

HazardFilter 透過型プロキシ構成での設定と注意事項

株式会社 YE DIGITAL

【 質問 】

HazardFilter で、透過型プロキシ構成での設定と注意事項を教えてください。

【 回答 】

透過プロキシ環境において、HTTP および HTTPS 通信の Web フィルタリングが可能です。

※ブラウザからの通信が対象です。

I. 設定方法、構成例について

1. 「サーバ管理」 → 「サーバ設定」 を選択します。



HazardFilter Ver.3.1 Build1500 on Linux 64bit ログインユーザ: root ログアウト

ホーム グループ/ユーザ管理 共通アクセス管理 個別アクセス管理 規制解除申請管理 **サーバ管理** 設定情報管理 ログ管理

サーバ管理 > **サーバ設定**

▶ サーバ情報 [+サーバを追加](#)

サーバ名	管理サービス 状態	フィルタリングサービス 状態	フィルタリングサービス 設定	
デフォルトサーバ (Primary)	正常動作中	稼働中 再起動 起動 終了	IPアドレス: 172.16.159.198 HTTPポート: 8080 HTTPSポート: 13443 FTP over HTTPポート: 8021	再表示 選択
レプリカサーバ	正常動作中	稼働中 再起動 起動 終了	IPアドレス: 172.16.159.199 HTTPポート: 8080 HTTPSポート: 13443 FTP over HTTPポート: 8021	選択

管理サービスおよび監視Webサービスは、管理画面から起動・停止・再起動できません。操作方法はヘルプを参照してください。

HazardFilter

2. 「サーバ設定」画面で、該当サーバの「選択」ボタンを選択します。

HazardFilter Ver 3.1 Build1600 on Linux 64bit ログインユーザ: root ログアウト

ホーム グループ/ユーザ管理 共通アクセス管理 個別アクセス管理 規制解除申請管理 サーバ管理 設定情報管理 ログ管理

サーバ管理 > サーバ設定 > 前画面へ戻る

サーバ設定編集

保存

▶ サーバ情報

* サーバ名	デフォルトサーバ
* IPアドレス	172.16.159.198

▶ 管理画面設定

* ポート	2319
-------	------

※ このポートは、ログレポートツールとの通信にも利用しています。
※ 設定変更を反映するには、管理している全てのサーバで監聴Webサービスの再起動が必要になります。

▶ フィルタリングサービス設定

HTTP	* ポート	8080	* プロセス数	450
HTTPS	* ポート	13443	* プロセス数	300
FTP over HTTP	* ポート	8021	* プロセス数	100
プロセス数警告設定	プロセス使用率が以下を超えると警告通知を行う。 80 %			

※ 設定変更を反映するには、フィルタリングサービスの再起動が必要です。
(同じ設定を使用するレガシーサーバでも、フィルタリングサービスの再起動が必要になります。)
※ 通知を有効にするには「サーバ1の通知設定」でサービス警告完全通知を有効にして頂く必要があります。

3. 「サーバ設定編集」画面の「透過プロキシ」の「有効」にチェックを入れると、フィルタリングサービス設定の「FTP over HTTP」は非表示となります。

▶ フィルタリングサービス共通設定

リクエストモード	転送しない	※ 追加ヘッダの扱いを設定します。
* 転送バッファサイズ	2048 byte	
POST転送バッファサイズ	<input type="radio"/> 転送バッファサイズと同じ値を使用する <input checked="" type="radio"/> POST転送バッファサイズを設定する	
	8192 byte	
* サーバ接続タイムアウト値	60000 ms	
サーバ転送Nagleアルゴリズム	<input checked="" type="checkbox"/> 無効	
* クライアント接続タイムアウト値	60000 ms	
クライアント転送Nagleアルゴリズム	<input checked="" type="checkbox"/> 無効	
* HTTPS通信タイムアウト値	90000 ms	
* 最大ヒープサイズ	256 Mbyte	
* ヘルスチェック間隔	60 s	
Keep-Alive設定	全て有効	
HTTPバージョン設定	<input checked="" type="radio"/> HTTP/1.1対応 <input type="radio"/> HTTP/1.0のみ使用	
プロトコル利用制御	<input type="checkbox"/> HTTP/2, WebSocket, QUICの利用を抑制する	
透過プロキシ	<input type="checkbox"/> 有効	
	全選択 全解除	
HTTPメソッド転送許可設定	<input checked="" type="checkbox"/> PUT <input checked="" type="checkbox"/> DELETE <input type="checkbox"/> MKCOL <input type="checkbox"/> COPY <input type="checkbox"/> MOVE <input type="checkbox"/> PROPFIND <input type="checkbox"/> PROPPATCH <input type="checkbox"/> LOCK <input type="checkbox"/> UNLOCK ※ 選択されたメソッドの転送を許可します。	
ロードバランサ補助設定	<input type="checkbox"/> 有効	

※ 「HTTPメソッド転送許可設定」を除く設定変更を反映するには、管理している全てのサーバでフィルタリングサービス、管理サービスの再起動が必要になります。

HazardFilter の設定のみでは、透過プロキシは実現出来ません。

上記設定と共に、クライアントからの通信を行うには、NetSHAKER の透過型プロキシ設定も行う必要がございます。

構成例



NetSHAKER の設定

[サービス] → [プロキシサーバ管理] → [プロキシサーバ詳細] 画面の透過型プロキシを設定します。

プロキシサーバ詳細設定

動作ポート番号	8080										
SSLポート番号	443 563										
x-forwarded-forを追加する	<input type="radio"/> Yes <input checked="" type="radio"/> No										
ユーザ認証を行う	<input type="radio"/> Yes <input checked="" type="radio"/> No										
キャッシュディスクサイズ	1GB										
透過型プロキシ	<input checked="" type="radio"/> 使用する <table border="1"> <thead> <tr> <th></th> <th>転送元ポート(複数指定可)</th> <th>転送先ポート</th> </tr> </thead> <tbody> <tr> <td>HTTP</td> <td>80</td> <td>8085</td> </tr> <tr> <td>HTTPS</td> <td>443 563</td> <td>8086</td> </tr> </tbody> </table>			転送元ポート(複数指定可)	転送先ポート	HTTP	80	8085	HTTPS	443 563	8086
	転送元ポート(複数指定可)	転送先ポート									
HTTP	80	8085									
HTTPS	443 563	8086									
	<input type="radio"/> 使用しない										
透過型プロキシ 動作ポート番号(HTTP)	18085										
透過型プロキシ 動作ポート番号(HTTPS)	18086										

設定 取り消し

[注意]

NetSHAKER のプロキシを利用しない場合は、プロキシサービスを停止してください。

NetSHAKER のプロキシを利用する場合は、透過型プロキシの転送先ポートと動作ポート番号は、異なったポート番号を設定してください。

HazardFilter の設定

「サーバ設定編集」画面のフィルタリングサービス設定の HTTP、HTTPS のポート番号を設定します。

NetSHAKER の透過型プロキシの転送先ポート番号と HazardFilter のフィルタリングサービス設定のポート番号に同じポート番号を設定してください。

▶ フィルタリングサービス設定

HTTP	* ポート 8085	* プロセス数 450
HTTPS	* ポート 8086	* プロセス数 450
プロセス数警告設定	プロセス使用率が以下を超えると警告通知を行う。 80 %	

※ 設定変更を反映するには、フィルタリングサービスの再起動が必要になります。
(同じ設定を使用する追加サーバでも、フィルタリングサービスの再起動が必要になります。)
※ 通知を有効にするには「メール通知設定」でサービス警告発生通知を有効にしておく必要があります。

Ⅱ. 注意事項、制限事項

- 透過プロキシ構成では、HazardFilter のアカウント認証は利用できません。
- 透過プロキシ構成では、https のポートと、http のポートを同一には設定できません。それぞれのポートを個別に設定する必要があります。
- 透過プロキシ構成の HTTPS 通信では転送先のホスト情報を SSL/TLS の拡張情報の SNI(Server Name Indication)から取得します。
- Google Chrome など、一般的な Web ブラウザのほとんどは SNI に対応しており問題ございませんが、SNI 非対応のアプリケーションからの通信など、SNI が取得できない場合は通信を遮断する仕様になっております。