(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2010-68075
(P2010-68075A)
(43)公開日　平成22年3月25日(2010.3.25)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 12/28	(2006.01)	H04L	12/28	200M	5B089
H04L 12/56	(2006.01)	H04L	12/56	400Z	5K030
H04M 3/00	(2006.01)	H04M	3/00	E	5K033
H04M 11/00	(2006.01)	H04M	11/00	301	5K201
G06F 13/00	(2006.01)	G06F	13/00	351N	

審査請求 未請求　請求項の数 30　ＯＬ　（全 21 頁）

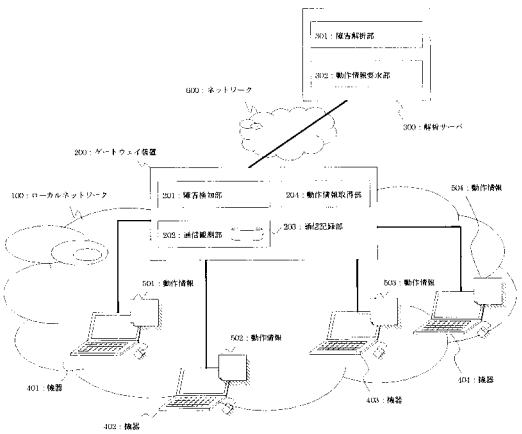
(21)出願番号　特願2008-230609 (P2008-230609)
(22)出願日　平成20年9月9日 (2008.9.9)

(71)出願人　000000295
沖電気工業株式会社
東京都港区西新橋三丁目１６番１１号
(71)出願人　504230604
森井　昌克
徳島県徳島市徳島町２－３２
(74)代理人　100085198
弁理士　小林　久夫
(74)代理人　100098604
弁理士　安島　清
(74)代理人　100125494
弁理士　山東　元希
(74)代理人　100061273
弁理士　佐々木　宗治

最終頁に続く

(54)【発明の名称】障害分析システム、障害分析方法

(57)【要約】
【課題】障害分析を行うために必要な最小限の情報を収集して解析先へ送信することのできる障害分析手法を得る。
【解決手段】ゲートウェイ装置２００は、第１ネットワーク１００上の１ないし複数の機器４０１～４０４の障害を検知する障害検知部２０１と、機器４０１～４０４間で通信が行われた際に各通信相手の識別情報を記録する通信状況記録部と、機器４０１～４０４の動作情報を取得して解析装置３００に送信する動作情報取得部２０４と、を備え、解析装置３００は、動作情報を用いて機器４０１～４０４の障害解析を行う障害解析部３０１を備え、動作情報取得部２０４は、通信状況記録部が記録している識別情報を用いて、障害検知部２０１が障害を検知した機器が過去に通信を行った相手機器を特定し、その通信相手の動作情報を取得して解析装置３００に送信する。
【選択図】図１



【特許請求の範囲】
【請求項１】
第１ネットワークに接続されたゲートウェイ装置と、
前記第１ネットワークとは異なる第２ネットワークに接続された解析装置と、
を有し、
前記ゲートウェイ装置は、
前記第１ネットワーク上の１ないし複数の機器の障害を検知する障害検知部と、
前記機器間で通信が行われた際に各通信相手の識別情報を記録する通信状況記録部と、
前記機器の動作情報を取得して前記解析装置に送信する動作情報取得部と、
を備え、
前記解析装置は、
前記動作情報を用いて前記機器の障害解析を行う障害解析部を備え、
前記動作情報取得部は、
前記通信状況記録部が記録している識別情報を用いて、
前記障害検知部が障害を検知した機器が過去に通信を行った相手機器を特定し、
その通信相手の動作情報を取得して前記解析装置に送信する
ことを特徴とする障害分析システム。
【請求項２】
前記通信状況記録部は、
前記機器間で行う全ての通信のパケットから送信元アドレスと送信先アドレスを抽出することにより前記識別情報を作成して記録する
ことを特徴とする請求項１記載の障害分析システム。
【請求項３】
前記通信状況記録部は、
前記機器間で行う通信のパケットをサンプリングし、
そのサンプリングしたパケットから送信元アドレスと送信先アドレスを抽出することにより前記識別情報を作成して記録する
ことを特徴とする請求項１記載の障害分析システム。
【請求項４】
前記通信状況記録部は、
前記機器間で行う通信のセッション開始パケットを捕捉し、
そのセッション開始パケットから前記機器のアドレスを取得することにより前記識別情報を作成して記録する
ことを特徴とする請求項１記載の障害分析システム。
【請求項５】
前記通信状況記録部は、
前記第１ネットワーク上を流れる機器発見パケットを捕捉し、
その機器発見パケットを用いて送信元アドレスと送信先アドレスを抽出することにより前記識別情報を作成して記録する
ことを特徴とする請求項１記載の障害分析システム。
【請求項６】
前記動作情報取得部は、
取得した前記動作情報のうち重要度の高いものをあらかじめ定められた重要度にしたがって絞り込んだ上で前記解析装置に送信する
ことを特徴とする請求項１ないし請求項５のいずれかに記載の障害分析システム。
【請求項７】
第１ネットワークに接続されたゲートウェイ装置と、
第２ネットワークに接続された解析装置と、
を有し、
前記ゲートウェイ装置は、

前記第１ネットワーク上の１ないし複数の機器の動作情報を取得して前記解析装置に送信する動作情報取得部を備え、
前記解析装置は、
前記動作情報を用いて前記機器の障害解析を行う障害解析部を備え、
前記動作情報取得部は、
取得した前記動作情報のうち重要度の高いものをあらかじめ定められた重要度にしたがって絞り込んだ上で前記解析装置に送信する
ことを特徴とする障害分析システム。
【請求項８】
前記障害解析部は、
前記動作情報の内容とその重要度を対応付ける対応規則情報を前記ゲートウェイ装置にあらかじめ送信しておき、
前記動作情報取得部は、
取得した前記動作情報のうち重要度の高いものを前記対応規則情報にしたがって絞り込んだ上で前記解析装置に送信する
ことを特徴とする請求項６または請求項７記載の障害分析システム。
【請求項９】
前記障害解析部は、
前記機器の障害解析結果に基づき前記動作情報に重要度を付与し、
その重要度を用いて前記対応規則情報を作成し前記ゲートウェイ装置に送信する
ことを特徴とする請求項８記載の障害分析システム。
【請求項１０】
前記解析装置は、
前記動作情報のうち前記障害解析部が障害解析を行うに際して有意であったものにマークを付与する重要情報指示部を備え、
前記障害解析部は、
前記重要情報指示部がマークを付与した頻度が高い前記動作情報ほど重要度が高くなるように前記対応規則情報を作成して前記ゲートウェイ装置に送信する
ことを特徴とする請求項９記載の障害分析システム。
【請求項１１】
前記対応規則情報は、
前記障害発生時刻から時刻が離れている前記動作情報ほど重要度が低くなるように構成されている
ことを特徴とする請求項６ないし請求項１０のいずれかに記載の障害分析システム。
【請求項１２】
前記解析装置は、
前記ゲートウェイ装置に前記動作情報を要求する動作情報要求部を備え、
前記動作情報取得部は、
前記動作情報要求部の要求にしたがって前記動作情報のうち重要度の高いものを絞り込んだ上で前記解析装置に送信し、
既に前記動作情報を送信済みであるときは、
先に送信した前記動作情報よりも重要度の低い動作情報を送信する
ことを特徴とする請求項６ないし請求項１１のいずれかに記載の障害分析システム。
【請求項１３】
前記解析装置は、
前記ゲートウェイ装置に対し障害が発生した機器の復旧を試みるよう要求する復旧要求部を備え、
前記動作情報取得部は、
前記復旧要求部から要求された機器の復旧を試みた後、
その機器の動作情報を取得して前記解析装置に送信する

ことを特徴とする請求項１ないし請求項１２のいずれかに記載の障害分析システム。
【請求項１４】
前記動作情報取得部は、
前記機器内で動作しているプロセスの一覧、そのプロセスのログ、またはこれらの双方を前記動作情報として取得する
ことを特徴とする請求項１ないし請求項１３のいずれかに記載の障害分析システム。
【請求項１５】
前記動作情報取得部は、
前記動作情報を取得する際に当該機器の個体識別情報を取得して当該動作情報に含める
ことを特徴とする請求項１ないし請求項１４のいずれかに記載の障害分析システム。
【請求項１６】
第１ネットワークに接続された１ないし複数の機器の障害を分析する方法であって、
前記第１ネットワークとは異なる第２ネットワークに解析装置を接続しておき、
前記機器間で通信が行われた際に各通信相手の識別情報を記録する通信状況記録ステップと、
前記機器の障害を検知する障害検知ステップと、
前記機器の動作情報を取得して前記解析装置に送信する動作情報取得ステップと、
を有し、
前記解析装置は、
前記動作情報を用いて前記機器の障害解析を行う障害解析ステップを実行し、
前記動作情報取得ステップでは、
前記通信状況記録ステップで記録した識別情報を用いて、
前記障害検知ステップで障害を検知した機器が過去に通信を行った相手機器を特定し、
その通信相手の動作情報を取得して前記解析装置に送信する
ことを特徴とする障害分析方法。
【請求項１７】
前記通信状況記録ステップでは、
前記機器間で行う全ての通信のパケットから送信元アドレスと送信先アドレスを抽出することにより前記識別情報を作成して記録する
ことを特徴とする請求項１６記載の障害分析方法。
【請求項１８】
前記通信状況記録ステップでは、
前記機器間で行う通信のパケットをサンプリングし、
そのサンプリングしたパケットから送信元アドレスと送信先アドレスを抽出することにより前記識別情報を作成して記録する
ことを特徴とする請求項１６記載の障害分析方法。
【請求項１９】
前記通信状況記録ステップでは、
前記機器間で行う通信のセッション開始パケットを捕捉し、
そのセッション開始パケットから前記機器のアドレスを取得することにより前記識別情報を作成して記録する
ことを特徴とする請求項１６記載の障害分析方法。
【請求項２０】
前記通信状況記録ステップでは、
前記第１ネットワーク上を流れる機器発見パケットを捕捉し、
その機器発見パケットを用いて送信元アドレスと送信先アドレスを抽出することにより前記識別情報を作成して記録する
ことを特徴とする請求項１６記載の障害分析方法。
【請求項２１】
前記動作情報取得ステップでは、

取得した前記動作情報のうち重要度の高いものをあらかじめ定められた重要度にしたがって絞り込んだ上で前記解析装置に送信する
ことを特徴とする請求項１６ないし請求項２０のいずれかに記載の障害分析方法。
【請求項２２】
第１ネットワークに接続された１ないし複数の機器の障害を分析する方法であって、
前記第１ネットワークとは異なる第２ネットワークに解析装置を接続しておき、
前記第１ネットワーク上の１ないし複数の機器の動作情報を取得して前記解析装置に送信する動作情報取得ステップを有し、
前記解析装置は、
前記動作情報を用いて前記機器の障害解析を行う障害解析ステップを実行し、
前記動作情報取得ステップでは、
取得した前記動作情報のうち重要度の高いものをあらかじめ定められた重要度にしたがって絞り込んだ上で前記解析装置に送信する
ことを特徴とする障害分析方法。
【請求項２３】
前記障害解析ステップでは、
前記動作情報の内容とその重要度を対応付ける対応規則情報を前記ゲートウェイ装置にあらかじめ送信しておき、
前記動作情報取得ステップでは、
取得した前記動作情報のうち重要度の高いものを前記対応規則情報にしたがって絞り込んだ上で前記解析装置に送信する
ことを特徴とする請求項２１または請求項２２記載の障害分析方法。
【請求項２４】
前記障害解析ステップでは、
前記機器の障害解析結果に基づき前記動作情報に重要度を付与し、
その重要度を用いて前記対応規則情報を作成し前記ゲートウェイ装置に送信する
ことを特徴とする請求項２３記載の障害分析方法。
【請求項２５】
前記解析装置は、
前記動作情報のうち前記障害解析ステップで障害解析を行うに際して有意であったものにマークを付与する重要情報指示ステップを実行し、
前記障害解析ステップでは、
前記重要情報指示ステップでマークを付与した頻度が高い前記動作情報ほど重要度が高くなるように前記対応規則情報を作成して前記ゲートウェイ装置に送信する
ことを特徴とする請求項２４記載の障害分析方法。
【請求項２６】
前記対応規則情報は、
前記障害発生時刻から時刻が離れている前記動作情報ほど重要度が低くなるように構成されている
ことを特徴とする請求項２１ないし請求項２５のいずれかに記載の障害分析方法。
【請求項２７】
前記解析装置は、
前記ゲートウェイ装置に前記動作情報を要求する動作情報要求ステップを実行し、
前記動作情報取得ステップでは、
前記動作情報要求ステップの要求にしたがって前記動作情報のうち重要度の高いものを絞り込んだ上で前記解析装置に送信し、
既に前記動作情報を送信済みであるときは、
先に送信した前記動作情報よりも重要度の低い動作情報を送信する
ことを特徴とする請求項２１ないし請求項２６のいずれかに記載の障害分析方法。
【請求項２８】

前記解析装置は、
前記ゲートウェイ装置に対し障害が発生した機器の復旧を試みるよう要求する復旧要求ステップを実行し、
前記動作情報取得ステップでは、
前記復旧要求ステップで要求された機器の復旧を試みた後、
その機器の動作情報を取得して前記解析装置に送信する
ことを特徴とする請求項１６ないし請求項２７のいずれかに記載の障害分析方法。
【請求項２９】
前記動作情報取得ステップでは、
前記機器内で動作しているプロセスの一覧、そのプロセスのログ、またはこれらの双方を前記動作情報として取得する
ことを特徴とする請求項１６ないし請求項２８のいずれかに記載の障害分析方法。
【請求項３０】
前記動作情報取得ステップでは、
前記動作情報を取得する際に当該機器の個体識別情報を取得して当該動作情報に含める
ことを特徴とする請求項１６ないし請求項２９のいずれかに記載の障害分析方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ネットワークに接続された機器の障害を解析する手法に関するものである。
【背景技術】
【０００２】
ネットワークの発達および情報通信機器の普及により、様々な機器がネットワークに接続され、情報を交換し合うようになってきている。このような状況は、一般家庭にも徐々に浸透し始め、各家庭内でネットワークを構築したホームネットワークという言葉も生まれた。
また、このホームネットワークに接続される機器も、従来のパーソナルコンピュータの他、テレビや冷蔵庫といった一般的な家電製品や、人間の存在を検知するセンサといったものまで含まれるようになってきている。
【０００３】
しかし、一般家庭におけるネットワークは、従来の専門家によって管理されてきたインターネットやイントラネットとは異なり、プライバシ等の問題から、外部の人間が無断でネットワークにアクセスできるようにすることは好ましくない。
そのため、ホームネットワーク内で障害が発生した場合、ユーザ自身がそれを発見して対処する必要がある。しかし、専門家ではないユーザが自らこれらを全て行うことは困難である。
【０００４】
そこで、パーソナルコンピュータやその他の通信機器をはじめとした各メーカ等は、サポートセンターやコールセンターを設け、ホームネットワーク上での障害に対する対処を行っている。
ユーザは、メーカ等のコールセンター等に電話をかける。コールセンター等のオペレータは、ユーザから発生状況を直接聞き取り、障害状況や原因、対処方法を、過去の事例や専門家の経験・勘などを元に導き出す。
【０００５】
一方、ネットワークの障害診断に関し、『ネットワークに発生する障害と障害の兆候を示すイベントとの因果関係に基づいて障害を特定するネットワーク障害診断装置において、管理対象ネットワークとの間のトラフィックを削減すること。』を目的とした技術として、『因果関係テーブル１０４が障害とイベントの因果関係を記憶し、監視イベント選択部１０５が、因果関係テーブル１０４を参照し、障害を特定するために必要最低限のイベントを抽出して監視イベントに設定し、取得イベント選択部１０７が、最新の障害候補に

基づいて因果関係テーブル１０４からイベントを選択し、選択した各イベントに対して障害を効率よく特定できる順番に優先度を設定し、イベント取得部１０２が、設定された優先度の順番にイベントを要求し、要求に対して応答されるイベントをイベント受信部１０３が受信し、順次受信されるイベントをもとに障害判定部１０８が障害の候補を絞り込むよう構成する。』というものが提案されている（特許文献１）。

【０００６】

また、障害予測に関し、『予測対象装置で生じたイベントの種類やその発生順序に基づいて障害発生の予測をすることができる障害予測システム等を提供すること』を目的とした技術として、『障害予測システム１は、予測対象装置１０に生じたイベントに関するイベントログ３５に対しデータマイニングを実施して、たとえばイベントの発生順序によって特定される前兆パターンを抽出し、解析対象ログに前兆パターンが検出されたときに予測対象装置１０に障害が発生すると予測するログ解析部３９を備えている。』というものが提案されている（特許文献２）。

【０００７】

【特許文献１】特開２００７－９６７９６号公報

【特許文献２】特開２００７－１７２１３１号公報

【発明の開示】

【発明が解決しようとする課題】

【０００８】

上記特許文献１や特許文献２に記載の技術では、ホームネットワーク上での機器障害を検知してユーザに通知することはできるが、ユーザがその通知を受けて障害に自ら対処することは一般に困難である。

【０００９】

また、ユーザがメーカ等のコールセンター等に障害復旧を依頼する場合でも、一般にユーザは機器や障害分析の知識をもっておらず、障害状況や原因をオペレータが判断するために必要な情報を的確に伝えることは困難である。したがって、オペレータが障害状況等を把握して障害復旧を完了するまでに時間がかかる。

【００１０】

一方、コールセンター側で、ホームネットワーク内に設置した機器からログ等の動作情報を取得して、障害状況の解析に用いることも考えられるが、プライバシ等の観点から家庭内の機器に関する情報を全てコールセンターに送信することは好ましくない。

さらには、仮に全ての情報を送信するとしても、送信のための通信量が膨大になってしまう懸念がある。

【００１１】

そのため、障害分析を行うために必要な最小限の情報を収集して解析先へ送信することのできる障害分析手法が望まれていた。

【課題を解決するための手段】

【００１２】

本発明に係る障害分析システムは、第１ネットワークに接続されたゲートウェイ装置と、前記第１ネットワークとは異なる第２ネットワークに接続された解析装置と、を有し、前記ゲートウェイ装置は、前記第１ネットワーク上の１ないし複数の機器の障害を検知する障害検知部と、前記機器間で通信が行われた際に各通信相手の識別情報を記録する通信状況記録部と、前記機器の動作情報を取得して前記解析装置に送信する動作情報取得部と、を備え、前記解析装置は、前記動作情報を用いて前記機器の障害解析を行う障害解析部を備え、前記動作情報取得部は、前記通信状況記録部が記録している識別情報を用いて、前記障害検知部が障害を検知した機器が過去に通信を行った相手機器を特定し、その通信相手の動作情報を取得して前記解析装置に送信するものである。

【発明の効果】

【００１３】

本発明に係る障害分析システムは、障害が発生した機器が過去に通信を行った相手機器

が障害に関係しているという想定の下、その相手機器の動作情報を解析装置に送信する。
即ち、ネットワーク上の全ての機器の動作情報を解析装置に送信することになるので、障害に関係していると思われる機器の動作情報のみを解析装置に送信し、通信量を抑えることができる。
また、障害解析に必要ない情報を送信せずに済み、送信する情報を必要最低限に抑えることができるので、情報漏えい・プライバシーの保護の観点からも好適に用いることができる。

【発明を実施するための最良の形態】

【００１４】

実施の形態１．

図１は、本発明の実施の形態１に係る障害解析システムの構成図である。
本実施の形態１に係る障害解析システムは、ゲートウェイ装置２００、解析サーバ３００を有する。以下、各装置等の構成を説明し、その後に本実施の形態１に係る障害解析システムの動作を説明する。

【００１５】

ゲートウェイ装置２００と解析サーバ３００は、ネットワーク６００を介して接続されている。また、ゲートウェイ装置２００の配下には、ローカルネットワーク１００が敷設されている。
図１では、記載の簡易の観点から、ネットワーク６００と解析サーバ３００が直接接続されているように記載したが、解析サーバ３００は、ローカルネットワーク１００と同様に組織内ネットワークに接続されていてもよい。

【００１６】

ローカルネットワーク１００は、ある組織内で閉じたネットワークである。例えば、家庭内のネットワーク（ホームネットワーク）がこれに相当する。

【００１７】

ゲートウェイ装置２００は、ローカルネットワーク１００とネットワーク６００の接続点に設置され、配下には機器４０１～４０４が接続されている。
ゲートウェイ装置２００は、機器４０１～４０４同士、または機器４０１～４０４と解析サーバ３００の間の通信を仲介するルータとしての機能を備えている。また、ゲートウェイ装置２００自身も、機器４０１～４０４、および解析サーバ３００と通信する機能を備える。

【００１８】

ゲートウェイ装置２００は、障害検知部２０１、通信観測部２０２、通信記録部２０３、動作情報取得部２０４を備える。

【００１９】

障害検知部２０１は、例えば特許文献１～２に記載されているような技術を用いて、機器４０１～４０４で発生する障害を検知する。
通信観測部２０２は、後述の図４で説明する手順を用いて、機器４０１～４０４間の通信を観測し、その状況を通信記録部２０３に格納する。

【００２０】

通信記録部２０３は、機器４０１～４０４間の通信状況を記録する。通信記録の具体例については、後述の図４で改めて説明する。
動作情報取得部２０４は、機器４０１～４０４がそれぞれ保持している動作情報５０１～５０４を取得する。動作情報取得部２０４の詳細動作については、後述の図３で改めて説明する。

【００２１】

解析サーバ３００は、ローカルネットワーク１００とは異なるネットワークに属するサーバ装置であり、機器４０１～４０４で発生した障害を解析する役割を有する。解析サーバ３００は、障害解析部３０１、動作情報要求部３０２を備える。

【００２２】

障害解析部３０１は、動作情報５０１～５０４を解析してその機器に発生した障害の原因を絞り込む。
動作情報要求部３０２は、機器４０１～４０４からそれぞれの動作情報５０１～５０４を取得して解析サーバ３００に送信するよう、ゲートウェイ装置２００に要求する。
【００２３】
機器４０１～４０４は、相互に通信する機能を有する。図１では４台構成の例を示したが、台数はこれに限られるものではない。また、機器４０１～４０４は、内部プロセスのログを出力する機能や、当該機器の外部にプロセス一覧を出力する機能を備える。
動作情報５０１～５０４は、機器４０１～４０４がそれぞれ記録または出力する、各機器の動作状況を表す情報である。
【００２４】
ネットワーク６００は、ローカルネットワーク１００と、解析サーバ３００が属するネットワークを接続する、例えばインターネット等のネットワークである。
【００２５】
障害検知部２０１、通信観測部２０２、動作情報取得部２０４、障害解析部３０１、動作情報要求部３０２は、これらの機能を実現する回路デバイスのようなハードウェアで構成することもできるし、マイコンやＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）のような演算装置とその動作を規定するソフトウェアで構成することもできる。また、必要な通信インターフェース等を適宜備える。
【００２６】
通信記録部２０３は、ＨＤＤ（Ｈａｒｄ　Ｄｉｓｋ　Ｄｒｉｖｅ）のような記憶装置で構成することができる。
【００２７】
本実施の形態１における「通信状況記録部」は、通信観測部２０２、通信記録部２０３が相当する。
【００２８】
以上、本実施の形態１に係る障害解析システムの各装置等の構成を説明した。
次に、本実施の形態１に係る障害解析システムの動作を説明する。
【００２９】
本実施の形態１に係る障害解析システムは、全体としては後述の図２で説明する動作を行う。また、ゲートウェイ装置２００は、障害解析システムの全体動作と並行して、後述の図４で説明する通信記録動作を行う。
以下では、まず始めに障害解析システムの全体動作を図２で説明し、個別の動作については図３～図５で説明する。
【００３０】
図２は、本実施の形態１に係る障害解析システムの動作フローである。以下、図２の各ステップについて説明する。
【００３１】
（Ｓ２０１）
図１の機器４０１で障害が発生したものと仮定する。
（Ｓ２０２）
ゲートウェイ装置２００の障害検知部２０１は、機器４０１で発生した障害を検知する。検知する手法としては、例えば動作情報取得部２０４が取得した動作情報５０１を解析する、機器４０１のプロセスを監視する、といった手法が考えられる。また、特許文献１～２に記載されているような公知の手法を用いてもよい。
【００３２】
（Ｓ２０３）
障害検知部２０１は、機器４０１に障害が発生した旨を、ネットワーク６００を介して解析サーバ３００に送信する。あるいは、障害検知部２０１は、機器４０１に障害が発生した旨を適当な手法でユーザに通知し、ユーザはその通知を受けて電話や電子メールでコ

ールセンターにその旨を連絡する。
なおここでは、コールセンターのオペレータは、解析サーバ３００に対し操作指示を行うことができる端末等を有しているものと仮定する。
【００３３】
（Ｓ２０４）
コールセンターのオペレータは、ステップＳ２０３で受けた障害発生の通知に基づき、障害原因の分析等を行うために必要な動作情報を取得するよう、解析装置３００に指示する。
なお、コールセンターのオペレータではなく、障害発生の通知に基づき、動作情報を取得するように自動的に指示する装置にしてもよい。
解析装置３００の動作情報要求部３０２は、その取得要求が、障害発生機器（ここでは機器４０１）の動作情報５０１を取得する要求であるか、それとも障害に関連する機器（例えば４０２、４０３、４０４）の動作情報（例えば５０２、５０３、５０４）を取得する要求であるかを判定する。
障害発生機器４０１についての取得要求であればステップＳ２０５へ進み、関連機器４０２等についての取得要求であればステップＳ２１１へ進む。
【００３４】
（Ｓ２０５）
解析装置３００の動作情報要求部３０２は、ゲートウェイ装置２００に対し、機器４０１の動作情報５０１を送信するよう要求する。
【００３５】
（Ｓ２０６）
ゲートウェイ装置２００の動作情報取得部２０４は、ステップＳ２０５の要求を受け取ったときは、機器４０１の動作情報５０１を取得する。また、ステップＳ２１１の要求を受け取ったときは、関連機器の動作情報を取得する。本ステップの詳細は、後述の図３で改めて説明する。
以下のステップＳ２０７～Ｓ２１０の説明では、本ステップでステップＳ２０５の要求を受け取ったものと仮定する。
【００３６】
（Ｓ２０７）
動作情報取得部２０４は、ステップＳ２０６で取得した動作情報５０１を、ネットワーク６００を介して解析サーバ３００に送信する。
このとき、動作情報取得部２０４は、ＡＥＳ（Ａｄｖａｎｃｅｄ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）のような共通鍵暗号や、ＲＳＡのような公開鍵暗号を用いて送信データを暗号化したり、ＳＳＬ（Ｓｅｃｕｒｅ　Ｓｏｃｋｅｔ　Ｌａｙｅｒ）やＩＰｓｅｃのような通信路暗号化技術を用いたりして、送信する内容に何らかのセキュリティ対策を施す。
【００３７】
（Ｓ２０８）
解析サーバ３００の障害解析部３０１は、機器４０１の動作情報５０１を受信する。次に、障害解析部３０１は、その動作情報５０１を解析し、障害原因などの分析を行う。
（Ｓ２０９）
障害解析部３０１は、より詳細な解析を行うために、動作情報５０１以外の動作情報（図１の例では５０２～５０４）が更に必要であるか否かを判断する。必要であると判断するときはステップＳ２０４へ戻り、必要でないと判断するときはステップＳ２１０へ進む。
【００３８】
（Ｓ２１０）
解析サーバ３００の障害解析部３０１は、障害分析を完了し、コールセンターのオペレータに結果を通知する。オペレータは、その結果に基づき、ユーザにアドバイスを行うな

どの対処を取る。これらを自動で行ってもよいが、セキュリティ等の観点から、このような手法用いる方が望ましい。
（Ｓ２１１）
一方、上記ステップ２０４において、関連機器４０２等についての取得要求であれば、解析装置３００の動作情報要求部３０２は、ゲートウェイ装置２００に対し、機器４０１の障害発生と関連のある動作情報を送信するよう要求し、上記Ｓ２０６に進む。
【００３９】
以上、本実施の形態１に係る障害解析システムの動作フローを説明した。
次に、ステップＳ２０６の詳細動作を説明する。
【００４０】
図３は、ステップＳ２０６の詳細動作を説明する動作フローである。以下、図３の各ステップについて説明する。なお、図３では、図２と同様に機器４０１に障害が発生した場合を想定する。
【００４１】
（Ｓ３０１）
ゲートウェイ装置２００の動作情報取得部２０４は、図２のステップＳ２０５またはＳ２１１で、機器４０１～４０４のいずれかの動作情報を取得するよう要求を受け取る。次に、この取得要求が、障害発生機器（図２の例では機器４０１）についての動作情報取得要求であるか否かを判定する。
障害発生機器についての動作情報取得要求であればステップＳ３０４へ進み、それ以外の場合はステップＳ３０２へ進む。
【００４２】
（Ｓ３０２）
動作情報取得部２０４は、通信記録部２０３が格納している通信記録の中から、機器４０１の通信記録を検索する。次に、機器４０１と過去に通信を行った機器（例えば、４０２、４０３、４０４）を、その検索結果に基づき抽出する。通信記録の具体例は後述の図５で示す。
本ステップは、機器４０１と過去に通信を行った機器が、機器４０１の障害発生に関連しているだろうとの想定の下、それらの機器を通信記録の中から検索する意義がある。
【００４３】
（Ｓ３０３）
動作情報取得部２０４は、ステップＳ３０２で検索した機器（例えば、４０２、４０３、４０４）の動作情報（例えば５０２、５０３、５０４）を取得する。このとき、当該機器のＩＰアドレス等、機器の個体識別を行うことのできる情報を併せて取得して動作情報に含めてもよい。ステップＳ３０４でも同様である。
（Ｓ３０４）
動作情報取得部２０４は、機器４０１の動作情報５０１を取得する。
【００４４】
以上、図２のステップＳ２０６の詳細動作について説明した。
次に、ゲートウェイ装置２００が機器４０１～４０４の通信状況を通信記録部２０３に記録する動作を説明する。
【００４５】
図４は、ゲートウェイ装置２００が常時行っている、機器４０１～４０４の通信状況を記録する動作のフローチャートである。ゲートウェイ装置２００は、図４の動作を、例えば所定時間間隔で実行し、機器４０１～４０４の通信状況を定常的に記録する。
以下、図４の各ステップについて説明する。なお、通信記録の記録形式の例については、後述の図５で改めて説明する。
【００４６】
（Ｓ４００）
ゲートウェイ装置２００の通信観測部２０２は、図２～図３で説明した各部の動作と並

行して、機器４０１～４０４間の通信を常時観測している。
（Ｓ４０１）
通信観測部２０２は、機器４０１～４０４間で通信が行われると、その通信パケットを捕捉する。
【００４７】
（Ｓ４０２）
通信観測部２０２は、ステップＳ４０１で捕捉したパケットから、送信元アドレスと送信先アドレスのペアを抽出する。ここではＩＰアドレスを抽出するものとする。
（Ｓ４０３）
通信観測部２０２は、ステップＳ４０１で抽出した送信元アドレスと送信先アドレスのペアが、通信記録部２０３に既に記録済みであるか否かを判定する。記録済みであればステップＳ４０５へ進み、記録済みでなければステップＳ４０４へ進む。
【００４８】
（Ｓ４０４）
通信観測部２０２は、ステップＳ４０２で抽出した送信元アドレスと送信先アドレスのペアを、抽出時刻とともに通信記録部２０３に格納する。
（Ｓ４０５）
通信観測部２０２は、ステップＳ４０２で抽出した送信元アドレスと送信先アドレスに該当する通信記録部２０３内の通信記録を、ステップＳ４０２の抽出時刻で時刻のみ更新する。
【００４９】
（Ｓ４０６）
通信観測部２０２は、現在時刻よりも所定時間以上前に通信記録部２０３に記録された通信記録を削除する。具体的には、現在時刻と、通信記録部２０３に記録されている通信記録の記録時刻とを比較し、所定時間以上前の通信記録を削除する。これにより、最新の通信状況だけが通信記録部２０３に残り、障害に関連する機器だけの情報が残せるとともに、通信記録部２０３の記憶領域が膨大なることを防ぐことができる。
【００５０】
以上、通信観測部２０２の動作を説明した。本動作フローを繰り返し実行することにより、機器４０１～４０４間の通信記録が通信記録部２０３に追加更新されていく。
【００５１】
図５は、通信記録部２０３が格納する通信記録の形式例である。ここではテーブル形式で記録する例を示したが、記録形式はこれに限られるものではない。
【００５２】
通信記録は、「ＩＰアドレス」列、「記録時刻」列を有する。
「ＩＰアドレス」列には、通信観測部２０２が捕捉した通信パケットの送信元ＩＰアドレスと送信先ＩＰアドレスのペアが格納される。本実施の形態１における「識別情報」は本列の値がこれに相当する。
「記録時刻」列には、「ＩＰアドレス」列のアドレスペアの通信を記録した最新時刻が格納される。
【００５３】
以下、図５のデータ例において、機器４０１のＩＰアドレスを「１９２．１６８．０．５」であると仮定し、図３のステップＳ３０２～Ｓ３０３における動作例を説明する。
【００５４】
（Ｓ３０２＿１）
図３のステップＳ３０２において、動作情報取得部２０４は、ＩＰアドレス「１９２．１６８．０．５」をキーにして、機器４０１の通信記録を検索する。図５のデータ例では、１行目と２行目のデータが検索にヒットする。
【００５５】
（Ｓ３０２＿２）

図３のステップＳ３０２において、動作情報取得部２０４は、上記ステップで取得した各行の相手方機器のアドレスを取得する。図５のデータ例では、「１９２．１６８．０．７」「１９２．１６８．０．９」を取得することになる。

このステップにより、過去に機器４０１の通信相手となって連係動作していた機器のアドレスを特定することができる。

【００５６】

（Ｓ３０３）

図３のステップＳ３０３において、動作情報取得部２０４は、上記ステップ（Ｓ３０２＿２）で取得したアドレス「１９２．１６８．０．７」「１９２．１６８．０．９」の各機器の動作情報を取得する。

【００５７】

以上、本実施の形態１に係る障害分析システムおよび各装置等の動作を説明した。

なお、図２のステップＳ２０４において、既に同じ機器についての動作情報を要求済みであるか否かにより、いずれの機器についての動作情報を要求するかを区別したが、区別する手順はこれに限られるものではない。

【００５８】

例えば、解析サーバ３００側では常に障害発生機器（本実施の形態１では機器４０１）についての動作情報を要求しておき、ゲートウェイ装置２００側で、既に機器４０１の動作情報５０１を送信したか否かに基づき、いずれの機器についての動作情報を要求するかを判定するようにしてもよい。

具体的には、以下のような手法が考えられる。

【００５９】

（ゲートウェイ装置２００側で送信済みか否かを判定する手法例）

ゲートウェイ装置２００の動作情報取得部２０４は、動作情報を送信した機器のリストを一定時間保持しておく。その一定時間内に再び同じ機器について動作情報を要求されたときは、その機器についての動作情報は既に送信済みであると判断する。

動作情報取得部２０４は、当該機器についての動作情報を既に送信済みであると判断したときは、通信記録部２０３の通信記録から、当該機器に関連する機器のアドレスを検索し、その機器の動作情報を代わりに送信する。

【００６０】

以上のように、本実施の形態１に係る障害分析システムは、機器４０１～４０４間の通信記録を一定時間通信記録部２０３に格納しておく。

また、例えば機器４０１に障害が発生したとき、動作情報取得部２０４は、その通信記録を用いて、直近で機器４０１と通信していた機器を特定することにより、障害に関連すると想定される機器を絞り込んだ上で、その関連機器の動作情報を解析サーバ３００に送信する。

【００６１】

これにより、解析サーバ３００は、障害が発生した機器４０１のみならず、障害に関連すると思われる機器の動作情報も解析することができるので、障害をより詳細に解析することができる。

【００６２】

また、本実施の形態１によれば、ローカルネットワーク１００上の全ての機器から動作情報を解析サーバ３００に送信するのではなく、障害に関連すると思われる機器の動作情報のみを送信するので、通信量を抑えることができる。

同時に、障害解析に関係しない動作情報がローカルネットワーク１００の外部へ流れることを抑制できるので、プライバシーの観点から好ましい。

【００６３】

また、本実施の形態１によれば、解析サーバ３００が解析すべき動作情報の量も、同様に抑えることができるので、障害解析部３０１が行う解析時間を短縮することができる。

【００６４】

実施の形態２．
実施の形態１では、ゲートウェイ装置２００の通信観測部２０２は、ローカルネットワーク１００上の全てのパケットを観測して通信相手機器のアドレスを抽出することとしたが、これ以外にも以下のようなアドレス抽出手法が考えられる。
【００６５】
（アドレス抽出手法１）
通信観測部２０２は、ローカルネットワーク１００上のパケットを適宜サンプリングした上で、そのサンプリングしたパケットから、送信元アドレスと送信先アドレスを抽出する。
【００６６】
（アドレス抽出手法２）
通信観測部２０２は、ＳＩＰ（Ｓｅｓｓｉｏｎ Ｉｎｉｔｉａｔｉｏｎ Ｐｒｏｔｏｃｏｌ）のような、機器４０１～４０４間で通信が開始される時にローカルネットワーク１００上を流れるパケットを捕捉し、そのパケットから送信元アドレスと送信先アドレスを抽出する。
【００６７】
（アドレス抽出手法３）
通信観測部２０２は、ＤＬＮＡ（Ｄｉｇｉｔａｌ Ｌｉｖｉｎｇ Ｎｅｔｗｏｒｋ Ａｌｌｉａｎｃｅ）やＥｃｈｏｎｅｔのようなホームネットワーク向けの通信規格などで定められている、ネットワーク内の機器を発見するためのパケットを捕捉し、そのパケットからローカルネットワーク１００上の機器４０１～４０４のアドレスを取得する。
【００６８】
実施の形態３．
図６は、本発明の実施の形態３に係る障害解析システムの構成図である。
本実施の形態３において、ゲートウェイ装置２００は、実施の形態１の図１で説明した構成に加え、新たにフィルタリング部２０５、フィルタ規則格納部２０６を備える。その他の各装置等の構成は、実施の形態１～２と同様である。
【００６９】
フィルタリング部２０５は、動作情報取得部２０４が取得した動作情報を、フィルタ規則格納部２０６が格納しているフィルタ規則にしたがってフィルタリングし、重要度の高い項目のみを抽出する。
フィルタ規則格納部２０６は、フィルタリング部２０５がフィルタリングを行うための規則を格納している。具体例は後述の図８で説明する。
【００７０】
フィルタリング部２０５は、その機能を実現する回路デバイスのようなハードウェアで構成することもできるし、マイコンやＣＰＵのような演算装置とその動作を規定するソフトウェアで構成することもできる。
【００７１】
フィルタ規則格納部２０６は、ＨＤＤのような記憶装置で構成することができる。
【００７２】
フィルタリング部２０５は、動作情報取得部２０４と一体的に構成してもよい。また、フィルタ規則格納部２０６は、通信記録部２０３と一体的に構成してもよい。
【００７３】
図７は、本実施の形態３に係る障害解析システムの動作フローである。以下、図７の各ステップについて説明する。なお、図２と同様に、機器４０１で障害が発生したものと仮定する。
【００７４】
（Ｓ７０１）～（Ｓ７０６）
図２のステップＳ２０１～Ｓ２０６と同様である。
（Ｓ７０７）

フィルタリング部２０５は、ステップＳ７０６で動作情報取得部２０４が取得した動作情報をフィルタリングし、重要度の高い項目を抽出する。本ステップの詳細は、後述の図１０で改めて説明する。

（Ｓ７０８）～（Ｓ７１２）

図２のステップＳ２０７～Ｓ２１１と同様である。

【００７５】

以上、本実施の形態３に係る障害解析システムの動作フローを説明した。

次に、フィルタリングに関して詳細を説明する。

【００７６】

図８は、フィルタ規則格納部２０６が格納しているフィルタ規則の例である。ここではテーブル形式で格納している例を示したが、フィルタ規則の形式はこれに限られるものではない。

【００７７】

フィルタ規則は、「抽出規則」列、「重要度」列を有する。

「抽出規則」列には、動作情報から項目を抽出する規則が格納される。

「重要度」列では、「抽出規則」列で抽出される動作情報項目の重要度が指定される。図８では、重要度「１」を最重要とし、数値が増えるほど重要度が下がるものとした。

重要度とは、当該動作情報項目の深刻度と概ね同義である。即ち、重要度が高い動作情報項目は深刻な障害もしくはその前兆を示している可能性が高い。

【００７８】

なお、図８では、説明の便宜上、日本語で各列の値を記載したが、実際には正規表現などの機械可読形式で各列を表した方が、処理の上では都合よい。

【００７９】

図９は、動作情報５０１のデータ例である。ここでは、機器４０１の内部プロセスのログを動作情報５０１とした例を示す。

動作情報５０１は、１行で１つのログ項目を表す。１つのログ項目には、そのログ項目の重要度を表す文字列（図９のＩＮＦＯ、ＥＲＲＯＲなど）と、ログの内容を表す文字列とが記載される。

【００８０】

図１０は、フィルタリング部２０５が行うフィルタリング処理のフローである。以下、図１０の各ステップについて説明する。なお、説明に際し、フィルタ規則は図８、動作情報５０１は図９のデータ例を用いる。

【００８１】

（Ｓ１００１）

フィルタリング部２０５は、フィルタ規則格納部２０６から、重要度が高い順にフィルタ規則を選択する。図８のフィルタ規則例では、本ステップを最初に実行するときは１行目と４行目のフィルタ規則を選択し、２回目に実行するときは２行目のフィルタ規則を選択することになる。

（Ｓ１００２）

フィルタリング部２０５は、図９の動作情報５０１に、ステップＳ１００１で選択したフィルタ規則を適用する。

【００８２】

（Ｓ１００３）

フィルタリング部２０５は、図９の動作情報５０１の各行に記載されている動作情報項目のうち、ステップＳ１００１で選択したフィルタ規則に適合するものを抽出する。

（Ｓ１００４）

フィルタリング部２０５は、図８の全てのフィルタ規則について以上のステップを実行したか否かを確認する。未処理のフィルタ規則が残っていればステップＳ１００１に戻って同様の処理を実行し、全て処理済であれば本動作フローを終了する。

【００８３】

図１１は、図１０の動作フローの処理結果として得られるフィルタリング後の動作情報５０１を示すものである。

図８のフィルタ規則を図９の動作情報５０１に適用すると、「重要度」が「ＦＡＴＡＬ」「ＥＲＲＯＲ」「ＷＡＲＮ」の３種類のログ項目が抽出され、図１１の３行が最終的に残ることになる。

【００８４】

なお、図８～図１１では、全てのフィルタ規則を適用する例を説明したが、フィルタ規則格納部２０６が格納しているフィルタ規則のうち一部のみを動作情報に適用するようにしてもよい。

【００８５】

以上のように、本実施の形態３によれば、フィルタリング部２０５は、フィルタ規則格納部２０６が格納しているフィルタ規則を用いて、動作情報取得部２０４が取得した動作情報から重要度が高いものを抽出した上で、解析サーバ３００に送信する。

これにより、ゲートウェイ装置２００は、解析サーバ３００が障害解析を行うために有用な、即ち重要度の高い動作情報のみを絞り込んで解析サーバ３００に送信することができるので、通信量をさらに抑えることができる。

また、ローカルネットワーク１００外に送信する情報を最小限に抑えることができるので、プライバシーの観点からも好ましい。

【００８６】

実施の形態４．

実施の形態３では、フィルタ規則格納部２０６はフィルタ規則をあらかじめ格納済みであることを想定したが、フィルタ規則を以下に述べる手法で生成することもできる。

いずれの手法であっても、フィルタ規則は、障害解析を行うに際して有用である項目に高い重要度が割り当てられるように生成される。

【００８７】

（フィルタ規則生成手法１）

コールセンターのオペレータや技術者等は、過去に障害解析を行った経験に基づき、障害解析に有用であった共通的な動作情報パターンを抽出する。抽出したパターンをフィルタ規則の形式に整形し、解析サーバ３００よりゲートウェイ装置２００のフィルタ規則格納部２０６に宛てて送信する。

【００８８】

（フィルタ規則生成手法２）

解析サーバ３００の障害解析部３０１は、障害解析結果に基づき、障害解析に有用であった動作情報の項目に重要度の値を割り当てる。次に、障害解析部３０１は、その重要度と動作情報の項目を用いてフィルタ規則を生成し、ゲートウェイ装置２００のフィルタ規則格納部２０６に宛てて送信する。

【００８９】

（フィルタ規則生成手法３）

障害解析に有用であった動作情報の項目にマークを付与する重要情報指示部を、解析サーバ３００に設けておく。具体的には、例えばオペレータが動作情報と障害解析結果を画面上で確認しながら、目視確認により動作情報の項目の中で重要なものを選別し、重要項目を画面上でクリックするなどしてマークする。

解析サーバ３００の障害解析部３０１は、オペレータが指示したマークの統計を取り、多くマークが付与された動作情報の項目に高い重要度を割り当てて、フィルタ規則を作成する。また、作成したフィルタ規則を、ゲートウェイ装置２００のフィルタ規則格納部２０６に宛てて送信する。

【００９０】

（フィルタ規則生成手法４）

ゲートウェイ装置２００の障害検知部２０１は、機器４０１～４０４の障害を検知すると、その時刻を解析サーバ３００の障害解析部３０１に通知する。

障害解析部３０１は、後に動作情報を用いてフィルタ規則を生成する。このとき、障害発生時刻から時間的に離れている動作情報項目ほど重要度が低くなるよう、フィルタ規則を生成する。

【００９１】

（フィルタ規則生成手法５）

フィルタ規則は、障害発生時刻から時刻が離れている動作情報ほど重要度が低くなるように構成することもできる。

この場合、フィルタ規則は、ゲートウェイ装置２００から解析サーバ３００へ障害発生時刻を通知して解析サーバ３００で生成することもできるし、ゲートウェイ装置２００で生成することもできる。

【００９２】

以上の（フィルタ規則生成手法１）～（フィルタ規則生成手法５）は、適宜組み合わせて用いることもできる。

【００９３】

実施の形態５．

実施の形態１～４では、解析サーバ３００の動作情報要求部３０２は、ゲートウェイ装置２００に対し、障害発生機器に関連する機器についての動作情報を送信するよう要求することを説明した。これは、先に送信した動作情報のみでは、障害解析に不十分であったことを示唆する。

【００９４】

しかし、実施の形態３～４で説明した場合のように、そもそも重要度の高い動作情報のみをフィルタリング抽出して解析サーバに送信しているときは、フィルタリングで排除された動作情報を改めて解析サーバ３００に送信すれば足りる可能性がある。

【００９５】

そこで、ゲートウェイ装置２００の動作情報取得部２０４は、解析サーバ３００の動作情報要求部３０２よりさらに動作情報を送信するよう要求されたとき、フィルタリング部２０５がフィルタリング処理で排除した動作情報を、解析サーバ３００に送るようにしてもよい。

その上でなお、さらに動作情報を送信するよう要求されたときは、改めて実施の形態１で説明したように関連機器の動作情報を取得し、解析サーバ３００に送信するとよい。

【００９６】

実施の形態６．

以上の実施の形態１～５で説明した解析サーバ３００に、障害を検知した機器４０１～４０４の復旧を試みるようゲートウェイ装置２００に要求する、復旧要求部３０３（図示せず）を設けることもできる。

【００９７】

復旧要求部３０３は、その機能を実現する回路デバイスのようなハードウェアで構成することもできるし、マイコンやＣＰＵのような演算装置とその動作を規定するソフトウェアで構成することもできる。また、必要な通信インターフェース等を適宜備える。

【００９８】

ゲートウェイ装置２００は、復旧要求部３０３より障害発生機器の復旧要求を受けるとその機器を再起動するなどして復旧を試みる。その後、動作情報取得部２０４は、その機器の動作情報を改めて取得し、解析サーバ３００に送信する。

解析サーバ３００は、その動作情報を受け取り、復旧が成功したか否かを知ることができる。オペレータはその結果に基づき、次の対処を行う。

【図面の簡単な説明】

【００９９】

【図１】実施の形態１に係る障害解析システムの構成図である。

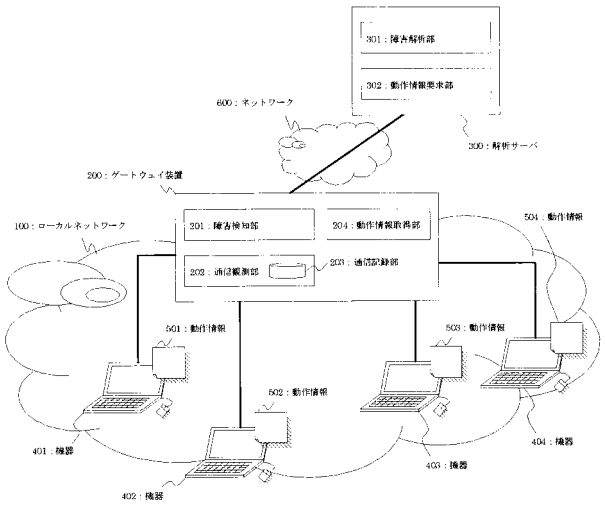
【図２】実施の形態１に係る障害解析システムの動作フローである。

【図３】ステップＳ２０６の詳細動作を説明する動作フローである。

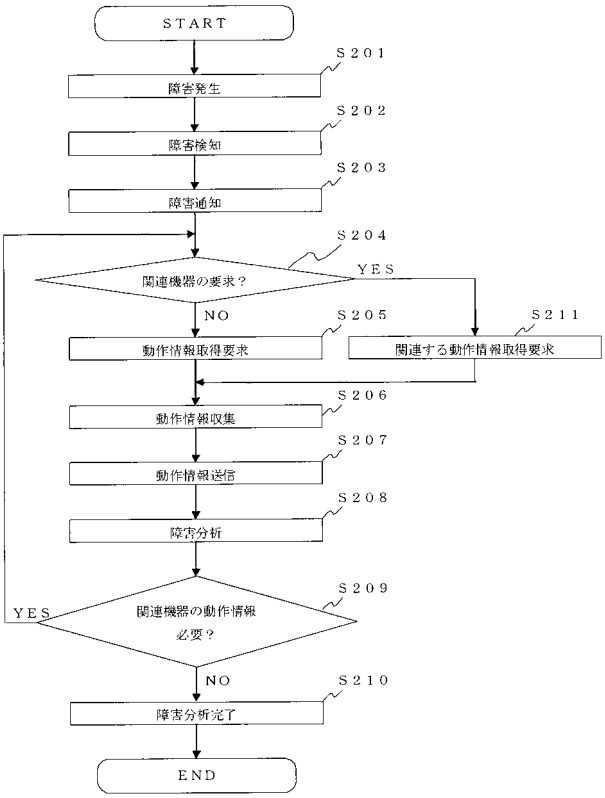
【図４】ゲートウェイ装置２００が機器４０１～４０４の動作情報５０１～５０４を記録する動作のフローチャートである。
【図５】通信記録部２０３が格納する通信記録の形式例である。
【図６】実施の形態３に係る障害解析システムの構成図である。
【図７】実施の形態３に係る障害解析システムの動作フローである。
【図８】フィルタ規則格納部２０６が格納しているフィルタ規則の例である。
【図９】動作情報５０１のデータ例である。
【図１０】フィルタリング部２０５が行うフィルタリング処理のフローである。
【図１１】図１０の動作フローの処理結果として得られるフィルタリング後の動作情報５０１を示すものである。

【符号の説明】
【０１００】
１００　ローカルネットワーク、２００　ゲートウェイ装置、２０１　障害検知部、２０２　通信観測部、２０３　通信記録部、２０４　動作情報取得部、２０５　フィルタリング部、２０６　フィルタ規則格納部、３００　解析サーバ、３０１　障害解析部、３０２　動作情報要求部、３０３　復旧要求部、４０１～４０４　機器、５０１～５０４　動作情報、６００　ネットワーク。

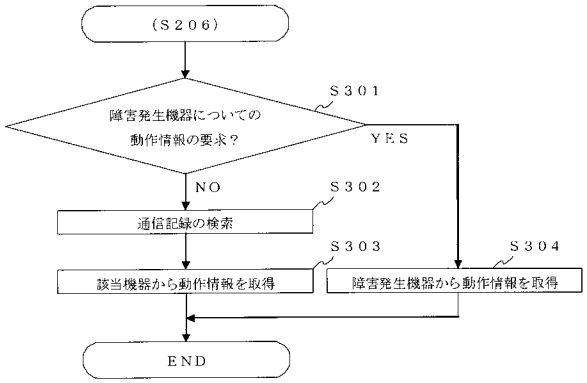
【図１】



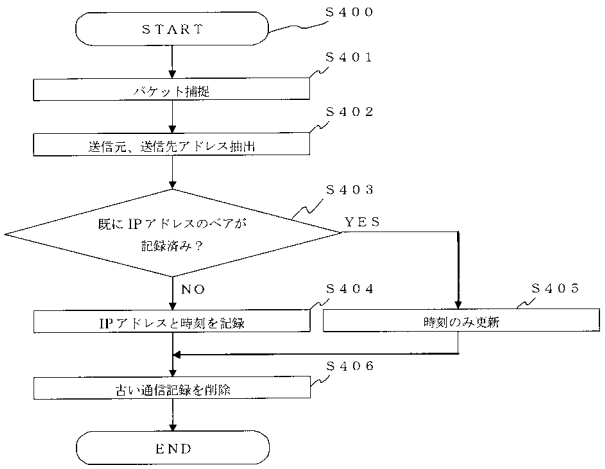
【図２】



【図３】



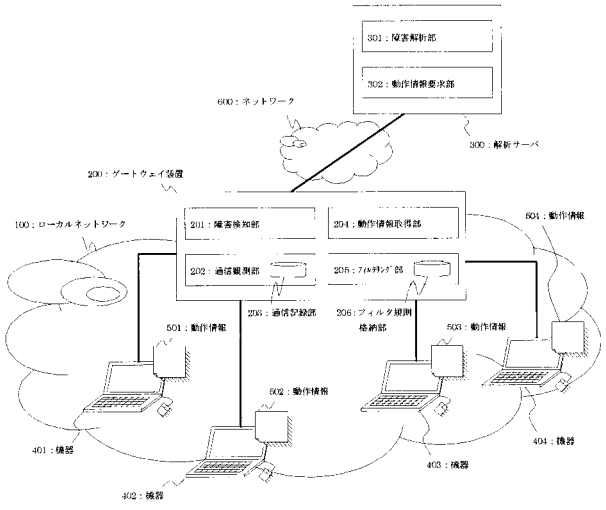
【図４】



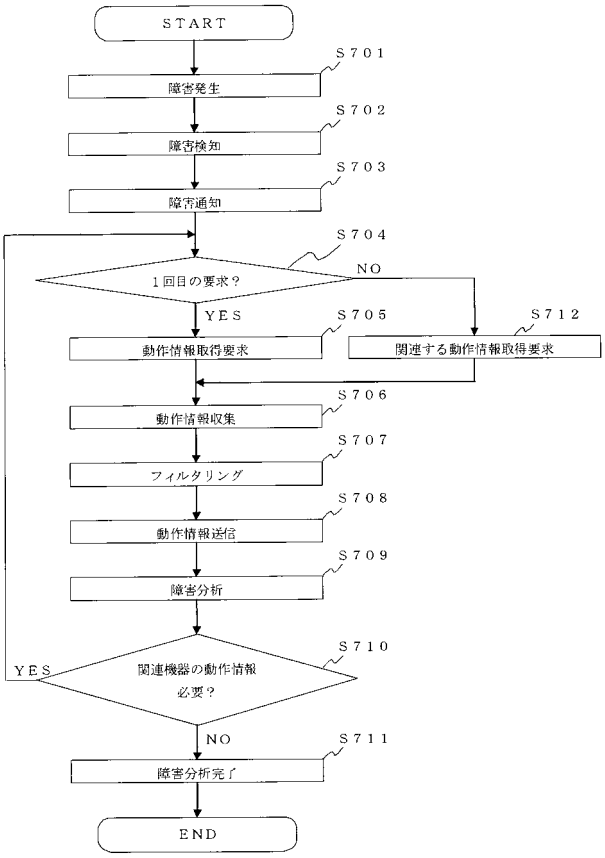
【図５】

ＩＰアドレス	記録時刻
<192.168.0.5, 192.168.0.7>	11：02：05
<192.168.0.5, 192.168.0.9>	11：04：23
<192.168.0.7, 192.168.0.9>	10：58：32

【図６】



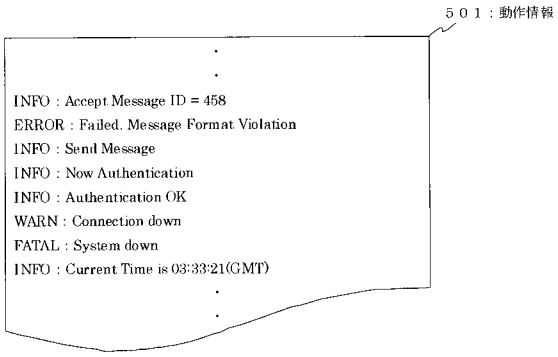
【図７】



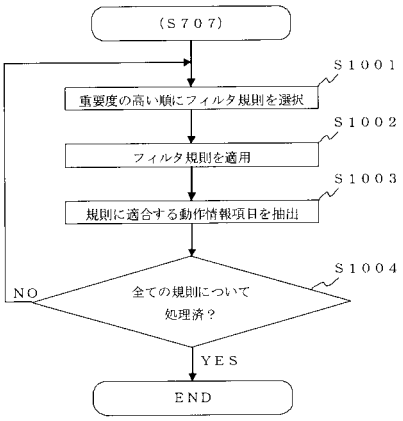
【図８】

抽出規則	重要度
文字列FATALを含む行	1
文字列ERRORを含む行	2
文字列WARNを含む行	3
文字列ACCEPTを含む行の次行がFAILEDまたはDENYを含む行	1

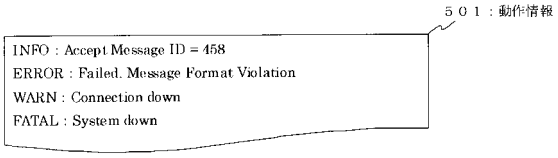
【図９】



【図１０】



【図１１】



フロントページの続き

(74)代理人 100070563
弁理士 大村 昇
(74)代理人 100087620
弁理士 高梨 範夫
(72)発明者 森井 昌克
徳島市徳島町２丁目３２ サーパス徳島中央公園１１０１
(72)発明者 伊加田 恵志
東京都港区西新橋三丁目１６番１１号 沖電気工業株式会社内
(72)発明者 濱口 佳孝
東京都港区西新橋三丁目１６番１１号 沖電気工業株式会社内

Ｆターム(参考) 5B089 MC01 MC11
5K030 GA12 HD03 HD06 KA07 LE07 MB01 MC09
5K033 AA06 BA01 DA01 DA06 DB20 EA03 EA04 EA07
5K201 BA02 CB10 CC09 EA08 EC06 EE04 FA03 FB08