(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2020-144954
(P2020-144954A)
(43)公開日　令和2年9月10日(2020.9.10)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 11/07	(2006.01)	G06F	11/07	175	5B042
G06F 11/32	(2006.01)	G06F	11/32	170	
		G06F	11/07	140A	

審査請求 未請求　請求項の数 10　OL　（全 14 頁）

(21)出願番号　特願2020-102233 (P2020-102233)
(22)出願日　令和2年6月12日 (2020.6.12)
(62)分割の表示　特願2018-134784 (P2018-134784)の分割
原出願日　平成30年7月18日 (2018.7.18)

(71)出願人　319013263
ヤフー株式会社
東京都千代田区紀尾井町１番３号
(74)代理人　100149548
弁理士　松沼　泰史
(74)代理人　100154852
弁理士　酒井　太一
(74)代理人　100181124
弁理士　沖田　壮男
(74)代理人　100194087
弁理士　渡辺　伸一
(72)発明者　望月　哲也
東京都千代田区紀尾井町１番３号　ヤフー株式会社内

最終頁に続く

(54)【発明の名称】監視装置、監視方法、およびプログラム

(57)【要約】
【課題】アラートの監視の負荷を軽減することが可能な監視装置、監視方法、およびプログラムを提供する。
【解決手段】本発明の一態様は、複数の監視対象に関するアラートにより示される事象間の関連の有無を判定することにより関連を有する事象をグループ化し、関連を有する事象の内、最初に発生した事象を第１事象として設定し、第１事象以外の事象を第２事象として設定する、判定部と、グループ化された事象ごとに、アラートにより示される事象の対応状況を管理する管理部と、グループ化された事象ごとに、第１事象の対応状況に関する情報と、第１事象に関連付けられた第２事象の情報とを含む第１画面を表示部に表示させる表示制御部と、を備え、管理部は、第１画面におけるオペレータの操作に基づいて第１事象の対応状況が対応完了に設定された場合、第１事象と関連付けられた第２事象の対応状況も自動的に対応完了に設定する、監視装置である。
【選択図】図２

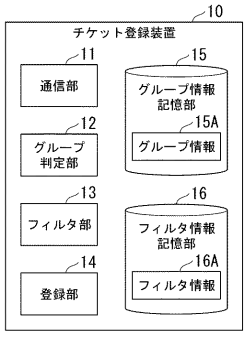

図２

【特許請求の範囲】
【請求項１】
複数の監視対象に関するアラートにより示される事象間の関連の有無を判定することにより関連を有する事象をグループ化し、前記関連を有する事象の内、最初に発生した事象を第１事象として設定し、前記第１事象以外の事象を第２事象として設定する、判定部と、
前記判定部によりグループ化された事象ごとに、前記アラートにより示される事象の対応状況を管理する管理部と、
前記判定部によりグループ化された事象ごとに、前記第１事象の対応状況に関する情報と、前記第１事象に関連付けられた前記第２事象の情報とを含む第１画面を表示部に表示させる表示制御部と、
を備え、
前記管理部は、前記第１画面におけるオペレータの操作に基づいて前記第１事象の対応状況が対応完了に設定された場合、前記第１事象と関連付けられた前記第２事象の対応状況も自動的に対応完了に設定する、
監視装置。
【請求項２】
前記表示制御部は、手動により追加の事象の登録が可能な前記第１画面を前記表示部に表示させ、
前記管理部は、前記第１画面における前記オペレータの操作に基づいて前記追加の事象の登録が行われた場合、前記追加の事象を前記第１事象に関連付けする、
請求項１に記載の監視装置。
【請求項３】
前記管理部は、前記第１画面における前記オペレータの操作に基づいて、前記判定部により前記第１事象と関連付けられなかった前記追加の事象を、前記第１事象に関連付けする、
請求項２に記載の監視装置。
【請求項４】
前記表示制御部は、サービスごとに関連付けられた事象を一覧表示する第２画面を前記表示部に表示させる、
請求項１から３のいずれか一項に記載の監視装置。
【請求項５】
前記表示制御部は、所望のアラートに関して、要対応、要確認、および対応不要として処理された事象の件数を示すグラフを表示する第３画面を前記表示部に表示させる、
請求項１から４のいずれか一項に記載の監視装置。
【請求項６】
前記判定部は、前記アラートに含まれる情報の中から前記監視対象を個別に特定するための情報を除去する編集処理を行い、編集処理後の前記アラートを互いに比較することで前記事象間の関連の有無を判定する、
請求項１から５のいずれか一項に記載の監視装置。
【請求項７】
予め定義された前記アラートごとの対応要否の条件を含むフィルタ情報に基づいて、前記アラートにより示される事象に対する対応要否を判定し、対応が不要な事象をフィルタリングするフィルタ部をさらに備え、
前記表示制御部は、前記判定部によりグループ化された事象ごとに、前記フィルタ部により対応が必要と判定された前記事象に関する情報を含む前記第１画面を前記表示部に表示させる、
請求項１から６のいずれか一項に記載の監視装置。
【請求項８】
前記表示制御部は、前記アラートごとの前記フィルタ情報の登録を受け付ける第４画面

を前記表示部に表示させる、
　請求項７に記載の監視装置。
【請求項９】
　コンピュータが、
　複数の監視対象に関するアラートにより示される事象間の関連の有無を判定することにより関連を有する事象をグループ化し、前記関連を有する事象の内、最初に発生した事象を第１事象として設定し、前記第１事象以外の事象を第２事象として設定し、
　グループ化された前記事象ごとに、前記アラートにより示される事象の対応状況を管理し、
　グループ化された前記事象ごとに、前記第１事象の対応状況に関する情報と、前記第１事象に関連付けられた前記第２事象の情報とを含む第１画面を表示部に表示させる、
　監視方法であって、
　前記第１画面におけるオペレータの操作に基づいて前記第１事象の対応状況が対応完了に設定された場合、前記第１事象と関連付けられた前記第２事象の対応状況も自動的に対応完了に設定する、
　監視方法。
【請求項１０】
　コンピュータに、
　複数の監視対象に関するアラートにより示される事象間の関連の有無を判定することにより関連を有する事象をグループ化させ、前記関連を有する事象の内、最初に発生した事象を第１事象として設定させ、前記第１事象以外の事象を第２事象として設定させ、
　グループ化された前記事象ごとに、前記アラートにより示される事象の対応状況を管理させ、
　グループ化された前記事象ごとに、前記第１事象の対応状況に関する情報と、前記第１事象に関連付けられた前記第２事象の情報とを含む第１画面を表示部に表示させる、
　プログラムであって、
　前記第１画面におけるオペレータの操作に基づいて前記第１事象の対応状況が対応完了に設定された場合、前記第１事象と関連付けられた前記第２事象の対応状況も自動的に対応完了に設定させる、
　プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
　本発明は、監視装置、監視方法、およびプログラムに関する。
【背景技術】
【０００２】
　従来、監視システムにより出力されるアラートメール、アラートログ等に基づいて、機器等の異常を監視する運用が行われている。例えば、特許文献１には、監視対象のサーバにより出力されるエラーログと、このエラーログに含まれるエラーコードに対応する手順マニュアルとをオペレータが使用する端末に送信するシステムが開示されている。
【先行技術文献】
【特許文献】
【０００３】
【特許文献１】特開２０１５－２１５７３９号公報
【発明の概要】
【発明が解決しようとする課題】
【０００４】
　多数のサーバを監視する場合、オペレータは、２４時間３６５日にわたって出力される膨大な数のアラートを確認し、各アラートに応じた対応を行う必要がある。このため、これらの確認および対応によるオペレータの作業負荷が増大していた。また、サービスごと

に設けられた複数の監視システムにより出力されるアラートを監視センター等で集約的に管理している場合、アラートの通知方法や内容が多種多様であり、これらの確認に手間を要していた。

【０００５】

また、これらのアラートは全てに対して対応が必要となるわけではなく、無視してもよいものも多く含まれているが、オペレータはその要否をアラートごとに判断する必要があった。また、アラートの対応漏れを常時確認する必要があり、作業効率の改善が望まれていた。

【０００６】

本発明は、このような事情を考慮してなされたものであり、アラートの監視の負荷を軽減することが可能な監視装置、監視方法、およびプログラムを提供することを目的の一つとする。

【課題を解決するための手段】

【０００７】

本発明の一態様は、複数の監視対象に関するアラートにより示される事象間の関連の有無を判定することにより関連を有する事象をグループ化し、前記関連を有する事象の内、最初に発生した事象を第１事象として設定し、前記第１事象以外の事象を第２事象として設定する、判定部と、前記判定部によりグループ化された事象ごとに、前記アラートにより示される事象の対応状況を管理する管理部と、前記判定部によりグループ化された事象ごとに、前記第１事象の対応状況に関する情報と、前記第１事象に関連付けられた前記第２事象の情報とを含む第１画面を表示部に表示させる表示制御部と、を備え、前記管理部は、前記第１画面におけるオペレータの操作に基づいて前記第１事象の対応状況が対応完了に設定された場合、前記第１事象と関連付けられた前記第２事象の対応状況も自動的に対応完了に設定する、監視装置である。

【発明の効果】

【０００８】

本発明の一態様によれば、アラートの監視の負荷を軽減することが可能である。

【図面の簡単な説明】

【０００９】

【図１】実施形態に係るアラート監視システム１の構成の一例を示す図である。

【図２】実施形態に係るチケット登録装置１０の機能構成の一例を示すブロック図である。

【図３】実施形態に係るグループ情報記憶部１５に記憶されたグループ情報１５Ａのレコードの一例を示すデータ構造図である。

【図４】実施形態に係るフィルタ情報記憶部１６に記憶されたフィルタ情報１６Ａの一例を示す図である。

【図５】実施形態に係るチケット管理装置３０の機能構成の一例を示すブロック図である。

【図６】実施形態に係るアラート監視システム１のチケット登録処理の流れの一例を示すフローチャートである。

【図７】実施形態に係るアラートメールＭのメール本文に対する編集処理およびハッシュ化処理の一例を説明するための図である。

【図８】実施形態に係るチケット管理装置３０のチケット情報記憶部３５に記憶されたチケット情報３５Ａの一例を示す図である。

【図９】実施形態に係る端末装置４０の表示部に表示されたチケット画面Ｄ１の一例を示す図である。

【図１０】実施形態に係る端末装置４０の表示部に表示されたアラートタスク管理画面Ｄ２の一例を示す図である。

【図１１】実施形態に係る端末装置４０の表示部に表示されたアラート推移グラフ画面Ｄ３の一例を示す図である。

【図１２】実施形態に係る端末装置４０の表示部に表示されたフィルタ設定画面Ｄ４の一例を示す図である。
【発明を実施するための形態】
【００１０】
以下、図面を参照し、本発明の監視装置、監視方法、およびプログラムの実施形態について説明する。本発明の監視装置は、複数の監視システムにより出力されるアラートをグループ化し、グループごとにアラートを監視する。本実施形態において、アラートとは、監視対象における何らかの異常、故障等（以下、単に「異常」と呼ぶ）を通知するものである。監視対象がサーバ等のハードウェア機器である場合、アラートはこのハードウェア機器の異常を通知する。ハードウェア機器の異常には、例えば、ハードディスクの容量不足、アクセス集中による処理負荷の上昇等が含まれる。監視対象がソフトウェアである場合、アラートはこのソフトウェアの処理の異常を通知する。ソフトウェアの処理の異常には、例えば、所定のバッチ処理の失敗等が含まれる。
【００１１】
また、アラートは、例えば、監視対象を監視する複数の監視システムにより自動的に送信されるアラートメール、所定のＡＰＩ（Application Programming Interface）等のインターフェースを介して監視対象に対して所定の処理を行うことにより出力されるアラートログ等を含む。アラートメールは、複数の監視システムにより出力されるアラートメールを集約的に監視する集約型監視システムから出力されるメールであってもよい。以下においては、監視対象がサーバ等のハードウェア機器であり、アラートがアラートメールにより通知される場合を例に挙げて説明する。
【００１２】
図１は、アラート監視システム１の構成の一例を示す図である。アラート監視システム１は、例えば、チケット登録装置１０と、サーバ情報データベース２０と、チケット管理装置３０とを備える。チケット登録装置１０は、監視対象Ｔであるサーバを監視する監視システムにより出力されるアラートメールＭに基づいて、監視対象Ｔに関するアラートをチケットとして起票してチケット管理装置３０に登録する処理を行う。チケットとは、アラートを可視化して管理する単位を示す。例えば、１通のアラートメールＭに対して、１つのチケットが起票され、以後このチケット単位でアラートが管理される。
【００１３】
チケット管理装置３０において管理されるチケット情報は、端末装置４０を用いて参照等することができる。監視対象Ｔと、チケット登録装置１０と、サーバ情報データベース２０と、チケット管理装置３０と、端末装置４０とは、ネットワークＮＷによって互いに接続されており、このネットワークＮＷを介して互いに通信する。ネットワークＮＷは、例えば、ＷＡＮ（Wide Area Network）やＬＡＮ（Local Area Network）、インターネット、専用回線、無線基地局、プロバイダ等を含む。
【００１４】
［監視対象］
監視対象Ｔは、例えば、複数の監視対象サーバを含む。監視対象サーバは、例えば、所定の機能を実現するサーバ、各種データを記憶するデータベース等を含む。これらの複数のサーバには、負荷分散等を目的として、所定の処理を分散して実行するように構成されたサーバ群（例えば、ラック構成とされたサーバ群）が含まれる。例えば、第１サーバ群Ｇ１は、ウェブサービスを実現するウェブサーバ群であって、監視対象サーバ１、監視対象サーバ２、および監視対象サーバ３を含む。第２サーバ群Ｇ２は、例えば、データを記憶するデータベース群であって、監視対象サーバ４、監視対象サーバ５、および監視対象サーバ６を含む。
【００１５】
同一のグループに属するサーバに関して出力されるアラートメールは、そのアラートの内容が共通する場合がある。例えば、監視対象サーバ１に関して高負荷である旨のアラートメールが通知された場合、監視対象サーバ２に関しても同様な内容のアラートメールが

通知される場合がある。本アラート監視システム１は、これらのアラートの内容が共通し、同種とみなすことが可能なアラートをグループ化して一括管理する。

【００１６】

［チケット登録装置］

図２は、チケット登録装置１０の機能構成の一例を示すブロック図である。チケット登録装置１０は、例えば、通信部１１と、グループ判定部１２（判定部）と、フィルタ部１３と、登録部１４（管理部）と、グループ情報記憶部１５と、フィルタ情報記憶部１６とを備える。通信部１１は、ネットワークＮＷを介して、監視対象Ｔを監視する監視システムにより出力されるアラートメールＭを受信する。また、通信部１１は、ネットワークＮＷを介して、他装置と通信する。通信部１１は、例えば、ＮＩＣ（Network Interface Card）等の通信インターフェースを含む。

【００１７】

グループ判定部１２は、グループ情報記憶部１５に記憶されたグループ情報１５Ａに基づいて、アラートメールＭにより通知されるアラートの種類を判定してグループ化する。すなわち、グループ判定部１２は、複数の監視対象に関するアラートにより示される事象間の関連の有無を判定し、関連を有する事象をグループ化する。すなわち、グループ判定部１２は、アラートメールＭに含まれる情報の中から、アラートに係る事象（障害、異常等）が発生した対象であるサーバを個別に特定するための情報を除去し、グループ化するためのもう１段上位の情報（障害内容）を抽出し、この抽出した情報を用いてグループ化を行う。換言すると、グループ判定部１２は、アラートメールＭに含まれる情報の中からサーバを個別に特定するための特徴的な情報を抽出するのではなく、グループ化されるサーバ群に関して共通する特徴を抽出する処理を行う。例えば、グループ判定部１２は、アラートメールＭのメール本文に対して、予め設定されたルールに基づく編集処理を行い、編集後の文字列をハッシュ化することにより、異常が発生したサーバと異常の種類との組み合わせを識別するハッシュ値を算出する。グループ判定部１２は、算出したハッシュ値に基づいて、アラートのグループ化を行う。アラートのグループ化処理の詳細については後述する。

【００１８】

フィルタ部１３は、フィルタ情報記憶部１６に記憶されたフィルタ情報１６Ａに基づいて、アラートメールＭの対象であるサービスを特定し、アラートメールＭにより通知されるアラートに対して何らかの処理等の対応が必要であるか否かを判定することで、対応要否のフィルタリングを行う。すなわち、フィルタ部１３は、アラートにより示される事象に対する対応要否を判定し、対応が不要な事象をフィルタリングする。

【００１９】

登録部１４は、監視対象Ｔに関するアラートをチケットとして起票してチケット管理装置３０に登録する。登録部１４は、グループ判定部１２により判定されたグループの情報と、フィルタ部１３により判定された対応要否の情報と、サーバ情報データベース２０から取得されたサーバの情報とを、アラートに関連付けしたチケットを起票してチケット管理装置３０に登録する。すなわち、登録部１４は、グループ判定部１２によりグループ化された事象ごとに、フィルタ部１３により対応が必要と判定された事象を管理する。

【００２０】

グループ情報記憶部１５は、アラートメールＭにより通知されるアラートの種類の判定に用いられるグループ情報１５Ａを記憶する。グループ情報記憶部１５は、例えば、ＫＶＳ（キーバリューストア）と称されるデータの管理手法を採用したデータベースである。図３は、グループ情報記憶部１５に記憶されたグループ情報１５Ａのレコードの一例を示すデータ構造図である。このレコードは、１つの親キーａに対して、複数の子キー（例えば、ｃ１からｃ４）が設定され、この親キーと子キーの各々とのペアに対してバリュー（例えば、ｂ１からｂ４）が設定可能なデータ構成を有する。親キーａとしては、例えば、グループ判定部１２によりハッシュ化されたメール本文のハッシュ値が設定される。子キーｃ１からｃ４としては、例えば、アラートメールＭのメールヘッダに含まれるメッセー

ジＩＤが設定される。バリューｂ１からｂ４としては、例えば、メール本文に含まれるアラートの発生日時が設定される。

【００２１】

フィルタ情報記憶部１６は、アラートに対して何らかの処理等の対応が必要であるか否かの判定に用いられるフィルタ情報１６Ａを記憶する。図４は、フィルタ情報記憶部１６に記憶されたフィルタ情報１６Ａの一例を示すデータ構造図である。フィルタ情報１６Ａは、例えば、ホスト名と、サービス名と、アラート内容と、対応要否１と、対応要否２とを含む。対応要否１は、恒久的な判定基準であり、対応要否２は、暫定的な判定基準である。対応要否２は、通常は設定されないが、例えば、メンテナンス等によりアラートの発生が予め想定される場合等に、オペレータによって暫定的に設定される。対応要否１と、対応要否２との両方に設定がある場合には、対応要否２に設定された基準が優先される。

【００２２】

グループ判定部１２、フィルタ部１３、および登録部１４は、例えば、ＣＰＵ（Central Processing Unit）等のハードウェアプロセッサがプログラム（ソフトウェア）を実行することにより実現される。チケット登録装置１０は、各機能部を実現するための複数のプロセッサを備えてもよい。また、これらの各機能部のうち一部または全部は、ＬＳＩ（Large Scale Integration）やＡＳＩＣ（Application Specific Integrated Circuit）、ＦＰＧＡ（Field-Programmable Gate Array）、ＧＰＵ（Graphics Processing Unit）等のハードウェア（回路部；circuitryを含む）によって実現されてもよいし、ソフトウェアとハードウェアの協働によって実現されてもよい。

【００２３】

グループ情報記憶部１５およびフィルタ情報記憶部１６は、例えば、ＲＡＭ（Random Access Memory）、ＲＯＭ（Read Only Memory）、ＨＤＤ（Hard Disk Drive）、フラッシュメモリ、またはこれらのうち複数が組み合わされたハイブリッド型記憶装置等により実現される。また、グループ情報記憶部１５およびフィルタ情報記憶部１６の一部または全部は、ＮＡＳ（Network Attached Storage）や外部のストレージサーバ等、チケット登録装置１０がアクセス可能な外部装置であってもよい。

【００２４】

［サーバ情報データベース］

サーバ情報データベース２０は、監視対象のサーバに関する各種情報を記憶する。各種情報は、例えば、サーバの設置場所の情報、サーバの使用状態に関する情報（ネットワーク情報）等を含む。また、サーバ情報データベース２０は、監視対象のサーバに関するアラート発生時における対応手順を示すマニュアルの所在情報、或いはマニュアルを記憶してもよい。

【００２５】

［チケット管理装置］

図５は、チケット管理装置３０の機能構成の一例を示すブロック図である。チケット管理装置３０は、例えば、通信部３１と、登録部３２（管理部）と、表示制御部３３と、編集部３４（管理部、受付部）と、チケット情報記憶部３５とを備える。通信部３１は、ネットワークＮＷを介して、他装置と通信する。通信部３１は、例えば、ＮＩＣ等の通信インターフェースを含む。

【００２６】

登録部３２は、チケット登録装置１０により出力されたチケットの情報をチケット情報記憶部３５に記憶する。表示制御部３３は、端末装置４０からの要求に応じて、所望のチケットの情報を端末装置４０に表示するための情報を生成し、端末装置４０に送信する。編集部３４は、端末装置４０からの要求に応じて、チケット情報記憶部３５に記憶されたチケット情報３５Ａを編集する。

【００２７】

登録部３２、表示制御部３３、および編集部３４は、例えば、ＣＰＵ等のハードウェアプロセッサがプログラム（ソフトウェア）を実行することにより実現される。チケット管

理装置３０は、各機能部を実現するための複数のプロセッサを備えてもよい。また、これらの各機能部のうち一部または全部は、ＬＳＩ、ＦＰＧＡ、ＧＰＵ等のハードウェア（回路部；circuitryを含む）によって実現されてもよいし、ソフトウェアとハードウェアの協働によって実現されてもよい。

【００２８】

チケット情報記憶部３５は、例えば、ＲＡＭ、ＲＯＭ、ＨＤＤ、フラッシュメモリ、またはこれらのうち複数が組み合わされたハイブリッド型記憶装置等により実現される。また、チケット情報記憶部３５の一部または全部は、ＮＡＳや外部のストレージサーバ等、チケット管理装置３０がアクセス可能な外部装置であってもよい。

【００２９】

［端末装置］

端末装置４０は、例えば、アラートの監視を行うオペレータによって操作される。端末装置４０には、例えば、チケット管理装置３０において管理されているチケットの情報を参照、編集するためのアプリケーションが予めインストールされていてよい。或いは、端末装置４０は、ブラウザを利用して、チケット管理装置３０において管理されているチケットの情報を参照、編集するものであってもよい。

【００３０】

端末装置４０は、例えば、デスクトップ型コンピュータ、ノート型コンピュータ、タブレット型コンピュータ、スマートフォン等の携帯電話やタブレット端末、ＰＤＡ（Personal Digital Assistant）、その他のコンピュータ装置である。尚、オペレータには、サービスごとに設けられた複数の監視システムから出力されるアラートメールを一時受けしてこれらを集約的に監視する監視センター担当者、各サービスのサービス担当者等が含まれる。

【００３１】

［チケット登録処理］

次に、図面を参照しながらアラート監視システム１のチケット登録処理について説明する。図６は、アラート監視システム１のチケット登録処理の流れの一例を示すフローチャートである。まず、チケット登録装置１０は、監視対象Ｔを監視する監視システムにより出力されるアラートメールＭを受信する（ステップＳ１０１）。

【００３２】

次に、チケット登録装置１０は、サーバ情報データベース２０から、アラートメールＭに含まれるホスト名と対応するサーバ情報を取得する（ステップＳ１０３）。次に、チケット登録装置１０は、受信したアラートメールＭのメール本文に対して、予め設定されたルールに基づく編集処理を行い、編集後のメール本文をハッシュ化する（ステップＳ１０５）。図７は、アラートメールＭのメール本文に対する編集処理およびハッシュ化処理の一例を説明するための図である。図７に示すように、チケット登録装置１０は、受信したアラートメールＭ１の中からメール本文Ｍ２を抽出する。次に、チケット登録装置１０は、メール本文Ｍ２に対して、予め定められたルールに基づく編集処理を行う。図７に示す例では、メール本文Ｍ２に含まれる文言のうち、アラートの発生元であるホスト名の末尾に存在する２桁の数字を除去し、さらに、アラート発生日時を示す数字を削除して、編集済みメール本文Ｍ３を得る。次に、チケット登録装置１０は、編集済みメール本文Ｍ３に対して、所定のハッシュ化処理を行い、ハッシュ値Ｍ４を得る。

【００３３】

上記のような編集処理およびハッシュ化処理を行うことで、単一の機能の実現のために構成された複数のサーバ（例えば、負荷分散を目的としてラック構成とされたサーバ群）においては、アラート内容が同じである場合、算出されるハッシュ値が同一となる。尚、アラートメールＭのメール本文のフォーマットは、サービスごとに（アラートメールＭを送信する監視システムごとに）異なる場合がある。このため、上記の編集処理において利用されるメール本文の編集のルールは、サービスごとに設定される。

【００３４】

次に、チケット登録装置１０は、グループ情報記憶部１５に記憶されたグループ情報１５Ａを参照し、ハッシュ値の比較を行う。例えば、チケット登録装置１０は、算出したハッシュ値と同じ値を親キー値として持ち、そのバリューがアラートメールＭ１のメール本文に含まれるアラート発生日時から所定の時間内（例えば、１５分以内、３０分以内等）であるレコードが存在するか否かを判定する（ステップＳ１０７）。すなわち、チケット登録装置１０は、アラートメールＭ１において通知されたアラートよりも前に発生したアラートであって、関連を有しており同種とみなしうるアラートを示すチケット（親チケット、第１事象）が既に存在するか否かを判定する。関連を有するアラートを示すチケットが複数存在している場合、最初に発生したアラートを示すチケットを親チケットとして設定する。ここで、親チケットの判定に「所定の時間内」という条件を設けている理由は、ハッシュ値が同一であっても、先のアラート発生から既にある程度時間が経過している場合には、同種とみなさずに、別のアラートとして管理することが適切であると考えられるためである。

【００３５】

チケット登録装置１０は、親チケットが存在すると判定した場合、アラートメールＭ１において通知されたアラートを、親チケットに関連付けされた子チケット（第２事象）として設定する（ステップＳ１０９）。一方、チケット登録装置１０は、親チケットが存在しないと判定した場合、アラートメールＭ１において通知されたアラートを親チケットとして設定する（ステップＳ１１１）。

【００３６】

次に、チケット登録装置１０は、受信したアラートメールＭ１の情報（すなわち、上記のハッシュ化処理が行われる前のアラートメールＭ１の情報）と、フィルタ情報記憶部１６に記憶されたフィルタ情報１６Ａとに基づいて、アラートメールＭの対象であるサービスを特定し、アラートメールＭにより通知されるアラートに対して何らかの対応（例えば、応急処置等）が必要であるか否かを判定することで、対応要否のフィルタリングを行う（ステップＳ１１３）。チケット登録装置１０は、例えば、アラートメールＭ１のメールヘッダに含まれる「Ｔｏアドレス」を検索キーとしてフィルタ情報記憶部１６を検索し、対応するレコードを参照することで、上記のサービスを特定、および対応要否のフィルタリングを行う。

【００３７】

例えば、図４に示されるフィルタ情報１６Ａにおいては、アラートメールＭ１のメールヘッダに含まれる「Ｔｏアドレス」が“aaa@aa.com”である場合、「サービス名」が“サービス１”であり、「アラート内容」が“ＨＩＧＨ”である場合には、「対応要否１」が“要”であることが分かる。尚、フィルタ情報１６ＡにアラートメールＭ１のメールヘッダに含まれる「Ｆｒｏｍアドレス」、アラートメールＭ１のメール本文に含まれる「ホスト名」等が記憶されている場合には、これらの情報がサービスの特定に用いられてもよい。

【００３８】

次に、チケット登録装置１０は、アラートメールＭ１に含まれるメール本文等の情報と、設定した親チケットまたは子チケットの区別情報と、特定したサービス名と、判定した対応要否の情報とを用いてチケットを起票し、チケット管理装置３０に登録する（ステップＳ１１５）。

【００３９】

図８は、チケット管理装置３０のチケット情報記憶部３５に記憶されたチケット情報３５Ａを示す図である。図８に示す例では、“グループ１”として、「ホスト名」が“hostA01”、“hostA02”、および“hostA03”である３つのチケットが登録されている。この内、“hostA01”のアラートが“親チケット”として設定され、“hostA02”および“hostA03”のアラートが“子チケット”として設定されている。以上により、本フローチャートの処理を終了する。

【００４０】

尚、チケット登録処理における処理ステップの順番は上記に例に限られず適宜変更が可能である。例えば、対応要否のフィルタリング処理（ステップＳ１１３）が、ハッシュ化処理（ステップＳ１０５）の前に行われてもよい。

【００４１】

［チケット参照および編集処理］

オペレータは、所望のチケットに関する情報を端末装置４０上で参照および編集することができる。図９は、端末装置４０の表示部に表示されたチケット画面Ｄ１の一例を示す図である。チケット画面Ｄ１においては、親チケットであるチケット番号「００００１」のチケットの対応状況に関する情報が表示されている。チケット画面Ｄ１においては、子チケットとして「チケット番号００００２」と、「チケット番号００００３」とが関連付けされて表示されている。また、「履歴」欄には、対応が正常に完了していることが登録されている。このようなチケット画面Ｄ１において、親チケットとして設定されたチケット番号「００００１」のチケットを管理することで、これと関連付けされている子チケットについてもまとめて管理することができる。例えば、オペレータの操作に基づいて、親チケットとして設定されたチケット番号「００００１」のチケットのステータスを対応完了に設定された場合、これと関連付けされている子チケットのステータスも自動的に対応完了に設定される。

【００４２】

尚、このチケット画面Ｄ１において、「子チケット」欄に設けられた「追加」リンクを押下することで、手動により子チケットを登録することもできる。また、親子関係は無いが、すなわち、互いに異なるアラートであるが、一緒に対応した方が良いことが想定される関連性のあるチケットを「関連するチケット」として手動で設定することもできる。尚、ホスト名や、アラート内容を予め関連付けしたテーブル等を定義しておくことで、関連するチケットが自動的に表示されるようにしてもよい。尚、チケット画面Ｄ１において、子チケットの表示は省略してもよい。

【００４３】

また、図１０は、端末装置４０の表示部に表示されたアラートタスク管理画面Ｄ２の一例を示す図である。アラートタスク管理画面Ｄ２においては、「サービス１」に関連付けされたチケット（親チケット、子チケット）が一覧表示されている。オペレータ（例えば、サービス担当者）は、自身が管理するサービスに関連付けされたチケットを一括して管理することができるため、個別にチケットを管理する手間を省くことができる。

【００４４】

［アラート推移の参照処理］

図１１は、端末装置４０の表示部に表示されたアラート推移グラフ画面Ｄ３の一例を示す図である。オペレータは、サービスの設定、或いは、アラートメールＭの件名および／または本文に対してキーワード検索をかけることで、所望のアラートに関して「要対応」、「要確認」、および「対応不要」として処理された件数を示すグラフを参照することができる。

【００４５】

［フィルタ設定］

図１２は、端末装置４０の表示部に表示されたフィルタ設定画面Ｄ４の一例を示す図である。オペレータは、このフィルタ設定画面Ｄ４において、アラートメールごとのフィルタ条件の登録を行うことができる。尚、このフィルタ設定画面Ｄ４において設定されたフィルタ条件は、図４に示すフィルタ情報１６Ａに設定される。

【００４６】

上記の実施形態に係るアラート監視システム１によれば、アラートの監視の負荷を軽減することが可能である。チケット間に親子関係を設定することで、関連するアラートや、一緒に対応したアラートの確認が容易となる。また、オペレータは、チケット画面Ｄ１を参照することで、アラートの発生元のサービスの種別、アラートの未対応・対応中等のステータスを容易に確認することが可能である。また、アラートの対応漏れを常時確認して

いた人的コストを削減することが可能である。また、フィルタ設定を可能とすることで、オペレータは、無視してよいアラートを覚える必要がなくなり、担当変更が生じた場合にも柔軟に対応することが可能である。

【００４７】

尚、上記の実施形態においては、チケット登録装置１０と、サーバ情報データベース２０と、チケット管理装置３０とが別の装置として構成される例を説明したが、これらの一部または全部が、１つの装置として構成されてもよい。

【００４８】

以上、本発明を実施するための形態について実施形態を用いて説明したが、本発明はこうした実施形態に何等限定されるものではなく、本発明の要旨を逸脱しない範囲内において種々の変形及び置換を加えることができる。

【符号の説明】

【００４９】

１‥アラート監視システム、１０‥チケット登録装置、１１‥通信部、１２‥グループ判定部、１３‥フィルタ部、１４‥登録部、１５‥グループ情報記憶部、１６‥フィルタ情報記憶部、２０‥サーバ情報データベース、３０‥チケット管理装置、３１‥通信部、３２‥登録部、３３‥表示制御部、３４‥編集部、３５‥チケット情報記憶部、ＮＷ‥ネットワーク

【図１】

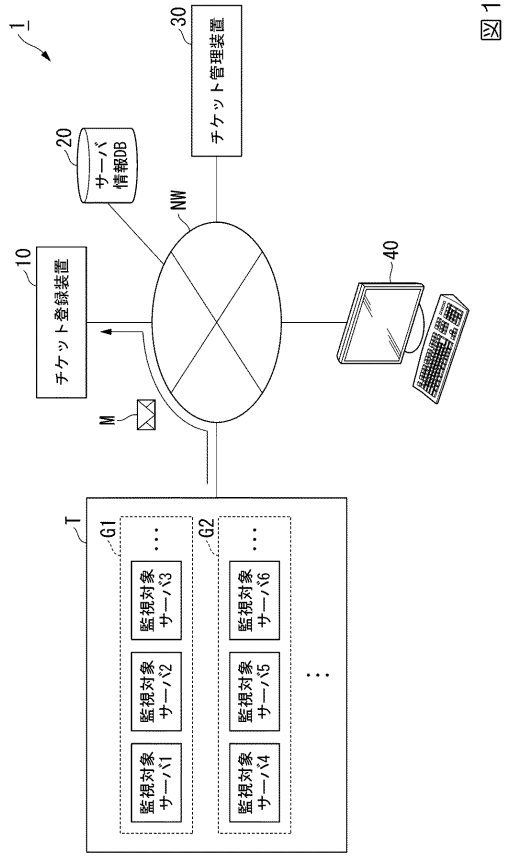

図１

【図２】

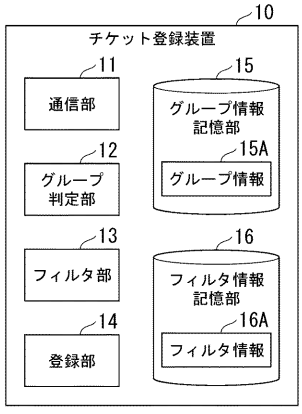

図２

【図３】

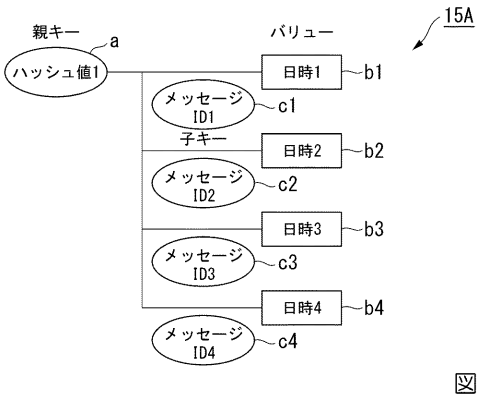

図３

【図４】

16A

Toアドレス	サービス名	アラート内容	対応要否1	対応要否2
aaa@aa.com	サービス1	HIGH	要	-
bbb@bb.com	サービス2	HIGH	要	-
ccc@cc.com	サービス3	HIGH	不要	-
ddd@dd.com	サービス4	DOWN	要	不要

⋮

図４

【図５】

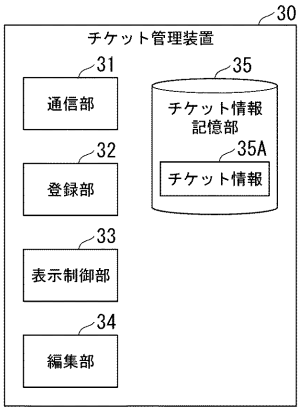

図５

【図６】

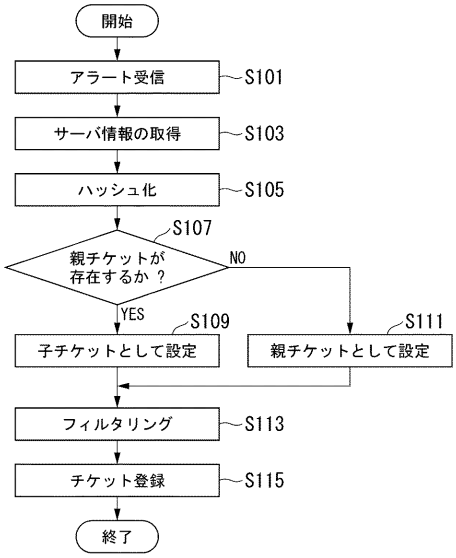

図６

【図７】

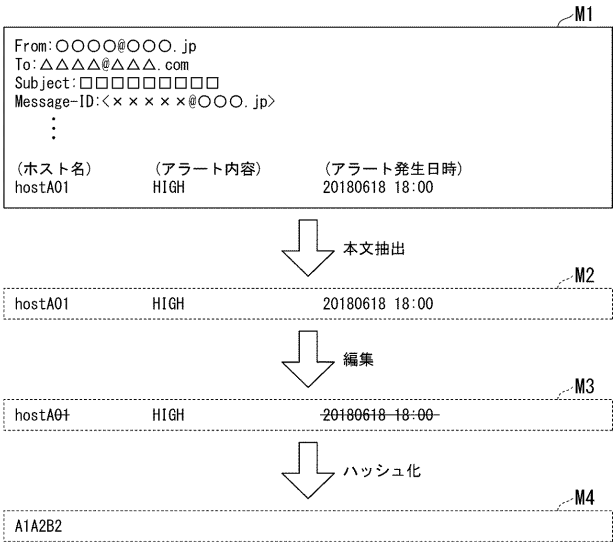

図７

【図８】

35A

グループ	チケット番号	ホスト名	親/子	サービス名	対応要否	メール本文	担当者	ステータス
グループ1	00001	hostA01	親	サービス1	要	＊＊＊	-	対応中
	00002	hostA02	子	サービス1	要	＊＊＊	-	対応中
	00003	hostA03	子	サービス1	要	＊＊＊	-	対応中
グループ2	00004	hostB25	親	サービス4	不要	＊＊＊	-	-

⋮

図８

【図９】

D1

チケット番号:00001
担当者:A

説明

[宛先]
XXXXXX@XXX.co.jp

[メール本文]
hostA01　　HIGH　　20180618 18:00

子チケット　　追加
チケット番号:00002
チケット番号:00003

関連するチケット　　追加

履歴
Aが20180618 18:05に更新
・ステータスを新規から一時対応中に変更
・一時担当をAにセット

Aが20180618 18:10に更新

□対応
手順書に従い、以下作業を実施しました。
・・・
□結果
正常完了

図９

【図１０】

D2

サービス名:サービス1

オペセン対応完了

チケット番号	作成日	サービス名	ステータス	一次対応者	二次対応者	題名
00001	20180618 18:00	サービス1	サービス担当者対応中	A		＊＊＊
00002	20180618 18:05	サービス1	サービス担当者対応中	A		＊＊＊
00003	20180618 18:08	サービス1	サービス担当者対応中	A		＊＊＊

図１０

【図１１】

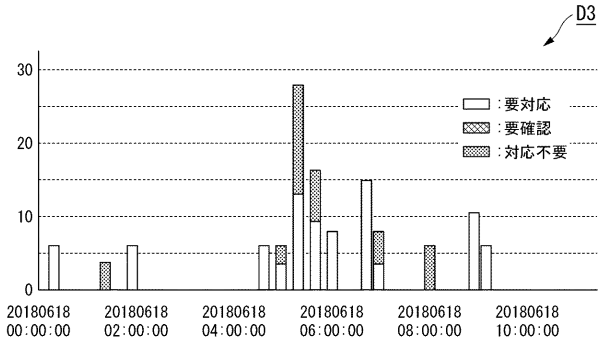

図１１

【図１２】

D4

フィルタ設定

優先度	仕分区分	件名	本文	補足	対象日	適用期間 From	適用期間 To
1	対応不要	＊＊＊	HIGH	メンテナンス	全期間	20180701 00:00	20180703 00:00
2	対応不要	＊＊＊	HIGH		全期間	20180701 00:00	20180731 00:00
3	対応不要	＊＊＊			全期間	20180705 07:00	20180705 12:00

優先度	仕分区分	件名	本文	補足	対象日	適用期間 From	適用期間 To
	対応不要 暫定対応		閾値 80%	メンテナンス	営業日	20180715 00:00	20180715 03:00

登録

図１２

フロントページの続き

(72)発明者　西村　舞
東京都千代田区紀尾井町１番３号　ヤフー株式会社内
(72)発明者　小野寺　朋崇
東京都千代田区紀尾井町１番３号　ヤフー株式会社内

Ｆターム(参考) 5B042 GA12 JJ03 KK13 MA08 MA11 MC15