11　プロセス監視

11.1 プロセス監視機能について

11.1.1 プロセス監視機能概要

プロセス監視は、クライアント上のプロセス(アプリケーション)の起動や終了を遠隔地にあるリモートマシン上から監視する機能です。このプロセス監視は、次の機能を実現しています。

- プロセスロギング機能
- プロセス状態表示機能
- コマンド実行機能
- 不正プロセスアラート通知機能

プロセス監視機能は、プロセス情報を収集するクライアントと、プロセス状態やプロセス起動終了ログを表示するGUIで構成しています。GUIは、ESMPRO統合ビューア(オペレーションウインドウ)又は、ESMPRO/CM データビューアから起動します。

11.1.2 プロセスロギング機能

プロセスロギング機能は、クライアント上で指定したプロセスの起動・終了履歴をログファイルとして記録し、遠隔地にあるGUIで表示する機能です。

ログを採取するプロセスの指定は、SG設定により行います。

11.1.3 プロセス状態表示機能

プロセス状態表示機能は、クライアント上で動作しているプロセスの状態(プロセス名／プロセスID／CPU使用時間)を一定間隔で表示する機能です。

11.1.4 コマンド実行機能

コマンド実行機能は、GUIからアプリケーション名を指定しクライアントPC上でアプリケーションを実行する機能です。

11.1.5 不正プロセスアラート通知機能

不正プロセスアラート通知機能は、クライアント上で不正なプロセスの動作をマネージャにアラートで通知する機能です。

不正なプロセスの動作は、履歴をアラートログに記録します。

不正なプロセスとは、プロセス監視機能のSGに登録されていないプロセスです。
アラート通知をしない設定でもアラートログには不正なプロセスの動作履歴が記録されます。

11.1.6 プロセス監視の実行手順

プロセス監視機能の実行手順は以下になります。
プロセス状態表示機能、コマンド実行機能を使用するには。

- データビューアからクライアントのプロセス監視機能を有効にします。
  「11.2 プロセス監視機能を有効にするには」を参照してください。
- オペレーションウインドウ、又はデータビューアからプロセス監視GUIを起動します。
  「11.3 プロセス監視GUIの起動」を参照してください。
- プロセス状態表示は、プロセス監視GUIが起動すると表示されます。
  「11.5 プロセス状態表示機能」を参照してください。
- コマンド実行は、プロセス監視GUIの「ツール」メニューから実行します。
  「11.6 コマンド実行機能」を参照してください。

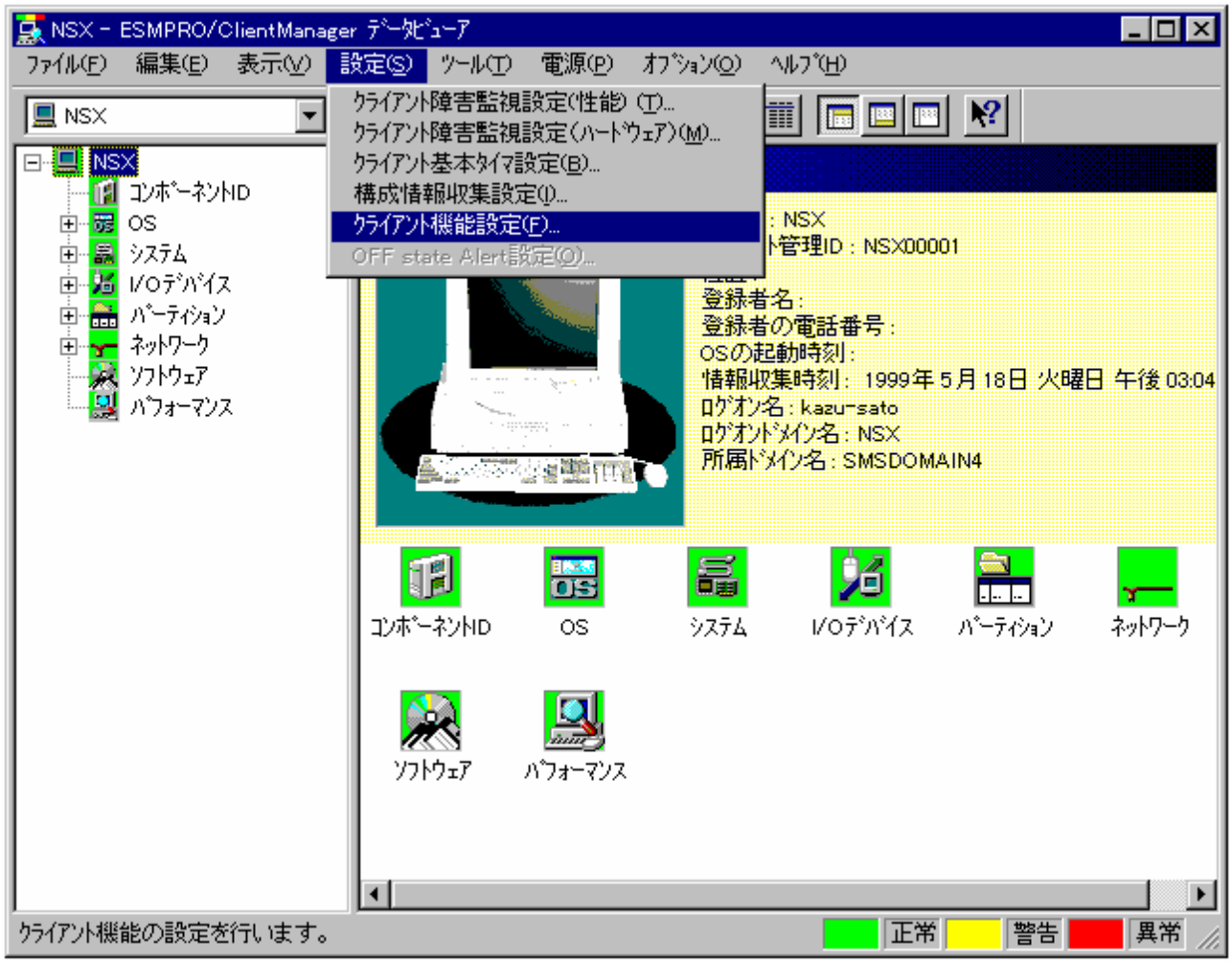
プロセスロギング機能、不正プロセスアラート通知機能を使用するには。

- マネージャ、又はクライアントでSG値を設定します。
  「11.8 SG設定」を参照してください。
- マネージャでSGファイルを設定した場合は、クライアントへ配布します。
  「11.8 SG設定」を参照してください。
- データビューアからクライアントのプロセス監視機能を有効にします。
  「11.2 プロセス監視機能を有効にするには」を参照してください。
- オペレーションウインドウ、又はデータビューアからプロセス監視GUIを起動します。
  「11.3 プロセス監視GUIの起動」を参照してください。
- ログ表示は、プロセス監視GUIの「ファイル」メニューから実行します。
  「11.4.2 ログ表示」を参照してください。

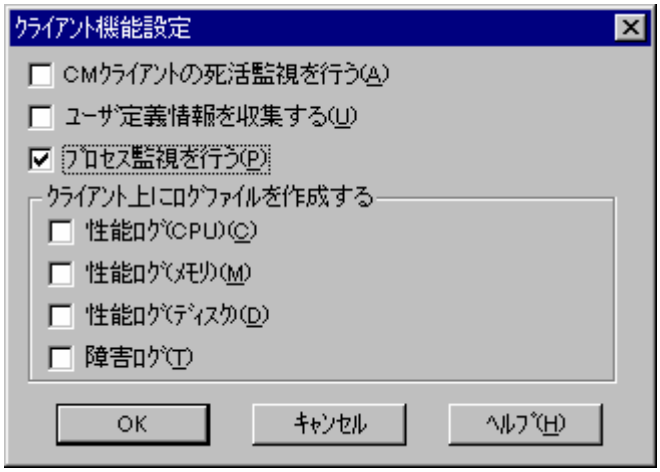
注意：プロセスロギング機能、不正プロセスアラート通知機能を使用する場合は、プロセス監視機能を有効にする前にクライアントのSGファイルにプロセスの一覧を設定するか、又はマネージャでプロセスの一覧を設定したSGファイルをクライアントにコピーしてください。

11.2 プロセス監視機能を有効にするには

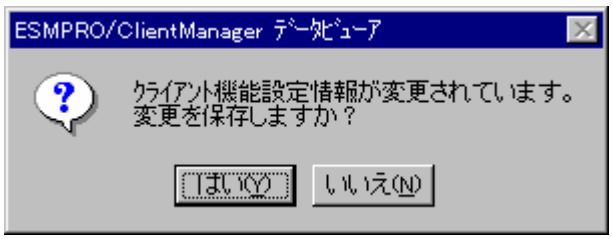
プロセス監視機能を有効にするには、CMデータビューアのメニューから設定します。
インストール直後はプロセス監視機能は無効に設定されています。



CMデータビューアの「設定」メニューから「クライアント機能設定」を選択し「クライアント機能設定」ダイアログを表示します。



「クライアント機能設定」ダイアログの「プロセス監視を行う」チェックボックスをチェックし＜OK＞ボタンを押します。



「クライアント機能設定情報が変更されています。変更を保存しますか？」メッセージボックスで＜はい＞ボタンを押します。

「クライアント機能情報は正常に保存されました。」メッセージボックスで＜OK＞ボタン押します。

以上の操作でクライアント上でプロセス監視機能が有効になります。

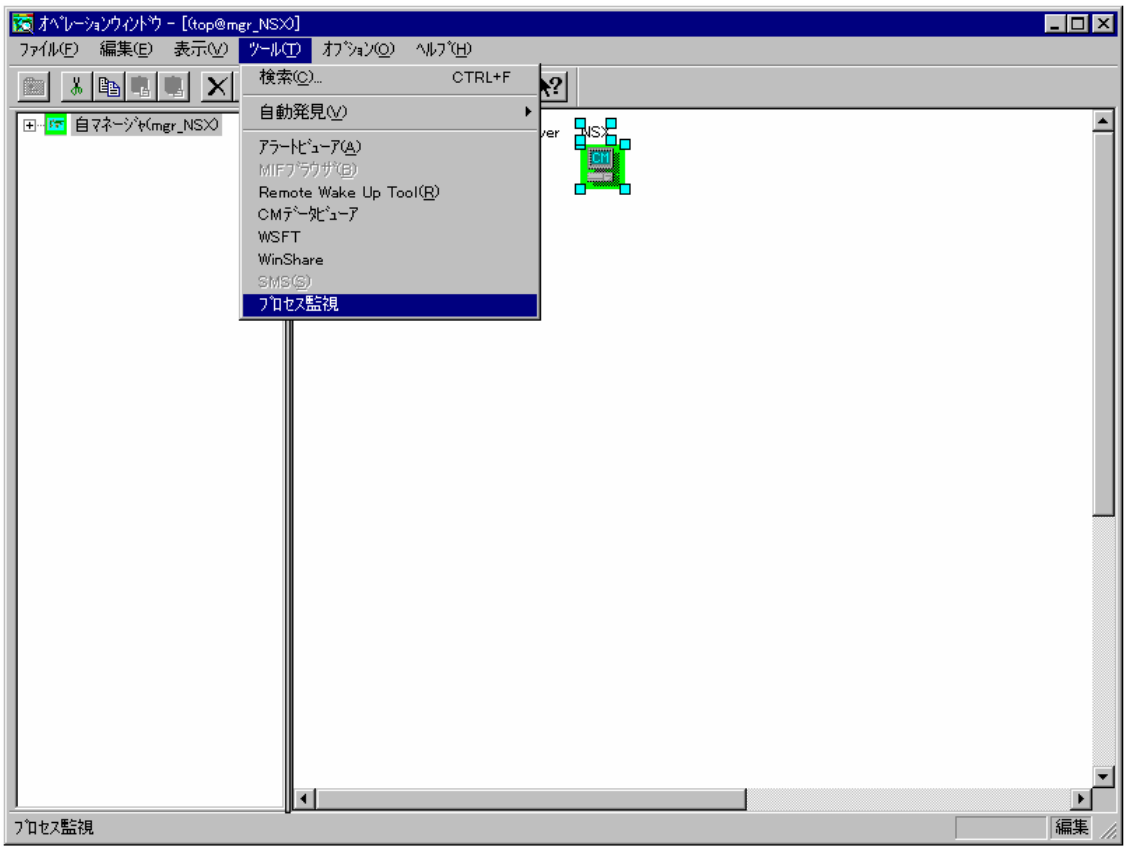
「クライアント機能設定」ダイアログの「プロセス監視を行う」チェックボックスをチェックしないでクライアント機能の設定をするとプロセス監視機能は無効になります。

「プロセス監視を行う」チェックボックスがチェックされているクライアントは、PC起動時からプロセス監視が有効になります。

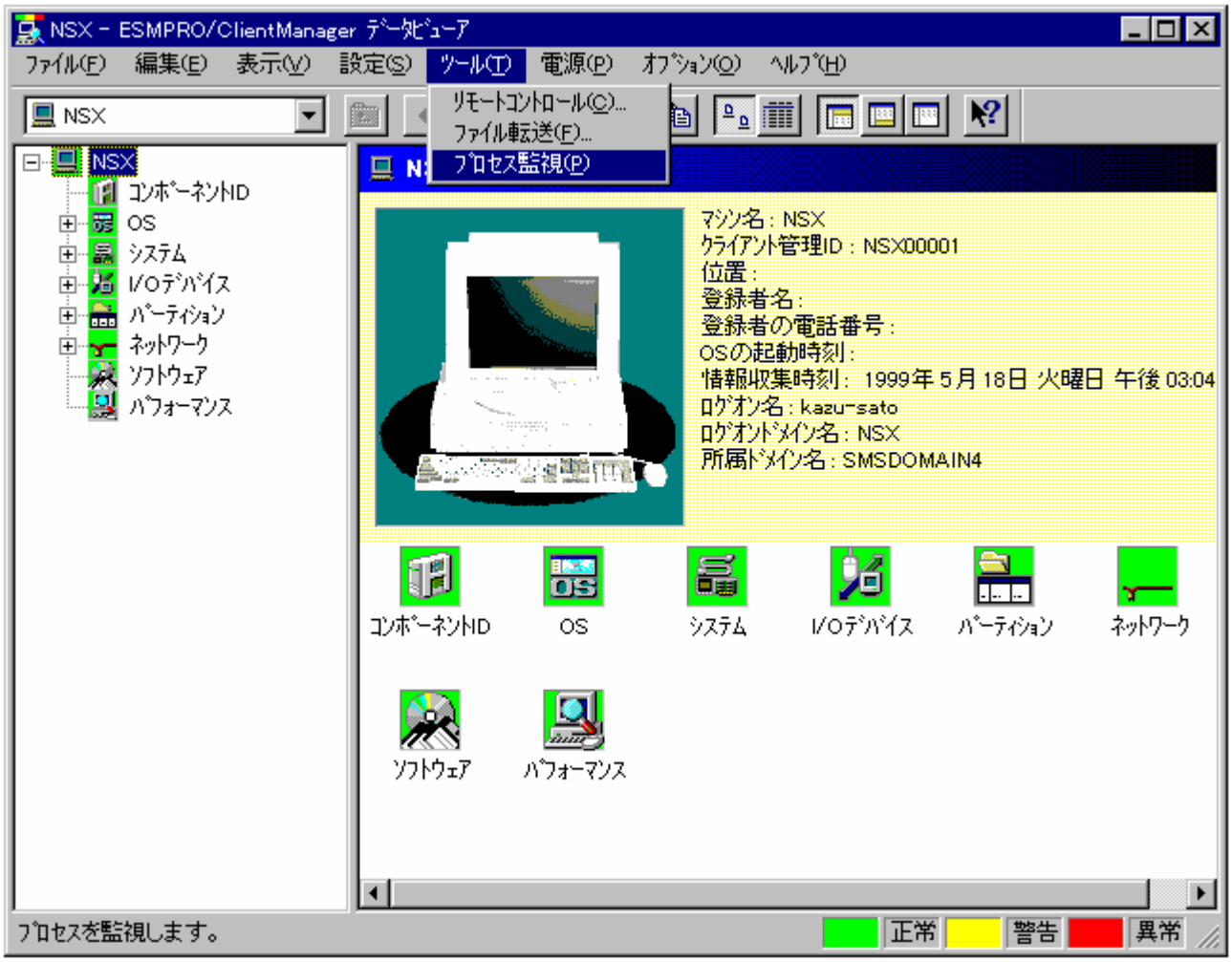
プロセス監視機能を無効にする場合はプロセス監視GUIを終了させてから行ってください。

11.3 プロセス監視 GUI の起動

プロセス監視GUIは、ESMPRO統合ビューア、又はCMデータビューアから起動します。



クライアントのプロセス監視機能を有効にしてからオペレーションウインドウ上にあるアイコンを選択状態にしたのち、「ツール」メニューから「プロセス監視」を選択してプロセス監視GUIを起動します。



又は、プロセス監視機能を有効にしてからCMデータビューアの「ツール」メニューから「プロセス監視」を選択してプロセス監視GUIを起動します。

11.4 プロセスロギング機能

プロセスロギング機能は、各クライアントで動作するプロセス（アプリケーション）の起動、終了をログに記録し管理する機能です。

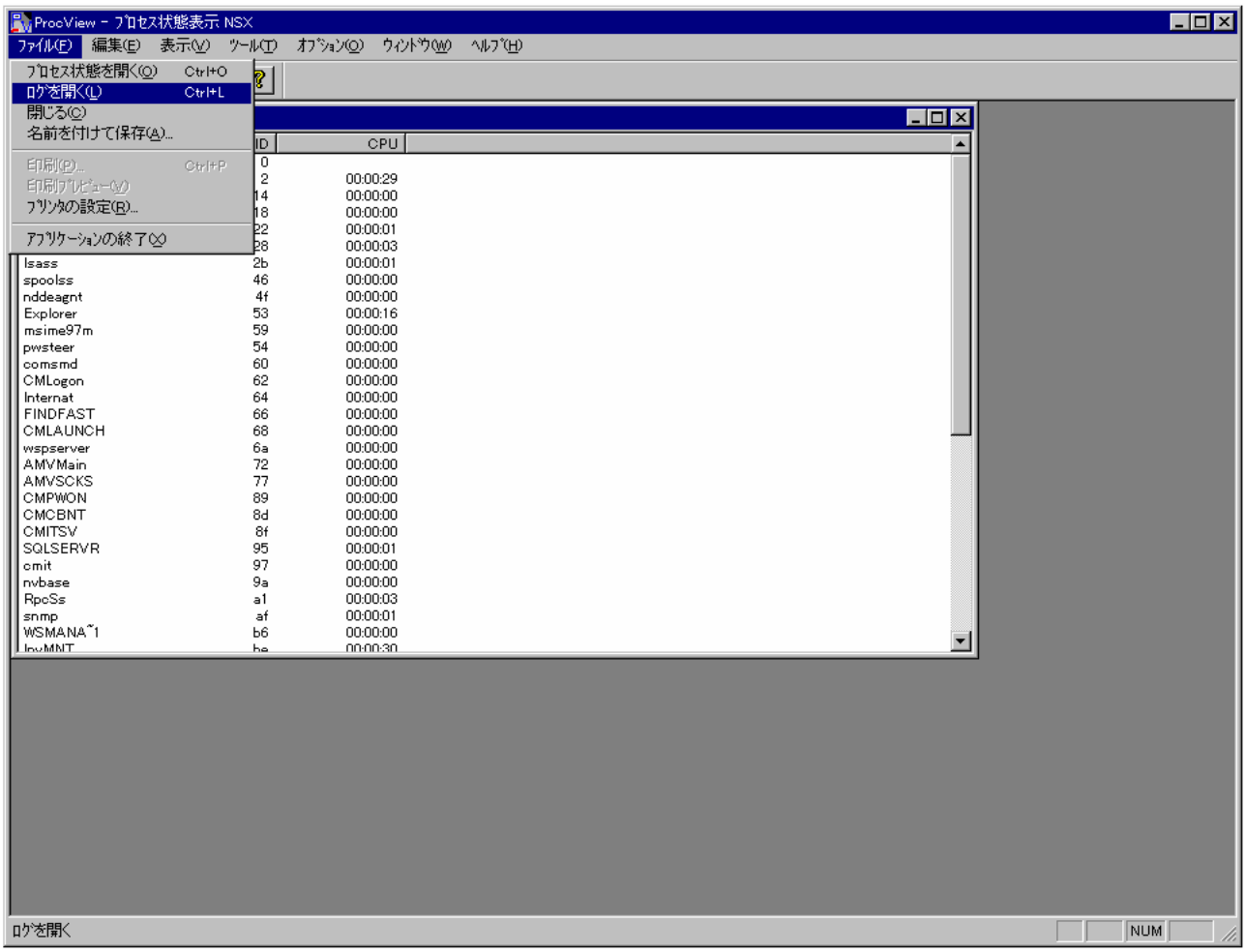
11.4.1 ログ設定

プロセスログを記録するには、プロセス監視のSGファイルに監視対象のプロセスを登録する必要があります。

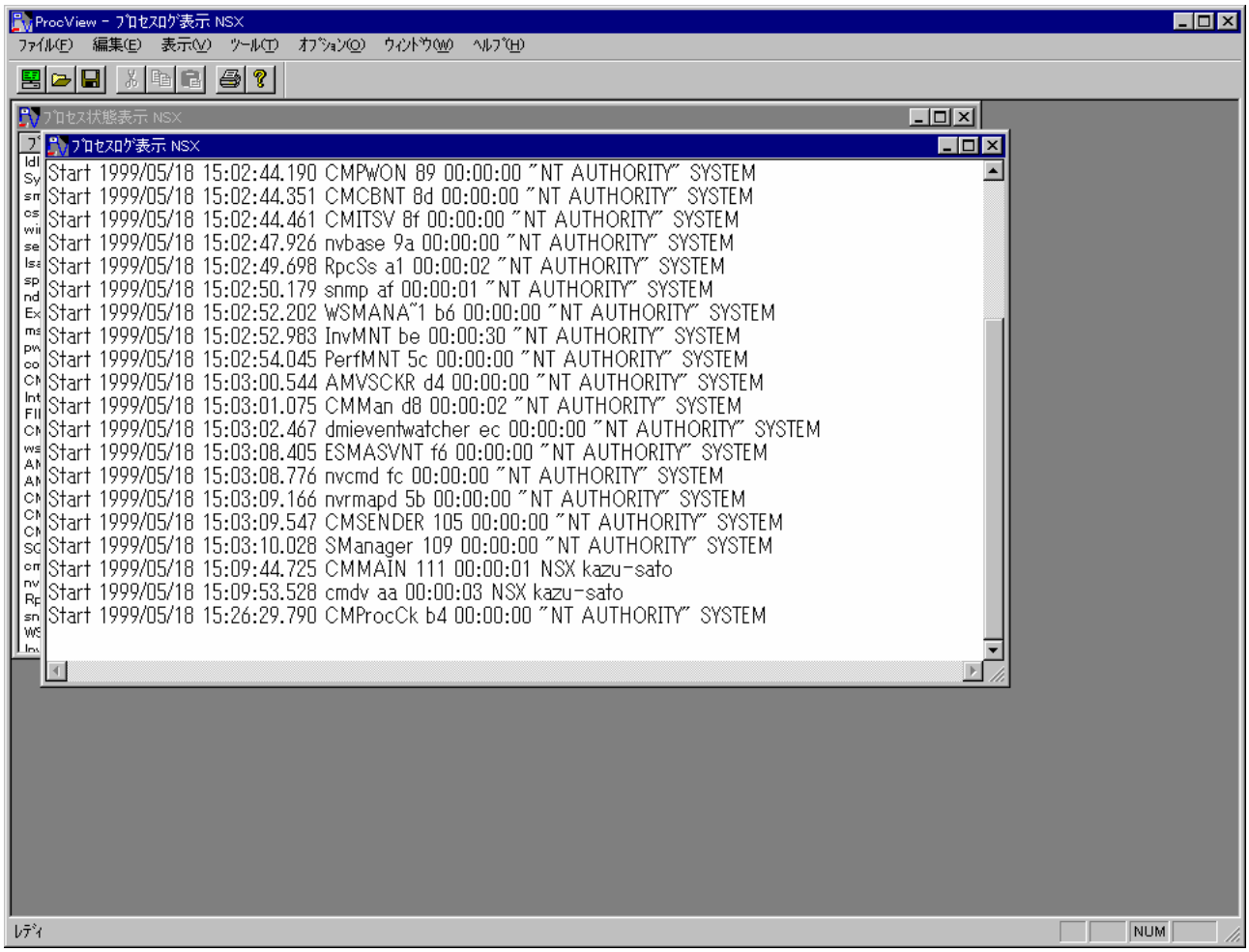
ログの設定は、クライアント、又はマネージャ上の「スタート」メニューから「プログラム」－「ESMPRO_CM」－「プロセス監視SG設定」を選択し「プロセス監視設定」ダイアログ起動し行います。「プロセス監視設定」ダイアログの使用方法については、「１２．８ SG設定」を参照してください。

11.4.2 ログ表示

ログ表示は、クライアント上で記録しているプロセスログを表示する機能です。



プロセスログの表示は、プロセス監視GUIの「ファイル」メニューから「ログを開く」を選択して表示します。



表示したプロセスログは、テキストファイルにセーブあるいは印刷が可能です。

テキストファイルにセーブするには、「ファイル」メニューの「名前を付けて保存」を選択し実行します。

印刷するには、「ファイル」メニューの「印刷」を選択し実行します。

注意：プロセスログをテキストファイルにセーブする際は、必ずファイル名を変更するかディレクトリを変更してセーブしてください。

11.4.3 ログ形式

ログの形式は、プロセスログとアラートログで共通の形式です。
ログ形式は、以下の通りです。

```
Action 年月日 時刻 ProcName PID CPU使用時間 DomainName UserName
```

各項目について以下に説明します。

*** Action**

プロセスの動作を記録します。プロセスの動作は、次の通りです。

Start	起動
End	終了

*** 年月日**

プロセスが起動・終了した年月日をyyyy/mm/ddの形式で記録します。

yyyy	西暦
mm	月
dd	日

クライアントOSがWindows95又はWindows98の場合は、正確な起動、終了の年月日で記録されません。プロセス監視機能が監視タイミングで検出した時の年月日で記録します。

*** 時刻**

プロセスが起動・終了した時刻をHH:MM:SS.mmmの形式で記録します。

HH	時刻
MM	分
SS	秒
mmm	ミリ秒

クライアントOSがWindows95又はWindows98の場合は、正確な起動、終了の時刻で記録されません。プロセス監視機能が監視タイミングで検出した時の時刻で記録します。

*** ProcName**

プロセス名を記録します。

*** PID**

プロセスIDを記録します。(16進数表示)

*** CPU使用時間**

プロセスが使用したCPU時間をHH:MM:SSの形式で記録します。

HH	時
MM	分
SS	秒

クライアントOS がWindows NTの時に記録します。

* DomainName

プロセスを起動・終了したユーザが属するドメイン名を記録します。ユーザがドメインにログオンしていない場合(ワークグループで使用している場合)は、ワークグループ名を記録します。

サービスプログラムのうちシステムアカウントで起動しているプロセスは、[NT AUTHORITY]となります。

クライアントOS がWindows NTの時に記録します。

* UserName

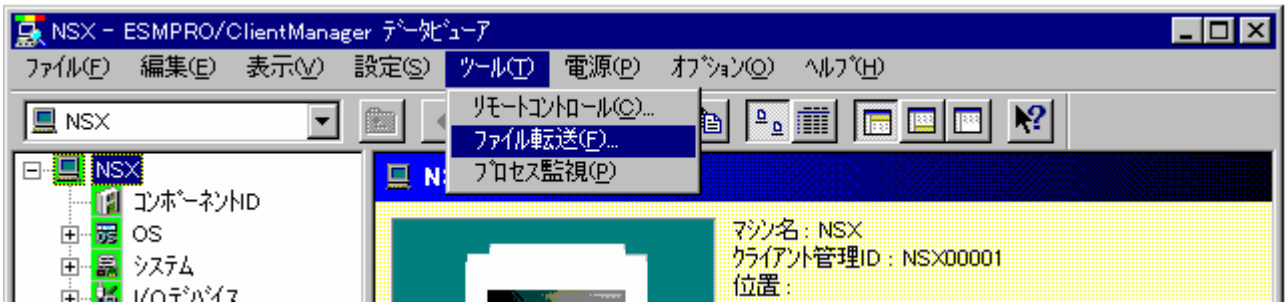
プロセスを起動・終了したユーザ名を記録します。

サービスプログラムのうちシステムアカウントで起動しているプロセスは、[SYSTEM]となります。

クライアントOS がWindows NTの時に記録します。

11.4.4 ログファイルの取得

ログファイルの取得は、CMデータビューアのファイル転送機能で行います。



CMデータビューアの「ツール」メニューからファイル転送を選択し「ファイル転送」ダイアログを表示します。

「ファイル転送」ダイアログから「プロセスログ」ラジオボタンを選択します。
ファイル転送の操作については、「6.2.5 ツールメニュー」を参照してください。

「ファイル転送」により転送されるファイル名はSG設定で指定したファイル名になります。
ログファイルの拡張子がLo_のファイルは前世代のファイルになります。

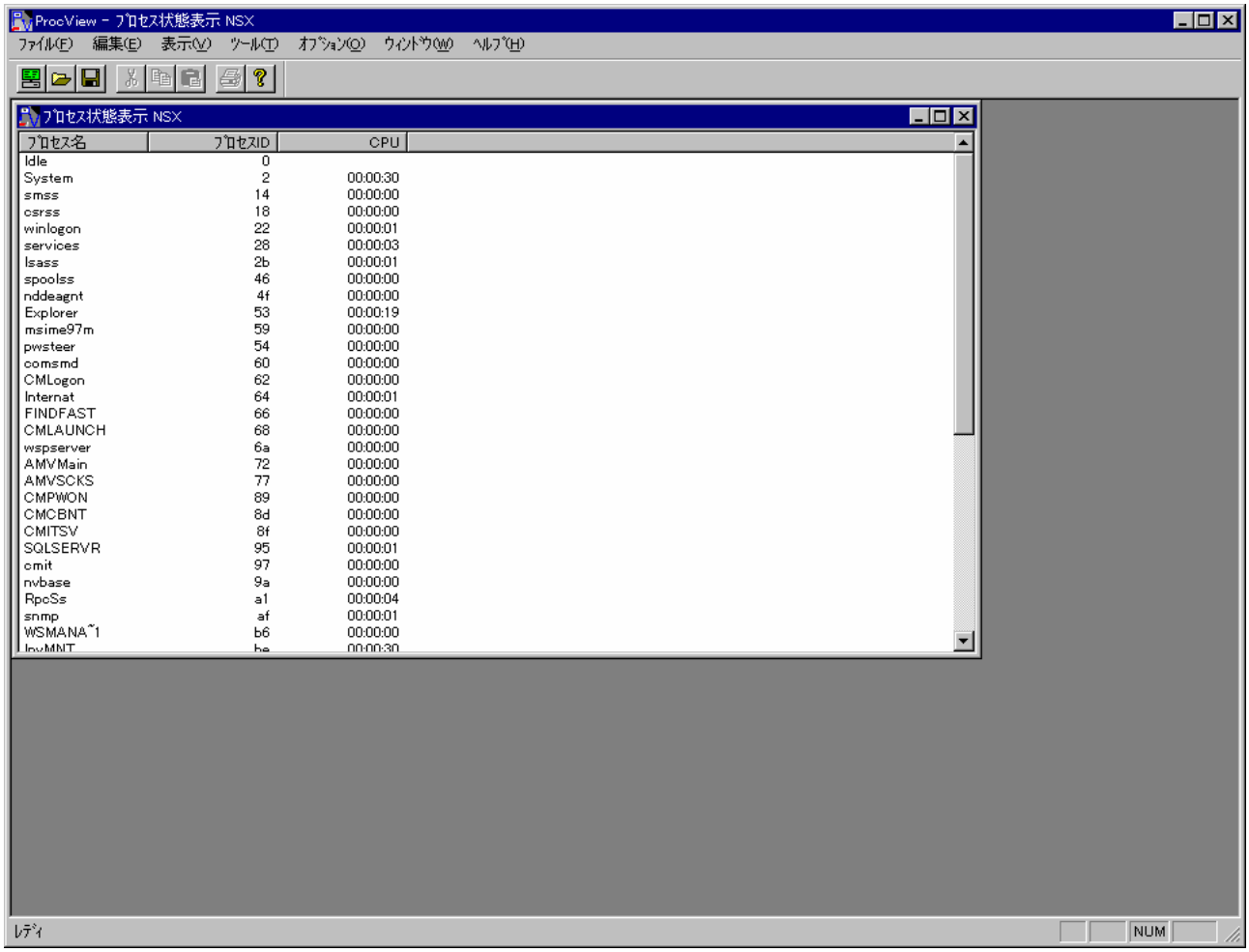
SGファイルの設定を行わないとプロセスログのファイル名がクライアント管理ID.Logになります。クライアント管理IDが XXX00001 の場合は、XXX00001.Log になります。この時プロセスログの内容は、プロセス監視機能の開始と終了を示す記録だけになります。

SGファイルの設定を行わないとアラートログのファイル名がPrcAlert.Logになります。この時アラートログには、すべてのプロセスの動作が記録の対象となります。

転送ディレクトリは「ファイル転送」で指定したディレクトリになります。

11.5 プロセス状態表示機能

プロセス状態表示機能は、クライアントのプロセス(アプリケーション)の状態を表示する機能です。



プロセス監視GUI起動時に「プロセス状態表示」ウィンドウが開きます。

＊プロセス名

クライアントで動作しているプロセス名を表示します。

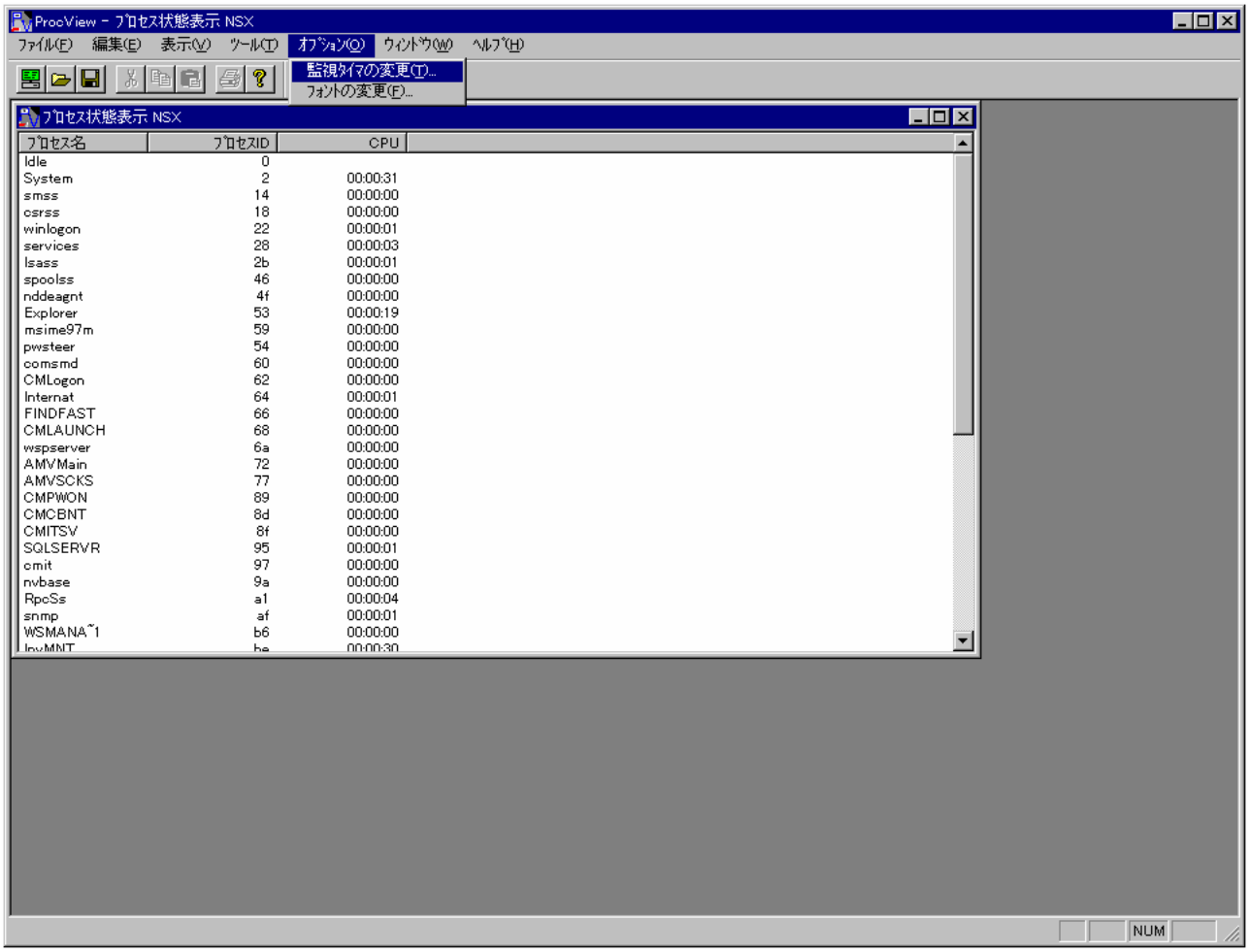
＊プロセスID

クライアントで動作しているプロセスのIDを表示します。

＊CPU

クライアントで動作しているプロセスのCPU使用時間を表示します。

クライアントのOSがWindows NT の時に表示します。



プロセス状態表示は、指定された間隔(既定値 5秒)でクライアントのプロセス状態を表示します。この間隔を変更する場合は、「オプション」メニューの「監視タイマの変更」を選択し、変更します。

「監視タイマの変更」ダイアログボックスでは、定期的な監視を行う場合の間隔を秒単位で指定します。定期的な監視を止める場合は、「定期的な監視を行う」チェックボックスをチェックしないで＜OK＞ボタンを押してください。

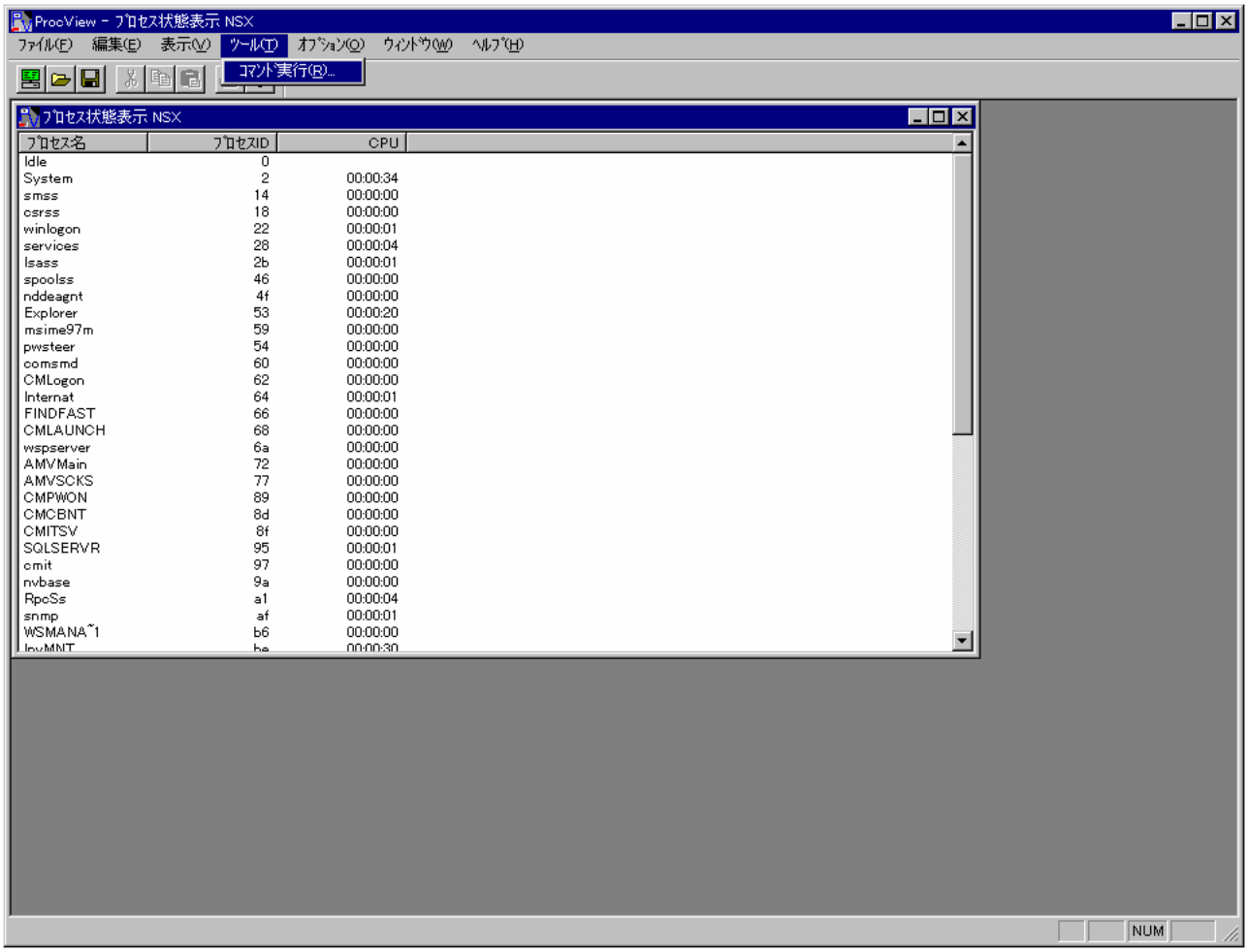
プロセス状態表示中にクライアントの負荷が高くなった時は、タイムアウトエラーになる場合があります。その場合一度「プロセス状態表示」ウィンドウを閉じて再度「ファイル」メニューの「プロセス状態を開く」を選択する事により再度クライアントに接続を行います。

クライアントのプロセス監視機能が無効に設定されている場合は、「ファイル」メニューの「プロセス状態を開く」を選択してもタイムアウトエラーになります。その場合は、CMデータビューアからクライアントのプロセス監視機能を有効にしてから再度「プロセス状態表示」ウィンドウを開いてください。

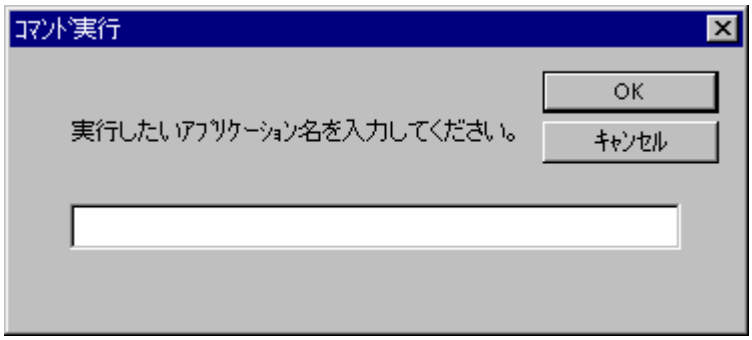
「プロセス状態表示」で表示している内容は、CSV形式(カンマで区切られた形式)のファイルに保存する事が可能です。ファイルの保存は、「ファイル」メニューの「名前を付けて保存」を選択し行います。

11.6 コマンド実行機能

コマンド実行機能は、プロセス監視GUIからクライアント上のアプリケーションを起動する機能です。



コマンド実行は、「ツール」メニューから「コマンド実行」を選択して「コマンド実行」ダイアログを表示します。



「コマンド実行」ダイアログの「実行したいアプリケーション名を入力してください。」エディットボックスに実行したいアプリケーション名を入力します。

アプリケーションは以下の規則にしたがって実行されます。

- アプリケーション名に拡張子が含まれていない場合は、.EXEであるとみなされます。
- アプリケーション名にディレクトリパスが含まれている場合は、そのパス内の指定したアプリケーションを実行します。
- アプリケーション名にディレクトリパスが含まれていない場合には、OSがPATH環境変数内にリストされているディレクトリを検索し指定したアプリケーションを実行します。

起動要求がOSに受け付けられた場合は、「コマンドの実行に成功しました。」メッセージボックスが表示されます。

「ProcView – XXX」の「XXX」にはクライアントのマシン名、又はIPアドレスが入ります。

コマンドの実行が失敗した場合は、「コマンドの実行に失敗しました。」メッセージボックスが表示されます。

コマンドの実行に失敗する原因としてアプリケーションファイル（又はその構成ファイル）が見つからない場合があります。パス及びアプリケーション名が正しいか、必要なライブラリがすべて利用可能かどうか、確認してください。

「ProcView – XXX」の「XXX」にはクライアントのマシン名、又はIPアドレスが入ります。
（Y）の カッコ内の Y は、システムのエラーコードが表示されます。
システムのエラーの例として以下があります。

- エラーコードが 2 の場合は、アプリケーションファイル（又はその構成ファイル）が見つからなかった事を示します。

通信に失敗した場合は、「通信接続に失敗しました。（タイムアウト）」メッセージボックスが表示されます。

「ProcView – XXX」の「XXX」にはクライアントのマシン名、又はIPアドレスが入ります。

11.7 不正プロセスアラート通知機能

不正プロセスアラート通知機能は、クライアント上で不正なプロセスの動作をマネージャにアラートで通知する機能です。

不正なプロセスの動作は、履歴をアラートログに記録します。

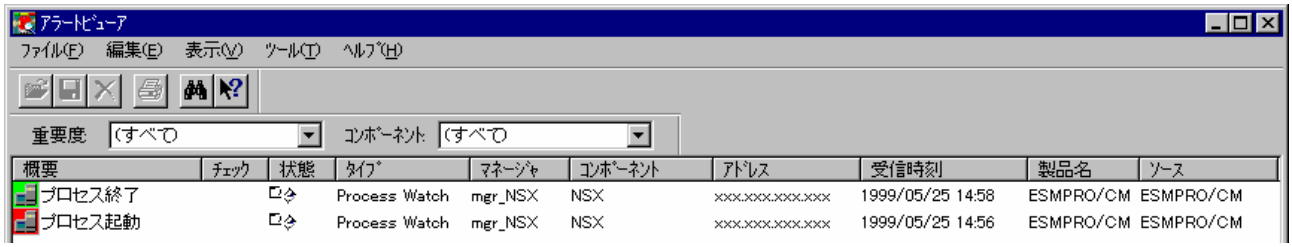
不正なプロセスとは、プロセス監視機能のSGに登録されていないプロセスです。

マネージャにアラートを通知するためには、SG設定によりアラートの通報設定をする必要があります。

SGの設定については「11.8 SG設定」を参照してください。

SG設定でアラート通知をしない設定でも不正なプロセスが動作した場合には、その履歴をアラートログに記録します。

不正プロセスのアラートはマネージャ上のアラートビューアに表示されます。



「プロセス起動」は、異常通知として行の先頭を赤色で表示します。

「プロセス終了」は、回復通知として行の先頭を緑色で表示します。

アラートログは、クライアント上に作成されます。

アラートログの取得は、CMデータビューアのファイル転送機能を使用します。「11.4.4 ログファイルの取得」を参照してください。

アラートログのファイル名はSG設定で指定したファイル名になります。既定値は、PrcAlert.Logです。

アラートログファイルの拡張子がLo_のファイルは前世代のファイルになります。

アラートログの形式は、プロセスログの形式と共通です。ログの形式は、「11.4.3 ログ形式」を参照してください。

SG設定を行わないと、全てのプロセスの動作がアラートログへの記録の対象となります。

11.8 SG 設定

プロセス監視機能のプロセスロギング機能、不正プロセスアラート通知機能を使用する場合、SGを設定する必要があります。SGの項目は、以下の通りです。

- 監視間隔
- ポート番号
- ログファイル名
- ログサイズ
- アラートログファイル名
- アラートログファイルサイズ
- アラート通報有無
- プロセス設定

SG設定は、「スタート」メニューの「プログラム」－「ESMPRO_CM」－「プロセス監視SG設定」を選択し、「プロセス監視設定」ダイアログで設定します。

*** 監視間隔**

プロセスの起動終了をチェックする間隔です。既定値は、60秒となります。

*** ポート番号**

GUIとの通信を行うためのポート番号です。既定値は、14375となります。

*** 異常回復通知**

CMマネージャに通知された不正プロセスが終了した時の回復アラートの設定です。チェックを付けると回復アラートが通知されます。既定値は回復アラートを通知する設定となります。

*** 送信頻度**

不正プロセスが起動した時のアラート通知を制限する数を設定します。
1分間に、設定された制限数を超える不正プロセスの起動はCMマネージャに通知しません。
不正プロセスが終了した時の回復アラートは制限されません。異常アラートを通知したプロセスのみ回復アラートが通知されます。既定値は、制限しない設定となります。

*** ログファイル名**

出力するログのファイル名を設定します。最初に表示されるファイル名はWatch.Logです。
SG設定を行わずにプロセス監視機能を有効にするとファイル名はクライアント管理ID.Logになります。クライアント管理IDが XXX00001 の場合は、XXX00001.Logになります。

*** ログサイズ**

プロセスの起動・終了ログを出力するファイルサイズをバイト単位で指定します。ログファイルは、最大「ログサイズ」で指定した2倍の情報を保持する事があります。ログファイルサイズは、30000未満を指定してください。既定値は、30000となります。

*** アラートログファイル名**

出力するアラートログのファイル名を指定します。既定値はPrcAlert.Log

*** アラートログサイズ**

不正プロセスの起動・終了ログを出力するファイルサイズをバイト単位で指定します。アラートログファイルは、最大「アラートログサイズ」で指定した2倍の情報を保持する事があります。既定値は、409600となります。

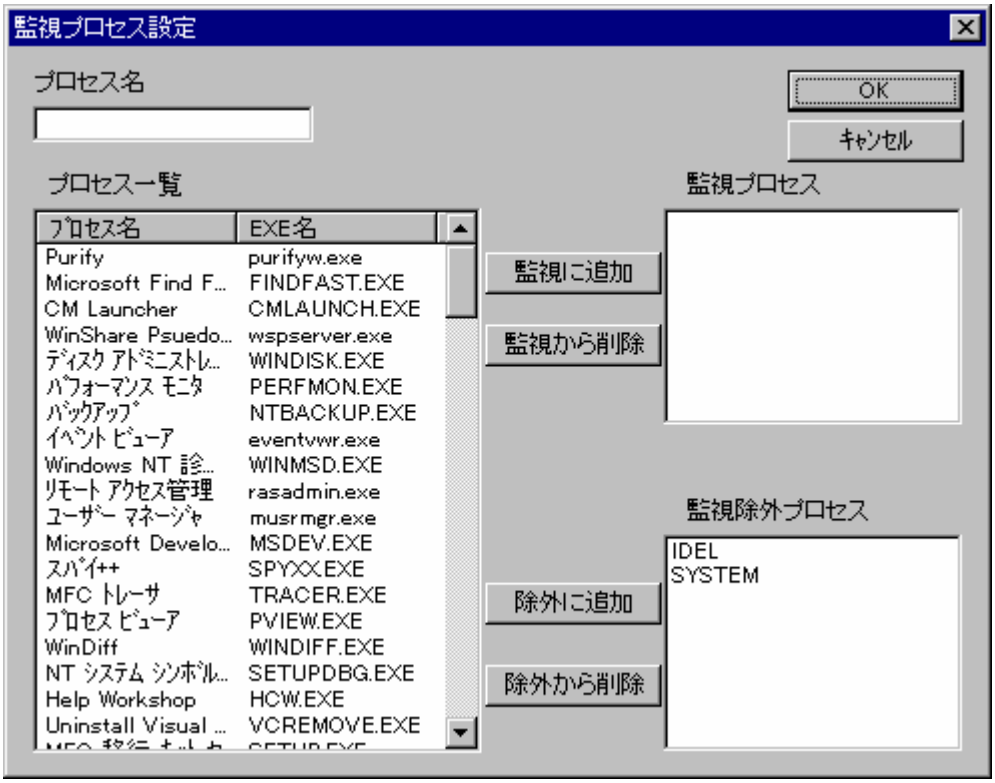
*** アラート通報有無**

不正プロセスの起動・終了時にCMマネージャへのアラートの通報を行うかを設定します。
チェックを付けると不正プロセスのアラートが通知されます。既定値はアラートを通知しない設定となります。

*** プロセス設定**

プロセスログ出力、アラート通知、アラートログ出力するプロセスを指定する場合はこのボタンを押し、「監視プロセス設定」ダイアログでプロセスの設定を行ってください。

注意：監視間隔で指定した時間内（ある監視時刻後から次回の監視時刻前までの間）に同一のプロセスが起動し終了した場合はそのプロセスの監視（ログ出力、アラート通知）は行えません。



「監視プロセス設定」ダイアログで、プロセスログ、アラート通知、アラートログそれぞれの対象にするプロセスを定義します。あるいは、ログやアラートの対象にしないプロセスを定義します。プロセスの定義は、次のように設定してください。

プロセスログ ・・・・「監視プロセス」にプロセス名を設定する。
アラート通知 ・・・・「監視プロセス」と「監視除外プロセス」のどちらにもプロセス名を設定しない。
アラートログ ・・・・「監視プロセス」と「監視除外プロセス」のどちらにもプロセス名を設定しない。
ログ不要 ・・・・「監視除外プロセス」にプロセス名を設定する。
アラート不要 ・・・・「監視除外プロセス」にプロセス名を設定する。

アラートを通知するには「プロセス監視設定」ダイアログの「アラート通報有無」チェックボックスにチェックをしてください。

「プロセス一覧」には、以下のプロセスを表示します。

- ディスクトップ(ALL User)に設定しているプロセス(*.EXEのみ)
- スタートメニュー(ALL User) に設定しているプロセス(*.EXEのみ)
- サービスに登録しているプロセス

「プロセス一覧」には、「監視プロセス設定」ダイアログが動作しているPCのプロセスの情報が表示されます。

「監視プロセス設定」ダイアログをマネージャで動作させた場合、プロセス一覧に表示する内容はマネージャのディスクトップ、スタートメニュー、サービスに登録されているプロセス名です。

クライアントのディスクトップ、スタートメニュー、サービスに登録されているプロセスを表示するためにはクライアント上で「監視プロセス設定」ダイアログを動作させます。

「監視プロセス設定」ダイアログを Windows NT バージョン3.51上で動作させた場合に「プロセス一覧」に表示されるのは、サービスに登録されているプロセスだけになります。

「監視プロセス」の追加手順については、以下の通りです。

- 「プロセス一覧」から選択して「監視に追加」ボタンを押します。
- 「プロセス一覧」にないプロセス名を監視したい場合は、「プロセス名」に監視するプロセス名(ファイル名)を記述し、＜監視に追加＞ボタンを押してください。

「監視プロセス」を削除手順については、以下の通りです。

- 監視を止める場合には、「監視プロセス」からプロセス名を選択して＜監視から削除＞ボタンを押してください。

「監視除外プロセス」も同様の手順で追加削除を行います。

SG設定は、クライアント上で動作しているプロセス監視機能の次回起動時から有効になります。そのため、SGの追加、修正を行いすぐに反映させるためにはクライアントPCを再起動するか、又はCMデータビューアよりプロセス監視機能を一度無効にした後、再度有効にしてください。

「プロセス監視設定」ダイアログにより作成されたSGファイルは、クライアント、又はマネージャの (ESMPROCM)¥DATAディレクトリ配下にあります。SGファイルは、以下の3個です。

- SG.DAT
- WatchInf.DAT
- NoWatch.DAT

マネージャでSGファイルを作成した場合はクライアントの (ESMPROCM)¥Data ディレクトリ配下にSGファイルをコピーしてください。

SG設定は、クライアント上で動作しているプロセス監視機能の次回起動時から有効になります。そのため、SGの追加、修正を行いすぐに反映させるためにはクライアントPCを再起動するか、又はCMデータビューアよりプロセス監視機能を一度無効にした後、再度有効にしてください。

プロセス監視機能を有効にするには、「11.2 プロセス監視機能を有効にするには」を参照してください。

【補足】

ESMPRO/PFWatcher（プロセス監視を行う製品）の設定ファイルの情報を表示する事もできます。

ESMPRO/ PFWatcherの設定ファイルで指定した監視プロセスを「プロセス一覧」に表示するためには、ESMPRO/ PFWatcherの設定ファイル(ESMpsrv.dat OR ESMpcom.dat)をあらかじめ(ESMPROCM)¥DATAディレクトリにコピーしてから「監視プロセス設定」ダイアログを動作させてください。

11.9 注意事項

以下の注意事項があります。

1. ログファイルサイズは30000バイト未満としてください。
2. 16ビットアプリケーションの監視は行えません。
3. 監視間隔で指定した時間内（ある監視時刻後から次回の監視時刻前までの間）に同一のプロセスが起動し終了した場合はそのプロセスの監視（ログ出力、アラート通知）は行えません。
4. プロセスログをテキストファイルにセーブする際は、必ずファイル名を変更するかディレクトリを変更してセーブしてください。
5. SG設定を行わずにプロセス監視機能を有効にするとクライアント上に作成されるアラートログに全てのプロセスの動作が記録されます。アラートログのサイズは既定値で409600バイトです。最大で既定値の2倍のサイズで情報を保持する事もあります。
6. クライアントで動作しているプロセスの名前にカンマが含まれていると、プロセス状態表示の該当プロセスとその次に表示されているプロセスがずれて表示されます。またプロセス状態表示から保存したファイルの内容も同様にずれて保存されます。