

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第6714693号
(P6714693)

(45) 発行日 令和2年6月24日 (2020.6.24)

(24) 登録日 令和2年6月9日 (2020.6.9)

(51) Int. Cl.	F I
G 0 6 F 9/50 (2006.01)	G 0 6 F 9/50 1 5 0 C
G 0 6 F 21/16 (2013.01)	G 0 6 F 21/16

請求項の数 20 (全 25 頁)

(21) 出願番号	特願2018-517828 (P2018-517828)	(73) 特許権者	390009531
(86) (22) 出願日	平成28年11月21日 (2016.11.21)		インターナショナル・ビジネス・マシーンズ・コーポレーション
(65) 公表番号	特表2018-535480 (P2018-535480A)		INTERNATIONAL BUSINESS MACHINES CORPORATION
(43) 公表日	平成30年11月29日 (2018.11.29)		アメリカ合衆国10504 ニューヨーク州 アーモンク ニュー オーチャードロード
(86) 国際出願番号	PCT/IB2016/057007		New Orchard Road, Armonk, New York 10504, United States of America
(87) 国際公開番号	W02017/089943		
(87) 国際公開日	平成29年6月1日 (2017.6.1)	(74) 代理人	100108501
審査請求日	平成31年4月19日 (2019.4.19)		弁理士 上野 剛史
(31) 優先権主張番号	14/953, 353		
(32) 優先日	平成27年11月29日 (2015.11.29)		
(33) 優先権主張国・地域又は機関	米国 (US)		

最終頁に続く

(54) 【発明の名称】 複数のデプロイメントロケーションにわたるアプリケーションのセキュア・デプロイメント

(57) 【特許請求の範囲】

【請求項 1】

デプロイメントロケーションへのアプリケーションのセキュア・デプロイメントのためのコンピュータ実装方法であって、

分析のために前記アプリケーションを提供することであって、前記アプリケーションが、異なるロケーションにデプロイできる処理ノードに分割されることが可能であり、前記アプリケーションが、データ・アスペクトに対するデプロイメント制約を定義するアノテーションを含んでいるメッセージ・モデルに基づいてメッセージを処理し、前記データ・アスペクトがメッセージ全体、あるいは前記メッセージのデータ・フィールド、データ要素、またはデータ構造を含む、前記提供することと、

前記デプロイメント制約を有するデータ・アスペクトを参照する処理ノードを識別するために前記アプリケーションを分析することと、

前記参照されているデータ・アスペクトの前記デプロイメント制約に基づいて、処理ノードのデプロイメントに関する制限を決定することと、

前記決定された制限に従って前記アプリケーションの各処理ノードをデプロイすることと

を含む、コンピュータ実装方法。

【請求項 2】

前記分析することおよび前記決定することが前記アプリケーションのデプロイメントで動的に実行される、請求項 1 に記載の方法。

【請求項 3】

前記分析することおよび前記決定することが前記アプリケーションの前記デプロイメントよりも前に実行され、前記方法が、

前記処理ノードによって参照されるデータ・アスペクトに関連するメッセージ・モデル内でアノテートされたデプロイメント制約に対応する制限メタデータを使用して当該処理ノードにマークを付けることを含む、請求項 1 に記載の方法。

【請求項 4】

デプロイすることが、前記制限メタデータを読み取り、前記制限に従って各処理ノードをデプロイすることによって、マークが付けられた処理ノードに対して実行される、請求項 3 に記載の方法。

10

【請求項 5】

前記デプロイメント制約を有するデータ・アスペクトを追跡することと、

前記デプロイメント制約を有するデータ・アスペクトが、デプロイメント制約を有していないターゲットデータ・アスペクトに移動したかどうかを決定することと、

前記ターゲットデータ・アスペクトがデプロイメント制約を有することを記録することを含む、請求項 1 に記載の方法。

【請求項 6】

前記アプリケーションを分析することが、前記デプロイメント制約を有するとしてデータ・アスペクトが追跡されているどうかを決定することを含む、請求項 5 に記載の方法。

【請求項 7】

前記メッセージ・モデル内でアノテートされた前記デプロイメント制約を決定するために前記メッセージ・モデルにアクセスすることを含む、請求項 1 に記載の方法。

20

【請求項 8】

前記データ・アスペクトに対するデプロイメント制約を決定するために追跡データにアクセスすることを含む、請求項 5 に記載の方法。

【請求項 9】

前記メッセージ・モデルと前記アプリケーションのコードとの間の論理的分離が提供され、デプロイメント制約が前記メッセージ・モデル内でのみ定義されることを可能にする、請求項 1 に記載の方法。

【請求項 10】

前記アプリケーションが、分散リソースにデプロイすることができる処理ノードを含んでいる分散アプリケーションである、請求項 1 に記載の方法。

30

【請求項 11】

前記アプリケーションが、1 つまたは複数のインバウンド・インターフェイスおよび 1 つまたは複数のアウトバウンド・インターフェイスを有する処理ノードを含む統合フローであり、前記データ・アスペクトを参照する処理ノードを識別するために前記アプリケーションを分析することが、インバウンド・インターフェイスまたはアウトバウンド・インターフェイスがデプロイメント制約を有する前記データ・アスペクトを含むかどうかを決定することを含む、請求項 1 に記載の方法。

【請求項 12】

前記アプリケーションが、ハイブリッド・クラウド環境内にデプロイされることが可能であり、前記デプロイメント制約が、前記ハイブリッド・クラウド環境内の、ローカルなクライアントのデプロイメント、オンプレミスのデプロイメント、企業内のデプロイメント、地理的位置内のデプロイメント、またはパブリック・クラウド内のデプロイメントのグループのうちの 1 つまたは複数を含むデプロイメントのロケーションに関連する、請求項 1 に記載の方法。

40

【請求項 13】

デプロイメントロケーションへのアプリケーションのセキュア・デプロイメントのためのシステムであって、

プロセッサおよびメモリを備え、前記プロセッサが、

50

分析のために前記アプリケーションを提供することであって、前記アプリケーションが、異なるロケーションにデプロイできる処理ノードに分割されることが可能であり、前記アプリケーションが、データ・アспектに対するデプロイメント制約を定義するアノテーションを含んでいるメッセージ・モデルに基づいてメッセージを処理し、前記データ・アспектがメッセージ全体、あるいは前記メッセージのデータ・フィールド、データ要素、またはデータ構造を含む、前記提供することと、

前記デプロイメント制約を有するデータ・アспектを参照する処理ノードを識別するために前記アプリケーションを分析することと、

前記参照されているデータ・アспектの前記デプロイメント制約に基づいて、処理ノードのデプロイメントに関する制限を決定することと、

前記決定された制限に従って前記アプリケーションの各処理ノードをデプロイすることと

を実行するように構成される、システム。

【請求項 14】

前記分析することおよび前記決定することが前記アプリケーションのデプロイメントで動的に実行される、請求項 13 に記載のシステム。

【請求項 15】

前記分析することおよび決定することが前記アプリケーションの前記デプロイメントよりも前に実行され、前記プロセッサが、前記処理ノードによって参照されるデータ・アспектに関連するメッセージ・モデル内でアノテートされたデプロイメント制約に対応する制限メタデータを使用して当該処理ノードにマークを付けるようにさらに構成される、請求項 13 に記載のシステム。

【請求項 16】

デプロイすることが、前記制限メタデータを読み取り、前記制限に従って各処理ノードをデプロイすることによって、マークが付けられた処理ノードに対して実行される、請求項 15 に記載のシステム。

【請求項 17】

前記プロセッサが、

前記デプロイメント制約を有するデータ・アспектを追跡することと、

前記デプロイメント制約を有するデータ・アспектが、デプロイメント制約を有していないターゲットデータ・アспектに移動したかどうかを決定することと、

前記ターゲットデータ・アспектがデプロイメント制約を有することを記録することを実行するようにさらに構成される、請求項 13 に記載のシステム。

【請求項 18】

前記アプリケーションを分析することが、デプロイメント制約を有するとして特定のデータのアспектが追跡されているかどうかを決定することを含む、請求項 17 に記載のシステム。

【請求項 19】

前記プロセッサが、前記メッセージ・モデル内でアノテートされた前記デプロイメント制約を決定するために前記メッセージ・モデルにアクセスするようにさらに構成される、請求項 13 に記載のシステム。

【請求項 20】

デプロイメントロケーションへのアプリケーションのセキュア・デプロイメントのためのコンピュータ・プログラムであって、前記コンピュータ・プログラムが、プログラム命令を備え、プロセッサによって実行可能な前記プログラム命令が、前記プロセッサに、

分析のために前記アプリケーションを提供することであって、前記アプリケーションが、異なるロケーションにデプロイできる処理ノードに分割されることが可能であり、前記アプリケーションが、データ・アспектに対するデプロイメント制約を定義するアノテーションを含んでいるメッセージ・モデルに基づいてメッセージを処理し、前記データ・アспектがメッセージ全体、あるいは前記メッセージのデータ・フィールド、データ要

10

20

30

40

50

素、またはデータ構造を含む、前記提供することと、

前記デプロイメント制約を有するデータ・アスペクトを参照する処理ノードを識別するために前記アプリケーションを分析することと、

前記参照されているデータ・アスペクトの前記デプロイメント制約に基づいて、処理ノードのデプロイメントに関する制限を決定することと、

前記決定された制限に従って前記アプリケーションの各処理ノードをデプロイすることと

を実行させる、コンピュータ・プログラム。

【発明の詳細な説明】

【技術分野】

10

【0001】

本発明は、複数のデプロイメントロケーションにわたるアプリケーションのセキュア・デプロイメントに関する。

【背景技術】

【0002】

IBM Integration Bus (IBMおよびIntegration BusはInternational Business Machines Corporationの商標である)などの製品は、エンタープライズ・サービス・バス(ESB:enterprise service bus)技術に基づく汎用統合基盤(universal integration foundation)のオプションを提供する。各実装は、任意の産業における任意のサイズのビジネスに関する、クラウド環境およびメインフレーム・サーバを含むプラットフォームの範囲をカバーする、異種情報技術環境での接続および変換を可能にするのに役立つ。

20

【0003】

特定の統合フローは、データが流れることができる場所に関連付けられた制限を有する可能性が高い極秘データを含んでいるメッセージに対する操作を実行することができる。例えば、特定のデータは企業のファイアウォール内に留まる必要があるか、または国外に出ることが許可されない場合がある。

【0004】

企業は、クラウド技術を利用することによって、弾力的にスケーリングして、需要に対処し、情報技術インフラストラクチャを削減および合理化し、運用のコストを削減し、システムをより高速、簡単、かつオンデマンドにデプロイすることができる。

30

【0005】

特定のエンドツーエンド統合アプリケーションまたはサービスはハイブリッド・クラウド環境内で実行される場合があり、ハイブリッド・クラウド環境では、一部の処理がパブリック・クラウド空間内で実行され、セキュア・データを使用する場合のある一部の処理が企業のファイアウォール内でオンプレミスで実行される。

【0006】

ファイアウォールの背後にあるシステムに接続するセキュア・コネクタが知られている。データベースなどのシステムの場合、統合を実行するためにセキュア・コネクタが必要になる。セキュア・コネクタによって、パブリック・クラウド空間内で実行されている統合アプリケーションを、企業のファイアウォールの背後でオンプレミスで実行されているアプリケーションに接続することが可能になる。

40

【発明の概要】

【発明が解決しようとする課題】

【0007】

複数のデプロイメントロケーションにわたるアプリケーションのセキュア・デプロイメントのための方法、システム、プログラムを提供する。

【課題を解決するための手段】

【0008】

本発明の一実施形態によれば、デプロイメントロケーションへのアプリケーションのセ

50

セキュア・デプロイメントのためのコンピュータ実装方法が提供され、このコンピュータ実装方法は、分析のためにアプリケーションを提供することであって、このアプリケーションが、異なるロケーションにデプロイできる処理ノードに分割されることが可能であり、このアプリケーションが、データ・アスペクト (aspect) に対するデプロイメント制約を定義するアノテーションを含んでいるメッセージ・モデルに基づいてメッセージを処理し、データ・アスペクトがメッセージ全体、あるいはメッセージのデータ・フィールド、データ要素、またはデータ構造を含む、提供することと、デプロイメント制約を有するデータ・アスペクトを参照する処理ノードを識別するためにアプリケーションを分析することと、参照されているデータ・アスペクトのデプロイメント制約に基づいて、処理ノードに関する制限を決定することと、決定された制限に従ってアプリケーションの各処理ノードをデプロイすることを含む。

10

【0009】

本発明の第2の実施形態によれば、デプロイメントロケーションへのアプリケーションのセキュア・デプロイメントのためのシステムが提供され、このシステムは、プロセッサと、定義された機能を提供するように配置された次のコンポーネントの機能を実行するためにコンピュータ・プログラム命令をプロセッサに提供するように構成されたメモリとを備え、それらのコンポーネントは、分析のためにアプリケーションを提供するための提供コンポーネントであって、このアプリケーションが、異なるロケーションにデプロイできる処理ノードに分割されることが可能であり、このアプリケーションが、データ・アスペクトに対するデプロイメント制約を定義するアノテーションを含んでいるメッセージ・モデルに基づいてメッセージを処理し、データ・アスペクトがメッセージ全体、あるいはメッセージのデータ・フィールド、データ要素、またはデータ構造を含む、提供コンポーネント、デプロイメント制約を有するデータ・アスペクトを参照する処理ノードを識別するためにアプリケーションを分析する分析コンポーネント、参照されているデータ・アスペクトのデプロイメント制約に基づいて、処理ノードのデプロイメントに関する制限を決定するための決定コンポーネント、決定された制限に従ってアプリケーションの各処理ノードをデプロイするためのデプロイメント・コンポーネントである。

20

【0010】

本発明の第3の実施形態によれば、デプロイメントロケーションへのアプリケーションのセキュア・デプロイメントのためのコンピュータ・プログラム製品が提供され、このコンピュータ・プログラム製品は、具現化されたプログラム命令を含んでいるコンピュータ可読記憶媒体を備え、プロセッサによって実行可能なこのプログラム命令は、プロセッサに、分析のためにアプリケーションを提供することであって、このアプリケーションが、異なるロケーションにデプロイできる処理ノードに分割されることが可能であり、このアプリケーションが、データ・アスペクトに対するデプロイメント制約を定義するアノテーションを含んでいるメッセージ・モデルに基づいてメッセージを処理し、データ・アスペクトがメッセージ全体、あるいはメッセージのデータ・フィールド、データ要素、またはデータ構造を含む、提供することと、デプロイメント制約を有するデータ・アスペクトを参照する処理ノードを識別するためにアプリケーションを分析することと、参照されているデータ・アスペクトのデプロイメント制約に基づいて、処理ノードのデプロイメントに関する制限を決定することと、決定された制限に従ってアプリケーションの各処理ノードをデプロイすることとを実行させる。

30

40

【0011】

本発明で説明される態様は、アプリケーションを例えば分散環境またはハイブリッド・クラウド環境にデプロイすることを望む顧客に、デプロイメント・モデルをシンプルかつ簡単に使用できるという利点を提供する。

【0012】

本発明と見なされる対象は、本明細書の最後の部分において詳細に指摘され、明確に特許請求される。本発明は、添付の図面と併せて読まれたときに、以下の詳細な説明を参照することによって、処理の構造および方法に関して、本発明の対象、特徴、および利点と

50

共に、最もよく理解することができる。

【0013】

以下の図面を参照し、単に例として本発明の実施形態例について説明する。

【図面の簡単な説明】

【0014】

【図1】本発明に記載された方法の実施形態例のフロー図である。

【図2】本発明に記載された方法の実施形態例のフロー図である。

【図3】本発明に記載された方法のさらに詳細な実施形態例のフロー図である。

【図4】本発明に記載されたシステムの実施形態例のブロック図である。

【図5】本発明が実装されてよいコンピュータ・システムの実施形態のブロック図である

10

。

【図6】本発明に記載された方法を示す、統合環境内のメッセージ・フローのデプロイメントの例の概略図である。

【図7】本発明に記載された方法を示す、統合環境内のメッセージ・フローのデプロイメントの例の概略図である。

【図8】本発明に記載された、定義された追跡の態様を示すメッセージ・フローのデプロイメントの第2の例の概略図である。

【図9】本発明が実装されてよいコンピュータ・システムまたはクラウド・サーバの実施形態のブロック図である。

【図10】本発明が実装されてよいクラウド・コンピューティング環境の概略図である。

20

【図11】本発明が実装されてよいクラウド・コンピューティング環境の抽象モデル・レイヤの図である。

【発明を実施するための形態】

【0015】

説明を簡単かつ明確にするために、図に示された各要素の縮尺は、必ずしも一定ではないということが理解されるであろう。例えば、一部の要素の寸法は、明確に示すために、他の要素よりも誇張されている場合がある。さらに、適切であると見なされる場合、参照番号は、対応する特徴または類似する特徴を示すために、図間で繰り返されることがある。

。

【0016】

30

情報は、複数のハードウェア・プラットフォームおよびソフトウェア・プラットフォームにまたがって、全く異なるアプリケーション間を流れることが必要になる場合がある。これをサポートする1つのアーキテクチャは、サービス指向アーキテクチャにおいてアプリケーションとサービスの間の統合された接続を提供するエンタープライズ・サービス・バス・アーキテクチャである。IBM Integration Bus（以前の名称はWebSphere Message Brokerであり、IBMおよびWebSphereはInternational Business Machines Corporationの商標である）は、そのようなアーキテクチャの例であり、ビジネス情報を、データにルールが適用され、情報をルーティングおよび変換するための統合ノード（メッセージ・ブローカーとも呼ばれる）を介して成長する統合アプリケーションとして、

40

流すことができるようにする。

【0017】

その他のアーキテクチャは分散コンピューティングを含むことができ、分散コンピューティングでは分散システムがソフトウェア・システムであり、このソフトウェア・システムにおいて、コンポーネントがネットワーク・コンピュータ上に配置され、メッセージを渡すことによって通信し、それらの動作を調整する。分散アプリケーションは、分散コンピューティング・アーキテクチャ全体で処理されてよい。

【0018】

記載された方法およびシステムは、ハイブリッド・クラウド環境を使用することを含めてさまざまなロケーションにデプロイされてよい、統合フローまたは統合アプリケーショ

50

ンの分野において説明される。ただし、等価な方法およびシステムが分散コンピューティング環境に適用されてよいということが、当業者によって理解されるであろう。

【0019】

記載された方法およびシステムでは、例えばメッセージ・モデルの形態であってよいデータ構造の記述またはモデルが、特定の制限を有するフィールドまたは構造、あるいは構造内の要素などのアスペクトを識別するためにアノテートされる。例えば、特定のフィールドまたは構造内のデータは、企業の構内に制限されること、企業のファイアウォール内に制限されること、国に制限されること、または制限されず、パブリック・クラウドに自由に入れることがある。

【0020】

その後、統合アプリケーションは、アプリケーションの特定の処理が作用するデータ・フィールドまたはデータ構造を決定するために、分析される。この分析は、メッセージ・モデル内で提供される制限に基づいて、さまざまな制限を使用して実行される場合のある処理ノードを識別することができる。これらの制限は、処理を、メッセージ・モデル内で定義された制限に対応する特定のロケーションまたはロケーションのカテゴリに制限することができる。処理ノードには、制限を示すメタデータを使用してマークが付けられてよい。

【0021】

分析および制限メタデータ (restricting metadata) のマーキングは、アプリケーションが開発され、アプリケーションのノード内で制限メタデータにマークが付けられてパッケージ化されるときに実行されてよい。あるいは、これは、アプリケーションのデプロイ時に実行されてよく、その場合、メタデータはノードでマークが付けられなくてよく、代わりにノードは、適用可能な制限に従ってデプロイされてよい。

【0022】

統合アプリケーションがデプロイされるときに、処理ノードが処理しているデータ・フィールドまたはデータ構造に基づいて、処理ノードが環境内で適切にデプロイされる。

【0023】

有利なことに、最高情報セキュリティ責任者 (CISO: Chief Information Security Officer) またはその他の適切な管理者は、データ・セキュリティに関して前もって制限を設定することができ、その後、それらの制限はメッセージ・モデルに適用される。その後、アプリケーション開発者または統合開発者 (integration developer) および管理者は、データに関して存在している制限について詳細な知識を有する必要がある。これによって、ハイブリッド・クラウド環境内でより効率的にアプリケーションの開発および管理を行い、コストおよび複雑さを低減する。

【0024】

データが安全に (すなわち、オンプレミスで) 処理されることが可能であるか、または安全性の低い環境 (例えば、クラウド) 内で処理されてよい、データを処理するためのシステム内のデプロイメント・システムは、セキュリティまたはプライバシーに関連する制限メタデータ (ノード内でマークが付けられるか、またはリアルタイムに生成される) を調べることによって処理を分散することができ、ルールに基づいて、そのデータの特定の部分を、より安全な環境内で処理されることに制限しながら、機密性の低いデータを安全性の低い環境内で処理することができる。

【0025】

この方法は、メッセージ・モデルを拡大すること、および、それをアプリケーション分析と連携して使用して、分散アプリケーションのさまざまな部分の適切なデプロイメントロケーションであり、後で処理が行われる必要があるロケーションを決定することについて説明する。記載された方法およびシステムは、データの伝搬に対する制限が適切な設計者によってメッセージ・モデル・レベルで設定されるため、開発者がそのような制限について知る必要がないように、メッセージ・モデルとコードの間の論理的分離を提供する。

【0026】

一般に、メッセージ・モデルはコードとメッセージの記述の間の分離を提供する。この分離は、セキュア・データにアクセスするアプリケーションの、ハイブリッド・クラウド環境へのデプロイメントにおいて利益を得るために使用される。

【0027】

図1および2は、記載された方法の2つの実施形態例を示すフロー図100、150を、1つはアプリケーションの開発で、もう1つはそのアプリケーションのデプロイメントで示している。図1を参照すると、フロー図100は、記載された方法の実施形態例を示しており、複数のシステムにまたがってデプロイされてよいアプリケーションのアプリケーション開発段階で実行されてよい。

【0028】

準備手順として、メッセージ・モデルは、メッセージのアスペクト内のデータの使用に対する制限を提供するために、制約を使用してアノテートされてよい。制約が適用されるメッセージのアスペクトは、メッセージ全体、複合要素（子複合要素または単純な要素／フィールドを含むことができる）、あるいはメッセージの個別の要素またはフィールドであってよい。制限は、データがデプロイされてよいロケーションを定義するメッセージ・モデル内の制約として提供されてよい。メッセージ・モデルにアノテートすることによって、境界X内、境界Y内など（すなわち、部署内、ファイアウォール内、国内など）に留まる必要があるデータ・フィールドまたはデータ構造を識別することができる。メッセージ・モデルは、アプリケーションによって処理される一時データ、およびデプロイメントロケーションの決定にこの一時データを使用することを記述するように拡大される。

【0029】

メッセージ・モデルは、メッセージ形式のアノテートされたモデルを提供し、例えばメッセージ・モデルは、アノテートされた拡張マークアップ言語（XML: Extensible Markup Language）スキーマ・モデルまたはデータ・フォーマット記述言語（DFDL: Data Format Description Language）スキーマ・モデルであってよい。

【0030】

メッセージ・モデルを作成する場合、管理者は、要素またはフィールドを作成することができ、制約を指定するために、要素またはフィールドに対してプロパティを設定することができる。既存のメッセージ・モデルが変更される場合、管理者は、適切な制約プロパティを設定することによって、既存の要素またはフィールドを変更することができる。アプリケーションは、メッセージ・モデルによって定義されたメッセージを処理するアプリケーションのノードまたはサブセットによって使用するために、開発時に、メッセージ・モデルをアプリケーション・フローに取り込むことができる。アプリケーションの開発において、分析のためにアプリケーションが提供されてよい（101）。このアプリケーションは、例えばネットワーク全体（つまり、ハイブリッド・クラウド環境）に分散される場合のある複数のシステムにまたがってデプロイされてよい処理ノードまたはコードのサブセットを含むことができる。

【0031】

アプリケーションの分析が実行されて、メッセージ・モデル内で制約が課されたデータ・フィールド、データ要素、またはデータ構造を参照するアプリケーションの処理ノード、またはそのような制約が課されたメッセージを処理するアプリケーションの処理ノードを識別する（102）。分析は、アノテートされたメッセージ・モデルにアクセスすることができ（103）、このメッセージ・モデルにおいて、フィールド、要素、または構造、あるいはこれらの組み合わせに含まれるデータのデプロイメントロケーションに対する制限の詳細を取得するために、データ・フィールド、データ要素、またはデータ構造、あるいはこれらの組み合わせなどのメッセージのアスペクトは、制約を使用してアノテートされている。

【0032】

一実施形態では、分析は、制限が適用され、制約されないメッセージのターゲットのアスペクトに移動したメッセージのアスペクトに関連する追跡データにアクセスすることも

10

20

30

40

50

できる（１０４）。ターゲットのアスペクトは、追跡されてよく、それらのデータに適用される制約に対応することができる。ノードの分散に対する制約を示すために、アプリケーションのノードには、制限メタデータを使用してマークが付けられる（１０５）。制限メタデータは、ノードによって使用される方法のアスペクト（メッセージ、データ・フィールド、要素、または構造）に関連するメッセージ・モデル内の制約のアノテーションに基づく（１０６）。

【００３３】

アプリケーションの後でのデプロイメントでは、処理ノードの制限メタデータが読み取られてよく、アプリケーションのさまざまなノードが、そのノードの制限メタデータの要件を満たすシステムによって処理するために送信されてよい（１０７）。

10

【００３４】

図２を参照すると、フロー図１５０は、記載された方法の実施形態例を示しており、複数のシステムにまたがってデプロイされてよいアプリケーションのデプロイメントでリアルタイムに実行されてよい。図１の方法と同様に、準備手順として、メッセージ・モデルは、メッセージのアスペクト内のデータの使用に対する制限を提供するために、制約を使用してアノテートされてよい。デプロイメントのためのアプリケーションが提供されてよい（１５１）。このアプリケーションは、例えばネットワーク全体（つまり、ハイブリッド・クラウド環境）に分散される場合のある複数のシステムにまたがってデプロイされてよい処理ノードを含むことができる。

【００３５】

20

アプリケーションの分析が実行されて、メッセージ・モデル内で制約が課されたデータ・フィールド、データ要素、またはデータ構造を参照するアプリケーションの処理ノード、またはそのような制約が課されたメッセージを処理するアプリケーションの処理ノードを識別する（１５２）。分析は、アノテートされたメッセージ・モデルにアクセスすることができ（１５３）、このメッセージ・モデルにおいて、フィールド、要素、または構造、あるいはこれらの組み合わせに含まれるデータのデプロイメントロケーションに対する制限の詳細を取得するために、データ・フィールド、データ要素、またはデータ構造、あるいはこれらの組み合わせなどのメッセージのアスペクトは、制約を使用してアノテートされている。一実施形態では、分析は、制限が適用され、制約されないメッセージのターゲットのアスペクトに移動したメッセージのアスペクトに関連する追跡データにアクセスすることもできる（１５４）。ターゲットのアスペクトは、追跡されてよく、それらのデータに適用される制約に対応することができる。

30

【００３６】

処理ノードの制限は、メッセージ・モデル内の制約アノテーションおよび追跡データに基づいて決定されてよく（１５５）、アプリケーションのノードは、決定された制限に従ってデプロイされてよく（１５６）、アプリケーションのさまざまなノードは、そのノードの制限の要件を満たすシステムによって処理するために送信されてよい。デプロイメントのためにアプリケーションをノードに分割する（例えば、一部のノードがオンプレミスに存在し、一部のノードがパブリック・クラウド環境内に存在する）ことによって、オンプレミスのリソースが制約されるようになったときに、処理のクラウド・バースティングを可能にする。

40

【００３７】

図３を参照すると、フロー図２００は、複数のシステムにまたがってデプロイされてよいアプリケーションの開発後（２０１）に実行される、記載された方法の実施形態例をより詳細に示している。この実施形態は統合環境内で提供され、この統合環境では、アプリケーションは、１つまたは複数のインバウンド・インターフェイスおよび１つまたは複数のアウトバウンド・インターフェイスを有するノードを含む統合フローである。分散環境内の対応するアプリケーションは、同様の方法を使用することができる。

【００３８】

開発されたアプリケーションの静的分析が起動されてよく（２０２）、アプリケーショ

50

ンのノードがステップ203で分析されてよい。ノードのインバウンド・インターフェイスが制約されたフィールドまたはデータを含んでいるかどうか決定されてよい(204)。ステップ204では、フィールドまたはデータに対して提供された制約を決定するために、メッセージ・モデルを参照することができる。ステップ204では、制約が適用されたフィールドを記録する追跡記憶装置(tracking store)210も参照することができる。ノードが制約されたフィールドを含んでいない場合、この方法は下で説明されるステップ208に進む。

【0039】

ノードが制約されたフィールドを含んでいる場合、このノードは、適切に制限されているとしてマークが付けられてよい(205)。その後、このノードのロジックが制約されたフィールドをアウトバウンド・インターフェイス上のいずれかの他のフィールドに移動させたかどうか決定されてよい(206)。ロジックが制約されたフィールドを移動させない場合、この方法は下で説明されるステップ208に進むことができる。しかし、ロジックが制約されたフィールドをさらに移動させる場合、ステップ208に進む前に、ターゲットのフィールドが制約されたデータを含んでいるということが追跡記憶装置210内に記録される(207)。

【0040】

ステップ208で、ノードのアウトバウンド・インターフェイスが制約されたフィールドまたはデータを含んでいるかどうか決定されてよい。ステップ208では、制約が適用されたフィールドを記録する追跡記憶装置210も参照することができる。そのような制約されたフィールドが存在する場合、このノードは、それに応じて制限されているとしてマークが付けられてよい(209)。その後、アプリケーション内にさらにノードが存在するかどうか決定されてよい(211)。ノードが存在する場合、この方法は、ステップ203で次のノードを分析するためにループすることができる(213)。それ以上ノードが存在しない場合、アプリケーションは、ノード内でマークが付けられた制約に基づいて各ノードを適切なロケーションにデプロイして、ハイブリッド環境にデプロイされてよい(214)。

【0041】

この実施形態では、デプロイメントの前の分析時に追跡記憶装置210が使用される。静的分析は、制約を指定しないスキーマに基づいている新しいメッセージを作成するために、制約されたフィールドが使用されるということを認識すると、追跡記憶装置210を参照して、その新しいメッセージがその後のノードによって処理されるときに、現在使用されているモデルは制約を有していないが、このメッセージが、前のメッセージ・モデル内で制約されているとしてマークが付けられていたフィールドを含んでおり、したがって前記ノードのデプロイメントまたは処理の範囲を制限するということを識別することができる。

【0042】

追跡方法は、インターフェイスのみを分析するのとは対照的に、ノード自体に含まれるロジックを分析することを含むことができる。この分析は、APIの知識または一般的な変換技術を使用して、他のアウトバウンド・フィールドへの入力として移動させるか、または使用されるフィールドを理解するために、製品APIまたはさらに一般的なAPI(XSLT、XQueryなど)を分析することであってよい。

【0043】

図4を参照すると、ブロック図が、記載されたシステム300の一実施形態例を示している。システム300は、セキュア・デプロイメント・システム(secure deployment system)310を含む。セキュア・デプロイメント・システム310は、アプリケーション開発用の開発システムの一部、またはデプロイメントロケーションへのアプリケーションのデプロイメント用のデプロイメント・システムの一部として提供されてよい。図3では、セキュア・デプロイメント・コンポーネント320が独立して示されているが、セキュア・デプロイメント・コンポーネント320は、セキュア・デプロイメント・システム3

10がデプロイメント・システムとして提供される場合、セキュア・デプロイメント・システム310の出力コンポーネントとして組み込まれてよい。

【0044】

メッセージ・モデル・アノテーション・コンポーネント (message model annotating component) 330が提供されてよく、メッセージ・モデル・アノテーション・コンポーネント330は、セキュア・デプロイメント・システム310から独立してよく、本明細書に記載されているように、デプロイメント制約を使用してメッセージ・モデルにアノテートするための管理者用のユーザ・インターフェイスとして提供されてよい。メッセージ・モデル・アノテーション・コンポーネント330は、アプリケーション開発から独立してよい。セキュア・デプロイメント・システム310は、プロセッサ、および定義された機能を提供するように配置された以下のコンポーネントの機能を実行するためのコンピュータ・プログラム命令をプロセッサに提供するように構成されたメモリを含むことができる。

10

【0045】

セキュア・デプロイメント・システム310は、分析のためにアプリケーション312を受信するように配置された受信コンポーネント311を含むことができ、このアプリケーションは、さまざまなロケーションにデプロイされてよい処理ノード401~405に分割されることが可能である。アプリケーション312は、メッセージの特定のデータ・フィールドまたはデータ構造内のデータのデプロイメントに対する制約を定義するアノテーションを含んでいるメッセージ・モデル313に基づいてメッセージを処理する。必要なメッセージ・モデル313にアクセスするためのアクセス・コンポーネント317が提供されてよい。

20

【0046】

セキュア・デプロイメント・システム310は、メッセージ・モデル313内のアノテーションによって定義されたデプロイメント制約を有する特定のデータ・フィールドまたはデータ構造を参照する処理ノード401~405を識別するために、アプリケーションを分析するように配置された分析コンポーネント314を含むことができる。分析コンポーネント314は、デプロイメント制約を有するデータ・フィールドまたはデータ構造を追跡し、デプロイメント制約を有するデータ・フィールドまたはデータ構造を処理ノード501~505から移動させるかどうかを決定するように配置された追跡コンポーネント316を参照することもできる。追跡記憶装置318は、移動させたデータ・フィールドまたはデータ構造がデプロイメント制約を有することを記録するために提供されてもよい。

30

【0047】

セキュア・デプロイメント・システム310は、参照されるデータ・フィールドおよびデータ構造のデプロイメント制約に基づいて処理ノードに関する制限を決定するために、決定コンポーネント321を含むことができる。

【0048】

デプロイメントの前にセキュア・デプロイメント・システム310が運用される実施形態では、セキュア・デプロイメント・システム310は、処理ノードによってアクセスされる特定のデータ・フィールドまたはデータ構造に関連するメッセージ・モデル313内でアノテートされたデプロイメント制約に対応する制限メタデータを使用して処理ノード401~405にマークを付けるように配置されたマーキング・コンポーネント315を含むことができる。マーク付きアプリケーション出力コンポーネント (marked application output component) 319は、必要に応じて、マークが付けられたアプリケーションを独立したデプロイメント・コンポーネント320に出力することができる。デプロイメント・コンポーネント320は、制限メタデータを読み取り、デプロイメント制約に従って各処理ノード401~405をデプロイすることができる。

40

【0049】

セキュア・デプロイメント・システム310がアプリケーションのデプロイメントで運

50

用される実施形態では、決定コンポーネント 3 2 1 は、処理ノードに関する決定された制限を、それに応じて処理ノードをデプロイできるセキュア・デプロイメント・コンポーネント 3 2 0 に出力することができる。

【0050】

図 5 を参照すると、ブロック図は、記載された方法およびシステムが実装されてよいシステム例 4 0 0 を示している。示されたシステム例 4 0 0 は、ハイブリッド・クラウド環境全体にデプロイされた統合アプリケーションの形態でのアプリケーション 3 1 2 である。説明を簡単にするために、ハイブリッド・クラウド環境は、オンプレミス・システム 4 1 0 およびパブリック・クラウド 4 2 0 として示されている。

【0051】

オンプレミス・システム 4 1 0 およびパブリック・クラウド 4 2 0 は、ランタイム・エンジン 4 1 1、4 2 1 をそれぞれ含むことができる。ランタイム・エンジン 4 1 1、4 2 1 は、これらのランタイム・エンジンにデプロイされたアプリケーションを実行する。一実施形態例では、ランタイム・エンジンは統合サーバであってよい。アプリケーションは、メッセージ・モデル 3 1 3 などの関連するリソースを通常は格納することができるライブラリを参照する。

【0052】

統合アプリケーション 3 1 2 は、関連付けられたメッセージ・モデル 3 1 3 と共に処理ノード 4 0 1 ~ 4 0 5 を含んでいる。各ノード 4 0 1 ~ 4 0 5 は、オンプレミスではランタイム・エンジン 4 1 1 において実行されてよく、またはパブリック・クラウド（あるいは、さらに複雑な配置におけるその他のロケーション）ではランタイム・エンジン 4 2 1 において実行されてよい。アプリケーション 3 1 2 内のロジックがノード 4 0 1 ~ 4 0 5 に達したときに、ロジックがパブリック・クラウド 4 2 0 で実行される場合、処理されるメッセージおよびコンテキストがランタイム・エンジン 4 2 1 に送信される。ロジックがオンプレミス・システム 4 1 0 で実行される場合、処理されるメッセージおよびコンテキストがオンプレミス・システム 4 1 0 上のランタイム・エンジン 4 1 1 に送信される。

【0053】

セキュア・コネクタ 4 2 0 は、オンプレミスのランタイム・エンジン 4 1 1 をクラウド 4 2 0 内のランタイム・エンジン 4 2 1 に接続するロケーション（オンプレミス、クラウド内、またはこれら 2 つの間で分割される）で実行されるプロセスとして提供されてよい。処理がクラウドのランタイム・エンジン 4 2 1 において完了すると、制御がオンプレミスのランタイム・エンジン 4 1 1 に戻る。そのため、セキュア・コネクタ 4 2 0 は、呼び出されるランタイム・エンジン 4 1 1、4 2 1 に関連する外部プロセスであり、オンプレミスのランタイム・エンジン 4 1 1 をクラウド内のランタイム・エンジン 4 2 1 に接続する。

【0054】

記載されたセキュア・デプロイメント・コンポーネント 3 1 0 は、セキュア・コネクタ 4 2 0 で提供されてよく、処理ノード 4 0 1 ~ 4 0 5 で制限メタデータを読み取ることができる。ノードがデプロイされてよいランタイム・エンジン 4 1 1、4 2 1 を決定することができる。

【0055】

ここで、記載された方法を説明する例が提供される。

【0056】

管理者は、メッセージ・モデル（XML / DFDL スキーマなど）を使用してメッセージ構造を記述するときに、特定のデータ構造またはデータ・フィールドに対する制限を設定するアノテーションをさらに提供することができる。以下の例は、FIELD 2 が企業のファイアウォールから離れないという FIELD 2 に対する制限、および複合構造 PERSONAL__DATA 内のデータが国から離れることが許可されないという制限を課す。

HEADER :

10

20

30

40

50

```
FIELD1::STRING
BODY::
FIELD2::STRING::ONPREM
PERSONAL_DATA:::COUNTRY
FIELD3::INTEGER
FIELD4::STRING
FIELD5::STRING
FOOTER::
FIELD6::DATETIME
```

【0057】

FIELD2およびPERSONAL_DATAフィールド／要素（子要素FIELD3、FIELD4、およびFIELD5を含んでいる）は、制約を有する。ノードがこれらのフィールドとのインターフェイスを有する場合、そのノードは適切な環境内で実行されていなければならない。

【0058】

その後、統合フロー開発者は、前記メッセージ・モデルを、説明されたメッセージを処理する統合フローに取り込むことができる。アプリケーションが完成し、パッケージ化またはデプロイされるときに、コードの静的分析が行われ、メッセージ・モデル内で制約が課されたフィールドにアクセスするか、またはそのような制約が課されたメッセージを処理するアプリケーションのノードを決定することができる。有利なことに、この決定は、メッセージ・モデルから出たデータ（例えば、上のFIELD2から取り出し、アウトバウンド呼び出しを行うために、別のメッセージ・モデル内の制約されないフィールドに移動させたデータ）を追跡することをさらに含むことができる。

【0059】

その後、アプリケーションのノードは、デプロイされてよいロケーションに示すために、分析に基づいてマークが付けられてよい。「ONPREM」によって制約されたデータに作用するノードは、オンプレミス環境にのみデプロイされてよい。

【0060】

統合の第1の例およびその後のデプロイメントが図6および7に示されている。図6では、入力501、ルーティング502、変換503、SOAP要求504、変換505、および出力506のノードを通る統合のメッセージ・フロー500の実施形態例が示されている。メッセージ・ボックスが上下に重なって示されている場合、それは、上部のメッセージが下部のメッセージに変換されているか、または上部のメッセージが外部のサービスに送信され、下部のメッセージが返されていることを示している。

【0061】

メッセージ511は、メッセージ・フローへの入力段階501で受信される。メッセージ511は、メッセージ内の下線が引かれたフィールドに基づいてルーティングされる（502）。簡単にするために、このポイントから選択できる他のパスは示されていない。メッセージ513は、上部に示されたメッセージ513Aから下部に示されたメッセージ513Bに変換される（503）。下線が引かれたフィールドは、変換ノード503のアウトバウンド・メッセージに伝達するデータを示している。SOAP要求ノード504の上部のメッセージ514Aは、外部のSOAPサービスに送信され、下の応答514Bが受信される。このノードを安全性の低い環境内で実行できるように、どちらのインターフェイスも、制約されたフィールドを参照しない。変換ノード505の上部のメッセージ515Aは、下部に示されたメッセージ515Bに変換される。メッセージ516は、出力ノード506で統合から出力されることを示している。

【0062】

入力ノード501とルーティング・ノード502の間、およびルーティング・ノード502と変換ノード503の間のインターフェイスのメッセージ・モデルは、制約されているFIELD2フィールド、ならびにPERSONAL_DATAフィールドおよび要素

10

20

30

40

50

(子要素 F I E L D 3、F I E L D 4、および F I E L D 5 を含んでいる) を含む。そのため、ノードがこれらのフィールドとのインターフェイスを有する場合、そのノードは適切な環境内で実行されていなければならない。

【0063】

図7は、メッセージ・フロー500の統合デプロイメントの結果を示している。入力ノード501、ルーティング・ノード502、変換ノード503は、制約されたデータを処理しているため、オンプレミス520で処理される必要がある。これらのノードは、制限メタデータを使用してマークが付けられ、オンプレミスにデプロイされる。要求ノード504、第2の変換ノード505、および出力ノード506は、制約されたデータを処理していないため、パブリック・クラウド環境530内でデプロイされて処理されることが可能である。

10

【0064】

これらのノードは、前記環境の地理的位置が知られているか、または指定されることが可能である場合、クラウド環境内で使用されることが可能である。あるいは、これらのノードは、(例えば) データベースの位置が知られていないか、または前記地理的制約の範囲外にある場合、前記データベースに送信されることは不可能である。そのような状況の下では、データは送信されない(コンテンツから除去される)。これによって、アプリケーション内で、管理者/開発者に報告されるエラーが発生する可能性がある。

【0065】

図8を参照すると、統合の第2の例が示されており、値 P N 5 1 5 D L を含む追跡されるフィールド551を示している。変換ノード503と要求ノード504の間のインターフェイスのメッセージ・モデルは制約されたフィールドを含んでいないが、静的分析は、制約されたフィールド551(値 P N 5 1 5 D L を含んでいる)が制約されないフィールド552に移動したことを示した。フィールド552は、制約されたデータを含んでいるため、制約(すなわち、オンプレミス)から離れることができない。したがって、要求ノード504はオンプレミスで処理されなければならない。要求ノード504と変換ノード505の間、および変換ノード505と出力506の間のインターフェイスは制約されたデータを含んでおらず、これらのメッセージ・モデルに入る制約された追跡されているデータは存在せず、したがって最後の2つのノード505、506はパブリック環境で処理されてよい。

20

30

【0066】

上の実装および説明は統合アプリケーションに基づいているが、これらの方法は、構成要素に分割されてよい任意のアプリケーションにさらに広く適用可能である。

【0067】

ここで図9を参照すると、コンピュータ・システムまたはサーバの形態でのシステム600の例の概略図が示されている。

【0068】

コンピュータ・システムまたはサーバ612は、他の多数の汎用または専用のコンピューティング・システム環境または構成で運用されてよい。コンピュータ・システム/サーバ612での使用に適した既知のコンピューティング・システム、環境、または構成、あるいはこれらの組み合わせの例は、パーソナル・コンピュータ・システム、サーバ・コンピュータ・システム、シン・クライアント、シック・クライアント、ハンドヘルドまたはラップトップ・デバイス、マイクロプロセッサ・システム、マイクロプロセッサベース・システム、セット・トップ・ボックス、プログラマブル・コンシューマ・エレクトロニクス、ネットワーク P C、ミニコンピュータ・システム、メインフレーム・コンピュータ・システム、およびこれらの任意のシステムまたはデバイスを含む分散クラウド・コンピューティング環境などを含むが、これらに限定されない。

40

【0069】

コンピュータ・システム/サーバ612は、コンピュータ・システムによって実行されているプログラム・モジュールなどの、コンピュータ・システムによって実行可能な命令

50

の一般的な文脈において説明されてよい。通常、プログラム・モジュールは、特定のタスクを実行する、または特定の抽象データ型を実装するルーチン、プログラム、オブジェクト、コンポーネント、ロジック、データ構造などを含むことができる。コンピュータ・システム／サーバ612は、通信ネットワークを介してリンクされたりリモート処理デバイスによってタスクが実行される、分散クラウド・コンピューティング環境で実行されてよい。分散クラウド・コンピューティング環境において、プログラム・モジュールは、ローカルおよびリモートの両方のコンピュータ・システムの、メモリ・ストレージ・デバイスを含む記憶媒体に配置されてよい。

【0070】

図9では、コンピュータ・システム／サーバ612は、汎用コンピューティング・デバイスの形態で示されている。コンピュータ・システム／サーバ612のコンポーネントは、1つまたは複数のプロセッサまたはプロセッシング・ユニット616、システム・メモリ628、およびシステム・メモリ628を含むさまざまなシステム・コンポーネントをプロセッサ616に結合するバス618を含むことができるが、これらに限定されない。

【0071】

バス618は、メモリ・バスまたはメモリ・コントローラ、ペリフェラル・バス、アクセラレーテッド・グラフィックス・ポート、および任意のさまざまなバス・アーキテクチャを使用するプロセッサまたはローカル・バスを含む、1つまたは複数の任意の種類のバス構造を表す。例として、そのようなアーキテクチャは、ISA (Industry Standard Architecture) バス、MCA (Micro Channel Architecture) バス、EISA (Enhanced ISA) バス、VESA (Video Electronics Standards Association) ローカル・バス、およびPCI (Peripheral Component Interconnects) バスを含むが、これらに限定されない。

【0072】

コンピュータ・システム／サーバ612は、通常、さまざまなコンピュータ・システム可読媒体を含む。そのような媒体は、コンピュータ・システム／サーバ612によってアクセスできる任意の使用可能な媒体にすることができ、揮発性および不揮発性媒体、取り外し可能および取り外し不可の媒体を含む。

【0073】

システム・メモリ628は、ランダム・アクセス・メモリ (RAM) 630またはキャッシュ・メモリ632あるいはその両方などの、揮発性メモリの形態でのコンピュータ・システム可読媒体を含むことができる。コンピュータ・システム／サーバ612は、その他の取り外し可能／取り外し不可、揮発性／不揮発性のコンピュータ・システム記憶媒体をさらに含むことができる。単に例として、取り外し不可、不揮発性の磁気媒体 (図示されておらず、通常は「ハード・ドライブ」と呼ばれる) に対する読み取りと書き込みを行うために、ストレージ・システム634を提供することができる。図示されていないが、取り外し可能、不揮発性の磁気ディスク (例えば、「フロッピー (R) ・ディスク」) に対する読み取りと書き込みを行うための磁気ディスク・ドライブ、およびCD-ROM、DVD-ROM、またはその他の光媒体などの取り外し可能、不揮発性の光ディスクに対する読み取りと書き込みを行うための光ディスク・ドライブを提供することができる。そのような例では、それぞれを、1つまたは複数のデータ媒体インターフェイスによってバス618に接続することができる。下でさらに示され、説明されるように、メモリ628は、本発明の実施形態の機能を実行するように構成された一連の (例えば、少なくとも1つの) プログラム・モジュールを備える少なくとも1つのプログラム製品を含むことができる。

【0074】

プログラム・モジュール642のセット (少なくとも1つ) を含んでいるプログラム／ユーティリティ640は、例えばメモリ628に記憶されてよく、オペレーティング・システム、1つまたは複数のアプリケーション・プログラム、その他のプログラム・モジュール、およびプログラム・データにも記憶できるが、これらに限定されない。オペレーテ

10

20

30

40

50

ィング・システム、1つまたは複数のアプリケーション・プログラム、その他のプログラム・モジュール、およびプログラム・データまたはこれらの組み合わせは、それぞれネットワーク環境の実装を含むことができる。プログラム・モジュール642は、通常、本明細書に記載された本発明の実施形態の機能または方法あるいはその両方を実行する。

【0075】

また、コンピュータ・システム／サーバ612は、キーボード、ポインティング・デバイス、ディスプレイ624などの1つまたは複数の外部デバイス614、ユーザがコンピュータ・システム／サーバ612と情報をやりとりできるようにする1つまたは複数のデバイス、またはコンピュータ・システム／サーバ612が1つまたは複数の他のコンピューティング・デバイスと通信できるようにする任意のデバイス（例えば、ネットワーク・カード、モデムなど）、あるいはこれらの組み合わせと通信することもできる。そのような通信は、入力／出力（I/O：Input/Output）インターフェイス622を介して行うことができる。さらに、コンピュータ・システム／サーバ612は、ローカル・エリア・ネットワーク（LAN：Local Area Network）、一般的な広域ネットワーク（WAN：Wide Area Network）、またはパブリック・ネットワーク（例えば、インターネット）、あるいはこれらの組み合わせなどの1つまたは複数のネットワークと、ネットワーク・アダプタ620を介して通信することができる。図示されているように、ネットワーク・アダプタ620は、バス618を介してコンピュータ・システム／サーバ612の他のコンポーネントと通信する。図示されていないが、その他のハードウェア・コンポーネントまたはソフトウェア・コンポーネントあるいはその両方を、コンピュータ・システム／サーバ612と併用できるということが理解されるべきである。その例は、マイクロコード、デバイス・ドライバ、冗長プロセッシング・ユニット、外部ディスク・ドライブ・アレイ、RAIDシステム、テープ・ドライブ、およびデータ・アーカイブ・ストレージ・システムなどを含むが、これらに限定されない。

【0076】

本発明は、システム、方法、またはコンピュータ・プログラム製品、あるいはこれらの組み合わせであってよい。コンピュータ・プログラム製品は、プロセッサに本発明の態様を実行させるためのコンピュータ可読プログラム命令を含んでいる1つまたは複数のコンピュータ可読記憶媒体を含むことができる。

【0077】

コンピュータ可読記憶媒体は、命令実行デバイスによって使用するための命令を保持および記憶できる有形のデバイスにすることができる。コンピュータ可読記憶媒体は、例えば、電子ストレージ・デバイス、磁気ストレージ・デバイス、光ストレージ・デバイス、電磁ストレージ・デバイス、半導体ストレージ・デバイス、またはこれらの任意の適切な組み合わせであってよいが、これらに限定されない。コンピュータ可読記憶媒体のさらに具体的な例の非網羅的リストは、ポータブル・コンピュータ・ディスクレット、ハード・ディスク、ランダム・アクセス・メモリ（RAM：random access memory）、読み取り専用メモリ（ROM：read-only memory）、消去可能プログラマブル読み取り専用メモリ（EPROM：erasable programmable read-only memoryまたはフラッシュ・メモリ）、スタティック・ランダム・アクセス・メモリ（SRAM：static random access memory）、ポータブル・コンパクト・ディスク読み取り専用メモリ（CD-ROM：compact disc read-only memory）、デジタル多用途ディスク（DVD：digital versatile disk）、メモリ・スティック、フロッピー（R）・ディスク、パンチカードまたは命令が記録されている溝の中の隆起構造などの機械的にエンコードされるデバイス、およびこれらの任意の適切な組み合わせを含む。本明細書において使用されているコンピュータ可読記憶媒体は、本質的に、電波またはその他の自由に伝搬する電磁波、導波管またはその他の送信媒体を伝搬する電磁波（例えば、光ファイバ・ケーブルを通過する光パルス）、あるいはワイヤを介して送信される電気信号などの一時的信号であると解釈されるべきではない。

【0078】

本明細書に記載されたコンピュータ可読プログラム命令は、コンピュータ可読記憶媒体

から各コンピューティング・デバイス／処理デバイスへ、またはネットワーク（例えば、インターネット、ローカル・エリア・ネットワーク、広域ネットワーク、または無線ネットワーク、あるいはこれらの組み合わせ）を介して外部コンピュータまたは外部ストレージ・デバイスへダウンロードすることができる。このネットワークは、銅伝送ケーブル、光伝送ファイバ、無線送信、ルータ、ファイアウォール、スイッチ、ゲートウェイ・コンピュータ、またはエッジ・サーバ、あるいはこれらの組み合わせを備えてもよい。各コンピューティング・デバイス／処理デバイス内のネットワーク・アダプタ・カードまたはネットワーク・インターフェイスは、コンピュータ可読プログラム命令をネットワークから受信し、それらのコンピュータ可読プログラム命令を各コンピューティング・デバイス／処理デバイス内のコンピュータ可読記憶媒体に記憶するために転送する。

10

【0079】

本発明の処理を実行するためのコンピュータ可読プログラム命令は、アセンブラ命令、命令セット・アーキテクチャ（ISA）命令、マシン命令、マシン依存命令、マイクロコード、ファームウェア命令、状態設定データ、あるいは、Smalltalk（R）、C++などのオブジェクト指向プログラミング言語、および「C」プログラミング言語または同様のプログラミング言語などの従来の手続き型プログラミング言語を含む1つまたは複数のプログラミング言語の任意の組み合わせで記述されたソース・コードまたはオブジェクト・コードにすることができる。コンピュータ可読プログラム命令は、ユーザのコンピュータ上で全体的に実行すること、ユーザのコンピュータ上でスタンドアロン・ソフトウェア・パッケージとして部分的に実行すること、ユーザのコンピュータ上およびリモート・コンピュータ上でそれぞれ部分的に実行すること、あるいはリモート・コンピュータ上またはサーバ上で全体的に実行することができる。後者のシナリオでは、リモート・コンピュータを、ローカル・エリア・ネットワーク（LAN：local area network）または広域ネットワーク（WAN：wide area network）を含む任意の種類のネットワークを介してユーザのコンピュータに接続することができ、または接続を、（例えば、インターネット・サービス・プロバイダを使用してインターネットを介して）外部コンピュータに対して行うことができる。一部の実施形態では、本発明の態様を実行するために、例えばプログラマブル論理回路、フィールドプログラマブル・ゲート・アレイ（FPGA：field-programmable gate arrays）、またはプログラマブル・ロジック・アレイ（PLA：programmable logic arrays）を含む電子回路は、コンピュータ可読プログラム命令の状態情報を利用することによって、電子回路をカスタマイズするためのコンピュータ可読プログラム命令を実行できる。

20

30

【0080】

本発明の態様は、本明細書において、本発明の実施形態に記載された方法、装置（システム）、およびコンピュータ・プログラム製品のフローチャート図またはブロック図あるいはその両方を参照して説明される。フローチャート図またはブロック図あるいはその両方の各ブロック、ならびにフローチャート図またはブロック図あるいはその両方に含まれるブロックの組み合わせは、コンピュータ可読プログラム命令によって実装できるということが理解されるであろう。

【0081】

40

これらのコンピュータ可読プログラム命令は、コンピュータまたはその他のプログラム可能なデータ処理装置のプロセッサを介して実行される命令が、フローチャートまたはブロック図あるいはその両方の1つまたは複数のブロックに指定される機能／動作を実施する手段を作り出すべく、汎用コンピュータ、専用コンピュータ、または他のプログラム可能なデータ処理装置のプロセッサに提供されてマシンを作り出すものであってよい。これらのコンピュータ可読プログラム命令は、命令が記憶されたコンピュータ可読記憶媒体がフローチャートまたはブロック図あるいはその両方の1つまたは複数のブロックに指定される機能／動作の態様を実施する命令を含んでいる製品を備えるように、コンピュータ可読記憶媒体に記憶され、コンピュータ、プログラム可能なデータ処理装置、または他のデバイス、あるいはこれらの組み合わせに特定の方式で機能するように指示できるものであ

50

ってもよい。

【0082】

コンピュータ可読プログラム命令は、コンピュータ上、その他のプログラム可能な装置上、またはその他のデバイス上で実行される命令が、フローチャートまたはブロック図あるいはその両方の1つまたは複数のブロックに指定される機能／動作を実施するように、コンピュータ実装プロセスを生成すべく、コンピュータ、その他のプログラム可能なデータ処理装置、またはその他のデバイスに読み込まれ、コンピュータ上、その他のプログラム可能な装置上、またはその他のデバイス上で一連の動作可能なステップを実行させるものであってもよい。

【0083】

図内のフローチャートおよびブロック図は、本発明のさまざまな実施形態に記載されているシステム、方法、およびコンピュータ・プログラム製品の可能な実装のアーキテクチャ、機能、および処理を示す。これに関連して、フローチャートまたはブロック図内の各ブロックは、指定された論理機能を実装するための1つまたは複数の実行可能な命令を備える、命令のモジュール、セグメント、または部分を表すことができる。一部の代替の実装では、ブロックに示された機能は、図に示された順序とは異なる順序で発生させることができる。例えば、連続して示された2つのブロックは、実際には、含まれている機能に応じて、実質的に同時に実行されるか、または場合によっては逆の順序で実行されてもよい。ブロック図またはフローチャート図あるいはその両方の各ブロック、ならびにブロック図またはフローチャート図あるいはその両方に含まれるブロックの組み合わせは、指定された機能または動作を実行するか、または専用ハードウェアとコンピュータ命令を組み合わせる専用ハードウェアベースのシステムによって実装できるということにも注意する。

【0084】

クラウド・コンピューティング

本開示にはクラウド・コンピューティングの詳細な説明が含まれているが、本明細書において示された内容の実装は、クラウド・コンピューティング環境に限定されないということが、あらかじめ理解される。本発明の実施形態は、既知または今後開発される任意のその他の種類のコンピューティング環境と組み合わせて実装できる。

【0085】

クラウド・コンピューティングは、構成可能なコンピューティング・リソース（例えば、ネットワーク、ネットワーク帯域幅、サーバ、処理、メモリ、ストレージ、アプリケーション、仮想マシン、およびサービス）の共有プールへの便利なオンデマンドのネットワーク・アクセスを可能にするためのサービス提供モデルであり、管理上の手間またはサービス・プロバイダとのやりとりを最小限に抑えて、これらのリソースを迅速にプロビジョニングおよび解放することができる。このクラウド・モデルは、少なくとも5つの特徴、少なくとも3つのサービス・モデル、および少なくとも4つのデプロイメント・モデルを含むことができる。

【0086】

特徴は、次のとおりである。

【0087】

オンデマンドのセルフ・サービス：クラウドの利用者は、サーバの時間およびネットワーク・ストレージなどのコンピューティング能力を一方的に、サービス・プロバイダとの人間的なやりとりを必要とせず、必要に応じて自動的にプロビジョニングすることができる。

【0088】

幅広いネットワーク・アクセス：クラウドの能力は、ネットワークを経由して利用可能であり、標準的なメカニズムを使用してアクセスできるため、異種のシン・クライアントまたはシック・クライアント・プラットフォーム（例えば、携帯電話、ラップトップ、およびPDA）による利用を促進する。

【0089】

リソース・プール：プロバイダのコンピューティング・リソースは、プールされ、マルチテナント・モデルを使用して複数の利用者に提供される。さまざまな物理的および仮想的リソースが、要求に従って動的に割り当ておよび再割り当てされる。場所に依存しないという感覚があり、利用者は通常、提供されるリソースの正確な場所に関して管理することも知ることもないが、さらに高い抽象レベル（例えば、国、州、データセンター）では、場所を指定できる場合がある。

【0090】

迅速な順応性：クラウドの能力は、迅速かつ柔軟に、場合によっては自動的にプロビジョニングされ、素早くスケールアウトし、迅速に解放されて素早くスケールインすることができる。プロビジョニングに使用できる能力は、利用者には、多くの場合、無制限に見え、任意の量をいつでも購入できることである。

10

【0091】

測定されるサービス：クラウド・システムは、計測機能を活用することによって、サービスの種類（例えば、ストレージ、処理、帯域幅、およびアクティブなユーザのアカウント）に適した何らかの抽象レベルで、リソースの使用を自動的に制御および最適化する。リソースの使用量は監視、制御、および報告することができ、利用されるサービスのプロバイダと利用者の両方に透明性が提供される。

【0092】

サービス・モデルは、次のとおりである。

20

【0093】

SaaS（Software as a Service）：利用者に提供される能力は、クラウド・インフラストラクチャ上で稼働しているプロバイダのアプリケーションを使用することである。それらのアプリケーションは、Webブラウザ（例えば、Webベースの電子メール）などのシン・クライアント・インターフェイスを介して、さまざまなクライアント・デバイスからアクセスできる。利用者は、ネットワーク、サーバ、オペレーティング・システム、ストレージ、または個々のアプリケーション機能さえも含む基盤になるクラウド・インフラストラクチャを、限定的なユーザ固有のアプリケーション構成設定を行う可能性を除き、管理することも制御することもない。

【0094】

PaaS（Platform as a Service）：利用者に提供される能力は、プロバイダによってサポートされるプログラミング言語およびツールを使用して作成された、利用者が作成または取得したアプリケーションをクラウド・インフラストラクチャにデプロイすることである。利用者は、ネットワーク、サーバ、オペレーティング・システム、またはストレージを含む基盤になるクラウド・インフラストラクチャを管理することも制御することもないが、デプロイされたアプリケーション、および場合によってはアプリケーション・ホスティング環境の構成を制御することができる。

30

【0095】

IaaS（Infrastructure as a Service）：利用者に提供される能力は、処理、ストレージ、ネットワーク、およびその他の基本的なコンピューティング・リソースをプロビジョニングすることであり、利用者は、オペレーティング・システムおよびアプリケーションを含むことができる任意のソフトウェアをデプロイして実行できる。利用者は、基盤になるクラウド・インフラストラクチャを管理することも制御することもないが、オペレーティング・システム、ストレージ、およびデプロイされたアプリケーションを制御することができ、場合によっては、選択されたネットワーク・コンポーネント（例えば、ホスト・ファイアウォール）を限定的に制御できる。

40

【0096】

デプロイメント・モデルは、次のとおりである。

【0097】

プライベート・クラウド：このクラウド・インフラストラクチャは、組織のためにのみ

50

運用される。これは、この組織またはサード・パーティによって管理することができ、オンプレミスまたはオフプレミスに存在することができる。

【0098】

コミュニティ・クラウド：このクラウド・インフラストラクチャは、複数の組織によって共有され、関心事（例えば、任務、セキュリティ要件、ポリシー、および適合性に関する考慮事項）を共有している特定のコミュニティをサポートする。これは、これらの組織またはサード・パーティによって管理することができ、オンプレミスまたはオフプレミスに存在することができる。

【0099】

パブリック・クラウド：このクラウド・インフラストラクチャは、一般ユーザまたは大規模な業界団体が使用できるようになっており、クラウド・サービスを販売する組織によって所有される。

【0100】

ハイブリッド・クラウド：このクラウド・インフラストラクチャは、データとアプリケーションの移植を可能にする標準化された技術または独自の技術（例えば、クラウド間の負荷バランスを調整するためのクラウド・バースティング）によって固有の実体を残したまま互いに結合された2つ以上のクラウド（プライベート、コミュニティ、またはパブリック）の複合である。

【0101】

クラウド・コンピューティング環境は、ステートレス、疎結合、モジュール性、および意味的相互運用性に重点を置いたサービス指向の環境である。クラウド・コンピューティングの中心になるのは、相互接続されたノードのネットワークを備えるインフラストラクチャである。

【0102】

ここで図10を参照すると、クラウド・コンピューティング環境750の例が示されている。図示されているように、クラウド・コンピューティング環境750は、クラウドの利用者によって使用されるローカル・コンピューティング・デバイス（例えば、PDA（Personal Digital Assistant）または携帯電話754A、デスクトップ・コンピュータ754B、ラップトップ・コンピュータ754C、または自動車コンピュータ・システム754N、あるいはこれらの組み合わせなど）が通信できる1つまたは複数のクラウド・コンピューティング・ノード600を備える。ノード600は、互いに通信することができる。ノード600は、本明細書において前述されたプライベート・クラウド、コミュニティ・クラウド、パブリック・クラウド、またはハイブリッド・クラウド、あるいはこれらの組み合わせなど、1つまたは複数のネットワーク内で物理的または仮想的にグループ化されてよい（図示せず）。これによって、クラウド・コンピューティング環境750は、クラウドの利用者がローカル・コンピューティング・デバイス上でリソースを維持する必要のないインフラストラクチャ、プラットフォーム、またはソフトウェア、あるいはこれらの組み合わせをサービスとして提供できる。図10に示されたコンピューティング・デバイス754A～Nの種類は、例示のみが意図されており、コンピューティング・ノード600およびクラウド・コンピューティング環境750は、任意の種類のネットワークまたはネットワーク・アドレス指定可能な接続（例えば、Webブラウザを使用した接続）あるいはその両方を經由して任意の種類のコンピュータ制御デバイスと通信できるということが理解される。

【0103】

ここで図11を参照すると、クラウド・コンピューティング環境750（図10）によって提供される機能的抽象レイヤのセットが示されている。図11に示されたコンポーネント、レイヤ、および機能は、例示のみが意図されており、本発明の実施形態がこれらに限定されないということが、あらかじめ理解されるべきである。図示されているように、次のレイヤおよび対応する機能が提供される。

【0104】

ハードウェアおよびソフトウェア・レイヤ 860 は、ハードウェア・コンポーネントおよびソフトウェア・コンポーネントを含む。ハードウェア・コンポーネントの例は、メインフレーム 861、RISC (Reduced Instruction Set Computer) アーキテクチャベースのサーバ 862、サーバ 863、ブレード・サーバ 864、ストレージ・デバイス 865、ならびにネットワークおよびネットワーク・コンポーネント 866 を含む。一部の実施形態では、ソフトウェア・コンポーネントは、ネットワーク・アプリケーション・サーバ・ソフトウェア 867 およびデータベース・ソフトウェア 868 を含む。

【0105】

仮想化レイヤ 870 は、仮想サーバ 871、仮想ストレージ 872、仮想プライベート・ネットワークを含む仮想ネットワーク 873、仮想アプリケーションおよびオペレーティング・システム 874、ならびに仮想クライアント 875 などの仮想的実体を提供できる抽象レイヤを設ける。

10

【0106】

一例を挙げると、管理レイヤ 880 は、以下で説明される機能を提供することができる。リソース・プロビジョニング 881 は、クラウド・コンピューティング環境内でタスクを実行するために利用されるコンピューティング・リソースおよびその他のリソースの動的調達を行う。計測および価格設定 882 は、クラウド・コンピューティング環境内でリソースが利用された際のコスト追跡、およびそれらのリソースの利用に対する請求書の作成と送付を行う。一例を挙げると、それらのリソースは、アプリケーション・ソフトウェア・ライセンスを含むことができる。セキュリティは、クラウドの利用者およびタスクの ID 検証を行うとともに、データおよびその他のリソースの保護を行う。ユーザ・ポータル 883 は、クラウド・コンピューティング環境へのアクセスを利用者およびシステム管理者に提供する。サービス・レベル管理 884 は、必要なサービス・レベルを満たすように、クラウドのコンピューティング・リソースの割り当てと管理を行う。サービス水準合意 (SLA: Service Level Agreement) 計画および実行 885 は、今後の要求が予想されるクラウドのコンピューティング・リソースの事前準備および調達を、SLA に従って行う。

20

【0107】

ワークロード・レイヤ 890 は、クラウド・コンピューティング環境で利用できる機能の例を提供する。このレイヤから提供できるワークロードおよび機能の例は、マッピングおよびナビゲーション 891、ソフトウェア開発およびライフサイクル管理 892、仮想クラスルーム教育の配信 893、データ分析処理 894、トランザクション処理 895、およびデプロイメントロケーションへのセキュア・デプロイメントのためのデプロイメントおよび接続機能 896 を含む。

30

【0108】

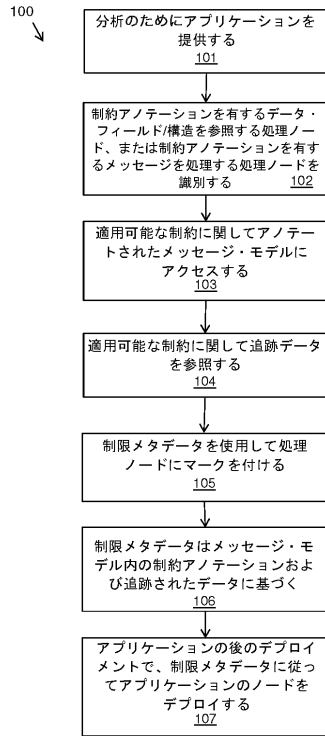
本発明のさまざまな実施形態の説明は、例示の目的で提示されているが、網羅的であることは意図されておらず、または開示された実施形態に限定されない。説明された実施形態の範囲および思想を逸脱することなく多くの変更および変形が、当業者にとって明らかになる。本明細書で使用された用語は、実施形態の原理、実際の適用、または市場で見られる技術を超える技術的改良を最も適切に説明するため、または他の当業者が本明細書で開示された実施形態を理解できるようにするため選択されている。

40

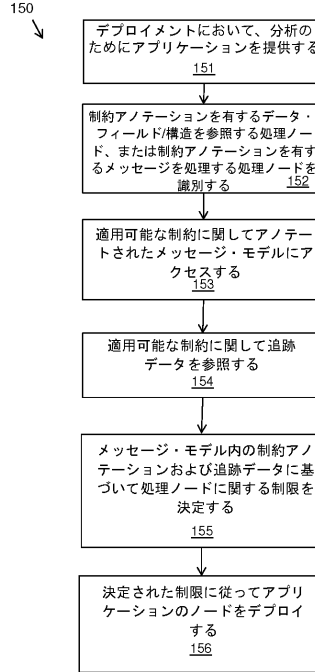
【0109】

本発明のさまざまな実施形態の説明は、例示の目的で提示されているが、網羅的であることは意図されておらず、または開示された実施形態に限定されない。開示された実施形態の範囲および思想を逸脱することなく多くの変更および変形が、当業者にとって明らかになる。本明細書で使用された用語は、実施形態の原理、実際の適用、または市場で見られる技術を超える技術的改良を最も適切に説明するため、または他の当業者が本明細書で開示された実施形態を理解できるようにするため選択されている。

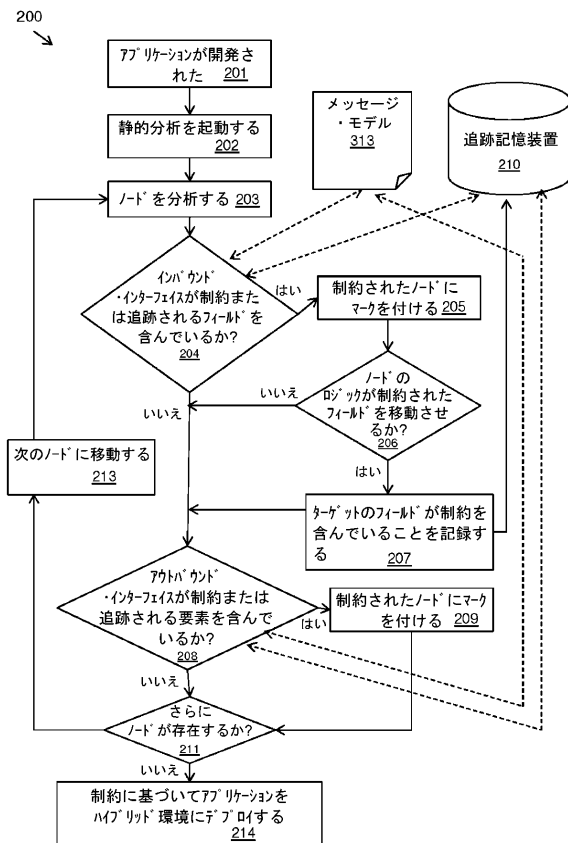
【図 1】



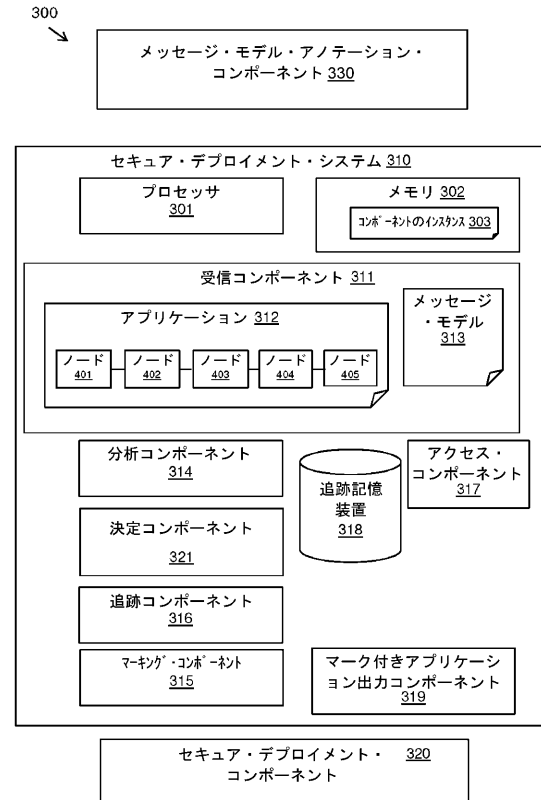
【図 2】



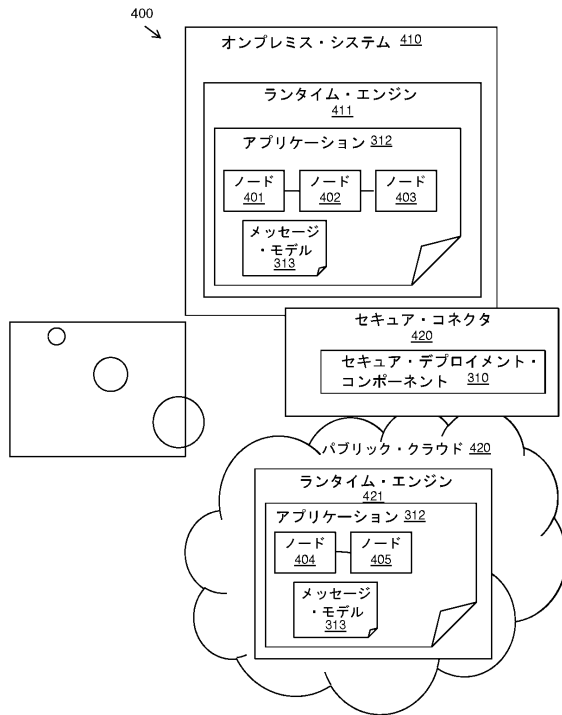
【図 3】



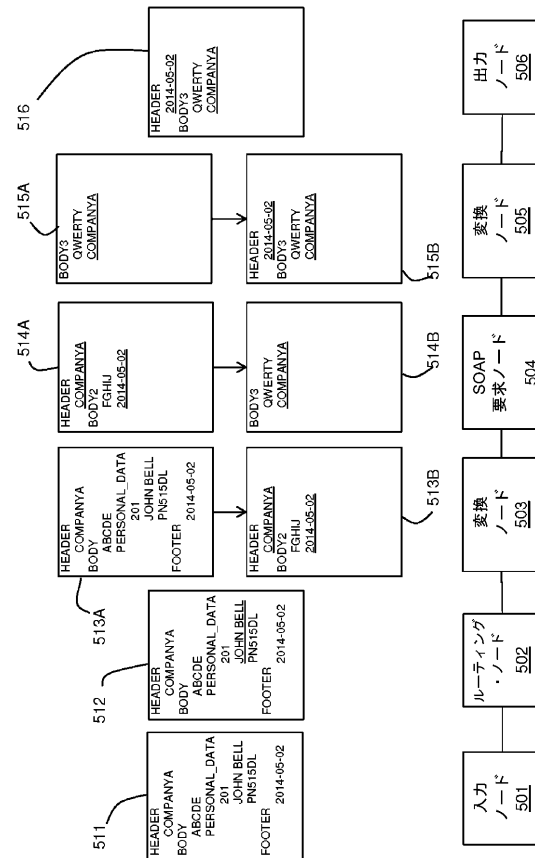
【図 4】



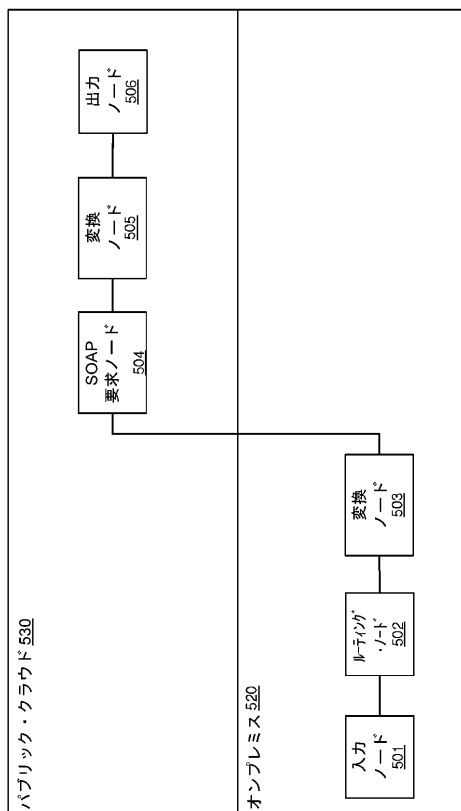
【図 5】



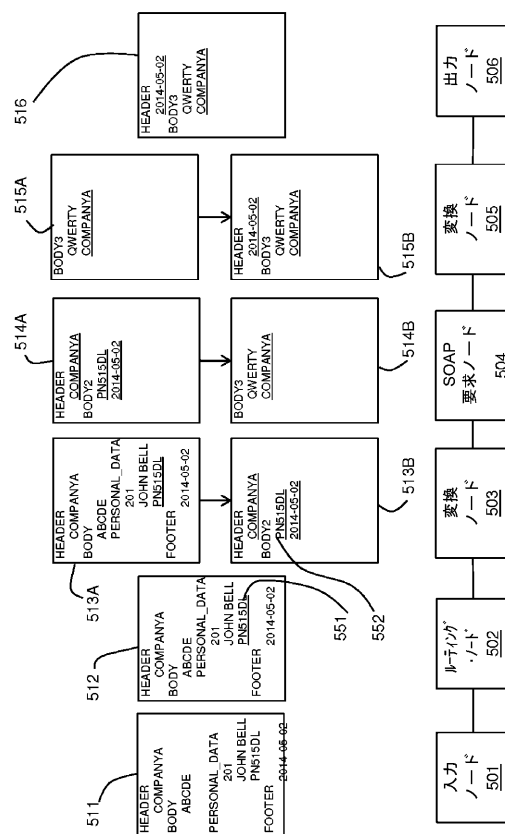
【図 6】



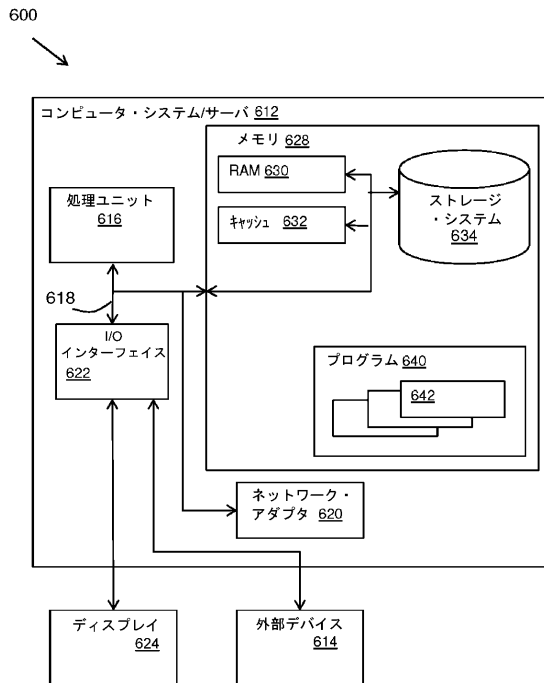
【図 7】



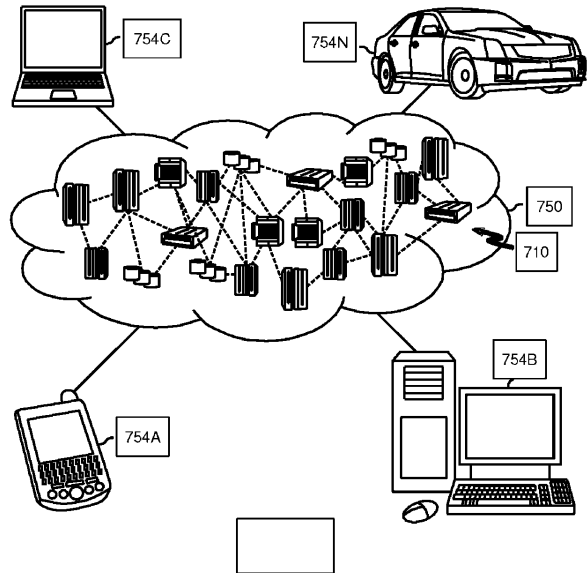
【図 8】



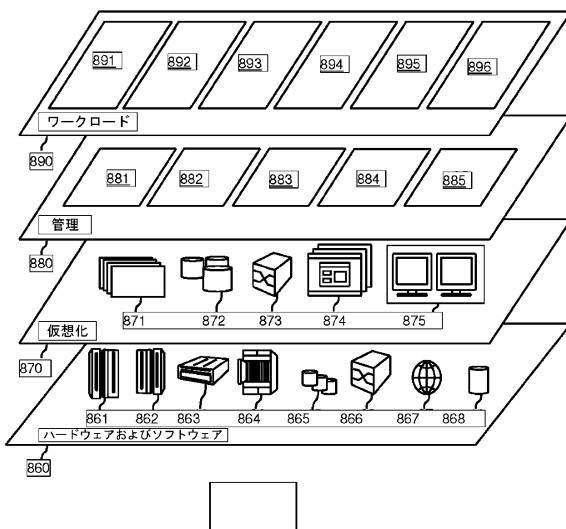
【図 9】



【図 10】



【図 11】



フロントページの続き

(74)代理人 100112690

弁理士 太佐 種一

(72)発明者 ロス、マーティン、アンドリュース

イギリス エスオー21 2ジェイエヌ ハンプシャー州ウィンチェスター ハースリー ハース
リーパーク

(72)発明者 ホージ、ジョン

イギリス エスオー21 2ジェイエヌ ハンプシャー州ウィンチェスター ハースリー ハース
リーパーク

(72)発明者 スターリング、クレイグ、ハワード

イギリス エスオー21 2ジェイエヌ ハンプシャー州ウィンチェスター ハースリー ハース
リーパーク

(72)発明者 ストレイ、ドミニク、ジョン

イギリス エスオー21 2ジェイエヌ ハンプシャー州ウィンチェスター ハースリー ハース
リーパーク

(72)発明者 マクギネス、ダニエル、ジェームズ

イギリス エスオー21 2ジェイエヌ ハンプシャー州ウィンチェスター ハースリー ハース
リーパーク

審査官 漆原 孝治

(56)参考文献 特表2015-534696 (JP, A)

特開2009-245362 (JP, A)

特開2007-199869 (JP, A)

特開2009-282652 (JP, A)

特開2012-084092 (JP, A)

(58)調査した分野(Int.Cl., DB名)

G06F 9/50

G06F 21/16