはその両方へのプロキシとして動作することができます。

RADIUS サーバのサポート

ASA 1000V は次の RFC 互換サーバの AAA 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

認証方法

ASA 1000V は、RADIUS 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。
- 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、および RSA/SDI から RADIUS 接続。

属性のサポート

ASA 1000V 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 のベンダー固有属性（VSA）は、RADIUS ベンダー ID 9 で識別されます。
- RFC 2548 に定義されている Microsoft VSA
- Cisco VSA（Cisco-Priv-Level）。標準的な 0 ～ 15 の数値で特権のランクを表し、1 は最低レベル、15 は最高レベル。0 は特権がないことを示します。最初のレベル（ログイン）では、このレベルで使用可能なコマンドへの特権 EXEC アクセスを許可します。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。

TACACS+ サーバのサポート

ASA 1000V は、ASCII、PAP、CHAP、および MS-CHAPv1 で TACACS+ 認証をサポートします。

RSA/SDI サーバのサポート

RSA SecureID サーバは、SDI サーバとも呼ばれます。

この項は、次の内容で構成されています。

RSA/SDI バージョンのサポート

ASA 1000V では、SDI バージョン 5.x、6.x、および 7.x をサポートしています。SDI は、SDI プライマリ サーバおよび SDI レプリカ サーバの概念を使用します。各プライマリおよびそのレプリカは、シングル ノード秘密ファイルを共有します。そのノード秘密ファイルの名前は .sdi が付加された ACE またはサーバ IP アドレスの 16 進数値に基づきます。

ASA 1000V で設定するバージョン 5.x、6.x、または 7.x の SDI サーバは、プライマリまたはレプリカのいずれかになることができます。ユーザ認証のための SDI エージェントによるサーバの選択方法の詳細については、「RSA/SDI プライマリ サーバおよびレプリカ サーバ」（P.18-7）を参照してください。

2 ステップ認証プロセス

SDI バージョン 5.x、6.x、および 7.x では 2 ステップのプロセスを使用して、侵入者が RSA SecurID 認証要求から情報を取り込み、それを使用して別のサーバに認証を証明しないように防止します。エージェントはまず、SecurID サーバにロック要求を送信してから、ユーザ認証要求を送信します。サーバはユーザ名をロックして、別の（レプリカ）サーバがユーザ名を受信できないようにします。このアクションは、同じユーザが、同じ認証サーバを同時に使用して、2 つの ASA 1000V に認証を証明することができないことを意味します。ユーザ名のロックに成功すると、ASA 1000V はパスコードを送信します。

RSA/SDI プライマリ サーバおよびレプリカ サーバ

ASA 1000V は、最初のユーザが設定済みサーバ（プライマリでもレプリカでもかまいません）に認証を証明するときに、サーバ リストを取得します。次に、ASA 1000V はリスト上の各サーバにプライオリティを割り当て、その後のサーバ選択では、この割り当てられたプライオリティのサーバから無作為に抽出します。最もプライオリティの高いサーバが選択される可能性が高くなります。

NT サーバのサポート

ASA 1000V では、NTLM バージョン 1 をサポートしている Microsoft Windows Server オペレーティング システム（ひとまとめにして「NT サーバ」と呼びます）がサポートされています。

（注）　NT サーバでは、ユーザ パスワードの最大長は 14 文字です。それより長いパスワードは、NTLM バージョン 1 の制限により切り捨てられます。

Kerberos サーバのサポート

ASA 1000V は、3DES、DES、および RC4 暗号タイプをサポートしています。

単純な Kerberos サーバ コンフィギュレーションの例については、例 18-2（P.18-15）を参照してください。

LDAP サーバのサポート

ASA 1000V では LDAP をサポートしています。この項は、次の内容で構成されています。

LDAP による認証

認証中、ASA 1000V は、ユーザの LDAP サーバへのクライアント プロキシとして機能し、プレーン テキストまたは Simple Authentication and Security Layer（SASL）プロトコルのいずれかを使って LDAP サーバに対する認証を行います。デフォルトで、ASA 1000V は、通常はユーザ名とパスワードである認証パラメータを LDAP サーバにプレーン テキストで渡します。

ASA 1000V では、次の SASL メカニズムをサポートしています。次に、強度の低い順番に示します。

- Digest-MD5：ASA 1000V は、ユーザ名とパスワードから計算した MD5 値を使用して LDAP サーバに応答します。
- Kerberos：ASA 1000V は、GSSAPI Kerberos メカニズムを使用して、ユーザ名と領域を送信することで LDAP サーバに応答します。

これらの SASL メカニズムの任意の組み合わせをサポートするように、ASA 1000V と LDAP サーバを設定できます。複数のメカニズムを設定した場合、ASA 1000V ではサーバに設定されている SASL メカニズムのリストが取得され、認証メカニズムは ASA 1000V とサーバの両方に設定されているメカニズムのなかで最も強力なものに設定されます。たとえば、LDAP サーバと ASA 1000V の両方がこれら両方のメカニズムをサポートしている場合、ASA 1000V は、より強力な方の Kerberos メカニズムを選択します。

ユーザ LDAP 認証が成功すると、LDAP サーバは認証されたユーザの属性を返します。

LDAP サーバのタイプ

ASA 1000V では LDAP バージョン 3 がサポートされており、Sun Microsystems JAVA System Directory Server（従来の Sun ONE Directory Server）、Microsoft Active Directory、Novell、OpenLDAP、およびその他の LDAPv3 ディレクトリ サーバとの互換性があります。

デフォルトでは、ASA 1000V によって Microsoft Active Directory、Sun LDAP、Novell、OpenLDAP、または汎用 LDAPv3 ディレクトリ サーバに接続しているかどうかが自動検出されます。ただし、自動検出により LDAP サーバのタイプが特定できなくても、そのサーバが、Microsoft Active Directory、Sun LDAP ディレクトリ サーバ、それ以外の LDAP サーバのいずれであるかがわかっている場合は、そのサーバ タイプを手動で設定できます。

サーバ タイプを設定する場合、次のガイドラインに注意してください。

- Sun ディレクトリ サーバにアクセスするように ASA 1000V で設定されている Distinguished Name（DN; 認定者名）は、そのサーバのデフォルト パスワード ポリシーにアクセスできる必要があります。DN として、ディレクトリ管理者、またはディレクトリ管理者権限を持つユーザを使用することを推奨します。または、デフォルト パスワード ポリシーに ACL を設定できます。
- Microsoft Active Directory および Sun サーバでのパスワード管理をイネーブルにするために LDAP over SSL を設定する必要があります。
- ASA 1000V では、Novell、OpenLDAP、およびその他の LDAPv3 ディレクトリ サーバを使用したパスワード管理はサポートされません。
- ASA 1000V は、ログイン認定者名（DN）とログイン パスワードを使用して、LDAP サーバとの信頼関係（バインド）を築きます。

ローカル データベースのサポート（フォールバック方式としての機能を含む）

ASA 1000V は、ユーザ プロファイルを取り込むことができるローカル データベースを管理します。

ローカル データベースは、複数の機能のフォールバック方式として動作できます。この動作は、ASA 1000V から誤ってロックアウトされないようにすることを意図しています。

フォールバック サポートを必要とするユーザについては、ローカル データベース内のユーザ名およびパスワードと、AAA サーバ上のユーザ名およびパスワードとを一致させることを推奨します。これにより、透過フォールバックがサポートされます。ユーザは、AAA サーバとローカル データベースのどちらがサービスを提供しているかが判別できないので、ローカル データベースのユーザ名およびパスワードとは異なるユーザ名およびパスワードを AAA サーバで使用することは、指定するべきユーザ名とパスワードをユーザが確信できないことを意味します。

ローカル データベースでサポートされているフォールバック機能は次のとおりです。

- コンソールおよびイネーブル パスワード認証：グループ内のサーバがすべて使用可能である場合、ASA 1000V ではローカル データベースを使用して管理アクセスを認証します。これには、イネーブル パスワード認証が含まれる場合があります。
- コマンド認可：グループ内の TACACS+ サーバがすべて使用できない場合、特権レベルに基づいてコマンドを認可するためにローカル データベースが使用されます。

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

サーバ グループ内に複数のサーバを設定し、サーバ グループのローカル データベースへのフォールバックをイネーブルにしている場合、ASA 1000V からの認証要求に対してグループ内のどのサーバからも応答がないと、フォールバックが発生します。次のシナリオで例証します。

サーバ 1、サーバ 2 の順で、LDAP サーバ グループに 2 台の Active Directory サーバを設定します。リモート ユーザがログインすると、ASA 1000V によってサーバ 1 に対する認証が試みられます。

サーバ 1 から認証エラー（「*user not found*」など）が返されると、ASA 1000V によるサーバ 2 に対する認証は試みられません。

タイムアウト期間内にサーバ 1 から応答がないと（または認証回数が、設定されている最大数を超えている場合）、ASA 1000V によってサーバ 2 に対する認証が試みられます。

グループ内のどちらのサーバからも応答がなく、ASA 1000V にローカル データベースへのフォールバックが設定されている場合は、ASA 1000V によってローカル データベースに対する認証が試みられます。

前提条件

管理認証の前提条件

ASA 1000V において Telnet ユーザ、SSH ユーザ、または HTTP ユーザを認証できるようにするには、その前に ASA 1000V との通信を許可されている IP アドレスを特定する必要があります。詳細については、「ASDM、Telnet、または SSH の ASA 1000V アクセスの設定」（P.17-1）を参照してください。

ローカル コマンド許可の前提条件

- **enable** 認証を設定します（「CLI および ASDM アクセス認証の設定」（P.18-21）を参照）。

  enable 認証は、ユーザが **enable** コマンドにアクセスした後にユーザ名を保持するために不可欠です。

  あるいは、設定を必要としない **login** コマンド（これは、認証されている **enable** コマンドと同じでローカル データベースの場合に限る）を使用することもできます。このオプションは **enable** 認証ほど安全ではないため、お勧めしません。

  CLI 認証を使用することもできますが、必須ではありません。

- 次に示すユーザ タイプごとの前提条件を確認してください。
  - ローカル データベース ユーザ：ローカル データベース内の各ユーザの特権レベルを 0 ～ 15 で設定します。
  - RADIUS ユーザ：ユーザの Cisco VSA CVPN3000-Privilege-Level を、0 ～ 15 の値で設定します。
  - LDAP ユーザ：ユーザを特権レベル 0 ～ 15 の間で設定し、次に「LDAP 属性マップの設定」（P.18-15）の説明に従って、LDAP 属性を Cisco VSA CVPN3000-Privilege-Level にマッピングします。

TACACS+ コマンド許可の前提条件

- CLI 認証を設定する（「CLI および ASDM アクセス認証の設定」（P.18-21）を参照）。
- **enable** 認証を設定する（「特権 EXEC モードにアクセスするための認証の設定（enable コマンド）」（P.18-21）を参照）。

管理アカウンティングの前提条件

- CLI 認証を設定する（「CLI および ASDM アクセス認証の設定」（P.18-21）を参照）。
- **enable** 認証を設定する（「特権 EXEC モードにアクセスするための認証の設定（enable コマンド）」（P.18-21）を参照）。

デフォルト設定

デフォルトでは、次のコマンドが特権レベル 0 に割り当てられます。その他のすべてのコマンドは特権レベル 15 に割り当てられます。

- **show checksum**
- **show curpriv**
- **enable**
- **help**
- **show history**
- **login**
- **logout**
- **pager**
- **show pager**
- **clear pager**
- **quit**
- **show version**

コンフィギュレーション モード コマンドを 15 より低いレベルに移動する場合は、**configure** コマンドも同じレベルに移動してください。このようにしないと、ユーザはコンフィギュレーション モードに入ることができません。

すべての特権レベルを表示する方法は、「ローカル コマンド特権レベルの表示」（P.18-28）を参照してください。

AAA サーバおよびローカル ユーザの設定

この項は、次の内容で構成されています。

AAA サーバを設定するためのタスク フロー

ステップ 1　次のいずれかまたは両方を実行します。

- AAA サーバ グループを追加します。「AAA サーバ グループの設定」（P.18-11）を参照してください。
- ローカル データベースにユーザを追加します。「ユーザ アカウントのローカル データベースへの追加」（P.18-17）を参照してください。

ステップ 2　LDAP サーバの場合は、LDAP 属性マップを設定します。「LDAP 属性マップの設定」（P.18-15）を参照してください。

ステップ 3　（任意）ユーザは公開キーを使用して認証できます。「SSH の公開キーを持つユーザの認証」（P.18-20）を参照してください。

AAA 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 AAA サーバを使用する場合は、まず AAA プロトコルあたり少なくとも 1 つの 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。各サーバ グループは、Kerberos、LDAP、NT、RADIUS、SDI、または TACACS+ というサーバの 1 つのタイプ専用となります。

ガイドライン

- 最大 100 個のサーバ グループを使用できます。
- 各グループは、最大 16 個のサーバを持つことができます。
- ユーザがログインすると、コンフィギュレーション内で指定されている最初のサーバから順に、サーバが応答するまでこれらのサーバが 1 つずつアクセスされます。グループ内のすべてのサーバが使用できない場合、ASA 1000V は、ローカル データベースがフォールバック方式として設定されていると、ローカル データベースに接続しようとします（管理認証および認可限定）。フォールバック方式として設定されていない場合、ASA 1000V は引き続き AAA サーバにアクセスしようとします。

手順の詳細

	コマンド	目的

ステップ 1	**aaa-server** *server_tag* **protocol** {**kerberos** | **ldap** | **nt** | **radius** | **sdi** | **tacacs+**}
	
	例：
	`hostname(config)# aaa-server servergroup1 protocol ldap`
	`hostname(config-aaa-server-group)#`
	
	`hostname(config)# aaa-server servergroup1 protocol radius`
	
	`hostname(config)# aaa-server servergroup1 protocol radius`
	`hostname(config-aaa-server-group)# ad-agent-mode`
		サーバ グループ名とプロトコルを識別します。たとえば、RADIUS を使用してネットワーク アクセスを認証し、TACACS+ を使用して CLI アクセスを認証するには、RADIUS サーバ用に 1 つ、TACACS+ サーバ用に 1 つというように、最低 2 つのサーバ グループを作成する必要があります。
		
		最大 100 個のサーバ グループを使用できます。各グループは、最大 15 個のサーバを持つことができます。
		
		aaa-server protocol コマンドを入力する場合は、コンフィギュレーション モードを開始します。
		
		ad-agent-mode オプションで、ASA 1000V と AD エージェント間の共有秘密を指定し、RADIUS サーバ グループがフル機能の 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 ID と関連付けることができるのは、**ad-agent-mode** オプションを使用して設定された RADIUS サーバ グループだけです。結果として、**ad-agent-mode** オプションを使用して設定されていない RADIUS サーバ グループを指定すると **test aaa-server** {**authentication** | **authorization**} *aaa-server-group* コマンドが使用できなくなります。

ステップ 2	**max-failed-attempts** *number* **例：** `hostname(config-aaa-server-group)# max-failed-attempts 2`	次のサーバを試す前にグループ内の AAA サーバに送信する要求の最大数を指定します。*number* 引数の範囲は 1 ～ 5 です。デフォルトは 3 です。 ローカル データベースを使用してフォールバック方式を設定し（管理アクセスだけの場合は、「ローカル コマンド許可の設定」（P.18-25）および「TACACS+ コマンド許可の設定」（P.18-31）を参照してフォールバック メカニズムを設定）、グループ内のすべてのサーバが応答できなかった場合、グループは非応答と見なされ、フォールバック方式が試行されます。サーバ グループで、追加の AAA 要求によるアクセスがない、非応答と見なされる時間が 10 分間（デフォルト）続くと、ただちにフォールバック方式が使用されます。非応答時間をデフォルトから変更するには、次のステップの **reactivation-mode** コマンドを参照してください。 フォールバック方式として設定されていない場合、ASA 1000V は引き続きグループ内のサーバにアクセスしようとします。

	コマンド	目的
ステップ 3	**reactivation-mode** {**depletion** [**deadtime** *minutes*] | **timed**} **例：** hostname(config-aaa-server-group)# reactivation-mode deadtime 20	グループ内で障害の発生したサーバを再度アクティブ化する方法（再アクティブ化ポリシー）を指定します。 **depletion** キーワードを指定すると、グループ内のすべてのサーバが非アクティブになった後に、障害の発生したサーバが再度アクティブ化されます。 **deadtime** *minutes* キーワード引数のペアには、グループ内の最後のサーバをディセーブルにしてから、次にすべてのサーバを再度イネーブルにするまでの経過時間を分単位で 0 ～ 1440 から指定します。デフォルトは 10 分です。 **timed** キーワードは、30 秒間のダウンタイムの後に障害が発生したサーバを再度アクティブ化します。
ステップ 4	**accounting-mode simultaneous** **例：** hostname(config-aaa-server-group)# accounting-mode simultaneous	グループ内のすべてのサーバにアカウンティング メッセージを送信します（RADIUS または TACACS+ のみ）。 アクティブ サーバだけ送信メッセージをデフォルトに戻すには、**accounting-mode single** コマンドを入力します。
ステップ 5	**aaa-server** *server_group* [*interface_name*] **host** *server_ip* **例：** hostname(config)# aaa-server servergroup1 [outside] host 10.10.1.1	サーバと、そのサーバが属する AAA サーバ グループを識別します。 *interface_name* 引数には、イーサネット インターフェイスの名前を指定します。 **aaa-server host** コマンドを入力すると、AAA サーバのホスト コンフィギュレーション モードを開始します。必要に応じて、ホスト コンフィギュレーション モード コマンドを使用して、さらに AAA サーバを設定します。 ホスト コンフィギュレーション モードでのコマンドは、すべての AAA サーバ タイプに適用されるわけではありません。表 18-2 に、使用可能なコマンド、適用先のサーバ タイプ、および新規 AAA サーバ定義にそのコマンドのデフォルト値が指定されているかどうかを示します。コマンドが、指定したサーバ タイプに適用可能で、デフォルト値が用意されていない場合は（「—」で示す）、コマンドを使用して値を指定します。

表 18-2　ホスト モード コマンド、サーバ タイプ、およびデフォルト

コマンド	適用可能な AAA サーバ タイプ	デフォルト値	説明
accounting-port	RADIUS	1646	
acl-netmask-convert	RADIUS	standard	
authentication-port	RADIUS	1645	
kerberos-realm	Kerberos	—	

表 18-2　ホスト モード コマンド、サーバ タイプ、およびデフォルト （続き）

コマンド	適用可能な AAA サーバ タイプ	デフォルト値	説明
key	RADIUS	—	
	TACACS+	—	
ldap-attribute-map	LDAP	—	
ldap-base-dn	LDAP	—	
ldap-login-dn	LDAP	—	
ldap-login-password	LDAP	—	
ldap-naming-attribute	LDAP	—	
ldap-over-ssl	LDAP	636	設定されていない場合は、ASA 1000V では LDAP 要求に sAMAccountName を使用します。SASL とプレーン テキストのどちらを使用する場合でも、ASA 1000V と LDAP サーバの間での通信のセキュリティは SSL で確保されます。SASL を設定しない場合、SSL で LDAP 通信を保護することを強くお勧めします。
ldap-scope	LDAP	—	
mschapv2-capable	RADIUS	enabled	
nt-auth-domain-controller	NT	—	
radius-common-pw	RADIUS	—	
retry-interval	Kerberos	10 秒	
	RADIUS	10 秒	
	SDI	10 秒	
sasl-mechanism	LDAP	—	
server-port	Kerberos	88	
	LDAP	389	
	NT	139	
	SDI	5500	
	TACACS+	49	
server-type	LDAP	auto-discovery	自動検出により LDAP サーバのタイプが特定できなくても、そのサーバが、Microsoft Active Directory、Sun LDAP ディレクトリ サーバ、それ以外の LDAP サーバのいずれであるかがわかっている場合は、そのサーバ タイプを手動で設定できます。
timeout	すべて	10 秒	

例

例 18-1 に、1 つのプライマリ サーバと 1 つのバックアップ サーバを持つ 1 つの TACACS+ グループ、単一のサーバを持つ 1 つの RADIUS グループ、および 1 つの NT ドメイン サーバを追加する方法を示します。

例 18-1　　複数の AAA サーバ グループおよびサーバ

```
hostname(config)# aaa-server AuthInbound protocol tacacs+
hostname(config-aaa-server-group)# max-failed-attempts 2
hostname(config-aaa-server-group)# reactivation-mode depletion deadtime 20
hostname(config-aaa-server-group)# exit
hostname(config)# aaa-server AuthInbound (inside) host 10.1.1.1
hostname(config-aaa-server-host)# key TACPlusUauthKey
hostname(config-aaa-server-host)# exit
hostname(config)# aaa-server AuthInbound (inside) host 10.1.1.2
hostname(config-aaa-server-host)# key TACPlusUauthKey2
hostname(config-aaa-server-host)# exit
hostname(config)# aaa-server AuthOutbound protocol radius
hostname(config-aaa-server-group)# exit
hostname(config)# aaa-server AuthOutbound (inside) host 10.1.1.3
hostname(config-aaa-server-host)# key RadUauthKey
hostname(config-aaa-server-host)# exit
hostname(config)# aaa-server NTAuth protocol nt
hostname(config-aaa-server-group)# exit
hostname(config)# aaa-server NTAuth (inside) host 10.1.1.4
hostname(config-aaa-server-host)# nt-auth-domain-controller primary1
hostname(config-aaa-server-host)# exit
```

例 18-2 に、watchdogs という名前の Kerberos AAA サーバ グループを設定し、そのグループに AAA サーバを追加して、そのサーバの Kerberos 領域を定義する方法を示します。例 18-2 では、リトライ インターバルと Kerberos サーバがリスンするポートを定義していないため、ASA 1000V は、これら 2 つのサーバ固有のパラメータにデフォルト値を使用します。表 18-2 に、すべての AAA サーバ ホスト モード コマンドのデフォルト値を示します。

（注） Kerberos 領域名では数字と大文字だけを使用します。ASA 1000V は領域名に小文字を受け入れますが、小文字を大文字に変換しません。大文字だけを使用してください。

例 18-2　　Kerberos サーバ グループおよびサーバ

```
hostname(config)# aaa-server watchdogs protocol kerberos
hostname(config-aaa-server-group)# aaa-server watchdogs host 192.168.3.4
hostname(config-aaa-server-host)# kerberos-realm EXAMPLE.COM
hostname(config-aaa-server-host)# exit
hostname(config)#
```

LDAP 属性マップの設定

ASA 1000V では、管理ユーザを認証するために LDAP ディレクトリを使用できます。

ガイドライン

属性マッピング機能を適切に使用するには、シスコの LDAP 属性の名前と値およびユーザ定義の属性の名前と値を理解する必要があります。

手順の詳細

	コマンド	目的
ステップ 1	**ldap attribute-map** *map-name* **例：** hostname(config)# ldap attribute-map att_map_1	空の LDAP 属性マップ テーブルを作成します。
ステップ 2	**map-name** *user-attribute-name Cisco-attribute-name* **例：** hostname(config-ldap-attribute-map)# map-name department IETF-Radius-Class	ユーザ定義の属性名 department を、シスコの属性にマッピングします。
ステップ 3	**map-value** *user-attribute-name Cisco-attribute-name* **例：** hostname(config-ldap-attribute-map)# map-value department Engineering group1	ユーザ定義のマップ値である department をユーザ定義の属性値とシスコの属性値にマッピングします。
ステップ 4	**aaa-server** *server_group* [*interface_name*] **host** *server_ip* **例：** hostname(config)# aaa-server [ldap_dir_1] host 10.1.1.4	サーバと、そのサーバが属する AAA サーバ グループを識別します。 *interface_name* 引数には、イーサネット インターフェイスの名前を指定します。
ステップ 5	**ldap-attribute-map** *map-name* **例：** hostname(config-aaa-server-host)# ldap-attribute-map att_map_1	属性マップを LDAP サーバにバインドします。

例

次の例は、accessType という名前の LDAP 属性に基づいて管理セッションを ASA 1000V に制限する方法を示しています。accessType 属性の有効な値は次の 2 つです。

- admin
- helpdesk

次の例では、各値が、ASA 1000V でサポートされる有効な IETF-Radius-Service-Type 属性のいずれかにマッピングされる方法を示します。有効なタイプには、admin（Service-Type 6）管理および nas-prompt（Service-Type 7）NAS プロンプトがあります。

```
hostname(config)# ldap attribute-map MGMT
hostname(config-ldap-attribute-map)# map-name accessType IETF-Radius-Service-Type
hostname(config-ldap-attribute-map)# map-value accessType admin 6
hostname(config-ldap-attribute-map)# map-value accessType helpdesk 7

hostname(config-ldap-attribute-map)# aaa-server LDAP protocol ldap
hostname(config-aaa-server-group)# aaa-server LDAP (inside) host 10.1.254.91
hostname(config-aaa-server-host)# ldap-base-dn CN=Users,DC=cisco,DC=local
hostname(config-aaa-server-host)# ldap-scope subtree
```

```
hostname(config-aaa-server-host)# ldap-login-password test
hostname(config-aaa-server-host)# ldap-login-dn
CN=Administrator,CN=Users,DC=cisco,DC=local
hostname(config-aaa-server-host)# server-type auto-detect
hostname(config-aaa-server-host)# ldap-attribute-map MGMT
```

次の例では、シスコの LDAP 属性名の全リストを表示します。

```
hostname(config)# ldap attribute-map att_map_1
hostname(config-ldap-attribute-map)# map-name att_map_1?

ldap mode commands/options:
cisco-attribute-names:
Access-Hours
  Allow-Network-Extension-Mode
  Auth-Service-Type
  Authenticated-User-Idle-Timeout
  Authorization-Required
  Authorization-Type
    :
    :
X509-Cert-Data
hostname(config-ldap-attribute-map)#
```

ユーザ アカウントのローカル データベースへの追加

ここでは、ローカル データベース内のユーザの管理方法について説明します。

ガイドライン

次の各機能は、ローカル データベースを使用して実行されます。

- ASDM ユーザごとのアクセス
- コンソール認証
- Telnet 認証および SSH 認証。
- **enable** コマンド認証

  この設定は、CLI アクセスにだけ使用され、ASDM ログインには影響しません。
- コマンド認可

  ローカル データベースを使用するコマンド認可を有効にすると、ASA 1000V では、ユーザ特権レベルを参照して、どのコマンドが使用できるかが特定されます。コマンド認可がディセーブルの場合は通常、特権レベルは参照されません。デフォルトでは、コマンドの特権レベルはすべて、0 または 15 のどちらかです。

手順の詳細

	コマンド	目的
ステップ 1	**username** *username* {**nopassword** | **password** *password*]} [**privilege** *priv_level*] **例：** `hostname(config)# username exampleuser1 privilege 1`	ユーザ アカウントを作成します。**username** *username* キーワードは、4 ～ 64 文字の文字列です。 **password** *password* キーワードは、3 ～ 32 文字の文字列です。**privilege** *level* キーワードでは、0 ～ 15 の特権レベルを設定します。デフォルトは 2 です。この特権レベルは、コマンド認可で使用されます。 ⚠ **注意** コマンド認可（**aaa authorization console LOCAL** コマンド）を使用していない場合、デフォルトのレベル 2 を使用して特権 EXEC モードにアクセスできます。特権 EXEC モードへのアクセスを制限する場合、特権レベルを 0 または 1 に設定するか、または **service-type** コマンドを使用します（ステップ 4 を参照）。 **nopassword** キーワードは、パスワードを指定しないユーザ アカウントを作成します。 通常、**encrypted** および **nt-encrypted** キーワードは表示専用です。**username** コマンド内のパスワードを定義すると、ASA 1000V はセキュリティを維持するため、そのパスワードをコンフィギュレーションに保存するときに暗号化します。**show running-config** コマンドを入力すると、**username** コマンドは実際のパスワードを表示しません。このコマンドは暗号化されたパスワードを表示し、次に **encrypted** または **nt-encrypted** キーワード（**mschap** を指定する場合）を表示します。たとえば、パスワードに「test」と入力すると、**show running-config** の出力には次のように表示されます。 `username user1 password DLaUiAX3l78qgoB5c7iVNw== nt-encrypted` 実際に CLI で **encrypted** または **nt-encrypted** キーワードを入力するのは、あるコンフィギュレーション ファイルを他の ASA 1000V にカット アンド ペーストして、同じパスワードを使用している場合だけです。

	コマンド	目的
ステップ 2	**aaa authorization exec authentication-server** **例：** `hostname(config)# aaa authorization exec authentication-server`	（任意）管理アクセスを認証するユーザに、ユーザ固有のアクセス レベルを強制します（**aaa authentication console LOCAL** コマンドを参照）。このコマンドは、ローカル、RADIUS、LDAP（マッピング済み）、および TACACS+ の各ユーザの管理認可をイネーブルにします。 **aaa authorization exec LOCAL** コマンドを使用して、ローカル データベースから属性を取得できるようにします。AAA サーバのユーザを管理認可が有効になるように設定する方法については、「管理認可によるユーザ CLI および ASDM アクセスの制限」（P.18-23）を参照してください。 次に示すユーザ タイプごとの前提条件を確認してください。 • **username** コマンドを使用して、0 ～ 15 の特権レベルでローカル データベースでユーザを設定します。**service-type** コマンドを使用して、アクセスのレベルを設定します。 • RADIUS ユーザに Cisco VSA CVPN3000-Privilege-Level の 0 ～ 15 の値を設定します。 • LDAP ユーザを特権レベル 0 ～ 15 を使用して設定し、**ldap map-attributes** コマンドを使用して LDAP 属性を Cisco VAS CVPN3000-Privilege-Level にマッピングします。 • コマンド特権レベルの設定については、**privilege** コマンドを参照してください。
ステップ 3	**service-type** {**admin** | **nas-prompt**} **例：** `hostname(config-username)# service-type admin`	（任意）ステップ 2 で管理認可を設定した場合は、ユーザ レベルを設定します。**admin** キーワードは、**aaa authentication console LOCAL** コマンドによって指定されたサービスへのフル アクセスを許可します。デフォルトは **admin** キーワードです。 **nas-prompt** キーワードは、**aaa authentication** {**telnet** | **ssh** | **serial**} **console LOCAL** コマンドを設定しているときに CLI へのアクセスを許可しますが、**aaa authentication http console LOCAL** コマンドを設定しているときは ASDM へのコンフィギュレーション アクセスを拒否します。ASDM モニタリング アクセスは許可します。**aaa authentication enable console LOCAL** コマンドを使用して認証をイネーブルにしている場合、ユーザは、**enable** コマンド（または **login** コマンド）を使用して特権 EXEC モードにアクセスできません。 詳細については、「管理認可によるユーザ CLI および ASDM アクセスの制限」（P.18-23）を参照してください。

例

次の例では、admin ユーザ アカウントに対して特権レベル 15 を割り当てます。

```
hostname(config)# username admin password password privilege 15
```

次の例では、パスワードを指定しないユーザ アカウントを作成します。

```
hostname(config)# username user34 nopassword
```

次の例では、管理認可をイネーブルにし、パスワードを指定するユーザ アカウントを作成し、ユーザ名属性コンフィギュレーション モードを開始して、**service-type** 属性を指定します。

```
hostname(config)# aaa authorization exec authentication-server
hostname(config)# username user1 password gOgeOus
hostname(config)# username user1 attributes
hostname(config-username)# service-type nas-prompt
```

SSH の公開キーを持つユーザの認証

ユーザは SSH の公開キーで認証を受けることができます。公開キーはハッシュすることもハッシュしないこともできます。

SSH の公開キーで認証を行うには、次のコマンドを入力します。

コマンド	目的
username {*user*} **attributes ssh authentication publickey** *key* **[hashed]** **例：** `hostname(config)# username anyuser ssh authentication publickey key [hashed]`	公開キー認証をユーザ単位でイネーブルにします。*key* 引数の値は次のいずれかになります。 • *key* 引数が指定され、ハッシュされたタグが指定されていない場合、キーの値は、SSH-RSA の未処理キーを生成することのできる SSH キー生成ソフトウェアによって生成される Base 64 で符号化された公開キーである必要があります（つまり、証明書は使用しません）。Base 64 符号化済みの公開キーを送信すると、そのキーは SHA-256 によってハッシュされ、対応する 32 バイトのハッシュがそれ以降の比較に使用されます。 • *key* 引数が指定され、ハッシュされたタグを指定した場合は、キーの値は、SHA-256 で事前にハッシュされている必要があります。長さは 32 バイトで、各バイトはコロンで区切られている必要があります（解析のため）。 設定を保存すると、ハッシュされたキー値はコンフィギュレーションに保存され、ASA 1000V のリブート時に使用されます。

管理アクセス用の AAA の設定

- 「管理アクセス アカウンティングの設定」（P.18-32）
- 「現在のログイン ユーザの表示」（P.18-34）
- 「ロックアウトからの回復」（P.18-33）

CLI および ASDM アクセス認証の設定

認証を設定するには、次のコマンドを入力します。

手順の詳細

コマンド	目的
aaa authentication {**telnet** | **ssh** | **http** | **serial**} **console** {**LOCAL** | *server_group* [**LOCAL**]} **例：** `hostname(config)# aaa authentication telnet console LOCAL`	管理アクセス用のユーザを認証します。**telnet** キーワードを使用すると、Telnet アクセスを制御できます。 **ssh** キーワードを使用すると、SSH アクセスを制御できます。SSH のデフォルト ユーザ名である asa および pix は現在はサポートされていません。 **http** キーワードを使用すると、ASDM アクセスを制御できます。 **serial** キーワードを使用すると、コンソール ポート アクセスを制御できます。 HTTP 管理認証では、AAA サーバ グループの SDI プロトコルをサポートしていません。 認証に AAA サーバ グループを使用する場合は、AAA サーバが使用できないときにローカル データベースをフォールバック方式として使用するように ASA 1000V を設定できます。サーバ グループ名の後ろに **LOCAL** を指定します（**LOCAL** は大文字と小文字を区別します）。ローカル データベースでは AAA サーバと同じユーザ名およびパスワードを使用することを推奨します。これは、ASA 1000V のプロンプトでは、いずれの方式が使用されているかが示されないためです。 **LOCAL** だけを入力して、ローカル データベースを認証の主要方式として（フォールバックなしで）使用することもできます。

特権 EXEC モードにアクセスするための認証の設定（enable コマンド）

ユーザが **enable** コマンドを入力したときに AAA サーバまたはローカル データベースでそれらのユーザを認証するように ASA 1000V を設定することができます。あるいは、ユーザは **login** コマンドを入力したときにローカル データベースで自動的に認証されます。この場合も、ローカル データベース内のユーザ レベルに応じて特権 EXEC モードにアクセスします。

ここでは、次の内容について説明します。

- 「enable コマンドの認証の設定」（P.18-22）
- 「login コマンドによるユーザの認証」（P.18-22）

enable コマンドの認証の設定

ユーザが **enable** コマンドを入力したときに認証されるように、ASA 1000V を設定できます。詳細については、「認証がある場合とない場合の CLI アクセスの比較」（P.18-3）を参照してください。

enable コマンドの入力時にユーザを認証するには、次のコマンドを入力します。

コマンド	目的
aaa authentication enable console {**LOCAL** | *server_group* [**LOCAL**]} **例：** hostname(config)# aaa authentication enable console LOCAL	**enable** コマンドを入力したユーザを認証します。ユーザ名とパスワードの入力を求めるプロンプトがユーザに対して表示されます。 認証に AAA サーバ グループを使用する場合は、AAA サーバが使用できないときにローカル データベースをフォールバック方式として使用するように ASA 1000V を設定できます。サーバ グループ名の後ろに **LOCAL** を指定します（**LOCAL** は大文字と小文字を区別します）。ローカル データベースでは AAA サーバと同じユーザ名およびパスワードを使用することを推奨します。これは、ASA 1000V のプロンプトでは、いずれの方式が使用されているかが示されないためです。 **LOCAL** だけを入力して、ローカル データベースを認証の主要方式として（フォールバックなしで）使用することもできます。

login コマンドによるユーザの認証

ユーザ EXEC モードから、**login** コマンドを使用してローカル データベース内のユーザ名でログインすることができます。

この機能を使用すると、ユーザは独自のユーザ名とパスワードでログインして特権 EXEC モードにアクセスすることができるので、システム イネーブル パスワードを全員に提供する必要がなくなります。ユーザがログイン時に特権 EXEC モード（およびすべてのコマンド）にアクセスできるようにするには、ユーザの特権レベルを 2（デフォルト）～ 15 に設定します。ローカル コマンド認可を設定した場合、ユーザは、その特権レベル以下のレベルに割り当てられているコマンドのみを入力できます。詳細については、「ローカル コマンド許可の設定」（P.18-25）を参照してください。

注意　CLI にアクセスできるユーザや特権 EXEC モードを開始できないようにするユーザをローカル データベースに追加する場合は、コマンド認可を設定する必要があります。コマンド認可がない場合、特権レベルが 2 以上（2 がデフォルト）のユーザは、CLI で自分のパスワードを使用して特権 EXEC モード（およびすべてのコマンド）にアクセスできます。あるいは、認証処理で AAA サーバを使用するか、またはすべてのローカル ユーザをレベル 1 に設定することにより、システム イネーブル パスワードを使用して特権 EXEC モードにアクセスできるユーザを制御できます。

ローカル データベースからユーザとしてログインするには、次のコマンドを入力します。

コマンド	目的
login **例：** hostname# **login**	ローカル データベースからユーザとしてログインします。ASA 1000V により、ユーザ名とパスワードの入力を求めるプロンプトが表示されます。パスワードを入力すると、ASA 1000V により、ユーザはローカル データベースで指定されている特権レベルに置かれます。

管理認可によるユーザ CLI および ASDM アクセスの制限

CLI 認証または **enable** 認証を設定すると、ローカル ユーザ、RADIUS、TACACS+、または LDAP ユーザ（LDAP 属性を RADIUS 属性にマッピングする場合）からの CLI、ASDM、または **enable** コマンドへのアクセスを制限できます。

（注）　シリアル アクセスは管理認証に含まれないため、**aaa authentication serial console** コマンドを設定している場合は、認証したユーザはすべてコンソール ポートにアクセスできます。

手順の詳細

	コマンド	目的
ステップ 1	**aaa authorization exec authentication-server** **例：** `hostname(config)# aaa authorization exec authentication-server`	ローカル、RADIUS、LDAP（マッピング済み）、および TACACS+ の各ユーザの管理認可をイネーブルにします。また、RADIUS からの管理ユーザ特権レベルのサポートもイネーブルになります。この特権レベルは、コマンド認可でのローカル コマンドの特権レベルと併用できます。詳細については、「ローカル コマンド許可の設定」（P.18-25）を参照してください。**aaa authorization exec LOCAL** コマンドを使用して、ローカル データベースから属性を取得できるようにします。

コマンド	目的

ステップ 2　ユーザを管理認証対象に設定するには、次の各 AAA サーバ タイプまたはローカル ユーザの要件を参照してください。

- RADIUS または LDAP（マッピング済み）ユーザ：IETF RADIUS 数値型属性の Service-Type を使用します。この属性は、次のいずれかの値にマッピングされます。
  - Service-Type 6（管理）：**aaa authentication console** コマンドで指定されたサービスへのフル アクセスを許可します。
  - Service-Type 7（NAS プロンプト）：**aaa authentication** {**telnet** | **ssh**} **console** コマンドを設定した場合は CLI へのアクセスを許可しますが、**aaa authentication http console** コマンドを設定した場合は ASDM コンフィギュレーション アクセスを拒否します。ASDM モニタリング アクセスは許可します。**aaa authentication enable console** コマンドでイネーブル認証を設定している場合、ユーザは **enable** コマンドを使用して特権 EXEC モードにアクセスできません。
  - Service-Type 5（発信）：管理アクセスを拒否します。ユーザは **aaa authentication console** コマンドで指定されたサービスを使用できません（**serial** キーワードを除きます。シリアル アクセスは許可されます）。IPSec ユーザはまだサイトツーサイト セッションを認証および終了できます。

  Cisco VSA CVPN3000-Privilege-Level を、0 ～ 15 の値で設定します。次に、**ldap map-attributes** コマンドを使用して LDAP 属性を Cisco VAS CVPN3000-Privilege-Level にマッピングします。詳細については、「LDAP 属性マップの設定」（P.18-15）を参照してください。
- TACACS+ ユーザ：「service=shell」で認可が要求され、サーバは PASS または FAIL で応答します。
  - PASS、特権レベル 1：設定およびモニタリング セクションへの限定的な読み取り専用アクセス権で ASDM へのアクセスと、権限レベル 1 の **show** コマンドのみへのアクセスを許可します。
  - PASS、特権レベル 2 以上：**aaa authentication** {**telnet** | **ssh**} **console** コマンドを設定した場合は CLI へのアクセスを許可しますが、**aaa authentication http console** コマンドを設定した場合は ASDM コンフィギュレーション アクセスを拒否します。ASDM モニタリング アクセスは許可します。**aaa authentication enable console** コマンドを使用して**イネーブル**認証を設定すると、ユーザは **enable** コマンドを使用して特権 EXEC モードにアクセスできません。イネーブルの特権レベルが 14 以下に設定されている場合は、**enable** コマンドを使用して特権 EXEC モードにアクセスすることはできません。
  - FAIL：管理アクセスを拒否します。**aaa authentication console** コマンドで指定されたサービスは使用できません（**serial** キーワードを除きます。シリアル アクセスは許可されます）。
- ローカル ユーザ：**service-type** コマンドを設定します。デフォルトの **service-type** は **admin** で、**aaa authentication console** コマンドで指定されたサービスへのフル アクセスを許可します。0 ～ 15 の特権レベルでローカル データベース ユーザを設定するには、**username** コマンドを使用します。詳細については、「ユーザ アカウントのローカル データベースへの追加」（P.18-17）を参照してください。

コマンド許可の設定

コマンドへのアクセスを制御する場合、ASA 1000V ではコマンド許可を設定でき、ユーザが使用できるコマンドを決定できます。デフォルトでは、ログインするとユーザ EXEC モードにアクセスでき、最低限のコマンドだけが提供されます。**enable** コマンド（または、ローカル データベースを使用するときは **login** コマンド）を入力すると、特権 EXEC モードおよびコンフィギュレーション コマンドを含む高度なコマンドにアクセスできます。

次の 2 つのコマンド許可方式のいずれかを使用できます。

- ローカル特権レベル
- TACACS+ サーバ特権レベル

このコマンド許可の詳細については、「コマンド許可に関する情報」（P.18-3）を参照してください。

ここでは、次の内容について説明します。

ローカル コマンド許可の設定

ローカル コマンド許可を使用して、コマンドを 16 の特権レベル（0 ～ 15）の 1 つに割り当てることができます。デフォルトでは、各コマンドは特権レベル 0 または 15 に割り当てられます。各ユーザを特定の特権レベルに定義でき、各ユーザは割り当てられた特権レベル以下のコマンドを入力できます。

ASA 1000V は、ローカル データベース、RADIUS サーバ、または LDAP サーバ（LDAP 属性を RADIUS 属性にマッピングする場合。「LDAP 属性マップの設定」（P.18-15）を参照してください）で定義されるユーザ特権レベルをサポートします。

ローカル コマンド許可を設定するには、次の手順を実行します。

手順の詳細

	コマンド	目的
ステップ 1	**privilege** [**show** | **clear** | **cmd**] **level** *level* [**mode** {**enable** | **cmd**}] **command** *command* **例：** `hostname(config)# privilege show level 5 command filter`	特権レベルにコマンドを割り当てます。 再割り当てする各コマンドに対してこのコマンドを繰り返します。 このコマンドのオプションは、次のとおりです。 • **show** | **clear** | **cmd**：これらのオプション キーワードを使用すると、コマンドの show、clear、または configure 形式に対してだけ特権を設定できます。コマンドの configure 形式は、通常、未修正コマンド（**show** または **clear** プレフィックスなしで）または **no** 形式として、コンフィギュレーションの変更を引き起こす形式です。これらのキーワードのいずれかを使用しない場合は、コマンドのすべての形式が影響を受けます。 • **level** *level*：0 ～ 15 のレベル。 • **mode** {**enable** | **configure**}：ユーザ EXEC モードまたは特権 EXEC モードおよびコンフィギュレーション モードでコマンドを入力することができ、そのコマンドが各モードで異なるアクションを実行する場合は、それらのモードの特権レベルを個別に設定することができます。 – **enable**：ユーザ EXEC モードと特権 EXEC モードの両方を指定します。 – **configure**：**configure terminal** コマンドを使用してアクセスされるコンフィギュレーション モードを指定します。 • **command** *command*：設定しているコマンド。設定できるのは、*main* コマンドの特権レベルだけです。たとえば、すべての **aaa** コマンドのレベルを設定できますが、**aaa authentication** コマンドと **aaa authorization** コマンドのレベルを個別に設定できません。

	コマンド	目的
ステップ 2	**aaa authorization exec authentication-server** **例：** `hostname(config)# aaa authorization exec authentication-server`	RADIUS からの管理ユーザ特権レベルをサポートします。 管理アクセスを認証するユーザに、ユーザ固有のアクセス レベルを強制します（**aaa authentication console LOCAL** コマンドを参照）。 このコマンドを入力しない場合、ASA 1000V は、ローカル データベース ユーザの特権レベルだけをサポートし、他のタイプのユーザをすべてデフォルトでレベル 15 に割り当てます。 このコマンドは、ローカル、RADIUS、LDAP（マッピング済み）、および TACACS+ の各ユーザの管理認可もイネーブルにします。 **aaa authorization exec LOCAL** コマンドを使用して、ローカル データベースから属性を取得できるようにします。AAA サーバのユーザを管理認可が有効になるように設定する方法については、「管理認可によるユーザ CLI および ASDM アクセスの制限」（P.18-23）を参照してください。
ステップ 3	**aaa authorization command LOCAL** **例：** `hostname(config)# aaa authorization command LOCAL`	ローカル コマンドの特権レベルの使用をイネーブルにします。ローカル コマンドの特権レベルを使用すると、ローカル データベース、RADIUS サーバ、または LDAP サーバ（マッピングされた属性を持つ）のユーザの特権レベルと比較して検査できます。 コマンド特権レベルを設定する場合は、このコマンドでコマンド認可を設定しない限り、コマンド認可は実行されません。

例

filter コマンドの形式は次のとおりです。

- **filter**（**configure** オプションで表されます）
- **show running-config filter**
- **clear configure filter**

特権レベルを形式ごとに個別に設定することができます。または、このオプションを省略してすべての形式に同じ特権レベルを設定することもできます。次は、各形式を個別に設定する方法の例です。

```
hostname(config)# privilege show level 5 command filter
hostname(config)# privilege clear level 10 command filter
hostname(config)# privilege cmd level 10 command filter
```

また、次の例では、すべての filter コマンドを同じレベルに設定する例を示します。

```
hostname(config)# privilege level 5 command filter
```

show privilege コマンドは、形式を分けて表示します。

次の例では、**mode** キーワードの使用方法を示します。**enable** コマンドは、ユーザ EXEC モードから入力する必要があります。一方、**enable password** コマンドは、コンフィギュレーション モードでアクセスでき、最も高い特権レベルが必要です。

```
hostname(config)# privilege cmd level 0 mode enable command enable
hostname(config)# privilege cmd level 15 mode cmd command enable
hostname(config)# privilege show level 15 mode cmd command enable
```

次に、**mode** キーワードを使用して、**configure** コマンドにレベルを設定する例を示します。

```
hostname(config)# privilege show level 5 mode cmd command configure
hostname(config)# privilege clear level 15 mode cmd command configure
hostname(config)# privilege cmd level 15 mode cmd command configure
hostname(config)# privilege cmd level 15 mode enable command configure
```

（注）　この最後の行は、**configure terminal** コマンドで使用します。

ローカル コマンド特権レベルの表示

次のコマンドを使用すると、コマンドの特権レベルを表示できます。

コマンド	目的
show running-config all privilege all	すべてのコマンドを表示します。
show running-config privilege level *level*	特定のレベルのコマンドを表示します。*level* は 0 ～ 15 の整数です。
show running-config privilege command *command*	特定のコマンドのレベルを表示します。

例

たとえば、**show running-config all privilege all** コマンドの場合、ASA 1000V は特権レベルに対する各 CLI コマンドの現在の割り当てを表示します。次に、このコマンドの出力例を示します。

```
hostname(config)# show running-config all privilege all
privilege show level 15 command aaa
privilege clear level 15 command aaa
privilege configure level 15 command aaa
privilege show level 15 command aaa-server
privilege clear level 15 command aaa-server
privilege configure level 15 command aaa-server
privilege show level 15 command access-group
privilege clear level 15 command access-group
privilege configure level 15 command access-group
privilege show level 15 command access-list
privilege clear level 15 command access-list
privilege configure level 15 command access-list
....
```

次の例は、特権レベル 10 に対するコマンドの割り当てを示しています。

```
hostname(config)# show running-config privilege level 10
privilege show level 10 command aaa
```

次の例は、**access-list** コマンドに対するコマンドの割り当てを示しています。

```
hostname(config)# show running-config privilege command access-list
privilege show level 15 command access-list
privilege clear level 15 command access-list
privilege configure level 15 command access-list
```

TACACS+ サーバでのコマンドの設定

グループまたは個々のユーザの共有プロファイル コンポーネントとしての Cisco Secure Access Control Server（ACS）TACACS+ サーバでコマンドを設定できます。サードパーティの TACACS+ サーバの場合は、コマンド許可サポートの詳細については、ご使用のサーバのマニュアルを参照してください。

Cisco Secure ACS バージョン 3.1 でコマンドを設定する場合は、次のガイドラインを参照してください。

- ASA 1000V は、「シェル」コマンドとして認可するコマンドを送信し、TACACS+ サーバでシェル コマンドとしてコマンドを設定します。

（注）　Cisco Secure ACS には、「pix-shell」と呼ばれるコマンド タイプが含まれている場合があります。このタイプを ASA 1000V コマンド認可には使用しないでください。

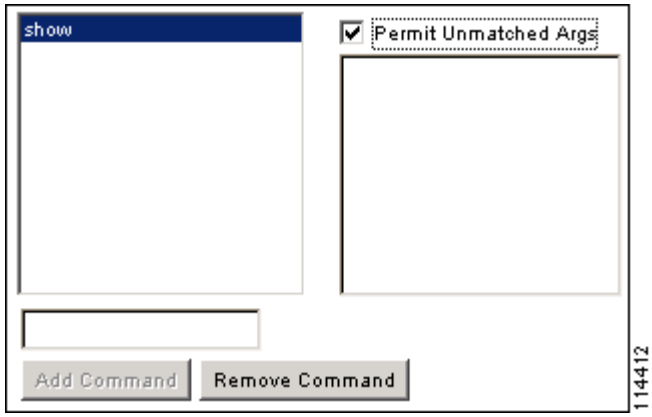
- コマンドの最初のワードは、メイン コマンドと見なされます。その他のワードはすべて引数と見なされます。これは、**permit** または **deny** の後に置く必要があります。

  たとえば、**show running-configuration aaa-server** コマンドを許可するには、コマンド フィールドに **show running-configuration** を追加し、引数フィールドに **permit aaa-server** を入力します。

- [Permit Unmatched Args] チェックボックスをオンにすると、明示的に拒否していないすべてのコマンド引数を許可できます。

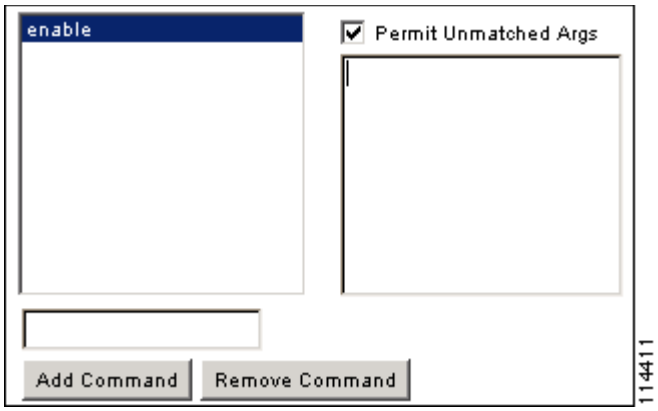
  たとえば、特定の **show** コマンドを設定するだけで、すべての **show** コマンドが許可されます。CLI の使用法を示す疑問符や省略形など、コマンドの変形をすべて予想する必要がなくなるので、この方法を使用することをお勧めします（図 18-1 を参照）。

図 18-1　　関連するすべてのコマンドの許可



- **enable** や **help** など、単一ワードのコマンドについては、そのコマンドに引数がない場合でも、一致しない引数を許可する*必要があります*（図 18-2 を参照）。

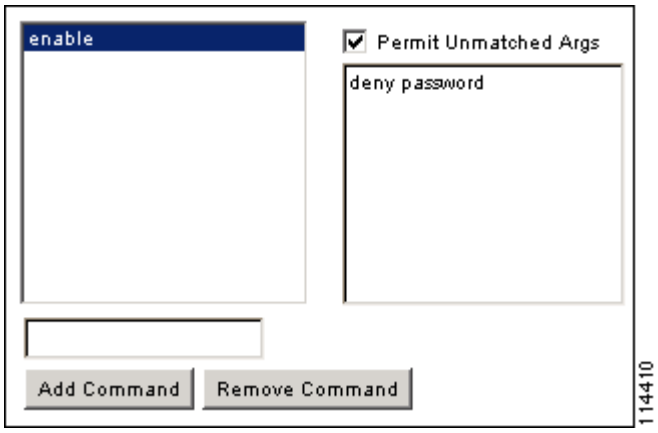
図 18-2　単一ワードのコマンドの許可



- 引数を拒否するには、その引数の前に **deny** を入力します。

  たとえば、**enable** コマンドを許可し、**enable password** コマンドを許可しない場合には、コマンド フィールドに **enable** を入力し、引数フィールドに **deny password** を入力します。**enable** だけが許可されるように、必ず、[Permit Unmatched Args] チェックボックスをオンにしてください（図 18-3 を参照）。

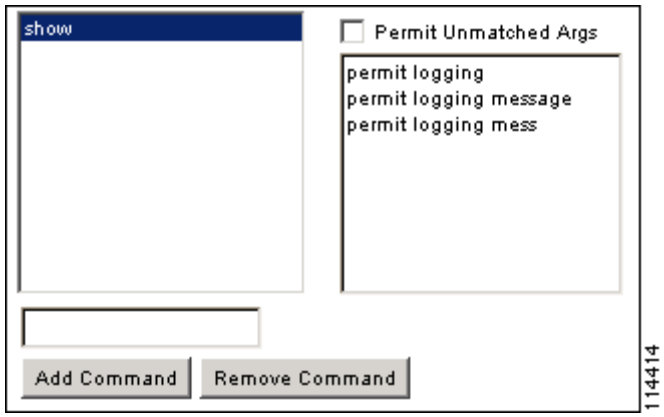
図 18-3　引数の拒否



- コマンドラインでコマンドを省略形で入力した場合、ASA 1000V はプレフィックスとメイン コマンドを完全なテキストに展開しますが、その他の引数は入力したとおりに TACACS+ サーバに送信します。

  たとえば、**sh log** と入力すると、ASA 1000V は完全なコマンド **show logging** を TACACS+ サーバに送信します。一方、**sh log mess** と入力すると、ASA 1000V は展開されたコマンド **show logging message** ではなく、**show logging mess** を TACACS+ サーバに送信します。省略形を予想して同じ引数に複数のスペルを設定できます（図 18-4 を参照）。

図 18-4　省略形の指定



- すべてのユーザに対して次の基本コマンドを許可することをお勧めします。
  - **show checksum**
  - **show curpriv**
  - **enable**
  - **help**
  - **show history**
  - **login**
  - **logout**
  - **pager**
  - **show pager**
  - **clear pager**
  - **quit**
  - **show version**

TACACS+ コマンド許可の設定

TACACS+ コマンド許可をイネーブルにし、ユーザが CLI でコマンドを入力すると、ASA 1000V はそのコマンドとユーザ名を TACACS+ サーバに送信し、コマンドが認可されているかどうかを判別します。

TACACS+ コマンド許可をイネーブルにする前に、TACACS+ サーバで定義されたユーザとして ASA 1000V にログインしていること、および ASA 1000V の設定を続けるために必要なコマンド許可があることを確認してください。たとえば、すべてのコマンドが認可された管理ユーザとしてログインする必要があります。このようにしないと、意図せずロックアウトされる可能性があります。

意図したとおりに機能することが確認できるまで、設定を保存しないでください。間違いによりロックアウトされた場合、通常は ASA 1000V を再起動することによってアクセスを回復できます。それでもロックアウトされたままの場合は、「ロックアウトからの回復」（P.18-33）を参照してください。

TACACS+ システムが完全に安定して信頼できることを確認します。必要な信頼性レベルについて、通常は、完全冗長 TACACS+ サーバ システムと ASA 1000V への完全冗長接続が必要です。たとえば、TACACS+ サーバ プールに、インターフェイス 1 に接続された 1 つのサーバとインターフェイス 2 に接続された別のサーバを含めます。TACACS+ サーバが使用できない場合にフォールバック方式としてローカル コマンド認可を設定することもできます。この場合は、「コマンド許可の設定」（P.18-24）

に示されている手順に従ってローカル ユーザとコマンド特権レベルを設定する必要があります。

TACACS+ コマンド認可を設定するには、次のコマンドを入力します。

手順の詳細

コマンド	目的
aaa authorization command *tacacs+_server_group* [**LOCAL**] **例：** hostname(config)# aaa authorization command group_1 LOCAL	TACACS+ サーバを使用してコマンド認可を実行します。 TACACS+ サーバを使用できない場合は、ローカル データベースをフォールバック方式として使用するように ASA 1000V を設定できます。フォールバックをイネーブルにするには、サーバ グループ名の後ろに **LOCAL** を指定します（**LOCAL** は大文字と小文字を区別します）。ローカル データベースでは TACACS+ サーバと同じユーザ名およびパスワードを使用することを推奨します。これは、ASA 1000V のプロンプトでは、どの方式が使用されているかが示されないためです。必ずローカル データベースのユーザ（「ユーザ アカウントのローカル データベースへの追加」（P.18-17）を参照）とコマンド特権レベル（「ローカル コマンド許可の設定」（P.18-25）を参照）を設定してください。

管理アクセス アカウンティングの設定

ユーザがログインするとき、ユーザが **enable** コマンドを入力するとき、またはユーザがコマンドを発行するときのアカウンティングを設定できます。

コマンド アカウンティングに使用できるサーバは、TACACS+ だけです。

管理アクセスおよびイネーブル コマンド アカウンティングを設定するには、次の手順を実行します。

手順の詳細

	コマンド	目的
ステップ 1	**aaa accounting** {**serial** | **telnet** | **ssh** | **enable**} **console** *server-tag* **例：** hostname(config)# aaa accounting telnet console group_1	管理アクセスに対する AAA アカウンティングのサポートをイネーブルにします。 有効なサーバ グループ プロトコルは RADIUS と TACACS+ です。
ステップ 2	**aaa accounting command** [**privilege** *level*] *server-tag* **例：** hostname(config)# aaa accounting command privilege 15 group_1	コマンド アカウンティングをイネーブルにします。TACACS+ サーバだけがコマンド アカウンティングをサポートします。 **privilege** *level* は最小特権レベルで、*server-tag* は、ASA 1000V がコマンド アカウンティング メッセージを送信する TACACS+ サーバ グループの名前です。

ロックアウトからの回復

状況によっては、コマンド許可や CLI 認証をオンにすると、ASA 1000V CLI からロックアウトされる場合があります。通常は、ASA 1000V を再起動することによってアクセスを回復できます。ただし、すでにコンフィギュレーションを保存した場合は、ロックアウトされたままになる可能性があります。表 18-3 に、一般的なロックアウト条件と回復方法を示します。

表 18-3　CLI 認証およびコマンド許可のロックアウト シナリオ

機能	ロックアウト条件	説明	回避策
ローカル CLI 認証	ローカル データベース内にユーザが存在しない。	ローカル データベース内にユーザが存在しない場合は、ログインできず、ユーザの追加もできません。	ログインし、パスワードと **aaa** コマンドをリセットします。
TACACS+ コマンド許可 TACACS+ CLI 認証 RADIUS CLI 認証	サーバがダウンしているか到達不能で、フォールバック方式を設定していない。	サーバが到達不能である場合は、ログインもコマンドの入力もできません。	1. ログインし、パスワードと AAA コマンドをリセットします。 2. サーバがダウンしたときにロックアウトされないように、ローカル データベースをフォールバック方式として設定します。
TACACS+ コマンド許可	十分な特権のないユーザまたは存在しないユーザとしてログインした。	コマンド許可がイネーブルになりますが、ユーザはこれ以上コマンドを入力できなくなります。	TACACS+ サーバのユーザ アカウントを修正します。 TACACS+ サーバへのアクセス権がなく、ASA 1000V をすぐに設定する必要がある場合は、メンテナンス パーティションにログインして、パスワードと **aaa** コマンドをリセットします。
ローカル コマンド許可	十分な特権のないユーザとしてログインしている。	コマンド許可がイネーブルになりますが、ユーザはこれ以上コマンドを入力できなくなります。	ログインし、パスワードと **aaa** コマンドをリセットします。

管理アクセス用の AAA のモニタリング

AAA サーバのモニタリング

AAA サーバをモニタするには、次のいずれかのコマンドを入力します。

コマンド	目的
`show aaa-server`	設定済みの AAA サーバの統計情報を表示します。 AAA サーバ コンフィギュレーションをクリアするには、**clear aaa-server statistics** コマンドを入力します。

show running-config aaa-server	AAA サーバ実行コンフィギュレーションを表示します。 AAA サーバの統計情報をクリアするには、**clear configure aaa-server** コマンドを入力します。
show running-config all ldap attribute-map	実行コンフィギュレーションのすべての LDAP 属性を表示します。 実行コンフィギュレーションのすべての LDAP 属性をクリアするには、**clear configuration ldap attribute-map** コマンドを使用します。
show running-config zonelabs-integrity	Zone Labs Integrity サーバ コンフィギュレーションを表示します。 Zone Labs Integrity サーバ コンフィギュレーションをクリアするには、**clear configure zonelabs-integrity** コマンドを使用します。
show ad-groups *name* [**filter** *string*]	LDAP を使用する AD サーバだけに適用し、AD サーバに登録されているグループを表示します。

現在のログイン ユーザの表示

現在のログイン ユーザを表示するには、次のコマンドを入力します。

```
hostname# show curpriv
```

次に、**show curpriv** コマンドの出力例を示します。

```
hostname# show curpriv
Username: admin
Current privilege level: 15
Current Mode/s: P_PRIV
```

表 18-4 に、**show curpriv** コマンドの出力の説明を示します。

表 18-4　show curpriv コマンド出力の説明

フィールド	説明
Username	ユーザ名。デフォルト ユーザとしてログインすると、名前は enable_1（ユーザ EXEC モード）または enable_15（特権 EXEC モード）になります。
Current privilege level	レベルの範囲は 0 ～ 15 です。ローカル コマンド許可を設定してコマンドを中間特権レベルに割り当てない限り、使用されるレベルはレベル 0 と 15 だけです。
Current Modes	使用可能なアクセス モードは次のとおりです。 • P_UNPR：ユーザ EXEC モード（レベル 0 と 1） • P_PRIV：特権 EXEC モード（レベル 2 ～ 15） • P_CONF：コンフィギュレーション モード

その他の参考資料

LDAP マッピングの実装に関するその他の情報については、次の項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』*

管理者アクセス用の AAA の機能履歴

表 18-5 に機能履歴を示します。

表 18-5　管理者アクセス用の AAA の機能履歴

機能名	プラットフォーム リリース	機能情報
管理アクセス用の AAA	8.7(1)	IETF RADIUS Service-Type 5（発信）属性を使用する RADIUS または LDAP（マッピング済み）ユーザの場合、リモート アクセス（SSL）ユーザはサポートされません。