SSL ルールを使用したトラフィック復号の調整

ASA FirePOWER モジュールで検査されるすべての暗号化トラフィックには、基本的な SSL ルールに基づいたアクションが適用されます。暗号化トラフィックをより詳細に復号および制御するには、特定タイプのトラフィックの処理およびログ記録を制御するルール条件を設定します。各 SSL ルールには 0 個、1 個、または複数の条件を設定できますが、トラフィックに SSL ルールが適用されるのは、そのルールのすべての条件にトラフィックが一致する場合のみです。

(注) トラフィックがルールに一致すると、ASA FirePOWER モジュールはそのルールのアクションをトラフィックに適用します。ログの記録が指定されている場合、接続が終了した時点でトラフィックに関するログが記録されます。詳細については、ルール アクションを使用した暗号化トラフィックの処理と検査の決定（16-9 ページ）およびアクセス コントロールの処理に基づく接続のロギング（36-11 ページ）を参照してください。

各ルール条件には、照合するトラフィックのプロパティを 1 つまたは複数指定できます。たとえば、以下のプロパティを指定できます。

- 通過するセキュリティ ゾーン、IP アドレスおよびポート、送信元または宛先の国などのトラフィック フロー
- 検出された IP アドレスに関連付けられたユーザ
- トラフィックで検出されたアプリケーションなどのトラフィック ペイロード
- 接続の暗号化に使用された SSL/TLS プロトコル バージョン、暗号スイート、サーバ証明書などの接続暗号化
- サーバ証明書の識別名に指定された URL のカテゴリおよびレピュテーション

詳細については、次の項を参照してください。

- SSL ルールによる復号可能接続のロギング（36-16 ページ）
- ネットワークベースの条件による暗号化トラフィックの制御（17-2 ページ）
- レピュテーションによる暗号化トラフィックの制御（17-8 ページ）
- サーバ証明書の特性に基づいたトラフィック制御（17-19 ページ）

ネットワークベースの条件による暗号化トラフィックの制御

ライセンス:任意（Any）

*SSL ポリシー*に追加する SSL *ルール*により、暗号化トラフィックの処理やログ記録を詳細に制御できます。ネットワークベースの条件を使用して、ネットワークを通過する暗号化トラフィックを管理できます。以下の条件を使用できます。

- 送信元と宛先セキュリティ ゾーン
- 送信元と宛先 IP アドレスまたは地理的位置
- 送信元と宛先のポート

ネットワークベースの複数の条件を組み合わせたり、他のタイプの条件と組み合わせたりして、SSL ルールを作成できます。これらの SSL ルールは単純にも複雑にも設定でき、複数の条件を使用してトラフィックを照合および検査できます。SSL ルールの詳細については、SSL ルールの準備（16-1 ページ）を参照してください。

詳細については、次の項を参照してください。

- ネットワーク ゾーンによる暗号化トラフィックの制御（17-2 ページ）
- ネットワークまたは地理的位置による暗号化トラフィックの制御（17-4 ページ）
- ポートによる暗号化トラフィックの制御（17-6 ページ）

ネットワーク ゾーンによる暗号化トラフィックの制御

ライセンス:任意（Any）

SSL ルールでゾーン条件を設定すると、暗号化トラフィックの送信元および宛先のセキュリティ ゾーンに応じてそのトラフィックを制御できます。

*セキュリティ ゾーン*は、1 つ以上のインターフェイスのグループです。*検出モード*と呼ばれる、デバイスの初期セットアップ時に選択するオプションによって、ASA FirePOWER モジュールが最初にデバイスのインターフェイスをどのように設定するか、およびこれらのインターフェイスがセキュリティ ゾーンに属するかどうかが決定します。

単純な例として、**インライン**検出モードを選択したデバイスでは、ASA FirePOWER モジュールにより内部と外部の 2 つのゾーンが作成され、そのデバイスの最初のインターフェイスのペアがそれらのゾーンに割り当てられます。内部側のネットワークに接続されたホストは、保護されている資産を表します。

ヒント　内部（または外部）のすべてのインターフェイスを 1 つのゾーンにグループ化する必要はありません。導入ポリシーおよびセキュリティ ポリシーが意味をなすグループ化を選択します。ゾーン作成の詳細については、セキュリティ ゾーンの操作（3-37 ページ）を参照してください。

この展開では、これらのホストにインターネットへの無制限アクセスを提供できますが、着信する暗号化トラフィックを復号および検査してホストを保護しなければなりません。

SSL インスペクションでこれを実現するには、[宛先ゾーン（Destination Zone）] を [内部（Internal）] に設定したゾーン条件を SSL ルールに定義します。この単純な SSL ルールでは、内部ゾーンのいずれかのインターフェイスからデバイスを離れるトラフィックが照合されます。

より複雑なルールを作成する場合は、1 つのゾーン条件で [送信元ゾーン（Source Zones）] および [宛先ゾーン（Destination Zones）] それぞれに対し、最大 50 のゾーンを追加できます。

- 特定のゾーンのインターフェイスからデバイスを*離れる*暗号化トラフィックを照合するには、そのゾーンを [宛先ゾーン（Destination Zones）] に追加します。

  パッシブに展開されたデバイスはトラフィックを送信しないため、パッシブなインターフェイスで構成されるゾーンを [宛先ゾーン（Destination Zones）] 条件で使用することはできません。

- 特定のゾーンのインターフェイスからデバイスに*入る*暗号化トラフィックを照合するには、そのゾーンを [送信元ゾーン（Source Zones）] に追加します。

送信元ゾーン条件と宛先ゾーン条件の両方をルールに追加する場合、一致するトラフィックは指定された送信元ゾーンの 1 つから発生し、宛先ゾーンの 1 つを通って出力する必要があります。

ゾーン内のすべてのインターフェイスが同じタイプ（インライン、パッシブ、スイッチド、またはルーテッド）である必要があるため、SSL ルールのゾーン条件で使用されているすべてのゾーンが同じタイプでなければならないことに注意してください。つまり、異なるタイプのゾーンを送信元/宛先とする暗号化トラフィックを照合する単一ルールを定義することはできません。

ゾーンにインターフェイスが含まれていないなど、無効な設定が検出されると、警告アイコンが表示されます。アイコンの上にポインタを置くと詳細が表示されます。

ゾーン条件に基づいて暗号化トラフィックを制御するには、次の手順を実行します。

手順 1　ゾーンに応じた暗号化トラフィック制御を設定する SSL ポリシーで、新しい SSL ルールを作成するか既存のルールを編集します。

詳細な手順については、SSL ルールの概要と作成（16-4 ページ）を参照してください。

手順 2　SSL ルール エディタで、[ゾーン（Zones）] タブを選択します。

[ゾーン（Zones）] タブが表示されます。

手順 3　[利用可能なゾーン（Available Zones）] から追加するゾーンを見つけて選択します。

追加するゾーンを検索するには、[利用可能なゾーン（Available Zones）] リストの上にある [名前で検索（Search by name）] プロンプトをクリックし、ゾーン名を入力します。入力すると、リストが更新されて一致するゾーンが表示されます。

クリックすると、ゾーンを選択できます。複数のゾーンを選択するには、Shift キーおよび Ctrl キーを使用するか、または右クリックして [すべて選択（Select All）] を選択します。

手順 4　[送信元に追加（Add to Source）] または [宛先に追加（Add to Destination）] をクリックして、選択したゾーンを適切なリストに追加します。

選択したゾーンをドラッグ アンド ドロップすることもできます。

手順 5　ルールを保存するか、編集を続けます。

変更を反映させるには、その SSL ポリシーに関連付けたアクセス コントロール ポリシーを適用する必要があります（設定変更の展開（4-13 ページ）を参照してください）。

ネットワークまたは地理的位置による暗号化トラフィックの制御

ライセンス：任意（Any）

SSL ルールでネットワーク条件を設定すると、暗号化トラフィックの送信元および宛先の IP アドレスに応じてそのトラフィックを制御および復号できます。次のいずれかの操作を実行できます。

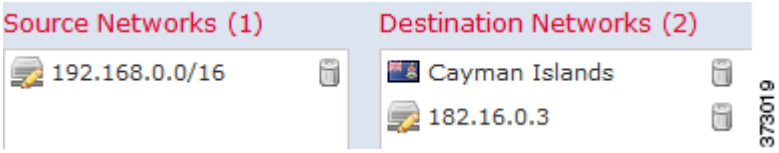
- 制御する暗号化トラフィックの送信元および宛先の IP アドレスを明示的に指定する。
- IP アドレスを地理的位置に関連付ける位置情報機能を使用して、その送信元または宛先の国または大陸に基づいて暗号化トラフィックを制御する。

ネットワークベースの SSL ルールの条件を作成する場合、IP アドレスと地理的位置を手動で指定できます。または、再利用可能で名前を 1 つ以上の IP アドレス、アドレス ブロック、国、大陸などに関連付けるネットワーク オブジェクトおよび位置情報*オブジェクト*を使用してネットワーク条件を設定できます。

ヒント　ネットワーク オブジェクトや位置情報オブジェクトを作成しておくと、それを使用して SSL ルールを作成したり、モジュール インターフェイスのさまざまな場所で IP アドレスを表すオブジェクトとして使用したりできます。これらのオブジェクトはオブジェクト マネージャを使用して作成できます。また、SSL ルールの設定時にネットワーク オブジェクトをオンザフライで作成することもできます。詳細については、再使用可能オブジェクトの管理（3-1 ページ）を参照してください。

地理的位置別にトラフィックを制御するルールを作成する場合は、確実に最新の位置情報データを使用してトラフィックをフィルタ処理する必要があります。このため、Cisco では ASA FirePOWER モジュールの位置情報データベース（GeoDB）を定期的に更新することを**強く**推奨しています。位置情報データベースの更新（46-22 ページ）を参照してください。

次の図は、内部ネットワークから発信され、ケイマン諸島（Cayman Islands）または海外にある持ち株会社のサーバ（182.16.0.3）のリソースにアクセスしようとする暗号化接続をブロックする SSL ルールのネットワーク条件を示しています。



この例では、持ち株会社のサーバの IP アドレスを手動で指定し、ケイマン諸島の IP アドレスを表す ASA FirePOWER モジュール提供の位置情報オブジェクト Cayman Islands を使用しています。

1 つのネットワーク条件で [送信元ネットワーク（Source Networks）] および [宛先ネットワーク（Destination Networks）] それぞれに対し、最大 50 の項目を追加でき、ネットワークベースの設定と位置情報ベースの設定を組み合わせることができます。

- 特定の IP アドレスまたは地理的位置*からの*暗号化トラフィックを照合するには、[送信元ネットワーク（Source Networks）] を設定します。
- 特定の IP アドレスまたは地理的位置*への*暗号化トラフィックを照合するには、[宛先ネットワーク（Destination Networks）] を設定します。

送信元（Source）ネットワーク条件と宛先（Destination）ネットワーク条件の両方をルールに追加する場合、送信元 IP アドレスから発信され**かつ**宛先 IP アドレスに送信される暗号化トラフィックの照合を行う必要があります。

ネットワーク条件を作成する際、警告アイコンは無効な設定を示します。アイコンの上にポインタを置くと詳細が表示されます。

ネットワークまたは地理的位置別にトラフィックを制御するには、次の手順を実行します。

アクセス：Admin/Access Admin/Network Admin

手順 1　ネットワークに応じた暗号化トラフィック制御を設定する SSL ポリシーで、新しい SSL ルールを作成するか既存のルールを編集します。

詳細な手順については、SSL ルールの概要と作成（16-4 ページ）を参照してください。

手順 2　SSL ルール エディタで、[ネットワーク（Networks）] タブを選択します。

[ネットワーク（Networks）] タブが表示されます。

手順 3　[利用可能なネットワーク（Available Networks）] から、次のように追加するネットワークを見つけて選択します。

- 追加するネットワーク オブジェクトとグループを表示するには [ネットワーク（Networks）] タブをクリックします。位置情報オブジェクトを表示するには [位置情報（Geolocation）] タブをクリックします。
- ここでネットワーク オブジェクトを作成してリストに追加するには、[利用可能なネットワーク（Available Networks）] リストの上にある追加アイコン（⊕）をクリックし、ネットワーク オブジェクトの操作（3-4 ページ）の手順に従います。
- 追加するネットワーク オブジェクトまたは位置情報オブジェクトを検索するには、適切なタブを選択し、[利用可能なネットワーク（Available Networks）] リストの上にある [名前または値で検索（Search by name or value）] プロンプトをクリックして、オブジェクトのコンポーネントの 1 つのオブジェクト名または値を入力します。入力すると、リストが更新されて一致するオブジェクトが表示されます。

オブジェクトを選択するには、そのオブジェクトをクリックします。複数のオブジェクトを選択するには、Shift キーおよび Ctrl キーを使用するか、または右クリックして [すべて選択（Select All）] を選択します。

手順 4　[送信元に追加（Add to Source）] または [宛先に追加（Add to Destination）] をクリックして、選択したオブジェクトを適切なリストに追加します。

選択したオブジェクトをドラッグ アンド ドロップすることもできます。

手順 5　手動で指定する送信元または宛先 IP アドレスまたはアドレス ブロックを追加します。

[送信元ネットワーク（Source Networks）] リストまたは [宛先ネットワーク（Destination Networks）] リストの下にある [IP アドレスの入力（Enter an IP address）] プロンプトをクリックし、1 つの IP アドレスまたはアドレス ブロックを入力して [追加（Add）] をクリックします。

手順 6　ルールを保存するか、編集を続けます。

変更を反映させるには、その SSL ポリシーに関連付けたアクセス コントロール ポリシーを適用する必要があります（設定変更の展開（4-13 ページ）を参照してください）。

ポートによる暗号化トラフィックの制御

ライセンス：任意（Any）

SSL ルールでポート条件を設定すると、暗号化トラフィックの送信元および宛先の TCP ポートに応じてそのトラフィックを制御できます。ポートベースの SSL ルールの条件を作成するときは、手動で TCP ポートを指定できます。または、再利用可能で名前を 1 つ以上のポートに関連付けるポート *オブジェクト*を使用してポート条件を設定できます。

ヒント　ポート オブジェクトを作成しておくと、それを使用して SSL ルールを作成したり、モジュール インターフェイスのさまざまな場所でポートを表すオブジェクトとして使用したりできます。ポート オブジェクトは、オブジェクト マネージャを使用して作成できます。また、SSL ルールの設定時に作成することもできます。詳細については、ポート オブジェクトの操作（3-10 ページ）を参照してください。

1 つのネットワーク条件で [選択した送信元ポート（Selected Source Ports）] および [選択した宛先ポート（Selected Destination Ports）] それぞれに対し、最大 50 の項目を追加できます。

- 特定の TCP ポートからの暗号化トラフィックを照合するには、[選択した送信元ポート（Selected Source Ports）] を設定します。
- 特定の TCP ポートへの暗号化トラフィックを照合するには、[選択した宛先ポート（Selected Destination Ports）] を設定します。
- [選択した送信元ポート（Selected Source Ports）] および [選択した宛先ポート（Selected Destination Ports）] の両方を設定すると、特定の送信元（Source）TCP ポートから発信されかつ特定の宛先（Destination）TCP ポートに送信される暗号化トラフィックが照合されます。

[選択した送信元ポート（Selected Source Ports）] および [選択した宛先ポート（Selected Destination Ports）] リストで設定できるのは TCP ポートだけです。非 TCP ポートを含んでいるポート オブジェクトは、[使用可能なポート（Available Ports）] リストでグレー表示されます。

ポート条件を作成する際、警告アイコンは無効な設定を示します。たとえば、オブジェクト マネージャを使用して使用中のポート オブジェクトを編集し、それらのオブジェクト グループを使用するルールを無効にできます。アイコンの上にポインタを置くと詳細が表示されます。

ポート別にトラフィックを制御するには、次の手順を実行します。

手順 1　TCP ポートに応じた暗号化トラフィック制御を設定する SSL ポリシーで、新しい SSL ルールを作成するか既存のルールを編集します。

詳細な手順については、SSL ルールの概要と作成（16-4 ページ）を参照してください。

手順 2　SSL ルール エディタで、[ポート（Ports）] タブを選択します。

[ポート（Ports）] タブが表示されます。

手順 3　[使用可能なポート（Available Ports）] で、追加する TCP ポートを選択します。

- ここで TCP ポート オブジェクトを作成してリストに追加するには、[使用可能なポート（Available Ports）] リストの上にある追加アイコン（⊕）をクリックし、ポート オブジェクトの操作（3-10 ページ）の手順に従います。
- 追加する TCP ベースのポート オブジェクトおよびグループを検索するには、[使用可能なポート（Available Ports）] リストの上にある [名前または値で検索（Search by name or value）] プロンプトをクリックし、オブジェクトの名前またはオブジェクトのポートの値を入力します。入力すると、リストが更新されて一致するオブジェクトが表示されます。たとえば、「443」と入力すると、ASA FirePOWER モジュール提供の HTTPS ポート オブジェクトが ASA FirePOWER モジュールに表示されます。

TCP ベースのポート オブジェクトをクリックして選択します。複数の TCP ベースのポート オブジェクトを選択するには、Shift キーまたは Ctrl キーを使用します。または、右クリックして [すべて選択（Select All）] を選択します。非 TCP ベースのポートを含んでいるオブジェクトは、ポート条件に追加できません。

手順 4　[送信元に追加（Add to Source）] または [宛先に追加（Add to Destination）] をクリックして、選択したオブジェクトを適切なリストに追加します。

選択したオブジェクトをドラッグ アンド ドロップすることもできます。

手順 5　送信元または宛先のポートを手動で指定するには、[選択した送信元ポート（Selected Source Ports）] または [選択した宛先ポート（Selected Destination Ports）] リストの下にある [ポート（Port）] にポート番号を入力します。0 ～ 65535 の値を持つ 1 つのポートを指定できます。

手順 6　[追加（Add）] をクリックします。

ASA FirePOWER モジュールでは、無効なポート設定はルール条件に追加されません。

手順 7　ルールを保存するか、編集を続けます。

変更を反映させるには、その SSL ポリシーに関連付けたアクセス コントロール ポリシーを適用する必要があります（設定変更の展開（4-13 ページ）を参照してください）。

ユーザ ベースの暗号化トラフィックの制御

ライセンス：Control

SSL ルールでユーザ条件を設定すると、Microsoft Active Directory サーバから取得されるユーザに応じてそのトラフィックを制御できます。SSL ルールのユーザ条件では、ホストにログインする LDAP ユーザに基づいてトラフィックのネットワーク通過を許可するユーザ*制御*が可能になります。

ユーザ制御は、*アクセス コントロールされたユーザ*と IP アドレスを関連付けることによって機能します。展開されたエージェントは、ホストにログインまたはホストからログアウトするとき、または他の理由で Active Directory クレデンシャルで認証する場合に、指定されたユーザをモニタします。たとえば、組織は一元化された認証のために Active Directory に依存するサービスまたはアプリケーションを使用できます。

ユーザ条件を設定した SSL ルールとトラフィックを一致させるには、モニタ対象のセッションにおける送信元または宛先ホストの IP アドレスと、ログインするアクセス コントロールされたユーザを関連付ける必要があります。個々のユーザまたはユーザが属しているグループに基づいてトラフィックを制御できます。

複数のユーザ条件を組み合わせたり、他のタイプの条件と組み合わせたりして、SSL ルールを作成できます。これらの SSL ルールは単純にも複雑にも設定でき、複数の条件を使用してトラフィックを照合および検査できます。SSL ルールの詳細については、SSL ルールの概要と作成（16-4 ページ）を参照してください。

ユーザ制御機能を使用するには、Control ライセンスが必要です。また、サポートされるのは LDAP ユーザとグループ（*アクセス コントロールされたユーザ*）だけで、Microsoft Active Directory サーバをモニタするユーザ エージェントからのログインおよびログアウト レコードが使用されます。

ユーザ条件を含む SSL ルールを作成する前に、組織内の少なくとも 1 つの Microsoft Active Directory サーバとASA FirePOWER モジュールとの間の接続を設定しておく必要があります。この設定は認証オブジェクトと呼ばれ、サーバの接続設定と認証フィルタ設定が含まれています。また、ユーザ条件で使用できるユーザも指定されます。

さらに、ユーザ エージェントをインストールする必要もあります。エージェントは、Active Directory クレデンシャルで認証するユーザをモニタし、このようなログインのレコードを ASA FirePOWER モジュールに送信します。これらのレコードによりユーザが IP アドレスに関連付けられ、これに基づいてユーザ条件を含んでいる SSL ルールがトリガー可能になります。

ユーザ条件に基づいて暗号化トラフィックを制御するには、次の手順を実行します。

手順 1　ユーザに応じた暗号化トラフィック制御を設定する SSL ポリシーで、新しい SSL ルールを作成するか既存のルールを編集します。

詳細な手順については、SSL ルールの概要と作成（16-4 ページ）を参照してください。

手順 2　SSL ルール エディタで、[ユーザ（Users）] タブを選択します。

[ユーザ（Users）] タブが表示されます。

手順 3　追加するユーザを検索するには、[使用可能なユーザ（Available Users）] リストの上にある [名前または値で検索（Search by name or value）] プロンプトをクリックし、ユーザ名を入力します。入力を開始するとリストが更新され、一致するユーザが表示されます。

ユーザをクリックして選択します。複数のユーザを選択するには、Shift キーまたは Ctrl キーを使用します。すべてのユーザを選択するには、右クリックして [すべて選択（Select All）] を選択します。

手順 4　[ルールに追加（Add to Rule）] をクリックして、選択したユーザを [選択されたユーザ（Selected Users）] リストに追加します。

選択したユーザをドラッグ アンド ドロップでリストに追加することもできます。

手順 5　ルールを保存するか、編集を続けます。

変更を反映させるには、その SSL ポリシーに関連付けたアクセス コントロール ポリシーを適用する必要があります（設定変更の展開（4-13 ページ）を参照してください）。

レピュテーションによる暗号化トラフィックの制御

ライセンス：Control または URL Filtering

SSL ルールでレピュテーション ベース条件を設定すると、ネットワーク トラフィックをコンテキスト化して状況に応じて制限することで、ネットワーク通過を許可する暗号化トラフィックを管理できます。SSL ルールでのレピュテーション ベースの制御には、以下のタイプがあります。

- アプリケーション条件による *アプリケーション制御*では、個々のアプリケーションだけでなく、アプリケーションの基本的な特性（タイプ、リスク、ビジネスとの関連性、およびカテゴリ）に基づいてアプリケーション トラフィックを制御できます。
- URL 条件では、Web サイトに割り当てられたカテゴリおよびレピュテーションに基づいて Web トラフィックを制御できます。

レピュテーションベースの複数の条件を組み合わせたり、他のタイプの条件と組み合わせたりして、SSL ルールを作成できます。これらの SSL ルールは単純にも複雑にも設定でき、複数の条件を使用してトラフィックを照合および検査できます。

詳細については、次の項を参照してください。

- アプリケーション ベースの暗号化トラフィックの制御（17-9 ページ）
- URL カテゴリおよびレピュテーションによる暗号化トラフィックの制御（17-15 ページ）

アプリケーション ベースの暗号化トラフィックの制御

ライセンス:Control

FirePOWER システムは、暗号化された IP トラフィックを分析するときに、ネットワーク上で一般的に使用されている暗号化アプリケーションを識別および分類してから暗号化セッションを復号します。ASA FirePOWER モジュールはこうした検出ベースの*アプリケーション認識*機能を使用して、ネットワーク上の暗号化されたアプリケーション トラフィックを制御できます。

SSL ルールのアプリケーション条件では、この*アプリケーション制御*を行います。1 つの SSL ルールにおいて、トラフィックの制御対象とするアプリケーションを複数の方法で指定できます。

- カスタム アプリケーションなどの個々のアプリケーションを選択できます。
- ASA FirePOWER モジュール提供の*アプリケーション フィルタ*を使用する。このフィルタは、基本的な特性(タイプ、リスク、ビジネスとの関連性、およびカテゴリ)に基づいてアプリケーションをグループ化して名前を付けたものを指します。
- 選択したアプリケーション(カスタム アプリケーションを含む)をグループ化するカスタム アプリケーション フィルタを作成し、使用できます。

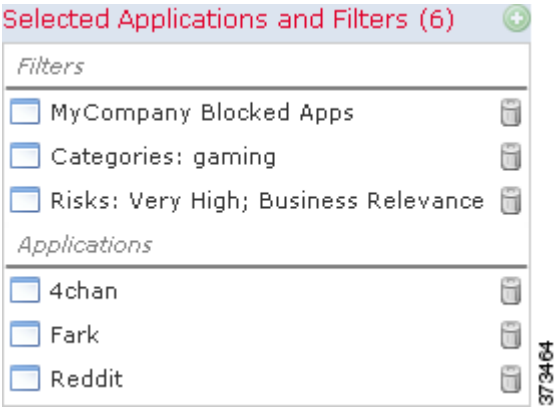
(注) アクセス コントロール ルールを使用してアプリケーション トラフィックをフィルタ処理する場合、フィルタ条件としてアプリケーション タグを使用できます。ただし、暗号化トラフィックはアプリケーション タグでフィルタ処理できません。そのことには意味がないからです。ASA FirePOWER モジュールが暗号化トラフィックのアプリケーションを検出するにはタグ付きの **SSL プロトコル**である必要があり、このタグが付けられていないアプリケーションは、非暗号化トラフィックまたは復号されたトラフィックでしか検出できません。

アプリケーション フィルタを利用すると、SSL ルールのアプリケーション条件を簡単に作成できます。このフィルタによって、ポリシーの作成と管理が簡素化され、モジュールは Web トラフィックを期待通りに確実に制御します。たとえば、暗号化トラフィックのリスクが高くビジネスとの関連性の低いアプリケーションをすべて識別して復号する SSL ルールを作成できます。ユーザがこれらのアプリケーションの使用を試みると、アクセス コントロールによってセッションが復号されて検査されます。

また、Cisco は、システムおよび脆弱性データベース(VDB)の更新を通じて頻繁にディテクタを更新し追加します。独自のディテクタを作成し、そのディテクタが検出するアプリケーションに特性(リスク、関連性など)を割り当てることもできます。アプリケーションの特性に基づいたフィルタを使用することで、モジュールは最新のディテクタを使用してアプリケーション トラフィックをモニタします。

アプリケーション条件を設定した SSL ルールとトラフィックを一致させるには、[選択済みのアプリケーションとフィルタ(Selected Applications and Filters)] リストに追加したいずれかのアプリケーションまたはフィルタにトラフィックが一致する必要があります。

次の図は、MyCompany のアプリケーション、リスクが高くビジネスとの関連性の低いすべてのアプリケーション、ゲーム アプリケーション、およびいくつかの指定アプリケーションからなるカスタム グループを復号する、SSL ルールのアプリケーション条件を示しています。



1 つのアプリケーション条件において、最大 50 の項目を [選択済みのアプリケーションとフィルタ（Selected Applications and Filters）] リストに追加できます。以下はそれぞれ 1 つの項目としてカウントされます。

- 個別またはカスタムな組み合わせの、[アプリケーション フィルタ（Application Filters）] リストからの 1 つ以上のフィルタ。この項目は、特性によってグループ化されたアプリケーションのセットを表します。
- [使用可能なアプリケーション（Available Applications）] リストにあるアプリケーションの検索結果を保存することで作成されたフィルタ。この項目は、部分文字列の一致によってグループ化されたアプリケーションのセットを表します。
- [使用可能なアプリケーション（Available Applications）] リストからの個々のアプリケーション。

モジュール インターフェイスでは、条件に追加されたフィルタは上部にリストされ、個別に追加されたアプリケーションとは分けられます。

SSL ポリシーの適用時には、ASA FirePOWER モジュールは、アプリケーション条件を持つルールごとに一致する固有のアプリケーションのリストを生成することに注意してください。つまり、完全なカバレッジを確保するために、重複フィルタおよび個々に指定されたアプリケーションを使用できます。

詳細については、次の項を参照してください。

- アプリケーション フィルタと暗号化トラフィックの照合（17-10 ページ）
- 個々のアプリケーションからのトラフィックの照合（17-12 ページ）
- SSL ルールへのアプリケーション条件の追加（17-13 ページ）
- 暗号化されたアプリケーションの制御に対する制限（17-14 ページ）

アプリケーション フィルタと暗号化トラフィックの照合

ライセンス：Control

SSL ルールのアプリケーション条件を作成するには、[アプリケーション フィルタ（Application Filters）] リストを使用して、照合するトラフィックの特性を基にアプリケーションをグループ化します。

便宜上、ASA FirePOWER モジュールは、指定された基準を使用して、検出したアプリケーションのそれぞれを特徴付けます。これらの基準をフィルタとして使用したり、フィルタのカスタムな組み合わせを作成してアプリケーション制御を実行したりできます。

SSL ルールでのアプリケーション フィルタの機能は、オブジェクト マネージャを使用した再利用可能なカスタム アプリケーション フィルタの作成と同じです(アプリケーション フィルタの操作(3-12 ページ)を参照してください)。また、オンザフライで作成した多数のフィルタを、アクセス コントロール ルールに新規の再利用可能なフィルタとして保存できます。ユーザが作成したフィルタはネストすることができないため、別のユーザが作成したフィルタを含むフィルタは保存できません。

フィルタの組み合わせ方について

フィルタを単独または組み合わせて選択すると、[使用可能なアプリケーション(Available Applications)] リストが更新され、条件を満たすアプリケーションのみが表示されます。ASA FirePOWER モジュールによって提供されるフィルタは組み合わせて選択できますが、カスタム フィルタはできません。

モジュールは、OR 演算を使用して同じフィルタ タイプの複数のフィルタをリンクします。たとえば、Risks(リスク)タイプの下の Medium(中)および High(高)フィルタを選択すると、結果として次のようなフィルタになります。

```
Risk: Medium OR High
```

Medium(中)フィルタに 110 個のアプリケーション、High(高)フィルタに 82 個のアプリケーションが含まれる場合、[使用可能なアプリケーション(Available Applications)] リストにはこれら 192 個のアプリケーションがすべて表示されます。

モジュールは、AND 演算を使用して異なるタイプのフィルタをリンクします。たとえば Risks(リスク)タイプで Medium(中)および High(高)フィルタを選択し、Business Relevance(ビジネスとの関連性)タイプで Medium(中)および High(高)フィルタを選択した場合、結果として次のようなフィルタになります。

```
Risk: Medium OR High
AND
Business Relevance: Medium OR High
```

この場合、モジュールは Medium(中)または High(高)の Risk(リスク)タイプと Medium(中)または High(高)の Business Relevance(ビジネスとの関連性)タイプの両方に含まれるアプリケーションだけを表示します。

フィルタの検索および選択

フィルタを選択するには、フィルタ タイプの横にある矢印をクリックしてそれを展開し、アプリケーションを表示/非表示にする各フィルタの横のチェック ボックスを選択/選択解除します。Cisco提供のフィルタ タイプ([リスク(Risks)]、[ビジネス関連性(Business Relevance)]、[タイプ(Types)]、または [カテゴリ(Categories)])を右クリックして、[すべて選択(Check All)] または [すべて選択解除(Uncheck All)] を選択することもできます。

フィルタを検索するには、[使用可能なフィルタ(Available Filters)] リストの上にある [名前で検索(Search by name)] プロンプトをクリックし、名前を入力します。入力すると、リストが更新されて一致するフィルタが表示されます。

フィルタを選択したら、[使用可能なアプリケーション(Available Applications)] リストを使用してそのフィルタをルールに追加し、個々のアプリケーションからのトラフィックの照合(17-12 ページ)の手順に従います。

個々のアプリケーションからのトラフィックの照合

ライセンス:Control

SSL ルールのアプリケーション条件を作成するには、[使用可能なアプリケーション(Available Applications)] リストを使用して、照合するトラフィックのアプリケーションを選択します。

アプリケーションのリストの参照

条件の作成を初めて開始するときは、リストは制約されておらず、モジュールが検出するすべてのアプリケーションを一度に 100 個ずつ表示します。

- アプリケーションを確認していくには、リストの下にある矢印をクリックします。
- アプリケーションの特性に関するサマリー情報と参照できるインターネットの検索リンクが示されているポップアップ ウィンドウを表示するには、アプリケーションの横にある情報アイコン( )をクリックします。

照合するアプリケーションの検索

照合するアプリケーションを見つけやすくするために、[使用可能なアプリケーション(Available Applications)] リストを次のように制約できます。

- アプリケーションを検索するには、リスト上部にある [名前で検索(Search by name)] プロンプトをクリックし、名前を入力します。入力すると、リストが更新されて一致するアプリケーションが表示されます。
- フィルタを適用してアプリケーションを制約するには、[アプリケーション フィルタ(Application Filters)] リストを使用します(アプリケーション フィルタと暗号化トラフィックの照合(17-10 ページ)を参照)。フィルタを適用すると、[使用可能なアプリケーション(Available Applications)] リストが更新されます。

制約されると、[フィルタに一致するすべてのアプリケーション(All apps matching the filter)] オプションが [使用可能なアプリケーション(Available Applications)] リストの上部に表示されます。このオプションを使用して、制約されたリスト内のすべてのアプリケーションを [選択済みのアプリケーションとフィルタ(Selected Applications and Filters)] リストにすべて一度に追加できます。

(注)　[アプリケーション フィルタ(Application Filters)] リストで 1 つ以上のフィルタを選択し、しかも [使用可能なアプリケーション(Available Applications)] リストを検索した場合、選択内容と検索フィルタ適用後の [使用可能なアプリケーション(Available Applications)] リストが AND 演算を使って結合されます。つまり [フィルタに一致するすべてのアプリケーション(All apps matching the filter)] 条件には、[使用可能なアプリケーション(Available Applications)] リストに現在表示されている個々のすべての条件と、[使用可能なアプリケーション(Available Applications)] リストの上で入力された検索文字列が含まれます。

条件内で照合する単一アプリケーションの選択

照合するアプリケーションを検索したら、それをクリックして選択します。複数のアプリケーションを選択するには、Shift キーおよび Ctrl キーを使用するか、または現在制約されているビュー内のすべてのアプリケーションを選択するには右クリックして [すべて選択(Select All)] を選択します。

1 つのアプリケーション条件において、アプリケーションの個別選択で追加できる最大数は 50 です。50 を超えるアプリケーションを追加するには、複数の SSL ルールを作成するか、フィルタを使用してアプリケーションをグループ化する必要があります。

条件のフィルタに一致するすべてのアプリケーションの選択

[アプリケーション フィルタ(Application Filters)] リストで検索またはフィルタを使用して制約されると、[フィルタに一致するすべてのアプリケーション(All apps matching the filter)] オプションが [使用可能なアプリケーション(Available Applications)] リストの上部に表示されます。

このオプションを使用して、制約された [使用可能なアプリケーション(Available Applications)] リスト内のアプリケーションのセット全体を [選択済みのアプリケーションとフィルタ(Selected Applications and Filters)] リストに同時に追加できます。アプリケーションを個別に追加するのとは対照的に、このアプリケーションのセットを追加すると、そのセットを構成する個々のアプリケーションの数にかかわらず、最大 50 のアプリケーションに対してただ 1 つのアイテムとしてカウントされます。

このようにアプリケーション条件を作成するときは、[選択済みのアプリケーションとフィルタ(Selected Applications and Filters)] リストに追加するフィルタの名前は、フィルタに表されているフィルタ タイプ + 各タイプの最大 3 つのフィルタの名前を連結させたものとなります。同じタイプのフィルタが 3 個を超える場合は、その後に省略記号(...)が表示されます。たとえば次のフィルタ名には、Risks(リスク)タイプの 2 つのフィルタと Business Relevance(ビジネスとの関連性)タイプの 4 つのフィルタが含まれています。

```
Risks: Medium, High Business Relevance: Low, Medium, High,...
```

[フィルタに一致するすべてのアプリケーション(All apps matching the filter)] で追加するフィルタに表されないフィルタ タイプは、追加するフィルタの名前に含まれません。[選択済みのアプリケーションとフィルタ(Selected Applications and Filters)] リスト内のフィルタ名の上にポインタを置いたときに表示される説明テキストは、これらのフィルタ タイプが [任意(any)] に設定されていることを示します。つまり、これらのフィルタ タイプはフィルタを制約しないので、任意の値が許可されます。

[フィルタに一致するすべてのアプリケーション(All apps matching the filter)] の複数のインスタンスをアプリケーション条件に追加でき、各インスタンスは [選択済みのアプリケーションとフィルタ(Selected Applications and Filters)] リストで個別の項目としてカウントされます。たとえば、リスクが高いすべてのアプリケーションを 1 つの項目として追加し、選択内容をクリアしてから、ビジネスとの関連性が低いすべてのアプリケーションを別の項目として追加できます。このアプリケーション条件は、リスクが高いアプリケーションまたはビジネスとの関連性が低いアプリケーションに一致します。

SSL ルールへのアプリケーション条件の追加

ライセンス:Control

アプリケーション条件を設定した SSL ルールと暗号化トラフィックを一致させるには、[選択済みのアプリケーションとフィルタ(Selected Applications and Filters)] リストに追加したいずれかのアプリケーションまたはフィルタにトラフィックが一致する必要があります。

1 条件ごとに最大 50 の項目を追加でき、条件に追加されたフィルタは上部にリストされ、個別に追加されたアプリケーションとは分けられます。アプリケーション条件を作成する際、警告アイコンは無効な設定を示します。アイコンの上にポインタを置くと詳細が表示されます。

アプリケーション条件に基づいて暗号化トラフィックを制御するには、次の手順を実行します。

手順 1　アプリケーションに応じたトラフィック制御を設定する SSL ポリシーで、新しい SSL ルールを作成するか既存のルールを編集します。

詳細な手順については、SSL ルールの概要と作成(16-4 ページ)を参照してください。

手順 2　SSL ルール エディタで、[アプリケーション(Applications)] タブを選択します。

[アプリケーション(Applications)] タブが表示されます。

手順 3　オプションで、フィルタを使用して [使用可能なアプリケーション（Available Applications）] リストに表示されるアプリケーションのリストを制約します。

[アプリケーション フィルタ（Application Filters）] リストで 1 つ以上のフィルタを選択します。詳細については、アプリケーション フィルタと暗号化トラフィックの照合（17-10 ページ）を参照してください。

手順 4　[使用可能なアプリケーション（Available Applications）] リストから追加するアプリケーションを見つけて選択します。

個々のアプリケーションを検索して選択するか、またはリストが制約されている場合は、[フィルタに一致するすべてのアプリケーション（All apps matching the filter）] を選択できます。詳細については、個々のアプリケーションからのトラフィックの照合（17-12 ページ）を参照してください。

手順 5　[ルールに追加（Add to Rule）] をクリックして、選択したアプリケーションを [選択済みのアプリケーションとフィルタ（Selected Applications and Filters）] リストに追加します。

選択したアプリケーションとフィルタをドラッグ アンド ドロップすることもできます。フィルタは [フィルタ（Filters）] という見出しの下に表示され、アプリケーションは [アプリケーション（Applications）] という見出しの下に表示されます。

ヒント　このアプリケーション条件に別のフィルタを追加する前に、[すべてのフィルタをクリア（Clear All Filters）] をクリックして既存の選択内容をクリアします。

手順 6　ルールを保存するか、編集を続けます。

変更を反映させるには、その SSL ポリシーに関連付けたアクセス コントロール ポリシーを適用する必要があります（設定変更の展開（4-13 ページ）を参照してください）。

暗号化されたアプリケーションの制御に対する制限

ライセンス：Control

アプリケーション制御を実行する際は、次の点に注意してください。

暗号化されたアプリケーションの識別

この ASA FirePOWER モジュールでは、StartTLS を使用して暗号化される非暗号化アプリケーションを識別できます。これには、SMTPS、POPS、FTPS、TelnetS、IMAPS などのアプリケーションが含まれます。また、TLS クライアントの hello メッセージ内の Server Name Indication、またはサーバ証明書のサブジェクト識別名の値に基づいて、特定の暗号化されたアプリケーションを識別できます。

アプリケーション識別の速度

ASA FirePOWER モジュールは、以下のすべての処理が完了するまで暗号化トラフィックのアプリケーション制御を実行できません。

- 暗号化された接続がクライアントとサーバ間で確立される。
- 暗号化セッション内のアプリケーションがモジュールにより識別される。

この識別が行われるのは、サーバ証明書が交換された後です。ハンドシェイク中に交換されるトラフィックでアプリケーションの識別が完了する前に、アプリケーション条件を含んでいる SSL ルール内の他のすべての条件に一致してしまうと、SSL ポリシーによりそのパケットの通過が許可されます。この動作により、ハンドシェイクが完了し、アプリケーションを識別できるようになります。便宜を図るため、影響を受けるルールは情報アイコン（ⓘ）でマークされます。

モジュールによる識別が完了すると、アプリケーション条件に一致する残りのセッション トラフィックに SSL ルールのアクションが適用されます。

URL カテゴリおよびレピュテーションによる暗号化トラフィックの制御

ライセンス：URL Filtering

SSL ルールの URL 条件では、ネットワーク上のユーザからアクセス可能な暗号化 Web サイト トラフィックの処理と復号を行います。要求された URL は、SSL ハンドシェイク時に提供される情報に基づいて検出されます。URL Filtering ライセンスでは、URL の一般的な分類である *カテゴリ*と、リスク レベルである *レピュテーション*に基づいた Web サイトへのアクセス コントロールが可能です。

(注)　特定の URL に対するトラフィックの処理と復号は、識別名の SSL ルール条件を定義することで行えます。証明書のサブジェクト識別名にある共通名属性には、サイトの URL が含まれています。詳細については、証明書の識別名による暗号化トラフィックの制御（17-19 ページ）を参照してください。

詳細については、以下を参照してください。

- レピュテーション ベースの URL ブロッキングの実行（17-15 ページ）
- URL 検出とブロッキングの制約事項（17-18 ページ）

レピュテーション ベースの URL ブロッキングの実行

ライセンス：URL Filtering

URL Filtering ライセンスでは、要求された URL のカテゴリおよびレピュテーションに基づいて、Web サイトへのユーザ アクセスを制御できます。

- URL *カテゴリ*とは、URL の一般的な分類です。たとえば ebay.com は [オークション（Auctions）] カテゴリ、monster.com は [求職（Job Search）] カテゴリに属します。1 つの URL は複数のカテゴリに属することができます。
- URL *レピュテーション*は、組織のセキュリティ ポリシーに反する目的でその URL が使用される可能性を表します。各 URL のリスクは、[高リスク（High Risk）]（レベル 1）から [ウェルノウン（Well Known）]（レベル 5）の範囲にまたがるものとなる可能性があります。

URL のカテゴリおよびレピュテーションは FirePOWER システムが Cisco クラウドから取得するもので、これを利用して SSL ルールの URL 条件を簡単に作成できます。たとえば、[乱用薬物（Abused Drugs）] カテゴリの**高リスク** URL をすべて識別してブロックする SSL ルールを作成できます。ユーザが暗号化接続でこのカテゴリおよびレピュテーションの URL にアクセスすると、そのセッションはブロックされます。

(注)　カテゴリとレピュテーション ベースの URL 条件の SSL ルールを使用するには、Ciscoクラウドとの通信を**有効**にしておく必要があります。これにより、ASA FirePOWER モジュールは URL データを取得できるようになります。詳細については、クラウド通信の有効化（44-2 ページ）を参照してください。

Cisco クラウドのカテゴリおよびレピュテーション データを使用すると、ポリシーの作成と管理がより簡単になります。また、暗号化された Web トラフィックの制御についての信頼度も向上します。最後に、クラウドは新しい URL だけでなく、既存の URL に対する新しいカテゴリとリスクで常に更新されるため、モジュールは確実に最新の情報を使用して要求された URL をフィルタします。マルウェア、スパム、ボットネット、フィッシングなど、セキュリティに対する脅威を表す悪意のあるサイトは、組織でポリシーを更新したり新規ポリシーを適用したりするペースを上回って次々と現れては消える可能性があります。

次に例を示します。

- ルールですべてのゲーム サイトをブロックする場合、新しいドメインが登録されて [ゲーム（Gaming）] に分類されると、これらのサイトをモジュールで自動的にブロックできます。
- ルールですべてのマルウェアをブロックする場合、あるブログ ページがマルウェアに感染すると、クラウドはその URL のカテゴリを [ブログ（Blog）] から [マルウェア（Malware）] に変更することができ、モジュールはそのサイトをブロックできます。
- ルールがリスクの高いソーシャル ネットワーキング サイトをブロックし、だれかがプロファイル ページに悪意のあるペイロードへのリンクが含まれるリンクを掲載すると、クラウドはそのページのレピュテーションを [無害なサイト（Benign sites）] から [高リスク（High Risk）] に変更でき、モジュールでそれをブロックできます。

なお、URL のカテゴリやレピュテーションがクラウドで不明な場合、または ASA FirePOWER モジュールがクラウドと通信できない場合、カテゴリやレピュテーションに基づく URL 条件を含む SSL ルールがトリガー**されない**ことに注意してください。URL に手動でカテゴリやレピュテーションを割り当てることはできません。

次の図は、すべてのマルウェア サイト、すべてのリスクの高いサイト、およびすべての安全でないソーシャル ネットワーキング サイトをブロックするアクセス コントロール ルールの URL 条件を示します。

ヒント　トラフィックを復号してからアクセス コントロールでブロックする場合、ユーザは警告ページをクリックして閉じることでブロックをバイパスできます。詳細については、インタラクティブ ブロッキング アクション：ユーザが Web サイト ブロックをバイパスすることを許可する（6-10 ページ）を参照してください。

1 つの URL 条件で [選択したカテゴリ（Selected Categories）] リストに最大 50 の項目を追加できます。任意でレピュテーションによって制限された各 URL カテゴリは、1 つの項目としてカウントされます。

次の表では、前述の条件を作成する方法を要約します。レピュテーションでリテラル URL または URL オブジェクトを制限できないことに注意してください。

表 17-1　例:URL 条件の作成

ブロックする対象	選択するカテゴリまたは URL オブジェクト	選択するレピュテーション
マルウェア サイト(レピュテーションに関係なく)	マルウェア サイト(Malware Sites)	任意(Any)
高リスクの URL(レベル 1)	任意(Any)	1 - 高リスク(High Risk)
無害(benign)よりも大きいリスクがあるソーシャル ネットワーキング サイト(レベル 1 ～ 3)	ソーシャル ネットワーク(Social Network)	3 - セキュリティ リスクのある無害なサイト(Benign sites with security risks)

URL 条件を作成する際、警告アイコンは無効な設定を示します。アイコンの上にポインタを置くと詳細が表示されます。また、アクセス コントロール ポリシーとルールのトラブルシューティング(4-14 ページ)を参照してください。

カテゴリ データおよびレピュテーション データを使用した要求された URL によるトラフィックの制御

手順 1　URL に応じた暗号化トラフィック制御を設定する SSL ポリシーで、新しい SSL ルールを作成するか既存のルールを編集します。

詳細な手順については、SSL ルールの概要と作成(16-4 ページ)を参照してください。

手順 2　SSL ルール エディタで、[カテゴリ(Categories)] タブを選択します。

[カテゴリ(Categories)] タブが表示されます。

手順 3　[カテゴリ(Categories)] リストで、追加する URL カテゴリを選択します。カテゴリを指定せずにすべての暗号化 Web トラフィックと一致させるには、[任意(Any)] カテゴリを選択します。

追加可能なカテゴリを検索するには、[カテゴリ(Categories)] リストの上にある [名前または値で検索(Search by name or value)] プロンプトをクリックし、カテゴリ名を入力します。入力すると、リストが更新されて一致するカテゴリが表示されます。

カテゴリを選択するには、そのカテゴリをクリックします。複数のカテゴリを選択するには、Shift キーおよび Ctrl キーを使用します。

ヒント　右クリックで表示される [すべて選択(Select All)] も利用できますが、この方法ですべてのカテゴリを追加すると、SSL ルールの最大項目数 50 を超えてしまいます。代わりに [任意(Any)] を使用してください。

手順 4　オプションで、[レピュテーション(Reputations)] リストからレピュテーション レベルをクリックして、カテゴリの選択内容を制限します。レピュテーション レベルを指定しない場合、モジュールはデフォルトとして [任意(Any)](つまりすべてのレベル)を設定します。

選択できるレピュテーション レベルは 1 つだけです。レピュテーションのレベルを選択すると、SSL ルールはその目的に応じて異なる動作をします。

- ルールで Web アクセスのブロックまたはトラフィックの復号を行う場合（ルール アクションが、[ブロック（Block）]、[リセットしてブロック（Block with reset）]、[復号 - 既知のキー（Decrypt - Known Key）]、[復号 - 再署名（Decrypt - Resign）]、または [モニタ（Monitor）] の場合）、選択したレピュテーション レベルよりも厳しいすべてのレピュテーションも自動的に選択されます。たとえば**疑わしいサイト（Suspicious sites）**（レベル 2）をブロックするようルールを設定した場合、**高リスク（High Risk）**（レベル 1）のサイトも自動的にブロックされます。
- ルールで Web アクセスを許可して、アクセス コントロールに従わせる場合（ルール アクションが [復号しない（Do not decrypt）] の場合）、選択したレピュテーション レベルよりも厳しくないすべてのレピュテーションも自動的に選択されます。たとえば**無害なサイト（Benign sites）**（レベル 4）を許可するようルールを設定した場合、**有名（Well known）**（レベル 5）サイトもまた自動的に許可されます。

ルールのアクションを変更した場合、モジュールは、上記の点に従って URL 条件のレピュテーション レベルを自動的に変更します。

手順 5　[ルールに追加（Add to Rule）] をクリックして、選択した項目を [選択したカテゴリ（Selected Categories）] リストに追加します。

選択した項目をドラッグ アンド ドロップすることもできます。

手順 6　ルールを保存するか、編集を続けます。

変更を反映させるには、その SSL ポリシーに関連付けたアクセス コントロール ポリシーを適用する必要があります（設定変更の展開（4-13 ページ）を参照してください）。

URL 検出とブロッキングの制約事項

ライセンス：URL Filtering

URL の検出とブロッキングを実行する際は、次の点に注意してください。

URL 識別の速度

モジュールによる URL のカテゴリ分類は、以下のすべての処理が完了するまで実行されません。

- モニタ対象の接続がクライアントとサーバの間で確立される。
- セッション内の HTTPS アプリケーションがモジュールにより識別される。
- 要求された URL をモジュールがクライアントの hello メッセージまたはサーバ証明書に基づいて識別する。

この識別が行われるのは、サーバ証明書が交換された後です。ハンドシェイク中に交換されるトラフィックで URL 識別が完了する前に、URL 条件を含んでいる SSL ルール内の他のすべての条件に一致してしまうと、SSL ポリシーによりそのパケットの通過が許可されます。この動作により接続が確立され、URL の識別が可能になります。便宜を図るため、影響を受けるルールは情報アイコン（ⓘ）でマークされます。

モジュールによる識別が完了すると、URL 条件に一致する残りのセッション トラフィックに SSL ルールのアクションが適用されます。

URL での検索クエリ パラメータ

モジュールでは、URL 条件の照合に URL 内の検索クエリ パラメータを使用しません。たとえば、すべてのショッピング トラフィックをブロックする場合を考えます。amazon.com を探すために Web 検索を使用してもブロックされませんが、amazon.com を閲覧しようとするとブロックされます。

サーバ証明書の特性に基づいたトラフィック制御

ライセンス：任意（Any）

サーバ証明書の特性に基づいて暗号化トラフックの処理および復号化を行う SSL ルールを作成できます。セッションの暗号化に使用されている暗号スイートまたはプロトコル バージョンを検出して、それに応じてトラフィックを処理できます。また、サーバ証明書を検出して、以下のサーバ証明書の特性に基づいてトラフィックを処理することもできます。

- サーバ証明書自体。
- 証明書の発行元。証明書が CA で発行されているか自己署名されているか。
- 証明書のホルダー。
- 証明書ステータス。証明書が有効であるか、発行元の CA により無効にされているかなど。

複数の暗号スイートを 1 つのルールで検出したり、証明書の発行元や証明書ホルダーを検出したりする場合は、再利用可能な暗号スイートのリストおよび識別名オブジェクトを作成してルールに追加できます。サーバ証明書および特定の証明書ステータスを検出するには、ルール用の外部証明書と外部 CA オブジェクトの作成が必要です。

詳細については、次の項を参照してください。

- 証明書の識別名による暗号化トラフィックの制御（17-19 ページ）
- 証明書による暗号化トラフィックの制御（17-22 ページ）
- 証明書ステータスによる暗号化トラフィックの制御（17-23 ページ）
- 暗号スイートによる暗号化トラフィックの制御（17-28 ページ）
- 暗号化プロトコルのバージョンによるトラフィックの制御（17-29 ページ）

証明書の識別名による暗号化トラフィックの制御

ライセンス：任意（Any）

SSL ルールで識別名条件を設定すると、証明書ホルダーまたはサーバ証明書を発行した CA に応じて暗号化トラフィックを処理および検査できます。発行元の識別名を基準にすると、サイトのサーバ証明書を発行した CA に基づいてトラフィックを処理できます。

ルール条件を設定する場合は、手動でリテラル値を指定するか、識別名オブジェクトを参照するか、または複数のオブジェクトを含んでいる識別名グループを参照できます。

（注）[復号 - 既知のキー（Decrypt - Known Key）] アクションを選択した場合、識別名条件を設定することはできません。このアクションでは、トラフィック復号用のサーバ証明書の選択が必要であるため、トラフィックの照合はすでにこの証明書で行われています。詳細については、[復号（Decrypt）] アクション：さらに検査するためにトラフィックを復号（16-11 ページ）を参照してください。

複数のサブジェクトおよび発行元の識別名との照合を単一の証明書ステータスのルール条件で行うことも可能ですが、ルールとの照合で一致する必要があるのは 1 つの共通名または識別名だけです。

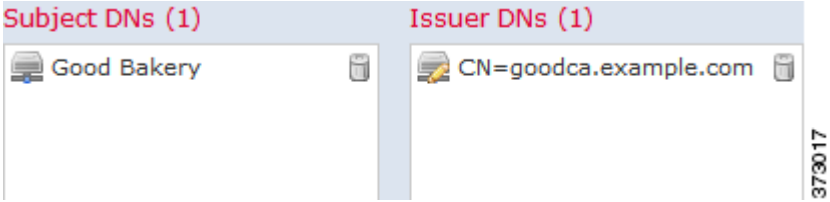
識別名を手動で追加する場合、共通名属性（**CN**）を含めることができます。「CN=」なしで共通名を追加すると、オブジェクトの保存時に「CN=」が追加されます。

さらに、次の表に示す属性を含む識別名を追加することもできます。属性はカンマで区切って使用します。

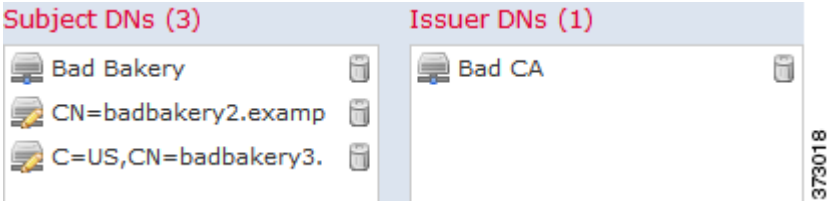
表 17-2　識別名の属性

属性（Attribute）	説明	使用可能な値
C	国コード（Country Code）	2 つの英字
CN	Common Name	最大 64 個の英数字、バックスラッシュ（\）、ハイフン（-）、引用符（"）、アスタリスク（*）、ピリオド（.）、またはスペース文字
O	Organization	
OU	組織	

次の図は、goodbakery.example.com に対して発行された証明書および goodca.example.com によって発行された証明書を検索する識別名ルール条件を示しています。これらの証明書で暗号化されたトラフィックは許可され、アクセス コントロールにより制御されます。



次の図は、badbakery.example.com および関連ドメインに対して発行された証明書および badca.example.com によって発行された証明書を検索する識別名ルール条件を示しています。これらの証明書で暗号化されたトラフィックは、再署名された証明書を使用して復号されます。



1 つの識別名条件で、[サブジェクト DN（Subject DNs）] リストおよび [発行元 DN（Issuer DNs）] リストにそれぞれ最大 50 のリテラル値および識別名オブジェクトを追加できます。

ASA FirePOWER モジュール提供の識別名オブジェクト グループである Sourcefire Undecryptable Sites には、モジュールで復号できないトラフィックの Web サイトが含まれています。このグループを識別名条件に追加すると、該当する Web サイトとのトラフィックがブロックしたり復号を無効にしたりでき、これらのトラフィックの復号に使用されるシステム リソースの浪費を回避できます。グループ内の各エントリは変更できますが、このグループを削除することはできません。システムによる更新によりこのリストのエントリが変更されることがありますが、モジュールではユーザによる変更が保持されます。

システムが新しいサーバへの暗号化セッションを最初に検出したときは、DN データを ClientHello の処理には使用できません。これは復号化されていない最初のセッションとなる可能性があります。最初のセッションの後に、管理対象デバイスは、サーバの証明書メッセージからのデータをキャッシュします。同じクライアントからの後続の接続で、システムは識別名条件を含むルールに ClientHello メッセージを最終的に一致させ、メッセージを処理して、復号化の可能性を最大化できます。

証明書のサブジェクトまたは発行元の識別名に基づいて暗号化トラフィックを検査するには、次の手順を実行します。

手順 1　証明書のサブジェクトまたは発行元の識別名に応じた暗号化トラフィック制御を設定する SSL ポリシーで、新しい SSL ルールを作成するか既存のルールを編集します。

詳細な手順については、SSL ルールの概要と作成（16-4 ページ）を参照してください。

手順 2　SSL ルール エディタで、[DN] タブを選択します。

[DN] タブが表示されます。

手順 3　[使用可能な DN（Available DNs）] で、追加する識別名を選択します。

- ここで識別名オブジェクトを作成してリストに追加するには、[使用可能な DN（Available DNs）] リストの上にある追加アイコン（ ）をクリックし、識別名オブジェクトの操作（3-38 ページ）の手順に従います。
- 追加する識別名オブジェクトおよびグループを検索するには、[使用可能な DN（Available DNs）] リストの上にある [名前または値で検索（Search by name or value）] プロンプトをクリックし、オブジェクトの名前またはオブジェクトの値を入力します。入力すると、リストが更新されて一致するオブジェクトが表示されます。

オブジェクトを選択するには、そのオブジェクトをクリックします。複数のオブジェクトを選択するには、Shift キーおよび Ctrl キーを使用するか、または右クリックして [すべて選択（Select All）] を選択します。

手順 4　次の選択肢があります。

- [サブジェクトに追加（Add to Subject）] をクリックして、選択したオブジェクトを [サブジェクト DN（Subject DNs）] リストに追加します。
- [発行元に追加（Add to Issuer）] をクリックして、選択したオブジェクトを [発行元 DN（Issuer DNs）] リストに追加します。

選択したオブジェクトをドラッグ アンド ドロップすることもできます。

手順 5　手動で指定するリテラル共通名または識別名がある場合は、それらを追加します。

[サブジェクト DN（Subject DNs）] または [発行元 DN（Issuer DNs）] リストの下にある [DN または CN の入力（Enter DN or CN）] プロンプトをクリックし、共通名または識別名を入力して [追加（Add）] をクリックします。

手順 6　ルールを追加するか、編集を続けます。

変更を反映させるには、その SSL ポリシーに関連付けたアクセス コントロール ポリシーを適用する必要があります（設定変更の展開（4-13 ページ）を参照してください）。

証明書による暗号化トラフィックの制御

ライセンス：任意（Any）

SSL ルールで証明書条件を設定すると、トラフィックの暗号化に使用されているサーバ証明書に応じて暗号化トラフィックを処理および検査できます。1 つの条件に 1 つまたは複数の証明書を設定でき、トラフィックの証明書がいずれかの条件の証明書と一致するとそのルールが適用されます。

証明書ベースの SSL ルール条件を作成するときにサーバ証明書をアップロードしたり、再利用可能な外部証明書*オブジェクト*として保存してサーバ証明書の名前を関連付けたりできます。また、既存の外部証明書オブジェクトやオブジェクト グループを使用して証明書条件を設定することもできます。

ルール条件の [使用可能な証明書（Available Certificates）] フィールドでは、外部証明書オブジェクトやオブジェクト グループを証明書の識別名に関する以下の特性に基づいて検索できます。

- サブジェクトまたは発行元の共通名（CN）
- サブジェクトまたは発行元の組織（O）
- サブジェクトまたは発行元の組織単位（OU）

1 つの証明書のルール条件で複数の証明書を照合することもでき、トラフィックの暗号化に使用されている証明書がアップロードされた証明書のいずれかと一致した場合、その暗号化トラフィックはルールに一致したと判定されます。

1 つの証明書条件で、[選択した証明書（Selected Certificates）] リストに最大 50 の外部証明書オブジェクトおよび外部証明書オブジェクト グループを追加できます。

次の点に注意してください。

- [復号 - 既知のキー（Decrypt - Known Key）] アクションも選択すると、証明書条件を設定できなくなります。このアクションでは、トラフィック復号用のサーバ証明書の選択が必要であるため、トラフィックの照合はすでにこの証明書で行われていることになります。詳細については、[復号（Decrypt）] アクション：さらに検査するためにトラフィックを復号（16-11 ページ）を参照してください。
- 証明書条件に外部証明書オブジェクトを設定する場合、暗号スイート条件に追加する暗号スイートまたは [復号 - 再署名（Decrypt - Resign）] アクションに関連付ける内部 CA オブジェクトのいずれかが、外部証明書の署名アルゴリズム タイプと一致する必要があります。たとえば、ルールの証明書条件で EC ベースのサーバ証明書を参照する場合は、追加する暗号スイート、または [復号 - 再署名（Decrypt - Resign）] アクションに関連付ける CA 証明書も EC ベースでなければなりません。署名アルゴリズム タイプの不一致が検出されると、ポリシー エディタでルールの横に警告アイコンが表示されます。詳細については、暗号スイートによる暗号化トラフィックの制御（17-28 ページ）および [復号（Decrypt）] アクション：さらに検査するためにトラフィックを復号（16-11 ページ）を参照してください。
- システムが新しいサーバへの暗号化セッションを最初に検出したときは、証明書データを ClientHello の処理には使用できません。これは復号されていない最初のセッションとなる可能性があります。最初のセッションの後に、管理対象デバイスは、サーバの証明書メッセージからのデータをキャッシュします。同じクライアントからの後続の接続で、システムは証明書条件を含むルールに ClientHello メッセージを最終的に一致させ、メッセージを処理して、復号化の可能性を最大化できます。

サーバ証明書に基づいて暗号化トラフィックを検査するには、次の手順を実行します。

手順 1　サーバ証明書に応じた暗号化トラフィック制御を設定する SSL ポリシーで、新しい SSL ルールを作成するか既存のルールを編集します。

詳細な手順については、SSL ルールの概要と作成（16-4 ページ）を参照してください。

手順 2　SSL ルール エディタで、[証明書（Certificate）] タブを選択します。

[証明書（Certificate）] タブが表示されます。

手順 3　[使用可能な証明書（Available Certificates）] で、追加するサーバ証明書を選択します。

- ここで外部証明書オブジェクトを作成してリストに追加するには、[使用可能な証明書（Available Certificates）] リストの上にある追加アイコン（ ）をクリックし、外部証明書オブジェクトの操作（3-47 ページ）の手順に従います。
- 追加する証明書オブジェクトおよびグループを検索するには、[使用可能な証明書（Available Certificates）] リストの上にある [名前または値で検索（Search by name or value）] プロンプトをクリックし、オブジェクトの名前またはオブジェクトの値を入力します。入力すると、リストが更新されて一致するオブジェクトが表示されます。

オブジェクトを選択するには、そのオブジェクトをクリックします。複数のオブジェクトを選択するには、Shift キーおよび Ctrl キーを使用するか、または右クリックして [すべて選択（Select All）] を選択します。

手順 4　[ルールに追加（Add to Rule）] をクリックして、選択したオブジェクトを [サブジェクト証明書（Subject Certificates）] リストに追加します。

選択したオブジェクトをドラッグ アンド ドロップすることもできます。

手順 5　ルールを追加するか、編集を続けます。

変更を反映させるには、その SSL ポリシーに関連付けたアクセス コントロール ポリシーを適用する必要があります（設定変更の展開（4-13 ページ）を参照してください）。

証明書ステータスによる暗号化トラフィックの制御

ライセンス：任意（Any）

SSL ルールで証明書ステータス条件を設定すると、トラフィックの暗号化に使用されているサーバ証明書のステータス（有効、失効済み、有効期限切れ、未有効化、自己署名、信頼できる CA によって署名済みなど）に応じて暗号化トラフィックの処理および検査できます。

CA が証明書を発行したか失効したかを確認するには、ルートおよび中間 CA 証明書とその関連 CRL をオブジェクトとしてアップロードする必要があります。その後で SSL ポリシーの信頼できる CA 証明書のリストに、これらの信頼できる CA のオブジェクトを追加します。

証明書ステータスの SSL ルール条件では、各ステータスの有無を基準にしたトラフィックの照合ができます。1 つのルール条件で複数のステータスを選択でき、いずれかのステータスと証明書が一致すれば、ルールとトラフィックが一致したと判定されます。

詳細については、以下を参照してください。

- 外部認証局の信頼（17-24 ページ）
- 証明書ステータスでのトラフィックの照合（17-25 ページ）

外部認証局の信頼

ライセンス：任意（Any）

SSL ポリシーでルートおよび中間 CA 証明書を追加することで信頼できる CA が設定され、トラフィックの暗号化に使用されているサーバ証明書の検証に、これらの信頼できる CA を使用できるようになります。検証されたサーバ証明書には、信頼できる CA によって署名された証明書が含まれます。

信頼できる CA 証明書の中にアップロードされた証明書失効リスト（CRL）が含まれている場合は、信頼できる CA により、暗号化証明書が失効されているかどうかも確認できます。詳細については、信頼できる CA オブジェクトに証明書失効リストを追加する（3-46 ページ）を参照してください。

SSL ポリシーに信頼できる CA 証明書を追加した後は、トラフィックと照合するさまざまな証明書ステータス条件を SSL ルールに設定することができます。詳細については、「信頼できる認証局オブジェクトの操作（3-45 ページ）」と「証明書ステータスによる暗号化トラフィックの制御（17-23 ページ）」を参照してください。

ヒント　信頼できるルート CA の信頼チェーン内にあるすべての証明書を、信頼できる CA 証明書のリストにアップロードしますが、これにはルート CA 証明書およびすべての中間 CA 証明書が含まれます。これを行わないと、中間 CA から発行された信頼できる証明書の検出が困難になります。

SSL ポリシーを作成すると、ASA FirePOWER モジュールにより、[信頼できる CA 証明書（Trusted CA Certificates）] タブにデフォルトの信頼できる CA オブジェクト グループ Cisco Trusted Authorities が入力されます。このグループ内の各エントリは変更が可能で、SSL ポリシーにこのグループを含めるかどうかを選択できます。このグループを削除することはできません。システムによる更新によりこのリストのエントリが変更されることがありますが、ユーザによる変更は保持されます。詳細については、基本 SSL ポリシーの作成（15-2 ページ）を参照してください。

ポリシーに信頼できる CA を追加するには、次の手順を実行します。

手順 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ポリシー（Policies）] > [SSL] の順に選択します。

[SSL ポリシー（SSL Policy）] ページが表示されます。

手順 2　設定する SSL ポリシーの横にある編集アイコン（）をクリックします。

SSL ポリシー エディタが表示されます。

手順 3　[信頼できる CA 証明書（Trusted CA Certificates）] タブを選択します。

[信頼できる CA 証明書（Trusted CA Certificates）] ページが表示されます。

手順 4　[使用可能な信頼できる CA（Available Trusted CAs）] で、追加する信頼できる CA を選択します。

- ここで信頼できる CA のオブジェクトを作成してリストに追加するには、[使用可能な信頼できる CA（Available Trusted CAs）] リストの上にある追加アイコン（）をクリックし、信頼できる認証局オブジェクトの操作（3-45 ページ）の手順に従います。
- 追加する信頼できる CA オブジェクトおよびグループを検索するには、[使用可能な信頼できる CA（Available Trusted CAs）] リストの上にある [名前または値で検索（Search by name or value）] プロンプトをクリックし、オブジェクトの名前またはオブジェクトの値を入力します。入力すると、リストが更新されて一致するオブジェクトが表示されます。

オブジェクトを選択するには、そのオブジェクトをクリックします。複数のオブジェクトを選択するには、Shift キーおよび Ctrl キーを使用するか、または右クリックして [すべて選択（Select All）] を選択します。

手順 5　[ルールに追加（Add to Rule）] をクリックして、選択したオブジェクトを [選択した信頼できる CA（Selected Trusted CAs）] リストに追加します。

選択したオブジェクトをドラッグ アンド ドロップすることもできます。

手順 6　ルールを追加するか、編集を続けます。

変更を反映させるには、その SSL ポリシーに関連付けたアクセス コントロール ポリシーを適用する必要があります（設定変更の展開（4-13 ページ）を参照してください）。

証明書ステータスでのトラフィックの照合

ライセンス：任意（Any）

証明書ステータス ベースのルール条件を設定すると、トラフィックの暗号化に使用されているサーバ証明書のステータスに基づいて暗号化トラフィックを照合できます。次の操作を実行できます。

- サーバ証明書のステータスをチェックする。
- 証明書にステータスがないことをチェックする。
- 証明書ステータスの有無のチェックをスキップする。

複数の証明書ステータスの有無の一致を単一の証明書ステータスのルール条件で選択することも可能ですが、ルールとの照合で証明書が一致する必要があるのは 1 つの基準だけです。

次の表は、暗号化用のサーバ証明書のステータスを基準に、ASA FirePOWER モジュールが暗号化トラフィックを評価する方法を示しています。

表 17-3　証明書ステータスのルール条件の基準

ステータスの確認	[はい（Yes）] を設定	[いいえ（No）] を設定
失効（Revoked）	ポリシーは、サーバ証明書を発行した CA を信頼しており、ポリシーにアップロードされた CA 証明書にはこのサーバ証明書を失効させる CRL が含まれています。	ポリシーは、サーバ証明書を発行した CA を信頼しており、ポリシーにアップロードされた CA 証明書にはこのサーバ証明書を失効させる CRL が含まれていません。
自己署名（Self-signed）	検出されたサーバ証明書が、同じサブジェクトと発行元の識別名を含んでいます。	検出されたサーバ証明書が、異なるサブジェクトと発行元の識別名を含んでいます。
有効（Valid）	以下のすべてを満たしています。 • 証明書を発行した CA をポリシーが信頼しています。 • 署名が有効です。 • 発行元が有効です。 • ポリシーの信頼できる CA のいずれも証明書を失効させていません。 • 現在の日付が証明書の有効期間の開始日と終了日の範囲内にあります。	以下の 1 つ以上を満たしています。 • 証明書を発行した CA をポリシーが信頼していません。 • 署名が無効です。 • 発行元が無効です。 • ポリシーの信頼できる CA の 1 つが証明書を失効させています。 • 現在の日付が証明書の有効期間の開始日より前です。 • 現在の日付が証明書の有効期限の終了日より後です。
署名が無効（Invalid signature）	証明書の内容に対して証明書の署名が適切に検証されません。	証明書の内容に対して証明書の署名が適切に検証されます。

表 17-3　証明書ステータスのルール条件の基準（続き）

ステータスの確認	[はい（Yes）] を設定	[いいえ（No）] を設定
発行元が無効（Invalid issuer）	発行元の CA 証明書が、ポリシーの信頼できる CA 証明書のリストに登録されていません。	発行元の CA 証明書が、ポリシーの信頼できる CA 証明書のリストに登録されています。
期限切れ	現在の日付が証明書の有効期限の終了日より後です。	現在の日付が証明書の有効期限の終了日であるかそれより前です。
まだ無効（Not yet valid）	現在の日付が証明書の有効期間の開始日より前です。	現在の日付が証明書の有効期間の開始日であるかそれより後です。

次の例を考えてみます。組織は Verified Authority という認証局を信頼しています。組織は Spammer Authority という認証局を信頼していません。システム管理者は、Verified Authority の証明書、および Verified Authority の発行した中間 CA 証明書をアップロードします。Verified Authority が以前に発行した証明書の 1 つを失効させたため、システム管理者は Verified Authority から配布された CRL をアップロードします。

次の図は、有効な証明書をチェックする証明書ステータスのルール条件を示しています。これにより、Verified Authority から発行されたが CRL には登録されておらず、現状で有効期間の開始日と終了日の範囲内にあるかどうかがチェックされます。この設定では、これらの証明書で暗号化されたトラフィックはアクセス コントロールにより復号および検査されません。

次の図は、ステータスが存在しないことをチェックする証明書ステータスのルール条件を示しています。この設定では、期限切れになっていない証明書を使用して暗号化されたトラフィックと照合し、そのトラフィックをモニタします。

次の図は、さまざまなステータスの有無に一致する証明書ステータスのルール条件を示しています。この設定でルールが一致するのは、着信トラフィックを暗号化した証明書が無効なユーザが発行元、自己署名、無効、または期限切れであった場合で、そうしたトラフィックを既知のキーで復号します。

1 つの証明書が複数のステータスに一致する場合でも、ルールがトラフィックに行うアクションは一度に 1 つだけであることに注意してください。

（注）　システムが新しいサーバへの暗号化セッションを最初に検出したときは、証明書ステータスを ClientHello の処理には使用できません。これは復号化されていない最初のセッションとなる可能性があります。最初のセッションの後に、管理対象デバイスは、サーバの証明書メッセージからのデータをキャッシュします。同じクライアントからの後続の接続で、システムは証明書ステータス条件を含むルールに ClientHello メッセージを最終的に一致させ、メッセージを処理して、復号化の可能性を最大化できます。

サーバ証明書のステータスで暗号化トラフィックを検査するには、次の手順を実行します。

手順 1　サーバ証明書のステータスに応じた暗号化トラフィック制御を設定する SSL ポリシーで、新しい SSL ルールを作成するか既存のルールを編集します。

詳細な手順については、SSL ルールの概要と作成（16-4 ページ）を参照してください。

手順 2　SSL ルール エディタで、[証明書のステータス（Cert Status）] タブを選択します。

[証明書のステータス（Cert Status）] タブが表示されます。

手順 3　各証明書ステータスには次のオプションがあります。

- 該当する証明書ステータスが存在するときに照合する場合は、[はい（Yes）] を選択します。
- 該当する証明書ステータスが存在しないときに照合する場合は、[いいえ（No）] を選択します。
- 該当する証明書ステータスを照合しない場合は [照合しない（Do Not Match）] を選択します。

手順 4　ルールを追加するか、編集を続けます。

変更を反映させるには、その SSL ポリシーに関連付けたアクセス コントロール ポリシーを適用する必要があります（設定変更の展開（4-13 ページ）を参照してください）。

暗号スイートによる暗号化トラフィックの制御

ライセンス：任意（Any）

SSL ルールで暗号スイート条件を設定すると、暗号化セッションのネゴシエートに使用される暗号スイートに応じて暗号化トラフィックを処理および検査できます。暗号スイートのルール条件に追加できる、Cisco 定義の暗号スイートが提供されています。複数の暗号スイートを含む、暗号スイートのリストのオブジェクトを追加することもできます。暗号スイートのリストの詳細については、位置情報オブジェクトの操作（3-49 ページ）を参照してください。

（注）　新しい暗号スイートを追加することはできません。定義済みの暗号スイートは変更も削除もできません。

1 つの暗号スイート条件で、[選択した暗号スイート（Selected Cipher Suites）] リストに最大 50 の暗号スイートおよび暗号スイート リストを追加できます。

次の点に注意してください。

- 展開でサポートされていない暗号スイートを追加した場合、その SSL ポリシーに関連付けられたアクセス コントロール ポリシーを適用することはできません。たとえば、パッシブ展開では、一時 Diffie-Hellman（DHE）および一時的楕円曲線 Diffie-Hellman（ECDHE）暗号スイートを使用したトラフィックの復号がサポートされません。これらの暗号スイートでルールを作成した場合、アクセス コントロール ポリシーは適用できません。
- 暗号スイート条件に暗号スイートを設定する場合は、証明書条件に追加する外部証明書オブジェクト、または [復号 - 再署名（Decrypt - Resign）] アクションに関連付ける内部 CA オブジェクトが、暗号スイートの署名アルゴリズム タイプと一致している必要があります。たとえば、ルールの暗号スイート条件で EC ベースの暗号スイートを参照する場合は、追加するサーバ証明書、または [復号 - 再署名（Decrypt - Resign）] アクションに関連付ける CA 証明書も EC ベースでなければなりません。署名アルゴリズム タイプの不一致が検出されると、ポリシー エディタでルールの横に警告アイコンが表示されます。詳細については、暗号スイートによる暗号化トラフィックの制御（17-28 ページ）および [復号（Decrypt）] アクション：さらに検査するためにトラフィックを復号（16-11 ページ）を参照してください。
- SSL ルールの暗号スイート条件に匿名の暗号スイートを追加できますが、次の点に注意してください。
  - システムは ClientHello 処理中に自動的に匿名の暗号スイートを削除します。ルールを使用するシステムでは、ClientHello の処理を防止するために SSL ルールを設定する必要があります。詳細については、SSL ルールの順序指定によるパフォーマンス向上とプリエンプション回避（16-19 ページ）を参照してください。
  - システムでは、匿名の暗号スイートで暗号化されたトラフィックは復号できないため、ルールに [復号 - 再署名（Decrypt - Resign）] または [復号 - 既知のキー（Decrypt - Known Key）] アクションを使用できません。
- 暗号スイートをルール条件として指定する際、ルールを ClientHello メッセージで指定された暗号スイートの完全なリストではなく、ServerHello メッセージのネゴシエートされた暗号スイートと照合することを検討してください。ClientHello の処理中に、管理対象デバイスは ClientHello メッセージからサポートされていない暗号スイートを削除します。ただし、これにより指定されたすべての暗号スイートが削除されることになる場合、システムでは元のリストを保持します。システムがサポートされていない暗号スイートを保持する場合、後続の評価は復号化されないセッションになります。

暗号化トラフィックを暗号スイートで検査するには、次の手順を実行します。

手順 1　暗号スイートに応じた暗号化トラフィック制御を設定する SSL ポリシーで、新しい SSL ルールを作成するか既存のルールを編集します。

詳細な手順については、SSL ルールの概要と作成（16-4 ページ）を参照してください。

手順 2　SSL ルール エディタで、[暗号スイート（Cipher Suite）] タブを選択します。

[暗号スイート（Cipher Suite）] タブが表示されます。

手順 3　[使用可能な暗号スイート（Available Cipher Suites）] で、追加する暗号スイートを選択します。

- ここで暗号スイート リストを作成してリストに追加するには、[使用可能な暗号スイート（Available Cipher Suites）] リストの上にある追加アイコン（ ）をクリックし、位置情報オブジェクトの操作（3-49 ページ）の手順に従います。
- 追加する暗号スイートおよびリストを検索するには、[使用可能な暗号スイート（Available Cipher Suites）] リストの上にある [名前または値で検索（Search by name or value）] プロンプトをクリックし、暗号スイートの名前または暗号スイートの値を入力します。入力を開始するとリストが更新され、一致する暗号スイートが表示されます。

暗号スイートをクリックして選択します。複数の暗号スイートを選択するには、Shift キーまたは Ctrl キーを使用します。すべての暗号スイートを選択するには、右クリックして [すべて選択（Select All）] を選択します。

手順 4　[ルールに追加（Add to Rule）] をクリックして、選択した暗号スイートを [選択した暗号スイート（Selected Cipher Suites）] リストに追加します。

選択した暗号スイートをドラッグ アンド ドロップでリストに追加することもできます。

手順 5　ルールを追加するか、編集を続けます。

変更を反映させるには、その SSL ポリシーに関連付けたアクセス コントロール ポリシーを適用する必要があります（設定変更の展開（4-13 ページ）を参照してください）。

暗号化プロトコルのバージョンによるトラフィックの制御

ライセンス：任意（Any）

SSL ルールでセッション条件を設定すると、トラフィックの暗号化に使用されている SSL または TLS のバージョンに応じて暗号化トラフィックを検査できます。SSL バージョン 3.0 または TLS バージョン 1.0、1.1、1.2 のいずれかで暗号化されたトラフィックとの照合を選択できます。デフォルトでは、ルールの作成時にすべてのプロトコルのバージョンが選択されます。複数のバージョンが選択されている場合、いずれかのバージョンと一致する暗号化トラフィックがルールに一致したと判定されます。ルール条件を保存するには、最低 1 つのプロトコル バージョンを選択する必要があります。

（注）　バージョンのルール条件で SSL バージョン 2.0 を選択することはできません。これは、ASA FirePOWER モジュールが SSL バージョン 2.0 で暗号化されたトラフィックの復号をサポートしていないためです。復号できないアクションを設定すれば、それ以上のインスペクションなしで、これらのトラフィックを許可またはブロックできます。詳細については、SSL ルールによる復号可能接続のロギング（36-16 ページ）を参照してください。

暗号化トラフィックを **SSL** または **TLS** のバージョンで検査するには、次の手順を実行します。

手順 1　暗号化プロトコルのバージョンに応じた暗号化トラフィック制御を設定する SSL ポリシーで、新しい SSL ルールを作成するか既存のルールを編集します。

詳細な手順については、SSL ルールの概要と作成（16-4 ページ）を参照してください。

手順 2　SSL ルール エディタで、[バージョン（Version）] タブを選択します。

[バージョン（Version）] タブが表示されます。

手順 3　照合するプロトコル バージョンを選択します。**SSL v3.0**、**TLS v1.0**、**TLS v1.1**、または **TLS v1.2** を選択できます。

手順 4　ルールを追加するか、編集を続けます。

変更を反映させるには、その SSL ポリシーに関連付けたアクセス コントロール ポリシーを適用する必要があります（設定変更の展開（4-13 ページ）を参照してください）。