# 復号ルール

ここでは、復号ルールの作成、設定、管理、トラブルシューティングの概要を示します。

（注） TLS と SSL は相互に使用されることが多いため、*TLS/SSL* という表現を使用していずれかのプロトコルについて説明していることを示しています。SSL プロトコルは、よりセキュアな TLS プロトコルを選択することにより IETF によって廃止されました。そのため、*TLS/SSL* は通常、TLS のみを指すものとして解釈できます。

SSL プロトコルと TLS プロトコルの詳細については、「SSL vs. TLS - What's the Difference?」[英語] などのリソースを参照してください。



# 復号ルールの概要

復号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、複数の管理対象デバイスをカバーしたきめ細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。

# 復号ルール の要件と前提条件

### サポートされるドメイン

任意

### ユーザの役割

- 管理者
- アクセス管理者
- ネットワーク管理者

# 復号ルール の注意事項と制限事項

復号ルール を設定するときは、次の点に注意してください。復号ルール を適切に設定するのは複雑なタスクですが、暗号化トラフィックを処理する効果的な導入環境の構築には不可欠なタスクです。ルールをどのように設定するかには、制御できない特定のアプリケーションの動作を含む、多くの要素が影響します。

さらに、ルールが互いをプリエンプトしたり、追加ライセンスが必要になったりすることがあります。また、ルールに無効な設定が含まれる可能性もあります。慎重に設定されたSSLルールは、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。過度に複雑なルールを作成し、ルールを誤って順序付けすると、パフォーマンスに悪影響を与える可能性があります。

詳細については、アクセス制御ルールのベストプラクティスを参照してください。

TLS暗号化アクセラレーションに特に関連するガイドラインについては、TLS暗号化アクセラレーションを参照してください。

### 関連トピック

ルールとその他のポリシーの警告
アクセス制御ルールのベストプラクティス
TLS/SSL 復号の使用上のガイドライン （3 ページ）
復号ルール サポートされていない機能 （4 ページ）
TLS/SSL 復号禁止のガイドライン （4 ページ）
TLS/SSL 復号：再署名のガイドライン （6 ページ）
TLS/SSL 復号：既知のキーのガイドライン （9 ページ）
TLS/SSL ブロックのガイドライン （10 ページ）
TLS/SSL 証明書のピン留めのガイドライン （10 ページ）
TLS/SSL ハートビートのガイドライン （10 ページ）
TLS/SSL 匿名の暗号スイートの制限事項 （11 ページ）

# TLS/SSL 復号の使用上のガイドライン

### 一般的なガイドライン

復号ルールには、パフォーマンスに影響を及ぼす可能性があるオーバーヘッドの処理が必要です。ポリシーまたはルールを設定する前に、復号してディープインスペクションの対象とする必要があるトラフィックを決定します。

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使用するデバイスでトラフィックを復号することはできません。

### 復号できないトラフィックのガイドライン

Web サイト自体が復号できない、または Web サイトで TLS/SSL ピン留めが使用されている場合、特定のトラフィックを復号できないと判断できます。SSL ピン留めでは、ブラウザにエラーが表示されることなく、復号されたサイトへのユーザーアクセスが効果的に阻止されます。

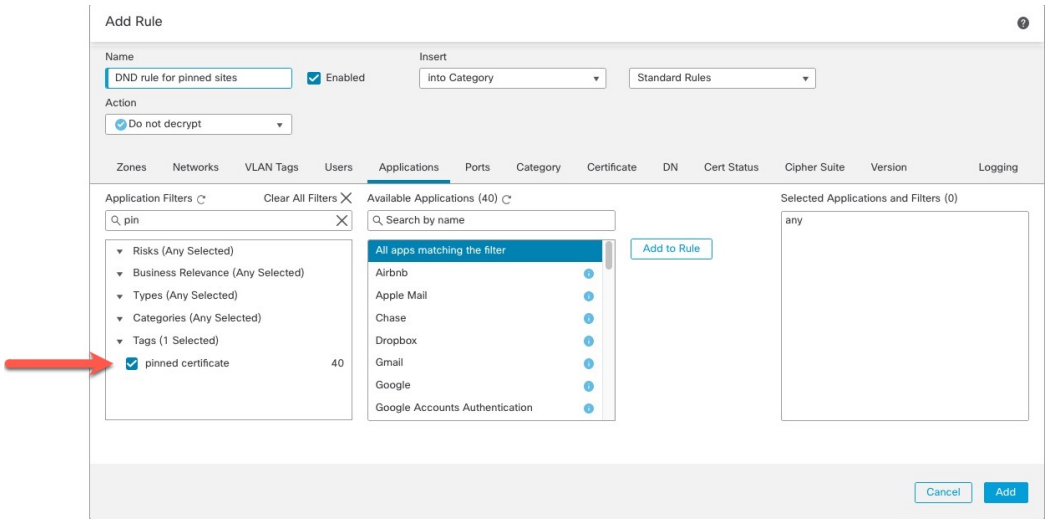
証明書のピン留めの詳細については、TLS/SSL のピニングについて （47 ページ）を参照してください。

そのようなサイトのリストは次のように管理されています。

- **Cisco-Undecryptable-Sites** という名前の識別名（DN）グループ
- **ピン留めされた証明書**または**復号不可**のアプリケーションフィルタ

トラフィックを復号しており、ユーザーが復号されたサイトにアクセスしたときにブラウザにエラーが表示されないようにする場合は、復号ルールの下部に [復号しない（Do Not Decrypt）] ルールを設定することを推奨します。

**ピン留めされた証明書**のアプリケーションフィルタの設定例を次に示します。




# 復号ルール サポートされていない機能

**RC4 暗号はサポートされていない**

Rivest Cipher 4（*RC4* または *ARC4* ともいう）暗号は脆弱性があることで知られており、安全でないと見なされています。

復号ポリシー は RC4 暗号スイートをサポート対象外としています。組織の要件と一致するように復号ポリシー ポリシーの **[復号不可のアクション（Undecryptable Actions）]** ページで、**[サポート対象外の暗号スイート（Unsupported Cipher Suite）]** アクションを設定する必要があります。詳細については、復号できないトラフィックのデフォルト処理オプションを参照してください。

**パッシブ、インラインタップモード、およびSPANインターフェイスはサポートされていません。**

TLS/SSL トラフィックは、パッシブ、インラインタップモード、または SPAN インターフェイスでは復号できません。

# TLS/SSL 復号禁止のガイドライン

次によって禁止されている場合は、トラフィックを復号してはいけません。

- 法律：たとえば、一部の法域では、財務情報の復号が禁止されています
- 会社のポリシー：たとえば、会社によって特権的な通信の復号が禁止されている場合があります
- プライバシー規制
- 証明書のピン留め（*TLS/SSL* ピニングとも呼ばれる）を使用するトラフィックは、接続の切断を防ぐため、暗号化されたままにする必要があります

暗号化されたトラフィックは、次のものを含むがこれらに限定されない任意の 復号ルール 条件で許可またはブロックできます。

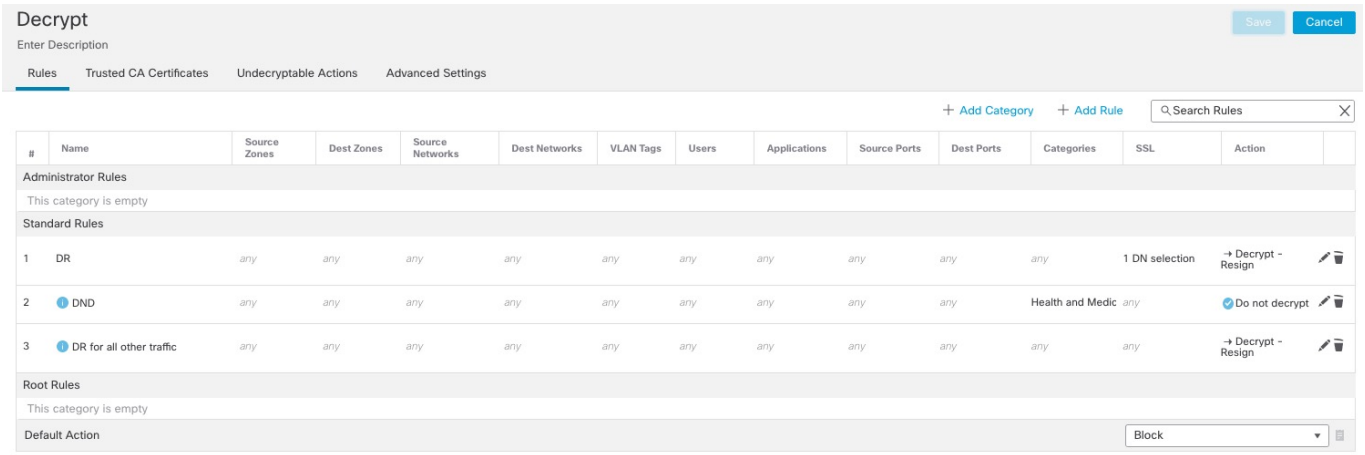
- 証明書のステータス（期限切れまたは無効な証明書など）
- プロトコル（セキュアでない SSL プロトコルなど）
- ネットワーク（セキュリティ ゾーン、IP アドレス、VLAN タグなど）
- 正確な URL または URL カテゴリ
- ポート
- ユーザー グループ

### [復号しない（Do Not Decrypt）] ルールのカテゴリの制限

必要に応じて、復号ポリシーにカテゴリを含めることができます。これらのカテゴリ（「URL フィルタリング」とも呼ばれる）は、Cisco Talos インテリジェンスグループによって更新されます。更新は、Web サイトの宛先から（場合によってはそのホスティングおよび登録情報から）取得可能な内容に従って、機械学習および人間の分析に基づいて行われます。分類は、宣言された会社の業種、意図、またはセキュリティに基づいて行われません。シスコでは、URL フィルタリングカテゴリの継続的な更新と改善に努めていますが、厳密に科学的なものではありません。一部の Web サイトはまったく分類されておらず、一部の Web サイトは不適切に分類されている可能性があります。

理由のないトラフィックの復号を避けるために、[復号しない（Do Not Decrypt）] ルールのカテゴリを過度に使用しないでください。たとえば、[健康と薬（Health and Medicine）] カテゴリには、患者のプライバシーを脅かさない WebMD の Web サイトが含まれています。

以下は、[健康と薬（Health and Medicine）] カテゴリの Web サイトの復号を防ぐ一方で、WebMD およびその他すべての復号を許可することができるサンプル復号ポリシーです。復号ルールに関する一般的な情報については、TLS/SSL 復号の使用上のガイドライン （3 ページ）を参照してください。



（注） URL フィルタリングとアプリケーション検出を混同しないでください。アプリケーション検出は、Web サイトからのパケットの一部を読み取り、それが何であるか（Facebook メッセージや Salesforce など）をより具体的に判断することに依存します。詳細については、アプリケーション制御の設定のベストプラクティスを参照してください。

# TLS/SSL 復号：再署名のガイドライン

[Decrypt - Resign] アクションには、1 つの内部認証局（CA）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、システムは CA 証明書を使用してサーバー証明書を再署名してから、中間者（man-in-the-middle）として機能します。ここでは 2 つの TLS/SSL セッションが作成され、1 つはクライアントと管理対象デバイスの間、もう 1 つは管理対象デバイスとサーバの間で使用されます。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、システムはこれを使用することでトラフィックの復号と再暗号化が行えます。

## ベスト プラクティス

次の点を推奨します。

- [Decrypt - Known Key] ルールアクションを推奨する着信トラフィックとは対照的に、発信トラフィックの復号に対しては [Decrypt - Resign] ルールアクションを使用します。

  [復号 - 既知のキー（Decrypt - Known Key）] の詳細については、TLS/SSL 復号：既知のキーのガイドライン （9 ページ）を参照してください。

- [復号-再署名（Decrypt - Resign）] ルールアクションを設定する場合は、必ず [キーのみを置換（Replace Key Only）] チェックボックスをオンにします。

  ユーザーが自己署名証明書を使用する web サイトを参照すると、web ブラウザにセキュリティ警告が表示され、セキュリティで保護されていないサイトと通信していることに気付きます。

  ユーザーが信頼できる証明書を使用する web サイトを参照すると、セキュリティ警告は表示されません。

## 詳細

[復号 - 再署名（Decrypt - Resign）] アクションをルールに設定すると、ルールによるトラフィックの照合は、設定されている他のルール条件に加えて、参照する内部 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 [復号 - 再署名（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、異なる署名アルゴリズムで暗号化された複数のタイプの発信トラフィックを復号する 復号ルール 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 [復号 - 再署名（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場合は、EC ベースの外部証明書と暗号スイートをルールに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 [復号 - 再署名（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とのみ一致します。EC アルゴリズムで暗号化された発信トラフィックは、設定されている他のルール条件がすべて一致したとしても、このルールには一致しません。

### 注意事項と制約事項

また次の点に注意してください。

#### 匿名の暗号スイートはサポート対象外

匿名の暗号スイートはその性質から、認証には使用されず、キー交換を使用しません。匿名の暗号スイートには限定的な用途があります。詳細については、RFC 5246 の付録 F.1.1.1 を参照してください。（TLS 1.3 では、代わりに RFC 8446 付録 C.5 を参照してください。）

匿名の暗号スイートは認証に使用されないため、ルールに [復号-再署名（Decrypt - Resign）] または [復号-既知のキー（Decrypt - Known Key）] アクションは使用できません。

#### バージョンまたは暗号スイートのルール条件を使用しない

重要 **[復号 - 再署名（Decrypt - Resign）]**、**[復号 - 証明書の置き換え（Decrypt - Replace Cert）]**、または **[復号 - 既知のキー（Decrypt - Known Key）]** ルールアクションを含むルールでは、**[暗号スイート（Cipher Suite）]** または **[バージョン（Version）]** ルール条件を決して使用しないでください。これらの条件をルールで他のルールアクションとともに使用すると、システムの ClientHello 処理に干渉し、予測できないパフォーマンスが生じる可能性があります。

#### [復号 - 再署名（Decrypt - Resign）] ルールアクションと証明書署名要求

[復号-再署名（Decrypt - Resign）] ルールアクションを使用するには、証明書署名要求（CSR）を作成し、信頼された証明機関によって署名する必要があります。（FMC を使用して CSR を作成できます：**[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** > **[PKI]** > **[内部CA（Internal CAs）]**。）

[復号-再署名（Decrypt - Resign）] ルールで使用するには、認証局（CA）に次の拡張機能の少なくとも 1 つが必要です。

- **CA: TRUE**

  詳細については、RFC3280、セクション 4.2.1.10 にある、基本制約に関する説明を参照してください。

- **KeyUsage=CertSign**

  詳細については、RFC 5280、セクション 4.2.1.3 を参照してください。

CSR または CA に前述の拡張機能の少なくとも 1 つがあることを確認するには、openssl のドキュメントなどの参考資料で説明されている、**openssl** コマンドを使用できます。

これが必要なのは、[復号 - 再署名（Decrypt - Resign）] インスペクションが機能するために、復号ポリシーで使用された証明書がオンザフライで証明書を生成し、中間者として機能し、すべての TLS/SSL 接続をプロキシするようにそれらに署名するためです。

### 証明書のピン留め

ブラウザが証明書ピニングを使用してサーバー証明書を確認する場合は、サーバー証明書に再署名しても、このトラフィックを復号できません。このトラフィックを許可するには、サーバー証明書の共通名または識別名と一致させるために、[復号しない（Do not decrypt）] アクションを使用して 復号ルール を設定します。

### 一致しない暗号スイート

証明書と一致しない暗号スイートで復号ルールを保存しようとすると、次のエラーが表示されます。この問題を解決するには、TLS/SSL 暗号スイートの確認 （52 ページ） を参照してください。

```
Traffic cannot match this rule; none of your selected cipher suites contain a
signature algorithm that the resigning CA's signature algorithm
```

### 信頼できない認証局

サーバー証明書の再署名に使用する認証局（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という警告がユーザーに出されます。これを防止するには、クライアントの信用できる 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。

### HTTP プロキシの制限

クライアントと管理対象デバイスの間に HTTP プロキシがあって、クライアントとサーバーが CONNECT HTTP メソッドを使用してトンネル TLS/SSL 接続を確立する場合、システムはトラフィックを復号できません。システム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（**Handshake Errors**）の復号できないアクションが決定します。

### 署名済み CA のアップロード

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は、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 を [復号 - 再署名（Decrypt - Resign）] アクションに使用できません。

### 署名アルゴリズムの不一致

[復号 - 再署名（Decrypt - Resign）] アクションをルールに設定し、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**（  ）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[警告（warning）]（  ）が表示され、復号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。

# TLS/SSL 復号：既知のキーのガイドライン

[復号 - 既知のキー（Decrypt - Known Key）] アクションを設定した場合は、1 つまたは複数のサーバー証明書と秘密キー 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、システム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する場合です。

また次の点に注意してください。

### 匿名の暗号スイートはサポート対象外

匿名の暗号スイートはその性質から、認証には使用されず、キー交換を使用しません。匿名の暗号スイートには限定的な用途があります。詳細については、RFC 5246 の付録 F.1.1.1 を参照してください。（TLS 1.3 では、代わりに RFC 8446 付録 C.5 を参照してください。）

匿名の暗号スイートは認証に使用されないため、ルールに [復号-再署名（Decrypt - Resign）] または [復号-既知のキー（Decrypt - Known Key）] アクションは使用できません。

### 識別名または証明書が一致しない

[復号 - 既知のキー（Decrypt - Known Key）] アクションを指定して 復号ルール を作成した場合は、[識別名（Distinguished Name）] や [証明書（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。

### バージョンまたは暗号スイートのルール条件を使用しない

重要 **[復号 - 再署名（Decrypt - Resign）]**、**[復号 - 証明書の置き換え（Decrypt - Replace Cert）]**、または **[復号 - 既知のキー（Decrypt - Known Key）]** ルール アクションを含むルールでは、**[暗号スイート（Cipher Suite）]** または **[バージョン（Version）]** ルール条件を決して使用しないでください。これらの条件をルールで他のルールアクションとともに使用すると、システムの ClientHello 処理に干渉し、予測できないパフォーマンスが生じる可能性があります。

### 楕円曲線デジタル署名アルゴリズム（*ECDSA*）証明書によってトラフィックがブロックされる

（TLS 1.3 復号が有効の場合のみ）[復号 - 既知のキー（Decrypt - Known Key）] アクションで ECDSA 証明書を使用すると、一致するトラフィックがブロックされます。これを回避するには、証明書を別のタイプの証明書とともに使用します。

# TLS/SSL ブロックのガイドライン

[インタラクティブブロック（Interactive Block）] または [リセット付きインタラクティブブロック（Interactive Block with reset）] アクション付きのアクセス コントロール ポリシーと 復号ルール が関連付けられている場合、システムはカスタマイズ可能な応答ページを表示します。

ルールでロギングを有効にすると、（**[分析（Analysis）] > [イベント（Events）] > [接続（Connections）]** で）2 つの接続イベントが表示されます。インタラクティブ ブロックのイベントと、ユーザーがサイトの継続を選択したかどうかを示す別のイベントです。

**関連トピック**

HTTP 応答ページの設定

# TLS/SSL 証明書のピン留めのガイドライン

一部のアプリケーションでは、アプリケーション自体に元のサーバー証明書のフィンガープリントを埋め込む、ピニングまたは証明書ピニングと呼ばれる技術が使用されます。*TLS/SSL* そのため、[復号 - 再署名（Decrypt - Resign）] アクションで 復号ルール を設定した場合は、アプリケーションが管理対象デバイスから再署名された証明書を受信すると、検証が失敗し、接続が中断されます。

TLS/SSL のピン留めは中間者攻撃を避けるために使用されるため、防止または回避する方法はありません。ピニングトラフィックが復号対象から除外されるように、[復号 - 再署名（Decrypt - Resign）] ルールの前に [復号しない（Do Not Decrypt）] ルールを追加することを推奨します。

- そのアプリケーション用に、[復号-再署名（Decrypt - Resign）] ルールよりも順序が前の、[復号しない（Do Not Decrypt）] ルールを作成します。
- Web ブラウザを使用してアプリケーションにアクセスするようユーザに指示します。

ルールの順序の詳細については、SSL ルールの順序を参照してください。

アプリケーションが TLS/SSL のピン留めを使用しているかどうかを判断するには、TLS/SSL ピニングのトラブルシューティング （48 ページ）を参照してください。

# TLS/SSL ハートビートのガイドライン

一部のアプリケーションでは、RFC6520 で定義されている Transport Layer Security（TLS）および Datagram Transport Layer Security（DTLS）プロトコルに対して、TLS ハートビート エクステンションが使用されます。TLS ハートビートは、接続がまだ有効であることを確認する方法を提供します。クライアントまたはサーバが指定されたバイト数のデータを送信し、応答を返すように相手に要求します。これが成功した場合は、暗号化されたデータが送信されます。

ネットワーク分析ポリシー（NAP）で [最大ハートビート長（Max Heartbeat Length）] を設定して TLS ハートビートの処理方法を決定できます。詳細については、SSL プリプロセッサを参照してください。

詳細については、「TLS ハートビートについて （46 ページ）」を参照してください。

# TLS/SSL 匿名の暗号スイートの制限事項

匿名の暗号スイートはその性質から、認証には使用されず、キー交換を使用しません。匿名の暗号スイートには限定的な用途があります。詳細については、RFC 5246 の付録 F.1.1.1 を参照してください。（TLS 1.3 では、代わりに RFC 8446 付録 C.5 を参照してください。）

匿名の暗号スイートは認証に使用されないため、ルールに [復号-再署名（Decrypt - Resign）] または [復号-既知のキー（Decrypt - Known Key）] アクションは使用できません。

復号ルール の [暗号スイート（Cipher Suite）] 条件に匿名の暗号スイートを追加することはできますが、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 復号ルール を設定する必要があります。詳細については、SSL ルールの順序を参照してください。

# TLS/SSL 正規化のガイドライン

インライン正規化プリプロセッサで [余剰ペイロードの正規化（Normalize Excess Payload）] オプションを有効にすると、プリプロセッサによる復号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。これで TLS/SSL セッションは終了しません。トラフィックが許可された場合、トリミングされたパケットは TLS/SSL セッションの一部として暗号化されます。

# その他の 復号ルール ガイドライン

### ユーザーとグループ

ルールにグループまたはユーザを追加した後、そのグループまたはユーザを除外するようにレルムの設定を変更すると、ルールは適用されなくなります。（レルムを無効にする場合も同様です。）レルムの詳細については、LDAP レルムまたは Active Directory レルムおよびレルムディレクトリの作成を参照してください。

### 復号ルール のカテゴリ

復号ポリシーに [復号-再署名（Decrypt - Resign）] アクションがあっても Web サイトが復号されない場合は、そのポリシーに関連付けられているルールの [カテゴリ（Category）] ページを確認します。

場合によっては、認証などの目的で Web サイトが別のサイトにリダイレクトされ、リダイレクト先のサイトの URL カテゴリが復号を試みているサイトとは異なることがあります。たとえば、`gmail.com`（[Webベース電子メール（Web based email）] カテゴリ）は認証のために `accounts.gmail.com`（[インターネットポータル（Internet Portals）] カテゴリ）にリダイレクトされます。関連するすべてのカテゴリを必ず SSL ルールに含めます。

（注） URL カテゴリに基づいてトラフィックを完全に処理するには、URL フィルタリングも設定する必要があります。URL フィルタリングの章を参照してください。

### ローカル データベースにない URL のクエリ

[復号-再署名（Decrypt - Resign）] ルールを作成し、ローカル データベースにカテゴリとレピュテーションがない Web サイトをユーザが参照すると、データが復号されないことがあります。一部の Web サイトはローカル データベースで分類されません。分類されない場合、その Web サイトのデータはデフォルトでは復号されません。

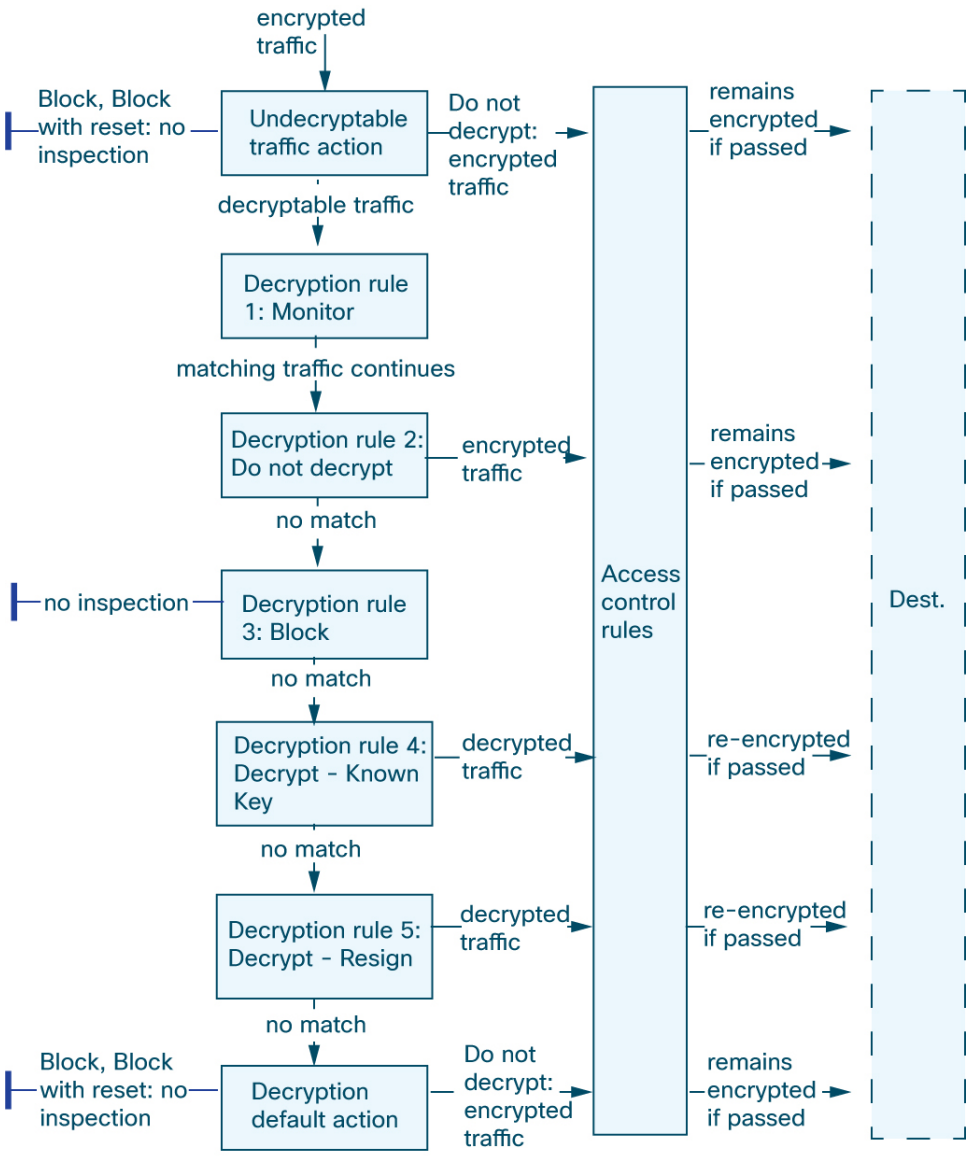
[システム（System）]>[統合（Integration）]> **クラウド サービス** を設定して、[不明なURLをCisco Cloudに問い合わせる（Query Cisco cloud for unknown URLs）] チェック ボックスをオンにすることで、この動作を制御できます。

# 復号ルールトラフィック処理

トラフィックはユーザーが指定した順序で 復号ルール と照合されます。ほとんどの場合、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復号ルールに従って実行されます。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、VLAN、ポート、アプリケーション、要求されたURL、ユーザー、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。

各ルールにはアクションも設定されます。アクションにより、アクセス制御と一致する暗号化または復号トラフィックに対してモニター、ブロック、検査のいずれを行うかが決まります。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、暗号化ペイロードの侵入およびファイル検査を、システムは無効化します。

次のシナリオは、インライン展開での 復号ルール によるトラフィックの処理を要約しています。




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。復号できないトラフィックについてシステムは、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。
- **復号ルール1：モニター（Monitor）**は、暗号化トラフィックを次に評価します。モニタールールは、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。システム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。

- **復号ルール 2**：**復号しない（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。システムはこのトラフィックをアクセス 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。
- **復号ルール3**：**ブロック（Block）**は、暗号化トラフィックを4番目に評価します。一致するトラフィックは、追加のインスペクションなしでブロックされます。一致しないトラフィックは、引き続き次のルールと照合されます。
- **復号ルール 4**：**復号 - 既知のキー（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、ユーザーのアップロードする秘密キーを使用して復号されます。復号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。この追加検査の結果、システム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。復号ルールに一致しないトラフィックは、引き続き次のルールと照合されます。
- **復号ルール 5**：**復号 - 再署名（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、システムはアップロードされた CA 証明書を使用してサーバー証明書を再署名してから、中間者（man-in-the-middle）としてトラフィックを復号します。復号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。この追加検査の結果、システム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。
- **復号ポリシーデフォルトアクション**は、いずれの 復号ルール にも一致しない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、あるいは復号しないで、アクセス コントロールによる検査を行います。

# 暗号化トラフィック インスペクションの設定

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）の証明書の復号ポリシーへのアップロード時、復号ルールの作成時、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

セッション暗号化に使用するサーバー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、システムは着信する暗号化トラフィックを復号できます。[復号-既知のキー（Decrypt - Known Key）] アクションが設定された復号ポリシールールでそのオブ

ジェクトを参照している場合に、当該ルールにトラフィックが一致すると、アップロードされた秘密キーを使用してセッションが復号されます。

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、システムは発信トラフィックの復号もできます。[復号 - 再署名（Decrypt - Resign）] アクションが設定された復号ルールでそのオブジェクトを参照している場合に、当該ルールにトラフィックが一致すると、クライアントブラウザに渡されたサーバー証明書が再署名され、システムが中間者（man-in-the-middle）として機能してセッションが復号されます。 オプションで、証明書全体ではなく自己署名証明書キーのみを置き換えることができます。この場合、ユーザはブラウザで自己署名証明書キー通知を確認します。

### 暗号化セッションの特性に基づいたトラフィック制御

システムによる暗号化トラフィックの制御は、セッション ネゴシエートに使用されたサーバー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、復号ルール条件でオブジェクトを参照してトラフィックを照合できます。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用される暗号スイートが、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 |
| 組織が信頼する 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ー証明書を信頼する<br>• CA が証明書を直接発行した<br>• サーバー証明書を発行した中間 CA に CA が証明書を発行した |
| サーバー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ー証明書が、アップロードされたサーバー証明書と一致する |
| 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、設定された識別名と一致する |

**関連トピック**

暗号スイート リスト
識別名
PKI

# 復号ルールの評価の順序

この情報は、レガシー復号のポリシーとルールにのみ適用されます。

復号ポリシーで復号ルールを作成する場合、ルールエディタの [挿入（Insert）] リストを使用してその位置を指定します。復号ポリシー内の復号ルールには、1 から始まる番号が付けられています。復号ルールは、ルール番号の昇順で上から順にトラフィックと照合されます。

ほとんどの場合、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復号ルールに従って実行されます。モニタールール（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ルール）の場合を除き、システムは、そのトラフィックがルールに一致した後、追加の優先順位の低いルールに対してトラフィックを評価し続けることはありません。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、VLAN、ポート、アプリケーション、要求されたURL、ユーザー、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。

各ルールにはアクションも設定されます。アクションにより、アクセス制御と一致する暗号化または復号トラフィックに対してモニター、ブロック、検査のいずれを行うかが決まります。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。暗号化されたトラフィックおよび復号できないトラフィックはアクセス コントロールの対象です。ただし、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ります。

特定の条件（ネットワークや IP アドレスなど）を使用するルールは、一般的な条件（アプリケーションなど）を使用するルールの前に順位付けする必要があります。オープン システム相互接続（OSI）モデルに精通している場合は、考え方として同様の順位付けを使用してください。レイヤ1、2、および3（物理、データリンク、およびネットワーク）の条件を持つルールは、ルールの最初に順位付けする必要があります。レイヤ5、6、および7（セッション、プレゼンテーション、およびアプリケーション）の条件は、ルールの後ろのほうに順序付けする必要があります。OSI モデルの詳細については、こちらの Wikipedia の記事を参照してください。

**ヒント** 適切な復号ルールの順序を指定することで、ネットワーク トラフィックの処理に必要なリソースが削減され、ルールのプリエンプションを回避できます。ユーザー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、ユーザー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。

番号ごとのルールの順序付けに加えて、カテゴリ別にルールをグループ化できます。デフォルトでは、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、システム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。

**関連トピック**

アクセス制御ルールのベストプラクティス
復号できないトラフィックのデフォルト処理オプション
SSL ルールの順序

# 復号ルール 条件

復号ルールの条件は、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、システム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SSLまたはTLSのバージョンにかかわりなく、セッションのネゴシエーションに使用されるサーバー証明書に基づいてトラフィックを評価します。

すべての復号ルールには、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：最も重要なこととして、ルール アクションはルールの条件に一致する暗号化トラフィックに対して、モニター、信頼、ブロック、または復号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。

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

- 復号ポリシーの復号できないアクションは、システムが復号できないトラフィックを処理します。
- ポリシーのデフォルトアクションは、モニター以外のどの復号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。

システム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のために復号した場合の接続ログを記録するようにシステムを強制することも可能で、これはその後でどのような処理やトラフィックの検査がされるかとは無関係です。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、接続終了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（[ブロック（Block）]、[リセットしてブロック（Block with reset）]）の場合、システムは即座にセッションを終了し、イベントを生成します。
- 復号しない（Do not decrypt）接続の場合、システムはセッション終了時にイベントを生成します

可能な場合は常に、一致基準の数を最小限にします（特にセキュリティゾーン、ネットワークオブジェクト、およびポートオブジェクトの場合）。基準を複数指定すると、指定した条件の内容について「すべて」の組み合わせと照合する必要があります。

⚠

**注意** TLS/SSL 復号が無効の場合（つまりアクセス コントロール ポリシーに 復号ポリシーが含まれない場合）に、アクティブな最初の認証ルールを追加するか、アクティブな最後の認証ルールを削除すると設定の変更を展開する際に Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲットデバイスがトラフィックを処理する方法に応じて異なります。詳細はSnort の再起動によるトラフィックの動作を参照してください。

アクティブな認証ルールに [アクティブ認証（Active Authentication）] ルールアクションが含まれるか、[パッシブ/VPNアイデンティティを確立できない場合にアクティブ認証を使用（Use active authentication if passive or VPN identity cannot be established）] が選択された [パッシブ認証（Passive Authentication）] ルールアクションが含まれることに注意してください。

**関連トピック**

セキュリティゾーンルール条件
ネットワークルール条件
VLAN タグルール条件
ユーザールール条件
アプリケーションルール条件
ポートルールの条件
カテゴリルール条件 （23 ページ）
サーバー証明書ベースの 復号ルール条件 （23 ページ）

# セキュリティゾーンルール条件

セキュリティゾーンはネットワークをセグメント化して複数のデバイス間でインターフェイスをグループ化することで、トラフィックフローを管理、分類、および復号しやすくします。

セキュリティゾーンは、トラフィックをその送信元と宛先のセキュリティゾーンで制御または復号します。送信元ゾーンと宛先ゾーンの両方をゾーン条件に追加すると、送信元ゾーンのいずれかにあるインターフェイスから発信され、宛先ゾーンのいずれかにあるインターフェイスを通過するトラフィックだけが一致することになります。

ゾーン内のすべてのインターフェイスは同じタイプ（すべてインライン、パッシブ、スイッチド、またはルーテッド）である必要があるのと同じく、ゾーン条件で使用するすべてのゾーンも同じタイプである必要があります。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、パッシブインターフェイスのあるゾーンを宛先ゾーンとして使用することはできません。

可能な場合は常に、一致基準の数を最小限にします（特にセキュリティゾーン、ネットワークオブジェクト、およびポートオブジェクトの場合）。基準を複数指定すると、指定した条件の内容について「すべて」の組み合わせと照合する必要があります。

ヒント　ゾーンによってルールを制限することは、システムのパフォーマンスを向上させる最適な手段の 1 つです。ルールがデバイスのインターフェイスを通過するトラフィックに適用しなければ、ルールがそのデバイスのパフォーマンスに影響することはありません。

## セキュリティ ゾーン条件とマルチテナンシー

マルチドメイン導入では、先祖ドメイン内に作成されるゾーンに、別のドメイン内にあるデバイス上のインターフェイスを含めることができます。子孫ドメイン内のゾーン条件を設定すると、その設定は表示可能なインターフェイスだけに適用されます。

# ネットワークルール条件

ネットワークは、内部ヘッダーを使用して、送信元と宛先の IP アドレスを基準にトラフィックを制御するか、復号します。外部ヘッダーを使用するトンネル ルールでは、ネットワーク条件の代わりにトンネル エンドポイント条件を使用します。

事前定義されたオブジェクトを使用してネットワーク条件を作成することも、個々の IP アドレスまたはアドレス ブロックを手動で指定することもできます。

可能な場合は常に、一致基準の数を最小限にします（特にセキュリティゾーン、ネットワークオブジェクト、およびポートオブジェクトの場合）。基準を複数指定すると、指定した条件の内容について「すべて」の組み合わせと照合する必要があります。

（注）　アイデンティティルールで FDQN ネットワークオブジェクトを使用することはできません。

# VLAN タグルール条件

（注）　アクセスルールの VLAN タグは、インラインセットにのみ適用されます。VLAN タグを持つアクセスルールは、ファイアウォール インターフェイス上のトラフィックを照合しません。

VLAN ルール条件によって、Q-in-Q（スタック VLAN）など、VLAN タグ付きトラフィックが制御されます。システムでは、プレフィルタ ポリシー（そのルールで最も外側の VLAN タグを使用する）を除き、最も内側の VLAN タグを使用して VLAN トラフィックをフィルタ処理します。

次の Q-in-Q サポートに注意してください。

- Firepower 4100/9300 上の Firewall Threat Defense：Q-in-Q をサポートしません（1 つの VLAN タグのみをサポート）。
- 他のすべてのモデルの Firewall Threat Defense

- インラインセットおよびパッシブインターフェイス：Q-in-Q をサポートします（最大 2 つの VLAN タグをサポート）。
- ファイアウォール インターフェイス：Q-in-Q をサポートしません（1 つの VLAN タグのみをサポート）。

事前定義のオブジェクトを使用して VLAN 条件を作成でき、また 1 ～ 4094 の VLAN タグを手動で入力することもできます。VLAN タグの範囲を指定するには、ハイフンを使用します。

クラスタで VLAN マッチングに問題が発生した場合は、アクセス コントロール ポリシーの詳細オプションである [トランスポート/ネットワークリプロセッサ設定（Transport/Network Preprocessor Settings）] を編集し、[接続の追跡時にVLANヘッダーを無視する（Ignore the VLAN header when tracking connections）] オプションを選択します。

# ユーザールール条件

接続を開始したユーザー、またはユーザーが属するグループに基づいてトラフィックが照合されます。たとえば、財務グループの全員がネットワークリソースにアクセスすることを禁止するブロックルールを設定できます。

Microsoft Active Directory レルムのユーザーに対してのみユーザー ルール条件を設定できます。

設定されたレルムのユーザーとグループの設定に加えて、次の特殊なアイデンティティユーザーのポリシーを設定できます。

- [失敗した認証（Failed Authentication）]：キャプティブポータルでの認証に失敗したユーザー。
- [ゲスト（Guest）]：キャプティブポータルでゲストユーザーとして設定されたユーザー。
- [認証不要（No Authentication Required）]：アイデンティティの [認証不要（No Authentication Required）] ルールアクションに一致するユーザー。
- [不明（Unknown）]：識別できないユーザー。たとえば、設定されたレルムによってダウンロードされていないユーザー。

アクセス制御ルールのみの場合、ID ポリシーをアクセス コントロール ポリシーに最初に関連付ける必要があります（アクセス制御への他のポリシーの関連付けを参照）。

# アプリケーションルール条件

システムはIP トラフィックを分析する際、ネットワークで一般的に使用されているアプリケーションを識別および分類できます。このディスカバリベースのアプリケーション認識は、アプリケーション制御、つまりアプリケーション トラフィック制御機能の基本です。

システム提供のアプリケーション フィルタは、アプリケーションの基本特性（タイプ、リスク、ビジネスとの関連性、カテゴリ、およびタグ）にしたがってアプリケーションを整理することで、アプリケーション制御に役立ちます。システム提供のフィルタの組み合わせやアプリ

ケーションの任意の組み合わせをもとに、ユーザー定義の再利用可能フィルタを作成できます。

ポリシーのアプリケーション ルール条件ごとに、少なくとも 1 つのディテクタが有効にされている必要があります。有効になっているディテクタがないアプリケーションについては、システム提供のすべてのディテクタが自動的に有効になります。ディテクタが存在しない場合は、そのアプリケーションについて最後に変更されたユーザー定義ディテクタが有効になります。アプリケーション ディテクタの詳細については、アプリケーション ディテクタの基本を参照してください。

アプリケーション フィルタと個別に指定されたアプリケーションの両方を使用することで、完全なカバレッジを確保できます。ただし、アクセス コントロール ルールの順序を指定する前に、次の注意事項を確認してください。

### アプリケーション フィルタの利点

アプリケーション フィルタにより、迅速にアプリケーション制御を設定できます。たとえば、システム提供のフィルタを使って、リスクが高く、ビジネスとの関連性が低いアプリケーションをすべて認識してブロックするアクセス コントロール ルールを簡単に作成できます。ユーザーがそれらのアプリケーションの 1 つを使用しようとすると、システムがセッションをブロックします。

アプリケーション フィルタを使用することで、ポリシーの作成と管理は簡単になります。この方法によりアプリケーション トラフィックが期待どおりに制御されます。シスコは、システムと脆弱性データベース（VDB）の更新を通して、頻繁にアプリケーション ディテクタを更新しています。このため、アプリケーション トラフィックは常に最新のディテクタによってモニターされます。また、独自のディテクタを作成し、どのような特性のアプリケーションを検出するかを割り当て、既存のフィルタを自動的に追加することもできます。

### アプリケーションの特性

システムは、次の表に示す基準を使用して、検出された各アプリケーションの特性を判別します。これらの特性をアプリケーション フィルタとして使用します。

**表 *1:* アプリケーションの特性**

| 特性 | 説明 | 例 |
|---|---|---|
| タイプ | アプリケーション プロトコルは、ホスト間の通信を意味します。<br>クライアントは、ホスト上で動作しているソフトウェアを意味します。<br>Web アプリケーションは、HTTP トラフィックの内容または要求された URL を意味します。 | HTTP と SSH はアプリケーション プロトコルです。<br>Web ブラウザと電子メール クライアントはクライアントです。<br>MPEG ビデオと Facebook は Web アプリケーションです。 |
| リスク（Risk） | アプリケーションが組織のセキュリティ ポリシーに違反することがある目的で使用される可能性。 | ピアツーピア アプリケーションはリスクが極めて高いと見なされます。 |

| 特性 | 説明 | 例 |
|---|---|---|
| ビジネスとの関連性（Business Relevance） | アプリケーションが、娯楽目的ではなく、組織のビジネス活動の範囲内で使用される可能性。 | ゲームアプリケーションはビジネスとの関連性が極めて低いと見なされます。 |
| カテゴリ | アプリケーションの最も不可欠な機能を表す一般的な分類。各アプリケーションは、少なくとも1つのカテゴリに属します。 | Facebookはソーシャルネットワーキングのカテゴリに含まれます。 |
| タグ | アプリケーションに関する追加情報。アプリケーションには任意の数のタグを付けることができます（タグなしも可能）。 | ビデオストリーミングWebアプリケーションには、ほとんどの場合、`high bandwidth`と`displays ads`というタグが付けられます。 |

**関連トピック**

アプリケーション制御の設定のベストプラクティス

# ポートルールの条件

ポート条件を使用することで、トラフィックの送信元および宛先のポートに応じてそのトラフィックを制御できます。

可能な場合は常に、一致基準の数を最小限にします（特にセキュリティゾーン、ネットワークオブジェクト、およびポートオブジェクトの場合）。基準を複数指定すると、指定した条件の内容について「すべて」の組み合わせと照合する必要があります。

### ポートベースのルールのベストプラクティス

ポートの指定は、アプリケーションをターゲット指定するための従来の方法です。ただし、アプリケーションは、固有のポートを使用してアクセス コントロール ブロックをバイパスするように設定することが可能です。そのため、可能な場合は常に、ポート基準ではなくアプリケーション フィルタリング基準を使用してトラフィックをターゲット指定します。

アプリケーションフィルタリングは、制御フローとデータフローのために個別のチャネルを動的に開くアプリケーション（FTD など）にも推奨されます。ポートベースのアクセス コントロール ルールを使用すると、これらの種類のアプリケーションが正しく動作しなくなり、望ましい接続がブロックされる可能性があります。

### 送信元と宛先ポートの制約の使用

送信元ポートと宛先ポートの両方を制約に追加する場合、単一のトランスポート プロトコル（TCP または UDP）を共有するポートのみを追加できます。たとえば、送信元ポートとして DNS over TCP を追加する場合は、宛先ポートとして Yahoo Messenger Voice Chat（TCP）を追加できますが、Yahoo Messenger Voice Chat（UDP）は追加できません。

送信元ポートのみ、あるいは宛先ポートのみを追加する場合は、異なるトランスポートプロトコルを使用するポートを追加できます。たとえば、DNS over TCP および DNS over UDP の両方を 1 つのアクセス コントロール ルールの送信元ポート条件として追加できます。

# カテゴリルール条件

必要に応じて、復号ポリシーにカテゴリを含めることができます。これらのカテゴリ（「URL フィルタリング」とも呼ばれる）は、Cisco Talos インテリジェンスグループによって更新されます。更新は、Web サイトの宛先から（場合によってはそのホスティングおよび登録情報から）取得可能な内容に従って、機械学習および人間の分析に基づいて行われます。分類は、宣言された会社の業種、意図、またはセキュリティに基づいて行われません。

詳細については、URL フィルタリングの概要を参照してください。

[復号しない（Do Not Decrypt）] ルールアクションを含むルールの復号ポリシーでカテゴリルール条件を使用している場合は、復号ルール [復号しない（Do Not Decrypt）] アクション （38 ページ）を参照してください。

# サーバー証明書ベースの 復号ルール条件

復号ルールでは、サーバー証明書の特性に基づいて暗号化トラフックを処理および復号できます。復号ルールは、以下のサーバー証明書属性に基づいて設定することができます。

- 識別名条件を設定すると、証明書所有者またはサーバー証明書の発行元 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、サイトのサーバー証明書を発行した CA に基づいてトラフィックを処理できます。
- 復号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。
- 復号ルールの証明書ステータス条件では、トラフィックの暗号化に使用されたサーバー証明書のステータスに基づいて暗号化されたトラフィックを処理して、証明書が有効か、失効しているか、期限切れか、まだ有効でないか、自己署名済みか、信頼できる CA によって署名済みか、証明書失効リスト（CRL）が有効かどうか、証明書のサーバー名指定（SNI）が要求内のサーバーと一致するかどうかなどの検査を行うことができます。
- 復号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。
- 復号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。

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。サーバー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。

**関連トピック**

証明書の 復号ルール条件 （24 ページ）
証明書ステータスの 復号ルール条件 （31 ページ）
外部認証局の信頼 （30 ページ）
証明書ステータスでのトラフィックの照合
暗号スイートの 復号ルール 条件 （34 ページ）
暗号化プロトコルバージョンの復号ルール条件 （37 ページ）

# 証明書の 復号ルール条件

証明書ベースの復号ルール条件を作成するときにサーバー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証明書を保存して、サーバー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）、あるいは URL が証明書のサブジェクト代替名（SAN）に含まれている

  ユーザーがブラウザに入力する URL が共通名（CN）と一致する

- 件名または発行元の組織（O）
- 件名または発行元の部門（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ー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。
- 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 [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が表示されます。

- システムが新しいサーバー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、サーバー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、復号の可能性を最大化できます。

## 識別名（DN）のルール条件

このトピックでは、復号ルールで識別名条件を使用する方法について説明します。よくわからない場合は、Web ブラウザを使用して証明書のサブジェクト代替名（SAN）と共通名を見つけ、それらの値を識別名条件として 復号ルール ルールに追加できます。

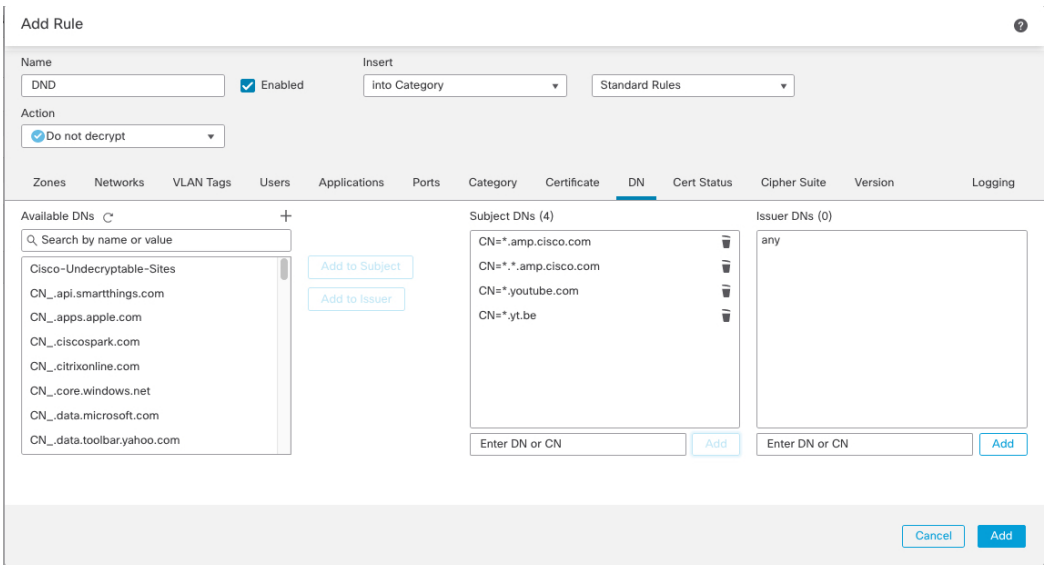
SAN の詳細については、RFC 528、セクション 4.2.1.6 を参照してください。

ここでは、次の点について説明します。

- DN ルールマッチングの例
- システムでの SNI と SAN の使用方法
- 証明書の共通名とサブジェクト代替名を見つける方法
- DN ルール条件を追加する方法

### DN ルールマッチングの例

以下は、[復号しない（Do Not Decrypt）] ルールの DN ルール条件の例です。`amp.cisco.com` または YouTube に向かうトラフィックを復号しないようにしたいとします。次のように DN 条件を設定できます。



前述の DN ルール条件は次の URL に一致するため、トラフィックは復号されません。以前のルールによって復号は防止されました。

- www.amp.cisco.com
- auth.amp.cisco.com
- auth.us.amp.cisco.com
- www.youtube.com
- kids.youtube.com
- www.yt.be

前述の DN ルール条件は、次の URL のいずれにも一致しないため、トラフィックは [復号しない（Do Not Decrypt）] ルールには一致しませんが、同じ 復号ポリシー内の他の 復号ルールには一致する可能性があります。

- amp.cisco.com
- youtube.com
- yt.be

上記のホスト名のいずれかと一致するには、ルールに CN を追加します（たとえば、`CN=yt.be` を追加すると、その URL に一致します）。

### システムでの SNI と SAN の使用方法

クライアント要求の URL のホスト名部分は、サーバー名指定（SNI）です。クライアントは、TLS ハンドシェイクの SNI 拡張を使用して、接続するホスト名（たとえば、`auth.amp.cisco.com`）を指定します。次に、サーバーは、単一の IP アドレスですべての証明書をホストしながら、接続を確立するために必要な、対応する秘密キーと証明書チェーンを選択します。

SNI と証明書の CN または SAN が一致する場合、ルールにリストされている DN と比較するときに SNI を使用します。SNI がない場合、または証明書と一致しない場合は、ルールにリストされている DN と比較するときに、証明書の CN を使用します。

### 証明書の共通名とサブジェクト代替名を見つける方法

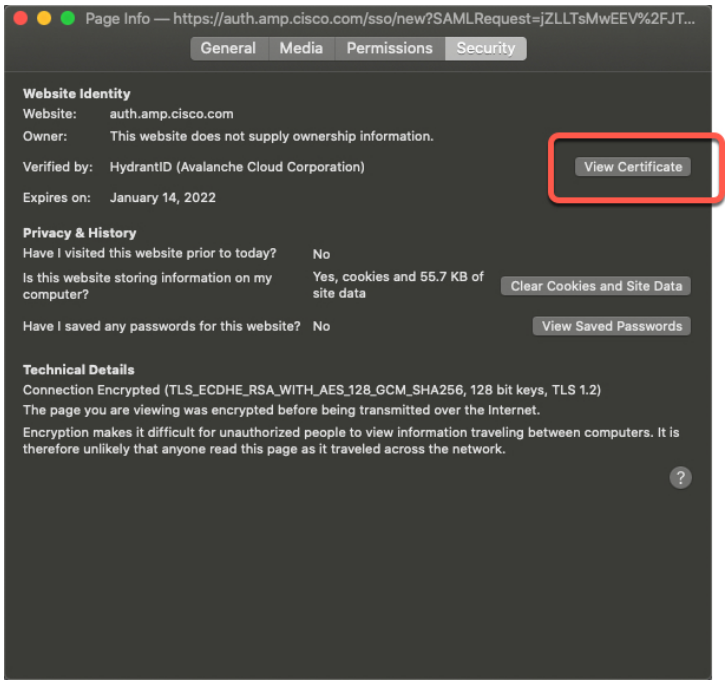
証明書の共通名を見つけるには、次の手順を使用します。これらの手順を使用して、自己署名証明書の共通名と SAN を見つけることもできます。

これらの手順は Firefox 用ですが、他のブラウザも同様です。次の手順では、例として `amp.cisco.com` を使用します。

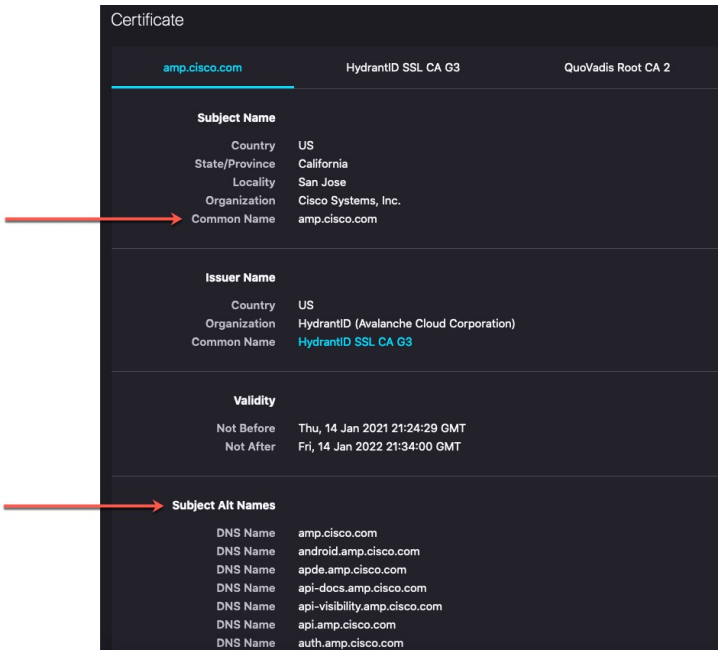
1. Firefox で `amp.cisco.com` にアクセスします。
2. ブラウザのロケーションバーで、URL の左側にある をクリックします。
3. **[この接続は保護されています（Connection secure）] > [詳細情報（More Information）]** をクリックします

（セキュリティで保護されていない場合、または自己署名証明書の場合は、**[この接続は保護されていません（Connection not secure）]** > **[詳細情報（More Information）]** をクリックします）。

4. [ページ情報（Page Info）] ダイアログボックスで、[証明書の表示（View Certificate）] をクリックします。




5. 次のページには、証明書の詳細が表示されます。



次の点に注意してください。

- CN=auth.amp.cisco.com をDNルール条件として使用すると、そのホスト名（つまり、SNI）のみに一致します。SNI amp.cisco.com は一致しません。
- できるだけ多くのドメイン名フィールドに一致させるには、ワイルドカードを使用します。

  たとえば、auth.us.amp.cisco.com と一致させるには、CN=*.*.amp.cisco.com を使用します。auth.us.amp.cisco.com と一致させるには、CN=*.*.amp.cisco.com を使用します。

  CN=*.example.com のようなDNは www.example.com に一致しますが、example.com には一致しません。両方のSNIに一致させるには、ルール条件で2つのDNを使用します。
- ただし、ワイルドカードは使いすぎないでください。たとえば、CN=*.google.com のようなDNオブジェクトは、非常に多数のSANに一致します。CN=*.google.com の代わりに、CN=*.youtube.com などのDNオブジェクトをDNオブジェクトとして使用して、www.youtube.com などの名前と一致させるようにします。

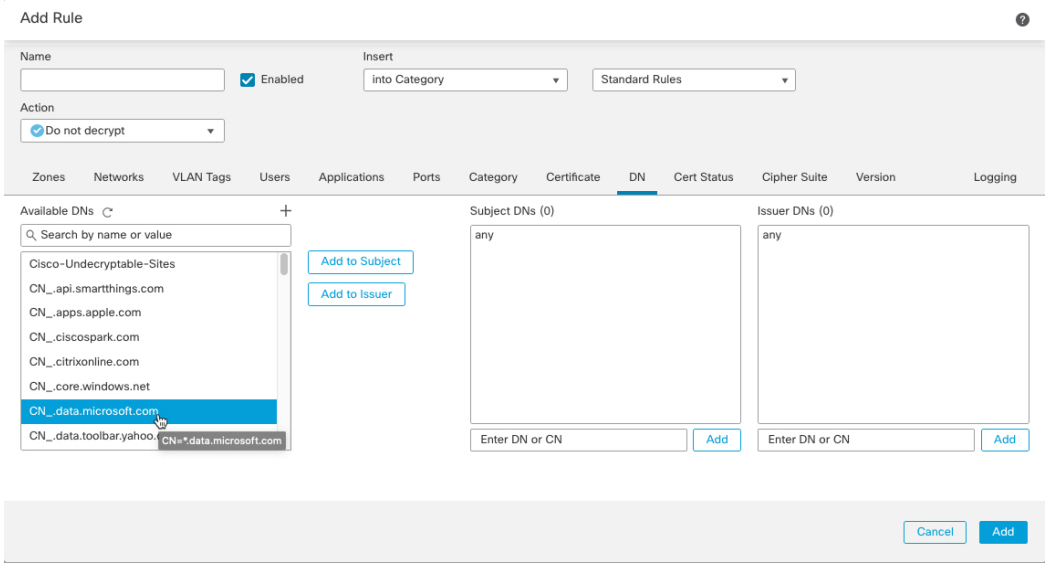
  CN=*.youtube.com、CN=youtu.be、CN=*.yt.be などのSANに一致するSNIのバリエーションを使用することもできます。
- 自己署名証明書も同じように機能するはずです。発行元DNがサブジェクトDNと同じであるという事実によって、自己署名証明書であることを確認できます。

### DN ルール条件を追加する方法

一致させるCNがわかったら、次のいずれかの方法で 復号ルール を編集します。

- 既存のDNを使用します。

  DNの名前をクリックし、[サブジェクトに追加（Add to Subject）] または [発行元に追加（Add to Issuer）] をクリックします（[サブジェクトに追加（Add to Subject）] の方がはるかに一般的です）。DNオブジェクトの値を表示するには、マウスポインタをその上に移動します。

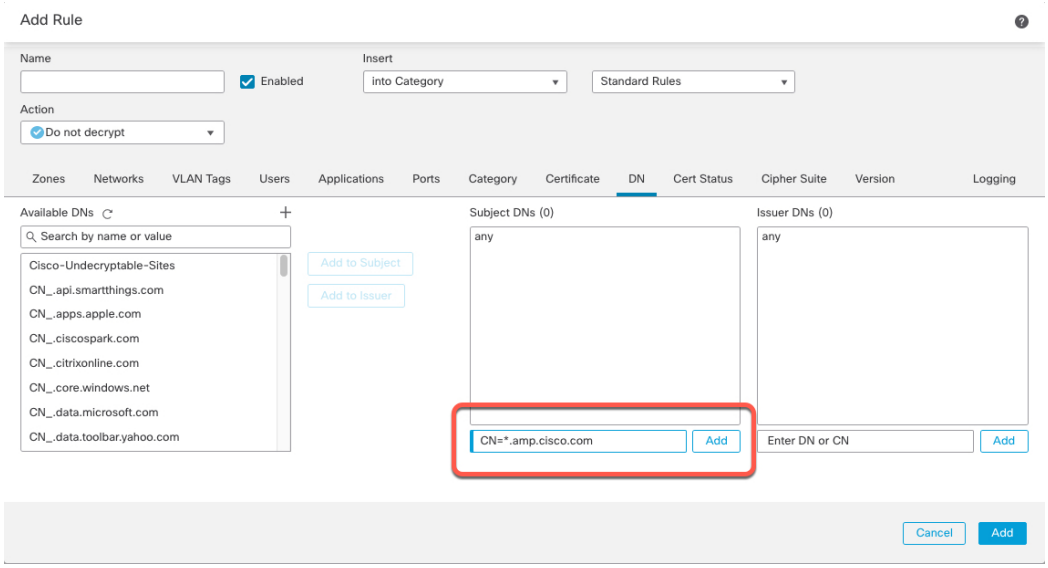



- 新しい DN オブジェクトを作成します。

  [利用可能なDN（Available DNs）] の右側にある [追加（Add）] (＋) をクリックします。DN オブジェクトは、名前と値で構成されている必要があります。

- DN を直接追加します。

  [サブジェクトDN（Subject DNs）] フィールドまたは [発行元DN（Issuer DNs）] フィールドの下部にあるフィールドに DN を入力します（[サブジェクトDN（Subject DNs）] のほうが一般的です）。DN を入力したら、[追加（Add）] をクリックします。




## 関連トピック

識別名

# 外部認証局の信頼

復号ポリシーにルートおよび中間 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ー証明書の検証に、これらの信頼できる CA を使用できるようになります。

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。

**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。また、ルート発行者 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条件を設定する場合、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、復号する必要はなく、復号せずに許可することができます。

詳細については、信頼できる CA オブジェクトを参照してください。

**（注）** 復号ポリシーを作成すると、ポリシーの [信頼できるCA証明書（Trusted CA Certificate）] タブページに、いくつかの信頼できる CA 証明書が入力されます。これらには、[信頼できるCAの選択（Select Trusted CAs）] リストに追加される **Cisco-Trusted-Authorities** グループが含まれます。

## 手順

**ステップ 1** まだ Firewall Management Center にログインしていない場合は、ログインします。

**ステップ 2** **[ポリシー（Policies）]** > **[アクセス制御（Access Control）] 見出し** > **[復号（Decryption）]** をクリックします。

**ステップ 3** 編集する 復号ポリシー の横にある [編集（Edit）]（✎） をクリックします。

**ステップ 4** [ルールの追加（Add Rule）] をクリックして新しい復号ルールを追加するか、[編集（Edit）]（✎） をクリックして既存のルールを編集します。

**ステップ 5** [証明書（Certificates）] タブをクリックします。

**ステップ 6** 次のように、[使用可能な証明書（Available Certificates）] で、追加する信頼できる CA を見つけます。

- 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、[使用可能な証明書（Available Certificates）] リストの上にある [追加（Add）] (＋) をクリックします。
- 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。入力を開始するとリストが更新され、一致するオブジェクトが表示されます。

**ステップ 7** 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。すべてのオブジェクトを選択するには、右クリックして [すべて選択（Select All）] を選択します。

**ステップ 8** [Add to Rule] をクリックします。

**ヒント**
選択したオブジェクトをドラッグ アンド ドロップでリストに追加することもできます。

**ステップ 9** ルールを追加するか、編集を続けます。

### 次のタスク

- SSL ルールに証明書ステータスの復号ルール ルール条件を追加します。詳細については、証明書ステータスでのトラフィックの照合を参照してください。
- 設定変更を展開します設定変更の展開を参照してください。

## 証明書ステータスの 復号ルール条件

設定する証明書ステータスの復号ルール ごとに、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。

複数の証明書ステータスの有無を単一の証明書ステータス ルール条件で照合するように選択できます（いずれか 1 つの基準に一致するだけで、その証明書はルールに一致します）。

このパラメータを設定するときは、復号ルールを設定するのか、ブロック ルールを設定するのかを検討する必要があります。通常、ブロック ルールでは [はい（Yes）]、復号ルールでは [いいえ（No）] をクリックします。次に例を示します。

- [復号 - 再署名（Decrypt - Resign）] ルールを設定している場合、デフォルトの動作は、期限切れの証明書でのトラフィックを復号します。その動作を変更するには、[期限切れ（Expired）] で [いいえ（No）] をクリックし、期限切れの証明書を持つトラフィックが復号され、再署名されないようにします。
- [ブロック（Block）] ルールを設定している場合、デフォルトの動作は、期限切れの証明書を持つトラフィックを許可します。その動作を変更するには、[期限切れ（Expired）] で [はい（Yes）] をクリックし、期限切れの証明書を持つトラフィックをブロックします。

次の表は、暗号化用のサーバー証明書のステータスを基準に、システム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 *2:* 証明書ステータスのルール条件の基準

| ステータス チェック | Yes を設定 | No を設定 |
|---|---|---|
| Revoked | ポリシーは、サーバー証明書を発行した 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ー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頼しており、ポリシーにアップロー証明書にはこのサーバ証明書を失効が含まれていません。 |
| Self-signed | 検出されたサーバー証明書が、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、異なるトと発行元の識別名を含んでいます |
| Valid | 以下のすべてを満たしています。<br>• ポリシーが証明書を発行した CA を信用できる。<br>• 署名は有効である。<br>• 発行元は有効である。<br>• 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。<br>• 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る。 | 以下の 1 つ以上を満たしています。<br>• 証明書を発行した CA をポリシていない。<br>• 署名が無効である。<br>• 発行元が無効である。<br>• ポリシーの信用できる CA の 1証明書が失効している。<br>• 現在の日付が証明書の有効期間り前です。<br>• 現在の日付が証明書の有効期限り後です。 |
| 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証されます。 |
| 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CA 証明書のリストに登録されてい |
| Expired | 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かそれより前です。 |
| Not yet valid | 現在の日付が証明書の有効期限の開始日より前です。 | 現在の日付が証明書の有効期限の開かそれより後です。 |

| ステータス チェック | Yes を設定 | No を設定 |
|---|---|---|
| 無効な証明書 | 証明書が有効ではありません。以下の 1 つ以上を満たしています。<br>• 証明書の拡張子が無効であるか一貫していません。つまり、証明書の拡張子に無効な値（たとえば間違ったエンコーディング）が含まれているか、他の拡張子と矛盾する値がいくつか含まれています。<br>• 指定された目的に証明書を使用できません。<br>• 基本的制約のパス長パラメータを超過しています。<br>詳細については、RFC 5280、セクション 4.2.1.9 を参照してください。<br>• 証明書の発行日付または有効期限の値が無効です。これらの日付は、UTCTime または GeneralizedTime としてエンコードできます。<br>詳細については、RFC 5280、セクション 4.1.2.5 を参照してください。<br>• 名前制約の形式が認識されていません。たとえば、電子メールアドレス形式のフォームは RFC 5280、セクション 4.2.1.10 で言及されていません。これは、不適切な拡張子や、一部の新機能が現時点でサポートされていないことが原因で発生する場合があります。<br>サポートされていない名前制約タイプが見つかりました。OpenSSL では、ディレクトリ名、DNS 名、電子メール、および URI タイプのみがサポートされています。<br>• 指定された目的に関してルート認証局を信頼できません。<br>• ルート認証局が指定された目的を拒否しています。 | 証明書は有効です。以下のすべます。<br>• 有効な証明書の拡張子。<br>• 指定した目的に証明書を使<br>• 有効な基本的制約のパス長<br>• 有効な発行日付または有効<br>• 有効な名前制約。<br>• 指定された目的に関してル頼できる。<br>• ルート証明書が指定した目いる。 |

| ステータス チェック | Yes を設定 | No を設定 |
|---|---|---|
| 無効な CRL | 証明書失効リスト（CRL）のデジタル署名が有効ではありません。以下の 1 つ以上を満たしています。<br>• CRL の [次回の更新（Next Update）] または [最後の更新（Last Update）] フィールドの値が無効である。<br>• CRL がまだ有効ではない。<br>• CRL の期限が切れている。<br>• CRL パスを確認する際にエラーが発生した。拡張CRLの確認が有効になっている場合にのみ、このエラーが発生する。<br>• CRL が検出できない。<br>• 検出できた唯一のCRLが証明書の範囲と一致しなかった。 | CRLが無効です。以下のすべてを満す。<br>• [次回の更新（Next Update）] と新（Last Update）] フィールドのある。<br>• CRL の日付が有効である。<br>• パスが有効である。<br>• CRL が検出された。<br>• CRL が証明書の範囲と一致する |
| サーバーの不一致 | サーバー名がサーバーのサーバー名指定（SNI）名と一致しません。これは、サーバー名を偽装しようとする試みを示している可能性があります。 | サーバー名は、クライアントがアクしているサーバーの SNI 名と一致し |

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。

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、信頼できるCA証明書の復号ポリシーのリストに、信頼できる CA のオブジェクトを追加します。

## 暗号スイートの 復号ルール 条件

ブロックまたはリセット付きブロックのルールアクションのために暗号スイートのルール条件に追加できる、システム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。

**重要** 暗号スイートルール条件は、トラフィックをブロックするためだけに使用する必要があります。トラフィックを復号するためには使用しないでください。

（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。暗号スイート条件に追加できる暗号スイートとして、次のものがサポートされています。

- SSL_RSA_FIPS_WITH_3DES_EDE_CBC_SHA
- SSL_RSA_FIPS_WITH_DES_CBC_SHA
- TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
- TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256
- TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
- TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256
- TLS_DHE_RSA_WITH_DES_CBC_SHA
- TLS_DH_Anon_WITH_AES_128_GCM_SHA256
- TLS_DH_Anon_WITH_AES_256_GCM_SHA384
- TLS_DH_Anon_WITH_CAMELLIA_128_CBC_SHA
- TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA256
- TLS_DH_Anon_WITH_CAMELLIA_256_CBC_SHA
- TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_NULL_SHA
- TLS_ECDHE_ECDSA_WITH_RC4_128_SHA
- TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_NULL_SHA
- TLS_ECDHE_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256
- TLS_RSA_WITH_DES_CBC_SHA
- TLS_RSA_WITH_NULL_MD5
- TLS_RSA_WITH_NULL_SHA
- TLS_RSA_WITH_RC4_128_MD5
- TLS_RSA_WITH_RC4_128_SHA

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すると、設定を展開できません。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。それら

の暗号スイートを使用してルールを作成すると、アクセス コントロール ポリシーを展開できなくなります。

- ルールを使用するには、復号ポリシー で [暗号スイート（Cipher Suite）] 条件に匿名の暗号スイートを追加できます。また、ClientHello が処理されない順序で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」を参照してください。
- 暗号スイー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。

## 暗号化プロトコルバージョンの復号ルール条件

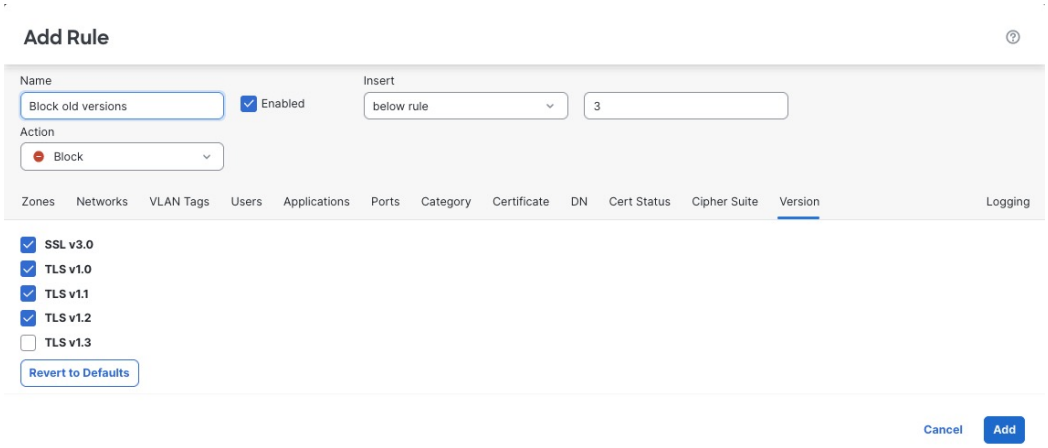
SSL バージョン 3.0 または TLS バージョン 1.0、1.1、1.2 のいずれかで暗号化されたトラフィックとの照合を選択できます。デフォルトでは、ルールの作成時にすべてのプロトコルのバージョンが選択されます。複数のバージョンが選択されている場合、いずれかのバージョンと一致する暗号化トラフィックがルールに一致したと判定されます。ルール条件を保存するには、最低 1 つのプロトコル バージョンを選択する必要があります。

SSL 3.0 は、[復号しない（Do Not Decrypt）]、[ブロック（Block）]、または [リセット付きブロック（Block with Reset）] ルールアクションで使用できます。

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、SSL バージョン 2.0 で暗号化されたトラフィックの復号がサポートされていないためです。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、復号できないトラフィックのデフォルト処理を設定するを参照してください。

**重要** プロトコルバージョンルール条件は、トラフィックをブロックするためだけに使用する必要があります。トラフィックを復号するためには使用しないでください。

たとえば、すべての SSL v3.0、TLS v1.0、TLS v1.1、TLS v1.2 トラフィックをブロックするには、次のようにオプションを設定します。




# 復号ルール アクション

ここでは、復号ルールで利用可能なアクションについて説明します。

## 復号ルール モニターアクション

[Monitor] アクションは、トラフィックを許可または拒否するように設計されていません。むしろ、その主な目的は、一致するトラフィックが最終的にどのように処理されるかに関係なく、接続ロギングを強制することです。トラフィックが [モニター（Monitor）] ルール条件に一致する場合、ClientHello メッセージは変更されません。

その後、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、復号するかが決定されます。モニター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、システムはデフォルト アクションを使用します。

モニター ルールの主要な目的はネットワーク トラフィックを追跡することであるため、ルールのロギング設定や、あとで接続を処理するデフォルトのアクションにかかわらず、システムはモニター対象トラフィックの接続終了イベントを自動的に Secure Firewall Management Center データベースに記録します。

## 復号ルール [復号しない（Do Not Decrypt）] アクション

[復号しない（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。暗号化トラフィックに対しては、侵入やファイル インスペクションなどのディープ インスペクションを行うことはできません。

[復号しない（Do Not Decrypt）] ルール アクションの一般的な理由は、以下のとおりです。

- TLS/SSL トラフィックの復号が法律によって禁止されている。
- 信頼できると判明しているサイトである。
- トラフィックを調べることによって中断できるサイト（Windows Update など）である。
- TLS/SSL フィールドの値を表示するには、接続イベントを使用します。（接続イベント フィールドを表示するためにトラフィックを復号する必要はありません。）詳細については、Cisco Secure Firewall Management Center アドミニストレーション ガイドの「Requirements for Populating Connection Event Fields」を参照してください。

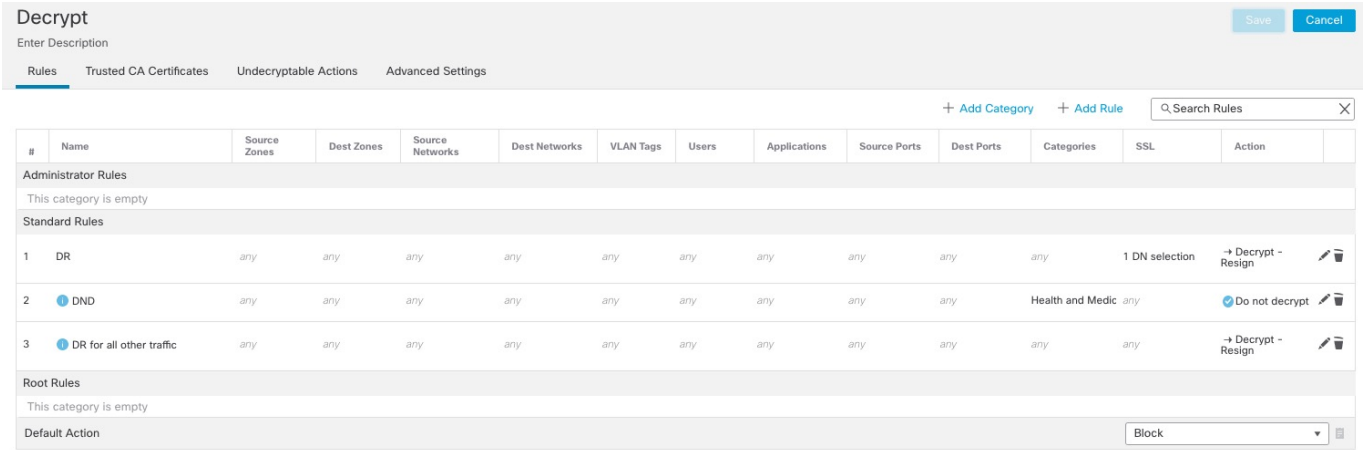
詳細については、「復号できないトラフィックのデフォルト処理オプション」を参照してください。

### [復号しない（Do Not Decrypt）] ルールのカテゴリの制限

必要に応じて、復号ポリシーにカテゴリを含めることができます。これらのカテゴリ（「URL フィルタリング」とも呼ばれる）は、Cisco Talos インテリジェンスグループによって更新されます。更新は、Web サイトの宛先から（場合によってはそのホスティングおよび登録情報から）取得可能な内容に従って、機械学習および人間の分析に基づいて行われます。分類は、宣言された会社の業種、意図、またはセキュリティに基づいて行われません。シスコでは、URL フィルタリングカテゴリの継続的な更新と改善に努めていますが、厳密に科学的なものではありません。一部の Web サイトはまったく分類されておらず、一部の Web サイトは不適切に分類されている可能性があります。

理由のないトラフィックの復号を避けるために、[復号しない（Do Not Decrypt）] ルールのカテゴリを過度に使用しないでください。たとえば、[健康と薬（Health and Medicine）] カテゴリには、患者のプライバシーを脅かさない WebMD の Web サイトが含まれています。

以下は、[健康と薬（Health and Medicine）] カテゴリの Web サイトの復号を防ぐ一方で、WebMD およびその他すべての復号を許可することができるサンプル復号ポリシーです。復号ルールに関する一般的な情報については、TLS/SSL 復号の使用上のガイドライン （3 ページ）を参照してください。



（注） URL フィルタリングとアプリケーション検出を混同しないでください。アプリケーション検出は、Web サイトからのパケットの一部を読み取り、それが何であるか（Facebook メッセージや Salesforce など）をより具体的に判断することに依存します。詳細については、アプリケーション制御の設定のベストプラクティスを参照してください。

# 復号ルールのブロックアクション

システムを通過させないトラフィックに対して次の復号ルールアクションが用意されています。

- [ブロック（Block）] では、接続が終了するため、クライアント ブラウザにエラーが表示されます。

  エラーメッセージには、ポリシーによってサイトがブロックされたことは示されません。代わりに、一般的な暗号化アルゴリズムがないと示される場合があります。このメッセージからは、故意に接続がブロックされたことは明らかになりません。

- [リセットしてブロック（Block with reset）] では、接続がリセットされるため、クライアント ブラウザにエラーが表示されます。

  このエラーでは、接続がリセットされたことはわかりますが、その理由はわかりません。

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ため、[ブロック（Block）] と [リセットしてブロック（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（Block）] または [リセットしてブロック（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（⚠）が表示されます。

# 復号ルールの復号アクション

**[復号 - 証明書の置き換え（Decrypt - Replace Cert）]**、**[復号 - 既知のキー（Decrypt - Known Key）]**、および **[復号 - 再署名（Decrypt - Resign）]** アクションは、暗号化トラフィックを復号します。復号されたトラフィックは、アクセス制御を使用して検査されます。アクセスコントロールルールは、復号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。ここではデータの確認に加えて、侵入、禁止ファイル、マルウェアを検出およびブロックできます。システムは、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。

信頼できる認証局（CA） からの証明書を使用してトラフィックを復号することをお勧めします。これにより、**Invalid Issuer** が接続イベント内の SSL 証明書ステータス列に表示されないようにします。

信頼できるオブジェクトを追加する方法の詳細については、信頼できる認証局オブジェクトを参照してください。

**関連項目**：TLS 1.3 復号のベストプラクティス

**関連トピック**

TLS 1.3 復号のベストプラクティス

# TLS/SSL ハードウェア アクセラレーションのモニター

次のトピックでは、TLS/SSL のステータスのモニター方法について説明します。

## 情報カウンタ

If a system under load is working well, you should see large counts for the following counters. Because there are 2 sides to the tracker process per connection, you can see these counters increase by 2 per connection. The PRIV_KEY_RECV and SECU_PARAM_RECV counters are the most important, and are highlighted. The CONTEXT_CREATED and CONTEXT_DESTROYED counters relate to the allocation of cryptographic chip memory.

```
> show counters
Protocol      Counter                          Value   Context
SSLENC        CONTEXT_CREATED                 258225   Summary
SSLENC        CONTEXT_DESTROYED               258225   Summary
TLS_TRK       OPEN_SERVER_SESSION             258225   Summary
TLS_TRK       OPEN_CLIENT_SESSION             258225   Summary
TLS_TRK       UPSTREAM_CLOSE                  516450   Summary
TLS_TRK       DOWNSTREAM_CLOSE                516450   Summary
TLS_TRK       FREE_SESSION                    516450   Summary
TLS_TRK       CACHE_FREE                      516450   Summary
TLS_TRK       PRIV_KEY_RECV                   258225   Summary
TLS_TRK       NO_KEY_ENABLE                   258225   Summary
TLS_TRK       SECU_PARAM_RECV                 516446   Summary
TLS_TRK       DECRYPTED_ALERT                 258222   Summary
TLS_TRK       DECRYPTED_APPLICATION         33568976   Summary
TLS_TRK       ALERT_RX_CNT                    258222   Summary
TLS_TRK       ALERT_RX_WARNING_ALERT          258222   Summary
TLS_TRK       ALERT_RX_CLOSE_NOTIFY           258222   Summary
TCP_PRX       OPEN_SESSION                    516450   Summary
TCP_PRX       FREE_SESSION                    516450   Summary
TCP_PRX       UPSTREAM_CLOSE                  516450   Summary
TCP_PRX       DOWNSTREAM_CLOSE                516450   Summary
TCP_PRX       FREE_CONN                       258222   Summary
TCP_PRX       SERVER_CLEAN_UP                 258222   Summary
TCP_PRX       CLIENT_CLEAN_UP                 258222   Summary
```

## アラート カウンタ

We implemented the following counters according to the TLS 1.2 specification. FATAL or BAD alerts could indicate issues; however, ALERT_RX_CLOSE_NOTIFY is normal.

For details, see RFC 5246 section 7.2.

```
TLS_TRK      ALERT_RX_CNT                                311   Summary
TLS_TRK      ALERT_TX_CNT                                  2   Summary
TLS_TRK      ALERT_TX_IN_HANDSHAKE_CNT                     2   Summary
TLS_TRK      ALERT_RX_IN_HANDSHAKE_CNT                     2   Summary
TLS_TRK      ALERT_RX_WARNING_ALERT                      308   Summary
TLS_TRK      ALERT_RX_FATAL_ALERT                          3   Summary
TLS_TRK      ALERT_TX_FATAL_ALERT                          2   Summary
TLS_TRK      ALERT_RX_CLOSE_NOTIFY                       308   Summary
TLS_TRK      ALERT_RX_BAD_RECORD_MAC                       2   Summary
TLS_TRK      ALERT_TX_BAD_RECORD_MAC                       2   Summary
TLS_TRK      ALERT_RX_BAD_CERTIFICATE                      1   Summary
```

# エラー カウンタ

These counters indicate system errors. These counts should be low on a healthy system. The BY_PASS counters indicate packets that have been passed directly to or from the inspection engine (Snort) process (which runs in software) without decryption. The following example lists some of the bad counters.

Counters with a value of 0 are not displayed. To view a complete list of counters, use the command **show counters description | include TLS_TRK**

```
> show counters
Protocol     Counter                          Value   Context
TCP_PRX      BYPASS_NOT_ENOUGH_MEM             2134   Summary
TLS_TRK      CLOSED_WITH_INBOUND_PACKET           2   Summary
TLS_TRK      ENC_FAIL                            82   Summary
TLS_TRK      DEC_FAIL                           211   Summary
TLS_TRK      DEC_CKE_FAIL                     43194   Summary
TLS_TRK      ENC_CB_FAIL                       4335   Summary
TLS_TRK      DEC_CB_FAIL                        909   Summary
TLS_TRK      DEC_CKE_CB_FAIL                    818   Summary
TLS_TRK      RECORD_PARSE_ERR                   123   Summary
TLS_TRK      IN_ERROR                         44948   Summary
TLS_TRK      ERROR_UPSTREAM_RECORD            43194   Summary
TLS_TRK      INVALID_CONTENT_TYPE               123   Summary
TLS_TRK      DOWNSTREAM_REC_CHK_ERROR           123   Summary
TLS_TRK      DECRYPT_FAIL                     43194   Summary
TLS_TRK      UPSTREAM_BY_PASS                   127   Summary
TLS_TRK      DOWNSTREAM_BY_PASS                 127   Summary
```

# 重大カウンタ

The fatal counters indicate serious errors. These counters should be at or near 0 on a healthy system. The following example lists the fatal counters.

```
> show counters
Protocol     Counter                          Value   Context
CRYPTO       RING_FULL                            1   Summary
CRYPTO       ACCELERATOR_CORE_TIMEOUT             1   Summary
CRYPTO       ACCELERATOR_RESET                    1   Summary
CRYPTO       RSA_PRIVATE_DECRYPT_FAILED           1   Summary
```

The RING_FULL counter is not a fatal counter, but indicates how often the system overloaded the cryptographic chip. The ACCELERATOR_RESET counter is the number of times the TLS 暗号化アクセラレーション process failed unexpectedly, which also causes the failure of pending operations, which

are the numbers you see in ACCELERATOR_CORE_TIMEOUT and RSA_PRIVATE_DECRYPT_FAILED.

If you have persistent problems, disable TLS 暗号化アクセラレーション ( or **config hwCrypto disable**) and work with Cisco TAC to resolve the issues.

（注） You can do additional troubleshooting using the **show snort tls-offload** and **debug snort tls-offload** commands. Use the **clear snort tls-offload** command to reset the counters displayed in the **show snort tls-offload** command to zero.

# 復号ルール のトラブルシューティング

次のトピックでは、復号ルール のトラブルシューティングの方法について説明します。

## TLS/SSL オーバーサブスクリプションについて

*TLS/SSL* オーバーサブスクリプションとは、管理対象デバイスが TLS/SSL トラフィックにより過負荷になっている状態です。すべての管理対象デバイスで TLS/SSL オーバーサブスクリプションが発生する可能性がありますが、TLS暗号化アクセラレーションをサポートする管理対象デバイスでのみ処理方法を設定できます。

TLS暗号化アクセラレーションが有効になっている管理対象デバイスがオーバーサブスクライブされた場合、管理対象デバイスによって受信されるパケットの扱いは、復号ポリシーの [復号不可のアクション（Undecryptable Actions）] の [ハンドシェイクエラー（Handshake Errors）] の設定に従います。

- デフォルト アクションを継承（Inherit default action）
- Do not decrypt
- Block
- Block with reset

復号ポリシー の [復号不可のアクション（Undecryptable Actions）] の [ハンドシェイクエラー（Handshake Errors）] の設定が [復号しない（Do Not decrypt）] で、関連付けられたアクセス コントロール ポリシーがトラフィックを検査するように設定されている場合は、インスペクションが行われます。復号は行われません。

### TLS/SSL オーバーサブスクリプションのトラブルシューティング

管理対象デバイスで TLS 暗号化アクセラレーションを有効にした場合は、接続イベントを表示して、デバイスに SSL オーバーサブスクリプションが発生しているかどうかを確認できます。接続イベント テーブル ビューに、少なくとも [SSLフローフラグ（SSL Flow Flags）] イベントを追加する必要があります。

### 始める前に

- [復号不可のアクション（Undecryptable Actions）] ページの [ハンドシェイクエラー（Handshake Error）] の設定を使用して、復号ポリシー を設定します。

  詳細については、復号できないトラフィックのデフォルト処理を設定するを参照してください。

- Secure Firewall Management Center と脅威防御管理ネットワーク管理ガイドの 復号ルール ルールでの復号可能な接続のロギングに関するセクションの説明に従い、SSL ルールのロギングを有効にします。

### 手順

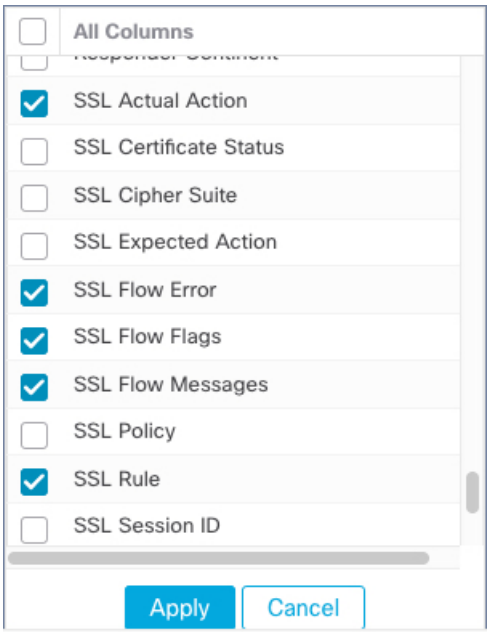
**ステップ 1** まだ Firewall Management Center にログインしていない場合は、ログインします。

**ステップ 2** **[分析（Analysis）] > [接続（Connection）] > [イベント（Events）]** の順にクリックします。

**ステップ 3** [接続イベントのテーブルビュー（Table View of Connection Events）] をクリックします。

**ステップ 4** 接続イベントテーブルの任意の列の [x] をクリックし、少なくとも [SSL Flow Flags] と [SSL Flow Messages] に追加の列を追加します。


次の例では、接続イベントのテーブル ビューに、[SSLの実際の動作（SSL Actual Action）]、[SSLフローエラー（SSL Flow Error）]、[SSLフローフラグ（SSL Flow Flags）]、[SSLフローメッセージ（SSL Flow Messages）]、[SSLポリシー（SSL Policy）]、および [SSLルール（SSL Rule）] 列を追加します。（ダイアログボックスの [無効になったカラム（Disabled Columns）] セクションで確認。）




カラムは、Cisco Secure Firewall Management Center アドミニストレーション ガイドの「*Connection and Security Intelligence Event Fields*」 で説明されている順序で追加されます。

**ステップ 5** [適用（Apply）] をクリックします。
TLS/SSL オーバーサブスクライブは、[SSL Flow Flags] 列の `ERROR_EVENT_TRIGGERED` および `OVER_SUBSCRIBED` の値で示されます。

**ステップ 6** TLS/SSL オーバーサブスクライブが発生している場合は、管理対象デバイスにログインして、次のコマンドのいずれかを入力します。

| コマンド（Command） | 結果 |
|---|---|
| **show counters** | **TCP_PRX BYPASS_NOT_ENOUGH_MEM** の値が大きい場合は、SSL トラフィックに対してより大きな容量を持つデバイスへのアップグレードを検討するか、または優先順位の低いトラフィックに [復号しない（Do Not Decrypt）] を使用します。 |
| **show snort tls-offload** | **BYPASS_NOT_ENOUGH_MEM** の値が大きい場合は、SSL トラフィックに対してより大きな容量を持つデバイスへのアップグレードを検討するか、または優先順位の低いトラフィックに [復号しない（Do Not Decrypt）] を使用します。 |

# TLS ハートビートについて

一部のアプリケーションでは、RFC6520 で定義されている Transport Layer Security（TLS）および Datagram Transport Layer Security（DTLS）プロトコルに対して、TLS ハートビート エクステンションが使用されます。TLS ハートビートは、接続がまだ有効であることを確認する方法を提供します。クライアントまたはサーバが指定されたバイト数のデータを送信し、応答を返すように相手に要求します。これが成功した場合は、暗号化されたデータが送信されます。

TLS 暗号化アクセラレーションが有効になっている管理対象デバイスは、TLS ハートビート エクステンションを使用するパケットを処理する場合、復号ポリシーの [復号不可のアクション（Undecryptable Actions）] の [復号エラー（Decryption Errors）] の設定で指定されているアクションを実行します。

- Block
- Block with reset

### 関連トピック

TLS ハートビートのトラブルシューティング （46 ページ）

# TLS ハートビートのトラブルシューティング

管理対象デバイスで TLS 暗号化アクセラレーションを有効にした場合は、接続イベントを表示して、デバイスが TLS ハートビート エクステンションを使用してトラフィックを監視しているかどうかを確認できます。接続イベント テーブル ビューに、少なくとも [SSLフローメッセージ（SSL Flow Messages）] イベントを追加する必要があります。

### 始める前に

SSL ハートビートは、接続イベント テーブル ビューの [SSLフローメッセージ（SSL Flow Messages）] 列の `HEARTBEAT` の値で示されます。ネットワーク内のアプリケーションが SSL ハートビートを使用しているかどうかを確認するには、最初に次のタスクを実行します。

- [復号できないアクション（Undecryptable Actions）] ページの [復号エラー（Decryption Error）] の設定で、復号ポリシー を設定します。

  詳細については、復号できないトラフィックのデフォルト処理を設定するを参照してください。

- Secure Firewall Management Center と脅威防御管理ネットワーク管理の説明に従って、SSL ルールのログを有効にします。

### 手順

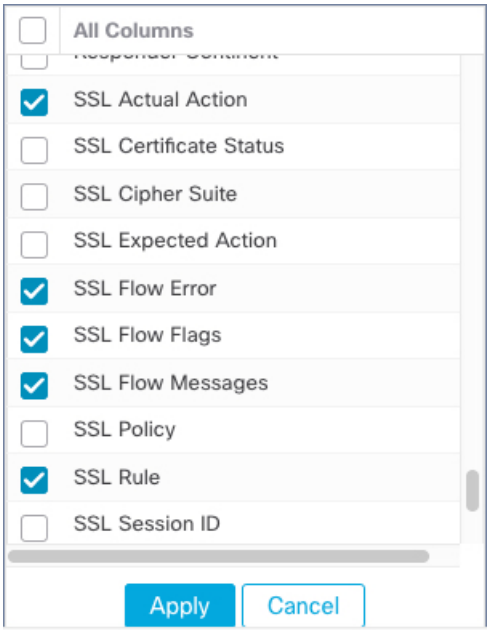
**ステップ 1** まだ Firewall Management Center にログインしていない場合は、ログインします。

**ステップ 2** **[分析（Analysis）] > [接続（Connection）] > [イベント（Events）]** をクリックします。

**ステップ 3** [接続イベントのテーブルビュー（Table View of Connection Events）] をクリックします。

**ステップ 4** 接続イベントテーブルの任意の列の [x] をクリックし、少なくとも [SSL Flow Flags] と [SSL Flow Messages] に追加の列を追加します。


次の例では、接続イベントのテーブル ビューに、[SSLの実際の動作（SSL Actual Action）]、[SSLフローエラー（SSL Flow Error）]、[SSLフローフラグ（SSL Flow Flags）]、[SSLフローメッセージ（SSL Flow Messages）]、[SSLポリシー（SSL Policy）]、および [SSLルール（SSL Rule）] 列を追加します。




カラムは、Cisco Secure Firewall Management Center アドミニストレーション ガイドの「*Connection and Security Intelligence Event Fields*」 で説明されている順序で追加されます。

**ステップ 5** [適用（Apply）] をクリックします。
TLS ハートビートは、[SSLフローメッセージ（SSL Flow Messages）] 列の `HEARTBEAT` の値で示されます。

**ステップ 6** ネットワーク上のアプリケーションで SSL ハートビートを使用する場合は、復号ルール の注意事項と制限事項 （2 ページ）を参照してください。

# TLS/SSL のピニングについて

一部のアプリケーションでは、アプリケーション自体に元のサーバー証明書のフィンガープリントを埋め込む、ピニングまたは証明書ピニングと呼ばれる技術が使用されます。*TLS/SSL* そのため、[復号 - 再署名（Decrypt - Resign）] アクションで 復号ルール を設定した場合は、アプ

リケーションが管理対象デバイスから再署名された証明書を受信すると、検証が失敗し、接続が中断されます。

TLS/SSL ピニングが行われていることを確認するには、Facebook などのモバイル アプリケーションへのログインを試みます。ネットワーク接続エラーが表示された場合は、Web ブラウザを使用してログインします。（たとえば、Facebook のモバイル アプリケーションにログインすることはできませんが、Safari または Chrome を使用して Facebook にログインすることはできます）。Firepower Management Center の接続イベントは、TLS/SSL ピニングのさらなる証明として使用できます

（注） TLS/SSL ピニングはモバイル アプリケーションに限定されません。

ネットワーク上のアプリケーションでSSL ピン留めを使用する場合は、TLS/SSL 証明書のピン留めのガイドライン （10 ページ）を参照してください。

**関連トピック**

TLS/SSL ピニングのトラブルシューティング （48 ページ）

## TLS/SSL ピニングのトラブルシューティング

デバイスで SSL ピニングが発生しているかどうかを確認するには、接続イベントを表示します。接続イベント テーブル ビューに、少なくとも [SSLフローフラグ（SSL Flow Flags）] と [SSLフローメッセージ（SSL Flow Messages）] 列を追加する必要があります。

### 始める前に

- Secure Firewall Management Center と脅威防御管理ネットワーク管理 ガイドの 復号ルールの復号可能な接続のログに関するセクションの説明に従い、復号ルールのログを有効にします。
- Facebook のようなモバイル アプリケーションにログインします。ネットワーク接続エラーが表示されたら、Chrome または Safari を使用して Facebook にログインします。Web ブラウザを使用してログインできても、ネイティブ アプリケーションではできない場合は、SSL ピニングが発生している可能性があります。

### 手順

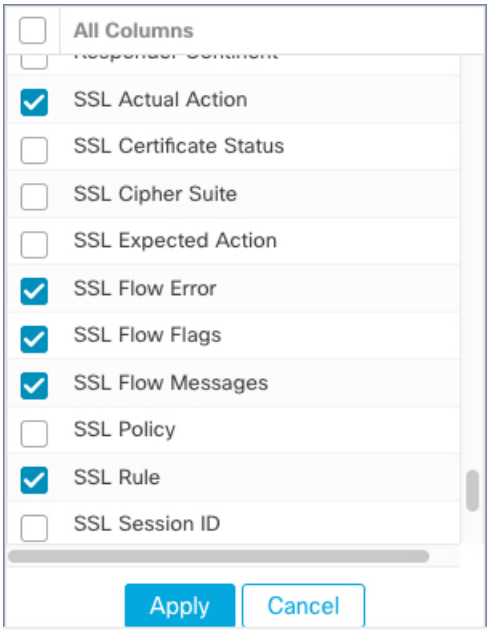
**ステップ 1** まだ Firewall Management Center にログインしていない場合は、ログインします。

**ステップ 2** **[分析（Analysis）] > [接続（Connection）] > [イベント（Events）]** の順にクリックします。

**ステップ 3** [接続イベントのテーブルビュー（Table View of Connection Events）] をクリックします。

**ステップ 4** 接続イベントテーブルの任意の列の [x] をクリックし、少なくとも [SSL Flow Flags] と [SSL Flow Messages] に追加の列を追加します。


次の例では、接続イベントのテーブル ビューに、[SSLの実際の動作（SSL Actual Action）]、[SSLフローエラー（SSL Flow Error）]、[SSLフローフラグ（SSL Flow Flags）]、[SSLフローメッセージ（SSL Flow Messages）]、[SSLポリシー（SSL Policy）]、および[SSLルール（SSL Rule）]列を追加します。




列は、Secure Firewall Management Center と脅威防御管理ネットワーク管理 ガイドの「Connection and Security Intelligence Event Fields」 セクションで説明されている順序で追加されます。

**ステップ 5** [適用（Apply）] をクリックします。

**ステップ 6** 次に SSL ピニングの動作を特定する方法について説明します。

**ステップ 7** ネットワーク内のアプリケーションでSSL ピニングが使用されていることを確認する場合は、復号ルール の注意事項と制限事項 （2 ページ）を参照してください。

### 次のタスク

TLS/SSL 接続イベントを使用して、次のいずれかが表示されれば、TLS/SSL ピニングの発生を確認できます。

- クライアントがサーバーから SERVER_HELLO、SERVER_CERTIFICATE、SERVER_HELLO_DONE メッセージを受信した後に TCP Reset を受信すると、SSL ALERT メッセージを送信するアプリケーションの場合、次のように表示されます。（パケットキャプチャを使用すると、アラート `Unknown CA (48)` が表示される場合があります）。

- [SSLフローフラグ（SSL Flow Flags）] 列に ALERT_SEEN は表示されますが、APP_DATA_C2S や APP_DATA_S2C は表示されません。
- 管理対象デバイスでSSLハードウェア アクセラレーションが有効になっている場合、[SSLフローメッセージ（SSL Flow Messages）] 列には通常、CLIENT_ALERT、CLIENT_HELLO、SERVER_HELLO、SERVER_CERTIFICATE、SERVER_KEY_EXCHANGE、SERVER_HELLO_DONE が表示されます。
- 管理対象デバイスで SSL ハードウェア アクセラレーションがサポートされていないか、ハードウェアアクセラレーション機能が無効になっている場合、[SSLフローメッセージ（SSL Flow Messages）] 列には通常、CLIENT_HELLO、SERVER_HELLO、SERVER_CERTIFICATE、SERVER_KEY_EXCHANGE、SERVER_HELLO_DONE が表示されます。
- [SSLフローエラー（SSL Flow Error）] 列には、Success が表示されます。

- SSL ハンドシェイク終了後にアラートではなく TCP Reset を送信するアプリケーションの場合は、次のように表示されます。
  - [SSLフローフラグ（SSL Flow Flags）] 列に ALERT_SEEN、APP_DATA_C2S、APP_DATA_S2C は表示されません。
  - 管理対象デバイスでSSLハードウェア アクセラレーションが有効になっている場合、[SSLフローメッセージ（SSL Flow Messages）] 列には通常、CLIENT_HELLO、SERVER_HELLO、SERVER_CERTIFICATE、SERVER_KEY_EXCHANGE、SERVER_HELLO_DONE、CLIENT_KEY_EXCHANGE、CLIENT_CHANGE_CIPHER_SPEC、CLIENT_FINISHED、SERVER_CHANGE_CIPHER_SPEC、SERVER_FINISHED が表示されます。
  - 管理対象デバイスで SSL ハードウェア アクセラレーションがサポートされていないか、ハードウェアアクセラレーション機能が無効になっている場合、[SSLフローメッセージ（SSL Flow Messages）] 列には通常、CLIENT_HELLO、SERVER_HELLO、SERVER_CERTIFICATE、SERVER_KEY_EXCHANGE、SERVER_HELLO_DONE、CLIENT_KEY_EXCHANGE、CLIENT_CHANGE_CIPHER_SPEC、CLIENT_FINISHED、SERVER_CHANGE_CIPHER_SPEC、SERVER_FINISHED が表示されます。
  - [SSLフローエラー（SSL Flow Error）] 列には、Success が表示されます。

**関連トピック**

不明または不正な証明書または認証局のトラブルシュート （50 ページ）

## 不明または不正な証明書または認証局のトラブルシュート

接続イベントを表示して、デバイスに不明な認証局、不正な証明書、または不明な証明書があるかどうかを判断できます。この手順は、TLS/SSL 証明書がピン留めされている場合にも使用できます。接続イベントテーブル ビューに、少なくとも [SSLフローフラグ（SSL Flow Flags）] と [SSLフローメッセージ（SSL Flow Messages）] 列を追加する必要があります。

### 始める前に

- 復号ルールを設定します。
- Secure Firewall Management Center と脅威防御管理ネットワーク管理 ガイドの 復号ルールの復号可能な接続のログに関するセクションの説明に従い、復号ルールのログを有効にします。

### 手順

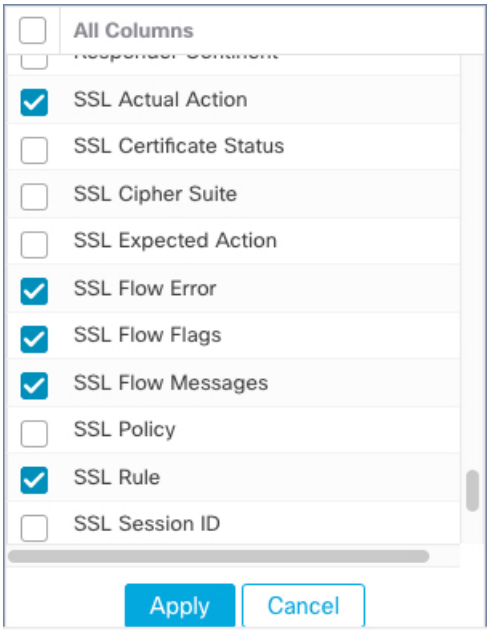
**ステップ 1** まだ Firewall Management Center にログインしていない場合は、ログインします。

**ステップ 2** **[分析（Analysis）] > [接続（Connection）] > [イベント（Events）]** の順にクリックします。

**ステップ 3** [接続イベントのテーブルビュー（Table View of Connection Events）] をクリックします。

**ステップ 4** 接続イベントテーブルの任意の列の [x] をクリックし、少なくとも [SSL Flow Flags] と [SSL Flow Messages] に追加の列を追加します。


次の例では、接続イベントのテーブル ビューに、[SSLの実際の動作（SSL Actual Action）]、[SSLフローエラー（SSL Flow Error）]、[SSLフローフラグ（SSL Flow Flags）]、[SSLフローメッセージ（SSL Flow Messages）]、[SSLポリシー（SSL Policy）]、および[SSLルール（SSL Rule）] 列を追加します。




列は、Secure Firewall Management Center と脅威防御管理ネットワーク管理 ガイドの「Connection and Security Intelligence Event Fields」 セクションで説明されている順序で追加されます。

**ステップ 5** [適用（Apply）] をクリックします。

**ステップ 6** 次の表は、証明書または認証局が不正か、または欠落しているかを判断する方法を説明しています。

| SSL フローフラグ | 意味 |
|---|---|
| CLIENT_ALERT_SEEN_UNKNOWN_CA | 有効な証明書チェーンまたは部分的なチェーンが SSL クライアントアプリケーションによって受信されましたが、CA 証明書が見つからなかったか、既知の信頼できる CA と一致しなかったため、証明書が受け入れられなかったことを示しています。このメッセージは、常に回復不能なエラーを示しています。 |
| CLIENT_ALERT_SEEN_BAD_CERTIFICATE | 証明書が破損しているか、正しく検証されていない署名が含まれているか、またはその他の問題がありました。 |
| CLIENT_ALERT_SEEN_CERTIFICATE_UNKNOWN | 証明書の処理中に他の（詳細不明の）問題が発生し、受け入れられなくなりました。 |

# TLS/SSL 暗号スイートの確認

### 始める前に

このトピックでは、暗号スイートの条件を持つ復号ルールを保存する際に次のエラーが表示された場合に実行する必要があるアクションについて説明します。

```
Traffic cannot match this rule; none of your selected cipher suites contain a signature
algorithm that matches the resigning CA's signature algorithm
```

このエラーは、復号ルールの条件として選択した 1 つ以上の暗号スイートが復号ルールに使用されている証明書と互換性がないことを示しています。この問題を解決するには、使用している証明書へのアクセス権が必要です。

（注） このトピックでのタスクには、TLS/SSL 暗号化がどのように機能するかの知識が必要です。

手順

**ステップ 1** 指定した暗号スイートで**[復号 - 再署名（Decrypt - Resign）]**、**[復号 - 証明書の置き換え（Decrypt - Replace Cert）]**、または **[復号 - 既知のキー（Known Key）]** のいずれかを持つ 復号ルール ルールを保存しようとすると、次のエラーが表示されます。

**例**：

```
Traffic cannot match this rule; none of your selected cipher suites contain a
signature algorithm that the resigning CA's signature algorithm
```

**ステップ 2** トラフィックの復号に使用している証明書を見つけ、必要に応じて、openssl コマンドを実行できるシステムにその総名所をコピーします。

**ステップ 3** 次のコマンドを実行し、証明書で使用されている署名アルゴリズムを表示します。

**openssl x509 -in** *CertificateName* **-text -noout**

出力の最初に次のような数行が表示されます。

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 4105 (0x1009)
    Signature Algorithm: ecdsa-with-SHA256
```

**ステップ 4** **Signature algorithm** によって次が通知されます。

- 使用されている暗号化関数（前の例では、**ECDSA** は楕円曲線デジタル署名アルゴリズム（楕円曲線 DSA）を意味します）。
- 暗号化されたメッセージのダイジェストの作成に使用されたハッシュ関数（前の例では **SHA256**）。

**ステップ 5** それらの値に一致する暗号スイーツのリソース（*OpenSSL at University of Utah* など）を検索します。暗号スイートは RFC 形式である必要があります。
また、その他のさまざまなサイト（Mozilla wiki の Server Side TLS や RFC 5246 の Appendix C など）も検索できます。マイクロソフトのドキュメントの Cipher Suites in TLS/SSL（Schannel SSP）[英語] には、暗号スイーツの詳細な説明があります。

**ステップ 6** 必要に応じて、OpenSSL 名を Firepower Management システムが使用している RFC 名に変換します。
`https://testssl.sh` サイトの『RFC mapping list』を参照してください。

**ステップ 7** 前の例の **ecdsa-with-SHA256** では、Mozilla wiki で『Modern Compatibility List』を参照できます。

a) 名前に **ECDSA** または **SHA-256** を持つ暗号スイートのみを選択します。これらの暗号スイートは次のように動作します。

```
ECDHE-ECDSA-AES128-GCM-SHA256
ECDHE-ECDSA-AES128-SHA256
```

b) 対応する RFC 暗号スイートを RFC マッピング リストで検索します。これらの暗号スイートは次のように動作します。

```
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
```

**ステップ 8** 前述の暗号スイートを復号ルールに追加します。

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。