リモート アクセス VPN のダイナミック アクセス ポリシーの管理（ASA 8.0+ デバイス）

この章では、リモート アクセス ユーザを接続プロファイル（トンネル グループ）に割り当てる Dynamic Access Policy（DAP; ダイナミック アクセス ポリシー）について説明します。これらのポリシーを、ASA 8.0+ デバイスのリモート アクセス IKEv1 IPsec、ASA 8.4(x) デバイスの IKEv2 IPsec および ASA 8.0+（8.5 を除く）デバイスの SSL VPN に設定できます。

ASA および PIX 7.0+ デバイスの他のリモート アクセス ポリシーの設定については、ASA および PIX 7.0+ デバイスでのリモートアクセス VPN の管理を参照してください。

この章は次のトピックで構成されています。

- ダイナミック アクセス ポリシーについて （1 ページ）
- ダイナミック アクセス ポリシーの設定 （3 ページ）
- [Dynamic Access] ページ（ASA） （14 ページ）

ダイナミック アクセス ポリシーについて

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、組織内の各ユーザー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 環境でのユーザー認可のタスクは、スタティックな設定のネットワークでの認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 Dynamic Access Policy（DAP; ダイナミック アクセス ポリシー）を使用すると、これらの多くの変数に対処する認可を設定できます。ダイナミック アクセス ポリシーは、特定のユーザー トンネルまたはユーザー 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 アプライアンスは、定義されるポリシーに基づいて、特定のセッションの特定のユーザにアクセス権を付与します。セキュリティ アプライアンスは、ユーザーが接続するときに、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ーの AAA 認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、ユーザー 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 選択設定ファイル：セッション確立時に 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 アプライアンス上に格納されています。Security Manager を使用すると、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、ユーザーが設定するすべての属性が記載されています。これには、AAA 属性、エンドポイント属性、およびネットワーク ACL と Web タイプ ACL のフィルタ、ポート転送、URL のリストとして設定されたアクセス ポリシーなどがあります。
- 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。

ヒント　ダイナミック アクセス ポリシーは、グループ ポリシーに優先します。ダイナミック アクセス ポリシーで設定を指定していない場合、ASA デバイスは設定を指定しているグループ ポリシーがないかどうかを確認します。

Cisco Secure Desktop と DAP の統合

Cisco Secure Desktop（CSD）機能は、セキュリティ アプライアンスによってダイナミック アクセス ポリシー（DAP）に統合されます。設定に応じて、セキュリティ アプライアンスでは、DAP を割り当てる条件として、1 つ以上のエンドポイント属性値を、オプションの AAA 属性値と組み合わせて使用します。DAP のエンドポイント属性でサポートされる Cisco Secure Desktop 機能には、OS 検出、プリログイン ポリシー、基本ホスト スキャン結果、およびエンドポイント評価があります。

管理者は、セッションに DAP を割り当てるために必要な条件を構成する属性を、単独で、または組み合わせて指定できます。DAP により、エンドポイント AAA 属性値に適したレベルでネットワーク アクセスが提供されます。設定したエンドポイント基準がすべて満たされたときに、セキュリティ アプライアンスによって DAP が適用されます。

関連項目

- ダイナミック アクセス ポリシーの設定　（3 ページ）
- DAP 属性の設定　（10 ページ）

ダイナミック アクセス ポリシーの設定

ここでは、ダイナミック アクセス ポリシーを作成または編集する方法について説明します。

関連項目

- ダイナミック アクセス ポリシーについて （1 ページ）
- DAP 属性について （5 ページ）
- ASA デバイスでの Cisco Secure Desktop ポリシーの設定 （12 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ASA デバイスを選択して、ポリシーセレクタから [リモートアクセス VPN（Remote Access VPN）] > [ダイナミックアクセス（Dynamic Access）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから、[リモートアクセス VPN（Remote Access VPN）] > [ダイナミックアクセス（ASA）（Dynamic Access (ASA)）] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[Dynamic Access] ページが開きます。このページの要素の詳細については、[Dynamic Access] ページ（ASA）（14 ページ）を参照してください。

ステップ 2 [作成（Create）] をクリックするか、またはテーブル内のポリシーを選択して [編集（Edit）] をクリックします。

[Add/Edit Dynamic Access Policy] ダイアログボックスが開き、デフォルトで [Main] タブが表示されます。このダイアログボックスの要素の詳細については、[Add Dynamic Access Policy]/[Edit Dynamic Access Policy] ダイアログボックス （16 ページ）を参照してください。

ステップ 3 DAP レコードの名前を入力します（最大 128 文字）。

ステップ 4 DAP レコードのプライオリティを指定します。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。

ステップ 5 DAP レコードの説明を入力します。

ステップ 6 [メイン（Main）] タブで、DAP 属性、およびセキュリティアプライアンスの DAP システムでサポートされるリモートアクセス方式のタイプを設定します。このタブの要素の詳細については、[Main] タブ （18 ページ）を参照してください。

a) テーブルの下の [作成（Create）] をクリックするか、またはテーブル内の DAP エントリを選択して [編集（Edit）] をクリックします。[Add/Edit DAP Entry] ダイアログボックスが開きます。このダイアログボックスの要素の詳細については、[Add DAP Entry]/[Edit DAP Entry] ダイアログボックス （27 ページ）を参照してください。

DAP 属性を定義する手順の詳細については、DAP 属性の設定 （10 ページ）を参照してください。

b) DAP システムで許可されるリモート アクセスのタイプを選択します。

c) [ネットワーク ACL（Network ACL）] タブを選択し、この DAP レコードに適用するネットワーク ACL を選択および設定します。Security Manager バージョン 4.10 以降では、拡張 ACL エントリに加えて統合 ACL エントリを選択できます。

このタブは、[Web Portal] 以外のアクセス方式を選択した場合にかぎり、使用可能です。

d) [WebType ACL] タブを選択し、この DAP レコードに適用する Web タイプ ACL を選択および設定します。

このタブは、AnyConnect Client 以外のアクセス方式を選択した場合にかぎり、使用可能です。

e) [Functions] タブを選択し、ファイル サーバー エントリとブラウジング、HTTP プロキシ、および DAP レコードの URL エントリを設定します。

このタブは、AnyConnect Client 以外のアクセス方式を選択した場合にかぎり、使用可能です。

f) [ポートフォワーディング（Port Forwarding）] タブを選択し、ユーザーセッションのポート転送リストを選択および設定します。

このタブは、AnyConnect Client 以外のアクセス方式を選択した場合にかぎり、使用可能です。

Cisco Security Manager 4.24 以降、[ポートフォワーディング（Port Forwarding）] ポリシーオブジェクトは ASA 9.17(1) 以降のバージョンのデバイスに対しては廃止されています。

（注） ASA デバイスを 9.17(1) 以降のバージョンにアップグレードする場合は、展開の失敗を避けるために、ポート設定 CLI を削除する必要があります。

g) [ブックマーク（Bookmark）] タブを選択し、ユーザーセッションの URL リストを選択および設定します。

このタブは、AnyConnect Client 以外のアクセス方式を選択した場合にかぎり、使用可能です。

h) [アクション（Action）] タブを選択し、許可されるリモートアクセスのタイプを設定します。

このタブは、どのタイプのアクセス方式でも使用できます。

i) [AnyConnect] タブを選択し、AnyConnect サービスプロファイルの Always-On VPN の設定を未変更のままにするか、無効にするか、AnyConnect プロファイル設定を使用する必要があるかを選択します。Always-On VPN を使用すると、システムにログオンした後、AnyConnnect で VPN セッションを自動的に確立できます。

j) [カスタム属性（Custom Attributes）] タブを選択し、AnyConnect カスタム属性を追加します。

このタブは、アクセス方式として [変更なし（Unchanged）]、[AnyConnect クライアント（AnyConnect Client）]、[両方、デフォルトは Web ポータル（Both Default Web Portal）]、または [両方、デフォルトは Anyconnect クライアント（Both Default Anyconnect Client）] を選択した場合にのみ使用できます。AnyConnect カスタム属性を追加する方法については、[AnyConnectカスタム属性の追加/編集（Add/Edit AnyConnect Custom Attribute）] ダイアログボックスを参照してください。

ステップ 7 [論理的な操作（Logical Operations）] タブを選択し、エンドポイント属性のタイプごとに複数のインスタンスを作成します。このタブの要素の詳細については、[論理的な操作（Logical Operators）] タブ （58 ページ）を参照してください。

ステップ 8 [拡張表現（Advanced Expressions）] タブを選択し、自由形式の LUA を使用して DAP の追加属性を設定します。このタブの要素の詳細については、[Advanced Expressions] タブ （61 ページ）を参照してください。

ステップ 9 [OK] をクリックします。

DAP 属性について

DAP レコードには、ユーザが設定するすべての属性が含まれています。これには、AAA 属性、エンドポイント属性、およびネットワーク ACL と Web タイプ ACL のフィルタ、ポート転送、URL のリストとして設定されたアクセス ポリシーなどがあります。

DAP と AAA 属性

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 認可情報および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 認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 サーバまたは LDAP サーバから受信するフル セットの応答属性から指定できます。

AAA 属性の定義

次の表に、DAP で使用できる AAA 選択属性名の定義を示します。属性名欄は、LUA 論理式での各属性名の入力方法を示しており、[Add Dynamic Access Policy]/[Edit Dynamic Access Policy] ダイアログボックスの [Advanced] タブでこのように入力する場合があります。

表 *1 : AAA* 属性の定義

属性タイプ	属性名	送信元	値	ストリングの最大長	説明
シスコ	aaa.cisco.memberof	AAA	string	128	memberof の値
	aaa.cisco.username	AAA	string	64	ユーザ名の値
	aaa.cisco.class	AAA	string	64	クラス属性値
	aaa.cisco.ipaddress	AAA	number	–	framed-ip アドレスの値
	aaa.cisco.tunnelgroup	AAA	string	64	トンネル グループ名
LDAP	aaa.ldap.<label>	LDAP	string	128	LDAP 属性値ペア
RADIUS	aaa.radius.<number>	RADIUS	string	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、設定された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。プリログイン ポリシーの一致、基本ホスト スキャン エントリ、ホスト スキャン拡張機能、またはこれらの属性と他のポリシー属性の任意の組み合わせを使用して、アクセス権および制約を適用できます。最低でも、プリログイン ポリシーごと、および基本ホスト スキャン エントリごとに割り当てられるように DAP を設定します。

ホスト スキャン拡張機能であるエンドポイント評価では、アンチウイルスとアンチスパイウェアのアプリケーション、関連する定義の更新、およびファイアウォールの大規模なコレクションについて、リモート コンピュータを検査します。この機能を使用すると、セキュリティ アプライアンスによって特定の DAP がセッションに割り当てられる前に、要件を満たすようにエンドポイント基準を組み合わせることができます。

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、ユーザー属性が、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。

エンドポイント属性の定義

次の表に、DAP で使用できるエンドポイント選択属性名の定義を示します。属性名欄は、LUA 論理式での各属性名の入力方法を示しており、[Add Dynamic Access Policy]/[Edit Dynamic Access

Policy] ダイアログボックスの [Advanced] タブでこのように入力する場合があります。*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 *2:* エンドポイント属性の定義

属性タイプ	属性名	送信元	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		string	32	アンチスパイウェアの説明
	endpoint.as.label.description		string	128	クラス属性値
	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）
アンチウイルス（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		string	32	アンチウイルスの説明
	endpoint.av.label.description		string	128	クラス属性値
	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）
アプリケーション	endpoint.application.clienttype	アプリケーション	string	–	クライアント タイプ： CLIENTLESS ANYCONNECT IPSEC L2TP
ファイル（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

属性タイプ	属性名	送信元	値	ストリングの最大長	説明
NAC	endpoint.nac.status	NAC	string	-	ユーザー定義ステータス ストリング
オペレーティング システム	endpoint.os.version	Secure Desktop	string	32	Windows のサービス パック
	endpoint.os.servicepack		整数	–	オペレーティング システム
パーソナル ファイア ウォール（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		string	32	Version
	endpoint.fw.label.description		string	128	パーソナル ファイア ウォールの説明
ポリシー（Policy）	endpoint.policy.location	Secure Desktop	string	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		string	255	プロセスのフル パス
Registry	endpoint.registry.label.type	セキュアなデスクトップ	dword ストリング	–	dword
	endpoint.registry.label.value		string	255	レジストリ エントリの値
VLAN	endpoint.vlan.type	CNA	sting	–	VLAN タイプ： ACCESS AUTH ERROR GUEST QUARANTINE ERROR STATIC TIMEOUT

AAA 属性またはエンドポイント属性の高度な式について

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、ここで入力された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、解析できない式があるとその式は廃棄されます。

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、指定された基準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的で、すべてを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。

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"
```

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 アプライアンスが、設定された NAC 値と Cisco Secure Desktop のホスト スキャン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 サーバーは、ユーザーの認可属性も返します。
4. セキュリティ アプライアンスが、セッションに AAA 認可属性を適用し、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、ユーザの AAA 認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。

関連項目

- ダイナミック アクセス ポリシーの設定　（3 ページ）
- ダイナミック アクセス ポリシーについて　（1 ページ）

• DAP 属性の設定 （10 ページ）

DAP 属性の設定

DAP ポリシーに定義する属性には、認可属性とエンドポイント属性を指定する必要があります。ネットワーク ACL と Web タイプ ACL、ファイル ブラウジング、ファイル サーバ エントリ、HTTP プロキシ、URL エントリ、ポート転送リスト、および URL リストを設定することもできます。

ここでは、DAP ポリシーに必要な AAA 属性およびエンドポイント属性を作成または編集する方法について説明します。

関連項目

• DAP 属性について （5 ページ）
• ダイナミック アクセス ポリシーの設定 （3 ページ）
• ダイナミック アクセス ポリシーについて （1 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ASA デバイスを選択して、ポリシーセレクタから [リモートアクセス VPN（Remote Access VPN）] > [ダイナミックアクセス（Dynamic Access）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから、[リモートアクセス VPN（Remote Access VPN）] > [ダイナミックアクセス（ASA）（Dynamic Access (ASA)）] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[Dynamic Access] ページが開きます。このページの要素の詳細については、[Dynamic Access] ページ（ASA）（14 ページ）を参照してください。

ステップ 2 [ダイナミックアクセス（Dynamic Access）] ポリシーページで [作成（Create）] をクリックするか、またはこのページのテーブル内のポリシー行を選択して [編集（Edit）] をクリックします。

[Add/Edit Dynamic Access Policy] ダイアログボックスが開き、[Main] タブが表示されます。[Main] タブの要素の詳細については、[Main] タブ （18 ページ）を参照してください。

ステップ 3 テーブルの下の [作成（Create）] をクリックするか、またはテーブル内の DAP エントリを選択して [編集（Edit）] をクリックします。[Add/Edit DAP Entry] ダイアログボックスが開きます。このダイアログボックスの要素の詳細については、[Add DAP Entry]/[Edit DAP Entry] ダイアログボックス （27 ページ）を参照してください。

ステップ 4 [Criterion] リストから属性タイプを選択し、適切な値を入力します。ダイアログボックスの値は、選択に応じて変わります。次のオプションがあります。

- AAA 属性 Cisco（表 6 : [DAPエントリの追加（Add DAP Entry）]/[DAPエントリの編集（Edit DAP Entry）] ダイアログボックス、[AAA属性Cisco（AAA Attributes Cisco）] （31 ページ）を参照）。

- AAA 属性 LDAP（表 7 : [DAPエントリの追加（Add DAP Entry）]/[DAPエントリの編集（Edit DAP Entry）] ダイアログボックス の AAA 属性 LDAP （33 ページ）を参照）
- AAA 属性 RADIUS（表 8 : [DAPエントリの追加/編集（Add/Edit DAP Entry）] ダイアログボックスの [AAA属性RADIUS（AAA Attributes RADIUS）] （35 ページ）を参照）。
- アンチスパイウェア（表 9 : [DAPエントリの追加/編集（Add/Edit DAP Entry）] ダイアログボックスの [スパイウェア対策（Anti-Spyware）] （36 ページ）を参照）。
- アンチウイルス（表 10 : [DAPエントリの追加（Add DAP Entry）]/[DAPエントリの編集（Edit DAP Entry）] ダイアログボックス > [アンチウイルス（Anti-Virus）] （37 ページ）を参照）。
- AnyConnect アイデンティティ（表 11 : [DAPエントリの追加/編集（Add/Edit DAP Entry）] ダイアログボックスの AnyConnect ID （39 ページ）を参照）。
- アプリケーション（表 12 : [DAPエントリの追加（Add DAP Entry）]/[DAPエントリの編集（Edit DAP Entry）] ダイアログボックスのアプリケーション （40 ページ）を参照）。
- デバイス（表 13 : [DAPエントリの追加（Add DAP Entry）]/[DAPエントリの編集（Edit DAP Entry）] ダイアログボックス > [デバイス（Device）] （41 ページ）を参照）。
- ファイル（表 14 : [DAPエントリの追加（Add DAP Entry）]/[DAPエントリの編集（Edit DAP Entry）] ダイアログボックスファイル （43 ページ） を参照）。
- NAC（表 15 : [DAPエントリの追加（Add DAP Entry）]/[DAPエントリの編集（Edit DAP Entry）] ダイアログボックスの [NAC] （45 ページ） を参照）。
- オペレーティングシステム（表 16 : [DAPエントリの追加/編集（Add/Edit DAP Entry）] ダイアログボックスの [オペレーティングシステム（Operating System）] （46 ページ）を参照）。
- パーソナルファイアウォール（表 17 : [DAP エントリの追加/編集（Add/Edit DAP Entry）] ダイアログボックスの [パーソナルファイアウォール（Personal Firewall）] （47 ページ）を参照）。
- ポリシー（表 18 : [DAPエントリの追加（Add DAP Entry）]/[DAPエントリの編集（Edit DAP Entry）] ダイアログボックスポリシー （49 ページ） を参照）。
- プロセス（表 19 : [DAPエントリの追加（Add DAP Entry）]/[DAPエントリの編集（Edit DAP Entry）] ダイアログボックスの [プロセス（Process）] （50 ページ）を参照）。
- レジストリ（表 20 : [DAPエントリの追加（Add DAP Entry）]/[DAPエントリの編集（Edit DAP Entry）] ダイアログボックスのレジストリ （51 ページ）を参照）。
- マルチ証明書認証（表 22 : [DAP エントリの追加（Add DAP Entry）]/[DAP エントリの編集（Edit DAP Entry）] ダイアログボックスの [マルチ証明書認証（Multiple Certificate Authentication）] （55 ページ）を参照）。

ステップ 5 [OK] をクリックします。

ASA デバイスでの Cisco Secure Desktop ポリシーの設定

Cisco Secure Desktop（CSD）は、クライアント システム上のセッション アクティビティおよび削除に、単一のセキュアなロケーションを提供することによって、機密データのすべてのトレースを確実に除去する方法を提供します。CSD では、機密データが SSL VPN セッションの間だけ共有されるセッションベースのインターフェイスを使用できます。すべてのセッション情報が暗号化され、セッションが終了したときに（たとえ接続が突然終了した場合でも）、セッションデータのすべてのトレースがリモートクライアントから削除されます。このため、クッキー、ブラウザ履歴、一時ファイル、およびダウンロードしたコンテンツがシステムに残ることはありません。

セッションを閉じた場合、CSD は Department of Defense（DoD; 米国国防総省）消去アルゴリズムを使用して、すべてのデータを上書きして削除し、エンドポイントの機密保持を行います。

（注） Cisco Secure Desktop プログラムの詳細な機能および設定については、このマニュアルでは説明しません。CSD の設定および CSD の機能については、http://www.cisco.com/en/US/products/ps6742/tsd_products_support_configure.html のオンラインで入手できる資料を参照してください。設定する CSD バージョンのコンフィギュレーション ガイドを選択してください。

ここでは、ASA デバイスで Cisco Secure Desktop 機能を設定する方法について説明します。

はじめる前に

- 接続プロファイルポリシーがデバイスに設定済みであることを確認します。接続プロファイルの設定（ASA、PIX 7.0+） を参照してください。

関連項目

- 接続プロファイルの設定（ASA、PIX 7.0+）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ASA デバイスを選択して、ポリシーセレクタから [リモートアクセス VPN（Remote Access VPN）] > [ダイナミックアクセス（Dynamic Access）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから、[リモートアクセス VPN（Remote Access VPN）] > [ダイナミックアクセス（ASA）（Dynamic Access (ASA)）] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[Dynamic Access] ページが開きます。このページの要素の詳細については、[Dynamic Access] ページ（ASA）（14 ページ）を参照してください。

ステップ 2 [Cisco Secure Desktop] セクションで [CSDを有効化（Enable CSD）] を選択し、ASA デバイスで CSD を有効にします。

（注） [CSDを有効化（Enable CSD）] オプションは、ASA 9.5(2) 以前のバージョンの ASA を実行しているデバイスで使用できます。Security Manager 4.10 以降では、ASA バージョン 9.5(2) 以降を実行しているデバイスでのみ、Hostscan を設定する（CSD を無効にする）ための新しいチェックボックスを使用できます。

ステップ 3 [CSDパッケージ（CSD Package）] フィールドで、デバイスにアップロードする Cisco Secure Desktop パッケージを示すファイルオブジェクトの名前を指定します。[選択（Select）] をクリックして既存のファイルオブジェクトを選択するか、新しいファイルオブジェクトを作成します。詳細については、[Add File Object]/[Edit File Object] ダイアログボックスを参照してください。

（注） パッケージ バージョンは、ASA オペレーティング システムのバージョンと互換性がある必要があります。デバイスビューでローカルポリシーを作成する場合、[バージョン（Version）] フィールドは選択すべき CSD パッケージのバージョンを示します。（バージョンはパッケージ ファイル名に含まれています。たとえば、securedesktop-asa_k9-3.3.0.118.pkg は CSD バージョン 3.3.0.118 です。) ポリシービューで共有ポリシーを作成する場合、[バージョン（Version）] フィールドは選択した CSD ファイルのバージョンを示します。バージョン互換性の詳細については、SSL VPN サポート ファイルの概要と管理を参照してください。

ステップ 4 （任意）[Hostscanパッケージ（Hostscan Package）] フィールドで、デバイスにアップロードする Host Scan パッケージを示すファイルオブジェクトの名前を指定します。[選択（Select）] をクリックして既存のファイルオブジェクトを選択するか、新しいファイルオブジェクトを作成します。詳細については、[Add File Object]/[Edit File Object] ダイアログボックスを参照してください。

ステップ 5 [設定（Configure）] をクリックして、セキュリティアプライアンスで CSD を設定できる Cisco Secure Desktop Manager（CSDM）ポリシーエディタを開きます。これは、Security Manager とは別のアプリケーションです。ポリシー エディタの使用方法については、上記の CSD のマニュアルを参照してください。

エディタに含まれる主な項目は、次のとおりです（コンテンツ テーブルで選択します）。

- [Prelogin Policies]：これは決定ツリーです。ユーザが接続を試みると、そのユーザのシステムがルールに照らして評価され、最初に一致したルールが適用されます。通常は、セキュアなロケーション、ホーム ロケーション、およびセキュアでないパブリック ロケーションのポリシーを作成します。レジストリ情報、特定のファイルまたは証明書があるかどうか、ワークステーションのオペレーティング システム、または IP アドレスに基づいてチェックを行うことができます。

編集を行う場合は、必ず右クリック メニューを使用します。ボックスまたは [+] 記号を右クリックして、関連する設定をアクティブにします（ある場合）。

エンド ノードの場合は、次のオプションを選択できます。

- [Access Denied]：基準に一致するワークステーションがネットワークにアクセスできなくなります。
- [Policy]：この時点での固有の許可ポリシーを定義します。ポリシーは、名前を付けた後にコンテンツ テーブルに追加されます。ポリシーの各項目を選択して、その設定を行います。
- [Subsequence]：追加チェックを実行します。このワークステーションを評価する次の決定ツリーの名前を入力します。
- [Host Scan]：基本ホスト スキャンの一部を構成する一連のレジストリ エントリ、ファイル名、およびプロセス名を指定できます。ホスト スキャンは、プリログイン評価が行われた後、ダイナミック アク

セス ポリシーが割り当てられる前に実行されます。セキュリティ アプライアンスは、基本ホスト スキャンの後、ログイン クレデンシャル、ホスト スキャン結果、プリログイン ポリシー、および設定された他の基準に基づいて、ダイナミック アクセス ポリシーを割り当てます。次のアセスメントをイネーブルにできます。

- [Endpoint Assessment]：リモート ワークステーションは、アンチウイルス、アンチスパイウェア、パーソナル ファイアウォールの各アプリケーション、および関連する更新の大規模なコレクションをスキャンします。
- [Advanced Endpoint Assessment]：すべてのエンドポイント評価機能を含みます。また、指定されたバージョン要件を満たすように、準拠していないワークステーションの更新を試みるよう設定できます。この機能を設定するには、ライセンスを購入してインストールする必要があります。

[Dynamic Access] ページ（ASA）

[Dynamic Access] ページを使用して、セキュリティ アプライアンスで定義されている Dynamic Access Policy（DAP; ダイナミック アクセス ポリシー）を参照します。このページから、DAP を作成、編集、または削除できます。

[Cisco Secure Desktop] セクションを使用して、選択した ASA デバイスで Cisco Secure Desktop（CSD）ソフトウェアをイネーブルにし、ダウンロードします。Cisco Secure Desktop は、クライアント システム上にセッション アクティビティおよび削除のためのセキュアなロケーションを 1 つだけ提供することで、機密性が高いデータを SSL VPN セッションの間だけ共有できるようにしています。

（注） SSL VPN ポリシーが適切に機能するためには、CSD クライアント ソフトウェアがデバイスにインストールされてアクティブになっている必要があります。

ヒント ダイナミック アクセス ポリシーは、グループ ポリシーに優先します。ダイナミック アクセス ポリシーで設定を指定していない場合、ASA デバイスは設定を指定しているグループ ポリシーがないかどうかを確認します。

ナビゲーション パス

- （デバイスビュー）ASA デバイスを選択し、ポリシーセレクタから [リモートアクセス VPN（Remote Access VPN）] > [ダイナミックアクセス（ASA）（Dynamic Access (ASA)）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから、[リモートアクセスVPN（Remote Access VPN）] > [ダイナミックアクセス（ASA）（Dynamic Access (ASA)）] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

関連項目

- ダイナミック アクセス ポリシーについて （1 ページ）
- ダイナミック アクセス ポリシーの設定 （3 ページ）
- DAP 属性について （5 ページ）
- DAP 属性の設定 （10 ページ）
- ASA デバイスでの Cisco Secure Desktop ポリシーの設定 （12 ページ）

フィールド リファレンス

表 *3 : [Dynamic Access Policy]* ページ（*ASA*）

要素	説明
プライオリティ	設定済みのダイナミック アクセス ポリシー レコードのプライオリティ。
名前	設定済みのダイナミック アクセス ポリシー レコードの名前。
Network ACL	セッションに適用されるファイアウォール ACL の名前。
WebType ACL	セッションに適用される Web タイプ VPN ACL。
ポート転送	セッションに適用されるポート転送リストの名前。
[Bookmarks（ブックマーク）]	セッションに適用される SSL VPN ブックマーク オブジェクトの名前。
終了（Terminate）	セッションが終了しているかどうかを示します。
説明	設定済みのダイナミック アクセス ポリシーに関する追加情報。
[Create] ボタン	このボタンをクリックして、ダイナミック アクセス ポリシーを作成します。 [Add Dynamic Access Policy]/[Edit Dynamic Access Policy] ダイアログボックス （16 ページ）を参照してください。
[編集（Edit）] ボタン	このボタンをクリックして、選択したダイナミック アクセス ポリシーを編集します。 [Add Dynamic Access Policy]/[Edit Dynamic Access Policy] ダイアログボックス （16 ページ）を参照してください。
[削除（Delete）] ボタン	このボタンをクリックして、選択したダイナミック アクセス ポリシーを削除します。
Cisco Secure Desktop ASA デバイスで CSD を設定する手順については、 ASA デバイスでの Cisco Secure Desktop ポリシーの設定 （12 ページ）を参照してください。	

要素	説明
Enable CSD	選択すると、デバイスで CSD がイネーブルになります。CSD をイネーブルにすると、指定した Cisco Secure Desktop パッケージがロードされます。CSDパッケージファイルを転送または置換する場合は、CSD をいったんディセーブルにしてから、CSD をイネーブルにしてファイルをロードします。
CSD Package	デバイスにアップロードする Cisco Secure Desktop パッケージを識別するファイル オブジェクトの名前を指定します。 [選択（Select）] をクリックして既存のファイルオブジェクトを選択するか、新しいファイルオブジェクトを作成します。詳細については、[Add File Object]/[Edit File Object] ダイアログボックスを参照してください。
Hostscan Package	デバイスにアップロードする Hostscan パッケージを識別するファイル オブジェクトの名前を指定します。 [選択（Select）] をクリックして既存のファイルオブジェクトを選択するか、新しいファイルオブジェクトを作成します。詳細については、[Add File Object]/[Edit File Object] ダイアログボックスを参照してください。
バージョン	パッケージ バージョンは、ASA オペレーティング システムのバージョンと互換性がある必要があります。デバイス ビューでローカル ポリシーを作成する場合、[Version] フィールドは選択する必要がある CSD パッケージ バージョンを示します（バージョンはパッケージ ファイル名に含まれています。たとえば、securedesktop-asa_k9-3.3.0.118.pkg は CSD バージョン 3.3.0.118 です）。ポリシービューで共有ポリシーを作成する場合、[バージョン（Version）] フィールドは選択した CSD ファイルのバージョンを示します。バージョン互換性の詳細については、SSL VPN サポート ファイルの概要と管理を参照してください。
設定（Configure）	[設定（Configure）] をクリックして、セキュリティアプライアンスで CSD を設定できる Cisco Secure Desktop Manager（CSDM）ポリシーエディタを開きます。このダイアログボックスの要素の詳細については、 [Cisco Secure Desktop Manager Policy Editor] ダイアログボックス（62 ページ）を参照してください。

[Add Dynamic Access Policy]/[Edit Dynamic Access Policy] ダイアログボックス

[Add Dynamic Access Policy]/[Edit Dynamic Access Policy] ダイアログボックスを使用して、セキュリティ アプライアンスで Dynamic Access Policy（DAP; ダイナミック アクセス ポリシー）

を設定します。追加するダイナミック アクセス ポリシーに名前を指定し、プライオリティを選択し、LUA 表現で属性を指定できます。また、ネットワークおよび Web タイプ ACL フィルタ、ファイル アクセス、HTTP プロキシ、URL エントリおよびリスト、ポート転送、およびクライアントレス SSL VPN アクセス方式に対して属性を設定できます。

（注） ダイナミック アクセス ポリシー属性の詳細については、DAP 属性について （5 ページ）を参照してください。

これらのタブは、[Add Dynamic Access Policy]/[Edit Dynamic Access Policy] ダイアログボックスで使用可能です。

- [Main] タブ （18 ページ）
- [論理的な操作（Logical Operators）] タブ （58 ページ）
- [Advanced Expressions] タブ （61 ページ）

ナビゲーション パス

[Dynamic Access] ページ（ASA） （14 ページ）を開き、[作成（Create）] をクリックするか、テーブルのダイナミック アクセス ポリシーを選択して [編集（Edit）] をクリックします。[Add Dynamic Access Policy]/[Edit Dynamic Access Policy] ダイアログボックスが表示されます。

関連項目

- ダイナミック アクセス ポリシーについて （1 ページ）
- ダイナミック アクセス ポリシーの設定 （3 ページ）

フィールド リファレンス

表 4 : [Add Dynamic Access Policy]/[Edit Dynamic Access Policy] ダイアログボックス

要素	説明
名前	ダイナミック アクセス ポリシー レコードの名前（最大 128 文字）。
プライオリティ	ダイナミック アクセス ポリシー レコードのプライオリティ。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。プライオリティ設定が同じで、ACL ルールが競合するダイナミック アクセス ポリシー レコードがある場合は、最も厳しいルールが適用されます。 プライオリティは、マルチコンテキスト ASA バージョン 9.6(2) 以降のデバイスの Security Manager バージョン 4.12 以降でサポートされています。

要素	説明
説明	ダイナミック アクセス ポリシー レコードに関する追加情報（最大 1024 文字）。 説明は、マルチコンテキスト ASA バージョン 9.6(2) 以降のデバイスの Security Manager バージョン 4.12 以降でサポートされています。
[メイン（Main）] タブ	ダイナミック アクセス ポリシー エントリを追加し、設定するリモート アクセスのタイプに応じてアクセス ポリシーの属性を設定できます。 このタブの要素の詳細については、[Main] タブ （18 ページ）を参照してください。
[論理的な操作（Logical Operators）] タブ	各タイプのエンドポイント属性の複数のインスタンスを作成できます。 このタブの要素の詳細については、[論理的な操作（Logical Operators）] タブ （58 ページ）を参照してください。
[Advanced Expressions] タブ	1 つ以上の論理式を設定して、[AAA] および [Endpoint] 領域で設定できない AAA 属性またはエンドポイント属性を設定できます。 このタブの要素の詳細については、[Advanced Expressions] タブ （61 ページ）を参照してください。

[Main] タブ

[Add Dynamic Access Policy]/[Edit Dynamic Access Policy] ダイアログボックスの [Main] タブを使用して、セキュリティ アプライアンスでサポートされるダイナミック アクセス ポリシー属性およびリモート アクセス方式のタイプを設定します。ネットワークおよび Web タイプ ACL フィルタ、ファイル アクセス、HTTP プロキシ、URL エントリおよびリスト、ポート転送、およびクライアントレス SSL VPN アクセス方式に対して属性を設定できます。

ナビゲーション パス

[Main] タブは、[Add Dynamic Access Policy]/[Edit Dynamic Access Policy] ダイアログボックス（16 ページ）を開くと表示されます。

関連項目

- ダイナミック アクセス ポリシーの設定 （3 ページ）
- DAP 属性の設定 （10 ページ）

フィールド リファレンス

表 5 : [ダイナミックアクセスポリシーの追加/編集（*Add/Edit Dynamic Access Policy*）] ダイアログボックス > [Main] タブ

要素	説明
Criteria ID	ダイナミック アクセス ポリシーに使用可能な AAA およびエンドポイントの選択属性名。
Content	セキュリティ アプライアンスがセッションの確立中にダイナミック アクセス ポリシー レコードを選択および適用するために使用する、AAA 属性およびエンドポイント属性の値。ここで設定した属性値は、AAA システム内の認可の値（既存のグループ ポリシー、トンネル グループ、およびデフォルト グループ レコード内の値を含む）を上書きします。
[Create] ボタン	このボタンをクリックして、AAA 属性および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します。[Add DAP Entry]/[Edit DAP Entry] ダイアログボックス （27 ページ）を参照してください。
[編集（Edit）] ボタン	このボタンをクリックして、選択したダイナミック アクセス ポリシーを編集します。[Add DAP Entry]/[Edit DAP Entry] ダイアログボックス （27 ページ）を参照してください。
[削除（Delete）] ボタン	このボタンをクリックして、選択したダイナミック アクセス ポリシーを削除します。
アクセス方式	許可されるリモート アクセスのタイプを指定します。 • [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ポータル（Web Portal）]：クライアントレス VPN を使用して接続します。 • [両方、デフォルトはWebポータル（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。 • [両方、デフォルトはAnyConnect（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。

要素	説明
[Network ACL] タブ：このダイナミック アクセス ポリシーに適用するネットワーク ACL を選択および設定できます。ダイナミック アクセス ポリシーの ACL には、許可ルールと拒否ルールのいずれか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る場合は、セキュリティ アプライアンスで拒否されます。	
Network ACL	SSL†VPN へのユーザ アクセスを制限するために使用されるアクセス コントロール リスト（ACL）が一覧表示されます。 Security Manager バージョン 4.10 以降、ネットワーク ACL は IPv6 エントリをサポートします。また、IPv6は、ソフトウェアバージョン ASA 9.0 以降を実行しているデバイスでサポートされています。これは、ネットワーク ACL と Web タイプ ACL の両方に適用されます。 [選択（Select）] ボタンをクリックして、Access Control Lists Selector を開きます。ここから選択できます。ACL には、パケットのトラフィック ストリームが記述された条件と、それらの条件に基づいて実行する処理が記述されたアクションが含まれます。許可ルールだけ、または拒否ルールだけが含まれている ACL だけが適格となります。 ネットワーク ACL は、マルチコンテキスト ASA バージョン 9.6(2) 以降のデバイスの Security Manager バージョン 4.12 以降でサポートされています。
[AnyConnect] タブ：AnyConnect サービスプロファイルの Always-on VPN の設定を未変更にするか、ディセーブルにするか、AnyConnect プロファイル設定を使用するかを選択できます。Always-On VPN を使用すると、システムにログオンした後、AnyConnnect で VPN セッションを自動的に確立できます。	
[カスタム属性] タブ：AnyConnect カスタム属性タイプとカスタム属性名を一覧表示します。AnyConnect カスタム属性により、ASA ソフトウェアをアップグレードすることなく、新しいクライアントコントロールの追加を総合的にサポートする機能を ASA に提供することで、新しいエンドポイント機能のより迅速な配信と展開が可能になります。バージョン 4.7 以降、Security Manager では、カスタム属性データを既存のカスタム属性タイプに追加できます。この機能は、ASA ソフトウェアバージョン 9.3(1) 以降を実行しているデバイスでサポートされています。	
属性タイプ	[AnyConnectカスタム属性の追加/編集（Add/Edit AnyConnect Custom Attribute）] ダイアログボックスページで設定した属性タイプを選択します。
属性名	[AnyConnectカスタム属性の追加/編集（Add/Edit AnyConnect Custom Attribute）] ダイアログボックスページで設定した属性名を選択します。

要素	説明
[WebType ACL] タブ：このダイナミック アクセス ポリシーに適用する Web タイプ ACL を選択および設定できます。ダイナミック アクセス ポリシーの 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。ACL に許可ルールと拒否ルールの両方が含まれる場合は、セキュリティ アプライアンスで拒否されます。	
Web Type ACL	SSL†VPN へのユーザ アクセスを制限するために使用される Web タイプ アクセス コントロール リストを指定します。 [選択（Select）] ボタンをクリックして、Access Control Lists Selector を開きます。ここから選択できます。許可ルールだけ、または拒否ルールだけが含まれている ACL だけが適格となります。バージョン 4.10 以降では、Web タイプ ACL に IPv6 値を入力できます。
[Functions] タブ：ファイル サーバのエントリとブラウズ、HTTP プロキシ、およびダイナミック アクセス ポリシーの URL エントリを設定できます。	
[ファイルサーバーブラウズ（File Server Browsing）]	ポータル ページで設定するファイル サーバ ブラウズ設定を指定します。 • [変更なし（Unchanged）]：このセッションに適用するグループ ポリシーの値を使用します。 • [有効（Enable）]：ファイルサーバーまたは共有機能に対する CIFS ブラウズをイネーブルにします。 • [無効（Disable）]：ファイルサーバーまたは共有機能に対する CIFS ブラウズをディセーブルにします。 （注） ブラウズには、NBNS（プライマリブラウザまたは 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。CIFS ブラウズ機能では、国際化がサポートされていません。

要素	説明
File Server Entry	ポータル ページで設定するファイル サーバ エントリ設定を指定します。 • [変更なし（Unchanged）]：このセッションに適用するグループ ポリシーの値を使用します。 • [有効（Enable）]：ユーザはポータルページでファイルサーバーのパスおよび名前を入力できます。 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ーエントリのドロワが配置されます。ユーザーは、Windows ファイルへのパス名を直接入力できます。ユーザーは、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 サーバーでユーザー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、ユーザー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。 • [無効（Disable）]：ユーザはポータルページでファイルサーバーのパスおよび名前を入力できません。

要素	説明
HTTP プロキシ	HTTPS 接続を終了して HTTP/HTTPS 要求を HTTP および HTTPS プロキシ サーバに転送するための、セキュリティ アプライアンスの設定を指定します。 • [変更なし（Unchanged）]：このセッションに適用するグループ ポリシーの値を使用します。 • [有効（Enable）]：HTTP アプレットプロキシのクライアントへの転送を許可します。 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、ブラウザの古いプロキシ設定を変更し、すべての HTTP および HTTPS 要求を新しいプロキシ設定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。 • [無効（Disable）]：HTTP アプレットプロキシのクライアントへの転送をディセーブルにします。 • [自動開始（Auto-start）]：HTTP プロキシをイネーブルにし、DAP レコードによりこれらの機能に関連付けられたアプレットが自動的に開始されるように設定します。

要素	説明
URL Entry	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のデータ送信のセキュリティを確保します。ユーザが（インターネットまたは内部ネットワークに存在する）HTTPS 以外の Web リソースにアクセスする場合、企業セキュリティ アプライアンスから宛先 Web サーバへの通信は保護されません。 クライアントレス VPN 接続では、セキュリティ アプライアンスがエンド ユーザ Web ブラウザとターゲット Web サーバの間のプロキシとして機能します。ユーザが SSL 対応の Web サーバに接続すると、セキュリティ アプライアンスによりセキュアな接続が確立され、サーバ SSL 証明書が検証されます。エンド ユーザー 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 アプライアンスが信頼できる CA 証明書検証を実行することも許可されません。このため、ユーザーは、SSL 対応の Web サーバーと通信する前に、そのサーバーにより提示された証明書を分析することはできません。 ポータル ページでの URL エントリの設定を指定します。 • [変更なし（Unchanged）]：このセッションに適用するグループ ポリシーの値を使用します。 • [有効（Enable）]：ユーザはポータルページで HTTP または HTTPS の URL を入力できます。この機能がイネーブルになっている場合、ユーザーは 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。 • [無効（Disable）]：ユーザはポータルページで HTTP または HTTPS の URL を入力できません。 （注） ユーザのインターネットアクセスを制限するには、[URL エントリ（URL Entry）] フィールドで [無効（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。

要素	説明
[Port Forwarding] タブ：ユーザ セッションのポート転送リストを選択および設定できます。 （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。	
ポート転送	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。 • [変更なし（Unchanged）]：実行コンフィギュレーションから属性を削除します。 • [有効（Enable）]：デバイスでポート転送をイネーブルにします。 • [無効（Disable）]：デバイスでポート転送をディセーブルにします。 • [自動開始（Auto-start）]：ポート転送をイネーブルにし、DAP レコードによりそ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開始されるように設定します。
Port Forwarding List	クライアントマシン上のポート番号から SSL VPN ゲートウェイの背後にあるアプリケーションの IP アドレスとポートへのマッピングを定義する、ポート転送リスト。 [選択（Select）]をクリックすると [ポート転送リストセレクタ（Port Forwarding List Selector）] が開き、そこで、ポート転送リストオブジェクトのリストから必要なポート転送リストを選択できます。ポート転送リストオブジェクトは、リモートクライアント上のポート番号から SSL VPN ゲートウェイの背後にあるアプリケーションの IP アドレスとポートへのマッピングを定義します。
[Bookmark] タブ：SSL VPN ブックマークをイネーブルにし、設定できます。イネーブルになっている場合、SSL VPN に正常にログインしたユーザに、定義済みのブックマークのリストを含むポータルページが表示されます。これらのブックマークにより、ユーザは [Clientless] アクセス モードで SSL VPN Web サイト上で使用可能なリソースにアクセスできます。	

要素	説明
Enable Bookmarks	ポータル ページで設定するファイル サーバ ブラウズ設定を指定します。 • [変更なし（Unchanged）]：このセッションに適用するグループ ポリシーの値を使用します。 • [有効（Enable）]：SSL VPN ポータルページのブックマークをイネーブルにします。 • [無効（Disable）]：SSL VPN ポータルページのブックマークをディセーブルにします。
ブックマーク	ユーザが SSL VPN Web サイトで使用可能なリソースにアクセスできるように、ポータルページにブックマークとして表示される Web サイトのリスト。 [選択（Select）] をクリックすると、[ブックマークセレクタ（Bookmarks Selector）] が開きます。このセレクタで適宜、リストから目的のブックマークを選択するか、新しいブックマークを作成できます。
[Action] タブ：特定の接続またはセッションに適用される特別な処理を指定します。 [アクション（Action）] タブは、マルチコンテキスト ASA バージョン 9.6(2) 以降のデバイスの Security Manager バージョン 4.12 以降でサポートされています。 ドロップダウン リストから、次のいずれかのオプションを選択します。	
続行（Continue）	（デフォルト）選択すると、セッションが続行されます。デフォルトでは、アクセス ポリシー属性がセッションに適用され、セッションは実行されます。
検疫（Quarantine）	選択すると、セッションが隔離されます。 検疫を使用すると、VPN経由ですでにトンネルを確立した特定のクライアントを制限できます。制限付き ACL がセッションに適用され、制限付きグループが形成されます。この基になるのは、選択された DAP レコードです。管理目的で定義されたポリシーにエンドポイントが準拠していないときも、ユーザは修復のためのサービス（たとえばアンチウイルスアプリケーションのアップデート）にアクセスできますが、そのユーザには制限が適用されます。修復後、ユーザーは再接続できます。この再接続により、新しいポスチャ アセスメントが起動されます。このアセスメントに合格すると、接続されます。 （注） このパラメータを使用するには、AnyConnect セキュア モビリティ機能をサポートしている AnyConnect リリースが必要です。

要素	説明
終了（Terminate）	選択した場合、セッションが終了します。デフォルトでは、アクセス ポリシー属性がセッションに適用され、セッションは実行されます。
ユーザ メッセージ	この DAP レコードが選択されたときにポータル ページに表示されるテキスト 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。複数の DAP レコードが選択されており、かつ、それぞれにユーザ メッセージが設定されている場合は、すべてのユーザ メッセージが表示されます。 （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、手順 を参照してください。 （注） ユーザメッセージは、マルチコンテキストモードでバージョン 9.6(2) 以降を実行している ASA デバイスの Security Manager バージョン 4.12 以降でサポートされています。

マルチコンテキスト ASA 9.6(2) デバイスの Security Manager バージョン 4.12 以降でサポートされるダイナミック アクセス ポリシー CLI は次のとおりです。

- Dynamic-access-policy-record アクション
- description
- exit
- help
- network-acl
- ×
- プライオリティ
- quit
- user-message

[Add DAP Entry]/[Edit DAP Entry] ダイアログボックス

[Add DAP Entry]/[Edit DAP Entry] ダイアログボックスを使用して、ダイナミック アクセス ポリシーの認可属性とエンドポイント属性を指定します。セキュリティ アプライアンスは、リモート デバイスのエンドポイント セキュリティ情報と認証済みユーザの AAA 認可情報に基づい

て、ダイナミック アクセス ポリシーを選択します。次に、そのダイナミック アクセス ポリシーをユーザ トンネルまたはセッションに適用します。

ダイナミック アクセス ポリシー属性の詳細については、DAP 属性について （5 ページ）を参照してください。

このダイアログボックスの内容は、選択した基準によって変わります。この基準は、セキュリティ アプライアンスがセッション確立中にダイナミック アクセス ポリシーを選択および適用するときに使用する選択基準として機能する認可またはエンドポイント属性です。次の基準から選択できます。

- [AAA Attributes Cisco]：AAA 階層モデルに格納されているユーザ認可属性を参照します。[DAPエントリの追加（Add DAP Entry）]/[DAPエントリの編集（Edit DAP Entry）] ダイアログボックス、[AAA属性Cisco（AAA Attributes Cisco）] （30 ページ）を参照してください
- [AAA Attributes LDAP]：LDAP クライアントにおいて、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、すべてのネイティブ LDAP 応答属性のペアが格納されるように設定します。[DAPエントリの追加（Add DAP Entry）]/[DAPエントリの編集（Edit DAP Entry）] ダイアログボックス の AAA 属性 LDAP （32 ページ）を参照してください。
- [AAA Attributes RADIUS]：RADIUS クライアントがユーザの AAA セッションに関連付けられたデータベースにすべてのネイティブ RADIUS 応答属性のペアを格納するように設定します。[DAPエントリの追加/編集（Add/Edit DAP Entry）] ダイアログボックスの [AAA属性RADIUS（AAA Attributes RADIUS）] （34 ページ）を参照してください。
- [Anti-Spyware]：[Anti-Spyware] タイプのエンドポイント属性を作成します。Cisco Secure Desktop のホスト スキャン モジュールを使用して、リモート コンピュータで実行されているアンチスパイウェア アプリケーションおよび更新をスキャンできます。[DAPエントリの追加/編集（Add/Edit DAP Entry）] ダイアログボックスの [スパイウェア対策（Anti-Spyware）] （35 ページ）を参照してください。
- [Anti-Virus]：[Anti-Virus] タイプのエンドポイント属性を作成します。Cisco Secure Desktop のホスト スキャン モジュールを使用して、リモート コンピュータで実行されているアンチウイルス アプリケーションおよび更新をスキャンできます。[DAPエントリの追加（Add DAP Entry）]/[DAPエントリの編集（Edit DAP Entry）] ダイアログボックス > [アンチウイルス（Anti-Virus）] （37 ページ）を参照してください。
- [AnyConnect アイデンティティ（AnyConnect Identity）]：[AnyConnect アイデンティティ（AnyConnect Identity）] タイプのエンドポイント属性を作成します。[DAPエントリの追加/編集（Add/Edit DAP Entry）] ダイアログボックスの AnyConnect ID （38 ページ）を参照してください。
- [Application]：リモート アクセス接続のタイプを示します。[DAPエントリの追加（Add DAP Entry）、]/[DAPエントリの編集（Edit DAP Entry）] ダイアログボックスのアプリケーション （40 ページ）を参照してください。
- [デバイス（Device）]：[デバイス（Device）] タイプのエンドポイント属性を作成します。[デバイス基準（Device Criterion）] では、関連付けられたプリログイン ポリシー チェック中に使用できる特定のデバイス情報を提供できます。[DAPエントリの追加（Add DAP

Entry）]/[DAPエントリの編集（Edit DAP Entry）] ダイアログボックス>[デバイス（Device）]（41 ページ）を参照してください。

- [File]：[File] タイプのエンドポイント属性を作成します。Cisco Secure Desktop Manager を使用して、基本ホスト スキャンによって実行されるファイル名チェックを明示的に設定する必要があります。[DAPエントリの追加（Add DAP Entry）]/[DAPエントリの編集（Edit DAP Entry）] ダイアログボックスファイル （42 ページ）を参照してください。
- [NAC]：[NAC] タイプのエンドポイント属性を作成します。NAC は、エンドポイント準拠を実行することにより、ワーム、ウイルス、および不正なアプリケーションの侵入や感染からエンタープライズ ネットワークを保護します。これらのチェックをポスチャ検証と呼びます。[DAPエントリの追加（Add DAP Entry）]/[DAPエントリの編集（Edit DAP Entry）] ダイアログボックスの [NAC] （44 ページ）を参照してください。
- [Operating System]：[Operating System] タイプのエンドポイント属性を作成します。CSD のプリログイン評価モジュールは、リモート デバイスの OS バージョン、IP アドレス、および Microsoft Windows レジストリ キーをチェックできます。[DAPエントリの追加/編集（Add/Edit DAP Entry）] ダイアログボックスの [オペレーティングシステム（Operating System）] （45 ページ）を参照してください。
- [Personal Firewall]：[Personal Firewall] タイプのエンドポイント属性を作成します。Cisco Secure Desktop のホスト スキャン モジュールを使用して、リモート コンピュータで実行されているパーソナル ファイアウォール アプリケーションおよび更新をスキャンできます。このダイアログボックスの要素の詳細については、[DAP エントリの追加/編集（Add/Edit DAP Entry）] ダイアログボックスの [パーソナルファイアウォール（Personal Firewall）] （47 ページ）を参照してください。
- [Policy]：[Policy] タイプのエンドポイント属性を作成します。[DAPエントリの追加（Add DAP Entry）]/[DAPエントリの編集（Edit DAP Entry）] ダイアログボックスポリシー （48 ページ）を参照してください。
- [Process]：Cisco Secure Desktop Manager を使用して、基本ホスト スキャンによって実行されるプロセス名チェックを明示的に設定する必要があります。[DAPエントリの追加（Add DAP Entry）]/[DAPエントリの編集（Edit DAP Entry）] ダイアログボックスの [プロセス（Process）] （49 ページ）を参照してください。
- [Registry]：[Registry] タイプのエンドポイント属性を作成します。レジストリ キー スキャンは、Microsoft Windows オペレーティング システムを実行しているコンピュータにだけ適用されます。[DAPエントリの追加/編集（Add/Edit DAP Entry）] ダイアログボックスのレジストリ （51 ページ）を参照してください。
- [複数証明書認証（Multiple Certificate Authentication）]：[複数証明書認証（Multiple Certificate Authentication）] タイプのエンドポイント属性を作成します。リモート VPN ユーザーの複数証明書認証の属性を指定できます。[DAP エントリの追加（Add DAP Entry）]/[DAP エントリの編集（Edit DAP Entry）] ダイアログボックスの [マルチ証明書認証（Multiple Certificate Authentication）] （54 ページ）を参照してください。

（注） 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のないダイナミック アクセス ポリシーを設定する場合は、すべての選択基準が満たされるため、セキュリティ アプライアンスでは常にそのポリシーが選択されます。

ナビゲーション パス

[Add Dynamic Access Policy]/[Edit Dynamic Access Policy] ダイアログボックス （16 ページ）を開いて [メイン（Main）] タブを選択し、[作成（Create）] をクリックするか、テーブルでダイナミック アクセス ポリシーを選択して [編集（Edit）] をクリックします。[Add DAP Entry]/[Edit DAP Entry] ダイアログボックスが表示されます。

関連項目

- DAP 属性について （5 ページ）
- DAP 属性の設定 （10 ページ）
- ダイナミック アクセス ポリシーの設定 （3 ページ）

[DAPエントリの追加（Add DAP Entry）]/[DAPエントリの編集（Edit DAP Entry）] ダイアログボックス、[AAA属性Cisco（AAA Attributes Cisco）]

ダイナミック アクセス ポリシーの選択基準として AAA 属性を設定するには、[Add DAP Entry]/[Edit DAP Entry] ダイアログボックスで、セッションの確立中にダイナミック アクセス ポリシーを選択および適用するときに使用する選択基準として [AAA Attributes Cisco] を設定します。これらの属性を、入力した値と一致するように、または一致しないように設定できます。各ダイナミック アクセス ポリシーの AAA 属性の数に制限はありません。

（注） 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のないダイナミック アクセス ポリシーを設定する場合は、すべての選択基準が満たされるため、セキュリティ アプライアンスでは常にそのポリシーが選択されます。

ナビゲーション パス

[Add Dynamic Access Policy]/[Edit Dynamic Access Policy] ダイアログボックス （16 ページ）を開いて [メイン（Main）] タブを選択し、[作成（Create）] をクリックするか、テーブルでダイナミック アクセス ポリシーを選択して [編集（Edit）] をクリックします。[Add DAP Entry]/[Edit DAP Entry] ダイアログボックスが表示されます。[基準（Criterion）] として [AAA属性Cisco（AAA Attributes Cisco）] を選択します。

関連項目

- DAP 属性について （5 ページ）

• DAP 属性の設定 （10 ページ）
• ダイナミック アクセス ポリシーの設定 （3 ページ）

フィールド リファレンス

表 *6 : [DAP*エントリの追加（*Add DAP Entry*）*]/[DAP*エントリの編集（*Edit DAP Entry*）*]* ダイアログボックス、*[AAA*属性 *Cisco*（*AAA Attributes Cisco*）*]*

要素	説明
基準	選択基準として [AAA Attributes Cisco] が表示されます。
[グループ ポリシー（Group Policy）]	チェックボックスをオンにし、ドロップダウンリストから一致基準（[次に一致する（is）] など）を選択して、ユーザーに関連付けられた AAA サーバーグループの名前を入力します。64 文字まで指定できます。 AAA サーバ グループは、ネットワーク セキュリティ ポリシー全体の特定の側面を実施することに焦点を当てた、認証サーバの集合を表します。
IPv4 アドレス	チェックボックスをオンにし、ドロップダウンリストから一致基準（[次に一致する（is）] など）を選択して、割り当てられた IP アドレスを入力します。 アドレスは、定義済みのネットワーク オブジェクトです。また、[選択（Select）] をクリックすると、使用可能なすべてのネットワークホストが一覧表示されたダイアログボックスが開きます。このダイアログボックスで、ネットワーク ホスト オブジェクトを作成または編集できます。 **ヒント** このオプションを選択して、あとでルールを ASDM で参照すると、IP アドレス属性は [Assigned IP Address] になります。
IPv6 アドレス （Security Manager バージョン 4.12 以降および ASA バージョン 9.0 以降）	チェックボックスをオンにし、ドロップダウンリストから一致基準（[次に一致する（is）] など）を選択して、割り当てられた IP アドレスを入力します。 アドレスは、定義済みのネットワーク オブジェクトです。また、[選択（Select）] をクリックすると、使用可能なすべてのネットワークホストが一覧表示されたダイアログボックスが開きます。このダイアログボックスで、ネットワーク ホスト オブジェクトを作成または編集できます。 **ヒント** このオプションを選択して、あとでルールを ASDM で参照すると、IP アドレス属性は [Assigned IP Address] になります。

要素	説明
Member-of	チェックボックスをオンにし、ドロップダウンリストから一致基準（[次に一致する（is）] など）を選択して、ユーザーに適用されるグループポリシー名をカンマ区切りの文字列として入力します。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。最大長は 128 文字です。 **ヒント** このオプションを選択して、あとでルールを ASDM で参照すると、このオプションは表示されません。このオプションは [memberof LDAP] 属性と間違いやすいため、通常はこのオプションは使用されません。このルールはローカル認証にも適用されるため、[Member-of] 属性の代わりに [Username] 属性を使用できます。
ユーザー名	チェックボックスをオンにし、ドロップダウンリストから一致基準（[次に一致する（is）] など）を選択して、認証済みユーザーのユーザー名を入力します。最大 64 文字を使用できます。
[ユーザー名2（Username 2）]	チェックボックスをオンにし、ドロップダウンリストから一致基準（[次に一致する（is）] または [次に一致しない（isn't）] など）を選択して、認証済みユーザーのセカンダリユーザー名を入力します。
接続プロファイル	チェックボックスをオンにし、ドロップダウンリストから一致基準（[次に一致する（is）] など）を選択して、セキュリティアプライアンスで定義されているすべての SSL VPN Connection Profile ポリシーのリストから接続プロファイルを選択します。 SSL VPN 接続プロファイルは、VPN トンネル接続プロファイル ポリシーを含む一連のレコードで構成されます。このレコードには、トンネルそのものの作成に関連する属性も含まれます。 （注） SSL VPN Connection Profiles ポリシーの設定手順については、接続プロファイルの設定（ASA、PIX 7.0+）を参照してください。
必要な SCEP	チェックボックスをオンにし、ドロップダウンリストから一致基準（[次に一致する（is）] または [次に一致しない（isn't）]）を選択して、[True] または [False] を選択します。この属性により、接続が証明書認証に失敗したかどうかを照合できます。

[DAPエントリの追加（Add DAP Entry）]/[DAPエントリの編集（Edit DAP Entry）] ダイアログボックス の AAA 属性 LDAP

LDAP クライアントでは、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、すべての LDAP 応答属性値のペアが格納されます。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廃棄されます。ユーザー レコードとグループ レコードの両方が LDAP サーバー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。ユーザー 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。

（注） 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のないダイナミック アクセス ポリシーを設定する場合は、すべての選択基準が満たされるため、セキュリティ アプライアンスでは常にそのポリシーが選択されます。

ナビゲーション パス

[Add Dynamic Access Policy]/[Edit Dynamic Access Policy] ダイアログボックス （16 ページ）を開いて [メイン（Main）] タブを選択し、[作成（Create）] をクリックするか、テーブルでダイナミック アクセス ポリシーを選択して [編集（Edit）] をクリックします。[Add DAP Entry]/[Edit DAP Entry] ダイアログボックスが表示されます。[基準（Criterion）] として [AAA属性LDAP（AAA Attributes LDAP）] を選択します。

関連項目

- DAP 属性について （5 ページ）
- DAP 属性の設定 （10 ページ）
- ダイナミック アクセス ポリシーの設定 （3 ページ）

フィールド リファレンス

表 *7 : [DAP*エントリの追加（*Add DAP Entry*）*]/[DAP*エントリの編集（*Edit DAP Entry*）*]* ダイアログボックス の *AAA* 属性 *LDAP*

要素	説明
基準	選択基準として [AAA Attributes LDAP] が表示されます。
属性 ID	ダイナミック アクセス ポリシー内の LDAP 属性マップの名前を指定します。LDAP 属性マップは、ユーザが定義した属性名をシスコ定義の属性にマッピングします。最大 64 文字を使用できます。

要素	説明
値	ドロップダウンリストから一致基準（*is* など）を選択して、Cisco マップ値にマップされるカスタムマップ値を入力するか、カスタムマップ値にマップされる Cisco マップ値を入力します。複数の値を入力するには、各値を区切り文字の**;** で区切ります。 属性マップには、カスタマーのユーザ定義属性値をカスタマー属性名および一致する Cisco 属性の名前と値に適用する値マッピングが読み込まれます。 または、[ADグループのフェッチ（Fetch AD Groups）] ボタンをクリックして、[ADグループのフェッチ（Fetch AD Groups）] ダイアログボックスを開きます。ダイアログボックスの表には、選択できる使用可能な LDAP サーバーのユーザグループ ID とユーザグループ名がリストされます。1 つ以上の行を選択し、[選択（Select）] ボタンをクリックします。 リスト内の特定のユーザグループを検索するには、[フィルター（Filter）] テキストボックスにテキストを入力して、[検索（Search）] をクリックします。条件を満たすユーザグループ名がリストに表示されます。 （注） 使用可能な LDAP サーバーのリストを表示できるようにするには、最初にドメインから AD サーバーグループへのマッピングを設定する必要があります。このタスクを実行するには、[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] に移動し、コンテンツテーブルから [設定の確認（Identity Settings）] を選択します。詳細については、[Identity Settings] ページを参照してください。

[DAPエントリの追加/編集（Add/Edit DAP Entry）] ダイアログボックスの [AAA属性RADIUS（AAA Attributes 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すべての RADIUS 応答属性値のペアを格納します。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廃棄されます。ユーザー レコードおよびグループ レコードの両方が RADIUS サーバー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。ユーザー 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。

（注） 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のないダイナミック アクセス ポリシーを設定する場合は、すべての選択基準が満たされるため、セキュリティ アプライアンスでは常にそのポリシーが選択されます。

ナビゲーション パス

[Add Dynamic Access Policy]/[Edit Dynamic Access Policy] ダイアログボックス （16 ページ）を開いて [メイン（Main）] タブを選択し、[作成（Create）] をクリックするか、テーブルでダイナミック アクセス ポリシーを選択して [編集（Edit）] をクリックします。[Add DAP Entry]/[Edit DAP Entry] ダイアログボックスが表示されます。[基準（Criterion）] として [AAA属性RADIUS（AAA Attributes RADIUS）] を選択します。

関連項目

- DAP 属性について （5 ページ）
- DAP 属性の設定 （10 ページ）
- ダイナミック アクセス ポリシーの設定 （3 ページ）

フィールド リファレンス

表 *8*:*[DAP*エントリの追加/編集（*Add/Edit DAP Entry*）*]*ダイアログボックスの *[AAA*属性*RADIUS*（*AAA Attributes RADIUS*）*]*

要素	説明
基準	選択基準として [AAA Attributes RADIUS] が表示されます。
属性 ID	ダイナミック アクセス ポリシー内の RADIUS 属性の名前または番号を指定します。最大 64 文字を使用できます。 3 つのセキュリティ アプライアンスすべて（VPN 3000、PIX、および ASA）に対するサポートをより反映するために、RADIUS 属性名に cVPN3000 プレフィックスは含まれていません。アプライアンスは、属性名ではなく数値の属性 ID に基づいて、RADIUS 属性を使用します。LDAP 属性は、ID ではなく属性名で使用します。
値	ドロップダウンリストから一致基準（[は（is）] など）を選択して、属性値を入力します。

[DAPエントリの追加/編集（Add/Edit DAP Entry）] ダイアログボックスの [スパイウェア対策（Anti-Spyware）]

Cisco Secure Desktop 機能のホスト スキャン機能を使用して、リモート コンピュータで実行されているアンチウイルス、パーソナルファイアウォール、およびアンチスパイウェアのアプリケーションと更新をスキャンできます。プリログイン ポリシーおよびホスト スキャンのオプションの設定に続いて、ホスト スキャン結果の 1 つまたは任意の組み合わせの一致を設定して、ユーザ ログイン後のダイナミック アクセス ポリシーに割り当てることができます。

（注） 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のないダイナミック アクセス ポリシーを設定する場合は、すべての選択基準が満たされるため、セキュリティ アプライアンスでは常にそのポリシーが選択されます。

ナビゲーション パス

[Add Dynamic Access Policy]/[Edit Dynamic Access Policy] ダイアログボックス （16 ページ）を開いて [メイン（Main）] タブを選択し、[作成（Create）] をクリックするか、テーブルでダイナミック アクセス ポリシーを選択して [編集（Edit）] をクリックします。[Add DAP Entry]/[Edit DAP Entry] ダイアログボックスが表示されます。[基準（Criterion）] として [スパイウェア対策（Anti-Spyware）] を選択します。

関連項目

- DAP 属性について （5 ページ）
- DAP 属性の設定 （10 ページ）
- ダイナミック アクセス ポリシーの設定 （3 ページ）

フィールド リファレンス

表 *9 : [DAP*エントリの追加/編集（*Add/Edit DAP Entry*）*]* ダイアログボックスの *[*スパイウェア対策（*Anti-Spyware*）*]*

要素	説明
基準	選択基準として [Anti-Spyware] が表示されます。
タイプ（Type）	次のいずれかのオプションを選択し、関連する値を割り当てます。 • [未インストール（Not Installed）]：指定されたマルウェア対策がリモートPC上にないことを、設定するプリログインポリシーに一致するための十分条件とする場合に選択します。 • [インストール済みで有効（Installed and enabled）]：指定されたマルウェア対策がリモートPC上に存在して有効になっていることを、設定するプリログインポリシーに一致するための十分条件とする場合に選択します。 • [インストール済みで無効（Installed and disabled）]：指定されたマルウェア対策がリモートPC上に単に存在していることを、設定するプリログインポリシーに一致するための十分条件とする場合に選択します。
ベンダー名（Vendor Name）	アプリケーションベンダーを説明するテキストをリストから選択します。
製品 ID	リストから選択したベンダーによってサポートされる製品の固有識別情報を選択します。
製品の説明	[一致（Matches）] を [タイプ（Type）] として選択した場合にだけ使用可能です。 チェックボックスをオンにし、リストから製品の説明を選択します。
バージョン	[一致（Matches）] を [タイプ（Type）] として選択した場合にだけ使用可能です。 アプリケーションのバージョンを識別し、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。

要素	説明
Last Update	[一致（Matches）] を [タイプ（Type）] として選択した場合にだけ使用可能です。 最後の更新からの日数を指定します。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。

[DAPエントリの追加（Add DAP Entry）]/[DAPエントリの編集（Edit DAP Entry）] ダイアログボックス > [アンチウイルス（Anti-Virus）]

アンチウイルス アプリケーションおよび更新のスキャンを、Cisco AnyConnect またはクライアントレス SSL VPN 接続の完了の条件として設定できます。プリログイン評価に続いて、Cisco Secure Desktop ではエンドポイント評価チェックをロードし、ダイナミック アクセス ポリシーの割り当てに使用できるように、セキュリティ アプライアンスに結果を返します。

（注） 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のないダイナミック アクセス ポリシーを設定する場合は、すべての選択基準が満たされるため、セキュリティ アプライアンスでは常にそのポリシーが選択されます。

ナビゲーション パス

[Add Dynamic Access Policy]/[Edit Dynamic Access Policy] ダイアログボックス （16 ページ）を開いて [メイン（Main）] タブを選択し、[作成（Create）] をクリックするか、テーブルでダイナミック アクセス ポリシーを選択して [編集（Edit）] をクリックします。[Add DAP Entry]/[Edit DAP Entry] ダイアログボックスが表示されます。[基準（Criterion）] として [アンチウイルス（Anti-Virus）] を選択します。

関連項目

- DAP 属性について （5 ページ）
- DAP 属性の設定 （10 ページ）
- ダイナミック アクセス ポリシーの設定 （3 ページ）

フィールド リファレンス

表 *10 : [DAPエントリの追加（Add DAP Entry）]/[DAPエントリの編集（Edit DAP Entry）] ダイアログボックス > [アンチウイルス（Anti-Virus）]*

要素	説明
基準	選択基準として [Anti-Virus] が表示されます。

要素	説明
タイプ（Type）	次のいずれかのオプションを選択し、関連する値を割り当てます。 • [未インストール（Not Installed）]：指定されたアンチウイルスがリモート PC 上にないことを、設定するプリログインポリシーに一致するための十分条件とする場合に選択します。 • [インストール済みで有効（Installed and enabled）]：指定されたアンチウイルスがリモート PC 上に存在して有効になっていることを、設定するプリログインポリシーに一致するための十分条件とする場合に選択します。 • [インストール済みで無効（Installed and disabled）]：指定されたアンチウイルスがリモート PC 上に存在していることを、設定するプリログインポリシーに一致するための十分条件とする場合に選択します。
ベンダー名（Vendor Name）	アプリケーションベンダーを説明するテキストをリストから選択します。
製品 ID	リストから選択したベンダーによってサポートされる製品の固有識別情報を選択します。
製品の説明	ダイナミック アクセス ポリシーのエンドポイント属性と一致する基準を選択した場合にだけ使用可能です。 チェックボックスをオンにし、リストから製品の説明を選択します。
バージョン	ダイナミック アクセス ポリシーのエンドポイント属性と一致する基準を選択した場合にだけ使用可能です。 アプリケーションのバージョンを識別し、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	ダイナミック アクセス ポリシーのエンドポイント属性と一致する基準を選択した場合にだけ使用可能です。 最後の更新からの日数を指定します。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。

[DAPエントリの追加/編集（Add/Edit DAP Entry）] ダイアログボックスの AnyConnect ID

ダイナミック アクセス ポリシーの選択基準として AnyConnect ID 属性を設定するには、[DAP エントリの追加/編集（Add/Edit DAP Entry）] ダイアログボックスで AnyConnect ID を選択基準として設定します。ASA は、AnyConnect モバイル クライアントから受信した AnyConnect 識別属性に基づいて DAP エンドポイント属性を生成します。Security Manager を使用して Cisco Secure Desktop がこれらの特定の属性を設定できるようにする必要はありません。

ダイナミック アクセス ポリシーを割り当てる目的で、特定の DAP エントリに複数の AnyConnect アイデンティティ属性を設定した場合、いずれかの属性値が true の場合、エントリは一致と見

なされます。各ダイナミック アクセス ポリシーの AnyConnect アイデンティティ属性の数に制限はありません。

（注） 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のないダイナミック アクセス ポリシーを設定する場合は、すべての選択基準が満たされるため、セキュリティ アプライアンスでは常にそのポリシーが選択されます。

ナビゲーション パス

[Add Dynamic Access Policy]/[Edit Dynamic Access Policy] ダイアログボックス （16 ページ）を開いて [メイン（Main）] タブを選択し、[作成（Create）] をクリックするか、テーブルでダイナミック アクセス ポリシーを選択して [編集（Edit）] をクリックします。[Add DAP Entry]/[Edit DAP Entry] ダイアログボックスが表示されます。基準として [AnyConnectアイデンティティ（AnyConnect Identity）] を選択します。

関連項目

- DAP 属性について （5 ページ）
- DAP 属性の設定 （10 ページ）
- ダイナミック アクセス ポリシーの設定 （3 ページ）

フィールド リファレンス

表 *11 : [DAP*エントリの追加/編集（*Add/Edit DAP Entry*）*]* ダイアログボックスの *AnyConnect ID*

要素	説明
基準	選択基準として [AnyConnectアイデンティティ（AnyConnect Identity）] を表示します。
クライアント バージョン（Client Version）	チェックボックスをオンにし、ドロップダウンリストから一致基準（*is* など）を選択して、AnyConnect クライアントのバージョン番号を入力します。
プラットフォーム	チェックボックスをオンにし、ドロップダウンリストから一致基準（*is*など）を選択して、ドロップダウンリストから適切なプラットフォームを選択します。
プラットフォーム バージョン（Platform Version）	チェックボックスをオンにし、ドロップダウンリストから一致基準（*is*など）を選択して、プラットフォームの適切なバージョン番号を入力します。

要素	説明
デバイスタイプ	チェックボックスをオンにし、ドロップダウンリストから一致基準（*is* など）を選択して、ドロップダウンリストから適切なデバイスタイプを選択します。
デバイス固有 ID	チェックボックスをオンにし、ドロップダウンリストから一致基準（*is* など）を選択して、固有のデバイス ID を入力します。この ID はデバイスを識別し、そのデバイス専用のポリシーを設定できるようにします。

[DAPエントリの追加（Add DAP Entry）、]/[DAPエントリの編集（Edit DAP Entry）] ダイアログボックスのアプリケーション

このダイアログボックスを使用して、ダイナミック アクセス ポリシーのエンドポイント属性としてリモート アクセス接続のタイプを指定します。

（注） 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のないダイナミック アクセス ポリシーを設定する場合は、すべての選択基準が満たされるため、セキュリティ アプライアンスでは常にそのポリシーが選択されます。

ナビゲーション パス

[Add Dynamic Access Policy]/[Edit Dynamic Access Policy] ダイアログボックス （16 ページ）を開いて [メイン（Main）] タブを選択し、[作成（Create）] をクリックするか、テーブルでダイナミック アクセス ポリシーを選択して [編集（Edit）] をクリックします。[Add DAP Entry]/[Edit DAP Entry] ダイアログボックスが表示されます。基準として [アプリケーション（Application）] を選択します。

関連項目

- DAP 属性について （5 ページ）
- DAP 属性の設定 （10 ページ）
- ダイナミック アクセス ポリシーの設定 （3 ページ）

フィールド リファレンス

表 *12*：*[DAP*エントリの追加（*Add DAP Entry*）*]/[DAP*エントリの編集（*Edit DAP Entry*）*]* ダイアログボックスのアプリケーション

要素	説明
基準	選択基準として [Application] が表示されます。

要素	説明
Client Type	チェックボックスをオンにし、ドロップダウンリストから一致基準（*is* または *isn't* など）を選択して、リストからリモートアクセス接続のタイプ（[AnyConnect]、[Clientless]、[Cut-through Proxy]、[IPsec]、[Generic IKEv2 Client]、または [L2TP]）を指定します。 （注） クライアント タイプとして [AnyConnect] を選択した場合は、必ず Cisco Secure Desktop をイネーブルにしてください。Cisco Secure Desktop がイネーブルになっていないと、Security Manager でエラーが生成されます。

[DAPエントリの追加（Add DAP Entry）]/[DAPエントリの編集（Edit DAP Entry）] ダイアログボックス > [デバイス（Device）]

[DAP Device Criterion] では、関連付けられたプリログイン ポリシー チェック中に使用できる特定のデバイス情報を提供できます。[ホスト名（host name）]、[MACアドレス（MAC address）]、[ポート番号（port number）]、[プライバシー保護の選択（Privacy Protection selection）] のうち、1 つ以上のデバイス属性を指定し、属性ごとに照合対象（[is] または [isn't]）を指定できます。

[isn't] は排他的であることに注意してください。たとえば、Host Name isn't zulu_2 という基準を指定した場合、zulu_2 以外の名前のデバイスがすべて一致します。

ナビゲーション パス

[Add Dynamic Access Policy]/[Edit Dynamic Access Policy] ダイアログボックス （16 ページ）を開いて [メイン（Main）] タブを選択し、[作成（Create）] をクリックするか、テーブルでダイナミック アクセス ポリシーを選択して [編集（Edit）] をクリックします。[Add DAP Entry]/[Edit DAP Entry] ダイアログボックスが表示されます。[基準（Criterion）] として [デバイス（Device）] を選択します。

関連項目

- DAP 属性について （5 ページ）
- DAP 属性の設定 （10 ページ）
- ダイナミック アクセス ポリシーの設定 （3 ページ）

フィールド リファレンス

表 *13 : [DAPエントリの追加（Add DAP Entry）]/[DAPエントリの編集（Edit DAP Entry）] ダイアログボックス > [デバイス（Device）]*

要素	説明
基準	選択された [Criterion] として [Device] が表示されます。

要素	説明
ホスト名	このオプションを選択し、関連するドロップダウンリストから一致基準（[is] または [isn't]）を選択して、照合するデバイスホスト名を入力します。
MAC アドレス	このオプションを選択し、関連するドロップダウンリストから一致基準（[is] または [isn't]）を選択して、照合するデバイスの MAC アドレスを入力します。
BIOS シリアル番号	このオプションを選択し、関連するドロップダウンリストから一致基準（[is] または [isn't]）を選択して、照合するデバイスの BIOS シリアル番号値を入力します。数値フォーマットは、製造業者固有です。フォーマット要件はありません。
ポート番号（Port Number）	このオプションを選択し、一致基準（[is] または [isn't]）を選択して、照合するデバイスポートを入力するか、または選択します。
TCP/UDPポート番号（TCP/UDP Port Number）	このオプションを選択し、一致基準（[is] または [isn't]）を選択して、照合するリスニング状態の TCP/UDP ポートを入力するか、または選択します。 TCP/UDP コンボボックスでは、照合対象のポートの種類（TCP（IPv4）、UDP（IPv4）、TCP（IPv6）、または UDP（IPv6））を選択します。バージョン 4.12 以降、Cisco Security Manager では、バージョン 9.0 以降を実行している ASA デバイスの IPv6 アドレスがサポートされています。複数のポートを照合する場合は、DAP の個々のエンドポイント属性ルールを複数作成し、各ルールにポートを 1 つ指定します。
Privacy Protection	このオプションを選択し、一致基準（[is] または [isn't]）を選択し、デバイスで定義されている [プライバシー保護（Privacy Protection）] オプション（[none]、[cache cleaner]、または [secure desktop]）を選択します。
CSDバージョン（CSD Version）	このオプションを選択し、関連するドロップダウンリストから一致基準（[is] または [isn't]）を選択して、エンドポイントで実行中の Host Scan イメージのバージョンを入力します。
エンドポイント評価バージョン（Endpoint Assessment Version）	このオプションを選択し、関連するドロップダウンリストから一致基準（[is] または [isn't]）を選択して、照合するエンドポイント評価（OPSWAT）のバージョンを入力します。

[DAPエントリの追加（Add DAP Entry）]/[DAPエントリの編集（Edit DAP Entry）] ダイアログボックスファイル

ファイル基準プリログイン チェックにより、関連付けられたプリログイン ポリシーに対して適格となる条件として、特定のファイルが存在すること、または存在しないことを指定できます。たとえば、ファイル プリログイン チェックを使用して、プリログイン ポリシーの割り当

て前に、企業ファイルが必ず存在すること、あるいは悪意のあるソフトウェアを含む1つ以上のピアツーピア ファイル共有プログラムが存在してはならないことを指定できます。

（注） 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のないダイナミック アクセス ポリシーを設定する場合は、すべての選択基準が満たされるため、セキュリティ アプライアンスでは常にそのポリシーが選択されます。

ナビゲーション パス

[Add Dynamic Access Policy]/[Edit Dynamic Access Policy] ダイアログボックス （16 ページ）を開いて [メイン（Main）] タブを選択し、[作成（Create）] をクリックするか、テーブルでダイナミック アクセス ポリシーを選択して [編集（Edit）] をクリックします。[Add DAP Entry]/[Edit DAP Entry] ダイアログボックスが表示されます。基準として [ファイル（File）] を選択します。

関連項目

- DAP 属性について （5 ページ）
- DAP 属性の設定 （10 ページ）
- ダイナミック アクセス ポリシーの設定 （3 ページ）

フィールド リファレンス

表 *14 : [DAPエントリの追加（Add DAP Entry）]/[DAPエントリの編集（Edit DAP Entry）] ダイアログボックスファイル*

要素	説明
基準	選択基準として [File] が表示されます。
タイプ（Type）	このエンドポイント属性が、セッションの確立中にダイナミック アクセス ポリシーを選択および適用するために設定した基準と一致する必要があるか、または一致しない必要があるかを指定します。
エンドポイント ID（Endpoint ID）	ファイルのエンドポイントを識別する文字列を選択します。ダイナミック アクセス ポリシーでは、この ID を使用して、ダイナミック アクセス ポリシー選択の 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。
ファイル名	ファイル名を指定します。

要素	説明
Last Update	ダイナミック アクセス ポリシーのエンドポイント属性と一致する基準を選択した場合にだけ使用可能です。 最後の更新からの日数を指定します。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。
チェックサム（Checksum）	DAP レコードのエンドポイント属性と一致する基準を選択した場合にだけ使用可能です。 このチェックボックスをオンにして、ファイルを認証するようにチェックサムを指定し、次に、0x で始まる 16 進形式でチェックサムを入力します。 バージョン 4.7 以降、Security Manager には、ファイルの CRC32 チェックサムを計算するユーティリティが用意されています。[CRC32チェックサムの計算（Compute CRC32 Checksum）] ボタンをクリックして、[チェックサムの計算（Compute Checksum）] ダイアログ ボックスを開きます。[参照（Browse）] をクリックしてファイルブラウザを開き、必要なファイルを選択して [計算（Compute）] ボタンをクリックします。ファイルの CRC32 チェックサムが計算され、[チェックサム（Checksum）] フィールドに入力されます。 （注） Compute CRC32 チェックサムユーティリティでは、クライアント側の参照のみがサポートされています。デフォルトでは、クライアント側の参照が有効になっています。これを無効にすると、[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] を選択し、コンテンツテーブルから [デスクトップのカスタマイズ（Customize Desktop）] を選択します。詳細については、[Customize Desktop] ページを参照してください。

[DAPエントリの追加（Add DAP Entry）]/[DAPエントリの編集（Edit DAP Entry）] ダイアログボックスの [NAC]

NAC は、エンドポイント準拠および脆弱性チェックをネットワークへの実稼働アクセスの条件として実行することにより、ワーム、ウイルス、および不正なアプリケーションの侵入や感染からエンタープライズネットワークを保護します。これらのチェックをポスチャ検証と呼びます。イントラネット上の脆弱なホストにアクセスする前に、ポスチャ検証を設定して、AnyConnect またはクライアントレス SSL VPN セッションを使用するホスト上のアンチウイルス ファイル、パーソナル ファイアウォール ルール、または侵入防御ソフトウェアが最新の状態であることを確認できます。ポスチャ検証の一部として、リモートホストで実行されているアプリケーションが最新のパッチで更新されているか検証することもできます。NACは、ユーザ認証およびトンネルの設定の完了後に行われます。自動ネットワーク ポリシー実施が適用されないホスト（ホームPCなど）からエンタープライズネットワークを保護する場合は、NACが特に有用です。セキュリティ アプライアンスは、Extensible Authentication Protocol（EAP）overUDP（EAPoUDP）メッセージングを使用して、リモートホストのポスチャを検証します。

エンドポイントとセキュリティアプライアンスの間にトンネルが確立されると、ポスチャ検証がトリガーされます。クライアントがポスチャ検証要求に応答しない場合に、クライアントの

IP アドレスを任意指定の監査サーバに渡すように、セキュリティ アプライアンスを設定できます。監査サーバ（Trend サーバなど）では、ホスト IP アドレスを使用して、ホストに対して直接チャレンジを行い、ホストのヘルスを評価します。たとえば、ホストに対してチャレンジを行い、そのウイルス チェック ソフトウェアがアクティブで最新の状態かどうかを判断します。監査サーバは、リモート ホストとの対話を完了すると、リモート ホストのヘルスを示すトークンをポスチャ検証サーバに渡します。

（注） 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のないダイナミック アクセス ポリシーを設定する場合は、すべての選択基準が満たされるため、セキュリティ アプライアンスでは常にそのポリシーが選択されます。

ナビゲーション パス

[Add Dynamic Access Policy]/[Edit Dynamic Access Policy] ダイアログボックス （16 ページ）を開いて [メイン（Main）] タブを選択し、[作成（Create）] をクリックするか、テーブルでダイナミック アクセス ポリシーを選択して [編集（Edit）] をクリックします。[Add DAP Entry]/[Edit DAP Entry] ダイアログボックスが表示されます。[基準（Criterion）] として [NAC] を選択します。

関連項目

- DAP 属性について （5 ページ）
- DAP 属性の設定 （10 ページ）
- ダイナミック アクセス ポリシーの設定 （3 ページ）

フィールド リファレンス

表 *15 : [DAP*エントリの追加（*Add DAP Entry*）*]/[DAP*エントリの編集（*Edit DAP Entry*）*]* ダイアログボックスの *[NAC]*

要素	説明
基準	選択基準として [NAC] が表示されます。
ポスチャ ステータス	ドロップダウンリストから一致基準（[は（is）] など）を選択して、ACS から受け取ったポスチャ トークン文字列を入力します。

[DAPエントリの追加/編集（Add/Edit DAP Entry）] ダイアログボックスの [オペレーティングシステム（Operating System）]

プリログイン評価には、VPN 接続の確立を試行する OS のチェックが含まれます。ただし、ユーザが接続を試行すると、OS プリログイン チェックを挿入したかどうかに関係なく、Cisco Secure Desktop によって OS がチェックされます。

接続に割り当てられているプリログイン ポリシーの Secure Desktop（Secure Session）がイネーブルになっており、かつ、リモート PC で Microsoft Windows XP または Windows 2000 が実行

されている場合は、OS プリログイン チェックを挿入したかどうかに関係なく、Secure Session がインストールされます。プリログイン ポリシーの Secure Desktop がイネーブルになっており、かつ、オペレーティング システムが Microsoft Windows Vista、Mac OS X 10.4、または Linux の場合は、代わりにキャッシュ クリーナが実行されます。このため、キャッシュ クリーナの設定が、Secure Desktop またはキャッシュ クリーナをインストールするように設定したプリログイン ポリシーに対して適切であることを確認する必要があります。Cisco Secure Desktop により OS がチェックされますが、プリログイン ポリシーを適用して OS ごとに後続のチェックを分離するための条件として OS プリログイン チェックを挿入することもできます。

（注） 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のないダイナミック アクセス ポリシーを設定する場合は、すべての選択基準が満たされるため、セキュリティ アプライアンスでは常にそのポリシーが選択されます。

ナビゲーション パス

[Add Dynamic Access Policy]/[Edit Dynamic Access Policy] ダイアログボックス （16 ページ）を開いて [メイン（Main）] タブを選択し、[作成（Create）] をクリックするか、テーブルでダイナミック アクセス ポリシーを選択して [編集（Edit）] をクリックします。[Add DAP Entry]/[Edit DAP Entry] ダイアログボックスが表示されます。[基準（Criterion）] として [オペレーティング システム（Operating System）] を選択します。

関連項目

- DAP 属性について （5 ページ）
- DAP 属性の設定 （10 ページ）
- ダイナミック アクセス ポリシーの設定 （3 ページ）

フィールド リファレンス

表 *16 : [DAPエントリの追加/編集（Add/Edit DAP Entry）] ダイアログボックスの [オペレーティングシステム（Operating System）]*

要素	説明
基準	選択基準として [Operating System] が表示されます。
OS Version	チェックボックスをオンにし、ドロップダウンリストから一致基準（[is] など）を選択して、リストから OS バージョンを選択します。iPhone および同様のデバイスには、[Apple Plugin] を選択します。
サービス パック	チェックボックスをオンにし、ドロップダウンリストから一致基準（[is] など）を選択して、オペレーティングシステムのサービスパックを選択します。

[DAP エントリの追加/編集（Add/Edit DAP Entry）] ダイアログボックスの [パーソナルファイアウォール（Personal Firewall）]

Cisco Secure Desktop インターフェイスで [Host Scan] をクリックして、エンドポイント評価をイネーブルにします。エンドポイント評価は、リモート コンピュータで実行されているパーソナル ファイアウォールのスキャンです。一部を除くほとんどのパーソナル ファイアウォール プログラムでは、アクティブなスキャンがサポートされています。つまり、このようなスキャンでは、プログラムがメモリに常駐するため、常に動作中になります。

（注） 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のないダイナミック アクセス ポリシーを設定する場合は、すべての選択基準が満たされるため、セキュリティ アプライアンスでは常にそのポリシーが選択されます。

重要 パーソナルファイアウォールの基準は、Host Scan バージョン 4.6 より前の場合は **FW**、バージョン 4.6 以降の場合は **PFW** として示されます。

ナビゲーション パス

[Add Dynamic Access Policy]/[Edit Dynamic Access Policy] ダイアログボックス （16 ページ）を開いて [メイン（Main）] タブを選択し、[作成（Create）] をクリックするか、テーブルでダイナミック アクセス ポリシーを選択して [編集（Edit）] をクリックします。[Add DAP Entry]/[Edit DAP Entry] ダイアログボックスが表示されます。[基準（Criterion）] として [AAA属性Cisco（AAA Attributes Cisco）] を選択します。

関連項目

- DAP 属性について （5 ページ）
- DAP 属性の設定 （10 ページ）
- ダイナミック アクセス ポリシーの設定 （3 ページ）

フィールド リファレンス

表 17 : [DAP エントリの追加/編集（Add/Edit DAP Entry）] ダイアログボックスの [パーソナルファイアウォール（Personal Firewall）]

要素	説明
基準	選択基準として [Personal Firewall] が表示されます。

要素	説明
タイプ（Type）	次のいずれかのオプションを選択し、関連する値を割り当てます。 • [未インストール（Not Installed）]：指定されたパーソナルファイアウォールがリモート PC 上にないことを、設定するプリログインポリシーに一致するための十分条件とする場合に選択します。 • [インストール済みで有効（Installed and enabled）]：設定するプリログインポリシーに適合させるために、指定されたパーソナルファイアウォールがリモート PC 上に存在し、有効になっているかどうかを選択します。 • [インストール済みで無効（Installed and disabled）]：指定されたパーソナルファイアウォールがリモート PC 上に単に存在していることを、設定するプリログインポリシーに一致するための十分条件とする場合に選択します。
ベンダー名（Vendor Name）	アプリケーションベンダーを説明するテキストをリストから選択します。
製品 ID	リストから選択したベンダーによってサポートされる製品の固有識別情報を選択します。
製品の説明	このエンドポイント属性とそのすべての設定がリモート PC で使用可能である必要があることを選択した場合にだけ使用可能です。 チェックボックスをオンにし、リストから製品の説明を選択します。
バージョン	このエンドポイント属性とそのすべての設定がリモート PC で使用可能である必要があることを選択した場合にだけ使用可能です。 アプリケーションのバージョンを識別し、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。

[DAPエントリの追加（Add DAP Entry）]/[DAPエントリの編集（Edit DAP Entry）] ダイアログボックスポリシー

Windows ロケーションを使用すると、クライアントとバーチャル プライベート ネットワークとの接続方法を判断して適宜に保護できます。たとえば、NAT デバイスの背後にある 10.x.x.x ネットワークの職場 LAN 内から接続しているクライアントが、機密情報を公開するリスクはほとんどないと考えられます。これらのクライアントに対しては、10.x.x.x ネットワーク上の IP アドレスで指定された Work という名前の Cisco Secure Desktop Windows ロケーションを設定し、このロケーションに対してキャッシュ クリーナと Secure Desktop 機能の両方をディセーブルにします。Cisco Secure Desktop は、[Windows Location Settings] ウィンドウのリスト内の順序でロケーションをチェックし、最初に一致したロケーション定義に基づいてクライアント PC に権限を付与します。

（注） 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のないダイナミック アクセス ポリシーを設定する場合は、すべての選択基準が満たされるため、セキュリティ アプライアンスでは常にそのポリシーが選択されます。

ナビゲーション パス

[Add Dynamic Access Policy]/[Edit Dynamic Access Policy] ダイアログボックス （16 ページ）を開いて [メイン（Main）] タブを選択し、[作成（Create）] をクリックするか、テーブルでダイナミック アクセス ポリシーを選択して [編集（Edit）] をクリックします。[Add DAP Entry]/[Edit DAP Entry] ダイアログボックスが表示されます。基準として [ポリシー（Policy）] を選択します。

関連項目

- DAP 属性について （5 ページ）
- DAP 属性の設定 （10 ページ）
- ダイナミック アクセス ポリシーの設定 （3 ページ）

フィールド リファレンス

表 *18 : [DAP*エントリの追加（*Add DAP Entry*）*]/[DAP*エントリの編集（*Edit DAP Entry*）*]* ダイアログボックスポリシー

要素	説明
基準	選択基準として [Policy] が表示されます。
参照先	ドロップダウンリストから一致基準（[is] など）を選択して、リストから Cisco Secure Desktop Microsoft Windows ロケーションプロファイルを選択します。Cisco Secure Desktop Manager で設定されたすべてのロケーションは、このリストに表示されます。

[DAPエントリの追加（Add DAP Entry）]/[DAPエントリの編集（Edit DAP Entry）] ダイアログボックスの [プロセス（Process）]

基本ホスト スキャンの一部となる一連のプロセス名を指定できます。ホスト スキャンは、基本ホスト スキャンとエンドポイント評価または拡張エンドポイント評価で構成され、プリログイン評価の終了後、ダイナミック アクセス ポリシーの割り当ての前に行われます。基本ホスト スキャンに続いて、セキュリティ アプライアンスはログイン クレデンシャル、ホスト スキャン結果、プリログイン ポリシー、および DAP の割り当て用に設定したその他の基準を使用します。

（注） 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のないダイナミック アクセス ポリシーを設定する場合は、すべての選択基準が満たされるため、セキュリティ アプライアンスでは常にそのポリシーが選択されます。

ナビゲーション パス

[Add Dynamic Access Policy]/[Edit Dynamic Access Policy] ダイアログボックス （16 ページ）を開いて [メイン（Main）] タブを選択し、[作成（Create）] をクリックするか、テーブルでダイナミック アクセス ポリシーを選択して [編集（Edit）] をクリックします。[Add DAP Entry]/[Edit DAP Entry] ダイアログボックスが表示されます。[基準（Criterion）] として [プロセス（Process）] を選択します。

関連項目

- DAP 属性について （5 ページ）
- DAP 属性の設定 （10 ページ）
- ダイナミック アクセス ポリシーの設定 （3 ページ）

フィールド リファレンス

表 *19 : [DAPエントリの追加（Add DAP Entry）]/[DAPエントリの編集（Edit DAP Entry）] ダイアログボックスの [プロセス（Process）]*

要素	説明
基準	選択基準として [Process] が表示されます。
タイプ（Type）	次のいずれかのオプションを選択し、関連する値を割り当てます。 • [一致する（Matches）]：指定されたプロセスがリモート PC 上に存在することだけを、設定するプリログインポリシーと一致していることの十分条件とする場合は、これを選択します。 • [一致しない（Doesn't Match）]：指定されたプロセスがリモート PC 上に存在しないことを、設定するプリログインポリシーに一致していることの十分条件とする場合は、これを選択します。
エンドポイント ID（Endpoint ID）	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示す文字列。ダイナミック アクセス ポリシーでは、この ID を使用して、ダイナミック アクセス ポリシー選択の 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。

要素	説明
パス（Path）	チェックボックスをオンにし、ドロップダウンリストから一致基準（[次に一致する（is）] など）を選択して、プロセスの名前を入力します。これを Microsoft Windows で表示するには、[Windows Task Manager] ウィンドウを開いて [Processes] タブをクリックします。 この属性を設定する前に、[Host Scan] を設定します。[Host Scan] を設定すると、設定がこのペインに表示されるため、DAP を設定する場合にこのエントリをエンドポイント属性として割り当てるとき、この設定を選択して同じインデックスを指定できます。これにより、入力や構文のエラーを減少させることができます。

[DAPエントリの追加/編集（Add/Edit DAP Entry）] ダイアログボックスのレジストリ

レジストリ キー スキャンは、Microsoft Windows オペレーティング システムを実行しているコンピュータにだけ適用されます。基本ホスト スキャンでは、コンピュータで Mac OS または Linux が実行されている場合にレジストリ キー スキャンを無視します。

（注） 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のないダイナミック アクセス ポリシーを設定する場合は、すべての選択基準が満たされるため、セキュリティ アプライアンスでは常にそのポリシーが選択されます。

ナビゲーション パス

[Add Dynamic Access Policy]/[Edit Dynamic Access Policy] ダイアログボックス （16 ページ）を開いて [メイン（Main）] タブを選択し、[作成（Create）] をクリックするか、テーブルでダイナミック アクセス ポリシーを選択して [編集（Edit）] をクリックします。[Add DAP Entry]/[Edit DAP Entry] ダイアログボックスが表示されます。[基準（Criterion）] として [レジストリ（Registry）] を選択します。

関連項目

- DAP 属性について （5 ページ）
- DAP 属性の設定 （10 ページ）
- ダイナミック アクセス ポリシーの設定 （3 ページ）

フィールド リファレンス

表 *20 : [DAP*エントリの追加（*Add DAP Entry*）*]/[DAP*エントリの編集（*Edit DAP Entry*）*]* ダイアログボックスのレジストリ

要素	説明
基準	選択基準として [Registry] が表示されます。

要素	説明
タイプ（Type）	次のいずれかのオプションを選択し、関連する値を割り当てます。 • [一致する（Matches）]：指定されたレジストリキーがリモート PC 上に存在することだけを、設定するプリログインポリシーと一致していることの十分条件とする場合は、これを選択します。たとえば、プリログインポリシーを割り当てるための基準と一致する条件として、HKEY_LOCAL_MACHINE\SOFTWARE\<Protective_Software> というレジストリ キーが存在することを要求する場合は、このオプションを選択します。 • [一致しない（Doesn't Match）]：指定されたレジストリキーがリモート PC 上に存在しないことを、設定するプリログインポリシーに一致していることの十分条件とする場合は、これを選択します。たとえば、プリログインポリシーを割り当てるための基準と一致する条件として、HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\<Evil_SpyWare> というレジストリ キーが存在しないことを要求する場合は、このオプションを選択します。
エンドポイント ID（Endpoint ID）	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示す文字列。ダイナミック アクセス ポリシーでは、この ID を使用して、ダイナミック アクセス ポリシー選択の 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。
Registry Name	レジストリ名を説明するテキストをリストから選択します。
値	リストから [dword] または [string] の値を選択し、一致基準（等しいか等しくないか）を選択します。次に、リモート PC 上のレジストリキーの dword または文字列の値と比較する 10 進数または文字列を入力します。 （注） 「DWORD」は、[レジストリ基準の追加（Add Registry Criterion）]/[レジストリ基準の編集（Edit Registry Criterion）] ダイアログボックス内の属性を参照します。「Dword」は、レジストリキーに表示される属性を参照します。Windows コマンドラインからアクセスできる regedit アプリケーションを使用して、レジストリ キーの Dword 値を確認します。または、このアプリケーションを使用して、Dword 値をレジストリ キーに追加して、設定する要件を満たします。
Ignore Case	選択すると、レジストリエントリ内に文字列が含まれている場合に、大文字と小文字の違いが無視されます。

[DAPエントリの追加（Add DAP Entry）]/[DAPエントリの編集（Edit DAP Entry）] ダイアログボックス > [マルウェア対策（Anti-Malware）]

Host Scan バージョン 4.6 以降では、ウイルス対策（AV）、スパイウェア対策（AS）、およびファイアウォール（FW）基準がサポートされなくなりました。ただし、代わりに 2 つの新し

い基準であるマルウェア対策（AM）とパーソナルファイアウォール（PFW）が追加されており、Host Scan の設定時に使用できます。

Cisco Secure Desktop インターフェイスで [Host Scan] をクリックして、リモートコンピュータで実行されているパーソナルファイアウォールのスキャンであるエンドポイント評価を有効にします。プリログインポリシーおよび Host Scan のオプションの設定に続いて、Host Scan 結果の 1 つまたは任意の組み合わせに関する一致を設定して、ユーザーログイン後のダイナミック アクセス ポリシーに割り当てることができます。

ナビゲーション パス

[Add Dynamic Access Policy]/[Edit Dynamic Access Policy] ダイアログボックス （16 ページ）を開いて [メイン（Main）] タブを選択し、[作成（Create）] をクリックするか、テーブルでダイナミック アクセス ポリシーを選択して [編集（Edit）] をクリックします。[Add DAP Entry]/[Edit DAP Entry] ダイアログボックスが表示されます。[基準（Criterion）] として [マルウェア対策（Anti-Malware）] を選択します。

関連項目

- DAP 属性について （5 ページ）
- DAP 属性の設定 （10 ページ）
- ダイナミック アクセス ポリシーの設定 （3 ページ）

フィールド リファレンス

表 *21 : [DAP*エントリの追加（*Add DAP Entry*）*]/[DAP*エントリの編集（*Edit DAP Entry*）*]* ダイアログボックス *> [*マルウェア対策（*Anti-Malware*）*]*

要素	説明
基準	選択基準として [スパイウェア対策（Anti-Spyware）] が表示されます。
タイプ（Type）	次のいずれかのオプションを選択し、関連する値を割り当てます。 • [未インストール（Not Installed）]：指定されたマルウェア対策がリモート PC 上にないことを、設定するプリログインポリシーに一致するための十分条件とする場合に選択します。 • [インストール済みで有効（Installed and enabled）]：設定するプリログインポリシーと一致させるために、名前付きマルウェア対策がリモート PC 上に存在し、有効になっている必要があるかどうかを選択します。 • [インストール済みで無効（Installed and disabled）]：指定されたマルウェア対策がリモート PC 上に存在していることを、設定するプリログインポリシーに一致するための十分条件とする場合に選択します。

要素	説明
ベンダー名（Vendor Name）	アプリケーション ベンダーを説明するテキストをリストから選択します。
製品 ID	リストから選択したベンダーによってサポートされる製品の固有識別情報を選択します。
製品の説明	ダイナミック アクセス ポリシーのエンドポイント属性と一致する基準を選択した場合にだけ使用可能です。 チェックボックスをオンにし、リストから製品の説明を選択します。
バージョン	ダイナミック アクセス ポリシーのエンドポイント属性と一致する基準を選択した場合にだけ使用可能です。 アプリケーションのバージョンを識別し、エンドポイント属性をそのバージョンに対して次のいずれかにするかどうかを指定します。 • 等しくない • 等しい • より少ない • より大きい • 以下 • 以上
Last Update	ダイナミック アクセス ポリシーのエンドポイント属性と一致する基準を選択した場合にだけ使用可能です。 最後の更新からの日数を指定します。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。

[DAP エントリの追加（Add DAP Entry）]/[DAP エントリの編集（Edit DAP Entry）] ダイアログボックスの [マルチ証明書認証（Multiple Certificate Authentication）]

DAP マルチ証明書認証基準により、関連付けられたプリログイン ポリシー チェック中に使用できる特定のデバイス情報を提供できます。Cisco Security Manager は、リモート VPN ユーザーを認証するための 2 つの証明書をサポートしています。証明書には、サブジェクト、発行者、サブジェクト代替名、シリアル番号、および証明書ストアの 1 つ以上の属性を指定できます。

（注） 証明書オプション以外の DAP エントリを変更できます。

ナビゲーション パス

[Add Dynamic Access Policy]/[Edit Dynamic Access Policy] ダイアログボックス （16 ページ）を開いて [メイン（Main）] タブを選択し、[作成（Create）] をクリックするか、テーブルでダイナミック アクセス ポリシーを選択して [編集（Edit）] をクリックします。[Add DAP Entry]/[Edit DAP Entry] ダイアログボックスが表示されます。[基準（Criterion）] として [マルチ証明書認証（Multiple Certificate Authentication）] を選択します。

関連項目

- DAP 属性について （5 ページ）
- DAP 属性の設定 （10 ページ）
- ダイナミック アクセス ポリシーの設定 （3 ページ）

フィールド リファレンス

表 *22 : [DAP* エントリの追加（*Add DAP Entry*）*]/[DAP* エントリの編集（*Edit DAP Entry*）*]* ダイアログボックスの *[*マルチ証明書認証（*Multiple Certificate Authentication*）*]*

要素	説明
基準	選択基準として [マルチ証明書認証（Multiple Certificate Authentication）] が表示されます。
証明書	4.13 ではマルチ証明書は 2 つの証明書による認証を指します。次のいずれかのオプションを選択し、関連する属性を割り当てます。 • [証明書 1（Cert1）] : 設定しているプリログインポリシーに一致する証明書 1 の詳細を提供する場合に選択します。 • [証明書 2（Cert2）] : 設定しているプリログインポリシーに一致する証明書 2 の詳細を提供する場合に選択します。 （注） 証明書オプションを編集/変更することはできません。

要素	説明
Subject	ドロップダウンリストから、証明書のサブジェクト名からドメイン名（DN）属性フィールドを選択します。 • dnq：ドメイン名修飾子 • fulldn：完全なサブジェクト名 • ser：シリアル番号 • cn：一般名 • i：イニシャル • ou：組織ユニット • sp：州/都道府県 • o：組織 • n：名前 • sn：姓 • t：役職 • uid：ユーザー識別子 • genq：世代識別子 • c：国 • l：市町村名 • gn：名 • ea：電子メールアドレス 隣のテキストボックスに、選択したサブジェクトの DAP エントリ値を入力します。 （注） テキストボックスを空白のままにすると、保存時にエラーメッセージが表示されます。

要素	説明
発行元（Issuer）	ドロップダウンリストから、証明書の発行元名からドメイン名（DN）属性フィールドを選択します。 • dnq：ドメイン名修飾子 • fulldn：完全な発行元名 • ser：シリアル番号 • cn：一般名 • i：イニシャル • ou：組織ユニット • sp：都道府県 • o：組織 • n：名前 • sn：姓 • t：役職 • uid：ユーザー識別子 • genq：世代識別子 • c：国 • l：局所性 • gn：名 • ea：電子メールアドレス 隣のテキストボックスに、選択した発行元の DAP エントリ値を入力します。 （注） テキストボックスを空白のままにすると、保存時にエラーメッセージが表示されます。
Subject Alternate Name	シリアル番号を設定するには、このドロップダウンリストから [upn] を選択します。隣のテキストボックスに、証明書の [サブジェクト代替名（Subject Alt Name）] フィールドからのユーザープリンシパル名を入力します。
シリアル番号	照合する証明書のシリアル番号を入力します。この値は 16 進数（0 ～ 9 および A ～ F の組み合わせ）である必要があります。 （注） 16 進数以外を入力すると、保存時にエラーメッセージが表示されます。

要素	説明
証明書のストア	認証用の証明書がある関連ストアを選択します。 • [なし（None）]：証明書のタイプが分からない場合に選択します。 • [マシン（Machine）]：証明書がマシンに関連する（特権プロセスでのみアクセス可能）場合に選択します。証明書 1 と証明書 2 の両方にこのオプションを選択することはできません。 • [ユーザー（User）]：証明書がユーザーログインに関連する（ログインしたユーザーが所有するプロセスでのみアクセス可能）場合に選択します。 （注） Windows の場合、ストアは a）1 つのマシンと 1 人のユーザーまたは b）2 人のユーザーです。Windows 以外のプラットフォームの場合、常に 2 つのユーザー証明書が表示されます。

[論理的な操作（Logical Operators）] タブ

[ダイナミックアクセスポリシーの追加（Add Dynamic Access Policy）]/[ダイナミックアクセスポリシーの編集（Edit Dynamic Access Policy）] ダイアログボックスの [論理的な操作（Logical Operators）] タブを使用して、AAA の複数のインスタンスと、[DAPエントリ（DAP Entry）] ダイアログボックスで定義したエンドポイント属性の各タイプを設定します。このタブで、エンドポイント属性または AAA 属性の各タイプについて、タイプのインスタンスの 1 つのみを必要とするか（[Match Any] = OR）か、またはタイプのすべてのインスタンス（[Match All] = AND）を必要とするかを設定します。

- 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。
- エンドポイント属性によっては、複数のインスタンスを設定しても有用でない場合があります。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。

ナビゲーション パス

[Add Dynamic Access Policy]/[Edit Dynamic Access Policy] ダイアログボックス （16 ページ）を開き、[論理的な操作（Logical Operators）] タブをクリックします。

関連項目

- DAP 属性について （5 ページ）
- DAP 属性の設定 （10 ページ）

• ダイナミック アクセス ポリシーの設定 （3 ページ）

フィールド リファレンス

表 *23 : [ダイナミックアクセスポリシーの追加（Add Dynamic Access Policy）]/[ダイナミックアクセスポリシーの編集（Edit Dynamic Access Policy）]* ダイアログボックスの *[論理的な操作（Logical Operators）]* タブ

要素	説明
AAA	ダイナミック アクセス ポリシー内に AAA 属性を定義した場合は、次のいずれかのオプションを選択します。 • [Match Any]：属性間に OR 関係を作成します。基準のいずれかに一致する属性が、フィルタに追加されます。セキュリティ アプライアンスは、属性のいずれか1つがすべての基準に一致していても、特定のユーザに対して、特定のセッションへのアクセスを許可します。 • [Match All]：属性間に AND 関係を作成します。セキュリティ アプライアンスは、属性がすべての基準に一致している場合にだけ、特定のユーザに対して、特定のセッションへのアクセスを許可します。 • [Match None]：属性間に NOT 関係を作成します。ダイナミック アクセス ポリシーは、セッションへのアクセスを許可するために、ユーザの属性のいずれも一致する必要がないことを指定します。
Anti-Spyware	エンドポイント属性として [Anti-Spyware] を定義した場合は、次のいずれかのオプションを選択します。 • [Match Any]：属性間に OR 関係を作成します。基準のいずれかのインスタンスに一致するポリシーが、ユーザの認可に使用されます。 • [Match All]：属性間に AND 関係を作成します。すべての基準に一致する属性だけが、ユーザの認可に使用されます。
ウイルス対策	エンドポイント属性として [Anti-Virus] を定義した場合は、次のいずれかのオプションを選択します。 • [Match Any]：ユーザ認可属性が、設定しているアンチウイルス エンドポイント属性のいずれかの値と一致する必要があることを設定します。 • [Match All]：ユーザ認可属性が、設定しているエンドポイント属性のすべての値と一致し、AAA 属性も満たす必要があることを設定します。

要素	説明
Application	エンドポイント属性として [Application] を定義した場合は、次のいずれかのオプションを選択します。 • [Match Any]：ユーザ認可属性が、設定しているアンチウイルスエンドポイント属性のいずれかの値と一致する必要があることを設定します。 • [Match All]：ユーザ認可属性が、設定しているエンドポイント属性のすべての値と一致し、AAA 属性も満たす必要があることを設定します。
ファイル（File）	エンドポイント属性として [File] を定義した場合は、次のいずれかのオプションを選択します。 • [Match Any]：ユーザ認可属性が、設定しているアンチウイルスエンドポイント属性のいずれかの値と一致する必要があることを設定します。 • [Match All]：ユーザ認可属性が、設定しているエンドポイント属性のすべての値と一致し、AAA 属性も満たす必要があることを設定します。
Personal Firewall	パーソナル ファイアウォール ルールを使用すると、ファイアウォールが許可またはブロックするアプリケーションおよびポートを指定できます。エンドポイント属性として [Personal Firewall] を定義した場合は、次のいずれかのオプションを選択します。 • [Match Any]：ユーザ認可属性が、設定しているアンチウイルスエンドポイント属性のいずれかの値と一致する必要があることを設定します。 • [Match All]：ユーザ認可属性が、設定しているエンドポイント属性のすべての値と一致し、AAA 属性も満たす必要があることを設定します。
プロセス	エンドポイント属性として [Process] を定義した場合は、次のいずれかのオプションを選択します。 • [Match Any]：ユーザ認可属性が、設定しているアンチウイルスエンドポイント属性のいずれかの値と一致する必要があることを設定します。 • [Match All]：ユーザ認可属性が、設定しているエンドポイント属性のすべての値と一致し、AAA 属性も満たす必要があることを設定します。

要素	説明
レジストリ	レジストリ キー スキャンは、Microsoft Windows オペレーティング システムを実行しているコンピュータにだけ適用されます。基本ホスト スキャンでは、コンピュータで Mac OS または Linux が実行されている場合にレジストリ キー スキャンを無視します。 エンドポイント属性として [Registry] を定義した場合は、次のいずれかのオプションを選択します。 • [Match Any]：ユーザ認可属性が、設定しているアンチウイルス エンドポイント属性のいずれかの値と一致する必要があることを設定します。 • [Match All]：ユーザ認可属性が、設定しているエンドポイント属性のすべての値と一致し、AAA 属性も満たす必要があることを設定します。

[Advanced Expressions] タブ

[Add Dynamic Access Policy]/[Edit Dynamic Access Policy] ダイアログボックスの [Advanced Expressions] タブを使用して、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。各タイプのエンドポイント属性の複数のインスタンスを設定できます。これは、LUA（www.lua.org）の知識を必要とする高度な機能であることに注意してください。

ナビゲーション パス

[Add Dynamic Access Policy]/[Edit Dynamic Access Policy] ダイアログボックス （16 ページ）を開き、[拡張表現（Advanced Expressions）] タブをクリックします。

関連項目

- DAP 属性について （5 ページ）
- DAP 属性の設定 （10 ページ）
- ダイナミック アクセス ポリシーの設定 （3 ページ）

フィールド リファレンス

表 *24 : [ダイナミックアクセスポリシーの追加/編集（Add/Edit Dynamic Access Policy）] ダイアログボックス > [拡張表現（Advanced Expressions）] タブ*

要素	説明
Basic Expressions	このテキスト ボックスには、ダイナミック アクセス ポリシー内に設定したエンドポイント属性および AAA 属性に基づいて基本表現が入力されます。

要素	説明
[Relationship] ドロップダウン リスト	基本選択ルールと、このタブに入力した論理式の間の関係を指定します。つまり、新しい属性を、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追加するか、それとも置き換えるかを指定します。次のオプションのいずれかを選択します。 • [基本AND拡張（Basic AND Advanced）]：基本表現と拡張表現の間に AND 関係を作成します。ダイナミック アクセス ポリシー内で定義されている基本表現と拡張表現の両方が、ユーザの認証中に考慮されます。 デフォルトでは、このオプションが選択されています。 • [基本OR拡張（Basic OR Advanced）]：基本表現と拡張表現の間に OR 関係を作成します。ダイナミック アクセス ポリシー内の基本表現または拡張表現のいずれかがユーザ ポリシーに一致すると、ユーザはセッションへのアクセスを許可されます。 • [基本のみ（Basic Only）]：DAP エントリ内に定義されている基本表現だけを使用して、セキュリティアプライアンスが特定のセッションに対するアクセスをユーザーに許可するかどうかが決定されます。 • [拡張のみ（Advanced Only）]：DAP エントリ内に定義されている拡張表現だけを使用して、SSL VPN セッションに対してユーザーが認可されます。
Advanced Expressions	1 つ以上の論理式を入力して、上記の [AAA] および [Endpoint] 領域で設定できない AAA 属性またはエンドポイント属性を設定します。 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。ここで入力したテキストは、Security Manager によって検証されず、ダイナミック アクセス ポリシーの XML ファイルにコピーされるだけです。このテキストはセキュリティアプライアンスによって処理され、解析できない表現はすべて廃棄されます。

[Cisco Secure Desktop Manager Policy Editor] ダイアログボックス

[Cisco Secure Desktop Manager (CSDM) Policy Editor] ダイアログボックスを使用して、プリログイン ポリシーの設定、ユーザがセキュリティ アプライアンスとの接続を確立してからログイン クレデンシャルを入力するまでの間に実行されるチェックの指定、およびホスト スキャンの設定を実行できます。ASA デバイスでの CSD の設定の詳細については、ASA デバイスでの Cisco Secure Desktop ポリシーの設定 （12 ページ）を参照してください。

（注） Cisco Secure Desktop Manager Policy Editor は、独立したプログラムです。CSD の設定および CSD の機能については、https://www.cisco.com/c/ja_jp/products/index.html で入手できる資料を参照してください。具体的には、プリログイン ポリシーおよびホスト スキャンの設定に関する情報を参照してください。設定する CSD バージョンのコンフィギュレーション ガイドを選択してください。

ナビゲーション パス

[Dynamic Access] ページ（ASA） （14 ページ）を開き、[Cisco Secure Desktop] セクションから [設定（Configure）] をクリックします（最初に CSD パッケージを指定する必要があります）。[CSDM Policy Editor] ダイアログボックスが表示されます。

関連項目

- DAP 属性について （5 ページ）
- DAP 属性の設定 （10 ページ）
- ダイナミック アクセス ポリシーの設定 （3 ページ）

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。