

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第5458308号
(P5458308)

(45) 発行日 平成26年4月2日(2014.4.2)

(24) 登録日 平成26年1月24日(2014.1.24)

| | | | | | |
|-------------------|------------------|------------|-----|---|--|
| (51) Int. Cl. | | F I | | | |
| G06F 11/30 | (2006.01) | G06F 11/30 | | A | |
| G06F 9/46 | (2006.01) | G06F 9/46 | 350 | | |
| G06F 11/34 | (2006.01) | G06F 11/34 | | B | |

請求項の数 15 (全 42 頁)

| | | | |
|-----------|-------------------------------|-----------|---------------------|
| (21) 出願番号 | 特願2010-133708 (P2010-133708) | (73) 特許権者 | 000005108 |
| (22) 出願日 | 平成22年6月11日 (2010.6.11) | | 株式会社日立製作所 |
| (65) 公開番号 | 特開2011-258098 (P2011-258098A) | | 東京都千代田区丸の内一丁目6番6号 |
| (43) 公開日 | 平成23年12月22日 (2011.12.22) | (74) 代理人 | 100114236 |
| 審査請求日 | 平成25年2月20日 (2013.2.20) | | 弁理士 藤井 正弘 |
| | | (74) 代理人 | 100075513 |
| | | | 弁理士 後藤 政喜 |
| | | (74) 代理人 | 100120260 |
| | | | 弁理士 飯田 雅昭 |
| | | (72) 発明者 | 森木 俊臣 |
| | | | 東京都国分寺市東恋ヶ窪一丁目280番地 |
| | | | 株式会社日立製作所 中央研究所内 |
| | | (72) 発明者 | 保田 淑子 |
| | | | 東京都国分寺市東恋ヶ窪一丁目280番地 |
| | | | 株式会社日立製作所 中央研究所内 |
| | | | 最終頁に続く |

(54) 【発明の名称】 仮想計算機システム、仮想計算機システムの監視方法及びネットワーク装置

(57) 【特許請求の範囲】

【請求項1】

クライアント計算機に接続されたネットワーク装置と、
前記ネットワーク装置に接続されて前記クライアント計算機にサービスを提供するサーバ計算機と、
前記ネットワーク装置とサーバ計算機に接続された性能低下要因特定装置と、を備え、
前記サーバ計算機は、
演算を行うプロセッサと、
情報を格納する記憶部と、
前記ネットワーク装置に接続されるネットワークインタフェースと、
前記サーバ計算機の物理資源を仮想化する仮想化部と、
前記仮想化された物理資源上でOS及び前記サービスを提供するアプリケーションを稼働させる複数の仮想マシンと、を有し、
前記ネットワーク装置は、
前記クライアント計算機からの処理要求を前記仮想マシンに転送し、当該処理要求に対する処理応答を前記仮想マシンから受信して前記クライアント計算機に転送し、前記性能低下要因特定装置から設定された監視条件を満たす通信について、前記処理要求の転送から前記処理要求に対する処理応答を転送するまでの遅延時間を監視し、前記遅延時間が所定の閾値を超えたときに、前記性能低下要因特定装置に遅延が増大したことを示す遅延通知を送信する遅延監視部を有し、

10

20

前記性能低下要因特定装置は、

前記ネットワーク装置が送受信する情報のうち、監視対象とする通信の前記監視条件と前記サーバ計算機と仮想マシンの対応関係を設定した通信フロー情報と、

前記サーバ計算機の計算機資源及び前記サーバ計算機に接続された計算機資源について前記仮想マシン間で共有する計算機資源を特定する共有資源情報と、

前記ネットワーク装置から前記遅延通知を受信したときに、前記通信フロー情報を参照して遅延が増大した仮想マシン及びサーバ計算機を特定する遅延増大特定部と、

前記共有資源情報を参照して前記遅延が増大した仮想マシンと計算機資源を共有する他の仮想マシンを抽出する情報収集範囲特定部と、

前記抽出された仮想マシン及びサーバ計算機と、前記遅延が増大した仮想マシン及びサーバ計算機について、物理的な計算機資源の性能情報と、仮想的な計算機資源の性能情報を取得して、前記遅延が増大した部位を特定する要因特定部と、

を備えたことを特徴とする仮想計算機システム。

【請求項 2】

請求項 1 に記載の仮想計算機システムであって、

前記クライアント計算機とネットワーク装置は、広域ネットワークを介して接続されたことを特徴とする仮想計算機システム。

【請求項 3】

請求項 2 に記載の仮想計算機システムであって、

前記ネットワーク装置は、

前記サーバ計算機と前記広域ネットワークに接続された第 1 のネットワーク装置と、

前記クライアント計算機と前記広域ネットワークに接続された第 2 のネットワーク装置と、を含み、

前記第 1 のネットワーク装置は、

前記性能低下要因特定装置から設定された監視条件を満たす通信について、前記処理要求の転送から前記処理要求に対する処理応答を転送するまでの遅延時間を監視し、前記遅延時間が予め設定された第 1 の閾値を超えたときに、前記性能低下要因特定装置に遅延が増大したことを示す遅延通知を送信する第 1 の遅延監視部を有し、

前記第 2 のネットワーク装置は、

前記性能低下要因特定装置から設定された監視条件を満たす通信について、前記処理要求の転送から前記処理要求に対する処理応答を転送するまでの遅延時間を監視し、前記遅延時間が予め設定された第 2 の閾値を超えたときに、前記性能低下要因特定装置に遅延が増大したことを示す遅延通知を送信する第 2 の遅延監視部を有することを特徴とする仮想計算機システム。

【請求項 4】

請求項 3 に記載の仮想計算機システムであって、

前記第 1 のネットワーク装置は、前記性能低下要因特定装置を含むことを特徴とする仮想計算機システム。

【請求項 5】

請求項 1 に記載の仮想計算機システムであって、

前記サーバ計算機の追加または削除を管理する管理計算機をさらに有し、

前記性能低下要因特定装置は、

前記管理計算機が前記サーバ計算機の変更を実施したときに、前記通信フロー情報と前記共有資源情報を前記サーバ計算機の変更に対応して更新することを特徴とする仮想計算機システム。

【請求項 6】

請求項 1 に記載の仮想計算機システムであって、

前記仮想マシンの追加または削除あるいは移動を管理する管理計算機をさらに有し、

前記性能低下要因特定装置は、

前記管理計算機が前記仮想マシンの変更を実施したときに、前記通信フロー情報と前記

10

20

30

40

50

共有資源情報を前記仮想マシンの変更に対応して更新することを特徴とする仮想計算機システム。

【請求項 7】

請求項 1 に記載の仮想計算機システムであって、

前記仮想化部は、

前記プロセッサを仮想化した仮想プロセッサを前記仮想マシンに割り当て、前記ネットワークインタフェースを仮想化した仮想ネットワークインタフェースを前記仮想マシンに割り当て、

前記プロセッサの性能情報を物理的なプロセッサの性能情報として取得し、前記仮想プロセッサの性能情報を仮想的なプロセッサの性能情報として取得するプロセッサ性能情報取得部と、

10

前記ネットワークインタフェースの性能情報を物理的なネットワークインタフェースの性能情報として取得し、前記仮想ネットワークインタフェースの性能情報を仮想的なネットワークインタフェースの性能情報として取得するネットワークインタフェース性能情報取得部と、を有し、

前記要因特定部は、

前記物理的な計算機資源の性能情報と仮想的な計算機資源の性能情報と、を前記プロセッサ性能情報取得部と前記ネットワークインタフェース性能情報取得部からそれぞれ取得することを特徴とする仮想計算機システム。

【請求項 8】

20

クライアント計算機に接続されたネットワーク装置と、前記ネットワーク装置に接続されて前記クライアント計算機にサービスを提供するサーバ計算機と、前記ネットワーク装置とサーバ計算機に接続された性能低下要因特定装置と、を備えた仮想計算機システムの監視方法であって、

前記サーバ計算機は、演算を行うプロセッサと、情報を格納する記憶部と、前記ネットワーク装置に接続されるネットワークインタフェースと、前記サーバ計算機の物理資源を仮想化する仮想化部と、前記仮想化された物理資源上で OS 及び前記サービスを提供するアプリケーションを稼働させる複数の仮想マシンと、を有し、

前記監視方法は、

前記性能低下要因特定装置が、前記ネットワーク装置に通信の監視条件を設定する第 1 のステップと、

30

前記ネットワーク装置が、前記クライアント計算機からの処理要求を前記仮想マシンに転送し、当該処理要求に対する処理応答を前記仮想マシンから受信して前記クライアント計算機に転送し、前記監視条件を満たす通信について、前記処理要求の転送から前記処理要求に対する処理応答を転送するまでの遅延時間を監視する第 2 のステップと、

前記ネットワーク装置が、前記遅延時間が所定の閾値を超えたときに、前記性能低下要因特定装置に対して遅延が増大したことを示す遅延通知を送信する第 3 のステップと、

前記性能低下要因特定装置が、前記ネットワーク装置から前記遅延通知を受信したときに、監視対象とする通信の前記監視条件と前記サーバ計算機と仮想マシンの対応関係を設定した通信フロー情報を参照して遅延が増大した仮想マシン及びサーバ計算機を特定する第 4 のステップと、

40

前記性能低下要因特定装置が、前記サーバ計算機の計算機資源及び前記サーバ計算機に接続された計算機資源について前記仮想マシン間で共有する計算機資源を特定する共有資源情報を参照して、前記遅延が増大した仮想マシンと計算機資源を共有する他の仮想マシンを抽出する第 5 のステップと、

前記性能低下要因特定装置が、前記抽出された仮想マシン及びサーバ計算機と、前記遅延が増大した仮想マシン及びサーバ計算機について、物理的な計算機資源の性能情報と、仮想的な計算機資源の性能情報を取得して、前記遅延が増大した部位を特定する第 6 のステップと、

を含むことを特徴とする仮想計算機システムの監視方法。

50

【請求項 9】

請求項 8 に記載の仮想計算機の監視方法であって、
前記クライアント計算機とネットワーク装置は、広域ネットワークを介して接続されたことを特徴とする仮想計算機システムの監視方法。

【請求項 10】

請求項 9 に記載の仮想計算機システムの監視方法であって、
前記ネットワーク装置は、前記サーバ計算機と前記広域ネットワークに接続された第 1 のネットワーク装置と、前記クライアント計算機と前記広域ネットワークに接続された第 2 のネットワーク装置と、を含み、

前記第 3 のステップは、

前記第 1 のネットワーク装置が、前記遅延時間が予め設定された第 1 の閾値を超えたときに、前記性能低下要因特定装置に対して遅延が増大したことを示す遅延通知を送信するステップと、

前記第 2 のネットワーク装置が、前記遅延時間が予め設定された第 2 の閾値を超えたときに、前記性能低下要因特定装置に遅延が増大したことを示す遅延通知を送信するステップと、

を含むことを特徴とする仮想計算機システムの監視方法。

10

【請求項 11】

請求項 10 に記載の仮想計算機システムの監視方法であって、

前記第 1 のネットワーク装置は、前記性能低下要因特定装置を含むことを特徴とする仮想計算機の監視方法。

20

【請求項 12】

請求項 8 に記載の仮想計算機システムの監視方法であって、

前記サーバ計算機の追加または削除を管理する管理計算機をさらに有し、

前記性能低下要因特定装置は、前記管理計算機が前記サーバ計算機の変更を実施したときに、前記通信フロー情報と前記共有資源情報を前記サーバ計算機の変更に対応して更新するステップをさらに含むことを特徴とする仮想計算機システムの監視方法。

【請求項 13】

請求項 8 に記載の仮想計算機システムの監視方法であって、

前記仮想マシンの追加または削除あるいは移動を管理する管理計算機をさらに有し、

前記性能低下要因特定装置は、前記管理計算機が前記仮想マシンの変更を実施したときに、前記通信フロー情報と前記共有資源情報を前記仮想マシンの変更に対応して更新するステップをさらに含むことを特徴とする仮想計算機システムの監視方法。

30

【請求項 14】

請求項 8 に記載の仮想計算機システムの監視方法であって、

前記仮想化部は、

前記プロセッサを仮想化した仮想プロセッサを前記仮想マシンに割り当て、前記ネットワークインタフェースを仮想化した仮想ネットワークインタフェースを前記仮想マシンに割り当て、前記プロセッサの性能情報を物理的なプロセッサの性能情報として取得し、前記仮想プロセッサの性能情報を仮想的なプロセッサの性能情報として取得するプロセッサ性能情報取得部と、前記ネットワークインタフェースの性能情報を物理的なネットワークインタフェースの性能情報として取得し、前記仮想ネットワークインタフェースの性能情報を仮想的なネットワークインタフェースの性能情報として取得するネットワークインタフェース性能情報取得部と、を有し、

40

前記第 6 のステップは、

前記性能低下要因特定装置が、前記物理的な計算機資源の性能情報と仮想的な計算機資源の性能情報と、を前記プロセッサ性能情報取得部と前記ネットワークインタフェース性能情報取得部からそれぞれ取得することを特徴とする仮想計算機システムの監視方法。

【請求項 15】

クライアント計算機とサービスを提供するサーバ計算機との間で送受信を行うネットワ

50

ーク装置であって、

前記サーバ計算機は、

前記サーバ計算機の物理資源を仮想化する仮想化部と、

前記仮想化された物理資源上でOS及び前記サービスを提供するアプリケーションを稼動させる複数の仮想マシンと、を有し、

前記ネットワーク装置は、

前記クライアント計算機からの処理要求を前記仮想マシンに転送し、当該処理要求に対する処理応答を前記仮想マシンから受信して前記クライアント計算機に転送する通信処理部と、

予め設定された監視条件を満たす通信について、前記処理要求の転送から前記処理要求に対する処理応答を転送するまでの遅延時間を監視し、前記遅延時間が所定の閾値を超えたときに、性能低下要因特定部に遅延が増大したことを示す遅延通知を送信する遅延監視部と、

前記性能低下要因特定部は、

前記通信処理部が送受信する情報のうち、監視対象とする通信の前記監視条件と前記サーバ計算機と仮想マシンの対応関係を設定した通信フロー情報と、

前記サーバ計算機の計算機資源及び前記サーバ計算機に接続された計算機資源について前記仮想マシン間で共有する計算機資源を特定する共有資源情報と、

前記遅延監視部から前記遅延通知を受信したときに、前記通信フロー情報を参照して遅延が増大した仮想マシン及びサーバ計算機を特定する遅延増大特定部と、

前記共有資源情報を参照して前記遅延が増大した仮想マシンと計算機資源を共有する他の仮想マシンを抽出する情報収集範囲特定部と、

前記抽出された仮想マシン及びサーバ計算機と、前記遅延が増大した仮想マシン及びサーバ計算機について、物理的な計算機資源の性能情報と、仮想的な計算機資源の性能情報を取得して、前記遅延が増大した部位を特定する要因特定部と、
を備えたことを特徴とするネットワーク装置。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、複数の仮想計算機で実行するサービスを、ネットワークを介して提供する仮想計算機システムにおいて、処理能力が低下した部位を特定する技術に関し、特に、クラウドコンピューティングを提供する仮想計算機システムの改良に関する。

【背景技術】

【0002】

経済のグローバル化と競争激化に伴い、企業は絶え間ない変革を求められている。企業活動を支えるITシステムにおいても、1～2ヵ月程度の超短期間でシステム構築とサービスの提供開始が要求されることも珍しくなくなっており、企業がITシステムを自社（インハウス）で構築して所有し続けるコストが重荷となっている。そこで、近年広帯域化が著しいワイドエリアネットワーク（WAN）を活用したサービスとして、ITシステムをデータセンタの事業者に出外して、企業は必要な期間のみ計算機資源を利用可能なクラウドコンピューティングが台頭している。

【0003】

クラウドコンピューティングが提供するサービスの形態は、提供するITリソースの柔軟度に応じて、IaaS（Infrastructure as a Service）、PaaS（Platform as a Service）、SaaS（Software as a Service）の3種類のクラウドサービスに大別される。IaaSは電力や設置場所、ネットワークバックボーン等のインフラを貸し出すクラウドサービスであり、PaaSはインフラに加えてIT機器のハードウェアと仮想マシンモニタ（Virtual Machine Monitor = VMM）、仮想マシン、OSまでをデータセンタ事業者が準備して、企業に仮想マシン（Virtual Machine）を貸し出すクラウドサービスである。SaaSは更に仮想マシンに加えて業務アプリケーションまでもデータセンタ事業

10

20

30

40

50

者が準備し、企業は時間貸しで業務アプリケーションを利用するサービス形態となる。

【0004】

グローバルで先行するクラウドベンダは、PaaSやSaaS相当のビジネスを行っている。これらのベンダのサービスは俗にパブリッククラウドと呼ばれ、インターネット経由でサービスが提供される。パブリッククラウドは非常に低価格かつ迅速なサービス提供開始が可能である一方、インターネットでの一時的な通信の混雑や切断が生じるため、エンドtoエンド(クライアントの端末から業務アプリケーション)での安定的なサービス提供が難しいという性質を有する。そのため信頼性に対する不安から、企業の中核的なITシステムに対してはパブリッククラウドの適用が進んでいない。

【0005】

一方、インターネットではなく、キャリアが提供する専用線、IP-VPN、広域イーサネット(登録商標)等の回線サービスを利用するWANサービスは、インターネットに比して信頼性及び通信品質が高く、企業の中核的なITシステムに適している。WANを利用したクラウドサービスとしては、PaaSに相当する仮想マシン単位でのサーバリソースの貸出を行うサービスが知られている(例えば、Harmonious Cloud(<http://www.hitachi.co.jp/products/it/harmonious/cloud/solution/paas.html>))。WANを用いたPaaSは、パブリッククラウドとは異なり高い信頼性を特長としており安定的なクラウドサービスの提供が可能である。

【0006】

WANとPaaSを組み合わせたクラウドサービス(以下、当該クラウドサービスという)では、通信インフラ(WAN、LAN)、サーバハードウェア、仮想マシン(または仮想サーバ)までをデータセンタ事業者がワンストップで提供し、顧客となる企業は仮想マシンで稼働させる業務アプリケーションを準備するのみで利用できる。当該クラウドサービスでは、顧客企業は拠点のクライアントからデータセンタ事業者と提携したキャリアのWANを介して、データセンタ内の仮想マシンにアクセスするものである。

【0007】

当該クラウドサービスでは、サービスを提供するWANやデータセンタ内のLAN機器、仮想マシンモニタ、物理計算機が複数の企業で共用されている。このため、ある企業で利用している業務アプリケーション等で処理能力低下等の問題が発生した場合に、処理能力が低下した部位を迅速に特定する必要がある。データセンタ事業者は問題の生じた部位に応じて、問題の生じた部位の運用管理を担当する部門に通知を行って業務の処理能力低下を回避または修復する。例えば、業務の処理能力低下の要因がWANであれば、事業者は提携先のキャリアに問題の発生を通知し、データセンタ内のLAN機器やVMMが業務の処理能力低下の要因であれば、データセンタのPaaSの運用管理部門に通知し、仮想マシン上の業務アプリケーション自体が業務の処理能力低下の要因であればデータセンタ事業者は業務アプリケーションを開発した顧客の企業に迅速に通知する必要がある。

【0008】

計算機システムにおいて処理能力低下の要因を特定する技術としては、特許文献1~4が知られている。

【0009】

特許文献1は、複数のキャリアでネットワークが構成される場合、キャリア間の中継ノードで通信品質を監視して利用者に通知を行うもので、WANの障害を検知することができる。

【0010】

特許文献2には、ネットワークと業務サーバ間で障害の切り分けを行う技術が開示され、データセンタ内のLANの障害やWANの障害を検知可能である。

【0011】

特許文献3には、仮想計算機を構成するVMMで物理サーバの性能情報を取得し、仮想マシンにエージェントを稼働させて仮想マシンの性能情報を取得する技術が開示され、仮想計算機内の処理能力低下の部位を特定することができる。

10

20

30

40

50

【 0 0 1 2 】

特許文献 4 には、サーバと LAN 機器を含む計算機システムにおいて、サーバで稼動するアプリケーション及びネットワークトラフィックの性能情報を収集し、収集した情報を多変量解析して、所定の相関関係に基づいて障害部位の推定を行う技術が開示される。

【 先行技術文献 】

【 特許文献 】

【 0 0 1 3 】

【 特許文献 1 】 特開 2 0 0 2 - 3 7 4 3 0 1 号公報

【 特許文献 2 】 特開 2 0 0 6 - 6 5 6 1 9 号公報

【 特許文献 3 】 米国特許出願公開第 2 0 0 9 / 0 2 4 9 9 4 号明細書

10

【 特許文献 4 】 特開 2 0 0 1 - 1 9 5 2 8 5 号公報

【 発明の概要 】

【 発明が解決しようとする課題 】

【 0 0 1 4 】

上記特許文献 1 では、WAN に起因する通信遅延増などの障害の検出が可能となる。しかし、特許文献 1 の技術では、データセンタ内の LAN 機器とサーバ、およびサーバ内部の OS や業務アプリケーションについて障害を検出することができない。

【 0 0 1 5 】

上記特許文献 2 では、データセンタ内の LAN 機器に起因する業務の処理能力低下などの障害を検出できる。しかし、特許文献 2 の技術では、VMM と仮想マシンのソフトウェア間のように、サーバ内部については障害が発生した部位を特定することはできない。

20

【 0 0 1 6 】

上記特許文献 3 では、エージェントを用いて VMM および仮想マシン上のゲスト OS の双方から性能監視情報を取得して、サーバ内部の障害が発生した部位を特定することができる。しかし、上記特許文献 3 では、サーバ外部の WAN や LAN が障害発生 of 要因を特定できない。

【 0 0 1 7 】

上記特許文献 4 では、サーバと LAN 機器を含む計算機システムから取得する性能監視情報を詳細化することで原理的には WAN ~ サーバ内部の任意の粒度で障害が発生した部位を特定することが可能である。しかしながら、上記特許文献 4 の技術をデータセンタの事業者が導入した場合、LAN 機器やサーバなど個別の機器から発生する大量の性能情報を予め収集して多変量解析を行う必要があり、障害が発生した部位を特定するまでに多大な時間を要し、迅速に障害発生 of 検出を行うことができない、という問題がある。

30

【 0 0 1 8 】

また、上記特許文献 1 ~ 3 を組み合わせた場合も、上記特許文献 4 と同様に、WAN ~ サーバ内部で障害が発生した部位を特定するためには、クラウドコンピューティングを構成する全ての機器から性能監視情報を取得して、解析を行う必要があるため多大な時間を要し、迅速に障害発生 of 検出を行うことができない、という問題がある。

【 0 0 1 9 】

特に、上述したクラウドコンピューティングのように、WAN を用いた PaaS の場合、データセンタの事業者は、障害が発生した部位が WAN であれば速やかにキャリアへ通知し、業務アプリケーションに障害が発生した場合は顧客企業へ速やかに通知する必要がある。無論、障害が発生した部位がデータセンタ内の LAN 機器や物理サーバまたは VMM、仮想マシンであれば、データセンタの事業者は速やかに機器運用管理担当者に通知を行って、修復を行う。このように WAN を用いた PaaS では、パブリッククラウドに比して高い信頼性を提供するために、障害が発生した部位を迅速に特定し、障害が発生した部位に応じて速やかに通知を行うことが安定したサービスを提供する要件となる。

40

【 0 0 2 0 】

そこで本発明は、上記問題点に鑑みてなされたもので、クラウドコンピューティングを構成する WAN と、データセンタ内の LAN 機器と、サーバの VMM と、VMM 上の仮想

50

マシンで発生する処理の遅延増大を検知し、かつ、遅延増大の要因となった部位を迅速に特定することで信頼性の高いサービスを提供することを目的とする。

【課題を解決するための手段】

【0021】

本発明は、クライアント計算機に接続されたネットワーク装置と、前記ネットワーク装置に接続されて前記クライアント計算機にサービスを提供するサーバ計算機と、前記ネットワーク装置とサーバ計算機に接続された性能低下要因特定装置と、を備え、前記サーバ計算機は、演算を行うプロセッサと、情報を格納する記憶部と、前記ネットワーク装置に接続されるネットワークインタフェースと、前記サーバ計算機の物理資源を仮想化する仮想化部と、前記仮想化された物理資源上でOS及び前記サービスを提供するアプリケーションを稼働させる複数の仮想マシンと、を有し、前記ネットワーク装置は、前記クライアント計算機からの処理要求を前記仮想マシンに転送し、当該処理要求に対する処理応答を前記仮想マシンから受信して前記クライアント計算機に転送し、前記性能低下要因特定装置から設定された監視条件を満たす通信について、前記処理要求の転送から前記処理要求に対する処理応答を転送するまでの遅延時間を監視し、前記遅延時間が所定の閾値を超えたときに、前記性能低下要因特定装置に遅延が増大したことを示す遅延通知を送信する遅延監視部を有し、前記性能低下要因特定装置は、前記ネットワーク装置が送受信する情報のうち、監視対象とする通信の前記監視条件と前記サーバ計算機と仮想マシンの対応関係を設定した通信フロー情報と、前記サーバ計算機の計算機資源及び前記サーバ計算機に接続された計算機資源について前記仮想マシン間で共有する計算機資源を特定する共有資源情報と、前記ネットワーク装置から前記遅延通知を受信したときに、前記通信フロー情報を参照して遅延が増大した仮想マシン及びサーバ計算機を特定する遅延増大特定部と、

前記共有資源情報を参照して前記遅延が増大した仮想マシンと計算機資源を共有する他の仮想マシンを抽出する情報収集範囲特定部と、前記抽出された仮想マシン及びサーバ計算機と、前記遅延が増大した仮想マシン及びサーバ計算機について、物理的な計算機資源の性能監視情報と、仮想的な計算機資源の性能監視情報を取得して、前記遅延が増大した部位を特定する要因特定部と、を備える。

【発明の効果】

【0022】

したがって、本発明は、仮想計算機システムを運用するデータセンタ内のネットワークと、サーバ計算機の仮想化部と、仮想マシンで発生する処理の遅延増大を検知し、かつ、遅延増大の要因となった部位を迅速に特定することができる。

【図面の簡単な説明】

【0023】

【図1】本発明の第1の実施形態を示し、WANを用いたクラウドサービスを提供する計算機システムの一部を示すブロック図である。

【図2】本発明の第1の実施形態を示し、業務サーバ115aの構成を示すブロック図である。

【図3】本発明の第1の実施形態を示し、ネットワーク監視サーバ118の構成を示すブロック図である。

【図4】本発明の第1の実施形態を示し、ネットワーク監視サーバ118が保持する通信フロー情報301の一例を示す説明図である。

【図5】本発明の第1の実施形態を示し、ネットワーク監視サーバ118が保持する共有資源情報302の一例を示す説明図である。

【図6】本発明の第1の実施形態を示し、顧客サイトからデータセンタの業務サーバで稼働するOSにアクセスする際の処理の遅延を示すタイムチャートである。

【図7】本発明の第1の実施形態を示し、ネットワーク監視サーバ118で実行される処理の一例を示すフローチャートである。

【図8】本発明の第1の実施形態を示し、ネットワーク監視端末119のディスプレイで遅延増大が発生した部位を表示するインターフェースの一例を示す画面イメージである。

10

20

30

40

50

【図9】本発明の第1の実施形態を示し、図8に示した遅延増大が発生した部位を特定する処理のシーケンス図である。

【図10A】本発明の第1の実施形態を示し、ネットワーク監視サーバの業務サーバ監視部とVM監視部及び情報更新処理部で行われる処理の一例を示すフローチャートの前半部である。

【図10B】本発明の第1の実施形態を示し、ネットワーク監視サーバの業務サーバ監視部とVM監視部及び情報更新処理部で行われる処理の一例を示すフローチャートの後半部である。

【図11】本発明の第2の実施形態を示し、業務サーバ115のブロック図である。

【図12】第3の実施形態を示し、ルータ1200のブロック図である。

10

【発明を実施するための形態】

【0024】

以下、本発明の一実施形態を添付図面に基づいて説明する。

【0025】

図1は、本発明の第1の実施形態を示し、WANを用いたクラウドサービスを提供する計算機システムの一例を示すブロック図である。

【0026】

クラウドサービスを提供するデータセンタ110は、広域ネットワーク（以下、WAN：Wide Area Network）150を介して顧客サイト101a、101b、101cに接続される。データセンタ110のクラウドサービスを利用する顧客サイト101aは、WAN150に接続されてパケットの送受信を行うルータ102aと、ルータ102aに接続されてデータセンタ110のクラウドサービスを受けるクライアント端末104aから構成される。他の顧客サイト101b、101cも同様にWAN150に接続されたルータ102b、102cとクラウドサービスを受けるクライアント端末104b、104cが接続される。なお、顧客サイト101a～101cは、同様の構成であるので、以下の説明では、顧客サイト101aのみについて説明し、他の顧客サイト101b、101cの説明を省略する。

20

【0027】

本実施形態では、WAN150からデータセンタ110の仮想マシンまでを顧客（顧客サイト）に貸し出すPaaS（Platform as a Service）の例を示し、顧客は仮想マシン上で所望の業務アプリケーションをインストールし、実行する。データセンタ110の事業者は、データセンタ110内のネットワークと、ハードウェア資源から仮想マシンまでの業務サーバを管理し、WAN150は通信事業者が管理し、仮想マシン上の業務アプリケーションは顧客が管理する例を示す。

30

【0028】

顧客サイト101aのルータ102aは、予め設定した監視条件に基づいて、クライアント端末104aからデータセンタ110あての処理要求を受信した時刻と、この処理要求に対してデータセンタ110が応答した処理結果を受信し、クライアント端末104aへ送信した時刻との差分を処理（または通信）の遅延時間として求め、この遅延時間が所定の閾値TH2を超えたときに処理（または通信）の遅延が増大したことを検出する遅延監視部103aを含む。遅延監視部103aは、管理用回線151を介してデータセンタ110のネットワーク監視サーバ118に接続される。そして、遅延監視部103aは、処理の遅延時間が、所定の閾値TH2を超えたときには、障害などにより処理の遅延の増大が発生したと判定し、ネットワーク監視サーバ118に対して遅延の増大が発生したことを通知する。なお、WAN150とは独立した管理用回線151を利用できない場合は、遅延監視部103aとネットワーク監視サーバ118をWAN150により接続することができる。なお、上記遅延時間は、クライアント端末104a～104cから観測したときの処理及び通信の遅延時間（応答時間）を示す。

40

【0029】

また、顧客サイト101aのクライアント端末104aは、プロセッサとメモリ及びス

50

トレージ装置を備えた計算機で構成され、ルータ102a及びWAN150を介してデータセンタ110からサービスを受ける。

【0030】

データセンタ110内には、WAN150に接続されたルータ(ネットワーク装置)120と、顧客サイト101aのクライアント端末104a等にサービスを提供する業務サーバ115a~115d(#1~#4)と、業務サーバ115a~115dとルータ120を接続する業務ネットワークを構成するL2(Layer 2)スイッチ114a、114bと、業務サーバ115a~115dとストレージ装置116を接続するSAN(Storage Area Network)と、管理ネットワークを構成する管理用スイッチ122a、122bに接続されて業務サーバ115a~115dの仮想化部211を管理する仮想化管理サーバ130と、管理LANネットワークを構成する管理用スイッチ122a、122bと管理用回線151に接続されて、処理の遅延増大を検知したときには、データセンタ110内の計算機資源から性能監視情報を収集して、遅延が増大した部位と、遅延増大の要因となった部位を特定してネットワーク監視端末119に通知するネットワーク監視サーバ118とを主体にして構成される。なお、仮想化部211は、ハイパーバイザやVMM(Virtual Machine Monitor)で構成することができる。

10

【0031】

WAN150に接続されるルータ120は、業務ネットワークのL2スイッチ114a、114bに接続されて、顧客サイト101a~101cから処理要求を受信し、処理要求に含まれる通信フロー情報からあて先となる業務サーバ115a~115dに処理要求を転送する。そして、ルータ120は、業務サーバ115a~115dが送信した処理結果を、当該処理結果に含まれる通信フロー情報からあて先となる顧客サイト101a~101cに処理結果を転送する。なお、通信フロー情報は、WAN150、業務ネットワークにTCP/IPを用いる場合には、あて先IPアドレス、ポート番号、発信元IPアドレスを含む情報である。

20

【0032】

また、ルータ120は、データセンタ110内部の処理の遅延の増大を検知してネットワーク監視サーバ118に通知する遅延監視部121を有する。遅延監視部121は、予め設定した監視条件に基づいて、顧客サイト101a~101cから受信した処理要求の時刻と、この処理要求に対して業務サーバ115a~115dが応答した処理結果の送信時刻と、所定の閾値TH1から、データセンタ110内における処理の遅延が増大したことを検出する。遅延監視部121は、処理要求の受信時刻と、処理結果の送信時刻の差が、所定時間である閾値TH1を超えたときには、データセンタ110内部で障害などによる遅延の増大が発生したと判定してネットワーク監視サーバ118に遅延の発生を通知する。

30

【0033】

ネットワーク監視サーバ118と遅延監視部121及び業務サーバ115a~115dはスイッチ122a、122bからなる管理ネットワークを介して接続される。ネットワーク監視サーバ118は、管理ネットワークを経由して遅延監視部121からの遅延増大の通知を受信し、管理用回線151を経由して顧客サイト101a~101cの遅延監視部103a~103cからの遅延増大の通知を受信する。また、ネットワーク監視サーバ118は、管理ネットワークを介して業務サーバ115a~115dに接続され、遅延の増大の発生が疑われる業務サーバ115a~115d及び仮想マシンから性能監視情報を収集する。

40

【0034】

ネットワーク監視サーバ118は、顧客サイト101a~101cのルータ102a~102cやデータセンタ110内のルータ120から遅延増大発生の通知を受信すると、複数の業務サーバ115a~115dのうち、遅延が発生した業務サーバ115a~115d及び仮想マシンを通信フロー情報から特定して、検査対象の物理サーバ(業務サーバ115a~115d)及び仮想マシンを絞り込む。そして、ネットワーク監視サーバ1

50

18は、遅延の増大発生が特定された業務サーバ115a～115d及び仮想マシンの性能監視情報を収集し、遅延増大の要因となった部位（性能低下要因）を特定する。特に、ネットワーク監視サーバ118は、遅延の増大が発生した部位が仮想マシンの場合には、当該仮想マシンと計算機資源を共有する他の仮想マシンの性能監視情報を収集して、遅延の増大の要因となった部位を性能低下要因として特定する。

【0035】

ネットワーク監視サーバ118は、上記特定した遅延増大が発生した部位と、遅延増大の要因となった部位をネットワーク監視端末119に通知する。ネットワーク監視端末119は、ネットワーク監視サーバ118から受信した通知から、遅延増大が発生した部位と、遅延増大の要因となった部位を、計算機システムの業務の処理能力が低下した要因として表示装置上に表示する。なお、遅延増大が発生した部位と、遅延増大の要因となった部位が同一の部位（例えば、仮想マシン）である場合と、遅延増大が発生した部位と、遅延増大の要因となった部位が異なる部位の場合が存在する。

10

【0036】

仮想化管理サーバ130はスイッチ122a、122bからなる管理ネットワークを介して業務サーバ115a～115dに接続される。仮想化管理サーバ130は、業務サーバ115a～115dの仮想化部211を管理して、仮想マシンの生成、削除や移動を実施する。また、本実施形態では、仮想化管理サーバ130が業務サーバ115a～115dの追加や削除を管理する。

【0037】

20

ストレージ装置116はSAN117に接続され、業務サーバ115a～115dがアクセスする論理ユニット（LU）#101、#102、#201を備える。なお、各LU#101～#201は、図6で示すように、ストレージ装置116内のRAIDグループの識別子に対応付けられていてもよい。

【0038】

なお、以下の説明では、顧客サイト101a～101cの総称を顧客サイト101とし、ルータ102a～102cの総称をルータ102とし、遅延監視部103a～103cの総称を遅延監視部103とし、クライアント端末104a～104cの総称をクライアント端末104とする。

【0039】

30

図2は、業務サーバ115aの構成を示すブロック図である。なお、業務サーバ115b～115dも同一の構成であるので、重複する説明は省略する。

【0040】

業務サーバ115aは、顧客サイト101に所定のサービスを提供する。業務サーバ115aは、ハードウェア資源210として、演算処理を行う物理CPU（または物理プロセッサ）222と、データやプログラム及び仮想化部や仮想マシンを格納するメモリ223と、複数の物理NIC（または物理ネットワークI/F）221と、SAN117に接続されるHBA（Host Bus Adapter）224とを備える。なお、複数の物理NIC221は、L2スイッチ114a、114bで構成された業務ネットワークと、管理用スイッチ122a、122bで構成された管理ネットワークにそれぞれ接続される。

40

【0041】

業務サーバ115aでは、仮想化部（VMM）211が実行され、仮想化部211は仮想化管理サーバ130の指令に応じて業務サーバ115aの物理的な計算機リソースを複数の仮想マシン212-1～212-nに割り当てて、各仮想マシンを実行する。

【0042】

仮想化部211上ではn個の仮想マシン212-1～212-nが実行される。各仮想マシン212-1～212-nでは、それぞれOS261-1～261-nが実行され、各OS（ゲストOS）上では業務アプリケーション262-1～262-nが実行されて顧客サイト101に対してサービスを提供する。各仮想マシン212-1～212-nには仮想化部211によって識別子（VM#1～VM#n）が付与される。また、仮想化部

50

211は、CPU制御部234とNIC制御部232により各仮想マシン212-1~212-nに仮想CPU#1~#nと、仮想NIC#1~#nを割り当てる。なお、以下の説明では、OS261-1~261-nの総称をOS261とし、業務アプリケーション262-1~262-nの総称を業務アプリケーション262とし、仮想マシン212-1~212-nの総称を仮想マシン212とする。

【0043】

仮想化部211は、ハードウェア資源210を仮想化して各仮想マシン212に割り当てる。ハードウェア資源210の仮想化及び仮想化された資源を仮想マシン212へ割り当てる手法については、公知又は周知の手法を用いることができるので、ここでは詳述しない。

10

【0044】

仮想化部211は、物理CPU222を仮想化した仮想CPUを仮想マシン212に提供するCPU制御部234と、物理NIC221を仮想化した仮想NICを仮想マシン212に提供するNIC制御部232と、を備える。なお、図示はしないが、仮想化部211はHBAを仮想化した仮想HBAを提供する制御部も備える。

【0045】

CPU制御部234は、各仮想マシン212に割り当てた仮想CPUを仮想CPUインスタンス235として管理する。仮想CPUインスタンス235は、各仮想マシン212に対応する仮想CPU#1~#nが実行する処理と、物理CPU222が実行する処理を調停する。また、仮想CPUインスタンス235は、仮想CPU#1~#n毎に性能監視情報(例えば、CPU使用率またはビジー率)を取得する。なお、仮想CPU#1~#nの性能監視情報は、仮想マシン212-1~212-nのOS261-1~261-nから取得するようにしてもよい。

20

【0046】

NIC制御部232は、仮想マシン212-1~212-nにそれぞれ割り当てた仮想NICを仮想NICインスタンス233として管理する。仮想NICインスタンス233は、各仮想マシン212-1~212-nに対応する仮想NIC#1~#nと物理NIC221の通信を調停する。また、NIC制御部232は、仮想NIC#1~#n毎に性能監視情報を取得する。仮想NIC#1~#n毎に性能監視情報は、例えば、単位時間当たりのデータ転送量、パケットのレイテンシなどで構成される。TCP/IPの例では、L2(第2層)の性能監視情報としては単位時間当たりのパケット転送量とパケットの種別(ARP、TCP、UDPなど)であり、L3(第3層)の性能監視情報としては、TCPコネクション毎の単位時間当たりのパケット転送量またはレイテンシなどを用いることができる。これらのうち予め設定した単位時間当たりのデータ転送量やパケットのレイテンシを性能監視情報として用いればよい。なお、仮想NIC#1~#nの性能監視情報は、仮想マシン212-1~212-nのOS261-1~261-nから取得するようにしてもよい。

30

【0047】

仮想化部211は、遅延の増大が発生した要因を特定するために、CPUの性能監視情報を収集するCPU性能情報収集部242と、NICの性能監視情報を収集するNIC性能情報収集部241と、所定の周期でCPU性能情報収集部242及びNIC性能情報収集部241を機能させるためのタイマ割り込みハンドラ231を備える。

40

【0048】

タイマ割り込みハンドラ231は、所定の周期(例えば、10msec)となる度にCPU性能情報収集部242及びNIC性能情報収集部241へトリガを送信する。CPU性能情報収集部242及びNIC性能情報収集部241はタイマ割り込みハンドラ231からのトリガを受信する度に性能監視情報を収集する。

【0049】

CPU性能情報収集部242は、物理CPU222から性能監視情報(例えば、CPU使用率)を収集し、CPU制御部234の仮想CPUインスタンス235から各仮想CP

50

U # 1 ~ # n の性能監視情報を収集し、CPU性能統計情報 2 4 4 に格納する。なお、CPU性能統計情報 2 4 4 には性能監視情報を収集した時刻のタイムスタンプを保持してもよい。

【 0 0 5 0 】

CPU性能情報収集部 2 4 2 は、CPU性能統計情報 2 4 4 に物理CPU 2 2 2 の識別子または仮想CPUの識別子と上記収集した性能監視情報を対応付けて格納する。ここで、CPU性能統計情報 2 4 4 は、所定時間（例えば、10分間または20分間）の物理CPU 2 2 2 及び仮想CPUの性能監視情報が所定の周期毎に格納される。

【 0 0 5 1 】

最新の物理CPU 2 2 2 及び仮想CPUの性能監視情報を格納する際に、CPU性能統計情報 2 4 4 の T__tail に格納された最も古いデータを削除し、T__head 以降のデータを T__tail 側にシフトしてから最新のデータを T__head に格納する。あるいは、CPU性能統計情報 2 4 4 の記憶領域をリングバッファで構成し、最も古いデータ T__tail に最新のデータを書き込むようにポインタを移動させてもよい。

10

【 0 0 5 2 】

NIC性能情報収集部 2 4 1 は、物理NIC 2 2 1 から性能監視情報（例えば、仮想NICと同様の、単位時間当たりのデータ転送量またはパケットのレイテンシなど）を収集し、また、NIC制御部 2 3 2 の仮想NICインスタンス 2 3 3 から各仮想NIC # 1 ~ # n の性能監視情報を収集し、NIC性能統計情報 2 4 3 に格納する。なお、NIC性能統計情報 2 4 3 には性能監視情報を収集した時刻のタイムスタンプを保持してもよい。

20

【 0 0 5 3 】

NIC性能情報収集部 2 4 1 は、NIC性能統計情報 2 4 3 に物理NIC 2 2 1 の識別子または仮想NICの識別子と上記収集した性能監視情報を対応付けて格納する。なお、物理NIC 2 2 1 または仮想NICの識別子としてはMACアドレスを用いることができ、仮想NICのMACアドレスは、仮想化部 2 1 1 または仮想化管理サーバ 1 3 0 が付与した値である。ここで、NIC性能統計情報 2 4 3 は、所定時間（例えば、10分間または20分間）の物理NIC 2 2 1 及び仮想NICの性能監視情報が所定の周期毎に格納される。最新の物理NIC 2 2 1 及び仮想NICの性能監視情報を格納する際に、NIC性能統計情報 2 4 3 の T__tail に格納された最も古いデータを削除し、T__head 以降のデータを T__tail 側にシフトしてから最新のデータを T__head に格納する。あるいは、NIC性能統計情報 2 4 3 の記憶領域をリングバッファで構成し、最も古いデータ T__tail に最新のデータを書き込むようにポインタを移動させてもよい。

30

【 0 0 5 4 】

仮想化部 2 1 1 は、遅延の増大が発生した要因を特定するために、情報切り出し部 2 5 1 を備える。情報切り出し部 2 5 1 は、ネットワーク監視サーバ 1 1 8 から性能監視情報取得要求 3 1 3 を受信すると、CPU性能統計情報 2 4 4 と、NIC性能統計情報 2 4 3 を取得して、性能監視情報通知 2 5 2 として、ネットワーク監視サーバ 1 1 8 に送信する。

【 0 0 5 5 】

なお、仮想化部 2 1 1 は仮想化管理サーバ 1 3 0 の指令に応じて、業務サーバ 1 1 5 a ~ 1 1 5 d の物理資源を仮想化して各仮想マシン 2 1 2 - 1 ~ 2 1 2 - n に割り当てるが、仮想マシンへの物理資源の割り当てについては公知または周知の手法を用いればよいので、個々では詳述しない。

40

【 0 0 5 6 】

図 3 は、ネットワーク監視サーバ 1 1 8 の構成を示すブロック図である。ネットワーク監視サーバ 1 1 8 は、顧客サイト 1 0 1 のルータ 1 0 2 と、データセンタ 1 1 0 内のルータ 1 2 0 を監視し、データセンタ 1 1 0 が提供するサービスに遅延の増大が発生した場合、遅延増大が発生した部位を特定し、また、遅延増大の要因と推定される部位を特定して、ネットワーク監視端末 1 1 9 へ出力する。すなわち、ネットワーク監視サーバ 1 1 8 は、ルータ 1 2 0 およびルータ 1 0 2 における遅延増大の発生を検知したときに、処理能力

50

の低下要因を特定するシステム性能低下要因特定装置として機能する。

【0057】

ネットワーク監視サーバ118は、ハードウェア資源340として、演算処理を行う物理CPU（または物理プロセッサ）342と、物理CPU342が実行するプログラム及びデータを格納するメモリ343と、複数の物理NIC（または物理ネットワークI/F）341と、プログラムを格納する記憶媒体として不揮発性の記憶装置344を備える。なお、複数の物理NIC341は、管理用回線151と、ネットワーク監視端末119と、管理用スイッチ122a、122bで構成された管理ネットワークにそれぞれ接続される。また、ネットワーク監視サーバ118は、記憶装置344としてストレージ装置116を利用するようにHBAを備えてもよい。

10

【0058】

ネットワーク監視サーバ118は、ネットワーク監視端末119から受け付けた通信フロー情報301と共有資源情報302をメモリ343に格納する。ネットワーク監視サーバ118は、通信フロー情報301と共有資源情報302に基づいて処理を行うモジュールとして、監視条件設定部303、情報収集範囲特定部304、情報取得指示部305、要因特定部306を実行する。これらのモジュールは、プログラムとして記憶装置344に格納され、物理CPU342がメモリ343にロードして実行する。

【0059】

通信フロー情報301と共有資源情報302は、管理者などがネットワーク監視端末119から入力した初期設定情報333に含まれる情報である。

20

【0060】

通信フロー情報301は後述するように、顧客サイト101からの処理要求に含まれる通信先のIPアドレスと、業務サーバ115a～115dの識別子と、仮想マシン212-1～212-nの識別子との対応関係を設定したテーブルである。

【0061】

共有資源情報302は後述するように、業務サーバ115a～115dの識別子と、仮想マシン212-1～212-nの識別子と、業務サーバ115a～115dが利用するストレージ装置116の識別子及び記憶領域の識別子の対応関係を設定したテーブルである。なお、本実施形態では、ストレージ装置116内の記憶領域の識別子を論理ユニット(LU)#101、#102、#201で示すが、これに限定されるものではない。

30

【0062】

業務サーバ監視部321は、業務サーバの追加または削除を監視する。業務サーバ監視部321は、仮想化管理サーバ130等から業務サーバの変更通知（追加または削除）331を受信したときに追加または削除された業務サーバを検出し、情報更新処理部323へ通知する。なお、業務サーバの変更通知331には、変更内容（追加、削除のいずれか）と、業務サーバ115の識別子などが含まれる。

【0063】

VM監視部322は、業務サーバ115a～115dの仮想マシン212の追加、移動または削除を監視する。VM監視部322は、仮想化管理サーバ130から仮想マシン(VM)の変更通知（追加、移動または削除）332を受信し、当該通知に含まれる仮想マシンの追加、移動または削除を情報更新処理部323へ通知する。なお、仮想マシンの変更通知332には、変更内容（追加、削除、移動のいずれか）と、仮想マシン212の識別子とIPアドレス、業務サーバ115の識別子、他の仮想マシン212と共有する計算機資源の識別子などが含まれる。

40

【0064】

情報更新処理部323は、業務サーバや仮想マシンの構成変更に応じて、通信フロー情報301と共有資源情報302を更新する（図中通信フロー再設定334，共有資源情報再設定335）。

【0065】

監視条件設定部303は、通信フロー情報301に基づいて、顧客サイト101のルー

50

タ 1 0 2 の遅延監視部 1 0 3 a ~ 1 0 3 c とデータセンタ 1 1 0 内のルータ 1 2 0 の遅延監視部 1 2 1 に遅延増大の発生について監視すべき通信の条件（監視条件）を設定する。本実施形態では、監視条件として、顧客サイト 1 0 1 からの処理要求に含まれる通信先の IP アドレスと、処理要求の受信から処理応答の送信までの時間の閾値を用いる例を示す。なお、監視条件としては、顧客サイト 1 0 1 のクライアント端末 1 0 4 が要求した処理に対して、データセンタ 1 1 0 からの応答が閾値を超えて遅延したことを検知できればよいので、IP アドレスに限定されるものではなく、また、TCP/IP に限定されるものではない。

【 0 0 6 6 】

クライアント端末からの処理要求から処理応答までの時間の閾値は、データセンタ 1 1 0 内のルータ 1 2 0 の遅延監視部 1 2 1 に設定する閾値 TH 1（第 1 の閾値）と、顧客サイト 1 0 1 のルータ 1 0 2 の遅延監視部 1 0 3 に設定する閾値 TH 2（第 2 の閾値）をそれぞれネットワーク監視端末 1 1 9 から設定する。

【 0 0 6 7 】

ルータ 1 0 2、ルータ 1 2 0 の遅延監視部 1 0 3、1 2 1 は、監視条件設定部 3 0 3 から設定された IP アドレスを含む通信（パケット）について、処理要求を受信した時刻から応答するまでの時刻を監視し、処理要求から応答までの時間が閾値 TH 1 または TH 2 を超えたときに、ネットワーク監視サーバ 1 1 8 に対して処理の遅延の増大が発生したことを示す遅延通知 3 1 2 を送信する。

【 0 0 6 8 】

ルータ 1 2 0 の遅延監視部 1 2 1 に設定される閾値 TH 1 は、データセンタ 1 1 0 内の処理時間に対する閾値で、例えば、数 msec に設定される。ルータ 1 2 0 の遅延監視部 1 2 1 は、クライアント端末 1 0 4 からの処理要求に対して応答するまでの時間が閾値 TH 1 を超えると、ルータ 1 2 0 の遅延監視部 1 2 1 は、データセンタ 1 1 0 内で処理の遅延の増大が発生したと判定して、通信先の IP アドレスとルータ 1 2 0 の識別子を含む遅延通知 3 1 2 をネットワーク監視サーバ 1 1 8 に送信する。

【 0 0 6 9 】

ルータ 1 0 2 の閾値 TH 2 は、データセンタ 1 1 0 内の処理時間に WAN 1 5 0 の回線遅延を加味した閾値である。この閾値 TH 2 の値は、WAN 1 5 0 の通信速度及び顧客サイト 1 0 1 とデータセンタ 1 1 0 の距離に応じて適宜設定される。例えば、顧客サイト 1 0 1 とデータセンタ 1 1 0 の所在が共に国内であれば閾値 TH 2 は、1 0 ~ 2 0 msec に設定し、顧客サイト 1 0 1 が国内で、データセンタ 1 1 0 の所在が海外であれば閾値 TH 2 は、1 0 0 ~ 1 2 0 msec に設定する。なお、閾値 TH 1、閾値 TH 2 は、ネットワーク監視サーバ 1 1 8 を操作する管理者などが初期設定情報 3 3 3 等によって設定することができる。

【 0 0 7 0 】

クライアント端末 1 0 4 からの処理要求に対して応答するまでの時間が第 2 の閾値 TH 2 を超えると、ルータ 1 0 2 の遅延監視部 1 0 3 は、WAN 1 5 0 またはデータセンタ 1 1 0 で処理の遅延の増大が発生したと判定してネットワーク監視サーバ 1 1 8 に対してクライアント端末からの通信先の IP アドレスとルータ 1 0 2 の識別子を含む遅延通知 3 1 2 を送信する。

【 0 0 7 1 】

ここで、ルータ 1 0 2 及びルータ 1 2 0 の遅延監視部 1 0 3、1 2 1 は、顧客サイト 1 0 1 とデータセンタ 1 1 0 間の全ての通信について監視を行う必要がなく、遅延監視部 1 2 1 で指定された通信先 IP アドレスを含む通信のみについて遅延の増大の発生を監視すればよい。これにより、ルータ 1 0 2 及びルータ 1 2 0 の監視処理に要する負荷の増大を抑制できる。

【 0 0 7 2 】

監視条件設定部 3 0 3 は、通信フロー情報 3 0 1 が更新される度に、各ルータ 1 0 2 a ~ 1 0 2 c 及びルータ 1 2 0 の遅延監視部 1 0 3 a ~ 1 0 3 c、1 2 1 に監視条件を通知

10

20

30

40

50

し、更新させる。

【0073】

情報収集範囲特定部304は、ルータ102a～102cまたはルータ120の何れかより遅延通知312を受信すると、通信フロー情報301及び共有資源情報302を参照して遅延の増大が発生した要因について検査すべき計算機資源の範囲を特定する。遅延通知312には、処理の遅延の増大が発生した通信先のIPアドレスが含まれる。

【0074】

情報収集範囲特定部304は、遅延通知312に含まれる通信先のIPアドレスから、業務サーバ115xと仮想マシン212-yを処理の遅延増大が発生した被擬対象として特定する。業務サーバ115xは、図1の業務サーバ115a～115dの何れかであり、仮想マシン212-yは図2の仮想マシン212-1～212-nの何れかを示す。

10

【0075】

次に、情報収集範囲特定部304は、処理の遅延増大の発生部位として特定された業務サーバ115x上の仮想マシン212-xと計算機資源を共有している仮想マシン212-zを性能監視情報の収集範囲として設定する。つまり、被擬対象の仮想マシン212-yの遅延が増大した要因が、被擬対象の仮想マシン212-yのみであるのか、あるいは、仮想マシン212-yが他の仮想マシンと共有する計算機資源に処理能力の低下が発生した結果、当該仮想マシン212-yの遅延が増大したのか、を判定する必要がある。

【0076】

この遅延大の発生の要因としては、物理サーバである業務サーバ115xまたは仮想化部211に処理能力の低下が生じた場合と、仮想マシン212-yが他の仮想マシン212-zと共有している計算機資源に処理能力の低下が発生した場合が考えられる。仮想マシン212-yが他の仮想マシン212-zと共有する計算機資源としては業務サーバ115xのハードウェア資源210、仮想化部211やストレージ装置116及びSAN117などである。

20

【0077】

このように、性能監視情報の収集範囲を、被擬対象部位と計算機資源を共有する仮想マシン212-zまで広げることで、処理の遅延増大が発生した要因がデータセンタ110内の何れの部位であるかを正確に特定できる。

【0078】

情報収集範囲特定部304は、処理の遅延増大が発生した被擬対象として特定した業務サーバ115x、仮想マシン212-y及び計算機資源を共有している仮想マシン212-zを性能監視情報の収集範囲として情報取得指示部305に通知する。

30

【0079】

情報取得指示部305は、情報収集範囲特定部304が特定した業務サーバ115xに対して性能監視情報取得要求313を送信する。この性能監視情報取得要求313は、業務サーバ115xと仮想マシン212-y及び仮想マシン212-zの性能監視情報として、CPU性能統計情報244とNIC性能統計情報243を要求する。なお、後述するように、情報取得指示部305は、NIC性能統計情報243とCPU性能統計情報244を個別に要求してもよい。個別に要求する場合には、性能監視情報取得要求に、取得対象がCPUあるいはNICなのか識別可能な情報が含まれる。あるいはCPU性能監視情報性能監視情報取得要求とNIC性能監視情報性能監視情報取得要求のように複数の性能監視情報性能監視情報取得要求を備えてもよい。

40

【0080】

業務サーバ115xの情報切り出し部251は、性能監視情報取得要求313に対してCPU性能統計情報244とNIC性能統計情報243をネットワーク監視サーバ118に回答する。

【0081】

ネットワーク監視サーバ118では、要因特定部306が業務サーバ115xからのCPU性能統計情報244とNIC性能統計情報243を受け付ける。なお、被擬対象の業

50

務サーバ115xは、CPU性能統計情報244とNIC性能統計情報243をそのまま送信してもよいし、要求された仮想マシン212-y、zと業務サーバ115xのCPU性能統計情報244とNIC性能統計情報243を業務サーバ115xが抽出してから送信してもよい。業務サーバ115xが、CPU性能統計情報244とNIC性能統計情報243をそのまま送信した場合は、要因特定部306がCPU性能統計情報244とNIC性能統計情報243から被擬対象の仮想マシン212-y、zと業務サーバ115xの性能監視情報を抽出すればよい。

【0082】

要因特定部306は、後述するように、遅延通知312の送信元と、通信先IPアドレスから処理の遅延増大が発生した部位を被擬対象部位として特定する。そして、要因特定部306は、被擬対象部位のNIC性能統計情報243から取得した業務サーバ115xにおける処理遅延の有無と、CPU性能統計情報244から仮想CPUの使用率の増加の有無から、処理の遅延増大の要因として、処理能力の低下が発生した部位を特定する。被擬対象部位及び処理能力の低下を生じた部位としてはWAN150、データセンタ110内のネットワーク、仮想化部211または業務サーバ115x、仮想マシン212-y上の業務アプリケーション262である。

10

【0083】

要因特定部306は、上記特定した被擬対象部位と処理能力が低下した部位をネットワーク監視端末119に出力する。データセンタ110の管理者は、処理能力の低下が発生した部位がWAN150であればWAN150の運営会社に通知する。データセンタ110の管理者は、被擬対象部位または処理能力の低下が発生した部位がWAN150であればWAN150の運営会社に通知する。

20

【0084】

また、被擬対象部位または処理能力が低下した部位が仮想化部211であれば、管理者は仮想化部211のベンダに通知する。また、被擬対象部位または処理能力が低下した部位がデータセンタ110内のネットワークであれば、管理者はデータセンタ内のネットワークの運用管理担当者に修復を指示する。また、被擬対象部位または処理能力が低下した部位が業務サーバ115xであれば、管理者は業務サーバ115a~115dの担当者に修復またはリソースの増強を指示する。また、被擬対象部位または処理能力が低下した部位が仮想マシン212-yであれば、当該仮想マシン212-y上の業務アプリケーションを運用している顧客に遅延増大の発生を通知する。

30

【0085】

本実施形態のネットワーク監視サーバ118は、ルータ102またはルータ120から遅延通知312を受信すると、まず、遅延増大の発生した部位がWAN150とデータセンタ110内のいずれであるかを判定する。

【0086】

ネットワーク監視サーバ118は、遅延増大の発生した部位がWAN150であれば、ネットワーク監視端末119から管理者に対してWAN150を管理する通信事業者に修復を依頼するように警告する。

【0087】

40

遅延増大が発生した部位がデータセンタ110内であれば、ネットワーク監視サーバ118は、処理遅延の増大が発生したIPアドレスに対応する仮想マシン212-y及び業務サーバ115xを被擬対象（遅延増大の発生）の部位として特定する。ネットワーク監視サーバ118は、さらに、被擬対象の仮想マシン212-yと計算機資源を共有する仮想マシン212-zにまで性能監視情報の収集範囲を広げることで、仮想化部211の処理能力低下（または障害発生）や物理計算機（業務サーバ115x）の処理能力の低下を迅速に特定して、処理能力の低下（遅延増大）の要因となった部位を特定することができる。これにより、顧客サイト101から通信のない業務サーバ115a~115dと仮想マシン212を監視の対象から除外して、性能監視情報を取得する計算機資源を絞り込むことでネットワーク監視サーバ118の処理負荷が過大になるのを抑制し、処理の遅延増

50

大の要因となった部位を極めて迅速に特定することが可能となるのである。

【0088】

ネットワーク監視端末119は、プロセッサとメモリ及び記憶装置を備えた計算機で構成され、ネットワーク監視サーバ118に接続される。

【0089】

図4は、ネットワーク監視サーバ118が保持する通信フロー情報301の一例を示す説明図である。

【0090】

通信フロー情報301は、顧客サイト101のクライアント端末104に対してサービスを提供する業務サーバ115a~115dの通信に関する情報と、物理計算機(業務サーバ)に関する情報と、仮想マシンに関する情報を関連づけるテーブルである。通信フロー情報301は、ネットワーク監視端末119から管理者が入力した初期設定情報333によって生成され、業務サーバ115a~115dや仮想マシン212の変更に応じて情報更新処理部323によって更新される。

【0091】

通信フロー情報301は、サービスを提供する仮想マシン212に割り当てられたIPアドレスを格納する通信先IPアドレス501と、仮想マシン212を実行する業務サーバ115a~115dの識別子を格納する業務サーバ番号502と、当該仮想マシンに設定された識別子を格納するVM番号503から一つのエントリが構成される。

【0092】

通信先IPアドレス501は、顧客サイト101のクライアント端末104が宛先IPアドレスとして使用するアドレスで、管理者などがネットワーク監視端末119から設定した値である。

【0093】

業務サーバ番号502は、データセンタ110内で業務サーバ115a~115dを識別するために、管理者などがネットワーク監視端末119から設定した値である。

【0094】

VM番号503は、業務サーバ115a~115d内で仮想マシン212-1~212-nを識別するために、仮想化部211が設定した値である。

【0095】

図示の例では、エントリ511、512が業務サーバ115a(APserv#1)で2つの仮想マシンVM#1とVM#2が稼動してそれぞれサービスを提供することを示し、エントリ513は、業務サーバ115b(APserv#2)で1つの仮想マシンVM#1が稼動してサービスを提供することを示す。

【0096】

図5は、ネットワーク監視サーバ118が保持する共有資源情報302の一例を示す説明図である。

【0097】

共有資源情報302は、仮想マシン212-1~212-nが共有するデータセンタ110内の物理リソースの設定情報を格納するテーブルである。共有資源情報302は、ネットワーク監視端末119から管理者が入力した初期設定情報333によって生成され、業務サーバ115a~115dや仮想マシン212の変更に応じて情報更新処理部323によって更新される。

【0098】

共有資源情報302は、業務サーバ115a~115dの識別子を格納する業務サーバ番号601と、仮想マシンに設定された識別子を格納するVM番号602と、当該仮想マシンに割り当てられたストレージ装置116の識別子を格納するストレージ装置番号603と、ストレージ装置116内の記憶領域の識別子を格納するLU番号604から一つのエントリが構成される。

【0099】

10

20

30

40

50

業務サーバ番号601は、通信フロー情報301の業務サーバ番号502と同様であり、データセンタ110内で業務サーバ115a~115dを識別するために、管理者などがネットワーク監視端末119から設定した値である。

【0100】

VM番号602は、通信フロー情報301のVM番号503と同様であり、業務サーバ115a~115d内で仮想マシン212-1~212-nを識別するために、仮想化部211が設定した値である。

【0101】

ストレージ装置番号603は、データセンタ110内でストレージ装置を特定するために、管理者などがネットワーク監視端末119から設定した値である。

10

【0102】

LU番号604は、ストレージ装置116内で記憶領域を識別するために、管理者などがネットワーク監視端末119から設定した値である。

【0103】

図示の例では、エントリ611、612が業務サーバ115a(APserv#1)で2つの仮想マシンVM#1とVM#2が稼働し、仮想マシンVM#1にはストレージ装置116(RAID#1)のLU#101が割り当てられ、仮想マシンVM#2にはストレージ装置116(RAID#1)のLU#102が割り当てられた例を示す。すなわち、業務サーバ115a(仮想化部211)とストレージ装置116が業務サーバ115a(APserv#1)上の仮想マシンVM#1とVM#2で共有されることを示す。

20

【0104】

図6は、顧客サイト101aからデータセンタ110の業務サーバ115a(APserv#1)で稼働するOS261-1にアクセスする際の処理の遅延を示すタイムチャートである。図示の例では、顧客サイト101aのクライアント端末104aがOS261-1(仮想マシン212-1(VM#1))上の業務アプリケーション262-1にアクセスする例を示す。

【0105】

顧客サイト101aのクライアント端末104aが、データセンタ110の業務サーバ115aで実行されるOS261-1(仮想マシン212-1)上の業務アプリケーションに対して処理要求を送信し、図中時刻T1で顧客サイト101aのルータ102aが処理要求を受信する。

30

【0106】

ルータ102aの遅延監視部103aは、予めデータセンタ110の監視条件設定部303から監視条件として通信先IPアドレス501を受信して保持する。そして、ルータ102aの遅延監視部103aは、クライアント端末104aから受信した処理要求に対する応答をデータセンタ110から受信するまでの時間の監視を開始する。ルータ102aは、クライアント端末104aから受信した処理要求を、WAN150を介してデータセンタ110のルータ120に送信する。

【0107】

なお、図示の例では、処理要求がHTTPリクエストであり、処理応答がHTTPレスポンスの例を示す。HTTPリクエストまたはHTTPレスポンスは、TCPの通信端点(発信元IPアドレス、発信元ポート番号、通信先IPアドレス、通信先ポート番号)毎に1つの要求に対して1つの応答が送受信されるため、HTTPリクエストに対するHTTPレスポンスを監視することで、通信を含む処理の遅延時間を測定することができる。

40

【0108】

時刻T2では、データセンタ110のルータ120が、WAN150を介して顧客サイト101aのルータ102aから処理要求を受信する。

【0109】

ルータ120の遅延監視部121は、顧客サイト101aから受信した処理要求に対す

50

る応答を業務サーバ115aから受信し、顧客サイト101aに返信するまでの時間の監視を開始する。ルータ120は、WAN150から受信した処理要求を、業務ネットワーク(L2スイッチ114a)を介して通信先IPアドレスの業務サーバ115aに送信する。

【0110】

時刻T3では、業務サーバ115aの物理NIC221が業務ネットワークから処理要求を受信し、仮想化部211が当該処理要求を通信先IPアドレスに対応するOS261-1(仮想マシン212-1)に送信する。時刻T4ではOS261-1が物理NIC221を制御する仮想化部211から処理要求を受信し、OS上で稼動する業務アプリケーション262-1で処理を開始、時刻T5で処理を完了する。OS261-1は、時刻T5で、処理要求に対する処理結果を処理応答として仮想化部211を介して物理NIC221から顧客サイト101aに送信する。

10

【0111】

時刻T6では、OS261-1から処理要求を受信した仮想化部211が、物理NIC221を介して業務ネットワーク(L2スイッチ114a)に処理応答を送信する。時刻T7では、データセンタ110のルータ120が、業務ネットワークから受信した業務サーバ115aからの処理応答を受信し、時刻T7で処理応答をWAN150に送信する。

【0112】

時刻T7において、ルータ120の遅延監視部121は、顧客サイト101aから受け付けた処理要求に含まれる通信先IPアドレスXと送信元IPアドレスYを受信した時刻T2と、業務サーバ115aから受信した処理応答の通信先IPアドレスがY、送信元IPアドレスがXの場合、この処理応答を顧客サイト101aへ送信した時刻T7との差分をデータセンタ110内の処理の遅延時間として求める。

20

【0113】

そして、ルータ120の遅延監視部121は、処理の遅延時間が予め設定された閾値TH1を超えていれば、ネットワーク監視サーバ118に遅延時間の増大が発生したことを通知する。

【0114】

時刻T8では、顧客サイト101aのルータ102aが、WAN150を介してデータセンタ110から処理応答を受信する。

30

【0115】

また、ルータ102aの遅延監視部103aは、時刻T1で受信したクライアント端末104aからの処理要求に含まれる通信先IPアドレスXと送信元IPアドレスYを保持し、データセンタ110から受信した処理応答の通信先IPアドレスがY、送信元IPアドレスがXの場合、この処理応答をクライアント端末104aへ送信した時刻T8とし、時刻T8とT1の差分を顧客サイト101aから見た処理(または通信)の遅延時間として求める。

【0116】

そして、ルータ102aの遅延監視部103aは、処理の遅延時間が予め設定された閾値TH2を超えていれば、管理用回線151を介してネットワーク監視サーバ118に遅延の増大が発生したことを通知する。

40

【0117】

図6において、顧客サイト101aのクライアント端末104aから見た処理の遅延時間1001は、顧客サイト101aのルータ102aで観測される時刻T8-T1となる。また、データセンタ110内の処理の遅延時間1002は、時刻T7-T2となる。また、業務サーバ115a内の処理の遅延時間(または処理時間)1003は、時刻T6-T3となる。そして、OS261-1上の処理の遅延時間(または処理時間)は、時刻T5-T4となる。また、顧客サイト101aのクライアント端末104aから観測したWAN150の通信に伴う遅延時間1005は、時刻T8-T1-T7+T2となる。

【0118】

50

以上のように、顧客サイト101aのルータ102aでは、顧客サイト101aから見た、処理の遅延時間1001を閾値TH2により監視し、データセンタ110のルータ120では、データセンタ110内の処理の遅延時間1002を閾値TH1により監視する。そして各ルータ102a、120は、処理の遅延時間が閾値TH1またはTH2を超えると、ネットワーク監視サーバ118に処理の遅延が増大したことを、通信先のIPアドレスを含めて通知する。

【0119】

なお、図6では、顧客サイト101aのクライアント端末104aの例について説明したが、顧客サイト101b～101cについても同様である。

【0120】

図7は、ネットワーク監視サーバ118で実行される処理の一例を示すフローチャートである。この処理は、ネットワーク監視サーバ118の情報収集範囲特定部304が、顧客サイト101a～101cのルータ102a～102cまたはデータセンタ110のルータ120からの何れかひとつから遅延検知312を受信したときに実行される。

【0121】

ステップS402では、情報収集範囲特定部304が処理の遅延増大が発生した部位がWAN150であるか否かを判定する。この判定は、情報収集範囲特定部304が遅延検知312を受信したルータの識別子が顧客サイト101のルータ102a～102cまたはデータセンタ110のルータ120の何れであるかを判定し、顧客サイト101のルータ102a～102cのいずれかから遅延検知312を受信した場合には、WAN150に遅延の増大が発生したと判定して、ステップS409に進む。ステップS409では、情報収集範囲特定部304が要因特定部306に、処理の遅延の増大が発生した部位がWAN150であることを通知する。そして、要因特定部306はネットワーク監視端末119にWAN150に処理の遅延増大が発生したことをシステム性能低下要因通知314として通知する。システム性能低下要因通知314を受信したネットワーク監視端末119では、WAN150の障害などによる遅延の増大が生じたことをディスプレイ(図示省略)に表示する。

【0122】

一方、情報収集範囲特定部304がデータセンタ110のルータ120から遅延検知312を受信した場合、または、データセンタ110のルータ120と顧客サイト101のルータ102の双方から遅延検知312を受信した場合には、データセンタ110内で遅延の増大の要因を探索するため、ステップS403へ進む。

【0123】

ステップS403では、ネットワーク監視サーバ118の情報収集範囲特定部304が、遅延検知312に含まれるIPアドレスで通信フロー情報301を検索し、通信先IPアドレス501と一致する業務サーバ番号502とVM番号503から、処理の遅延増大が発生した部位として、業務サーバ115xと仮想マシン212-yを特定する。

【0124】

ステップS404では、ネットワーク監視サーバ118は、遅延増大の要因となった部位を特定するため、被擬対象の業務サーバ115x及び仮想マシン212-yから性能監視情報を取得する。この処理は、情報収集範囲特定部304が情報取得指示部305に対して被擬対象の業務サーバ115xと仮想マシン212-yのNICに関する性能監視情報を取得する指令を通知する。情報取得指示部305は指令された被擬対象の業務サーバ115xの情報切り出し部251に対してNICの性能監視情報を要求する性能監視情報取得要求313を送信する。被擬対象の業務サーバ115xでは、情報切り出し部251がNIC性能統計情報243を取得し、性能監視情報通知252としてネットワーク監視サーバ118に返信する。

【0125】

ネットワーク監視サーバ118は、業務サーバ115xからNICに関する性能監視情報通知252を受信すると、ステップS405で業務サーバ115x内のNIC(物理N

10

20

30

40

50

IC221及び仮想NIC)で処理の遅延増大が発生したか否かを判定する。この判定は、要因特定部306で行われる。要因特定部306は、性能監視情報通知252のNICの性能監視情報のうち、レイテンシが所定の閾値を超えたデータ(パケット)またはデータ転送量が所定の閾値を超えたデータがある場合には、被擬対象の業務サーバ115xまたは仮想マシン212-yのNICで処理の遅延増大が発生したと判定し、ステップS406に進む。一方、要因特定部306はNICの性能監視情報に処理の遅延増大がない場合にはステップS410へ進む。

【0126】

ステップS410では、要因特定部306は、被擬対象の業務サーバ115xに処理の遅延増大の要因がないと判定し、かつ、データセンタ110のルータ120で処理の遅延増大が発生していることから、データセンタ110内の業務ネットワークに障害が発生したと判定する。要因特定部306は、ネットワーク監視端末119に対して、データセンタ110内の業務ネットワークに障害が発生した可能性がある旨をシステム性能低下要因通知314として通知する。システム性能低下要因通知314を受信したネットワーク監視端末119では、データセンタ110内の業務ネットワークに障害などによる遅延の増大が生じたことをディスプレイ(図示省略)に表示する。

10

【0127】

ステップS406では、被擬対象の業務サーバ115xまたは仮想マシン212-yのNICに処理の遅延増大が発生しているため、さらに、遅延増大の要因を特定する。このため、情報収集範囲特定部304は、共有資源情報302を参照して、被擬対象の仮想マシン212-yと物理的な計算機資源を共有する仮想化部211と仮想マシンを抽出する。

20

【0128】

ステップS407では、情報収集範囲特定部304が、上記ステップS406で抽出した被擬対象の仮想マシン212-yと物理的な計算機資源を共有する仮想化部211及び仮想マシン212を実行する業務サーバ115xからCPUに関する性能監視情報を取得する指令を情報取得指示部305に通知する。情報取得指示部305は、被擬対象の業務サーバ115xに対して性能監視情報取得要求313を送信し、上記抽出した仮想化部211及び仮想マシン212のCPUの性能監視情報を要求する。

【0129】

業務サーバ115xの情報切り出し部251は、性能監視情報取得要求313に対するCPU性能統計情報244を取得し、性能監視情報通知252としてネットワーク監視サーバ118に返信する。

30

【0130】

ネットワーク監視サーバ118は、業務サーバ115xからCPUに関する性能監視情報通知252を受信すると、ステップS407で業務サーバ115xの仮想マシン212-yに割り当てられた仮想CPUの使用率が増大したか否かを判定する。この判定は、要因特定部306で行われる。要因特定部306は、性能監視情報通知252のCPUの性能監視情報のうち、被擬対象の仮想マシン212-yの仮想CPUの使用率と、物理的な計算機資源を共有する他の仮想マシン212の仮想CPUの使用率を抽出し、各仮想CPUの使用率が増加したか否かを判定する。この判定は、仮想CPUの使用率を時系列的に比較して使用率の増加を検知してもよいし、あるいは、仮想CPUの使用率が所定の閾値(例えば、90%)を超えていればCPUの使用率が増加したと判定してもよい。

40

【0131】

要因特定部306は、仮想CPUの使用率が所定の閾値を超えて増加したと判定した場合は、ステップS412へ進んで、仮想マシン212上の業務アプリケーション262に障害またはエラーが発生して、処理の遅延増大が発生したことをネットワーク監視端末119にシステム性能低下要因通知314として通知する。ネットワーク監視端末119は、ネットワーク監視サーバ118からのシステム性能低下要因通知314に基づいて、仮想マシン212-y上で稼動している業務アプリケーション262に障害が発生している

50

通知をディスプレイ（図示省略しない）等に表示し、業務アプリケーション 262 を運用及び管理している顧客に連絡することを促す。

【0132】

一方、要因特定部 306 は、仮想 CPU の使用率が増加していないと判定した場合は、ステップ S411 へ進んで、仮想マシン 212 を稼働させる仮想化部 211 に障害が発生して、処理の遅延増大が発生したと判定してネットワーク監視端末 119 にシステム性能低下要因通知 314 を通知する。すなわち、仮想 CPU の使用率が増大せず、業務サーバ 115x で処理の遅延増大が発生している場合は、仮想化部 211 の障害、あるいは業務サーバ 115x のハードウェア資源 210 に障害が発生していることが考えられる。このため、ネットワーク監視サーバ 118 からシステム性能低下要因通知 314 を受けたネットワーク監視端末 119 は、データセンタ 110 の管理者に仮想化部 211 のベンダへの連絡や、業務サーバ 115x の増強を検討することを促す警告を図示しないディスプレイなどに表示する。

10

【0133】

以上の処理によって、顧客サイト 101 のルータ 102 と、データセンタ 110 のルータ 120 で、予め設定した通信先 IP アドレスのみについて遅延時間を監視し、遅延の増大が発生した場合には該当する IP アドレスとともに遅延通知 312 としてネットワーク監視サーバ 118 に通知する。ネットワーク監視サーバ 118 は、遅延通知 312 を受信すると、WAN 150 の障害であるか否かを特定する。WAN 150 の障害でない場合には、ネットワーク監視サーバ 118 は、遅延通知 312 に含まれる IP アドレスから被擬対象の業務サーバ 115x と仮想マシン 212 - y を遅延増大が発生した部位として特定する。そして、ネットワーク監視サーバ 118 は、これらの被擬対象（遅延増大が発生した部位）について NIC の性能監視情報を収集して、遅延の増大の要因がデータセンタ 110 内の業務ネットワークであるか否かを特定する。遅延の増大の要因が業務ネットワークでない場合には、ネットワーク監視サーバ 118 は被擬対象の仮想マシン 212 - y と物理的な計算機資源を共有するリソースも被擬対象に加えて CPU の性能監視情報を取得し、遅延の増大の要因が仮想化部 211 と仮想マシン 212 - y 上の業務アプリケーション 262 の何れであるかを特定する。

20

【0134】

そして、ネットワーク監視サーバ 118 は、上記のように遅延の増大の要因となった部位を特定してネットワーク監視端末 119 に通知し、ネットワーク監視端末 119 では遅延の増大が発生した部位をディスプレイなどに表示する。ネットワーク監視端末 119 を使用する管理者は、ディスプレイの表示から、遅延の増大の要因として特定された部位に応じて障害の復旧を指示する相手を迅速に判断することができる。

30

【0135】

このように、業務アプリケーション 262 を実際に利用している通信のみを監視し、通信先 IP アドレス 501 からデータセンタ 110 内で遅延の増大が発生した部位を絞り込み、絞り込んだ業務サーバ 115x、仮想マシン 212 - y から性能監視情報を取得し、遅延の増大が発生した部位を特定する。さらに、被擬対象の仮想マシン 212 - y と物理的な計算機資源を共有する部位（物理計算機、仮想化部 211、他の仮想マシン 212）についても性能監視情報を取得して遅延増大の要因となった部位を特定することができる。

40

【0136】

これにより、前記従来例のようにネットワーク監視サーバ 118 が、すべての業務サーバ 115 及び仮想マシン 212 の性能監視情報を収集する必要はなく、また、遅延の増大が発生した部位の特定や、遅延増大の要因となった部位を特定するために取得する性能監視情報のデータ量を前記従来例よりも大幅に低減でき、遅延増大が発生した部位を迅速に特定し、さらに、遅延増大の要因となった部位も迅速に特定することが可能となる。

【0137】

以上より、クラウドコンピューティングを構成する WAN 150 と、データセンタ内の

50

業務ネットワークを構成する機器と、業務サーバ 1 1 5 の仮想化部 2 1 1 と、仮想化部 2 1 1 上の仮想マシン 2 1 2 で発生する障害を検知し、かつ、処理能力（システム性能）が低下した要因を迅速に特定することで信頼性の高いサービスを提供することが可能となる。

【 0 1 3 8 】

図 8 は、ネットワーク監視端末 1 1 9 のディスプレイで遅延の増大が発生した部位を表示するインターフェースの一例を示す画面イメージである。

【 0 1 3 9 】

ネットワーク監視端末 1 1 9 のインターフェースは、計算機システムの構成を示す領域 7 1 0 と、システム性能低下要因通知 3 1 4 を表示する領域 7 2 0 の 2 つに大別される。領域 7 1 0 では、処理の遅延増大が検出された通信経路 7 0 1 が枠によって表示される。そして、領域 7 1 0 には、上記図 7 の処理によって処理の遅延増大が検知された部位として仮想マシン（VM # 1）に注意を喚起するアイコン 7 0 3 が表示される。また、領域 7 1 0 には、上記図 7 の処理によって遅延増大の要因と判定された部位として他の仮想マシン（VM # 1）に動作の異常を示すアイコン 7 0 4 が表示される。さらに、領域 7 1 0 では、処理の遅延増大が検出された仮想マシン 2 1 2 と物理的な計算機資源を共有する要素が枠内に表示される。

10

【 0 1 4 0 】

システム性能低下要因通知 3 1 4 を表示する領域 7 2 0 は、遅延の増大の種類として、通信経路の領域 7 1 1、通信エンドポイントの領域 7 1 2、資源共有範囲の領域 7 1 3 及び VM 処理能力低下の領域 7 1 4 の 4 種類で構成した例を示す。そして、システム性能低下要因通知 3 1 4 に含まれる遅延増大の要因には、チェックマーク 7 1 5、7 1 6 が表示される。

20

【 0 1 4 1 】

図示の例では、通信経路の領域 7 1 1 と、資源共有範囲の領域 7 1 3 にチェックマーク 7 1 5、7 1 6 が設定される。これらの、領域 7 1 1、7 1 3 のアラート内容としては、領域 7 1 0 に対応したテキストが表示される。領域 7 1 1 のアラート内容には、通信経路 7 0 1 で遅延増大が発生したことが表示され、領域 7 1 3 のアラート内容には、遅延増大が発生した部位として特定された業務サーバ（AP Ser v # 1）及び仮想マシン（VM # 1）と計算機資源を共有する装置の範囲 7 0 2 が表示される。

30

【 0 1 4 2 】

データセンタ 1 1 0 の管理者は、計算機システムの構成をグラフィックで示す領域 7 1 0 の注意及び警告と、領域 7 2 0 のテキストによる詳細な表示により、遅延増大が発生した部位を迅速かつ容易に理解することができる。

【 0 1 4 3 】

図 9 は、図 8 に示した遅延増大が発生した部位を特定する処理のシーケンス図である。

【 0 1 4 4 】

ステップ 1 では、ネットワーク監視サーバ 1 1 8 が顧客サイト 1 0 1 a のルータ 1 0 2 a とデータセンタ 1 1 0 のルータ 1 2 0 からそれぞれ遅延通知 3 1 2 を受信する。

【 0 1 4 5 】

ステップ 2 では、ネットワーク監視サーバ 1 1 8 が、遅延増大が発生した部位が、WAN 1 5 0 とデータセンタ 1 1 0 の何れであるかを判定する。この処理は、図 7 のステップ S 4 0 2 である。この例では、顧客サイト 1 0 1 a のルータ 1 0 2 a とデータセンタ 1 1 0 のルータ 1 2 0 が共に遅延増大を検知しているので、ネットワーク監視サーバ 1 1 8 は、データセンタ 1 1 0 内に遅延増大の要因が存在すると判定する。ネットワーク監視サーバ 1 1 8 は、ルータからの遅延通知 3 1 2 に含まれる IP アドレスから、遅延増大の発生した部位の被擬対象が、業務サーバが業務サーバ 1 1 5 a で、被擬対象の仮想マシン 2 1 2 - 1（VM # 1）であると特定する。この処理は、図 7 のステップ S 4 0 3 である。

40

【 0 1 4 6 】

ステップ 3 では、ネットワーク監視サーバ 1 1 8 が、被擬対象の業務サーバ 1 1 5 a が

50

らNICの性能監視情報を取得する。この処理は、図7のステップS404である。

【0147】

ステップ4では、ネットワーク監視サーバ118が、取得したNICの性能監視情報から遅延増大の要因が業務ネットワークと業務サーバ115aの何れであるかを判定する。この処理は、図7のステップS405である。この例では、NICの性能監視情報にシステム性能低下要因を検知したため、業務サーバ115aに遅延増大の要因があると判定する。

【0148】

ステップ5では、ネットワーク監視サーバ118が共有資源情報302を参照して、被擬対象の仮想マシン212-1と物理的な計算機資源を共有する仮想化部211と他の仮想マシン212を抽出する。この処理は、図7のステップS406である。この例では、業務サーバ115bの仮想マシン212とストレージ装置116のLUを共有している場合を示す。

10

【0149】

ステップ6では、ネットワーク監視サーバ118が被擬対象の業務サーバ115aの仮想化部211及び仮想マシン212-1のCPUの性能監視情報を取得し、ステップ7では、被擬対象の仮想マシン212-1が実行される業務サーバ115a上の他の仮想マシン212のCPUの性能監視情報を取得する。また、ステップ8、ステップ9では、ネットワーク監視サーバ118が、被擬対象の仮想マシン212-1と物理的な計算機資源を共有する業務サーバ115bの仮想化部211及び仮想マシン212のCPUの性能監視情報を取得する。これら処理は、図7のステップS407である。

20

【0150】

ステップ10では、上記取得したCPUの性能監視情報から、ネットワーク監視サーバ118は業務サーバ115bの仮想マシン(#VM1)で仮想CPUの使用率が増大したことを検出し、当該仮想マシンが遅延増大の要因となった部位であると特定する。

【0151】

こうして、業務アプリケーション262を実際に利用している通信から顧客サイト101とデータセンタ110のルータで処理の遅延増大をそれぞれ検知し、検知した通信に含まれる宛先アドレス(通信先IPアドレス501)からネットワーク監視サーバ118が処理の遅延が増大した業務サーバ115(物理計算機)と仮想マシン212(仮想計算機)を特定する。

30

【0152】

そして、被擬対象の仮想マシン212-yと物理的な計算機資源を共有する他の仮想マシン212、他の業務サーバ115からもCPUの性能監視情報を取得することで、業務サーバ115bの仮想マシン#VM1が遅延増大の要因となった部位であることを特定できる。

【0153】

この例では、業務サーバ115a(APServ#1)の仮想マシン#VM1と、業務サーバ115b(APServ#2)の仮想マシン#VM1がストレージ装置116のLUを共有している。ルータによって遅延増大を検知されたのは業務サーバAPServ#1の仮想マシン#VM1であるが、ストレージ装置116のLUを共有する業務サーバAPServ#2の仮想マシン#VM1に障害が発生したため、業務サーバAPServ#1の仮想マシン#VM1のアクセスが遅延したことが推測できる。また、データセンタ110のストレージ装置116の管理者に対しては、業務サーバAPServ#1、#2の仮想マシン212が共有するLUに障害がないかを確認する契機を提供することができる。

40

【0154】

このように、本発明では、処理の遅延増大を検知した仮想マシン212-yと、実際に障害等が発生した仮想マシン#VM1(APServ#2)を特定することが可能となる。

50

【 0 1 5 5 】

図 1 0 A、図 1 0 B はネットワーク監視サーバ 1 1 8 の業務サーバ監視部 3 2 1 と、V M監視部 3 2 2 及び情報更新処理部 3 2 3 で行われる処理の一例を示すフローチャートである。この処理は、ネットワーク監視サーバ 1 1 8 が、仮想化管理サーバ 1 3 0 から業務サーバの変更通知（追加または削除）3 3 1 や仮想マシン 2 1 2 の変更通知（追加、移動または削除）3 3 2 を受信したときに実行される。図 1 0 A のステップ S 9 0 1 ~ S 9 0 7 の処理が業務サーバ監視部 3 2 1 及び情報更新処理部 3 2 3 の処理に相当し、図 1 0 B のステップ S 9 0 8 ~ S 9 1 9 の処理が V M監視部 3 2 2 及び情報更新処理部 3 2 3 の処理に相当する。

【 0 1 5 6 】

ステップ S 9 0 1 では、業務サーバ監視部 3 2 1 が、業務サーバの変更通知 3 3 1 を受信したか否かを判定する。業務サーバの変更通知 3 3 1 を受信していなければ図 1 0 B のステップ S 9 0 8 に進む。一方、業務サーバの変更通知 3 3 1 が業務サーバ 1 1 5 の追加であればステップ S 9 0 2 へ進み、削除であればステップ S 9 0 5 に進む。

【 0 1 5 7 】

ステップ S 9 0 2 では、業務サーバ監視部 3 2 1 が業務サーバの変更通知 3 3 1 から追加された業務サーバ 1 1 5 を特定し、当該業務サーバ 1 1 5 の仮想化部 2 1 1 から定義されている仮想マシン 2 1 2 に関する情報を取得する。

【 0 1 5 8 】

ステップ S 9 0 3 では、業務サーバ監視部 3 2 1 が業務サーバ 1 1 5 から取得した仮想マシン 2 1 2 の I P アドレス、仮想マシン 2 1 2 の識別子（番号）、業務サーバ 1 1 5 の識別子（番号）を、通信フロー情報 3 0 1 に設定する。

【 0 1 5 9 】

ステップ S 9 0 4 では、業務サーバ監視部 3 2 1 は、業務サーバ 1 1 5 から取得した仮想マシン 2 1 2 が共有する計算機資源の情報を共有資源情報 3 0 2 に設定する。

【 0 1 6 0 】

上記ステップ S 9 0 2 ~ S 9 0 4 により、ネットワーク監視サーバ 1 1 8 が受信した業務サーバ変更通知 3 3 1 で追加された業務サーバ 1 1 5 の一つについて、ルータの監視対象となる仮想マシン 2 1 2 の通信先 I P アドレス 5 0 1 等が通信フロー情報 3 0 1 に加えられ、追加された業務サーバ 1 1 5 上の仮想マシン 2 1 2 が共有する計算機資源が共有資源情報 3 0 2 に加えられる。

【 0 1 6 1 】

ステップ S 9 0 5 では、業務サーバ監視部 3 2 1 が、業務サーバの変更通知 3 3 1 から削除された業務サーバ 1 1 5 の識別子（番号）を取得する。

【 0 1 6 2 】

ステップ S 9 0 6 では、業務サーバ監視部 3 2 1 が、業務サーバ 1 1 5 の識別子と一致する業務サーバ番号 5 0 2 を含むエントリを、通信フロー情報 3 0 1 から検索し、当該エントリを削除する。

【 0 1 6 3 】

ステップ S 9 0 6 では、業務サーバ監視部 3 2 1 が、業務サーバ 1 1 5 の識別子と一致する業務サーバ番号 6 0 1 を含むエントリを、共有資源情報 3 0 2 から検索し、当該エントリを削除する。

【 0 1 6 4 】

上記ステップ S 9 0 5 ~ S 9 0 7 により、ネットワーク監視サーバ 1 1 8 は、受信した業務サーバ変更通知 3 3 1 に含まれる削除された業務サーバ 1 1 5 の一つについて、通信フロー情報 3 0 1 と共有資源情報 3 0 2 から削除する。

【 0 1 6 5 】

次に、業務サーバの変更通知 3 3 1 を受信していなければ図 1 0 B のステップ S 9 0 8 では、V M監視部 3 2 2 が、仮想マシン 2 1 2 の変更通知 3 3 2 を受信したか否かを判定する。仮想マシン 2 1 2 の変更通知 3 3 2 を受信していなければステップ S 9 2 0 に進む

10

20

30

40

50

。一方、仮想マシン 2 1 2 の変更通知 3 3 2 が仮想マシン 2 1 2 の追加であればステップ S 9 0 9 へ進み、削除であればステップ S 9 1 2 へ進み、移動であればステップ S 9 1 5 へ進む。

【 0 1 6 6 】

ステップ S 9 0 9 では、VM 監視部 3 2 2 が仮想マシン 2 1 2 の変更通知 3 3 2 で追加された仮想マシン 2 1 2 と、当該仮想マシン 2 1 2 が稼動する業務サーバ 1 1 5 の識別子を特定し、当該業務サーバ 1 1 5 の仮想化部 2 1 1 から追加された仮想マシン 2 1 2 に関する情報を取得する。

【 0 1 6 7 】

ステップ S 9 1 0 では、VM 監視部 3 2 2 が業務サーバ 1 1 5 から取得した仮想マシン 2 1 2 の IP アドレス、仮想マシン 2 1 2 の識別子（番号）、業務サーバ 1 1 5 の識別子（番号）を、通信フロー情報 3 0 1 に設定する。

10

【 0 1 6 8 】

ステップ S 9 1 1 では、VM 監視部 3 2 2 は、業務サーバ 1 1 5 から取得した仮想マシン 2 1 2 の情報から他の仮想マシン 2 1 2 と共有する計算機資源の情報を共有資源情報 3 0 2 に設定する。

【 0 1 6 9 】

上記ステップ S 9 0 9 ~ S 9 1 1 により、ネットワーク監視サーバ 1 1 8 が受信した仮想マシン変更通知 3 3 2 で追加された仮想マシン 2 1 2 の一つについて、ルータの監視対象となる仮想マシン 2 1 2 の通信先 IP アドレス 5 0 1 等が通信フロー情報 3 0 1 に加えられ、追加された仮想マシン 2 1 2 が共有する計算機資源が共有資源情報 3 0 2 に加えられる。

20

【 0 1 7 0 】

次に、ステップ S 9 1 2 では、VM 監視部 3 2 2 が仮想マシンの変更通知 3 3 2 で削除された仮想マシン 2 1 2 の識別子と、当該仮想マシン 2 1 2 が稼動する業務サーバ 1 1 5 の識別子を取得する。

【 0 1 7 1 】

ステップ S 9 1 3 では、VM 監視部 3 2 2 が、業務サーバ 1 1 5 の識別子及び仮想マシン 2 1 2 の識別子が一致する業務サーバ番号 5 0 2 及び VM 番号 5 0 3 を含むエントリを、通信フロー情報 3 0 1 から検索し、当該エントリを削除する。

30

【 0 1 7 2 】

ステップ S 9 1 4 では、VM 監視部 3 2 2 が、業務サーバ 1 1 5 の識別子及び仮想マシン 2 1 2 の識別子と一致する業務サーバ番号 6 0 1 及び VM 番号 6 0 2 を含むエントリを、共有資源情報 3 0 2 から検索し、当該エントリを削除する。

【 0 1 7 3 】

上記ステップ S 9 1 2 ~ S 9 1 4 により、ネットワーク監視サーバ 1 1 8 は、受信した仮想マシンの変更通知 3 3 2 に含まれる削除された仮想マシン 2 1 2 の一つについて、通信フロー情報 3 0 1 と共有資源情報 3 0 2 から削除する。

【 0 1 7 4 】

次に、ステップ S 9 1 5 では、VM 監視部 3 2 2 が仮想マシンの変更通知 3 3 2 で移動された仮想マシン 2 1 2 の識別子と、当該仮想マシン 2 1 2 が稼動する業務サーバ 1 1 5 の識別子を取得する。これらの識別子は、移動元の仮想マシン及び業務サーバの識別子と、移動先の仮想マシン 2 1 2 及び業務サーバ 1 1 5 の識別子を含む。

40

【 0 1 7 5 】

ステップ S 9 1 6 では、VM 監視部 3 2 2 が、移動元の業務サーバ 1 1 5 の識別子及び仮想マシン 2 1 2 の識別子が一致する業務サーバ番号 5 0 2 及び VM 番号 5 0 3 を含むエントリを、通信フロー情報 3 0 1 から検索し、当該エントリを削除する。

【 0 1 7 6 】

ステップ S 9 1 7 では、VM 監視部 3 2 2 が、移動元の業務サーバ 1 1 5 の識別子及び仮想マシン 2 1 2 の識別子と一致する業務サーバ番号 6 0 1 及び VM 番号 6 0 2 を含むエ

50

ントリを、共有資源情報 302 から検索し、当該エントリを削除する。

【0177】

上記ステップ S916 ~ S917 により、ネットワーク監視サーバ 118 は、受信した仮想マシンの変更通知 332 に含まれる移動された仮想マシン 212 の一つについて、移動元の仮想マシン 212 の情報を通信フロー情報 301 と共有資源情報 302 から削除する。

【0178】

ステップ S918 では、VM 監視部 322 が仮想マシンの変更通知 332 から取得した移動先の業務サーバ 115 の仮想化部 211 から、移動先の仮想マシン 212 の IP アドレス、仮想マシン 212 の識別子(番号)、業務サーバ 115 の識別子、移動先の仮想マシン 212 が他の仮想マシンと共有する計算機資源の識別子を取得する。そして、VM 監視部 322 が、移動先の仮想マシン 212 の IP アドレス、仮想マシン 212 の識別子(番号)、業務サーバ 115 の識別子を、通信フロー情報 301 に設定する。

10

【0179】

ステップ S919 では、VM 監視部 322 は、移動先の仮想マシン 212 を実行する業務サーバ 115 から取得した他の仮想マシンと共有する計算機資源の識別子を共有資源情報 302 に設定する。

【0180】

上記ステップ S915 ~ S919 により、ネットワーク監視サーバ 118 は、受信した仮想マシン変更通知 332 で移動された仮想マシン 212 の一つについて、通信フロー情報 301 と共有資源情報 302 を更新し、移動元の情報を移動先の情報に書き換える。

20

【0181】

次に、ステップ S920 では、ネットワーク監視サーバ 118 が、業務サーバの変更通知 331 または仮想マシンの変更通知 332 に含まれる全ての仮想マシン 212 について処理が完了したか否かを判定する。未処理の仮想マシン 212 があれば、ステップ S901 に戻って上記処理を繰り返す。一方、全ての仮想マシン 212 について処理が完了していれば当該フローチャートを終了する。

【0182】

上記処理により、データセンタ 110 内で業務サーバ 115 や仮想マシン 212 の変更があった場合には、ネットワーク監視サーバ 118 が通信フロー情報 301 及び共有資源情報 302 を更新する。そして、ネットワーク監視サーバ 118 は、更新した通信フロー情報 301 を顧客サイト 101 のルータ 102 とデータセンタ 110 のルータ 120 に送信し、監視対象の通信を更新させる。

30

【0183】

以上のように、本実施形態によれば、業務サーバ 115 や仮想マシン 212 の構成が変更されると、通信フロー情報 301 と共有資源情報 302 を更新し、常に最新の監視条件をルータ 102、120 に設定することができる。

【0184】

そして、ネットワーク監視サーバ 118 は、ルータ 102、120 の監視部 103、121 から遅延通知 312 を受信すると、通信フロー情報 301 を参照して遅延が増大した業務サーバ 115 x と仮想マシン 212 - y を被擬対象として特定する。そして、ネットワーク監視サーバ 118 は、被擬対象の仮想化部 211 から、物理的な計算機資源(CPU、NIC)の性能監視情報と、仮想的な計算機資源(仮想CPU、仮想NIC)の性能監視情報を取得し、遅延が増大した要因を特定する。さらに、ネットワーク監視サーバ 118 は、被擬対象仮想マシン 212 - y と物理的な計算機資源を共有する他の仮想マシンについても、当該他の仮想マシンの仮想化部 211 から、物理的な計算機資源の性能監視情報と、仮想的な計算機資源の性能監視情報を取得し、遅延が増大した要因を特定する。

40

【0185】

これにより、ネットワーク監視サーバ 118 は、WAN 150、データセンタ 110 内の業務ネットワーク、業務サーバ 115、業務アプリケーション 262 の何れに遅延が増

50

大した要因が存在するのかを迅速かつ高精度で検出することが可能となる。

【0186】

<第2の実施形態>

図11は第2の実施形態を示し、業務サーバ115のブロック図である。第2の実施形態の業務サーバ115は、前記第1の実施形態の仮想化部211内のCPU性能情報収集部242を、仮想マシン212のOS261上で実行される仮想CPUエージェントとしたもので、前記第1実施形態のCPU性能情報収集部242を仮想化部211からOS261上に移動した変形例である。なお、その他の構成は前記第1の実施形態と同様である。

【0187】

各仮想マシン212-1~212-nのOS261-1~261-n上では、前記第1実施形態の業務アプリケーション262-1~262-nが実行されるのに加え、本第2実施形態では、仮想CPU監視エージェント1101-1~1101-nが実行される。仮想CPU監視エージェント1101-1~1101-nは同一の構成であるので、以下では図示の仮想CPU監視エージェント1101-nについてのみ説明する。なお、仮想マシン212-1~212-n及びOS261-1~261-nの総称は、それぞれ仮想マシン212、OS261とする。

【0188】

仮想CPU監視エージェント1101-nは、各仮想マシン212のOS261に割り当てられた仮想CPUの性能監視情報を収集するCPU性能情報収集部242と、収集した仮想CPUの性能監視情報を格納するCPU性能統計情報244と、性能監視情報取得要求313からの指令に応じてCPU性能統計情報244を取得し、性能監視情報通知1104bとしてネットワーク監視サーバ118に送信する情報切り出し部2510と、を含む。

【0189】

CPU性能情報収集部242は、所定の周期(例えば、10msec)で仮想CPUの性能監視情報(例えば、使用率)を取得する。仮想CPUの性能監視情報は、OS261から取得してもよいし、OS261のログ(図中sarllog)から取得してもよい。

【0190】

そして、CPU性能情報収集部242は、取得した仮想CPUの性能監視情報をCPU性能統計情報244に格納する。なお、CPU性能統計情報244には性能監視情報を収集した時刻のタイムスタンプを保持してもよい。また、CPU性能統計情報244は、前記第1実施形態と同様に、所定時間(例えば、10分間または20分間)の仮想CPUの性能監視情報が所定の周期毎に格納される。

【0191】

ネットワーク監視サーバ118が性能監視情報取得要求313を送信すると、業務サーバ115では、情報切り出し部251あるいは情報切り出し部2510が受信する。情報切り出し部251は、性能監視情報取得要求313の収集対象がNICの場合に、前記第1の実施形態と同様にしてNIC稼働統計情報243を性能監視情報通知1104としてネットワーク監視サーバ118に送信する。情報切り出し部2510は、性能監視情報取得要求313の収集対象がCPUである場合に、CPUの性能監視情報を送信するように指令する。指令を受けた仮想マシン212-1~212-nの情報切り出し部2510は、CPU稼働統計情報244を性能監視情報通知1104bとしてネットワーク監視サーバ118に送信する。各仮想マシン212-1~212-nでは、仮想CPUエージェント1101-1~1101-nがそれぞれ仮想CPUの性能監視情報を取得してCPU性能統計情報244に格納する。ネットワーク監視サーバ118は、CPUの性能監視情報を取得する仮想マシン212の識別子を性能監視情報取得要求313で指定して業務サーバ115の仮想マシン212の情報切り出し部2510に通知する。仮想マシン212の仮想CPUエージェント1101は、情報切り出し部2510からCPU性能統計情報244を応答する。

10

20

30

40

50

【 0 1 9 2 】

以上のように、各仮想マシン 2 1 2 に仮想 CPU エージェント 1 1 0 1 - 1 ~ 1 1 0 1 - n をそれぞれ配置することで、ネットワーク監視サーバ 1 1 8 は、指定した仮想マシン 2 1 2 のみの CPU の性能監視情報を取得することが可能となる。なお、物理 CPU 2 2 2 の性能監視情報については、仮想化部 2 1 1 に物理 CPU 専用の性能情報収集部を設けてもよい。

【 0 1 9 3 】

本第 2 実施形態においても、前記第 1 実施形態と同様に、ネットワーク監視サーバ 1 1 8 が、業務アプリケーション 2 6 2 を実際に利用している通信のみを監視し、通信先 IP アドレス 5 0 1 からデータセンタ 1 1 0 内で遅延の増大が発生した部位（業務サーバ 1 1 5 x 及び仮想マシン 2 1 2 - y）を特定する。さらに、ネットワーク監視サーバ 1 1 8 は、被擬対象の仮想マシン 2 1 2 - y と物理的な計算機資源を共有する部位（物理計算機、仮想化部 2 1 1、他の仮想マシン 2 1 2）についても性能監視情報を取得して遅延増大の要因となった部位（性能低下部位）を特定することができる。

【 0 1 9 4 】

なお、上記第 2 実施形態では、ネットワーク監視サーバ 1 1 8 が性能監視情報取得要求 3 1 3 を送信すると、業務サーバ 1 1 5 では、情報切り出し部 2 5 1 あるいは情報切り出し部 2 5 1 0 が受信する例を示したが、情報切り出し部 2 5 1 が性能監視情報取得要求 3 1 3 を情報切り出し部 2 5 1 0 に転送するようにしてもよい。すなわち、情報切り出し部 2 5 1 は、性能監視情報取得要求 3 1 3 が CPU であれば、要求された仮想マシン 2 1 2 - 1 ~ 2 1 2 - n の情報切り出し部 2 5 1 0 に対して CPU の性能情報を送信するように指令する。指令を受けた仮想マシン 2 1 2 - 1 ~ 2 1 2 - n の情報切り出し部 2 5 1 0 は、CPU 性能統計情報 2 4 4 を性能監視情報通知 1 1 0 4 b としてネットワーク監視サーバ 1 1 8 に送信する。なお、情報切り出し部 2 5 1 は、性能監視情報取得要求 3 1 3 が NIC であれば、前記第 1 実施形態と同様にして NIC 性能統計情報 2 4 3 を性能監視情報通知 1 1 0 4 としてネットワーク監視サーバ 1 1 8 に送信する。

【 0 1 9 5 】

< 第 3 の実施形態 >

図 1 2 は第 3 の実施形態を示し、ルータ 1 2 0 0 のブロック図である。本第 3 の実施形態のルータ 1 2 0 0 は、前記第 1 実施形態の図 3 に示したネットワーク監視サーバ 1 1 8 の機能要素を、ルータ 1 2 0 に含めたもので、処理能力低下の要因特定部を備えたネットワーク装置として機能させることができる。

【 0 1 9 6 】

ルータ 1 2 0 0 のハードウェア資源 1 2 1 0 は、CPU 1 2 2 1、メモリ 1 2 2 3、記憶装置 1 2 2 4 及び複数のポートを備えた通信処理部 1 2 2 2 から構成される。

【 0 1 9 7 】

前記第 1 実施形態の通信監視部 1 2 1 と図 3 に示したネットワーク監視サーバ 1 1 8 の各機能要素は、ルータ 1 2 0 0 の内部で接続されており、前記第 1 実施形態と同一のものに同一の符号を付して、前記第 1 実施形態と重複する説明は省略する。

【 0 1 9 8 】

本第 3 実施形態においても、前記第 1 実施形態と同様に、ルータ 1 2 0 0 が業務アプリケーション 2 6 2 を実際に利用している通信のみを監視し、通信先 IP アドレス 5 0 1 からデータセンタ 1 1 0 内で遅延の増大が発生した部位（業務サーバ 1 1 5 x 及び仮想マシン 2 1 2 - y）を特定する。さらに、ルータ 1 2 0 0 は、被擬対象の仮想マシン 2 1 2 - y と物理的な計算機資源を共有する部位（物理計算機、仮想化部 2 1 1、他の仮想マシン 2 1 2）についても性能監視情報を取得して遅延増大の要因となった部位（処理能力低下部位）を特定することができる。

【 0 1 9 9 】

なお、上記各実施形態では、ルータ 1 0 2 a ~ 1 0 2 c 及びルータ 1 2 0 で処理の遅延増大の発生を監視する例を示したが、通信先の IP アドレスと閾値 TH 1、TH 2 により

10

20

30

40

50

処理の遅延増大の発生を検知可能なネットワーク装置であればよい。この種のネットワーク装置としては、L3スイッチやロードバランサなどを用いることができる。

【0200】

また、上記各実施形態では、PaaSに本発明を適用した例を示したがSaaS (Software as a Service) やIaaS (Infrastructure as a Service) に適用することができる。

【0201】

また、上記各実施形態では、処理要求を受信した時刻から処理応答を受信して転送した時刻までを遅延時間として算出したが、処理要求を受信した時刻から処理応答を受信した時刻までを遅延時間として算出してもよく、あるいは、処理要求を転送した時刻から処理応答を受信して転送した時刻までを遅延時間として算出してもよい。

10

【0202】

また、上記各実施形態では、顧客サイト101のルータ102とデータセンタ110のルータ120の双方で遅延増大の検出を行う例を示したが、データセンタ110のルータ120のみで遅延増大の検出を行って、データセンタ110内の処理能力の低下要因を特定するようにしてもよい。

【産業上の利用可能性】

【0203】

以上のように、本発明はWANを介してクラウドコンピューティングを提供する計算機システム及びクラウドコンピューティングの管理方法及び管理プログラムに適用することができる。また、クラウドコンピューティングを提供する計算機システム内の処理能力低下要因特定装置として提供することもできる。

20

【符号の説明】

【0204】

- 101a ~ 101c 顧客サイト
- 102a ~ 102c ルータ
- 103a ~ 103c 遅延監視部
- 104a ~ 104c クライアント端末
- 110 データセンタ
- 120 ルータ
- 121 遅延監視部
- 114a、114b L2スイッチ
- 115a ~ 115d 業務サーバ
- 116 ストレージ装置
- 118 ネットワーク監視サーバ
- 119 ネットワーク監視端末
- 210 ハードウェア資源
- 211 仮想化部
- 212 - 1 ~ 212 - n 仮想マシン
- 241 NIC性能情報収集部
- 242 CPU性能情報収集部
- 251 情報切り出し部
- 261 - 1 ~ 261 - n OS
- 262 - 1 ~ 262 - n 業務アプリケーション
- 301 通信フロー情報
- 302 共有資源情報
- 303 監視条件設定部
- 304 情報収集範囲特定部
- 305 情報取得指示部
- 306 要因特定部

30

40

50

【図4】

| | | |
|-----------|----------|------|
| 501 | 502 | 503 |
| 通信先IPアドレス | 業務サーバ番号 | VM番号 |
| 10.1.2.3 | APServ#1 | VM#1 |
| 10.1.2.4 | APServ#1 | VM#2 |
| 10.2.1.1 | APServ#2 | VM#1 |
| ... | ... | ... |

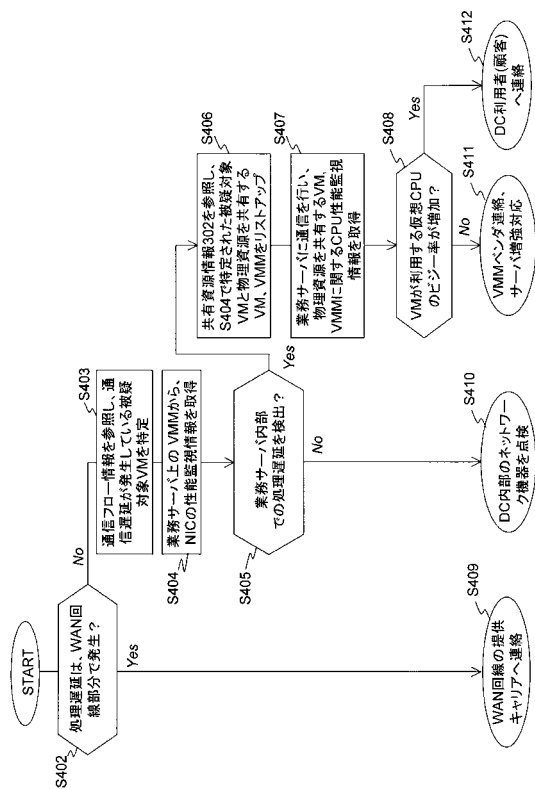
301 通信フロー情報

【図5】

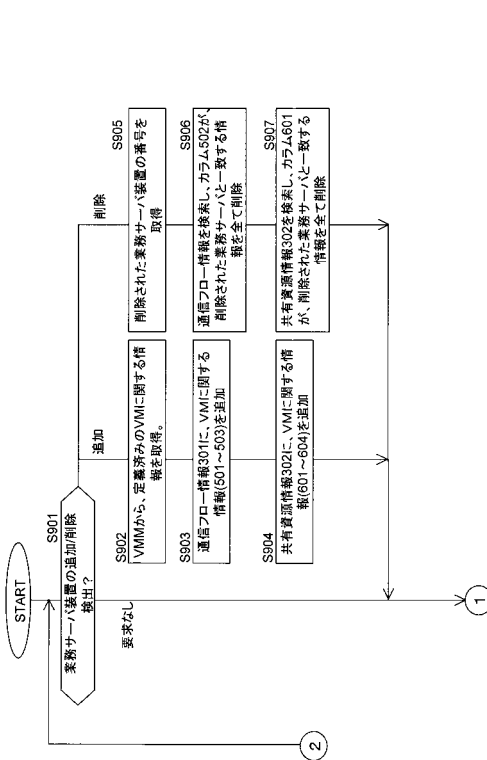
| | | | |
|----------|------|-----------|--------|
| 601 | 602 | 603 | 604 |
| 業務サーバ番号 | VM番号 | ストレージ装置番号 | LU番号 |
| APServ#1 | VM#1 | RAID#1 | LU#101 |
| APServ#1 | VM#2 | RAID#1 | LU#102 |
| APServ#2 | VM#1 | RAID#1 | LU#201 |

302 共有資源情報

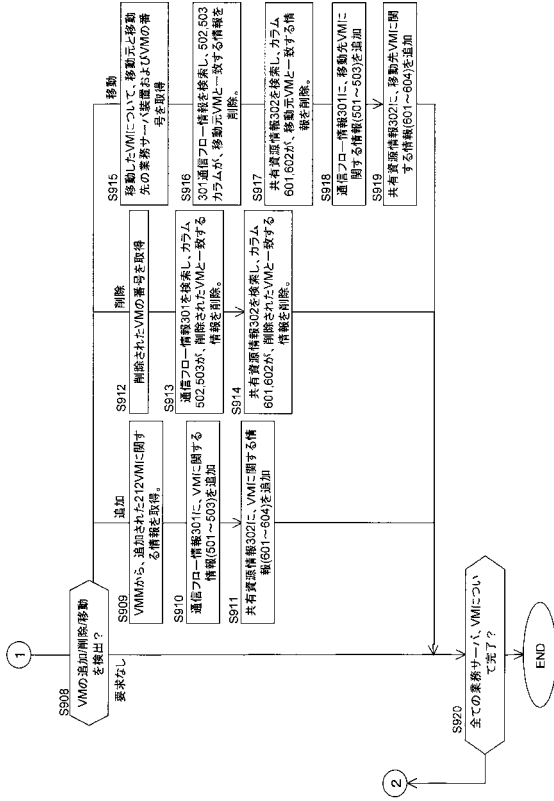
【図7】



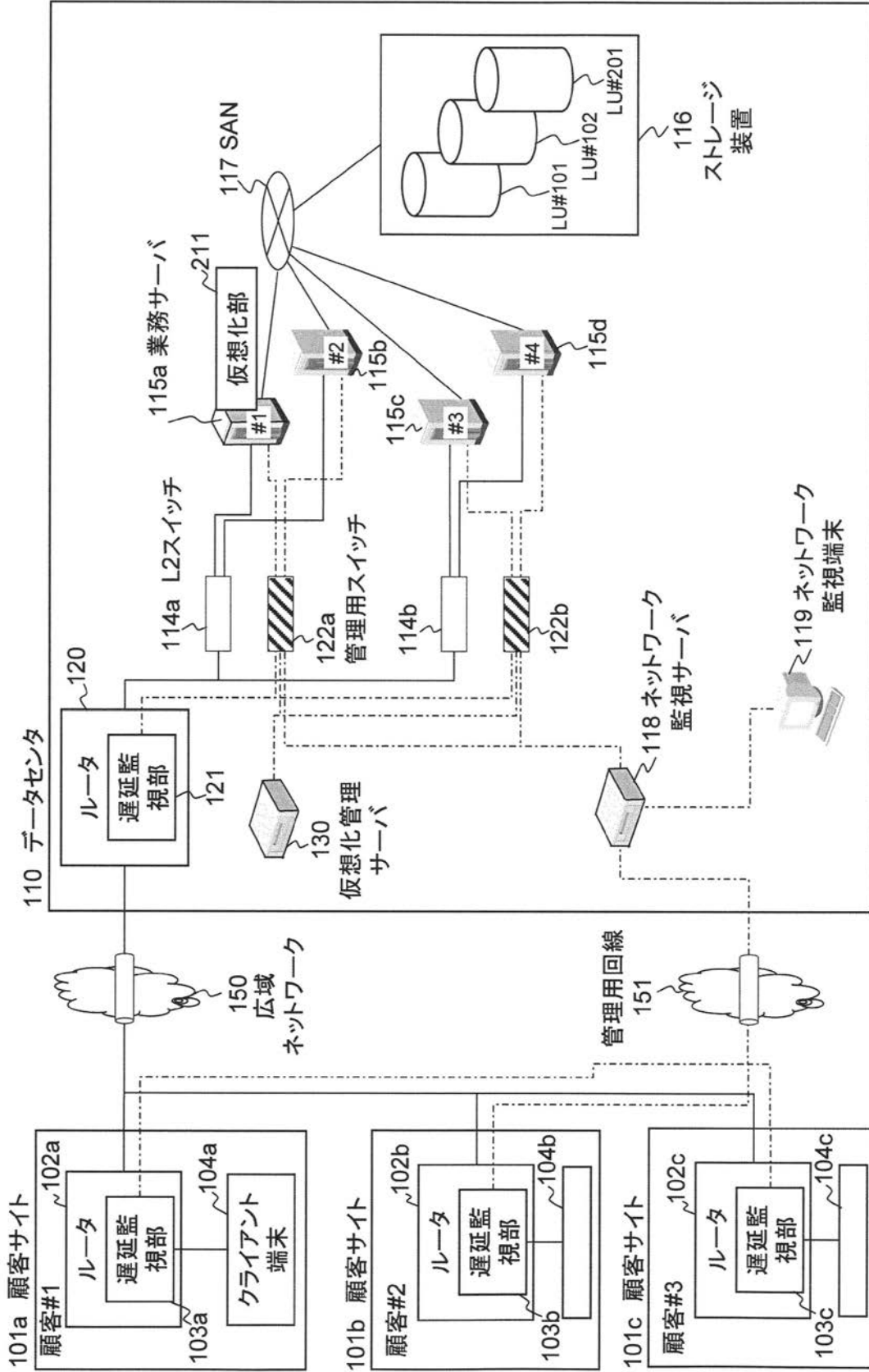
【図10A】



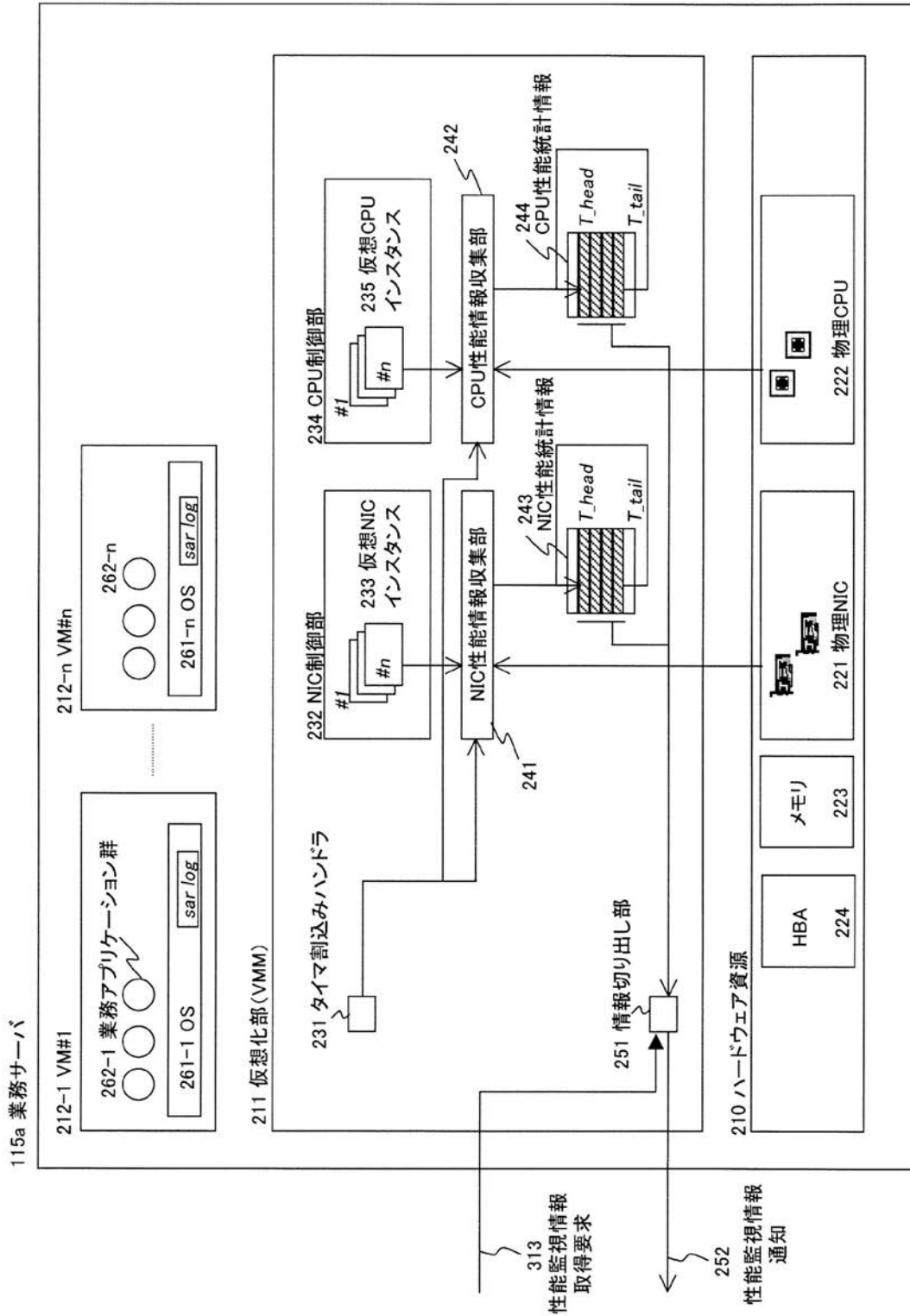
【 図 10 B 】



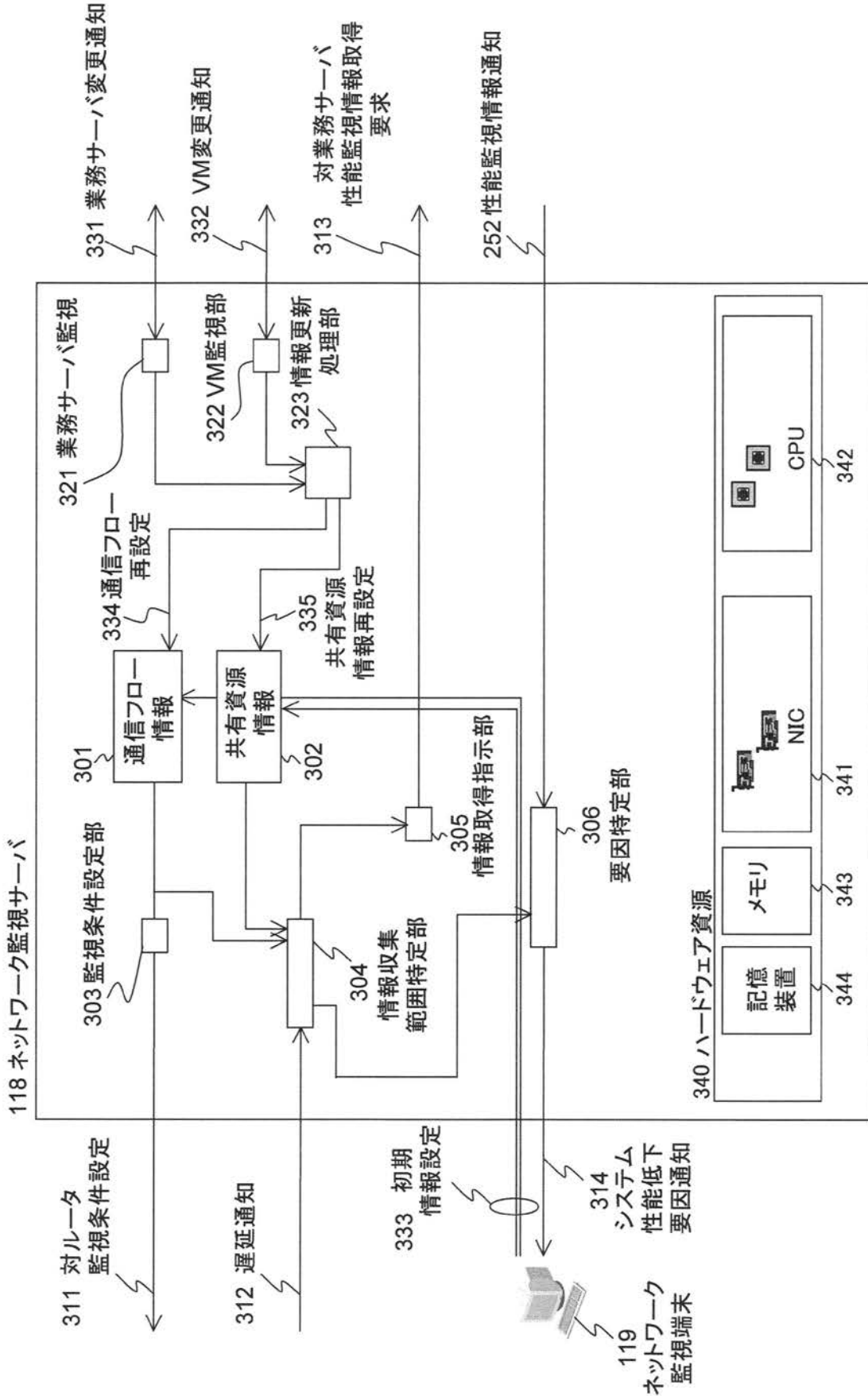
【 図 1 】



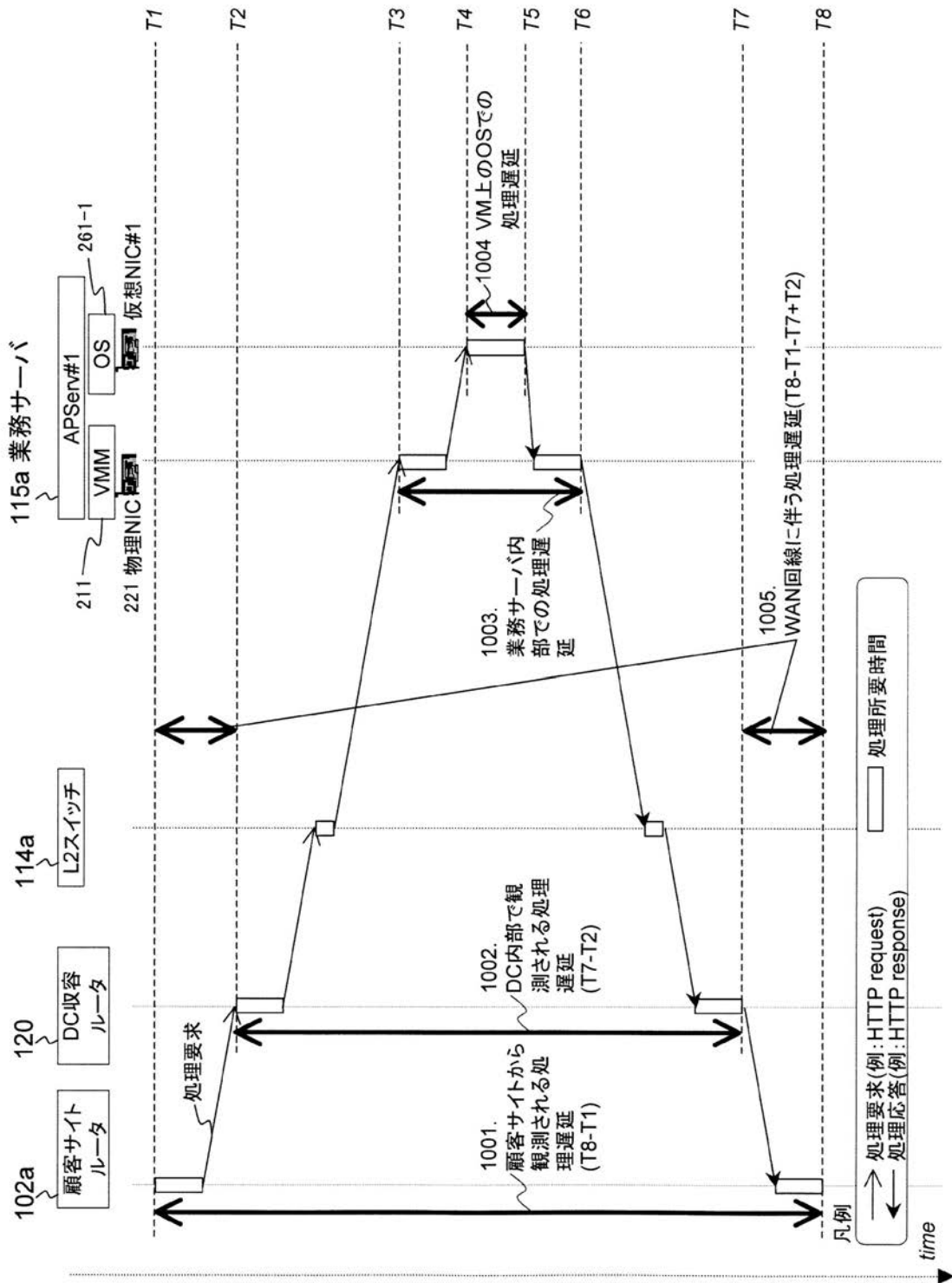
【図2】



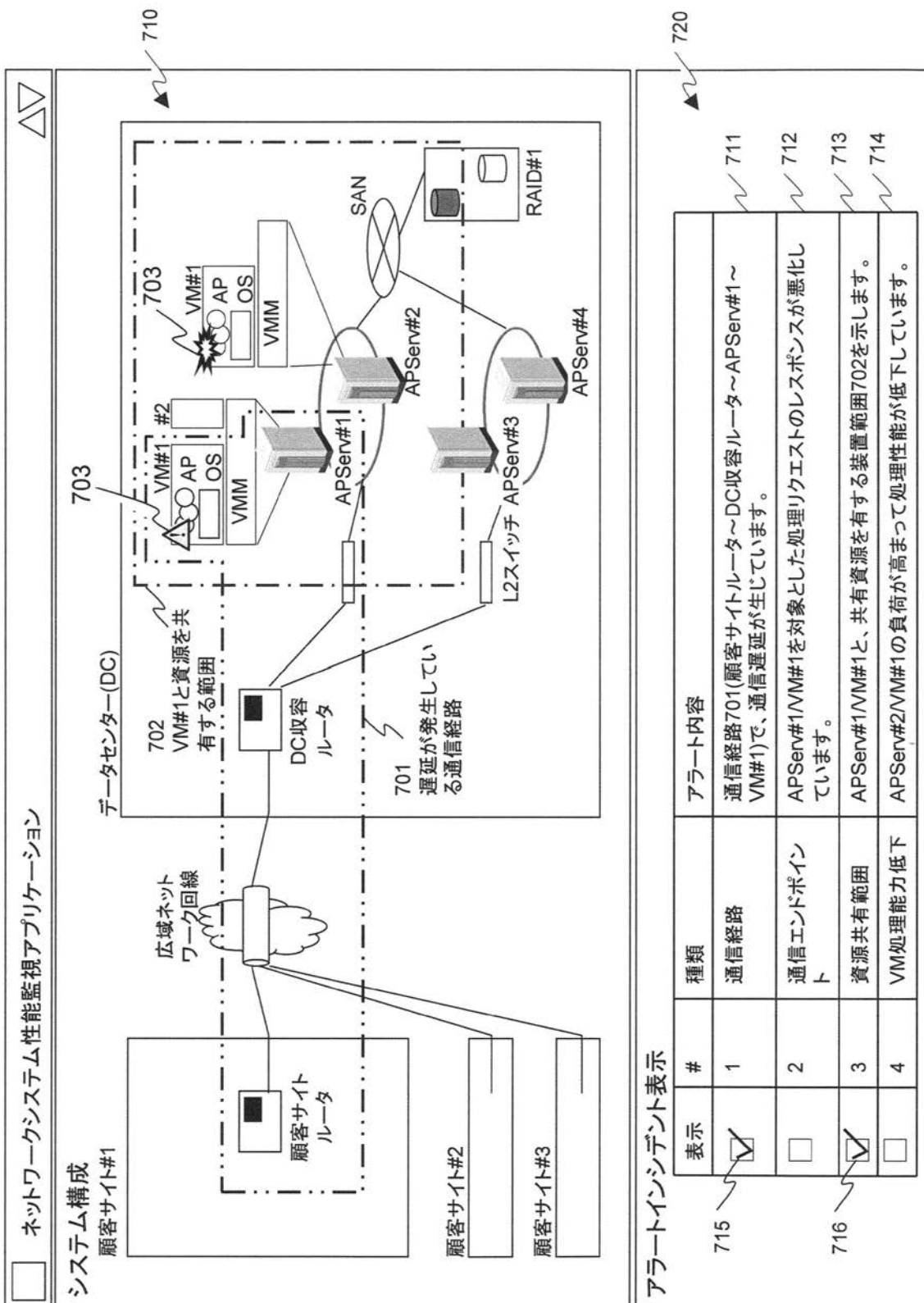
【 図 3 】



【 図 6 】



【 図 8 】



ネットワークシステム性能監視アプリケーション

システム構成
顧客サイト#1

広域ネットワーク回線

データセンター(DC)

顧客サイト
ルータ

顧客サイト#2

顧客サイト#3

DC 收容
ルータ

702
VM#1と資源を共有する範囲

703
VM#1
AP
OS
VMM

703
VM#2
AP
OS
VMM

701
遅延が発生している通信経路

710

APServ#1

APServ#2

APServ#3

APServ#4

L2スイッチ

SAN

RAID#1

アラートインシデント表示

| 表示 | # | 種類 | アラート内容 |
|-------------------------------------|---|-----------|---|
| <input checked="" type="checkbox"/> | 1 | 通信経路 | 通信経路701(顧客サイトルータ~DC收容ルータ~APServ#1~VM#1)で、通信遅延が生じています。 |
| <input type="checkbox"/> | 2 | 通信エンドポイント | APServ#1/VM#1を対象とした処理リクエストのレスポンスが悪化しています。 |
| <input checked="" type="checkbox"/> | 3 | 資源共有範囲 | APServ#1/VM#1と、共有資源を有する装置範囲702を示します。 |
| <input type="checkbox"/> | 4 | VM処理能力低下 | APServ#2/VM#1の負荷が高まって処理性能が低下しています。 |

715

716

711

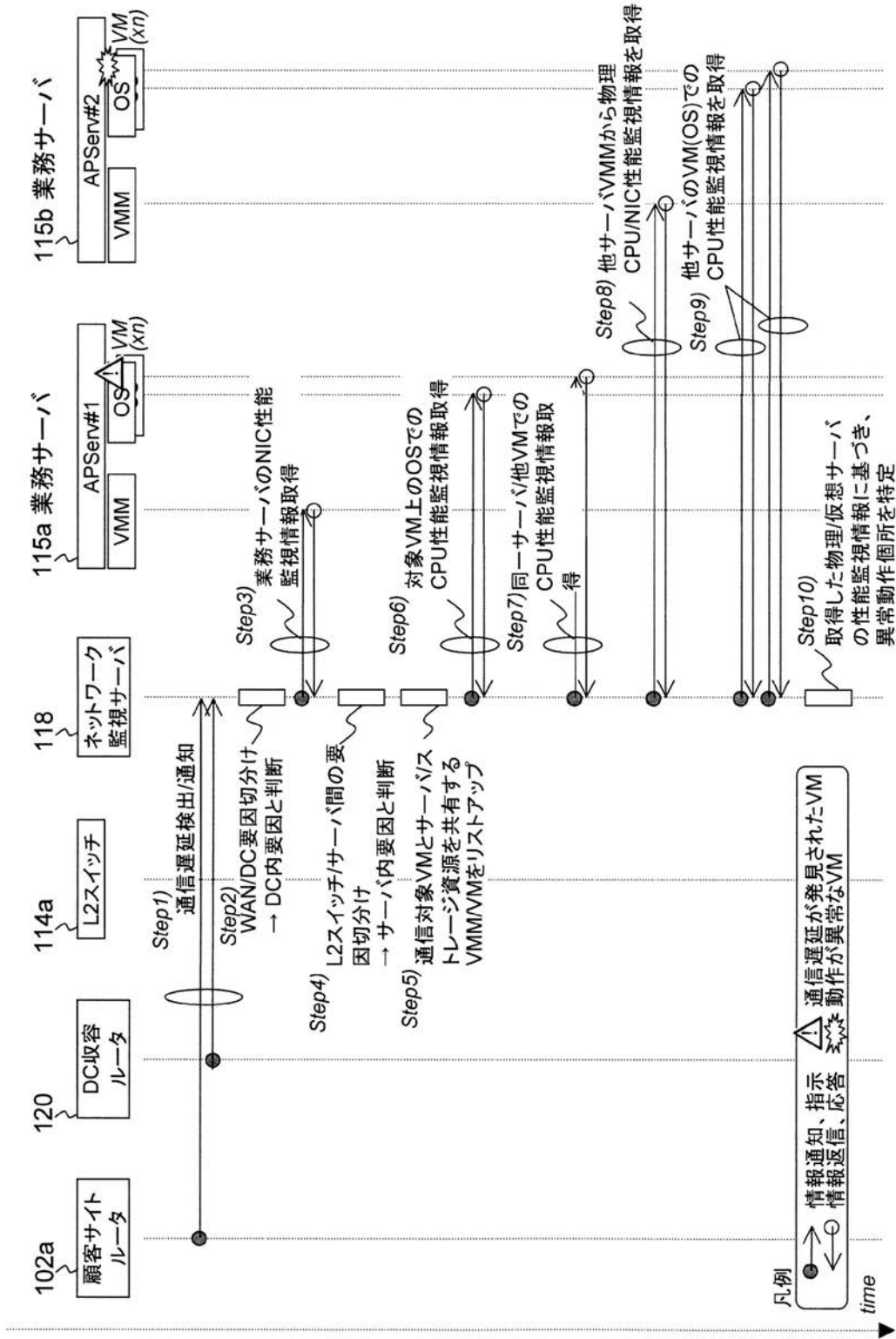
712

713

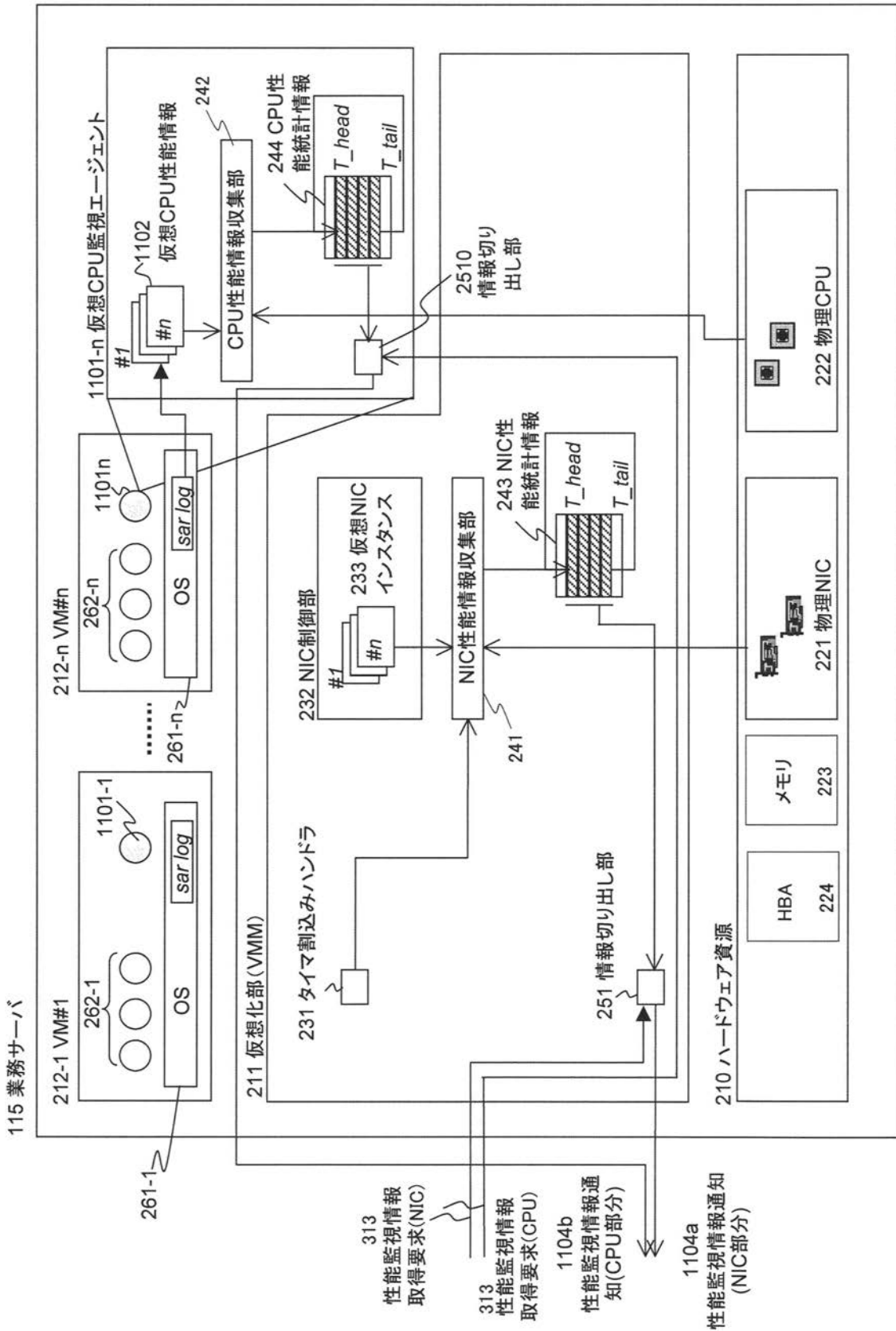
714

720

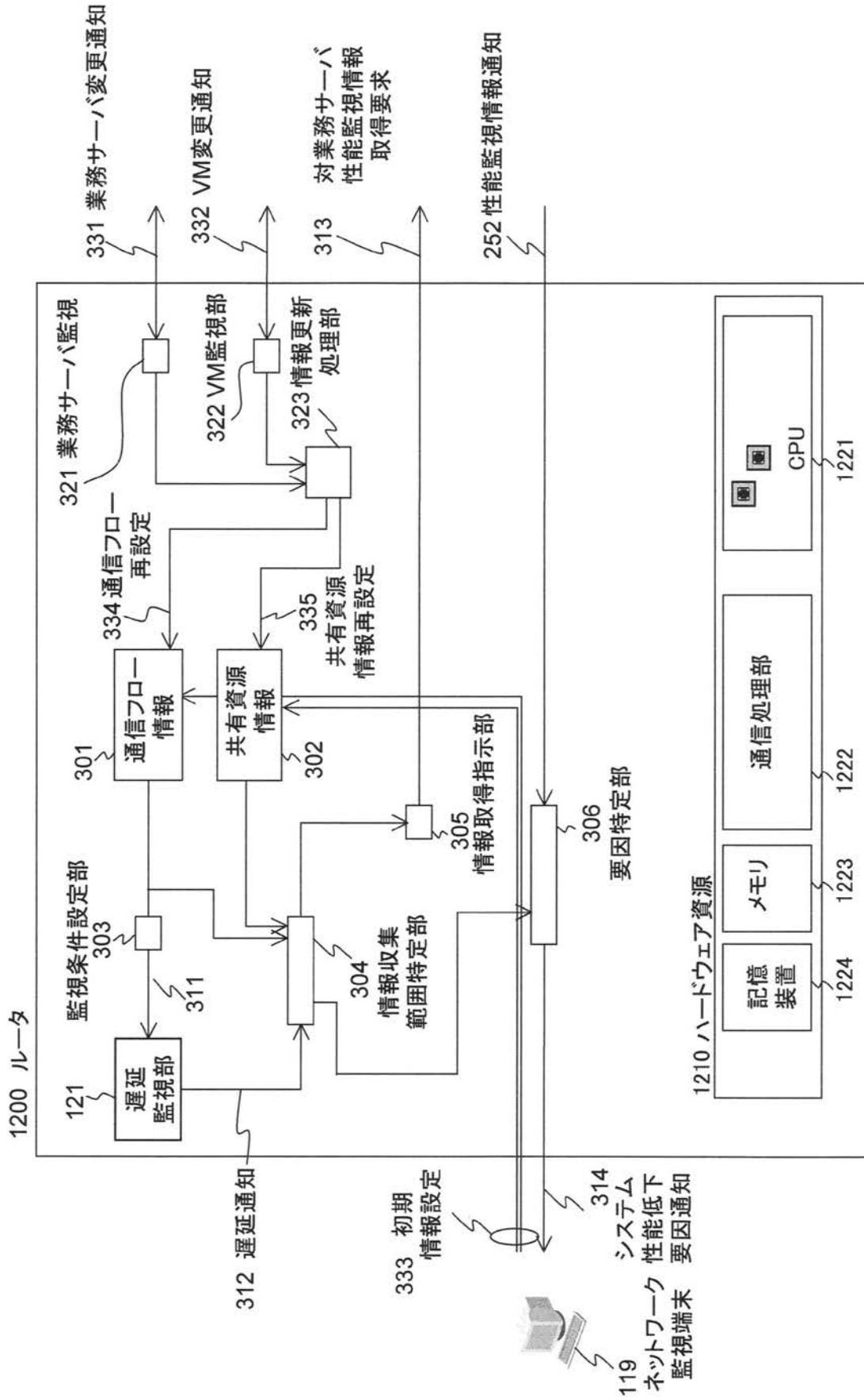
【図9】



【 図 1 1 】



【 図 1 2 】



フロントページの続き

審査官 相崎 裕恒

- (56)参考文献 特開2008-293117(JP,A)
特開2009-080704(JP,A)
特表2003-508849(JP,A)
国際公開第2005/041038(WO,A1)
特開2004-104540(JP,A)

(58)調査した分野(Int.Cl., DB名)

G06F 9/46 - 9/54, 11/28 - 11/34, 13/00