(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4708754号
(P4708754)
(45)発行日　平成23年6月22日(2011.6.22)　(24)登録日　平成23年3月25日(2011.3.25)

(51)Int.Cl.　F I
G06F 15/00 (2006.01)　G06F 15/00 320J
G06F 11/22 (2006.01)　G06F 11/22 310R
G06F 11/22 310W
G06F 11/22 330H

請求項の数 4　(全 38 頁)

(21)出願番号　特願2004-285953 (P2004-285953)
(22)出願日　平成16年9月30日 (2004.9.30)
(65)公開番号　特開2006-99510 (P2006-99510A)
(43)公開日　平成18年4月13日 (2006.4.13)
審査請求日　平成19年9月5日 (2007.9.5)

(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　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
(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

最終頁に続く

(54)【発明の名称】サーバクライアントシステム、クライアント、データ処理方法、およびプログラム

(57)【特許請求の範囲】
【請求項１】
サーバとクライアントからなるサーバクライアントシステムを構成するクライアントにおいて、
前記サーバは、
セッション単位で変化する、データの暗号化に関する暗号関連処理を行う第１の処理手段と、
負荷試験用の前記暗号関連処理を行う第２の処理手段と、
前記第１または第２の処理手段のうちの一方を選択し、前記クライアントとやりとりするデータに対する前記暗号関連処理を行わせる選択手段と
を有し、
前記クライアントは、
他の装置が、前記サーバに送信した、暗号化されたデータを記憶する記憶手段と、
前記選択手段によって前記第２の処理手段が選択された場合に、前記記憶手段に記憶されたデータを復号する復号手段と、
前記復号手段において復号されたデータの一部を、前記第２の処理手段による処理結果に対応するように書き換える書き換え手段と、
前記書き換え手段において一部が書き換えられたデータを暗号化し、前記記憶手段に記憶させる暗号化手段と、
前記記憶手段に記憶された、一部が書き換えられ、暗号化されたデータを送信する送

信手段と
を有し、
前記書き換え手段によるデータの一部の書き換え、前記暗号化手段によるデータの暗号化、および、前記送信手段によるデータの送信が、多重的に、多数回繰り返される
ことを特徴とするクライアント。
【請求項２】
サーバとクライアントからなるサーバクライアントシステムを構成するクライアントのデータ処理方法において、
前記サーバは、
セッション単位で変化する、データの暗号化に関する暗号関連処理を行う第１の処理手段と、
負荷試験用の前記暗号関連処理を行う第２の処理手段と、
前記第１または第２の処理手段のうちの一方を選択し、前記クライアントとやりとりするデータに対する前記暗号関連処理を行わせる選択手段と
を有し、
前記クライアントは、他の装置が、前記サーバに送信した、暗号化されたデータを記憶する記憶手段を有し、
前記選択手段によって前記第２の処理手段が選択された場合に、前記記憶手段に記憶されたデータを復号する復号ステップと、
前記復号ステップにおいて復号されたデータの一部を、前記第２の処理手段による処理結果に対応するように書き換える書き換えステップと、
前記書き換えステップにおいて一部が書き換えられたデータを暗号化し、前記記憶手段に記憶させる暗号化ステップと、
前記記憶手段に記憶された、一部が書き換えられ、暗号化されたデータを送信する送信ステップと
を含み、
前記書き換えステップの処理によるデータの一部の書き換え、前記暗号化ステップの処理によるデータの暗号化、および、前記送信ステップの処理によるデータの送信が、多重的に、多数回繰り返される
ことを特徴とするデータ処理方法。
【請求項３】
サーバとクライアントからなるサーバクライアントシステムを構成するクライアントに実行させるプログラムにおいて、
前記サーバは、
セッション単位で変化する、データの暗号化に関する暗号関連処理を行う第１の処理手段と、
負荷試験用の前記暗号関連処理を行う第２の処理手段と、
前記第１または第２の処理手段のうちの一方を選択し、前記クライアントとやりとりするデータに対する前記暗号関連処理を行わせる選択手段と
を有し、
前記クライアントは、他の装置が、前記サーバに送信した、暗号化されたデータを記憶する記憶手段を有し、
前記選択手段によって前記第２の処理手段が選択された場合に、前記記憶手段に記憶されたデータを復号する復号ステップと、
前記復号ステップにおいて復号されたデータの一部を、前記第２の処理手段による処理結果に対応するように書き換える書き換えステップと、
前記書き換えステップにおいて一部が書き換えられたデータを暗号化し、前記記憶手段に記憶させる暗号化ステップと、
前記記憶手段に記憶された、一部が書き換えられ、暗号化されたデータを送信させる送信ステップと

を含み、
前記書き換えステップの処理によるデータの一部の書き換え、前記暗号化ステップの処理によるデータの暗号化、および、前記送信ステップの処理によるデータの送信が、多重的に、多数回繰り返される
ことを特徴とするプログラム。
【請求項４】
サーバとクライアントとからなるサーバクライアントシステムにおいて、
前記サーバは、
セッション単位で変化する、データの暗号化に関する暗号関連処理を行う第１の処理手段と、
負荷試験用の前記暗号関連処理を行う第２の処理手段と、
前記第１または第２の処理手段のうちの一方を選択し、前記クライアントとやりとりするデータに対する前記暗号関連処理を行わせる選択手段と
を有し、
前記クライアントは、
他の装置が、前記サーバに送信した、暗号化されたデータを記憶する記憶手段と、
前記選択手段によって前記第２の処理手段が選択された場合に、前記記憶手段に記憶されたデータを復号する復号手段と、
前記復号手段において復号されたデータの一部を、前記第２の処理手段による処理結果に対応するように書き換える書き換え手段と、
前記書き換え手段において一部が書き換えられたデータを暗号化し、前記記憶手段に記憶させる暗号化手段と、
前記記憶手段に記憶された、一部が書き換えられ、暗号化されたデータを送信する送信手段と
を有し、
前記書き換え手段によるデータの一部の書き換え、前記暗号化手段によるデータの暗号化、および、前記送信手段によるデータの送信が、多重的に、多数回繰り返される
ことを特徴とするサーバクライアントシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、サーバクライアントシステム、クライアント、データ処理方法、およびプログラムに関し、特に、データを暗号化してクライアントに送信するサーバの負荷試験を、セキュア、かつ容易に行うことができるようにするサーバクライアントシステム、クライアント、データ処理方法、およびプログラムに関する。
【背景技術】
【０００２】
近年、代金決済において、IC(Integrated Circuit)チップを利用した、いわゆる電子マネーを用いることが普及しつつある。
【０００３】
例えば、ユーザは、PC(Personal Computer)に接続されたR/W(Reader/Writer)に、ICチップを内蔵するICカードを載置することによって、インターネット上のショッピングサイトにおいて購入した代金の支払いを、ICチップにチャージされた電子マネーによって行うことができる。また、ユーザは、実際の店舗において、ICチップを内蔵した携帯電話機を、店舗に設定されたR/Wに近づけることによって、商品の代金の支払いを、ICチップにチャージされた電子マネーによって行うことができる（例えば、特許文献１参照）。この商品の代金の支払いのための処理は、PC，R/W、およびICカード（ICチップ）がクライアントとなって、またはICチップを内蔵する携帯電話機がクライアントとなって、サーバからの指示に対し、クライアントが応答することによって行われる。
【０００４】

なお、サーバとクライアントとの間でやりとりされるデータは、商品の代金として支払う金額やICチップに登録（チャージ）された残高等のプライバシーに関するデータであるので、セキュリティを保つために、暗号化が必要となる。そこで、サーバとクライアントとの間でやりとりされるデータは暗号化されるようになっている。即ち、サーバは、クライアントに送信するデータを暗号化して送信し、クライアントも、サーバに送信するデータを暗号化して送信する。

【０００５】

【特許文献１】特開2002-374570号公報

【発明の開示】

【発明が解決しようとする課題】

【０００６】

上述したサーバは、例えば、ICチップにチャージされている電子マネーの残高の管理や、その残高から商品の代金を減額する処理などの決済処理を行うことによって、電子マネーによる商品の代金の支払いを行う電子マネーサービスを、クライアントに提供することができる。

【０００７】

また、サーバは、電子マネーサービスに限らず、サーバ自体が行う処理に応じた各種のサービスを提供することができる。

【０００８】

ところで、あるサービス提供者が、サーバを用いて、新たなサービスの提供を開始する場合、サーバの負荷試験を行うことがある。

【０００９】

サーバの負荷試験は、例えば、実際に、多数のクライアントから、サーバにアクセスすることによって、あるいは、クライアントの処理をエミュレートするエミュレータとしてのソフトウェアを作成し、そのエミュレータを多重に実行することにより、擬似的に多数のクライアントからのアクセスが行われた状態をつくり出すことによって行われる。

【００１０】

しかしながら、実際に、多数のクライアントからサーバにアクセスするには、その多数のクライアントを用意する必要がある。

【００１１】

また、クライアントの処理をエミュレートするエミュレータを用いて負荷試験を行う場合には、その負荷試験の対象のサーバによってサービスを提供しようとするサービス提供者に対し、負荷試験のために、エミュレータを渡す必要があるが、この場合、そのエミュレータがエミュレートするクライアントの処理、特に、データの暗号化／復号の処理の内容が、外部に漏洩するおそれが生じ、セキュリティの観点から好ましくない。

【００１２】

そこで、例えば、サーバとクライアントとの間でやりとりされるデータ（通信データ）をキャプチャし、その通信データのコピーを、サーバに送信することを繰り返すことにより、サーバに負荷を発生させる負荷発生用のソフトウェア（例えば、LoadRunnerと呼ばれている製品）がある。

【００１３】

しかしながら、上述したようなサーバとクライアントとからなるサーバクライアントシステムでは、サーバが行う、暗号化や復号などの暗号化に関連する暗号関連処理が、セッション単位で変化する。即ち、例えば、サーバにおいて、暗号化や復号に用いられる鍵（暗号鍵）や、相互認証に用いられる乱数などが、セッション単位で変化する。

【００１４】

従って、負荷発生用のソフトウェアにおいては、通信データのコピーが繰り返し送信されるため、セッションが異なっていても、通信データが変わらないのに対して、サーバでは、鍵や乱数などがセッション単位で変化するため、例えば、サーバが相互認証を行う場合には、その相互認証に失敗し、サーバにおいて正常な処理が行われる場合の負荷試験を

行うことが困難であった。

【００１５】

本発明は、このような状況に鑑みてなされたものであり、サーバにおいて正常な処理が行われる負荷試験を、セキュア、かつ容易に行う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】

【００２０】

本発明のクライアントは、他の装置が、サーバに送信した、暗号化されたデータを記憶する記憶手段と、記憶手段に記憶されたデータを復号する復号手段と、復号手段において復号されたデータの一部を書き換える書き換え手段と、書き換え手段において一部が書き換えられたデータを暗号化し、記憶手段に記憶させる暗号化手段と、記憶手段に記憶された、一部が書き換えられ、暗号化されたデータを送信する送信手段とを有し、書き換え手段によるデータの一部の書き換え、暗号化手段によるデータの暗号化、および、送信手段によるデータの送信が、多重的に、多数回繰り返されることを特徴とする。

【００２１】

本発明のデータ処理方法は、他の装置が、サーバに送信した、暗号化されたデータを記憶する記憶手段に記憶されたデータを復号する復号ステップと、復号ステップにおいて復号されたデータの一部を書き換える書き換えステップと、書き換えステップにおいて一部が書き換えられたデータを暗号化し、記憶手段に記憶させる暗号化ステップと、記憶手段に記憶された、一部が書き換えられ、暗号化されたデータを送信する送信ステップとを含み、書き換えステップの処理によるデータの一部の書き換え、暗号化ステップの処理によるデータの暗号化、および、送信ステップの処理によるデータの送信が、多重的に、多数回繰り返されることを特徴とする。

【００２２】

本発明のプログラムは、他の装置が、サーバに送信した、暗号化されたデータを記憶する記憶手段に記憶されたデータを復号する復号ステップと、復号ステップにおいて復号されたデータの一部を書き換える書き換えステップと、書き換えステップにおいて一部が書き換えられたデータを暗号化し、記憶手段に記憶させる暗号化ステップと、記憶手段に記憶された、一部が書き換えられ、暗号化されたデータを送信させる送信ステップとを含み、書き換えステップの処理によるデータの一部の書き換え、暗号化ステップの処理によるデータの暗号化、および、送信ステップの処理によるデータの送信が、多重的に、多数回繰り返されることを特徴とする。

本発明のサーバクライアントシステムは、サーバが、セッション単位で変化する、データの暗号化に関する暗号関連処理を行う第１の処理手段と、負荷試験用の暗号関連処理を行う第２の処理手段と、第１または第２の処理手段のうちの一方を選択し、クライアントとやりとりするデータに対する暗号関連処理を行わせる選択手段とを有し、クライアントが、他の装置が、サーバに送信した、暗号化されたデータを記憶する記憶手段と、選択手段によって第２の処理手段が選択された場合に、記憶手段に記憶されたデータを復号する復号手段と、復号手段において復号されたデータの一部を、第２の処理手段による処理結果に対応するように書き換える書き換え手段と、書き換え手段において一部が書き換えられたデータを暗号化し、記憶手段に記憶させる暗号化手段と、記憶手段に記憶された、一部が書き換えられ、暗号化されたデータを送信する送信手段とを有し、書き換え手段によるデータの一部の書き換え、暗号化手段によるデータの暗号化、および、送信手段によるデータの送信が、多重的に、多数回繰り返されることを特徴とする。

【００２５】

本発明のクライアント、データ処理方法、プログラム、およびサーバクライアントシステムにおいては、他の装置が、サーバに送信した、暗号化されたデータを記憶する記憶手段に記憶されたデータが復号され、その復号されたデータの一部が書き換えられる。そして、その一部が書き換えられたデータが暗号化されて、記憶手段に記憶され、記憶手段に記憶された、一部が書き換えられ、暗号化されたデータが送信され、データの一部の書き換え、データの暗号化、および、データの送信が、多重的に、多数回繰り返される。

【発明の効果】
【００２６】
本発明によれば、サーバの負荷試験を、セキュア、かつ容易に行うことが可能となる。
【発明を実施するための最良の形態】
【００２７】
以下に本発明の実施の形態を説明するが、請求項に記載の構成要件と、発明の実施の形態における具体例との対応関係を例示すると、次のようになる。この記載は、請求項に記載されている発明をサポートする具体例が、発明の実施の形態に記載されていることを確認するためのものである。従って、発明の実施の形態中には記載されているが、構成要件に対応するものとして、ここには記載されていない具体例があったとしても、そのことは、その具体例が、その構成要件に対応するものではないことを意味するものではない。逆に、具体例が構成要件に対応するものとしてここに記載されていたとしても、そのことは、その具体例が、その構成要件以外の構成要件には対応しないものであることを意味するものでもない。
【００２８】
さらに、この記載は、発明の実施の形態に記載されている具体例に対応する発明が、請求項に全て記載されていることを意味するものではない。換言すれば、この記載は、発明の実施の形態に記載されている具体例に対応する発明であって、この出願の請求項には記載されていない発明の存在、すなわち、将来、分割出願されたり、補正により追加される発明の存在を否定するものではない。
【００３３】
請求項１に記載のクライアントは、
サーバとクライアントからなるサーバクライアントシステム（例えば、図１２のサーバクライアントシステム）を構成するクライアント（例えば、図１２の負荷発生用クライアント側装置１１１）において、
前記サーバ（例えば、図１２のサーバ側装置２）は、
セッション単位で変化する、データの暗号化に関する暗号関連処理を行う第１の処理手段（例えば、図１４のセキュアチップ処理モジュール２３や、図１６の鍵／乱数発生モジュール１３２）と、
負荷試験用の前記暗号関連処理を行う第２の処理手段（例えば、図１４の負荷試験用セキュアチップ処理モジュール１２２や、図１６の負荷試験用鍵／乱数発生モジュール１３３）と、
前記第１または第２の処理手段のうちの一方を選択し、前記クライアントとやりとりするデータに対する前記暗号関連処理を行わせる選択手段（例えば、図１４のモジュール選択部１２１や、図１６のモジュール選択部１３１）と
を有し、
前記クライアントは、
他の装置（例えば、図１２のクライアント側装置１）が、前記サーバに送信した、暗号化されたデータを記憶する記憶手段（例えば、図１８の記憶部１１３）と、
前記選択手段によって前記第２の処理手段が選択された場合に、前記記憶手段に記憶されたデータを復号する復号手段（例えば、図１８の負荷用暗号／復号ロジック部１４１）と、
前記復号手段において復号されたデータの一部を、前記第２の処理手段による処理結果に対応するように書き換える書き換え手段（例えば、図１８の通信データ書き換えロジック部１４２）と、
前記書き換え手段において一部が書き換えられたデータを暗号化し、前記記憶手段に記憶させる暗号化手段（例えば、図１８の負荷用暗号／復号ロジック部１４１）と、
前記記憶手段に記憶された、一部が書き換えられ、暗号化されたデータを送信する送信手段（例えば、図１８の通信制御部１１４）と
を有し、

前記書き換え手段によるデータの一部の書き換え、前記暗号化手段によるデータの暗号化、および、前記送信手段によるデータの送信が、多重的に、多数回繰り返される
ことを特徴とする。

【００３４】

請求項２に記載のデータ処理方法は、

サーバとクライアントからなるサーバクライアントシステム（例えば、図１２のサーバクライアントシステム）を構成するクライアント（例えば、図１２の負荷発生用クライアント側装置１１１）のデータ処理方法において、

前記サーバは、

セッション単位で変化する、データの暗号化に関する暗号関連処理を行う第１の処理手段（例えば、図１４のセキュアチップ処理モジュール２３や、図１６の鍵／乱数発生モジュール１３２）と、

負荷試験用の前記暗号関連処理を行う第２の処理手段（例えば、図１４の負荷試験用セキュアチップ処理モジュール１２２や、図１６の負荷試験用鍵／乱数発生モジュール１３３）と、

前記第１または第２の処理手段のうちの一方を選択し、前記クライアントとやりとりするデータに対する前記暗号関連処理を行わせる選択手段（例えば、図１４のモジュール選択部１２１や、図１６のモジュール選択部１３１）と

を有し、

前記クライアントは、他の装置が、前記サーバに送信した、暗号化されたデータを記憶する記憶手段（例えば、図１８の記憶部１１３）を有し、

前記選択手段によって前記第２の処理手段が選択された場合に、前記記憶手段に記憶されたデータを復号する復号ステップ（例えば、図１９のステップＳ１３２）と、

前記復号ステップにおいて復号されたデータの一部を、前記第２の処理手段による処理結果に対応するように書き換える書き換えステップ（例えば、図１９のステップＳ１４１）と、

前記書き換えステップにおいて一部が書き換えられたデータを暗号化し、前記記憶手段に記憶させる暗号化ステップ（例えば、図１９のステップＳ１３５）と、

前記記憶手段に記憶された、一部が書き換えられ、暗号化されたデータを送信する送信ステップ（例えば、図１９のステップＳ１５２）と

を含み、

前記書き換えステップの処理によるデータの一部の書き換え、前記暗号化ステップの処理によるデータの暗号化、および、前記送信ステップの処理によるデータの送信が、多重的に、多数回繰り返されることを特徴とする。

【００３５】

請求項３に記載のプログラムは、

サーバとクライアントからなるサーバクライアントシステム（例えば、図１２のサーバクライアントシステム）を構成するクライアント（例えば、図１２の負荷発生用クライアント側装置１１１）に実行させるプログラムにおいて、

前記サーバは、

セッション単位で変化する、データの暗号化に関する暗号関連処理を行う第１の処理手段（例えば、図１４のセキュアチップ処理モジュール２３や、図１６の鍵／乱数発生モジュール１３２）と、

負荷試験用の前記暗号関連処理を行う第２の処理手段（例えば、図１４の負荷試験用セキュアチップ処理モジュール１２２や、図１６の負荷試験用鍵／乱数発生モジュール１３３）と、

前記第１または第２の処理手段のうちの一方を選択し、前記クライアントとやりとりするデータに対する前記暗号関連処理を行わせる選択手段（例えば、図１４のモジュール選択部１２１や、図１６のモジュール選択部１３１）と

を有し、

前記クライアントは、他の装置が、前記サーバに送信した、暗号化されたデータを記憶する記憶手段（例えば、図１８の記憶部１１３）を有し、

前記選択手段によって前記第２の処理手段が選択された場合に、前記記憶手段に記憶されたデータを復号する復号ステップ（例えば、図１９のステップＳ１３２）と、

前記復号ステップにおいて復号されたデータの一部を、前記第２の処理手段による処理結果に対応するように書き換える書き換えステップ（例えば、図１９のステップＳ１４１）と、

前記書き換えステップにおいて一部が書き換えられたデータを暗号化し、前記記憶手段に記憶させる暗号化ステップ（例えば、図１９のステップＳ１３５）と、

前記記憶手段に記憶された、一部が書き換えられ、暗号化されたデータを送信させる送信ステップ（例えば、図１９のステップＳ１５２）と

を含み、

前記書き換えステップの処理によるデータの一部の書き換え、前記暗号化ステップの処理によるデータの暗号化、および、前記送信ステップの処理によるデータの送信が、多重的に、多数回繰り返されることを特徴とする。

請求項４に記載のサーバクライアントシステムは、

前記サーバ（例えば、図１２のサーバ側装置２）は、

セッション単位で変化する、データの暗号化に関する暗号関連処理を行う第１の処理手段（例えば、図１４のセキュアチップ処理モジュール２３や、図１６の鍵／乱数発生モジュール１３２）と、

負荷試験用の前記暗号関連処理を行う第２の処理手段（例えば、図１４の負荷試験用セキュアチップ処理モジュール１２２や、図１６の負荷試験用鍵／乱数発生モジュール１３３）と、

前記第１または第２の処理手段のうちの一方を選択し、前記クライアントとやりとりするデータに対する前記暗号関連処理を行わせる選択手段（例えば、図１４のモジュール選択部１２１や、図１６のモジュール選択部１３１）と

を有し、

前記クライアントは、

他の装置（例えば、図１２のクライアント側装置１）が、前記サーバに送信した、暗号化されたデータを記憶する記憶手段（例えば、図１８の記憶部１１３）と、

前記選択手段によって前記第２の処理手段が選択された場合に、前記記憶手段に記憶されたデータを復号する復号手段（例えば、図１８の負荷用暗号／復号ロジック部１４１）と、

前記復号手段において復号されたデータの一部を、前記第２の処理手段による処理結果に対応するように書き換える書き換え手段（例えば、図１８の通信データ書き換えロジック部１４２）と、

前記書き換え手段において一部が書き換えられたデータを暗号化し、前記記憶手段に記憶させる暗号化手段（例えば、図１８の負荷用暗号／復号ロジック部１４１）と、

前記記憶手段に記憶された、一部が書き換えられ、暗号化されたデータを送信する送信手段（例えば、図１８の通信制御部１１４）と

を有し、

前記書き換え手段によるデータの一部の書き換え、前記暗号化手段によるデータの暗号化、および、前記送信手段によるデータの送信が、多重的に、多数回繰り返される

ことを特徴とする。

【００３６】

以下、図面を参照して、本発明の実施の形態について説明する。

【００３７】

図１は、本発明が適用される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）の構成例を示している。

【００３８】
図１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１と、いわゆるサーバであるサーバ側装置２とが、例えば、インターネットなどのネットワーク３、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４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１は、セキュアチップを内蔵している。セキュアチップは、例えば、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、外部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１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、ハンディーターミナルなどがある。また、クライアント側装置１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(R)などに採用されているFeliCa(R)などがある。
【００４１】
サーバ側装置２は、ネットワーク３、さらには、必要に応じて、ネットワーク４を介して、クライアント側装置１との間でデータ（コマンドを含む）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１のセキュアチップに、電子マネーが記憶されている場合において、サーバ側装置２が、クライアント側装置１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よって、クライアント側装置１の電子マネーの金額を更新する処理等を制御することにより、サーバ側装置２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１は、サーバ側装置２に送信するデータを暗号化して送信し、サーバ側装置２も、クライアント側装置１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１におけるデータの暗号化や復号、暗号化／復号に用いられる鍵の発生や管理、相互認証（のためのデータの暗号化／復号など）、相互認証に用いられる乱数の発生、その他のデータの暗号化（秘密化）に関連する暗号関連処理は、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２における暗号関連処理は、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２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、暗号関連処理には、特に高い秘匿性が要求される暗号関連処理と、それ以外の暗号関連処理とがあり、サーバ側装置２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関連処理のみを、HSM内で行い、それ以外の暗号関連処理を、サーバ側装置２を実現するソフトウェアなどで行うことができる。
【００４５】
次に、図２は、クライアント側装置１とサーバ側装置２の機能的な構成例を示している。
【００４６】
クライアント側装置１は、セキュアチップ１１およびクライアントアプリケーション１２、さらには、必要なR/W１３で構成される。
【００４７】
セキュアチップ１１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、外部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。
【００４８】
即ち、セキュアチップ１１は、クライアントアプリケーション１２と直接、またはR/W

１３を介して通信し、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１２から送信されてくるコマンドにしたがって処理を行う。さらに、セキュアチップ１１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１２に対して、直接、またはR/W１３を介して送信する。また、セキュアチップ１１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関連処理を行う。

【００４９】

クライアントアプリケーション１２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、サーバ側装置２の後述するサーバアプリケーション２１のクライアントとして機能する。クライアントアプリケーション１２は、サーバアプリケーション２１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１１に対して、直接、またはR/W１３を介して、コマンド等を送信することで、セキュアチップ１１に対するデータの読み書き等を行い、これにより、各種のサービスの提供を実現する。

【００５０】

即ち、例えば、クライアントアプリケーション１２およびサーバアプリケーション２１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１１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には、セキュアチップ１１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よって、セキュアチップ１１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１２とサーバアプリケーション２１との間で行われる。

【００５１】

なお、クライアントアプリケーション１２には、サーバアプリケーション２１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。

【００５２】

R/W１３は、セキュアチップ１１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１２から供給されるコマンド等を、セキュアチップ１１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１２に供給する。

【００５３】

サーバアプリケーション２１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、クライアント側装置１のクライアントアプリケーション１２のサーバとして機能する。サーバアプリケーション２１は、クライアントアプリケーション１２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。

【００５４】

また、サーバアプリケーション２１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関連処理を、セキュアサーバ２２に依頼する。

【００５５】

なお、サーバアプリケーション２１には、クライアントアプリケーション１２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。

【００５６】

セキュアサーバ２２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、サーバアプリケーション２１からの暗号関連処理の依頼に応じて、自身で暗号関連処理を行い、あるいは、暗号関連処理を、セキュアチップ処理モジュール２３に依頼する。

【００５７】

即ち、セキュアサーバ２２は、サーバアプリケーション２１から依頼される暗号関連処理のうちの、特に高い秘匿性が要求される暗号関連処理を、セキュアチップ処理モジュール２３に依頼し、それ以外の暗号関連処理を、自身（セキュアサーバ２２内）で行う。

【００５８】
セキュアチップ処理モジュール２３は、セキュアサーバ２２からの依頼に応じて、暗号関連処理（特に高い秘匿性が要求される暗号関連処理）を行う。
【００５９】
なお、セキュアチップ処理モジュール２３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２３は、例えば、セキュアサーバ２２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。
【００６０】
次に、図３は、クライアント側装置１とサーバ側装置２の具体的なハードウェアの構成例を示している。
【００６１】
図３において、クライアント側装置１は、ハードウェアであるR/W１３，ICカード３１、およびPC３２で構成されている。
【００６２】
ICカード３１は、ハードウェアであるセキュアチップ１１を内蔵し、例えば、電子マネーを格納するEdy(R)などのカードに相当する。PC３２は、例えば、ICカード３１のユーザが所有するPCで、そこには、クライアントアプリケーション１２がインストールされている。ユーザは、PC３２を操作することにより、ICカード３１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、電子マネーによる代金の支払い等を行うことができる。
【００６３】
図３において、サーバ側装置２は、ハードウェアであるセキュアチップ処理モジュール２３およびコンピュータ３３で構成されている。
【００６４】
コンピュータ３３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２１とセキュアサーバ２２がインストールされている。
【００６５】
次に、図４は、クライアント側装置１とサーバ側装置２の具体的なハードウェアの他の構成例を示している。なお、図４において、サーバ側装置２のハードウェアの構成は、図３における場合と同様になっている。
【００６６】
図４において、クライアント側装置１は、ハードウェアである携帯電話機３４で構成されている。
【００６７】
携帯電話機３４は、ハードウェアであるセキュアチップ１１を内蔵している。さらに、携帯電話機３４には、クライアントアプリケーション１２がインストールされている。ユーザは、携帯電話機３４を操作することにより、例えば、セキュアチップ１１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、電子マネーによる代金の支払い等を行うことができる。
【００６８】
なお、携帯電話機３４の外部から、携帯電話機３４が内蔵するセキュアチップ１１へのアクセスは、携帯電話機３４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４では図示していないR/W１３に対して、携帯電話機３４、ひいては、その携帯電話機３４が内蔵するセキュアチップ１１を近づけることにより行うこともできる。
【００６９】
次に、図５は、クライアントアプリケーション１２がインストールされる図３のPC３２のハードウェアの構成例を示している。
【００７０】
PC３２は、CPU(Central Processing Unit)４２を内蔵している。CPU４２には、バス４

１を介して、入出力インタフェース５０が接続されており、CPU４２は、入出力インタフェース５０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４７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)４３に格納されているプログラムを実行する。あるいは、また、CPU４２は、ハードディスク４５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４８で受信されてハードディスク４５にインストールされたプログラム、またはドライブ４９に装着されたリムーバブル記録媒体５１から読み出されてハードディスク４５にインストールされたプログラムを、RAM(Random Access Memory)４４にロードして実行する。これにより、CPU４２は、各種の処理を行う。そして、CPU４２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５０を介して、LCD(Liquid Crystal Display)やスピーカ等で構成される出力部４６から出力、あるいは、通信部４８から送信、さらには、ハードディスク４５に記録等させる。

【００７１】

なお、入出力インタフェース５０には、例えば、USB(Universal Serial Bus)端子が設けられており、図３におけるR/W１３は、そのUSB端子に接続することができる。CPU４２（によって、実行されるクライアントアプリケーション１２）は、入出力インタフェース５０に接続されたR/W１３を介して、セキュアチップ１１（図３）にアクセスすることができる。

【００７２】

ここで、クライアントアプリケーション１２その他のプログラムは、PC３２に内蔵されている記録媒体としてのハードディスク４５やROM４３に予め記録しておくことができる。

【００７３】

あるいはまた、プログラムは、フレキシブルディスク、CD-ROM(Compact Disc Read Only Memory), MO(Magneto Optical)ディスク, DVD(Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体５１に、一時的あるいは永続的に格納（記録）しておくことができる。このようなリムーバブル記録媒体５１は、いわゆるパッケージソフトウエアとして提供することができる。

【００７４】

なお、プログラムは、上述したようなリムーバブル記録媒体５１からPC３２にインストールする他、ダウンロードサイトから、ディジタル衛星放送用の人工衛星を介して、PC３２に無線で転送したり、LAN(Local Area Network)、インターネットといったネットワーク３を介して、PC３２に有線で転送し、PC３２では、そのようにして転送されてくるプログラムを、通信部４８で受信し、内蔵するハードディスク４５にインストールすることができる。

【００７５】

次に、図６は、サーバアプリケーション２１およびセキュアサーバ２２がインストールされる図３のコンピュータ３３のハードウェアの構成例を示している。

【００７６】

ここで、図６において、コンピュータ３３を構成するバス６１乃至リムーバブル記録媒体７１は、図５のバス４１乃至リムーバブル記録媒体５１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。

【００７７】

なお、図３や図４において、セキュアチップ処理モジュール２３は、通信部６８または入出力インタフェース７０を介して、コンピュータ３３に接続される。

【００７８】

次に、図７は、図２のセキュアチップ１１のハードウェアの構成例を示している。

【００７９】

セキュアチップ１１は、大きく分けて、通信処理部８１とデータ処理部８２とから構成される。通信処理部８１は、セキュアチップ１１の外部と、接触通信または非接触通信を

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８２に供給し、また、データ処理部８２からのデータを、外部に送信する。

【００８０】

ここで、セキュアチップ１１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。また、セキュアチップ１１が電源を有しない場合には、通信処理部８１では、外部からの信号から電源（電力）を生成する処理も行われる。

【００８１】

データ処理部８２は、例えば、CPU９１、暗号関連処理部９２、およびメモリ９３で構成され、通信処理部８１から供給されるコマンド等にしたがい、各種の処理を行う。

【００８２】

即ち、CPU９１は、暗号関連処理部９２の制御やメモリ９３の管理を行う。また、CPU９１は、通信処理部８１から供給されるコマンドにしたがい、メモリ９３に対するデータの読み書きや、メモリ９３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、CPU９１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９３に記憶されている。

【００８３】

暗号関連処理部９２は、CPU９１の制御にしたがい、暗号関連処理を行う。ここで、暗号関連処理には、データ（コマンドを含む）の暗号化／復号の他に、例えば、いわゆるチャレンジアンドレスポンス方式での相互認証（相互認証に用いられる乱数の発生等を含む）、暗号化／復号に用いられる鍵（暗号鍵となる情報）の発生（生成）なども含まれる。

【００８４】

メモリ９３は、不揮発性のメモリで、データやプログラムなどを記憶する。なお、メモリ９３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９３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は、揮発性のメモリを採用することができる。揮発性メモリには、例えば、CPU９１の動作上一時的に記憶しておく必要があるデータなどが記憶される。

【００８５】

次に、CPU９１では、メモリ９３の記憶領域が階層化されて管理されるようになされている。

【００８６】

即ち、図８は、メモリ９３のディレクトリ構造を示している。

【００８７】

メモリ９３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ようになっている。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、下位（子）の階層のディレクトリに相当するエリア定義領域や、ファイルに相当する、後述するサービス領域を管理する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。

【００８８】

エリア定義領域は、メモリ９３のデータ記憶領域の一部で、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。

【００８９】

ここで、CPU９１は、メモリ９３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、エリア定義領域が管理するデータ記憶領域の空き容量など

は、このブロックの数（ブロック数）によって管理される。

【００９０】

図８の実施の形態では、管理者Ａに最上位階層のエリア定義領域が割り当てられており、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。

【００９１】

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９３のデータ記憶領域の一部で、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。

【００９２】

サービス領域は、データ記憶領域の一部で、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。

【００９３】

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、電子マネーの金額（残高）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）、商品を購入した年月日などが記憶される。

【００９４】

次に、図９は、図２のセキュアサーバ２２の詳細な構成例を示している。

【００９５】

セキュアサーバ２２は、セキュアチップコマンドモジュール１０１とセキュアチップマネージャモジュール１０２とから構成される。

【００９６】

セキュアチップコマンドモジュール１０１は、例えば、サーバアプリケーション２１からのコマンドの作成の要求（依頼）に応じて、セキュアチップ１１用のコマンドを作成し、サーバアプリケーション２１に供給する。

【００９７】

即ち、サーバアプリケーション２１は、クライアント側装置１のセキュアチップ１１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１０１に要求し、セキュアチップコマンドモジュール１０１は、その要求に応じ、セキュアチップ１１用のコマンドを作成して、サーバアプリケーション２１に供給する。

【００９８】

従って、サーバアプリケーション２１は、セキュアチップ１１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２１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。

【００９９】

即ち、サーバアプリケーション２１は、セキュアチップコマンドモジュール１０１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い。

【０１００】

ここで、セキュアチップコマンドモジュール１０１は、上述したように、サーバアプリケーション２１からの要求に応じて、セキュアチップ１１用のコマンドを作成し、サーバ

アプリケーション２１に供給するが、コマンドをサーバアプリケーション２１に供給する前に、セキュアチップマネージャモジュール１０２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１０１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１０２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２１に供給する。

【０１０１】

セキュアチップマネージャモジュール１０２は、セキュアチップコマンドモジュール１０１からの要求に応じて、コマンドの暗号化等の暗号関連処理を行い、あるいは、暗号関連処理を、セキュアチップ処理モジュール２３に要求する。そして、セキュアチップマネージャモジュール１０２は、自身（セキュアチップマネージャモジュール１０２）またはセキュアチップ処理モジュール２３による暗号関連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１０１に供給する。

【０１０２】

なお、セキュアチップマネージャモジュール１０２は、セキュアチップ１１用の暗号関連処理を行い、あるいは、セキュアチップ処理モジュール２３に、セキュアチップ１１用の暗号関連処理を行わせる。

【０１０３】

即ち、例えば、セキュアチップ１１は、セキュアチップ１１用の暗号化が行われたコマンド（データ）等のみの処理が可能となっている。具体的には、データ（コマンドを含む）の暗号化には、例えば、様々なアルゴリズムの暗号化が存在し、セキュアチップ１１では、あるアルゴリズムの暗号化が採用されている。セキュアチップ１１で採用されている暗号化のアルゴリズムを表す情報（そのアルゴリズムによる暗号化に用いられる鍵を表す情報を含む）を、暗号処理種別ということとすると、セキュアチップマネージャモジュール１０２は、セキュアチップ１１に対応した暗号処理種別の暗号化等を行い、あるいは、セキュアチップ処理モジュール２３に、セキュアチップ１１に対応した暗号処理種別の暗号化等を行わせる。

【０１０４】

なお、セキュアチップマネージャモジュール１０２は、セキュアチップ１１の暗号処理種別と異なる暗号処理種別の暗号化等も行うように構成することができる。セキュアチップ処理モジュール２３も同様である。

【０１０５】

また、暗号化は、例えば、認証や、後述する通信路の暗号化、同じく後述するパッケージの作成などのために行われるが、暗号処理種別は、これらの認証、通信路の暗号化、パッケージの作成のための暗号化それぞれごとに決めることが可能である。さらに暗号処理種別には、認証や、通信路の暗号化、パッケージの作成に関連する情報、即ち、例えば、認証として、相互認証を行うのか、または、片側認証を行うのかといった情報を含めることが可能である。

【０１０６】

次に、図１０を参照して、クライアント側装置１とサーバ側装置２の動作について説明する。

【０１０７】

クライアントアプリケーション１２が起動されると、クライアントアプリケーション１２は、まず最初に、ステップＳ２１において、セキュアチップ１１に対して、セキュアチップ１１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。

【０１０８】

セキュアチップ１１は、ステップＳ１１において、クライアントアプリケーション１２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１２に送信する。

【０１０９】

クライアントアプリケーション１２は、ステップＳ２２において、セキュアチップ１１

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２に対して接続を要求するサーバ(Server)接続要求を送信する。

【０１１０】

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１２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１２が接続しようとするサーバ側装置２のサーバアプリケーション２１を指定するサーバ(Server)アプリ指定（の情報）が含まれる。

【０１１１】

また、セキュアチップ情報には、セキュアチップ１１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１１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１１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)などが含まれる。

【０１１２】

さらに、クライアント情報には、クライアント側装置１のハードウェアを表す情報（例えば、クライアント側装置１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１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１２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１２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含まれる。

【０１１３】

ここで、クライアントアプリケーション１２では、例えば、サーバアプリケーション２１に接続した後に、サーバアプリケーション２１からの、セキュアチップ情報その他の初期情報の要求を待って、その要求に応じて、セキュアチップ１１からセキュアチップ情報を取得し、初期情報に含めて、サーバアプリケーション２１に送信することもできる。

【０１１４】

但し、図１０に示したように、クライアントアプリケーション１２において、セキュアチップ１１からセキュアチップ情報を取得しておき、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２１に送信する場合の方が、クライアントアプリケーション１２とサーバアプリケーション２１との間のやりとりが少なくて済み、処理に要する時間の短縮化を図ることが可能となる。

【０１１５】

さらに、この場合、サーバ側装置２は、クライアント側装置１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１２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１２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１２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１２に適したコマンドやメッセージなどを意味する。

【０１１６】

サーバアプリケーション２１は、ステップＳ４１において、クライアントアプリケーション２３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１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。

【０１１７】

ステップＳ４２では、サーバアプリケーション２１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２２のセキュアチップマネージャモジュール１０２に供給する。セキュアチップマネージャモジュール

１０２は、ステップＳ６１において、サーバアプリケーション２１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２３に送信する。

【０１１８】

セキュアチップ処理モジュール２３は、ステップＳ８１において、セキュアチップマネージャモジュール１０２からのセキュアチップ情報に基づき、セキュアチップ１１からのアクセスに対する処理の範囲を設定する。

【０１１９】

即ち、セキュアチップ処理モジュール２３は、様々なセキュアチップやサービスの暗号関連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関連処理に必要な鍵を内蔵している。そして、セキュアチップ１１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２３は、セキュアチップ１１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暗号関連処理のみを行う（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２３は、セキュアチップ１１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。

【０１２０】

一方、セキュアチップマネージャモジュール１０２は、ステップＳ６１でサーバアプリケーション２１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、セキュアチップ１１とクライアントアプリケーション１２に対応した処理を行う状態となる。

【０１２１】

即ち、セキュアチップマネージャモジュール１０２は、各種のセキュアチップやクライアントアプリケーションに対応した処理を行うことができるようになっており、セキュアチップマネージャモジュール１０２は、ステップＳ６１でサーバアプリケーション２１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、セキュアチップ１１とクライアントアプリケーション１２に対応した処理を行う状態となる。

【０１２２】

例えば、セキュアチップマネージャモジュール１０２は、セキュアチップ１１に対する処理を行うのに必要なリソースを確保するとともに、クライアント側装置１のセキュアチップ１１の種別（例えば、ICカードに内蔵されるセキュアチップであるとか、携帯電話機に内蔵されるセキュアチップであるとかなど）に対応するコマンド体系を表す情報であるコマンド種別と、セキュアチップ１１の暗号処理種別を、セキュアチップ情報等から認識し、その後は、クライアント側装置１に対して送信されるコマンド等に対して、セキュアチップ１１の暗号処理種別に対応した暗号化等を行う状態となる。

【０１２３】

そして、セキュアチップマネージャモジュール１０２は、ステップＳ６２において、セキュアチップコマンドモジュール１０１に対し、初期化の指令を、セキュアチップ１１のコマンド種別とともに送信し、セキュアチップコマンドモジュール１０１は、ステップＳ５１において、その指令とコマンド種別を受信して、自身の状態を、セキュアチップ１１に対応した処理を行うことができるように初期化する。即ち、これにより、セキュアチップコマンドモジュール１０１は、サーバアプリケーション２１からのコマンドの作成の依頼に対して、セキュアチップ１１用のコマンド（セキュアチップ１１のコマンド種別が表すコマンド体系のコマンド）を作成する状態となる。

【０１２４】

その後、サーバアプリケーション２１は、例えば、セキュアチップ処理モジュール２３との間で、いわゆるなりすましを防止するための相互認証を行い、その相互認証が成功すると、セキュアチップ１１とセキュアチップ処理モジュール２３との間でも、なりすましを防止するための認証が行われる。

【０１２５】
ここで、セキュアチップ１１とセキュアチップ処理モジュール２３との間の認証は、セキュアチップ１１の暗号処理種別に基づいて行われる。即ち、セキュアチップ１１の暗号処理種別が、例えば、チャレンジアンドレスポンス方式の相互認証を表している場合には、セキュアチップ１１とセキュアチップ処理モジュール２３との間では、チャレンジアンドレスポンス方式による相互認証が行われる。なお、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２３は（セキュアチップ１１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１１との間でやりとりすることにより、相互認証を行う。この相互認証が成功すると、例えば、その相互認証時に、セキュアチップ処理モジュール２３が発生した乱数が、セキュアチップ１１とセキュアチップ処理モジュール２３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。

【０１２６】
この後、サーバ側装置２では、セキュリティチップ１１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、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１に送信される。また、クライアント側装置１でも、セキュリティチップ１１からサーバ側装置２に送信されるデータ等は、セキュリティチップ１１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２に送信される。

【０１２７】
このように、クライアント側装置１とサーバ側装置２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１とサーバ側装置２との間の通信路の暗号化、即ち、いわばVPN(Virtual Private Network)が実現される。なお、セッションキーを鍵として用いた暗号化は、セキュアチップ１１の暗号処理種別が表すアルゴリズムにしたがって行われる。

【０１２８】
サーバアプリケーション２１は、ステップＳ４３において、セキュアチップ１１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１０１に送信し、セキュアチップコマンドモジュール１０１は、ステップＳ５２において、サーバアプリケーション２１からのコマンドの作成の要求を受信する。

【０１２９】
そして、セキュアチップコマンドモジュール１０１は、ステップＳ５３において、サーバアプリケーション２１からのコマンドの作成の要求に応じて、セキュアチップ１１用のコマンドを作成し、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１０２に供給する。セキュアチップマネージャモジュール１０２は、ステップＳ６３において、セキュアチップコマンドモジュール１０１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Ｓ６４に進み、その要求を、セキュアチップ処理モジュール２３に送信する。

【０１３０】
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２３内にあるので、セキュアチップマネージャモジュール１０２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２３に要求する。

【０１３１】
セキュアチップ処理モジュール２３は、ステップＳ８２において、セキュアチップマネージャモジュール１０２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。そして、セキュアチップ処理モジュール２３は、ステップＳ８３において、その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１０２に送信し、セキュアチップマネージャモジュール１０２は、ステップＳ６５において、セキュアチップ処理モジュール２３からの暗号情報を受信する。

【０１３２】
そして、セキュアチップマネージャモジュール１０２は、ステップＳ６６において、セ

キュアチップ処理モジュール２３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１０１に送信する。

【０１３３】

セキュアチップコマンドモジュール１０１は、ステップＳ５４において、セキュアチップマネージャモジュール１０２からの暗号情報を受信して、ステップＳ５５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２１に送信する。

【０１３４】

サーバアプリケーション２１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１０１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、例えば、クライアント側装置１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１２に送信する。

【０１３５】

クライアントアプリケーション１２は、ステップＳ２４において、サーバアプリケーション２１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１１に送信する。

【０１３６】

セキュアチップ１１は、ステップＳ１３において、クライアントアプリケーション１２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。さらに、セキュアチップ１１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１２に送信する。なお、レスポンスデータは、セキュアチップ１１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。

【０１３７】

クライアントアプリケーション１２は、ステップＳ２６において、セキュアチップ１１からのレスポンスデータを受信して、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２１に送信する。

【０１３８】

サーバアプリケーション２１は、クライアントアプリケーション１２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１０１、セキュアチップマネージャモジュール１０２に送信する。

【０１３９】

なお、ユーザがクライアント側装置１を操作し、何らかのデータ（ユーザ入力データ）を入力した場合には、クライアントアプリケーション１２は、そのデータを、サーバアプリケーション２１に送信する。

【０１４０】

一方、セキュアチップマネージャモジュール１０２は、ステップＳ６７において、セキュアチップ処理モジュールに対して、セッションキーの要求を送信する。

【０１４１】

セキュアチップ処理モジュール２３は、ステップＳ８４において、セキュアチップマネージャモジュール１０２からのセッションキーの要求を受信して、ステップＳ８５に進み、その要求に応じて、セキュアチップ１１との相互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１０２に送信する。

【０１４２】

セキュアチップマネージャモジュール１０２は、ステップＳ６８において、セキュアチップ処理モジュール２３からのセッションキーを受信して保持する。

【０１４３】

ここで、その後は、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１０２で行われ、より高い秘匿性が要求される暗号化は、セキュアチップ処理モジュール２３内で行われる。

【０１４４】
従って、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１０２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、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２３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２３において、すべての暗号化（暗号関連処理）を行う場合に比較して、セキュアチップ処理モジュール２３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２３における処理時間を短くすることができる。
【０１４５】
なお、耐タンパ性のあるセキュアチップ処理モジュール２３を複数設け、その複数のセキュアチップ処理モジュール２３に、異なるセキュアチップに対する暗号関連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２３の負荷を軽減することができる。
【０１４６】
その後、サーバアプリケーション２１は、ステップＳ４６において、セキュアチップ１１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１０１に送信し、セキュアチップコマンドモジュール１０１は、ステップＳ５６において、サーバアプリケーション２１からのコマンドの作成の要求を受信する。
【０１４７】
そして、セキュアチップコマンドモジュール１０１は、ステップＳ５７において、サーバアプリケーション２１からのコマンドの作成の要求に応じて、セキュアチップ１１用のコマンドを作成し、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１０２に供給する。セキュアチップマネージャモジュール１０２は、ステップＳ６９において、セキュアチップコマンドモジュール１０１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。
【０１４８】
セキュアチップコマンドモジュール１０１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１０２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Ｓ７２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１０１に送信する。
【０１４９】
一方、セキュアチップコマンドモジュール１０１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１０２は、ステップＳ７０において、その特別なコマンドを実行する権利である実行権を表す権利書（権利証）（のデータ）の要求を、セキュアチップ処理モジュール２３に送信する。
【０１５０】
ここで、特別なコマンドとしては、例えば、セキュアチップ１１に対するエリア定義領域やサービス定義領域（図８）の登録や削除を要求するコマンドなどがある。
【０１５１】
セキュアチップ処理モジュール２３は、ステップＳ８６において、セキュアチップマネージャモジュール１０２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（権利証）（のデータ）を生成して暗号化する。さらに、セキュアチップ処理モジュール２３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Ｓ８７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１０２に送信する。
【０１５２】
なお、セキュアチップ処理モジュール２３は、過去に得たパッケージを記憶しており、セキュアチップマネージャモジュール１０２からの要求が、過去に生成された権利書を要求するものであり、その権利書を含むパッケージが記憶されている場合には、単に、その

パッケージを、セキュアチップマネージャモジュール１０２に送信する。
【０１５３】
セキュアチップマネージャモジュール１０２は、ステップＳ７１において、セキュアチップ処理モジュール２３からのパッケージを受信して、ステップＳ７２に進み、特別なコマンドをセク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１０１に送信する。
【０１５４】
セキュアチップコマンドモジュール１０１は、ステップＳ５８において、セキュアチップマネージャモジュール１０２からの暗号情報を受信して、ステップＳ５９に進み、その暗号情報を、サーバアプリケーション２１に送信する。
【０１５５】
サーバアプリケーション２１は、ステップＳ４７において、セキュアチップコマンドモジュール１０１からの暗号情報を受信して、ステップＳ４８に進み、その暗号情報を、例えば、クライアント側装置１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１２に送信する。
【０１５６】
クライアントアプリケーション１２は、ステップＳ２８において、サーバアプリケーション２１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１１に送信する。
【０１５７】
セキュアチップ１１は、ステップＳ１５において、クライアントアプリケーション１２からの暗号情報を受信し、その暗号情報を、セクションキーを用いて、コマンドに復号する。さらに、セキュアチップ１１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１２に送信する。
【０１５８】
クライアントアプリケーション１２は、ステップＳ３０において、セキュアチップ１１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２１に送信する。
【０１５９】
サーバアプリケーション２１は、ステップＳ４９において、クライアントアプリケーション１２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。
【０１６０】
その後、サーバアプリケーション２１は、クライアント側装置１との通信を終了する場合には、ステップＳ５０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１２を送信する。クライアントアプリケーション１２は、ステップＳ３２において、サーバアプリケーション２１からの終了通知を受信する。
【０１６１】
上述したように、セキュアサーバ２２（セキュアチップコマンドモジュール１０１およびセキュアチップマネージャモジュール１０２）と、セキュアチップ処理モジュール２３とは、例えば、暗号処理種別その他の仕様が異なる複数のセキュアチップ１１に対応することができるように構成することができる。そして、セキュアサーバ２２とセキュアチップ処理モジュール２３において、クライアント側装置１から送信されてくるセキュアチップ１１のセキュアチップ情報に応じて、セキュアチップ１１に対応した処理を行うことにより、暗号処理種別その他の仕様が異なるセキュアチップ１１ごとに、サーバアプリケーション２１を変更する必要がなくなる。即ち、各種の仕様のセキュリティチップ１１に対して、同一のサーバアプリケーション２１を使用することができる。
【０１６２】
次に、サービス提供者が、サーバ側装置２を用いて、新たなサービスの提供を開始する

場合には、一般に、サーバ側装置２の負荷試験が行われる。

【０１６３】

図１１は、サーバ側装置２の負荷試験を行う場合のサーバクライアントシステムの構成例を示している。

【０１６４】

図１１においては、サーバ側装置２に対して、多数のクライアント側装置１がネットワーク３を介して接続されている。そして、負荷試験は、多数のクライアント側装置１が、ネットワーク３を介してサーバ装置２にアクセスすることで行われる。

【０１６５】

図１１で説明した負荷試験によれば、多数のクライアント側装置１を用意する必要がある。

【０１６６】

そこで、図１２は、多数のクライアント側装置１を用いずに、擬似的に、多数のクライアント側装置１がサーバ側装置２にアクセスした状態をつくり出すことによって負荷試験を行う場合のサーバクライアントシステムの構成例を示している。

【０１６７】

図１２においては、１台のクライアント側装置１、サーバ側装置２、および負荷発生用クライアント側装置１１１が、ネットワーク３を介して接続されている。

【０１６８】

負荷発生用クライアント側装置１１１は、クライアント側装置１とサーバ側装置２との間のネットワーク３を介しての通信をモニタし、クライアント側装置１とサーバ側装置２とでやりとりされたデータを記憶する。そして、負荷発生用クライアント側装置１１１は、クライアント側装置１とサーバ側装置２とでやりとりされたデータのうちの、クライアント側装置１がサーバ側装置２に送信したデータを、ネットワーク３を介し、サーバ側装置２に繰り返し送信し、これにより、多数のクライアント側装置１がサーバ側装置２にアクセスした状態をつくり出す。

【０１６９】

図１３は、負荷発生用クライアント側装置１１１の機能的な構成例を示している。なお、負荷発生用クライアント側装置１１１のハードウェアの構成例は、例えば、クライアント側装置１のPC３２（図５）と同様である。

【０１７０】

負荷発生ツール１１２は、クライアント側装置１とサーバ側装置２との間でやりとりされるデータをキャプチャするソフトウェアであり、クライアント側装置１とサーバ側装置２との間の通信をモニタし、クライアント側装置１とサーバ側装置２とでやりとりされたデータを、記憶部１１３に供給する。なお、負荷発生ツール１１２としては、通信路をモニタする市販のツールなどを用いることができる。

【０１７１】

記憶部１１３は、負荷発生ツール１１２からのデータを記憶する。なお、負荷発生ツール１１２から記憶部１１３に供給されるデータは、クライアント側装置１とサーバ側装置２とでやりとりされたデータであるが、記憶部１１３では、そのデータのうちの、クライアント側装置１がサーバ側装置２に送信したデータだけを記憶するようにすることができる。

【０１７２】

通信制御部１１４は、記憶部１１３に記憶された、クライアント側装置１がサーバ側装置２に送信したデータをコピーし、ネットワーク３を介して、サーバ側装置２に、繰り返し送信する。

【０１７３】

ところで、サーバ側装置２においては、暗号化や復号などの暗号化に関連する暗号関連処理が、セッション単位で変化する。

【０１７４】

即ち、サーバ側装置２において、例えば、セキュアチップ処理モジュール２３は、セッションごとに、乱数を発生し、その乱数を用いて相互認証を行う。また、サーバ側装置２では、セキュアチップ処理モジュール２３における相互認証の成功後、例えば、その相互認証に用いられた乱数をセッションキーとして、そのセッションキーが、上述した通信路の暗号化に用いられる。

【０１７５】

一方、負荷発生用クライアント側装置１１１（図１３）では、通信制御部１１４が、記憶部１１３に記憶されたデータをコピーし、サーバ側装置２に繰り返し送信するため、サーバ側装置２でセッションごとに発生された乱数を用いて行われる相互認証に失敗し、サーバ側装置２において正常な処理が行われる場合の負荷試験を行うことができないことになる。

【０１７６】

そこで、図１４は、サーバ側装置２において正常な処理が行われる負荷試験を行うことができるようにするサーバ側装置２の機能的な構成例を示している。なお、図中、図２や図９に示した場合と対応する部分については、同一の符号を付してあり、以下では、その説明は、適宜省略する。即ち、図１４のサーバ側装置２は、モジュール選択部１２１と負荷試験用セキュアチップ処理モジュール１２２が新たに設けられている他は、図２や図９における場合と同様に構成されている。

【０１７７】

モジュール選択部１２１は、セキュアチップ処理モジュール２３と負荷試験用セキュアチップ処理モジュール１２２のうちの一方を選択してセキュアサーバ２２に接続し、これにより、選択した方に、クライアント側装置１や負荷発生用クライアント側装置１１１とやりとりするデータに対する暗号関連処理を行わせる。

【０１７８】

負荷試験用セキュアチップ処理モジュール１２２は、負荷試験用の暗号関連処理を行う。即ち、負荷試験用セキュアチップ処理モジュール１２２は、例えば、セッション単位で変化しない暗号関連処理、つまり、セッションごとに同一の暗号関連処理を行う。

【０１７９】

次に、図１５のフローチャートを参照して、図１４のサーバ側装置２の、負荷試験時の処理について説明する。

【０１８０】

まず最初に、ステップＳ１０１において、モジュール選択部１２１は、セキュアチップ処理モジュール２３と負荷試験用セキュアチップ処理モジュール１２２のうちの、負荷試験用セキュアチップ処理モジュール１２２を選択してセキュアサーバ２２に接続し、これにより、サーバ側装置２を、負荷試験用セキュアチップ処理モジュール１２２にクライアント側装置１や負荷発生用クライアント側装置１１１とやりとりするデータに対する暗号関連処理を行わせる状態にする。

【０１８１】

なお、セキュアチップ処理モジュール２３と負荷試験用セキュアチップ処理モジュール１２２のうちの一方を選択するように、モジュール選択部１２１を制御することは、例えば、サービス提供者（のオペレータ）が、サーバ側装置２を直接操作することによって行うこともできるし、クライアント側装置１や負荷発生用クライアント側装置１１１から、ネットワーク３を介してサーバ側装置２にアクセスすることによって行うこともできる。

【０１８２】

サーバ側装置２では、その後、ステップＳ１０１からＳ１０２に進み、クライアント側装置１や負荷発生用クライアント側装置１１１からのアクセスに対して、例えば、図１０で説明した処理（サーバ側処理）が行われる。但し、サーバ側装置２において、図１０で説明した処理のうちの、セキュアチップ処理モジュール２３が行う処理は、負荷試験用セキュアチップ処理モジュール１２２で行われ、これにより、セキュアチップ処理モジュール２３が行う処理として、負荷試験用セキュアチップ処理モジュール１２２において、セ

ッションに依存しない暗号関連処理、即ち、例えば、異なるセッションに対して、常に一定の暗号情報を作成する処理（同一のデータに対して、常に、同一の暗号化結果が得られる処理）が行われる。

【０１８３】

一方、サービス提供者（のオペレータ）は、クライアント側装置１を操作し、これにより、クライアント側装置１とサーバ側装置２との間で、サービスを提供するためのデータのやりとりを行わせる。なお、このとき、サーバ側装置２では、上述したように、負荷試験用セキュアチップ処理モジュール１２２において、セッションに依存しない暗号関連処理が行われる。

【０１８４】

また、サービス提供者（のオペレータ）は、負荷発生用クライアント側装置１１１（図１３）を操作し、負荷発生ツール１１２に、クライアント側装置１とサーバ側装置２との間でやりとりされるデータをキャプチャさせ、記憶部１１３に供給して記憶させる。

【０１８５】

さらに、サービス提供者（のオペレータ）は、負荷発生用クライアント側装置１１１（図１３）を操作し、記憶部１１３に記憶されたデータのうちの、クライアント側装置１がサーバ側装置２に送信したデータをコピーし、クライアント側装置１がサーバ側装置２に送信したのと同様の手順で、サーバ側装置２に送信させる。

【０１８６】

負荷発生用クライアント側装置１１１では、記憶部１１３に記憶されたデータのコピーと、サーバ側装置２への送信とを、多重的（並列的）に、多数回繰り返し、これにより、擬似的に、多数のクライアント側装置１がサーバ側装置２にアクセスした状態をつくり出す。

【０１８７】

サーバ側装置２においては、上述したように、セキュアチップ処理モジュール２３と負荷試験用セキュアチップ処理モジュール１２２のうちの、負荷試験用セキュアチップ処理モジュール１２２が選択され、セッションに依存しない暗号関連処理が行われるので、即ち、例えば、すべてのセッションについて、同一の値（乱数）を用いて相互認証を行い、さらに、その相互認証の成功後は、その値がセッションキーとされるので、相互認証に失敗することにより、サーバ側装置２において正常な処理が行われなくなることを防止することができる。

【０１８８】

従って、サーバ側装置２において正常な処理が行われる場合の負荷試験を、セキュア、かつ容易に行うことができる。

【０１８９】

即ち、クライアント側装置１の処理をエミュレートするエミュレータを用い、そのエミュレータを、サービス提供者に貸し出すといった、クライアント側装置１の暗号関連処理の内容（ひいては、サーバ側装置２の暗号関連処理の内容）が外部に漏洩するおそれが生じるようなことをせずに（セキュアに）、サーバ側装置２の負荷試験を行うことができる。

【０１９０】

さらに、多数のクライアント側装置１を用意せずに、通信路をモニタする市販のツールなどの負荷発生ツール１１２を利用して（容易に）、サーバ側装置２の負荷試験を行うことができる。

【０１９１】

なお、サーバ側装置２の負荷試験が終了し、通常の運用がされるときには、モジュール選択部１２１は、セキュアチップ処理モジュール２３を選択するように制御される。この制御は、例えば、サービス提供者（のオペレータ）が、サーバ側装置２を直接操作することによって行うこともできるし、クライアント側装置１や負荷発生用クライアント側装置１１１から、ネットワーク３を介してサーバ側装置２にアクセスすることによって行うこ

ともできる。

【０１９２】

次に、図１６は、サーバ側装置２において正常な処理が行われる負荷試験を行うことができるようにするサーバ側装置２の他の機能的な構成例を示している。なお、図中、図２や図９に示した場合と対応する部分については、同一の符号を付してあり、以下では、その説明は、適宜省略する。

【０１９３】

図１６においては、サーバ側装置２のセキュアチップ処理モジュール２３が、モジュール選択部１３１、鍵／乱数発生モジュール１３２、および負荷試験用鍵／乱数発生モジュール１３３を内蔵している。

【０１９４】

モジュール選択部１３１は、鍵／乱数発生モジュール１３２と負荷試験用鍵／乱数発生モジュール１３３のうちの一方を選択してセキュアサーバ２２に接続し、これにより、選択した方に、クライアント側装置１や負荷発生用クライアント側装置１１１とやりとりするデータに対する暗号関連処理、即ち、ここでは、特に、データの暗号化／復号に用いる鍵の発生や、相互認証に用いる乱数の発生を行わせる。

【０１９５】

鍵／乱数発生モジュール１３２は、通常時（負荷試験時等でない、サーバ側装置２が通常の運用をされるとき）に、モジュール選択部１３１によって選択され、セッションごとに異なる鍵や乱数を発生する。

【０１９６】

負荷試験用鍵／乱数発生モジュール１３３は、負荷試験時に、モジュール選択部１３１によって選択され、セッションに依存しない鍵や乱数を発生する。

【０１９７】

なお、図１６のセキュリティチップ処理モジュール２３では、鍵／乱数発生モジュール１３２と負荷試験用鍵／乱数発生モジュール１３３のうちの、モジュール選択部１３１が選択している方が発生する鍵や乱数を用いて、データの暗号化／復号や相互認証などが行われる。

【０１９８】

次に、図１７のフローチャートを参照して、図１６のサーバ側装置２の、負荷試験時の処理について説明する。

【０１９９】

まず最初に、ステップＳ１１１において、モジュール選択部１３１は、鍵／乱数発生モジュール１３２と負荷試験用鍵／乱数発生モジュール１３３のうちの、負荷試験用鍵／乱数発生モジュール１３３を選択してセキュアサーバ２２に接続し、これにより、サーバ側装置２を、負荷試験用鍵／乱数発生モジュール１３３にクライアント側装置１や負荷発生用クライアント側装置１１１とやりとりするデータに対する暗号関連処理としての鍵や乱数の発生を行わせる状態にする。

【０２００】

なお、鍵／乱数発生モジュール１３２と負荷試験用鍵／乱数発生モジュール１３３のうちの一方を選択するように、モジュール選択部１３１を制御することは、例えば、サービス提供者（のオペレータ）が、サーバ側装置２を直接操作することによって行うこともできるし、クライアント側装置１や負荷発生用クライアント側装置１１１から、ネットワーク３を介してサーバ側装置２にアクセスすることによって行うこともできる。

【０２０１】

サーバ側装置２では、その後、ステップＳ１１１からＳ１１２に進み、クライアント側装置１や負荷発生用クライアント側装置１１１からのアクセスに対して、例えば、図１０で説明した処理（サーバ側処理）が行われる。但し、サーバ側装置２において、データの暗号化／復号に用いられる鍵や、相互認証に用いられる乱数の発生は、負荷試験用鍵／乱数発生モジュール１３３で行われ、これにより、セキュアチップ処理モジュール２３では

、セッションに依存しない鍵や乱数を用いて、データの暗号化／復号鍵や相互認証が行われる。

【０２０２】

一方、サービス提供者（のオペレータ）は、クライアント側装置１を操作し、これにより、クライアント側装置１とサーバ側装置２との間で、サービスを提供するためのデータのやりとりを行わせる。なお、このとき、サーバ側装置２では、上述したように、負荷試験用鍵／乱数発生モジュール１３３において、セッションに依存しない鍵や乱数が発生され、セキュアチップ処理モジュール２３において、その鍵や乱数を用いて、データの暗号化／復号鍵や相互認証、即ち、セッションに依存しない暗号化／復号鍵や、相互認証が行われる。

【０２０３】

また、サービス提供者（のオペレータ）は、負荷発生用クライアント側装置１１１（図１３）を操作し、負荷発生ツール１１２に、クライアント側装置１とサーバ側装置２との間でやりとりされるデータをキャプチャさせ、記憶部１１３に供給して記憶させる。

【０２０４】

さらに、サービス提供者（のオペレータ）は、負荷発生用クライアント側装置１１１（図１３）を操作し、記憶部１１３に記憶されたデータのうちの、クライアント側装置１がサーバ側装置２に送信したデータをコピーし、クライアント側装置１がサーバ側装置２に送信したのと同様の手順で、サーバ側装置２に送信させる。

【０２０５】

負荷発生用クライアント側装置１１１では、記憶部１１３に記憶されたデータのコピーと、サーバ側装置２への送信とを、多重的に、多数回繰り返し、これにより、擬似的に、多数のクライアント側装置１がサーバ側装置２にアクセスした状態をつくり出す。

【０２０６】

サーバ側装置２においては、上述したように、鍵／乱数発生モジュール１３２と負荷試験用鍵／乱数発生モジュール１３３のうちの、負荷試験用鍵／乱数発生モジュール１３３が選択され、セッションに依存しない鍵や乱数が発生され、その鍵や乱数を用いて、データの暗号化／復号鍵や相互認証が行われるので、サーバ側装置２においては、負荷発生用クライアント側装置１１１から送信されてくる、クライアント側装置１がサーバ側装置２に送信したデータのコピーを対象に、正常な処理を行うことができる。

【０２０７】

従って、図１６のサーバ側装置２でも、図１４における場合と同様に、サーバ側装置２において正常な処理が行われる場合の負荷試験を、セキュア、かつ容易に行うことができる。

【０２０８】

なお、サーバ側装置２の負荷試験が終了し、通常の運用がされるときには、モジュール選択部１３１は、鍵／乱数発生モジュール１３２を選択するように制御される。この制御は、例えば、サービス提供者（のオペレータ）が、サーバ側装置２を直接操作することによって行うこともできるし、クライアント側装置１や負荷発生用クライアント側装置１１１から、ネットワーク３を介してサーバ側装置２にアクセスすることによって行うこともできる。

【０２０９】

ところで、サーバ側装置２のサーバアプリケーション２１（図２）が提供するサービスによっては、サーバ側装置２において、クライアント側装置１の情報が管理される場合があり、この場合、クライアント側装置１とサーバ側装置２との間のやりとりによって、サーバ側装置２で管理されているクライアント側装置１の情報が書き換えられることがある。

【０２１０】

一方、負荷発生用クライアント側装置１１１は、上述したように、クライアント側装置１がサーバ側装置２に送信したデータのコピーを送信するため、負荷発生用クライアント

側装置１１１がサーバ側装置２に送信するデータは、クライアント側装置１がサーバ側装置２に送信したデータのまま変化しない。

【０２１１】

従って、サーバ側装置２で管理されているクライアント側装置１の情報が変化する（書き換えられる）のに対して、負荷発生用クライアント側装置１１１からサーバ側装置２に送信されるデータは変化しないため、例えば、クライアント側装置１がサーバ側装置２に送信するデータに、クライアント側装置１の情報が含まれ、かつ、サーバ側装置２が、自身が管理するクライアント側装置１の情報と、クライアント側装置１から送信されてきたデータに含まれるクライアント側装置１の情報との一致性を判定し、その一致性がある場合にのみ正常な処理を行うときには、サーバ側装置２において、正常な処理が行われず、その結果、サーバ側装置２において正常な処理が行われる場合の負荷試験を行うことができないことがある。

【０２１２】

具体的には、例えば、サーバ側装置２のサーバアプリケーション２１が、電子マネーサービスを提供するアプリケーションで、クライアント側装置１（図２）のユーザが、そのクライアント側装置１（のセキュアチップ１１）に電子マネーをチャージしておき、サーバ側装置２が、クライアント側装置１にチャージされている電子マネーの残高の範囲内で、電子マネーによる商品を購入することができる電子マネーサービスを提供することとする。

【０２１３】

また、クライアント側装置１は、電子マネーサービスの提供を受けるにあたって、自身（クライアント側装置１（のセキュアチップ１１））にチャージされている電子マネーの残高を含むデータを、サーバ側装置２に送信するものとする。

【０２１４】

さらに、サーバ側装置２は、電子マネーサービスの提供にあたって、クライアント側装置１（のセキュアチップ１１）にチャージされている電子マネーの残高を管理し、クライアント側装置１から送信されているデータに含まれる、クライアント側装置１にチャージされている電子マネーの残高と、サーバ側装置２が管理する残高とが一致する場合にのみ、電子マネーの残高からの商品の代金の減額等の処理を行うものとする。

【０２１５】

この場合、例えば、クライアント側装置１に、10000円の電子マネーがチャージされており、その電子マネーを用いて、100円の商品を購入する場合、クライアント側装置１からサーバ側装置２には、クライアント側装置１にチャージされている電子マネーの残高である10000円を含むデータが送信される。サーバ側装置２では、クライアント側装置１から送信されてきたデータに含まれる10000円が、サーバ側装置２が管理するクライアント側装置１の電子マネーの残高と一致すれば、10000円から、商品の代金である100円を減額する処理が行われる。さらに、サーバ側装置２では、その減額の結果である9900円によって、クライアント側装置１の電子マネーの残高が更新される。即ち、サーバ側装置２では、サーバ側装置２が管理している（クライアント側装置１の）電子マネーの残高が、10000円から9900円に書き換えられる。

【０２１６】

また、サーバ側装置２は、クライアント側装置１に対して、チャージされている電子マネーの残高を9900円に更新するコマンドを送信し、クライアント側装置１は、サーバ側装置２からのコマンドに応じて、電子マネーの残高を更新する。即ち、クライアント側装置１では、自身が記憶している電子マネーの残高が、10000円から9900円に書き換えられる。

【０２１７】

従って、クライアント側装置１において、次回の商品購入時には、更新後の残高である9900円が送信され、この残高は、サーバ側装置２で管理されているクライアント側装置１の電子マネーの残高と一致するので、サーバ側装置２では、次回の商品購入時においても

、前回と同様に、商品の代金を減額する処理等の正常な処理が行われる。

【０２１８】

以上のように、サーバ側装置２が、自身が管理するクライアント側装置１の情報と、クライアント側装置１から送信されてきたデータに含まれるクライアント側装置１の情報との一致性を判定し、その一致性がある場合にのみ正常な処理を行う場合、負荷試験時に、負荷発生用クライアント側装置１１１において、クライアント側装置１がサーバ側装置２に送信したデータの、いわゆるデットコピーが送信されると、サーバ側装置２において、正常な処理が行われないことになる。

【０２１９】

即ち、負荷発生用クライアント側装置１１１は、クライアント側装置１とサーバ側装置２との間のデータのやりとりをモニタし、クライアント側装置１からサーバ側装置２に送信されたデータのコピーを送信する。従って、負荷発生用クライアント側装置１１１において、例えば、クライアント側装置１に10000円の電子マネーがチャージされていたときの、クライアント側装置１とサーバ側装置２との間のやりとりがモニタされた場合には、負荷発生用クライアント側装置１１１は、クライアント側装置１（負荷発生用クライアント側装置１１１）にチャージされている電子マネーの残高として、常に、10000円を送信する。

【０２２０】

この電子マネーの残高（10000円）は、サーバ側装置２で管理されている、商品の代金が減額された残高（9900円）と一致しないため、サーバ側装置２では、商品の代金を減額する処理等の正常な処理が行われず、その結果、サーバ側装置２において正常な処理が行われる場合の負荷試験を行うことができない。

【０２２１】

そこで、サーバ側装置２において、サーバアプリケーション２１が行う処理のうちの、電子マネーのサービスを提供するための処理（例えば、上述したような残高の一致性を判定する処理など）をバイパスして、負荷試験を行う方法がある。

【０２２２】

しかしながら、電子マネーのサービスを提供するための処理をバイパスして、負荷試験を行ったのでは、サーバ側装置２において、電子マネーのサービスを提供するための処理を含めた、実際の運用時にサーバ側装置２にかかるすべての負荷を考慮した負荷試験を行うことができない。

【０２２３】

そこで、図１８は、負荷発生用クライアント側装置１１１の他の機能的な構成例を示している。なお、図中、図１３における場合と対応する部分については、同一の符号を付してあり、以下では、その説明は、適宜省略する。即ち、図１８の負荷発生用クライアント側装置１１１は、負荷用暗号／復号ロジック部１４１および通信データ書き換えロジック部１４２が新たに設けられている他は、図１３における場合と同様に構成されている。

【０２２４】

負荷用暗号／復号ロジック部１４１は、記憶部１１３に記憶された、クライアント側装置１がサーバ側装置２に送信したデータ（暗号化されたデータ）を読み出して復号し、その結果得られる復号データを、通信データ書き換えロジック部１４２に供給する。また、負荷用暗号／復号ロジック部１４１は、通信データ書き換えロジック部１４２から供給されるデータを暗号化し、その結果得られる暗号情報を、記憶部１１３に供給して記憶させる。

【０２２５】

通信データ書き換えロジック部１４２は、負荷用暗号／復号ロジック部１４１から供給される復号データの一部を書き換え、負荷用暗号／復号ロジック部１４１に供給する。

【０２２６】

以上のように構成される負荷発生用クライアント装置１１１では、負荷用暗号／復号ロジック部１４１が、記憶部１１３に記憶されたデータを復号データに復号し、通信データ

書き換えロジック部１４２が、その復号データの一部を書き換え、負荷用暗号／復号ロジック部１４１に供給する。負荷用暗号／復号ロジック部１４１は、一部が書き換えられた復号データを暗号情報に暗号化し、記憶部１１３に記憶させる。そして、通信制御部１４１は、以上のようにして記憶部１１３に記憶された、復号データの一部が書き換えられ、暗号化された暗号情報が、サーバ側装置２に送信される。

【０２２７】

即ち、クライアント側装置１（図２）では、基本的に、データを、サーバ側装置２に送信する場合に、そのデータが、セキュアチップ１１で、暗号情報に暗号化される。従って、負荷発生ツール１１２によりモニタされ、記憶部１１３に記憶された、クライアント側装置１からサーバ側装置２に送信されたデータは、暗号情報に暗号化されている。

【０２２８】

そこで、負荷用暗号／復号ロジック部１４１では、記憶部１１３に記憶された、クライアント側装置１からサーバ側装置２に送信されたデータとしての暗号情報を、元のデータ（いわゆる平文）としての復号データに復号する。

【０２２９】

また、記憶部１１３に記憶された、クライアント側装置１からサーバ側装置２に送信されたデータに、クライアント側装置１の情報が含まれる場合には、上述したように、サーバ側装置２において正常な処理が行われないことがある。

【０２３０】

そこで、通信データ書き換えロジック部１４２では、負荷用暗号／復号ロジック部１４１からの復号データの一部である、その復号データに含まれるクライアント側装置１の情報を書き換える。

【０２３１】

即ち、復号データに含まれるクライアント側装置１の情報が、例えば、クライアント側装置１にチャージされている電子マネーの残高であり、サーバ側装置２のサーバアプリケーション２１において、その残高から、例えば、負荷試験用に固定の金額を減額する処理が行われる場合には、通信データ書き換えロジック部１４２は、復号データに含まれるクライアント側装置１の情報としての、クライアント側装置１にチャージされている電子マネーの残高を、適宜書き換える。

【０２３２】

即ち、通信制御部１１４が、最初に、サーバ側装置２に送信するデータについては、通信データ書き換えロジック部１４２は、そのデータに含まれる残高を、その残高から、固定の金額を減額した値に書き換える。また、通信制御部１１４が、２回目に、サーバ側装置２に送信するデータについては、通信データ書き換えロジック部１４２は、そのデータに含まれる残高を、その残高から、固定の金額の２倍の金額を減額した値に書き換える。さらに、通信制御部１１４が、３回目に、サーバ側装置２に送信するデータについては、通信データ書き換えロジック部１４２は、そのデータに含まれる残高を、その残高から、固定の金額の３倍の金額を減額した値に書き換える。以下、同様に、通信データ書き換えロジック部１４２は、サーバ側装置１に送信されるデータに含まれる残高を、サーバ側装置２で管理されている残高に一致するように書き換えていく。

【０２３３】

なお、ここでは、通信制御部１１４がサーバ側装置２に送信するデータに含まれる残高を書き換えるようにしたが、残高以外の情報（データ）を書き換えるようにすることも可能である。

【０２３４】

即ち、例えば、クライアント側装置１のセキュアチップ１１が、例えば、ICカード３１（図３）に内蔵されており、さらに、クライアント側装置１からサーバ側装置２に送信されるデータに、ICカード３１に付されたユニークなIDであるカードIDが含まれるとする。

【０２３５】

また、サーバ側装置２は、カードIDに対応付けて、そのカードIDに対応するICカードの

電子マネーの残高を管理し、クライアント側装置１からのデータに含まれるカードIDに対応付けられている残高を、商品の代金を減額した減額結果に更新するようになっているものとする。

【０２３６】

そして、サーバ側装置２では、負荷試験用に、多数のカードIDに対応付けて、一定額の電子マネーが記憶されており、さらに、クライアント側装置１でも、負荷試験用に、その一定額の電子マネーが記憶されているものとする。

【０２３７】

この場合、通信データ書き換えロジック部１４２において、通信制御部１１４がサーバ側装置２に送信するデータに含まれるカードID（ICカード３１のカードID）を、サーバ側装置２に記憶されている多数のカードIDのそれぞれに順次書き換えることにより、通信制御部１１４がサーバ側装置２に送信するデータに含まれる残高を書き換えなくても、サーバ側装置２では、正常な処理が行われることになる。

【０２３８】

即ち、この場合、負荷試験において、クライアント側装置１がサーバ側装置２に送信するデータに含まれる、クライアント側装置１にチャージされている電子マネーの残高は、サーバ側装置２で多数のカードIDに対応付けて記憶されている電子マネーの残高それぞれに等しい。

【０２３９】

従って、通信データ書き換えロジック部１４２において、クライアント側装置１がサーバ側装置２にデータを送信するごとに、そのデータに含まれるカードIDを、サーバ側装置２に記憶されている多数のカードIDの、まだ、サーバ側装置２に送信するデータに含めていない１つに書き換えることにより、そのデータに含まれる電子マネーの残高と、そのデータに含まれるカードIDに対応付けてサーバ側装置２に記憶されている電子マネーの残高とは、必ず一定額で一致するので、サーバ側装置２では、正常な処理が行われることになる。

【０２４０】

次に、図１９を参照して、図１８の負荷発生用クライアント側装置１１１の動作について、さらに説明する。

【０２４１】

サービス提供者（のオペレータ）は、クライアント側装置１を操作し、これにより、クライアント側装置１とサーバ側装置２との間で、サービスを提供するためのデータのやりとりを行わせる。

【０２４２】

ここで、サーバ側装置２では、図１５または図１７で説明した処理が行われる。

【０２４３】

サービス提供者（のオペレータ）は、負荷発生用クライアント側装置１１１（図１８）を操作し、負荷発生ツール１１２に、クライアント側装置１とサーバ側装置２との間でやりとりされるデータをキャプチャさせ、記憶部１１３に供給して記憶させる。

【０２４４】

さらに、サービス提供者（のオペレータ）は、負荷発生用クライアント側装置１１１（図１８）を操作し、記憶部１１３に記憶されたデータのうちの、クライアント側装置１がサーバ側装置２に送信したデータをコピーし、その一部を書き換えた上で、クライアント側装置１がサーバ側装置２に送信したのと同様の手順で、サーバ側装置２に送信させる。

【０２４５】

即ち、記憶部１１３は、ステップＳ１２１において、そこに記憶されているデータのうちの、クライアント側装置１がサーバ側装置２に送信したデータとしての暗号情報を読み出し、負荷用暗号／復号ロジック部１４１に供給する。

【０２４６】

負荷用暗号／復号ロジック部１４１は、ステップＳ１３１において、記憶部１１３から

の暗号情報を受信して、ステップＳ１３２に進み、その暗号情報を復号データに復号する。

【０２４７】

なお、サーバ側装置２では、上述したように、セッションに依存しないセッションキーを鍵として用いて暗号化／復号が行われる。従って、負荷試験時には、クライアント側装置１でも、そのようなセッションキーを鍵として用いて暗号化／復号が行われるから、記憶部１１３に記憶されている暗号情報は、セッションに依存しないセッションキーを鍵として用いて復号することができる。

【０２４８】

負荷用暗号／復号ロジック部１４１は、ステップＳ１３２で復号データを得ると、ステップＳ１３３に進み、その復号データを、通信データ書き換えロジック部１４２に送信する。

【０２４９】

通信データ書き換えロジック部１４２は、ステップＳ１４１において、負荷用暗号／復号ロジック部１４１からの復号データを受信して、ステップＳ１４２に進み、その復号データの一部、即ち、例えば、その復号データに含まれる電子マネーの残高や、カードIDなど書き換える。

【０２５０】

そして、通信データ書き換えロジック部１４２は、ステップＳ１４３において、一部を書き換えた復号データを、負荷用暗号／復号ロジック部１４１に送信する。

【０２５１】

負荷用暗号／復号ロジック部１４１は、ステップＳ１３４において、通信データ書き換えロジック部１４２からの復号データを受信して、ステップＳ１３５に進み、その復号データを暗号情報に暗号化する。

【０２５２】

なお、ステップＳ１３５の暗号化は、例えば、ステップＳ１３２における復号に用いられた鍵を用いて行われる。

【０２５３】

負荷用暗号／復号ロジック部１４１は、ステップＳ１３６において、ステップＳ１３５で得た暗号情報を、記憶部１１３に供給する。

【０２５４】

記憶部１１３は、ステップＳ１２２において、負荷用暗号／復号ロジック部１４１からの暗号情報を受信して記憶し、ステップＳ１２３に進み、その暗号情報を、送信制御部１１４に供給する。

【０２５５】

通信制御部１１４は、ステップＳ１５１において、記憶部１３３からの暗号情報を受信して、ステップＳ１５２に進み、その暗号情報を、サーバ側装置２に送信する。

【０２５６】

図１８の負荷発生用クライアント側装置１１１では、以上のような、記憶部１１３に記憶されたデータのコピーの一部の書き換えと、その書き換え後のデータの、サーバ側装置２への送信とが、多重的に、多数回繰り返され、これにより、擬似的に、多数のクライアント側装置１がサーバ側装置２にアクセスした状態がつくり出される。

【０２５７】

なお、負荷用暗号／復号ロジック部１４１は、例えば、耐タンパ性のある装置内に設けるようにすることができる。

【図面の簡単な説明】

【０２５８】

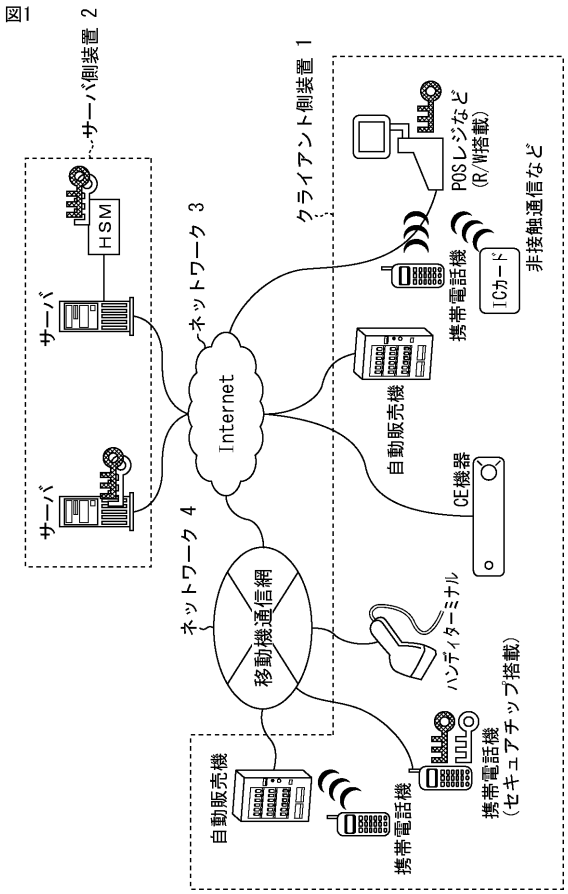
【図１】本発明が適用されるサーバクライアントシステムの構成例を示す図である。

【図２】クライアント側装置１とサーバ側装置２の機能的な構成例を示すブロック図である。

【図３】クライアント側装置１とサーバ側装置２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。
【図４】クライアント側装置１とサーバ側装置２の他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。
【図５】クライアントアプリケーション１２がインストールされるPC３２のハードウェアの構成例を示すブロック図である。
【図６】サーバアプリケーション２１およびセキュアサーバ２２がインストールされるコンピュータ３３のハードウェアの構成例を示すブロック図である。
【図７】セキュアチップ１１のハードウェアの構成例を示すブロック図である。
【図８】メモリ９３のディレクトリ構造を示す図である。
【図９】セキュアサーバ２２の詳細な構成例を示すブロック図である。
【図１０】クライアント側装置１とサーバ側装置２の動作を説明するための図である。
【図１１】サーバ側装置２の負荷試験を行う場合のサーバクライアントシステムの構成例を示す図である。
【図１２】擬似的に、多数のクライアント側装置１がサーバ側装置２にアクセスした状態をつくり出すことによって負荷試験を行う場合の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１３】負荷発生用クライアント側装置１１１の機能的な構成例を示すブロック図である。
【図１４】サーバ側装置２において正常な処理が行われる負荷試験を行うことができるようにするサーバ側装置２の機能的な構成例を示すブロック図である。
【図１５】サーバ側装置２の、負荷試験時の処理を説明するフローチャートである。
【図１６】サーバ側装置２において正常な処理が行われる負荷試験を行うことができるようにするサーバ側装置２の他の機能的な構成例を示すブロック図である。
【図１７】サーバ側装置２の、負荷試験時の処理を説明するフローチャートである。
【図１８】負荷発生用クライアント側装置１１１の他の機能的な構成例を示すブロック図である。
【図１９】負荷発生用クライアント側装置１１１の動作を説明するための図である。
【符号の説明】
【０２５９】
１　クライアント側装置，　２　サーバ側装置，　３，４　ネットワーク，　１１　セキュアチップ，　１２　クライアントアプリケーション，　１３　R/W，　２１　サーバアプリケーション，　２２　セキュアサーバ，　２３　セキュアチップ処理モジュール，　３１　ICカード，　３２　PC，　３３　コンピュータ，　３４　携帯電話機，　４１　バス，　４２　CPU，　４３　ROM，　４４　RAM，　４５　ハードディスク，　４６　出力部，　４７　入力部，　４８　通信部，　４９　ドライブ，　５０　入出力インタフェース，　５１　リムーバブル記録媒体，　６１　バス，　６２　CPU，　６３　ROM，　６４　RAM，　６５　ハードディスク，　６６　出力部，　６７　入力部，　６８　通信部，　６９　ドライブ，　７０　入出力インタフェース，　７１　リムーバブル記録媒体，　８１　通信処理部，　８２　データ処理部，　９１　CPU，　９２　暗号関連処理部，　９３　メモリ，　１０１　セキュアチップコマンドモジュール，　１０２　セキュアチップマネージャモジュール，　１１１　負荷発生用クライアント側装置，　１１２　負荷発生ツール，　１１３　記憶部，　１１４　通信制御部，　１２１　モジュール選択部，　１２２　負荷試験用セキュアチップ処理モジュール，　１３１　モジュール選択部，　１３２　鍵／乱数発生モジュール，　１３３　負荷試験用鍵／乱数発生モジュール，　１４１　負荷用暗号／復号ロジック部，　１４２　通信データ書き換えロジック部

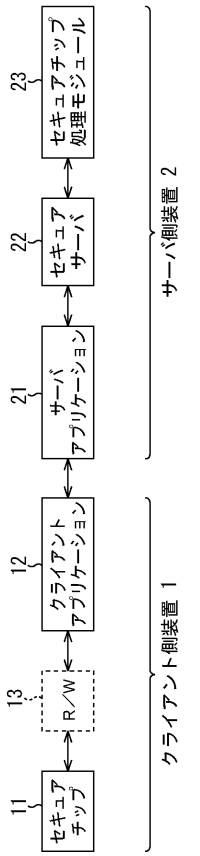
【図１】

図1



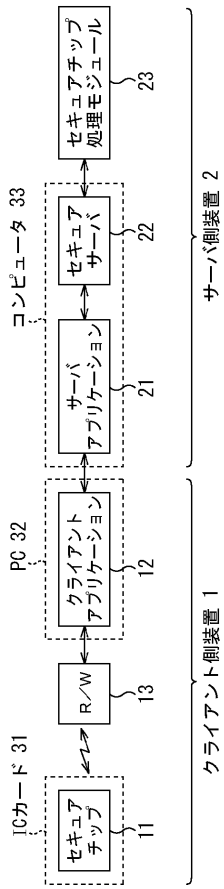
【図２】

図2



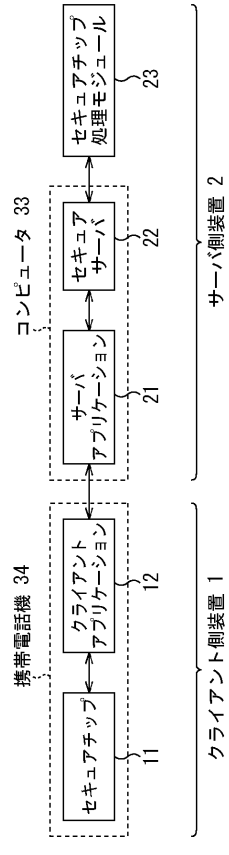
【図３】

図3

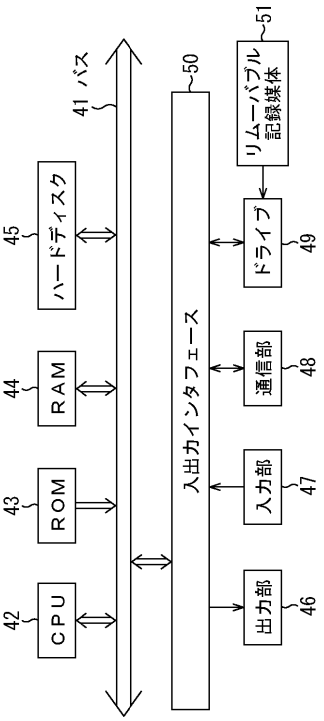


【図４】

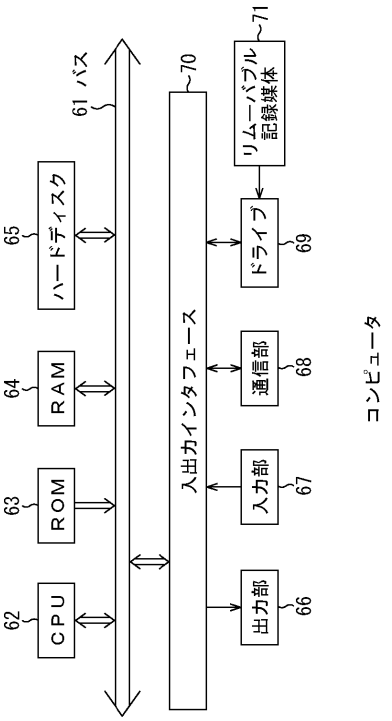
図4



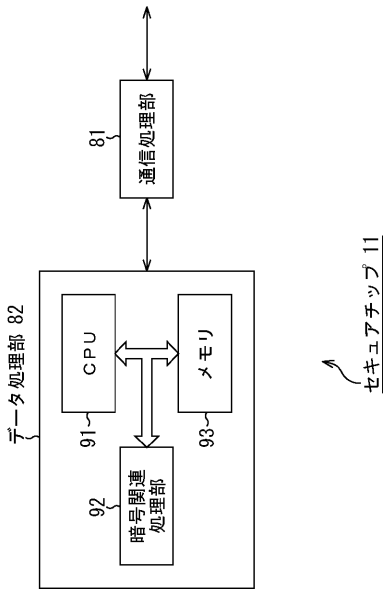
【図５】
図5



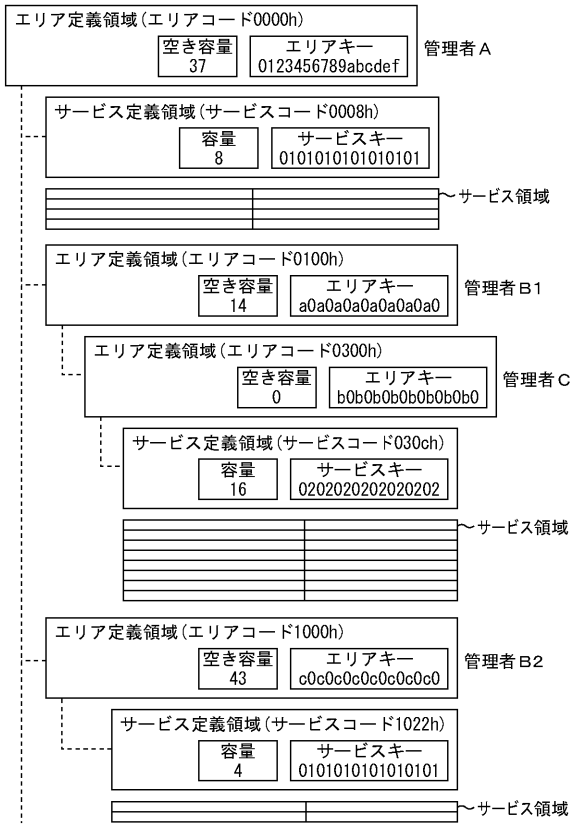
【図６】
図6



【図７】
図7

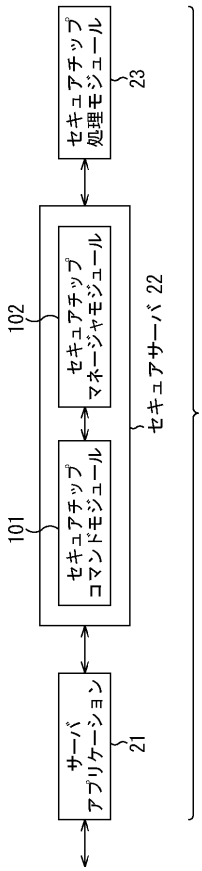


【図８】
図8

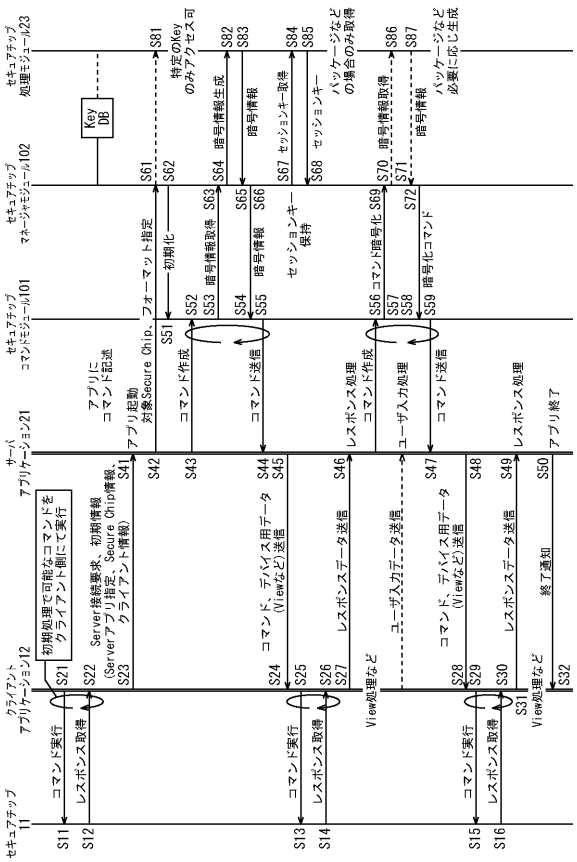


ディレクト構造

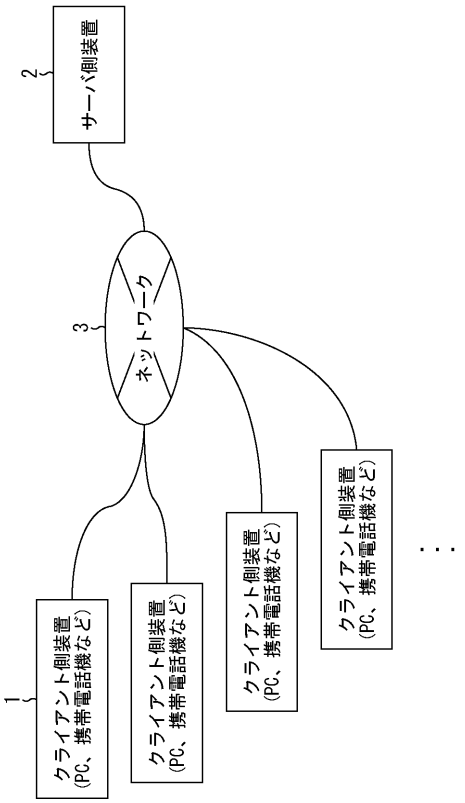
【図９】
図9



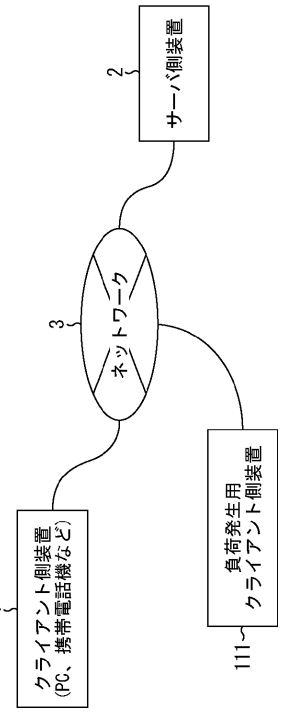
【図１０】
図10



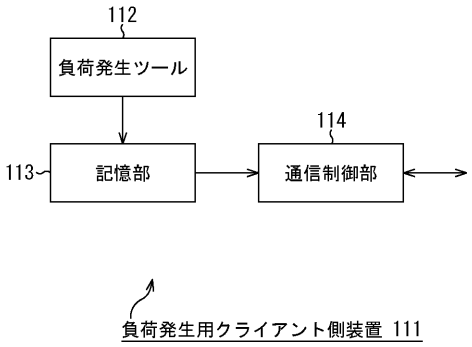
【図１１】
図11



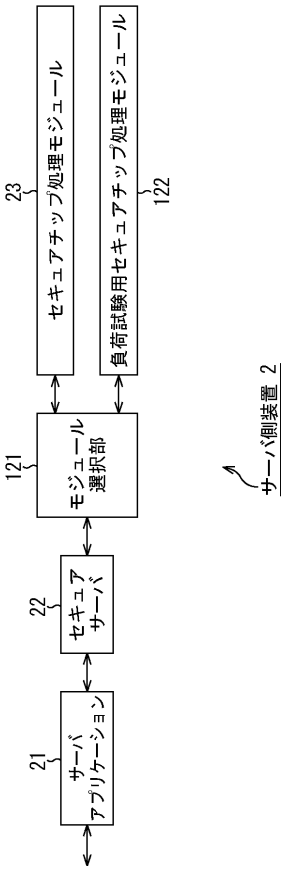
【図１２】
図12



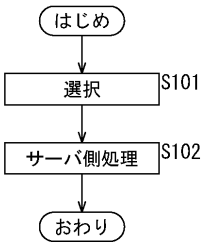
【図１３】
図13



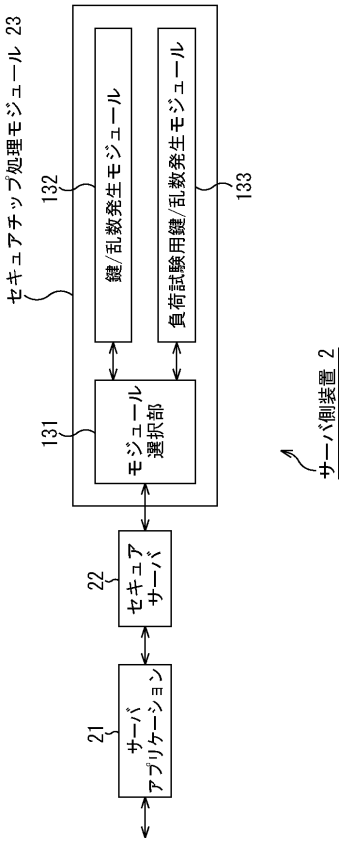
【図１４】
図14



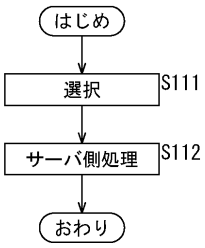
【図１５】
図15



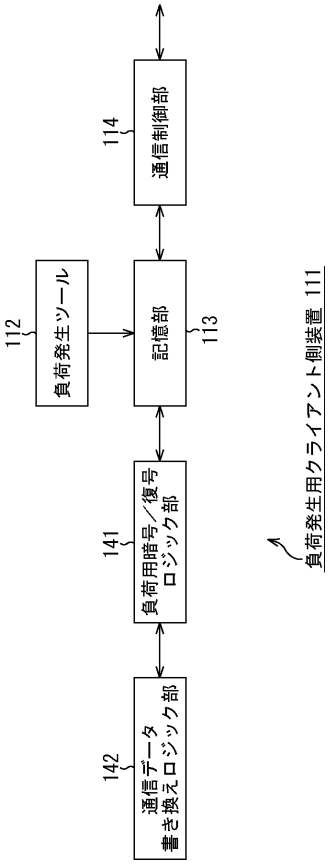
【図１６】
図16



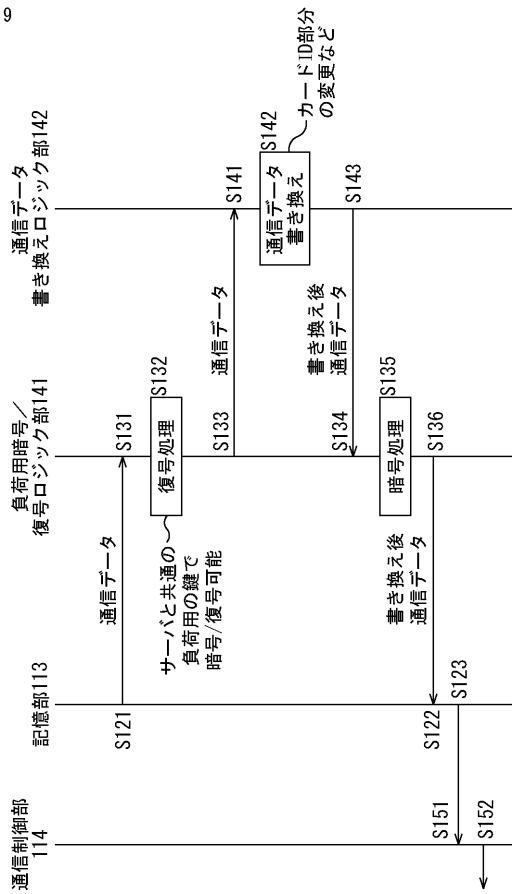
【図１７】
図17



【図１８】
図18



【図１９】
図19



フロントページの続き

審査官　桑原　雅子

(56)参考文献　特開２００３－１７３２７７（ＪＰ，Ａ）
林　經正、外６名，ＩＧＡＰを用いたＩＰマルチキャストコンテンツ配信システムの検討，電子情報通信学会技術研究報告，社団法人電子情報通信学会，２００３年　６月１２日，第１０３巻，第１２１号，ｐ．２５－２８
清水　亮博、外１名，キャッシュ可能なＨＴＴＰのアクセス制御手法，情報処理学会研究報告，社団法人情報処理学会，１９９７年１１月　７日，第９７巻，第１０４号，ｐ．２１３－２１８

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　１５／００
Ｇ０６Ｆ　１３／００
Ｇ０６Ｆ　１１／２２