SonicOS 7

動作オブジェクト

管理者ガイド

SONICWALL®

目次

1

アプリケーション ルールの動 作

ユーザ定義の動作オブジェクトを作成するか、定義済みの規定の動作の 1 つを選択することができます。

動作オブジェクトを表示するには、「**オブジェクト > 動作オブジェクト > アプリケーション ルールの動作**」に移動します。

名前	動作オブジェクトの名前。
動作種別	動作オブジェクトが提供する動作の種別 (**帯域幅管理**、**パケット監視**など)。
内容	帯域幅管理動作オブジェクトの場合、三角アイコンが表示されます。 ユーザが構成した動作オブジェクトの場合、「**動作オブジェクトの設定**」ダイアログで指定した内容が表示されます。
構成	• **編集**アイコン システムが提供する動作オブジェクトの場合、編集アイコンは淡色表示となり、動作オブジェクトを変更できません。 • **削除**アイコン システムが提供する動作オブジェクトの場合、削除アイコンは淡色表示となり、動作オブジェクトを削除できません。

トピック:

- 動作オブジェクトについて
- 帯域幅管理を用いた動作について
- 動作オブジェクトの作成
- 動作オブジェクトの変更
- パケット監視を使用した動作の関連タスク

動作オブジェクトについて

動作オブジェクトは、一致イベントに対するアプリケーション ルール ポリシーの動作を定義します。ユーザ定義の動作オブジェクトを作成するか、定義済みの規定の動作の 1 つを選択することができます。

トピック:

- システム定義済みの規定の動作オブジェクトについて
- ユーザ定義の動作オブジェクトのタイプについて

システム定義済みの規定の動作オブジェクトについて

SonicOS によってあらかじめ定義されたシステム定義の既定の動作がいくつかあります。これらの規定の動作は編集または削除できません。既定の動作は、「**ポリシー > アプリケーション ルール**」ページでポリシーを追加または編集する際に「**アプリケーション制御ポリシーの追加/編集**」ダイアログに表示されます。

既定の動作オブジェクト

多くの帯域幅管理動作オブジェクト オプションも、あらかじめ定義された既定の動作リストで利用可能です。この帯域幅管理動作オプションは、「**オブジェクト > プロファイル オブジェクト > 帯域幅**」ページの「帯域幅管理種別」の設定によって異なります。

バイパス動作オブジェクト オプションも、既定の動作リストで利用可能です。示されたセキュリティ サービスがファイアウォール上でライセンスされている場合に利用できます。

定義済みの動作タイプについては、下の表を参照してください。帯域幅管理動作の詳細については、「帯域幅管理を用いた動作について」を参照してください。

定義済みの規定の動作オブジェクトについて

動作種別	説明
WAN 帯域幅管理–高	受信と送信帯域幅を管理し、変動可能な値で保証された帯域幅、および利用可能帯域幅全体の最大 100%までの最大/バースト帯域幅使用

	率の設定が可能です。事前定義
動作なし	動作を指定しないでポリシーを指定することができます。これで「ログのみ」のポリシー種別を使用できます。
DPI をバイパス	精密パケット検査コンポーネントの IPS、GAV、アンチスパイウェア、およびアプリケーション制御をバイパスします。この動作は、トリガーされた直後から接続期間全体にわたって維持されます。アプリケーション制御検査用にバイパスされることのない FTP 制御チャンネルに対しては特殊な操作が適用されます。この動作は、FTP データ チャンネルの適切な処理をサポートします。DPI のバイパスでは、「**ネットワーク > ファイアウォール > SSL 制御**」ページで有効化されたフィルタの停止が行われません。
パケット監視	SonicOS のパケット監視機能を使用して、セッション内の着信パケットと発信パケットを監視するか、ミラーリングが構成されている場合はパケットを別のインターフェースにコピーします。キャプチャ結果は WireShark で表示や分析ができます。
高度な帯域幅管理 – 高	受信と送信帯域幅を管理し、変動可能な値で保証された帯域幅、および利用可能帯域幅全体の最大 100%までの最大/バースト帯域幅使用率の構成が可能で、優先順位 1 に設定されています。
高度な帯域幅管理 – 中	受信と送信帯域幅を管理し、変動可能な値 (既定は50%) で保証された帯域幅、および利用可能帯域幅全体の最大 100%までの最大/バースト帯域幅使用率の構成が可能で、優先順位 4 に設定されています。
高度な帯域幅管理 – 低	受信と送信帯域幅を管理し、変動可能な値 (既定は20%) で保証された帯域幅、および利用可能帯域幅全体の最大 100%までの最大/バースト帯域幅使用率の構成が可能で、優先順位 6 に設定されています。
GAV をバイパス	ポリシーに一致するトラフィックのゲートウェイ アンチウィルス検査をバイパスします。この動作は、トリガーされた直後から接続期間全体にわたって維持されます。アプリケーション制御検査用にバイパスされることのない FTP 制御チャンネルに対しては特殊な操作が適用されます。この動作は、FTP データ チャンネルの適切な処理をサポートします。
IPS をバイパス	ポリシーに一致するトラフィックの 侵入防御サービス検査をバイパスします。この動作は、トリガーされた直後から接続期間全体にわたって維持されます。アプリケーション制御検査用にバイパスされることのない FTP 制御チャンネルに対しては特殊な操作が適用されます。この動作は、FTP データ チャンネルの適切な処理をサポートします。
SPY をバイパス	ポリシーに一致するトラフィックのアンチスパイウェア検査をバイパスします。この動作は、トリガーされた直後から接続期間全体にわたって維持されます。アプリケーション制御検査用にバイパスされることのない FTP 制御チャンネルに対しては特殊な操作が適用されます。この動作は、FTP データ チャンネルの適切な処理をサポートします。
キャプチャ ATP をバイパス	マルウェアではないことが確実なファイルについて Capture Advanced Threat Protection (ATP) の分析をスキップする場合に使用できます。この動作は、トリガーされた直後から接続期間全体にわたって維持されます。 このオプションを選択しても、GAV やクラウド アンチウィルスのような他のアンチ脅威コンポーネントによるファイルの判定はスキップされません。

ユーザ定義の動作オブジェクトのタイプについて

ユーザ定義の動作オブジェクトを作成するために使用できる**動作**タイプは、「**動作オブジェクトの設定**」ダイアログに表示されます。このダイアログは「**オブジェクト > 動作オブジェクト > アプリ ルール動作**」ページ上部の「**追加**」をクリックすると表示されます。

動作種別の説明については、下の表を参照してください。

ⓘ **補足:** ユーザ定義動作オブジェクトは、「**動作オブジェクトの設定**」ダイアログで作成できます。既定の定義済み動作オブジェクトは、編集または削除できません。ポリシーを作成する場合、「**動作オブジェクトの設定**」ダイアログでは、あらかじめ定義されている動作や定義したカスタマイズ済み動作を選択できます。

ユーザ定義の動作オブジェクトの動作タイプ

動作種別	説明
SMTP 電子メールを遮断 — エラー応答の送信	SMTP 電子メールを遮断し、カスタマイズされたエラーメッセージを送信者に通知します。
電子メール添付ファイルを無効化 — テキストの追加	電子メールの添付ファイルを無効にし、カスタマイズされたテキストを追加します。
電子メール — テキストの追加	電子メールの末尾に個別テキストを追加します。
FTP 通知の応答	接続を終了せずに FTP 制御チャンネルを介してクライアントにテキストを返します。
HTTP 遮断ページ	個別 HTTP 遮断ページを設定できます。色も選択できます。
HTTP リダイレクト	HTTP リダイレクト機能を提供します。例えば、Google ウェブ サイトにユーザをリダイレクトする場合は、カスタマイズ可能な部分を *http://www.google.com* のように設定します。フォームが開いているブラウザにアプリケーション制御から HTTP リダイレクトが送信されると、フォーム内の情報は失われます。
帯域幅管理	アクセス ルール BWM ポリシー定義と同じセマンティ

クスを持つ帯域幅管理制限を定義できます。

優先順位 0 の設定は、最高優先順位です。すべての帯域幅管理レベルに対する保証帯域幅の合計は、100% を超えることはできません。

帯域幅管理を用いた動作について

アプリケーション層帯域幅管理（BWM）を利用すると、プロトコル内の特定のファイル タイプに対しては帯域幅の消費を制限する一方で、それ以外のファイル タイプに対しては帯域幅を無制限に使用するポリシーを作成できます。これにより、同じプロトコル内で好ましいトラフィックと好ましくないトラフィックを区別できます。アプリケーション層帯域幅管理は、すべてのアプリケーション一致や、HTTP クライアント、HTTP サーバ、個別、および FTP ファイル転送の種別を使用する個別アプリケーション ルール ポリシーでサポートされます。ポリシーの種別に関する詳細は、「**ポリシー > アプリケーション ルール > アプリケーション ルールの追加**」セクションを参照してください。

ベスト プラクティスとして、「**オブジェクト > プロファイル オブジェクト > 帯域幅**」ページのグローバル帯域幅管理の設定は、常にいかなる帯域幅管理ポリシーの設定よりも前に行う必要があります。

「動作オブジェクト」ページと帯域幅管理種別

アプリケーション層の帯域幅管理の設定は、アクセス ルールの帯域幅管理の設定と同じ方法で処理されます。しかしながら、アクセス ルールではできないすべての内容種別を指定することが、アアプリケーション ルールでは可能です。

帯域幅管理の使用事例として、管理者が就業時間内の .mp3 および実行可能ファイルのダウンロードを 1Mbps を超えないように制限する場合があります。同時に、.doc や .pdf など、業務との関連性の高いファイル種別のダウンロードについては、利用可能な最大帯域幅まで許可し、場合によっては業務との関連性の高いコンテンツのダウンロードに可能な限り最高の優先順位を与えたい場合もあります。もう 1 つの例として、特定の種別のピアツーピア（P2P）トラフィックには帯域幅制限をかける一方で、その他の種別の P2P には制限なしの帯域幅を許可したい、というケースがあります。アプリケーション層の帯域幅管理により、これらを実施するポリシーを作成することが可能になります。

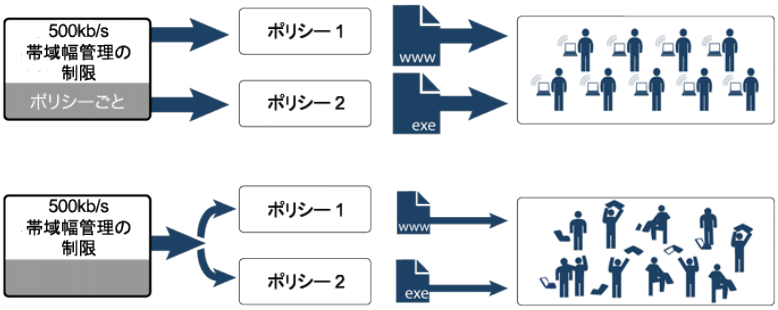
多くの帯域幅管理動作オプションも、あらかじめ定義された既定の動作リストで利用可能です。この帯域幅管理動作オプションは、「**オブジェクト > プロファイル オブジェクト帯域幅**」ページの「帯域幅管理種別」の設定によって異なります。

ⓘ | **補足:** すべての帯域幅管理レベルに対する保証帯域幅の合計は、100% を超えることはできません。

帯域幅管理方式

帯域幅管理機能は、次の 2 つの方法で実装できます。

帯域幅管理: 実装方法



- **ポリシーごとの方法** – ポリシーで指定した帯域幅制限がポリシーごとに個別に適用されます。
  例: 2 つのポリシーがそれぞれ独立して 500 (KB/秒) の制限を受けるとき、この 2 つのルールによる可能な合計の帯域幅は 1000 (KB/秒) となります。
- **動作ごとの総計による方法** – 帯域幅制限の動作が適用対象のすべてのポリシーに (共用的に) 適用されます。
  例: 2 つのポリシーが 500 (KB/秒) の帯域幅管理の制限を共用するとき、合計の帯域幅は 500 (KB/秒) に制限されます。

帯域幅管理動作オブジェクト情報の表示

帯域幅管理動作オブジェクトに関する情報を表示するには、動作オブジェクトの三角アイコンをクリックします。帯域幅管理の詳細が表示されます。

動作オブジェクトの作成

SonicOS には、規定のあらかじめ定義されている動作オブジェクトがあります。これについては、「システム定義済みの規定の動作オブジェクトについて」を参照してください。これらの動作オブジェクトは、変更や削除ができません。

あらかじめ定義された動作を使用しない場合は、新しい動作オブジェクトを構成します。以下に示す「**動作オブジェクトの設定**」ダイアログでは、設定可能な動作をテキストまたは URL を使用してカスタマイズできます。「**動作**」ドロップダウン リストで使用可能な動作タイプを選択できます。あらかじめ定義された動作に加え、これまでに作成した設定可能な動作も、アプリケーション ルール ポリシーの作成時に選択肢として表示されます。

動作オブジェクトを構成するには、以下の手順に従います:

1. 「**オブジェクト > 動作オブジェクト > アプリケーション ルールの動作**」に移動します。
2. ページの上部にある「 **追加**」を選択します。
3. 「**動作オブジェクトの設定**」ダイアログの「**動作名**」フィールドに、わかりやすい動作名を入力します。
4. 「**動作**」ドロップダウン メニューで、目的の動作タイプを選択します。
5. 「**内容**」フィールドに、動作で使用するテキストまたは URL を入力します。
6. 「**HTTP 遮断ページ**」を動作タイプとして選択すると、オプション項目が変わります。
    a. 「**内容**」フィールドに、ページが遮断された場合に表示する内容を入力します。
    b. 「**色**」ドロップダウン メニューから遮断ページの背景色を選択します。
        - 白
        - 黄
        - 赤
        - 青
    c. 遮断ページ メッセージのプレビューを表示するには、「**プレビュー**」ボタンを選択します。
7. 「**帯域幅管理**」を動作タイプとして選択すると、オプション項目が変わります。これらのオプションの設定方法については、「帯域幅管理を用いた動作について」を参照してください。
8. 「**OK**」をクリックします。

動作オブジェクトの変更

ユーザが構成した個別動作オブジェクトは変更することができます。システム定義済みの既定の動作オブジェクトは変更できません。

動作オブジェクトを変更するには、以下の手順に従います

1. 「**オブジェクト > 動作オブジェクト > アプリ ルール動作**」に移動します。
2. 変更するオブジェクトにマウス カーソルを重ね、**編集**アイコンをクリックします。「**動作オブジェクトの設定**」ダイアログが表示されます。
3. 「動作オブジェクトの作成」セクションの**ステップ 3** から**ステップ 8** を実行してください。

パケット監視を使用した動作の関連タスク

事前定義済みのパケット監視動作がポリシーに対して選択されている場合、SonicOS は「**監視 > ツールと監視 > パケット**」ページで構成した設定に応じてトラフィックをキャプチャまたはミラーします。既定では、Wireshark™ で参照可能なキャプチャ ファイルを作成します。Wireshark に関する詳細は、「**ポリシー > アプリケーション制御**」の章を参照してください。

パケット監視動作を用いてポリシーを構成した後、実際にパケットをキャプチャするために、「**パケット**」ページで「**キャプチャの開始**」を選択する必要があります。欲しいパケットをキャプチャした後で、「**ミラーの停止**」を選択します。

ポリシーに関連するパケットのキャプチャ

ポリシーに関連するパケットのみをキャプチャするようにパケット監視動作を制御するには、以下の手順に従います。

1. 「**監視 > ツールと監視 > パケット監視**」ページに移動します。

2. 「**一般**」ボタンをクリックします。

3. 「**一般**」ダイアログで、「**監視フィルタ**」をクリックします。

4. 「**ファイアウォール/アプリケーション ルールによるフィルタを有効にする**」を選択します。このオプションは、既定では選択されていません。

   このモードでは、「**パケットのキャプチャ**」ページで「**キャプチャの開始**」オプションをクリックした後で、トラフィックがアプリケーション制御ポリシー（またはアクセス ルール）を始動させるまではパケットはキャプチャされません。ポリシーがトリガされると、「**監視 > ログ > システム イベント**」ページで警告メッセージを確認できます。

   これは、パケット監視の動作タイプを持つアクション オブジェクト、またはパケット監視を使用する「**ポリシー > アクセス ルール**」で作成されたポリシーを使用して作成されたアプリケーション ルール ポリシーで機能し、キャプチャまたはミラーリング対象の設定またはフィルタリングを指定できます。例えば、キャプチャを異なる形式でダウンロードして、ブラウザ内で参照できます。
5. 「**保存**」をクリックします。

ミラーリングの設定

ミラーリングを設定するには、以下の手順に従います:

1. 「**監視 > ツールと監視 > パケット監視**」ページに移動します。

2. 「**一般**」ボタンをクリックします。
3. 「**一般**」ウィンドウで、「**ミラー**」をクリックします。

4. 「**ローカル ミラー設定**」の下の「**フィルタされたパケットをインターフェースにミラーする**」ドロップダウン メニューからでミラーされたパケットを送信する先のインターフェースを選択します。
5. また、**リモート**設定のうち 1 つを構成できます。これにより、アプリケーション パケットを別のコンピュータにミラーしてすべてをハードディスク上に保存することが可能です。例えば、MSN インスタント メッセンジャー トラフィックをキャプチャして会話を読むことができます。
6. 「**保存**」をクリックします。

2

コンテンツ フィルタの動 作

SonicWall コンテンツ フィルタ サービス (CFS) では、教育機関、企業、図書館、政府機関向けにコンテンツ フィルタが強化されています。こうした組織では、コンテンツ フィルタ オブジェクトの活用により、ウェブサイトを制御したり、学生や従業員が IT 部門から支給されたコンピュータを使用して組織のファイアウォールの背後からのアクセスを行ったりできるようになります。

ⓘ **補足:** 古いバージョンから CFS 4.0 へのアップグレードについては、『*SonicWallコンテンツ フィルタ サービス アップグレード ガイド*』を参照してください。また、これらのオブジェクトを CFS ポリシーに適用するには、「*SonicOS セキュリティ サービス*」の「*ポリシー > セキュリティ サービス > コンテンツ フィルタ*」セクションを参照してください。

トピック:

- コンテンツ フィルタ オブジェクトについて
- CFS 動作オブジェクトの管理
- コンテンツ フィルタ オブジェクトの適用

コンテンツ フィルタ オブジェクトについて

CFS は、セキュリティ保護されるオブジェクトをコンテンツのフィルタ処理に使用します。セキュア オブジェクトとその使用方法については、『*SonicOS システム セットアップ*』ドキュメントの「*ネットワーク > インターフェース*」の下にある「SonicOS セキュア オブジェクト」セクションを参照してください。CFS は、以下のオブジェクトをコンテンツのフィルタ処理に使用します。

- CFS 動作オブジェクト – 「CFS 動作オブジェクトについて」を参照してください

「**CFS デフォルト アクション**」および「**CFS デフォルト プロファイル**」以外のオブジェクトは、SonicOS によって作成、追加、編集、または削除できます。

パスフレーズ機能と確認 (規約) 機能も、コンテンツ フィルタ オブジェクト内で構成されます。パスフレーズ機能は、ユーザが正しいパスフレーズまたはパスワードを入力しない限り、ウェブ アクセスを制限します。確認機能は、ユーザがウェブ サイトに進むことを確認しない限り、ウェブ アクセスを制限します。次を参照してください。

- パスワード機能について
- 確認機能について

SonicOS は、すべての種類のコンテンツ フィルタ オブジェクトについて、その作成時に UUID (Universally Unique Identifier) を自動的に生成してバインドします。詳細は、「CFS オブジェクトの UUID について」を参照してください。

CFS 動作オブジェクトについて

CFS 動作オブジェクトは、パケットが CFS によってフィルタリングされた後の動作を定義し、CFS ポリシーと一致します。

パスワード機能について

パスワード機能は、確認機能と連携し、パスワードに基づいてウェブへのアクセスを制限します。禁止 URI リストの特別な URI 種別またはドメインを考慮して、パスワード操作を構成することができます。禁止された URI にアクセスするには、正しいパスワードを入力するように求められます。そうしないと、ウェブ アクセスがブロックされます。

ⓘ **重要:** パスワードは、HTTP 要求に対してのみ機能します。HTTPS 要求は、「パスワード」ページにはリダイレクトできません。

確認機能については、「確認機能について」を参照してください。

パスワード操作は、次の仕組みで機能します。

1. ユーザが制限されたウェブサイトへのアクセスを試みます。
2. 「パスワード」ページがユーザのブラウザに表示されます。
3. ユーザは、パスフレーズまたはパスワードを入力して送信する必要があります。
4. CFS が送信されたパスフレーズ/パスワードをウェブサイトのパスワードと照合します。
    - パスフレーズ/パスワードが一致すると、ウェブ アクセスは許可されます。これ以上の確認は不要です。確認機能に対して設定されている「動作時間」の間、ユーザは引き続き同じ種別のウェブサイトにアクセスできます。既定値は 60 分です。
    - パスフレーズ/パスワードが一致しない場合、アクセスは遮断され、「遮断」ページがユーザに送信されます。

      ⓘ **補足:** ユーザがパスフレーズ/パスワードを入力できるのは 3 回までです。すべて失敗するとサイトは遮断されます。

    ユーザが「**キャンセル**」を選択すると、サイトは直ちに遮断されます。

確認機能について

確認機能（規約とも呼ばれます）は、アクセスを許可する前にユーザに確認を求めることにより、ウェブ アクセスを制限します。特別な URI 種別またはドメインを考慮して、確認操作を構成する必要があります。また、ユーザは、こうした URI 種別またはドメインへの最初のアクセス時にウェブ要求の確認を行うことができます。

ⓘ **重要:** 確認は、HTTP 要求に対してのみ機能します。HTTPS 要求は、「確認」（同意）ページにはリダイレクトできません。

確認操作は、次の仕組みで機能します。

1. ユーザが遮断されたウェブサイトへのアクセスを試みます。
2. 確認を要求するポップアップ ダイアログが表示されます。
3. ユーザは「**継続**」または「**閉じる**」を選択すると必要があります。

- ユーザがこの種別のウェブサイトへのアクセスを確認すると、確認の対象となった最初のウェブサイトにリダイレクトされます。これ以上の確認は不要です。確認機能に対して設定されている「動作時間」の間、ユーザは引き続き同じ種別のウェブサイトにアクセスできます。既定値は 60 分です。
- 「**閉じる**」を選択した場合、ユーザには「遮断」ページが表示され、設定されている動作時間の間、その種別のウェブサイトから遮断されます。

CFS オブジェクトの UUID について

SonicOS は、これらのコンテンツ フィルタ オブジェクト/グループについて、その作成時に UUID (Universally Unique Identifier) を自動的に生成してバインドします。

- URI リスト オブジェクト
- URI リスト グループ
- CFS 動作オブジェクト
- CFS プロファイル オブジェクト

SonicOS は、コンテンツ フィルタ ポリシーの作成時にも UUID を生成してバインドします。UUID は、ハイフンで区切られた 5 文字のグループで表示された 32 桁の 16 進数で構成されています。UUID は、オブジェクトの作成時に生成されます。そのオブジェクトを変更したり、ファイアウォールを再起動しても変化しません。UUID は、オブジェクトが削除されると削除され、削除された UUID は再利用されません。UUID は、装置を工場出荷時の既定の設定で再起動すると再生成されます。

既定では、UUID は表示されません。UUID の表示は、内部的な設定によってコントロールされます。内部設定の詳細については、SonicWall テクニカル サポートまでお問い合わせください。

表示状態になると、UUID は各オブジェクト/グループの種別に対応する CFS オブジェクト テーブルに現れます。

CFS オブジェクトは UUID のおかげで次の機能が促進されます。

- 管理インターフェースのグローバル検索機能を使用すると、UUID で CFS オブジェクトを検索できます。
- UUID 付きのオブジェクトが UUID 付きの別のエンティティから参照されている場合、参照カウントと参照元のエンティティを表示するには、CFS オブジェクト上のバルーンにマウス カーソルを重ねます。

  CFS 動作オブジェクト、CFS プロファイル オブジェクト、URI リスト オブジェクト、または URI リスト グループがコンテンツ フィルタ ポリシーで使用されている場合、当該オブジェクトのページ上で「**オブジェクト**」の下にある「コメント」列のバルーンにマウス カーソルを重ねると、参照カウントと参照されるポリシーを表示できます。

CFS 動作オブジェクトの管理

トピック:

- CFS 動作オブジェクト テーブルについて
- CFS 動作オブジェクトの設定
- CFS 動作オブジェクトの編集
- CFS 動作オブジェクトの削除

CFS 動作オブジェクト テーブルについて

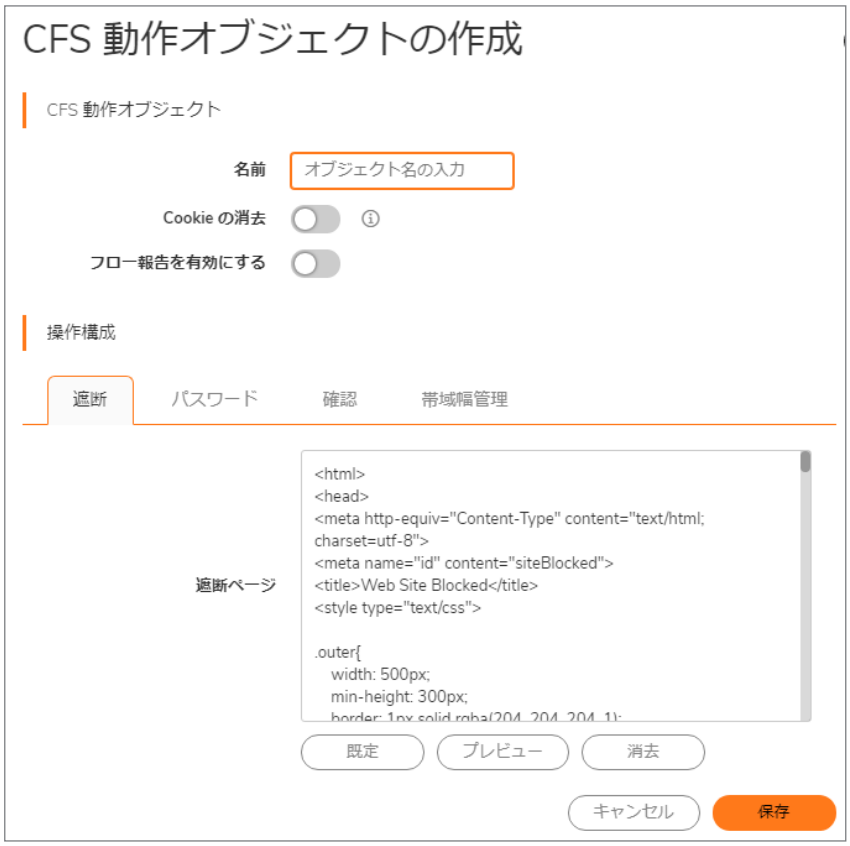
名前	CFS 動作オブジェクトの名前。既定の名前は "**CFS Default Action**" です。既定のオブジェクトは編集可能ですが、削除はできません。
遮断	「遮断」ページが「構成済み」であるかどうかを示します。
パスワード	「パスフレーズ」ページが「構成済み」であるかどうかを示します。
確認	「確認」ページが「構成済み」であるかどうかを示します。
帯域幅管理	「帯域幅管理」ページが「構成済み」であるかどうかを示します。
コメント	CFS 動作オブジェクトの作成中に追加されたコメントを含みます。
UUID	コンテンツ フィルタ オブジェクトおよびグループの自動生成 UUID (Universally Unique Identifier) を含みます。

CFS 動作オブジェクトの設定

既定の CFS 動作オブジェクトである **CFS Default Action** は、SonicOS によって作成されます。この CFS 動作 オブジェクトは、構成および編集は可能ですが、削除することはできません。

CFS 動作オブジェクトを構成するには、以下の手順に従います

1. 「**オブジェクト > 動作オブジェクト > コンテンツ フィルタの動作**」ページに移動します。
2. ページの上部にある「**追加**」を選択します。「**CFS 動作オブジェクト**」ダイアログが表示されます。



3. 「**名前**」フィールドに CFS 動作 オブジェクトの名前を設定します。
4. プライバシーを保護するために Cookie を自動的に削除するには、「**Cookie の消去**」オプションを選択します。このオプションとクライアント DPI-SSL コンテンツ フィルタの両方が有効になっていると、HTTPS サイトの Cookie が削除されます。このオプションは、既定では選択されていません。

   ⓘ **重要:** このオプションを有効にすると、一部の検索エンジンのセーフ サーチ強制機能が侵害されることがあります。
5. AppFlow 監視に URI 情報を送信するには、「**フロー報告を有効にする**」オプションを選択します。このオプションは、既定では選択されていません。
6. サイトが遮断されたときにどのページを表示するかを、以下のように構成できます。

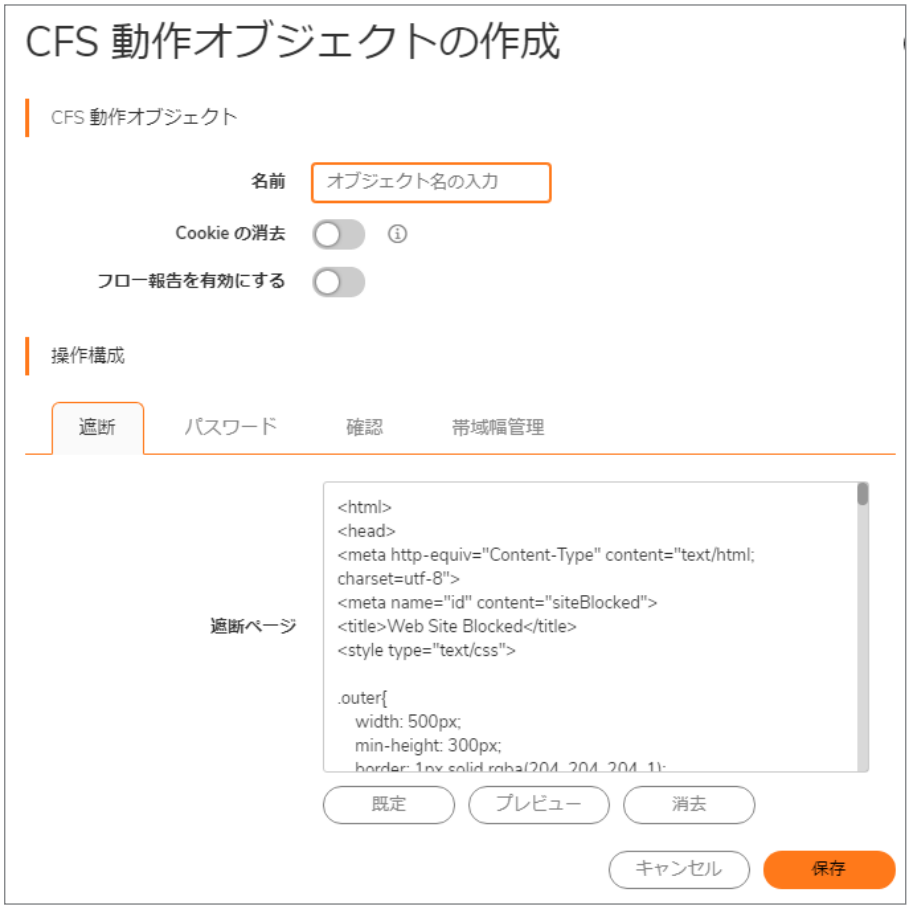
   ⓘ **補足:** これらのページには、既定のバージョンが作成済みです。既定のページを使用するほかに、必要に応じてそれを変更したり、新しいページを作成したりすることができます。

- 会社ポリシー別の遮断サイトの場合は、「遮断オプション」に進みます。
- パスワードで保護されたウェブページの場合は、「パスフレーズ オプション」に進みます。
- ユーザが表示する前に確認が求められる制限ウェブページの場合は、「確認オプション」に進みます。
- 脅威 API 強制による遮断サイトの場合は、「脅威 API オプション」に進みます。

7. 帯域幅リソースを CFS 動作オブジェクトの一部として割り当てることができます。「BWM オプション」を参照してください。
8. 「**保存**」をクリックします。新しい CFS 動作オブジェクトが「CFS 動作オブジェクト」テーブルに追加されます。

遮断オプション

「**CFS 動作オブジェクトの追加**」ダイアログにこの画面が表示されます。ダイアログを開くには、「**オブジェクト > 動作オブジェクト > コンテンツ フィルタの動作**」に移動して、ページ上部の「**追加**」ボタンをクリックします。



サイトが遮断されたときに表示されるページを作成するには、以下の手順に従います

1. 「**操作構成**」で、「**遮断**」タブをクリックします。

既定のページが既に定義されていますが、遮断されたサイトにアクセスしようとしたときにユーザに表示されるウェブ ページは全面的にカスタマイズできます。または、ページを独自に作成することもできます。

2. プレビューを表示するには、「**プレビュー**」ボタンを選択します。
3. 与えられたコードを変更していなければ、「**プレビュー**」ボタンを選択すると既定のウェブ ページが表示されます。遮断ポリシー、クライアント IP アドレス、遮断理由が表示されます。

   「遮断ページ」フィールドからすべてのコンテンツを削除するには、「**消去**」ボタンをクリックします。

   既定の遮断ページ メッセージに戻すには、「**既定**」ボタンをクリックします。

パスフレーズ オプション

ⓘ | **補足:** パスフレーズ機能については、「パスワード機能について」を参照してください。

「**CFS 動作オブジェクトの追加**」ダイアログにこの画面が表示されます。ダイアログを開くには、「**オブジェクト > 動作オブジェクト > コンテンツ フィルタの動作**」ページに移動して、ページ上部の「**追加**」ボタンをクリックします。

パスワードで保護されたウェブ ページを作成するには、以下の手順に従います

1. 「**操作構成**」で、「**パスワード**」タブをクリックします。

2. 「**パスワードの入力**」フィールドに、ウェブサイトのパスフレーズ/パスワードを入力します。パスワードは最大 64 文字です。
3. 「**パスワードの確認**」フィールドに同じパスフレーズ/パスワードを再入力します。
4. 入力中のパスワードを隠すには、「**パスワードを隠す**」オプションを選択します。このオプションは、既定では選択されています。

   ⓘ **重要:** このオプションの選択を外すと、パスワードが通常の文字のまま表示され、「**パスワードの確認**」フィールドの入力が無効になります。
5. 種別またはドメインに基づくパスフレーズの有効時間を「**動作時間 (分)**」フィールドに入力します。時間の最小値は 1 分、最大値は 9999 分、既定値は **60** 分です。

6. 既定のページが既に定義されていますが、遮断されたサイトにアクセスしようとしたときにユーザに表示されるウェブ ページは全面的にカスタマイズできます。または、ページを独自に作成することもできます。サイトが遮断されたときに表示されるページを作成するには、以下の手順に従います:

   - プレビューを表示するには、「**プレビュー**」ボタンを選択します。
   - 与えられたコードを変更していなければ、「**プレビュー**」ボタンを選択すると既定のウェブ ページが表示されます。ウェブサイトの URL、クライアント IP アドレス、ポリシー、理由、および動作分数が、パスワード入力用フィールドと共に表示されます。

     「パスワード ページ」フィールドからすべてのコンテンツを削除するには、「**消去**」ボタンを選択します。

     既定のパスフレーズ ページ メッセージに戻すには、「**既定**」ボタンをクリックします。

確認オプション

ⓘ **補足:** 確認（同意）の要求は、HTTP 要求に対してのみ機能します。HTTPS 要求は、「確認」ページにはリダイレクトできません。詳細については、「確認機能について」を参照してください。

「**CFS 動作オブジェクトの追加**」ダイアログにこの画面が表示されます。ダイアログを開くには、「**オブジェクト > 動作オブジェクト > コンテンツ フィルタの動作**」ページに移動して、ページ上部の「**追加**」ボタンをクリックします。

ユーザが表示する前に確認が求められる制限ウェブ ページを作成するには、以下の手順に従います:

1. 「**操作構成**」で、「**確認**」タブをクリックします。

2. 種別またはドメインに基づく確認済みユーザの有効時間を「**動作時間 (分)**」フィールドに入力します。時間の最小値は 1 分、最大値は 9999 分、既定値は **60** 分です。
3. 既定のページが既に定義されていますが、確認サイトにアクセスしようとしたときにユーザに表示されるウェブ ページは全面的にカスタマイズできます。または、ページを独自に作成することもできます。
   - プレビューを表示するには、「**プレビュー**」ボタンを選択します。
   - 与えられたコードを変更していなければ、「**プレビュー**」ボタンを選択すると既定のウェブ ページが表示されます。ウェブサイトの URL、クライアント IP アドレス、遮断ポリシー、および遮断の理由が、確認入力用フィールドと共に表示されます。

     「確認ページ」フィールドからすべてのコンテンツを削除するには、「**消去**」ボタンを選択します。

     既定の遮断ページ メッセージに戻すには、「**既定**」ボタンをクリックします。

BWM オプション

ⓘ **重要:** CFS 動作帯域幅オブジェクトは、「**オブジェクト > プロファイル オブジェクト > 帯域幅**」ページで作成される帯域幅オブジェクトと似ていますが、同じものではありません。CFS 動作帯域幅管理オブジェクトは、「**オブジェクト > プロファイル オブジェクト > 帯域幅**」ページに表示されません。また、帯域幅管理帯域幅オブジェクトは、「**オブジェクト > 動作オブジェクト > コンテンツ フィルタの動作**」ページに表示されません。

ⓘ **補足:** 帯域幅管理については、「帯域幅管理を用いた動作について」を参照してください。

ⓘ | **重要:** CFS 動作帯域幅オブジェクトを作成するには、帯域幅管理を有効にする必要があります。

「**CFS 動作オブジェクトの追加**」ダイアログにこの画面が表示されます。ダイアログを開くには、「**オブジェクト > 動作オブジェクト > コンテンツ フィルタの動作**」ページに移動して、ページ上部の「**追加**」ボタンをクリックします。

コンテンツ フィルタに使う帯域幅リソースを割り当てるには、以下の手順に従います

1. 「**操作構成**」で、「**帯域幅管理**」タブをクリックします。

2. 「**帯域幅統合方式**」ドロップダウン メニューから、BWM オブジェクトを適用する方法を選択します。
   - ポリシー毎 (既定)
   - 動作毎
3. 送信トラフィックで BWM を有効にするには、「**送信帯域幅管理を有効にする**」オプションをオンにします。このオプションは、既定では選択されていません。
   「**帯域幅オブジェクト**」ドロップダウン メニューと「**帯域幅使用状況の追跡を有効にする**」オプションが有効になります。
   a. 「**帯域幅オブジェクト**」ドロップダウン メニューで、次のどちらかを選択します。
      - 既存の BWM オブジェクト。
      - 「帯域幅オブジェクトの作成」。「帯域幅オブジェクトの追加」ダイアログが表示されます。帯域幅オブジェクトの新規作成に関する詳細は、「**オブジェクト > プロファイル オブジェクト > 帯域幅**」の章を参照してください。
4. 受信トラフィックで BWM を有効にするには、「**受信帯域幅管理を有効にする**」オプションをオンにします。このオプションは、既定では選択されていません。
   「帯域幅オブジェクト」ドロップダウン メニューが有効になります。
   a. 「**帯域幅オブジェクト**」ドロップダウン メニューで、次のどちらかを選択します。
      - 既存の BWM オブジェクト。
      - 「帯域幅オブジェクトの作成」。「帯域幅オブジェクトの追加」ダイアログが表示されます。帯域幅オブジェクトの新規作成に関する詳細は、「**オブジェクト > プロファイル オブジェクト > 帯域幅**」の章を参照してください。
5. 帯域幅使用状況を追跡にするには、「**帯域幅使用状況の追跡を有効にする**」オプションをオンにします。このオプションは、既定では選択されていません。

ⓘ **補足:** 「送信帯域幅管理を有効にする」または「受信帯域幅管理を有効にする」（またはこの両方）を選択し、「帯域幅使用状況の追跡を有効にする」オプションを有効にする必要があります。

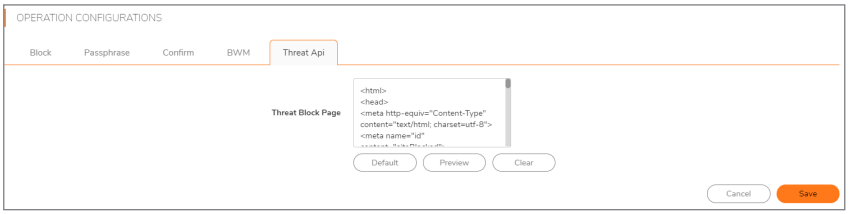
脅威 API オプション

ⓘ | **重要:** 脅威 API は、設定前に有効にする必要があります。

「**CFS 動作オブジェクトの追加**」ダイアログにこの画面が表示されます。ダイアログを開くには、「**オブジェクト > 動作オブジェクト > コンテンツ フィルタの動作**」ページに移動して、ページ上部の「**追加**」ボタンをクリックします。

脅威リストに含まれる URL を遮断するポリシーを追加するには、以下の手順に従います

1. 「**操作構成**」で、「**脅威 API**」タブをクリックします。

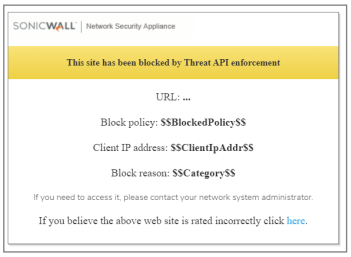


2. 既定のページが既に定義されていますが、遮断されたサイトにアクセスしようとしたときにユーザに表示されるウェブ ページは全面的にカスタマイズできます。または、ページを独自に作成することもできます。サイトが遮断されたときに表示されるページを作成するには、以下の手順に従います:

   - プレビューを表示するには、「**プレビュー**」ボタンを選択します。
   - 与えられたコードを変更していなければ、「**プレビュー**」ボタンを選択すると既定のウェブ ページが表示されます。ウェブサイトの URL、クライアント IP アドレス、遮断ポリシー、および遮断の理由が、確認入力用フィールドと共に表示されます。

     「確認ページ」フィールドからすべてのコンテンツを削除するには、「**消去**」ボタンを選択します。

     既定の確認ページ メッセージに戻すには、「**既定**」ボタンをクリックします。



CFS 動作オブジェクトの編集

CFS 動作オブジェクトを編集するには、以下の手順に従います

1. 「**オブジェクト > 動作オブジェクト > コンテンツ フィルタの動作**」タブに移動します。
2. 編集する CFS 動作 オブジェクトにマウス カーソルを重ね、**編集**アイコンをクリックします。「**CFS 動作オブジェクトの編集**」ダイアログが表示されます。このダイアログは、「**CFS 動作オブジェクトの追加**」ダイアログと同じです。
3. 変更を行うには、「CFS 動作オブジェクトの設定」の適切な手順に従ってください。.

CFS 動作オブジェクトの削除

CFS 動作オブジェクトを削除するには、以下の手順に従います

1. 「**オブジェクト > 動作オブジェクト > コンテンツ フィルタの動作**」ページに移動します。
2. 以下のいずれかを実行します。
    - 動作オブジェクトにマウス カーソルを重ね、「**削除**」アイコンをクリックします。
    - 削除する 1 つ以上の動作オブジェクトのチェックボックスをオンにします。「**削除**」ボタンをクリックします。

コンテンツ フィルタ オブジェクトの適用

コンテンツ フィルタ オブジェクトの設定が終わった後で、オブジェクトをコンテンツ フィルタ ポリシーに適用する必要があります。コンテンツ フィルタの設定は、「**ポリシー > セキュリティ サービス > コンテンツ フィルタ**」ページで行えます（「*セキュリティ サービス*」の「*SonicOSコンテンツ フィルタリング サービスの設定*」セクションを参照）。

3

SonicWall サポート

有効なメンテナンス契約が付属する SonicWall 製品をご購入になったお客様は、テクニカル サポートを利用できます。

サポート ポータルには、問題を自主的にすばやく解決するために使用できるセルフヘルプ ツールがあり、24 時間 365 日ご利用いただけます。サポート ポータルにアクセスするには、次の URL を開きます:
https://www.sonicwall.com/ja-jp/support

サポート ポータルでは、次のことができます。

- ナレッジ ベースの記事や技術文書を閲覧する。
- 次のサイトでコミュニティ フォーラムのディスカッションに参加したり、その内容を閲覧したりする:
  https://community.sonicwall.com/technology-and-support
- ビデオ チュートリアルを視聴する。
- https://mysonicwall.com にアクセスする。
- SonicWall のプロフェッショナル サービスに関して情報を得る。
- SonicWall サポート サービスおよび保証に関する情報を確認する。
- トレーニングや認定プログラムに登録する。
- テクニカル サポートやカスタマー サービスを要請する。

SonicWall サポートに連絡するには、次の URL を開きます: https://www.sonicwall.com/ja-jp/support/contact-support

このドキュメントについて

補足: メモ アイコンは、補足情報があることを示しています。

重要: 重要アイコンは、補足情報があることを示しています。

ヒント: ヒント アイコンは、参考になる情報があることを示しています。

注意: 注意アイコンは、手順に従わないとハードウェアの破損やデータの消失が生じる恐れがあることを示しています。

警告: 警告アイコンは、物的損害、人身傷害、または死亡事故につながるおそれがあることを示します。

SonicOS 動作オブジェクト 管理者ガイド
更新日 – 2021 年 3 月
ソフトウェア バージョン – 7
232-005635-10 Rev A

エンド ユーザ製品利用規約

SonicWall エンド ユーザ製品利用規約を参照する場合は、次に移動してください: https://www.sonicwall.com/ja-jp/legal

オープン ソース コード

SonicWall Inc. では、該当する場合は、GPL、LGPL、AGPL のような制限付きライセンスによるオープン ソース コードについて、コンピュータで読み取り可能なコピーをライセンス要件に従って提供できます。コンピュータで読み取り可能なコピーを入手するには、「SonicWall Inc.」を受取人とする 25.00 米ドルの支払保証小切手または郵便為替と共に、書面によるリクエストを以下の宛先までご送付ください。

General Public License Source Code Request
Attn: Jennifer Anderson
1033 McCarthy Blvd
Milpitas, CA 95035