(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4485528号
(P4485528)

(45)発行日　平成22年6月23日(2010.6.23)　(24)登録日　平成22年4月2日(2010.4.2)

(51)Int.Cl.		F I		
G06K 19/10	(2006.01)	G06K	19/00	R
G06K 17/00	(2006.01)	G06K	17/00	T
G06F 21/24	(2006.01)	G06F	12/14	540A
G09C 1/00	(2006.01)	G06F	12/14	530D
		G09C	1/00	660A

請求項の数 16　(全 27 頁)

(21)出願番号　特願2006-531136 (P2006-531136)
(86)(22)出願日　平成16年8月20日 (2004.8.20)
(86)国際出願番号　PCT/JP2004/011964
(87)国際公開番号　WO2006/018890
(87)国際公開日　平成18年2月23日 (2006.2.23)
審査請求日　平成19年4月25日 (2007.4.25)

(73)特許権者　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目７番３号
(74)代理人　100099461
弁理士　溝井　章司
(72)発明者　米田　健
日本国東京都千代田区丸の内二丁目７番３号　三菱電機株式会社内

審査官　相崎　裕恒

最終頁に続く

(54)【発明の名称】メモリカード、データ交換システム及びデータ交換方法

(57)【特許請求の範囲】

【請求項１】

書込み装置からデータを受信し、受信したデータを記憶し、記憶したデータを読取装置に送信するメモリカードにおいて、

前記書込み装置がデータを暗号化して生成した親展データを前記書込み装置から受信する親展データ受信部と、

前記親展データ受信部が受信した親展データを格納するパブリック格納部と、

前記読取装置が送信した認証データを受信する認証データ受信部と、

正規の認証データを格納する認証データ格納部と、

前記認証データ受信部が受信した認証データを前記認証データ格納部に格納された正規の認証データと照合して認証を行う認証部と、

前記認証部が行った認証が成功した場合、前記パブリック格納部に格納された親展データを復号化して得られるデータを格納するプライベート格納部と、

前記認証部が行った認証が成功した場合、前記プライベート格納部に格納されたデータを前記読取装置に送信するカードデータ送信部とを備えることを特徴とするメモリカード。

【請求項２】

前記カードデータ送信部は、

前記パブリック格納部に格納された親展データを前記読取装置に送信し、

前記メモリカードは、さらに、

前記カードデータ送信部が送信した親展データを前記読取装置が復号化して取得したデータを前記読取装置から受信するカードデータ受信部を備え、
前記プライベート格納部は、
前記認証部が行った認証が成功した場合、前記カードデータ受信部が受信したデータを格納することを特徴とする請求項１に記載のメモリカード。
【請求項３】
前記メモリカードは、さらに、
第１の公開鍵を含む証明書を格納するカード証明書格納部と、
前記カード証明書格納部に格納された証明書を前記書込み装置に送信する証明書送信部と、
前記第１の公開鍵と対を成す第１の秘密鍵を格納するカード秘密鍵格納部と、
前記読取装置が送信した暗号化された共通鍵を受信するカード共通鍵受信部と、
前記カード秘密鍵格納部に格納された第１の秘密鍵を用いて前記カード共通鍵受信部が受信した共通鍵を復号化する共通鍵復号部と、
前記共通鍵復号部が復号化した共通鍵を前記読取装置に送信するカード共通鍵送信部とを備えることを特徴とする請求項２に記載のメモリカード。
【請求項４】
前記認証データ格納部は、
正規の認証データとして暗証番号（ＰＩＮ，Ｐｅｒｓｏｎａｌ　Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ　Ｎｕｍｂｅｒ）を格納することを特徴とする請求項３に記載のメモリカード。
【請求項５】
前記メモリカードは、さらに、
前記パブリック格納部に格納された親展データを復号化して得られるデータを取得するデータ取得部を備え、
前記プライベート格納部は、
前記データ取得部が取得したデータを格納することを特徴とする請求項１に記載のメモリカード。
【請求項６】
前記メモリカードは、さらに、
第１の公開鍵を含む証明書を格納するカード証明書格納部と、
前記カード証明書格納部に格納された証明書を前記書込み装置に送信する証明書送信部と、
前記第１の公開鍵と対を成す第１の秘密鍵を格納するカード秘密鍵格納部と、
前記パブリック格納部に格納された親展データから暗号化された署名データを取得する署名データ取得部と、
前記パブリック格納部に格納された親展データから暗号化された共通鍵を取得する共通鍵取得部と、
前記カード秘密鍵格納部に格納された第１の秘密鍵を用いて前記共通鍵取得部が取得した共通鍵を復号化する共通鍵復号部と、
前記共通鍵復号部が復号化した共通鍵を用いて前記署名データ取得部が取得した署名データを復号化する署名データ復号部と、
前記署名データ復号部が復号化した署名データからデジタル署名を取得するデジタル署名取得部と、
前記署名データ復号部が復号化した署名データから第２の公開鍵を含む証明書を取得する証明書取得部と、
前記証明書取得部が取得した証明書を検証し、当該証明書に含まれる第２の公開鍵を取得するシステム証明書検証部と、
前記データ取得部が取得したデータと前記システム証明書検証部が取得した第２の公開鍵とを用いて前記デジタル署名取得部が取得したデジタル署名を検証するデジタル署名検証部とを備え、

前記データ取得部は、
前記署名データ復号部が復号化した署名データからデータを取得することを特徴とする請求項５に記載のメモリカード。
【請求項７】
前記メモリカードは、さらに、
証明書を発行する認証局（ＣＡ，Ｃｅｒｔｉｆｉｃａｔｅ　Ａｕｔｈｏｒｉｔｙ）から証明書を取得する認証局通信部を備え、
前記システム証明書検証部は、
前記認証局通信部が取得した証明書を基に前記証明書取得部が取得した証明書を検証することを特徴とする請求項６に記載のメモリカード。
【請求項８】
前記認証データ格納部は、
正規の認証データとして暗証番号（ＰＩＮ，Ｐｅｒｓｏｎａｌ　Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ　Ｎｕｍｂｅｒ）を格納することを特徴とする請求項７に記載のメモリカード。
【請求項９】
データを書込む書込み装置と、データを読取る読取装置と、前記書込み装置からデータを受信し、受信したデータを記憶し、記憶したデータを前記読取装置に送信するメモリカードとを備えるデータ交換システムにおいて、
前記メモリカードは、
請求項２に記載のメモリカードであり、
前記書込み装置は、
データを入力する入力部と、
前記入力部が入力したデータを格納するデータ格納部と、
前記データ格納部に格納されたデータを暗号化して親展データを生成する親展データ生成部と、
前記親展データ生成部が生成した親展データを前記親展データ受信部に送信する親展データ送信部とを備え、
前記読取装置は、
前記カードデータ送信部が送信した親展データを受信する読取装置データ受信部と、
前記読取装置データ受信部が受信した親展データを復号化して得られるデータを取得するデータ取得部と、
前記データ取得部が取得したデータを出力する出力部と、
前記データ取得部が取得したデータを前記カードデータ受信部に送信する読取装置データ送信部と、
認証データを入力する操作部と、
前記操作部が入力した認証データを前記認証データ受信部に送信する認証データ送信部とを備えることを特徴とするデータ交換システム。
【請求項１０】
データを書込む書込み装置と、データを読取る読取装置と、前記書込み装置からデータを受信し、受信したデータを記憶し、記憶したデータを前記読取装置に送信するメモリカードとを備えるデータ交換システムにおいて、
前記メモリカードは、
請求項３に記載のメモリカードであり、
前記書込み装置は、
データを入力する入力部と、
前記入力部が入力したデータを格納するデータ格納部と、
前記証明書送信部が送信した証明書を受信する証明書受信部と、
前記証明書受信部が受信した証明書を検証し、当該証明書に含まれる第１の公開鍵を取得するカード証明書検証部と、
第２の秘密鍵を格納するシステム秘密鍵格納部と、

前記データ格納部に格納されたデータと前記システム秘密鍵格納部に格納された第２の秘密鍵とを用いてデジタル署名を生成するデジタル署名生成部と、
前記第２の秘密鍵と対を成す第２の公開鍵を含む証明書を格納するシステム証明書格納部と、
前記データ格納部に格納されたデータと前記デジタル署名生成部が生成したデジタル署名と前記システム証明書格納部に格納された証明書とを用いて署名データを生成する署名データ生成部と、
共通鍵を生成する共通鍵生成部と、
前記共通鍵生成部が生成した共通鍵を用いて前記署名データが生成した署名データを暗号化する署名データ暗号部と、
前記カード証明書検証部が取得した第１の公開鍵を用いて前記共通鍵生成部が生成した共通鍵を暗号化する共通鍵暗号部と、
前記署名データ暗号部が暗号化した署名データと前記共通鍵暗号部が暗号化した共通鍵とを用いて親展データを生成する親展データ生成部と、
前記親展データ生成部が生成した親展データを前記親展データ受信部に送信する親展データ送信部とを備え、
前記読取装置は、
前記カードデータ送信部が送信した親展データを受信する読取装置データ受信部と、
前記読取装置データ受信部が受信した親展データから暗号化された署名データを取得する署名データ取得部と、
前記読取装置データ受信部が受信した親展データから暗号化された共通鍵を取得する共通鍵取得部と、
前記共通鍵取得部が取得した暗号化された共通鍵を前記カード共通鍵受信部に送信する読取装置共通鍵送信部と、
前記カード共通鍵送信部が送信した復号化された共通鍵を受信する読取装置共通鍵受信部と、
前記読取装置共通鍵受信部が受信した共通鍵を用いて前記署名データ取得部が取得した署名データを復号化する署名データ復号部と、
前記署名データ復号部が復号化した署名データからデータを取得するデータ取得部と、
前記署名データ復号部が復号化した署名データからデジタル署名を取得するデジタル署名取得部と、
前記署名データ復号部が復号化した署名データから証明書を取得する証明書取得部と、
前記証明書取得部が取得した証明書を検証し、当該証明書に含まれる第２の公開鍵を取得するシステム証明書検証部と、
前記データ取得部が取得したデータと前記システム証明書検証部が取得した第２の公開鍵とを用いて前記デジタル署名取得部が取得したデジタル署名を検証するデジタル署名検証部と、
前記デジタル署名検証部が行った検証の結果を基に前記データ取得部が取得したデータを出力する出力部と、
前記データ取得部が取得したデータを前記カードデータ受信部に送信する読取装置データ送信部と、
認証データを入力する操作部と、
前記操作部が入力した認証データを認証データ受信部に送信する認証データ送信部とを備えることを特徴とするデータ交換システム。

【請求項１１】

データを書込む書込み装置と、データを読取る読取装置と、前記書込み装置からデータを受信し、受信したデータを記憶し、記憶したデータを前記読取装置に送信するメモリカードとを備えるデータ交換システムにおいて、
前記メモリカードは、
請求項５に記載のメモリカードであり、

前記書込み装置は、
データを入力する入力部と、
前記入力部が入力したデータを格納するデータ格納部と、
前記データ格納部に格納されたデータを暗号化して親展データを生成する親展データ生成部と、
前記親展データ生成部が生成した親展データを前記親展データ受信部に送信する親展データ送信部とを備え、
前記読取装置は、
認証データを入力する操作部と、
前記操作部が入力した認証データを前記認証データ受信部に送信する認証データ送信部と、
前記カードデータ送信部が送信したデータを受信する読取装置データ受信部と、
前記読取装置データ受信部が受信したデータを出力する出力部とを備えることを特徴とするデータ交換システム。

【請求項１２】
データを書込む書込み装置と、データを読取る読取装置と、前記書込み装置からデータを受信し、受信したデータを記憶し、記憶したデータを前記読取装置に送信するメモリカードとを備えるデータ交換システムにおいて、
前記メモリカードは、
請求項６に記載のメモリカードであり、
前記書込み装置は、
データを入力する入力部と、
前記入力部が入力したデータを格納するデータ格納部と、
前記証明書送信部が送信した証明書を受信する証明書受信部と、
前記証明書受信部が受信した証明書を検証し、当該証明書に含まれる第１の公開鍵を取得するカード証明書検証部と、
第２の秘密鍵を格納するシステム秘密鍵格納部と、
前記データ格納部に格納されたデータと前記システム秘密鍵格納部に格納された第２の秘密鍵とを用いてデジタル署名を生成するデジタル署名生成部と、
前記第２の秘密鍵と対を成す第２の公開鍵を含む証明書を格納するシステム証明書格納部と、
前記データ格納部に格納されたデータと前記デジタル署名生成部が生成したデジタル署名と前記システム証明書格納部に格納された証明書とを用いて署名データを生成する署名データ生成部と、
共通鍵を生成する共通鍵生成部と、
前記共通鍵生成部が生成した共通鍵を用いて前記署名データが生成した署名データを暗号化する署名データ暗号部と、
前記カード証明書検証部が取得した第１の公開鍵を用いて前記共通鍵生成部が生成した共通鍵を暗号化する共通鍵暗号部と、
前記署名データ暗号部が暗号化した署名データと前記共通鍵暗号部が暗号化した共通鍵とを用いて親展データを生成する親展データ生成部と、
前記親展データ生成部が生成した親展データを前記親展データ受信部に送信する親展データ送信部とを備え、
前記読取装置は、
認証データを入力する操作部と、
前記操作部が入力した認証データを前記認証データ受信部に送信する認証データ送信部と、
前記カードデータ送信部が送信したデータを受信する読取装置データ受信部と、
前記読取装置データ受信部が受信したデータを出力する出力部とを備えることを特徴とするデータ交換システム。

【請求項１３】
メモリカードが、書込み装置からデータを受信し、受信したデータを記憶し、記憶したデータを前記読取装置に送信するデータ交換方法において、
前記メモリカードは、
前記書込み装置がデータを暗号化して生成した親展データを前記書込み装置から受信し、
受信した親展データを格納し、
格納された親展データを前記読取装置に送信し、
送信した親展データを前記読取装置が復号化して取得したデータを前記読取装置から受信し、
前記読取装置が送信した認証データを受信し、
正規の認証データを格納し、
受信した認証データを格納された正規の認証データと照合して認証を行い、
認証が成功した場合、前記読取装置から受信したデータを格納し、
認証が成功した場合、格納されたデータを前記読取装置に送信し、
前記書込み装置は、
データを入力し、
入力したデータを格納し、
格納されたデータを暗号化して親展データを生成し、
生成した親展データを前記メモリカードに送信し、
前記読取装置は、
前記メモリカードが送信した親展データを受信し、
受信した親展データを復号化して得られるデータを取得し、
取得したデータを出力し、
取得したデータを前記メモリカードに送信し、
認証データを入力し、
入力した認証データを前記メモリカードに送信することを特徴とするデータ交換方法。
【請求項１４】
前記メモリカードは、さらに、
第１の公開鍵を含む証明書を格納し、
格納された証明書を前記書込み装置に送信し、
前記第１の公開鍵と対を成す第１の秘密鍵を格納し、
前記読取装置が送信した暗号化された共通鍵を受信し、
格納された第１の秘密鍵を用いて、受信した共通鍵を復号化し、
復号化した共通鍵を前記読取装置に送信し、
前記書込み装置は、さらに、
前記メモリカードが送信した証明書を受信し、
受信した証明書を検証し、当該証明書に含まれる第１の公開鍵を取得し、
第２の秘密鍵を格納し、
格納されたデータと第２の秘密鍵とを用いてデジタル署名を生成し、
前記第２の秘密鍵と対を成す第２の公開鍵を含む証明書を格納し、
格納されたデータと生成したデジタル署名と格納された第２の公開鍵を含む証明書とを用いて署名データを生成し、
共通鍵を生成し、
生成した共通鍵を用いて、生成した署名データを暗号化し、
取得した第１の公開鍵を用いて、生成した共通鍵を暗号化する共通鍵暗号部と、
暗号化した署名データと共通鍵とを用いて親展データを生成し、
前記読取装置は、
受信した親展データから暗号化された署名データを取得し、
受信した親展データから暗号化された共通鍵を取得し、

取得した暗号化された共通鍵を前記メモリカードに送信し、
前記メモリカードが送信した復号化された共通鍵を受信し、
受信した共通鍵を用いて、取得した署名データを復号化し、
復号化した署名データからデータを取得し、
復号化した署名データからデジタル署名を取得し、
復号化した署名データから証明書を取得し、
取得した証明書を検証し、当該証明書に含まれる第２の公開鍵を取得し、
取得したデータと第２の公開鍵とを用いて、取得したデジタル署名を検証し、
検証の結果を基に取得したデータを出力することを特徴とする請求項１３に記載のデータ交換方法。

【請求項１５】
メモリカードが、書込み装置からデータを受信し、受信したデータを記憶し、記憶したデータを前記読取装置に送信するデータ交換方法において、
前記メモリカードは、
前記書込み装置がデータを暗号化して生成した親展データを前記書込み装置から受信し、
受信した親展データを格納し、
格納された親展データを復号化して得られるデータを取得し、
取得したデータを格納し、
前記読取装置が送信した認証データを受信し、
正規の認証データを格納し、
受信した認証データを格納された正規の認証データと照合して認証を行い、
認証が成功した場合、格納されたデータを前記読取装置に送信し、
前記書込み装置は、
データを入力し、
入力したデータを格納し、
格納されたデータを暗号化して親展データを生成し、
生成した親展データを前記メモリカードに送信し、
前記読取装置は、
認証データを入力し、
入力した認証データを前記メモリカードに送信し、
前記メモリカードが送信したデータを受信し、
受信したデータを出力することを特徴とするデータ交換方法。

【請求項１６】
前記メモリカードは、さらに、
第１の公開鍵を含む証明書を格納し、
格納された証明書を前記書込み装置に送信し、
前記第１の公開鍵と対を成す第１の秘密鍵を格納し、
復号化した署名データからデータを取得し、
格納された親展データから暗号化された署名データを取得し、
格納された親展データから暗号化された共通鍵を取得し、
格納された第１の秘密鍵を用いて、取得した共通鍵を復号化し、
復号化した共通鍵を用いて、取得した署名データを復号化し、
復号化した署名データからデジタル署名を取得し、
復号化した署名データから第２の公開鍵を含む証明書を取得し、
取得した証明書を検証し、当該証明書に含まれる第２の公開鍵を取得し、
取得したデータと第２の公開鍵とを用いて、取得したデジタル署名を検証し、
前記書込み装置は、
データを入力し、
入力したデータを格納し、

前記メモリカードが送信した証明書を受信し、
受信した証明書を検証し、当該証明書に含まれる第１の公開鍵を取得し、
第２の秘密鍵を格納し、
格納されたデータと第２の秘密鍵とを用いてデジタル署名を生成し、
前記第２の秘密鍵と対を成す第２の公開鍵を含む証明書を格納し、
格納されたデータと生成したデジタル署名と格納された第２の公開鍵を含む証明書とを用いて署名データを生成し、
共通鍵を生成し、
生成した共通鍵を用いて、生成した署名データを暗号化し、
取得した第１の公開鍵を用いて、生成した共通鍵を暗号化し、
暗号化した署名データと共通鍵とを用いて親展データを生成し、
生成した親展データを前記メモリカードに送信し、
前記読取装置は、
認証データを入力し、
入力した認証データを前記メモリカードに送信し、
前記メモリカードが送信したデータを受信し、
受信したデータを出力することを特徴とする請求項１５に記載のデータ交換方法。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、安全なデータの交換をするためのメモリカード、データ交換システム及びデータ交換方法に関するものである。

【背景技術】

【０００２】

身分証明書や会員券や診察券にＩＣカードを利用することが可能となってきた。ＩＣカードには書込み・読み出しが可能な領域を持たせることが可能である。ある機関がＩＣカードに情報を書込み、ＩＣカード所有者や別の機関がその情報をＩＣカードから読み出すことで、情報を受け渡したり、共有したりすることができるようになってきた。特許文献１では、患者のＩＣカードにある医療機関が医療情報を書込むと、別の医療機関がその医療情報を参照することができる仕組みを提示している。

【特許文献１】特開２０００－２８５１８９公報

【発明の開示】

【発明が解決しようとする課題】

【０００３】

ＩＣカードの利用者がそのＩＣカードの正しい所有者であることを検証するために、ＩＣカードを利用するシステムでは、現金自動預け払い機（ＡＴＭ，Ａｕｔｏｍａｔｅｄ Ｔｅｌｌｅｒ Ｍａｃｈｉｎｅ）のように、ＩＣカードの所有者しか知らないＰＩＮ（Ｐｅｒｓｏｎａｌ Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ Ｎｕｍｂｅｒ）を入力させることが一般的である。しかし、その場合、ＩＣカードの挿入されるシステムが、利用者の入力するＰＩＮ情報を不正に蓄積したり利用したりすることのない信用できるシステムでなければならない。そこで、ＰＩＮの入力が必要なＩＣカードを用いるシステムでは、ＩＣカードとＩＣカードの挿入されるシステム間で相互認証をするのが一般的である。相互認証をするためには、共通鍵暗号方式における鍵情報を安全に共有したり、公開鍵暗号方式における公開鍵・秘密鍵のペアを安全に持ち合ったりする必要がある。

【０００４】

また、ＰＩＮの入力が必要なＩＣカードを用いるシステムでは、ＩＣカードをある機関に手渡し、その機関にてＩＣカードに対してＰＩＮが必要な処理をする場合、機関内の操作者だけでは処理が遂行できず、ＩＣカードの所有者にＰＩＮを入力してもらう必要がある。その結果、ＩＣカード所有者がＰＩＮを入力するために機関のシステムの傍に待機していなくてはならないといった制約がある。

【０００５】
本発明の目的は、ＰＩＮの入力をしなくても、ＩＣカードの所有者しか読めない情報をＩＣカードに書込むことができ、かつ書込まれた情報の作成者の認証及び改ざんの防止を実現することで、ＩＣカードに書込まれたデータが、ＩＣカードの所有者しか読めないこと、書込まれたデータの作者が特定できること、書込まれたデータが改ざんされていないことを保証することである。
【課題を解決するための手段】
【０００６】
本発明のメモリカードは、
前記書込み装置がデータを暗号化して生成した親展データを前記書込み装置から受信する親展データ受信部と、
前記親展データ受信部が受信した親展データを格納するパブリック格納部と、
前記読取装置が送信した認証データを受信する認証データ受信部と、
正規の認証データを格納する認証データ格納部と、
前記認証データ受信部が受信した認証データを前記認証データ格納部に格納された正規の認証データと照合して認証を行う認証部と、
前記認証部が行った認証が成功した場合、前記パブリック格納部に格納された親展データを復号化して得られるデータを格納するプライベート格納部と、
前記認証部が行った認証が成功した場合、前記プライベート格納部に格納されたデータを前記読取装置に送信するカードデータ送信部とを備えることを特徴とする。
【０００７】
また、前記カードデータ送信部は、
前記パブリック格納部に格納された親展データを前記読取装置に送信し、
前記メモリカードは、さらに、
前記カードデータ送信部が送信した親展データを前記読取装置が復号化して取得したデータを前記読取装置から受信するカードデータ受信部を備え、
前記プライベート格納部は、
前記認証部が行った認証が成功した場合、前記カードデータ受信部が受信したデータを格納することを特徴とする。
【０００８】
また、前記メモリカードは、さらに、
第１の公開鍵を含む証明書を格納するカード証明書格納部と、
前記カード証明書格納部に格納された証明書を前記書込み装置に送信する証明書送信部と、
前記第１の公開鍵と対を成す第１の秘密鍵を格納するカード秘密鍵格納部と、
前記読取装置が送信した暗号化された共通鍵を受信するカード共通鍵受信部と、
前記カード秘密鍵格納部に格納された第１の秘密鍵を用いて前記カード共通鍵受信部が受信した共通鍵を復号化する共通鍵復号部と、
前記共通鍵復号部が復号化した共通鍵を前記読取装置に送信するカード共通鍵送信部とを備えることを特徴とする。
【０００９】
また、前記認証データ格納部は、
正規の認証データとして暗証番号（ＰＩＮ，Ｐｅｒｓｏｎａｌ　Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ　Ｎｕｍｂｅｒ）を格納することを特徴とする。
【００１０】
また、前記メモリカードは、さらに、
前記パブリック格納部に格納された親展データを復号化して得られるデータを取得するデータ取得部を備え、
前記プライベート格納部は、
前記データ取得部が取得したデータを格納することを特徴とする。

【００１１】
また、前記メモリカードは、さらに、
第１の公開鍵を含む証明書を格納するカード証明書格納部と、
前記カード証明書格納部に格納された証明書を前記書込み装置に送信する証明書送信部と、
前記第１の公開鍵と対を成す第１の秘密鍵を格納するカード秘密鍵格納部と、
前記パブリック格納部に格納された親展データから暗号化された署名データを取得する署名データ取得部と、
前記パブリック格納部に格納された親展データから暗号化された共通鍵を取得する共通鍵取得部と、
前記カード秘密鍵格納部に格納された第１の秘密鍵を用いて前記共通鍵取得部が取得した共通鍵を復号化する共通鍵復号部と、
前記共通鍵復号部が復号化した共通鍵を用いて前記署名データ取得部が取得した署名データを復号化する署名データ復号部と、
前記署名データ復号部が復号化した署名データからデジタル署名を取得するデジタル署名取得部と、
前記署名データ復号部が復号化した署名データから第２の公開鍵を含む証明書を取得する証明書取得部と、
前記証明書取得部が取得した証明書を検証し、当該証明書に含まれる第２の公開鍵を取得するシステム証明書検証部と、
前記データ取得部が取得したデータと前記システム証明書検証部が取得した第２の公開鍵とを用いて前記デジタル署名取得部が取得したデジタル署名を検証するデジタル署名検証部とを備え、
前記データ取得部は、
前記署名データ復号部が復号化した署名データからデータを取得することを特徴とする。
【００１２】
また、前記メモリカードは、さらに、
証明書を発行する認証局（ＣＡ，Ｃｅｒｔｉｆｉｃａｔｅ　Ａｕｔｈｏｒｉｔｙ）から証明書を取得する認証局通信部を備え、
前記システム証明書検証部は、
前記認証局通信部が取得した証明書を基に前記証明書取得部が取得した証明書を検証することを特徴とする。
【００１３】
また、前記認証データ格納部は、
正規の認証データとして暗証番号（ＰＩＮ，Ｐｅｒｓｏｎａｌ　Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ　Ｎｕｍｂｅｒ）を格納することを特徴とする。
【００１４】
本発明のデータ交換システムは、
データを書込む書込み装置と、データを読取る読取装置と、前記書込み装置からデータを受信し、受信したデータを記憶し、記憶したデータを前記読取装置に送信するメモリカードとを備え、
前記メモリカードは、
前述のメモリカードであり、
前記書込み装置は、
データを入力する入力部と、
前記入力部が入力したデータを格納するデータ格納部と、
前記データ格納部に格納されたデータを暗号化して親展データを生成する親展データ生成部と、
前記親展データ生成部が生成した親展データを前記親展データ受信部に送信する親展デ

ータ送信部とを備え、
前記読取装置は、
前記カードデータ送信部が送信した親展データを受信する読取装置データ受信部と、
前記読取装置データ受信部が受信した親展データを復号化して得られるデータを取得するデータ取得部と、
前記データ取得部が取得したデータを出力する出力部と、
前記データ取得部が取得したデータを前記カードデータ受信部に送信する読取装置データ送信部と、
認証データを入力する操作部と、
前記操作部が入力した認証データを前記認証データ受信部に送信する認証データ送信部とを備えることを特徴とする。

【００１５】

本発明のデータ交換システムは、
データを書込む書込み装置と、データを読取る読取装置と、前記書込み装置からデータを受信し、受信したデータを記憶し、記憶したデータを前記読取装置に送信するメモリカードとを備え、
前記メモリカードは、
前述のメモリカードであり、
前記書込み装置は、
データを入力する入力部と、
前記入力部が入力したデータを格納するデータ格納部と、
前記証明書送信部が送信した証明書を受信する証明書受信部と、
前記証明書受信部が受信した証明書を検証し、当該証明書に含まれる第１の公開鍵を取得するカード証明書検証部と、
第２の秘密鍵を格納するシステム秘密鍵格納部と、
前記データ格納部に格納されたデータと前記システム秘密鍵格納部に格納された第２の秘密鍵とを用いてデジタル署名を生成するデジタル署名生成部と、
前記第２の秘密鍵と対を成す第２の公開鍵を含む証明書を格納するシステム証明書格納部と、
前記データ格納部に格納されたデータと前記デジタル署名生成部が生成したデジタル署名と前記システム証明書格納部に格納された証明書とを用いて署名データを生成する署名データ生成部と、
共通鍵を生成する共通鍵生成部と、
前記共通鍵生成部が生成した共通鍵を用いて前記署名データが生成した署名データを暗号化する署名データ暗号部と、
前記カード証明書検証部が取得した第１の公開鍵を用いて前記共通鍵生成部が生成した共通鍵を暗号化する共通鍵暗号部と、
前記署名データ暗号部が暗号化した署名データと前記共通鍵暗号部が暗号化した共通鍵とを用いて親展データを生成する親展データ生成部と、
前記親展データ生成部が生成した親展データを前記親展データ受信部に送信する親展データ送信部とを備え、
前記読取装置は、
前記カードデータ送信部が送信した親展データを受信する読取装置データ受信部と、
前記読取装置データ受信部が受信した親展データから暗号化された署名データを取得する署名データ取得部と、
前記読取装置データ受信部が受信した親展データから暗号化された共通鍵を取得する共通鍵取得部と、
前記共通鍵取得部が取得した暗号化された共通鍵を前記カード共通鍵受信部に送信する読取装置共通鍵送信部と、
前記カード共通鍵送信部が送信した復号化された共通鍵を受信する読取装置共通鍵受信

部と、
前記読取装置共通鍵受信部が受信した共通鍵を用いて前記署名データ取得部が取得した署名データを復号化する署名データ復号部と、
前記署名データ復号部が復号化した署名データからデータを取得するデータ取得部と、
前記署名データ復号部が復号化した署名データからデジタル署名を取得するデジタル署名取得部と、
前記署名データ復号部が復号化した署名データから証明書を取得する証明書取得部と、
前記証明書取得部が取得した証明書を検証し、当該証明書に含まれる第２の公開鍵を取得するシステム証明書検証部と、
前記データ取得部が取得したデータと前記システム証明書検証部が取得した第２の公開鍵とを用いて前記デジタル署名取得部が取得したデジタル署名を検証するデジタル署名検証部と、
前記デジタル署名検証部が行った検証の結果を基に前記データ取得部が取得したデータを出力する出力部と、
前記データ取得部が取得したデータを前記カードデータ受信部に送信する読取装置データ送信部と、
認証データを入力する操作部と、
前記操作部が入力した認証データを認証データ受信部に送信する認証データ送信部とを備えることを特徴とする。
【００１６】
本発明のデータ交換システムは、
データを書込む書込み装置と、データを読取る読取装置と、前記書込み装置からデータを受信し、受信したデータを記憶し、記憶したデータを前記読取装置に送信するメモリカードとを備え、
前記メモリカードは、
前述のメモリカードであり、
前記書込み装置は、
データを入力する入力部と、
前記入力部が入力したデータを格納するデータ格納部と、
前記データ格納部に格納されたデータを暗号化して親展データを生成する親展データ生成部と、
前記親展データ生成部が生成した親展データを前記親展データ受信部に送信する親展データ送信部とを備え、
前記読取装置は、
認証データを入力する操作部と、
前記操作部が入力した認証データを前記認証データ受信部に送信する認証データ送信部と、
前記カードデータ送信部が送信したデータを受信する読取装置データ受信部と、
前記読取装置データ受信部が受信したデータを出力する出力部とを備えることを特徴とする。
【００１７】
本発明のデータ交換システムは、
データを書込む書込み装置と、データを読取る読取装置と、前記書込み装置からデータを受信し、受信したデータを記憶し、記憶したデータを前記読取装置に送信するメモリカードとを備え、
前記メモリカードは、
前述のメモリカードであり、
前記書込み装置は、
データを入力する入力部と、
前記入力部が入力したデータを格納するデータ格納部と、

前記証明書送信部が送信した証明書を受信する証明書受信部と、
前記証明書受信部が受信した証明書を検証し、当該証明書に含まれる第１の公開鍵を取得するカード証明書検証部と、
第２の秘密鍵を格納するシステム秘密鍵格納部と、
前記データ格納部に格納されたデータと前記システム秘密鍵格納部に格納された第２の秘密鍵とを用いてデジタル署名を生成するデジタル署名生成部と、
前記第２の秘密鍵と対を成す第２の公開鍵を含む証明書を格納するシステム証明書格納部と、
前記データ格納部に格納されたデータと前記デジタル署名生成部が生成したデジタル署名と前記システム証明書格納部に格納された証明書とを用いて署名データを生成する署名データ生成部と、
共通鍵を生成する共通鍵生成部と、
前記共通鍵生成部が生成した共通鍵を用いて前記署名データが生成した署名データを暗号化する署名データ暗号部と、
前記カード証明書検証部が取得した第１の公開鍵を用いて前記共通鍵生成部が生成した共通鍵を暗号化する共通鍵暗号部と、
前記署名データ暗号部が暗号化した署名データと前記共通鍵暗号部が暗号化した共通鍵とを用いて親展データを生成する親展データ生成部と、
前記親展データ生成部が生成した親展データを前記親展データ受信部に送信する親展データ送信部とを備え、
前記読取装置は、
認証データを入力する操作部と、
前記操作部が入力した認証データを前記認証データ受信部に送信する認証データ送信部と、
前記カードデータ送信部が送信したデータを受信する読取装置データ受信部と、
前記読取装置データ受信部が受信したデータを出力する出力部とを備えることを特徴とする。

【００１８】

本発明のデータ交換方法では、
前記メモリカードは、
前記書込み装置がデータを暗号化して生成した親展データを前記書込み装置から受信し、
受信した親展データを格納し、
格納された親展データを前記読取装置に送信し、
送信した親展データを前記読取装置が復号化して取得したデータを前記読取装置から受信し、
前記読取装置が送信した認証データを受信し、
正規の認証データを格納し、
受信した認証データを格納された正規の認証データと照合して認証を行い、
認証が成功した場合、前記読取装置から受信したデータを格納し、
認証が成功した場合、格納されたデータを前記読取装置に送信し、
前記書込み装置は、
データを入力し、
入力したデータを格納し、
格納されたデータを暗号化して親展データを生成し、
生成した親展データを前記メモリカードに送信し、
前記読取装置は、
前記メモリカードが送信した親展データを受信し、
受信した親展データを復号化して得られるデータを取得し、
取得したデータを出力し、

取得したデータを前記メモリカードに送信し、
認証データを入力し、
入力した認証データを前記メモリカードに送信することを特徴とする。
【００１９】
また、前記メモリカードは、さらに、
第１の公開鍵を含む証明書を格納し、
格納された証明書を前記書込み装置に送信し、
前記第１の公開鍵と対を成す第１の秘密鍵を格納し、
前記読取装置が送信した暗号化された共通鍵を受信し、
格納された第１の秘密鍵を用いて、受信した共通鍵を復号化し、
復号化した共通鍵を前記読取装置に送信し、
前記書込み装置は、さらに、
前記メモリカードが送信した証明書を受信し、
受信した証明書を検証し、当該証明書に含まれる第１の公開鍵を取得し、
第２の秘密鍵を格納し、
格納されたデータと第２の秘密鍵とを用いてデジタル署名を生成し、
前記第２の秘密鍵と対を成す第２の公開鍵を含む証明書を格納し、
格納されたデータと生成したデジタル署名と格納された第２の公開鍵を含む証明書とを用いて署名データを生成し、
共通鍵を生成し、
生成した共通鍵を用いて、生成した署名データを暗号化し、
取得した第１の公開鍵を用いて、生成した共通鍵を暗号化する共通鍵暗号部と、
暗号化した署名データと共通鍵とを用いて親展データを生成し、
前記読取装置は、
受信した親展データから暗号化された署名データを取得し、
受信した親展データから暗号化された共通鍵を取得し、
取得した暗号化された共通鍵を前記メモリカードに送信し、
前記メモリカードが送信した復号化された共通鍵を受信し、
受信した共通鍵を用いて、取得した署名データを復号化し、
復号化した署名データからデータを取得し、
復号化した署名データからデジタル署名を取得し、
復号化した署名データから証明書を取得し、
取得した証明書を検証し、当該証明書に含まれる第２の公開鍵を取得し、
取得したデータと第２の公開鍵とを用いて、取得したデジタル署名を検証し、
検証の結果を基に取得したデータを出力することを特徴とする。
【００２０】
本発明のデータ交換方法では、
前記メモリカードは、
前記書込み装置がデータを暗号化して生成した親展データを前記書込み装置から受信し、
受信した親展データを格納し、
格納された親展データを復号化して得られるデータを取得し、
取得したデータを格納し、
前記読取装置が送信した認証データを受信し、
正規の認証データを格納し、
受信した認証データを格納された正規の認証データと照合して認証を行い、
認証が成功した場合、格納されたデータを前記読取装置に送信し、
前記書込み装置は、
データを入力し、
入力したデータを格納し、

格納されたデータを暗号化して親展データを生成し、
生成した親展データを前記メモリカードに送信し、
前記読取装置は、
認証データを入力し、
入力した認証データを前記メモリカードに送信し、
前記メモリカードが送信したデータを受信し、
受信したデータを出力することを特徴とする。

【００２１】

また、前記メモリカードは、さらに、
第１の公開鍵を含む証明書を格納し、
格納された証明書を前記書込み装置に送信し、
前記第１の公開鍵と対を成す第１の秘密鍵を格納し、
復号化した署名データからデータを取得し、
格納された親展データから暗号化された署名データを取得し、
格納された親展データから暗号化された共通鍵を取得し、
格納された第１の秘密鍵を用いて、取得した共通鍵を復号化し、
復号化した共通鍵を用いて、取得した署名データを復号化し、
復号化した署名データからデジタル署名を取得し、
復号化した署名データから第２の公開鍵を含む証明書を取得し、
取得した証明書を検証し、当該証明書に含まれる第２の公開鍵を取得し、
取得したデータと第２の公開鍵とを用いて、取得したデジタル署名を検証し、
前記書込み装置は、
データを入力し、
入力したデータを格納し、
前記メモリカードが送信した証明書を受信し、
受信した証明書を検証し、当該証明書に含まれる第１の公開鍵を取得し、
第２の秘密鍵を格納し、
格納されたデータと第２の秘密鍵とを用いてデジタル署名を生成し、
前記第２の秘密鍵と対を成す第２の公開鍵を含む証明書を格納し、
格納されたデータと生成したデジタル署名と格納された第２の公開鍵を含む証明書とを用いて署名データを生成し、
共通鍵を生成し、
生成した共通鍵を用いて、生成した署名データを暗号化し、
取得した第１の公開鍵を用いて、生成した共通鍵を暗号化し、
暗号化した署名データと共通鍵とを用いて親展データを生成し、
生成した親展データを前記メモリカードに送信し、
前記読取装置は、
認証データを入力し、
入力した認証データを前記メモリカードに送信し、
前記メモリカードが送信したデータを受信し、
受信したデータを出力することを特徴とする。

【発明の効果】

【００２２】

本発明により、ＰＩＮの入力をしなくても、ＩＣカードの所有者しか読めない情報をＩＣカードに書込むことができ、かつ書込まれた情報の作成者の認証及び改ざんの防止を実現できる。また、ＩＣカードに書込まれたデータが、ＩＣカードの所有者しか読めないこと、書込まれたデータの作者が特定できること、書込まれたデータが改ざんされていないことを保証することが可能となる。

【発明を実施するための最良の形態】

【００２３】

以下、本発明の実施の形態を図に基づいて説明する。なお、下記実施の形態１及び２に係るメモリカードは、暗号認証機能をもったメモリカードであるとし、これをセキュアメモリカードと呼ぶ。ただし、メモリカードと同様の機能を備えるＩＣカード等も適用可能である。

【００２４】

また、下記実施の形態１及び２では、書込み装置の例として、ＰＣ（パーソナルコンピュータ）を用いて説明するが、メモリカードにデータを書込む機能を有していれば他の装置でも適用可能である。同様に、下記実施の形態１及び２では、読取装置の例として、携帯電話を用いて説明するが、メモリカードからデータを読取る機能を有していれば他の装置でも適用可能である。

【００２５】

実施の形態１.

本実施の形態では、セキュアメモリカードに格納した証明書とセキュアメモリカードのＰＩＮ認証なしで書込むことができるパブリック格納部を利用して、薬局においてセキュアメモリカードを用いて投薬指示書を安全に利用者に提供できるようにしている。

【００２６】

図１に以下のような利用者と薬局のやりとりの概要を示す。

（１）利用者１０４は、薬局の受付にて、病院から発行された処方箋と携帯電話１０３に挿入されていたセキュアメモリカード１０１を提供する。

（２）薬局員１０５は、セキュアメモリカード１０１に投薬指示書を書込む。

（３）利用者１０４は、セキュアメモリカード１０１を携帯電話１０３に装着して投薬指示書の内容を見る。

【００２７】

利用者１０４は携帯電話１０３にセキュアメモリカード１０１を装着している。薬局に入ると紙の処方箋と携帯電話１０３から取り出したセキュアメモリカード１０１を受付に渡す。薬局内では、薬局員１０５が利用者１０４に提供する薬を用意した後、ＰＣ１０２にセキュアメモリカード１０１を装着し、その薬の投薬指示書を、ＰＣ１０２を用いてセキュアメモリカード１０１に書込む。そして、利用者１０４に薬とセキュアメモリカード１０１を渡す。利用者１０４は携帯電話１０３にセキュアメモリカード１０１を装着し、投薬指示書を携帯電話１０３の画面で閲覧する。

【００２８】

図２は本実施の形態に係るシステムのセキュアメモリカード１０１とＰＣ１０２との構成を示している。また、図３は本実施の形態に係るシステムのセキュアメモリカード１０１と携帯電話１０３との構成を示している。本システムはセキュアメモリカード１０１、セキュアメモリカード１０１を所有する利用者１０４しか読めない情報をセキュアメモリカード１０１に書込むＰＣ１０２、セキュアメモリカード１０１から情報を読み出し表示する携帯電話１０３から成る。

【００２９】

セキュアメモリカード１０１は、ＲＳＡ（Ｒｉｖｅｓｔ　Ｓｈａｍｉｒ　Ａｄｌｅｍａｎ）や楕円暗号等の公開鍵暗号方式における秘密鍵を格納するカード秘密鍵格納部２０８、携帯電話１０３から共通鍵を受信するカード共通鍵受信部２４２、カード秘密鍵格納部２０８に格納された秘密鍵を使ってこの共通鍵を復号化する共通鍵復号部２３５、復号化した共通鍵を携帯電話１０３に送信するカード共通鍵送信部２０９、この秘密鍵と対を成す公開鍵の証明書を格納し、削除は不可であるが、読み出しは認証なしで可能であるカード証明書格納部２０２、この証明書をＰＣ１０２に送信する証明書送信部２０１、セキュアメモリカード所有者しか知らないＰＩＮを格納する認証データ格納部２０５、携帯電話１０３で入力されたＰＩＮを受信する認証データ受信部２０７、ＰＩＮ照合を行う認証部２０６、正しいＰＩＮが入力された場合のみ外部から読み書きできるプライベート格納部２０３、携帯電話１０３からデータを受信するカードデータ受信部２０４、ＰＩＮ照合なしで外部から読み書きできるパブリック格納部２１０、ＰＣ１０２から親展データを受信

する親展データ受信部２１１、携帯電話１０３にデータを送信するカードデータ送信部２１２から構成される。

【００３０】

ここで、親展データとは、例えばＲＦＣ－２６３０（“Ｃｒｙｐｔｏｇｒａｐｈｉｃ Ｍｅｓｓａｇｅ Ｓｙｎｔａｘ，” ＩＥＴＦ Ｎｅｔｗｏｒｋ Ｗｏｒｋｉｎｇ Ｇｒｏｕｐ，Ｒ．Ｈｏｕｓｌｅｙ，ＲＦＣ－２６３０，Ｊｕｎｅ １９９９）に開示されているＥｎｖｅｌｏｐｅｄＤａｔａであり、暗号対象データとこの暗号対象データの暗号化に使用された暗号化された共通鍵とから構成される。本実施の形態では、暗号対象データは署名データである。

【００３１】

署名データとは、例えばＲＦＣ－２６３０に開示されているＳｉｇｎｅｄＤａｔａであり、投薬指示書等、ＰＣ１０２のユーザがセキュアメモリカード１０１の所有者に送ろうとするデータと、ＰＣ１０２又はＰＣ１０２のユーザのデジタル署名と証明書とから構成される。

【００３２】

セキュアメモリカード１０１に利用者１０４しか読めないデータを書込むＰＣ１０２は、薬局員１０５のようなユーザからの入力を受け付ける入力部２１３、入力されたデータ等を格納するデータ格納部２１５、セキュアメモリカード１０１から証明書を受信する証明書受信部２１４、この証明書の正当性を検証するカード証明書検証部２１６、ＲＳＡや楕円暗号等の公開鍵暗号方式における秘密鍵を格納するシステム秘密鍵格納部２１８、この秘密鍵と対をなす公開鍵の証明書を格納するシステム証明書格納部２１７、デジタル署名を生成するデジタル署名生成部２２０、データ格納部２１５に格納されたデータとシステム証明書格納部２１７に格納された証明書とデジタル署名生成部２２０が生成したデジタル署名とを用いて、署名データを生成する署名データ生成部２１９、この署名データを暗号化する署名データ暗号部２２２、共通鍵を生成する共通鍵生成部２２１、この共通鍵を暗号化する共通鍵暗号部２２３、これらの暗号化された署名データと共通鍵とを用いて、親展データを生成する親展データ生成部２２４、セキュアメモリカード１０１にこの親展データを送信する親展データ送信部２２５から構成される。暗号機能を有する各部は、共通鍵暗号方式や公開鍵暗号方式の暗号・復号、ハッシュの計算、乱数の生成等を行う。また、図示していないが、本実施の形態ではＰＣ１０２は液晶ディスプレイ（ＬＣＤ）等の表示部を有することとする。

【００３３】

利用者１０４の所有する携帯電話１０３は、セキュアメモリカード１０１にデータを送信する読取装置データ送信部２２６、セキュアメモリカード１０１からデータを受信する読取装置データ受信部２３９、セキュアメモリカード１０１から受信した親展データに含まれる共通鍵を取得する共通鍵取得部２３７、セキュアメモリカード１０１にこの共通鍵を送信する読取装置共通鍵送信部２４１、セキュアメモリカード１０１が復号化した共通鍵をセキュアメモリカード１０１から受信する読取装置共通鍵受信部２３３、セキュアメモリカード１０１から受信した親展データに含まれる署名データを取得する署名データ取得部２４０、この署名データを復号化する署名データ復号部２３８、復号化された署名データから投薬指示書等のデータを取得するデータ取得部２２７、復号化された署名データからデジタル署名を取得するデジタル署名取得部２３２、このデジタル署名の正当性を検証するデジタル署名検証部２３１、復号化された署名データから証明書を取得する証明書取得部２３６、この証明書の正当性を検証するシステム証明書検証部２３４、利用者１０４からの入力を受け付けるダイヤルボタン等の操作部２２８、利用者１０４に対するインタフェースを提供する液晶ディスプレイ（ＬＣＤ）等の出力部２２９、セキュアメモリカード１０１にＰＩＮを送信する認証データ送信部２３０から構成される。復号機能を有する各部は、共通鍵暗号方式や公開鍵暗号方式の暗号・復号、ハッシュの計算、乱数の生成等を行う。

【００３４】

図４は、セキュアメモリカード１０１に対して、薬局にあるＰＣ１０２を用いて薬局員１０５が利用者１０４しか読めない投薬指示書をＰＩＮ入力なしに書込む処理を示すシーケンス図である。また、図５は同様の処理を示すフロー図である。

【００３５】

上記処理の前に、薬局員１０５は、利用者１０４に発行する投薬指示書をＰＣ１０２で特定すると、セキュアメモリカード１０１を、薬局にあるＰＣ１０２に装着する。そして薬局員がＰＣ１０２の入力部２１３から投薬指示書の発行指示をＰＣ１０２に対して行う。ＰＣ１０２のデータ格納部２１５は、入力された投薬指示書のデータを格納する。これ以降の処理フローを以下に説明する。

【００３６】

ＰＣ１０２は、セキュアメモリカード１０１に対して証明書の取得要求を送付する。セキュアメモリカード１０１の証明書送信部２０１は、証明書取得要求を受け取ると、カード証明書格納部２０２から利用者１０４の証明書を読み出し、ＰＣ１０２に送付する。ＰＣ１０２の証明書受信部２１４は、この証明書を受信する（Ｓ５０１）。

【００３７】

カード証明書検証部２１６は、入手した利用者１０４の証明書（以降、利用者証明書）を検証する（Ｓ５０２）。カード証明書検証部２１６は、信用する認証局（ＣＡ，Ｃｅｒｔｉｆｉｃａｔｅ　Ａｕｔｈｏｒｉｔｙ）が発行する証明書や証明書の失効リスト（ＣＲＬ，Ｃｅｒｔｉｆｉｃａｔｅ　Ｒｅｖｏｃａｔｉｏｎ　Ｌｉｓｔ）を保持し、証明書検証に利用する。利用者証明書の検証処理において、認証局の証明書や証明書の失効リストを通信により外部から入手することも可能である。

【００３８】

利用者証明書の正当性が確認されなかった（検証結果がＮＧ）場合、処理を終了する。利用者証明書の正当性が確認された（検証結果がＯＫ）場合、デジタル署名生成部２２０において、システム秘密鍵格納部２１８に格納される秘密鍵を用いて投薬指示書に対するデジタル署名を生成する。そして、投薬指示書とデジタル署名とシステム証明書格納部２１７に格納される証明書（以降薬局証明書）とを署名データ生成部２１９において結合し、署名データを生成する（Ｓ５０３）。

【００３９】

次に、共通鍵生成部２２１が共通鍵をランダムに生成する。署名データ暗号部２２２は、その共通鍵で署名データを暗号化する。共通鍵暗号部２２３は、その共通鍵を利用者証明書に含まれる公開鍵で暗号化する。そして親展データ生成部２２４は、暗号化された投薬指示書と暗号化された共通鍵とを結合して親展データを生成する（Ｓ５０４）。

【００４０】

親展データは、ＰＣ１０２の親展データ送信部２２５からセキュアメモリカード１０１の親展データ受信部２１１に送信される。セキュアメモリカード１０１は、受信した親展データをパブリック格納部２１０にファイルとして書込む（Ｓ５０５）。ファイル名には、例えば「投薬指示書２００４０４０１」等の内容と作成年月日がわかりやすい名前をつける。この書込み処理は、パブリック格納部２１０への書込み処理なので、ＰＩＮの入力操作は不要である。

【００４１】

図６は、セキュアメモリカード１０１に書込まれた暗号化された投薬指示書を利用者１０４が所有する携帯電話１０３を用いて閲覧する処理を示すシーケンス図である。また、図７は同様の処理を示すフロー図である。

【００４２】

薬局でセキュアメモリカード１０１を受け取った利用者１０４は、携帯電話１０３にセキュアメモリカード１０１を装着する。携帯電話１０３は、セキュアメモリカード１０１のパブリック格納部２１０のファイル一覧を取得する（Ｓ７０１）。

【００４３】

利用者１０４は、一覧の中から投薬指示書を操作部２２８より選択する。このとき、利

用者１０４のためにそのファイル一覧を出力部２２９に表示してもよい。選択されたファイルの取得要求を携帯電話１０３から受信したセキュアメモリカード１０１は、親展データのファイル（親展ファイル）となっている投薬指示書をパブリック格納部２１０から取り出し、カードデータ送信部２１２より送信する。携帯電話１０３の読取装置データ受信部２３９は、この親展ファイルを受信する（Ｓ７０２）。

【００４４】

携帯電話１０３は、読み出した親展データをデコードし、共通鍵取得部２３７において、暗号化された共通鍵を取得する。また、署名データ取得部２４０において、その共通鍵で暗号化された投薬指示書の署名データを取得する。そして、読取装置共通鍵送信部２４１は、この暗号化された共通鍵をセキュアメモリカード１０１に送信する。セキュアメモリカード１０１は、カード共通鍵受信部２４２において、この共通鍵を受信し、共通鍵復号部２３５において、カード秘密鍵格納部２０８に格納された秘密鍵を使ってこの共通鍵を復号化する。復号化された共通鍵は、カード共通鍵送信部２０９によって携帯電話１０３に送信される。携帯電話１０３は、読取装置共通鍵受信部２３３において、この復号化された共通鍵を受信する。署名データ復号部２３８は、この共通鍵を用いて、暗号化された投薬指示書の署名データを復号化する（Ｓ７０３）。

【００４５】

復号化された署名データは、投薬指示書、デジタル署名、薬局証明書に分離され、それぞれデータ取得部２２７、デジタル署名取得部２３２、証明書取得部２３６に渡される。そして、システム証明書検証部２３４は、証明書取得部２３６が取得した薬局証明書の検証を行う。システム証明書検証部２３４は、信用する認証局が発行した証明書や証明書の失効リストを保持し、証明書検証に利用する。薬局証明書の検証処理において、認証局の証明書や証明書の失効リストを通信により外部から入手することも可能である。薬局証明書の正当性が確認できた場合、デジタル署名検証部２３１において、投薬指示書と薬局証明書に含まれる公開鍵とデジタル署名とを用いて、デジタル署名の正当性を検証する（Ｓ７０４）。

【００４６】

デジタル署名の正当性が確認できなかった（検証結果がＮＧ）場合、処理を終了する。デジタル署名の正当性が確認できた（検証結果がＯＫ）場合、データ取得部２２７が取得した投薬指示書を出力部２２９より利用者１０４が閲覧できるようにする（Ｓ７０５）。

【００４７】

投薬指示書の閲覧が完了すると、携帯電話１０３は、投薬指示書をプライベート格納部２０３に格納する要求をセキュアメモリカード１０１に送信する（Ｓ７０６）。

【００４８】

すると、セキュアメモリカード１０１は、ＰＩＮの入力を携帯電話１０３に求める。利用者１０４は操作部２２８を用いてＰＩＮを入力する（Ｓ７０７）。このとき、例えば出力部２２９にＰＩＮ入力ウィンドウを表示し、利用者１０４にＰＩＮ入力ウィンドウの所定のフィールドにＰＩＮを入力させてもよい。入力されたＰＩＮは、携帯電話１０３の認証データ送信部２３０から、セキュアメモリカード１０１の認証データ受信部２０７に送信される。

【００４９】

セキュアメモリカード１０１の認証部２０６は、受け取ったＰＩＮと認証データ格納部２０５に格納されているＰＩＮを比較することでＰＩＮを照合し、認証を行う。認証が失敗した（照合結果がＮＧ）場合、処理を終了する。認証が成功した（照合結果がＯＫ）場合、携帯電話１０３の読取装置データ送信部２２６は投薬指示書のファイルをセキュアメモリカード１０１に送信する。セキュアメモリカード１０１のカードデータ受信部２０４は、このファイルを受け取り、プライベート格納部２０３に格納する（Ｓ７０８）。この後、パブリック格納部２１０の暗号化された投薬指示書は削除してもよい。

【００５０】

以上のように、本実施の形態では、薬局員１０５が投薬指示書をセキュアメモリカード

１０１に書込む際にセキュアメモリカード１０１のＰＩＮを入力する必要がないので、そのＰＩＮを知っている利用者１０４にＰＩＮの入力処理を依頼する必要がない。また、投薬指示書は薬局のデジタル署名が付加された署名データとなっているので、携帯電話１０３による署名データの検証により投薬指示書の改ざんがないこと、及び、投薬指示書が薬局にて作成されたことを確認することができる。また、投薬指示書を含む署名データは、セキュアメモリカード１０１の所有者である利用者１０４しか復号できないように暗号化されているので、投薬指示書がセキュアメモリカード１０１の所有者以外に盗み見されることはない。そして、再度投薬指示書を閲覧したい場合には、ＰＩＮの入力・照合処理のみが必要で、復号、署名の検証等の暗号処理は不要となる。

【００５１】

実施の形態２.

図８は本実施の形態に係るシステムの構成を示している。本実施の形態では、実施の形態１における携帯電話１０３のデータ取得部２２７、デジタル署名検証部２３１、デジタル署名取得部２３２、システム証明書検証部２３４、共通鍵復号部２３５、証明書取得部２３６、共通鍵取得部２３７、署名データ復号部２３８、署名データ取得部２４０が、セキュアメモリカード１０１に移されている。セキュアメモリカード１０１にデータを書込むＰＣ１０２の構成は、図８では省略しているが、実施の形態１と同一である（図２）。

【００５２】

ＰＣ１０２からセキュアメモリカード１０１に投薬指示書を書込む際の処理の流れ、実施の形態１と同一である（図４及び図５）。

【００５３】

図９は、セキュアメモリカード１０１に書込まれた暗号化された投薬指示書を利用者１０４が所有する携帯電話１０３を用いて閲覧する処理を示すシーケンス図である。また、図１０は同様の処理を示すフロー図である。

【００５４】

薬局でセキュアメモリカード１０１を受け取った利用者１０４は、携帯電話１０３にセキュアメモリカード１０１を装着する。セキュアメモリカード１０１は、パブリック格納部２１０に投薬指示書の親展ファイルがあるか確認する（Ｓ１００１）。

【００５５】

親展ファイルが存在する場合、セキュアメモリカード１０１は、パブリック格納部２１０の親展ファイルを復号化・検証し、プライベート格納部２０３に移動することに対する承諾依頼を携帯電話１０３に送信する。携帯電話１０３は、この承諾依頼を出力部２２９に表示する。利用者１０４が操作部２２８を介して承諾の意思を伝えると、携帯電話１０３からセキュアメモリカード１０１に承諾通知が送信される。承諾通知を得ると、セキュアメモリカード１０１は、親展ファイルをデコードし、共通鍵取得部２３７において、暗号化された共通鍵を取得する。また、署名データ取得部２４０において、その共通鍵で暗号化された投薬指示書の署名データを取得する。そして、共通鍵復号部２３５は、セキュアメモリカード１０１の秘密鍵を用いて、この共通鍵を復号化する。ここで、セキュアメモリカード１０１の秘密鍵は、カード秘密鍵格納部２０８に格納されたものを用いる。署名データ復号部２３８は、復号化された共通鍵を用いて、暗号化された投薬指示書の署名データを復号化する（Ｓ１００２）。

【００５６】

復号化された署名データは、投薬指示書、デジタル署名、薬局証明書に分離され、それぞれデータ取得部２２７、デジタル署名取得部２３２、証明書取得部２３６に渡される。そして、システム証明書検証部２３４は、証明書取得部２３６が取得した薬局証明書の検証を行う。システム証明書検証部２３４は、信用する認証局が発行した証明書や証明書の失効リストを保持し、証明書検証に利用する。セキュアメモリカード１０１が図示していない認証局通信部を有し、この認証局通信部が、薬局証明書の検証処理において、認証局の証明書や証明書の失効リストを通信により外部から入手するという形態も可能である。薬局証明書の正当性が確認された場合、デジタル署名検証部２３１において、投薬指示書

と薬局証明書に含まれる公開鍵とデジタル署名とを用いて、デジタル署名の正当性を検証する（Ｓ１００３）。

【００５７】

デジタル署名の正当性が確認されなかった（検証結果がＮＧ）場合、処理を終了する。デジタル署名の正当性が確認された（検証結果がＯＫ）場合、データ取得部２２７が取得した投薬指示書をプライベート格納部２０３にコピーする（Ｓ１００４）。

【００５８】

投薬指示書のコピーが完了すると、セキュアメモリカード１０１は、投薬指示書の親展ファイルをパブリック格納部２１０から削除する（Ｓ１００５）。

【００５９】

携帯電話１０３は、セキュアメモリカード１０１のプライベート格納部２０３のファイル一覧を要求する（Ｓ１００６）。

【００６０】

すると、セキュアメモリカード１０１は、ＰＩＮの入力を携帯電話１０３に求める。利用者１０４は操作部２２８を用いてＰＩＮを入力する（Ｓ１００７）。このとき、例えば出力部２２９にＰＩＮ入力ウィンドウを表示し、利用者１０４にＰＩＮ入力ウィンドウの所定のフィールドにＰＩＮを入力させてもよい。入力されたＰＩＮは、携帯電話１０３の認証データ送信部２３０から、セキュアメモリカード１０１の認証データ受信部２０７に送信される。

【００６１】

セキュアメモリカード１０１の認証部２０６は、受け取ったＰＩＮと認証データ格納部２０５に格納されているＰＩＮを比較することでＰＩＮを照合し、認証を行う。認証が失敗した（照合結果がＮＧ）場合、処理を終了する。認証が成功した（照合結果がＯＫ）場合、セキュアメモリカード１０１のカードデータ送信部２１２はファイル一覧を携帯電話１０３に送信する。携帯電話１０３の読取装置データ受信部２３９は、このファイル一覧を受け取り、出力部２２９に出力する（Ｓ１００８）。

【００６２】

このファイル一覧には既にパブリック格納部２１０からプライベート格納部２０３に移された投薬指示書のファイルが含まれている。利用者１０４がこのファイルを操作部２２８により選択すると、セキュアメモリカード１０１のカードデータ送信部２１２は投薬指示書のファイルを携帯電話１０３に送信する。携帯電話１０３の読取装置データ受信部２３９は、このファイルを受け取り、出力部２２９に出力し、利用者１０４は投薬指示書を閲覧することが可能となる（Ｓ１００９）。

【００６３】

以上のように、本実施の形態では、セキュアメモリカード１０１が、親展データを復号し、親展データに含まれるデジタル署名や証明書を用いて、同じく親展データに含まれる投薬指示書のデータの正当性を確認することが可能である。したがって、携帯電話１０３に予めこれらの機能を実装する必要がない。

【００６４】

上記実施の形態１及び２では、セキュアメモリカード１０１の所有者である利用者１０４のみが投薬指示書のデータを閲覧できるとしたが、複数の利用者が同一のセキュアメモリカード１０１を使用することも可能である。

【００６５】

また、上記実施の形態１及び２では、薬局のＰＣ１０２が投薬指示書のデータをセキュアメモリカード１０１に書込む例を用いたが、本発明は、他の場所で同様の機能を持つ書込み装置が他の種類のデータをセキュアメモリカード１０１に書込む場合にも適用可能である。

【００６６】

このように、実施の形態１で説明したセキュアメモリカードシステムは、

メモリカードやＩＣカードにデータを書込み、書込まれたデータをカード所有者が閲覧

するメモリカードシステムにおいて、メモリカードが、認証することなくデータを書込めるパブリック格納領域、ＰＩＮによる認証により認証された場合のみ読み書きができるプライベート格納領域、カード所有者の証明書が格納され、書込みは不可だが、読み出しは認証することなく行える証明書格納領域、カード利用者の秘密鍵を格納する秘密鍵格納領域、カード利用者のみが知るＰＩＮを格納するＰＩＮ格納領域、カードに対する外部からの処理要求や外部へのイベント通知や内部処理を、各格納領域の情報にアクセスしながら制御する制御部を持つことを特徴とするセキュアメモリカード、及び、署名データ、親展データを生成するために、秘密鍵格納部、証明書格納部、暗号フォーマット処理部、を備え、入手した証明書の検証を行う証明書検証部を備え、署名データ、親展データの生成、及び証明書の検証に必要な暗号機能を有する暗号部を備えることを特徴としたカードデータ書込み装置、及び、親展データの復号、署名データの検証を行うために、証明書検証部、暗号フォーマット処理部、暗号部を備えることを特徴としたカードデータ閲覧装置、とからなることを特徴とする。

【００６７】

また、実施の形態２で説明したセキュアメモリカードシステムは、

メモリカードやＩＣカードにデータを書込み、書込まれたデータをカード所有者が閲覧するメモリカードシステムにおいて、メモリカードが、認証することなくデータを書込めるパブリック格納領域、ＰＩＮによる認証により認証された場合のみ読み書きができるプライベート格納領域、カード所有者の証明書が格納され、書込みは不可だが、読み出しは認証することなく行える証明書格納領域、カード利用者の秘密鍵を格納する秘密鍵格納領域、カード利用者のみが知るＰＩＮを格納するＰＩＮ格納領域、親展データの復号や署名データの検証に用いる、証明書格納部、暗号フォーマット処理部、暗号部、カードに対する外部からの処理要求や外部へのイベント通知、内部処理を、各格納領域の情報にアクセスしながら制御する制御部を持つことを特徴とするセキュアメモリカード、及び、署名データ、親展データを生成するために、秘密鍵格納部、証明書格納部、暗号フォーマット処理部を備え、入手した証明書の検証を行う証明書検証部を備え、署名データ、親展データを生成、証明書検証に必要な暗号機能を有する暗号部を備えることを特徴としたカードデータ書込み装置、及び、セキュアメモリカードからデータを読み出し、表示するためのカードデータ閲覧装置、とから構成されることを特徴とする。

【００６８】

前述した各実施の形態で、セキュアメモリカード１０１、ＰＣ１０２、携帯電話１０３は、コンピュータで実現できるものである。

図示していないが、セキュアメモリカード１０１、ＰＣ１０２、携帯電話１０３は、プログラムを実行するＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）を備えている。

【００６９】

例えば、ＣＰＵは、バスを介して、ＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）、ＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）、通信ボード、表示装置、Ｋ／Ｂ（キーボード）、マウス、ＦＤＤ（Ｆｌｅｘｉｂｌｅ　Ｄｉｓｋ　Ｄｒｉｖｅ）、ＣＤＤ（コンパクトディスクドライブ）、磁気ディスク装置、光ディスク装置、プリンタ装置、スキャナ装置等と接続されている。

ＲＡＭは、揮発性メモリの一例である。ＲＯＭ、ＦＤＤ、ＣＤＤ、磁気ディスク装置、光ディスク装置は、不揮発性メモリの一例である。これらは、記憶装置、記憶部あるいは格納部の一例である。

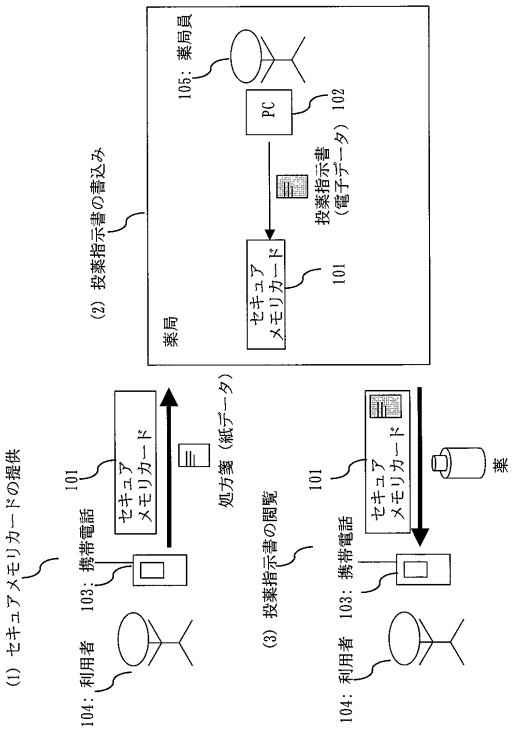
前述した各実施の形態のセキュアメモリカード１０１、ＰＣ１０２、携帯電話１０３が扱うデータや情報は、記憶装置、記憶部あるいは格納部に保存され、セキュアメモリカード１０１、ＰＣ１０２、携帯電話１０３の各部により、記録され読み出されるものである。

【００７０】

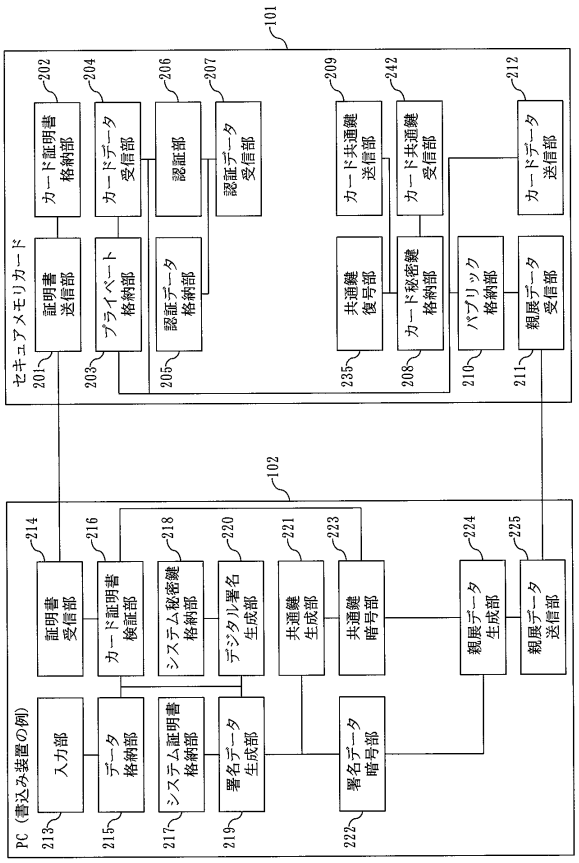
また、通信ボードは、例えば、ＬＡＮ、インターネット、あるいはＩＳＤＮ等のＷＡＮ

（ワイドエリアネットワーク）に接続されている。
【００７１】
磁気ディスク装置には、オペレーティングシステム（ＯＳ）、ウィンドウシステム、プログラム群、ファイル群（データベース）が記憶されている。
プログラム群は、ＣＰＵ、ＯＳ、ウィンドウシステムにより実行される。
【００７２】
上記セキュアメモリカード１０１、ＰＣ１０２、携帯電話１０３の各部は、一部あるいはすべてコンピュータで動作可能なプログラムにより構成しても構わない。あるいは、ＲＯＭに記憶されたファームウェアで実現されていても構わない。あるいは、ソフトウェアあるいは、ハードウェアあるいは、ソフトウェアとハードウェアとファームウェアとの組み合わせで実施されても構わない。
【００７３】
上記プログラム群には、実施の形態の説明において「～部」として説明した処理をＣＰＵに実行させるプログラムが記憶される。これらのプログラムは、例えば、Ｃ言語やＨＴＭＬやＳＧＭＬやＸＭＬ等のコンピュータ言語により作成される。
【００７４】
また、上記プログラムは、磁気ディスク装置、ＦＤ（Ｆｌｅｘｉｂｌｅ　Ｄｉｓｋ）、光ディスク、ＣＤ（コンパクトディスク）、ＭＤ（ミニディスク）、ＤＶＤ（Ｄｉｇｉｔａｌ　Ｖｅｒｓａｔｉｌｅ　Ｄｉｓｋ）等のその他の記録媒体に記憶され、ＣＰＵにより読み出され実行される。
【図面の簡単な説明】
【００７５】
【図１】実施の形態１及び２に係るデータ交換システムの利用者間のやりとりを示す概念図。
【図２】実施の形態１に係る書込み装置とメモリカードの構成を示すブロック図。
【図３】実施の形態１に係るメモリカードと読取装置の構成を示すブロック図。
【図４】実施の形態１に係る書込み装置とメモリカードが行う処理を示すシーケンス図。
【図５】実施の形態１に係る書込み装置とメモリカードが行う処理を示すフロー図。
【図６】実施の形態１に係るメモリカードと読取装置が行う処理を示すシーケンス図。
【図７】実施の形態１に係るメモリカードと読取装置が行う処理を示すフロー図。
【図８】実施の形態１に係るメモリカードと読取装置の構成を示すブロック図。
【図９】実施の形態１に係るメモリカードと読取装置が行う処理を示すシーケンス図。
【図１０】実施の形態１に係るメモリカードと読取装置が行う処理を示すフロー図。
【符号の説明】
【００７６】
１０１　セキュアメモリカード、１０２　ＰＣ、１０３　携帯電話、１０４　利用者、１０５　薬局員、２０１　証明書送信部、２０２　カード証明書格納部、２０３　プライベート格納部、２０４　カードデータ受信部、２０５　認証データ格納部、２０６　認証部、２０７　認証データ受信部、２０８　カード秘密鍵格納部、２０９　カード共通鍵送信部、２１０　パブリック格納部、２１１　親展データ受信部、２１２　カードデータ送信部、２１３　入力部、２１４　証明書受信部、２１５　データ格納部、２１６　カード証明書検証部、２１７　システム証明書格納部、２１８　システム秘密鍵格納部、２１９　署名データ生成部、２２０　デジタル署名生成部、２２１　共通鍵生成部、２２２　署名データ暗号部、２２３　共通鍵暗号部、２２４　親展データ生成部、２２５　親展データ送信部、２２６　読取装置データ送信部、２２７　データ取得部、２２８　操作部、２２９　出力部、２３０　認証データ送信部、２３１　デジタル署名検証部、２３２　デジタル署名取得部、２３３　読取装置共通鍵受信部、２３４　システム証明書検証部、２３５　共通鍵復号部、２３６　証明書取得部、２３７　共通鍵取得部、２３８　署名データ復号部、２３９　読取装置データ受信部、２４０　署名データ取得部、２４１　読取装置共通鍵送信部、２４２　カード共通鍵受信部。

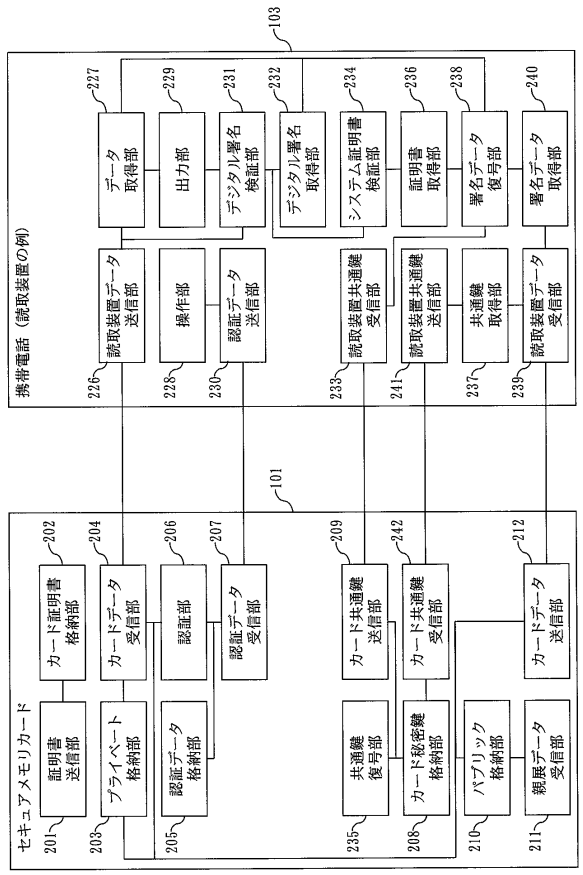
【図１】


(1) セキュアメモリカードの提供
104: 利用者
103: 携帯電話
101
セキュア メモリカード
処方箋（紙データ）
(2) 投薬指示書の書込み
薬局
105: 薬局員
PC
102
投薬指示書（電子データ）
セキュア メモリカード
101
(3) 投薬指示書の閲覧
104: 利用者
103: 携帯電話
101
セキュア メモリカード
薬

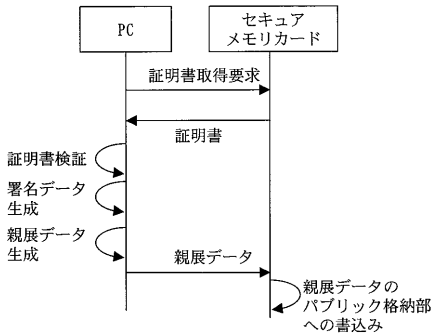
【図２】


101
セキュアメモリカード
201 証明書 送信部
202 カード証明書 格納部
203 プライベート 格納部
204 カードデータ 受信部
205 認証データ 格納部
206 認証部
207 認証データ 受信部
208 カード秘密鍵 格納部
209 カード共通鍵 送信部
210 パブリック 格納部
211 親展データ 受信部
212 カードデータ 送信部
235 共通鍵 復号部
242 カード共通鍵 受信部
102
PC（書込み装置の例）
213 入力部
214 証明書 受信部
215 データ 格納部
216 カード証明書 検証部
217 システム証明書 格納部
218 システム秘密鍵 格納部
219 署名データ 生成部
220 デジタル署名 生成部
221 共通鍵 生成部
222 署名データ 暗号部
223 共通鍵 暗号部
224 親展データ 生成部
225 親展データ 送信部

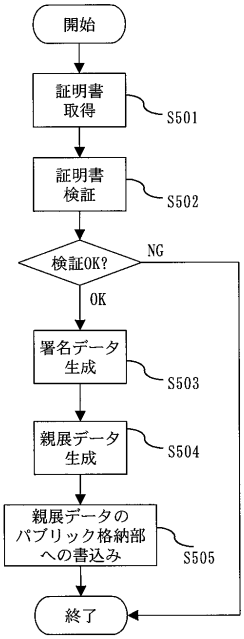
【図３】


103
携帯電話（読取装置の例）
226 読取装置データ 送信部
227 データ 取得部
228 操作部
229 出力部
230 認証データ 送信部
231 デジタル署名 検証部
232 デジタル署名 取得部
233 読取装置共通鍵 受信部
234 システム証明書 検証部
236 証明書 取得部
237 共通鍵 取得部
238 署名データ 復号部
239 読取装置データ 受信部
240 署名データ 取得部
101
セキュアメモリカード
201 証明書 送信部
202 カード証明書 格納部
203 プライベート 格納部
204 カードデータ 受信部
205 認証データ 格納部
206 認証部
207 認証データ 受信部
208 カード秘密鍵 格納部
209 カード共通鍵 送信部
210 パブリック 格納部
211 親展データ 受信部
212 カードデータ 送信部
235 共通鍵 復号部
241 読取装置共通鍵 送信部
242 カード共通鍵 受信部

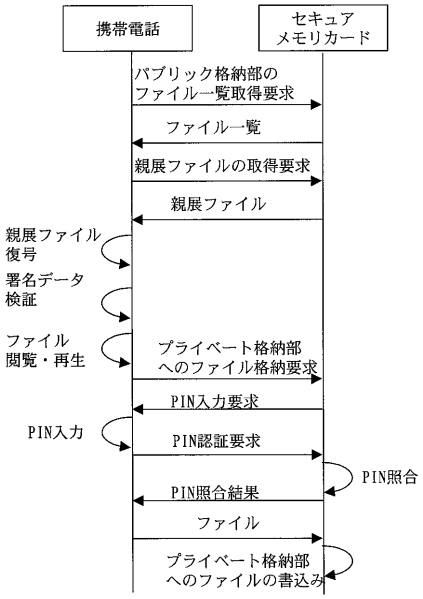
【図４】


PC
セキュア メモリカード
証明書取得要求
証明書
証明書検証
署名データ 生成
親展データ 生成
親展データ
親展データの パブリック格納部 への書込み

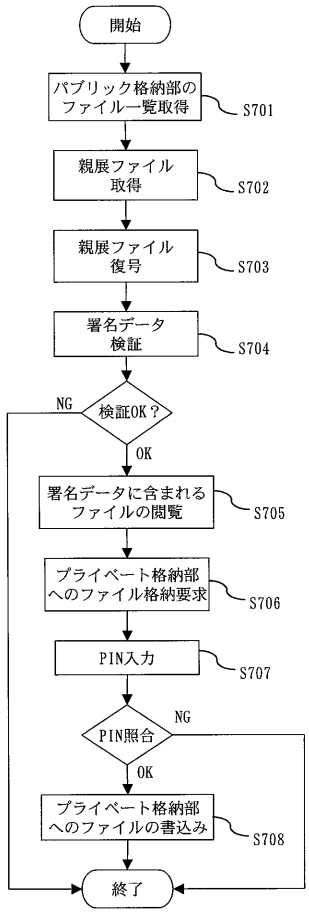
【図５】


開始
証明書取得
S501
証明書検証
S502
検証OK?
NG
OK
署名データ生成
S503
親展データ生成
S504
親展データのパブリック格納部への書込み
S505
終了

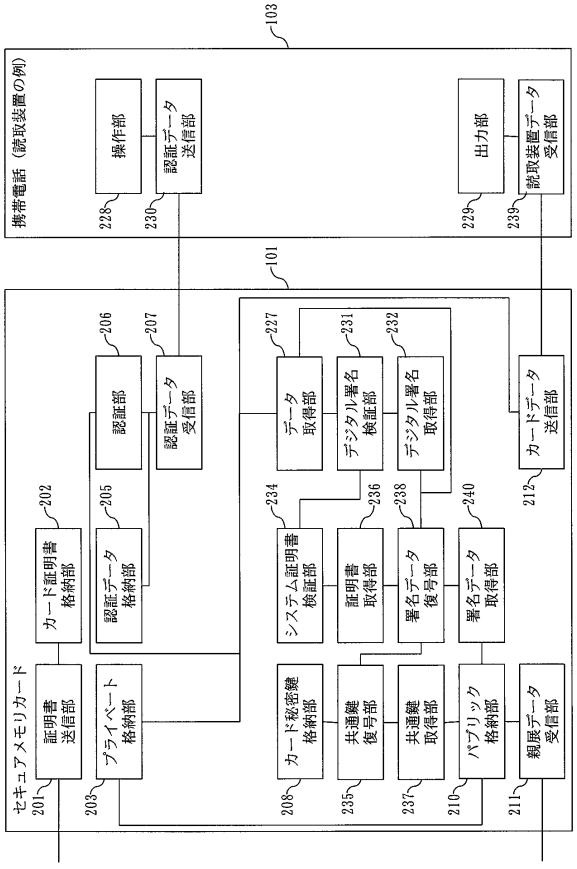
【図６】


携帯電話
セキュアメモリカード
パブリック格納部のファイル一覧取得要求
ファイル一覧
親展ファイルの取得要求
親展ファイル
親展ファイル復号
署名データ検証
ファイル閲覧・再生
プライベート格納部へのファイル格納要求
PIN入力要求
PIN入力
PIN認証要求
PIN照合
PIN照合結果
ファイル
プライベート格納部へのファイルの書込み

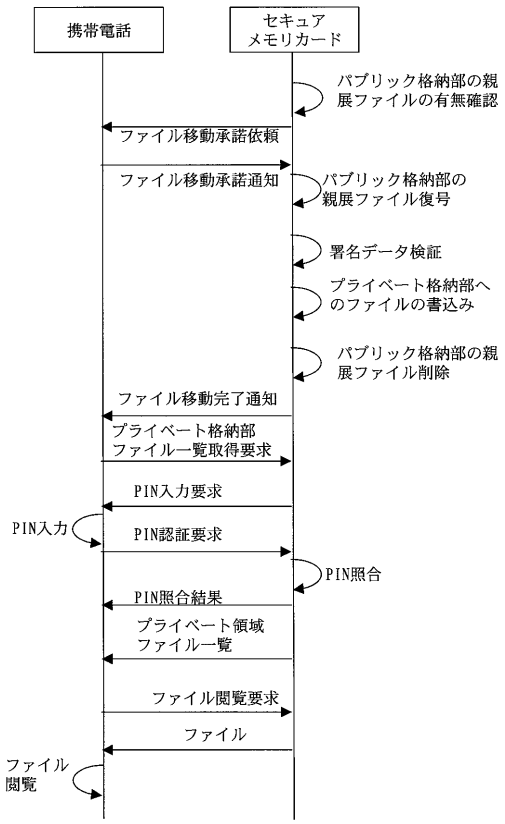
【図７】


開始
パブリック格納部のファイル一覧取得
S701
親展ファイル取得
S702
親展ファイル復号
S703
署名データ検証
S704
NG
検証OK？
OK
署名データに含まれるファイルの閲覧
S705
プライベート格納部へのファイル格納要求
S706
PIN入力
S707
PIN照合
NG
OK
プライベート格納部へのファイルの書込み
S708
終了

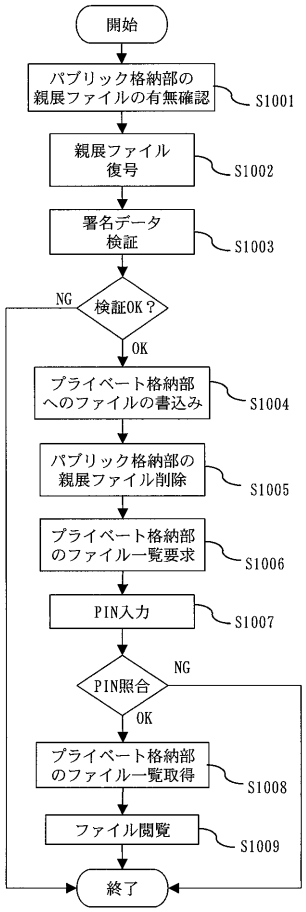
【図８】


103
携帯電話（読取装置の例）
操作部
228
認証データ送信部
230
出力部
229
読取装置データ受信部
239
101
セキュアメモリカード
カード証明書格納部
202
証明書送信部
201
認証部
206
認証データ格納部
205
認証データ受信部
207
プライベート格納部
203
データ取得部
227
デジタル署名検証部
231
デジタル署名取得部
232
カードデータ送信部
212
システム証明書検証部
234
証明書取得部
236
署名データ復号部
238
署名データ取得部
240
カード秘密鍵格納部
208
共通鍵復号部
235
共通鍵取得部
237
パブリック格納部
210
親展データ受信部
211

【図９】


携帯電話
セキュア
メモリカード
パブリック格納部の親
展ファイルの有無確認
ファイル移動承諾依頼
ファイル移動承諾通知
パブリック格納部の
親展ファイル復号
署名データ検証
プライベート格納部へ
のファイルの書込み
パブリック格納部の親
展ファイル削除
ファイル移動完了通知
プライベート格納部
ファイル一覧取得要求
PIN入力要求
PIN入力
PIN認証要求
PIN照合
PIN照合結果
プライベート領域
ファイル一覧
ファイル閲覧要求
ファイル
ファイル
閲覧

【図１０】


開始
パブリック格納部の
親展ファイルの有無確認
S1001
親展ファイル
復号
S1002
署名データ
検証
S1003
NG
検証OK？
OK
プライベート格納部
へのファイルの書込み
S1004
パブリック格納部の
親展ファイル削除
S1005
プライベート格納部
のファイル一覧要求
S1006
PIN入力
S1007
NG
PIN照合
OK
プライベート格納部
のファイル一覧取得
S1008
ファイル閲覧
S1009
終了

フロントページの続き

(56)参考文献 特開２００３－１０８９５２（ＪＰ，Ａ）
特開２００４－０２１７５５（ＪＰ，Ａ）
特開平０９－２８２３９３（ＪＰ，Ａ）
特開２００４－０３８２７０（ＪＰ，Ａ）
特開平１１－２０３４３９（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06K 19/10
G06F 21/24
G06K 17/00
G09C 1/00