# Web 要求の代行受信

この章で説明する内容は、次のとおりです。


- Web 要求の代行受信の概要 （1 ページ）
- Web 要求の代行受信のためのタスク （1 ページ）
- Web 要求の代行受信のベスト プラクティス （2 ページ）
- Web 要求を代行受信するための Web プロキシ オプション （3 ページ）
- ドメイン マップ （18 ページ）
- Web 要求をリダイレクトするためのクライアント オプション （20 ページ）
- クライアント アプリケーションによる PAC ファイルの使用 （21 ページ）
- FTP プロキシ サービス （24 ページ）
- SOCKS プロキシ サービス （27 ページ）
- Cisco Umbrella シームレス ID （30 ページ）
- 要求の代替受信に関するトラブルシューティング （32 ページ）


## Web 要求の代行受信の概要

Secure Web Applianceは、ネットワーク上のクライアントまたは他のデバイスから転送された要求を代行受信します。

アプライアンスは他のネットワーク デバイスと連携してトラフィックを代行受信します。そのようなデバイスとして、一般的なスイッチ、トランスペアレント リダイレクション デバイス、ネットワーク タップ、およびその他のプロキシ サーバーまたは Secure Web Applianceなどがあげられます。

## Web 要求の代行受信のためのタスク

| 手順 | タスク | 関連項目および手順へのリンク |
|---|---|---|
| ステップ 1 | ベスト プラクティスを検討します。 | • Web 要求の代行受信のベスト プラクティス （2 ページ） |

| 手順 | タスク | 関連項目および手順へのリンク |
|---|---|---|
| ステップ 2 | （任意）以下のネットワーク関連のフォローアップ タスクを実行します。<br>• アップストリーム プロキシを接続および設定する。<br>• ネットワーク インターフェイス ポリシーを設定する。<br>• 透過リダイレクション デバイスを設定する。<br>• TCP/IP ルートを設定する。<br>• VLAN の設定。 | • アップストリーム プロキシ<br>• ネットワーク インターフェイス<br>• トランスペアレント リダイレクションの設定<br>• TCP/IP トラフィック ルートの設定<br>• VLAN の使用によるインターフェイス能力の向上 |
| ステップ 3： | （任意）次の Web プロキシのフォローアップ タスクを実行する。<br>• 転送モードまたは透過モードで動作するように Web プロキシを設定する。<br>• 代行受信するプロトコル タイプに追加のサービスが必要かどうかを決定。<br>• IP スプーフィングの設定。<br>• Web プロキシ キャッシュの管理。<br>• カスタム Web 要求ヘッダーの使用。<br>• 一部の要求に対してプロキシをバイパス。 | • Web 要求を代行受信するための Web プロキシ オプション （3 ページ）<br>• Web プロキシの設定 （4 ページ）<br>• Web 要求を代行受信するための Web プロキシ オプション （3 ページ）<br>• Web プロキシ キャッシュ （8 ページ）<br>• Web プロキシの IP スプーフィング （11 ページ）<br>• Web プロキシのバイパス （14 ページ） |
| ステップ 4： | 以下のクライアント タスクを実行します。<br>• クライアントが Web プロキシに要求をリダイレクトする方法を決定。<br>• クライアントとクライアント リソースの設定。 | • Web 要求をリダイレクトするためのクライアント オプション （20 ページ）<br>• クライアント アプリケーションによる PAC ファイルの使用 （21 ページ） |
| ステップ 5： | （任意）FTP プロキシを有効化して設定します。 | • FTP プロキシ サービス （24 ページ） |

# Web 要求の代行受信のベスト プラクティス

• 必要なプロキシ サービスのみをイネーブルにします。

- Secure Web Applianceで定義されているすべての WCCP サービスに対して、同じ転送方式とリターン方式（L2 または GRE）を使用します。これによって、プロキシ バイパス リストが確実に機能します。
- ユーザーが企業ネットワークの外部から PAC ファイルにアクセスできないことを確認します。これによって、モバイル ワーカーは、企業ネットワーク上にいるときは Web プロキシを使用し、それ以外の場合は Web サーバーに直接接続できます。
- 信頼できるダウンストリーム プロキシまたはロードバランサからの X-Forwarded-For ヘッダーのみが Web プロキシで許可されるようにします。
- 当初は明示的な転送だけを使用していた場合でも、Webプロキシをデフォルトの透過モードのままにしておきます。透過モードでは、明示的な転送要求も許可されます。

# Web 要求を代行受信するための Web プロキシ オプション

単独では、Web プロキシは HTTP（FTP over HTTP を含む）および HTTPS を使用する Web 要求を代行受信できます。プロトコル管理を向上させるために、さらに次のプロキシモジュールを利用できます。

- **FTP プロキシ。**FTP プロキシを使用すると、（HTTP でエンコードされた FTP トラフィックだけでなく）ネイティブ FTP トラフィックを代行受信できます。
- **HTTPS プロキシ。**HTTPS プロキシは HTTPS トラフィックの復号化をサポートしているので、Web プロキシは、暗号化されていない HTTPS 要求をコンテンツ分析のためにポリシーに渡すことができます。

（注） 透過モードでは、HTTPS プロキシがイネーブルでない場合、Web プロキシは透過的にリダイレクトされたすべての HTTPS 要求をドロップします。透過的にリダイレクトされた HTTPS 要求がドロップされた場合、その要求のログ エントリは作成されません。

- **SOCKS プロキシ。**SOCKS プロキシを使用すると、SOCKS トラフィックを代行受信できます。

これらの追加のプロキシのそれぞれが機能するには、Web プロキシが必要です。Web プロキシをディセーブルにすると、これらをイネーブルにできません。

（注） Webプロキシはデフォルトでイネーブルになります。デフォルトでは、他のプロキシはすべてディセーブルになります。

### 関連項目

- FTP プロキシ サービス （24 ページ）

• SOCKS プロキシ サービス （27 ページ）

# Web プロキシの設定

### 始める前に

Web プロキシをイネーブルにします。

**ステップ 1** [セキュリティサービス（Security Services）] > [Webプロキシ（Web Proxy）] を選択します。

**ステップ 2** [設定の編集（Edit Settings）] をクリックします。

**ステップ 3** 必要に応じて基本的な Web プロキシ設定項目を設定します。

| プロパティ | 説明 |
|---|---|
| プロキシを設定する HTTP ポート（HTTP Ports to Proxy） | Web プロキシが HTTP 接続をリッスンするポート |
| キャッシング（Caching） | Web プロキシによるキャッシングをイネーブルにするかディセーブルにするかを指定します。<br>Web プロキシは、パフォーマンスを向上させるためにデータをキャッシュします。 |
| プロキシ モード（Proxy Mode） | • [透過（Transparent）]（推奨）：Web プロキシがインターネット ターゲットを指定できるようにします。このモードでは、Web プロキシは、透過的または明示的に転送された Web 要求を代行受信できます。<br>• [転送（Forward）]：クライアント ブラウザがインターネット ターゲットを指定できるようにします。Web プロキシを使用するように各 Web ブラウザを個々に設定する必要があります。このモードでは、Web プロキシは明示的に転送された Web 要求のみを代行受信できます。 |

| プロパティ | 説明 |
|---|---|
| IP スプーフィング接続タイプ | [プロキシモード（Proxy Mode）] に [透過的（Transparent）] を選択した場合は、IP スプーフィング接続タイプのいずれかを選択します。<br>• [透過的な接続に対してのみ（For Transparent Connections Only）]：透過接続の場合にのみ、IP スプーフィングを設定します。<br>• [すべての接続に対して（For All connections）]：透過的な接続と明示的な接続に IP スプーフィングを設定します。<br>[プロキシモード（Proxy Mode）] に [転送（Forward）] を選択した場合は、[IP スプーフィング接続タイプ（IP Spoofing Connection Type）] は常に [明示的（Explicit）] になります。<br>（注） 選択した IP スプーフィング接続タイプは、ネイティブ FTP、HTTP、および HTTPS のすべてのプロトコルに適用されます。<br>ルーティングポリシーに IP スプーフィングプロファイルを追加するには、次を参照してください。 ルーティングポリシーへのルーティング先と IP スプーフィングプロファイルの追加 |

**ステップ 4** 必要に応じて Web プロキシの詳細設定を完了します。

| プロパティ | 説明 |
|---|---|
| 永続的接続のタイムアウト（Persistent Connection Timeout） | トランザクションが完了し、その他のアクティビティが検出されなかった後に、Web プロキシがクライアントまたはサーバーとの接続を開いたままにしておく最大時間（秒単位）。<br>• **[クライアント側（Client side）]**。クライアントとの接続のタイムアウト値。<br>• **[サーバー側（Server side）]**。サーバーとの接続のタイムアウト値。<br>これらの値を大きくすると、接続が開いたままになっている時間が延長され、接続の開閉に費やされるオーバーヘッドが低減します。ただし、永続的な同時接続の数が最大数に達した場合に Web Proxy が新しい接続を開く機能も低下します。<br>接続を確立して SSL ハンドシェイクを実行した後、クライアント要求がプロキシに送信されない場合、プロキシは永続的な接続タイムアウトを待ってから、クライアントとの接続を停止します。<br>シスコは、デフォルト値を維持することを推奨します。 |
| 使用中接続タイムアウト（In-Use Connection Timeout） | 現在のトランザクションが完了していないときに、Web プロキシがアイドル状態のクライアントまたはサーバーからのデータをさらに待機する最大時間（秒単位）。<br>• **[クライアント側（Client side）]**。クライアントとの接続のタイムアウト値。<br>• **[サーバー側（Server side）]**。サーバーとの接続のタイムアウト値。 |

| プロパティ | 説明 |
| --- | --- |
| 同時永続的接続（サーバー最大数）（Simultaneous Persistent Connections (Server Maximum Number)） | Webプロキシサーバーがサーバーに対して開いたままにする接続（ソケット）の最大数。 |
| クライアントあたりの最大接続数 | クライアントによって開始される同時接続数を、設定した値に制限します。接続数が設定した制限値を超えると、接続がドロップされ、管理者にアラートが送信されます。<br>（注） デフォルトでは、[クライアントあたりの最大接続数（Maximum Connections Per Client）] は無効になっています。<br>制限値を設定するには、[クライアントあたりの最大接続数（Maximum Connections Per Client）] チェックボックスをオンにして、次の手順を実行します。<br>• [接続（Connections）]：許可される同時接続数を入力します。<br>• [除外対象のダウンストリームプロキシまたはロードバランサ（Exempted Downstream Proxy or Load Balancer）]：ダウンストリームプロキシ、ロードバランサ、またはその他のクライアントIPアドレスのIPアドレスを入力します（サブネットまたはホスト名を設定することはできません）。Webプロキシには、この除外リストに含まれる IP アドレスの同時接続の制限が適用されません。 |

| プロパティ | 説明 |
|---|---|
| ヘッダーの生成（Generate Headers） | 要求に関する情報をエンコードするヘッダーを生成して追加します。<br>• **X-Forwarded-For** ヘッダーは、HTTP 要求を発信したクライアントの IP アドレスをエンコードします。<br>（注）<br>• ヘッダーの転送をオン/オフするには、`advancedproxyconfig` CLI コマンドの Miscellaneous オプション「HTTP X-Forwarded-For ヘッダーを通過させますか?（Do you want to pass HTTP X-Forwarded-For headers?）」を使用します。<br>• 明示的な転送アップストリーム プロキシを使用して、プロキシ認証によりユーザー認証やアクセス制御を管理するには、これらのヘッダーを転送する必要があります。<br>• 透過的 HTTPS 要求の場合、アプライアンスは XFF ヘッダーを復号できません。明示的要求の場合、アプライアンスは接続要求で受信される XFF ヘッダーを使用し、SSL トンネル内の XFF を復号しないため、X-Forwarded-For によるクライアント IP アドレスの識別が HTTPS 透過的要求に適用されることはありません。<br>• **Request Side VIA** ヘッダーは、クライアントからサーバーへの要求が通過するプロキシをエンコードします。<br>• **Response Side VIA** ヘッダーは、サーバーからクライアントへの要求が通過するプロキシをエンコードします。 |
| Received ヘッダーの使用（Use Received Headers） | アップストリーム プロキシとして展開された Web プロキシが、ダウンストリーム プロキシから送信された X-Forwarded-For ヘッダーを使用してクライアントを識別できるようにします。Web プロキシは、リストに含まれていない送信元からの X-Forwarded-For ヘッダーの IP アドレスを受け入れません。<br>これをイネーブルにする場合は、ダウンストリーム プロキシまたはロード バランサの IP アドレスが必要です（サブネットやホスト名は入力できません）。 |
| 範囲要求の転送（Range Request Forwarding） | 範囲要求の転送をイネーブルまたはディセーブルにするには、[範囲要求の転送の有効化（Enable Range Request Forwarding）] チェックボックスを使用します。詳細については、Web アプリケーションへのアクセスの管理を参照してください。 |

**ステップ 5** 変更を送信し、保存します。

### 次のタスク

- Web プロキシ キャッシュ （8 ページ）

- トランスペアレント リダイレクションの設定

# Web プロキシ キャッシュ

Webプロキシは、パフォーマンスを向上させるためにデータをキャッシュします。AsyncOS には「セーフ」から「アグレッシブ」の範囲の定義済みキャッシュ モードがあり、またカスタマイズしたキャッシングも使用できます。キャッシュ対象から特定の URL を除外することもできます。これを行うには、そのURLをキャッシュから削除するか、無視するようにキャッシュを設定します。

## Web プロキシ キャッシュのクリア

**ステップ 1** [セキュリティサービス（Security Services）] > [Webプロキシ（Web Proxy）] を選択します。

**ステップ 2** [キャッシュを消去（Clear Cache）] をクリックしてアクションを確定します。

## Web プロキシ キャッシュからの URL の削除

**ステップ 1** CLI にアクセスします。

**ステップ 2** `webcache> evict` コマンドを使用して、必要なキャッシング エリアにアクセスします。

```
example.com> webcache
Choose the operation you want to perform:
- EVICT - Remove URL from the cache
- DESCRIBE - Describe URL cache status
- IGNORE - Configure domains and URLs never to be cached
[]> evict
Enter the URL to be removed from the cache.
[]>
```

**ステップ 3** Enter the URL to be removed from the cache.

（注） URL にプロトコルが含まれていない場合は、URL に `http://` が追加されます（たとえば、`www.cisco.com` は `http://www.cisco.com` となります）。

## Web プロキシによってキャッシュしないドメインまたは URL の指定

**ステップ 1** CLI にアクセスします。

**ステップ 2** `webcache -> ignore` コマンドを使用して、必要なサブメニューにアクセスします。

```
example.com> webcache
Choose the operation you want to perform:
```

```
- EVICT - Remove URL from the cache
- DESCRIBE - Describe URL cache status
- IGNORE - Configure domains and URLs never to be cached
[]> ignore
Choose the operation you want to perform:
- DOMAINS - Manage domains
- URLS - Manage urls
[]>
```

**ステップ 3** 管理するアドレス タイプを入力します（DOMAINS または URLS）。

```
[]> urls
Manage url entries:
Choose the operation you want to perform:
- DELETE - Delete entries
- ADD - Add new entries
- LIST - List entries
[]>
```

**ステップ 4** **add** と入力して新しいエントリを追加します。

```
[]> add
Enter new url values; one on each line; an empty line to finish
[]>
```

**ステップ 5** 以下の例のように、1 行に 1 つずつ、ドメインまたは URL を入力します。

```
Enter new url values; one on each line; an empty line to finish
[]> www.example1.com
Enter new url values; one on each line; an empty line to finish
[]>
```

ドメインまたは URL を指定する際に、特定の正規表現（regex）文字を含めることができます。DOMAINS オプションでは、前にピリオドを付けることで、キャッシュ対象からドメインとそのサブドメイン全体を除外できます。たとえば、google.com ではなく、.google.com と入力すると、www.google.com、docs.google.com などを除外することができます。

URLS オプションでは、正規表現文字の全一式を使用できます。正規表現の使用方法については、正規表現を参照してください。

**ステップ 6** 値の入力を終了するには、メイン コマンドライン インターフェイスに戻るまで Enter キーを押します。

**ステップ 7** 変更を保存します。

## Web プロキシのキャッシュ モードの選択

**ステップ 1** CLI にアクセスします。

**ステップ 2** advancedproxyconfig -> caching コマンドを使用して、必要なサブメニューにアクセスします。

```
example.com> advancedproxyconfig
Choose a parameter group:
- AUTHENTICATION - Authentication related parameters
- CACHING - Proxy Caching related parameters
```

```
- DNS - DNS related parameters
- EUN - EUN related parameters
- NATIVEFTP - Native FTP related parameters
- FTPOVERHTTP - FTP Over HTTP related parameters
- HTTPS - HTTPS related parameters
- SCANNING - Scanning related parameters
- PROXYCONN - Proxy connection header related parameters
- CUSTOMHEADERS - Manage custom request headers for specific domains
- MISCELLANEOUS - Miscellaneous proxy related parameters
- SOCKS - SOCKS Proxy parameters
[]> caching
Enter values for the caching options:
The following predefined choices exist for configuring advanced caching
options:
1. Safe Mode
2. Optimized Mode
3. Aggressive Mode
4. Customized Mode
Please select from one of the above choices:
[2]>
```

**ステップ 3** 必要な Web プロキシ キャッシュ設定に対応する番号を入力します。

| 入力 | モード | 説明 |
|---|---|---|
| 1 | セーフ | 他のモードと比較して、キャッシングが最も少なく、RFC #2616 には最大限準拠します。 |
| 2 | 最適化 | キャッシングと RFC #2616 への準拠が適度です。セーフ モードと比較した場合、Last-Modified ヘッダーが存在するときにキャッシング時間が指定されていない場合に、最適化モードでは Web プロキシがオブジェクトをキャッシュします。Web プロキシは、ネガティブ応答をキャッシュします。 |
| 3 | アグレッシブ | キャッシングが最も多く、RFC #2616 への準拠は最小限です。最適化モードと比較した場合、アグレッシブ モードでは、認証済みコンテンツ、ETag の不一致、および Last-Modified ヘッダーのないコンテンツがキャッシュされます。Web プロキシは非キャッシュ パラメータを無視します。 |
| 4 | カスタマイズド モード | 各パラメータを個々に設定します。 |

**ステップ 4** オプション 4（カスタマイズ モード）を選択した場合は、各カスタム設定の値を入力します（または、デフォルト値のままにします）。

**ステップ 5** メイン コマンド インターフェイスに戻るまで、Enter キーを押します。

**ステップ 6** 変更を保存します。

### 次のタスク

### 関連項目

- Web プロキシ キャッシュ （8 ページ）。

# Web プロキシの IP スプーフィング

デフォルトでは、Webプロキシは要求を転送する際に、自身のアドレスに合わせて要求の送信元 IP アドレスを変更します。これによってセキュリティは強化されますが、IP スプーフィングを実装してこの動作を変更し、 Secure Web Applianceからではなく、要求がクライアント IP やその他のルーティング可能なカスタム IP アドレスから発信されたように見せることができます。Web プロキシ IP スプーフィングを設定するには、カスタム IP アドレスの IP スプーフィングプロファイルを作成し、それらをルーティングポリシーに追加します。

IP スプーフィングは、透過的または明示的に転送されたトラフィックに対して機能します。Webプロキシが透過モードで展開されている場合は、透過的にリダイレクトされた接続のみ、またはすべての接続（透過的にリダイレクトされた接続と明示的に転送された接続）に対して（IP スプーフィング接続タイプを設定できる）ことができます。明示的に転送された接続で IP スプーフィングを使用する場合は、リターンパケットを Secure Web Applianceにルーティングする適切なネットワークデバイスがあることを確認してください。

IP スプーフィングがイネーブルで、アプライアンスが WCCP ルータに接続されている場合は、2 つの WCCP サービス（送信元ポートに基づくサービスと宛先ポートに基づくサービス）を設定する必要があります。

IP スプーフィングプロファイルには、HTTPS トラフィックが透過的にリダイレクトされる場合の制限があります。URL カテゴリ基準を使用しているルーティング ポリシーによる HTTPS サイトへのアクセス を参照してください。

### 関連項目

- IP スプーフィングプロファイルの作成 （11 ページ）
- Web プロキシの設定 （4 ページ）
- WCCP サービスの設定

## IP スプーフィングプロファイルの作成

### 始める前に

Web プロキシ設定でプロキシモードと IP スプーフィング接続タイプが選択されていることを確認します。詳細については、Web プロキシの設定 （4 ページ）を参照してください。

**ステップ 1** [Web Security Manager] > [IP スプーフィングプロファイル（IP Spoofing Profiles）] を選択します。
**ステップ 2** [プロファイルを追加（Add Profile）] をクリックします。
**ステップ 3** IP スプーフィングプロファイルの名前を入力します。
**ステップ 4** スプーフィングプロファイル名に割り当てる IP アドレスを入力します。
**ステップ 5** 変更を送信し、保存します。

### 次のタスク

IP スプーフィングプロファイルをルーティングポリシーに追加します。詳細については、ルーティングポリシーへのルーティング先と IP スプーフィングプロファイルの追加を参照してください。

### 関連トピック

IP スプーフィングプロファイルの編集 （12 ページ）
IP スプーフィングプロファイルの削除 （12 ページ）

## IP スプーフィングプロファイルの編集

（注） IP スプーフィングプロファイルを更新すると、そのプロファイルに関連付けられているすべてのルーティングポリシーでそのプロファイルが更新されます。

**ステップ 1** [Web Security Manager] > [IP スプーフィングプロファイル（IP Spoofing Profiles）] を選択します。
**ステップ 2** 編集する IP スプーフィングプロファイル名のリンクをクリックします。
**ステップ 3** プロファイルの詳細を変更します。
**ステップ 4** 変更を送信し、保存します。

## IP スプーフィングプロファイルの削除

**ステップ 1** [Web Security Manager] > [IP スプーフィングプロファイル（IP Spoofing Profiles）] を選択します。
**ステップ 2** 削除する IP スプーフィングプロファイルに対応するゴミ箱アイコンをクリックします。

（注） 削除しようとしている IP スプーフィングプロファイルが 1 つ以上のルーティングポリシーに割り当てられている場合は、アプライアンスによって警告が表示されます。この場合は、影響を受けるすべてのルーティングポリシーに割り当てる別の IP スプーフィングプロファイルを選択します。

**ステップ 3** 変更を送信し、保存します。

# Web プロキシのカスタム ヘッダー

特定の発信トランザクションにカスタムヘッダーを追加することにより、宛先サーバーによる特別な処理を要求できます。たとえば、YouTube for Schools と関係がある場合、カスタム ヘッダーを使用して、YouTube.com へのトランザクション要求を自身のネットワークから発信された、特別な処理を必要とする要求として識別させることができます。

# Web 要求へのカスタム ヘッダーの追加

**ステップ 1** CLI にアクセスします。

**ステップ 2** `advancedproxyconfig -> customheaders` コマンドを使用して、必要なサブメニューにアクセスします。

```
example.com> advancedproxyconfig
Choose a parameter group:
- AUTHENTICATION - Authentication related parameters
- CACHING - Proxy Caching related parameters
- DNS - DNS related parameters
- EUN - EUN related parameters
- NATIVEFTP - Native FTP related parameters
- FTPOVERHTTP - FTP Over HTTP related parameters
- HTTPS - HTTPS related parameters
- SCANNING - Scanning related parameters
- PROXYCONN - Proxy connection header related parameters
- CUSTOMHEADERS - Manage custom request headers for specific domains
- MISCELLANEOUS - Miscellaneous proxy related parameters
- SOCKS - SOCKS Proxy parameters
[]> customheaders
Currently defined custom headers:
Choose the operation you want to perform:
- DELETE - Delete entries
- NEW - Add new entries
- EDIT - Edit entries
[]>
```

**ステップ 3** 次のように、必要なサブコマンドを入力します。

| オプション | 説明 |
|---|---|
| [削除（Delete）] | 指定するカスタム ヘッダーを削除します。コマンドで返されたリストのヘッダーに関連付けられている番号を使用して削除するヘッダーを指定します。 |
| [新規（New）] | 指定するドメインの使用に提供するヘッダーを作成します。<br>ヘッダーの例：<br>X-YouTube-Edu-Filter: ABCD1234567890abcdef<br>（この場合の値は、YouTube で提供される固有キーです）。<br>ドメインの例：<br>youtube.com |
| [編集（Edit）] | 既存のヘッダーを指定したヘッダーと置き換えます。コマンドで返されたリストのヘッダーに関連付けられている番号を使用して削除するヘッダーを指定します。 |

**ステップ 4** メイン コマンド インターフェイスに戻るまで、Enter キーを押します。

**ステップ 5** 変更を保存します。

# Web プロキシのバイパス

• Web プロキシのバイパス（Web 要求の場合） （14 ページ）
• Web プロキシのバイパス設定（Web 要求の場合） （14 ページ）
• Web プロキシのバイパス設定（アプリケーションの場合） （15 ページ）

## Web プロキシのバイパス（Web 要求の場合）

特定のクライアントからの透過的要求や特定の宛先への透過的要求が Web プロキシをバイパスするように、 Secure Web Applianceを設定できます。

Web プロキシをバイパスすることによって、以下のことが可能になります。

- HTTP ポートを使用しているが、適切に機能しない HTTP 非対応の（または独自の）プロトコルが、プロキシ サーバーに接続するときに干渉されないようにします。
- ネットワーク内の特定のマシンからのトラフィックが、マルウェアのテストマシンなど、ネットワーク プロキシおよび組み込みのセキュリティ保護をすべてバイパスすることを確認します。

バイパスは、Web プロキシに透過的にリダイレクトされる要求に対してのみ機能します。Web プロキシは、トランスペアレントモードでも転送モードでも、クライアントから明示的に転送されたすべての要求を処理します。

## Web プロキシのバイパス設定（Web 要求の場合）

**ステップ 1** [Webセキュリティマネージャ（Web Security Manager）]>[バイパス設定（Bypass Settings）] を選択します。

**ステップ 2** [バイパス設定の編集（Edit Bypass Settings）] をクリックします。

**ステップ 3** Web プロキシをバイパスするアドレスを入力します。

（注） /0 をバイパスリスト内の任意の IP のサブネットマスクとして設定すると、アプライアンスはすべての Web トラフィックをバイパスします。この場合、アプライアンスは設定を 0.0.0.0/0 として解釈します。

**ステップ 4** プロキシバイパスリストに追加するカスタム URL カテゴリを選択します。

（注） [正規表現（Regular Expressions）] に Web プロキシバイパスを設定することはできません。

（注） カスタム URL カテゴリをプロキシバイパスリストに追加すると、カスタム URL カテゴリのすべての IP アドレスとドメイン名が、送信元と宛先の両方でバイパスされます。

**ステップ 5** 変更を送信し、保存します。

## Web プロキシのバイパス設定（アプリケーションの場合）

**ステップ 1** [Webセキュリティマネージャ（Web Security Manager）]>[バイパス設定（Bypass Settings）] を選択します。
**ステップ 2** [アプリケーションのスキップ設定を編集（Edit Application Bypass Settings）] をクリックします。
**ステップ 3** スキャンをバイパスするアプリケーションを選択します。
**ステップ 4** 変更を送信し、保存します。

（注） Webex バイパス設定は、HTTPS トラフィックにのみ適用されます。ただし、HTTP トラフィックの場合、アプリケーションはアクセスポリシーを介してブロックできます。

# ポリシーごとの Web プロキシ カスタム ヘッダー

HTTP リクエストのカスタムヘッダープロファイルを設定し、ヘッダー書き換えプロファイルの下に複数のヘッダーを作成できます。各プロファイルには最大 12 のヘッダーを設定できます。既存のヘッダー プロファイルを変更または削除することもできます。既存のアクセス ポリシーにヘッダー書き換えプロファイルを追加して、特定のアクセス ポリシーが適用されるすべてのトランザクションにヘッダーを含めることができます。

ヘッダー書き換えプロファイル機能を使用すると、認証が成功した後、アプライアンスがユーザとグループの情報を別のアップストリームデバイスに渡すことができます。アップストリーム プロキシはユーザを認証済みと見なし、追加の認証をバイパスし、定義されたアクセス ポリシーに基づいてユーザにアクセスを提供します。

- HTTP Web リクエストのヘッダー書き換えプロファイルの作成 （15 ページ）
- ユーザー名とグループ ヘッダー形式の変更 （17 ページ）（任意）
- アクセス ポリシーへのヘッダー プロファイルの追加 （17 ページ）

AsyncOS バージョン 14.0 以降では、CLI コマンド `advancedproxyconfig-> customheader` を使用した Web プロキシ カスタム ヘッダーの作成を避けることを推奨します。

## HTTP Web リクエストのヘッダー書き換えプロファイルの作成

**ステップ 1** [Web Security Manager] > [HTTP 書き換えプロファイル（HTTP Rewrite Profiles）] を選択します
**ステップ 2** [プロファイルを追加（Add Profile）] をクリックします。
**ステップ 3** 作成するヘッダー書き換えプロファイルに一意の名前を割り当てます。
**ステップ 4** [ヘッダー（Headers）] エリアで、次の情報を入力します。

（注） [ヘッダー書き換えプロファイル（Header Rewrite Profiles）] には空または Null のヘッダー値を入力できます。ヘッダーを保存して、Null または値なしで送信すると、ヘッダーは発信リクエストに含まれません。たとえば、アウトバウンド サーバーへのヘッダー `Via` を非表示にする場合は、値「""」でHTTP書き換えプロファイルにヘッダー名 `Via` を追加します。

- [ヘッダー名（Header Name）]：HTTP リクエストに追加するヘッダー名を入力します。例：X-Client-IP、X-Authenticated-User、X-Authenticated-Groups など
- [ヘッダー値（Header Value）]：ヘッダー名に対応するリクエスト ヘッダーに含める値を入力します。ヘッダー変数のプレフィックス：
  - `$ ReqMeta`：クライアント IP、ユーザー、グループなどの標準 HTTP ヘッダー変数を取得します。たとえば、リクエスト ヘッダーにユーザー名を含める場合、形式は `($ReqMeta[X-Authenticated-User])` です。
  - `$ReqHeader`：標準の HTTP ヘッダーの値、または同じヘッダー書き換えプロファイルに定義された他のヘッダーのヘッダーの値を使用します。

    たとえば、

    ```
    Header1:32

    Header2: 44-($ReqHeader[Header1])-46
    ```

    ヘッダー 2 の値は `44-32-46` になります
- [テキスト形式（Text Format）]：エンコーディングのテキスト形式を選択します。使用可能なオプションは ASCII と UTF-8 です。
- [バイナリ エンコーディング（Binary Encoding）]：リクエスト ヘッダーにバイナリ エンコーディング（Base64）を使用するかどうかを選択します。

（注） サーバー タイプに基づいて、送信されたリクエスト ヘッダー フィールドのサイズがサーバーの上限を超えた場合、アプライアンスはエラー メッセージを表示します。たとえば、異なるサーバー タイプは異なるヘッダー長をサポートします。

- Apache 2.0、2.2：8k
- Nginx：4k ー 8k
- IIS（バージョンによって異なります）：8K ー 16K
- Tomcat ：（バージョンによって異なります）8K

ISE を使用したユーザー識別の場合、グローバル X-authentication ヘッダー設定（X-Authenticated-User および X-Authenticated-Groups）は、プレフィックスとしてドメインおよび認証メカニズムを適用しません。

ASCII としてテキスト形式を選択した場合でも、`($ ReqMeta [HTTP_header])` 値として UTF+8 を入力できます。現在、次のヘッダーは `($ReqMeta[HTTP_header])` をサポートしています。

- X-Authenticated-User
- X-Authenticated-Groups
- X-Client-IP

ヘッダーの値が Null の場合、ヘッダーは発信リクエストに含まれません。これは、以下を実行しない場合に発生します。

- プロキシ認証を有効にします。
- アクセス ポリシー、復号化ポリシー、またはルーティング ポリシーのメンバーシップ基準でグループを定義します。

**ステップ 5** 変更を送信し、保存します。

## ユーザー名とグループ ヘッダー形式の変更

**ステップ 1** [Web Security Manager] > [HTTP 書き換えプロファイル（HTTP Rewrite Profiles）] を選択します。

**ステップ 2** [設定の編集（Edit Settings）] をクリックします。

**ステップ 3** 形式を変更します。

許可される形式は次のとおりです。

- ユーザー名：`$authMechanism://$domainName/$userName`、`$authMechanism:\\$domainName\$userName`、`$domainName/$userName`、`$domainName\$userName`、`$userName`
- グループ：`$authMechanism://$domainName/$groupName`、`$authMechanism:\\$domainName\$groupName`、`$domainName/$groupName`、`$domainName\$groupName`、`$groupName`

  カンマ（,）、コロン（:）、セミコロン（;）、バックスラッシュ（\）、縦棒（|）などのデリミタも変更できます。

**ステップ 4** 変更を送信し、保存します。

## アクセス ポリシーへのヘッダー プロファイルの追加

### 始める前に

アクセス ポリシーの設定ポリシーの作成 を参照してください。

**ステップ 1** [Web セキュリティ マネージャ（Web Security Manager）] > [アクセス ポリシー（Access Policies）] を選択します。

**ステップ 2** [アクセス ポリシー（Access Policies）] ページで、[HTTP 書き換えプロファイル（HTTP Rewrite Profile）] のリンクをクリックします。

新しいアクセス ポリシーを作成し、それにヘッダー書き換えプロファイルを追加することもできます。新しいアクセス ポリシーを作成するには、次を参照してください。ポリシーの作成

**ステップ 3** ポリシーに追加するヘッダー書き換えプロファイルを選択します。追加すると、特定のアクセス ポリシーが適用される HTTP トランザクションにヘッダーが含まれます。

**ステップ 4** 変更を送信し、保存します。

アクセス ポリシーにリンクされたヘッダー書き換えプロファイルは削除できます。削除する前に、別のプロファイルを選択すると、選択したプロファイルがアクセス ポリシーに自動的に適用されます。

# Web プロキシ使用規約

Secure Web Appliance を設定して、Web アクティビティのフィルタリングとモニタリングが行われていることをユーザに通知できます。アプライアンスは、ユーザーが初めてブラウザにアクセスしたときに、一定時間の経過後、エンドユーザー確認ページを表示します。エンドユーザー確認ページが表示されたら、ユーザーはリンクをクリックして、要求した元のサイトまたは他の Web サイトにアクセスする必要があります。

### 関連項目

- エンドユーザーへのプロキシ アクションの通知

# ドメイン マップ

特定のクライアントからの透過的 HTTPS 要求や特定の宛先への透過的 HTTPS 要求が HTTPS プロキシをバイパスするように、 Secure Web Applianceを設定できます。

トラフィックがアプライアンスを通過することを必要とするアプリケーションに関して、変更や宛先サーバーの証明書チェックを行わずに、パススルーを使用することができます。

## 特定アプリケーションのドメインマップ

### 始める前に

特定のサーバーへのパススルートラフィックを必要とするデバイスに関して定義された識別ポリシーがあることを確認してください。詳細については、ユーザーおよびクライアント ソフトウェアの分類を参照してください。具体的には、次のことを行う必要があります。

- [認証/識別から除外（Exempt from authentication/identification）] をオンします。
- この識別プロファイルを適用するアドレスを指定します。IP アドレス、CIDR ブロック、およびサブネットを入力できます。

**ステップ 1** HTTPSプロキシを有効にします。詳細については、HTTPSプロキシのイネーブル化を参照してください。

**ステップ 2** [Webセキュリティマネージャ（Web Security Manager）]>[ドメインマップ（Domain Map）] を選択します。

a) [ドメインの追加（Add Domain）] をクリックします。
b) [ドメイン名（Domain Name）] に宛先サーバーのドメイン名を入力します。
c) 既存のドメインが指定されている場合は、優先順位を選択します。
d) IP アドレスを入力します。

e) [送信（Submit）] をクリックします。

**ステップ 3** [Webセキュリティマネージャ（Web Security Manager）] > [カスタムおよび外部URLカテゴリ（Custom and External URL Categories）] を選択します。

a) [Add Category] をクリックします。

b) 次の情報を入力します。

| 設定 | 説明 |
|---|---|
| カテゴリ名（Category Name） | この URL カテゴリの識別子を入力します。この名前は、ポリシー グループに URL フィルタリングを設定するときに表示されます。 |
| リスト順（List Order） | カスタム URL カテゴリのリストで、このカテゴリの順序を指定します。リスト内の最初の URL カテゴリに「1」を入力します。<br>URL フィルタリング エンジンでは、指定した順序でカスタム URL カテゴリに対してクライアント要求が評価されます。 |
| カテゴリ タイプ（Category Type） | [ローカルカスタムカテゴリ（Local Custom Category）] を選択します。 |
| 詳細設定（Advanced） | このセクションに、追加のアドレスセットを指定する正規表現を入力できます。<br>正規表現を使用して、入力したパターンと一致する複数のアドレスを指定できます。<br>正規表現の使用方法については、正規表現を参照してください。 |

c) 変更を送信し、保存します。

**ステップ 4** [Webセキュリティマネージャ（Web Security Manager）] > [復号化ポリシー（Decryption Policies）] を選択します。

a) 新しい復号化ポリシーを作成します。

b) 特定のアプリケーションの HTTPS トラフィックをバイパスするために作成した識別プロファイルを選択します。

c) [詳細設定（Advanced）] パネルで、[URLカテゴリ（URL Categories）] のリンクをクリックします。

d) [追加（Add）] カラムをクリックして、手順 3 で作成したカスタム URL カテゴリを追加します。

e) [完了（Done）] をクリックします。

f) [復号化ポリシー（Decryption Policies）] ページで、[URLフィルタリング（URL Filtering）] のリンクをクリックします。

g) [パススルー（Pass Through）] を選択します。

h) 変更を送信し、保存します。

**%(**フォーマット指定子を使用してアクセスログ情報を表示することができます。詳細については、アクセス ログのカスタマイズを参照してください。

（注）
- ドメインマップ機能は HTTPS 透過モードで動作します。
- この機能は、明示モードでは動作せず、HTTP トラフィックについても動作しません。
- この機能を使用してトラフィックを許可するには、ローカルカスタムカテゴリを設定する必要があります。
- この機能を有効にすると、SNI 情報が利用できる場合でも、ドメインマップで設定されたサーバー名に従ってサーバー名の変更または割り当てが行われます。
- この機能は、ドメイン名に基づくトラフィックがドメインマップと一致し、対応するカスタムカテゴリ、復号化ポリシー、パススルーアクションが設定されている場合、そのトラフィックをブロックしません。
- 認証をこのパススルー機能と併用することはできません。認証には復号化が必要ですが、この場合、トラフィックは復号化されません。
- UDP トラフィックはモニターされません。 Secure Web Applianceに到達しないように UDP トラフィックを設定する必要があります。代わりに、WhatsApp、Telegram などのアプリケーションのためにファイアウォールを経由してインターネットに直接アクセスする必要があります。
- WhatsApp、Telegram、およびSkypeは透過モードで動作します。ただし、WhatsAppなどの一部のアプリケーションは、アプリケーションの制限のために、明示モードでは動作しません。

# Web 要求をリダイレクトするためのクライアント オプション

クライアントから Web プロキシに明示的に要求を転送することを選択した場合は、それを実行するためのクライアントの設定方法も指定する必要があります。以下の方法から選択します。

- **明示的な設定を使用してクライアントを設定する。**Webプロキシのホスト名とポート番号を使ってクライアントを設定します。設定方法の詳細については、個々のクライアントのマニュアルを参照してください。

（注） デフォルトでは、Web プロキシ ポートはポート番号 80 と 3128 を使用します。クライアントはいずれかのポートを使用できます。

- **プロキシ自動設定（PAC）ファイルを使用してクライアントを設定する。**PAC ファイルは、Web要求の送信先をクライアントに指示します。このオプションを使用すると、プロキシの詳細に対する以降の変更を一元管理できます。

PAC ファイルを使用する場合は、PAC ファイルの保存場所とクライアントがそれらを検出する方法を選択する必要があります。

**関連項目**

- クライアント アプリケーションによる PAC ファイルの使用 （21 ページ）

# クライアントアプリケーションによるPACファイルの使用

## プロキシ自動設定（PAC）ファイルのパブリッシュ オプション

クライアントがアクセスできる場所に PAC ファイルをパブリッシュする必要があります。有効な場所は以下のとおりです。

- **Web サーバー**
- **Secure Web Appliance**。クライアントに対しては Web ブラウザとして表示される Secure Web Applianceに PAC ファイルを配置できます。アプライアンスには、さまざまなホスト名、ポート、ファイル名を使用している要求に対応する機能など、PACファイルを管理するための追加オプションもあります。
- **ローカル マシン。**クライアントのハードディスクに PAC ファイルをローカルに配置できます。これを一般的な解決方法として使用することは推奨されません。自動 PAC ファイル検出には適していませんが、テストには役立つ可能性があります。

**関連項目**

- Secure Web Applianceでの PAC ファイルのホスト （22 ページ）
- クライアント アプリケーションでの PAC ファイルの指定 （23 ページ）
- Secure Web Applianceでの PAC ファイルのホスト （22 ページ）
- クライアント アプリケーションでの PAC ファイルの指定 （23 ページ）

## プロキシ自動設定（PAC）ファイルを検索するクライアント オプション

クライアントに対して PAC ファイルを使用する場合は、クライアントが PAC ファイルを検索する方法を選択する必要があります。以下の 2 つの対処法があります。

- **PAC ファイルの場所をクライアントに設定する。**この PAC ファイルを明確に差し指す URL をクライアントに設定します。

- **PAC ファイルの場所を自動的に検出するようにクライアントを設定する。**DHCP または DNS とともに WPAD プロトコルを使用して PAC ファイルを自動的に検索するようにクライアントを設定します。

## PAC ファイルの自動検出

WPAD は、DHCP および DNS ルックアップを使用してブラウザが PAC ファイルの場所を判別できるようにするプロトコルです。

- **DHCP と共に WPAD を使用するには、**DHCP サーバーに PAC ファイルの場所の URL と共にオプション 252 を設定します。ただし、すべてのブラウザが DHCP をサポートしているわけではありません。
- **DNS と共に WPAD を使用するには、**PAC ファイルのホスト サーバーを指し示すように DNS レコードを設定します。

いずれかまたは両方のオプションを設定できます。WPAD は最初に DHCP を使用して PAC ファイルの検出を試み、検出できなかった場合は DNS を使って試みます。

**関連項目**

- クライアントでの PAC ファイルの自動検出 （24 ページ）

# Secure Web Applianceでの PAC ファイルのホスト

**ステップ 1** [セキュリティ サービス（Security Services）] > [PAC ファイル ホスティング（PAC File Hosting）] を選択します。

**ステップ 2** [設定の有効化と編集（Enable and Edit Settings）] をクリックします。

**ステップ 3** （任意）以下の基本設定項目を設定します。

| オプション | 説明 |
|---|---|
| PAC サーバー ポート（PAC Server Ports） | Secure Web Applianceが PAC ファイル要求のリッスンに使用するポート。 |
| PAC ファイルの有効期限（PAC File Expiration） | ブラウザ キャッシュで指定されている分数が経過した後に PAC ファイルを期限切れにできます。 |

**ステップ 4** [PACファイル（PAC Files）] セクションで [参照（Browse）] をクリックし、 Secure Web Applianceにアップロードする PAC ファイルをローカルマシンから選択します。

（注） 選択したファイルの名前が `default.pac` である場合は、ブラウザで場所を設定するときにファイル名を指定する必要がありません。名前が指定されていない場合、 Secure Web Applianceは `default.pac` というファイルを検索します。

**ステップ 5** [アップロード（Upload）] をクリックして、ステップ 4 で選択した PAC ファイルを Secure Web Appliance にアップロードします。

**ステップ 6** （任意）[PAC ファイルサービスを直接提供するホスト名（Hostnames for Serving PAC Files Directly）] セクションで、ポート番号を含まない PAC ファイル要求のホスト名と関連ファイル名を設定します。

| オプション | 説明 |
|---|---|
| ホスト名（Hostname） | Secure Web Applianceが要求を処理する場合に、PAC ファイル要求に含める必要があるホスト名。要求にはポート番号が含まれていないため、要求は Web プロキシの HTTP ポート（ポート80）を使用して処理され、ホスト名評価から PAC ファイル要求として識別できます。 |
| プロキシ ポートを通じた「GET」要求に対するデフォルト PAC ファイル（Default PAC File for "Get/" Request through Proxy Port） | 同じ行のホスト名に関連付けられる PAC ファイル名。ホスト名に対する要求は、ここで指定した PAC ファイルを返します。<br>アップロード済みの PAC ファイルのみを選択できます。 |
| 行を追加（Add Row） | 別の行を追加して、追加のホスト名と PAC ファイル名を指定します。 |

**ステップ 7** 変更を送信し、保存します。

# クライアント アプリケーションでの PAC ファイルの指定

• クライアントでの PAC ファイルの場所の手動設定 （23 ページ）
• クライアントでの PAC ファイルの自動検出 （24 ページ）

## クライアントでの PAC ファイルの場所の手動設定

**ステップ 1** PAC ファイルを作成してパブリッシュします。

**ステップ 2** ブラウザの PAC ファイル設定領域に PAC ファイルの場所を示す URL を入力します。

Secure Web Applianceが PAC ファイルをホストしている場合、有効な URL 形式は以下のようになります。

```
http://server_address[.domain][:port][/filename] | http://WSAHostname[/filename]
```

*WSAHostname* は、 Secure Web Applianceに PAC ファイルをホストするときに設定した [ホスト名（hostname）] の値です。ホストしていない場合、URL の形式は格納場所と（場合によっては）クライアントに応じて異なります。

### 次のタスク

• Secure Web Applianceでの PAC ファイルのホスト （22 ページ）

## クライアントでの PAC ファイルの自動検出

**ステップ 1** wpad.dat という名前の PAC ファイルを作成し、Web サーバーまたは Secure Web Applianceにパブリッシュします（DNS と共に WPAD を使用する場合は、Web サーバーのルートフォルダにファイルを配置する必要があります）。

**ステップ 2** 次の MIME タイプで .dat ファイルを設定するように Web サーバーを設定します。

```
application/x-ns-proxy-autoconfig
```

（注） Secure Web Applianceはこれを自動的に実行します。

**ステップ 3** DNS ルックアップをサポートするには、「wpad」から始まる、内部的に解決可能な DNS 名を作成して（例：wpad.example.com）、wpad.dat ファイルをホストしているサーバーの IP アドレスに関連付けます。

**ステップ 4** DHCP ルックアップをサポートするには、DHCP サーバーのオプション 252 に wpad.dat ファイルの場所の URL を設定します（例：「http://wpad.example.com/wpad.dat」）。URL には、IP アドレスなど、有効な任意のホスト アドレスを使用できます。特定の DNS エントリは必要ありません。

### 次のタスク

- クライアント アプリケーションによる PAC ファイルの使用 （21 ページ）
- Secure Web Applianceでの PAC ファイルのホスト （22 ページ）
- Firefox で WPAD を使用できない

# FTP プロキシ サービス

- FTP プロキシ サービスの概要 （24 ページ）
- FTP プロキシの有効化と設定 （25 ページ）

## FTP プロキシ サービスの概要

Web プロキシは、以下の 2 種類の FTP 要求を代行受信できます。

- **ネイティブ FTP。**ネイティブ FTP 要求は、専用 FTP クライアントによって生成されます（または、ブラウザで組み込みの FTP クライアントを使用して生成されます）。FTP プロキシが必要です。
- **FTP over HTTP。**ブラウザは、ネイティブ FTP を使用する代わりに、HTTP 要求内に FTP 要求をエンコードすることがあります。FTP プロキシは必要ありません。

### 関連項目

- FTP プロキシの有効化と設定 （25 ページ）
- FTP 通知メッセージの設定

# FTP プロキシの有効化と設定

（注） FTP over HTTP 接続に適用されるプロキシ設定を設定するには、Web プロキシの設定 （4 ページ）を参照してください。

**ステップ 1** [セキュリティ サービス（Security Services）] > [FTP プロキシ（FTP Proxy）] を選択します。

**ステップ 2** [設定の有効化と編集（Enable and Edit Settings）] をクリックします（表示されるオプションが [設定の編集（Edit Settings）] だけの場合、FTP プロキシは設定済みです。）

**ステップ 3** （任意）基本的な FTP プロキシ設定項目を設定します。

| プロパティ | 説明 |
|---|---|
| プロキシ リスニング ポート（Proxy Listening Port） | FTP プロキシが FTP 制御接続をリッスンするポート。クライアントは、（FTP サーバーに接続するためのポート（通常はポート 21 を使用）としてではなく）FTP プロキシを設定するときにこのポートを使用する必要があります。 |
| キャッシング（Caching） | 匿名ユーザーからのデータ接続をキャッシュするかどうか。<br>（注） 匿名ではないユーザーからのデータはキャッシュされません。 |
| サーバー側の IP スプーフィング（Server Side IP Spoofing） | FTP プロキシが FTP サーバーの IP アドレスをシミュレートできるようにします。これによって、IP アドレスが制御接続とデータ接続で異なる場合に、トランザクションを許可しない FTP クライアントに対応できます。 |
| クライアント IP スプーフィング | FTP プロキシが FTP クライアントの送信元 IP アドレスを模倣できるようにします。有効にすると、FTP 要求は FTP プロキシではなく FTP クライアントから発信されたように見えます。 |
| 認証形式（Authentication Format） | FTP クライアントと通信するときに FTP プロキシが使用する認証形式を選択できるようにします。 |
| パッシブモードのデータポート範囲（Passive Mode Data Port Range） | パッシブ モード接続で FTP プロキシとのデータ接続を確立するために FTP クライアントが使用する TCP ポートの範囲。 |

| プロパティ | 説明 |
|---|---|
| アクティブモードのデータポート範囲（Active Mode Data Port Range） | アクティブ モード接続で FTP プロキシとのデータ接続を確立するために FTP サーバーが使用する TCP ポートの範囲。この設定は、ネイティブ FTP および FTP over HTTP 接続の両方に適用されます。<br>ポート範囲を大きくすると、同じ FTP サーバーからのさらに多くの要求に対応できます。TCP セッションの TIME-WAIT 遅延（通常数分）によって、ポートは使用された直後に、同じ FTP サーバーで再び使用できるようになりません。その結果、所定の FTP サーバーは短時間アクティブ モードで *n* 回以上 FTP プロキシに接続できません。ここでは *n* は、このフィールドに指定されたポート数です。 |
| ウェルカム バナー（Welcome Banner） | 接続時に FTP クライアントに表示されるウェルカム バナー。次から選択します。<br>• **[FTP サーバーメッセージを（FTP server message）]**。メッセージは宛先 FTP サーバーによって表示されます。このオプションは、Web プロキシが透過モードに設定されている場合にのみ利用でき、透過接続にのみ適用されます。<br>• **[カスタム メッセージ（Custom message）]**。このオプションをオンにすると、すべてのネイティブ FTP 接続に対してこのカスタム メッセージが表示されます。オフにした場合は、明示的な転送ネイティブ FTP 接続に使用されます。 |

**ステップ 4** （任意）FTP プロキシの詳細設定を設定します。

| プロパティ | 説明 |
|---|---|
| 制御接続のタイムアウト（Control Connection Timeouts） | 現在のトランザクションが完了していない場合に、アイドル状態の FTP クライアントまたは FTP サーバーからの制御接続による通信を、FTP プロキシがさらに待機する最大時間（秒単位）。<br>• **[クライアント側（Client side）]**。アイドル状態の FTP クライアントとの制御接続のタイムアウト値。<br>• **[サーバー側（Server side）]**。アイドル状態の FTP サーバーとの制御接続のタイムアウト値。 |
| データ接続のタイムアウト（Data Connection Timeouts） | 現在のトランザクションが完了していない場合に、アイドル状態の FTP クライアントまたは FTP サーバーからのデータ接続による通信を、FTP プロキシがさらに待機する時間。<br>• **[クライアント側（Client side）]**。アイドル状態の FTP クライアントとのデータ接続のタイムアウト値。<br>• **[サーバー側（Server side）]**。アイドル状態の FTP サーバーとのデータ接続のタイムアウト値。 |

**ステップ 5** 変更を送信し、保存します。

### 次のタスク

- FTP プロキシ サービスの概要 （24 ページ）

# SOCKS プロキシ サービス

- SOCKS プロキシ サービスの概要 （27 ページ）
- SOCKS トラフィックの処理のイネーブル化 （27 ページ）
- SOCKS プロキシの設定 （28 ページ）
- SOCKS ポリシーの作成 （28 ページ）

## SOCKS プロキシ サービスの概要

Secure Web Applianceには、SOCKS トラフィックを処理するための SOCKS プロキシが含まれます。SOCKSポリシーは、SOCKSトラフィックを制御するアクセス ポリシーと同等です。アクセス ポリシーと同様に、識別プロファイルを使用して、各 SOCKS ポリシーによってどのトランザクションを管理するかを指定できます。SOCKS ポリシーをトランザクションに適用すると、ルーティング ポリシーによてトラフィックのルーティングを管理できます。

SOCKS プロキシでは、以下の点に注意してください。

- SOCKS プロトコルは、直接転送接続のみをサポートしています。
- SOCKSプロキシは、アップストリームプロキシをサポートしていません（アップストリーム プロキシに転送されません）。
- SOCKS プロキシは、Application Visibility and Control（AVC）、 Data Loss Prevention（DLP）、およびマルウェア検出に使用されるスキャニングサービスをサポートしていません。
- SOCKS プロキシは、ポリシー追跡をサポートしていません。
- SOCKS プロキシは、SSL トラフィックを復号化できません。これは、クライアントからサーバーにトンネリングします。

## SOCKS トラフィックの処理のイネーブル化

### 始める前に

Web プロキシをイネーブルにします。

**ステップ 1** [セキュリティ サービス（Security Services）] > [SOCKS プロキシ（SOCKS Proxy）] を選択します。

**ステップ 2** [設定の編集（Edit Settings）] をクリックします。

**ステップ 3** [SOCKS プロキシを有効にする（Enable SOCKS Proxy）] を選択します。

**ステップ 4** 変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

# SOCKS プロキシの設定

**ステップ 1** [セキュリティ サービス（Security Services）] > [SOCKS プロキシ（SOCKS Proxy）] を選択します。

**ステップ 2** [設定の編集（Edit Settings）] をクリックします。

**ステップ 3** [SOCKS プロキシを有効にする（Enable SOCKS Proxy）] を選択します。

**ステップ 4** 基本および高度な SOCKS プロキシ設定を設定します。

| | |
|---|---|
| SOCKS プロキシ（SOCKS Proxy） | イネーブル。 |
| SOCKS コントロール ポート（SOCKS Control Ports） | SOCKS 要求を受け入れるポート。デフォルトは 1080 です。 |
| UDP リクエスト ポート（UDP Request Ports） | SOCKS サーバーがリッスンする必要がある UDP ポート。デフォルトは 16000 ～ 16100 です。 |
| プロキシネゴシエーション タイムアウト（Proxy Negotiation Timeout） | ネゴシエーション段階で SOCKS クライアントからデータを送受信するのを待機する時間（秒単位）。デフォルトは 60 です。 |
| UDP トンネル タイムアウト（Tunnel Timeout） | UDP トンネルを閉じる前に UDP クライアントまたはサーバーからのデータを待機する時間（秒単位）。デフォルトは 60 です。 |

# SOCKS ポリシーの作成

**ステップ 1** [Web セキュリティ マネージャ（Web Security Manager）] > [SOCKS ポリシー（SOCKS Policies）] を選択します。

**ステップ 2** [ポリシーを追加（Add Policy）] をクリックします。

**ステップ 3** [ポリシー名（Policy Name）] フィールドに名前を割り当てます。

（注） 各ポリシー グループ名は、英数字またはスペース文字のみを含む、一意の名前とする必要があります。

**ステップ 4** （任意）説明を追加します。

**ステップ 5** [上記ポリシーを挿入（Insert Above Policy）] フィールドで、この SOCKS ポリシーに挿入する SOCKS ポリシーの場所を選択します。

（注） 複数の SOCKS ポリシーを設定する場合、各ポリシーの論理的な順序を決定します。照合が適切に行われるように、ポリシーの順序を指定してください。

**ステップ 6** [アイデンティティとユーザー（Identities and Users）] セクションで、このグループ ポリシーに適用する 1 つ以上の ID を選択します。

**ステップ 7** （任意）[詳細（Advanced）] セクションを拡張して、追加のメンバーシップ要件を定義します。

| | |
|---|---|
| プロキシ ポート（Proxy Ports） | ブラウザに設定されたポート。<br>（任意）Web プロキシへのアクセスに使用するプロキシ ポートによってポリシー グループのメンバーシップを定義します。[プロキシ ポート（Proxy Ports）] フィールドに、1 つ以上のポート番号を入力します。複数のポートを指定する場合は、カンマで区切ります。<br>あるポート上に要求を明示的に転送するように設定されたクライアントのセットがあり、別のポート上に要求を明示的に転送するように設定された別のクライアントのセットがある場合、プロキシ ポート上でポリシー グループのメンバーシップを定義することがあります。<br>（注） このポリシー グループに関連付けられている ID が この詳細設定によって ID メンバーシップを定義している場合、SOCKS ポリシー グループ レベルではこの設定項目を設定できません。 |
| サブネット（Subnets） | （任意）サブネットまたは他のアドレスでポリシー グループのメンバーシップを定義します。<br>関連付けられた **ID** で**定義**できる**アドレス**を使用するか、または**特定のアドレス**をここに入力できます。<br>（注） ポリシー グループに関連付けられている ID が、アドレスによってグループのメンバーシップを定義している場合は、このポリシー グループに、ID のアドレスのサブセットであるアドレスを入力する必要があります。ポリシー グループにアドレスを追加することにより、このグループ ポリシーに一致するトランザクションのリストを絞り込めます。 |
| 時間範囲（Time Range） | （任意）時間範囲別にポリシー グループのメンバーシップを定義します。<br>1. [時間範囲（Time Range）] から時間範囲を選択します。<br>2. このポリシー グループが選択した時間範囲内または範囲外の時間に適用されるかどうかを指定します。 |

**ステップ 8** 変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

### 次のタスク

- （任意）SOCKS ポリシーで使用するための ID を追加します。
- SOCKS トラフィックを管理する 1 つ以上の SOCKS ポリシーを追加します。

# Cisco Umbrella シームレス ID

Cisco Umbrella シームレス ID 機能を使用すると、正常に認証された後に、アプライアンスからユーザ識別情報を Cisco Umbrella セキュア Web ゲートウェイ（SWG）にパスすることができます。Cisco Umbrella SWG は、 Secure Web Applianceから受信した認証済み識別情報に基づいて、Active Directory のユーザー情報をチェックします。Cisco Umbrella SWG は、ユーザを認証済みと見なし、定義されたセキュリティポリシーに基づいてユーザにアクセスを提供します。

Secure Web Applianceは、X-USWG-PKH、X-USWG-SK、および X-USWG-Data を含む HTTP ヘッダーを使用して Cisco Umbrella SWG にユーザー識別情報を渡します。

（注）

- Cisco Umbrella シームレス ID ヘッダーは、 Secure Web Appliance上の同じ名前のヘッダーを上書きします。
- Cisco Umbrella シームレス ID 機能は、Active Directory でのみ認証方式をサポートします。この機能は、LDAP、Cisco Identity Services Engine（ISE）、および Cisco Context Directory Agent（CDA）をサポートしていません。
- Cisco Umbrella SWG は FTP および SOCKS トラフィックをサポートしていません。

表 *1 : HTTPS* トラフィックの動作

| 構成モード | サロゲート | 認証のための復号化 | Secure Web Appliance 認証 | Cisco Umbrella シームレス ID の共有 |
|---|---|---|---|---|
| Explicit | IP サロゲート | はい/いいえ | 対応 | 対応 |
| 透過 | IP サロゲート | 対応 | 対応 | 対応 |
| 透過 | IP サロゲート | 非対応 | 認証をスキップ | 非対応 |
| Explicit | Cookie、クレデンシャルの暗号化なし | はい/いいえ | 対応 | 対応 |
| Explicit | Cookie、クレデンシャルの暗号化あり | はい/いいえ | 対応 | × |
| 透過 | Cookie、クレデンシャル暗号化あり/なし | はい/いいえ | 認証をスキップ | 非対応 |

（注） Secure Web Applianceは、認証されたユーザーの UPN 値を Active Directory から取得し、Cisco Umbrella シームレス ID でユーザーに正しい Web ポリシーを適用できるようにします。この機能を利用するには、すべての Active Directory ユーザーにデフォルトまたはカスタマイズされた UPN 値を割り当てる必要があります。

ここでは、次の内容について説明します。

- Cisco Umbrella シームレス ID の設定
- Cisco Umbrella SWG のルーティング先の設定

# Cisco Umbrella シームレス ID の設定

始める前に

- **[ネットワーク（Network）]** > **[証明書の管理（Certificate Management）]** > **[信頼できるルート証明書の管理（Manage Trusted Root Certificates）]**を選択して、ルートまたはカスタムの Umbrella 証明書をアプライアンスに手動でアップロードします。「証明書の管理」を参照してください。
- 認証用の識別プロファイルが設定されていることを確認します。
- 設定済みの識別プロファイルを使用してルーティングポリシーを定義します。

**ステップ 1** **[Webセキュリティマネージャ（Web Security Manager）]** > **[Cisco UmbrellaシームレスID（Cisco Umbrella Seamless ID）]**を選択します。

**ステップ 2** **[設定の編集（Edit Settings）]** をクリックします。

**ステップ 3** Cisco Umbrella SWG ホスト名または IP アドレスを入力します。

**ステップ 4** HTTP および HTTPS トラフィック用の SWG のポート番号を入力します。

最大 6 つのポート番号を入力できます。

**ステップ 5** （オプション）[接続テスト（Connectivity Test）] をクリックして、ポートを介した Cisco Umbrella SWG の接続と証明書の検証が正常に行われていることを確認します。

**ステップ 6** Cisco Umbrella SWG の一意のカスタマー組織 ID を入力します。

**ステップ 7** 送信して確定します。

# Cisco Umbrella SWG のルーティング先の設定

新しいルーティングポリシーを作成するには、「ルーティングポリシーへのルーティング先と IP スプーフィングプロファイルの追加」を参照してください。

。

**ステップ 1** **[Webセキュリティマネージャ（Web Security Manager）]** > **[ルーティングポリシー（Routing Policies）]**を選択します。

**ステップ 2** [ルーティングポリシー（Routing Policies）] ページで、必要なポートを含む Cisco Umbrella シームレス ID を設定するルーティングポリシーの [ルーティング先（Routing Destination）] 列の下にあるリンクをクリックします。

**ステップ 3** ポリシーのアップストリーム プロキシグ グループとして、ポートを含む適切な Cisco Umbrella シームレス ID を選択します。[アップストリームプロキシグループ（Upstream Proxy Group）] ドロップダウンリストには、**[Cisco Umbrellaシームレス ID（Cisco Umbrella Seamless ID）]** ページ（**[Webセキュリティマネージャ（Web Security Manager）]** > **[Cisco Umbrellaシームレス ID（Cisco Umbrella Seamless ID）]**）で設定したすべての Cisco Umbrella シームレス ID とポートが表示されます。

（注） ルーティングポリシーにすでにリンクされているポート番号を持つ **Cisco Umbrella シームレス ID** を削除すると（**[Webセキュリティマネージャ（Web Security Manager）]** > **[Cisco Umbrella シームレス ID（Cisco Umbrella Seamless ID）]**）、ルーティング先が [直接接続（Direct Connection）] に変わります。

**ステップ 4** 変更を送信し、保存します。

# 要求の代替受信に関するトラブルシューティング


- URL カテゴリが一部の FTP サイトをブロックしない
- 大規模 FTP 転送の切断
- ファイルのアップロード後に FTP サーバーにゼロ バイト ファイルが表示される
- アップストリーム プロキシ経由で FTP 要求をルーティングできない
- HTTPS および FTP over HTTP 要求が、認証を必要としないアクセス ポリシーにのみ一致する
- HTTPS 要求および FTP over HTTP 要求の場合にユーザーがグローバル ポリシーに一致

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。