

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号

特許第7102499号

(P7102499)

(45)発行日 令和4年7月19日(2022.7.19)

(24)登録日 令和4年7月8日(2022.7.8)

(51)国際特許分類

F I

G 0 6 F 21/62 (2013.01)

G 0 6 F 21/62 3 5 4

G 0 9 C 1/00 (2006.01)

G 0 9 C 1/00 6 6 0 D

請求項の数 14 (全31頁)

(21)出願番号 特願2020-500849(P2020-500849)
(86)(22)出願日 平成30年6月8日(2018.6.8)
(65)公表番号 特表2020-527794(P2020-527794 A)
(43)公表日 令和2年9月10日(2020.9.10)
(86)国際出願番号 PCT/IB2018/054139
(87)国際公開番号 WO2019/012343
(87)国際公開日 平成31年1月17日(2019.1.17)
審査請求日 令和2年11月30日(2020.11.30)
(31)優先権主張番号 15/648,179
(32)優先日 平成29年7月12日(2017.7.12)
(33)優先権主張国・地域又は機関
米国(US)

(73)特許権者 390009531
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
INTERNATIONAL BUSI
NESS MACHINES CORPO
RATION
アメリカ合衆国 1 0 5 0 4 ニューヨー
ク州 アーモンク ニュー オーチャード
ロード
New Orchard Road, A
rmonk, New York 1 0 5
0 4, United States of
America
(74)代理人 100112690
弁理士 太佐 種一

最終頁に続く

(54)【発明の名称】 匿名の暗号化データ

(57)【特許請求の範囲】

【請求項 1】

プロセッサに動作可能に結合されたシステムによって、距離に基づくクラスタ化アルゴリズムである機械学習アルゴリズムと、暗号化データのソースに関する地理的座標を指定する位置識別子とを使用して、前記暗号化データを複数含むデータセットから暗号化データの複数のクラスタを生成することと、

前記システムによって、前記暗号化データの匿名性を促進する定義された基準に基づいて、前記複数のクラスタを変更することとを含んでいる、コンピュータ実装方法。

【請求項 2】

前記定義された基準が、複数のクラスタのクラスタごとのメンバーの最小数を設定する、請求項 1 に記載のコンピュータ実装方法。

【請求項 3】

前記複数のクラスタを変更することが、前記データセットから除去される暗号化データの量を指定する抑制しきい値に基づいて、前記複数のクラスタのあるクラスタを抑制することを含んでいる、請求項 1 に記載のコンピュータ実装方法。

【請求項 4】

前記抑制することが、
前記システムによって、暗号化データに関連付けられた位置インジケータに基づいて、除去される前記クラスタ内の前記暗号化データを識別することと、
前記システムによって、前記識別された暗号化データを前記暗号化されたデータセットか

ら除去して、第2の暗号化されたデータセットを生成することと、前記システムによって、前記機械学習アルゴリズムを使用して、前記第2の暗号化されたデータセットから暗号化データの第2の複数のクラスタを生成することとを含んでいる、請求項3に記載のコンピュータ実装方法。

【請求項5】

前記抑制することが、前記抑制されたクラスタを前記複数のクラスタから除去することを含んでいる、請求項3に記載のコンピュータ実装方法。

【請求項6】

前記複数のクラスタを変更することが、パラメータに基づいて、前記暗号化データを前記複数のクラスタの第1のクラスタから前記複数のクラスタの第2のクラスタに割り当て直すことを含んでいる、請求項1に記載のコンピュータ実装方法。

10

【請求項7】

前記パラメータが、割り当て直されている前記暗号化データに関連付けられた位置インジケータである、請求項6に記載のコンピュータ実装方法。

【請求項8】

前記複数のクラスタを変更することが、パラメータに基づいて、前記第2の暗号化されたデータセットの前記暗号化データを前記複数のクラスタの第1のクラスタから前記複数のクラスタの第2のクラスタに割り当て直すことを含んでいる、請求項4に記載のコンピュータ実装方法。

【請求項9】

20

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、前記メモリに操作可能に結合され、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備えているシステムであって、前記コンピュータ実行可能コンポーネントが、

距離に基づくクラスタ化アルゴリズムである機械学習アルゴリズムと、暗号化データのソースに関する地理的座標を指定する位置識別子とを使用して、前記暗号化データを複数含むデータセットから暗号化データの複数のクラスタを生成するクラスタ化コンポーネントと、

前記暗号化データの匿名性を促進する定義された基準に基づいて、前記複数のクラスタを変更する変更コンポーネントとを備えている、システム。

30

【請求項10】

前記クラスタ化コンポーネントおよび前記変更コンポーネントが、フェデレーテッド・クラウド環境内で動作する、請求項9に記載のシステム。

【請求項11】

前記クラスタ化コンポーネントが、前記複数のクラスタのあるクラスタに関してクラスタの代表をさらに生成する、請求項9に記載のシステム。

【請求項12】

クラスタが前記定義された基準よりも少なく含んでいることに応答して、前記変更コンポーネントが、前記クラスタの抑制および前記クラスタの前記暗号化データの再割り当てから成る群から選択された動作を使用して前記複数のクラスタを変更する、請求項9に記載のシステム。

40

【請求項13】

前記クラスタの前記抑制が、抑制しきい値に基づいて、前記暗号化データの一部を前記複数のクラスタから除去することを含んでいる、請求項12に記載のシステム。

【請求項14】

暗号化されたデータセットを匿名にすることを容易にするコンピュータ・プログラムであって、プロセッサに、

距離に基づくクラスタ化アルゴリズムである機械学習アルゴリズムと、暗号化データのソースに関する地理的座標を指定する位置識別子とを使用して、前記暗号化データを複数含むデータセットから暗号化データの複数のクラスタを生成することと、

50

前記暗号化データの匿名性を促進する定義された基準に基づいて、前記複数のクラスタを変更することを実行させる、コンピュータ・プログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、暗号化データを匿名にすることに関し、より詳細には、クラウド環境を介して暗号化データを匿名にすることに関する。

【発明の概要】

【発明が解決しようとする課題】

【0002】

匿名の暗号化データを実現するためのコンピュータ実装方法、システム、およびコンピュータ・プログラムを提供する。

【課題を解決するための手段】

【0003】

以下に、本発明の1つまたは複数の実施形態の基本的理解を可能にするための概要を示す。この概要は、主要な要素または重要な要素を特定するよう意図されておらず、特定の実施形態の範囲または特許請求の範囲を正確に説明するよう意図されていない。この概要の唯一の目的は、後で提示されるより詳細な説明のための前置きとして、概念を簡略化された形態で提示することである。本明細書に記載された1つまたは複数の実施形態では、1つまたは複数のクラウド環境を介して暗号化データを匿名にすることができるシステム、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、あるいはその組合せが説明される。

【0004】

本発明の一実施形態によれば、コンピュータ実装方法が提供される。このコンピュータ実装方法は、プロセッサに動作可能に結合されたシステムによって、機械学習アルゴリズムを使用して、暗号化されたデータセットから暗号化データの複数のクラスタを生成することを含むことができる。このコンピュータ実装方法は、システムによって、暗号化データの匿名性を促進できる定義された基準に基づいて、複数のクラスタを変更することを含むこともできる。

【0005】

本発明の別の実施形態によれば、システムが提供される。このシステムは、コンピュータ実行可能コンポーネントを格納できるメモリを備えることができる。このシステムは、メモリに操作可能に結合され、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ことができる、プロセッサを備えることもできる。コンピュータ実行可能コンポーネントは、機械学習アルゴリズムを使用して、暗号化されたデータセットから暗号化データの複数のクラスタを生成できる、クラスタ化コンポーネントを含むことができる。さらに、コンピュータ実行可能コンポーネントは、暗号化データの匿名性を促進できる定義された基準に基づいて複数のクラスタを変更できる、変更コンポーネントを含むことができる。

【0006】

本発明の別の実施形態によれば、コンピュータ・プログラム製品が提供される。このコンピュータ・プログラム製品は、暗号化されたデータセットを匿名にすることができる。このコンピュータ・プログラム製品は、プログラム命令が具現化されているコンピュータ可読記憶媒体を備えることができる。それらのプログラム命令は、プロセッサに、機械学習アルゴリズムを使用して、暗号化されたデータセットから暗号化データの複数のクラスタを生成させるために、プロセッサによって実行可能であることができる。また、それらのプログラム命令は、プロセッサに、暗号化データの匿名性を促進できる定義された基準に基づいて、複数のクラスタをさらに変更させることができる。

【図面の簡単な説明】

【0007】

10

20

30

40

50

【図 1】本発明の 1 つまたは複数の実施形態によるクラウド・コンピューティング環境を示す図である。

【図 2】本発明の 1 つまたは複数の実施形態による抽象モデル・レイヤを示す図である。

【図 3】本発明の 1 つまたは複数の実施形態による、信頼されていない環境内で暗号化データを匿名にすることを容易にすることができる、例示的な非限定的システムのブロック図である。

【図 4】本発明の 1 つまたは複数の実施形態による、信頼されていない環境内で暗号化データを匿名にすることを容易にすることができる、例示的なシステムのブロック図である。

【図 5】本発明の 1 つまたは複数の実施形態による、信頼されていない環境内で暗号化データを匿名にすることを容易にすることができる、例示的なシステムの別のブロック図である。

10

【図 6】本発明の 1 つまたは複数の実施形態による、信頼されていない環境内で暗号化データを匿名にすることを容易にすることができる、例示的なシステムの別のブロック図である。

【図 7】本発明の 1 つまたは複数の実施形態による、機械学習アルゴリズムを使用してクラスタ化している暗号化データの図である。

【図 8】本発明の 1 つまたは複数の実施形態による、暗号化データを匿名にすることを容易にするための 1 つまたは複数のセキュリティ要件に従ってクラスタ化している、変更されたデータの図である。

【図 9】本発明の 1 つまたは複数の実施形態による、機械学習アルゴリズムを使用してクラスタ化している暗号化データの別の図である。

20

【図 10】本発明の 1 つまたは複数の実施形態による、暗号化データを匿名にすることを容易にするための 1 つまたは複数のセキュリティ要件に基づいてクラスタ化している、変更されたデータの別の図である。

【図 11】本発明の 1 つまたは複数の実施形態による、信頼されていない環境内で暗号化データを匿名にすることを容易にすることができる、例示的なコンピュータ実装方法のフローチャートである。

【図 12】本発明の 1 つまたは複数の実施形態による、信頼されていない環境内で暗号化データを匿名にすることを容易にすることができる、例示的なコンピュータ実装方法の別のフローチャートである。

30

【図 13】本発明の 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な動作環境のブロック図である。

【発明を実施するための形態】

【0008】

以下の詳細な説明は、例にすぎず、本発明もしくは本出願またはその両方の実施形態、あるいはそのような実施形態の使用を制限するよう意図されていない。さらに、先行する「背景技術」または「発明の概要」のセクション、あるいは「発明を実施するための形態」のセクションで提示された、いずれかの明示されたか、または暗示された情報によって制約されるという意図はない。

【0009】

ここで、図面を参照して本発明の 1 つまたは複数の実施形態が説明され、図面全体を通じて、類似する参照番号が、類似する要素を参照するために使用されている。以下の説明では、説明の目的で、本発明を十分に理解できるように、多数の特定の詳細が示されている。しかし、これらの特定の詳細がなくても、さまざまな事例において、本発明の 1 つまたは複数の実施形態が実践され得るということは明らかである。

40

【0010】

本開示にはクラウド・コンピューティングに関する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理解されるべきである。本発明の実施形態は、現在既知であるか、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。

50

【 0 0 1 1 】

クラウド・コンピューティングは、構成可能な計算リソース（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。

【 0 0 1 2 】

特徴は、次のとおりである。

【 0 0 1 3 】

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、ネットワーク・ストレージなどの計算能力を一方的に、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。

【 0 0 1 4 】

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。

【 0 0 1 5 】

リソース・プール：プロバイダの計算リソースは、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では、場所（例えば、国、州、またはデータセンター）を指定できる場合がある。

【 0 0 1 6 】

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、任意の量をいつでも無制限に購入できるように見える。

【 0 0 1 7 】

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。

【 0 0 1 8 】

サービス・モデルは、次のとおりである。

【 0 0 1 9 】

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の利用である。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を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。

【 0 0 2 0 】

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

10

20

30

40

50

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。

【 0 0 2 1 】

I a a S (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計算リソースのプロビジョニングであり、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、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。

10

【 0 0 2 2 】

デプロイメント・モデルは、次のとおりである。

【 0 0 2 3 】

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、組織のためにのみ運用される。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。

20

【 0 0 2 4 】

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。

【 0 0 2 5 】

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。

30

【 0 0 2 6 】

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。

【 0 0 2 7 】

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含んでいるインフラストラクチャである。

40

【 0 0 2 8 】

ここで図 1 を参照すると、例示的なクラウド・コンピューティング環境 5 0 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 5 0 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、パーソナル・デジタル・アシスタント (P D A : personal digital assistant) または携帯電話 5 4 A 、デスクトップ・コンピュータ 5 4 B 、ラップトップ・コンピュータ 5 4 C 、または自動車コンピュータ・システム 5 4 N 、あるいはその組合せなど) 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 1 0 を含んでいる。ノード 1 0 は、互いに通

50

信することができる。ノード10は、1つまたは複数のネットワーク内で、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合せなどに、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50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SaaS、あるいはその組合せを提供できる。図1に示されたコンピューティング・デバイス54A～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10およびクラウド・コンピューティング環境50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。

10

【0029】

ここで図2を参照すると、クラウド・コンピューティング環境50（図1）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。本明細書に記載された本発明の他の実施形態で採用されている類似する要素の説明の繰り返しは、簡潔にするために省略されている。図2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。本明細書に記載された本発明の他の実施形態で採用されている類似する要素の説明の繰り返しは、簡潔にするために省略されている。

20

【0030】

ハードウェアおよびソフトウェア・レイヤ60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としては、メインフレーム61、RISC（Reduced Instruction Set Computer）アーキテクチャベースのサーバ62、サーバ63、ブレード・サーバ64、ストレージ・デバイス65、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66が挙げられる。本発明の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67およびデータベース・ソフトウェア68を含む。

【0031】

仮想化レイヤ70は、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などの仮想的実体を提供できる抽象レイヤを備える。

30

【0032】

一例を挙げると、管理レイヤ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計算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、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・ライセンスを含んでよい。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83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84は、必要なサービス・レベルを満たすように、クラウドの計算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85は、今後の要求が予想されるクラウドの計算リソースの事前準備および調達を、SLAに従って行う。

40

【0033】

ワークロード・レイヤ90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示している。このレイヤから提供されてよいワークロードおよび機能の例としては、マ

50

ッピングおよびナビゲーション 9 1、ソフトウェア開発およびライフサイクル管理 9 2、仮想クラスルーム教育の配信 9 3、データ分析処理 9 4、トランザクション処理 9 5、およびデータ匿名化 9 6 が挙げられる。本発明のさまざまな実施形態は、図 1 および図 2 を参照して説明されたクラウド・コンピューティング環境を利用して、信頼されていない環境（例えば、パブリック・クラウド環境）で暗号化データを匿名にすることを容易にすることができる。

【0034】

データ共有およびデータの貨幣化を容易にすることに関する現在のビジネス上の必要性をサポートするために、データ保護アルゴリズムがますます重要になってきている。データを匿名にすることは、データを共有する前の重要なステップであり、データを格納して管理するための効率的な解決策として、クラウド・サービスの人気が高まっている。しかし多くの場合、個人情報または極秘データあるいはその両方を平文で格納するために、第三者は信頼されない。したがって、個人情報または極秘データあるいはその両方を読み取ろうとする意図的な試みおよび意図的でない試みから保護するために、データ暗号化が採用された。したがって、信頼されていない環境内では、平文データを格納することを必要とせずに、暗号化データを匿名にすることに対する必要性が存在する。

【0035】

本発明のさまざまな実施形態は、信頼されていない環境内で暗号化データを匿名にすることの効率、効果、および匿名性を（例えば、直接的な人間による誘導なしで）促進する、コンピュータ処理システム、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、あるいはその組合せを対象にすることができる。例えば、本明細書に記載された本発明の 1 つまたは複数の実施形態は、クラスタ化手法を使用して、信頼されていない環境において、暗号化データを匿名にすることができる。本明細書において使用されるとき、「信頼されていない環境」という用語は、その環境に格納されるデータの所有者ではない第三者によって維持され、運用されている環境を指すことができる。信頼されていない環境の例としては、パブリック・クラウド・サービス・プロバイダが挙げられるが、これに限定されない。さらに、本明細書に記載された本発明の 1 つまたは複数の実施形態は、暗号化データの類似するレコードをクラスタ化することができ、1 つまたは複数のセキュリティ要件を満たすように、クラスタを変更することができる。さらに、本明細書に記載された本発明のさまざまな実施形態は、最小限の数のメンバーを含んでいるクラスタを生成して、匿名性の望ましいレベルを得るために、暗号化データのクラスタの抑制または再割り当てあるいはその両方を実行することができる。

【0036】

コンピュータ処理システム、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、あるいはその組合せは、本質的に高度に技術的であり、抽象的ではなく、人間による一連の精神的活動として実行できない、問題（例えば、平文データを暗号化すること、暗号化データを信頼されていない環境に転送すること、および信頼されていない環境内で暗号化データを匿名にすること）を解決するための、ハードウェアまたはソフトウェアあるいはその両方を採用する。例えば、暗号化データを匿名にするために、1 人または複数の人間が暗号化データを効率的に解析して、複数のクラスタを生成することはできない。対照的に、本明細書に記載されたハードウェアまたはソフトウェアあるいはその両方を採用するコンピュータ処理システム、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、あるいはその組合せのさまざまな実施形態は、膨大な量の暗号化データを効率的に解析し、クラスタに基づく匿名性を実行することができる。さらに、本明細書に記載された本発明の実施形態の利点のうちの 1 つは、処理されたデータが匿名であることであるため、1 人または複数の人間を使用してそのような努力を試みようとするこ

とさえ、望ましくない。人間を使用して、本明細書に記載された本発明の実施形態を実行しようとすることは、少なくとも 1 人の人間が、匿名であるよう意図されているデータについて複雑な知識を有することにつながるため、データを匿名にする目的に反することになる。

10

20

30

40

50

【 0 0 3 7 】

本発明の1つまたは複数の実施形態は、任意の可能な統合の技術的詳細レベルで、システム、方法、またはコンピュータ・プログラム製品、あるいはその組合せであってよい。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コンピュータ可読記憶媒体を含んでよい。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格納できる有形のデバイスであることができる。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合せであってよいが、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、ハード・ディスク、ランダム・アクセス・メモリ (R A M : random access memory)、読み取り専用メモリ (R O M : read-only memory)、消去可能プログラマブル読み取り専用メモリ (E P R O M : 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 (S R A M : 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 (C D - R O M : compact disc read-only memory)、デジタル多用途ディスク (D V D : digital versatile disk)、メモリ・スティック、フロッピー・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合せを含む。本明細書において使用されるとき、コンピュータ可読記憶媒体は、それ自体が、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過性の信号であると解釈されるべきではない。

【 0 0 3 8 】

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、あるいはその組合せ) 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され得る。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、あるいはその組合せを備えてよい。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格納するために転送する。

【 0 0 3 9 】

本発明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 (I S A : instruction-set-architecture) 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、集積回路のための構成データ、あるいは、 S m a l l t a l k (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合せで記述されたソース・コードまたはオブジェクト・コードであってよい。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・コンピュータは、ローカル・エリア・ネットワーク (L A N : local area network) または広域ネットワーク (W A N : wide areanet work) 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されてよく

10

20

30

40

50

、または接続は、（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われてよい。本発明の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してよい。

【0040】

本発明の態様は、本明細書において、本発明の実施形態による、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に含まれるブロックの組合せが、コンピュータ可読プログラム命令によって実装され得るということが理解されるであろう。

10

【0041】

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、命令が格納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格納され、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、あるいはその組合せに特定の方式で機能するように指示できるものであってもよい。

20

【0042】

コンピュータ可読プログラム命令は、コンピュータ上、他のプログラム可能な装置上、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るべく、コンピュータ、他のプログラム可能なデータ処理装置、または他のデバイスに読み込まれ、一連の動作可能なステップを、コンピュータ上、他のプログラム可能な装置上、または他のデバイス上で実行させるものであってもよい。

30

【0043】

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、規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、または部分を表してよい。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してよい。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合せは、規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の組合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され得るということにも留意されたい。

40

【0044】

図3は、信頼されていない環境内で暗号化データを匿名にすることを容易にすることができる、例示的なシステム300のブロック図である。本明細書に記載された本発明の他の実施形態で採用されている類似する要素の説明の繰り返しは、簡潔にするために省略されている。本発明のさまざまな実施形態におけるシステム（例えば、システム300など）

50

、装置、またはプロセスの態様は、1つまたは複数のマシン内で具現化された（例えば、1つまたは複数のマシンに関連付けられた1つまたは複数のコンピュータ可読媒体内で具現化された）1つまたは複数の機械実行可能コンポーネントを構成することができる。そ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）によって実行された場合に、マシンに、説明された動作を実行させることができる。

【0045】

図3に示されているように、システム300は、1つまたは複数の第1のサーバ302と、1つまたは複数のネットワーク304と、1つまたは複数の第2のサーバ306と、1つまたは複数のクライアント・デバイス308とを備えることができる。第1のサーバ302は、処理コンポーネント310を備えることができる。処理コンポーネント310は、第1の受信コンポーネント312と、暗号化コンポーネント314と、暗号解読コンポーネント316と、セキュリティ・コンポーネント317とを、さらに備えることができる。また、第1のサーバ302は、少なくとも1つの第1のメモリ318を備えるか、またはその他の方法で少なくとも1つの第1のメモリ318に関連付けられ得る。第1のサーバ302は、処理コンポーネント310および関連するコンポーネント、第1のメモリ318、または第1のプロセッサ322、あるいはその組合せなどの、ただしこれらに限定されない、さまざまなコンポーネントに結合することができる。第1のシステム・バス320をさらに備えることができる。図3では第1のサーバ302が示されているが、他の実施形態では、さまざまな種類の複数のデバイスが、図3に示されている特徴に関連付けられるか、または図3に示されている特徴を備えることができる。さらに、第1のサーバ302は、1つまたは複数のネットワーク304を介して、図1および図2に示されたクラウド環境と通信することができる。本発明のさまざまな実施形態では、「第1のサーバ」または「第2のサーバ」あるいはその両方は、本発明のさまざまな実施形態において、プロセッサ、またはハードウェアもしくはソフトウェアまたはその両方のうちの1つまたは複数、あるいはその組合せから成ることができる。

【0046】

1つまたは複数のネットワーク304は、セルラー・ネットワーク、広域ネットワーク（WAN）（例えば、インターネット）またはローカル・エリア・ネットワーク（LAN）を含むが、これらに限定されない、有線ネットワークおよび無線ネットワークを含むことができる。例えば、第1のサーバ302は、例えばセルラー方式、WAN、ワイヤレス・フィディリティ（Wi-Fi: wireless fidelity）、Wi-Max、WLAN、またはBluetooth技術、あるいはその組合せなどを含むが、これらに限定されない、実質的に任意の望ましい有線技術または無線技術を使用して、第2のサーバ306と（およびその逆方向に）通信することができる。さらに、示されている本発明の実施形態では、処理コンポーネント310を1つまたは複数の第1のサーバ302上に設けることができるが、システム300のアーキテクチャがそのように制限されないということが理解されるべきである。例えば、処理コンポーネント310または処理コンポーネント310の1つまたは複数のコンポーネントは、別のサーバ・デバイス、クライアント・デバイスなどの別のコンピュータ・デバイスに存在することができる。

【0047】

第2のサーバ306は、分類コンポーネント324を備えることができる。分類コンポーネント324は、第2の受信コンポーネント326と、クラスタ化コンポーネント328と、変更コンポーネント330とを、さらに備えることができる。また、第2のサーバ306は、少なくとも1つの第2のメモリ332を備えるか、またはその他の方法で少なくとも1つの第2のメモリ332に関連付けられ得る。第2のサーバ306は、分類コンポーネント324および関連するコンポーネント、第2のメモリ332、または第2のプロセッサ336、あるいはその組合せなどの、ただしこれらに限定されない、さまざまなコンポーネントに結合することができる。第2のシステム・バス334をさらに備えることができる。図3では第2のサーバ306が示されているが、本発明の他の実施形態では、

さまざまな種類の複数のデバイスが、図 3 に示されている特徴に関連付けられるか、または図 3 に示されている特徴を備えることができる。さらに、第 2 のサーバ 306 は、1 つまたは複数のネットワーク 304 を介して、図 1 および図 2 に示されたクラウド環境と通信することができる。

【0048】

1 つまたは複数のクライアント・デバイス 308 は、第 1 のサーバ 302 を管理する 1 つまたは複数の実体によって所有されているデータを解析すること、格納すること、またはその他の方法で使用する、あるいはその組合せをしたいと考えている実体によって操作される、コンピュータまたはコンピュータ制御デバイスあるいはその両方であることができる。1 つまたは複数のクライアント・デバイス 308 は、1 つまたは複数のネットワーク 304 を介して（例えば、インターネット、ローカル・ネットワーク、または直接的電気接続、あるいはその組合せを介して）、第 1 のサーバ 302 および第 2 のサーバ 306 に、操作可能に結合され得る。さらに、1 つまたは複数のクライアント・デバイス 308 は、第 1 の手段を使用して第 1 のサーバ 302 に操作可能に結合することができ、第 2 の手段を使用して第 2 のサーバ 306 に操作可能に結合することができ、第 1 および第 2 の手段は、1 つまたは複数のネットワーク 304 を介して利用可能であり得る。例えば、1 つまたは複数のクライアント・デバイス 308 は、インターネットを介して第 2 のサーバ 306 に操作可能に結合されながら、第 1 のサーバ 302 に直接的に電気接続され得る。

10

【0049】

第 1 の受信コンポーネント 312 は、第 1 のシステム・バス 320 を介して、暗号化コンポーネント 314、暗号解読コンポーネント 316、第 1 のメモリ 318、または第 1 のプロセッサ 322、あるいはその組合せに、操作可能に結合され得る。さらに、本発明の 1 つまたは複数の実施形態では、第 1 の受信コンポーネント 312 は、1 つまたは複数のネットワーク 304（例えば、ローカル・エリア・ネットワーク）を介して、暗号化コンポーネント 314、暗号解読コンポーネント 316、第 1 のメモリ 318、または第 1 のプロセッサ 322、あるいはその組合せに、操作可能に結合され得る。同様に、第 2 の受信コンポーネント 326 は、第 2 のシステム・バス 334 を介して、クラスタ化コンポーネント 328、変更コンポーネント 330、第 2 のメモリ 332、または第 2 のプロセッサ 336、あるいはその組合せに、操作可能に結合され得る。さらに、本発明の 1 つまたは複数の実施形態では、第 2 の受信コンポーネント 326 は、1 つまたは複数のネットワーク 304（例えば、ローカル・エリア・ネットワーク）を介して、クラスタ化コンポーネント 328、変更コンポーネント 330、第 2 のメモリ 332、または第 2 のプロセッサ 336、あるいはその組合せに、操作可能に結合され得る。

20

30

【0050】

セキュリティ・コンポーネント 317 は、1 つまたは複数のセキュリティ要件を、第 1 のサーバ 302 のオペレータから受信することができる。1 つまたは複数のセキュリティ要件によって規定されたパラメータは、第 2 のサーバ 306 によって出力される匿名クラスタの望ましい数またはクラスタごとのメンバーの望ましい数（例えば、クラスタごとに少なくとも k 個のメンバー（ k は 0 より大きい整数））あるいはその両方を含むことができるが、これらに限定されない。

40

【0051】

クラスタ化コンポーネント 328 は、機械学習アルゴリズムを使用して、暗号化データをクラスタ化することができる。機械学習アルゴリズムは、 k 平均クラスタ化アルゴリズムなどの、距離に基づくアルゴリズムであることができる。機械学習アルゴリズム（例えば、 k 平均クラスタ化アルゴリズム）は、暗号化データを、位置識別子（例えば、全地球測位座標）などの 1 つまたは複数のパラメータに基づいて複数のクラスタに分割することができる。しかし、クラスタごとのメンバーの数は、データに依存し、機械学習アルゴリズムは、クラスタごとの最小の数のメンバーを生成することをサポートしない。言い換えると、クラスタ化コンポーネント 328 は、機械学習アルゴリズムを使用して、1 つまたは複数のパラメータに基づいて、各クラスタのメンバーが類似している複数のクラスタを生

50

成することができるが、各クラスタのメンバーの数は保証されないことがある。

【0052】

本発明のさまざまな実施形態では、変更コンポーネント330は、定義された基準（例えば、セキュリティ要件のうちの1つまたは複数）に基づいて、暗号化データを匿名にすることを容易にするように、複数のクラスタを変更できる。本発明の1つまたは複数の実施形態では、変更コンポーネント330は、 k -匿名性を実現するように、複数のクラスタを変更することができ、 k は各クラスタを構成するメンバーの数であり、0より大きい整数である。例えば、変更コンポーネント330は、2-匿名性を実現するように複数のクラスタを変更することができ、その場合、1つまたは複数のセキュリティ要件が、各クラスタが少なくとも2つのメンバーを含むということを規定する。

10

【0053】

例えば、クラスタ化コンポーネント328は、機械学習アルゴリズムを使用して、暗号化データの10個のレコードから、クラスA、B、およびCを生成できる。この例では、クラスAは4つのメンバーを含むことができ、クラスBは5つのメンバーを含むことができ、クラスCは1つのメンバーを含むことができる。さらに、1つまたは複数のセキュリティ要件は、各クラスタが少なくとも2つのメンバーを含むことが望ましいということを規定することができる。変更コンポーネント330は、2-匿名性を実現するために、変更されたクラスタのセットが少なくとも2つのメンバーをそれぞれ含むように、クラスA、B、またはC、あるいはその組合せを変更することができる。

【0054】

本発明のさまざまな実施形態では、変更コンポーネント330は、抑制動作または再割り当て動作あるいはその両方を実行することによって、複数のクラスタを変更できる。変更コンポーネント330は、抑制動作を実行しながら、複数のクラスタから外れ値を取り除くために、定義された量の暗号化データまたはクラスタあるいはその両方を除去することができる。変更コンポーネント330は、再割り当て動作を実行しながら、1つもしくは複数の暗号化データ・レコード（encrypted data records）または1つもしくは複数のクラスタあるいはその両方を別のクラスタに割り当て直すことができる。

20

【0055】

本発明の1つまたは複数の実施形態では、変更コンポーネント330は、抑制しきい値に基づいて、定義された量の暗号化データを抑制できる。抑制しきい値は、破棄できる暗号化データの量（例えば、レコードの割合）を定義する入力パラメータであることができる。1つまたは複数のセキュリティ要件を満たすことができない（例えば、最小の数のメンバーを含むことができない）クラスタのメンバーごとに、変更コンポーネント330は、各メンバーと、クラスタの他のメンバーの重心との間の距離を計算し、それらの距離の最小値のみを保存することができる。次に変更コンポーネント330は、保存された最小距離を降順に並べ替え、抑制しきい値の量を遠い外れ値として識別することができる。このようにして、クラスタの他のメンバーからの最大の最小距離を有するメンバーが、遠い外れ値として識別される。さらに、変更コンポーネント330は、遠い外れ値を除去するか、または遠い外れ値の除去を指示するか、あるいはその両方を実行することができる。1つまたは複数の実施形態では、変更コンポーネント330は、1つまたは複数のクラスタ全体を破棄するための抑制を利用することができる。本発明の1つまたは複数の実施形態では、変更コンポーネント330は、抑制を利用して新しい暗号化データのセットを生成することができ、この暗号化データのセットから、クラスタ化コンポーネント328が新しい複数のクラスタを生成できる。

30

【0056】

本発明の1つまたは複数の実施形態では、変更コンポーネント330は、あるクラスタからの1つまたは複数の暗号化データ・レコードを別のクラスタに割り当て直すか、または既存のクラスタをマージするか、あるいはその両方を実行できる。例えば、クラスタがセキュリティ要件を満たすことができない場合（例えば、最小の数のメンバーを含むことができない場合）、変更コンポーネント330は、過剰なメンバーを含むクラスタ（例えば

40

50

、最小の数のメンバーより多くのメンバーを含むクラスタ)の最も近いメンバーを、不適合なクラスタに割り当て直すことができる。別の例では、クラスタがセキュリティ要件を満たすことができない場合(例えば、最小の数のメンバーを含むことができない場合)、変更コンポーネント330は、不適合なクラスタのメンバーを、そのメンバーに対して最も近いクラスタに割り当て直すことができる。別の例では、クラスタがセキュリティ要件を満たすことができない場合(例えば、最小の数のメンバーを含むことができない場合)、変更コンポーネント330は、不適合なクラスタを、最も近いクラスタにマージすることができる。

【0057】

本発明のさまざまな実施形態では、再割り当て動作を実行するときに、変更コンポーネント330は、セキュリティ要件を満たすことができない(例えば、最小の数のメンバーを含むことができない)クラスタを、(例えば、最も少ないメンバーを含むクラスタから最も多いメンバーを含むクラスタまで)サイズで並べ替えることができる。変更コンポーネント330は、最小のクラスタ(例えば、最も少ないメンバーを含む不適合なクラスタ)から開始して、最小のクラスタの各メンバーを最も近いクラスタに割り当て直すことができる。最小のクラスタのメンバーが割り当て直された後に、変更コンポーネント330は、前述のクラスタを複数のクラスタから除去し、不適合なクラスタに関して、複数のクラスタを再解析することができる。さらに、変更コンポーネント330は、残りのすべてのクラスタが1つまたは複数のセキュリティ要件に従うまで、再割り当てプロセスを繰り返すことができる。

【0058】

図4は、第1のサーバ302と第2のサーバ306の間で実行できる例示的なプロセスのブロック図である。本明細書に記載された本発明の他の実施形態で採用されている類似する要素の説明の繰り返しは、簡潔にするために省略されている。第1のメモリ318は、暗号化されていないデータの1つまたは複数のレコードを含むことができる1つまたは複数の平文データベース402を格納することができる。第1のメモリ318は、第1のシステム・バス320を介して、処理コンポーネント310に操作可能に結合され得る。暗号化コンポーネント314は、1つまたは複数の平文データベース402を(例えば、第1のメモリ318から)取り出し、平文データベース402に対して1つまたは複数の暗号化方式404を適用して、1つまたは複数の暗号化されたデータセット406を生成することができる。暗号化方式404は、暗号化アルゴリズムまたは暗号鍵あるいはその両方を使用して、平文データベース402を暗号化することができる。例示的な暗号化方式404は、AES(advanced encryption standard)、BGN(Boneh, Goh, and Nissim)の暗号システム、トリプルDES(triple data encryption standard)、RSA(Rivest, Shamir, and Adelman)暗号化アルゴリズム、Blowfish暗号化、またはTwofish暗号化、あるいはその組合せを含むことができるが、これらに限定されない。本発明の1つまたは複数の実施形態では、暗号化コンポーネント314は、平文データベース402に対して複数の異なる暗号化方式404を適用して、同じ平文データベース402に基づいて複数の暗号化されたデータセット406を生成することができる。例えば、暗号化コンポーネント314は、平文データベース402に対してAES暗号化およびBGN暗号化を適用して、2つの暗号化されたデータセット406を作成することができる。

【0059】

第1のサーバ302は(例えば、暗号化コンポーネント314を介して)、1つまたは複数の暗号化されたデータセット406を、1つまたは複数のネットワーク304を介して第2のサーバ306に送信できる。さらに、第1のサーバ302は(例えば、セキュリティ・コンポーネント317を介して)、1つまたは複数のセキュリティ要件を第2のサーバ306に送信できる。セキュリティ要件は、1つまたは複数の暗号化されたデータベースを匿名にするときに第2のサーバ306が満たす必要がある1つまたは複数のパラメータを含むことができる。例示的なセキュリティ要件は、1つまたは複数の生成されたクラ

10

20

30

40

50

スタ内で許容されるメンバーの最小数を示す数を含むことができるが、これに限定されない。

【 0 0 6 0 】

第2のサーバ306は、信頼されていない環境であることができる。さらに、第2のサーバ306は、フェデレーテッド・クラウド環境 (federated cloud environment) を含むことができる。例えば、図4に示されているように、第2のサーバ306は、第1のクラウド408および第2のクラウド410を含むことができる。本発明のさまざまな実施形態では、第2のサーバ306は、3つ以上のクラウド (例えば、3つ、4つ、5つ以上のクラウド) を含むことができる。第2の受信コンポーネント326は、第1のクラウド408上に存在することができ、1つまたは複数の暗号化されたデータセット406および1つまたは複数のセキュリティ要件を受信することができる。

10

【 0 0 6 1 】

クラスタ化コンポーネント328は、第1のクラウド408上または第2のクラウド418上に存在することができる。変更コンポーネント316も、第1のクラウド408上または第2のクラウド410上に存在することができる。第1のクラウド408および第2のクラウド410は、クラスタ化通信412を容易にするために、1つまたは複数のネットワーク304を介して操作可能に結合され得る。第1のクラウド408と第2のクラウド410の間のクラスタ化通信412は、暗号化されたデータセット406を匿名にすることを容易にすることができる。本発明のさまざまな実施形態では、第2のサーバ306 (例えば、信頼されていないフェデレーテッド・クラウド環境) は、1つまたは複数のセキュリティ要件に従って、暗号化されたデータセット406から匿名の暗号化されたデータセット414を生成できる。このようにして、第2のサーバ306は、データの影響を受ける実体が識別され得ないということを保証しながら、暗号化されたデータセット406の実際的な有用性 (例えば、匿名の暗号化データから引き出された任意の洞察が、匿名でない暗号化データから引き出された洞察に類似することができること) を維持することができる。

20

【 0 0 6 2 】

第2のサーバ306は、1つまたは複数の匿名の暗号化されたデータセット414を、1つまたは複数のネットワーク304を介して第1のサーバ302に送信できる。第1の受信コンポーネント312は、匿名の暗号化データを受信し、匿名の暗号化データを暗号解読コンポーネント316に送信することができる。暗号解読コンポーネント316は、暗号解読方式416を使用して匿名の暗号化されたデータセット414を暗号解読し、匿名の平文データベース418を生成することができる。

30

【 0 0 6 3 】

図5は、システム300によって実行できる通信およびプロセスの例のブロック図である。本明細書に記載された本発明の他の実施形態で採用されている類似する要素の説明の繰り返しは、簡潔にするために省略されている。502で、第1のサーバ302が、1つもしくは複数の暗号化されたデータセット406または1つもしくは複数のセキュリティ要件あるいはその両方を、第2のサーバ306の第1のクラウド408に送信することができる。例えば、第1のサーバ302は、AESによって暗号化されたデータセット406およびBGNによって暗号化されたデータセット406を、第1のクラウド408に送信することができる。また、AESによって暗号化されたデータセット406およびBGNによって暗号化されたデータセット406は、同じ平文データベース402に基づくことができる。本発明のさまざまな実施形態では、第1のサーバ302によって (例えば、セキュリティ・コンポーネント317を介して) 第1のクラウド408に送信される1つまたは複数のセキュリティ要件は、クラスタ化コンポーネント328によって生成され、変更コンポーネント316によって変更される、クラスタごとの最小の数のメンバーなどの、1つまたは複数の暗号化されたデータセット406の匿名性を促進する定義された基準を含むことができる。第2のメモリ332は、第1のクラウド408内に存在することができ、1つまたは複数の暗号化されたデータセット406および1つまたは複数のセキュ

40

50

リティ要件を格納することができる。

【 0 0 6 4 】

5 0 4 で、第 1 のサーバ 3 0 2 が、1 つまたは複数のネットワーク 3 0 4 を介して、暗号化されたデータセット 4 0 6 のうちの 1 つまたは複数に関する秘密暗号鍵を、第 2 のサーバ 3 0 6 の第 2 のクラウド 4 1 0 に送信することができる。例えば、第 1 のサーバ 3 0 2 は、A E S によって暗号化されたデータセット 4 0 6 および B G N によって暗号化されたデータセット 4 0 6 を第 1 のクラウド 4 0 8 に送信することができ、B G N によって暗号化されたデータセット 4 0 6 に関する B G N の秘密鍵を、第 2 のクラウド 4 1 0 に送信することもできる。

【 0 0 6 5 】

5 0 6 で、第 1 のクラウド 4 0 8 が（例えば、クラスタ化コンポーネント 3 2 8 を介して）、複数のクラスタの最初の中心として機能するための複数の暗号化データ・レコードを、暗号化されたデータセット 4 0 6 からランダムに選択することができる。最初の中心の数は、1 つまたは複数のセキュリティ要件によって指定され得る。本発明のさまざまな実施形態では、暗号化データ・レコードのパラメータに基づいて、1 つまたは複数の暗号化データ・レコードが、複数のクラスタの最初の中心として選択され得る。例えば、暗号化データ・レコードに関連付けられた 1 つまたは複数の位置識別子に基づいて、1 つまたは複数の暗号化データ・レコードを選択することができ、これらの位置識別子は、対象の暗号化データ・レコードのソースに関する 1 つまたは複数の地理的座標を指定できる。

【 0 0 6 6 】

5 1 0 で、第 1 のクラウド 4 0 8 が（例えば、クラスタ化コンポーネント 3 2 8 を介して）、暗号化されたクラスタの合計および数を第 2 のクラウド 4 1 0（例えば、変更コンポーネント 3 3 0）に送信できる。さまざまな実施形態では、第 1 のクラウド 4 0 8（例えば、クラスタ化コンポーネント 3 2 8）が、1 つまたは複数の暗号化されたデータセット 4 0 6 内の暗号化データ・レコードに関連付けられた位置識別子に基づいて、クラスタを生成できる。例えば、クラスタ化コンポーネント 3 2 8 は、各暗号化データ・レコードとランダムに選択された最初のクラスタの中心との間の距離を決定できる。第 1 のクラウド 4 0 8 は、第 2 のクラウド 4 1 0 に、対象の暗号化されたデータセット 4 0 6 内の暗号化データ・レコードの総数、決定された距離（例えば、クラスタ化コンポーネント 3 2 8 によって決定される）、望ましいクラスタの数（例えば、1 つまたは複数のセキュリティ要件によって指定される）、最初のクラスタの中心（例えば、クラスタ化コンポーネント 3 2 8 によって選択される）、または望ましいクラスタのメンバーの数（例えば、1 つまたは複数のセキュリティ要件によって指定される）、あるいはその組合せを送信できる。

【 0 0 6 7 】

5 1 2 で、第 2 のクラウド 4 1 0 は（例えば、変更コンポーネント 3 3 0 を介して）、第 1 のクラウド 4 0 8 から受信された入力に基づいて、対象の暗号化されたデータセット 4 0 6 の暗号化データ・レコードをクラスタ化するための新しい手段を計算できる。本発明の 1 つまたは複数の実施形態では、第 2 のクラウド 4 1 0 が（例えば、変更コンポーネント 3 3 0 を介して）、各クラスタの数によってクラスタの合計を分割することによってクラスタ化するための新しい手段を決定することができる。

【 0 0 6 8 】

5 1 4 で、第 2 のクラウド 4 1 0 が（例えば、変更コンポーネント 3 3 0 を介して）、計算された新しいクラスタ化の手段を、第 1 のクラウド 4 0 8 のクラスタ化コンポーネント 3 2 8 に返すことができ、そのときクラスタ化コンポーネント 3 2 8 は、新しいクラスタ化の手段に基づいて、生成された 1 つまたは複数のクラスタを調整できる。第 1 のクラウド 4 0 8 と第 2 のクラウド 4 1 0 の間（例えば、5 0 8、5 1 0、および 5 1 4 で）の通信は、クラスタ化通信 4 1 2 を含むことができる。さまざまな実施形態では、第 2 のサーバ 3 0 6 は、少なくとも 1 つまたは複数のセキュリティ要件に基づいて望ましい収束を生成するために、クラスタ化通信 4 1 2 を複数回繰り返すことができる。このようにして、第 1 のクラウド 4 0 8 は、望ましいパラメータに基づいて、最初のクラスタの中心に対す

10

20

30

40

50

る1つまたは複数の暗号化データ・レコードの類似性などの、暗号化されたデータセット406に関する最小限の情報量を公開しながら、第2のクラウド410を利用して、1つまたは複数の暗号化されたデータセット406の暗号化データ・レコードを分割することができる。

【0069】

図6は、クライアント・デバイス308の照会に関してシステム300によって実行できる通信およびプロセスの別の例のブロック図である。本明細書に記載された本発明の他の実施形態で採用されている類似する要素の説明の繰り返しは、簡潔にするために省略されている。602で、第1のサーバ302が（例えば、暗号化コンポーネント314および1つまたは複数のネットワーク304を介して）、暗号化されたデータセット406のうちの1つまたは複数に関する公開暗号鍵を、クライアント・デバイス308のうちの1つまたは複数に送信することができる。例えば、第1のサーバ302は、AESによって暗号化されたデータセット406およびBGNによって暗号化されたデータセット406を第1のクラウド408に送信することができ、BGNによって暗号化されたデータセット406に関するBGNの公開鍵を、1つまたは複数のクライアント・デバイス308に送信することもできる。604で、クライアント・デバイス308のうちの1つまたは複数が、公開暗号鍵を使用して暗号化された照会を（例えば、1つまたは複数のネットワーク304を介して）第1のクラウド408に送信できる。

【0070】

606で、第1のクラウド408が（例えば、クラスタ化コンポーネント328を介して）、1つまたは複数の暗号化データ・レコードと暗号化された照会との距離（例えば、ユークリッド距離の二乗）を計算できる。608で、第1のクラウド408が（例えば、クラスタ化コンポーネント328を介して）、1つまたは複数の識別子（例えば、匿名の識別子）と共に、暗号化された距離を第2のクラウド410に送信できる。これらの識別子は、距離に関連付けられた各暗号化データ・レコードを考慮することができる。これらの識別子の例としては、暗号化されたデータセット406内の暗号化データ・レコードの位置を示す行識別子（例えば、匿名の行識別子）が挙げられるが、これに限定されない。

【0071】

第1のクラウド408が同じ平文データベース402に関する複数の暗号化されたデータセット406を受信する、本発明のさまざまな実施形態では、第1のクラウド408は、暗号化されたデータセット406のうちの1つの暗号化された距離のみを送信し、暗号化されたデータセット406が、504で第2のクラウド410に送信された秘密暗号鍵に関連する暗号化方式を含んでいるのが好ましい。例えば、第1のクラウド408がAESによって暗号化されたデータセット406およびBGNによって暗号化されたデータセット406を受信し、第2のクラウド410がBGNによって暗号化された秘密鍵を受信する場合、第1のクラウド408は、BGNによって暗号化された距離のみを第2のクラウド410に送信できる。このようにして、第2のクラウド410は、暗号化された秘密鍵を利用して、計算された暗号化済みの距離を暗号解読することができる。

【0072】

610で、第2のクラウド410が（例えば、変更コンポーネント330を介して）、1つまたは複数の距離（例えば、ユークリッド距離の二乗）を暗号解読し、少なくとも既定の値の距離に関連付けられた識別子を見つけることができる。例えば、第2のクラウド410は（例えば、変更コンポーネント330を介して）、暗号化された照会からの最小の計算された距離を含む距離を識別することができる。さらに、第2のクラウド410は（例えば、変更コンポーネント330を介して）、1つまたは複数のセキュリティ要件に基づいて識別された距離の最小数を識別することができる。

【0073】

本発明の1つまたは複数の実施形態では、第2のクラウド410が（例えば、変更コンポーネント330を介して）、複数のセキュリティ要件に基づいて識別子を選択できる。例えば、複数のセキュリティ要件は、1つまたは複数の暗号化されたデータセット406を

10

20

30

40

50

分割するためのクラスタの最小数およびクラスタごとのメンバーの最小数を規定できる。

【 0 0 7 4 】

6 1 2で、第2のクラウド4 1 0が（例えば、変更コンポーネント3 3 0を介して）、選択された識別子を第1のクラウド4 0 8に送信できる。選択された識別子に基づいて、第1のクラウド4 0 8は（例えば、クラスタ化コンポーネント3 2 8を介して）、暗号化されたデータセット4 0 6のうちの1つまたは複数から、1つまたは複数の暗号化データ・レコードを識別できる。さらに、第1のクラウド4 0 8は（例えば、クラスタ化コンポーネント3 2 8を介して）、1つまたは複数の識別子に関連付けられたクラスタごとにクラスタの代表を生成し、匿名の暗号化されたデータセット4 1 4を生成できる。このようにして、第1のクラウド4 0 8は、暗号化されたデータセット4 0 6を暗号解読せずに、暗号化データをクラスタ化することができ、第2のクラウドは、暗号化されたデータセット4 0 6について、計算された距離を除いて知ることなく、複数のクラスタを変更できる。

10

【 0 0 7 5 】

6 1 4で、第1のクラウド4 0 8が（例えば、クラスタ化コンポーネント3 2 8を介して）、匿名の暗号化されたデータセット4 1 4を第1のサーバ3 0 2に送信できる。第1のサーバ3 0 2は、匿名の暗号化されたデータセット4 1 4を（例えば、第1の受信コンポーネント3 1 2を介して）受信し、暗号解読方式4 1 6を使用して（例えば、暗号解読コンポーネント3 1 6を介して）、匿名の暗号化されたデータセット4 1 4を暗号解読し、匿名の平文データベース4 1 8を生成することができる。6 1 6で、第1のサーバ3 0 2が、匿名の平文データベース4 1 8を、6 0 4で暗号化された照会を送信した1つまたは複数のクライアント・デバイス3 0 8に送信できる。

20

【 0 0 7 6 】

図7、図8、図9、および図10は、システム3 0 0によって実行され得るクラスタ変更のさまざまな図である。本明細書に記載された本発明の他の実施形態で採用されている類似する要素の説明の繰り返しは、簡潔にするために省略されている。図7は、15個の暗号化データ・レコードを円形として表すことができる図7 0 0であり、これらの暗号化データ・レコードは、点々のある円形で示された第1のクラスタ7 0 2、斜めの縞模様のある円形で示された第2のクラスタ7 0 4、および空の円形で示された第3のクラスタ7 0 6という、3つのクラスタに分割され得る。図7 0 0は、変更なしでクラスタ化コンポーネント3 2 8によって生成され得る3つの例示的なクラスタを示している。

30

【 0 0 7 7 】

図8は、同じ15個の暗号化データ・レコードの別の図7 0 8であるが、第1のクラスタ7 0 2および第3のクラスタ7 0 6が、1つまたは複数のセキュリティ要件に基づいて（例えば、変更コンポーネント3 3 0を介して）変更されている。図7 0 8に示されている変更に関しては、セキュリティ要件が、各クラスタが少なくとも3つのメンバーを含むということを規定できる。図7に示されているように、第3のクラスタ7 0 6は、3つのメンバーというセキュリティ要件より少ない2つのメンバーのみで構成されている。セキュリティ要件を満たすために、変更コンポーネント3 3 0は、第3のクラスタ7 0 6にすでに含まれている2つの暗号化データ・レコードが第1のクラスタ7 0 2に割り当て直されるように、第1のクラスタ7 0 2および第3のクラスタ7 0 6を変更できる。このようにして、変更コンポーネント3 3 0は、1つまたは複数のセキュリティ要件に基づいて、1つもしくは複数の暗号化データ・レコードまたは1つもしくは複数のクラスタ全体あるいはその両方を、異なるクラスタに割り当て直すことができる。

40

【 0 0 7 8 】

図9は、第1のクラスタ7 0 2、第2のクラスタ7 0 4、第3のクラスタ7 0 6、および水平の縞模様のある円形で示された第4のクラスタ7 1 2に分割された16個の暗号化データ・レコードの別の図7 1 0である。図7 1 0は、変更なしでクラスタ化コンポーネント3 2 8によって生成され得る4つの例示的なクラスタを示している。

【 0 0 7 9 】

図10は、同じ16個の暗号化データ・レコードの別の図7 1 4であるが、第3のクラスタ

50

タ 7 0 6 および第 4 のクラスタ 7 1 2 が、1 つまたは複数のセキュリティ要件に基づいて（例えば、変更コンポーネント 3 3 0 を介して）変更されている。図 7 1 4 に示されている変更に関しては、セキュリティ要件が、各クラスタが少なくとも 3 つのメンバーを含むということを規定できる。図 9 に示されているように、（2 つのメンバーを含む）第 3 のクラスタ 7 0 6 および（1 つのメンバーを含む）第 4 のクラスタ 7 1 2 は、セキュリティ要件によって規定された 3 つのメンバーより少ないメンバーをそれぞれ含んでいる。変更コンポーネント 3 3 0 は、各クラスタ内のメンバーの数に基づいてクラスタを順序付け、最小の数のメンバーを含むクラスタ（例えば、第 4 のクラスタ 7 1 2）から開始する順序で、クラスタを変更できる。図 1 0 に示されているように、変更コンポーネント 3 3 0 は、1 つまたは複数のセキュリティ要件（例えば、少なくとも 3 つという最小数のメンバー）を満たすために、あるクラスタ（例えば、第 4 のクラスタ 7 1 2）の暗号化データ・レコードを別のクラスタ（例えば、第 3 のクラスタ 7 0 6）に割り当て直すことができる。このようにして、クラスタ化コンポーネント 3 2 8 が、1 つまたは複数のセキュリティ要件を満たすことができない複数のクラスタを生成する場合に、変更コンポーネント 3 3 0 は、1 つまたは複数のセキュリティ要件を満たすクラスタを形成するために、複数の不適合なクラスタと一緒にマージすることができる。

10

【0080】

図 1 1 は、信頼されていない環境内で暗号化データを匿名にすることを容易にすることができる、コンピュータ実装方法 8 0 0 のフローチャートである。8 0 2 で、方法 8 0 0 は、プロセッサ（例えば、第 1 のプロセッサ 3 2 2）に動作可能に結合されたシステム 3 0 0 によって、機械学習アルゴリズムを使用して（例えば、クラスタ化コンポーネント 3 2 8 を介して）、暗号化されたデータセット 4 0 6 から暗号化データの複数のクラスタを生成することを含むことができる。8 0 4 で、方法 8 0 0 は、システム 3 0 0 によって、暗号化データの匿名性を促進できる定義された基準に基づいて（例えば、変更コンポーネント 3 3 0 を介して）、複数のクラスタを変更することを含むこともできる。

20

【0081】

図 1 2 は、信頼されていない環境内で暗号化データを匿名にすることを容易にすることができる、コンピュータ実装方法 9 0 0 のフローチャートである。9 0 2 で、方法 9 0 0 は、プロセッサ（例えば、第 1 のプロセッサ 3 2 2）に動作可能に結合されたシステム 3 0 0 によって、機械学習アルゴリズムを使用して（例えば、クラスタ化コンポーネント 3 2 8 を介して）、暗号化されたデータセット 4 0 6 から暗号化データの複数のクラスタを生成することを含むことができ、この機械学習アルゴリズムは、距離に基づくアルゴリズムであることができる。また、複数のクラスタを生成することは、暗号化データに関連付けられた 1 つまたは複数の位置識別子に基づくことができる。

30

【0082】

9 0 4 で、方法 9 0 0 は、システム 3 0 0 によって、暗号化データの匿名性を促進できる定義された基準に基づいて（例えば、変更コンポーネント 3 3 0 を介して）、複数のクラスタを変更することを含むこともできる。例えば、定義された基準は、複数のクラスタのクラスタごとのメンバーの最小数を設定できる。9 0 6 で、方法 9 0 0 は（例えば、クラスタ化コンポーネント 3 2 8 を介して）、複数のクラスタのクラスタごとにクラスタの代表を生成することを、さらに含むことができる。クラスタの代表は、複数のクラスタの変更の前または後に生成され得る。

40

【0083】

本発明のさまざまな実施形態では、複数のクラスタを変更することが、暗号化されたデータセット 4 0 6 から除去される暗号化データの量を指定できる抑制しきい値に基づいて、複数のクラスタのあるクラスタを抑制することを含むことができる。また、クラスタを抑制することは、システム 3 0 0 によって（例えば、変更コンポーネント 3 3 0 を介して）、暗号化データに関連付けられた位置識別子に基づいて、除去されるクラスタ内の暗号化データを識別することと、システム 3 0 0 によって（例えば、変更コンポーネント 3 3 0 を介して）、識別された暗号化データを暗号化されたデータセット 4 0 6 から除去して、

50

第2の暗号化されたデータセットを生成することと、システム300によって（例えば、クラスタ化コンポーネント328を介して）、機械学習アルゴリズムを使用して、第2の暗号化されたデータセットから暗号化データの第2の複数のクラスタを生成することを含むことができる。

【0084】

本発明の1つまたは複数の実施形態では、複数のクラスタを変更することが、パラメータ（例えば、位置識別子）に基づいて、暗号化データを複数のクラスタのあるクラスタ（例えば、第3のクラスタ706）から複数のクラスタの別のクラスタ（例えば、第1のクラスタ702）に割り当て直すことを含むことができる。本発明のさまざまな実施形態では、変更コンポーネント330は、暗号化データに対する抑制動作および再割り当て動作の両方を実行できる。本発明の1つまたは複数の実施形態では、変更コンポーネント330は、暗号化データに対する抑制動作のみを実行できる。本発明の1つまたは複数の実施形態では、変更コンポーネント330は、暗号化データに対する再割り当て動作のみを実行できる。

【0085】

本発明のさまざまな態様の背景を提供するために、図13および以下の説明は、本発明のさまざまな態様が実装され得る適切な環境の概要を示すよう意図されている。図13は、本発明の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な非限定的動作環境のブロック図を示している。本明細書に記載された本発明の他の実施形態で採用されている類似する要素の説明の繰り返しは、簡潔にするために省略されている。図13を参照すると、本発明のさまざまな態様を実装するための適切な動作環境1000は、コンピュータ1012を含むことができる。コンピュータ1012は、処理ユニット1014、システム・メモリ1016、およびシステム・バス1018を含むこともできる。システム・バス1018は、システム・メモリ1016を含むが、これに限定されないシステム・コンポーネントを、処理ユニット1014に操作可能に結合することができる。処理ユニット1014は、さまざまな使用可能なプロセッサのいずれかであることができる。デュアル・マイクロプロセッサおよびその他のマルチプロセッサ・アーキテクチャが、処理ユニット1014として採用されてもよい。システム・バス1018は、ISA（Industry Standard Architecture）、MCA（Micro Channel Architecture）、EISA（Enhanced ISA）、IDE（Intelligent Drive Electronics）、VESAローカル・バス（VLB：VESA Local Bus）、PCI（Peripheral Component Interconnects）、カードバス、ユニバーサル・シリアル・バス（USB：Universal Serial Bus）、AGP（Advanced Graphics Port）、FireWire、および小型コンピュータ・システム・インターフェイス（SCSI：Small Computer Systems Interface）を含むが、これらに限定されない、任意のさまざまな使用可能なバス・アーキテクチャを使用する、メモリ・バスもしくはメモリ・コントローラ、ペリフェラル・バスもしくは外部バス、またはローカル・バス、あるいはその組合せを含む、複数の種類のバス構造のいずれかであることができる。システム・メモリ1016は、揮発性メモリ1020および不揮発性メモリ1022を含むこともできる。起動中などにコンピュータ1012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出力システム（BIOS：basic input/output system）が、不揮発性メモリ1022に格納され得る。不揮発性メモリ1022の例としては、読み取り専用メモリ（ROM：read only memory）、プログラマブルROM（PROM：programmable ROM）、電氣的プログラマブルROM（EPROM：electrically programmable ROM）、電氣的消去可能プログラマブルROM（EEPROM：electrically erasable programmable ROM）、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：random access memory）（例えば、強誘電体RAM（FeRAM：ferroelectric RAM））が挙げられるが、これらに限定されない。揮発性メモリ1020は、外部キャッシュ・メモリとして機能するランダム・アクセス・メモリ（RAM）を含むこともできる。例えばRAMは、スタティックRAM（SRAM：static RAM）、ダイナミックRAM（DRAM：dynamic RAM）、シンクロナスDRAM

10

20

30

40

50

(S D R A M : synchronous D R A M)、ダブル・データ・レート S D R A M (D D R S D R A M : double data rate S D R A M)、拡張 S D R A M (E S D R A M)、シンクリンク D R A M (S L D R A M : Synchlink D R A M)、ダイレクト・ラムバス R A M (D R R A M : direct Rambus R A M)、ダイレクト・ラムバス・ダイナミック R A M (D R D R A M : direct Rambus dynamic R A M)、およびラムバス・ダイナミック R A M などの、ただしこれらに限定されない、多くの形態で利用可能である。

【 0 0 8 6 】

コンピュータ 1 0 1 2 は、取り外し可能 / 取り外し不可能な揮発性 / 不揮発性のコンピュータ記憶媒体を含むこともできる。例えば図 1 3 は、ディスク・ストレージ 1 0 2 4 を示している。ディスク・ストレージ 1 0 2 4 は、磁気ディスク・ドライブ、フロッピー・ディスク・ドライブ、テープ・ドライブ、J a z ドライブ、Z i p ドライブ、L S - 1 0 0 ドライブ、フラッシュ・メモリ・カード、またはメモリ・スティックなどの、ただしこれらに限定されない、デバイスを含むこともできる。ディスク・ストレージ 1 0 2 4 は、コンパクト・ディスク R O M デバイス (C D - R O M : compact disk R O M device)、記録可能 C D ドライブ (C D - R ドライブ : C D recordable drive)、再書き込み可能 C D ドライブ (C D - R W ドライブ : C D rewritable drive)、またはデジタル多用途ディスク R O M ドライブ (D V D - R O M : digital versatile disk R O M drive) 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記憶媒体を、別々に、または他の記憶媒体と組合せて、含むこともできる。システム・バス 1 0 1 8 へのディスク・ストレージ 1 0 2 4 の接続を容易にするために、インターフェイス 1 0 2 6 などの、取り外し可能または取り外し不可能なインターフェイスが使用され得る。図 1 3 は、ユーザと、適切な動作環境 1 0 0 0 において説明された基本的なコンピュータ・リソースとの間の仲介として機能できるソフトウェアも示している。そのようなソフトウェアは、例えば、オペレーティング・システム 1 0 2 8 を含むこともできる。ディスク・ストレージ 1 0 2 4 に格納できるオペレーティング・システム 1 0 2 8 は、コンピュータ 1 0 1 2 のリソースを制御し、割り当てるように動作する。システムのアプリケーション 1 0 3 0 は、プログラム・モジュール 1 0 3 2 を介して、オペレーティング・システム 1 0 2 8 によるリソースの管理を利用し、例えばシステム・メモリ 1 0 1 6 またはディスク・ストレージ 1 0 2 4 のいずれかに格納されたデータ 1 0 3 4 をプログラムすることができる。さまざまなオペレーティング・システムまたはオペレーティング・システムの組合せを使用して本発明が実装され得るということが、理解されるべきである。ユーザは、1 つまたは複数の入力デバイス 1 0 3 6 を介して、コマンドまたは情報をコンピュータ 1 0 1 2 に入力する。入力デバイス 1 0 3 6 は、マウス、トラックボール、スタイラス、タッチ・パッド、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、T V チューナー・カード、デジタル・カメラ、デジタル・ビデオ・カメラ、W e b カメラなどのポインティング・デバイスを含むことができるが、これらに限定されない。これらおよびその他の入力デバイスは、1 つまたは複数のインターフェイス・ポート 1 0 3 8 を介してシステム・バス 1 0 1 8 を通り、処理ユニット 1 0 1 4 に接続することができる。1 つまたは複数のインターフェイス・ポート 1 0 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 (U S B) を含むことができる。1 つまたは複数の出力デバイス 1 0 4 0 は、入力デバイス 1 0 3 6 と同じ種類のポートの一部を使用できる。このようにして、例えば、U S B ポートを使用して、入力をコンピュータ 1 0 1 2 に提供し、コンピュータ 1 0 1 2 から出力デバイス 1 0 4 0 に情報を出力できる。出力アダプタ 1 0 4 2 は、特殊なアダプタを必要とする出力デバイス 1 0 4 0 の中でも特に、モニタ、スピーカ、およびプリンタのような何らかの出力デバイス 1 0 4 0 が存在することを示すために提供され得る。出力アダプタ 1 0 4 2 の例としては、出力デバイス 1 0 4 0 とシステム・バス 1 0 1 8 の間の接続の手段を提供するビデオ・カードおよびサウンド・カードが挙げられるが、これらに限定されない。1 つまたは複数のリモート・コンピュータ 1 0 4 4 などの、その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が、入力機能および出力機能の両方を提供するというに、留意さ

10

20

30

40

50

りたい。

【 0 0 8 7 】

コンピュータ 1 0 1 2 は、リモート・コンピュータ 1 0 4 4 などの 1 つまたは複数のリモート・コンピュータへの論理接続を使用して、ネットワーク環境内で動作できる。リモート・コンピュータ 1 0 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機器、ピア・デバイス、またはその他の一般的なネットワーク・ノードなどであることができ、通常は、コンピュータ 1 0 1 2 に関連して説明された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 0 4 6 のみが、リモート・コンピュータ 1 0 4 4 と共に示されている。リモート・コンピュータ 1 0 4 4 は、ネットワーク・インターフェイス 1 0 4 8 を介してコンピュータ 1 0 1 2 に論理的に接続されてから、通信接続 1 0 5 0 を介して物理的に接続され得る。さらに、動作は、複数の（ローカルおよびリモートの）システムにわたって分散され得る。ネットワーク・インターフェイス 1 0 4 8 は、ローカル・エリア・ネットワーク（LAN：local-area networks）、広域ネットワーク（WAN：wide-area networks）、セルラー・ネットワークなどの、有線通信ネットワークまたは無線通信ネットワークあるいはその両方を包含できる。LAN 技術は、光ファイバ分散データ・インターフェイス（FDDI：Fiber Distributed Data Interface）、銅線分散データ・インターフェイス（CDDI：Copper Distributed Data Interface）、イーサネット（R）、トークン・リングなどを含む。WAN 技術は、ポイントツーポイント・リンク、総合デジタル通信網（ISDN：Integrated Services Digital Networks）およびその変形などの回路交換網、パケット交換網、およびデジタル加入者回線（DSL：Digital Subscriber Lines）を含むが、これらに限定されない。1 つまたは複数の通信接続 1 0 5 0 は、ネットワーク・インターフェイス 1 0 4 8 をシステム・バス 1 0 1 8 に接続するために採用されたハードウェア/ソフトウェアのことを指す。通信接続 1 0 5 0 は、説明を明確にするために、コンピュータ 1 0 1 2 内に示されているが、コンピュータ 1 0 1 2 の外部に存在することもできる。ネットワーク・インターフェイス 1 0 4 8 に接続するためのハードウェア/ソフトウェアは、単に例示の目的で、通常の電話の等級のモデム、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）・カードなどの、内部および外部の技術を含むこともできる。

【 0 0 8 8 】

本発明の実施形態は、任意の可能な統合の技術的詳細レベルで、システム、方法、装置、またはコンピュータ・プログラム製品、あるいはその組合せであることができる。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コンピュータ可読記憶媒体を含むことができる。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格納できる有形のデバイスであることができる。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合せであることができるが、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、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・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合せを含むこともできる。本明細書において使用されるとき、コンピュータ可読記憶媒体は、それ自体が、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

10

20

30

40

50

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過性の信号であると解釈されるべきではない。

【0089】

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、あるいはその組合せ）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され得る。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、あるいはその組合せを含むことができる。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格納するために転送する。本発明のさまざまな態様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：instruction-set-architecture）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、集積回路のための構成データ、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合せで記述されたソース・コードまたはオブジェクト・コードであることができる。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・コンピュータは、ローカル・エリア・ネットワーク（LAN）または広域ネットワーク（WAN）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、または接続は、（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われ得る。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することができる。

【0090】

本発明の態様は、本明細書において、本発明の実施形態による、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に含まれるブロックの組合せが、コンピュータ可読プログラム命令によって実装され得るという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は、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ることができる。これらのコンピュータ可読プログラム命令は、命令が格納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含むように

10

20

30

40

50

、コンピュータ可読記憶媒体に格納され、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、あるいはその組合せに特定の方式で機能するように指示できるものであることもできる。コンピュータ可読プログラム命令は、コンピュータ上、他のプログラム可能な装置上、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るべく、コンピュータ、他のプログラム可能なデータ処理装置、または他のデバイスに読み込まれ、一連の操作可能な動作を、コンピュータ上、他のプログラム可能な装置上、または他のデバイス上で実行させることもできる。

【0091】

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、規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含んでいる、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することができる。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得る。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、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合せは、規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の組合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され得るということにも留意されたい。

【0092】

本発明の実施形態は、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との一般的な関連において前述されたが、当業者は、本開示がその他のプログラム・モジュールと組み合わせられるか、またはその他のプログラム・モジュールと組合せて実装されてもよいということを認識するであろう。通常、プログラム・モジュールは、特定のタスクを実行するか、または特定の抽象データ型を実装するか、あるいはその両方を行うルーチン、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、当業者は、本発明のコンピュータ実装方法が、シングルプロセッサ・コンピュータ・システム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、コンピュータ、ハンドヘルド・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またはプログラム可能な家庭用電化製品または産業用電子機器などを含む、その他のコンピュータ・システム構成を使用して実践され得るということを理解するであろう。示された態様は、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、分散コンピューティング環境内で実践されてもよい。ただし、本発明の態様の全部ではないとしても一部は、スタンドアロン・コンピュータ上で実践され得る。分散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メモリ・ストレージ・デバイスに配置され得る。

【0093】

本明細書において使用されるとき、「コンポーネント」、「システム」、「プラットフォーム」、「インターフェイス」などの用語は、1つまたは複数の特定の機能を含むコンピュータ関連の実体または操作可能なマシンに関連する実体を指すことができるか、またはそれらの実体を含むことができるか、あるいはその両方が可能である。本明細書で開示された実体は、ハードウェア、ハードウェアとソフトウェアの組合せ、ソフトウェア、または実行中のソフトウェアのいずれかであることができる。例えば、コンポーネントは、プロセッサ上で実行されるプロセス、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、あるいはその組合せであることができる

10

20

30

40

50

が、これらに限定されない。例として、サーバ上で実行され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ることができる。1つまたは複数のコンポーネントが、プロセス内または実行のスレッド内あるいはその両方に存在することができ、コンポーネントは、1つのコンピュータ上に局在するか、または2つ以上のコンピュータ間で分散されるか、あるいはその両方が可能である。別の例では、各コンポーネントは、さまざまなデータ構造が格納されているさまざまなコンピュータ可読媒体から実行できる。コンポーネントは、1つまたは複数のデータ・パケット（例えば、ローカル・システム内または分散システム内の別のコンポーネントと情報をやりとりするか、またはインターネットなどのネットワークを経由して、信号を介して他のシステムと情報をやりとりするか、あるいはその両方によって情報をやりとりする、1つのコンポーネントからのデータ）を含んでいる信号などに従って、ローカルまたはリモートあるいはその両方のプロセスを介して通信できる。別の例として、コンポーネントは、電気または電子回路によって操作される機械的部品によって提供される特定の機能を有する装置であることができ、プロセッサによって実行されるソフトウェア・アプリケーションまたはファームウェア・アプリケーションによって操作される。そのような場合、プロセッサは、装置の内部または外部に存在することができ、ソフトウェア・アプリケーション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、機械的部品を含まない電子コンポーネントを介して特定の機能を提供する装置であることができ、それらの電子コンポーネントは、電子コンポーネントの機能の少なくとも一部を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その他の手段を含むことができる。1つの態様では、コンポーネントは、例えばクラウド・コンピューティング・システム内で、仮想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。

【0094】

加えて、「または」という用語は、排他的論理和ではなく、包含的論理和を意味するよう意図されている。すなわち、特に指定されない限り、または文脈から明らかでない限り、「XがAまたはBを採用する」は、自然な包含的順列のいずれかを意味するよう意図されている。すなわち、XがAを採用するか、XがBを採用するか、またはXがAおよびBの両方を採用する場合、「XがAまたはBを採用する」が、前述の事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「a」および「an」は、単数形を対象にすることが特に指定されない限り、または文脈から明らかでない限り、「1つまたは複数」を意味すると一般に解釈されるべきである。本明細書において使用されるとき、「例」または「例示的」あるいはその両方の用語は、例、事例、または実例となることを意味するために使用される。誤解を避けるために、本明細書で開示された主題は、そのような例によって制限されない。加えて、「例」または「例示的」あるいはその両方として本明細書に記載された任意の態様または設計は、他の態様または設計よりも好ましいか、または有利であると必ずしも解釈されず、当業者に知られている同等の例示的な構造および技術を除外するよう意図されていない。

【0095】

本明細書において使用されるとき、「プロセッサ」という用語は、シングルコア・プロセッサと、ソフトウェアのマルチスレッド実行機能を備えるシングルプロセッサと、マルチコア・プロセッサと、ソフトウェアのマルチスレッド実行機能を備えるマルチコア・プロセッサと、ハードウェアのマルチスレッド技術を備えるマルチコア・プロセッサと、並列プラットフォームと、分散共有メモリを備える並列プラットフォームとを含むが、これらに限定されない、実質的に任意の計算処理ユニットまたはデバイスを指すことができる。さらに、プロセッサは、集積回路、特定用途向け集積回路（ASIC：application specific integrated circuit）、デジタル信号プロセッサ（DSP：digital signal processor）、フィールド・プログラマブル・ゲート・アレイ（FPGA：field programmable gate array）、プログラマブル・ロジック・コントローラ（PLC：programmable logic controller）、複合プログラム可能論理デバイス（CPLD：complex programma

10

20

30

40

50

ble logic device)、個別のゲートまたはトランジスタ論理、個別のハードウェア・コンポーネント、あるいは本明細書に記載された機能を実行するように設計されたこれらの任意の組合せを指すことができる。さらに、プロセッサは、空間利用を最適化し、ユーザ機器の性能を向上するために、分子および量子ドットベースのトランジスタ、スイッチ、およびゲートなどの、ただしこれらに限定されない、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、計算処理ユニットの組合せとして実装されてもよい。本明細書では、コンポーネントの動作および機能に関連する「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」、および実質的に任意のその他の情報格納コンポーネントなどの用語は、「メモリ・コンポーネント」、「メモリ」内に具現化された実体、またはメモリを含んでいるコンポーネントを指すために使用される。本明細書に記載されたメモリまたはメモリ・コンポーネントあるいはその両方が、揮発性メモリまたは不揮発性メモリのいずれかであることができ、あるい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ということが、理解されるべきである。不揮発性メモリの例としては、読み取り専用メモリ(ROM)、プログラマブルROM(PROM)、電氣的プログラマブル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))が挙げられるが、これらに限定されない。揮発性メモリは、例えば外部キャッシュ・メモリとして機能できる、RAMを含むことができる。例えば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)、拡張SDRAM(ESDRAM)、シンクリンクDRAM(SLDRAM)、ダイレクト・ラムバスRAM(DRRAM)、ダイレクト・ラムバス・ダイナミックRAM(DRDRAM)、およびラムバス・ダイナミックRAM(RDRAM: Rambus dynamic RAM)などの、ただしこれらに限定されない、多くの形態で利用可能である。さらに、本明細書において開示されたシステムまたはコンピュータ実装方法のメモリ・コンポーネントは、これらおよび任意のその他の適切な種類のメモリを含むが、これらに限定されない、メモリを含むよう意図されている。

【0096】

前述した内容は、システム、コンピュータ・プログラム製品、およびコンピュータ実装方法の単なる例を含んでいる。当然ながら、本発明を説明する目的で、コンポーネント、製品、またはコンピュータ実装方法、あるいはその組合せの考えられるすべての組合せについて説明することは不可能であるが、当業者は、本発明の多くのその他の組合せおよび並べ替えが可能であるということを認識できる。さらに、「含む」、「有する」、「所有する」などの用語が、発明を実施するための形態、特許請求の範囲、付録、および図面において使用される範囲では、それらの用語は、「備えている」が特許請求における暫定的な用語として使用されるときに解釈されるような、用語「備えている」と同様の方法で、包含的であるよう意図されている。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、開示された実施形態に制限されない。本発明の範囲を逸脱することなく多くの変更および変形が可能であることは、当業者にとって明らかである。本明細書で使用された用語は、本発明の原理、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発明を理解できるようにするために選択されている。

10

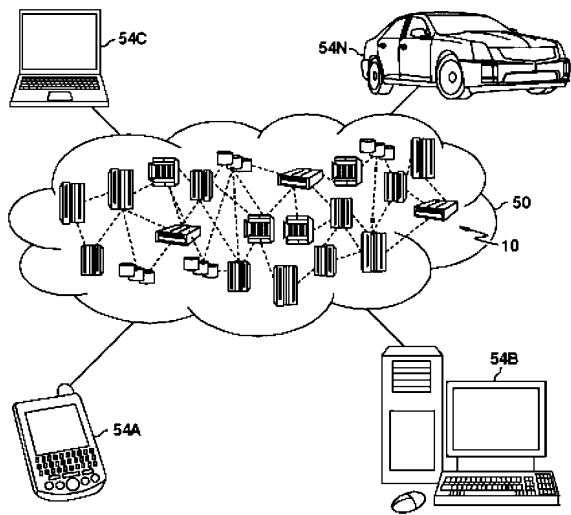
20

30

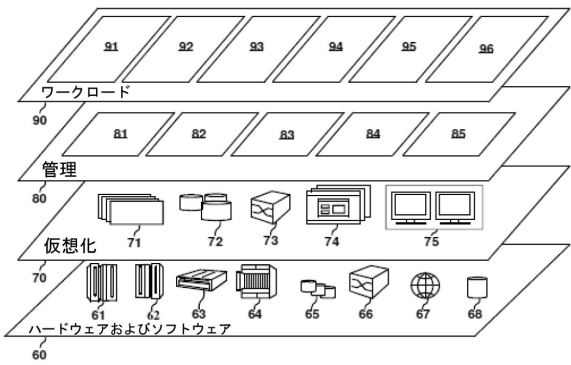
40

【図面】

【図 1】

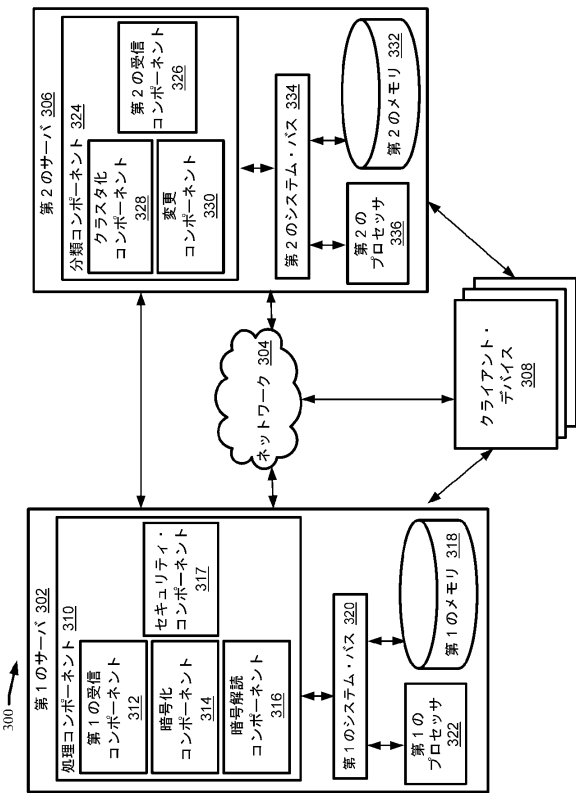


【図 2】

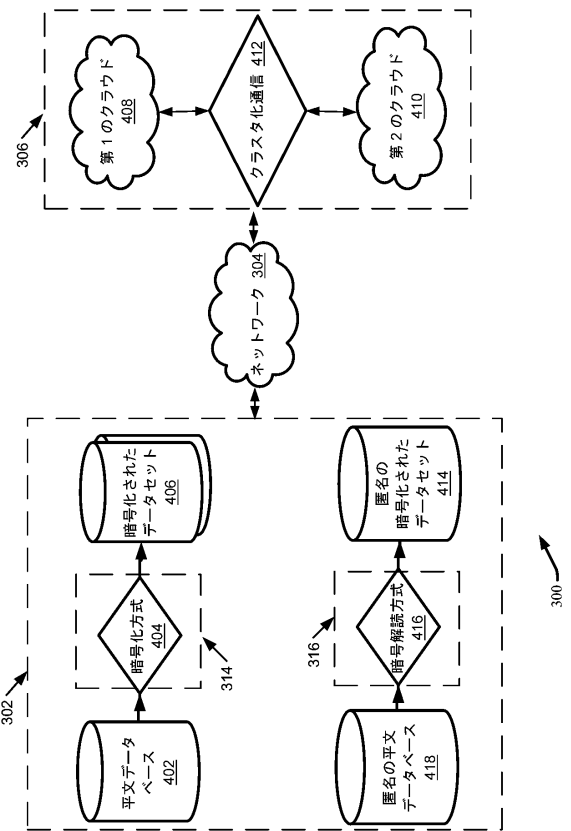


10

【図 3】



【図 4】



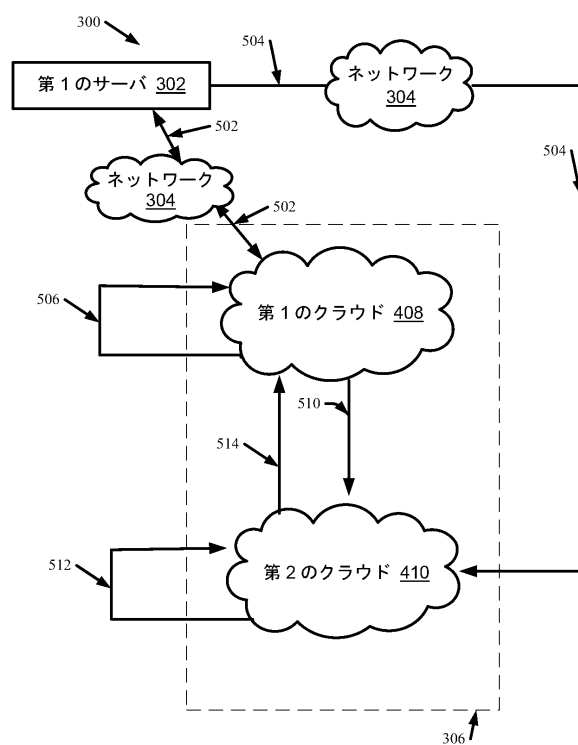
20

30

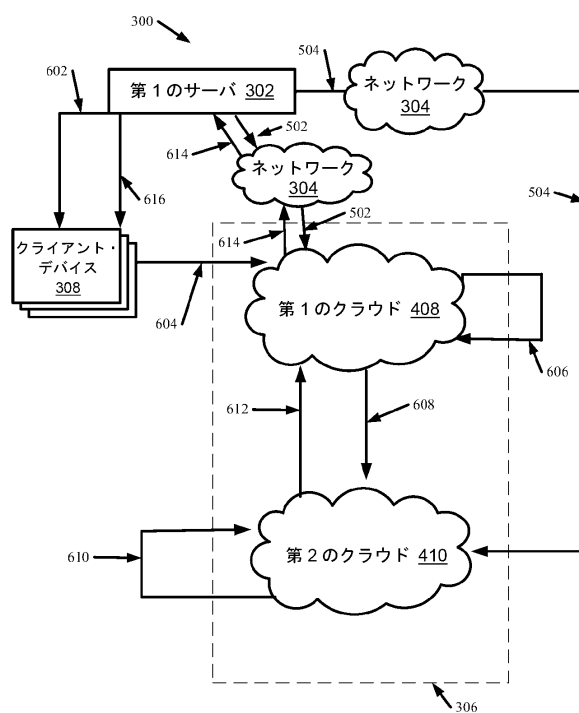
40

50

【 図 5 】



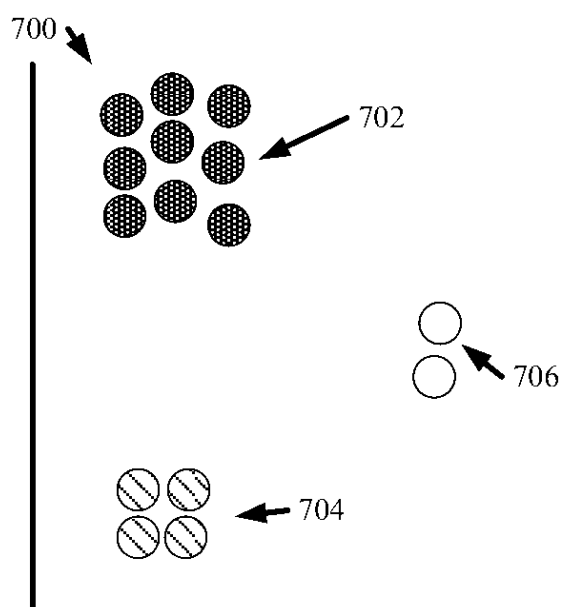
【 図 6 】



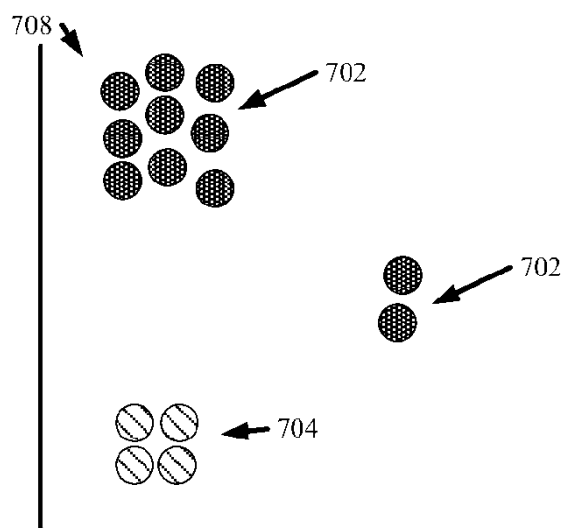
10

20

【圖 7】



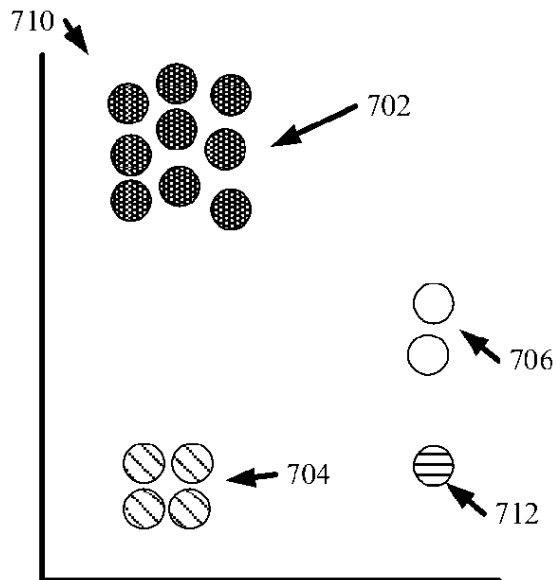
【圖 8】



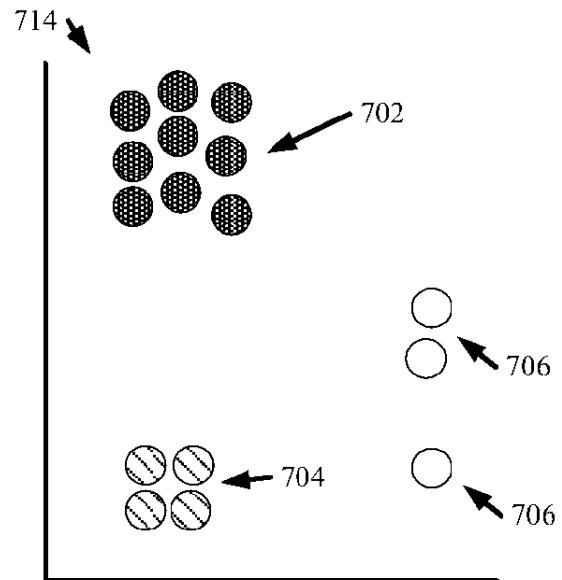
30

40

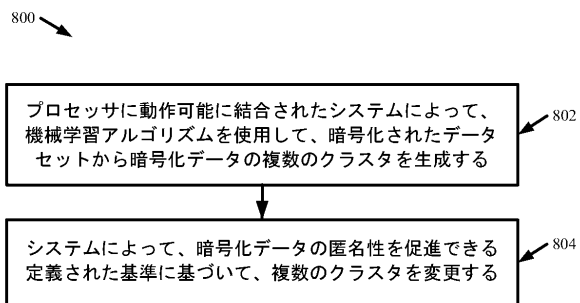
【図 9】



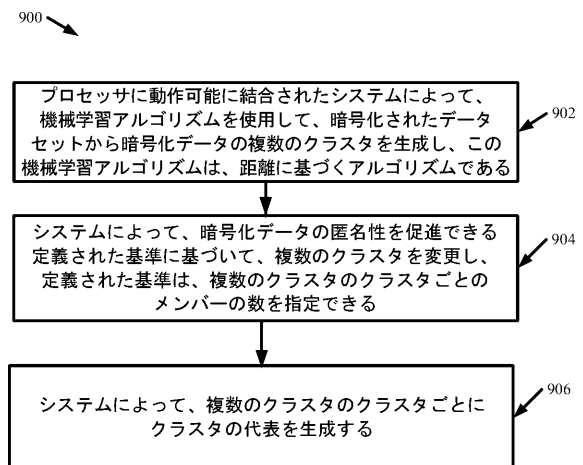
【図 10】



【図 11】



【図 12】



10

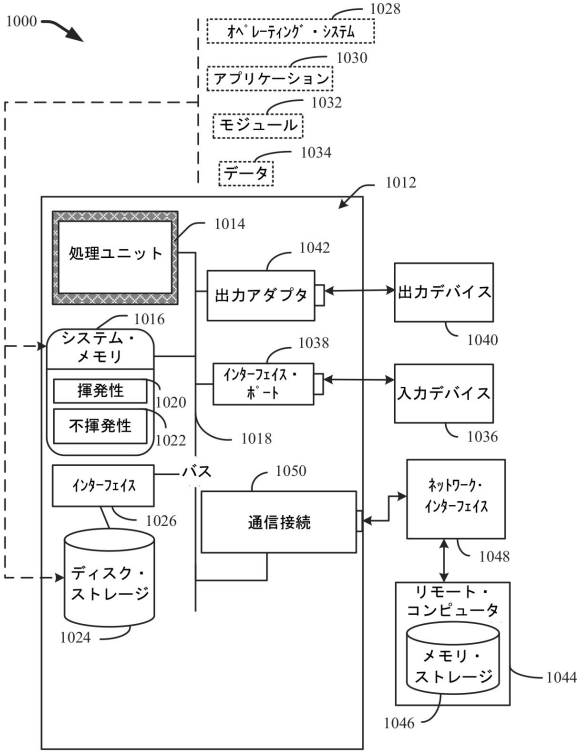
20

30

40

50

【図 13】



10

20

30

40

50

フロントページの続き

- (72)発明者 アントナトス、スピリドン
 アイルランド モルハダート 1 5 ダマスタウン インダストリアル エステイト テクノロジーキャンパス
- (72)発明者 ブラーギン、ステファーン
 アイルランド モルハダート 1 5 ダマスタウン インダストリアル エステイト テクノロジーキャンパス
- (72)発明者 ケサーワーニ、マニッシュ
 インド ケーエー 5 6 0 0 4 5 バンガロール ラチェナハリ アンド ナガワラ・ビレッジ マニヤータ・ビー・エンパシー アウター・リング・ロード
- (72)発明者 カウル、アクシャル
 インド ケーエー 5 6 0 0 4 5 バンガロール ラチェナハリ アンド ナガワラ・ビレッジ マニヤータ・ビー・エンパシー アウター・リング・ロード
- (72)発明者 メータ、サミーブ
 インド ケーエー 5 6 0 0 4 5 バンガロール ラチェナハリ アンド ナガワラ・ビレッジ マニヤータ・ビー・エンパシー アウター・リング・ロード
- 審査官 吉田 歩
- (56)参考文献 特開 2 0 1 6 - 0 5 3 6 9 3 (J P , A)
 特開 2 0 1 7 - 0 2 7 1 3 7 (J P , A)
 米国特許出願公開第 2 0 1 7 / 0 0 7 6 1 0 5 (U S , A 1)
- (58)調査した分野 (Int.Cl., D B 名)
 G 0 6 F 2 1 / 6 2
 G 0 9 C 1 / 0 0