



**NetSTAR**

<http://netstar.jp>

# URL単位での規制方法について

1.0版

2010年1月13日

Copyright(C) 2010 NetSTAR Inc., All rights reserved.

## はじめに

本マニュアルでは、URL単位で閲覧を許可/規制する手順を説明しています。  
『サイトアンパイアの初期設定』の設定が終わっていることを前提としているため  
まだ設定が終わっていない場合は、ブラウザより下記URLにアクセスし  
<http://www.netstar-inc.com/smb/router/rt58i/manual.html>  
『サイトアンパイアの初期設定』を先に実施して下さい。

デフォルトルールでは「オンラインゲーム」  
は規制対象



弊社で開設しているオンラインゲーム  
サイト[<http://samplegame.com>]は  
規制対象から外したい

対象サイトのURL名を入力

内部データベース

samplegame.com

フィルタタイプを「pass」にすることで  
<http://samplegame.com>サイトは  
デフォルトルールに関係なく閲覧可能に

「通信販売一般」は規制対象ではないが  
A店のサイトだけは規制対象としたい。



例) A店のサイト  
<http://A-shop.com>を  
をブラックリストとして登録

内部データベース

A-shop

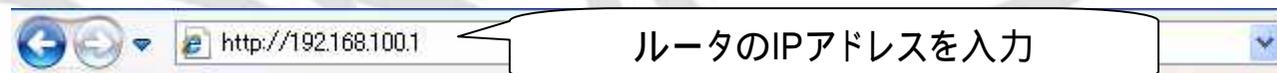
フィルタタイプ: reject

フィルタタイプを「reject」にすることで  
<http://A-shop.com>サイトはフィルタリング  
ルールに関係なく規制対象に

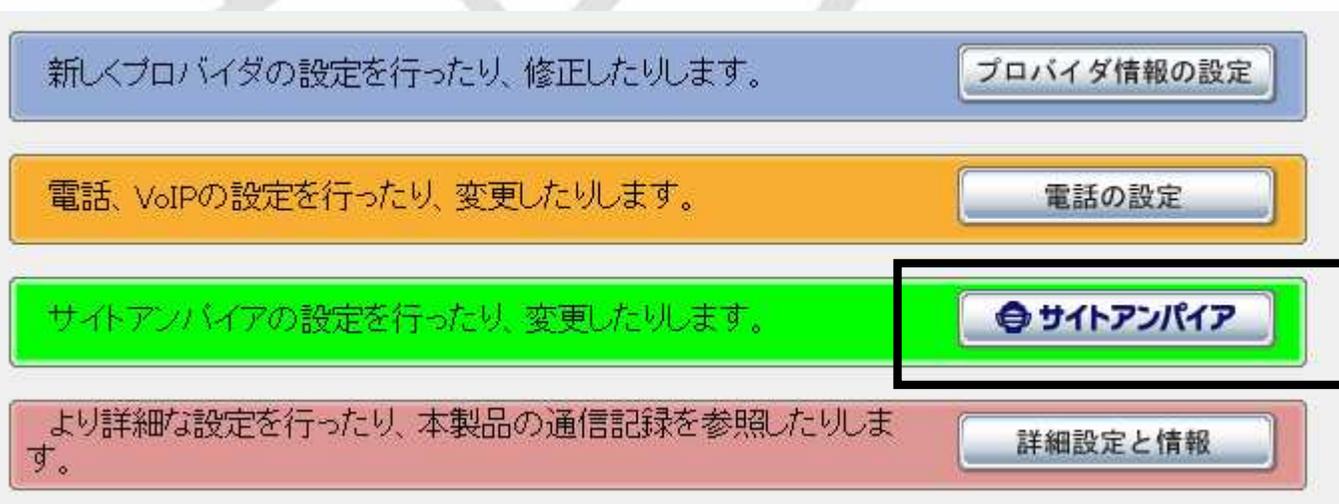


1. ブラウザのアドレスバーにルータのIPアドレスを入力し[Enter]キーをクリックして下さい。

デフォルト時は「http://192.168.100.1」(ルータに割り振られたIPアドレス)になります。



2. Top画面、黒四角で囲った箇所「サイトアンパイア」をクリックして下さい。



3. 黒四角で囲った「設定」をクリックして下さい。

### サイトアンパイアの設定 ヘルプ

[\[トップ\]](#) > [サイトアンパイアの設定]

#### URLフィルタの共通設定

URLフィルタの共通設定	設定
URLフィルタ(サイトアンパイア)の共通設定	設定

#### URLフィルタの設定インターフェース

インターフェース	設定名	URLフィルタ 入	URLフィルタ 出	状態の表示
LANポート		設定	設定	実行
WANポート	未設定	設定	設定	実行

トップへ戻る

#### 4. 黒四角で囲った「追加」をクリックして下さい。

内部データベース参照型URLフィルタの一覧

番号	適用	タイプ	ログ	キーワード	送信元 IPアドレス	削除
登録されていません						

追加

URLフィルタ(サイトアンパイア)の一覧

番号	適用	タイプ	ログ	カテゴリ	送信元 IPアドレス	削除
<a href="#">50</a>	<input checked="" type="checkbox"/>	reject	する	違法と思われる行為, 違法と思われる薬物, 不適切な薬物利用, テロリズム・過激派, 武器・兵器, 告発・中傷, 自殺・家出, 主張一般, 性行為, ヌード画像, 性風俗, アダルト検索・リンク集, ハッキング, 不正コード配布, 公開プロキシ, 検索キャッシュ, 出会い・異性紹介, 結婚紹介, ギャンブル一般, 宝くじ・スポーツくじ, オンラインゲーム, ゲーム一般, グロテスク, 成人娯楽, 水着・下着・フェチ画像, 文章による性的表現, コスプレ, オカルト, 同性愛, 広告・バナー, 懸賞, 迷惑メールリンク	*	<input type="checkbox"/>
<a href="#">127</a>	<input checked="" type="checkbox"/>	pass	しない	*	*	<input type="checkbox"/>

追加

5. 黒四角で囲んだ「フィルタ・タイプ」のプルダウンを開いて下さい。

特定のURLの閲覧を規制したい場合は5 - 1へ

特定のURLの閲覧を許可したい場合は5 - 2へ

サイトアンパイアの設 定		内部データベース参照型 URLフィルタの登録	ヘルプ
<a href="#">[トップ]</a> > <a href="#">[サイトアンパイアの設定]</a> > <a href="#">[URLフィルタ[入]側の設定[LANポート] LAN接続]</a> > <a href="#">[内部データベース参照型URL フィルタの登録]</a>			
<b>内部データベース参照型URLフィルタの登録</b>			
適用インタフェース	LAN		
フィルタ番号	0		
フィルタ・タイプ	pass (ログなし)		
キーワード	*		
送信元IPアドレス	*		
<b>設定の確定</b>			
<a href="#">トップへ戻る</a>			

## 5 - 1 . 特定のURLの閲覧を規制したい場合

黒四角で囲んだ「フィルタ・タイプ」を「reject(ログなし)」「reject(ログあり)」の何れかを  
選択して下さい。

(ログあり)を選択した場合は「[トップ] [詳細設定と情報] [URLフィルタの統計情報の表示]」にて、  
規制されたURLを確認することができます。

### サイトアンパイアの設 定

内部データベース参照型  
URLフィルタの登録

ヘルプ

[\[トップ\]](#) > [\[サイトアンパイアの設定\]](#) > [\[URLフィルタ\[入\]側の設定\[LANポート\] LAN接続\]](#) > [\[内部データベース参照型URL  
フィルタの登録\]](#)

#### 内部データベース参照型URLフィルタの登録

適用インタフェース	LAN
フィルタ番号	0
フィルタ・タイプ	pass (ログなし)
キーワード	pass (ログなし)
送信元IPアドレス	pass (ログあり)
	reject (ログなし)
	reject (ログあり)

設定の確定

トップへ戻る

## 5 - 2 . 特定のURLの閲覧を許可したい場合

黒四角で囲んだ「フィルタ・タイプ」を「pass(ログなし)」「pass(ログあり)」の何れかを  
選択して下さい。

(ログあり)を選択した場合は「[トップ] [詳細設定と情報] [URLフィルタの統計情報の表示]」にて、  
許可されたURLを確認することができます。

### サイトアンパイアの設 定

内部データベース参照型  
URLフィルタの登録

ヘルプ

[\[トップ\]](#) > [\[サイトアンパイアの設定\]](#) > [\[URLフィルタ\[入\]側の設定\[LANポート\] LAN接続\]](#) > [\[内部データベース参照型URL  
フィルタの登録\]](#)

#### 内部データベース参照型URLフィルタの登録

適用インタフェース	LAN
フィルタ番号	0
フィルタ・タイプ	pass (ログなし)
キーワード	<input type="text"/>
送信元IPアドレス	<input type="text"/>

pass (ログなし)  
pass (ログあり)  
reject (ログなし)  
reject (ログあり)

設定の確定

トップへ戻る

6. 黒四角で囲んだ「キーワード」にURLのキーワードを入れて下さい。  
例では[http://www.netstar-inc.com]を登録するために、「\*」を消して、キーワードとなる「netstar」を入力しています。  
入力が終わったら「設定の確定」をクリックして下さい。

### サイトアンパイアの設定

内部データベース参照型 URLフィルタの登録 ヘルプ

[\[トップ\]](#) > [\[サイトアンパイアの設定\]](#) > [\[URLフィルタ\[入\]側の設定\[LANポート\] LAN接続\]](#) > [\[内部データベース参照型URLフィルタの登録\]](#)

#### 内部データベース参照型URLフィルタの登録

適用インタフェース	LAN
フィルタ番号	0
フィルタ・タイプ	reject (ログあり)
キーワード	netstar
送信元IPアドレス	*

設定の確定 トップへ戻る

7. 「トップへ戻る」をクリックして下さい。

2つ以上キーワードを登録したい場合は、再度同じ手順を実施して下さい。

**サイトアンパイアの設定** 内部データベース参照型URLフィルタ  
の登録

[\[トップ\]](#) > [\[サイトアンパイアの設定\]](#) > [\[URLフィルタ\[入\]側の設定\[LANポート\] LAN接続\]](#) > [\[内部データベース参照型URL  
フィルタの登録\]](#)

内部データベース参照型URLフィルタの登録

フィルタを登録しました。