

# SWAでの実行可能ファイルのダウンロードのブロック

## 内容

---

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[はじめる前に](#)

[設定手順](#)

[ファイル拡張子ブロックの検証](#)

[関連情報](#)

---

## はじめに

このドキュメントでは、実行可能ファイルのダウンロードをブロックするようにSecure Web Appliance(SWA)を設定するプロセスについて説明します。

## 前提条件

### 要件

次の項目に関する知識が推奨されます。

- SWAのグラフィックユーザインターフェイス(GUI)へのアクセス
- SWAへの管理アクセス。

### 使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## はじめる前に

Cisco SWAは、Webコンテンツの(Multipurpose Internet Mail Extensions)MIMEタイプを検査することで、実行可能ファイルのダウンロードを効果的にブロックできます。SWAは、application/x-

msdownload、application/x-msi、およびその他の関連するMIMEタイプなどのファイルタイプを特定することで、実行可能ファイルがユーザに配信されるのを防ぐポリシーを適用します。MIMEタイプの検出に加えて、SWAはファイル拡張子フィルタリング、レピュテーションベースの分析、およびカスタムポリシールールを活用して、不要なダウンロードやリスクのあるダウンロードに対する保護をさらに強化できます。これらの機能により、組織はセキュアなブラウジング環境を維持し、マルウェア感染のリスクを軽減できます。

 ヒント:SWAは、トラフィックが復号されない限り、ファイルのMIMEタイプを特定できません。

application/octet-streamは、ファイルにバイナリデータが含まれていることを示すために使用される汎用MIMEタイプです。ファイルの性質を指定しないため、より特定のMIMEタイプに適合しない任意のファイルに使用できます。このタイプは、通常、実行可能ファイル、インストーラ、および他の非テキストファイルに割り当てられます。これは、Webサーバが正確なタイプを判別できない場合に使用されます。

## 設定手順

ステップ1:WebサイトのカスタムURLカテゴリを作成します。

ステップ1.1.GUIからWeb Security Managerに移動し、Custom and External URL Categoriesを選択します。

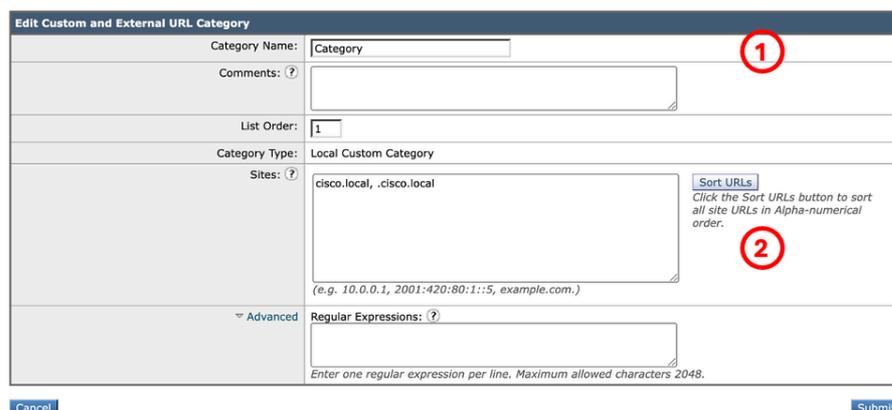
ステップ1.2 : カテゴリの追加をクリックして、新しいカスタムURLカテゴリを作成します。

ステップ1.3:新しいカテゴリの名前を入力します。

ステップ1.4:アップロードトラフィックをブロックするWebサイトのドメインまたはサブドメイン (あるいはその両方) を定義します (この例ではcisco.localとそのすべてのサブドメインです)。

ステップ1.5:変更を送信します。

### Custom and External URL Categories: Edit Category



The screenshot shows the 'Edit Category' form with the following details:

- Category Name:** Category (marked with a red circle 1)
- Comments:** (empty text area)
- List Order:** 1
- Category Type:** Local Custom Category
- Sites:** cisco.local, .cisco.local (marked with a red circle 2)
- Sort URLs:** Click the Sort URLs button to sort all site URLs in Alpha-numerical order.
- Advanced:** Regular Expressions (empty text area)

	<p>イメージ - カスタムURLカテゴリの作成</p> <p> ヒント：カスタムURLカテゴリの設定方法の詳細については、次のサイトを参照してください。  <a href="https://www.cisco.com/c/en/us/support/docs/security/secure-web-appliance-virtual/220557-configure-cu...">https://www.cisco.com/c/en/us/support/docs/security/secure-web-appliance-virtual/220557-configure-cu...</a></p>
<p>ステップ2:URLのトラフィックを復号化します。</p>	<p> 注意：大量のURLを復号化すると、パフォーマンスが低下する可能性があります。</p> <p>ステップ 2.1： GUIから、Web Security Managerに移動し、chooseDecryption Policiesを選択します。</p> <p>ステップ2.2:Add Policyをクリックします。</p> <p>ステップ2.3：新しいポリシーのNameを入力します。</p> <p>ステップ2.4. ( オプション ) このポリシーを適用する必要があるIDプロファイルを選択します。</p> <p> ヒント: ( オプション ) すべてのユーザが認証されていない場合でもポリシーを適用する場合は、All Users (authenticated and unauthenticated users)を選択します。</p> <p>ステップ2.5:FromPolicy Member Definitionセクションで、URL Categorieslinksをクリックして、カスタムURLカテゴリを追加します。</p> <p>ステップ2.6:ステップ1で作成したURLカテゴリを選択します。</p> <p>ステップ2.7:ClickSubmitをクリックします。</p>

## Decryption Policy: DecryptingTraffic

**Policy Settings**

**Enable Policy**

Policy Name:  (e.g. my IT policy) 1

Description:

Insert Above Policy:

Policy Expires:

Set Expiration for Policy

On Date:

At Time:  :

**Policy Member Definition**

Membership is defined by the combination of the following options. All criteria must be met for the policy to take effect.

Identification Profiles and Users:

All Identification Profiles

All Authenticated Users

Selected Groups and Users (?)

Groups: No groups entered

Users: No users entered

All Users (authenticated and unauthenticated users) 2

*If the "All Users" option is selected, at least one Advanced membership option must also be selected. Authentication information may not be available at HTTPS connection time. For transparent proxy traffic, user agent information is unavailable for decryption policies.*

**Advanced**

Use the Advanced options to define or edit membership by proxy port, subnet, Time Range, destination (URL Category), or User Agents.

The following advanced membership criteria have been defined:

**Proxy Ports:** None Selected

**Subnets:** None Selected

**Time Range:** No Time Range Definitions Available (see Web Security Manager > Defined Time Ranges)

**URL Categories:**  2

**User Agents:** None Selected

イメージ：復号化ポリシーの作成

ステップ2.8:InDecryption Policies ページで、新しいポリシーの fromURL Filtering リンクをクリックします。

## Decryption Policies

Policies						
<input type="button" value="Add Policy..."/>						
Order	Group	URL Filtering	Web Reputation	Default Action	Clone Policy	Delete
1	<b>DecryptingTraffic</b> Identification Profile: All All Identified users URL Categories: Category	<span style="border: 1px solid red; border-radius: 50%; padding: 2px;">Monitor: 1</span>	(global policy)	(global policy)		
	<b>Global Policy</b> Identification Profile: All	Monitor: 107 Decrypt: 1	Enabled	Decrypt		

イメージ：URLフィルタリングの選択

ステップ2.9：カスタムURLカテゴリのアクションとして ChooseDecryptを使用します。

ステップ2.10:ClickSubmitをクリックします。

## Decryption Policies: URL Filtering: DecryptingTraffic

**Custom and External URL Category Filtering**

These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.

Category	Category Type	Use Global Settings	Override Global Settings					
			Pass Through	Monitor	Decrypt	Drop	Quota-Based	Time-Based
Category	Custom (Local)	Select all	Select all	Select all	<span style="border: 1px solid red; border-radius: 50%; padding: 2px;">Select all </span>	Select all	(Unavailable)	(Unavailable)

イメージ - アクションとして復号化を設定

ステップ3.1:GUIから、Web Security Managerに移動し、Access Policiesを選択します。

ステップ3.2:Add Policyをクリックします。

ステップ3.3 : 新しいポリシーのNameを入力します。

ステップ3.4. ( オプション ) このポリシーを適用する必要があるIDプロファイルを選択します。

 ヒント: ( オプション ) すべてのユーザが認証されていない場合でもポリシーを適用する場合は、All Users (authenticated and unauthenticated users)を選択します。

ステップ3.5:ポリシーメンバー定義の使用」セクションで、URLカテゴリのリンクをクリックして、カスタムURLカテゴリを追加します。

ステップ3.6:ステップ1で作成したURLカテゴリを選択します。

ステップ3.7:ClickSubmitをクリックします。

ステップ3:実行可能ファイルのブロック

#### Access Policy: Block Exec

**Policy Settings**

Enable Policy

Policy Name:  (e.g. my IT policy) 1

Description:

Insert Above Policy:

Policy Expires:  Set Expiration for Policy

On Date:  MM/DD/YYYY

At Time:  :

**Policy Member Definition**

Membership is defined by the combination of the following options. All criteria must be met for the policy to take effect.

Identification Profiles and Users:

All Authenticated Users

Selected Groups and Users ?

Groups: No groups entered

Users: No users entered

All Users (authenticated and unauthenticated users) 2

*If the "All Users" option is selected, at least one Advanced membership option must also be selected.*

Use the Advanced options to define or edit membership by protocol, proxy port, subnet, Time Range, destination (URL Category), or User Agents.

The following advanced membership criteria have been defined:

**Protocols:** None Selected

**Proxy Ports:** None Selected

**Subnets:** None Selected

**Time Range:** No Time Range Definitions Available (see Web Security Manager > Defined Time Ranges)

**URL Categories:**  2

**User Agents:** None Selected

イメージ - アクセスポリシー

 ヒント：レポート目的のために、他のアクセス/復号化ポリシーと同じではない名前を選択するのが最善です。

ステップ3.8:InAccess Policiesページで、URL FilteringアクションがMonitorに設定されていることを確認します。

ステップ 3.9： Access Policiesページで、新しいポリシーのObjectsからのリンクをクリックします。

#### Access Policies

Policies									
Add Policy...									
Order	Group	Protocols and User Agents	URL Filtering	Applications	Objects	Anti-Malware and Reputation	HTTP ReWrite Profile	Clone Policy	Delete
1	<b>Block Exec</b> Identification Profile: All All identified users URL Categories: Category	(global policy)	Monitor: 1	Monitor: 325	(global policy)	(global policy)	(global policy)		
	<b>Global Policy</b> Identification Profile: All	No blocked items	Monitor: 108	Monitor: 325	No blocked items	Web Reputation: Enabled Secure Endpoint: Enabled Anti-Malware Scanning: Enabled	None		

Edit Policy Order...

イメージ - オブジェクトを選択

イメージ：URLフィルタリングの選択

ステップ 3.10： ドロップダウンメニューから、Define Custom Objects Blocking Settingsの順に選択します。

#### Access Policies: Objects: Block Exec

Edit Objects Blocking Settings	
<input checked="" type="checkbox"/> Use Global Policy Objects Blocking Settings	
<input checked="" type="checkbox"/> Define Custom Objects Blocking Settings	
<input type="checkbox"/> Disable Object Blocking for this Policy	
HTTP/HTTPS Max Download Size:	No Maximum
FTP Max Download Size:	No Maximum
<b>Block Object Type</b>	
Not Defined	
<b>Custom MIME Types</b>	
Block Custom MIME Types:	Not Defined
<input type="button" value="Cancel"/>	<input type="button" value="Submit"/>

イメージ - カスタムオブジェクトを定義

ステップ3.11:ClickExecutable Codeを使用して、ブロックするオブジェクトのタイプを選択します。

ステップ3.12:インストーラをクリックして、ブロックするオブジェクトのタイプを選択します。

ステップ 3.13： また、「カスタムMIMEタイプ」セクションにブロックするファイルのMIMEタイプを入力することもできます。

## Access Policies: Objects: Block Exec

**Edit Objects Blocking Settings**

Define Custom Objects Blocking Settings

**Objects Blocking Settings**

**Object Size**

HTTP/HTTPS Max Download Size:  MB  No Maximum

FTP Max Download Size:  MB  No Maximum

**Block Object Type**

Object and MIME Type Reference

Archives

Inspectable Archives ?

Document Types

Executable Code **1**

Java Applet

UNIX Executable

Windows Executable

Installers **2**

UNIX/LINUX Packages

Media

P2P Metafiles

Web Page Content

Miscellaneous

**Custom MIME Types**

Object and MIME Type Reference

Block Custom MIME Types: application/x-msdownload  
application/x-msdos-program  
application/x-msi **3**

(Enter multiple entries on separate lines. Example: audio/x-mpeg3 or audio/\* are valid entries. Maximum allowed characters 2048.)

Cancel Submit

イメージ : ブロックするオブジェクトの設定

 ヒント:MIMEタイプのリストを表示するには、オブジェクトおよびMIMEタイプのリファレンスをクリックします。

ステップ3.14:送信。

ステップ3.15:変更を確定します。

## ファイル拡張子ブロックの検証

この例では、ユーザが実行可能ファイルをダウンロードしようとする、次の警告ページが表示されます。





## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。