CHAPTER 38

Cisco Common Classification Policy Language

Cisco Common Classification Policy Language（C3PL）は機能固有の設定コマンドの代わりに使用できる、構造化された言語です。C3PL を使用すると、イベント、条件、およびアクションに基づくトラフィック ポリシーを作成できます。Cisco Configuration Professional（Cisco CP）では、C3PL を使用してポリシー マップおよびクラス マップが作成されます。これについては、次の各トピックで説明しています。

ポリシー マップ

ポリシー マップでは、定義されている条件にトラフィックが一致した場合に実行されるアクションを指定します。各トラフィック タイプおよび条件は、ポリシー マップに関連付けられたクラス マップで定義します。ポリシー マップとそれに関連付けられたクラス マップの情報をルータで使用できるようにするには、ポリシー マップをゾーンペアに関連付ける必要があります。ゾーンおよびゾーン ペアの設定方法の詳細については、「ゾーンベースのポリシー ファイアウォール」を参照してください。

ポリシー マップ ウィンドウ

ポリシー マップ ウィンドウでは、QoS、HTTP、および他の種類のトラフィックに対するポリシー マップを確認、作成、および編集できます。ウィンドウ上部には設定済みのポリシー マップが一覧表示され、ウィンドウ下部には強調表示したポリシー マップの詳細が表示されます。ポリシー マップを編集する場合、または詳細情報を確認する場合は［編集］をクリックして、表示されたダイアログ ボックスで情報を確認し、必要な変更を加えます。

このヘルプ トピックでは、ポリシー マップ ウィンドウの全般的な説明、およびいくつかのサンプル データを示します。

追加

［追加］をクリックすると、ポリシー マップを設定できるダイアログ ボックスが表示されます。

編集

［編集］をクリックすると、選択したポリシー マップを編集できるダイアログ ボックスが表示されます。［編集］ボタンは、ポリシー マップが 1 つも設定されていない場合は無効にされています。

削除

選択したポリシー マップを削除するには、［削除］をクリックします。

ポリシー マップ リスト エリア

このエリアには、特定のプロトコルまたは機能に対して設定されたポリシー マップが一覧表示されます。ここでポリシー マップを選択すると、画面下部にその詳細情報が表示されます。次に、2 つの IM ポリシーの例を示します。

ポリシー マップ名	説明
im-pmap-g	guest policy
im-pmap-e	employee policy

ポリシー マップの詳細

選択したポリシー マップの詳細には、ポリシー マップの設定内容が表示されます。表示される詳細情報の内容は、ポリシー マップの種類によって異なります。

HTTP、IM、P2P、IMAP、および POP3 では、一致するクラス名、アクション、およびログのカラムが表示されます。次の表は、IM ポリシー マップの詳細を示しています。ルータでは、AOL トラフィックがブロックされますが、その他の種類の IM トラフィックはすべて許可されます。

一致するクラス名	アクション	ログ
aol-cmap	無効	無効
class-default	有効	無効

プロトコル インスペクション、SMTP、および SUNRPC ポリシー マップの詳細には、［一致するクラス名］カラムおよび［アクション］カラムが表示されます。次の表は、SUNRPC ポリシー マップの詳細を示しています。

一致するクラス名	アクション
cmap-sunrpc1	許可
cmap-sunrpc2	なし

QoS ポリシー マップの追加 / 編集

QoS ポリシー マップの追加または編集時には、次の情報を使用します。

ポリシー名および説明

新規ポリシー マップを作成する場合は、これらのフィールドにポリシー マップの名前と説明を入力します。ポリシー マップを編集する場合は、これらのフィールドは表示専用です。

クラス マップ、キューイング、DSCP の設定、および廃棄

これらのカラムには、ポリシー マップ内の各クラス マップについての概要が表示されます。次に、音声クラス マップのエントリの例を示します。

```
Voice-FastEthernet0/1  LLQ 70%     ef          No
```

このクラス マップでは、低遅延キューイングを使用し、このインターフェイスの帯域幅の 70% を使用しています。DSCP 値は ef に設定されており、このタイプのパケットは廃棄されません。

このリストのクラス マップ情報を変更するには、［追加］、［編集］、［削除］、［上へ移動］、および［下へ移動］の各ボタンをクリックします。

インターフェイスへのポリシー マップ関連付け

この画面では、ポリシー マップを選択したインターフェイスに関連付けます。

フィールド リファレンス

表 38-1　ポリシー マップへの関連付けのフィールド

項目	説明
ポリシー マップ	インターフェイスに関連付けるポリシー マップを選択します。
ポリシー マップの詳細	
クラス マップ	［クラス マップ］カラムには、そのポリシー マップに含まれているクラス マップが表示されます。

表 38-1　ポリシー マップへの関連付けのフィールド（続き）

項目	説明

キューイング	［キューイング］カラムには、クラス マップで使用されるキューイングのタイプ、およびこのクラスに割り当てられた帯域幅のパーセント値が表示されます。たとえば、［キューイング］カラムには、次のようなエントリが表示されます。
	
	`LLQ - 33%`
	`CBWFQ - 5%`
	`CBWFQ - 5% Remaining`
	`Fair Queue`
	
	1 つのクラス マップで低遅延キューイング（LLQ）、2 つのクラス マップで Class-Based Weighted Fair Queuing（CBWFQ）、もう 1 つのクラス マップでフェア キューイングが使用されています。パーセント値は、これらの各クラス マップに割り当てられた帯域幅、または残りの帯域幅を示します。

シェーピング	［シェーピング］カラムでは、クラス マップでシェーピングが設定されているかどうかが示されます。 • ［はい］— シェーピングが設定されている。 • ［いいえ］— シェーピングが設定されていない。
ポリシング	［ポリシング］カラムでは、クラス マップでポリシングが設定されているかどうかが示されます。 • ［はい］— ポリシングが設定されている。 • ［いいえ］— ポリシングが設定されていない。
DSCP の設定	［DSCP の設定］カラムには、クラス マップで使用されている DSCP マーキングが一覧表示されます。
廃棄	

インスペクション ポリシー マップの追加

インスペクション ポリシー マップでは、関連付けられたクラス マップの条件と一致したトラフィックに対してルータが実行するアクションを指定します。ルータが実行できるアクションは、トラフィックの通過の許可、トラフィックの廃棄（およびオプションでイベントのログ記録）、またはトラフィックの検査です。

入力した名前と説明は、ポリシー マップの確認ウィンドウに表示されます。［クラス マップ］および［アクション］カラムには、このポリシー マップに関連付けられたクラス マップ、およびクラス マップで指定されたトラフィックに対してルータが実行するアクションがそれぞれ表示されます。リストに新規クラス マップを追加してアクションを設定するには、［追加］をクリックします。クラス マップの設定を変更するには、［編集］をクリックします。クラス マップの評価順序を変更するには、［上へ移動］および［下へ移動］ボタンをクリックします。

レイヤ 7 ポリシー マップ

このウィンドウでは、選択したアプリケーションの検査に使用するレイヤ 7 ポリシー マップを選択できます。このウィンドウには、選択したアプリケーションに対して使用可能なポリシー マップが一覧表示されます。ポリシー マップを選択して、［OK］をクリックします。

アプリケーションのインスペクション

アプリケーション インスペクション ポリシーは、Open Systems Interconnect（OSI）モデルのレイヤ 7 に適用されます。このレイヤでは、アプリケーションによる便利な機能の提供を許可するメッセージがユーザ アプリケーション間で送受信されます。アプリケーションによっては、不要な機能や脆弱な機能を提供するものがあります。したがって、このような機能に関連付けられたメッセージは適切にフィルタリングし、アプリケーション サービスに対する動作を制限する必要があります。

Cisco IOS ソフトウェアのゾーンポリシー ファイアウォールでは、HTTP、SMTP、POP3、IMAP、SUNRPC、P2P、および IMAP アプリケーション サービスに対するアプリケーション インスペクションおよび制御を実行できます。詳細については、次のリンクを参照してください。

- HTTP インスペクション クラス マップの追加
- SMTP クラス マップの追加 / 編集
- POP3 クラス マップの追加 / 編集
- IMAP クラス マップの追加 / 編集
- SUNRPC クラス マップの追加 / 編集

- ポイントツーポイント クラス マップの追加 / 編集
- インスタント メッセージング クラス マップの追加 / 編集

詳細パケット インスペクションの設定

レイヤ 7（アプリケーション）インスペクションは、サービス固有のアクション（選択されたファイル検索、ファイル転送、およびテキスト チャット機能のブロックまたは許可など）を認識および適用する機能によって、レイヤ 4 インスペクションを強化します。サービス固有の機能は、サービスによって異なります。

新規ポリシー マップを作成する場合は、[ポリシー マップ名] フィールドに名前を入力します。説明を追加することもできます。新規のポイントツーポイント クラス マップを作成するには、[追加] > [新しいクラス マップ] の順にクリックします。このタイプのクラス マップの作成方法については、「ポイントツーポイント クラス マップの追加 / 編集」を参照してください。デフォルトのクラス マップを追加するには、[追加] > [クラスのデフォルト] の順にクリックします。

表にクラス マップが表示されたら、一致トラフィックが検出された場合に実行するアクション、および一致内容をログに記録するかどうかを指定します。[<なし>]、[リセット]、または [許可] を指定できます。次の例は、Gnutella および eDonkey の P2P クラス マップを示しています。

一致するクラス名	アクション	ログ
gnutellaCMap	許可	
eDonkeyCMap	リセット	X

クラス マップ

クラス マップでは、ゾーンポリシー ベース ファイアウォール（ZPF）によってポリシーの適用対象として選択されるトラフィックを定義します。レイヤ 4 クラス マップでは、次の条件に基づいてトラフィックが分類されます。

- アクセス グループ — 標準、拡張、または名前付きのアクセス コントロール リストを使用して、送信元と宛先の IP アドレス、および送信元と宛先のポートを基準にしてトラフィックをフィルタ処理できます。
- プロトコル — レイヤ 4 プロトコル（TCP、UDP、および ICMP）およびアプリケーション サービス（HTTP、SMTP、DNS など）が基準になります。一般に認知されたサービス、または PAM で認識可能なユーザ定義サービスはすべて指定できます。
- クラス マップ — 追加の一致条件を指定する下位のクラス マップを、別のクラス マップ内にネストできます。

クラス マップには、「いずれかと一致」または「すべてに一致」演算子を適用して、一致条件の適用方法を定義できます。「いずれかと一致」を指定した場合は、トラフィックが、クラス マップ内のいずれか 1 つの一致条件だけを満たす必要があります。「すべてに一致」を指定した場合は、クラス マップのすべての条件を満たすトラフィックだけが、この特定のクラスに属するものとみなされます。

クラス マップの関連付け

クラス マップをインスペクション ポリシー マップに関連付けるには、次の操作を行います。

ステップ 1　クラス　マップ名を指定します。そのためには、名前のフィールドの右側にあるボタンをクリックし、［クラス マップの追加］、［クラス マップの選択］、または class-default を選択します。

ステップ 2　［アクション］ボックスで［通過］、［廃棄］、または［検査］をクリックします。［廃棄］をクリックした場合は、オプションで［ログ］をクリックすると、廃棄イベントをログに記録できます。［検査］をクリックした場合は、［詳細オプション］をクリックして、このクラスのトラフィックに対するパラメータ マップ、インスペクション ポリシー、またはポリシングを指定します。

ステップ 3　［OK］をクリックしてこのダイアログ ボックスを閉じ、インスペクション ポリシー マップの追加または修正ダイアログ ボックスに戻ります。

クラス マップの詳細オプション

トラフィックに対して［検査］アクションを選択した場合は、パラメータ マップ、アプリケーション インスペクション、および ZPF ポリシングを指定できます。

インスペクション パラメータ マップ

インスペクション パラメータ マップでは、TCP、DNS、および UDP のタイムアウトおよびセッション制御に関する各パラメータを指定します。既存のパラメータ マップを選択できます。設定済みのパラメータ マップが存在しない場合は、このフィールドは無効になります。［表示］をクリックすると、このダイアログ ボックスを終了せずに、選択したパラメータ マップを表示できます。

URL フィルタリング パラメータ マップ

URL フィルタリング パラメータ マップを使用すると、URL フィルタリング サーバおよびローカル URL リストを指定できます。既存のパラメータ マップを選択できます。設定済みのパラメータ マップが存在しない場合は、このフィールドは無効になります。［表示］をクリックすると、このダイアログ ボックスを終了せずに、選択したパラメータ マップを表示できます。

アプリケーション インスペクションの有効化

アプリケーション インスペクション ポリシーでは、指定のアプリケーションのパケットから検査するデータ タイプを指定します。既存のアプリケーション インスペクション ポリシーを選択できます。設定済みのアプリケーション インスペクション ポリシーが存在しない場合は、このフィールドは無効になります。［表示］をクリックすると、このダイアログ ボックスを終了せずに、選択したアプリケーション インスペクション ポリシーを表示できます。

ポリシング レートおよびバースト

トラフィックを指定のポリシング レートに限定して、バースト値を指定できます。ポリシング レートには毎秒 8,000 ～ 2,000,000,000 ビットの範囲の値を指定できます。バースト レートには 1,000 ～ 512,000,000 バイトの範囲の値を指定できます。

QoS クラス マップ

このウィンドウでは、QoS クラス マップの情報を表示および編集できます。QoS クラス マップは、QoS ポリシー マップ内でトラフィック タイプを定義するために使用されます。

クラス マップ名をクリックすると、［クラス マップの詳細］エリアにこのクラス マップの詳細情報が表示されます。

クラス マップ詳細情報では、トラフィックを定義するための一致条件となるプロトコルを確認できます。次の例は、音声シグナリング クラス マップの詳細を示しています。

```
Details of Class Map:SDMSignal-FastEthernet0/1

    Item Name                          Item Value
Match Protocols                        h323,rtcp
```

H.323 および RTCP は、一致条件となる音声シグナリング プロトコルです。

QoS クラス マップの追加 / 編集

次の情報は、QoS クラス マップの追加または編集時に役立ちます。新規の QoS クラス マップを追加する場合は、このフィールドの右側のボタンをクリックし、コンテキスト メニューから［クラス マップの追加］または［クラス マップの選択］を選択します。

［廃棄］、［DSCP の設定］、および［キューイング］のオプションについては、「アクション」を参照してください。

QoS クラス マップの追加 / 編集

作成する QoS クラス マップには、識別および使用しやすいように、名前と説明を入力します。［分類］ボックスの［任意］、［すべて］、［編集］の各ボタンの説明については、［分類］を参照してください。

クラス マップの選択

選択するクラス マップ名をクリックして、［OK］をクリックします。このダイアログ ボックスを起動したウィンドウに、このクラス マップ エントリが追加されます。

詳細インスペクション

詳細インスペクションを使用すると、アプリケーション固有のパラメータに対するクラス マップを作成できます。たとえば、eDonkey、Gnutella、Kazaa2 などの一般的な P2P アプリケーションに対するクラス マップを作成できます。

クラス マップおよびアプリケーション サービス グループ ウィンドウ

クラス マップ ウィンドウでは、HTTP、SMTP、POP3 などのプロトコルに対するクラス マップの確認、作成、および編集が可能です。ウィンドウの［クラス マップ］エリアには設定済みのクラス マップの一覧が、ウィンドウ下部には選択したクラス マップの詳細情報がそれぞれ表示されます。クラス マップを編集する場合、または詳細情報を参照する場合は、［編集］をクリックして、表示されたダイアログ ボックスで情報を確認し、必要な変更を加えます。

追加

［追加］をクリックすると、選択したタイプのクラス マップを新規作成し、設定内容を入力するためのダイアログ ボックスが表示されます。

編集

［編集］をクリックすると、選択したクラス マップの設定内容を変更できます。

削除

選択したクラス マップを削除するには［削除］をクリックします。他のクラス マップで使用される可能性がある下位クラス マップやパラメータ マップなどの依存関係がこの設定に関連付けられている場合、Cisco CP に追加のダイアログボックスが表示される場合があります。

クラス マップ エリア

このエリアには、選択したプロトコルに対して設定されたクラス マップが表示されます。ここには設定されたクラス マップの名前、および他の関連情報が表示されます。

QoS クラス マップ

QoS クラス マップ情報は、［クラス マップ名］および［説明］カラムから成る表形式で表示されます。次に、この表の例を示します。

クラス マップ名	説明
CMAP-DMZ	FTP および HTTP QoS クラス マップ
CMAP-3	テスト

インスペクション、HTTP、SMTP、SUN RPC、IMAP、および POP3 クラス マップ

これらのタイプのクラス マップ情報は、［クラス マップ名］および［使用元］カラムから成る表形式で表示されます。次に、HTTP クラス マップの表の例を示します。

クラス マップ名	使用元
http-rqst	pmap-5
http-rsp-body	pmap-5

インスタント メッセージング サービス グループおよびピアツーピア アプリケーション サービス グループ

インスタント メッセージング サービス グループおよびピアツーピア（P2P）アプリケーション サービス グループでは、Yahoo! Messenger インスタント メッセージング アプリケーションや Gnutella P2P アプリケーションなどの個別のアプリケーションに対するクラス マップが設定されるため、カラムが追加されます。次の表は、P2P アプリケーション サービス グループのデータの例を示しています。

クラス マップ名	使用元	クラス マップ タイプ
cmap-gnutella	pmap-7	Gnutella
cmap-edonkey	pmap-7	eDonkey
cmap-bittorrent	pmap-7	bittorrent

クラス マップの詳細

［クラス マップの詳細］エリアには、特定のクラス マップの設定内容が表示されます。このエリアは、［項目名］および［項目値］カラムから構成されます。

項目名

設定する項目名です。たとえば、HTTP クラス マップでは、［要求のヘッダー］、［ポートの誤使用］、［プロトコル違反］などを設定できます。

項目値

各設定項目の値です。たとえば、HTTP の［要求のヘッダー］に「Length > 500」という値を設定し、［ポートの誤使用］フラグを無効にすることができます。

クラス マップ詳細の追加情報

これらのウィンドウに表示されるクラス マップの詳細情報については、次の該当リンクをクリックしてください。

- QoS クラス マップの追加 / 編集
- インスペクション クラス マップの追加 / 編集

- HTTP インスペクション クラス マップの追加
- インスタント メッセージング クラス マップの追加 / 編集
- ポイントツーポイント クラス マップの追加 / 編集
- SMTP クラス マップの追加 / 編集
- SUNRPC クラス マップの追加 / 編集
- IMAP クラス マップの追加 / 編集
- POP3 クラス マップの追加 / 編集

インスペクション クラス マップの追加 / 編集

インスペクション クラス マップを作成すると、さまざまな種類のトラフィックをインスペクションに使用できます。［クラス名］フィールドには、このクラス マップを識別する名前を入力します。説明を入力することもできます。クラス マップの編集時には、名前を変更することはできません。クラスにマッピングする条件を指定したら、［OK］をクリックします。

クラスを任意の条件と一致させるか、またはすべての条件と一致させるかの指定

クラスが選択した条件のうちのいずれか 1 つ以上と一致する必要がある場合は、［任意］をクリックします。クラスがすべての条件と一致する必要がある場合は、［すべて］をクリックします。

インスペクション クラス マップの一致条件の選択

左側のカラムには、クラス マップの一致条件が表示されます。ノードの隣のプラス記号（+）をクリックすると、子ノードが表示されます。たとえば、［HTTP］をクリックすると、子ノード［http］および［https］が表示されます。項目を選択するには、必要な項目をクリックしてから［追加 >>］をクリックします。右側のカラムに追加した項目を削除するには、必要な項目をクリックしてから［<< 削除］をクリックします。

一致順序の変更

いずれかの条件との一致を必要とする［任意］を選択した場合は、右側のカラムに表示される各項目の一致順序を変更できます。項目をリスト内で 1 つ上に移動するには、対象の項目を選択して［上へ移動］をクリックします。項目をリスト内で 1 つ下に移動するには、対象の項目を選択して［下へ移動］をクリックします。リストの最上部にある項目をックリックした場合、［上へ移動］ボタンは無効になります。リストの最下部にある項目をクリックした場合、［下へ移動］ボタンは無効になります。

パラメータ マップの関連付け

このダイアログ ボックスには、クラス マップに関連付けることのできるパラメータ マップが表示されます。クラス マップに関連付けるパラメータ マップの隣にある［選択］チェック ボックスを選択してください。

HTTP インスペクション クラス マップの追加

HTTP インスペクション クラス マップを使用すると、さまざまな種類の HTTP リクエスト、レスポンス、およびリクエストレスポンス データをインスペクションに使用できます。

HTTP インスペクション クラス マップを作成するには、次の手順に従います。

ステップ 1　クラス マップを識別するクラス名を入力します。［HTTP クラス マップ］ウィンドウに表示される説明を入力することもできます。

ステップ 2　HTTP ツリーで、インスペクションに使用するデータ タイプが存在するブランチをクリックします。HTTP リクエスト、レスポンス、およびリクエストレスポンスに対するクラス マップを作成できます。

ステップ 3　適切なサブブランチをクリックし、必要なデータ　タイプの詳細情報を指定します。

ステップ 4　表示されるフィールドで、クラス マップ データを設定します。

ステップ 5　一致条件を指定します。クラス マップがいずれか 1 つ以上の条件と一致する必要がある場合は、[次のいずれかの状態] をクリックします。クラス マップが指定したすべての条件と一致する必要がある場合は、[以下に指定するものすべて] をクリックします。

HTTP リクエスト ヘッダー

HTTP リクエスト ヘッダー属性に対するクラス マップ条件を入力します。

次の値を超える長さ

1 つのパケットにおける、グローバル リクエスト ヘッダー長の上限を指定するには、このチェック ボックスを選択して、必要なバイト数を入力します。

次の値を超えるカウント

1 つのパケットにおける、リクエスト ヘッダー フィールドの合計数の上限を指定するには、このチェック ボックスを選択して、必要なフィールド数を入力します。

正規表現

照合する正規表現を指定する場合は、このチェック ボックスを選択します。検査対象の文字列と一致する既存の正規表現クラス マップを選択するか、新規作成します。正規表現の作成の詳細については、「正規表現の追加 / 編集」を参照してください。このダイアログ ボックスを閉じないで既存のマップを確認するには、[既存のマップの選択] リストでマップを選択して [表示] をクリックします。

フィールド名および設定オプション

ヘッダー内のフィールドをインスペクションの条件に含めて、検査する長さ、フィールド数、および文字列を指定できます。フィールドを含めるには、[追加] をクリックして、表示されるダイアログ ボックスに必要な条件を入力します。

HTTP リクエスト ヘッダー フィールド

リストからヘッダー フィールドのタイプを選択し、これに対するインスペクション条件を指定します。

次の値を超える長さ

このフィールドの長さの上限を指定するには、このチェック ボックスを選択して、必要なバイト数を入力します。たとえば、cookie フィールドが 256 バイトを超えるリクエストをブロックしたり、user-agent フィールドが 128 バイトを超えるリクエストをブロックしたりできます。

次の値を超えるカウント

ヘッダー内でこのフィールドが繰り返される回数の上限を指定するには、このチェック ボックスを選択して、必要な数値を入力します。たとえば、1 という値を入力すると、content-length ヘッダー行が複数含まれるリクエストをブロックできます。この例は、セッションのスマグリングを阻止するための効果的な手段を示しています。

正規表現

照合する正規表現を指定する場合は、このチェック ボックスを選択します。検査対象の文字列と一致する既存の正規表現クラス マップを選択するか、新規作成します。正規表現の作成の詳細については、「正規表現の追加 / 編集」を参照してください。このダイアログ ボックスを閉じないで既存のマップを確認するには、［既存のマップの選択］リストでマップを選択して［表示］をクリックします。

一致フィールド

クラス マップが選択したフィールド タイプと一致しているかどうかを調べる場合は、このチェック ボックスを選択します。

このダイアログ ボックスのその他のフィールド

選択した HTTP ヘッダー フィールドによっては、このダイアログ ボックスにその他のフィールドが表示されることがあります。それらのフィールドでは、その他の基準を指定できます。たとえば、content-type フィールドを選択した場合は、リクエストとレスポンス間のコンテンツ タイプの不一致、未知のコンテンツ タイプ、および特定のコンテンツ タイプに対するプロトコル違反を検査できます。transfer-encoding フィールドを選択した場合は、さまざまなタイプの圧縮およびエンコーディングを検査できます。

HTTP リクエスト ボディ

HTTP リクエスト ボディの長さと文字列を検査できます。

長さ

リクエスト ボディの長さの上限を指定するには、このチェック ボックスを選択して、[より大きい (>)] を選択します。下限を指定するには [より小さい (<)] を選択します。

正規表現

文字列を検査するには、このチェック ボックスを選択します。検査対象の文字列と照合する既存の正規表現クラス マップを選択するか、新規作成します。正規表現の作成方法の詳細については、「正規表現の追加 / 編集」を参照してください。このダイアログ ボックスを終了しないで既存のマップを確認するには、[既存マップの選択] リストから必要なマップを選択し、[表示] をクリックします。

HTTP リクエスト ヘッダーの引数

リクエストで送信された引数の長さ、および設定した正規表現と一致する文字列を検査できます。

次の値を超える長さ

リクエスト ヘッダー引数の合計長の上限となるバイト数を指定するには、このチェック ボックスを選択します。

正規表現

照合する正規表現を指定する場合は、このチェック ボックスを選択します。検査する文字列と一致させる既存の正規表現クラス マップを選択するか、またはクラス マップを新たに作成します。正規表現の作成方法の詳細については、「正規表現の追加 / 編集」を参照してください。このダイアログ ボックスを終了しないで既存のマップを確認するには、［既存マップの選択］リストから必要なマップを選択し、［表示］をクリックします。

HTTP メソッド

HTTP メソッドでは、HTTP リクエストの目的を指定します。検査対象の HTTP メソッドを［メソッド リスト］カラムから選択し、メソッドの隣の［選択］チェック ボックスを選択します。

リクエスト ポートの誤使用

IM、P2P、トンネリング、およびその他のアプリケーションでは、HTTP ポート #80 が使用される場合があります。検査対象のポートの誤使用タイプを選択します。あらゆるタイプのポートの誤使用、IM アプリケーションによるポートの誤使用、P2P アプリケーション ポートの誤使用、およびトンネリング アプリケーションによるポートの誤使用を検査できます。

リクエスト URI

クラス マップに含める Universal Resource Identifier（URI）条件を入力します。

次の値を超える長さ

1 つのパケットにおける、URI の長さの上限を指定するには、このチェック ボックスを選択し、必要なバイト数を入力します。

正規表現

照合する正規表現を指定する場合は、このチェック ボックスを選択します。検査する文字列と一致させる既存の正規表現クラス マップを選択するか、またはクラス マップを新たに作成します。正規表現の作成方法の詳細については、「正規表現の追加 / 編集」を参照してください。このダイアログ ボックスを終了しないで既存のマップを確認するには、［既存マップの選択］リストから必要なマップを選択し、［表示］をクリックします。

使用例

次のいずれかの正規表現と URI が一致するリクエストをブロックする HTTP クラス マップを設定します。

"*cmd.exe"

".*sex"

".*gambling"

レスポンス ヘッダー

クラス マップに含める HTTP レスポンス ヘッダーの条件を入力します。

次の値を超える長さ

1 つのパケットにおける、グローバル レスポンス ヘッダー長の上限を指定するには、このチェック ボックスを選択して、必要なバイト数を入力します。

次の値を超えるカウント

1 つのパケットにおける、レスポンス ヘッダー フィールドの合計数の上限を指定するには、このチェック ボックスを選択して、必要なフィールド数を入力します。

正規表現

照合する正規表現を指定する場合は、このチェック ボックスを選択します。検査する文字列と一致させる既存の正規表現クラス マップを選択するか、またはクラス マップを新たに作成します。正規表現の作成方法の詳細については、「正規表現の追加 / 編集」を参照してください。このダイアログ ボックスを終了しないで既存のマップを確認するには、［既存マップの選択］リストから必要なマップを選択し、［表示］をクリックします。

レスポンス ヘッダーのフィールド

リストからヘッダー フィールドのタイプを選択し、これに対するインスペクション条件を指定します。

次の値を超える長さ

1 つのパケットにおける、フィールドの長さの上限を指定するには、このチェック ボックスを選択し、必要なバイト数を入力します。

次の値を超えるカウント

1 つのパケットにおける、このタイプのフィールドの合計数の上限を指定するには、このチェック ボックスを選択して、必要なフィールド数を入力します。

正規表現

照合する正規表現を指定する場合は、このチェック ボックスを選択します。検査する文字列と一致させる既存の正規表現クラス マップを選択するか、またはクラス マップを新たに作成します。正規表現の作成方法の詳細については、「正規表現の追加 / 編集」を参照してください。このダイアログ ボックスを終了しないで既存のマップを確認するには、［既存マップの選択］リストから必要なマップを選択し、［表示］をクリックします。

このダイアログ ボックスのその他のフィールド

選択した HTTP ヘッダー フィールドによっては、このダイアログ ボックスにその他のフィールドが表示されることがあります。それらのフィールドでは、その他の基準を指定できます。たとえば、**content-type** フィールドを選択した場合は、リクエストとレスポンス間のコンテンツ タイプの不一致、未知のコンテンツ タイプ、および特定のコンテンツ タイプのプロトコル違反を検査できます。**transfer-encoding** フィールドを選択した場合は、さまざまなタイプの圧縮およびエンコーディングを検査できます。

一致フィールド

クラス マップが選択したフィールド タイプと一致しているかどうかを調べる場合は、このチェック ボックスを選択します。

HTTP レスポンス ボディ

検査する HTTP レスポンス ボディの条件を指定します。

HTTP レスポンスの Java アプレット

HTTP レスポンスの Java アプレットを検査する場合は、このチェック ボックスを選択します。

長さ

レスポンス ボディの長さの上限を指定するには、このチェック ボックスを選択して、［より大きい（>)］演算子を選択します。下限を指定するには［より小さい（<)］を選択します。

正規表現

照合する正規表現を指定する場合は、このチェック ボックスを選択します。検査する文字列と一致させる既存の正規表現クラス マップを選択するか、またはクラス マップを新たに作成します。正規表現の作成方法の詳細については、「正規表現の追加 / 編集」を参照してください。このダイアログ ボックスを終了しないで既存のマップを確認するには、［既存マップの選択］リストから必要なマップを選択し、［表示］をクリックします。

HTTP レスポンスのステータス行

レスポンスのステータス行を検査するには、このチェック ボックスを選択して、照合する正規表現を指定します。検査する文字列と一致させる既存の正規表現クラス マップを選択するか、またはクラス マップを新たに作成します。

使用例

禁止されたページへのアクセスが試行されるたびにアラームがログに記録されるように、ルータを設定します。禁止されたページには通常、ステータス コード 403、および "HTTP/1.0 403 page forbidden\r\n" のようなステータス行が含まれます。

この場合の正規表現は次のようになります。

```
[Hh][Tt][Tt][Pp][/][0-9][.][0-9][ \t]+403
```

HTTP クラス マップが関連付けられるポリシー マップに、ロギングを指定します。

正規表現の作成方法の詳細については、「正規表現の追加 / 編集」を参照してください。このダイアログ ボックスを終了しないで既存のマップを確認するには、［既存マップの選択］リストから必要なマップを選択し、［表示］をクリックします。

リクエスト / レスポンス ヘッダーの条件

HTTP リクエスト / レスポンス ヘッダーに対するクラス マップ条件を入力します。

次の値を超える長さ

1 つのパケットにおける、グローバル リクエスト / レスポンス ヘッダー長の上限を指定するには、このチェック ボックスを選択して、必要なバイト数を入力します。

次の値を超えるカウント

1 つのパケットにおける、リクエスト / レスポンス ヘッダー フィールドの合計数の上限を指定するには、このチェック ボックスを選択して、必要なフィールド数を入力します。

正規表現

照合する正規表現を指定する場合は、このチェック ボックスを選択します。検査する文字列と一致させる既存の正規表現クラス マップを選択するか、またはクラス マップを新たに作成します。正規表現の作成方法の詳細については、「正規表現の追加 / 編集」を参照してください。このダイアログ ボックスを終了しないで既存のマップを確認するには、［既存マップの選択］リストから必要なマップを選択し、［表示］をクリックします。

HTTP リクエスト / レスポンス ヘッダー フィールド

クラス マップに含める HTTP リクエスト / レスポンスヘッダー フィールドを選択します。

次の値を超える長さ

1 つのパケットにおける、フィールドの長さの上限を指定するには、このチェック ボックスを選択し、必要なバイト数を入力します。

次の値を超えるカウント

1 つのパケットにおける、このタイプのフィールドの合計数の上限を指定するには、このチェック ボックスを選択して、必要なフィールド数を入力します。

正規表現

照合する正規表現を指定する場合は、このチェック ボックスを選択します。検査する文字列と一致させる既存の正規表現クラス マップを選択するか、またはクラス マップを新たに作成します。正規表現の作成方法の詳細については、「正規表現の追加 / 編集」を参照してください。このダイアログ ボックスを終了しないで既存のマップを確認するには、［既存マップの選択］リストから必要なマップを選択し、［表示］をクリックします。

このダイアログ ボックスのその他のフィールド

選択した HTTP ヘッダー フィールドによっては、このダイアログ ボックスにその他のフィールドが表示されることがあります。それらのフィールドでは、その他の基準を指定できます。たとえば、**content-type** フィールドを選択した場合は、リクエストとレスポンス間のコンテンツ タイプの不一致、未知のコンテンツ タイプ、および特定のコンテンツ タイプのプロトコル違反を検査できます。**transfer-encoding** フィールドを選択した場合は、さまざまなタイプの圧縮およびエンコーディングを検査できます。

一致フィールド

選択したフィールド タイプにクラス マップを一致させるには、このチェック ボックスを選択します。

リクエスト / レスポンス ボディ

ルータでは、リクエスト / レスポンス ボディの長さ、およびリクエスト / レスポンス ボディに含まれる特定のテキスト文字列を検査できます。

長さ

リクエスト / レスポンス ボディの長さの上限を指定するには、このチェック ボックスを選択して、［より大きい（>）］演算子を選択します。下限を指定するには［より小さい（<）］を選択します。

正規表現

照合する正規表現を指定する場合は、このチェック ボックスを選択します。検査する文字列と一致させる既存の正規表現クラス マップを選択するか、またはクラス マップを新たに作成します。正規表現の作成方法の詳細については、「正規表現の追加 / 編集」を参照してください。このダイアログ ボックスを終了しないで既存のマップを確認するには、［既存マップの選択］リストから必要なマップを選択し、［表示］をクリックします。

リクエスト / レスポンスのプロトコル違反

HTTP リクエスト / レスポンスのプロトコル違反を検査するには、[プロトコル違反] をクリックします。

IMAP クラス マップの追加 / 編集

Internet Message Access Protocol（IMAP）インスペクション用のクラス マップを作成すると、ユーザのクレデンシャルが危険にさらされないように、ユーザにセキュアな認証メカニズムを使用させることができます。

[クラス名] フィールドには、このクラス マップを識別する名前を入力します。説明を入力することもできます。クラス マップの編集時には、名前を変更することはできません。

セキュリティ保護されていないログインの IMAP トラフィックがルータで検査されるようにするには、[クリアテキストのログイン文字列] チェック ボックスを選択します。

無効なコマンドの IMAP トラフィックがルータで検査されるようにするには、[無効なプロトコル コマンド] チェック ボックスを選択します。

SMTP クラス マップの追加 / 編集

Simple Mail Transfer Protocol（SMTP）クラス マップを使用すると、コンテンツの長さを制限し、プロトコルへの準拠を徹底できます。

[クラス名] フィールドには、このクラス マップを識別する名前を入力します。また、表示されたフィールドに説明を入力することもできます。

[セッションで許可されている最大データ転送] フィールドには、ルータで SMTP セッションに対して許可される最大バイト数を入力します。

SUNRPC クラス マップの追加 / 編集

SUN Remote Procedure Call（SUNRPC）クラス マップを使用すると、ルータでトラフィックを検査するプログラムの番号を指定できます。

［クラス名］フィールドには、このクラス マップを識別する名前を入力します。説明を入力することもできます。クラス マップの編集時には、名前を変更することはできません。

プログラム番号を追加するには、［一致するプログラム番号］ボックスの［追加］をクリックします。

インスタント メッセージング クラス マップの追加 / 編集

インスタント メッセージング（IM）クラス マップを使用すると、検査するインスタント メッセージングのタイプを指定できるほか、すべての IM サービスに対するトラフィックを検査するか、またはテキスト チャット サービスのトラフィックだけを検査するかを指定できます。

［クラス マップ タイプ］フィールドでは、America Online を表す［aol］、Microsoft Networks Messenger を表す［msnmsgr］、または Yahoo! Messenger を表す［ymsgr］を選択します。

［一致条件］ボックスでは、全サービスを検査する場合は［すべてのサービス］、テキスト チャット トラフィックだけを検査する場合は［テキスト チャット サービス］をクリックします。

ポイントツーポイント クラス マップの追加 / 編集

P2P クラス マップでは、P2P アプリケーション、および一致条件を指定します。1 つのクラス マップでは、1 つのアプリケーションのみを指定できます。

クラス名

クラス マップを新規作成するには、新規クラス名を入力します。フィールドの右側のボタンをクリックすると、既存のクラス マップを選択して編集できます。クラス マップの一致条件は編集できますが、クラス マップ タイプを変更することはできません。

クラス マップ タイプ

次のタイプの P2P サービスに対し、P2P クラス マップを作成できます。

- eDonkey
- Fasttrack
- Gnutella
- Kazaa2

一致条件と値

［追加］をクリックして、トラフィック クラスで識別される接続タイプを指定する一致条件を入力します。

ファイル転送接続は、トラフィック クラス Fasttrack、Gnutella、および kazaa2 によって識別されるように指定できます。eDonkey の場合は、ファイル転送接続、ファイル名要求（検索ファイル名）、およびテキスト チャットがこのトラフィック クラスで識別されるように指定できます。一致条件の値には、任意の正規表現を指定できます。たとえば、すべてのファイル転送接続が識別されるように指定するには、「*」を入力します。

P2P ルールの追加

トラフィック クラスで識別される接続タイプを指定する一致条件を入力します。ファイル転送接続は、トラフィック クラス Fasttrack、Gnutella、および kazaa2 によって識別されるように指定できます。eDonkey の場合は、ファイル転送接続、ファイル名要求（search-file-name）、およびテキスト チャットがこのトラフィック クラスによって識別されるように指定できます。一致条件の値には、任意の正規表現を指定できます。たとえば、すべてのファイル転送接続が識別されるように指定するには、「*」を入力します。

POP3 クラス マップの追加 / 編集

Post Office Protocol version 3（POP3）インスペクション用のクラス マップを作成すると、ユーザのクレデンシャルが危険にさらされないように、ユーザにセキュアな認証メカニズムを使用させることができます。

［クラス名］フィールドには、このクラス マップを識別する名前を入力します。説明を入力することもできます。クラス マップの編集時には、名前を変更することはできません。

セキュリティ保護されていないログインの POP3 トラフィックがルータで検査されるようにするには、［クリアテキストのログイン文字列］チェック ボックスを選択します。

無効なコマンドの POP3 トラフィックがルータで検査されるようにするには、［無効なプロトコル コマンド］チェック ボックスを選択します。

パラメータ マップ

パラメータ マップでは、DoS（サービス拒否対策）、セッション タイマーと接続タイマー、およびログ記録などを設定する各パラメータに対し、ゾーンポリシーファイアウォールによるインスペクションの動作を指定できます。また、パラメータ マップをレイヤ 7 クラス マップ、およびポリシー マップと合わせて適用すると、HTTP オブジェクト、POP3 と IMAP の認証要件、およびその他のアプリケーション固有情報などのアプリケーション固有動作を定義することもできます。

パラメータ マップ ウィンドウ

［パラメータ マップ］ウィンドウには、プロトコル情報、URL フィルタリング、正規表現に設定されたパラメータ マップ、およびその他のタイプのパラメータ マップの一覧が表示されます。パラメータ マップがクラス マップに関連付けられている場合は、［使用元］カラムにクラス マップ名が表示されます。ウィンドウ下部には、選択したパラメータ マップの詳細情報が表示されます。パラメータ マップは、追加、編集、および削除が可能です。クラス マップで使用されているパラメータ マップを削除しようとすると Cisco CP による警告が表示されます。

これらのウィンドウに表示されるパラメータ マップの詳細については、次の該当リンクをクリックしてください。

- インスペクション パラメータ マップと CBAC のタイムアウトおよびしきい値
- プロトコル情報のパラメータ マップの追加 / 編集
- URL フィルタリングの全般設定
- URL フィルタ サーバの追加 / 編集
- ローカル URL リスト
- 正規表現の追加 / 編集

プロトコル情報のパラメータ マップの追加 / 編集

必要に応じて、IM アプリケーションなどの特定タイプのアプリケーション用のサーバを指定し、それらのサーバがテキスト チャットなどの特定のアクティビティで使用されるように制限することができます。

パラメータ マップ名

このパラメータ マップの用途を表す名前を入力します。たとえば、Yahoo! Instant Messenger のテキスト チャット サーバに対するサーバ リストを作成する場合は、**ymsgr-pmap** といった名前を使用できます。

サーバの詳細

画面のこのエリアには、サーバ名、サーバの IP アドレス、または IP アドレス範囲が一覧表示されます。

サーバ エントリの追加 / 編集

個々のサーバに対するホスト名または IP アドレス、またはサーバ グループに割り当てられる IP アドレスの範囲を指定できます。

ルータがネットワーク上の DNS サーバに接続して、サーバの IP アドレスを解決できる環境であれば、［名前］フィールドにホスト名を入力します。1 つのサーバに対する IP アドレスを入力する場合は、［単一 IP］フィールドにアドレスを入力します。IP アドレス範囲を使用する複数のサーバが存在する場合は、［IP 範囲］フィールドを使用します。左側のフィールドには最小 IP アドレスを入力し、右側のフィールドには最大 IP アドレスを入力します。たとえば、103.24.5.67 ～ 99 という範囲を入力するには、左側のフィールドに「**103.24.5.67**」、右側のフィールドに「**103.24.5.99**」とそれぞれ入力します。

正規表現の追加 / 編集

正規表現では、リテラルに指定された文字列と完全に一致するテキスト文字列、またはメタ文字を使用して指定された文字列と一部が一致するテキスト文字列を検出できます。正規表現を使用すると、特定のアプリケーション トラフィックの内容の中から一致するものを検出できます。たとえば、HTTP パケット内の一致する本文テキストを検出できます。

作成した正規表現は、ゾーンベース ポリシー ファイアウォールの各画面の、正規表現が必要なすべての項目で使用できます。正規表現に使用するメタ文字の一覧と、その使用方法については、「正規表現のメタ文字」を参照してください。

名前

正規表現を識別する名前を入力します。正規表現を編集している場合、このフィールドは読み取り専用です。

パターン リスト

1 つの正規表現には、複数のパターンを含めることができます。[追加] をクリックすると、新規の正規表現パターンを入力するためのダイアログ ボックスが表示されます。作成したパターンは、このリストに自動的に追加されます。別の正規表現内のパターンをコピーするには、[パターンのコピー] をクリックし、正規表現名の隣のプラス記号（+）をクリックして、必要なパターンをクリックしてから [OK] をクリックします。

パターン リストの例を次に示します。

```
parameter-map type regex ref_regex
pattern "\.delfinproject\.com"
pattern "\.looksmart\.com"
parameter-map type regex host_regex
pattern "secure\.keenvalue\.com"
pattern "\.looksmart\.com"
parameter-map type regex usragnt_regex
pattern "Peer Points Manager"
```

パターンの追加

このウィンドウに入力したパターンは、編集している正規表現パラメータ マップの末尾に追加されます。パラメータ マップ内の各パターンの順序を変更するには、［正規表現の編集］ウィンドウを使用します。

パターン

正規表現に追加するパターンを入力します。

ガイド ボタン

［ガイド］ボタンをクリックすると、正規表現の作成に役立つ［正規表現の作成］ダイアログ ボックスが表示されます。［ガイド］ボタンをクリックすると、［パターン］フィールドに入力したすべてのテキストが、［正規表現の作成］ダイアログ ボックスの［正規表現］フィールドに表示されます。

正規表現の作成

［正規表現の作成］ダイアログ ボックスでは、文字およびメタ文字を使用して正規表現を作成できます。メタ文字を挿入したフィールドでは、フィールド名のメタ文字がかっこで囲まれて表示されます。

スニペットの作成

このエリアでは、正規表現のテキスト スニペットを作成したり、［正規表現］フィールドにメタ文字を挿入したりできます。

- ［行頭（^）から開始］— キャレット（^）メタ文字を使用して、スニペットを行の先頭から開始するように指定します。このオプションを指定したスニペットはすべて、正規表現の先頭に挿入する必要があります。
- ［文字列の指定］— テキスト文字列を手動で入力します。
  - ［文字列］— テキスト文字列を入力します。

- ［特殊文字のエスケープ］— リテラルに使用するテキスト文字列内にメタ文字を入力した場合は、このチェック ボックスを選択することで、メタ文字の直前にエスケープ記号（\）が追加されます。たとえば、「example.com」と入力した場合にこのオプションを選択すると、「example\.com」と変換されます。
- ［大文字小文字を区別しない］— 大文字と小文字を区別せずに一致させたい場合は、このチェック ボックスを選択すると、大文字と小文字の両方に一致させるように、テキストが自動的に追加されます。たとえば「cats」は、「[cC][aA][tT][sS]」と変換されます。

文字列の指定

このエリアでは、正規表現に挿入するメタ文字を指定します。

- ［文字の否定］— 特定した文字とは一致させないように指定します。
- ［任意の文字 (.)］— 任意の文字と一致するピリオド（.）メタ文字を挿入します。たとえば、「**d.g**」と指定すると、*dog*、*dag*、*dtg* などのほか、*doghouse* など、これらの文字を含むあらゆる単語と一致します。
- ［文字セット］— 文字セットを挿入します。テキストは、この文字セット内の任意の文字と一致します。使用できる文字セットは次のとおりです。

  [0-9A-Za-z]

  [0-9]

  [A-Z]

  [a-z]

  [aeiou]

  [\n\f\r\t]（改行、フォーム フィード、リターン、またはタブと一致）

  たとえば [0-9A-Za-z] と指定した場合、このスニペットは A ～ Z の任意の文字（大文字または小文字）、または 0 ～ 9 の任意の数字と一致します。
- ［特殊文字］— \、?、*、+、|、.、[、(、^ など、エスケープの必要な文字を挿入します。エスケープ文字は \ 記号であり、このオプションを選択すると自動的に入力されます。
- ［空白文字］— 空白文字には \n（改行）、\f（フォーム フィード）、\r（キャリッジ リターン）、および \t（タブ）があります。
- ［3 桁の 8 進数］— ASCII 文字を 8 進数値（最大 3 桁）とみなして一致させます。たとえば、文字 \040 はスペースを表します。\ 記号が自動的に入力されます。

- ［2 桁の 16 進数］— ASCII 文字を 16 進数値（2 桁）とみなして一致させます。\ 記号が自動的に入力されます。
- ［指定文字］— 単一の任意の文字を入力します。

スニペットのプレビュー

*表示のみ可能です。*ここには、正規表現に入力されるスニペットが表示されます。

- ［スニペットの追加］— スニペットを正規表現の末尾に追加します。
- ［代替としてスニペットを追加］— スニペットを、正規表現の末尾にパイプ文字（|）で区切って追加します。これにより、パイプ文字の前後のどちらの表現とも一致するようになります。たとえば **dog|cat** と入力すると、dog または cat と一致します。
- ［カーソル位置にスニペットを挿入］— スニペットをカーソル位置に挿入します。

正規表現

この領域には、手動で入力可能な、スニペットによって構築された正規表現テキストが表示されます。［正規表現］フィールドのテキストを選択し、そのテキストに対して繰り返し回数を適用できます。

- ［選択回数］—［正規表現］フィールドのテキストを選択し、次のいずれかのオプションをクリックして、［選択を適用］をクリックします。たとえば、正規表現が "test me" の場合に "me" を選択し、［1 回以上 (+)］を選択すると、この正規表現は "test (me)+" に変わります。
  - ［ゼロ回以上 (?)］— 直前の表現が 0 回または 1 回繰り返されることを示します。たとえば、**lo?se** は、lse または lose と一致します。
  - ［1 回以上 (+)］— 直前の表現が 1 回以上繰り返されることを示します。たとえば、**lo+se** は、lose や loose と一致しますが、lse とは一致しません。
  - ［任意の回数 (*)］— 直前の表現が任意の回数だけ（0 を含む）繰り返されることを示します。たとえば、**lo*se** は、lse、lose、loose などと一致します。
  - ［最小限］— 少なくとも指定の回数だけ繰り返されます。たとえば、**ab(xy){2,}z** は、abxyxyz、abxyxyxyz などと一致します。
  - ［完全一致］— 指定された回数のとおりに繰り返されます。たとえば、**ab(xy){3}z** は、abxyxyxyz と一致します。
- ［選択を適用］— 選択した部分に繰り返し回数を適用します。

正規表現のメタ文字

次の表は、特別な意味を持つメタ文字の一覧を示します。

文字	説明	意味
.	ドット	任意の 1 文字と一致します。たとえば、**d.g** は、dog、dag、dtg　などのほか、これらの文字を含むあらゆる単語（doggonnit など）とも一致します。
(*exp*)	サブ表現	サブ表現を使用すると、特定の文字を周囲の文字と分けて、別のメタ文字を使用できるようになります。たとえば、**d(o|a)g** は、dog および dag と一致しますが、**do|ag** は do および ag と一致します。また、サブ表現を繰り返し回数と共に使用すると、反復する文字を区別できます。たとえば、**ab(xy){3}z** は、abxyxyxyz と一致します。
|	論理和	区切られた表現のうち、いずれかと一致します。たとえば **dog|cat** と入力すると、dog または cat と一致します。
?	疑問符	直前の表現が 0 回または 1 回繰り返されることを示します。たとえば、**lo?se** は、lse または lose と一致します。 **（注）** 疑問符は **Ctrl + V** の後に入力しないと、ヘルプ機能が起動します。
*	アスタリスク	直前の表現が任意の回数だけ（0 を含む）繰り返されることを示します。たとえば、**lo*se** は、lse、lose、loose などと一致します。
+	プラス	直前の表現が 1 回以上繰り返されることを示します。たとえば、**lo+se** は、lose や loose と一致しますが、lse とは一致しません。
{*x*}	繰り返し回数	指定された回数のとおりに繰り返されます。たとえば、**ab(xy){3}z** は、abxyxyxyz と一致します。
{*x*,}	最小繰り返し回数	少なくとも指定の回数だけ繰り返されます。たとえば、**ab(xy){2,}z** は、abxyxyz、abxyxyxyz などと一致します。
[*abc*]	文字クラス	角カッコ内の任意の文字と一致します。たとえば、**[abc]** は、a、b、または c と一致します。

文字	説明	意味
[^*abc***]**	文字クラスの否定	角カッコ内に含まれない 1 文字と一致します。たとえば、**[^abc]** では、a、b、または c 以外の任意の 1 文字と一致します。**[^A-Z]** では、大文字以外の任意の 1 文字と一致します。
[*a-c***]**	文字範囲クラス	範囲内の任意の文字と一致します。**[a-z]** は任意の小文字と一致します。文字と範囲を組み合わせて指定することもできます。**[abcq-z]** は a、b、c、q、r、s、t、u、v、w、x、y、z と一致しますが、これは **[a-cq-z]** と同じ結果となります。 ダッシュ記号（-）は、**[abc-]** または **[-abc]** のように、ブラケット内で最後または先頭の文字である場合にだけ、リテラルとみなされます。
""	引用符	文字列内の末尾または先頭のスペースを維持します。たとえば **" test"** と指定すると、一致文字列の検索時に先頭スペースが維持されます。
^	キャレット	行の先頭を指定します。
\	エスケープ文字	メタ文字に使用すると、リテラル文字と一致します。たとえば **\[** は、左向きの角カッコと一致します。
char	文字	メタ文字以外の文字は、リテラル文字と一致します。
\r	キャリッジ リターン	キャリッジ リターン 0x0d と一致します。
\n	改行	改行 0x0a と一致します。
\t	タブ	タブ 0x09 と一致します。
\f	フォーム フィード	フォーム フィード 0x0c と一致します。
\x*NN*	エスケープした 16 進数値	ASCII 文字を 16 進数値（2 桁）とみなして一致させます。
NNN	エスケープした 8 進数値	ASCII 文字を 8 進数値（3 桁）とみなして一致させます。たとえば、文字 040 はスペースを表します。