(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4156663号
(P4156663)

(45)発行日　平成20年9月24日(2008.9.24)　(24)登録日　平成20年7月18日(2008.7.18)

(51)Int.Cl.　F I
G06F 11/30 (2006.01)　G06F 11/30　D
G06F 13/00 (2006.01)　G06F 13/00　351M

請求項の数 3　(全 31 頁)

(21)出願番号　特願平7-525905
(86)(22)出願日　平成7年4月3日(1995.4.3)
(65)公表番号　特表平10-501907
(43)公表日　平成10年2月17日(1998.2.17)
(86)国際出願番号　PCT/US1995/004109
(87)国際公開番号　WO1995/027249
(87)国際公開日　平成7年10月12日(1995.10.12)
審査請求日　平成14年3月27日(2002.3.27)
審判番号　不服2005-9147(P2005-9147/J1)
審判請求日　平成17年5月16日(2005.5.16)
(31)優先権主張番号　08/223,221
(32)優先日　平成6年4月5日(1994.4.5)
(33)優先権主張国　米国(US)

(73)特許権者　591003943
インテル・コーポレーション
アメリカ合衆国　９５０５２　カリフォルニア州・サンタクララ・ミッション　カレッジ　ブーレバード・２２００
(74)代理人　100064621
弁理士　山川　政樹
(74)代理人　100067138
弁理士　黒川　弘朗
(74)代理人　100076392
弁理士　紺野　正幸
(74)代理人　100081743
弁理士　西山　修
(74)代理人　100098394
弁理士　山川　茂樹

最終頁に続く

(54)【発明の名称】ネットワーク内でプログラムを監視し、制御する方法および装置

(57)【特許請求の範囲】
【請求項１】
ネットワーク内で複数のワークステーションを制御するためのシステムであって、
前記ワークステーションの１つで実行中のプログラムに関して発生しているイベントを識別するための手段と、
前記ワークステーションの１つに設けられ、前記イベントを識別するアラートを管理コンソールに送るための手段と、
少なくとも１つの手順を記憶するための前記管理コンソールに設けられた手段であって、前記の少なくとも１つの手順が複数の記憶されたトリガを含み、前記複数の記憶されたトリガのそれぞれが、前記ネットワーク内で特定の処置がとられるようになされた手段と、
前記アラートを管理コンソールに送るための手段からのアラートの受信またはネットワーク管理者の指示に応答して、前記少なくとも１つの手順を、前記管理コンソールから前記ワークステーションに設けられたエージェント手段に送るための前記管理コンソールに設けられた手順を送信する手段と、
前記ワークステーションの１つに設けられ、前記送信された少なくとも１つの手順内の前記複数の記憶されたトリガを自動的に開始するための手段と、
前記ワークステーションの１つに設けられ、前記ワークステーション上で新たにアクティブ化したエージェント手段を自動的に発見するための、および前記新たにアクティブ化したエージェント手段を前記管理コンソールに確認させるための手段とから構成され、
前記イベントを識別するための手段が前記ワークステーション上でネットワーク管理者の

介在を必要としない問題を検出した場合、前記アラートを管理コンソールに送るための手段が前記管理コンソールに当該問題情報を報告するとともに、この報告に応答して前記手順を送信する手段が前記問題を是正するトリガを含む手順を前記ワークステーションのエージェント手段に送信し、
前記イベントを識別するための手段が前記ワークステーション上でネットワーク管理者の介在を必要とする問題を検出した場合、前記アラートを管理コンソールに送るための手段が前記管理コンソールに推奨訂正処置を含む当該問題情報を報告するとともに、前記ネットワーク管理者の指示に応答して前記手順を送信する手段が前記問題を是正するトリガを含む手順を前記ワークステーションのエージェント手段に送信し、
さらに、前記イベントを識別するための手段が前記ワークステーション上のファイルアクティブを監視してアクセス侵害が生じたか否か検出し、このアクセス侵害によりユーザの特権が侵害される前にネットワーク管理者が当該ワークステーションをフリーズすることができるよう、該アクセス侵害が生じた時に前記アラートを管理コンソールに送るための手段が前記管理コンソールに当該アクセス侵害情報を報告するとともに、前記ネットワーク管理者の指示に応答して前記手順を送信する手段が前記ワークステーションをフリーズさせるフリーズ・トリガを含む手順を前記ワークステーションのエージェント手段に送信することを特徴とするシステム。

【請求項２】

少なくとも２つのワークステーションと、前記少なくとも２つのワークステーションに接続されている管理コンソールとを含むネットワークを監視し、制御するシステムであって、
ワークステーション上で実行中のプログラムに関してイベントが発生していることを示すアラートを伝送するための、前記ワークステーションに設けられた少なくとも１つの一般エージェント手段と、
前記少なくとも１つの一般エージェント手段のいずれかによって伝送されるアラートをログするための、前記管理コンソールに設けられたモニタ手段と、
前記管理コンソールに保持される少なくとも１つの手順であって、前記手順が複数の記憶されたトリガを含み、前記複数の記憶されたトリガのそれぞれが前記ネットワーク内で特定の訂正処置を行う訂正処理トリガである、前記手順を記憶保持する手段と、
前記少なくとも１つの一般エージェント手段の動作を監視し、制御する前記少なくとも１つの一般エージェント手段に結合されているマネージャ手段であって、アラートに応答してまたはネットワーク管理者の指示に応答して前記少なくとも１つの手順を前記少なくとも１つの一般エージェント手段に送るようにさらに構成されているマネージャ手段と、
前記少なくとも１つの手順内で前記複数の記憶されたトリガを自動的に開始するように構成されている前記少なくとも２つのワークステーションに設けられ、前記少なくとも２つのワークステーション上で新たにアクティブ化されたエージェント手段を自動的に発見するための、および前記管理コンソールに対して前記新たにアクティブ化されたエージェント手段を識別するための手段とから構成され、
前記一般エージェント手段が前記ワークステーション上でネットワーク管理者の介在を必要としない問題を検出した場合、前記マネージャ手段が前記アラートに応答して前記問題を是正するトリガを含む手順を前記一般エージェント手段に送信し、
前記一般エージェント手段が前記ワークステーション上でネットワーク管理者の介在を必要とする問題を検出した場合、前記管理コンソールに推奨訂正処置を含む当該問題情報を報告するとともに、前記ネットワーク管理者の指示に応答して前記マネージャ手段が前記問題を是正するトリガを含む手順を前記一般エージェント手段に送信し、
さらに、前記一般エージェント手段が前記ワークステーション上のファイルアクティブを監視してアクセス侵害が生じたか否か検出し、このアクセス侵害によりユーザの特権が侵害される前にネットワーク管理者が当該ワークステーションをフリーズすることができるよう、該アクセス侵害が生じた時に前記モニタ手段に当該アクセス侵害情報を報告するとともに、前記マネージャ手段が前記ネットワーク管理者の指示に応答して前記ワークステ

ーションをフリーズさせるフリーズ・トリガを含む手順を前記一般エージェント手段に送信することを特徴とするシステム。

【請求項３】

少なくとも２つのワークステーションと、前記少なくとも２つのワークステーションのそれぞれに接続されている管理コンソールとを含むネットワークを監視し、制御するシステムであって、

ワークステーション上で実行中のプログラムに関してイベントが発生していることを示すアラートを伝送するように構成されている前記少なくとも２つのワークステーションのそれぞれに設けられた少なくとも１つの一般エージェント手段と、

前記少なくとも１つの一般エージェント手段のいずれかによって送られるアラートをログするように構成されている前記管理コンソールに設けられたモニタ手段と、

少なくとも１つの手順を定義する前記管理コンソールであって、前記手順が複数の記憶されたトリガを含み、前記複数の記憶されたトリガのそれぞれが前記ネットワーク内で特定の訂正処置がとられるようになされている管理コンソールと、

前記少なくとも１つの一般エージェント手段に結合されており、前記少なくとも１つの一般エージェント手段の動作を監視し、制御するように構成されているマネージャ手段であって、前記アラートに応答してまたはネットワーク管理者の指示に応答して前記少なくとも１つの一般エージェント手段に前記少なくとも１つの手順を送るようにさらに構成されているマネージャ手段と、

特定ユーザ・プログラムを実行中に問題を処理する前記少なくとも２つのワークステーションのそれぞれに設けられた少なくとも１つの特定エージェント手段と、

前記少なくとも１つの手順内の前記複数の記憶されたトリガを自動開始するように構成されている前記少なくとも２つのワークステーションの前記１つとから構成され、

前記一般エージェント手段が前記ワークステーション上でネットワーク管理者の介在を必要としない問題を検出した場合、前記マネージャ手段が前記アラートに応答して前記問題を是正するトリガを含む手順を前記一般エージェント手段に送信し、

前記一般エージェント手段が前記ワークステーション上でネットワーク管理者の介在を必要とする問題を検出した場合、前記管理コンソールに推奨訂正処置を含む当該問題情報を報告するとともに、前記ネットワーク管理者の指示に応答して前記マネージャ手段が前記問題を是正するトリガを含む手順を前記一般エージェント手段に送信し、

さらに、前記一般エージェント手段が前記ワークステーション上のファイルアクティブを監視してアクセス侵害が生じたか否か検出し、このアクセス侵害によりユーザの特権が侵害される前にネットワーク管理者が当該ワークステーションをフリーズすることができるよう、該アクセス侵害が生じた時に前記モニタ手段に当該アクセス侵害情報を報告するとともに、前記マネージャ手段が前記ネットワーク管理者の指示に応答して前記ワークステーションをフリーズさせるフリーズ・トリガを含む手順を前記一般エージェント手段に送信することを特徴とするシステム。

【発明の詳細な説明】

背景

本発明は、ネットワーク内でプログラムを制御する方法および装置を対象とする。特に、本発明は、ネットワーク・ワークステーション上で動作中のプログラム内で発生しているエラー状態を自動的に検出し、訂正する方法および装置を対象とする。

現在のネットワークはサイズおよび複雑さが拡大しつつある。ネットワーク管理者は、一般に、ネットワークの設計、編成および保守を監督する。管理者の責任には、ネットワークのハードウェアとソフトウェア問題のトラブルシューティングだけでなく、ネットワーク内の各ワークステーション上のハードウェアとソフトウェア問題のトラブルシューティングも含まれる。ユーザが動作させている各プログラムに特有の問題を含むワークステーション上の問題のトラブルシューティングに管理者の時間の８０％ほどが費やされる。ネットワーク管理者がユーザに関する問題を修正するまで、ワークステーションは休止する。そのような休止時間は、その動作がネットワークおよびそのワークステーションが適切

に機能することに依存する編成にとって損失が大きくなる。さらに、ネットワーク管理者は、ネットワーク上で動作中のすべてのプログラムに関して発生するどんな問題でも診断し、修正できなければならないので、少なくともすべてのネットワーク・プログラムの作業知識を有する高度に熟練した個人でなければならない。

本発明は、ネットワーク管理者がネットワーク内で遭遇する問題を解決するのを援助するシステムに関する。ネットワーク問題を検出し、それらを報告する本発明によるプログラムのいくつかの初期版が一年以上市販されている。１９９２年１１月に発売されたこれらの最新版は、カリフォルニア州マウンテンビューのＳｈａｎｙ社から市販されているＡｌｅｒｔＶＩＥＷ™、Ｖｅｒｓｉｏｎ２．０である。これらの初期版は、１つのネットワークのワークステーション上で動作する特定のアプリケーション・プログラムに関して問題が発生していることをネットワーク管理者に知らせるものである。しかしながら、従来版は、問題の検出に応答して、すなわち管理コンソールにおいてアラートを受け取った際に、ワークステーションに単一のコマンドまたはトリガしか送ることができないので有限の能力しか有しない。特に、管理コンソールは、ワークステーションのフリーズ、アンフリーズまたはリブート、前景（foreground）内で動作中のプログラムの開始および停止、メッセージの送信、または特定のアラートに応答して実施されるようにユーザが指示するカスタム・トリガの形で任意の単一コマンドを送信するなどの処置（action）のうちの１つを行わせるトリガを送る。

概要

したがって、本発明の目的は、ワークステーションにおいて発生する問題を処理する際にフレキシビリティが増大するような形で、上記のプログラムの初期版を改善することである。

本発明の目的は、ネットワーク・ワークステーション上で動作中のプログラムの故障を識別でき、かつこれらの故障をもたらす問題を訂正する適切な訂正処置をとることができるネットワーク保守システムを提供することである。

本発明の他の目的は、ワークステーション上でアクティブしているエージェントにそれぞれ１つまたは複数のとるべき処置から構成される手順を送ることによって、ネットワーク内のワークステーション上で発生している問題を訂正できるシステムを提供することである。

本発明の他の目的は、ネットワーク管理者によるネットワーク・ワークステーションの統合遠隔アクセスおよび制御が可能なネットワーク保守システムを提供することである。

本発明の他の目的は、ネットワーク管理者が、ネットワーク管理タスクおよび保守タスクの自動実行をスケジューリングできるシステムを提供することである。

本発明の他の目的は、ネットワーク管理者が、ネットワーク内のワークステーションにキーストローク・ジョブを自動的に送ることができるシステムを提供することである。

本発明の他の目的は、エージェントの自動回復が可能なシステムを提供することである。

本発明の他の目的は、特定のアプリケーションに適合するように開発された特定エージェントを提供するシステムを提供することである。

一実施態様によれば、ネットワーク内の少なくとも２つのワークステーションのうちの任意のワークステーション上で実行できる少なくとも１つのプログラムを制御するシステムが提供される。ネットワークは、各ワークステーション上に常駐する少なくとも１つのエージェント・モジュール、および各ワークステーションに接続された管理コンソールを含む。本システムは、１つのワークステーション上で実行中のプログラムに関して発生している事象（event）を識別する手段、事象を識別するアラートを管理コンソールへ送る手段、および複数のトリガを記憶する手段を含む。各トリガは、ネットワーク内で処理がとられるようになされている。さらに、本システムは、少なくとも１つのトリガを含む少なくとも１つの手順を記憶する手段、およびアラートの受取りに応答して、手順のうちの少なくとも１つを管理コンソールから１つのワークステーション上に常駐するエージェント・モジュールへ送る手段を含む。

他の実施態様によれば、ネットワーク内で少なくとも１つのプログラムを監視し、制御す

るシステムが提供される。ネットワークは、少なくとも２つのワークステーション、および各ワークステーションに接続された管理コンソールを含む。本システムは、各ワークステーション上に常駐し、ワークステーション上で実行中のプログラムに関する事象の発生を示すアラートを送信する少なくとも１つの一般アラート手段、および管理コンソール上に常駐し、いずれかのエージェント手段によって送信されたアラートをログする監視手段を含む。さらに、本システムは、事象に応答してエージェント手段に処置をとらせるコマンドを含み、監視手段からエージェント手段へ送るべき複数のトリガを記憶する手段、記憶されたトリガのうちの少なくとも１つを含む少なくとも１つの手順を定義する手段、およびアラートに応答してエージェント手段に手順を送る手段を含むエージェント手段の動作を監視し、制御するマネージャ手段を含む。

他の実施態様によれば、ネットワーク内の少なくとも２つのワークステーションのうちの任意のワークステーション上で実行できる少なくとも１つのプログラムを監視し、制御する方法が提供される。ネットワークは、各ワークステーション上に常駐する少なくとも１つのエージェント・モジュール、および各ワークステーションに接続された管理コンソールを含む。本方法は、それぞれネットワーク内で処置がとられるようになされた複数のトリガを記憶するステップと、その複数のトリガのうちの少なくとも１つのトリガを含む少なくとも１つの手順を記憶するステップと、１つのワークステーション上で発生している事象を識別するステップと、事象を識別するアラートを管理コンソールへ送るステップと、アラートの受取りに応答して手順のうちの少なくとも１つを管理コンソールから１つのワークステーション上に常駐するエージェント・モジュールへ送るステップとを含む。

本発明の他の目的、特徴および付随する利点は、添付の図面と関連して行い、本発明に従って構成された実施形態の以下の詳細な説明を読めば当業者に明らかとなろう。

次に、本明細書の発明について、本システムの好ましい実施形態と関連して、例としてのみ、添付の図面と関連して詳細に説明する。

【図面の簡単な説明】

本明細書の発明について、単に例として行った本システムの好ましい実施形態と関連して、添付の図面を参照しながら説明する。

第１図は、本発明の一実施形態によるネットワーク・システムのブロック図である。

第２図は、本発明によるコンピュータ・システムの例示の実施形態のブロック図である。

第３図は、本発明の一実施形態による第１図のシステム内で使用される一般エージェントのブロック図である。

第４図は、本発明の一実施形態による第１図のシステム内で使用されるモニタのブロック図である。

第５図は、第１図のシステム内で使用されるマネージャのブロック図である。

第６図は、本発明の一実施形態による第１図のシステム内で使用される一般エージェントの初期設定段階についてのルーチンの流れ図である。

第７図は、本発明の一実施形態による第１図のシステム内で使用される一般エージェントの動作段階についてのルーチンの流れ図である。

第８図は、本発明の一実施形態による第１図のシステム内で使用される一般エージェントの障害管理段階についてのルーチンの流れ図である。

第９図は、本発明の一実施形態による第１図のシステム内で使用される一般エージェントの制御および管理段階についてのルーチンの流れ図である。

第１０図は、本発明の一実施形態による第１図のシステム内で使用されるモニタの動作段階についてのルーチンの流れ図である。

第１１図は、本発明の一実施形態による第１図のシステム内で使用されるマネージャの動作段階についてのルーチンの流れ図である。

第１２図は、本発明の一実施形態による特定エージェントについてのネットワーク・システムのブロック図である。

第１３図は、本発明の一実施形態による、非ＴＳＲアプリケーションとしてロードされた第１２図の特定エージェントの動作についてのルーチンの流れ図である。

第１４図は、本発明の一実施形態による、ＴＳＲアプリケーションとしてロードされた第１２図の特定エージェントの動作の初期設定段階についてのルーチンの流れ図である。
第１５図は、本発明の一実施形態による、ＴＳＲアプリケーションとしてロードされた第１３図の特定エージェントの動作についてのルーチンの流れ図である。
概括的な説明
本発明は、ネットワーク内のワークステーション上で実行中のプログラムを監視し、制御することによって、ネットワーク・プログラムの問題に対して実時間解決を実現できるネットワーク管理ツールに関する。本明細書でいうプログラムとは、通信ソフトウェア、ネットワーク・オペレーティング・システム・プログラム、オペレーティング・システム・プログラム、およびエンド・ユーザ・アプリケーション・プログラムを含む。
本発明によるシステムでは、最も一般的な困難で時間のかかる種類の問題を代表するエンド・ユーザ・プログラム・エラーの検出、報告、訂正および防止を行う。本発明によるシステムでは、ユーザの休止時間が大幅に短縮され、すべてのネットワーク・プログラムの実時間制御およびサポートを行い、ネットワーク管理者がもどかしいトラブルシューティングの時間から解放され、また管理者が最適効率でネットワークを管理することができる。本システムは、プログラムに集中することによって、面倒なユーザ・サポート・タスクを満足な結果指向経験に転換する。
本発明によるシステムでは、プログラムが連続的にスムーズ動作するために必要なハウスキーピング・タスクを自動的に開始する手順を管理者がスケジューリングすることができる。本システムは、ネットワーク・プログラム問題の優先権を分析するための情報を保持しており、この情報を使用して問題の再発生を防止することができる。また、この情報を使用して、ワークステーションが安全に動作するようにワークステーション上で必要な処置を実行するスケジューリング手順を指定することによって、またより小さい問題の発生に反応してより大きい問題の発生を防止する訂正手順を指定することによって、ネットワークを保守することができる。また、本発明によるシステムは、それ自体のスケジュール手順を管理し、保守タスクおよびバックアップ・タスクがうまく完了することを保証する。
本発明によるシステムは、ネットワーク・ワークステーション上に常駐して、ユーザ、アプリケーション、システム・ソフトウェア間の対話を能動的に監視し、ネットワーク管理者に問題の実時間検出を与えるエージェントを含む。ユーザに使用できないまたは理解できない情報を含めて、重要な事象の詳細は連続的に収集される。この説明では、事象とは、ワークステーション上の割込みまたはプログラムに関する問題が発生することである。
本発明によるシステムは、実時間問題解決を提供し、問題、問題の位置、問題が発生している間のプログラム、および問題を訂正する勧告を識別し、管理者に知らせる貴重なデータを管理者に提供する。本発明によるシステムは、完全保護侵害、エラー・メッセージ、フリーズステーション、およびその他の時間のかかる問題の原因を検出するので、多くのもどかしい当て推量の時間の除去が達成される。
ネットワークを介して、本発明によるエージェントは、各事象が発生した際にそれに関する理解できる詳細な情報を含むアラートを送信し、したがってネットワーク管理者が、印刷エラー、安全保護侵害、およびネットワークのスムーズな動作にとって重要なその他のプログラム・エラーに集中し、アドレス指定することができる。本システムは、報告されたすべての詳細の正確で完全な通信を保証する。本システムのメモリ能力があれば、通信が有限または不十分なことはなくなる。本システムは、ネットワーク管理者がどこにいるかにかかわらず、電子メール、モデムまたはネットワークを介して重要なプログラム問題をネットワーク管理者に直接能動的に報告し、したがって管理者が報告手順をカスタマイズすることができる。例えば、アラートを引き起こした事象に関連したアプリケーション・ファイル・サーバ、印刷待ち行列などに関する詳細な報告を含めて、問題を明確に理解するために必要な情報が完全に報告されるので、ネットワーク管理者がネットワークの問題を迅速に解決することができる。
代表的なネットワークでは、ワークステーションのユーザが遭遇する問題の４０パーセン

トが毎日繰り返されている。本発明によるシステムは、これらの問題を自動的に訂正し、したがってユーザ・サポート時間を貴重な生産時間に転換することができ、また管理者が適時のサポート・コールの時間から解放される。本システムは、各事象ごとに適切な訂正手順を決定するために、存在するアラートを分析し、推量作業なしにネットワーク管理者に即時解決を提供する。本発明は、ワークステーション上の問題を訂正するために２つ以上のコマンドまたはトリガから構成される手順をエージェントに送る能力を含めて、いくつかの点で上述のＡｌｅｒｔＶＩＥＷ^{TM}の従来版と異なる。これは、本発明によるプログラムのフレキシビリティ、汎用性および能力が増大する利点を提供する。

本発明によるシステムでは、ユーザのプログラムを中断することなく、背景内で訂正処置を初期設定できる。対話式の分析および訂正は、本システムのアプリケーション制御パネルおよび遠隔アクセス特徴によってサポートされ、したがって管理者が簡単な手順によってユーザの機械を完全に制御することができる。アプリケーション制御パネルは、動作中のプログラムの表示、プログラムの開始／停止、およびシステム基準入力と出力のリダイレクトを含むエンド・ユーザの機械の様々な面をネットワーク管理者が管理コンソールを介して制御し、表示することができるユーザ・インタフェースを提供する。

例えば、ユーザは、ネットワーク管理者に印刷できないと苦情を言ってくることが多い。本発明によるシステムは、印刷問題を自動的に解決し、したがってネットワークおよびワークステーションのサポート・コールの単一の最も一般的な原因が事実上なくなる。エージェントは、使用できないプリンタを使用するユーザの試みを検出し、ネットワークを介してアラートを送ることによってその状態を報告する。その場合、システムの管理者が問題を積極的に訂正するのがユーザに見える。エージェントによりプリンタをリダイレクトすることによって、本システムは、ユーザをネットワーク・プリンタに自動的に接続し、ユーザに印刷を再試行するように求める。本システムは、印刷アラートのカスタマイズされたビューを提供し、それにより管理者が印刷セットアップを最適化でき、かつそれ以上の問題が防止できる。

ユーザがシステム・メッセージ「Ｔｏｏ　ｍａｎｙ　ｏｐｅｎ　ｆｉｌｅｓ」を受信した場合、他の例が発生する。複雑なデータベース尋問などプログラムがシステム・セットアップにおいて割り当てられているよりも多くのファイルを開いている場合、エージェントは、その状態がユーザに表示される前でもそれを検出する。本システムは「Ｔｏｏ　ｍａｎｙ　ｏｐｅｎ　ｆｉｌｅｓ」アラートをシステム管理者に報告し、システム管理者は、構成ファイルに対して適切な変更を行い、ワークステーションをリブートするようにエージェントを自動的にトリガすることによって状況を訂正する。これらの変更は永久的になるので、本システムではそれ以上の発生が自動的に防止される。

ネットワーク・オペレーティング・システムによる将来ユーザに対してアクセスを否定した場合、他の例が発生する。本発明によるシステムのエージェントは、各ワークステーション上のファイルアクティブを絶えず監視し、安全保護およびアクセス侵害が発生した際にそれらを検出する。本発明によるシステムのエージェントは、アクセスされたファイルおよび侵害の性質に関する明確な情報とともに各事象を報告する。本システムでは、ユーザがファイルへのアクセス権を得る前に、また実際にユーザの特権が侵害される前に、ネットワーク管理者が犯罪ワークステーションをフリーズまたは切り離しできるので、重大な安全保護侵害が継続するのが防止される。さらに、本システムは、すべての失敗したアクセス試みに関する詳細な情報をネットワーク管理者に提供することによって、アクセス問題が進行するのを防止する。

詳細な説明

本発明は、ネットワーク・プログラムの動作を管理する方法および装置に関する。好ましい実施形態によれば、本発明は、複数のソフトウェア・モジュールを使用して、監視タスク、管理タスクおよびログ・タスクを実行することによって実施される。

第１図は、本発明の一実施形態によるシステムのブロック図である。ネットワーク管理者は、管理コンソール１がそれにインストールされたコンピュータ（ネットワーク・サーバ端末でないことが好ましい）にアクセスできる。管理コンソール１は、モニタ２とマネー

ジャ４の２つの主要なモジュールから構成される。ネットワークは、複数のユーザ・ワークステーション１０を含む。各ワークステーション１０は、１つまたは複数のエンド・ユーザ・アプリケーション１２、オペレーティング・システム１６、通信ソフトウェア１８、およびネットワーク・オペレーティング・システム２０を含む。

第２図は、本発明に従って使用されるコンピュータ・システムのブロック図である。第２図のコンピュータ・システムは、ワークステーション・コンピュータおよび管理コンソール・コンピュータの例示の実施形態である。使用すべき管理コンソールおよびワークステーション・コンソールの特定の構成は、本発明の開示を一度得た当業者が修正することができる。コンピュータ４００は、メイン・セクション４０２（波線で示される）および周辺セクション４０４を含む。メイン・セクション４０２は、中央演算処理装置（ＣＰＵ）４０６、ハード・ディスク４０８、読取り専用メモリ（ＲＯＭ）４１０、ランダム・アクセス・メモリ（ＲＡＭ）４１２、および入出力（Ｉ／Ｏ）コントローラ４１４を含む。入出力（Ｉ／Ｏ）コントローラ４１４は、メイン・セクション４０２を周辺セクション４０４に接続する。周辺セクション４０４、一実施形態によれば、プリンタ４１６、カーソル・コントロール４１８、キーボード４２０、ビデオ・モニタ４２２、ＣＤ－ＲＯＭリーダ４２４、およびテープ・ドライブ４２６を含む。周辺機器は、メイン・セクションの構成要素と同様に、ユーザのニーズに応じて変更することができる。一実施形態によれば、本発明を実施する各種のルーチンおよびファイルは、ハードディスク４０８上に記憶され、ルーチンはＣＰＵ４０６によって実行される。カーソル制御装置４１８は、マウス、ペン、またはその他の任意の互換デバイスでよい。

第１図に戻ると、ネットワーク管理システム（ＮＭＳ）マップ・モジュール３は、モニタ２およびマネージャ４に接続されている。モジュール３は、ＮＯＶＥＬＬ™のネットワーク管理システム・マップ用のマッピング統合を行う。特に、ルーチンは、エージェントがワークステーション上で動作中であることを示すために、マップ上のアイコンの色を変更する。このモジュールは、ＮＭＳマップを変更するために、ネットワーク管理者によっていつでも動作できる。したがって、管理者は、ＮＭＳマップによって本発明によるシステムが提供する機能にアクセスできる。変更されたアイコンにアクセスした場合、モニタ／マネージャ・ユーザ・インタフェースなど、本発明によって得られる各管理者機能ごとにアイコンが表示される。

本発明によるシステムは、第１図に示されるワークステーション１０の各構成要素ならびに管理コンソール１と通信するエージェント１４を含む。エージェント１４は、異なる多数のプログラムからエラーを処置できる一般エージェント、またはある特定のプログラム内で発生しているエラーをアドレス指定するように設計された特定エージェントである。特定エージェントの一実施形態について以下に説明する。

また、それぞれＤＯＳ™、ＷＩＮＤＯＷＳ™、またはＯＳ／２™など特定のオペレーティング・システム用に設計された２つ以上の一般エージェント、またはそれぞれ異なるプログラムを処理するように設計された２つ以上の特定エージェントがワークステーション上で実行できる。すなわち、一般に、１つの一般エージェントだけが特定のワークステーション上でアクティブできる。しかしながら、多数のオペレーティング・システムを使用している場合、これ以外の例が発生する。ワークステーションがＤＯＳ™オペレーティング・システムとＷＩＮＤＯＷＳ™オペレーティング・システムの両方を動作させている場合、ＤＯＳ™エージェントもＷＩＮＤＯＷＳ™エージェントも同じワークステーション上でアクティブする。ＯＳ／２™、ＤＯＳ™またはＷＩＮＤＯＷＳ™を動作させているワークステーションの場合、これら３つのオペレーティング・システムに対して３つのエージェントが同時に実行できる。しかしながら、後者の状況では、ＯＳ／２™エージェントとＤＯＳ™エージェントは同じ通信プロトコルを使用しない。

本発明の開示に記載のエージェント１４は、例示の実施形態としてのＤＯＳ™エージェントを指す。しかしながら、上述のように、ＤＯＳ™、ＷＩＮＤＯＷＳ™またはＯＳ／２™の少なくとも異なる３つの一般エージェントが使用できる。すべての割込みおよびサービスについて説明している間、その環境内にのみこれらすべてのものが存在するので、本発

明の開示はＤＯＳ™を指す。しかしながら、ＷＩＮＤＯＷＳ™オペレーティング・システムはそのサービスの大部分についてＤＯＳ™に依存するので、同じＤＯＳ™エージェントは、例えば「ＡＣＣＥＳＳ　ＤＥＮＩＥＤ」問題または「ＦＩＬＥ　ＮＯＴ　ＦＯＵＮＤ」問題をＷＩＮＤＯＷＳ™アプリケーション内で同様に検出できる。ＷＩＮＤＯＷＳ™エージェントは、ＤＯＳ™エージェントが実行できない機能についてＤＯＳ™エージェントを補足する。これらの機能は、ＷＩＮＤＯＷＳ™アプリケーションの名前を決定し、それらをＤＯＳ™エージェントに供給すること、ＷＩＮＤＯＷＳ™アプリケーションの開始と停止を実行すること、重要なＷＩＮＤＯＷＳ™資源利用を監視すること、およびＷＩＮＤＯＷＳ™アプリケーションの一般保護トラップを監視することを含む。ＷＩＮＤＯＷＳ™エージェントは、このようなすべての情報をＤＯＳ™エージェントに供給する。ＯＳ／２™エージェントは、重要割込みをインタセプトする代わりに、システムまたは通信ダイナミック・リンク・ライブラリ（ＤＬＬ）をインタセプトする点がＤＯＳ™エージェントおよびＷＩＮＤＯＷＳ™エージェントと異なる。しかしながら、一般に、２つの一般エージェントの構成は同じである。本発明の一実施形態によれば、異なる一般エージェントは、Ｆ２ｈ割込みなど所定の割込みを使用して、それら自体の間で内部通信できる。

エージェント１４は、アプリケーションおよびオペレーティング・システムを監視し、割込みが発生した場合、その割り込みをフックまたはトラップし、エラー状態が存在するかを決定する。エラー状態が存在する場合、そのエラーはアラートとして記録され、このアラートがモニタ２へ報告される。アラートは、エージェントによってモニタ２へ送られ、問題の種類、問題が発生したワークステーション、エラーを引き起こしたプログラムの名前、および推奨される訂正処置の識別を含む。この推奨される処置は、それを実行する前に管理者によって変更できる。

本発明の一実施形態に従ってトラップされる割込みのリストを表１に示す。

表１

割込み	処　置
割込み２Ｆｈ	ＤＯＳ™およびＷＩＮＤＯＷＳ™用のマルチプレクサ
割込み１３ｈ	ハード・ディスク・ハンドラ
割込み２１ｈ	ＤＯＳ™およびＷＩＮＤＯＷＳ™オペレーティング・システム・サービス・コール
割込み ＮＯＶＥＬＬ™２１ｈ	ＮＯＶＥＬＬ™ＤＯＳ™シェル・サービス
割込み２４ｈ	重要エラー・ハンドラ
割込み５Ｃｈ	ＮｅｔＢＩＯＳ™通信サービス
割込み１７ｈ	プリンタ・インタフェース
割込み７Ｂｈ	ＮＯＶＥＬＬ™　Ｂｔｒｉｅｖｅサービス
割込み０８ｈ	タイマ・ハンドラ
割込み２８ｈ	アイドル・ハンドラ
割込み０９ｈ	キーボード
割込み１６ｈ	キーボード・バッファ・インタフェース
任意のＩＰＸ™／ ＳＰＸ™コール	ＮＯＶＥＬＬ™からのＩＰＸ割込み
NOSおよびOS/2™の 通信ＤＬＬ	

一般に、モニタ２はエージェント１４から来たすべてのアラートをログし、かつ報告し、マネージャ４は各ワークステーション１０上でエージェント１４の動作を監視し、制御する。さらに、モニタ２は、特定のアラートがワークステーション１０にいずれかによって報告された場合に、動作の要求をマネージャ４に伝達する。また、モニタ２は、スケジュール９が手順を実行する明確な時刻が到来したことを示した場合に、エージェント１４に対してとるべき処置の要求をマネージャ４に伝達する。マネージャ４は、制御された（または管理された）ワークステーション１０と通信し、具体的には、セット・オペレーションまたはゲット・オペレーションを介してエージェント１４と通信する。セット・オペレーションでは、ワークステーション上で何らかの動作を実行するために、コマンドをマネージャ４からエージェント１４へ送る必要があり、ゲット・オペレーションでは、情報をマネージャへ送り返すよう要求するために、コマンドまたは手順をマネージャ４からエージェント１４へ送る必要がある。これらについては後で詳細に検討する。

一実施形態によれば、ネットワーク管理者は、（第４図に示される）ユーザ・インタフェース５２を介して使用可能情報のサブセットを所与の時刻において閲覧できるように、管理コンソール１をセットアップすることができる。特に、管理者は、ネットワーク内のいくつかのまたはすべてのワークステーションからの様々なアラートを表示する１つまたは複数の事象ビュー６をセットアップすることができる。例えば、１つの可能なビューは、任意のワークステーション上で動作中のＷＯＲＤＰＥＲＦＥＣＴ™アプリケーション内で発生しているすべてのアラートを示す。さらに、管理者は、ネットワーク統計に関する情報を表示する１つまたは複数の統計ビュー７をセットアップすることができる。特に、統

計ビュー７は、プログラム障害またはアラート統計に関する情報、例えば、プログラムが何回開始されたか、何種類の異なる事象がプログラム内に発生したか（例えば、特定のプログラム中または特定のワークステーション上で「Ｔｏｏ　ｍａｎｙ　ｆｉｌｅｓ　ｏｐｅｎ」が何回発生したか）などを表示する。
また、管理者は、１つまたは複数のトリガ８を訂正手順の形でいずれかのビューに付加できる。特に、トリガは、モニタ２からマネージャ４に送られ、次いでエージェント１４に送られて、一般にエージェントに処置をとらせる特定のコマンドである。例えば、ＷＯＲＤＰＥＲＦＥＣＴ™アプリケーションに関して問題が検出された場合、本システムは、適切なビューにアクセスし、故障したアプリケーションを動作させているワークステーションにフリーズ・ワークステーション・トリガを送る。
トリガ８は、一実施形態によれば、（実際にはＷＩＮＤＯＷＳ™のＤＬＬである）トリガ・ライブラリと呼ばれるモジュール内に記憶される記憶トリガを表す。１つのトリガ・ライブラリは２つ以上のトリガを含む。いくつかのトリガ・ライブラリは、種々の目的で本システムを具備する。１つのトリガは、トリガ・ライブラリ内に記憶される機能（またはコマンド）であり、モニタ２によって手順の一部として自動的に実行するようにコールされる。トリガは、訂正手順がアラートに応答して実行された場合か、またはスケジュール手順がスケジュール・モジュール９００によってセットアップされた所望の時刻において実行された場合の２つの場合に自動的にコールされる。
表２は、本発明の一実施形態に従う手順に含まれる定義済みトリガのリストである。表２の第１の列内の番号はこの説明のためのものにすぎず、プログラミング重要度を持たない。
定義済みトリガは、上述のように、メモリ例えばハード・ディスク４０８またはＲＯＭ４１０に記憶されたトリガ・ライブラリ内に記憶される。また、ネットワーク管理者は、モニタ・メニュー・ユーザ・インタフェース５２からセットアップ・トリガ・オプションを選択することによって、カスタム・トリガをセットアップし、設計することができる。これらのカスタム・トリガは、ＮＯＲＴＯＮ™ユーティリティなど使用可能プログラムを実行するためのコマンドである。あるいは、管理者は、ソフトウェア開発者のキットを使用して、所望の機能を実行する新しいプログラムを書くことによって新しいカスタム・トリガを生成することができる。

表２

エージェントへ送るべきトリガのリスト	
1	ＣＯＮＦＩＧ．ＳＹＳ内のファイルを変更する
2	ＡＵＴＯＥＸＥＣ．ＢＡＴへラインを追加する
3	ドライバをインストールする
4	ディスクを検査する
5	メッセージを送る
6	キーストローク・ジョブを送る
7	プログラムを開始する
8	プログラムを停止する
9	ＳＮＭＰトラップを送る
１０	モデム／ｃｃ：メイル／ページャを介してアラートを送る
１１	ワークステーションをフリーズする
１２	ワークステーションをリブートする
１３	ローカル・ワークステーション上でプログラムを動作させる
１４	ワークステーションをアンフリーズする
１５	ｎｍｓアラートを発生させる
１６	ファイルをコピーする
１７	最後のドライブをセットする
１８	ディスク・バッファをセットする

表３は、本発明の他の実施形態に従って使用できる追加のトリガのリストである。再び、表３の第１の列内の番号は説明のためのものにすぎず、プログラミング重要度を持たない。

表３

エージェントへ送るべきトリガのリスト	
１９	名前によってプログラムを停止する
２０	休止する
２１	故障したプログラムを停止する
２２	ＮＣＢの数をセットする
２３	データベース、テキストまたはプリンタ・ファイルにアラートをコピーする

表２および表３中のリストは、説明を簡単にするために共に説明するが、訂正手順またはスケジュール手順に含まれる可能なトリガの種類のリストである。これらのリストは、徹底的という意味ではなく、実行できる動作の種類の例である。その他のトリガの実施は、本発明の開示を一度得た当業者の技術の範囲内に入る。

トリガ１では、ＣＯＮＦＩＧ．ＳＹＳファイル内の指定された数のファイルを変更するようにマネージャ４がエージェント１４に通知する。このトリガは、例えば、割込み２１ｈからのエラー・コードの検出に応答して、プログラムが前に指定されたよりも多くのファイル・オープンを必要とすることを示すアラートをエージェントが示した場合に実施される。トリガ２では、アラートの発生を引き起こす問題を必要に応じて訂正するためにＡＵＴＯＥＸＥＣ．ＢＡＴファイルを修正するようにマネージャ４がエージェント１４に通知する。トリガ３では、アラートが発生したワークステーションにおいてスタートアップ手順中にドライバをインストールするようにマネージャ４がエージェント１４に通知する。例えば、プリンタまたはマウス・ドライバが無くなり、特定のプログラムによって必要とされている場合、無くなったドライバをインストールするトリガを実行する。トリガ４では、スケジュール時刻か、または重大なディスク・エラーが報告された時に不良セクタまたはスポットについてディスクを検査するようにマネージャ４がエージェント１４に通知する。

トリガ５では、マネージャ４がネットワーク内のいずれかのワークステーションにメッセージを送る。トリガ６では、マネージャ４が、キーストローク・ジョブ、すなわち実行のための一連のキーストロークを特定のワークステーション上のエージェント１４へ送る。トリガ７およびトリガ８では、プログラムを開始するようにまたは前景内で現在実行中のプログラムを停止するようにマネージャ４がエージェント１４に通知する。

トリガ１９では、特定のプログラムを名前によって停止するようにマネージャ４がエージェント１４に通知する。このトリガは、ワークステーションの背景動作において実行中のプログラムを停止するのに有用である。トリガ２１では、故障したプログラム、すなわちアラートが発生した場合に実行中であったプログラムを停止するようにマネージャ４がエージェント１４に通知する。

トリガ９では、マネージャ４がシンプル・ネットワーク管理プログラム（ＳＮＭＰ）トラップを送る。すなわち、ネットワークがＳＮＭＰ管理コンソールを有する場合、トラップまたはアラートをそのコンソールに送り、それにエラーについて通知する。トリガ１０では、マネージャが他の電子媒体を介してアラートを転送し、ネットワークに接続されていない位置への問題通知を行う。トリガ１１は、アラートを引き起こした問題が修正されるまでワークステーションをフリーズして、それ以上の問題を防止する。次いで、問題が訂正された場合、トリガ１４を使用して、ワークステーションをアンフリーズする。

トリガ１２では、必要に応じてワークステーションをリブートするようにマネージャ４がエージェント１４に通知する。例えば、ＡＵＴＯＥＸＥＣ．ＢＡＴファイルまたはＣＯＮ

ＦＩＧ．ＳＹＳファイルがトリガ１およびトリガ２によって変更されている場合、リブート・トリガを実行すると、その変更が有効になる。トリガ１３では、ワークステーション上で特定のプログラムを動作させるようにマネージャ４がエージェント１４に通知し、音声アラームまたは視覚的アラームによってカスタム通知などの処置をサポートする。トリガ１５では、マネージャ４がＮＯＶＥＬＬ™管理システム（ＮＭＳ）アラームを発生させて、ワークステーション上でアラートが発生したことをＮＯＶＥＬＬ™管理システムに通知する。

トリガ１６では、アラートを発生したワークステーションにファイルをコピーするようにマネージャ４がエージェント１４に通知して、必要に応じて問題を訂正する。例えば、デバイス・ドライバ、プログラム・モジュールまたはデータ・ファイルをワークステーションへ転送する。トリガ１７では、ＣＯＮＦＩＧ．ＳＹＳ内の最後のドライブをセットするようにマネージャ４がエージェント１４に通知する。トリガ１８では、ＣＯＮＦＩＧ．ＳＹＳ内のディスク・バッファの数をセットするようにマネージャ４がエージェント１４に通知する。

トリガ２０では、マネージャ４がある期間手順を休止させる。これは、ワークステーションが手順の一部を完了するまで待機するのに使用できる。トリガ２２では、ＣＯＮＦＩＧ．ＳＹＳ内のネットワーク制御ブロック（ＮＣＢ）の数をセットするようにマネージャ４がエージェント１４に通知する。これは、ＮｅｔＢＩＯＳ™に関する問題、具体的には割込み５Ｃｈに応答して使用される。トリガ２３では、アラートが検討または記憶のためにデータベース、テキストまたはプリンタ・ファイルにコピーされる。

第１図に戻ると、自動手順５は、１つまたは複数のトリガ・ライブラリから選択した指定パラメータを有する一組のトリガから構成されるネットワーク管理者によってセットアップされる。この手順はそれぞれ、事象に応答してまたはスケジュール時刻において順に実行される１つまたは複数のトリガから構成される。したがって、そのような手順は、事象ビュー６かまたはスケジュール９に付加できる。第１の例では、手順は訂正手順と呼ばれる。第２の例では、手順はスケジュール手順と呼ばれる。もちろん、同じ手順を訂正手順としてもスケジュール手順としても使用できる。

手順中のトリガは、それらの関連するパラメータとともに表２および表３に記載されたトリガのうちの１つであるか、またはカスタム・トリガである。例えば、パラメータ５０を供給された「ｃｈａｎｇｅ　ＦＩＬＥＳ　ｉｎ　ＣＯＮＦＩＧ．ＳＹＳ」は、ＣＯＮＦＩＧ．ＳＹＳファイル内にＦＩＬＥＳ＝５０をセットするコマンドになる。このようにして、表２および表３は、手順を組み立てるためのコマンドを記載する。

いずれにせよ、モニタ２は、トリガが含まれている手順に従ってトリガを自動的にかつ連続的にコールする。一実施形態によれば、手順は、ワークステーション上の背景内で実行され、したがってワークステーションのユーザには見えない。モニタ２は、訂正手順がそれに関連する事象ビューに新しいアラートが到達した場合に、訂正手順からすべてのトリガをコールする。モニタ２は、スケジュール手順において指定された時間間隔が経過した場合にスケジュール手順からトリガをコールする。

スケジュール９は、手順が所望の時刻においていずれかのワークステーション上で動作するように、管理者によってセットアップできる。例えば、ディスク検査手順４、バックアップ機能およびデータベース保守機能は、その週または月、およびセットした時刻が与えられた後の自動ワークステーション・ログオフの間のスケジュール時刻において動作できる。

第３図は、本発明の一実施形態による一般エージェント１４のブロック図である。プログラム２１モジュールは、エージェント、特に第１図に示されるエンド・ユーザ・アプリケーション１２、オペレーティング・システム１６、通信ソフトウェア１８、およびネットワーク・オペレーティング・システム２０を除いて、ワークステーション内のすべての機能ブロックを含む。プログラム２１が一般エージェント１４と通信する方法には、アプリケーション・プログラマ・インタフェース（ＡＰＩ）を介するかプローブ・モジュール32_nを介するかの２通りがある。プログラム２１は、エラー状態が発生した場合にＡＰＩ

を介してアラートをディスパッチャ２４に送るモジュール２２を介してエージェント１４と通信する。また、プログラム２１は、その機能について以下に説明する各プローブ・モジュール32_i，32_{i+1}．．．32_nに接続されている。

ディスパッチャ２４は、ＡＰＩモジュール２２、受信機モジュール３４または「制御」モジュール２６から受信した通信に基づいてエージェント内で実行すべき機能を決定する意志決定手順である。ディスパッチャ２４は、決定を行った後、エージェント制御モジュール２６にコマンドを送る。エージェント制御モジュール２６は、エージェント・エンジン・モジュール２８によってエージェントの動作を制御する。特に、一般エージェント１４は、オペレーティング・システムまたはワークステーション上で、プログラムの開始、ファイルの変更、キーボードのフリーズ、メッセージの表示など処置を実行するようにトリガによって命令される。エージェント制御モジュール２６は、ワークステーション上でこれらの機能を実行する。プローブ・モジュール32_i、32_{i+1}．．．32_nは、割込みをフックするのに使用される。本システムによって処理されるすべての割込みにプローブ・モジュール32_iがある。エージェント・エンジン・モジュール２８は、プローブ・モジュール32_iから受け取った事象の処理を実行し、実際のアラートをエージェント制御モジュール２６を介してネットワーク１００を通ってモニタ２へ導く。

プログラム２１が「ｓｅｎｄ　ａｌｅｒｔ　ＡＰＩ」モジュール２２を介してエージェント１４にアクセスした場合、プログラム２１は、特定のアプリケーション・アラートを実際に生成し送る。特に、エージェント１４は、どんなプログラムにも起こりうる一般的なエラーを検出する。また、エージェントは、任意のプログラムに特定のアラートを生成させ、それをエージェント１４を介してモニタ２に送るＡＰＩ（ｓｅｎｄ　ａｌｅｒｔ　ＡＰＩ）を提供する。例えば、ＷＯＲＤＰＥＲＦＥＣＴ™アプリケーションは、このＡＰＩを使用して、「Ｐａｒａｇｒａｐｈ　ｆｏｒｍａｔｔｉｎｇ　ｅｒｒｏｒ」に関するアラートを送ることができる。エージェント１４は、このアラートをネットワークへ伝送し、さらに本システムによって処理するためにモニタ２へ伝送する。この場合については上述した。しかしながら、ユーザ・プログラムがプローブ32_nを介して間接的に一般エージェント１４にアクセスすることもできる。プログラムがオペレーティング・システムまたは他の任意のシステム・サービスをコールした場合、エージェント１４のプローブ32_nは制御権を得る。この処理について第７図に関して以下に説明する。

受信機モジュール３４および送信機モジュール３６は、ネットワーク１００と通信するためにエージェント１４によって使用される。受信機モジュール３４および送信機モジュール３６は、ネットワーク・カードの通信ソフトウェアとインタフェースする。一実施形態によれば、受信機モジュールおよび送信機モジュールは、４つのネットワーク通信プロトコルＩＰＸ™、ＮｅｔＢＩＯＳ™、ＤＬＣ™８０２．２、ＴＣＰ／ＩＰ™のうちのいずれか１つを使用して通信できる。現在周知であるかまたは将来開発される他のプロトコルを使用して通信する能力を提供することは、当業者の技術の範囲内に入る。

エージェント自動発見（オートディスカバリ）モジュール３８は、マネージャ４による新たにアクティブ化したエージェント１４の自動発見を容易にするために送信機３６および受信機３４と通信するので、ネットワーク管理者が各ユーザを手動で画定する退屈なプロセスを実行する必要がない。オートディスカバリ・モジュール３８は、マネージャ４によって発見されるべき新たにアクティブ化したエージェント１４の識別パケットをマネージャ４に送る。この送信は、新しいエージェントがアクティブ化した時に行われ、その後、オートディスカバリ・モジュール３８がマネージャ４から新たにアクティブ化したエージェントを発見したという確認を受け取るまで所定の間隔で行われる。一実施形態によれば、所定の間隔は約６０秒である。

第４図は、本発明の一実施形態によるモニタ２のブロック図である。モニタ２は、ネットワーク１００を通して個々のワークステーション上の一般エージェントおよび特定エージェントと通信する。情報は、ネットワーク１００から受信機４０を通って受信される。一実施形態によれば、受信機４０は、受信機３４に関して上記の能力を有する。特に、受信機は、４つのネットワーク通信プロトコルのいずれか１つを使用して通信できる。もちろ

ん、受信機４０は、代わりにプロトコルの１つを使用してのみ通信できるようにすることができる。受信機４０は、ネットワーク１００から受け取ったアラートを事象ログ・マネージャ・モジュール４２へ伝送する。モニタ２から受け取ったアラートはすべて事象ログ・マネージャ・モジュール４２によって事象ログ・データベース４４内に記憶される。事象ログ・マネージャ・モジュール４２は、データをＤＢＡＳＥ™フォーマットまたは他のいくつかのデータベース・フォーマットにエクスポートできる。

本発明の一実施形態によれば、事象ログ・データベース４４は、それぞれ表４および表６に示される２つのファイル、事象詳細ファイル、および事象索引ファイルから構成される。表５はアラート詳細構造を示す。事象詳細ファイルは可変長レコードを含み、事象索引ファイルは固定長レコードを含む。

表４

サイズ	フィールド名
ワード	ａｌｅｒｔ＿ｏｒｄ
ｅｖｎｉｄｘ	ａｌｅｒｔ＿ｉｄｘ
バイト	ａｌｅｒｔ＿ｄｅｔ［ｍａｘｄｅｔａｉｌ］

表５

２ｂ	詳細長	２ｂ
詳細長＋４	アラートＳＮＡサブベクトル	詳細長＋４

表６

サイズ	フィールド名
バイト	ｒｉ＿ｔｙｐｅ
バイト	ｒｉ＿ｒｅｓｅｒｖ
長い整数	ｒｉ＿ｄｅｔ＿ｏｆｆ
ワード	ｒｉ＿ｄｅｔ＿ｌｅｎ
ワード	ｒｉ＿ｉｄｘ
ワード	ｒｉ＿ｉｄｘｉｄ
バイト	ｒｉ＿ｇｔｙｐｅ
バイト	ｒｉ＿ｔｉｍｅ［３］
バイト	ｒｉ＿ｄｅｔａ［３］
バイト	ｒｉ＿ａｄａｐｔｅｒ［ｍａｃａｄｄｒ＿ｓｉｚｅ］
ワード	ｒｉ＿ｓｅｇｍｅｎｔ
バイト	ｒｉ＿ｐｒｏｎａｍｅ［ｐｒｏｎａｍｅ＿ｓｉｚｅ］
バイト	ｒｉ＿ｒｅｓｎａｍｅ［ｒｅｓｎａｍｅ＿ｓｉｚｅ］
バイト	ｒｉ＿ｒｅｓｔｙｐｅ

表４において、１バイトから構成されるａｌｅｒｔ＿ｏｒｄフィールドは、各アラートごとに一意のアラート序数を記憶する。ａｌｅｒｔ＿ｉｄｘフィールドは、事象索引レコードのサイズに等しいサイズｅｖｎｉｄｘを有する表６のアラート・キー・フィールドを含む。ｍａｘｄｅｔａｉｌのフィールド・サイズを有するａｌｅｒｔ＿ｄｅｔフィールドは、表５に示されるレイアウト内にアラート詳細を含む。特に、最初の２バイトと最後の２バイトは詳細長＋４バイトを含み、中央「詳細長」バイトはアラートＳＮＡサブベクトルから構成される。ＳＮＡサブベクトルは、ＩＢＭによってネットワーク内でアラート用に使用されるＳＮＡネットワーク管理ベクトル転送（ＮＭＶＴ）システムを指す。

表６において、ｒｉ＿ｔｙｐｅフィールドは、レコード・タイプを識別するためのレコード・タイプ・フィールドである。特に、本発明の一実施形態によれば、このデータベース内のレコードの大部分は、エージェントによって報告された事象である。レコードのいくつかはモニタによって発生する。この後者のタイプの事象の例は、ネットワーク内の輻輳である。これらのタイプのレコードのどれかがレコード・タイプ・フィールドによって識別される。ｒｉ＿ｒｅｓｅｒｖフィールドは、将来の使用のために保留される。ｒｉ＿ｄｅｔ＿ｏｆｆフィールドは、詳細レコード・オフセット、すなわち事象詳細ファイル内の位置である。ｒｉ＿ｄｅｔ＿ｌｅｎファイルは詳細レコード長である。

ｒｉ＿ｉｄｘは、アラートを識別するのに使用されるテキスト記述を表す各アラートに割り当てられた６進数である。各可能なアラートごとのｒｉ＿ｉｄｘ値はすべて、別個のデータベース内に記憶され、このデータベースはｒｉ＿ｉｄｉｘ値によって索引付けされる。したがって、ｒｉ＿ｉｄｉｘ値は、（第５図の）ユーザ・データベース７４の一部であるインデックス・データベース内の特定のアラート・エントリを指す索引番号である。

ｒｉ＿ｇｔｙｐｅフィールドは、報告されたアラートをフィルタリングするのに使用されるタイプの事象を含む。ｒｉ＿ｔｉｍｅフィールドおよびｒｉ＿ｄａｔｅフィールドは、

アラートを引き起こした事象が発生した時刻および日付を示す。ｒｉ＿ａｄａｐｔｅｒフィールドは、アラートが発生したワークステーションの実際のアドレスを表すアダプタ番号を含む。ｒｉ＿ｓｅｇｍｅｎｔフィールドは、ワークステーションがあるネットワークのセグメントを示すセグメント番号である。ｒｉ＿ｐｒｏｎａｍｅフィールドは、フィールドを引き起こしたプログラムの製品名を示す。ｒｉ＿ｒｅｓｎａｍｅフィールドは、アダプタ番号に対応するワークステーションのユーザ名である。ｒｉ＿ｒｅｓｔｙｐｅフィールドは、アラートが発生した場合に使用される資源、例えばプリンタやその他のシステム構成要素の名前である。

以下に説明する手順マネージャ５４によって維持されるメッセージ・ログ・データベース４５が備えられている。メッセージ・ログ・データベース４５は、データベースのサイズを示しかつモジュールの動作をサポートするトリガの結果、すなわち事象やトリガなどのカウンタを含む。メッセージ・ログ・データベース４５の内容は、ユーザ・インタフェース５２を介して管理者に表示される。

統計ビュー・モジュール７００は、所望の統計ビュー７を生成、修正、削除およびアクセスするために、ユーザ・インタフェース５２を介してエンド・ユーザ５０によってアクセスされる。事象ビュー・モジュール６００は、所望の事象ビュー６を生成、修正、削除およびアクセスするために、ユーザ、インタフェース５２を介してアクセスされる。さらに、スケジューリング・モジュール９００は、マネージャ４によって所望の時刻においてワークステーション上で実行されるべきエージェントに送るべきスケジュール手順を生成、修正、削除およびアクセスするために、ユーザ・インタフェース５２を介してアクセスされる。

事象ログ・マネージャ・モジュール４２は、各アラートを事象リスト・マネージャ・モジュール４６へ伝達する。このモジュール４６は、各新しい事象を読み取り、モジュール４６が選択した統計ビュー７または事象ビュー６内で要求されていない事象またはアラートをフィルタリングにより除去した後、管理コンソール１が管理者によってセットアップされたビューの１つの中に常駐するコンピュータのディスプレイ上にそれを表示する。

トリガ・マネージャ・モジュール５６では、管理者がカスタム・トリガを生成、修正、および削除することを含めて、カスタム・トリガを管理することができる。訂正手順モジュール５８では、上述のように、１つまたは複数のトリガ（定義済みトリガかまたはカスタム・トリガ）を含む手順を生成することができる。

手順マネージャ・モジュール５４は、事象ビュー・モジュール６００およびスケジュール・モジュール９００からの出力をとり、アラートに応答してスケジュールまたは選択した事象ビューと関連するマネージャ４に送るべき１つまたは複数の手順を選択する。特に、手順マネージャ・モジュール５４は、報告されたアラートに割り当てられたビューに割り当てられた訂正手順を選出し、その訂正手順を実行のためにマネージャ４に送る。もちろん、２つ以上のビューに１つのアラートを割り当てること、および２つ以上の訂正手順を任意のビューに割り当てることができる。さらに、手順マネージャ５４は、スケジュール時刻においてスケジュール手順を選出し、それを実行のためにマネージャ４に送る。

第５図は、本発明の一実施形態によるマネージャ４のブロック図である。ネットワーク１００は、エージェント１４とともに使用する第３図に示される受信機３４および送信機３６に関して上述したタイプの受信機６２および送信機６４を介してマネージャ４と通信する。受信機６２および送信機６４はディスパッチャ６０と通信する。ディスパッチャ６０は、第３図に示されるディスパッチャ２４に関して上述したのと同じタイプのものである。モニタ2およびマネージャ・カーネル６７は、ＡＰＩインタフェース６６を介してディスパッチャ６０と通信する。マネージャ・カーネル６７は、トリガリング事象が発生した際に訂正手段においてトリガ・セットアップを実行し、所望の時刻においてスケジュール手順を実行する。これについて、第１１図と関連して以下に説明する。

エンド・ユーザ５０は、ユーザ・インタフェース５２を介してマネージャ４と通信する。ディスパッチャ６０は、メニュー・システム６８と通信する。また、ユーザ・インタフェース５２は、管理者がそれを介して実行すべき機能を選択するメニュー・システム６８と

通信する。メニュー・システム６８では、事象テーブル・マネージャ及びエディタ７０、情報マネージャ７２、エージェント監視モジュール８０、遠隔アクセス・モジュール８２、セットアップ管理モジュール８４にアクセスできる。
事象テーブル・マネージャ及びエディタ７０では、管理者が事象テーブルを編集および管理することができる。事象テーブルは、報告すべき事象の仕様である。これらのテーブルは、各種の制御機能、最も重要なことにネットワークを介して報告すべき事象を決定するためのマスキング仕様を指定する。情報マネージャ７２では、管理者がいくつかのデータベース７４、７６および７８のいずれかにアクセスすることができる。ユーザ・データベース７４は、エージェントに関する情報、すなわちワークステーション上のエージェントのセットアップに関する情報を記憶する。特に、ユーザ・データベース７４は、ログイン名、およびアドレス、マスクおよびエージェント制御パラメータを記憶する。また、ユーザ・データベースは、上述のように各アラートごとに索引番号によって索引付けされた索引定義を記憶する。インベントリ構成データベース７６は、各ワークステーションの構成に関する情報を記憶する。特に、この情報は、機械のタイプ、プロセッサ・タイプ、メモリ・サイズなどから構成される。セットアップ・データベース７８は、マネージャ４のカスタマイズされたセットアップ構成を記憶する。特に、セットアップ・データベース７８は、データベース・ファイルの位置、それを使用して作業する事象テーブルのセット、テキストに使用されるフォントなど、マネージャ４用の共通パラメータの集合を記憶する。
また、メニュー・システム６８には、アプリケーション制御モジュール（ＡＣＰ）５７も接続されている。ＡＣＰ５７では、現在遠隔ワークステーション内にロードされている管理者がすべてのプログラム、デバイス・ドライバおよびＴＳＲを閲覧することができる。さらに、ＡＣＰ５７は、遠隔ワークステーション内で実行中のユーザ・アプリケーションの背景動作中にプログラムを開始および停止する。特に、プログラムが遠隔ワークステーション上で実行されている場合、ＡＣＰ５７は、ワークステーションの前景動作中に実行されているプログラムの実行を停止または休止させることなく、背景内のワークステーションのキャプチャを開始／実行することができる。ＡＣＰ５７を使用して、管理者は、エンド・ユーザのワークステーションの制御権を得ることによりエンド・ユーザを妨害することなく、背景内の更新／ビュー遠隔ワークステーション上の任意の構成ファイルを閲覧または更新することができる。
これは、ＤＯＳ™、ＷＩＮＤＯＷＳ™、またはＯＳ／２™の場合とわずかに異なって達成される。ＤＯＳ™の場合、ＡＣＰ５７は、マルチタスク・オペレーティング・システムではないので、非ドキュメント・バックドア特徴を使用する。特に、ＡＣＰ５７は、バックドアと呼ばれるハンドルを介してＤＯＳ™へのアクセス権を得、変更を行うために背景アプリケーションを開始し、バックドアを閉じ、制御権を前景アプリケーションに戻す。ＷＩＮＤＯＷＳ™の場合、第２のタスクが背景内で開始され、それが前景アプリケーションと共存できるように新しいタスクの焦点がセットされる。ＯＳ／２™の場合、手順は同じであるが、タスクはプロセスと呼ばれる。
エージェント監視モジュール８０は、ネットワーク内のワークステーション上のエージェントの挙動の監視を実行する。エージェント監視モジュール８０は、ユーザがネットワーク上に登録するのを検出するオートディスカバリ・モジュール３８と関連して作動し、マネージャ４用のアクティブエージェントに関する情報を維持し、また未定義のアクティブエージェントを識別する（オートディスカバリ）。遠隔アクセス・モジュール８２では、管理コンソールが各ワークステーションへ遠隔アクセスすることができる。すなわち、管理コンソールは、個人ワークステーションの「マスター」になる。このようにして、管理者は各ワークステーション上の動作を直接制御することができる。特に、遠隔アクセス・モジュール８２は、各ワークステーションのスクリーン、キーボード、およびマウスを周知の方法で直接制御することができる。セットアップ管理モジュール８４は、マネージャのセットアップを制御し、したがってセットアップ・データベース７８に接続される。
第６図は、本発明の一実施形態による一般エージェント・プログラムの初期段階を実行するルーチンの流れ図である。エージェントがワークステーション上で開始された場合はい

つでもこのルーチンを実行する。まず、一般エージェントをＴＳＲプログラムとしてロードする（エージェントをロードする）。
ステップ１０２において初期設定を開始する。コマンド・ラインを解析し、ルーチンは、エージェントがロードされているかどうか検査する。さらに、ルーチンは、ネットワークおよびネットワーク・プロトコルの存在を検査し、必要に応じてネットワークおよびＯＳ／ＮＯＳ資源を割り当てる。
ＮＯＶＥＬＬ™ネットワーク上の本発明によるプログラムは、ファイル・サーバ・ログイン・スクリプトを介してファイル・サーバ上に自動的にインストールされる。したがって、ＮＯＶＥＬＬ™ネットワークでは、ハード・ドライブ内のプログラムを各ワークステーション上にインストールする必要はない。ユーザがその人のワークステーションにログインした場合、本発明によるプログラムはワークステーション上に自動的にダウンロードされる。通常どおり、ＮＯＶＥＬＬ™ログイン・スクリプトでは、ユーザがログインした場合にバッチ・ファイルをワークステーション上で実行することはできるが、ＮＯＶＥＬＬ™ログインは終了時にメモリを自動的にクリアするので、終了後常駐型（ＴＳＲ）プログラムを実行することはできない。本発明による導入プログラムは、ＮＯＶＥＬＬ™終了ログインによって触れられないメモリの保護領域内にロードすべきＴＳＲのスタンプを押すログイン・スクリプト内で実行される「ｔｓｒロード」モジュールを含む。その場合、ログイン・スクリプトが終了した場合、導入プログラムは、ＤＯＳから制御権を受け取り、保護領域にアクセスし、ＴＳＲおよびそのパラメータを受け取り、それらをクリーンなメモリ内にロードする。
ステップ１０２における初期設定が成功した場合、ステップ１０４においてマネージャへの接続を開始する。接続要求を送る。エージェントは、マネージャからの応答を待ち、次いで事象テーブル・セットアップおよびエージェント・パラメータをロードする。事象テーブル・セットアップおよびエージェント・パラメータは、ユーザ・データベース７４からメモリ常駐エージェント・データベース３０へダウンロードされる。事象テーブル・セットアップは、ネットワーク上の事象の報告を制御するフィルタの仕様を含む。エージェント・パラメータは、例えば、ワークステーションのフリーズ／アンフリーズ状態など、フィルタ・セットアップ以外のエージェントに関する状態および制御情報を含む。
この動作が成功した場合、ステップ１０６においてエージェントをインストールする。特に、表１に記載されている割込みをセットアップし、エージェントは、通常ワークステーション上に存在する割込みの代わりに表１に記載されている割込みを使用する。このようにして、プログラムが表１中のリスト上の１つに対応する割込みをコールした場合はいつでもエージェントは制御権を得る、換言すれば、割込みをフックまたはトラップし、置換された命令を実行する。戻りコードを検査し、割込み動作が失敗した場合、アラートを故障の報告とともにモニタ２に送る。ステップ１０６では、また、エージェントは、ワークステーション環境情報を得、拡張メモリ・システム（ＥＭＳ）サポートをインストールし、ＡＰＩインタフェースをインストールする。
ステップ１０６においてエージェントの導入が成功した場合、ステップ１０８において開始が成功している。すべての手順を開始し、ソフトウェア割込みへのフックを使用可能にする。最後に、ＯＳコマンド割込みに戻る。
ステップ１０２、１０４および１０６における動作のいずれか１つが失敗した場合、ステップ１１０において失敗メッセージを印刷する。特に、ステップ１０２が失敗した場合、「初期設定失敗」メッセージを送る。ステップ１０４が失敗した場合、「開始失敗」メッセージを送る。最後に、ステップ１０６が失敗した場合、「インストール失敗」メッセージを送る。
第７図は、本発明の一実施形態による一般エージェント・プログラムの動作段階についてのルーチンの流れ図である。ステップ１１２において、エンド・ユーザ・プログラムがＯＳ、ＮＯＳ、通信、デバイス・ドライバまたはその他のソフトウェア割込みをコールしたことが検出された場合、エージェントの動作が始まる。ステップ１１４において、ＯＳは、ＤＯＳ™またはＯＳ／２™ＤＬＬ／ＯＳサービスまたはＷＩＮＤＯＷＳ™保護モードを

ソフトウェア割込みハンドラにコールする。
エントリ・ポイント１１６、１１７、１１８、１２０および１２２は、ステップ１２６においてエラーまたはマスクされていない事象が発生しているかどうかをエージェントに判定させる事象が発生した場合の可能なオプションを示す。エントリ・ポイント１１６は、一般エージェントによって実行されるシステム監視及びポーリング機能を表す。エントリ・ポイント１１７は、通信及びネットワーク・オペレーティング・システム（ＮＯＳ）サービスからの割込みを表す。エントリ・ポイント１１８は、割込み２１ｈ、ＤＯＳ™オペレーティング・システム・サービス・コールおよびＷＩＮＤＯＷＳ™オペレーティング・システム・サービス・コール用の割込みハンドラを表す。エントリ・ポイント１２０は、割込み２Ｆｈ、ＤＯＳ™およびＷＩＮＤＯＷＳ™用のマルチプレクサ用の割込みハンドラを表す。表１に記載されている割込みのいずれか１つを実行すると、エラーまたはマスクされていない事象が発生しているかどうかを判定するように一般エージェントがトリガされることを概略的に示すために、複数のエントリ・ポイント１２０が示されている。エントリ・ポイント１２２は、すべてのＯＳ／２™ＤＬＬおよびＯＳカーネル・サービスを表す。
これらの動作についてエラーがない場合または事象がマスクされた事象である場合、ステップ１２８においてオペレーティングＳＹＳＴＥＭ　ＳＥＲＶＩＣＥを実行し、制御権をコール側に戻す。ステップ１２６において、１１６、１１７、１１８、１２０および１２２において識別されたプログラムまたは機能の１つの実行中にエラーが発生した場合、およびそのエラーがマスクされていない事象である場合、（第８図に示される）ステップ１３０において制御権をＰＲＡＶ００１に送る。
ステップ１２６におけるテストの目的を以下に説明する。エージェントがエラー、すなわち事象を検出した場合、エージェントは、その事象がマスクされているかフィルタリングされているかに基づいて、報告およびアラートを送るべきかどうかを決定することができる。特に、いくつかの事象は、事象がモニタに報告されることを妨害するために、エージェント・レベルにおいてマスクすることができる。事象がエージェント・レベルにおいてマスクされていない場合、アラートはモニタに送られる。特に、ネットワーク管理者は、いくつかの事象のみをいくつかの条件下で報告させるマネージャ内でフィルタをセットアップすることができる。この場合、第５図に関して上述したユーザ・データベース７４を生成する必要がある。
第８図は、本発明の一実施形態による一般エージェントの障害管理段階についてのルーチンの流れ図である。ステップ１３０は、第７図から入ったＰＲＡＶ００１ルーチンである。まず、ステップ１３２において、事象アラートを記憶する必要があるかどうか判定する。事象アラートを記憶しない場合、ルーチンはコール側に戻る。次いで、事象が飽和しているかどうか判定する。特に、一般エージェントが、ネットワークのオーバーフローを回避するために、絶えず繰り返すアラートを発生した場合、エージェントは、事象テーブル内で定義されたパラメータに従ってアラートを報告することのを止める。この飽和はモニタに伝達され、その結果モニタは、事象が飽和し、それ以上報告されないことを知る。
最後に、事象をフィルタリングすべきかを判定する。事象をフィルタリングする場合は、事象を報告しない。特に、例えば、特定の事象が特定のプログラムからのみ報告されるようにフィルタをセットアップすることができる。この場合、事象が非特定プログラムから発生した場合、事象を報告しない。上述のように、第７図のステップ１２６において、マスクされた事象およびマスクされていない事象について基本的フィルタリングが行う。このステップ（ステップ１３２）において、アラートを発生したプログラム名またはファイル名を任意選択でユーザ・インタフェース５２内でセットアップされた名前テーブルと比較し、ユーザ・データベース７４内に記憶し、エージェント・データベース３０にダウンロードされる。プログラムが名前テーブル内に見つからない場合、アラートを送らない。
ステップ１３４において、ステップ１３２におけるテストの結果から、アプリケーション・アラートをモニタに送る必要があるかどうかを判定する。アプリケーション・アラートをモニタに送る必要がない場合、ステップ１３６において制御権をコール側に戻す。ステ

ップ１３４においてアラートを送るべきであると判定した場合、ステップ１３８においてアプリケーション・アラートを生成し、送る。次いで、エージェントは、ステップ１４２において、新しい割込みを受容することができる初期状態にそれ自体をリセットすることによって、次の動作の準備をする。次いで、ステップ１４８において制御権をコール側に戻す。

第９図は、一般エージェントの制御および管理段階についてのルーチンの流れ図である。マネージャ４から管理要求が得られた場合、ステップ１５０においてこの段階に入る。ステップ１５２において、要求の種類が処置（セット）であるか要求（ゲット）であるか判定する。要求がセット要求である場合、実行すべき処置を決定するディスパッチャ１５４にそれを送る。ステップ１５６において、ワークステーション用のブート・セット・コマンド、フリーズ・セット・コマンドまたはアンフリーズ・セット・コマンドを実行する。ステップ１５８において、メッセージ、キーストローク・ジョブ、開始プログラムまたは停止プログラムの命令、ワークステーションの制御権を得るまたは放棄する命令を実行する。また、マネージャ４は、ステップ１６０において、新しい事象テーブルをダウンロードするためにセット要求を一般エージェントに送る。最後に、マネージャ４は、ステップ１６２において実行されるファイル修正要求を送る。このモジュールは、ＣＯＮＦＩＧ．ＳＹＳファイルまたはＡＵＴＯＥＸＥＣ．ＢＡＴファイルを変更するなど修正命令を実行する。ステップ１５６、１５８、１６０および１６２における処置を実行した後、ステップ１６４においてマネージャ４に確認を返送する。

ステップ１５２においてゲット要求が検出された場合、ステップ１６６、１６８、１７０および１７２における機能のうちの１つを実行するディスパッチャ１６５にゲット・コマンドを送る。マネージャ４がプログラム・リストを要求した場合、ステップ１６６においてそれを送る。このプログラム・リストは、受信側エージェントが要求を受信した時刻においてワークステーション上で動作しているプログラムのリストである。基本的構成情報が要求された場合、ステップ１６８においてこれを送る。ビデオ・ドライバ、マウス、またはオペレーティング・システム情報など、情報が遠隔アクセスに必要な場合、ステップ１７０においてその情報を収集する。このゲット命令からの情報を使用して、マネージャ４は、ステップ１５８において処理されたセット要求によってエージェントのワークステーションを制御することができる。マネージャが事象テーブル情報を要求した場合、ステップ１７２においてそれを検索する。ステップ１７４において、ステップ１６６、１６８、１７０および１７２からの要求された結果をマネージャ４に送る。

第１０図は、本発明の一実施形態によるモニタ２の動作段階ついてのルーチンの流れ図である。ステップ１７６において、ネットワークからアラートを受信し、ステップ１７８において事象ログ・データベース４４に送る。次いで、エラーの性質、プログラムの名前、エラーの位置、および訂正処置の勧告など、事象の詳細な説明を含んでいる事象ログ・データベース４４に事象を書き込む。事象ログ・データベース４４の書式は上述したものと同じである。本発明の一実施形態によれば、アラートを発生したすべての事象を事象ログ・データベース４４に書き込む。ネットワーク管理者によってセットアップされたフィルタを使用して事象のリストを管理する管理事象リスト・モジュール１８０が備えられている。ビューを実時間でフィルタリングする事象フィルタリング・エンジン１８２が備えられている。換言すれば、管理事象リスト・モジュール１８０は、事象ログ・データベース４４に事象を書き込んだり、事象ログ・データベース４４から事象を検索したりするデータベース・マネージャである。実時間事象フィルタリング・エンジン１８２は、実行ビュー機能１８４に送るために事象ログ・データベース４４から事象を選択する。事象は、様々なビュー内に表示するためにフィルタリングされる。特に、各ビューがネットワーク管理者によってセットアップされている場合、アラートのうちのいくつかのみを表示する。ステップ１８４においてビュー機能を実行する。

各事象ごとに、ステップ１８６において、その事象について訂正手順が定義されているかどうか判定する。換言すれば、上述のように、ネットワーク管理者、またはデフォルトによるシステムは、一般にエージェントによって処置がとられるように、モニタによってマ

ネージャに送られる特定のコマンドであるトリガをセットアップする。上述のように、訂正手順は、事象に応答して順に実行される一組のトリガである。例えば、「Ｔｏｏ ｍａｎｙ ｆｉｌｅｓ」エラーが検出されると、２つのトリガから構成される訂正手順がワークステーションに送られる。第１のトリガは、ファイルの数を増やすためにＣＯＮＦＩＧ．ＳＹＳファイルを修正するトリガである。次いで、その変更を有効にするためにワークステーションをリブートするリブート・トリガがくる。

訂正手順がステップ１７６において受信されたアラートに応答して実行されるように定義されている場合、ステップ１８８において訂正手順がアクティブかどうか判定する。特に、訂正手順またはトリガのセットは、モニタのユーザによって「アクティブ」または「非アクティブ」に定義される。ネットワーク管理者は、事象をログし、閲覧している間、様々な理由で自動訂正特徴を一時的に中断することを望むので、特定の手順を非アクティブにセットする。手順がアクティブの場合、ステップ１９０においてマネージャに手順を実行するようにコールする。ステップ１８６および１８８における返答が非アクティブの場合、またはマネージャがステップ１９０においてトリガ手順を実行した後、ステップ１９２において（トリガの結果、統計、カウンタなどを含む）メッセージ・ログ・データベース４５の維持を実行する。特に、データベースのサイズを示すためおよびシステムの動作をサポートするために、事象、トリガなどのカウンタを維持する。さらに、今度特定の事象が発生した場合に訂正手順が実行されるように、手順マネージャ５４を使用して、管理者に訂正手順を定義する機会を与える。

第１１図は、本発明の一実施形態によるマネージャ４の動作段階についてのルーチンの流れ図である。マネージャ４は、ステップ１９４においてエージェント１４から通信を得るか、またはステップ２１８においてモニタ２から通信を得る。いずれにせよ、通信はそれぞれのディスパッチャ１９６および２２０に送られる。

通信がエージェントからのものである場合、その通信は１つまたは複数のモジュール１９８～２０８を実行するための命令である。モジュール１９８は、ワークステーションの存在の状態を所定の間隔で更新するハートビート手順である。一実施形態によれば、マネージャ４は、所定の周波数においてエージェント１４がアクティブしていることを示すハートビートを具備する。一実施形態によれば、１秒～８秒の範囲内でハートビート周波数を画定する構成可能パラメータは、４０秒のデフォルトを具備する。モジュール１９９は、エージェント１４からのエージェントのワークステーションに関するソフトウェア／ハードウェア情報を更新する構成通信である。モジュール２００は、エージェントのプログラム・リストを更新するＡＣＰ通信である。モジュール２０１は、事象テーブルを定められたフィルタに従ってセットアップするフィルタ手順である。モジュール２０２は、表２および表３に記載されている手順に従って制御を実行する制御手順である。

モジュール２０３は、セットアップ・メニューを実行するセットアップ手順である。セットアップ・メニューは、一実施形態によれば、ユーザ・リスト（すなわち、管理されたワークステーション）にアクセスする手順、未定義のユーザ（すなわち、データベース内でまだ定義されていないアクティブエージェントを有するワークステーション）を監視する手順、定義済みワークステーションについてデフォルト事象テーブルをセットする手順、および各エージェント・タイプごとに索引番号をセットする手順を含めて、マネージャ・データベース用のセットアップ手順を含む。索引番号は、管理者によって事前定義された修正可能な事象および事象の特性に対する参照番号である。モジュール２０４は、キーストローク・ジョブ管理トリガによって送られたキーストロークを実行のためにエージェントへ転送する。モジュール２０６はファイル・メニューへのアクセスを行う。ファイル・メニューは、一実施形態によれば、データベースから現在のエージェント・パラメータ（すなわち、名前、タイプなど）を示す機能、モニタを開始する機能、およびマネージャを出る機能を含む。モジュール２０７は、新しいユーザまたはワークステーションがネットワークに追加された場合に使用される発見手順である。発見モジュールは、第３図に示されるオートディスカバリ・モジュール３８から新しいアクティブ・エージェントに関する識別パケットを受信した際に実行される。最後に、モジュール２０８はユーザのデータベ

ース７４を管理する。
通信がディスパッチャ２２０を介してモニタ２からきたものである場合、通信は、表２または表３中に記載されているコマンドまたはトリガのうちの１つであるか、または１つまたは複数のトリガである。図示の実施形態によれば、ブロック２２２内に示されるリストは、カスタム・トリガを加えた表２中に記載されているトリガのみを含む。表３中に記載されているトリガをこのブロックに追加することは、本発明の開示を一度得た当業者の技術の範囲内に入る。この手順をディスパッチャ１９６に送ると、それぞれの機能を実行するように各種のモジュール１９８～２０７を実行させることができる。
さらに、実行すべきセット実行ジュール２１４を介してブロック２２２内の手順を送る。
また、モジュール２００、２０１、２０２、２０３および２０４はセット実行モジュール２１４に接続される。ゲット実行モジュール２１２の出力はモジュール１９８、１９９、または２０７に適宜送られる。
メニュー６８では、ネットワーク管理者がモジュール１９７～２０７のいずれか、ならびにゲット実行モジュール２１２、セット実行モジュール２１４、ユーザ・メニュー・コマンド・ゲット・モジュール２１６にアクセスできる。モジュール２１２は上述のようにゲット動作を実行してワークステーションから情報を得る。モジュール２１４は、上述のように、情報をセットしたり、ワークステーション内でトリガを実行するセット動作を実行する。モジュール２１６は、マネージャ・メニュー選択肢からユーザ選択を得る手順を実行する。
以下の段階では、本発明によるシステムがどのように動作するかを示す２つの例について説明する。
割込みＩｎｔ１７ｈ（表１）を実行した際に、要求されたプリンタが使用不能であることを示すエラーが発生した場合、モニタ２にアラートを報告する。アラートをログし、フィルタリングされていないかまたは飽和していない場合、適切なビュー（この場合、印刷アラーのカスタマイズされたビューが好ましい）内に表示する。訂正手順がこのアラートを処理するように定義されている場合、手順をマネージャ４に送り、次いでアラートを発生したエージェント１４に送る。訂正手順は、例えば、プリンタをネットワーク・プリンタにリダイレクトするキャプチャ・アプリケーションを開始するトリガ（６）、および印刷を再試行するメッセージをユーザに送るトリガ（５）を含むことができる。
ＮＯＳ割込みの実行中にネットワーク・オペレーティング・システムによって将来ユーザへのアクセスが否定されることを示すエラーが発生した場合、モニタ２にアラートを報告する。上記の例の場合と同様に、アラートをログし、フィルタリングされていないかまたは飽和していない場合、適切なビュー内に表示する。訂正手順が定義されている場合、手順をマネージャ４に送り、次いでエージェント１４に送る。訂正手順は、許可されていないアクセス試みを示すメッセージをユーザに送るトリガ（５）、さらにワークステーションをフリーズするトリガ（１１）を含むことができる。
第１図～第１１図の上記説明は、一般エージェントおよび一般エージェントと通信するために提供された管理コンソールを含む本発明によるシステムの一実施形態を説明するものである。さらに、本発明の他の実施形態によれば、特定のプログラムの実行中に発生するエラーまたは問題を処理する特定エージェントが提供される。例えば、ＬＯＴＵＳ™ｃｃ：ＭＡＩＬ™アプリケーション内に発生しているエラーを処理する特定エージェントが提供される。ＬＯＴＵＳ™ｃｃ：ＭＡＩＬ™は、マサチューセッツ州ケンブリッジのＬｏｔｕｓ　Ｄｅｖｅｌｏｐｍｅｎｔ社から市販されている電子メール・プログラムである。そのような特定エージェントの実施形態の例を第１２図～第１５図に示す。上述のように、特定エージェントは、管理コンソール内で実行するように定義されたワークステーション上で得られる一般エージェントを有する必要がある。しかしながら、１つまたは複数の特定のプログラムならびにネットワーク上のワークステーション内で発生する一般的なエラーを処理する一般特定混合エージェントを提供することは、本発明の開示を一度得た当業者の技術の範囲内に入る。
第１２図は、例示の特定エージェント、特にｃｃ：ＭＡＩＬ™ルータ用の特定エージェン

トのシステム・ビューのブロック図である。ｃｃ：ＭＡＩＬ™ルータは、電子メール・メッセージを電子ポスト・オフィス間でダイレクトするプログラムである。ｃｃ：ＭＡＩＬ™ルータ用の特定エージェントは、ｃｃ：ＭＡＩＬ™ルータの動作を監視し、その状態ならびにその通信の結果、すなわち成功か失敗かを報告する。これらの報告を使用して、一般エージェントの場合に行った方法と同じ方法で訂正手順を初期設定することができる。特定エージェントの各種の要素は、一般システムに接続され、特にエージェント１４およびモニタ２に接続される。第１２図では、第２図に示されるものと同じ要素には同じ参照番号が付いている。

まず、ブロック３００において、セットアップ／定義ファイル（．ＩＮＩ）が提供される。セットアップ／定義ファイル３００は、ＬＯＴＵＳ™ｃｃ：ＭＡＩＬ™ルータ・エラー・ログ・ファイル３１２を処理しかつ事象をエージェント１４に転送するための仕様を含む。これは、ブロック３１０内に提供されたｃｃ：ＭＡＩＬ™ルータ用の特定エージェントと通信する。ＬＯＴＵＳ™ｃｃ：ＭＡＩＬ™ルータの実行中に発生した事象を追跡するエラー・ログ・ファイル３１２が提供される。特定エージェント３１０は、第３図に示される標準アラートＡＰＩを介して一般システムのエージェント１４と通信する。さらにブロック３１４では新たに索引データベースの形でｃｃ：ＭＡＩＬ™に索引が提供される。特定エージェントでは、追加の特殊目的索引をこのデータベースに追加する必要がある。これらの索引は、ユーザ・データベース（第５図中のモジュール７４）の一部である。各特定の事象ごとに、このデータベース内にこのアラートをテキスト形式で記述する索引が１つなければならない。したがって、任意の特定エージェントをシステムに追加する場合、このデータベースは、この新しい特定エージェントが発生させる各アラートごとに索引定義を含む。

特定エージェントは、ＴＳＲプログラムとしてかまたは非ＴＳＲプログラムとしてロードされる。両方の導入の実施形態について説明する。

第１３図は、非ＴＳＲアプリケーションとしてロードされたｃｃ：ＭＡＩＬ™ルータ特定エージェントについてのルーチンの流れ図である。まず、ステップ３１６においてエージェントをロードし、次いでコマンド・ラインを解析する初期設定段階に入り、一般エージェントがロードされているかどうか判定する。次に、ステップ３１８において、特定エージェント内からＬＯＴＵＳ™ｃｃ：ＭＡＩＬ™ルータを開始する。特定エージェントは、ルータに対する保護シェルの役目をする。すなわち、特定エージェントは、事実上、ルータを包囲し、ルータによるすべての外部通信を観測し、制御することができるプログラムである。ステップ３２０において、ｃｃ：ＭＡＩＬ™ルータ・エラー・ログへの接続を確認し、ステップ３２２において、ログをポールし、新しいルータ事象が発生したかどうかを判定する。

ステップ３１６、３１８またはステップ３２０において、エラーが発生した場合、ステップ３３６において故障メッセージを印刷する。特に、ステップ３１６において一般エージェントがロードされていない場合、ステップ３３６においてエラー・メッセージ「ｆａｉｌ　ｔｏ　ｉｎｉｔｉａｌｉｚｅ」を印刷する。ステップ３１８が故障した場合は「ｆａｉｌ　ｔｏ　ｌｏａｄ」メッセージを印刷し、ステップ３２０が故障した場合は「ｆａｉｌ　ｔｏ　ｃｏｎｎｅｃｔ」メッセージを印刷する。

ステップ３２２において、ルータ・エラー・ログをポールし、新しいルータ事象が検出されたかどうか判定する。ステップ３２３においてルータ事象がエラーであると判定された場合、ステップ３２４においてルータ誤動作アラートを生成する。問題が検出されない場合、ステップ３２６において動作またはセッションが成功したかどうか判定する。セッションが成功していない場合は、ステップ３２８において所定の数秒間待ち状態に入る。一実施形態によれば、この待ち状態に３秒間入るが、この値は変更することができる。所定の数秒間が経過した後、新しいルータ事象が発生したかどうか判定するために、制御権が再びステップ３２２に移る。ステップ３２６において動作またはセッションの成功が検出された場合、ステップ３３０においてルータ動作を繰り返す。ステップ３３２において、ステップ３２４および３３０からのアラートまたはルータ動作を報告するために、一般エ

ージェント１４にアクセスする。続いてステップ３３４において、制御権が一般エージェント１４に移る。

第１４図は、ＤＯＳ™ＴＳＲアプリケーションとしてロードされた特定エージェントｃｃ：ＭＡＩＬ™ルータについての初期設定段階についてのルーチンの流れ図である。まず、コマンド・ラインを解析し、ステップ３３６において一般エージェントがロードされているかどうか判定する。一般エージェントがロードされていない場合、ステップ３３７において「ｆａｉｌ　ｔｏ　ｉｎｉｔｉａｌｉｚｅ」エラー・メッセージを印刷する。一般エージェントがロードされている場合、ステップ３３８において表１中に記載されている割込みをセットアップする。特に、割込み０８ｈ、２８ｈ、０９ｈおよび１６ｈをセットアップする。次いで、ｃｃ：ＭＡＩＬ™ルータ特定エージェントをメモリ内に常駐させるステップ３４０を実行する。

第１５図は、ＤＯＳ™ＴＳＲとしてロードされたｃｃ：ＭＡＩＬ™ルータ特定エージェントの動作段階についてのルーチンの流れ図である。ステップ３４２において割込みハンドラへのシステム・コールが検出された場合、ステップ３４４においてルータ・エージェント割込みハンドラにアクセスする。ステップ３４６では古い割込みハンドラへのジャンプを実行する。ステップ３４８ではＴＳＲをウェイクアップさせる。すなわち、ステップ３４６における古い割込みハンドラへのジャンプにより、制御権がＬＯＴＵＳ™ｃｃ：ＭＡＩＬ™ルータ・プログラムに戻り、その結果ＬＯＴＵＳ™ｃｃ：ＭＡＩＬ™ルータ・プログラムがその正常機能を完了することができる。ステップ３４８におけるウェイクアップ機能は、特定エージェントＴＳＲを刺激して、事象を解析し、報告する動作を開始させる。特に、一実施形態によれば、第１５図のブロック３４２を介してシステムから毎秒１８回制御権を得るｃｃ：ＭＡＩＬ™ルータ特定エージェント用のタイマ割込みハンドラが提供される。次いで、ブロック３４４内で、ｃｃ：ＭＡＩＬ™ルータ特定エージェントは、最後のウェイクアップ（または作業の始め）から指定された時間が経過したかを決定する。指定された時間が経過している場合、特定エージェントをウェイクアップさせるようにブロック３４８に呼びかける。指定された時間は、上述の待ち状態パラメータによって決定される。指定された時間が経過していない場合、ブロック３４４では、古い割込みハンドラ（すなわち、システム・タイマ）へのジャンプを実行するようにブロック３４８に呼びかける。

ステップ３４８においてＴＳＲをウェイクアップした後、第１３図に関して上述した方法と同じ方法でｃｃ：ＭＡＩＬ™ルータ・プロセスを実行する。動作は同じなので、それについて再び説明しない。ただし、図面では、第１３図で使用されているのと同じ参照番号が付いている。

上述のソフトウェア・モジュールは、動作のために、ＰＣ－ＤＯＳ™、ＭＳ－ＤＯＳ™、ＷＩＮＤＯＷＳ™、ＯＳ／２™またはその他の互換オペレーティング・システムを具備する。一実施形態によれば、本発明は、管理コンソール内の４ＭＢ　ＲＡＭ、８ＭＢハードディスク・スペース、ＭＩＣＲＯＳＯＦＴ™ ＷＩＮＤＯＷＳ™３．０以降、ＮＯＶＥＬＬ™ＮＥＴＷＡＲＥ™２．２以上、ＩＢＭ™ＬＡＮサーバ、ＭＩＣＲＯＳＯＦＴ™ＬＡＮマネージャ、またはその他の任意のＮｅｔＢＩＯＳ™、ＩＰＸ™、ＤＬＣ™、またはＴＣＰ／ＩＰ™互換ネットワークを必要とする。ソフトウェア・モジュールの詳細な実施は、本発明の開示を一度得た当業者の技術の範囲内に入る。さらに、ソフトウェア・モジュールを他のシステム上で動作させるのに必要な修正も、本発明の開示を一度得た当業者の技術の範囲内に入る。

特定の実施形態についての以下の説明から、一般概念から逸脱することなく、他人が現行の知識を適用することによってそのような実施形態を容易に修正し、各種の用途に合わせて改変することができ、したがって、そのような改変および修正は、開示の実施形態の同等物の意味および範囲内で理解すべきであるという本発明の一般性質が完全に明らかとなろう。本明細書で使用されている用語または術語は、説明のためのものであり、限定的なものではないことを理解されたい。

【図１】

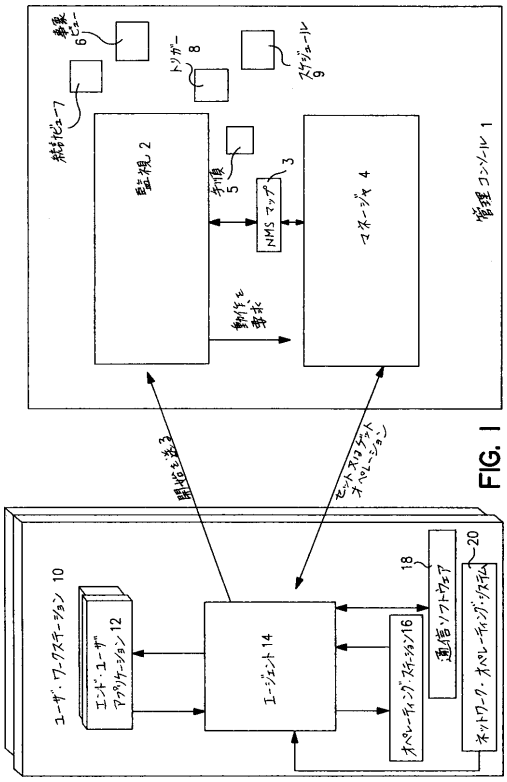

FIG. 1

【図２】

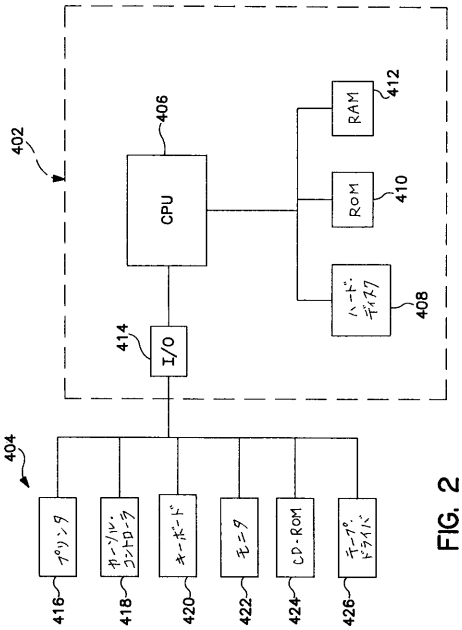

FIG. 2

【図３】

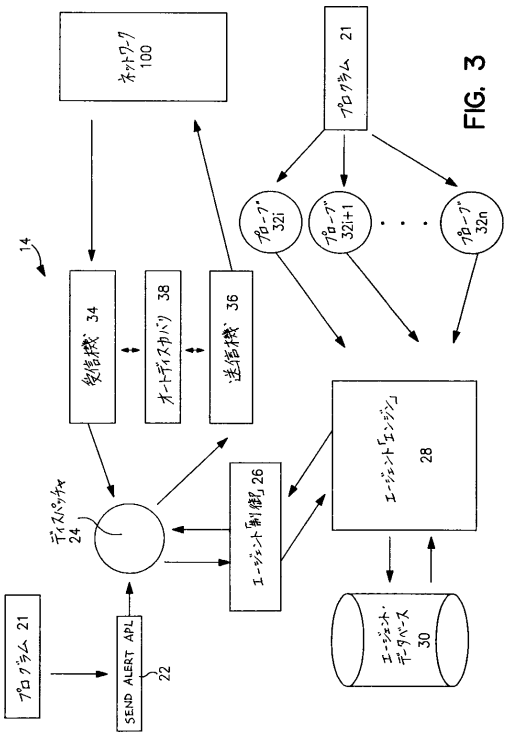

FIG. 3

【図４】

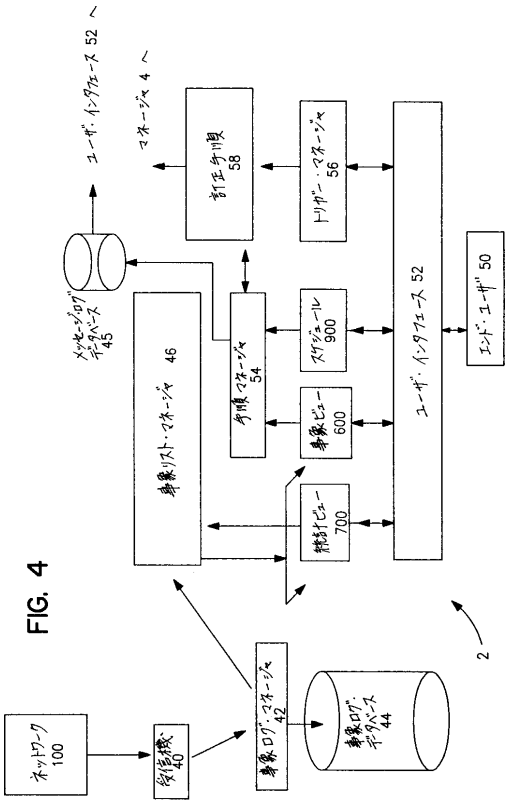

FIG. 4

【図５】

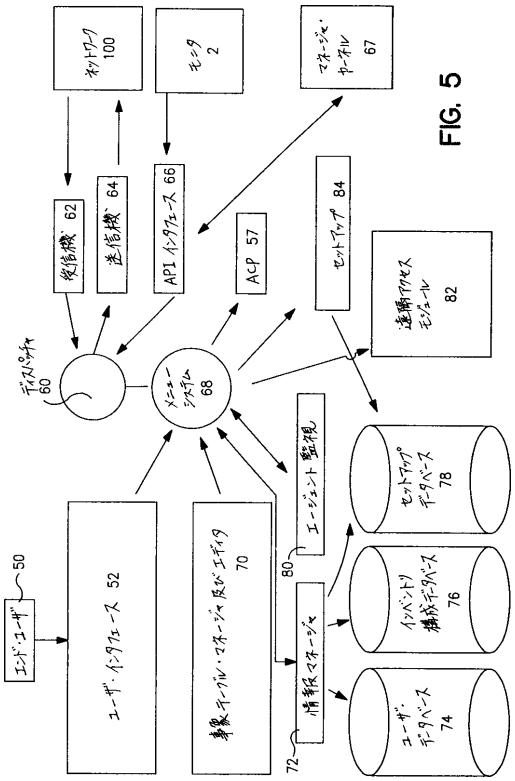

FIG. 5

【図６】

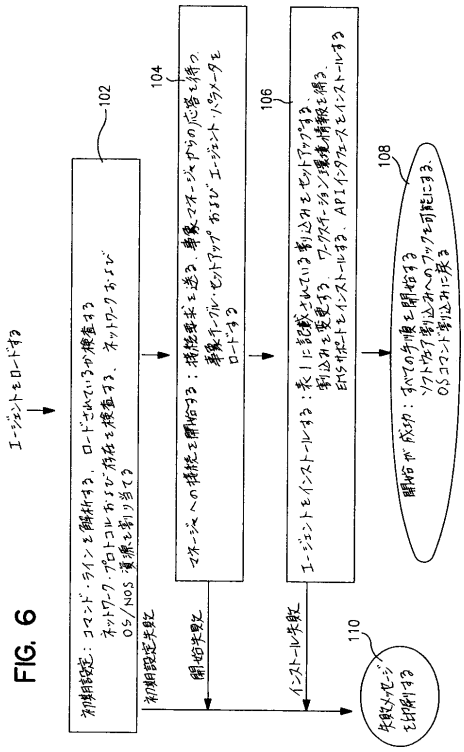

FIG. 6

【図７】

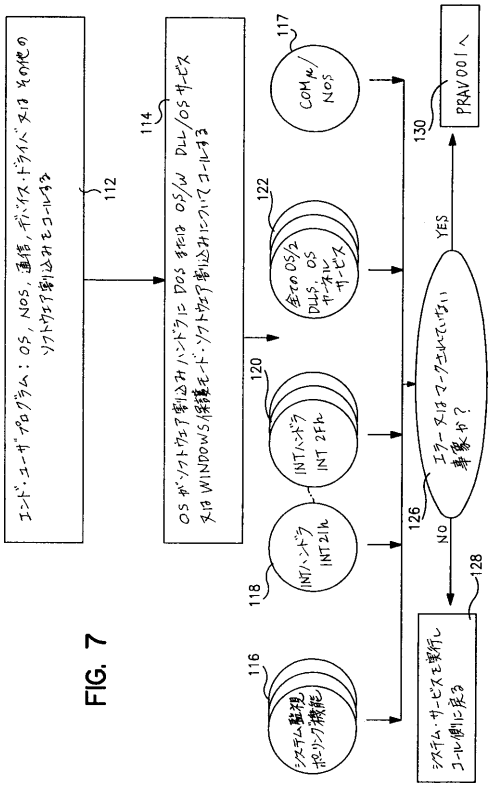

FIG. 7

【図８】

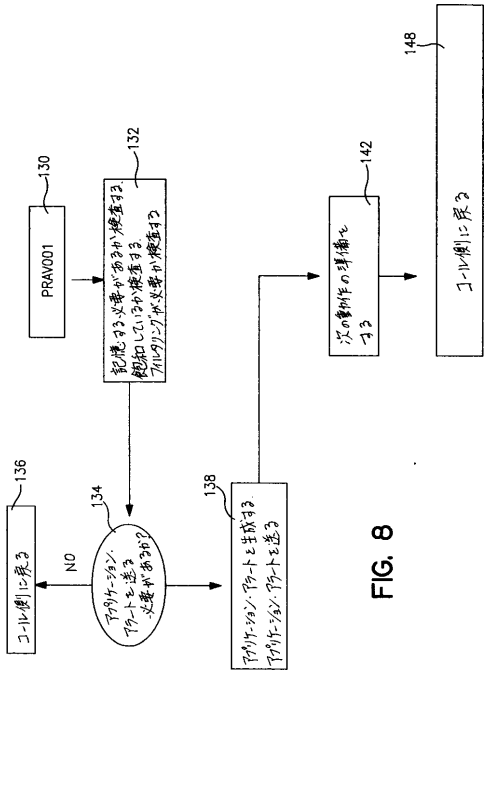

FIG. 8

【図９】

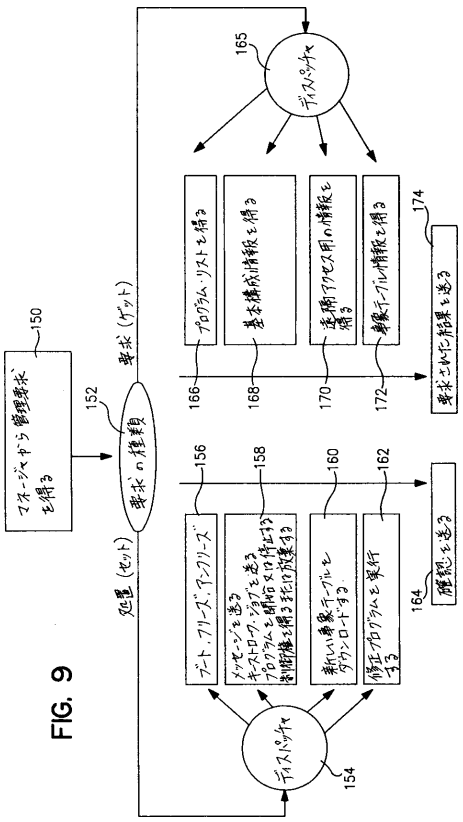

FIG. 9

【図１０】

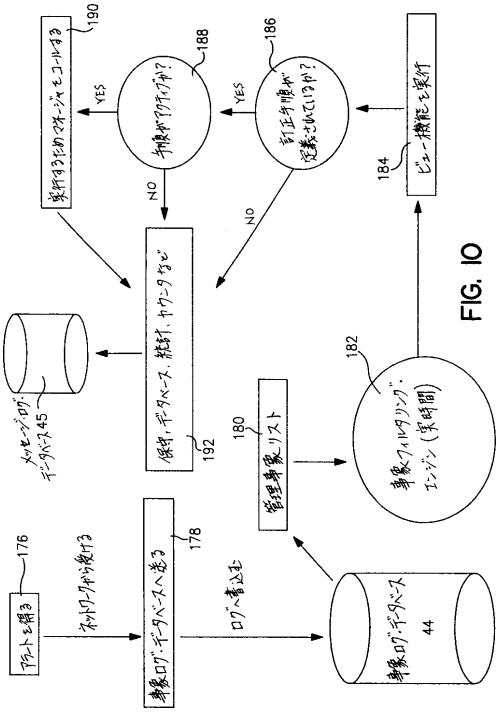

FIG. 10

【図１１】

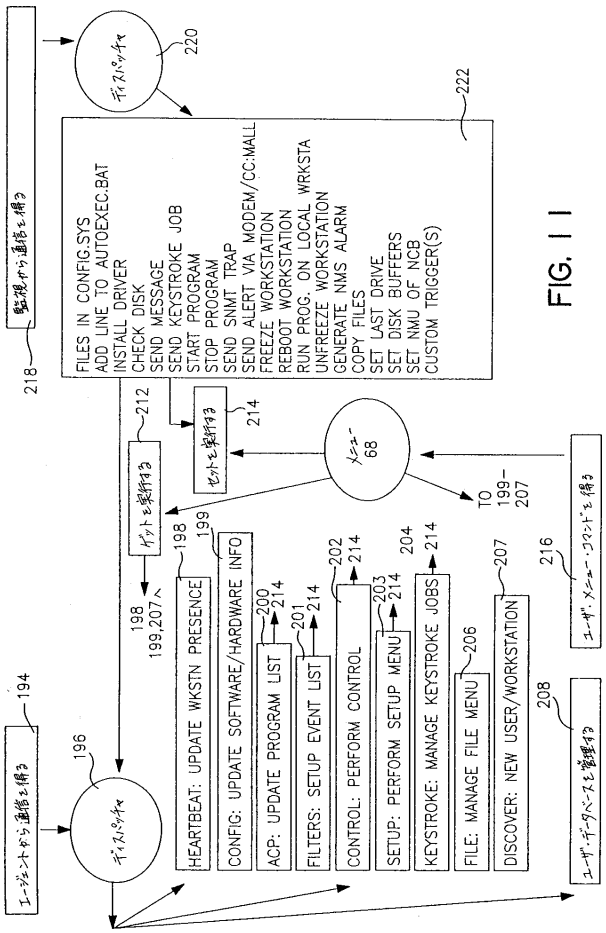

FIG. 11

【図１２】

FIG. 12

【図１３】

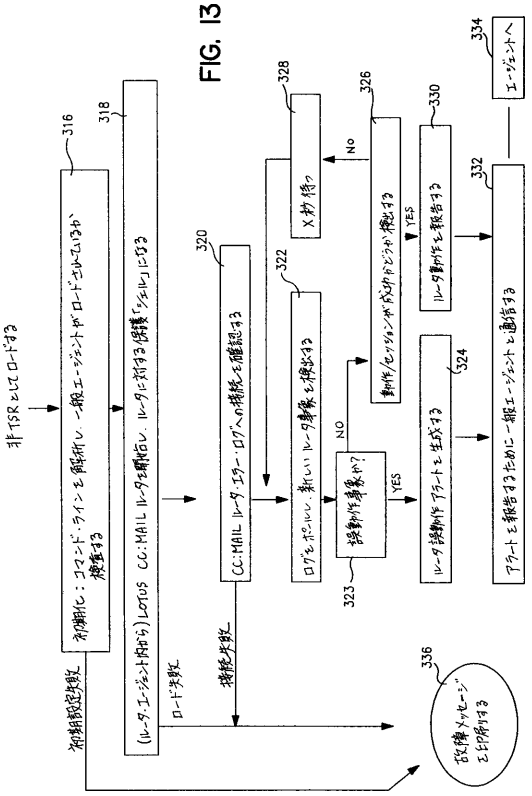

FIG. 13

【図１４】

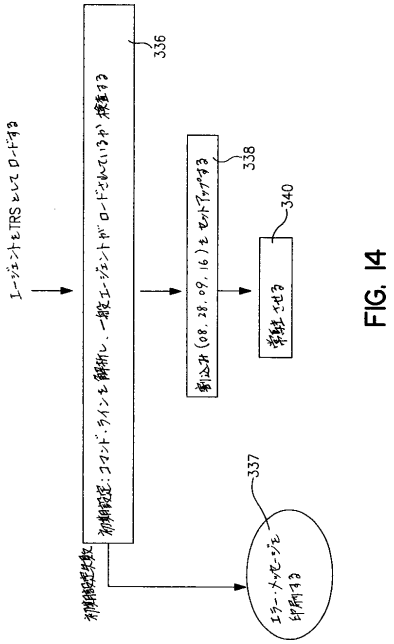

FIG. 14

【図１５】

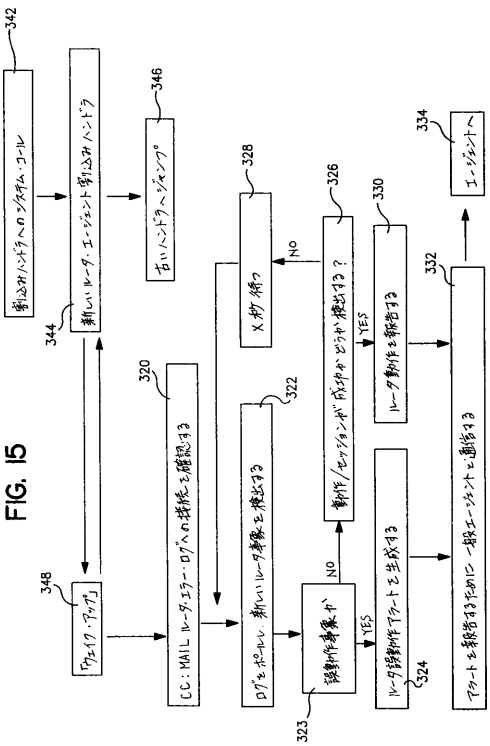

FIG. 15

フロントページの続き

(72)発明者　トウボウル，シュロモ
イスラエル国・４２４９５・ケファール　ハイム（番地なし）

合議体
審判長　吉岡　浩
審判官　野仲　松男
審判官　山崎　達也

(56)参考文献　特開昭６４－５７３４７（ＪＰ，Ａ）
特開平２－９１７３５（ＪＰ，Ａ）
Ｆｅｒｒｉｌｌ，”Ｕｐｄａｔｅｄ Ｓｈａｎｙ ｎｅｔｗｏｒｋ ｍｏｎｉｔｏｒ ｉｓ ｅａｓｉｅｒ ｔｏ ｉｎｓｔａｌｌ ａｎｄ ｕｓｅ”，ＩｎｆｏＷｏｒｌｄ，（米），１９９３年１２月１３日，Ｖｏｌ．１５，Ｉｓｓ．５０，ｐ．８７，９０，９１，９４
Ｈｅｙｗｏｏｄ，”Ｔｒｏｕｂｌｅｓｈｏｏｔｉｎｇ Ａｐｐｌｉｃａｔｉｏｎｓ Ｆｒｏｍ ｔｈｅ Ｉｎｓｉｄｅ”，Ｄａｔａ Ｃｏｍｍｕｎｉｃａｔｉｏｎｓ，（米），１９９３年1月，Ｖｏｌ．２２，Ｉｓｓ．１，ｐ．１１５－１１６

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F11/30-11/34
G06F13/00