コンテンツ規制

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。このシステムでは、ご使用のネットワーク全体にこれらの機能を拡大できます。

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。

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 クエリの制限状態を、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（Supported devices）	任意（Any）	Secure Firewall 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）	はい	はい
SSL ポリシーが必要（SSL policy required）	はい	非対応
ホストは IPv4 の使用が必要（Hosts must be using IPv4）	非対応	はい
接続イベント ロギング（Connection event logging）	はい	はい

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）]

コンテンツ制限の要件と前提条件

モデルのサポート

すべて、または手順に示されているとおり。

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

コンテンツ制限のガイドラインと制限事項

- セーフサーチは Snort 2 でのみサポートされています。
- YouTube と Google は、アクセス制御ルールに実装された YouTubeEDU 機能をサポートしていません。YouTubeEDU を設定するアクセス制御ルールは完全には機能していないため、削除してください。関連する復号ルールも削除できます。

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

次の手順では、コンテンツを制限するアクセス制御ルールを設定する方法について説明します。

（注） アクセス制御ルールでセーフサーチが有効になっている場合、インライン正規化が自動的に有効になります。

手順

ステップ 1 復号ポリシーを作成します。

ステップ 2 セーフサーチ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 [アクション（Action）] として [復号 - 再署名（Decrypt - Resign）] を選択します。
- [アプリケーション（Applications）] 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。
  - 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。

ステップ 3 追加したルール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。

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、復号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 [アクション（Action）] として [許可（Allow）] を選択します。
- [アプリケーション（Applications）] で、**セーフサーチ**（ ） のアイコンをクリックし、関連する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 （5 ページ）
- [アプリケーション（Applications）] で、[選択済みのアプリケーションとフィルタ（Selected Applications and Filters）] リストのアプリケーション選択を絞り込みます。

  ほとんどの場合、セーフサーチを有効にすると、[選択済みのアプリケーションとフィルタ（Selected Applications and Filters）] リストに適切な値が入力されます。セーフサーチ機能を有効にしたときに、セーフサーチアプリケーションがすでにリストに含まれている場合、リストへの自動入力は行われません。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。
  - 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。

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。

アクセス制御ルールの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。

セーフサーチの有効化
このルールに一致するトラフィックのセーフサーチ フィルタリングを有効にします。

対応していない検索トラフィック
対応していない検索エンジンからのトラフィックを処理する場合は、システム上での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

DNS シンクホールを使用したコンテンツ制限の実施

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 サーバーが含まれる場合、Firewall Threat Defense デバイスをプロキシ サーバー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は適用できません。

始める前に

この手順は Firewall Threat Defense にのみ適用され、IPS ライセンスが必要です。

手順

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 Firewall 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 Secure Firewall 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`）。
- [シンクホールへの接続のログ（Log Connections to Sinkhole）]：[ログ接続（Log Connections）] 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（基本的な 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 ルールの作成と編集を参照）。

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] 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）] 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ーに限定します。たとえば、学生ユーザー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。

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。