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

特許第6252309号
(P6252309)

(45)発行日　平成29年12月27日(2017.12.27)　(24)登録日　平成29年12月8日(2017.12.8)

(51)Int.Cl.		F I		
G06F 13/00	(2006.01)	G06F	13/00	351N
G06F 11/34	(2006.01)	G06F	11/34	
G06Q 50/10	(2012.01)	G06Q	50/10	

請求項の数 8　(全 22 頁)

(21)出願番号　特願2014-71075(P2014-71075)
(22)出願日　平成26年3月31日(2014.3.31)
(65)公開番号　特開2015-194797(P2015-194797A)
(43)公開日　平成27年11月5日(2015.11.5)
審査請求日　平成28年12月6日(2016.12.6)

(73)特許権者　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(74)代理人　100094525
弁理士　土井　健二
(74)代理人　100094514
弁理士　林　恒徳
(72)発明者　石原　俊
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　有賀　光希
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

最終頁に続く

(54)【発明の名称】監視漏れ特定処理プログラム，監視漏れ特定処理方法及び監視漏れ特定処理装置

(57)【特許請求の範囲】
【請求項１】
複数の被監視デバイスから第１のログ項目蓄積装置に転送された事象の発生時刻を含むログ項目を，前記第１のログ項目蓄積装置から収集し，収集した前記ログ項目を収集した収集時刻の情報と共に第２のログ項目蓄積装置に蓄積し，
前記第２のログ項目蓄積装置内の前記ログ項目から，前記第１のログ項目蓄積装置への転送遅延が生じた監視漏れログ項目を検出し，
前記監視漏れログ項目の発生時刻と近接する発生時刻を有し，前記監視漏れログ項目の被監視デバイスとは別の被監視デバイスのログ項目の収集時刻を，前記監視漏れログ項目の前記転送遅延の発生時刻と特定する
処理をコンピュータに実行させる監視漏れ特定プログラム。
【請求項２】
前記転送遅延の発生時刻を特定する処理では，
前記監視漏れログ項目を発生した被監視デバイスと，同等または類似する転送間隔を有する第１の被監視デバイスをグループ化し，
前記別の被監視デバイスのログ項目を，前記グループ化した第１の被監視デバイスのログ項目から検出する
請求項１に記載の監視漏れ特定プログラム。
【請求項３】
前記転送遅延の発生時刻を特定する処理では，

前記監視漏れログ項目を発生した被監視デバイスと，同等または類似する転送間隔を有する第１の被監視デバイスをグループ化し，
前記グループ化された第１の被監視デバイスから，前記監視漏れログ項目の発生時刻に転送遅延の発生確率が最も低い第２の被監視デバイスを選択し，
前記他の被監視デバイスのログ項目を，前記選択された第２の被監視デバイスのログ項目から検出する請求項１に記載の監視漏れ特定プログラム。
【請求項４】
前記第２のログ項目蓄積装置に蓄積する処理では，
前記第１のログ項目蓄積装置に転送された前記ログ項目を第１の収集間隔で収集し，
前記第１のログ項目蓄積装置に転送された前記ログ項目を前記第１の収集間隔より長い第２の収集間隔で収集し，
前記監視漏れログ項目を検出する処理では，前記第１の収集間隔で収集した第１のログ項目群内に存在せず，前記第２の収集間隔で収集した第２のログ項目群内に存在するログ項目を前記監視漏れログとして検出する
請求項１～３のいずれかに記載の監視漏れ特定プログラム。
【請求項５】
前記処理は，更に，
前記特定された転送遅延の発生時刻までの時間帯における，前記監視漏れログの被監視デバイスの負荷値の推移情報を前記収集したログ項目から抽出して，前記抽出した負荷値の推移情報を監視漏れパターンとして蓄積し，
監視中の被監視デバイスの負荷値の推移情報が，前記監視漏れパターンの負荷値の推移情報と一致するか否かを監視し，
前記監視漏れパターンと一致した被監視デバイスに監視漏れが発生する予兆を検出する請求項１に記載の監視漏れ特定プログラム。
【請求項６】
前記被監視デバイスによりサービスシステムが構成され，
前記監視漏れパターンは，前記負荷値の推移情報に加えて前記サービスシステムを構成する被監視デバイス数を有し，
前記監視漏れパターンと一致するか否かを監視する処理では，更に，前記監視中のサービスシステムを構成する被監視デバイス数が，前記監視漏れパターンの被監視デバイス数と一致するか否かを判定し，被監視デバイス数が一致した監視漏れパターンについて，前記監視処理を実行する
請求項５に記載の監視漏れ特定プログラム。
【請求項７】
複数の被監視デバイスから第１のログ項目蓄積装置に転送された事象の発生時刻を含むログ項目を，前記第１のログ項目蓄積装置から収集し，収集した前記ログ項目を収集した収集時刻の情報と共に第２のログ項目蓄積装置に蓄積し，
前記第２のログ項目蓄積装置内の前記ログ項目から，前記第１のログ項目蓄積装置への転送遅延が生じた監視漏れログ項目を検出し，
前記監視漏れログ項目の発生時刻と近接する発生時刻を有し，前記監視漏れログ項目の被監視デバイスとは別の被監視デバイスのログ項目の収集時刻を，前記監視漏れログ項目の前記転送遅延の発生時刻と特定する
処理をコンピュータに実行させる監視漏れ特定処理方法。
【請求項８】
複数の被監視デバイスから第１のログ項目蓄積装置に転送された事象の発生時刻を含むログ項目を，前記第１のログ項目蓄積装置から収集し，収集した前記ログ項目を収集した収集時刻の情報と共に第２のログ項目蓄積装置に蓄積する手段と，
前記第２のログ項目蓄積装置内の前記ログ項目から，前記第１のログ項目蓄積装置への転送遅延が生じた監視漏れログ項目を検出する手段と，
前記監視漏れログ項目の発生時刻と近接する発生時刻を有し，前記監視漏れログ項目の

被監視デバイスとは別の被監視デバイスのログ項目の収集時刻を，前記監視漏れログ項目の前記転送遅延の発生時刻と特定する手段とを有する監視漏れ特定処理装置。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は，監視漏れ特定処理プログラム，監視漏れ特定処理方法及び監視漏れ特定処理装置に関する。

【背景技術】

【０００２】

クラウドコンピューティングには，仮想サーバやネットワークを提供するIaaS （Infrastructure as a Service)や，仮想サーバやネットワークの提供に加えて，OSのインストール，データベースの提供も行うPaaS (Platform as a Service)などがある。いずれの場合でも，クラウドコンピューティングを利用するユーザは，ユーザのサービスシステムを複数のインスタンス（仮想マシン，仮想デバイス，物理マシン，物理デバイス等を含む）で構成する。そして，サービスシステムを構成する複数のインスタンスは，サービスの負荷やスケジュールに応じてそのインスタンス数が頻繁に増減する。

【０００３】

ユーザは，上記のサービスシステムを監視するために，各インスタンスが出力するログ項目を適切に収集して管理する。ログ項目には，例えば，サービスシステムのイベントログや，一定間隔でサンプリングされる性能情報ログなどがある。性能情報ログは，例えば，インスタンスのCPU利用率，メモリ利用量，ネットワーク転送量，イベント数などの負荷値を含む。

【０００４】

これらのログ項目を一元的に管理する方法として，複数のインスタンスそれぞれが，それぞれで発生したログ項目を共通のログ項目蓄積装置に定期的に転送して集約し，監視サーバが，そのログ項目蓄積装置を定期的にポーリングしてログ項目を収集する技術が提案されている。そ監視サーバは，収集した各インスタンスのログ項目に基づいて，各インスタンスの状態及び異常をリアルタイムに監視する。また，上記の共通のログ項目蓄積装置内のデータベースとして，処理の高速性や拡張性の観点からKVS（Key Value Store）型のデータベースが利用される。

【先行技術文献】

【特許文献】

【０００５】

【特許文献１】特開２０１３－７３４９７号公報

【特許文献２】特開２００５－１１５７２４号公報

【発明の概要】

【発明が解決しようとする課題】

【０００６】

しかしながら，各インスタンスは，負荷集中などによりデータベースへのログ項目の転送ができない場合がある。その場合，監視サーバはログ項目蓄積装置からログ項目を収集できず，ログ項目の欠落が発生する。そのようなログ項目の欠落が生じると，監視サーバは適切にクラウドサービスシステムを監視することができない。

【０００７】

さらに，各ログ項目は，ログ項目の発生時刻とログ項目の内容（事象）を有しているが，インスタンスからログ項目蓄積装置への転送時刻は有していない。そのため，ログ項目の欠落により監視漏れが発生した場合，転送遅延による監視漏れの発生時刻を知ることができない。

【０００８】

そこで，１つの側面では、本発明の目的は，転送遅延による監視漏れの発生時刻を特定する監視漏れ特定処理プログラム，監視漏れ特定処理方法及び監視漏れ特定処理装置を提

供することにある。
【課題を解決するための手段】
【０００９】
開示された実施の形態の第１の側面は，複数の被監視デバイスから第１のログ項目蓄積装置に転送された事象の発生時刻を含むログ項目を，前記第１のログ項目蓄積装置から収集し，収集した前記ログ項目を収集した収集時刻の情報と共に第２のログ項目蓄積装置に蓄積し，
前記第２のログ項目蓄積装置内の前記ログ項目から，前記第１のログ項目蓄積装置への転送遅延が生じた監視漏れログ項目を検出し，
前記監視漏れログ項目の発生時刻と近接する発生時刻を有し，前記監視漏れログ項目の被監視デバイスとは別の被監視デバイスのログ項目の収集時刻を，前記監視漏れログ項目の前記転送遅延の発生時刻と特定する
処理をコンピュータに実行させる監視漏れ特定プログラムである。
【発明の効果】
【００１０】
第１の側面によれば，転送遅延による監視漏れの発生時刻を高精度に特定することができる。
【図面の簡単な説明】
【００１１】
【図１】本実施の形態の監視漏れ発生時刻を特定する対象のクラウドコンピューティングの構成を示す図である。
【図２】監視サーバによるログの収集処理を示す図である。
【図３】KVS型データベースのログのデータ構成例である。
【図４】監視漏れを防止する第１の方法例を示す図である。
【図５】監視漏れを防止する第２の方法例を示す図である。
【図６】転送時刻が不明のため監視漏れ発生時間帯の高精度な推定が困難であることを示す図である。
【図７】本実施の形態における監視サーバ３０の構成を示す図である。
【図８】本実施の形態におけるクラウドコンピューティングセンタと監視サーバの構成と処理を示す図である。
【図９】本実施の形態における監視漏れのないリアルタイムログ監視の処理の概略を示すフローチャート図である。
【図１０】監視漏れ発生時刻の特定処理S1のフローチャート図である。
【図１１】監視サーバによるログ収集について説明する図である。
【図１２】監視サーバによるログ収集について説明する図である。
【図１３】本実施の形態における監視漏れログの発生時刻と最も近い発生時刻を有するログを特定する処理S16のフローチャート図である。
【図１４】各インスタンスのログ転送間隔を推定する方法示す図である。
【図１５】各インスタンスのログ転送間隔を推定する方法示す図である。
【図１６】監視サーバにより時刻差が近接しているとしてグルーピングされたインスタンスB,C,Eのログの例を示す図である。
【図１７】監視漏れ発生時刻の特定処理S1により特定された監視漏れ発生時刻の例を示す図である。
【図１８】監視漏れパターンの構築処理S2のフローチャート図である。
【図１９】監視漏れパターンの例を示す図である。
【図２０】図９の監視漏れ発生の予兆検出と個別ポーリング処理S3のフローチャート図である。
【図２１】監視漏れ発生の予兆検出における監視漏れパターンと監視中の負荷値の推移データとの一致を説明する図である。
【図２２】本実施の形態において監視漏れ発生の予兆を検出した場合の個別収集を示す図

である。

【発明を実施するための形態】

【００１２】

図１は，本実施の形態の監視漏れ発生時刻を特定する対象のクラウドコンピューティングの構成を示す図である。サーバファシリティ（施設）であるクラウドコンピューティングセンタ１内には，ハードウエア群１０と，管理サーバ１３と，ハードディスクなどの大容量の保守情報記憶装置１４とが設けられる。そして，センタ１には，インターネットやイントラネットなどのネットワークNETを介して，クラウドコンピューティングサービスのユーザ端末２０と，ユーザのサービスシステムにアクセスしてそのサービスを利用するクライアント端末２２と，ユーザのサービスシステムを監視する監視サーバ３０などが，接続可能になっている。

【００１３】

ユーザは，ユーザ端末２０から管理サーバ１３にアクセスして，クラウドコンピューティングサービスの利用契約を締結し，ハードウエア群１０を仮想化した仮想化マシン（以下インスタンスとも称する）１２によるサービスシステムを構築する。

【００１４】

一方，ユーザのサービスシステムを利用するクライアントは，クライアント端末２２からネットワークNETを経由してサービスシステムを構成する仮想化マシン１２にアクセスし，サービスを受ける。

【００１５】

ハードウエア群１０は，複数のサーバを有し，各サーバは，CPUとメモリ（RAM)とハードディスク（HDD)などの大容量記憶装置とネットワークなどを有する。クラウドコンピューティングサービスを受けるユーザは，ユーザ端末２０から管理サーバ１３にアクセスして，ユーザのサービスシステムを構築するために必要な仕様を選択し，クラウドコンピューティングサービスの利用契約を締結する。

【００１６】

例えば，ユーザは，ユーザ端末２０から，ユーザのサービスシステムに必要な仮想化マシンの仕様，例えばCPUのクロック周波数，メモリの容量，ハードディスクの容量，ネットワークの帯域幅，OS,データベース，プログラム言語などを選択する。

【００１７】

そして，管理サーバ１３は，ハードウエア群１０のホストマシンの仮想化ソフトウエア（ハイパバイザ）１３に依頼して，利用契約に基づいてハードウエア群１０を仮想化して仮想化マシン１２に割り当て，ユーザのサービスシステムを構成する単一又は複数の仮想化マシン１２を構築する。また，管理サーバ１３は，仮想化ソフトウエア１３と連携して，ユーザのサービスシステムを構成する仮想化マシン１２の運用状態を管理する。管理サーバ１３は，例えば，ある仮想化マシン１２に負荷が集中した場合に，新たな仮想化マシンを生成するスケールアウトを仮想化ソフトウエア１３に要求する。したがって，サービスシステムを構成する仮想化マシン（以下インスタンスと称する）の数は，負荷や業務スケジュールに応じて頻繁に増減する。

【００１８】

ユーザのサービスシステムの障害時の原因調査などのために，監視サーバ３０が，サービスシステムが所定の頻度で出力するイベントログや，一定間隔でサンプリングした性能情報ログを収集する。監視サーバ３０は，ユーザにより運用される場合もあり，またはユーザから委託された業者により運用される場合もある。

【００１９】

イベントログには，例えば，サービス起動，サービス停止などの通常イベントや，起動失敗，ファイルアクセス失敗，ファイル書き込み失敗などのエラーイベントなどが含まれる。また，性能情報ログには，CPU利用率，メモリ使用量，イベント発生数，ネットワーク転送量などが含まれる。

【００２０】

監視サーバ３０によるイベントログや性能情報ログの収集は，概略的には，次のように行われる。まず，サービスシステムを構成する複数のインスタンス１２は，各インスタンスで発生したイベントログとサンプリングした性能情報ログを，保守情報記憶装置１４に格納されている共通のデータベースに非同期に転送する。これにより，頻繁に発生，消滅するインスタンスの増減に対応して，ログを一元的に蓄積して管理することができる。

【００２１】

この転送頻度である転送間隔は，例えば，利用契約時にユーザによりインスタンス毎に設定される。通常，緊急性の高いインスタンスについてのイベントログには，例えば数分毎のように短い転送間隔が設定され，緊急性の低いインスタンスについてのイベントログには，それより長い転送間隔が設定される。また，性能情報ログは，比較的長い転送間隔に設定される。

【００２２】

また，保守情報記憶装置１４内のイベントログデータベース（DB)や性能情報ログデータベース（DB)は，処理の高速性や拡張性の観点から，例えばKVS（Key Value Store)型のデータベースが用いられる。

【００２３】

次に，監視サーバ３０は，保守情報記憶装置１４内のデータベースに蓄積された最新のログを実質的にリアルタイムに収集して，監視サーバ３０の保守情報記憶装置３１のイベントログ管理DBと性能情報ログ管理DB内に格納する。これにより，監視サーバ３０は，サービスシステムのインスタンスの異常をリアルタイムに監視する。

【００２４】

本実施の形態では，監視サーバ３０が仮想マシンが転送するログを蓄積した保守情報記憶装置１４からログを収集し，収集したログに基づいて仮想マシンの状態を監視する。ここで，「ログ」とはログファイルにレコードとして格納される個々のログであり，ログファイルと区別するためにログ項目と称する場合もある。また，保守情報記憶装置１４に記憶されたデータベースに個々のログ項目が蓄積されるので，保守情報記憶装置１４はログ項目蓄積装置である。監視サーバ３０が管理する保守情報記憶装置３１も同様にログ項目蓄積装置である。さらに，本実施の形態において監視サーバ３０は，仮想マシン以外にも，物理マシン，物理マシンに設けられる物理デバイス，仮想マシンに設けられる仮想デバイスなども監視対象のデバイスとして，それらのログを収集する。したがって，以下の「インスタンス」とは，仮想マシン，仮想デバイス，物理マシン，物理デバイスなどを含む被監視デバイスの意味で使用する。

【００２５】

［ログ収集の課題］

図２は，監視サーバによるログの収集処理を示す図である。第１に，サービスシステムを構成する複数のインスタンスA,Bが，それぞれログを発生する。各インスタンスがログを発生する時刻を発生時刻ｔ１と称する。各インスタンスは，イベントログや性能情報ログを発生する。図２の例では，インスタンスAが，ログA1を発生時刻13:22に，ログA2を発生時刻13:32にそれぞれ発生している。また，インスタンスBが，ログB1を発生時刻13:23に，ログB2を発生時刻13:33にそれぞれ発生している。

【００２６】

図３は，KVS型データベースのログのデータ構成例である。ログA1は，KEYとして発生時刻，VALUとしてイベント内容（発生した事象の内容），インスタンスIDなどを有する。このようなデータ構成の場合，例えば，発生時刻をキーにしてログを抽出することができる。

【００２７】

第２に，各インスタンスA,Bは，利用契約で設定された転送間隔で，それぞれが発生したログをクラウドコンピューティングセンタ内の保守情報記憶装置１４内のログDBに転送する。以下，このインスタンスが保守情報記憶装置１４内のログDBに転送する時刻を，転送時刻ｔ２と称する。図２の例では，インスタンスA,Bは，共に，１０分の転送間隔で13:

20,13:30,13:40に発生したログを転送する。

【００２８】

第３に，監視サーバ３０は，定期的にログ収集ポーリングを行って，保守情報記憶装置１４内のログDBからログを収集する。監視サーバによるログ収集の時刻を収集時刻ｔ３と称する。図２の例では，監視サーバ３０が１０分の収集間隔で収集時刻13:22,13:32,13:42に，ログ収集のポーリングを行っている。このログ収集では，監視サーバ３０は，ログの発生時刻をキーにして，前回のポーリング時に収集したログの最新の発生時刻より後の発生時刻を有するログを収集する。監視サーバ３０は，各インスタンスの転送時刻を知ることはできないので，上記のように，前回収集したログの最新の発生時刻より後の発生時刻を有するログを収集することで，収集するログが重複しないようにすることができる。

【００２９】

しかしながら，上記のログ収集では次のような課題がある。すなわち，負荷集中などで特定のインスタンスのみログDBに転送することができず，その転送漏れにより次に転送できるまで転送遅延が生じたとする。図２の例では，インスタンスAが，負荷集中により，転送時刻13:30でログA1の転送を行っていない。つまり，ログA1は転送時刻13:30の時点で転送漏れログとなっている。しかし，監視サーバ３０は定期的なログ収集のポーリングを繰り返し，毎回のログ収集では，前回収集したログの最新発生時刻より後の発生時刻を有するログを収集する。その結果，監視サーバは，収集時刻13:32の収集ではインスタンスBのログB1を収集するがインスタンスAのログA1は収集できず，更に，転送時刻13:40でログA1が遅れて転送された後の収集時刻13:42の収集でも，収集キーがログB1の発生時刻13:13より後の発生時刻となるため，やはりログA1を収集できない。つまり，転送遅延したログA1は，その後のログ収集では収集されない。この収集されないログA1は，転送漏れし転送遅延したことによる監視漏れログであり，監視漏れログが発生することで監視漏れが発生する。

【００３０】

図４は，監視漏れを防止する第１の方法例を示す図である。図４には，図２と同じログの発生と転送例が示されている。監視漏れを防止する第１の方法例では，監視サーバは，ログを収集する時のキーを，前回収集したログの最新発生時刻より一定時間TBだけ巻き戻した時刻より後の発生時刻を有するログとし，毎回の収集ポーリングで，少しずつ余分に過去に発生したログを収集し，収集済みの重複したログを削除する。

【００３１】

この第１の方法によれば，図４において，監視サーバは，収集時刻13:32の収集では，前回収集したログB0の発生時刻13:13より巻き戻し時間TB早い時刻13:13-TBより後の発生時刻を有するログを収集し，ログB1に加えてログB0を再度収集している。したがって，監視サーバは，重複するログB0を削除する。さらに，監視サーバは，収集時刻13:42の収集では，ログB1の発生時刻13:23より巻き戻し時間TB早い13:23-TBより後の発生時刻を有するログを収集し，ログA1,A2,B1,B2を収集している。したがって，監視サーバは，重複するログB1を削除する。但し，監視サーバは，転送遅延していたログA1を収集することができている。

【００３２】

上記の第１の方法では，巻き戻し時間TBを長くすれば収集漏れを減らすことができるものの，重複して収集するログが増大し，収集時の通信トラフィック量が増大するという問題がある。一方，巻き戻し時間TBを短くすれば，重複して収集するログは減少し，通信トラフィック量も減少するが，収集漏れの可能性が高くなる。そして，巻き戻し時間TBは，経験則的に人手で決定しなければならず，日や時刻に応じてインスタンスの負荷が異なり，負荷集中が発生する時刻や時間帯の長さなどの予測が難しく，巻き戻し時間TBの最適化が困難である。

【００３３】

図５は，監視漏れを防止する第２の方法例を示す図である。図５には，図２と同じログの発生と転送例が示されている。監視漏れを防止する第２の方法例では，監視サーバは，

インスタンスA,Bを個別に収集するポーリングを実行する。この個別収集によれば，監視サーバは，それぞれのインスタンスに対して，前回収集したログの中の最新の発生時刻より後の発生時刻を有するログを収集する。したがって，インスタンス毎に収集するキーの発生時刻が異なる。

【００３４】

図５の例では，収集時刻13:22より前の個別収集で，インスタンスA，Bのログの最新の発生時刻がそれぞれTa，Tbだったとする。監視サーバは，収集時刻13:22での個別収集でログB0を収集する。さらに，監視サーバは，収集時刻13:32での個別収集で，インスタンスAについては時刻Taより後の発生時刻のログを，インスタンスBについてはログB0の発生時刻13:13より後の発生時刻のログを，それぞれ収集し，ログB1を収集する。このとき，インスタンスAは負荷集中によりログA1を転送できなかったため，監視サーバは，転送遅延しているログA1を収集できない。そして，監視サーバは，収集時刻13:42での個別収集で，インスタンスAについては再度時刻Taより後の発生時刻のログを，インスタンスBについてはログB1の発生時刻13:23より後の発生時刻のログを，それぞれ収集する。その結果，監視サーバは，インスタンスAへの個別収集で，ログA2に加えて転送遅延していたログA1を収集し，インスタンスBへの個別収集でログB2を収集する。

【００３５】

このように，監視サーバが，インスタンス毎に個別に収集すれば，転送遅延を起こしたログを確実に収集することができる。上記の例で，ログA1は転送遅延されていて遅れて転送されているが，転送後の収集ポーリングで確実に収集されている。したがって，監視漏れ発生を回避することができる。

【００３６】

しかしながら，ユーザのサービスシステムを構成するインスタンス数が膨大になると，個別収集のポーリング回数も膨大になり，監視サーバの負担が増大することが問題になる。したがって，常時個別収集のポーリングを実行することは好ましくない。

【００３７】

［本実施の形態］

本実施の形態では，監視サーバは，ログの転送が行われずにログが滞留して監視漏れが発生する時間帯を分析し，監視対象のサービスシステムの各インスタンスについて監視漏れ発生の予兆を検出し，予兆が検出されたインスタンスに対して，ログの滞留が解消されるまで個別収集等のポーリングを実行する。

【００３８】

そこで，監視漏れが発生する時間帯を分析するにあたっての課題としては，ログの転送時刻を知ることができないことである。すなわち，監視漏れログは，監視サーバにより収集済みのログ管理DB内のログと，転送済みの保守情報記憶装置１４内のログDB内のログとを対比することにより，特定することができる。しかし，各インスタンスのログ転送時刻を知ることができないので，どの時間帯で負荷集中が発生してログ転送が実行されずログの転送遅延が発生したかを分析することができない。前述のとおり，利用契約ではユーザは各インスタンスについて転送間隔を設定する。しかし，ログの転送時刻は，クラウドコンピューティングサービス提供者の管理下にあり，また，クラウドコンピューティングサービスの監視に不要な情報であるので，一般に，監視サーバが転送時刻を取得することはできない。

【００３９】

図６は，転送時刻が不明のため監視漏れ発生時間帯の高精度な推定が困難であることを示す図である。図６のログの発生と転送と収集の例は，図２と同じである。

【００４０】

上記の通り，各インスタンスの転送時刻を知ることはできない。そこで，もし保守情報記憶装置１４内のログDB内のログと，監視サーバ側のログ管理DB内のログとを対比させて，監視漏れログA1を検出したとする。ログA1の発生時刻は，監視情報として必要であるのでログA1のデータに含まれている。しかし，ログAを発生したインスタンスAの転送時刻は

不明である。そのため，監視漏れログA1の監視漏れ原因となった転送漏れが発生して転送遅延によりログが滞留した時間帯は，少なくとも，収集時刻13:42より前でログA1の発生時刻13:22より後であるとしか推定できない。

【００４１】

上記の推定した転送遅延によりログが滞留した時間帯は長いので，そのような長い時間にわたりインスタンスAに対する個別収集のポーリングを実行することは，監視サーバの負担が大きい。もし，インスタンスAのログ転送時刻を知ることができれば，例えば，監視漏れログA1の発生時刻後の転送時刻13:30で転送漏れが発生し，次の転送時刻13:40で転送が再開されたことを正しく推定できる。その結果，転送漏れが発生した転送時刻13:30以降から転送再開した転送時刻13:40までに，インスタンスAに対して個別収集のポーリングを実施することができ，最短の時間帯での個別収集で監視漏れログA1をタイムリに収集することができる。

【００４２】

以下，本実施の形態について，概略説明の後に，転送漏れにより監視漏れが発生した時刻を特定する方法について説明し，その後，監視漏れをなくすログ収集方法について説明する。

【００４３】

［概略］

図７は，本実施の形態における監視サーバ３０の構成を示す図である。監視サーバ３０は，CPU３０１と，入出力装置３０２と，メインメモリ（RAM)３０３と，大容量記憶装置（HDD)を有する。大容量記憶装置には，ログの監視を実行する監視プログラム３０５，収集したイベントログ管理DBと性能情報管理DB３０５，監視漏れパターンDB３０６が格納される。CPU３０１がメモリ３０３内に展開した監視プログラム３０５を実行することにより，監視サーバ３０は，クラウドコンピューティングサービスセンタ１内の保守情報記憶装置１４内に集約されたログDB内のログを収集し，転送漏れし転送遅延が生じた監視漏れログを検出し，監視漏れが発生したインスタンスの転送漏れ発生前の性能情報パターンをデータベース化し，その転送漏れパターンに基づいて監視中のサービスシステムのインスタンスにおける転送漏れによる監視漏れ発生の予兆を検出し，検出されたインスタンスに対して個別収集のポーリングを実行する。

【００４４】

図８は，本実施の形態におけるクラウドコンピューティングセンタと監視サーバの構成と処理を示す図である。図９は，本実施の形態における監視漏れのないリアルタイムログ監視の処理の概略を示すフローチャート図である。

【００４５】

図９に示されるとおり，監視サーバ３０は，CPUが監視プログラム３０４を実行することにより，収集したログから監視漏れログを検出し，その検出した監視漏れログの転送漏れによる転送漏れの発生時刻を特定する処理を実行する（S1)。

【００４６】

さらに，監視サーバ３０は，CPUが監視プログラム３０４を実行することにより，特定した監視漏れ発生時刻前後におけるインスタンスの数やインスタンスの性能情報（負荷値など）の推移データを，監視漏れパターンとして監視漏れパターンDB内に格納する（S2)。

【００４７】

そして，監視サーバ３０は，CPUが監視プログラム３０４を実行することにより，監視用ポーリングで収集した性能情報に対して，監視漏れパターンとの一致度評価を実行し，監視漏れ発生の予兆を検出し，予兆が検出されたインスタンスに個別収集ポーリングを実行する（S3)。

【００４８】

次に，上記の３つの処理S1,S2,S3について詳述する。

【００４９】

まず，前提として，図８に示すとおり，クラウドコンピューティングセンタ１内において，ユーザのサービスシステムを構成するインスタンス１２の保守情報転送部１２Ａが，ユーザと締結した利用契約に基づくサービス管理情報１５内のログの転送間隔を参照して，その転送間隔で保守情報記憶装置１４内のログDBに発生したログを転送する（図中（１）（２））。

【００５０】

［図９の転送漏れし転送遅延したことによる監視漏れ発生時刻を特定する処理S1］

図１０は，監視漏れ発生時刻の特定処理S1のフローチャート図である。また，図１１，図１２は，監視サーバによるログ収集について説明する図である。

【００５１】

第１に，図１１に示されるとおり，監視サーバ３０は，監視プログラムを実行することにより，監視用ポーリングで収集したログを，それらのログを収集したポーリングの収集時刻と共に，ログ管理DBに格納する。図１１にはイベントログ管理DBの一例が示されている。ログデータは，図３で説明したとおり，ログの発生時刻とイベント内容（事象の発生時刻と事象の内容）とインスタンスIDとが含まれている。そして，図１１に示されるとおり，監視サーバ３０は，上記のログデータに，ログの収集時刻を追加してログ管理DBに格納する。

【００５２】

図１１中，インスタンス名はインスタンスIDに対応し，イベント内容を示すメッセージとイベントの緊急度レベルを示すレベルはイベント内容に対応する。そして，図１１では，各ログは，さらに，発生時刻と収集時刻を有する。図１１に示したメッセージの例は，上から，ロード失敗，サービス開始通知，サービス停止通知，ファイル検出不能，起動不能，プロセスエラーである。

【００５３】

第２に，図１２に示されるとおり，監視サーバ３０は，保守情報記憶装置１４内のログDBからの収集のポーリングについて，本来の第１の収集間隔で行う監視用ポーリングに加えて，第１の収集間隔より十分に長い第２の収集間隔で，且つ望ましくはサービスの負担が低く発生するログが少ない時間帯に，監視漏れチェック用ポーリングを実行する。監視漏れチェック用ポーリングも，監視用ポーリングと同様に，前回収集したログのうち最新発生時刻をキーにして，クエリを実行する。

【００５４】

図１２の例では，監視用ポーリングを実施する第１の収集間隔は１０分毎であり，一方，監視漏れチェック用ポーリングを実施する第２の収集間隔は１日毎である。このように監視漏れチェック用ポーリングの頻度を低くすることで，さらに望ましくはサービスの負担が低い時間帯に実施することで，監視サーバ３０の負担を最小限に抑える。

【００５５】

図１２の例では，監視サーバ３０は，監視用ポーリングで収集されたログを，監視サーバ３０の保守情報記憶装置３１内のログ管理DBに格納する。ただし，図２で説明したとおり，監視用ポーリングで収集したログ管理DB３１には，転送漏れ，転送遅延により監視漏れしたログA1は収集されていない。一方，監視漏れチェック用ポーリングで収集したログ３２には，転送遅延により監視漏れしたログA1が含まれている。

【００５６】

監視サーバ３０は，監視漏れチェック用ポーリングで収集したログは，保守情報記憶装置３１には格納せず，ログ管理DB内の監視用ポーリングで収集したログと突き合わせを行い，一致するか否かをチェックする。これにより，監視サーバ３０は，転送遅延により監視漏れしたログA1を検出する。監視サーバ３０は，監視漏れチェック用ポーリングで収集したログを，上記のチェック後に破棄する。これにより，保守情報記憶装置３１の容量を最小限に抑えることができる。

【００５７】

図１０を参照して，転送漏れによる監視漏れ発生時刻を特定する処理S1について説明す

る。前述の通り，監視サーバ３０は，CPUが監視プログラムを実行することで，通常の監視用ポーリングと，それより長い収集間隔で監視漏れチェック用ポーリングを実行する（S11)。

【００５８】

そして，監視漏れチェック用ポーリングを完了した段階で，監視サーバ３０は，CPUによる監視プログラムの実行により，管理漏れチェック用ポーリングで収集した全てのログ（図１２の３２）から１件のログを選択し（S12)，選択したログが監視用ポーリングで収集したイベントログ管理DB内にも存在するか否か確認し，確認後破棄する（S13)。もし存在するのであれば，監視サーバは，次のログを選択し（S12)，イベントログ管理DB内に存在するか否か確認する（S13)ことを繰り返す。そして，監視サーバは，選択したログがイベントログ管理DB内に存在しない場合は，その選択したログを監視漏れログと判断する（S15)。

【００５９】

次に，監視サーバ３０は，CPUが監視プログラムを実行することで，イベントログ管理DB内の上記検出した監視漏れログのインスタンスとは別のインスタンスのログのうち，監視漏れログの発生時刻と最も近いまたは近接する発生時刻を有するログを特定する（S16)。そして，監視サーバは，特定したログの収集時刻を，転送遅延による監視漏れ発生時刻と特定する（S17)。

【００６０】

監視サーバは，監視漏れチェック用ポーリングで収集したログ全てについて，上記の処理S12-S17を実行し，全ての監視漏れログの監視漏れ発生時刻を特定する。

【００６１】

図８を参照して，以上の処理について再度説明する。監視サーバ３０の定期収集部３１０の監視用収集部３１２が，監視用ポーリングを実行して保守情報記憶装置１４内のログを収集して，監視サーバ３０側の保守情報記憶装置３１内のイベントログ管理DB及び性能情報管理DB３０５に格納する（図中(3)(4)）。一方，定期収集部３１０の監視漏れチェック収集部３１１が，監視漏れチェック用ポーリングを実行して保守情報記憶装置１４内のログを収集し（図中(3)(4)')，監視漏れ発生時刻特定部３１４が，イベントログ管理DB内のログと突き合わせして，監視漏れログを特定する（図中(5))。

【００６２】

次に，図１０の監視漏れログの発生時刻と最も近い発生時刻を有するログを特定する処理S16について詳述する。

【００６３】

図１３は，本実施の形態における監視漏れログの発生時刻と最も近い発生時刻を有するログを特定する処理S16のフローチャート図である。このログを特定する処理S16は，次の３つの処理により行われる。

【００６４】

まず前提として，ユーザのサービスシステムは複数のインスタンスで負荷分散するので，負荷集中などによる転送漏れによる監視漏れが複数のインスタンスで同時に発生する確率は低い。そこで，監視サーバは，イベントログDB内の転送漏れが発生していない他のインスタンスのログのうち，転送漏れにより監視漏れが発生したログの発生時刻と最も近いまたは近接する発生時刻を有するログの収集時刻を，監視漏れ発生時刻と推定する。

【００６５】

（１）図１３の３つの処理のうち第１の処理では，監視サーバは，サービスシステムを構成する複数のインスタンスの中から，監視漏れログの発生元インスタンスとログ転送間隔が同じまたは近いインスタンスを選択して，グルーピングする（S161)。ここで，各インスタンスのログ転送間隔は，収集したログの発生時刻と収集時刻との時刻差に基づいて推定することができる。または，ユーザが利用契約を締結したときに設定した転送間隔を含む管理情報にアクセス可能な場合は，その設定済みの転送間隔を利用しても良い。

【００６６】

図１４，図１５は，各インスタンスのログ転送間隔を推定する方法示す図である。図１４には，サービスシステムを構成する複数のインスタンスが発生したログと，それらログの保守情報記憶装置１４内のログDBへの転送と，監視サーバ側の保守情報記憶装置３１内のログ管理DBへの収集例を示す。複数のインスタンスは，例えばインスタンスA,B,C,D,Eを有するが，図１４にはその内インスタンスA,Bだけが示されている。インスタンスC,D,Eについては示していない。また，この例では，インスタンスA,Bのログの転送漏れは発生していないが，図示していないインスタンスEのログに転送漏れが発生しているものとする。

【００６７】

そして，図１４に示されるように，インスタンスAはログA1,A2を発生し，比較的長い転送間隔の２０分毎に転送している。インスタンスBはログB1-B4を発生し，比較的短い転送間隔の５分毎に転送している。また，監視サーバは，比較的短い収集間隔の５分毎に転送されたログを収集している。

【００６８】

図１５は，インスタンス毎のログの収集時刻と発生時刻の時刻差とその平均値の例を示している。図１４のインスタンスAのログA1,A2と，インスタンスBのログB1-B3とについて示している。インスタンスAの２つのログの収集時刻と発生時刻の時刻差の平均は１３分３０秒であるのに対して，インスタンスBの４つのログの収集時刻と発生時刻の時刻差の平均は２分１５秒である。

【００６９】

収集間隔が比較的短い場合，この時刻差が短いほどログの転送間隔は短く，時刻差が長いほどログの転送間隔は長い傾向になる。したがって，多数のログについて時刻差の平均を取得できれば，各インスタンスの転送間隔が同じまたは近いか否かを判定することができる。図１５の例では，インスタンスＢとＣとＥが時刻差の平均値が近接している。このような時刻差の平均値を比較することで，監視サーバは，インスタンスB,C,Eをグルーピングする。

【００７０】

（２）図１３の３つの処理のうち第２の処理では，監視サーバは，グループ内のインスタンスから，監視漏れログの発生時刻に転送漏れによる転送遅延の発生確率が最も低かったインスタンスを選択する（S162)。この処理について図１６を参照して説明する。

【００７１】

図１６は，監視サーバにより時刻差が近接しているとしてグルーピングされたインスタンスB,C,Eのログの例を示す図である。この例では，インスタンスEのログE5が転送漏れにより監視漏れログになっている。したがって，監視サーバは，インスタンスEのログE5が監視漏れログであり，その発生時刻13:58におけるインスタンスB,Cの負荷値を参照して，負荷値が最も低いインスタンスを選択する。図１６の例では，インスタンスBが最も負荷値が低く転送漏れが発生した確率が最も低いインスタンスとして選択される。負荷値には，例えばCPU利用率，メモリ使用量が含まれ，これらの値が低いインスタンスは，転送漏れによる監視漏れが発生していないと推定できる。

【００７２】

（３）図１３の３つの処理のうち第３の処理では，監視サーバは，転送漏れによる転送遅延の発生確率が最も低かったインスタンスのログから，監視漏れログと最も発生時刻が近いログを選択する（S163)。図１６の例で説明すると，監視サーバは，負荷が低く転送漏れによる転送遅延の発生確率が最も低かったインスタンスBのログから，監視漏れログE5の発生時刻13:58と同じ発生時刻を有するログB8を選択する。これで，監視サーバは，図１０の処理S16のイベントログ管理DB内の，転送遅延の発生確率が最も低かった他のインスタンスのログのうち，監視漏れログE5の発生時刻と最も近い発生時刻を有するログB8を特定することができた。

【００７３】

そして，図１０に戻り，監視サーバは，処理S16で特定したログの収集時刻を，監視漏

れ発生時刻と特定する（S17)。図１６の例で説明すると，監視サーバは，特定したログB8の収集時刻13:59を，監視漏れログE5の転送漏れによる監視漏れ発生時刻と推定する。

【００７４】

前述の図１３の第１の処理S161では，図１５で説明したとおり，複数のインスタンスのうち監視漏れログのインスタンスと転送間隔が同じまたは近接するインスタンスを選択してグルーピングした。この処理S161で，監視サーバは，転送間隔が同じまたは近接するインスタンスとして，監視漏れログのインスタンスと同程度に短い転送間隔のインスタンスを選択することが望ましい。すなわち，そもそも監視漏れログを検出して監視漏れ発生時刻を特定するのは，そのインスタンスのログ収集の緊急性またはリアルタイム性が高いからである。そして，ログ収集の緊急性が高いインスタンスには，一般に短い転送間隔が設定される。転送間隔が長いと，ログの発生から収集まで最悪長時間を要する場合があるからである。

【００７５】

したがって，監視漏れ発生時刻を特定すべきインスタンスは，転送間隔が十分に短いので，上記処理S161で転送漏れが発生したインスタンスと転送間隔が近いインスタンスとは，転送間隔が長いインスタンスを排除して，同等の短い転送間隔を有するインスタンスを意味する。

【００７６】

以上で図９の監視漏れ発生時刻の特定処理S1が完了した。図２の例で説明すると，図２ではログA1が監視漏れログであり，そのインスタンスAと転送間隔が近接し監視漏れログA1の発生時刻13:22において負荷が最も軽かったインスタンスがインスタンスBであるとすると，そのインスタンスのログB1が監視漏れログA1の発生時刻と近接している。したがって，ログB1の収集時刻13:32が転送漏れによる監視漏れが発生した時刻と推定される。

【００７７】

図１７は，監視漏れ発生時刻の特定処理S1により特定された監視漏れ発生時刻の例を示す図である。図１７のインスタンスA,Bが発生するログA1,A2,B1,B2は図２の例と同じである。但し，図２と異なり，インスタンスAでは，負荷集中による転送遅延が，転送時刻13:30と13:40で発生している。この場合は，監視サーバは，監視漏れ発生時刻の特定処理S1により，監視漏れログA1に対する監視漏れ発生時刻をログB1の収集時刻13:32と推定し，監視漏れログA2に対する監視漏れ発生時刻をログB2の収集時刻13:40と推定する。その結果，監視サーバは，監視漏れ発生時間帯を，時刻13:32から13:42と推定する。

【００７８】

［図９の監視漏れパターンの構築処理S2］

監視サーバ３０は，CPUが監視プログラム３０４を実行することにより，特定した監視漏れ発生時刻前後におけるインスタンスの数やインスタンスの性能情報（負荷値など）の推移データを監視漏れパターンとして監視漏れパターンDB内に格納する（S2)。

【００７９】

図１８は，監視漏れパターンの構築処理S2のフローチャート図である。監視サーバは，CPUにより監視プログラムを実行して，監視漏れ発生時刻の前後におけるサービスシステムのインスタンス数と，各インスタンスの負荷値の推移情報とを，イベントログ管理DBと性能情報管理DBから抽出する（S21)。そして，監視サーバは，抽出したインスタンス数と，各インスタンスの負荷値の推移情報を，監視漏れパターンとして，監視漏れパターンDBに格納する（S22)。

【００８０】

図１９は，監視漏れパターンの例を示す図である。監視サーバは，監視漏れログ毎に，監視漏れパターンを監視漏れパターンDBに格納する。図１８に示した管理漏れパターン例は，サービスシステムを構成するインスタンスA,Bのインスタンス数「２」と，監視漏れ発生時刻と，監視漏れログを発生した発生元インスタンス「A」と，インスタンスA,Bの負荷値の監視漏れ発生時刻前の５分間の推移データとを有する。負荷値は，例えばCPU使用率，メモリ使用量，イベント発生数，ネットワーク転送量の４種類であり，図１９にはそ

のいずれかが示されている。図１９に示された例によれば，インスタンスAは負荷値が急増しているが，インスタンスBは負荷値が低下している。

【００８１】

以上で，監視サーバは，図９の監視漏れパターンの構築処理S2を終了した。図８を参照して再度説明すると，監視サーバ３０の監視漏れパターン生成部３１５は，監視漏れ発生時刻特定部３１４が特定した監視漏れ発生時刻に基づいて(図８中(6)参照），その監視漏れ発生時刻前後の性能情報管理DBを抽出して，監視漏れパターンを生成し，監視漏れパターンDB３０６に格納する（図８中(8))。

【００８２】

次に，監視サーバは，過去に収集したログを分析することにより蓄積した監視漏れパターンを利用して，今後の監視対象のサービスシステムのインスタンスの性能情報の推移について，監視漏れパターンとの一致度を監視しながら，監視漏れ発生の予兆を検出する。それが，図９の監視漏れ発生の予兆検出と個別ポーリングの処理S3である。

【００８３】

［図９の監視漏れ発生の予兆検出と個別ポーリング処理S3］

監視サーバは，CPUにより監視プログラムを実行することで，監視漏れパターンによる予兆検出を行う。すなわち，監視サーバは，毎回の監視用ポーリングが終了したタイミングで，一定時間前の過去の時刻から最新時刻までの負荷値の推移パターンと，監視漏れパターンDB内の監視漏れパターンとの一致度を比較し，一致度が高い監視漏れパターンの監視漏れログの発生元インスタンスのパターンと一致するインスタンスに，監視漏れ発生の予兆があることを検出する。

【００８４】

図２０は，図９の監視漏れ発生の予兆検出と個別ポーリング処理S3のフローチャート図である。監視サーバは，監視対象のサービスシステムを構成するインスタンスのイベントログと性能情報ログを収集し続けている。そして，監視サーバは，毎回の監視ポーリングが終了したタイミングで図２０の処理を実行する。

【００８５】

まず，監視サーバは，監視漏れパターンDBから，現在監視中のサービスシステムのインスタンス数と一致する監視漏れパターン群を選択する（S31)。サービスシステムのインスタンス数に依存して監視漏れが発生する場合と発生しない場合があるので，インスタンス数に基づいて比較対象の監視漏れパターン群を絞り込むことが望ましい。ただし，インスタンス数が一致しなくても近接する数の監視漏れパターンを選択するようにしてもよい。

【００８６】

次に，監視サーバは，選択した監視漏れパターン群から，１つの監視漏れパターンを選択する（S32)。そして，選択する監視漏れパターンが存在している場合は（S33のNO)，監視サーバは，イベントログ管理DBと性能情報管理DB内の監視中の最新データ，即ち各インスタンスの負荷値の最新データと，選択した監視漏れパターンとの一致度を検出する（S34)。つまり，最新の負荷値の推移データと，監視漏れパターン内の負荷値の推移データとの一致度を，公知の一致度算出方法により検出する。したがって，各インスタンスの負荷値の最新データを収集するために，性能情報ログをある程度短い間隔で転送及び収集することが望ましい。

【００８７】

そして，監視サーバは，選択した監視漏れパターンの全てのインスタンスの負荷値の推移データが，監視中のサービスシステムの全てのインスタンスの最新の負荷値の推移データと一致するか否かチェックする（S35)。このチェックは，負荷値が３種類あれば，全ての負荷値で一致することを要する。そして，全ての負荷値についてそれぞれ全てのインスタンスの推移データが一致することが検出されると（S35のYES)，監視サーバは，監視漏れパターンの監視漏れ元インスタンスと，推移データが一致したインスタンスを特定し，そのインスタンスについて個別ポーリングを実行する（S36)。上記の処理S32-S36は，選択した監視漏れパターン群全てについて実施した後に，終了する（S33のYES)。

【００８８】
図２１は，監視漏れ発生の予兆検出における監視漏れパターンと監視中の負荷値の推移データとの一致を説明する図である。図２１中，処理S32で監視漏れパターン群から選択された１つの監視漏れパターン５０は，３つの負荷値の推移データ５０－１，５０－２，５０－３を有し，それぞれ３つのインスタンスA,B,Cの負荷値の推移データを有する。一方，監視中のサービスシステムについての負荷値の推移データ６０も，３つの負荷値の推移データ６０－１，６０－２，６０－３を有し，それぞれ３つのインスタンスA,B,Cの負荷値の推移データを有する。図２１の例では，負荷値は，CPU使用率，メモリ使用量，ネットワーク転送量である。
【００８９】
監視サーバは，監視漏れパターン５０のうち一つの負荷値についての監視漏れパターン５０－１と，監視中の同じ負荷値の推移データ６０－１との一致度を検出する。図２１の例では，監視漏れパターン５０と監視中の負荷値の推移データ６０－１とが一致している。同様に，監視サーバは，監視漏れパターン５０－２，５０－３についても，それぞれ監視中の負荷値の推移データ６０－２，６０－３との一致度を検出する。そして，監視サーバは，３つの負荷値について全て一致度が高かった（一致した）場合に，監視漏れ発生の予兆を検出する。以上が，図２０の処理S32からS35までに対応する。
【００９０】
そして，監視漏れ発生の予兆を検出すると，監視サーバは，監視漏れパターンの監視漏れ元インスタンスと，推移データが一致したインスタンスを特定し，その特定したインスタンスに対して個別ポーリングを行う。
【００９１】
図２２は，本実施の形態において監視漏れ発生の予兆を検出した場合の個別収集を示す図である。図２２のインスタンスA,Bは，それぞれログA1,A2,A3，ログB1,B2,B3を生成し，インスタンスAが負荷集中で時刻13:30と13:40で転送漏れを生じ転送遅延になっている。図２２の例は，図１７の例とはログA3,B3が発生していることを除いて同じである。そして，図２２の例では，時刻13:50で転送を行っている。その結果，保守情報記憶装置１４内のログDBには，図示されるログが転送されている。
【００９２】
図２２の例では，監視サーバが，インスタンスAに監視漏れ発生の予兆を検出した例であり，監視サーバは，収集時刻13:32，13:42，13:52で，インスタンスAに対して個別収集のポーリングを実行する。その結果，監視サーバは，収集時刻13:32，13:42ではインスタンスAのログを収集できないが，収集時刻13:52で，ログA3を一括収集と個別収集で重複して収集するとともに，インスタンスAの個別収集により転送遅延になったログA1,A2を収集する。収集時刻13:52で前回の収集時刻より前に発生しているログA1,A2を収集したので，監視サーバは，次回以降の収集時刻では，インスタンスAへの個別収集を停止し，通常の監視ポーリングのみで収集を行う。
【００９３】
図８で以上の処理を再度説明すると，監視サーバ３０の監視漏れ予兆検知部３１３が，管理漏れパターン３０６と性能情報管理DB３０５内の性能データの推移データとの一致度を監視し（図８の(9)），監視漏れの予兆が検出されたら，監視サーバ３０の個別収集部３１６が，そのインスタンスに対して個別収集を実行する（図８の(10)(11)）。この個別収集により転送漏れにより転送遅延していたログを収集することができる。
【００９４】
以上のとおり，本実施の形態によれば，収集したログに基づいて監視漏れ発生時刻を高精度に推定することができる。その結果，監視漏れ発生時刻前後のサービスシステムを構成するインスタンスの性能情報の推移データを利用して，将来，監視中のサービスシステムのインスタンスにおける監視漏れ発生の予兆を検出して，予兆が検出されたインスタンスに個別ポーリングを実行して転送遅延したログを実質的にリアルタイムに収集することができる。

【符号の説明】

【００９５】

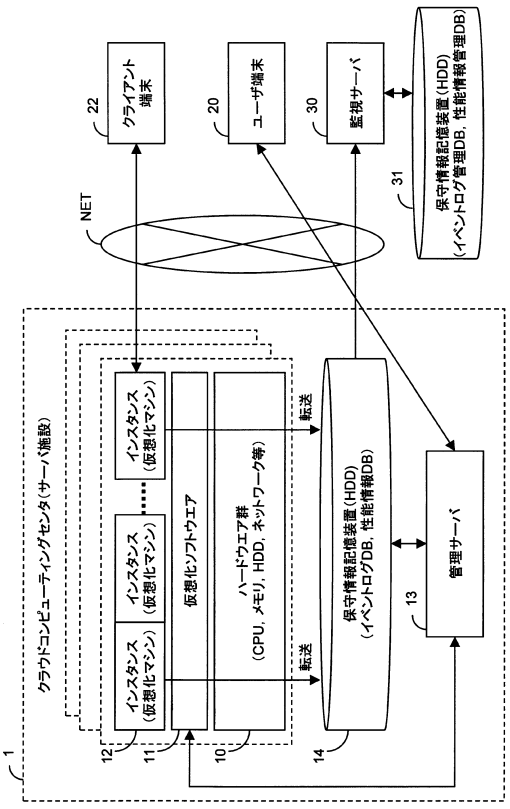
１２：インスタンス（仮想化マシン，仮想デバイス，物理マシン，物理デバイス，被監視デバイス）

１４：第１のデータベース，ログDB（第１のログ項目蓄積装置）

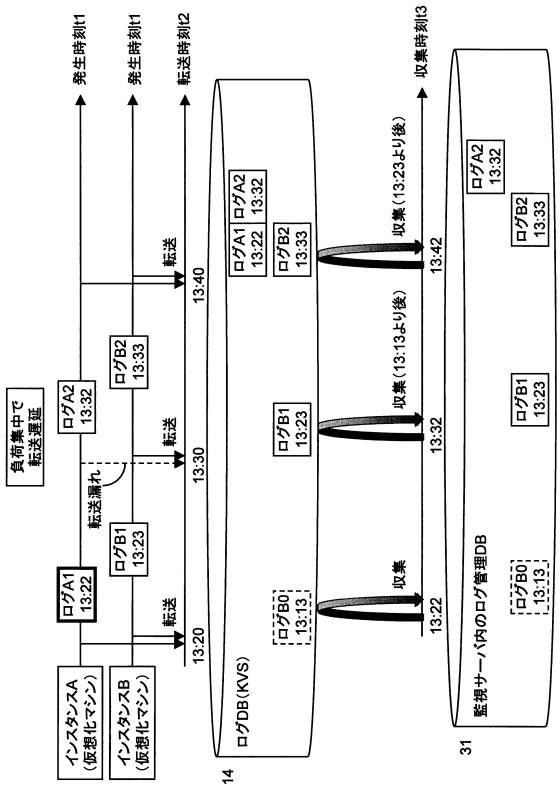
３０：監視サーバ

３１：第２のデータベース，ログ管理DB（第２のログ項目蓄積装置）

【図１】



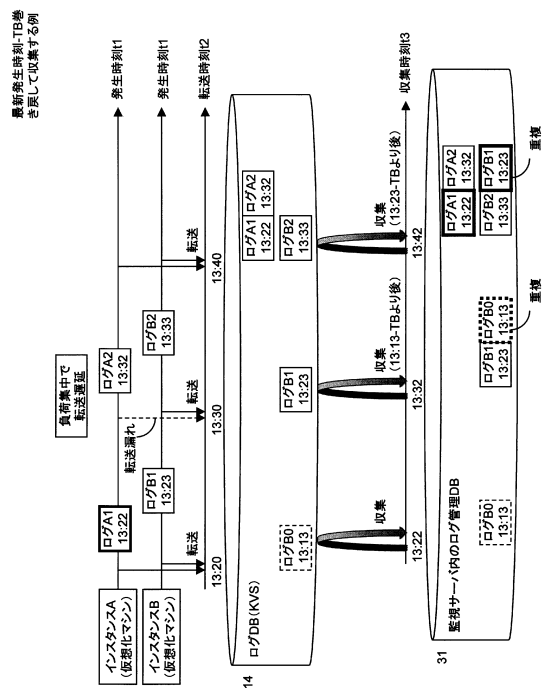
【図２】



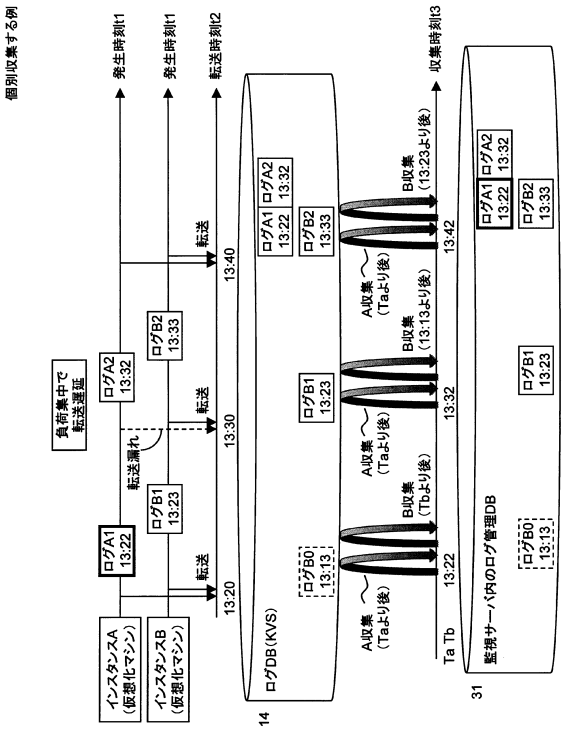
【図３】


ログA1
13:22
KEY
VALU_1
VALU_2
発生時刻
イベント内容
インスタンス
ID

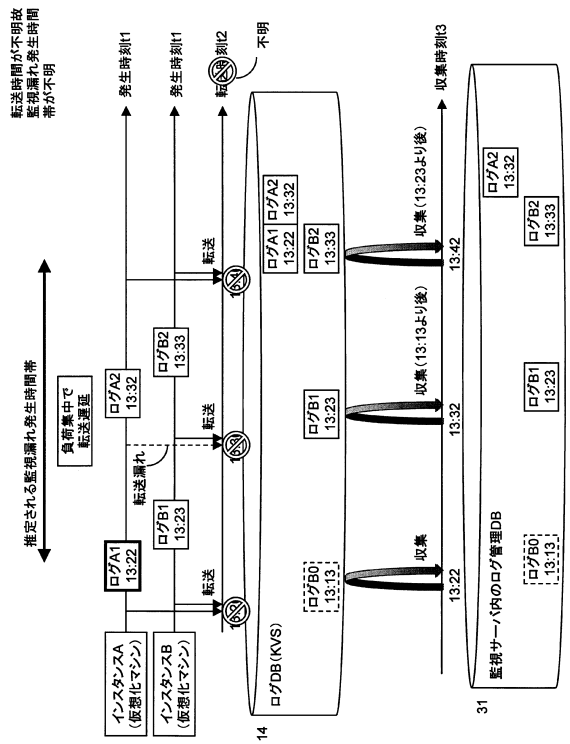
【図４】


最新発生時刻-TB巻き戻して収集する例
発生時刻t1
発生時刻t1
転送時刻t2
収集時刻t3
負荷集中で転送遅延
転送漏れ
転送
収集
重複
インスタンスA（仮想化マシン）
インスタンスB（仮想化マシン）
ログDB(KVS)
監視サーバ内のログ管理DB
14
31

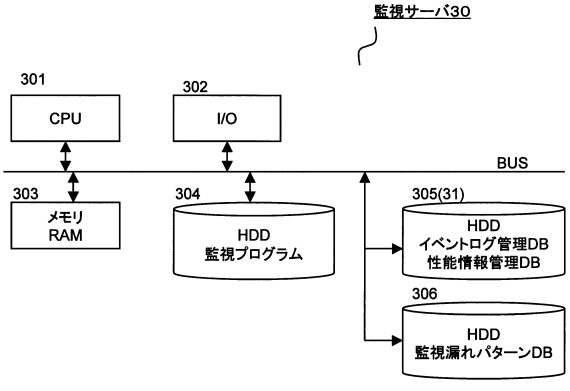
【図５】


個別収集する例
発生時刻t1
発生時刻t1
転送時刻t2
収集時刻t3
負荷集中で転送遅延
転送漏れ
転送
A収集（Taより後）
B収集（Tbより後）
B収集（13:13より後）
B収集（13:23より後）
インスタンスA（仮想化マシン）
インスタンスB（仮想化マシン）
ログDB(KVS)
監視サーバ内のログ管理DB
14
31

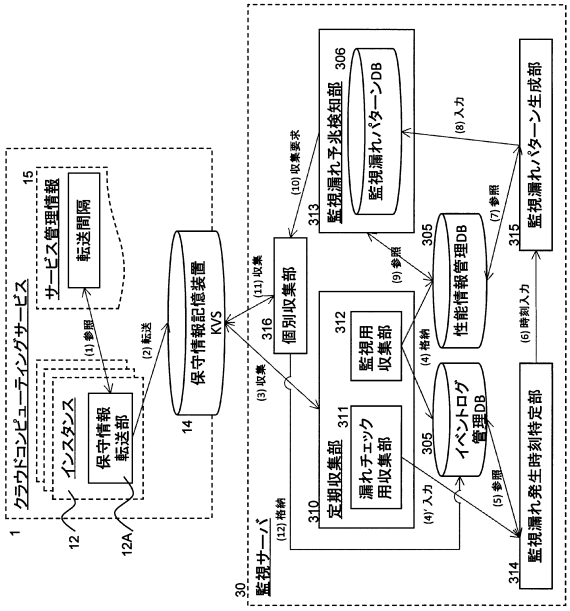
【図６】


転送時間が不明故監視漏れ発生時間帯が不明
推定される監視漏れ発生時間帯
発生時刻t1
発生時刻t1
転送時刻t2
不明
収集時刻t3
負荷集中で転送遅延
転送漏れ
転送
収集（13:23より後）
収集（13:13より後）
収集
インスタンスA（仮想化マシン）
インスタンスB（仮想化マシン）
ログDB(KVS)
監視サーバ内のログ管理DB
14
31

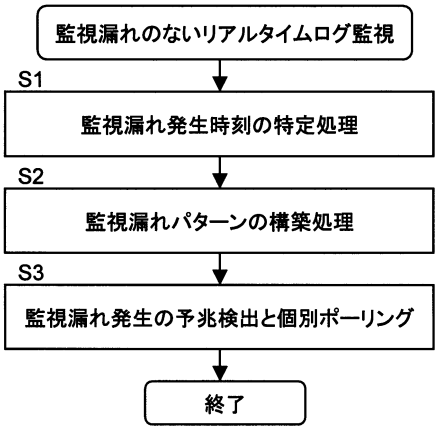
【図７】


監視サーバ30
301
CPU
302
I/O
BUS
303
メモリ
RAM
304
HDD
監視プログラム
305(31)
HDD
イベントログ管理DB
性能情報管理DB
306
HDD
監視漏れパターンDB

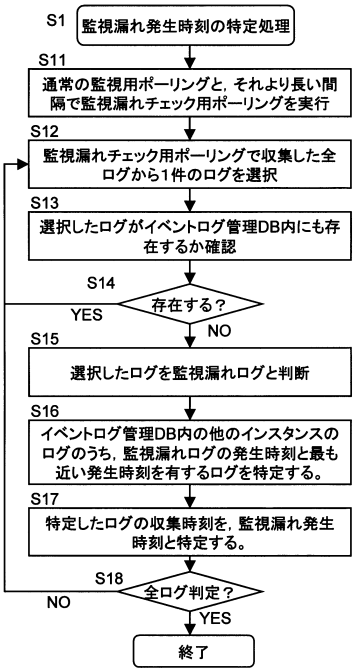
【図８】



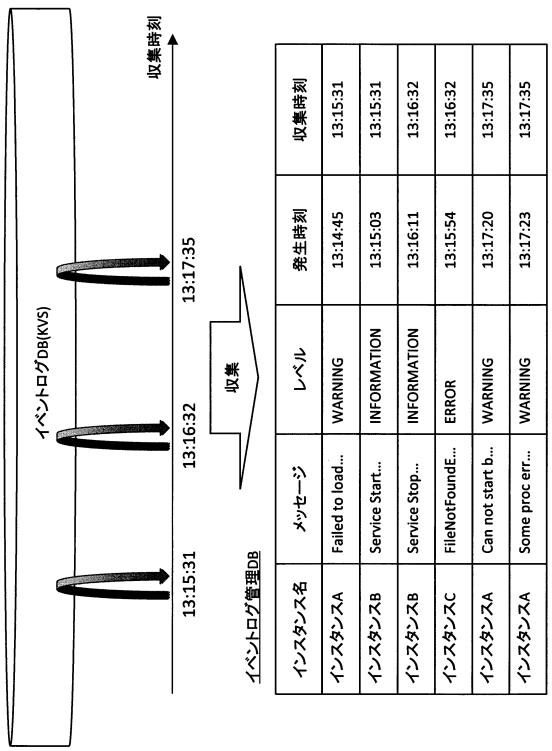
【図９】



【図１０】

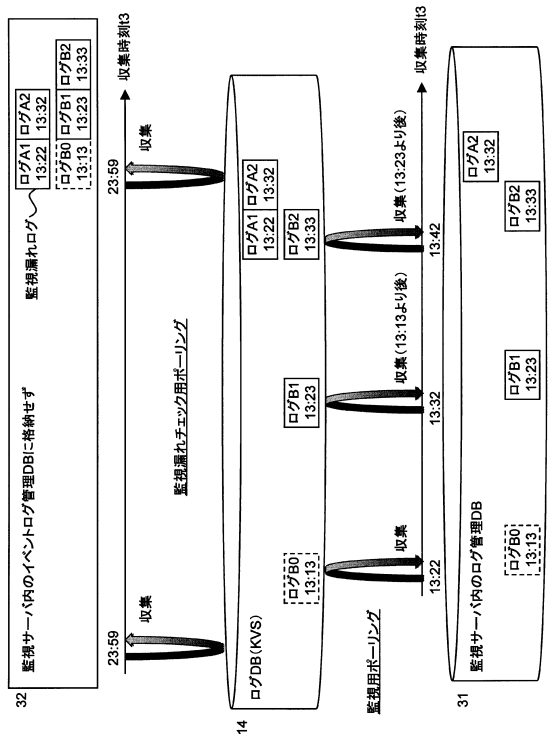


【図１１】

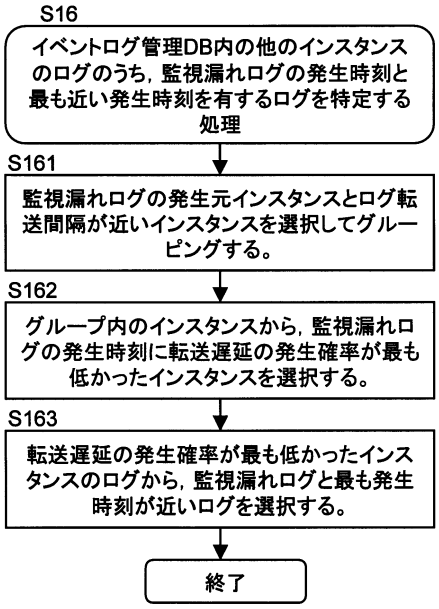


インスタンス名	メッセージ	レベル	発生時刻	収集時刻
インスタンスA	Failed to load...	WARNING	13:14:45	13:15:31
インスタンスB	Service Start...	INFORMATION	13:15:03	13:15:31
インスタンスB	Service Stop...	INFORMATION	13:16:11	13:16:32
インスタンスC	FileNotFoundE...	ERROR	13:15:54	13:16:32
インスタンスA	Can not start b...	WARNING	13:17:20	13:17:35
インスタンスA	Some proc err...	WARNING	13:17:23	13:17:35

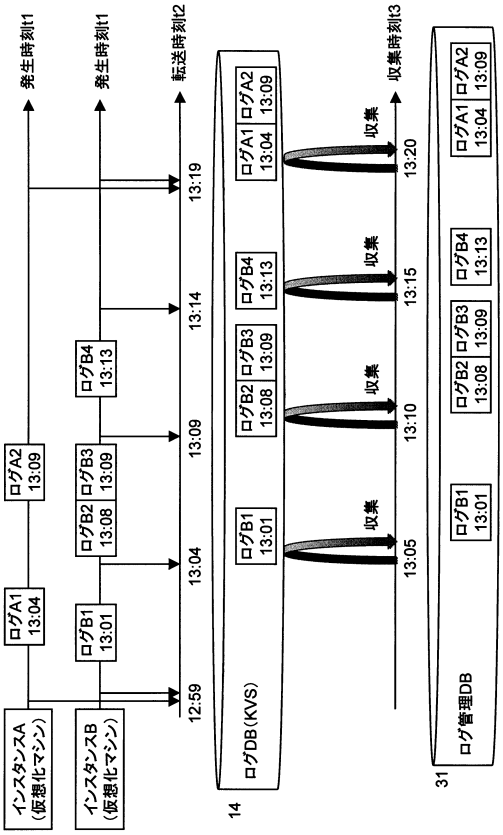
【図１２】



【図１３】



【図１４】

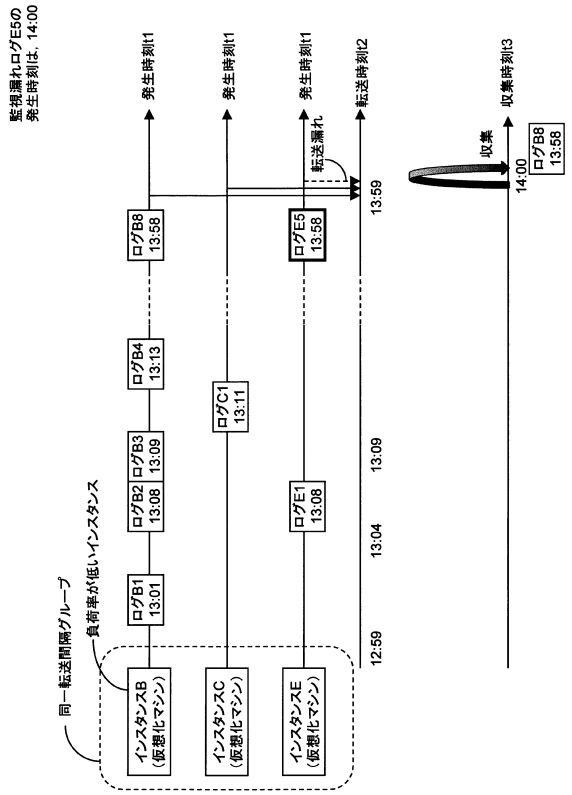


【図１５】

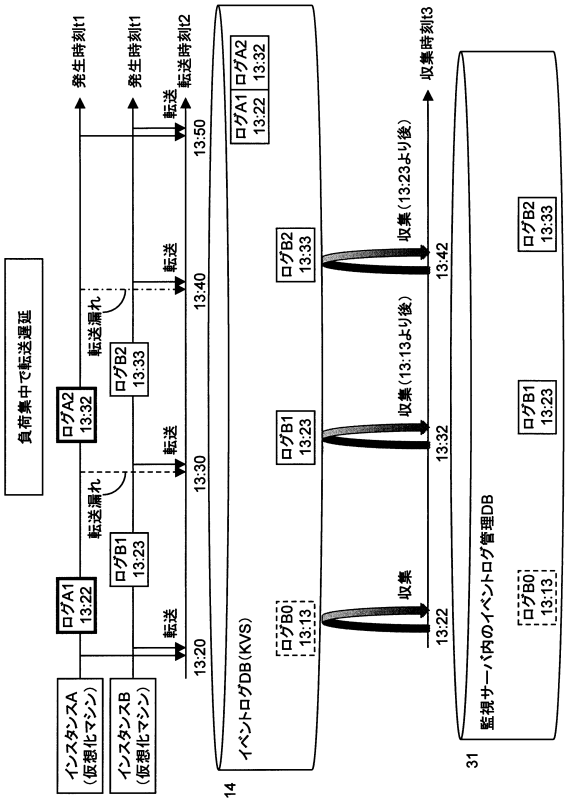
ログ収集時刻－ログ発生時刻の平均値表

インスタンス	ログ発生時刻	ログ収集時刻	時刻差	時刻差平均
A	13:04	13:20	00:16	00:13:30
A	13:09	13:20	00:11	
B	13:01	13:05	00:04	00:02:15
B	13:08	13:10	00:02	
B	13:09	13:10	00:1	
B	13:13	13:15	00:2	
C	----	----	----	00:02:30
D	----	----	----	00:14:15
E（漏れログ）	----	----	----	00:02:20

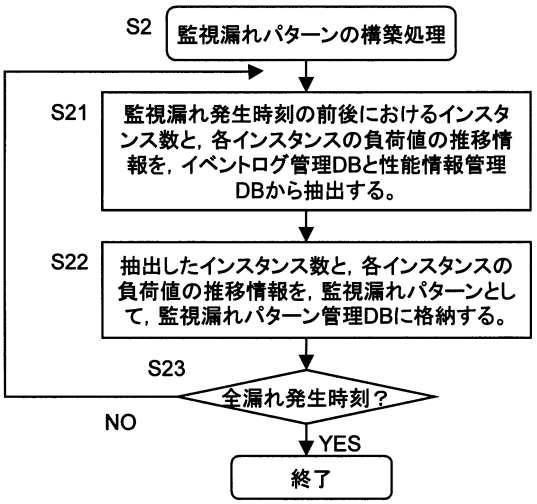
【図１６】



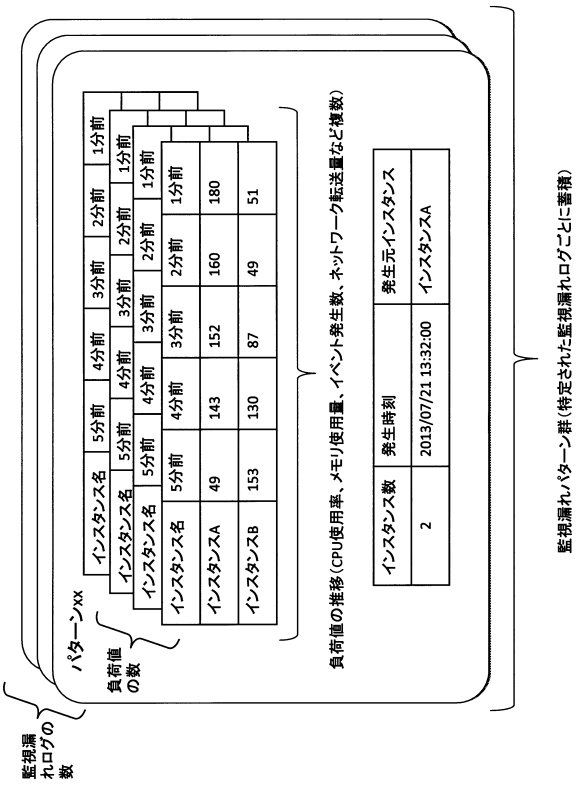
【図１７】



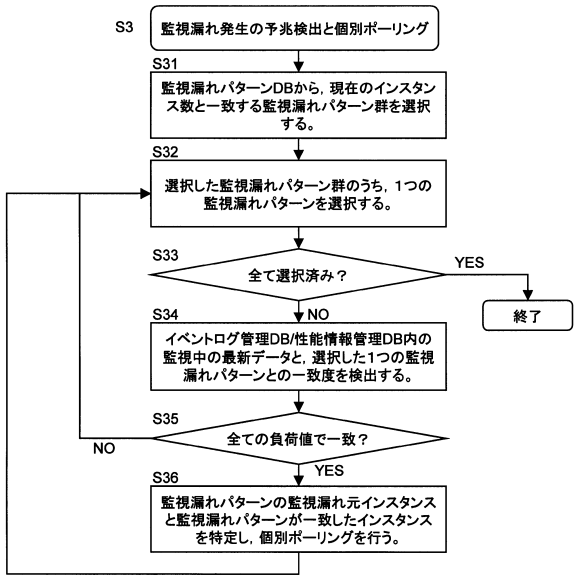
【図１８】



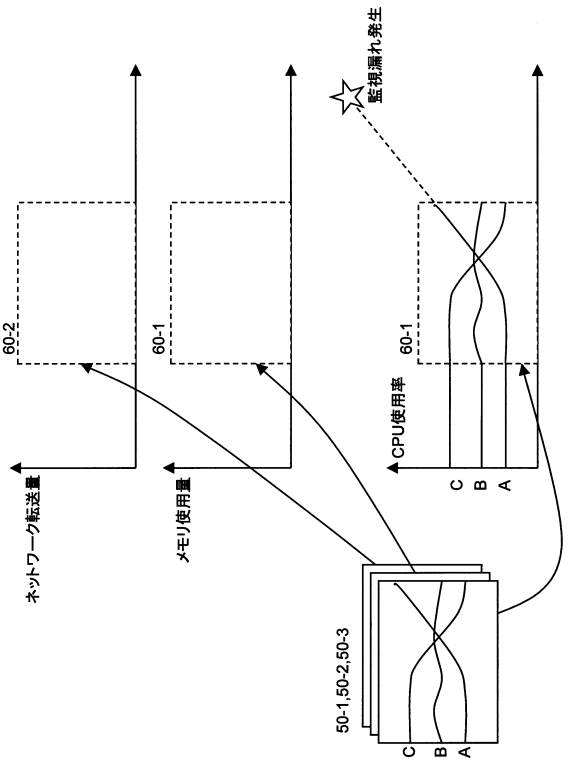
【図１９】



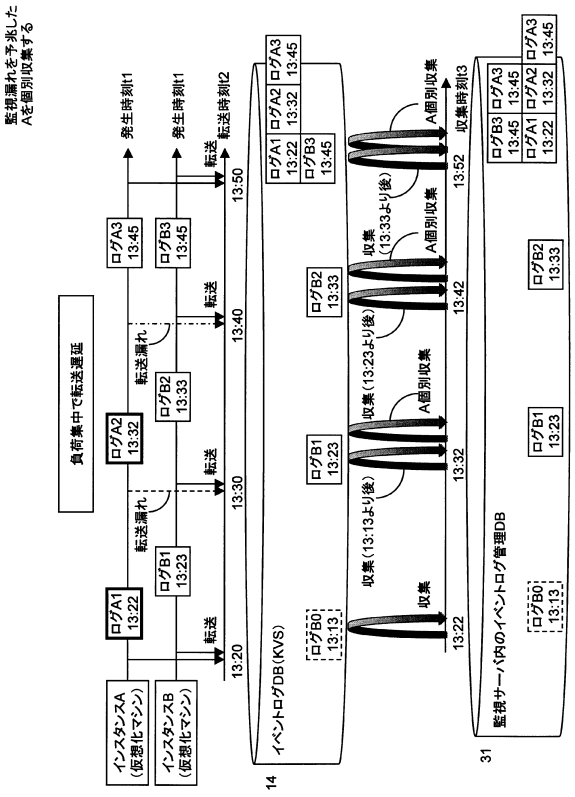
【図２０】


S3
監視漏れ発生の予兆検出と個別ポーリング
S31
監視漏れパターンDBから，現在のインスタンス数と一致する監視漏れパターン群を選択する。
S32
選択した監視漏れパターン群のうち，1つの監視漏れパターンを選択する。
S33
全て選択済み？
YES
終了
NO
S34
イベントログ管理DB/性能情報管理DB内の監視中の最新データと，選択した1つの監視漏れパターンとの一致度を検出する。
S35
全ての負荷値で一致？
NO
YES
S36
監視漏れパターンの監視漏れ元インスタンスと監視漏れパターンが一致したインスタンスを特定し，個別ポーリングを行う。

【図２１】


監視漏れ発生
60-2
60-1
60-1
CPU使用率
C
B
A
ネットワーク転送量
メモリ使用量
50-1,50-2,50-3
C
B
A

【図２２】


監視漏れを予兆したAを個別収集する
負荷集中で転送遅延
発生時刻t1
発生時刻t1
転送時刻t2
収集時刻t3
ログA3 13:45
ログB3 13:45
ログB2 13:33
ログA2 13:32
ログB1 13:23
ログA1 13:22
ログB0 13:13
転送
転送漏れ
13:50
13:40
13:30
13:20
インスタンスA（仮想化マシン）
インスタンスB（仮想化マシン）
イベントログDB(KVS)
14
収集
収集（13:13より後）
収集（13:23より後）
収集（13:33より後）
A個別収集
13:52
13:42
13:32
13:22
監視サーバ内のイベントログ管理DB
31

フロントページの続き

(72)発明者　長谷尾　慎司
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

審査官　安藤　一道

(56)参考文献　特開２０１３－０７３４９７（ＪＰ，Ａ）
特開２００５－１１５７２４（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　１３／００
Ｇ０６Ｆ　１１／３４
Ｇ０６Ｑ　５０／１０