(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7030778号
(P7030778)

(45)発行日　令和4年3月7日(2022.3.7)

(24)登録日　令和4年2月25日(2022.2.25)

(51)国際特許分類

Ｈ０４Ｌ　9/08　(2006.01)	Ｈ０４Ｌ	9/08	Ｃ
Ｇ０６Ｆ　21/44　(2013.01)	Ｇ０６Ｆ	21/44	

請求項の数　14　（全20頁）

(21)出願番号　特願2019-503258(P2019-503258)
(86)(22)出願日　平成29年7月27日(2017.7.27)
(65)公表番号　特表2019-523595(P2019-523595A)
(43)公表日　令和1年8月22日(2019.8.22)
(86)国際出願番号　PCT/EP2017/068987
(87)国際公開番号　WO2018/019928
(87)国際公開日　平成30年2月1日(2018.2.1)
審査請求日　令和2年5月28日(2020.5.28)
(31)優先権主張番号　62/367,705
(32)優先日　平成28年7月28日(2016.7.28)
(33)優先権主張国・地域又は機関
米国(US)
(31)優先権主張番号　62/511,376
(32)優先日　平成29年5月26日(2017.5.26)
最終頁に続く

(73)特許権者　590000248
コーニンクレッカ フィリップス エヌヴェ
Ｋｏｎｉｎｋｌｉｊｋｅ Ｐｈｉｌｉｐｓ Ｎ．Ｖ．
オランダ国 ５６５６ アーヘー アインドーフェン ハイテック キャンパス ５２
Ｈｉｇｈ Ｔｅｃｈ Ｃａｍｐｕｓ ５２，５６５６ ＡＧ Ｅｉｎｄｈｏｖｅｎ，Ｎｅｔｈｅｒｌａｎｄｓ
(74)代理人　100122769
弁理士　笛田 秀仙
(74)代理人　100163809
弁理士　五十嵐 貴裕
(74)代理人　100145654
最終頁に続く

(54)【発明の名称】　データの複製先であるネットワークノードの識別

(57)【特許請求の範囲】
【請求項１】
データが複製される先となるネットワーク内のネットワークノードを識別するための装置により実行される方法であって、
属性ベースの暗号化スキームに従ってセッション鍵を暗号化するステップと、
前記ネットワーク内に前記暗号化されたセッション鍵をブロードキャストするステップと、
前記ネットワーク内の少なくとも１つのネットワークノードから前記セッション鍵を用いて暗号化された少なくとも１つのメッセージを受信するステップと、
前記データが複製される先となるネットワークノードを、当該ネットワークノードが前記セッション鍵を用いてメッセージを暗号化することが可能であることに基づいて、前記少なくとも１つのネットワークノードから選択するステップと、
を有する方法。
【請求項２】
前記少なくとも１つのネットワークノードは、少なくとも１つの仮想マシンを有する、請求項１に記載の方法。
【請求項３】
前記セッション鍵を暗号化するために用いられる属性は、１つ以上の地理的な位置を規定する地理位置方針を有する、請求項１又は２に記載の方法。
【請求項４】
前記地理位置方針は、データが複製されることが許可された位置として、１つ以上の地理

的な位置のうちの少なくとも１つを識別する、請求項３に記載の方法。
【請求項５】
前記地理位置方針は、データが複製されることが許可されていない位置として、１つ以上の地理的な位置のうちの少なくとも１つを識別する、請求項３又は４に記載の方法。
【請求項６】
前記選択されたネットワークノード以外の、前記ネットワーク内の特定のネットワークノードから、前記暗号化されたセッション鍵が前記特定のネットワークノードにより復号化されることができないことを示すメッセージを受信するステップを更に有する、請求項１乃至５のいずれか一項に記載の方法。
【請求項７】
前記暗号化するステップ及び前記ブロードキャストするステップは、前記ネットワーク内の少なくとも１つのセキュアなトンネルの失効に応答して実行される、請求項１乃至６のいずれか一項に記載の方法。
【請求項８】
ネットワーク内のデータ複製を容易化するための、ネットワークノードにおける処理装置により実行される方法であって、
属性ベースの暗号化スキームに従って暗号化されたセッション鍵を含むメッセージを、元の装置から受信するステップと
方針鍵を用いて前記メッセージを復号化するよう試みるステップと、
前記メッセージを復号化する試みが成功したか否かを決定するステップと、
前記メッセージを復号化する試みが成功したとの決定に応じて、
前記セッション鍵によって返答メッセージを暗号化するステップと、
前記元の装置からの前記メッセージを復号化することが可能であることを示すために前記元の装置に前記返答メッセージを送信するステップと、
を有する方法。
【請求項９】
前記メッセージを復号化する試みが失敗したとの決定に応じて、
前記復号化が失敗したことの示唆を前記元の装置に送信するステップ
を更に有する、請求項８に記載の方法。
【請求項１０】
前記セッション鍵を暗号化するために用いられる属性は、１つ以上の地理的な位置を規定する地理位置方針を有し、
前記方針鍵は、前記処理装置が位置する地理的な位置に特有なものである、
請求項８又は９に記載の方法。
【請求項１１】
前記処理装置が位置する地理的な位置に割り当てられた鍵サーバを識別するステップと、
前記鍵サーバを用いて認証するステップと、
前記鍵サーバから方針鍵を受信するステップと、
を更に有する、請求項１０に記載の方法。
【請求項１２】
前記元の装置から複製されるべきデータを受信するステップと、
後のアクセスのため前記複製されるべきデータを保存するステップと、
を更に有する、請求項８に記載の方法。
【請求項１３】
請求項１乃至７のいずれか一項に記載の方法を実行するための命令を有する、プロセッサによる実行のための命令をエンコードされた、持続性機械読み取り可能媒体。
【請求項１４】
請求項８乃至１２のいずれか一項に記載の方法を実行するための命令を有する、プロセッサによる実行のための命令をエンコードされた、持続性機械読み取り可能媒体。
【発明の詳細な説明】

【技術分野】
【０００１】
ここで記載される種々の実施例は、データ複製に関し、限定するものではないが更に詳細には、ネットワーク間でのデータ複製に関する。
【背景技術】
【０００２】
今日、相互接続された健康システムは、協調を通して、患者のための改善された、またより効率の良いケアを提供することが可能となっている。斯かるシステムにおいては、医療は病院の外に出て、このデータからより多くのスマートな知識を抽出する解析ツールに近づいている。これらのタイプの解析は、医療を患者により合わせたものとし、それ故より正確なものとしている。
【０００３】
医療ツールに及び最終的には患者に権限を持たせること／能力を付与することは、（種々のプラットフォーム上の）世界中の複数のデータ記憶装置でデータが複製されることを必要とする。データは、データクエリの性能、負荷バランシング及び被災時の復旧に関する要件のため、世界中の異なる記憶媒体に複製される。複製は、データがいずれの地理的な位置（例えば国又は大陸）からいずれの記憶媒体にも保存されることができる場合には簡潔となり得るが、現実世界ではこのことはしばしば当てはまらず、データ記憶プラットフォームは、政府のエンティティにより課される種々の地理的位置的な指示、規定又は要件、及び顧客又はエンドユーザにより定義されるその他の要件を、遵守する必要がある。例えば、地域的な制約の下、データは或る地域又は国から別の地域又は国へと自由に流れることができない場合がある。斯かる制約は、協定から又はデータの所有者（例えば患者）によって、１つ以上の国の方針によって決定され得る。
【発明の概要】
【発明が解決しようとする課題】
【０００４】
この状況は、仮想マシンのようなクラウドベースの計算システムにおいて増大する信頼性要件により、更に複雑化している。地理的な要件は、斯かる相互接続された健康プラットフォームに存在し得、ここでは多テナント、多データセンタのデータ管理が、以下のような地理的な要件を履行する必要がある：
・データの一部は、グローバルに管理される必要がある（例えばマスタデータ、サービス構成、認証ソース）。
・データの一部は、「ローカル」のままであるべきである（ローカルとは、施設内又は定義された地理的な領域内であり得る）。
・テナントがドイツ国の顧客である場合、データはドイツ国内にとどまる必要がある。
・データは、テナントに応じて隔離される必要がある（例えば多テナント状況の場合）。
・データは全て、１つのデータベースに保たれる必要がある。
・データは、テナント毎のスキーマ／データベースに制限される必要がある。
【０００５】
これらの地理的な要件の１つ以上に加え、又はこれらの要件の代わりに、以下のような他の地理的な要件が存在し得る：
・位置の認識：ユーザは、ユーザのデータを処理する実行環境（ＥＥ）の物理的な位置を認識しているべきである。
・位置の制御：ユーザは、ユーザのデータが処理され得る、可能な物理的な位置（例えば国レベル）のセットを定義することが可能であるべきである。
【０００６】
相互接続された健康プラットフォームが、単一のデータ保存プロバイダ（例えば単一のクラウドプロバイダ）内でデータを保存及び管理する場合、許可された地理的な場所にのみデータを保存することは、実施が容易であり得る。斯かる場合には、クラウドプロバイダは、上述したプラットフォームの展開のため利用されるコンピュータシステム及び／又は

仮想マシン（ＶＭ）の全体を制御することができ、これらコンピュータシステム及び／又はＶＭ及びその付与されたデータ記憶媒体がどこに位置するかを知っている。

【０００７】

この状況は、プラットフォームが多数の位置に跨る多数のクラウドプロバイダに亘る場合、又は幾つかの施設内の病院システムが上述した相互接続された健康プラットフォームの一部である場合、より複雑となる。この場合には、異なるコンピューティングプロバイダに属する複数のコンピュータシステム／ＶＭが相互接続され、それ故、複数のコンピューティングプロバイダに跨る同期のため、複製のための集中化された方法がより困難となる。斯かる相互接続された健康システムにおいては、展開されるコンピュータシステム／ＶＭの構成は動的であり、種々の要件（例えば空き状況、バックアップ処理、又は新たなサービス）により、コンピュータシステム及びＶＭは、種々のコンピューティングプラットフォームに展開されたり又はそこから取り除かれたりする。この場合には、システムの動的さに適合することが可能な発見方法が、適所にある必要がある。

【０００８】

ひとつの方法は、データを暗号化し該データをネットワークを通してブロードキャストすることであり、このときデータは、該データを復号化することを許可されているコンピュータシステム又はＶＭのみが復号化できるように暗号化される。斯かる方法のみでは、相互接続された健康システムにおいてしばしば当てはまるような、複製される必要があるデータのサイズが大きい場合には、不十分であり得る。他の方法は、相互接続された健康システム内のリソースのリストを保持する中央ブローカを持つことである。しかしながら、プラットフォームは動的であり、幾つかの場合においては斯かるリストを保持することを困難とする。斯かる状況においては、全てのコンピュータプロバイダが、最終的には信頼される必要があり得る、該プロバイダのリソース／ＶＭのリスト及びその地理位置を通信及び同期する必要があり得る。

【０００９】

地理的な制約のような、種々の制約の下でのデータ複製の問題のためのデフォルトの方法は、データ源とデータが複製される必要がある場所との間にセキュアなトンネル（他仮想プライベートネットワーク、ＶＰＮ）を設定することを含み得る。第１のステップは、データが複製され得る候補リソースの発見を必要とし、第２のステップは、該発見されたリソースの認証を含み、第３のステップは、元のデータ源と該データが複製され得る新たに発見されたリソースとの間にセッション鍵を設定することから成る。殆どの場合において、第２のステップ及び第３のステップはともに、認証鍵共有プロトコルの一部である。斯かるプロトコルは、認証のための公開鍵基盤又は事前共有対称鍵を用いる。ここで、複製要件（例えば地理位置）は、どのサーバがどのデータにより信頼され得るかに関する、帯域外通信を介して実施される。

【００１０】

地理位置を提供する認証鍵共有プロトコルはないように思われる。斯かるプロトコルを提供する際の障害は、地理位置の認証方法が、大きくは開発されておらず、ひとつの方法は、インターネットプロトコル（ＩＰ）アドレス認証の利用であるが、これは不正確なものとなり得、幾つかの場合においては容易になりすましが可能であり得る。

【００１１】

従って、ここで記載される種々の実施例は、特定の方針要件、規定及び指示を履行しつつ、データが複製されることができるリソースのセキュアな認証された発見を可能とする。上述したように、この問題を解決するため提案されたステップは、順に、発見（ＩＰアドレスに基づく）、認証（公開鍵暗号化基盤を必要とし得る）、及び対称鍵の交渉である。ここで開示される種々の実施例は、より効率的でセキュアな方法で、これらの全てを組み合わせる。

【００１２】

種々の実施例は、ネットワークのノードを認証するための特定の属性を利用する、多認証者の、属性ベースの暗号化を利用する。例えば、データが複製されことができる、許可さ

れた地理的な場所に位置するノードを認証するために地理位置属性が用いられ得る。サーバは、地理的な位置を認証することができる地域的な認証者から、秘密鍵を受信する。

【００１３】

ネットワークのなかのコンピュータシステム又はＶＭは、セッション鍵の復号化を試みることにより認証されても良い。該コンピュータシステム又はＶＭが、クラウドプロバイダ又は病院のローカルサーバとは独立して、データ源の装置からのデータ複製が許可されている地理的な位置にある場合には、セッション鍵を復号化することが可能となり、複製の候補となる。

【００１４】

幾つかの例においては、セッション鍵及び／又はそのそれぞれのセキュアなトンネルは、失効日を持っても良い。このことは、暗号化鍵が定期的に変更されるため、システムの安全性に寄与する。更に、当該失効日は、複製のための新たな装置／ＶＭの再発見を強いることとなり、システムを新鮮に保ち、相互接続された健康システムの動的性に適合する。

【００１５】

該方法は、幾つかの例においては、暗号化のタイプが属性ベースである、公開鍵基盤を利用し得る。幾つかの例においては、以上に例示された地理位置の複製に合致させるため、地理位置が該属性の１つである。地理位置属性を含む方針の例は、（ＵＳ，ＤＥ，！ＣＮ）である。この方針の例によれば、データは米国及びドイツ国において複製されることができるが、中国においては複製されることができない。斯かる方針は、クラウドデータ管理インタフェース（ＣＤＭＩ）規定における「cdmi_geographic_placement」フィールドにおけるように、暗号化の履行なしで既に使用されている。

【００１６】

幾つかの実施例においては、成功する使用は、サーバの全てが、関連する属性について適切な秘密鍵を取得することに依存する。このことは、異なる認証者が異なる属性について責任を持つ認可処理を含んでも良い。一例として、サーバに関連する属性「ＵＳ」は、該サーバが米国に物理的に位置することを宣言する。本例においては、サーバが当該国に位置しているか否かをチェックする認可処理を持つ鍵認証者が米国に存在し得る。この認可が完了すると、該鍵認証者は、多認証者の属性ベースの暗号化スキームから、秘密鍵を該サーバに提供しても良い。サーバに提供された秘密鍵は、方針に「ＵＳ」を含む暗号文を復号化することを許可される。含まれる他の国について同様の認証者が存在しても良く、或る国についての属性（例えば「ＵＳ」）は、他のいずれかの国については負に観測されても（例えば「！ＣＮ」）良い。該鍵が他のサーバにコピーされることを防止するため、該鍵は例えばスマートカード又はハードウェアドングルに保存されても良い。他の例においては、例えば法律的な要件又は制約に関するような種々の属性に基づいて鍵を提供することができる認証者が存在しても良い。一例として、グローバルな組織が、１９９６年のＨＩＰＡＡ（Health Insurance Portability and Accountability Act）の遵守についてデータセンタを評価し、次いで「ＨＩＰＡＡ」属性に基づいて鍵を提供しても良い。

【課題を解決するための手段】

【００１７】

本開示は、データが複製される先となる１つ以上の仮想マシン（ＶＭ）を識別するための装置により実行される方法に関する。該方法を実行する装置は、仮想マシンであっても良い。該方法は、属性ベースの暗号化スキームに従ってセッション鍵を暗号化するステップであって、前記セッション鍵を暗号化するために用いられる属性は、１つ以上の地理的な位置を規定する地理位置方針を有するステップと、前記ネットワーク内に前記暗号化されたセッション鍵をブロードキャストするステップと、ネットワークドメイン内の少なくとも１つのＶＭから前記セッション鍵を用いて暗号化された少なくとも１つのメッセージを受信するステップと、前記データが複製される先となるＶＭを、前記少なくとも１つのＶＭから選択するステップと、を有する。

【００１８】

前記地理位置方針は、データが複製されることが許可された位置として、１つ以上の地理

的な位置のうちの少なくとも１つを識別する。前記地理位置方針は、データが複製されることが許可されていない位置として、１つ以上の地理的な位置のうちの少なくとも１つを識別する。

【００１９】

該方法は、前記ネットワークドメイン内の別のＶＭから、前記暗号化されたセッション鍵が該別のＶＭによって復号化されることできなかったことを示すメッセージを、受信するステップを更に有する。

【００２０】

前記暗号化するステップ及び前記ブロードキャストするステップは、前記ネットワークドメイン内の少なくとも１つのセキュアなトンネルの失効に応答して実行されても良い。

【００２１】

本開示はまた、通信インタフェースと、メモリと、以上に説明された方法を実行するよう構成されたプロセッサと、を有する装置に関する。

【００２２】

本開示はまた、以上に説明された方法を実行するための命令を有する、プロセッサによる実行のための命令をエンコードされた、持続性機械読み取り可能媒体に関する。

【００２３】

本発明はまた、ネットワークドメイン内のデータ複製を容易化するための、仮想マシン（ＶＭ）により実行される方法であって、属性ベースの暗号化スキームに従って暗号化されたセッション鍵を含むメッセージを、元の装置から受信するステップであって、前記セッション鍵を暗号化するために用いられる属性は、１つ以上の地理的な位置を規定する地理位置方針を有するステップと、方針鍵を用いて前記メッセージを復号化するよう試みるステップであって、前記方針鍵は、前記ＶＭが位置する地理的な位置に特有なものであるステップと、前記方針鍵によって返答メッセージを暗号化するステップと、前記元の装置に前記返答メッセージを送信するステップと、を有する方法に関する。

【００２４】

該方法は更に、前記メッセージを復号化する試みが成功したか否かを決定するステップと、該試みが失敗したと決定された場合に、前記復号化が失敗したことの示唆を前記元の装置に送信するステップと、を有しても良く、このとき前記返答メッセージを暗号化するステップ及び送信するステップは、前記試みが成功したと決定された場合に実行される。

【００２５】

該方法は更に、該ＶＭが位置する地理的な位置に割り当てられた鍵サーバを識別するステップと、前記鍵サーバを用いて認証するステップと、前記鍵サーバから方針鍵を受信するステップと、を有しても良い。

【００２６】

該方法は更に、前記元の装置から複製されるべきデータを受信するステップと、後のアクセスのため前記複製されるべきデータを保存するステップと、を有しても良い。

【００２７】

本開示はまた、通信インタフェースと、メモリと、以上に説明された方法を実行するよう構成されたプロセッサと、を有する装置に関する。

【００２８】

本開示はまた、以上に説明された方法を実行するための命令を有する、プロセッサによる実行のための命令をエンコードされた、持続性機械読み取り可能媒体に関する。

【００２９】

本開示においては、ネットワーク内のコンピュータシステム及び／又は仮想マシンは、該ネットワークのノードに位置するものとみなされ得る。ネットワークノードは、無線で（例えばクラウド環境において）又は有線接続を介して（例えば有線ネットワーク内で）互いに接続されていても良い。

【００３０】

第１の態様によれば、本発明は、データが複製される先となるネットワーク内のネットワ

ークノードを識別するための装置により実行される方法であって、属性ベースの暗号化スキームに従ってセッション鍵を暗号化するステップと、前記ネットワーク内に前記暗号化されたセッション鍵をブロードキャストするステップと、前記ネットワーク内の少なくとも１つのネットワークノードから前記セッション鍵を用いて暗号化された少なくとも１つのメッセージを受信するステップと、前記データが複製される先となるネットワークノードを、前記少なくとも１つのネットワークノードから選択するステップと、を有する方法を提供する。

【００３１】

前記少なくとも１つのネットワークノードは、少なくとも１つの仮想マシンを有しても良い。幾つかの実施例においては、該方法を実行する装置は、処理装置及び／又は仮想マシンを有しても良い。

【００３２】

前記セッション鍵を暗号化するために用いられる属性は、１つ以上の地理的な位置を規定する地理位置方針を有しても良い。幾つかの実施例においては、前記地理位置方針は、データが複製されることが許可された位置として、１つ以上の地理的な位置のうちの少なくとも１つを識別しても良い。前記地理位置方針は、データが複製されることが許可されていない位置として、１つ以上の地理的な位置のうちの少なくとも１つを識別しても良い。

【００３３】

該方法は更に、前記選択されたネットワークノード以外の、前記ネットワーク内の特定のネットワークノードから、前記暗号化されたセッション鍵が前記特定のネットワークノードにより復号化されることができないことを示すメッセージを受信するステップを有しても良い。

【００３４】

前記暗号化するステップ及び前記ブロードキャストするステップは、前記ネットワーク内の少なくとも１つのセキュアなトンネルの失効に応答して実行されても良い。

【００３５】

第２の態様によれば、本発明は、ネットワーク内のデータ複製を容易化するための、ネットワークノードにおける処理装置により実行される方法であって、属性ベースの暗号化スキームに従って暗号化されたセッション鍵を含むメッセージを、元の装置から受信するステップと方針鍵を用いて前記メッセージを復号化するよう試みるステップと、前記メッセージを復号化する試みが成功したか否かを決定するステップと、前記メッセージを復号化する試みが成功したとの決定に応じて、前記方針鍵によって返答メッセージを暗号化するステップと、前記元の装置に前記返答メッセージを送信するステップと、を有する方法を提供する。

【００３６】

幾つかの実施例においては、該第２の態様の方法は、仮想マシンにより実行されても良い。

【００３７】

該方法は更に、前記メッセージを復号化する試みが失敗したとの決定に応じて、前記復号化が失敗したことの示唆を前記元の装置に送信するステップを有しても良い。

【００３８】

幾つかの実施例においては、前記セッション鍵を暗号化するために用いられる属性は、１つ以上の地理的な位置を規定する地理位置方針を有しても良い。前記方針鍵は、前記処理装置が位置する地理的な位置に特有なものであっても良い。

【００３９】

該方法は更に、前記処理装置が位置する地理的な位置に割り当てられた鍵サーバを識別するステップと、前記鍵サーバを用いて認証するステップと、前記鍵サーバから方針鍵を受信するステップと、を有しても良い。

【００４０】

該方法は更に、前記元の装置から複製されるべきデータを受信するステップと、後のアクセスのため前記複製されるべきデータを保存するステップと、を有しても良い。

【００４１】
第３の態様によれば、本発明は、通信インタフェースと、メモリと、プロセッサと、を有する装置を提供する。該プロセッサは、以上の第１の態様による方法及び／又は以上の第２の態様による方法を実行するよう構成される。
【００４２】
第４の態様によれば、本発明は、以上の第１の態様による方法及び／又は以上の第２の態様による方法を実行するための命令を有する、プロセッサによる実行のための命令をエンコードされた、持続性機械読み取り可能媒体を提供する。
【００４３】
本発明の他の特徴は、以下の説明から明らかとなるであろう。
【００４４】
種々の実施例をより良く理解するため、添付図面への参照が為される。
【図面の簡単な説明】
【００４５】
【図１】複数のノードを含むネットワークの例を示す図である。
【図２】ネットワーク内のネットワークノードを識別するための、元の装置により実行されることが可能な方法の例を示すフロー図である。
【図３】認証された発見プロトコルの例を示す図である。
【図４】多クラウド基盤の例を示す図である。
【図５】ネットワーク内のネットワークノードを識別するための、元の装置により実行されることが可能な方法の更なる例を示すフロー図である。
【図６】ネットワーク内のデータ複製を容易化するための、ネットワークノードにより実行されることが可能な方法の例を示すフロー図である。
【図７】ネットワーク内のデータ複製を容易化するための、ネットワークノードにより実行されることが可能な方法の更なる例を示すフロー図である。
【図８】ネットワーク内のデータ複製を容易化するための、ネットワークノードにより実行されることが可能な方法の更なる例を示すフロー図である。
【図９】ネットワーク内のデータ複製を容易化するための、ネットワークノードにより実行されることが可能な方法の更なる例を示すフロー図である。
【図１０】ここで説明される方法を実行するための装置の例の簡略化された模式図である。
【図１１】持続性機械読み取り可能媒体及びプロセッサの簡略化された模式図である。
【発明を実施するための形態】
【００４６】
ここで示される記載及び図面は、種々の原理を説明する。当業者は、ここで明示的には記載され又は示されていなくても、これらの原理を実施化し、本開示の範囲内に含まれる、種々の構成を案出することが可能であろうことは理解されよう。ここで用いられる「又は」なる語は、特に示されていない限り（例えば「そうでなければ又は」又は「代替として」）、排他的ではない（即ち及び／又は）ことを示す。更に、ここで説明される種々の実施例は、必ずしも相互に排他的なものではなく、組み合わせられてここで説明される原理を組み入れた更なる実施例をもたらしても良い。
【００４７】
本発明は、複数の部屋、部門、建物、組織、国及び／又は大陸に跨るコンピュータネットワークに実装され得る。ネットワークの例１００が、図１に示されている。ネットワーク１００は、種々のノード１０２を含み、該ノードのそれぞれが、病院の建物（Ｈ１又はＨ２）又はクラウドコンピューティングプラットフォーム（ＣＣＰ１又はＣＣＰ２）のような、１つ以上の建物、組織又はクラウドコンピューティングプラットフォーム内に位置している。これらノード１０２は、米国（ＵＳ）、オランダ（ＮＬ）、ドイツ（ＤＥ）及び中国（ＣＮ）を含む、種々の国に分散されている。図１に示される例においては、これらのノードの幾つかは、互いに接続されている。他の例においては、種々の接続が存在し得る。例えば、ネットワークノード１０２ｂは病院又は病院グループＨ２のネットワーク内

にありオランダに位置しているが、ネットワークノード１０２ａはネットワークノード１０２ｂと同じ病院グループＨ２内にあるが米国に位置している。

【００４８】

一例においては、ノード１０２ａは、該ネットワーク内の１つ以上の他のノードにおいて複製されるべきデータ（例えば患者に関する医療データ）を含む、元のノード又は元ノードとして機能し得る。該データは、１つ以上の方針に示され得る、複製に関する１つ以上の制約を受け得る。例えば、該データは、該データが米国及びドイツ内のノードにおいては複製されても良いが中国内のノードにおいては複製され得ないことを示す「（ＵＳ，ＤＥ，！ＣＮ）」のような、地理位置方針を課される。斯かる方針の下では、元のノード１０２ａからのデータは、ノード１０２ｅ及び１０２ｇにおいては複製されることができるが、ノード１０２ｂ、１０２ｃ、１０２ｄ又は１０２ｆにおいては複製されることができない。

【００４９】

図２は、データが複製される先となる、ネットワーク内のネットワークノードを識別するための方法２００の例を示すフロー図である。該方法は、複製されるべきデータを含む装置により実行されても良い。該方法２００を実行する装置は、複製されるべきデータの元となり得る装置であるため、元の装置又は元装置とも呼ばれ得る。該元の装置は、処理装置、コンピューティング装置又は仮想マシンであっても良く、該元の装置は、元のノードとも呼ばれ得る。理解されるように、複製されるべきデータは、幾つかの実施例においては、他のどこかに起因しても良く、該元の装置から送信されても良い。方法２００は、ステップ２０２において、属性ベースの暗号化スキームに従ってセッション鍵を暗号化するステップを有する。該セッション鍵は、既知の手段を用いて暗号化されても良い。例えば、該暗号化ステップは、対称暗号化セッション鍵として適格なビット文字列をランダムに選択するステップと、属性ベースの暗号化スキームに従って該ビット文字列を暗号化するステップと、を含んでも良い。該セッション鍵は、例えばデータの複製先となり得るノードに関する属性のような、いずれの属性を用いて暗号化されても良い。幾つかの実施例においては、該セッション鍵を暗号化するために用いられる属性は、地理位置属性であっても良い。従って、該セッション鍵を暗号化するために用いられる属性は、１つ以上の地理的な位置を規定する地理位置方針を有しても良い。幾つかの実施例においては、該地理位置方針は、データが複製されることを許可された位置として、１つ以上の地理的な位置のうちの少なくとも１つを識別しても良い。幾つかの実施例においては、該地理位置方針は、データが複製されることを許可されていない位置として、１つ以上の地理的な位置のうちの少なくとも１つを識別しても良い。

【００５０】

ここで用いられる「地理位置（geolocation）」なる語は、データの複製先となるべきネットワークノードの位置のような、現実世界の地理的な位置を示すことを意図されている。要求される正確さに依存して、地理位置は、座標、グリット基準、建物、通り、市、国又は大陸で定義されても良い。他の例においては、セッション鍵は、異なる属性を用いて暗号化されても良い。例えば、セッション鍵は、オフィスの番号、会社若しくは組織の部門、又は会社若しくは組織自体に基づく属性を用いて暗号化されても良い。

【００５１】

幾つかの例においては、該少なくとも１つのネットワークノードは、少なくとも１つの仮想マシンを有しても良い。

【００５２】

ステップ２０４において、方法２００は、該ネットワーク内で該暗号化されたセッション鍵をブロードキャストするステップを有する。該暗号化されたセッション鍵は、いずれの既知の適切な手段を用いてブロードキャストされても良い。例えば、該鍵は、ネットワークブロードキャスト又はネットワークマルチキャストを介して送信されても良い。

【００５３】

該暗号化されたセッション鍵が該ネットワーク内のノードにブロードキャストされると、

以下に説明されるように、各ノードにおいて該セッション鍵を復号化する試みが実行されても良い。

【００５４】

方法２００は、ステップ２０６において、該ネットワーク内の少なくとも１つのネットワークノードから、該セッション鍵を用いて暗号化された少なくとも１つのメッセージを受信するステップを有する。斯くして、幾つかの実施例においては、該ネットワークノードにより受信されたセッション鍵が、該ネットワークノードから元の装置へと送られる（例えば処理装置、コンピューティング装置又は仮想マシンによって）べきメッセージを暗号化するために用いられる。

【００５５】

幾つかの場合においては、単一のネットワークノードが、ステップ２０６において受信されたメッセージを送信しても良い。他の場合においては、複数のノードがセッション鍵を用いて暗号化されたメッセージを送信しても良く、このとき該メッセージはステップ２０６において元の装置により受信される。ステップ２０８において、方法２００は更に、データが複製される先となるネットワークノードを、該少なくとも１つのネットワークノードから選択するステップを有する。幾つかの実施例においては、データ複製のため単一のノードが選択されても良く、他の実施例においては、複数のノードが選択されても良い。それ故、複製のための特定のネットワークノードの選択は、当該特定のノードがセッション鍵を用いてメッセージを暗号化することが可能であるか否かに基づく。

【００５６】

元の装置とデータが複製される先となるべきノードとの間に、セキュアなトンネル（例えばＶＰＮ）が生成されても良い。更に安全性を改善するため、元のノードと複製ノードとの間に生成される１つ以上のセキュアなトンネル（例えばデータが送信又は複製されるときに介するセキュアなトンネル）は、一時的なものであっても良い。換言すれば、セキュアなトンネルは、定義された継続時間の後に失効しても良い。幾つかの実施例においては、暗号化するステップ２０２及びブロードキャストするステップ２０４は、該ネットワーク内の少なくとも１つのセキュアなトンネルの失効に応答して実行されても良い。このようにして、データが複製される先となり得るネットワークノードのリストが、定期的にリフレッシュされ、適切なノードの識別が、方針における何らかの変更を考慮することができるようになる。

【００５７】

以上に説明された方法２００は、図３を参照しながら特定の例に関して説明される。種々の実施例は、図３に示されるようなプロトコルを含む。該プロトコルは、以下の３つのステップを含む。

・元のノードが、「全ノード」（即ち該ネットワークにおける全てのノード）にメッセージ：Policy、E_{policy}(sessionKey)をブロードキャストする。本例におけるメッセージは、２つの連結した部分を含み、第１の部分は、機械読み取り可能な暗号化されていない表現で記述された方針自体であり、第２の部分は、公開鍵「Policy」を用いた平文「sessionKey」の暗号化（Ｅ）に起因する暗号文である。

（ここで、該元のノードは、例えばデータクエリの性能、負荷バランシング及び被災時の復旧に関する要件のため、データを複製することを決定するノードである。図１においては、該元のノードはノード１０２ａである）

・複製先（即ち該ネットワークにおけるノードの残り）は、該元のノードによりブロードキャストされたメッセージを受信する。これら複製先の全ては、それぞれの秘密鍵を用いてブロードキャストされたメッセージを復号化することを試み、各ノードの応答は以下の２つのうちの一方となり得る：

－「解読できない」

・・・斯かる応答は、該メッセージを復号化するのに必要な鍵を持たないノードにより送信される。このことは、これらノードが要求される方針を満足しないことを暗黙的に意味する。

－「ＯＫ。ここにデータを複製可能」。ノードは、セッション鍵$E_{sessionKey}$(src,dst,Policy)を用いて暗号化されたメッセージを元の装置に送信する。この応答は、「候補」とみなされるノードにより与えられる。ここで「src」はデータ源であり、「dst」は複製先であり、該メッセージは鍵「sessionKey」を用いた平文「src,dst,Policy」の暗号化（E）に起因する暗号文である。事実上、当該応答を送信することにより、ノードは、元のメッセージを復号化することが可能であること、及び方針を満足する（「sessionKey」鍵を利用することができるため）ことを確認する。該ノードはまた、要求がどこから来たが（「dst」）及び方針は何かを反復し、誰が応答を送信したか（「src」）を説明する。
・・・当該応答を送信するノードは、ブロードキャストされたメッセージを復号化するために必要とされる鍵を持つ。このことは、例えば属性をノードに割り当てる種々の認証者により主張される、要求される方針を該ノードが満足することを暗黙的に意味する。
・・・複製先は、「ＯＫ」メッセージ及びセッション鍵を用いて暗号化されたメッセージを元のノードに送信し、該複製先が方針における要件を満足すること（例えば許可される地理的位置に位置していること）を示す。

【００５８】

元の装置は、データが複製される先となる１つ以上のノード（例えばコンピューティングシステム／ＶＭ）を選択し、これら選択されたノードが図３において「選択されたノード」として示されている。次いで、元の装置は、元のメッセージにおいて提案されたセッション鍵を用いて暗号化された、複製されるべきデータ（例えば機密データ）を送信する。それ故、複製先ノードに送信されるメッセージは、$E_{sessionKey}$(data)である。

【００５９】

図３に示された認証された発見プロトコルは、多クラウド基盤４００内に統合されても良く、その例は図４に示されている。基盤４００は、計算抽象化面（abstraction plane）４０２、データ抽象化面４０４、及びネットワーク抽象化面４０６により示されている。該統合は、データ複製を別個に取り扱う構成要素を、クラウドコンピューティングプラットフォームの全ノード（例えばＶＭ）１０２において展開することを含む。該構成要素は、「データ複製サービス」４０８と示される。斯かる構成要素４０８は、必要なときに秘密鍵を提供される。該鍵は、クラウドプラットフォームの「計算」面４０２に存在する。「データ複製サービス」４０８は、認証された発見プロトコルを起動し、発見メッセージをブロードキャストするためのクラウドプラットフォームのネットワーク面４０６に依存する（図４において「１」と記された線により示されるステップ）。次いで、各候補ノード（例えばＶＭ）１０２ｂ乃至ｇからの「データ複製サービス」要素４０８が、該発見メッセージに回答する（例えば応答する）（図４において「２」と記された線により示されるステップ）。図４のステップ３（「３」と記された線により示される）において、元の装置１０２ａの「データ複製サービス」４０８が、複製のため、選択されたノード（例えばＶＭ）に暗号化されたデータを送信する。矢印３は「データ抽象化面」４０４を通り進み、それ故当該面は該データの複製されたバージョンを認識する必要がある。

【００６０】

図４の例に示された処理は、更なるユーザがアプリケーション（「App」４１０により示される）を利用し、それ故システムのより好適な性能のために負荷バランシングが必要となったときに、起動されても良い。例えば、多くのユーザが仮想マシンを同時に利用している場合、該仮想マシンはどこかの時点で負荷に対処できなくなり得る。これを防止するため、それぞれが負荷の一部に対処する複数の仮想マシンが利用されても良い。

【００６１】

中国からの多くのユーザにより米国におけるＶＭが過負荷となった場合、中国において新たなＶＭを起動し、該ＶＭ及びユーザが近くにいるサーバに全てのデータを複製することは合理的である。このことは、データが実際に複製されることが許可される場所を見つけ出すことを意味する。

【００６２】

ここで説明されるシステム及び方法は、いずれのタイプのデータをも処理することができ

る。複製される必要があるデータは、パッケージング、パッケージの暗号化、パッケージの移送、パッケージの復号化、及び最終的なアンパッケージングというステップを受け得る。例えば、データベースについて、提案される方法は、複製されるべきデータベースの部分のダンプ（dump）を必要とし得る（例えばレコード及び列）。次いで、当該ダンプファイルが暗号化され、提案される認証された発見プロトコルを介して、データが複製される場所へと送信される。次いで、受信された暗号化されたパッケージが、受信複製ノード（例えばＶＭ）により復号化される。

【００６３】

該アーキテクチャにおいて、相互接続された健康システムは、U-Cloud（登録商標）のようなクラウドプラットフォームとして展開されても良く、それ故、図４に示されたような抽象化面（計算、データ、ネットワーク）を用いても良い。図４において、ステップ１、２、３は、図３に示されたプロトコルステップに、それ故方法２００のステップに、マッピングされることができる。

【００６４】

図２を参照しながら以上に説明された方法２００においては、セッション鍵を用いて暗号化されたメッセージを受信するステップ２０６は、適切な候補ノードが見出されたときにのみ実行される。１つ以上のノードが、元の装置１０２ａによりブロードキャストされたメッセージに応答することが可能であり得るが、方針における要件を満たさず、それ故元の装置１０２ａに応答することが可能ではない１つ以上のノードがあり得る。図５は、データが複製される先となるネットワーク内のネットワークノードを識別するための方法の例を示すフロー図である。具体的には、方法５００は、ネットワークノードが、暗号化されたメッセージによって元の装置に応答することができない場合に、元の装置１０２ａにおいて実行される処理の例を示す。方法５００は、方法２００のステップ２０２乃至２０８を含んでも良い。方法５００は、選択されたネットワークノード以外の該ネットワーク内の特定のネットワークノードから、暗号化されたセッション鍵が当該特定のネットワークノードによって復号化されることができなかったことを示すメッセージを受信するステップを有する。斯くして、元の装置によりブロードキャストされたセッション鍵を復号化することができないネットワークノードは、該ノードが該セッション鍵を復号化できないことを確認するメッセージを該元の装置に送信し得る。

【００６５】

ネットワーク１００のなかのネットワークノード１０２ｂ乃至ｇは、元の装置１０２によりブロードキャストされているメッセージに応答して種々のステップを実行しても良い。図６は、ネットワーク内のデータ複製を容易化するための方法６００の例を示す。方法６００は、ネットワークノードにおける処理装置により実行されても良い。方法６００は、ステップ６０２において元の装置からメッセージを受信するステップを有し、該メッセージは、属性ベースの暗号化スキームに従って暗号化されたセッション鍵を含む。該受信されるメッセージは、上述した方法２００のステップ２０４の間に元の装置によりブロードキャストされたセッション鍵であっても良いし、又は該セッション鍵を含んでも良い。該元の装置は、元装置とも呼ばれ得る。

【００６６】

ステップ６０４において、方法６００は、方針鍵を用いて該メッセージを復号化することを試みるステップを有する。方針鍵は、属性ベースの暗号化において用いられる秘密鍵である。従って、方針鍵は秘密鍵とも呼ばれ得る。本例においては、該方針鍵は、属性のセットから導出される秘密鍵であり、該方針鍵は、暗号化のために用いられる方針がこれらの属性に合致する場合に、属性ベースの暗号文を復号化することができる。

【００６７】

該方法は、ステップ６０６において、メッセージを復号化する試みが成功したか否かを決定するステップを有する。ステップ６０８において、方法６００は、メッセージを復号化する試みが成功したとの決定に応答して、方針鍵に従って返答メッセージを暗号化するステップを有する。ステップ６１０において、方法６００は、元の装置に返答メッセージを

送信するステップを有する。斯くして、元の装置からのメッセージを受信したネットワークノードが該メッセージを復号化することが可能である場合、該ノードは該元の装置に暗号化されたメッセージ（方針鍵を用いて暗号化されたもの）を送信する。上述したように、該方針鍵は、ネットワークノードが元の装置からのデータを複製するために満たさなければならない要件を定義する特定の方針に従って生成された秘密鍵である。

【００６８】

方法６００の暗号化するステップ６０８及び送信するステップ６１０は、ネットワークノードが元の装置からのメッセージを復号化することが可能である場合に実行される。元の装置によりブロードキャストされたメッセージを復号化することができないネットワークノードは、何も動作を実行しなくても良いし、又は別の態様で該元の装置に応答しても良い。図７は、ネットワーク内のデータ複製を容易化するための方法の例７００のフロー図である。方法７００は、方法６００の１つ以上のステップを含んでも良い。方法７００は、ステップ７０２において、メッセージを復号化する試みが失敗したとの決定に応答して、元の装置に、復号化が失敗したことの示唆を送信するステップを有する。

【００６９】

方法２００を参照しながら上述したように、セッション鍵を暗号化するために用いられる属性は、１つ以上の地理的な位置を規定する地理位置方針を有する。方針鍵は、処理装置が位置する地理的な位置に特有のものであっても良い。

【００７０】

図８は、ネットワーク内のデータ複製を容易化するための方法の例８００のフロー図である。方法８００は、方法６００及び方法７００の１つ以上のステップを含んでも良い。方法８００は、ステップ８０２において、処理装置が位置する地理的な位置に割り当てられた鍵サーバを識別するステップを有する。ステップ８０４において、方法８００は、該鍵サーバを用いて認証するステップを有しても良い。方法８００は、ステップ８０６において、該鍵サーバから方針鍵を受信するステップを有しても良い。斯くして、幾つかの実施例においては、１つ以上のネットワークノードが、方針鍵を所有し得るが、他の実施例においては、ネットワークノードは、該ノードに関連する又は該ノードが位置する場所に関連する鍵サーバのような鍵サーバと通信し、該鍵サーバから方針鍵を取得し得る。

【００７１】

ネットワーク内のデータ複製を容易化するための方法の更なる例９００が、図９のフロー図に示されている。方法９００は、方法６００、方法７００及び方法８００の１つ以上のステップを含んでも良い。方法９００は、ステップ９０２において、元の装置から複製されるべきデータを受信するステップを有する。ステップ９０４において、方法９００は、後のアクセスのために、該複製されるべきデータを保存するステップを有しても良い。複製されたデータは、ネットワークノードに関連する記憶媒体に保存されても良い。例えば、複製されたデータは、ネットワークノードに位置する装置の記憶装置に保存されても良いし、又は該ノードに関連するサーバに保存されても良い。

【００７２】

以上に説明された方法に加えて、本発明の更なる態様は、該方法を実行するための装置に関する。図１０は、以上に説明された方法を実行するための機器又は装置の例の簡略化された模式図である。装置１０００は、通信インタフェース１００２、メモリ１００４及びプロセッサ１００６を有する。装置１０００は、例えばコンピューティング装置又はサーバを有しても良い。プロセッサ１００６は、以上に説明された方法２００、５００のステップを実行するよう構成されても良い。このようにして、装置１０００は、元の装置又は元のノード１０２ａとして機能し得る。代替としては、該プロセッサは、以上に説明された方法６００、７００、８００、９００のステップを実行するよう構成されても良い。このようにして、装置１０００は、目的のノード、又は複製先のノード１０２ｂ乃至ｇ（即ちデータが複製されるべきノード、又は複製の試みが為されるべきノード）として機能し得る。

【００７３】

本発明の更なる態様は、持続性機械読み取り可能媒体に関する。図１１は、持続性機械読み取り可能媒体１１０２及びプロセッサ１００６を模式的に示す。持続性機械読み取り可能媒体１１０２は、プロセッサ１００６による実行のための命令をエンコードされている。該持続性機械読み取り可能媒体は、以上に説明された方法２００、５００、６００、７００、８００及び／又は９００のいずれかを実行するための命令を有する。

【００７４】

ここで説明されたシステム及び方法は、より短い、それ故より高速なプロトコルを用いることにより、データの高速な複製を実行する。３つの異なるプロトコル交換（発見、認証、鍵照合）を含む既知の方法は、一般に更に多くのステップを含み、それ故低速である。例えば、既知の方法は、９個のステップを含み得る。

【００７５】

斯かるデフォルトの方法のプロトコルに比べると、ここで説明されたシステム及び方法は、種々の実施例が、単一の交換の２ステップのプロトコルに発見、認証及び鍵照合を組み込んでおり、より効率が良いという事実に少なくとも部分的に基づいて、より優れた性能を実現することができる。種々の実施例は、１つのプロトコル交換のみしか利用せず、該１つの交換は、発見ブロードキャストを満たすサーバによって完了される必要があるのみである。種々の実施例においては、複製のために選択されたネットワークノードが、元の装置により送信された発見メッセージを復号化することが可能であることにより、該ノード自身を元の装置に対して認証する。該復号化は、属性ベースの認可者からの秘密鍵の取得に基づく。幾つかの実施例においては、複製のために選択されたノードの属性は、必ずしも正確に方針における属性と合致する必要はない。例えば、方針における属性として地理位置が用いられる場合、正確な地理位置は困難であることは知られているため、該位置は地理位置に完全に合致する必要はなくても良い。ファジー手法が用いられても良い。例えば、ノードが定義された地理位置から５０キロメートル位内にある場合には、該ノードは方針における地理位置に位置しているとみなされても良い。

【００７６】

他のローカルな病院サーバに付随された、多クラウドシステムにおける複製は、例えばトランスポート層セキュリティ（ＴＬＳ）プロトコルを用いた、異なるタイプのシステム間の統合を必要とし得る。斯かる要件は、ここで説明された種々の実施例においては除去される。ここで説明された新たに挿入されるプラットフォーム非依存のプロトコルは、コンピューティングプロバイダ間の密な統合に依存しないため、異質な（例えば多クラウドの状況）システムにも容易に統合され得る。種々の実施例は、あり得る通信及び多クラウドシステムについて展開された規定に依存することなく、暗号化されたコンテンツの交換及びピアツーピア接続されたノード（例えばＶＭ）にのみ基づく。例えば、発見フェーズは、プラットフォーム依存ではない暗号化されたメッセージの送信にのみ依存する。

【００７７】

種々の実施例は、該プロトコルを実行する時点の現在のトポロジに関連する発見処理を用いるため、過去に生じたものであり得る動的な変化を自動的に考慮に入れる。更に、種々の実施例は、当該発見を調整する中央エンティティを持つ必要なく、場所（データが複製されることが許可された場所）の分散された発見を実現する。

【００７８】

種々の実施例は、クラウド、更には、クラウド／多クラウドシステムが信頼して全てのサービスレベル合意（ＳＬＡ）を履行させる、とり得る多クラウド展開を信頼する必要がなく、複製が許可された地理的な領域のみを利用する。更に、地理位置属性ベースの暗号化の認証のため、ファジーな認証手法は、種々の認可者間で、又は種々の地理位置測定（例えばping、hops等）について秘密鍵を解放する半信用されたランドマーク間で、信用を分割し得る。上述したように、該信用は、元のノードと複製ノードとの間に生成されたセキュアなトンネルに対する失効日の使用によって、更に消散させられ得る。セキュアなトンネルが失効すると、新たな鍵が交渉される。このようにして、発見処理の安全性が向上させられる。更に、当該失効は、より好適な（例えばより近い）複製ノードを発見し得る

発見処理を起動する。

【００７９】

種々の実施例は、クラウドのメッシュ、そのセキュリティ方法、セキュリティ方法の統合、ＳＬＡ及び協調ＳＬＡから、明確なプロトコルの信頼へと、信用を移す。該プロトコルの簡潔さ及び明確さは、攻撃面を最小化する。このことは、認可者及び鍵生成者へと信用を移す。

【００８０】

全てのユーザに完全に信頼され、ユーザの属性を信頼性高く監視する、単一の認可者を利用することは、小さなシステムにおいては合理的である。しかしながら、相互接続された健康システムのような大型の分散されたシステムについては、このことは当てはまらない場合がある。この問題に対処するため、多認証局鍵生成システム（ＭＡ－ＫＧＳ）が提案されている。これらのシステムにおいては、特定の属性に関するユーザの秘密鍵の一部を生成するタスクが、いわゆる鍵生成局（key Generation Authorities、ＫＧＡ）により実行される。認可者により生成されたシステムに亘る公開鍵とは別に、各鍵生成局は、その属性のそれぞれについて属性公開鍵を生成する。ユーザは、担当する属性（のサブセット）について各ＫＧＡから秘密鍵部分を要求する。幾つかのシステムにおいては、ユーザはまた、認可局からユーザ秘密鍵を最初に要求する。ユーザは、全てのＫＧＡから受信された秘密鍵の各部分を１つの秘密鍵へと統合する。それ故、悪意のあるＫＧＡは、限られた数の属性についてしか、秘密鍵を発行できない。しかしながら、ＫＧＡの鍵材料が損なわれると、該材料が他のユーザの秘密鍵と組み合わせられ、本来ならアクセス可能ではない材料へのアクセスが得られてしまうため、依然としてリスクをもたらす。

【００８１】

ＫＧＡの鍵材料が損なわれ、それにより必要とされるＫＧＡにおける信用のレベルが低減するリスクを低減させるため、多認証局鍵生成システムが用いられても良い。斯かるシステム（例えば図４に示される）においては、ユーザは、発見メッセージを復号化することを可能とするため、多数のＫＧＡから秘密鍵を受信する必要がある。これらの秘密鍵は、地理位置属性の種々のサブセット（例えばping時間、hops数、ＩＰアドレス、ＤＮＳ）に関連付けられる。セキュアな分散された鍵生成方法は、複製ノードに秘密鍵を提供するためにも利用され得る。

【００８２】

種々の実施例は、データの複製が必要とされる場合、及び当該データが許可された場所においてのみ複製されるべきである場合に、用いられることができる。ここで説明されたシステム及び方法は、データが複製される必要がある場所に暗号化された鍵を送信することによって鍵の照合を可能とするため、単に認証された発見について一般化され得る。該暗号化は地理位置とは異なる属性を用いて為されても良く、ファジーな認証が利用されても良い。種々の実施例は、コンピューティングプロバイダ（例えばクラウドプロバイダ、病院サーバ）間に新たに統合された方法を展開することに依存せず、プラットフォーム非依存である暗号化プロトコルにのみ依存する。

【００８３】

上述したように、種々の実施例によれば、持続性媒体（例えば揮発性又は不揮発性メモリ）は、ここで説明された機能を実行するためのプロセッサ（例えばマイクロプロセッサ又はその他の同様のハードウェア装置）による実行のための命令をエンコードされても良い。例えば、斯かる命令は、以下の疑似コードに少なくとも部分的に対応しても良い。

```
Origin:
replReqID = random identifier number;
Policy = get_geolocation_requirement(plaintext);
sessionKey = generate fresh session key;
discovery_message=(replReqID, Policy, sessionKey);
ciphertext = fuzzy_encrypt(Policy, discovery_message);
broadcast (policy,ciphertext);     //(ネットワークレベル/面)
```

```
Targets:
(policy, ciphertext) = received_broadcast();
geolocation = fetch known geolocation from cloud provider;
if (geolocation in policy) {        //ポリシー例: TODO later
abeSecretKey = get secret key from Key Generation Authority;
(repReqID, Policy, sessionKey) = fuzzy_decrypt(ciphertext);
response=(src, dst, Policy);
//ここでsrc = source, dst = destination
encrypted_response = encrypt(sessionKey, response)
send_to_origin(encrypted_response);
}
Origin:
responses = receive encrypted responses;
//応答を復号化し候補のリストを取得
candidates_VMs = decrypt(sessionKey, responses);
//発見メッセージを正しく復号化したものからランダムに選択
selected_VMs = select VMs where to replicate the data;
encrypted_data = encrypt(sessionKey, data);
send_to_selected_VMs(encrypted_data)
Targets:
encrypted_data = receive encrypted replicated data;
data = decrypt(sessionKey, encrypted_data);
```

【００８４】

以上の説明から、本発明の種々の実施例がハードウェア又はファームウェアで実装され得ることは、明らかである。更に、種々の実施例は、ここで詳細に説明された動作を実行するために少なくとも１つのプロセッサにより読み取られ実行され得る、機械読み取り可能な記憶媒体に保存された命令として実装され得る。機械読み取り可能な記憶媒体は、パーソナルコンピュータ、ラップトップ型コンピュータ、サーバ又はその他の計算装置のような、機械により読み取り可能な形で情報を保存するための、いずれの機構を含んでも良い。従って、機械読み取り可能な記憶媒体は、読み取り専用メモリ（ＲＯＭ）、ランダムアクセスメモリ（ＲＡＭ）、磁気ディスク記憶媒体、光記憶媒体、フラッシュメモリ装置、及び同様の記憶媒体を含み得る。

【００８５】

ここでのいずれのブロック図もが、本発明の原理を実施化する回路の例の概念図を表すことは、当業者により理解されるべきである。同様に、いずれのフロー図、フローダイアグラム、状態遷移図、疑似コード等もが、機械読み取り可能な媒体に略表され、明示的に示されているか否かにかかわらずコンピュータ又はプロセッサによりそのように実行可能な種々の処理を表すことは、理解されるであろう。

【００８６】

種々の実施例は、特定の態様を具体的に参照しながら詳細に説明されたが、本発明は他の実施例でも可能なものであり、本発明の詳細は種々の明白な観点で変更が可能であることは、理解されるべきである。当業者には明白であるように、本発明の精神及び範囲内に留まりつつ変形及び変更が実現可能である。従って、以上の開示、説明及び図は、単に説明の目的のためのものであり、いずれの態様においても、請求項によってのみ定義される本発明を限定するものではない。

【図面】

【図１】

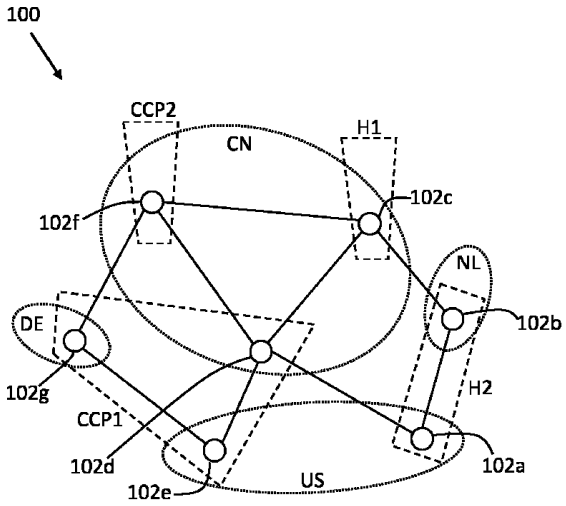


Figure 1

【図２】

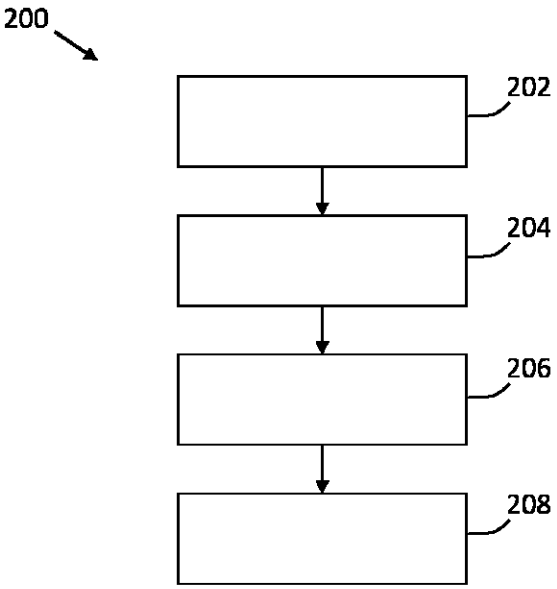
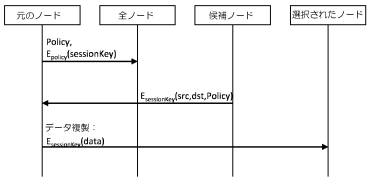
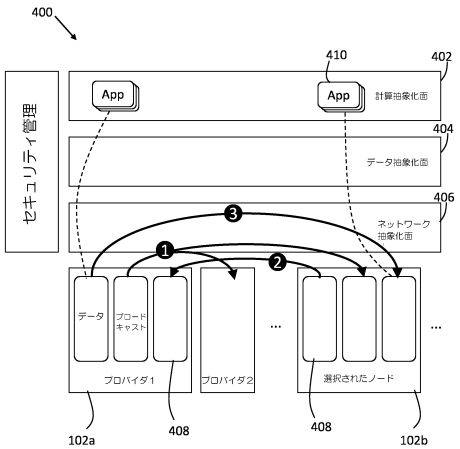


Figure 2

【図３】



【図４】



【図５】

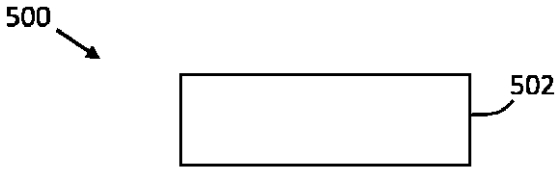


Figure 5

【図６】

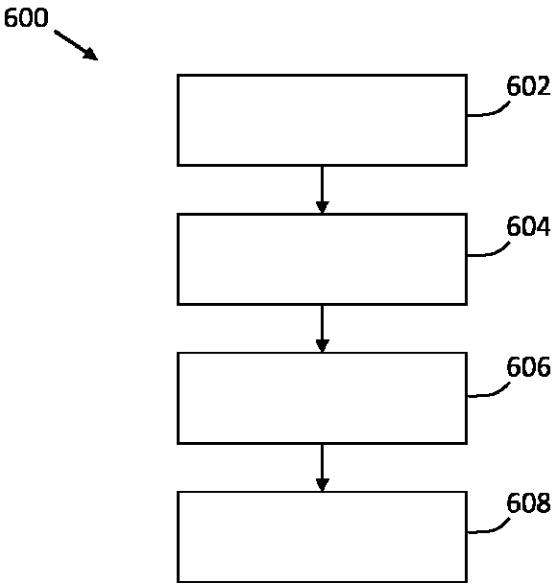


Figure 6

【図７】

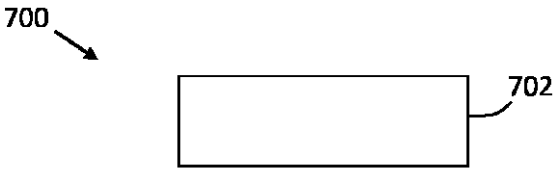


Figure 7

【図８】

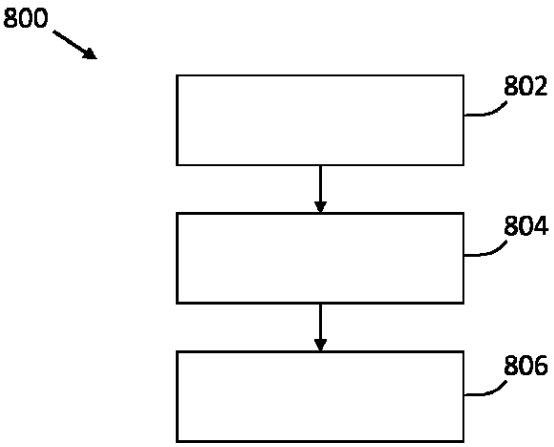


Figure 8

【図９】

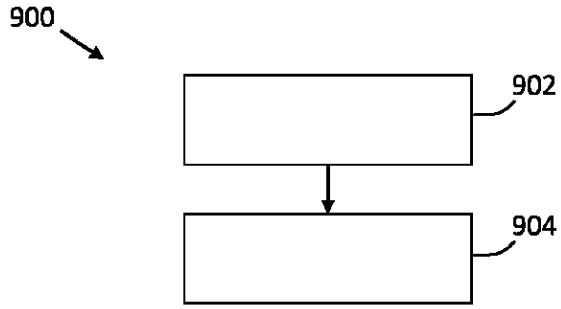


Figure 9

【図１０】

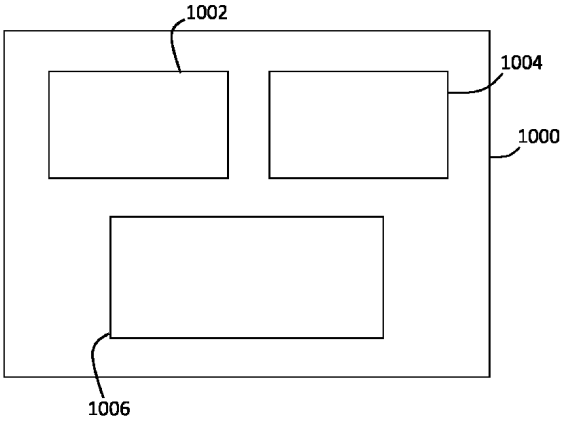


Figure 10

【図１１】

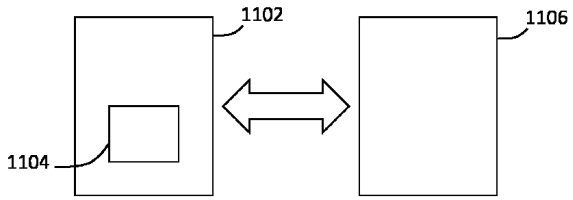


Figure 11

フロントページの続き

(33)優先権主張国・地域又は機関
米国(US)
弁理士　矢ヶ部 喜行
(72)発明者　プレテア ダニエル
オランダ国 ５６５６ アーエー アインドーフェン ハイ テック キャンパス ５
(72)発明者　ファン リースドンク ペーター ペトルス
オランダ国 ５６５６ アーエー アインドーフェン ハイ テック キャンパス ５
審査官　行田 悦資
(56)参考文献　特開２０１２－０４３２２４（ＪＰ，Ａ）
特開２００６－１５５０８２（ＪＰ，Ａ）
米国特許出願公開第２０１１／００７２２０６（ＵＳ，Ａ１）
WANG, C. et al.，Implementing a Personal Health Record Cloud Platform Using Ciphertext-Policy Attribute-Based Encryption，2012 Fourth International Conference on Intelligent Networking and Collaborative Systems，IEEE，2012年09月19日，pp.8-14，〈DOI:10.1109/iNCoS.2012.65〉
(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　９／０８
Ｇ０６Ｆ　２１／４４