CHAPTER 15

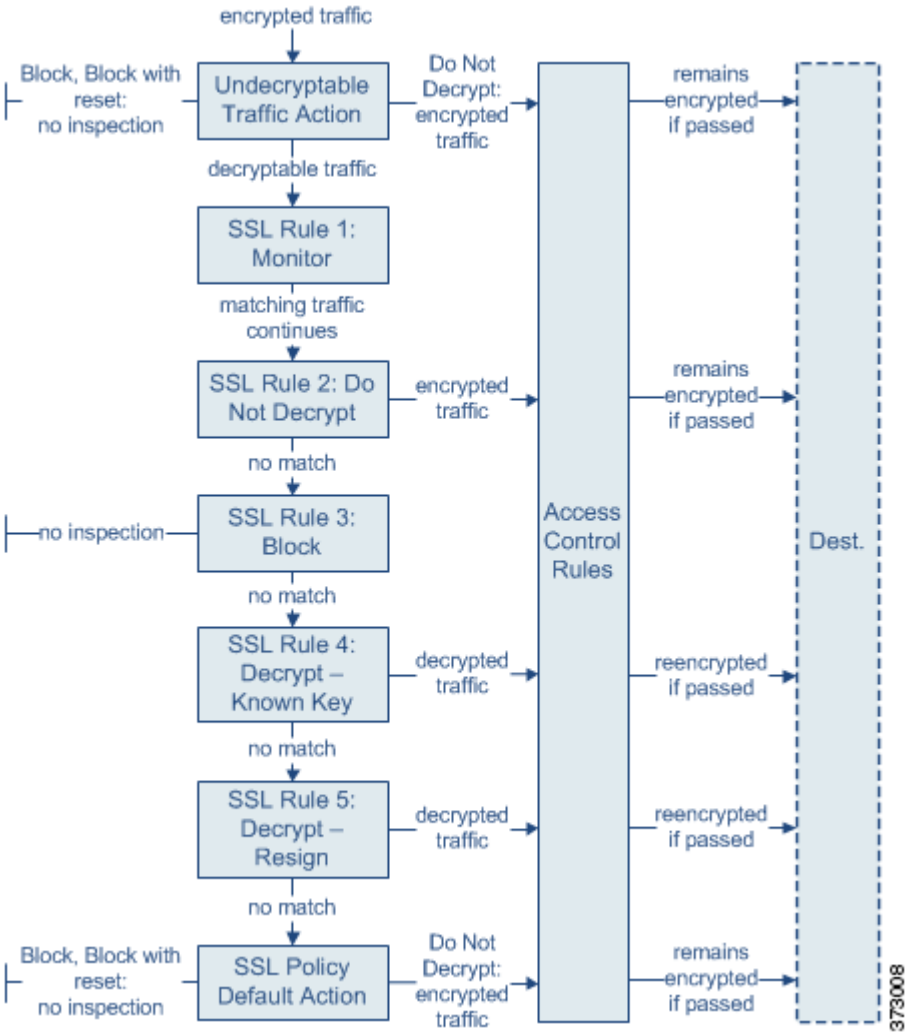
# SSL ルール クイック スタート ガイド

SSL ポリシー内に、各種の *SSL ルール*を設定することで、それ以上のインスペクションなしでトラフィックをブロックする、トラフィックを復号化せずにアクセスコントロールで検査する、あるいはアクセス コントロールの分析用にトラフィックを復号するなど、きめ細やかな暗号化トラフィックの処理メソッドを構築できます。

ASA FirePOWER モジュールは指定した順序で SSL ルールをトラフィックと照合します。ほとんどの場合、モジュールによる暗号化トラフィックの処理は、すべてのルールの条件がトラフィックに一致する*最初の* SSL ルールに従って行われます。こうした条件には、単純なものと複雑なものがあります。セキュリティ ゾーン、ネットワークまたは地理的位置、ポート、アプリケーション、要求された URL、ユーザ、証明書、証明書の識別名、証明書ステータス、暗号スイート、暗号化プロトコル バージョンなどによってトラフィックを制御できます。

また、各ルールには 1 つの *アクション*があり、一致するトラフィックの復号化後にオプションでモニタするか、ブロックするか、または一致したトラフィックをアクセス コントロールで検査するかを決定します。システムがブロックした暗号化トラフィックは、それ以上のインスペクションが**行われない**ことに注意してください。暗号化後および復号化できないトラフィックは、アクセス コントロールを使用して検査します。ただし、一部のアクセス コントロール ルールの条件では暗号化されていないトラフィックを必要とするため、暗号化されたトラフィックに一致するルール数が少なくなる場合があります。またデフォルトでは、モジュールは暗号化ペイロードの侵入およびファイルのインスペクションを無効化します。

次のシナリオは、インライン展開での SSL ルールによるトラフィックの処理を示します。




このシナリオでは、トラフィックは次のように評価されます。

- **復号化できないトラフィック アクション（Undecryptable Traffic Action）**は、暗号化されたトラフィックを最初に評価します。復号化できないトラフィックについて、モジュールはそれ以上のインスペクションなしでブロックするか、あるいはアクセス コントロールによるインスペクション用に渡します。一致しなかった暗号化トラフィックは、次のルールへと進められます。
- **SSL ルール 1：モニタ（SSL Rule 1: Monitor）**は、暗号化トラフィックを次に評価します。モニタ ルールは、暗号化トラフィックのログ記録と追跡を行いますが、トラフィック フローには影響しません。モジュールは引き続きトラフィックを追加のルールと照合し、許可するか拒否するかを決定します。
- **SSL ルール 2：復号化しない（SSL Rule 2: Do Not Decrypt）**は、暗号化トラフィックを 3 番目に評価します。一致したトラフィックは復号されません。モジュールはこのトラフックをアクセス コントロールにより検査しますが、ファイルや侵入インスペクションは行いません。一致しなかったトラフィックは、次のルールへと進められます。
- **SSL ルール 3：ブロック（SSL Rule 3: Block）**は、暗号化トラフィックを 4 番目に評価します。一致したトラフィックは、それ以上のインスペクションは行わずに、ブロックされます。一致しなかったトラフィックは、次のルールへと進められます。

- **SSL ルール 4：復号化 - 既知のキー（SSL Rule 4: Decrypt - Known Key）**は、暗号化トラフィックを 5 番目に評価します。ネットワークへの着信トラフィックで一致したものは、ユーザのアップロードする秘密キーを使用して復号化されます。復号化トラフィックはその後、アクセス コントロール ルールで評価されます。アクセス コントロール ルールは、復号化されたトラフィックと暗号化されていないトラフィックで同じ処理をします。この追加のインスペクションの結果、そのモジュールがトラフィックをブロックする場合があります。他のすべてのトラフィックは、宛先への送信が許可される前に再暗号化されます。SSL ルールに一致しなかったトラフィックは、次のルールへと進められます。
- **SSL ルール 5：復号化 - 再署名（SSL Rule 5: Decrypt - Resign）**は、最後のルールです。トラフィックがこのルールに一致した場合、モジュールはアップロードされた CA 証明書を使用してサーバ証明書を再署名してから、中間者としてトラフィックを復号化します。復号化トラフィックはその後、アクセス コントロール ルールで評価されます。アクセス コントロール ルールは、復号化されたトラフィックと暗号化されていないトラフィックで同じ処理をします。この追加のインスペクションの結果、そのモジュールがトラフィックをブロックする場合があります。他のすべてのトラフィックは、宛先への送信が許可される前に再暗号化されます。SSL ルールに一致しなかったトラフィックは、次のルールへと進められます。
- **SSL ポリシーのデフォルト アクション（SSL Policy Default Action）**は、他の SSL ルールに一致しなかったすべてのトラフィックを処理します。デフォルト アクションでは、暗号化トラフィックをそれ以上のインスペクションなしでブロックするか、あるいは復号化しないままにして、アクセス コントロールによる検査を行います。

詳細については、次の項を参照してください。

- サポートする検査情報の設定（15-3 ページ）
- SSL ルールの概要と作成（15-4 ページ）
- ポリシー内の SSL ルールの管理（15-13 ページ）

# サポートする検査情報の設定

**ライセンス：**すべて

暗号化セッションの特性に基づいた暗号化トラフィックの制御および暗号化トラフィックの復号化には、再利用可能な公開キー インフラストラクチャ（PKI）オブジェクトの作成が必要です。この情報の追加は、信頼できる認証局（CA）の証明書の SSL ポリシーへのアップロード、SSL ルール条件の作成、およびプロセスでの関連オブジェクトの作成時に、臨機応変に実行できます。ただし、これらのオブジェクトを事前に設定しておくと、不適切なオブジェクトが作成される可能性を抑制できます。

### 証明書とキー ペアによる暗号化トラフィックの復号化

セッション暗号化に使用するサーバ証明書と秘密キーをアップロードして内部証明書オブジェクトを設定しておくと、ASA FirePOWER モジュールは着信する暗号化トラフィックを復号化できます。**Decrypt - Known Key** のアクションが設定された SSL ルールでそのオブジェクトを参照し、当該ルールにトラフィックが一致すると、モジュールはアップロードされた秘密キーを使用してセッションを復号化します。

CA 証明書と秘密キーをアップロードして内部 CA オブジェクトを設定した場合、モジュールは発信トラフィックの復号化もできます。**Decrypt - Resign** のアクションが設定された SSL ルールでそのオブジェクトを参照し、当該ルールにトラフィックが一致すると、システムはクライアント ブラウザに渡されたサーバ証明書を再署名した後、中間者としてセッションを復号化します。

詳細については、次の各項を参照してください。

- 内部証明書オブジェクトの操作（2-45 ページ）
- 内部認証局オブジェクトの操作（2-39 ページ）

### 暗号化セッションの特性に基づいたトラフィック制御

ASA FirePOWER モジュールによる暗号化トラフィックの制御は、セッションのネゴシエートに使用されるサーバ証明書または暗号スイートに基づいて実行できます。複数の異なる再利用可能オブジェクトの 1 つを設定し、SSL ルール条件でオブジェクトを参照しトラフィックを照合することができます。次の表に、設定できる再利用可能なオブジェクトのタイプを示します。

| 設定する内容 | 暗号化トラフィック制御に使用する条件 |
|---|---|
| 1 つまたは複数の暗号スイートが含まれる暗号スイートのリスト | 暗号化セッションのネゴシエートに使う暗号スイートが、暗号スイート リストにある暗号スイートのいずれかに一致する。 |
| 組織の信頼する CA 証明書のアップロードによる信頼できる CA オブジェクト | この信頼できる CA は、次のいずれかにより、セッションの暗号化に使用されたサーバ証明書を信頼する。<br>• CA が証明書を直接発行した。<br>• サーバ証明書を発行した中間 CA に CA が証明書を発行した。 |
| サーバ証明書のアップロードによる外部証明書オブジェクト | セッションの暗号化に使用されたサーバ証明書が、アップロードされたサーバ証明書と一致する。 |
| 発行元の識別名または証明書サブジェクトを含む識別名オブジェクト | セッション暗号化に使用された証明書で、サブジェクトまたは発行元の共通名、国、組織、組織単位のいずれかが、設定された識別名に一致する。 |

詳細については、次の各項を参照してください。

- 地理位置情報オブジェクトの操作（2-46 ページ）
- 信頼できる認証局オブジェクトの操作（2-43 ページ）
- 外部証明書オブジェクトの操作（2-45 ページ）
- 識別名オブジェクトの操作（2-36 ページ）

# SSL ルールの概要と作成

**ライセンス:** すべて

SSL ポリシー内で、SSL ルールによってネットワーク トラフィックを処理するためのきめ細かなメソッドが提供されます。各 SSL ルールには、一意の名前以外にも、次の基本コンポーネントがあります。

**状態**

デフォルトでは、ルールが有効状態になります。ルールを無効にすると、モジュールはネットワーク トラフィックの評価にそのルールを使用せず、そのルールに対する警告とエラーの生成を停止します。

**位置**

SSL ポリシーのルールには 1 から始まる番号が付いています。モジュールは、ルール番号の昇順で、ルールを上から順にトラフィックと照合します。モニタ ルールを除き、トラフィックが一致する最初のルールがそのトラフィックを処理するルールになります。

### 条件

条件は、ルールで処理する特定のトラフィックを指定します。こうした条件では、セキュリティ ゾーン、ネットワークまたは地理的位置、ポート、アプリケーション、要求された URL、ユーザ、証明書、証明書のサブジェクトまたは発行元、証明書ステータス、暗号スイート、暗号化プロトコル バージョンなどによってトラフィックを照合できます。条件には、単純なものと複雑なものがあり、デバイスのライセンスによって用途が異なります。

### アクション

ルールのアクションによって、一致するトラフィックをモジュールがどのように処理するかが決まります。一致したトラフィックに対して行える処理は、モニタする、信頼する、ブロックする、あるいは復号化するです。復号化したトラフィックには、さらにインスペクションが適用されます。モジュールは、ブロックされた暗号化トラフィックと信頼された暗号化トラフィックに対してインスペクションを実行**しない**ことに注意してください。

### ロギング

ルールのロギング設定によって、モジュールが処理するトラフィックについて記録するレコードが管理されます。各ルールに一致したトラフィックのレコードを維持できます。SSL ポリシーでの設定に従って、モジュールが暗号化セッションをブロックするか、あるいはインスペクションなしで渡すことを許可するときに、その接続をログに記録できます。アクセス コントロール ルールに従ってより詳細な評価を行うために復号化した接続をログに記録するようにモジュールを強制することも可能です。これはその後でどのようなトラフィックの処理や検査がなされるかに関係なく行うことができます。接続のログは、モジュール ログ（syslog）または SNMP トラップ サーバに記録できます。

**ヒント**　SSL ルールを適切に作成して順序付けることは複雑な作業ですが、これは効果的な展開を構築する上で不可欠な要素です。慎重なポリシーの設計を怠ると、他のルールをプリエンプション処理したり、追加ライセンスが必要となったり、無効な設定を含んだルールになる可能性があります。予期したとおりにモジュールでトラフィックが確実に処理されるようにするために、SSL ポリシー インターフェイスには、ルールに関する強力な警告およびエラーのフィードバック システムが用意されています。詳細については、SSL ルールのトラブルシューティング（15-16 ページ）を参照してください。

**SSL ルールを作成または変更する手順:**

**ステップ 1**　[Configuration] > [ASA FirePOWER Configuration] > [Policies] > [SSL]の順に選択します。

[SSL Policy] ページが表示されます。

**ステップ 2**　ルールを追加する 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、[Rules] タブにフォーカスが移動します。

**ステップ 3**　次の選択肢があります。

- 新しいルールを追加するには、[Add Rule]をクリックします。
- 既存のルールを編集するには、そのルールの横にある編集アイコン（  ）をクリックします。

SSL ルール エディタが表示されます。

**ステップ 4**　[Name]にルールの名前を入力します。

各ルールには一意の名前が必要です。30 文字までの印刷可能文字を使用できます。スペースや特殊文字を含めることができますが、コロン（:）は使用できません。

**ステップ 5**　前述の説明に従い、ルール コンポーネントを設定します。次の設定をするか、デフォルト設定をそのまま使用することができます。

- ルールを有効にするかどうか [Enabled]を指定します。
- ルールの位置を指定します。「SSL ルールの評価順序の指定（15-6 ページ）」を参照してください。
- ルールの[Action] を選択します。「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（15-9 ページ）」を参照してください。
- ルールの条件を設定します。「条件を使用したルールによる暗号化トラフィックの処理の指定（15-7 ページ）」を参照してください。
- [Logging]オプションを指定します。「SSL ルールによる復号可能接続のロギング（35-15 ページ）」を参照してください。

**ステップ 6**　[Save]をクリックしてルールを保存します。

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（4-12 ページ）を参照してください）。

# SSL ルールの評価順序の指定

**ライセンス：**すべて

SSL ルールを最初に作成するときに、ルール エディタの [Insert] ドロップダウン リストを使用して、その位置を指定します。SSL ポリシーの SSL ルールには 1 から始まる番号が付いています。ASA FirePOWER モジュールは、ルール番号の昇順で、SSL ルールを上から順にトラフィックと照合します。

ほとんどの場合、モジュールによるネットワーク トラフィックの処理は、*すべて*のルールの条件がトラフィックに一致する*最初の* SSL ルールに従って行われます。Monitor ルールの場合を除き（トラフィックをログに記録するが、トラフィック フローには影響しない）、いずれかのルールとトラフィックが一致した後、モジュールは優先順位の低い追加ルールとの突き合わせによるトラフィックの評価は続行**しません**。

**ヒント**　適切な SSL ルールの順序は、ネットワーク トラフィックの処理に必要なリソースを軽減し、ルールのプリエンプションを回避します。ユーザが作成するルールはすべての組織と展開に固有のものですが、ユーザのニーズに対処しながらもパフォーマンスを最適化できるルールを順序付けする際に従うべきいくつかの一般的なガイドラインがあります。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（15-18 ページ）を参照してください。

ルールは数値で順序付けするだけでなく、カテゴリ別にグループ化することもできます。デフォルトで、システムには 3 つのカテゴリ（管理者、標準、ルート）があります。カスタム カテゴリを追加できますが、ASA FirePOWER モジュール提供のカテゴリを削除したり、それらの順序を変更したりすることはできません。既存のルールの位置またはカテゴリの変更の詳細については、「SSL ルールの位置またはカテゴリの変更（15-15 ページ）」を参照してください。

**ルールの編集や作成中にルールをカテゴリに追加する手順：**

**ステップ 1**　SSL ルール エディタの [Insert] ドロップダウン リストで [Into Category] を選択し、適用するカテゴリを選択します。

ルールを保存すると、そのカテゴリの最後に配置されます。

**ルールの編集や作成中にルールの位置を数値で指定する手順:**

**ステップ 1**　SSL ルール エディタの [Insert] ドロップダウン リストで [above rule] または [below rule] を選択し、適切なルール番号を入力します。

ルールを保存すると、指定した位置に配置されます。

# 条件を使用したルールによる暗号化トラフィックの処理の指定

**ライセンス:**機能によって異なる

SSL ルールの条件は、ルールで処理する暗号化トラフィックのタイプを特定します。条件には、単純なものと複雑なものがあり、ルールごとに複数の条件タイプを指定できます。トラフィックにルールが適用されるのは、トラフィックがルールの条件をすべて満たしている場合だけです。

ルールに対し特定の条件を設定しない場合、モジュールはその基準に基づいてトラフィックを照合しません。たとえば、証明書の条件が設定されバージョンの条件が設定されていないルールは、セッション ネゴシエーションに使用されるサーバ証明書に基づいてトラフィックを評価し、セッション SSL または TLS のバージョンは関係しません。

SSL ルールを追加および編集するときは、ルール エディタ下部の左側にあるタブを使用して、ルール条件の追加と編集を行います。SSL ルールに追加できる条件を次の表に示します。

*表 15-1　SSL ルールの条件タイプ*

| 条件 | 一致する暗号化トラフィック | 詳細 |
|---|---|---|
| ゾーン | 特定のセキュリティ ゾーンでインターフェイスを介したデバイスへの着信またはデバイスからの発信 | セキュリティ ゾーンは、ご使用の導入ポリシーおよびセキュリティ ポリシーに準じた 1 つ以上のインターフェイスの論理グループです。ゾーン条件を作成するには、ネットワーク ゾーンによる暗号化トラフィックの制御（16-2 ページ）を参照してください。 |
| ネットワーク | 送信元、宛先 IP アドレス、国、または大陸 | 明示的に IP アドレスを指定できます。位置情報の機能では、送信元または宛先となる国や大陸を基準にしたトラフィック制御もできます。ネットワーク条件の作成については、「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（16-4 ページ）」を参照してください。 |
| ポート | 送信元ポートまたは宛先ポート | TCP ポートに基づいて暗号化トラフィックを制御できます。ポート条件の作成については、「ポートによる暗号化トラフィックの制御（16-5 ページ）」を参照してください。 |
| ユーザ | セッションに参加しているユーザ | 暗号化されたモニタ対象セッションの関連ホストにログインしている LDAP ユーザに基づいて暗号化トラフィックを制御できます。Microsoft Active Directory サーバから取得された個別ユーザまたはグループに基づいてトラフィックを制御できます。ユーザ条件の作成については、「ユーザ ベースの暗号化トラフィックの制御（16-7 ページ）」を参照してください。 |

*表 15-1　SSL ルールの条件タイプ（続き）*

| 条件 | 一致する暗号化トラフィック | 詳細 |
|---|---|---|
| アプリケーション | セッションで検出されるアプリケーション | タイプ、リスク、ビジネスとの関連性、カテゴリの基本的な特性に従って、フィルタ アクセスまたは暗号化セッションの各アプリケーションへのアクセスを制御できます。アプリケーション条件の作成については、「アプリケーションベースの暗号化トラフィックの制御（16-9 ページ）」を参照してください。 |
| カテゴリ | 証明書サブジェクトの識別名に基づいてセッションで要求される URL | URL の一般分類とリスク レベルに基づいて、ネットワークのユーザがアクセスできる Web サイトを制限できます。URL 条件の作成については、「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（16-14 ページ）」を参照してください。 |
| 識別名 | 暗号化セッションのネゴシエートに使用されたサーバ証明書のサブジェクトまたは発行元の識別名 | サーバ証明書を発行した CA またはサーバ証明書ホルダーに基づいて、暗号化トラフィックを制御できます。識別名条件の作成については、「証明書の識別名による暗号化トラフィックの制御（16-18 ページ）」を参照してください。 |
| 証明書 | 暗号化セッションのネゴシエートに使用されるサーバ証明書 | 暗号化セッションのネゴシエート用にユーザのブラウザに渡されるサーバ証明書に基づいて、暗号化されたトラフィックを制御できます。証明書条件の作成については、「証明書ステータスによる暗号化トラフィックの制御（16-22 ページ）」を参照してください。 |
| 証明書のステータス | 暗号化セッションのネゴシエートに使用されるサーバ証明書のプロパティ | 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制御できます。証明書ステータス条件の作成については、「証明書ステータスによる暗号化トラフィックの制御（16-22 ページ）」を参照してください。 |
| 暗号スイート | 暗号化セッションのネゴシエートに使用する暗号スイート | 暗号化セッションのネゴシエート用にサーバで選択された暗号スイートに基づいて、暗号化トラフィックを制御できます。暗号スイート条件の作成については、「暗号スイートによる暗号化トラフィックの制御（16-27 ページ）」を参照してください。 |
| バージョン | セッションの暗号化に使用される SSL または TLS のバージョン | セッションの暗号化に使用される SSL または TLS のバージョンに基づいて、暗号化トラフィックを制御できます。バージョン条件の作成については、「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（16-28 ページ）」を参照してください。 |

暗号化トラフィックの制御と検査は可能ですが、トラフィックの制御に検出されたアプリケーション、URL カテゴリ、またはユーザを使用するには追加ライセンスが必要です。また過度に複雑なルールは、多くのリソースを消費し、状況によってはポリシーを適用できなくなる場合があります。詳細については、SSL ルールのトラブルシューティング（15-16 ページ）を参照してください。

# 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

**ライセンス:**すべて

すべての SSL ルールには、一致する暗号化トラフィックに対して次の判定をする関連アクションがあります。

- 処理: まず、ルール アクションは、ASA FirePOWER モジュールがルールの条件に一致する暗号化トラフィックに対して、モニタ、信頼、ブロック、または復号化を行うかどうかを判定します
- ロギング: ルール アクションは一致する暗号化トラフィックの詳細をいつ、どのようにログに記録するかを判定します。

SSL インスペクション設定では、次のように復号化されたトラフィックの処理、検査、ログ記録を行います。

- SSL ポリシーの復号化できないアクションは、ASA FirePOWER モジュールが復号化できないトラフィックを処理します。復号化できないトラフィックのデフォルト処理の設定（14-5 ページ）を参照してください。
- ポリシーのデフォルト アクションは、Monitor 以外のどの SSL ルールの条件にも一致しないトラフィックを処理します。「暗号化トラフィックのデフォルトの処理と検査の設定（14-4 ページ）」を参照してください。

ASA FirePOWER モジュールが暗号化セッションを信頼またはブロックしたときに、接続イベントをログに記録できます。アクセス コントロール ルールに従ってより詳細な評価を行うために復号化した接続をログに記録するようにモジュールを強制することも可能です。これはその後でどのようなトラフィックの処理や検査がなされるかに関係なく行うことができます。暗号化セッションの接続ログには、セッションの暗号化に使用される証明書など、暗号化の詳細が含まれます。ただし次の場合は、接続の終了（end-of-connection）イベントだけをログに記録できます。

- ブロックされた接続（Block、Block with reset）の場合、システムは即座にセッションを終了してイベントを生成します
- 信頼された接続（Do not decrypt）の場合、システムはセッション終了後にイベントを生成します

ルール アクションの詳細および、ルール アクションが処理とログに与える影響の詳細については、次のセクションを参照してください。

- モニタ アクション: アクションの遅延とログの確保（15-9 ページ）
- 復号化しない（Do Not Decrypt）アクション: 暗号化トラフィックを検査なしで転送（15-10 ページ）
- ブロッキング（Block）アクション: 検査なしで暗号化トラフィックをブロック（15-10 ページ）
- 復号化アクション: さらに検査するためにトラフィックを復号化（15-10 ページ）
- ポリシー内の SSL ルールの管理（15-13 ページ）

# モニタ アクション: アクションの遅延とログの確保

**ライセンス:**すべて

**モニタ** アクションは暗号化トラフィック フローに影響を与えません。つまり、一致するトラフィックがただちに許可または拒否されることはありません。その代わり、追加のルールが存在する場合はそのルールに照らしてトラフィックが照合され、信頼するか、ブロックするか、復号化するかが決定されます。モニタ ルール以外の一致する最初のルールが、トラフィック フローおよび追加のインスペクションを決定します。さらに一致するルールがない場合、ASA FirePOWER モジュールはデフォルトのアクションを使用します。

Monitor ルールの主な目的はネットワーク トラフィックのトラッキングなので、モジュールはモニタ対象トラフィックの接続終了イベントを自動的にログに記録します。つまり、ルールのロギング設定または後で接続を処理するデフォルト アクションとは無関係に、モジュールは接続の終了時に常にログに記録します。言い換えると、パケットが他のルールに一致せず、デフォルト アクションでロギングが有効になっていない場合でも、パケットがモニタ ルールに一致すれば必ず接続がロギングされます。

## 復号化しない（Do Not Decrypt）アクション：暗号化トラフィックを検査なしで転送

**ライセンス：**すべて

復号化しない（**Do Not Decrypt**）アクションは、アクセス コントロール ポリシーのルールおよびデフォルト アクションに従って暗号化トラフィックを評価するため転送します。一部のアクセス コントロール ルールの条件では暗号化されていないトラフィックを必要とするため、こうしたトラフィックに一致するルール数が少なくなる場合があります。侵入やファイル インスペクションなど、暗号化トラフィックのディープ インスペクションは実行できません。

## ブロッキング（Block）アクション：検査なしで暗号化トラフィックをブロック

**ライセンス：**すべて

**Block** および **Block with reset** アクションは、アクセス コントロール ルールのブロックとリセット付きブロック アクション（Block および Block with reset）に類似したものです。これらのアクションは、クライアントとサーバによる SSL 暗号化セッションの確立と暗号化トラフィックの転送を防止します。リセット付きブロック ルールでは接続のリセットも行います。

ブロックされた暗号化トラフィックに対しては、ASA FirePOWER モジュールは設定された応答ページを表示しないことに注意してください。その代わりに、ユーザの要求する禁止された URL の接続は、リセットまたはタイムアウトされます。詳細については、「ブロックされた URL のカスタム Web ページの表示（8-16 ページ）」を参照してください。

ヒント　パッシブまたはインライン（タップ モード）展開では、デバイスがトラフィックを直接検査しないので、ブロックおよびリセット付きブロック（Block および Block with reset）アクションを使用できないことに注意してください。パッシブまたはインライン（タップ モード）インターフェイスを含むセキュリティ ゾーン条件内で、ブロックおよびリセット付きブロック（Block および Block with reset）アクションを使用したルールを作成すると、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。

## 復号化アクション：さらに検査するためにトラフィックを復号化

**ライセンス：**すべて

**Decrypt - Known Key** および **Decrypt - Resign** アクションは、暗号化トラフィックを復号化します。ASA FirePOWER モジュールはアクセス コントロールを使用して復号化されたトラフィックを検査します。アクセス コントロール ルールは、復号化されたトラフィックと暗号化されていないトラフィックで同じ処理をします。ここでは、侵入、禁止ファイル、マルウェアの検出とブロックができます。モジュールは許可されたトラフィックを再暗号化してから宛先に渡します。

**Decrypt - Known** アクションを設定した場合は、1 つまたは複数のサーバ証明書と秘密キー ペアをアクションに関連付けることができます。トラフィックがルールに一致して、トラフィックの暗号化に使用された証明書とアクションに関連付けられた証明書が一致した場合、モジュールは適切な秘密キーを使用してセッションの暗号化と復号化キーを取得します。秘密キーへのアクセスが必要なため、このアクションが最も適しているのは、組織の管理下にあるサーバへの入力トラフィックを復号化する場合です。

同様に **Decrypt - Resign** アクションには、1 つの認証局証明書と秘密キーを関連付けることができます。トラフィックがこのルールに一致した場合、モジュールは CA 証明書を使用してサーバ証明書を再署名してから、中間者として機能します。ここでは、1 つはクライアントとデバイスの間、もう 1 つはデバイスとサーバの間をつなぐ、2 つの SSL セッションが作成されます。各セッションには、さまざまな暗号セッションの詳細が含まれており、モジュールはこれを使用することでトラフィックの復号化と再暗号化が行えます。このアクションは、証明書の秘密キーを各自の管理下にあるキーに置き換えてセッション キーを取得するため、発信トラフィックに適しています。

サーバ証明書の再署名では、証明書の公開キーを CA 証明書の公開キーに置き換えるか、あるいは証明書全体が置き換えられます。通常、サーバ証明書全体を置き換える場合は、SSL 接続が確立された時点で、証明書が信頼できる認証局によって署名されていないことがクライアント ブラウザで警告されます。ただし、その CA をクライアント ブラウザで信頼できることがポリシーに設定されている場合、ブラウザは証明書が信頼できないことの警告をしません。オリジナルのサーバ証明書が自己署名の場合、ASA FirePOWER モジュールは証明書全体を置き換えて再署名する CA を信頼しますが、ユーザのブラウザは証明書が自己署名されていることを警告しません。この場合、サーバ証明書の公開キーを交換するだけで、クライアント ブラウザは証明書が自己署名であることを警告します。

**Decrypt - Resign** アクションを設定した場合、ルールによるトラフィックの照合は、設定したすべてのルール条件に加えて、参照される内部 CA 証明書の署名アルゴリズム タイプに基づいて実施されます。各 **Decrypt - Resign** アクションにはそれぞれ 1 つの CA 証明書が関連付けられるので、暗号化の署名アルゴリズムが異なる複数タイプの発信トラフィックを復号化する SSL ルールは作成できません。また、ルールに追加する暗号スイートと外部証明書のオブジェクトのすべては、関連する CA 証明書の暗号化アルゴリズム タイプに一致する必要があります。

たとえば、楕円曲線暗号（EC）アルゴリズムで暗号化された発信トラフィックが **Decrypt - Resign** ルールに一致するのは、アクションが EC ベースの CA 証明書を参照している場合だけです。証明書と暗号スイートのルール条件を作成するには、ルールに EC ベースの外部証明書と暗号スイートを追加する必要があります。同様に、RSA ベースの CA 証明書を参照する **Decrypt - Resign** ルールは、RSA アルゴリズムで暗号化された発信トラフィックのみを照合します。EC アルゴリズムで暗号化された発信トラフィックは、設定した他のすべてのルール条件が一致したとしても、このルールには一致しません。

次の点に注意してください。

- SSL 接続確立用の暗号スイートで一時 Diffie-Hellman（DHE）または楕円曲線 Diffie-Hellman（ECDHE）キー交換アルゴリズムが使用されている場合、パッシブ展開では **Decrypt - Known Key** アクションを使用できません。SSL ポリシーの対象がパッシブまたはインライン（タップ モード）インターフェイスであり、そのポリシーに含まれる **Decrypt - Known Key** ルールで DHE または ECDHE を含む暗号スイート条件が使われている場合、ASA FirePOWER モジュールによりルールの横に情報アイコン（ ）が表示されます。パッシブまたはインライン（タップ モード）インターフェイスを含む SSL ルールに後からゾーンを追加すると、モジュールにより警告アイコン（ ）が表示されます。
- デバイスがトラフィックを直接検査しないため、パッシブまたはインライン（タップ モード）展開では **Decrypt - Resign** アクションを使用できません。セキュリティ ゾーン内にパッシブまたはインライン（タップ モード）インターフェイスを含む **Decrypt - Resign** アクションを使用したルールを作成した場合、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。SSL ポリシーの対象がパッシブまたはインライン（タップ モード）インターフェイ

スであり、そのポリシーに **Decrypt - Resign** ルールが含まれる場合、モジュールによりルールの横に情報アイコン( )が表示されます。パッシブまたはインライン(タップ モード)インターフェイスを含む SSL ルールに後からゾーンを追加すると、モジュールにより警告アイコン( )が表示されます。パッシブまたはインライン(タップ モード)インターフェイスを含むデバイスに、Decrypt - Resign ルールを含む SSL ポリシーを適用した場合、このルールに一致する SSL セッションはすべて失敗します。

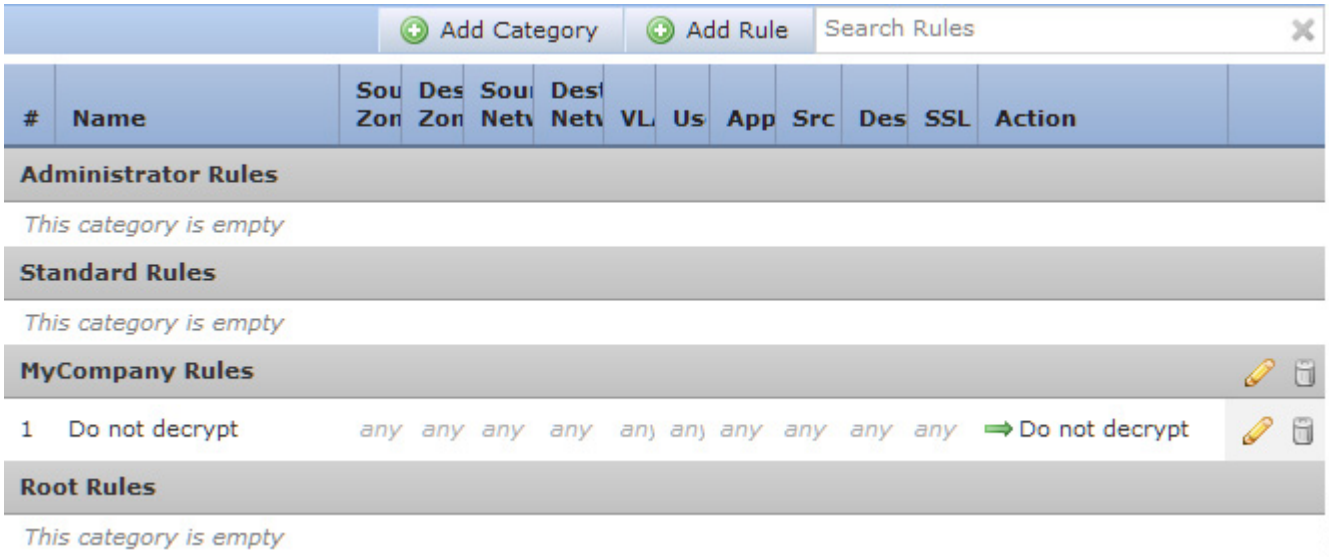
- サーバ証明書の再署名に使用する CA をクライアントが信頼していない場合、証明書が信頼できないことの警告がユーザに出されます。これを防ぐには、クライアントの信頼できる CA ストアに CA 証明書をインポートします。または組織にプライベート PKI がある場合は、組織の全クライアントで自動的に信頼されるルート CA が署名する中間 CA 証明書を発行して、その CA 証明書をデバイスにアップロードすることもできます。
- SSL ルールの**暗号スイート**条件に匿名の暗号スイートを追加できますが、次の点に注意してください。
  - システムは ClientHello 処理中に自動的に匿名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(15-18 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化できないため、ルールに **Decrypt - Resign** または **Decrypt - Known Key** アクションを使用できません。
- クライアントとデバイスの間に HTTP プロキシがあり、クライアントとサーバが CONNECT HTTP メソッドを使用してトンネル SSL 接続を確立する場合、ASA FirePOWER モジュールはトラフィックを復号化できません。モジュールによるこのトラフィックの処理法は、**ハンドシェイク エラー**の復号化できないアクションが決定します。詳細については、「復号化できないトラフィックのデフォルト処理の設定(14-5 ページ)」を参照してください。
- SSL ルールに **Decrypt - Known Key** アクションを付けて作成した場合、**Distinguished Name** または **Certificate** 条件による照合はできません。ここでの前提は、このルールがトラフィックと一致する場合、証明書、サブジェクト DN、および発行元 DN は、ルールに関連付けられた証明書とすでに一致済みであることです。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(15-9 ページ)を参照してください。
- 内部 CA オブジェクトを作成して証明書署名要求(CSR)の生成を選択した場合、オブジェクトに署名付き証明書をアップロードするまで、この CA は **Decrypt - Resign** アクションに使用できません。詳細については、新しい署名付き証明書の取得およびアップロード(2-41 ページ)を参照してください。
- **Decrypt - Resign** アクションのルールを設定して、1 つまたは複数の外部証明書オブジェクトまたは暗号スイートで署名アルゴリズム タイプの不一致が生じた場合、ポリシー エディタでルールの横に情報アイコン( )が表示されます。すべての外部証明書オブジェクトまたはすべての暗号スイートで署名アルゴリズム タイプの不一致が生じた場合、ポリシーのルールの横には警告アイコン( )が表示され、SSL ポリシーに関連付けたアクセス コントロール ポリシーは適用できなくなります。詳細については、証明書による暗号化トラフィックの制御(16-21 ページ)および暗号スイートによる暗号化トラフィックの制御(16-27 ページ)を参照してください。
- **Interactive Block** または **Interactive Block with reset** アクションのアクセス コントロール ルールと復号化トラフィックが一致する場合、ASA FirePOWER モジュールは一致する接続をインタラクションなしでブロックし、応答ページを表示**しません**。
- インライン正規化プリプロセッサで **Normalize Excess Payload** オプションをイネーブルにすると、プリプロセッサによる復号化トラフィックの標準化時に、パケットがドロップされてトリミングされたパケットに置き換えられる場合があります。これは SSL セッションを終了させません。トラフィックが許可された場合、SSL セッションの一部としてトリミングされたパケットは暗号化されます。このオプションの詳細については、「インライン トラフィックの正規化(23-6 ページ)」を参照してください。

- ブラウザが証明書ピニングを使用してサーバ証明書を確認する場合は、サーバ証明書に再署名しても、このトラフィックを復号化できません。このトラフィックを許可するには、サーバ証明書の共通名または識別名と突き合わせるように、Do not decrypt アクションを使用して SSL ルールを設定します。

# ポリシー内の SSL ルールの管理

**ライセンス:**すべて

SSL ポリシー エディタの [Rules] タブでは、以下の図に示すように、ポリシー内の SSL ルールの追加、編集、検索、移動、有効化、無効化、削除、その他の管理が行えます。




各ルールについて、ポリシー エディタでは、その名前、条件のサマリー、およびルール アクションが表示されます。警告、エラー、その他の重要な情報がアイコンで示されます。無効なルールはグレーで表示され、ルール名の下に [(disabled)] というマークが付きます。アイコンの詳細については、「SSL ルールのトラブルシューティング（15-16 ページ）」を参照してください。

SSL ルールの管理の詳細については、次を参照してください。

- SSL ルールの検索（15-13 ページ）
- SSL ルールのイネーブル化とディセーブル化（15-14 ページ）
- SSL ルールの位置またはカテゴリの変更（15-15 ページ）

# SSL ルールの検索

**ライセンス:**すべて

スペースおよび印刷可能な特殊文字を含む英数字文字列を使用して、SSL ルールのリストで一致する値を検索できます。この検索では、ルール名およびルールに追加したルール条件が検査されます。ルール条件の場合は、条件タイプ（ゾーン、ネットワーク、アプリケーションなど）ごとに追加できる任意の名前または値が検索照合されます。これには、個々のオブジェクト名または値、グループ オブジェクト名、グループ内の個々のオブジェクト名または値、およびリテラル値が含まれます。

検索文字列のすべてまたは一部を使用できます。照合ルールごとに、一致する値のカラムが強調表示されます。たとえば、100Bao という文字列のすべてまたは一部を基準に検索すると、少なくとも、100Bao アプリケーションを追加した各ルールの [Applications] カラムが強調表示されます。100Bao という名前のルールもある場合は、[Name] カラムと [Applications] カラムの両方が強調表示されます。

1 つ前または次の照合ルールに移動することができます。ステータス メッセージには、現行の一致および合計一致数が表示されます。

複数ページのルール リストでは、どのページでも一致が検出される可能性があります。最初の一致が検出されたのが最初のページではない場合は、最初の一致が検出されたページが表示されます。最後の一致が現行の一致となっている場合、次の一致を選択すると、最初の一致が表示されます。また、最初の一致が現行の一致となっている場合、前の一致を選択すると、最後の一致が表示されます。

**ルールの検索方法:**

**ステップ 1**　検索するポリシーの SSL ポリシー エディタで、[Search Rules]プロンプトをクリックし、検索文字列を入力してから Enter を押します。検索を開始するには、Tab キーを使用するか、ページの空白部分をクリックします。

一致する値を含むルールのカラムが強調表示されます。表示されている（最初の）一致は、他とは区別できるように強調表示されます。

**ステップ 2**　目的のルールを探すには次の操作が利用できます。

- 照合ルールの間を移動する場合は、次の一致アイコン（ ▼ ）または前の一致アイコン（ ▲ ）をクリックします。
- ページを更新し、検索文字列および強調表示をクリアする場合は、クリア アイコン（ ✖ ）をクリックします。

# SSL ルールのイネーブル化とディセーブル化

**ライセンス:** すべて

作成した SSL ルールは、デフォルトでイネーブルになっています。ルールを無効にすると、ASA FirePOWER モジュールはネットワーク トラフィックの評価にそのルールを使用せず、そのルールに対する警告とエラーの生成を停止します。SSL ポリシーのルール リストを表示すると、無効なルールはグレー表示されますが、変更は可能です。またはルール エディタを使用して SSL ルールをイネーブルまたはディセーブルにできることに注意してください。「SSL ルールの概要と作成（15-4 ページ）」を参照してください。

**SSL ルールの状態を変更するには、次の手順に従います。**

**ステップ 1**　イネーブルまたはディセーブルにするルールを含むポリシーの SSL ポリシー エディタで、ルールを右クリックして、ルールの状態を選択します。

- 非アクティブなルールをイネーブルにするには、[State] > [Enable]を選択します。
- アクティブなルールをディセーブルにするには、[State] > [Disable]を選択します。

**ステップ 2**　[Store ASA FirePOWER Changes]をクリックします。

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（4-12 ページ）を参照してください）。

# SSL ルールの位置またはカテゴリの変更

**ライセンス:**すべて

SSL ルールを編成しやすいように、SSL ポリシーには、管理者ルール、標準ルール、ルート ルールという、ASA FirePOWER モジュールが提供する 3 つのルール カテゴリが用意されています。これらのカテゴリの移動、削除、名前変更はできませんが、カスタム カテゴリの作成は可能です。

詳細については、以下を参照してください。

- SSL ルールの移動（15-15 ページ）
- 新しい SSL ルール カテゴリの追加（15-15 ページ）

## SSL ルールの移動

**ライセンス:**すべて

適切な SSL ルールの順序は、ネットワーク トラフィックの処理に必要なリソースを軽減し、ルールのプリエンプションを回避します。

次の手順は、SSL ポリシー エディタを使用して 1 つまたは複数のルールを同時に移動する方法を説明しています。またはルール エディタを使用して個々の SSL ルールを移動することもできます。「SSL ルールの概要と作成（15-4 ページ）」を参照してください。

**規則を移動するには、次の手順を実行します。**

**ステップ 1**　移動するルールを含むポリシーの SSL ポリシー エディタで、ルールごとに空白部分をクリックして、ルールを選択します。複数のルールを選択するには、Ctrl キーと Shift キーを使用します。

選択したルールは強調表示されます。

**ステップ 2**　ルールを移動します。カット アンド ペーストおよびドラッグ アンド ドロップを使用することもできます。

新しい場所にルールをカット アンド ペーストするには、選択したルールを右クリックし、[Cut] を選択します。次に、貼り付けたい位置に隣接するルールの空白部分を右クリックし、[Paste above] または [Paste below] を選択します。2 つの異なる SSL ポリシーの間では、SSL ルールのコピー アンド ペーストはできないことに注意してください。

**ステップ 3**　[Store ASA FirePOWER Changes] をクリックします。

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（4-12 ページ）を参照してください）。

## 新しい SSL ルール カテゴリの追加

**ライセンス:**すべて

SSL ルールを編成しやすいように、SSL ポリシーには、管理者ルール、標準ルール、ルート ルールという、ASA FirePOWER モジュールが提供する 3 つのルール カテゴリが用意されています。これらのカテゴリの移動、削除、名前変更はできませんが、Standard Rules と Root Rules 間でのカスタム カテゴリの作成は可能です。

カスタム カテゴリを追加すると、追加のポリシーを作成しなくても、ルールをさらに細かく編成できます。追加したカテゴリは、名前変更と削除ができます。これらのカテゴリの移動はできませんが、ルールのカテゴリ間およびカテゴリ内外への移動は可能です。

新しいカテゴリを追加するには、次の手順に従います。

**ステップ 1**　ルール カテゴリを追加するポリシーの SSL ポリシー エディタで、[Add Category]をクリックします。

**ヒント**　ポリシーにルールがすでに含まれている場合は、追加する前に既存のルールの行の空白部分をクリックすることで、新しいカテゴリの位置を設定できます。既存のルールを右クリックし、[Insert new category]を選択することもできます。

[Add Category] ポップアップ ウィンドウが表示されます。

**ステップ 2**　[Name]に、一意のカテゴリ名を入力します。

最大 30 文字の英数字の名前を入力できます。名前には、スペース、および印刷可能な特殊文字を含めることができます。

**ステップ 3**　次の選択肢があります。

- 既存のカテゴリのすぐ上に新しいカテゴリを配置する場合は、最初の [Insert] ドロップダウン リストから [above Category] を選択した後、2 番目のドロップダウン リストからカテゴリを選択します。ここで選択したカテゴリの上にルールが配置されます。
- 既存のルールの下に新しいカテゴリを配置する場合は、ドロップダウン リストから [below rule]を選択した後、既存のルール番号を入力します。このオプションが有効なのは、ポリシーに少なくとも 1 つのルールが存在する場合のみです。
- 既存のルールの上にルールを配置する場合は、ドロップダウン リストから [above rule]を選択した後、既存のルール番号を入力します。このオプションが有効なのは、ポリシーに少なくとも 1 つのルールが存在する場合のみです。

**ステップ 4**　[OK]をクリックします。

カテゴリが追加されます。名前を編集するには、カスタム カテゴリの横にある編集アイコン（ ）をクリックします。カテゴリを削除するには、削除アイコン（ ）をクリックします。削除するカテゴリに含まれるルールは、その上にあるカテゴリに追加されます。

**ステップ 5**　[Store ASA FirePOWER Changes]をクリックしてポリシーを保存します。

# SSL ルールのトラブルシューティング

**ライセンス:** すべて

SSL ルールを適切に作成して順序付けることは複雑な作業ですが、これは効果的な展開を構築する上で不可欠な要素です。慎重なポリシーの設計を怠ると、他のルールをプリエンプション処理したり、追加ライセンスが必要となったり、無効な設定を含んだルールになる可能性があります。ASA FirePOWER モジュールにより、トラフィックが予期したとおりに確実に処理されるようにするために、SSL ポリシー インターフェイスには、ルールに関する強力な警告およびエラーのフィードバック システムが用意されています。

各ルールについては、次の表に示すように、ポリシー エディタのアイコンによる警告とエラーの表示がされます。アイコンにポインタを合わせると、警告、エラー、情報の内容を示すテキストを確認できます。

*表 15-2　SSL のエラー アイコン*

| アイコン | 説明 | 詳細 |
|---|---|---|
|  | 警告 | 問題によっては、ルールやその他の警告を示している SSL ポリシーであっても、適用が可能な場合があります。この場合、間違いのある設定は機能しません。たとえば、プリエンプションされたルールはトラフィックを評価しません。ただし、警告アイコンがライセンス エラーまたはモデルの不一致を示している場合は、問題が解消されるまでそのポリシーは適用できません。<br>警告が出されているルールを無効にすると、警告アイコンが消えます。潜在する問題を修正せずにルールを有効にすると、警告アイコンが再表示されます。 |
|  | エラー | ルールまたはその他の SSL ポリシー設定にエラーがある場合、問題が解消されるまでそのポリシーは適用できません。 |
|  | 情報 | 情報アイコンは、トラフィックのフローに影響する可能性がある設定に関する有用な情報を伝送します。これらの問題は重大ではなく、ポリシーの適用を妨げません。 |

SSL ルールを適切に設定することは、ネットワーク トラフィックの処理に必要なリソースの軽減にも寄与します。複雑なルールを作成したりルールの順番が不適切であると、パフォーマンスに影響する場合があります。

詳細については、以下を参照してください。

- ルールのプリエンプションと無効な設定の警告について（15-17 ページ）
- 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（15-18 ページ）

## ルールのプリエンプションと無効な設定の警告について

**ライセンス：**すべて

SSL ルールを適切に設定して順序付けることは、効果的な展開を構築する上で不可欠な要素です。SSL ポリシーの内部では、SSL ルール間で他のルールのプリエンプションが発生したり、無効な設定を含んだ状態になる場合があります。これらの問題を示すために、モジュールでは警告およびエラーのアイコンを使用します。

### ルールのプリエンプションの警告について

SSL ルールの条件が後続のルールによるトラフィックの照合をプリエンプション処理する場合があります。次に例を示します。

```
Rule 1: do not decrypt Administrators
Rule 2: block Administrators
```

上記の 2 番目のルールによってトラフィックがブロックされることはありません。なぜなら、最初のルールによってトラフィックは既に許可されるためです。

### 無効な設定の警告の概要

SSL ポリシーが依存する外部の設定は変更される可能性があるため、有効であった SSL ポリシー設定が無効になる場合があります。次の例について考えてみます。

- URL カテゴリ条件を含むルールは、URL フィルタリングライセンスを持たないモジュールをターゲットにすることで無効になる場合があります。その時点で、ルールの横にエラー アイコンが表示され、ポリシーをそのデバイスに適用できなくなります。適用可能にするには、このルールを編集または削除するか、ポリシーのターゲットを変更するか、または適切なライセンスを有効にする必要があります。
- Decrypt - Resign ルールを作成し、後でパッシブ インターフェイスでセキュリティ ゾーンをゾーン条件に追加した場合、ルールの横に警告アイコンが表示されます。パッシブ展開では証明書の再署名によるトラフィックの復号化はできないので、パッシブ インターフェイスをルールから削除するか、またはルール アクションを変更するまで、このルールは機能しません。
- ルールにユーザを追加した後、LDAP ユーザ認識設定を変更してそのユーザを除外すると、ユーザはアクセス コントロールの対象ユーザではなくなるため、そのルールは効果がなくなります。

## 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

**ライセンス:**すべて

SSL ポリシーのルールには 1 から始まる番号が付いています。ASA FirePOWER モジュールは、ルールの順番の昇順で、ルールを上から順にトラフィックと照合します。Monitor ルールを除き、トラフィックが最初に一致するルールが、当該トラフィックを処理するためのルールになります。

適切な SSL ルールの順序は、ネットワーク トラフィックの処理に必要なリソースを軽減し、ルールのプリエンプションを回避します。作成するルールは組織や展開に固有なものですが、必要な要件を満たしながらパフォーマンスを最適化するようルールを順番付けるには、従うべきいくつかの一般的なガイドラインがあります。

### 重要性が最も高いルールから最も低いルールへの順序付け

最初に、組織のニーズに適するルールを順序付けする必要があります。すべてのトラフィックに適用する必要があるプライオリティ ルールをポリシーの先頭部分付近に配置します。たとえば、ある 1 人のユーザからの発信トラフィックは詳細な分析用に復号化するが（Decrypt - Resign ルールを使用）、その部門の他のすべてのユーザからのトラフィックは復号化しない（Do not decrypt ルールを使用）場合は、この順序で 2 つの SSL ルールを配置します。

### 特定のルールから一般的なルールへの順序付け

特定のルール、つまり、処理するトラフィックを狭く定義するルールを先に配置することで、パフォーマンスを向上できます。適用範囲が広いルールは多くの異なる種類のトラフィックに一致し、後続の具体的なルールをプリエンプション処理する可能性があることからも、これは重要です。

ここで 1 つのシナリオとして、信頼できる CA（Good CA）が悪意のあるエンティティ（Bad CA）に間違って CA 証明書を発行してしまい、その証明書を取り消していない状況を考えてみましょう。信頼できない CA によって発行された証明書で暗号化されたトラフィックはブロックしたいが、信頼できる CA の信頼チェーン内にあるそれ以外のトラフィックは許可したいとします。ここで必要となるのは、CA 証明書およびすべての中間 CA 証明書をアップロードし、その後に次のようにルールを順序付けることです。

```
ルール 1:発行元 CN=www.badca.com をブロック
ルール 2:発行元 CN=www.goodca.com を復号化しない
```

次のようにルールを逆にしたらどうなるでしょうか。

```
ルール 1:発行元 CN=www.goodca.com を復号化しない
ルール 2:発行元 CN=www.badca.com をブロック
```

最初のルールは Good CA によって信頼されたすべてのトラフィックに一致し、その中には Bad CA によって信頼されたトラフィックも含まれます。どのトラフィックも 2 番目のルールに一致しないため、悪意のあるトラフィックはブロックされずに許可される可能性があります。

### 証明書でピニングしたサイトからのトラフィックを許可するルールの配置

証明書のピニングを行うと、SSL セッションが確立される前に、サーバの公開キー証明書が、サーバに既に関連付けられているブラウザの証明書と一致しているかどうかを、クライアントのブラウザが強制的に確認します。Decrypt - Resign アクションにはサーバ証明書を変更してからクライアントに渡すという動作が含まれているため、ブラウザが既にその証明書をピニングしている場合は、変更された証明書が拒否されます。

たとえば、クライアント ブラウザが、証明書のピニングを使用するサイト `windowsupdate.microsoft.com` に接続されており、そのトラフィックと一致する SSL ルールを Decrypt - Resign アクションを使用して設定すると、ASA FirePOWER モジュールはサーバ証明書に再署名してから、クライアント ブラウザ渡します。この変更されたサーバ証明書は、ブラウザでピニングした `windowsupdate.microsoft.com` の証明書と一致しないため、クライアント ブラウザは接続を拒否します。

このトラフィックを許可するには、サーバ証明書の共通名または識別名と突き合わせるように、Do not decrypt アクションを使用して SSL ルールを設定します。SSL ポリシーでは、このルールを、トラフィックと一致するすべての Decrypt - Resign ルールの前に配置してください。Web サイトに正常に接続された後で、クライアント ブラウザから、ピニングされた証明書を取得できます。接続が成功した場合も、失敗した場合も、ログに記録された接続イベントから証明書を表示できます。

### トラフィックを復号化するルールは後方に配置する

トラフィックの復号化はリソースを必要とする処理なので、トラフィックの復号化を実行しないルール（Do not decrypt、Block）を、実行するルール（Decrypt - Known Key、Decrypt - Resign）より前に配置することで、パフォーマンスが向上する可能性があります。この理由は、トラフィック復号化のコマンドには多量のリソースを消費するものがあるからです。また、Block ルールにより、ASA FirePOWER モジュールが復号化やインスペクションの対象とするはずのトラフィックが迂回する可能性があります。他の要素がすべて同等、つまり、より重要なものがなくプリエンプションが問題ではない場合にルールのセットを与えると仮定すると、次の順序でルールを配置することを検討します。

- 一致した接続のログ記録はするがその他のアクションをトラフィックに実行しない Monitor ルール
- それ以上のインスペクションなしでトラフィックをブロックする Block ルール
- 暗号化トラフィックを復号化しない Do not decrypt ルール
- 既知の秘密キーを使用して着信トラフィックを復号する Decrypt - Known Key ルール
- サーバ証明書に再署名することによって発信トラフィックを復号化する Decrypt - Resign ルール

### ClientHello の変更の優先順位付け

ClientHello の変更を優先順位付けするには、ServerHello またはサーバ証明書条件に一致するルールの前に、ClientHello メッセージで使用可能な条件に一致するルールを配置します。

管理対象デバイスが SSL ハンドシェイクを処理するときに、ClientHello メッセージを変更して、復号化の可能性を高めることができます。たとえば、FirePOWER システムは圧縮されたセッションを復号化できないので、圧縮メソッドを削除できます。

システムは Decrypt - Resign アクションを含む SSL ルールに最終的に一致させることができる場合、ClientHello メッセージを変更するのみです。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、サーバ証明書データを 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。同じクライアントからの後続の接続で、システムはサーバ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。

ServerHello またはサーバ証明書条件（証明書、識別名、証明書のステータス、暗号スイート、バージョン）と一致するルールを、ClientHello 条件（ゾーン、ネットワーク、VLAN タグ、ポート、ユーザ、アプリケーション、URL カテゴリ）と一致するルールの前に配置する場合、ClientHello の変更をプリエンプション処理し、復号化されていないセッションの数を増やすことができます。

# パフォーマンスを改善する SSL インスペクション設定

**ライセンス:** すべて

複雑な SSL ポリシーおよびルールのコマンドには、多量のリソースを消費するものがあります。SSL ポリシーが適用されると、ASA FirePOWER モジュールはすべてのルールをまとめて評価し、ネットワーク トラフィックの評価にデバイスが使用する条件の拡張セットを作成します。デバイスでサポートされる SSL ルールの最大数を超えていることを警告するポップアップ ウィンドウが表示される場合があります。この最大値は、デバイスの物理メモリやプロセッサ数などの、さまざまな要因によって異なります。

### ルールの単純化

次のガイドラインは、SSL ルールの単純化とパフォーマンスの向上に役立ちます。

- ルールを構築するときは、条件内で使用する個々の要素は可能な限り少なくします。たとえば、ネットワーク条件では、個々の IP アドレスではなく IP アドレス ブロックを使用します。ポート条件では、ポート範囲を使用します。アプリケーション制御および URL フィルタリングを実行する場合はアプリケーション フィルタと URL カテゴリおよびレピュテーションを使用し、ユーザ制御を実行する場合は LDAPユーザ グループを使用します。

  SSL ルール条件で使用するオブジェクトに要素を結合してもパフォーマンスは向上しないことに注意してください。たとえば、50 の個別の IP アドレスを含むネットワーク オブジェクトを使用しても、その条件内のそれらの IP アドレスに対するものを含む、組織的な（パフォーマンスではない）利点が個別に与えられるだけです。

- できる限り、セキュリティ ゾーンごとにルールを制限します。デバイスのインターフェイスがゾーン制限されたルールのゾーンの 1 つにない場合、ルールはそのデバイスのパフォーマンスに影響を与えません。
- ルールを過度に設定しないでください。1 つの条件が処理するトラフィックに一致するのに十分な場合は、2 つ使用しないでください。

### トラフィック復号化の設定

トラフィック復号化を設定する際は、次の注意事項に従ってください。

- トラフィックの復号化は、トラフィックを復号化してアクセス コントロールによるチェックを実行するため、リソースを必要とする処理です。処理対象を絞り込んだ復号化ルールを作成すると、ASA FirePOWER モジュールが復号化するトラフィック量が、処理対象が広範な復号化ルールより減るので、結果として、トラフィックの復号化に必要な処理のリソースも削減されます。トラフィックをいったん復号化した後にアクセス コントロール ルールを使用して許可またはブロックするのではなく、暗号化トラフィックはできるだけブロックするか復号化しないことを選択するようにします。
- ルート発行元 CA に基づいてトラフィックを信頼するように証明書ステータスの条件を設定する場合は、ルート CA 証明書およびルート CA 信頼チェーン内のすべての中間 CA 証明書を SSL ポリシーにアップロードするようにします。信頼できる CA の信頼チェーン内のすべてのトラフィックは復号化なしで許可されるようになり、不要な復号化は実施されません。