(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7649607号
(P7649607)

(45)発行日　令和7年3月21日(2025.3.21)

(24)登録日　令和7年3月12日(2025.3.12)

(51)国際特許分類

		FI		
H04L	*9/08 (2006.01)*	H04L	9/08	B
H04L	*9/14 (2006.01)*	H04L	9/14	

請求項の数　23　（全30頁）

(21)出願番号　特願2023-501301(P2023-501301)
(86)(22)出願日　令和3年6月23日(2021.6.23)
(65)公表番号　特表2023-532810(P2023-532810A)
(43)公表日　令和5年7月31日(2023.7.31)
(86)国際出願番号　PCT/EP2021/067134
(87)国際公開番号　WO2022/008247
(87)国際公開日　令和4年1月13日(2022.1.13)
審査請求日　令和5年11月14日(2023.11.14)
(31)優先権主張番号　16/925,403
(32)優先日　令和2年7月10日(2020.7.10)
(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　100112690
弁理士　太佐 種一

最終頁に続く

(54)【発明の名称】　暗号化データオブジェクトの配布

(57)【特許請求の範囲】

【請求項１】

暗号化データを生成するために、１つまたは複数のプロセッサによってセッション鍵に少なくとも部分的に基づいてデータを暗号化する段階と、

暗号化セッション鍵を生成するために、前記１つまたは複数のプロセッサによって送信側鍵に少なくとも部分的に基づいて前記セッション鍵を暗号化する段階であって、前記送信側鍵は鍵管理システム（ＫＭＳ）から事前に取得される、段階と、

前記１つまたは複数のプロセッサによって、暗号化送信側鍵インデックスのための要求を前記ＫＭＳに伝送する段階であって、前記要求は前記送信側鍵のインデックスと１つまたは複数のさらなる鍵のそれぞれのインデックスを含む、段階と、

前記１つまたは複数のプロセッサによって、前記ＫＭＳから前記暗号化送信側鍵インデックスを受信する段階であって、前記暗号化送信側鍵インデックスは、前記ＫＭＳによって、前記送信側鍵インデックスと前記１つまたは複数のさらなる鍵とに少なくとも部分的に基づいて生成される、段階と、

前記１つまたは複数のプロセッサによって、前記暗号化データと、前記暗号化セッション鍵と、前記１つまたは複数のさらなる鍵のそれぞれの前記インデックスと、前記暗号化送信側鍵インデックスとを含むオブジェクトを生成する段階であって、前記オブジェクトを介した前記データへのアクセスは、受信側が前記送信側鍵および前記１つまたは複数のさらなる鍵へのアクセスを含むか否かに少なくとも部分的に基づいて制御される、段階と

を備える方法。

【請求項２】
前記オブジェクトを介した前記データへのアクセスはさらに、前記送信側鍵および前記１つまたは複数のさらなる鍵が有効であるか否かに少なくとも部分的に基づいて制御される、請求項１に記載の方法。
【請求項３】
前記受信側が前記オブジェクトを介して前記データにアクセスすることを防止する段階をさらに備え、前記防止する段階は、前記送信側鍵を無効にするために前記ＫＭＳに要求を伝送する段階を有する、請求項２に記載の方法。
【請求項４】
前記受信側が前記オブジェクトを介して前記データにアクセスすることを防止する段階をさらに備え、前記防止する段階は、前記１つまたは複数のさらなる鍵のうちの少なくとも１つを無効にするために前記ＫＭＳに要求を伝送する段階を有する、請求項２に記載の方法。
【請求項５】
前記オブジェクトを介した前記データへのアクセスは、前記ＫＭＳが前記送信側鍵へのアクセスを有するユーザのリストから前記受信側を追加または削除することに応じて修正される、請求項１に記載の方法。
【請求項６】
前記オブジェクトを介した前記データへのアクセスは、前記ＫＭＳが前記１つまたは複数のさらなる鍵のうちのさらなる鍵へのアクセスを有するユーザのリストから前記受信側を追加または削除することに応じて修正される、請求項１に記載の方法。
【請求項７】
前記受信側に前記オブジェクトを伝送する段階をさらに備える、請求項１から６のいずれか一項に記載の方法。
【請求項８】
前記伝送する段階はネットワークを介して行われる、請求項７に記載の方法。
【請求項９】
コンピュータ可読命令を実行するための１つまたは複数のプロセッサを備えるシステムであって、前記コンピュータ可読命令は１つまたは複数のプロセッサを制御して
暗号化データを生成するために、セッション鍵に少なくとも部分的に基づいてデータを暗号化することと、
暗号化セッション鍵を生成するために、送信側鍵に少なくとも部分的に基づいて前記セッション鍵を暗号化することであって、前記送信側鍵は鍵管理システム（ＫＭＳ）から事前に取得される、ことと、
暗号化送信側鍵インデックスのための要求を前記ＫＭＳに伝送することであって、前記要求は前記送信側鍵のインデックスと１つまたは複数のさらなる鍵のそれぞれのインデックスを含む、ことと、
前記ＫＭＳから前記暗号化送信側鍵インデックスを受信することであって、前記暗号化送信側鍵インデックスは、前記ＫＭＳによって、前記送信側鍵インデックスと前記１つまたは複数のさらなる鍵とに少なくとも部分的に基づいて生成される、ことと、
前記暗号化データと、前記暗号化セッション鍵と、前記１つまたは複数のさらなる鍵のそれぞれの前記インデックスと、前記暗号化送信側鍵インデックスとを含むオブジェクトを生成することであって、前記オブジェクトを介した前記データへのアクセスは、受信側が前記送信側鍵および前記１つまたは複数のさらなる鍵へのアクセスを含むか否かに少なくとも部分的に基づいて制御される、ことと
を含む操作を実行させる、システム。
【請求項１０】
前記オブジェクトを介した前記データへのアクセスはさらに、前記送信側鍵および前記１つまたは複数のさらなる鍵が有効であるか否かに少なくとも部分的に基づいて制御される、請求項９に記載のシステム。

【請求項１１】
前記操作は、前記受信側が前記オブジェクトを介して前記データにアクセスすることを防止することをさらに含み、前記防止することは、前記送信側鍵を無効にするために前記ＫＭＳに要求を伝送することを含む、請求項１０に記載のシステム。
【請求項１２】
前記操作は、前記受信側が前記オブジェクトを介して前記データにアクセスすることを防止することをさらに含み、前記防止することは、前記１つまたは複数のさらなる鍵のうちの少なくとも１つを無効にするために前記ＫＭＳに要求を伝送することを含む、請求項１０に記載のシステム。
【請求項１３】
前記オブジェクトを介した前記データへのアクセスは、前記ＫＭＳが前記送信側鍵へのアクセスを有するユーザのリストから前記受信側を追加または削除することに応じて修正される、請求項９に記載のシステム。
【請求項１４】
前記オブジェクトを介した前記データへのアクセスは、前記ＫＭＳが前記１つまたは複数のさらなる鍵のうちのさらなる鍵へのアクセスを有するユーザのリストから前記受信側を追加または削除することに応じて修正される、請求項９に記載のシステム。
【請求項１５】
プログラム命令を備えるコンピュータプログラムであって、前記プログラム命令は１つまたは複数のプロセッサによって実行可能であり、前記１つまたは複数のプロセッサに、
暗号化データを生成するために、セッション鍵に少なくとも部分的に基づいてデータを暗号化することと、
暗号化セッション鍵を生成するために、送信側鍵に少なくとも部分的に基づいて前記セッション鍵を暗号化することであって、前記送信側鍵は鍵管理システム（ＫＭＳ）から事前に取得される、ことと、
暗号化送信側鍵インデックスのための要求を前記ＫＭＳに伝送することであって、前記要求は前記送信側鍵のインデックスと１つまたは複数のさらなる鍵のそれぞれのインデックスを含む、ことと、
前記ＫＭＳから前記暗号化送信側鍵インデックスを受信することであって、前記暗号化送信側鍵インデックスは、前記ＫＭＳによって、前記送信側鍵インデックスと前記１つまたは複数のさらなる鍵とに少なくとも部分的に基づいて生成される、ことと、
前記暗号化データと、前記暗号化セッション鍵と、前記１つまたは複数のさらなる鍵のそれぞれの前記インデックスと、前記暗号化送信側鍵インデックスとを含むオブジェクトを生成することであって、前記オブジェクトを介した前記データへのアクセスは、受信側が前記送信側鍵および前記１つまたは複数のさらなる鍵へのアクセスを含むか否かに少なくとも部分的に基づいて制御される、ことと
を含む操作を実行させる、コンピュータプログラム。
【請求項１６】
１つまたは複数のプロセッサによって、暗号化データと、暗号化セッション鍵と、１つまたは複数のさらなる鍵のそれぞれのインデックスと、暗号化送信側鍵インデックスとを含むオブジェクトを受信する段階と、
前記１つまたは複数のプロセッサによって、鍵管理システム（ＫＭＳ）に、前記暗号化送信側鍵インデックスに対応する送信側鍵のための要求を伝送する段階であって、前記要求は要求元からのものであり、前記要求は前記暗号化送信側鍵インデックスと前記１つまたは複数のさらなる鍵のそれぞれの前記インデックスとを含む、段階と、
前記ＫＭＳから前記送信側鍵を受信することに応じて、
セッション鍵を生成するために、前記送信側鍵に少なくとも部分的に基づいて前記暗号化セッション鍵を解読する段階と、
暗号化されていないデータを生成するために、前記セッション鍵に少なくとも部分的に基づいて前記暗号化データを解読する段階であって、前記送信側鍵は、前記要求元が前記

送信側鍵および前記１つまたは複数のさらなる鍵のそれぞれへのアクセスを有するという前記ＫＭＳによる判断に応じて、前記ＫＭＳによって前記要求元に送信される、段階と
を備える方法。
【請求項１７】
前記要求元が前記送信側鍵へのアクセスを有しないという前記ＫＭＳによる判断に応じて、前記ＫＭＳからエラーメッセージを受信する段階をさらに備える、請求項１６に記載の方法。
【請求項１８】
前記送信側鍵が無効である場合、前記要求元が前記送信側鍵へのアクセスを有しないと判断される、請求項１７に記載の方法。
【請求項１９】
前記要求元が前記少なくとも１つまたは複数のさらなる鍵の全てへのアクセスを有しないという前記ＫＭＳによる判断に応じて、前記ＫＭＳからエラーメッセージを受信する段階をさらに備える、請求項１６に記載の方法。
【請求項２０】
前記１つまたは複数のさらなる鍵のうちの少なくとも１つが無効である場合、前記要求元が前記１つまたは複数のさらなる鍵の全てへのアクセスを有しないと判断される、請求項１９に記載の方法。
【請求項２１】
１つまたは複数のプロセッサによって、送信側鍵のための要求を要求元から受信する段階であって、前記要求は暗号化送信側鍵インデックスと、１つまたは複数のさらなる鍵のそれぞれのインデックスとを含む、段階と、
前記要求元が１つまたは複数のさらなる鍵のそれぞれの前記インデックスによって識別される前記１つまたは複数のさらなる鍵へのアクセスを有するか否かを判断する段階と、
前記要求元が前記１つまたは複数のさらなる鍵へのアクセスを有するという判断に応じて、
送信側鍵インデックスを生成するために、前記暗号化送信側鍵インデックスを解読する段階と、
前記送信側鍵インデックスに少なくとも部分的に基づいて前記送信側鍵を配置する段階と、
前記要求元が前記送信側鍵へのアクセスを有するか否かを判断する段階と、
前記要求元が前記送信側鍵へのアクセスを有するとの判断に基づいて前記要求元に前記送信側鍵を伝送する段階と
を備える方法。
【請求項２２】
前記送信側鍵インデックスと前記１つまたは複数のさらなる鍵のそれぞれの前記インデックスとに少なくとも部分的に基づいて前記暗号化送信側鍵インデックスを生成する段階をさらに備える、請求項２１に記載の方法。
【請求項２３】
前記生成する段階は、
前記１つまたは複数のさらなる鍵のそれぞれのインデックスに少なくとも部分的に基づいて前記１つまたは複数のさらなる鍵を配置する段階と、
前記１つまたは複数のさらなる鍵を組み合わせられたさらなる鍵に組み合わせる段階と、
前記組み合わせられたさらなる鍵に少なくとも部分的に基づいて前記送信側鍵インデックスを暗号化する段階と
を有する、請求項２２に記載の方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、概してデータ安全に関し、より具体的には、暗号化に使用した暗号化鍵をデ

ータオブジェクトのメタデータとして含む暗号化データオブジェクトを配布することに関する。

【背景技術】

【０００２】

データ保護およびセキュリティは年間数十億ドル規模の産業であるが、それでもデータ漏洩は依然として発生している。これは、データ保護の本質的な難しさ、保護基準の競合、多くの異なるハードウェアおよびソフトウェアソリューション、さらに保護を実施する個人または組織のスキルレベルが大きく異なるなどを含む多くの理由による。

【０００３】

ネットワークおよびクラウドソリューションにおけるデータのセキュリティは、オンライン上に保存されるデータの量が増加するにつれて、ますます懸念されるようになり続けている。データを保護する方法の１つに暗号法がある。暗号法は、暗号化鍵と暗号化アルゴリズムとを使用して、２つ以上のシステム間でデータを送信しながら暗号化および解読する技術である。ネットワークおよびクラウドソリューションによるデータ保護には、飛行中の保護および静止中の保護の２つの基本的形態を取ってよい。飛行中の保護はネットワーク上のデータを保護し、静止中の保護はストレージ内のデータを保護する。

【０００４】

現在、対称鍵などの暗号化鍵は主に、他方側に送信する前に対称鍵を非対称鍵を使用して暗号化することにより、他方側に送信する前に対称鍵を第２の対称鍵下で暗号化することにより、または紙を使用して対称鍵を配信することにより交換される。これらの一般的な方法のそれぞれには、様々な問題がある。最も困難な問題のうちの１つは、対称鍵の交換のために両者の間に直接的な関係が確立しなければならないことである。この直接的な関係を確立し、管理することは困難であり、鍵の有効期限が短い場合若しくは多くのユーザーがシステムを使用している場合またはその組み合わせには、その困難さはさらに増す。他の問題は鍵の転送に時間がかかること、若しくは交換されている鍵の安全性が破られること、またはその組み合わせを含む。

【０００５】

鍵の交換がうまく実施できても、鍵は安全に管理および保存され、どのデータにどの鍵が使われたかを追跡できるようにしなければならない。通常、ビジネス論理に基づき、データを保護するために所定の鍵を選択することができる。送信側と受信側との両方が、所定のデータに対して特定の鍵があるべきとうまく判断するためのビジネス論理が何であるかを知っていなければならない。そのためには、鍵の選択方法およびビジネス論理に関する必要な情報を交換するために、両側が予め定められた関係を持つ必要がある。

【０００６】

安全な鍵を提供し、暗号化データを交換する関係者間の直接的な関係の必要性を回避する試みとして、鍵管理に対する異なるアプローチが使用されていた。鍵管理は、クライアント（デバイス、アプリケーションなど）の暗号化鍵を生成、配布、より一般的には管理する鍵管理システム（ＫＭＳ）によって行うことができる。ＫＭＳは、鍵の安全な生成から、クライアントシステムでの鍵の安全な取り扱いと保存に至るまで、セキュリティのいくつかの態様を扱うことができる。ＫＭＳは通常、鍵の生成、配布、交換のためのバックエンド機能を含む。さらに、鍵を導入するための特定のクライアント機能、クライアントデバイスでの鍵の保存および管理を統合してよい。

【０００７】

現在のＫＭＳには欠点がある。例えば、暗号化データオブジェクトが作成された後、複数の関係者が、オブジェクトの受信側と複数の鍵を共有することを必要とせず、独立して暗号化データオブジェクトへのアクセスを制御する機能をサポートしていない。さらに、現在のアプローチでは、暗号化データオブジェクトの受信側が、暗号化鍵を取得して受信側に送信するために、ＫＭＳに保存されている暗号化鍵のインデックス、または他の識別子を送信する必要がある。これにより、複数のデータオブジェクトが同じ鍵で暗号化されており、受信側による鍵へのアクセスが破棄された場合、安全性が破られることを引き起

こし得る。このように、ＫＭＳは暗号化鍵管理には利点を提供するが、セキュリティおよびアクセス制御は改善できる。

【発明の概要】

【０００８】

本発明の１つまたは複数の実施形態は、暗号化情報をメタデータとして持つ暗号化データオブジェクトを配布することに向けられている。非限定的な例示的コンピュータ実装方法は、暗号化データを生成するために、セッション鍵に少なくとも部分的に基づいてデータを暗号化する段階を含む。暗号化セッション鍵を生成するために、セッション鍵は、鍵管理システム（ＫＭＳ）から事前に取得された送信側鍵に少なくとも部分的に基づいて暗号化される。暗号化送信側鍵インデックスのための要求はＫＭＳに伝送され、要求は送信側鍵のインデックスと１つまたは複数のさらなる鍵のそれぞれのインデックスとを含む。送信側鍵と１つまたは複数のさらなる鍵とに少なくとも部分的に基づいてＫＭＳにより生成された暗号化送信側鍵インデックスは受信される。暗号化データと暗号化セッション鍵と１つまたは複数のさらなる鍵のそれぞれのインデックスと暗号化送信側鍵インデックスとを含むオブジェクトが生成される。オブジェクトを介したデータへのアクセスは、受信側が送信側鍵および１つまたは複数のさらなる鍵へのアクセスを有するか否かに少なくとも部分的に基づいて制御される。

【０００９】

本発明の１つまたは複数の実施形態は、暗号化情報をメタデータとして持つ暗号化データオブジェクトを配布するためのシステムに向けられている。システムの非限定的な例は、コンピュータ可読命令を実行するためのコンピュータ可読命令と１つまたは複数のプロセッサとを含むメモリを有する。コンピュータ可読命令は上記の方法を実施してよい。

【００１０】

本発明の１つまたは複数の実施形態は暗号化情報をメタデータとして持つ暗号化データオブジェクトを配布するためのコンピュータプログラム製品と、それに具現化されたプログラム命令を含むコンピュータ可読記憶媒体を有するコンピュータプログラム製品とに向けられている。プログラム命令は、上記の方法をプロセッサに実行させるようにプロセッサによって実行可能である。

【００１１】

このように、有利には、暗号化鍵および暗号化鍵インデックスが全ての関係者に配布されないように保護しながら、複数の関係者間でデータを共有することが容易になる。さらに、データの送信側およびその他の関係者は、暗号化データを使用不可能にレンダリングするためにそれらの鍵を無効にすることによってデータへのアクセスを制御する。

【００１２】

さらに、または上記と代替的に、本発明の１つまたは複数の実施形態において、オブジェクトを介したデータへのアクセスは、送信側鍵および１つまたは複数のさらなる鍵が有効であるか否かに少なくとも部分的に基づいてさらに制御される。このように、有利には、データへのアクセスは、送信側が送信側鍵を無効にすることによって、または権限付与された関係者がさらなる鍵のうちの１つを無効にすることによって、破棄され得る。

【００１３】

さらに、または上記と代替的に、本発明の１つまたは複数の実施形態において、受信側は、ＫＭＳに送信側鍵を無効にする要求を伝送することにより、オブジェクトを介したデータへのアクセスを防止する。このように、有利には、送信側鍵管理を一元化することができる。

【００１４】

さらに、または上記と代替的に、本発明の１つまたは複数の実施形態において、受信側は、ＫＭＳに１つまたは複数のさらなる鍵のうちの少なくとも１つを無効にする要求を伝送することにより、オブジェクトを介したデータへのアクセスを防止する。このように、有利には、送信側鍵管理およびデータへのアクセスを一元化することができる。

【００１５】

さらに、または上記と代替的に、本発明の１つまたは複数の実施形態において、オブジェクトを介したデータへのアクセスは、ＫＭＳが送信側鍵へのアクセスを有するユーザのリストから要求元を追加または削除することに応じて修正される。このように、有利には、データへのアクセスは、ユーザが送信側鍵にアクセスが与えられたユーザのグループにいるか否かに基づいて管理され得る。

【００１６】

さらに、または上記と代替的に、本発明の１つまたは複数の実施形態において、オブジェクトを介したデータへのアクセスは、ＫＭＳが１つまたは複数のさらなる鍵のうちのさらなる鍵へのアクセスを有するユーザのリストから受信側を追加または削除することに応じて修正される。このように、有利には、データへのアクセスは、ユーザがさらなる鍵にアクセスが与えられたユーザのグループにいるか否かに基づいて管理され得る。

【００１７】

さらに、または上記と代替的に、本発明の１つまたは複数の実施形態において、オブジェクトは受信側に伝送される。このように、有利には、データおよびアクセス管理は配布される。

【００１８】

さらに、または上記と代替的に、本発明の１つまたは複数の実施形態において、オブジェクトはネットワークを介して受信側に伝送される。このように、有利には、データおよびアクセス管理は配布される。

【００１９】

本発明の１つまたは複数の実施形態は、暗号化情報をメタデータとして持つ暗号化データオブジェクトを配布するためのコンピュータ実装方法に向けられている。コンピュータ実装方法の非限定的な例は、暗号化データと暗号化セッション鍵と１つまたは複数のさらなる鍵のそれぞれのインデックスと暗号化送信側鍵インデックスとを含むオブジェクトを受信する段階を備える。暗号化送信側鍵インデックスに対応する送信側鍵のための要求はＫＭＳに伝送される。要求は要求元からのものであり、要求は暗号化送信側鍵インデックスと１つまたは複数のさらなる鍵のそれぞれのインデックスとを含む。ＫＭＳから送信側鍵を受信することに応じて、セッション鍵を生成するために、暗号化セッション鍵は、送信側鍵に少なくとも部分的に基づいて解読され、暗号化されていないデータを生成するために、暗号化データはセッション鍵に少なくとも部分的に基づいて解読される。要求元が送信側鍵および１つまたは複数のさらなる鍵のそれぞれへのアクセスを有するというＫＭＳによる判断に応じて、送信側鍵はＫＭＳによって要求元へ送信される。

【００２０】

本発明の１つまたは複数の実施形態は、暗号化情報をメタデータとして持つ暗号化データオブジェクトを配布するためのシステムに向けられている。システムの非限定的な例は、コンピュータ可読命令を実行するためのコンピュータ可読命令と１つまたは複数のプロセッサとを含むメモリを有する。コンピュータ可読命令は上記の方法を実施してよい。

【００２１】

本発明の１つまたは複数の実施形態は暗号化情報をメタデータとして持つ暗号化データオブジェクトを配布するためのコンピュータプログラム製品と、それに具現化されたプログラム命令を含むコンピュータ可読記憶媒体を有するコンピュータプログラム製品とに向けられている。プログラム命令は、上記の方法をプロセッサに実行させるようにプロセッサによって実行可能である。

【００２２】

このように、有利には、暗号化鍵および暗号化鍵インデックスが全ての関係者に配布されないように保護しながら、複数の関係者間でデータを共有することが容易になる。さらに、データの送信側およびその他の関係者は、暗号化データを使用不可能にレンダリングするためにそれらの鍵を無効にすることによってデータへのアクセスを制御する。

【００２３】

さらに、または上記と代替的に、本発明の１つまたは複数の実施形態において、エラー

メッセージは、要求元が送信側鍵へのアクセスを有しないというＫＭＳによる判断に応じてＫＭＳから受信される。このように、有利には、オブジェクトへのアクセスが拒否される場合に要求元が通知を受ける。

【００２４】

さらに、または上記と代替的に、本発明の１つまたは複数の実施形態において、送信側鍵が無効である場合に、要求元が送信側鍵へのアクセスを有しないと判断される。このように、データへのアクセスは、有利には、送信側が送信側鍵を無効にすることによって破棄され得る。

【００２５】

さらに、または上記と代替的に、本発明の１つまたは複数の実施形態において、エラーメッセージは、要求元が少なくとも１つまたは複数のさらなる鍵へのアクセスを有しないというＫＭＳによる判断に応じてＫＭＳから受信される。このように、有利には、オブジェクトへのアクセスが拒否される場合に要求元が通知を受ける。

【００２６】

さらに、または上記と代替的に、本発明の１つまたは複数の実施形態において、１つまたは複数のさらなる鍵のうちの少なくとも１つが無効である場合、要求元が１つまたは複数の鍵の全てへのアクセスを有しないと判断される。このように、有利には、データへのアクセスは、権限付与された関係者がさらなる鍵のうちの１つを無効にすることによって破棄され得る。

【００２７】

本発明の１つまたは複数の実施形態は、暗号化情報をメタデータとして持つ暗号化データオブジェクトを配布するためのコンピュータ実装方法に向けられている。コンピュータ実装方法の非限定的な例は、送信側鍵のための要求を受信する段階を含み、要求は要求元からのものであり、要求は暗号化送信側鍵インデックスと１つまたは複数のさらなる鍵のそれぞれのインデックスとを含む。要求元が１つまたは複数のさらなる鍵のそれぞれのインデックスによって識別される１つまたは複数のさらなる鍵へのアクセスを有するか否かを判断する。要求元が１つまたは複数のさらなる鍵へのアクセスを有するとの判断に応じて、送信側鍵インデックスを生成するために、暗号化送信側鍵インデックスは解読され、送信側鍵は送信側鍵インデックスに少なくとも部分的に基づいて配置される。さらに、要求元が送信側鍵へのアクセスを有するか否かを判断する。送信側鍵は、要求元が送信側鍵へのアクセスとの判断に基づいて要求元に伝送される。

【００２８】

本発明の１つまたは複数の実施形態は、暗号化情報をメタデータとして持つ暗号化データオブジェクトを配布するためのシステムに向けられている。システムの非限定的な例は、コンピュータ可読命令を実行するためのコンピュータ可読命令と１つまたは複数のプロセッサとを含むメモリを有する。コンピュータ可読命令は上記の方法を実施してよい。

【００２９】

本発明の１つまたは複数の実施形態は暗号化情報をメタデータとして持つ暗号化データオブジェクトを配布するためのコンピュータプログラム製品と、それに具現化されたプログラム命令を含むコンピュータ可読記憶媒体を有するコンピュータプログラム製品とに向けられている。プログラム命令は、上記の方法をプロセッサに実行させるようにプロセッサによって実行可能である。

【００３０】

このように、有利には、暗号化鍵および暗号化鍵インデックスが全ての関係者に配布されないように保護しながら、複数の関係者間でデータを共有することが容易になる。さらに、データの送信側およびその他の関係者は、暗号化データを使用不可能にレンダリングするためにそれらの鍵を無効にすることによってデータへのアクセスを制御する。

【００３１】

さらに、または上記と代替的に、本発明の１つまたは複数の実施形態において、暗号化送信側鍵インデックスは送信側鍵インデックスと１つまたは複数のさらなる鍵のそれぞれ

のインデックスとに少なくとも部分的に基づいて生成される。このように、有利には、データへのアクセスは、複数の鍵によって保護され、複数の鍵のそれぞれは異なる権限付与されたユーザによって制御され得る。

【００３２】

さらに、または上記と代替的に、本発明の１つまたは複数の実施形態において、暗号化送信側鍵インデックスを生成する段階は、１つまたは複数のさらなる鍵のそれぞれのインデックスに少なくとも部分的に基づいて１つまたは複数のさらなる鍵を配置する段階と、それらを組み合わせられたさらなる鍵に組み合わせる段階とを含む。送信側鍵インデックスは、組み合わせられたさらなる鍵に少なくとも部分的に基づいて暗号化される。このように、有利には、データへのアクセスは、複数の鍵によって保護され、複数の鍵のそれぞれは異なる権限付与されたユーザによって制御され得る。

【００３３】

さらなる技術的特徴および利益が、本発明の技術を通じて実現される。本発明の実施形態および態様は、本明細書において詳細に説明され、特許請求される主題の一部とみなされる。より良く理解するために、詳細な説明および図面を参照されたい。

【図面の簡単な説明】

【００３４】

本明細書に説明される排他的権利の詳細が特に指し示されており、明細書の結論における請求項で明確に主張されている。本発明の実施形態の上記および他の特徴並びに利点は、添付の図面と関連して記載される以下の詳細な説明から明らかである。

【００３５】

【図１】本発明の１つまたは複数の実施形態に係る、暗号化情報をメタデータとして持つ暗号化データオブジェクトを配布するための環境のブロック図を示す図である。

【００３６】

【図２】本発明の１つまたは複数の実施形態によって利用される暗号化スキームのブロック図を示す図である。

【００３７】

【図３】本発明の１つまたは複数の実施形態に係る、暗号化データオブジェクトを作成するための方法のフロー図を示す図である。

【００３８】

【図４】本発明の１つまたは複数の実施形態に係る暗号化データオブジェクトを示す図である。

【００３９】

【図５】本発明の１つまたは複数の実施形態に係る、暗号化送信側鍵インデックスを生成する方法のフロー図を示す図である。

【００４０】

【図６】本発明の１つまたは複数の実施形態に係る、暗号化データオブジェクトに含まれるデータを解読するための方法のフロー図を示す図である。

【００４１】

【図７】本発明の１つまたは複数の実施形態に係る、送信側鍵を生成するための方法のフロー図を示す図である。

【００４２】

【図８】本発明の１つまたは複数の実施形態に係るクラウドコンピューティング環境を示す図である。

【００４３】

【図９】本発明の１つまたは複数の実施形態に係る抽象化モデル層を示す図である。

【００４４】

【図１０】本発明の１つまたは複数の実施形態に係る、暗号化オブジェクトのクリエータが識別され得るように、オブジェクトを暗号化するためのシステムを示す図である。

【００４５】

本明細書に図示される図面は、例示的である。本発明の範囲を逸脱することなく、図、またはそこに説明された操作に多くの変形例があり得る。例えば、動作は異なる順序で実行され得、または、動作は追加、削除または修正され得る。また、「連結」という用語、およびその変形は、２つの要素間に通信経路を有することを説明するものであり、要素間に介在する要素／接続がなく直接接続されていることを示唆するものではない。これらの変形の全ては、明細書の一部とみなされる。

【発明を実施するための形態】

【００４６】

本発明の１つまたは複数の実施形態は、データオブジェクトの暗号化に使用した暗号化鍵が、暗号化データオブジェクト内のメタデータとして利用可能である暗号化データオブジェクトを提供する。本発明の１つまたは複数の実施形態により、１つの関係者である送信側は、送信側鍵と、１つまたは複数の関係者に属する１つまたは複数のさらなる暗号化鍵とでデータを暗号化する。これにより、送信側および任意の他の関係者はそれらの鍵を無効にし、暗号化データを使用不可能にレンダリングすることができる。

【００４７】

本発明の１つまたは複数の実施形態は、暗号化鍵を全ての関係者に配布しないように保護しながら、複数の関係者（例えば、送信側と受信側と）の間でデータの共有を容易にする。送信側鍵情報を保護するために鍵のセットを使用することによって、１つまたは複数の実施形態は、送信側鍵インデックスへのアクセスを許可または禁止することのいずれかによって、複数の関係者がデータへの同意を制御するための設備を提供する。さらに、送信側が特定の送信者鍵を制御するため、送信側はアクセスの許可または禁止を最終的に決定することができる。

【００４８】

本発明の１つまたは複数の実施形態は、暗号化されるデータと共に、送信側鍵および１つまたは複数のさらなる暗号化鍵に関する情報を暗号化データオブジェクトにパッケージ化する。本発明の１つまたは複数の実施形態により、本明細書で「暗号化データオブジェクト」と称される保護されたデータは、１つまたは複数の周辺鍵インデックスと、暗号化送信側鍵インデックスと、暗号化セッション鍵と、暗号化データとを含む。

【００４９】

本明細書において使用されるように、「セッション鍵」という用語は、送信プロセッサなどの送信側によって暗号化されるデータを暗号化するために暗号化アルゴリズムによって使用される暗号化鍵を指す。本発明の１つまたは複数の実施形態により、送信側は、セッション鍵を生成するための最良の方法を判断することができる。セッション鍵は、鍵管理システム（ＫＭＳ）から取得されることができ、またはそれはある間隔（例えば、オブジェクトごと、１日ごと、１万個のオブジェクトごとなど）で送信側によって動的に生成されることができる。本発明の１つまたは複数の実施形態により、（オブジェクトでパッケージ化される）セッション鍵はＫＭＳによって生成されるが、ＫＭＳによって保存されない。

【００５０】

本明細書において使用されるように、「暗号化セッション鍵」という用語は、送信側鍵で暗号化された後のセッション鍵を指す。

【００５１】

本明細書において使用されるように、「送信側鍵」という用語は、セッション鍵を暗号化するために、暗号化アルゴリズムによって使用される暗号化鍵を指す。送信側鍵は、送信側がデータ転送のために使用する暗号化鍵である。本発明の１つまたは複数の実施形態により、送信側鍵へのアクセスはＫＭＳによって制御される。ＫＭＳは、送信側鍵インデックスを介してアクセス可能である送信側鍵を保存する。送信側鍵インデックスは、対応する送信側鍵を配置するために、ＫＭＳによって使用される識別子（例えば、ラベル、ハンドル）である。

【００５２】

本明細書において使用されるように、「周辺鍵」という用語は、データにアクセスできる１つまたは複数の関係者（例えば、受信側）のグループを定義する鍵である。グループの例は、米国にいるユーザまたは人事部にいるユーザ、または特定のユーザの識別子を含むが、これらに限定されない。周辺鍵は、データをオープン化できることに関心を持つユーザのために方法を提供する。周辺へのアクセスは、送信側以外の関係者によって許可、修正、若しくは破棄またはその組み合わせが可能であるため、他の関係者によるデータへのアクセス制御が可能になる。本発明の１つまたは複数の実施形態により、周辺鍵へのアクセスはＫＭＳによって制御される。ＫＭＳは１つまたは複数の周辺鍵を保存した。周辺鍵インデックスは、対応する周辺鍵を配置するために、ＫＭＳによって使用される識別子（例えば、ラベル、ハンドル）である。

【００５３】

本明細書において使用されるように、「組み合わせた周辺鍵」という用語は、１つまたは複数の周辺鍵から導出される複合暗号鍵を指す。本発明の１つまたは複数の実施形態により、組み合わせた周辺鍵は、１つまたは複数の周辺鍵の値に対して排他的論理和（ＸＯＲ）演算を行うことによって導出される。組み合わせた周辺鍵は、複合鍵を作成するために、複数の鍵部分を使用する機能を提供する。複合鍵は、パッケージまたは暗号化データオブジェクトが作成された時に作成され、次に、暗号化データオブジェクトがオープン化される、または非暗号化される時に再生成される。オープン化の時に、組み合わせた周辺鍵を作成したために必要な任意の鍵部分が利用可能ではない場合、暗号化データは解読できないため、その時点から暗号化データは利用できなくなる。

【００５４】

本明細書において使用されるように、「暗号化送信側鍵インデックス」という用語は、ＫＭＳにおける、組み合わせた周辺鍵インデックスで暗号化された後の送信側鍵のインデックスを指す。

【００５５】

本発明の１つまたは複数の実施形態により、暗号化データオブジェクトが作成されているとき、送信側は、セッション鍵を暗号化するために、送信側の送信側鍵を使用する。上記で説明したように、送信側鍵はＫＭＳによって制御され、送信側は組み合わせた周辺鍵でそれらの送信側鍵インデックスを暗号化するようにＫＭＳに要求する。組み合わせた周辺鍵は、少なくとも１つの鍵（例えば、ある組織の鍵）を含むが、それはより多くの鍵（例えば、受信側鍵、他の所有者がいるさらなる鍵、ランダム鍵部分など）も含み得る。

【００５６】

本発明の１つまたは複数の実施形態により、暗号化データオブジェクトの受信側（「受信側」と称される）が暗号化データオブジェクトをオープン化することを望む場合、それは周辺鍵インデックスおよび暗号化送信側鍵インデックスをＫＭＳに送信する必要があり、ＫＭＳはセッション鍵を解読するために使用され得る送信側鍵を受信側に提供することになる。１つまたは複数の実施形態により、周辺鍵インデックスおよび暗号化送信側鍵インデックスを受信すると、ＫＭＳはまず組み合わせた周辺鍵を再度組み合わせ、組み合わせた周辺鍵の任意のコンポーネントが要求元に対して利用できない場合、操作が失敗になり、受信側が暗号化データオブジェクトにおける暗号化データを解読できなくなる。

【００５７】

組み合わせた周辺鍵の全てのコンポーネントが利用可能である場合、それらは送信側鍵インデックスを解読するために、ＫＭＳによって使用されることになる。次に、ＫＭＳにおける送信側鍵を見つけるために、送信側鍵インデックスはＫＭＳによって使用される。送信側鍵が要求元に対して利用できない場合であると、操作が失敗になり、受信側が暗号化データを解読できなくなる。全ての鍵素材が要求元に対して利用可能であってアクセス可能である場合であると、送信側鍵はＫＭＳによって暗号化データオブジェクトの要求受信側に戻される。本発明の１つまたは複数の実施形態により、要求元に鍵へのアクセス許可を与えた場合、鍵は要求元によってアクセス可能である。

【００５８】

本発明の１つまたは複数の実施形態の上記の態様は、暗号化鍵および暗号化鍵インデックスを全ての関係者に配布しないように保護しながらデータの共有を容易にすることによって、従来技術の１つまたは複数の欠点に対処する。さらに、送信側鍵情報を保護するために周辺鍵のセットを使用することにより、複数の関係者が送信側鍵インデックスへのアクセスを許可または禁止することのいずれかによってデータへのアクセスを制御することができる。送信側はその対応する送信側鍵へのアクセスを制御するため、送信側は、データにアクセスするための要求元の機能を最終的に決定する。

【００５９】

さらに、本発明の１つまたは複数の実施形態は明確的な（非暗号化）送信側鍵を受信側に提供するが、受信側は送信側鍵をその対応する送信側鍵インデックスに紐付けて戻すことができなくなる。データへのアクセスは、送信側の鍵（送信側鍵）を無効にする送信側によって、若しくは周辺鍵の一部である任意の鍵を無効にする権限を持つ送信側または他の関係者によって、またはその組み合わせによって破棄され得る。

【００６０】

さらに、本発明の１つまたは複数の実施形態は、周辺鍵の代わりに、周辺鍵インデックスを受信側に送信するため、周辺鍵が損なうリスクを低減させる。

【００６１】

さらに、本発明の１つまたは複数の実施形態は、同じセッション鍵を、送信側システムに完全にローカルな、かなりの量のデータに対して使用することができるように、鍵の使用量のスケーリングを提供する。次に、小さな操作である（例えば、比較的少ない量のコンピューティングリソースを使用する）セッション鍵の最終的なラッピング操作を、ＫＭＳによって行われることができる。

【００６２】

本発明の１つまたは複数の実施形態は、周辺鍵を利用して対応する周辺鍵へのアクセスを有する１人または複数のユーザのグループを定義することができ、データオブジェクトを暗号化するために使用される周辺鍵に対応するグループにおけるユーザの共通点は、（送信側が送信側鍵を破棄していない限り）データオブジェクトへのアクセスが与えられる。権限付与された管理者は、各グループのユーザを更新することができる。

【００６３】

１つの例において、データは、米国（ＵＳ：Ｕｎｉｔｅｄ　Ｓｔａｔｅｓ）従業員に関するデータを含む人事データであってよい。この例において、第１の周辺鍵は、ユーザが米国に配置していることを必要とし、第２の周辺鍵は、ユーザが人事部にいることを必要とすることができる。ユーザに関するこれらの判断は、コンピュータユーザ識別子に関連付けられたメタデータに基づいて行われることができる。例えば、ユーザ識別子がユーザのためにセットアップされる場合、メタデータは、ユーザの地理的な場所および勤務先部署を指定することができる。このメタデータは、ユーザのステータスへの変化に基づいて更新されることができる。暗号化データオブジェクトの受信側は、第１の周辺鍵および第２の周辺鍵の両方（および送信側鍵）へのアクセスを有する場合であると、受信側は米国に配置され、人事部にいて、従って暗号化データオブジェクトにおけるデータにアクセスする、またはデータを解読することができる。受信側が第１の周辺鍵、第２の周辺鍵または送信側鍵の任意へのアクセスを有しない場合であると、受信側は暗号化データオブジェクトにおけるデータにアクセスできない。本発明の実施形態はデータの任意のタイプに対して操作可能であるため、この例は本発明の１つまたは複数の実施形態の態様を示すことを意図するものであり、実施形態を人事データに限定する意図するものではない。

【００６４】

暗号化データオブジェクトにおけるデータへのアクセスを制御するために、データ所有者（例えば、送信側）または他の権限付与された関係者は、特定のユーザが周辺鍵にアクセスすることを破棄するようにＫＭＳに命令することができる。暗号化データオブジェクトにおけるデータへの将来のアクセスを全て防止するために、データ所有者または他の権限付与された関係者は、特定の周辺鍵を無効にするようにＫＭＳに命令することもできる

。さらに、暗号化データオブジェクトにおけるデータへの全ての将来のアクセスを防止するために、データ所有者（例えば、データの送信側）または他の権限付与された関係者は、送信側鍵を無効するようにＫＭＳに命令することもできる。

【００６５】

ここで図１を見ると、暗号化情報をメタデータとして持つ暗号化データオブジェクトを配布するための環境のブロック図１００は、本発明の１つまたは複数の実施形態に従って一般的に示されている。図１は、送信側システム１０４と、受信側システム１０６と、鍵管理システム（ＫＭＳ）１１０とを含む。図１は、本明細書でまとめてデータ１０８と称されたデータ１０８ａおよびデータ１０８ｂと、暗号化データオブジェクト１０２と、送信側鍵およびインデックス１１２と、周辺鍵およびインデックス１１４とも含む。本発明の１つまたは複数の実施形態により、データ１０８ａとデータ１０８ｂとは同じ値を持ち、データ１０８ａは送信側システム１０４に配置され、または送信側システム１０４によってアクセス可能であり、データ１０８ｂは受信側システム１０６に配置され、または受信側システム１０６によってアクセス可能である。

【００６６】

送信側システム１０４は、本明細書にさらに説明されるように、例えば、図１０のコンピュータ１００１に配置されるプロセッサ１００５上、若しくは図８のクラウドコンピューティングノード１０に配置されるプロセッサ上、またはその組み合わせで実行されるコンピュータハードウェア、若しくはソフトウェア命令またはその組み合わせによって実施され得る。本発明の１つまたは複数の実施形態により、以下に図３を参照すると、例えば、送信側システム１０４は、説明されるように、送信側の処理を行う。図１に示されたように、送信側システム１０４は、安全な方式で受信側システム１０６に送信されるデータ１０８ａを受信する。データ１０８ａは、当技術分野で知られている任意のデジタルフォーマットとすることができる。送信側システム１０４は、暗号化フォーマットとするデータ１０８と暗号化データオブジェクト１０２を解読するために受信側システム１０６によって使用されるメタデータとを含む暗号化データオブジェクト１０２を作成する。

【００６７】

本発明の１つまたは複数の実施形態により、送信側システム１０４は、安全な方式で送信されるデータ１０８ａ、暗号化データ、暗号化データオブジェクト１０２のための暗号化送信側鍵インデックス、セッション鍵、送信側鍵インデックス、送信側鍵および１つまたは複数の周辺鍵インデックスを保存する、若しくはアクセスを有する。

【００６８】

図１の実施形態に示されたように、送信側システム１０４は、暗号化データオブジェクト１０２を生成するために、ＫＭＳ１１０と相互作用する。図１に示されたように、ＫＭＳ１１０は、送信側鍵、およびそれらの対応するインデックスまたは識別子を含む送信側鍵およびインデックス１１２へのアクセスを制御する。ＫＭＳ１１０は送信側鍵のインデックスを使用して、対応する送信側鍵にアクセスする。図１に示されたように、ＫＭＳ１１０は、周辺鍵、およびそれらの対応するインデックスまたは識別子を含む周辺鍵およびインデックス１１４へのアクセスも制御する。ＫＭＳ１１０は周辺鍵のインデックスを使用して対応する周辺鍵にアクセスする。

【００６９】

鍵管理システム（ＫＭＳ）１１０は、本明細書にさらに説明されるように、例えば、図１０のコンピュータ１００１に配置されるプロセッサ１００５上、若しくは図８のクラウドコンピューティングノード１０に配置されるプロセッサ上、またはその組み合わせで実行されるコンピュータハードウェア、若しくはソフトウェア命令またはその組み合わせによって実施され得る。本発明の１つまたは複数の実施形態により、ＫＭＳ１１０は、以下で図５および７を参照して説明される鍵管理処理を行う。図１に示されたように、ＫＭＳ１１０は、例えば、送信側鍵インデックスおよび１つまたは複数の周辺鍵インデックスを送信側システム１０４から受信し、それに応じて暗号化送信側鍵インデックスを要求送信側システム１０４に戻すことによって、送信側システム１０４と相互作用する。ＫＭＳ１

１０は、例えば、暗号化送信側鍵インデックスおよび１つまたは複数の周辺鍵インデックスを受信側システム１０６から受信し、それに応じて送信側鍵を要求受信側システム１０６に戻すことによって、受信側システム１０６と相互作用することもできる。さらに、ＫＭＳは、データ１０８の所有者、または別の権限付与された関係者からコマンドを受信して、送信側鍵インデックス１１２、周辺鍵およびインデックス１１４のコンテンツを更新することができる。

【００７０】

受信側システム１０６は、本明細書にさらに説明されるように、例えば、図１０のコンピュータ１００１に配置されるプロセッサ１００５上、若しくは図８のクラウドコンピューティングノード１０に配置されるプロセッサ上、またはその組み合わせで実行されるコンピュータハードウェア、若しくはソフトウェア命令またはその組み合わせによって実施され得る。本発明の１つまたは複数の実施形態により、以下に図６を参照すると、例えば、受信側システム１０６は、説明されるように、受信側の処理を行う。図１に示されたように、受信側システム１０６は、送信側システム１０４から暗号化データオブジェクト１０２を受信する。受信側システム１０６がデータへのアクセスを有する場合、受信側システム１０６は暗号化データオブジェクト１０２を解読して非暗号化フォーマットとするデータ１０８ｂを生成する。

【００７１】

図１に示されたデータ１０８、暗号化データオブジェクト１０２、送信側鍵およびインデックス１１２、周辺鍵およびインデックス１１４は、当技術分野で知られている任意の方法（例えば、データベース、インデックス、ファイルなど）で、１つまたは複数の記憶装置における１つまたは複数の位置に保存されてよい。

【００７２】

図１は単一のＫＭＳ１１０、単一の送信側システム１０４および単一の受信側システム１０６を含む一実施形態を示すが、本発明は図１に示された実施形態に限定されない。例えば、１つまたは複数の他の実施形態は、複数の送信側システム１０４、複数の受信側システム１０６若しくは複数のＫＭＳ１１０またはその組み合わせを含んでよい。

【００７３】

図１に示されたコンポーネントの全てまたはサブセットは、有線または無線コンポーネントを使用して連結される、または接続される通信可能な１つまたは複数のプロセッサによって形成された１つまたは複数のネットワークを介して、互いに通信できる。本発明の１つまたは複数の実施形態により、図１に示されたコンポーネントの全てまたはサブセットはクラウドネットワーク、若しくはインターネットまたはその組み合わせを介して通信可能に連結される。

【００７４】

本明細書で図１のブロック図１００に関連して説明される実施形態は、任意の適切な論理が実施されてよく、本明細書で参照されるような論理は、様々な実施形態において、任意の適切なハードウェア（例えば、とりわけプロセッサ、埋込みコントローラ若しくは特定用途向け集積回路）、ソフトウェア（例えば、とりわけアプリケーション）、ファームウェア、またはハードウェア、ソフトウェアおよびファームウェアの任意の好適な組み合わせを含むことができる。

【００７５】

ここで図２を見ると、本発明の１つまたは複数の実施形態によって利用される暗号化スキームのブロック図２００は一般的に示されている。図２に示されたように、ブロック２０２において、図１のデータ１０８ａなどのデータはセッション鍵で暗号化され、セッション鍵は送信側鍵で暗号化される。図２のブロック２０４に示されたように、組み合わせた周辺鍵を生成するために、周辺鍵を組み合わせる。周辺鍵を、例えば、それらの値にＸＯＲを行うことによって、または鍵派生関数を使用するような、これに限定されないいくつかの他の繰返し可能な方式で組み合わせてよい。図２のブロック２０６に示されたように、組み合わせた周辺鍵は、セッション鍵を暗号化するために使用された送信側鍵のイン

デックスを暗号化することに使用され、その結果、送信側鍵は組み合わせた周辺鍵で暗号化される。図２に示された暗号化スキームの実施形態の使用は、送信側だけでなく、複数の他の関係者または組織に、ＫＭＳを介してデータのオープン化するためのアクセスを監視する機能を提供する。

【００７６】

ここで図３を見ると、暗号化データオブジェクトを作成するための方法３００のフロー図は、本発明の１つまたは複数の実施形態に従って一般的に示されている。図３に示された処理の全てまたは一部は、例えば、図１の送信側システム１０４に対して実行されるコンピュータハードウェア命令、若しくはソフトウェア命令またはその組み合わせによって行われることができる。ブロック３０２において、図１のデータ１０８ａなどのデータは、送信側システムによって受信され、セッション鍵を使用して送信側システムによって暗号化される。ブロック３０４において、セッション鍵は送信側鍵で暗号化される。当技術分野で知られている任意の暗号化アルゴリズムは、ブロック３０２および３０４で、任意の利用可能なモード（例えば、暗号ブロック連鎖（ＣＢＣ：Ｃｉｐｈｅｒ Ｂｌｏｃｋ Ｃｈａｉｎｉｎｇ））での高度暗号化標準（ＡＥＳ：Ａｄｖａｎｃｅｄ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ）、任意のサイズの鍵長（例えば、１２８、１９６、２５６）を有するガロア／カウンタモード（ＧＣＭ：Ｇａｌｏｉｓ／Ｃｏｕｎｔｅｒ Ｍｏｄｅ）など、これらに限定されない暗号化を行うために利用されてよい。

【００７７】

図３のブロック３０６において、送信側システムは、組み合わせた周辺鍵で送信側鍵のインデックスを暗号化するために、図１のＫＭＳ１１０などのＫＭＳに要求を送信し、ブロック３０８において、暗号化送信側鍵インデックスはＫＭＳから受信される。ブロック３１０において、送信側システムは、図１および図４の暗号化データオブジェクト１０２などの暗号化データオブジェクトを構築する。図３のブロック３１０において、暗号化データオブジェクトは生成されると、処理はブロック３１２で続ける。ブロック３１２において、暗号化データオブジェクトは、図１の受信側システム１０６などの受信側に伝送される。

【００７８】

図３のプロセスフロー図は、方法３００の操作は任意の特定の順序で実行される、または方法３００の全ての操作は全部の場合に含まれることを示すことに意図するものではない。さらに、方法３００は好適な数のさらなる操作を含むことができる。

【００７９】

ここで図４を見ると、暗号化データオブジェクト１０２または保護されたデータの一実施形態は、本発明の１つまたは複数の実施形態に従って一般的に示されている。図４に示された暗号化データオブジェクト１０２は、セッション鍵４０２で暗号化されたデータと、送信側鍵４０４で暗号化されたセッション鍵と、１つまたは複数の周辺鍵インデックス４０６と、組み合わせた周辺鍵４０８で暗号化された送信側鍵インデックスとを含む。

【００８０】

ここで図５を見ると、図４の組み合わせた周辺鍵４０８で暗号化された送信側鍵インデックスなどの暗号化送信側鍵インデックスを作成するための方法５００のフロー図は、本発明の１つまたは複数の実施形態に従って一般的に示されている。図５に示された処理の全てまたは一部は、例えば、図１のＫＭＳ１１０に対して実行されるコンピュータハードウェア命令、若しくはソフトウェア命令またはその組み合わせによって行われることができる。ブロック５０２において、送信側鍵インデックスおよび図４の周辺鍵インデックス４０４などの１つまたは複数の周辺鍵インデックスは、図１の送信側システム１０４などの要求元から受信される。処理は、受信された周辺鍵インデックスに対応する１つまたは複数の周辺鍵を取得しながら、ブロック５０４で続ける。対応する周辺鍵は、例えば、図１の周辺鍵およびインデックス１１４から取得されることができる。

【００８１】

図５のブロック５０６において、周辺鍵を組み合わせ、ブロック５０８において、ブロ

ック５０２で受信された送信側鍵インデックスを組み合わせた周辺鍵で暗号化する。鍵で排他的論理和（ＸＯＲ）を行う方法、または鍵派生関数（例えば、ＨＭＡＣベースの抽出および展開（ＨＫＤＦ：ＨＭＡＣ－ｂａｓｅｄ　Ｅｘｔｒａｃｔ－ａｎｄ－Ｅｘｐａｎｄ）、若しくはパスワードベースの鍵派生関数２（ＰＢＫＤＦ２：Ｐａｓｓｗｏｒｄ　Ｂａｓｅｄ　Ｋｅｙ　Ｄｅｒｉｖａｔｉｏｎ　Ｆｕｎｃｔｉｏｎ　２）またはその組み合わせ）を使用する方法など、鍵を組み合わせる任意の方法を利用することができるが、これらに限定されない。当技術分野で知られている任意の暗号化スキームは、任意の利用可能なモード（例えば、暗号ブロック連鎖（ＣＢＣ））での高度暗号化標準（ＡＥＳ）、任意のサイズの鍵長（例えば、１２８、１９６、２５６）を有するガロア／カウンタモード（ＧＣＭ）など、これらに限定されない送信側鍵インデックスを暗号化するために利用されてよい。ブロック５１０において、暗号化送信側鍵インデックスは要求元に伝送される。

【００８２】

図５のプロセスフロー図は、方法５００の操作は任意の特定の順序で実行される、または方法５００の全ての操作は全部の場合に含まれることを示すことに意図するものではない。さらに、方法５００は好適な数のさらなる操作を含むことができる。

【００８３】

ここで図６を見ると、暗号化データオブジェクトに含まれるデータを解読するための方法６００のフロー図は、本発明の１つまたは複数の実施形態に従って一般的に示されている。図６に示された処理の全てまたは一部は、例えば、図１の受信側システム１０６に対して実行されるコンピュータハードウェア命令、若しくはソフトウェア命令またはその組み合わせによって行われることができる。ブロック６０２において、図１および図４の暗号化データオブジェクト１０２などのオブジェクトは受信される。本発明の１つまたは複数の実施形態により、オブジェクトは、セッション鍵で暗号化されたデータと、送信側鍵で暗号化されたセッション鍵と、１つまたは複数の周辺鍵インデックスと、組み合わせた周辺鍵で暗号化された送信側鍵インデックスとを含む。

【００８４】

ブロック６０４において、受信されたオブジェクトに含まれた暗号化送信側鍵インデックスおよび１つまたは複数の周辺鍵インデックスから送信側鍵を導出するために、要求は図１のＫＭＳ１１０などのＫＭＳに送信される。受信側システムに、受信されたオブジェクトにおける１つまたは複数の周辺鍵インデックスに対応する全ての周辺鍵への、および送信側鍵へのアクセスが与えられた場合、ブロック６０６において送信側鍵はＫＭＳから受信され、１つまたは複数の周辺鍵および送信側鍵はＫＭＳにおいて有効鍵であり、それらはこの要求の前にＫＭＳから削除されていないことを意味する。

【００８５】

受信側システムに、受信されたオブジェクトにおける１つまたは複数の周辺鍵インデックスに対応する全ての周辺鍵への、および送信側鍵へのアクセスが与えられていない場合、または周辺鍵のうちの１つ若しくは複数または送信側鍵が無効鍵である場合、ブロック６０６において送信側鍵はＫＭＳから受信されない。これが発生する場合、本発明の１つまたは複数の実施形態において、ＫＭＳは要求元にエラーメッセージを送信し、他の実施形態において、ＫＭＳは単に要求に応答しない。

【００８６】

ブロック６０８は、ブロック６０６で受信された送信側鍵に応じて行われる。ブロック６０８において、暗号化セッション鍵は受信された送信側鍵を使用して解読される。図１のデータ１０８ｂなどの暗号化されていないデータを生成するために、処理は、セッション鍵を使用してオブジェクトにおけるセッション鍵で暗号化されたデータを解読しながらブロック６１０で続ける。次に、データ１０８ｂをコンピュータプログラムに保存または入力することができる。

【００８７】

図６のプロセスフロー図は、方法６００の操作は任意の特定の順序で実行される、または方法６００の全ての操作は全部の場合に含まれることを示すことに意図するものではな

い。さらに、方法６００は好適な数のさらなる操作を含むことができる。
【００８８】
ここで図７を見ると、送信側鍵を生成するための方法７００のフロー図は、本発明の１つまたは複数の実施形態に従って一般的に示されている。図７に示された処理の全てまたは一部は、例えば、図１のＫＭＳ１１０に対して実行されるコンピュータハードウェア命令、若しくはソフトウェア命令またはその組み合わせによって行われることができる。ブロック７０２において、暗号化送信側鍵インデックスおよび１つまたは複数の周辺鍵インデックスは図１の受信側システム１０６などの要求元から受信される。ブロック７０４において、１つまたは複数の周辺鍵インデックスに対応する周辺鍵は、例えば、図１の周辺鍵およびインデックス１１４から取得される。
【００８９】
ブロック７０６において、１つまたは複数の周辺鍵インデックスに対応する全ての周辺鍵が有効であり、要求元がそれらの全てへのアクセスを有する場合であると、周辺鍵を図５のブロック５０６で組み合わせた方法と同じように組み合わせ、処理はブロック７０８で続ける。１つまたは複数の周辺鍵インデックスに対応する全ての周辺鍵が有効ではない場合、若しくは要求元がそれらの全てへのアクセスを有しない場合、またはその組み合わせであると、図７に示された処理は終了する。いくつかの実施形態において、エラーメッセージは要求元に送信され、他の実施形態において、エラーメッセージは送信されない。
【００９０】
ブロック７０８において、送信側鍵が有効であり、要求元が送信側鍵へのアクセスを有する場合、送信側鍵インデックスは組み合わせたパラメータ鍵を使用して解読され、ブロック７１０は要求元に送信側鍵を伝送するために実行される。ブロック７０８において、送信側鍵が有効ではない場合、若しくは要求元が送信側鍵へのアクセスを有しない場合またはその組み合わせであると、図７に示された処理は終了する。いくつかの実施形態において、エラーメッセージは要求元に送信され、他の実施形態において、エラーメッセージは送信されない。
【００９１】
図７のプロセスフロー図は、方法７００の操作は任意の特定の順序で実行される、または方法７００の全ての操作は全部の場合に含まれることを示すことに意図するものではない。さらに、方法７００は好適な数のさらなる操作を含むことができる。
【００９２】
本開示がクラウドコンピューティングに対する詳細な説明を含むが、本明細書で記載されている教示の実装がクラウドコンピューティング環境に限定されないことが理解される。むしろ、本発明の実施形態は、現在知られている、または、今後開発される他の任意のタイプのコンピューティング環境と併せて実装することが可能である。
【００９３】
クラウドコンピューティングは、最小限の管理労力、またはサービスプロバイダとの最小限の対話で迅速にプロビジョニングおよび解放され得る構成可能なコンピューティングリソース（例えば、ネットワーク、ネットワーク帯域幅、サーバ、処理、メモリ、ストレージ、アプリケーション、仮想マシン、およびサービス）の共有プールへの簡便かつオンデマンドネットワークアクセスを可能にするためのサービス提供のモデルである。このクラウドモデルは、少なくとも５つの特徴、少なくとも３つのサービスモデル、および少なくとも４つの展開モデルを含み得る。
【００９４】
特徴は、以下の通りである。
【００９５】
オンデマンドセルフサービス：クラウドコンシューマは、サービスプロバイダとの人間相互作用を必要とすることなく必要に応じて自動的に、サーバタイムおよびネットワークストレージなどのコンピューティング機能を一方的にプロビジョニングすることができる。
【００９６】

幅広いネットワークアクセス：ネットワーク経由で機能を利用でき、異種のシンクライアントプラットフォームまたはシッククライアントプラットフォーム（例えば、携帯電話、ラップトップ、およびＰＤＡ）による使用を促進する標準メカニズムを通じて機能にアクセスする。

【００９７】

リソースのプール化：プロバイダのコンピューティングリソースをプール化して、マルチテナントモデルを使用する複数のコンシューマにサービスを提供する。複数の異なる物理リソースおよび仮想リソースが需要に従って動的に割り当てられ、再割り当てられる。コンシューマは概して提供されたリソースの正確なロケーションに対して制御または知識を有していないが、より高いレベルの抽象化（例えば、国、州、またはデータセンタ）において位置を指定することが可能である場合があるという点で、位置の独立性がある。

【００９８】

迅速な順応性：機能を迅速かつ順応的に、場合によっては自動的にプロビジョニングして素早くスケールアウトし、迅速に解除して素早くスケールインすることができる。コンシューマにとっては、多くの場合、プロビジョニングに利用可能な機能が無制限にあるように感じられ、また、いつでもどんな量でも購入可能である。

【００９９】

測定されたサービス（Ｍｅａｓｕｒｅｄ　ｓｅｒｖｉｃｅ）：クラウドシステムは、サービスのタイプ（例えば、ストレージ、処理、帯域幅、および有効なユーザアカウント）に適切なある抽象化レベルでの計測機能を活用することによって、リソース使用量を自動的に制御および最適化する。リソース使用は、監視され、制御され、また報告されるので、利用されるサービスのプロバイダおよびコンシューマの両方に透明性を提供することができる。

【０１００】

サービスモデルは、以下の通りである。

【０１０１】

ソフトウェアアズアサービス（ＳａａＳ）：コンシューマに提供される機能は、クラウドインフラストラクチャ上で実行されるプロバイダのアプリケーションを使用することである。このアプリケーションは、ウェブブラウザ（例えば、ウェブベースの電子メール）などのシンクライアントインタフェースを通じて、様々なクライアントデバイスからアクセス可能である。コンシューマは、ネットワーク、サーバ、オペレーティングシステム、ストレージ、または個々のアプリケーション機能さえも含む基礎となるクラウドインフラストラクチャを管理することも、制御することもないが、限定的なユーザ固有のアプリケーション構成設定は例外となる場合がある。

【０１０２】

プラットフォームアズアサービス（ＰａａＳ）：コンシューマに提供される機能は、クラウドインフラストラクチャ上に、プロバイダによってサポートされるプログラミング言語およびツールを使用して作成されたコンシューマが作成または取得したアプリケーションを展開することである。コンシューマは、ネットワーク、サーバ、オペレーティングシステム、またはストレージを含む基礎となるクラウドインフラストラクチャを管理することも、制御することもないが、展開されたアプリケーション、および場合によってはアプリケーションをホストする環境設定に対する制御権を有する。

【０１０３】

サービスとしてのインフラストラクチャ（Ｉｎｆｒａｓｔｒｕｃｔｕｒｅ　ａｓ　ａ　Ｓｅｒｖｉｃｅ：ＩａａＳ）：コンシューマに提供される機能は、処理と、ストレージと、ネットワークと、コンシューマが任意のソフトウェア（オペレーティングシステムおよびアプリケーションを含み得る）を展開および実行できる他の基礎的なコンピューティングリソースとをプロビジョニングすることである。コンシューマは、基礎となるクラウドインフラストラクチャを管理することも、制御することもないが、オペレーティングシステム、ストレージ、展開されたアプリケーションに対する制御権を有し、場合によっては選

択したネットワーキングコンポーネント（例えば、ホストファイアウォール）の限定的な制御権を有する。

【０１０４】

展開モデルは以下の通りである。

【０１０５】

プライベートクラウド：クラウドインフラストラクチャが組織のためだけに運用される。それは、組織または第三者によって管理することができ、オンプレミスまたはオフプレミスで存在することができる。

【０１０６】

コミュニティクラウド：クラウドインフラストラクチャがいくつかの組織により共有され、関心事項（例えば、ミッション、セキュリティ要件、ポリシ、およびコンプライアンス上の考慮事項）を共有している特定のコミュニティをサポートする。これは、組織または第三者により管理することができ、オンプレミスまたはオフプレミスに存在することができる。

【０１０７】

パブリッククラウド：クラウドインフラストラクチャが一般人または大規模な業界団体が利用できるようになっており、クラウドサービスを販売する組織により所有される。

【０１０８】

ハイブリッドクラウド：クラウドインフラストラクチャは、固有のエンティティのままであるが、データおよびアプリケーションの移植性（例えば、クラウド間の負荷分散のためのクラウドバースティング）を可能にする標準化された技術または専用の技術によって結び付けられる２つ以上のクラウド（プライベート、コミュニティ、またはパブリック）の合成である。

【０１０９】

クラウドコンピューティング環境は、ステートレス性、低結合性、モジュール性、およびセマンティック相互運用性を重視したサービス指向型である。クラウドコンピューティングの中核には、相互接続されたノードからなるネットワークを含むインフラストラクチャが存在する。

【０１１０】

ここで、図８を参照すると、例示的なクラウドコンピューティング環境５０が示されている。図示のように、クラウドコンピューティング環境５０は、クラウドコンシューマにより使用されるローカルコンピューティングデバイス（例えば、パーソナルデジタルアシスタント（ＰＤＡ）若しくはセルラ電話機５４Ａ、デスクトップコンピュータ５４Ｂ、ラップトップコンピュータ５４Ｃ、または、自動車コンピュータシステム５４Ｎ、あるいは、またはその組み合わせなど）が通信をすることができる１つまたは複数のクラウドコンピューティングノード１０を含む。ノード１０は、互いに通信してよい。それらは、本明細書の上記で説明されたようなプライベートクラウド、コミュニティクラウド、パブリッククラウド、若しくはハイブリッドクラウド、またはこれらの組み合わせなどの、１つまたは複数のネットワーク内で物理的にまたは仮想的にグループ化されてよい（図示せず）。これにより、クラウドコンピューティング環境５０は、サービスとしてインフラストラクチャ、プラットフォーム、若しくはソフトウェア、またはその組み合わせを提供することが可能になり、こうしたもののために、クラウドコンシューマがローカルコンピューティングデバイス上にリソースを維持する必要がない。図８に示すコンピューティングデバイス５４Ａ～５４Ｎのタイプは単なる一例であることを意図したものであり、コンピューティングノード１０およびクラウドコンピューティング環境５０は、任意のタイプのネットワーク若しくはネットワークアドレス可能な接続またはその両方によって（例えば、ウェブブラウザを用いて）、任意のタイプのコンピュータ化デバイスと通信できることが理解される。

【０１１１】

ここで、図９を参照すると、クラウドコンピューティング環境５０（図８）によって提

供された機能抽象化層のセットが示されている。図９に示されているコンポーネント、層、および機能が例示のみを意図したものであり、本発明の実施形態がそれらに限定されないことが事前に理解されるべきである。示されているように、以下の層および対応する機能が提供されている。

【０１１２】

ハードウェアおよびソフトウェア層６０はハードウェアおよびソフトウェアコンポーネントを含む。ハードウェアコンポーネントの例には、メインフレーム６１、ＲＩＳＣ（縮小命令セットコンピュータ）アーキテクチャベースのサーバ６２、サーバ６３、ブレードサーバ６４、記憶装置６５、並びにネットワークおよびネットワーキングコンポーネント６６が含まれている。いくつかの実施形態において、ソフトウェアコンポーネントには、ネットワークアプリケーションサーバソフトウェア６７およびデータベースソフトウェア６８が含まれている。

【０１１３】

仮想化層７０は、仮想エンティティの以下の例が提供されてよい抽象化層を提供し、その例とは、仮想サーバ７１、仮想ストレージ７２、仮想プライベートネットワークを含む仮想ネットワーク７３、仮想アプリケーションおよびオペレーティングシステム７４並びに仮想クライアント７５である。

【０１１４】

１つの例において、管理層８０は、以下で説明される機能を提供し得る。リソースプロビジョニング８１では、クラウドコンピューティング環境内でタスクを実行するのに利用されるコンピューティングリソースおよび他のリソースの動的調達を提供する。計測および価格設定８２では、クラウドコンピューティング環境内でリソースが利用されると費用の追跡を行い、これらのリソースの消費に対して請求書作成または請求書送付を提供する。１つの例において、これらのリソースは、アプリケーションソフトウェアライセンスを含み得る。セキュリティが、クラウドコンシューマおよびタスクについての身元確認、並びに、データおよび他のリソースについての保護を提供する。ユーザポータル８３では、コンシューマおよびシステム管理者のためにクラウドコンピューティング環境へのアクセスを提供する。サービスレベル管理８４では、必要なサービスレベルが満たされるように、クラウドコンピューティングリソースの割り当ておよび管理を提供する。サービスレベル合意書（ＳＬＡ）の立案および履行８５では、将来の要件がＳＬＡに従って予測されるクラウドコンピューティングリソースの事前準備およびその調達を提供する。

【０１１５】

ワークロード層９０は、クラウドコンピューティング環境が利用され得る機能の例を提供する。この層から提供され得るワークロードおよび機能の例には、マッピングおよびナビゲーション９１、ソフトウェア開発およびライフサイクル管理９２、仮想教室教育の提供９３、データ分析処理９４、トランザクション処理９５、およびデータ暗号化／復号９６が含まれる。

【０１１６】

本発明の１つまたは複数の実施形態は、現在既知のまたは後に開発される任意の他のタイプのコンピューティング環境と併せて実施されることが可能であることが理解されている。

【０１１７】

ここで図１０を見ると、暗号化情報をメタデータとして持つ暗号化データオブジェクトを配布するためのコンピュータシステムは、本発明の１つまたは複数の実施形態に従って一般的に示されている。本明細書で説明される方法は、ハードウェア、ソフトウェア（例えば、ファームウェア）またはその組み合わせで実施され得る。本発明の１つまたは複数の例示的な実施形態において、本明細書で説明される方法は、パーソナルコンピュータ、ワークステーション、ミニコンピュータまたはメインフレームコンピュータなどの専用または汎用デジタルコンピュータのマイクロプロセッサの一部として、ハードウェアで実施される。従って、システム１０００は、Ｏ／Ｓの複数のインスタンスを同時に実行するこ

とが可能である汎用コンピュータまたはメインフレーム１００１を含んでよい。
【０１１８】
本発明の１つまたは複数の例示的な実施形態において、ハードウェアアーキテクチャに関して、図１０に示されたように、コンピュータ１００１は、１つまたは複数のプロセッサ１００５と、メモリコントローラ１０１５に連結されたメモリ１０１０と、ローカル入力／出力コントローラ１０３５を介して通信可能に連結された１つまたは複数の入力もしくは出力またはその両方の（Ｉ／Ｏ）デバイス１０４０、１０４５（若しくは周辺機器）とを含む。入力／出力コントローラ１０３５は、例えば、当技術分野で知られているような、１つまたは複数のバスまたは他の有線若しくは無線接続であり得るが、これらに限定されない。入力／出力コントローラ１０３５は、簡潔のために省略されている、通信を可能にするコントローラ、バッファ（キャッシュ）、ドライバ、リピータ、および受信側などのさらなる要素を有し得る。さらに、ローカルインタフェースは、上記コンポーネントの間での適切な通信を可能にする、アドレス、制御、もしくはデータ接続、またはその組み合わせを含み得る。入力／出力コントローラ１０３５は、出力デバイス１０４０および１０４５にアクセスするように構成された複数のサブチャネルを含んでよい。サブチャネルは光ファイバ通信ポートを含んでよい。
【０１１９】
プロセッサ１００５は、特にキャッシュストレージまたはメモリ１０１０などのストレージ１０２０に保存されたソフトウェアを実行するためのハードウェアデバイスである。プロセッサ１００５は、任意のカスタムメイドまたは市販のプロセッサ、中央処理装置（ＣＰＵ：ｃｅｎｔｒａｌ　ｐｒｏｃｅｓｓｉｎｇ　ｕｎｉｔ）、コンピュータ１００１に関連するいくつかのプロセッサのうちの補助プロセッサ、（マイクロチップまたはチップセットの形態での）半導体ベースのマイクロプロセッサ、マクロプロセッサ、または一般的に命令を実行する任意のデバイスであることができる。
【０１２０】
メモリ１０１０は、揮発性メモリ要素（例えば、ランダムアクセスメモリ（ＤＲＡＭ、ＳＲＡＭ、ＳＤＲＡＭなどのようなＲＡＭ））および不揮発性メモリ要素（例えば、ＲＯＭ、消去可能プログラム可能リードオンリメモリ（ＥＰＲＯＭ：Ｅｒａｓａｂｌｅ　Ｐｒｏｇｒａｍｍａｂｌｅ　Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）、電気的消去可能なプログラム可能リードオンリメモリ（ＥＥＰＲＯＭ：Ｅｌｅｃｔｒｉｃａｌｌｙ　Ｅｒａｓａｂｌｅ　Ｐｒｏｇｒａｍｍａｂｌｅ　Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）、プログラム可能リードオンリメモリ（ＰＲＯＭ：Ｐｒｏｇｒａｍｍａｂｌｅ　Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）、テープ、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）、ディスク、ディスケット、カートリッジ、カセットなどのうちのいずれか１つまたはその組み合わせを含むことができる。また、メモリ１０１０は、電子、磁気、光、もしくは他のタイプの記憶媒体、またはその組み合わせを組み込み得る。メモリ１０１０は、様々なコンポーネントが互いに離れた場所に位置しているが、プロセッサ１００５によってアクセスすることができる、分散アーキテクチャを有することができることに留意されたい。
【０１２１】
メモリ１０１０における命令は、１つまたは複数の別々のプログラムを含んでもよく、各プログラムは、論理機能を実施するための実行可能命令の順序付きリストを含む。図１０の例において、メモリ１０１０における命令は適切なオペレーティングシステム（ＯＳ）１０１１を開始する。オペレーティングシステム１０１１は本質的に他のコンピュータプログラムの実行を制御し、スケジュール、入出力制御、ファイルおよびデータ管理、メモリ管理、通信制御および関連サービスを提供する。
【０１２２】
本発明の１つまたは複数の実施形態により、メモリ１０１０は複数の論理パーティション（ＬＰＡＲ：ｌｏｇｉｃａｌ　ｐａｒｔｉｔｉｏｎ）を含むことができ、各ＬＰＡＲがオペレーティングシステムのインスタンスを実行する。ＬＰＡＲは、メモリ１０１０に保

存されてプロセッサ１００５によって実行されるプログラムであり得るハイパーバイザによって、管理されてよい。

【０１２３】

本発明の１つまたは複数の例示的な実施形態において、従来のキーボード１０５０およびマウス１０５５は、入力／出力コントローラ１０３５に連結されることができる。Ｉ／Ｏデバイス１０４０、１０４５などの他の出力デバイスは、例えば、プリンタ、スキャナ、マイクロフォンなどの入力デバイスを含んでよいが、これらに限定されない。最後に、Ｉ／Ｏデバイス１０４０、１０４５は、入力および出力の両方を通信する、例えば、（他のファイル、デバイス、システム、若しくはネットワークにアクセスするための）ネットワークインタフェースカード（ＮＩＣ）または変調器／復調器、無線周波数（ＲＦ）または他の送受信側、電話インタフェース、ブリッジ、ルータ、および同様のもののようなデバイスをさらに含み得るが、これらに限定されない。システム１０００は、ディスプレイ１０３０に連結されたディスプレイコントローラ１０２５をさらに含むことができる。

【０１２４】

本発明の１つまたは複数の例示的な実施形態において、システム１０００は、ネットワーク１０６５に連結するために、ネットワークインタフェース１０６０をさらに含むことができる。ネットワーク１０６５は、ブロードバンド接続を介した、コンピュータ１００１、任意の外部サーバ、クライアント、および同様のものの間の通信用のＩＰベースのネットワークであり得る。ネットワーク１０６５は、コンピュータ１００１と外部システムとの間でデータを伝送および受信する。例示的な実施形態において、ネットワーク１０６５はサービスプロバイダによって管理される管理ＩＰネットワークであることができる。ネットワーク１０６５は、例えば、ＷｉＦｉ（登録商標）、ＷｉＭａｘ（登録商標）などのような無線プロトコルおよび技術を使用して、無線方式で実装されてよい。ネットワーク１０６５はまた、ローカルエリアネットワーク、ワイドエリアネットワーク、メトロポリタンエリアネットワーク、インターネットネットワーク、または、他の類似のタイプのネットワーク環境などのパケット交換ネットワークであり得る。ネットワーク１０６５は、固定無線ネットワーク、無線ローカルエリアネットワーク（ＬＡＮ）、無線ワイドエリアネットワーク（ＷＡＮ）、パーソナルエリアネットワーク（ＰＡＮ）、仮想プライベートネットワーク（ＶＰＮ）、イントラネットまたは他の好適なネットワークシステムであってよく、信号を受信および伝送するための機器を含む。

【０１２５】

コンピュータ１００１がＰＣ、ワークステーション、インテリジェントデバイスなどである場合、メモリ１０１０における命令は基本入力出力システム（ＢＩＯＳ）（簡潔さのために省略される）をさらに含んでよい。ＢＩＯＳは、起動時にハードウェアを初期化およびテストし、ＯＳ１０１１を開始し、ハードウェアデバイス間のデータの転送をサポートする基本的ソフトウェアルーチンのセットである。ＢＩＯＳは、コンピュータ１００１が起動されている時にＢＩＯＳが実行され得るように、ＲＯＭに保存されている。

【０１２６】

コンピュータ１００１が動作中である場合、データをメモリ１０１０との間に通信し、命令に従がってコンピュータ１００１の操作を一般的に制御するために、プロセッサ１００５はメモリ１０１０内に保存された命令を実行するように構成される。本発明の１つまたは複数の実施形態により、コンピュータ１００１は、図８のクラウドコンピューティングノード１０の一例である。

【０１２７】

本発明の様々な実施形態は、関連図面を参照して本明細書に説明される。本発明の代替的な実施形態は、本発明の範囲から逸脱することなく考案され得る。以下の説明および図面における要素間で、様々な接続関係および位置関係（例えば、上方、下方、隣接など）が記載される。これらの接続関係若しくは位置関係またはその組み合わせは、別途指定がない限り、直接的または間接的であり得、本発明はこの点で限定的であることを意図するものではない。従って、エンティティ間の連結は、直接的または間接的な連結を指してよ

く、エンティティ間の位置関係は、直接的または間接的な位置関係であり得る。さらに、本明細書で説明される様々なタスクおよびプロセス段階は、本明細書で詳細に説明されていない追加の段階または機能を有する、より広範囲の手順またはプロセスに組み込まれ得る。

【０１２８】

本明細書で説明された方法のうちの１つまたは複数は、データ信号に応じた論理機能を実施する論理ゲートを有する個別論理回路、適切な組み合わせ論理ゲートを有する特定用途向け集積回路（ＡＳＩＣ）、プログラム可能ゲートアレイ（ＰＧＡ）、フィールドプログラマブルゲートアレイ（ＦＰＧＡ）など、当技術分野で全てよく知られている技術のうちの任意の１つまたは組み合わせによって実施され得る。

【０１２９】

簡潔さのために、本発明の態様を作成および使用することに関連する従来技術は、本明細書で詳細に説明されてもよく、またはされなくてもよい。具体的には、コンピューティングシステム、および本明細書で説明される様々な技術的特徴を実装するための特定のコンピュータプログラムの様々な態様は周知である。従って、簡潔の目的で、多くの従来の実装の詳細は本明細書では簡潔にのみ言及されるか、あるいは、周知のシステムおよび／若しくはプロセスまたはその両方の詳細を提供することなく完全に省略される。

【０１３０】

いくつかの実施形態において様々な機能または動作は、所与の位置で、もしくは、１つまたは複数の装置若しくはシステムの操作に関連して、またはその組み合わせで行われ得る。いくつかの実施形態において、所与の機能または動作の一部を第１のデバイスまたは位置で実行することができ、機能または動作の残りを１つまたは複数の追加のデバイスまたは位置で実行することができる。

【０１３１】

本明細書で使用される用語は、特定の実施形態のみを説明するためのものであり、限定することを意図するものではない。

本明細書において使用されるように、文脈が別途明確に示さない限り、単数形の「ａ」、「ａｎ」および「ｔｈｅ」は、複数形も含むことを意図する。本明細書で使用される場合、用語「ｃｏｍｐｒｉｓｅ」もしくは「ｃｏｍｐｒｉｓｉｎｇ」またはその両方は、記載された特徴、整数、段階、操作、要素、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指定するが、１つまたは複数の他の特徴、整数、段階、操作、要素のコンポーネント、もしくはそれらのグループ、またはその組み合わせの存在または追加を排除しないことがさらに理解されるであろう。

【０１３２】

以下の特許請求の範囲における全ての手段または段階プラス機能要素の対応する構造、材料、動作、および均等物は、具体的に請求された他の請求項の要素と組み合わせて機能を実行するための任意の構造、材料、または動作を含むことを意図している。本開示は、例示および説明の目的のために提示されたものであるが、網羅的であること、または開示された形態に限定されることを意図するものではない。本開示の範囲を逸脱することなく、多くの修正および変形が当業者には明らかであろう。実施形態は、本開示の原理および実際の適用を最もよく説明するために、また、当業者が、企図される特定の用途に適するように様々な変更を伴う様々な実施形態について本開示を理解できるように、選択および説明された。

【０１３３】

本明細書に図示される図面は、例示的である。この図またはそこに記載されている段階（または操作）には、多くの変形例があり得る。例えば、動作は異なる順序で実行され得、または、動作は追加、削除または修正され得る。また、「連結」という用語は、２つの要素間に信号経路を有することを説明し、その間に介在する要素／接続がなく、要素間が直接接続されていることを示唆するものではない。これらの変形例は、全て本開示の一部とみなされる。

【０１３４】
以下の定義および略語は、特許請求の範囲および明細書の解釈に使用される。本明細書において使用されるように、「備える（ｃｏｍｐｒｉｓｅｓ）」、「備える（ｃｏｍｐｒｉｓｉｎｇ）」、「含む（ｉｎｃｌｕｄｅｓ）」、「含む（ｉｎｃｌｕｄｉｎｇ）」、「有する（ｈａｓ）」、「有する（ｈａｖｉｎｇ）」、「含む（ｃｏｎｔａｉｎｓ）」、若しくは「含む（ｃｏｎｔａｉｎｉｎｇ）」という用語、またはそれらの他の変形は、非排他的包含をカバーすることを意図している。例えば、要素のリストを含む組成物、混合物、プロセス、方法、物品、または装置は、必ずしもこれらの要素のみに限定されず、明示的に列挙されていない、またはそのような組成物、混合物、プロセス、方法、物品、または装置に固有の他の要素のリストを含んでもよい。

【０１３５】
さらに、「例示的」という用語は、本明細書において、「例、インスタンス、または例示として機能する」ことを意味するために使用される。本明細書において「例示的」として説明される任意の実施形態または設計は、必ずしも、他の実施形態または設計よりも好ましいまたは有利であると解釈されるものではない。「少なくとも１つ」および「１つまたは複数」という用語は、１よりも大きいまたはそれに等しい任意の整数、すなわち、１、２、３、４などを含むと理解される。「複数の」という用語は、２よりも大きいまたはそれに等しい任意の整数、すなわち、２、３、４、５などを含むと理解される。「接続」という用語は、間接的な「接続」と直接的な「接続」の両方を含むことができる。

【０１３６】
「約（ａｂｏｕｔ）」、「実質的に（ｓｕｂｓｔａｎｔｉａｌｌｙ）」、「およそ（ａｐｐｒｏｘｉｍａｔｅｌｙ）」という用語およびそれらの変形は、出願時に利用可能な機器に基づいて特定の数量の測定に関連付けられた誤差の程度を含むことを意図している。例えば、「約」とは、所与の値の、±８％または５％、または２％の範囲を含み得る。

【０１３７】
本発明は、任意の可能な技術的詳細レベルの統合におけるシステム、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り得る。コンピュータプログラム製品は、プロセッサに本発明の態様を実行させる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記憶媒体（または複数の媒体）を含んでよい。

【０１３８】
コンピュータ可読記憶媒体は、命令実行デバイスによる使用のための命令を保持および保存できる有形デバイスとすることができる。コンピュータ可読記憶媒体は、例えば、電子記憶装置、磁気記憶装置、光学記憶装置、電磁記憶装置、半導体記憶装置、または上記ものの任意の好適な組み合わせであり得るが、これらに限定されない。コンピュータ可読記憶媒体のより具体的な例の非網羅的なリストは、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）、リードオンリメモリ（ＲＯＭ）、消去可能プログラマブルリードオンリメモリ（ＥＰＲＯＭまたはフラッシュメモリ）、スタティックランダムアクセスメモリ（ＳＲＡＭ）、ポータブルコンパクトディスクリードオンリメモリ（ＣＤ－ＲＯＭ）、デジタル多用途ディスク（ＤＶＤ）、メモリスティック、フロッピディスク、パンチカードまたは命令が記録されている溝内の隆起構造などの機械的にエンコードされたデバイス、および、上記ものの任意の好適な組み合わせを含む。コンピュータ可読記憶媒体は、本明細書において使用されるように、電波若しくは他の自由に伝搬する電磁波、導波路若しくは他の伝送媒体を通じて伝搬する電磁波（例えば、光ファイバケーブルを通過する光パルス）、またはワイヤを通じて伝送される電気信号などの一時的な信号自体と解釈されてはならない。

【０１３９】
本明細書に説明されるコンピュータ可読プログラム命令は、コンピュータ可読記憶媒体からそれぞれのコンピューティング／処理デバイスに、または、ネットワーク、例えばインターネット、ローカルエリアネットワーク、ワイドエリアネットワーク若しくは無線ネットワークまたはその組み合わせを介して外部コンピュータまたは外部記憶装置にダウン

ロードできる。ネットワークは、銅伝送ケーブル、光伝送ファイバ、無線伝送、ルータ、ファイアウォール、スイッチ、ゲートウェイコンピュータ、若しくはエッジサーバ、またはその組み合わせを備え得る。各コンピューティング／処理デバイスにおけるネットワークアダプタカードまたはネットワークインタフェースは、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、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記憶媒体に保存するためにコンピュータ可読プログラム命令を転送する。

【０１４０】

本発明の操作を実行するためのコンピュータ可読プログラム命令は、アセンブラ命令、命令セットアーキテクチャ（ＩＳＡ）命令、機械命令、機械依存命令、マイクロコード、ファームウェア命令、状態設定データ、集積回路用の構成データ、または、Ｓｍａｌｌｔａｌｋ（登録商標）若しくはＣ＋＋などといったオブジェクト指向プログラミング言語、および「Ｃ」プログラミング言語若しくは同様のプログラミング言語などの手続型プログラミング言語を含む、１つまたは複数のプログラミング言語の任意の組み合わせで書き込まれたソースコードまたはオブジェクトコードのいずれかであり得る。コンピュータ可読プログラム命令は、ユーザのコンピュータ上で全て実行され得るか、スタンドアロンソフトウェアパッケージとしてユーザのコンピュータ上で部分的に実行され得るか、部分的にユーザのコンピュータ上で且つ部分的にリモートコンピュータ上で実行され得るか、または、リモートコンピュータ若しくはサーバ上で全て実行され得る。後者のシナリオでは、リモートコンピュータは、ローカルエリアネットワーク（ＬＡＮ）若しくはワイドエリアネットワーク（ＷＡＮ）を含む任意のタイプのネットワークを介してユーザのコンピュータに接続されてもよく、またはその接続は、外部コンピュータに対して（例えば、インターネットサービスプロバイダを使用してインターネットを介して）行われてもよい。いくつかの実施形態において、例えば、プログラマブル論理回路、フィールドプログラマブルゲートアレイ（ＦＰＧＡ）、またはプログラマブル論理アレイ（ＰＬＡ）を含む電子回路は、本発明の態様を実行するべく、コンピュータ可読プログラム命令の状態情報を利用して電子回路をパーソナライズすることにより、コンピュータ可読プログラム命令を実行し得る。

【０１４１】

本発明の態様は、本発明の実施形態に従う方法、装置（システム）、およびコンピュータプログラム製品のフローチャート図もしくはブロック図、またはその両方を参照して本明細書で説明される。フローチャート図若しくはブロック図、またはその両方の各ブロック、並びに、フローチャート図若しくはブロック図、またはその両方のブロックの組み合わせは、コンピュータ可読プログラム命令によって実装することができることが理解されよう。

【０１４２】

これらのコンピュータ可読プログラム命令は、機械を生成するように汎用コンピュータ、専用コンピュータまたは他のプログラム可能なデータ処理装置のプロセッサに提供され、その結果、コンピュータまたは他のプログラム可能なデータ処理装置のプロセッサを介して実行される命令が、フローチャート若しくはブロック図またはその両方の単数若しくは複数のブロックにおいて指定されている機能／動作を実装する手段を作成するようにしてよい。また、これらのコンピュータ可読プログラム命令は、コンピュータ可読記憶媒体に保存されてよく、当該命令は、コンピュータ、プログラマブルデータ処理装置若しくは他のデバイス、またはその組み合わせに対し、特定の方法で機能するよう命令することができ、それにより、命令を保存したコンピュータ可読記憶媒体は、フローチャート若しくはブロック図、またはその両方の単数または複数のブロックで指定された機能／動作の態様を実装する命令を含む製品を含むようになる。

【０１４３】

コンピュータ可読プログラム命令はまた、コンピュータ、他のプログラム可能なデータ処理装置、または他のデバイス上で一連の演算段階を実行させてコンピュータ実装プロセスを生成するように、コンピュータ、他のプログラム可能な装置、または他のデバイス上

にロードされ得、その結果、コンピュータ、他のプログラム可能な装置、または他のデバイス上で実行する命令は、フローチャートもしくはブロック図、またはその両方の１つのブロックまたは複数のブロックで指定された機能／動作を実装する。

【０１４４】

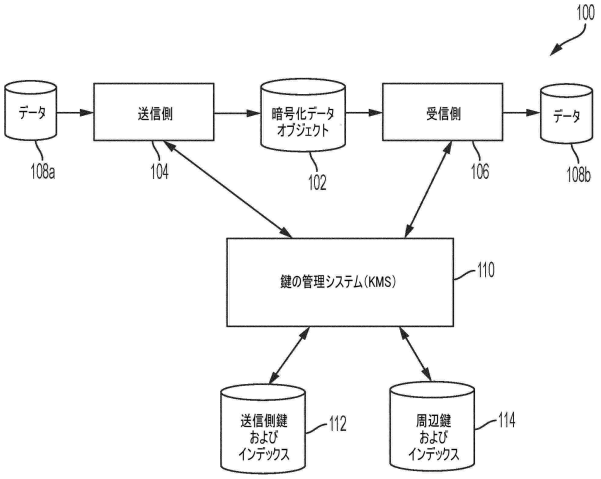
図面内のフローチャートおよびブロック図は、本発明の様々な実施形態に従うシステム、方法、およびコンピュータプログラム製品の可能な実装のアーキテクチャ、機能、および操作を示す。これに関して、フローチャートまたはブロック図における各ブロックは、指定された論理機能を実装する１つまたは複数の実行可能命令を含む命令のモジュール、セグメント、または一部を表し得る。いくつかの代替的な実装形態において、ブロックに記されている機能は、図面に記されている順序とは異なる順序で行われ得る。例えば、連続して示されている２つのブロックは、実際には、実質的に同時に実行されてもよいし、ブロックは、関与する機能に依存して逆の順序で実行される場合もあり得る。ブロック図若しくはフローチャート図またはその組み合わせの各ブロック、および、ブロック図若しくはフローチャート図またはその組み合わせにおけるブロックの組み合わせが、指定された機能若しくは動作を実行する、または特定用途向け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行する、特定用途向けハードウェアベースのシステムによって実装され得ることにも留意されたい。

【０１４５】

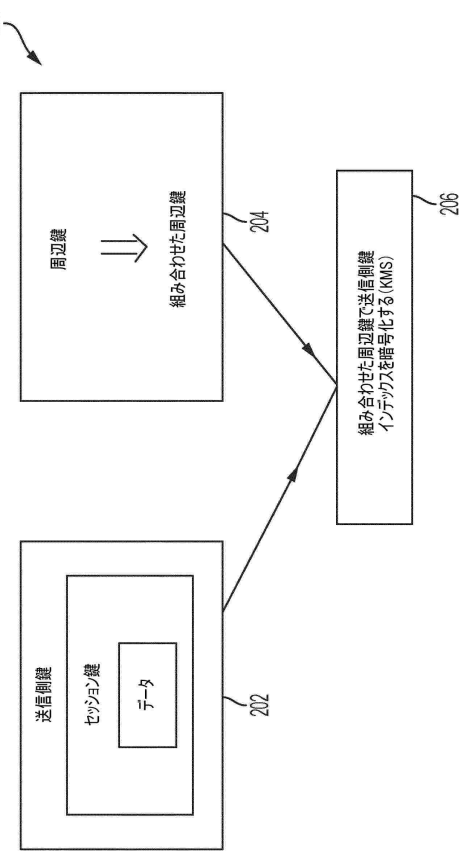
本発明の様々な実施形態の説明は、説明のために提示されたが、開示された実施形態を網羅し、限定することを意図するものではない。説明された実施形態の範囲から逸脱することなく、多くの修正および変形が、当技術分野における当業者には明らかであろう。本明細書で使用される用語は、実施形態の原理、実際の適用、若しくは市場で見られる技術に対する技術的改善点を最も良く説明するため、あるいは、他の当業者が本明細書に説明される実施形態を理解することを可能にするために選択された。

【図面】

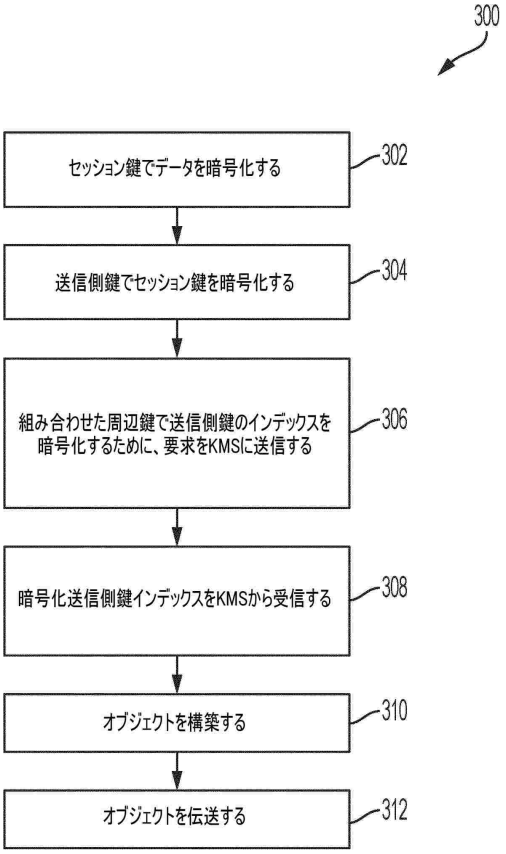
【図１】


100
データ
送信側
暗号化データ
オブジェクト
受信側
データ
108a
104
102
106
108b
鍵の管理システム(KMS)
110
送信側鍵
および
インデックス
112
周辺鍵
および
インデックス
114

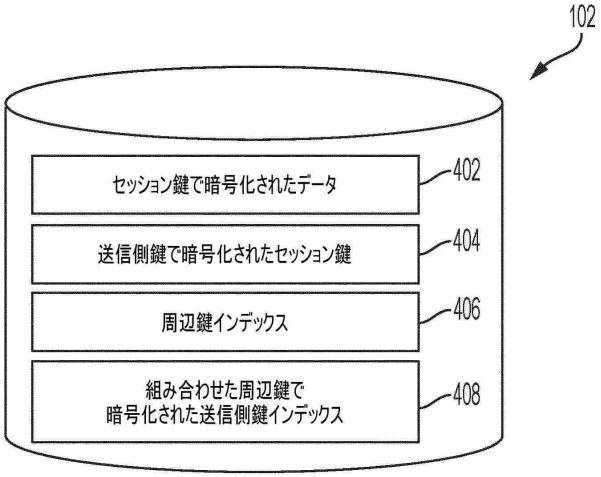
【図２】


200
周辺鍵
組み合わせた周辺鍵
204
206
組み合わせた周辺鍵で送信側鍵
インデックスを暗号化する(KMS)
送信側鍵
セッション鍵
データ
202

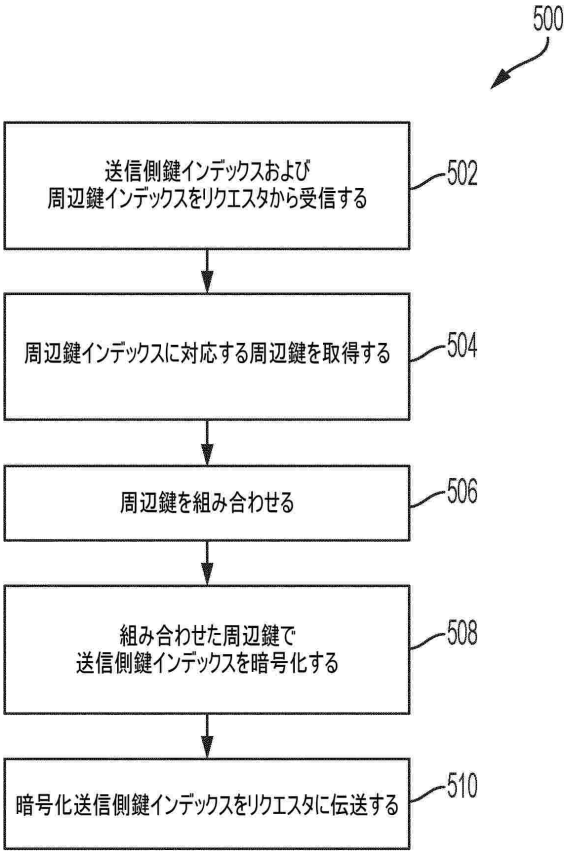
【図３】


300
セッション鍵でデータを暗号化する
302
送信側鍵でセッション鍵を暗号化する
304
組み合わせた周辺鍵で送信側鍵のインデックスを暗号化するために、要求をKMSに送信する
306
暗号化送信側鍵インデックスをKMSから受信する
308
オブジェクトを構築する
310
オブジェクトを伝送する
312

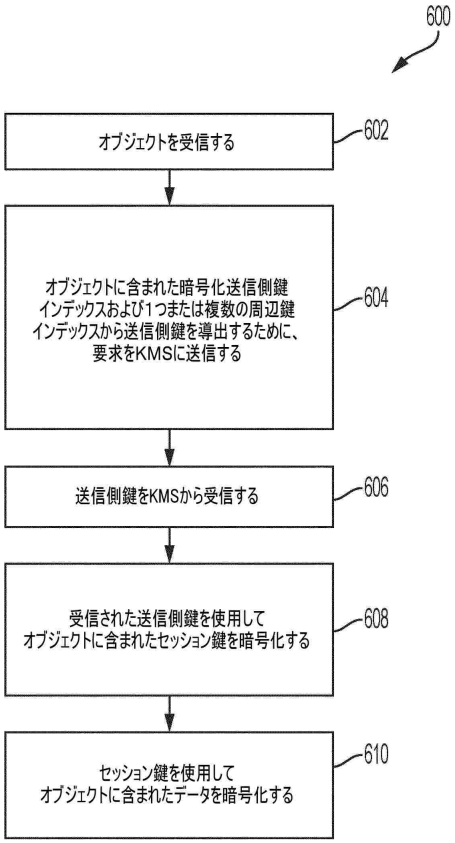
【図４】


102
セッション鍵で暗号化されたデータ
402
送信側鍵で暗号化されたセッション鍵
404
周辺鍵インデックス
406
組み合わせた周辺鍵で暗号化された送信側鍵インデックス
408

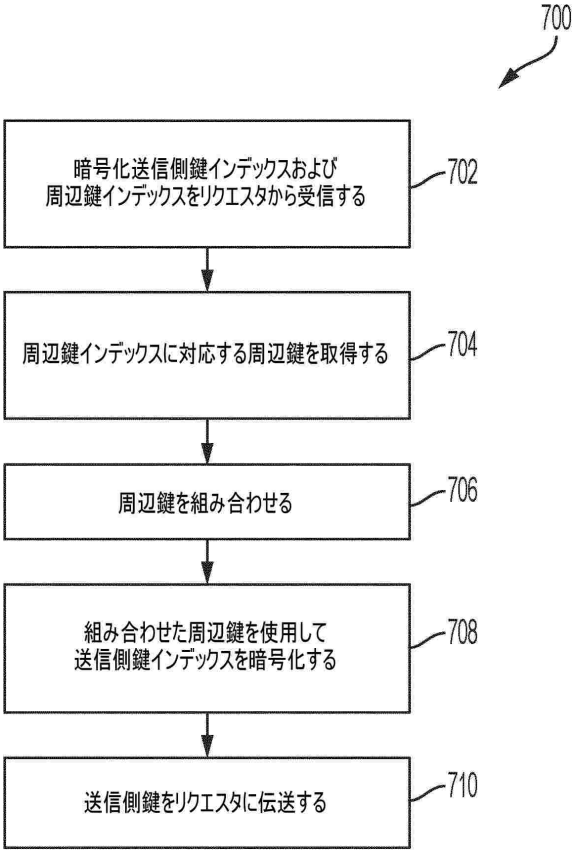
【図５】


500
送信側鍵インデックスおよび周辺鍵インデックスをリクエスタから受信する
502
周辺鍵インデックスに対応する周辺鍵を取得する
504
周辺鍵を組み合わせる
506
組み合わせた周辺鍵で送信側鍵インデックスを暗号化する
508
暗号化送信側鍵インデックスをリクエスタに伝送する
510

【図６】


600
オブジェクトを受信する
602
オブジェクトに含まれた暗号化送信側鍵インデックスおよび1つまたは複数の周辺鍵インデックスから送信側鍵を導出するために、要求をKMSに送信する
604
送信側鍵をKMSから受信する
606
受信された送信側鍵を使用してオブジェクトに含まれたセッション鍵を暗号化する
608
セッション鍵を使用してオブジェクトに含まれたデータを暗号化する
610

【図７】



【図８】

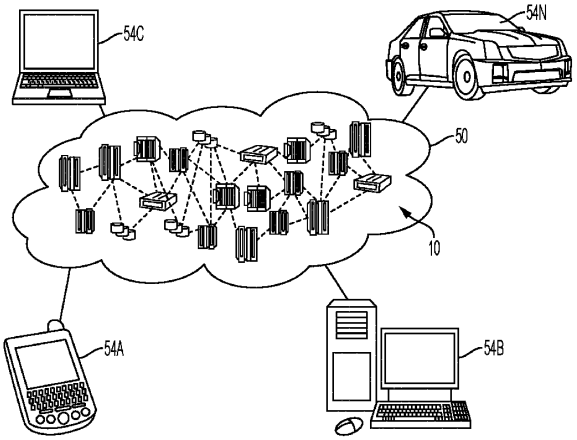
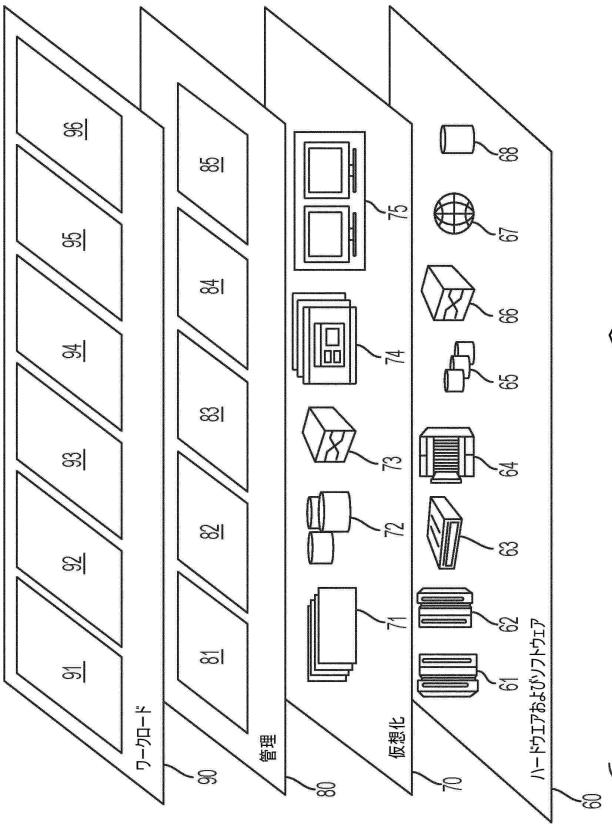
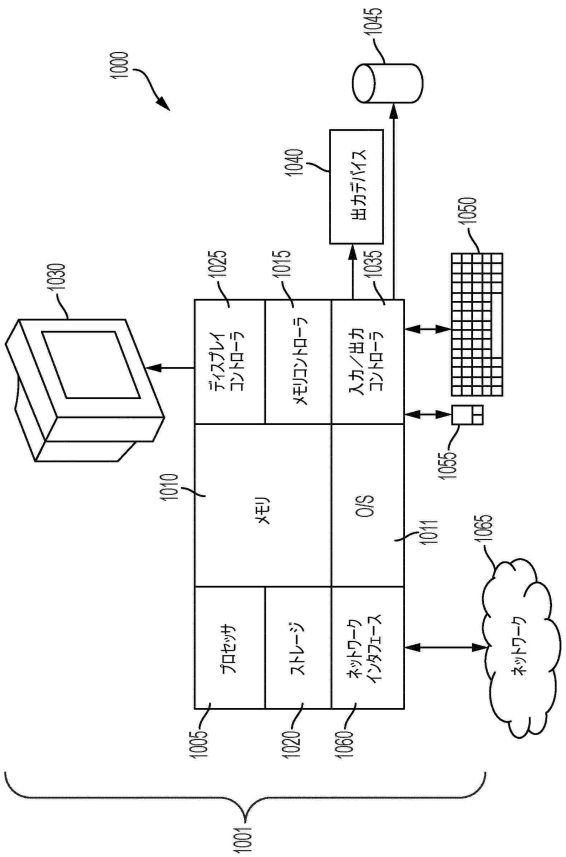


FIG. 8

【図９】



【図１０】



フロントページの続き

(74)代理人　100120710
弁理士　片岡 忠彦
(72)発明者　ソフィア、アンソニー、トーマス
アメリカ合衆国 １２６０１－５４００ ニューヨーク州、ポキプシー サウス ロード ２４５５
アイビーエム コーポレーション
審査官　中里 裕正
(56)参考文献　特開２００４－１６６１５４（ＪＰ，Ａ）
米国特許出願公開第２０１５／０３７２９９１（ＵＳ，Ａ１）
米国特許第１００３３７０３（ＵＳ，Ｂ１）
国際公開第２０１９／２０４４８７（WO，Ａ１）
(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　９／０８
Ｈ０４Ｌ　９／１４