

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号

特許第7129474号

(P7129474)

(45)発行日 令和4年9月1日(2022.9.1)

(24)登録日 令和4年8月24日(2022.8.24)

(51)国際特許分類

F I

G 0 6 F 21/57 (2013.01)

G 0 6 F 21/57 3 7 0

G 0 6 F 21/56 (2013.01)

G 0 6 F 21/56

請求項の数 18 (全28頁)

(21)出願番号	特願2020-516821(P2020-516821)	(73)特許権者	521555742
(86)(22)出願日	平成30年9月25日(2018.9.25)		キンドリル・インク
(65)公表番号	特表2020-535515(P2020-535515 A)		Kyndryl Inc.
(43)公表日	令和2年12月3日(2020.12.3)		アメリカ合衆国ニューヨーク州、ニュー
(86)国際出願番号	PCT/IB2018/057407		ヨーク、ヴァンダービルト・アベニュー
(87)国際公開番号	WO2019/064176		1
(87)国際公開日	平成31年4月4日(2019.4.4)		One Vanderbilt Avenue, 15th Floor, New Y
審査請求日	令和3年2月22日(2021.2.22)		ork, New York 10017, USA
(31)優先権主張番号	15/721,566	(74)代理人	110000420弁理士法人M I P
(32)優先日	平成29年9月29日(2017.9.29)	(72)発明者	フワン、ジンホ
(33)優先権主張国・地域又は機関	米国(US)		アメリカ合衆国10598 ニューヨー
前置審査			ク州ヨークタウン・ハイツ キッチャワ
			ン・ロード1101
			最終頁に続く

(54)【発明の名称】 サーバ・グループを管理するためのシステム、方法、コンピュータ・プログラム、および記録媒体

(57)【特許請求の範囲】

【請求項1】

サーバ・グループを管理するためのシステムであって、
コンピュータ実行可能コンポーネントを格納するメモリと、
前記メモリに格納された前記コンピュータ実行可能コンポーネントを実行するプロセッサと、を含み、

前記コンピュータ実行可能コンポーネントは、

第1のサーバ・デバイスに関連する第1のリスクにตอบสนองして、前記第1のサーバ・デバイスおよび第2のサーバ・デバイスの脆弱性を軽減するために、前記第1のサーバ・デバイスおよび前記第2のサーバ・デバイスからなる前記サーバ・グループが前記サーバ・グループにパッチを適用するように動作可能なリスク評価コンポーネントと、

前記サーバ・グループに対してパッチを適用することにより第2のリスクを軽減するため、以前のリスク及び遠隔デバイスを介して受領した入力データを分析して前記サーバ・グループに対する前記第2のリスクに関連するデータを監視するように動作可能な監視コンポーネントと、

を含み、

前記サーバ・グループの修正は、前記第2のリスクを軽減するために、前記サーバ・グループから前記第2のサーバ・デバイスを除去する、システム。

【請求項2】

10

20

前記第 1 のリスクは、マルウェア攻撃に対する前記第 1 のサーバ・デバイスの脆弱性に関連する、

請求項 1 に記載のシステム。

【請求項 3】

前記コンピュータ実行可能コンポーネントは、前記サーバ・グループの前記第 2 のリスクを軽減するため、以前のリスク及び遠隔デバイスを介して受領した入力データを分析して前記サーバ・グループを修正して、サーバ・グループの修正をもたらすように動作可能な調整コンポーネントをさらに含む、

請求項 1 または 2 に記載のシステム。

【請求項 4】

前記監視コンポーネントは、前記サーバ・グループが修正されたという示唆を受信するように動作可能である、

請求項 1 ないし 3 のいずれか 1 項に記載のシステム。

【請求項 5】

前記リスク評価コンポーネントは、前記第 1 のサーバ・デバイスに関連するリスクを表すリスク・データを受信するように動作可能である、

請求項 1 ないし 4 のいずれか 1 項に記載のシステム。

【請求項 6】

前記サーバ・グループは第 1 のサーバ・グループであり、前記リスク評価コンポーネントは、前記第 1 のサーバ・グループではない第 2 のサーバ・グループの第 3 のリスクを評価するように動作可能である、

請求項 1 ないし 5 のいずれか 1 項に記載のシステム。

【請求項 7】

ワークステーション・デバイスから受信した以前のリスクに関連するリスク・データを分析し、リスク予測をもたらす学習コンポーネントをさらに含む、

請求項 1 ないし 6 のいずれか 1 項に記載のシステム。

【請求項 8】

前記リスク予測は、前記サーバ・グループに対する第 3 のリスクを軽減するために、前記監視コンポーネントへの入力として使用される、

請求項 7 に記載のシステム。

【請求項 9】

サーバ・グループを管理するためのコンピュータ実装方法であって、

第 1 のサーバ・デバイスに関連する第 1 のリスクに応じて、プロセッサに動作可能に結合されたデバイスによって、前記第 1 のサーバ・デバイスおよび第 2 のサーバ・デバイスの脆弱性を軽減するために、前記第 1 のサーバ・デバイスおよび前記第 2 のサーバ・デバイスからなる前記サーバ・グループが前記サーバ・グループにパッチを適用することと、

前記デバイスによって、前記サーバ・グループに対して前記パッチを適用することにより第 2 のリスクを軽減するために、前記サーバ・グループに対する前記第 2 のリスクに関連するデータを監視することと、

前記サーバ・グループの修正は、前記第 2 のリスクを軽減するために、前記サーバ・グループから前記第 2 のサーバ・デバイスを除去することと、

を含む、コンピュータ実装方法。

【請求項 10】

前記第 1 のリスクは、マルウェア攻撃に対する前記第 1 のサーバ・デバイスの脆弱性に関連する、

請求項 9 に記載のコンピュータ実装方法。

【請求項 11】

前記デバイスによって、前記サーバ・グループの前記第 2 のリスクを軽減するために、前記サーバ・グループを修正し、サーバ・グループの修正をもたらすことをさらに含む、

請求項 9 または 10 のいずれか 1 項に記載のコンピュータ実装方法。

10

20

30

40

50

【請求項 1 2】

前記サーバ・グループが修正されたという示唆を受信することをさらに含む、
請求項 9 ないし 1 1 のいずれか 1 項に記載のコンピュータ実装方法。

【請求項 1 3】

前記第 1 のサーバ・デバイスに関連するリスクを表すリスク・データを受信することをさらに含む、

請求項 9 ないし 1 2 のいずれか 1 項に記載のコンピュータ実装方法。

【請求項 1 4】

前記サーバ・グループは第 1 のサーバ・グループであり、前記方法は、前記第 1 のサーバ・グループではない第 2 のサーバ・グループの第 3 のリスクを評価することをさらに含む、

請求項 9 ないし 1 3 のいずれか 1 項に記載の方法。

【請求項 1 5】

ワークステーション・デバイスから受信した以前のリスクに関連するリスク・データを分析し、リスク予測をもたらすことをさらに含む、

請求項 9 ないし 1 4 のいずれか 1 項に記載の方法。

【請求項 1 6】

前記リスク予測は、前記サーバ・グループに対する第 3 のリスクを軽減するために、監視コンポーネントへの入力として使用される、

請求項 1 5 に記載の方法。

【請求項 1 7】

サーバ・グループを管理するためのコンピュータ・プログラムであって、

請求項 9 ないし 1 6 のいずれか 1 項に記載の方法の各ステップをコンピュータに実行させる、コンピュータ・プログラム。

【請求項 1 8】

請求項 1 7 に記載の前記コンピュータ・プログラムをコンピュータ可読記録媒体に記録した記録媒体。

【発明の詳細な説明】**【技術分野】****【0 0 0 1】**

本開示は、クラウド管理に関し、より具体的には、ストリーム・クラスタリングを使用したパッチ・グループの動的な再構成に関する。

【背景技術】**【0 0 0 2】**

同じ環境内で動作するマシンは、共通の脆弱性を軽減するために同じソフトウェアパッチ（例えばパッチ・グループ）の恩恵を受けることができる。例えば、アプリケーションは複数のサーバで実行することができる。したがって、ウェブ・サーバ、データベース、またはキャッシュあるいはその組み合わせは、複数のサーバまたは異なる物理マシンでアプリケーションを実行することができ、これにより、マルウェア、ウイルス、攻撃などに対する脆弱性が増加する可能性がある。通常、マシンには一度に 1 つのパッチを適用することができる。

【0 0 0 3】

パッチ・グループは共通の脆弱性を共有しているため、一緒に処理する必要がある。パッチ・グループは、主題の専門家（SME）の知識に基づいて手動で静的に作成されるが、これは共有インフラストラクチャ、ネットワーク、ワークロードなどの異なる粒度を反映していない。

【発明の概要】**【発明が解決しようとする課題】****【0 0 0 4】**

したがって、本発明の課題はストリーム・クラスタリングを使用したパッチ・グループ

10

20

30

40

50

の動的な再構成方法、システム、プログラム、記録媒体を提供することである。上記の問題に対処する技術が必要である。

【課題を解決するための手段】

【0005】

以下は、本開示の1つまたは複数の実施形態の基本的理解を与えるための概要を提示する。この概要は、重要なもしくは重大な要素を特定すること、または特定の実施形態のあらゆる範囲もしくはあらゆる特許請求の範囲を特定することを意図するものではない。この概要の唯一の目的は、後述する詳細な説明の前置きとして本発明の概念を簡易的な形態で示すことである。本明細書に説明される1つまたは複数の実施形態において、ストリーム・クラスタリングを使用したパッチ・グループの動的な再構成を容易にするデバイス、システム、コンピュータ実装方法、装置、またはコンピュータ・プログラム製品あるいはその組み合わせが説明される。

10

【0006】

第1の態様の観点では、本発明は、サーバ・グループを管理するためのシステムを提供し、システムは、コンピュータ実行可能コンポーネントを格納するメモリと、メモリに格納されたコンピュータ実行可能コンポーネントを実行するプロセッサと、を含み、コンピュータ実行可能コンポーネントは、第1のサーバ・デバイスに関連する第1のリスクにตอบสนองして、第1のサーバ・デバイスおよび第2のサーバ・デバイスの脆弱性を軽減するために、サーバ・グループにパッチを適用するように動作可能なリスク評価コンポーネントであって、サーバ・グループが第1のサーバ・デバイスおよび第2のサーバ・デバイスからなる、リスク評価コンポーネントと、サーバ・グループに対する第2のリスクを軽減するために、サーバ・グループに対する第2のリスクに関連するデータを監視するように動作可能な監視コンポーネントと、を含む。

20

【0007】

さらなる態様の観点では、本発明は、サーバ・グループを管理するためのコンピュータ実装方法を提供し、方法は、第1のサーバ・デバイスに関連する第1のリスクに応じて、プロセッサに動作可能に結合されたデバイスによって、第1のサーバ・デバイスおよび第2のサーバ・デバイスの脆弱性を軽減するために、サーバ・グループにパッチ適用することであって、サーバ・グループが第1のサーバ・デバイスおよび第2のサーバ・デバイスからなる、パッチ適用することと、デバイスによって、サーバ・グループに対する第2のリスクを軽減するために、サーバ・グループに対する第2のリスクに関連するデータを監視することと、を含む。

30

【0008】

さらなる態様の観点では、本発明は、サーバ・グループを管理するためのコンピュータ・プログラム製品を提供し、コンピュータ・プログラム製品は、処理回路によって読み取り可能であり、本発明の方法を実行するために処理回路によって実行される命令を格納するコンピュータ読み取り可能な記憶媒体を含む。

【0009】

さらなる態様の観点では、本発明は、コンピュータ可読媒体に格納されたコンピュータ・プログラムを提供し、コンピュータ・プログラムは、ソフトウェアコード部分を含み、プログラムがコンピュータで実行されるときにデジタルコンピュータの内部メモリにロード可能な、本発明の方法を実行するためのものである。

40

【0010】

一実施形態によれば、システムは、コンピュータ実行可能コンポーネントを格納するメモリと、メモリに格納されたコンピュータ実行可能コンポーネントを実行するプロセッサと、を含むことができる。システムのコンピュータ実行可能コンポーネントは、第1のサーバ・デバイスに関連する第1のリスクにตอบสนองして、第1のサーバ・デバイスおよび第2のサーバ・デバイスの脆弱性を軽減するために、サーバ・グループにパッチを適用するリスク管理コンポーネントを含むことができ、サーバ・グループが前記第1のサーバ・デバイスおよび前記第2のサーバ・デバイスからなる。システムのコンピュータ実行可能コン

50

ポーネントは、サーバ・グループに対する第2のリスクを軽減するために、サーバ・グループに対する第2のリスクに関連するデータを監視する監視コンポーネントを含むこともできる。

【0011】

別の実施形態によれば、サーバ・グループのパッチングを容易にするコンピュータ・プログラム製品は、具体化されたプログラム命令を有するコンピュータ可読記憶媒体を含むことができる。プログラム命令は、プロセッサによって実行可能であり、プロセッサは、第1のサーバ・デバイスに関連する第1のリスクに応じて、第1のサーバ・デバイスおよび第2のサーバ・デバイスの脆弱性を軽減するために、サーバ・グループにパッチを適用することができ、サーバ・グループは、第1のサーバ・デバイスおよび第2サーバ・デバイスからなる。プログラム命令は、プロセッサによって、サーバ・グループに対する第2のリスクを軽減するために、サーバ・グループに対する第2のリスクに関連するデータを監視するために実行可能にすることもできる。

10

【0012】

さらに別の実施形態によれば、コンピュータ実装方法が提供される。コンピュータ実装方法は、第1のサーバ・デバイスに関連する第1のリスクに応じて、プロセッサに動作可能に結合されたデバイスによって、第1のサーバ・デバイスおよび第2のサーバ・デバイスの脆弱性を軽減するために、サーバ・グループにパッチを適用することを含むことができ、サーバ・グループは、第1のサーバ・デバイスおよび第2のサーバ・デバイスからなる。コンピュータ実装方法はまた、デバイスによって、サーバ・グループに対する第2のリスクを軽減するために、サーバ・グループに対する第2のリスクに関連するデータを監視することを含むことができる。

20

【0013】

さらに別の実施形態によれば、システムは、コンピュータ実行可能コンポーネントを格納するメモリと、メモリに格納されたコンピュータ実行可能コンポーネントを実行するプロセッサとを含むことができる。システムのコンピュータ実行可能コンポーネントは、第1のサーバ・デバイスに関連する第1のリスクに応じて、第1のサーバ・デバイスおよび第2のサーバ・デバイスの脆弱性を軽減するために、サーバ・グループにパッチを適用するリスク管理コンポーネントを含むことができ、サーバ・グループは、第1のサーバ・デバイスおよび第2のサーバ・デバイスからなる。システムのコンピュータ実行可能コンポーネントは、サーバ・グループに対する第2のリスクを軽減するために、サーバ・グループに対する第2のリスクに関連するデータを監視する監視コンポーネントを含むこともできる。さらに、システムのコンピュータ実行可能コンポーネントは、ワークステーション・デバイスから受信した以前のリスクに関連するリスク・データを分析し、リスク予測をもたらす学習コンポーネントも含むことができる。

30

【0014】

さらに別の実施形態によれば、サーバ・グループのパッチングを容易にするコンピュータ・プログラム製品は、具体化されたプログラム命令を有するコンピュータ可読記憶媒体を含むことができる。プログラム命令は、プロセッサによって実行可能であり、プロセッサは、第1のサーバ・デバイスに関連する第1のリスクに応じて、第1のサーバ・デバイスおよび第2のサーバ・デバイスの脆弱性を軽減するために、サーバ・グループにパッチを適用することができ、サーバ・グループは、第1のサーバ・デバイスおよび第2のサーバ・デバイスからなる。プログラム命令は、プロセッサによって、サーバ・グループに対する第2のリスクを軽減するために、サーバ・グループに対する第2のリスクに関連するデータを監視するように実行可能にすることもできる。プログラム命令は、プロセッサによって、ワークステーション・デバイスから受信した以前のリスクに関連するリスク・データを分析し、リスク予測をもたらすように実行可能にすることもできる。

40

【0015】

幾つかの実施形態では、システム、コンピュータ実装方法、またはコンピュータ・プログラムプログラムあるいはその組み合わせに関連して説明された上記の要素の1つまたは

50

複数は、コンピュータ実装方法、コンピュータ・プログラム製品、またはシステムなどさまざまな形で実現することができる。

【 0 0 1 6 】

本発明は、以下の図に示されるように、好ましい実施形態を参照して、例示のためだけに説明される。

【図面の簡単な説明】

【 0 0 1 7 】

【図 1】図 1 は、本明細書で説明される 1 つまたは複数の実施形態による、マシンのグループ化およびパッチ適用を容易にする例示的で非限定的なシステムのブロック図を示す。

【図 2】図 2 は、本明細書で説明される 1 つまたは複数の実施形態による、マシンのグループ化分析を容易にする例示的で非限定的なシステムの別のブロック図を示す。

【図 3】図 3 は、本明細書で説明される 1 つまたは複数の実施形態による、例示的で非限定的なマシン・パッチング・コンポーネントの追加のブロック図を示す。

【図 4】図 4 は、本明細書で説明される 1 つまたは複数の実施形態による、ストリーム・クラスタリングを容易にする例示的で非限定的なシステムのさらに別のブロック図を示す。

【図 5】図 5 は、本明細書で説明される 1 つまたは複数の実施形態による、マイクロストリーム・クラスタリングを容易にする例示的で非限定的なシステムの追加のブロック図を示す。

【図 6】図 6 は、本明細書で説明される 1 つまたは複数の実施形態による、例示的で非限定的なプロセス概要のフロー図を示す。

【図 7】図 7 は、本明細書に記載の 1 つまたは複数の実施形態による、リスク測定値の評価を容易にする例示的で非限定的なフロー図を示す。

【図 8】図 8 は、本明細書で説明する 1 つまたは複数の実施形態による、マシンのグループ化およびパッチ適用を容易にする例示的で非限定的なコンピュータ実装方法のフロー図を示す。

【図 9】図 9 は、本明細書で説明する 1 つまたは複数の実施形態による、マシンのグループ化およびパッチ適用を容易にする別の例示的で非限定的なコンピュータ実装方法のフロー図を示す。

【図 10】図 10 は、本明細書で説明する 1 つまたは複数の実施形態による、マシンのグループ化およびパッチ適用を容易にする別の例示的で非限定的なコンピュータ実装方法のフロー図を示す。

【図 11】図 11 は、本明細書で説明される 1 つまたは複数の実施形態を容易にすることができる例示的で非限定的な動作環境のブロック図を示す。

【図 12】図 12 は、本明細書で説明される 1 つまたは複数の実施形態による、例示的で非限定的なクラウド・コンピューティング動作環境のブロック図を示す。

【図 13】図 13 は、本明細書で説明される 1 つまたは複数の実施形態による、例示的で非限定的な抽象化モデル層のブロック図を示す。

【発明を実施するための形態】

【 0 0 1 8 】

以下の詳細な説明は例証にすぎず、実施形態または実施形態の用途あるいはその両方もしくはは使用を制限することを意図するものではない。さらに、前述の背景または概要セクション、または詳細な説明セクション内に提示されたいずれの表現された情報または暗黙的情報 (implied information) にも制約されることを意図しない。

【 0 0 1 9 】

ここで、全体を通して同様の要素を指すために同様の参照番号が用いられる図面を参照して、1 つまたは複数の実施形態を説明する。以下の説明において、説明のために、1 つまたは複数の実施形態のより完全な理解を与えるために、多数の特定の詳細が説明される。しかしながら、さまざまな場合において、1 つまたは複数の実施形態は、これらの特定の詳細なしに実施できることが明らかである。

【 0 0 2 0 】

本開示はクラウド・コンピューティングに関する詳細な説明を含むが、本明細書に列挙される教示の実装はクラウド・コンピューティング環境に限定されないことを理解されたい。むしろ、本発明の実施形態は、現在知られているまたは後に開発される他の任意のタイプのコンピューティング環境と組み合わせて実装することができる。

【0021】

クラウド・コンピューティングは、最小限の管理作業またはサービスのプロバイダとの対話で迅速にプロビジョニングおよびリリースされる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、サービス）の共有プールへの便利なオンデマンド・ネットワーク・アクセスを可能にするためのサービス配信のモデルである。このクラウド・モデルは、少なくとも5つの特性、少なくとも3つのサービス・モデル、および少なくとも4つの展開モデルを含むことができる。

10

【0022】

同じ環境内で動作するマシンは、共通の脆弱性を軽減するために同じソフトウェアパッチ（パッチ・グループなど）の恩恵を受けることができる。例えば、アプリケーションは複数のサーバで実行できる。したがって、ウェブ・サーバ、データベース、またはキャッシュあるいはその組み合わせは、複数のサーバまたは異なる物理マシンでアプリケーションを実行でき、マルウェア、ウイルス、攻撃などに対する脆弱性を高める可能性がある。一部のマシンは共通の脆弱性を共有できるため、マシンをまとめてグループにパッチを適用すると、マシンに1つずつパッチを適用するのではなく、共通の脆弱性に対するより良い防御またはセキュリティあるいはその両方を作成することができる。

20

【0023】

本明細書で説明する1つまたは複数の実施形態は、共通の脆弱性を共有するマシンのグループにパッチを当てることができる。パッチ・グループはさまざまな粒度で定義でき、パッチ・グループは動的に調整できる。本明細書で説明する1つまたは複数の実施形態は、マシンのパッチ適用を容易にするシステム、コンピュータ実装方法、装置、およびコンピュータ・プログラム製品を含む。

【0024】

図1は、本明細書で説明される1つまたは複数の実施形態による、マシンのグループ化およびパッチ適用を容易にする例示的で非限定的なシステムのブロック図を示す。さまざまな実施形態において、システム100は、データ分析システム、データ処理システム、グラフ分析システム、グラフ処理システム、ビッグデータ・システム、ソーシャル・ネットワーク・システム、音声認識システム、画像認識システム、グラフィカル・モデリング・システム、バイオインフォマティクス・システム、データ圧縮システム、人工知能システム、認証システム、構文パターン認識システム、医療システム、健康監視システム、ネットワーク・システム、コンピュータ・ネットワーク・システム、通信システム、ルータ・システム、サーバ・システムなどに関連付けられるか、または含まれることができる。

30

【0025】

図示のように、システム100は、制御デバイス112と、1つまたは複数のクラウド・ネットワーク102、108に通信可能に結合された1つまたは複数の物理マシン104、106、110を含むことができる。幾つかの実施形態では、クラウド・ネットワーク102、108は、（図示していない）仮想マシンを含むことができる。制御デバイス112、物理マシン104、106、110、または1つまたは複数の仮想マシンあるいはその組み合わせは、1つまたは複数の実施形態において互いに電氣的または通信可能あるいはその両方に結合することができる。

40

【0026】

一実施形態では、制御デバイス112は、共通のリスクを共有するマシンを識別することにより、マシンのパッチングを実行することができる。共通のリスクには、これらに限定されるわけではないが、マルウェア、ウイルス、メモリ・リーク、サイバー攻撃などが含まれ得る。この開示を参照すると、マシンはサーバ・デバイス、仮想マシン、中央処理

50

装置（CPU）、物理マシンなどであり得る。一実施形態では、制御デバイス112は、クラウド・ネットワーク102内の物理マシン104、106、110をグループ化することができる。物理マシン104、106、110は、仮想マシンを表すこともできる。

【0027】

幾つかの実施形態では、物理マシン104、106、110は、物理マシン104、106、110の共通の特性または共通の脅威あるいはその両方、または脆弱性に基づいて、制御デバイス112によってグループ化することができる。制御デバイス112は、個々の物理マシンまたは物理マシンのグループあるいはその両方を監視できる。例えば、物理マシンのオペレーティング・システム（OS）でメモリ・リークが発生した場合、制御デバイス112は、物理マシン104の脆弱性に関連するデータを受信できる。物理マシン106はクラウド・ネットワーク102内の物理マシン104とグループ化されているため、制御デバイス112は、物理マシン106もメモリ・リークの危険性があり、物理マシン104の脆弱性は物理マシン106のOSを攻撃にさらす可能性があるとは判断できる。したがって、制御デバイス112は、脆弱性を軽減するために、クラウド・ネットワーク102に関連付けられた環境内で実行されているソフトウェア、ミドルウェア、またはOSあるいはその組み合わせに共通のパッチを適用することができる。時々、制御デバイス112は、物理マシン104、106、110からデータが送信されるのを待つのではなく、物理マシン104、106、110でシステムチェックを実行して、物理マシンの1つまたは複数に関連する脆弱性があるかどうかを先取りして決定することも理解されたい。

【0028】

幾つかの実施形態では、移行、スケーラビリティ、スナップショット、および複製などのクラウド操作は、アプリケーションまたは物理マシンの状態の変化をもたらし得る。例えば、制御デバイス112は、アプリケーションまたは物理マシンの状態（例えば、使用中、再起動中など）に変化が起こったことを判定することができる。したがって、状態の変化は環境のデータ構造を変化させる可能性があり、本明細書で説明する1つまたは複数の実施形態では、制御デバイス112によって変化するようにグループ化を促し、動的な環境変化をもたらす。例えば、最初の時点で、物理マシンは最初の地理的領域でアプリケーションを実行でき、2番目の時点で別の物理的マシンによってアプリケーションを2番目の地理的領域で実行できる。移行によりアプリケーションはさまざまな地理的場所で行うことができるため、アプリケーションの複数のインスタンスを地理的に分散したデータセンターにスケール・アウトすると、脆弱性の露出が増加する可能性がある。したがって、本明細書で説明するさまざまな実施形態では、環境に変化があるたびにパッチ・グループを動的に再構成することができる。

【0029】

その結果、クラウド・ネットワーク102に関連付けられた物理マシン104、106と同じ特性または脆弱性あるいはその両方を示す別の物理マシン110に応じて、制御デバイス112はクラウド・ネットワーク108に物理マシンをグループ化し、それにより動的な環境変更を引き起こすことができる。動的に変化する環境では、物理マシンまたはデータ構造のスペースの変更も共通である。したがって、制御デバイス112は、物理マシン104、106、110に情報を送信して、パッチ・グループの変更を引き起こす、または物理マシン104、106、110に関連するソフトウェアにパッチを適用させるあるいはその両方を行うことができる。パッチ・グループは、共通の脆弱性を軽減するために同じソフトウェアパッチの恩恵を受けることができる同じ環境内で動作するマシンのグループである。一部のマシンは共通の脆弱性を共有し得るため、マシンに個別にパッチを適用するのではなく、マシンをグループ化し、グループにパッチを適用することで、共通の脆弱性に対する防御またはセキュリティあるいはその両方を強化できる。

【0030】

パッチは、マシンの脆弱性を修正または軽減するために開発され、マシンに送信またはマシンによって受信され、あるいはその両方であり得る。パッチは、脆弱性の観点から評

10

20

30

40

50

価でき、パッチが修正に与える影響を評価できる。したがって、ソフトウェアの脆弱性の測定は、共通脆弱性識別子（CVE）数として表すことができる。例えば、CVEには脆弱性（例えば低、中、高）のスコアリングが含まれる。その結果、パッチはCVE数（例えば0 - 10のスコア）に関連付けることができる。したがって、暴露のリスクが高いほど、CVE数は高くなる。したがって、10のスコアは、問題をすぐに解決する必要があることを示す。例えば、特定の物理マシンのCVEが10である場合、10のレーティングのパッチを物理マシンに適用して脆弱性を軽減することができる。さらに、パッチは任意の環境で実行されているソフトウェアに適用することができ、これは、誰でもクラウドにアクセスできるため、クラウド・ネットワーク102、108の運用において特に重要である。

10

【0031】

クラウド・ネットワーク102、108では、マシンは、複数のサーバ上で実行されるアプリケーションを有することができる。したがって、1つのサーバが危険にさらされると、他のサーバも危険にさらされる可能性がある。例えば、サーバに関連付けられたファイアウォールが侵害された場合、（侵害を受けたサーバだけでなく）そのファイアウォールの背後にある1つまたは複数のサーバを見ることができる。したがって、共通の脆弱性を共有するサーバのグループにパッチを適用すると、システムの効率を向上することができる。脆弱性またはCVEあるいはその両方に基づいて、制御デバイス112は、脆弱性を緩和するためにどのパッチを使用するかを正確に決定することができる。

【0032】

20

システム100は、ハードウェアまたはソフトウェアあるいはその両方を使用して、抽象的ではなく例えばマシンのグループ化やパッチの適用を容易にするために必要な処理機能のため人間が一連の精神的行為として実行することができない本質的に高度に技術的な問題（例えば、ソフトウェアのパッチング、マシンのグループ化、ストリーム・クラスタリングなど）を解決するために使用できる。さらに、実行されるプロセスの一部（例えば、コンピュータ処理、脆弱性パターン認識など）は、メモリ操作に関連する定義済みタスクを実行するための専用コンピュータによって実行され得る。例えば、ソフトウェアのパッチ適用などに関連するタスクを実行するために、専用のコンピュータを使用することができる。専用コンピュータは、物理マシン104、106、110が脆弱性の影響を受けやすいという示唆に応じて、クラウド・ネットワーク環境を自動的に調整することができる。

30

【0033】

図2は、本明細書で説明する1つまたは複数の実施形態によるマシングループ化分析を容易にする例示的で非限定的なシステム200の別のブロック図を示す。本明細書で説明される他の実施形態で使用される同様の要素の繰り返しの説明は、簡潔さのために省略される。

【0034】

別の実施形態では、制御デバイス112は、物理マシンに関連付けられた特性に基づいてマシンのグループ化を実行することができる。例えば、図2に示されるように、グループAでは物理マシンはマシンのワークロード・グループであり、グループBでは物理マシンはマシンのネットワーク・グループであり、グループCでは物理マシンはマシンのインフラストラクチャ・グループであり得る。

40

【0035】

制御デバイス112は、それらの機能（例えば、ワークロード、ネットワーク、インフラストラクチャなど）に従って物理マシンを個別にグループ化することができるが、特定の物理マシンは複数の特性を含み、複数のグループにグループ化できる。例えば、物理マシン110のうちの2つは、3つのグループA、B、Cすべてにグループ化できる。したがって、物理マシン110については3つのグループA、B、Cすべてにオーバーラップする。他のグループABCのいずれかにある物理マシン104、202B、202Cが脆弱性にさらされる場合、3つのグループA、B、Cすべてに関連する2つの物理マシン1

50

10も同じ脆弱性にさらされる。したがって、他のグループのいずれかにある他の物理マシン104、202B、202Cのいずれかが制御デバイス112から特定のパッチを受信する場合、2つの物理マシン110も制御デバイス112から同じパッチを受信できる。同様に、物理マシン104はグループA、Bに関連付けられている。したがって、物理マシン104、202Bのいずれかが脆弱性にさらされている場合、物理マシン104も脆弱性にさらされる可能性がある。したがって、物理マシン104、202Bに適用されるパッチは、物理マシン104にも適用されるべきである。前述のシナリオのすべての齟齬は図2に関して議論されていないが、同じ原則は同様の方法でグループ化されている他の物理マシンに適用されることを理解するべきである。

【0036】

図3は、本明細書で説明される1つまたは複数の実施形態による、例示的で非限定的な機械パッチング構成要素の追加のブロック図を示す。本明細書で説明される他の実施形態で使用される同様の要素の繰り返しの説明は、簡潔さのために省略される。

【0037】

図3に示す実施形態では、システム300は、遠隔ワークステーション・デバイス316から入力データを受信できるマシン・パッチング・コンポーネント302を備えることができる。サブコンポーネント（例えば、監視コンポーネント304、学習コンポーネント310、調整コンポーネント306、リスク評価コンポーネント308、パターン・データベース318、およびパッチ・データベース320）、プロセッサ314、およびメモリ312は、互いに電氣的または通信可能にあるいはその両方で結合することができる。代替実施形態では、サブコンポーネント、プロセッサ314、またはメモリ312あるいはその組み合わせを含むがこれらに限定されない他のコンポーネントは、マシン・パッチング・コンポーネント302の外部にあり得ることに留意されたい。例えば、他の実施形態において、パターン・データベース318およびパッチ・データベース320は、マシン・パッチング・コンポーネント302の外部にあってもよい。

【0038】

図3の1つの態様では、リスク評価コンポーネント308は、サーバ・デバイスに関連するリスクを評価することができる。例えば、リスクは、以前のリスク、ソフトウェア、手動入力、性能の低下などに基づいて決定することができる。例えば、制御デバイス112が、物理マシン104、106、110が性能の低下を経験したという示唆を受信した場合、制御デバイス112はマルウェアの兆候について物理マシン104、106、110をスキャンすることができる。マルウェアが見つかった場合、制御デバイスはマルウェアに関連付けられたCVEを判別し、マルウェアに関連付けられたCVEに相関するパッチを送信することができる。リスク評価コンポーネント308により第1のサーバ・デバイスに関してリスクが決定されると、リスク評価コンポーネント308は、サーバ・グループにパッチを当てて、サーバ・グループの第1のサーバ・デバイスおよび第2のサーバ・デバイスの脆弱性を緩和することができる。監視コンポーネント304は、さまざまなマシンに関連するリスクを監視することができる。例えば、サーバ・グループの第3のサーバ・デバイスが脆弱性を経験する場合、監視コンポーネント304は脆弱性を観察し、サーバ・グループの他のサーバ・デバイスが第3のサーバ・デバイスと同時にパッチされるべきであることを示すことができる。

【0039】

監視コンポーネント304は、学習コンポーネント310を含むこともでき、学習コンポーネント310は、以前のリスクおよび遠隔ワークステーション・デバイス316から受信した入力データを分析し、サーバ・デバイスに対する将来のリスクまたは脆弱性を予測することができる。例えば、物理マシン104が以前にマルウェア攻撃を受けやすい場合、学習アルゴリズムに従って、マルウェア攻撃、物理マシン104、およびマルウェア攻撃を緩和するソフトウェアパッチを保存することができる。次に、学習アルゴリズムは前述のデータを使用して、同じまたは類似のマルウェア攻撃が物理マシン104で発生するかどうかを判断し、グループ化された物理マシン106と同じまたは類似のパッチを共

10

20

30

40

50

有することができる。

【 0 0 4 0 】

学習コンポーネント 3 1 0 は、確率的または統計ベースあるいはその両方の分析を使用して、実行可能なアクションを予測または推測することができる。サポート・ベクター・マシン (S V M) は、使用できる分類子の例である。 S V M は、可能な入力空間で超曲面を見つけることで動作することができる。他の有向および無向の分類アプローチには、例えば、ナイーブ・ベイズ、ベイジアン・ネットワーク、決定木、ニューラル・ネットワーク、ファジィ論理モデル、および独立性の異なるパターンを提供する確率的分類モデルが含まれる。本明細書で使用される C V E 数に従ったリスクの分類には、優先度のモデルを開発するために利用される統計的回帰も含まれる場合がある。開示された態様は、（例えば、一般的な訓練データを介して）明示的に訓練された分類器および（例えば、ソフトウェアコードに関連する入力用語の使用を観察すること、外部情報を受信することなどを介して）暗黙的に訓練された分類器を使用することができる。

10

【 0 0 4 1 】

学習コンポーネント 3 1 0 は、 S V M を利用して、グループ・パターンのマルチラベルに学習ベースのアルゴリズムを採用することができる。マルチラベル・グループ・パターンは、異なる環境に関連付けられているグループ・パターンである。例えば、グループ・パターンは、ネットワーク・グラウンドに関連付け、インフラストラクチャ・グループに関連付けることができる。 S V M への入力は、ラベル付きセット D_1 、ラベルなしセット D_u 、ステップ数 T 、反復あたりのサンプル数 $S_{t=1}$ を含む。 $t = T$ の間に、マルチラベル S V M 分類器 f はトレーニング・データ D_1 に基づいてトレーニングすることができる。 D_u 内の x の 1 つまたは複数のインスタンスでは、 S V M は、ラベル・ベクトル

20

【数 1】

\underline{y}

を、損失低減 (L R) ベースの予測方法を使用して予測することができる。

式 1 :

【数 2】

$$D^*_s = \operatorname{argmax}_{D_s} (\sum_{x \in D_s} \sum_{i=1}^n ((1 - \underline{y}^i f_i(x)) / 2))$$

30

【数 3】

$$\underline{y}^i \in \{-1, 1\}$$

に制約 (最大の信頼性を備えた最大損失低減の式)

40

【 0 0 4 2 】

期待される損失低減は、最も信頼できるラベル・ベクトル

【数 4】

\underline{y}

を用いて計算することができる。

式 2 :

【数 5】

50

$$\text{スコア}(x) = \sum_{i=1}^k ((1 - y_i f_i(x)) / 2)$$

【 0 0 4 3 】

スコア (x) は、D_u内のすべてのxについて学習コンポーネント310によって降順でソートすることができる。したがって、最大スコアを有するS個の例D^{*}_Sのセットを選択（または遠隔ワークステーション・デバイス316を介して入力）することができ、トレーニング・セットD₁ ← D₁ + D^{*}_Sを更新することができる。その後、D₁を有するマルチラベル学習器1は、学習コンポーネント310によって訓練することができ、ここで、t = t + 1である。f_i (x) は、クラスiに関連するSVM分類器である。x₁ . . . x_n データ・ポイントは、ネットワーク・セグメント、ワークロード、データ駆動型など、1つまたは複数のグループ化パターンのベクトルを特徴とすることができる。学習アルゴリズムを使用して、グループ・パターンを定義し、履歴を再利用してパターンをキャプチャし、既知の脆弱性のパッチを繰り返し使用することができる。

10

【 0 0 4 4 】

調整コンポーネント306は、クラウド・ネットワーク102、108環境を修正または調整あるいはその両方を行うことができる。例えば、特定の物理マシン104がリスク要因を高めやすい場合、調整コンポーネント306は、物理マシン106、110のグループから物理マシン104を取り外してリスクを軽減することができる。調整コンポーネント306は、物理マシン110に関連するパッチを他の物理マシン104、106に適用できるように、物理マシン110を物理マシン104、106の特定のグループに追加することもできることに留意されたい。逆に、遠隔ワークステーション・デバイス316を使用して、マシン・パッチング・コンポーネント302による分析のための追加の入力データを提供することができる。例えば、遠隔ワークステーション・デバイス316からのユーザ入力と競合する自動化プロセスに応答して、ユーザ入力は自動化されたプロセスを上書きすることができる。

20

【 0 0 4 5 】

遠隔ワークステーション・デバイス316からの入力データは、マシン・パッチング・コンポーネント302による分析および再利用のために学習コンポーネント310に送信することができる。遠隔ワークステーション・デバイス316からの入力データは、パッチ・データベース320またはパターン・データベース318あるいはその両方に保存することができる。パターン・データベース318は、パッチ・グループ、クラスタリング、動的環境に関連するデータを保存し、それに関連するパターンを識別するように構成することができる。例えば、学習コンポーネント310によって認識されるパターンは、パターン・データベース318に格納することができる。パッチ・データベース320は、さまざまなパッチに関連し、特定のパッチ・グループに対して脆弱性を軽減するデータを格納するように構成することができる。

30

【 0 0 4 6 】

プロセッサ314の態様は、マシン内で具体化される、例えば、1つまたは複数のマシンに関連する1つまたは複数のコンピュータ可読媒体で具体化されるマシン実行可能コンポーネントを構成することができる。このようなコンポーネントは、1つまたは複数のマシン、例えばコンピュータ、コンピューティング・デバイス、仮想マシンなどによって実行されると、マシン・パッチング・コンポーネント302に記述された操作をマシンに実行させることができる。一態様では、マシン・パッチング・コンポーネント302は、コンピュータ実行可能コンポーネントおよび命令を格納するメモリ312も含むことができる。

40

【 0 0 4 7 】

図4は、本明細書で説明される1つまたは複数の実施形態によるストリーム・クラスタリングを容易にする例示的で非限定的なシステム400のさらに別のブロック図を示す。本明細書で説明される他の実施形態で使用される同様の要素の繰り返しの説明は、簡潔さ

50

のために省略される。

【 0 0 4 8 】

システム 4 0 0 は、データ抽象化コンポーネント 4 0 2、データ構造統計要約コンポーネント 4 0 4、およびクラスタリング・コンポーネント 4 0 6 を備え、前述のコンポーネントは互いに電氣的または通信可能あるいはその両方で結合される。

【 0 0 4 9 】

物理マシン 1 0 4 に遅れが生じていることを制御デバイス 1 1 2 が決定することに応答して、制御デバイス 1 1 2 は、制御情報を生成して物理マシン 1 0 6 に送信し、物理マシン 1 0 6 に動作速度を増加させて物理マシン 1 0 6 のパフォーマンス（動的環境の変化など）を補償させることができる。したがって、制御デバイス 1 1 2 は、物理マシン 1 0 4 と物理マシン 1 0 6 を異なるグループにグループ化することができる。動的な環境の変化に応じてデータ・ポイントを継続的かつ絶えずに受信できるため、データ・ストリームをデータのチャンクとして処理することができる。物理マシングループを作成または削除あるいはその両方を行うクラスタリング・アルゴリズムを使用して、クラウド・ネットワーク 1 0 2、1 0 8 を変更することができる。継続的なデータ・ストリームは、環境の変化を表し、環境の変化を起こすことができる。したがって、クラスタリング・アルゴリズムが（図 5 に関して後述するマイクロクラスタの単位で）実行されると、データ抽象化コンポーネント 4 0 2 は、アルゴリズムへの入力としてデータを要約することができる。データはそのデータ・ソースに固有またはカスタムである可能性があるため、データ構造統計要約コンポーネント 4 0 4 のターゲット・データ構造に従ってデータをフォーマットする（例えば、平均、頻度など）ことができる。その後、クラスタリング・コンポーネント 4 0 6 は、クラスタリングを実行するためにフォーマットされたデータを受信することができる。

【 0 0 5 0 】

図 5 は、本明細書で説明される 1 つまたは複数の実施形態によるマイクロストリーム・クラスタリングを容易にする例示的で非限定的なシステムの追加のブロック図を示す。本明細書で説明される他の実施形態で使用される同様の要素の繰り返しの説明は、簡潔さのために省略される。

【 0 0 5 1 】

システム 5 0 0 は、マイクロクラスタ $5 0 2_1 \dots 5 0 2_q$ としてセグメント化されたデータ・パケットを含むことができる。さまざまなストリームベースのクラスタリング・アルゴリズム（例えば、マイクロクラスタなど）が異なる方法でクラスタリングを実行できることを理解されたい。例えば、クラスタリング・コンポーネント 4 0 6 は、マイクロクラスタ $5 0 2_1 \dots 5 0 2_q$ のリストを生成することができる。 N_2 、 LS_2 、 SS_2 、 LST_2 、および $SSST_2$ というさまざまな名前でもマイクロクラスタ $5 0 2_2$ を表すことができる。さらに、1 つまたは複数の物理マシン 1 0 4、1 0 6、1 1 0 は、マイクロクラスタ名で表すことができる。したがって、制御デバイス 1 1 2 は、物理マシンと、物理マシンを関連付けることができる 1 つまたは複数のマイクロクラスタを迅速に識別することができる。

【 0 0 5 2 】

図 6 は、本明細書で説明される 1 つまたは複数の実施形態による例示的で非限定的なプロセス概要のフロー図を示す。本明細書で説明される他の実施形態で使用される同様の要素の繰り返しの説明は、簡潔さのために省略される。

【 0 0 5 3 】

方法 6 0 0 は、前述のシステムを促進するために使用することができる。要素 6 0 2 では、物理マシンが動作している環境を発見でき、環境は動的に変化する可能性があることに注意する。システムは、要素 6 0 4 で（例えば、リスク評価コンポーネント 3 0 8 を介して）共通性分析を実行して、パッチ・グループ・セットおよび共有要素を構成することができる。共通性分析は、物理マシンに関連する知覚された脆弱性に基づくことができる。要素 6 0 6 では、パッチ・データベース 3 2 0 から受信したデータに基づいて、物理マ

10

20

30

40

50

シンはクラスタ・パッチ・グループであると判断でき、要素 6 0 8 では（例えば、リスク評価コンポーネント 3 0 8 を介して）クラスタ・パッチ・グループのリスク測定値を評価することができる。

【 0 0 5 4 】

要素 6 0 8 でのリスク測定値に基づいて、要素 6 1 0 で（例えば、監視コンポーネント 3 0 4 を介して）クラスタ・パッチ・グループにパッチ・ポリシーを適用することができる。要素 6 1 2 で、（例えば、監視コンポーネント 3 0 4 を介して）（例えば、サーバの追加、サーバの削除など）サーバを監視することができ、マイクロクラスタ・セットを構成することができる。次いで、要素 6 1 4 で（例えば、リスク評価コンポーネント 3 0 8 を介して）マイクロクラスタのリスク測定値を評価することができ、要素 6 1 6 で（例えば、監視コンポーネント 3 0 4 を介して）マイクロクラスタのための別のパッチを適用することができる。要素 6 1 8 で、グループ・データを更新し、パターン・データベース 3 1 8 に格納されたパターンを評価することができる。要素 6 2 0 で、システムは、（例えば、マシン学習アルゴリズムを活用する学習コンポーネント 3 1 0 を介して）パターンが既知かどうかを判定することができる。要素 6 2 0 で、方法 6 0 0 は、脆弱性およびパッチ根拠に関連するパターンを識別することを含むことができる。パターンが見つからない場合、プロセスは要素 6 1 2 を繰り返すことができる。しかしながら、パターンが見つかった場合、パターンは要素 6 2 2 で既知のパターンとして決定され、パターン・データベース 3 1 8 で更新される。その結果、要素 6 2 4 で、要素 6 1 2 で監視されるように新しいパターンを更新することができる。

【 0 0 5 5 】

図 7 は、本明細書で説明される 1 つまたは複数の実施形態によるリスク測定値の評価を容易にする例示的で非限定的なフロー図 7 0 0 を示す。本明細書で説明される他の実施形態で使用される同様の要素の繰り返しの説明は、簡潔さのために省略される。

【 0 0 5 6 】

リスク測定値を評価するプロセスは、ブロック 7 0 2 で開始することができる。システムは、ブロック 7 0 4 で、（例えば、リスク評価コンポーネント 3 0 8 を介して）マシンがリスクを被りやすいかどうかを決定することができる。マシンがリスクを被りやすい場合は、プロセスはブロック 7 0 6 で終了することができる。しかし、システムがブロック 7 0 4 でリスクを被りやすいマシンを特定する場合、システムは（例えば、監視コンポーネント 3 0 4 を介して）マシンに関連するリスクを評価することができる。例えば、高リスクの可能性が 1 % を超える、または中リスクが 2 0 % を超えるあるいはその両方の場合、ブロック 7 1 0 でマシンは（例えば、リスク評価コンポーネント 3 0 8 を介して）高リスク・マシンとしてラベル付けすることができ、プロセスはブロック 7 0 6 で終了することができる。逆に、高リスクが 1 % 未満または中リスクの 2 0 % 未満あるいはその両方である場合、システムは他のリスク要因のチェックに進むことができる。サーバが 0 % より大きく 1 % 以下の高リスク・マシン、または 2 % から 2 0 % の間の中リスク・マシン、または 5 0 % より大きい低リスク・マシンを有しているとシステムが判断した場合、マシンは（例えば、リスク評価コンポーネント 3 0 8 を介して）中程度のリスクとしてラベル付けすることができ、プロセスはブロック 7 0 6 で終了することができる。逆に、前述の要因のいずれかが満たされない場合、システムは、要素 7 1 6 で（例えば、リスク評価コンポーネント 3 0 8 を介して）マシンを低リスクとしてラベル付けして、ブロック 7 0 6 で終了することができる。本開示に関連して前述のリスクのパーセンテージおよび仕切りが使用されたが、他のパーセンテージおよび仕切りをリスクのしきい値に基づいて使用することができることを理解されたい。

【 0 0 5 7 】

図 8 は、本明細書で説明する 1 つまたは複数の実施形態による、マシンのグループ化およびパッチ適用を容易にする例示的で非限定的なコンピュータ実装方法 8 0 0 のフロー図を示す。本明細書で説明される他の実施形態で使用される同様の要素の繰り返しの説明は、簡潔さのために省略される。

【 0 0 5 8 】

要素 8 0 2 において、方法 8 0 0 は、第 1 のサーバ・デバイスに関連する第 1 のリスクに応じて、プロセッサに動作可能に結合されたデバイスによって、第 1 のサーバ・デバイスおよび第 2 のサーバ・デバイスの脆弱性を軽減するために、（例えば、リスク評価コンポーネント 3 0 8 を介して）サーバ・グループにパッチ適用することを含み、サーバ・グループは第 1 のサーバ・デバイスおよび第 2 のサーバ・デバイスからなる。要素 8 0 4 で、方法 8 0 0 は、デバイスによって、サーバ・グループに対する第 2 のリスクを軽減するために、（例えば、監視コンポーネント 3 0 4 を介して）サーバ・グループに対する第 2 のリスクに関連するデータを監視することを含む。

【 0 0 5 9 】

図 9 は、本明細書で説明する 1 つまたは複数の実施形態による、マシンのグループ化およびパッチ適用を容易にする別の例示的で非限定的なコンピュータ実装方法 9 0 0 のフロー図を示す。本明細書で説明される他の実施形態で使用される同様の要素の繰り返しの説明は、簡潔さのために省略される。

【 0 0 6 0 】

要素 9 0 2 において、方法 9 0 0 は、第 1 のサーバ・デバイスに関連する第 1 のリスクに応じて、プロセッサに動作可能に結合されたデバイスによって、第 1 のサーバ・デバイスおよび第 2 のサーバ・デバイスの脆弱性を軽減するために、（例えば、リスク評価コンポーネント 3 0 8 を介して）サーバ・グループにパッチ適用することを含み、サーバ・グループは第 1 のサーバ・デバイスおよび第 2 のサーバ・デバイスからなる。要素 9 0 4 で、方法 9 0 0 は、デバイスによって、サーバ・グループに対する第 2 のリスクを軽減するために、（例えば、監視コンポーネント 3 0 4 を介して）サーバ・グループに対する第 2 のリスクに関連するデータを監視することを含む。加えて、要素 9 0 6 で、方法 9 0 0 は、デバイスによって、サーバ・グループの第 2 のリスクを軽減するために、（例えば、調整コンポーネント 3 0 6 を介して）サーバ・グループを修正し、サーバ・グループの修正をもたらすことを含む。

【 0 0 6 1 】

図 1 0 は、本明細書で説明する 1 つまたは複数の実施形態による、マシンのグループ化およびパッチ適用を容易にする別の例示的で非限定的なコンピュータ実装方法 1 0 0 0 のフロー図を示す。本明細書で説明される他の実施形態で使用される同様の要素の繰り返しの説明は、簡潔さのために省略される。

【 0 0 6 2 】

要素 1 0 0 2 で、方法 1 0 0 0 は、第 1 のサーバ・デバイスに関連する第 1 のリスクに応じて、プロセッサに動作可能に結合されたデバイスによって、第 1 のサーバ・デバイスおよび第 2 のサーバ・デバイスの脆弱性を軽減するために、（例えば、リスク評価コンポーネント 3 0 8 を介して）サーバ・グループにパッチ適用することを含み、サーバ・グループは第 1 のサーバ・デバイスおよび第 2 のサーバ・デバイスからなる。要素 1 0 0 4 で、方法 1 0 0 0 は、デバイスによって、サーバ・グループに対する第 2 のリスクを軽減するために、（例えば、監視コンポーネント 3 0 4 を介して）サーバ・グループに対する第 2 のリスクに関連するデータを監視することを含む。さらに、要素 1 0 0 6 で、方法は、（例えば、調整コンポーネント 3 0 6 を介して）サーバ・グループが修正されたという示唆を受信することを含むことができる。

【 0 0 6 3 】

開示される主題の種々の態様についての文脈を与えるために、図 1 1 および以下の説明は、開示される主題の種々の態様を実装できる適切な環境の一般的な説明を提供するように意図される。図 1 1 は、本明細書に説明される 1 つまたは複数の実施形態を容易にすることができる限定されない例示的動作環境のブロック図を示す。簡潔にするために、本明細書で説明される他の実施形態において用いられる同様の要素の反復的な説明は省略する。図 1 1 を参照すると、本開示の種々の態様を実施するための好適な動作環境 1 1 0 0 が、コンピュータ 1 1 1 2 を含むこともできる。コンピュータ 1 1 1 2 は、処理ユニット 1

10

20

30

40

50

114、システム・メモリ1116およびシステム・バス1118を含むこともできる。システム・バス1118は、これに限定されるものではないが、システム・メモリ1116を含むシステム・コンポーネントを処理ユニット1114に結合する。処理ユニット1114は、種々の利用可能なプロセッサのいずれかとして行うことができる。二重マイクロプロセッサおよび他のマルチプロセッサ・アーキテクチャを処理ユニット1114として用いることもできる。システム・バス1118は、メモリ・バスまたはメモリ・コントローラ、周辺バスまたは外部バス、または、これらに限定されるものではないが、業界標準アーキテクチャ (ISA)、マイクロチャネル・アーキテクチャ (MSA)、拡張ISA (EISA)、Intelligent Drive Electronics (IDE)、VESA Local Bus (VLB)、Peripheral Component Interconnect (PCI)、カード・バス、ユニバーサル・シリアル・バス (USB)、Advanced Graphics Port (AGP)、Firewire (IEEE1394)、およびSmall Computer Systems Interface (SCSI)を含む任意の種々の利用可能なバス・アーキテクチャを用いたローカル・バスあるいはその組み合わせを含む、幾つかのタイプのバス構造体のいずれかとして行うことができる。

【0064】

システム・メモリ1116はまた、揮発性メモリ1120および不揮発性メモリ1122を含むこともできる。起動の際などにコンピュータ1112内の要素間で情報を転送するための基本ルーチンを含む基本入力/出力システム (BIOS) は、不揮発性メモリ1122内に格納される。限定ではなく例証として、不揮発性メモリ1122は、読み取り専用メモリ (ROM)、プログラム可能ROM (PROM)、電氣的プログラム可能ROM (EPROM)、電氣的消去可能ROM (EEPROM)、フラッシュ・メモリ、または不揮発性ランダム・アクセス・メモリ (RAM) (例えば、強誘電体RAM (FeRAM))を含むことができる。揮発性メモリ1120は、外部キャッシュ・メモリとして働くランダム・アクセス・メモリ (RAM)を含むことができる。限定ではなく例証として、RAMは、スタティックRAM (SRAM)、ダイナミックRAM (DRAM)、シンクロナスDRAM (SDRAM)、ダブル・データ・レートSDRAM (DDR SDRAM)、エンハンストSDRAM (ESDRAM)、シンクリンク (Synchlink) DRAM (SLDRAM)、ダイレクト・ランバス (Rambus) RAM (DRRAM)、ダイレクト・ランバス・ダイナミックRAM (DRDRAM)、およびランバス・ダイナミックRAMのような多くの形態で利用可能である。

【0065】

コンピュータ1112はまた、取り外し可能/取り外し不能な揮発性/不揮発性コンピュータ・ストレージ媒体を含むこともできる。図11は、例えば、ディスク・ストレージ1124を示す。ディスク・ストレージ1124は、これらに限定されるものではないが、磁気ディスク・ドライブ、フロッピー (R) ・ディスク・ドライブ、テープ・ドライブ、Jazドライブ、Zipドライブ、LS-100ドライブ、フラッシュ・メモリ・カード、またはメモリ・スティックのようなデバイスを含むこともできる。ディスク・ストレージ1124は、別個の、またはコンパクト・ディスクROMデバイス (CD-ROM)、CD記録可能ドライブ (CD-Rドライブ)、CD書き換え可能ドライブ (CD-RWドライブ) またはデジタル多用途ディスクROMドライブ (DVD-ROM) などの光ディスク・ドライブを含むがこれらに限定されない他のストレージ・メディアと組み合わせたストレージ・メディアを含むこともできる。システム・バス1118へのディスク・ストレージ1124の接続を容易にするために、一般的に、インターフェース1126のような、取り外し可能または取り外し不能インターフェースが用いられる。図11は、ユーザと好適な動作環境1100において説明される基本コンピュータ・リソースとの間の媒介として働くソフトウェアも示す。そうしたソフトウェアは、例えば、オペレーティング・システム1128を含むこともできる。ディスク・ストレージ1124上に格納することができるオペレーティング・システム1128は、コンピュータ1112のリソースを

制御し、割り当てるように働く。

【 0 0 6 6 】

システム・アプリケーション 1 1 3 0 は、例えばシステム・メモリ 1 1 1 6 内またはディスク・ストレージ 1 1 2 4 上に格納された、プログラム・モジュール 1 1 3 2 およびプログラム・データ 1 1 3 4 を通じたオペレーティング・システム 1 1 2 8 によるリソースの管理を利用する。この開示は、種々のオペレーティング・システム、またはオペレーティング・システムの組み合わせにより実施できることを認識されたい。ユーザは、入力デバイス 1 1 3 6 を通じてコマンドまたは情報をコンピュータ 1 1 1 2 に入力する。入力デバイス 1 1 3 6 は、これらに限定されるものではないが、マウス、トラックボール、スタイラス、タッチ・パッドのようなポインティング・デバイス、キーボード、マイクロホン、ジョイスティック、ゲーム・パッド、衛星放送受信アンテナ、スキャナ、TVチューナ・カード、デジタル・カメラ、デジタル・ビデオ・カメラ、ウェブ・カメラ等を含む。これらおよび他の入力デバイスは、インターフェース・ポート 1 1 3 8 を介してシステム・バス 1 1 1 8 を通じて処理ユニット 1 1 1 4 に接続される。インターフェース・ポート 1 1 3 8 は、例えば、シリアル・ポート、パラレル・ポート、ゲーム・ポートおよびユニバーサル・シリアル・バス (USB) を含む。出力デバイス 1 1 4 0 は、入力デバイス 1 1 3 6 と同じタイプのポートの一部を使用する。したがって、例えば、USB ポートを用いて、コンピュータ 1 1 1 2 への入力を提供し、出力情報をコンピュータ 1 1 1 2 から出力デバイス 1 1 4 0 に提供することができる。出力アダプタ 1 1 4 2 は、特別なアダプタを必要とする他の出力デバイス 1 1 4 0 の中でも、モニタ、スピーカおよびプリンタのような幾つかの出力デバイス 1 1 4 0 があることを示すように提供される。出力アダプタ 1 1 4 2 は、限定ではなく例示として、出力デバイス 1 1 4 0 とシステム・バス 1 1 1 8 との間の接続手段を提供するビデオおよび音声カードを含む。遠隔コンピュータ 1 1 4 4 のような、他のデバイスまたはデバイスのシステムあるいはその両方は、入力および出力の機能の両方を提供することに留意されたい。

【 0 0 6 7 】

コンピュータ 1 1 1 2 は、遠隔コンピュータ 1 1 4 4 のような 1 つまたは複数の遠隔コンピュータへの論理接続を用いるネットワーク化環境で動作することができる。遠隔コンピュータ 1 1 4 4 は、コンピュータ、サーバ、ルータ、ネットワーク PC、ワークステーション、マイクロプロセッサ・ベースのアプライアンス、ピア・デバイス、または他の共通ネットワーク・ノード等とすることができ、一般的に、コンピュータ 1 1 1 2 に関して記載される要素の多くまたはすべてを含むこともできる。簡潔にするために、メモリ・ストレージ・デバイス 1 1 4 6 だけが、遠隔コンピュータ 1 1 4 4 と共に示されている。遠隔コンピュータ 1 1 4 4 は、ネットワーク・インターフェース 1 1 4 8 を通じてコンピュータ 1 1 1 2 に論理的に接続され、次に、通信接続 1 1 5 0 を介して物理的に接続される。ネットワーク・インターフェース 1 1 4 8 は、ローカルエリア・ネットワーク (LAN)、広域エリア・ネットワーク (WAN)、セルラー・ネットワーク等のような有線または無線あるいはその両方の通信ネットワークを含む。LAN 技術として、Fiber Distributed Data Interface (FDDI)、Copper Distributed Data Interface (CDDI)、イーサネット (R)、トークン・リング等が挙げられる。WAN 技術として、これらに限定されるものではないが、ポイントツーポイント・リンク、統合サービス・デジタル網 (Integrated Service Digital Networks: ISDN) およびその変形のような回路交換網、パケット交換網、およびデジタル加入者線 (Digital Subscriber Line: DSL) が挙げられる。通信接続 1 1 5 0 は、ネットワーク・インターフェース 1 1 4 8 をシステム・バス 1 1 1 8 に接続するために用いられるハードウェア/ソフトウェアを指す。通信接続 1 1 5 0 は、明確に示すためにコンピュータ 1 1 1 2 内部に示されるが、これはコンピュータ 1 1 1 2 の外部にあってもよい。ネットワーク・インターフェース 1 1 4 8 への接続のためのハードウェア/ソフトウェアは、例示のためだけに、正規電話グレード・モデム (regular telephone grade

10

20

30

40

50

modem)、ケーブル・モデムおよびDSLモデムを含むモデム、ISDNアダプタ、およびイーサネット(R)・カードのような内部および外部技術を含むこともできる。

【0068】

ここで図12を参照すると、例証的なクラウド・コンピューティング環境1200が示される。図示のように、クラウド・コンピューティング環境1200は、クラウド50、および、例えば、携帯情報端末(PDA)または携帯電話54A、デスクトップ・コンピュータ54B、ラップトップ・コンピュータ54C、または自動車コンピュータ・システム54Nあるいはその組み合わせなどといった、クラウド・コンシューマによって用いられるローカル・コンピューティング・デバイスが通信することができる、1つまたは複数のクラウド・コンピューティング・ノード10を含む。ノード10は、互いに通信することができる。ノード10は、上述のようなプライベート・クラウド、コミュニティ・クラウド、パブリック・クラウド、もしくはハイブリッド・クラウド、また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において物理的または仮想的にグループ化することができる(図示せず)。これにより、クラウド・コンピューティング環境1200は、クラウド・コンシューマがローカル・コンピューティング・デバイス上にリソースを保持する必要のないサービスとして、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その組み合わせを提供することが可能になる。図12に示されるコンピューティング・デバイス54A~Nのタイプは単に例示であることを意図し、コンピューティング・ノード10およびクラウド50は、いずれのタイプ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あるいはその両方でも(例えば、ウェブ・ブラウザを用いて)、いずれのタイプのコンピュータ化された装置とも通信できることを理解されたい。

10

20

【0069】

ここで図13を参照すると、クラウド・コンピューティング環境1200(図12)によって提供される機能抽象化層1300のセットが示される。図13に示されるコンポーネント、層、および機能は単に例示であることを意図し、本発明の実施形態はそれらに限定されないことを予め理解されたい。図示されるように、以下の層および対応する機能が提供される。

【0070】

ハードウェアおよびソフトウェア層60は、ハードウェア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として、メインフレーム61と、RISC(Reduced Instruction Set Computer(縮小命令セット・コンピュータ))アーキテクチャ・ベースのサーバ62と、サーバ63と、ブレード・サーバ64と、ストレージ・デバイス65と、ネットワークおよびネットワークング・コンポーネント66とが含まれる。幾つかの実施形態において、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67およびデータベース・ソフトウェア68を含む。

30

【0071】

仮想化層70は、抽象化層を提供し、この層により、仮想エンティティの以下の例、すなわち、仮想サーバ71、仮想ストレージ72、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73、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74、ならびに仮想クライアント75を提供することができる。

40

【0072】

一例においては、管理層80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81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・リソースおよび他のリソースの動的な調達を提供する。計量および価格決定82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る際のコスト追跡と、リソースの消費に対する課金または請求とを提供する。1つの例においては、これらのリソースは、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・コンシューマおよびタスクに対する識

50

別情報の検証と、データおよび他のリソースに対する保護とを提供する。ユーザ・ポータル 83 は、コンシューマおよびシステム管理者のために、クラウド・コンピューティング環境へのアクセスを提供する。サービス・レベル管理 84 は、要求されるサービス・レベルが満たされるように、クラウド・コンピューティング・リソースの割り当ておよび管理を提供する。サービス・レベル・アグリーメント (Service Level Agreement、SLA) の計画および履行 85 は、SLA に従って将来の要件が予測されるクラウド・コンピューティング・リソースの事前配置および調達を提供する。

【0073】

ワークロード層 90 は、クラウド・コンピューティング環境を利用することができる機能の例を提供する。この層から提供することができるワークロードおよび機能の例には、マッピングおよびナビゲーション 91、ソフトウェア開発およびライフサイクル管理 92、仮想教室教育配信 93、データ分析処理 94、トランザクション処理 95、およびストリーム・クラスタリングを使用したパッチ・グループの動的な再構成が含まれる。

【0074】

本発明は、統合のいずれかの可能な技術的詳細レベルにおける、システム、方法、装置、またはコンピュータ・プログラム製品あるいはその組み合わせとすることができる。コンピュータ・プログラム製品は、プロセッサに本開示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有するコンピュータ可読ストレージ媒体を含むことができる。コンピュータ可読ストレージ媒体は、命令実行デバイスにより使用される命令を保持および格納できる有形デバイスとすることができる。コンピュータ可読ストレージ媒体は、例えば、これらに限定されるものではないが、電子記憶装置、磁気記憶装置、光学記憶装置、電磁気記憶装置、半導体記憶装置、または上記のいずれかの適切な組み合わせとすることができる。コンピュータ可読ストレージ媒体のより具体的な例の非網羅的なリストとして、以下のもの：すなわち、ポータブル・コンピュータ・ディスク、ハード・ディスク、ランダム・アクセス・メモリ (RAM)、読み出し専用メモリ (ROM)、消去可能プログラム可能読み出し専用メモリ (EPROM 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)、ポータブル・コンパクト・ディスク読み出し専用メモリ (CD-ROM)、デジタル多用途ディスク (DVD)、メモリ・スティック、フロッピー (R)・ディスク、パンチカードもしくは命令がそこに記録された溝内の隆起構造のような機械的にエンコードされたデバイス、および上記のいずれかの適切な組み合わせが挙げられる。本明細書で使用される場合、コンピュータ可読ストレージ媒体は、電波、または他の自由に伝搬する電磁波、導波管もしくは他の伝送媒体を通じて伝搬する電磁波 (例えば、光ファイバケーブルを通る光パルス)、またはワイヤを通して送られる電気信号などの、一時的信号自体として解釈されない。

【0075】

本明細書で説明されるコンピュータ可読プログラム命令は、コンピュータ可読ストレージ媒体からそれぞれのコンピューティング/処理デバイスに、または、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その組み合わせなどのネットワークを介して外部コンピュータまたは外部ストレージ・デバイスにダウンロードすることができる。ネットワークは、銅伝送ケーブル、光伝送ファイバ、無線伝送、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・サーバあるいはその組み合わせを含むことができる。各コンピューティング/処理デバイスにおけるネットワーク・アダプタ・カードまたはネットワーク・インターフェースは、ネットワークからコンピュータ可読プログラム命令を受け取り、コンピュータ可読プログラム命令を転送して、それぞれのコンピューティング/処理デバイス内のコンピュータ可読ストレージ媒体内に格納する。本開示の動作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、集積回路の構成データ、または、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もしくは類似のプ

10

20

30

40

50

プログラミング言語など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・コードのいずれかとすることができる。コンピュータ可読プログラム命令は、完全にユーザのコンピュータ上で実行される場合もあり、一部がユーザのコンピュータ上で、独立型ソフトウェア・パッケージとして実行される場合もあり、一部がユーザのコンピュータ上で実行され、一部が遠隔コンピュータ上で実行される場合もあり、または完全に遠隔コンピュータもしくはサーバ上で実行される場合もある。最後のシナリオにおいて、遠隔コンピュータは、ローカル・エリア・ネットワーク（LAN）もしくは広域ネットワーク（WAN）を含むいずれかのタイプのネットワークを通じてユーザのコンピュータに接続される場合もあり、または外部コンピュータへの接続がなされる場合もある（例えば、インターネット・サービス・プロバイダを用いたインターネットを通じて）。幾つかの実施形態において、例えば、プログラム可能論理回路、フィールド・プログラマブル・ゲート・アレイ（FPGA）、またはプログラム可能論理アレイ（PLA）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用いて、電子回路を個人化することによりコンピュータ可読プログラム命令を実行し、本開示の態様を実施することができる。

10

【0076】

本開示の態様は、本開示の実施形態による方法、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内の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ことが理解されるであろう。これらのコンピュータ可読プログラム命令を、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データ処理装置のプロセッサに与えてマシンを製造し、それにより、コンピュータまたは他のプログラム可能データ処理装置のプロセッサによっ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内で指定された機能／動作を実施するための手段を作り出すようにすることができる。これらのコンピュータ・プログラム命令を、コンピュータ、プログラム可能データ処理装置、または他のデバイスを特定の方式で機能させるように指示することができるコンピュータ可読媒体あるいはその組み合わせに格納し、それにより、そのコンピュータ可読媒体内に格納された命令が、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おいて指定された機能／動作の態様を実施する命令を含む製品を含むようにすることもできる。コンピュータ・プログラム命令を、コンピュータ、他のプログラム可能データ処理装置、または他のデバイス上にロードして、一連の動作ステップをコンピュータ、他のプログラム可能データ処理装置、または他のデバイス上で行わせてコンピュータ実施のプロセスを生成し、それにより、コンピュータ、他のプログラム可能装置、または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おいて指定された機能／動作を実行するようにすることもできる。

20

30

【0077】

図面内のフローチャートおよびブロック図は、本開示の種々の実施形態による、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、機能および動作を示す。この点に関して、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命令を含む、モジュール、セグメント、または命令の一部を表すことができる。幾つかの代替的な実装において、ブロック内に示される機能は、図に示される順序とは異なる順序で生じることがある。例えば、連続して示される２つのブロックは、関与する機能に応じて、実際には実質的に同時に実行されることもあり、またはこれらのブロックはときとして逆順で実行されることもある。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、および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、または専用のハードウェアとコンピュータ命令との組み合

40

50

わせを実行する、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ことに留意されたい。

【 0 0 7 8 】

本主題は、1つのコンピュータまたは複数のコンピュータあるいはその両方で実行されるコンピュータ・プログラム製品のコンピュータ実行可能命令の一般的な文脈で上述されたが、当業者であれば、本開示は、他のプログラム・モジュールと組み合わせて実装するまたは実装されることも可能であることを認識するであろう。一般に、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あるいはその両方の、ルーチン、プログラム、コンポーネント、データ構造などを含む。さらに、当業者であれば、本発明のコンピュータ実施方法は、シングルプロセッサまたはマルチプロセッサ・コンピュータ・システム、ミニコンピューティング・デバイス、メインフレーム・コンピュータ、ならびにコンピュータ、手持ち式コンピューティング・デバイス（例えば、PDA、電話）、マイクロプロセッサベースのまたはプログラム可能なコンシューマもしくは産業用電子機器等を含む、他のコンピュータ・システム構成で実施できることを理解するであろう。示される態様は、通信ネットワークを通じてリンクされる遠隔処理デバイスによってタスクが実行される分散型コンピューティング環境で実施することもできる。しかしながら、本開示のすべてではないが一部の態様をスタンドアロン・コンピュータ上で実施することができる。分散型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、ローカルおよび遠隔両方のメモリ・ストレージ・デバイス内に配置することができる。

【 0 0 7 9 】

本出願において用いられるとき、「コンポーネント」、「システム」、「プラットフォーム」、「インターフェース」等の用語は、コンピュータに関連するエンティティ、または1つまたは複数の特定の機能を有する動作マシンに関連するエンティティを指すこと、または含むことあるいはその両方ができる。本明細書に開示されるエンティティは、ハードウェア、ハードウェアとソフトウェアの組み合わせ、ソフトウェア、または実行中のソフトウェアとすることができる。例えば、コンポーネントは、これらに限定されるものではないが、プロセッサ上で実行されているプロセス、プロセッサ、オブジェクト、実行可能ファイル、実行のスレッド、プログラム、またはコンピュータあるいはその組み合わせとすることができる。例証として、サーバ上で実行されているアプリケーションおよびサーバの両方が、コンポーネントであり得る。1つまたは複数のコンポーネントは、プロセスまたは実行のスレッドあるいはその両方内にあることができ、コンポーネントは、1つのコンピュータ上に局所化されること、または2つまたはそれより多いコンピュータ間で分散されることあるいはその両方が可能である。別の例において、それぞれのコンポーネントは、種々のデータ構造が格納された種々のコンピュータ可読媒体から実行することができる。コンポーネントは、1つまたは複数のデータ・パケットを有する信号（例えば、ローカル・システム、分散型システムにおいて、または信号を介する他のシステムと共にあるいはその両方でインターネットなどのネットワークにわたって、別のコンポーネントと対話する1つのコンポーネントからのデータ）などに従って、ローカルまたは遠隔あるいはその両方のプロセスを介して通信することができる。別の例において、コンポーネントは、電気もしくは電子回路により動作される機械的部品により与えられる特定の機能を有し、プロセッサにより実行されるソフトウェアまたはファームウェア・アプリケーションにより動作される装置とすることができる。こうした場合において、プロセッサは、装置の内部にあってもまたは外部にあってもよく、ソフトウェアまたはファームウェア・アプリケーションの少なくとも一部を実行することができる。さらに別の例として、コンポーネントは、機械的部品なしに電子コンポーネントを通じて特別な機能を提供する装置とことができ、電子コンポーネントは、電子コンポーネントの機能を少なくとも部分的に与えるソフトウェアまたはファームウェアを実行するためのプロセッサまたは他の手段を含むことができる。1つの態様において、コンポーネントは、例えば、クラウド・コンピューティング・システム内の物理マシンを介して電子コンポーネントをエミュレートす

ることができる。

【 0 0 8 0 】

付加的に、用語「または (or)」は、排他的「または」ではなく包含的「または」を意味するよう意図される。つまり、特に断らない限りまたは文脈から明らかな場合、「XはAまたはBを用いる」は、自然の包含的順列 (natural inclusive permutation) のいずれかを意味するように意図される。つまり、XはAを用いる；XはBを用いる；または、XはAおよびBの両方を用いる場合、「XはAまたはBを用いる」は、上記の例のいずれかにおいて満たされる。さらに、本明細書および添付の図面において使用される冠詞「1つ (aおよびan)」は一般的に、特に断らない限りまたは文脈から明らかな場合、「1つまたはそれ以上」を単数の形態に向けることを意味するように解釈すべきである。本明細書で用いられる場合、用語「例」または「例示的」あるいはその両方は、例、事例、または例証としての役割を果たすように用いられる。誤解を避けるために、本明細書に開示される主題は、こうした例に限定されない。さらに、用語「例」または「例示的」あるいはその両方として本明細書に説明されるいずれの態様または設計も、他の態様または設計と比べて好ましいまたは有利であるとは限らず、または当業者には周知の同等の例示的構造および技術を排除することを意味するものではない。

【 0 0 8 1 】

本明細書で用いられるとき、用語「プロセッサ」は、これらに限定されるものではないが、シングルコア・プロセッサ、ソフトウェア・マルチスレッド実行能力を有するシングルプロセッサ、マルチコア・プロセッサ、ソフトウェア・マルチスレッド実行能力を有するマルチコア・プロセッサ、ハードウェア・マルチスレッド技術を有するマルチコア・プロセッサ、並列プラットフォーム、および分散型共有メモリを有する並列プラットフォームを含む、実質的にあらゆるコンピューティング処理ユニットまたはデバイスを指すことができる。付加的に、プロセッサは、集積回路、特定用途向け集積回路 (ASIC)、デジタル・シグナル・プロセッサ (DSP)、フィールド・プログラマブル・ゲート・アレイ (FPGA)、プログラマブル論理コントローラ (PLC)、結合プログラム可能論理デバイス (complex programmable logic device、CPLD)、ディスクリート・ゲートまたはトランジスタ論理、ディスクリート・ハードウェア・コンポーネント、または本明細書で説明される機能を実施するように設計されたそれらの任意の組み合わせを指すことができる。さらに、プロセッサは、空間使用量を最適化するまたはユーザ機器の性能を高めるために、これらに限定されるものではないが、分子および量子ドット・ベースのトランジスタ、スイッチおよびゲートのようなナノスケール・アーキテクチャを利用することができる。プロセッサはまた、コンピューティング処理ユニットの組み合わせとして実装することもできる。本開示において、「ストア」、「ストレージ」、「データ・ストア」、「データ・ストレージ」、「データベース」、ならびに動作およびコンポーネントの機能に関連した実質的に他のいずれかの情報ストレージ・コンポーネントのような用語は、「メモリ・コンポーネント」、「メモリ」内に具体化されたエンティティ、またはメモリを含むコンポーネントを指すために用いられる。本明細書で説明されるメモリまたはメモリ・コンポーネントあるいはその両方は、揮発性メモリもしくは不揮発性メモリのいずれかとなることができ、または揮発性メモリおよび不揮発性メモリの両方を含むことができることを認識されたい。限定ではなく例証として、不揮発性メモリは、読み取り専用メモリ (ROM)、プログラム可能ROM (PROM)、電氣的プログラム可能ROM (EPROM)、電氣的消去可能ROM (EEPROM)、フラッシュ・メモリ、または不揮発性ランダム・アクセス・メモリ (RAM) (例えば、強誘電体RAM (FeRAM)) を含むことができる。揮発性メモリは、例えば外部キャッシュ・メモリとして働くRAMを含むことができる。限定ではなく例証として、RAMは、シンクロナスRAM (SRAM)、ダイナミックRAM (DRAM)、シンクロナスDRAM (SDRAM)、ダブル・データ・レートSDRAM (DDR SDRAM)、エンハンスドSDRAM (ESDRAM)、シンクリンクDRAM (SLDRAM)、ダイレクト・ランバスRAM (DRRAM)、ダイレクト・ランバス・ダイナミックRAM (DRDRAM)、およびランバ

10

20

30

40

50

ス・ダイナミック R A M のような多くの形態で利用可能である。さらに、システムまたはコンピュータ実施方法の開示されたメモリ・コンポーネントは、これらおよび他のいずれかの好適なタイプのメモリを含むが、これらに限定されないことを意図する。

【 0 0 8 2 】

上述したものは、システムおよびコンピュータ実施方法の単なる例を含む。もちろん、本開示を説明するためにコンポーネントまたはコンピュータ実施方法のあらゆる考えられる組み合わせを説明することはできないが、当業者であれば、本開示の多くのさらなる組み合わせおよび順列が可能であることを認識することができる。さらに、用語「含む (include)」、「有する (have)」、「持っている (possess)」等が詳細な説明、特許請求の範囲、および添付図面に用いられる範囲で、そうした用語は、用語「備える (comprising)」が特許請求の範囲中で移行語として用いられるときに解釈されるように用語「備える (comprising)」と同様に包括的であることが意図されている。

10

【 0 0 8 3 】

種々の実施形態の説明が例証のために提示されたが、網羅的であることまたは開示される実施形態を制限することを意図するものではない。当業者には、説明される実施形態の範囲および思想から逸脱することなく、多くの変更および変形が明らかであろう。本明細書で用いられる用語は、実施形態の原理、実際の用途、または市場で見出される技術に優る技術の改善を最もよく説明するために、または、当業者が本明細書で開示される実施形態を理解することができるように、選択された。

20

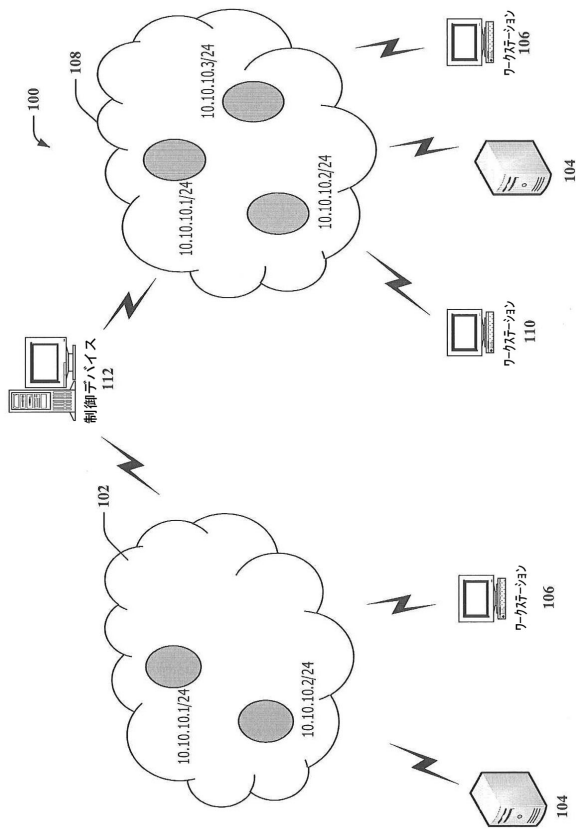
30

40

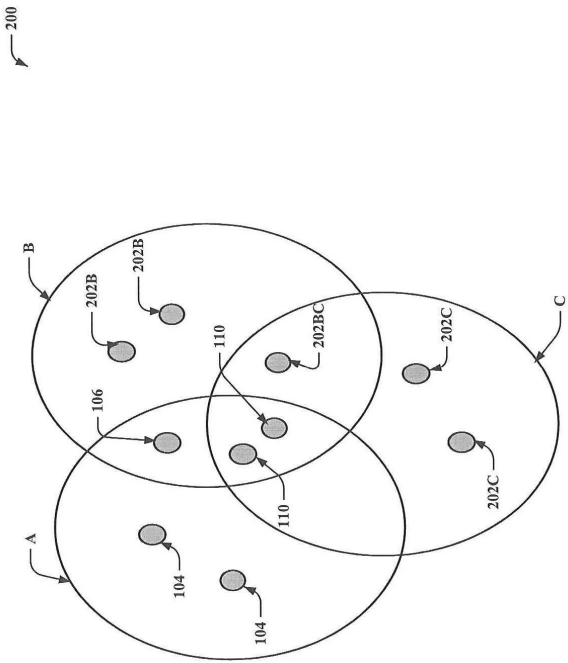
50

【図面】

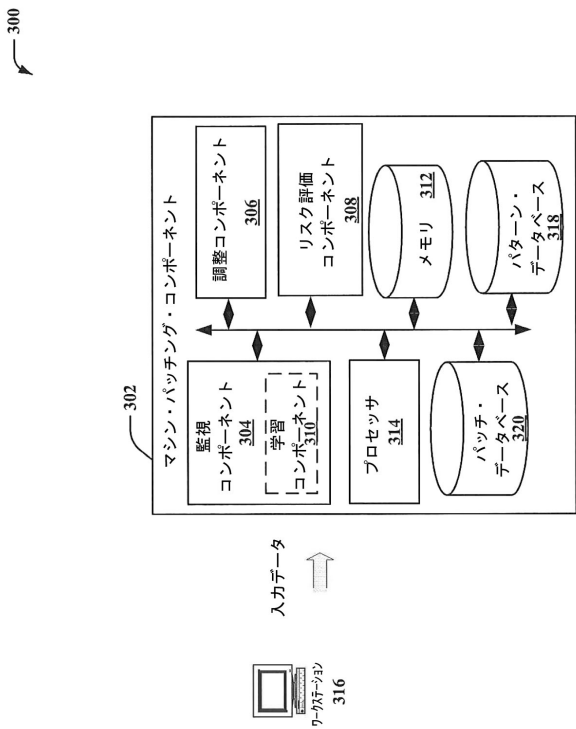
【図 1】



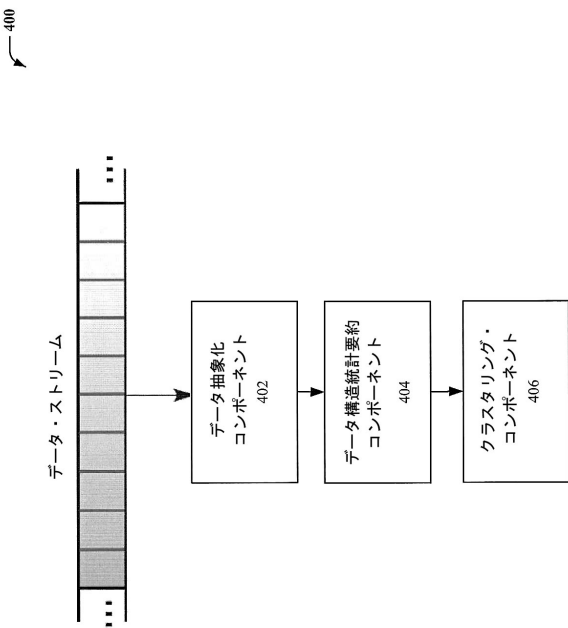
【図 2】



【図 3】



【図 4】



10

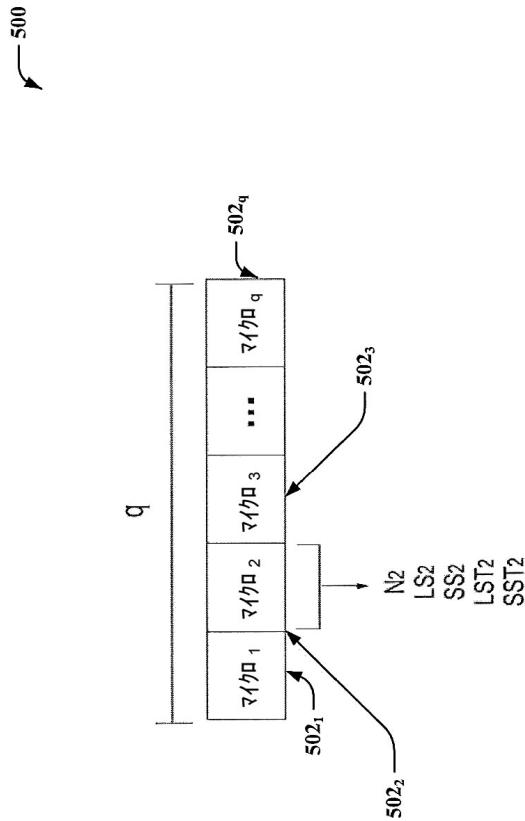
20

30

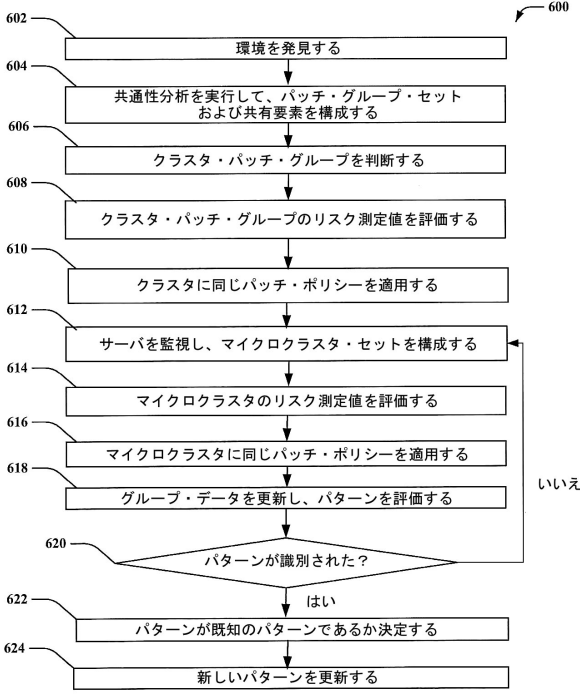
40

50

【図 5】



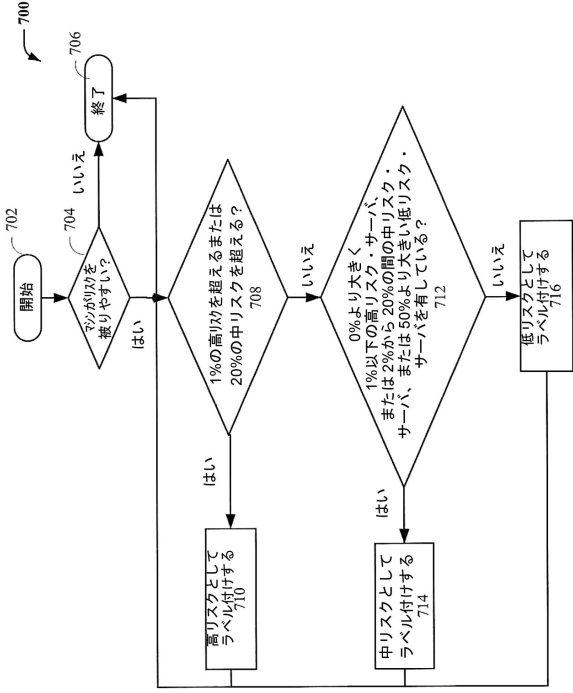
【図 6】



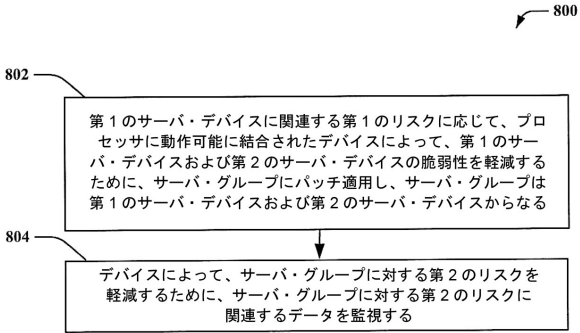
10

20

【図 7】



【図 8】

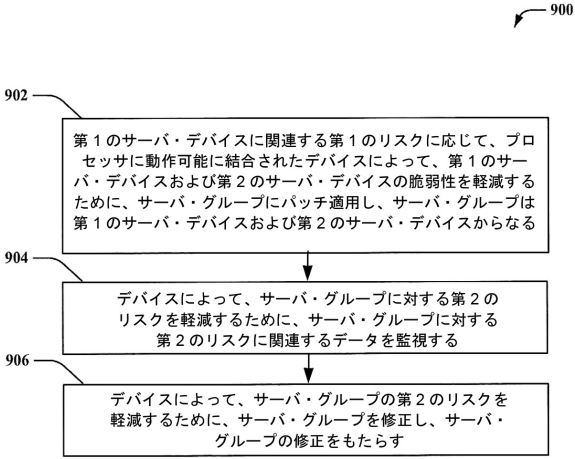


30

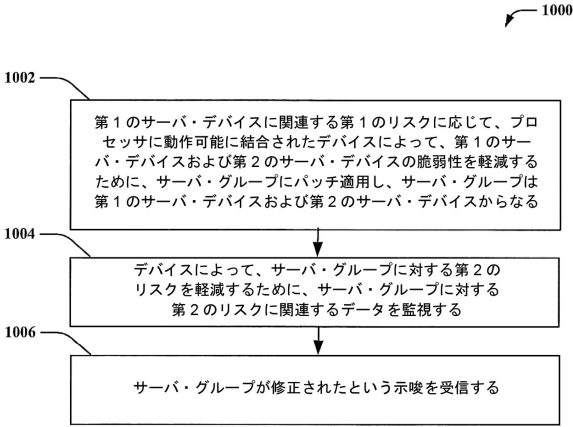
40

50

【図 9】

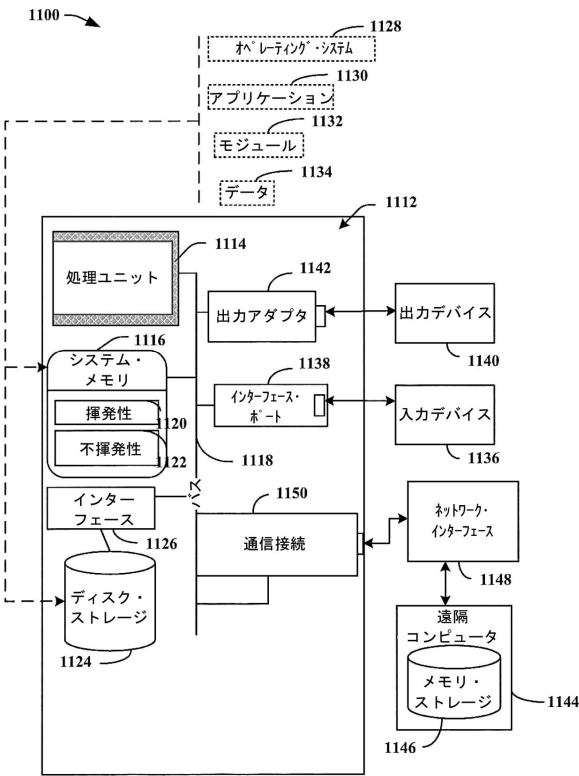


【図 10】

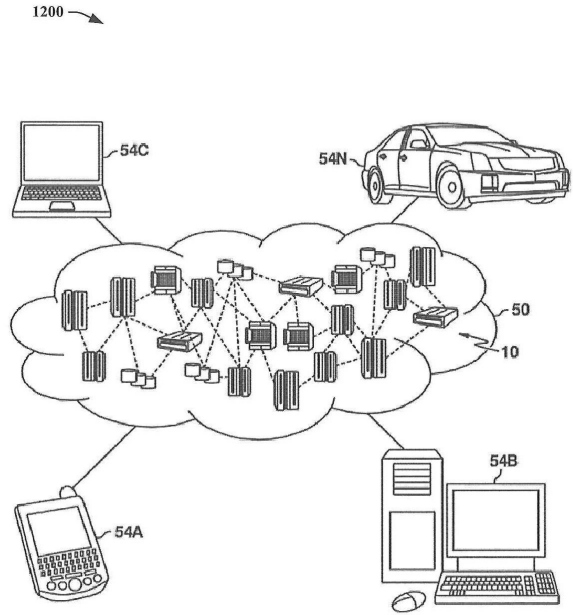


10

【図 11】



【図 12】



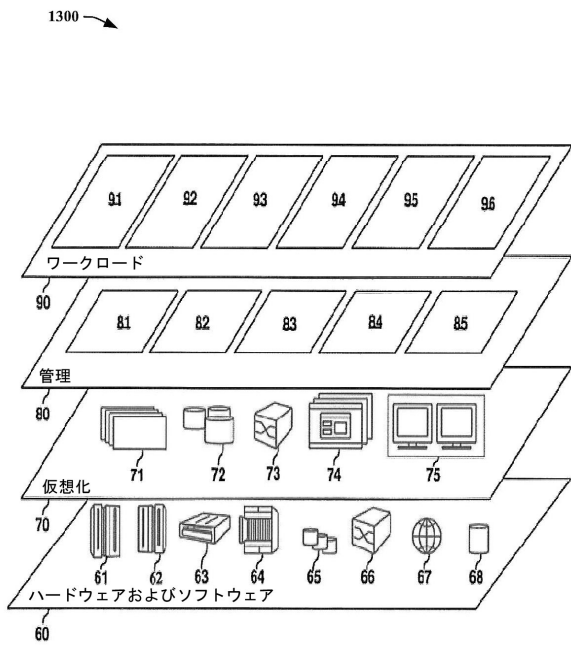
20

30

40

50

【図 13】



10

20

30

40

50

フロントページの続き

- (72)発明者 ブルート、ムハンマド、フェイス
 アメリカ合衆国 1 0 5 9 8 ニューヨーク州ヨークタウン・ハイツ キッチャワン・ロード 1 1 0 1
- (72)発明者 スレーダール、バグラナム
 アメリカ合衆国 1 0 5 9 8 ニューヨーク州ヨークタウン・ハイツ キッチャワン・ロード 1 1 0 1
- (72)発明者 ズン、サイ
 アメリカ合衆国 1 0 5 9 8 ニューヨーク州ヨークタウン・ハイツ キッチャワン・ロード 1 1 0 1
- 審査官 松平 英
- (56)参考文献 米国特許出願公開第 2 0 1 3 / 0 3 4 0 0 7 4 (U S , A 1)
 特開 2 0 0 6 - 3 5 0 5 4 3 (J P , A)
 特開 2 0 1 0 - 0 8 6 3 1 1 (J P , A)
 米国特許第 0 7 7 1 2 1 3 7 (U S , B 1)
 米国特許第 0 7 9 0 0 2 5 9 (U S , B 1)
- (58)調査した分野 (Int.Cl. , D B 名)
 G 0 6 F 1 2 / 1 4
 2 1 / 0 0 - 2 1 / 8 8
 G 0 9 C 1 / 0 0 - 5 / 0 0
 H 0 4 K 1 / 0 0 - 3 / 0 0
 H 0 4 L 9 / 0 0 - 9 / 4 0