

i-FILTER®

Ver.9

導入マニュアル

本マニュアルについて	2
改訂履歴	3
凡例	4
関連ドキュメント	4
第1章 動作環境	5
1-1 「i-FILTER」動作環境	6
第2章 インストール・アンインストール	8
2-1 インストール・アンインストール概要	9
2-2 Proxy Server for Windows	9
2-2-1 インストール	9
2-2-2 アンインストール	10
2-2-3 起動と停止	11
2-3 Proxy Server for Linux	12
2-3-1 インストール	12
2-3-2 アンインストール	12
2-3-3 起動と停止	13
2-4 ICAP Server for Linux	14
2-4-1 インストール	14
2-4-2 アンインストール	14
2-4-3 起動と停止	15
第3章 ICAP クライアントの設定	16
3-1 Blue Coatを設定する場合	17
3-2 Squid を設定する場合	23
3-3 HTTPSリクエストへの対応設定	24
3-4 管理画面を開く	25
第4章 初期設定	26
4-1 クライアントが使用するブラウザの設定	27
4-2 ユーザー登録	28
4-3 アドミニストレーターの設定	33
4-4 ネットワークの設定	34
4-4-1 ポート番号の変更	34
4-4-2 上位プロキシサーバーの設定	34
4-5 ログの設定	35
4-6 認証サーバーの設定	36
4-6-1 「i-FILTER for Linux」でのNTLM 認証について	36
4-6-2 「i-FILTER for Windows」でのNTLM認証について	36
4-7 AV Adapter設定	38
4-7-1 AV Adapter 機能を有効にする	38
4-7-2 ICAPサーバー設定(Kaspersky Anti-Virus for Proxy Server)	39
4-7-3 ICAPクライアント設定	40
第5章 運用設定	42
5-1 運用設定をする	43
第6章 ライセンス	44
6-1 ライセンス更新手続き	45
6-2 登録内容の変更	45
6-2-1 お客様情報の変更	45
6-2-2 システムの変更	45
第7章 トラブルシューティング	46
7-1 「i-FILTER」が起動しない場合	47
7-2 「i-FILTER」のユーザー登録に失敗する場合	48
7-3 認証機能が正常動作しない場合	49
7-4 設定画面へのログインパスワードを忘れた場合	49
7-5 パフォーマンス向上について	50
7-5-1 サーバー機のCPU 処理能力の不足	50
7-5-2 「i-FILTER」のプロキシスレッド数の不足	51
7-5-3 OS のファイルディスクリプタの不足	53
7-5-4 メモリ不足	55
7-5-5 外的要因に依存する「i-FILTER」処理の遅延	55
7-6 新規インストール後にエラーログが出力される	56

本マニュアルについて

- 本マニュアルは「i-FILTER」Ver.9の内容について記載しています。
- 本マニュアルの内容は、2022年9月30日時点の情報に基づいて作成しております。
- 本マニュアルの内容は、将来予告なしに変更される場合があります。
- 本マニュアルの全部または一部を無断転載、無断複写することは禁止されております。
- 本マニュアルは細心の注意を払って作成しておりますが、記述に誤りや欠落があっても、デジタルアーツ株式会社はいかなる責任も負わないものとします。
- 本マニュアルにご不明点や誤り、記載漏れなどお気づきの点がありましたら当該製品のサポート窓口までご連絡ください。
- 本製品の最新情報をホームページで公開しています。「デジタルアーツ株式会社 サポート情報サイト」
<<https://download.daj.co.jp/user/>>」
- Safariは、米国および他の国々で登録されたApple Inc.の商標です。iOSはApple Inc.のオペレーティング・システムの名称です。IOSはCisco Systems, Inc.の商標または登録商標です。FireEyeは、FireEye, Inc.の登録商標です。Android、Google、ChromeはGoogle Inc.の商標です。Red Hat Enterprise Linuxは、米国およびその他の国におけるRed Hat, Inc.の登録商標です。Linux®は、Linus Torvalds氏の日本およびその他の国における登録商標または商標です。Windows、Microsoft、Internet Explorer、Microsoft Edgeは、米国Microsoft Corporationの、米国およびその他の国における登録商標または商標です。MozillaおよびFirefoxは、Mozilla Foundationの登録商標です。Blue Coatは、シマンテック・コーポレーションの、米国およびその他の国における登録商標または商標です。Deep Discovery Inspectorは、トレンドマイクロ株式会社の登録商標です。
- デジタルアーツ、DIGITAL ARTS、i-FILTER、i-FILTER Anti-Virus & Sandbox、i-FILTER@Cloud Anti-Virus & Sandbox、info board、Active Rating System、D-SPA、Anti-Virus & Sandbox for D-SPA、NET FILTER、SP-Cache、White Web、ZBRAIN、クレデンシャルプロテクション、ホワイト運用、m-FILTER、m-FILTER MailFilter、m-FILTER Archive、m-FILTER Anti-Spam、m-FILTER Anti-Virus & Sandbox、m-FILTER@Cloud Anti-Virus & Sandbox、m-FILTER File Scan、Mail Detox、m-FILTER EdgeMTA、EdgeMTA、FinalCode、i-フィルター、DigitalArts@Cloud、Desk@Cloud、Desk、DアラートおよびDコンテンツその他の弊社・弊社製品関連の各種名称・ロゴ・アイコン・デザイン等はデジタルアーツ株式会社の登録商標または商標です。
- その他、本マニュアルに記載されている各社の社名、製品名およびサービス名は、各社の商標または登録商標です。

「i-FILTER」Ver.9 導入マニュアル

2022年9月30日 第10版

デジタルアーツ株式会社

〒100-0004 東京都千代田区大手町1-5-1 大手町ファーストスクエア ウエストタワー14F

<https://www.daj.jp/>

Copyright © 2016 Digital Arts Inc.

改訂履歴

本マニュアルの主な改訂内容を記載します。

版数	改訂日	内容	製品バージョン
第10版	2022年9月30日	更新 1-1 「i-FILTER」動作環境 4-1 クライアントが使用するブラウザの設定	Ver.9.50R12
第9版	2021年5月13日	更新 1-1 「i-FILTER」動作環境 4-7-3 ICAPクライアント設定	Ver.9.50R10
第8版	2020年5月28日	更新 1-1 「i-FILTER」動作環境	Ver.9.50R09
第7版	2019年8月29日	更新 1-1 「i-FILTER」動作環境 その他 - マニュアル名称を『「i-FILTER」Ver.9 導入マニュアル』に変更	Ver.9.50R08
第6版	2018年12月6日	更新 1-1 「i-FILTER」動作環境	Ver.9.50R06
第5版	2017年9月13日	更新 1-1 「i-FILTER」動作環境 その他 - マニュアル名称を『「i-FILTER」Ver.9/Ver.8.7 導入マニュアル』に変更	Ver.9.50R03
第4版	2017年4月21日	更新 1-1 「i-FILTER」動作環境 4-7 AV Adapter設定	Ver.9.50R03
第3版	2017年1月10日	更新 1-1 「i-FILTER」動作環境 その他 - AV Adapter、SSL Adapter、Info Boardの設定について別マニュアルの案内を掲載	Ver.9.50R01
第2版	2016年8月16日	更新 1-1 「i-FILTER」動作環境 第2章 インストール・アンインストール(全体) 6-1 SSL Adapter機能を有効にする	Ver.9.40R01
第1版	2016年7月13日	「i-FILTER」導入マニュアル新規作成 ※「i-FILTER」Ver.9導入マニュアル第9版からの移行	Ver.9.40R01

注意

- 誤字誤植、名称変更、パラメーター値変更ほか、細かい内容については本ページへの記載を省略している場合があります。
- 製品更新の詳細はサポート情報より更新履歴（リリースノート）を参照してください。

<https://download.daj.co.jp/user/ifilter/V9/>

※ 製品の「シリアルNo.」とお客様「E-Mailアドレス」によるログインが必要です。ログイン情報の確認方法は「4-2 ユーザー登録」を参照してください。

凡例

■ 固有機能

 Proxy	「i-FILTER Proxy Server」固有の説明に関して記載しています。
 ICAP	「i-FILTER ICAP Server」固有の説明に関して記載しています。

■ アイコン凡例

イメージ	ラベル	説明
	補足	補足説明や関連する記述のあるドキュメント名もしくはドキュメントの参照先を示します。
	注意	特に注意が必要な事項について説明します。
	制限	制限事項について説明します。
	例	設定例です。

関連ドキュメント

ドキュメント名	説明
「i-FILTER」 Ver.9 導入マニュアル(本書)	「i-FILTER」のインストールから初期設定、チューニング方法などを掲載したマニュアルです。本書では『導入マニュアル』と表記します。
「i-FILTER」 Ver.9 機能マニュアル	「i-FILTER」の機能全般の説明や各種設定方法、トラブルシューティングを掲載したマニュアルです。本書では『機能マニュアル』と表記します。
「i-FILTER」 Ver.9 運用マニュアル	運用事例をベースに「i-FILTER」でよく利用される機能の設定手順を掲載したマニュアルです。本書では『運用マニュアル』と表記します。
「i-FILTER Reporter」 Ver.7 マニュアル	「i-FILTER」 Ver.9のアクセスログ集計、レポート、ログ検索を提供する「i-FILTER Reporter」のマニュアルです。

+ 補足

- 上記以外のドキュメントについては「[サポート情報サイト※](#)」を確認してください。
 ※ 製品の「シリアルNo.」とお客様「E-Mailアドレス」によるログインが必要です。ログイン情報の確認方法は「[4-2 ユーザー登録](#)」を参照してください。

第1章 動作環境

この章では、動作環境について説明します。

1-1 「i-FILTER」動作環境

1-1 「i-FILTER」動作環境

OS	Windows	Windows Server 2022 Standard Windows Server 2019 Standard Windows Server 2016 Standard Windows Server 2012 R2 Standard Windows Server 2012 Standard
	Linux	Red Hat Enterprise Linux 8.0～8.6 ※ ¹ Red Hat Enterprise Linux 7.0～7.9 ※ ¹
仮想環境		上記対応 OS の動作を保証している仮想環境 ※ ²
CPU		Xeonデュアルコアプロセッサ2GHz以上
メモリ		4GBBytes 以上 ※ ³
ハードディスク容量		10GBBytes 以上 ※ ⁴
対応ブラウザ	管理用	Microsoft Edge PC版
	クライアント用	Microsoft Edge PC版 Mozilla Firefox ※ ⁵ Google Chrome ※ ⁶ Safari

- ※¹ 32bitのRed Hat Enterprise Linuxでは動作しません。
- ※² マイグレーション機能などの仮想化ソフトウェア独自の機能の利用時には注意が必要となる場合がございます。
- ※³ メモリーサイズは小規模ユーザー、デフォルト設定で必要なサイズです。
ユーザー数や設定内容等、運用に必要なサイズは別途見積もる必要があります。
- ※⁴ HDD容量はアクセスログ等、運用に必要な容量は別途見積もる必要があります。
- ※⁵ PC版のみへの対応となります。
- ※⁶ FTP over HTTPプロトコルには対応していません。（2016年1月28日現在）

+ 補足

- 最新の動作環境は下記URLにてご確認ください。

<https://www.daj.jp/bs/i-filter9/sysreq/requirements/>

⚠ 注意

- 「i-FILTER for Linux」を使用する場合、以下の内容を確認してください。
 - 以下のライブラリファイルがインストールされている必要があります。

・ libstdc++.so.6
 ・ gcc-4.X.X

 ※ XX-Xはご利用のOSのバージョンに含まれるファイルの値に読み替えてください
 - 利用するスレッド数などに応じてLinuxカーネルパラメーター上限を変更する必要があります。詳細は「7-5-3 OS のファイルディスクリプタの不足」「■ Linux」項目を参照してください。
 - 「i-FILTER」をフィルタリングサーバーとして利用する場合には、出口対策を有効に行うため、DNSサーバーによる名前解決が可能な環境に配置することを強く推奨します。

■ キャッシュサーバー対応状況表(ICAPサーバー機能)

Blue Coat ProxySG				
4.2.5.1 ※1	5.2.6.1	5.5.10.1	6.2.10.3 ※2	6.4.6.1 ※2

- ※1
- 「Blue Coat ProxySG」の不具合により、仮想ホスト経由では「POSTログの詳細内容」が表示できません。
- ※2
- SSLプロキシ機能を利用している場合、HTTPSリクエストにおいて「i-FILTER」のLDAP認証/独自認証が正常に動作しません。

Squid	
3.4.6 ※1、※2、※3、※4	3.5.20 ※1、※2、※3、※4

- ※1
- 「Squid」の不具合により、Options-TTLは30以上に設定する必要があります。
- ※2
- ssl_bumpを利用している場合、HTTPSリクエストにおいて「i-FILTER」のLDAP認証/独自認証が正常に動作しません。
- ※3
- 動的SSL証明書生成機能（ssl-bump generate-host-certificates=on）有りでの動作確認もしています。
- ※4
- Squid 3.4以降でICAPサーバーでの認証を許容しない制限が確認されました。そのため「i-FILTER」でのLDAP認証/独自認証は正常に動作しません。Squid側で認証し、「i-FILTER」側でICAP認証を設定する構成では動作します。

○ 動作要素の説明

ブロック画面对応方式	キャッシュサーバーが「i-FILTER」より受け取るブロック画面の対応方式です。 ICAPによる転送方式の方が高速ですが、ブロック画面は全体のアクセス数の内の数%であることから、速度が問題になるケースは少ないと考えられます。
再起動直後の管理画面表示	管理画面から、「i-FILTER」を再起動した場合に、管理画面の再表示が正常に行えるかを示しています。
ブロック画面・画像サイズの制限	「Blue Coat ProxySG」にてブロック画面の転送サイズの制限を受けるかどうかを表しています。（○＝制限無し）
ICAP Keep-Alive	ICAPプロトコル上で、セッションを継続して使用するかを選択できます。 現時点で、「Blue Coat ProxySG」と「NetCache」でこの仕様に対しての対応状況が異なります。
HTTPSのブロックアクション	HTTPSのリクエストに対して、キャッシュサーバー側で設定を行い、「i-FILTER」でブロック出来るかを示します。×の場合は、キャッシュサーバー側でHTTPSをICAPで使わない設定を行う必要があります。
仮想サーバー名の使用	「i-FILTER」の仮想サーバー名をデフォルトのまま使用できるかを示します。 仮想サーバー名をキャッシュサーバーで解決する必要があるのかは、この考慮には含まれていません。

第2章 インストール・アンインストール

この章では、インストール・アンインストールについて説明します。

2-1 インストール・アンインストール概要

2-2 Proxy Server for Windows

- 2-2-1 インストール
- 2-2-2 アンインストール
- 2-2-3 起動と停止

2-3 Proxy Server for Linux

- 2-3-1 インストール
- 2-3-2 アンインストール
- 2-3-3 起動と停止

2-4 ICAP Server for Linux

- 2-4-1 インストール
 - 2-4-2 アンインストール
 - 2-4-3 起動と停止
-

2-1 インストール・アンインストール概要

製品種別およびOSによりインストール・アンインストール方法が異なります。ご使用の動作環境をご確認の上、記載された方法にしたがってインストール・アンインストールを行ってください。

⚠ 注意

- 1台のサーバーに「i-FILTER」を複数インストールすることはできません。

+ 補足

- 新規インストール後はproxy.log0000にフィルターデータベース初期化エラーが出力されます。詳細は「7-6 新規インストール後にエラーログが出力される」を参照してください。

2-2 Proxy Server for Windows

📘 Proxy

Administrator(管理者)権限を持つユーザーでログインし、以下の操作を行ってください。
起動中のほかのプログラムはすべて終了してから実行してください。

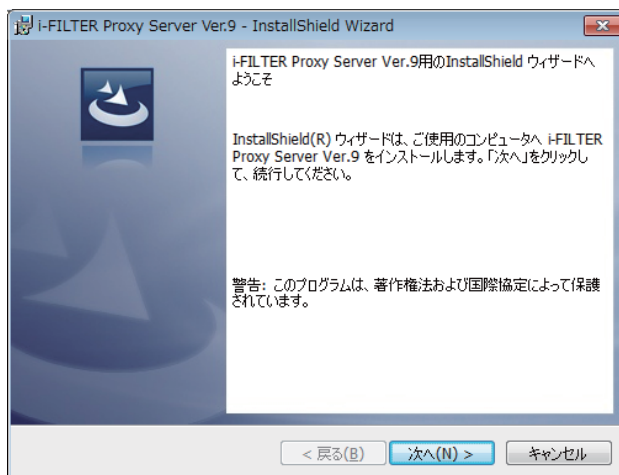
2-2-1 インストール

○ STEP1 パッケージファイルを実行

パッケージファイル「i-FILTER-Proxy-x.xx_jp-xx-xxxxxxx.exe」を実行します。

○ STEP2 インストールウィザードを実行

InstallShieldの指示に従ってインストールを行います。



【図:インストーラー起動時画面】

⚠ 注意

- インストール先を変更してインストールを行った場合、アップデートインストール時に「セットアップタイプ」ダイアログが表示されることがあります。その場合はカスタムを選択し、インストール先を再度変更してください。

+ 補足

- 「i-FILTER」のインストールが完了すると、自動的にサービスを開始します。

2-2-2 アンインストール

⚠ 注意

- 「i-FILTER」のサービスを停止してからアンインストール作業を行ってください。

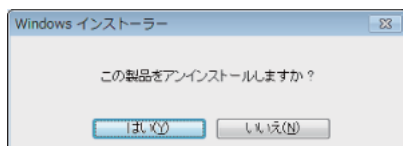
○ STEP1

スタートメニューより、「アンインストール」メニューを選択します。

[スタート]→[すべてのプログラム]→[i-FILTER Proxy Server Ver.9]→[i-FILTER Ver.9 アンインストール]

○ STEP2

以下のダイアログが表示されます。[はい]を選択してください。



【図:アンインストール開始画面】

⚠ 注意

- アンインストール後にOSの再起動の案内が表示された場合は、必ずOSの再起動を行ってください。

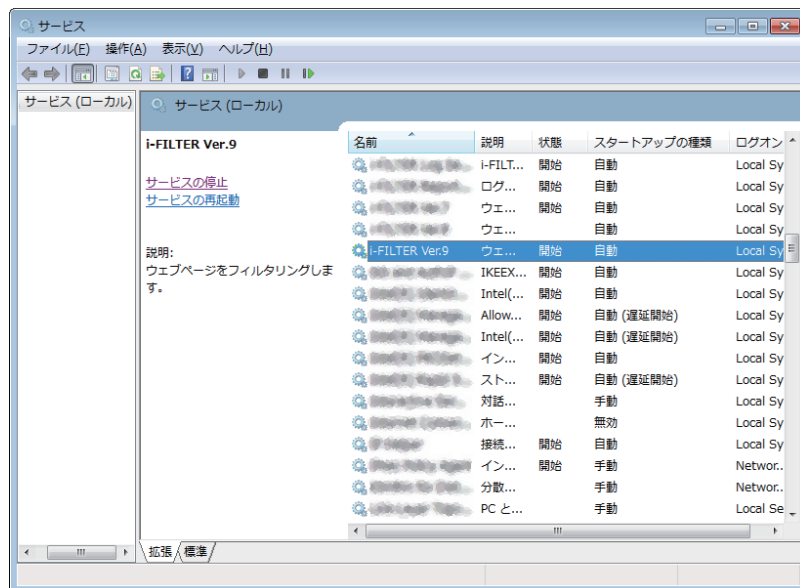
+ 補足

- インストール後に作成されたファイルは削除されません。

2-2-3 起動と停止

「i-FILTER」の起動と停止はWindowsの管理ツール(サービス)を使用して行います。Windowsのスタートメニューより、「サービス」メニューを選択します。

- [スタート]→[コントロールパネル]→[管理ツール]→[サービス]



【図:サービス一覧画面】

サービス名「i-FILTER Ver.9」を選択し、以下の操作を行ってください。

サービス起動	[操作(A)]→[開始(S)]をクリック
サービス確認	[操作(A)]→[プロパティ(R)]をクリック
サービス停止	[操作(A)]→[停止(O)]をクリック
サービス再起動	[操作(A)]→[再起動(E)]をクリック

+ 補足

- [再起動(E)]はサービスがすでに起動されているときのみに有効です。

2-3 Proxy Server for Linux

Proxy

root 権限を持つユーザーでログインし、以下の操作を行ってください。

2-3-1 インストール

○ STEP1

パッケージファイルを実行します。

ダウンロードしたパッケージファイル「i-FILTER-Proxy-x.xx_jp-xxx_xxxxxxxx.x86_64.rpm」をコマンドラインから実行します。パッケージのあるディレクトリに移動し、以下のコマンドを実行してください。

```
# rpm -Uvh i-FILTER-Proxy-x.xx_jp-xxx_xxxxxxxx.x86_64.rpm
```

○ STEP2

/usr/local以下にifilter9ディレクトリが作成され、各ファイルがインストールされます。また、/etc/init.d以下に起動と終了を行うためのスクリプトがインストールされます。

補足

- インストールが完了してもプロセスは自動的に起動しません。

2-3-2 アンインストール

注意

- 「i-FILTER」のプロセスを停止してからアンインストール作業を行ってください。

○ STEP1

コマンドラインから、以下のコマンドを実行します。

```
# rpm -e i-FILTER-Proxy9
```

補足

- インストール後に作成されたファイルは削除されません。

2-3-3 起動と停止

「i-FILTER」サービスの操作はコマンドラインから以下のコマンドを実行します。

起動	# /etc/init.d/ifilter9 start
確認	# /etc/init.d/ifilter9 status
停止	# /etc/init.d/ifilter9 stop
再起動	# /etc/init.d/ifilter9 restart

2-4 ICAP Server for Linux

iCAP

2-4-1 インストール

○ STEP1

パッケージファイルを実行します。

パッケージファイル「i-FILTER-Proxy-9.xx_jp-xxx_xxxxxxxx.x86_64.rpm」をコマンドラインから実行します。また、パッケージのあるディレクトリに移動し、以下のコマンドを実行します。

```
# rpm -Uvh i-FILTER-Proxy-9.xx_jp-xxx_xxxxxxxx.x86_64.rpm
```

○ STEP2

インストールにより/usr/local以下にifilter9ディレクトリが作成され、各ファイルが作成されます。また、/etc/init.d以下に起動と終了を行うためのスクリプトがインストールされます。

補足

- インストールが完了してもプロセスは自動的に起動しません。

○ STEP3

インストール後、/usr/local/ifilter9/toolsディレクトリに移動し、「configure_icap_mode」コマンドを実行後、「i-FILTER」を起動します。

```
# cd /usr/local/ifilter9/tools
# ./configure_icap_mode
# /etc/init.d/ifilter9 start
```

補足

- サービス操作の詳細は「2-4-3 起動と停止」を参照してください。

2-4-2 アンインストール

注意

- 「i-FILTER」のプロセスを停止してからアンインストール作業を行ってください。

○ STEP1

コマンドラインから、以下のコマンドを実行します。

```
# rpm -e i-FILTER-Proxy9
```

補足

- インストール後に作成されたファイルは削除されません。

2-4-3 起動と停止

「i-FILTER」サービスの操作はコマンドラインから以下のコマンドを実行します。

サービス起動	<code># /etc/init.d/ifilter9 start</code>
サービス確認	<code># /etc/init.d/ifilter9 status</code>
サービス停止	<code># /etc/init.d/ifilter9 stop</code>
サービス再起動	<code># /etc/init.d/ifilter9 restart</code>

第3章 ICAP クライアントの設定

ICAP

この章では、「ICAP」を利用する際のICAP クライアントの設定について解説します。

3-1 Blue Coatを設定する場合

3-2 Squid を設定する場合

3-3 HTTPSリクエストへの対応設定

3-4 管理画面を開く

3-1 Blue Coatを設定する場合

注意

- 本項ではBlue Coat 5.xの設定例を記載しています。その他の基本的な設定や環境固有の設定については別途Blue CoatのマニュアルあるいはBlue Coatを購入された代理店にお問い合わせください。

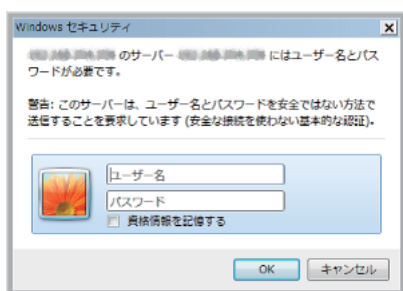
○ STEP1 設定画面へのログイン

Blue Coat環境の設定を行うにはBlue Coat設定画面にログインする必要があります。Blue Coat設定画面へログインするには、以下URLをWebブラウザに入力します。

`http://Blue Coat-IP※1:Blue Coat -Port※2/`

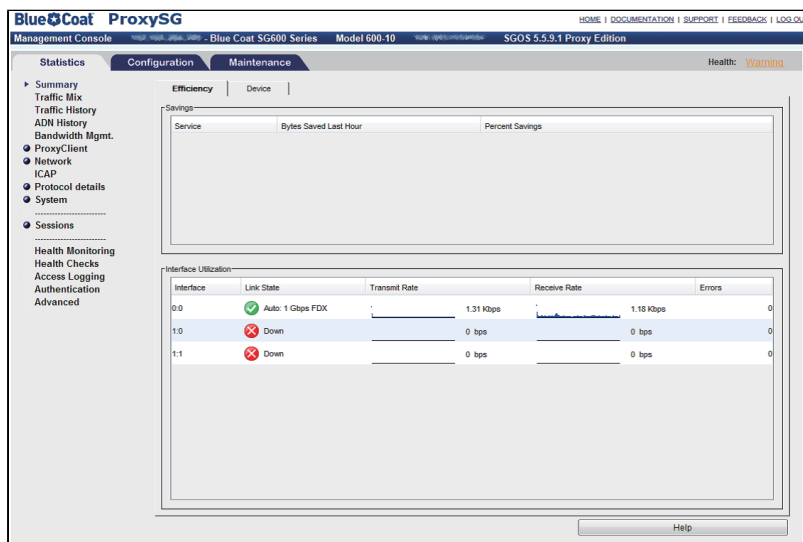
※1 Blue Coat-IP:Blue Coat サーバーのIP アドレス

※2 Blue Coat-Port:Blue Coat サーバーのポート番号(デフォルト8081)



【図 : Blue Coat設定画面ログインダイアログ】

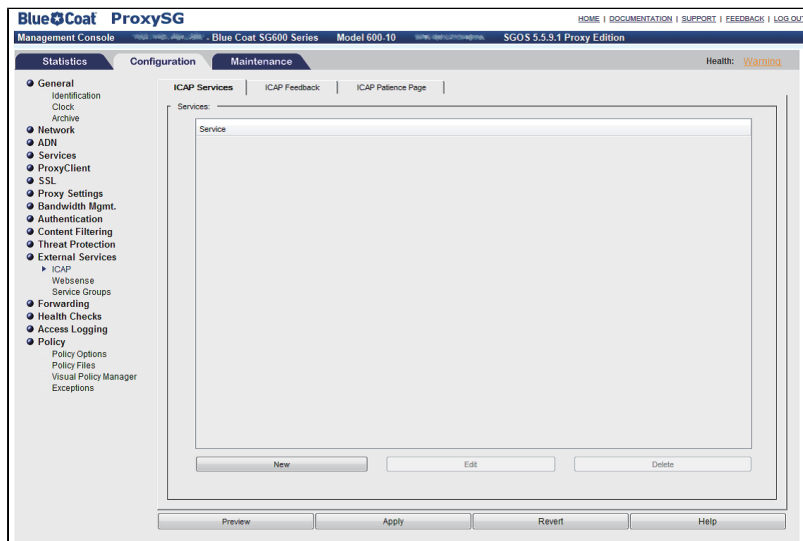
【図 : Blue Coat設定画面ログインダイアログ】が表示されるので、Blue Coatの管理者アカウント、パスワードを入力します。ログインに成功すると、【図 : Blue Coat設定画面】が表示されます。



【図 : Blue Coat設定画面】

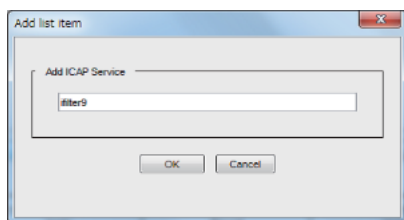
○ STEP2 ICAPサービスの登録

「i-FILTER ICAP Server」との連携のために、Blue CoatへICAPサービスの登録を行います。ICAPサービス登録のためには、ICAP設定画面を開き、以下の手順で設定を行います。【図：Blue Coat設定画面】から「Configuration(タブ)」>「External Service」>「ICAP」と遷移し、以下【図：ICAP設定画面】のページを開きます。



【図：ICAP設定画面】

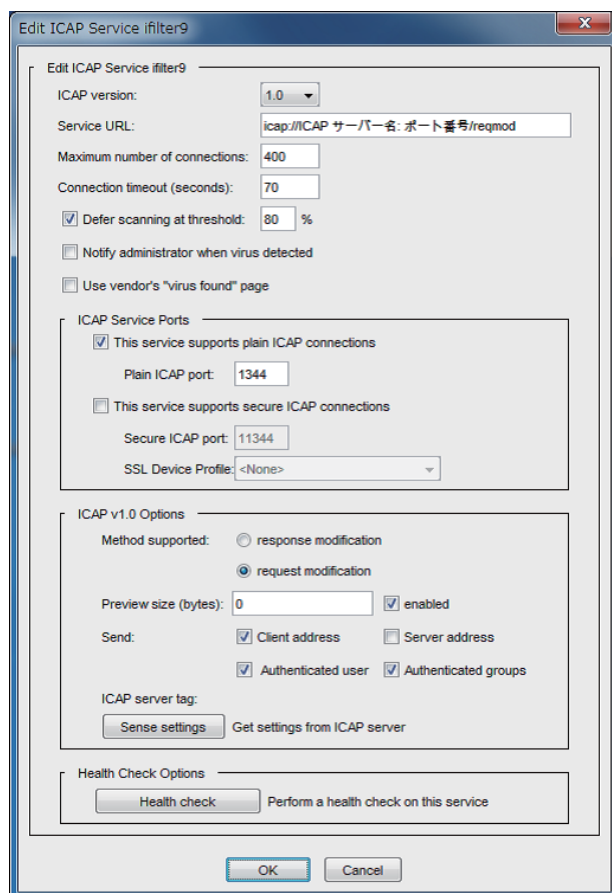
この画面より、「New」ボタンをクリックして、「Add listitem」ダイアログを開きます。このダイアログに、登録するICAPサービスの名前を入力します。ここでは、登録するICAPサービス名を「ifilter9」と入力しています。入力が終了したら、[OK]ボタンをクリックしてダイアログを閉じます。



【図：Add listitemダイアログ】

次に、登録したいICAPサービスに対して設定を行います。設定を行うには【図：ICAP設定画面】より、設定を行いたいICAPサービスを選択して[Edit]ボタンをクリックします。[Edit ICAP Service]ダイアログが表示されますので、以下のように設定を行います。

ICAP version	1.0
Service URL	icap://ICAP サーバー名: ポート番号/reqmod
Maximum number of connections	400 ※ Sense setting ボタンクリックにより「i-FILTER ICAP Server」から設定を取得します
Connection timeout (seconds)	70(初期値)
Notify administrator when virus detected	OFF
Method supported	request modification
Send -> Client address	ON
Send -> Server address	OFF
ICAP server tag	ICAP サービス名が表示 ※Sense settings ボタンで取得



【図：Edit ICAP Serviceダイアログ】

設定が終了後、[Sense settings]ボタンをクリックします。最後に[OK]ボタンをクリックしてダイアログを閉じます。

【図：ICAP設定画面】より、[Apply]ボタンをクリックして設定を反映させます。

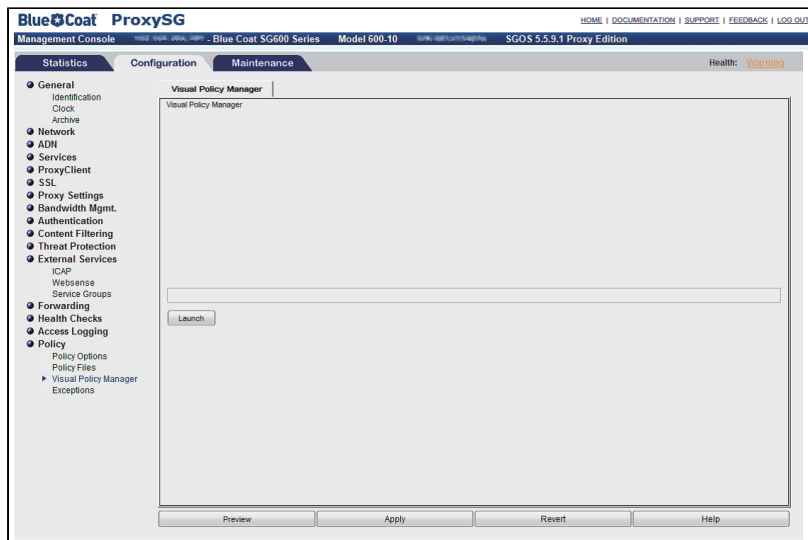
⚠ 注意

- [Sense settings]ボタンを押す際、「i-FILTER ICAP Server」が起動している必要があります。

○ STEP3 ポリシーを有効にする

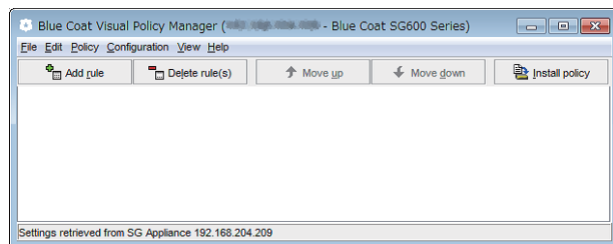
ICAPサービスに対してポリシーを設定するには以下の手順で行います。

【図：Blue Coat設定画面】から、「Configuration(タブ)」>「Policy」>「Visual Policy Manager」と遷移します。



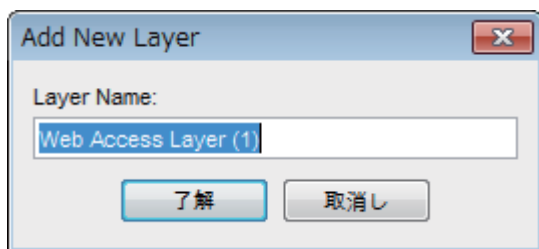
【図：ICAP設定画面】

次に[Launch]ボタンをクリックして、「Visual Policy Manager」ウィンドウを開きます。



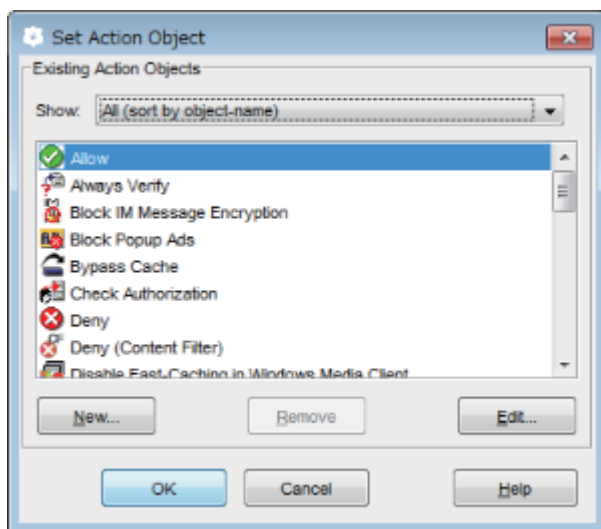
【図：Visual Policy Manager】

「Policy」メニューから、「Add Web Access Layer」を選択すると以下のようなダイアログが表示されますので、任意の名前を付けて[了解]ボタンをクリックします。



【図 : AddNewLayerダイアログ】

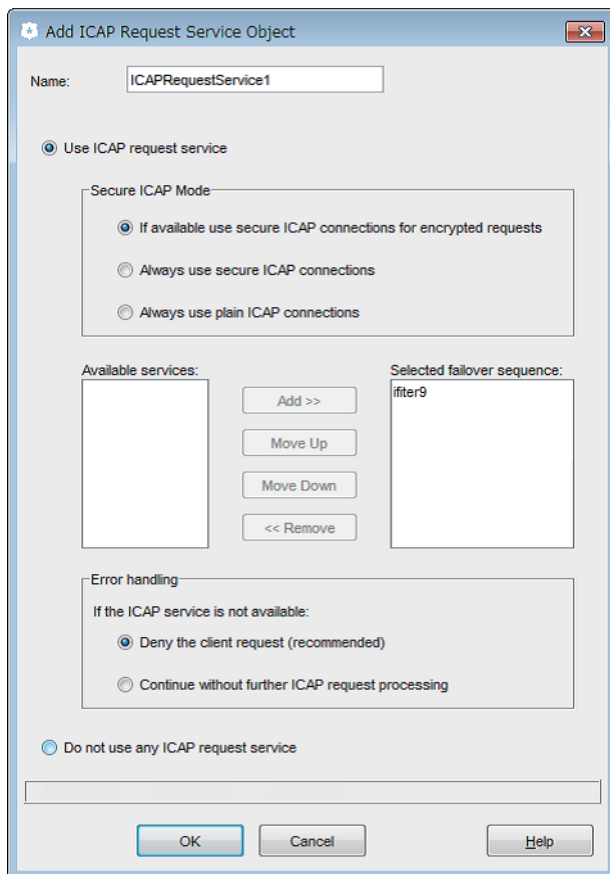
【図 : Visual Policy Managerウィンドウ】の「Action」欄から、「右クリック」>「Set」を選択すると、【図 : Set Action Objectダイアログ】のダイアログが表示されます。このダイアログの[New...]ボタンをクリックして、「Set ICAP request Service...」を選択します。



【図 : Set Action Objectダイアログ】

「Add ICAP Request Service Object」ダイアログを表示し、以下のように設定を行います。

Name	任意の名前
Use Icap request service	登録済みICAP サービスの名前を選択
On Communication error with ICAP service	[Deny the request] を選択



【図 : Add ICAP Request Service Objectダイアログ】

設定が完了したら、[OK]ボタンをクリックしてください。最後に【図 : Set Action Objectダイアログ】の「Visual Policy Manager」ウィンドウの[Install Policy]ボタンをクリックして設定を反映させます。

+ 補足

- 「i-FILTER」がデコードしたHTTPSリクエスト受信時のログ出力を有効にする場合は、「[3-3 HTTPSリクエストへの対応設定](#)」を参照してください。

3-2 Squid を設定する場合

⚠ 注意

- 本項では「squid-3.2.STABLE-X」の設定例を掲載しています。その他の基本的な設定や環境固有の設定については<http://www.squid-cache.org/>などの情報を参照してください。
- 動作確認済みのSquidバージョンは『1-1 「i-FILTER」動作環境』をご確認ください。

○ STEP1 Configureの実行

tar.gzファイル展開後、以下オプションを付けて、"./configure"を実行します。

```
# ./configure --enable-icap-client --enable-ssl
```

"./configure"実行後、"make"、"make install"を実行し、インストールを完了します。

○ STEP2 squid.confの修正

ICAPクライアントとして動作させるため、squid.conf中の以下のパラメーターを編集します。

```
icap_enable on
icap_send_client_ip on
icap_send_client_username on
icap_service ifservice_1 reqmod_precache bypass=off icap://i-FILTER ICAP Server のIP: ポート番号/reqmod
adaptation_service_set ifclass_1 ifservice_1
adaptation_access ifclass_1 allow all
```

ポート番号など、基本設定を終了した後、squidを起動します。

○ STEP3 ssl-bumpを利用する場合

squid.conf中の以下のパラメーターを編集します。

```
ssl_bump allow all
always_direct allow all
sslproxy_cert_error allow all
sslproxy_flags DONT_VERIFY_PEER
http_port 3128 ssl-bump cert=[ 証明書ファイルパス ] key=[ 秘密鍵ファイルパス ]
```

○ STEP4 「i-FILTER」側で認証を行う場合の設定

「i-FILTER」側でLDAP認証、独自認証を行う場合には認証が通りません。下記設定を行うことにより「i-FILTER」側で認証が可能となります。

1. 下記ファイルをテキストエディタで開きます。

```
<「i-FILTER」インストールディレクトリ>/conf/ifilter.conf
```

2. 下記パラメーターを以下のように変更します。

```
icap_squid3_correspondence = on
```

3. ファイルを保存し、「i-FILTER」を再起動してください。

+ 補足

- 「i-FILTER」がデコードしたHTTPSリクエスト受信時のログ出力を有効にする場合は、『3-3 HTTPSリクエストへの対応設定』を参照してください。

3-3 HTTPSリクエストへの対応設定

「i-FILTER」で下記の設定を行うことにより、ICAPクライアントでデコードしたHTTPSリクエストに対し、正常にフィルタリングを行い適切にログを出力します。

○ STEP1

下記ファイルをテキストエディタで開きます。

```
「i-FILTER」インストールディレクトリ/conf/ifilter.conf
```

○ STEP2

下記パラメーターを変更します。

```
icap_ssl_support = on
```

○ STEP3

ファイルを保存し、「i-FILTER」を再起動してください。

注意

- ICAP版でHTTPSリクエストのフィルタリングを正常に動作させるためには、ICAPクライアントでHTTPSリクエストがデコードされている必要があります。

3-4 管理画面を開く

「i-FILTER」管理画面ではユーザー登録処理や、「i-FILTER ICAP Server」に関する設定を行います。

The screenshot shows the i-FILTER management interface. At the top, there's a navigation bar with tabs: グループ設定, 共通設定, ルールセット, ログ, システム設定, オプション. Below this, a header bar shows 'i-FILTER' and 'ログインユーザー: admin' with a 'ログアウト' button. The main content area is divided into several sections:

- 運用情報:** サーバアクセス時刻: 2014年 9月 17日 (水) 12時 29分 46秒. Includes links for '重要なお知らせ', 'サポートページ', and 'よくある質問'.
- ログイン情報:** ユーザー名: admin.
- i-FILTER情報:**
 - バージョン情報:** Ver. 9.11R01-20140912.
 - ファイルデータベース:** バージョン: 20140917_01, 最終更新時刻: 2014/09/17 12:29:01, 最終確認時刻: 2014/09/17 12:29:01. Includes links for 'Webサービス更新情報' and 'webサービスID参照'.
 - プロセス情報:** iプロセス / 400 スレッド.
 - 使用中スレッド数:** 0.
- アクセス情報:** A table listing various access categories and their counts.

アクセス情報	集計
脅威情報サイト	0
ボット・アダルトサイト	0
ヌード・アダルトグッズ	0
グラフィック・写真集	0
性教育・性の話題	0
暴力・暴力描写	0
犯罪・犯罪関係	0
麻薬・薬品薬物	0
カルト・テロリズム	0
自殺	0
乗出	0
ハッキング・クラッキング	0
不正プログラム配布・リンク集	0
違法ソフト・反社会行為	0
フィッシング詐欺	0
クラッシャーサイト	0
迷惑メールリンク	0
コンピューターサバイ	0
オフィスサバイ	0
オークション	0
オンラインショッピング	0
ポイントサービス	0
クーポン総合サイト	0
出会い	0
Webメール	0

【図：トップ画面】

「i-FILTER」管理画面へアクセスするには、Webブラウザのアドレス欄に「i-FILTER ICAP Server」がインストールされているサーバーの「IPアドレス」と「設定画面用待ち受けポート番号(初期値：15081)」を指定します。

http://<「i-FILTER」IPアドレス>:15081/



注意

- 「i-FILTER ICAP Server」の各種設定は管理画面から行います。指示がある場合を除き、設定ファイルの直接編集を行った場合は、「i-FILTER」が正常動作しなくなる場合があります。

第4章 初期設定

この章では、「i-FILTER」をインストールした後に、まず設定しておきたい項目について解説します。

4-1 クライアントが使用するブラウザーの設定

4-2 ユーザー登録

4-3 アドミニストレーターの設定

4-4 ネットワークの設定

- 4-4-1 ポート番号の変更
- 4-4-2 上位プロキシサーバーの設定

4-5 ログの設定

4-6 認証サーバーの設定

- 4-6-1 「i-FILTER for Linux」でのNTLM 認証について
- 4-6-2 「i-FILTER for Windows」でのNTLM認証について

4-7 AV Adapter設定

- 4-7-1 AV Adapter 機能を有効にする
 - 4-7-2 ICAPサーバー設定(Kaspersky Anti-Virus for Proxy Server)
 - 4-7-3 ICAPクライアント設定
-

4-1 クライアントが使用するブラウザの設定

「i-FILTER」ではクライアントがProxyを経由して通信を行うよう、ブラウザのプロキシサーバー設定を変更します。

■ Microsoft Edgeの場合

○ STEP1



(スタート) をクリックします。

○ STEP2

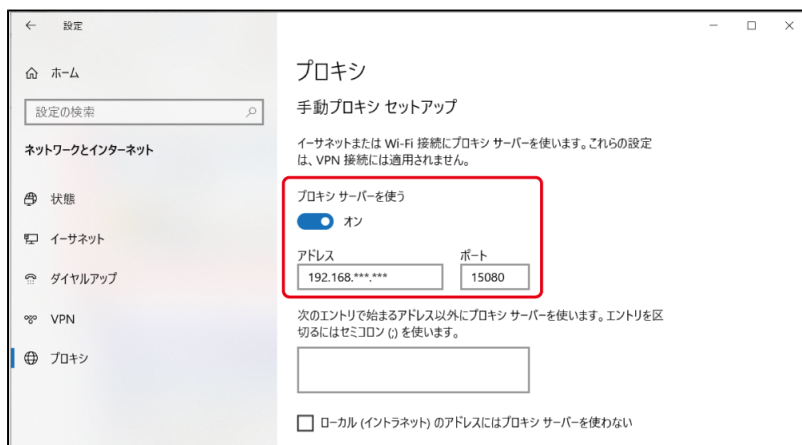
「ネットワークとインターネット」をクリックします。



【図:Windowsの設定画面】

○ STEP3

「プロキシ」をクリックし、「プロキシサーバーを使う」をオンに設定して「i-FILTER」のIPアドレスとポート番号を入力します。



【図:プロキシ設定】

+ 補足

- 「i-FILTER」のポート番号を変更している場合には必ず変更後のポート番号を入力してください。

⚠ 注意

- 「i-FILTER」の管理画面にはJavaScriptやcssが使用されているため、Webブラウザのキャッシュクリアを行わないと古い版のJavaScriptが残ることがあります。この状態で設定作業を実施すると、管理画面が崩れるなどの異常動作をする可能性があります。バージョンアップした際には必ずWebブラウザのキャッシュクリアを実施してください。
- 管理画面へのアクセスを目的とする場合は、「i-FILTER」が対応しているブラウザ以外は使用しないでください。

4-2 ユーザー登録

「i-FILTER」をご利用いただくには、ユーザー登録が必要です。ユーザー登録はセキュアプロトコルを使用してインターネット経由で行います。

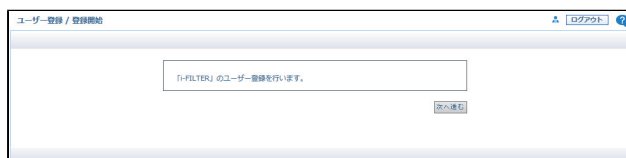
○ STEP1 「i-FILTER」管理画面にアクセス

Webブラウザのアドレス欄に、以下のいずれかを入力して「i-FILTER」の管理画面にアクセスします。

1	http://<IPアドレス>:15081/
2	http://inetnf.conf/ ※ Webブラウザのプロキシサーバー設定で「i-FILTER」を指定している場合

+ 補足

- 管理画面の待ち受けポート番号のデフォルト値は、「15081」となります。



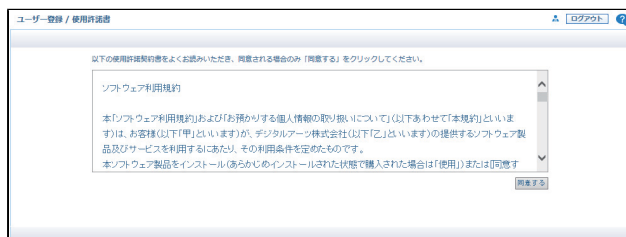
【図:ユーザー登録/登録開始画面】

! 注意

- 管理画面にアクセスした際、「ユーザー登録/登録開始」画面が表示されず、Webブラウザが真っ白な状態で表示されてしまう場合、Webブラウザの設定に問題がある場合があります。IEの場合では、「インターネットオプション」>「セキュリティ」>「レベルのカスタマイズ」>「スクリプト」>「アクティブスクリプト」を「有効にする」に設定することで表示されることがあります。

○ STEP2 使用許諾書画面を表示

使用許諾書の内容を確認の上、同意される場合は「同意する」をクリックします。



【図:ユーザー登録/使用許諾書画面】

○ STEP3 登録情報入力画面を表示

ユーザー登録 / 登録情報入力

以下のフォームにユーザー登録情報を入力してください。【※】は入力必須項目です。
ユーザー登録の際に使用する上位プロキシサーバーの設定は、メニューバー「システム設定」から行ってください。

シリアル情報	
製品シリアルNo. ※必須	
利用ライセンス数 ※必須	0
ユーザー情報	
企業名 ※必須	
部署名 ※必須	
所在地 ※必須	〒 - 都道府県 市町村
担当者名 ※必須	
電話番号 ※必須	
Eメールアドレス ※必須	
Eメールアドレス (確認) ※必須	
サービス情報	
パスワード	 ※ライセンス情報サイトにアクセスする際のパスワードを設定します。
サービス情報配信	☐ サービス情報の配信を希望する 配信送信用Eメールアドレス 配信送信用Eメールアドレス (確認) ※デジタルアーツ株式会社からの配信メールを受信するEメールアドレスを入力します。

【図:ユーザー登録/登録情報入力画面】

■ 登録情報入力の流れ

1. 上位プロキシサーバー設定

⚠ 注意

- 直接インターネットに接続できる場合は上位プロキシサーバー設定は不要です。

必要な場合に応じて上位プロキシサーバーの設定を行います。「システム設定」→「上位プロキシサーバー」→「サーバー設定」をクリックすると、「システム設定/上位プロキシサーバー/サーバー設定」画面に移動します。

システム設定 / 上位プロキシサーバー / サーバー設定

ログインユーザー: admin

サーバー一覧

新規設定

上位プロキシサーバー設定	
アドレス:ポート番号	:
サーバー状態	☐ 利用 ☐ 待機 ☒ 無効
振り分け比率	1
「i-FILTER」通信	☒ 利用する
プロキシ認証	
認証設定	☐ 認証を行う
アカウント	☐ パスワードを更新する (※現在、パスワードが設定されていません。) ユーザー名 新パスワード 新パスワード (確認)
認証情報の転送	☐ 認証情報を上位プロキシサーバーに転送する

【図:システム設定/上位プロキシサーバー/サーバー設定】

システム設定 / 上位プロキシサーバー / 基本設定

ログインユーザー: admin ログアウト

保存

上位プロキシサーバー

有効設定 ☒ 有効にする

バランシング ラウンドロビン

i-FILTER通信

有効設定 ☒ 有効にする

上位プロキシルール設定

接続エラー判定

☒ しない ☐ 接続エラー回数で判定する

接続回数設定 30 秒間に 10 回接続に失敗した場合、「接続エラー」と判定する

挙動設定

☐ 待機サーバーに切り替える

☐ 待機サーバーがない場合、一時的に接続を中断する

復帰条件設定 接続エラー時、入れ替えを行った場合に復帰させる時間: 600 秒

【図:システム設定/上位プロキシサーバー/基本設定】

+ 補足

- 「システム設定/上位プロキシサーバー/サーバー設定」、「システム設定/上位プロキシサーバー/基本設定」画面についての詳細な設定方法は、『機能マニュアル』を参照してください。

2. シリアル情報

ライセンス証書に記載されている、「シリアルNo.」と利用ライセンス数を入力します。

シリアル情報

製品シリアルNo. ※必須 XXXX-YYYYYYYYYY-ZZZZ-NN

利用ライセンス数 ※必須

【図:シリアル情報】

+ 補足

- 「シリアルNo.」は以下の書式で入力します。

XXXX-YYYYYYYYYY-ZZZZ-NN	- X:半角数字4桁 - Y:半角英字10桁 - Z:半角英字4桁 - N:半角数字2桁(枝番)
-------------------------	---

- 「i-FILTER」を複数台のサーバーにインストールして運用する場合は、個々の「i-FILTER」のライセンス数の合計が、ライセンス証書に記載されているライセンス数になるように入力してください。

【例】ご購入ライセンス数が2000で、2台で運用する場合

- サーバーA:1000
- サーバーB:1000

- 複数台のサーバーで、同じ「シリアルNo.」は使用できません。追加「シリアルNo.」の発行は販売代理店もしくはデジタルアーツまでお問い合わせください。

3. ユーザー情報

「i-FILTER」をご利用いただくユーザー様情報を入力します。

ユーザー情報	
企業名 ※必須	デジタルアーツ
部署名 ※必須	開発部
所在地 ※必須	〒 123 - 4567 東京都 1丁目
担当者名 ※必須	佐藤 太郎
電話番号 ※必須	111-222-3333
Eメールアドレス ※必須	digital@djinc.co.jp
Eメールアドレス (確認) ※必須	digital@djinc.co.jp

【図:ユーザー情報】

4. サービス情報

デジタルアーツからお客様に向けて行うサービスに必要な情報を入力します。

サービス情報	
パスワード	password ※ライセンス情報サイトにアクセスする際のパスワードを設定します。
サービス情報配信	☒ サービス情報の配信を希望する 情報送信用Eメールアドレス digital@djinc.co.jp 情報送信用Eメールアドレス (確認) digital@djinc.co.jp ※デジタルアーツ株式会社からの情報メールを受信するEメールアドレスを入力します。

【図:サービス情報】

パスワード	ライセンス情報サイトにアクセスするためのパスワードを設定します。
サービス情報配信	「サービス情報の配信を希望する」にチェックを入れてユーザー登録を行った場合、「情報送信用Eメールアドレス」にご入力いただいたEメールアドレスへ、デジタルアーツからの各種ニュース情報を配信いたします。

「2.」～「4.」までを正しく入力し、「入力内容確認」ボタンをクリックします。

○ STEP4 登録情報確認画面

入力内容を確認の上、「送信する」ボタンをクリックします。

システム設定 / ユーザー登録・確認 / 登録情報確認

以下の内容で間違いありませんか？ 確認の上、「送信する」ボタンを押してください。
修正する場合は下の「戻る」ボタンで前の画面に戻ってください。

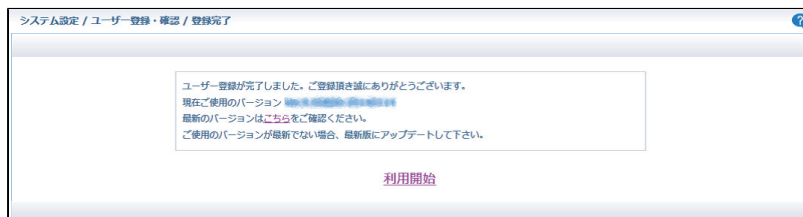
登録情報	
製品シリアルNo.	000000000000000000000000
企業名	デジタルアーツ
部署名	開発部
所在地	〒123-4567 東京都1丁目
担当者名	佐藤 太郎
電話番号	111-2222-3333
Eメールアドレス	digital@djinc.co.jp
パスワード	password
サービス情報配信	希望する (情報送信用Eメールアドレス: digital@djinc.co.jp)

戻る 送信する

【図:ユーザー登録/登録情報確認画面】

○ STEP5 ライセンス確認処理

「利用開始」リンクをクリックすると、「i-FILTER」のログイン画面を表示します。



【図:登録完了画面】

⚠ 注意

- サーバーの時刻とクライアントPCの時刻が大きくずれている場合、ログインできないことがあります。
- ライセンス認証に失敗している場合は、登録完了画面が表示されません。ライセンス登録時の失敗については、「7-2 「i-FILTER」のユーザー登録に失敗する場合」を参照してください。
- ルート管理者が「システム設定/ユーザー登録・確認」画面からユーザー登録を実施した後、「i-FILTER」を再起動する必要があります。これは標準装備されるSSL Adapterなどの機能を有効にするためです。再起動を行わないとSSL Adapterが有効にならず、SSL Adapterを利用したWebサービス制御も機能しなくなりますので必ず実施するようお願いいたします。

4-3 アドミニストレーターの設定

「i-FILTER」の管理画面にアクセスする際に、ユーザー名とパスワードの入力が必要になります。ルート管理者でログインを行い、メニューバーから、「システム設定」→「管理者設定」→「アドミニストレーター設定」を選択します。

+ 補足

- デフォルトの管理者ID・パスワードは以下が設定されています。

ルート管理者	ID「root」 パスワード「password」
アドミニストレーター管理者	ID「admin」 パスワード「password」

セキュリティ上、デフォルトの管理者ID・パスワードは変更してご利用いただくことを推奨しています。

The screenshot displays the i-FILTER administrator interface. At the top, there's a navigation bar with tabs like 'グループ設定', '共通設定', 'ルールセット', 'ログ', 'システム設定', and 'オプション'. Below this, a '運用情報' (Operational Information) section shows the server access time as '2014年 9月 17日 (水) 12時 29分 46秒'. The 'ログイン情報' (Login Information) section indicates the user 'admin' is logged in. The 'i-FILTER情報' (i-FILTER Information) section shows the version 'Ver. 9.11R01-20140912' and the 'フィルターデータベース' (Filter Database) version '20140917_01'. The 'プロセス情報' (Process Information) shows '1 プロセス / 400 スレッド'. The 'アクセス情報' (Access Information) section lists various access categories and their counts, such as '脅威情報サイト' (0), 'ボット・アダルトサイト' (0), 'アダルトグッズ' (0), 'グラビア・写真集' (0), '性教育・性の話題' (0), '暴力・猟奇描写' (0), '犯罪・武器凶器' (0), '麻薬・薬品薬物' (0), 'カルト・テロリズム' (0), '自殺' (0), '家出' (0), 'ハッキング・クラッキング' (0), '不正プログラム配布・リンク集' (0), '違法ソフト・反社会行為' (0), 'フィッシング詐欺' (0), 'クラッシャーサイト' (0), '迷惑メールリンク' (0), 'コンピューターサブライ' (0), 'オフィスサブライ' (0), 'オークション' (0), 'オンラインショッピング' (0), 'ポイントサービス' (0), 'クーポン総合サイト' (0), '出会い' (0), and 'Webメール' (0).

【図: アドミニストレーター設定画面】

4-4 ネットワークの設定

「i-FILTER」がインターネットにアクセスするために必要な設定を行います。

+ 補足

- アドミニストレーター権限のユーザーでログインし、設定を行います。

4-4-1 ポート番号の変更

必要に応じてポート番号を変更します。メニューバー「システム設定」>「システムパラメーター設定」>「システム機能設定」から設定を行ってください。変更した場合、「i-FILTER」の再起動が必要です。

+ 補足

- 詳細は『機能マニュアル』を参照してください。

4-4-2 上位プロキシサーバーの設定

ユーザー登録の際に設定した値が適用された状態となります。

メニューバー「システム設定」>「上位プロキシサーバー」>「基本設定」または「サーバー設定」を選択します。必要に応じて変更を行います。

+ 補足

- 詳細は『機能マニュアル』を参照してください。

4-5 ログの設定

「i-FILTER」は、動作中にアクセスログをはじめとした各種ログを出力することができます。メニューバー「システム設定」>「ログ設定」をクリックし、「ログ設定」画面からログ出力先を変更することができます。

○ システムログ

以下のログはシステム動作に関するメッセージが出力されます。出力ディレクトリを確認の上、必要があれば変更してください。

- プロセス別実行ログ(if_run)
- プロセス別実行ログ(if_server)
- プロセス別実行ログ(if_proxy)
- プロセス別実行ログ(if_eweb)
- プロセス別実行ログ(if_dl)
- プロセス別実行ログ(if_cache)
- プロセス別実行ログ(if_dweb)

○ 通信ログ/設定変更履歴

以下のログは、アクセス数に比例してディスク消費量が多くなります。サーバーのハードディスク容量などを考慮の上、必要があれば変更してください。

- アクセスログ
- ブロックログ
- POSTログ
- 設定変更履歴

4-6 認証サーバーの設定

「i-FILTER」を使用するユーザーに対して、各種認証サーバーを使用して認証を行うことで、詳細なユーザー管理を行うことができます。

- 認証しない
- LDAP 認証
- NTLM 認証
- 独自認証
- SNOOP 認証
- ICAP認証
- 詳細モード

上記の設定は以下の画面で設定できます。メニューバーから、「システム設定」>「ユーザー認証」>「基本設定」を選択します。

4-6-1 「i-FILTER for Linux」でのNTLM 認証について

「i-FILTER for Linux」でのNTLM認証はSMB署名には対応していません。NTLM認証にて認証先に指定するドメインコントローラー上の「ドメインコントローラセキュリティポリシー」にて、以下の設定を「無効」にしてください。

[Microsoftネットワークサーバー:常に通信にデジタル署名を行う]

+ 補足

- SMB署名の無効化については下記マニュアルを参照してください。

- 『機能マニュアル 11-4-5 SMB署名の無効化設定』
- 『運用マニュアル 3-2-2 「i-FILTER for Linux」』

4-6-2 「i-FILTER for Windows」でのNTLM認証について

認証を行うために必要なユーザー名とパスワードをActiveDirectoryサーバーに照会することで実現します。NTLM認証を使用する場合、以下の条件を満たす必要があります。

1. 「i-FILTER」がインストールされているサーバーがドメイン参加している

複数ドメインを認証に使用する場合は、そのいずれかに参加しており、全ドメイン間に信頼関係が結ばれている必要があります。

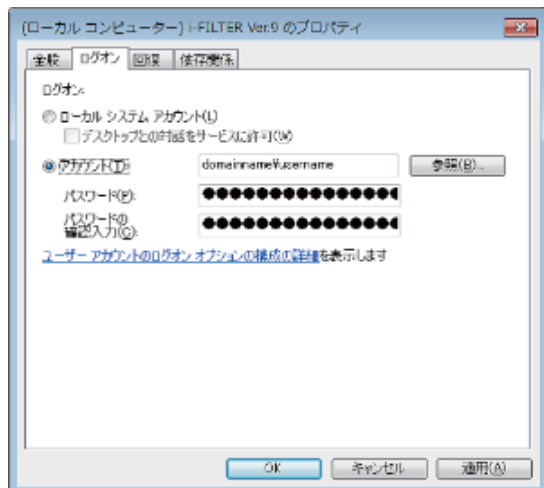
2. 「i-FILTER」のサービス(i-FILTER Ver.X)の起動ユーザーを「ドメイン管理者」に変更

※「X」は当該バージョン

デフォルトでは「ローカルシステムアカウント」になっています。これを変更しない場合、NTLM認証は利用できません。

⚠ 注意

- アップデートパッチ、自動アップデート機能により、i-FILTERのバージョンアップを行うと「ローカルシステムアカウント」に戻ります。「ドメイン管理者」に設定し直す必要があります。



【図:サービスのプロパティログオン】

ブラウザと「i-FILTER」(if_proxy)の間で行われるHTTP上での認証方式はNTLM認証となります。ブラウザがNTLM認証に対応していない場合は、対応できません。

+ 補足

- 「i-FILTER for Windows」のNTLM認証については『「i-FILTER」運用マニュアル 「3-2-1 「i-FILTER for Windows」」』を参照してください。

4-7 AV Adapter設定

Proxy

ここでは、AV Adapter機能を有効する手順および、ICAPクライアントとして動作させるための手順について説明します。この機能を使うことにより、「i-FILTER」とICAPサーバーとして動作する他社製ウイルススキャンサーバーとの連携が可能になります。

4-7-1 AV Adapter 機能を有効にする

注意

- 「AV Adapter」機能はオプションツールとして提供されています。使用するためにはライセンスが必要です。製品のご購入元、または弊社までお問い合わせください。
- 「AV Adapter」機能はICAPクライアントとして動作を行います。AV Adapterの機能を利用するためには、対応したICAPサーバー製品が必要です。AV Adapterが対応しているICAPサーバー製品の情報につきましては、弊社へお問い合わせください<<https://www.daj.jp/support/contact/>>。
- 「AV Adapter」機能を利用するためには、必ずSSL接続終端処理もしくはSSL Adapterをご利用いただく必要があります。
- 「AV Adapter」機能は「i-FILTER Proxy Server」固有の機能です。

AV Adapter機能を有効にするための手順は、以下の通りです。

○ STEP1

アドミニストレーター権限を持つユーザーでログインを行い、管理画面のメニューバーから「オプション」をクリックします。以下のように「AV Adapter」項目が表示されている場合はライセンス確認が正常に行われているため、「STEP2」以降の作業は不要です。



【図:ライセンス状態】

「AV Adapter」項目が表示されない場合は、ライセンス確認が行われていないため「STEP2」でライセンス登録を行います。

○ STEP2

ルート管理者でログインを行い、管理画面のメニューバーから「システム設定」→「ユーザー登録・確認」をクリックします。



【図:管理画面のメニュー】

ライセンスに関する事務手続きが完了していることを確認の上、ユーザー登録を行います。

ソフトウェア上で認証処理を行うため、[入力内容確認]ボタンをクリックし、さらに[送信する]ボタンをクリックします。ライセンスが有効になったかどうか確認するため「STEP3」に進みます。

○ STEP3

アドミニストレーター権限を持つユーザーでログインを行い、管理画面の「メニューバー」から「オプション」をクリックします。

管理画面に「AV Adapter」が表示されます。ライセンス有効となったことを確認後、再起動が必要になるので「i-FILTER」の再起動を行います。

4-7-2 ICAPサーバー設定(Kaspersky Anti-Virus for Proxy Server)

本項では「Kaspersky Anti-Virus for Proxy Server(以下、Kaspersky Anti-Virus)」のインストール、設定が終了しているものとして説明します。

+ 補足

- インストール、設定方法につきましては「Kaspersky Anti-Virus for Proxy Server管理者ガイド」を参照してください。
- 本項では「Kaspersky Anti-Virus」のIPアドレス、待ち受けポート番号が、以下のように設定してあるものとして手順を記載しています。

IP アドレス:192.168.1.200
ポート番号:1344

「i-FILTER」と連携する場合、「Kaspersky Anti-Virus」では以下の作業が必要です。

○ STEP1 設定ファイルの書き換え

設定ファイル「/etc/opt/kaspersky/kav4proxy.conf」を修正します。

【修正前】

```
[icapserver.network]

# Address where icap server listens for connections
ListenAddress=localhost:1344
```

【修正後】

```
[icapserver.network]

# Address where icap server listens for connections
ListenAddress=192.168.1.200:1344
```

※ localhostの箇所を「Kaspersky Anti-Virus」が動作しているサーバーのIPアドレスに書き換えます

○ STEP2 ブロック画面表示のための作業

ウイルス検出時に、「i-FILTER」側でブロック画面を表示するため、/opt/kaspersky/kav4proxy/share/notify内の通知用テンプレートファイルを、『「AV Adapter」利用時の付属ファイル一式』と置き換えます。

・対象ファイル

```
object_corrupted
object_cured
object_error
object_infected
object_protected
object_suspicious
object_warning
```

+ 補足

- 『「AV Adapter」利用時の付属ファイル一式』は、下記ページよりダウンロードしてください。

<https://download.daj.co.jp/user/ifilter/V9/>

※ 製品の「シリアルNo.」とお客様「E-Mailアドレス」によるログインが必要です。

○ STEP3 再起動

「Kaspersky Anti-Virus」の再起動を実施します。

4-7-3 ICAPクライアント設定

「i-FILTER」側では、ICAPサービス設定(ICAPサーバー登録)および、ICAPサーバー転送ポリシー設定を行うことで連携が行えます。

■ ICAPサービス設定

「i-FILTER」のメニューバーから、「オプション」>「AV Adapter」>「ICAPサービス設定」をクリックし、「ICAPサービス設定」画面を開きます。ICAPサーバーと連携するために、以下「STEP1」～「STEP3」を設定していきます。

○ STEP1

ICAPサーバーの登録を行います。「ICAPサービス設定」画面の一覧にある[追加]ボタンをクリックして、ICAPサービス設定を行います。以下の項目に値を設定します。

設定名	「ICAP サーバー1」(任意)
ICAPサーバーURL	icap://192.168.1.200:1344/av/reqmod (REQMOD用に設定する場合) icap://192.168.1.200:1344/av/respmo (RESPMOD用に設定する場合)
その他の項目	入力不可

○ STEP2

サーバーからの情報を取得します。

[設定取得]ボタンをクリックすると、ICAPサーバーへ情報を問い合わせます。問い合わせに成功すれば、「STEP1」で入力不可になっている部分が、入力できるようになりますので、各項目に任意の値を設定してください。

○ STEP3

AV Adapter機能を使用するために、「i-FILTER」のメニューバーから、「オプション」>「AV Adapter」>「基本設定」をクリックし、「基本設定」画面を開きます。また、「ICAPクライアント機能」の「有効」にチェックを入れます。

■ ICAPサーバー転送ポリシー設定

ICAPサーバーの設定に成功すると、一覧に設定が追加されます。

【図:AV Adapter/ICAPサービス設定画面】

登録したICAPサーバー設定は、管理画面の「AV Adapter」→「ICAPサーバー転送ポリシー設定」画面より、「ICAPサーバー転送ポリシー設定」を登録します。

【図:ICAPサーバー転送ポリシー設定画面】

■ 動作確認

Webサーバーから、ウイルスを含んだファイルをダウンロードしようとしたとき、クライアントには、以下のようなブロック画面が表示されます。

【図:ウイルスを検知時に「i-FILTER」が表示するブロック画面】

+ 補足

- 各機能の説明については、『機能マニュアル』を参照してください。

第5章 運用設定

5-1 運用設定をする

5-1 運用設定をする

初期設定が完了したらご利用環境に必要な運用設定を行います。設定においては以下のマニュアルを参考にしてください。

『運用マニュアル』	運用事例をベースに「i-FILTER」でよく利用される機能の設定手順を掲載したマニュアルです。 目的別に設定を行う場合にご利用ください。
『機能マニュアル』	「i-FILTER」の機能全般の説明や各種設定方法、トラブルシューティングを掲載したマニュアルです。 設定の過程で各種機能についてご不明点があればこちらをご確認ください。

+ 補足

- その他のマニュアルやドキュメントの入手方法については「[関連ドキュメント](#)」を参照してください。

第6章 ライセンス

この章では、ライセンスについて説明します。

6-1 ライセンス更新手続き

6-2 登録内容の変更

- 6-2-1 お客様情報の変更
 - 6-2-2 システムの変更
-

6-1 ライセンス更新手続き

「i-FILTER」を続けてお使いいただくには、ライセンス契約期間の更新が必要となります。ライセンス更新手続きの手順は購入形態により異なります。ライセンスの更新・追加については、製品のご購入元までお問い合わせください。

6-2 登録内容の変更

6-2-1 お客様情報の変更

ルート管理者にてログインした状態で「i-FILTER」のメニュー画面のユーザー登録・確認をクリックすると、導入時に登録したユーザー情報を確認することができます。

登録後にEメールアドレスや担当者名など、登録情報が変わった場合には、こちらの画面で項目を変更して「送信」ボタンをクリックすると登録内容を変更することができます。

+ 補足

- 詳細は『「i-FILTER」運用マニュアル 「8-3 ユーザー登録情報を確認・変更」』を参照してください。

6-2-2 システムの変更

ユーザー登録を管理しているサーバーでは、ご利用OSのハッシュ情報（Windows）、MACアドレス(Linux)を使用してライセンス管理を行っています。

これらの値が変更された場合は、ユーザー登録、ライセンス認証に失敗したことを示すエラーメッセージが表示されます。

以下の変更を行う場合は、サポートサービスをご提供している販売店もしくは代理店にご確認の上、「ライセンス情報サイト」より再アクティベーション手続きを行ってください。

○ ライセンス情報サイト

<https://sec2.daj.co.jp/license/ifilterV9/>

■ Windows

- 「i-FILTER」を運用しているサーバー機を変更する場合
- 「i-FILTER」を運用しているサーバーが使用しているネットワークカードを変更する場合
- 「i-FILTER」のアンインストールを行った際に、インストール後に作成されたファイルすべてを削除した場合
- 「i-FILTER」を運用しているサーバー機のOS を再インストールしたり、OS のバージョンを変更する場合

■ Linux

- 「i-FILTER」を運用しているサーバー機を変更する場合
- 「i-FILTER」を運用しているサーバー機が使用しているeth0 のネットワークカードを変更する場合
- 「i-FILTER」のアンインストールを行った際に、インストール後に作成されたファイルすべてを削除した場合

再アクティベーション手続き完了後、「i-FILTER」の管理画面より、再度ユーザー登録を行ってください。

+ 補足

- サーバー機のIP アドレス変更では、ライセンス（アクティベーション）エラーは発生しません。

第7章 トラブルシューティング

この章では、トラブルシューティングについて説明します。

7-1 「i-FILTER」が起動しない場合

7-2 「i-FILTER」のユーザー登録に失敗する場合

7-3 認証機能が正常動作しない場合

7-4 設定画面へのログインパスワードを忘れた場合

7-5 パフォーマンス向上について

- 7-5-1 サーバー機のCPU 処理能力の不足
- 7-5-2 「i-FILTER」のプロキシスレッド数の不足
- 7-5-3 OS のファイルディスクリプタの不足
- 7-5-4 メモリ不足
- 7-5-5 外的要因に依存する「i-FILTER」処理の遅延

7-6 新規インストール後にエラーログが出力される

7-1 「i-FILTER」が起動しない場合

「i-FILTER」の起動処理を行っても正常に起動しない場合は、以下の点を確認してください。

■ ポート番号の確認(全OS共通)

初回起動時「i-FILTER」はデフォルトのポート(15080,15081)を使用して起動しようとするため、ポートの重複がないか確認します。

ポートが重複していた場合、一時的に重複したポートを使用しているサービスを停止し、「i-FILTER」を起動しポート設定を変更後、「i-FILTER」と既存サービスの再起動を行います。

管理画面の「メニューバー」から「システム設定」→「システムパラメーター設定」→「システム機能設定」を選択し、サービスポート番号設定の「管理画面」を変更します。

■ 「i-FILTER for Linux」の場合

○ 「i-FILTER」のログを確認

「i-FILTER」のログを参照し、起動に失敗している原因を調べます。

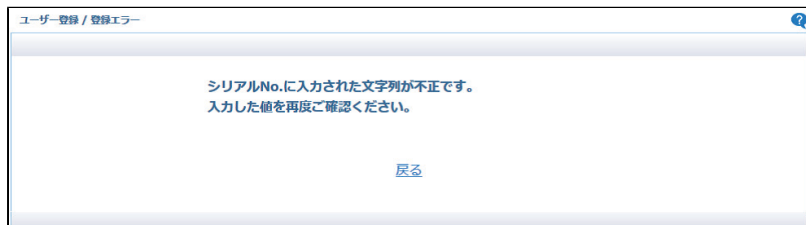
【ログのデフォルトパス】

- /usr/local/ifilter9/logs/run.log
- /usr/local/ifilter9/logs/dl.log
- /usr/local/ifilter9/logs/eweb.log
- /usr/local/ifilter9/logs/listen.log

7-2 「i-FILTER」のユーザー登録に失敗する場合

ユーザー登録が正常に行えなかった場合、画面に表示されるエラーメッセージと、対応方法をご参照の上、「ユーザー登録・確認」画面で入力した内容を確認してください。

ユーザー情報を登録サーバーに送信する際、正常に通信が行えなかった場合や、ユーザー登録サーバーにおける認証処理エラーに関しては、対応方法の欄にその詳細が表示されます。



【図:エラーメッセージ出力例】

+ 補足

- エラーメッセージの内容はエラーの種類によって異なります。

■ ユーザー登録時のエラーメッセージ一覧

初期化エラーが発生しました。
内部エラー(101)が発生しました。
接続エラー(201) 通信経路上に問題が発生している可能性があります。 DNS エラーの可能性があります。 ユーザー登録サーバーが停止している可能性があります。 時間をあけてから再度実行してください。
送信エラー(202) 通信経路上に問題が発生している可能性があります。 時間をあけてから再度実行してください。
受信エラー(203) 通信経路上に問題が発生している可能性があります。 時間をあけてから再度実行してください。
受信エラー(204) 通信経路上に問題が発生している可能性があります。 時間をあけてから再度実行してください。
受信エラー(205) 通信経路上に問題が発生している可能性があります。 時間をあけてから再度実行してください。
シリアルNo.に入力された文字列が不正です。 入力した値を再度ご確認ください。
Eメールアドレスの形式が正しくありません。
このシリアルNo.は一時停止中です。販売店にお問い合わせください。
マシン固有情報が前回登録時と異なります。販売店にお問い合わせください。
入力したライセンス数をご契約いただいたライセンス数より多いか、ゼロが入力されています。 入力した値を再度ご確認ください。 複数サーバーに導入する場合は、個々のサーバーのライセンス数の合計値が ご契約いただいたライセンス数になるように振り分けてご入力ください。
ライセンス期限が切れています。 継続してご利用いただくためには、販売店にご連絡ください。
登録サーバー上でエラーが発生しました。 サーバーがメンテナンス中である場合があります。 時間をあけてから再度実行してください。
ライセンスは無効になりました。 期限切れ、一時停止中、マシン固有情報異常、またはライセンス数不正の可能性があります。

7-3 認証機能が正常動作しない場合

認証に失敗し、認証ダイアログが表示され続ける場合、LDAPサーバーへの通信が届いていないか、ユーザーが正しく設定されていない可能性があります。「i-FILTER」に設定した文字列を引数として、ldapsearchコマンドを実行し、入力値に誤りがないかを確認します。

【例】

```
# ldapsearch -h 10.0.23.26 -b "dc=daj.co.jp" "uid=guest"
```

< 成功した場合>

```
uid=guest,dc=daj.co.jp
uid=guest
cn=guest
givenname=user
sn=1
objectclass=top
objectclass=person
objectclass=organizationlPerson
objectclass=inetorgperson
```

< 失敗した場合>

```
ldap_simple_bind_s:Invalid credentials
```

⚠ 注意

- ldapsearchコマンドはご使用のOS、バージョンにより、オプション、表示が異なります。ご使用の環境に応じてコマンドを実行してください。

7-4 設定画面へのログインパスワードを忘れた場合

管理画面へのログインパスワードを忘れた場合は、サポートにお問い合わせください。

+ 補足

- お問い合わせ先につきましては、『機能マニュアル 12-2 サポート情報』を参照してください。

7-5 パフォーマンス向上について

多数のクライアントがある環境で、始業・昼休み・日報記入などによりアクセス負荷が急増した場合、クライアント側のWebアクセスに著しい遅延が生じたり、アクセスが不可能になったりという現象が起こる場合があります。

この章では、設定や性能面に起因するこのようなトラブルの解決や導入時設定の際の予防を目的とし、これらの現象の具体的な原因・解決法などを提示します。

7-5-1 サーバー機のCPU 処理能力の不足

○ 現象

vmstatなどによるOSの確認でCPU使用率が90%を超えている(Windowsはvmstatの代わりにタスクマネージャーを利用することで確認が可能です)。

○ 発生しやすい環境・条件

- サーバーのハードウェアが古く、CPU性能が十分でない。
- サーバースペックに対してユーザー数・アクセス数が多い。
- 単語フィルターが有効になっている。
- 正規表現を使用するユーザー定義リストなどが大量に登録されている。
- CPUリソースを消費するほかのアプリケーションが同一サーバーに同居している。

○ 対策

- 「i-FILTER」のサーバーを増設し、複数台で負荷分散を行う。
- CPU性能の高いサーバーに交換する。
- 単語フィルターを無効にする。
- 正規表現を使用するユーザー定義リストなどを減らす。

○ 参考

「i-FILTER」の処理内容は、(設定によって異なりますが)宛先URLのチェックおよびプロキシとしての動作となりますが、この一連の動作では多くの場合CPUに最も大きな負荷がかかります。そのため、「i-FILTER」自身の負荷やほかのアプリケーションの負荷によりCPUが飽和状態になるとそれ以上のアクセスを受けつけられなくなります。この状態は、vmstatなどで簡単に発見でき、容易に解決策を見出せます。

7-5-2 「i-FILTER」のプロキシスレッド数の不足

○ 特徴

netstatによる「i-FILTER」プロセスの接続数が、以下の式を満たしている。

ESTABLISHED ≧ スレッド数×プロセス数

補足

- ここでのESTABLISHEDの数はif_proxyへの待ち受けポートへの接続を指します。

○ 発生しやすい環境・条件

- アクセス先URLのレスポンスが悪く、スレッドの解放に時間がかかる。
- 「i-FILTER」より上位にあるいずれかの設備（上位プロキシ・ルーターなど・回線等）に、何らかの理由（過負荷・設定ミス・障害等）により遅延などが発生している。
- 外部への回線が非常に細い。
- 昼休みなどで短時間に大量のアクセスが集中している。
- ストリーミング・大量ダウンロードなど、長時間コネクションを維持するようなアクセスを行うユーザーが多い。
 - + 上位or下位とのKeep-Aliveが有効で、ユーザー数が多い。
 - + 上位or下位とのKeep-Aliveが有効で、タイムアウトの設定時間が長い。

○ 対策

- 「スレッド数」を増やす。
- 「i-FILTER」の上位にある設備の状況を調査する。
- 上位とのKeep-Aliveを無効にする。

○ 参考

十分なハードウェア性能がある場合でも、クライアント数がある程度以上多い場合(状況によって異なりますが8,000以上)には、「スレッド数」をデフォルトの400に下げて運用することは危険です。

理論上はまったく問題のない環境であっても、レスポンスの悪いサイトやストリーミング受信サイトなどへの接続によりスレッド占有時間が長くなることは考えられ、そのような場合にクライアント数が多いと400のスレッドは埋まってしまいます。上位回線が細い場合や、上位プロキシなどが遅い場合も同様の現象が起こる可能性があります。

このような場合は、まず「スレッド数」の値を調整してください。また、上位にほかのプロキシ(キャッシュ・ウイルススキャンなど)がある場合、それらが適正に動作しているかどうか、負荷状態・設定を再度見直します。

○ 適正な値の考え方・設定値の目安

プロキシからのリクエストに対してWEBサーバーが即座に応答を返すと仮定するとスレッドは即時に解放されることになり、スレッド数はあまり問題にはなりません。実際には長時間にわたる通信や様々な理由による遅延などのためにスレッドが占有される機会があるため、スレッドが埋まることによる著しいアクセス遅延などの起こる余地が生まれます。

たとえば、上位にウイルススキャン処理を行うプロキシがある場合、一般的にウイルス検索の負荷はWEBフィルタリングより負荷が高いため、スレッドを長く占有する可能性が高くなります。

例として、秒間アクセス数が200 Request/Secの環境を想定した場合にスレッド数設定がデフォルトの400であったとすると、1アクセスあたりの平均所要時間が2秒を超えると $200 \times 2 = 400$ となりすべてのスレッドは埋まり、以後著しい遅延が発生することになります(実際に取得に2秒を超えるようなケースは稀だと思われます)。

秒間アクセス数と同時接続数の関係に関する目安は以下の式になります。

$$\text{同時接続数} = \text{秒間アクセス数} \times \text{平均送受信完了秒数} + \text{余剰値}$$

具体的に8,000ユーザーの環境で、Webアクセスの平均所要時間が2秒と仮定すると、

$$8,000 \times 0.3 \times 2 = 4,800$$

(アクセス数のピーク値をライセンス数の30%と仮定)

となり、4,800以上のスレッド数が必要という結果となります。

設定目安としては、ピーク時の秒間アクセス数と同数が最低限、その2.5～3倍程度を安全圏と考えるとよいと思われます。ライセンス数ごとに数字を大雑把に見積もると、以下の表のようになります(秒間最大アクセス数をライセンス数の30%と推定)。

ユーザー人数(人)	推定最大秒間アクセス数(≒ユーザー数×0.3)	スレッド数安全圏 (≒推定最大アクセス数×3)
1,000	300	900
3,000	900	2,700
5,000	1,500	4,500
9,999	3,000	9,000

【表:スレッド設定値目安】



注意

- 極端な値を設定するとOS・メモリにかかる負荷が無駄に大きくなり性能劣化を招く可能性があります。

7-5-3 OS のファイルディスクリプタの不足

○ 特徴

netstatによる全プロセスの接続数にて、以下の式を満たしている。

ESTABLISHED+TIME_WAIT≦ファイルディスクリプタ上限値

○ 発生しやすい環境・条件

- 同一サーバーにほかのプロキシサーバー、メールサーバーなど、ネットワーク接続を大量に張るアプリケーションが同居している。
- クライアントからのアクセス要求数が非常に多い。
- 「スレッド数」に非常に大きい値を設定している。
- Keep-Aliveを無効に設定している。

○ 対策

- 同居しているほかのアプリケーションを外し、ほかのサーバー機へ移植する。
- TIME_WAIT開放までの待機時間を短くする。
- ファイルディスクリプタの上限値を上げる(Linuxの場合)。
- 上位方向へのKeep-Aliveを有効に設定する。

○ 参考

「i-FILTER」との通信終了後、接続が閉じられるときにTIME_WAIT状態になりますが、このTIME_WAIT状態のソケットが非常に多い場合、OS側に設定されている接続数上限に引っかかり新しいソケットを作成できなくなるため、接続解放待ち行列が発生し著しい遅延が発生します。

1台のサーバーにほかのプロキシと「i-FILTER」が同居して多段プロキシの構成になっているような環境では、この状況が発生する可能性が特に高くなります。

■ Windows

TIME_WAIT待ち時間の変更には、レジストリのHKEY_LOCAL_MACHINE以下にキーを作成し値を設定します。

HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥Tcpip¥Parameters¥TcpTimedWaitDelay

+ 補足

- 設定詳細はMicrosoft社サイト等を参照してください。

⚠ 注意

- 接続数の上限については、Unix系OSと異なり明確な上限値を設定することはできません。

生成可能な最大ソケット数を多くすることで、接続数の上限を間接的に増加することができます。以下のレジストリキーを作成し、値を設定します。

HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥Tcpip¥Parameters¥MaxUserPort

- ※ Windowsのデフォルトの生成可能な最大ソケット数は5000となっています。
- ※ 上記レジストリキーの最大値は65534です。設定を行う際には、最大値を設定することを推奨します。

■ Linux

OSおよび「i-FILTER」の実行ユーザー(root)のファイルディスクリプタを十分な値に設定することで、接続数増加への対応が可能です。

例

- OSの接続数上限を「600000」、ユーザーの接続数上限を「100000」に設定する場合

1. OSの接続数上限値を変更

```
# vi /etc/sysctl.conf

kernel.threads-max=600000
fs.file-max=600000
kernel.pid_max=600000
vm.max_map_count=600000

# sysctl -p()
```

2. ユーザーの接続数上限値を変更(rootで実行)

```
# ulimit -n 100000
# /etc/init.d/ifilter9 restart (設定を反映)
```

※ OSの接続数上限値がユーザーの接続数上限値を上回るように設定してください。
※ 実環境への適用は利用状況を確認の上、適切な設定値および設定方法にて実施してください。

7-5-4 メモリ不足

○ 特徴

メモリにスワップが発生している。

○ 発生しやすい環境・条件

- 「スレッド数」に非常に大きい値が設定されている。
- ほかのアプリケーション・OSがメモリを大量に消費している。
- 物理メモリの搭載量が少ない。

○ 対策

- 「スレッド数」の値を適切な値に調整する。
- メモリを大量に消費するアプリケーションを外す。
- 物理メモリを増設する。
- メニューバーから「システム設定」→「システムパラメーター設定」→「システム機能設定」を選択し、プロキシ機能パラメーターの フィルターDBを[ファイルシステム]にする。

○ 参考

「i-FILTER」側が原因で起こる可能性としては、OSの空きメモリ容量を超える「スレッド数」を設定した場合が考えられます。

また、タスクマネージャーやvmstat、topなどでメモリの使用状況から「i-FILTER」以外のアプリケーションやOSの動作に問題がないかを確認してください。

7-5-5 外的要因に依存する「i-FILTER」処理の遅延

○ 特徴

CPU／メモリ使用率やnetstatによるネットワーク状態のいずれにも問題がない。

○ 発生しやすい環境・条件

- | | |
|---|--|
| ◎ | DNS引きに時間がかかっている
(特にアクセスログにDNSの逆引き結果を追加の場合)。 |
| ○ | LDAP/NTLMなどの認証を使用している場合、認証サーバーの応答が遅い。 |

○ 対策

- | | |
|---|---|
| ◎ | DNS応答の改善策を別途講じるか、あるいは「DNS逆引き機能」有効時はこれを無効に設定する。 |
| ○ | 認証サーバー応答の改善策を別途講じるか、あるいは認証情報のキャッシュ時間を長く設定する。
([メニュー]-[オプション]-[システムパラメーター]) |

○ 参考

これらは「i-FILTER」自体の遅延ではありません。上記のような条件を満たすよう設定している場合は、試験的にこれらの設定を外していただくことをお勧めします。

7-6 新規インストール後にエラーログが出力される

「i-FILTER」を新規インストールした後、サービス初回起動時はif_proxy(.exe)プロセスの実行ログに以下のエラーが出力されます。

ログファイルパス	<インストールディレクトリ>/logs/proxy.log0000
出力内容	[ERR] YYYY/MM/DD/hh:mm:ss フィルターデータベース制御機能の初期化に失敗しました。(XXX)

上記エラーは、インストール直後にフィルターデータベースファイルが存在しないために出力されますが、その後、フィルターデータベースの自動更新が実行されるため問題はありません。

フィルターデータベースの自動更新は、if_dl(.exe)プロセスの実行ログから以下の出力を確認してください。

ログファイルパス	<インストールディレクトリ>/logs/dl.log
出力内容	[INFO] YYYY/MM/DD/hh:mm:ss 更新処理が終了しました。データが更新されました。

www.daj.jp