

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7558911号
(P7558911)

(45)発行日 令和6年10月1日(2024.10.1)

(24)登録日 令和6年9月20日(2024.9.20)

(51)国際特許分類

F I

H O 4 L 9/08 (2006.01) H O 4 L 9/08 B

H O 4 L 9/12 (2006.01) H O 4 L 9/12

請求項の数 5 (全24頁)

(21)出願番号	特願2021-148022(P2021-148022)	(73)特許権者	000003078 株式会社東芝 東京都港区芝浦一丁目1番1号
(22)出願日	令和3年9月10日(2021.9.10)	(73)特許権者	301063496 東芝デジタルソリューションズ株式会社 神奈川県川崎市幸区堀川町72番地34
(65)公開番号	特開2023-40843(P2023-40843A)	(74)代理人	110001737 弁理士法人スズエ国際特許事務所
(43)公開日	令和5年3月23日(2023.3.23)	(72)発明者	長嶋 悠貴 神奈川県川崎市幸区堀川町72番地34 東芝デジタルソリューションズ株式会社 内
審査請求日	令和6年3月27日(2024.3.27)	(72)発明者	澤崎 武 神奈川県川崎市幸区堀川町72番地34 東芝デジタルソリューションズ株式会社 最終頁に続く

(54)【発明の名称】 クラウド鍵管理サービス基盤システム

(57)【特許請求の範囲】

【請求項1】

非量子鍵の暗号鍵を管理するクラウド鍵管理サービスを含む各種サービスを提供するクラウドシステム上で前記クラウド鍵管理サービスのインターフェースに準じた拡張インターフェースによる量子鍵の提供を含む量子暗号通信サービスを提供するクラウド鍵管理サービス基盤システムであって、

前記クラウドシステムは、前記量子暗号通信サービスの提供拠点となる複数のデータセンタを有し、前記複数のデータセンタによって、各々が1以上のデータセンタで形成される複数のサービスエリアを設定し、

前記複数のデータセンタのそれぞれは、

直接的に接続されている他のデータセンタとの間の量子暗号通信のための量子鍵であるQ鍵を生成して前記他のデータセンタとの間で共有化する量子鍵配送システムと、

量子暗号通信を行うユーザに提供する量子鍵であるG鍵を、前記他のデータセンタとの間で前記Q鍵を用いた量子暗号通信によって送受信する量子鍵流通システムと、

前記G鍵をサービスエリア単位で管理する鍵管理システムと、を具備し、

前記鍵管理システムは、ユーザからの前記G鍵の要求を前記拡張インターフェースによって受け付け、量子鍵用の鍵提供API(Application Programming Interface)によって前記量子鍵流通システムから取得した前記G鍵を当該ユーザに提供し、

第1サービスエリア内の各データセンタは、前記第1サービスエリア内の他のデータセ

ンタと協働して、前記第1サービスエリア内の他のユーザとの間で量子暗号通信を行う前記第1サービスエリア内のユーザ向けの第1 G 鍵を生成し、または、前記第1サービスエリア内および前記第1サービスエリアと異なる第2サービスエリア内の他のデータセンタと協働して、前記第2サービスエリア内の他のユーザとの間で量子暗号通信を行う前記第1サービスエリア内のユーザ向けの第2 G 鍵を生成し、

前記複数のサービスエリア内の任意の2点間で量子暗号通信を行う両ユーザに対して当該2点間で共有化された前記第1 G 鍵または前記第2 G 鍵を前記拡張インターフェースによって提供するクラウド鍵管理サービス基盤システム。

【請求項2】

前記第1サービスエリア内の各データセンタは、前記第1サービスエリア内の他のデータセンタと協働して、前記第1サービスエリア内での前記第1 G 鍵および前記第2 G 鍵のレプリケーションを実行する請求項1に記載のクラウド鍵管理サービス基盤システム。

【請求項3】

前記クラウド鍵管理サービスのインターフェースは、マスターキーの指定を含むエンベロップ暗号化のためのインターフェースであり、前記拡張インターフェースは、前記マスターキーの属性情報として少なくとも通信先のサービスエリアが追加されている請求項1または2に記載のクラウド鍵管理サービス基盤システム。

【請求項4】

前記拡張インターフェースは、前記エンベロップ暗号化でのデータキーとして前記 G 鍵が適用され、かつ、鍵情報として前記 G 鍵の識別子が適用される請求項3に記載のクラウド鍵管理サービス基盤システム。

【請求項5】

前記量子鍵用の鍵提供APIは、ETSI GS QKD 014 準拠の鍵提供APIである請求項1～4のいずれか1項に記載のクラウド鍵管理サービス基盤システム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明の実施形態は、クラウド鍵管理サービス基盤システムに関する。

【背景技術】

【0002】

近年、通信経路上でのデータの漏洩を防止するために、データを暗号化して送受信する暗号通信が広く行われている。暗号通信でデータの保護を図るためには、たとえば複数の拠点間で共有する暗号鍵の管理も重要である。このようなことから、インターネット経由で暗号鍵の管理サービスを提供するクラウドシステムが登場するに至っている。

【0003】

また、最近では、量子力学の原理を利用して暗号鍵（量子鍵）を2拠点間で安全に共有することができる量子鍵配送（QKD: Quantum Key Distribution）が注目を集めている。量子鍵配送は、光子の挙動を利用する技術であり、光ファイバなどを媒体として2拠点間で光子によって暗号鍵情報を送受信する。量子鍵配送によって2拠点間で共有化された量子鍵を用いた当該2拠点間における暗号通信は、量子暗号通信などと称される。量子暗号通信に関しては、ETSIにおいて鍵提供API（Application Programming Interface）が標準化されるに至っている（ETSI GS QKD 014）。

【先行技術文献】

【特許文献】

【0004】

【文献】特許第6609010号公報

【発明の概要】

【発明が解決しようとする課題】

【0005】

10

20

30

40

50

量子暗号通信の導入にあたっては、量子鍵配送で光ファイバの敷設が必要となる等、ユーザによっては、量子暗号通信のための設備を独自に構築することはコスト的に困難な場合がある。従って、既存の非量子鍵の暗号鍵管理サービスと同様に、クラウドサービスとして、量子鍵の提供を含む暗号鍵管理サービスが提供されることを望む声も多い。

【0006】

しかし、量子鍵配送は2拠点間での量子鍵の共有を前提としている。一方、既存の非量子鍵の暗号鍵管理サービスを含む各種サービスを提供するクラウドシステムは、ある程度の地理的範囲毎に1以上のデータセンタによってサービスエリアを形成し、当該サービスエリア毎に各種サービスを提供・管理することが一般的である。そして、クラウドシステムでは、各種サービスを提供・管理する拠点が、各サービスエリアを形成するデータセンタの論理的な集合体で表現される。なお、クラウドシステムは、狭域のサービスエリアを下位層とし、複数の狭域のサービスエリアを含む広域のサービスエリアを上位層とする多階層のサービスエリアを設定する場合がある。

10

【0007】

そのため、2拠点間での量子鍵の共有という量子鍵配送の概念は、各拠点が1以上のデータセンタの論理的な集合体で表現されるクラウドシステムには馴染まない。従って、クラウドサービスの1つとして、既存の非量子鍵の暗号鍵管理サービスを、単純に、量子鍵の暗号鍵管理サービスへと移植することはできない。

【0008】

本発明が解決しようとする課題は、クラウドシステム上で量子鍵の提供を含む量子暗号通信サービスを提供するクラウド鍵管理サービス基盤システムを提供することである。

20

【課題を解決するための手段】

【0009】

実施形態によれば、クラウド鍵管理サービス基盤システムは、非量子鍵の暗号鍵を管理するクラウド鍵管理サービスを含む各種サービスを提供するクラウドシステム上でクラウド鍵管理サービスのインターフェースに準じた拡張インターフェースによる量子鍵の提供を含む量子暗号通信サービスを提供する。クラウドシステムは、量子暗号通信サービスの提供拠点となる複数のデータセンタを有し、複数のデータセンタによって、各々が1以上のデータセンタで形成される複数のサービスエリアを設定する。複数のデータセンタのそれぞれは、量子鍵配送システムと、量子鍵流通システムと、鍵管理システムと、を具備する。量子鍵配送システムは、直接的に接続されている他のデータセンタとの間の量子暗号通信のための量子鍵であるQ鍵を生成して他のデータセンタとの間で共有化する。量子鍵流通システムは、量子暗号通信を行うユーザに提供する量子鍵であるG鍵を、他のデータセンタとの間でQ鍵を用いた量子暗号通信によって送受信する。鍵管理システムは、G鍵をサービスエリア単位で管理する。鍵管理システムは、ユーザからのG鍵の要求を拡張インターフェースによって受け付け、量子鍵用の鍵提供API (Application Programming Interface) によって量子鍵流通システムから取得したG鍵をユーザに提供する。第1サービスエリア内の各データセンタは、第1サービスエリア内の他のデータセンタと協働して、第1サービスエリア内の他のユーザとの間で量子暗号通信を行う前記第1サービスエリア内のユーザ向けの第1G鍵を生成し、または、第1サービスエリア内および第1サービスエリアと異なる第2サービスエリア内の他のデータセンタと協働して、第2サービスエリア内の他のユーザとの間で量子暗号通信を行う第1サービスエリア内のユーザ向けの第2G鍵を生成する。クラウド鍵管理サービス基盤システムは、複数のサービスエリア内の任意の2点間で量子暗号通信を行う両ユーザに対して当該2点間で共有化された第1G鍵または第2G鍵を拡張インターフェースによって提供する。

30

40

【図面の簡単な説明】

【0010】

【図1】実施形態のクラウド鍵管理サービス基盤システム（基盤システム）の概要を示す図

【図2】第1比較例の量子暗号通信システムを示す図

50

【図 3】第 2 比較例のクラウドシステムで用いられるエンベロープ暗号化を説明するための図

【図 4】第 2 比較例のクラウドシステムのクラウド鍵管理サービスの概要を示す図

【図 5】第 2 比較例のクラウドシステムのクラウド鍵管理サービスの一利用形態例を示す図

【図 6】第 2 比較例のクラウドシステムによるサービスエリアの一形成例を示す図

【図 7】実施形態の基盤システムでのクラウドシステムへの量子鍵配送の一適用例を示す図

【図 8】実施形態の基盤システムのシステム全体の機能ブロックの一例を示す図

【図 9】実施形態の基盤システムのデータセンタの機能ブロックの一例を示す図

【図 10】実施形態の基盤システムの量子鍵流通システムの機能ブロックの一例を示す図

【図 11】実施形態の基盤システムの量子鍵配送システム 30 の機能ブロックの一例を示す図

10

【図 12】実施形態の基盤システムにおける量子暗号通信サービス利用開始時の動作の流れを示すフローチャート

【図 13】実施形態の基盤システムにおける量子鍵を用いた暗号化を行う場合の動作の流れを示すフローチャート

【図 14】実施形態の基盤システムにおける量子鍵を用いた復号を行う場合の動作の流れを示すフローチャート

【図 15】実施形態の基盤システムにおける量子暗号通信サービス利用終了時の動作の流れを示すフローチャート

【図 16】実施形態の基盤システムの第 1 ユースケースを示す図

20

【図 17】実施形態の基盤システムの第 2 ユースケースを示す図

【図 18】実施形態の基盤システムの第 3 ユースケースを示す図

【発明を実施するための形態】

【0011】

以下、実施の形態について、図面を参照して説明する。

図 1 は、実施形態のクラウド鍵管理サービス基盤システム 1 の概要を示す図である。図 1 には、ユーザ（A、B）によるクラウド鍵管理サービス基盤システム 1 の利用イメージが併せて示されている。なお、以下、クラウド鍵管理サービス基盤システム 1 を、単に、基盤システム 1 と称することがある。基盤システム 1 は、インターネット経由で各種サービスを提供するクラウドシステム上で量子鍵の提供を含む量子暗号通信サービスを提供する。

30

【0012】

図 1 では、ユーザ A が、基盤システム 1 から量子鍵（a1）を取得し、当該取得した量子鍵でデータを暗号化してユーザ B へ送信する。一方、ユーザ B も、基盤システム 1 から量子鍵を取得し、暗号化されたデータを復号する。つまり、ユーザ A とユーザ B とが、基盤システム 1 から量子鍵の提供を受けて量子暗号通信（a2）を行う。

【0013】

換言すれば、基盤システム 1 は、クラウドシステムのサービスエリア内の任意の 2 点間で量子暗号通信を行うユーザ A とユーザ B とのそれぞれに対して、両者が共有すべき量子鍵をクラウドサービスとして提供する。

40

【0014】

クラウドシステムは、複数のデータセンタ 100 でサービスエリアを形成する。複数のデータセンタ 100 のそれぞれは、鍵管理システム（KMS：Key Management Service）10 と、量子鍵流通システム 20 と、量子鍵配送システム 30 とを有する。なお、以下、量子鍵流通システム 20 および量子鍵配送システム 30 を、QKD システムと総称することがある。

【0015】

鍵管理システム 10 は、既存の非量子鍵の暗号鍵管理サービスに加えて、量子鍵の暗号鍵管理サービスを提供する機能を有する。鍵管理システム 10 は、ユーザが通信相手との間で共有すべき量子鍵を、たとえば ETSI GS QKD 014 準拠の鍵提供 API に

50

よって量子鍵流通システム20から取得し、既存の非量子鍵の暗号鍵管理サービスのインターフェースに準じた拡張インターフェースによってユーザに提供する。従って、ユーザは、量子鍵用の鍵提供APIを持つ必要がなく、非量子鍵の暗号鍵管理サービス用の既存のインターフェースに準じた拡張インターフェース(a3)で量子鍵を取得することができる。既存のインターフェースや拡張インターフェースについては後述する。以下、非量子鍵の暗号鍵管理サービスおよび量子鍵の暗号鍵管理サービスを、クラウド鍵管理サービスと総称することがある。

【0016】

量子鍵流通システム20は、ユーザに提供する量子鍵を生成し、ユーザの実質的な窓口となっているデータセンタ100間で当該量子鍵を共有化するための通信を実行する。具体的には、量子鍵流通システム20は、隣接する、即ち直接的に接続されているデータセンタ100（または中継拠点）の量子鍵流通システム20との間で、ユーザに供給する量子鍵を量子暗号通信によって送受信する。つまり、量子鍵は、たとえば複数のデータセンタ100（または中継拠点）の量子鍵流通システム20の中継を経て、ユーザの実質的な窓口となっているデータセンタ100間で送受信される。

【0017】

量子鍵配送システム30は、量子鍵流通システム20が他の量子鍵流通システム20との間で量子暗号通信を行うための量子鍵を生成する。量子鍵配送システム30は、他の量子鍵配送システム30と協働して、量子鍵流通システム20の量子暗号通信のための量子鍵の共有化を実行する。

【0018】

つまり、基盤システム1は、水面下で、量子鍵の中継を適応的に行うことで、クラウドシステムのサービスエリア内の任意の2点間で量子暗号通信を行う両ユーザに対して、両者が共有すべき量子鍵を供給することを実現している。量子鍵の中継を量子暗号通信で行うことで、当該量子鍵の保護も図っている。以下、ユーザに提供する量子鍵をG鍵(Global key)と称することがあり、G鍵の暗号化のための量子鍵をQ鍵(Quantum key)と称することがある。

【0019】

ここで、図2を参照して、第1比較例について説明する。第1比較例は、ETSI GSKD 014準拠の鍵提供APIによってユーザへ量子鍵を提供する量子暗号通信システムである。図2中、二重線の枠は、物理的にセキュリティが確保された拠点であることを表している。

【0020】

暗号アプリなどの暗号化処理を行う主体(master SAE [Secure Application Entity])は、復号アプリなどの復号処理を行う主体(slave SAE)の識別子(slave SAE ID)をパラメータ等として含む量子鍵の要求を、自拠点の量子鍵流通システム(量子鍵流通システム_x)20に対して鍵提供APIによって送信する(1)。この要求を受信した量子鍵流通システム20は、量子鍵(G鍵)と、量子鍵の識別子(鍵ID)とをmaster SAEに送信する(2)。

【0021】

master SAEは、量子鍵流通システム20から受け取った量子鍵でデータを暗号化し(3)、slave SAEに対して、暗号データと、その暗号データの暗号化に用いた量子鍵の鍵IDとを送信する(4)。

【0022】

一方、slave SAEは、master SAEの識別子(master SAE ID)と、master SAEから受信した鍵IDとをパラメータ等として含む量子鍵の要求を、自拠点の量子鍵流通システム(量子鍵流通システム_z)20に対して鍵提供APIによって送信する(5)。この要求を受信した量子鍵流通システム20は、鍵IDで示される量子鍵(G鍵)をslave SAEに送信する(6)。

【0023】

s l a v e S A Eは、量子鍵流通システム20から受け取った量子鍵を用いて、m a s t e r S A Eから受信した暗号データを復号する(7)。

【0024】

ここでは、m a s t e r S A Eの拠点とs l a v e S A Eの拠点との間に1つの中継拠点が介在しているものと想定する。m a s t e r S A Eの拠点の量子鍵配送システム(量子鍵配送システム_A)30は、中継拠点の量子鍵配送システム(量子鍵配送システム_B)30との間でQ鍵(Q鍵_{AB})の共有化を実行する。また、s l a v e S A Eの拠点の量子鍵配送システム(量子鍵配送システム_D)30は、中継拠点の量子鍵配送システム(量子鍵配送システム_C)30との間でQ鍵(Q鍵_{CD})の共有化を実行する。

【0025】

m a s t e r S A Eの拠点の量子鍵流通システム(量子鍵流通システム_X)20は、中継拠点との間で共有化されているQ鍵(Q鍵_{AB})を用いて、m a s t e r S A Eに提供した量子鍵(G鍵)を暗号化し、中継拠点の量子鍵流通システム(量子鍵流通システム_Y)20に送信する。なお、m a s t e r S A Eの拠点の量子鍵流通システム(量子鍵流通システム_X)20は、パラメータ等として受け取ったs l a v e S A E I Dに基づき、s l a v e S A Eの拠点の量子鍵流通システム(量子鍵流通システム_Z)20を認識し、その上で、量子鍵(G鍵)の直接的な送信先として、中継拠点の量子鍵流通システム(量子鍵流通システム_Y)20を特定する。

【0026】

中継拠点の量子鍵流通システム(量子鍵流通システム_Y)20は、Q鍵(Q鍵_{AB})を用いて、m a s t e r S A Eの拠点の量子鍵流通システム(量子鍵流通システム_X)20から受信した、暗号化された状態の量子鍵(G鍵)を復号する。そして、中継拠点の量子鍵流通システム(量子鍵流通システム_Y)20は、s l a v e S A Eの拠点との間で共有化されているQ鍵(Q鍵_{CD})を用いて、量子鍵(G鍵)を再暗号化し、s l a v e S A Eの拠点の量子鍵流通システム(量子鍵流通システム_Z)20に送信する。中継拠点の量子鍵流通システム(量子鍵流通システム_Y)20は、m a s t e r S A Eの拠点の量子鍵流通システム(量子鍵流通システム_X)20によって設定された量子鍵(G鍵)の宛先情報に基づき、s l a v e S A Eの拠点の量子鍵流通システム(量子鍵流通システム_Z)20へ量子鍵(G鍵)を送信すべきことを認識する。

【0027】

s l a v e S A Eの拠点の量子鍵流通システム(量子鍵流通システム_Z)20は、Q鍵(Q鍵_{CD})を用いて、中継拠点の量子鍵流通システム(量子鍵流通システム_Y)20から受信した、暗号化された状態の量子鍵(G鍵)を復号する。そして、s l a v e S A Eの拠点の量子鍵流通システム(量子鍵流通システム_Z)20は、パラメータ等として受け取ったm a s t e r S A E I Dで示されるm a s t e r S A Eの拠点の量子鍵流通システム(量子鍵流通システム_X)20との間で共有化されている量子鍵(G鍵)であって、同じくパラメータ等として受け取った鍵I Dで示される量子鍵(G鍵)を、s l a v e S A Eに供給する。

【0028】

この第1比較例の、E T S I G S Q K D 014準拠の鍵提供A P Iを適用した量子暗号通信システムでは、ユーザが、鍵提供A P Iに対応したアプリケーション(暗号アプリや復号アプリ)を使用する必要がある。

【0029】

続いて、図3から図5を参照して、第2比較例について説明する。第2比較例は、既存の非量子鍵の暗号鍵管理サービス(クラウド鍵管理サービス)を提供するクラウドシステムである。

【0030】

クラウド鍵管理サービスでは、一般的に、鍵管理システム10を介した鍵の共有が、エンベロップ暗号化を利用して行われる。図3は、エンベロップ暗号化を説明するための図である。

10

20

30

40

50

【0031】

エンベロープ暗号化は、暗号鍵をさらに別の鍵で暗号化することである。データの暗号化・復号に用いられる鍵は、データキーなどと称される。また、データキーの暗号化・復号に用いられる鍵は、マスターキーなどと称される。鍵管理システム10は、マスターキーを保存・管理する機能を有する。鍵管理システム10は、マスターキーによって暗号化が施されるデータキーの保存・管理は行わない。

【0032】

図3(A)は、エンベロープ暗号化を利用する鍵管理システム10におけるデータキーの暗号化の概要を示している。

【0033】

鍵管理システム10は、たとえば暗号通信を行う送信側ユーザと受信側ユーザとのうちの送信側ユーザからの要求に応じて、データの暗号化に用いるデータキーをマスターキーによって暗号化する。たとえば暗号通信を行う送信側ユーザと受信側ユーザとは、鍵管理システム10によって暗号化されたデータキー（暗号化済みデータキー）を、当該データキーによって暗号化したデータと共に共有する。なお、送信側ユーザと受信側ユーザとによるデータの共有は、暗号通信に限らず、たとえば記憶装置を介して授受するものであってもよい。

【0034】

図3(B)は、エンベロープ暗号化を利用する鍵管理システム10における暗号化済みデータキーの復号の概要を示している。

【0035】

鍵管理システム10は、たとえば暗号通信を行う送信側ユーザと受信側ユーザとのうちの受信側ユーザからの要求に応じて、暗号化済みデータキーをマスターキーによって復号する。受信側ユーザは、鍵管理システム10によって復号されたデータキーを用いて、当該データキーによって暗号化したデータ（暗号データ）を復号する。

【0036】

図4は、エンベロープ暗号化を利用する鍵管理システム10が提供するクラウド鍵管理服务の概要を示す図である。

【0037】

鍵管理システム10は、マスターキー（CMS: Customer Master key）を管理するにあたり、各マスターキーについてアクセスポリシーを設定する。このアクセスポリシーは、たとえば、特定のグループに属するユーザにアクセス権限を付与するといったものであってもよいし、特定のユーザにアクセス権限を付与するといったものであってもよい。あるいは、特定の属性を持つユーザにアクセス権限を付与するといったものであってもよい。

【0038】

たとえば、あるマスターキーのアクセスポリシーが、あるグループに属するユーザにアクセス権限を付与するといったものであった場合、そのグループに属する各ユーザは、そのマスターキーを介して、当該グループに属する他のユーザとの間でデータを安全に共有することができる。

【0039】

図5は、エンベロープ暗号化を利用する鍵管理システム10が提供するクラウド鍵管理服务の一利用様態例を示す図である。ここでは、あるマスターキーのアクセス権限を持つユーザAとユーザBとが記憶装置を介してデータを共有する場合を想定する。

【0040】

たとえばユーザAは、鍵管理システム10に対して、自身がアクセス権限を持つマスターキー（CMK）を指定して、データキーの暗号化を要求する（1）。この要求を受けた鍵管理システム10は、データキーの生成を行い（2）、かつ、指定されたマスターキーによる当該データキーの暗号化を行う（3）。そして、鍵管理システム10は、データキーと暗号化済みデータキーとをユーザAに提供する（4）。前述したように、鍵管理シス

10

20

30

40

50

テム10は、データキーの保存・管理は行わない。

【0041】

ユーザAは、鍵管理システム10から受け取ったデータキーを用いて、ユーザBと共有するデータ（平文）を暗号化する（5）、ユーザAは、暗号データと暗号化済みデータキーとを記憶装置に保存する（6）。

【0042】

一方、ユーザBは、暗号化済みデータキーを記憶装置から取得し（11）、鍵管理システム10へ送信する（12）。鍵管理システム10は、ユーザBがアクセス権限を持つマスターキーを用いて、暗号化済みデータキーの復号を行い（13）、得られたデータキーをユーザBに提供する（14）。

【0043】

ユーザBは、鍵管理システム10から受け取ったデータキーを用いて、記憶装置に保存されている暗号データの復号を行う（15）。

【0044】

記憶装置に保存されている暗号化済みデータキーは、当該暗号化済みデータキーの暗号化に用いられたマスターキーのアクセス権限を持つユーザのみが復号でき、かつ、データキーは鍵管理システム10にも存在しないので、マスターキーのアクセス権限を持つユーザ間でのデータの安全な共有が実現される。

【0045】

また、図6は、クラウド鍵管理サービスを含む各種サービスを提供するクラウドシステムによるサービスエリアの一形成例を示す図である。

【0046】

クラウドシステムは、たとえば、ゾーンb1、リージョンb2、グローバルb3といった多階層のサービスエリアを設定する。ゾーンb1は、各種サービスの提供拠点となる1以上のデータセンタ100によって形成され、当該ゾーンb1を形成する1以上のデータセンタ100によってゾーンサービスb11が提供される。

【0047】

リージョンb2は、複数のゾーンb1を含む、ゾーンb1の上位層のサービスエリアである。リージョンb2では、当該リージョンb2配下の複数のデータセンタ100によってリージョンサービスb12が提供される。さらに、グローバルb3は、複数のリージョンb2を含む、リージョンb2の上位層のサービスエリアである。グローバルb3では、当該グローバルb3配下の複数のデータセンタ100によってグローバルサービスb13が提供される。

【0048】

つまり、クラウドシステムでは、ゾーンサービスb11、リージョンサービスb12およびグローバルサービスb13の提供拠点が、データセンタ100の論理的な集合体であるゾーンb1、リージョンb2およびグローバルb3として表現される。たとえば、第1ゾーンb1におけるゾーンサービスb11の提供は、現実的には、当該第1ゾーンb1配下のいずれかのデータセンタ100が拠点となって行われるが、その拠点は第1ゾーンとして抽象化される。リージョンサービスb12およびグローバルサービスb13も同様である。

【0049】

以上の第1比較例および第2比較例を踏まえて、次に、図7を参照して、実施形態の基盤システム1が、サービスの提供拠点が各サービスエリアを形成するデータセンタの論理的な集合体で表現されるクラウドシステムに対して、2拠点間で量子鍵を共有する量子鍵配送を適用する一例について説明する。

【0050】

実施形態の基盤システム1では、G鍵を共有する最小単位をリージョンb2とする。基盤システム1は、（1）リージョンb2間でのG鍵の共有のための量子鍵配送、（2）各リージョンb2配下のデータセンタ100間でのG鍵のレプリケーションのための量子鍵

10

20

30

40

50

配送、(3) ユーザと当該ユーザが属するリージョンb2配下のデータセンタ100間でのG鍵の授受のための量子鍵配送、の3種類の量子鍵配送をクラウドシステム上にマッピングする。

【0051】

(2)のG鍵のレプリケーションは、各リージョンb2内のデータセンタ100が協働してG鍵の一貫性を保つための処理を行うことである。このG鍵のレプリケーションによって、G鍵をサービスエリア内でプール化することにより、たとえば第1リージョンb2と第2リージョンb2との間で量子暗号通信を並列に行っている複数組のユーザの各組に対して、当該第1リージョンb2と第2リージョンb2との間で共有化されたG鍵を重複なく割り振って供給することが可能となる。また、このG鍵のレプリケーションによって、2つのリージョンb2間でのG鍵の共有化を、その時々で変化する需要量に応じて適応的に行うことが可能となる。

10

【0052】

(3)の量子鍵配送について、ユーザは、あるデータセンタ100との間で光ファイバの敷設などが必要となるが、当該ユーザが多数の他のユーザとの間で量子鍵配送を行う場合、本来、当該多数の他のユーザ間の各々について光ファイバの敷設などが必要となるところ、1つのデータセンタ100との間の光ファイバの敷設などで済む。たとえばN箇所の拠点を有する企業などにおいて、当該N箇所の拠点間で量子鍵配送を行うための設備を独自に構築するとした場合、 $(N \times (N - 1) / 2)$ 個の組み合わせの2拠点間すべてについて光ファイバの敷設などが必要となるが、各拠点からデータセンタ100までのN個の光ファイバの敷設などで済む。

20

【0053】

以上の3種類の量子鍵配送をクラウドシステム上にマッピングすることで、実施形態の基盤システム1は、任意の2拠点で量子暗号通信を行う両ユーザのそれぞれに対して、各ユーザが属するリージョンb2配下のデータセンタ100から、当該両ユーザが共有すべき量子鍵を提供することを可能とする。

【0054】

さらに、実施形態の基盤システム1は、ユーザが、自身が属するリージョンb2（より詳しくは、当該リージョンb2配下のいずれかのデータセンタ100）から量子鍵の提供を受けるためのインターフェースとして、エンベロップ暗号化におけるマスターキーの指定といった既存のインターフェースに準じた拡張インターフェースを採用する。拡張インターフェースの例としては、パラメータの流用や追加などが挙げられる。

30

【0055】

具体的には、鍵管理システム10は、たとえばETSI GS QKD 014準拠の鍵提供APIで授受される情報を、エンベロップ暗号化のためのインターフェースで授受される情報に当て嵌める。鍵管理システム10は、ユーザとの間のエンベロップ暗号化のためのインターフェースを、量子鍵流通システム20との間のたとえばETSI GS QKD 014準拠の鍵提供APIに変換し、また、量子鍵流通システム20との間のたとえばETSI GS QKD 014準拠の鍵提供APIを、ユーザとの間のエンベロップ暗号化のためのインターフェースに変換することを内部的に実行する。

40

【0056】

この拡張インターフェースの採用によって、ユーザは、既存の非量子鍵の暗号鍵管理サービスと同じ感覚で量子鍵を取得することができ、たとえば量子鍵流通システム20から量子鍵を取得するためのETSI GS QKD 014準拠の鍵提供APIなどをユーザが持つことを不要とすることができる。

【0057】

図8は、実施形態の基盤システム1のシステム全体の機能ブロックの一例を示す図である。

【0058】

前述したように、クラウドシステムは、ゾーンb1、リージョンb2およびグローバル

50

b 3 といった多階層のサービスエリアを設定する。各ゾーン b 1 は、1 以上のデータセンタ 1 0 0 によって形成される。各リージョン b 2 は、複数のゾーン b 1 によって形成される。基盤システム 1 は、このリージョン b 2 を、G 鍵を共有する最小単位とする。そのために、基盤システム 1 は、2 つのリージョン b 2 間に量子暗号通信のための 1 以上の中継拠点を設けている。中継拠点は、量子鍵流通システム 2 0 と量子鍵配送システム 3 0 とを有する。なお、近距離のリージョン b 2 間では、中継拠点を設けず、直接的に量子暗号通信を行うことも可能である。

【0059】

また、前述したように、各データセンタ 1 0 0 は、鍵管理システム 1 0 と、量子鍵流通システム 2 0 と、量子鍵配送システム 3 0 とを有する。各データセンタ 1 0 0 の量子鍵流通システム 2 0 は、同一ゾーン b 1 内の隣接する他のデータセンタ 1 0 0 の量子鍵流通システム 2 0 と古典通信網 (c 1) で接続されている。古典通信網とは、光子による暗号鍵情報に特化していない一般的なデータを送受信するための通信網である。各データセンタ 1 0 0 の量子鍵配送システム 3 0 は、同一ゾーン b 1 内の隣接する他のデータセンタ 1 0 0 の量子鍵配送システム 3 0 と量子通信網 (c 2) で接続されている。量子通信網とは、光子による量子鍵情報の送受信のための通信網である。

【0060】

また、各ゾーン b 1 のいくつかのデータセンタ 1 0 0 の量子鍵流通システム 2 0 および量子鍵配送システム 3 0 は、同一リージョン b 2 内の他のゾーン b 1 のデータセンタ 1 0 0 の量子鍵流通システム 2 0 および量子鍵配送システム 3 0 と接続されている。

【0061】

さらに、各リージョン b 2 のいくつかのデータセンタ 1 0 0 の量子鍵流通システム 2 0 および量子鍵配送システム 3 0 は、他のリージョン b 2 との間に介在する中継拠点の量子鍵流通システム 2 0 および量子鍵配送システム 3 0 と接続されている。

【0062】

つまり、実施形態の基盤システム 1 は、リージョン b 2 内において G 鍵のレプリケーションを行うことができ、かつ、リージョン b 2 間において G 鍵の共有化を行うことができる通信網 (c 1、c 2) を有している。

【0063】

図 9 は、データセンタ 1 0 0 の機能ブロックの一例を示す図である。図 2 と同様、二重線の枠は、物理的にセキュリティが確保された拠点であることを表している。

【0064】

前述したように、データセンタ 1 0 0 は、鍵管理システム 1 0 と、量子鍵流通システム 2 0 と、量子鍵配送システム 3 0 とを有する。

【0065】

たとえば、あるデータセンタ 1 0 0 が、N 個の他のデータセンタ (隣接ノード) 1 0 0 と接続されているものとする。隣接ノードの中には、同一ゾーン b 1 内の他のデータセンタ 1 0 0 だけでなく、同一リージョン b 2 内の他のゾーン b 1 のデータセンタ 1 0 0 が含まれ得るし、他のリージョン b 2 との間に介在する中継拠点が含まれ得る。

【0066】

量子鍵配送システム 3 0 は、N 個の隣接ノードの量子鍵配送システム 3 0 のそれぞれと協働して、各隣接ノードとの間で共有化された Q 鍵を生成する。つまり、データセンタ 1 0 0 内には、隣接ノード分の Q 鍵が蓄えられている。

【0067】

量子鍵流通システム 2 0 は、量子鍵配送システム 3 0 から Q 鍵の供給を受けて、隣接ノードの量子鍵流通システム 2 0 との間で G 鍵を送受信するための量子暗号通信を行う。具体的には、量子鍵流通システム 2 0 は、G 鍵を Q 鍵で暗号化して送信し、または、暗号化された状態の G 鍵を受信して Q 鍵で復号する。この量子鍵流通システム 2 0 による G 鍵の送受信は、異なるリージョン b 2 間での G 鍵の共有化のために実行され得るし、同一のリージョン b 2 内での G 鍵のレプリケーションのために実行され得る。

10

20

30

40

50

【0068】

前述したように、基盤システム1は、G鍵を共有する最小単位をリージョンb2としている。各リージョンb2内には、同一のリージョンb2に属する他のユーザとの間で量子暗号通信を行うユーザへ提供するG鍵と、異なるリージョンb2に属する他のユーザとの間で量子暗号通信を行うユーザへ提供するG鍵との、（自リージョンb2を含む）各リージョンb2分のG鍵が蓄えられる。各リージョンb2内で蓄えられるG鍵は、一貫性が保たれるのであれば、各リージョンb2内の複数のデータセンタ100によってどのように保持されるのかは問わない。たとえば、各データセンタ100がすべて（複製）を保持してもよいし、データセンタ100間で分散して保持してもよい。一貫性を保つためのG鍵のレプリケーションの手法は、特定の手法に限らず、様々な手法を適用し得る。

10

【0069】

鍵管理システム10は、たとえば、あるリージョンb2に属する他のユーザと量子暗号通信を行うユーザからのG鍵の要求を、既存の非量子鍵の暗号鍵管理サービスのインターフェースに準じた拡張インターフェースで受け付け、当該あるリージョンb2との間で共有化されたG鍵を、たとえばETSI GS QKD 014準拠の鍵提供APIによって量子鍵流通システム20から取得して、当該ユーザに供給する。つまり、鍵管理システム10は、クラウドサービスとして、量子鍵を提供するサービスを提供する。ユーザとの間のG鍵の送受信も量子暗号通信で行われるが、ここでは、ユーザとの間の量子暗号通信の説明は省略する。なお、鍵管理システム10は、既存の非量子鍵の暗号鍵管理サービスも継続して提供する。よって、ユーザは、たとえばデータの機密レベルに応じて、暗号通信方法を選択する等が可能である。

20

【0070】

図10は、量子鍵流通システム20の機能ブロックの一例を示す図である。二重線の枠は、ここでも、物理的にセキュリティが確保された拠点であることを表している。

【0071】

量子鍵流通システム20は、乱数生成装置21と、暗号化装置22と、復号装置23と、鍵提供API24とを有する。なお、データセンタ（リージョン#1）100側の量子鍵流通システム20には復号装置23が示されておらず、一方、データセンタ（リージョン#2）100側の量子鍵流通システム20には乱数生成装置21および暗号化装置22が示されていないが、これらは、説明を分かり易くするために、便宜的に不図示としたものである。

30

【0072】

たとえば、リージョン（#1）b2のデータセンタ100で稼働する量子鍵流通システム（量子鍵流通システム_x）20の乱数生成装置21は、リージョン（#2）b2のデータセンタ100との間で共有すべきG鍵を生成する。暗号化装置22は、リージョン（#1）b2のデータセンタ100とリージョン（#1）b2のデータセンタ100との間に介在する中継拠点との間で共有されるQ鍵（Q鍵_{AB}）の供給を量子鍵配送システム30から受け、当該Q鍵（Q鍵_{AB}）でG鍵を暗号化する。量子鍵流通システム20は、中継拠点の量子鍵流通システム（量子鍵流通システム_y）20に対して、暗号化したG鍵を送信する。

40

【0073】

一方、中継拠点の量子鍵流通システム（量子鍵流通システム_y）20では、復号装置23が、リージョン（#1）b2のデータセンタ100との間で共有されるQ鍵（Q鍵_{AB}）の供給を量子鍵配送システム30から受け、一旦、当該Q鍵（Q鍵_{AB}）で、暗号化されているG鍵を復号する。続いて、暗号化装置22が、リージョン（#2）b2のデータセンタ100との間で共有されるQ鍵（Q鍵_{BC}）の供給を量子鍵配送システム30から受け、当該Q鍵（Q鍵_{BC}）でG鍵を再暗号化する。量子鍵流通システム20は、リージョン（#2）b2のデータセンタ100の量子鍵流通システム（量子鍵流通システム_z）20に対して、再暗号化したG鍵を送信する。

【0074】

50

リージョン（＃２）ｂ２のデータセンタ１００で稼働する量子鍵流通システム（量子鍵流通システム_Z）２０では、復号装置２３が、中継拠点との間で共有されるＱ鍵（Ｑ鍵_{B C}）の供給を量子鍵配送システム３０から受け、当該Ｑ鍵（Ｑ鍵_{B C}）で、暗号化されているＧ鍵を復号する。

【００７５】

そして、量子鍵流通システム（量子鍵流通システム_X）２０および量子鍵流通システム（量子鍵流通システム_X）２０の鍵提供ＡＰＩ２４は、たとえばＥＴＳＩ ＧＳ ＱＫＤ ０１４準拠の鍵提供ＡＰＩによる鍵管理システム１０からの要求に応じて、以上のような手順で共有化を行ったＧ鍵を鍵管理システム１０に提供する。

【００７６】

図１１は、量子鍵配送システム３０の機能ブロックの一例を示す図である。二重線の枠は、ここでも、物理的にセキュリティが確保された拠点であることを表している。

【００７７】

量子鍵配送システム３０は、乱数生成装置３１と、送信機３２と、受信機３３と、鍵蒸留装置３４とを有する。なお、左側の量子鍵配送システム３０には受信機３３が示されておらず、一方、右側の量子鍵配送システム３０には乱数生成装置３１および送信機３２が示されていないが、これらは、説明を分かり易くするために、便宜的に不図示としたものである。

【００７８】

乱数生成装置３１は、他のデータセンタ１００または中継拠点の量子鍵配送システム３０との間で送受信する乱数列（暗号鍵情報）を生成する。送信機３２は、乱数生成装置３１が生成する乱数列を量子通信網（ｃ２）経由で他のデータセンタ１００または中継拠点の量子鍵配送システム３０に送信する。一方、受信機３３は、他のデータセンタ１００または中継拠点の量子鍵配送システム３０から量子通信網（ｃ２）経由で送られてくる乱数列を受信する。

【００７９】

鍵蒸留装置３４は、乱数列の送信側と受信側とが協働して、当該乱数列の中の盗聴の可能性のある部分を取り除く秘匿性増強処理を実行する。送信側と受信側との間で送受信された乱数列の中の不適切部分が鍵蒸留装置３４によって除去された乱数列が、当該送信側と受信側との間で共有されるＱ鍵として双方で蓄えられる。

【００８０】

図１２は、実施形態の基盤システム１における、ユーザが量子鍵の提供を含む量子暗号通信サービスの利用を開始する場合の動作の流れを示すフローチャートである。なお、図１２の「クラウドＫＭＳ」とは、ある１つのリージョンｂ２内の複数のデータセンタ１００の鍵管理システム１０の論理的な集合体である。換言すれば、「クラウドＫＭＳ」の実体は、ある１つのリージョンｂ２内の複数のデータセンタ１００に分散配置されている。

【００８１】

量子暗号通信サービスの利用を開始するユーザは、自身が属するリージョンｂ２（より詳しくは、当該リージョンｂ２配下のいずれかのデータセンタ１００）の鍵管理システム１０に対して、マスターキーの作成を要求する（Ｓ１０１）。このとき、ユーザは、属性情報として宛先リージョンｂ２を入力する（Ｓ１０２）。宛先リージョンｂ２は、通信相手のユーザが属するリージョンｂ２である。さらに、ユーザは、当該マスターキーについてのアクセスポリシーの定義等を必要に応じて入力する（Ｓ１０３）。

【００８２】

一方、ユーザからの要求を受け付けた当該リージョンｂ２の鍵管理システム１０は、ユーザから入力された情報に基づき、マスターキーを作成する（Ｓ１０４）。当該リージョンｂ２の鍵管理システム１０は、宛先リージョンｂ２の鍵管理システム１０に対して、同一のマスターキーの作成を指示する。この指示を受けた宛先リージョンｂ２の鍵管理システム１０は、同一のマスターキーを作成する（Ｓ１０５）。当該リージョンｂ２の鍵管理システム１０は、作成したマスターキーのＩＤをユーザへ送信する（Ｓ１０６）。

10

20

30

40

50

【0083】

図13は、実施形態の基盤システム1における、ユーザが量子鍵を用いた暗号化を行う場合の動作の流れを示すフローチャートである。図13の「クラウドKMS」は、前述の「クラウドKMS」と同様である。また、図13の「QKDシステム」は、ある1つのリージョンb2内の複数のデータセンタ100のQKDシステム（量子鍵流通システム20および量子鍵配送システム30）の論理的な集合体である。換言すれば、「QKDシステム」の実体は、ある1つのリージョンb2内の複数のデータセンタ100に分散配置されている。

【0084】

ユーザは、自身が属するリージョンb2（より詳しくは、当該リージョンb2配下のいずれかのデータセンタ100）の鍵管理システム10に対して、データの暗号化に用いるデータキーを要求する（S201）。このとき、ユーザは、量子暗号通信サービスの利用開始時に入手したマスターキーIDを入力する（S202）。このマスターキーIDの入力は、既存の非量子鍵の暗号鍵管理サービスのインターフェースに準じている。

10

【0085】

鍵管理システム10は、ユーザから受け取ったマスターキーIDに基づき、当該マスターキーIDで示されるマスターキーの属性情報、即ち宛先リージョンを参照する（S203）。鍵管理システム10は、その宛先リージョン名を、たとえばETSI GS QKD 014準拠の鍵提供APIで用いられるSAE IDに変換し（S204）、当該SAE IDを自リージョンb2（より詳しくは、自データセンタ100）のQKDシステム（量子鍵流通システム20および量子鍵配送システム30）へ送信する（S205）。

20

【0086】

当該QKDシステムは、受信したSAE IDに対応する目的のQKDシステムを特定し（S206）、当該目的のQKDシステムとの間で鍵共有を行う（S207）。これにより、宛先リージョンのQKDシステムは、ユーザが属するリージョンb2のQKDシステムとの間で共有化されたG鍵を蓄積する（S208）。なお、当該G鍵の蓄積は、自リージョンのQKDシステムでも行われる。また、当該2つのリージョンのユーザによる量子鍵暗号は、複数並列に実行され得るので、各リージョン内でG鍵のレプリケーションが行われる。当該QKDシステム（自リージョンb2のQKDシステム）は、宛先リージョンのQKDシステムとの間で共有化されたG鍵と、当該G鍵のIDとを鍵管理システム10に送信する（S209）。

30

【0087】

鍵管理システム10は、QKDシステムから受け取ったG鍵をデータキーとし、同じくQKDシステムから受け取ったG鍵IDを暗号化済みデータキーとして、当該G鍵およびG鍵IDをユーザへ送信する（S210）。当該G鍵およびG鍵IDの送信も、既存の非量子鍵の暗号鍵管理サービスのインターフェースに準じている。

【0088】

ユーザは、鍵管理システム10からデータキー（G鍵）と暗号化済みデータキー（G鍵ID）とを入手すると（S211）、当該データキーを用いてデータを暗号化し（S212）、暗号データ、マスターキーIDおよび暗号化済みデータキーを（たとえば量子暗号通信の相手である）他のユーザと共有する（S213）。

40

【0089】

図14は、実施形の基盤システム1における、ユーザが量子鍵を用いた暗号データの復号を行う場合の動作の流れを示すフローチャートである。図14の「クラウドKMS」および「QKDシステム」は、前述の「クラウドKMS」および「QKDシステム」と同様である。

【0090】

ユーザは、（たとえば量子暗号通信の相手である）他のユーザから暗号データ、マスターキーIDおよび暗号化済みデータキーを入手する（S301）。ユーザは、自身が属するリージョンb2（より詳しくは、当該リージョンb2配下のいずれかのデータセンタ1

50

00)の鍵管理システム10に対して、暗号データを復号するためのデータキーを要求する(S302)。このとき、ユーザは、暗号データと共に入手したマスターキーIDおよび暗号化済みデータキーを入力する(S303)。このマスターキーIDの入力は、既存の非量子鍵の暗号鍵管理サービスのインターフェースにパラメータを追加することで対応できる。

【0091】

鍵管理システム10は、ユーザから受け取ったマスターキーIDに基づき、当該マスターキーIDで示されるマスターキーの属性情報、即ち宛先リージョンを参照する(S304)。鍵管理システム10は、その宛先リージョン名を、たとえばETSI GS QKD 014準拠の鍵提供APIで用いられるSAE IDに変換し、かつ、ユーザから受け取った暗号化済みデータキーをG鍵IDに変換する(S305)。鍵管理システム10は、当該変換後のSAE IDおよびG鍵IDを自リージョンb2(より詳しくは、自データセンタ100)のQKDシステムへ送信する(S306)。

10

【0092】

QKDシステムは、鍵管理システム10から受け取ったG鍵IDに対応するG鍵のデータを参照し(S307)、当該G鍵を鍵管理システム10に送信する(S308)。鍵管理システム10は、QKDシステムから受け取ったG鍵をデータキーとしてユーザへ送信する(S309)。このデータキーとしてのG鍵の送信は、既存の非量子鍵の暗号鍵管理サービスのインターフェースに準じている。

20

【0093】

ユーザは、鍵管理システム10からデータキー(G鍵)を入手すると(S310)、そのデータキーを用いて、暗号データの復号を実施する(S311)。

【0094】

図15は、実施形態の基盤システム1における、ユーザが量子鍵の提供を含む量子暗号通信サービスの利用を終了する場合の動作の流れを示すフローチャートである。図15の「クラウドKMS」は、前述の「クラウドKMS」と同様である。

【0095】

量子暗号通信サービスの利用を終了するユーザは、自身が属するリージョンb2(より詳しくは、当該リージョンb2配下のいずれかのデータセンタ100)の鍵管理システム10に対して、マスターキーの削除を要求する(S401)。このとき、ユーザは、マスターキーIDを入手する(S402)。

30

【0096】

一方、ユーザからの要求を受け付けた当該リージョンb2の鍵管理システム10は、マスターキーIDで示されるマスターキーを削除する(S403)。当該リージョンb2の鍵管理システム10は、当該マスターキーに付随する属性情報で示される宛先リージョンb2の鍵管理システム10に対して、同一のマスターキーの削除を指示する。この指示を受けた宛先リージョンb2の鍵管理システム10は、同一のマスターキーを削除する(S405)。

【0097】

以上のように、実施形態の基盤システム1は、(1)リージョンb2間でのG鍵の共有のための量子鍵配送、(2)各リージョンb2配下のデータセンタ100間でのG鍵のレプリケーションのための量子鍵配送、(3)ユーザと当該ユーザが属するリージョンb2配下のデータセンタ100間でのG鍵の授受のための量子鍵配送、の3種類の量子鍵配送をクラウドシステム上にマッピングし、かつ、たとえばETSI GS QKD 014準拠の鍵提供APIで授受される情報を、エンベロープ暗号化のためのインターフェースで授受される情報に当て嵌めるための変換を内部的に行うことによって、既存の非量子鍵の暗号鍵管理サービスと同じ感覚で利用可能な量子鍵の提供を含む量子暗号通信サービスをクラウドシステム上で提供することができる。

40

【0098】

次に、実施形態の基盤システム1において想定され得るいくつかのユースケースについ

50

て説明する。

【0099】

図16は、実施形態の基盤システム1の第1ユースケースを示す図である。第1ユースケースは、同一リージョンb2のクラウド上のアプリケーション（App）同士が鍵管理システム10で共有された量子鍵を取得するケースである。このケースは、たとえば、ユーザに対して、量子鍵の提供だけでなく、当該量子鍵を用いた通信（量子暗号通信）用の設備を提供する場合などが該当する。

【0100】

送信側のアプリケーションは、誰に暗号データを送りたいか決定し、その相手に対応するマスターキーの作成を鍵管理システム10に要求する（1）。あるいは、マスターキーが作成済みである場合、アプリケーションは、その相手に対応するマスターキーを選択する。マスターキーの作成時には、アプリケーションは、鍵種別（d1）、アクセスポリシー、宛先リージョン（d2）などを入力する。鍵種別（d1）および宛先リージョン（d2）は、既存のインターフェースからの拡張部分である。鍵種別は、たとえば量子鍵か否かを示す情報である。量子鍵を示す情報（QKD）が入力された場合に、宛先リージョンが入力される。マスターキーに関する情報は、たとえばマスターキーメタデータとして鍵管理システム10によって管理される。

【0101】

送信側のアプリケーションは、暗号データを送る相手に対応するマスターキーを作成または選択すると、そのマスターキーIDを指定して、データキーの作成を鍵管理システム10に要求する（2）。このとき、鍵管理システム10は、マスターキーの作成時に入力されたアクセスポリシー等に基づき、アプリケーションの認証処理を実行する。

【0102】

鍵管理システム10は、宛先リージョンとの間（ここでは、同一リージョン内）で共有化されたG鍵を、たとえばETSI GS QKD 014 準拠の鍵提供APIによってQKDシステム（量子鍵流通システム20および量子鍵配送システム30）から取得する（3）。鍵管理システム10は、当該取得したG鍵をデータキーとし、そのG鍵IDを鍵情報として、G鍵およびG鍵IDをアプリケーションへ送信する（4）。

【0103】

送信側のアプリケーションは、鍵管理システム10から供給されたG鍵を用いてデータを暗号化し、暗号化済みデータと、マスターキーIDおよびG鍵ID（d3）を含む鍵情報とを取得する（5）。鍵情報中のG鍵ID（d3）は、既存のインターフェースからの拡張部分である。送信側のアプリケーションは、受信側のアプリケーションに対して、暗号データ（暗号化済みデータ）と、暗号化済みデータキー（G鍵ID）およびマスターキーIDとを送信し、これらを受信側のアプリケーションとの間で共有する（6）。

【0104】

一方、受信側のアプリケーションは、送信側のアプリケーションから受け取った鍵情報（マスターキーIDおよびG鍵ID（d3））を指定して、データキーの復号を鍵管理システム10に要求する（7）。前述したように、鍵情報中のG鍵ID（d3）は、既存のインターフェースからの拡張部分である。このとき、鍵管理システム10は、マスターキーの作成時に入力されたアクセスポリシー等に基づき、アプリケーションの認証処理を実行する。

【0105】

鍵管理システム10は、送信側のアプリケーションが属するリージョンとの間（ここでは、同一リージョン内）で共有化されたG鍵を、たとえばETSI GS QKD 014 準拠の鍵提供APIによってQKDシステムから取得する（8）。鍵管理システム10は、当該取得したG鍵をデータキーとしてアプリケーションへ送信する（9）。受信側のアプリケーションは、鍵管理システム10から供給されたG鍵を用いて、暗号データを復号する（10）。

【0106】

10

20

30

40

50

図17は、実施形態の基盤システム1の第2ユースケースを示す図である。第2ユースケースは、量子鍵通信を行う、オンプレミスのサイトA、サイトBのユーザ（アプリケーション）が、鍵管理システム10で共有された量子鍵を同一リージョンb2から取得するケースである。

【0107】

サイトAのアプリケーションは、誰に暗号データを送りたいか決定し、その相手に対応するマスターキーの作成を鍵管理システム10に要求する（1）。あるいは、マスターキーが作成済みである場合、アプリケーションは、その相手に対応するマスターキーを選択する。マスターキーの作成時には、アプリケーションは、鍵種別（d1）、アクセスポリシー、宛先リージョン（d2）などを入力する。前述したように、鍵種別（d1）および宛先リージョン（d2）は、既存のインターフェースからの拡張部分である。

10

【0108】

サイトAのアプリケーションは、暗号データを送る相手に対応するマスターキーを作成または選択すると、そのマスターキーIDと鍵の長さを指定して、データキーの作成を鍵管理システム10に要求する（2）。鍵の長さは、たとえば規定値と異なる長さのデータキーを要求する場合のオプションである。また、このとき、鍵管理システム10は、マスターキーの作成時に入力されたアクセスポリシー等に基づき、アプリケーションの認証処理を実行する。

【0109】

鍵管理システム10は、宛先リージョンとの間（ここでは、同一リージョン内）で共有化されたG鍵を、たとえばETSI GS QKD 014準拠の鍵提供APIによってQKDシステム（量子鍵流通システム20および量子鍵配送システム30）から取得する（3）。鍵管理システム10は、当該取得したG鍵をデータキーとし、そのG鍵IDを鍵情報として、G鍵およびG鍵IDをサイトAのアプリケーションへ送信する（4）。

20

【0110】

サイトAのアプリケーションは、鍵管理システム10から供給されたG鍵を用いてデータを暗号化し、暗号化済みデータと、マスターキーIDおよびG鍵ID（d3）を含む鍵情報とを取得する（5）。前述したように、鍵情報中のG鍵ID（d3）は、既存のインターフェースからの拡張部分である。サイトAのアプリケーションは、サイトBのアプリケーションに対して、暗号データ（暗号化済みデータ）と、暗号化済みデータキー（G鍵ID）およびマスターキーIDとを送信し、これらをサイトBのアプリケーションとの間で共有する（6）。

30

【0111】

一方、サイトBのアプリケーションは、サイトAのアプリケーションから受け取った鍵情報（マスターキーIDおよびG鍵ID（d3））を指定して、データキーの復号を鍵管理システム10に要求する（7）。前述したように、鍵情報中のG鍵ID（d3）は、既存のインターフェースからの拡張部分である。このとき、鍵管理システム10は、マスターキーの作成時に入力されたアクセスポリシー等に基づき、アプリケーションの認証処理を実行する。

【0112】

鍵管理システム10は、サイトAのアプリケーションが属するリージョンとの間（ここでは、同一リージョン内）で共有化されたG鍵を、たとえばETSI GS QKD 014準拠の鍵提供APIによってQKDシステムから取得する（8）。鍵管理システム10は、当該取得したG鍵をデータキーとしてサイトBのアプリケーションへ送信する（9）。サイトBのアプリケーションは、鍵管理システム10から供給されたG鍵を用いて、暗号データを復号する（10）。

40

【0113】

図18は、実施形態の基盤システム1の第3ユースケースを示す図である。第3ユースケースは、サイトA、サイトBのアプリケーションが、鍵管理システム10で共有された量子鍵を、それぞれ別リージョンb2（リージョンA、リージョンB）から取得するケー

50

スである。

【0114】

サイトAのアプリケーションは、誰に暗号データを送りたいか決定し、その相手に対応するマスターキーの作成をリージョンAの鍵管理システム10に要求する(1)。あるいは、マスターキーが作成済みである場合、サイトAのアプリケーションは、その相手に対応するマスターキーを選択する。マスターキーの作成時には、サイトAのアプリケーションは、鍵種別(d1)、アクセスポリシー、宛先リージョン(d2)などを入力する。前述したように、鍵種別(d1)および宛先リージョン(d2)は、既存のインターフェースからの拡張部分である。

【0115】

サイトAのアプリケーションは、暗号データを送る相手に対応するマスターキーを作成または選択すると、そのマスターキーIDを指定して、データキーの作成をサイトAの鍵管理システム10に要求する(2)。このとき、サイトAの鍵管理システム10は、マスターキーの作成時に入力されたアクセスポリシー等に基づき、アプリケーションの認証処理を実行する。

【0116】

リージョンAの鍵管理システム10は、宛先リージョン(リージョンB)との間で共有化されたG鍵を、たとえばETSI GS QKD 014準拠の鍵提供APIによってQKDシステム(量子鍵流通システム20および量子鍵配送システム30)から取得する(3)。リージョンAの鍵管理システム10は、当該取得したG鍵をデータキーとし、そのG鍵IDを鍵情報として、G鍵およびG鍵IDをサイトAのアプリケーションへ送信する(4)。

【0117】

サイトAのアプリケーションは、リージョンAの鍵管理システム10から供給されたG鍵を用いてデータを暗号化し、暗号化済みデータと、マスターキーIDおよびG鍵ID(d3)を含む鍵情報とを取得する(5)。前述したように、鍵情報中のG鍵ID(d3)は、既存のインターフェースからの拡張部分である。サイトAのアプリケーションは、サイトBのアプリケーションに対して、暗号データ(暗号化済みデータ)と、暗号化済みデータキー(G鍵ID)およびマスターキーIDとを送信し、これらをサイトBのアプリケーションとの間で共有する(6)。

【0118】

一方、サイトBのアプリケーションは、サイトAのアプリケーションから受け取った鍵情報(マスターキーIDおよびG鍵ID(d3))を指定して、データキーの復号をリージョンBの鍵管理システム10に要求する(7)。前述したように、鍵情報中のG鍵ID(d3)は、既存のインターフェースからの拡張部分である。このとき、リージョンBの鍵管理システム10は、リージョンAの鍵管理システム10が管理するマスターキー情報を確認し(8)、アクセスポリシー等に基づき、サイトBのアプリケーションの認証処理を実行する。

【0119】

リージョンBの鍵管理システム10は、サイトAのアプリケーションが属するリージョン(リージョンA)との間で共有化されたG鍵を、たとえばETSI GS QKD 014準拠の鍵提供APIによってQKDシステムから取得する(9)。リージョンBの鍵管理システム10は、当該取得したG鍵をデータキーとしてサイトBのアプリケーションへ送信する(10)。サイトBのアプリケーションは、鍵管理システム10から供給されたG鍵を用いて、暗号データを復号する(11)。

【0120】

図17および図18から明らかなように、実施形態の基盤システム1では、量子暗号通信を行う双方のユーザが、同一リージョンから量子鍵を取得する場合と、それぞれ別リージョンから量子鍵を取得する場合とのいずれであっても、ユーザは同じ手続き(インターフェース)によって量子鍵を取得することができる。また、基盤システム1は、既存のイ

10

20

30

40

50

ンターフェースに準じた拡張インターフェースを採用するので、ユーザが、既存の非量子鍵の暗号鍵管理サービスと同じ感覚で量子鍵を取得することを可能とし、たとえば E T S I G S Q K D 0 1 4 準拠の鍵提供 A P I などを持つことを不要にできる。

【0121】

つまり、実施形態の基盤システム1は、クラウドシステム上で量子鍵の提供を含む量子暗号通信サービスを提供することができる。

【0122】

本発明のいくつかの実施形態を説明したが、これらの実施形態は、例として提示したものであり、発明の範囲を限定することは意図していない。これら新規な実施形態は、その他の様々な形態で実施されることが可能であり、発明の要旨を逸脱しない範囲で、種々の省略、置き換え、変更を行うことができる。これら実施形態やその変形は、発明の範囲や要旨に含まれるとともに、特許請求の範囲に記載された発明とその均等の範囲に含まれる。

【符号の説明】

【0123】

1…基盤システム、10…鍵管理システム(KMS)、20…量子鍵流通システム、30…量子鍵配送システム、100…データセンタ。

10

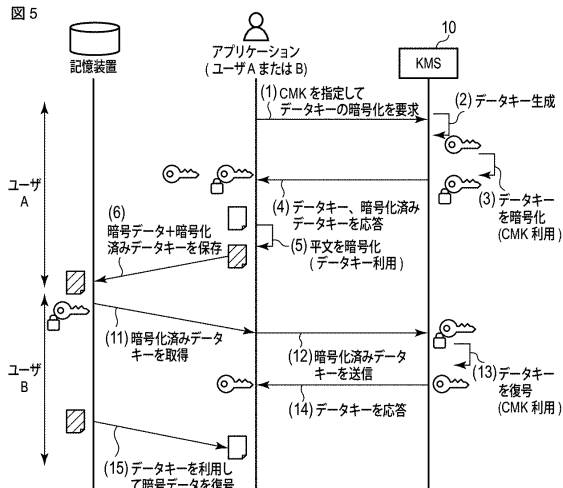
20

30

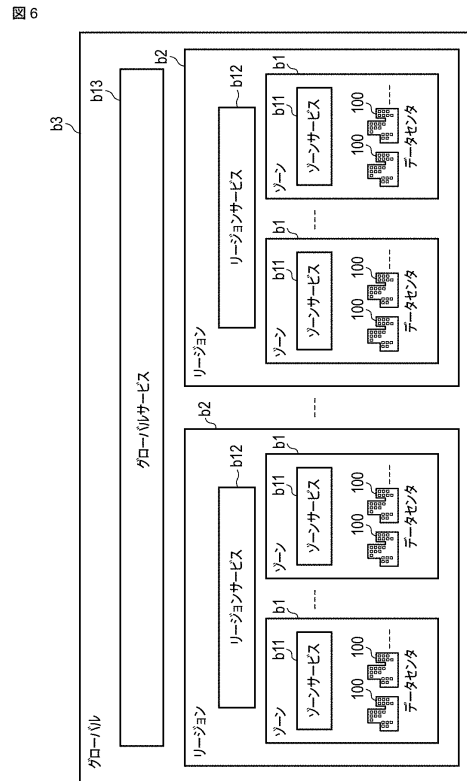
40

50

【図 5】



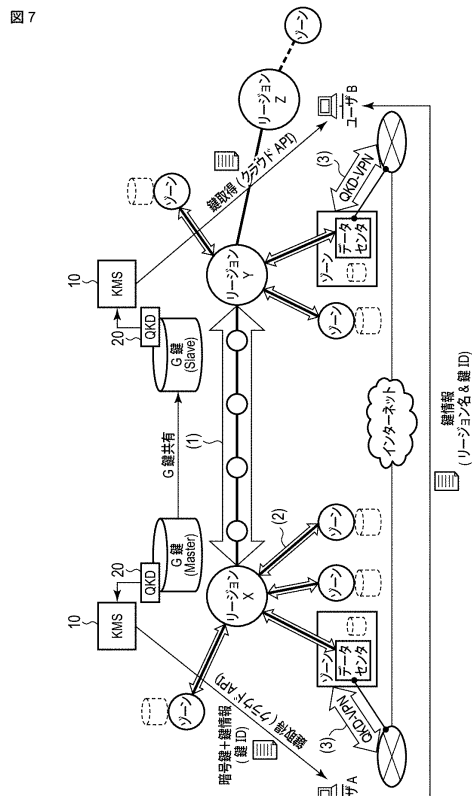
【図 6】



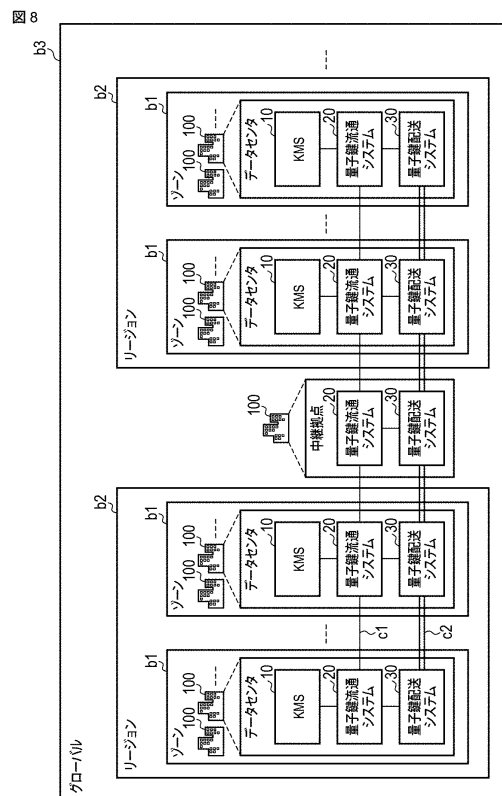
10

20

【圖 7】



【図 8】



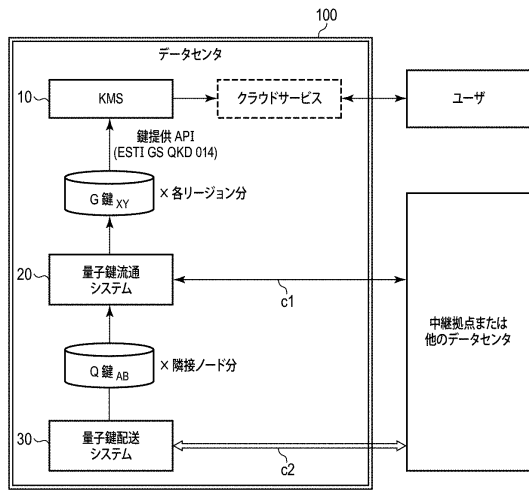
30

40

50

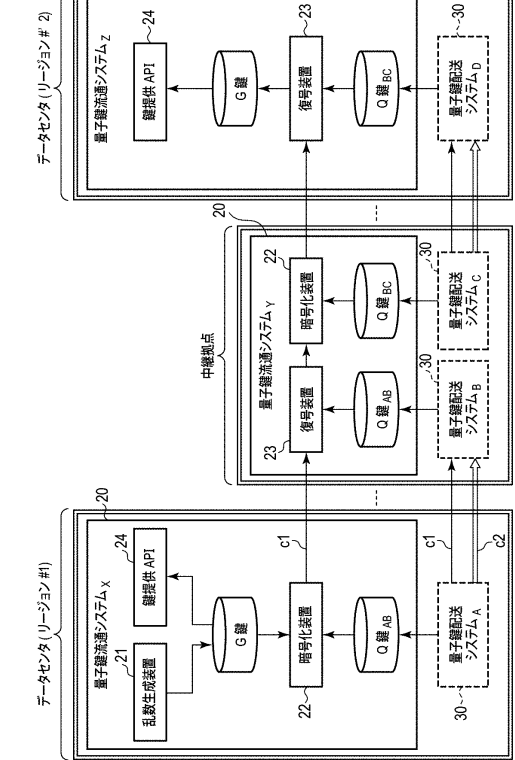
【図 9】

図 9



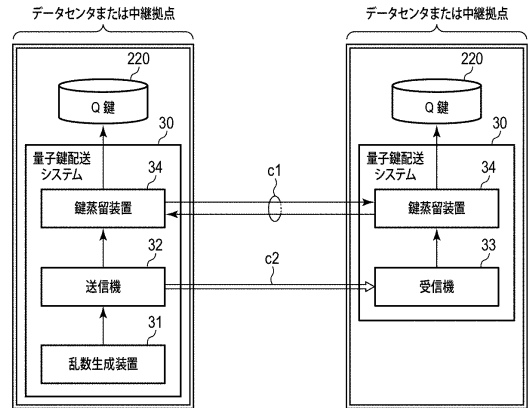
【図 10】

図 10



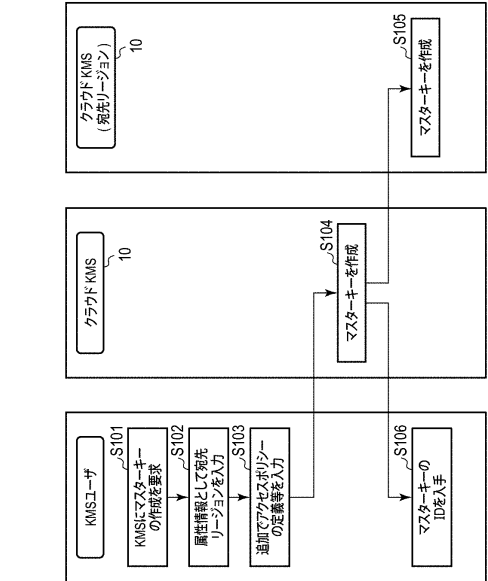
【図 11】

図 11



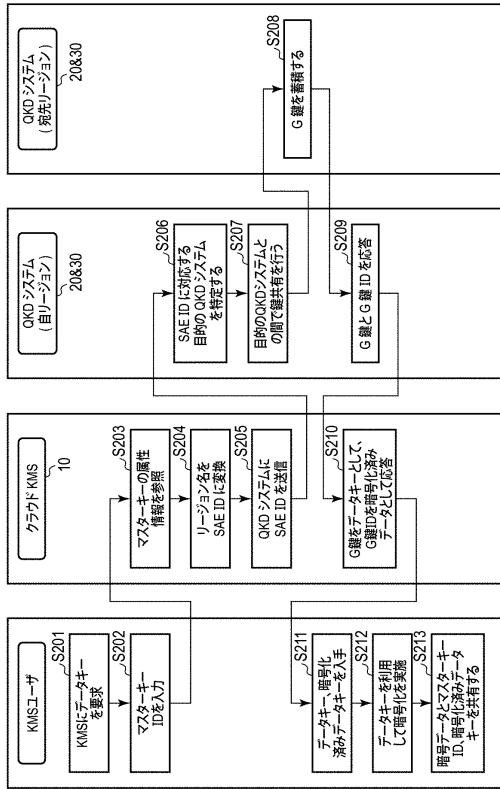
【図 12】

図 12



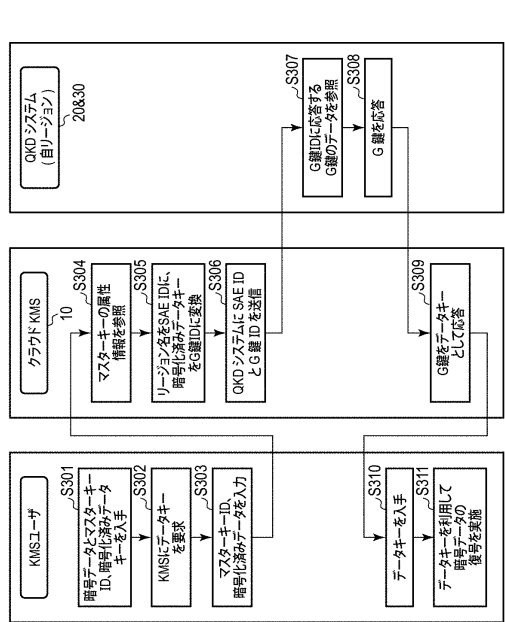
【図 13】

図 13



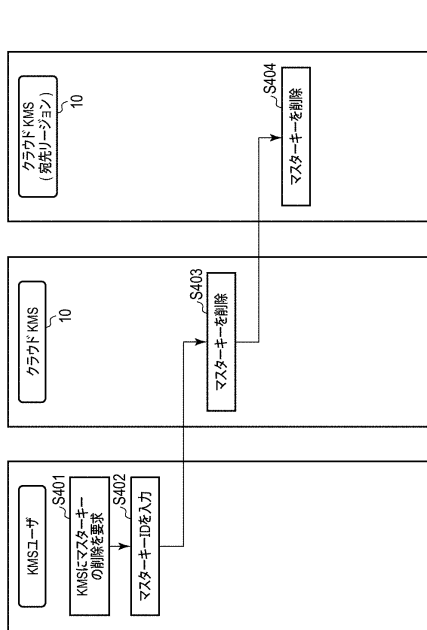
【図 14】

図 14



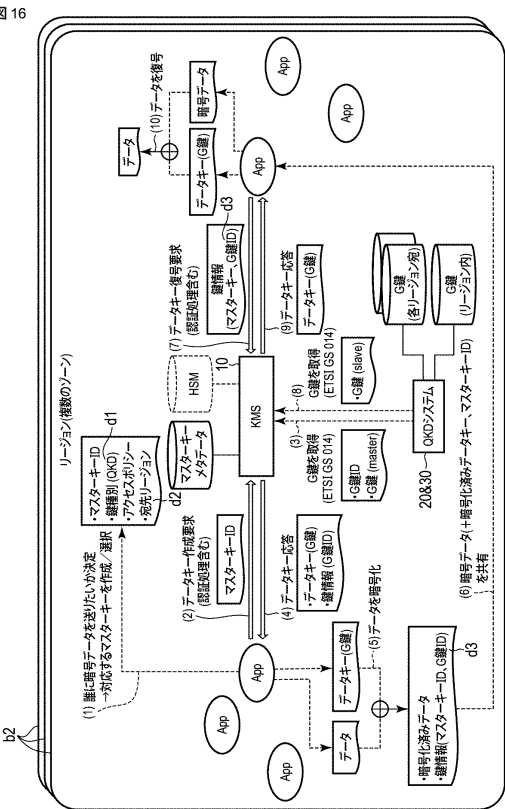
【図 15】

図 15



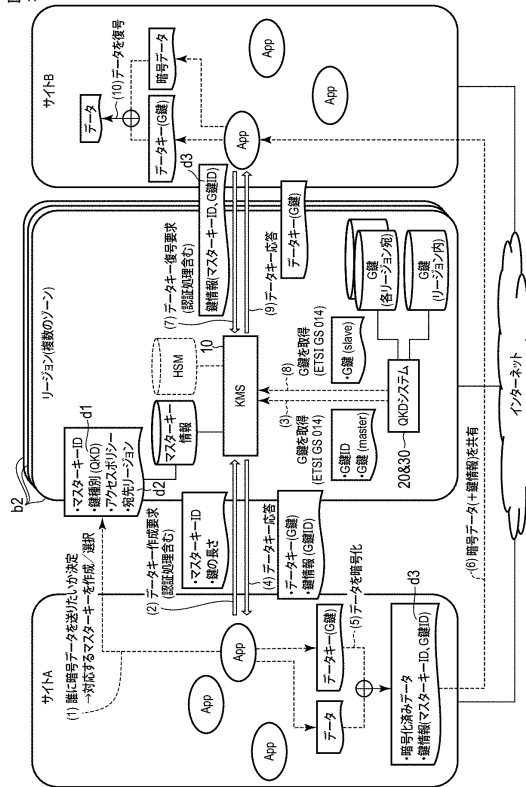
【図 16】

図 16



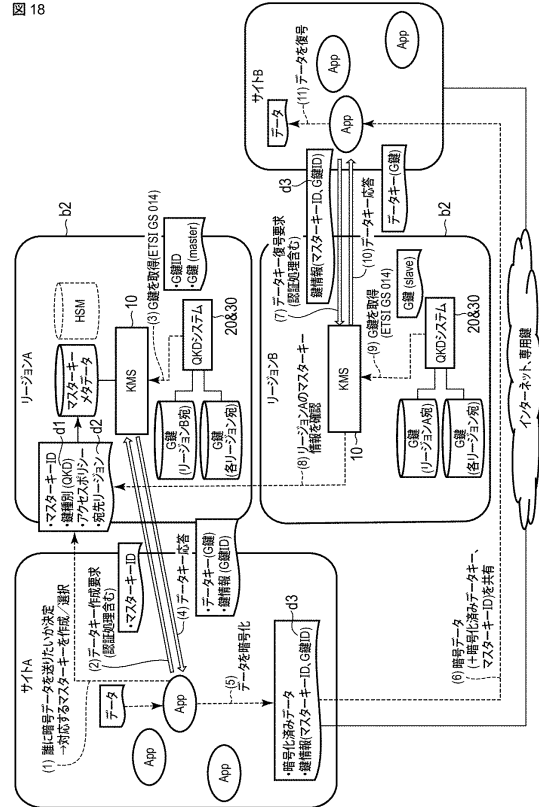
【図 17】

图 17



【図 18】

图 18



フロントページの続き

内
審査官 塩澤 如正
(56)参考文献 特開 2 0 1 8 - 2 0 7 3 4 8 (J P , A)
(58)調査した分野 (Int.Cl., D B 名)
H 0 4 L 9 / 0 8
H 0 4 L 9 / 1 2