CHAPTER 4

仮想 Web アプリケーションに関する作業

この章では、Web アプリケーションのセキュリティ設定方法について説明します。内容は次のとおりです。

仮想 Web アプリケーションの作成

仮想 Web アプリケーションは、一連のルールおよびセキュリティ動作を特定のトラフィック クラスに適用します。一般的には、保護を適用する実際のバックエンド Web アプリケーションごとに 1 つの仮想 Web アプリケーションをポリシーに追加する必要があります。しかし、仮想 Web アプリケーションと実際のバックエンド アプリケーションとの間のやり取りはそのアプリケーションの性質によって異なります。

仮想 Web アプリケーションの作成時には、適用するメッセージを選択するユーザ インターフェイスを定義します。メッセージ照合を曖昧にしないために、Manager では 2 つの仮想 Web アプリケーションに同一のトラフィック フィルタリング基準を設定できません。しかし、プレフィクス照合、正規表現、または他の重複するフィルタリング条件を使用することによって、1 つのメッセージで照合できる複数の仮想 Web アプリケーションを導入することはそれでもなお可能です。メッセージと複数の仮想 Web アプリケーションに互換性がある場合、一致度の高いユーザ インターフェイスを持つアプリケーションが優先されます。もう少し具体的に述べると、ユーザ インターフェイスとは、たとえばより長いパスまたはより多数の選択パラメータが設定されている仮想 URL です。

新しい仮想 Web アプリケーションは、次の 2 つの基本モードで作成できます。

- [Basic Virtual URL] オプションを使用する。ユーザが入力する URL に基づいて、仮想 Web アプリケーションのユーザ インターフェイスの各種設定が Manager によって自動的に生成されます。
- [Custom Virtual URL with Filters] オプションを使用する。パラメータまたは HTTP ヘッダー値に基づいてトラフィックを選択できる機能など、仮想 Web アプリケーション用に生成されたユーザ インターフェイスのきめ細かいコントロールを提供します。

仮想 URL および要求フィルタ設定は、仮想 Web アプリケーションのユーザ インターフェイスを構成します。このアプリケーションでは要求パラメータのフィルタリングなど詳細なトラフィック選択基準が不要な場合、[Basic Virtual URL] メニュー オプションを使用してインターフェイスを設定できます。

[Custom Virtual URL with Filters] オプションで提供される設定は、[Basic Virtual URL] オプションを使用して作成される仮想 Web アプリケーションで使用できることに注意してください。したがって、ほとんどの場合、Basic Virtual URL モードで仮想 Web アプリケーションを作成し、必要に応じて後で詳細なフィルタリング プロパティを変更するのが妥当です。

仮想 Web アプリケーションに対するメッセージは、Reactor 処理エンジンによって処理されます。仮想 Web アプリケーションの設定時には、ポリシー内のサーバ定義および Reactor 対応のポートだけと互換性があることを覚えておく必要があります。Flex Path だけを使用するように設定されたポートまたはサーバ定義は、これらの属性を仮想 Web アプリケーションを割り当てるときにユーザ インターフェイスで使用できません。仮想 Web アプリケーション作成後に、そのポートまたはサーバ定義が Flex Path を使用するように変更されると、ポリシー コンパイル エラーが生成されます。

[Basic Virtual URL] を使用した仮想 Web アプリケーションの作成

Basic Virtual URL モードを使用して新しい仮想 Web アプリケーションを作成するには、次の手順を実行します。

ステップ 1　操作メニューで [Virtual Web Applications] リンクをクリックします。

ステップ 2　[New Virtual Web Application] ボタンをクリックして、ポリシーで新しい仮想 Web アプリケーションの定義を作成します。仮想 Web アプリケーションは、ACE Web Application Firewall でトラフィックの処理と検証を行う、特定のバックエンド アプリケーションの設定をカプセル化します。

ステップ 3　次の表の情報を使用して、仮想 Web アプリケーションを設定します。

表 4-1　仮想 Web アプリケーションの設定

ラベル	説明
[Name]	ポリシーでこの仮想 Web アプリケーション定義を識別するのに使用される記述名。この名前は、ポリシー内の仮想 Web アプリケーションで一意である必要があります。この名前は、この仮想 Web アプリケーションに関連付けられているイベントのログ記述に表示されます。したがって、イベント ログのユーザが理解できる名前にする必要があります。
[Web App Group]	この仮想 Web アプリケーションが作成されるグループ。メニューにリスト表示される既存のグループから選択するか、[new Web App Group] を選択し、グループの名前を入力することによってアプリケーションの新しいグループを作成できます。 一般的には、グループは、同時管理および監視が必要な仮想 Web アプリケーションをすべて含む必要があります。グループで実行できる管理作業には、動作モードの設定、仮想 Web アプリケーションの無効化などがあります。グループは、監視用の基準点でもあります。Web App Firewall Incidents レポートは、グループごとに情報を示すからです。

ラベル	説明
[Basic Virtual URL]	このオプションを使用して、この仮想 Web アプリケーションで処理される受信要求内の要求 URL の識別部分を次のように指定します。 http://example.com/oakinsurance/ これは、Firewall に対する要求にユーザが対応するアドレスです。要求 URL に対して*プレフィクス照合*を実行するために使用されます。この URL または任意のサブパスに対する要求は、この仮想 Web アプリケーションと合致する必要があります。たとえば、http://example.com/oakinsurance/customer です。要求 URL の後続部分が存在する場合には、送信要求に反映されます。 URL のホスト部分には、ホスト名または IP アドレスを設定できます。ポリシーが導入される ACE Web Application Firewall のネットワーク インターフェイスでも設定されている場合に限り、IP アドレスを指定します。それ以外の場合、ポリシー導入後には Firewall で Reactor 処理を開始できません。 入力する Basic Virtual URL 値は、仮想 Web アプリケーションの複数のプロパティを挿入するために次のように使用されます。 • ホストとポートの組み合わせに対してポート/ホスト名オブジェクトが存在しない場合、新しいポート/ホスト名オブジェクトを作成するのに値のホスト部分が使用されます。 • デフォルトでは、要求ホストに基づいてサーバ定義が作成され、新しい仮想 Web アプリケーション オブジェクトの宛先サーバとして設定されます。 • パスのホスト名以外の部分は、仮想 Web アプリケーション オブジェクトの Path 値として使用されます。パスとポート ホスト名は、Cisco ACE Web Application Firewall によって Web アプリケーションがクライアントに公開される URL を構成します。 仮想 Web アプリケーション エディタによって生成されたポート/ホスト名オブジェクトを後で設定して、仮想ホスト名での正規表現照合を実行することは可能ですが、仮想 Web アプリケーションの作成時に [Basic Virtual URL] フィールドに正規表現を直接入力することはできません。このフィールドでは、文字、数字、ドット、およびハイフン文字だけが受け入れられます。
[Matching Mode]（Custom Virtual URL with Filters 設定）	入力したパスに基づいて、ACE Web Application Firewall が値を使用して要求を照合する方法を選択します。このオプションのチェックボックスを選択することによって、大文字と小文字を区別する方法で値を照合するかどうかも選択します。 詳細については、[Path] フィールドに関する前述の説明を参照してください。

ラベル	説明
[Destination Server]	この仮想 Web アプリケーションのバックエンドの宛先として機能する HTTP サーバ。Cisco ACE Web Application Firewall は、この仮想 Web アプリケーションによって認められたトラフィックをこの宛先ホストに送信します。このメニューに表示されるサーバは、[Destination HTTP Servers] ページで設定されているサーバです。 [same as virtual URL] に設定すると、宛先サーバは [Virtual URL] フィールドで識別されるホストに自動設定されます。[Custom Virtual URL with Filters] オプションを選択すると、宛先サーバは、[Port/Hostname] フィールドにマップされます。 **（注）** 仮想 Web アプリケーションは、Reactor 処理だけを使用する宛先サーバに割り当てることができます。Flex Path 処理を使用する宛先サーバとの互換性はありません。仮想 Web アプリケーションの設定ページでは、Flex Path 処理を使用する宛先サーバは、宛先サーバの選択メニューに表示されません。Flex Path 処理を使用するように後で変更された宛先サーバに仮想 Web アプリケーションが割り当てられている場合、この仮想 Web アプリケーションは正しく機能せず、ポリシーのコンパイル中にエラーが発生します。HTTP ポートについても同様です。
[Timeout]	ACE Web Application Firewall が、各要求に対する宛先サーバからの応答を待機する時間。
[Firewall Profile]	この Web アプリケーションに適用するトラフィック処理および検証プロファイル。プロファイルとは、ルールとアクティブなセキュリティ設定の指定の集合です。この設定には、指定のルールが有効かどうか、およびその設定パラメータが含まれます。 使用するプロファイルが存在しない場合、プロファイルに組み込みプロファイルの 1 つを設定し、後で変更できます。
[Monitor Mode]	選択した場合、仮想 Web アプリケーションの初期動作モードは監視モードに設定されます。監視モードでは、アプリケーション プロファイルのメッセージ インスペクション ルールを起動させるメッセージが遮断されません。その代わりに、イベントがログに記録されて通過します。 仮想 Web アプリケーション設定を初めて導入し、テストするときに監視モードにしておくと、役立つ場合が多くあります。これによって、実際の稼動トラフィックに影響を与えることなく、false positive（つまり、正規のトラフィックではあるものの、攻撃シグニチャに合致するトラフィック）がないかどうかを確認できます。仮想 Web アプリケーションによって false positive が生成される場合には、イベントのログ記述から、遮断イベントを起動したルールから合致したトラフィックを除外する修飾子をただちに作成できます。 メッセージ リライト ルールは、監視モードの仮想 Web アプリケーションによって処理されるトラフィックに適用されることに注意してください。 また有効モードでは、メッセージが最初にルールに違反した時点で拒否され、プロファイルの他のルールに対して評価が行われることはありません。イベント ログまたはインシデント レポートでは、メッセージ遮断の原因となったルールだけを示します。メッセージが違反した可能性があるが、処理が続行された他のルールは示されません。一方、監視モードでは、メッセージが違反したすべてのルールが示されます。

ステップ 4　完了したら [Save Changes] をクリックして、新しい仮想 Web アプリケーションを作業ポリシーに渡します。

[Custom Virtual URL With Filters] を使用した仮想 Web アプリケーションの作成

Custom Virtual URL With Filters モードを使用して新しい仮想 Web アプリケーションを作成するには、「[Basic Virtual URL] を使用した仮想 Web アプリケーションの作成」（P.4-2）の手順に従います。しかし [Basic Virtual URL] オプションではなく、[Custom Virtual URL With Filters] を選択し、このオプションに特有の設定を行います。

表 4-2　Virtual URL フィルタの設定

ラベル	説明
[Port/Hostname]（Custom Virtual URL with Filters 設定）	仮想 Web アプリケーションがこの Web アプリケーションのトラフィックを待ち受ける、ポート オブジェクト。ポートは、リスニング ポートの番号および仮想ホスト名を定義します。ポートは、Cisco ACE Web Application Firewall におけるヘルス チェックに使用できる固定応答ページの設定も提供します。ポートがメニューに表示されない場合は、[HTTP Ports & Hostnames] ページで作成します。 [Destination Server] オプションが [same as virtual URL] に設定されている場合、[Port/Hostname] の値が仮想 Web アプリケーションの宛先サービスとして自動的に反映されます。既存の宛先サーバ設定を維持したままポートおよびホスト名の値を変更するには、[Destination Server] を [same as virtual URL] オプションから特定の宛先サーバの定義に変更します。 **（注）** 仮想 Web アプリケーションは、Reactor 処理だけを使用するポートに割り当てることができます。Flex Path 処理を使用するポートとの互換性はありません。仮想 Web アプリケーションの設定ページでは、Flex Path 処理を使用するポートは、ポートの選択メニューに表示されません。仮想 Web アプリケーションがポートに割り当てられ、Flex Path 処理を使用するように後で変更された場合、この仮想 Web アプリケーションは正しく機能せず、ポリシーのコンパイル中にエラーが発生します。HTTP サーバについても同様です。

ラベル	説明
[Path]（Custom Virtual URL with Filters 設定）	この仮想 Web アプリケーションと照合する着信要求によって対応されるパス。パスの [Matching Mode] 設定で指定されるように、パスは次のとおりになります。 • 照合するメッセージの実際の要求パス（oakinsurance/customer など） これは、追加文字を使用せずに文字列全体を要求パスとして指定する要求だけに合致します。 • 要求パスに対するプレフィクス（oakinsurance/ など） このパスは、oakinsurance/customer/getquote または oakinsurance/partners など oakinsurance/ で始まるすべての要求アドレスに合致します。 • 正規表現要素を含むように作成されたパス（oakinsurance/.*/getquote など） この場合、任意の文字の照合に正規表現のコマンド シーケンス（.*）が使用され、oakinsurance/customer/getquote と oakinsurance/partners/getquote の両方が合致するようになります。 このフィールドでは、バックスラッシュ文字を使用して正規表現のコマンド文字をエスケープできます。 Cisco ACE Web Application Firewall の Web アプリケーション セキュリティ機能における正規表現の実装は、Perl-Compatible Regular Expressions（PCRE）に基づいています。
[Matching Mode]（Custom Virtual URL with Filters 設定）	入力したパスに基づいて、ACE Web Application Firewall が値を使用して要求を照合する方法を選択します。このオプションのチェックボックスを選択することによって、大文字と小文字を区別する方法で値を照合するかどうかも選択します。詳細については、[Path] フィールドに関する前述の説明を参照してください。
[Methods]（Custom Virtual URL with Filters 設定）	この仮想 Web アプリケーションと照合する要求の HTTP 要求方式。この方式は、「GET /images/logo.gif HTTP/1.1」の GET のように、要求の要求行の最初のトークンとして表示されます。次のオプションがあります。 • [ignore] : HTTP 要求方式は考慮されません。 • [basic HTTP methods (GET/POST/HEAD)] : DELETE または TRACE など他の方式の要求を除き、リスト表示されている方式だけと照合します。 • [any standard HTTP 1.x method] : 要求は、GET、POST、HEAD、PUT、DELETE、OPTIONS、または TRACE など HTTP 1.0 または 1.1 標準方式として定義された要求です。 • [specified HTTP 1.x methods] : 選択した、HTTP 1.0 または 1.1 標準方式。 • [custom] : ユーザが指定する任意の方式。1 つ以上の方式を入力した場合、1 行ごとに 1 つの方式を指定します。名前は、要求の 1 行目で指定された方式と完全に合致する必要があります。入力した方式名は、自動的に大文字に変換されます。これらは、大文字と小文字を区別する方法でメッセージと照合されます。

ラベル	説明
[HTTP Headers]（Custom Virtual URL with Filters 設定）	要求内の 1 つまたはそれ以上の HTTP ヘッダーの存在または値に基づいてこの仮想 Web アプリケーションと要求を照合するには、このオプションを設定します。指定の HTTP ヘッダーまたは値が含まれない要求は、この仮想 Web アプリケーションでは処理されません。HTTP ヘッダー値は大文字と小文字を区別する方法で照合されますが、HTTP ヘッダー名は、大文字と小文字を区別しない方法で照合されます。
[Parameters]（Custom Virtual URL with Filters 設定）	1 つまたはそれ以上の要求パラメータ の存在または値に基づいてこの仮想 Web アプリケーションと要求を照合するには、このオプションを設定します。要件に合致しないパラメータを持つ要求は、この仮想 Web アプリケーションでは処理されません。パラメータ名および値は、大文字と小文字を区別する方法でメッセージと比較されます。 パラメータは、要求内の URL 引数または POST 要求の本文中のパラメータである場合もあります。URL 引数は、「zip」パラメータおよび「session」パラメータで示されるように、要求 URL 内のアンパサンドで区切られた名前と値のペアとして表示されます。たとえば、次のとおりです。 oakinsurance/partners/getquote?zip=94114&session=01234 パラメータの要件は、Perl 形式の正規表現を使用して、または名前でパラメータを識別することによって、設定できます。次の演算子を使用して要求パラメータの要件を指定します。 • exists：メッセージには、指定パラメータが含まれる必要があります。 • matches regex：指定パラメータの値は、指定した regex に合致する必要があります。 • is：指定パラメータの値は、大文字小文字を区別する方法で指定した文字に合致する必要があります。 • is not：指定パラメータの値は、大文字小文字を区別する方法で指定した文字に合致する必要はありません。 照合または非照合（「is not」）を指定するのに、要求内にパラメータが含まれている必要はありません。つまり、それ以外ではフィルタに合致する要求が、照合値または非照合値を指定したパラメータを含まない場合、要求は受け入れられます。

監視モードの使い方

仮想 Web アプリケーションの処理モードは、次のいずれかです。

- 有効：ACE Web Application Firewall は、メッセージ インスペクション ルールに違反するメッセージを遮断し、コンテンツ リライト ルールおよびアクティブなセキュリティ機能を適用します。
- 監視モード：選択した場合、ACE Web Application Firewall は、メッセージ インスペクション ルールに合致するか、アクティブなセキュリティ設定に違反するトラフィックを遮断しません。その代わりに、イベントをログに記録します。このモードは、トラフィック フローに影響を与えずに設定テストまたは潜在的に悪意のあるトラフィック普及の監視を行うのに便利です。仮想 Web アプリケーションが監視モードの場合でも、トラフィックにはメッセージ リライト ルール、HTTP 処理、例外マッピング、および cookie セキュリティが適用されます。
- 無効：ACE Web Application Firewall が、仮想 Web アプリケーションに定義されたユーザ インターフェイスでトラフィックを受信しないようにします。無効になっている仮想 Web アプリケーションで照合されたメッセージに合致する、一致度の低い仮想 Web アプリケーションのユーザ インターフェイスが存在する場合を除き、トラフィックは遮断されます。

監視モードは、ポリシーのテスト時および作成時に特に役立ちます。有効モードでは、メッセージが最初にルールに違反した時点で拒否されます。プロファイル内の他のルールに対して評価されることはありません。イベント ログまたはインシデント レポートでは、メッセージ遮断の原因となったルールだけを示します。メッセージが違反した可能性があるが、処理が続行された他のルールは示されません。一方、監視モードでは、メッセージがルールに違反していることが判明した場合、プロファイル内の他のルールによる処理は続行されます。これにより、最初に起動された遮断ルールだけではなく、メッセージが違反するすべてのルールをログに表示できます。

動作状態は、次の複数の状況でポリシー内に設定できます。

- プロファイル内のルールのため
- 個々の仮想 Web アプリケーションのため
- グループのため
- ポリシー内のすべての仮想 Web アプリケーションのため

新たに作成した仮想 Web アプリケーションには、デフォルト モードも指定できます。ネットワーク トラフィックに影響を及ぼす前に仮想 Web アプリケーションとネットワーク トラフィックとの対話に注意することが、常に推奨されるからです。

指定の仮想 Web アプリケーションでは、監視モードは同じ方法（ポリシー全体に設定されるか、グループから設定されるか、または仮想 Web アプリケーションだけに設定されるか）で機能します。

動作モードをポリシー全体に設定するには、次の手順を実行します。

ステップ 1　操作メニューで [Virtual Web Applications] リンクをクリックします。

ステップ 2　仮想 Web アプリケーションの [Set all virtual web apps to] メニューで、使用する動作モード（有効、監査モード、または無効）を選択します。

グループごとに動作モードを設定するには、次の手順を実行します。

ステップ 1　操作メニューで [Virtual Web Applications] リンクをクリックします。

ステップ 2　設定する仮想 Web アプリケーション グループの名前をクリックします。グリーンの影付きヘディングにグループ名が表示されます。

ステップ 3　グループのページの [Set all virtual web apps to] メニューで、使用する動作モード（有効、監査モード、または無効）を選択します。

個別の仮想 Web アプリケーションに動作モードを設定するには、次の手順を実行します。

ステップ 1　操作メニューで [Virtual Web Applications] リンクをクリックします。

ステップ 2　設定する仮想 Web アプリケーションの名前をクリックします。グリーンの影付きヘディングにグループ名が表示されます。

ステップ 3　概要ヘッダーの右側にある [edit] リンクから

ステップ 4　ページ最下部にある [Monitor Mode] チェックボックスをクリックします。

モードの変更は、1 回限りのイベントとして適用されます。つまり、このコントロールで監視モードを設定すると、グループまたは仮想 Web グループの動作モードは、個別に変更できます。

修飾子の作成

仮想 Web アプリケーションは、1 つ以上の修飾子を含むことができます。仮想 Web アプリケーションと同様に、修飾子は、選択されたトラフィックにルールおよびセキュリティ動作を適用します。しかし、修飾子は、仮想 Web アプリケーションで処理されるトラフィックからのトラフィックだけを選択します。修飾子は、それが含まれる仮想 Web アプリケーションによって処理されるトラフィックのサブセットにトラフィック処理設定を適用します。

修飾子の設定は、元は仮想 Web アプリケーションから得られたものですが、この仮想 Web アプリケーションからは独立しています。つまり、修飾子によって選択されたメッセージは、その処理設定だけに従います。修飾子の設定および仮想 Web アプリケーションの設定には従いません。

修飾子は、直接、またはイベント ログから作成できます。仮想 Web アプリケーション ルールに関連付けられているイベントの場合、イベント ログ記述に [Create Exemption] リンクが含まれています。このリンクでは、ポリシーを迅速に変更して、false positive を回避できます。このリンクによって、仮想アプリケーション向けの新しい修飾子のページが、イベントに基づいたプリセットの設定を備えた状態で作成されます。

（注）　修飾子は、異なる処理または検証を実行するトラフィックの明確なサブクラスが仮想 Web アプリケーションに存在する場合にだけ使用します。多くの場合、false positive を生成した要求の品質は、修飾子によって選択されたトラフィックのサブクラスに対してだけではなく、Web アプリケーションの他の部分に対する要求にも存在します。この場合は、修飾子を追加するのではなく、プロファイルレベルの変更を行うことによって false positive に対応する方が適切なことが多くなります。

修飾子を作成すると、そのトラフィック フィルタには、必須のフィルタ基準が仮想 Web アプリケーションから事前設定されます。必須設定を変更しようとすると、インターフェイスにエラー メッセージが表示されます。仮想 Web アプリケーションのフィルタ基準を変更して、既存の修飾子と互換性のないようにすると、コンパイル時のエラーが生成されます。

修飾子の直接作成

修飾子を直接作成する（つまり、イベント ログ インシデントを使用しない）には、次の手順を実行します。

ステップ 1　操作メニューで [Virtual Web Applications] リンクをクリックします。

ステップ 2　修飾子を作成する仮想 Web アプリケーションの名前をクリックします。

ステップ 3　[add modifier] リンクをクリックします。

ステップ 4　[Request Filter for Firewall Modifier] ページで、この修飾子が適用するトラフィック選択基準を選択します。設定は、仮想 Web アプリケーションのトラフィック選択基準で事前に設定されます。

修飾子は、要求フィルタ基準に基づいて仮想 Web アプリケーションによって処理されたトラフィック フローからトラフィックを選択することに注意してください。したがって、修飾子選択基準は、より具体的な基準ですが、仮想 Web アプリケーションの基準との互換性も必要です。たとえば URL パスによって選択される修飾子では、修飾子のパスが仮想 Web アプリケーションのパスを拡張する必要があることを意味します。

次の表に記載されたフィルタ設定を設定します。

表 4-3　フィルタ設定

ラベル	説明
[Path]	この修飾子を適用するメッセージを選択する要求パス。修飾子は、仮想 Web アプリケーションによって処理されたトラフィック ストリームからメッセージを選択します。したがってパスは、仮想 Web アプリケーションのパスを拡張する必要があります。たとえば、仮想 Web アプリケーションのパスが「/oakinsurance」の場合、修飾子のパスは「/oakinsurance/customer」または「/oakinsurance/partners/quotes/」とすることができます。
[Methods]	仮想 Web アプリケーションで受け入れられる HTTP 方式から、この修飾子のサブセットが受け入れる方式を選択します。仮想 Web アプリケーションで受け入れられる方式は、要求フィルタで事前設定されています。
[HTTP Headers]	受信要求内の HTTP ヘッダー値に基づいて、トラフィック選択基準を指定します。
[Parameters]	受信要求内のパラメータに基づいてトラフィック選択基準を指定します。

ステップ 5　[Save Changes] をクリックします。

ステップ 6　[Edit Firewall Modifier] ページに、親の仮想 Web アプリケーションによって適用されるプロファイルが表示されます。ルールのオーバーライド リンクをクリックすることによって、この修飾子のトラフィック処理に適切な設定に変更します。修飾子によって適用される個別のセキュリティ動作、メッセージ インスペクション ルール、およびメッセージ リライト ルールを設定できます。

ステップ 7　完了したら、[Exit to Virtual Web App Group] リンクをクリックします。

インシデントベースの修飾子の作成

ACE XML Manager では、Firewall での実際のトラフィックによって生成されたインシデントに基づいて、ポリシーを迅速に調整できます。この機能では、ポリシーを迅速に設定して、特に false positive の結果として（つまり、誤ってセキュリティ上の脅威として分類された正規のメッセージのために）インシデントを生成したトラフィックを受け入れます。

（注）　デフォルトでは、インシデントベースの修飾子は、非常に具体的なトラフィック選択基準を生成します。これは、仮想 Web アプリケーションにおける独立したトラフィックのサブクラスに異なる処理または検証を行うことだけを目的として作成する必要があります。多くの場合、false positive を生成した要求の品質は、修飾子によって選択されたトラフィックのサブクラスに対してだけではなく、Web アプリケーションの他の部分に対する要求にも存在します。この場合は、修飾子を追加するのではなく、プロファイルレベルの変更を行うことによって false positive に対応する方が適切なことが多くなります。

インシデントベースの修飾子を作成するには、次の手順を実行します。

ステップ 1　操作メニューで [Event Log] リンクをクリックします。

ステップ 2　修飾子を作成する場所で、イベントのログ記述を探します。ページ上部でのログ表示フィルタリング基準の調整が必要な場合があります。

Web アプリケーションのセキュリティ イベントに関するイベント記述には、[Create Exemption] リンクが含まれます。

ステップ 3　項目の [Create Exemption] リンクをクリックします。イベントに基づいて、修飾子を作成できるページが開きます。

ステップ 4　必要に応じてデフォルトの設定を調整し、設定を保存します。修飾子の設定に関する詳細については、「修飾子の直接作成」（P.4-10）を参照してください。