

Vol.

3



だいこくネット

File Access Log

操作ガイド



FILE ACCESS LOG

操作ガイド

だいこくネット

©2002-2011

目次

はじめに.....	2
機能概要.....	2
機能説明.....	3
動作環境.....	4
アプリケーション構成.....	5
セットアップ.....	6
インストール先の決定.....	6
インストール方法.....	6
アンインストール方法.....	6
クイックセットアップ方法.....	7
アクセス情報のリスト項目説明.....	11
接続時間.....	11
アクション.....	11
TreeID.....	12
クライアント.....	12
サーバ.....	12
サイズ.....	12
パス.....	12
操作.....	12
メニュー項目の説明.....	13
メインメニュー.....	13
オプションダイアログ.....	14
ライセンスキーの設定方法.....	16
ログファイルへの収集方法.....	17
監視管理機能設定方法.....	19
監視管理画面の表示.....	19
監視除外情報の初期エントリについて.....	20
監視除外情報の追加.....	21
監視除外情報の有効化・無効化.....	22
FAL Hosts の設定方法.....	24
ini ファイルの隠し定義.....	25
名前解決処理抑止機能.....	25
多重ログ出力抑止機能.....	25

ログ出力形式	26
エラーログ	27
サービスの登録方法	28
NIC が2枚以上ある場合の設定方法	30
メッセージ一覧	31
バグ、問題点、改善点	32
ご使用にあたって	32
免責 等	32
著作権と使用範囲	32

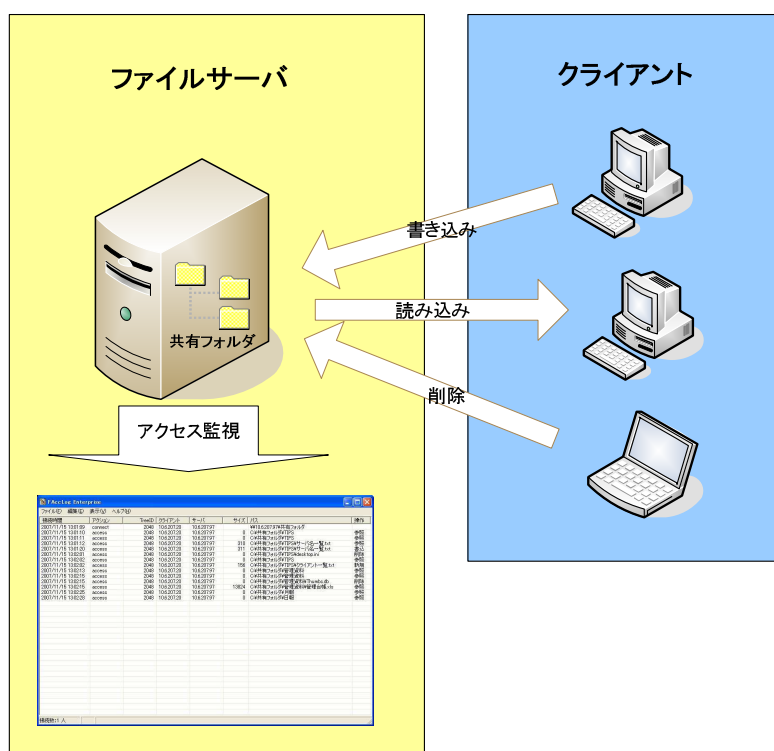
はじめに

FAccLog (File Access Log)は、ファイルサーバのアクセスを監視し情報漏えいのリスクを低減させることができるアプリケーションです。

FAccLogを導入することで、ファイルサーバにアクセスしてきたユーザの履歴が収集でき、収集したアクセスログは、監査用としての情報源として利用することが可能です。アクセス収集はリアルタイムで可能で重要なファイルサーバへ「いつ」「誰が」「どこに」「どんなアクションをしたか」を瞬時に把握が可能です。

機能概要

これまでアクセス監視を行うには、いろいろな手間と時間がかかり、不正アクセスへの監視はサーバ管理者の負担を大きくしてきました。FAccLog Ultimate は、これまでの煩わしいクライアントPCへの設定作業を一切なくし、ファイルサーバのみのインストールでアクセス監視が可能になり手軽に導入いただけます。



機能説明

- ・ **アクセス監視機能**

エクスプローラ形式で共有フォルダへのアクセス履歴が表示されます。表示情報には、「接続時間」「アクション」「TreeID」「クライアント IP アドレス」「サーバ IP アドレス」「サイズ」「パス」「操作」が表示され、管理者は容易にアクセス状況を把握可能です。

- ・ **アクセス除外監視機能**

特定のフォルダ・ファイルに対してアクセスを監視、又は、除外可能です。収集さしたくない情報、また、特定のフォルダ・ファイルのみ監視したい場合には有効です。除外、及び監視範囲として「ファイル単位」・「フォルダ内」・「フォルダ配下」を選択可能です。

- ・ **アクセスログ取得機能**

アクセス監視で検出した履歴をログとしてファイルに保存可能です。また、ログファイルはファイルサイズ及び日付によってローテーションが可能です。

動作環境

OS

- Windows 2000 (Professional,Server,Advanced Server) ※2,※3,※4
- Windows 2003 (Standard,Server,Ultimate,Datacenter,Small Business Server) ※2,※4
- Windows 2008 (Server SP2,Server R2,Small Business Server) ※1,※4
- Windows Vista,Windows 7 ※1,※4
- Windows XP ※2,※4

※1 … SMB1.0、SMB2.0 でのアクセス収集が可能です。

※2 … SMB1.0 のみアクセス収集が可能です。

※3 … 動作検証を行っておりません。

※4 … 64bit 版 OS は未検証です。

必要な動作環境

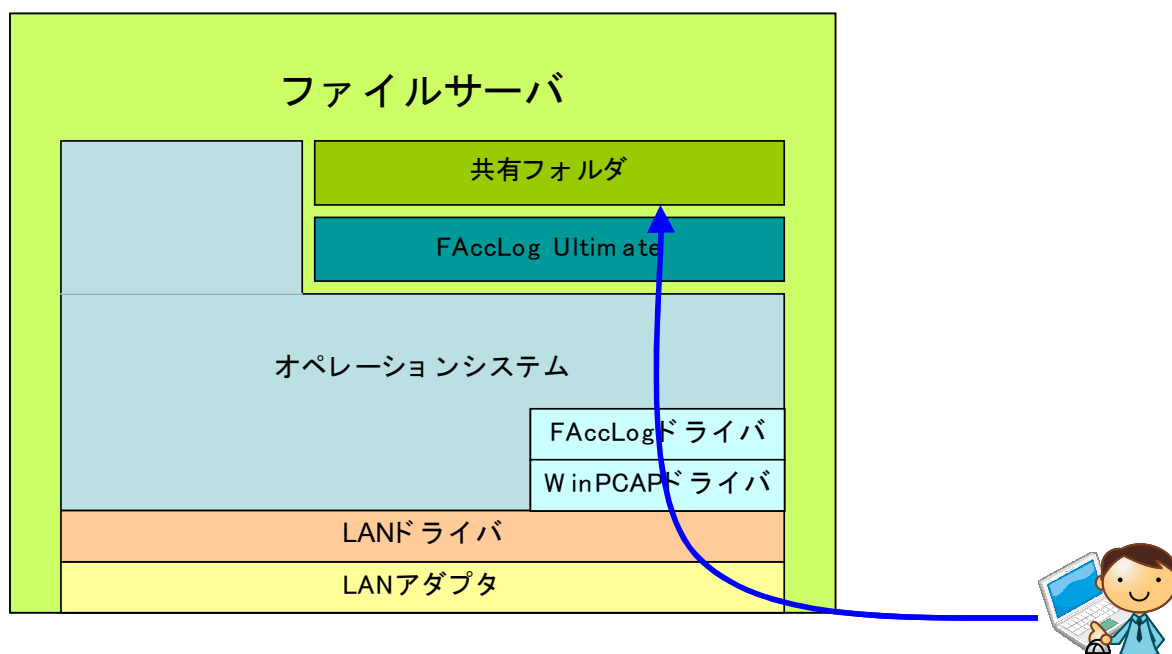
- PentiumⅢ 1GHz 以上のプロセッサ
- 10MB 以上の空メモリ
- 10M 以上の空き HDD 容量(起動環境のみ)
- .NET Framework ランタイム
- 有線LANアダプタ形式の NIC
- WinPcap ドライバ (FAccLog Ultimate のみ)

推奨環境

- PentiumⅣ 2GHz 以上のプロセッサ
- 1GB 以上のメモリ搭載
- アクセスログに応じた空き HDD 容量

アプリケーション構成

FAccLog Ultimate は、クライアント PC からのファイルアクセスに対し、OS 情報、及び、WinPcap ドライバを使用して LAN アダプタからパケットキャプチャリングを行い、各アクセス情報を収集しログ情報として出力します。



セットアップ

インストール先の決定

FAccLog Ultimate のインストール先のディレクトリは、任意にディレクトリを作成し、ダウンロードしたアーカイブファイルを解凍し配置します。

インストール方法

1. FAccLog_Ultimate.zip をダウンロードする。
2. FAccLog_Ultimate.zip アーカイブの解凍する。
解凍後、右記のフォルダが作成される。 → “FAccLog_Ultimate”
3. 任意のインストールフォルダに配置する。
例) C:\FAccLog_Ultimate

メモ

インストーラは同伴されていないので、配布アーカイブを解凍後、ご使用の環境にあわせ配置をしてください。

アンインストール方法

1. インストール手順で、配置した任意のインストールフォルダを削除する。

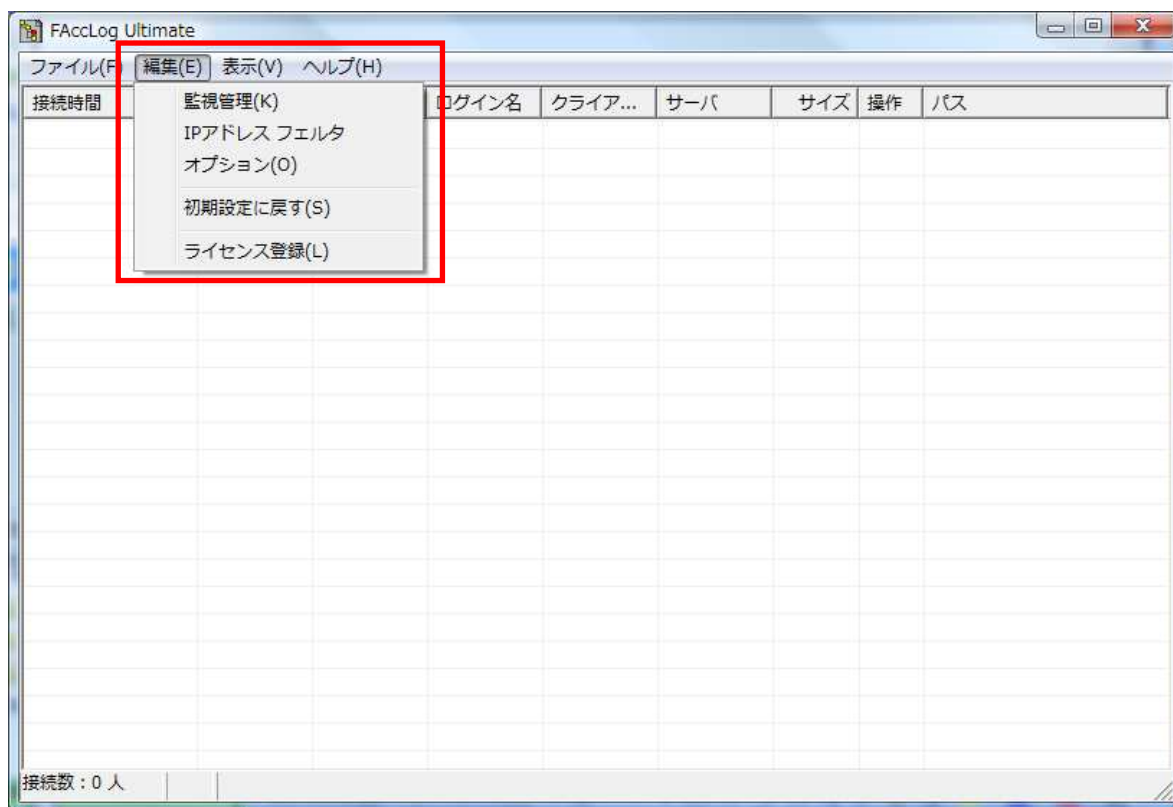
メモ

インストールフォルダ以外に FAccLog Ultimate に関わる情報ファイルはありません。

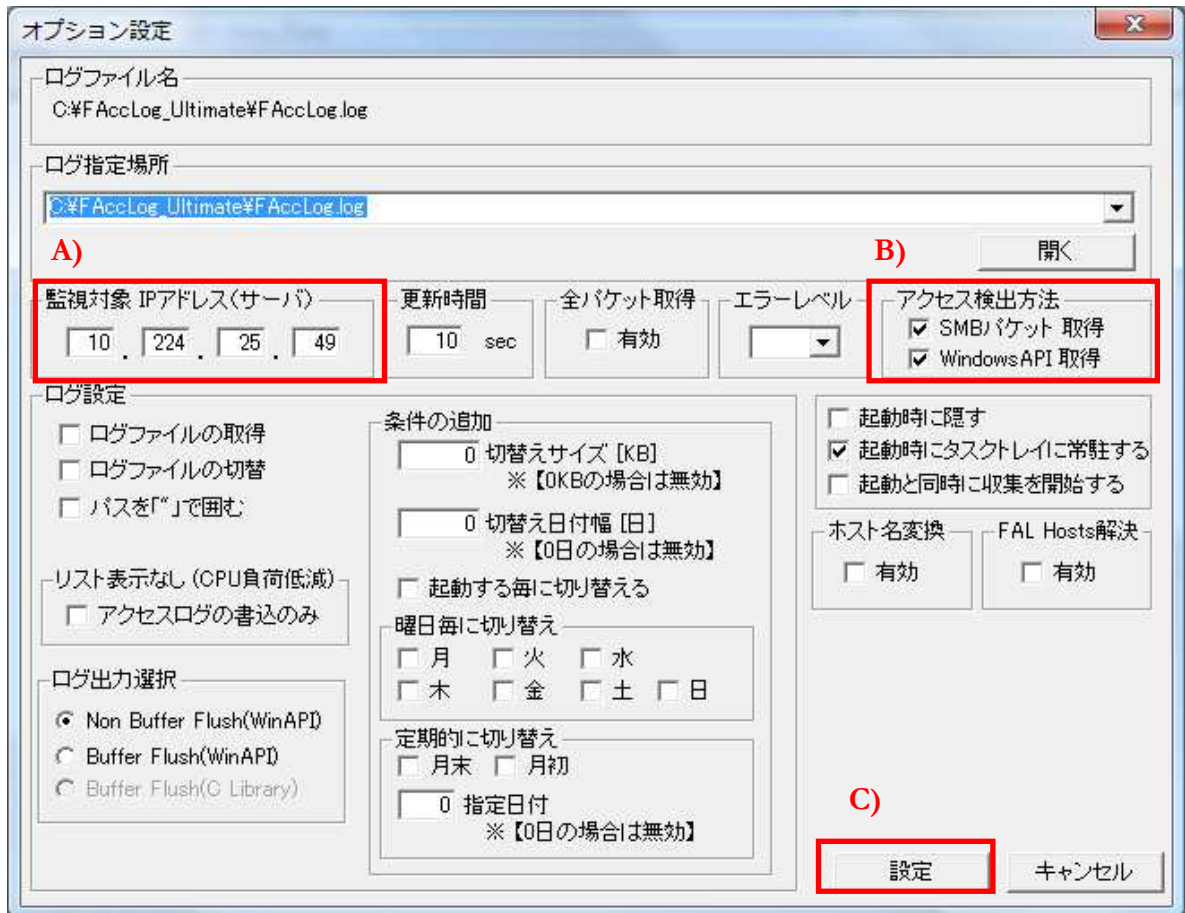
クイックセットアップ方法

FAccLog Ultimate のセットアップ方法について、次の手順を実行してください。

1. 任意のインストールフォルダから「FAccLogUltimate.exe」をダブルクリックし、実行する。
2. FAccLogUltimate が起動後、「編集」メニューの「オプション」を選択する。



オプション画面が表示され、下記の設定項目を任意に設定する。



A) 監視対象 IP アドレス

FAccLog Ultimate をインストールされた、ファイルサーバの IP アドレスを設定する。

B) アクセス検出方法 ※詳細については、「オプション項目」を参照

- ・ 「SMB パケット」をチェックする
- ・ 「WindowsAPI 取得」をチェックする。

C) 設定

オプション設定内容を反映する。

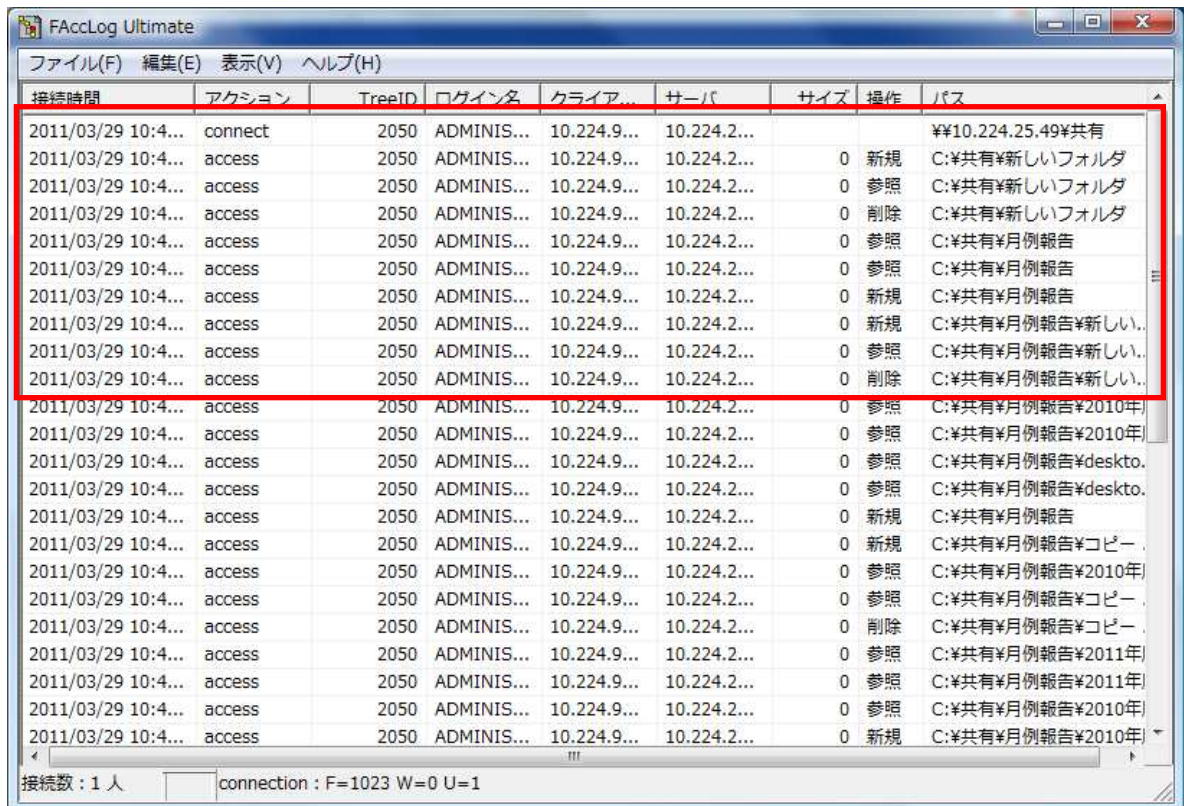
D) 設定内容を有効にするため、FAccLog Ultimate を再起動する。

メモ

オプション設定を変更した場合、変更内容を有効にするためには、FAccLogUltimate の再起動をしてください。

3. アクセスログの収集イメージ

A) アクセス情報がリストビュー画面にリアルタイムで表示される。



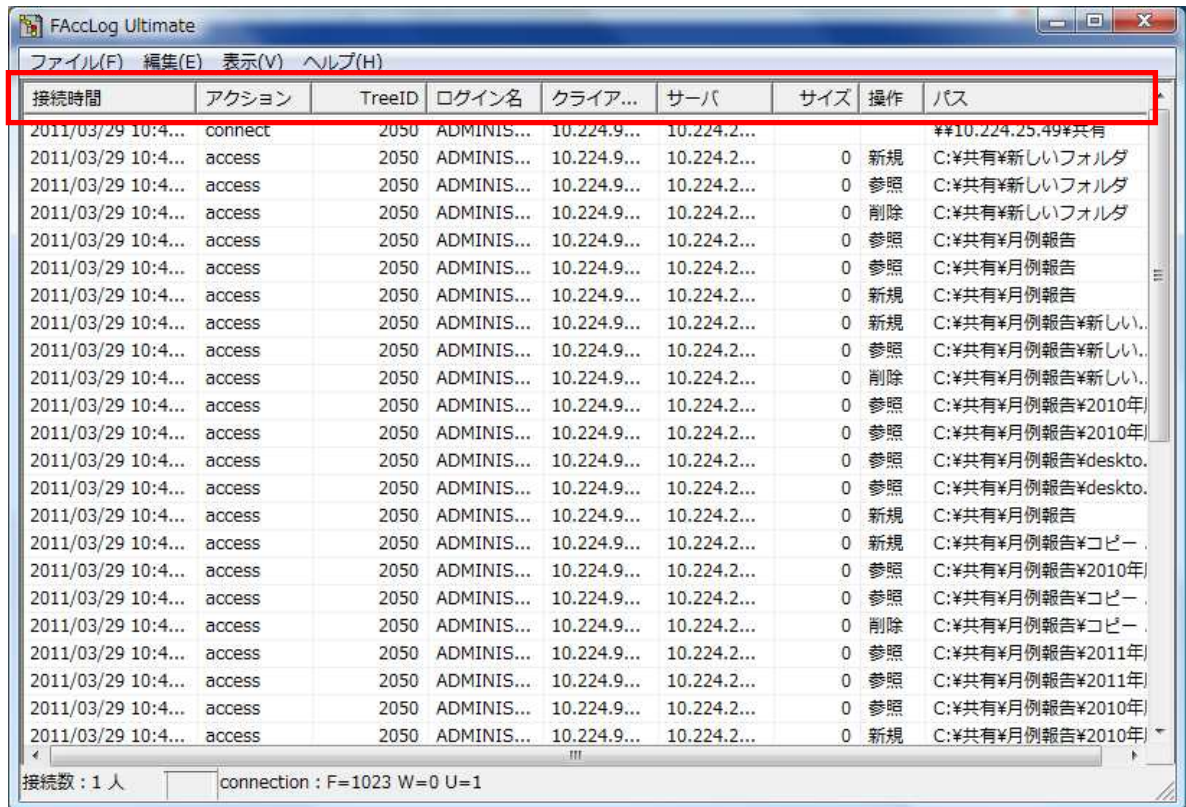
接続時間	アクション	TreeID	ログイン名	クライアント	サーバ	サイズ	操作	パス
2011/03/29 10:4...	connect	2050	ADMINIS...	10.224.9...	10.224.2...			¥¥10.224.25.49¥共有
2011/03/29 10:4...	access	2050	ADMINIS...	10.224.9...	10.224.2...	0	新規	C:¥共有¥新しいフォルダ
2011/03/29 10:4...	access	2050	ADMINIS...	10.224.9...	10.224.2...	0	参照	C:¥共有¥新しいフォルダ
2011/03/29 10:4...	access	2050	ADMINIS...	10.224.9...	10.224.2...	0	削除	C:¥共有¥新しいフォルダ
2011/03/29 10:4...	access	2050	ADMINIS...	10.224.9...	10.224.2...	0	参照	C:¥共有¥月例報告
2011/03/29 10:4...	access	2050	ADMINIS...	10.224.9...	10.224.2...	0	参照	C:¥共有¥月例報告
2011/03/29 10:4...	access	2050	ADMINIS...	10.224.9...	10.224.2...	0	新規	C:¥共有¥月例報告¥新しい..
2011/03/29 10:4...	access	2050	ADMINIS...	10.224.9...	10.224.2...	0	参照	C:¥共有¥月例報告¥新しい..
2011/03/29 10:4...	access	2050	ADMINIS...	10.224.9...	10.224.2...	0	削除	C:¥共有¥月例報告¥新しい..
2011/03/29 10:4...	access	2050	ADMINIS...	10.224.9...	10.224.2...	0	参照	C:¥共有¥月例報告¥2010年
2011/03/29 10:4...	access	2050	ADMINIS...	10.224.9...	10.224.2...	0	参照	C:¥共有¥月例報告¥2010年
2011/03/29 10:4...	access	2050	ADMINIS...	10.224.9...	10.224.2...	0	参照	C:¥共有¥月例報告¥deskto.
2011/03/29 10:4...	access	2050	ADMINIS...	10.224.9...	10.224.2...	0	参照	C:¥共有¥月例報告¥deskto.
2011/03/29 10:4...	access	2050	ADMINIS...	10.224.9...	10.224.2...	0	新規	C:¥共有¥月例報告
2011/03/29 10:4...	access	2050	ADMINIS...	10.224.9...	10.224.2...	0	新規	C:¥共有¥月例報告¥コピー
2011/03/29 10:4...	access	2050	ADMINIS...	10.224.9...	10.224.2...	0	参照	C:¥共有¥月例報告¥2010年
2011/03/29 10:4...	access	2050	ADMINIS...	10.224.9...	10.224.2...	0	参照	C:¥共有¥月例報告¥コピー
2011/03/29 10:4...	access	2050	ADMINIS...	10.224.9...	10.224.2...	0	削除	C:¥共有¥月例報告¥コピー
2011/03/29 10:4...	access	2050	ADMINIS...	10.224.9...	10.224.2...	0	参照	C:¥共有¥月例報告¥2011年
2011/03/29 10:4...	access	2050	ADMINIS...	10.224.9...	10.224.2...	0	参照	C:¥共有¥月例報告¥2011年
2011/03/29 10:4...	access	2050	ADMINIS...	10.224.9...	10.224.2...	0	参照	C:¥共有¥月例報告¥2010年
2011/03/29 10:4...	access	2050	ADMINIS...	10.224.9...	10.224.2...	0	新規	C:¥共有¥月例報告¥2010年

接続数 : 1 人 connection : F=1023 W=0 U=1

A)

アクセス情報のリスト項目説明

FAccLog Ultimate で使われているリスト項目の説明について記載します。



接続時間	アクション	TreeID	ログイン名	クライア...	サーバ	サイズ	操作	パス
2011/03/29 10:4...	connect	2050	ADMINIS...	10.224.9...	10.224.2...			##10.224.25.49#共有
2011/03/29 10:4...	access	2050	ADMINIS...	10.224.9...	10.224.2...	0	新規	C:\共有\新しいフォルダ
2011/03/29 10:4...	access	2050	ADMINIS...	10.224.9...	10.224.2...	0	参照	C:\共有\新しいフォルダ
2011/03/29 10:4...	access	2050	ADMINIS...	10.224.9...	10.224.2...	0	削除	C:\共有\新しいフォルダ
2011/03/29 10:4...	access	2050	ADMINIS...	10.224.9...	10.224.2...	0	参照	C:\共有\月例報告
2011/03/29 10:4...	access	2050	ADMINIS...	10.224.9...	10.224.2...	0	参照	C:\共有\月例報告
2011/03/29 10:4...	access	2050	ADMINIS...	10.224.9...	10.224.2...	0	新規	C:\共有\月例報告
2011/03/29 10:4...	access	2050	ADMINIS...	10.224.9...	10.224.2...	0	参照	C:\共有\月例報告\新しい...
2011/03/29 10:4...	access	2050	ADMINIS...	10.224.9...	10.224.2...	0	削除	C:\共有\月例報告\新しい...
2011/03/29 10:4...	access	2050	ADMINIS...	10.224.9...	10.224.2...	0	参照	C:\共有\月例報告\2010年...
2011/03/29 10:4...	access	2050	ADMINIS...	10.224.9...	10.224.2...	0	参照	C:\共有\月例報告\2010年...
2011/03/29 10:4...	access	2050	ADMINIS...	10.224.9...	10.224.2...	0	参照	C:\共有\月例報告\desкто...
2011/03/29 10:4...	access	2050	ADMINIS...	10.224.9...	10.224.2...	0	参照	C:\共有\月例報告\desкто...
2011/03/29 10:4...	access	2050	ADMINIS...	10.224.9...	10.224.2...	0	新規	C:\共有\月例報告
2011/03/29 10:4...	access	2050	ADMINIS...	10.224.9...	10.224.2...	0	新規	C:\共有\月例報告\コピー...
2011/03/29 10:4...	access	2050	ADMINIS...	10.224.9...	10.224.2...	0	参照	C:\共有\月例報告\2010年...
2011/03/29 10:4...	access	2050	ADMINIS...	10.224.9...	10.224.2...	0	参照	C:\共有\月例報告\コピー...
2011/03/29 10:4...	access	2050	ADMINIS...	10.224.9...	10.224.2...	0	削除	C:\共有\月例報告\コピー...
2011/03/29 10:4...	access	2050	ADMINIS...	10.224.9...	10.224.2...	0	参照	C:\共有\月例報告\2011年...
2011/03/29 10:4...	access	2050	ADMINIS...	10.224.9...	10.224.2...	0	参照	C:\共有\月例報告\2011年...
2011/03/29 10:4...	access	2050	ADMINIS...	10.224.9...	10.224.2...	0	参照	C:\共有\月例報告\2010年...
2011/03/29 10:4...	access	2050	ADMINIS...	10.224.9...	10.224.2...	0	新規	C:\共有\月例報告\2010年...

接続数: 1 人 connection : F=1023 W=0 U=1

接続時間

アクセスを行った日時

フォーマット : YYYY/MM/DD hh:mm:ss

YYYY 西暦
MM 月
DD 日
hh 時
mm 分
ss 秒

アクション

アクセスに対応するステータス情報

login セッション接続をした状態
connect 共有フォルダにアクセスした状態
access 共有フォルダ・共有ファイルに対してのアクセス
unknown TreeID の関連系が把握できないアクセス
disconnect アクセスした状態からセッション接続のみしている状態に移行した状態
logout セッション切断をした状態

TreeID

クライアント PC がファイルサーバへ接続を行ってからの一連の動作を追える管理番号

接続してからどのようなパスをたどったか、どのようなファイル操作を行ったかが、

この管理 ID から抽出可能です。

また、この TreeID はセッション単位で発行・管理されますので、1 台のクライアント PC がファイルサーバに対し複数フォルダを開いたり、多数アプリケーションから操作を行った場合であっても、それぞれの操作に一意の TreeID が付加されます。

クライアント

クライアント PC の IP アドレス、または、コンピュータ名

サーバ

ファイルサーバの IP アドレス、または、コンピュータ名

サイズ

アクセス対象のファイルサイズ

※フォルダは、「0 バイト」表示

パス

アクセス対象のパス名

※アクションが「unknown」の場合、無加工のまま SMB パケットのパス情報を表示

操作

アクセス形式





参照	フォルダ・ファイルに読み取り
書込	ファイルに書き込み
削除	フォルダ・ファイルを削除
改名	フォルダ・ファイルをリネーム
新規	フォルダ・ファイルの新規作成

メニュー項目の説明





FAccLog Ultimate で使われているメニュー項目の説明について記載する。設定内容をカスタマイズする場合には、内容をよく理解してご使用ください。

メインメニュー







1. 「ファイル(F)」

- 収集開始
 アクセス収集を開始する。
- 収集停止
 アクセス収集を停止する。
- FAL_hostsを読み込み
 FAL_hostsを読み込み。
- 終了
 FAccLog Ultimateを終了する。


2. 「編集(E)」

- 監視管理
 アクセスログの監視、及び、除外設定を行う。
- オプション
 オプション設定を行う。
- 初期設定に戻す
 オプション設定の内容を初期値に戻す。
- ライセンス登録
 ライセンス登録を行う。

3. 「表示(V)」


- ログ表示
 収集中のログファイル表示を行う。
- タスクトレイアイコン
 タスクトレイアイコンの常駐
 タスクトレイアイコンの削除
- タスクトレイに格納
 タスクトレイに格納し非表示にする。
- スクロールを最後尾に固定
 リスト表示を常に最後尾に固定する。
- 常に手前に表示
 ウインドのトップに配置する。

- 参照

-  リスト表示中のアクセスログを選択し、参照をクリックするとアクセスフォルダ、又はファイルを開くことができる。

4. 「ヘルプ(H)」

- アップデート

-  アップデート情報のサイトへ接続(インターネット)する。

- バージョン

-  バージョン情報、および、ライセンスキー表示をする。

オプションダイアログ

1. 「ログファイル名」

- 現在設定されているログファイル名

2. 「ログ指定場所」

- 現在設定されているログファイル名

3. 「監視対象 IP アドレス」

- アクセス収集を行いたい IP アドレス

4. 「更新時間」

- リスト表示されているアクセス情報を更新する最短時間

5. 「全パケット取得」

- SMB パケットとして流れるパイプファイルも検出を行う

6. 「エラーレベル」

- 0 … 重要なエラーのみ出力
- 1 … チューニングに関わるエラーの出力
- 2 … すべてのエラーを出力

7. 「アクセス検出方法」

- SMB パケット取得 … SMB パケットからのアクセス情報取得
- WindowsAPI 取得 … WindowsAPI からのアクセス情報取得

※ご使用環境に問題がなければ、2つの設定をブレンドした形でご使用ください。

8. 「ログファイルの取得」

- 収集ログをファイルに出力

9. 「ログファイルの切替」

- 収集ログファイルをアプリケーションの起動ごとに切り替える

10. 「条件追加:切替えサイズ」

- 収集ログファイルが指定されたサイズに達した時点でファイルを切り替える

11. 「条件追加:切替え日付幅」

- 収集ログファイルが指定された日付ごとにファイルを切り替える

12. 「起動時に隠す」

- 「FAccLog Ultimate」を起動時にタスクトレイに格納する

13. 「起動時に隠す」

- 「FAccLog Ultimate」を起動時にタスクトレイにアイコンを常駐する

14. 「起動と同時に収集を開始する」

- 「FAccLog Ultimate」を起動同時に「収集開始」を行う

15. 「ホスト名変換」

- リスト表示・アクセスログの IP アドレス表示にホスト(コンピュータ)名を付与する

16. 「FAL Hosts 解決」

- アクセス収集、ホスト名変換時に使用する名前解決の予約を行う。

※ 名前解決ができない場合や独自の名前解決時に利用できます。

名前解決ができていないことを検出するには、エラーログに出力される

「IP アドレス変換失敗。NetWkSessionInfo[%d].sesi502_cname = xxxxxxx」の、

xxxxxx 部分のホスト(コンピュータ)名が解決できていないものです。

※ 起動時に自動的に FAL Hosts ファイルを読み込ませるには、

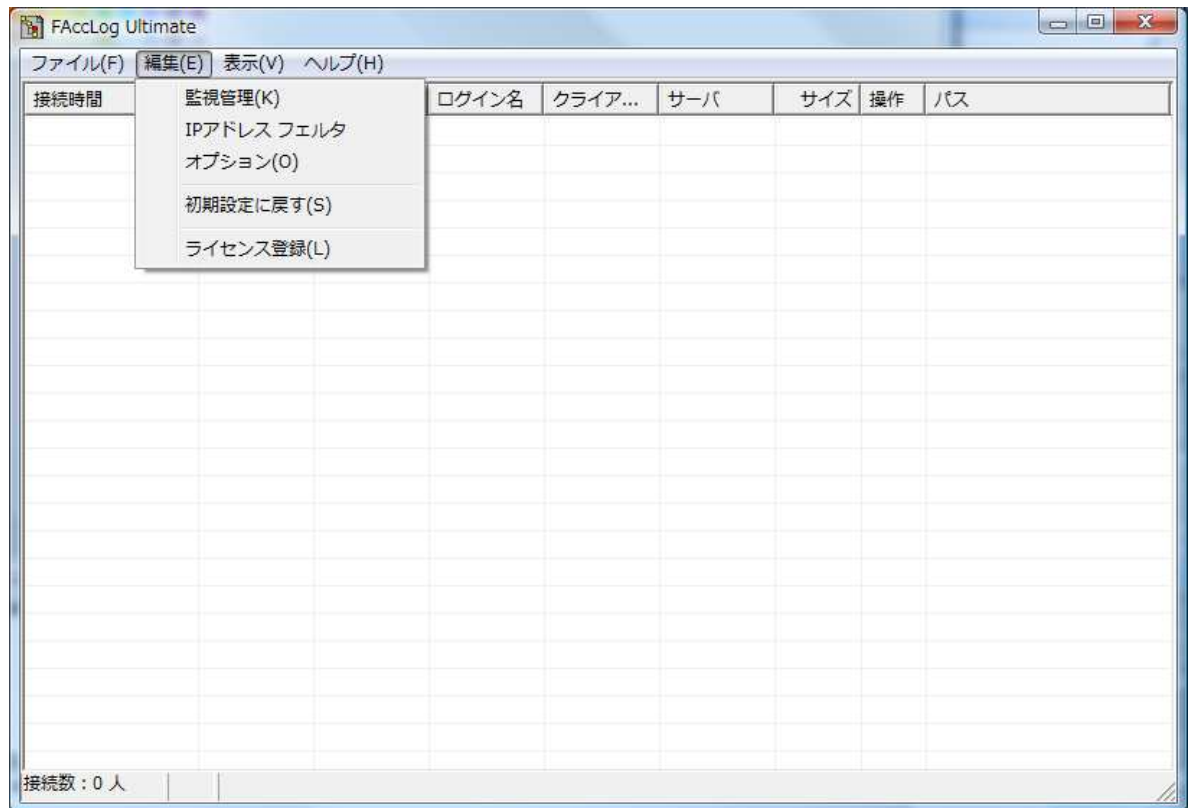
FAccLogUltimate 起動フォルダ内に「FAL_Hosts.hst」ファイル名で

FAL Hosts 定義を作成することで、「FAL Hosts 解決」オプションを有効した場合、

自動で定義ファイルを読み込ませることができます。

ライセンスキーの設定方法

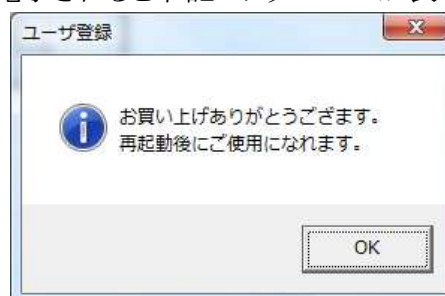
1. 「編集」メニューの「ライセンス登録」を選択する。



2. 「ユーザ登録」画面の入力ラインに、発行されたライセンスキーを入力する。



3. 「ユーザ登録」が正しく完了されると下記のメッセージが表示する。

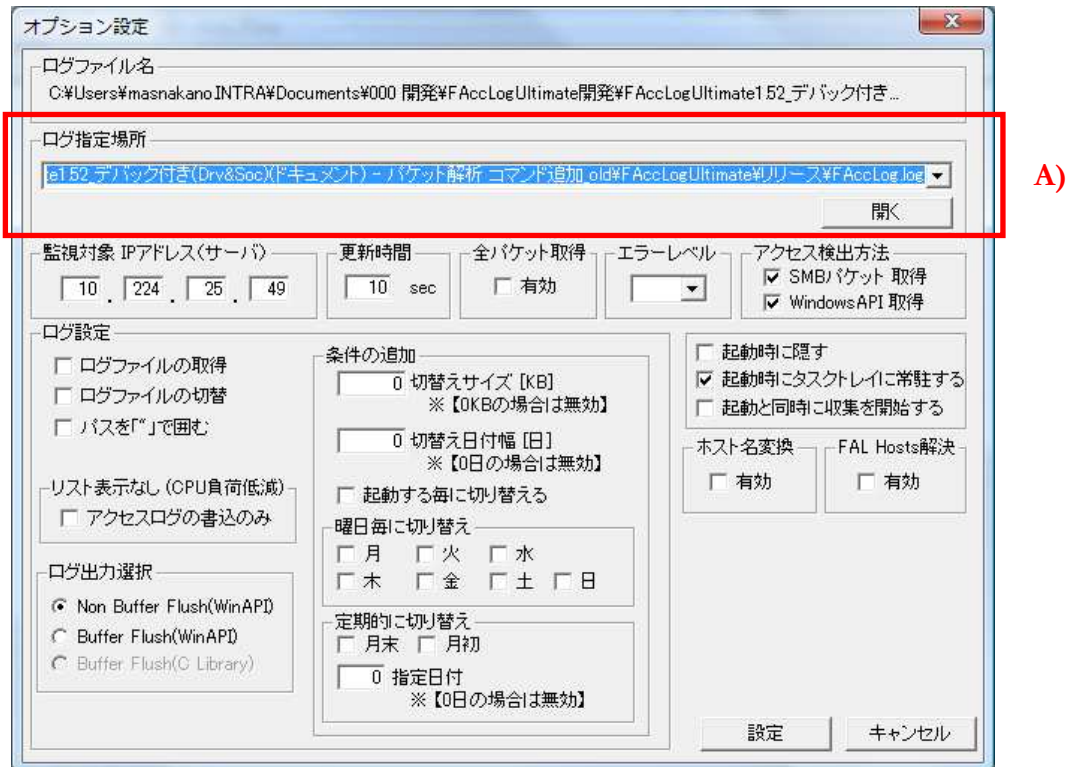


※ライセンスキーは、FAccLog を再起動した後に有効となる。

ログファイルへの収集方法

アクセスログの収集方法について

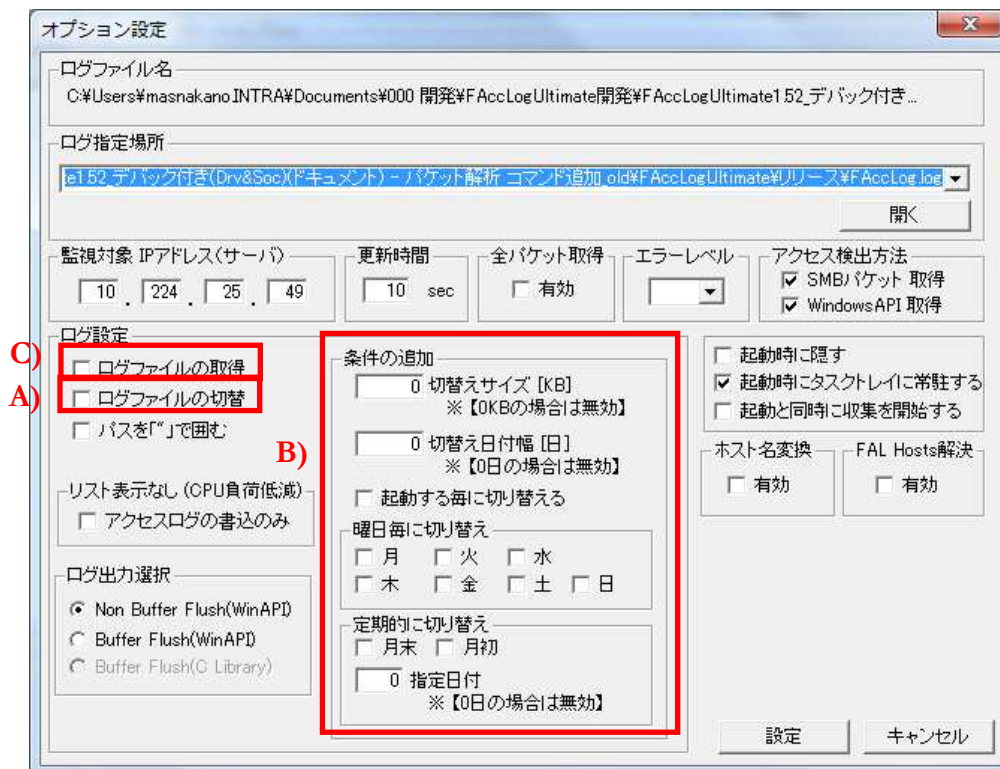
1. ログファイル出力先を指定する。



[編集] メニューの [オプション] を選択し、オプション画面を表示する。

A) 「ログ指定場所」にログファイルの出力先をフルパスで指定するか、又は、「開く」ボタンから GUI 形式で出力先を選択します。

2. ログファイル出力方法を設定する。



A) 「ログファイルの取得」にチェックを入れた場合、FAccLogUltimate の起動時にログファイルを切り替えて出力します。

B) 「ログファイルの切替」設定に切り替えタイミングの条件を追加します。

切替えサイズ … ログファイルが指定したサイズに満たした場合切り替える。

切替え日付幅 … 指定した日付ごとに切り替える。

起動する毎に切り替える … FAccLog を起動するタイミングで切り替える。

曜日毎に切り替える … 指定された曜日で切り替える。

定期的に切り替える … 月末、月初、指定日で切り替える。

C) 「ログファイルの取得」を有効にした場合、ログファイルの収集を行います。

メモ

条件の追加は、条件を満たしたもののから有効になります。

監視管理機能設定方法

監視管理には、「監視」、及び、「除外」から選択し、アクセスログの収集を制御できます。

監視管理の基準として、2つの観点があります。

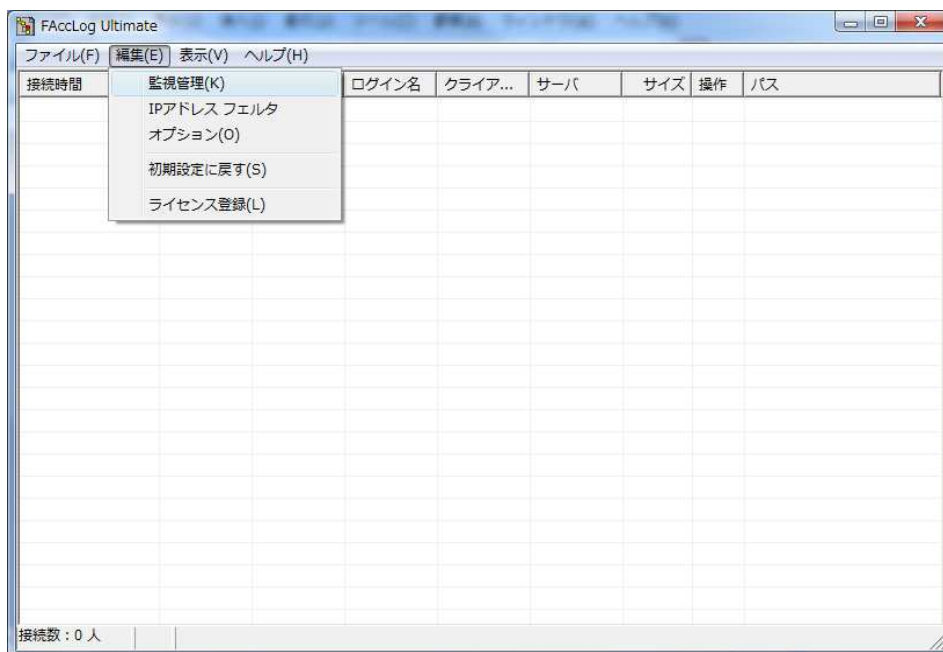
- 1) 共有フォルダを全て監視し、必要のないフォルダに対して監視を除外する。
- 2) 共有フォルダを全て除外し、必要なフォルダに対して監視する。

また、監視・除外のエントリは、混合できるが、優先順位として、

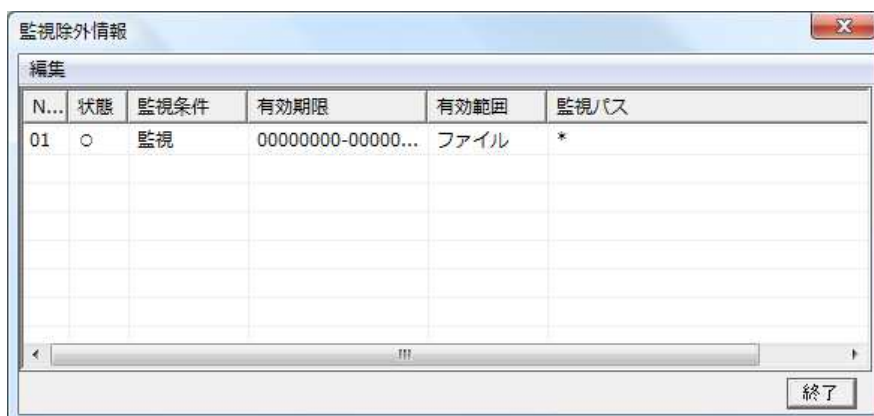
監視 < 除外

となるため、混合したエントリの追加は上記の優先順位を考慮して定義をしてください。

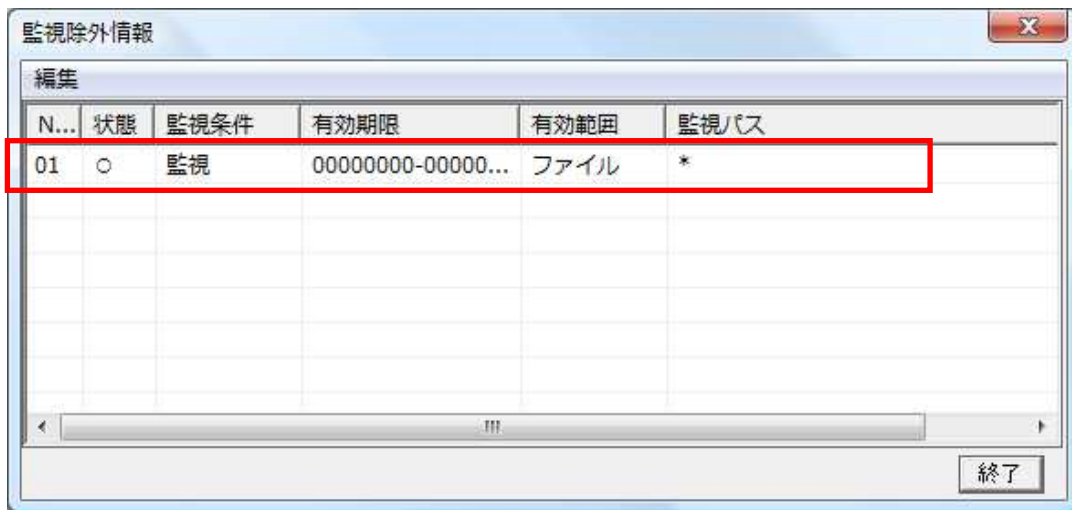
監視管理画面の表示



2. 「監視除外情報」画面の表示



監視除外情報の初期エントリについて



N...	状態	監視条件	有効期限	有効範囲	監視パス
01	○	監視	00000000-00000...	ファイル	*

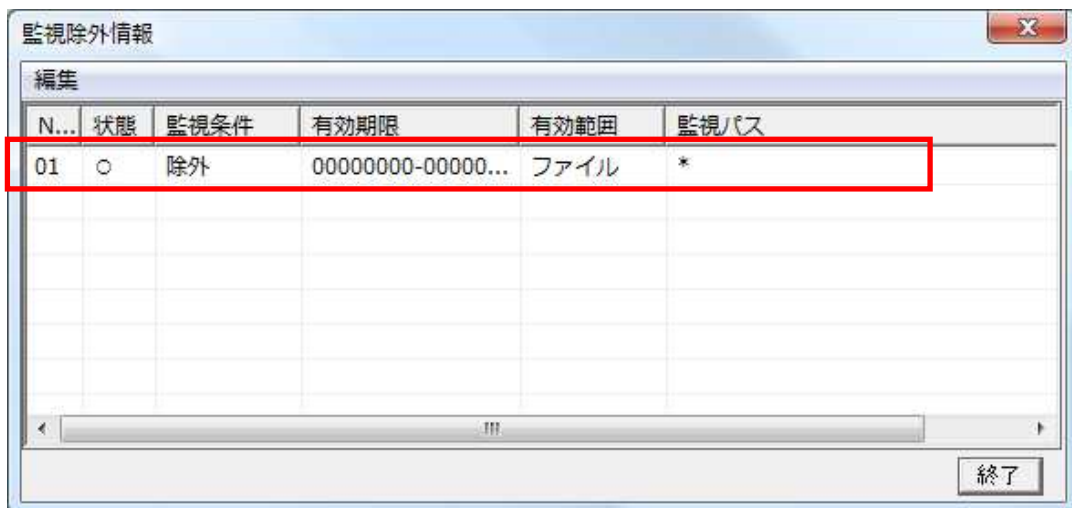
「監視除外情報」で、デフォルトで追加されているエントリが追加されています。

これは、監視管理の基準を、

「共有フォルダを全て監視し、必要のないフォルダに対して監視を除外する」
という定義になります。

また、この基準を

「共有フォルダを全て除外し、必要なフォルダに対して監視する」
する場合、下記のエントリに変更します。



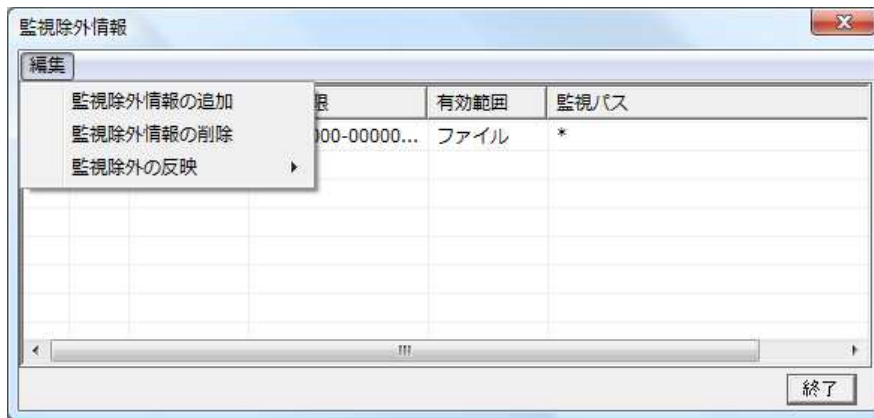
N...	状態	監視条件	有効期限	有効範囲	監視パス
01	○	除外	00000000-00000...	ファイル	*

監視管理の基準のエントリは、上記のどちらか1つの基準を必ず定義すること。

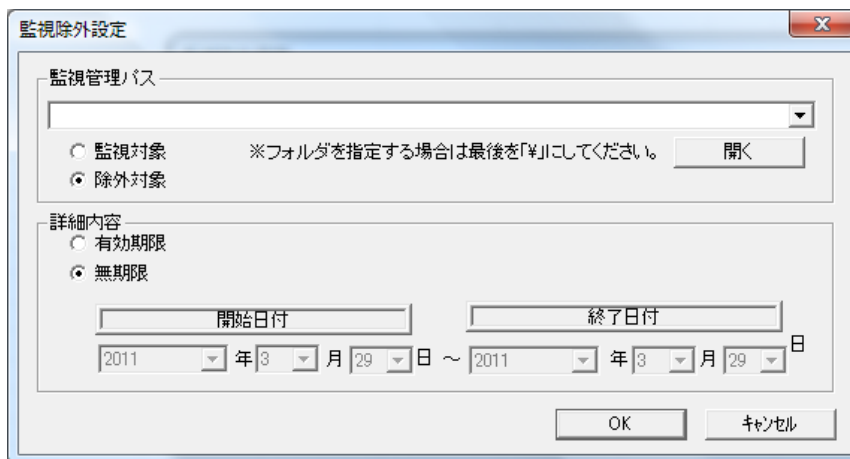
※ 追加方法については、下記の「監視除外情報の追加」で記載します。

監視除外情報の追加

1. 「監視管理画面」から「監視除外情報」の「監視除外情報の追加」を選択する。



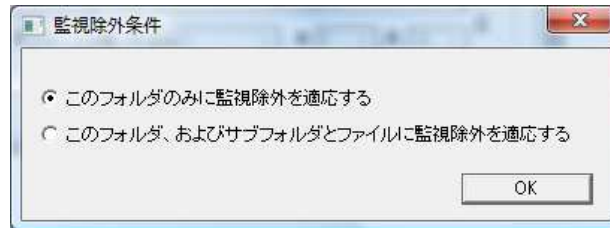
2. 「監視除外設定」から監視、あるいは、除外のエントリを追加する。



- 「監視管理パス」 … 監視、又は、除外対象のパス
- 「監視対象」 … 「監視管理パス」 に対しての監視を行う
- 「除外対象」 … 「監視管理パス」 に対しての除外を行う
- 「有効期間」 … 監視管理のエントリに対して設定が有効な期間を設定する。
- 「無期限」 … 監視管理のエントリに対して期限なしで有効とする。

△ 監視・除外パスのエントリ追加方法

- ◆ 「監視管理パス」 に監視、または、除外したいフルパスを記入する。
例) C:¥tools
- ◆ 監視管理の基準に従い 「監視対象」、又は、「除外対象」のどちらかを選択する。
- ◆ 「有効期限」、または「無期限」を選択する。
- ◆ 「監視管理パス」 に設定したパスがフォルダの場合、下記のどちらかを選択する。



- ・「このフォルダのみに監視除外を適応する」
… 指定したパス内のファイル・フォルダのみ監視・除外を行う設定。
- ・「このフォルダ、およびサブフォルダとファイルに監視除外を適応する」
… 指定したパス配下のファイル・フォルダすべての監視・除外を行う設定。

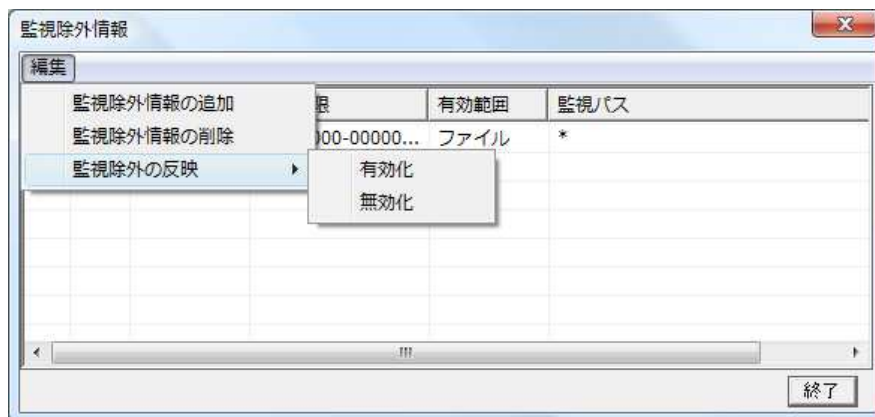
△ 監視管理の基準のエントリの追加方法について

- ◆ 「監視管理パス」は、「*」を記入する。
- ◆ 監視管理の基準に従い「監視対象」、又は、「除外対象」のどちらかを選択する。
- ◆ 「無期限」を選択する。

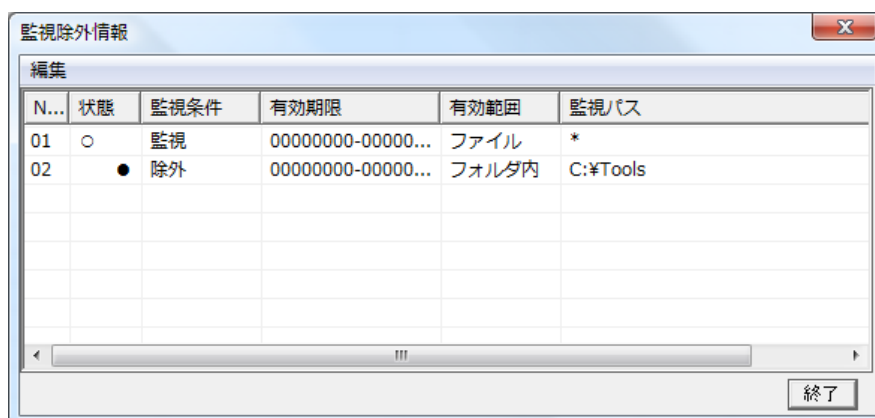
※ 監視管理の基準のエントリは、必ず1つどちらかを定義すること。

監視除外情報の有効化・無効化

エントリを追加した定義について、有効、または、無効化を行うことができる。



「監視管理画面」から「監視除外情報」の「監視除外の反映」から「有効化」または「無効化」を選択します。



N...	状態	監視条件	有効期限	有効範囲	監視パス
01	○	監視	00000000-00000...	ファイル	*
02	●	除外	00000000-00000...	フォルダ内	C:¥Tools

例では、No.02 エントリ定義を無効化したもので、
「状態」フィールドのアイコンが、「○」から「●」へ変化し、無効化されます。

エントリ定義の状態フィールドの詳細については下記に示す。

状態	意味
○	有効
●	無効
×	期限終了

FAL Hosts の設定方法

FAL Hosts とは、予約変換ホスト名を定義し、アクセス検出時に名前解決ができないエラーを回避でき、また、IP アドレスに関連付けた独自のコンピュータ名に変換が可能になります。

<フォーマット形式>

コンピュータ名, IP アドレス

定義例を下記に示す。

```
USER1, 192. 168. 1. 1  
USER2, 192. 168. 1. 2  
USER3, 192. 168. 1. 3
```

- 名前解決ができない場合のエラー回避方法として、
名前解決ができていないことを検出するには、エラーログに出力される
「IP アドレス変換失敗。NetWkSessionInfo[%d].sesi502_cname = xxxxxxx」の、
xxxxxx 部分のコンピュータ名を FAL Hosts 定義することで回避できます。
定義例を下記に示します。

エラーログ

```
IP アドレス変換失敗。NetWkSessionInfo[1].sesi502_cname = USER001  
IP アドレス変換失敗。NetWkSessionInfo[2].sesi502_cname = USER002  
:
```

エラーを回避するための定義内容

```
USER001, 192. 168. 1. 10  
USER002, 192. 168. 1. 20
```

※ 起動時に自動的に FAL Hosts ファイルを読み込ませるには

FAccLogUltimate 起動フォルダ内に「FAL_Hosts.hst」ファイル名で
FAL Hosts 定義を作成することで、「FAL Hosts 解決」オプションを有効した場合、
自動で定義ファイルを読み込ませることができます。

ini ファイルの隠し定義

FAccLog Ultimate に、特別な使用方法がある場合、FAccLog.ini にエントリを定義し、機能を有効にすることが可能です。

名前解決処理抑止機能

エラーログに「IP アドレス変換失敗」のメッセージが出力されている場合、FAL_Hosts で名前解決の予約をさせて回避させるが、名前解決処理自体を使用しないでエラーを回避するオプションです。

通常の名前解決処理を使った処理では、変換できなかった場合、タイムアウトを起こすまで、アクセスの収集が中断するため、取りこぼしが発生するが、FAL_Hosts 定義なしで回避するためのオプションです。

名前解決処理を行わない場合のデメリットとして、アクション定義「connect」「login」「logout」が、正しい順番、又は、表示(ログ出力)がされない場合があります。

ただし、「access」は正しいタイミングで表示(ログ出力)され、表示(ログ出力)されないことはありません。

定義「HostNameChg」

値 0:無効 1:有効

デフォルト 1

例) HostNameChg=0

多重ログ出力抑止機能

クライアントがアクセスを行った際、同様なアクションを繰り返すリトライ通信が発生した場合、表示(ログ出力)に重複して出力されます。

多重ログ出力を抑止する機能を有効とした場合、抑止す判断する範囲時間内に連続する出力に対して、表示(ログ出力)の抑止を行います。

多重ログ出力を抑止する機能を有効化

定義 1 「SameAccNonLogFlg」

値 0:無効 1:有効

デフォルト 0

多重ログ出力を抑止す判断する範囲時間(単位:ms)

定義 2 「SameAccNonLogTime」

値 0~3600000 (単位:ms)

デフォルト 5000

例) SameAccNonLogFlg=1

SameAccNonLogTime=5000

ログ出力形式

```
[2007/11/05 21:19:39],login,WAIT0,10.6.207.97,10.6.207.20,,¥¥HPDEVCL097¥TEST
[2007/11/05 21:20:00],connect,2049,10.6.207.97,10.6.207.20,,¥¥HPDEVCL097¥TEST
[2007/11/05 21:20:00],access,2049,10.6.207.97,10.6.207.20,参照,0,C:¥TEST
[2007/11/15 15:38:42],unconnected,2049,10.6.207.97,10.6.207.20,,¥¥10.6.207.20¥CTC
[2007/11/15 15:57:12],logout,2049,10.6.207.97,10.6.207.20,,¥¥10.6.207.20¥CTC
```

```
[2007/11/05 21:20:00],access,2049,10.6.207.97,10.6.207.20,参照,0,C:¥TEST,
      (1)          (2)  (3)      (4)          (5)      (6) (7)  (8)
```

- (1) … 接続日時
 [YYYY/MM/DD hh:mm:ss]
 YYYY … 西暦
 MM … 月
 DD … 日
 hh … 時
 mm … 分
 ss … 秒
- (2) … アクション
 login … セッション接続をした状態
 connect … 共有フォルダにアクセスした状態
 access … 共有フォルダ・共有ファイルに対してのアクセス
 unknown … TreeID の関連系が把握できないアクセス
 unconnect … アクセスした状態からセッション接続のみしている
 状態に移行した状態
 logout … セッション切断をした状態
- (3) … TreeID
 アクセスユーザがセッション接続してからの管理番号
 接続してからどのような経路や操作がこの管理 ID から抽出可能
- (4) … サーバ IP アドレス
- (5) … クライアント IP アドレス
- (6) … アクセス形式
 参照 … フォルダ・ファイルに読み取り
 書込 … ファイルに書き込み
 削除 … フォルダ・ファイルを削除
 改名 … フォルダ・ファイルをリネーム

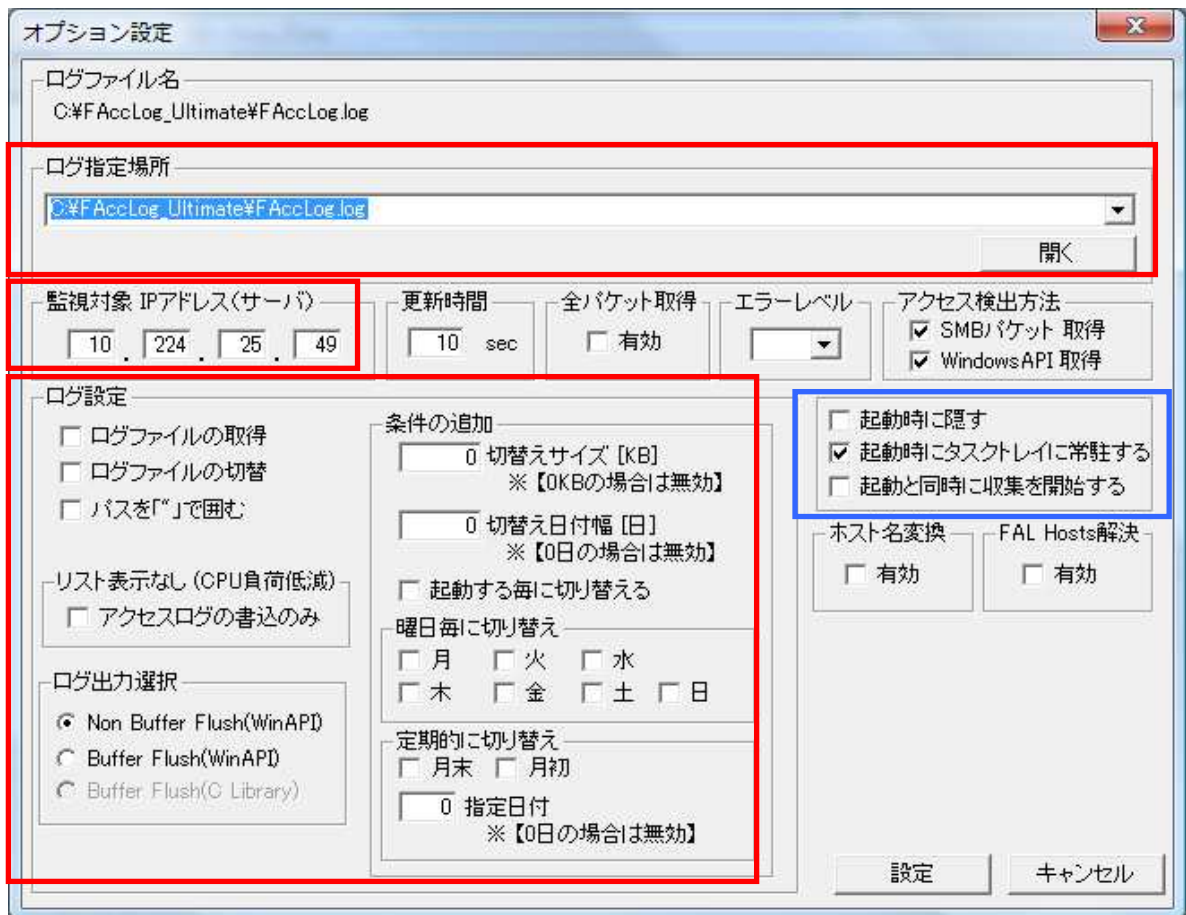
- (7) … ファイルサイズ
ディレクトリは「0 バイト」
- (8) … アクセスパス
ファイルサーバに対してのフルパス
「unknown」の場合、SMB パケットのアクセスパスをそのまま出力

エラーログ

- ・ 「[FAccLog 実行フォルダ]¥FALkernel」 配下に動作ログが出力される。
出力形式) FALkernelxx.log
xx … 秒数

サービスの登録方法

FAccLogUltimate を、サービス起動するには、FAccLogUltimate のオプション設定で、自動起動設定を行う必要があります、サービスで起動されたときに自動的にアクセス収集を行えるようにしなければなりません。



設定方法としては、FAccLogUltimate のオプション設定から赤枠で囲まれた部分の設定、及び、青枠内のチェック項目を

- ・「起動時に隠す」
- ・「起動時にタスクトレイに常駐する」
- ・「起動と同時に収集を開始する」

にチェックを入れ有効にする。

※事前に起動と同時にアクセス収集が行われるか動作確認をすることをお勧めします。

自動起動の設定が完了したのち、サービス登録を行う。サービス登録には、サービス登録アプリケーション「FAccLogServiceSet.」を起動後、下記の設定をし実行します。



A) プログラムの場所(N)

B) 起動時のオプション(O)

C) サービス名(S)

D) 終了方法(E)

E) オプション設定

F) 起動・削除

- A) 「プログラムの場所」に FAccLogUltimate.exe を配置した箇所を指定する。
- B) 「起動時のオプション」に「SC」を指定する。
- C) 「サービス名」に Windows のサービスに登録されるサービス名を指定する。
- D) 「終了方法」に「WM_SYSCOMMAND→WM_CLOSE」を指定する。
- E) 「オプション設定」に「自動起動」をチェック、及び、「デスクトップとの対話を許可」にチェックをする。
- F) 最後に「起動・削除」で設定した内容の動作チェックを行い、サービスから FAccLogUltimate が起動することを確認する。

NIC が2枚以上ある場合の設定方法

アクセス監視対象の NIC を複数ある場合や IP アドレスが複数ある場合、
「FAccLog Ultimate」は、複数起動させることで、アクセス収集が可能です。

別のフォルダへインストール、または、事前にインストールされているフォルダを複製し、
アクセスを監視したい個数分インストールします。

このとき、フォルダをコピーする場合は、コピー先フォルダの「FAccLog.ini」ファイルを削除し
てください。

複製後は、それぞれの「FAccLog Ultimate」を起動し、オプション設定を対応した IP アドレス
に設定してください。

また、ログ出力先は、同一のログ出力先とならないように設定をしてください。

メッセージ一覧

メッセージコード	レベル	メッセージ
FAL_I01-001	Information	FAccLog Ultimate を起動します。
FAL_I01-002	Information	FAccLog Ultimate を終了しました。
FAL_E02-001	Error	起動位置のパス取得に失敗。
FAL_E02-002	Error	ini ファイル読み込み失敗。
FAL_E02-003	Error	ログファイル設定失敗。LogPathBuf=%s
FAL_E02-004	Error	リスト表示設定失敗。
FAL_E02-005	Error	監視監視ファイル読み込み失敗。NorInfoFilePath=%s
FAL_I02-001	Information	自動起動フラグ ON。
FAL_E03-001	Error	ソケットの生成失敗。
FAL_E03-002	Error	ログスレッドの生成処理起動作成失敗。
FAL_E04-001	Error	TreeID 管理の空き領域がありません。
FAL_E05-001	Error	IP アドレス変換失敗。 NetWkSessionInfo[%d].sesi502_cname = %s
FAL_E05-002	Error	TreeConnect Info Delete error. TreeID = %s
FAL_E06-001	Error	TreeID が一致するデータがありません。TreeID = %d
FAL_E07-001	Error	NetShareEnum buf error.
FAL_E08-001	Error	NetFileEnum buf error.
FAL_E09-001	Error	NetSessionEnum buf error.
FAL_E10-001	Error	ログファイルのサイズ取得失敗。
FAL_I10-001	Information	ログファイルのサイズ切り替え。
FAL_I10-002	Information	ログファイルの日付け切り替え。

バグ、問題点、改善点

※不具合等でご連絡をくださる際に

- ・不具合の内容
- ・使用していたバージョン
- ・最後に行った操作
- ・イベントログ ... など、

調査で役立つ情報があれば大変助かります

ご使用にあたって

本プログラムはシェアウェアです。

ライセンス未購入でも1ヶ月間試用できます

免責等

- ・本プログラムはシェアウェアです。
- ・こちらで用意したアーカイブ形式でのみ再配布可能です。
Web、雑誌への紹介、CD-ROMに収録する場合は必ず連絡してください。
- ・作者はプログラムの完全な動作を保証する物ではありません。
- ・本プログラムを使用した上で生じたいかなる損害についても、製作者は一切の責任を負いません。
- ・プログラムの著作権は、「だいこくネット 中野 真良」が保有します。
- ・ライセンス発行者に使用を認めるもので、第三者へ転売は認めません。
- ・動作保証や将来的な機能拡張を保証するものではありません。
- ・バグを発見した場合の問題対処はその都度行いますが、すべてのバグに対処は行いません。
報告していただいた内容は率直に受け止め、更なる動作の安定、より良い機能を追加していきます。
- ・最新版およびお知らせはこちらから。
http://www2s.biglobe.ne.jp/~masa-nak/fal_down.htm
- ・バグ、問題点、改善点などありましたら、こちらまで。
daikoku@kss.biglobe.ne.jp
ご質問の内容によりご回答までにお時間を要することがございます。
- ・追加機能やカスタマイズについてはご相談にのります。
- ・安心してお使いいただくために、トラブルシューティング、障害切り分け、操作説明などをはじめ、充実したメンテナンスサポートについては別途ご相談にのります。

著作権と使用範囲

FAccLog Ultimate の著作権は、だいこくネットに帰属します。