(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2009-238155
(P2009-238155A)
(43)公開日　平成21年10月15日(2009.10.15)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/22	(2006.01)	G06F	9/06	660G	5B017
G06F 21/24	(2006.01)	G06F	9/06	660F	5B176
G06F 21/20	(2006.01)	G06F	12/14	530C	5B276
G06F 9/445	(2006.01)	G06F	15/00	330C	5B285
H04L 9/10	(2006.01)	G06F	9/06	610J	5J104

審査請求 未請求　請求項の数 4　ＯＬ　（全 12 頁）　最終頁に続く

(21)出願番号　特願2008-86644(P2008-86644)
(22)出願日　平成20年3月28日(2008.3.28)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(74)代理人　100081341
弁理士　小林　茂
(74)代理人　100112863
弁理士　阪間　和之
(72)発明者　浦田　昌和
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　細田　泰弘
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

最終頁に続く

(54)【発明の名称】データ記憶システムおよびデータ記憶方法

(57)【要約】
【課題】利用者端末のセキュリティを向上させる。
【解決手段】ＩＣカード１０２は、アプリケーション配信サーバ１１７と相互認証を行うための秘密鍵１０９と、秘密鍵１０９を使用してアプリケーション配信サーバ１１７と相互認証したのちに、アプリケーション配信サーバ１１７から端末ＯＳ１１１と端末アプリケーション１１２とを取得するカードマネージャ１１４とを有し、利用者端末１０１は、ＩＣカード１０２と相互認証を行うための鍵１１６を有する耐タンパ性の耐タンパモジュール１１５と、鍵１１６を使用してＩＣカード１０２と相互認証したのちに、ＩＣカード１０２から端末ＯＳ１１１と端末アプリケーション１１２とを取得し、端末ＯＳ１１１と端末アプリケーション１１２とを実行するＣＰＵ１０５とを有する。
【選択図】　図１

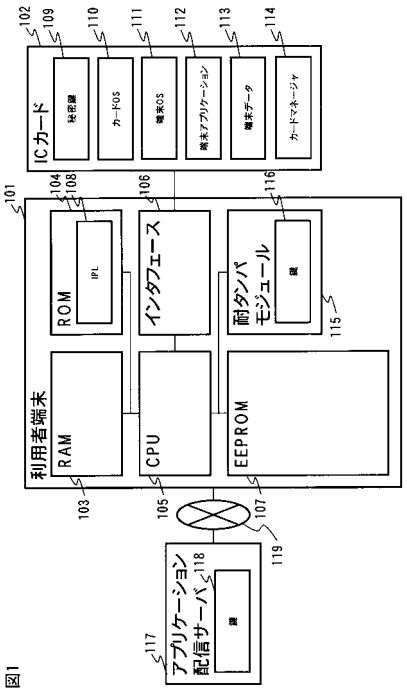

図1

【特許請求の範囲】
【請求項１】
耐タンパ性を有するＩＣカードに格納された情報を読み取り可能な利用者端末にデータを記憶するデータ記憶システムにおいて、
上記ＩＣカードは、
上記利用者端末のＯＳとアプリケーションとを有し、
上記利用者端末は、
上記ＩＣカードと相互認証を行うための第１の鍵を有する耐タンパ性の耐タンパモジュール部と、
上記第１の鍵を使用して上記ＩＣカードと相互認証したのちに、上記ＩＣカードから上記ＯＳと上記アプリケーションとを取得し、上記ＯＳと上記アプリケーションとを実行する実行部とを備えた
ことを特徴とするデータ記憶システム。
【請求項２】
上記利用者端末は、上記ＯＳと上記アプリケーションとを上記耐タンパモジュール部に格納することを特徴とする請求項１に記載のデータ記憶システム。
【請求項３】
上記ＩＣカードは、
ＳＩＭカードである
ことを特徴とする１または２に記載のデータ記憶システム。
【請求項４】
耐タンパ性を有するＩＣカードに格納された情報を読み取り可能な利用者端末にデータを記憶するデータ記憶方法において、
上記ＩＣカードが上記利用者端末のＯＳとアプリケーションとを記憶するステップと、
上記利用者端末が、耐タンパ性の耐タンパモジュール部に格納された第１の鍵を使用して上記ＩＣカードと相互認証を行うステップと、
上記第１の鍵を使用して上記ＩＣカードと相互認証したのちに、上記利用者端末が、上記ＩＣカードから上記ＯＳと上記アプリケーションとを取得し、上記ＯＳと上記アプリケーションとを実行するステップとを有する
ことを特徴とするデータ記憶方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、耐タンパ性を有するＩＣカードに格納された情報を読み取り可能な利用者端末にデータを記憶するデータ記憶システムおよび上記データ記憶システムのデータ記憶方法に関するものである。
【背景技術】
【０００２】
サービス提供者が、利用者にインターネット、携帯電話網等のネットワークを利用してサービスを提供することがある。この場合、利用者は端末（パーソナルコンピュータ、携帯電話機等）とＩＣカードを利用して遠隔地にいながらサービスを受けることができる。
【０００３】
従来のＩＣカードでは、メモリ上の制約から、認証用の鍵や暗号処理用のアプリケーションを格納する利用形態であったが、メモリ容量の増加、ＵＳＢ等の高速通信インタフェース仕様が制定されてきたこと、Java（登録商標）カードのような高機能カードが登場してきたことにより、端末アプリケーションのような大容量の情報を格納することが可能となってきた。また、端末側のセキュリティを担保する方法として、ソフトウェアだけによる方法では困難になってきており、端末側のセキュリティを担保する手法が求められている。
【０００４】

図４を用いて、従来技術に係るデータ記憶システムについて説明する。図４は、従来技術に係るデータ記憶システムの構成図である。図に示すように、このデータ記憶システムは、利用者端末４０１、ＩＣカード４０２を備えている。利用者端末４０１は、ＲＡＭ４０３、ＲＯＭ４０４、ＣＰＵ４０５、インタフェース４０６、ＥＥＰＲＯＭ４０７を備えている。ＲＯＭ４０４は、ＩＰＬ（Initial Program Loader：初期アプリケーションローダ）４０８を有している。ＥＥＰＲＯＭ４０７は、端末ＯＳ４０９（利用者端末４０１上のＯＳ）、端末アプリケーション４１０（利用者端末４０１上のアプリケーション）、端末データ４１１（利用者端末４０１上のデータ）を有している。ＩＣカード４０２は、秘密鍵４１２、カードＯＳ４１３（ＩＣカード４０２上のＯＳ）を有している。

【０００５】

このような従来技術に係るデータ記憶システムにおいては、認証用の秘密鍵を耐タンパデバイスであるＩＣカード４０２内に格納することにより、不正な利用を防止している。

【０００６】

続いて、図５を用いて、従来技術に係る他のデータ記憶システムについて説明する。図５は、従来技術に係る他のデータ記憶システムの構成図である。図に示すように、このデータ記憶システムは、利用者端末５０１を備えている。利用者端末５０１は、ＴＰＭ（Trusted Platform Module）５０２、ＲＡＭ５０３、ＲＯＭ５０４、ＣＰＵ５０５、インタフェース５０６、ＥＥＰＲＯＭ５０７を備えている。ＴＰＭ５０２は、秘密鍵５１２、実行環境５１３、端末アプリケーションの状態情報（ハッシュ）５１４を有している。ＲＯＭ５０４は、ＩＰＬ５０８を有している。ＥＥＰＲＯＭ５０７は、端末ＯＳ５０９（利用者端末５０１上のＯＳ）、端末アプリケーション５１０（利用者端末５０１上のアプリケーション）、端末データ５１１（利用者端末５０１上のデータ）を有している。

【０００７】

このような従来技術に係るデータ記憶システム（たとえば非特許文献１、２、３に開示されたデータ記憶システム）においては、事前に耐タンパデバイスであるＴＰＭ５０２内に端末アプリケーションの状態情報（ハッシュ）を記憶しておくことにより、端末アプリケーションの改ざんを検出している。すなわち、端末アプリケーションの状態情報（ハッシュ）を計算し、ＴＰＭ５０２内に格納されているハッシュ値と比較することにより、端末アプリケーションの改ざんを検出することが可能であり、また、端末アプリケーションの状態情報（ハッシュ）を不正に書き換えることが不可能である。

【０００８】

続いて、図６を用いて、従来技術に係る他のデータ記憶システムについて説明する。図６は、従来技術に係る他のデータ記憶システムの構成図である。図に示すように、このデータ記憶システムは、利用者端末６０１、認証モジュール（耐タンパ領域を有するデバイス）６０２を備えている。利用者端末６０１は、ＲＡＭ６０３、ＲＯＭ６０４、ＣＰＵ６０５、インタフェース６０６、ＥＥＰＲＯＭ６０７を備えている。ＲＯＭ６０４は、ＩＰＬ６０８を有している。ＥＥＰＲＯＭ６０７は、端末ＯＳ６０９（利用者端末６０１上のＯＳ）、検証用公開鍵６１０、端末データ６１１（利用者端末６０１上のデータ）を有している。認証モジュール６０２は、端末アプリケーション６１２、ディジタル署名６１３、カードＯＳ６１４を有している。

【０００９】

このような従来技術に係るデータ記憶システム（たとえば特許文献１に開示されたデータ記憶システム）においては、耐タンパ性を有するモジュール内に、ディジタル署名付きの端末アプリケーションを格納し、端末アプリケーションの改ざんを防止することが可能であり、また、利用者端末で端末アプリケーションをダウンロードする際に、ディジタル署名の検証を行い、端末アプリケーションの改ざんを検出することが可能である。

【特許文献１】特開２００３－１１８８０９号公報

【非特許文献１】https://www.trustedcomputinggroup.org/specs/TPM/mainP1DPrev103.zip

【非特許文献２】https://www.trustedcomputinggroup.org/specs/TPM/mainP2Structrev1

03.zip
【非特許文献３】https://www.trustedcomputinggroup.org/specs/TPM/mainP3Commandsrev103.zip
【発明の開示】
【発明が解決しようとする課題】
【００１０】
しかしながら、図４、図５に示した従来技術においては、利用者端末４０１、５０１は、サービス提供者ではなく利用者によって管理されることが一般的であり、サービス提供者が要求するセキュリティ条件を満たさない場合があるため、端末アプリケーション（端末上のアプリケーション）の不正な改造が行われる可能性がある。
【００１１】
すなわち、このような従来技術では、端末アプリケーションが、ＨＤＤ、ＥＥＰＲＯＭ等の利用者端末４０１、５０１内の耐タンパ性の低い（内部データの不正な読み出し、改ざんが容易である）記憶領域に格納されていたため、利用者端末４０１、５０１に搭載されているＯＳにセキュリティホールがあった場合、その脆弱性を利用して端末アプリケーションにアクセスし、改ざんすることが可能である。
【００１２】
また、図６に示した従来技術においては、端末アプリケーション６１２が、耐タンパ性を有する認証モジュール６０２に格納されているものの、検証用公開鍵６１０が、利用者端末６０１内の耐タンパ性の低い（内部データの不正な読み出し、改ざんが容易である）記憶領域であるＥＥＰＲＯＭ６０７に格納されているため、検証用公開鍵６１０が安全に保護されず、セキュリティ上の耐攻撃性が低い。
【００１３】
本発明は、上述の課題を解決するためになされたものであり、利用者端末のセキュリティを向上させることが可能なデータ記憶システムおよびデータ記憶方法を提供することを目的とする。
【課題を解決するための手段】
【００１４】
この目的を達成するため、本発明においては、耐タンパ性を有するＩＣカードに格納された情報を読み取り可能な利用者端末にデータを記憶するデータ記憶システムにおいて、上記ＩＣカードは、上記利用者端末のＯＳとアプリケーションとを有し、上記利用者端末は、上記ＩＣカードと相互認証を行うための第１の鍵を有する耐タンパ性の耐タンパモジュール部と、上記第１の鍵を使用して上記ＩＣカードと相互認証したのちに、上記ＩＣカードから上記ＯＳと上記アプリケーションとを取得し、上記ＯＳと上記アプリケーションとを実行する実行部とを備えたことを特徴とする。
【００１５】
この場合、上記利用者端末は、上記ＯＳと上記アプリケーションとを上記耐タンパモジュール部に格納することを特徴としてもよい。
【００１６】
これらの場合、上記ＩＣカードは、ＳＩＭカードであることを特徴としてもよい。
【００１７】
また、耐タンパ性を有するＩＣカードに格納された情報を読み取り可能な利用者端末にデータを記憶するデータ記憶方法において、上記ＩＣカードが上記利用者端末のＯＳとアプリケーションとを記憶するステップと、上記利用者端末が、耐タンパ性の耐タンパモジュール部に格納された第１の鍵を使用して上記ＩＣカードと相互認証を行うステップと、上記第１の鍵を使用して上記ＩＣカードと相互認証したのちに、上記利用者端末が、上記ＩＣカードから上記ＯＳと上記アプリケーションとを取得し、上記ＯＳと上記アプリケーションとを実行するステップとを有することを特徴とする。
【発明の効果】
【００１８】

本発明に係るデータ記憶システム、データ記憶方法においては、ＩＣカードと相互認証を行うための第１の鍵を耐タンパ性の耐タンパモジュール部に格納し、かつ耐タンパ性を有するＩＣカードから利用者端末のＯＳとアプリケーションとを取得するから、第１の鍵、利用者端末のＯＳ、アプリケーションの解析や改ざんに対するセキュリティを向上させることができる。

【００１９】

また、利用者端末のＯＳ、アプリケーションを耐タンパモジュール部に格納したときには、既存の耐タンパデバイスの運用管理技術を利用することができるから、利用者端末のＯＳ、アプリケーションを安全に管理（登録、変更、照会、削除等）することができる。

【発明を実施するための最良の形態】

【００２０】

最初に、図１を用いて、本発明に係るデータ記憶システムについて説明する。図１は、本発明に係るデータ記憶システムの構成図である。図に示すように、このデータ記憶システムは、利用者端末１０１、耐タンパ性を有するＩＣカード１０２、アプリケーション配信サーバ１１７（管理サーバ）、通信網１１９を備えている。利用者端末１０１は、通信網１１９を介して、アプリケーション配信サーバ１１７に接続されている。利用者端末１０１は、ＲＡＭ１０３、ＲＯＭ１０４、ＣＰＵ１０５（実行部）、インタフェース１０６、ＥＥＰＲＯＭ１０７、耐タンパモジュール１１５（耐タンパモジュール部）を備えている。ＲＯＭ１０４は、ＩＰＬ（Initial Program Loader：初期アプリケーションローダ）１０８を有している。耐タンパモジュール１１５は、第１の鍵１１６を有している。ＩＣカード１０２は、秘密鍵１０９（アプリケーション配信サーバ１１７と相互認証を行うための鍵）、カードＯＳ１１０、端末ＯＳ１１１、端末アプリケーション１１２、端末データ１１３、カードマネージャ１１４を有している。アプリケーション配信サーバ１１７は、鍵１１８を有している。

【００２１】

利用者端末１０１は、たとえばパーソナルコンピュータ（ＰＣ）であり、ＣＰＵ、ＲＯＭ、ＲＡＭ、ＥＥＰＲＯＭ、ディスプレイ等を有し、特にＥＥＰＲＯＭには、ブラウザアプリケーションが記憶されている。さらに、携帯端末、インターネット接続機能付携帯電話、ＰＤＡ等も含まれる。また、利用者端末１０１は、ＩＣカード１０２に格納された情報を読み取り可能である。

【００２２】

ＩＣカード１０２は、たとえば利用者端末１０１の利用者の契約情報が記録され、携帯電話会社によって発行されるＳＩＭカード（Subscriber Identity Module card）である。また、このＩＣカード１０２は、アプリケーション配信サーバ１１７に格納された情報を書き込み（ダウンロード）可能である。

【００２３】

ＲＡＭ１０３は揮発性メモリであり、一時的なデータを読み書きするためのメモリである。アプリケーション配信サーバ１１７は、ＩＣカード１０２に対して、端末ＯＳ１１１、端末アプリケーション１１２を配信する。通信網１１９は、インターネット、公衆網、専用線、移動体通信網等の通信網である。

【００２４】

ＲＯＭ１０４は読み出し専用不揮発性メモリであり、データの読み出し専用のメモリである。ＣＰＵ１０５は、中央処理装置であり、ＲＯＭ１０４に格納されたメインアプリケーションや、ＲＡＭ１０３等に展開されたアプリケーション、一時的に格納されたデータ等に基づき転送や演算処理を実行する。また、このＣＰＵ１０５は、ＩＣカード１０２に格納された端末ＯＳ１１１と端末アプリケーション１１２とを耐タンパモジュール１１５に格納された鍵を用いて取得し、利用者端末１０１のＯＳとアプリケーションとを実行する。

【００２５】

インタフェース１０６は、ＩＣカード１０２とデータ交換を行う。ＥＥＰＲＯＭ１０７

は、読み出し書き込み可能不揮発性メモリであり、データを読み書きするためのメモリである。耐タンパモジュール１１５は、ＩＣカード１０２と相互認証を行うための鍵１１６を有する耐タンパ性のモジュールである。また、この耐タンパモジュール１１５は、ＣＰＵ１０５が取得した端末ＯＳ１１１と端末アプリケーション１１２とを格納するようにしてもよい。

【００２６】

ＩＰＬ１０８は、初期プログラム（利用者端末１０１の電源を入れた直後にＯＳ等のシステムアプリケーションを読み込むために実行されるコンピュータ本体に予め組み込まれ、最初に実行されるプログラム）をロードするためのコードである。鍵１１６は、ＩＣカード１０２とデータ交換を行うときに使用される認証用の鍵である。

【００２７】

秘密鍵１０９は、利用者端末１０１とデータ交換を行うときに使用される認証用の鍵である。カードＯＳ１１０は、ＩＣカード１０２上のＯＳである。端末ＯＳ１１１は、利用者端末１０１上のＯＳである。端末アプリケーション１１２は、利用者端末１０１上のアプリケーションである。端末データ１１３は、利用者端末１０１上のデータである。

【００２８】

カードマネージャ１１４は、ＩＣカード１０２の管理を行うモジュールであり、ＩＣカード１０２の発行者の権限によりＩＣカード１０２のデータ（ＩＣカード属性情報、鍵・証明書、リソース情報アプリケーション属性情報等）を管理する。また、このカードマネージャ１１４は、ＡＰＩ（Application Programming Interface）の提供、各アプリケーションの分離・実行に関する機能を実行環境として定義する。また、このカードマネージャ１１４は、秘密鍵１０９を使用してアプリケーション配信サーバ１１７と相互認証したのちに、アプリケーション配信サーバ１１７から端末ＯＳ１１１と端末アプリケーション１１２とを取得する。

【００２９】

鍵１１８は、ＩＣカード１０２とデータ交換を行うときに使用される認証用の鍵である。

【００３０】

続いて、図２、図３を用いて、図１に示したデータ記憶システムの動作すなわち本発明に係るデータ記憶方法について説明する。このデータ記憶方法は、データダウンロード方法とデータ読込方法とを有する。

【００３１】

図２を用いて、本発明に係るデータダウンロード方法の動作について説明する。図２は、本発明に係るデータダウンロード方法の動作を示すシーケンス図である。

【００３２】

まず、アプリケーション配信サーバ１１７が、利用者端末１０１に対して、ダウンロード要求情報を送信する。つぎに、アプリケーション配信サーバ１１７からダウンロード要求情報を受信した利用者端末１０１は、ＩＣカード１０２のカードマネージャ１１４に対して、ＡＴＲ（Answer To Reset：リセット応答）を実行することにより、ＩＣカード１０２のリセットを行う。つぎに、利用者端末１０１によりＡＴＲを実行されたＩＣカード１０２のカードマネージャ１１４は、ＩＣカード１０２のリセットが正常に行われたとき、利用者端末１０１に対して、ＯＫを送信する。ここで、利用者端末１０１によりＡＴＲを実行されたＩＣカード１０２のカードマネージャ１１４は、ＩＣカード１０２のリセットが正常に行われなかったとき、たとえば‘正しいカードを入れてください’というメッセージを利用者端末１０１に表示する。つぎに、ＩＣカード１０２のカードマネージャ１１４からＯＫを受信した利用者端末１０１は、ＩＣカード１０２のカードマネージャ１１４に対して、ＳＥＬＥＣＴ　ＦＩＬＥコマンドを実行する。ここで、ＳＥＬＥＣＴ　ＦＩＬＥコマンドは、ＳＥＬＥＣＴ　ＦＩＬＥ　ＡＩＤ＝’カードマネージャＩＤ’のようにカードマネージャＩＤ（カードマネージャ１１４を識別するための情報）を特定して実行される。つぎに、利用者端末１０１によりＳＥＬＥＣＴ　ＦＩＬＥコマンドを実行された

ＩＣカード１０２のカードマネージャ１１４は、ＳＥＬＥＣＴ　ＦＩＬＥコマンドが実行されることにより、端末ＯＳ１１１、カードマネージャ１１４のＡＩＤ（アプリケーションＩＤ：アプリケーションを識別するための情報）が選択されたとき、利用者端末１０１に対して、ＯＫを送信する。つぎに、ＩＣカード１０２のカードマネージャ１１４からＯＫを受信した利用者端末１０１は、ＩＣカード１０２のカードマネージャ１１４に対して、ＳＡＣ　ＩＮＩＴコマンドを実行する。ここで、ＳＡＣ　ＩＮＩＴコマンドとは、利用者端末１０１とＩＣカード１０２のカードマネージャ１１４間で、プロファイル情報、乱数、証明書（データ部）を交換することにより、相互認証の処理を行うためのコマンドである。つぎに、利用者端末１０１によりＳＥＬＥＣＴ　ＦＩＬＥコマンドを実行されたＩＣカード１０２のカードマネージャ１１４は、ＳＡＣ　ＩＮＩＴコマンドが実行されることにより、相互認証の処理が正常に行われたとき、利用者端末１０１に対して、ＯＫを送信する。このＯＫの送信が完了することにより、利用者端末１０１とＩＣカード１０２のカードマネージャ１１４間における相互認証が完了する。なお、この相互認証には、鍵１１６と秘密鍵１０９とが用いられる。つぎに、アプリケーション配信サーバ１１７とＩＣカード１０２間における相互認証と暗号化通信路の確立とを行う。なお、この相互認証と暗号化通信路の確立には、鍵１１８と秘密鍵１０９とが用いられる。つぎに、アプリケーション配信サーバ１１７は、暗号化通信路によりＩＣカード１０２のカードマネージャ１１４に対して、端末ＯＳ１１１のダウンロードを実行する。つぎに、アプリケーション配信サーバ１１７により端末ＯＳ１１１のダウンロードが正常に実行されたときには、ＩＣカード１０２のカードマネージャ１１４は、利用者端末１０１に対して、ＯＫを送信し、アプリケーション配信サーバ１１７に対して、ＯＫを送信する。つぎに、ＩＣカード１０２のカードマネージャ１１４からＯＫを受信したアプリケーション配信サーバ１１７は、暗号化通信路によりＩＣカード１０２のカードマネージャ１１４に対して、端末アプリケーション１１２のダウンロードを実行する。つぎに、アプリケーション配信サーバ１１７により端末アプリケーション１１２のダウンロードが正常に実行されたときには、ＩＣカード１０２のカードマネージャ１１４は、利用者端末１０１に対して、ＯＫを送信し、アプリケーション配信サーバ１１７に対して、ＯＫを送信する。

【００３３】

図３を用いて、本発明に係るデータ読込方法の動作について説明する。図３は、本発明に係るデータ読込方法の動作を示すシーケンス図である。

【００３４】

まず、利用者が利用者端末１０１の電源をＯＮにする。つぎに、利用者端末１０１は、ＲＯＭ１０４に記憶されたＩＰＬ１０８を読み込み、ＩＰＬ１０８を実行する。つぎに、利用者端末１０１は、ＩＣカード１０２に対して、ＡＴＲを実行することにより、ＩＣカード１０２のリセットを行う。つぎに、利用者端末１０１によりＡＴＲを実行されたＩＣカード１０２は、ＩＣカード１０２のリセットが正常に行われたとき、利用者端末１０１に対して、ＯＫを送信する。ここで、利用者端末１０１によりＡＴＲを実行されたＩＣカード１０２のカードマネージャ１１４は、ＩＣカード１０２のリセットが正常に行われなかったとき、たとえば‘正しいカードを入れてください’というメッセージを利用者端末１０１に表示する。つぎに、ＩＣカード１０２からＯＫを受信した利用者端末１０１は、ＩＣカード１０２に対して、ＳＥＬＥＣＴ　ＦＩＬＥコマンドを実行する。ここで、ＳＥＬＥＣＴ　ＦＩＬＥコマンドは、ＳＥＬＥＣＴ　ＦＩＬＥ　ＡＩＤ＝’端末ＯＳＩＤ’のように端末ＯＳＩＤ（端末ＯＳ１１１を識別するための情報）を特定して実行される。つぎに、利用者端末１０１によりＳＥＬＥＣＴ　ＦＩＬＥコマンドを実行されたＩＣカード１０２は、ＳＥＬＥＣＴ　ＦＩＬＥコマンドが実行されることにより、端末ＯＳ１１１のＡＩＤが選択されたとき、利用者端末１０１に対して、ＯＫを送信する。つぎに、ＩＣカード１０２からＯＫを受信した利用者端末１０１は、利用者に対してＰＩＮ（Personal Identification Number）の入力を要求する。ここで、ＰＩＮとは、広義的には、クレジットカード等で使用される暗証番号のことであり、ネットへの不正なアクセスを防止するため個人識別番号として使われるものである。また、ＰＩＮ認証により、たとえば利用者

端末１０１が携帯電話機の場合において、利用者以外の第三者が携帯電話機を拾ったときに携帯電話機を利用することを防止できる。また、ＩＣカード１０２に記憶されたデータの読み出し、ＩＣカード１０２へのデータの書き込みは、ＰＩＮ認証が必要であり、予め定められたインタフェースでしかできないようになっている。つぎに、利用者端末１０１からＰＩＮの入力を要求された利用者は、利用者端末１０１によりＰＩＮを入力する。つぎに、利用者によりＰＩＮを入力された利用者端末１０１は、ＩＣカード１０２に対して、ＰＩＮ　ＶＥＲＩＦＹコマンドを実行する。つぎに、利用者端末１０１によりＰＩＮ　ＶＥＲＩＦＹコマンドを実行されたＩＣカード１０２は、ＰＩＮ　ＶＥＲＩＦＹコマンドが実行されることにより、ＰＩＮが照合される。つぎに、ＩＣカード１０２は、このＰＩＮの照合が完了したとき、利用者端末１０１に対して、ＯＫを送信する。つぎに、利用者端末１０１とＩＣカード１０２間における相互認証と暗号化通信路の確立とを行う。なお、この相互認証と暗号化通信路の確立には、鍵１１６と秘密鍵１０９とが用いられる。この相互認証により、端末アプリケーション１１２を読み込むべきＩＣカード１０２が正しく（偽造されていなく）、かつ利用者端末１０１が正しいか否かを確認することができる。つぎに、ＩＣカード１０２からＯＫを受信した利用者端末１０１は、ＩＣカード１０２に対して、ＲＥＡＤ　ＢＩＮＡＲＹコマンドを実行する。ここで、ＲＥＡＤ　ＢＩＮＡＲＹコマンドとは、ＩＣカード１０２に記憶されたバイナリデータを読み出すためのコマンドである。すなわち、ここでは端末ＯＳ１１１のバイナリデータを読み出す。つぎに、利用者端末１０１によりＲＥＡＤ　ＢＩＮＡＲＹコマンドを実行されたＩＣカード１０２は、ＲＥＡＤ　ＢＩＮＡＲＹコマンドが実行されることにより、利用者端末１０１により端末ＯＳ１１１が正常に読み込まれたとき、利用者端末１０１に対して、ＯＫを送信する。この場合、ＣＰＵ１０５は、端末ＯＳ１１１を耐タンパモジュール１１５に格納するようにしてもよい。つぎに、ＩＣカード１０２からＯＫを受信した利用者端末１０１は、端末ＯＳ１１１を起動する。つぎに、この利用者端末１０１は、ＩＣカード１０２に対して、ＳＥＬＥＣＴ　ＦＩＬＥコマンドを実行する。ここで、ＳＥＬＥＣＴ　ＦＩＬＥコマンドは、ＳＥＬＥＣＴ　ＦＩＬＥ　ＡＩＤ＝’端末アプリケーションＩＤ’のように端末アプリケーションＩＤ（端末アプリケーション１１２を識別するための情報）を特定して実行される。つぎに、利用者端末１０１によりＳＥＬＥＣＴ　ＦＩＬＥコマンドを実行されたＩＣカード１０２は、ＳＥＬＥＣＴ　ＦＩＬＥコマンドが実行されることにより、端末アプリケーション１１２のＡＩＤが選択されたとき、利用者端末１０１に対して、ＯＫを送信する。つぎに、ＩＣカード１０２のカードマネージャ１１４からＯＫを受信した利用者端末１０１は、ＩＣカード１０２に対して、ＲＥＡＤ　ＢＩＮＡＲＹコマンドを実行する。すなわち、ここでは端末アプリケーション１１２のバイナリデータを読み出す。つぎに、利用者端末１０１によりＲＥＡＤ　ＢＩＮＡＲＹコマンドを実行されたカード１０２は、ＲＥＡＤ　ＢＩＮＡＲＹコマンドが実行されることにより、利用者端末１０１により端末アプリケーション１１２が正常に読み込まれたとき、利用者端末１０１に対して、ＯＫを送信する。この場合、ＣＰＵ１０５は、端末アプリケーション１１２を耐タンパモジュール１１５に格納するようにしてもよい。つぎに、ＩＣカード１０２からＯＫを受信した利用者端末１０１は、端末アプリケーション１１２を起動する。

【００３５】

上述したデータ記憶システム、データ記憶方法においては、ＩＣカード１０２と相互認証を行うための鍵１１６を耐タンパ性の耐タンパモジュール１１５に格納し、かつ耐タンパ性を有するＩＣカード１０２から端末ＯＳ１１１と端末アプリケーション１１２とを取得するから、鍵１１６、端末ＯＳ１１１、端末アプリケーション１１２の解析や改ざんに対するセキュリティを向上させることができる。

【００３６】

また、端末ＯＳ１１１、端末アプリケーション１１２を耐タンパモジュール１１５に格納するから、既存の耐タンパデバイスの運用管理技術を利用することができるから、端末ＯＳ１１１、端末アプリケーション１１２を安全に管理（登録、変更、照会、削除等）することができる。

【００３７】
　また、ＩＣカード１０２がアプリケーション配信サーバ１１７と相互認証を行うための秘密鍵１０９を有するから、ＩＣカード１０２とアプリケーション配信サーバ１１７との間の情報通信を安全に行うことができる。
【００３８】
　なお、本発明は以上の実施の形態に限定されるものではなく、また、本発明の要旨を逸脱しない範囲において種々の変更が可能であることは勿論である。
【図面の簡単な説明】
【００３９】
【図１】本発明に係るデータ記憶システムの構成図である。
【図２】本発明に係るデータダウンロード方法の動作を示すシーケンス図である。
【図３】本発明に係るデータ読込方法の動作を示すシーケンス図である。
【図４】従来技術に係るデータ記憶システムの構成図である。
【図５】従来技術に係る他のデータ記憶システムの構成図である。
【図６】従来技術に係る他のデータ記憶システムの構成図である。
【符号の説明】
【００４０】
　１０１…利用者端末
　１０２…ＩＣカード
　１０５…ＣＰＵ
　１０９…秘密鍵
　１１１…端末ＯＳ
　１１２…端末アプリケーション
　１１４…カードマネージャ
　１１５…耐タンパモジュール
　１１６…鍵
　１１７…アプリケーション配信サーバ

【図１】

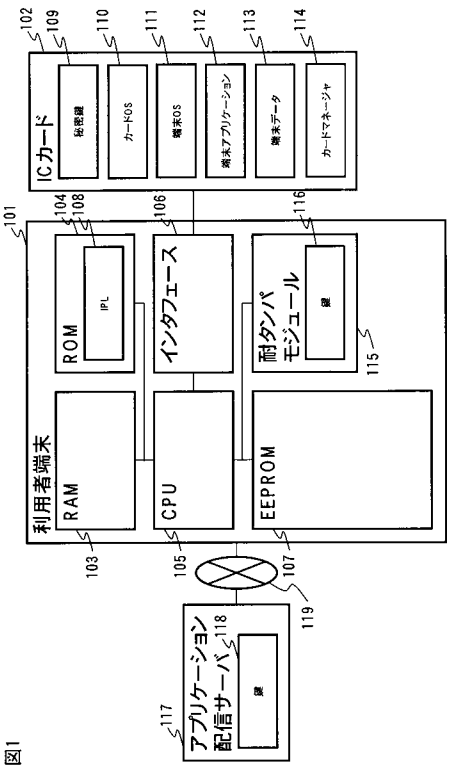

図1

【図２】

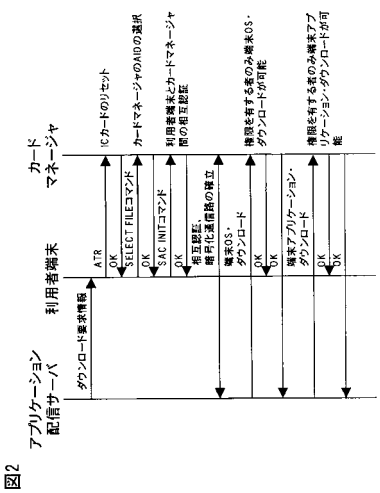

図2

【図３】

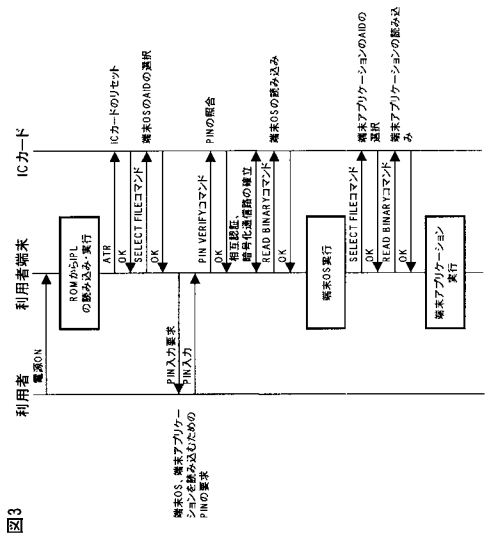

図3

【図４】

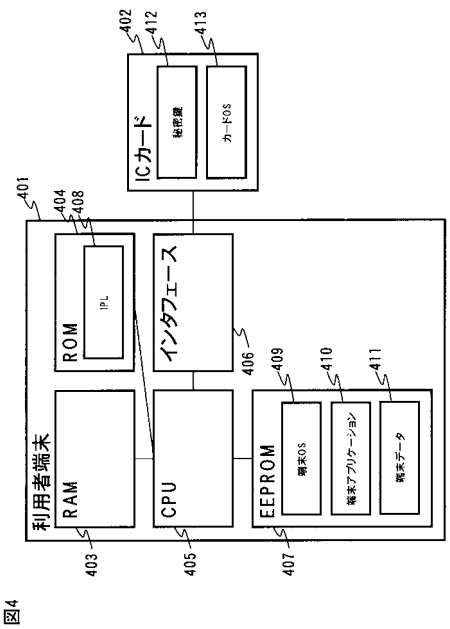

図4

【図５】

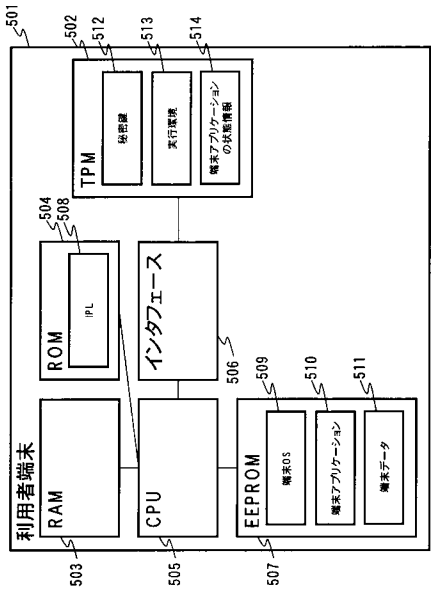
501
502
512
513
514
TPM
秘密鍵
実行環境
端末アプリケーションの状態情報
504
508
ROM
IPL
インタフェース
506
509
510
511
利用者端末
RAM
CPU
EEPROM
端末OS
端末アプリケーション
端末データ
503
505
507

図5

【図６】

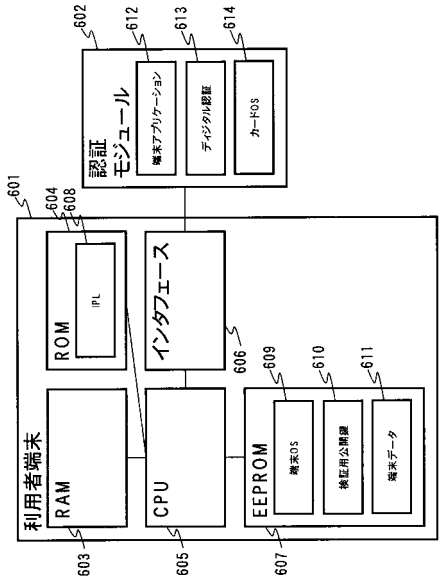
602
612
613
614
認証モジュール
端末アプリケーション
ディジタル証証
カードOS
601
604
608
ROM
IPL
インタフェース
606
609
610
611
利用者端末
RAM
CPU
EEPROM
端末OS
検証用公開鍵
端末データ
603
605
607

図6

フロントページの続き

(51)Int.Cl.		F I		テーマコード（参考）
G06F 21/06	*(2006.01)*	H04L 9/00	621A	
		G06F 12/14	560E	

Fターム(参考) 5B017 AA01 BA05 BA07 BA09 BB09 CA14 CA15
5B176 BA10 BB04
5B276 FA20 FB06 FB20 FD02
5B285 AA01 AA05 BA02 BA03 BA06 BA11 CA41 CA52 CB07 CB42
CB44 CB72 CB74 CB75 CB76 CB82 DA01 DA03 DA05 DA08
5J104 AA07 AA16 EA04 EA08 EA16 KA02 NA02 NA35 NA37 NA42
PA07