(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2016-9887
(P2016-9887A)
(43)公開日　平成28年1月18日(2016.1.18)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/32	(2006.01)	H04L	9/00	675A	5J104
G06F 21/64	(2013.01)	G06F	21/24	167A	
G06F 21/62	(2013.01)	G06F	21/24	166E	

審査請求 未請求　請求項の数 12　ＯＬ　（全 25 頁）

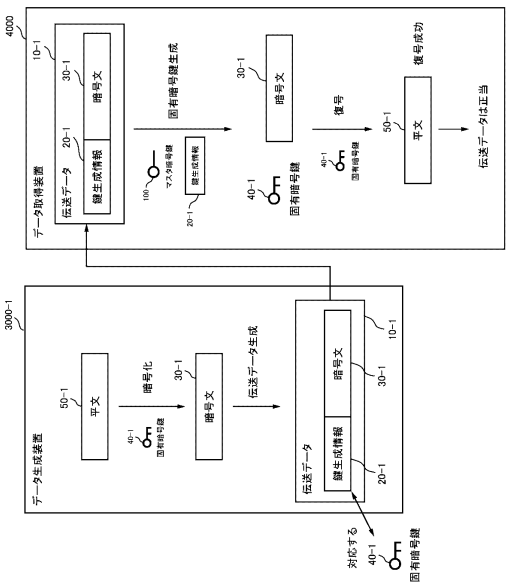
(21)出願番号　特願2014-127670 (P2014-127670)
(22)出願日　平成26年6月20日 (2014.6.20)

(71)出願人　800000068
学校法人東京電機大学
東京都足立区千住旭町５番
(74)代理人　100110928
弁理士　速水　進治
(72)発明者　鈴木　秀一
東京都足立区千住旭町５番　学校法人東京電機大学内

Ｆターム(参考)　5J104 AA08 AA16 EA04 EA08 EA18 JA03 LA02 NA02 NA37 NA38 PA14

(54)【発明の名称】データ伝送システム、データ伝送方法、データ生成装置、データ取得装置、及びプログラム

(57)【要約】
【課題】電子署名の実行速度を高速化する。
【解決手段】データ生成装置３０００－１は、データ生成装置３０００－１の固有暗号鍵である固有暗号鍵４０－１を用いて平文５０－１を暗号化することで、暗号文３０－１を生成する。そして、データ生成装置３０００－１は、固有暗号鍵４０－１に対応する鍵生成情報２０－１と、暗号文３０－１とを組み合わせて、伝送データ１０－１を生成する。データ取得装置４０００は、伝送データ１０－１に含まれる鍵生成情報２０－１及びマスタ暗号鍵１００を用いて、固有暗号鍵４０－１を生成する。そして、データ取得装置４０００は、固有暗号鍵４０－１を用いて伝送データ１０－１に含まれる暗号文３０－１を復号する。データ取得装置４０００は、暗号文３０－１が正しく復号できた場合、伝送データ１０－１が正当であると判定する。以上のように、秘密鍵暗号を用いて電子署名を行うことで、高速な電子署名を実現している。
【選択図】図４



【特許請求の範囲】
【請求項１】
データ生成装置及びデータ取得装置を有するデータ伝送システムであって、
前記データ生成装置は、
当該データ生成装置に固有の鍵生成情報である固有鍵生成情報を格納する固有鍵生成情報格納部と、
前記固有鍵生成情報に対して一意に対応する暗号鍵である固有暗号鍵を、当該データ生成装置の外部から読み取り不可能な状態で格納している固有暗号鍵格納部と、
前記固有暗号鍵を用いて平文を暗号化することで暗号文を生成し、その暗号文と前記固有鍵生成情報とを対応付けた伝送データを生成する伝送データ生成部と、を有し、
前記データ取得装置は、
前記固有鍵生成情報からその固有鍵生成情報に対して一意に対応する前記固有暗号鍵を生成するための暗号鍵であるマスタ暗号鍵を、当該データ取得装置の外部から読み取り不可能な状態で格納するマスタ暗号鍵格納部と、
前記伝送データを取得する伝送データ取得部と、
前記伝送データにおいて前記暗号文と対応付けられている固有鍵生成情報と前記マスタ暗号鍵を用いて、その固有鍵生成情報に対して一意に対応する前記固有暗号鍵を生成する固有暗号鍵生成部と、
生成した前記固有暗号鍵を用いて、前記伝送データに含まれる暗号文を復号する復号部と、
前記復号部の処理結果を用いて前記伝送データの正当性を判定する正当性判定部と、を有し、
前記固有暗号鍵生成部によって生成された固有暗号鍵は、当該データ取得装置の外部から読み取り不可能であり、
前記マスタ暗号鍵は別の暗号鍵から算出できないことを特徴とするデータ伝送システム。
【請求項２】
前記伝送データ生成部は、前記固有鍵生成情報格納部に格納されている固有鍵生成情報を前記平文に追加して第２平文を生成し、前記第２平文を暗号化して前記暗号文を生成し、
前記正当性判定部は、前記復号部によって前記暗号文から算出された前記第２平文に、伝送データにおいて前記暗号文と対応付けられている固有鍵生成情報が含まれている場合に、前記伝送データが正当であると判定する請求項１に記載のデータ伝送システム。
【請求項３】
前記伝送データ生成部は、前記伝送データに対象マークを付与し、
前記データ取得装置は、前記伝送データ取得部によって取得された伝送データに前記対象マークが付与されているか否かを判定するディスパッチ部を有し、
前記正当性判定部は、前記対象マークが付与されていると判定された伝送データについて正当性を判定する請求項１又は２に記載のデータ伝送システム。
【請求項４】
前記平文は１つのパケットである請求項１乃至３いずれか一項に記載のデータ伝送システム。
【請求項５】
データ生成装置及びデータ取得装置を有するデータ伝送システムによって実行されるデータ伝送方法であって、
前記データ生成装置は、
当該データ生成装置に固有の鍵生成情報である固有鍵生成情報を格納する固有鍵生成情報格納部と、
前記固有鍵生成情報に対して一意に対応する暗号鍵である固有暗号鍵を、当該データ生成装置の外部から読み取り不可能な状態で格納している固有暗号鍵格納部と、を有し、

前記データ取得装置は、前記固有鍵生成情報からその固有鍵生成情報に対して一意に対応する前記固有暗号鍵を生成するための暗号鍵であるマスタ暗号鍵を、当該データ取得装置の外部から読み取り不可能な状態で格納するマスタ暗号鍵格納部を有し、
前記データ生成装置が、前記固有暗号鍵を用いて平文を暗号化することで暗号文を生成し、その暗号文と前記固有鍵生成情報とを対応付けた伝送データを生成する伝送データ生成ステップと、
前記データ取得装置が、前記伝送データを取得する伝送データ取得ステップと、
前記データ取得装置が、前記伝送データにおいて前記暗号文と対応付けられている固有鍵生成情報と前記マスタ暗号鍵を用いて、その固有鍵生成情報に対して一意に対応する前記固有暗号鍵を生成する固有暗号鍵生成ステップと、
前記データ取得装置が、生成した前記固有暗号鍵を用いて、前記伝送データに含まれる暗号文を復号する復号ステップと、
前記データ取得装置が、前記復号ステップの処理結果を用いて前記伝送データの正当性を判定する正当性判定ステップと、を有し、
前記固有暗号鍵生成部によって生成された固有暗号鍵は、当該データ取得装置の外部から読み取り不可能であり、
前記マスタ暗号鍵は別の暗号鍵から算出できないことを特徴とするデータ伝送方法。
【請求項６】
前記伝送データ生成ステップは、前記固有鍵生成情報格納部に格納されている固有鍵生成情報を前記平文に追加し、追加後の平文を暗号化して前記暗号文を生成し、
前記正当性判定ステップは、前記復号ステップによって前記暗号文から算出された平文に、伝送データにおいて前記暗号文と対応付けられている固有鍵生成情報が含まれている場合に、前記伝送データが正当であると判定する請求項５に記載のデータ伝送方法。
【請求項７】
前記伝送データ生成ステップは、前記伝送データに対象マークを付与し、
当該データ伝送方法は、前記データ取得装置が、前記伝送データ取得ステップで取得された伝送データに前記対象マークが付与されているか否かを判定するディスパッチステップを有し、
前記正当性判定ステップは、前記対象マークが付与されていると判定された伝送データについて正当性を判定する請求項５又は６に記載のデータ伝送方法。
【請求項８】
前記平文は１つのパケットである請求項５乃至７いずれか一項に記載のデータ伝送方法。
【請求項９】
請求項１乃至４いずれか一項に記載のデータ伝送システムにおけるデータ生成装置。
【請求項１０】
コンピュータを、請求項１乃至４いずれか一項に記載のデータ伝送システムにおけるデータ生成装置として動作させるプログラム。
【請求項１１】
請求項１乃至４いずれか一項に記載のデータ伝送システムにおけるデータ取得装置。
【請求項１２】
コンピュータを、請求項１乃至４いずれか一項に記載のデータ伝送システムにおけるデータ取得装置として動作させるプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、暗号技術に関する。
【背景技術】
【０００２】
ネットワークなどを通じて配布されるデータ（以下、配布データ）の提供元を保証する

方法として、電子署名を利用する方法がある。配布データの生成者は、生成した配布データに電子署名を付す。例えば電子署名は、生成した配布データのハッシュ値を暗号化することで生成される。電子署名付きの配布データを取得したユーザは、電子署名を復号して得られる値と、取得した配布データから算出したハッシュ値とが一致することを確認する。もしこれらが一致していれば、配布データと電子署名との組み合わせが正しいことが分かる。その結果、配布データの提供元が正しいことが分かる。

【０００３】

例えば電子署名に関する先行技術として、特許文献１に開示されている技術がある。特許文献１は、UIM（User Identity Module）等の IC チップ内に格納された公開鍵暗号プログラムを用いて、ウイルス研究対象プログラムに電子署名を付す技術を開示している。

【先行技術文献】

【特許文献】

【０００４】

【特許文献１】特開２００３－２１６４４８号公報

【発明の概要】

【発明が解決しようとする課題】

【０００５】

特許文献１に開示されている技術に代表されるように、電子署名の暗号化と復号は公開鍵暗号方式で行われている。公開鍵暗号方式を用いた電子署名の場合、配布データの生成者は、自身の秘密鍵を用いて電子署名を生成する。そして、その電子署名が付された配布データを取得したユーザは、その電子署名を配布データの生成者の公開鍵を用いて復号する。

【０００６】

一般に、公開鍵暗号方式における暗号化及び復号は、共通鍵暗号方式における暗号化及び復号と比較して低速である。そのため、例えば配布データの処理に利用できる時間が限られているような環境では、公開鍵暗号方式を利用した電子署名を利用することが難しい。

【０００７】

本発明は、以上の課題を鑑みてなされたものである。本発明の目的は、電子署名の実行速度を高速化する技術を提供することである。

【課題を解決するための手段】

【０００８】

本発明が提供するデータ伝送システムは、データ生成装置及びデータ取得装置を有する。

前記データ生成装置は、

当該データ生成装置に固有の鍵生成情報である固有鍵生成情報を格納する固有鍵生成情報格納部と、

前記固有鍵生成情報に対して一意に対応する暗号鍵である固有暗号鍵を、当該データ生成装置の外部から読み取り不可能な状態で格納している固有暗号鍵格納部と、

前記固有暗号鍵を用いて平文を暗号化することで暗号文を生成し、その暗号文と前記固有鍵生成情報とを対応付けた伝送データを生成する伝送データ生成部と、を有する。

前記データ取得装置は、

前記固有鍵生成情報からその固有鍵生成情報に対して一意に対応する前記固有暗号鍵を生成するための暗号鍵であるマスタ暗号鍵を、当該データ取得装置の外部から読み取り不可能な状態で格納するマスタ暗号鍵格納部と、

前記伝送データを取得する伝送データ取得部と、

前記伝送データにおいて前記暗号文と対応付けられている固有鍵生成情報と前記マスタ暗号鍵を用いて、その固有鍵生成情報に対して一意に対応する前記固有暗号鍵を生成する固有暗号鍵生成部と、

生成した前記固有暗号鍵を用いて、前記伝送データに含まれる暗号文を復号する復号

部と、
　前記復号部の処理結果を用いて前記伝送データの正当性を判定する正当性判定部と、を有する。
　前記固有暗号鍵生成部によって生成された固有暗号鍵は、当該データ取得装置の外部から読み取り不可能である。前記マスタ暗号鍵は別の暗号鍵から算出できない。
【０００９】
　本発明が提供するデータ伝送方法は、データ生成装置及びデータ取得装置を有するデータ伝送システムによって実行される。
　前記データ生成装置は、
　当該データ生成装置に固有の鍵生成情報である固有鍵生成情報を格納する固有鍵生成情報格納部と、
　前記固有鍵生成情報に対して一意に対応する暗号鍵である固有暗号鍵を、当該データ生成装置の外部から読み取り不可能な状態で格納している固有暗号鍵格納部と、を有する。
　前記データ取得装置は、前記固有鍵生成情報からその固有鍵生成情報に対して一意に対応する前記固有暗号鍵を生成するための暗号鍵であるマスタ暗号鍵を、当該データ取得装置の外部から読み取り不可能な状態で格納するマスタ暗号鍵格納部を有する。
　当該データ伝送方法は、
　前記データ生成装置が、前記固有暗号鍵を用いて平文を暗号化することで暗号文を生成し、その暗号文と前記固有鍵生成情報とを対応付けた伝送データを生成する伝送データ生成ステップと、
　前記データ取得装置が、前記伝送データを取得する伝送データ取得ステップと、
　前記データ取得装置が、前記伝送データにおいて前記暗号文と対応付けられている固有鍵生成情報と前記マスタ暗号鍵を用いて、その固有鍵生成情報に対して一意に対応する前記固有暗号鍵を生成する固有暗号鍵生成ステップと、
　前記データ取得装置が、生成した前記固有暗号鍵を用いて、前記伝送データに含まれる暗号文を復号する復号ステップと、
　前記データ取得装置が、前記復号ステップの処理結果を用いて前記伝送データの正当性を判定する正当性判定ステップと、を有する。
　前記固有暗号鍵生成部によって生成された固有暗号鍵は、当該データ取得装置の外部から読み取り不可能である。前記マスタ暗号鍵は別の暗号鍵から算出できない。
【００１０】
　本発明が提供するデータ生成装置は、本発明が提供するデータ伝送システムにおけるデータ生成装置である。
【００１１】
　本発明が提供する第１のプログラムは、コンピュータを、本発明が提供するデータ伝送システムにおけるデータ生成装置として動作させる。
【００１２】
　本発明が提供するデータ取得装置は、本発明が提供するデータ伝送システムにおけるデータ取得装置である。
【００１３】
　本発明が提供する第２のプログラムは、コンピュータを、本発明が提供するデータ伝送システムにおけるデータ取得装置として動作させる。
【発明の効果】
【００１４】
　本発明によれば、電子署名処理を高速化する技術が提供される。
【図面の簡単な説明】
【００１５】
【図１】実施形態１に係るデータ伝送システムを例示するブロック図である。
【図２】データ生成装置によって生成される伝送データのデータ構造を例示する図である

。
【図３】固有暗号鍵を用いた暗号化と復号を概念的に例示する図である。
【図４】データ伝送システムにおける処理の流れを概念的に例示する図である。
【図５】マスタ暗号鍵と鍵生成情報を用いて暗号鍵を生成する機能の概念図である。
【図６】データ取得装置が不正な伝送データを取得した場合における処理の流れを概念的に例示する図である。
【図７】実施形態１のデータ取得装置によって実行される処理の流れを例示するフローチャートである。
【図８】暗号化対象のデータである平文のデータ構造を例示する図である。
【図９】鍵生成情報を例示する第１の図である。
【図１０】鍵生成情報を例示する第２の図である。
【図１１】再配置暗号方式における暗号化を例示する図である。
【図１２】実施形態２に係るデータ伝送システムを例示するブロック図である。
【図１３】実施形態２に係るデータ取得装置によって実行される処理の流れを例示するフローチャートである。
【図１４】実施例のデータ伝送システムが扱う伝送データのデータ構造を例示する図である。
【図１５】実施例のデータ伝送システムによって実行される処理を概念的に例示する図である。
【図１６】実施例に係るデータ生成装置の構成を例示するブロック図である。
【図１７】第２伝送データ生成部が第２伝送データを生成する処理の流れを概念的に例示する図である。
【図１８】実施例に係るデータ取得装置の構成を例示するブロック図である。
【図１９】第２伝送データ処理部が第２伝送データを処理する流れを概念的に例示する図である。
【発明を実施するための形態】
【００１６】
以下、本発明の実施の形態について、図面を用いて説明する。尚、すべての図面において、同様な構成要素には同様の符号を付し、適宜説明を省略する。また、各ブロック図において、矢印の流れは、情報の流れを示している。さらに、各ブロック図において、各ブロックは、ハードウエア単位の構成ではなく、機能単位の構成を示している。
【００１７】
[実施形態１]
図１は、実施形態１に係るデータ伝送システム２０００を例示するブロック図である。図１において、矢印の流れは情報の流れを示している。さらに、図１において、各ブロックは、ハードウエア単位の構成ではなく、機能単位の構成を表している。
【００１８】
データ伝送システム２０００は、データ生成装置３０００及びデータ取得装置４０００を有する。データ取得装置４０００は、データ生成装置３０００によって生成された伝送データを取得する。ここで伝送データには、データ取得装置４０００へ伝達する暗号文と、その暗号文の提供元を示す情報とが含まれている。データ取得装置４０００は、この提供元を示す情報が正当であるか否かを判定することで、伝送データの正当性を確認する。これにより、例えば暗号文の提供元を示す情報をすり替えることで暗号文の提供元を偽る攻撃（なりすまし）を防ぐことができる。
【００１９】
以下、データ伝送システム２０００の理解を容易にするため、図１に示す各機能構成部について説明する前に、データ伝送システム２０００の動作の概要を説明する。各動作の具体的な実現方法については、図１に示す各機能構成部と共に後述する。なお、ここで行われる説明は、あくまでデータ伝送システム２０００の理解を容易にするための説明であり、データ伝送システム２０００の実現方法を限定するものではない。

【００２０】
＜伝送データの概要＞
図２は、データ生成装置３０００によって生成される伝送データ１０のデータ構造を表す図である。伝送データ１０は、鍵生成情報２０及び暗号文３０を有する。鍵生成情報２０はデータ生成装置３０００に固有の情報である。そのため、暗号文３０の提供元を表す情報となる。さらに鍵生成情報２０は、暗号鍵の生成に用いられる情報でもある。鍵生成情報２０を用いて暗号鍵を生成する方法については後述する。
【００２１】
暗号文３０は、データ生成装置３０００によって暗号化された暗号文である。ここで、暗号文３０の暗号化は、暗号化を行ったデータ生成装置３０００に固有の暗号鍵を用いて行われる。以下、データ生成装置３０００に固有の暗号鍵を固有暗号鍵と表記する。ある固有暗号鍵で暗号化された暗号文は、その固有暗号鍵を用いなければ正しく復号できない。つまりデータ伝送システム２０００では、公開鍵暗号方式ではなく共通鍵暗号方式で暗号化と復号を行う。
【００２２】
図３は、固有暗号鍵を用いた暗号化と復号を概念的に例示する図である。図３では、固有暗号鍵４０－１を用いて平文５０を暗号化することで、暗号文３０が生成されている。固有暗号鍵４０－１を用いて暗号文３０を復号すると、元の平文５０が算出される。しかし、固有暗号鍵４０－１以外の固有暗号鍵である固有暗号鍵４０－２や固有暗号鍵４０－３を用いても、平文５０は算出されない。
【００２３】
＜伝送データの生成＞
図４は、データ伝送システム２０００における処理の流れを概念的に例示する図である。図４において、データ生成装置３０００－１の中には、データ生成装置３０００－１が伝送データ１０－１を生成する流れを概念的に示している。まずデータ生成装置３０００－１は、データ生成装置３０００－１の固有暗号鍵である固有暗号鍵４０－１を用いて平文５０－１を暗号化することで、暗号文３０－１を生成する。そして、データ生成装置３０００－１は、固有暗号鍵４０－１と対応する鍵生成情報２０－１と、暗号文３０－１とを組み合わせて、伝送データ１０－１を生成する。鍵生成情報２０－１は、データ生成装置３０００－１に固有の鍵生成情報である。
【００２４】
ここで、データ生成装置３０００－１は、そのデータ生成装置３０００－１の外部からは読み出し不可能な状態で固有暗号鍵４０－１を格納している。またデータ生成装置３０００は、データ生成装置３０００－１の外部に固有暗号鍵４０－１を出力しない。したがって、データ生成装置３０００－１の外部にある装置（データ取得装置４０００など）は、データ生成装置３０００－１から固有暗号鍵４０－１を取得することはできない。
【００２５】
＜伝送データの正当性の確認＞
データ取得装置４０００は、受信した伝送データ１０－１に含まれる暗号文３０－１を正しく復号できるか否かで、伝送データ１０－１の正当性を確認する。ただし上述のように、データ取得装置４０００は、暗号文３０－１を復号するために必要な固有暗号鍵４０－１をデータ生成装置３０００－１から取得することはできない。
【００２６】
そこでデータ取得装置４０００は、固有暗号鍵と対応する鍵生成情報を用いて、その固有暗号鍵を生成する機能を有する。この機能は、データ取得装置４０００の内部に格納されているマスタ暗号鍵を用いて実現される。データ生成装置３０００の固有暗号鍵は、マスタ暗号鍵、及びそのデータ生成装置３０００に固有の鍵生成情報に基づいて生成できる暗号鍵となっている。例えばデータ生成装置３０００－１の固有暗号鍵４０－１は、マスタ暗号鍵、及びデータ生成装置３０００－１に固有の鍵生成情報である鍵生成情報２０－１によって生成できる。なお、マスタ暗号鍵はデータ取得装置４０００の外部からは読み

出し不可能となっている。

【００２７】

マスタ暗号鍵と鍵生成情報を用いて暗号鍵を生成する機能の概念図を図５に示す。データ取得装置４０００は、マスタ暗号鍵１００、及び固有暗号鍵４０－１と対応する鍵生成情報２０－１から、鍵生成情報２０－１に対して一意に対応する固有暗号鍵４０－１を生成できる。同様に、データ取得装置４０００は、マスタ暗号鍵１００、及び固有暗号鍵４０－２と対応する鍵生成情報２０－２から、鍵生成情報２０－２に対して一意に対応する固有暗号鍵４０－２を生成できる。ただし、データ取得装置４０００が鍵生成情報及びマスタ暗号鍵１００を用いて生成できる暗号鍵は、その鍵生成情報に対して一意に対応する暗号鍵のみである。よって、データ取得装置４０００は、鍵生成情報２０－１から固有暗号鍵４０－２を生成したり、鍵生成情報２０－２から固有暗号鍵４０－１を生成したりすることはできない。

【００２８】

伝送データ１０には、暗号文３０の提供元を表す情報として、鍵生成情報２０が含まれている。そこで、データ取得装置４０００は、伝送データ１０に含まれる鍵生成情報２０及びマスタ暗号鍵を用いて固有暗号鍵４０を生成し、伝送データ１０に含まれる暗号文３０を生成した固有暗号鍵４０で復号する。鍵生成情報２０が正当な情報であれば、鍵生成情報２０は暗号文３０を生成したデータ生成装置３０００の固有暗号鍵と対応する鍵生成情報である。そのためデータ取得装置４０００は、鍵生成情報２０から生成した固有暗号鍵４０を用いて暗号文３０を正しく復号できる。データ取得装置４０００は、暗号文３０を正しく復号できた場合に、「伝送データ１０は正当なデータである」と判定する。

【００２９】

図４において、データ取得装置４０００の中には、データ取得装置４０００が正当な伝送データを取得した場合における処理の流れを概念的に示している。伝送データ１０－１は、正当なデータであるため、鍵生成情報２０－１及び暗号文３０－１を含んでいる。データ取得装置４０００は、マスタ暗号鍵１００及び伝送データ１０－１に含まれる鍵生成情報２０－１を用いて暗号鍵を生成する。生成される暗号鍵は、固有暗号鍵４０－１である。そして、データ取得装置４０００は、固有暗号鍵４０－１を用いて暗号文３０－１を復号する。ここで、固有暗号鍵４０－１は暗号文３０－１の生成に用いられた暗号鍵であるため、データ取得装置４０００は暗号文３０－１を正しく復号することができ、平文５０－１を算出できる。よってデータ取得装置４０００は、伝送データ１０－１は正当であると判定する。

【００３０】

一方、図６は、データ取得装置４０００が不正な伝送データを取得した場合における処理の流れを概念的に示している。図６において取得される伝送データ１０－Ｘは、データ生成装置３０００－１によって生成された暗号文３０－１と、データ生成装置３０００－１とは異なるデータ生成装置３０００－Ｘに固有の鍵生成情報である鍵生成情報２０－Ｘを含んでいる。

【００３１】

データ取得装置４０００は、マスタ暗号鍵１００及び鍵生成情報２０－Ｘを用いて暗号鍵を生成する。生成される暗号鍵は、固有暗号鍵４０－１とは異なる固有暗号鍵４０－Ｘである。そしてデータ取得装置４０００は、固有暗号鍵４０－Ｘを用いて暗号文３０－１を復号しようとする。しかし固有暗号鍵４０－Ｘは暗号文３０－１の暗号化に用いられた固有暗号鍵４０－１ではないため、データ取得装置４０００は暗号文３０－１を正しく復号できない。よってデータ取得装置４０００は、伝送データ１０－Ｘは不正であると判定する。

【００３２】

例えば伝送データ１０－Ｘは、伝送データ１０－１を取得した悪意ある第３者が伝送データ１０－１に含まれる鍵生成情報２０－１を鍵生成情報２０－Ｘとすり替えることによって生成される。仮にデータ取得装置が鍵生成情報２０－Ｘを参照することだけをもって

伝送データ１０の提供元を判定すると、暗号文３０－１の提供元はデータ生成装置３０００－Ｘであると判定してしまう。その結果、悪意ある第３者によるなりすまし攻撃が成功してしまう。

【００３３】

これに対し本実施形態のデータ取得装置４０００を用いると、鍵生成情報２０がすり替えられていた場合、暗号文３０を正しく復号できないことをもって、伝送データ１０が不正であることが分かる。その結果、悪意ある第３者によるなりすまし攻撃を防ぐことができる。

【００３４】

ここで前述したように、データ伝送システム２０００では、公開鍵暗号方式ではなく、共通鍵暗号方式で暗号化及び復号が行われる。一般に、共通鍵暗号方式において暗号化及び復号に要する時間は、公開鍵暗号方式において暗号化及び復号に要する時間よりも短い。そのため、本実施形態によれば、公開鍵暗号方式を利用する場合と比較し、暗号文の暗号化及び復号を短い時間で行うことができる。その結果、伝送データ１０の提供元が正しいか否かを高速に判定することができる。

【００３５】

なお、データ取得装置４０００は、生成した固有暗号鍵を暗号文の復号のみに利用できるように構成されており、その固有暗号鍵を用いて暗号文を生成したり、その暗号鍵を外部に出力したりすることはできない。そのため、データ取得装置４０００によってデータ生成装置３０００の固有暗号鍵が漏洩されることはない。また前述したように、データ生成装置３０００も固有暗号鍵を漏洩することはない。よってデータ伝送システム２０００において、固有暗号鍵が漏洩することはない。

【００３６】

以上のようなデータ伝送システム２０００の各機能を実現するために、データ伝送システム２０００は、図１に示す構成を有する。以下、データ伝送システム２０００が有する各機能構成部について説明する。

【００３７】

＜データ生成装置３０００＞

データ生成装置３０００は、固有鍵生成情報格納部３０２０、固有暗号鍵格納部３０４０、及び伝送データ生成部３０６０を有する。

【００３８】

＜＜固有鍵生成情報格納部３０２０＞＞

固有鍵生成情報格納部３０２０は、その固有鍵生成情報格納部３０２０を有するデータ生成装置３０００の固有鍵生成情報を格納する。固有鍵生成情報は、データ生成装置３０００の固有暗号鍵と対応する鍵生成情報である。そのため、固有鍵生成情報は、データ生成装置３０００に固有の鍵生成情報である。

【００３９】

＜＜固有暗号鍵格納部３０４０＞＞

固有暗号鍵格納部３０４０は固有暗号鍵を格納する。この固有暗号鍵は、固有鍵生成情報格納部３０２０に格納されている固有鍵生成情報に対して一意に対応する。ここで、固有暗号鍵格納部３０４０は、その固有暗号鍵格納部３０４０を有するデータ生成装置３０００の外部からは読み取り不可能な状態で固有暗号鍵を格納している。

【００４０】

＜＜伝送データ生成部３０６０＞＞

伝送データ生成部３０６０は、その伝送データ生成部３０６０を有するデータ生成装置３０００の固有暗号鍵を用いて平文を暗号化することにより、暗号文を生成する。さらに伝送データ生成部３０６０は、生成した暗号文と固有鍵生成情報とを対応付けた伝送データを生成する。

【００４１】

＜データ取得装置４０００＞

データ取得装置４０００は、マスタ暗号鍵格納部４０２０、伝送データ取得部４０４０、固有暗号鍵生成部４０６０、復号部４０８０、及び正当性判定部４１００を有する。

【００４２】

＜＜伝送データ取得部４０４０＞＞

伝送データ取得部４０４０は、伝送データを取得する。前述したように、伝送データには、固有鍵生成情報と暗号文とが含まれる。

【００４３】

＜＜マスタ暗号鍵格納部４０２０＞＞

マスタ暗号鍵格納部４０２０は前述のマスタ暗号鍵を格納する。マスタ暗号鍵は、固有鍵生成情報からその固有鍵生成情報に対して一意に対応する固有暗号鍵を生成するための元となる暗号鍵である。ここで、マスタ暗号鍵格納部４０２０は、そのマスタ暗号鍵格納部４０２０を有するデータ取得装置４０００の外部からは読み取り不可能な状態でマスタ暗号鍵を格納している。

【００４４】

ここで、マスタ暗号鍵を生成する方法は公開されていない。そのため、マスタ暗号鍵を悪意ある第３者が生成することはできない。また前述したように、マスタ暗号鍵を外部から読み取ることはできない。そのため、たとえ悪意ある第３者がデータ取得装置４０００を手に入れたとしても、その第３者はデータ取得装置４０００からマスタ暗号鍵を読み出して利用することはできない。

【００４５】

＜＜固有暗号鍵生成部４０６０＞＞

固有暗号鍵生成部４０６０は、伝送データ取得部４０４０によって取得された伝送データに含まれる固有鍵生成情報と、マスタ暗号鍵格納部４０２０に格納されているマスタ暗号鍵とを用いて、固有暗号鍵を生成する。

【００４６】

＜＜復号部４０８０＞＞

復号部４０８０は、生成した固有暗号鍵を用いて、伝送データに含まれる暗号文を復号する。前述したように、暗号文は、その暗号文を生成するために利用された固有暗号鍵によってのみ正しく復号できる。

【００４７】

＜＜正当性判定部４１００＞＞

正当性判定部４１００は、復号部４０８０の処理結果を用いて伝送データの正当性を判定する。

【００４８】

＜処理の流れ＞

図７は、実施形態１のデータ取得装置４０００によって実行される処理の流れを例示するフローチャートである。ステップＳ１０２において、伝送データ取得部４０４０は伝送データを取得する。ステップＳ１０４において、固有暗号鍵生成部４０６０は、伝送データにおいて暗号文と対応付けられている固有鍵生成情報とマスタ暗号鍵を用いて、固有暗号鍵を生成する。ステップＳ１０６において、復号部４０８０は、生成した固有暗号鍵を用いて、伝送データに含まれる暗号文を復号する。ステップＳ１０８において、正当性判定部４１００は、復号部の処理結果を用いて伝送データの正当性を判定する。

【００４９】

＜作用・効果＞

本実施形態において、データ取得装置４０００が受信した伝送データに含まれる固有鍵生成情報が、伝送データに含まれる暗号文の生成に利用された固有暗号鍵に対応する鍵生成情報でない場合、復号部４０８０は暗号文を正しく復号できない。一方、データ取得装置４０００が受信した伝送データに含まれる固有鍵生成情報が、伝送データに含まれる暗号文の生成に利用された固有暗号鍵に対応する鍵生成情報である場合、復号部４０８０は暗号文を正しく復号できる。そのため、本実施形態によれば、データ取得装置４０００に

おいて伝送データに含まれる暗号文を復号できるか否かを判定することによって、伝送データの正当性を確認できる。

【００５０】

また前述したように、データ伝送システム２０００では、公開鍵暗号方式ではなく、共通鍵暗号方式で暗号化及び復号が行われる。よって、本実施形態によれば、公開鍵暗号方式を利用する場合と比較し、伝送データの提供元が正当であるか否かを高速に把握することができる。

【００５１】

また一般に、共通鍵暗号方式では、暗号文を取得する取得装置において、暗号鍵の生成に用いられる共通鍵を事前に取得しておく必要があり、手間がかかる。これに対し本実施形態の場合、データ取得装置４０００は、データ生成装置３０００が暗号化に用いる固有暗号鍵を事前に取得しておく必要がない。さらに、データ生成装置３０００から送信される伝送データに暗号鍵を含めるということはしないため、データ取得装置４０００が伝送データを取得する際に暗号鍵が漏洩する危険性もない。よって、本実施形態によれば、安全かつユーザに手間がかからない方法で共通暗号鍵方式を実現することができる。

【００５２】

＜主な利用例＞

本実施形態によれば、データ取得装置４０００において、伝送データに含まれる暗号文３０の提供元が正当であることを確認できる。そのため、本実施形態の伝送データは、いわゆる電子署名付きのデータとしてみることができる。したがって、本実施形態によれば、共通鍵暗号方式による電子署名を実現することができる。

【００５３】

本実施形態によれば、共通鍵暗号方式で電子署名を実現できるため、高速に送受信されるデータに電子署名を付与することができるようになる。そのため、例えば、GPS (Global Positioning System) 衛星から送信される GPS 信号に電子署名を付すことが可能になる。GPS 信号は、例えば対象物体の位置の追跡などに利用される。そのため、GPS 信号を悪意ある第３者に改ざんされると、対象物体を正しく追跡できなくなるといった問題がある。そこで、GPS 衛星が GPS 信号に電子署名を付して送信するようにすることで、GPS 信号の提供元が正当であることを確認できるようにすることが好ましい。しかし、対象物体の追跡などのように短い時間間隔で GPS 信号を処理する必要がある場合、低速な公開鍵暗号方式で実現した電子署名を GPS 信号に付すと、GPS 信号を処理しきれなくなる。

【００５４】

これに対し、本実施形態のデータ伝送システム２０００を GPS に適用すれば、GPS 信号の正当性を高速に判定できるようになる。そのため、受信するデータを短い時間で処理することが要求されるシステムにおいても、データの提供元を確認することができるようになる。この場合、GPS 衛星においてデータ生成装置３０００を利用して GPS 信号を送信し、GPS 信号を利用する各種装置においてデータ取得装置４０００を利用して GPS 信号を取得する。

【００５５】

同様に、本実施形態のデータ伝送システム２０００を電波時計のシステムに適用すれば、電波時計が利用する標準電波の正当性を高速に判定できるようになる。この場合、標準電波の送信局においてデータ生成装置３０００を利用して標準電波を送信し、標準電波を利用する各種電波時計においてデータ取得装置４０００を利用して標準電波を取得する。

【００５６】

以下、本実施形態のデータ伝送システム２０００について、さらに詳細に説明する。

【００５７】

＜ハードウエア構成＞

データ生成装置３０００及びデータ取得装置４０００は、例えば、LSI (Large Scale Integration) などの集積回路、又は集積回路とソフトウエアの組み合わせとして実装される。ただし、データ生成装置３０００及びデータ取得装置４０００の実装方法は、集積回

路を用いた実装方法に限定されない。

【００５８】

例えばデータ生成装置３０００とデータ取得装置４０００はそれぞれ、PC（Personal Computer）、サーバ、携帯端末等の種々の計算機が有するネットワークインタフェース上に設けられる。こうすることで、データ生成装置３０００によって生成された伝送データがネットワークを経由してデータ取得装置４０００によって受信される。

【００５９】

例えば、伝送データ生成部３０６０、伝送データ取得部４０４０、固有暗号鍵生成部４０６０、復号部４０８０、及び正当性判定部４１００は、ワイヤードロジックなどにより、ハードウエアとして実装される。その他にも例えば、上記各機能構成部は、ソフトウエアとハードウエアの組み合わせとして実装される。ソフトウエアとハードウエアの組み合わせとは、例えば、プロセッサ、メモリ、及びストレージなどのハードウエアと、メモリ又はストレージに格納されたプログラムの組み合わせである。プロセッサは、例えば、上記各機能構成部を実現する各プログラムをメモリに読み出して実行することで、上記各機能構成部が有する機能を実現する。

【００６０】

固有鍵生成情報格納部３０２０は、例えば、ROM (Read Only Memory) や RAM (Random Access Memory) として実装される。この場合、固有鍵生成情報は、この ROM や RAM に格納される。その他にも例えば、固有鍵生成情報格納部３０２０は、ワイヤードロジックなどを用いて実装されてもよい。この場合、固有鍵生成情報は、固有鍵生成情報格納部３０２０に組み込まれた物理的な電気回路として実装される。

【００６１】

固有暗号鍵格納部３０４０は、例えば、データ生成装置３０００の外部との間に通信路を持たない ROM や RAM として実装される。この場合、固有暗号鍵は、この ROM や RAM に格納される。その他にも例えば、固有暗号鍵格納部３０４０は、ワイヤードロジックなどを用いて実装されてもよい。この場合、固有暗号鍵は、固有暗号鍵格納部３０４０に組み込まれた物理的な電気回路として実装される。

【００６２】

マスタ暗号鍵格納部４０２０は、固有暗号鍵格納部３０４０と同様の方法で実装される。

【００６３】

＜伝送データ取得部４０４０の詳細＞

伝送データ取得部４０４０が伝送データを取得する方法は様々である。例えば伝送データ取得部４０４０は、データ生成装置３０００によって送信される伝送データを受信する。また例えば、伝送データ取得部４０４０は、伝送データが格納されている格納部から伝送データを取得する。この格納部は、データ生成装置３０００の内部又は外部に設けられており、データ生成装置３０００は生成した伝送データをこの格納部に格納する。

【００６４】

＜正当性判定部４１００の詳細＞

正当性判定部４１００は、復号部４０８０が暗号文３０を正しく復号できたか否かに基づいて、伝送データの正当性を判定する。ここで、「復号部４０８０が暗号文３０を正しく復号できたか否か」を判定する方法は様々である。例えばデータ伝送システム２０００は、平文５０のデータ構造を図８に示す構造にすることにより、「復号部４０８０が暗号文３０を正しく復号できたか否か」を判定できるようにする。図８は、暗号化対象のデータである平文５０のデータ構造を例示する図である。平文５０には、データ生成装置３０００の固有鍵生成情報である鍵生成情報２０、及びユーザに伝達するデータである伝達データ６０が含まれる。

【００６５】

例えば伝達データ６０は、パケット通信における１つのパケットである。データ伝送システム２０００は高速に暗号処理を行えるため、１つ１つのパケットについて電子署名を

実現できる。また、伝達データ６０は、パケットの集合であってもよい。なお、伝達データ６０は、パケットで構成されるデータに限定されるものではなく、任意のデータでよい。

【００６６】

伝送データ生成部３０６０は、この平文５０を暗号化して、暗号文３０を生成する。ここで、鍵生成情報２０の大きさはＸビットであり、鍵生成情報２０は平文５０の先頭に格納されているとする。復号部４０８０は、暗号文３０を復号して平文を得る。正当性判定部４１００は、得られた平文の先頭Ｘビットと、伝送データ１０に含まれている鍵生成情報２０とを比較する。そして、正当性判定部４１００は、平文の先頭Ｘビットと、伝送データ１０に含まれている鍵生成情報２０とが一致する場合、暗号文３０を正しく復号できた（平文５０を算出できた）と判定する。一方、正当性判定部４１００は、平文の先頭Ｘビットと、伝送データ１０に含まれている鍵生成情報２０とが一致しない場合、暗号文３０を正しく復号できなかったと判定する。

【００６７】

平文５０における鍵生成情報２０の位置は任意である。ただし、平文５０における鍵生成情報２０の位置を復号部４０８０が把握できるようにしておく必要がある。例えば平文５０における鍵生成情報２０の位置は、予めデータ生成装置３０００とデータ取得装置４０００との間で取り決められているものとする。また、平文５０における鍵生成情報２０の位置を示す情報を、伝送データ１０に含めるようにしてもよい。

【００６８】

また例えば、データ生成装置３０００は、伝達データに基づいてチェックデジットを生成し、生成したチェックデジットを伝達データに付加することで、暗号化対象の平文５０を生成してもよい。この場合、正当性判定部４１００は、復号部４０８０によって復号された平文に含まれる伝達データとチェックデジットとの関係が正しいか否かを判定することにより、暗号文３０を正しく復号できたか否かを判定する。

【００６９】

正当性判定部４１００は、判定結果を表す情報を出力してもよいし、出力せずに内部に記憶してもよい。ここで、判定結果を表す情報のデータ構造は任意である。例えば判定結果を表す情報は、正当である場合に値が１であり、正当でない場合に値が０である１ビットのフラグである。また例えば、判定結果を表す情報は、復号された平文である。正当性判定部４１００が、伝送データが正当であると判定した場合のみ平文を出力又は記憶するようにすれば、平文が出力又は記憶された場合に伝送データが正当であることが分かる。

【００７０】

＜鍵生成情報の詳細＞

鍵生成情報は、暗号鍵を生成するための情報である。１つの鍵生成情報に対応する暗号鍵は１つのみである。つまり、暗号鍵は、鍵生成情報に対して一意に対応する。

【００７１】

鍵生成情報のデータ構造は任意である。例えば鍵生成情報は、複数のデータの組み合わせによって構成されることで、階層構造（例：木構造）を持つ。図９は、鍵生成情報を例示する第１の図である。図９において、鍵生成情報T_aは、固定の長さを持つ８つのデータT_{a1}～T_{a8}によって構成されている。T_{a1}～T_{a8}の各サイズは、例えば１６バイトである。例えば鍵生成情報が木構造を表す場合、鍵生成情報T_aは、T_{a1}が根であり、T_{a8}が葉である木構造を表す鍵生成情報となる。

【００７２】

図１０は、鍵生成情報を例示する第２の図である。図１０において、鍵生成情報T_bは、サイズが異なる複数のデータT_{b1}～T_{b3}、及び各データのサイズを表すヘッダによって構成されている。T_{b1}～T_{b3}のサイズはそれぞれ５バイト、１６バイト、２５６バイトである。

【００７３】

なお、鍵生成情報は暗号鍵に対して衝突困難であればよく、上記の構成には限定されな

い。

【００７４】

＜暗号鍵の詳細＞

暗号鍵は、鍵生成情報に基づいて生成することができる。例えば暗号鍵は、鍵生成情報を入力とする関数によって算出される値である。例えばこの関数は、SHA-256 等のハッシュ関数である。この関数は、一方向性又は原像計算困難性を有する必要がある。さらにこの関数は、単射であるか又は衝突困難性を有する必要がある。単射である場合、異なる鍵生成情報からは必ず異なる暗号鍵が生成される。また、衝突困難性を有する場合、異なる鍵生成情報から同じ暗号鍵が生成されうるものの、同じ暗号鍵が生成されるような複数の鍵生成情報の組を求めることが計算量的に困難である。

【００７５】

例えば前述した SHA-256 は、一般に原像困難性及び衝突困難性を有すると言われており、少なくともデータ伝送システム２０００で利用される鍵生成情報の集合（例えば、100 億個程度の鍵生成情報の集合）については、原像困難性及び衝突困難性を有すると考えられる。なお、上記の「100 億個程度」はあくまで例示であり、データ伝送システム２０００を運用する際に利用可能な鍵生成情報の集合の大きさを限定するものではない。

【００７６】

また、少数の鍵生成情報の集合に対して異なる鍵生成情報から同じ暗号鍵が生成される確率が低い関数を用いることが好ましい。

【００７７】

マスタ暗号鍵は、鍵生成情報に基づいて固有暗号鍵を生成するために用いられる。前述したように、マスタ暗号鍵の生成方法は公開されていないため、第３者がマスタ暗号鍵を生成することはできない。また、マスタ暗号鍵格納部４０２０からマスタ暗号鍵を読み出すこともできない。

【００７８】

なお、データ伝送システム２０００で利用される全ての暗号鍵は、データ伝送システム２０００で用いられる暗号方式に対応する暗号鍵である。ここで、データ伝送システム２０００は、様々な暗号方式を用いることができる。例えばデータ伝送システム２０００は、DES (Data Encryption Standard) 暗号、AES (Advanced Encryption Standard) 暗号、又は再配置暗号などを用いる。再配置暗号の詳細については後述する。また、DES 暗号や AES 暗号などのブロック暗号を用いる場合、その利用モードは任意である。ブロック暗号の利用モードには、例えば、ECB (Electric Code Book) モード、CFB (Cipher Feed Back) モード、OFB (Output Feed Back) モード、CBC (Cipher Block Chaining) モード、又はカウンタモードなどがある。

【００７９】

＜暗号鍵生成の実施例＞

固有暗号鍵生成部４０６０が固有暗号鍵を生成する方法の実施例を説明する。上述したように、データ伝送システム２０００は、様々な暗号方式を利用できる。以下では、３つの具体例を説明する。

【００８０】

＜＜方法１＞＞

例えば固有暗号鍵生成部４０６０は、式（１）を用いて、鍵生成情報T_1に対して一意に対応する暗号鍵K_1を算出する。Hは一方向性及び衝突困難性を有するハッシュ関数である。K_mはマスタ暗号鍵である。$T_1 | K_m$は、T_1を構成するビット列とK_mを構成するビット列を結合したものである。例えばT_1が 001 であり、K_mが 101 の場合、$T_1 | K_m$は 001101 となる。

【数１】

$$K_1 = H(T_1 | K_m) \cdots (1)$$

【００８１】
なお、固有暗号鍵生成部４０６０は、Ｈ（Ｔ$_{1}$｜Ｋ$_{m}$）を構成するビット列の一部を暗号鍵Ｋ$_{1}$として用いてもよい。例えば固有暗号鍵生成部４０６０は、Ｈ（Ｔ$_{1}$｜Ｋ$_{m}$）の先頭１２８ビットを暗号鍵Ｋ$_{1}$とする。例えば AES 暗号方式を利用する場合に、Ｈ（Ｔ$_{1}$｜Ｋ$_{m}$）のサイズと AES 暗号方式のブロックサイズとが異なるとき、固有暗号鍵生成部４０６０は、暗号鍵Ｋ$_{1}$のサイズをブロックサイズと等しくするために、Ｈ（Ｔ$_{1}$｜Ｋ$_{m}$）の一部分を暗号鍵Ｋ$_{1}$とする。
【００８２】
＜＜方法２＞＞
また例えば、固有暗号鍵生成部４０６０は、式（２）を用いて、鍵生成情報Ｔ$_{b}$に対して一意に対応する暗号鍵Ｋ$_{b}$を生成する。鍵生成情報Ｔ$_{b}$は、図１０に示される鍵生成情報である。Ｅ$_{a}$は、鍵生成情報を構成する部分データＴ$_{b1}$などを任意の値に変換する関数である。ここで、AES 暗号方式を利用する場合、Ｅ$_{a}$は、部分データＴ$_{b1}$などを、利用する AES 暗号方式のブロックサイズと等しい大きさを持つ任意の値に変換する。
【数２】

$$K_1 = Ea(K_m, T_{b1}),$$
$$K_2 = Ea(K_1, T_{b2}),$$
$$K_b = Ea(K_2, T_{b3}) \quad \cdots(2)$$

【００８３】
＜＜方法３＞＞
また例えば、固有暗号鍵生成部４０６０は、再配置暗号方式に用いる暗号鍵をマスタ暗号鍵及び鍵生成情報から生成する。再配置暗号方式は、暗号化するデータを複数に分割し、分割したそれぞれのデータを、暗号鍵に示される情報に基づいて再配置することで、データを暗号化する。詳しくは、特許第４７３７３３４号公報に記載されている。
【００８４】
再配置暗号方式の簡単な例について、図１１を用いて説明する。図１１は、再配置暗号方式における暗号化を例示する図である。Ｄは暗号化されるデータであり、Ｋは暗号鍵である。ここで、暗号鍵は、再配置表とも呼ばれる。暗号鍵Ｋは、「３，１，２」という数字の並びである。
【００８５】
暗号鍵Ｋは、合計で３つの数字から成り、１番目が３であり、２番目が１であり、３番目が２である。この暗号鍵は、暗号化するデータを３つに分割した複数の部分データのうち、１番目の部分データを３番目に再配置し、２番目の部分データを１番目に再配置し、３番目のデータを２番目に再配置することを表している。
【００８６】
そこで、図１１において、データＤは、３つの部分データｄ$_{1}$～ｄ$_{3}$に分割される。そして、ｄ$_{1}$～ｄ$_{3}$は、暗号鍵Ｋが示す配置へ再配置される。こうすることで、データＤは、暗号化されたデータＥ$_{r}$（Ｄ，Ｋ）へ変換される。
【００８７】
再配置暗号に用いられる暗号鍵Ｋ$_{x}$を、鍵生成情報Ｔ$_{x}$とマスタ暗号鍵から生成する方法は、例えば次に示す方法である。ここで、各暗号鍵は、暗号化するデータを２５６個の部分データに分割して、各部分データを再配置するための暗号鍵であるとする。したがって、各暗号鍵は、１～２５６の各数字を重複しないように有する順列で表される。ここで、マスタ暗号鍵は、Ｋ$_{m}$＝（２５４，５，・・・１２７，９８）であるとする。
【００８８】

鍵生成情報T_xは、T_{x1}～T_{x3}を有しているとする。T_{x1}～T_{x3}はそれぞれ、２５６バイトの整数配列である。まず、T_{x1}を基に、疑似乱数を生成する。そして、生成した疑似乱数を用いて、マスタ暗号鍵K_mを Fisher-Yates Shuffle で攪拌し、K_1を生成する。同様に、T_{x2}を基に、疑似乱数を生成する。そして、生成した疑似乱数を用いて、K_1を Fisher-Yates Shuffle で攪拌し、K_2を生成する。さらに同様に、T_{x3}を基に、疑似乱数を生成する。そして、生成した疑似乱数を用いて、K_2を Fisher-Yates Shuffle で攪拌し、生成された配列をK_xとする。

【００８９】

［実施形態２］

図１２は、実施形態２に係るデータ伝送システム２０００を例示するブロック図である。図１２において、矢印の流れは情報の流れを示している。さらに、図１２において、各ブロックは、ハードウエア単位の構成ではなく、機能単位の構成を表している。

【００９０】

実施形態２の伝送データ生成部３０６０は、伝送データに対象マークを付与する。実施形態２のデータ取得装置４０００は、ディスパッチ部４１２０を有する。ディスパッチ部４１２０は、伝送データ取得部４０４０によって取得された伝送データに対象マークが付与されているか否かを判定する。正当性判定部４１００は、対象マークが付与されていると判定された伝送データの正当性を判定する。

【００９１】

＜処理の流れ＞

図１３は、実施形態２に係るデータ取得装置４０００によって実行される処理の流れを例示するフローチャートである。ステップＳ２０２において、ディスパッチ部４１２０は、伝送データに対象マークが付与されているか否かを判定する。伝送データに対象マークが付与されている場合、図１３の処理はステップＳ１０４に進む。一方、伝送データに対象マークが付与されていない場合、図１３の処理は終了する。

【００９２】

なお、図１３のステップＳ１０４以降で行われる処理の流れは、図７のステップＳ１０４以降で行われる処理の流れと同様である。そのため、図１３において、ステップＳ１０４の内容の記述及びステップＳ１０６以降の処理は省略されている。

【００９３】

＜作用・効果＞

実施形態２のデータ伝送システム２０００では、伝送データに対象マークが付与される。そのため、データ取得装置４０００において、対象マークが付与されている伝送データと対象マークが付与されていない伝送データとで、扱いを変えることができる。具体的には、対象マークが付与されている伝送データについて伝送データの正当性が判定される。

【００９４】

［実施例］

対象マークが付与されている伝送データと付与されていない伝送データの双方を扱うデータ伝送システム２０００を、実施例として示す。なお、下記に示すのはあくまでデータ伝送システム２０００の利用方法の１つを例示するものであり、データ伝送システム２０００の利用方法を限定するものではない。

【００９５】

＜データ伝送システム２０００が扱う伝送データ＞

本実施例に係るデータ伝送システム２０００は、２種類の伝送データを扱う。データ伝送システム２０００が扱う第１の種類の伝送データ（以下、第１伝送データ）は、特定の宛先が指定されておらず、不特定多数のユーザに配布することができる伝送データである。これは、上述の各実施形態に係るデータ伝送システム２０００が扱う伝送データに相当する。例として、Web ページで配布されるアプリケーションなどが挙げられる。一方、データ伝送システム２０００が扱う第２の種類の伝送データ（以下、第２伝送データ）は、特定の宛先が指定されている伝送データである。例として、電子メールなどが挙げられる

。
【００９６】
図１４は、本実施例のデータ伝送システム２０００が扱う伝送データのデータ構造を表す図である。図１４（ａ）は、伝送データの基本構造２００を示す図である。伝送データは、基本構造２００に示すように、第１領域２１０、第２領域２２０、及び第３領域２３０という３つのデータ領域を有する。第１伝送データと第２伝送データでは、これらのデータ領域に格納されるデータが異なる。
【００９７】
＜＜第１伝送データのデータ構造＞＞
図１４（ｂ）は、第１伝送データ３００のデータ構造を示す図である。第１伝送データにおいて、第１領域２１０には、提供元鍵生成情報１１０が格納されている。提供元鍵生成情報１１０は、伝送データを生成するデータ生成装置３０００に固有の鍵生成情報である。つまり提供元鍵生成情報１１０は、第１伝送データ３００を生成するデータ生成装置３０００の固有鍵生成情報格納部３０２０に格納されている固有鍵生成情報である。
【００９８】
第１伝送データ３００は、特定の宛先が指定されない伝送データである。そのため、第１伝送データ３００において、第２領域２２０には、「宛先を特定しない」ということを表す情報が格納されている。具体的には、第２領域２２０には、実施形態２で説明した対象マーク（対象マーク１２０）が格納される。
【００９９】
第１伝送データ３００において、第３領域２３０には、第１暗号文１３０が格納されている。第１暗号文１３０は、上述の各実施形態における暗号文３０と同様、データ生成装置３０００の固有暗号鍵で暗号化された暗号文である。
【０１００】
＜＜第２伝送データのデータ構造＞＞
図１４（ｃ）は、第２伝送データ４００のデータ構造を示す図である。第２伝送データ４００において、第１領域２１０には、提供元鍵生成情報１１０が格納されている。よって、第１領域２１０に格納されるデータは、第１伝送データ３００と第２伝送データ４００とで共通である。
【０１０１】
第２伝送データ４００は、特定の宛先が指定されて送信される伝送データである。そのため、第２伝送データ４００において、第２領域２２０には、宛先を特定するための情報を格納している。具体的には、第２領域２２０には、宛先のデータ取得装置４０００に固有の鍵生成情報である宛先鍵生成情報１４０が格納されている。ここで、本実施例における鍵生成情報は、データ生成装置３０００だけでなく、データ取得装置４０００についても固有であるとする。つまり鍵生成情報は、各データ生成装置３０００及び各データ取得装置４０００について、それぞれ固有に存在する。
【０１０２】
第２伝送データ４００において、第３領域２３０には、第２暗号文１５０が格納されている。第２暗号文１５０は、第１暗号文１３０とは異なり、宛先鍵生成情報１４０に対して一意に対応する固有暗号鍵で暗号化された暗号文である。そのため、本実施例におけるデータ生成装置３０００は、宛先のデータ取得装置４０００に固有の固有暗号鍵を用いて暗号文を生成する機能を有する。この機能の実現方法については後述する。
【０１０３】
＜データ生成装置３０００が実行する処理の概要＞
図１５は、本実施例のデータ伝送システム２０００によって実行される処理を概念的に示す図である。データ生成装置３０００は、提供元鍵情報１１０、第２領域データ１７０、及び伝達データ１８０を取得する。第２領域データ１７０は、対象マーク１２０又は宛先鍵生成情報１４０のいずれかである。
【０１０４】

まずデータ生成装置３０００は、提供元鍵生成情報１１０、第２領域データ１７０、及び伝達データ１８０を用いて平文１６０を生成する。

【０１０５】

次にデータ生成装置３０００は、以下のようにして中間データ５００を生成する。中間データ５００は、伝送データと同様に基本構造２００を有するデータである。まずデータ生成装置３０００は、中間データ５００の第１領域２１０に提供元鍵情報１１０を格納する。次にデータ生成装置３０００は、中間データ５００の第２領域２２０に第２領域データ１７０を格納する。そしてデータ生成装置３０００は、平文１６０をデータ生成装置３０００の固有暗号鍵４０（以下、固有暗号鍵４０－Ａ）で暗号化して第１暗号文１３０を生成し、中間データ５００の第３領域２３０に格納する。

【０１０６】

ここで、第２領域データ１７０が対象マーク１２０である場合、データ生成装置３０００は、中間データ５００を生成することによって、第１伝送データ３００を生成したこととなる。そこでデータ生成装置３０００は、第２領域データ１７０が対象マーク１２０である場合、伝送データの生成処理を終了する。

【０１０７】

一方、第２領域データ１７０が宛先鍵生成情報１４０である場合、中間データ５００は、第２伝送データ４００とは異なる。そこでデータ生成装置３０００は、中間データ５００を用いて第２伝送データ４００を生成する処理を行う。データ生成装置３０００が中間データ５００から第２伝送データ４００を生成する処理の流れについては後述する。

【０１０８】

＜データ取得装置４０００が実行する処理の概要＞

本実施例のデータ取得装置４０００は、取得した伝送データに対象マーク１２０が含まれているか否かによって、取得した伝送データが第１伝送データ３００と第２伝送データ４００のどちらであるかを判別する。データ取得装置４０００は、実施形態２で説明したディスパッチ部４１２０を用いて、伝送データに対象マーク１２０が含まれているか否かを判定する。伝送データに対象マーク１２０が含まれている場合、取得した伝送データは第１伝送データ３００である。そのため、データ取得装置４０００は、第１伝送データ３００に関する処理を行う。データ取得装置４０００が第１伝送データ３００に関して実行する処理は、実施形態１で説明したデータ取得装置４０００の処理と同様である。具体的には、まずデータ取得装置４０００は、提供元鍵生成情報１１０とマスタ暗号鍵１００を用いてデータ生成装置３０００の固有暗号鍵４０－Ａを生成する。次にデータ取得装置４０００は、生成した固有暗号鍵４０－Ａを用いて第１暗号文１３０を復号する。そして、データ取得装置４０００は、復号結果に基づいて、第１伝送データ３００の正当性を判定する。

【０１０９】

具体的には、データ取得装置４０００は、第１伝送データ３００に含まれている提供元鍵情報１１０と、復号結果の平文に含まれている提供元鍵情報が一致するか否かを判定する。例えばデータ生成装置３０００が平文１６０の先頭に提供元情報を格納する場合、データ取得装置４０００は、第１伝送データ３００に含まれている提供元鍵情報１１０と、復号して得た平文の先頭にある提供元鍵情報１１０と同サイズのデータ領域とを比較する。これらが一致する場合、データ取得装置４０００は、第１伝送データ３００が正当であると判定する。一方、これらが一致しない場合、データ取得装置４０００は、第１伝送データ３００が不正であると判定する。

【０１１０】

伝送データに対象マーク１２０が含まれていない場合、取得した伝送データは第２伝送データ４００である。そこでデータ取得装置４０００は、第２伝送データ４００に関する処理を行う。データ取得装置４０００が第２伝送データ４００に関して行う処理については後述する。

【０１１１】

以上の流れにより、データ生成装置３０００及びデータ取得装置４０００は、第１伝送データ３００と第２伝送データ４００の双方を扱うことができる。以下、データ生成装置３０００とデータ取得装置４０００が第２伝送データ４００について実行する処理について説明する。

【０１１２】

＜データ生成装置３０００による第２伝送データ４００の生成＞

図１６は、実施例に係るデータ生成装置３０００の構成を例示するブロック図である。本実施例におけるデータ生成装置３０００は、中間データ５００から第２伝送データ４００を生成するために、第２伝送データ生成部３２００及びマスタ暗号鍵格納部３２２０を有する。マスタ暗号鍵格納部３２２０は、マスタ暗号鍵格納部４０２０と同様にマスタ暗号鍵を格納する。ここで、マスタ暗号鍵は全てのデータ生成装置３０００及びデータ取得装置４０００について共通である。したがって、マスタ暗号鍵格納部３２２０に格納されているマスタ暗号鍵とマスタ暗号鍵格納部４０２０に格納されているマスタ暗号鍵は同内容のデータである。

【０１１３】

図１７は、第２伝送データ生成部３２００が第２伝送データ４００を生成する処理の流れを概念的に示す図である。まず第２伝送データ生成部３２００は、提供元鍵生成情報１１０及びマスタ暗号鍵１００を用いて、データ生成装置３０００の固有暗号鍵４０－Ａを生成する。そして、第２伝送データ生成部３２００は、生成した固有暗号鍵４０－Ａを用いて第１暗号文１３０を復号して平文１６０を算出する。第２伝送データ生成部３２００は、算出した伝達データ６０を、宛先のデータ取得装置４０００の固有暗号鍵（以下、固有暗号鍵４０－Ｂ）を用いて暗号化する。そのために、第２伝送データ生成部３２００は、マスタ暗号鍵１００及び宛先鍵生成情報１４０を用いて、宛先のデータ取得装置４０００の固有暗号鍵４０－Ｂを生成する。そして、第２伝送データ生成部３２２０は、生成した固有暗号鍵４０で伝達データ６０を暗号化して第２暗号文１５０を生成する。最後に、第２伝送データ生成部３２２０は、提供元鍵生成情報１１０、宛先鍵生成情報１４０、及び第２暗号文１５０を含む第２伝送データ４００を生成する。

【０１１４】

＜データ取得装置４０００による第２伝送データ４００の処理＞

図１８は、実施例に係るデータ取得装置４０００の構成を例示するブロック図である。本実施例におけるデータ取得装置４０００は、第２伝送データ４００を処理するために、第２伝送データ処理部４２００及び固有暗号鍵格納部４２２０を有する。固有暗号鍵格納部４２２０は、データ取得装置４０００の固有暗号鍵を格納する。

【０１１５】

図１９は、第２伝送データ処理部４２００が第２伝送データ４００を処理する流れを概念的に示す図である。第２伝送データ４００に含まれる第２暗号文１５０は、データ取得装置４０００の固有暗号鍵４０－Ｂを用いて暗号化されている。そのため、第２伝送データ処理部４２００は、固有暗号鍵格納部４２２０に格納されている固有暗号鍵４０－Ｂを用いて第２暗号文１５０を復号する。

【０１１６】

なお、第２伝送データ処理部４２００は、第２暗号文１５０を復号して得られた平文１６０を用いて、第２伝送データ４００の提供元が正しいか否かを確認してもよい。具体的には、第２伝送データ処理部４２００は、平文１６０に含まれる提供元鍵生成情報１１０が、第２伝送データ４００の第１領域２１０に含まれる提供元鍵生成情報１１０と一致するか否かを判定する。これらが一致することは、第２伝送データ４００の第１領域２１０に含まれている提供元鍵生成情報１１０が正しい提供元を表していることを意味する。そのため、第２伝送データ処理部４２００は、第２伝送データ４００の提供元が正しいか否かを確認することができる。

【０１１７】

以上、図面を参照して本発明の実施形態及び実施例について述べたが、これらは本発明

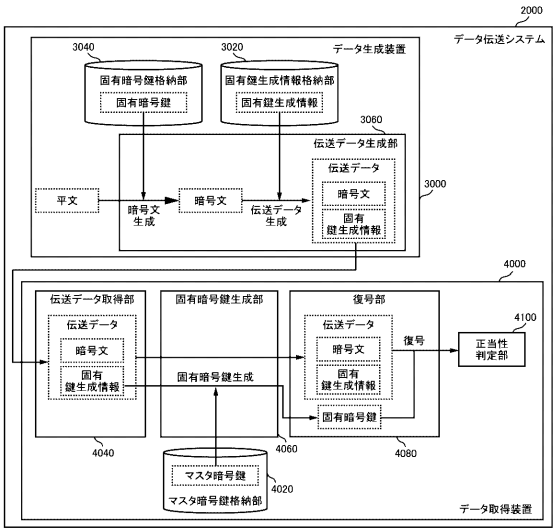
の例示であり、上記実施形態や実施例の組み合わせ、及び上記実施形態や実施例以外の様々な構成を採用することもできる。

【符号の説明】

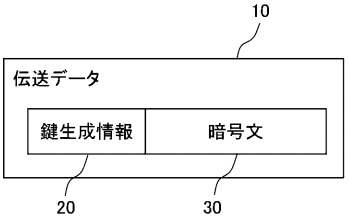
【０１１８】

１０　伝送データ
２０　鍵生成情報
３０　暗号文
４０　固有暗号鍵
５０　平文
６０　伝達データ
１００　マスタ暗号鍵
１１０　提供元鍵生成情報
１２０　対象マーク
１３０　第１暗号文
１４０　宛先鍵生成情報
１５０　第２暗号文
１６０　平文
１７０　第２領域データ
１８０　伝達データ
２００　基本構造
２１０　第１領域
２２０　第２領域
２３０　第３領域
３００　第１伝送データ
４００　第２伝送データ
５００　中間データ
２０００　データ伝送システム
３０００　データ生成装置
３０２０　固有鍵生成情報格納部
３０４０　固有暗号鍵格納部
３０６０　伝送データ生成部
３２００　第２伝送データ生成部
３２２０　マスタ暗号鍵格納部
４０００　データ取得装置
４０２０　マスタ暗号鍵格納部
４０４０　伝送データ取得部
４０６０　固有暗号鍵生成部
４０８０　復号部
４１００　正当性判定部
４１２０　ディスパッチ部
４２００　第２伝送データ処理部
４２２０　固有暗号鍵格納部

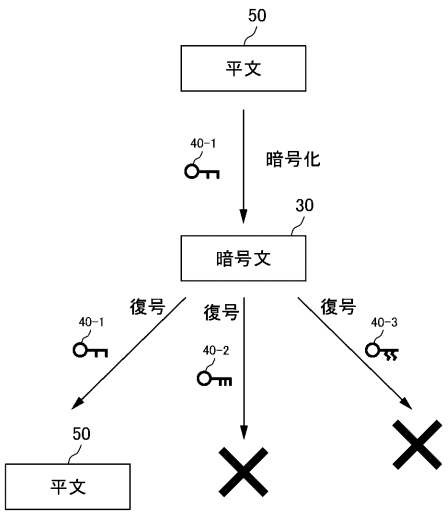
【図１】


2000
データ伝送システム
3040
固有暗号鍵格納部
固有暗号鍵
3020
固有鍵生成情報格納部
固有鍵生成情報
データ生成装置
3060
伝送データ生成部
伝送データ
暗号文
固有鍵生成情報
平文
暗号文生成
暗号文
伝送データ生成
3000
4000
伝送データ取得部
伝送データ
暗号文
固有鍵生成情報
固有暗号鍵生成部
固有暗号鍵生成
復号部
伝送データ
暗号文
固有鍵生成情報
固有暗号鍵
復号
4100
正当性判定部
4040
4060
4080
マスタ暗号鍵
4020
マスタ暗号鍵格納部
データ取得装置

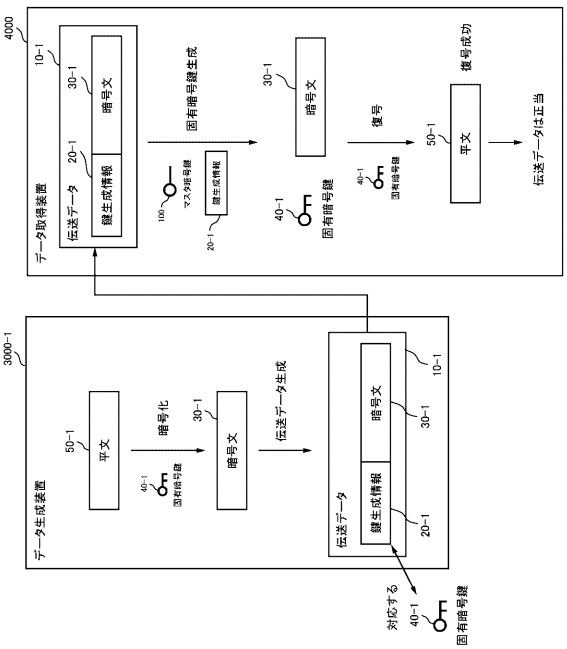
【図２】


10
伝送データ
鍵生成情報
暗号文
20
30

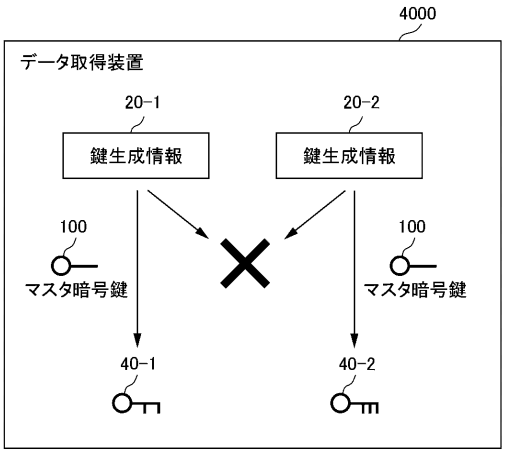
【図３】


50
平文
40-1
暗号化
30
暗号文
復号
復号
復号
40-1
40-2
40-3
50
平文

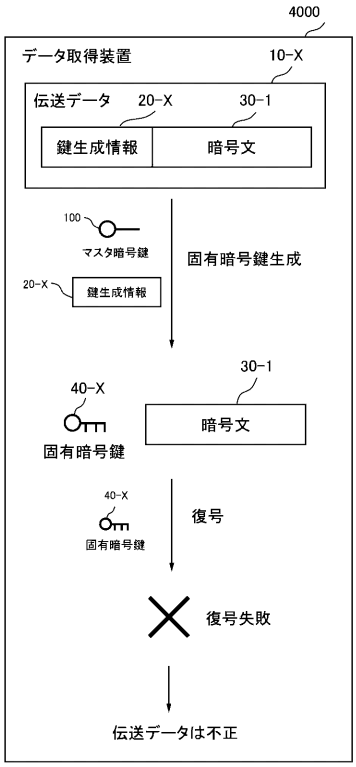
【図４】


4000
データ取得装置
10-1
伝送データ
30-1
暗号文
20-1
鍵生成情報
固有暗号鍵生成
100
マスタ暗号鍵
固有暗号鍵
復号
復号成功
50-1
平文
伝送データは正当
3000-1
データ生成装置
暗号化
伝送データ生成
対応する
固有暗号鍵

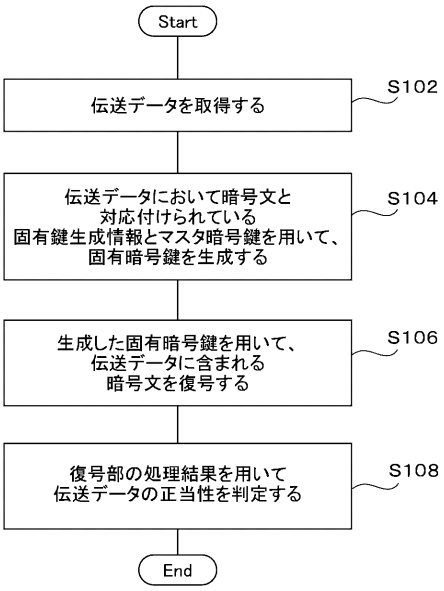
【図５】


4000
データ取得装置
20-1
20-2
鍵生成情報
鍵生成情報
100
100
マスタ暗号鍵
マスタ暗号鍵
40-1
40-2

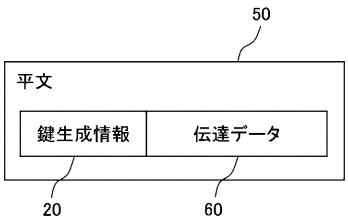
【図６】


4000
データ取得装置
10-X
伝送データ
20-X
30-1
鍵生成情報
暗号文
100
マスタ暗号鍵
固有暗号鍵生成
20-X
鍵生成情報
40-X
固有暗号鍵
30-1
暗号文
40-X
固有暗号鍵
復号
復号失敗
伝送データは不正

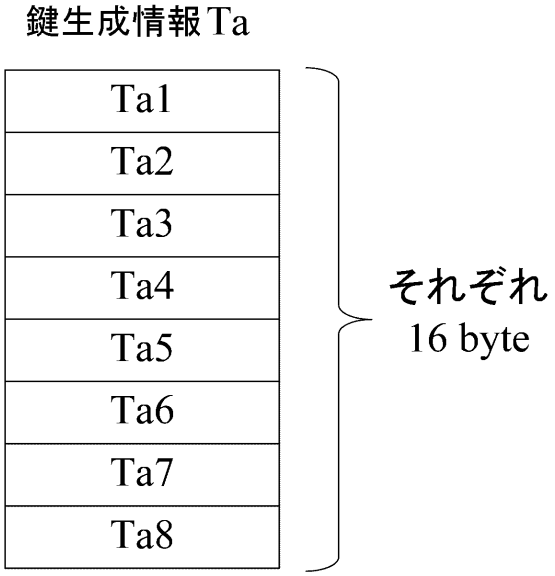
【図７】


Start
伝送データを取得する
S102
伝送データにおいて暗号文と
対応付けられている
固有鍵生成情報とマスタ暗号鍵を用いて、
固有暗号鍵を生成する
S104
生成した固有暗号鍵を用いて、
伝送データに含まれる
暗号文を復号する
S106
復号部の処理結果を用いて
伝送データの正当性を判定する
S108
End

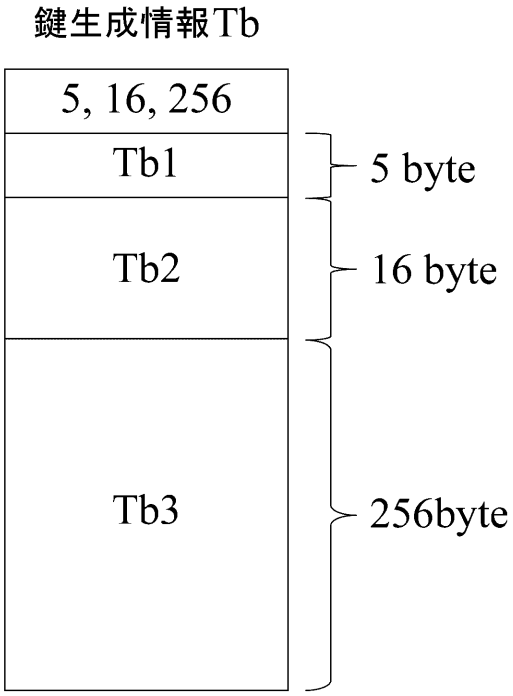
【図８】


50
平文
鍵生成情報
伝達データ
20
60

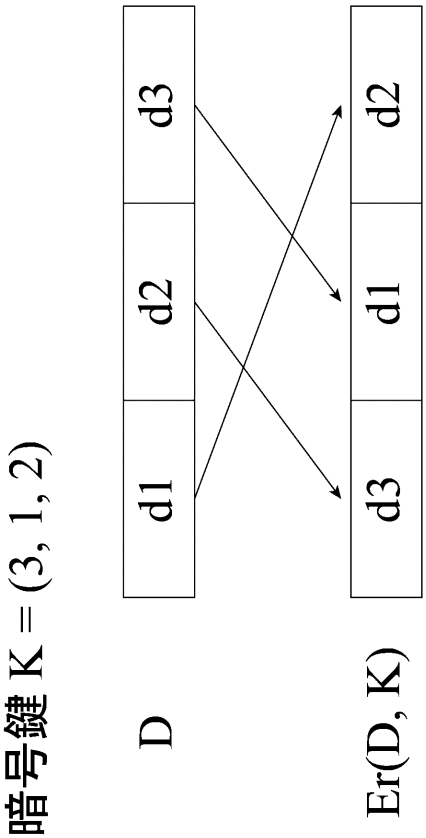
【図９】



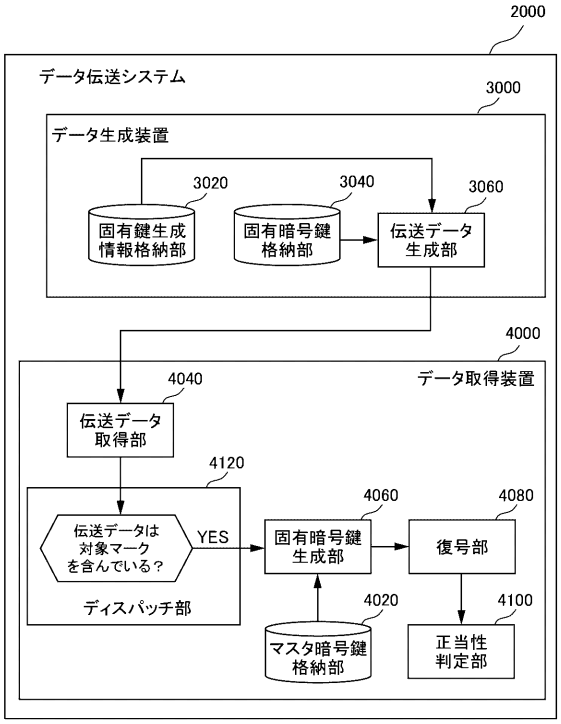
【図１０】



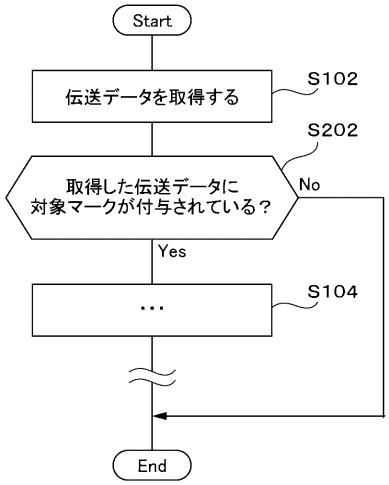
【図１１】



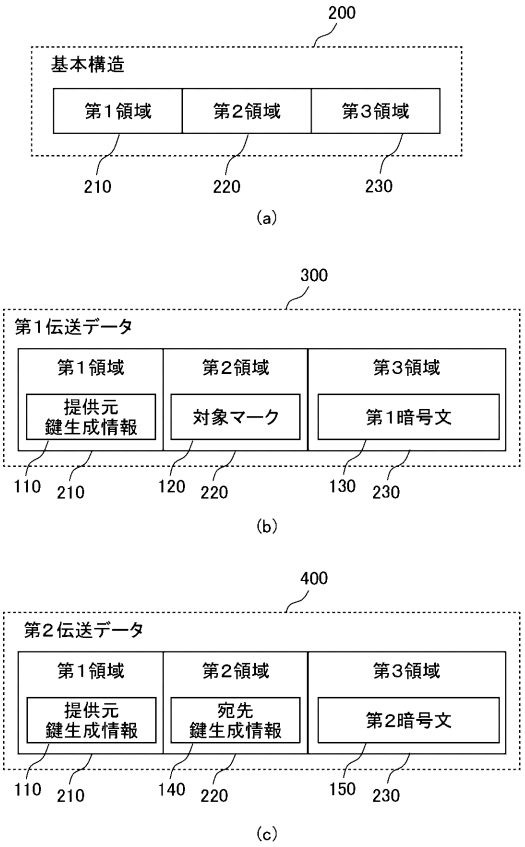
【図１２】



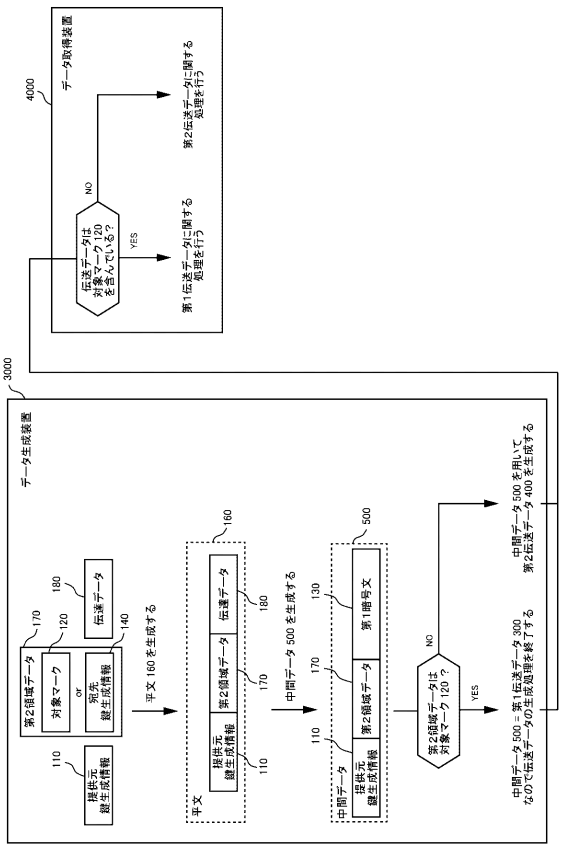
【図１３】



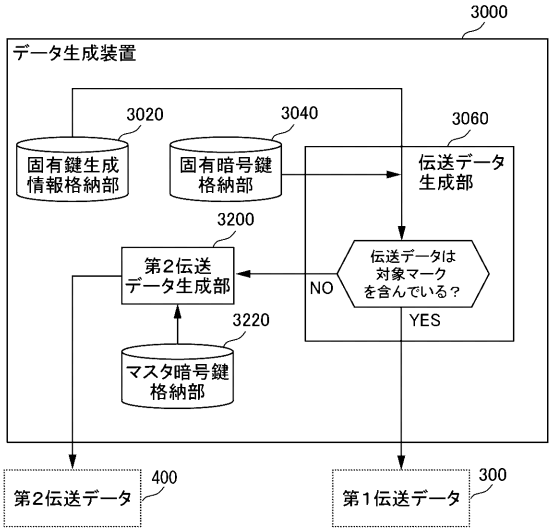
【図１４】



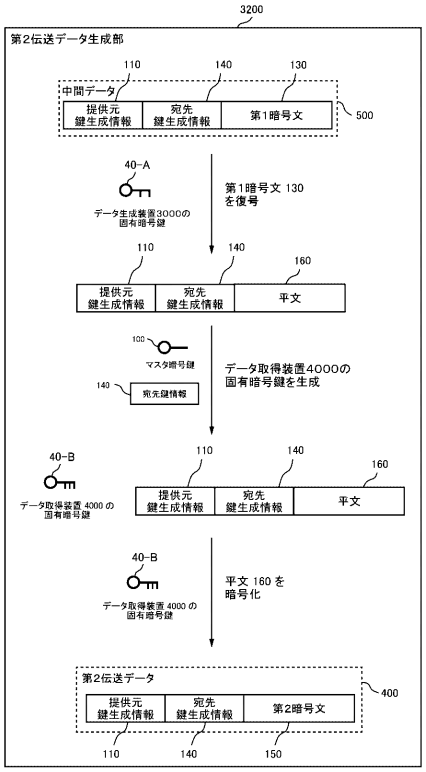
【図１５】



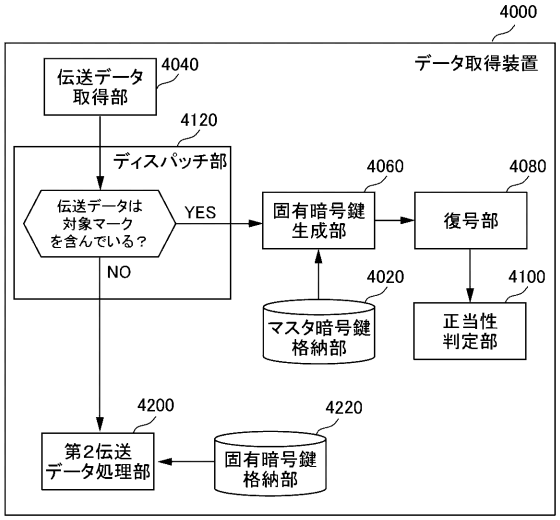
【図１６】



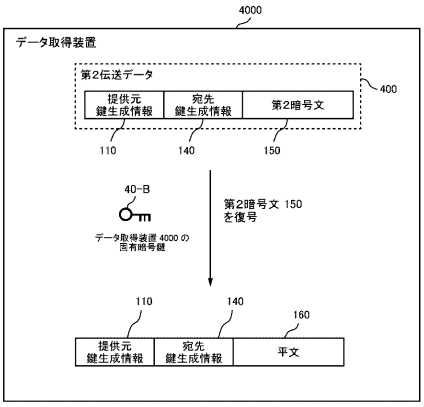
【図１７】


3200
第2伝送データ生成部
110
140
130
中間データ
提供元鍵生成情報
宛先鍵生成情報
第1暗号文
500
40-A
データ生成装置3000の固有暗号鍵
第1暗号文 130を復号
110
140
160
提供元鍵生成情報
宛先鍵生成情報
平文
100
マスタ暗号鍵
140
宛先鍵情報
データ取得装置4000の固有暗号鍵を生成
40-B
データ取得装置 4000 の固有暗号鍵
110
140
160
提供元鍵生成情報
宛先鍵生成情報
平文
40-B
データ取得装置 4000 の固有暗号鍵
平文 160 を暗号化
第2伝送データ
400
提供元鍵生成情報
宛先鍵生成情報
第2暗号文
110
140
150

【図１８】


4000
データ取得装置
伝送データ取得部
4040
4120
ディスパッチ部
伝送データは対象マークを含んでいる？
YES
NO
4060
固有暗号鍵生成部
4080
復号部
4020
マスタ暗号鍵格納部
4100
正当性判定部
4200
第2伝送データ処理部
4220
固有暗号鍵格納部

【図１９】


4000
データ取得装置
第2伝送データ
400
提供元鍵生成情報
宛先鍵生成情報
第2暗号文
110
140
150
40-B
データ取得装置 4000 の固有暗号鍵
第2暗号文 150を復号
110
140
160
提供元鍵生成情報
宛先鍵生成情報
平文