CHAPTER 33

ダイナミック アクセス ポリシーの設定

次の項では、ダイナミック アクセス ポリシーについての情報を提供します。

VPN 環境でのアクセス ポリシーについて

VPN ゲートウェイは動的な環境で動作します。個々の VPN 接続には、頻繁に変更されるイントラネット設定、組織内の各ユーザが持つさまざまなロール、および設定とセキュリティ レベルが異なるリモート アクセス サイトからのログインなど、複数の変数が影響する可能性があります。VPN 環境でのユーザ許可のタスクは、スタティックな設定のネットワークでの許可タスクよりもかなり複雑です。

セキュリティ アプライアンスでのダイナミック アクセス ポリシー（DAP）により、これらの多くの変数に対処する許可機能を設定できます。ダイナミック アクセス ポリシーは、特定のユーザ トンネルまたはユーザ セッションに関連付ける一連のアクセス コントロール属性を設定して作成します。これらの属性により、複数のグループ メンバーシップやエンドポイント セキュリティの問題に対処します。つまり、セキュリティ アプライアンスでは、定義したポリシーに基づき、特定のユーザに対して、特定のセッションのアクセスが許可されます。セキュリティ アプライアンスは、ユーザが接続するときに、1 つまたは複数の DAP レコードから属性を選択または集約して、DAP を生成します。DAP レコードは、リモート デバイスのエンドポイント セキュリティ情報および認証されたユーザの AAA 許可情報に基づいて選択されます。選択された DAP レコードは、ユーザ トンネルまたはセッションに適用されます。

DAP システムには、注意を必要とする次のコンポーネントがあります。

- DAP 選択コンフィギュレーション ファイル：セッション確立中に DAP レコードを選択および適用するためにセキュリティ アプライアンスが使用する、基準が記述されたテキスト ファイル。セキュリティ アプライアンスに保存されています。ASDM を使用して、このファイルを変更したり、XML データ形式でセキュリティ アプライアンスにアップロードしたりできます。DAP 選択設定ファイルには、ユーザが設定するすべての属性が記載されています。たとえば、AAA 属性、エンドポイント属性、ネットワーク ACL と Web-type ACL のフィルタで設定されるアクセス ポリシー、ポート転送リスト、および URL リストなどがあります。
- DfltAccess ポリシー：常に DAP サマリー テーブルの最後のエントリで、プライオリティは必ず 0。デフォルト アクセス ポリシーのアクセス ポリシー属性を設定できますが、AAA 属性またはエンドポイント属性は含まれておらず、これらの属性は設定できません。DfltAccessPolicy は削除できません。また、サマリー テーブルの最後のエントリになっている必要があります。

ダイナミック アクセス ポリシーの詳細については、次のリンクをクリックしてください。

- リモート アクセス接続タイプに対する DAP サポート
- DAP と AAA
- DAP とエンドポイント セキュリティ

- DAP 接続シーケンス
- Tesy Dynamic Access Policies
- DAP の例

ダイナミック アクセス ポリシーの設定

ダイナミック アクセス ポリシーを設定するには、ASDM の [Configuration] > [Remote Access VPN] > [Network (Client) Access] *または* [Clientless SSL VPN Access] > [Dynamic Access Policies] ペインで、次の手順を実行します。

ステップ 1　特定のアンチウイルス、アンチスパイウェア、またはパーソナル ファイアウォールのエンドポイント属性を含めるには、ペインの最上部近くの [*CSD configuration*] リンクをクリックします。次に、Cisco Secure Desktop *および*ホスト スキャンの拡張機能をイネーブルにします。このリンクは、これら両方の機能をすでにイネーブルにしている場合には表示されません。

Cisco Secure Desktop 拡張機能をイネーブルにして Host Scan 拡張機能はイネーブルにしない場合、変更を適用すると、ASDM は Host Scan コンフィギュレーションをイネーブルにするリンクを表示します。

ステップ 2　新しいダイナミック アクセス ポリシーを作成するには、[Add] をクリックします。既存のポリシーを変更するには、[Edit] をクリックします。

ステップ 3　すでに設定済みのポリシーをテストするには、[Test Dynamic Access Policies] ボタンをクリックします。

フィールド

- [Priority]：DAP レコードのプライオリティを表示します。セキュリティ アプライアンスは、複数の DAP レコードからネットワーク ACL と Web-type ACL を集約するときに、この値を使用してアクセス リストを論理的に順序付けします。セキュリティ アプライアンスは、最上位のプライオリティ番号から最下位のプライオリティ番号の順にレコードを並べ、最下位のプライオリティをテーブルの一番下に配置します。番号が大きいほどプライオリティが高いことを意味します。たとえば、値が 4 の DAP レコードは値が 2 のレコードよりも高いプライオリティを持つことになります。プライオリティは、手動での並べ替えはできません。
- [Name]：DAP レコードの名前を表示します。
- [Network ACL List]：セッションに適用されるファイアウォール アクセス リストの名前を表示します。
- [Web-Type ACL List]：セッションに適用される SSL VPN アクセス リストの名前を表示します。
- [Description]：DAP レコードの目的を説明します。
- [Test Dynamic Access Policies] ボタン：設定済みの DAP レコードをテストします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	—

リモート アクセス接続タイプに対する DAP サポート

DAP システムは、次のリモート アクセス方式をサポートします。

- IPsec VPN
- クライアントレス（ブラウザベース）SSL VPN
- Cisco AnyConnect SSL VPN
- PIX カットスルー プロキシ（ポスチャ評価は使用不可）

DAP と AAA

DAP は AAA サービスを補完します。用意されている許可属性のセットはかぎられていますが、それらの属性によって AAA で提供される許可属性を無効にできます。セキュリティ アプライアンスは、ユーザの AAA 許可情報とセッションのポスチャ評価情報に基づいて DAP レコードを選択します。セキュリティ アプライアンスは、この情報に基づいて複数の DAP レコードを選択でき、それらのレコードを集約して DAP 許可属性を作成します。

AAA 属性は、Cisco AAA 属性階層から、またはセキュリティ アプライアンスが RADIUS または LDAP サーバから受信する一式の応答属性セットから指定できます。

AAA 属性の定義

表 33-1 に、DAP で使用できる AAA 選択属性名の定義を示します。属性名フィールドは、LUA 論理式での各属性名の入力方法を示しており、[Add/Edit Dynamic Access Policy] ペインの [Advanced] セクションで使用します。

表 33-1　AAA 選択属性名

属性タイプ	属性名	ソース	値	ストリングの最大長	説明
シスコ	aaa.cisco.memberof	AAA	文字列	128	memberof の値
	aaa.cisco.username	AAA	文字列	64	ユーザ名の値
	aaa.cisco.class	AAA	文字列	64	クラス属性値
	aaa.cisco.ipaddress	AAA	番号	-	framed-ip アドレスの値
	aaa.cisco.tunnelgroup	AAA	文字列	64	トンネル グループ名
LDAP	aaa.ldap.<label>	LDAP	文字列	128	LDAP 属性値ペア
RADIUS	aaa.radius.<number>	RADIUS	文字列	128	RADIUS 属性値ペア

DAP とエンドポイント セキュリティ

セキュリティ アプライアンスは、設定するポスチャ評価方式を使用してエンドポイント セキュリティの属性を取得します。これには、Cisco Secure Desktop および NAC が含まれます。詳細については、「ASDM」の「Cisco Secure Desktop」セクションを参照してください。表 33-2 に、DAP がサポートしている各リモート アクセス プロトコル、その方式で使用可能なポスチャ評価ツール、およびそのツールによって提供される情報を示します。

表 33-2　DAP ポスチャ評価

リモート アクセス プロトコル	Cisco Secure Desktop	ホスト スキャン	NAC	Cisco NAC アプライアンス
	ファイル情報、レジストリ キーの値、実行プロセス、オペレーティング システムを返す	アンチウイルス、アンチスパイウェア、およびパーソナル ファイアウォール ソフトウェアの情報を返す	NAC ステータスを返す	VLAN タイプと VLAN ID を返す
IPsec VPN	No	No	Yes	Yes
Cisco AnyConnect VPN	Yes	Yes	Yes	Yes
Clientless VPN	Yes	Yes	No	No
PIX Cut-through Proxy	No	No	No	No

エンドポイント属性の定義

表 33-3 に DAP で使用可能なエンドポイント選択属性名の定義を示します。属性名フィールドは、LUA 論理式での各属性名の入力方法を示しており、[Add/Edit Dynamic Access Policy] ペインの [Advanced] エリアで使用します。*label* 変数は、アプリケーション、ファイル名、プロセス、またはレジストリ エントリを示します。

表 33-3　エンドポイント属性の定義

属性タイプ	属性名	ソース	値	ストリングの最大長	説明
アンチスパイウェア（Cisco Secure Desktop が必要）	endpoint.as.*label*.exists	ホスト スキャン	true	—	アンチスパイウェア プログラムが存在する
	endpoint.as.*label*.version		文字列	32	バージョン
	endpoint.as.*label*.description		文字列	128	アンチスパイウェアの説明
	endpoint.as.*label*.lastupdate		整数	—	アンチスパイウェア定義を更新してからの経過時間（秒）
ウイルス対策（Cisco Secure Desktop が必要）	endpoint.av.*label*.exists	ホスト スキャン	true	—	アンチウイルス プログラムが存在する
	endpoint.av.*label*.version		文字列	32	バージョン
	endpoint.av.*label*.description		文字列	128	アンチウイルスの説明
	endpoint.av.*label*.lastupdate		整数	—	アンチウイルス定義を更新してからの経過時間（秒）

表 33-3　エンドポイント属性の定義 （続き）

属性タイプ	属性名	ソース	値	ストリングの最大長	説明
アプリケーション	endpoint.application.clienttype	アプリケーション	文字列	—	クライアント タイプ： CLIENTLESS ANYCONNECT IPSEC L2TP
File	endpoint.file.*label*.exists	Secure Desktop	true	—	ファイルが存在する
	endpoint.file.*label*.lastmodified		整数	—	ファイルが最後に変更されてからの経過時間（秒）
	endpoint.file.*label*.crc.32		整数	—	ファイルの CRC32 ハッシュ
NAC	endpoint.nac.status	NAC	文字列	—	ユーザ定義ステータス ストリング
オペレーティング システム	endpoint.os.version	Secure Desktop	文字列	32	オペレーティング システム
	endpoint.os.servicepack		整数	—	Windows のサービス パック
Personal Firewall （Secure Desktop が必要）	endpoint.fw.*label*.exists	ホスト スキャン	true	—	パーソナル ファイアウォールが存在する
	endpoint.fw.*label*.version		文字列	32	バージョン
	endpoint.fw.*label*.description		文字列	128	パーソナル ファイアウォールの説明
Policy	endpoint.policy.location	Secure Desktop	文字列	64	Cisco Secure Desktop からのロケーション値
プロセス	endpoint.process.*label*.exists	Secure Desktop	true	—	プロセスが存在する
	endpoint.process.*label*.path		文字列	255	プロセスのフル パス
Registry	endpoint.registry.*label*.type	Secure Desktop	*dword* *文字列*	—	dword
	endpoint.registry.*label*.value		文字列	255	レジストリ エントリの値
VLAN	endoint.vlan.type	CNA	文字列	—	VLAN タイプ： ACCESS AUTH ERROR GUEST QUARANTINE ERROR STATIC TIMEOUT

DAP とアンチウイルス、アンチスパイウェア、およびパーソナル ファイアウォール プログラム

セキュリティ アプライアンスは、ユーザ属性が、設定済みの AAA 属性およびエンドポイント属性に一致する場合に DAP ポリシーを使用します。Cisco Secure Desktop のプリログイン評価モジュールおよびホスト スキャン モジュールは、設定済みエンドポイント属性の情報をセキュリティ アプライアンスに返し、DAP サブシステムでは、その情報に基づいてそれらの属性値に一致する DAP レコードを選択します。

すべてではありませんが、ほとんどのアンチウイルス、アンチスパイウェア、およびパーソナル ファイアウォールのプログラムは、アクティブ スキャンをサポートしています。つまり、それらのプログラムはメモリ常駐型であり、常に動作しています。ホスト スキャンは、エンドポイントにプログラムがインストールされているかどうか、およびそのプログラムがメモリ常駐型かどうかを、次のようにしてチェックします。

- インストールされているプログラムがアクティブ スキャンをサポートしない場合、ホスト スキャンはそのソフトウェアの存在をレポートします。DAP システムは、そのプログラムを指定する DAP レコードを選択します。
- インストールされているプログラムがアクティブ スキャンをサポートしており、そのプログラムでアクティブ スキャンがイネーブルになっている場合、ホスト スキャンはそのソフトウェアの存在をレポートします。この場合も、セキュリティ アプライアンスは、そのプログラムを指定する DAP レコードを選択します。
- インストールされているプログラムがアクティブ スキャンをサポートしており、そのプログラムでアクティブ スキャンがディセーブルになっている場合、ホスト スキャンはそのソフトウェアの存在を無視します。セキュリティ アプライアンスは、そのプログラムを指定する DAP レコードを選択しません。さらに、そのプログラムがインストールされているとしても、DAP についての情報が多く含まれる **debug trace** コマンドの出力にはプログラムの存在が示されません。

DAP 接続シーケンス

次のシーケンスに、標準的なリモート アクセス接続を確立する場合の概要を示します。

1. リモート クライアントが VPN 接続を試みます。
2. セキュリティ アプライアンスは、設定された NAC 値と Cisco Secure Desktop の Host Scan 値を使用してポスチャ評価を実行します。
3. セキュリティ アプライアンスが、AAA を介してユーザを認証します。AAA サーバは、ユーザの許可属性も返します。
4. セキュリティ アプライアンスが、AAA 許可属性をそのセッションに適用し、VPN トンネルを確立します。
5. セキュリティ アプライアンスが、AAA 許可情報とセッションのポスチャ評価情報に基づいて DAP レコードを選択します。
6. セキュリティ アプライアンスが、選択した DAP レコードから DAP 属性を集約します。集約された属性が DAP ポリシーを構成します。
7. セキュリティ アプライアンスがその DAP ポリシーをセッションに適用します。

Tesy Dynamic Access Policies

このペインでは、許可属性値のペアを指定することによって、デバイスで設定される DAP レコードセットが取得されるかどうかをテストできます。属性値のペアを指定するには、[AAA Attribute] テーブルと [Endpoint Attribute] テーブルに関連づけられた [Add/Edit] ボタンを使用します。[Add/Edit] ボタンをクリックすると表示されるダイアログは、[Add/Edit AAA Attributes] ウィンドウと [Add/Edit Endpoint Attributes] ウィンドウに表示されるダイアログに似ています。

属性値のペアを入力して [Test] ボタンをクリックすると、デバイス上の DAP サブシステムはこれらの値を参照して、各レコードの AAA およびエンドポイント選択属性を評価します。結果は、[Test Results] テキスト領域に表示されます。

フィールド

- [Selection Criteria]：ダイナミック アクセス ポリシーを取得するときにテストする AAA 属性とエンドポイント属性を決定します。
- AAA 属性
  - [AAA Attribute]：AAA 属性を特定します。
  - [Operation Value]：属性を指定された値に対して =/!= として指定します。
  - [Add/Edit]：AAA 属性を追加または編集します。
- [Endpoint Attributes]：エンドポイント属性を特定します。
  - [Endpoint ID]：エンドポイント属性 ID を入力します。
  - [Name/Operation/Value]：
  - [Add/Edit/Delete]：エンドポイント属性を追加、編集、または削除します。
- [Test Result]：テスト結果を表示します。
- [Test]：設定したポリシーが取得されることをテストします。
- [Close]：ペインを閉じます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	—

ダイナミック アクセス ポリシーの追加および編集

ダイナミック アクセス ポリシーを追加または編集するには、次の手順を実行します。

ステップ 1　[Add/Edit Dynamic Access Policy] ペインの上部で、このダイナミック アクセス ポリシーの名前（必須）と説明（任意）を入力します。

ステップ 2　[Priority] フィールドで、そのダイナミック アクセス ポリシーのプライオリティを設定します。セキュリティ アプライアンスは、ここで設定される順序に従ってアクセス ポリシーを適用します。最も大きな番号のプライオリティが最上位のプライオリティです。プライオリティの設定が同じで ACL ルールが競合する DAP レコードの場合は、最も制約の多いルールが適用されます。

ステップ 3　[Add/Edit AAA Attributes] フィールドの [ANY/ALL/NONE] ドロップダウン ボックス（ラベルなし）を使用して、このダイナミック アクセス ポリシーを使用するために、ユーザは設定する AAA 属性値のいずれかまたはすべてを必要とするのか、または一切不要なのかを選択します。

ステップ 4　AAA 属性を設定するには、[AAA Attributes] フィールドの [Add/Edit] をクリックします。

ステップ 5　エンドポイント属性を設定する前に、CSD Host Scan を設定します。

ステップ 6　エンドポイント セキュリティ属性を設定するには、[Endpoint ID] フィールドの [Add/Edit] をクリックします。

ステップ 7　各タイプのエンドポイント属性のインスタンスを複数作成できます。これらのタイプごとに、ユーザがあるタイプのインスタンスのすべてを持つように DAP ポリシーで要求する（Match all = AND）のか、またはそれらのインスタンスを 1 つだけ持つように要求する（Match Any = OR）のかを決定する必要があります。エンドポイント属性のそれぞれに対してこの値を設定するには、[Logical Op.] ボタンをクリックします。

ステップ 8　[Advanced] フィールドには、上の [AAA] 領域および [Endpoint] 領域で入力可能な属性以外の AAA またはエンドポイントの属性を設定する論理式を 1 つ以上入力できます。

ステップ 9　ネットワーク /Web-type ACL、ファイル ブラウジング、ファイル サーバ入力、HTTP プロキシ、URL 入力、ポート転送リスト、および URL リストを設定するには、[Access Policy Attributes] の各フィールドで値を設定します。

フィールド

- [Policy Name] : 4 ～ 32 文字の文字列。スペースは使用できません。
- [Description] :（任意）DAP レコードの目的を説明します。最大 80 文字です。
- [Priority] : DAP のプライオリティを設定します。セキュリティ アプライアンスは、ここで設定した順序でアクセス ポリシーを適用します。数が大きいほどプライオリティは高くなります。有効値の範囲は 0 ～ 2147483647 です。デフォルト = 0。
- [ANY/ALL/NONE] ドロップダウン ボックス : ユーザ許可属性が、設定する AAA 属性の値のいずれかまたはすべてに一致するか、あるいはいずれの値にも一致せず、同時にすべてのエンドポイント属性を満たすように要求する場合に設定します。重複するエントリは許可されません。AAA またはエンドポイント属性なしの DAP レコードを設定すると、セキュリティ アプライアンスは常にそのレコードを選択します。これは、そのレコードがすべての選択基準を満たすことになるからです。
- [AAA Attributes] : 設定された AAA 属性を表示します。
  - [Attribute] : AAA 属性の名前を表示します。
  - [Operation/Value] : =/!=
  - [Add/Edit/Delete] : 選択した AAA 属性を追加、編集、または削除する場合にクリックします。
- [Endpoint Attributes] : 設定されたエンドポイント属性を表示します。
  - [Endpoint ID] : エンドポイント属性を識別します。
  - [Name/Operation/Value] : エンドポイント属性ごとに設定されている値の概要を表示します。
  - [Add/Edit/Delete] : 選択したエンドポイント属性を追加、編集、または削除します。

（注） Cisco Secure Desktop により、Application と NAC 以外のすべてのエンドポイント属性をセキュリティ アプライアンスに対して指定できます。他のすべてのエンドポイント属性を設定するには、まず Cisco Secure Desktop をイネーブルにし、そこで関連するエンドポイント属性も設定する必要があります。

  - [Logical Op.] : それぞれのタイプのエンドポイント属性のインスタンスを複数作成できます。ユーザがあるタイプのインスタンスのすべてを持つように DAP ポリシーで要求する（Match all = AND）のか、またはそれらのインスタンスを 1 つだけ持つように要求する（Match Any = OR）のかを設定します。たとえば OS などの一部のエンドポイント属性では、ユーザが属性のインスタンスを複数持つことはありません。

- [Advanced]：ダイナミック アクセス ポリシーの追加属性を設定します。これは、LUA についての知識が要求される高度な機能です。
- [AND/OR]：基本的な選択ルールと、ここで入力する論理式との関係を定義します。つまり、すでに設定されている AAA 属性およびエンドポイント属性に新しい属性を追加するのか、またはそれら設定済みの属性に置き換えるのかを指定します。デフォルトの設定は AND です。
- [Logical Expressions]：それぞれのタイプのエンドポイント属性のインスタンスを複数設定できます。新しい AAA 選択属性またはエンドポイント選択属性（あるいはその両方）を定義するフリー形式の LUA テキストを入力します。ASDM は、ここで入力されるテキストの検証を行わず、単にこのテキストを DAP XML ファイルにコピーします。セキュリティ アプライアンスがそれを処理し、解析不能な式があれば破棄します。
- [Guide]：これらの論理演算の作成に関するオンライン ヘルプを表示します。

- [Access Policy Attributes]：これらのタブにより、ネットワーク ACL と Web-type ACL のフィルタ、ファイル アクセス、HTTP プロキシ、URL エントリとリスト、ポート転送、およびクライアントレス SSL VPN アクセス方式の属性を設定できます。ここで設定する属性値は、既存のユーザ、グループ、トンネル グループ、およびデフォルトのグループ レコードを含め、AAA システムの許可値を上書きします。
- [Action] タブ
  - [Action]：特定の接続またはセッションに適用する特殊な処理を指定します。
  - [Continue]：（デフォルト）セッションにアクセス ポリシー属性を適用します。
  - [Terminate]：セッションを終了します。
  - [User Message]：この DAP レコードが選択されるときに、ポータル ページに表示するテキスト メッセージを入力します。最大 128 文字を入力できます。ユーザ メッセージは、黄色のオーブとして表示されます。ユーザがログインすると、メッセージは 3 回点滅してから静止します。数件の DAP レコードが選択され、それぞれにユーザ メッセージがある場合は、ユーザ メッセージがすべて表示されます。

（注）　このようなメッセージには、URL やその他の埋め込みテキストを含めることができます。この場合は、正しい HTML タグを使用する必要があります。

例：すべてのコントラクタは、ご使用のアンチウイルス ソフトウェアのアップグレード手順について、http://wwwin.abc.com/procedure.html を参照してください。

- [Network ACL Filters] タブ：この DAP レコードに適用するネットワーク ACL を選択および設定できます。DAP の ACL には、許可ルールまたは拒否ルールを含めることができますが、両方を含めることはできません。ACL に許可ルールと拒否ルールの両方が含まれている場合、セキュリティ アプライアンスはその ACL を拒否します。
  - [Network ACL] ドロップダウン ボックス：この DAP レコードに追加する、すでに設定済みのネットワーク ACL を選択します。すべての許可ルールまたはすべての拒否ルールを含む ACL だけが適格とされ、これらの適格な ACL だけがここに表示されます。
  - [Manage...]：ネットワーク ACL を追加、編集、および削除するときにクリックします。
  - [Network ACL] リスト：この DAP レコードのネットワーク ACL が表示されます。
  - [Add]：ドロップダウン ボックスから選択したネットワーク ACL を右側の [Network ACLs] リストに追加します。
  - [Delete]：クリックすると、強調表示されているネットワーク ACL が [Network ACLs] リストから削除されます。セキュリティ アプライアンスから ACL を削除するには、まず DAP レコードからその ACL を削除する必要があります。

- [Web-Type ACL Filters] タブ：この DAP レコードに適用する Web-type ACL を選択および設定できます。DAP の ACL には、許可または拒否ルールだけを含めることができます。ACL に許可ルールと拒否ルールの両方が含まれている場合、セキュリティ アプライアンスはその ACL を拒否します。
  - [Web-Type ACL] ドロップダウン ボックス：この DAP レコードに追加する、設定済みの Web-type ACL を選択します。すべての許可ルールまたはすべての拒否ルールを含む ACL だけが適格とされ、これらの適格な ACL だけがここに表示されます。
  - [Manage...] : Web-type ACL を追加、編集、および削除するときにクリックします。
  - [Web-Type ACL] リスト：この DAP レコードの Web-type ACL が表示されます。
  - [Add] : ドロップダウン ボックスから選択した Web-type ACL を右側の [Web-Type ACLs] リストに追加します。
  - [Delete] : クリックすると、Web-type ACL の 1 つが [Web-Type ACLs] リストから削除されます。セキュリティ アプライアンスから ACL を削除するには、まず DAP レコードからその ACL を削除する必要があります。
- [Functions] タブ : DAP レコードのファイル サーバ入力とブラウジング、HTTP プロキシ、および URL 入力を設定できます。
  - [File Server Browsing] : ファイル サーバまたは共有機能の CIFS ブラウジングをイネーブルまたはディセーブルにします。

    （注） ブラウズには、NBNS（マスター ブラウザまたは WINS）が必要です。NBNS に障害が発生した場合や、NBNS が設定されていない場合は、DNS を使用します。

    （注） CIFS ブラウズ機能では、国際化がサポートされていません。

  - [File Server Entry] : ポータル ページでユーザがファイル サーバのパスおよび名前を入力できるようにするかどうかを設定します。イネーブルになっている場合、ポータル ページにファイル サーバ エントリのドロワが配置されます。ユーザは、Windows ファイルへのパス名を直接入力できます。ユーザは、ファイルをダウンロード、編集、削除、名前変更、および移動できます。また、ファイルおよびフォルダを追加することもできます。適用可能な Windows サーバでユーザ アクセスに対して共有を設定する必要もあります。ネットワークの要件によっては、ユーザがファイルへのアクセス前に認証を受ける必要があることもあります。
  - [HTTP Proxy] : クライアントへの HTTP アプレット プロキシの転送に関与します。このプロキシは、適切なコンテンツ変換に干渉するテクノロジー（Java、ActiveX、Flash など）に対して有用です。このプロキシによって、セキュリティ アプライアンスの使用を継続しながら、マングリングを回避できます。転送されたプロキシは、自動的にブラウザの古いプロキシ コンフィギュレーションを変更して、すべての HTTP および HTTPS 要求を新しいプロキシ コンフィギュレーションにリダイレクトします。HTTP アプレット プロキシでは、HTML、CSS、JavaScript、VBScript、ActiveX、Java など、ほとんどすべてのクライアント側テクノロジーがサポートされています。サポートされているブラウザは、Microsoft Internet Explorer だけです。
  - [URL Entry] : ポータル ページでユーザが HTTP/HTTPS URL を入力できるようにするかどうかを設定します。この機能がイネーブルになっている場合、ユーザは URL エントリ ボックスに Web アドレスを入力できます。また、クライアントレス SSL VPN を使用して、これらの Web サイトにアクセスできます。

SSL VPN を使用しても、すべてのサイトとの通信が必ずしもセキュアになるとはかぎりません。SSL VPN は、リモート ユーザの PC またはワークステーションと、企業ネットワークのセキュリティ アプライアンスの間におけるデータ送信のセキュリティを確保します。したがって、ユーザが HTTPS 以外の Web リソース（インターネット上や内部ネットワーク上にあるもの）にアクセスする場合、企業のセキュリティ アプライアンスから目的の Web サーバまでの通信はセキュアではありません。

クライアントレス VPN 接続では、セキュリティ アプライアンスはエンド ユーザの Web ブラウザとターゲット Web サーバとの間のプロキシとして機能します。ユーザが SSL 対応 Web サーバに接続すると、セキュリティ アプライアンスはセキュアな接続を確立し、SSL 証明書を検証します。エンド ユーザ ブラウザでは提示された証明書を受信しないため、証明書を調査して検証することはできません。SSL VPN の現在の実装では、期限切れになった証明書を提示するサイトとの通信は許可されません。また、セキュリティ アプライアンスは、信頼できる CA 証明書の検証も実行しません。このため、ユーザは、SSL 対応の Web サーバと通信する前に、そのサーバにより提示された証明書を分析することはできません。

ユーザのインターネット アクセスを制限するには、[URL Entry] フィールドで [Disable] を選択します。これにより、SSL VPN ユーザはクライアントレス VPN 接続中に Web をサーフィンできなくなります。

- [Unchanged]：（デフォルト）クリックすると、このセッションに適用されるグループ ポリシーからの値が使用されます。
- [Enable/Disable]：機能をイネーブルにするかディセーブルにするかを指定します。
- [Auto-start]：クリックすると HTTP プロキシがイネーブルになり、これらの機能に関連付けられたアプレットが DAP レコードによって自動的に起動するようになります。

- [Port Forwarding Lists] タブ：ユーザ セッションのためのポート転送リストを選択して設定できます。

  ポート転送によりグループ内のリモート ユーザは、既知の固定 TCP/IP ポートで通信するクライアント / サーバ アプリケーションにアクセスできます。リモート ユーザは、ローカル PC にインストールされたクライアント アプリケーションを使用して、そのアプリケーションをサポートするリモート サーバに安全にアクセスできます。シスコでは、Windows Terminal Services、Telnet、Secure FTP（FTP over SSH）、Perforce、Outlook Express、および Lotus Notes についてテストしています。その他の TCP ベースのアプリケーションの一部も機能すると考えられますが、シスコではテストしていません。

（注） ポート転送は、一部の SSL/TLS バージョンでは使用できません。

注意 ポート転送（アプリケーション アクセス）およびデジタル証明書をサポートする Sun Microsystems Java™ Runtime Environment（JRE）1.4+ がリモート コンピュータにインストールされていることを確認します。

- [Port Forwarding]：この DAP レコードに適用されるポート転送リストのオプションを選択します。このフィールドのその他の属性は、[Port Forwarding] を [Enable] または [Auto-start] に設定した場合にだけイネーブルになります。
- [Unchanged]：クリックすると、属性が実行コンフィギュレーションから削除されます。
- [Enable/Disable]：ポート転送をイネーブルにするかディセーブルにするかを指定します。
- [Auto-start]：クリックするとポート転送がイネーブルになり、DAP レコードのポート転送リストに関連付けられたポート転送アプレットが自動的に起動するようになります。

  - [Port Forwarding List] ドロップダウン ボックス：DAP レコードに追加する、すでに設定済みのポート転送リストを選択します。
  - [New...]：新規のポート転送リストを設定するときにクリックします。
  - [Port Forwarding Lists]（ラベルなし）：DAP レコードのポート転送リストが表示されます。
  - [Add]：ドロップダウン ボックスから選択したポート転送リストを右側のポート転送リストに追加する場合にクリックします。
  - [Delete]：クリックすると、選択されているポート転送リストがポート転送リストから削除されます。セキュリティ アプライアンスからポート転送リストを削除するには、まず DAP レコードからそのリストを削除する必要があります。
- [URL Lists] タブ：ユーザ セッションでの URL リストを選択して設定できます。
  - [Enable URL Lists]：イネーブルにします。このボックスが選択されていない場合は、接続のポータル ページに URL リストが表示されません。
  - [URL List] ドロップダウン ボックス：DAP レコードに追加する、設定済みの URL リストを選択します。
  - [Manage...]：URL リストを追加、インポート、エクスポート、および削除します。
  - [URL Lists]（ラベルなし）：DAP レコードの URL リストを表示します。
  - [Add]：ドロップダウン ボックスから選択した URL リストを右側の URL リスト ボックスに追加する場合にクリックします。
  - [Delete]：選択した URL リストを URL リスト ボックスから削除する場合にクリックします。セキュリティ アプライアンスから URL リストを削除するには、まず DAP レコードからそのリストを削除する必要があります。
- [Access Method] タブ：許可するリモート アクセスのタイプを設定できます。
  - [Unchanged]：現在のリモート アクセス方式を引き続き使用します。
  - [AnyConnect Client]：Cisco AnyConnect VPN クライアントを使用して接続します。
  - [Web-Portal]：クライアントレス VPN で接続します。
  - [Both-default-Web-Portal]：クライアントレスまたは AnyConnect クライアントを介して接続します。デフォルトはクライアントレスです。
  - [Both default AnyConnect Client]：クライアントレスまたは AnyConnect クライアントを介して接続します。デフォルトは AnyConnect です。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	—

Add/Edit AAA Attributes

DAP レコードの選択基準として AAA 属性を設定するには、[Add/Edit AAA Attributes] ダイアログ ボックスで、使用する Cisco、LDAP、または RADIUS 属性を設定します。これらの属性は、入力する値に対して「=」または「!=」のいずれかに設定できます。各 DAP レコードに設定可能な AAA 属性の数に制限はありません。AAA 属性の詳細については、「AAA 属性の定義」を参照してください。

フィールド

- [AAA Attributes Type]：ドロップダウン ボックスを使用して、Cisco、LDAP、または RADIUS 属性を選択します。
- [Cisco]：AAA 階層モデルに保存されているユーザ許可属性を参照します。DAP レコードの AAA 選択属性に、これらのユーザ許可属性の小規模なサブセットを指定できます。次の属性が含まれます。
  - [Class]：ユーザに関連付けられた AAA グループ名。最大 64 文字です。
  - [IP Address]：割り当てられている IP アドレス。
  - [Member of]：ユーザに適用するグループ ポリシー名のカンマ区切り文字列。この属性により、複数のグループ メンバーシップを指定できます。最大 128 文字を入力できます。
  - [Tunnel Group]：接続名。最大 64 文字です。
  - [Username]：認証されたユーザのユーザ名。最大 64 文字です。
  - [=/!=]：と等しい / と等しくない
- [LDAP]：LDAP クライアントは、ユーザの AAA セッションに関連付けられたデータベースにあるすべてのネイティブ LDAP 応答属性値のペアを保存します。LDAP クライアントでは、受信した順に応答属性をデータベースに書き込みます。その名前の後続の属性はすべて破棄されます。ユーザ レコードとグループ レコードの両方が LDAP サーバから読み込まれると、このシナリオが発生する場合があります。ユーザ レコード属性が最初に読み込まれ、グループ レコード属性よりも常に優先されます。

  Active Directory グループ メンバーシップをサポートするために、AAA LDAP クライアントでは、LDAP memberOf 応答属性に対する特別な処理が行われます。AD memberOf 属性は、AD 内のグループ レコードの DN 文字列を指定します。グループの名前は、DN 文字列内の最初の CN 値です。LDAP クライアントでは、DN 文字列からグループ名を抽出して、AAA memberOf 属性として格納し、応答属性データベースに LDAP memberOf 属性として格納します。LDAP 応答メッセージ内に追加の memberOf 属性が存在する場合、それらの属性からグループ名が抽出され、前の AAA memberOf 属性と結合されて、グループ名がカンマで区切られた文字列が生成されます。この文字列は応答属性データベース内で更新されます。

  LDAP 属性は、DAP レコード内の属性名と属性値のペアで構成されています。
- [RADIUS]：RADIUS クライアントは、ユーザの AAA セッションに関連付けられたデータベースにあるすべてのネイティブ RADIUS 応答属性値のペアを保存します。RADIUS クライアントは、受け取った順序で応答属性をデータベースに書き込みます。その名前の後続の属性はすべて破棄されます。ユーザ レコードおよびグループ レコードの両方が RADIUS サーバから読み込まれた場合、このシナリオが発生する可能性があります。ユーザ レコード属性が最初に読み込まれ、グループ レコード属性よりも常に優先されます。

  RADIUS 属性は、DAP レコード内の属性番号と属性値のペアで構成されています。
- LDAP および RADIUS 属性には、次の値があります。
  - [Attribute ID]：属性の名前 / 番号。最大 64 文字です。
  - [Value]：
  - [=/!=]：と等しい / と等しくない

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	—

エンドポイント属性の追加および編集

エンドポイント属性には、エンドポイント システム環境、ポスチャ評価結果、およびアプリケーションに関する情報が含まれています。セキュリティ アプライアンスは、セッション中にエンドポイント属性の集合体を動的に生成し、それらの属性をセッションに関連付けられたデータベースに保存します。各 DAP レコードに設定可能なエンドポイント属性の数に制限はありません。

各 DAP レコードには、セキュリティ アプライアンスが DAP レコードを選択するために満たす必要があるエンドポイント選択属性が指定されます。セキュリティ アプライアンスは、設定されたすべての条件を満たす DAP レコードだけを選択します。

エンドポイント属性の詳細については、次のリンクをクリックしてください。

- エンドポイント属性の定義

エンドポイント属性を DAP レコードの選択基準として設定するには、[Add/Edit Endpoint Attribute] ダイアログボックスでコンポーネントを設定します。これらのコンポーネントは、選択する属性のタイプに応じて異なります。

フィールド

- [Endpoint Attribute Type]：設定するエンドポイント属性をドロップダウン リストから選択します。[Antispyware]、[Antivirus]、[Application]、[File]、[NAC]、[Operating System]、[Personal Firewall]、[Process]、[Registry]、[VLAN]、および [Priority] から選択できます。

エンドポイント属性にはこれらのコンポーネントがありますが、すべての属性にすべてのコンポーネントが含まれているわけではありません。次の説明では、各コンポーネントが適用される属性を括弧で囲んで示しています。

- [Exists/Does not exist] ボタン（[Antispyware]、[Antivirus]、[Application]、[File]、[NAC]、[Operating System]、[Personal Firewall]、[Process]、[Registry]、[VLAN]、[Priority]）：適切なボタンをクリックして、選択したエンドポイント属性とそれに伴う修飾子（[Exists/Does not exist] ボタン下のフィールド）を表示するかどうかを指定します。
- [Vendor ID]（[Antispyware]、[Antivirus]、[Personal Firewall]）：アプリケーション ベンダーの ID です。
- [Vendor Description]（[Antispyware]、[Antivirus]、[Personal Firewall]）：アプリケーション ベンダーの説明をテキストで入力します。
- [Version]（[Antispyware]、[Antivirus]、[Personal Firewall]）：アプリケーションのバージョンを特定し、エンドポイント属性をそのバージョンと等しくするかどうかを指定します。
- [Last Update]（[Antispyware]、[Antivirus]、[File]）：最後の更新時からの経過日数を指定します。更新を、ここで入力した日数よりも早く（[<]）実行するか、遅く（[>]）実行するかを指定できます。

- [Client Type]（[Application]）：リモート アクセス接続のタイプを、AnyConnect、Clientless、Cut-through Proxy、IPsec、または L2TP から指定します。
- [Checksum]（File）：ファイルを選択し、[Compute Checksum] ボタンをクリックしてこの値を求めます。
- [Compute CRC32 Checksum]（File）：このカルキュレータを使用してファイルのチェックサム値を求めます。
- [Posture Status]（NAC）：ACS から受け取るポスチャ トークン文字列が含まれています。
- [OS Version]（Operating System）：Windows（複数のバージョン）、MAC、Linux、Pocket PC。
- [Service Pack]（Operating System）：オペレーティング システムのサービス パックを指定します。
- [Endpoint ID]（[File]、[Process]、[Registry]）：ファイル、プロセス、またはレジストリ エントリのエンドポイントを識別する文字列。DAP は、この ID を使用して、DAP 選択で Cisco Secure Desktop ホスト スキャン属性を照合します。この属性を設定する前に、[Host Scan] を設定する必要があります。[Host Scan] を設定した場合は設定がこのペインに表示されるため、設定を選択して、入力エラーまたは構文エラーの可能性を低減できます。
- [Path]（[Process]、[Policy]）：この属性を設定する前に Host Scan を設定します。[Host Scan] を設定した場合は設定がこのペインに表示されるため、設定を選択して、入力エラーまたは構文エラーの可能性を低減できます。
- [Value]（[Registry]）：dword または文字列。
- [Caseless]（[Registry]）：レジストリ エントリの大文字と小文字を区別しない場合に選択します。
- [VLAN ID]（[VLAN]）：1 ～ 4094 の範囲の有効な 802.1q 番号。
- [VLAN Type]（[VLAN]）：次の値を指定できます。

ACCESS	ポスチャ評価合格
STATIC	適用するポスチャ評価なし
TIMEOUT	応答がないためにポスチャ評価失格
AUTH	ポスチャ評価は依然アクティブ
GUEST	ポスチャ評価合格、ゲスト VLAN に切り替え
QUARANTINE	ポスチャ評価失格、隔離 VLAN に切り替え
ERROR	重大エラーのためにポスチャ評価失格

- [Policy]（[Location]）：Cisco Secure Desktop Microsoft Windows のロケーション プロファイルを、大文字と小文字を区別して入力します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	—

ガイド

この項では、AAA またはエンドポイント属性の論理式の作成方法について説明します。これを行うには、LUA（www.lua.org）についての高度な知識が必要になります。

テキスト ボックスに、AAA またはエンドポイント、あるいはその両方の選択論理演算を表す自由形式の LUA テキストを入力します。ASDM は、ここで入力されるテキストを検証せず、このテキストを単に DAP ポリシー ファイルにコピーするだけです。セキュリティ アプライアンスがそれを処理し、解析不能な式があれば破棄されます。

このオプションは、上の説明にある AAA およびエンドポイントの属性領域で指定可能な基準以外の選択基準を追加する場合に有効です。たとえば、指定された条件のいずれかまたはすべてを満たす、あるいはいずれも満たさない AAA 属性を使用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。エンドポイント属性は累積され、すべて満たす必要があります。セキュリティ アプライアンスが任意のエンドポイント属性を使用できるようにするには、LUA で適切な論理式を作成し、ここでその式を入力する必要があります。

- 論理式を作成する場合の正しい名前の構文を含む AAA 選択属性のリストについては、表 33-1 を参照してください。
- 論理式を作成する場合の正しい名前の構文を含むエンドポイント選択属性のリストについては、表 33-3 を参照してください。

DAP 論理式の例

LUA で論理式を作成する場合は、次の例を参考にしてください。

- この AAA LUA 式は、「b」で始まるユーザ名に一致するかどうかをテストします。この式では、ストリング ライブラリおよび正規表現を使用しています。

```
not(string.find(aaa.cisco.username, "^b") == nil)
```

- このエンドポイント式は、CLIENTLESS または CVC クライアント タイプに一致するかどうかをテストします。

```
endpoint.application.clienttype=="CLIENTLESS" or
endpoint.application.clienttype=="CVC"
```

- このエンドポイント式は、Norton Antivirus バージョン 10.x かどうかをテストしますが、10.5.x は除外します。

```
(endpoint.av.NortonAV.version > "10" and endpoint.av.NortonAV.version < "10.5") or
endpoint.av.NortonAV.version > "10.6"
```

Operator for Endpoint Category

各タイプのエンドポイントのインスタンスを複数設定できます。このペインでは、あるタイプのインスタンスを 1 つだけ必要とする（Match Any = OR）ように、またはあるタイプのインスタンスのすべてを持つ（Match All = AND）ように、各タイプのエンドポイントを設定します。

- エンドポイント カテゴリの 1 つのインスタンスだけを設定する場合、値を設定する必要はありません。
- 一部のエンドポイント属性の場合は、複数のインスタンスを設定しても意味がありません。たとえば、複数の OS を実行するユーザがいない場合、などです。
- 各エンドポイント タイプ内に [Match Any]/[Match All] 操作を設定するとします。

この場合、セキュリティ アプライアンスは、エンドポイント属性の各タイプを評価したあと、設定されたすべてのエンドポイントで論理 AND 演算を実行します。つまり、各ユーザは、AAA 属性だけでなく、設定したエンドポイントのすべての条件を満たす必要があります。

DAP の例

次の各項に、便利なダイナミック アクセス ポリシーの例を示します。

DAP を使用したネットワーク リソースの定義

この例は、ユーザまたはグループのネットワーク リソースを定義する方法として、ダイナミック アクセス ポリシーを設定する方法を示しています。Trusted_VPN_Access という名前の DAP ポリシーは、クライアントレス VPN アクセスと AnyConnect VPN アクセスを許可します。Untrusted_VPN_Access という名前のポリシーは、クライアントレス VPN アクセスだけを許可します。表 33-4 に、これらのポリシーそれぞれのコンフィギュレーションをまとめています。

ASDM パスは、[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Dynamic Access Policies] > [Add/Edit Dynamic Access Policy] > [Endpoint] です。

表 33-4　ネットワーク リソースの簡単な DAP コンフィギュレーション

属性	Trusted_VPN_Access	Untrusted_VPN_Access
Endpoint Attribute Type Policy	信頼できる	信頼できない
Endpoint Attribute Process	ieexplore.exe	—
Advanced Endpoint Assessment	AntiVirus= McAfee Attribute	
CSD Location	信頼できる	信頼できない
LDAP memberOf	Engineering、Managers	ベンダー
ACL		Web-Type ACL
Access	**AnyConnect** ***および*** **Web Portal**	**Web Portal**

DAP を使用した WebVPN ACL の適用

DAP では、Network ACLs（IPsec および AnyConnect の場合）、Clientless SSL VPN Web-Type ACLs、URL リスト、および Functions を含め、アクセス ポリシー属性のサブセットを直接適用できます。グループ ポリシーが適用されるバナーまたはスプリット トンネル リストなどには、直接適用できません。[Add/Edit Dynamic Access Policy] ペインの [Access Policy Attributes] タブには、DAP が直接適用される属性の完全なメニューが表示されます。

Active Directory/LDAP は、ユーザ グループ ポリシー メンバーシップをユーザ エントリの「memberOf」属性として保存します。DAP は、AD グループ（memberOf）のユーザ＝セキュリティ アプライアンスが設定済み Web-Type ACL を適用する Engineering となるように定義できます。このタスクを完了するには、次の手順を実行します。

ステップ 1　[Add AAA Attributes] ペイン（[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Dynamic Access Policies] > [Add/Edit Dynamic Access Policy] > [AAA Attributes] セクション > [Add AAA Attribute]）に移動します。

ステップ 2　AAA 属性タイプとしては、ドロップダウン メニューを使用して [LDAP] を選択します。

ステップ 3　[Attribute ID] フィールドに、ここに示されるとおり「memberOf」と入力します。大文字と小文字の区別は重要です。

ステップ 4　[Value] フィールドで、ドロップダウン メニューを使用して [=] を選択し、隣のテキスト ボックスに「Engineering」と入力します。

ステップ 5　ペインの [Access Policy Attributes] 領域で、[Web-Type ACL Filters] タブをクリックします。

ステップ 6　[Web-Type ACL] ドロップダウン メニューを使用して、AD グループ（memberOf）= Engineering のユーザに適用する ACL を選択します。

CSD チェックの強制と DAP によるポリシーの適用

この例では、ユーザが 2 つの特定 AD/LDAP グループ（Engineering および Employees）と 1 つの特定 ASA トンネル グループに属することをチェックする DAP を作成します。その後、ACL をユーザに適用します。

DAP が適用される ACL により、リソースへのアクセスを制御します。それらは、セキュリティ アプライアンスのグループ ポリシーで定義されるどの ACL よりも優先されます。またセキュリティ アプライアンスは、スプリット トンネリング リスト、バナー、および DNS など、DAP で定義または制御しない要素の通常の AAA グループ ポリシー継承ルールおよび属性を適用します。

ステップ 1　[Add AAA Attributes] ペイン（[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Dynamic Access Policies] > [Add/Edit Dynamic Access Policy] > [AAA Attributes] セクション > [Add AAA Attribute]）に移動します。

ステップ 2　AAA 属性タイプとしては、ドロップダウン メニューを使用して [LDAP] を選択します。

ステップ 3　[Attribute ID] フィールドに、ここに示されるとおり「memberOf」と入力します。大文字と小文字の区別は重要です。

ステップ 4　[Value] フィールドで、ドロップダウン メニューを使用して [=] を選択し、隣のテキスト ボックスに「Engineering」と入力します。

ステップ 5　[Attribute ID] フィールドに、ここに示されるとおり「memberOf」と入力します。大文字と小文字の区別は重要です。

ステップ 6　[Value] フィールドで、ドロップダウン メニューを使用して [=] を選択し、隣のテキスト ボックスに「Employees」と入力します。

ステップ 7　AAA 属性タイプとしては、ドロップダウン メニューを使用して [Cisco] を選択します。

ステップ 8　[Tunnel] グループ ボックスをオンにし、ドロップダウン メニューを使用して [=] を選択し、隣のドロップダウン ボックスで適切なトンネル グループ（接続ポリシー）を選択します。

ステップ 9　[Access Policy Attributes] 領域の [Network ACL Filters] タブで、前のステップで定義した DAP 基準を満たすユーザに適用する ACL を選択します。