(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4391375号
(P4391375)
(45)発行日　平成21年12月24日(2009.12.24)　(24)登録日　平成21年10月16日(2009.10.16)

(51)Int.Cl.　　F I
G06K 17/00 (2006.01)　　G06K 17/00 D
G06F 21/24 (2006.01)　　G06K 17/00 E
G06F 12/14 540B

請求項の数 3　(全 26 頁)

(21)出願番号　特願2004-285950 (P2004-285950)
(22)出願日　平成16年9月30日 (2004.9.30)
(65)公開番号　特開2006-99509 (P2006-99509A)
(43)公開日　平成18年4月13日 (2006.4.13)
審査請求日　平成17年9月26日 (2005.9.26)

前置審査

(73)特許権者　504134520
フェリカネットワークス株式会社
東京都品川区大崎１丁目１１番１号
(74)代理人　100082131
弁理士　稲本　義雄
(72)発明者　赤鹿　秀樹
東京都品川区大崎１丁目１１番１号　フェリカネットワークス株式会社内
(72)発明者　荻嶋　淳
東京都品川区大崎１丁目１１番１号　フェリカネットワークス株式会社内
(72)発明者　花木　直文
東京都品川区大崎１丁目１１番１号　フェリカネットワークス株式会社内

最終頁に続く

(54)【発明の名称】情報管理装置および方法、並びにプログラム

(57)【特許請求の範囲】
【請求項１】
IC(Integrated Circuit)チップの種別と、所定のコマンドを実行させるクライアントにおけるICチップに実行させるコマンドの種別を対応付けて管理するとともに、ICチップの種別に対応付けて、ICチップとの認証方法と、ICチップに実行させるコマンドを含む、ICチップに送信するデータに施す暗号化の方法を管理する管理手段と、
制御対象とするICチップの種別を含むICチップ情報と、前記クライアントにおいて実行されるアプリケーションを特定する情報を含むクライアント情報とを、前記クライアントから情報管理装置自身に対する接続要求と共に取得する取得手段と、
前記管理手段により管理されている複数の異なる種別のコマンドのうち、前記取得手段により取得された前記ICチップ情報に含まれるICチップの種別に対応付けられている種別のコマンドを作成するコマンド作成手段と、
前記コマンド作成手段により作成されたコマンドを含む前記制御対象とするICチップに送信するデータに、対応付けられたICチップの種別に応じて暗号化を施す暗号化手段と、
前記暗号化手段により暗号化された前記コマンドと、前記取得手段により取得された前記クライアント情報に含まれる情報により特定される前記アプリケーションに応じたメッセージを含むデータを前記制御対象とするICチップに送信するコマンド送信手段と
を備えることを特徴とする情報管理装置。
【請求項２】
IC(Integrated Circuit)チップの種別と、所定のコマンドを実行させるクライアントに

おけるICチップに実行させるコマンドの種別を対応付けて管理するとともに、ICチップの種別に対応付けて、ICチップとの認証方法と、ICチップに実行させるコマンドを含む、ICチップに送信するデータに施す暗号化の方法を管理する管理ステップと、

制御対象とするICチップの種別を含むICチップ情報と、前記クライアントにおいて実行されるアプリケーションを特定する情報を含むクライアント情報とを、前記クライアントから情報管理装置自身に対する接続要求と共に取得する取得ステップと、

前記管理ステップの処理により管理されている複数の異なる種別のコマンドのうち、前記取得ステップの処理により取得された前記ICチップ情報に含まれるICチップの種別に対応付けられている種別のコマンドを作成するコマンド作成ステップと、

前記コマンド作成ステップの処理により作成されたコマンドを含む前記制御対象とするICチップに送信するデータに、対応付けられたICチップの種別に応じて暗号化を施す暗号化ステップと、

前記暗号化ステップの処理により暗号化された前記コマンドと、前記取得ステップの処理により取得された前記クライアント情報に含まれる情報により特定される前記アプリケーションに応じたメッセージを含むデータを前記制御対象とするICチップに送信するコマンド送信ステップと

を含むことを特徴とする情報管理方法。

【請求項３】

IC(Integrated Circuit)チップの種別と、所定のコマンドを実行させるクライアントにおけるICチップに実行させるコマンドの種別を対応付けて管理するとともに、ICチップの種別に対応付けて、ICチップとの認証方法と、ICチップに実行させるコマンドを含む、ICチップに送信するデータに施す暗号化の方法を管理する管理ステップと、

制御対象とするICチップの種別を含むICチップ情報と、前記クライアントにおいて実行されるアプリケーションを特定する情報を含むクライアント情報とを、前記クライアントから情報管理装置自身に対する接続要求と共に取得する取得ステップと、

前記管理ステップの処理により管理されている複数の異なる種別のコマンドのうち、前記取得ステップの処理により取得された前記ICチップ情報に含まれるICチップの種別に対応付けられている種別のコマンドを作成するコマンド作成ステップと、

前記コマンド作成ステップの処理により作成されたコマンドを含む前記制御対象とするICチップに送信するデータに、対応付けられたICチップの種別に応じて暗号化を施す暗号化ステップと、

前記暗号化ステップの処理により暗号化された前記コマンドと、前記取得ステップの処理により取得された前記クライアント情報に含まれる情報により特定される前記アプリケーションに応じたメッセージを含むデータを前記制御対象とするICチップに送信するコマンド送信ステップと

を含む処理をコンピュータに実行させることを特徴とするプログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、情報管理装置および方法、並びにプログラムに関し、特に、１つのサーバからの要求に応じて、複数の異なる種別のICチップに対応したコマンドを作成することができるようにする情報管理装置および方法、並びにプログラムに関する。

【背景技術】

【０００２】

近年、クレジットカードや携帯電話機に埋め込まれたFeliCa（登録商標）などの非接触ICチップに電子マネーをチャージ（入金）し、そのチャージされた電子マネーを用いて、商品購入時の代金の支払いをしたりすることが普及しつつある。

【０００３】

代金の支払い時には、自分のクレジットカードや携帯電話機を店舗に設置された端末（リーダライタ）にかざすだけであるから、ユーザは、代金の支払いを迅速に行うことがで

きる。

【０００４】

このような電子マネーシステムは、例えば、図１に示すような構成からなる。

【０００５】

電子マネーシステムのサーバ側はサーバ装置１とSAM(Secure Application Module)２からなり、クライアント側はクライアント装置３とR/W（リーダ／ライタ）４からなる。サーバ装置１とクライアント装置３は、ネットワーク５を介して接続されている。

【０００６】

図１の例においては、クライアント側のR/W４には非接触ICチップ１３が内蔵された携帯電話機６が近接されており、電磁誘導を用いた近距離通信を介してクライアント装置３に接続されている。

【０００７】

サーバ装置１に実装されるサーバアプリケーション１１は、クライアント装置３に実装されるクライアントアプリケーション１２との間で通信を行い、クライアントアプリケーション１２からの要求に応じて作成したコマンド（非接触ICチップ１３に実行させるコマンド）をSAM２に出力する。また、サーバアプリケーション１１は、暗号化が施されたコマンドがSAM２から供給されてきたとき、それをネットワーク５を介してクライアント装置３のクライアントアプリケーション１２に送信する。

【０００８】

SAM２は、耐タンパ性を有する装置であり、暗号処理、および、その暗号処理で用いる鍵の管理を行う。SAM２は、サーバアプリケーション１１から供給されてきたコマンドに暗号化を施し、暗号化されたコマンドをサーバアプリケーション１１に出力する。SAM２と非接触ICチップ１３は、それぞれ共通の鍵を持っており、その鍵で暗号化された情報を送受信することによりSAM２と非接触ICチップ１３の間で暗号通信が実現される。

【０００９】

クライアント装置３のクライアントアプリケーション１２は、所定の要求をサーバ装置１のサーバアプリケーション１１に送信するとともに、サーバアプリケーション１１からコマンドが送信されてきたとき、それをR/W４を介して非接触ICチップ１３に送信し、実行させる。

【００１０】

非接触ICチップ１３は、R/W４等を介してSAM２から送信されてきたコマンドに施されている暗号化を復号し、それを実行する。コマンドの内容が電子マネーの書き換えである場合、このコマンドには書き換える金額の情報なども含まれている。

【００１１】

例えば、このような構成を有する電子マネーシステムにおいて、非接触ICチップ１３に記憶されている電子マネーを用いて携帯電話機６のユーザが購入した商品の代金を支払う場合、クライアント装置３のクライアントアプリケーション１２により、サーバ装置１のサーバアプリケーション１１に対して、商品の代金の支払い要求が送信され、その要求を受信したサーバアプリケーション１１により、電子マネーの残高の読み出しを非接触ICチップ１３に要求するコマンド（Readコマンド）が作成される。

【００１２】

サーバアプリケーション１１により作成されたReadコマンドは、SAM２により暗号化が施された後、サーバ装置１のサーバアプリケーション１１、ネットワーク５、クライアント装置３のクライアントアプリケーション１２、およびR/W４を介して非接触ICチップ１３に送信され、非接触ICチップ１３において復号された後、実行される。Readコマンドが実行されることによって読み出された残高は、非接触ICチップ１３により暗号化が施された後、サーバアプリケーション１１に対するレスポンスとして、R/W４、クライアント装置３のクライアントアプリケーション１２、ネットワーク５、およびサーバ装置１のサーバアプリケーション１１を介してSAM２に送信される。SAM２においては、非接触ICチップ１３から送信されてきた残高に施されている暗号化が復号され、復号された残高がサーバ

アプリケーション１１に送信される。
【００１３】
これにより、サーバアプリケーション１１は、非接触ICチップ１３に記憶されている現在の電子マネーの残高を確認することができる。
【００１４】
残高を確認したとき、サーバ装置１のサーバアプリケーション１１により、電子マネーの残高の書き換え（商品の代金の分だけ減額した残高への書き換え）を非接触ICチップ１３に要求するコマンド（Writeコマンド）が作成される。
【００１５】
サーバアプリケーション１１により作成されたWriteコマンドは、先に送信されたReadコマンドと同様に、SAM２により暗号化が施された後、サーバ装置１のサーバアプリケーション１１、ネットワーク５、クライアント装置３のクライアントアプリケーション１２、およびR/W４を介して非接触ICチップ１３に送信され、非接触ICチップ１３において復号された後、実行される。このWriteコマンドには、残高をいくらにするのかを表す情報なども含まれている。これにより、非接触ICチップ１３に記憶されている電子マネーの残高が商品の代金の分だけ減額された状態になる。
【００１６】
例えば、残高の減額が完了したことを通知するメッセージが非接触ICチップ１３からサーバアプリケーション１１に送信されるなどの処理が行われた後、一連の処理が終了される。このような一連の処理により、商品の代金の支払いが実現される。
【００１７】
このような構成からなるサーバ－クライアントシステムより、以上のような商品の代金の支払いの他に、例えば、店舗が発行するポイントの管理や、電車の駅の改札機としてクライアント装置３が設けられている場合、乗車料金の支払いなどが実現される。ポイントの管理や乗車料金の支払いの場合も、基本的には、上述した代金の支払いの場合と同様の処理が図１の各装置により行われる。
【００１８】
図１に示すような構成からなるサーバ－クライアントシステムについては特許文献１に開示されている。
【特許文献１】特開２００３－１４１０６３号公報
【発明の開示】
【発明が解決しようとする課題】
【００１９】
ところで、図１に示すような従来のサーバ－クライアントシステムにおいては、制御対象とする非接触ICチップの種別毎に、異なるサーバアプリケーションをサーバ装置１に用意しなければならない。
【００２０】
例えば、クライアント装置３が店舗に設置されている端末であり、制御対象の非接触ICチップが、その店舗の端末のR/Wにかざされている携帯電話機に内蔵されている場合と、クライアント装置３がパーソナルコンピュータであり、制御対象の非接触ICチップが、そのパーソナルコンピュータのR/Wに置かれているカードに埋め込まれている場合とでは、非接触ICチップが入っている場所が異なり、その種別が異なるから、同じサービスを提供するときでも異なるサーバアプリケーションがそれぞれサーバ装置１に用意されている必要がある。
【００２１】
従って、サービス提供者側からすれば、制御対象としたい非接触ICチップの種別毎にサーバアプリケーションを用意する必要があり、それが大きな負担になるという課題があった。
【００２２】
本発明はこのような状況に鑑みてなされたものであり、１つのサーバからの要求に応じ

て、複数の異なる種別のICチップに対応したコマンドを作成することができるようにするものである。

【課題を解決するための手段】

【００２３】

本発明の情報管理装置は、ICチップの種別と、所定のコマンドを実行させるクライアントにおけるICチップに実行させるコマンドの種別を対応付けて管理するとともに、ICチップの種別に対応付けて、ICチップとの認証方法と、ICチップに実行させるコマンドを含む、ICチップに送信するデータに施す暗号化の方法を管理する管理手段と、制御対象とするICチップの種別を含むICチップ情報と、クライアントにおいて実行されるアプリケーションを特定する情報を含むクライアント情報とを、クライアントから情報管理装置自身に対する接続要求と共に取得する取得手段と、管理手段により管理されている複数の異なる種別のコマンドのうち、取得手段により取得されたICチップ情報に含まれるICチップの種別に対応付けられている種別のコマンドを作成するコマンド作成手段と、コマンド作成手段により作成されたコマンドを含む制御対象とするICチップに送信するデータに、対応付けられたICチップの種別に応じて暗号化を施す暗号化手段と、暗号化手段により暗号化されたコマンドと、取得手段により取得されたクライアント情報に含まれる情報により特定されるアプリケーションに応じたメッセージを含むデータを制御対象とするICチップに送信するコマンド送信手段とを備えることを特徴とする。

【００２６】

本発明の情報管理方法は、ICチップの種別と、所定のコマンドを実行させるクライアントにおけるICチップに実行させるコマンドの種別を対応付けて管理するとともに、ICチップの種別に対応付けて、ICチップとの認証方法と、ICチップに実行させるコマンドを含む、ICチップに送信するデータに施す暗号化の方法を管理する管理ステップと、制御対象とするICチップの種別を含むICチップ情報と、クライアントにおいて実行されるアプリケーションを特定する情報を含むクライアント情報とを、クライアントから情報管理装置自身に対する接続要求と共に取得する取得ステップと、管理ステップの処理により管理されている複数の異なる種別のコマンドのうち、取得ステップの処理により取得されたICチップ情報に含まれるICチップの種別に対応付けられている種別のコマンドを作成するコマンド作成ステップと、コマンド作成ステップの処理により作成されたコマンドを含む制御対象とするICチップに送信するデータに、対応付けられたICチップの種別に応じて暗号化を施す暗号化ステップと、暗号化ステップの処理により暗号化されたコマンドと、取得ステップの処理により取得されたクライアント情報に含まれる情報により特定されるアプリケーションに応じたメッセージを含むデータを制御対象とするICチップに送信するコマンド送信ステップとを含むことを特徴とする。

【００２７】

本発明のプログラムは、ICチップの種別と、所定のコマンドを実行させるクライアントにおけるICチップに実行させるコマンドの種別を対応付けて管理するとともに、ICチップの種別に対応付けて、ICチップとの認証方法と、ICチップに実行させるコマンドを含む、ICチップに送信するデータに施す暗号化の方法を管理する管理ステップと、制御対象とするICチップの種別を含むICチップ情報と、クライアントにおいて実行されるアプリケーションを特定する情報を含むクライアント情報とを、クライアントから情報管理装置自身に対する接続要求と共に取得する取得ステップと、管理ステップの処理により管理されている複数の異なる種別のコマンドのうち、取得ステップの処理により取得されたICチップ情報に含まれるICチップの種別に対応付けられている種別のコマンドを作成するコマンド作成ステップと、コマンド作成ステップの処理により作成されたコマンドを含む制御対象とするICチップに送信するデータに、対応付けられたICチップの種別に応じて暗号化を施す暗号化ステップと、暗号化ステップの処理により暗号化されたコマンドと、取得ステップの処理により取得されたクライアント情報に含まれる情報により特定されるアプリケーションに応じたメッセージを含むデータを制御対象とするICチップに送信するコマンド送信ステップとを含むことを特徴とする。

【００２８】
本発明の情報管理装置および方法、並びにプログラムにおいては、制御対象とするICチップの種別を含むICチップ情報と、クライアントにおいて実行されるアプリケーションを特定する情報を含むクライアント情報とが、クライアントから情報管理装置自身に対する接続要求と共に取得され、管理されている複数の異なる種別のコマンドのうち、ICチップ情報に含まれるICチップの種別に対応付けられている種別のコマンドが作成される。また、作成されたコマンドを含む制御対象とするICチップに送信するデータに、対応付けられたICチップの種別に応じて暗号化が施され、暗号化されたコマンドと、取得されたクライアント情報に含まれる情報により特定されるアプリケーションに応じたメッセージを含むデータが制御対象とするICチップに送信される。

【発明の効果】
【００２９】
本発明によれば、１つのサーバからの要求に応じて、複数の異なる種別のICチップに対応したコマンドを作成することができる。
【発明を実施するための最良の形態】
【００３６】
以下、本発明の実施の形態について図を参照して説明する。
【００３７】
図２は、本発明を適用したサーバ－クライアントシステム（システムとは、複数の装置が論理的に集合した物をいい、各構成の装置が同一筐体中にあるか否かは問わない）の構成例を示す図である。
【００３８】
図２のサーバ－クライアントシステムは、いわゆるクライアントである各種のクライアント側装置３１と、いわゆるサーバであるサーバ側装置３２とが、例えば、インターネットなどのネットワーク３３、さらには、必要に応じて、例えば、移動機（体）通信網などのネットワーク３４を介して接続されて構成されている。
【００３９】
クライアント側装置３１はセキュアチップを内蔵している。セキュアチップは、耐タンパ性のあるセキュアなICチップであり、接触または非接触で他の装置とデータのやりとりを行うことができるようになっている。
【００４０】
なお、クライアント側装置３１としては、例えば、携帯電話機やPDA(Personal Digital Assistant)などの携帯端末、PC, POS(Point Of Sales)レジ（POSシステム用のレジスタ）、自動販売機、ハンディターミナルなどがある。また、クライアント側装置３１が内蔵するセキュアチップとしては、例えば、電子的な定期券等としてのSuica（登録商標）などに採用されているFeliCa（登録商標）などがある。
【００４１】
サーバ側装置３２は、ネットワーク３３、さらには、必要に応じてネットワーク３４を介して、クライアント側装置３１との間でデータをやりとりし、これにより、各種のサービスを提供する。即ち、例えば、クライアント側装置３１のセキュアチップに電子マネーが記憶されている場合、サーバ側装置３２が、クライアント側装置３１の電子マネーを対象として、商品の代金を差し引き、その差し引き後の金額になるようにクライアント側装置３１の電子マネーを更新する処理などを制御することにより、サーバ側装置３２は電子マネーサービスを提供する。
【００４２】
なお、クライアント側装置３１は、サーバ側装置３２に送信するデータを暗号化して送信し、サーバ側装置３２も、クライアント側装置３１に送信するデータを暗号化して送信する。
【００４３】

クライアント側装置３１における暗号化、さらには、暗号化されたデータの復号などの暗号処理は、耐タンパ性のあるセキュアチップ内で行われるが、サーバ側装置３２における暗号処理は、耐タンパ性のある専用のハードウェアであるHSM(Hardware Security Module)内で行われる場合と、そのような耐タンパ性のあるHSMを利用せず、サーバ側装置３２を実現するソフトウェアなどで行われる場合がある。

【００４４】

また、暗号処理には、特に高い秘匿性が要求される暗号処理と、それ以外の暗号処理とがあり、サーバ側装置３２がHSMを備える場合には、特に高い秘匿性が要求される暗号処理のみをHSM内で行い、それ以外の暗号処理をサーバ側装置３２を実現するソフトウェアなどで行うことができる。

【００４５】

図３は、クライアント側装置３１とサーバ側装置３２の機能的な構成例を示すブロック図である。

【００４６】

クライアント側装置３１は、セキュアチップ４１およびクライアントアプリケーション４２、さらには、必要なR/W４３で構成される。

【００４７】

セキュアチップ４１は、耐タンパ性のあるセキュアなICチップであり、接触または非接触で、他の装置とデータのやりとりを行う。

【００４８】

即ち、セキュアチップ４１は、クライアントアプリケーション４２と直接、またはR/W４３を介して通信を行い、例えば、その通信によってクライアントアプリケーション４２から送信されてくるコマンドにしたがって処理を行う。また、セキュアチップ４１は、その処理後、コマンドに対するレスポンスとしてのレスポンスデータを、クライアントアプリケーション４２に対して、直接、またはR/W４３を介して送信する。セキュアチップ４１は、セキュリティを確保するために、送受信するデータ等に対する暗号処理も行う。

【００４９】

クライアントアプリケーション４２は、例えば、ハードウェアであるコンピュータで実行されるソフトウェアであり、サーバ側装置３２の後述するサーバアプリケーション５１のクライアントとして機能する。サーバアプリケーション５１のクライアントとして機能し、セキュアチップ４１にコマンドなどを送信したりするから、クライアントアプリケーション４２は、通信経路上、セキュアチップ４１とサーバアプリケーション５１の間に存在する。

【００５０】

クライアントアプリケーション４２は、サーバアプリケーション５１との間でデータ（コマンドを含む）をやりとりし、また、セキュアチップ４１に対して、直接、またはR/W４３を介してコマンド等を送信することで、セキュアチップ４１に対するデータの読み書き等を行い、これにより各種のサービスを実現する。

【００５１】

即ち、例えば、クライアントアプリケーション４２およびサーバアプリケーション５１が、電子マネーサービスを提供するソフトウェアであり、セキュアチップ４１内に電子マネーサービス用の記憶領域が確保されている場合、セキュアチップ４１に記憶された電子マネーから、商品の代金を差し引き、その差し引き後の金額になるように、セキュアチップ４１に記憶された電子マネーの金額を更新するといった、電子マネーサービスのための処理に必要なデータ（コマンドを含む）のやりとりがクライアントアプリケーション４２とサーバアプリケーション５１との間で行われる。

【００５２】

なお、クライアントアプリケーション４２には、サーバアプリケーション５１との間の通信を制御するモジュールが必要に応じて含まれる。

【００５３】

R/W４３は、セキュアチップ４１と非接触通信または接触通信を行い、クライアントアプリケーション４２から供給されるコマンド等をセキュアチップ４１に送信し、また、セキュアチップ１２から送信されてくるデータ等を受信して、クライアントアプリケーション４２に供給する。

【００５４】

サーバアプリケーション５１は、例えば、ハードウェアであるコンピュータで実行されるソフトウェアであり、クライアント側装置３１のクライアントアプリケーション４２のサーバとして機能する。サーバアプリケーション５１は、クライアントアプリケーション４２との間でデータ（コマンドを含む）をやりとりすることにより、上述した電子マネーサービスその他の各種のサービスを実現する。

【００５５】

また、サーバアプリケーション５１は、セキュリティを確保するため、送受信するデータ等に対する暗号処理をセキュアサーバ５２に依頼する。

【００５６】

なお、サーバアプリケーション５１には、クライアントアプリケーション４２との間の通信を制御するモジュールが必要に応じて含まれる。

【００５７】

セキュアサーバ５２は、例えば、ハードウェアであるコンピュータで実行されるソフトウェアであり、サーバアプリケーション５１からの暗号処理の依頼に応じて、自身で暗号処理を行い、あるいは、暗号処理をセキュアチップ処理モジュール５３に依頼する。

【００５８】

即ち、セキュアサーバ５２は、サーバアプリケーション５１から依頼される暗号処理のうちの、特に高い秘匿性が要求される暗号処理をセキュアチップ処理モジュール５３に依頼し、それ以外の暗号処理を自身（セキュアサーバ５２内）で行う。

【００５９】

セキュアチップ処理モジュール５３は、セキュアサーバ５２からの依頼に応じて、暗号処理（特に高い秘匿性が要求される暗号処理）を行う。

【００６０】

なお、セキュアチップ処理モジュール５３は、ここでは、例えば、耐タンパ性のある専用のハードウェア内に格納されていることとする。但し、セキュアチップ処理モジュール５３は、例えば、セキュアサーバ５２の１つのモジュール（ソフトウェア）とすることも可能である。セキュアチップ処理モジュール５３を格納するハードウェアが、例えば、図１のSAM２に対応する。

【００６１】

図４は、クライアント側装置３１とサーバ側装置３２の具体的なハードウェアの構成例を示すブロック図である。

【００６２】

図４において、クライアント側装置３１は、R/W４３，ICカード６１、およびPC６２で構成されている。

【００６３】

ICカード６１は、ハードウェアであるセキュアチップ４１を内蔵し、例えば、電子マネーを格納するEdy（登録商標）などのカードに相当する。

【００６４】

PC６２は、例えば、ICカード６１のユーザが所有するPCであり、そこには、クライアントアプリケーション４２がインストールされる。ユーザは、PC６２を操作することにより、ICカード６１（セキュアチップ４１）に格納されている電子マネーの残高照会や、電子マネーのチャージ等を行うことができる。

【００６５】

図４において、サーバ側装置３２は、セキュアチップ処理モジュール５３およびコンピュータ６３で構成されている。

【００６６】
コンピュータ６３は、例えば、ハードウェアとしてのサーバ（マシン）で、そこには、サーバアプリケーション５１とセキュアサーバ５２がインストールされる。
【００６７】
図５は、クライアント側装置３１とサーバ側装置３２の具体的なハードウェアの他の構成例を示すブロック図である。なお、図５において、サーバ側装置３２のハードウェア構成は、図４における場合と同様である。
【００６８】
図５において、クライアント側装置３１は携帯電話機６４で構成されている。
【００６９】
携帯電話機６４は、ハードウェアであるセキュアチップ４１を内蔵している。さらに、携帯電話機６４には、クライアントアプリケーション４２がインストールされる。ユーザは、携帯電話機６４を操作することにより、例えば、セキュアチップ４１に格納されている電子マネーの残高照会や、電子マネーのチャージ等を行うことができる。
【００７０】
なお、携帯電話機６４が内蔵するセキュアチップ４１へのアクセスは、携帯電話機６４が有する通信機能を利用して行うこともできるし、また、図５では図示していないR/W４３に対して携帯電話機６４（携帯電話機６４が内蔵するセキュアチップ４１）を近づけることにより行うこともできる。
【００７１】
図６は、クライアントアプリケーション４２がインストールされる図４のPC６２のハードウェア構成例を示すブロック図である。
【００７２】
PC６２は、CPU(Central Processing Unit)７２を内蔵している。CPU７２には、バス７１を介して入出力インタフェース８０が接続されており、CPU７２は、入出力インタフェース８０を介して、ユーザによって、キーボードや、マウス、マイク等で構成される入力部７７が操作等されることにより指令が入力されると、それにしたがって、ROM(Read Only Memory)７３に格納されているプログラムを実行する。
【００７３】
また、CPU７２は、ハードディスク７５に格納されているプログラム、衛星若しくはネットワークから転送され、通信部７８で受信されてハードディスク７５にインストールされたプログラム、またはドライブ７９に装着されたリムーバブル記録媒体８１から読み出されてハードディスク７５にインストールされたプログラムをRAM(Random Access Memory)７４にロードして実行する。
【００７４】
これにより、CPU７２は各種の処理を行う。そして、CPU７２は、その処理結果を、必要に応じて、例えば、入出力インタフェース８０を介してLCD(Liquid Crystal Display)やスピーカ等で構成される出力部７６から出力、または、通信部７８から送信、さらには、ハードディスク７５に記録等させる。
【００７５】
なお、入出力インタフェース８０には、例えば、USB(Universal Serial Bus)端子が設けられており、図４のR/W４３は、そのUSB端子に接続することができる。
【００７６】
図７は、サーバアプリケーション５１およびセキュアサーバ５２がインストールされる図４のコンピュータ６３のハードウェア構成例を示すブロック図である。
【００７７】
図７において、コンピュータ６３を構成するバス９１乃至リムーバブル記録媒体１０１は、図６のバス７１乃至リムーバブル記録媒体８１とそれぞれ同様に構成されるものであるため、その説明は省略する。
【００７８】

図８は、図３のセキュアチップ４１のハードウェア構成例を示すブロック図である。

【００７９】

セキュアチップ４１は、大きく分けて、通信処理部１１１とデータ処理部１１２とから構成される。通信処理部１１１は、接触して、または非接触で、セキュアチップ４１の外部と通信するために必要な処理を行い、これにより、外部から送信されてくるデータ（コマンドを含む）をデータ処理部１１２に供給し、また、データ処理部１１２からのデータを外部に送信する。セキュアチップ４１で行われる、外部と通信するために必要な処理としては、データ等の符号化／復号や、変調／復調等がある。

【００８０】

データ処理部１１２は、例えば、CPU１２１、暗号処理部１２２、およびメモリ１２３で構成され、通信処理部１１１から供給されるコマンドにしたがい、各種の処理を行う。

【００８１】

即ち、CPU１２１は、暗号処理部１２２の制御やメモリ１２３の管理を行う。また、CPU１２１は、通信処理部１１１から供給されるコマンドにしたがい、メモリ１２３に対するデータの読み書きや、メモリ１２３に記憶されたデータを対象としたデータ処理等を行う。なお、CPU１２１は、プログラムを実行することにより各種の処理を行うが、そのプログラムはメモリ１２３に記憶されている。

【００８２】

暗号処理部１２２は、CPU１２１の制御にしたがい、データ（コマンドを含む）の暗号化／復号の暗号処理の他に、例えば、いわゆるチャレンジアンドレスポンス方式での認証に用いる乱数の発生、暗号化／復号に用いる鍵（暗号鍵となる情報）の発生（生成）などの認証処理も行う。即ち、暗号処理部１２２は、暗号化されたデータを用いた各種の処理を行う。

【００８３】

メモリ１２３は不揮発性のメモリであり、データやプログラムなどを記憶する。なお、メモリ１２３は、物理的に１つのメモリであっても良いし、複数のメモリであっても良い。また、メモリ１２３を物理的に複数のメモリで構成する場合には、その一部のメモリとして揮発性のメモリを採用することができる。

【００８４】

CPU１２１では、図９に示すように、メモリ１２３の記憶領域が階層化されて管理される。

【００８５】

図９は、メモリ１２３のディレクトリ構造を示す図である。

【００８６】

メモリ１２３の記憶領域のうちの一部は、各種のサービスを提供するためのデータを記憶するデータ記憶領域として使用される。このデータ記憶領域は、いわゆるディレクトリに相当するエリア定義領域を階層とする階層構造をなしており、エリア定義領域は、エリア定義領域およびサービス定義領域を有することができるようになされている。

【００８７】

エリア定義領域は、メモリ１２３のデータ記憶領域の一部であり、サービスを提供するサービス提供者を管理する管理者（サービス提供者自身である場合もある）に割り当てられる。エリア定義領域には、そのエリア定義領域を識別するための名前として使用可能な識別コードとしてのエリアコード、使用可能な空きブロック数を表す空き容量、エリア定義領域（そのエリア定義領域の下位階層のエリア定義領域やサービス定義領域を含む）にアクセスするのに必要な鍵としてのエリアキーなどが配置される。

【００８８】

図９の実施の形態では、管理者Ａに割り当てられたエリア定義領域が最上位階層を構成しており、これを親の階層として、管理者Ｂ１およびＢ２のエリア定義領域が作成されている。さらに、管理者Ｂ１のエリア定義領域を親の階層として、管理者Ｃのエリア定義領域が作成されている。

【００８９】
サービス定義領域は、後述するサービス領域を管理するためのメモリ１２３のデータ記憶領域の一部であり、サービス提供者が提供するサービスに割り当てられる。サービス定義領域には、そのサービス定義領域を識別するための名前として使用可能な識別コードとしてのサービスコード、サービスの提供に必要なデータを記憶するサービス領域の容量を表すブロック数、サービス定義領域（サービス定義領域が管理するサービス領域を含む）にアクセスするのに必要な鍵としてのサービスキーなどが配置される。
【００９０】
サービス領域は、データ記憶領域の一部であり、サービスの提供に必要なデータが記憶される、０以上のブロックで構成される。サービス領域を構成するブロック数が、そのサービス領域を管理するサービス定義領域の容量として配置される。
【００９１】
ここで、CPU１２１は、メモリ１２３のデータ記憶領域を、固定の記憶容量のブロック単位で管理するようになっており、図９における空き容量やサービス領域の容量は、このブロックの数によって管理される。
【００９２】
サービス提供者は、ある管理者が管理するエリア定義領域の下位階層にサービス定義領域を作成し、そのサービス定義領域で管理されるサービス領域を使用して、各種のサービスを提供する。例えば、電子マネーサービスの提供にあたっては、サービス領域に、例えば、電子マネーの金額（残額）や、電子マネーによって購入した商品の情報（例えば、商品名や値段など）などが記憶される。
【００９３】
図１０は、図３のセキュアサーバ５２の詳細な構成例を示すブロック図である。
【００９４】
セキュアサーバ５２は、セキュアチップコマンドモジュール１３１とセキュアチップマネージャモジュール１３２とから構成される。
【００９５】
セキュアチップコマンドモジュール１３１は、例えば、サーバアプリケーション５１からのコマンドの作成の要求（依頼）に応じて、制御対象としているセキュアチップ４１用のコマンドを作成し、サーバアプリケーション５１に供給する。即ち、サーバアプリケーション５１は、クライアント側装置３１のセキュアチップに対して何らかの処理を指示する場合、その処理に対応するコマンドの作成をセキュアチップコマンドモジュール１３１に要求する。
【００９６】
セキュアチップコマンドモジュール１３１は、後述するように、いま制御対象としているセキュアチップ４１のチップ種別を取得し、サーバアプリケーション５１からの要求に応じて、セキュアチップ４１のチップ種別に応じたコマンドを作成して、それをセキュアチップ４１用のコマンドとする。セキュアチップコマンドモジュール１３１により作成されたセキュアチップ４１用のコマンドはサーバアプリケーション５１に供給される。
【００９７】
従って、サーバアプリケーション５１は、制御対象としているセキュアチップ４１用のコマンドを（知っていても良いが）知っている必要はないので、様々なコマンド体系のセキュアチップ（コマンドとしてのオペコードや、コマンドがとるパラメータ、コマンドの種類などの違いがあるセキュアチップ）が存在する場合であっても、サーバアプリケーション５１を、そのような様々なコマンド体系のセキュアチップごとに製作する必要がない。
【００９８】
即ち、サーバアプリケーション５１は、セキュアチップコマンドモジュール１３１が解釈することができるコマンド体系を使用することができるものであれば良く、これにより、１つのサーバアプリケーション５１で複数の異なる種別のセキュアチップ４１に対応す

ることができる。

【００９９】

ここで、セキュアチップコマンドモジュール１３１は、サーバアプリケーション５１からの要求に応じて、セキュアチップ４１用のコマンドを作成し、サーバアプリケーション５１に供給するが、コマンドをサーバアプリケーション５１に供給する前に、セキュアチップマネージャモジュール１３２に供給して、そのコマンドの暗号化を要求する。そして、セキュアチップコマンドモジュール１３１は、その要求に応じてセキュアチップマネージャモジュール１３２から供給される暗号情報（暗号化後のコマンド等）を、サーバアプリケーション５１に供給する。

【０１００】

セキュアチップマネージャモジュール１３２は、制御対象としているセキュアチップ４１の種別と対応付けて、そのセキュアチップ４１に実行させるコマンドの種別と、そのセキュアチップ４１に実行させるコマンドの暗号化の方法や、セキュアチップ４１との間で行う認証方法を含む暗号処理の種別とを管理しており、サーバアプリケーション５１から通知されてきた、いま、制御対象としているセキュアチップの種別に基づいてコマンドの種別と暗号処理の種別（以下、適宜、それぞれ、コマンド種別、暗号処理種別という）を選択する。

【０１０１】

例えば、セキュアチップマネージャモジュール１３２により選択されたコマンド種別はセキュアチップコマンドモジュール１３１に通知され、セキュアチップコマンドモジュール１３１において、セキュアチップマネージャモジュール１３２から通知されたコマンド種別のコマンドが作成される。これにより、上述したように、いま制御対象としているセキュアチップ用のコマンドが作成されることになる。

【０１０２】

図１１は、セキュアチップマネージャモジュール１３２により管理される対応テーブルの例を示す図である。

【０１０３】

図１１の対応テーブルにおいては、「FeliCa１」、「FeliCa２」、「GP１」、および「GP２」のそれぞれのセキュアチップの種別（Chip種別）に対して、コマンド種別と暗号処理種別が対応付けられている。

【０１０４】

例えば、「FeliCa１」に対しては、コマンド種別「Type１１」と暗号処理種別「Type１２」が対応付けられ、「FeliCa２」に対しては、コマンド種別「Type１２」と暗号処理種別「Type１２」が対応付けられている。同様に、「GP１」に対しては、コマンド種別「Type２１」と暗号処理種別「Type２１」が対応付けられ、「GP２」に対しては、コマンド種別「Type２２」と暗号処理種別「Type２１」が対応付けられている。

【０１０５】

例えば、セキュアチップマネージャモジュール１３２は、サーバアプリケーション５１から、いま制御対象としているセキュアチップ４１の種別が「FeliCa１」であることが通知されてきた場合、図１１の対応テーブルから、コマンド種別「Type１１」を選択し、コマンド種別が「Type１１」であることをセキュアチップコマンドモジュール１３１に通知する。セキュアチップコマンドモジュール１３１においては、いま制御対象としているセキュアチップ４１の種別「FeliCa１」に関与するコマンドが組み合わされることによって「Type１１」の種別のコマンドが作成され、それが、セキュアチップ４１用のコマンドとされる。

【０１０６】

具体的には、例えば、issueコマンド、Readコマンド、Writeコマンドの３種類のコマンドが規定されているものとし、サーバアプリケーション５１からそのうちのissueコマンドが要求された場合、セキュアチップコマンドモジュール１３１においては、セキュアチップマネージャモジュール１３２から通知されている、いま制御対象としているセキュア

チップ４１の種別に関与するコマンドが組み合わされることによって、「RegisterCommand」、および「CommitCommand」が作成される。即ち、この場合、issueコマンドに対して、セキュアチップ４１の種別「FeliCa１」に関与するコマンド「RegisterCommand」と「CommitCommand」の両者が対応付けられており、セキュアチップの種別に応じて一意に特定のセキュアチップに対応するコマンド群が選択される。

【０１０７】

また、セキュアチップマネージャモジュール１３２は、図１１の対応テーブルから選択した暗号処理種別「Type１２」（いま制御対象としている「FeliCa１」の種別のセキュアチップ４１の暗号処理種別）に応じて自分自身でコマンドの暗号処理を行い、また、暗号処理種別「Type１２」に応じた暗号処理が行われるようにセキュアチップ処理モジュール５３による暗号処理を制御する。

【０１０８】

暗号処理には次のようなものがあり、例えば、セキュアチップ４１の種別に応じて次の暗号処理が適宜組み合わされることによって、制御対象のセキュアチップ４１との間で使用する暗号処理が決定される。

【０１０９】

１．認証方法

（１）サーバ側装置３２－セキュアチップ４１間にて相互の認証を行うか、または、片側の認証を行うか

（２）相互または片側の認証と同時に、後述する通信路暗号用のセッション鍵を共有するか否か

２．コマンドの暗号化方法（通信路の暗号化方法）

（１）コマンドの全体を暗号化するか、一部を暗号化するか

（２）暗号化するための暗号鍵を、セッション単位で異なるもの（セッション鍵）を用いるか否か

３．後述する特別なコマンドを実行する実行権を表す権利書（のデータ）の暗号処理の方法

（１）実行権を表す権利書に所定の鍵を用いた暗号化を施すか

（２）実行権を表す権利書に署名を付加するか

（３）実行権を表す権利書を所定のハッシュ関数を適用してハッシュ値を得るか

【０１１０】

具体的には、いま制御対象としているセキュアチップ４１の種別に応じて、サーバ側装置３２－セキュアチップ４１間の認証方法（１．の選択）として相互の認証を行うこと、その相互の認証と同時に通信路暗号用のセッション鍵を共有すること、コマンドの暗号化方法（２．の選択）としてコマンドの全体を暗号化すること、暗号化するための暗号鍵をセッション単位で異なるものを用いること、実行権を表す権利書の暗号処理の方法（３．の選択）として実行権を表す権利書に暗号化を施さず、また、ハッシュ関数を適用しないが署名を付加すること、が選択される。

【０１１１】

また、認証や通信路の暗号化、実行権の暗号処理において具体的に用いられる暗号・署名アルゴリズム(DES、T-DES、RSA、EC-DSAなど)や認証でのチャレンジ/レスポンスの方法や具体的な暗号・署名を行う対象のフォーマットやパディングルールなどもセキュアチップ種別により特定される。

【０１１２】

これにより、サーバアプリケーション５１は、制御対象としているセキュアチップ４１の種別を気にすることなく、上述したようなissueコマンド、Readコマンド、Writeコマンドを要求するだけで、チップ種別に応じたセキュアチップ４１用のコマンドであって、かつ、コマンド全体に暗号化が施されたものなど、セキュアチップの種別に応じた暗号処理が行われたコマンドを得ることができる。このことは、サーバアプリケーション５１から見ればコマンドや暗号処理のいわば仮想化が行われているといえる。

【０１１３】
図１２は、コマンドと暗号処理の仮想化の具体例について示す図である。
【０１１４】
例えば、図１２に示すように、パラメータ１および２のパラメータデータを含むissueコマンドの作成がサーバアプリケーション５１から要求されたとき、そのうちのパラメータ２に対しては、「Type１２」で識別される暗号処理（図中の「実際の暗号処理方法」で示す暗号処理）が施される。なお、図１２においては、暗号処理の種別は、まず、「Type１」と「Type２」に分岐し、そのうちの「Type１」はさらに「Type１１」と「Type１２」に分岐している。また、「Type２」はさらに「Type２１」と「Type２２」に分岐している。
【０１１５】
制御対象のセキュアチップ４１の種別に関係なく、サーバアプリケーション５１がパラメータ１および２を含むissueコマンドの作成を要求するだけで、そのセキュアチップ４１の種別に応じた種別の暗号処理としてパラメータ２に暗号化が施されるから、これにより、暗号処理の仮想化が実現される。
【０１１６】
同様に、例えば、図１２に示すように、パラメータ１および２のパラメータデータを含むWriteコマンドの作成がサーバアプリケーション５１から要求されたとき、パラメータデータ部分を除くコマンド部分として、「Type１２」で識別されるコマンド（図中の「実際のコマンド」で示すコマンド）が選択される。なお、図１２においては、コマンドの種別は、まず、「Type１」と「Type２」に分岐し、そのうちの「Type１」はさらに「Type１１」と「Type１２」に分岐している。また、「Type２」はさらに「Type２１」と「Type２２」に分岐している。
【０１１７】
制御対象のセキュアチップ４１の種別に関係なく、サーバアプリケーション５１がパラメータ１および２を含むWriteコマンドを要求するだけで、セキュアチップ４１の種別に応じた種別のコマンドとして「Type１２」のコマンドが選択されるから、これにより、コマンドの仮想化が実現される。
【０１１８】
図１０の説明に戻り、また、セキュアチップマネージャモジュール１３２は、自身（セキュアチップマネージャモジュール１３２）またはセキュアチップ処理モジュール５３による暗号処理により得られる暗号情報をセキュアチップコマンドモジュール１３１に供給する。
【０１１９】
次に、図１３のフローチャートを参照して、クライアント側装置３１とサーバ側装置３２の動作について説明する。
【０１２０】
クライアントアプリケーション４２が起動されると、クライアントアプリケーション４２は、まず最初に、ステップＳ２１において、セキュアチップ４１に対して、セキュアチップに関するセキュアチップ(Secure Chip)情報を要求するコマンドを送信する。
【０１２１】
セキュアチップ４１は、ステップＳ１１において、クライアントアプリケーション４２からのコマンドを受信して、ステップＳ１２に進み、そのコマンドに対するレスポンスとして、セキュアチップ情報をクライアントアプリケーション４２に送信する。
【０１２２】
クライアントアプリケーション４２は、ステップＳ２２において、セキュアチップ４１からのセキュアチップ情報を受信して、ステップＳ２３に進み、そのセキュアチップ情報を含む初期情報とともに、サーバ側装置３２に対して、接続を要求するサーバ(Server)接続要求を送信する。
【０１２３】

なお、初期情報には、セキュアチップ情報の他、クライアントアプリケーション４２に関するクライアント情報や、クライアントアプリケーション４２が接続しようとするサーバ側装置３２のサーバアプリケーション５１を指定するサーバ(Server)アプリ指定（の情報）が含まれる。

【０１２４】

また、セキュアチップ情報としては、セキュアチップ４１がどのような種類のものかを表す情報であるセキュアチップ種別、セキュアチップ４１で採用されているOS(Operating System)を表す情報であるセキュアチップOS種別、セキュアチップ４１におけるデータの管理に関する情報であるセキュアチップファイル構造(ファイルフォーマット、エリアコードのリスト、サービスコードのリストなど)などがある。これにより、サーバ側装置３２において、いま制御対象としているセキュアチップ４１の種別が特定される。

【０１２５】

さらに、クライアント情報としては、クライアント側装置３１のハードウェアを表す情報（例えば、クライアント側装置３１が携帯電話機、PC、またはPOSレジであるなどの情報）であるクライアント種別、クライアント側装置３１で採用されているOSを表す情報であるクライアントOS種別、クライアントアプリケーション４２を特定する情報であるクライアントアプリID(Identification)、クライアントアプリケーション４２のバージョンを表す情報であるアプリバージョンなどがある。

【０１２６】

ここで、クライアントアプリケーション４２では、例えば、サーバアプリケーション５１に接続した後に行われる、セキュアチップ情報その他の初期情報のサーバアプリケーション５１からの要求に応じて、セキュアチップ４１からセキュアチップ情報を取得し、取得したセキュアチップ情報を初期情報に含めてサーバアプリケーション５１に送信することもできる。

【０１２７】

但し、図１３に示すように、クライアントアプリケーション４２において、セキュアチップ４１からセキュアチップ情報を取得してから、そのセキュアチップ情報を含む初期情報をサーバ接続要求とともにサーバアプリケーション５１に送信する場合の方が、クライアントアプリケーション４２とサーバアプリケーション５１との間のやりとりが少なくて済む。

【０１２８】

さらに、この場合、サーバ側装置３２は、クライアント側装置３１からのアクセスの開始と同時にクライアント情報を受信することができるので、そのクライアント情報に基づき、クライアントアプリケーション４２に適したコマンドやメッセージ（画面等のGUI(Graphical User Interface)など）の送受信を行うことが可能となる。ここで、クライアントアプリケーション４２に適したコマンドやメッセージとは、例えば、内容がクライアントアプリケーション４２に適したコマンドやメッセージ、あるいは、一度に送受信する長さや個数がクライアントアプリケーション４２に適したコマンドやメッセージなどを意味する。

【０１２９】

サーバアプリケーション５１は、ステップＳ４１において、クライアントアプリケーション４２からのサーバ接続要求と初期情報を受信し、クライアント側装置３１に必要なサービスを提供するためのアプリケーション（ソフトウェア）を起動して、ステップＳ４２に進む。

【０１３０】

ステップＳ４２では、サーバアプリケーション５１は、ステップＳ４１で受信した初期情報に含まれるセキュアチップ情報とクライアント情報をセキュアサーバ５２のセキュアチップマネージャモジュール１３２に供給する。

【０１３１】

セキュアチップマネージャモジュール１３２は、ステップＳ１１１において、サーバア

プリケーション５１からのセキュアチップ情報とクライアント情報を受信し、そのうちのセキュアチップ情報をセキュアチップ処理モジュール５３に供給する。

【０１３２】

セキュアチップ処理モジュール５３は、ステップＳ１５１において、セキュアチップマネージャモジュール１３２からのセキュアチップ情報に基づき、セキュアチップ４１からのアクセスに対する処理の範囲を設定する。

【０１３３】

即ち、セキュアチップ処理モジュール５３は、様々なセキュアチップやサービスの暗号処理を行うことができるようになっており、さらに、その様々なセキュアチップやサービスの暗号処理に必要な鍵を内蔵している（セキュアチップ４１のメモリ１２３に形成された各領域に設定されている鍵に対応する鍵も内蔵している）。

【０１３４】

そして、セキュアチップ４１が、例えば、電子マネーサービスのみの提供を受けうるものであれば、セキュアチップ処理モジュール５３は、セキュアチップ４１からのアクセスに対して、電子マネーサービスを提供するのに必要な処理のみを行う（許可する）。また、電子マネーサービスにおけるデータの暗号化／復号に使用する鍵があらかじめ決まっている場合には、セキュアチップ処理モジュール５３は、セキュアチップ４１からのアクセスに対して、電子マネーサービスにおけるデータの暗号化／復号に使用する鍵のみの使用のみを許可し、他のサービスにおけるデータの暗号化／復号に使用する鍵の使用は許可しない。

【０１３５】

一方、セキュアチップマネージャモジュール１３２は、ステップＳ１１１でサーバアプリケーション５１から受信したセキュアチップ情報とクライアント情報に基づき、いま制御対象としているセキュアチップ４１とクライアントアプリケーション４２に対応した処理を行う状態となる。

【０１３６】

即ち、セキュアチップマネージャモジュール１３２は、サーバアプリケーション５１から供給されてきたセキュアチップ情報に基づいて、いま制御対象としているセキュアチップ４１の種別を特定し、特定した種別に応じたコマンド種別と暗号処理種別を、図１１に示したような対応テーブルから選択する。これにより、以降の処理において作成、送信されるコマンドは、ここで選択された種別のコマンドとされ、以降の処理において必要な認証処理やコマンドの暗号処理などは、ここで選択された暗号処理種別に応じた処理とされる。

【０１３７】

そして、セキュアチップマネージャモジュール１３２は、ステップＳ１１２において、セキュアチップコマンドモジュール１３１に対し、初期化の指令を供給する。

【０１３８】

セキュアチップコマンドモジュール１３１は、ステップＳ７１において、その指令を受信し、自身の状態を、セキュアチップ４１に対応した処理を行うことができるように初期化する。例えば、ここでセキュアチップマネージャモジュール１３２から供給される初期化の指令には、セキュアチップマネージャモジュール１３２により選択されたコマンド種別を表す情報も含まれている。従って、これ以降、セキュアチップコマンドモジュール１３１は、コマンドの作成要求がサーバアプリケーション５１から供給されてきたとき、いま制御対象としているセキュアチップ４１の種別に応じた種別のコマンドを作成することが可能になる。

【０１３９】

その後、例えば、サーバアプリケーション５１とセキュアチップ処理モジュール５３の間で相互認証が行われ、その認証が成功すると、次に、セキュアチップ４１とセキュアチップ処理モジュール５３との間で認証が行われる。ここで行われる認証は、例えば、セキュアチップマネージャモジュール１３２により選択された暗号処理種別の認証とされる。

【０１４０】
なお、セキュアチップ４１とセキュアチップ処理モジュール５３との間の認証は、例えば、チャレンジアンドレスポンス方式で行われる。チャレンジアンドレスポンス方式では、セキュアチップ処理モジュール５３は（セキュアチップ４１でも同様）、乱数を発生し、その乱数を暗号化して、セキュアチップ４１との間でやりとりすることにより認証を行う。この認証が成功すると、例えば、その認証時に、セキュアチップ処理モジュール５３が発生した乱数が、セキュアチップ４１とセキュアチップ処理モジュール５３との間のセッションを識別するためのセッションキーとされる。
【０１４１】
この後、例えば、選択された暗号処理種別により、通信路暗号用のセッションキーを共有することが定められている場合、サーバ側装置３２では、セキュアチップ４１に送信するコマンド（コマンドに付随するパラメータその他のデータを含む）は、ここでの認証処理により生成されたセッションキーを鍵として暗号化されて、クライアント側装置３１に送信される。また、クライアント側装置３１でも、セキュアチップ４１からサーバ側装置３２に送信されるデータ等は、セキュアチップ４１においてセッションキーを鍵として暗号化されて、サーバ側装置３２に送信される。
【０１４２】
このように、クライアント側装置３１とサーバ側装置３２のそれぞれにおいて、データ等がセッションキーを鍵として暗号化されて送受信されることにより、そのクライアント側装置３１とサーバ側装置３２との間の通信路が暗号化、即ち、いわばVPN(Virtual Private Network)が実現される。
【０１４３】
サーバアプリケーション５１は、ステップＳ４３において、セキュアチップ４１に送信するコマンドの作成要求をセキュアチップコマンドモジュール１３１に供給し、セキュアチップコマンドモジュール１３１は、ステップＳ７２において、サーバアプリケーション５１からのコマンドの作成要求を受信する。
【０１４４】
そして、セキュアチップコマンドモジュール１３１は、ステップＳ７３において、サーバアプリケーション５１からのコマンドの作成要求に応じて、セキュアチップ４１用のコマンド（セキュアチップ４１の種別に応じたコマンド）を作成し、そのコマンドを暗号化して暗号情報とすることの要求をセキュアチップマネージャモジュール１３２に供給する。
【０１４５】
セキュアチップマネージャモジュール１３２は、ステップＳ１１３において、セキュアチップコマンドモジュール１３１からの、コマンドを暗号化して暗号情報とすることの要求を受信して、ステップＳ１１４に進み、その要求を、セキュアチップ処理モジュール５３に供給する。
【０１４６】
即ち、いまの場合、通信路の暗号化に用いられるセッションキーはセキュアチップ処理モジュール５３内にあるので、セキュアチップマネージャモジュール１３２は、そのセッションキーによるコマンドの暗号化をセキュアチップ処理モジュール５３に要求する。
【０１４７】
セキュアチップ処理モジュール５３は、ステップＳ１５２において、セキュアチップマネージャモジュール１３２からの要求を受信し、その要求に応じて、コマンドを暗号化する。セキュアチップマネージャモジュール１３２からの要求には、例えば、暗号処理種別を表す情報も含まれているから、セキュアチップ処理モジュール５３においては、その種別に応じた暗号処理が適宜行われる。
【０１４８】
セキュアチップ処理モジュール５３は、ステップＳ１５３において、コマンドの暗号化により得られた暗号情報をセキュアチップマネージャモジュール１３２に供給する。

【０１４９】
セキュアチップマネージャモジュール１３２は、ステップＳ１１５において、セキュアチップ処理モジュール５３からの暗号情報を受信し、ステップＳ１１６に進み、セキュアチップ処理モジュール５３から受信した暗号情報をセキュアチップコマンドモジュール１３１に供給する。
【０１５０】
セキュアチップコマンドモジュール１３１は、ステップＳ７４において、セキュアチップマネージャモジュール１３２からの暗号情報を受信して、ステップＳ７５に進み、その暗号情報（暗号化されたコマンド）をサーバアプリケーション５１に供給する。
【０１５１】
サーバアプリケーション５１は、ステップＳ４４において、セキュアチップコマンドモジュール１３１からの暗号情報を受信して、ステップＳ４５に進み、その暗号情報（暗号化されたコマンド）を、クライアント側装置３１としてのハードウェアに対するメッセージであるデバイス用データとともにクライアントアプリケーション４２に送信する。
【０１５２】
クライアントアプリケーション４２は、ステップＳ２４において、サーバアプリケーション５１からの暗号情報およびデバイス用データを受信して、ステップＳ２５に進み、暗号情報をセキュアチップ４１に送信する。
【０１５３】
セキュアチップ４１は、ステップＳ１３において、クライアントアプリケーション４２からの暗号情報を受信し、その暗号情報を、セッションキーを用いてコマンドに復号する。また、セキュアチップ４１は、そのコマンドに応じた処理を実行し、ステップＳ１４において、そのコマンドに対応するレスポンスとしてのレスポンスデータをクライアントアプリケーション４２に送信する。なお、レスポンスデータは、セキュアチップ４１において、必要に応じて、セッションキーを用いて暗号化されている。
【０１５４】
クライアントアプリケーション４２は、ステップＳ２６において、セキュアチップ４１からのレスポンスデータを受信し、ステップＳ２７に進み、そのレスポンスデータをサーバアプリケーション５１に送信する。
【０１５５】
サーバアプリケーション５１は、ステップＳ４６において、クライアントアプリケーション４２からのレスポンスデータを受信し、そのレスポンスデータに応じた処理を行い、あるいは、そのレスポンスデータを、セキュアチップコマンドモジュール１３１、セキュアチップマネージャモジュール１３２に供給する。
【０１５６】
一方、セキュアチップマネージャモジュール１３２は、ステップＳ１１７において、セキュアチップ処理モジュール５３に対してセッションキーの要求を供給する。
【０１５７】
セキュアチップ処理モジュール５３は、ステップＳ１５４において、セキュアチップマネージャモジュール１３２からのセッションキーの要求を受信して、ステップＳ１５５に進み、その要求に応じて、セキュアチップ４１との認証で得たセッションキーをセキュアチップマネージャモジュール１３２に供給する。
【０１５８】
セキュアチップマネージャモジュール１３２は、ステップＳ１１８において、セキュアチップ処理モジュール５３からのセッションキーを受信して保持する。
【０１５９】
その後、例えば、セッションキーを用いた暗号化はセキュアチップマネージャモジュール１３２で行われ、より高い秘匿性が要求される暗号化のみがセキュアチップ処理モジュール５３内で行われる。なお、セキュアチップマネージャモジュール１３２により行われる暗号化、またはセキュアチップ処理モジュール５３により行われる暗号化は、セキュア

チップ処理モジュール５３により選択された種別に応じたもの（例えば、コマンドの全部を暗号化するとか、一部を暗号化することなど）とされる。

【０１６０】

このように、セッションキーを用いた暗号化をセキュアチップマネージャモジュール１３２で行い、より高い秘匿性が要求される暗号化（暗号化を利用して行われる相互認証や、後述するパッケージの作成などを含む）だけをセキュアチップ処理モジュール５３で行うようにすることにより、セキュアチップ処理モジュール５３において、すべての暗号処理を行う場合に比較して、セキュアチップ処理モジュール５３の負荷を軽減することができ、その結果、セキュアチップ処理モジュール５３における処理時間を短くすることができる。

【０１６１】

なお、耐タンパ性のあるセキュアチップ処理モジュール５３を複数設け、その複数のセキュアチップ処理モジュール５３に、処理を分散して行わせることにより、１つあたりのセキュアチップ処理モジュール５３の負荷を軽減することができる。

【０１６２】

その後、サーバアプリケーション５１は、ステップＳ４７において、セキュアチップ４１に送信するコマンドの作成の要求をセキュアチップコマンドモジュール１３１に供給する。

【０１６３】

セキュアチップコマンドモジュール１３１は、ステップＳ７６において、サーバアプリケーション５１からのコマンドの作成の要求を受信する。

【０１６４】

セキュアチップコマンドモジュール１３１は、ステップＳ７７において、サーバアプリケーション５１からのコマンドの作成の要求に応じて、セキュアチップ４１用のコマンド（コマンド種別に応じたコマンド）を作成し、そのコマンドを暗号化して暗号情報とすることの要求を、セキュアチップマネージャモジュール１３２に供給する。

【０１６５】

セキュアチップマネージャモジュール１３２は、ステップＳ１１９において、セキュアチップコマンドモジュール１３１からの、コマンドを暗号化して暗号情報とすることの要求を受信する。

【０１６６】

セキュアチップコマンドモジュール１３１からの要求が特別なコマンド以外のコマンドの暗号化の要求である場合には、セキュアチップマネージャモジュール１３２は、保持しているセッションキーでコマンドを暗号化し、ステップＳ１２２において、その結果得られる暗号情報をセキュアチップコマンドモジュール１３１に供給する。

【０１６７】

一方、セキュアチップコマンドモジュール１３１からの要求が特別なコマンドの暗号化の要求である場合、セキュアチップマネージャモジュール１３２は、ステップＳ１２０において、その特別なコマンドの実行権を作成するための暗号化の要求をセキュアチップ処理モジュール５３に供給する。

【０１６８】

ここで、特別なコマンドとしては、例えば、セキュアチップ４１に対するエリア定義領域やサービス定義領域の登録や削除を要求するコマンドなどがある。

【０１６９】

セキュアチップ処理モジュール５３は、ステップＳ１５６において、セキュアチップマネージャモジュール１３２からの要求を受信し、その要求に応じて、その特別なコマンドを実行する実行権を表す権利書（のデータ）に暗号処理を施す。ここで行われる暗号処理も、例えば、セキュアチップマネージャモジュール１３２により選択された種別の暗号処理とされる。

【０１７０】

さらに、セキュアチップ処理モジュール５３は、その権利書が正当なものであることを証明する証明書（のデータ）を、権利書の暗号化結果に付加し、ステップＳ１５７において、その証明書と権利書（の暗号化結果）とをパッケージとして、セキュアチップマネージャモジュール１３２に供給する。

【０１７１】

セキュアチップマネージャモジュール１３２は、ステップＳ１２１において、セキュアチップ処理モジュール５３からのパッケージを受信して、ステップＳ１２２に進み、特別なコマンドをセッションキーで暗号化し、その暗号化結果とパッケージとをセットにした暗号情報をセキュアチップコマンドモジュール１３１に供給する。

【０１７２】

セキュアチップコマンドモジュール１３１は、ステップＳ７８において、セキュアチップマネージャモジュール１３２からの暗号情報を受信して、ステップＳ７９に進み、その暗号情報をサーバアプリケーション５１に供給する。

【０１７３】

サーバアプリケーション５１は、ステップＳ４８において、セキュアチップコマンドモジュール１３１からの暗号情報を受信して、ステップＳ４９に進み、その暗号情報を、クライアント側装置３１としてのハードウェアに対するメッセージであるデバイス用データとともに、クライアントアプリケーション４２に送信する。

【０１７４】

クライアントアプリケーション４２は、ステップＳ２８において、サーバアプリケーション５１からの暗号情報およびデバイス用データを受信して、ステップＳ２９に進み、暗号情報をセキュアチップ４１に送信する。

【０１７５】

セキュアチップ４１は、ステップＳ１５において、クライアントアプリケーション４２からの暗号情報を受信し、その暗号情報をコマンドに復号する。さらに、セキュアチップ４１は、必要に応じて、コマンドの実行権を確認した上で、そのコマンドに応じた処理を実行し、ステップＳ１６において、そのコマンドに対応するレスポンスとしてのレスポンスデータをクライアントアプリケーション４２に送信する。

【０１７６】

クライアントアプリケーション４２は、ステップＳ３０において、セキュアチップ４１からのレスポンスデータを受信して、ステップＳ３１に進み、そのレスポンスデータをサーバアプリケーション５１に送信する。

【０１７７】

サーバアプリケーション５１は、ステップＳ５０において、クライアントアプリケーション４２からのレスポンスデータを受信し、そのレスポンスデータに応じた処理を行う。

【０１７８】

その後、サーバアプリケーション５１は、クライアント側装置３１との通信を終了する場合には、ステップＳ５１において、その旨のメッセージとしての終了通知をクライアントアプリケーション４２に送信する。

【０１７９】

クライアントアプリケーション４２は、ステップＳ３１において、サーバアプリケーション５１からの終了通知を受信する。これにより、一連の処理が終了される。

【０１８０】

上述した一連の処理は、ハードウェアにより実行させることもできるが、ソフトウェアにより実行させることもできる。

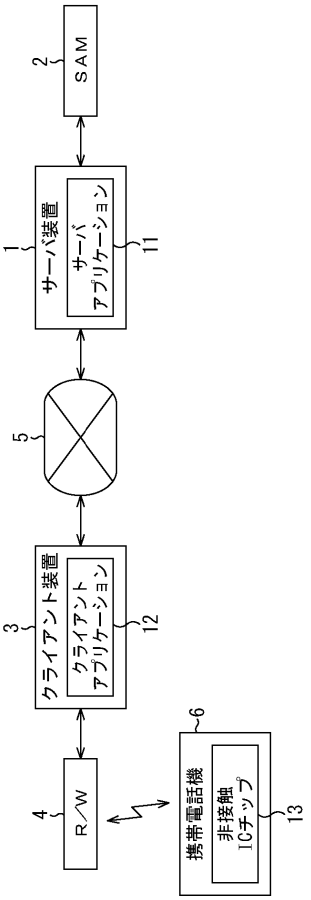
【０１８１】

一連の処理をソフトウェアにより実行させる場合には、そのソフトウェアを構成するプログラムが、専用のハードウェアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば、汎用のパーソナルコンピュータなどに、ネットワークや記録媒体からインストールされる。

【０１８２】
この記録媒体は、図６に示されるように、装置本体とは別に、ユーザにプログラムを提供するために配布される、プログラムが記録されている磁気ディスク（フレキシブルディスクを含む）、光ディスク（CD-ROM(Compact Disk-Read Only Memory), DVD(Digital Versatile Disk)を含む）、光磁気ディスク（MD（登録商標）(Mini-Disk)を含む）、もしくは半導体メモリなどよりなるリムーバブル記録媒体５１により構成されるだけでなく、装置本体に予め組み込まれた状態でユーザに提供される、プログラムが記録されているROM７３やハードディスク７５などで構成される。
【０１８３】
なお、本明細書において、各ステップは、記載された順序に従って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。
【０１８４】
また、本明細書において、システムとは、複数の装置により構成される装置全体を表わすものである。
【図面の簡単な説明】
【０１８５】
【図１】従来の電子マネーシステムの構成例を示すブロック図である。
【図２】本発明を適用したサーバ－クライアントシステムの構成例を示すブロック図である。
【図３】図２のクライアント側装置とサーバ側装置の機能構成例を示すブロック図である。
【図４】クライアント側装置とサーバ側装置のハードウェア構成の具体例を示すブロック図である。
【図５】クライアント側装置とサーバ側装置のハードウェア構成の他の具体例を示すブロック図である。
【図６】図４のPCのハードウェア構成例を示すブロック図である。
【図７】図４のコンピュータのハードウェア構成例を示すブロック図である。
【図８】図３のセキュアチップのハードウェア構成例を示すブロック図である。
【図９】セキュアチップのディレクトリ構造の例を示す図である。
【図１０】図３のセキュアサーバの詳細な構成例を示すブロック図である。
【図１１】セキュアチップマネージャモジュールにより管理される対応テーブルの例を示す図である。
【図１２】コマンドと暗号処理の仮想化の具体例について示す図である。
【図１３】クライアント側装置とサーバ側装置の動作について説明するフローチャートである。
【符号の説明】
【０１８６】
３１　クライアント側装置，　３２　サーバ側装置，　４１　セキュアチップ，　４２　R/W，　４３　クライアントアプリケーション，　５１　サーバアプリケーション，　５２　セキュアサーバ，　５３　セキュアチップ処理モジュール，　１３１　セキュアチップコマンドモジュール，　１３２　セキュアチップマネージャモジュール

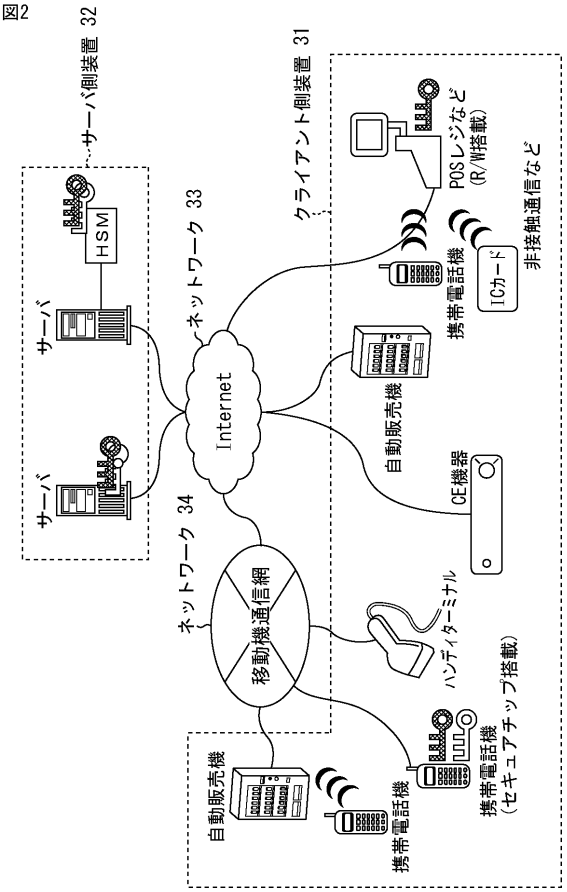
【図１】

図1



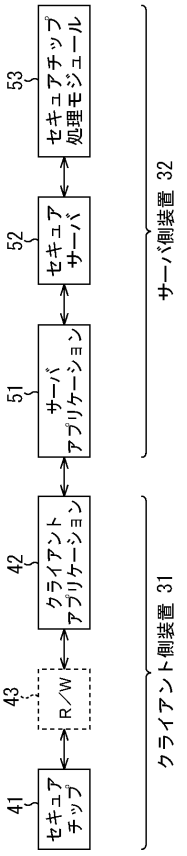
【図２】

図2



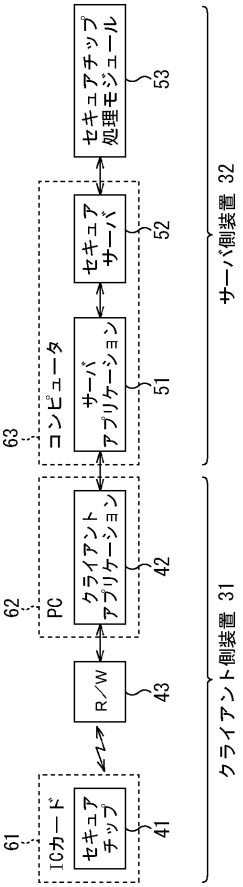
【図３】

図3

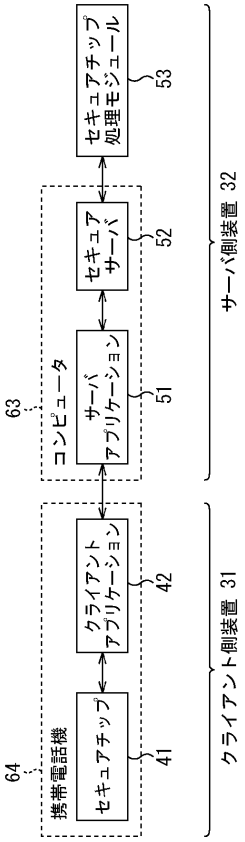


【図４】

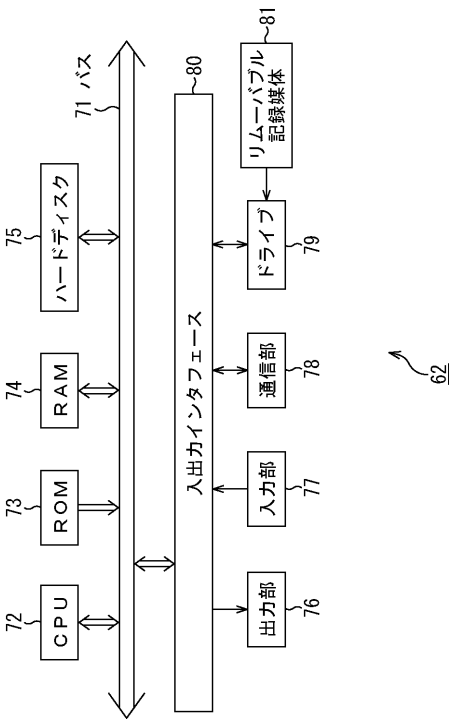
図4



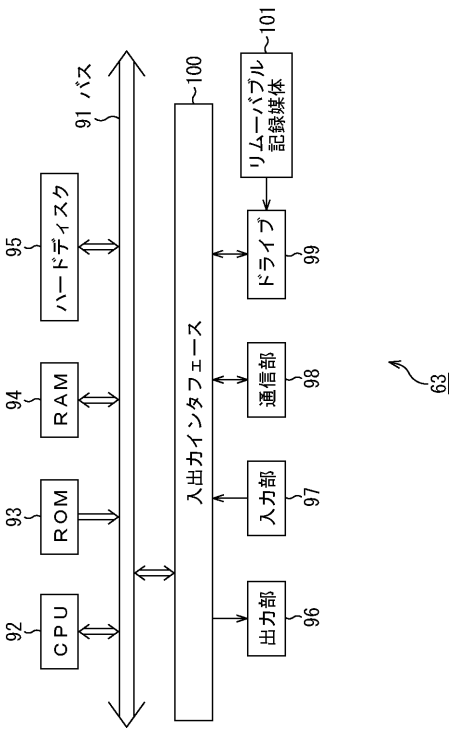
【図５】
図5



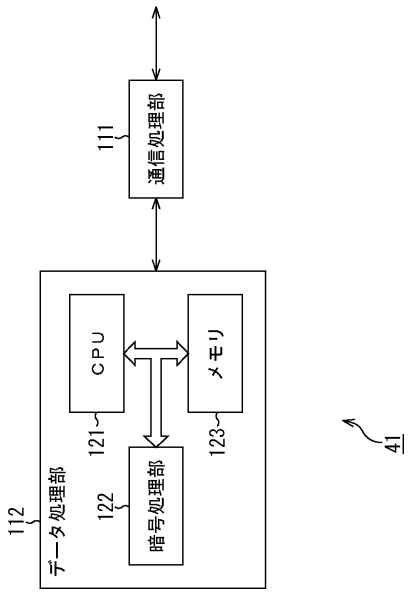
【図６】
図6



【図７】
図7

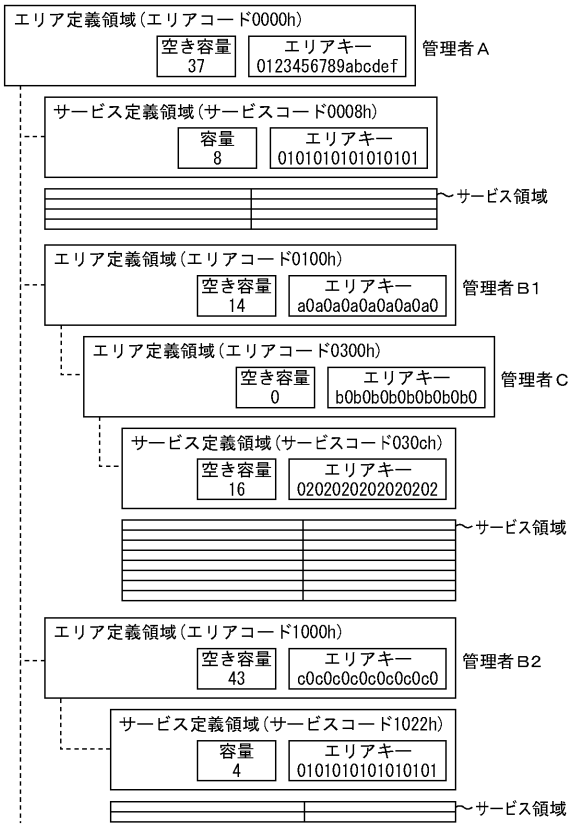


【図８】
図8



【図９】

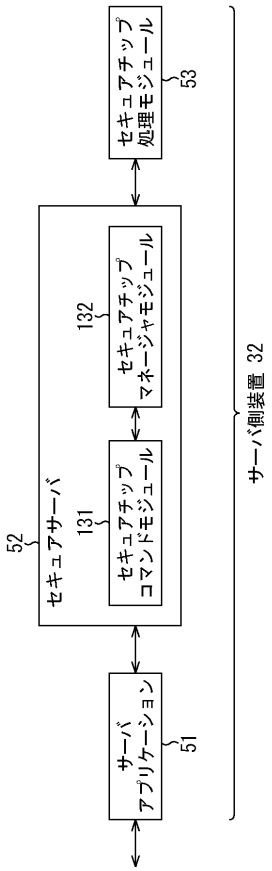
図9



ディレクトリ構造

【図１０】

図10



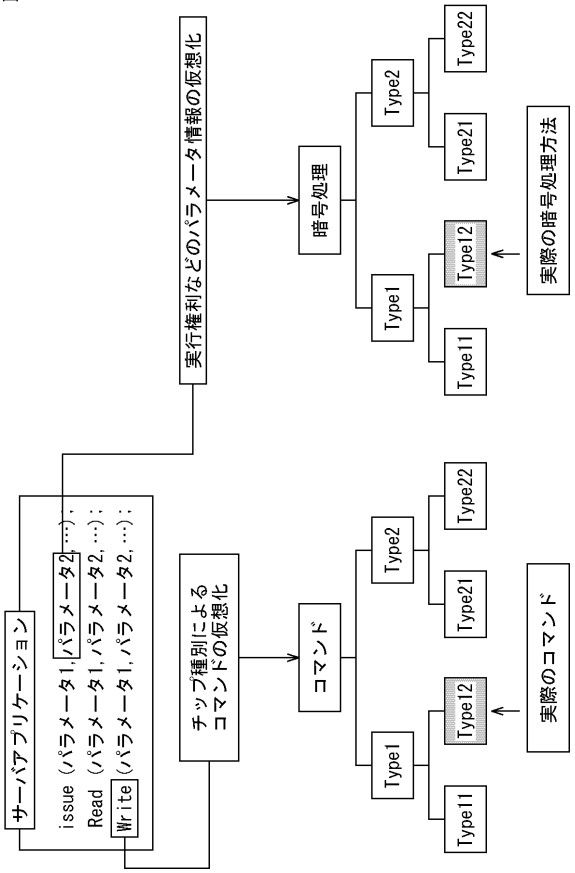
【図１１】

図11

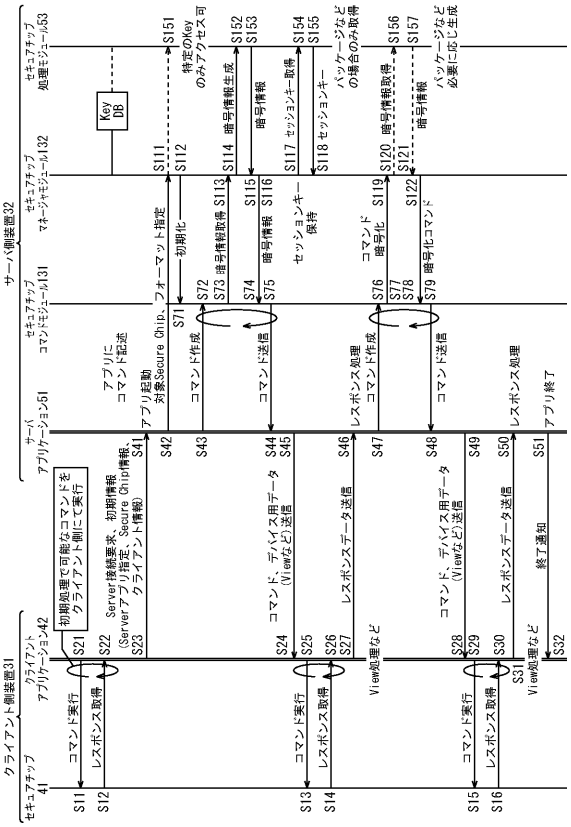
Chip種別	コマンド種別	暗号処理種別
FeliCa1	Type11	Type12
FeliCa2	Type12	Type12
GP1	Type21	Type21
GP2	Type22	Type21

【図１２】

図12



【図１３】
図13


クライアント側装置31
セキュアチップ 41
クライアント アプリケーション42
サーバ側装置32
サーバ アプリケーション51
セキュアチップ コマンドモジュール131
セキュアチップ マネージャモジュール132
セキュアチップ 処理モジュール53
Key DB
初期処理で可能なコマンドを クライアント側に通知
Server接続要求、初期情報 (Serverアプリ指定、Secure Chip情報、 クライアント情報)
アプリに コマンド記述
アプリ起動 対象Secure Chip、フォーマット指定
初期化
特定のKey のみアクセス可
コマンド作成
暗号情報取得
暗号情報生成
暗号情報
コマンド送信
セッションキー取得
セッションキー 保持
パッケージなど の場合のみ取得
コマンド 暗号化
暗号情報取得
暗号化コマンド
パッケージなど 必要に応じ生成
コマンド、デバイス用データ (Viewなど)送信
レスポンスデータ送信
レスポンス処理 コマンド作成
Viewなど
レスポンス処理
アプリ終了
終了通知
コマンド実行
レスポンス取得
S11 S12 S13 S14 S15 S16
S21 S22 S23 S24 S25 S26 S27 S28 S29 S30 S31 S32
S41 S42 S43 S44 S45 S46 S47 S48 S49 S50 S51
S71 S72 S73 S74 S75 S76 S77 S78 S79
S111 S112 S113 S114 S115 S116 S117 S118 S119 S120 S121 S122
S151 S152 S153 S154 S155 S156 S157

フロントページの続き

審査官　村田　充裕

(56)参考文献　特開２０００－３５３２１６（ＪＰ，Ａ）
特開２００４－２６４９２１（ＪＰ，Ａ）
特開平１１－２８２９８２（ＪＰ，Ａ）
特開２００４－１５３７１１（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｋ　１７／００
Ｇ０６Ｋ　１９／００－１９／０８
Ｇ０６Ｆ　１２／１４
Ｂ４２Ｄ　１５／１０