(19)日本国特許庁(JP)

# (12)特許公報(B2)

(11)特許番号
特許第7015904号
(P7015904)

(45)発行日　令和4年2月3日(2022.2.3)

(24)登録日　令和4年1月26日(2022.1.26)

(51)国際特許分類

| | | | | |
|---|---|---|---|---|
| *Ｇ０６Ｆ　21/62　(2013.01)* | | Ｇ０６Ｆ | 21/62 | ３１８ |
| *Ｈ０４Ｌ　9/08　(2006.01)* | | Ｈ０４Ｌ | 9/08 | Ｃ |

請求項の数　17　（全29頁）

(21)出願番号　特願2020-500817(P2020-500817)
(86)(22)出願日　平成30年7月5日(2018.7.5)
(65)公表番号　特表2020-527791(P2020-527791A)
(43)公表日　令和2年9月10日(2020.9.10)
(86)国際出願番号　PCT/IB2018/054958
(87)国際公開番号　WO2019/016641
(87)国際公開日　平成31年1月24日(2019.1.24)
審査請求日　令和2年12月22日(2020.12.22)
(31)優先権主張番号　15/652,314
(32)優先日　平成29年7月18日(2017.7.18)
(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　ＢＵＳＩＮＥＳＳ　ＭＡＣＨＩＮＥＳ　ＣＯＲＰＯＲＡＴＩＯＮ
アメリカ合衆国１０５０４　ニューヨーク州　アーモンク　ニュー　オーチャード　ロード
Ｎｅｗ　Ｏｒｃｈａｒｄ　Ｒｏａｄ，　Ａｒｍｏｎｋ，　Ｎｅｗ　Ｙｏｒｋ　１０５０４，　Ｕｎｉｔｅｄ　Ｓｔａｔｅｓ　ｏｆ　Ａｍｅｒｉｃａ
(74)代理人　100108501
弁理士　上野 剛史

最終頁に続く

(54)【発明の名称】　セキュア実行プラットフォームのクラスタ

(57)【特許請求の範囲】
【請求項１】
データ・ストレージに対する接続性を有するセキュア実行プラットフォーム（ＳＥＰ）のクラスタを含むシステムであって、前記クラスタの各ＳＥＰはキーを用いてデータを処理する際にデータの機密性を維持するように構成され、
前記キーは前記クラスタの前記ＳＥＰ間で共有され、前記キーは前記クラスタまたはその一部分によって自動的に生成され、かつ任意の非クラスタ・エンティティには利用不可能であり、
前記データ・ストレージは前記キーを用いて暗号化された暗号化データを保持し、
前記クラスタの第１のＳＥＰは、前記キーを用いてクライアント・データを暗号化して暗号化クライアント・データを得て、前記暗号化クライアント・データを前記データ・ストレージに保存するように構成され、
前記クラスタの第２のＳＥＰは、前記データ・ストレージから暗号化保存データを検索し、前記キーを用いて前記暗号化保存データを復号して前記暗号化保存データの非暗号化形を得るように構成され、
前記クラスタの第３のＳＥＰは、前記クラスタに新たなＳＥＰを加えるように構成され、
前記第３のＳＥＰはセキュアな通信チャネルを通じて前記新たなＳＥＰに前記キーを転送するように構成され、
前記第３のＳＥＰは、セキュアなチャネルを通じて前記キーを転送する前に、前記新たなＳＥＰが前記キーを受信することを許可されていることを確認するために掲示板を観察す

るように構成される、システム。
【請求項２】
前記第２のＳＥＰは、クライアント・デバイスからのクエリに応答して前記暗号化保存データを検索するように構成され、前記クエリに対する応答を提供するために前記暗号化保存データの前記非暗号化形が使用されることによって、前記クライアント・デバイスが前記データ・ストレージにアクセスすることなく前記クエリが実現される、請求項１に記載のシステム。
【請求項３】
前記第１のＳＥＰと前記第２のＳＥＰとは同じＳＥＰである、請求項１に記載のシステム。
【請求項４】
前記第１のＳＥＰは前記データ・ストレージへの書込み専用のアクセス許可を有し、前記第２のＳＥＰは前記データ・ストレージへの読取り専用のアクセス許可を有する、請求項１に記載のシステム。
【請求項５】
前記第３のＳＥＰは、セキュアなチャネルを通じて前記キーを転送する前に、認証機構を用いて前記新たなＳＥＰのコードおよびプラットフォームの正しさを確認するように構成される、請求項１に記載のシステム。
【請求項６】
前記新たなＳＥＰは、前記第３のＳＥＰからの前記キーを受け入れる前に、認証機構を用いて前記第３のＳＥＰのコードおよびプラットフォームの正しさを確認するように構成される、請求項１に記載のシステム。
【請求項７】
前記掲示板は分散フォールト・トレラント・スキームを用いて実現される、請求項１に記載のシステム。
【請求項８】
前記掲示板は専用のＳＥＰを用いて実現される、請求項１に記載のシステム。
【請求項９】
前記第３のＳＥＰは、前記掲示板において観察される情報が閾値よりも大きい数の管理者によって署名されていることを確認するように構成される、請求項８に記載のシステム。
【請求項１０】
前記新たなＳＥＰは前記キーを転送することを禁じられる、請求項１に記載のシステム。
【請求項１１】
前記第３のＳＥＰは前記新たなＳＥＰに対する予め定められた寿命を設定するように構成され、前記新たなＳＥＰは前記予め定められた寿命の最後に前記クラスタから除去されるように構成される、請求項１に記載のシステム。
【請求項１２】
前記第３のＳＥＰは、前記クラスタ内のＳＥＰの数が予め規定された閾値未満であることに応答して前記クラスタに前記新たなＳＥＰを加えるように構成される、請求項１に記載のシステム。
【請求項１３】
前記第３のＳＥＰは、前記第１のＳＥＰまたは前記第２のＳＥＰが非動作的になったことに応答して前記クラスタに前記新たなＳＥＰを加えるように構成され、それによって前記新たなＳＥＰは非動作的ＳＥＰと置き換わるように構成される、請求項１に記載のシステム。
【請求項１４】
前記第３のＳＥＰは、前記第１のＳＥＰまたは前記第２のＳＥＰと同じＳＥＰである、請求項１に記載のシステム。
【請求項１５】
前記キーは前記クラスタの第３のＳＥＰによって生成され、前記第３のＳＥＰは前記キーを前記クラスタ内の他のＳＥＰに分配するように構成される、請求項１に記載のシステム。

【請求項１６】
前記クラスタは、前記キーを生成することに応答して、前記キーに合意するためにコンセンサス・プロトコルを使用するように構成される、請求項１に記載のシステム。
【請求項１７】
前記クラスタまたは前記データ・ストレージの管理者は前記キーを有さない、請求項１に記載のシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
本開示は一般的にデータ・セキュリティに関し、特にセキュア実行プラットフォームに関する。
【背景技術】
【０００２】
今日、一般的に極秘データと呼ばれる機密データまたはプライベート・データが、しばしば中央データ・ストレージに保持される。こうした極秘データのソースはさまざまであってもよい。その極秘データは、データ・ストレージに自身の取引上の秘密を預けるビジネス・エンティティから受け取ったものか、生体サンプルを提供することが法律により要求される一般市民から受け取ったものか、または任意のその他のソースからのものかどうかにかかわらず、保存されるデータの機密性が維持される必要がある。
【０００３】
データ・ストレージはクライアント・クエリに応答してサーバによってアクセス可能であってもよく、それによって極秘データの適度かつ制限された使用が可能になってもよい。場合によっては、サーバはクライアントがこうしたクエリを行う許可を有すること、およびその動作パターンがクライアントの役割と矛盾しないことを確実にする。サーバは情報を処理するときに匿名化し、返答として匿名データを提供してもよい。
【発明の概要】
【発明が解決しようとする課題】
【０００４】
しかし、サーバはなおも極秘データを処理しており、未処理のデータ自体へのアクセスを有する。結果として、サーバ内に漏洩点となり得るところがないことを確実にすることが重要であろう。場合によっては、こうしたサーバの管理者は注意深く選択され、サーバへのアクセスを与えられる前に厳重な精査を受ける。管理者はサーバ内に保持されるデータに対する制限されないアクセスを保持してもよく、結果として中央データ・ストレージに保持されるすべての極秘データに対する無制限のアクセスを有してもよい。よって発明が解決しようとする課題はセキュア実行プラットフォームのクラスタを含むシステムおよびそのプログラムを提供することである。
【課題を解決するための手段】
【０００５】
開示される主題の１つの例示的実施形態はシステムであり、このシステムは、データ・ストレージに対する接続性を有するセキュア実行プラットフォーム（ＳＥＰ：Ｓｅｃｕｒｅ Ｅｘｅｃｕｔｉｏｎ Ｐｌａｔｆｏｒｍｓ）のクラスタを含み、前記クラスタの各ＳＥＰはキーを用いてデータを処理する際にデータの機密性を維持するように構成され、キーは前記クラスタのＳＥＰ間で共有され、キーは前記クラスタまたはその一部分によって自動的に生成され、かつ任意の非クラスタ・エンティティには利用不可能であり、前記データ・ストレージはキーを用いて暗号化された暗号化データを保持し、前記クラスタの第１のＳＥＰは、キーを用いてクライアント・データを暗号化して暗号化クライアント・データを得て、この暗号化クライアント・データを前記データ・ストレージに保存するように構成され、前記クラスタの第２のＳＥＰは、前記データ・ストレージから暗号化保存データを検索し、キーを用いて暗号化保存データを復号して暗号化保存データの非暗号化形を得るように構成される。

【０００６】
開示される主題の別の例示的実施形態は、コンピュータ環境内のセキュア実行プラットフォーム（ＳＥＰ）によって実行されるべき命令を保持する非一時的コンピュータ可読ストレージ媒体を含むコンピュータ・プログラム製品であり、コンピュータ環境はデータ・ストレージに対する接続性を有するＳＥＰのクラスタを含み、データ・ストレージはキーを用いて暗号化された暗号化データを保持し、キーはクラスタのＳＥＰ間で共有され、キーはクラスタまたはその一部分によって自動的に生成され、かつ任意の非クラスタ・エンティティには利用不可能であり、クラスタはＳＥＰを含み、前記クラスタの各ＳＥＰはキーを用いてデータを処理する際にデータの機密性を維持するように構成され、命令はＳＥＰによって実行されるときにＳＥＰに、第１のクライアント・デバイスからセキュアな通信チャネルを通じて第１のクライアント・データを受信したことに応答して、キーを用いて第１のクライアント・データを暗号化して暗号化クライアント・データを得て、暗号化クライアント・データをデータ・ストレージに保存することによって、データ・ストレージに保持される第１のクライアント・データが任意の非コンピュータ・エンティティには得られないようにするステップと、保持されるデータへのアクセスを必要とする第２のクライアント・デバイスからアクセス・クエリを受信したことに応答して、データ・ストレージから保持されるデータの暗号化形を検索し、キーを用いて暗号化形を復号して第２のクライアント・データを得て、セキュアな通信チャネルを通じて第２のクライアント・デバイスへの応答を提供するステップとを行わせ、この応答は第２のクライアント・データに基づく。
【０００７】
本開示の主題は、図面とともになされる以下の詳細な説明からより完全に理解および認識されることとなり、図面における対応または類似の番号または文字は、対応または類似の構成要素を示す。別様に示されない限り、図面はこの開示の例示的実施形態または態様を提供するものであり、この開示の範囲を限定することはない。
【図面の簡単な説明】
【０００８】
【図１】開示される主題のいくつかの例示的実施形態によるシステムを示すブロック図である。
【図２】開示される主題のいくつかの例示的実施形態による方法を示す流れ図である。
【図３】開示される主題のいくつかの例示的実施形態による方法を示す流れ図である。
【図４】開示される主題のいくつかの例示的実施形態による方法を示す流れ図である。
【図５】開示される主題のいくつかの例示的実施形態による方法を示す流れ図である。
【図６】開示される主題のいくつかの例示的実施形態によるシステムを示す概略図である。
【発明を実施するための形態】
【０００９】
開示される主題によって対処される技術的課題の１つは、データを処理する際にデータの機密性を維持することである。
【００１０】
多くのアプリケーションおよびプログラムは、極秘データの処理および対処を伴ってもよい。極秘データは、権限付与されていないアクセスまたはより高い特権レベルにおいて実行される不正ソフトウェアによる改変から保護されるべきである。正規のソフトウェアまたはユーザが極秘データに関連するプラットフォーム・リソースを使用するかまたは使用の管理をする能力を妨げることなく、極秘データの機密性および完全性を保存することが必要とされてもよい。
【００１１】
いくつかの例示的実施形態において、極秘データは、正規のソフトウェアまたはユーザがそれに対するアクセスを有して、既存のデータの機密性に影響することなく新たなデータを加えること、または異なるサービスの提供において既存のデータを用いることなどの能力を有し得るようなやり方で保持されてもよい。いくつかの例示的実施形態において、信

頼されないアプリケーションおよびユーザが極秘データの読取りまたは更新を行うためにそれにアクセスすることが防止されることが望ましくてもよい。

【００１２】

開示される主題によって対処される別の技術的課題は、たとえば人間の管理者またはユーザなどの脆弱な非コンピュータ・エンティティによって知覚されるリスクを低減することである。

【００１３】

極秘データに関連する多くのアプリケーションおよびサービスは、それらを管理し実行する中央の信頼された機関に依拠し得る。場合によっては、たとえば管理者などの信頼された機関が極秘データを悪用するか、または取り扱いを誤ってセキュリティ違反をもたらすことがある。一例として、セキュアな個人の健康管理データを保持するデータベースの取り扱いのために信頼された機関が用いられてもよい。別の例として、管理者はセキュアなバイオメトリック・データベースを管理してもよい。さらに別の例として、データ・ストレージは、たとえば証券会社が発行する商取引を取り扱うか、または競売を行って入札を受け取ることなどを行うシステムなどの場合に、金融データを保存してもよい。開示される主題は、情報エスクロー、バイオインフォマティクス・データ・プラットフォーム、または健康管理サービス・プラットフォームなどにも用いられてもよい。

【００１４】

場合によっては、たとえばスノーデンの漏洩などのように、ハッカーまたは悪質な職員などが、特権アカウントへの侵入、極秘データへのアクセス、または極秘データのコピーもしくは漏洩などによって極秘データのセキュリティを危機にさらすことがある。

【００１５】

開示される主題によって対処されるさらに別の技術的課題は、一旦動作的になると人間のユーザから完全にデータを隠匿し、いかなる人間の支配も受けないコンピュータ・プラットフォームを提供することである。

【００１６】

保護されていないコンピュータ・エンティティまたはユーザからデータを隠匿し続けることは、実際のセキュアな実行における最も困難な課題の１つである。通常、実行プラットフォームは人間のユーザによって管理される。たとえ実行プラットフォームが処理データを暗号化するために暗号化キーを使用しても、たとえばサーバがつぶれてそれと置き換えるために新たなサーバを実行させる必要があり、極秘データを復号するためにキーを必要とする場合などに、こうしたキーは人間のユーザに知られるか、または取得され得る。キーを得た攻撃者は暗号化データから元のデータを復元して、悪用または拡散できる。攻撃者はキーを知っている人間のエンティティから、たとえば盗むこと、買い取ること、人為的エラー、またはソーシャル・エンジニアリングなどによってキーを得ることがある。付加的または代替的に、攻撃者は悪質なソフトウェア・エージェントを導入して実行プラットフォームで実行させることによって、キーを得ることがある。たとえばソーシャル・エンジニアリングの使用などを通じて、悪質なソフトウェア・エージェントに管理者の許可が与えられるかもしれず、結果としてプラットフォームの管理者がアクセス可能なすべての情報に通じるかもしれない。

【００１７】

１つの技術的解決策は、セキュア実行プラットフォーム（ＳＥＰ）のクラスタによってキーを自動的に生成することである。キーは、データを処理する際にデータの機密性を維持するために使用されてもよい。キーは、クラスタのＳＥＰのみが利用可能であってもよい。クラスタのメンバーではない他のコンピュータ・エンティティ、たとえばサーバ、ＳＥＰ、またはコンピュータ装置などはキーへのアクセスを有さなくてもよく、かつキーを得ることができなくてもよい。さらに、ＳＥＰによって実行されるたとえばソフトウェア、ファームウェア、ハードウェア、それらの組み合わせなどにおいて実現されるエージェントは、もしそのエージェントが「権限付与された」とみなされなければキーへのアクセスを制限されてもよい。場合によっては、ＳＥＰが権限付与および非権限付与エージェント

を同時に実行して、権限付与エージェントのみにキーへのアクセスを許可してもよく、これは開示される主題によるプロトコルに従って行われる。いくつかの例示的実施形態において、ＳＥＰによって実行される権限付与エージェントは、キーを得ること、キーを用いて極秘データを復号すること、キーを用いて極秘データを暗号化すること、および復号データを処理することを行い得る唯一のエージェントであってもよい。付加的または代替的に、権限付与エージェントは、他のエージェントまたはＳＥＰにキーを転送できる唯一のエージェントであってもよい。

【００１８】

いくつかの例示的実施形態において、ＳＥＰのクラスタは、極秘データを保持するように構成されたデータ・ストレージに接続されてもよい。データ・ストレージは、キーを用いて暗号化されたデータの暗号化形を保持してもよい。データ・ストレージに保存されたデータは、クラスタのＳＥＰによって実行される権限付与エージェントにアクセスされてもよく、この権限付与エージェントは暗号化を復号できてもよい。データは、キーを用いてその暗号化形に基づいて再構築されてもよい。

【００１９】

いくつかの例示的実施形態において、ＳＥＰの権限付与エージェントは、キーを用いてデータを復号し、たとえこうしたデータが計算に使用されるときにも復号データへの任意のアクセスを防ぐように構成されてもよい。復号データは、処理自体を行う権限付与エージェントを除く、ＳＥＰによって実行されるすべての特権ソフトウェア（例、カーネル、ハイパーバイザなど）がアクセスできないセキュアなコンテナ内でＳＥＰによって保持されてもよく、結果として権限付与エージェントのみが復号形の極秘データへのアクセスを有する。

【００２０】

いくつかの例示的実施形態において、キーはクラスタのＳＥＰ間で共有されてもよい。クラスタの各ＳＥＰは、キーを用いてデータを処理する際にデータの機密性を維持するように構成されてもよい。

【００２１】

いくつかの例示的実施形態において、クラスタのＳＥＰは、キーを用いてデータを暗号化して暗号化データを得るように構成されてもよい。クラスタのＳＥＰは、次いで暗号化データをデータ・ストレージに保存してもよい。クラスタのＳＥＰはさらに、たとえば権限付与エージェントを実行することなどによって、データ・ストレージから暗号化データを検索し、キーを用いて暗号化保存データを復号して、暗号化保存データの非暗号化形を得るように構成されてもよい。場合によっては、ＳＥＰはクライアント・デバイスからのクライアント・クエリを扱い、こうしたクエリを実現するためにデータ・ストレージにアクセスするように構成されてもよい。

【００２２】

いくつかの例示的実施形態において、ＳＥＰの１つ、またはいくつかのＳＥＰの組み合わせなどによって、キーが自律的に生成されてもよい。たとえばＰＡＸＯＳ、Ｃｈａｎｄｒａ－Ｔｏｕｅｇ合意アルゴリズム、またはラフトなどのコンセンサス・プロトコルを用いて、キーがクラスタによって合意されてもよい。いくつかの例示的実施形態においては、キー自体を生成するリーダー（ｌｅａｄｅｒ）を選択するためにコンセンサス・プロトコルが使用されてもよい。付加的または代替的に、いくつかのＳＥＰがランダムな値を生成し、それらが組み合わされてキーを作成してもよい。クラスタによって用いられるキーは、決して表示されたり別様に人間のユーザに出力されたりしてはならず、かつクラスタの一部ではない任意の他のコンピュータ・デバイス、またはたとえクラスタのＳＥＰによって実行されるエージェントであっても任意の非権限付与エージェントへの分配が制限されてもよい。こうして、人間のユーザまたはその他の非権限付与エンティティはキーを認識しなくてもよく、こうしたエンティティはもし損なわれても極秘データのセキュリティを損なわなくてもよい。

【００２３】

いくつかの例示的実施形態において、クラスタはオン・ザ・フライで複製を作成し、クラスタに新たなＳＥＰを加えるように構成されてもよい。場合によっては、クラスタ内のＳＥＰの数が予め定められた閾値未満に落ちたときに、クラスタに新たなＳＥＰが加えられ、権限付与エージェントは新たなＳＥＰの各々において開始される。新たなＳＥＰは、すでにクラスタのメンバーであるＳＥＰからキーを受信してもよい。いくつかの例示的実施形態において、キーを失う可能性およびそれとともに極秘データを失う可能性を回避するために、クラスタは最小限のサイズを保ってもよい。

【００２４】

いくつかの例示的実施形態において、クラスタのＳＥＰには異なるタスクおよび特権が提供されてもよい。いくつかの例示的実施形態において、いくつかのＳＥＰはデータ・ストレージにデータを書込むことができてもよく、一方でいくつかのＳＥＰはデータ・ストレージからデータを読取ることができてもよい。付加的または代替的に、いくつかのＳＥＰはクラスタに新たなＳＥＰを加えることができてもよい。いくつかの例示的実施形態において、作成された新たなＳＥＰには特定のタスク（例、書込みまたは読取りなど）が与えられてもよい。新たなＳＥＰには、たとえば１日または１時間などの予め定められた寿命が与えられてもよい。予め定められた寿命の最後に、新たなＳＥＰは自動的にクラスタから出てもよい。いくつかの例示的実施形態において、新たなＳＥＰは、他のＳＥＰを含む他のデバイスにキーを分配することを禁じられることによって、クラスタに新たなＳＥＰを加えることで生じ得るリスクを減らしてもよい。

【００２５】

開示される主題を使用することの１つの技術的効果は、内部攻撃、悪質な職員、特権ユーザのデバイスのハッキング、または管理者のソーシャル・エンジニアリングなどの結果もたらされるデータ漏洩を防ぐことである。

【００２６】

いくつかの例示的実施形態において、クラスタは極秘データに対する唯一の有効なゲートウェイの役割をすることによって、中央データ・ストアからのデータ漏洩の可能性を限定する。

【００２７】

いくつかの例示的実施形態において、開示される主題は、人間の介在なしに動作でき、かつハードウェア自体へのアクセスを有するユーザを含む人間に制御されるシステムから秘密キーを守り、かつそれによって実行されるオペレーティング・システムにおけるルート特権を有することのできる自律的コンピュータ・エンティティを提供する。

【００２８】

別の技術的効果は、極秘データの損失を効果的に防ぐことであってもよい。単一のＳＥＰとは異なり、ＳＥＰのクラスタを用いることで、同時にすべてのＳＥＰが非動作的になる可能性が低くなり、よってＳＥＰのみに知られるキーが失われる可能性も低くなる。もしキーが失われれば、暗号化データが無益になり得る。

【００２９】

さらに別の技術的効果は、自律的データ管理、すなわちデータに対する責任を管理者からセキュアなハードウェアに移すことを提供することであってもよい。自律的データ管理は、任意の外部機関による影響または検査を受け得ない。自律的データ管理の決定的な特性は、自身が行うようにプログラミングされたことのみを行うことである。

【００３０】

開示される主題は、任意の既存の技術および当該技術分野において以前からルーチンまたは従来のものとなっていた任意の技術を上回る１つまたはそれ以上の技術的改善を提供してもよい。

【００３１】

本開示に鑑みて、当業者には付加的な技術的課題、解決策、および効果が明らかとなってもよい。

【００３２】

ここで、開示される主題のいくつかの例示的実施形態によるシステムの例示を示す図１を参照する。

【００３３】

いくつかの例示的実施形態において、システム１００はＳＥＰ１２２、１２４、１２６、および１２８のクラスタ１２０を含んでもよい。クラスタ１２０は任意の数のＳＥＰを含んでもよく、図１は単なる例示である。各ＳＥＰは、たとえばインテル（Ｉｎｔｅｌ）（Ｒ）のＳｏｆｔｗａｒｅ Ｇｕａｒｄ Ｅｘｔｅｎｓｉｏｎｓ（ＴＭ）（ＳＧＸ（ＴＭ））、トラステッド・エグゼキューション・テクノロジー（ＴＸＴ：Ｔｒｕｓｔｅｄ Ｅｘｅｃｕｔｉｏｎ Ｔｅｃｈｎｏｌｏｇｙ）を有するサーバ、コンピュータ装置トラステッド・プラットフォーム・モジュール（ＴＰＭ：Ｔｒｕｓｔｅｄ Ｐｌａｔｆｏｒｍ Ｍｏｄｕｌｅ）、ＩＢＭ（ＩＢＭ社の登録商標）のＳｅｃｕｒｅ Ｂｌｕｅ＋＋（ＴＭ）、またはＡＭＤ（Ｒ）のＳｅｃｕｒｅ Ｍｅｍｏｒｙ Ｅｎｃｒｙｐｔｉｏｎ（ＴＭ）（ＳＭＥ（ＴＭ））などの信頼されるハードウェア実行プラットフォームに基づいていてもよい。

【００３４】

一例として、ＳＧＸ（ＴＭ）は、すべての特権ソフトウェア（たとえばカーネルまたはハイパーバイザなど）が悪質な可能性のあるコンピュータにおいて行われるセキュリティ極秘計算に対して完全性および機密性の保証を提供することを目的とする、インテル（Ｒ）アーキテクチャに対するハードウェア／ソフトウェア・エクステンションのセットであってもよい。信頼されるハードウェアはセキュアなコンテナを確立してもよく、リモート計算サービス・ユーザはこのセキュアなコンテナに所望の計算およびデータをアップロードしてもよい。信頼されるハードウェアは、データの計算が行われる際にデータの機密性および完全性を保護してもよい。信頼されるハードウェアをホストとするセキュアなコンテナにおいて実行されるソフトウェアの特定の部分と通信するユーザに対する認証検査も、ＳＧＸ（ＴＭ）製品によって提供される。

【００３５】

いくつかの例示的実施形態において、ＳＥＰは、セキュアかつ安全な計算およびソフトウェアの実行を提供し、かつシステムの破損、基本入力／出力システム（ＢＩＯＳ：Ｂａｓｉｃ Ｉｎｐｕｔ／Ｏｕｔｐｕｔ Ｓｙｓｔｅｍ）コード、またはプラットフォームの構成の改変などによって極秘データにアクセスすることを目的としたソフトウェアに基づく攻撃を防御するように構成された内蔵型のセキュア実行プラットフォームであってもよい。

【００３６】

クラスタ１２０の各ＳＥＰはキー１３０を保持してもよい。キー１３０は、クラスタ１２０のＳＥＰ間で共有されてもよい。キー１３０は、任意の非クラスタ・エンティティには利用不可能であってもよい。クラスタ１２０のＳＥＰは権限付与および非権限付与エージェントを実行してもよいことが注目されるだろう。クラスタ１２０のＳＥＰによって実行される権限付与エージェントのみがクラスタ・エンティティとみなされてもよい。

【００３７】

いくつかの例示的実施形態において、キー１３０はクラスタ１２０またはその一部分によって自動的に生成されてもよい。キー１３０は、クラスタ１２０のすべてのＳＥＰに転送されてもよい。クラスタ１２０の各ＳＥＰは、キー１３０を用いてデータを処理する際にデータの機密性を維持するように構成されてもよい。キー１３０は、データまたはその表現を暗号化する暗号アルゴリズムの関数出力を定めるために、ＳＥＰによって使用されてもよい。一例として、キー１３０はデータのプレーンテキスト表現をその暗号文表現に変換し、復号アルゴリズムに対してその逆も同様に変換することを指定してもよい。キー１３０は、たとえばデジタル署名スキームまたはメッセージ認証コードなどの他の暗号アルゴリズムにおける変換を指定してもよい。

【００３８】

いくつかの例示的実施形態において、キー１３０は、データの暗号化および復号の両方に用いられる対称キーとなるように生成されてもよい。付加的または代替的に、キー１３０は一対のキーを含む非対称キーであってもよく、その一方が暗号化に用いられ、他方が復

号に用いられてもよい。
【００３９】
いくつかの例示的実施形態において、キー１３０はクラスタ１２０の特定のＳＥＰ、たとえばＳＥＰ１２６などによって生成されてもよい。ＳＥＰ１２６は、キー１３０を他のＳＥＰ１２２、１２４、および１２８に分配するように構成されてもよい。ＳＥＰ１２６は、キー１３０を生成するために暗号システムを使用してもよい。
【００４０】
いくつかの例示的実施形態において、クラスタ１２０は、キー１３０の生成に応答して、キー１３０に合意するためのコンセンサス・プロトコルを使用するように構成されてもよい。いくつかの例示的実施形態において、ＳＥＰ１２６はクラスタ１２０のリーダーとして機能してもよい。リーダーは予め定められて選択されるか、ＳＥＰ間の予め規定された順序に基づいて定められるか、またはクラスタ１２０によって動的に選択されるなどしてもよい。リーダーはキー１３０を生成するように構成されてもよく、その生成されたキーが用いられる。付加的または代替的に、各ＳＥＰがキー１３０を生成できるような異なるＳＥＰの間で競争があってもよい。次いでクラスタ１２０は、たとえばコンセンサス・プロトコルを用いるなどして、生成されたキーのうちのどれをクラスタ１２０のキー１３０として用いるかを選択してもよい。付加的または代替的に、いくつかのＳＥＰがたとえば各々キー１３０の異なる部分を定めるなどして、一緒にキー１３０を生成してもよい。一例として、各ＳＥＰは２５６ビットを生成してもよく、キー１３０は４セットの２５６ビットで構成されてもよい。
【００４１】
いくつかの例示的実施形態において、システム１００はデータ・ストレージ１１０を含んでもよい。データ・ストレージ１１０は、データを保持できるコンピュータ可読ストレージを含んでもよい。いくつかの例示的実施形態において、データ・ストレージ１１０は独立ディスク冗長アレイ（ＲＡＩＤ：Ｒｅｄｕｎｄａｎｔ Ａｒｒａｙ ｏｆ Ｉｎｄｅｐｅｎｄｅｎｔ Ｄｉｓｋｓ）、ネットワーク接続ストレージ（ＮＡＳ：Ｎｅｔｗｏｒｋ Ａｔｔａｃｈｅｄ Ｓｔｏｒａｇｅ）、ストレージ・エリア・ネットワーク（ＳＡＮ：Ｓｔｏｒａｇｅ Ａｒｅａ Ｎｅｔｗｏｒｋ）、ＮｏＳＱＬもしくはＳＱＬデータベース、またはオブジェクト・ストアなどであってもよい。データ・ストレージ１１０は、キー１３０を用いて暗号化された暗号化データを保持するように構成されてもよい。いくつかの例示的実施形態において、暗号化はデータ・ストレージ１１０ではなくクラスタ１２０のＳＥＰによって行われる。
【００４２】
一例として、データ・ストレージ１１０は、ある国の国民の指紋のデジタル表現のバイオメトリック・データベースを保持してもよい。データ・ストレージ１１０内のデータは、生体認証可能な身分証明書およびパスポートの作製、政府の調査の実行、個人の識別、ならびに犯罪行為の容疑者であり得る人物の識別などに使用されてもよい。
【００４３】
いくつかの例示的実施形態において、データ・ストレージ１１０の管理者がデータ・ストレージ１１０を管理してもよい。管理者はデータ・ストレージ１１０への制限されないアクセスを有してもよい。付加的または代替的に、管理者はデータ・ストレージ１１０内の記録を作成、検索、および更新してもよい。しかし、キー１３０がないとき、管理者は復号形の極秘データにアクセスできなくてもよい。一例として、バイオメトリック・データベースは、国立のバイオメトリック・データベース管理当局の職員である管理者によって管理されてもよい。管理者は、キー１３０を有することなくバイオメトリック・データベースの管理、記録の更新、新たな記録の作成、または記録の削除などができてもよい。一例として、管理者は、データベースに構造化クエリ言語（ＳＱＬ：Ｓｔｒｕｃｔｕｒｅｄ Ｑｕｅｒｙ Ｌａｎｇｕａｇｅ）コマンドを発行するために用いられるカウンセルへの制限されないアクセスを有してもよい。しかし、管理者はキー１３０を有さないため、データ・ストレージ１１０に保持される暗号化データを復号できない。いくつかの例示的実施

形態において、管理者は、キー１３０へのアクセスを有することなくキー１３０を用いて復号可能となり得る新たな暗号化データをデータ・ストレージ１１０に導入できなくてもよい。

【００４４】

クラスタ１２０の各ＳＥＰは、データ・ストレージ１１０に接続されてもよい。いくつかのＳＥＰは、データ・ストレージ１１０へのデータの書込み、データ・ストレージ１１０からのデータの読取り、またはデータ・ストレージ１１０に対するデータの読取りおよび書込みなどを行うように構成されてもよい。いくつかの例示的実施形態においては、クラスタ１２０に含まれるＳＥＰのみがデータ・ストレージ１１０の読取りおよび書込みを可能にされてもよく、データ・ストレージ１１０はクラスタ１２０のメンバーによって行われていない任意のアクセスの試みを拒絶するように構成されてもよい。

【００４５】

いくつかの例示的実施形態において、ＳＥＰ１２２によって実行される権限付与エージェントは、キー１３０を用いてクライアント・データを暗号化して暗号化クライアント・データを得るように構成されてもよい。ＳＥＰ１２２によって実行される権限付与エージェントは、暗号化クライアント・データをデータ・ストレージ１１０に保存してもよい。データ・ストレージ１１０に保持されるクライアント・データは、任意の非クラスタ・エンティティによって取得できなくてもよい。データ・ストレージ１１０に対する書込みアクセスのみを有するＳＥＰ１２２は、ライタＳＥＰと呼ばれることがある。

【００４６】

いくつかの例示的実施形態において、ＳＥＰ１２２によって実行される権限付与エージェントは、クライアント・デバイス１４０からクライアント・データを受信したことに応答してクライアント・データを暗号化するように構成されてもよい。暗号化クライアント・データは、クライアント・デバイス１４０によって直接取得できなくてもよい。付加的または代替的に、クライアント・デバイス１４０は、データ・ストレージ１１０に保持される極秘データの一部分のみを提供してもよい。結果として、クライアント・デバイス１４０からの情報漏洩の可能性は限定されたリスクとなり、データベース全体が非権限付与エンティティによってアクセスされるリスクはもたらさない。

【００４７】

いくつかの例示的実施形態において、ＳＥＰ１２４によって実行される権限付与エージェントは、データ・ストレージ１１０から暗号化保存データを検索するように構成されてもよい。ＳＥＰ１２４によって実行される権限付与エージェントは、キー１３０を用いて暗号化保存データを復号して、暗号化保存データの非暗号化形を得るように構成されてもよい。データ・ストレージ１１０に対する読取りアクセスのみを有するＳＥＰ１２４は、リーダ（ｒｅａｄｅｒ）ＳＥＰと呼ばれることがある。

【００４８】

いくつかの例示的実施形態において、ＳＥＰ１２４によって実行される権限付与エージェントは、クライアント・デバイス１４０からアクセス・クエリを受信したことに応答して、暗号化保存データを検索および復号するように構成されてもよい。クライアント・デバイス１４０は、データ・ストレージ１１０内の保持データへのアクセスを要求してもよい。クライアント・デバイス１４０はデータ・ストレージ１１０に直接アクセスするための許可を有さないため、クライアント・デバイス１４０は、クラスタ１２０またはたとえばＳＥＰ１２４などのクラスタ１２０のＳＥＰに直接クエリを送信することによって、データ・ストレージ１１０に保存される暗号化データの指定された部分にアクセスすることを要求してもよい。クライアント・デバイス１４０がデータ・ストレージ１１０へのアクセスを有することなく、ＳＥＰ１２４によって実行される権限付与エージェントがデータ・ストレージ１１０から関連保持データの暗号化形を検索し、キー１３０を用いて暗号化形を復号し、非暗号化データをクライアント・デバイス１４０に提供してもよい。当然のことながら、たとえクライアント・デバイスがデータ・ストレージ１１０へのアクセスを有すると仮定しても、クライアント・デバイスはキー１３０を有することができないため、

クライアント・デバイスは保存データを復号できないだろう。
【００４９】
いくつかの例示的実施形態において、たとえばＳＥＰ１２２などの同じＳＥＰが、データの暗号化および復号の両方を行うために使用されてもよい。付加的または代替的に、たとえばＳＥＰ１２２などのいくつかのＳＥＰはデータ・ストレージ１１０への書込み専用のアクセス許可を有してもよく、たとえばＳＥＰ１２４などの他のものはデータ・ストレージ１１０への読取り専用のアクセス許可を有してもよい。
【００５０】
いくつかの例示的実施形態において、クライアント・デバイス１４０は、たとえばパーソナル・コンピュータ、ラップトップ、またはモバイル・デバイスなどの非ＳＥＰデバイスであってもよい。クライアント・デバイス１４０は人間のユーザによって、たとえばクエリの使用または専用のユーザ・インタフェースの使用などによってデータ・ストレージ１１０にアクセスするために用いられてもよい。いくつかの例示的実施形態において、クライアント・デバイス１４０は、ユーザ入力に基づいてクエリを生成するためのウェブに基づくユーザ・インタフェースを提供し、かつクラスタ１２０にそのクエリを発行するように構成されたサーバであってもよい。
【００５１】
当然のことながら、クライアント・デバイス１４０はＳＥＰ１２２または別のＳＥＰに直接接続されてもよいし、されなくてもよい。いくつかの例示的実施形態において、クライアント・デバイス１４０は、クラスタ１２０のゲートウェイ・デバイス（図示せず）によって受信されるクエリを発行してもよい。ゲートウェイ・デバイスはそれに応答して、たとえば負荷バランシングの考慮、ＳＥＰのアクセス許可、またはクエリのタイプなどに基づいて、そのクエリを取り扱うクラスタ１２０のＳＥＰを選択してもよい。場合によっては、いくつかのＳＥＰが特定のタイプのクエリを取り扱うことが演繹的に指定されていてもよく、クラスタ１２０はクエリを適切なＳＥＰに経路付けるように構成されてもよい。
【００５２】
バイオメトリック・データベースの例を参照して、内務省の職員は、国民からバイオメトリック識別データを集め、そのデータをバイオメトリック・データベース（例、１１０）に移すために権限付与されるだろう。内務省の職員は、たとえばクライアント・デバイス１４０などのデバイスを用いて、バイオメトリック・データベースにデータを加える更新または挿入クエリを発行してもよい。クエリはＳＥＰ１２２によって受信されてもよく、ＳＥＰ１２２はキー１３０を用いてデータを暗号化し、その暗号化データをバイオメトリック・データベースに保存してもよい。一旦データが暗号化されると、職員は決してキー１３０に露出されないため、職員はバイオメトリック・データベースからデータを抽出することができなくてもよい。
【００５３】
他方で、バイオメトリック・データベースに保存されるデータは、居住者識別文書の発行または個人の身元の確認などのために用いられてもよい。たとえば警察官または治安当局の職員などの権限付与されたメンバーが、個人のバイオメトリック識別データの再チェックを要求してもよい。それを行うために、権限付与されたメンバーはクライアント・デバイス１４０を用いてもよく、自身の許可に基づいて、クラスタ１２０のたとえば１２４などのＳＥＰにアクセス・クエリを送ることができてもよい。ＳＥＰはキー１３０を有してもよく、したがって関連する暗号化された個人のバイオメトリック識別データを検索し、暗号化された個人のバイオメトリック識別データを復号し、バイオメトリック識別データを処理して、クライアント・デバイス１４０を介して権限付与されたメンバーに処理結果を提供することができてもよく、ここで権限付与されたメンバーはキー１３０を知ることも、バイオメトリック・データベースへの直接アクセスを有することもない。いくつかの例示的実施形態において、ユーザの許可に基づいて、ユーザは特定のタイプのクエリの実行または異なる粒度のデータの受信などが制限されてもよい。一例として、ある職員は新たなデータの挿入のみができてもよく、一方で他の職員は特定の人々に関する個別のデー

タを検索するために権限付与されていてもよい。さらに他の職員は確認プロセスへのアクセスを有してもよく、この確認プロセスは、たとえばバイオメトリック読取りを得てそれをＳＥＰに送信し、次いでＳＥＰがそれを保存されたバイオメトリック・データに対して確認することなどによって、職員をバイオメトリック情報自体に露出させることなくバイオメトリック情報の正しさを確認する。さらに他の職員は、限定数のクエリを発行するために権限付与されてもよい。

【００５４】

いくつかの例示的実施形態において、クラスタ１２０のＳＥＰは、たとえばクラスタ１２０の一部ではない他のＳＥＰなどの任意の非クラスタ・エンティティ、または任意の他の装置にキー１３０を転送することを可能にされなくてもよい。ＳＥＰは、自身のユーザ・インタフェースにおいてキー１３０を示したり、別様に人間のユーザにキー１３０を提供したりしないようにプログラミングされてもよい。クラスタ１２０のＳＥＰおよびそれによって実行されるその他の非権限付与エージェントのユーザは、ＳＥＰへのアクセスを有していてもキー１３０を得ることができなくてもよい。

【００５５】

いくつかの例示的実施形態において、ＳＥＰ１２８は、たとえば新たなＳＥＰ１２９などの新たなＳＥＰをクラスタ１２０に加えるように構成されてもよい。増加クラスタ１２０ｂが定められてもよい。ＳＥＰ１２８は、増加クラスタ１２０ｂを形成するときにクラスタ１２０に新たなＳＥＰ１２９を加えるプロセスの一部として、セキュアな通信チャネルを通じて新たなＳＥＰ１２９にキー１３０を転送するように構成されてもよい。ＳＥＰ１２８はグロワーＳＥＰと呼ばれることがある。

【００５６】

いくつかの例示的実施形態において、たとえばグロワーＳＥＰなどの別のエンティティにキー１３０を転送する任意のＳＥＰは、キーを転送する前にその新たなＳＥＰが確かに権限付与エージェントを実行するＳＥＰであることを認証を用いて確認してもよい。新たなＳＥＰは、送られたキーを受け入れる前に、グロワーＳＥＰが確かに権限付与エージェントを実行するＳＥＰであることを認証を用いて確認してもよい。

【００５７】

いくつかの例示的実施形態において、新たなＳＥＰ１２９は任意のコンピュータ装置にキー１３０を転送することを禁じられてもよい。いくつかの例示的実施形態において、新たなＳＥＰ１２９自体はグロワーＳＥＰにならなくてもよく、結果として増加クラスタ１２０ｂのサイズの増加を続けられなくてもよい。

【００５８】

いくつかの例示的実施形態において、ＳＥＰ１２８は新たなＳＥＰ１２９に対して、たとえば数分間、１時間、または１日などの予め定められた寿命を設定するように構成されてもよい。新たなＳＥＰ１２９は、予め定められた寿命の最後にクラスタ１２０ｂから除去されるように構成されてもよい。新たなＳＥＰは、自身で自動的にクラスタを出るか、またはたとえばＳＥＰ１２８もしくはクラスタ１２０の別の管理デバイス（図示せず）などの別のデバイスによって増加クラスタ１２０ｂから除去されるなどするように構成されてもよい。いくつかの例示的実施形態において、新たなＳＥＰ１２９は、増加クラスタ１２０ｂを出るときに自身が保持するキー１３０のコピーを削除またはパージするように構成されてもよい。

【００５９】

いくつかの例示的実施形態において、ＳＥＰ１２８は、クラスタ１２０内のＳＥＰの数がたとえば２、３、または１０などの予め規定された閾値未満であることに応答して、クラスタ１２０に新たなＳＥＰ１２９を加えるように構成されてもよい。いくつかの例示的実施形態においては、たとえばキー１３０のすべてのコピーを失う可能性を減らすなどのために、最小限の数のＳＥＰを維持することが望ましくてもよい。ＳＥＰの数が最小閾値に達するとき、キー１３０の十分な数のコピーが共存することを確実にするために、グロワーＳＥＰはクラスタ１２０に加えられる新たなＳＥＰの生成を開始するように構成されて

もよい。
【００６０】
付加的または代替的に、ＳＥＰ１２８は、ＳＥＰ１２２またはＳＥＰ１２４が非動作的になったことに応答してクラスタ１２０に新たなＳＥＰ１２９を加えるように構成されてもよい。新たなＳＥＰ１２９は、非動作的ＳＥＰと置き換わるように構成されてもよい。いくつかの例示的実施形態において、新たなＳＥＰ１２９の寿命は、非動作的ＳＥＰが再び動作的になるまでに十分であると推定される予め定められた寿命に限定されてもよい。
【００６１】
当然のことながら、場合によってはたとえばＳＥＰ１２２、ＳＥＰ１２４、またはＳＥＰ１２６などの他のＳＥＰが、クラスタ１２０またはクラスタ１２０ｂに新たなＳＥＰを加えることができてもよい。たとえば新たなＳＥＰ１２９などの新たなＳＥＰは、デフォルトで、増加クラスタ１２０ｂに新たなＳＥＰを加えることを禁じられていてもよい。しかし場合によっては、たとえば新たなＳＥＰ１２９が増加クラスタ１２０ｂのバックボーンの一部になった場合、またはグロワーＳＥＰが非動作的になった場合などに、クラスタ１２０の管理者が新たなＳＥＰ１２９に新たなメンバーを加えることを許可してもよい。いくつかの例示的実施形態において、管理者はＳＥＰの寿命を元の予め定められた寿命よりも延長する許可を有してもよい。
【００６２】
ここで、主題のいくつかの例示的実施形態による方法の流れ図を示す図２を参照する。
【００６３】
ステップ２１０において、クライアント・データが受信されてもよい。いくつかの例示的実施形態において、クライアント・データは、コンピュータ環境内でたとえば図１の１２２などのＳＥＰによって受信されてもよい。ＳＥＰは、たとえば図１の１１０などのデータ・ストレージとの接続性を有する、たとえば図１の１２０などのＳＥＰのクラスタのメンバーであってもよい。データ・ストレージは、キーを用いて暗号化された暗号化データを保持してもよい。キーは、クラスタのＳＥＰ間で共有されてもよい。前記クラスタの各ＳＥＰは、キーを用いてデータを処理する際にデータの機密性を維持するように構成されてもよい。
【００６４】
いくつかの例示的実施形態において、クライアント・データは、たとえば患者のプロフィル、医療情報、国家のセキュリティ・データ、担保付き支払い方法のデータ、金融記録、または機密データなどの極秘データを含んでもよい。極秘データは、将来の使用のためにセキュアなデータ・ストレージ内に内密に保存されることが望まれてもよい。
【００６５】
いくつかの例示的実施形態において、クライアント・データは、たとえば図１の１４０などのクライアント・デバイスから受信されてもよい。クライアント・デバイスは、たとえばサーバまたはコンピュータ装置などの非ＳＥＰデバイスであってもよい。クライアント・デバイスは、人間のユーザによって動作されてもよいし、されなくてもよい。クライアント・デバイスは、ユーザが発行されるべきクエリを規定することを可能にしてもよい。クエリは、新たなデータを導入するか、またはデータ・ストレージ内に存在する記録を更新する書込みクエリであってもよい。クライアント・デバイスによって実行されるネイティブ・プログラム、ユーザ・デバイスによって実行されるときにグラフィカル・ユーザ・インタフェース（ＧＵＩ：Ｇｒａｐｈｉｃａｌ　Ｕｓｅｒ　Ｉｎｔｅｒｆａｃｅ）を表示し、かつクエリをクライアント・デバイスに転送するプログラム、またはクライアント・デバイスによって実行されて、たとえばウェブ・ブラウザを実行するコンピュータなどのユーザ・デバイスを用いてユーザにアクセス可能であるウェブに基づくインタフェースなどを用いて、クエリが規定されてもよい。クライアント・デバイスはキーへのアクセスを有することも、こうしたキーを保持することもなくてよい。いくつかの例示的実施形態において、クライアント・デバイスはデータ・ストレージへの直接アクセスを有さなくてもよい。

【００６６】
いくつかの例示的実施形態において、クライアント・デバイスはクライアント・データをＳＥＰに直接提供してもよい。付加的または代替的に、クライアント・デバイスはクラスタのゲートウェイにコンタクトしてもよく、ゲートウェイはクライアント・デバイスからの通信を処理のための目標ＳＥＰ（単数または複数）に向かわせてもよい。
【００６７】
ステップ２１５において、キーを用いてクライアント・データが暗号化されて、暗号化クライアント・データが得られてもよい。クライアント・データは、キーを有するＳＥＰのみがそれを復号できるようなやり方でコード化されてもよい。いくつかの例示的実施形態において、ステップ２１５は、ＳＥＰによって実行される権限付与エージェントによって行われてもよい。
【００６８】
いくつかの例示的実施形態において、クライアント・データは、暗号化アルゴリズムを用いて暗号化されてもよい。キーは暗号化アルゴリズムの一部であるか、または暗号化アルゴリズムのパラメータなどであってもよい。ＳＥＰは、キーを用いて暗号化クライアント・データを復号できてもよい。
【００６９】
ステップ２２０において、暗号化クライアント・データはデータ・ストレージに保存されてもよい。
【００７０】
ここで、主題のいくつかの例示的実施形態による方法の流れ図を示す図３を参照する。
【００７１】
ステップ２３０において、たとえば図１の１２４などのＳＥＰによって、クライアント・クエリが受信されてもよい。ＳＥＰは、データ・ストレージとの接続性を有するＳＥＰの、たとえば図１の１２０などのクラスタのメンバーであってもよい。データ・ストレージは、たとえばステップ２２０において保存された暗号化クライアント・データなどの、キーを用いて暗号化された暗号化データを保持してもよい。
【００７２】
いくつかの例示的実施形態において、クエリは、たとえば図１の１４０などのクライアント・デバイスによって得られるべき保存データの部分を規定してもよい。付加的または代替的に、クエリは自身に基づく結果をクライアント・デバイスに提供する前に、処理のためにＳＥＰによって得られるべき保存データの部分を規定してもよい。
【００７３】
ステップ２３５において、ＳＥＰによってデータ・ストレージがアクセスされてもよい。いくつかの例示的実施形態において、データ・ストレージはクラスタのＳＥＰのみによってアクセス可能であってもよい。ＳＥＰは、クエリを実現するために関係する暗号化データを検索してもよい。
【００７４】
ステップ２４０において、データ・ストレージから検索された暗号化データは、ＳＥＰによってキーを用いて復号されてもよい。暗号化データは、そのＳＥＰまたはクラスタからの異なるＳＥＰによって、キーを用いて過去に暗号化されていてもよい。復号によって、暗号化データの非暗号化形が得られてもよい。いくつかの例示的実施形態において、ステップ２４０は、ＳＥＰによって実行される権限付与エージェントによって行われてもよい。
【００７５】
ステップ２４５において、クエリが実現されてもよい。ＳＥＰは、クエリを実現して関連情報をクライアント・デバイスに提供するために、暗号化データの非暗号化形を使用してもよい。いくつかの例示的実施形態において、クエリは、極秘データ自体をクライアント・デバイスに露出することなく、たとえば権限付与エージェントなどによって、ＳＥＰでオンボードで行われる極秘データの処理を必要としてもよい。処理が完了してから、処理の結果（例、ＰＡＳＳ／ＦＡＩＬ結果）を戻すことによって、クエリが実現されてもよい

。付加的または代替的に、クエリは、たとえば極秘データを保持する記録のあるフィールドの内容などの、極秘データの一部分を提供することを要求してもよい。こうした場合、クライアント・デバイスには、最終的にデータ・ストレージに保持される極秘データの一部分が提供されてもよい。クライアント・デバイスがデータ・ストレージへの直接アクセスを有することも、その中に保持される暗号化データを復号する独立の方式を有することもなく、クエリが実現されてもよい。

【００７６】

ここで、主題のいくつかの例示的実施形態による方法の流れ図を示す図４を参照する。

【００７７】

ステップ２５０において、キーが自動的に生成されてもよい。いくつかの例示的実施形態において、キーはＳＥＰのクラスタによって生成されてもよい。

【００７８】

いくつかの例示的実施形態において、キーはクラスタの１つまたはそれ以上のＳＥＰによって生成されてもよい。一例として、複数のＳＥＰの各々がキーの異なる部分を生成することによって一緒にキーを生成してもよく、たとえばそれらの異なる部分を連結することなどによってそれらがともに組み合わされてキーを作成してもよい。別の例として、単一のＳＥＰがキーを生成してもよい。

【００７９】

ステップ２５５において、キーに対して合意するために、クラスタによってコンセンサス・プロトコルが使用されてもよい。コンセンサス・プロトコルは、さまざまなＳＥＰが共通のキーに対して合意することを可能にしてもよい。いくつかの例示的実施形態において、ＳＥＰの各々がキーの候補値を生成し（例、ステップ２５０）、互いに通信して、キーに対する単一のコンセンサス値に合意してもよい。付加的または代替的に、コンセンサス・プロトコルはステップ２５０において生成された単一の候補キーに対して使用され、コンセンサス値に達するまで反復的に繰り返されて反復ごとに新たな候補キーを生成してもよい。

【００８０】

いくつかの例示的実施形態において、コンセンサス・プロトコルは、クラスタに対するキーを指示するリーダーＳＥＰに合意するために適用されてもよい。付加的または代替的に、コンセンサス・プロトコルは、ＳＥＰの過半数またはその他の定数がキーに対して合意することに基づいてもよい。

【００８１】

いくつかの例示的実施形態において、コンセンサス・プロトコルは、設定の際にＳＥＰに提供されるＳＥＰではない１またはそれ以上の管理者によって実行されてもよい。

【００８２】

いくつかの例示的実施形態において、コンセンサス投票に基づいて、クラスタはクラスタによって用いられるキーに合意してもよい。いくつかの例示的実施形態において、この決定は取り消し不能であってもよい。付加的または代替的に、クラスタは第２のキーに合意することによって、キーを変えることを定期的に決定してもよい。極秘データはキーを用いて復号され、再び保存される前に第２のキーを用いて暗号化されてもよい。

【００８３】

ステップ２６０において、キーはクラスタのすべてのメンバーに分配されてもよい。いくつかの例示的実施形態において、キーはリーダーＳＥＰによって、またはコンセンサス・プロトコルを適用するステップの一部としてメンバーに分配されてもよい。リーダーＳＥＰは、すでにキーを保持していないクラスタの各ＳＥＰにキーを転送するように構成されてもよい。いくつかの例示的実施形態においては、コンセンサス・プロトコルの際にすでにＳＥＰにキーが通知されているため、分配は必要ない。

【００８４】

ステップ２６５において、データの機密性を維持するためにキーが用いられてもよい。キーは、データを処理する際にデータの機密性を維持するためにクラスタのＳＥＰによって

使用されてもよい。キーは任意の非クラスタ・エンティティには利用できなくてもよく、ＳＥＰは任意の非ＳＥＰデバイスおよびクラスタの新たなメンバーではないＳＥＰデバイスにキーを分配することを禁じられてもよい。

【００８５】

いくつかの例示的実施形態において、キーは、データをデータ・ストレージに保存する前に暗号化し、かつデータを使用する前に暗号化データを復号するために用いられてもよい。

【００８６】

ここで、主題のいくつかの例示的実施形態による方法の流れ図を示す図５を参照する。

【００８７】

ステップ２７０において、クラスタのメンバーの数が予め定められた閾値未満であると判断されてもよい。予め定められた閾値は、たとえば約２、約３、または約１０などであってもよい。いくつかの例示的実施形態において、予め定められた閾値はクラスタの目標サイズに関連してもよく、たとえば所望の最適サイズの約４０％などであってもよい。いくつかの例示的実施形態において、予め定められた閾値は、最小絶対サイズと最小相対サイズとの組み合わせであってもよい。

【００８８】

いくつかの例示的実施形態において、閾値は、クラスタのすべてのＳＥＰの機能不全をもたらしてキーを失う可能性のある大災害のリスクの可能性に関係してもよい。いくつかの例示的実施形態において、閾値はＳＥＰの所望の冗長性を提供してもよい。付加的または代替的に、閾値は、ＳＥＰがたとえば少なくとも３つの異なる場所などの異なる地理的位置に分散されることを要求してもよい。付加的または代替的に、閾値は、すべてのＳＥＰが同時に機能不全を起こすリスクを減らすリスク因子に関係してもよい。

【００８９】

付加的または代替的に、その判断は、クラスタのＳＥＰが非動作的になったという判断であってもよい。結果として、クラスタの非動作的ＳＥＰの代わりに新たなＳＥＰを加えることが望まれてもよい。

【００９０】

ステップ２７５において、クラスタに新たなメンバーが加えられてもよい。新たなメンバーはＳＥＰであってもよい。いくつかの例示的実施形態において、新たなＳＥＰは、クラスタ内にすでに存在するＳＥＰと同じタイプのＳＥＰであってもよい。

【００９１】

いくつかの例示的実施形態において、新たなメンバーは、グロワーＳＥＰによってクラスタに加えられてもよい。グロワーＳＥＰは、クラスタに新たなメンバーを加えるように構成されたクラスタのメンバーであってもよい。グロワーＳＥＰは、ステップ２７０の判断に応答して新たなメンバーを加えるように構成されてもよい。グロワーＳＥＰは、クラスタの一部になったときに新たなＳＥＰによって使用されるべき、新たなＳＥＰにロードされるべきソフトウェアを送ってもよい。当然のことながら、新たなメンバーを加えるタスクに加えて、グロワーＳＥＰはデータ・ストレージへの書込み、そこからの読取り、またはそれらの組み合わせを行う際に、データを処理するように構成されてもよい。

【００９２】

付加的または代替的に、新たなメンバーはクラスタの任意の元のメンバーによって加えられてもよい。クラスタの元のメンバーは、クラスタが最初に生成されたときにクラスタに加えられたＳＥＰであってもよい。元のメンバーは、クラスタに新たなメンバーを加えること、または新たなＳＥＰにキーを転送することなどに対する許可を有してもよい。たとえば新たなメンバーなどの、元からのものでないＳＥＰは、新たなメンバーを加えることを許可されてもよいし、されなくてもよい。

【００９３】

いくつかの例示的実施形態において、新たなメンバーは一時的なメンバーであってもよい。グロワーＳＥＰは、新たなメンバーに対する予め定められた寿命を設定するように構成されてもよい。新たなメンバーは、予め定められた寿命の最後にクラスタから除去される

ように構成されてもよい。予め定められた寿命は１０分間、１時間、１０時間、または１日などに設定されてもよい。予め定められた寿命は新たなメンバーを加える理由に基づいて設定されてもよく、一例として、たとえば作業負荷サージの際に新たなデータを加えるなどの特定のタスクを行うために新たなメンバーが加えられた場合は、新たなＳＥＰが新たなデータを加えるために十分であるように予め定められた寿命が設定されてもよい。別の例として、非動作的ＳＥＰと置き換えるために新たなＳＥＰが加えられる場合は、予め定められた寿命は非動作的ＳＥＰの回復の予想時間に基づいてもよい。

【００９４】

ステップ２８０において、新たなメンバーにキーが転送されてもよい。新たなメンバーは、キーを用いてデータを処理する際にデータの機密性を維持するように構成されてもよい。新たなメンバーは、キーを任意の非クラスタ・エンティティに出力すること、またはキーをクラスタの一部ではない任意のデバイスに転送することを禁じられてもよい。

【００９５】

いくつかの例示的実施形態において、メンバーは、クラスタの管理者によって加えられてもよい。グロワーＳＥＰは、新たなメンバーにキーを提供するように構成されてもよい。

【００９６】

いくつかの例示的実施形態において、グロワーＳＥＰはキーを転送する前に、新たなメンバーがクラスタに加えられることを許容できる権限付与ＳＥＰであることを確認するように構成されてもよい。グロワーＳＥＰは、新たなメンバーが権限付与エージェントを実行しているかどうかをチェックしてもよい。付加的または代替的に、新たなメンバーはキーを受け入れる前に、たとえば認証などに基づいてグロワーＳＥＰが権限付与エージェントを実行するＳＥＰであることを確認するように構成されてもよい。

【００９７】

いくつかの例示的実施形態において、新たなメンバーは、グロワーＳＥＰ、クラスタの管理者、または新たなメンバーを加えた任意の他のＳＥＰによって提供された許可に基づいて、たとえばクラスタに接続されたデータ・ストレージへの書込みまたはそこからの読取りなどのためにキーを用いるように構成されてもよい。新たなメンバーは、キーを用いてクライアント・データを暗号化して暗号化クライアント・データを得て、その暗号化クライアント・データをデータ・ストレージに保存するように構成されてもよい。付加的または代替的に、新たなメンバーは、前記データ・ストレージから暗号化保存データを検索し、キーを用いて暗号化保存データを復号して、暗号化保存データの非暗号化形を得るように構成されてもよい。なお、新たなメンバーは、たとえばデータ・ストレージに対する書込み専用または読取り専用のアクセス許可を有することなどによって、特定の活動を行うように制限されてもよい。

【００９８】

ステップ２８５において、新たなメンバーの予め定められた寿命が到達されたと判断されてもよい。いくつかの例示的実施形態において、この判断はグロワーＳＥＰによって行われてもよい。付加的または代替的に、この判断は新たなメンバーによって行われてもよい。

【００９９】

ステップ２９０において、クラスタから新たなメンバーが除去されてもよい。いくつかの例示的実施形態において、新たなメンバーがステップ２８５において予め定められた寿命が到達されたと判断したことに応答して、新たなメンバーはキーをパージしてクラスタから出てもよい。いくつかの例示的実施形態においては、新たなメンバーがキーをパージすることに依拠する代わりに、たとえば図４に関して示したとおり、代替的なキーが定められて用いられてもよい。

【０１００】

実施形態

開示される主題の実施形態が実現された。この実施形態ではすべての極秘データが、インテル（Ｒ）のＳＧＸ（ＴＭ）エンクレーブ（Ｅｎｃｌａｖｅｓ）の内側で実行されるソフトウェアのみに知られるキーによって暗号化された。エンクレーブは、暗号化データに対

するすべての計算を実行するインテル（Ｒ）Ｓｋｙｌａｋｅ（ＴＭ）プロセッサにおける特殊な計算モードである。リモート認証能力（コードおよびプラットフォーム確認機構）と結合して、エンクレーブはすべてのデータ関係の動作を実行するための所望のロボットの働きをし得る。この実施形態は、暗号化データに対するキーがエンクレーブの内側で実行される権限付与エージェントの内側にのみ存在するために、暗号化データはエンクレーブを介してアクセスされたときにのみ有用となり得ることを確実にする。ある意味で、この実施形態は特権管理者およびソフトウェア環境を、セキュアな実行環境で実行されるロボット・コードで置き換えるものである。

【０１０１】

この実施形態において、もし永続的なハードウェアの故障によって暗号化キーが失われれば、データは無益なものとなる。この実施形態は、単一のエンクレーブではなく、同じ秘密の暗号化キーを共有するエージェントのクラスタを実行する。このことはキーの耐久性を確実にすると同時に、データ・サービスのスケーラビリティ達成の助けとなる。

【０１０２】

ここで、実施形態の概略図を示す図６を参照する。

【０１０３】

この実施形態は、「ＡＥキー」と呼ばれる秘密キーを共有するエンクレーブ・エージェントの集合を含む。たとえば４１０、４１２、４１４などのエージェントは、一般的にオン・プレミスまたはクラウド内で実行され得る。それらのエージェントがエンクレーブにおいて実行されるという事実は、それらが信頼される環境または信頼されない環境で実行されていても、それらのセキュリティを確実にする。この実施形態は、これらのエージェントをコア（ｃｏｒｅ）エージェント（「Ｃ」、たとえば４１０など）、リーダ（ｒｅａｄｅｒｓ）（「Ｒ」、たとえば４１４など）、およびライタ（ｗｒｉｔｅｒｓ）（「Ｗ」、たとえば４１２など）に分類する。コア・エージェントは、ＡＥキーを活動させ続けてこのキーをリーダおよびライタに提供することの責任を負う。このように、いくつかの物理的位置またはデータ・センタにコアを分散させて、通常は各々の位置に少数のコア・エージェントを伴うことが賢明である。リーダおよびライタは、目下の作業負荷を取り扱うために要求に応じて作成されるべきである。このように、コア・エージェントの数は不変のままでよくバランスが取れているのに対し、リーダおよびライタは作業負荷の特徴によって変動することが予期される。図６は、３つの異なる物理的位置４２０、４２２、４２４におけるエージェントの推奨される配置の例を示す。

【０１０４】

この実施形態の設計は、エージェント・エンクレーブの内側で行われる活動を最小化し、可能なときはいつも非セキュア・コンピュータ・ノードに責任をリレーすることを試みている。ストレージ４３０はこの主要な例であり、ここでエージェントは共有ストレージに暗号化データを書込み、共有ストレージはさまざまな配置場所にわたる利用可能性および信頼性を提供する。これはオブジェクト・ストレージ、または内蔵型の複製を伴うクラスタ化ファイルシステム、ＮｏＳＱＬデータベース、または複製を伴う標準的データベースであり得る。

【０１０５】

認証サービス４４０は、エンクレーブ・コードとシステム内のさまざまなエンティティとインテル（Ｒ）認証サービス（ＩＡＳ（ＴＭ）：Ｉｎｔｅｌ（Ｒ）Ａｔｔｅｓｔａｔｉｏｎ　Ｓｅｒｖｉｃｅ）との中間段階であり、ここではＳＧＸ（ＴＭ）ハードウェア確認が実際に行われる。この実施形態の設計は、一旦エンクレーブが作成されると、それに対するリモート認証が行われて公的に確認可能なレポート（ＭＲＥＮＣＬＡＶＥの値によって表されるエンクレーブ・アイデンティティを含む）ならびに認証および通信のための特定のエンクレーブ・パブリック・キーを生成することを要求する。一旦この確認レポートが公表されると、それはさまざまなエンティティがエンクレーブの妥当性を確認してそれによって新たなセキュアな通信チャネルを作成するための手段の役割をする。

【０１０６】

管理４５０は、クラスタの最初の開始ならびに利用可能性および耐久性に対するクラスタのスケーリングの両方に対するエージェント・ノードの作成（および終了）を含むクラスタ全体の編成を担当する。管理４５０を構成する主要なサブコンポーネントは２つある。オーケストレータ４５２サブコンポーネントは、新たなエージェントの作成および冗長または機能不全エージェントの終了を含む実際の動作の駆動を担当する。これらの動作は手動で取り扱われ得るが、この実施形態においてはエージェント内で自動ＤｅｖＯｐｓ機構が実現される。新たなエージェントが作成された後、それらが複数の管理者によって承認されて登録されるまで、それらの新しいエージェントは完全に機能的にならない。登録は第２のサブコンポーネントである掲示板４５４において行われ、掲示板４５４はクラスタの決定的状態の役割をする認証レジストリである。掲示板４５４におけるこのエージェント情報は、公的クライアントおよび実際のエージェント・エンクレーブの両方による消費のために公開される。掲示板４５４の主要データは、さまざまなエージェントのリスト、それらの役割、パブリック・キー、および認証レポートを含むクラスタ構成を含む。

【０１０７】

クライアント・アイデンティティ管理（ＩｄＭ：Ｉｄｅｎｔｉｔｙ Ｍａｎａｇｅｍｅｎｔ）４６０は、ＩＴ組織がどのようにユーザ・アイデンティティおよびそれらの特権を規定するかに対処する管理コンポーネントである。我々のシステムにおいて、ＩｄＭ４６０は、クライアント・エンティティおよびあるエンティティが何の許可またはアクセス権を有するかを規定する責任を負う。バイオメトリックＤＢ使用の場合、クライアントは国境管理職員またはキオスクであってもよい。健康管理サービスなどのアクセス制御中央使用の場合、これは各職員がどの情報を検索する資格を有するかに関する厳格なポリシーを伴う健康管理職員のクレデンシャルであり得る。リーダおよびライタの役割は、ＩｄＭ４６０によって述べられるポリシーを実施することである。なお、こうしたシナリオにおいて、ＩｄＭ４６０はチェーンにおける弱いリンクとなり、攻撃を受けやすくなり得る。この実施形態の設計は、たとえ管理者がデータに自由にアクセスするためのツールを有しているときでも、このデータ・アクセスは検出されないものではなく、少なくともオーディット・トレイルを有する状況を作ることを試みるものである。

【０１０８】

設定において、ＩｄＭ４６０を保護するための付加的な方策を用いることができる。たとえば、クライアントおよびプロパティのリストがあまり動的でない場合、それらはセキュアな方式でエージェントに配達されて、それらを用いる前にそこで監査され得る。加えて、いくつかのキー・クレデンシャルは、この情報のタンパリングを防ぐためにエージェント・コードにハードコード化されていてもよい。最後に、たとえば単独の個人が単一の日に抽出できるデータの量に対する厳格な制限を設ける（かつ、別様には特権を与えられたユーザによる疑わしい挙動にフラグを立てる）などのために、いくつかの厳格なルールが与えられて常に実施され得る。

【０１０９】

クライアント４７０は、この実施形態によって管理されているデータのユーザである（例、国境管理キオスクまたは健康管理シナリオにおける医師／研究所）。クライアント４７０は、エージェントのパブリック・キーに基づいてセキュアな通信チャネル（例、セキュア・ソケット・レイヤー（ＳＳＬ：Ｓｅｃｕｒｅ Ｓｏｃｋｅｔｓ Ｌａｙｅｒ））を介してリーダおよびライタと対話する。それらのクライアントがどのように配置され、どのシステムおよびどの言語で実現されるかは限定されない。

【０１１０】

実行中のクラスタにおいて、クライアント４７０はリーダおよびライタ・エージェント（例、４１４、４１２）によって扱われ、それらのエージェントのリストは掲示板４５４を介してアクセスされ得る。（掲示板４５４を信頼せずに）リーダ／ライタのアイデンティティをさらに確認することを望むクライアントは、掲示板４５４において公開されている対応のエンクレーブの認証レポートを確認することによって、それを行ってもよい。次いでクライアント４７０は、リーダ／ライタによってＳＳＬセッション（または代替的なセ

キュア通信チャネル）を開き、それを通じて自身の入力を送る。エージェントはセキュアな部分とセキュアでない部分とでできている。標準的なプロセスとして実行されるセキュアでない部分は、エンクレーブにおいて実行されるセキュアな部分とのすべての通信を取り扱う。クライアントとのすべての対話において、最初のステップは、このクライアントが要求するタスクを行うために十分な特権を有するかどうかを確認することである。この確認はＩｄＭ４６０からの情報に基づく。

【０１１１】

特権が確立されてから、リーダまたはライタは自身のそれぞれのタスクを行って、セキュアなチャネルを通じて応答を戻し得る。なお、応答のロジックはかなり複雑であってもよく、きめ細かいアクセス制御ポリシーを含み得る。たとえば、リーダは（何らかのパラメータＸに対する）Ｘクエリのみに応答できるか、または何らかのデータ依存性のルールが満たされたときにのみ応答できる。

【０１１２】

リーダおよびライタは、オーケストレータ４５２による要求に応じて生成される。それらは認証されて掲示板４５４に挿入される。掲示板４５４において可視になると、それらは開始され、掲示板４５４に従ってそれらの役割が確認され、それらはコア・エージェントの１つ（例、４１０）から秘密キーのＡＥキーを受信する。初期設定の際に、それらは自身の時間リースを規定する制限時間を保存する（このために、インテル（Ｒ）ＳＧＸ（ＴＭ）ＳＤＫにおいて提供されるｓｇｘ＿ｇｅｔ＿ｔｒｕｓｔｅｄ＿ｔｉｍｅ関数が用いられてもよい）。リーダおよびライタは時間制限されており、自身のリースの経過後にそれらは自滅する（かつＡＥキーを消去する）か、または自身のリースを延長するべきである。一般的に、セキュアな部分は受動的であってクロックに基づく動作を駆動できないため、リーダのリースの延長はエージェントのセキュアでない部分によって駆動されるべきである。しかし、このコードは信頼できないため、この実施形態はクライアントの要求取り扱いコードの内側にリース検証ステップを加えることによって、エンクレーブはそのリースが経過したかどうかを知るためにローカル・クロックをテストして、もしそうであればさらなる要求を拒否する。もしセキュアでない部分が正しく動作していれば、エンクレーブは時間制限が理由でクエリを拒絶しないだろう。時間リースの延長を実現するためのいくつかの選択肢が存在し、最も単純なものはリーダ／ライタ・エージェントが管理掲示板においてまだ有効かどうかをチェックし、もしそうであればエージェントのセキュア部分に新たなリースをセットアップすることである。

【０１１３】

クラスタの開始は最も脆弱な段階の１つであり、たとえば悪質コード投入、分割クラスタまたはシャドー・エンクレーブの作成などのさまざまな攻撃を受けやすい。この感受性のために、この実施形態はクラスタ開始に対する注意深いアプローチを取ることによって、完全に成功したセットアップのみが許容可能となり、任意の失敗はプロセスの完全な中断およびスクラッチからの再スタートをもたらす。クラスタは、このプロセスが完了してリード（ｌｅａｄ）コア・エージェントによって確認された後に初めて書込みおよび読取りに対して動作的となり、データが投入される。エージェント・エンクレーブの内側で複雑なリーダー選挙コードを実施するのではなく、このプロセスは管理レベルで取り扱われ、掲示板４５４において公表される。管理４５０は、コア・エージェントのリストおよび指定されたリーダーを含むクラスタ構成に合意し、以下の段階においてセットアップを開始する。

【０１１４】

（１）エージェント・エンクレーブの作成。エージェントをホストする各ノードにおいて、エージェント・コードがアップロードされてエンクレーブが生成される。この段階において、エージェントは自身が消費することとなる情報を確認する能力に対して決定的であるいくつかの重要なパブリック・キーを得る。具体的には、すべての認証レポートを確認するためにインテル（Ｒ）Ｒｅｐｏｒｔ Ｓｉｇｎｉｎｇ Ｐｕｂｌｉｃ Ｋｅｙが用いられ、管理掲示板４５４から読取られた情報を確認するために管理４５０パブリック・キー

が用いられる。
【０１１５】
（２）エージェントのシールおよび認証。エンクレーブが生成された後の第１のステップは、標準的なシールおよび認証段階を開始することである。この段階において、インテル（Ｒ）の認証サービスによるエージェント・エンクレーブの検証を含むレポートが作成される。この段階は、認証サービス４４０によって管理される。生成されるレポートは、エージェントのコードの測定値、およびエンクレーブとその新たに生成されたパブリック・キーとのエンタングルメントを含む。このパブリック・キーは、エージェントとのすべての外部通信の手段である（通信の暗号化およびその認証の両方に対する）。認証段階の一部として、エージェント・エンクレーブは自身のコードの測定値を作成するように要求される。このステップは、エージェント測定値（ＡＥ－ＭＲと示される）を記録するためにも用いられ、このエージェント測定値は任意の将来の対話においてその他のエージェントを確認するために後で用いられることとなる。
【０１１６】
（３）管理掲示板の投入。ここで管理４５０は自身の掲示板４５４をセットアップして、そこにクラスタを形成するすべてのエージェントのリストを投入できる。各エントリはエージェントの役割（コア／リーダ／ライタ）、そのＩＰアドレス、そのパブリック・キー、およびエージェントのコード測定値とそのパブリック・キーとをエンタングルする完全な認証レポートを保持するべきである。
【０１１７】
（４）エージェントの初期設定。ここでクラスタのビューによってさまざまなエージェントを初期設定できる。これは、掲示板４５４からクラスタ・リストを読取ること（およびリストの妥当性を確認すること）によって行われる。これは、エージェントがクラスタにおける自身のそれぞれの役割を想定するための手段である。
【０１１８】
（５）コア・エージェントのハンドシェークおよびキー作成段階。この段階において、指定されたリード・コア・エージェントは主要なキー（ＡＥキー）を生成する。残りのコア・エージェントはリード・エージェントにコンタクトして、以下に考察されるコアからエージェントへのキー・ハンドオーバ・プロトコルを用いてＡＥキーを検索しなければならない。セットアップ段階の感受性のため、かつ分割クラスタを作成するさまざまな攻撃を避ける手段として、リード・コア・エージェントは、ＡＥキーをその他すべてのコア・エージェント（代替的には予め規定された閾値のコア・エージェント）に送ることに成功したときにのみ、このステップの成功を承認することとなる。このことが所与の時間閾値以内に起こらなかった場合、このプロセスは中断されてステップ１から再スタートされる。他方で、成功したプロセスは最後にリード・コア・エージェントが「読取りを行う」メッセージを生成してそれを掲示板４５４にポストする（このメッセージはリード・コアのパブリック・キーを用いて確認され得る）。このメッセージがポストされた後に初めて、クラスタがＩＯ動作のためにアクティブになる。なお、リード・コア・エージェントの役割は新たなクラスタを提出することのみに関するため、リード・コア・ノードの（一時的または永続的な）故障は、単なる短期間サイクルの事項である。こうした故障はプロセスの中断と、エージェントの新たなセットによるスタートとをもたらすことになる。
【０１１９】
（６）ライタおよびリーダ・エージェントのセットアップ。クラスタのコアが設定されてから、同じハンドシェークおよびキー提供がライタおよびリーダ・エージェントとコア・エージェントとの間で行われ得る。この対話は、コアからエージェントへのキー・ハンドオーバ・プロトコルと同じプロトコルに従う。
【０１２０】
この実施形態のコアからエージェントへのキー・ハンドオーバ・プロトコル。上述のとおり、新たなエージェントは掲示板４５４からコア・エージェントにコンタクトすることによって、ＡＥキーに対する要求を開始する。通常は地理的に近いところが選択されてもよ

く、この選択およびハンドオーバの開始はエージェントのセキュアでない部分によって行われる。ハンドオーバ・プロセスの流れは、関与する２つのエージェントの相互認証テストを含む。なお、キー・ハンドオーバは極秘動作であり、管理４５０に依拠できない。そうではなく、コア・エージェントは、彼のコードとまったく同じコード測定値を有するエージェントにのみキーを提供する。この方式で、たとえ新たなエージェントが悪意をもって作成されたとしても、その作成を誰がどこで開始したかにかかわらず、それが真のエンクレーブで実行されて合法的動作のみを行うことが確実にされる。反対方向も等しく重要であり、新たなエンクレーブが悪質な機関（クラスタ全体を損なわれたキーによって動作させる可能性がある）からキーを受信しないことを確実にする。

【０１２１】

なお、合法的エージェントの測定値（ＭＲＥＮＣＬＡＶＥ）は、エージェントが適切なエージェントと通信していることを確認できるようにするために、エージェント自身に知られる必要がある。しかし、この測定値をコードにハードコード化することはできない。なぜなら、コードの任意の部分は測定値自体に含まれるからである（測定値はハードコード化されると変化するだろう）。このことを解決する１つの選択肢は、掲示板４５４において測定値を公開させて、それを認証が開始する直前に読取ることである（測定値はパブリック・キーと並んでユーザ・データに加えることができ、よってエンクレーブの認証レポートにおいて確認され得る）。この方法においては、異なる測定値のリストを有することができ、その１つはコア・エージェントに対するもの、他のものはリーダおよびライタ・エージェントに対するものである。問題は、このことが掲示板４５４に大きく依拠することである。代わりにこの実施形態が用いる解決策では、すべてのエージェントがまったく同じコードを有し、まったく同じコードを実行するエンクレーブのみとキーを共有することとなる。この実施は、コードに起こり得るソフトウェア・アップグレードの際に制限を有するが、キーの秘密特性が正しいコードの実施（公的に確認され得る）のみに依拠し、管理４５０の損傷に影響され得ないという点で、強力なセキュリティの利点を有する。

【０１２２】

オーケストレータ４５２はクラスタの開始を駆動するが、クラスタの連続的動作も担当している。オーケストレータ４５２は、ノード故障の場合にコア・エージェントを加えること、および作業負荷が増大または縮小する際にサービスの高い利用可能性を確実にするためにリーダおよびライタを加える（または停止させる）ことの責任を負う。こうした動作はすべて、２つの主要タイプの活動を必要とする。第１の活動はエージェントに対する直接の動作であり、それはエージェントの作成、その認証の開始、およびその動作のスタートを含み、第２の活動はエージェントを掲示板４５４に登録することである。

【０１２３】

動作の態様に対して、この実施形態はドッカー化エンクレーブを用いて、たとえばＫｕｂｅｒｎｅｔｅｓ（ＴＭ）またはＭａｒａｔｈｏｎ（ＴＭ）などの管理ツールを使用する。これらの管理動作は信頼されないエンティティによって実行され得る。なぜなら、エンクレーブは掲示板４５４に相談することなく任意の活動を開始することはないからである。よって、編成活動の不正行為は失敗またはサービスの拒否をもたらし得るが、我々の主要なセキュリティの目標には影響しないだろう。登録される前に、新たなエントリは最小数ｋの管理者の承認を必要とし、ここでｋは動作自体に依存する設定可能なパラメータである。たとえば、比較的頻繁なリーダまたはライタの追加などである。

【０１２４】

掲示板４５４の役割は、実行中のライブ・エージェントの中心的かつ決定的なリストを形成することである。掲示板４５４は、いくつかの管理エンティティによって管理される分散サービスである。このサービスは次の主要特性を達成すべきである。１）一貫性　－　掲示板４５４において提示されるデータは任意のオブザーバに対して同じとなる。２）認証および活動性　－　掲示板４５４のデータ読取りは偽造できず、古いデータは識別され得る（これは中間者攻撃を避けるためである）。

【０１２５】

この実施形態は、掲示板４５４に対して２つの代替的実施を使用する。
（１）掲示板エンクレーブ。この実施においては、掲示板４５４を管理するために特別なエンクレーブが作成される。このエンクレーブは管理者から新たなエントリを取り込み、それらの署名を検証してそれらを登録する。加えてこのエンクレーブはさまざまなコンポーネントからのクエリを扱い、現行の決定的クラスタ状態によって応答する。このエンクレーブは、掲示板エンクレーブのみに知られる秘密キーを用いて情報に署名する。別の特性は、掲示板エンクレーブが自身の上に現れるすべての動作からなるオーディット・ログを容易に生成できることである。このことは、悪意ある敵がエージェントを登録できず、それを通知されることなく迅速に除去することを確実にする。
【０１２６】
一貫性の特性は、単一のエンクレーブのみが掲示板の機能を扱うことを指示する。このことは、このエンクレーブが永続的に故障した場合に、その秘密キーを管理４５０によって検索可能にする必要があることを意味する。この情報は極めて極秘であるため、それに対する責任は執行委員会メンバーに委ねられてもよい（例、これは比較的大きな管理者のグループおよび高ランクの幹部であってもよい）。クラスタ開始の際に、掲示板エンクレーブが作成されて実行される。その第１のステップは、掲示板４５４に対するパブリック－秘密キー対を生成することである。パブリック・キーは公開され、次いでエージェント・コードにハードコード化される。秘密キーから、エンクレーブはｌ－ｏｕｔ－ｏｆ－ｎ秘密共有スキーム（例、シャミール（Ｓｈａｍｉｒ）秘密共有）に対する秘密共有を作成し、その共有をセキュア・チャネルを通じて執行委員会メンバーのリスト（そのリストは掲示板エンクレーブにハードコード化される）に送る。この情報も、一時的故障から回復する手段として掲示板エンクレーブによってシールされる。エンクレーブを実行するマシンの永続的な故障の場合は、新たな掲示板エンクレーブが作成されるが、それは新たなキーを生成するのではなく、執行委員会メンバーによって送られた秘密共有からキーを再生する。
【０１２７】
（２）実用的ビザンチン・フォールト・トレラント（ＰＢＦＴ：Ｐｒａｃｔｉｃａｌ Ｂｙｚａｎｔｉｎｅ Ｆａｕｌｔ Ｔｏｌｅｒａｎｔ）。掲示板４５４の代替的実施形態は、分散フォールト・トレラント・スキームを実現する実用的ビザンチン・フォールト・トレラント（ＰＢＦＴ）クラスタの実行に基づいている。このサービスは、ブロックチェーン技術に対するオープン・ソース努力の一部として、ハイパーレッジャー（Ｈｙｐｅｒｌｅｄｇｅｒ）プロジェクトのファブリックにおいて実施された。身近な脅威モデルから開始する通常の故障と反対の、ビザンチン・フォールトに対するフォールト・トレランスの必要性。すなわち、不正な管理者が悪質なメッセージを注入することによって掲示板に影響し得る可能性。なお、掲示板４５４は大きなトラフィック負荷を取り扱う必要はなく、小さいクラスタに基づいてもよく、よって大規模ＰＢＦＴを実行する性能制限は重要でない。この実施形態は通信に何らかの複雑さを加えるが、故障またはサービスの拒否を引き起こす試みに直面したときの高い利用可能性という利点を有する。
【０１２８】
どちらの場合にも、ノンスによって掲示板４５４にクエリを行い、エンクレーブまたはＰＢＦＴにノンスを署名に組み込ませることによって、データの活動性をテストできる。
【０１２９】
この実施形態の設計は不変量を有し、この不変量によってＡＥキーが伝達されるときはまったく同じエージェント・コードを有するエンクレーブに対するときのみとなり、この事実はこの実施形態のキー秘密保証の基礎となる。このことはコードのアップグレードを問題あるものにし、こうしたシナリオを取り扱うための特別な機構を必要とする。こうした極秘の場合には、少数の管理者による検証を必要とするのではなく、執行委員会メンバー（使用の場合によって、これは高ランクの個人群の委員会であり得る）からの承認が必要となるだろう。こうしたプロセスを確認するためのアップグレード・パブリック・キーは、コード作成の際にハードコード化されている。アップグレードが開始されてから、新た

なコード・ベースの測定値が掲示板４５４において公開されることとなり、コア・エンクレーブの古いセットはＡＥキーを新たなコアに送り、一方で新たなＭＲＥＮＣＬＡＶＥが好適であることを検証する。プロセスの最後に、古いエンクレーブは終了することとなる。

【０１３０】

本発明はシステム、方法、もしくはコンピュータ・プログラム製品、またはその組み合わせであってもよい。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有するコンピュータ可読ストレージ媒体（または複数の媒体）を含んでもよい。

【０１３１】

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って使用するための命令を保持および保存できる有形デバイスであり得る。コンピュータ可読ストレージ媒体は、たと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、電磁気ストレージ・デバイス、半導体ストレージ・デバイス、または前述の任意の好適な組み合わせなどであってもよいが、それに限定されない。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リストは以下を含む。ポータブル・コンピュータ・ディスケット、ハード・ディスク、ランダム・アクセス・メモリ（ＲＡＭ：ｒａｎｄｏｍ ａｃｃｅｓｓ ｍｅｍｏｒｙ）、リード・オンリ・メモリ（ＲＯＭ：ｒｅａｄ－ｏｎｌｙ ｍｅｍｏｒｙ）、消去可能プログラマブル・リード・オンリ・メモリ（ｅｒａｓａｂｌｅ ｐｒｏｇｒａｍｍａｂｌｅ ｒｅａｄ－ｏｎｌｙ ｍｅｍｏｒｙ）（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：ｓｔａｔｉｃ ｒａｎｄｏｍ ａｃｃｅｓｓ ｍｅｍｏｒｙ）、ポータブル・コンパクト・ディスク・リード・オンリ・メモリ（ＣＤ－ＲＯＭ：ｃｏｍｐａｃｔ ｄｉｓｃ ｒｅａｄ－ｏｎｌｙ ｍｅｍｏｒｙ）、デジタル多用途ディスク（ＤＶＤ：ｄｉｇｉｔａｌ ｖｅｒｓａｔｉｌｅ ｄｉｓｋ）、メモリ・スティック、フロッピー（Ｒ）ディスク、機械的にコード化されたデバイス、たとえばパンチ・カードまたは溝に命令が記録された隆起構造など、および前述の任意の好適な組み合わせ。本明細書において用いられるコンピュータ可読ストレージ媒体は、たとえば電波もしくはその他の自由に伝播する電磁波、導波路もしくはその他の伝送媒体を通じて伝播する電磁波（例、光ファイバ・ケーブルを通過する光パルス）、またはワイヤを通じて伝送される電気信号など、それ自体が一時的信号のものであると解釈されるべきではない。

【０１３２】

本明細書に記載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／処理デバイスにダウンロードされ得るか、またはたと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、もしくは無線ネットワーク、また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され得る。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、もしくはエッジ・サーバ、またはその組み合わせを含んでもよい。各コンピューティング／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信して、そのコンピュータ可読プログラム命令を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に記憶するために転送する。

【０１３３】

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（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、または１つもしくはそれ以上のプログラミング言語の任意の組み合わせで書かれたソース・コードもしくはオブジェクト・コードであってもよく、このプログラミング言語はオブジェクト指向プログラミング言語、たとえばＳｍａｌｌｔａｌｋ、またはＣ＋＋など、および従来の手続き型プログラミング言語、たとえば「Ｃ」プログラミン

グ言語または類似のプログラミング言語などを含む。コンピュータ可読プログラム命令は、すべてがユーザのコンピュータで実行されてもよいし、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ユーザのコンピュータで実行されてもよいし、一部がユーザのコンピュータで、一部がリモート・コンピュータで実行されてもよいし、すべてがリモート・コンピュータまたはサーバで実行されてもよい。後者のシナリオにおいて、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：ｌｏｃａｌ ａｒｅａ ｎｅｔｗｏｒｋ）または広域ネットワーク（ＷＡＮ：ｗｉｄｅ ａｒｅａ ｎｅｔｗｏｒｋ）を含む任意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てもよいし、（たとえば、インターネット・サービス・プロバイダを用いてインターネットを通じて）外部コンピュータへの接続が行われてもよい。いくつかの実施形態において、たとえばプログラマブル・ロジック回路、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）などを含む電子回路は、本発明の態様を行うために電子回路をパーソナライズするためのコンピュータ可読プログラム命令の状態情報を使用することによって、コンピュータ可読プログラム命令を実行してもよい。

【０１３４】

本明細書においては、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・プログラム製品の流れ図もしくはブロック図またはその両方を参照して、本発明の態様を説明している。流れ図もしくはブロック図またはその両方の各ブロック、および流れ図もしくはブロック図またはその両方におけるブロックの組み合わせは、コンピュータ可読プログラム命令によって実現され得ることが理解されるだろう。

【０１３５】

これらのコンピュータ可読プログラム命令は、汎用目的コンピュータ、特定目的コンピュータ、またはマシンを生成するためのその他のプログラマブル・データ処理装置のプロセッサに提供されることによって、そのコンピュータまたはその他のプログラマブル・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、流れ図もしくはブロック図またはその両方の単数または複数のブロックにおいて指定される機能／動作を実現するための手段を生じてもよい。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、プログラマブル・データ処理装置、もしくはその他のデバイスまたはその組み合わせに特定の方式で機能するように指示できるコンピュータ可読ストレージ媒体にも保存されることによって、命令が保存されたコンピュータ可読ストレージ媒体が、流れ図もしくはブロック図またはその両方の単数または複数のブロックにおいて指定される機能／動作の態様を実現する命令を含む製造物を含んでもよい。

【０１３６】

コンピュータ可読プログラム命令は、コンピュータ、他のプログラマブル・データ処理装置、または他のデバイスにもロードされて、コンピュータに実現されるプロセスを生成するためにコンピュータ、他のプログラマブル装置、または他のデバイスにおいて一連の動作ステップを行わせることによって、そのコンピュータ、他のプログラマブル装置、または他のデバイスにおいて実行される命令が、流れ図もしくはブロック図またはその両方の単数または複数のブロックにおいて指定される機能／動作を実現してもよい。

【０１３７】

図面における流れ図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施のアーキテクチャ、機能、および動作を示すものである。これに関して、流れ図またはブロック図の各ブロックは、指定される論理機能（単数または複数）を実現するための１つまたはそれ以上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してもよい。いくつかの代替的実施において、ブロック内に示される機能は、図面に示されるものとは異なる順序で起こってもよい。たとえば、連続して示される２つのブロックは、実際には実質的に同時に実行されてもよいし、関与する機能によってはこれらのブロックがときに逆の順序で実行され

てもよい。加えて、ブロック図もしくは流れ図またはその両方の各ブロック、およびブロック図もしくは流れ図またはその両方のブロックの組み合わせは、指定された機能を行うか、特定目的のハードウェアおよびコンピュータ命令の組み合わせを実施または実行する特定目的のハードウェア・ベースのシステムによって実現され得ることが注目されるだろう。

【０１３８】

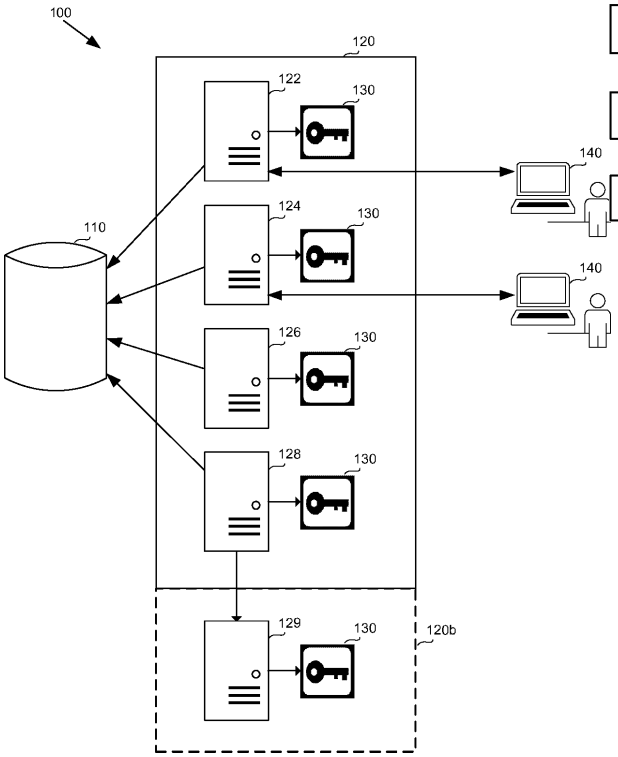
本明細書において用いられる用語は、特定の実施形態を説明する目的のみのためのものであり、本発明を限定することは意図されない。本明細書において用いられる単数形の「ａ」、「ａｎ」、および「ｔｈｅ」は、状況が別様を明瞭に示さない限り複数形も含むことが意図されている。さらに、本明細書において用いられるときの「含む（ｃｏｍｐｒｉｓｅｓ）」もしくは「含む（ｃｏｍｐｒｉｓｉｎｇ）」またはその両方の用語は、記述される特徴、整数、ステップ、動作、エレメント、もしくはコンポーネント、またはその組み合わせの存在を明示するが、１つまたはそれ以上の他の特徴、整数、ステップ、動作、エレメント、コンポーネント、もしくはそのグループ、またはその組み合わせの存在または追加を除外するものではないことが理解されるだろう。

【０１３９】

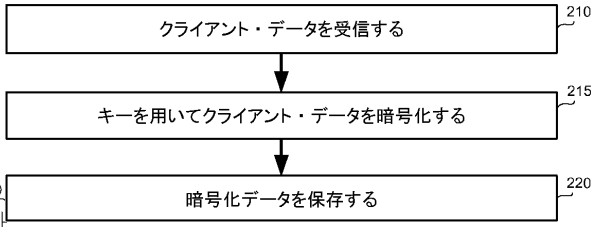
以下の請求項におけるすべての手段またはステップ・プラス機能要素に対応する構造、材料、動作、および均等物は、特定的に請求される他の請求要素と組み合わせてその機能を行うための任意の構造、材料または動作を含むことが意図される。本発明の説明を例示および説明の目的のために提供したが、開示される形の本発明に対して網羅的または限定的になることは意図されていない。本発明の範囲および趣旨から逸脱することなく、当業者には多くの修正および変更が明らかになるだろう。実施形態は、本発明の原理および実際の適用を最もよく説明し、かつ他の当業者が予期される特定の使用に好適であるようなさまざまな修正を伴うさまざまな実施形態に対して本発明を理解できるようにするために選択されて記載されたものである。

【図面】

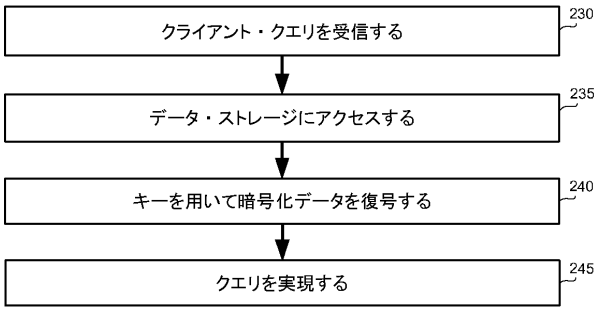
【図１】


100
120
122
130
124
130
126
130
128
130
129
130
120b
110
140
140

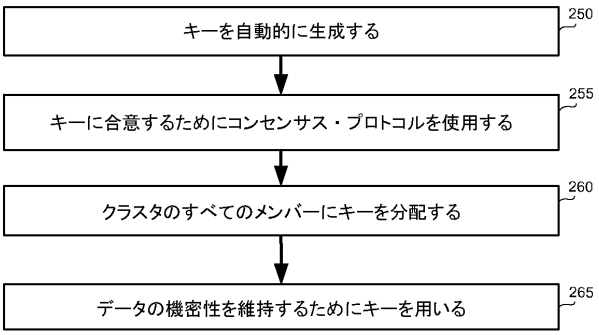
【図２】


クライアント・データを受信する
210
キーを用いてクライアント・データを暗号化する
215
暗号化データを保存する
220

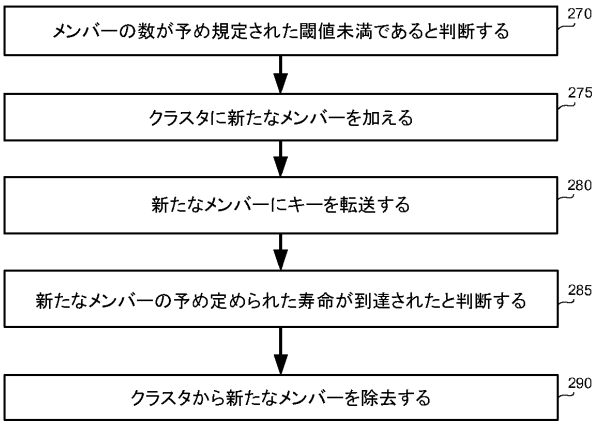
【図３】


クライアント・クエリを受信する
230
データ・ストレージにアクセスする
235
キーを用いて暗号化データを復号する
240
クエリを実現する
245

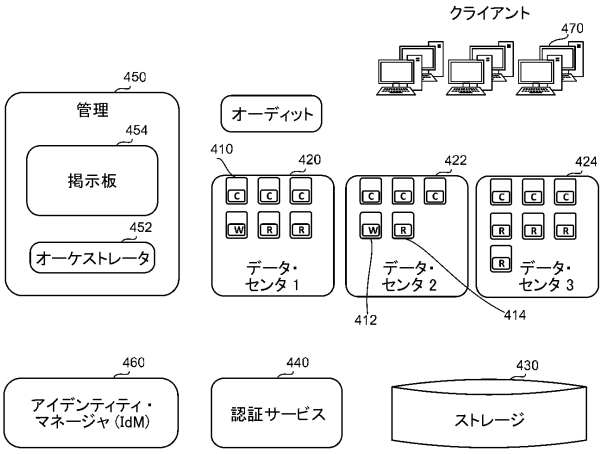
【図４】


キーを自動的に生成する
250
キーに合意するためにコンセンサス・プロトコルを使用する
255
クラスタのすべてのメンバーにキーを分配する
260
データの機密性を維持するためにキーを用いる
265

【図５】


メンバーの数が予め規定された閾値未満であると判断する
270
クラスタに新たなメンバーを加える
275
新たなメンバーにキーを転送する
280
新たなメンバーの予め定められた寿命が到達されたと判断する
285
クラスタから新たなメンバーを除去する
290

【図６】


クライアント
470
450
管理
454
掲示板
452
オーケストレータ
オーディット
410
420
422
424
C
W
R
データ・
センタ 1
データ・
センタ 2
データ・
センタ 3
412
414
460
アイデンティティ・
マネージャ (IdM)
440
認証サービス
430
ストレージ

フロントページの続き

(74)代理人　100112690
弁理士　太佐 種一
(72)発明者　ハルニク、ダニー
イスラエル国 テルアビブ ピーオービー １１ ギバタイム アリエル・シャロン・ストリート ４
(72)発明者　ターシュマ、パウラ、キム
イスラエル国 テルアビブ ピーオービー １１ ギバタイム アリエル・シャロン・ストリート ４
(72)発明者　ウェインスバーグ、ヨロン
イスラエル国 ３１９０５ ハイファ マウント・カーメル ハイファ・ユニバーシティ
(72)発明者　ヘルシュコビッチ、モシク
イスラエル国 テルアビブ ピーオービー １１ ギバタイム アリエル・シャロン・ストリート ４
審査官　岸野 徹
(56)参考文献　特開２０１１－０７８１００（ＪＰ，Ａ）
米国特許出願公開第２０１５／０１４３１３４（ＵＳ，Ａ１）
国際公開第２０１６／０５３５１４（WO，Ａ１）
国際公開第２０１６／１７８３１６（WO，Ａ１）
国際公開第２０１０／１４０１９４（WO，Ａ１）
米国特許出願公開第２０１６／０１６２３２０（ＵＳ，Ａ１）
特開２０１５－１９４９５８（ＪＰ，Ａ）
特開２０１５－１８１０４５（ＪＰ，Ａ）
米国特許出願公開第２００５／００９１０７８（ＵＳ，Ａ１）
米国特許出願公開第２０１８／０１０７５０３（ＵＳ，Ａ１）
特表２０１７－５３８２０４（ＪＰ，Ａ）
米国特許出願公開第２０１５／０２７７９５６（ＵＳ，Ａ１）
(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／６２
Ｈ０４Ｌ　９／０８