

Web コンテンツフィルタサービス 利用・管理マニュアル

「お客さまシステム管理者さま向け」

2011 年 10 月 19 日 Version 1.8

bit-drive

目次

1	マニュアルの概要	3
2	ご利用にあたっての注意点	3
2-1	注意事項.....	3
3	管理サーバへのログインおよび基本設定.....	4
3-1	管理サーバへログインする.....	4
3-2	IPアドレスを確認する.....	5
3-3	アカウント・パスワードを変更する	6
4	フィルタールールの設定(簡易設定)	7
4-1	フィルタールールを登録する.....	7
4-2	フィルタールールを適用する.....	9
5	フィルタールールの設定(詳細設定)	12
5-1	フィルタールールを変更・削除する	12
5-2	ルールを適用するスケジュールを設定する	13
5-3	スケジュールを変更・削除する.....	16
5-4	例外URLを設定する.....	18
5-5	規制オプションを設定する.....	20
5-6	カテゴリ別規制メッセージを設定する	22
6	URLのデータベース登録状況の確認.....	24
6-1	URLのデータベース登録状況を確認する.....	24
7	アクセスログの管理	26
7-1	アクセスログをダウンロード・削除する.....	26
8	サービスを利用するための設定.....	27
8-1	プロキシサーバがある場合の設定.....	27
8-2	プロキシサーバがない場合の設定(例:Windows Internet Explorer).....	28
9	よくある質問	30

1 マニュアルの概要

この手順書は、Web コンテンツフィルタサービスをご利用になるための手順について説明しています。
お客さまの技術担当者さまにおいて、利用開始・設定変更の際にご覧ください。

2 ご利用にあたっての注意点

2-1 注意事項

[1] 事前設定

サービスのご利用にあたり、「8 サービスを利用するための設定」を必ず一読ください。

[2] httpsサイトの規制

https のサイトを規制対象に設定した場合、以下の制限事項がありますのでご注意ください。許可カテゴリであれば、通常どおり閲覧可能となります。

- 規制画面にカテゴリが表示されません。
- オーバーライドの動作は、規制と同じになります。
- 書き込みの規制は行えません。書き込みが可能になります。
- 規制画面表示時に証明書の警告が表示されます。

これは、Web ブラウザが元のアクセス先のサイト名と規制画面のサイト名が一致していないと認識して表示するものですので、規制動作に問題はありません。

[3] 管理サーバへのアクセスについて

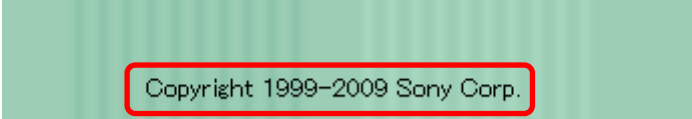
管理サーバ(<https://www.filter.bit-drive.ne.jp:8443>)へは、フィルタサーバを介してアクセスしないようにお願いします。

- ブラウザのプロキシ設定において、例外リストに「www.filter.bit-drive.ne.jp」を記入してください。
- 社内プロキシも、可能な限り、管理サーバへは上位プロキシのフィルタサーバ経由ではなく社内プロキシから直接アクセスするように設定してください。

[4] ネットワークサーバー"DigitalGate"を社内プロキシとして使用している場合

DigitalGate のバージョンを Ver.2.01 build27 以上にバージョンアップしてご利用ください。

バージョンの確認は、DigitalGate のシステム管理用トップページから以下を赤枠部分をクリックし、ご確認ください。



Copyright 1999-2009 Sony Corp.

3 管理サーバへのログインおよび基本設定

3-1 管理サーバへログインする

[1] Webブラウザを起動し、<https://www.filter.bit-drive.ne.jp:8443/>にアクセスします。

[2] 「アカウント」に「コンテンツフィルタID¥admin」と入力します。

※「コンテンツフィルタ ID」は、bit-drive からお送りしております「ご利用 ID 確定のお知らせ」メールに記述されています。

[3] 「パスワード」に「パスワード」を入力します。

※「パスワード」は、bit-drive からお送りしております「コンテンツフィルタ ID」のパスワードのお知らせ」メールに記述されています。

[4] 「ログイン」をクリックします。



3-2 IPアドレスを確認する

[1] 「グループ/ユーザ管理」をクリックします。



[2] 「コンテンツフィルタID」をクリックします。

[3] フィルタサーバにアクセス可能なIPアドレスの範囲をご確認ください。

※「グループ名」の変更は絶対にしないでください



3-3 アカウント・パスワードを変更する

[1] 「アカウント」をクリックします。

[2] 3-1.2 でログイン時に利用した「admin」部分を変更する場合は、「アカウント」に変更後の文字列を入力します。

[3] 「パスワード」を変更する場合は、「パスワード」および「パスワード(確認)」に入力します。

[4] 「更新」をクリックします。

※メールアドレスを設定することもできます。

このメールアドレスは、データベース登録を依頼に対する NetSTAR 社の返信先として利用されます。

(「5-4 例外 URL を登録する」と「6-1 URL のデータベース登録状況を確認する」をご覧ください)



The screenshot shows the INTERSAFE web interface for user management. The main content area is titled 'グループユーザ選択' (Group User Selection). On the left, there is a search box for accounts, showing a result for 'CF99999-9999'. Below this are buttons for '追加' (Add), '移動' (Move), '削除' (Delete), and '全削除' (Delete All), along with a 'CSV出力' (CSV Export) button. The main table has a header 'アカウント更新' (Account Update) and a sub-header 'アカウント情報を更新します。' (Update account information). The table contains one row with the following fields: 'グループ' (Group) set to 'CF99999-9999', 'アカウント' (Account) set to 'admin', 'パスワード' (Password) set to '*****', 'パスワード(確認)' (Password Confirmation) set to '*****', 'メールアドレス' (Email Address) (empty), and 'グループ管理者' (Group Administrator) checked. A red box highlights the '更新' (Update) button in the top right corner of the table. At the bottom left of the interface, there is a navigation menu with 'IPアドレス' (IP Address) and 'アカウント' (Account) highlighted, and the ALSI logo.

4 フィルタールールの設定(簡易設定)

4-1 フィルタールールを登録する

- [1] 「フィルタリング設定」をクリックします。
- [2] 「コンテンツフィルタID」をクリックします。
- [3] 「カテゴリ別ルール登録」をクリックします。



- [4] 「カテゴリ別ルール選択」で、「DEFAULT RULE」を選びます。
- [5] 「選択」ボタンをクリックします。

※グループ選択では、「ルートグループ」と「ID」が選択可能ですが、初期はルートグループしか選択できません。1つ以上のルール登録後は、「ID」を選択することが可能となります。

※「ルートグループ」を選択すると「DEFAULT RULE」「小学校」「中学校」「高校」「大学」「企業」「官公庁」の6つの中から選択が可能となりますが、ここでは、新たにルールを作成するために使用するテンプレートを選択することができます。



[6] 「カテゴリ別ルール名」に登録したい任意のルール名を入力します。

[7] 各カテゴリに対し、お客さまのポリシーに合わせ規制内容の設定を行います。

<規制内容>

- 許可

自由にアクセスを許可します。
- オーバーライド

規制画面を表示しますが、パスワードを入力すると一定時間だけ許可動作になります。パスワードや有効時間は、規制オプション設定画面で設定できます。

※デフォルトではパスワードなしでオーバーライドを利用する設定になっています。
- 書き込み規制

掲示板などへの書き込みを禁止します。

対象の URL は、http プロトコルで POST、PUT メソッドを使用しているもののみとなります。

※https や Java を使用したサイトは書き込み規制の対象になりません。
- 規制

アクセスを規制し、規制画面を表示します。

[8] 「登録」ボタンをクリックします。

「登録が完了しました。」と画面の上部に表示されます。

[9] 「コンテンツフィルタID」をクリックし、TOPページに戻ります。

この時点では、まだルールが適用されていないのでご注意ください



4-2 フィルタルールを適用する

[1] 「スケジュール設定へ」をクリックします。



[2] 「選択」をクリックします。



[3] 「基本設定」→「基本ルール」→「グループ>カテゴリ別ルール」をお客さまの「コンテンツフィルタID」と「登録したルール」を選択し「更新」をクリックします。

「更新が完了しました」と画面の上部に表示されます。

※この時点で登録したルールが適用されます。

[4] 「コンテンツフィルタID」をクリックし、TOPページに戻ります。



ALSI

[5] 「グループ適用フィルタリング表示」をクリックします。



ALSI

[6] 「フィルタリング情報」にて現在のルール適用状況を確認できます。

グループ適用フィルタリング設定情報

スケジュール情報 | 例外URL | 規則アクション | カテゴリ別規制メッセージ | 閉じる

グループ: CF9999-9999

■ フィルタリング情報

当該グループユーザには以下のフィルタリングを設定しています。

カテゴリ別ルール: *DEF.ALL RULE | *アダルト禁止

スケジュール

曜日	2	4	6	8	10	12	14	16	18	20	22	24
月												
火												
水												
木												
金												
土												
日												

特定日一覧

日付	曜日
2009/3/20 日	
2009/4/29 日	
2009/5/3 日	
2009/5/4 日	
2009/5/5 日	

あと58件の登録があります

[7] 適用されている時間帯(グレー部)をクリックすると、ルール情報が表示されます。

カテゴリ別フィルタリングルール情報

閉じる | 戻る

■ カテゴリ別フィルタリングルール

カテゴリ別フィルタリングルールが設定されています。

カテゴリ別ルール: アダルト禁止

所有グループ: CF9999-9999

凡例: 許可 オーバーライド 書き込み規制 規制

オーバーライドがカテゴリでは一定時間間隔することができます。
また、書き込み規制がカテゴリではサイトへの書き込みが行えません。

カテゴリ	サブカテゴリ	設定
ユーザ設定		
	ユーザ設定1	<input checked="" type="checkbox"/>
	ユーザ設定2	<input checked="" type="checkbox"/>
	ユーザ設定3	<input checked="" type="checkbox"/>
	ユーザ設定4	<input checked="" type="checkbox"/>
	ユーザ設定5	<input checked="" type="checkbox"/>
	ユーザ設定6	<input type="checkbox"/>
	ユーザ設定7	<input type="checkbox"/>
	ユーザ設定8	<input type="checkbox"/>
	ユーザ設定9	<input type="checkbox"/>
	ユーザ設定10	<input type="checkbox"/>
不法	違法と思われる行為	<input checked="" type="checkbox"/>

5 フィルタルールの設定(詳細設定)

5-1 フィルタルールを変更・削除する

- [1] 「フィルタリング設定」をクリックします。
- [2] 「コンテンツフィルタID」をクリックします。
- [3] 「カテゴリ別ルール変更・削除」をクリックします。



- [4] 変更・削除したいルールをプルダウンメニューから選択します。
- [5] 「選択」ボタンをクリックします。



[6] カテゴリごとに規制の内容を変更します。規制ルールの詳細は、「4-1 フィルタルールの登録」をご覧ください。

[7] 変更の場合は「更新」ボタンをクリックします。削除の場合は「削除」ボタンをクリックします。

※スケジュールに適用されているルールは削除できません。スケジュールの適用を外してから削除してください。

※スケジュールの変更・削除後は、フィルタルール適用状況確認画面にてルールの適用状況を確認してください。



5-2 ルールを適用するスケジュールを設定する

[1] 「フィルタリング設定」をクリックします。

[2] 「コンテンツフィルタID」をクリックします。

[3] 「スケジュール設定へ」をクリックします。



[4] 「選択」をクリックします。



[5] 新たなルールを適用する曜日、時間を選択します。

[6] その曜日、時間に適用したいルールを選択します。

[7] 「登録」ボタンをクリックします。

※例えば、通常の業務時間は厳しいルール1を適用するが、昼休み時間は規制の弱いルール2を適用するなどが可能となります。

※複数のスケジュールを登録することも可能です。



[8] 「コンテンツフィルタID」をクリックしTOPページに戻ります。

[9] 「グループ適用フィルタリング表示」をクリックします。



[10] 適用されたスケジュールを確認します。

グループ適用フィルタリング設定情報

スケジュール情報 例外URL 規制オプション カテゴリ別規制メッセージ 閉じる

グループ CF9999-9999

■フィルタリング情報

当該グループユーザには以下のフィルタリングを設定しています。

カテゴリ別ルール

- ★DEF.ALSI RULE
- アダルト禁止

スケジュール

曜日	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
日																								
月																								
火																								
水																								
木																								
金																								
土																								
日																								

特定日一覧

日付	曜日
2009/3/20 日	
2009/4/29 日	
2009/5/3 日	
2009/5/4 日	
2009/5/5 日	

あと58件の登録があります

5-3 スケジュールを変更・削除する

- [1] 「フィルタリング設定」をクリックします。
- [2] 「コンテンツフィルタID」をクリックします。
- [3] 「スケジュール設定へ」をクリックします



- [4] 「選択」をクリックします。



- [5] 曜日時間を変更する場合は、新たな曜日、時間を選択します。
- [6] ルールを変更する場合は、新たなルールを選択します。
- [7] 「更新」ボタンをクリックします
- [8] スケジュールを削除したい場合は、「削除」をクリックします。



[9] 「コンテンツフィルタID」をクリックしTOPページに戻ります。

[10] 「グループ適用フィルタリング表示」をクリックします。



[11] 適用されたスケジュールを確認します。

グループ適用フィルタリング設定情報



5-4 例外URLを設定する

- [1] 「フィルタリング設定」をクリックします。
- [2] 「コンテンツフィルタID」をクリックします。
- [3] 「例外URL設定へ」をクリックします



- [4] 「例外URL登録へ」をクリックします。

※「例外 URL 送信」をチェックする必要はありません。チェックしなくても例外 URL の設定は可能です。

- 「例外 URL 送信」チェックボックスがオンになっている状態で、例外 URL が登録されると、「例外 URL を送信しますか」という確認のポップアップが立ち上がります。
- ここで「OK」を押すと、例外 URL が NetSTAR 社に送信されます。
- 例外 URL を送信すると、NetSTAR 社で審査が行われます。NetSTAR 社ではお客さまからのフィードバックを DB の精度向上に役立てています。
- 結果については、メールで返信されますのでチェックを入れた場合は、返信先のメールアドレスを、「グループ/ユーザ管理」メニューから、管理者のメールアドレスを設定してください。
- 「例外 URL 送信」が適用されるには、「更新」ボタンをクリックします。



[5] 「カテゴリ」「サブカテゴリ」を選択します。

[6] 例外としたいURLを入力します。

[7] 「登録」ボタンをクリックします。

※URL の指定がプロトコルのみの場合、そのプロトコル全体を指定したことになります。

許可カテゴリは、全体の URL の入力が必要です。許可カテゴリには、utext,ufile を指定できません。



「URL」の入力

- http:// HTTP を使用する URL
- https:// HTTPS を使用する URL。
- ftp:// FTP over HTTP を使用する URL
- utext:// 入力した文字列を含む URL を指定する場合に使用します。

(例)「utext://chat」とすると以下のような URL が該当する

chat.bit-drive.ne.jp、www.bit-drive.ne.jp/chat.cgi、www.bit-drive.ne.jp/chat/main.html

- ufile:// ファイルの拡張子(末尾)を指定します

(例)「ufile://cgi」とすると以下のような URL が該当する

www.bit-drive.ne.jp/board.cgi、www.bit-drive.ne.jp/cgi-bin/register.cgi

[8] 登録結果を確認してください。



5-5 規制オプションを設定する

- [1] 「フィルタリング設定」をクリックします。
- [2] 「コンテンツフィルタID」をクリックします。
- [3] 「規制オプション設定へ」をクリックします



[4] 各項目を入力します。

- 規制メッセージ:
規制画面に表示するメッセージを変更したい場合に入力します。
- オーバーライドパスワード:
オーバーライド規制をかけたページをみるためのパスワードを設定できます。パスワードが空欄の場合は、パスワードなしでオーバーライドを利用できます。
- オーバーライドタイマー:
オーバーライドを有効にする制限時間を設定できます。(初期値は 120 秒、1 秒から 3600 秒を設定可能)
- オーバーライド: 表1を参照。
- IP アドレス規制:
有効にすると、IP アドレスで指定されたリクエストを拒否します。(URL が IP アドレスになっているもの)
- 検索キーワード規制: 検索サイトなどで、指定したキーワードを使用した検索を規制します。
- 規制検索キーワード: 検索キーワード規制のキーワードをここで指定します。
キーワードを最大 20 文字で設定します。テキストボックスにキーワードを入力し、「追加」ボタンをクリックします。登録したキーワードを変更、削除する場合、キーワードをクリックして、「変更」または「削除」ボタンをクリックします。
- 書き込み規制: 表1を参照。

[5] 「更新」ボタンをクリックします。



表1

カテゴリ別 ルールでの規制内容	規制オプション設定		オーバーライド 有効		オーバーライド 無効		オーバーライド 無効	
	書き込み規制	有効	書き込み規制	有効	書き込み規制	無効	書き込み規制	無効
規制	オーバーライド問い合わせ パスワード入力後は許可	オーバーライド問い合わせ パスワード入力後は許可	オーバーライド問い合わせ パスワード入力後は許可	オーバーライド問い合わせ パスワード入力後は許可	規制		規制	
オーバーライド	オーバーライド問い合わせ パスワード入力後は許可	オーバーライド問い合わせ パスワード入力後は許可	オーバーライド問い合わせ パスワード入力後は許可	オーバーライド問い合わせ パスワード入力後は許可	オーバーライド問い合わせ パスワード入力後は 閲覧可能 書き込みは規制		オーバーライド問い合わせ パスワード入力後は許可	
書き込み規制	閲覧可能。書き込み時、 オーバーライド問い合わせ パスワード入力後は許可	閲覧可能。書き込み時、 オーバーライド問い合わせ パスワード入力後は許可	閲覧可能。書き込み時、 オーバーライド問い合わせ パスワード入力後は許可	閲覧可能。書き込み時、 オーバーライド問い合わせ パスワード入力後は許可	閲覧可能 書き込み規制		閲覧可能 書き込み規制	
許可	閲覧可能。書き込み時、 オーバーライド問い合わせ パスワード入力後は許可		許可		閲覧可能 書き込み規制		許可	

※カテゴリ別ルールで設定したものより、規制オプションが優先的に適用されます

また、規制オプションのオーバーライドと書き込み規制が両方有効の場合は、オーバーライドになります。(=書き込み規制にはなりません。常にオーバーライド画面になります)

※書き込み処理時にオーバーライド画面が表示された場合は、パスワード入力後の遷移画面には以前に入力した内容は、クリアされてしまい書き込みに反映されません。

「オーバーライド」実行後、「オーバーライドタイマー」にて設定された時間内は書き込みを行うことができます。

[6] 登録結果を確認してください。



5-6 カテゴリ別規制メッセージを設定する

- [1] 「フィルタリング設定」をクリックします。
- [2] 「コンテンツフィルタID」をクリックします。
- [3] 「カテゴリ別規制メッセージ設定へ」をクリックします



[4] 各カテゴリに対して、個別に規制画面のメッセージを入力します。

※「規制オプション」で全体への規制メッセージを設定している場合には、両方が表示されます。

[5] 「更新」ボタンをクリックします。



INTERSAFE

POST NOW Powered By NetSTAR Inc.

HOME ID7722

グループユーザ管理 ファイルダウンロード管理 アクセス管理

グループ設定 個別ユーザ設定

グループ設定

CF9999-9999

カテゴリ別規制メッセージ設定

カテゴリ別規制メッセージを設定します。 **更新**

カテゴリ名	カテゴリ別規制メッセージ
ユーザ設定	
不法	
著作権	
アダルト	
セキュリティ・プロキシ	
出会い	
金融	
ギャンブル	
ゲーム	
ショッピング	
コミュニケーション	

6 URLのデータベース登録状況の確認

6-1 URLのデータベース登録状況を確認する

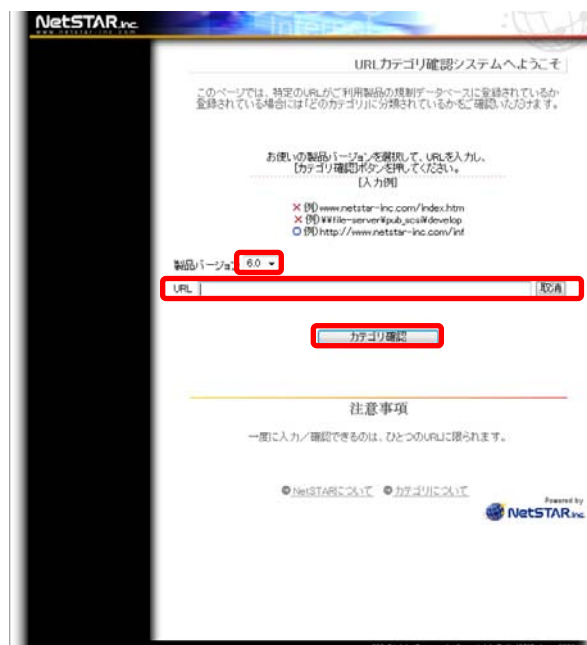
[1] 右上にある「NetSTAR」のバナーをクリックします。



[2] 「製品バージョン」で 6.0 を選択してください。

[3] 「URL」に確認したいURLを入力します。

[4] 「カテゴリ確認」をクリックします。



- 登録されている場合

「確認の結果」に登録先のカテゴリが表示されますのでご確認ください。

確認の結果

■ 入力されたURL

http://news.xxxxx.xx.jp

■ 確認の結果

カテゴリ : 2501.[ニュース]-[ニュース一般] に登録されております。

*URLのカテゴリ分類作業は、所定の基準に従い、細心の注意を払って進めておりますがカテゴリ分類に誤りがある場合や、内容についての疑問や不明点がございましたら、製品マニュアルに記載されているサポート窓口へお問い合わせください。

*連続して操作する場合は、この画面の「閉じる」ボタンを押してウィンドウを閉じてください。

- 登録されていない場合

「確認の結果」に「指定 URL は登録されておられません。」と表示されます。その場合、メールアドレスの入力欄が表示されます。データベースへの登録を希望する場合は、メールアドレス欄に登録結果の回答先メールアドレスを入力して「登録」ボタンを押してください。

メールアドレスを入力せずに「登録」ボタンを押した場合、「グループ/ユーザ管理」メニューから設定する管理者のメールアドレスへ登録結果が送信されます。

確認の結果

■ 入力されたURL

http://www.bit-drive.ne.jp

■ 確認の結果

カテゴリ : 指定URLは登録されておられません。

■ データベース候補リスト登録

*データベース候補リストへ登録をご希望の場合は、「メールアドレス」に登録結果の回答先メールアドレスを入力して「登録」ボタンを押してください。

「メールアドレス」を入力せずに「登録」ボタンを押した場合、登録者ご自身のアカウント情報に設定されたメールアドレス、またはシステム管理者指定の連絡先へ登録結果が送信されます。

*登録せずに連続して操作する場合は、この画面の「閉じる」ボタンを押してウィンドウを閉じてください。

メールアドレス:

7 アクセスログの管理

7-1 アクセスログをダウンロード・削除する

- [1] 「アクセス管理」をクリックします。
- [2] 「アクセスログ管理」をクリックします。
- [3] 対象のファイルをチェックします。

※ダウンロードはローテート済みのログが対象となります。

- [4] ダウンロードする場合は「ダウンロード」をクリックします
- [5] 削除する場合は「削除」をクリックします

※ログファイルは1日毎に、前日以前のものが表示されます。ファイル名の日付から1日前のログになります(更新日時を参考にしてください)。

※ログファイルは31日分がサーバに保管されます。それ以降は自動で削除されますので、早めのダウンロードをお願いいたします。(ダウンロード後は削除してください)



アクセスログのフォーマット

```
2009/01/04,12:02:31,"HTTP","202.94.143.xxx","CF99999-9999","","","Allowed","",0,"www.bit-drive.ne.jp",0,0,"","コミュニケーション¥掲示板","http://www.bit-drive.ne.jp/cgi-bin/bbs.cgi?"
2009/01/04,12:07:00,"HTTP","202.94.143.xxx","CF99999-9999","","","Blocked","",0,"news.bit-drive.ne.jp",0,0,"text",
```

以下の CSV 形式になっています。

『日付,時間,プロトコル名,ソースIP,ID,(未使用),(未使用),転送状態,(未使用),(未使用),リクエスト先サーバホスト名,(未使用),(未使用),ファイルタイプ、カテゴリ名、リクエストURL』

転送状態は以下の5種類が記録されます。

- Blocked(ルールにて規制を適用した URL)
- Allowed(ルールにて許可を適用した URL)
- Release(ルールにてオーバーライドを適用した URL)
- BkPost(ルールにて書き込み規制を適用した URL)

また、ファイルタイプは、ファイルタイプが特定された場合のみ出力されます。

本サービスでは記録されない項目については(未使用)となります。

なお、規制カテゴリに登録されていない URL へのアクセスの場合はアクセスログに記録されません。

8 サービスを利用するための設定

8-1 プロキシサーバがある場合の設定

[1] 社内プロキシの設定

社内プロキシは上位プロキシに以下を指定してください。

アドレス : proxy.filter.bit-drive.ne.jp

ポート : 8080

可能な限り社内プロキシから管理サーバには、直接アクセスするように設定してください。

・例として、Squid の追加設定を挙げます

```
cache_peer proxy.filter.bit-drive.ne.jp parent 8080 0
acl Safe_ports port 80 21128
acl SSL_ports port 443
acl www_filter_server dstdomain www.filter.bit-drive.ne.jp
always_direct allow www_filter_server
```

※社内サイトへの通信に社内プロキシを経由させなければならない場合は、以下の設定を追加してください
(アドレスなどは環境に合わせてください)。

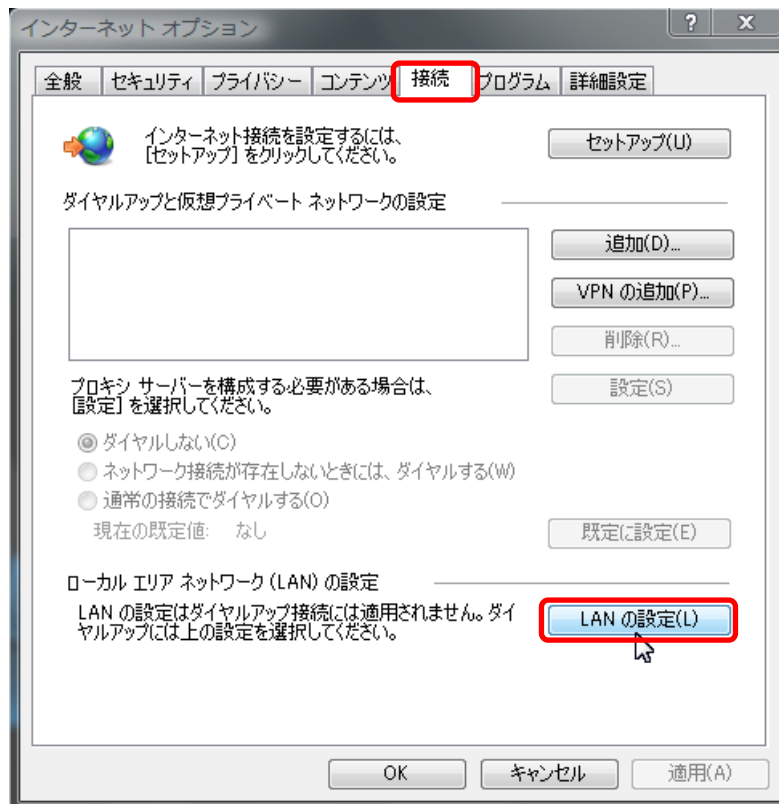
```
acl local-servers dst 192.168.0.0/16
always_direct allow local-servers
```

※上位プロキシとして弊社マネージドイントラネットをご利用のお客さまは、オンラインマニュアルをご覧ください。

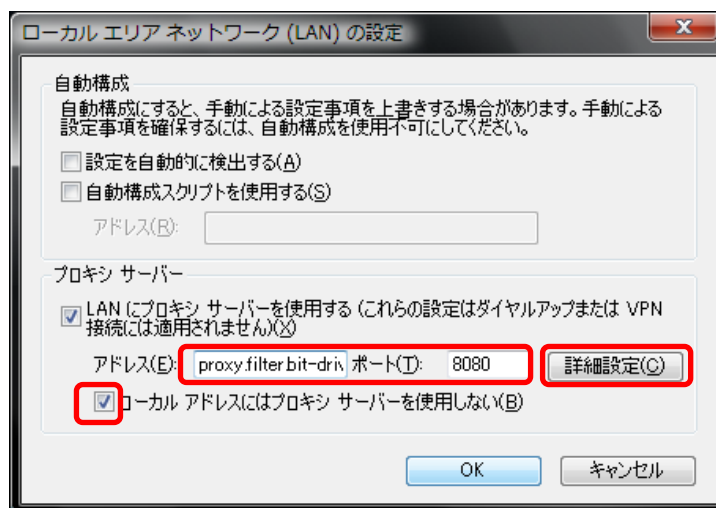
オンラインマニュアル目次 > システム管理メニュー > サービスサーバ > サーバ設定 > プロキシ > 上位プロキシ

8-2 プロキシサーバがない場合の設定(例: Windows Internet Explorer)

- [1] 本サービスを利用するクライアントPCにてWindows Internet Explorerを起動します。
- [2] 「ツール」→「インターネットオプション」→「接続」タブ→「LANの設定」をクリックします。



- [3] 「LANにプロキシサーバを使用する」にチェックを入れます。
- [4] 「アドレス」に「proxy.filter.bit-drive.ne.jp」を入力します。
- [5] 「ポート」に「8080」を入力します。
- [6] 「ローカルアドレスにはプロキシサーバを利用しない」にチェックをします。
- [7] 「詳細設定」ボタンをクリックします。



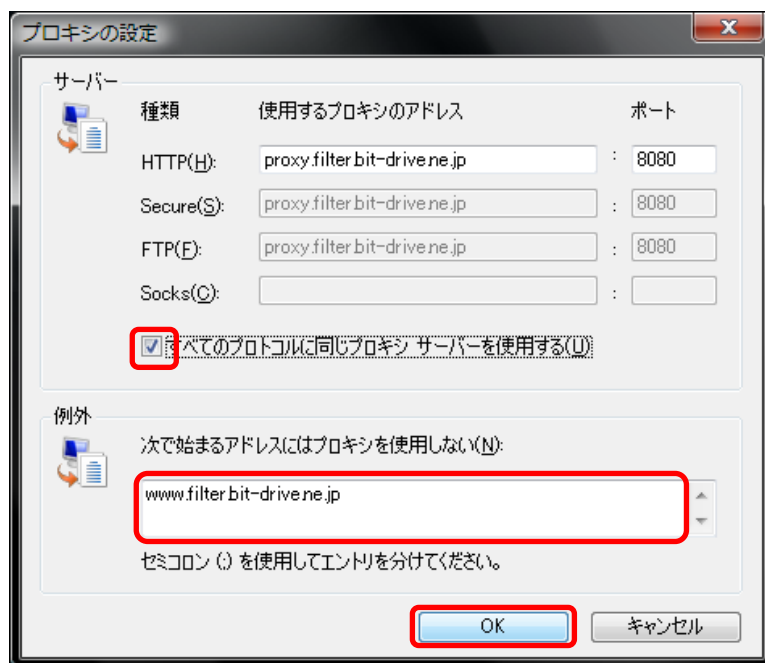
[8] 「すべてのプロトコルに同じプロキシサーバを使用する」をチェックします。

[9] 「例外」に社内サイトのアドレスを入力します。

※企業管理者は、「www.filter.bit-drive.ne.jp」を入力してください。

[10] 「OK」をクリックします。

※その他のブラウザをお使いの方は、各ブラウザのマニュアルをご確認ください。



9 よくある質問

Q 現在、URL データベースに登録されているおおよそのページ数を教えてください。

A おおよそ約 7,148 万ページ(2008 年 4 月現在)規制対象となっており、このうち約 7 割が日本語で記述されたページです。登録されるページは日々増加します。

Q URL データベースはいつ更新されますか？

A 毎日 3 回以上更新されます。

Q 海外のサイトも登録されていますか？

A サイトのあるサーバの所在地に関係なく、登録しております。また日本語以外では、英語・中国語等のアダルトサイトを中心に登録してあります。

Q データベースの内容を公開してもらえますか？

A 申し訳ありませんが、データベースは非公開となっております。

管理画面より使用可能な URL 検索サイトがご利用できます。管理画面にある NetSTAR 社ロゴボタンをクリックすると検索ウィンドウが開きます。任意の URL を入力してご確認ください。

Q 規制されていない URL を見つけた場合は？

A 管理画面にある NetSTAR 社ロゴボタンをクリックし、URL が未登録であることを確認のうえ、NetSTAR 社へ登録依頼することもできます

なおその際は、NetSTAR 社よりメールにて回答を差し上げるメールアドレスを記入してください。

Q 管理画面のグループ/ユーザ管理画面にて、グループ名(ID)の更新ができてしまいますが？

A 誠に申し訳ございませんがグループ名(ID)は変更なされないようお願いいたします。

万が一変更してしまった場合は、大変お手数ではございますが bit-drive インフォメーションセンターまでご連絡いただきますようお願い申し上げます。

Q どのような基準でフィルタリングされるのですか？

A 76 のカテゴリに該当するサイトをフィルタリング可能です。

日本の法令や文化、流行、お客さまからのご要望を元に独自の基準による分類方式を採用し、単に有害なサイトだけではなく、業務でのインターネット利用に際し、不必要と思われるサイトを規制できるようなカテゴリをご用意しております。

Q 規制されるサイトを許可したいのですが？

A 例外 URL にて、【許可カテゴリ】に対象となる URL をご登録ください。

Q カテゴリを追加することはできますか？

A できません。ただし、「ユーザ設定」というカテゴリを用意しています。10種類ですがお客さま専用の分類として、新たなカテゴリとして扱うことが可能です。

Q ルールに規制を加えたが、ブラウザでアクセスしても規制画面にならない

A プロキシやブラウザのキャッシュが使用されている可能性があります。ブラウザの再起動やキャッシュを削除後、再度確認をお願いいたします。

Q 規制対象が https のサイトの場合、規制画面しか表示されません。

A 規制対象が https のサイトの場合は規制のみの動作となり、オーバーライドなどを指定しても規制画面になります。また規制画面にはカテゴリが表示されません。https を許可対象にした場合は、通常の動作となります。

Q 規制対象の https のサイトにアクセスした場合、証明書の警告ウインドウが表示される。

A https の規制画面を表示する際の証明書が使用されるためです。この時ブラウザは、元のサイトから規制画面の証明書が使用されるためにサイト名が一致せず警告ウインドウが現れます。https 用規制画面の証明書は認証機関から発行した正規のものでございますのでご安心ください。

URL の規制動作に影響はなく、警告ウインドウで続行して(「はい」を押す)いただくと規制画面に遷移します。ただし上の Q&A の通りオーバーライドなどを指定していても規制画面になります。

なお対象のサイトが許可カテゴリの場合、警告ウインドウは出現しません。

Q Web メール、メッセージなどの使用を規制することは可能か？

A カテゴリの「コミュニケーション」→「メッセージ」や「ウェブメール」を規制対象にご指定いただければ規制されます。

ただし、ウェブメールなどで https を使用していると、上記の Q&A の現象が起こりますのでご了承ください。

Q ブラウザからのファイルのダウンロードを規制することは可能ですか？また対応するプロトコルは何ですか？

A 規制対象プロトコルは、HTTP, HTTPS, FTP over HTTP の3つです。これらのプロトコルを使用してアクセスする場合には、ブラウザやソフトウェアの種類に関わらず、フィルタリングを行うことが可能です。

Q FTP サイトが規制されません。

A デフォルト設定の Windows Internet Explorer はプロキシの設定がされていても直接 FTP サイトにアクセスを試みます。Windows Internet Explorer のインターネットオプションの詳細設定タブ内のブラウザ項目で、「FTP サイト用フォルダビューを使用する」にチェックをはずしてください。チェックをはずすと、プロキシ経由で FTP サイトにアクセスするようになります。

Q 利用可能な OS やブラウザには制限はありますか？

A 基本的には、プロキシ設定可能なブラウザであれば制限はありません。

Q あるサイトにアクセスした際、別ウィンドウで表示される広告や、ページの一部にアダルト画像が貼り付けられている場合などは、どのように動作するのでしょうか？

A ベースとなるフレームセットのページが規制対象であった場合、ページ自体が表示されませんが、外部へのリンクなどで一部のフレームのみが規制対象となる場合、該当のフレームのみが規制画面になります。また、バナーなど画像ファイルのみが規制対象リンク先の場合、その画像だけが表示されません(Windows Internet Explorer であれば、×マーク)。独立したポップアップウィンドウの場合も同様の現象となります。

Q ファイアウォールを使用していますが、フィルタリングサービスを利用する際、変更などは必要でしょうか？

A フィルタサーバへアクセスするため、フィルタサーバの TCP ポート 8080 番へのアクセスを許可してください。

また、管理サーバへは、TCP ポート 8443 番を許可してください。

なお、各サーバの IP アドレスは変更することもありますのでご了承ください。

Q 社内に既にプロキシがあるが、その上位プロキシとしてフィルタサーバを利用できますか？

A 可能です。詳細な設定や注意事項についてはマニュアルをご覧ください。bit-drive インフォメーションセンターまでお問い合わせください。

なお、DigitalGateを社内プロキシとしてご利用のお客さまは、上位プロキシの設定を行うとDigitalGate経由ではお客さまの社内サイトにアクセス不可となります。詳細はマニュアルをご覧ください。bit-drive インフォメーションセンター、bit-drive DigitalGate ヘルプデスクまでお問い合わせください。

Q 管理サーバにフィルタサーバ経由でアクセスしても構わないか？

A 可能な限り、管理サーバに対してはフィルタサーバを経由しないようお願いいたします。

Webブラウザの除外リストにwww.filter.bit-drive.ne.jpを設定いただきますようお願いいたします。

お客さまの社内にプロキシがありフィルタサーバを上位プロキシとして設定いただく場合も、管理サーバ(www.filter.bit-drive.ne.jp)に対しては社内プロキシから直接アクセスいただくようお願いいたします。

詳細はマニュアルをご覧ください。bit-driveインフォメーションセンターまでお問い合わせください。

Q ウィルス対策ソフトを使用しています。動作に問題はないでしょうか？

A 問題ありません。Web ブラウザと同様にプロキシとしてフィルタサーバをご指定してください(お客さま社内にプロキシがある場合はそちらをご指定ください)。

Q サービスを利用することで Web の閲覧速度が遅くなったりすることはないのでしょうか？

A Web サイトの画面表示を行う前に規制有無を確認するため、画像が多く貼り付けられたページなどでは若干表示速度が遅くなる場合があります。しかしながら、規制有無の確認には 100 分の 3~4 秒程度の時間しか要さないため、通常の閲覧において明らかに遅くなったと感じるようなことはありません。

Q 例外 URL 設定にて規制対象 URL に <http://www.sample.co.jp/index.html> を登録した場合、<http://www.sample.co.jp/>はアクセスできてしまいます。

A あくまで「<http://www.sample.co.jp/index.html>」に対して DB との照合を行っているため規制されません。

Q 例外 URL 設定にて、https のサイトのディレクトリ以下を入力できないと表示されます。

A プロトコルの性質上、ディレクトリ以下の指定はできませんのでご了承ください。

Q URL データベース(ブラックリスト)、規制 URL リスト(ユーザ設定)、許可 URL リストで URL フィルタの処理優先度は？

A 優先順位は1)許可 URL リスト、2)例外 URL の規制 URL リスト、3)URL データベースの順に行います。

Q 社内の中で別々のポリシーを設定することはできますか？

A お客様の環境・契約内容にもよりますので、bit-drive インフォメーションセンターまでお問い合わせください。

Q リアルタイムのアクセス状況を表示することはできますか？

A ございません。アクセス状況の確認はアクセスログファイルをご覧ください。なおログファイルは当日のログファイルは確認できませんので、1 日前以前のログファイルを確認いただくこととなります。

Q アクセスログの保存期間は？

A 1 日毎に 1 ファイルが作成され、31 日分保存されます。32 日目からは削除されますので、早めにダウンロードをお願いいたします。

Q ログのフォーマット形式は？

A CSV 形式で以下のフォーマットでテキストとして出力されます。

フォーマットは、以下のようになっております。

『日付,記録時間,プロトコル名,ソース IP,ID,(未使用),(未使用),転送状態,(未使用),(未使用),リクエスト先サーバホスト名,(未使用),(未使用),ファイルタイプ、カテゴリ名、リクエスト URL』

転送状態とは、Blocked(規制カテゴリで登録され、ポリシーで許可されていない URL。クライアント側でブロッキング画面が表示される)、Allowed(規制カテゴリで登録されているが、ポリシーで許可されている URL)、Release(規制カテゴリで登録され、ポリシーで許可されていない URL をオーバーライドにより参照した URL)、BlkPost(書き込み規制によって規制された URL)の5種類が記録されます。

また、ファイルタイプは、ファイルタイプが特定された場合のみ出力されます。

本サービスでは記録されない項目については(未使用)と記載してありますのでご注意ください。

なお、規制カテゴリに登録されていない URL へのアクセスの場合はアクセスログに記録されません。

Q 管理者を複数登録できますか？

A 「グループ/ユーザ選択」からアカウントを作成し、グループ管理者のチェックボックスにチェックを入れてください。また、管理者アカウントを削除する場合は、新規に管理者アカウントを登録後、新たに作成したグループ管理者のアカウントでログインし、不要となったアカウントを削除してください。

Q 本サービスで利用できない管理者メニューを教えてください。

A 使用することはできませんが、本サービスにおいては意味を成さないメニューがあります。

『一括登録/削除』『グループの登録』『下位グループ指定』『最低基準設定』『例外ユーザ用スケジュール登録』です。本サービスでは一般アカウントでのサービス提供は行っておりません。『一括登録/削除』ではグループ管理者以外の一般ユーザを登録しても使用できません。『例外ユーザ用スケジュール登録』も同様です。

Q 管理画面にログインできません。または管理画面にログインしましたが、「アカウント更新」の画面が表示されません。

A 管理画面のログインページが表示されない場合は管理画面の URL を確認してください。

管理画面のログインページよりログインできない場合、コンテンツフィルタ ID、管理者アカウント名、パスワードを確認してください。アカウント欄には、「コンテンツフィルタ ID≠管理者アカウント名」を入力してください。

パスワードがわからなくなった場合は、bit-drive インフォメーションセンターまでお問い合わせください。

「アカウント更新」の画面が表示される場合は、お客さまがユーザ登録した際にグループ管理者のチェックボックスをチェックしていない場合、一般ユーザとしてパスワード変更の画面が表示されますので、再度正しいグループ管理者でログインし、登録した内容を確認してください。

Q 登録している IP アドレスを変更できません。

A IP アドレスの管理は bit-drive にて行っております。本サービスの IP アドレスに関するお問い合わせは bit-drive インフォメーションセンターまでお願いいたします。

Q アクセスログファイルが1件も出力されていません。

A ブラウザのプロキシ設定またはお客様のプロキシの上位プロキシにフィルタサーバが設定されていないため、フィルタサーバを経由していない可能性がありますので設定を確認してください。
または、すべて規制対象ではないサイトにアクセスしている可能性があります。

Q カテゴリ別ルール設定にて、表示されるカテゴリが 26 しかありません。

A カテゴリは全 86(お客様が自由に使用可能なユーザ設定カテゴリ 10 を含みます)あります。これらは大きな分類として 26 分類に分かれています。大分類毎にポリシーを設定する場合は、そのまま規制ルールを指定します。カテゴリ名の前にある+マークをクリックすると、そのカテゴリに含まれる詳細なカテゴリが表示されますので、個々に規制ルールを登録することもできます。

Q カテゴリ別ルール設定にて、カテゴリ名のすぐ横に設定されているルールが表示されているものとされていないものがあります。違いは何ですか？

A カテゴリは大きな分類として 26 分類、詳細は分類として 86(お客様が自由に使用可能なユーザ設定カテゴリ 10 を含みます)あります。大きな分類に含まれるすべてのカテゴリが同じルールの場合、大きな分類カテゴリ横に設定されたルールが表示されます。詳細なカテゴリのルールが違う場合は表示されません。

Q コンテンツフィルタを経由して Web サイトにアクセスする際に使用する IP アドレスは何ですか？

A お客様サポートサイト内、bit-drive サーバー一覧をご覧ください。