コンテンツ制限を使用したアクセス制御

次のトピックでは、コンテンツ制限機能を使用するようにアクセス コントロール ポリシーを設定する方法について説明します。

コンテンツ制限について

主要な検索エンジンやコンテンツ配信サービスは、検索結果と Web サイトのコンテンツを制限できる機能を提供しています。たとえば学校では、「子どもをインターネットから保護する法律」（CIPA）を順守するために、コンテンツ制限機能を使用します。

コンテンツ制限機能は、検索エンジンやコンテンツ配信サービスで実行する場合には、個々のブラウザやユーザを対象にしか実施できません。FirePOWER システムは、これらの機能をご使用のネットワーク全体に拡大できます。

このシステムにより、以下を実施できます。

- セーフサーチ：多くの主要な検索エンジンでサポートされているこのサービスは、ビジネス、行政、および教育の環境で不愉快であると分類されている、露骨なアダルト向けコンテンツを除外します。システムは、サポートされている検索エンジンのホームページへのユーザのアクセス機能は制限しません。
- *YouTube EDU*：このサービスは、教育環境向けに YouTube コンテンツをフィルタリングします。これにより学校は、教育的なコンテンツへのアクセスを設定しながら、非教育的なコンテンツへのアクセスを制限できます。YouTube EDU は YouTube 制限付きモードとは別の機能であり、Google のセーフサーチ機能の一部として YouTube 検索に対する制限を実施します。YouTube 制限付きモードは、セーフサーチのサブ機能であることに注意してください。YouTube EDU を使用すると、ユーザは標準の YouTube ホームページではなく、YouTube EDU ホームページにアクセスします。

次の 2 つの方法を使用して、これらの機能を実施するようにシステムを設定できます。

方法：アクセス コントロール ルール
コンテンツ制限機能は、検索またはコンテンツ照会の制限状態を、要求URIの要素、関連するCookie、またはカスタムHTTPヘッダー要素により通信します。システムがトラフィックを処理するときに、これらの要素を変更するためのアクセス コントロール ルールを設定できます。

方法：DNS シンクホール
Google 検索では、セーフサーチ（YouTube 制限付きモードを含む）のフィルタを課すGoogle SafeSearch 仮想 IP アドレス（VIP）にトラフィックをリダイレクトするように、システムを設定できます。

次の表では、これらの実施方法の違いについて説明します。

表 *1:* コンテンツ制限方法の比較

属性	方法：アクセス コントロール ルール	方法：DNS シンクホール
サポートされるデバイス	任意（Any）	Firepower Threat Defense のみ
[サポートされる検索エンジン（Search engines supported）]	ルールエディタの[アプリケーション（Applications）]タブのタグ付きのすべての `safesearch supported`	Google のみ
[サポートされる YouTube 制限付きモード（YouTube Restricted Mode supported）]	あり	あり
[サポートされる YouTube EDU（YouTube EDU supported）]	あり	なし
[SSL ポリシーが必要（SSL policy required）]	あり	なし
[ホストは IPv4 の使用が必要（Hosts must be using IPv4）]	なし	あり
[接続イベント ロギング（Connection event logging）]	あり	あり

使用する方法を決定する際には、次の制限事項を考慮します。

- アクセス コントロール ルール方法には SSL ポリシーが必要で、これはパフォーマンスに影響を及ぼします。
- Google セーフサーチ VIP は IPv4 トラフィックのみをサポートします。Google 検索を管理するように DNS シンクホールを設定する場合は、影響を受けるネットワークのすべてのホストが IPv4 を使用している必要があります。

接続イベントの[理由（Reason）]フィールドに、方法に応じて異なる値がログ記録されます。

- アクセス コントロール ルール：[コンテンツの制限（Content Restriction）]
- DNS シンクホール：[DNS ブロック（DNS Block）]

アクセスコントロールルールを使用したコンテンツ制限の実施

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Control	いずれか（Any）	いずれか（Any）	Admin/Access Admin/Network Admin

注意 ルールのプリエンプションを避けるため、SSL とアクセス コントロール ポリシーの両方で、YouTube EDU を制御するルールは、セーフサーチを制御するルールの上に配置します（コンテンツ規制ルールの順序を参照）。

ステップ 1 SSL ポリシーを作成します。基本的な SSL ポリシーの作成を参照してください。

ステップ 2 セーフサーチと YouTube EDU のトラフィックを処理するための SSL ルールを追加します。

- ルールの [アクション（Action）] として [復号 - 再署名（Decrypt - Resign）] を選択します。システムは、コンテンツ制限処理にこれ以外のアクションをサポートしません。
- [アプリケーション（Applications）] タブで、選択内容を [選択済みのアプリケーションとフィルタ（Selected Applications and Filters）] リストに追加します。
  - YouTube EDU：`YouTube` と `YouTube Upload` アプリケーションを追加します。
  - セーフサーチ：[カテゴリ：検索エンジン（Category: search engine）] フィルタを追加します。

詳細については、アプリケーション条件（アプリケーション制御）を参照してください。

ステップ 3 追加した SSL ルールのための、ルールの位置を設定します。クリックしてドラッグするか、または右クリック メニューを使用してカット アンド ペーストを実行します。

プリエンプションを避けるため、セーフサーチ ルールを YouTube EDU ルールの後に配置します。

ステップ 4 アクセス コントロール ポリシーを作成または編集して、SSL ポリシーとアクセス コントロール ポリシーを関連付けます。

詳細については、アクセス制御への他のポリシーの関連付けを参照してください。

ステップ 5 アクセス コントロール ポリシーに、セーフサーチと YouTube EDU トラフィックを処理するためのルールを追加します。

- ルールの [Action] として [Allow] を選択します。システムは、コンテンツ制限処理にこれ以外のアクションは許可しません。
- [アプリケーション（Applications）] タブで、セーフサーチ（）または YouTube EDU（）のいずれかの淡色表示されているアイコンをクリックして、関連オプションを設定します（アクセス制御ルールのセーフサーチ オプション （4 ページ）およびアクセス制御ルールの YouTube EDU オプション（5 ページ）を参照）。

  ルールに [Allow] 以外の [Action] を選択すると、これらのアイコンは淡色表示されるのではなく無効になります。

  同じアクセス コントロール ルールに対してセーフサーチと YouTube EDU の制限を有効にすることはできません。
- [Applications] タブで、[Selected Applications and Filters] リストのアプリケーション選択を絞り込みます。

  たいていの場合、セーフサーチまたは YouTube EDU を有効にすると、[Selected Applications and Filters] リストに適切な値が入力されます。セーフサーチまたは YouTube アプリケーションを有効にしたときにそれらの機能がすでにリストにある場合、システムはリストへの自動入力を行いません。予期したとおりにアプリケーションが入力を行わない場合は、それらを以下のように手動で追加します。

  - YouTube EDU：`YouTube` と `YouTube Upload` アプリケーションを追加します。
  - セーフサーチ：[カテゴリ：検索エンジン（Category: search engine）] フィルタを追加します。

詳細については、アプリケーション条件とフィルタの設定を参照してください。

ステップ 6 追加したアクセス コントロール ルールに対してルールの位置を設定します。クリックしてドラッグするか、または右クリック メニューを使用してカット アンド ペーストを実行します。

プリエンプションを避けるため、セーフサーチ ルールを YouTube EDU ルールの後に配置します。

ステップ 7 システムが制限付きコンテンツをブロックするときに表示する HTTP 応答ページを設定します（HTTP 応答ページの選択を参照）。

ステップ 8 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。

アクセス制御ルールのセーフサーチ オプション

Firepower System は、特定の検索エンジンのセーフサーチ フィルタリングにのみ対応しています。対応している検索エンジンのリストについては、アクセス制御ルール エディタの [アプリケーション（Applications）] タブのアプリケーションにタグ付けされている `safesearch supported` を参照してください。対応していない検索エンジンのリストについては、アプリケーションにタグ付けされている `safesearch` を参照してください。

アクセス コントロール ルールに対してセーフサーチを有効にするには、次のパラメータを設定します。

セーフサーチを有効にする
このルールに一致するトラフィックに対して、セーフサーチフィルタリングを有効にします。

サポートされない検索トラフィック
サポートされていない検索エンジンからのトラフィックを処理するときにシステムが取るアクションを指定します。[ブロック（Block）] または [リセットによるブロック（Block with Reset）] を選択すると、いつ制限されたコンテンツをブロックするかを表示する HTTP 応答ページを設定する必要があります。HTTP 応答ページの選択

アクセス制御ルールの YouTube EDU オプション

アクセス コントロール ルールに対して YouTube EDU を有効にするには、次のパラメータを設定します。

YouTube EDU の有効化
このルールに一致するトラフィックに対して、YouTube EDU フィルタリングを有効にします。

カスタム ID
学校または地域のネットワークを固有に識別する値を YouTube EDU イニシアチブに指定します。YouTube は、学校または地域が YouTube EDU アカウントの登録をすると、この ID を提供します。

（注） [Enable YouTube EDU] をオンにした場合は、[Custom ID] を入力する必要があります。この ID は、YouTube によって外部に定義されます。システムは、YouTube システムに対するユーザの入力内容は検証しません。無効な ID を入力すると、YouTube EDU の制限が予期したとおりに実行されない場合があります。

DNS シンクホールを使用したコンテンツ制限の実施

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
Threat	Protection	Firepower Threat Defense	いずれか（Any）	Admin/Access Admin/Network Admin

通常、DNS シンクホールは、トラフィックを特定のターゲットからそらします。この手順では、Google セーフサーチ仮想 IP アドレス（VIP）にトラフィックをリダイレクトする（つまり、Google と YouTube の検索結果にコンテンツ フィルタを適用する）ように DNS シンクホールを設定する方法について説明します。

Google セーフ サーチは VIP に単一の IPv4 アドレスを使用するため、ホストは IPv4 アドレッシングを使用する必要があります。

注意 ネットワークにプロキシ サーバが含まれる場合、Firepower Threat Defense デバイスをプロキシ サーバとインターネットの間に配置しない限り、この方法でのコンテンツ制限は効果的ではありません。

この手順では、Google 検索のみにコンテンツ制限を適用する方法について説明します。他の検索エンジンに対してコンテンツ制限を適用する場合は、アクセス コントロール ルールを使用したコンテンツ制限の実施 （3 ページ）を参照してください。

ステップ 1 次の URL を使用して、サポートされる Google ドメインのリストを取得します。https://www.google.com/supported_domains

ステップ 2 ローカル コンピュータにカスタム DNS リストを作成し、次のエントリを追加します。

- Google セーフサーチを適用するには、サポートされる Google ドメインごとにエントリを追加します。
- YouTube 制限モードを適用するには、「youtube.com」エントリを追加します。

カスタム DNS リストは、テキスト ファイル（.txt）形式にする必要があります。テキスト ファイルの各行に、先頭ピリオドを除いた状態で、個々のドメイン名を指定する必要があります。たとえば、サポートされるドメインが「.google.com」の場合、「google.com」として指定する必要があります。

ステップ 3 カスタム DNS リストを Firepower Management Center にアップロードします（新しいセキュリティ インテリジェンス リストの Firepower Management Center へのアップロードを参照）。

ステップ 4 Google セーフサーチ VIP の IPv4 アドレスを判別します。たとえば、forcesafesearch.google.com で `nslookup` を実行します。

ステップ 5 セーフサーチ VIP のシンクホール オブジェクトを作成します（シンクホール オブジェクトの作成を参照）。

このオブジェクトでは、次の値が使用されます。

- [IPv4 アドレス（IPv4 Address）]：セーフ サーチ VIP アドレスを入力します。
- [IPv6 アドレス（IPv6 Address）]：IPv6 ループバック アドレスを入力します（`::1`）。
- [ログをシンクホールに接続する（Log Connections to Sinkhole）]：このラジオ ボタンをクリックします。
- [タイプ（Type）]：[なし（None）] を選択します。

ステップ 6 基本 DNS ポリシーを作成します（基本 DNS ポリシーの作成を参照）。

ステップ 7 シンクホールの DNS ルールを追加します（DNS ルールの作成および編集を参照）。

このルールでは、

- [有効（Enabled）] チェックボックスをオンにします。
- [アクション（Action）] ドロップダウン リストから [シンクホール（Sinkhole）] を選択します。
- [シンクホール（Sinkhole）] ドロップダウン リストから、作成したシンクホール オブジェクトを選択します。

- 作成したカスタム DNS リストを [DNS] タブの [選択した項目（Selected Items）] リストに追加します。
- （オプション）[ネットワーク（Networks）] タブでネットワークを選択し、コンテンツ制限を特定のユーザに限定します。たとえば、学生ユーザにコンテンツ制限を限定したい場合、学生を教員とは別のサブネットに割り当て、このルールにそのサブネットを指定します。

ステップ 8 アクセス コントロール ポリシーと DNS ポリシーを関連付けます（アクセス制御への他のポリシーの関連付けを参照）。

ステップ 9 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。