ICAP インターフェイスのサポート

この章では、コア ネットワーク サービス サブスクライバ用の外部アクティブ コンテンツ フィルタリング サーバーの設定について説明します。この章では、この機能の導入に使用する設定とコマンドについても説明します。

この章に記載の手順を実行する前に、各製品のアドミニストレーション ガイドの説明に従って、ご使用のサービスモデルに最適な設定例を選択し、そのモデルに必要な要素を設定することを推奨します。

現在、次の製品が ICAP インターフェイス機能をサポートしています。

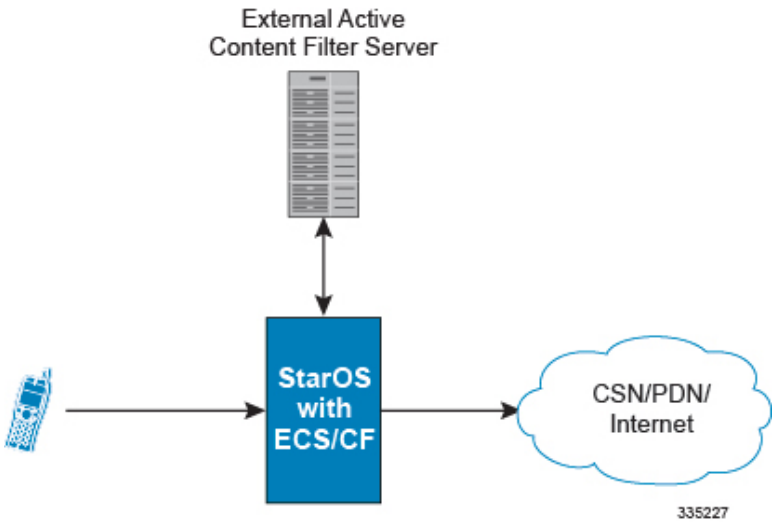
- GGSN
- P-GW

ICAP インターフェイスサポートの概要

この機能は、合理化された ICAP インターフェイスをサポートし、ディープ パケット インスペクション（DPI）を活用して、外部アプリケーションサーバーが DPI 機能を実行せずに、またデータフローに挿入されることなく、そのサービスを提供できるようにします。たとえば、外部のアクティブコンテンツフィルタリング（ACF）プラットフォームの使用時などが該当します。

次の図に、外部 ACF に対する合理化された ICAP インターフェイスサポートの概要を示します。

図 *1:* 外部 *ACF* を使用して合理化された *ICAP* インターフェイスの概要図



ECS を使用するシステムは、DPI をサポートするように構成されており、システムはこの機能をコンテンツ課金にも使用します。WAP および HTTP トラフィックは、ICAP インターフェイスを介してコンテンツがフィルタリングされます。アダルトコンテンツを含むRTSP トラフィックも ICAP インターフェイスでコンテンツをフィルタリングできます。RTSP 要求パケットだけが、ICAP インターフェイスを介したコンテンツフィルタリングの対象となります。

サブスクライバが WAP（WAP1.x または WAP2.0）または Web セッションを開始すると、後続の GET/POST 要求が DPI 機能によって検出されます。GET/POST 要求の URL が抽出され、サブスクライバ識別情報とサブスクライバ要求とともに ICAP メッセージでアプリケーションサーバーに渡されます。アプリケーションサーバーは、カテゴリや、タイプ、アクセスレベル、コンテンツカテゴリなどの他の分類に基づいて URL をチェックし、要求を許可、ブロック、またはリダイレクトする必要があるかどうかを、次のメッセージでGET/POST メッセージに応答して決定します。

- 要求が受け入れられる場合、200 OK メッセージ。
- リダイレクトの場合、302 リダイレクトメッセージ。このリダイレクトメッセージには、サブスクライバのリダイレクト先となる URL が含まれます。
- RTSP 要求の拒否応答コード 200 はサポートされていません。403 "Forbidden" 拒否応答コードのみがサポートされます。

受信した応答に応じて、ECS を備えたシステムは要求を変更なしで渡すか、またはメッセージを破棄して、適切なリダイレクトメッセージまたはブロックメッセージでサブスクライバに応答します。

コンテンツの課金は、要求がアプリケーションサーバーによって制御された後にのみ、アクティブ課金サービス（ACS）によって実行されます。これにより、外部アプリケーションとコンテンツベースの課金との間の適切なインターワーキングが保証されます。特に、これにより、リダイレクトの場合に課金が適切な要求に適用されることが保証され、発生する可能性が

ある課金ベースのリダイレクト（課金通知、追加課金ページなど）が、アプリケーションサーバーによって行われる決定と干渉しないことが保証されます。

ACF には次の機能が含まれます。

- ICAP メッセージで渡されたサブスクライバのアイデンティティに基づくサブスクライバポリシーの取得
- サブスクライバのプロファイルに基づいた、コンテンツのタイプに応じて実行する適切なアクション（許可、拒否、リダイレクト）の決定
- URL に対するアクション（許可、拒否、またはリダイレクト）決定を ACS モジュールに戻す

サポート対象のネットワークとプラットフォーム

この機能は、システムで設定されているコアネットワークサービス用の Cisco ASR 5500 プラットフォームをサポートします。

プラットフォームの詳細については、該当する『*System Administration Guide*』[英語] を参照するか、シスコのアカウント担当者にお問い合わせください。

ライセンス要件

Internet Content Adaptation Protocol（ICAP）インターフェイスによる外部コンテンツ フィルタリング サーバーのサポートは、シスコのライセンス機能です。別の機能ライセンスが必要になる場合があります。特定のライセンス要件の詳細については、シスコのアカウント担当者にお問い合わせください。

ライセンスのインストールと確認の詳細については、『システム管理ガイド』の「ソフトウェア管理操作」の「ライセンスキーの管理」の項を参照してください。

再送信されたパケットでの障害アクション

再送信パケットのフローの ICAP 要求に対してデフォルトの ICAP 障害アクションが実行された場合、再送信パケットに対して ICAP 評価が有効になります。接続をリセットする必要があり、他に使用可能な冗長接続がない場合、ICAP デフォルト障害アクションは、接続で保留中の ICAP 要求に対して実行されます。たとえば、ICAP 要求タイムアウトのシナリオや、ICAP 接続タイムアウトのシナリオの場合があります。これらの場合、アップリンク方向に再送信されたパケットは、ICAP 評価のために再送信されます。

WAP CO の場合、ICAP 障害アクションが実行された WAP トランザクションのアップリンク再送信パケットが、ICAP 評価のために送信されます。再送信パケットの WSP ヘッダーは、WSP アナライザによって解析されません。そのトランザクションの前のパケットで受信した URL が、ICAP 評価に使用されます。同じフローの複数の WTP トランザクションで障害アクションが実行された場合（WTP 連結 GET 要求の場合など）、各トランザクションのアップリンク再送信パケットが評価のために再送信されます。

HTTP の場合、ICAP 障害アクションが実行された HTTP フローのアップリンク再送信パケットが、ICAP 評価のために送信されます。現在のセカンダリセッション（最後のアップリンク要求）に存在する URL が、ICAP 評価に使用されます。ただし、同じフロー（パイプライン処理された要求）に対して複数の未処理の ICAP 要求がある場合、再送信パケットについては、評価のために送信される URL は、最後の GET 要求の URL になります。

元の要求に対する ICAP 応答を受信せず、再送信された要求が着信した場合に、再送信パケットに対して実行されるさまざまな障害アクションにおける再送信は、次のとおりです。

- WSP CO：
  - Permit：アップリンクパケットが ICAP 評価のために送信され、ICAP 応答に応じて、WTP トランザクションが許可またはブロックされます。WAP ゲートウェイが、許可された GET 要求に対する応答を送信する可能性があります。そのため、競合状態が発生し、サブスクライバは、評価が redirect または content insert であった場合でも、Web ページを表示できる可能性があります。
  - Content Insert：再送信パケットは、ICAP 評価のために送信されません。
  - Redirect：再送信パケットは、ICAP 評価のために送信されません。
  - Discard：アップリンクパケットが ICAP 評価のために送信され、ICAP 応答に応じて、WTP トランザクションが許可またはブロックされます。
  - Terminate flow：アップリンクパケットが ICAP 評価のために送信され、ICAP 応答に応じて、WTP トランザクションが許可またはブロックされます。フローの終了中に送信された WSP 切断パケットが WAP ゲートウェイによって受信された場合、WAP ゲートウェイは、この GET 要求の中止トランザクションを送信する場合があります。
- [HTTP]：
  - Permit：アップリンクパケットが ICAP 評価のために送信され、ICAP 応答に応じて、最後の HTTP GET 要求が送信されます。HTTP サーバーが、許可された GET 要求に対する応答を送信する可能性があります。そのため、競合状態が発生し、サブスクライバは、評価が redirect または content insert であった場合でも、Web ページを表示できる可能性があります。
  - Content Insert：再送信パケットはドロップされ、課金されません。
  - Redirect：再送信パケットはドロップされ、課金されません。
  - Discard：アップリンクパケットが ICAP 評価のために送信され、ICAP 応答に応じて、WTP トランザクションが許可またはブロックされます。
  - Terminate flow：再送信パケットはドロップされ、課金されません。
- RTSP：

  次のシナリオでは、クライアントから RTSP 要求を受信した場合の障害アクションについて説明します。ICAP が有効になっている場合、要求は、コンテンツフィルタリングのために ICAP サーバーに送信されます。

- Allow：設定されている障害アクションが「allow」である場合、RTSP 要求パケットは、適切な判定結果アクションの適用後に送信されます。この場合、フローは、受信した ICAP 応答が 200 OK のときと同じであるままになります。
- Content Insert：設定された障害アクションが「content-insertion <string of size 1 to 128>」である場合、RTSP 要求に対するこの障害アクションはサポートされません。代わりに、このような RTSP 要求に対して障害アクション「Discard」がサポートされます。
- Redirect-URL：設定された障害アクションが「redirect-url <string of size 1 to 128>」である場合、RTSP「302 Moved Temporarily」応答ヘッダーを含む TCP FIN_ACK パケットが、リダイレクト用に指定された URL を含むクライアントに向けて挿入されます。TCP RST パケットがサーバーに向けて挿入されます。そのため、基礎となる TCP 接続が閉じられます。RTSP クライアントが、リダイレクトされた URL を再試行する場合は、新しい TCP 接続を開くことが開始される必要があります。
- Discard：設定された障害アクションが「discard」である場合、クライアントから受信した RTSP 要求パケットはサイレントに廃棄され、クライアントに通知は送信されません。
- Terminate flow：設定された障害アクションが「terminate-flow」である場合、クライアントに向けて TCP FIN-ACK を挿入し、サーバーに向けて RST パケットを挿入することによって、TCP 接続が切断されます。ただし、このフローの終了に関しては、RTSP クライアントおよびサーバーに通知が送信されません。

RFC 3507 準拠の ICAP クライアント通信

ICAP コンテンツ フィルタリング ソリューションは、RFC 3507（Internet Content Adaptation Protocol（ICAP））に準拠して、Cisco ASR 5500 P-GW および HA 上の ICAP サーバーとの ICAP クライアント通信をサポートするように拡張されています。このリリースでは、RFC 3507 に基づく HTTP 要求の変更とエラーコードの部分的な拡張にのみ対応しています。P-GW/HA で実行されている ICAP クライアントは、ICAP プロトコルを介して外部 ICAP サーバーと通信します。サブスクライバのコンテンツフィルタリングが有効になっている場合、そのサブスクライバからのすべての HTTP GET 要求がコンテンツフィルタリングサーバー（ICAP サーバー）によって検証され、コンテンツ分類要求に応じて、許可、拒否、またはリダイレクトされます。

コンテンツフィルタリングは、事前定義された静的ルールのオーバーライド制御（OC）機能、または L7 ダイナミックルールのアクティブ化機能のいずれかによって、サブスクライバに対して有効になります。設定可能なオプションがコンテンツ フィルタリングのサーバー グループ コンフィギュレーション モードに追加されました。これにより、サブスクライバの番号情報と CIPA（児童インターネット保護法）カテゴリの 2 つのパラメータを含む ICAP ヘッダーが設定されます。

重要 オーバーライド制御と L7 ダイナミックルールの有効化は、ライセンスにより制御される機能です。これらの機能を設定する前に、有効な機能ライセンスをインストールする必要があります。詳細については、シスコのアカウント担当者にお問い合わせください。

- サブスクライバ番号：「Subscription ID」AVP は、CCR メッセージでゲートウェイから PCRF に送信されます。AVP 値は、HSS からゲートウェイに送られます。ゲートウェイでは、CCI-A メッセージでこの AVP を受信しません。
- CIPA カテゴリ：カテゴリ文字列は PCRF によって提供され、ICAP 要求変更メッセージの拡張ヘッダーとして組み込まれます。AVP は、CCA-I または RAR で PCRF から受信されます。

ディクショナリおよび AVP のサポート

新しいコンテンツフィルタリング（CF）ディクショナリの「custom4」が導入され、次の新しい AVP が r8-gx-standard ディクショナリと custom4 ディクショナリに追加されます。

- Override-Content-Filtering-State：この属性は、ルールまたは課金アクションのコンテンツ フィルタリング ステータス（CF 状態）に関する情報を伝送します。この AVP は、静的ルールや事前定義されたルールのコンテンツ フィルタリング ステータスを上書きするために使用されます。この属性は Override-Control grouped AVP に含まれます。
- CIPA：この属性には、ICAP プランの識別子として扱われる児童インターネット保護法（CIPA）カテゴリの文字列値が含まれます。この識別子は、ICAP サーバーが正しいコンテンツ フィルタリング プラン（パケットの処理に基づく CIPA カテゴリ）を特定するのに役立ちます。

  この属性値は Gx インターフェイスを介して PCRF から受信され、ICAP 要求の送信時に ICAP ヘッダーに追加されます。
- L7-Content-Filtering-State：この属性は、L7 ルールのコンテンツ フィルタリング ステータス（CF 状態）に関する情報を伝送します。この属性は、PCRF からのインストールで受信した L7 課金ルール定義に対して ICAP 機能が有効か無効かを示します。この属性値に基づいて、ダイナミックルールに一致するトラフィックが ICAP サーバーに送信されます。

  L7 ルール処理のために、この属性が L7-Application-Description grouped AVP に追加されます。これは、HTTP プロトコルにのみ適用されます。

重要 OC および L7 ダイナミックルール機能を介してコンテンツフィルタリングを制御するための CIPA およびフラグは、r8-gx-standard ディクショナリにのみ適用されます。

新しい AVP のサポートに加えて、L7-Application-Description grouped AVP の L7-Field AVP は、ANY-MATCH を入力データとして受け入れるようにエンコードされます。現在のフレームワークは、課金アクション内にあるオーバーライド制御の既存の「vlan-id」フィールドをサポート

していません。したがって、Override-Content-Filtering-State AVP で Override-VLAN-ID を置き換えて OC をサポートします。

サブスクライバがセッション作成要求を開始すると、P-GW/HA は CCR-I メッセージを PCRF に送信してサブスクライバプロファイルを取得します。このサブスクライバの ICAP 機能が有効になっている場合、PCRF は CIPA と OC の情報を含む CCA-I メッセージで応答します。

L7 ダイナミックルールの場合、L7-Application-Description grouped AVP で L7-Content-Filtering-State AVP を送信すると、コンテンツフィルタリング機能が有効になります。ダイナミックルールの L7-Content-Filtering-State を受信した場合は、少なくとも 1 つの L7 フィルタが存在するはずです。L7-Content-Filtering-state AVP が L7 フィルタ情報 AVP とともに送信された場合、Content-Filtering の状態は考慮されません。したがって、L7-Content-Filtering-State で受信したフィルタは処理されず、L7 ルールが破棄されます。

オーバーライド制御の場合、サブスクライバに対してコンテンツフィルタリングが有効になっていると、PCRF は Override-Control AVP を介して ICAP フラグを送信します。この AVP は、そのサブスクライバの ICAP 機能を有効にするために課金アクションを上書きします。

サポートされる AVP の詳細については、『*AAA Interface Administration and Reference*』[英語] を参照してください。

制限事項

この機能の制限事項は次のとおりです。

- IPv4 アドレス方式のみがサポートされています。
- ICAP コンテンツフィルタリングは HTTP トラフィックにのみ適用されます。HTTPS トラフィックは、ICAP クライアントではサポートされていません。
- 高速パスは、この機能ではサポートされていません。

ICAP インターフェイスサポートの設定

ここでは、ICAP クライアントと ACF サーバー（ICAP サーバー）間の Internet Content Adaptation Protocol（ICAP）インターフェイスを介してコンテンツ フィルタリング サーバー グループ（CFSG）を設定する方法について説明します。

重要 システムの ICAP インターフェイスで外部コンテンツ フィルタリング サーバーを設定するための最小の命令セットについて説明します。追加のパラメータとオプションを設定するコマンドの詳細については、『*Command Line Interface Reference*』の「*CFSG Configuration Mode Commands*」の章を参照してください。

外部コンテンツ フィルタリング サーバーで ICAP インターフェイスをサポートするようにシステムを設定するには、次の手順を実行します。

手順

ステップ 1 ICAP サーバーグループの作成およびアドレスのバインド （8 ページ）の設定例を適用して、コンテンツ フィルタリング サーバー グループを作成し、シャーシの発信元（ローカル）IP アドレスを使用して ICAP インターフェイスを作成します。

ステップ 2 ICAP サーバーおよびその他のパラメータの設定 （8 ページ）の設定例を適用して、アクティブなコンテンツ フィルタリング サーバー（ICAP サーバー）の IP アドレスを指定し、CAP サーバーグループのその他のパラメータを設定します。

ステップ 3 ICAP サーバーグループの ECS ルールベースの設定 （9 ページ）の設定例を適用して、ECS ルールベースのコンテンツ フィルタリング モードを外部コンテンツ フィルタリング サーバー グループ モードに設定します。

ステップ 4 ICAP サーバーグループの課金アクションの設定 （10 ページ）の設定例を適用して、アクティブ課金設定モードで ICAP インターフェイス上の外部コンテンツ フィルタリング サーバーに HTTP/RTSP/WAP GET 要求を転送するよう課金アクションを設定します。

ステップ 5 ICAP サーバーグループ設定の確認 （10 ページ）の手順に従って、ICAP インターフェイスと外部コンテンツ フィルタリング サーバー グループの設定を確認します。

ステップ 6 EXEC モードコマンド **save configuration** を使用して、フラッシュメモリ、外部メモリデバイス、もしくはネットワーク上の場所に設定を保存します。構成ファイルを検証して保存する方法の詳細については、『*System Administration Guide*』および『*Command Line Interface Reference*』を参照してください。

ICAP サーバーグループの作成およびアドレスのバインド

ICAP サーバーグループを作成し、IP アドレスをバインドするには、次の例に示すコマンドを使用します。

```
configure
   context <icap_ctxt_name> [ -noconfirm ]
      content-filtering server-group <icap_svr_grp_name> [ -noconfirm ]
         origin address <ip_address>
         end
```

注：

- <*ip_address*> is local IP address of the CFSG endpoint.

ICAP サーバーおよびその他のパラメータの設定

次の例を使用して、アクティブ コンテンツ フィルタリング（ICAP サーバー）および関連する他のパラメータを設定します。

```
configure
   context <icap_context_name>
      content-filtering server-group <icap_server_grp_name>
```

```
        icap server <ip_address> [ port <port_number> ] [ max <max_msgs>] [
priority <priority> ] [ standby ]
        connection retry-timeout <retry_timeout>
        deny-message <msg_string>
        dictionary { custom1 | custom2 | custom3 | custom4 | standard
 }
        failure-action { allow | content-insertion <content_string> |
discard | redirect-url <url> | terminate-flow }
        header extension options { cipa-category cipa_category_name |
subscriber-number subscriber_num_name } +
        response-timeout <timeout>
        end
```

注：

- コンテンツ フィルタリング サーバー グループごとに 1 つの ICAP サーバーのみを設定できます。
- **standby** キーワードを使用して、ICAP サーバーをスタンバイに設定できます。コンテンツ フィルタリング サーバー グループあたり最大 10 のアクティブおよびスタンバイ ICAP サーバーを設定できます。同じサーバーグループのアクティブサーバーとスタンバイサーバーは、アクティブ/スタンバイモードで動作するように設定できます。
- オプションの **max** <*max_msgs*> キーワードを使用して設定された、ICAP 接続あたりの未処理要求の最大数は 1 つに制限されています。したがって、**max** キーワードを使用して設定された他の値は無視されます。
- オプションです。ICAP URL 抽出動作を設定するには、コンテンツ フィルタリング サーバー グループ コンフィギュレーション モードで次のコマンドを入力します。

  url-extraction { after-parsing | raw }

  デフォルトでは、ACF クライアントから ICAP サーバーに送信される URL のパーセントエンコードされた 16 進文字は、対応する ASCII 文字に変換されて送信されます。
- **custom4** ディクショナリは、ICAP 要求メッセージのユーザー定義情報を指定するカスタム定義のディクショナリです。ICAP 要求メッセージには、サブスクライバ番号と CIPA カテゴリ値が含まれます。

  custom4 ディクショナリが設定されている場合、ICAP 要求は ICAP RFC 3507 要求モード要求の一部として作成されます。その他のディクショナリが設定されている場合、ICAP クライアントの以前の実装は一部 RFC に準拠しません。
- **header extension options** コマンドは、ICAP ヘッダーパラメータ（サブスクライバ番号と CIPA カテゴリ）を設定します。

ICAP サーバーグループの ECS ルールベースの設定

コンテンツフィルタリングの ECS ルールベースでコンテンツ フィルタリング モードを ICAP サーバーモードに設定するには、次の例を使用します。

```
configure
   require active-charging
   active-charging service <acs_svc_name> [ -noconfirm ]
      rulebase <rulebase_name> [ -noconfirm ]
         content-filtering mode server-group <cf_server_group>
         end
```

注：

- **optimized-mode** キーワードは使用できません。

重要 **configure**、**require active-charging**,、**active-charging service** <*acs_svc_name*> **[-noconfirm]**、**rulebase** CLI コマンドを設定した後、設定を保存し、シャーシをリロードしてコマンドを有効にする必要があります。設定ファイルを保存してシャーシをリロードする方法については、使用している展開の『*System Administration Guide*』を参照してください。

ICAP サーバーグループの課金アクションの設定

次の例を使用して、コンテンツ処理のために HTTP/WAP GET 要求を ICAP サーバーに転送するように課金アクションを設定します。

```
configure
   active-charging service <acs_svc_name>
      charging-action <charging_action_name> [ -noconfirm ]
         [ no ] content-filtering processing server-group
         end
```

注：

- 課金アクションによって提供されるコンテンツ フィルタリング フラグがオーバーライド制御機能の設定に必要な場合は、**no content-filtering processing** コマンドを設定する必要があります。これにより、コンテンツフィルタリング処理のオーバーライドを、オーバーライド制御機能を通じて有効または無効にすることができます。

ICAP サーバーグループ設定の確認

ここでは、cfgファイルに設定を保存した後に、それらの設定を表示して確認する方法と、サービスのアクティブな設定内のエラーや警告情報を取得する方法について説明します。

重要 ここに記載されているコマンドはすべて Exec モードで実行します。すべてのプラットフォームですべてのコマンドを使用できるわけではありません。

次の手順は、この機能の設定を確認するために使用します。

手順

ステップ 1 Exec モードで次のコマンドを入力して、ICAP コンテンツ フィルタリング サーバー グループの設定を確認します。

show content-filtering server-group

次に、出力例を示します。この例では、*icap_cfsg1* という名前の ICAP コンテンツ フィルタリング サーバー グループが設定されています。

```
Content Filtering Group:         icap_cfsg1
    Context:                             icap1
    Origin Address:                      1.2.3.4
    ICAP Address(Port):                  1.2.3.4(1344)
    Max Outstanding:                     256
    Priority:                            1
    Response Timeout: 30(secs)  Connection Retry Timeout: 30(secs)
    Dictionary:                          standard
    Timeout Action:                      terminate-flow
    Deny Message:                        "Service Not Subscribed"
    URL-extraction:                      after-parsing
    Header Extension Options:            subscriber-number i-sub
    Content Filtering Group Connections: NONE
Total content filtering groups matching specified criteria:  1
```

ステップ 2 Exec モードで次のコマンドを入力して、設定内のエラーを確認します。

show configuration errors

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。