

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第4706220号
(P4706220)

(45) 発行日 平成23年6月22日 (2011.6.22)

(24) 登録日 平成23年3月25日 (2011.3.25)

(51) Int. Cl.

F I

G06K 19/10 (2006.01)
 G06F 21/02 (2006.01)
 G06F 21/24 (2006.01)
 H04L 9/10 (2006.01)
 G09C 1/00 (2006.01)

G06K 19/00 R
 G06F 12/14 510C
 G06F 12/14 520A
 H04L 9/00 621A
 G09C 1/00 660A

請求項の数 8 (全 37 頁) 最終頁に続く

(21) 出願番号 特願2004-283107 (P2004-283107)
 (22) 出願日 平成16年9月29日 (2004.9.29)
 (65) 公開番号 特開2006-99311 (P2006-99311A)
 (43) 公開日 平成18年4月13日 (2006.4.13)
 審査請求日 平成19年8月2日 (2007.8.2)

前置審査

(73) 特許権者 000002185
 ソニー株式会社
 東京都港区港南1丁目7番1号
 (74) 代理人 100082131
 弁理士 稲本 義雄
 (72) 発明者 吉田 里志
 東京都品川区北品川6丁目7番35号 ソ
 ニー株式会社内
 (72) 発明者 伊藤 勲
 東京都品川区北品川6丁目7番35号 ソ
 ニー株式会社内

審査官 小山 満

最終頁に続く

(54) 【発明の名称】 情報処理装置および方法、記録媒体、並びにプログラム

(57) 【特許請求の範囲】

【請求項1】

送信されてくる、所定の処理の実行を要求する旨の指令を受信する受信手段と、
 所定のデータを記憶するとともに、予め定められた複数の状態であって、記憶している
 前記データによって定まる、ライフサイクルにおける自分自身の状態のうち、自分自身が
 どの状態であるかを示す第1の情報と、前記状態ごとに定められた、前記状態において実
 行可能な指令を示す第2の情報とを記憶する記憶手段と、

前記第1の情報および前記第2の情報を基に、受信した前記指令が、自分自身の前記状
 態において、実行可能な指令であるか否かを判定する判定手段と、

前記記憶手段に前記データとして、ユーザに関するデータが記憶され、少なくとも前記
 ユーザに関するデータの読み出しまたは書き込みの何れかの前記指令を実行可能な第1の
 状態から、前記記憶手段に前記ユーザに関するデータが記憶される前の状態である第2の
 状態に前記状態を変化させる前記指令が受信された場合、前記判定手段の判定結果に応じ
 て、前記第2の状態に前記状態を変化させる前記指令を実行し、前記記憶手段から前記ユ
 ーザに関するデータを消去させるとともに、実行した前記指令に応じて、自分自身の前記
 状態を変化させるように、前記第1の情報の更新を制御する制御手段と

を備えることを特徴とする情報処理装置。

【請求項2】

前記第1の状態および前記第2の状態において、前記記憶手段には、前記データとして
 、前記ユーザに関するデータを利用して前記ユーザにサービスを提供する事業者に関する

10

20

データが記憶されており、

前記制御手段は、前記第1の状態において、前記記憶手段に前記事業者に関するデータが記憶される前の第3の状態に前記状態を変化させる前記指令が受信された場合、前記第3の状態に前記状態を変化させる前記指令を前記判定結果に応じて実行し、前記記憶手段から前記ユーザに関するデータおよび前記事業者に関するデータを消去させるとともに、前記第1の情報の更新を制御する

ことを特徴とする請求項1に記載の情報処理装置。

【請求項3】

前記記憶手段は、自分自身が特定の状態である場合、所定の前記指令を実行できないことを示す情報を含む、前記第2の情報を記憶し、

前記判定手段は、自分自身が前記特定の状態である場合、前記第1の情報および前記第2の情報を基に、受信した前記所定の前記指令が、実行可能な指令でないと判定する

ことを特徴とする請求項1に記載の情報処理装置。

【請求項4】

送信されてくる、所定の処理の実行を要求する旨の指令の受信を制御する受信制御ステップと、

予め定められた複数の状態であって、記憶手段に記憶しているデータによって定まる、ライフサイクルにおける自分自身の状態のうち、自分自身がどの状態であるかを示す第1の情報の記憶を制御する記憶制御ステップと、

前記第1の情報と、前記状態ごとに定められた、前記状態において実行可能な指令を示す第2の情報とを基に、受信した前記指令が、自分自身の前記状態において、実行可能な指令であるか否かを判定する判定ステップと、

前記記憶手段に前記データとして、ユーザに関するデータが記憶され、少なくとも前記ユーザに関するデータの読み出しまたは書き込みの何れかの前記指令を実行可能な第1の状態から、前記記憶手段に前記ユーザに関するデータが記憶される前の状態である第2の状態に前記状態を変化させる前記指令が受信された場合、前記判定ステップにおける判定結果に応じて、前記第2の状態に前記状態を変化させる前記指令を実行し、前記記憶手段から前記ユーザに関するデータを消去させるとともに、実行した前記指令に応じて、自分自身の前記状態を変化させるように、前記第1の情報の更新を制御する制御ステップと

を含むことを特徴とする情報処理方法。

【請求項5】

送信されてくる、所定の処理の実行を要求する旨の指令の受信を制御する受信制御ステップと、

予め定められた複数の状態であって、記憶手段に記憶しているデータによって定まる、ライフサイクルにおける自分自身の状態のうち、自分自身がどの状態であるかを示す第1の情報の記憶を制御する記憶制御ステップと、

前記第1の情報と、前記状態ごとに定められた、前記状態において実行可能な指令を示す第2の情報とを基に、受信した前記指令が、自分自身の前記状態において、実行可能な指令であるか否かを判定する判定ステップと、

前記記憶手段に前記データとして、ユーザに関するデータが記憶され、少なくとも前記ユーザに関するデータの読み出しまたは書き込みの何れかの前記指令を実行可能な第1の状態から、前記記憶手段に前記ユーザに関するデータが記憶される前の状態である第2の状態に前記状態を変化させる前記指令が受信された場合、前記判定ステップにおける判定結果に応じて、前記第2の状態に前記状態を変化させる前記指令を実行し、前記記憶手段から前記ユーザに関するデータを消去させるとともに、実行した前記指令に応じて、自分自身の前記状態を変化させるように、前記第1の情報の更新を制御する制御ステップと

を含む情報処理をコンピュータに実行させることを特徴とするプログラムが記録されている記録媒体。

【請求項6】

送信されてくる、所定の処理の実行を要求する旨の指令の受信を制御する受信制御ステ

10

20

30

40

50

ップと、

予め定められた複数の状態であって、記憶手段に記憶しているデータによって定まる、ライフサイクルにおける自分自身の状態のうち、自分自身がどの状態であるかを示す第1の情報の記憶を制御する記憶制御ステップと、

前記第1の情報と、前記状態ごとに定められた、前記状態において実行可能な指令を示す第2の情報とを基に、受信した前記指令が、自分自身の前記状態において、実行可能な指令であるか否かを判定する判定ステップと、

前記記憶手段に前記データとして、ユーザに関するデータが記憶され、少なくとも前記ユーザに関するデータの読み出しまたは書き込みの何れかの前記指令を実行可能な第1の状態から、前記記憶手段に前記ユーザに関するデータが記憶される前の状態である第2の状態に前記状態を変化させる前記指令が受信された場合、前記判定ステップにおける判定結果に応じて、前記第2の状態に前記状態を変化させる前記指令を実行し、前記記憶手段から前記ユーザに関するデータを消去させるとともに、実行した前記指令に応じて、自分自身の前記状態を変化させるように、前記第1の情報の更新を制御する制御ステップと

を含む情報処理をコンピュータに実行させることを特徴とするプログラム。

【請求項7】

相手との相互認証処理を行い、前記相手が認証されてから、所定のデータの送受信を行う情報処理装置において、

送信されてくる、所定の処理の実行を要求する旨の指令を受信する受信手段と、

予め定められた複数の状態であって、記憶しているデータによって定まる、ライフサイクルにおける自分自身の状態のうち、自分自身がどの状態であるかを示す第1の情報と、前記状態ごとに定められた、前記状態において実行可能な指令を示す第2の情報とを記憶する第1の記憶手段と、

前記第1の情報および前記第2の情報を基に、受信した前記指令が、自分自身の前記状態において、実行可能な指令であるか否かを判定する判定手段と、

前記相手との前記相互認証処理に用いられる認証用データであって、前記状態ごとに関係付けられた、所定のデータを暗号化するか、または復号するための認証用データを記憶する第2の記憶手段と、

前記第2の記憶手段にユーザに関するデータが記憶され、少なくとも前記ユーザに関するデータの読み出しまたは書き込みの何れかの前記指令を実行可能な第1の状態から、前記第2の記憶手段に前記ユーザに関するデータが記憶される前の状態である第2の状態に前記状態を変化させる前記指令が受信された場合、前記判定手段の判定結果に応じて、前記第2の状態に前記状態を変化させる前記指令を実行し、前記第2の記憶手段から、前記ユーザに関するデータと、前記ユーザに関するデータを暗号化するか、または復号するための前記認証用データとを消去させるとともに、実行した前記指令に応じて、自分自身の前記状態を変化させるように、前記第1の情報の更新を制御する制御手段と

を備えることを特徴とする情報処理装置。

【請求項8】

前記第1の状態および前記第2の状態において、前記第2の記憶手段には、前記ユーザに関するデータを利用して前記ユーザにサービスを提供する事業者に関するデータが記憶されており、

前記制御手段は、前記第1の状態において、前記第2の記憶手段に前記事業者に関するデータが記憶される前の第3の状態に前記状態を変化させる前記指令が受信された場合、前記第3の状態に前記状態を変化させる前記指令を前記判定結果に応じて実行し、前記第2の記憶手段から前記ユーザに関するデータ、前記ユーザに関するデータを暗号化するか、または復号するための前記認証用データ、および前記事業者に関するデータを消去させるとともに、前記第1の情報の更新を制御する

ことを特徴とする請求項7に記載の情報処理装置。

【発明の詳細な説明】

【技術分野】

10

20

30

40

50

【0001】

本発明は情報処理装置および方法、記録媒体、並びにプログラムに関し、特に、データの改竄および情報の漏洩を防止することができるようにした情報処理装置および方法、記録媒体、並びにプログラムに関する。

【背景技術】

【0002】

情報処理技術の発達にともない、大量の情報が、通信網を介して通信されるようになってきている。例えば、電子マネーシステムやセキュリティーシステムなどにおいて利用されているＩＣカード（スマートカード）は、各種の処理を行うCPU（Central Processing Unit）や、処理に必要なデータなどを記憶するメモリを内蔵しており、所定のリーダライタに電氣的に接触させた状態で、データの送受信が行われる。

10

【0003】

ところで、ＩＣカードに対して、そのライフサイクルにおいて、サービスを提供するために必要なデータを格納するフォルダを新たに追加したり、また、データへのアクセスに必要な鍵を変更したりするための、いわゆる発券作業が行われる。

【0004】

図１は、従来のＩＣカードのライフサイクルを説明するための図である。

【0005】

まず、ＩＣカードは、所定のカード製造業者によって製造され、サービスを提供するために必要なデータや、データへのアクセスに必要な鍵が記録されていない状態（以下、工場出荷状態と称する）で、ＩＣカードを発券する発券業者に出荷される。

20

【0006】

そして、発券業者によって、ＩＣカードの記憶領域に、データを格納するためのメインフォルダ（MF（Main Folder））が生成され、相互認証処理に用いられる認証鍵を記録する処理（以下、０次発券と称する）が行われる。ＩＣカードは、記憶領域に、データを格納するためのメインフォルダおよび相互認証処理に用いられる認証鍵を記録した状態（以下、０次発券済み状態と称する）で、ＩＣカードを利用して、ユーザに所定のサービスを提供する事業者に出荷される。

【0007】

次に、事業者によって、ＩＣカードに記憶されているメインフォルダ内に、サービスを提供するために必要な記憶領域（DF（Dedicated File））が確保され、その記憶領域にアクセスするために必要な鍵を書き込む処理（以下、１次発券と称する）が行われる。

30

【0008】

さらに、１次発券されたＩＣカードは、メインフォルダにDFおよびDFにアクセスするために必要な鍵が書き込まれた状態（以下、１次発券済み状態と称する）で、事業者の各事業所などの、ユーザに対してサービスを提供する施設に配布される。

【0009】

そして、各事業所において、１次発券済み状態のＩＣカードのDFに、ユーザがサービスを受けるために必要な個人情報などのデータおよびそのデータにアクセスするために必要な鍵を書き込む処理（以下、２次発券と称する）が行われ、そのＩＣカードがユーザに配布される。

40

【0010】

ユーザは、事業所から配布された、ユーザがサービスを受けるために必要な個人情報などのデータおよびそのデータにアクセスするために必要な鍵が書き込まれた状態（以下、２次発券済み状態と称する）のＩＣカードを利用して、事業者から提供されるサービスを受ける。

【0011】

また、ユーザによって利用され、不要になったＩＣカードは、事業者によって回収される。事業者は、回収したＩＣカードが記憶している全てのデータを消去（削除）し、データが記録されていない状態（廃棄可能状態）のＩＣカードを、ＩＣカードを物理的に廃棄

50

する廃棄業者に配送する。そして、廃棄業者は、配送されてきた廃棄可能状態のＩＣカードを廃棄する。

【００１２】

このようにして、ＩＣカードのライフサイクルの各状態において、ＩＣカードを発券する発券作業が行われる。

【００１３】

また、従来のＩＣカードとして、ＩＣカードの発券作業において、発券機から送信されてきた、暗号化された発券情報を受信し、受信した発券情報を復号しているものもある（例えば、特許文献１参照）。すなわち、このＩＣカードにおいては、受信した発券情報を復号し、復号した発券情報を記録することによって、ＩＣカードの発券が行われる。

10

【００１４】

【特許文献１】特開２０００－３６０１４号公報

【発明の開示】

【発明が解決しようとする課題】

【００１５】

しかしながら、上述した技術においては、ＩＣカードのライフサイクルにおける各状態において、ＩＣカードが実行可能な処理が異なっているにも関わらず、ＩＣカードは、ＩＣカードの各状態において、本来処理されないコマンドを含む、全てのコマンドを受信し、受信したコマンドを実行してしまうという問題があった。

20

【００１６】

また、通信する相手との相互認証処理に用いられる認証鍵は、ＩＣカードのライフサイクルの各状態において同一の鍵が用いられているため、認証鍵を保持している発券業者または事業者は、ＩＣカードに本来処理されないコマンドを送信し、ＩＣカードに送信したコマンドを実行させることができるという問題があった。

【００１７】

さらに、ＩＣカードを廃棄可能状態にする場合、ＩＣカードに記録されているデータを消去したり、相互認証処理に用いられる認証鍵を変更することはできたが、ＩＣカードが、本来処理されないコマンドを含む、全てのコマンドを受信し、コマンドを実行してしまうため、消去したデータが復元されてしまう恐れがあった。

30

【００１８】

したがって、データの改竄や情報の漏洩を防止することが非常に困難であるという課題があった。

【００１９】

本発明は、このような状況に鑑みてなされたものであり、ＩＣカードのライフサイクルにおける各状態において、実行できる処理を制限することができるようにするものである。また、ＩＣカードのライフサイクルにおける各状態において、異なる認証鍵を用いて、相互認証の処理を行うことが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】

【００２０】

本発明の情報処理装置は、送信されてくる、所定の処理の実行を要求する旨の指令を受信する受信手段と、所定のデータを記憶するとともに、予め定められた複数の状態であって、記憶しているデータによって定まる、ライフサイクルにおける自分自身の状態のうち、自分自身がどの状態であることを示す第１の情報と、状態ごとに定められた、状態において実行可能な指令を示す第２の情報とを記憶する記憶手段と、第１の情報および第２の情報を基に、受信した指令が、自分自身の状態において、実行可能な指令であるか否かを判定する判定手段と、記憶手段にデータとして、ユーザに関するデータが記憶され、少なくともユーザに関するデータの読み出しまたは書き込みの何れかの指令を実行可能な第１の状態から、記憶手段にユーザに関するデータが記憶される前の状態である第２の状態に状態を変化させる指令が受信された場合、判定手段の判定結果に応じて、第２の状態に状態を変化させる指令を実行し、記憶手段からユーザに関するデータを消去させるとともに、

40

50

実行した指令に応じて、自分自身の状態を変化させるように、第1の情報の更新を制御する制御手段とを備えることを特徴とする。

【0021】

第1の状態および第2の状態において、記憶手段には、データとして、ユーザに関するデータを利用してユーザにサービスを提供する事業者に関するデータが記憶されるようにし、制御手段には、第1の状態において、記憶手段に事業者に関するデータが記憶される前の第3の状態にライフサイクルの状態を変化させる指令が受信された場合、第3の状態に状態を変化させる指令を判定結果に応じて実行させ、記憶手段からユーザに関するデータおよび事業者に関するデータを消去させるとともに、第1の情報の更新を制御させることができる。

10

【0022】

記憶手段は、自分自身が特定の状態である場合、所定の指令を実行できないことを示す情報を含む、第2の情報を記憶し、判定手段は、自分自身が特定の状態である場合、第1の情報および第2の情報を基に、受信した所定の指令が、実行可能な指令でないと判定するようにすることができる。

【0023】

本発明の情報処理方法、記録媒体のプログラム、またはプログラムは、送信されてくる、所定の処理の実行を要求する旨の指令の受信を制御する受信制御ステップと、予め定められた複数の状態であって、記憶手段に記憶しているデータによって定まる、ライフサイクルにおける自分自身の状態のうち、自分自身がどの状態であることを示す第1の情報の記憶を制御する記憶制御ステップと、第1の情報と、状態ごとに定められた、状態において実行可能な指令を示す第2の情報とを基に、受信した指令が、自分自身の状態において、実行可能な指令であるか否かを判定する判定ステップと、記憶手段にデータとして、ユーザに関するデータが記憶され、少なくともユーザに関するデータの読み出しまたは書き込みの何れかの指令を実行可能な第1の状態から、記憶手段にユーザに関するデータが記憶される前の状態である第2の状態に状態を変化させる指令が受信された場合、判定ステップにおける判定結果に応じて、第2の状態に状態を変化させる指令を実行し、記憶手段からユーザに関するデータを消去させるとともに、実行した指令に応じて、自分自身の状態を変化させるように、第1の情報の更新を制御する制御ステップとを含むことを特徴とする。

20

30

【0026】

本発明の情報処理装置は、送信されてくる、所定の処理の実行を要求する旨の指令を受信する受信手段と、予め定められた複数の状態であって、記憶しているデータによって定まる、ライフサイクルにおける自分自身の状態のうち、自分自身がどの状態であることを示す第1の情報と、状態ごとに定められた、状態において実行可能な指令を示す第2の情報とを記憶する第1の記憶手段と、第1の情報および第2の情報を基に、受信した指令が、自分自身の状態において、実行可能な指令であるか否かを判定する判定手段と、相手との相互認証処理に用いられる認証用データであって、状態ごとに関係付けられた、所定のデータを暗号化するか、または復号するための認証用データを記憶する第2の記憶手段と、第2の記憶手段にユーザに関するデータが記憶され、少なくともユーザに関するデータの読み出しまたは書き込みの何れかの指令を実行可能な第1の状態から、第2の記憶手段にユーザに関するデータが記憶される前の状態である第2の状態に状態を変化させる指令が受信された場合、判定手段の判定結果に応じて、第2の状態に状態を変化させる指令を実行し、第2の記憶手段から、ユーザに関するデータと、ユーザに関するデータを暗号化するか、または復号するための認証用データとを消去させるとともに、実行した指令に応じて、自分自身の状態を変化させるように、第1の情報の更新を制御する制御手段とを備えることを特徴とする。

40

【0027】

第1の状態および第2の状態において、第2の記憶手段には、ユーザに関するデータを利用してユーザにサービスを提供する事業者に関するデータが記憶されてるようにし、制

50

御手段には、第1の状態において、第2の記憶手段に事業者に関するデータが記憶される前の第3の状態に状態を変化させる指令が受信された場合、第3の状態に状態を変化させる指令を判定結果に応じて実行させ、第2の記憶手段からユーザに関するデータ、ユーザに関するデータを暗号化するか、または復号するための認証用データ、および事業者に関するデータを消去させるとともに、第1の情報の更新を制御させることができる。

【0028】

本発明の情報処理装置および方法、記録媒体、並びにプログラムにおいては、送信されてくる、所定の処理の実行を要求する旨の指令が受信され、所定のデータが記憶されるとともに、予め定められた複数の状態であって、記憶手段に記憶しているデータによって定まる、ライフサイクルにおける自分自身の状態のうち、自分自身がどの状態であるかを示す第1の情報と、状態ごとに定められた、状態において実行可能な指令を示す第2の情報とが記憶され、第1の情報および第2の情報を基に、受信した指令が、自分自身の状態において、実行可能な指令であるか否かが判定され、記憶手段にデータとして、ユーザに関するデータが記憶され、少なくともユーザに関するデータの読み出しまたは書き込みの何れかの指令を実行可能な第1の状態から、記憶手段にユーザに関するデータが記憶される前の状態である第2の状態に状態を変化させる指令が受信された場合、判定結果に応じて、第2の状態に状態を変化させる指令が実行され、記憶手段からユーザに関するデータが消去されるとともに、実行した指令に応じて、自分自身の状態を変化させるように、第1の情報の更新が制御される。

【0029】

本発明の情報処理装置においては、送信されてくる、所定の処理の実行を要求する旨の指令が受信され、予め定められた複数の状態であって、記憶しているデータによって定まる、ライフサイクルにおける自分自身の状態のうち、自分自身がどの状態であるかを示す第1の情報と、状態ごとに定められた、状態において実行可能な指令を示す第2の情報とが記憶される。そして、第1の情報および第2の情報を基に、受信した指令が、自分自身の状態において、実行可能な指令であるか否かが判定され、相手との相互認証処理に用いられる認証用データであって、状態ごとに関係付けられた、所定のデータを暗号化するか、または復号するための認証用データが記憶され、第2の記憶手段にユーザに関するデータが記憶され、少なくともユーザに関するデータの読み出しまたは書き込みの何れかの指令を実行可能な第1の状態から、第2の記憶手段にユーザに関するデータが記憶される前の状態である第2の状態に状態を変化させる指令が受信された場合、判定結果に応じて、第2の状態に状態を変化させる指令が実行され、第2の記憶手段から、ユーザに関するデータと、ユーザに関するデータを暗号化するか、または復号するための認証用データとが消去されるとともに、実行した指令に応じて、自分自身の状態を変化させるように、第1の情報の更新が制御される。

【0030】

また、通信とは、無線通信および有線通信は勿論、無線通信と有線通信とが混在した通信、即ち、ある区間では無線通信が行われ、他の区間では有線通信が行われるようなものであっても良い。さらに、ある装置から他の装置への通信が有線通信で行われ、他の装置からある装置への通信が無線通信で行われるようなものであっても良い。

【発明の効果】

【0031】

本発明によれば、情報の改竄および漏洩を防止することができる。

【発明を実施するための最良の形態】

【0032】

以下に本発明の実施の形態を説明するが、本明細書に記載の発明と、発明の実施の形態との対応関係を例示すると、次のようになる。この記載は、本明細書に記載されている発明をサポートする実施の形態が本明細書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、発明に対応するものとして、ここには記載されていない実施の形態があったとしても、そのことは、その実施の形態が、

その発明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、実施の形態が発明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、その実施の形態が、その発明以外の発明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。

【0033】

さらに、この記載は、本明細書に記載されている発明の全てを意味するものではない。換言すれば、この記載は、本明細書に記載されている発明であって、この出願では請求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、補正により出現、追加される発明の存在を否定するものではない。

【0034】

請求項1に記載の情報処理装置は、送信されてくる、所定の処理の実行を要求する旨の指令を受信する受信手段（例えば、図5のアンテナ101）と、所定のデータを記憶するとともに、予め定められた複数の状態であって、記憶しているデータによって定まる、ライフサイクルにおける自分自身の状態のうち、自分自身がどの状態であるかを示す第1の情報（例えば、図8に示すライフサイクル状態テーブル）と、状態ごとに定められた、状態において実行可能な指令を示す第2の情報（例えば、図9に示すコマンドテーブル）とを記憶する記憶手段（例えば、図5のテーブル保持部108）と、第1の情報および第2の情報を基に、受信した指令が、自分自身の状態において、実行可能な指令であるか否かを判定する判定手段（例えば、図5の判定部131）と、記憶手段にデータとして、ユーザに関するデータが記憶され、少なくともユーザに関するデータの読み出しまたは書き込みの何れかの指令を実行可能な第1の状態から、記憶手段にユーザに関するデータが記憶される前の状態である第2の状態に状態を変化させる指令が受信された場合、判定手段の判定結果に応じて、第2の状態に状態を変化させる指令を実行し、記憶手段からユーザに関するデータを消去させるとともに、実行した指令に応じて、自分自身の状態を変化させるように、第1の情報の更新を制御する制御手段（例えば、図5の制御部104）とを備えることを特徴とする。

【0039】

請求項7に記載の情報処理装置は、送信されてくる、所定の処理の実行を要求する旨の指令を受信する受信手段（例えば、図5のアンテナ101）と、予め定められた複数の状態であって、記憶しているデータによって定まる、ライフサイクルにおける自分自身の状態のうち、自分自身がどの状態であるかを示す第1の情報（例えば、図8に示すライフサイクル状態テーブル）と、状態ごとに定められた、状態において実行可能な指令を示す第2の情報（例えば、図9に示すコマンドテーブル）とを記憶する第1の記憶手段（例えば、図5のテーブル保持部108）と、第1の情報および第2の情報を基に、受信した指令が、自分自身の状態において、実行可能な指令であるか否かを判定する判定手段（例えば、図5の判定部131）と、相手との相互認証処理に用いられる認証用データ（例えば、図12を参照して説明する出荷鍵Aおよび出荷鍵B）であって、状態ごとに関係付けられた、所定のデータを暗号化するか、または復号するための認証用データを記憶する第2の記憶手段（例えば、図5の記録部107）と、第2の記憶手段にユーザに関するデータが記憶され、少なくともユーザに関するデータの読み出しまたは書き込みの何れかの指令を実行可能な第1の状態から、第2の記憶手段にユーザに関するデータが記憶される前の状態である第2の状態に状態を変化させる指令が受信された場合、判定手段の判定結果に応じて、第2の状態に状態を変化させる指令を実行し、第2の記憶手段から、ユーザに関するデータと、ユーザに関するデータを暗号化するか、または復号するための認証用データとを消去させるとともに、実行した指令に応じて、自分自身の状態を変化させるように、第1の情報の更新を制御する制御手段（例えば、図5の制御部104）とを備えることを特徴とする。

【0041】

本発明は、有線または無線の通信網を介して、データを送受信する情報処理システム、ICカードを利用した電子マネーシステムまたはセキュリティーシステムなどに適用できる。

【0042】

以下、図を参照して本発明を適用した実施の形態について説明する。

【0043】

図2は、本発明に係るICカードのライフサイクルを説明する図である。

【0044】

ICカードは、所定のカード製造業者によって製造され、サービスを提供するために必要なデータや、データへのアクセスに必要な鍵が記録されていない状態（以下、工場出荷状態と称する）で、ICカードを発券する発券業者に出荷される。工場出荷状態のICカードには、ICカードを製造したカード製造業者を特定するための情報である、製造者番号が記録されている。

10

【0045】

ここで、ICカードのライフサイクルにおける各状態は、ICカードが記録しているデータによって定まり、発券を行うためのコマンドなど、所定のコマンドを実行することにより、ICカードの状態は変化する。

【0046】

発券業者は、発券機（リーダライタ）を操作することによって、工場出荷状態であるICカードに、0次発券を行う旨の0次発券コマンドを送信し、ICカードに所定の処理を実行させることによって、0次発券を行う。

【0047】

工場出荷状態であるICカードは、リーダライタから送信されてきた、0次発券コマンドを受信し、受信した0次発券コマンドを実行する。この場合、例えば、ICカードは、0次発券コマンドに含まれている、ICカードを特定するための情報であるデバイス識別番号、サービスを提供するために必要なデータを格納するためのMF、および事業者との相互認証処理に用いられる認証鍵である、出荷鍵を記録する。

20

【0048】

発券業者は、0次発券が行われた状態（以下、0次発券済み状態と称する）のICカードを、ICカードを利用して、ユーザに所定のサービスを提供する事業者に出荷する。

【0049】

事業者は、リーダライタを操作することによって、0次発券済み状態であるICカードに、1次発券を行う旨の1次発券コマンドを送信し、ICカードに所定の処理を実行させることによって、1次発券を行う。

30

【0050】

0次発券済み状態であるICカードは、リーダライタから送信されてきた、1次発券コマンドを受信し、受信した1次発券コマンドを実行する。この場合、例えば、ICカードは、1次発券コマンドに基づいて、サービスを利用するために必要なデータを格納するためのDFおよびEF（Elementary File）、DFまたはEFにアクセスするために必要な認証鍵などを、MFに従属するデータとして記録する。

【0051】

ここで、DFは、フォルダやディレクトリに相当し、DFには、ファイルに相当するEFが格納される。なお、DFおよびEFは、ISO（International Organization for Standardization）7816に規定されている。

40

【0052】

事業者は、1次発券が行われた状態（以下、1次発券済み状態と称する）のICカードを、事業者の各事業所などの、ユーザに対してサービスを提供する施設に配布する。

【0053】

ICカードが配布された事業所において、事業者は、リーダライタを操作することによって、1次発券済み状態であるICカードに、2次発券を行う旨の2次発券コマンドまたは、ICカードに記録されているデータを消去（削除）し、ICカードを0次発券済み状態にする旨のオールリセットコマンドを送信し、ICカードに所定の処理を実行させる。

【0054】

50

例えば、ＩＣカードは、リーダライタから送信されてきたオールリセットコマンドを受信すると、記録しているＤＦ、ＥＦ、ＤＦまたはＥＦにアクセスするために必要な認証鍵などを削除する。オールリセットコマンドを実行したＩＣカードの状態（ライフサイクル状態）は、０次発券状態に戻る。

【００５５】

また、例えば、ＩＣカードは、リーダライタから送信されてきた２次発券コマンドを受信すると、２次発券コマンドに基づいて、記録しているＤＦに従属するデータとして、ユーザがサービスを受けるために必要な個人情報などのデータおよびそのデータにアクセスするために必要な認証鍵を記録する。

【００５６】

換言すれば、ＩＣカードは、２次発券コマンドに基づいて、記録しているＤＦに従属するデータとして、ユーザがサービスを受けるために必要な個人情報などのデータおよびそのデータにアクセスするために必要な認証鍵をＥＦに格納する。

【００５７】

また、事業所において、事業者は、リーダライタを操作することによって、２次発券済み状態であるＩＣカードに、ＩＣカードに記録されているデータを消去し、ＩＣカードを０次発券済み状態にする旨のオールリセットコマンド、またはＩＣカードに記録されているユーザの個人情報などを消去し、ＩＣカードを１次発券済み状態にする旨のデータリセットコマンドを送信し、ＩＣカードに所定の処理を実行させる。

【００５８】

例えば、ＩＣカードは、リーダライタから送信されてきたオールリセットコマンドを受信すると、記録しているＤＦおよびＥＦ、ＤＦまたはＥＦにアクセスするために必要な認証鍵などを削除する。オールリセットコマンドを実行したＩＣカードのライフサイクル状態は、０次発券状態に戻る。

【００５９】

また、例えば、ＩＣカードは、リーダライタから送信されてきたデータリセットコマンドを受信すると、記録しているユーザがサービスを受けるために必要な個人情報などのデータおよびそのデータにアクセスするために必要な認証鍵などを削除する。データリセットコマンドを実行したＩＣカードのライフサイクル状態は、１次発券状態に戻る。

【００６０】

２次発券が行われた状態（２次発券済み状態）のＩＣカードは、各事業所において、ユーザに配布される。ユーザは、ユーザの個人情報などが記録されている、２次発券済み状態のＩＣカードを、例えば、電子的な定期券や財布として利用し、事業者から提供されるサービスを受ける。

【００６１】

ユーザによって利用され、不要になったＩＣカードは、事業者によって回収される。ユーザからＩＣカードを回収した事業者は、リーダライタを操作することによって、２次発券済み状態であるＩＣカードに、ＩＣカードに記録されているデータを消去し、ＩＣカードが、如何なるコマンドも実行しない状態（廃棄可能状態）にする旨のターミネートコマンドを送信し、ＩＣカードに所定の処理を実行させる。

【００６２】

例えば、ＩＣカードは、リーダライタから送信されてきたターミネートコマンドを受信すると、記録しているデータを消去する。ターミネートコマンドを実行したＩＣカードのライフサイクル状態は、廃棄可能状態となり、廃棄可能状態のＩＣカードは、如何なるコマンドも実行しない。

【００６３】

そして、ユーザからＩＣカードを回収した事業者は、廃棄可能状態のＩＣカードを、ＩＣカードを物理的に廃棄する廃棄業者に配送する。廃棄業者は、配送されてきた廃棄可能状態のＩＣカードを廃棄する。

【００６４】

このようにして、ＩＣカードのライフサイクルの各状態において、ＩＣカードの発券作業が行われる。なお、ＩＣカードは、自分自身のライフサイクル状態および各状態において実行できるコマンドを示す情報を記憶しており、各状態において、実行できるコマンドとして記憶されていないコマンドの実行が指示されても、そのコマンドを実行しない。

【００６５】

ＩＣカードは、ライフサイクルの各状態において、リーダライタから送信されてきた各種のコマンドを受信し、受信したコマンドを実行する。

【００６６】

ここで、図３は、リーダライタおよびＩＣカードからなる無線通信システムを説明する図である。この無線通信システムは、無線通信するリーダライタ１１およびＩＣカード１２から構成され、リーダライタ１１とＩＣカード１２との間では、電磁波を利用して非接触でのデータの送受信が行われるようになされている。

10

【００６７】

リーダライタ１１は、電波（電磁波）を放射し、例えば、ポーリングなどの処理を行うことによって、ＩＣカード１２を検出する。

【００６８】

ＩＣカード１２がリーダライタ１１に近接し、リーダライタ１１によって、ＩＣカード１２が検出されると、リーダライタ１１およびＩＣカード１２は、必要に応じて、所定のデータを送受信することによって、相互認証処理を行う。

【００６９】

20

そして、相互認証処理によって、認証がなされると、リーダライタ１１は、ＩＣカード１２に対して、発券を行うための処理など、所定の処理を実行させるためのコマンドを生成し、生成したコマンドを、無線通信によりＩＣカード１２あてに送信する。

【００７０】

ＩＣカード１２は、リーダライタ１１から送信されてきたコマンドを受信し、記憶しているＩＣカード１２のライフサイクル状態および各状態において実行できるコマンドを示す情報を基に、受信したコマンドが、ＩＣカード１２のライフサイクル状態において実行できるコマンドであるか否かを判定する。

【００７１】

ＩＣカード１２は、受信したコマンドが、ＩＣカード１２のライフサイクル状態において実行できるコマンドであると判定された場合、受信したコマンドを実行する。また、ＩＣカード１２は、受信したコマンドが、ＩＣカード１２のライフサイクル状態において実行できるコマンドでないと判定された場合、受信したコマンドを実行しない。

30

【００７２】

したがって、例えば、ＩＣカード１２のライフサイクル状態が、工場出荷状態であり、工場出荷状態において、０次発券を行うためのコマンドだけが実行できる場合、ＩＣカード１２が１次発券を行うためのコマンドを受信したとき、ＩＣカード１２は、受信したコマンドが、ＩＣカード１２のライフサイクル状態において実行できるコマンドでないと判定し、受信した１次発券を行うためのコマンドを実行しない。

【００７３】

40

また、ＩＣカード１２のライフサイクル状態が、廃棄可能状態である場合には、ＩＣカード１２は、相互認証処理を行わず、また、受信したコマンドも実行しない。

【００７４】

図４は、リーダライタ１１の機能の構成を示すブロック図である。

【００７５】

リーダライタ１１は、制御部３１、記録部３２、ＳＰＵ（Signal Processing Unit）３３、変調部３４、発振回路３５、アンテナ３６、復調部３７、およびドライバ３８を含むように構成される。

【００７６】

制御部３１は、ＩＣカード１２に対して、所定の処理を実行させる、各種のコマンドを

50

生成し、生成したコマンドをSPU 3 3 に供給する。例えば、制御部 3 1 は、0 次発券コマンド、オールリセットコマンド、ターミネートコマンド、または相互認証を行うためのコマンド（以下、相互認証コマンドとも称する）を生成し、生成したコマンドを、SPU 3 3 に供給する。

【0077】

制御部 3 1 は、暗号化部 5 1 および復号部 5 2 を備えている。制御部 3 1 は、必要に応じて、各種のコマンドに格納するデータを生成する。制御部 3 1 の暗号化部 5 1 は、制御部 3 1 が生成した、コマンドに格納するデータを、必要に応じて、記録部 3 2 に記録されている相互認証を行うための認証鍵を用いて、暗号化する。例えば、制御部 3 1 の暗号化部 5 1 は、制御部 3 1 が生成した、相互認証を行うためのコマンドに格納するデータを、記録部 3 2 に記録されている認証鍵を用いて、暗号化する。

10

【0078】

制御部 3 1 の復号部 5 2 は、SPU 3 3 から供給されたデータを、必要に応じて記録部 3 2 に記録されている認証鍵を用いて復号する。すなわち、制御部 3 1 の復号部 5 2 は、SPU 3 3 から供給されたデータが、所定の方式により暗号化されている場合、記録部 3 2 に記録されている認証鍵を用いて、暗号化方式に対応する復号方式により、SPU 3 3 から供給されたデータを復号する。制御部 3 1 は、制御部 3 1 の復号部 5 2 が復号したデータを、必要に応じて記録部 3 2 に供給する。

【0079】

制御部 3 1 の復号部 5 2 は、SPU 3 3 から供給されたデータが暗号化されていない場合、SPU 3 3 から供給されたデータを復号しない。

20

【0080】

制御部 3 1 は、必要に応じて装着された、ドライブ 3 8 から供給されたプログラムを読み込んで、読み込んだプログラムを実行する。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 に供給し、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する。

【0081】

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、各種のデータを記録している。また、記録部 3 2 は、記録しているデータを制御部 3 1 に供給する。

30

【0082】

記録部 3 2 は、IC カード 1 2 が記録しているデータに関係付けられた認証鍵を記録している。記録部 3 2 は、記録している認証鍵を制御部 3 1 に供給する。また、記録部 3 2 は、制御部 3 1 から供給されたデータを記録する。

【0083】

SPU 3 3 は、制御部 3 1 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 3 4 に供給する。また、SPU 3 3 は、復調部 3 7 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 3 1 に供給する。

40

【0084】

例えば、SPU 3 3 は、IC カード 1 2 あてに送信するコマンドが、制御部 3 1 から供給されてきた場合、そのコマンドに、例えば、マンチェスター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 3 4 に出力する。また、SPU 3 3 は、IC カード 1 2 からのデータが復調部 3 7 から供給されてきた場合、そのデータに対して、例えば、マンチェスター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、制御部 3 1 に供給する。

【0085】

変調部 3 4 は、発振回路 3 5 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

50

波を生成する。変調部 3 4 は、搬送波に基づいて、SPU 3 3 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 3 6 に供給する。例えば、変調部 3 4 は、SPU 3 3 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。

【0086】

より具体的には、例えば、変調部 3 4 は、発振回路 3 5 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、SPU 3 3 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 3 6 から出力させる。

【0087】

発振回路 3 5 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 3 4 に供給する。

【0088】

アンテナ 3 6 は、変調部 3 4 から供給されたコマンドを、無線通信により IC カード 1 2 へてに送信する。すなわち、例えば、アンテナ 3 6 は、変調部 3 4 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 3 6 は、IC カード 1 2 から送信されてきたデータを受信し、受信したデータを復調部 3 7 に供給する。

【0089】

復調部 3 7 は、アンテナ 3 6 から供給されたデータを、変調部 1 1 0（図 5）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 SPU 3 3 に供給する。例えば、復調部 3 7 は、アンテナ 3 6 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 SPU 3 3 に出力する。

【0090】

ドライブ 3 8 は、磁気ディスク 7 1、光ディスク 7 2、光磁気ディスク 7 3、或いは半導体メモリ 7 4 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 3 1 または IC カード 1 2 に転送される。また、IC カード 1 2 に転送（送信）されたプログラムは、IC カード 1 2 により、必要に応じて記録されるか、または実行される。

【0091】

図 5 は、IC カード 1 2 の機能の構成を示すブロック図である。

【0092】

IC カード 1 2 は、アンテナ 1 0 1、復調部 1 0 2、SPU 1 0 3、制御部 1 0 4、ROM (Read Only Memory) 1 0 5、RAM (Random Access Memory) 1 0 6、記録部 1 0 7、テーブル保持部 1 0 8、発振回路 1 0 9、変調部 1 1 0、および電力発生部 1 1 1 を含むように構成される。

【0093】

アンテナ 1 0 1 は、リーダライタ 1 1 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 1 0 2 に供給する。また、アンテナ 1 0 1 は、変調部 1 1 0 から供給されたデータを、無線通信により、リーダライタ 1 1 へてに送信する。すなわち、例えば、アンテナ 1 0 1 は、変調部 1 1 0 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 1 0 1 においては、リーダライタ 1 1 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。

【0094】

復調部 1 0 2 は、アンテナ 1 0 1 から供給されたコマンドを、変調部 3 4（図 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 SPU 1 0 3 に供給する。例えば、復調部 1 0 2 は、アンテナ 1 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 SPU 1 0 3 に出力する。

【0095】

SPU 1 0 3 は、復調部 1 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 1 0 4 に供給する。SPU 1 0 3 は、制御部 1 0 4 から供給されたデ

10

20

30

40

50

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 110 に供給する。例えば、SPU 103 は、復調部 102 において復調されたコマンドがマンチェスター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 (マンチェスターコードのデコード) を行い、復号したコマンドを制御部 104 に供給する。例えば、SPU 103 は、制御部 104 から供給されたデータを、マンチェスター方式で符号化し、符号化したデータを変調部 110 に供給する。

【0096】

制御部 104 は SPU 103 から供給された各種のコマンドを実行する。制御部 104 は、判定部 131、暗号化部 132、および復号部 133 を備えている。

10

【0097】

制御部 104 の判定部 131 は、テーブル保持部 108 に保持されているライフサイクル状態テーブルおよびコマンドテーブルを基に、SPU 103 から供給されたコマンドが、IC カード 12 のライフサイクル状態において、実行してもよいコマンドであるか否かを判定する。

【0098】

ここで、ライフサイクル状態テーブルには、IC カード 12 のライフサイクル状態を示す情報が含まれている。また、コマンドテーブルには、IC カード 12 の各ライフサイクル状態において、IC カード 12 が実行することができるコマンドを示す情報が含まれている。なお、ライフサイクル状態テーブルおよびコマンドテーブルの詳細は、後述する。

20

【0099】

制御部 104 は、SPU 103 から供給されたコマンドが、IC カード 12 のライフサイクル状態において、実行してもよいコマンドであると判定された場合、SPU 103 から供給されたコマンドを実行する。また、制御部 104 は、SPU 103 から供給されたコマンドが、IC カード 12 のライフサイクル状態において、実行してもよいコマンドでないと判定された場合、SPU 103 から供給されたコマンドを実行しない。

【0100】

例えば、制御部 104 は、SPU 103 から相互認証を行うためのコマンドが供給されると、供給された相互認証を行うためのコマンドを実行する。このとき、例えば、制御部 104 の暗号化部 132 は、相互認証を行うために必要な、乱数、タイムスタンプなどのデータを、記録部 107 に記録されている認証鍵を用いて暗号化する。制御部 104 は、制御部 104 の暗号化部 132 が暗号化したデータを SPU 103 に供給する。

30

【0101】

また、例えば、制御部 104 は、SPU 103 から供給されたコマンドに応じて、記録部 107 を制御し、記録部 107 に記録されているデータを消去させるか、または上書きさせる (書き換える)。

【0102】

制御部 104 の復号部 133 は、SPU 103 から供給されたコマンドに含まれているデータが、所定の方式により暗号化されている場合、記録部 107 に記録されている認証鍵を用いて、暗号化方式に対応する復号方式により、SPU 103 から供給されたコマンドに含まれているデータを復号する。制御部 104 は、制御部 104 の復号部 133 が復号したデータを、必要に応じて記録部 107 に供給する。また、制御部 104 の復号部 133 は、SPU 103 から供給されたコマンドに含まれているデータが、暗号化されていない場合、データを復号しない。

40

【0103】

制御部 104 は、テーブル保持部 108 を制御し、テーブル保持部 108 が保持しているライフサイクル状態テーブルを更新させる。例えば、制御部 104 が、0 次発券コマンドを実行することによって、0 次発券を行った場合、制御部 104 は、テーブル保持部 108 を制御し、ライフサイクル状態が 0 次発券済み状態であることを示すように、ライフサイクル状態テーブルを更新させる。

50

【0104】

制御部104は、必要に応じて、ROM105に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する。制御部104は、必要に応じて、データをRAM106に供給する。また、制御部104は、必要に応じて、RAM106が一時的に記憶しているデータを取得する。

【0105】

ROM105は、制御部104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。ROM105は、記録しているプログラム、その他のデータなどを制御部104に供給する。

【0106】

RAM106は、制御部104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。RAM106は、記憶しているデータを制御部104に供給する。

【0107】

記録部107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に送信される、秘匿すべきデータなどの各種データを記録している。また、記録部107は、リーダライタ11との相互認証処理に用いられる認証鍵を記録している。

【0108】

テーブル保持部108は、例えば、フラッシュメモリ、EEPROM、MRAM、またはFeRAMなどの不揮発性メモリなどにより構成され、ライフサイクル状態テーブルおよびコマンドテーブルを保持している。テーブル保持部108は、制御部104の制御のもと、保持しているライフサイクル状態テーブルを更新する。

【0109】

発振回路109は、アンテナ101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110に供給する。例えば、発振回路109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。

【0110】

変調部110は、発振回路109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110は、搬送波に基づいて、SPU103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101に供給する。例えば、変調部110は、SPU103から供給された、マンチェスター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101を介して、リーダライタ11に送信する。

【0111】

また、例えば、変調部110は、SPU103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101に並列に接続させることにより、アンテナ101の負荷を変動させる。ASK変調されたデータは、アンテナ101の負荷の変動により、アンテナ101を介して、リーダライタ11に送信される(リーダライタ11のアンテナ36の端子電圧を変動させる)。

【0112】

電力発生部111は、アンテナ101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12の各部に供給する。

【0113】

次に、図6のフローチャートを参照して、リーダライタ11による、コマンド送信の処理を説明する。

【0114】

ステップS 1 1において、リーダライタ1 1は、必要に応じて、乱数などのデータを送受信し、I Cカード1 2との相互認証を行う。例えば、ステップS 1 1において、リーダライタ1 1は、ISO/IEC (International Organization for Standardization/International Electrotechnical Commission) 9798-2およびJIS (Japanese Industrial Standards) X5056-2において定義されている、対称暗号アルゴリズムを用いた方式により、I Cカード1 2との相互認証を行う。

【0 1 1 5】

このとき、例えば、リーダライタ1 1は、アクセスするデータまたはI Cカード1 2に対して実行させるコマンドごとに、予め定められた認証鍵を用いて、送受信するデータを暗号化するか、または復号する。なお、リーダライタ1 1は、I Cカード1 2のライフサイクル状態が、工場出荷状態または廃棄可能状態である場合、相互認証の処理を行わない。また、相互認証の処理において、正規のI Cカード1 2であると認証されなかった場合、コマンド送信の処理は終了する。

10

【0 1 1 6】

相互認証がなされると、ステップS 1 2において、制御部3 1は、所定の処理を実行させるための、各種のコマンドを生成し、生成したコマンドをSPU 3 3に供給する。

【0 1 1 7】

例えば、ステップS 1 2において、制御部3 1は、0次発券コマンド、オールリセットコマンド、ターミネートコマンドなどを生成し、生成したコマンドを、SPU 3 3に供給する。なお、制御部3 1が生成した各種のコマンドには、必要に応じて、コマンドの実行に必要なデータが格納されている。

20

【0 1 1 8】

ステップS 1 3において、SPU 3 3は、制御部3 1から供給されたコマンドを、所定の符号化方式により符号化し、符号化したコマンドを変調部3 4に供給する。例えば、ステップS 1 3において、SPU 3 3は、制御部3 1から供給されたコマンドを、マンチェスター方式などの符号化方式により符号化し、符号化したコマンドを変調部3 4に供給する。

【0 1 1 9】

ステップS 1 4において、変調部3 4は、SPU 3 3から供給されたコマンドを変調し、変調したコマンドをアンテナ3 6に供給する。例えば、ステップS 1 4において、変調部3 4は、発振回路3 5から供給されたクロック信号に対応する、所定の周波数（例えば、13.56MHz）の搬送波に基づいて、SPU 3 3から供給されたコマンドを、所定の方式により変調する。変調部3 4は、変調したコマンドをアンテナ3 6に供給する。

30

【0 1 2 0】

より詳細には、例えば、ステップS 1 4において、変調部3 4は、ASK方式、PSK (Phase Shift Keying) 方式、またはFSK (Frequency Shift Keying) 方式などの変調方式によりコマンドを変調し、変調したコマンドをアンテナ3 6に供給する。

【0 1 2 1】

ステップS 1 5において、アンテナ3 6は、変調部3 4から供給されたコマンドを、無線通信によってI Cカード1 2あてに送信し、コマンド送信の処理は終了する。例えば、ステップS 1 5において、アンテナ3 6は、変調部3 4から供給されたコマンドを伝送する電波を、放射することによりコマンドを送信する。

40

【0 1 2 2】

このようにして、リーダライタ1 1は、コマンドを生成し、生成したコマンドを、無線通信によりI Cカード1 2あてに送信する。

【0 1 2 3】

図7のフローチャートを参照して、I Cカード1 2による、コマンド実行の処理を説明する。

【0 1 2 4】

ステップS 3 1において、I Cカード1 2は、必要に応じて、乱数などのデータを送受

50

信し、リーダライタ 1 1 との相互認証を行う。例えば、ステップ S 3 1 において、I C カード 1 2 は、ISO/IEC9798-2 および JIS X5056-2 において定義されている、対称暗号アルゴリズムを用いた方式などにより、リーダライタ 1 1 との相互認証を行う。

【0 1 2 5】

このとき、例えば、I C カード 1 2 は、アクセスが要求されたデータまたは実行が要求されたコマンドごとに、予め定められた認証鍵を用いて、送受信するデータを暗号化するか、または復号する。なお、I C カード 1 2 は、I C カード 1 2 のライフサイクル状態が、工場出荷状態または廃棄可能状態である場合、相互認証の処理を行わない。また、相互認証の処理において、正規のリーダライタ 1 1 であると認証されなかった場合、コマンド実行の処理は終了する。

10

【0 1 2 6】

ステップ S 3 1 において、相互認証がなされると、リーダライタ 1 1 からコマンドが送信されてくるので、ステップ S 3 2 において、アンテナ 1 0 1 は、リーダライタ 1 1 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 1 0 2 に供給する。

【0 1 2 7】

ステップ S 3 3 において、復調部 1 0 2 は、アンテナ 1 0 1 から供給されたコマンドを、変調部 3 4 (図 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 SPU 1 0 3 に供給する。

【0 1 2 8】

ステップ S 3 4 において、SPU 1 0 3 は、復調部 1 0 2 から供給されたコマンドを、SPU 3 3 (図 4) の符号化方式に対応する復号方式により復号し、復号したコマンドを制御部 1 0 4 に供給する。

20

【0 1 2 9】

ステップ S 3 5 において、制御部 1 0 4 の判定部 1 3 1 は、テーブル保持部 1 0 8 が保持している、ライフサイクル状態テーブルを参照して、ライフサイクル状態が工場出荷状態であるか否かを判定する。

【0 1 3 0】

ここで、テーブル保持部 1 0 8 は、例えば、図 8 に示すライフサイクル状態テーブルを保持している。

【0 1 3 1】

ライフサイクル状態テーブルには、I C カード 1 2 のライフサイクル状態の各状態に対応するフラグが含まれている。

30

【0 1 3 2】

すなわち、ライフサイクル状態テーブルには、工場出荷状態に対応するフラグ、0 次発券済み状態に対応するフラグ、1 次発券済み状態に対応するフラグ、2 次発券済み状態に対応するフラグ、および廃棄可能状態に対応するフラグが含まれている。

【0 1 3 3】

ここで、セットされている(例えば、“1”が設定されている)フラグは、I C カード 1 2 のライフサイクル状態が、フラグに対応する状態であることを示し、リセットされている(例えば、“0”が設定されている)フラグは、I C カード 1 2 のライフサイクル状態が、フラグに対応する状態でないことを示している。

40

【0 1 3 4】

また、ライフサイクル状態テーブルに含まれるフラグは、ライフサイクル状態の各状態に対応するフラグのうち、何れか 1 つのフラグだけが必ずセットされており、それ以外のフラグ(残りの 4 つのフラグ)は、必ずリセットされている。

【0 1 3 5】

したがって、この場合、工場出荷状態に対応するフラグが“1”に設定されて(セットされて)おり、0 次発券済み状態に対応するフラグ、1 次発券済み状態に対応するフラグ、2 次発券済み状態に対応するフラグ、および廃棄可能状態に対応するフラグのそれぞれが、“0”に設定されて(リセットされて)いるので、I C カード 1 2 のライフサイクル

50

状態が、工場出荷状態であることを示している。

【0136】

図7のフローチャートの説明に戻り、例えば、ステップS35において、制御部104の判定部131は、テーブル保持部108が保持している、図8に示すライフサイクル状態テーブルを参照して、ライフサイクル状態が、工場出荷状態であるか否かを判定する。

【0137】

この場合、図8に示すライフサイクル状態テーブルにおいて、工場出荷状態に対応するフラグが、セットされている（“1”に設定されている）ので、制御部104の判定部131は、ライフサイクル状態が、工場出荷状態であると判定する。

【0138】

ステップS35において、ライフサイクル状態が、工場出荷状態であると判定された場合、ステップS36に進み、ICカード12は、工場出荷状態におけるコマンド実行の処理を行い、コマンド実行の処理は終了する。

【0139】

なお、工場出荷状態におけるコマンド実行の処理の詳細は後述するが、工場出荷状態におけるコマンド実行の処理において、ICカード12は、テーブル保持部108が保持しているコマンドテーブルを参照して、SPU103から供給されたコマンドのうち、工場出荷状態において実行することができるコマンドだけを実行する。

【0140】

ここで、テーブル保持部108は、例えば、図9に示すコマンドテーブルを保持している。コマンドテーブルには、ICカード12のライフサイクル状態の各状態において、実行することができるコマンドを示す情報が含まれている。

【0141】

すなわち、コマンドテーブルには、工場出荷状態において実行できるコマンドが、トラッキングコマンドおよび0次発券コマンドであることを示す情報が含まれている。ここで、トラッキングコマンドとは、ICカード12が記録している、ICカード12を製造したカード製造業者を特定するための情報である製造者番号を、無線通信により、リーダライタ11に送信するためのコマンドをいう。

【0142】

また、コマンドテーブルには、0次発券済み状態において実行できるコマンドが、相互認証コマンド、トラッキングコマンド、および1次発券コマンドであることを示す情報が含まれており、1次発券済み状態において実行できるコマンドが、相互認証コマンド、オールリセットコマンド、および2次発券コマンドであることを示す情報が含まれている。

【0143】

同様に、コマンドテーブルには、2次発券済み状態において実行できるコマンドが、相互認証コマンド、オールリセットコマンド、デタリセットコマンド、通常運用コマンド、およびターミネートコマンドであることを示す情報が含まれている。

【0144】

ここで、通常運用コマンドとは、ユーザが事業者からサービスの提供を受けるために必要な処理を実行するためのコマンドをいう。したがって、例えば、ICカード12は、通常運用コマンドを実行することによって、ユーザの個人情報などのデータを、記録部107に記録したり、ユーザの個人情報などのデータを記録部107から読み出して、無線通信により、リーダライタ11あてに送信する。

【0145】

さらに、コマンドテーブルには、廃棄可能状態において実行できるコマンドがないことを示す情報が含まれている。すなわち、廃棄可能状態においては、ICカード12は、如何なるコマンドも実行しない。

【0146】

したがって、例えば、ステップS36において、ICカード12は、SPU103から供給されたコマンドのうち、トラッキングコマンドまたは0次発券コマンドだけを実行する

10

20

30

40

50

。

【0147】

一方、ステップS35において、ライフサイクル状態が、工場出荷状態でないと判定された場合、工場出荷状態において実行できるコマンドは、実行されないので、ステップS37に進み、制御部104の判定部131は、テーブル保持部108が保持している、ライフサイクル状態テーブルを参照して、ライフサイクル状態が、0次発券済み状態であるか否かを判定する。

【0148】

例えば、ステップS37において、制御部104の判定部131は、図8に示すライフサイクル状態テーブルを参照して、ライフサイクル状態が、0次発券済み状態であるか否

10

【0149】

したがって、制御部104の判定部131は、0次発券済み状態に対応するフラグがセットされている（例えば、“1”に設定されている）場合、ライフサイクル状態が、0次発券済み状態であると判定し、0次発券済み状態に対応するフラグがリセットされている（例えば、“0”に設定されている）場合、ライフサイクル状態が、0次発券済み状態でないと判定する。

【0150】

ステップS37において、ライフサイクル状態が、0次発券済み状態であると判定された場合、ステップS38に進み、ICカード12は、0次発券済み状態におけるコマンド

20

実行の処理を行い、コマンド実行の処理は終了する。

【0151】

なお、0次発券済み状態におけるコマンド実行の処理の詳細は後述するが、0次発券済み状態におけるコマンド実行の処理において、ICカード12は、テーブル保持部108が保持しているコマンドテーブルを参照して、SPU103から供給されたコマンドのうち、0次発券済み状態において実行することができるコマンドだけを実行する。

【0152】

したがって、例えば、テーブル保持部108が、図9に示すコマンドテーブルを保持している場合、ICカード12は、ステップS38において、SPU103から供給されたコマンドのうち、トラッキングコマンドまたは1次発券コマンドだけを実行する。

30

【0153】

また、ステップS37において、ライフサイクル状態が、0次発券済み状態でないと判定された場合、0次発券済み状態において実行できるコマンドは、実行されないので、ステップS39に進み、制御部104の判定部131は、テーブル保持部108が保持している、ライフサイクル状態テーブルを参照して、ライフサイクル状態が、1次発券済み状態であるか否かを判定する。

【0154】

例えば、ステップS39において、制御部104の判定部131は、図8に示すライフサイクル状態テーブルを参照して、ライフサイクル状態が、1次発券済み状態であるか否

40

【0155】

したがって、制御部104の判定部131は、1次発券済み状態に対応するフラグがセットされている（例えば、“1”に設定されている）場合、ライフサイクル状態が、1次発券済み状態であると判定し、1次発券済み状態に対応するフラグがリセットされている（例えば、“0”に設定されている）場合、ライフサイクル状態が、1次発券済み状態でないと判定する。

【0156】

ステップS39において、ライフサイクル状態が、1次発券済み状態であると判定された場合、ステップS40に進み、ICカード12は、1次発券済み状態におけるコマンド

50

実行の処理を行い、コマンド実行の処理は終了する。

【0157】

なお、1次発券済み状態におけるコマンド実行の処理の詳細は後述するが、1次発券済み状態におけるコマンド実行の処理において、ICカード12は、テーブル保持部108が保持しているコマンドテーブルを参照して、SPU103から供給されたコマンドのうち、1次発券済み状態において実行することができるコマンドだけを実行する。

【0158】

したがって、例えば、テーブル保持部108が、図9に示すコマンドテーブルを保持している場合、ICカード12は、ステップS40において、SPU103から供給されたコマンドのうち、オールリセットコマンドまたは2次発券コマンドだけを実行する。

【0159】

また、ステップS39において、ライフサイクル状態が、1次発券済み状態でないと判定された場合、1次発券済み状態において実行できるコマンドは、実行されないので、ステップS41に進み、制御部104の判定部131は、テーブル保持部108が保持している、ライフサイクル状態テーブルを参照して、ライフサイクル状態が、2次発券済み状態であるか否かを判定する。

【0160】

例えば、ステップS41において、制御部104の判定部131は、図8に示すライフサイクル状態テーブルを参照して、ライフサイクル状態が、2次発券済み状態であるか否かを判定する。

【0161】

したがって、制御部104の判定部131は、1次発券済み状態に対応するフラグがセットされている（例えば、“1”に設定されている）場合、ライフサイクル状態が、2次発券済み状態であると判定し、2次発券済み状態に対応するフラグがリセットされている（例えば、“0”に設定されている）場合、ライフサイクル状態が、2次発券済み状態でないと判定する。

【0162】

ステップS41において、ライフサイクル状態が、2次発券済み状態であると判定された場合、ステップS42に進み、ICカード12は、2次発券済み状態におけるコマンド実行の処理を行い、コマンド実行の処理は終了する。

【0163】

なお、2次発券済み状態におけるコマンド実行の処理の詳細は後述するが、2次発券済み状態におけるコマンド実行の処理において、ICカード12は、テーブル保持部108が保持しているコマンドテーブルを参照して、SPU103から供給されたコマンドのうち、2次発券済み状態において実行することができるコマンドだけを実行する。

【0164】

したがって、例えば、テーブル保持部108が、図9に示すコマンドテーブルを保持している場合、ICカード12は、ステップS42において、SPU103から供給されたコマンドのうち、オールリセットコマンド、データリセットコマンド、通常運用コマンド、またはターミネートコマンドだけを実行する。

【0165】

一方、ステップS41において、ライフサイクル状態が、2次発券済み状態でないと判定された場合、ライフサイクル状態は、廃棄可能状態であり、ICカード12は、如何なるコマンドも実行しないので、ステップS42の処理はスキップされ、コマンド実行の処理は終了する。

【0166】

このようにして、ICカード12は、リーダライタ11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実行する。

【0167】

このように、ICカード12のライフサイクルにおける各状態において、予め定められたコマンドだけを実行することにより、データの改竄や情報の漏洩を防止することができ

10

20

30

40

50

る。

【0168】

図10のフローチャートを参照して、図7のステップS36の処理に対応する、工場出荷状態におけるコマンド実行の処理を説明する。

【0169】

ステップS61において、制御部104の判定部131は、SPU103から供給されたコマンドが、トラッキングコマンドであるか否かを判定する。ステップS61において、SPU103から供給されたコマンドが、トラッキングコマンドであると判定された場合、工場出荷状態において、トラッキングコマンドは実行できるので、ステップS62に進み、制御部104は、トラッキングコマンドを実行する。

10

【0170】

すなわち、ステップS62において、制御部104は、記録部107に記録されている製造者番号を取得し、取得した製造者番号を、SPU103に供給する。

【0171】

ここで、ICカード12のライフサイクル状態に、工場出荷状態が設定されている場合、記録部107には、例えば、図11に示すように、ICカード12を製造したカード製造業者を特定するための情報である、製造者番号だけが記録されている。また、製造者番号の他に、ICカード12の製造年月日などの情報を記録するようにしてもよい。

【0172】

ステップS63において、SPU103は、制御部104から供給された製造者番号を、所定の符号化方式により符号化し、符号化した製造者番号を変調部110に供給する。例えば、ステップS63において、SPU103は、制御部104から供給された製造者番号を、マンチェスター方式により符号化し、符号化した製造者番号を変調部110に供給する。

20

【0173】

ステップS64において、変調部110は、SPU103から供給された製造者番号を、所定の方式により変調し、変調した製造者番号をアンテナ101に供給する。例えば、ステップS64において、変調部110は、発振回路109から供給されたクロック信号により生成した搬送波を基に、SPU103から供給された製造者番号を、ASK変調方式により変調し、変調した製造者番号をアンテナ101に供給する。

30

【0174】

ステップS65において、アンテナ101は、変調部110から供給された、変調されている製造者番号を、無線通信により、リーダライタ11aに送信し、処理は終了する。例えば、ステップS65において、アンテナ101は、変調部110から供給された製造者番号を伝送する電波を放射することにより、製造者番号を送信する。リーダライタ11は、ICカード12から送信されてきた製造者番号を受信することによって、ICカード12の製造元を確認する。

【0175】

一方、ステップS61において、SPU103から供給されたコマンドが、トラッキングコマンドでないと判定された場合、トラッキングコマンドを実行しないので、ステップS66に進み、制御部104の判定部131は、SPU103から供給されたコマンドが、0次発券コマンドであるか否かを判定する。

40

【0176】

ステップS66において、SPU103から供給されたコマンドが、0次発券コマンドであると判定された場合、工場出荷状態において、0次発券コマンドは実行できるので、ステップS67に進み、制御部104は、0次発券コマンドを実行する。

【0177】

すなわち、ステップS67において、制御部104は、SPU103から供給された0次発券コマンドに含まれているデバイス識別番号を、記録部107に供給する。そして、記録部107は、制御部104から供給されたデバイス識別番号を記録する。

50

【0178】

ここで、デバイス識別番号とは、ICカード12を特定するための、ICカード12に固有の識別番号をいう。

【0179】

ステップS68において、制御部104は、MFの設定を行う。例えば、ステップS68において、制御部104は、MFおよびMFに含まれるデータを管理するための情報を生成し、生成したMFおよびMFに含まれるデータを管理するための情報を、記録部107に供給する。記録部107は、制御部104から供給された、MFおよびMFに含まれるデータを管理するための情報を記録する。ここで、MFに含まれるデータを管理するための情報には、例えば、MFに含まれるDFおよびEFの数など、MFの属性を示す情報が含まれている。

10

【0180】

ステップS69において、制御部104は、0次発券コマンドに含まれている、MFに対する認証鍵としての出荷鍵を記録部107に供給する。記録部107は、制御部104から供給された出荷鍵を、MFに対する認証鍵として記録する。ここで、出荷鍵は、1次発券作業を行う事業者が、リーダーライタ11を操作して、ICカード12にトラッキングコマンドまたは1次発券コマンドを実行させる場合に、相互認証処理において用いられる認証鍵である。

【0181】

ステップS70において、テーブル保持部108は、制御部104の制御のもと、ライフサイクル状態が、0次発券済み状態であることを示すようにライフサイクル状態テーブルを更新し、処理は終了する。

20

【0182】

例えば、ステップS70において、テーブル保持部108は、制御部104の制御のもと、テーブル保持部108が保持している、図8に示すライフサイクル状態テーブルの工場出荷状態に対応するフラグをリセット（例えば、“0”に設定する）し、0次発券済み状態に対応するフラグをセット（例えば、“1”に設定する）することにより、ライフサイクル状態テーブルを更新する。

【0183】

また、ライフサイクル状態が、0次発券済み状態である場合、記録部107には、例えば、図12に示すように、製造者番号、デバイス識別番号、MF151、出荷鍵A、および出荷鍵Bが記録されている。

30

【0184】

ここで、MF151は、記録部107において、階層構造に記録されるデータ（フォルダ）のうち、最上位の階層のフォルダである。また、記録部107には、MF151とともに、MF151に含まれるデータを管理するための情報が記録されている。

【0185】

さらに、記録部107には、認証鍵として、出荷鍵Aおよび出荷鍵Bが記録されている。すなわち、ICカード12は、ライフサイクル状態が0次発券済み状態であり、リーダーライタ11から送信されてきた、トラッキングコマンドを送信する旨の相互認証コマンド、または1次発券コマンドを送信する旨の相互認証コマンドを受信した場合、出荷鍵Aおよび出荷鍵Bを用いて、リーダーライタ11との相互認証処理を行う。

40

【0186】

図10のフローチャートの説明に戻り、ステップS66において、SPU103から供給されたコマンドが、0次発券コマンドでないと判定された場合、SPU103から供給されたコマンドは、工場出荷状態において、実行できるコマンドではないので、ステップS67の処理乃至ステップS70の処理はスキップされ、処理は終了する。

【0187】

したがって、例えば、SPU103から供給されたコマンドが、1次発券コマンドであった場合、ステップS66において、SPU103から供給されたコマンドが、0次発券コマ

50

ンドでないと判定され、1次発券コマンドは、工場出荷状態において実行できるコマンドではないので、処理は終了する。

【0188】

このようにして、制御部104は、SPU103から供給された、トラッキングコマンドまたは0次発券コマンドを実行する。

【0189】

このように、ICカード12のライフサイクルにおける工場出荷状態において、予め定められたコマンドだけを実行することにより、データの改竄や情報の漏洩を防止することができる。

【0190】

次に、図13のフローチャートを参照して、図7のステップS38の処理に対応する、0次発券済み状態におけるコマンド実行の処理を説明する。

【0191】

ステップS101において、制御部104の判定部131は、SPU103から供給されたコマンドが、トラッキングコマンドであるか否かを判定する。ステップS101において、SPU103から供給されたコマンドが、トラッキングコマンドであると判定された場合、0次発券済み状態において、トラッキングコマンドは実行できるので、ステップS102に進み、制御部104は、トラッキングコマンドを実行する。

【0192】

なお、ステップS102の処理乃至ステップS105の処理のそれぞれは、図10におけるステップS62の処理乃至ステップS65の処理のそれぞれと同様なので、その説明は省略する。

【0193】

ステップS101において、SPU103から供給されたコマンドが、トラッキングコマンドでないと判定された場合、トラッキングコマンドを実行しないので、ステップS106に進み、制御部104の判定部131は、SPU103から供給されたコマンドが、1次発券コマンドであるか否かを判定する。

【0194】

ステップS106において、SPU103から供給されたコマンドが、1次発券コマンドであると判定された場合、工場出荷状態において、1次発券コマンドは実行できるので、ステップS107に進み、制御部104は、1次発券コマンドを実行する。

【0195】

すなわち、ステップS107において、制御部104は、1次発券コマンドに含まれている、認証鍵としての事業者鍵を、記録部107に供給する。記録部107は、記録している認証鍵を、制御部104から供給された事業者鍵に書き換える。ここで、事業者鍵は、2次発券作業を行う事業者が、リーダーライタ11を操作して、ICカード12にオールリセットコマンド、2次発券コマンド、データリセットコマンド、またはターミネートコマンドを実行させる場合に、相互認証処理において用いられる認証鍵である。

【0196】

ステップS108において、制御部104は、DFの設定を行う。例えば、ステップS108において、制御部104は、MF151に従属するDFおよびDFに含まれるデータを管理するための情報を生成し、生成したDFおよびDFに含まれるデータを管理するための情報を、記録部107に供給する。記録部107は、制御部104から供給された、DFおよびDFに含まれるデータを管理するための情報を記録する。ここで、DFに含まれるデータを管理するための情報には、例えば、DFに含まれるデータの書き換えを禁止したり、DFに含まれる一部のデータのみを書き換え可能にするなどの情報を含むDFの属性を示す情報、DFに対する認証鍵などが含まれている。

【0197】

ステップS109において、制御部104は、EFの設定を行う。例えば、ステップS109において、制御部104は、DFに従属するEFおよびEFに含まれるデータを管

10

20

30

40

50

理するための情報を生成し、生成した E F および E F に含まれるデータを管理するための情報を、記録部 107 に供給する。記録部 107 は、制御部 104 から供給された、E F および E F に含まれるデータを管理するための情報を記録する。ここで、E F に含まれるデータを管理するための情報には、例えば、E F に含まれるデータの書き換えを禁止したり、E F に含まれる一部のデータのみを書き換え可能にするなどの情報を含む E F の属性を示す情報、E F に対する認証鍵などが含まれている。

【0198】

ステップ S110 において、制御部 104 は、1 次発券コマンドに含まれている、事業者番号を記録部 107 に供給する。記録部 107 は、制御部 104 から供給された事業者番号を記録する。ここで、事業者番号とは、1 次発券作業を行う事業者を特定するための情報である。

10

【0199】

ステップ S111 において、テーブル保持部 108 は、制御部 104 の制御のもと、ライフサイクル状態が、1 次発券済み状態であることを示すように、ライフサイクル状態テーブルを更新し、処理は終了する。

【0200】

例えば、ステップ S111 において、テーブル保持部 108 は、制御部 104 の制御のもと、テーブル保持部 108 が保持している、ライフサイクル状態テーブルの 0 次発券済み状態に対応するフラグをリセット（例えば、“0”に設定する）し、1 次発券済み状態に対応するフラグをセット（例えば、“1”に設定する）することにより、ライフサイクル状態テーブルを更新する。

20

【0201】

また、ライフサイクル状態が、1 次発券済み状態である場合、記録部 107 には、例えば、図 14 に示すように、製造者番号、デバイス識別番号、MF151、事業者鍵 A、事業者鍵 B、事業者番号 152、DF153-1、DF153-2、および EF154-1 乃至 EF154-4 が記録されている。なお、図中、図 12 における場合と対応する部分には、同一の符号を付してあり、繰り返しになるので、その説明は適宜、省略する。

【0202】

ここで、MF151 には、MF151 に従属するデータとして、1 次発券作業を行う事業者を特定するための事業者番号 152 が含まれている。また、MF151 には、MF151 に従属する DF153-1、DF153-2、および EF154-1 が含まれている。

30

【0203】

DF153-1 には、DF153-1 に従属するデータとして、EF154-2 および EF154-3 が含まれている。また、記録部 107 には、DF153-1 とともに、DF153-1 に対する認証鍵を含む、DF153-1 を管理するための情報が記録されている。同様に、記録部 107 には、EF154-2 および EF154-3 とともに、EF154-2 または EF154-3 に対する認証鍵を含む、EF154-2 または EF154-3 を管理するための情報が記録されている。この場合、EF154-2 に対する認証鍵として、それぞれ、“0000000”に設定された 4 つの認証鍵が記録されており、同様に、EF154-3 に対する認証鍵として、それぞれ、“0000000”に設定された 4 つの認証鍵が記録されている。

40

【0204】

DF153-2 には、DF153-2 に従属するデータとして、EF154-4 が含まれている。また、記録部 107 には、DF153-2 とともに、DF153-2 に対する認証鍵を含む、DF153-2 を管理するための情報が記録されている。同様に、記録部 107 には、EF154-4 とともに、EF154-4 に対する認証鍵を含む、EF154-4 を管理するための情報が記録されている。この場合、EF154-4 に対する認証鍵として、それぞれ、“0000000”に設定された 4 つの認証鍵が記録されている。

【0205】

50

また、記録部107には、MF151に従属するEF154-1とともに、EF154-1に対する認証鍵を含む、EF154-1を管理するための情報が記録されている。この場合、EF154-1に対する認証鍵として、それぞれ、“0000000”に設定された4つの認証鍵が記録されている。

【0206】

なお、以下、DF153-1およびDF153-2を個々に区別する必要のない場合、単に、DF153と称する。また、以下、EF154-1乃至EF154-4のそれぞれを個々に区別する必要のない場合、単にEF154と称する。

【0207】

さらに、記録部107には、認証鍵として、事業者鍵Aおよび事業者鍵Bが記録されている。ICカード12は、ライフサイクル状態が1次発券済み状態または2次発券済み状態であり、リーダライタ11から送信されてきた、オールリセットコマンド、2次発券コマンド、データリセットコマンド、またはターミネートコマンドを送信する旨の相互認証コマンドを受信した場合、事業者鍵Aおよび事業者鍵Bを用いて、リーダライタ11との相互認証処理を行う。

10

【0208】

図13のフローチャートの説明に戻り、ステップS106において、SPU103から供給されたコマンドが、1次発券コマンドでないと判定された場合、SPU103から供給されたコマンドは、0次発券済み状態において、実行できるコマンドではないので、ステップS107の処理乃至ステップS111の処理はスキップされ、処理は終了する。

20

【0209】

したがって、例えば、SPU103から供給されたコマンドが、2次発券コマンドであった場合、ステップS106において、SPU103から供給されたコマンドが、1次発券コマンドでないと判定され、2次発券コマンドは、0次発券済み状態において実行できるコマンドではないので、処理は終了する。

【0210】

このようにして、制御部104は、SPU103から供給された、トラッキングコマンドまたは1次発券コマンドを実行する。

【0211】

このように、ICカード12のライフサイクルにおける0次発券済み状態において、予め定められたコマンドだけを実行することにより、データの改竄や情報の漏洩を防止することができる。また、ICカード12のライフサイクルにおける状態によって、相互認証処理に用いられる認証鍵を書き換え、異なる認証鍵を用いて相互認証の処理を行うことで、データの改竄や情報の漏洩を防止することができる。

30

【0212】

図15のフローチャートを参照して、図7のステップS40の処理に対応する、1次発券済み状態におけるコマンド実行の処理を説明する。

【0213】

ステップS131において、制御部104の判定部131は、SPU103から供給されたコマンドが、オールリセットコマンドであるか否かを判定する。ステップS131において、SPU103から供給されたコマンドが、オールリセットコマンドであると判定された場合、1次発券済み状態において、オールリセットコマンドは実行できるので、ステップS132に進み、制御部104は、オールリセットコマンドを実行する。

40

【0214】

ステップS132において、記録部107は、制御部104の制御のもと、記録しているMFに従属する、事業者番号、DF、およびEFを削除する。例えば、ステップS132において、記録部107は、制御部104の制御のもと、図14に示されるMF151に従属する、事業者番号152、DF153、およびEF154を削除する。

【0215】

ステップS133において、テーブル保持部108は、制御部104の制御のもと、ラ

50

ライフサイクル状態が、0次発券済み状態であることを示すようにライフサイクル状態テーブルを更新し、処理は終了する。

【0216】

例えば、ステップS133において、テーブル保持部108は、制御部104の制御のもと、テーブル保持部108が保持している、ライフサイクル状態テーブルの1次発券済み状態に対応するフラグをリセット（例えば、“0”に設定する）し、0次発券済み状態に対応するフラグをセット（例えば、“1”に設定する）することにより、ライフサイクル状態テーブルを更新する。

【0217】

この場合、例えば、記録部107には、MFに対する認証鍵として事業者鍵が記録されており、0次発券済み状態においてトラッキングコマンドまたは0次発券コマンドを実行するときに行われる、相互認証処理においては、認証鍵として、事業者鍵が用いられる。

10

【0218】

ステップS131において、SPU103から供給されたコマンドが、オールリセットコマンドでないと判定された場合、オールリセットコマンドを実行しないので、ステップS134に進み、制御部104の判定部131は、SPU103から供給されたコマンドが、2次発券コマンドであるか否かを判定する。

【0219】

ステップS134において、SPU103から供給されたコマンドが、2次発券コマンドであると判定された場合、1次発券済み状態において、2次発券コマンドは実行できるので、ステップS135に進み、制御部104は、2次発券コマンドを実行する。

20

【0220】

すなわち、ステップS135において、制御部104は、DFの設定を行う。例えば、ステップS135において、制御部104は、2次発券コマンドに含まれるデータを基に、MF151に従属するDF153に格納される、ユーザの個人情報などのデータ、およびDF153に含まれるデータを管理するための情報を生成し、生成したDF153に格納されるデータおよびDF153に含まれるデータを管理するための情報を、記録部107に供給する。記録部107は、制御部104から供給された、DF153に格納されるデータ、およびDF153に含まれるデータを管理するための情報を記録する。

【0221】

30

ステップS136において、制御部104は、EFの設定を行う。例えば、ステップS136において、制御部104は、2次発券コマンドに含まれるデータを基に、DF153に従属するEF154に格納される、ユーザの個人情報などのデータ、およびEF154に含まれるデータを管理するための情報を生成し、生成したEF154に格納されるデータおよびEF154に含まれるデータを管理するための情報を、記録部107に供給する。

【0222】

記録部107は、制御部104から供給された、EF154に格納されるデータ、およびEF154に含まれるデータを管理するための情報を記録する。ここで、EF154に含まれるデータを管理するための情報には、例えば、新たに設定された、EF154に対する認証鍵が含まれている。すなわち、記録部107は、EF154に含まれるデータを管理するための情報を記録することによって、EF154に対する認証鍵を書き換える。

40

【0223】

ステップS137において、テーブル保持部108は、制御部104の制御のもと、ライフサイクル状態が、2次発券済み状態であることを示すように、ライフサイクル状態テーブルを更新し、処理は終了する。

【0224】

例えば、ステップS137において、テーブル保持部108は、制御部104の制御のもと、テーブル保持部108が保持している、ライフサイクル状態テーブルの1次発券済み状態に対応するフラグをリセット（例えば、“0”に設定する）し、2次発券済み状態

50

に対応するフラグをセット（例えば、“1”に設定する）することにより、ライフサイクル状態テーブルを更新する。

【0225】

また、ライフサイクル状態が、2次発券済み状態である場合、記録部107には、例えば、図16に示すように、製造者番号、デバイス識別番号、MF151、事業者鍵A、事業者鍵B、事業者番号152、DF153-1、DF153-2、およびEF154-1乃至EF154-4が記録されている。なお、図中、図14における場合と対応する部分には、同一の符号を付してあり、繰り返しになるので、その説明は適宜、省略する。

【0226】

ここで、DF153およびEF154には、事業者が提供するサービスを受けるために必要な、ユーザの個人情報などのデータが格納されている。また、この場合、EF154-1には、EF154-1に対する認証鍵として、“0454879”、“0679831”、“9864136”、および“8794246”が設定されている。

10

【0227】

同様に、EF154-2には、EF154-2に対する認証鍵として、“4657564”、“4301445”、“4315798”、および“4687144”が設定されており、EF154-3には、EF154-3に対する認証鍵として、“0038432”、“4863204”、“6870680”、および“3654640”が設定されており、EF154-4には、EF154-4に対する認証鍵として、“4687063”、“4013698”、“4430413”、および“2444545”が設定されている。

20

【0228】

図15のフローチャートの説明に戻り、ステップS134において、SPU103から供給されたコマンドが、2次発券コマンドでないと判定された場合、SPU103から供給されたコマンドは、1次発券済み状態において、実行できるコマンドではないので、ステップS135の処理乃至ステップS137の処理はスキップされ、処理は終了する。

【0229】

したがって、例えば、SPU103から供給されたコマンドが、1次発券コマンドであった場合、ステップS134において、SPU103から供給されたコマンドが、2次発券コマンドでないと判定され、1次発券コマンドは、1次発券済み状態において実行できるコマンドではないので、処理は終了する。

30

【0230】

このようにして、制御部104は、SPU103から供給された、オールリセットコマンドまたは2次発券コマンドを実行する。

【0231】

このように、ICカード12のライフサイクルにおける1次発券済み状態において、予め定められたコマンドだけを実行することにより、データの改竄や情報の漏洩を防止することができる。また、ICカード12のライフサイクルにおける状態によって、相互認証処理に用いられる認証鍵を書き換え、ライフサイクルの状態によって、異なる認証鍵を用いて、相互認証の処理を行うことで、データの改竄や情報の漏洩を防止することができる。

40

【0232】

次に、図17のフローチャートを参照して、図7のステップS42の処理に対応する、2次発券済み状態におけるコマンド実行の処理を説明する。

【0233】

ステップS151において、制御部104の判定部131は、SPU103から供給されたコマンドが、オールリセットコマンドであるか否かを判定する。ステップS151において、SPU103から供給されたコマンドが、オールリセットコマンドであると判定された場合、2次発券済み状態において、オールリセットコマンドは実行できるので、ステップS152に進み、制御部104は、オールリセットコマンドを実行する。

50

【0234】

なお、ステップS152の処理およびステップS153の処理は、図15におけるステップS132の処理およびステップS133の処理と同様なので、その説明は省略する。

【0235】

ステップS151において、SPU103から供給されたコマンドが、オールリセットコマンドでないと判定された場合、オールリセットコマンドを実行しないので、ステップS154に進み、制御部104の判定部131は、SPU103から供給されたコマンドが、データリセットコマンドであるか否かを判定する。

【0236】

ステップS154において、SPU103から供給されたコマンドが、データリセットコマンドであると判定された場合、2次発券済み状態において、データリセットコマンドは実行できるので、ステップS155に進み、記録部107は、データリセットコマンドを実行する。

10

【0237】

すなわち、ステップS155において、記録部107は、制御部104の制御のもと、記録している、MFに従属するDFおよびEFを初期化する。例えば、ステップS155において、記録部107は、制御部104の制御のもと、記録している、図16に示すMF151に従属するDF153およびEF154に格納されているデータ、DF153およびEF154を管理するための情報を消去することによって、DF153およびEF154を初期化する。

20

【0238】

ステップS156において、テーブル保持部108は、制御部104の制御のもと、ライフサイクル状態が、1次発券済み状態であることを示すように、ライフサイクル状態テーブルを更新し、処理は終了する。

【0239】

例えば、ステップS156において、テーブル保持部108は、制御部104の制御のもと、テーブル保持部108が保持している、ライフサイクル状態テーブルの2次発券済み状態に対応するフラグをリセット（例えば、“0”に設定する）し、1次発券済み状態に対応するフラグをセット（例えば、“1”に設定する）することにより、ライフサイクル状態テーブルを更新する。

30

【0240】

ステップS154において、SPU103から供給されたコマンドが、データリセットコマンドでないと判定された場合、データリセットコマンドを実行しないので、ステップS157に進み、制御部104の判定部131は、SPU103から供給されたコマンドが、通常運用コマンドであるか否かを判定する。

【0241】

ステップS157において、SPU103から供給されたコマンドが、通常運用コマンドであると判定された場合、2次発券済み状態において、通常運用コマンドは実行できるので、ステップS158に進み、ICカード12は、通常運用コマンドに応じた処理を実行し、処理は終了する。

40

【0242】

例えば、SPU103から、EFに格納されているデータの書き換えを要求する旨の通常運用コマンドが供給された場合、ステップS158において、制御部104は、通常運用コマンドに含まれているデータを、記録部107に供給する。そして、記録部107は、記録している、EFに格納されているデータを、制御部104から供給されたデータに書き換える。なお、この場合、より詳細には、通常運用コマンドに含まれているデータが、所定の方式により暗号化されているとき、制御部104の復号部133は、通常運用コマンドに含まれているデータを、復号し、制御部104は、制御部104の復号部133が復号したデータを、記録部107に供給する。

【0243】

50

また、例えば、SPU 1 0 3 から、E F に格納されているデータの送信を要求する旨の通常運用コマンドが供給された場合、ステップ S 1 5 8 において、制御部 1 0 4 は、記録部 1 0 7 から、送信が要求されたデータを取得し、取得したデータを SPU 1 0 3 に供給する。

【0 2 4 4】

SPU 1 0 3 は、制御部 1 0 4 から供給されたデータを、例えば、マンチェスター方式により符号化し、符号化したデータを変調部 1 1 0 に供給する。変調部 1 1 0 は、SPU 1 0 3 から供給されたデータを、例えば、ASK 変調し、変調したデータをアンテナ 1 0 1 に供給する。そして、アンテナ 1 0 1 は、変調部 1 1 0 から供給されたデータを、無線通信により、リーダライタ 1 1 あてに送信する。なお、この場合、リーダライタ 1 1 あてに送信するデータを、必要に応じて、制御部 1 0 4 の暗号化部 1 3 2 が、所定の方式により暗号化するようにしてもよい。

10

【0 2 4 5】

ステップ S 1 5 7 において、SPU 1 0 3 から供給されたコマンドが、通常運用コマンドでないと判定された場合、通常運用コマンドを実行しないので、ステップ S 1 5 9 に進み、制御部 1 0 4 の判定部 1 3 1 は、SPU 1 0 3 から供給されたコマンドが、ターミネートコマンドであるか否かを判定する。

【0 2 4 6】

ステップ S 1 5 9 において、SPU 1 0 3 から供給されたコマンドが、ターミネートコマンドであると判定された場合、2 次発券済み状態において、ターミネートコマンドは実行できるので、ステップ S 1 6 0 に進み、記録部 1 0 7 は、制御部 1 0 4 の制御のもと、記録している全てのデータを削除する。

20

【0 2 4 7】

ステップ S 1 6 1 において、テーブル保持部 1 0 8 は、制御部 1 0 4 の制御のもと、ライフサイクル状態が、廃棄可能状態であることを示すように、ライフサイクル状態テーブルを更新し、処理は終了する。

【0 2 4 8】

例えば、ステップ S 1 6 1 において、テーブル保持部 1 0 8 は、制御部 1 0 4 の制御のもと、テーブル保持部 1 0 8 が保持している、ライフサイクル状態テーブルの 2 次発券済み状態に対応するフラグをリセット（例えば、“0”に設定する）し、廃棄可能状態に対応するフラグをセット（例えば、“1”に設定する）することにより、ライフサイクル状態テーブルを更新する。

30

【0 2 4 9】

ステップ S 1 5 9 において、SPU 1 0 3 から供給されたコマンドが、ターミネートコマンドでないと判定された場合、SPU 1 0 3 から供給されたコマンドは、2 次発券済み状態において、実行できるコマンドではないので、ステップ S 1 6 0 の処理およびステップ S 1 6 1 の処理はスキップされ、処理は終了する。

【0 2 5 0】

したがって、例えば、SPU 1 0 3 から供給されたコマンドが、2 次発券コマンドであった場合、ステップ S 1 5 9 において、SPU 1 0 3 から供給されたコマンドが、ターミネートコマンドでないと判定され、2 次発券コマンドは、2 次発券済み状態において実行できるコマンドではないので、処理は終了する。

40

【0 2 5 1】

このようにして、制御部 1 0 4 は、SPU 1 0 3 から供給された、オールリセットコマンド、データリセットコマンド、通常運用コマンド、またはターミネートコマンドを実行する。

【0 2 5 2】

このように、I C カード 1 2 のライフサイクルにおける 2 次発券済み状態において、予め定められたコマンドだけを実行することにより、データの改竄や情報の漏洩を防止することができる。これにより、ユーザから I C カード 1 2 を回収した事業者は、廃棄可能状

50

態の I C カード 1 2 を、I C カード 1 2 を物理的に廃棄する廃棄業者に配送するとき、データの改竄や情報の漏洩などの心配がなくなる。

【0253】

なお、I C カード 1 2 が、自分自身のライフサイクル状態において、実行することができないコマンドを受信した場合、コマンドを送信してきたリーダライタ 1 1 に対して、無応答とするようにしてもよく、自分自身のライフサイクル状態において、実行することができないコマンドを受信した旨のエラー通知信号を、リーダライタ 1 1 あてに送信するようにしてもよい。また、テーブル保持部 1 0 8 が、記録部 1 0 7 に含まれる構成とする 것도可能である。

【0254】

さらに、より詳細には、1 次発券コマンドまたは 2 次発券コマンドを実行することによって、認証鍵を書き換える処理は、1 次発券コマンドまたは 2 次発券コマンドに含まれる、認証鍵を書き換えるコマンド（以下、鍵変更コマンドと称する）を実行することによって行われる。

【0255】

したがって、例えば、2 次発券コマンドを実行することによって、記録部 1 0 7 が記録している、M F に対する事業者鍵を書き換えることも可能であるが、1 次発券コマンドを実行することによって、出荷鍵（M F に対する認証鍵）だけしか書き換えができないようにし、2 次発券コマンドを実行することによって、D F に対する認証鍵および E F に対する認証鍵だけしか書き換えができないようにすることも可能である。この場合、2 次発券済み状態においては、認証鍵の書き換えができないようになされている。

【0256】

さらに、また、1 次発券済み状態または 2 次発券済み状態において、コマンドを実行するとき、認証鍵として、事業者鍵を用いて、相互認証処理を行うと説明したが、例えば、2 次発券コマンドを実行するとき、図 1 4 に示す事業者鍵 A を用いて、相互認証処理を行い、2 次発券済み状態において、コマンド（例えば、ターミネートコマンド）を実行するとき、図 1 6 に示す事業者鍵 B を用いて、相互認証処理を行うようにしてもよい。

【0257】

このようにすることで、2 次発券作業を行う事業者と、2 次発券済み状態において、コマンドを実行させる事業者とが異なる場合においても、同一の認証鍵を共有することなく、それぞれのコマンドを実行させることが可能である。

【0258】

さらに、また、記録している事業者鍵を基に、異なる認証鍵を生成し、2 次発券コマンドを実行する場合における相互認証処理と、ターミネートコマンドを実行する場合における相互認証処理とで、異なる認証鍵を用いるようにしてもよい。

【0259】

すなわち、2 次発券コマンドを実行する場合、制御部 1 0 4 は、例えば、図 1 4 に示す事業者鍵 A および事業者鍵 B の論理和を演算することにより、相互認証処理に用いる認証鍵を生成し、ターミネートコマンドを実行する場合、制御部 1 0 4 は、図 1 6 に示す事業者鍵 A および事業者鍵 B の排他的論理和を演算することにより、認証鍵を生成する。このようにすることで、実行するコマンドごとに、アクセス権を設定することが可能となる。

【0260】

以上のように、I C カードのライフサイクルにおける各状態において、予め定められたコマンドだけを実行することにより、データの改竄や情報の漏洩を防止することができる。また、I C カードのライフサイクルにおける各状態において、異なる認証鍵を用いるようにしたので、データの改竄や情報の漏洩を防止することができる。

【0261】

本発明によれば、データを記録するようにしたので、データを送受信することができる。また、本発明によれば、I C カードのライフサイクルにおける各状態において、予め定められたコマンドだけを実行するようにしたので、データの改竄や情報の漏洩を防止する

10

20

30

40

50

ことができる。さらに、本発明によれば、ＩＣカードのライフサイクルにおける各状態において、異なる認証鍵を用いるようにしたので、データの改竄や情報の漏洩を防止することができる。

【０２６２】

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が、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、記録媒体からインストールされる。

10

【０２６３】

この記録媒体は、図４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７１（フレキシブルディスクを含む）、光ディスク７２（ＣＤ-ROM(Compact Disc-Read Only Memory)、DVD(Digital Versatile Disc)を含む）、光磁気ディスク７３（ＭＤ(Mini-Disc)（商標）を含む）、若しくは半導体メモリ７４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や、記録部３２に含まれるハードディスクなどで構成される。

【０２６４】

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。

20

【０２６５】

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。

【図面の簡単な説明】

【０２６６】

【図１】従来のＩＣカードのライフサイクルを説明するための図である。

30

【図２】本発明に係るＩＣカードのライフサイクルを説明するための図である。

【図３】本発明に係る無線通信システムを説明する図である。

【図４】リーダライタの機能の構成を示すブロック図である。

【図５】ＩＣカードの機能の構成を示すブロック図である。

【図６】コマンド送信の処理を説明するフローチャートである。

【図７】コマンド実行の処理を説明するフローチャートである。

【図８】ライフサイクル状態テーブルを説明する図である。

【図９】コマンドテーブルを説明する図である。

【図１０】工場出荷状態におけるコマンド実行の処理を説明するフローチャートである。

【図１１】工場出荷状態を説明するための図である。

40

【図１２】０次発券済み状態を説明するための図である。

【図１３】０次発券済み状態におけるコマンド実行の処理を説明するフローチャートである。

【図１４】１次発券済み状態を説明するための図である。

【図１５】１次発券済み状態におけるコマンド実行の処理を説明するフローチャートである。

【図１６】２次発券済み状態を説明するための図である。

【図１７】２次発券済み状態におけるコマンド実行の処理を説明するフローチャートである。

【符号の説明】

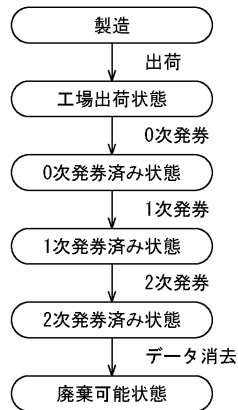
50

【0267】

11 リーダライタ, 12 ICカード, 31 制御部, 32 記録部, 36 アンテナ, 51 暗号化部, 52 復号部, 71 磁気ディスク, 72 光ディスク, 73 光磁気ディスク, 74 半導体メモリ, 101 アンテナ, 104 制御部, 105 ROM, 106 RAM, 107 記録部, 108 テーブル保持部, 131 判定部, 132 暗号化部, 133 復号部

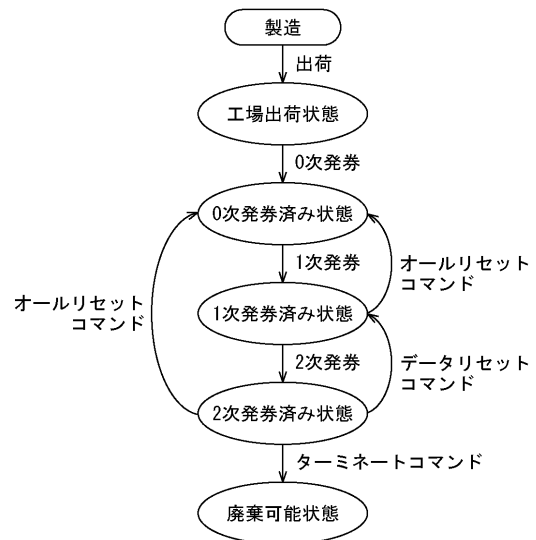
【図1】

図1



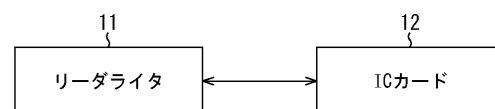
【図2】

図2

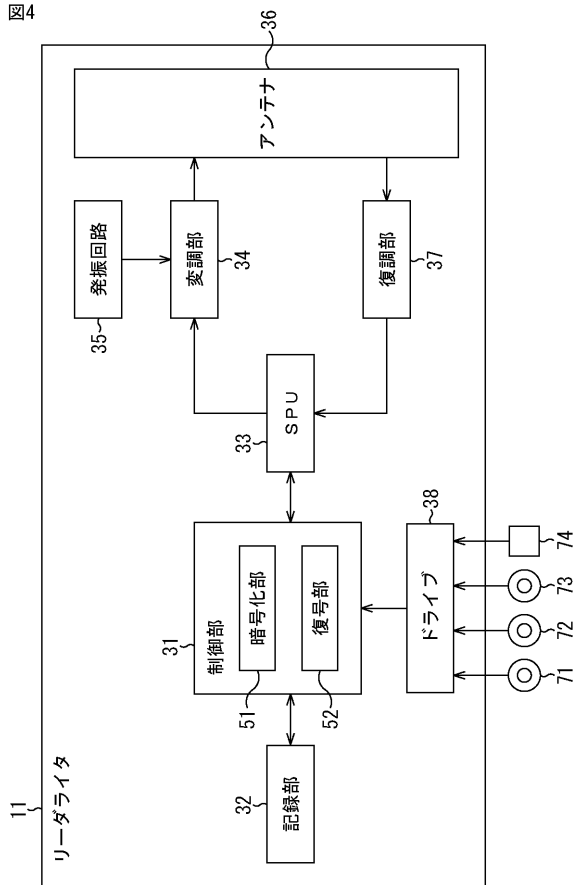


【図3】

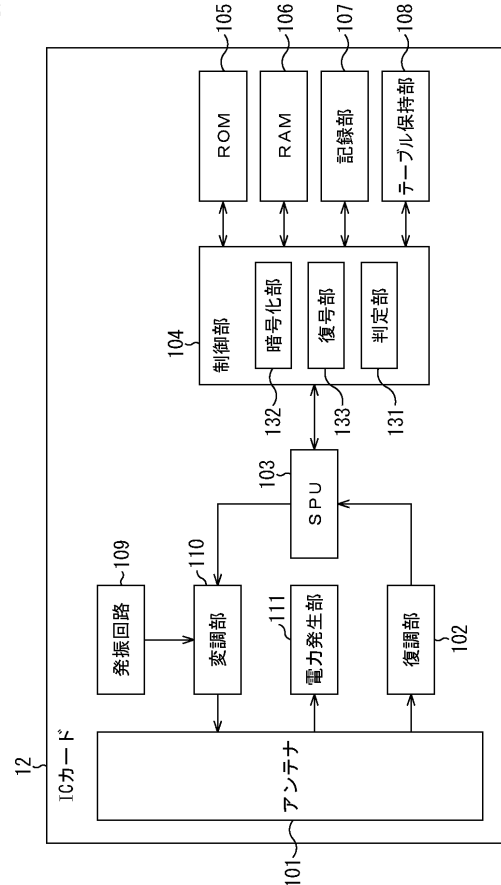
図3



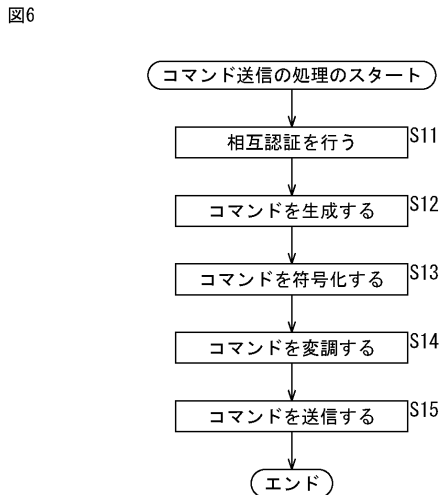
【図 4】



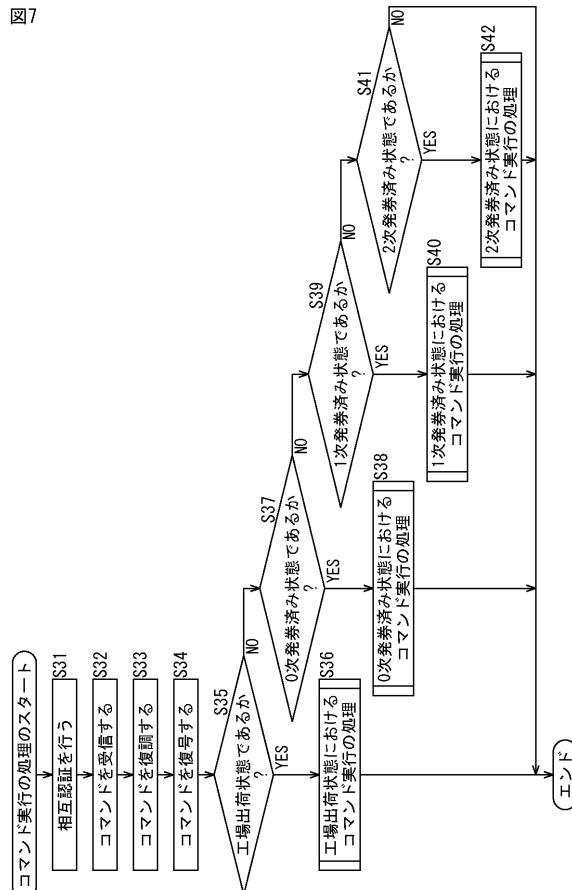
【図 5】



【图 6】



【图 7】



【図 8】

図8

ライフサイクル状態テーブル

工場出荷状態	1
0次発券済み状態	0
1次発券済み状態	0
2次発券済み状態	0
廃棄可能状態	0

【図 9】

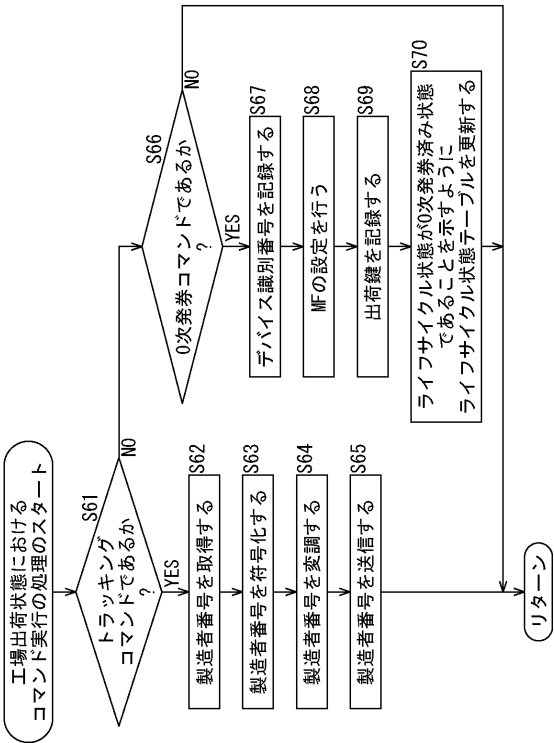
図9

コマンドテーブル

状態	コマンド
工場出荷状態	トラッキングコマンド
	0次発券コマンド
0次発券済み状態	相互認証コマンド
	トラッキングコマンド
	1次発券コマンド
1次発券済み状態	相互認証コマンド
	オールリセットコマンド
	2次発券コマンド
2次発券済み状態	相互認証コマンド
	オールリセットコマンド
	データリセットコマンド
	通常運用コマンド
	ターミネートコマンド
廃棄可能状態	

【図 10】

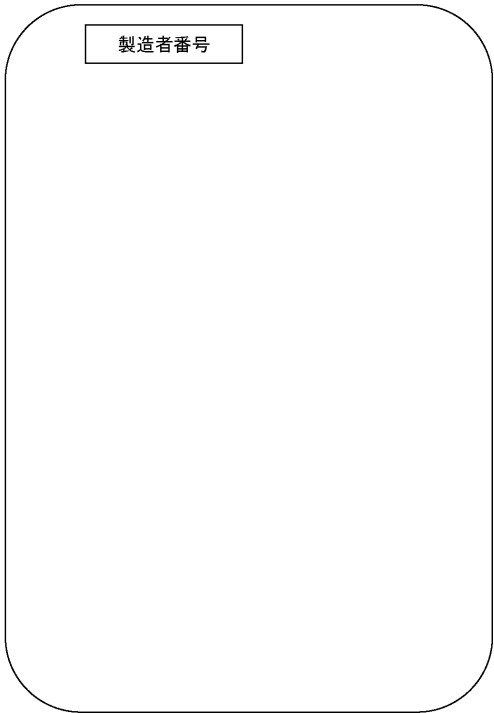
図10



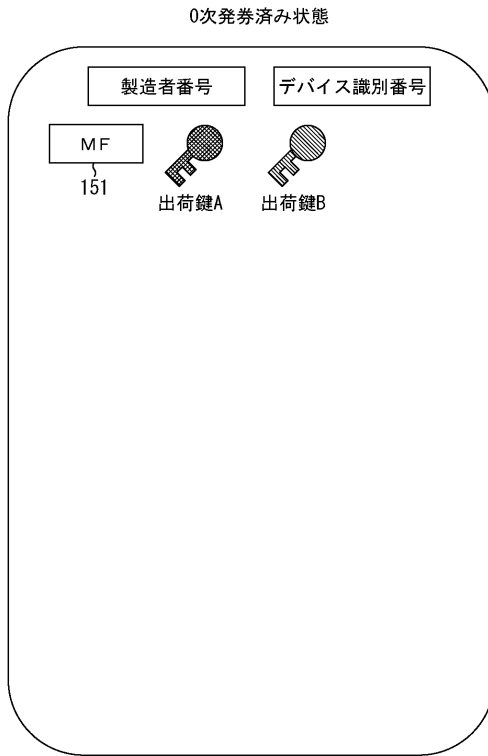
【図 11】

図11

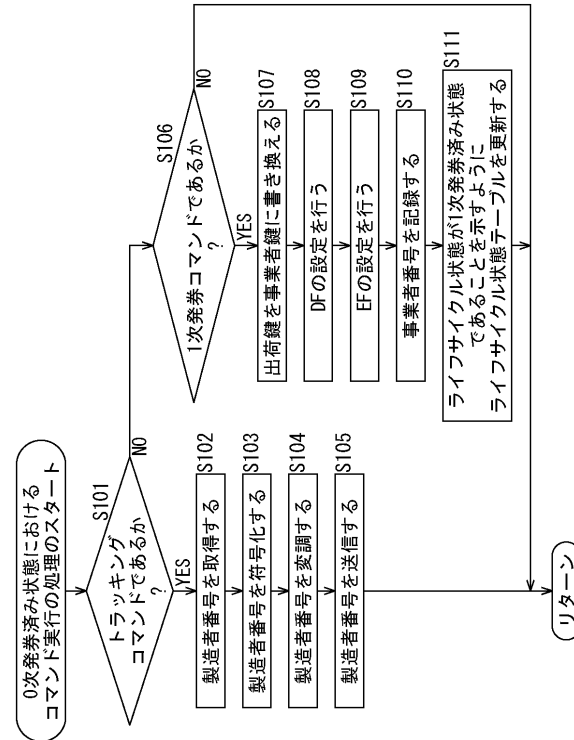
工場出荷状態



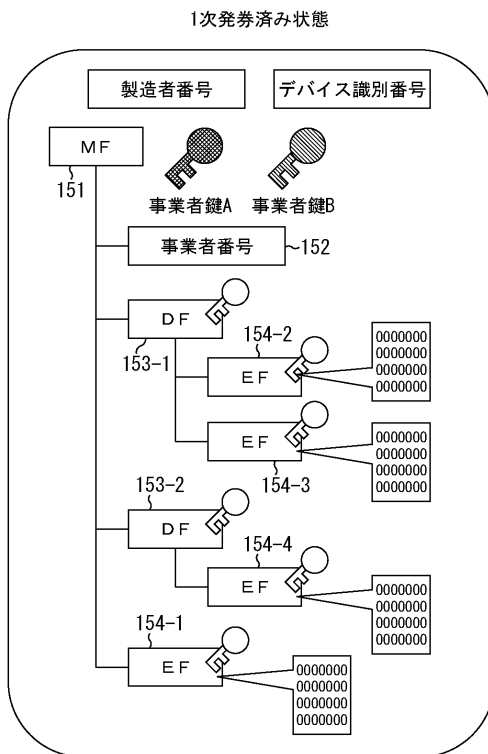
【図 1 2】
図12



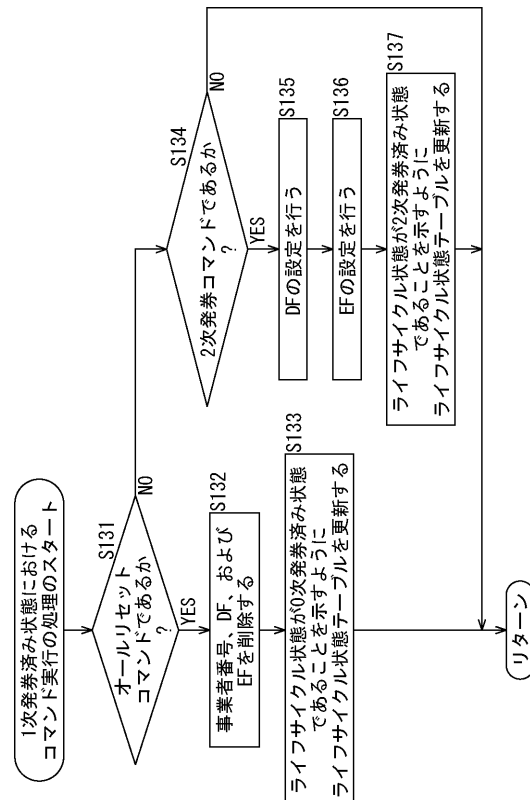
【図 1 3】
図13



【図 1 4】
図14

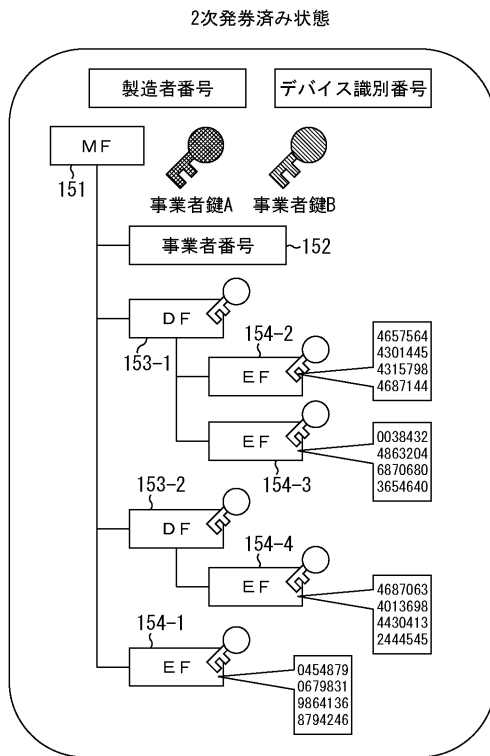


【図 1 5】
図15



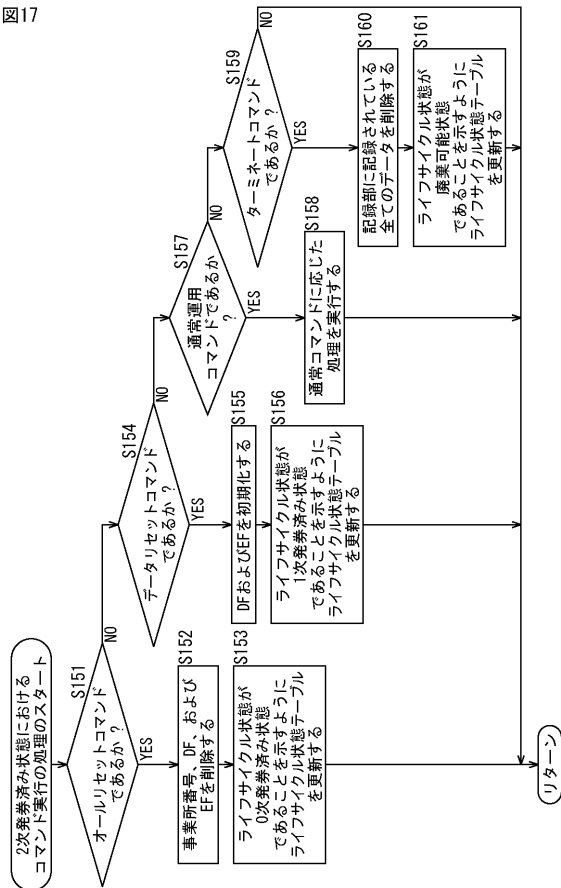
【図 16】

図16



【図 17】

図17



フロントページの続き

(51)Int.Cl. F I
G 0 6 K 19/07 (2006.01) G 0 6 K 19/00 H

(56)参考文献 特開平02-157988 (JP, A)
特開平06-131515 (JP, A)
特開2004-094692 (JP, A)
特開2000-307567 (JP, A)

(58)調査した分野(Int.Cl., DB名)
G 0 6 K 19/00-19/10
G 0 6 F 21/02
G 0 6 F 21/24
G 0 9 C 1/00
H 0 4 L 9/10