

(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2014年3月6日(06.03.2014)



(10) 国際公開番号

WO 2014/033894 A1

- (51) 国際特許分類:
G06F 11/34 (2006.01) G06F 11/30 (2006.01)
- (21) 国際出願番号: PCT/JP2012/072097
- (22) 国際出願日: 2012年8月31日(31.08.2012)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (71) 出願人(米国を除く全ての指定国について): 株式会社日立製作所(HITACHI, LTD.) [JP/JP]; 〒1008280 東京都千代田区丸の内一丁目6番6号 Tokyo (JP).
- (72) 発明者; および
- (75) 発明者/出願人(米国についてのみ): 和田 清美(WADA, Kiyomi) [JP/JP]; 〒2440817 神奈川県横浜市戸塚区吉田町2-9-2番地 株式会社日立製作所横浜研究所内 Kanagawa (JP). 増田 峰義(MASUDA, Mineyoshi) [JP/JP]; 〒2440817 神奈川県横浜市戸塚区吉田町2-9-2番地 株式会社日立製作所横浜研究所内 Kanagawa (JP). 渡邊 健太郎(WATANABE, Kentaro) [JP/JP]; 〒2440817 神奈川県横浜市戸塚区吉田町2-9-2番地 株式会社日立製作所横浜研究所内 Kanagawa (JP).

- (74) 代理人: 井上 学, 外(INOUE, Manabu et al.); 〒1008220 東京都千代田区丸の内一丁目6番1号 株式会社日立製作所内 Tokyo (JP).
- (81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.
- (84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:

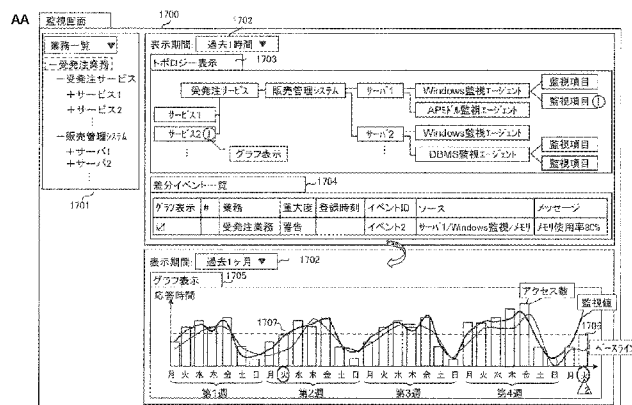
— 国際調査報告(条約第21条(3))

(54) Title: METHOD FOR MONITORING SERVICE PERFORMANCE

(54) 発明の名称: サービス性能監視方法

[図17]

【図17】



AA Monitoring screen

(57) Abstract: According to the present invention, a monitoring system, which monitors a service implementation platform that provides a service to a client computer over a network, manages a baseline for a component monitoring value for each service load provided by the platform, and makes appropriate use of the baseline in accordance with the current service load. When the monitoring system detects an abnormal service monitoring value or a component monitoring value via the baseline, the monitoring system compares an event that occurred a prescribed time prior to most recently and an event within the baseline time slot, and identifies a difference event (that is, the most recent event that is not normal).

(57) 要約:

[続葉有]

WO 2014/033894 A1



ネットワークを通じてクライアント計算機にサービスを提供するサービス実行基盤を監視対象とする監視システムは、同基盤が提供するサービスの負荷毎にコンポーネントの監視値のベースラインを管理し、現在のサービス負荷に応じてベースラインを使い分ける。また、監視システムはベースラインでサービス監視値又はコンポーネント監視値の異常を検知した場合は、直近から所定時間分前までのイベントと、ベースラインの時間帯内のイベントとを比較して、差分イベント（つまり普通でない直近のイベント）を特定する。

明 細 書

発明の名称： サービス性能監視方法

技術分野

[0001] 実施例は、情報システムを課監視する技術に関する。

背景技術

[0002] 従来、システム監視では、監視対象サーバおよび当該サーバで監視可能な監視項目に対して、閾値を設定して、各監視項目ごとに閾値監視をすることで、異常検知を行っていた。しかし、各監視項目に対して適切な閾値を設定することは難しく、設定作業負荷も大きいため、特許文献１では、「計算機システム１の過去の負荷情報に基づいてシステムの負荷の時間的な推移を示す負荷モデルデータを作成する負荷モデルデータ作成手段１４と、負荷モデルデータに指定されたしきい値補正データを加算し、しきい値データを時系列に算出するしきい値データ作成手段１６と、システム１の現在の負荷情報とそれに対応する時刻のしきい値データを比較することによりシステムの異常負荷を検出する異常負荷検出手段１７とを具備する」技術を開示している。

先行技術文献

特許文献

[0003] 特許文献１：特開２００１－１４２７４６号公報

発明の概要

発明が解決しようとする課題

[0004] 特許文献１に開示の技術では、ネットワークを通じてクライアント計算機にサービスを提供するシステムを監視対象とすることが難しい。その困難さはたとえば以下の（１）又は（２）である。

[0005] （１）ネットワークサービスを提供するシステム（サービス実行基盤）のコンポーネントを監視する場合、端末からのリクエスト内容（例えば、リクエストタイプや、単位時間当たりのリクエスト数）によって監視値は変化し

得るが、特許文献 1 ではそういったリクエスト内容を加味して過去の監視値をベースラインとして管理していないため、誤った異常検知が多発する。

[0006] (2) サービス実行基盤で異常を検知した場合、迅速に当該システムで発生するイベントの分析をすることができない。

課題を解決するための手段

[0007] 以上の課題、特に上記 (1) を解決するため、サービス実行基盤を監視する監視システムは、同基盤が提供するサービスの負荷毎にコンポーネントの監視値のベースラインを管理し、現在のサービス負荷に応じてベースラインを使い分ける。また、上記 (2) を解決するため、監視システムはベースラインでサービス監視値又はコンポーネント監視値の異常を検知した場合は、直近から所定時間分前までのイベントと、ベースラインの時間帯内のイベントとを比較して、差分イベント（つまり普通でない直近のイベント）を特定する。

発明の効果

[0008] 本発明によって、ネットワークサービスを提供するサービス実行基盤を効果的に監視することができる。

図面の簡単な説明

[0009] [図1]実施例 1 の情報システムを示す図である。

[図2]実施例 1 の計算機のハードウェア構成を示す図である。

[図3]実施例 1 のサービス監視サーバの構成を示す図である。

[図4]実施例 1 のストリームデータ処理システムを用いたサービス監視マネージャの性能解析処理フローを示す図である。

[図5A]実施例 1 の構成情報の例である。

[図5B]実施例 1 のシステム実行基盤の一例である Web システムの構成例である。

[図6]実施例 1 のシステム実行基盤のサービスに関する、サービス監視情報ストリームと業務情報付きサービス監視情報ストリームの内容を示す図である。

[図7]実施例1のシステム実行基盤のコンポーネントに関する、システム監視情報ストリームと業務情報付きシステム監視情報ストリームの内容を示す図である。

[図8]実施例1のシステム実行基盤に関する、イベント監視情報ストリームと業務情報付きイベント情報ストリームの内容を示す図である。

[図9]実施例1の業務情報付きイベント情報ストリームの格納先の、イベント情報テーブル、差分イベント情報テーブル、及び類似イベント情報テーブルを示す図である。

[図10]実施例1の業務情報付きサービス性能情報ストリームの格納先の、サービス性能情報テーブルを示す図である。

[図11]実施例1の業務情報付きシステム性能情報ストリームの格納先の、システム性能情報テーブルを示す図である。

[図12]実施例1の業務情報付きサービスグループベースライン情報ストリームの格納先の、サービスグループ性能要約情報テーブルを示す図である。

[図13]実施例1の業務情報付きシステムベースライン情報ストリームの格納先の、システム性能要約情報テーブルを示す図である。

[図14]実施例1のサービスカタログテーブルと、サービスカタログに基づくシステム稼働情報テーブルを示す図である。

[図15]実施例1の性能解析処理部のフロー図である。

[図16]実施例1の類似事象検出処理のフロー図である。

[図17]実施例1の監視画面を示す図である。

[図18]実施例1の監視画面を示す図である。

[図19]実施例2の情報システムを示す図である。

[図20]実施例2のストリームデータ処理システムを用いたサービス監視マネージャの性能解析処理フローを示す図である。

[図21]実施例2のインシデントを取り扱うための情報を示した図である。

[図22]実施例2の類似事象検出処理のフロー図である。

[図23]実施例2のインシデント検索処理のフロー図である。

[図24]実施例2の監視画面を示す図である。

発明を実施するための形態

- [0010] 以下に実施例の内容を説明する。なお、以後の説明では以下の用語を用いるがその意味は少なくとも以下である。
- [0011] ストリーム：イベントや測定値等、時間によって変化し得る情報の時間推移を表した、情報の流れである。
- [0012] ベースライン：異常を判断する際の元となる過去の監視値又は監視値を統計処理した値である。
- [0013] なお、以後の説明では「aaaテーブル」、「aaaリスト」、「aaaDB」、「aaaキュー」等の表現にて本発明の情報を説明するが、これら情報は必ずしもテーブル、リスト、DB、キュー、等のデータ構造以外で表現されていてもよい。そのため、データ構造に依存しないことを示すために「aaaテーブル」、「aaaリスト」、「aaaDB」、「aaaキュー」等について「aaa情報」と呼ぶことがある。
- [0014] さらに、各情報の内容を説明する際に、「識別情報」、「識別子」、「名」、「名前」、「ID」という表現を用いるが、これらについてはお互いに置換が可能である。
- [0015] 以後の説明では「プログラム」を主語として説明を行う場合があるが、プログラムはプロセッサによって実行されることで定められた処理をメモリ及び通信ポート（通信制御デバイス）を用いながら行うため、プロセッサを主語とした説明としてもよい。また、プログラムを主語として開示された処理は管理サーバ等の計算機、情報処理装置が行う処理としてもよい。また、プログラムの一部または全ては専用ハードウェアによって実現されてもよい。
- [0016] また、各種プログラムはプログラム配布サーバや、計算機が読み取り可能な記憶メディアによって各計算機にインストールされてもよい。この場合、プログラム配布サーバはCPUと記憶資源を含み、記憶資源はさらに配布プログラムと配布対象であるプログラムを記憶している。そして、配布プログラムをCPUが実行することで、プログラム配布サーバのCPUは配布対象

のプログラムを他の計算機に配布する。

実施例 1

- [0017] 図1は、監視システムを含む情報システムの構成図である。監視対象は、サービス実行基盤のWebシステム101と、エンドユーザが各端末102からWebブラウザ103を用いてネットワーク104経由で利用するサービスである。監視システムは複数のWebシステムとその上で利用可能なサービスを監視する。なお、本実施例ではサービスの一例としてWebを例示するが、その他ファイル共有サービスや、その他のネットワークサービスがサービスに含まれる。
- [0018] Webシステム101は、サーバ（プロセッサ、記憶資源、ネットワーク等から構成される）、OS、ミドルウェア等の物理的又は論理的なコンポーネントから構成されるサービス実行基盤である。そしてWebシステム101を監視する場合、たとえば監視対象サーバ内に常駐してOSやミドルウェアの稼働性能を監視するOS監視エージェント105やミドルウェア監視エージェント106が監視する。あるいは、システムリモート監視サーバ107が、システムを構成するサーバのOSやミドルウェアの稼働性能をリモート監視するOSリモート監視108やミドルウェアリモート監視109が監視する。OS監視エージェント105、ミドルウェア監視エージェント106、OSリモート監視108、ミドルウェアリモート監視109は、それぞれが監視対象としているコンポーネントの所定の監視項目についての監視値を、サービス監視サーバ113に送信する。
- [0019] Webアクセスで利用するサービス監視は、ネットワークスイッチ110のミラーポートからWebシステム101の送受信パケットをミラーリングして、トラフィック監視サーバ111に送る。トラフィック監視サーバ111に搭載されたトラフィック監視エージェント112がHttpパケットを解析して、応答時間を算出する。トラフィック監視サーバ111は、監視結果のHttpパケットの概要と応答時間を、サービス監視サーバ113に送信する。ここで、トラフィック監視サーバ111が複数あり、それぞれ接続

先スイッチからパケットを収集して解析してもよい。また、トラフィック監視サーバ 111 に限らず、ネットワークを流れるパケットを収集して、H t t p パケットを解析して、応答時間を算出して、H t t p パケット情報と応答時間を出力する機能を有するものであればよい。なおサービス監視の方法はこれ以外の方法、例えば、サービス実行基盤のW e bサーバに応答時間を算出可能なプログラムを追加するといった方法を採用してもよい。

[0020] イベント監視サーバ 115 内のイベント監視マネージャ 116 は、監視対象であるW e bシステム 101 や、各種監視サーバ 107 や 111 から通知される全てのイベント情報を取得する。なお、サービス実行基盤で発生する（別な言い方をするとイベント監視サーバが検知（受信も含む）する）イベントの種別としては、コンポーネントの障害や警告、コンポーネントの性能などの監視値が所定の基準を超えた場合、サービス実行基盤内で何らかの処理が始まった場合（例えばウィルススキャンやガーベージコレクション、デフラグ等）、とったものが例として考えられるが他の例でもかまわない。

[0021] サービス監視サーバ 113 に搭載されたサービス監視マネージャ 114 は、コンポーネント監視値をベースラインと比較し、異常判定を行い、異常通知をイベント監視サーバ 115 内イベント監視マネージャ 116 に通知する。また、H t t p パケット概要と応答時間に基づいて、監視対象サービス毎に応答時間とベースラインとを比較し、異常判定を行い、異常通知イベントをイベント監視サーバ 115 内イベント監視マネージャ 116 に通知する。

[0022] ここで、コンポーネント監視値またはサービス性能が異常の場合は、当該サービスと関連システムに関するイベントのうち、ベースラインに採用した正常時間帯と異常時間帯のイベントを比較し、異常時に出現する差分イベントまたはイベントの組み合わせを検出する。そして、当該差分イベントと類似イベントまたはイベントの組み合わせが、過去のイベントの中に含まれているかどうかを検索する。

[0023] さらに、応答時間を平準化するための数値計算を行い、監視結果に基づいてベースラインを設定する。

[0024] サービス監視の結果は、端末 117 の Web ブラウザ 118 を用いて、リモートから見ることができる。もちろん、サービス監視の結果を表示する端末 117 は、サービス提供を受ける端末 102 と同じであってもよく、別であってもよい。

[0025] なお、本実施例におけるサービス実行基盤を監視する監視システムはトラフィック監視サーバ 111、サービス監視サーバ 113、イベント監視サーバ 115 の 3 つのサーバより構成されているが、最低 1 つのサーバで以後に示すトラフィック監視とサービス監視が処理できればよい。さらに、請求項において表示や入力について触れているのであれば監視システムには上記趣旨に沿った端末 117 が含まれてもよい。反対に、サービス監視サーバ等トラフィック監視やサービス監視処理を行うサーバで表示や入力を行うのであれば、監視システムには端末を含まなくても良い。また、監視処理の高信頼化や並列化、分散化といった目的で複数のサーバで監視処理を分担するのであればこれら処理を担うサーバをまとめた存在が監視システムである。

[0026] なお、以後はコンポーネントの監視値は性能値を例として説明を行うが、その他の監視値（コンポーネントへのアクセスリトライ数、パケットロス率、コンテキストスイッチ数、コンポーネントへのリクエストキュー長やキュー溢れ回数等）にも適用可能である。

[0027] 次に実施例の端末 102、Web システム 101 に含まれるサーバ、トラフィック監視サーバ 111、システムリモート監視サーバ 107、イベント監視サーバ 115、端末 117 以外の計算機のハードウェア構成を図 2 に示す。図 2 にあるようにこれら計算機は、プロセッサ 201、メモリ 202、記憶デバイス 203、通信インターフェース 204 を含み、これらは互いに接続される。なお、計算機は必要であれば入力デバイス 206、出力デバイス 207 を含むことがある。なお、各サーバ、端末をまとめて図 2 で説明したが、これら計算機が必ずしも同一ハードウェアでなくてもよい。そして、図 1 の各計算機の隅丸の四角で表されたプログラムは、メモリ 202 又は記憶デバイス 203（以後、まとめて記憶資源と呼ぶ）に格納され、プロセッ

サ 2 0 1 によって実行される。

[0028] 図 3 は、図 2 で示した計算機の記憶資源に格納される情報、プログラムを表した図である。なお、図ではサービス監視マネージャプログラム 1 1 4（以後は単にサービス監視マネージャと呼ぶ）はメモリ 2 0 2、そのほかの情報は記憶デバイス 2 0 3 に格納されているが、記憶資源に格納されるのであれば各プログラム及び情報はどちらに記憶されても良い。サービス監視マネージャ 1 1 4 は画面表示処理部 3 0 1 と性能解析処理部 3 0 3 を含む。記憶デバイス 2 0 3 には、構成情報 3 0 4、性能情報 3 0 5、ベースライン情報 3 0 6、イベント情報 3 0 7、システム稼働情報 3 0 8 が格納される。端末 1 1 7 から Web ブラウザ 1 1 8 経由でやりとりする入出力情報、Web システム 1 0 1 やシステムリモート監視サーバ 1 0 7 から受信するコンポーネント監視値情報、トラフィック監視サーバ 1 1 1 から受信する H t t p パケットの情報、イベント監視サーバ 1 1 5 から受信するイベント情報は、通信インターフェース 2 0 4 により入出力される。なお、図 2 及び図 3 では入力デバイスと出力デバイスは別なデバイスとして図されているが、スマートフォンやタブレットコンピュータのような計算機がサーバや端末として用いることも想定されることから、入力デバイスと出力デバイスは 1 つのデバイスが兼ねても良い。

[0029] 図 4 は、サービス監視サーバ 1 1 3 内の、サービス監視マネージャ 1 1 4 の構成と処理フローの例である。サービス監視マネージャ 1 1 4 は、ストリームデータ処理システム 3 0 2 を用いた性能解析処理部 3 0 3 をもつ。クエリリポジトリ 4 0 6 には、性能解析処理部 3 0 3 の各処理内容の実行コードが格納されている。ストリームデータ処理システム内部で、ストリームデータを格納する方法、受け付けられたクエリの解析、最適化および生成されたクエリ実行形式の登録方法などについては、特開 2 0 0 6 - 3 3 8 4 3 2 号公報に開示された技術を用いればよい。ただし、ただし本発明は必ずしも特開 2 0 0 6 - 3 3 8 4 3 2 号公報で実現する必要はなく、以下に示す入力ストリームからベースライン情報 3 0 6、性能情報 3 0 5、イベント情報 3 0

7を更新又は作成できれば他の実現方式であってもよい。

- [0030] ストリームデータ処理システム302は、トラフィック監視サーバ111からサービス監視情報ストリーム401、Webシステム101やシステムリモート監視サーバ107からシステム監視情報ストリーム402、イベント監視サーバ105からイベント監視情報ストリーム403を受信する。これら入力ストリーム（監視情報ストリーム）401から403は、ストリームデータフローマネージャ404を経由して、クエリ処理エンジン405を使用して、性能解析処理を行う。性能解析処理部303は、業務識別処理410、異常判定処理411、類似事象検出処理412、ベースライン設定処理413の順で実行される。
- [0031] 業務識別処理410では、入力ストリーム（監視情報ストリーム）401から403に、構成情報304のサービスとシステムからなる業務情報を付加した業務情報付き監視情報ストリームを生成する。業務情報付きイベント情報ストリーム407は、イベント情報307に格納する。
- [0032] 異常判定処理411では、所定時間内（例えば1分間）の業務情報付きサービス性能ストリームを、サービス毎に、性能値を統計処理（平均値、最大値、最小値、分散値を算出）し、統計値を、ベースライン情報306の業務別サービスグループ毎の、ベースライン採用日時のサービス性能要約情報と比較し、ベースライン許容範囲内かどうかを判定し、判定結果を含むサービス性能情報ストリーム408を、性能情報305に格納する。また、業務情報付きシステム監視情報ストリームの性能値を、ベースライン情報306の業務別システム毎の、ベースライン採用日時の、各ホストのエージェント別監視項目のサーバ性能要約情報と比較し、ベースライン許容範囲内かどうかを判定し、判定結果を含むシステム性能情報ストリーム408を、性能情報305に格納する。ここで、サービス性能およびシステム性能に対して異常と判定された場合は、イベント監視サーバ115に通知する。
- [0033] 類似事象検出処理412は、サービス性能またはシステム稼働性能がベースライン許容範囲を超過した場合に、イベント情報307から、当該業務に

関する、異常となった時間帯のイベントと、ベースラインに採用した正常時間帯のイベントを取り出して比較し、異常時にしか現れない差分イベントを検出する。イベント情報307のうち、当該業務に関する過去のイベントに、差分イベントと類似のイベントがないかどうかを検索する。当該業務内に類似イベントがなければ、システム稼働情報308から、当該業務のシステム構成と類似のシステムを検出し、イベント情報307のうち、類似システムに関する業務のイベント情報も、検索対象とする。当該処理の結果、差分イベント情報407と類似イベント情報407を、イベント情報308に格納する。

[0034] ベースライン設定処理413は、所定時間内（例えば1時間）内の業務情報付きサービス性能ストリームを、サービスグループ毎に、性能値を統計処理（平均値、最大値、最小値、分散値を算出）し、ベースライン情報306に格納する。また、所定時間内（例えば1時間）内の業務情報付きシステム性能情報ストリームを、各ホストのエージェント別の監視項目毎に、性能値を統計処理（平均値、最大値、最小値、分散値を算出）し、ベースライン情報306に格納する。所定時間（例えば1時間）単位で、サービスグループ毎の、スループット／分の平均値と、ベースライン情報306に格納されている過去の同一時間帯のスループット／分の値が近い日時を検出して、翌時間帯の業務別ベースライン採用日時を、当該検出日の翌時間帯として、ベースライン情報306に格納する。

[0035] 図5Aは、構成情報304を示す模式図である。構成情報304は、Webシステムに含まれる業務グループを含むコンポーネントに関する情報（例えばコンポーネントの設定情報や属性情報）や、コンポーネント同士の関係（通信関係や包含関係等）を格納している。図5では構成情報304に含まれる例として構成情報502、サービスグループ情報503、システム情報504、サービス情報505を含むことを示している。

[0036] 業務情報502の内容は、業務名502a、サービスグループ名502b、システム名502cである。サービスグループ情報503の内容は、サー

ビスグループ名502b、URIパス503aである。サービス情報505の内容は、サービスグループ名502b、サービス名505a、サービス内容505b、URIパス505c、URIクエリ505dである。システム情報504の内容は、システム名502c、ホスト名504a、IPアドレス504bである。

[0037] 図5BはWebシステムの構成例を示した図である。業務グループ501は、複数の業務502から成る。業務502は、サービスグループ503とシステム504から成る。サービスグループ503は、複数のサービス505から成る。システム504は複数のホスト506から成る。ホスト506は複数のエージェントから成る。なお、1監視システム及びWebシステムで複数の業務を扱わないのであれば、業務グループは存在しなくてもよい。同様に複数のサービスを提供しないのであればサービスグループは存在しなくてもよい。

[0038] 図6は、サービス監視情報ストリーム401と、業務識別処理410の出力結果の業務情報付きサービス監視情報ストリーム605である。

[0039] サービス監視情報ストリーム401は、時刻601、リクエスト情報602、レスポンス情報603、応答時間604より成る。リクエスト情報602の内容は、送信元IPアドレス602a、メソッド602b、URIパス602c、URIクエリ602dである。レスポンス情報603の内容は、HTTPステータスコード603a、転送データ量603bである。

[0040] 業務情報付きサービス監視情報ストリームは、時刻601、業務名502a、サービスグループ名502b、サービス情報505、リクエスト情報602、レスポンス情報603、応答時間604から成る。サービス情報505の内容は、サービス名505a、サービス内容505bである。

[0041] 図7は、システム監視情報ストリーム402と、業務識別処理410の出力結果の業務情報付きシステム監視情報ストリーム706である。

[0042] システム監視情報ストリーム402は、時刻701、ホスト情報702、エージェント名703、監視項目704、性能値705である。ホスト情報

702の内容は、ホスト名702a、IPアドレス702bである。監視項目704の内容は、レコード名704a、フィールド名704bである。

[0043] 業務情報付きシステム監視情報ストリーム706は、時刻701、業務名502a、システム名502c、ホスト情報702、エージェント名703、監視項目704、性能値705から成る。

[0044] 図8は、イベント監視情報ストリーム403と、業務識別処理410の出力結果の業務情報付きサービスイベント情報ストリーム407aおよび業務情報付きシステムイベント情報ストリーム407bである。

[0045] イベント監視情報ストリーム403は、時刻801、イベント情報802、オブジェクトタイプ803、オブジェクト情報804から成る。イベント情報802の内容は、重大度802a、登録時刻802b、イベントID802c、ソース802d、メッセージ802e、アクション802fである。オブジェクトタイプ803は、イベント発行元を識別するための情報で、サービス情報、システム情報、ジョブ情報などである。

[0046] 業務情報付きサービスイベント情報ストリーム407aは、時刻801、業務名502a、サービスグループ名502b、サービス情報505、イベント情報802から成る。

[0047] 業務情報付きシステムイベント情報ストリーム407bは、時刻801、業務名502a、システム名502c、ホスト情報702、イベント情報802から成る。

[0048] 図9は、業務情報付きイベント情報ストリーム407を格納するイベント情報307内のイベント情報テーブル307a、類似事象検索処理412で差分イベントおよび類似イベントの、業務情報付きイベント監視情報ストリームを格納する、差分イベント情報テーブル307b、類似イベント情報テーブル307cのテーブル構成である。各イベント情報テーブル307a、307b、307cは、同一テーブル構成で、時刻801、業務名502a、サービスグループ名502b、サービス情報505、システム名502c、ホスト情報702、イベント情報802から成る。

[0049] 図10は、業務情報付きサービス監視情報ストリーム605に対して、異常判定処理411で統計値を求めてベースライン判定した結果の、サービス性能情報ストリーム408aを格納する、性能情報306内のサービス性能情報テーブル305aである。業務情報付きサービス性能情報ストリーム408aは、時間1001、業務名502a、サービスグループ名502b、サービス情報505、判定1002、1分あたりの応答時間の統計値1003、1分あたりのスループット累積値1004、1分あたりのエラー率累積値1005から成る。サービス性能情報テーブル305aの内容は、時間1001、業務名502a、サービスグループ名502b、サービス情報505、判定1002、1分あたりの応答時間の統計値1003、1分あたりのスループット累積値1004、1分あたりのエラー率の累積値1005である。

[0050] 図11は、業務情報付きシステム監視情報ストリーム706に対して、異常判定処理411でベースライン判定した結果の、システム性能情報ストリーム408bを格納する、性能情報306内のシステム性能情報テーブル305bである。業務情報付きシステム性能情報ストリーム408bは、時刻1101、業務名502a、システム名502c、ホスト情報702、エージェント名703、監視項目704、性能情報705、判定1102から成る。システム性能情報テーブル305bの内容は、時刻1101、業務名502a、システム名502c、ホスト情報702、エージェント名703、監視項目704、性能情報705、判定1102である。

[0051] 図12は、業務情報付きサービス性能情報ストリーム408aに対して、ベースライン設定処理413で、所定時間（例えば1時間）で、サービスグループ毎の、サービス性能の統計値を求めて、同一サービスグループ内、同一時間帯で、1分あたりのスループット平均値が最も近い日を検出し、当該検出日の翌時間帯を、翌時間帯の業務別ベースライン採用日時とする、業務情報付きサービスグループベースライン情報ストリーム409aを格納する、ベースライン情報306のサービスグループ性能要約情報テーブル306

aである。業務情報付きサービス性能ベースライン情報ストリーム409aは、時間1201、業務名502a、サービスグループ名502b、スループット（統計値）1202、エラー率（統計値）1203、応答時間（統計値）1204、ベースライン採用日時1205から成る。サービスグループ性能要約情報テーブル306aの内容は、時間1201、業務名502a、サービスグループ名502b、スループット統計値（1202）、エラー率（統計値）1203、応答時間（統計値）1204、ベースライン採用日時1205である。

[0052] 図13は、業務情報付きシステム性能情報ストリーム408bに対して、ベースライン設定処理413で、所定時間（例えば1時間）で、システム内のホストのエージェントの監視項目に対する性能値の統計値を求めて、結果の業務情報付きシステムベースライン情報ストリーム409bを格納する、ベースライン情報306のシステム性能要約情報テーブル306bである。業務情報付きシステムベースライン情報ストリーム409bは、時間1301、業務名502a、システム名502c、ホスト情報702、エージェント名703、監視項目704、性能値（統計値）1302から成る。システム性能要約情報テーブル306bの内容は、時間1301、業務名502a、システム名502c、ホスト情報702、エージェント名703、監視項目704、性能値（統計値）1302である。

[0053] 図7の業務情報付きシステム監視情報ストリーム706の時刻701が属する時間帯の、業務名502aと一致する、図12のサービスグループ性能要約情報テーブル306aの時間1201と業務名502aの、ベースライン採用日時1205をみて、図13のシステム性能要約情報テーブル306bの性能値（統計値）を使用する。

[0054] 図14は、システム稼働情報308に含まれるサービスカタログテーブル1401と、システム稼働情報テーブル1402である。サービスカタログテーブル1401の内容は、システム種別1403、サーバスペック1404、OS種別1405、ミドルウェア種別1406、数量1407から成る

。

- [0055] システム稼働情報テーブル1402の内容は、システム名502c、システム種別1403、UP (User Program) 情報1408、累積稼働日数1409、アラート発生件数1410、障害件数1411、所定期間の平均サービス性能情報1412、所定期間の平均システム性能情報1413から成る。
- [0056] サービスカタログテーブル1401は、PaaS (Platform as a Service) 提供者が、提供サービスを登録する。
- [0057] システム稼働情報テーブル1402は、システムを構築時や更改時に、システム名502cと、サービスカタログテーブル1401から選択したシステム種別1403と、UP情報1408を登録する。また、累積稼働日数1409、アラート発生件数1410、障害件数1411は、別に管理されているインシデント管理から、定期的に登録更新される。さらに所定期間の平均サービス性能情報1412、所定期間の平均システム性能情報1413は、性能情報305から、定期的に集計処理されて登録更新される。
- [0058] システム稼働情報テーブル1402は、対象システムとシステム種別1403が同一のシステムを検索したり、類似システムのうち、稼働実績の長いあるいは近いシステムを選択するために必要である。
- [0059] 図15は、性能解析処理部303の処理の流れである。性能解析処理部303は、業務識別処理410、異常判定処理411、類似事象検出処理412、ベースライン設定処理413の順で処理する。
- [0060] 業務識別処理410は、監視情報ストリームを受信する処理1501と、監視情報ストリームに業務情報を付加する処理1502からなる。受信処理1501は監視情報ストリームの新しい情報を受信する。
- [0061] 監視情報ストリームに業務情報を付加する処理1502は、構成情報304を参照して、サービス監視情報ストリームの場合は、URIが共通のサービスグループに関連する業務を取得し、URIとクエリが共通のサービス情報を取得し、業務種別付きサービス監視情報ストリームを作成する。

- [0062] システム監視情報ストリームの場合は、ホストが含まれるシステムに関連する業務を取得し、業務情報付きシステム監視情報ストリームを作成する。
- [0063] イベント監視情報ストリームの場合は、オブジェクトタイプがサービスの場合は、オブジェクト情報に格納されているサービス情報のうちのサービスグループに関連する業務を取得し、業務種別付きイベント監視情報を作成する。オブジェクトタイプがホストの場合は、ホストが含まれるシステムに関連する業務を取得し、業務種別付きイベント監視情報を作成する。業務種別付きイベント監視情報は、イベント情報 307 に格納する。
- [0064] 異常判定処理 411 は、所定時間内に到着する業務種別付きサービス監視情報ストリームに対して、性能値の統計値（平均、最大、最小、分散）を求めて、業務種別付きサービス性能情報ストリームを作成する処理 1503 と、業務種別付きサービス性能情報の統計値が、ベースラインを超過していないかを判定し、業務種別付きサービス性能情報ストリームを性能情報 305 に登録する、または業務種別付きシステム監視情報のホスト内エージェントの監視項目に対する性能値がベースラインを超過していないかを判定し、業務種別付きシステム性能情報ストリームを性能情報 305 に登録する処理 1504 から成る。
- [0065] ベースライン許容範囲を超過するか否かの判定部 1505 の結果、ベースラインを超過する場合、類似事象検出処理 412 を実行する。類似事象検出処理 412 は、正常時と異常時のイベント情報を比較して差分イベントを検出する、イベント情報比較処理 1506 と、差分イベントと類似のイベントが過去に存在するかどうかを検索する、類似イベント検索処理 1507 から成る。
- [0066] ベースライン設定処理 413 において、まず、所定時間内の性能要約情報を作成する処理 1508 は、業務毎に、サービスグループ毎の単位時間（例えば 1 分）あたりのサービス性能（応答時間、スループットなど）の、所定時間（例えば 1 時間）内の統計値を算出して、サービス性能要約情報を作成する。また、同処理 1508 は、システム内の各ホストのエージェント毎の

監視項目の性能値の所定時間（例えば１時間）内の統計値を算出して、システム性能要約情報を作成する。同処理１５０８は、単位時間（例えば１分）おきに、性能情報の統計値（最大値、最小値、平均値）を累積していく。

次に、所定時間内のスループット統計値と近い過去の統計値を検出して翌時間帯のベースラインを決定する処理１５０９は、所定時間（例えば１時間）分の性能要約情報が累積された時点で、同一業務のサービスグループの、過去同一時間帯のスループット統計値のうち、最も近い日にちを見つけて、翌時間帯のベースライン採用日として、ベースライン情報３０６に格納する。

[0067] 図１６は、類似事象検出処理４１２の処理の流れである。類似事象検出処理４１２は、イベント情報比較処理１５０６と類似イベント検索処理１５０７から成る。

[0068] イベント情報比較処理１５０６は、業務毎に、ベースライン超過時点を含む直近の所定時間内のイベント情報を取得する処理１６０１と、ベースライン採用時間帯（正常時）のイベント情報を取得する処理１６０２と、ベースライン超過時間帯（異常時）のイベントと、ベースライン採用時間帯（正常時）のイベントで、イベントＩＤを比較し、正常時には出現しないが異常時に出現する差分イベントを検出し、差分イベントをイベント情報３０７に格納する処理１６０３から成る。

[0069] 類似イベント検索処理１５０７は、同一業務の過去のイベントから、差分イベント（組み合わせ）とイベントＩＤが一致するものを検索する処理１６０４と、差分イベントとの適合性判定部１６０５と、適合イベントが見つかった場合に類似イベント（組み合わせ）をイベント情報３０７に格納する処理１６０６と、システム稼働情報３０８を参照して、当該業務と関連するシステムと、同一のシステム構成をもつ他システムを検索する処理１６０７と、システム類似度判定部１６０８と、類似システム関連業務の過去イベントから、差分イベント（組み合わせ）とイベントＩＤが一致するものを検索する処理１６０９成る。

[0070] 図１７から図１８は、サービス監視サーバ１１３にインストールされたサ

ービス監視マネージャ 114 の画面表示処理部 301 によって実行され、端末 117 の Web ブラウザ 118 上で表示する監視画面である。

[0071] 図 17 は、業務別に、サービスと関連システム性能をベースライン監視した結果、ベースライン超過を検知し、正常時には出現しない差分イベントを検出した際の、監視画面 1700 である。監視画面 1700 は、業務一覧表示部 1701、表示期間指定部 1702、トポロジー表示部 1703、差分イベント一覧表示部 1704、グラフ表示部 1705 から構成される。

[0072] 本監視画面の使い方は、まず、統合イベント監視ツール側で、業務内サービスあるいはホストでの異常に気付くと、監視画面 1700 で、業務一覧表示部 1701 より、確認したい業務を選択する。次に、表示期間指定部 1702 で期間を指定して、トポロジー表示部 1703 により、業務を構成するサービスおよびシステム内ホストの稼働状況を確認する。また、このとき、差分イベント一覧表示部 1704 で、異常時にしか現れないイベントが表示される。そして、グラフ表示部 1705 では、表示期間指定部 1702 で指定した期間内の、トポロジー表示部 1703 で選択した異常箇所の性能傾向と、差分イベント一覧で選択したイベントの発生状況を、確認する。グラフ表示部 1705 において、ベースラインに採用するのは、直近のアクセス数が最も近い同一時間帯の日付の性能値であるため、イベント 2 が発生している日 1706 の応答時間のベースラインは、最もアクセス数が近い日 1707 の応答時間をベースラインとしている。

[0073] 図 18 は、図 17 で検出した差分イベントに対して、同一業務および、同一システム構成の他業務の過去イベントのなかから、類似イベントを検出した結果の監視画面 1800 である。監視画面 1800 は、業務一覧表示部 1801、表示期間指定部 1802、差分イベント一覧表示部 1803、類似イベント一覧表示部 1804、グラフ表示部 1805 から構成される。

[0074] 本監視画面の使い方は、図 17 で検出した異常時の差分イベントについて、差分イベント一覧表示部 1803 で、表示期間指定部 1802 で期間を指定して、差分イベントの発生状況を発生件数で確認する。ここで、差分イベ

ントが頻繁に発生しており、無視できるイベントなのか、めったに発生しない注意すべきイベントなのかを判別する。

[0075] 続いて、発生件数の少ない注意すべきイベントの場合、同一業務または類似システムからなる業務に関わる過去のイベントのなかから、類似イベントを検索し、検索結果を類似イベント一覧 1804 で表示する。

[0076] グラフ表示部 1805 で、類似イベント発生状況と性能傾向を、現時点と過去と比較し、障害発生を予測し、障害発生前に対処が可能な情報を提示する。

[0077] 以上が実施例 1 の説明である。

実施例 2

[0078] 次に実施例 2 を図を用いて説明する。

[0079] 図 19 は、実施例 2 の構成を示した図であり、実施例 1 との差異はインシデント管理サーバ 119 を追加したことである。インシデント管理サーバ 119 内には、インシデント管理 120 プログラムを記憶資源に格納し、実行する。

[0080] 図 20 は、図 4 のサービス監視サーバ 113 内の、サービス監視マネージャ 114 の構成と処理フローに、インシデント管理サーバ 119 のインシデント管理 120 と連携して、類似インシデント情報を追加する場合の構成と処理フローである。ストリームデータ処理システム 302 内の性能解析処理部 303 において、類似事象検出処理 412 は、サービス性能またはシステム稼働性能がベースライン許容範囲を超過した場合に、イベント情報 307 から、当該業務に関する、異常となった時間帯のイベントと、ベースラインに採用した正常時間帯のイベントを取り出して比較し、異常時にしか現れない差分イベントを検出する。そして、インシデント管理サーバ 119 内インシデント管理 120 のインシデント検索処理 2001 で、差分イベントが、当該業務に関する過去のイベントに基づいて登録済みのインシデント情報 2002 のなかに、類似のインシデント情報が存在するかどうかを検索する。検索の結果、類似インシデントが見つかった場合には、業務情報付きインシ

デント情報ストリーム 2003 を生成し、類似インシデント情報 2004 に格納する。

[0081] 図 21 は、図 20 のインシデント検索処理 2001 の、入力情報 2101 と出力情報 2103、インシデント情報 2002 内のインシデント情報テーブル 2101 と、類似インシデント情報 2004 内の類似インシデント情報テーブル 2104 である。

[0082] インシデント検索のための入力情報 2101 は、検索対象期間を示す開始日時 2105 と終了日時 2106、検索対象の業務名 502a、サービスグループ名 502b、システム名 502c、インシデントに関連するイベント ID 2107 からなる。

[0083] インシデント情報テーブル 2102 は、タイトル 2108、重要度 2109、インシデント ID 2110、インシデント ID への URL 2111、業務名 502a、サービスグループ名 502b、システム名 502c、発生日時 2112、インシデントに関連するイベント ID 2113 から成る。

[0084] インシデント検索結果の出力情報 2103 は、2102 のインシデント情報テーブルの各項目に対応する内容である。

[0085] 類似インシデント情報テーブル 2104 は、2103 のインシデント検索結果を格納するために、インシデント情報に対応する各項目から成る。

[0086] 図 22 は、図 16 の類似事象検出処理 412 の処理の流れに、類似障害検索処理 2201 を追加した処理フローである。類似事象検出処理 412 において、イベント情報比較処理 1506 により、差分イベントを検出し、イベント情報 307 に格納する。

[0087] 次に、類似障害検索処理 2201 で、差分イベント（組み合わせ）と類似の関連イベントに基づくインシデントが存在するかどうかを検索する。類似障害検索処理 2201 は、検索期間と業務情報と差分イベント（組み合わせ）から成るデータセットを作成する処理 2202 と、作成したデータセットを入力パラメータとして、類似インシデントを返り値とする検索コマンドを生成する処理 2203 と、生成した検索コマンドをインシデント管理に送信

し、類似インシデント情報一覧を受信する処理 2204 から成る。

[0088] 類似障害検索処理 2201 の結果、類似インシデントが見つかったか否かの判定処理 2205 を行い、類似インシデントが見つかった場合は、類似インシデント情報一覧を類似インシデント情報テーブルに格納する処理 2206 を行い、類似インシデント情報 2004 に格納する。るインシデントが見つからなかった場合は、類似イベント検索処理 1507 を実行する。

[0089] 図 23 は、インシデント管理サーバ 119 内のインシデント管理 120 での、インシデント検索処理 2001 の処理の流れである。インシデント検索処理 2001 は、検索開始日時から終了日時の期間内で、同一業務のインシデントを抽出する処理 2301 と、抽出したインシデントのうち、関連イベントが含まれるインシデントを抽出する処理 2302 と、抽出したインシデント情報から、“タイトル”、“重大度”、“インシデント ID”、“インシデント ID への URL”、“業務名”、“発生日時”、“関連イベント ID” から成るデータセットを作成する処理 2303 と、作成したデータセットを送信する処理 2304 から成る。

[0090] 図 24 は、サービス監視サーバ 113 にインストールされたサービス監視マネージャ 114 の画面表示処理部 301 によって実行され、端末 117 の Web ブラウザ 118 上で表示する監視画面である。図 24 は、図 18 の、差分イベントに対して、類似イベントを検出した結果の監視画面 1800 と異なり、類似インシデントを検出した結果の監視画面 2400 である。

[0091] 監視画面 2400 において、差分イベント一覧 2401 に対して、検索期間 2402 を指定すると、当該イベントの発生件数が表示される。

[0092] 次に、類似検索対象にチェック 2403 の付与されたイベント（組み合わせ）に関するインシデントを検索した結果が、類似インシデント一覧 2404 に表示される。

[0093] さらに、インシデント ID 2405 をクリックすると、インシデント詳細 URL 先のインシデント画面 2406 が表示される。インシデント画面 2406 内には、インシデント情報 2407 が表示され、現在発生しているイベ

ントが、障害につながるかどうかを判断することができる。さらに、インシデント画面 2406 には、回避策や解決策といったサービス実行基盤の管理者が行い、そして入力した内容が表示されるため、サービス実行基盤の管理者は、これら表示情報を参考にして、障害発生前に対処することが可能となる。

[0094] 以上、実施例 1 及び 2 の監視システムによって、例えば、不確定に変動するサービス利用と、定時に定型処理するバッチジョブなどのシステム内部処理とで、両方共に類似の利用状況の過去の性能情報であるベースラインを見つけるのは困難であったが、同一時間帯の過去のサービスのスループットのなかで、現在のスループットと近い日にちを見つけるので、定時実行内部処理を加味したシステムおよびサービスのベースラインを、短期間に精度よく見つけることができるようになった。

[0095] また、実施例 1 及び 2 の監視システムによって、ベースラインの許容範囲を超過した場合、この先放っておくと障害に至ってしまうため対処が必要なケースと、時間経過とともに自然回復するため対処が不要なケースがあるが、予兆段階で正しい判断をするための情報を提示できるようになった。

[0096] さらに、実施例 1 及び 2 の監視システムによって、サービス利用状況が近い、同一時間帯のシステム稼動性能をベースラインとすることで、外部アクセス変動(外乱)によらない、システム内部処理異常に気づくことができるようになった。従って、外部アクセスによる外的要因か、内部処理異常の内部要因かを切り分けられるようになり、原因調査に要する時間を削減でき、適切な対象方法をとることができるようになった。

[0097] なお、図 16 にあるように、ステップ 1602 にて取得するイベント情報は、採用されたベースラインの時間帯のイベント情報であるため、結果的に取得されるイベント情報もその時のサービス監視の値に適したものが選択される。これは例えばサービスリクエストが多い時と少ない時とで発生するイベントが相違する場合に好適である。しかし、図 16 の類似事象検出処理はベースラインをサービス監視の値と関連付けて管理しない場合でも適用する

ことで、サービス実行基盤で異常を検知後に迅速にイベント分析は可能である。これは図 2 2 も同様である。

[0098] なお、コンポーネントの異常検知に用いるベースラインをその時のサービス監視値に近いベースラインを 1 つ選ぶ代わりに、複数のベースラインから擬似的なベースラインを合成（例えば 2 つのベースラインの平均化等）してもよい。このような合成はサービス実行基盤のサービス負荷がわずかに増加した場合にコンポーネントの監視値が急激に変化しない場合は好適である。一方の 1 つのベースラインを選択する場合は、図 1 7 のようなベースライン表示をした場合に、表示ベースラインは事実として発生したものであることから、監視システムのユーザーは事実ベースでの分析をより深く行うことが出来る。また、1 つのベースラインを選択した場合のほうが、対応するイベント情報を選択しやすい。

[0099] なお、イベント監視サーバ 1 1 5 からストリームとして送信されてきたイベントは、イベント監視サーバ 1 1 5 が Web システム 1 0 1 からイベントの内容を示すメッセージを受信したことでイベント監視サーバ 1 1 5 が検知するが考えられる。また、他のイベント検知の方法としては、イベント監視サーバ 1 1 5 がサービス実行基盤に状態取得要求を送信し、そこで受信した状態によってイベント検知を行う方法も考えられる。しかし、イベント検知は他の方法で実現してもよい。

符号の説明

[0100] 1 0 1 . . . Web システム、1 0 2 . . . 端末、1 1 1 . . . トラフィック監視サーバ、1 1 3 サービス監視サーバ

請求の範囲

[請求項1]

複数のコンポーネントを含み、前記コンポーネントを用いて所定のサービスを提供するサービス実行基盤と通信可能な通信インターフェースと、

記憶資源と、

前記サービス実行基盤から、前記所定のサービスの監視値であるサービス監視ストリームと、前記コンポーネントの監視値であるコンポーネント監視ストリームと、を受信処理するプロセッサと、

を有する監視システムであって、

前記プロセッサは、

(A) 過去の所定の時間帯のコンポーネント監視ストリームに基づいてコンポーネントベースラインを作成し、

(B) 過去の所定の時間帯のサービス測定ストリームの統計値を計算し、

(C) 前記作成したコンポーネントベースラインを、前記所定の時間帯及び(B)で計算した統計値と対応付けて前記記憶資源に格納し、

(D) 前記コンポーネントベースライン作成後、サービス監視ストリーム及びコンポーネント監視ストリームを新たに受信したら、当該新規受信したサービス監視ストリームに適するコンポーネントベースラインを選択し、前記選択したコンポーネントベースラインを基準に当該新規受信したコンポーネント監視ストリームの異常を判断する、
を処理する監視システム。

[請求項2]

請求項1記載の監視システムであって、

前記監視システムは表示装置を有し、

前記プロセッサは、

前記新規受信したサービス監視値と、

前記新規受信したコンポーネント監視値と、

前記選択したコンポーネントベースラインと、
を前記表示装置に表示させる、
監視システム。

[請求項3] 請求項2記載の監視システムであって、
前記プロセッサは、

(E) 前記サービス実行基盤のイベントを検知し、検知した時間と共に記憶資源に格納し、

(F) (D) にて異常と判断した場合、(D) のコンポーネントベースラインに対応付けられた前記所定の時間帯を取得し、取得した時間帯内に検知したイベントを選択し、

(G) 選択したイベントに基づいて、前記所定の時間帯では検知しなかった直近から所定期間前までのイベントを選択し、

(H) (G) で選択したイベントの内容を表示する、
監視システム。

[請求項4] 請求項3記載の監視システムであって、
前記プロセッサは、

(I) (G) で選択したイベントを過去のイベントから検索することで、類似するイベントを当該類似イベントの検知時間と共に表示する、
監視システム。

[請求項5] 請求項4記載の監視システムであって、
前記検索対象となる過去のイベントには、システム構成上類似する他のサービス実行基盤のイベントも含まれる、
監視システム。

[請求項6] 請求項3記載の監視システムであって、
前記プロセッサは、

(J) (G) で選択したイベントをインシデント情報に含まれるイベントと比較することで、前記直近から所定期間前までに新たに検知

したイベントに関連する可能性があるインシデントの内容を表示する

、

監視システム。

[請求項7]

複数のコンポーネントを含み、前記コンポーネントを用いて所定のサービスを提供するサービス実行基盤を監視する監視システムで実行する監視プログラムであって、

前記監視プログラムは、

前記サービス実行基盤から、前記所定のサービスの監視値であるサービス監視ストリームと、前記コンポーネントの監視値であるコンポーネント監視ストリームと、を受信し、

(A) 過去の所定の時間帯のコンポーネント監視ストリームに基づいてコンポーネントベースラインを作成し、

(B) 過去の所定の時間帯のサービス測定ストリームの統計値を計算し、

(C) 前記作成したコンポーネントベースラインを、前記所定の時間帯及び(B)で計算した統計値と対応付けて前記監視システムの記憶資源に格納し、

(D) 前記コンポーネントベースライン作成後、サービス監視ストリーム及びコンポーネント監視ストリームを新たに受信したら、当該新規受信したサービス監視ストリームに適するコンポーネントベースラインを選択し、前記選択したコンポーネントベースラインを基準に当該新規受信したコンポーネント監視ストリームの異常を判断する、

ステップを含む監視プログラム。

[請求項8]

請求項7記載の監視プログラムであって、

前記監視プログラムは、

前記新規受信したサービス監視値と、

前記新規受信したコンポーネント監視値と、

前記選択したコンポーネントベースラインと、

を前記監視システムの表示装置に表示させる、
ステップを含む監視プログラム。

[請求項9]

請求項8記載の監視プログラムであって、
前記監視プログラムは、

(E) 前記サービス実行基盤のイベントを検知し、検知した時間と共に記憶資源に格納し、

(F) (D) にて異常と判断した場合、(D) のコンポーネントベースラインに対応付けられた前記所定の時間帯を取得し、取得した時間帯内に検知したイベントを選択し、

(G) 選択したイベントに基づいて、前記所定の時間帯では検知しなかった直近から所定期間前までのイベントを選択し、

(H) (G) で選択したイベントの内容を表示する、
ステップを含む監視プログラム。

[請求項10]

請求項9記載の監視プログラムであって、
前記監視プログラムは、

(I) (G) で選択したイベントを過去のイベントから検索することで、類似するイベントを当該類似イベントの検知時間と共に表示する、

ステップを含む監視プログラム。

[請求項11]

請求項10記載の監視プログラムであって、

前記検索対象となる過去のイベントには、システム構成上類似する他のサービス実行基盤のイベントも含まれる、
監視プログラム。

[請求項12]

請求項9記載の監視プログラムであって、
前記監視プログラムは、

(J) (G) で選択したイベントをインシデント情報に含まれるイベントと比較することで、前記直近から所定期間前までに新たに検知したイベントに関連する可能性があるインシデントの内容を表示する

、

ステップを含む監視プログラム。

[請求項13]

請求項3記載の監視システムであって、

前記イベントの検知とは、

前記監視システムが前記サービス実行基盤からイベントの内容を記した情報を受信すること、

または

前記サービス実行基盤の状態を取得することで、前記監視システムが前記サービス実行基盤にてイベントが発生したと判断する、

ことを特徴とする監視システム。

[請求項14]

請求項9記載の監視プログラムであって、

前記イベントの検知とは、

前記監視システムが前記サービス実行基盤からイベントの内容を記した情報を受信すること、

または

前記サービス実行基盤の状態を取得することで、前記監視システムが前記サービス実行基盤にてイベントが発生したと判断する、

ことを特徴とする監視プログラム。

[請求項15]

複数のコンポーネントを含み、前記コンポーネントを用いて所定のサービスを提供するサービス実行基盤と、

前記サービス実行基盤の監視値を含む監視ストリームを受信処理する監視システムと、

を有するシステムであって、

前記監視システムは、

(1) 前記サービス実行基盤のイベントを検知し、検知した時間と共に記憶資源に格納し、

(2) 過去の監視ストリームに基づいてベースラインを作成し、

(3) 前記作成したベースラインを、基となった前記過去の監視ス

トリームの時間帯と関連付けて前記記憶資源に格納し、

(4) 前記ベースライン作成後、監視ストリームを新たに受信したら、前記ベースラインを基準に当該新規受信した監視ストリームの異常を判断し、

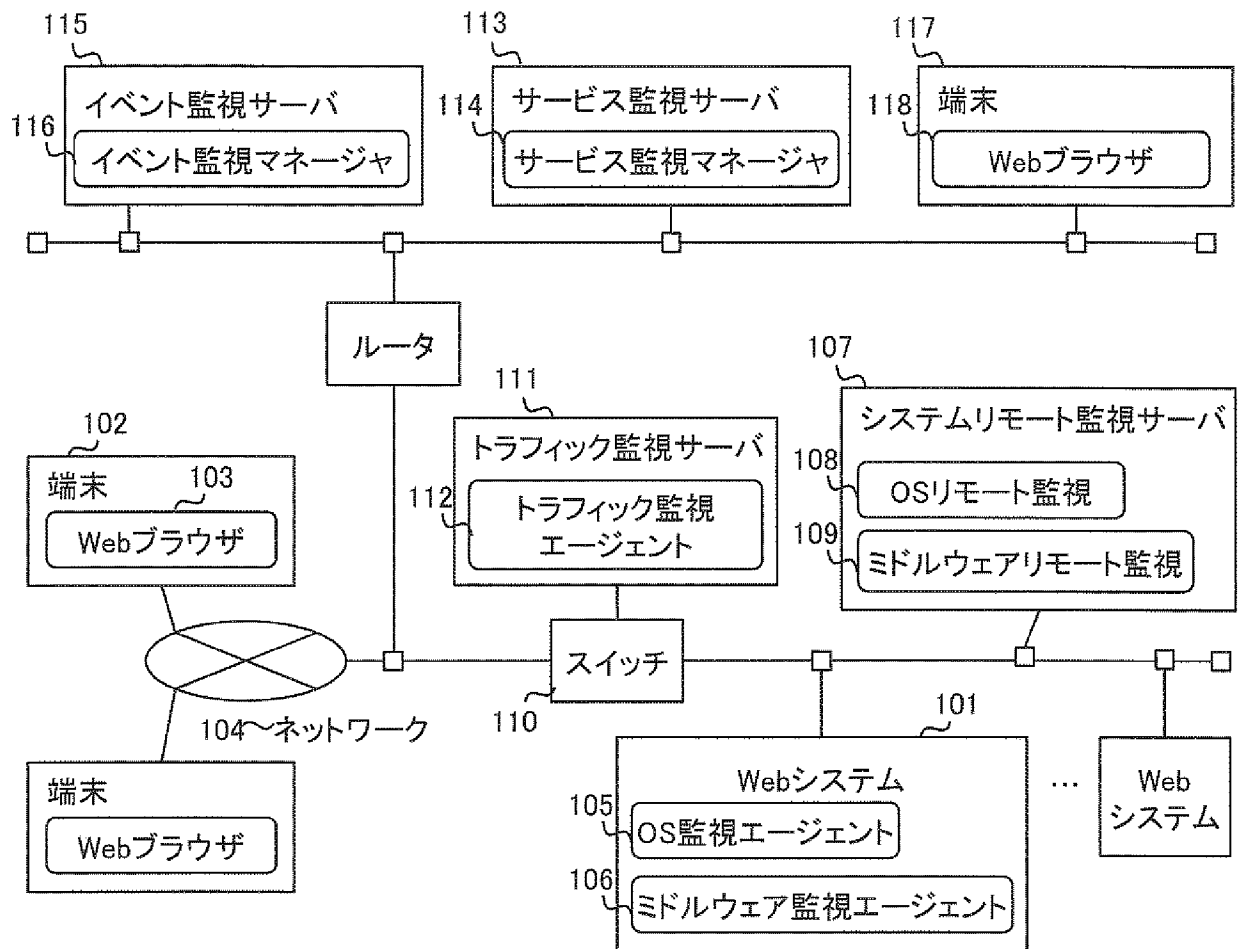
(5) (4) にて異常と判断した場合、(4) のベースラインに対応付けられた時間帯を取得し、取得した時間帯内に検知したイベントを選択し、

(6) 選択したイベントに基づいて、前記取得した時間帯では検知してなかった直近から所定期間前までのイベントを選択し、

(7) (G) で選択したイベントの内容を表示する、
システム。

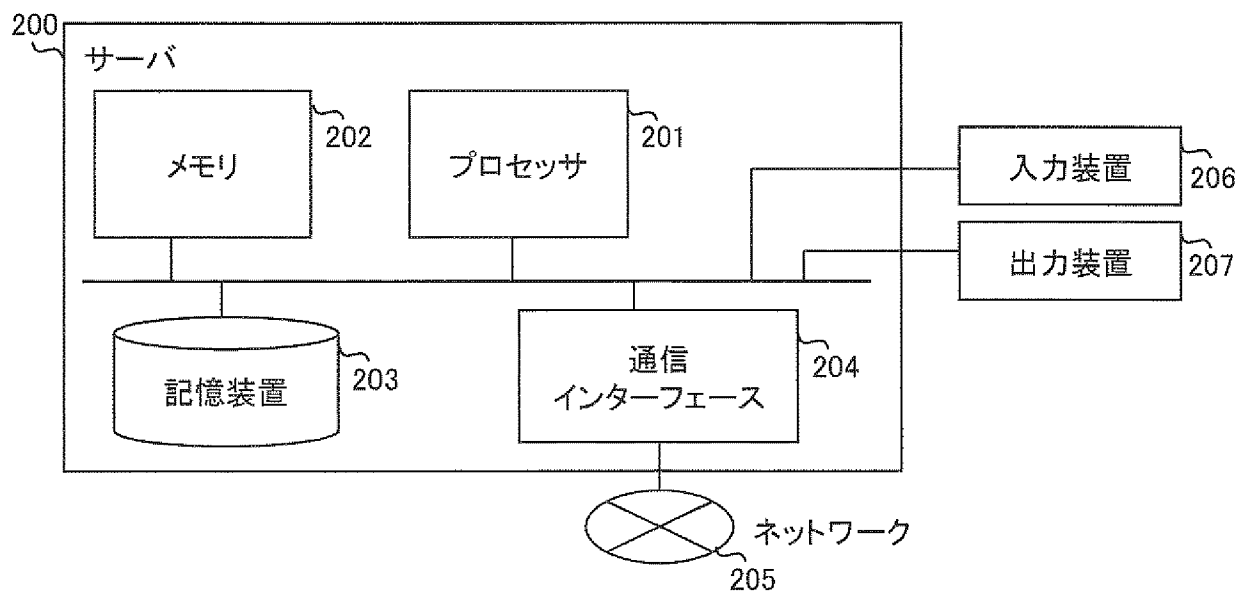
[図1]

【図1】



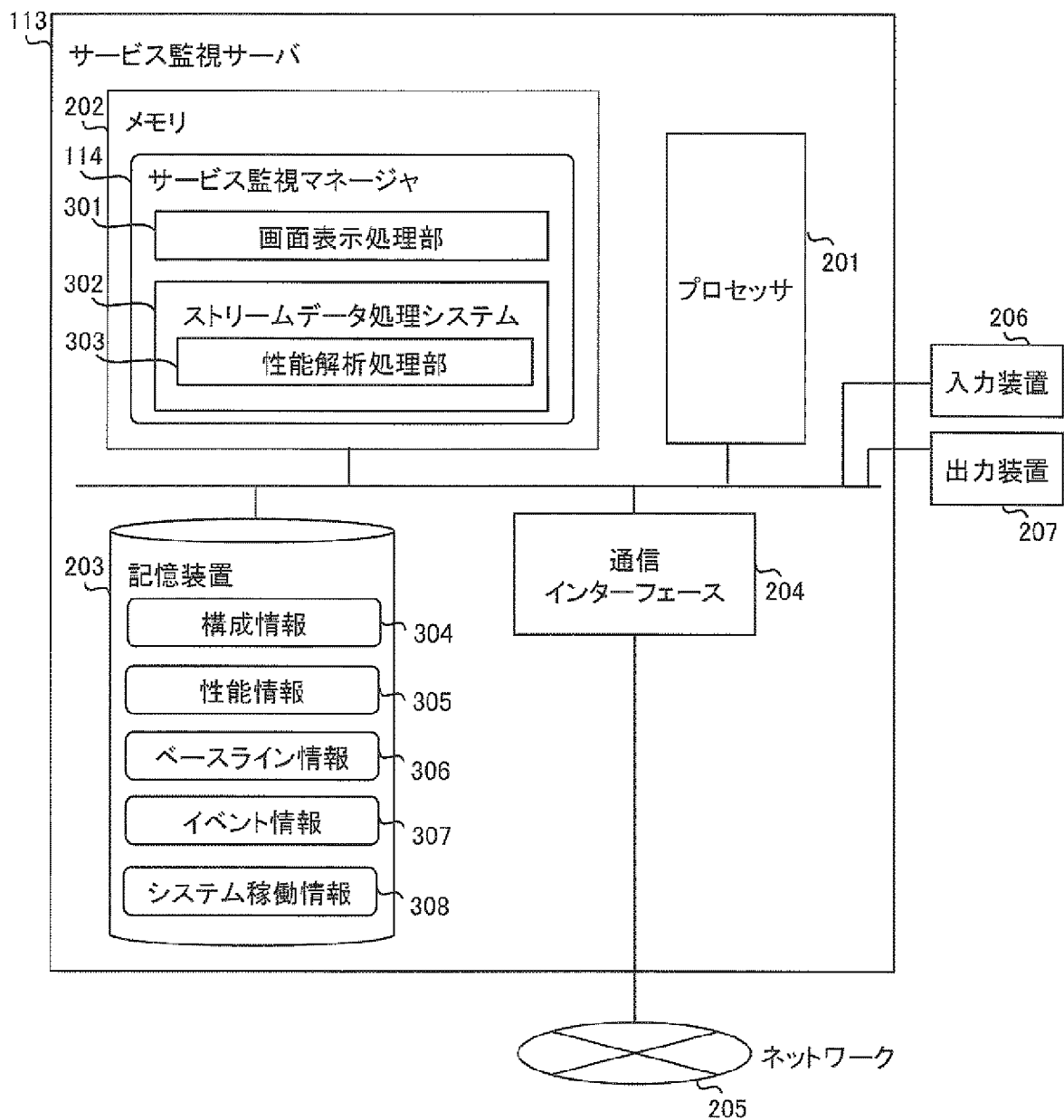
[図2]

【図2】



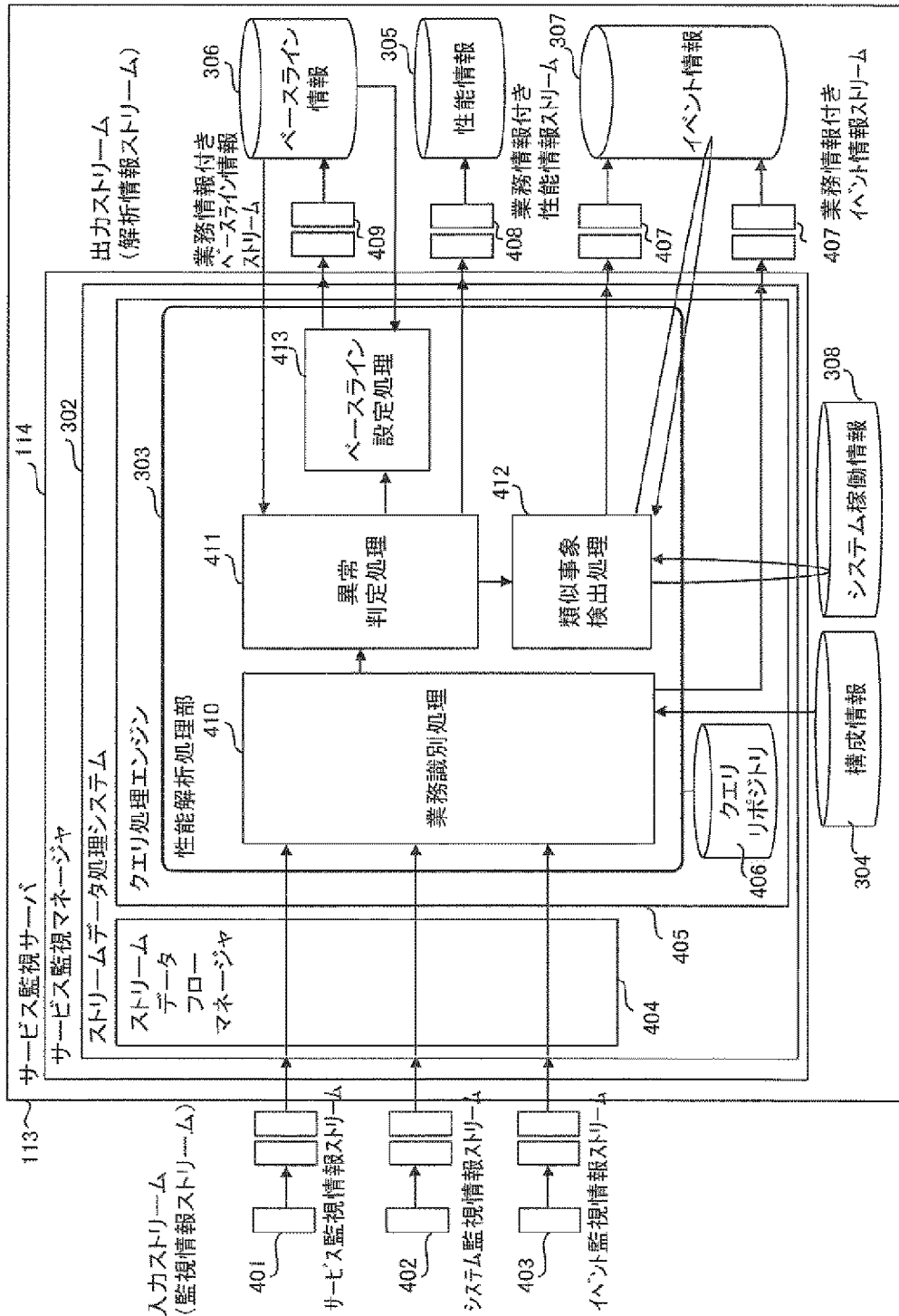
[図3]

【図3】



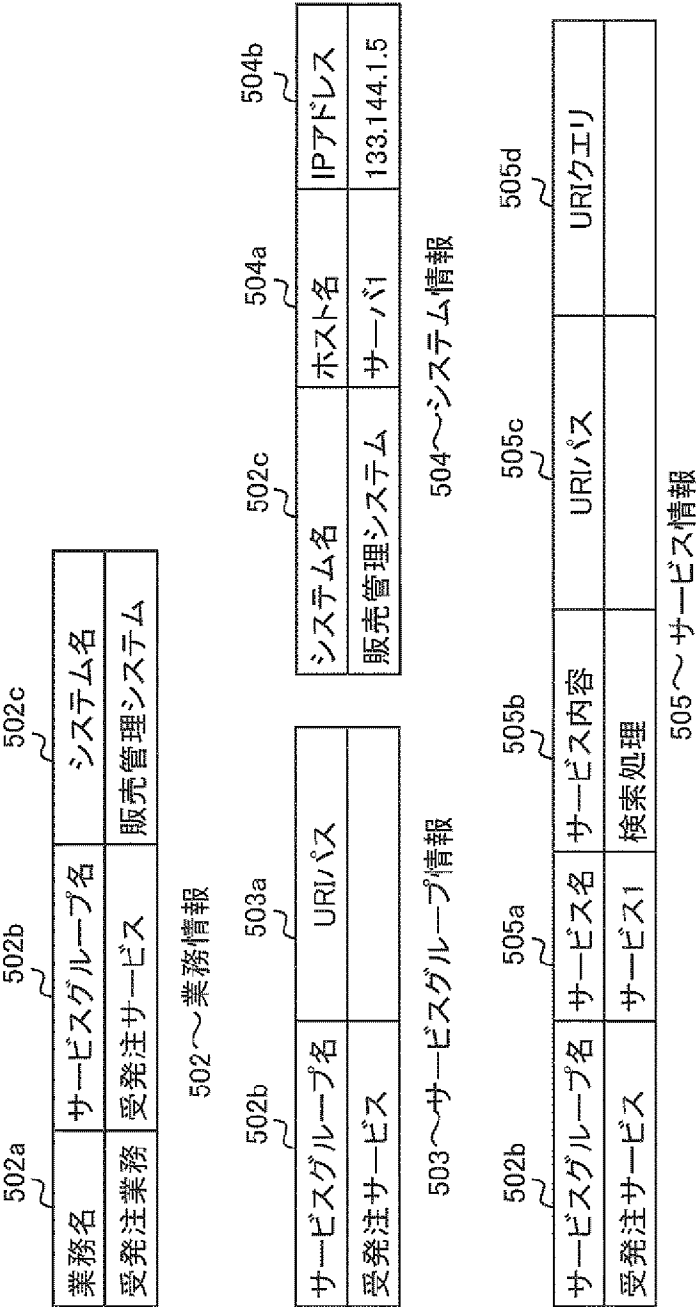
[図4]

【図4】



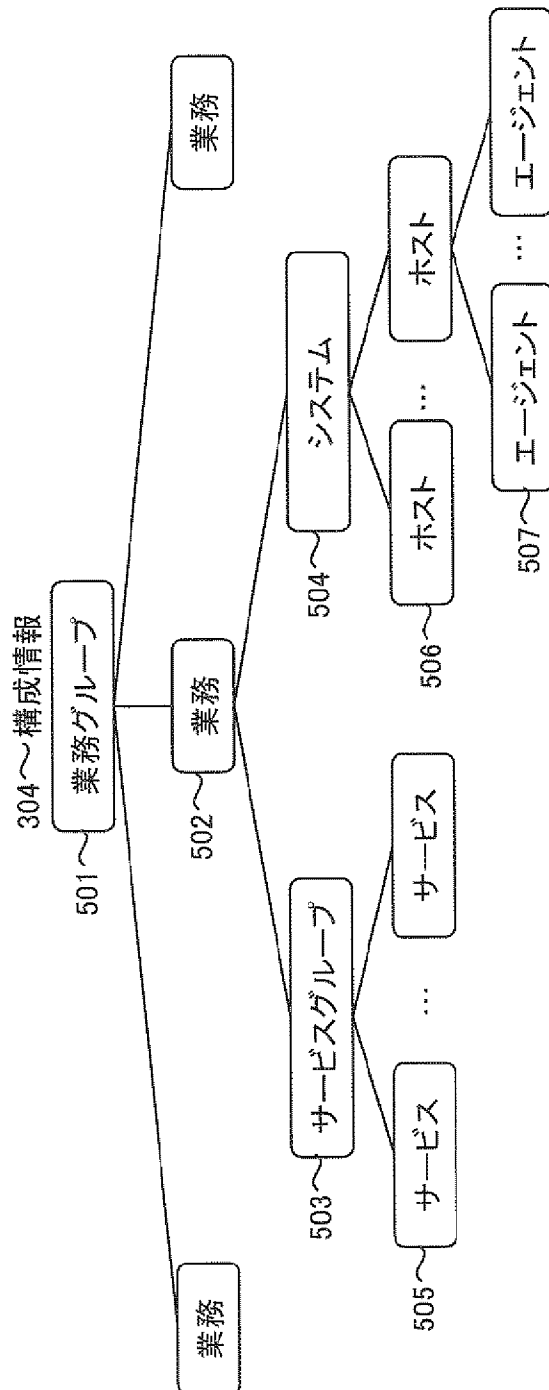
[図5A]

【図5A】



[図5B]

【図5B】



【图6】

605～業務情報付きサービスマニタリングシステム

【圖7】

706～業務情報付きシステム監視情報ストーリーム

[図8]

【図8】

801	802a	802b	802c	802d	802e	802f	803	804
時刻	イベント情報						オブジェクトタイプ	オブジェクト情報
	重大度	登録時刻	イベントID	ソース	メッセージ	アクション		
'12/01/31 15:21	警告						サービス	サービス情報

403～イベント監視情報ストリーム

801	502a	502b	505a	505	505b	802
時刻	業務名	サービスグループ名	サービス情報			イベント情報
			サービス名	内容		
	受発注業務	受発注サービス	サービス1	検索処理		

407a～業務情報付きサービスイベント情報ストリーム

801	802a	802b	802c	802d	802e	802f	803	804
時刻	イベント情報						オブジェクトタイプ	オブジェクト情報
	重大度	登録時刻	イベントID	ソース	メッセージ	アクション		
	情報						ホスト	ホスト情報

403～イベント監視情報ストリーム

801	502a	502c	702a	702	702b	802
時刻	業務名	システム名	ホスト情報			イベント情報
			ホスト名	IPアドレス		
	受発注業務	販売管理システム	サーバ2	133.144.1.5		

407b～業務情報付きシステムイベント情報ストリーム

【図9】

【图9】

[illegible]

307a～イベント情報テーブル

時刻	業務名	サービスグループ名	サービス情報		システム名	ホスト情報		イベント情報
			サービス名	処理内容		ホスト名	IPアドレス	
'12/07/31 15:21	受発注業務	受発注サービス	サービス1	検索処理	販売管理システム	サーバ1	133.144.1.5	

307b～差分イベント情報テーブル

時刻	業務名	サービスグループ名	サービス情報		システム名	ホスト情報		イベント情報
			サービス名	処理内容		ホスト名	IPアドレス	
'12/07/31 15:21	受発注業務	受発注サービス	サービス1	検索処理	販売管理システム	サーバ1	133.144.1.5	

37c～類似イベント情報データベース

[図10]

【図10】

1001		502a	502b	505	1002	1003	1004	1005
時間	業務名	サービスグループ名	サービス情報	判定	応答時間/分(統計値)	スループット/分(累積値)	エラー率/分(累積値)	
408a ～ 業務情報付きサービス性能情報ストリーム								
1001	502a	502b	505	1002	1003	1004	1005	
時間	業務名	サービスグループ名	サービス情報	判定	応答時間/分(統計値)	スループット/分(累積値)	エラー率/分(累積値)	
'12/07/31 15:20	受発注業務	受発注サービス	サービス名	内容	平均	最小	最大	分散
			サービス1	検索処理	3.0	1.0	5.0	σ
			サービス2	登録処理	5.0	3.0	8.0	σ
'12/07/31 15:21								

305a ～ サービス性能情報テーブル

[図11]

【図11】

1101		502a	502c	702	703	704	705	1102
時刻	業務名	システム名	ホスト情報	エージェント名	監視項目	性能情報	判定	
403b 〜 業務情報付きシステム性能情報ストリーム								
1101		502a	502c	702a	702b	703	704a	704b
時刻	業務名	システム名	ホスト情報		エージェント名	監視項目		性能情報
			ホスト名	IPアドレス		レコード名	フィールド名	
	'12/07/31	受発注業務	サーバ1	133.144.1.5	Windows監視	CPU	使用率	70%
	15:21	販売管理システム				メモリ	使用率	60%
305b 〜 システム性能情報テーブル								
						ディスクIO	使用率	40%
								正常
								正常
								正常

[図12]

【図12】

1201		502a	502b	1202		1203		1204	1205		
時間		業務名	サービスグループ名	スループット/分		エラー率/分		応答時間/分		ベースライン採用日時	
				平均	最小	最大	分散	平均	最小	最大	分散
				100	40	120	σ	1	0	5	σ
'12/07/31 15:00		受発注業務	受発注サービス								
'12/07/31 16:00		受発注業務	受発注サービス								'12/07/05 16:00

306a へサービスグループ性能要約情報テーブル

[図13]

【図13】

1301		502a	502c	702	703	704	1302					
時間	業務名	システム名	ホスト情報	エージェント名	監視項目	性能値/分 (統計値)						
409b ～ 業務情報付きシステムベースライン情報ストリーム												
1301		502a	502c	702a	702	702b	703	704a	704	704b	1302	
時間	業務名	システム名	ホスト情報		エージェント名		監視項目					性能値/分
			ホスト名	IPアドレス			レコード名	フィールド名	平均	最小	最大	分散
	'12/07/31	受発注業務	サーバー1	133.144.1.5	Windows監視		CPU	使用率	50%			
	15:00	販売管理システム					メモリ	使用率	50%			
							ディスクIO	使用率	30%			

306b ～ システム性能要約情報テーブル

[図14]

【図14】

1401〜サービスカタログテーブル

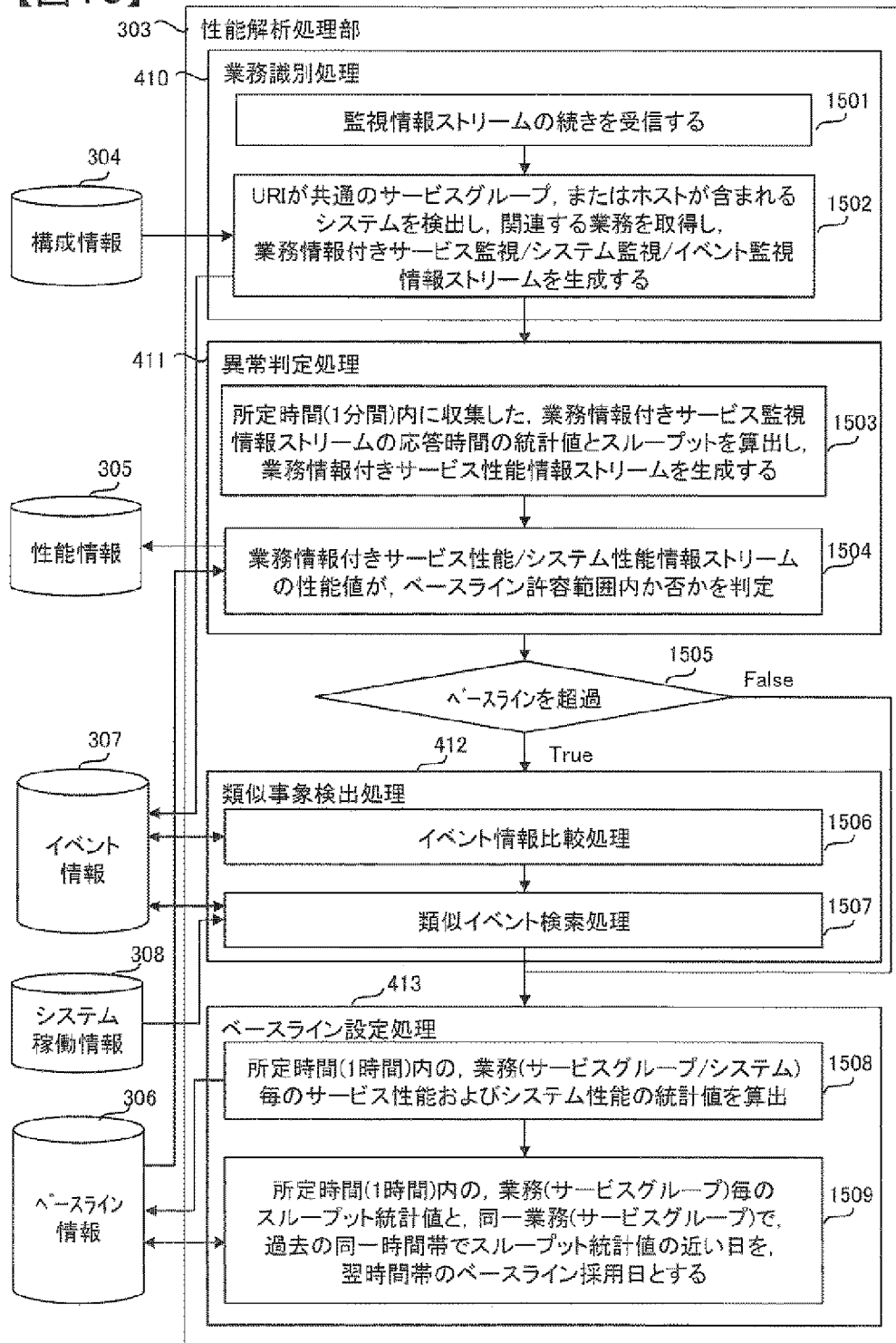
システム種別	サーバスペック	OS種別	ミドルウェア種別	数量
X1システム	Standard	Win2008	IIS	1
	Standard	Win2008	MSSQL	1
	Standard	Win2008	IIS	2
X2システム	Premium	Win2008	MSSQL	1
	Standard	Win2008	Apache/Tomcat	1
Yシステム	Premium	Win2008	Oracle	1
	Standard	Win2008	uCOSmi	1
Zシステム	Premium	Win2008	HiRDB	1

1402〜システム稼働情報テーブル

システム名	システム種別	UP情報	累積稼働日数	アラート発生件数	障害件数	所定期間の平均 サービス性能情報	所定期間の平均 システム性能情報
旧Aシステム	X1システム	a1アプリ	430日	800件	50件	100件/分	CPU使用率...40% メモリ使用率...60% DiskIO使用率...40%
		a2アプリ					
新Aシステム	X2システム	a1アプリ	200日	360件	40件	500件/分	
Bシステム	Yシステム	bアプリ	180日	250件	20件	1000件/分	
Cシステム	Yシステム	cアプリ	100日	180件	18件	1200件/分	

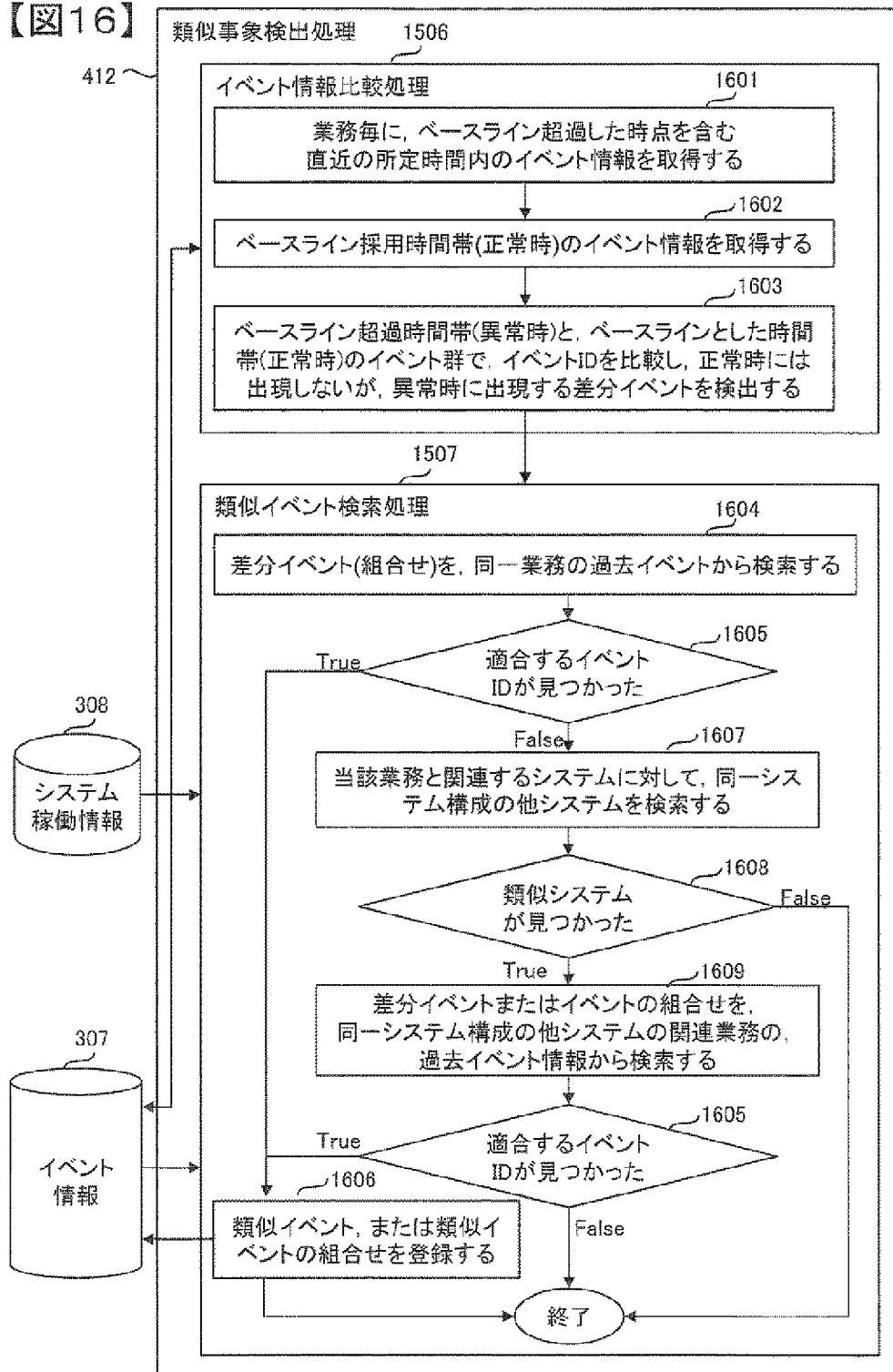
[図15]

【図15】



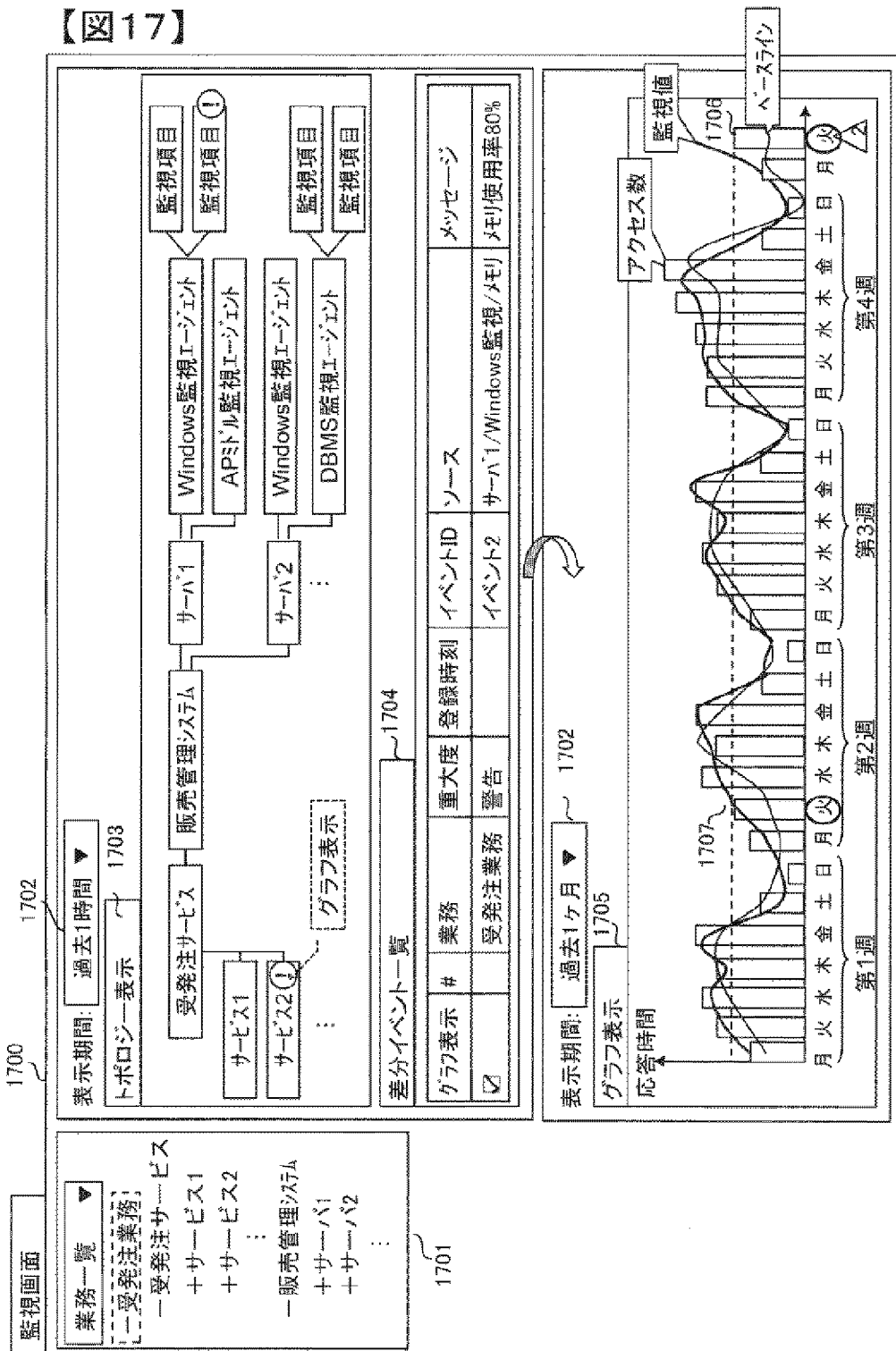
[図16]

【図16】

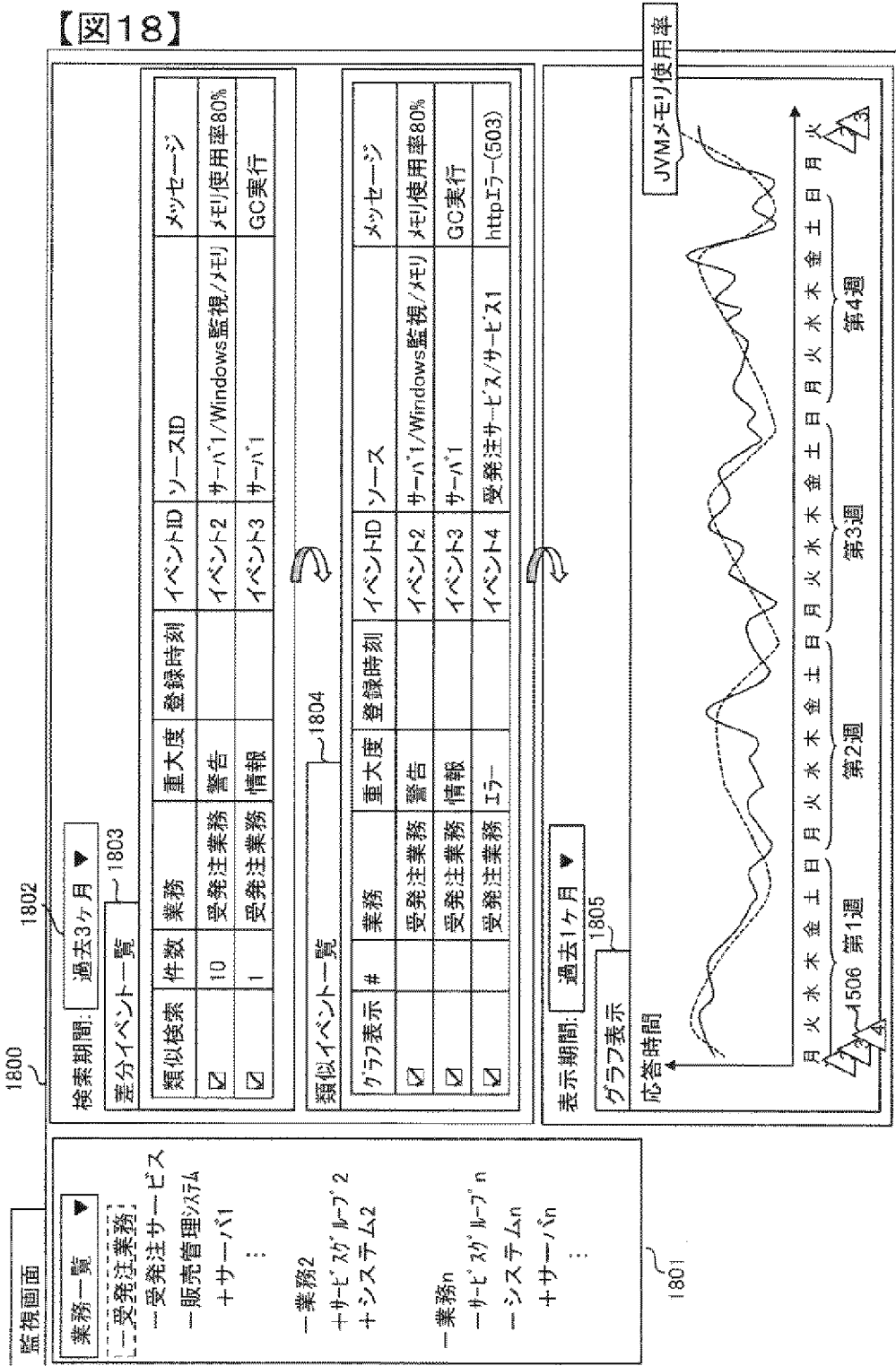


[図17]

【図17】



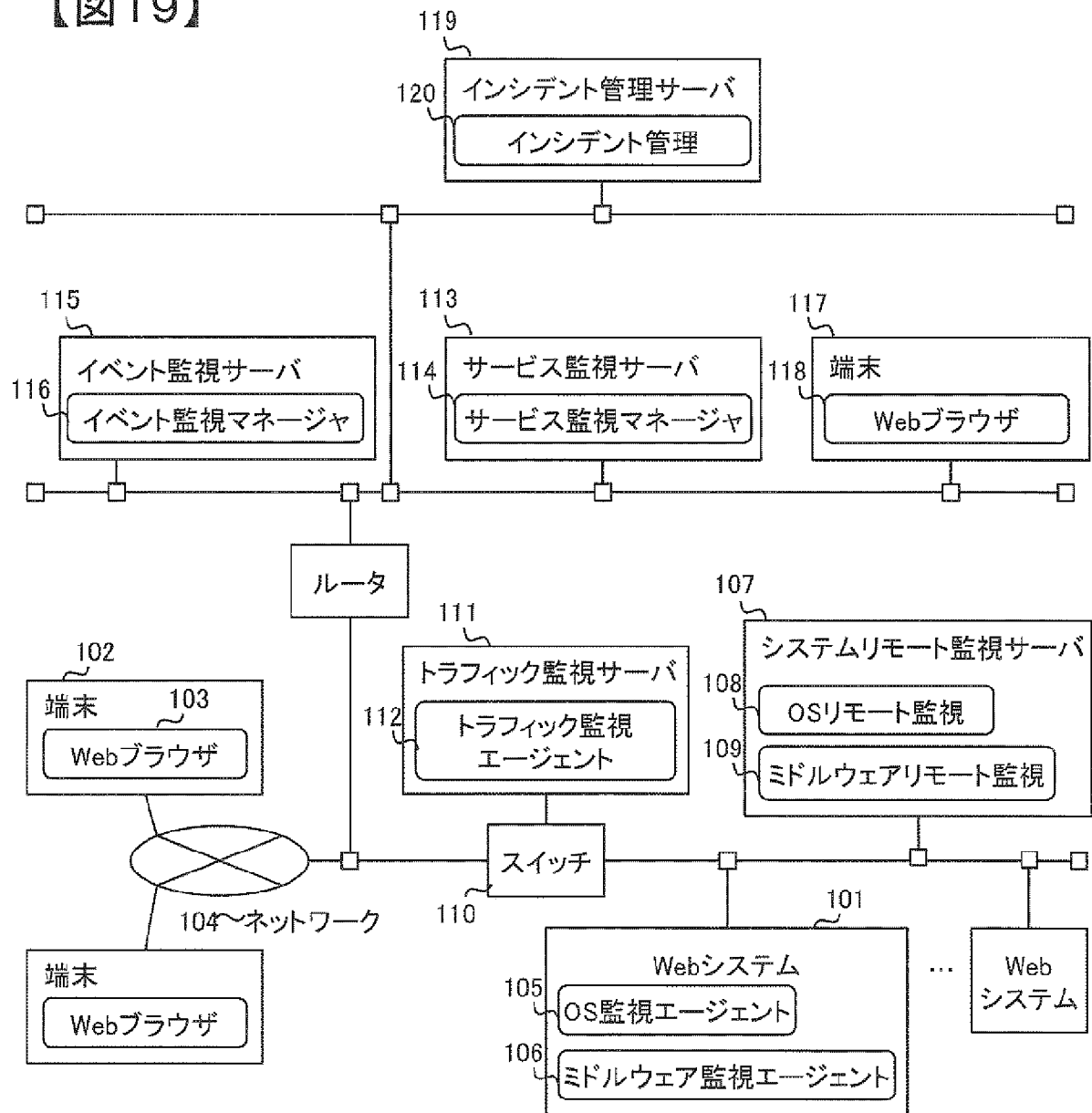
[図18]



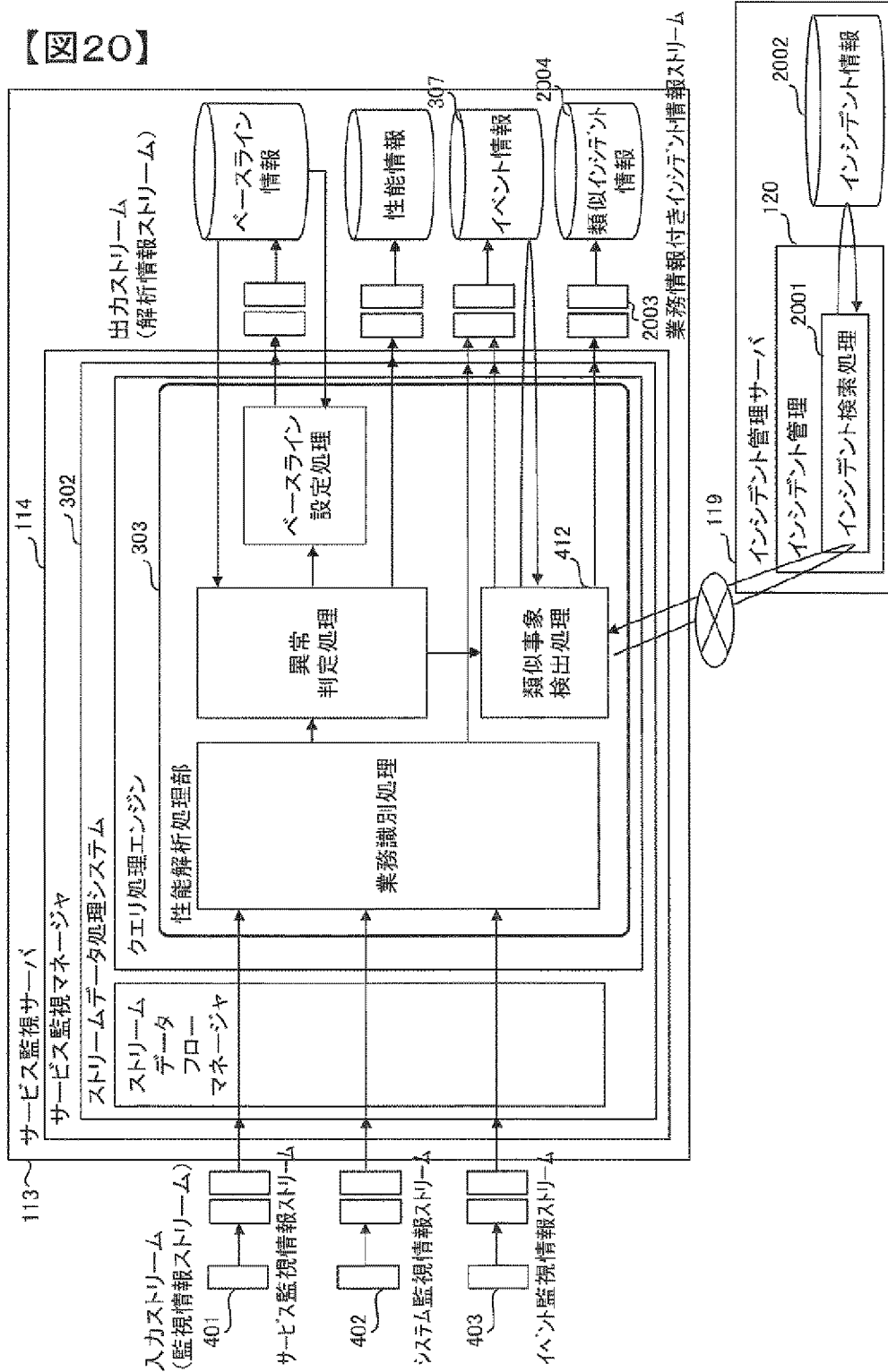
【図18】

[図19]

【図19】



【図20】



[図21]

【図21】

2105	2106	502a	502b	502c	2107
開始日時	終了日時	業務名	サービスグループ名	システム名	差分イベントID (複数イベントは、で区切る)
		受発注業務			

2101 〜インシデント検索のための入力情報

2108	2109	2110	2111	502a	502b	502c	2112	2113
タイトル	重大度	インシデントID	インシデントIDへのURL	業務名	サービスグループ名	システム名	発生日時	関連イベントID (複数イベントは、で区切る)
		インシデント1		受発注業務				

2102 〜インシデント情報テーブル

2108	2109	2110	2111	502a	502b	502c	2112	2113
タイトル	重大度	インシデントID	インシデントIDへのURL	業務名	サービスグループ名	システム名	発生日時	関連イベントID (複数イベントは、で区切る)
		インシデント1		受発注業務				

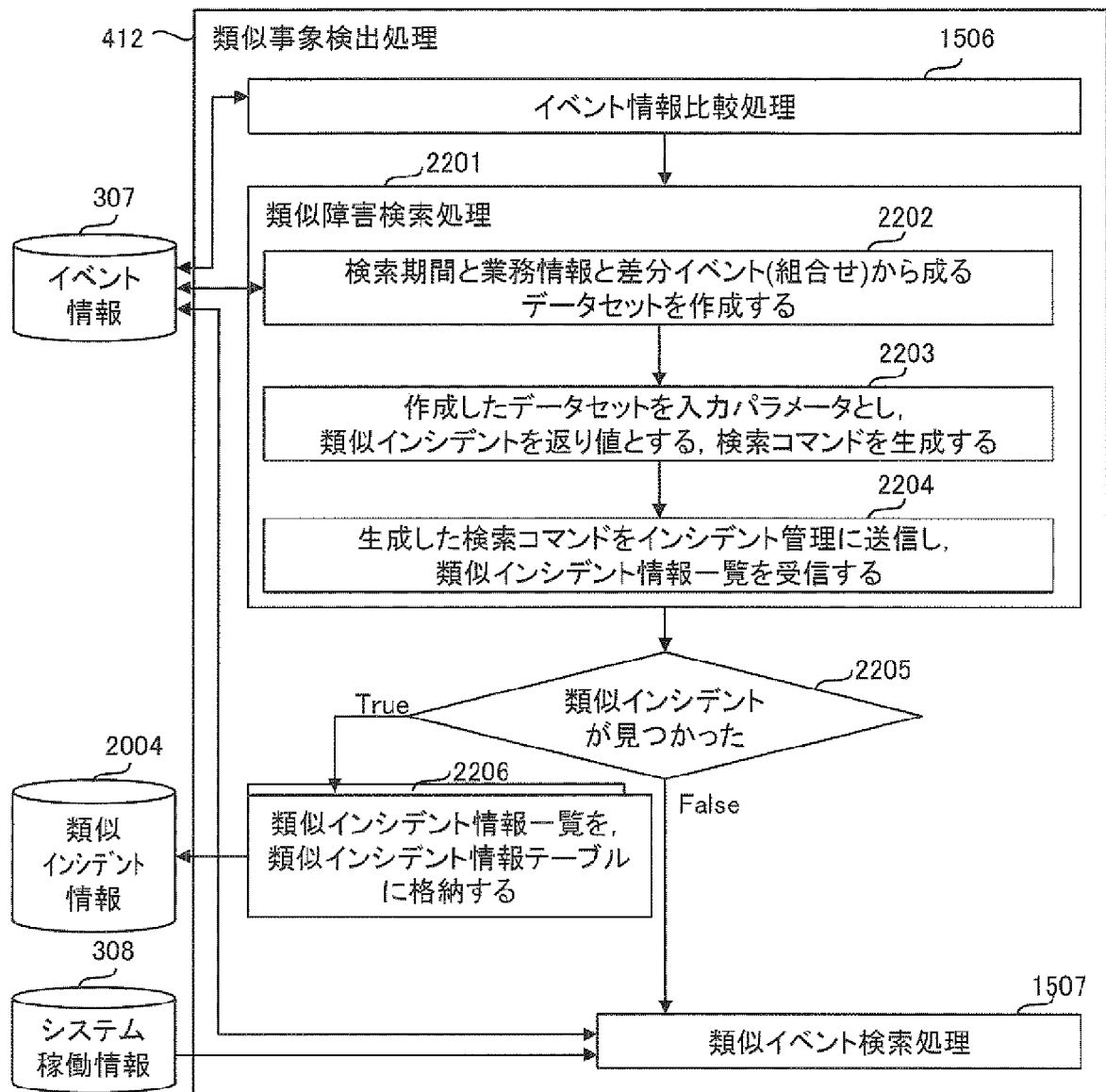
2103 〜インシデント検索結果の出力情報

502a	2109	2110	2111	2112	2118	2113
業務名	重大度	インシデントID	インシデントIDへのURL	発生日時	タイトル	関連イベントID (複数イベントは、で区切る)
受発注業務		インシデント1				

2104 〜類似インシデント情報テーブル

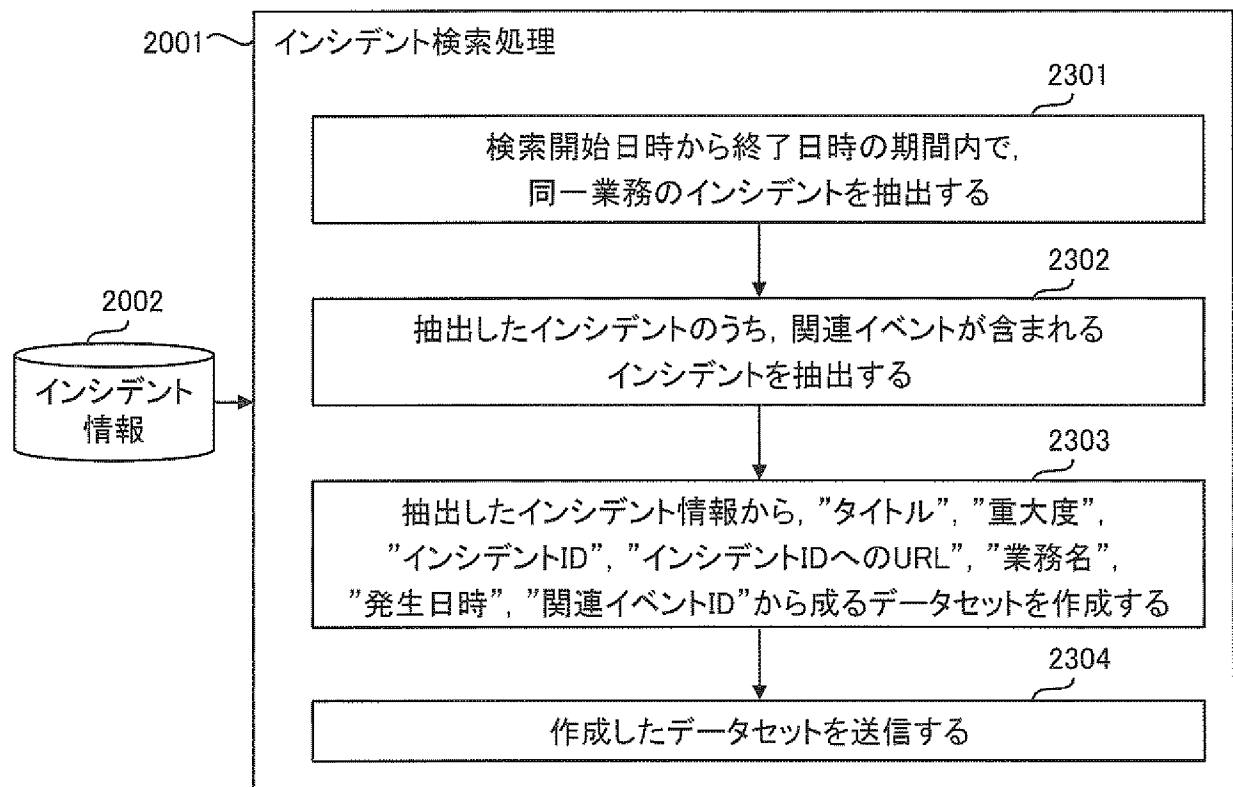
[図22]

【図22】



[図23]

【図23】



【图24】

2400 監視画面

2402

業務一覧 ▼

受発注業務

受発注サービス

販売管理システム

+サーバーバ

2403

業務2

+サーバーグループ2

+システム2

:

検索期間: 過去3ヶ月 ▼

差分イベント一覧 ~ 2401

類似検索	件数	業務	重大度	登録時刻	イベントID	ソースID	メッセージ
☒	10	受発注業務	警告		イベント2	サーバー1/Windows監視/メモリ使用率80%	
☒	1				イベント3	サーバー1	GC実行

類似インシデント一覧 ~ 2404

#	業務	重大度	インシデントID	発生日時	タイトル	関連イベント
1	受発注業務	大	インシデント1	2405	受発注サービス利用不可	イベント2; イベント3; イベント4
2	受発注業務	中	インシデント10		受発注振票シヨフ遅延	イベント2; イベント3; イベント5

インシデント詳細URL

2406 インシデント画面

インシデント情報 ~ 2407

タイトル	: 受発注サービス利用不可		
インシデントID	: インシデント1	関連イベント	: イベント2; イベント3; イベント4
業務	: 受発注業務	システム	: 受発注システム
概要			
発生日時	作業期限		
要因	根本原因		
回避策	解決策		

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2012/072097

A. CLASSIFICATION OF SUBJECT MATTER

G06F11/34(2006.01)i, G06F11/30(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F11/34, G06F11/30

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2012
Kokai Jitsuyo Shinan Koho	1971-2012	Toroku Jitsuyo Shinan Koho	1994-2012

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2001-142746 A (NEC Software Chubu, Ltd.), 25 May 2001 (25.05.2001), entire text; all drawings (Family: none)	1-15
A	JP 2005-316808 A (NEC Software Chubu, Ltd.), 10 November 2005 (10.11.2005), entire text; all drawings (Family: none)	1-15
A	JP 2011-034208 A (Hitachi, Ltd.), 17 February 2011 (17.02.2011), entire text; all drawings & US 2011/0029817 A1	1-15



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

“A” document defining the general state of the art which is not considered to be of particular relevance

“E” earlier application or patent but published on or after the international filing date

“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

“O” document referring to an oral disclosure, use, exhibition or other means

“P” document published prior to the international filing date but later than the priority date claimed

“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

“&” document member of the same patent family

Date of the actual completion of the international search
05 November, 2012 (05.11.12)

Date of mailing of the international search report
13 November, 2012 (13.11.12)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

A. 発明の属する分野の分類（国際特許分類（I P C））
Int.Cl. G06F11/34(2006.01)i, G06F11/30(2006.01)i

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（I P C））

Int.Cl. G06F11/34, G06F11/30

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922-1996年
日本国公開実用新案公報	1971-2012年
日本国実用新案登録公報	1996-2012年
日本国登録実用新案公報	1994-2012年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
A	JP 2001-142746 A（中部日本電気ソフトウェア株式会社） 2001.05.25, 全文, 全図（ファミリーなし）	1-15
A	JP 2005-316808 A（中部日本電気ソフトウェア株式会社） 2005.11.10, 全文, 全図（ファミリーなし）	1-15
A	JP 2011-034208 A（株式会社日立製作所）2011.02.17, 全文, 全図 & US 2011/0029817 A1	1-15

☐ C欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの

「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「O」口頭による開示、使用、展示等に言及する文献

「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」同一パテントファミリー文献

国際調査を完了した日

05.11.2012

国際調査報告の発送日

13.11.2012

国際調査機関の名称及びあて先

日本国特許庁（I S A/J P）

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官（権限のある職員）

多胡 滋

5 B

3562

電話番号 03-3581-1101 内線 3545