

(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2006-155190

(P2006-155190A)

(43) 公開日 平成18年6月15日(2006.6.15)

(51) Int. Cl.		F I		テーマコード (参考)
G06F 21/24	(2006.01)	G06F 12/14	530P	5B017
G06F 21/02	(2006.01)	G06F 12/14	510C	5B035
H04L 9/32	(2006.01)	G06F 12/14	540A	5J104
G06K 19/10	(2006.01)	H04L 9/00	675B	
H04L 9/08	(2006.01)	G06K 19/00	R	
審査請求 未請求 請求項の数 9 O L (全 40 頁) 最終頁に続く				

(21) 出願番号 特願2004-344183 (P2004-344183)

(22) 出願日 平成16年11月29日 (2004.11.29)

(71) 出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(74) 代理人 100082131

弁理士 稲本 義雄

(72) 発明者 森田 直

東京都品川区北品川6丁目7番35号 ソ

ニー株式会社内

Fターム(参考) 5B017 AA02 AA03 BA04 BA05 BA07

BB05 CA14 CA16

5B035 BB09 CA11 CA23 CA29

5J104 KA04 LA06 PA07

(54) 【発明の名称】 データ記憶装置、データ処理方法、記録媒体、およびプログラム

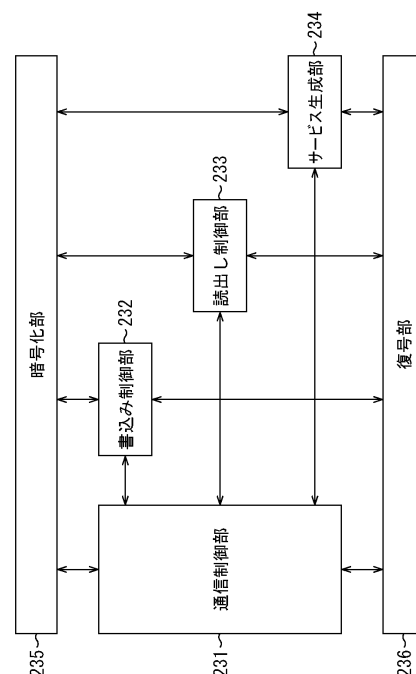
(57) 【要約】

【課題】より簡単にデータを安全に授受できるようにする。

【解決手段】 書込み制御部232は、書込みフラグがオフの場合、受信したデータを書込み、書込みフラグをオンする。読出し制御部233は、受信した読出し鍵が一致した場合、書込みフラグをオフし、データを送信する。あるいは、書込み制御部232は、受信した書込み鍵が一致した場合、受信したデータを書込み、暗号化フラグをオフする。読出し制御部231は、暗号化フラグがオフの場合、受信した暗号化鍵で暗号化したデータを送信し、暗号化フラグをオンし、暗号化フラグがオンの場合、すでに暗号化されているデータを送信する。本発明は、ICカードに適用することができる。

【選択図】 図8

図8



【特許請求の範囲】

【請求項 1】

記憶領域を有する記憶部を備えたデータ記憶装置において、

第 1 の情報処理装置から送信されてくる、前記記憶領域からのデータの読出しを許可する第 1 の読出し鍵を登録する読出し鍵登録手段と、

前記記憶領域に記憶されているデータが最初に読出されるまで、前記記憶領域への新たなデータの書込みを禁止するように前記記憶部へのデータの書込みを制御する書込み制御手段と、

前記第 1 の情報処理装置または前記第 1 の情報処理装置とは異なる第 2 の情報処理装置により前記記憶領域からのデータの読出しが要求された場合、前記第 1 の情報処理装置または前記第 2 の情報処理装置から送信されてくる第 2 の読出し鍵と前記第 1 の読出し鍵とが一致するとき、前記記憶領域からのデータの読出しを許可するように前記記憶部からのデータの読出しを制御する読出し制御手段と

を含むことを特徴とするデータ記憶装置。

10

【請求項 2】

前記書込み制御手段は、前記記憶領域に書込むデータとともに送信されてくる前記記憶領域に書込むデータを暗号化したデジタル署名をさらに前記記憶領域に書込むように前記記憶部へのデータの書込みを制御し、

前記読出し制御手段は、前記第 1 の情報処理装置または前記第 2 の情報処理装置により前記第 2 の鍵が送信されずに前記記憶領域に記憶されているデータの内容の確認が要求された場合、前記記憶領域から前記デジタル署名を読出し、前記第 1 の情報処理装置または前記第 2 の情報処理装置に前記デジタル署名を送信するように前記記憶部からのデータの読出しを制御する

20

ことを特徴とする請求項 1 に記載のデータ記憶装置。

【請求項 3】

記憶領域を有する記憶部を備えたデータ記憶装置のデータ処理方法において、

第 1 の情報処理装置から送信されてくる、前記記憶領域からのデータの読出しを許可する第 1 の読出し鍵を登録する読出し鍵登録ステップと、

前記記憶領域に記憶されているデータが最初に読出されるまで、前記記憶領域への新たなデータの書込みを禁止するように前記記憶部へのデータの書込みを制御する書込み制御ステップと、

30

前記第 1 の情報処理装置または前記第 1 の情報処理装置とは異なる第 2 の情報処理装置により前記記憶領域からのデータの読出しが要求された場合、前記第 1 の情報処理装置または前記第 2 の情報処理装置から送信されてくる第 2 の読出し鍵と前記第 1 の読出し鍵とが一致するときのみ、前記記憶領域からのデータの読出しを許可するように前記記憶部からのデータの読出しを制御する読出し制御ステップと

を含むことを特徴とするデータ処理方法。

【請求項 4】

記憶領域を有する記憶部を備えたデータ記憶装置のデータ処理用のプログラムであって

40

第 1 の情報処理装置から送信されてくる、前記記憶領域からのデータの読出しを許可する第 1 の読出し鍵を登録する読出し鍵登録ステップと、

前記記憶領域に記憶されているデータが最初に読出されるまで、前記記憶領域への新たなデータの書込みを禁止するように前記記憶部へのデータの書込みを制御する書込み制御ステップと、

前記第 1 の情報処理装置または前記第 1 の情報処理装置とは異なる第 2 の情報処理装置により前記記憶領域からのデータの読出しが要求された場合、前記第 1 の情報処理装置または前記第 2 の情報処理装置から送信されてくる第 2 の読出し鍵と前記第 1 の読出し鍵とが一致するときのみ、前記記憶領域からのデータの読出しを許可するように前記記憶部からのデータの読出しを制御する読出し制御ステップと

50

を含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。

【請求項 5】

記憶領域を有する記憶部を備えたデータ記憶装置に、データ処理を行なわせるプログラムであって、

第 1 の情報処理装置から送信されてくる、前記記憶領域からのデータの読出しを許可する第 1 の読出し鍵を登録する読出し鍵登録ステップと、

前記記憶領域に記憶されているデータが最初に読出されるまで、前記記憶領域への新たなデータの書き込みを禁止するように前記記憶部へのデータの書き込みを制御する書き込み制御ステップと、

10

前記第 1 の情報処理装置または前記第 1 の情報処理装置とは異なる第 2 の情報処理装置により前記記憶領域からのデータの読出しが要求された場合、前記第 1 の情報処理装置または前記第 2 の情報処理装置から送信されてくる第 2 の読出し鍵と前記第 1 の読出し鍵とが一致するときのみ、前記記憶領域からのデータの読出しを許可するように前記記憶部からのデータの読出しを制御する読出し制御ステップと

を含むことを特徴とするプログラム。

【請求項 6】

記憶領域を有する記憶部を備えたデータ記憶装置において、

第 1 の情報処理装置から送信されてくる、前記記憶領域へのデータの書き込みを許可する第 1 の書き込み鍵を登録する書き込み鍵登録手段と、

20

前記第 1 の情報処理装置または前記第 1 の情報処理装置とは異なる第 2 の情報処理装置により前記記憶領域へのデータの書き込みが要求された場合、前記第 1 の情報処理装置または前記第 2 の情報処理装置から送信されてくる第 2 の書き込み鍵が前記第 1 の書き込み鍵と一致するときのみ、前記記憶領域へのデータの書き込みを許可するように前記記憶部へのデータの書き込みを制御する書き込み制御手段と、

前記第 1 の情報処理装置または前記第 2 の情報処理装置により前記記憶領域からのデータの読出しが要求された場合、前記記憶領域に記憶されているデータが最初に読出されるとき、前記第 1 の情報処理装置または前記第 2 の情報処理装置より送信されてくる暗号化鍵を用いて前記記憶領域に記憶されているデータを暗号化する暗号化手段と、

前記第 1 の情報処理装置または前記第 2 の情報処理装置により前記記憶領域からのデータの読出しが要求された場合、前記記憶領域に記憶されているデータが最初に読出されるとき、前記暗号化手段により暗号化されたデータを前記第 1 の情報処理装置または前記第 2 の情報処理装置に送信し、前記記憶領域に記憶されているデータが 2 回目以降に読出されるとき、前記暗号化手段によりすでに暗号化されているデータを前記記憶領域から読出し、前記読出したデータを前記第 1 の情報処理装置または前記第 2 の情報処理装置に送信する送信制御手段と

30

を含むことを特徴とするデータ記憶装置。

【請求項 7】

記憶領域を有する記憶部を備えたデータ記憶装置のデータ処理方法において、

第 1 の情報処理装置から送信されてくる、前記記憶領域へのデータの書き込みを許可する第 1 の書き込み鍵を登録する書き込み鍵登録ステップと、

40

前記第 1 の情報処理装置または前記第 1 の情報処理装置とは異なる第 2 の情報処理装置により前記記憶領域へのデータの書き込みが要求された場合、前記第 1 の情報処理装置または前記第 2 の情報処理装置から送信されてくる第 2 の書き込み鍵が前記第 1 の書き込み鍵と一致するときのみ、前記記憶領域へのデータの書き込みを許可するように前記記憶部へのデータの書き込みを制御する書き込み制御ステップと、

前記第 1 の情報処理装置または前記第 2 の情報処理装置により前記記憶領域からのデータの読出しが要求された場合、前記記憶領域に記憶されているデータが最初に読出されるとき、前記第 1 の情報処理装置または前記第 2 の情報処理装置より送信されてくる暗号化鍵を用いて前記記憶領域に記憶されているデータを暗号化する暗号化ステップと、

50

前記第 1 の情報処理装置または前記第 2 の情報処理装置により前記記憶領域からのデータの読出しが要求された場合、前記記憶領域に記憶されているデータが最初に読出されるとき、前記暗号化ステップの処理により暗号化されたデータを前記第 1 の情報処理装置または前記第 2 の情報処理装置に送信し、前記記憶領域に記憶されているデータが 2 回目以降に読出されるとき、前記暗号化ステップの処理によりすでに暗号化されているデータを前記記憶領域から読出し、前記読出したデータを前記第 1 の情報処理装置または前記第 2 の情報処理装置に送信する送信制御ステップと

を含むことを特徴とするデータ処理方法。

【請求項 8】

記憶領域を有する記憶部を備えたデータ記憶装置のデータ処理用のプログラムであって 10

第 1 の情報処理装置から送信されてくる、前記記憶領域へのデータの書込みを許可する第 1 の書込み鍵を登録する書込み鍵登録ステップと、

前記第 1 の情報処理装置または前記第 1 の情報処理装置とは異なる第 2 の情報処理装置により前記記憶領域へのデータの書込みが要求された場合、前記第 1 の情報処理装置または前記第 2 の情報処理装置から送信されてくる第 2 の書込み鍵が前記第 1 の書込み鍵と一致するときのみ、前記記憶領域へのデータの書込みを許可するように前記記憶部へのデータの書込みを制御する書込み制御ステップと、

前記第 1 の情報処理装置または前記第 2 の情報処理装置により前記記憶領域からのデータの読出しが要求された場合、前記記憶領域に記憶されているデータが最初に読出されるとき、前記第 1 の情報処理装置または前記第 2 の情報処理装置より送信されてくる暗号化鍵を用いて前記記憶領域に記憶されているデータを暗号化する暗号化ステップと、 20

前記第 1 の情報処理装置または前記第 2 の情報処理装置により前記記憶領域からのデータの読出しが要求された場合、前記記憶領域に記憶されているデータが最初に読出されるとき、前記暗号化ステップの処理により暗号化されたデータを前記第 1 の情報処理装置または前記第 2 の情報処理装置に送信し、前記記憶領域に記憶されているデータが 2 回目以降に読出されるとき、前記暗号化ステップの処理によりすでに暗号化されているデータを前記記憶領域から読出し、前記読出したデータを前記第 1 の情報処理装置または前記第 2 の情報処理装置に送信する送信制御ステップと

を含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。 30

【請求項 9】

記憶領域を有する記憶部を備えたデータ記憶装置に、データ処理を行なわせるプログラムであって、

第 1 の情報処理装置から送信されてくる、前記記憶領域へのデータの書込みを許可する第 1 の書込み鍵を登録する書込み鍵登録ステップと、

前記第 1 の情報処理装置または前記第 1 の情報処理装置とは異なる第 2 の情報処理装置により前記記憶領域へのデータの書込みが要求された場合、前記第 1 の情報処理装置または前記第 2 の情報処理装置から送信されてくる第 2 の書込み鍵が前記第 1 の書込み鍵と一致するときのみ、前記記憶領域へのデータの書込みを許可するように前記記憶部へのデータの書込みを制御する書込み制御ステップと、 40

前記第 1 の情報処理装置または前記第 2 の情報処理装置により前記記憶領域からのデータの読出しが要求された場合、前記記憶領域に記憶されているデータが最初に読出されるとき、前記第 1 の情報処理装置または前記第 2 の情報処理装置より送信されてくる暗号化鍵を用いて前記記憶領域に記憶されているデータを暗号化する暗号化ステップと、

前記第 1 の情報処理装置または前記第 2 の情報処理装置により前記記憶領域からのデータの読出しが要求された場合、前記記憶領域に記憶されているデータが最初に読出されるとき、前記暗号化ステップの処理により暗号化されたデータを前記第 1 の情報処理装置または前記第 2 の情報処理装置に送信し、前記記憶領域に記憶されているデータが 2 回目以降に読出されるとき、前記暗号化ステップの処理によりすでに暗号化されているデータを 50

前記記憶領域から読出し、前記読出したデータを前記第1の情報処理装置または前記第2の情報処理装置に送信する送信制御ステップと

を含むことを特徴とするプログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、データの安全性を確保するようにしたデータ記憶装置、データ処理方法、記録媒体、およびプログラムに関する。

【背景技術】

【0002】

近年、情報処理技術の発展に伴い、毎日大量の情報がインターネットなどの伝送路や各種の記録媒体を介して授受されている。このような情報の授受において、情報を安全に伝達するために、暗号技術が用いられる。

【0003】

例えば、暗号技術の1つとして秘密鍵暗号方式がある。これは、送信者と受信者が共通の秘密鍵を持ち、送信者が秘密鍵を用いて暗号化したデータを送信し、受信者が暗号化されたデータを秘密鍵を用いて復号する方式である。

【0004】

例えば、秘密鍵方式を利用した暗号技術の一例として、通信を行なう二者間の相互認証を二種類の秘密鍵を用いて行なう方法が提案されている（例えば、特許文献1参照）。

【0005】

また、近年、秘密鍵方式に代わる暗号方式として、公開鍵方式が普及してきている。公開鍵方式は、対になる2つの鍵を使ってデータを暗号化および復号する方式であり、2つの鍵のうち一方の鍵は、公開鍵として他人に広く公開され、もう一方の鍵は、秘密鍵として公開鍵を公開した人が厳重に保管する。秘密鍵で暗号化したデータは対になる公開鍵でしか復号できず、公開鍵で暗号化したデータは対になる秘密鍵でしか復号できないようになっている。従って、公開鍵を用いて暗号化したデータは秘密鍵を保管する人が入手するまで復号できないため、データを安全に送信することができる。また、秘密鍵方式では、第三者が入手できないように安全な経路を用いてデータの授受相手に秘密鍵を送付する必要があるのに対し、公開鍵方式では、公開鍵の送付経路の安全性は特に問われないため、鍵の管理が楽であり、また、鍵の盗難を心配する必要がない。

【0006】

例えば、公開鍵暗号方式を利用したセキュリティ基盤として、PKI(Public Key Infrastructure)が知られている。

【特許文献1】特開平10-20780号公報

【発明の開示】

【発明が解決しようとする課題】

【0007】

しかしながら、秘密鍵方式では、データの授受を行なう前に安全な経路を用いて秘密鍵を送付する必要があるとあり、また、授受相手ごとに異なる秘密鍵を用いてデータを暗号化する必要があり、鍵の管理やデータ授受の手順が煩雑になってしまうという課題があった。

【0008】

さらに、公開鍵方式では、データの授受を行なう前に、データの受信者が公開鍵を公開し、データの送信者が公開鍵を入手する必要があるとあり、また、送信者は、異なる受信者に対して、それぞれ異なる公開鍵を用いてデータを暗号化して送信する必要があるとあり、鍵の管理やデータ授受の手順が煩雑になってしまうという課題があった。

【0009】

さらに、PKIにおいては、公開鍵の持ち主を証明する証明書を発行する第三者の機関である認証局を設ける必要があるとあり、システムが大規模になってしまうとともに、データ授受の手順が煩雑になってしまうという課題があった。

10

20

30

40

50

【 0 0 1 0 】

本発明は、このような状況に鑑みてなされたものであり、より簡単にデータを安全に授受できるようにするものである。

【課題を解決するための手段】

【 0 0 1 1 】

本発明の第 1 のデータ記憶装置は、記憶領域を有する記憶部を備えたデータ記憶装置であって、第 1 の情報処理装置から送信されてくる、記憶領域からのデータの読出しを許可する第 1 の読出し鍵を登録する読出し鍵登録手段と、記憶領域に記憶されているデータが最初に読出されるまで、記憶領域への新たなデータの書込みを禁止するように記憶部へのデータの書込みを制御する書込み制御手段と、第 1 の情報処理装置または第 1 の情報処理装置とは異なる第 2 の情報処理装置により記憶領域からのデータの読出しが要求された場合、第 1 の情報処理装置または第 2 の情報処理装置から送信されてくる第 2 の読出し鍵と第 1 の読出し鍵とが一致するとき、記憶領域からのデータの読出しを許可するように記憶部からのデータの読出しを制御する読出し制御手段とを含むことを特徴とする。 10

【 0 0 1 2 】

書込み制御手段は、記憶領域に書込むデータとともに送信されてくる記憶領域に書込むデータを暗号化したデジタル署名をさらに記憶領域に書込むように記憶部へのデータの書込みを制御し、読出し制御手段は、第 1 の情報処理装置または第 2 の情報処理装置により第 2 の鍵が送信されずに記憶領域に記憶されているデータの内容の確認が要求された場合、記憶領域からデジタル署名を読出し、第 1 の情報処理装置または第 2 の情報処理装置にデジタル署名を送信するように記憶部からのデータの読出しを制御するようにすることができる。 20

【 0 0 1 3 】

本発明の第 1 のデータ処理方法は、記憶領域を有する記憶部を備えたデータ記憶装置のデータ処理方法であって、第 1 の情報処理装置から送信されてくる、記憶領域からのデータの読出しを許可する第 1 の読出し鍵を登録する読出し鍵登録ステップと、記憶領域に記憶されているデータが最初に読出されるまで、記憶領域への新たなデータの書込みを禁止するように記憶部へのデータの書込みを制御する書込み制御ステップと、第 1 の情報処理装置または第 1 の情報処理装置とは異なる第 2 の情報処理装置により記憶領域からのデータの読出しが要求された場合、第 1 の情報処理装置または第 2 の情報処理装置から送信されてくる第 2 の読出し鍵と第 1 の読出し鍵とが一致するときのみ、記憶領域からのデータの読出しを許可するように記憶部からのデータの読出しを制御する読出し制御ステップとを含むことを特徴とする。 30

【 0 0 1 4 】

本発明の第 1 の記録媒体に記録されているプログラムは、記憶領域を有する記憶部を備えたデータ記憶装置のデータ処理用のプログラムであって、第 1 の情報処理装置から送信されてくる、記憶領域からのデータの読出しを許可する第 1 の読出し鍵を登録する読出し鍵登録ステップと、記憶領域に記憶されているデータが最初に読出されるまで、記憶領域への新たなデータの書込みを禁止するように記憶部へのデータの書込みを制御する書込み制御ステップと、第 1 の情報処理装置または第 1 の情報処理装置とは異なる第 2 の情報処理装置により記憶領域からのデータの読出しが要求された場合、第 1 の情報処理装置または第 2 の情報処理装置から送信されてくる第 2 の読出し鍵と第 1 の読出し鍵とが一致するときのみ、記憶領域からのデータの読出しを許可するように記憶部からのデータの読出しを制御する読出し制御ステップとを含むことを特徴とする。 40

【 0 0 1 5 】

本発明の第 1 のプログラムは、記憶領域を有する記憶部を備えたデータ記憶装置に、データ処理を行なわせるプログラムであって、第 1 の情報処理装置から送信されてくる、記憶領域からのデータの読出しを許可する第 1 の読出し鍵を登録する読出し鍵登録ステップと、記憶領域に記憶されているデータが最初に読出されるまで、記憶領域への新たなデータの書込みを禁止するように記憶部へのデータの書込みを制御する書込み制御ステップと 50

、第1の情報処理装置または第1の情報処理装置とは異なる第2の情報処理装置により記憶領域からのデータの読出しが要求された場合、第1の情報処理装置または第2の情報処理装置から送信されてくる第2の読出し鍵と第1の読出し鍵とが一致するときのみ、記憶領域からのデータの読出しを許可するように記憶部からのデータの読出しを制御する読出し制御ステップとを含むことを特徴とする。

【0016】

本発明の第2のデータ記憶装置は、記憶領域を有する記憶部を備えたデータ記憶装置であって、第1の情報処理装置から送信されてくる、記憶領域へのデータの書込みを許可する第1の書込み鍵を登録する書込み鍵登録手段と、第1の情報処理装置または第1の情報処理装置とは異なる第2の情報処理装置により記憶領域へのデータの書込みが要求された場合、第1の情報処理装置または第2の情報処理装置から送信されてくる第2の書込み鍵が第1の書込み鍵と一致するときのみ、記憶領域へのデータの書込みを許可するように記憶部へのデータの書込みを制御する書込み制御手段と、第1の情報処理装置または第2の情報処理装置により記憶領域からのデータの読出しが要求された場合、記憶領域に記憶されているデータが最初に読出されるとき、第1の情報処理装置または第2の情報処理装置より送信されてくる暗号化鍵を用いて記憶領域に記憶されているデータを暗号化する暗号化手段と、第1の情報処理装置または第2の情報処理装置により記憶領域からのデータの読出しが要求された場合、記憶領域に記憶されているデータが最初に読出されるとき、暗号化手段により暗号化されたデータを第1の情報処理装置または第2の情報処理装置に送信し、記憶領域に記憶されているデータが2回目以降に読出されるとき、暗号化手段によりすでに暗号化されているデータを記憶領域から読出し、読出したデータを第1の情報処理装置または第2の情報処理装置に送信する送信制御手段とを含むことを特徴とする。

【0017】

本発明の第2のデータ処理方法は、記憶領域を有する記憶部を備えたデータ記憶装置のデータ処理方法であって、第1の情報処理装置から送信されてくる、記憶領域へのデータの書込みを許可する第1の書込み鍵を登録する書込み鍵登録ステップと、第1の情報処理装置または第1の情報処理装置とは異なる第2の情報処理装置により記憶領域へのデータの書込みが要求された場合、第1の情報処理装置または第2の情報処理装置から送信されてくる第2の書込み鍵が第1の書込み鍵と一致するときのみ、記憶領域へのデータの書込みを許可するように記憶部へのデータの書込みを制御する書込み制御ステップと、第1の情報処理装置または第2の情報処理装置により記憶領域からのデータの読出しが要求された場合、記憶領域に記憶されているデータが最初に読出されるとき、第1の情報処理装置または第2の情報処理装置より送信されてくる暗号化鍵を用いて記憶領域に記憶されているデータを暗号化する暗号化ステップと、第1の情報処理装置または第2の情報処理装置により記憶領域からのデータの読出しが要求された場合、記憶領域に記憶されているデータが最初に読出されるとき、暗号化ステップの処理により暗号化されたデータを第1の情報処理装置または第2の情報処理装置に送信し、記憶領域に記憶されているデータが2回目以降に読出されるとき、暗号化ステップの処理によりすでに暗号化されているデータを記憶領域から読出し、読出したデータを第1の情報処理装置または第2の情報処理装置に送信する送信制御ステップとを含むことを特徴とする。

【0018】

本発明の第2の記録媒体に記録されているプログラムは、記憶領域を有する記憶部を備えたデータ記憶装置のデータ処理用のプログラムであって、第1の情報処理装置から送信されてくる、記憶領域へのデータの書込みを許可する第1の書込み鍵を登録する書込み鍵登録ステップと、第1の情報処理装置または第1の情報処理装置とは異なる第2の情報処理装置により記憶領域へのデータの書込みが要求された場合、第1の情報処理装置または第2の情報処理装置から送信されてくる第2の書込み鍵が第1の書込み鍵と一致するときのみ、記憶領域へのデータの書込みを許可するように記憶部へのデータの書込みを制御する書込み制御ステップと、第1の情報処理装置または第2の情報処理装置により記憶領域からのデータの読出しが要求された場合、記憶領域に記憶されているデータが最初に読出

10

20

30

40

50

されるとき、第 1 の情報処理装置または第 2 の情報処理装置より送信されてくる暗号化鍵を用いて記憶領域に記憶されているデータを暗号化する暗号化ステップと、第 1 の情報処理装置または第 2 の情報処理装置により記憶領域からのデータの読出しが要求された場合、記憶領域に記憶されているデータが最初に読出されるとき、暗号化ステップの処理により暗号化されたデータを第 1 の情報処理装置または第 2 の情報処理装置に送信し、記憶領域に記憶されているデータが 2 回目以降に読出されるとき、暗号化ステップの処理によりすでに暗号化されているデータを記憶領域から読出し、読出したデータを第 1 の情報処理装置または第 2 の情報処理装置に送信する送信制御ステップとを含むことを特徴とする。

【0019】

本発明の第 2 のプログラムは、記憶領域を有する記憶部を備えたデータ記憶装置に、データ処理を行なわせるプログラムであって、第 1 の情報処理装置から送信されてくる、記憶領域へのデータの書込みを許可する第 1 の書込み鍵を登録する書込み鍵登録ステップと、第 1 の情報処理装置または第 1 の情報処理装置とは異なる第 2 の情報処理装置により記憶領域へのデータの書込みが要求された場合、第 1 の情報処理装置または第 2 の情報処理装置から送信されてくる第 2 の書込み鍵が第 1 の書込み鍵と一致するときのみ、記憶領域へのデータの書込みを許可するように記憶部へのデータの書込みを制御する書込み制御ステップと、第 1 の情報処理装置または第 2 の情報処理装置により記憶領域からのデータの読出しが要求された場合、記憶領域に記憶されているデータが最初に読出されるとき、第 1 の情報処理装置または第 2 の情報処理装置より送信されてくる暗号化鍵を用いて記憶領域に記憶されているデータを暗号化する暗号化ステップと、第 1 の情報処理装置または第 2 の情報処理装置により記憶領域からのデータの読出しが要求された場合、記憶領域に記憶されているデータが最初に読出されるとき、暗号化ステップの処理により暗号化されたデータを第 1 の情報処理装置または第 2 の情報処理装置に送信し、記憶領域に記憶されているデータが 2 回目以降に読出されるとき、暗号化ステップの処理によりすでに暗号化されているデータを記憶領域から読出し、読出したデータを第 1 の情報処理装置または第 2 の情報処理装置に送信する送信制御ステップとを含むことを特徴とする。

【0020】

本発明の第 1 のデータ記憶装置、第 1 のデータ処理方法、第 1 の記録媒体、および第 1 のプログラムによれば、第 1 の情報処理装置から送信されてくる、記憶領域からのデータの読出しを許可する第 1 の読出し鍵が登録され、記憶領域に記憶されているデータが最初に読出されるまで、記憶領域への新たなデータの書込みを禁止するように記憶部へのデータの書込みが制御され、第 1 の情報処理装置または第 1 の情報処理装置とは異なる第 2 の情報処理装置により記憶領域からのデータの読出しが要求された場合、第 1 の情報処理装置または第 2 の情報処理装置から送信されてくる第 2 の読出し鍵と第 1 の読出し鍵とが一致するとき、記憶領域からのデータの読出しを許可するように記憶部からのデータの読出しが制御される。

【0021】

本発明の第 2 のデータ記憶装置、第 2 のデータ処理方法、第 2 の記録媒体、および第 2 のプログラムによれば、第 1 の情報処理装置から送信されてくる、記憶領域へのデータの書込みを許可する第 1 の書込み鍵が登録され、第 1 の情報処理装置または第 1 の情報処理装置とは異なる第 2 の情報処理装置により記憶領域へのデータの書込みが要求された場合、第 1 の情報処理装置または第 2 の情報処理装置から送信されてくる第 2 の書込み鍵が第 1 の書込み鍵と一致するとき、記憶領域へのデータの書込みを許可するように記憶部へのデータの書込みが制御され、第 1 の情報処理装置または第 2 の情報処理装置により記憶領域からのデータの読出しが要求された場合、記憶領域に記憶されているデータが最初に読出されるとき、第 1 の情報処理装置または第 2 の情報処理装置より送信されてくる暗号化鍵を用いて記憶領域に記憶されているデータが暗号化され、第 1 の情報処理装置または第 2 の情報処理装置により記憶領域からのデータの読出しが要求された場合、記憶領域に記憶されているデータが最初に読出されるとき、暗号化されたデータが第 1 の情報処理装置または第 2 の情報処理装置に送信され、記憶領域に記憶されているデータが 2 回目以降に

読出されるとき、すでに暗号化されているデータを記憶領域から読出し、読出したデータが第１の情報処理装置または第２の情報処理装置に送信される。

【発明の効果】

【００２２】

本発明によれば、データを授受することができる。また、本発明によれば、より簡単にデータを安全に授受することができる。

【発明を実施するための最良の形態】

【００２３】

以下に本発明の実施の形態を説明するが、請求項に記載の構成要件と、発明の実施の形態における具体例との対応関係を例示すると、次のようになる。この記載は、請求項に記載されている発明をサポートする具体例が、発明の実施の形態に記載されていることを確認するためのものである。従って、発明の実施の形態中には記載されているが、構成要件に対応するものとして、ここには記載されていない具体例があったとしても、そのことは、その具体例が、その構成要件に対応するものではないことを意味するものではない。逆に、具体例が構成要件に対応するものとしてここに記載されていたとしても、そのことは、その具体例が、その構成要件以外の構成要件には対応しないものであることを意味するものでもない。

【００２４】

さらに、この記載は、発明の実施の形態に記載されている具体例に対応する発明が、請求項に全て記載されていることを意味するものではない。換言すれば、この記載は、発明の実施の形態に記載されている具体例に対応する発明であって、この出願の請求項には記載されていない発明の存在、すなわち、将来、分割出願されたり、補正により追加される発明の存在を否定するものではない。

【００２５】

請求項１に記載のデータ記憶装置（例えば、図１のＩＣカード１３）は、記憶領域（例えば、サービス領域）を有する記憶部（例えば、図７の記憶部２０７）を備えたデータ記憶装置であって、第１の情報処理装置（例えば、図１のリーダライタ１１）から送信されてくる、前記記憶領域からのデータの読出しを許可する第１の読出し鍵を登録する読出し鍵登録手段（例えば、図８のサービス生成部２３４）と、前記記憶領域に記憶されているデータが最初に読出されるまで、前記記憶領域への新たなデータの書込みを禁止するように前記記憶部へのデータの書込みを制御する書込み制御手段（例えば、図８の書込み制御部２３２）と、前記第１の情報処理装置または前記第１の情報処理装置とは異なる第２の情報処理装置（例えば、図１のリーダライタ１２）により前記記憶領域からのデータの読出しが要求された場合、前記第１の情報処理装置または前記第２の情報処理装置から送信されてくる第２の読出し鍵と前記第１の読出し鍵とが一致するとき、前記記憶領域からのデータの読出しを許可するように前記記憶部からのデータの読出しを制御する読出し制御手段（例えば、図８の読出し制御部２３３）とを含むことを特徴とする。

【００２６】

請求項２に記載のデータ記憶装置（例えば、図１のＩＣカード１３）は、前記書込み制御手段は、前記記憶領域に書込むデータとともに送信されてくる前記記憶領域に書込むデータを暗号化したデジタル署名（例えば、シグネチャー）をさらに前記記憶領域に書込むように前記記憶部へのデータの書込みを制御し、前記読出し制御手段は、前記第１の情報処理装置または前記第２の情報処理装置により前記第２の鍵が送信されずに前記記憶領域に記憶されているデータの内容の確認が要求された場合、前記記憶領域から前記デジタル署名を読出し、前記第１の情報処理装置または前記第２の情報処理装置に前記デジタル署名を送信するように前記記憶部からのデータの読出しを制御することを特徴とする。

【００２７】

請求項３に記載のデータ処理方法は、記憶領域（例えば、サービス領域）を有する記憶部（例えば、図７の記憶部２０７）を備えたデータ記憶装置（例えば、図１のＩＣカード１３）のデータ処理方法であって、第１の情報処理装置（例えば、図１のリーダライタ１１

10

20

30

40

50

）から送信されてくる、前記記憶領域からのデータの読出しを許可する第１の読出し鍵を登録する読出し鍵登録ステップ（例えば、図９のステップＳ１２）と、前記記憶領域に記憶されているデータが最初に読出されるまで、前記記憶領域への新たなデータの書込みを禁止するように前記記憶部へのデータの書込みを制御する書込み制御ステップ（例えば、図１１のステップＳ５３乃至Ｓ５５）と、前記第１の情報処理装置または前記第１の情報処理装置とは異なる第２の情報処理装置（例えば、図１のリーダライタ１２）により前記記憶領域からのデータの読出しが要求された場合、前記第１の情報処理装置または前記第２の情報処理装置から送信されてくる第２の読出し鍵と前記第１の読出し鍵とが一致するとき、前記記憶領域からのデータの読出しを許可するように前記記憶部からのデータの読出しを制御する読出し制御ステップ（例えば、図１３のステップＳ１１３およびＳ１１５）とを含むことを特徴とする。 10

【００２８】

請求項４に記載の記録媒体（例えば、図３の磁気ディスク５１、光ディスク５２、光磁気ディスク５３、もしくは、半導体メモリ５４、または、図５の磁気ディスク１５１、光ディスク１５２、光磁気ディスク１５３、もしくは、半導体メモリ１５４）に記録されているプログラムは、記憶領域（例えば、サービス領域）を有する記憶部（例えば、図７の記憶部２０７）を備えたデータ記憶装置（例えば、図１のＩＣカード１３）のデータ処理用のプログラムであって、第１の情報処理装置（例えば、図１のリーダライタ１１）から送信されてくる、前記記憶領域からのデータの読出しを許可する第１の読出し鍵を登録する読出し鍵登録ステップ（例えば、図９のステップＳ１２）と、前記記憶領域に記憶されているデータが最初に読出されるまで、前記記憶領域への新たなデータの書込みを禁止するように前記記憶部へのデータの書込みを制御する書込み制御ステップ（例えば、図１１のステップＳ５３乃至Ｓ５５）と、前記第１の情報処理装置または前記第１の情報処理装置とは異なる第２の情報処理装置（例えば、図１のリーダライタ１２）により前記記憶領域からのデータの読出しが要求された場合、前記第１の情報処理装置または前記第２の情報処理装置から送信されてくる第２の読出し鍵と前記第１の読出し鍵とが一致するとき、前記記憶領域からのデータの読出しを許可するように前記記憶部からのデータの読出しを制御する読出し制御ステップ（例えば、図１３のステップＳ１１３およびＳ１１５）とを含むことを特徴とする。 20

【００２９】

請求項５に記載のプログラムは、記憶領域（例えば、サービス領域）を有する記憶部（例えば、図７の記憶部２０７）を備えたデータ記憶装置（例えば、図１のＩＣカード１３）に、データ処理を行なわせるプログラムであって、第１の情報処理装置（例えば、図１のリーダライタ１１）から送信されてくる、前記記憶領域からのデータの読出しを許可する第１の読出し鍵を登録する読出し鍵登録ステップ（例えば、図９のステップＳ１２）と、前記記憶領域に記憶されているデータが最初に読出されるまで、前記記憶領域への新たなデータの書込みを禁止するように前記記憶部へのデータの書込みを制御する書込み制御ステップ（例えば、図１１のステップＳ５３乃至Ｓ５５）と、前記第１の情報処理装置または前記第１の情報処理装置とは異なる第２の情報処理装置（例えば、図１のリーダライタ１２）により前記記憶領域からのデータの読出しが要求された場合、前記第１の情報処理装置または前記第２の情報処理装置から送信されてくる第２の読出し鍵と前記第１の読出し鍵とが一致するとき、前記記憶領域からのデータの読出しを許可するように前記記憶部からのデータの読出しを制御する読出し制御ステップ（例えば、図１３のステップＳ１１３およびＳ１１５）とを含むことを特徴とする。 30 40

【００３０】

請求項６に記載のデータ記憶装置（例えば、図１のＩＣカード１３）は、記憶領域（例えば、サービス領域）を有する記憶部（例えば、図７の記憶部２０７）を備えたデータ記憶装置であって、第１の情報処理装置（例えば、図１のリーダライタ１１）から送信されてくる、前記記憶領域へのデータの書込みを許可する第１の書込み鍵を登録する書込み鍵登録手段（例えば、図８のサービス生成部２３４）と、前記第１の情報処理装置または前記 50

第 1 の情報処理装置とは異なる第 2 の情報処理装置（例えば、図 1 のリーダライタ 1 2 ）により前記記憶領域へのデータの書込みが要求された場合、前記第 1 の情報処理装置または前記第 2 の情報処理装置から送信されてくる第 2 の書込み鍵が前記第 1 の書込み鍵と一致するとき、前記記憶領域へのデータの書込みを許可するように前記記憶部へのデータの書込みを制御する書込み制御手段（例えば、図 8 の書込み制御部 2 3 2 ）と、前記第 1 の情報処理装置または前記第 2 の情報処理装置により前記記憶領域からのデータの読出しが要求された場合、前記記憶領域に記憶されているデータが最初に読出されるとき、前記第 1 の情報処理装置または前記第 2 の情報処理装置より送信されてくる暗号化鍵を用いて前記記憶領域に記憶されているデータを暗号化する暗号化手段（例えば、図 8 の暗号化部 2 3 5 ）と、前記第 1 の情報処理装置または前記第 2 の情報処理装置により前記記憶領域からのデータの読出しが要求された場合、前記記憶領域に記憶されているデータが最初に読出されるとき、前記暗号化手段により暗号化されたデータを前記第 1 の情報処理装置または前記第 2 の情報処理装置に送信し、前記記憶領域に記憶されているデータが 2 回目以降に読出されるとき、前記暗号化手段によりすでに暗号化されているデータを前記記憶領域から読出し、前記読出したデータを前記第 1 の情報処理装置または前記第 2 の情報処理装置に送信する送信制御手段（例えば、図 8 の読出し制御部 2 3 3 ）とを含むことを特徴とする。

10

【0031】

請求項 7 に記載のデータ処理方法は、記憶領域（例えば、サービス領域）を有する記憶部（例えば、図 7 の記憶部 2 0 7 ）を備えたデータ記憶装置（例えば、図 1 の IC カード 1 3 ）のデータ処理方法であって、第 1 の情報処理装置（例えば、図 1 のリーダライタ 1 1 ）から送信されてくる、前記記憶領域へのデータの書込みを許可する第 1 の書込み鍵を登録する書込み鍵登録ステップ（例えば、図 1 4 のステップ S 2 1 2 ）と、前記第 1 の情報処理装置または前記第 1 の情報処理装置とは異なる第 2 の情報処理装置（例えば、図 1 のリーダライタ 1 2 ）により前記記憶領域へのデータの書込みが要求された場合、前記第 1 の情報処理装置または前記第 2 の情報処理装置から送信されてくる第 2 の書込み鍵が前記第 1 の書込み鍵と一致するとき、前記記憶領域へのデータの書込みを許可するように前記記憶部へのデータの書込みを制御する書込み制御ステップ（例えば、図 1 6 のステップ S 2 5 3 および S 2 5 4 ）と、前記第 1 の情報処理装置または前記第 2 の情報処理装置により前記記憶領域からのデータの読出しが要求された場合、前記記憶領域に記憶されているデータが最初に読出されるとき、前記第 1 の情報処理装置または前記第 2 の情報処理装置より送信されてくる暗号化鍵を用いて前記記憶領域に記憶されているデータを暗号化する暗号化ステップ（例えば、図 1 7 のステップ S 2 8 4 ）と、前記第 1 の情報処理装置または前記第 2 の情報処理装置により前記記憶領域からのデータの読出しが要求された場合、前記記憶領域に記憶されているデータが最初に読出されるとき、前記暗号化ステップの処理により暗号化されたデータを前記第 1 の情報処理装置または前記第 2 の情報処理装置に送信し、前記記憶領域に記憶されているデータが 2 回目以降に読出されるとき、前記暗号化ステップの処理によりすでに暗号化されているデータを前記記憶領域から読出し、前記読出したデータを前記第 1 の情報処理装置または前記第 2 の情報処理装置に送信する送信制御ステップ（例えば、図 1 7 のステップ S 2 8 6 ）とを含むことを特徴とする。

20

30

40

【0032】

請求項 8 に記載の記録媒体（例えば、図 3 の磁気ディスク 5 1、光ディスク 5 2、光磁気ディスク 5 3、もしくは、半導体メモリ 5 4、または、図 5 の磁気ディスク 1 5 1、光ディスク 1 5 2、光磁気ディスク 1 5 3、もしくは、半導体メモリ 1 5 4）に記録されているプログラムは、記憶領域（例えば、サービス領域）を有する記憶部（例えば、図 7 の記憶部 2 0 7 ）を備えたデータ記憶装置（例えば、図 1 の IC カード 1 3 ）のデータ処理用のプログラムであって、第 1 の情報処理装置（例えば、図 1 のリーダライタ 1 1 ）から送信されてくる、前記記憶領域へのデータの書込みを許可する第 1 の書込み鍵を登録する書込み鍵登録ステップ（例えば、図 1 4 のステップ S 2 1 2 ）と、前記第 1 の情報処理装置または前記第 1 の情報処理装置とは異なる第 2 の情報処理装置（例えば、図 1 のリーダラ

50

イタ１２）により前記記憶領域へのデータの書込みが要求された場合、前記第１の情報処理装置または前記第２の情報処理装置から送信されてくる第２の書込み鍵が前記第１の書込み鍵と一致するとき、前記記憶領域へのデータの書込みを許可するように前記記憶部へのデータの書込みを制御する書込み制御ステップ（例えば、図１６のステップＳ２５３およびＳ２５４）と、前記第１の情報処理装置または前記第２の情報処理装置により前記記憶領域からのデータの読出しが要求された場合、前記記憶領域に記憶されているデータが最初に読出されるとき、前記第１の情報処理装置または前記第２の情報処理装置より送信されてくる暗号化鍵を用いて前記記憶領域に記憶されているデータを暗号化する暗号化ステップ（例えば、図１７のステップＳ２８４）と、前記第１の情報処理装置または前記第２の情報処理装置により前記記憶領域からのデータの読出しが要求された場合、前記記憶領域に記憶されているデータが最初に読出されるとき、前記暗号化ステップの処理により暗号化されたデータを前記第１の情報処理装置または前記第２の情報処理装置に送信し、前記記憶領域に記憶されているデータが２回目以降に読出されるとき、前記暗号化ステップの処理によりすでに暗号化されているデータを前記記憶領域から読出し、前記読出したデータを前記第１の情報処理装置または前記第２の情報処理装置に送信する送信制御ステップ（例えば、図１７のステップＳ２８６）とを含むことを特徴とする。

10

【００３３】

請求項９に記載のプログラムは、記憶領域（例えば、サービス領域）を有する記憶部（例えば、図７の記憶部２０７）を備えたデータ記憶装置（例えば、図１のＩＣカード１３）に、データ処理を行なわせるプログラムであって、第１の情報処理装置（例えば、図１のリーダライタ１１）から送信されてくる、前記記憶領域へのデータの書込みを許可する第１の書込み鍵を登録する書込み鍵登録ステップ（例えば、図１４のステップＳ２１２）と、前記第１の情報処理装置または前記第１の情報処理装置とは異なる第２の情報処理装置（例えば、図１のリーダライタ１２）により前記記憶領域へのデータの書込みが要求された場合、前記第１の情報処理装置または前記第２の情報処理装置から送信されてくる第２の書込み鍵が前記第１の書込み鍵と一致するとき、前記記憶領域へのデータの書込みを許可するように前記記憶部へのデータの書込みを制御する書込み制御ステップ（例えば、図１６のステップＳ２５３およびＳ２５４）と、前記第１の情報処理装置または前記第２の情報処理装置により前記記憶領域からのデータの読出しが要求された場合、前記記憶領域に記憶されているデータが最初に読出されるとき、前記第１の情報処理装置または前記第２の情報処理装置より送信されてくる暗号化鍵を用いて前記記憶領域に記憶されているデータを暗号化する暗号化ステップ（例えば、図１７のステップＳ２８４）と、前記第１の情報処理装置または前記第２の情報処理装置により前記記憶領域からのデータの読出しが要求された場合、前記記憶領域に記憶されているデータが最初に読出されるとき、前記暗号化ステップの処理により暗号化されたデータを前記第１の情報処理装置または前記第２の情報処理装置に送信し、前記記憶領域に記憶されているデータが２回目以降に読出されるとき、前記暗号化ステップの処理によりすでに暗号化されているデータを前記記憶領域から読出し、前記読出したデータを前記第１の情報処理装置または前記第２の情報処理装置に送信する送信制御ステップ（例えば、図１７のステップＳ２８６）とを含むことを特徴とする。

20

30

40

【００３４】

以下、図を参照して、本発明の実施の形態について説明する。

【００３５】

図１は、本発明を適用した非接触ＩＣカードシステム１の一実施の形態を示している。非接触ＩＣカードシステム１において、リーダライタ１１とＩＣカード１３、または、リーダライタ１２とＩＣカード１３は、電磁波を利用して非接触でデータの送受信を行なう。例えば、非接触ＩＣカードシステム１において、リーダライタ１１は、ＩＣカード１３を所有するＩＣカード所有者のものとされ、リーダライタ１２は、ＩＣカード１３を利用した各種サービスを提供するサービス提供者のものとされる。

【００３６】

50

図 2 は、リーダライタ 1 1 と IC カード 1 3 との間、または、リーダライタ 1 2 と IC カード 1 3 との間で送受信されるコマンドのフォーマットの例を示す図である。

【 0 0 3 7 】

コマンドは、CMD フィールド、LEN フィールド、データフィールド、データシグネチャフィールド、および、CRC フィールドにより構成される。

【 0 0 3 8 】

CMD フィールドには、リーダライタ 1 1 と IC カード 1 3 との間、または、リーダライタ 1 1 と IC カード 1 3 との間、または、リーダライタ 1 2 と IC カード 1 3 との間において、各種の処理を指示したり、各種の情報を伝達したりするためのコードであるコマンドコードが設定される。

10

【 0 0 3 9 】

LEN フィールドには、データフィールドから CRC フィールドまでのデータ長（例えば、バイト数）が設定される。

【 0 0 4 0 】

データフィールドには、リーダライタ 1 1 と IC カード 1 3 との間、または、リーダライタ 1 2 と IC カード 1 3 との間で授受される各種のデータが格納される。

【 0 0 4 1 】

データシグネチャフィールドには、必要に応じて、データフィールドに格納されているデータを暗号化したデジタル署名であるシグネチャが格納される。シグネチャは、例えば、不可逆な一方向関数を含む MD5 (Message Digest 5) などのハッシュ関数を用いて、データフィールドに格納されているデータから生成されたハッシュ値とされる。

20

【 0 0 4 2 】

CRC フィールドには、データ伝送の誤り検出の一方式である CRC (Cyclical (Cyclic) Redundancy Check) 方式における CRC コードが設定される。

【 0 0 4 3 】

なお、図 2 のコマンドに、リーダライタ 1 1 または 1 2 を識別するための装置 ID、IC カード 1 3 を識別するためのカード ID などのコマンドの送受信に必要な情報が付加され、コマンドが送受信される。

【 0 0 4 4 】

図 3 は、リーダライタ 1 1 の機能の構成例を示すブロック図である。リーダライタ 1 1 は、制御部 3 1、記録部 3 2、SPU (Signal Processing Unit) 3 3、変調部 3 4、発振回路 3 5、アンテナ 3 6、復調部 3 7、およびドライブ 3 8 を含むように構成される。

30

【 0 0 4 5 】

制御部 3 1 は、必要に応じて装着される、ドライブ 3 8 から供給されるプログラムを読み込み、読み込んだプログラムを実行し、リーダライタ 1 1 全体を制御する。また、制御部 3 1 は、ドライブ 3 8 からプログラムやデータが供給された場合、供給されたプログラムやデータを必要に応じて記録部 3 2 に記録させる。そして、制御部 3 1 は、記録部 3 2 に記録されたプログラムを読み込み、読み込んだプログラムを実行し、リーダライタ 1 1 全体を制御する。

【 0 0 4 6 】

制御部 3 1 は、IC カード 1 3 に所定の処理を実行させるコマンドを生成し、生成したコマンドを SPU 3 3 に供給する。また、制御部 3 1 は、IC カード 1 3 から送信され、SPU 3 3 から供給されるコマンドに対応した処理を実行する。また、制御部 3 1 は、図示せぬ操作部を用いてユーザにより入力された指令に対応した処理を実行する。

40

【 0 0 4 7 】

記録部 3 2 は、書き換え可能で、電源が遮断されても記録内容を保持できる、いわゆる不揮発性の記憶媒体または記録媒体からなり、例えば、ハードディスクまたはフラッシュメモリなどにより構成される。記録部 3 2 は、制御部 3 1 が使用するプログラムやデータを記録する。

【 0 0 4 8 】

50

SPU33は、制御部31から供給されたコマンドを、所定の方式により符号化し、符号化したコマンドを変調部34に供給する。また、SPU33は、復調部37から供給されたデータを、データの符号化方式に対応する方式により復号し、復号したデータを制御部31に供給する。

【0049】

例えば、SPU33は、ICカード13あてに送信するコマンドが、制御部31から供給されてきた場合、そのコマンドに、マンチェスタコードへのコーディングなどの符号化処理を施し、これにより得られた信号を変調部34に出力する。また、例えば、SPU33は、ICカード13からのデータが復調部37から供給されてきた場合、そのデータに対して、マンチェスタコードのデコードなどの復号処理を施し、これにより得られた信号を、

10

【0050】

変調部34は、発振回路35から供給された所定の周波数のクロック信号を基に、搬送波を生成する。変調部34は、搬送波に基づいて、SPU33から供給されたコマンドを所定の方式により変調することにより変調したコマンドを生成し、変調したコマンドをアンテナ36に供給する。例えば、変調部34は、SPU33から供給されたコマンドに基づいて、搬送波の位相、振幅、周波数などを変化させることにより変調したコマンドを生成する。

【0051】

より具体的には、例えば、変調部34は、発振回路35から供給される13.56MHzの周波数のクロック信号を搬送波として、SPU33より供給されるデータをASK (Amplitude Shift Keying) 変調し、生成された変調波を、電磁波としてアンテナ36から出力させる。

20

【0052】

発振回路35は、所定の周波数の、基準となるクロック信号を生成し、生成したクロック信号を変調部34に供給する。

【0053】

アンテナ36は、変調部34から供給されたコマンドを、無線通信によりICカード13あてに送信する。すなわち、例えば、アンテナ36は、変調部34から供給されたコマンドを伝送するための電波を輻射（放射）する。また、アンテナ36は、ICカード13から

30

【0054】

復調部37は、アンテナ36から供給されたデータを、ICカード13の変調部209（図7）の変調方式に対応する復調方式により復調し、復調したデータをSPU33に供給する。例えば、復調部37は、アンテナ36を介して取得した変調波（ASK変調波）を復調し、復調したデータをSPU33に出力する。

【0055】

ドライブ38は、磁気ディスク51、光ディスク52、光磁気ディスク53、または半導体メモリ54などが装着されたとき、それらを駆動し、そこに記録されているプログラムやデータなどを取得する。取得されたプログラムやデータは、制御部31またはICカード13に転送される。また、ICカード13に転送（送信）されたプログラムは、ICカード13により、必要に応じて記録されるか、または実行される。

40

【0056】

図4は、所定のプログラムを実行する制御部31により実現される機能の構成例を示すブロック図である。制御部31がプログラムを実行することにより、通信制御部71、書込み制御部72、読出し制御部73、サービス生成要求部74、暗号化部75、および、復号部76が実現される。

【0057】

通信制御部71は、SPU33、変調部34、および、アンテナ36を介して、ポーリングコマンドを送信し、ポーリングコマンドに対するポーリング応答コマンドがICカード1

50

3 から送信されてきた場合、アンテナ 3 6、復調部 3 7、および、SPU 3 3 を介してポーリング応答コマンドを受信する。通信制御部 7 1 は、ICカード 1 3 からポーリング応答コマンドを受信した場合、SPU 3 3、変調部 3 4 または復調部 3 7、および、アンテナ 3 6 を介して、ICカード 1 3 と相互認証などのセッション確立処理を行ない、リーダライタ 1 1 と ICカード 1 3 との間の通信セッションを確立する。

【0058】

通信制御部 7 1 は、ICカード 1 3 から送信されてくる各種のコマンドを、アンテナ 3 6、復調部 3 7、および、SPU 3 3 を介して受信し、LENフィールドに設定された値に基づいて受信したコマンドのデータ長を確認したり、CRCコードに基づいて、コマンドのデータのエラー検出を行なう。通信制御部 7 1 は、必要に応じて、書込み制御部 7 2、読出し制御部 7 3、または、サービス生成要求部 7 4 に受信したコマンドを供給する。また、通信制御部 7 1 は、書込み制御部 7 2、読出し制御部 7 3、または、サービス生成要求部 7 4 から供給される各種のコマンドに、コマンドの送信に必要な情報を付加し、情報を付加したコマンドを、SPU 3 3、変調部 3 4、および、アンテナ 3 6 を介して ICカード 1 3 に送信する。

10

【0059】

書込み制御部 7 2 は、図 1 6 を参照して後述するように、ICカード 1 3 へのデータの書込みを要求する書込みコマンドを生成し、生成した書込みコマンドを通信制御部 7 1 に供給する。書込み制御部 7 2 は、書込みコマンドに対する ICカード 1 3 からの応答である書込み終了通知コマンドを、通信制御部 7 1 から取得する。

20

【0060】

読出し制御部 7 3 は、図 1 3 を参照して後述するように、ICカード 1 3 からのデータの読出しを要求する読出しコマンドを生成し、生成した読出しコマンドを通信制御部 7 1 に供給する。読出し制御部 7 3 は、読出しコマンドに対する ICカード 1 3 からの応答である読出し応答コマンドを、通信制御部 7 1 から取得する。読出し制御部 7 3 は、読出し応答コマンドに格納されている、ICカード 1 3 から読出したデータを、必要に応じて、リーダライタ 1 1 の各部に供給したり、記録部 3 2 に記録させたりする。

【0061】

サービス生成要求部 7 4 は、ICカード 1 3 への各種のサービスの生成を要求するサービス生成要求コマンドを生成し、生成したサービス生成要求コマンドを通信制御部 7 1 に供給する。例えば、サービス生成要求部 7 4 は、図 9 乃至図 1 3 を参照して後述するライトワンスサービスや、図 1 4 乃至図 1 7 を参照して後述するリードワンスサービスを ICカード 1 3 に生成させる。サービス生成要求部 7 4 は、サービス生成要求コマンドに対する ICカード 1 3 からの応答であるサービス生成通知コマンドを、通信制御部 7 1 から取得する。

30

【0062】

暗号化部 7 5 は、各種データの暗号化を行なう。例えば、暗号化部 7 5 は、通信制御部 7 1、書込み制御部 7 2、読出し制御部 7 3、または、サービス生成要求部 7 4 から供給されたデータを暗号化し、暗号化したデータをデータの供給元に返す。

【0063】

復号部 7 6 は、各種データの復号を行なう。例えば、復号部 7 6 は、通信制御部 7 1、書込み制御部 7 2、読出し制御部 7 3、または、サービス生成要求部 7 4 から供給されたデータを復号し、復号したデータをデータの供給元に返す。

40

【0064】

図 5 は、リーダライタ 1 2 の機能の構成例を示すブロック図である。リーダライタ 1 2 は、制御部 1 3 1、記録部 1 3 2、SPU 1 3 3、変調部 1 3 4、発振回路 1 3 5、アンテナ 1 3 6、復調部 1 3 7、およびドライブ 1 3 8 を含むように構成される。なお、図中、図 3 と対応する部分については下 2 桁が同じ符号を付してあり、処理が同じ部分に関しては、その説明は繰り返しになるので省略する。

【0065】

50

制御部 131 は、必要に応じて装着される、ドライブ 138 から供給されるプログラムを読み込み、読み込んだプログラムを実行し、リーダーライタ 12 全体を制御する。また、制御部 131 は、ドライブ 138 からプログラムやデータが供給された場合、供給されたプログラムやデータを必要に応じて記録部 132 に記録させる。そして、制御部 131 は、記録部 132 に記録されたプログラムを読み込み、読み込んだプログラムを実行し、リーダーライタ 12 全体を制御する。

【0066】

制御部 131 は、ICカード 13 に所定の処理を実行させるコマンドを生成し、生成したコマンドを SPU 133 に供給する。また、制御部 131 は、ICカード 13 から送信され、SPU 133 から供給されるコマンドに対応した処理を実行する。また、制御部 131 は、図 10 示せぬ操作部などを用いてユーザにより入力された指令に対応した処理を実行する。

【0067】

図 6 は、所定のプログラムを実行する制御部 131 により実現される機能の構成例を示すブロック図である。制御部 131 がプログラムを実行することにより、通信制御部 171、書込み制御部 172、読出し制御部 173、暗号化部 174、および、復号部 175 が実現される。

【0068】

通信制御部 171 は、SPU 133、変調部 134、および、アンテナ 136 を介して、ポーリングコマンドを送信し、ポーリングコマンドに対するポーリング応答コマンドが ICカード 13 から送信されてきた場合、アンテナ 136、復調部 137、および、SPU 133 を介してポーリング応答コマンドを受信する。通信制御部 171 は、ICカード 13 からポーリング応答コマンドを受信した場合、SPU 133、変調部 134 または復調部 137、および、アンテナ 136 を介して、ICカード 13 と相互認証などのセッション確立処理を行ない、リーダーライタ 12 と ICカード 13 との間の通信セッションを確立する。

【0069】

通信制御部 171 は、ICカード 13 から送信されてくる各種のコマンドを、アンテナ 136、復調部 137、および、SPU 133 を介して受信し、LENフィールドに設定された値に基づいて受信したコマンドのデータ長を確認したり、CRCコードに基づいて、コマンドのデータのエラー検出を行なう。通信制御部 171 は、必要に応じて、書込み制御部 172、または、読出し制御部 173 に受信したコマンドを供給する。また、通信制御部 171 は、書込み制御部 172、または、読出し制御部 173 から供給される各種のコマンドに、コマンドの送信に必要な情報を付加し、情報を付加したコマンドを、SPU 133、変調部 134、および、アンテナ 136 を介して ICカード 13 に送信する。

【0070】

書込み制御部 172 は、図 11 を参照して後述するように、ICカード 13 へのデータの書込みを要求する書込みコマンドを生成し、生成した書込みコマンドを通信制御部 171 に供給する。書込み制御部 172 は、書込みコマンドに対する ICカード 13 からの応答である書込み終了通知コマンドを、通信制御部 171 から取得する。

【0071】

また、書込み制御部 172 は、図 12 を参照して後述するように、ICカード 13 に書込んだデータの内容の確認を要求するデータ確認コマンドを生成し、生成したデータ確認コマンドを通信制御部 171 に供給する。書込み制御部 172 は、データ確認コマンドに対する ICカード 13 からの応答であるデータ確認応答コマンドを、通信制御部 171 から取得する。

【0072】

読出し制御部 173 は、図 12 を参照して後述するように、ICカード 13 からのデータの読出しを要求する読出しコマンドを生成し、生成した読出しコマンドを通信制御部 171 に供給する。読出し制御部 173 は、読出しコマンドに対する ICカード 13 からの応答である読出し応答コマンドを、通信制御部 171 から取得する。読出し制御部 173 は、読出し応答コマンドに格納されている、ICカード 13 から読出したデータを、必要に応じ

て、リーダライタ 1 2 の各部に供給したり、記録部 1 3 2 に記録させたりする。

【 0 0 7 3 】

暗号化部 1 7 4 は、各種データの暗号化を行なう。例えば、暗号化部 1 7 4 は、通信制御部 1 7 1、書込み制御部 1 7 2、または、読出し制御部 1 7 3 供給されたデータを暗号化し、暗号化したデータをデータの供給元に返す。

【 0 0 7 4 】

復号部 1 7 5 は、各種データの復号を行なう。例えば、復号部 1 7 5 は、通信制御部 1 7 1、書込み制御部 1 7 2、または、読出し制御部 1 7 3 から供給されたデータを復号し、復号したデータをデータの供給元に返す。

【 0 0 7 5 】

図 7 は、ICカード 1 3 の機能の構成例を示すブロック図である。ICカード 1 3 は、アンテナ 2 0 1、復調部 2 0 2、S P U 2 0 3、制御部 2 0 4、ROM (Read Only Memory) 2 0 5、RAM (Random Access Memory) 2 0 6、記憶部 2 0 7、発振回路 2 0 8、変調部 2 0 9、および電力発生部 2 1 0 を含むように構成される。

【 0 0 7 6 】

アンテナ 2 0 1 は、リーダライタ 1 1 または 1 2 から送信されてきたコマンドを受信し、受信したコマンドを復調部 2 0 2 に供給する。また、アンテナ 2 0 1 は、変調部 2 0 9 から供給されたデータ (例えば、コマンド) を、無線通信により、リーダライタ 1 1 または 1 2 あてに送信する。すなわち、例えば、アンテナ 2 0 1 は、変調部 2 0 9 から供給されたデータを伝送するための電波を放射する。また、アンテナ 2 0 1 においては、リーダライタ 1 1 または 1 2 から放射される所定の周波数の電波により、共振が生じ、起電力が発生する。

【 0 0 7 7 】

復調部 2 0 2 は、アンテナ 2 0 1 から供給されたコマンドを、リーダライタ 1 1 の変調部 3 4 またはリーダライタ 1 2 の変調部 1 3 4 の変調方式に対応する復調方式により復調し、復調したコマンドを S P U 2 0 3 に供給する。例えば、復調部 2 0 2 は、アンテナ 2 0 1 を介して受信した ASK 変調波であるコマンドを包絡線検波して復調し、復調したコマンドを S P U 2 0 3 に出力する。

【 0 0 7 8 】

S P U 2 0 3 は、復調部 2 0 2 から供給されたコマンドを所定の方式により復号し、復号したコマンドを制御部 2 0 4 に供給する。S P U 2 0 3 は、制御部 2 0 4 から供給されたデータを、所定の符号化方式により符号化し、符号化したデータを変調部 2 0 9 に供給する。例えば、S P U 2 0 3 は、復調部 2 0 2 において復調されたコマンドがマンチェスタ方式で符号化されている場合、図示せぬ PLL (Phase Locked Loop) 回路から供給されるクロック信号に基づいて、そのコマンドの復号 (マンチェスタコードのデコード) を行い、復号したコマンドを制御部 2 0 4 に供給する。例えば、S P U 2 0 3 は、制御部 2 0 4 から供給されたデータを、マンチェスタ方式で符号化し、符号化したデータを変調部 2 0 9 に供給する。

【 0 0 7 9 】

制御部 2 0 4 は、必要に応じて、ROM 2 0 5 または記憶部 2 0 7 に記憶または記録されているプログラムを読み込み、読み込んだプログラムを実行し、ICカード 1 3 全体を制御する。また、制御部 2 0 4 は、S P U 2 0 3 から供給された各種のコマンドに対応する処理を実行する。さらに、制御部 2 0 4 は、リーダライタ 1 1 または 1 2 から送信されてきたコマンドに応答するコマンドを生成し、S P U 2 0 3 に供給する。

【 0 0 8 0 】

ROM 2 0 5 は、制御部 2 0 4 が各種の処理を行うためのプログラム、その他のデータなどを記録している。

【 0 0 8 1 】

RAM 2 0 6 は、制御部 2 0 4 が各種の処理を行うとき、その処理の途中のデータなどを一時的に記憶する。

10

20

30

40

50

【0082】

記憶部207は、例えば、フラッシュメモリ、EEPROM(Electrically Erasable Programmable Read Only Memory)、MRAM(Magnetoresistive Random Access Memory(磁気抵抗メモリ))、またはFeRAM(強誘電体メモリ)などの不揮発性メモリなどにより構成され、リーダライタ11または12により書込みが指示されたデータや、制御部204が各種の処理を行うためのプログラム、その他のデータなどを記憶する。

【0083】

発振回路208は、アンテナ201が受信するコマンドの周波数と同じ周波数のクロック信号を生成し、生成したクロック信号を変調部209に供給する。例えば、発振回路208は、PLL回路を内蔵し、コマンドのクロック周波数と同一の周波数のクロック信号を発生する。 10

【0084】

変調部209は、発振回路208から供給された所定の周波数のクロック信号を基に、搬送波を生成する。変調部209は、搬送波に基づいて、SPU203から供給されたデータを、所定の方式によって変調することにより、変調したデータを生成し、変調したデータをアンテナ201に供給する。例えば、変調部209は、SPU203から供給された、マンチェスタ方式により符号化されたデータを、さらにASK変調し、変調したデータを、アンテナ201を介して、リーダライタ11または12に送信する。

【0085】

また、例えば、変調部209は、SPU203から供給されるデータに対して、所定のスイッチング素子(図示せず)をオン、オフさせ、スイッチング素子がオン状態であるときだけ、所定の負荷をアンテナ201に並列に接続させることにより、アンテナ201の負荷を変動させる。ASK変調されたデータは、アンテナ201の負荷の変動により、アンテナ201を介して、リーダライタ11または12に送信される(リーダライタ11のアンテナ36またはリーダライタ12のアンテナ136の端子電圧を変動させる)。 20

【0086】

電力発生部210は、アンテナ201に生じた交流の起電力を基に、直流電力を発生させ、発生させた直流電力をICカード13の各部に供給する。

【0087】

図8は、所定のプログラムを実行する制御部204により実現される機能の構成例を示すブロック図である。制御部204がプログラムを実行することにより、通信制御部231、書込み制御部232、読出し制御部233、サービス生成部234、暗号化部235、および、復号部236が実現される。 30

【0088】

通信制御部231は、アンテナ201、復調部202、およびSPU203を介して、リーダライタ11または12からポーリングコマンドを受信し、ポーリング応答コマンドを、SPU203、変調部209、およびアンテナ201を介してリーダライタ11または12に送信する。通信制御部231は、SPU203、変調部209または復調部202、および、アンテナ201を介して、リーダライタ11または12と相互認証などのセッション確立処理を行ない、リーダライタ11または12とICカード13との間の通信セッションを確立する。 40

【0089】

通信制御部231は、リーダライタ11または12から送信されてくる各種のコマンドを、アンテナ201、復調部202、およびSPU203を介して受信し、LENフィールドに設定された値に基づいて受信したコマンドのデータ長を確認したり、CRCコードに基づいて、コマンドのデータのエラー検出を行なう。通信制御部231は、必要に応じて、書込み制御部232、読出し制御部233、または、サービス生成部234に受信したコマンドを供給する。また、通信制御部231は、書込み制御部232、読出し制御部233、または、サービス生成部234から供給される各種のコマンドに、コマンドの送信に必要な情報を付加し、情報を付加したコマンドを、SPU203、変調部209、および、アン 50

テナ 2 0 1 を介してリーダライタ 1 1 または 1 2 に送信する。

【 0 0 9 0 】

書込み制御部 2 3 2 は、図 1 1 または図 1 6 を参照して後述するように、リーダライタ 1 1 または 1 2 から送信された書込みコマンドを通信制御部 2 3 1 から取得し、書込みコマンドに格納されているデータを記憶部 2 0 7 に書込む。また、書込み制御部 2 3 2 は、書込みコマンドに対する応答である書込み終了通知コマンドを生成し、生成した書込み終了通知コマンドを通信制御部 2 3 1 に供給する。

【 0 0 9 1 】

読出し制御部 2 3 3 は、図 1 3 または図 1 7 を参照して後述するように、リーダライタ 1 1 または 1 2 から送信された読出しコマンドを通信制御部 2 3 1 から取得する。読出し制御部 2 3 3 は、読出しコマンドに基づいて、記憶部 2 0 7 からデータを読出し、読出したデータを格納した読出し応答コマンドを生成し、生成した読出し応答コマンドを通信制御部 2 3 1 に供給する。 10

【 0 0 9 2 】

また、読出し制御部 2 3 3 は、図 1 2 を参照して後述するように、リーダライタ 1 1 または 1 2 から送信されたデータ確認コマンドを通信制御部 2 3 1 から取得する。読出し制御部 2 3 3 は、データ確認コマンドに基づいて、確認が要求されたデータとともに記憶されているデータのシグネチャーを記憶部 2 0 7 から読出し、読出したシグネチャーを格納したデータ確認応答コマンドを生成する。読出し制御部 2 3 3 は、生成したデータ確認応答コマンドを通信制御部 2 3 1 に供給する。 20

【 0 0 9 3 】

サービス生成部 2 3 4 は、リーダライタ 1 1 または 1 2 から送信されたサービス生成要求コマンドを通信制御部 2 3 1 から取得し、サービス生成要求コマンドに基づいて、記憶部 2 0 7 に各種のサービスを生成する。例えば、サービス生成部 2 3 4 は、図 9 を参照して後述するように、ライトワンスサービスを生成したり、図 1 4 を参照して後述するように、リードワンスサービスを生成したりする。サービス生成部 2 3 4 は、サービス生成要求通知に対する応答であるサービス生成通知コマンドを生成し、生成したサービス生成通知コマンドを通信制御部 2 3 1 に供給する。

【 0 0 9 4 】

暗号化部 2 3 5 は、各種データの暗号化を行なう。例えば、暗号化部 2 3 5 は、通信制御部 2 3 1、書込み制御部 2 3 2、または読出し制御部 2 3 3 から供給されたデータを暗号化し、暗号化したデータをデータの供給元に返す。 30

【 0 0 9 5 】

復号部 2 3 6 は、各種データの復号を行なう。例えば、復号部 2 3 6 は、通信制御部 2 3 1、書込み制御部 2 3 2、または読出し制御部 2 3 3 から供給されたデータを復号し、復号したデータをデータの供給元に返す。

【 0 0 9 6 】

次に、図 9 乃至図 1 3 を参照して、ライトワンスサービスを利用した IC カードシステム 1 の処理を説明する。

【 0 0 9 7 】

まず、図 9 のフローチャートを参照して、IC カードシステム 1 におけるライトワンスサービス生成処理を説明する。 40

【 0 0 9 8 】

最初に、ライトワンスサービス生成処理において、リーダライタ 1 1 により実行されるライトワンスサービス生成要求処理を説明する。

【 0 0 9 9 】

ステップ S 1 において、リーダライタ 1 1 の通信制御部 7 1 は、ポーリングコマンドを送信する。具体的には、通信制御部 7 1 は、所定の間隔ごとに、ポーリングすることを示すコマンドコードを CMD フィールドに設定したポーリングコマンドを生成し、生成したポーリングコマンドを、SPU 3 3、変調部 3 4、およびアンテナ 3 6 を介して送信する。 50

【0100】

ICカード13が、リーダライタ11に近接され、リーダライタ11から送信されたポーリングコマンドを受信した場合、ICカード13は、後述するステップS11において、ポーリングコマンドに対する応答であるポーリング応答コマンドを送信する。

【0101】

通信制御部71は、ICカード13から送信されたポーリング応答コマンドを、アンテナ36、復調部37およびSPU33を介して受信し、ICカード13との間で、相互認証などのセッション確立処理を行ない、リーダライタ11とICカード13との間で通信セッションが確立された後、処理はステップS2に進む。

【0102】

ステップS2において、サービス生成要求部74は、ICカード13に、ライトワンスサービスの生成を要求する。具体的には、サービス生成要求部74は、ライトワンスサービスの生成を要求するコマンドコードをCMDフィールドに設定し、ライトワンスサービス内に確保する領域（以下、サービス領域と称する）の数、サービス領域の番号（以下、サービス領域番号と称する）、サービス領域のサイズ、サービス領域からのデータの読出しを許可する読出し鍵など、ライトワンスサービスを生成するために必要なデータをデータフィールドに格納したサービス生成要求コマンドを生成する。サービス生成要求部74は、生成したサービス生成要求コマンドを、通信制御部71、SPU33、変調部34、およびアンテナ36を介してICカード13に送信する。

【0103】

ICカード13は、後述するステップS12において、サービス生成要求コマンドを受信し、ライトワンスサービスを生成した後、ステップS13において、サービス生成要求コマンドに対する応答であるサービス生成通知コマンドを送信する。

【0104】

ステップS3において、サービス生成要求部74は、ICカード13より送信されたサービス生成通知コマンドを、アンテナ36、復調部37、SPU33、および、通信制御部71を介して受信し、ライトワンスサービス生成要求処理は終了する。

【0105】

次に、リーダライタ11によるライトワンスサービス生成要求処理に対応して、ICカード13により実行されるライトワンスサービス生成処理を説明する。

【0106】

ステップS11において、ICカード13の通信制御部231は、ポーリングコマンドに応答する。具体的には、通信制御部231は、上述したステップS1において、リーダライタ11より送信されたポーリングコマンドを、アンテナ201、復調部202、およびSPU203を介して受信する。通信制御部231は、ポーリングに応答することを示すコマンドコードをCMDフィールドに設定し、データフィールドにICカード13のカードIDなどをデータフィールドに格納したポーリング応答コマンドを生成し、生成したポーリング応答コマンドを、SPU203、変調部209、およびアンテナ201を介してリーダライタ11に送信する。

【0107】

その後、通信制御部231は、リーダライタ11との間で、相互認証などのセッション確立処理を行ない、リーダライタ11とICカード13との間で通信セッションが確立された後、処理はステップS12に進む。

【0108】

ステップS12において、サービス生成部234は、ライトワンスサービスを生成する。具体的には、サービス生成部234は、上述したステップS2において、リーダライタ11より送信されたサービス生成要求コマンドを、アンテナ201、復調部202、SPU203、および通信制御部231を介して受信する。サービス生成部234は、サービス生成要求コマンドにより指示されたサイズのサービス領域を、サービス生成要求コマンドにより指示された数だけ記憶部207に確保し、サービス生成要求コマンドにより指示さ

10

20

30

40

50

れるサービス領域番号を各サービス領域に設定する（サービス領域の所定の位置に記憶させる）。

【0109】

サービス生成部234は、サービス生成要求コマンドのデータフィールドに格納されている、サービス領域からのデータの読出しを許可する読出し鍵を登録する（サービス領域の所定の位置に記憶させる）。また、サービス生成部234は、サービス領域へのデータの書込みの可否を示す書込みフラグを記憶する領域をサービス領域の所定の位置に確保し、書込みフラグの値を、データの書込みを許可するオフに設定する。

【0110】

これにより、ライトワンスサービスの各サービス領域の状態は、図10に示される状態301となる。すなわち、書込みフラグがオフされ、サービス領域へのデータの書込みが可能とされ、かつ、サービス領域にデータが書込まれていない状態となる。

10

【0111】

なお、サービス領域ごとにそれぞれ異なる読出し鍵を登録するようにしてもよいし、同じ読出し鍵を登録するようにしてもよい。サービス領域ごとに異なる読出し鍵を登録する場合、サービス生成要求コマンドのデータフィールドに全ての読出し鍵を格納するようにしてもよいし、1つ以上の読出し鍵から計算などにより複数の読出し鍵を生成するようにしてもよい。また、予め別の処理によりライトワンスサービスのサービス領域を記憶部207に登録（確保）しておいて、登録されているサービス領域にリーダライタ11により読出し鍵を登録するようにしてもよい。

20

【0112】

ステップS13において、サービス生成部234は、サービス生成通知コマンドをリーダライタ11に送信して、ライトワンスサービス生成処理は終了する。具体的には、サービス生成部234は、サービスの生成の終了を通知するコマンドコードをCMDフィールドに設定し、ライトワンスサービスの生成結果（例えば、サービスの生成が成功したか失敗したかなど）を示すデータをデータフィールドに格納したサービス生成通知コマンドを生成する。サービス生成部234は、生成したサービス生成通知コマンドを、通信制御部231、SPU203、変調部209、およびアンテナ201を介して、リーダライタ11に送信する。

【0113】

その後、例えば、リーダライタ11を用いてライトワンスサービスをICカード13に生成したユーザは、ライトワンスサービスのサービス領域へのデータの書込みを依頼する相手（リーダライタ12の所有者）に、ICカード13を送付するとともに、データの書込みを依頼するサービス領域のサービス領域番号を通知する。なお、このサービス領域番号は、後述するように、第三者に知られても安全であり、各種のセキュリティ対策を施して秘密裏に送信する必要があるため、管理が容易である。

30

【0114】

次に、図11のフローチャートを参照して、リーダライタ12およびICカード13との間で行なわれるライトワンスサービスへのデータ書込み処理を説明する。

【0115】

最初に、リーダライタ12により実行されるデータ書込み要求処理を説明する。

40

【0116】

ステップS41において、リーダライタ12の通信制御部171は、ポーリングコマンドを送信する。具体的には、通信制御部171は、所定の間隔ごとに、ポーリングすることを示すコマンドコードをCMDフィールドに設定したポーリングコマンドを生成し、生成したポーリングコマンドを、SPU133、変調部134、およびアンテナ136を介して送信する。

【0117】

ICカード13が、リーダライタ12に近接され、リーダライタ12から送信されたポーリングコマンドを受信した場合、ICカード13は、後述するステップS51において、ポ

50

ーリングコマンドに対する応答であるポーリング応答コマンドを送信する。

【0118】

通信制御部171は、ICカード13から送信されたポーリング応答コマンドを、アンテナ136、復調部137およびSPU133を介して受信し、ICカード13との間で、相互認証などのセッション確立処理を行ない、リーダライタ12とICカード13との間で通信セッションが確立された後、処理はステップS42に進む。

【0119】

ステップS42において、書込み制御部172は、ICカード13にデータの書込みを要求する。具体的には、書込み制御部172は、データの書込みを要求するコマンドコードをCMDフィールドに設定し、データを書込むライトワンスサービスのサービス領域のサービス領域番号、および、サービス領域に書込むデータをデータフィールドに格納し、サービス領域に書込むデータのデジタル署名であるシグネチャーをシグネチャーフィールドに格納した書込みコマンドを生成する。書込み制御部172は、生成した書込みコマンドを、通信制御部171、SPU133、変調部134、およびアンテナ136を介してICカード13に送信する。

10

【0120】

なお、以下、ICカード13の記憶部207のサービス領域に書込むデータを特に他のデータと区別する場合、記録データとも称する。

【0121】

ICカード13は、後述するステップS52において、リーダライタ12から送信された書込みコマンドを受信し、書込みコマンドに基づいて、書込みが指示されたサービス領域にデータを書込み、ステップS56において、データの書込みが終了したことを通知する書込み終了通知コマンドを送信する。

20

【0122】

ステップS43において、書込み制御部172は、ICカード13から送信された書込み終了通知コマンドを、アンテナ136、復調部137、SPU133、および通信制御部171を介して受信し、データ書込み要求処理は終了する。

【0123】

次に、リーダライタ12によるデータ書込み要求処理に対応して、ICカード13により実行されるデータ書込み処理を説明する。

30

【0124】

ステップS51において、上述した図9のステップS11の処理と同様に、ICカード13の通信制御部231は、上述したステップS41において、リーダライタ12から送信されたポーリングコマンドに応答する。

【0125】

その後、リーダライタ12とICカード13の間でセッション確立処理が実行され、リーダライタ12およびICカード13の間の通信セッションが確立された後、処理はステップS52に進む。

【0126】

ステップS52において、書込み制御部232は、上述したステップS42において、リーダライタ12より送信された書込みコマンドを、アンテナ201、復調部202、SPU203、および通信制御部231を介して受信する。

40

【0127】

ステップS53において、書込み制御部232は、書込みコマンドによりデータを書込むように指示されたライトワンスサービスのサービス領域の書込みフラグがオフであるかを判定する。書込みフラグがオフであると判定された場合、すなわち、書込みコマンドによりデータの書込みが指示されたサービス領域の状態が図10の状態301または303である場合、処理はステップS54に進む。

【0128】

ステップS54において、書込み制御部232は、記憶部207にデータを書込む。具

50

体的には、書込み制御部 2 3 2 は、書込みコマンドのデータフィールドに格納されている記録データ、および、シグネチャーフィールドに格納されている記録データのシグネチャーを、書込みコマンドにより指示されたサービス領域に書込む。

【0 1 2 9】

ステップ S 5 5 において、書込み制御部 2 3 2 は、データを書込んだサービス領域の書込みフラグをオンにする。これにより、データが書込まれたサービス領域の状態は、上述した図 1 0 の状態 3 0 1 または後述する状態 3 0 3 から状態 3 0 2 に遷移する。すなわち、書込みフラグがオンされ、サービス領域へのデータの書込みが禁止され、かつ、サービス領域にデータが書込まれている状態となる。

【0 1 3 0】

図 1 3 を参照して後述するように、リーダライタ 1 1 により、記録データが読出されるまで、データが書込まれたサービス領域の書込みフラグはオンとされ、サービス領域へのデータの書込みが禁止されるため、記録データの改ざんや消去が防止される。

【0 1 3 1】

ステップ S 5 3 において、書込みフラグがオンであると判定された場合、すなわち、書込みコマンドによりデータの書込みが指示されたサービス領域の状態が図 1 0 の状態 3 0 2 である場合、さらに換言すれば、書込みコマンドにより指示されたサービス領域の記録データがまだ読出されていない場合、ステップ S 5 4 および S 5 5 の処理はスキップされ、サービス領域にデータが書込まれずに、処理はステップ S 5 6 に進む。すなわち、サービス領域に記憶されている記録データが最初に読出されるまで、そのサービス領域への新たなデータの書込みが禁止される。

【0 1 3 2】

ステップ S 5 6 において、書込み制御部 2 3 2 は、書込み終了通知コマンドを送信し、データ書込み処理は終了する。具体的には、書込み制御部 2 3 2 は、データの書込みが終了したことを通知するコマンドコードを CMD フィールドに設定し、書込みコマンドに基づいてサービス領域にデータを書込んだ場合、書込みコマンドのシグネチャーフィールドに格納されていた記録データのシグネチャーをデータフィールドに格納し、サービス領域へのデータの書込みが失敗した場合、データの書込みが失敗したことを示すデータをデータフィールドに格納した書込み終了通知コマンドを生成する。書込み制御部 2 3 2 は、生成した書込み終了通知コマンドを、通信制御部 2 3 1、SPU 2 0 3、変調部 2 0 9、およびアンテナ 2 0 1 を介してリーダライタ 1 2 に送信する。

【0 1 3 3】

次に、図 1 2 のフローチャートを参照して、リーダライタ 1 2 および IC カード 1 3 との間で行なわれる、ライトワンスサービスのサービス領域に書込んだデータの確認処理を説明する。

【0 1 3 4】

最初に、リーダライタ 1 2 により実行されるデータ確認要求処理を説明する。

【0 1 3 5】

ステップ S 7 1 において、上述した図 1 1 のステップ S 4 1 と同様の処理により、リーダライタ 1 2 の通信制御部 1 7 1 は、ポーリングコマンドを送信する。送信したポーリングコマンドに対するポーリング応答コマンドが IC カード 1 3 から送信されてきた場合、リーダライタ 1 2 と IC カード 1 3 の間でセッション確立処理が実行され、リーダライタ 1 2 および IC カード 1 3 の間の通信セッションが確立された後、処理はステップ S 7 2 に進む。

【0 1 3 6】

ステップ S 7 2 において、書込み制御部 1 7 2 は、ライトワンスサービスのサービス領域に書込まれているデータの確認を要求する。具体的には、書込み制御部 1 7 2 は、データの確認を要求するコマンドコードを CMD フィールドに設定し、書込まれているデータの確認をするライトワンスサービスのサービス領域のサービス領域番号をデータフィールドに格納したデータ確認コマンドを生成する。書込み制御部 1 7 2 は、生成したデータ確認

10

20

30

40

50

コマンドを、通信制御部 171、SPU 133、変調部 134、およびアンテナ 136 を介して IC カード 13 に送信する。このとき、データ確認コマンドのデータフィールドに読出し鍵を格納する（読出し鍵を送信する）必要はない。

【0137】

IC カード 13 は、後述するステップ S82 において、リーダライタ 12 から送信されたデータ確認コマンドを受信し、データの確認が指示されたサービス領域の書込みフラグがオンである場合、すなわち、指示されたサービス領域から記録データがまだ読出されていない場合、ステップ S84 において、データ確認コマンドに対する応答であるデータ確認応答コマンドを送信する。なお、データ確認応答コマンドのデータフィールドには、データの確認が指示されたサービス領域に記録データとともに書込まれている記録データのシグネチャーが格納される。

10

【0138】

ステップ S73 において、書込み制御部 172 は、IC カード 13 から送信されたデータ確認応答コマンドを、アンテナ 136、復調部 137、SPU 133、および通信制御部 171 を介して受信し、データ確認要求処理は終了する。

【0139】

次に、リーダライタ 12 によるデータ確認要求処理に対応して、IC カード 13 により実行されるデータ確認応答処理を説明する。

【0140】

ステップ S81 において、上述した図 9 のステップ S11 の処理と同様に、IC カード 13 の通信制御部 231 は、上述したステップ S71 において、リーダライタ 12 から送信されたポーリングコマンドに応答する。

20

【0141】

その後、リーダライタ 12 と IC カード 13 の間でセッション確立処理が実行され、リーダライタ 12 および IC カード 13 の間の通信セッションが確立された後、処理はステップ S82 に進む。

【0142】

ステップ S82 において、読出し制御部 233 は、上述したステップ S72 において、リーダライタ 12 より送信されたデータ確認コマンドを、アンテナ 201、復調部 202、SPU 203、および、通信制御部 231 を介して受信する。

30

【0143】

ステップ S83 において、読出し制御部 233 は、データ確認コマンドによりデータの確認が指示されたライトワンスサービスのサービス領域の書込みフラグがオンであるかを判定する。書込みフラグがオンであると判定された場合、すなわち、サービス領域にデータが書込まれており、書込まれているデータ（記録データ）がまだ読出されていない場合、処理はステップ S84 に進む。

【0144】

ステップ S84 において、読出し制御部 233 は、データ確認応答コマンドを送信し、データ確認応答処理は終了する。具体的には、読出し制御部 233 は、データ確認コマンドに응答することを示すコマンドコードを CMD フィールドに設定し、データの確認が指示されたサービス領域に書込まれている記録データのシグネチャーをデータフィールドに格納したデータ確認応答コマンドを生成する。読出し制御部 233 は、生成したデータ確認応答コマンドを、通信制御部 231、SPU 203、変調部 209、およびアンテナ 201 を介してリーダライタ 12 に送信する。

40

【0145】

ステップ S83 において、書込みフラグがオフであると判定された場合、すなわち、サービス領域にデータが書込まれていないか、または、書込まれているデータ（記録データ）がすでに読出されている場合、ステップ S84 の処理はスキップされ、データ確認応答コマンドは送信されずに、データ確認応答処理は終了する。

【0146】

50

データ確認応答コマンドを受信したリーダライタ 1 2 は、ICカード 1 3 に書込みを要求した記録データのシグネチャーを再計算し、データ確認応答コマンドのデータフィールドに格納されている記録データのシグネチャーと比較することにより、データの確認を指示したサービス領域に書込まれている記録データの内容を確認することができる。再計算したシグネチャーと、データ確認応答コマンドに格納されているシグネチャーが一致する場合、記録データの書込みが成功し、かつ、その記録データがまだ読出されていないことが分かり、再計算したシグネチャーと、データ確認応答コマンドに格納されているシグネチャーが一致しない場合、記録データの書込みが失敗したか、すでに、別の記録データが書込まれていることが分かる。また、データ確認コマンドに対するデータ確認応答コマンドが返ってこない場合、指示したサービス領域から記録データがすでに読出されているか、または、記録データの書込みに失敗したことが分かる。 10

【0147】

さらに、読出し鍵を送信しなくてもサービス領域に書込まれている記録データの確認ができるとともに、第三者がサービス領域に書込まれている記録データの確認をしようとしても、不可逆な記録データのシグネチャーしか返されず、記録データを復元することができないため、第三者に記録データの内容を盗聴されることが防止される。

【0148】

その後、例えば、データの書込みを依頼したユーザ（リーダライタ 1 1 の所有者）は、リーダライタ 1 2 を用いて ICカード 1 3 にデータを書込んだユーザから ICカード 1 3 を取得する。 20

【0149】

次に、図 1 3 のフローチャートを参照して、リーダライタ 1 1 および ICカード 1 3 との間で行なわれる、ライトワンスサービスからのデータ読出し処理を説明する。

【0150】

最初に、リーダライタ 1 1 により実行されるデータ読出し要求処理を説明する。

【0151】

ステップ S 1 0 1 において、上述した図 9 のステップ S 1 と同様の処理により、リーダライタ 1 1 の通信制御部 7 1 は、ポーリングコマンドを送信する。送信したポーリングコマンドに対するポーリング応答コマンドが ICカード 1 3 から送信されてきた場合、リーダライタ 1 1 と ICカード 1 3 の間でセッション確立処理が実行され、リーダライタ 1 1 および ICカード 1 3 の間の通信セッションが確立された後、処理はステップ S 1 0 2 に進む。 30

【0152】

ステップ S 1 0 2 において、読出し制御部 7 3 は、ICカード 1 3 にデータの読出しを要求する。具体的には、読出し制御部 7 3 は、データの読出しを要求するコマンドコードを CMD フィールドに設定し、データを読出すライトワンスサービスのサービス領域のサービス領域番号、および、データの読出しの許可を得るための認証用の読出し鍵をデータフィールドに格納した読出しコマンドを生成する。読出し制御部 7 3 は、生成した読出しコマンドを、通信制御部 7 1、SPU 3 3、変調部 3 4、およびアンテナ 3 6 を介して ICカード 1 3 に送信する。

【0153】

ICカード 1 3 は、後述するステップ S 1 1 2 において、リーダライタ 1 1 から送信された読出しコマンドを受信し、データの読出しが指示されたサービス領域の読出し鍵と、読出しコマンドのデータフィールドに格納された読出し鍵が一致した場合、ステップ S 1 1 5 において、読出しが指示されたサービス領域から読出したデータ（記録データ）を格納した読出し応答コマンドを送信する。 40

【0154】

ステップ S 1 0 3 において、読出し制御部 7 3 は、ICカード 1 3 から送信された読出し応答コマンドを、アンテナ 3 6、復調部 3 7、SPU 3 3、および通信制御部 7 1 を介して受信し、データ読出し要求処理は終了する。

【0155】

次に、リーダライタ 1 1 によるデータ読出し要求処理に対応して、ICカード 1 3 により実行されるデータ読出し処理を説明する。

【0156】

ステップ S 1 1 1 において、上述した図 9 のステップ S 1 1 の処理と同様に、ICカード 1 3 の通信制御部 2 3 1 は、上述したステップ S 1 0 1 において、リーダライタ 1 1 から送信されたポーリングコマンドに応答する。

【0157】

その後、リーダライタ 1 1 と ICカード 1 3 の間でセッション確立処理が実行され、リーダライタ 1 1 および ICカード 1 3 の間の通信セッションが確立された後、処理はステップ S 1 1 2 に進む。

10

【0158】

ステップ S 1 1 2 において、読出し制御部 2 3 3 は、上述したステップ S 1 0 2 において、リーダライタ 1 1 より送信された読出しコマンドを、アンテナ 2 0 1、復調部 2 0 2、SPU 2 0 3、および通信制御部 2 3 1 を介して受信する。

【0159】

ステップ S 1 1 3 において、読出し制御部 2 3 3 は、読出しコマンドによりデータの読出しが指示されたサービス領域の読出し鍵と、読出しコマンドのデータフィールドに格納された読出し鍵が一致するか否かを判定する。読出し鍵が一致したと判定された場合、処理はステップ S 1 1 4 に進む。

【0160】

20

ステップ S 1 1 4 において、読出し制御部 2 3 3 は、読出しコマンドによりデータの読出しが指示されたサービス領域の読出しフラグをオフにする。これにより、サービス領域の状態は、現在図 1 0 の状態 3 0 2 である場合、状態 3 0 3 に遷移し、現在状態 3 0 3 である場合、状態 3 0 3 のままとなる。すなわち、書込みフラグがオフされ、サービス領域へのデータの書込みが可能となり、かつ、サービス領域にデータが書込まれている状態となる。

【0161】

ステップ S 1 1 5 において、読出し制御部 2 3 3 は、読出し応答コマンドを送信し、データ読出し処理は終了する。具体的には、読出し制御部 2 3 3 は、読出しコマンドに応答することを示すコマンドコードを CMD フィールドに設定し、読出しコマンドにより指示されたサービス領域から読出した記録データをデータフィールドに格納した読出し応答コマンドを生成する。読出し制御部 2 3 3 は、生成した読出し応答コマンドを、通信制御部 2 3 1、SPU 2 0 3、変調部 2 0 9、およびアンテナ 2 0 1 を介してリーダライタ 1 1 に送信する。

30

【0162】

ステップ S 1 1 3 において、読出し鍵が一致しないと判定された場合、ステップ S 1 1 4 および S 1 1 5 の処理はスキップされ、読出し応答コマンドがリーダライタ 1 1 に送信されずに、データ読出し処理は終了する。従って、読出し鍵が一致しない場合、サービス領域からのデータの読出しは許可されず、上述したように読出し鍵が一致する場合、サービス領域からのデータの読出しが許可される。

40

【0163】

このように、ライトワンスサービスでは、ライトワンスサービスを生成したユーザが所有する読出し鍵を、ライトワンスサービスにデータを書込む人などの他者に渡す必要がないため、読出し鍵が第三者の手に渡る危険性が軽減され、かつ、その読出し鍵を用いなければデータを読出すことができないため、書込まれたデータの盗聴が防止される。また、ライトワンスサービスのサービス領域にデータが書込まれた場合、書込まれたデータが読込まれるまで、そのサービス領域へのデータの書込みが禁止されるため、データの改ざんや消去が防止される。さらに、ライトワンスサービスでは、データを授受する二者間で共通の鍵を持ったり、鍵を交換したりする必要がないため、データを授受する手順が簡単になる。また、ライトワンスサービスでは、データを書込む相手によって読出し鍵やサービ

50

ス領域を必ずしも使い分ける必要がないため、鍵およびサービスの管理が容易である。

【0164】

なお、上述した図11および図12のリーダライタ12の処理をリーダライタ11により実行させるようにすることも可能である。すなわち、同じリーダライタを用いて、ICカード13にライトワンスサービスを生成し、ライトワンスサービスヘータを書込んだり、ライトワンスサービスからデータを読み出したりすることも可能である。

【0165】

また、データ確認コマンドと読み出しコマンドを特に区別せずに、読み出しコマンドのデータフィールドに読み出し鍵が格納されている場合、サービス領域に記憶されている記録データを読み出せるようにし、読み出しコマンドのデータフィールドに読み出し鍵が格納されていない場合、サービス領域に記憶されている記録データのシグネチャーのみを読み出せるようにしてもよい。

10

【0166】

次に、図14乃至図17を参照して、リードワンスサービスを利用したICカードシステム1の処理を説明する。

【0167】

まず、図14のフローチャートを参照して、ICカードシステム1におけるリードワンスサービス生成処理を説明する。

【0168】

最初に、リードワンスサービス生成処理において、リーダライタ11により実行されるリードワンスサービス生成要求処理を説明する。

20

【0169】

ステップS201において、上述した図9のステップS1と同様の処理により、リーダライタ11の通信制御部71は、ポーリングコマンドを送信する。送信したポーリングコマンドに対するポーリング応答コマンドがICカード13から送信されてきた場合、リーダライタ11とICカード13の間でセッション確立処理が実行され、リーダライタ11およびICカード13の間の通信セッションが確立された後、処理はステップS202に進む。

【0170】

ステップS202において、サービス生成要求部74は、ICカード13に、リードワンスサービスの生成を要求する。具体的には、サービス生成要求部74は、リードワンスサービス内に確保するサービス領域の数、サービス領域番号、サービス領域のサイズ、サービス領域にデータを書込むときの認証用の書込み鍵など、リードワンスサービスを生成するために必要なデータをデータフィールドに格納したサービス生成要求コマンドを生成する。サービス生成要求部74は、生成したサービス生成要求コマンドを、通信制御部71、SPU33、変調部34、およびアンテナ36を介してICカード13に送信する。

30

【0171】

ICカード13は、後述するステップS212において、サービス生成要求コマンドを受信し、リードワンスサービスを生成した後、ステップS213において、サービス生成要求コマンドに対する応答であるサービス生成通知コマンドを送信する。

40

【0172】

ステップS203において、サービス生成要求部74は、ICカード13より送信されたサービス生成通知コマンドを、アンテナ36、復調部37、SPU33、および、通信制御部71を介して受信し、リードワンスサービス生成要求処理は終了する。

【0173】

次に、リーダライタ11によるリードワンスサービス生成要求処理に対応して、ICカード13により実行されるリードワンスサービス生成処理を説明する。

【0174】

ステップS211において、上述した図9のステップS11の処理と同様に、ICカード13の通信制御部231は、上述したステップS201において、リーダライタ11から

50

送信されたポーリングコマンドに応答する。

【0175】

その後、リーダライタ11とICカード13の間でセッション確立処理が実行され、リーダライタ11およびICカード13の間の通信セッションが確立された後、処理はステップS212に進む。

【0176】

ステップS212において、サービス生成部234は、リードワンスサービスを生成する。具体的には、サービス生成部234は、上述したステップS202において、リーダライタ11より送信されたサービス生成要求コマンドを、アンテナ201、復調部202、SPU203、および通信制御部231を介して受信する。サービス生成部234は、サービス生成要求コマンドにより指示されたサイズのサービス領域を、サービス生成要求コマンドにより指示された数だけ記憶部207に確保し、サービス生成要求コマンドにより指示されたサービス領域番号を各サービス領域に設定する（サービス領域の所定の位置に記憶させる）。

10

【0177】

サービス生成部234は、サービス生成要求コマンドのデータフィールドに格納されている、サービス領域へのデータの書込みを許可する書込み鍵を登録する（サービス領域の所定の位置に記憶させる）。また、サービス生成部234は、サービス領域に記憶されているデータの暗号化の可否を示す暗号化フラグを記憶する領域をサービス領域の所定の位置に確保し、暗号化フラグの値を、データの暗号化を許可するオフに設定する。

20

【0178】

これにより、リードワンスサービスの各サービス領域の状態は、図15に示される状態311となる。すなわち、暗号化フラグがオフされ、かつ、サービス領域にデータが書込まれていない状態となる。

【0179】

なお、サービス領域ごとにそれぞれ異なる書込み鍵を登録するようにしてもよいし、同じ書込み鍵を登録するようにしてもよい。サービス領域ごとに異なる書込み鍵を登録する場合、サービス生成要求コマンドのデータフィールドに全ての書込み鍵を格納するようにしてもよいし、1つ以上の書込み鍵から計算などにより複数の書込み鍵を生成するようにしてもよい。また、予め別の処理によりリードワンスサービスのサービス領域を記憶部207に登録（確保）しておいて、登録されているサービス領域にリーダライタ11により読み出し鍵を登録するようにしてもよい。

30

【0180】

ステップS213において、サービス生成部234は、サービス生成通知コマンドをリーダライタ11に送信して、リードワンスサービス生成処理は終了する。具体的には、サービス生成部234は、サービスの生成の終了を通知するコマンドコードをCMDフィールドに設定し、リードワンスサービスの生成結果（例えば、サービスの生成が成功したか失敗したかなど）を示すデータをデータフィールドに格納したサービス生成通知コマンドを生成する。サービス生成部234は、生成したサービス生成通知コマンドを、通信制御部231、SPU203、変調部209、およびアンテナ201を介して、リーダライタ11に送信する。

40

【0181】

次に、図16のフローチャートを参照して、リーダライタ11およびICカード13との間で行なわれるリードワンスサービスへのデータ書込み処理を説明する。

【0182】

最初に、リーダライタ11により実行されるデータ書込み要求処理を説明する。

【0183】

ステップS241において、上述した図9のステップS1と同様の処理により、リーダライタ11の通信制御部71は、ポーリングコマンドを送信する。送信したポーリングコマンドに対するポーリング応答コマンドがICカード13から送信されてきた場合、リーダ

50

ライタ 1 1 と IC カード 1 3 の間でセッション確立処理が実行され、リーダライタ 1 1 および IC カード 1 3 の間の通信セッションが確立された後、処理はステップ S 2 4 2 に進む。

【 0 1 8 4 】

ステップ S 2 4 2 において、書込み制御部 7 2 は、IC カード 1 3 にデータの書込みを要求する。具体的には、書込み制御部 7 2 は、データの書込みを要求するコマンドコードを CMD フィールドに設定し、データを書込むリードワンスサービスのサービス領域のサービス領域番号、サービス領域に書込む記録データ、および、データの書込みの許可を得るための認証用の書込み鍵をデータフィールドに格納し、記録データのシグネチャーをシグネチャーフィールドに格納した書込みコマンドを生成する。書込み制御部 7 2 は、生成した書込みコマンドを、通信制御部 7 1、SPU 3 3、変調部 3 4、およびアンテナ 3 6 を介して IC カード 1 3 に送信する。 10

【 0 1 8 5 】

IC カード 1 3 は、後述するステップ S 2 5 2 において、リーダライタ 1 1 から送信された書込みコマンドを受信し、データの書込みが指示されたサービス領域の書込み鍵と、書込みコマンドのデータフィールドに格納された書込み鍵が一致した場合、書込みが指示されたサービス領域にデータを書込み、ステップ S 2 5 6 において、データの書込みが終了したことを通知する書込み終了通知コマンドを送信する。

【 0 1 8 6 】

ステップ S 2 4 3 において、書込み制御部 7 2 は、IC カード 1 3 から送信された書込み終了通知コマンドを、アンテナ 3 6、復調部 3 7、SPU 3 3、および通信制御部 7 1 を介して受信し、データ書込み要求処理は終了する。 20

【 0 1 8 7 】

次に、リーダライタ 1 1 によるデータ書込み要求処理に対応して、IC カード 1 3 により実行されるデータ書込み処理を説明する。

【 0 1 8 8 】

ステップ S 2 5 1 において、上述した図 9 のステップ S 1 1 の処理と同様に、IC カード 1 3 の通信制御部 2 3 1 は、上述したステップ S 2 4 1 において、リーダライタ 1 1 から送信されたポーリングコマンドに応答する。

【 0 1 8 9 】

その後、リーダライタ 1 1 と IC カード 1 3 の間でセッション確立処理が実行され、リーダライタ 1 1 および IC カード 1 3 の間の通信セッションが確立された後、処理はステップ S 2 5 2 に進む。 30

【 0 1 9 0 】

ステップ S 2 5 2 において、書込み制御部 2 3 2 は、上述したステップ S 2 4 2 において、リーダライタ 1 1 より送信された書込みコマンドを、アンテナ 2 0 1、復調部 2 0 2、SPU 2 0 3、および通信制御部 2 3 1 を介して受信する。

【 0 1 9 1 】

ステップ S 2 5 3 において、書込み制御部 2 3 2 は、書込みコマンドによりデータの書込みが指示されたサービス領域の書込み鍵と、書込みコマンドのデータフィールドに格納された書込み鍵が一致するか否かを判定する。書込み鍵が一致したと判定された場合、処理はステップ S 2 5 4 に進む。 40

【 0 1 9 2 】

ステップ S 2 5 4 において、書込み制御部 2 3 2 は、記憶部 2 0 7 にデータを書込む。具体的には、書込み制御部 2 3 2 は、書込みコマンドのデータフィールドに格納されている記録データ、および、シグネチャーフィールドに格納されている記録データのシグネチャーを、書込みコマンドにより指示されたサービス領域に書込む。

【 0 1 9 3 】

ステップ S 2 5 5 において、書込み制御部 2 3 2 は、書込みコマンドによりデータの書込みが指示されたサービス領域の暗号化フラグをオフにする。これにより、サービス領域の状態は、現在上述した図 1 5 の状態 3 1 1 または後述する状態 3 1 3 である場合、状態 50

3 1 2 に遷移し、現在状態 3 1 2 である場合、状態 3 1 2 のままとなる。すなわち、サービス領域に記憶されている記録データが暗号化されておらず、かつ、暗号化フラグがオフされ、記録データの暗号化が可能な状態となる。

【0 1 9 4】

ステップ S 2 5 6 において、書込み制御部 2 3 2 は、書込み終了通知コマンドを送信し、データ書込み処理は終了する。具体的には、書込み制御部 2 3 2 は、データの書込みが終了したことを通知するコマンドコードを CMD フィールドに設定し、書込みコマンドに基づいてサービス領域にデータを書込んだ場合、書込みコマンドのシグネチャーフィールドに格納されていた記録データのシグネチャーをデータフィールドに格納し、サービス領域へのデータの書込みが失敗した場合、データの書込みが失敗したことを示すデータをデータフィールドに格納した書込み終了通知コマンドを生成する。書込み制御部 2 3 2 は、生成した書込み終了通知コマンドを、通信制御部 2 3 1、SPU 2 0 3、変調部 2 0 9、およびアンテナ 2 0 1 を介してリーダライタ 1 1 に送信する。

10

【0 1 9 5】

ステップ S 2 5 3 において、書込み鍵が一致しないと判定された場合、ステップ S 2 5 4 乃至 S 2 5 6 の処理はスキップされ、サービス領域にデータが書込まれずに、データ書込み処理は終了する。従って、書込み鍵が一致しない場合、サービス領域へのデータの書込みは許可されず、上述したように書込み鍵が一致する場合、サービス領域へのデータの書込みが許可される。

【0 1 9 6】

その後、例えば、リーダライタ 1 1 を用いて IC カード 1 3 にデータを書込んだユーザは、リーダライタ 1 2 の所有者に IC カード 1 3 を送付する。

20

【0 1 9 7】

次に、図 1 7 のフローチャートを参照して、リーダライタ 1 2 および IC カード 1 3 との間で行なわれるリードワンスサービスからのデータ読出し処理を説明する。

【0 1 9 8】

最初に、リーダライタ 1 2 により実行されるデータ読出し要求処理を説明する。

【0 1 9 9】

ステップ S 2 7 1 において、上述した図 1 1 のステップ S 4 1 と同様の処理により、リーダライタ 1 2 の通信制御部 1 7 1 は、ポーリングコマンドを送信する。送信したポーリングコマンドに対するポーリング応答コマンドが IC カード 1 3 から送信されてきた場合、リーダライタ 1 2 と IC カード 1 3 の間でセッション確立処理が実行され、リーダライタ 1 2 および IC カード 1 3 の間の通信セッションが確立された後、処理はステップ S 7 2 に進む。

30

【0 2 0 0】

ステップ S 2 7 2 において、読出し制御部 1 7 3 は、IC カード 1 3 にデータの読出しを要求する。具体的には、読出し制御部 1 7 3 は、データの読出しを要求するコマンドコードを CMD フィールドに設定し、データを読出すリードワンスサービスのサービス領域のサービス領域番号、および、読出すデータを暗号化する暗号化鍵をデータフィールドに格納した読出しコマンドを生成する。データフィールドに格納される暗号化鍵は、リードワンスサービスが対応する暗号化方式（例えば、DES (Data Encryption Standard) など）に基づいたものであれば、リーダライタ 1 2 (読出し制御部 1 7 3) で独自に設定したものでよい。読出し制御部 1 7 3 は、生成した読出しコマンドを、通信制御部 1 7 1、SPU 1 3 3、変調部 1 3 4、およびアンテナ 1 3 6 を介して IC カード 1 3 に送信する。

40

【0 2 0 1】

後述するステップ S 2 8 2 において、IC カード 1 3 は、リーダライタ 1 2 から送信された読出しコマンドを受信する。そして、IC カード 1 3 は、データの読出しが指示されたサービス領域の暗号化フラグがオフの場合、すなわち、指示されたサービス領域に記憶されている記録データが暗号化されていない場合、読出しコマンドに格納された暗号化鍵を用いて記録データを暗号化し、後述するステップ S 2 8 6 において、暗号化した記録データ

50

を格納した読出し応答コマンドを送信する。また、ICカード 13 は、データの読出しが指示されたサービス領域の暗号化フラグがオンの場合、すなわち、サービス領域に記録されている記録データが暗号化されている場合、指示されたサービス領域から記録データを読出し、後述するステップ S 286 において、読出した記録データを格納した読出し応答コマンドを送信する。

【0202】

ステップ S 273 において、読出し制御部 173 は、読出し応答コマンドを受信したか否かを判定する。読出しコマンドを送信してから所定の時間内に、読出し応答コマンドを受信しなかったと判定された場合、例えば、リーダライタ 12 と ICカード 13 との距離が長くなり、読出しコマンドの送信や読出し応答コマンドの受信を失敗した場合、処理はステップ S 274 に進む。

10

【0203】

ステップ S 274 において、読出し制御部 173 は、読出し応答コマンドの再送を要求するか否かを判定する。読出し応答コマンドの再送を要求すると判定された場合、処理はステップ S 272 に戻り、ステップ S 273 において、読出し応答コマンドを受信したと判定されるか、または、ステップ S 274 において、読出し応答コマンドの再送を要求しないと判定されるまで、ステップ S 272 乃至 S 274 の処理が繰り返し実行され、リーダライタ 12 から ICカード 13 に読出しコマンドが繰り返し送信される。

【0204】

ステップ S 273 において、読出しコマンドを送信してから所定の時間内に、ICカード 13 から読出し応答コマンドが送信され、読出し制御部 173 が、アンテナ 136、復調部 137、SPU 133、および通信制御部 171 を介して読出し応答コマンドを受信したと判定された場合、処理はステップ S 275 に進む。

20

【0205】

ステップ S 275 において、復号部 175 は、ICカード 13 から読出したデータを復号し、データ読出し要求処理は終了する。具体的には、読出し制御部 173 は、読出しコマンドのデータフィールドに格納されている記録データと、読出しコマンドに格納して ICカード 13 に送信した暗号化鍵を復号部 175 に供給する。復号部 175 は、供給された暗号化鍵を用いて、記録データを復号し、復号した記録データを読出し制御部 173 に供給する。

30

【0206】

ステップ S 274 において、読出し応答コマンドの再送を要求しないと判定された場合、例えば、所定の回数読出しコマンドを送信したにも関わらず、ICカード 13 から読出し応答コマンドを受信できなかった場合、データ読出し要求処理は終了する。

【0207】

次に、リーダライタ 12 によるデータ読出し要求処理に対応して、ICカード 13 により実行されるデータ読出し処理を説明する。

【0208】

ステップ S 281 において、上述した図 9 のステップ S 11 の処理と同様に、ICカード 13 の通信制御部 231 は、上述したステップ S 271 において、リーダライタ 12 から送信されたポーリングコマンドに応答する。

40

【0209】

その後、リーダライタ 12 と ICカード 13 の間でセッション確立処理が実行され、リーダライタ 12 および ICカード 13 の間の通信セッションが確立された後、処理はステップ S 282 に進む。

【0210】

ステップ S 282 において、読出し制御部 233 は、上述したステップ S 272 において、リーダライタ 12 より送信された読出しコマンドを、アンテナ 201、復調部 202、SPU 203、および通信制御部 231 を介して受信する。

【0211】

50

ステップS 2 8 3において、読出し制御部 2 3 3は、読出しコマンドによりデータの読出しが指示されたサービス領域の暗号化フラグがオフであるか否かを判定する。暗号化フラグがオフであると判定された場合、すなわち、読出しコマンドによりデータの読出しが指示されたサービス領域の状態が図 1 5 の状態 3 1 2である場合、さらに換言すれば、指示されたサービス領域に記録されている記録データが暗号化されていない場合、処理はステップS 2 8 4に進む。

【 0 2 1 2 】

ステップS 2 8 4において、暗号化部 2 3 5は、データを暗号化する。具体的には、読出し制御部 2 3 3は、読出しコマンドにより指示されたサービス領域の記録データを読み出し、読み出した記録データと読出しコマンドを暗号化部 2 3 5に供給する。暗号化部 2 3 5は、読出しコマンドのデータフィールドに格納されている暗号化鍵を用いて、所定の暗号化方式により記録データを暗号化し、暗号化した記録データを、読出し制御部 2 3 3に供給するとともに、記録データが読出されたサービス領域に上書きする。

10

【 0 2 1 3 】

ステップS 2 8 5において、暗号化部 2 3 5は、暗号化した記録データを書込んだサービス領域の暗号化フラグをオンにする。これにより、このサービス領域の状態は、図 1 5 の状態 3 1 2から状態 3 1 3に遷移する。すなわち、サービス領域に記憶されている記録データが暗号化されており、かつ、暗号化フラグがオンされ、記録データの暗号化が禁止された状態となる。

【 0 2 1 4 】

20

ステップS 2 8 3において、暗号化フラグがオンであると判定された場合、すなわち、読出しコマンドによりデータの読出しが指示されたサービス領域の状態が図 1 5 の状態 3 1 3である場合、さらに換言すれば、今回の読出しコマンドで読出しが指示されたサービス領域の記録データが、先にリーダライタ 1 2、または、他のリーダライタから受信した読出しコマンドに基づいて、先に受信した読出しコマンドに格納されていた暗号化鍵で暗号化されている場合、ステップS 2 8 4およびS 2 8 5の処理はスキップされ、処理はステップS 2 8 6に進む。すなわち、読出しコマンドにより読出しが指示されたサービス領域の記録データは暗号化されない。

【 0 2 1 5 】

従って、サービス領域に記憶されている記録データが最初に読出される場合、記録データの読出しを指示する読出しコマンドに格納されている暗号化鍵を用いて記録データが暗号化され、サービス領域に記憶されている記録データが 2 回目以降に読出される場合、その記録データは新たに暗号化されない。すなわち、記録データは 1 回のみ暗号化される。

30

【 0 2 1 6 】

なお、上述したように、書込みコマンドによりサービス領域に新たに記録データが書込まれた場合、そのサービス領域の暗号化フラグがオフされ、サービス領域の状態は状態 3 0 3から状態 3 0 2に遷移し、記録データの暗号化が可能になる。

【 0 2 1 7 】

ステップS 2 8 6において、読出し制御部 2 3 3は、読出し応答コマンドを送信し、データ読出し処理は終了する。具体的には、読出し制御部 2 3 3は、読出しコマンドに応答することを示すコマンドコードをCMDフィールドに設定し、読出しコマンドにより指示されたサービス領域の記録データをデータフィールドに格納した読出し応答コマンドを生成する。読出し制御部 2 3 3は、生成した読出し応答コマンドを、通信制御部 2 3 1、SPU 2 0 3、変調部 2 0 9、およびアンテナ 2 0 1を介してリーダライタ 1 2に送信する。

40

【 0 2 1 8 】

このとき、データフィールドに格納される記録データは、ステップS 2 8 3において、暗号化フラグがオフであると判定された場合、ステップS 2 8 4において、今回受信した読出しコマンドに格納されている暗号化鍵を用いて暗号化されたデータとされ、ステップS 2 8 3において、暗号化フラグがオンであると判定された場合、指示されたサービス領域に記録されている記録データ、すなわち、以前受信した読出しコマンドに格納されてい

50

た暗号化鍵で暗号化されたデータとされる。すなわち、サービス領域に記憶されている記録データが最初に読出されるとき、ステップS 2 8 4の処理により暗号化された記録データがリーダライタ1 2に送信され、サービス領域に記憶されている記録データが2回目以降に読出されるとき、以前ICカード1 3によりデータ読出し処理が実行されたときのステップS 2 8 4の処理によりすでに暗号化されている記録データがサービス領域から読出され、読出された記録データがリーダライタ1 2に送信される。

【0 2 1 9】

なお、読出しコマンドのデータフィールドに有効な暗号化鍵が格納されていない場合、ICカード1 3は、その読出しコマンドに対する処理は行なわない。また、データが書込まれていないサービス領域（図1 5の状態3 1 1のサービス領域）からのデータの読出しが要求された場合、ステップS 2 8 6において、送信される読出し応答コマンドのデータフィールドには、データが書込まれていないことを示すデータが格納される。

10

【0 2 2 0】

このように、リードワンスサービスでは、リードワンスサービスを生成したユーザが所有する書込み鍵を、リードワンスサービスからデータを読出す人などの他者に渡す必要がないため、書込み鍵が第三者の手に渡る危険性が軽減され、かつ、その書込み鍵を用いなければデータを書込むことができないため、記録データの改ざんや、第三者が記録データを書込むこと（なりすまし）が防止される。また、リードワンスサービスでは、データを授受する二者間で共通の鍵を持ったり、鍵を交換したりする必要がないため、データを授受する手順が簡単になる。さらに、リードワンスサービスでは、データを読出す相手によって書込み鍵やサービス領域を必ずしも使い分ける必要がないため、鍵やサービスの管理が容易である。

20

【0 2 2 1】

また、リードワンスサービスから記録データを読出す場合、最初に読出したリーダライタにより独自に設定された暗号化鍵で記録データが暗号化されるため、最初に読出したユーザ（リーダライタ）のみ記録データの内容を確認することができる。従って、正式な相手（リードワンスサービスにデータを書込んだユーザからデータの読出しを依頼された相手）がリードワンスサービスから記録データをいったん読出せば、それ以降、その記録データの内容を第三者が盗聴することができなくなり、例えば、ICカード1 3を紛失したり、廃棄しても記録データの内容が第三者により盗聴されることがない。なお、正式な相手が記録データを読出す前に、第三者により記録データがリードワンスサービスから読出された場合、その記録データは第三者の独自の鍵で暗号化されるため、記録データが盗聴されたことを容易に知ることができ、その記録データを使用しないようにするなどの然るべき対策を迅速に施すことができる。

30

【0 2 2 2】

なお、上述した図1 7のリーダライタ1 2の処理をリーダライタ1 1により実行させるようにすることも可能である。すなわち、同じリーダライタを用いて、ICカード1 3にリードワンスサービスを生成し、リードワンスサービスへデータを書込んだり、リードワンスサービスからデータを読出したりすることも可能である。

【0 2 2 3】

以上のように、第1の情報処理装置から送信されてくる、記憶領域からのデータの読出しを許可する第1の読出し鍵を登録し、記憶領域に記憶されているデータが最初に読出されるまで、記憶領域への新たなデータの書込みを禁止するように記憶部へのデータの書込みを制御し、第1の情報処理装置または第1の情報処理装置とは異なる第2の情報処理装置により記憶領域からのデータの読出しが要求された場合、第1の情報処理装置または第2の情報処理装置から送信されてくる第2の読出し鍵と第1の読出し鍵とが一致するとき、記憶領域からのデータの読出しを許可するように記憶部からのデータの読出しを制御する場合には、データを授受することができる。また、より簡単にデータを安全に授受することができる。

40

【0 2 2 4】

50

また、第 1 の情報処理装置から送信されてくる、記憶領域へのデータの書込みを許可する第 1 の書込み鍵を登録し、第 1 の情報処理装置または第 1 の情報処理装置とは異なる第 2 の情報処理装置により記憶領域へのデータの書込みが要求された場合、第 1 の情報処理装置または第 2 の情報処理装置から送信されてくる第 2 の書込み鍵が第 1 の書込み鍵と一致するとき、記憶領域へのデータの書込みを許可するように記憶部へのデータの書込みを制御し、第 1 の情報処理装置または第 2 の情報処理装置により記憶領域からのデータの読出しが要求された場合、記憶領域に記憶されているデータが最初に読出されるとき、第 1 の情報処理装置または第 2 の情報処理装置より送信されてくる暗号化鍵を用いて記憶領域に記憶されているデータを暗号化し、第 1 の情報処理装置または第 2 の情報処理装置により記憶領域からのデータの読出しが要求された場合、記憶領域に記憶されているデータが最初に読出されるとき、暗号化されたデータを第 1 の情報処理装置または第 2 の情報処理装置に送信し、記憶領域に記憶されているデータが 2 回目以降に読出されるとき、すでに暗号化されているデータを記憶領域から読出し、読出したデータを第 1 の情報処理装置または第 2 の情報処理装置に送信する場合には、データを授受することができる。また、より簡単にデータを安全に授受することができる。

【0225】

なお、以上の説明では、非接触型の IC カードを用いた IC カードシステムを例に用いたが、本発明は、接触型の IC カード、または、上述した一連の処理を実行可能なコンピュータまたはハードウェアを内蔵した IC カード以外の記憶装置を用いたデータ授受システムにも適用することができる。

【0226】

上述した一連の処理は、ハードウェアにより実行させることもできるし、ソフトウェアにより実行させることもできる。一連の処理をソフトウェアにより実行させる場合には、そのソフトウェアを構成するプログラムが、専用のハードウェアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば汎用のパーソナルコンピュータなどに、ネットワークや記録媒体からインストールされる。

【0227】

この記録媒体は、図 3 および図 5 に示すように、コンピュータとは別に、ユーザにプログラムを提供するために配布される、プログラムが記録されている磁気ディスク（フレキシブルディスクを含む）51、151、光ディスク（CD-ROM（Compact Disc-Read Only Memory）、DVD（Digital Versatile Disc）を含む）52、152、光磁気ディスク（MD（Mini-Disc）（登録商標）を含む）53、153、若しくは半導体メモリ 54、154 などよりなるパッケージメディアにより構成されるだけでなく、コンピュータに予め組み込まれた状態でユーザに提供される、プログラムが記録されている ROM 205（図 7）や、記録部 32、132 に含まれるハードディスク、記憶部 207（図 7）などで構成される。

【0228】

なお、上述した一連の処理を実行させるプログラムは、必要に応じてルータ、モデムなどのインタフェースを介して、ローカルエリアネットワーク、インターネット、デジタル衛星放送といった、有線または無線の通信媒体を介してコンピュータにインストールされるようにしてもよい。

【0229】

また、本明細書において、記録媒体に格納されるプログラムを記述するステップは、記載された順序に沿って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

【0230】

また、本明細書において、システムの用語は、複数の装置、手段などにより構成される全体的な装置を意味するものである。

【図面の簡単な説明】

【0231】

10

20

30

40

50

【図 1】本発明を適用した IC カードシステムの一実施の形態を示す図である。

【図 2】図 1 の IC カードシステムにおいて送受信されるコマンドのフォーマットの例を示す図である。

【図 3】図 1 のリーダライタの機能の構成例を示すブロック図である。

【図 4】図 3 のリーダライタの制御部により実現される機能の構成例を示すブロック図である。

【図 5】図 1 のもう一方のリーダライタの機能の構成例を示すブロック図である。

【図 6】図 6 のリーダライタの制御部により実現される機能の構成例を示すブロック図である。

【図 7】図 1 の IC カードの機能の構成例を示すブロック図である。

10

【図 8】IC カードの制御部により実現される機能の構成例を示すブロック図である。

【図 9】図 1 の IC カードシステムのライトワンスサービス生成処理を説明するフローチャートである。

【図 10】ライトワンスサービスのサービス領域の状態の遷移を示す図である。

【図 11】図 1 の IC カードシステムのライトワンスサービスにおけるデータ書込み処理を説明するフローチャートである。

【図 12】図 1 の IC カードシステムのライトワンスサービスにおけるデータ確認処理を説明するフローチャートである。

【図 13】図 1 の IC カードシステムのライトワンスサービスにおけるデータ読出し処理を説明するフローチャートである。

20

【図 14】図 1 の IC カードシステムのリードワンスサービス生成処理を説明するフローチャートである。

【図 15】リードワンスサービスのサービス領域の状態の遷移を示す図である。

【図 16】図 1 の IC カードシステムのリードワンスサービスにおけるデータ書込み処理を説明するフローチャートである。

【図 17】図 1 の IC カードシステムのリードワンスサービスにおけるデータ読出し処理を説明するフローチャートである。

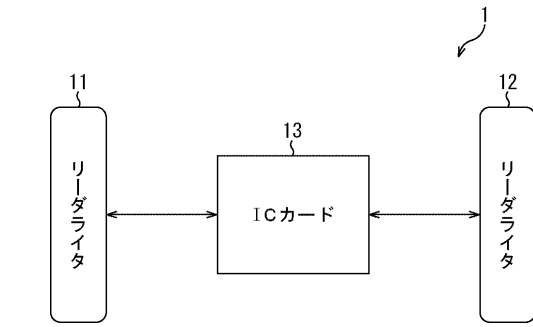
【符号の説明】

【0232】

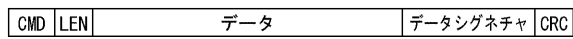
1 IC カードシステム, 11 リーダライタ, 12 リーダライタ, 13 IC カード, 31 制御部, 32 記録部, 38 ドライブ, 51 磁気ディスク, 52 光ディスク, 53 光磁気ディスク, 54 半導体メモリ, 72 書込み制御部, 73 読出し制御部, 74 サービス生成要求部, 131 制御部, 132 記録部, 138 ドライブ, 151 磁気ディスク, 152 光ディスク, 153 光磁気ディスク, 154 半導体メモリ, 172 書込み制御部, 173 読出し制御部, 204 制御部, 205 ROM, 207 記憶部, 231 通信制御部, 232 書込み制御部, 233 読出し制御部, 234 サービス生成部, 235 暗号化部

30

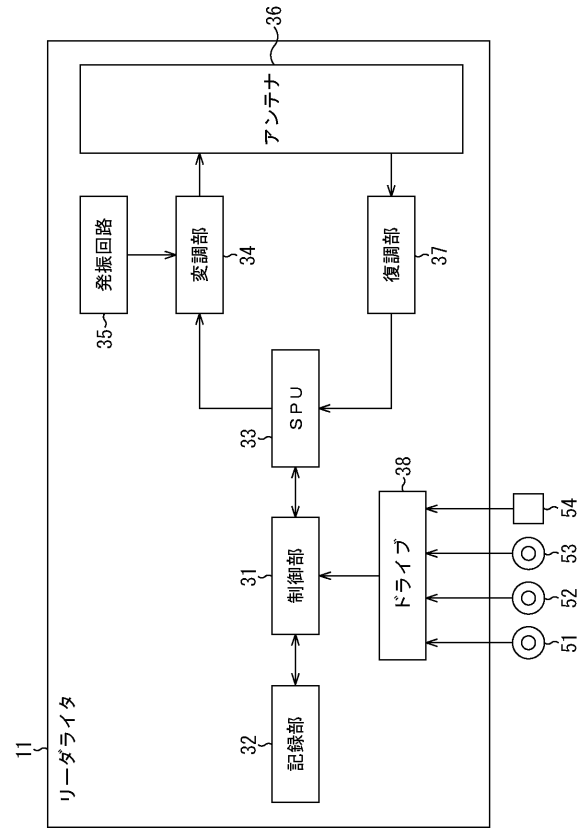
【図 1】



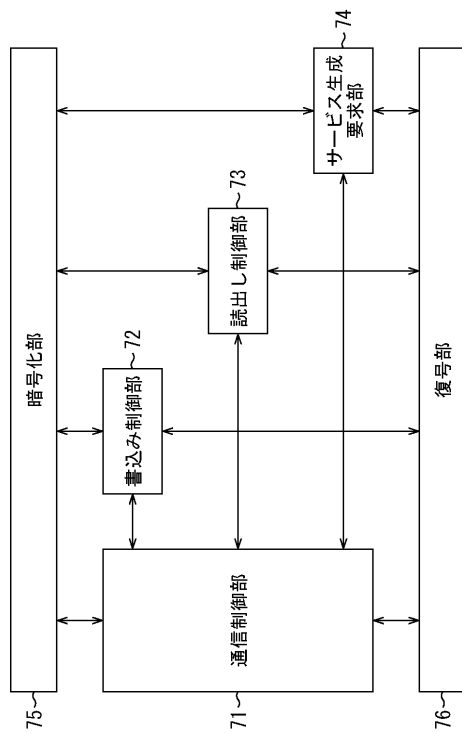
【図 2】



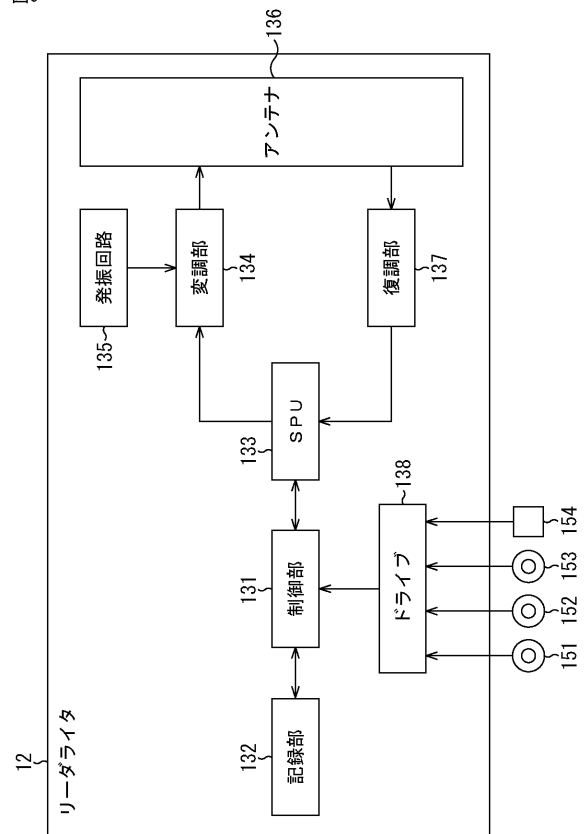
【図 3】

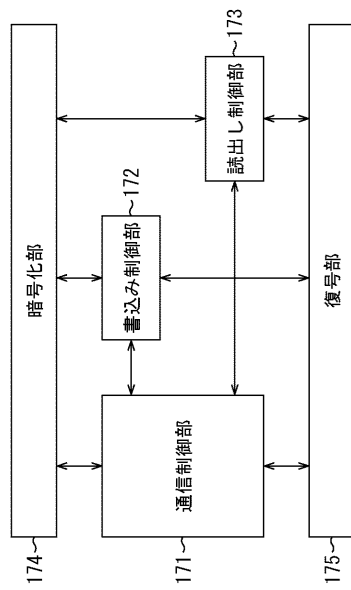
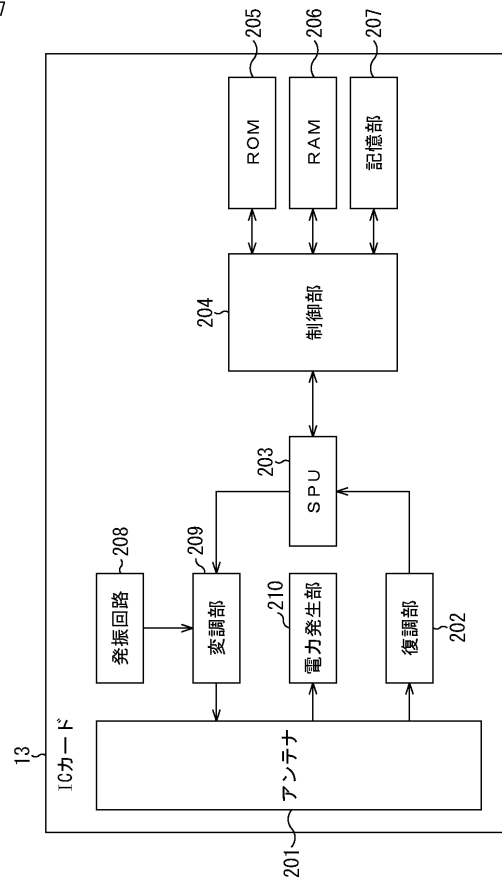
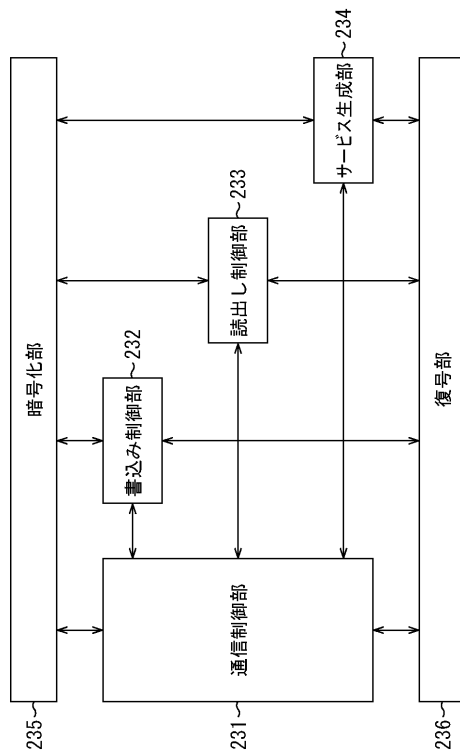
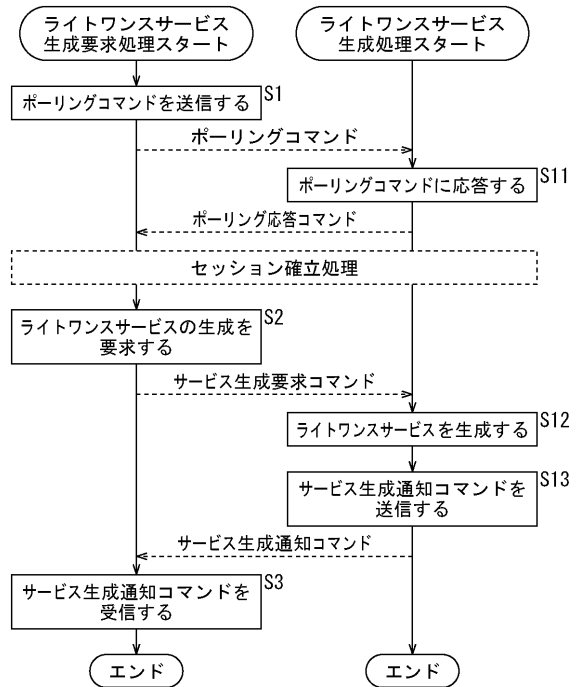


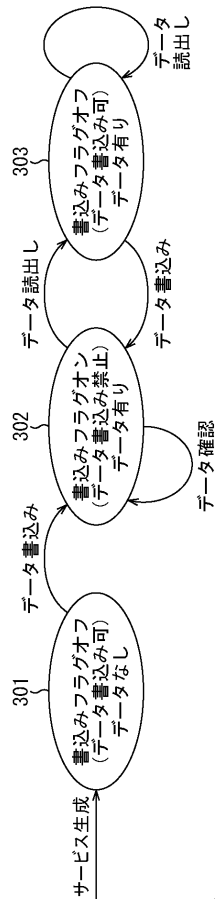
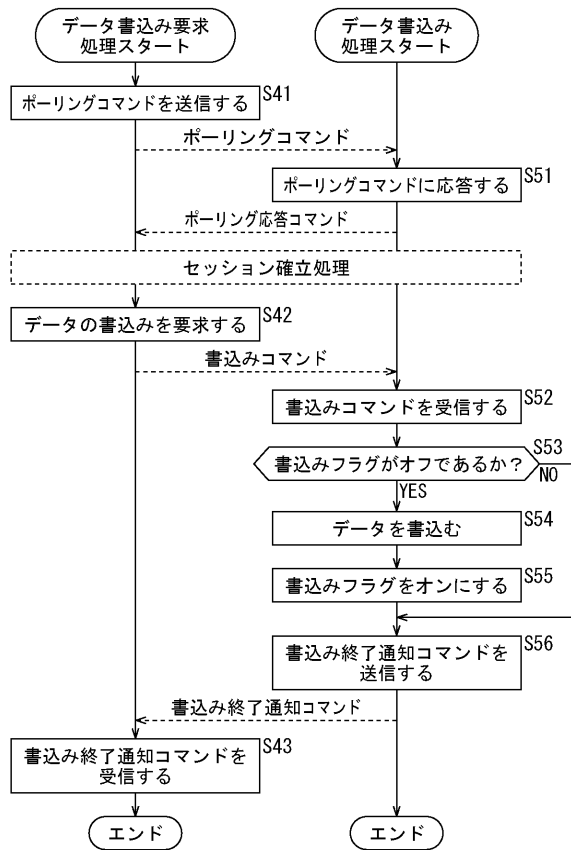
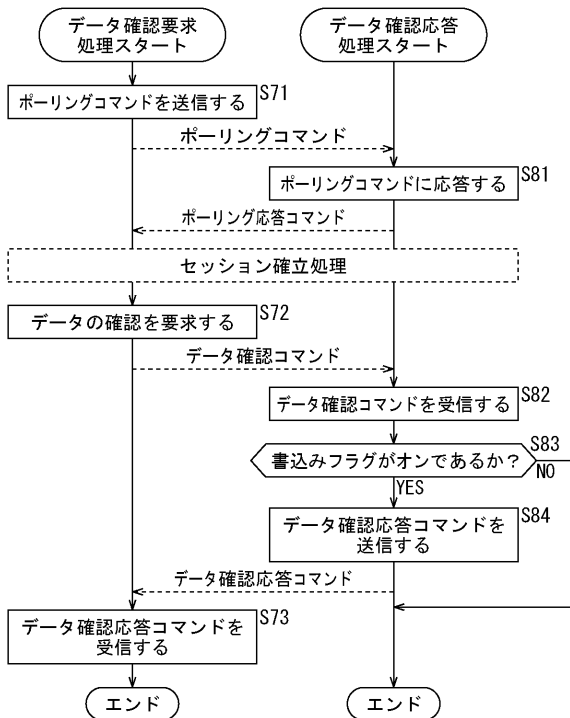
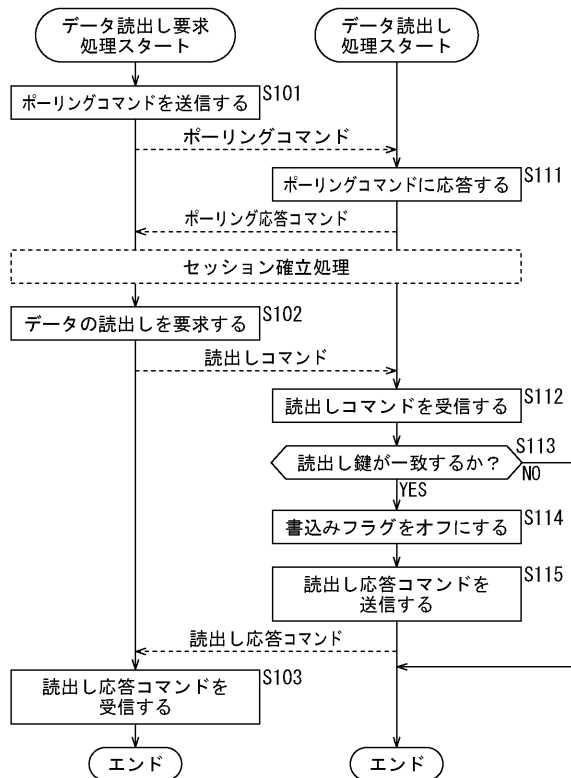
【図 4】



【図 5】

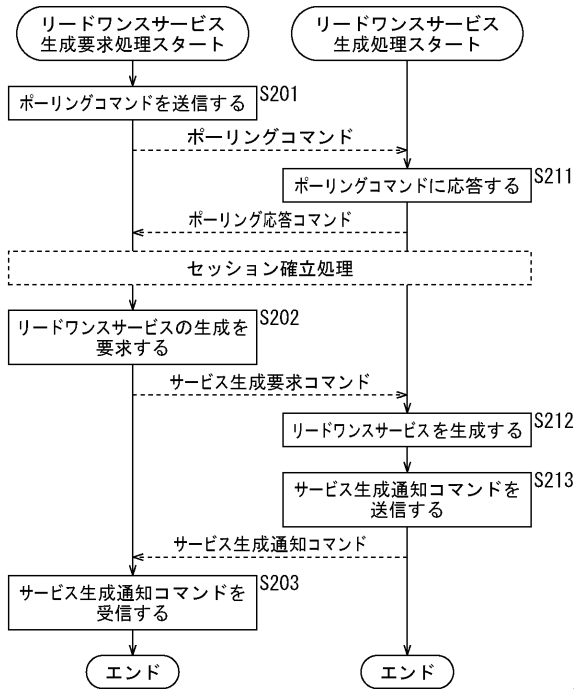


【図 6】
図6【図 7】
図7【図 8】
図8【図 9】
図9

【図 10】
図10【図 11】
図11【図 12】
図12【図 13】
図13

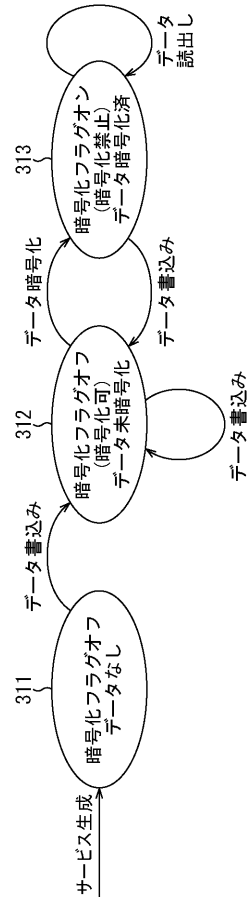
【図 14】

図14



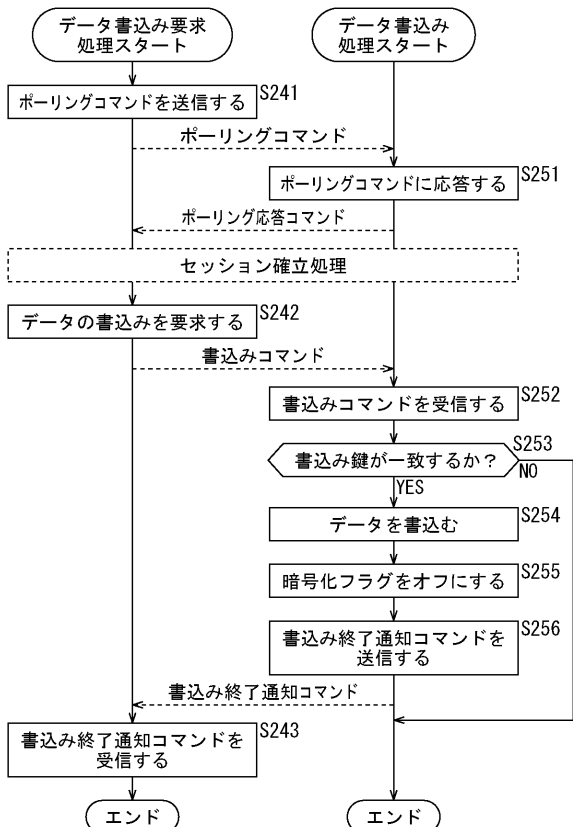
【図 15】

図15



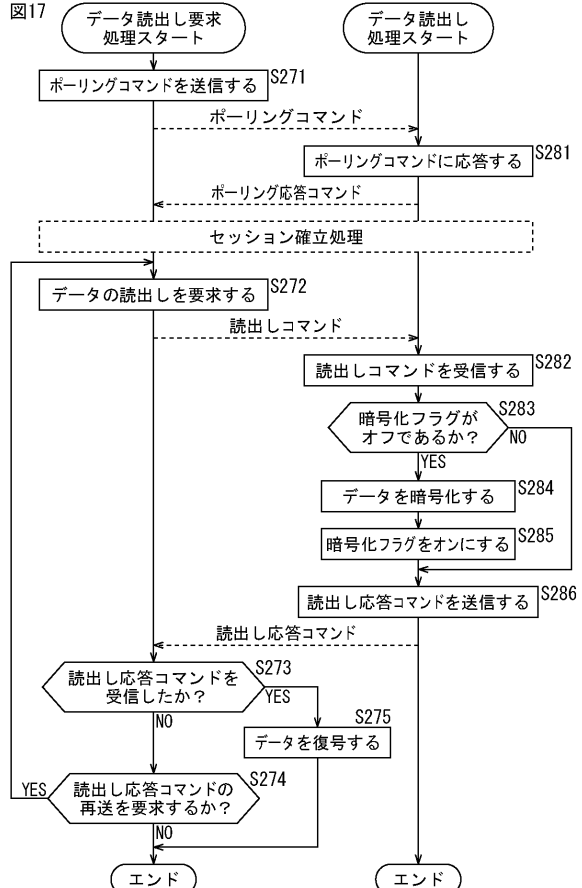
【図 16】

図16



【図 17】

図17



フロントページの続き

(51) Int.Cl.

F I

テーマコード (参考)

H 0 4 L 9/00 6 0 1 A