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

特許第5400611号
(P5400611)

(45)発行日　平成26年1月29日(2014.1.29)　(24)登録日　平成25年11月1日(2013.11.1)

(51)Int.Cl.		F I		
G06F 21/12	(2013.01)	G06F	21/22	112L
G06K 19/07	(2006.01)	G06K	19/00	N
G06K 19/073	(2006.01)	G06K	19/00	P
G06K 17/00	(2006.01)	G06K	17/00	D

請求項の数 9　(全 28 頁)

(21)出願番号　特願2009-516180 (P2009-516180)
(86)(22)出願日　平成20年5月23日 (2008.5.23)
(86)国際出願番号　PCT/JP2008/001289
(87)国際公開番号　WO2008/146476
(87)国際公開日　平成20年12月4日 (2008.12.4)
審査請求日　平成23年4月28日 (2011.4.28)
(31)優先権主張番号　特願2007-137649 (P2007-137649)
(32)優先日　平成19年5月24日 (2007.5.24)
(33)優先権主張国　日本国(JP)

(73)特許権者　000005821
パナソニック株式会社
大阪府門真市大字門真１００６番地
(74)代理人　100081422
弁理士　田中　光雄
(74)代理人　100100158
弁理士　鮫島　睦
(74)代理人　100125874
弁理士　川端　純市
(72)発明者　宗　広和
大阪府門真市大字門真１００６番地　パナソニック株式会社内
(72)発明者　竹内　康雄
大阪府門真市大字門真１００６番地　パナソニック株式会社内

最終頁に続く

(54)【発明の名称】メモリコントローラ、不揮発性記憶装置、不揮発性記憶システム、及びアクセス装置

(57)【特許請求の範囲】

【請求項１】

アプリケーションを識別するためのアプリケーション識別子と前記アプリケーションの有無及び前記アプリケーションを個別にカスタマイズするためのデータである個別データの有無によって決定されるアプリケーションの管理状態とを保持する記憶手段と、

外部と通信するための通信手段と、

外部から受信したアプリケーション識別子を含むインストールに関するデータを解釈するための解釈手段と、

前記解釈手段により、外部から受信した前記データから前記アプリケーション識別子を取得し、前記アプリケーション識別子から前記アプリケーションの管理状態を取得し、前記管理状態から署名検証の必要性を判断する状態判断手段と、

前記状態判断手段からの結果を受けて、

前記解釈手段により、外部から受信した前記データから署名対象データ、署名を取得し、

前記署名対象データに対してハッシュ処理を行うハッシュ生成手段と、

前記署名に対して復号処理を行う暗復号手段と、

前記ハッシュ生成手段が生成したハッシュと前記署名を復号した際に取得したハッシュを照合する照合手段と、

前記通信手段を使用して前記照合手段が判断した結果を外部に通知することを特徴とする不揮発性記憶装置。

【請求項２】
前記照合手段によって、前記署名対象データの正当性を検証した結果、正当であれば前記署名対象データを実行可能として前記記憶手段で保持する前記アプリケーションの管理状態を変更する登録手段を有することを特徴とする請求項１に記載の不揮発性記憶装置。
【請求項３】
前記通信手段が受信するデータは、少なくとも２分割されて送信され、前記署名が第１のデータに含まれ、前記署名対象データが第２のデータに含まれており、前記署名を前記暗復号手段で復号し、前記復号データに適切なパディング結果が含まれていない場合に、前記第２のデータを送信しないことを外部に通知することを特徴とする請求項２に記載の不揮発性記憶装置。
【請求項４】
アプリケーションを識別するためのアプリケーション識別子と前記アプリケーションの有無及び前記アプリケーションを個別にカスタマイズするためのデータである個別データの有無によって決定されるアプリケーションの管理状態とを保持する記憶手段にアクセスするための記憶制御手段と、
外部と通信するための通信手段と、
外部から受信したアプリケーション識別子を含むインストールに関するデータを解釈するための解釈手段と、
前記解釈手段により、外部から受信した前記データから前記アプリケーション識別子を取得し、前記アプリケーション識別子から前記アプリケーションの管理状態を取得し、前記管理状態から署名検証の必要性を判断する状態判断手段と、
前記状態判断手段からの結果を受けて、
前記解釈手段により、外部から受信した前記データから署名対象データ、署名を取得し、
前記署名対象データに対してハッシュ処理を行うハッシュ生成手段と、
前記署名に対して復号処理を行う暗復号手段と、
前記ハッシュ生成手段が生成したハッシュと前記署名を復号した際に取得したハッシュを照合する照合手段と、
前記通信手段を使用して前記照合手段が判断した結果を外部に通知することを特徴とするメモリコントローラ。
【請求項５】
前記照合手段によって、前記署名対象データの正当性を検証した結果、正当であれば前記署名対象データを実行可能として前記記憶手段で保持する前記アプリケーションの管理状態を変更する登録手段を有することを特徴とする請求項４に記載のメモリコントローラ。
【請求項６】
前記通信手段が受信するデータは、少なくとも２分割されて送信され、前記署名が第１のデータに含まれ、前記署名対象データが第２のデータに含まれており、前記署名を前記暗復号手段で復号し、前記復号データに適切なパディング結果が含まれていない場合に、前記第２のデータを送信しないことを外部に通知することを特徴とする請求項５に記載のメモリコントローラ。
【請求項７】
アクセス装置と、前記アクセス装置からのアクセス指示に応じてデータの読み出し、書き込みを行う不揮発性記憶装置とを有した不揮発性記憶システムであって、
前記不揮発性記憶装置は、
不揮発性メモリと、
アプリケーションを識別するためのアプリケーション識別子と前記アプリケーションの有無及び前記アプリケーションを個別にカスタマイズするためのデータである個別データの有無によって決定されるアプリケーションの管理状態とを保持する前記不揮発性記憶装置にアクセスするための記憶制御手段と、

前記アクセス装置と通信するための通信手段と、
前記アクセス装置から受信したアプリケーション識別子を含むインストールに関するデータを解釈するための解釈手段と、
前記解釈手段により、外部から受信した前記データから前記アプリケーション識別子を取得し、前記アプリケーション識別子から前記アプリケーションの管理状態を取得し、前記管理状態から署名検証の必要性を判断する状態判断手段と、
前記状態判断手段からの結果を受けて、
前記解釈手段により、外部から受信した前記データから署名対象データ、署名を取得し、
前記署名対象データに対してハッシュ処理を行うハッシュ生成手段と、
前記署名に対して復号処理を行う暗復号手段と、
前記ハッシュ生成手段が生成したハッシュと前記署名を復号した際に取得したハッシュを照合する照合手段からなるメモリコントローラを有し、
前記通信手段を使用して前記照合手段が判断した結果を前記アクセス装置に通知することを特徴とする不揮発性記憶システム。
【請求項８】
請求項１に記載の不揮発性記憶装置と接続して使用するアクセス装置であって、
前記アクセス装置は、
前記不揮発性記憶装置と通信するための通信手段と、
前記不揮発性記憶装置に送信するアプリケーション識別子を含むインストールに関するデータを記憶する記憶手段と、
前記記憶手段から前記不揮発性記憶装置に送信する前記データを読み出し、前記不揮発性記憶装置が受信可能なデータに変換するプロトコル変換手段を有し、
前記不揮発性記憶装置から通知される署名検証が必要かどうかの結果を受信し、前記結果に基づき、前記不揮発性記憶装置との通信を制御することを特徴とするアクセス装置。
【請求項９】
前記記憶手段は、前記アクセス装置の外部にあり通信路によって接続されている第２のアクセス装置内にあることを特徴とする請求項８に記載のアクセス装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、不揮発性メモリの制御を行うメモリコントローラ、不揮発性メモリを備えた半導体メモリカード等の不揮発性記憶装置、不揮発性記憶装置にアクセス装置を構成要件として加えた不揮発性記憶システム及びアクセス装置に関する。
【背景技術】
【０００２】
書き換え可能な不揮発性メモリを備える不揮発性記憶装置は、半導体メモリカードを中心にその需要が広まっている。半導体メモリカードは、光ディスクやテープメディアなどと比較して高価格なものではあるが、小型・軽量・耐震性・取り扱いの簡便さ等のメリットにより、デジタルスチルカメラや携帯電話などのポータブル機器の記録媒体としてその需要が広まり、最近では民生用動画記録機器や放送局向けのプロ用動画記録機器の記録媒体として利用されるようになってきた。更には、ポータブル機器だけではなくデジタルテレビやＤＶＤレコーダ等の据え置き機器にも半導体メモリカード用のスロットが標準装備され、デジタルスチルカメラで撮影した静止画をデジタルテレビで閲覧したり、民生用動画記録機器で撮影した動画をＤＶＤレコーダにダビングできるようになってきた。
【０００３】
不揮発性記憶装置の中には、特定の目的を持つアプリケーションを搭載可能なものもあり、内部に格納するデータを暗号化し、外部に出力する際に復号するような秘匿性を高めた機能や、著作権保護機能付きのカードがある。また、発行後にアプリケーションを追加できるダウンロード可能なカードも登場している。

【０００４】
このようなアプリケーションを後から発行する場合、カードはデータを受信し、カード内で動作するようにインストールと呼ばれるデータ変換、配置処理をする仕組みが必要になる。カードには、不揮発性の主記憶メモリとしてフラッシュメモリを備え、それを制御するメモリコントローラを有しており、前述の処理の場合、別のチップを搭載せずにメモリコントローラで実現することもできる。
【０００５】
搭載するアプリケーションに対して、カード上の動作を制御して異常動作をさせないように安全に実行できるＶＭ（Ｖｉｒｔｕａｌ　Ｍａｃｈｉｎｅ）を使った方法の他に、カード外で予めアプリケーションの動作をチェックし、安全なアプリケーションだと確認できたアプリケーションだけをカードにインストールする方法もある。後者の場合、カードにＶＭのようなチェック機構を搭載しなくて良い分、カード1枚当たりのコストが安くなる利点がある。
【０００６】
カードが外部からの受信したアプリケーションを正しいものとして確認する方法に、特許文献１がある。この文献では、アプリケーション（ロードモジュール）もしくは実行可能なプログラムに対して署名データを付与し、アプリケーションとその署名をカードに送付し、正当性をカード内で検証することで、アプリケーションをカード内で実行可能にするものである。この文献に開示された技術を応用することによって、アプリケーションに対する正当性を確認することができる。
【特許文献１】米国特許６１５７７２１号公報
【発明の開示】
【発明が解決しようとする課題】
【０００７】
しかしながら、送付するアプリケーションとカードが持つ管理状態との関係によって、カードに送付するデータに署名を含まない場合がある。また、アプリケーションと同時、もしくはその後に署名データを受信すると、署名データ自体が正しく復号できない場合でも、署名データと比較して大容量であるアプリケーションを必ず受信するため、負担が大きい。
【０００８】
そこで本発明は上記問題点に鑑み、アプリケーションを受信する前にカード内の管理状態を確認し、署名処理やアプリケーションの受信処理にかかる負担を軽減できるメモリコントローラ、不揮発性記憶装置、及び不揮発性記憶システム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】
【０００９】
前記目的を達成するため、本発明においては以下の技術的手段を講じた。すなわち、本発明における技術的手段は、外部からのアプリケーションを識別するためのアプリケーション識別子とアプリケーションと、前記アプリケーションが参照する参照データと、前記アプリケーションに対する署名を受信し、前記アプリケーションと前記参照データの書き込みを行うメモリコントローラであって、前記メモリコントローラは、外部からデータを受信する通信手段を持ち、前記アプリケーション識別子を受信した後、前記アプリケーション識別子とアプリケーションの管理状態を管理する記憶手段（１００５）にアクセスし、対象となるアプリケーションの管理状態を読み出し、その前記管理状態によって、必要なデータを判断する状態判断手段（１００８）を持ち、前記通信手段を使用して前記状態判断手段が算出した結果を外部に通知することを特徴とする。
【００１０】
また、前記状態判断手段（１００８）からの制御によって、署名検証が必要な場合は、前記署名の検証を行う暗号処理手段にアクセスし、前記署名と前記アプリケーションを渡し、アプリケーションの正当性を検証したのち、アプリケーションが正当であれば、アプ

リケーションを実行可能として前記記憶手段で管理する前記管理状態を変更する登録手段を有することを特徴とする。

【００１１】

また、前記暗号処理手段は、データの暗復号を行うデータ暗復号手段、データのハッシュを生成するハッシュ生成手段、生成した前記ハッシュと署名を復号して算出したハッシュを照合する照合手段と、を有していることが好ましい。

【００１２】

また、前記管理状態は、アプリケーションと参照データの両方が登録されている、アプリケーションだけが登録されている、参照データだけが登録されている、何も登録されていない、のうちの少なくとも１つであることが好ましい。

【００１３】

また、前記通信手段が受信するデータは、少なくとも２分割されて送信され、前記署名が第１のデータに含まれ、前記署名対象データが第２のデータに含まれており、前記署名を前記暗復号手段で復号し、前記復号データに特定の文字列が含まれていない場合に、前記第２のデータを送信しないことを外部に通知することを特徴とする。

【００１４】

また、本発明における技術的手段は、不揮発性メモリと、前記不揮発メモリに対してデータの読み出し、書き込みを行う前記メモリコントローラと、前記暗号処理を行う暗号処理手段と、を有した不揮発性記憶装置であって、前記不揮発性記憶装置は外部からアプリケーション識別子とアプリケーションと、前記アプリケーションが参照する参照データと、前記アプリケーションに対する署名を受信する通信手段を持ち、前記メモリコントローラは前記アプリケーション識別子を受信した後、前記アプリケーション識別子（Ｌ０１）とアプリケーションの管理状態（Ｌ０２）を管理する記憶手段にアクセスし、対象となるアプリケーションの前記管理状態（Ｌ０２）を読み出し、その前記管理状態によって、必要なデータを判断する状態判断手段（１００８）を持ち、前記通信手段を使用して前記状態判断手段が算出した結果を外部に通知することを特徴とする。

【００１５】

また、前記状態判断手段（１００８）からの制御によって、署名検証が必要な場合、前記署名検証を行う前記暗号処理手段にアクセスし、前記署名と前記アプリケーションを渡し、アプリケーションの正当性を検証したのち、前記アプリケーションが正当であれば、前記アプリケーションを実行可能として前記記憶手段で管理する前記管理状態を変更する登録手段を有することを特徴とする。

【００１６】

また、前記通信手段が受信するデータは、少なくとも２分割されて送信され、前記署名が第１のデータに含まれ、前記署名対象データが第２のデータに含まれており、前記署名を前記暗復号手段で復号し、前記復号データに特定の文字列が含まれていない場合に、記第２のデータを送信しないことを外部に通知することを特徴とする。

【００１７】

また、本発明における技術的手段は、アプリケーションと、アプリケーションが参照する参照データと、アプリケーション識別子と、アプリケーションに対する署名を持ち、不揮発性記憶装置と通信ができるアクセス装置と、前記アクセス装置からのアクセス指示に応じてデータの読み出し、書き込みを行う不揮発性記憶装置とを有した不揮発性記憶システムであって、前記不揮発性記憶装置は、不揮発性メモリと、前記メモリからの読み出しもしくは書き込みを制御する前記メモリコントローラを有することを特徴とする。

【００１８】

また、本発明における技術的手段は、不揮発性メモリを有する不揮発性記憶装置と接続して使用するアクセス装置であって、前記アクセス装置は、前記不揮発性記憶装置に送信するデータを記憶する記憶手段と、前記記憶手段から前記不揮発性記憶装置に送信するデータを読み出し、前記不揮発性記憶装置が受信可能なデータに変換するプロトコル変換手段とを有し、前記不揮発性記憶装置から通知される署名検証が必要性かどうかの結果を受

信し、前記結果に基づき、データの送信を制御することを特徴とする。
【００１９】
　また、前記記憶手段は、前記アクセス装置の外部にあり通信路によって接続されている第２のアクセス装置内にあることを特徴とする。
【発明の効果】
【００２０】
　アプリケーションを受信する前に、先に受信するアプリケーション識別子からデータ送信の必要性を検証し、無駄なデータ送信を抑えることができる。
【図面の簡単な説明】
【００２１】
【図１】図１はサーバ、外部機器、カードの関係図である。
【図２】図２はカード構成図である。
【図３】図３はサーバ、外部機器、カードの構成図である。
【図４】図４はプレイヤーの関係図である。
【図５】図５はアプリ開発者、サービス提供者、カード製造者、カード間での処理フローである。
【図６】図６はサーバ運用者、サービス提供者間での処理フローである。
【図７Ａ】図７Ａはサーバ運用者、サーバ、外部機器、カード間での処理フロー１である。
【図７Ｂ】図７Ｂはサーバ運用者、サーバ、外部機器、カード間での処理フロー２である。
【図７Ｃ】図７Ｃはサーバ運用者、サーバ、外部機器、カード間での処理フロー３である。
【図８】図８は個別データである。
【図９】図９は管理データフォーマットである。
【図１０】図１０はサーバでのデータ格納構成とカードバージョン情報との関係図である。
【図１１】図１１は領域制御手段を含むカード構成図である。
【図１２】図１２はカードと外部機器間の通信フローである。
【図１３】図１３は２系統保持するカードと外部機器間の通信フローである。
【図１４】図１４はデータ更新時での通信フローである。
【図１５Ａ】図１５Ａはデータ更新時の処理フロー１である。
【図１５Ｂ】図１５Ｂはデータ更新時の処理フロー２である。
【図１６Ａ】図１６Ａは２系統保持するカードとの処理フロー１である。
【図１６Ｂ】図１６Ｂは２系統保持するカードとの処理フロー２である。
【図１６Ｃ】図１６Ｃは２系統保持するカードとの処理フロー３である。
【図１６Ｄ】図１６Ｃは２系統保持するカードとの処理フロー４である。
【図１７】図１７はアプリケーション識別子と管理状態の関係図である。
【図１８】図１８はアプリケーションに対する状態遷移図である。
【符号の説明】
【００２２】
１００　カード
１００１　通信手段
１００２　コマンド解釈手段
１００３　記憶制御手段
１００４　数値計算手段
１００５　記憶手段
１００６　暗復号手段
１００７　照合手段
１００８　状態判断手段

１００９　ハッシュ生成手段
１０１０　領域制御手段
２００　外部機器
２００１　通信手段
２００２　プロトコル変換手段
２００３　一時記憶手段
３００　サーバ
３００１　通信手段
３００２　記憶制御手段
３００３　記憶手段
Ｐ１　カード製造者
Ｐ２　アプリケーション開発者
Ｐ３　サービス提供者
Ｐ４　サーバ運用者
Ｐ５　ユーザ
Ｐ６　カード販売者
Ｍ０１　製造者公開鍵
Ｍ０２　製造者秘密鍵
ＭＯ３　カード公開鍵
Ｍ０４　カード秘密鍵
Ａ０１　アプリケーション暗号鍵
Ａ０２　アプリケーション
Ａ０３　暗号化アプリケーション
Ａ０４　暗号化アプリケーション暗号鍵
Ａ０５　署名
Ｈ０１　個別データ暗号鍵
Ｈ０２　個別データ
Ｈ０３　暗号化個別データ
Ｈ０４　暗号化個別データ暗号鍵
Ｈ０５　個別データから生成したハッシュ
Ｈ０６　共通データ
Ｈ０７　管理データ
Ｈ０８　管理データ暗号鍵
Ｈ０９　暗号化した管理データ
Ｈ１０　暗号化した管理データ暗号鍵
Ｈ１１　署名から取得したハッシュ

【発明を実施するための最良の形態】

【００２３】

（第1の実施の形態）

本実施の形態では、図１、図３に示す通り、サーバ（３００）、外部機器（２００）、カード（１００）の３つの機器から構成されるシステムについて説明する。サーバ（３００）は、記憶手段（３００３）にアプリケーションの実体となるアプリケーションコード、アプリケーションが参照するアプリケーションデータ、対応するカード情報、その他外部端末に関する情報を保持しており、記憶制御手段（３００２）を経由して外部に出力する通信手段（３００１）をもつ。アプリケーションコード、プログラムなど実行コード、実行可能プログラムに当たる用語を、以後アプリケーション（Ａ０２）と記載する。記憶制御手段（３００２）は、通信手段（３００１）経由で外部からの要求に受け、前記要求に応じて、選択的にデータを読み出すことができる。外部機器（２００）は、サーバから受信したデータやコードを通信手段（２００１）で受信し、カードに送信可能なコマンドに変換するプロトコル変換手段（２００２）で変換した後、通信手段（２００１）を使っ

てカードにコマンドを渡す。サーバ（３００）から予めカードのコマンド仕様に準じたデータを受信した場合、外部機器（２００）は、受信したデータをそのままカード（１００）に送信するだけになる。カード（１００）（図２参照）は、通信手段（１００１）を用いて受信したコマンドを解釈するコマンド解釈手段（１００２）を持ち、受信したコマンドを解釈した結果に応じて、データの配置およびデータの変換、データの演算を行う数値計算手段（１００４）にデータを渡す。数値計算手段（１００４）では、必要に応じて暗復号処理を行う暗復号手段（１００６）とデータの比較、照合を行う照合手段（１００７）、データのハッシュ値を生成するハッシュ生成手段（１００９）と記憶手段（１００５）を制御する記憶制御手段（１００３）を用いて、暗号処理を行う。記憶手段（１００５）は、カード内のデータを保持しておく部分であり、記憶制御手段（１００４）を介してアクセスされる。また、記憶手段（１００５）が持つアプリケーション識別子とアプリケーションの状態から署名検証が必要であるかを判断する状態判断手段（１００８）を持つ。

【００２４】

本実施の形態では、上記システム構成とは別に、図４に示す外部機器を操作して、カードに対するデータをサーバに要求するトリガーを投げるプレイヤー（Ｐ５）（以後、ユーザとする）、アプリケーションを開発するプレイヤー（Ｐ２）（以後、アプリ開発者とする）、サービスを提供するプレイヤー（Ｐ３）（以後、サービス提供者とする）、サーバの運用を行うプレイヤー（Ｐ４）（以後、サーバ運用者とする）、カードを製造・発行するプレイヤー（Ｐ１）（以後、カード製造者とする）の５者が存在する。カード（１００）をユーザに販売するプレイヤー（Ｐ６）としてカード販売者が運用上は存在するが、本実施の形態には直接関係無いので省略する。その他のプレイヤーは、ユーザから見た場合、特に意識されるものではないが、システム上、実施する処理内容が異なると想定し、分けて考える。アプリ開発者（Ｐ２）は、共通的、汎用的に配布可能なアプリケーションを開発すると想定する。そのため、このアプリケーションは、サービスを提供する複数のサービス提供者に汎用的に提供することが可能であり、サービス提供者（Ｐ３）が識別情報や鍵情報などのサービス固有の情報を入れることで、アプリケーションをカスタマイズすることができる。サービス提供者（Ｐ３）は前述したアプリケーションをカスタマイズして、実際のサービスを運営するものであると想定する。サーバ運用者（Ｐ４）は、外部機器（２００）からの要求に応じて、データを出力する一般的なＷｅｂサーバを運用することを想定している。カード製造者（Ｐ１）は、カードの製造からカードに必要なデータを設定して市場で使うことができるカードの有効化までを行うものであり、アプリ開発者（Ｐ２）に開発環境の貸し出しやアプリケーションの署名付けを行うことを想定している。ここで考えたプレイヤーモデルはあくまで一例に過ぎず、一プレイヤーがいくつかのプレイヤーを兼任する場合や、もしくは一プレイヤーの処理がより細分化される場合も、本特許の範疇に含まれる。例えば、カード製造者（Ｐ１）は、カードの製造のみを行い、カードの有効化および開発環境の貸し出し、アプリケーションの署名付けを別のプレイヤーが行う場合もあり、前記では説明を省略したカード販売者が店頭でカードの有効化を行う場合やサービス提供者が作成したデータをカード製造者が受けてカードに設定する場合も想定できる。尚、サービス提供者（Ｐ３）やカード製造者（Ｐ１）がアプリ開発者（Ｐ２）を兼任する場合も考えられる。

【００２５】

次に図５、図６、図７Ａ、図７Ｂ、図７Ｃを使って、各プレイヤーが行う処理を説明する。まず、カード製造者（Ｐ１）は、カード製造者のＲＳＡ鍵ペアを事前に生成する（Ｓ０１）。そして、生成した鍵のうち、製造者のＲＳＡ公開鍵（Ｍ０１）をカードに設定する（Ｓ０２）。公開鍵の対称となる秘密鍵（Ｍ０２）は、アプリ開発者が作成したアプリケーションに対する署名付けを行う際に用いる。また、製造するカードに格納するＲＳＡ鍵ペアを事前に生成する（Ｓ０３）。生成した鍵のうち、カードのＲＳＡ公開鍵（Ｍ０３）は、アプリ開発者、サービス提供者に配布される（Ｓ０４）。カードのＲＳＡ秘密鍵（Ｍ０４）はカードに格納される（Ｓ０５）。尚、カード製造者が生成する鍵（Ｍ０１、Ｍ

０２、Ｍ０３、Ｍ０４）はＲＳＡ鍵に限定されるものではなく、楕円暗号方式、ＤＨ鍵配送方式、エルガマル暗号方式など他の公開鍵暗号方式を利用しても構わない。尚、同様にＲＳＡの鍵長も１０２４ｂｉｔ、２０４８ｂｉｔに限定されるわけではなく、カード運用のセキュリティポリシーに則って自由に変更しても構わない。

【００２６】

署名付けは、アプリ開発者による申請（アプリケーション（Ａ０２）の送付）（Ｓ０６）によって行われる。カード製造者は、提出されたアプリケーションの動作内容を確認し、問題がなければ、提出されたアプリケーションのハッシュデータを作成しパディング処理を施し、それに対してカード製造者のＲＳＡ秘密鍵を使って、署名を生成する（Ｓ０７）。生成された署名（Ａ０５）は、アプリ開発者に提供される（Ｓ０８）。尚、署名付けは、カード製造者のセキュリティポリシーによっては、アプリ開発者、またはサービス提供者に任される場合がある。その場合、カード製造者は署名付けを行うためのＲＳＡ秘密鍵（Ｍ０２）を提供するか、またはＲＳＡ秘密鍵（Ｍ０２）を使って、新規に生成した公開鍵ペア、もしくはアプリ開発者、またはサービス提供者が生成した公開鍵ペアに対して、証明書を生成する。その証明書をカードに送信し、カードがその証明書の有効性を確認できれば、一時的に証明書に記載された公開鍵をＲＳＡ公開鍵（Ｍ０１）の代わりに署名検証処理に用いることができる。

【００２７】

アプリ開発者（Ｐ２）は、カード製造者（Ｐ１）から事前にカード（１００）に対応した開発環境とカードの公開鍵（Ｍ０３）を受託している。その開発環境を利用して、アプリ開発者はカードに対応したアプリケーション開発を行う（Ｓ０９）。完成したアプリケーション（Ａ０２）は、カード製造者（Ｐ１）に送信され（Ｓ０６）、署名（Ａ０５）を付与してもらう（Ｓ０８）。アプリ開発者は、作成したアプリケーションをサービス提供者（Ｐ３）に譲渡するが、その際に暗号化して渡す。暗号化する理由は、カード製造者が配布した開発環境を用いて開発できるのはアプリ開発者だけであり、それを使って開発したアプリケーション内容をサービス提供者が閲覧可能であるのは秘情報の流出になるからである。プレイヤーをまたいで秘情報の共有をしている時に情報が漏洩した際、どちらの責任で漏洩が発生したかは曖昧になってしまい、最悪の場合切り分けができない事態に陥ることが考えられる。それに対して、本実施の形態では、まず、アプリ開発者が、独自に作成した鍵（Ａ０１）（以下、アプリケーション暗号鍵と呼ぶ）でアプリケーション（Ａ０２）を暗号化し、暗号化したアプリケーション（Ａ０３）を生成する（Ｓ１０）。またアプリケーション暗号鍵（Ａ０１）を事前に配布されたカードの公開鍵（Ｍ０３）で暗号化し、暗号化された鍵（Ａ０４）を生成する（Ｓ１１）。サービス提供者（Ｐ３）には、暗号化したアプリケーション（Ａ０３）と暗号化された鍵（Ａ０４）とアプリケーションの署名（Ａ０５）を譲渡する（Ｓ１２）。サービス提供者（Ｐ３）は、受け取ったどちらの暗号データ（Ａ０３、Ａ０４）も復号することができない。

【００２８】

サービス提供者（Ｐ３）は、アプリ開発者（Ｐ２）から受け取ったアプリケーションを個別にカスタマイズするためのデータ（以下、個別データとする）を作成する（図６：Ｓ２０）。尚、作成するすべてのデータをアプリケーション１つ１つ個別にデータを変更するか、あるデータは共通化するか等については、サービスの運用ポリシーに因るところであり、考慮しない。サービス提供者（Ｐ３）が個別データ（Ｈ０２）を作成する場合には、別途アプリ開発者（Ｐ２）からアプリケーションの外部仕様を受け取る必要がある。例として、最初の１００バイトは識別情報、次の１０００バイトは自己証明書データ、次の１０００バイトはルート証明書データ、次の３０００バイトはファイルシステム情報としてアプリケーションから参照するという外部仕様とする（図８を参照）。データの開始地点には長さを示す情報を設定し、その領域のどこまでを有効なデータとしてアプリケーションが参照するべきかを示す。

【００２９】

サービス提供者（Ｐ３）は、アプリ開発者（Ｐ２）と同様に、作成した個別データ（Ｈ

０２）を独自に作成した鍵（Ｈ０１）（以下、個別データ暗号鍵という）で暗号化し（Ｓ２１）する。そして暗号化した個別データ（Ｈ０３）を作成し、個別データ暗号鍵（Ｈ０１）を事前にカード製造者（Ｐ１）から配布されているカードの公開鍵（Ｍ０３）で暗号化し（Ｓ２２）、暗号化した個別データ暗号鍵（Ｈ０４）を作成する。この際、作成した個別データ（Ｈ０２）に対してハッシュ（Ｈ０５）を生成する（Ｓ２３）。

【００３０】

サービス提供者（Ｐ３）は、生成したハッシュ（Ｈ０５）と、アプリ開発者から受け取った署名（Ａ０５）と、その他にサービス提供者（Ｐ３）が作成する（Ｓ２４）アプリケーションを識別するための識別情報や著作権情報などのアプリケーション管理情報やサービス提供者情報（以下、共通データ（Ｈ０６）という）と一緒に管理する。これを以下、管理データ（Ｈ０７）という。図９に管理データ（Ｈ０７）のフォーマット例を記載する。サービス提供者（Ｐ３）は、管理データ（Ｈ０７）を独自に生成した鍵（以下、管理データ暗号鍵（Ｈ０８）という）で暗号化し、暗号化した管理データ（Ｈ０９）を作成し（Ｓ２５）、管理データ暗号鍵（Ｈ０８）を事前にカード製造者（Ｐ１）から配布されているカードの公開鍵（Ｍ０３）で暗号化し、暗号化した管理データ暗号鍵（Ｈ１０）を作成する（Ｓ２６）。

【００３１】

個別データ暗号鍵（Ｈ０１）と管理データ暗号鍵（Ｈ０８）はサービス提供者自身が作成し管理するものなので、一緒でも、別途用意しても良い。別にした場合、管理の手間が増えるが、鍵漏洩におけるセキュリティ対策はより強固になるので、本実施の形態では別に用意した場合について記載する。

【００３２】

サービス提供者（Ｐ３）は、アプリ提供者（Ｐ２）から受け取った暗号化されたアプリケーション（Ａ０３）とアプリケーション暗号鍵を暗号化したデータ（Ａ０４）、暗号化した個別データ（Ｈ０３）と個別データ暗号鍵を暗号化したデータ（Ｈ０４）、暗号化した管理データ（Ｈ０９）と管理データ暗号鍵（Ｈ０８）を暗号化したデータ（Ｈ１０）をサーバ運用者（Ｐ４）に配布する（Ｓ２７）。サーバ運用者（Ｐ４）は、受け取ったすべての暗号データ（Ａ０３、Ａ０４、Ｈ０３、Ｈ０４、Ｈ０９、Ｈ１０）を復号することができない。

【００３３】

本実施の形態では、アプリケーション暗号鍵（Ａ０１）、個別データ暗号鍵（Ｈ０１）、管理データ暗号鍵（Ｈ０８）の３つの鍵に用いている暗号アルゴリズムを共通鍵暗号方式とする。ここではデータの暗復号にかかる時間や鍵長を考慮して共通鍵を選択しており、共通鍵に限定していた仕様ではなく、公開鍵暗号方式を用いてもかまわない。尚、本実施の形態では共通鍵暗号方式のＡＥＳを用いているが、何ら限定しているわけではなく、ＤＥＳやＴ－ＤＥＳ、ＭＩＳＴＹ、Ｃａｍｅｌｌｉａ、ＲＣ６など知られている共通鍵暗号方式でもかまわない。尚、カードが暗号方式に対応するのであれば、今後公表される共通鍵暗号方式にも対応することは可能である。

【００３４】

サーバ運用者（Ｐ４）は、受け取ったデータ（Ａ０３），（Ａ０４），（Ｈ０３），（Ｈ０４），（Ｈ０９），（Ｈ１０）をサーバ（３００）の記憶手段（３００３）に登録する（図７Ａ：Ｓ３０）。登録する際、サービス提供者（Ｐ３）から受け取ったデータが、どのカードの、どのバージョンに対応したものであるかを知る必要がある。前記情報はカードの識別情報であり、外部機器（２００）がカード（１００）から取得し、サーバ（３００）に対してデータ要求する際に一緒にサーバ（３００）に送信される情報である。サーバ（３００）は前記識別情報に対応する複数の暗号データを外部機器に送信するために事前に知る必要があり、これらのデータは、サービス提供者、もしくはアプリ開発者から別途通知される情報である。カードが出力するバージョン情報とそれに対応したサーバ上のデータ管理形式の例を図１０に示す。カードが前記の識別情報を出力するためにコマンドが規定されており、そのコマンドに対応したレスポンスデータで外部機器に通知される

。コマンドは、カードに搭載されているアプリケーションや通信レイヤーで規定されたネゴシエーション時にやりとりされるものである。尚、1枚の１バージョンのカードだけを運用する場合には、カードの種別やバージョン情報は必要ない。

【００３５】

サーバ（３００）が外部機器（２００）からのデータ要求に対して、データを送信する順番は、管理データ暗号鍵、共通データ、個別データ暗号鍵、個別データ、アプリケーション暗号鍵、アプリケーションの順とする。尚、前記の順番は、カード内でできるだけデータを一時的に保持せず、順次処理するために行っているものであり、カードに十分な一時記憶領域が存在する場合は、これに限定するものではない。

【００３６】

カード（１００）と外部機器（２００）間の通信フローを図１２に示す。まず、通信手段（１００１）は管理データ暗号鍵を暗号化したデータ（Ｈ１０）を外部機器（２００）経由で受信し（Ｃ０１）、コマンド解釈手段（１００２）に渡す。コマンド解釈手段（１００２）は、前記データに付与されているコマンドをチェックし、そのコマンドが何を示しているか、どの目的で使われているのかを解釈する。本実施の形態では、コマンドの内容は、カードへのアプリケーションのインストールと想定して以下の動作を記載する。コマンド解釈手段（１００２）は、数値計算手段（１００４）にアプリケーションのインストールであることを通知し、受信データを渡す。数値計算手段（１００４）は、記憶手段（１００５）が保持するカードＲＳＡ秘密鍵（Ｍ０４）を記憶制御手段（１００３）経由で取得し、受信データを暗復号手段（１００６）で復号する（Ｓ３１）。数値計算手段（１００４）は復号した管理データ暗号鍵（Ｈ０８）を記憶制御手段（１００３）を経由して記憶手段（１００５）で保持する。前記の処理が問題なく行えれば、外部機器（２００）に対して正常終了という意味合いを持つコードを出力する（Ｃ０２）。

【００３７】

次に通信手段（１００１）は暗号化された管理データ（Ｈ０９）を外部機器経由で受信する（Ｃ０３）。数値計算手段（１００４）は、前記の管理データ暗号鍵（Ｈ０８）を用いて、暗復号手段（１００６）で暗号化された管理データ（Ｈ０９）の復号を行う（Ｓ３２）。復号した管理データ（Ｈ０７）は、予め規定してあるフォーマット（図９）に従っているので、数値計算手段（１００４）は前記フォーマットに従って、データを読み出す。管理データ（Ｈ０７）に含まれる共通データ（Ｈ０６）内にあるアプリケーションを識別するためのアプリケーション識別子（Ｌ０１）は、カード内の記憶手段（１００５）に格納されている管理状態（Ｌ０２）を読み出すために用いる。アプリケーション識別子（Ｌ０１）とアプリケーションの管理状態（Ｌ０２）は対で管理されている。

【００３８】

管理状態（Ｌ０２）は、アプリケーション（Ａ０２）と個別データ（Ｈ０２）の両方がインストールされているＩｎｓｔａｌｌｅｄ状態（Ｊ０４）と、アプリケーションだけがインストールされている個別データｄｅｌｅｔｅｄ状態（Ｊ０２）と、個別データだけがインストールされているアプリケーションｄｅｌｅｔｅｄ状態（Ｊ０３）が存在し、何もインストールされていない状態（Ｊ０１）を合わせて、４状態を管理状態（Ｌ０２）から知る事ができる。アプリケーション識別子（Ｌ０１）と管理状態（Ｌ０２）の対応表を示したのが、図１７である。また、それぞれの管理状態は、外部からの操作によって、遷移することが可能である（図１８）。インストールされていない状態（Ｊ０１）から正常にインストール処理（Ｊ０５）が完了すると、Ｉｎｓｔａｌｌｅｄ状態（Ｊ０４）になる。Ｉｎｓｔａｌｌｅｄ状態（Ｊ０４）から個別データＤｅｌｅｔｅ処理（Ｊ０９）を行うと、個別データＤｅｌｅｔｅｄ状態（Ｊ０２）になる。Ｉｎｓｔａｌｌｅｄ状態（Ｊ０４）からアプリケーションＤｅｌｅｔｅ処理（Ｊ１０）を行うと、アプリケーションＤｅｌｅｔｅｄ状態（Ｊ０３）になる。また、個別データＤｅｌｅｔｅｄ状態（Ｊ０２）から個別データだけをインストールする処理（Ｊ０６）を行うと、Ｉｎｓｔａｌｌｅｄ状態（Ｊ０４）に戻る。アプリケーションＤｅｌｅｔｅｄ状態（Ｊ０３）からアプリケーションだけをインストールする処理（Ｊ０７）を行っても、Ｉｎｓｔａｌｌｅｄ状態（Ｊ０４）に戻

る。それぞれの状態（Ｊ０２、Ｊ０３、Ｊ０４）でＡｌｌ　Ｄｅｌｅｔｅ処理（Ｊ０８）を行うと、未インストール状態（Ｊ０１）になる。この場合、一度インストールしたアプリケーション識別子を消さないで、前記の未インストール状態として管理しても、アプリケーション識別子と状態を合わせて、図１７の対応表から削除しても何ら影響はない。そのため、対象となるアプリケーション識別子が記憶手段内にない場合、もしくはアプリケーション識別子があっても未インストール状態（Ｊ０１）の場合、まだインストールされていないアプリケーションとなる。

【００３９】

アプリケーション識別子（Ｌ０１）を使って、管理状態（Ｌ０２）を取得する（Ｓ３３）。管理状態（Ｌ０２）によって、受信した管理データから必要とするデータが変わってくる。つまり、未インストール状態（Ｊ０１）であれば、すべての管理データが必要であるが、個別データＤｅｌｅｔｅｄ状態（Ｊ０２）であれば、管理データ(Ｈ０７)の中からと個別データのハッシュ（Ｈ０５）だけが必要になる。アプリケーションＤｅｌｅｔｅｄ状態（Ｊ０３）であれば、管理データ（Ｈ０７）の中から署名（Ａ０５）だけが必要になる。管理データの中に不要なデータが含まれている場合、無視して処理を行わない。そのため、最初に送付する時点で、無視されるデータは送信しなくても、何ら問題ない。逆に、必要なデータが含まれていない場合は、エラーとなる。その場合、数値計算手段（１００４）は、外部機器（２００）に結果を出力する（Ｃ０４）際、正常終了ではなく、フォーマット異常により終了したというエラーコードを出力する。問題なければ、管理状態（Ｌ０２）よって必要な共通データ（Ｈ０６）内のデータを記憶制御手段（１００３）経由で記憶手段（１００５）に仮格納する（Ｓ３４）。尚、上記のエラーに限定したものではなく、異常動作をした場合は、事前に外部と取り交わされたその旨を示すコードを出力する。本実施の形態では、未インストール状態（Ｊ０１）であり、すべての管理データが必要な場合とする。

【００４０】

状態によって、署名(Ａ０５)が必須のデータとなっている場合、署名に対して事前に復号処理を行う。数値計算手段（１００４）は、製造者の公開鍵（Ｍ０１）を使って署名（Ａ０５）を暗復号手段（１００６）で復号する。復号したデータに対して、適切なパディング処理をしているか確認する。適切なパディング処理であることを確認できた場合、少なくとも適切な秘密鍵で作成された署名であることが確認できたので、対象となるハッシュ（Ｈ１１）を取得する(Ｓ３４－１)。

【００４１】

適切なパディングが確認できなかった場合は、エラーとなる。問題が無かった場合には、正常であることを外部端末（２００）に通知する（Ｃ０４）。正常終了であることを通知するだけではなく、次に個別データを送る必要があることを外部端末（２００）に伝える方が処理を効率的にできるため好ましい。

【００４２】

アプリケーションの送付前に署名の復号を行う事により、署名と比べて大規模なアプリケーション（Ａ０２）が送信される前に、エラーのチェックができ、エラーの場合に無駄になる通信をなくすことができる。また、署名データが２０４８ｂｉｔのＲＳＡで作成されている場合、署名データサイズは２５６バイトになるが、ハッシュにＳＨＡ－１を利用している場合復号した後のハッシュデータだけだと２０バイトになり、ハッシュだけを取りだしておく方がカード内で必要とするメモリを節約する事ができる。

【００４３】

次に、通信手段（１００１）は個別データ暗号鍵を暗号化したデータ（Ｈ０４）を外部機器（２００）経由で受信し（図７Ｂ：Ｃ０５）、数値計算手段（１００４）に渡す。数値計算手段（１００４）は、記憶手段（１００５）で保持するカードＲＳＡ秘密鍵（Ｍ０４）を使って、暗復号手段（１００６）で復号する（Ｓ３５）。復号した個別データ暗号鍵（Ｈ０１）をカード内の記憶手段（１００５）で保持する。次に通信手段（１００１）は暗号化された個別データ（Ｈ０３）を外部機器（２００）経由で受信する（Ｃ０７）。

通信手段（１００１）は、前記データを数値計算手段（１００４）に渡す。数値計算手段（１００４）は、前記の個別データ暗号鍵（Ｈ０３）を用いて、暗号化された個別データの復号を暗復号手段（１００６）で行う（Ｓ３６）。個別データ（Ｈ０２）の内容は、後述のアプリケーション（Ａ０２）が解釈するものであり、カードが解釈する必要はない。数値計算手段（１００４）は、復号した個別データ（Ｈ０２）のハッシュをハッシュ生成手段（１００９）で生成し（Ｓ３７）、管理データに含まれていた個別データのハッシュ（Ｈ０５）と同じであるかを照合手段（１００７）を用いて確認する（Ｓ３８）。同じであれば、数値計算手段（１００４）は、個別データを記憶制御手段（１００３）経由で記憶手段（１００５）に仮格納する（Ｓ３９）。異なる場合、数値計算手段（１００４）はインストール処理を中止する（Ｓ４０）。外部機器に結果を出力する（Ｃ０８）際、正常終了ではなく、ハッシュが異なるという旨を示すエラーコードを出力する。問題が無かった場合には、正常であることを外部端末（２００）に通知する（Ｃ０８）。正常終了であることを通知するだけではなく、次にアプリケーション（Ａ０２）を送る必要があることを外部端末（２００）に伝える方が処理を効率的にできるため好ましい。

【００４４】

次に、通信手段（１００１）は、アプリケーション暗号鍵を暗号化したデータ（Ａ０４）を外部機器（２００）経由で受信し（図７Ｃ：Ｃ０９）、数値計算手段（１００４）に渡す。数値計算手段（１００４）は、記憶手段（１００５）で保持するカードＲＳＡ秘密鍵（ＭＯ４）を使って、暗復号手段（１００６）で復号する（Ｓ４１）。復号したアプリケーション暗号鍵（Ａ０１）をカード内の記憶手段（１００５）で保持する。次に通信手段（１００１）は暗号化されたアプリケーション（Ａ０３）を外部機器（２００）経由で受信する（Ｃ１１）。通信手段（１００１）は、前記データを数値計算手段（１００４）に渡す。数値計算手段（１００４）は、前記のアプリケーション暗号鍵（Ａ０１）を用いて、暗号化されたアプリケーションの復号を暗復号手段（１００６）で行う（Ｓ４２）。アプリケーションは、事前に製造者によって動作確認されているという前提があるので、カードで新たに前記アプリケーションの動作を検証する必要はない。数値計算手段（１００４）は、アプリケーションを記憶制御手段（１００３）経由で記憶手段（１００５）に仮格納する（Ｓ４３）。カードは復号したアプリケーション（Ａ０２）のハッシュをハッシュ生成手段（１００９）で生成する（Ｓ４４）。署名から取得したハッシュ（Ｈ１１）と、前記生成したアプリケーションのハッシュを照合手段（１００７）で照合する（Ｓ４５）。同じであれば、数値計算手段（１００４）は、アプリケーション（Ａ０２）を記憶手段（１００５）に格納する。異なる場合、数値計算手段（１００４）はインストール処理を中止する（Ｓ４６）。数値計算手段（１００４）は、外部機器（２００）に結果を出力する（Ｃ１０）際、正常終了ではなく、署名が異なるという旨を示すエラーコードを出力する。同じである場合、数値計算手段（１００４）はすべてのデータが正常であることを確認し、インストール処理を終了する。数値計算手段（１００４）は、署名が正当である場合、署名と一緒に暗号化されていた個別データのハッシュ、共通データを正当であると判断し、該当アプリケーションに関連する共通データ、個別データ、アプリケーションをカード内で動作可能な状態として、Ｉｎｓｔａｌｌｅｄ状態（Ｊ０４）に変更する。具体的には、外部機器（２００）からの要求によって、数値計算手段（１００４）が記憶制御手段（１００３）経由で記憶手段から前記管理状態（Ｌ０２）を確認し、アプリケーションとして動作可能であるＩｎｓｔａｌｌｅｄ状態（Ｊ０４）と示されていれば、アプリケーションを呼び出し、コマンド解釈手段（１００２）から送られてくるコマンドをアプリケーションに渡すように動作することになる。

【００４５】

本発明の不揮発性記憶装置は、アプリケーション識別子（Ｌ０１)とその管理状態（Ｌ０２）をカード内で管理することにより、送信されてきたデータから必要なデータを取捨選択することができる。そのため、すべての処理を一律行うのではなく、必要な処理だけを行うため、インストール処理を効率的に行う事が出来る。

【００４６】

取捨選択することにより、カード内のリソースの消費を最小限に抑えることができ、かつ処理時間を最小化することが出来る。

【００４７】

また、管理状態（Ｌ０２）によって署名（Ａ０５）を取得し処理できるため、事前に署名対象データを送信してよいかが分かり、カードは外部機器（２００）にその情報を通知するため、外部機器（２００）はカードに不要なデータを送ることがなくなり、無駄な通信を省く事が出来る。

【００４８】

次に、上記データの更新を行う手順を説明する。相互認証をしない場合、サーバ、カードお互いに相手のなりすましを防ぐ方法がないため、サーバはどのカードにアプリケーションがインストールされたのか管理することができず、カードは、どのサービス提供者のアプリケーションをインストールしたのか分からない。そのため、カード上のアプリケーションを更新する場合、同じサービス提供者から配布されたアプリケーションであるかをカードが確認することができない。そのため、一旦アプリケーションを削除して、再度インストールすることはできるが、更新時に最初のアプリケーションとの関連性が立証できないため、一部のデータをカードに残しておき、データ処理部だけを変更するといった更新処理を実現することが出来ない課題がある。そこで、前述のインストール方法を用いてインストールしたアプリケーションを更新する際、外部認証無しで適切なサービス提供者からのアプリケーションの更新であることを検証し、更新処理を実現する方法を以下に説明する。

【００４９】

データには前述したように、管理データ、個別データ、アプリケーションの３つが存在する。管理データは、個別データとアプリケーションに関連したデータを格納するため必ず存在するが、個別データ、もしくはアプリケーションだけを更新する場合が存在する。

【００５０】

個別データだけを更新する場合は、管理データの中に、個別データのハッシュ（Ｈ０５）と、更新するアプリケーション識別子（Ｌ０１）を共通データ（Ｈ０６）に格納して暗号化し、暗号化した個別データと一緒に送信する。アプリケーションだけを更新する場合、管理データの中に、アプリケーションの署名と、更新するアプリケーション識別子（Ｌ０１）を共通データ（Ｈ０６）に格納して暗号化し、暗号化したアプリケーションと一緒に送信する。

【００５１】

前記の通り、本発明の不揮発性記憶装置は、個別データだけの更新の場合、署名（Ａ０５）が含まれておらず、カードは信頼性を確立できない。そのため、更新を行う場合に備え、最初にインストールする際に、個別データ暗号鍵を一緒に保存しておき、更新時には公開鍵で暗号化された鍵データから鍵を復号するのではなく、予めカード内で保持している個別データ暗号鍵を利用して復号を行う。サービス提供者しか知りえない個別データ暗号鍵を使うことができ、復号したデータのハッシュが管理データで送られてきたハッシュと一致するということは、最初にインストールしたサービス提供者（Ｐ３）、またはそれに準ずる情報を持つ代理のサービス提供者であることが分かる。この方法を使うことにより、カードによる外部認証をせず、サーバによるアプリケーション管理をすることなく、カードだけで最初のインストール時と同一のサービス提供者だけを更新可能なプレイヤーに制限できる。

【００５２】

アプリケーションについても、上記の方法を利用することで、最初にインストールした時のアプリ開発者（Ｐ２）だけに制限した更新処理にすることができる。アプリケーションには署名（Ａ０５）が付いているため、アプリケーション自体を改ざんすることができないが、更新時には、個別データ（Ｈ０２）との関連性が見出せないため、すでにカードにインストール済みの他の個別データを持つアプリケーションに対して、アプリケーション部分だけをすり替えて他のアプリケーションの個別データを参照することができてしま

う。そのため、上記のような対策により更新を行うものに対して制限を付けることが重要である。

【００５３】

カード（１００）と外部機器（２００）間の通信フローを図１４で示し、図１５Ａ、図１５Ｂを使って、各プレイヤーが行う処理フローを説明する。アプリ開発者が再度アプリケーションを開発し、サービス提供者を通じてサーバ運用者（Ｐ０４）に納入され、サーバ運用者が暗号化されたアプリケーションを登録する部分について、新規インストールでのデータ準備と比較して、サービス提供者が個別データを生成しない点と個別データのハッシュを管理データに含めない点が異なるだけなので、フローについては割愛する。

【００５４】

サーバ運用者は、サービス提供者から納入された暗号化したアプリケーション（Ａ０３）、暗号化した管理データ（Ｈ０９）、暗号化した暗号用鍵（Ｈ１０）を更新用アプリケーションとして、サーバに登録する（Ｚ００）。外部機器からの要求に対応するために、更新用アプリケーションのバージョン情報や説明などを付与して外部から明示的に分かるようにしておく。または外部機器(２００)からの更新要求に予めなんらかの情報が含まれている場合は、サーバ(３００)は前記情報に対応して、アプリケーションを配信することになる。その際、外部機器(２００)から送信される前記情報には、アプリケーションの識別情報やカードに格納されている現在のアプリケーションのバージョン情報、カード識別情報などがある。

【００５５】

まず、通信手段（１００１）は管理データ暗号鍵を暗号化したデータ（Ｈ１０）を外部機器（２００）経由で受信し（Ｚ０１）、コマンド解釈手段（１００２）に渡す。コマンド解釈手段（１００２）は、前記データに付与されているコマンドをチェックし、そのコマンドが何を示しているか、どの目的で使われているのかを解釈する。コマンドの内容は、アプリケーションの更新処理と想定して以下の動作を記載する。更新作業を判別する部分については、コマンド解釈手段で更新処理であるかを確認する方法と、インストール処理として最初は処理し、アプリケーションの識別子に対応するアプリケーションの状態を確認することで、次に行う処理を更新処理としてカードが自動的に認識する方法がある。本実施の形態では、コマンドによる解釈を行い、処理内容を確定する場合を記載する。

【００５６】

コマンド解釈手段（１００２）は、数値計算手段（１００４）にアプリケーションの更新処理であることを通知し、受信データを渡す。数値計算手段（１００４）は、記憶手段（１００５）が保持するカードＲＳＡ秘密鍵（Ｍ０４）を記憶制御手段（１００３）経由で取得し、受信データを暗復号手段（１００６）で復号する。数値計算手段（１００４）は復号した管理データ暗号鍵（Ｈ０８）を記憶制御手段（１００３）経由で記憶手段（１００５）に保持する（Ｓ５１）。前述の処理が問題なく行えれば、外部機器（２００）に対して正常終了という意味合いを持つコードを出力する（Ｚ０２）。

【００５７】

次に通信手段（１００１）は暗号化された管理データ（Ｈ０９）を外部機器経由で受信する（Ｚ０３）。数値計算手段（１００４）は、前述の管理データ暗号鍵（Ｈ０８）を用いて、暗復号手段（１００６）で暗号化された管理データ（Ｈ０９）の復号を行う（Ｓ５２）。復号した管理データ（Ｈ０７）は、予め規定してあるフォーマット（図９）に従っているので、数値計算手段（１００４）は前記フォーマットに従って、データを読み出す。更新の場合、すべてのデータが埋められているわけではなく、更新時に必要な情報が含まれていればよい。本実施の形態の場合は、アプリケーションの更新にあたるため、個別データのバージョン情報、個別データのサイズ、個別データのハッシュが記載されていなくて良く、アプリケーション識別子長、アプリケーション識別子（Ｌ０１）、アプリケーションのバージョン情報、アプリケーションサイズ、アプリケーションの署名（Ａ０５）が必須になる。アプリケーションを識別するための情報は、更新するアプリケーションがカード内にあるかを調べるために用いる（Ｓ５３）。また更新対象のアプリケーションが

更新可能な状態を保持しているかを、記憶手段で保持しているアプリケーション識別子とその管理状態（Ｌ０２）の対応表（図１７）から確認する。同じ値を持つ識別子がない場合は、何も登録されていないため新規インストール処理として扱われることになるが、送信するデータには、新規インストール処理で必要なデータを含んでいる必要がある。

【００５８】

すでにＩｎｓｔａｌｌｅｄ状態（Ｊ０４）の場合は、数値計算手段はインストール処理を中止する。数値計算手段は、外部機器に結果を出力する（Ｚ０４）際、正常終了ではなく、インストール済みであることを示すエラーコードを出力する。アプリケーションＤｅｌｅｔｅｄ状態（Ｊ０３）であれば、共通データを記憶制御手段（１００３）経由で記憶手段（１００５）に仮格納する（Ｓ５４）。

【００５９】

アプリケーションＤｅｌｅｔｅｄ状態（Ｊ０３）は、署名(Ａ０５)が必須のデータとなっているため、署名に対して事前に復号処理を行う。数値計算手段（１００４）は、製造者の公開鍵（Ｍ０１）を使って署名（Ａ０５）を暗復号手段（１００６）で復号する。復号したデータに対して、適切なパディング処理をしているか確認する。適切なパディング処理であることを確認できた場合、少なくとも適切な秘密鍵で作成された署名であることが確認できたので、対象となるハッシュ（Ｈ１１）を取得する(Ｓ５４－１)。

【００６０】

尚、上記のエラーに限定したものではなく、異常動作をした場合は、事前に外部と取り交わされたその旨を示すコードを出力する。問題が無かった場合には、正常であることを外部端末（２００）に通知する（Ｚ０４）。正常終了であることを通知するだけではなく、次にアプリケーション（Ａ０２）を送る必要があることを外部端末（２００）に伝える方が処理を効率的にできるため好ましい。

【００６１】

次に通信手段（１００１）は暗号化されたアプリケーション（Ａ０３）を外部機器（２００）経由で受信する（図１５Ｂ：Ｚ０５）。通信手段（１００１）は、前記データを数値計算手段（１００４）に渡す。数値計算手段（１００４）は、更新対象のアプリケーション識別子（Ｌ０１）と管理状態がアプリケーションＤｅｌｅｔｅｄ状態（Ｊ０３）という情報から、最初のデータ格納時にデータを復号したアプリケーション暗号鍵（Ａ０１）を記憶手段（１００５）から取得する（Ｓ５５）。前記のアプリケーション暗号鍵（Ａ０１）を用いて、暗号化されたアプリケーションの復号を暗復号手段（１００６）で行う（Ｓ５６）。アプリケーションは、事前に製造者によって動作確認されているという前提があるので、カードで新たに前記アプリケーションの動作を検証する必要はない。数値計算手段（１００４）は、アプリケーションを記憶制御手段（１００３）経由で記憶手段（１００５）に仮格納する（Ｓ５７）。カードは復号したアプリケーション（Ａ０２）のハッシュをハッシュ生成手段（１００９）で生成する（Ｓ５８）。署名から取得したハッシュ（Ｈ１１）と、前記生成したアプリケーションのハッシュを照合手段（１００７）で照合する（Ｓ５９）。同じであれば、数値計算手段（１００４）は、アプリケーション（Ａ０２）を記憶手段（１００５）に格納する。異なる場合、数値計算手段（１００４）はインストール処理を中止する（Ｓ６０）。数値計算手段（１００４）は、外部機器（２００）に結果を出力する（Ｚ０６）際、正常終了ではなく、署名が異なるという旨を示すエラーコードを出力する。同じである場合、数値計算手段（１００４）はすべてのデータが正常であることを確認し、インストール処理を終了する。数値計算手段（１００４）は、署名が正当である場合、署名と一緒に暗号化されていた共通データを正当であると判断し、すでにインストールされている個別データと合わせて、該当アプリケーションに関連する共通データ、アプリケーションをカード内で動作可能なＩｎｓｔａｌｌｅｄ状態（Ｊ０４）に変更する。

【００６２】

また、前記の説明では、外部機器（２００）とカード（１００）間の通信路について詳細に記載していないが、高速に記憶部にアクセスできるが事前に領域指定ができないとい

けない通信路（以下、高速通信路と呼ぶ）と、それより速度は劣るが領域指定を内部で解釈して行ってくれる通信路（以下、低速通信路と呼ぶ）の２系統を保持するカード（図１１）がある。

【００６３】

カードが複数の通信方式に対応している場合、その処理内容によって、インストール途中で方式の切り替えをしたい場合がある。サーバ上のデータが暗号化されている場合、サーバ、外部機器は、その内容を見ることができず、切り替えるタイミングを把握することができない。また、サーバが事前に切り替えるタイミングを別の平文情報として持っていても、外部機器経由で切り替えを指定した場合に、外部機器を認証ができていないカードは、そのコマンドを信用することができない課題がある。そこで、前述のダウンロード、インストール方法を用いても、カードがもつ複数の通信方法を適切に動的に切り替える方法を提供する。

【００６４】

カード（１００）が内容を解釈してデータを格納する管理データ（Ｈ０７）は、低速通信路を使ってデータを書き込む必要があるが、カードが内容を解釈しない個別データ（Ｈ０２）、アプリケーションデータ（Ａ０２）は、高速通信路を使ってデータを書き込むことができる。特に個別データ、アプリケーションデータが大容量である場合は、その効果は大きく、インストール時間の短縮を図ることができる。また、低速通信路と高速通信路に分けた場合、そのデータが正常な外部機器から送られてきたかが不確かになるが、その部分は前記署名データ（Ａ０５）と前記ハッシュ（Ｈ０５）が２つの通信路の関連性を保障できるため問題ない。

【００６５】

カードが２系統通信路を保持している場合のカード（１００）と外部機器（２００）間の通信フローを図１３で示し、図１６Ａ、図１６Ｂ、図１６Ｃ、図１６Ｄを使って、各プレイヤーが行う処理フローを説明する。

【００６６】

まず、通信手段（１００１）は管理データ暗号鍵を暗号化したデータ（Ｈ１０）を外部機器（２００）経由で受信し（Ｃ０１）、コマンド解釈手段（１００２）に渡す。コマンド解釈手段は、前記データに付与されているコマンドをチェックし、そのコマンドが何を示しているか、どの目的で使われているのかを解釈する。本実施の形態では、コマンドの内容は、カードへのアプリケーションのインストールと想定して以下の動作を記載する。コマンド解釈手段（１００２）は、数値計算手段（１００４）にアプリケーションのインストールであることを通知し、受信データを渡す。数値計算手段（１００４）は、記憶手段（１００５）が保持するカードＲＳＡ秘密鍵（Ｍ０４）を記憶制御手段（１００３）経由で取得し、受信データを暗復号手段（１００６）で復号する（Ｓ３１）。数値計算手段（１００４）は復号した管理データ暗号鍵（Ｈ０８）を記憶制御手段（１００３）を経由して記憶手段（１００５）で保持する。前記の処理が問題なく行えれば、外部機器（２００）に対して正常終了という意味合いを持つコードを出力する（Ｃ０２）。

【００６７】

次に通信手段（１００１）は暗号化された管理データ（Ｈ０９）を外部機器（２００）経由で受信する（Ｃ０３）。数値計算手段（１００４）は、前記の管理データ暗号鍵（Ｈ０８）を用いて、暗復号手段（１００６）で暗号化された管理データ（Ｈ０９）の復号を行う（Ｓ３２）。復号した管理データ（Ｈ０７）は、予め規定してあるフォーマット（図９）に従っているので、数値計算手段（１００４）は前記フォーマットに従って、データを読み出す。管理データ（Ｈ０７）に含まれる共通データ（Ｈ０６）内にあるアプリケーションを識別するためのアプリケーション識別子（Ｌ０１）は、カード内の記憶手段（１００５）に格納されている管理状態（Ｌ０２）を読み出すために用いる。アプリケーション識別子（Ｌ０１）とアプリケーションの管理状態（Ｌ０２）は対で管理されている。

【００６８】

アプリケーション識別子（Ｌ０１）を使って、管理状態（Ｌ０２）を取得する（Ｓ３３

）。管理状態（Ｌ０２）によって、受信した管理データから必要とするデータが変わってくる。つまり、未インストール状態（Ｊ０１）であれば、すべての管理データが必要であるが、個別データＤｅｌｅｔｅｄ状態（Ｊ０２）であれば、管理データ(Ｈ０７)の中からと個別データのハッシュ（Ｈ０５）だけが必要になる。アプリケーションＤｅｌｅｔｅｄ状態（Ｊ０３）であれば、管理データ（Ｈ０７）の中から署名（Ａ０５）だけが必要になる。管理データの中に不要なデータが含まれている場合、無視して処理を行わない。そのため、最初に送付する時点で、数値計算手段（１００４）に無視されるデータは送信しなくても、何ら問題ない。逆に、必要なデータが含まれていない場合は、エラーとなる。その場合、数値計算手段（１００４）は、外部機器（２００）に結果を出力する（Ｃ０４）際、正常終了ではなく、フォーマット異常により終了したというエラーコードを出力する。問題なければ、管理状態（Ｌ０２）よって必要な共通データ（Ｈ０６）内のデータを記憶制御手段（１００３）経由で記憶手段（１００５）に仮格納する（Ｓ３４）。尚、上記のエラーに限定したものではなく、異常動作をした場合は、事前に外部と取り交わされたその旨を示すコードを出力する。本実施の形態では、未インストール状態（Ｊ０１）であり、すべての管理データが必要な場合とする。

【００６９】

状態によって、署名(Ａ０５)が必須のデータとなっている場合、署名に対して事前に復号処理を行う。数値計算手段（１００４）は、製造者の公開鍵（Ｍ０１）を使って署名（Ａ０５）を暗復号手段（１００６）で復号する。数値計算手段（１００４）は、復号したデータに対して、適切なパディング処理をしているかを確認する。数値計算手段（１００４）適切なパディング処理であることを確認できた場合、少なくとも適切な秘密鍵で作成された署名であることが確認できたので、対象となるハッシュ（Ｈ１１）を取得する(Ｓ３４－１)。

【００７０】

適切なパディングが確認できなかった場合は、エラーとなる。問題が無かった場合には、正常であることを外部端末（２００）に通知する（Ｃ０４）。

【００７１】

次に、通信手段（１００１）は個別データ暗号鍵を暗号化したデータ（Ｈ０４）を外部機器（２００）経由で受信し（図１６Ｂ：Ｃ０５）、数値計算手段（１００４）に渡す。数値計算手段（１００４）は、記憶手段（１００５）で保持するカードＲＳＡ秘密鍵（Ｍ０４）を使って、暗復号手段（１００６）で復号する（Ｓ３５）。復号した個別データ暗号鍵（Ｈ０１）をカード内の記憶手段（１００５）で保持する。数値計算手段（１００４）は、次の個別データを低速通信路ではなく、高速通信路を使ってデータを受信する判断をし、記憶制御手段（１００３）からデータを展開するアドレス情報を取得し、領域制御手段（１０１０）に通知する（Ｓ８０）。数値計算手段（１００４）は、復号した個別データ暗号鍵（Ｈ０１）を、領域制御手段（１０１０）に通知する。領域制御手段（１０１０）は、受信したアドレス情報を保持し、アドレス情報に対応した外部に公開するためのエリア番地とエリアサイズ（以下、前記２つの情報を合わせてエリア情報とする）を生成し、数値計算手段（１００４）に送信する。数値計算手段（１００４）は、前記エリア情報を外部機器に出力する（Ｄ０１）。領域制御手段（１０１０）は、受信した個別データ暗号鍵（Ｈ０１）を復号用鍵として設定する。前記エリア情報を通知するだけではなく、次に送る必要があるデータが個別データであることを識別子にして送ると、外部端末（２００）は効率的に処理を行う事ができるため好ましい。

【００７２】

外部機器（２００）は、受信したエリア情報を使って、高速通信路を利用して、書き込むエリア番地と書き込むエリアサイズをカードに通知するコマンド（以下、領域情報設定コマンドとする）を送信する（Ｄ０２）。エリアサイズは、通知されたサイズより小さくなってもかまわない。通信手段（１００１）は、前記領域情報設定コマンドを受信し、そのデータをコマンド解釈手段（１００２）に送信する。コマンド解釈手段（１００２）は、前記領域情報設定コマンドを解釈し、領域制御手段にエリア番地と書き込むサイズを通

知する。領域制御手段（１００４）は、エリア番地を確認し、書込みサイズを設定する（Ｓ８１）。番地が異なる場合や、サイズが予め通知したサイズより大きい場合はエラーとなる。

【００７３】

次に通信手段（１００１）は、高速通信路を使って送信された暗号化された個別データ（Ｈ０３）を受信する（Ｄ０３）。通信手段（１００１）は、前記データをコマンド解釈手段に渡す。コマンド解釈手段（１００２）は、受信したデータを領域制御手段（１０１０）に送信する。

【００７４】

領域制御手段（１０１０）は、前記の個別データ暗号鍵（Ｈ０１）を用いて、暗号化された個別データ（Ｈ０３）の復号を暗復号手段（１００６）で行い（Ｓ８２）、復号した個別データ（Ｈ０２）を記憶手段（１００５）に仮格納する（Ｓ８４）。そして図１６Ｃにおいて、領域制御手段（１０１０）は個別データ（Ｈ０２）のハッシュをハッシュ生成手段（１００９）で生成する（Ｓ８３）。

【００７５】

次に、通信手段（１００１）は、アプリケーション暗号鍵を暗号化したデータ（Ａ０４）を外部機器（２００）経由で受信し（Ｄ０４）、数値計算手段（１００４）に渡す。数値計算手段（１００４）は、領域制御手段（１０１０）で生成したハッシュを取得し、管理データに含まれていた個別データのハッシュ（Ｈ０５）と同じであるかを照合手段（１００７）を用いて確認する（Ｓ８５）。異なる場合、数値計算手段（１００４）はインストール処理を中止する。外部機器（２００）に結果を出力する（Ｄ０５）際、正常終了ではなく、ハッシュが異なるという旨を示すエラーコードを出力する（Ｓ８６）。数値計算手段（１００４）は、記憶手段（１００５）で保持するカードＲＳＡ秘密鍵（ＭＯ４）を使って、暗復号手段（１００６）でアプリケーション暗号鍵を暗号化したデータ（Ａ０４）を復号し、アプリケーション暗号鍵（Ａ０１）を取得する（Ｓ８７）。次のアプリケーションデータを低速通信路ではなく、高速通信路を使ってデータを受信する判断をし、記憶制御手段（１００３）からデータを展開するアドレス情報を取得し、領域制御手段（１０１０）に通知する。数値計算手段（１００４）は、復号したアプリケーション暗号鍵（Ａ０１）を、領域制御手段（１０１０）に通知する。領域制御手段（１０１０）は、受信したアドレス情報を保持し、アドレス情報に対応した外部に公開するためのエリア番地とエリアサイズ（以下、前記２つの情報を合わせてエリア情報とする）を生成し、数値計算手段（１００４）に送信する（Ｓ８８）。数値計算手段（１００４）は、前記エリア情報を外部機器（２００）に出力する（Ｄ０５）。領域制御手段（１００４）は、受信したアプリケーション暗号鍵（Ａ０１）を復号用鍵として設定する。前記エリア情報を通知するだけではなく、次に送る必要があるデータがアプリケーションであることを識別子にして送ると、外部端末（２００）は効率的に処理を行う事ができるため好ましい。

【００７６】

外部機器（２００）は、受信したエリア情報を使って、高速通信路を利用して、書き込むエリア番地と書き込むエリアサイズをカードに通知するコマンド（以下、領域情報設定コマンドとする）を送信する（Ｄ０６）。エリアサイズは、通知されたサイズより小さくなってもかまわない。通信手段（１００１）は、前記領域情報設定コマンドを受信し、そのデータをコマンド解釈手段（１００２）に送信する。次いで図１６Ｄにおいて、コマンド解釈手段（１００２）は、前記領域情報設定コマンドを解釈し、領域制御手段（１０１０）にエリア番地と書き込むサイズを通知する。領域制御手段（１０１０）は、エリア番地を確認し、書込みサイズを設定する（Ｓ８９）。番地が異なる場合や、サイズが予め通知したサイズより大きい場合はエラーとなる。

【００７７】

次に通信手段（１００１）は、高速通信路を使って送信された暗号化されたアプリケーションデータ（Ａ０３）を受信する（Ｄ０７）。通信手段（１００１）は、前記データをコマンド解釈手段（１００２）に渡す。コマンド解釈手段（１００２）は、受信したデー

タを領域制御手段（１０１０）に送信する。
【００７８】
領域制御手段（１０１０）は、前記のアプリケーション暗号鍵（Ａ０１）を用いて、暗復号手段（１００６）で暗号化された個別データの復号を行う（Ｓ９０）。領域制御手段（１０１０）はアプリケーション（Ａ０２）のハッシュをハッシュ生成手段（１００９）で生成する（Ｓ９１）。領域制御手段（１０１０）は、復号したアプリケーション（Ａ０２）を記憶手段（１００５）に仮格納する（Ｓ９２）。
【００７９】
次に、通信手段（１００１）は、照合を要求するコマンドを外部機器（２００）から受信し（Ｄ０８）、数値計算手段（１００４）に渡す。数値計算手段（１００４）は、署名から取得したハッシュ（Ｈ１１）と、前記取得したアプリケーションのハッシュを照合手段（１００７）で照合する（Ｓ９３）。異なる場合、数値計算手段（１００４）はインストール処理を中止する。数値計算手段（１００４）は、外部機器（２００）に結果を出力する（Ｄ０９）際、正常終了ではなく、ハッシュが異なるという旨を示すエラーコードを出力する。同じである場合、数値計算手段（１００４）は、インストール処理を終了する（Ｓ９４）。数値計算手段（１００４）は、署名が正当である場合、署名と一緒に暗号化されていた個別データのハッシュ、共通データを正当であると判断し、該当アプリケーションに関連する共通データ、個別データ、アプリケーションをカード内で動作可能な状態にするために記憶手段（１００５）が持つ管理状態（Ｌ０２）をＩｎｓｔａｌｌｅｄ状態（Ｊ０４）に変更する。数値計算手段（１００４）は、正常終了した旨を示すコードを外部機器（２００）に出力する（Ｄ０９）。
【００８０】
本発明では、外部機器（２００）は、カードからの出力データに付与された領域情報（Ｄ０１、Ｄ０５）を使って、高速通信路を使うタイミングと書き込み対象領域、対象領域サイズを知ることができる。外部端末は受信した前記領域情報をカードに送信して、次に高速通信路を使って書き込む領域情報とサイズをカードに伝える（Ｄ０２、Ｄ０６）。その次に高速通信路を使って、カードにデータ（個別データ、アプリケーションデータ）を書き込む（Ｄ０３、Ｄ０７）。
【００８１】
外部機器（２００）は、前記の通信路の本数についてはカードの識別情報から判別することも可能であり、タイミングについてはカードに送信する暗号データの種別を事前に外部機器（２００）が知っていれば、切り替えることが可能である。だが、データの書き込む領域についてはカードから情報を取得しないと知ることが不可能である。そのため前記領域情報を取得した時に切り替え作業を行う方が、他の判別方法を使わずに済み、効率が良い。
【００８２】
また、アプリ開発者（Ｐ２）がカード製造者（Ｐ１）に対して署名の申請をする方法において、アプリ開発者を物理的、視覚的、社会的に確認する方法は、システムの規定外であり、公共機関、金融機関等が実施している本人確認方法を利用しても構わない。また、生成された署名を配送する仕組みや、カード製造者（Ｐ１）からアプリ開発者（Ｐ２）に配布される開発環境を配送する仕組みにおいても同様に、一般的な配布方法を採用するとし言及しない。また、上記の開発環境を使って、署名の申請を行い、アプリ開発者先にある開発環境と製造者間で暗号セッションを構築し署名を配送することも可能であるが、開発環境の配布が正しく安全にできないと実現できない。
【００８３】
本実施の形態では、プレイヤーとしてアプリ開発者、サービス提供者、サーバ運用者の３者に分けているが、３者の処理内容として、共通に使うデータを構築する、個別に使うデータを構築する、それを配信するという形態に限定されるわけではない。
【００８４】
尚、本実施の形態で記載しているハッシュを生成する方法は一方向性関数を使っており

、従来技術では、ＳＨＡ－１やＭＤ５、ＳＨＡ－２５６などを指している。使用する目的とするところは、大規模なデータを要約し、少ないデータ量で識別することであり、前記データがすでに小さいもので、ハッシュを生成する必要がなければそのままの値を比較しても良い。

【００８５】

尚、本実施の形態で記載している署名は公開鍵暗号方式の場合に限って記載しているのではなく、利用する暗号アルゴリズムが共通鍵暗号方式であれば、署名はメッセージ認証コード（ＭＡＣ：Ｍａｓｓａｇｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｃｏｄｅ）に当たる。署名の生成方法に関して、本実施の形態ではハッシュを作成してから秘密鍵にて署名を施しているが、前記ハッシュを生成する方法でも記載したが、データがすでに小さいものであれば、前記データをハッシュとして利用しても構わない。

【００８６】

尚、本実施の形態では、サーバと外部機器間の通信路については、ＨＴＴＰ、もしくはＨＴＴＰＳと記載したが、それに限定されるものではなく、有線、無線に関連無く、一般的にサーバと外部機器が通信する方法であれば、本発明に何ら影響はない。よって、サーバと外部機器が独自に暗号通信を行うことも可能であり、前記暗号通信を行うことによってカードの振る舞いは変わらない。

【００８７】

本実施の形態において、カード（１００）は、不揮発性記憶装置であり、記憶手段（１００５）が不揮発性メモリであり、それ以外の通信手段（１００１）、コマンド解釈手段（１００２）、記憶制御手段（１００３）、数値計算手段（１００４）、暗復号手段（１００６）、照合手段（１００７）、ハッシュ生成手段（１００９）がメモリコントローラで実現する機能である。

【００８８】

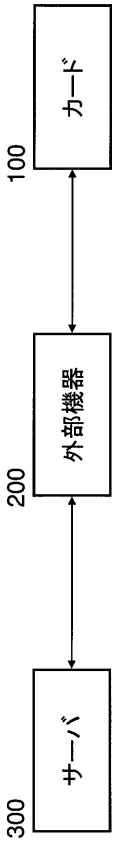
外部機器（２００）は、前記不揮発性記憶装置と通信するアクセス装置であり、サーバ（３００）は、前記不揮発性記憶装置に対するデータを保存しておく装置であり、アクセス装置自体が持つ記憶装置として含まれていても、何ら問題はない。この場合、前記アクセス装置と前記不揮発性記憶装置の２つを指して、不揮発性記憶システムとする。

【産業上の利用可能性】

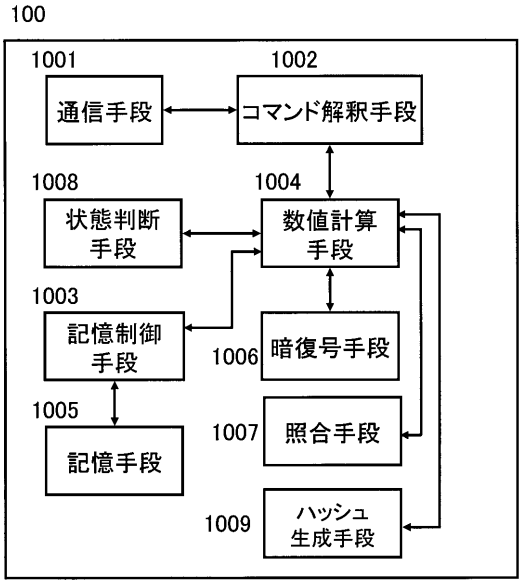
【００８９】

本発明にかかる不揮発性記憶システムは、不揮発性記憶装置に対して、データの格納処理を冗長にしないために提案するものであり、半導体メモリカードはいうまでもなく、半導体メモリカード等の不揮発性記憶装置を使用した静止画記録再生装置や動画記録再生装置、あるいは携帯電話においても有益である。

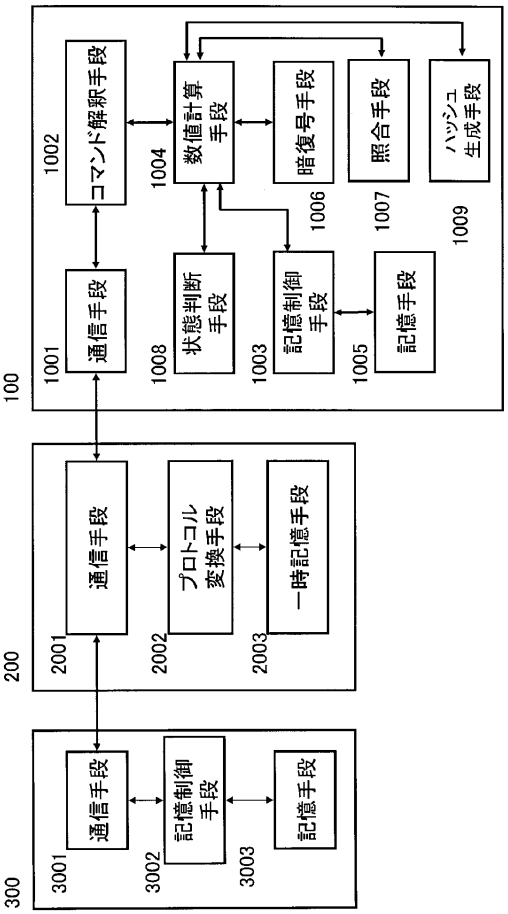
【図１】


カード
100
外部機器
200
サーバ
300

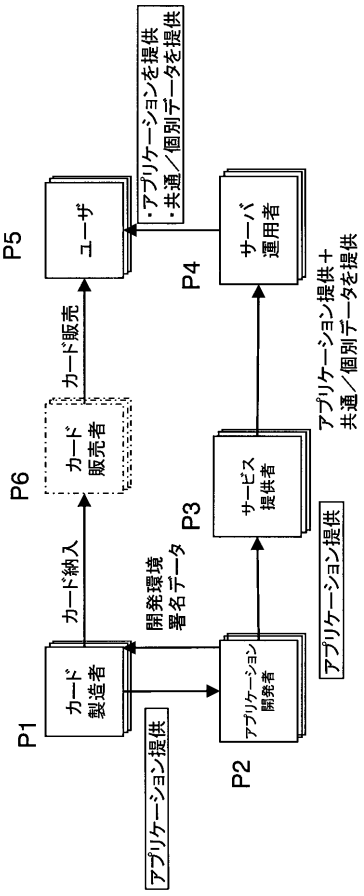
【図２】


100
1001
通信手段
1002
コマンド解釈手段
1008
状態判断手段
1004
数値計算手段
1003
記憶制御手段
1006
暗復号手段
1005
記憶手段
1007
照合手段
1009
ハッシュ生成手段

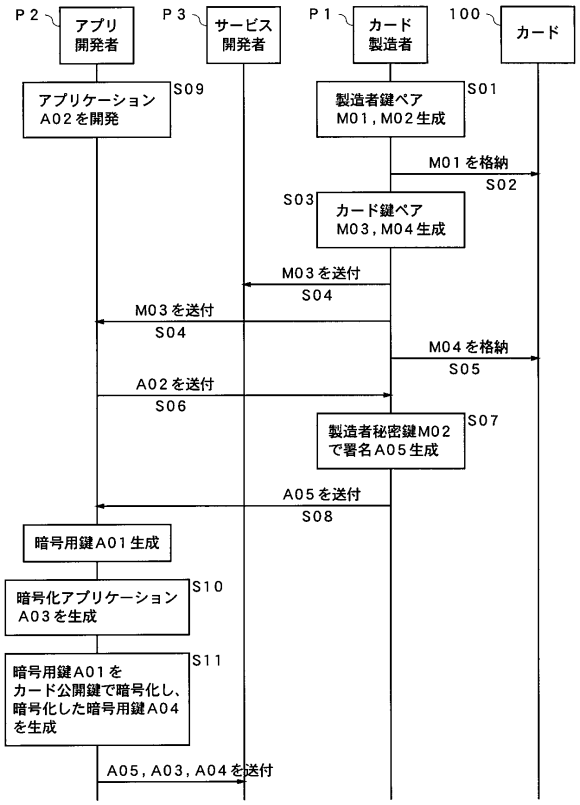
【図３】


100
1001
通信手段
1002
コマンド解釈手段
1008
状態判断手段
1004
数値計算手段
1003
記憶制御手段
1006
暗復号手段
1005
記憶手段
1007
照合手段
1009
ハッシュ生成手段
200
2001
通信手段
2002
プロトコル変換手段
2003
一時記憶手段
300
3001
通信手段
3002
記憶制御手段
3003
記憶手段

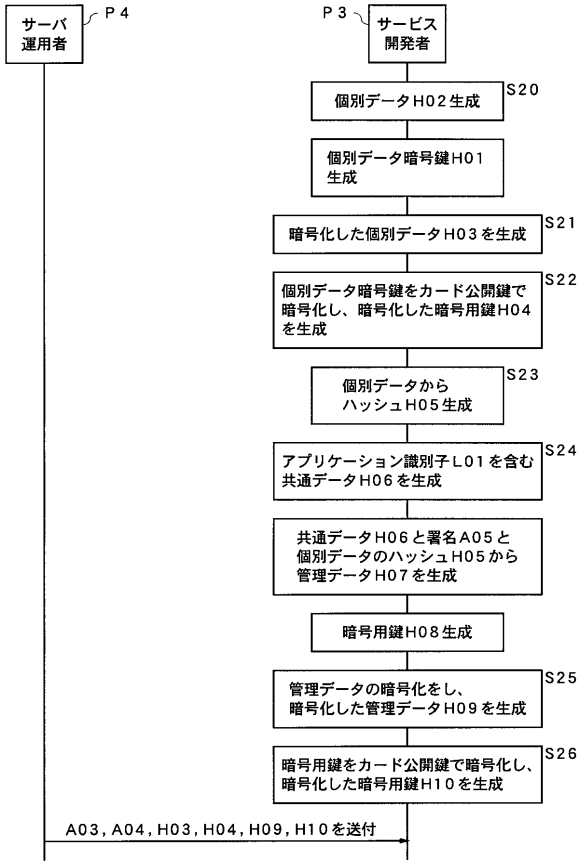
【図４】


P1
カード製造者
P2
アプリケーション開発者
P3
サービス提供者
P4
サーバ運用者
P5
ユーザ
P6
カード販売者
カード納入
カード販売
開発環境
署名データ
アプリケーション提供
アプリケーション提供
アプリケーション提供＋
共通／個別データを提供
・アプリケーションを提供
・共通／個別データを提供

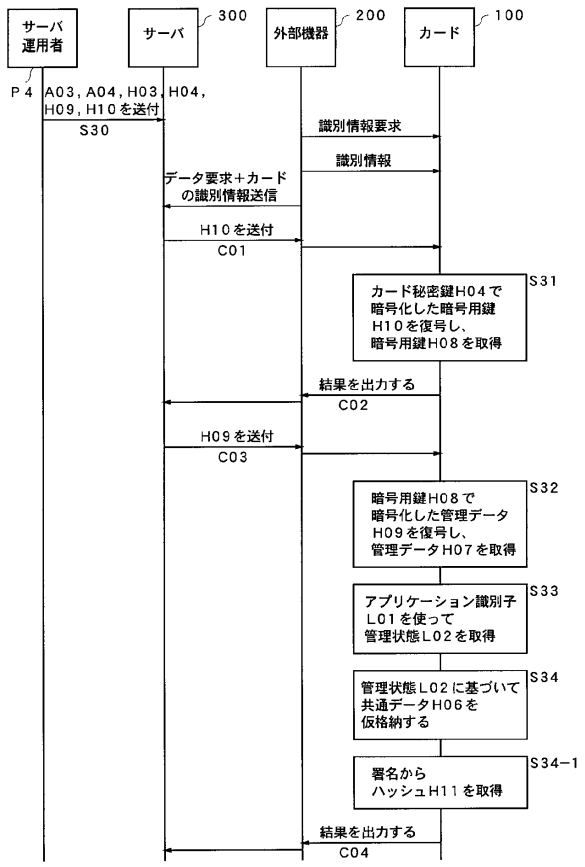
【図５】


P2
アプリ開発者
P3
サービス開発者
P1
カード製造者
100
カード
アプリケーションA02を開発
S09
製造者鍵ペアM01，M02生成
S01
M01を格納
S02
S03
カード鍵ペアM03，M04生成
M03を送付
S04
M03を送付
S04
M04を格納
S05
A02を送付
S06
製造者秘密鍵M02で署名A05生成
S07
A05を送付
S08
暗号用鍵A01生成
暗号化アプリケーションA03を生成
S10
暗号用鍵A01をカード公開鍵で暗号化し、暗号化した暗号用鍵A04を生成
S11
A05，A03，A04を送付

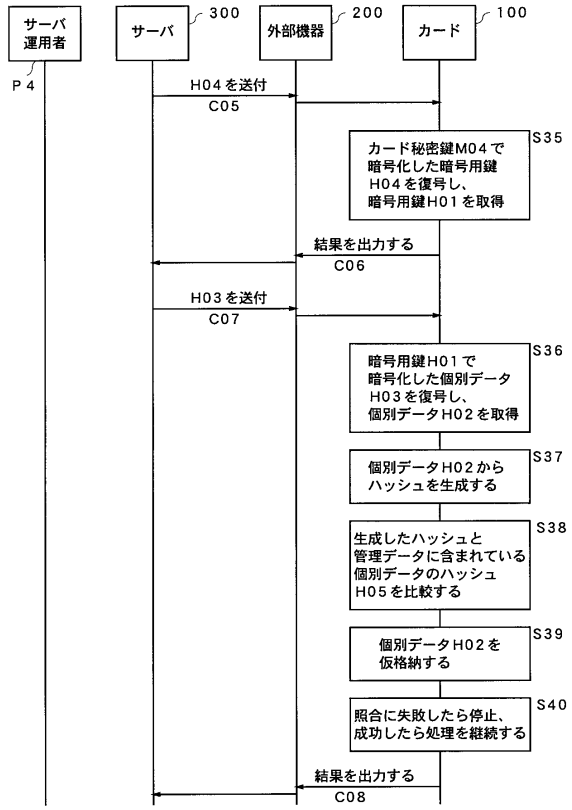
【図６】


サーバ運用者
P4
P3
サービス開発者
個別データH02生成
S20
個別データ暗号鍵H01生成
暗号化した個別データH03を生成
S21
個別データ暗号鍵をカード公開鍵で暗号化し、暗号化した暗号用鍵H04を生成
S22
個別データからハッシュH05生成
S23
アプリケーション識別子L01を含む共通データH06を生成
S24
共通データH06と署名A05と個別データのハッシュH05から管理データH07を生成
暗号用鍵H08生成
管理データの暗号化をし、暗号化した管理データH09を生成
S25
暗号用鍵をカード公開鍵で暗号化し、暗号化した暗号用鍵H10を生成
S26
A03，A04，H03，H04，H09，H10を送付

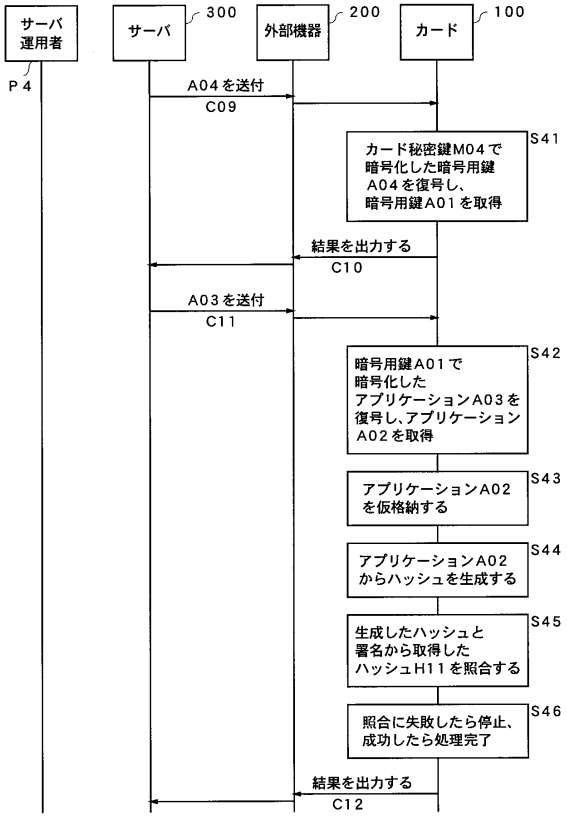
【図７Ａ】


サーバ運用者
P4
サーバ
300
外部機器
200
カード
100
A03，A04，H03，H04，H09，H10を送付
S30
識別情報要求
識別情報
データ要求＋カードの識別情報送信
H10を送付
C01
カード秘密鍵H04で暗号化した暗号用鍵H10を復号し、暗号用鍵H08を取得
S31
結果を出力する
C02
H09を送付
C03
暗号用鍵H08で暗号化した管理データH09を復号し、管理データH07を取得
S32
アプリケーション識別子L01を使って管理状態L02を取得
S33
管理状態L02に基づいて共通データH06を仮格納する
S34
署名からハッシュH11を取得
S34−1
結果を出力する
C04

【図７Ｂ】


サーバ運用者
P4
サーバ
300
外部機器
200
カード
100
H04を送付
C05
カード秘密鍵M04で暗号化した暗号用鍵H04を復号し、暗号用鍵H01を取得
S35
結果を出力する
C06
H03を送付
C07
暗号用鍵H01で暗号化した個別データH03を復号し、個別データH02を取得
S36
個別データH02からハッシュを生成する
S37
生成したハッシュと管理データに含まれている個別データのハッシュH05を比較する
S38
個別データH02を仮格納する
S39
照合に失敗したら停止、成功したら処理を継続する
S40
結果を出力する
C08

【図７Ｃ】



【図８】

個別データ

論理アドレス	割り当てられた値	データ例(Length+Data)
0-99	識別情報	0x08 + 0102030405060708 + 残り91byte はALL 0x00
100-1099	自己証明書	0x820300 + 0A0B0C0D0E…+ 残り229byte はALL 0x00
1100-2099	ルート証明書	0x820330 + 1A2A3A4A5A…+ 残り181byte はALL 0x00
2100-5099	ファイルシステム情報	0x8207D0 + 1B2B3B4B5B…+残り1997byte はALL 0x00

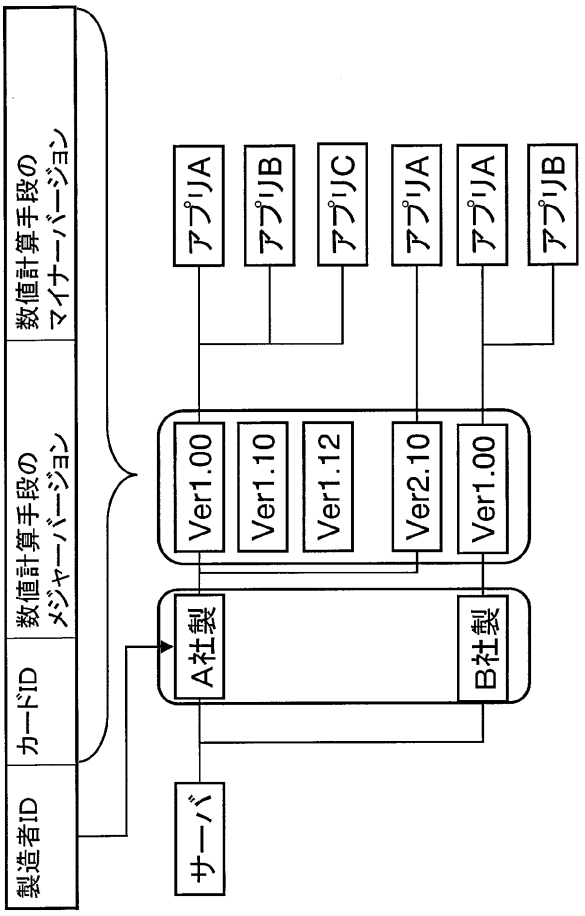
【図９】

管理データフォーマット

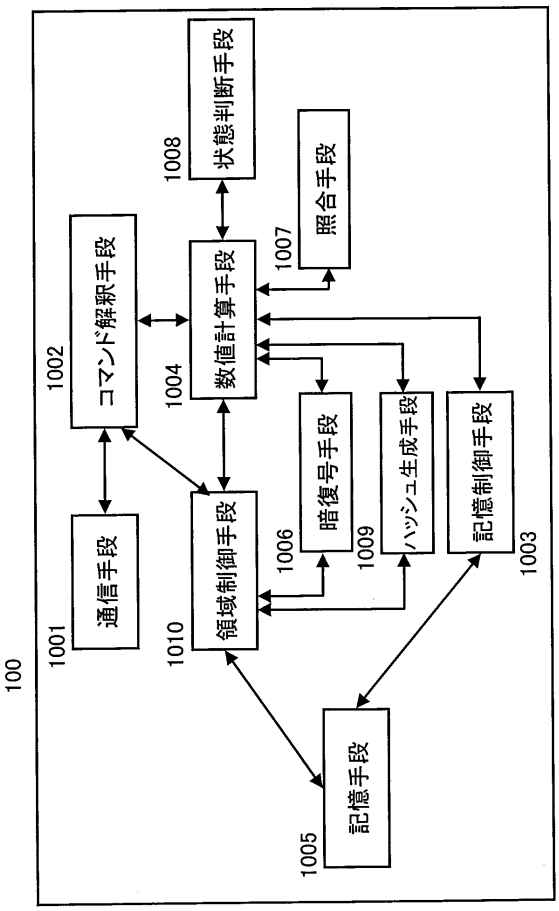
データ種別	長さ
アプリケーション識別子長	1
アプリケーション識別子	5-16
アプリケーションのバージョン情報	2
アプリケーションのサイズ	4
アプリケーションの署名	256
固別データのバージョン情報	2
固別データのサイズ	4
固別データのハッシュ	20
著作権情報などを記載できる備考欄長	1
備考欄	0-255

L01

【図１０】



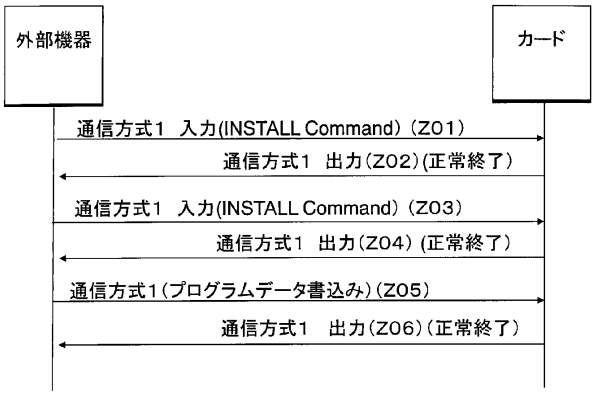
【図１１】



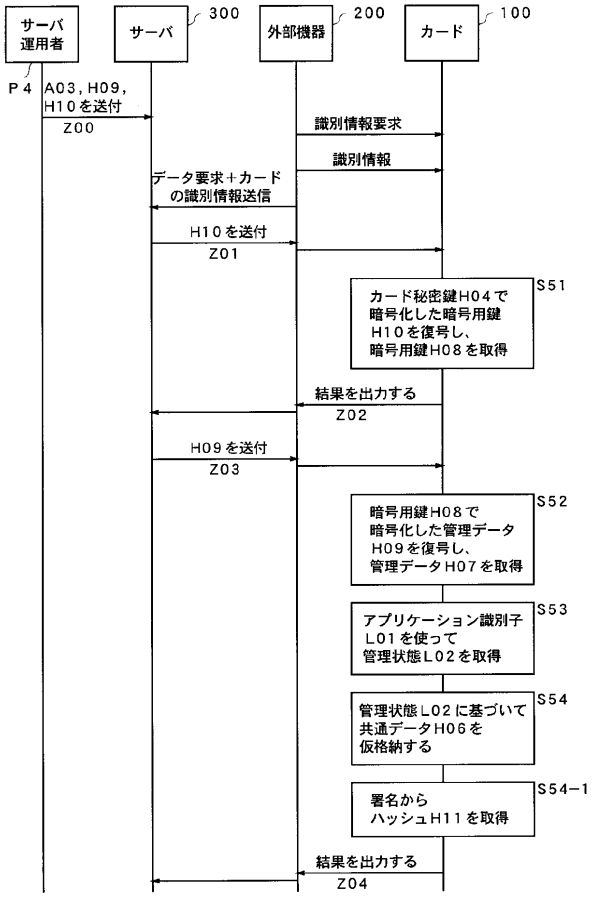
【図１２】

【図１３】

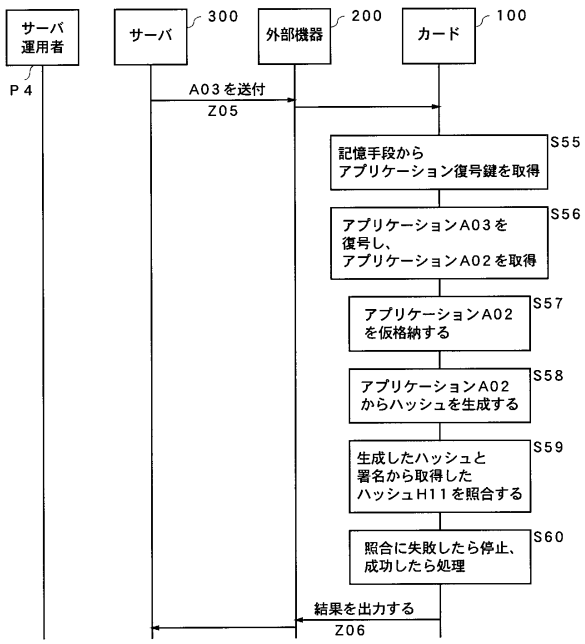
【図１４】



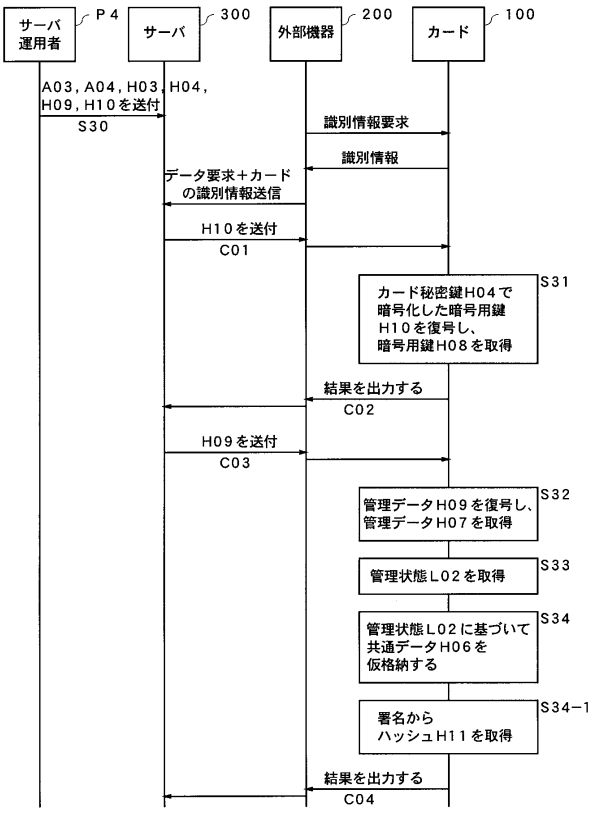
【図１５Ａ】



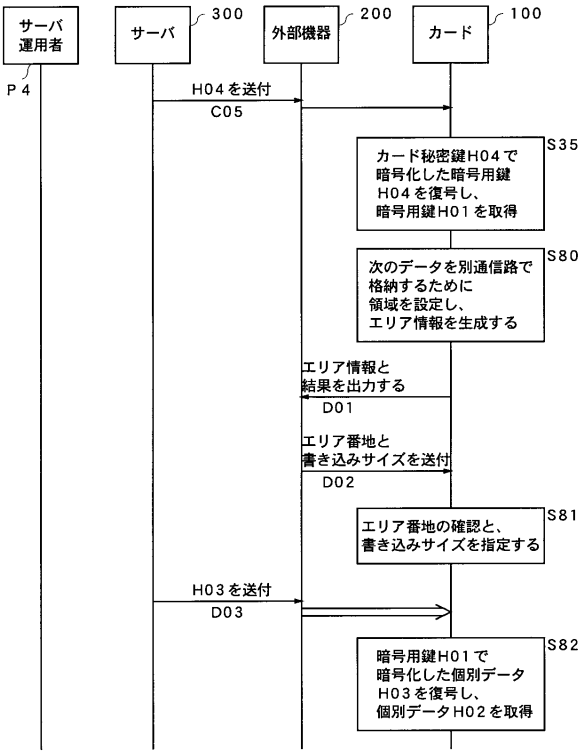
【図１５Ｂ】



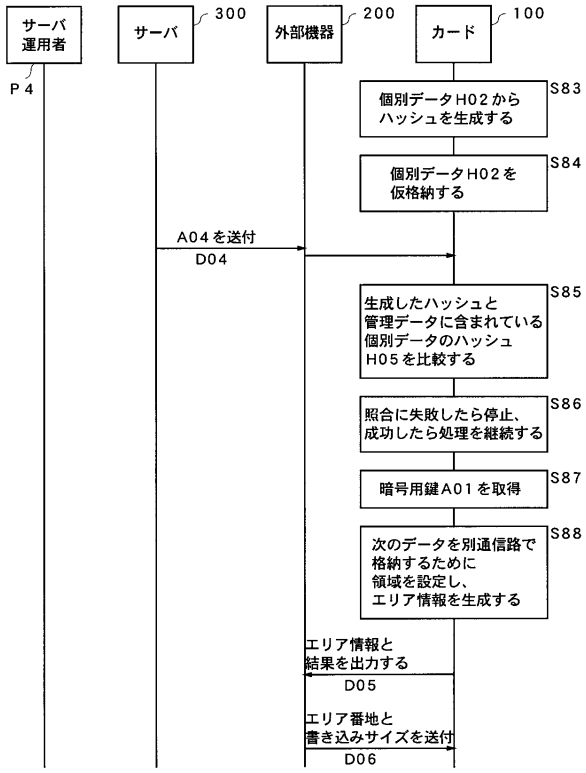
【図１６Ａ】



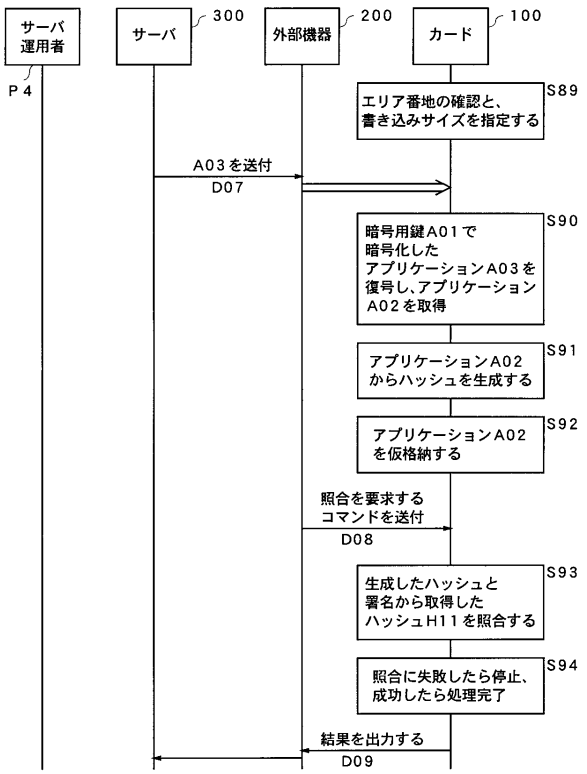
【図１６Ｂ】



【図１６Ｃ】



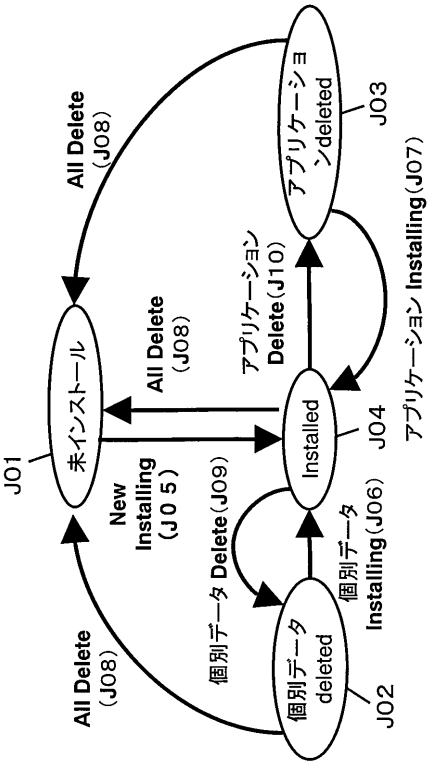
【図１６Ｄ】



【図１７】

アプリケーション識別子(L01)	管理状態(L02)
000000000001	Installed
123456789101	個別データdeleted
526374859607182 9	アプリケーションdeleted
015800940337009073	Installed
.....	.....
858503048584	Installed

【図１８】



フロントページの続き

(72)発明者　高木　佳彦
大阪府門真市大字門真１００６番地　パナソニック株式会社内
(72)発明者　佐々木　理
大阪府門真市大字門真１００６番地　パナソニック株式会社内

審査官　平井　誠

(56)参考文献　国際公開第２００８／１４６４７６（WO，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１