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

特許第4011889号
(P4011889)

(45)発行日　平成19年11月21日(2007.11.21)　(24)登録日　平成19年9月14日(2007.9.14)

(51)Int.Cl.		F I		
G06K 17/00	(2006.01)	G06K	17/00	V
G06K 19/10	(2006.01)	G06K	17/00	T
		G06K	17/00	B
		G06K	19/00	S
		G06K	19/00	R

請求項の数 1　(全 8 頁)

(21)出願番号　特願2001-342654 (P2001-342654)
(22)出願日　平成13年11月8日 (2001.11.8)
(65)公開番号　特開2003-141458 (P2003-141458A)
(43)公開日　平成15年5月16日 (2003.5.16)
審査請求日　平成16年11月5日 (2004.11.5)

(73)特許権者　000002897
大日本印刷株式会社
東京都新宿区市谷加賀町一丁目１番１号
(74)代理人　100111659
弁理士　金山　聡
(72)発明者　斎藤　賢一郎
東京都新宿区市谷加賀町一丁目１番１号
大日本印刷株式会社内

審査官　村田　充裕

最終頁に続く

(54)【発明の名称】ＩＣカード処理方法

(57)【特許請求の範囲】

【請求項１】

情報端末装置用のプログラムが格納されたメモリを有するＩＣカードと、前記ＩＣカードのメモリから読み取られた前記情報端末装置用のプログラムに基づいて処理を実行する情報端末装置とからなるＩＣカード処理方法であって、

前記ＩＣカードを利用して情報端末装置による処理を行なう際に、前記ＩＣカードのメモリに記憶されている認証用プログラムに対応して相互認証を行なうＩＣカードアクセス用プログラムである情報端末装置用のプログラムを、ＩＣカードリーダライタを介して前記情報端末装置の記憶手段にダウンロードするステップと、

前記ＩＣカードのメモリに記憶されている本人認証用情報である暗証番号のデータに対して、不可逆な一方向関数を含む特殊な関数であるハッシュ関数を利用して、特定の値であるハッシュ値を算出した後、このハッシュ値を秘密鍵により暗号化し、この暗号化されたデータを暗号化されていない暗証番号のデータと共にＩＣカードリーダライタを介して前記情報端末装置に送信するステップと、

前記情報端末装置において、前記ダウンロードされた情報端末装置用のプログラムに基づく処理として、前記受信した暗号化されたデータに対して、前記秘密鍵と対で使用され、前記秘密鍵で暗号化されたデータを復号化することができる公開鍵を用いることで復号してハッシュ値を得た後、前記受信した暗号化されていない暗証番号を上記と同じハッシュ関数で処理することでハッシュ値を計算し、このハッシュ値と前記した公開鍵を用いて復号してハッシュ値とを比較する処理を行うステップと、

前記比較照合の結果、一致した場合にＩＣカード利用者が正当な利用者であることが認証され、ＩＣカード利用者が正当な利用者であることが認証されると、その結果である認証情報が情報端末装置からＩＣカードリーダライタのデータ書込手段を介してＩＣカードに送信され、ＩＣカードの認証用プログラムから通常の処理を行なうための制御用プログラムに切り替わり制御用プログラムによる処理が開始されるステップと、

を有することを特徴とするＩＣカード処理方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ＩＣカードと、前記ＩＣカードのメモリから読み取られた情報に基づいて処理を実行する情報端末装置とからなるＩＣカード処理方法に関する。

【０００２】

【従来の技術】

従来、ＩＣカードを利用して種々の情報処理を行なう際には、予め情報端末装置に常時搭載されているプログラムを起動して、パーソナルコンピュータ等の情報端末装置に備えられたＩＣカードリーダライタを介し、ＩＣカードにアクセスし、ＩＣカードのメモリに格納されている種々のデータを読み取りなどしてデータ処理を行なったり、またこれらのデータをインターネット等のネットワークを介してサーバに送信するなどしてデータ処理を行なっている。

【０００３】

しかしながら、情報端末装置に常時プログラムを搭載しておくことは、不正に第三者によって搭載されているプログラムの解析が行われやすく、例えばＩＣカードに対するコマンド順序などのアクセス方法等の重要なプログラムが解析され、不正行為が行われる危険性があるなどの問題がある。

更に、不正に解析されたプログラムに基づいて、偽造ＩＣカードを製造し、種々の不正なアクセスが行われる危険性がある。

【０００４】

【発明が解決しようとする課題】

本発明のＩＣカード処理方法は、ＩＣカードを使用して情報端末装置による処理を行なう場合において、これらの処理に必要なプログラムが第三者によってプログラム解析がされたり、不正利用されることを未然に防止することができ、更に、ＩＣカード利用者が正当な権利を有する者であるか否かの認証も行なうことができるようにすることで、ＩＣカード利用に対する安全性を確保することができるＩＣカード処理方法を提供する。

【０００５】

【課題を解決するための手段】

本発明のＩＣカード処理方法は、情報端末装置用のプログラムが格納されたメモリを有するＩＣカードと、前記ＩＣカードのメモリから読み取られた前記情報端末装置用のプログラムに基づいて処理を実行する情報端末装置とからなるＩＣカード処理方法であって、前記ＩＣカードを利用して情報端末装置による処理を行なう際に、前記ＩＣカードのメモリに記憶されている認証用プログラムに対応して相互認証を行なうＩＣカードアクセス用プログラムである情報端末装置用のプログラムを、ＩＣカードリーダライタを介して前記情報端末装置の記憶手段にダウンロードするステップと、前記ＩＣカードのメモリに記憶されている本人認証用情報である暗証番号のデータに対して、不可逆な一方向関数を含む特殊な関数であるハッシュ関数を利用して、特定の値であるハッシュ値を算出した後、このハッシュ値を秘密鍵により暗号化し、この暗号化されたデータを暗号化されていない暗証番号のデータと共にＩＣカードリーダライタを介して前記情報端末装置に送信するステップと、前記情報端末装置において、前記ダウンロードされた情報端末装置用のプログラムに基づく処理として、前記受信した暗号化されたデータに対して、前記秘密鍵と対で使用され、前記秘密鍵で暗号化されたデータを復号化することができる公開鍵を用いることで復号してハッシュ値を得た後、前記受信した暗号化されていない暗証番号を上記と同じ

ハッシュ関数で処理することでハッシュ値を計算し、このハッシュ値と前記した公開鍵を用いて復号してハッシュ値とを比較する処理を行うステップと、前記比較照合の結果、一致した場合にＩＣカード利用者が正当な利用者であることが認証され、ＩＣカード利用者が正当な利用者であることが認証されると、その結果である認証情報が情報端末装置からＩＣカードリーダライタのデータ書込手段を介してＩＣカードに送信され、ＩＣカードの認証用プログラムから通常の処理を行なうための制御用プログラムに切り替わり制御用プログラムによる処理が開始されるステップと、を有することを特徴とする。

【０００７】

【発明の実施の形態】

以下、本発明の実施の形態を図面に基づいて詳細に説明する。

図１は、本発明のＩＣカード処理方法が適応されるＩＣカードシステムのシステム構成図、図２は、本発明のＩＣカード処理方法が適応されるＩＣカードのシステムブロック図、図３は、本発明のＩＣカード処理方法が適応されるＩＣカードリーダライタと情報端末装置のシステムブロック図、図４は、本発明のＩＣカード処理方法の処理手順を説明するフローチャートである。

【０００８】

図１に示すように、本発明のＩＣカード処理方法が適応されるＩＣカードシステムは、ＩＣカードリーダライタ１が備えられた情報端末装置２が、インターネット等のネットワーク３を介してサーバ４に通信可能に接続されている。

ＩＣカード利用者は、ＩＣカードリーダライタ１のＩＣカード挿入口にＩＣカード５を挿入することで電気的に接続され、情報端末装置２とＩＣカード５との間におけるアクセスが可能となる。

【０００９】

ＩＣカード５は、図２のＩＣカードのシステムブロック図に示すように、制御部であるＣＰＵ６、読み出し専用メモリであるＲＯＭ７と、書き換え可能な不揮発性メモリであるＥＥＰＲＯＭ８と、揮発性メモリであるＲＡＭ９とを有する。また、更にＩＣカード５には、電源電圧を供給するＶＣＣ端子１０、接地用のＧＮＤ端子１１、リセット信号を供給するＲＳＴ端子１２、クロック信号を供給するＣＬＫ端子１３、データ入出力用のＩ／Ｏ端子１４が備えられている。

そして、上記のＣＰＵ６と各メモリと各端子は、ＩＣモジュールとしてカード基材に埋設された構成を有する。

【００１０】

ＲＯＭ７には、ＩＣカード５がＩＣカードリーダライタ１と電気的に接続された後の処理手順が書き込まれた制御用プログラムと、認証用プログラムとが予め記憶されていて、ＣＰＵ６は、これらのプログラムに従った処理を実行する。

【００１１】

また、ＥＥＰＲＯＭ８には、ＩＣカードリーダライタ１を介して情報端末装置２の記憶手段にダウンロードして、情報端末装置２において実行される具体的な処理手順を示した情報端末装置用のプログラムや、ＩＣカードを使用する権利を有する正当な本人であることを認証するための認証用情報である暗証番号などが記憶されている。

したがって、情報端末装置２では、たとえＩＣカードリーダライタ１にＩＣカード５が挿入され電気的に接続されたとしても、情報端末装置用のプログラムがダウンロードされる前の段階では、ＩＣカード５によりその後の処理は実行することができない状態のまま中断されるように制御される。

【００１２】

そして、ＲＯＭ７に記憶されている制御用プログラムには、ＩＣカード５がＩＣカードリーダライタ１と電気的に接続された場合、まずＩＣカード５のＥＥＰＲＯＭ８に記憶されている情報端末装置用のプログラムをＩＣカードリーダライタ１を介して、情報端末装置２の記憶手段にダウンロードするステップが定められている。

そして、情報端末装置２では、まずＩＣカードリーダライタ１を介してダウンロードされ

た情報端末装置用のプログラムに基づいた処理が実行されるように制御されている。
【００１３】
ＩＣカードのＲＯＭ７に記憶されている認証用プログラムは、ＩＣカード利用者が正当な権利を有する者であるか否かを検証するための処理を実行する。
また、ＩＣカードリーダライタ１を介して情報端末装置２にダウンロードされる情報端末装置用のプログラムは、ＩＣカードリーダライタ１にＩＣカード５を挿入後、本来のデータ処理を行なう前の段階で、ＩＣカード使用者がＩＣカード５によるアクセスを行なう正当な権利を有する者である否かのチェックを行なうため、ＩＣカード５のＲＯＭ７に記憶されている認証用プログラムと相互認証を行なうことが可能なＩＣカードアクセス用プログラムとしての処理内容を有している。
【００１４】
次に、本発明のＩＣカード処理方法の処理手順を、図３のブロック図及び図４のフローチャートに基づいて説明する。
まず、ＩＣカード５をＩＣカードリーダライタ１に挿入しセットする（Ｓ１）。
ＩＣカードリーダライタ１のデータ読取手段１５により、ＲＯＭ７に記憶されている情報端末装置用のプログラムであるＩＣカードアクセス用プログラムが読み取られる（Ｓ２）。
【００１５】
次に、ＩＣカードリーダライタ１から情報端末装置２の記憶手段２０に、ＩＣカードアクセス用プログラムがダウンロードされる（Ｓ３）。
その後、情報端末装置２の制御手段２１は、このＩＣカードアクセス用プログラムに基づいた処理を実行する（Ｓ４）。
【００１６】
次に、ＩＣカード５のＲＯＭ７に記憶されている認証用プログラムにより、ＩＣカード利用者が正当な権利を有する者であるか否かを検証するための処理が実行される。
具体的には、ＩＣカード５のＥＥＰＲＯＭ８に記憶されている本人認証用情報である暗証番号が、公開鍵暗号方式による秘密鍵により暗号化され、暗証番号に電子署名を付す処理を行なう（Ｓ５）。
【００１７】
公開鍵暗号方式による秘密鍵により暗号化による処理は、暗証番号のデータに対して、不可逆な一方向関数を含む特殊な関数であるハッシュ関数を利用して、特定の値であるハッシュ値を算出した後、このハッシュ値を秘密鍵により暗号化し、この暗号化の結果得られるデータが電子署名と呼ばれ、この暗号化されたデータを暗号化されていない暗証番号のデータと共にＩＣカードリーダライタ１を介して情報端末装置２に送信するものである（Ｓ６）。
【００１８】
これらのデータを受信した情報端末装置２では、ＩＣカードアクセス用プログラムに基づく検証及び認証処理が実行される。
具体的には、情報端末装置２で受信した暗号化されたデータに対して、前記秘密鍵と対で使用され、前記秘密鍵で暗号化されたデータを復号化することができる公開鍵を用いることで復号してハッシュ値を得る。
【００１９】
更に、受信した暗号化されていない暗証番号を上記と同じハッシュ関数で処理することでハッシュ値を計算する。
このハッシュ値と前記した公開鍵を用いて復号してハッシュ値とを比較し、それぞれのデータが一致すれば送信されたデータが送信途中で改ざんされることなく受信されたことが検証でき、この検証で確認された場合にだけ次のステップに進むことができる（Ｓ７）。
尚、この検証処理で比較データが不一致の場合には、データが改ざんされたことになり、処理を終了する。
【００２０】

次に、ＩＣカード利用者は、正当な利用者であることを証明するために、情報端末装置２の入力手段１８から本人認証用情報である暗証番号を入力する（Ｓ８）。
この入力手段１８から入力された暗証番号は、情報端末装置２の制御手段２１においてＩＣカード５から受信し、検証で確認された暗証番号と比較照合が行われる（Ｓ９）。

【００２１】

この比較照合の結果（Ｓ１０）、一致した場合にＩＣカード利用者が正当な利用者であることが認証され、ＩＣカード利用者が正当な利用者であることが認証されると、その結果である認証情報が情報端末装置２からＩＣカードリーダライタ１のデータ書込手段１６を介してＩＣカード５に送信され、ＩＣカード５の認証用プログラムから通常の処理を行なうための制御用プログラムに切り替わり制御用プログラムによる処理が開始される（Ｓ１１）。

【００２２】

尚、比較照合の結果、不一致の場合には、処理が終了する。
情報端末装置２の表示手段１７には、これらの認証結果が表示され、確認することができるようにしてある。

【００２３】

そして、ＩＣカードリーダライタ１を介してＩＣカード５から読取られた情報により、情報端末装置２が、通信手段１９によりインターネット等のネットワーク３を介してサーバ４と通信を行ない種々のデータ処理を実行できる状態となる。

【００２４】

【発明の効果】

以上説明したように、本発明のＩＣカード処理方法は、ＩＣカードを使用した処理を行なう場合に、情報端末装置で必要なプログラムをＩＣカードに記憶させてＩＣカードの処理を行なう際に、そのプログラムをＩＣカードから情報端末装置にダウンロードさせた後に実行させるので、第三者にプログラムの解析がされ、不正利用されることを未然に防止することができるという効果がある。
更に、ＩＣカードから情報端末装置にダウンロードし実行する認証用プログラムを、ＩＣカードのメモリに記憶されている認証用プログラムと対応して相互認証を行なうＩＣカードアクセス用プログラムとしたことで、ＩＣカード利用者が正当な権利を有する者であるか否かの認証も行なうことができ、ＩＣカード利用に対する安全性を確保刷ることができるという効果がある。

【図面の簡単な説明】

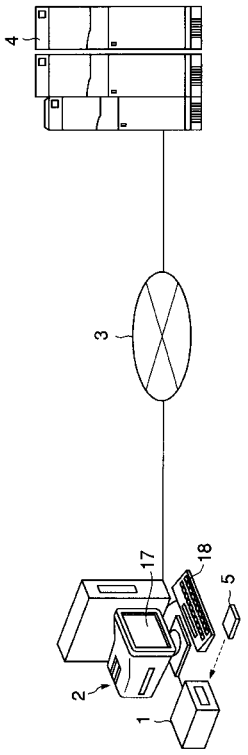
【図１】本発明のＩＣカード処理方法が適応されるＩＣカードシステムのシステム構成図である。
【図２】本発明のＩＣカード処理方法が適応されるＩＣカードのシステムブロック図である。
【図３】本発明のＩＣカード処理方法が適応されるＩＣカードリーダライタと情報端末装置のシステムブロック図である。
【図４】本発明のＩＣカード処理方法の処理手順を説明するフローチャートである。

【符号の説明】

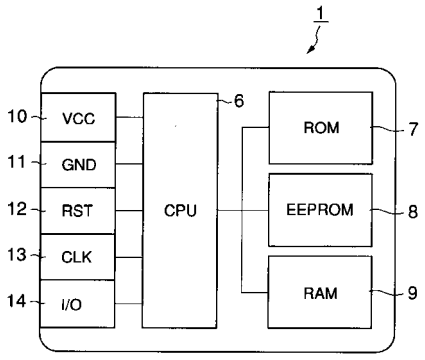
１　ＩＣカードリーダライタ
２　情報端末装置
３　ネットワーク
４　サーバ
５　ＩＣカード
６　ＣＰＵ
７　ＲＯＭ
８　ＥＥＰＲＯＭ
９　ＲＡＭ
１０　ＶＣＣ端子

１１　ＧＮＤ端子
１２　ＲＳＴ端子
１３　ＣＬＫ端子
１４　Ｉ／Ｏ端子
１５　データ読取手段
１６　データ書込手段
１７　表示手段
１８　入力手段
１９　通信手段
２０　記憶手段
２１　制御手段

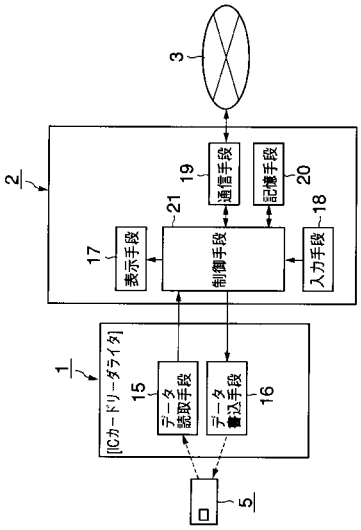
【図１】



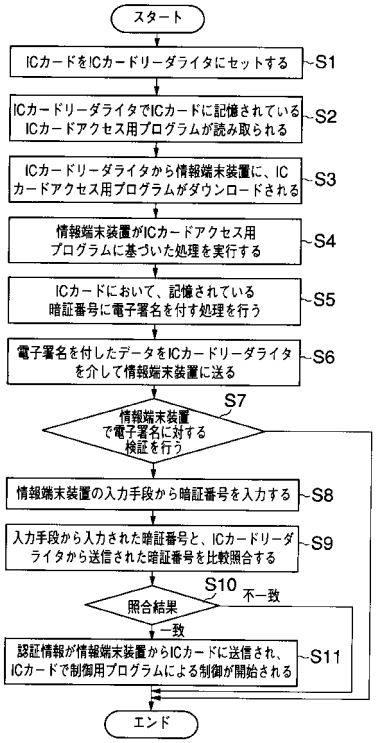
【図２】



【図３】


3
2
19
通信手段
20
記憶手段
21
18
17
表示手段
制御手段
入力手段
1
[ICカードリーダライタ]
15
データ読取手段
16
データ書込手段
5
口

【図４】


スタート
ICカードをICカードリーダライタにセットする
S1
ICカードリーダライタでICカードに記憶されている
ICカードアクセス用プログラムが読み取られる
S2
ICカードリーダライタから情報端末装置に、IC
カードアクセス用プログラムがダウンロードされる
S3
情報端末装置がICカードアクセス用
プログラムに基づいた処理を実行する
S4
ICカードにおいて、記憶されている
暗証番号に電子署名を付す処理を行う
S5
電子署名を付したデータをICカードリーダライタ
を介して情報端末装置に送る
S6
S7
情報端末装置
で電子署名に対する
検証を行う
情報端末装置の入力手段から暗証番号を入力する
S8
入力手段から入力された暗証番号と、ICカードリーダ
ライタから送信された暗証番号を比較照合する
S9
S10
照合結果
不一致
一致
認証情報が情報端末装置からICカードに送信され、
ICカードで制御用プログラムによる制御が開始される
S11
エンド

フロントページの続き

(56)参考文献 特開平０８－２９７６３４（ＪＰ，Ａ）
特開２００１－２０２３３２（ＪＰ，Ａ）
特開２０００－３０６３３０（ＪＰ，Ａ）
特開平１１－０４１２３０（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06K 17/00
G06K 19/00-19/08
B42D 15/10
G06F 15/00