(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2006-129143
(P2006-129143A)
(43)公開日　平成18年5月18日(2006.5.18)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/08	(2006.01)	H04L	9/00	601C	5J104
		H04L	9/00	601E	

審査請求 未請求　請求項の数 8　OL　（全 17 頁）

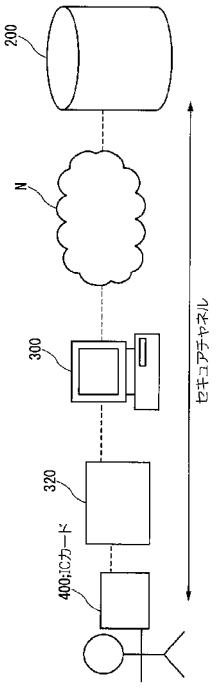
(21)出願番号　特願2004-315632 (P2004-315632)
(22)出願日　平成16年10月29日 (2004.10.29)

(71)出願人　000003193
凸版印刷株式会社
東京都台東区台東１丁目５番１号
(74)代理人　100064908
弁理士　志賀　正武
(74)代理人　100108578
弁理士　高橋　詔男
(74)代理人　100089037
弁理士　渡邊　隆
(74)代理人　100101465
弁理士　青山　正和
(74)代理人　100094400
弁理士　鈴木　三義
(74)代理人　100108453
弁理士　村山　靖彦

最終頁に続く

(54)【発明の名称】秘密情報送受信システム及び方法、サーバー装置及びプログラム、並びに鍵情報保持装置

(57)【要約】
【課題】　鍵情報保持装置（ICカード）とサーバー装置の間で安全な通信経路を確立する秘密情報送受信システム及び方法、サーバー装置及びプログラム、並びに鍵情報保持装置を提供する。
【解決手段】　インターネット網N上のサーバー２００は、サーバー証明書をＰＣ３００に送信する。ＰＣ３００は、サーバー証明書を検証する。ＩＣカード４００のセキュリティチップは、クライアント証明書をＰＣ３００に送信する。ＰＣ３００は、クライアント証明書をサーバー２００に送信する。サーバー２００は、クライアント証明書を検証する。サーバー２００は記憶部のセッション鍵を暗号化し、サーバーの秘密鍵で署名を生成し、これらをＰＣ３００に送信する。ＰＣ３００はサーバー証明書のサーバー公開鍵を用いて受信した署名を検証し、セキュリティチップに送信する。セキュリティチップは暗号化セッション鍵をクライアント秘密鍵で復号する。
【選択図】　図１



【特許請求の範囲】
【請求項１】
ネットワークに接続したサーバー装置及び前記サーバー装置とセッションを確立しデータを送受信する通信装置と、鍵情報を格納し、前記通信装置に組み込まれる鍵情報保持装置とを有する秘密情報送受信システムにおいて、
前記サーバー装置は、
第１の公開鍵および第１の秘密鍵と、前記第１の公開鍵の正当性を保障する証明書と、セッション鍵を格納するサーバー記憶手段と、
前記第１の公開鍵の正当性を保障する証明書を前記通信装置に送信する第１の証明書送信制御手段と、
前記通信装置から受信する、前記第２の公開鍵の正当性を保障する証明書が正当か否かを検証する第１の証明書検証手段と、
前記第２の公開鍵の正当性を保障する証明書から前記通信装置の公開鍵を取り出し、前記セッション鍵を前記通信装置の公開鍵で暗号化するセッション鍵暗号化手段と、
前記サーバー装置の秘密鍵で前記暗号化されたセッション鍵の正当性を示す情報を作成するセッション鍵正当情報生成手段と、
前記暗号化されたセッション鍵と前記セッション鍵の正当性を示す情報とを前記通信装置に送信する暗号化セッション鍵送信制御手段とを備え、
前記鍵情報保持装置は、
第２の公開鍵および第２の秘密鍵と、前記第２の公開鍵の正当性を保障する証明書とを格納する鍵情報保持装置記憶手段と、
前記第２の公開鍵の正当性を保障する証明書を前記通信装置に送信する第２の証明書送信制御手段と、
前記通信装置から受信する前記暗号化されたセッション鍵を、前記第２の秘密鍵で復号する暗号化セッション鍵復号手段とを備え、
前記通信装置は、
前記サーバー装置に前記第１の公開鍵の正当性を保障する証明書を送信するよう要求し、前記鍵情報保持装置に前記第２の公開鍵の正当性を保障する証明書を送信するよう要求する証明書要求手段と、
前記サーバー装置から受信する前記第１の公開鍵の正当性を保障する証明書が正当か否かを検証する第２の証明書検証手段と、
前記鍵情報保持装置から受信する前記第２の公開鍵の正当性を保障する証明書を前記サーバー装置に送信する証明書中継送信手段と、
前記第１の公開鍵の正当性を保障する証明書から前記第１の公開鍵を取り出し、前記サーバー装置から受信する前記暗号化されたセッション鍵の正当性を示す情報が正当か否かを前記第１の公開鍵で検証するセッション鍵正当情報検証手段と、
前記サーバー装置から受信する前記暗号化されたセッション鍵を前記鍵情報保持装置に送信する暗号化セッション鍵送信手段と
を備えることを特徴とする秘密情報送受信システム。
【請求項２】
ネットワークに接続したサーバー装置及び前記サーバー装置とセッションを確立しデータを送受信する通信装置と、鍵情報を格納し、前記通信装置に組み込まれる鍵情報保持装置とを有する秘密情報送受信システムにおいて、
前記サーバー装置は、
第１の公開鍵および第１の秘密鍵と、前記第１の公開鍵の正当性を保障する証明書を格納するサーバー記憶手段と、
前記第１の公開鍵の正当性を保障する証明書を前記通信装置に送信する第１の証明書送信制御手段と、
前記通信装置から受信する第２の公開鍵の正当性を保障する証明書が正当か否かを検証する第１の証明書検証手段と、

前記通信装置から受信する前記第２の公開鍵の正当性を保障する証明書から前記第２の公開鍵を取り出し、前記通信装置から受信する暗号化されたセッション鍵の正当性を示す情報が正当か否かを前記第２の公開鍵で検証するセッション鍵正当情報検証手段と、
前記暗号化されたセッション鍵を前記第１の秘密鍵で復号する暗号化セッション鍵復号手段とを備え、
前記鍵情報保持装置は、
前記第２の公開鍵および第２の秘密鍵と、前記第２の公開鍵の正当性を保障する証明書と、セッション鍵を格納する鍵情報保持装置記憶手段と、
前記第２の公開鍵の正当性を保障する証明書を前記通信装置に送信する第２の証明書送信制御手段と、
前記通信装置から前記第１の公開鍵を受信する公開鍵受信手段と、
前記セッション鍵を読み出し、前記受信した第１の公開鍵で暗号化するセッション鍵暗号化手段と、
前記第２の秘密鍵で前記暗号化されたセッション鍵の正当性を示す情報を作成するセッション鍵正当情報生成手段と、
前記暗号化されたセッション鍵と前記暗号化されたセッション鍵の正当性を示す情報とを前記通信装置に送信する暗号化セッション鍵送信制御手段とを備え、
前記通信装置は、
前記サーバー装置に前記第１の公開鍵の正当性を保障する証明書を送信するよう要求し、前記鍵情報保持装置に前記第２の公開鍵の正当性を保障する証明書を送信するよう要求する証明書要求手段と、
前記サーバー装置から受信する前記第１の公開鍵の正当性を保障する証明書が正当か否かを検証する第２の証明書検証手段と、
前記鍵情報保持装置から受信する前記第２の公開鍵の正当性を保障する証明書を前記サーバー装置に送信する証明書中継送信手段と、
前記第１の公開鍵の正当性を保障する証明書から前記第１の公開鍵を取り出し、前記第１の公開鍵を前記鍵情報保持装置に送信する公開鍵送信手段と、
前記鍵情報保持装置から受信する前記暗号化されたセッション鍵を前記サーバー装置に送信するよう要求する暗号化セッション鍵送信手段と
を備えることを特徴とする秘密情報送受信システム。

【請求項３】
前記セッション鍵は、セッションごとに異なることを特徴とする、請求項１または２に記載の秘密情報送受信システム。

【請求項４】
ネットワークに接続したサーバー装置及び前記サーバー装置とセッションを確立しデータを送受信する通信装置と、鍵情報を格納し、前記通信装置に組み込まれる鍵情報保持装置とを有する秘密情報送受信システムにおいて、
前記サーバー装置は、
前記第１の公開鍵および第１の秘密鍵と、セッション鍵を格納するサーバー記憶手段と、
前記第１の公開鍵を前記通信装置に送信する第１の公開鍵送信制御手段と、
前記通信装置から前記第２の公開鍵を受信し、前記セッション鍵を前記第２の公開鍵で暗号化するセッション鍵暗号化手段と、
前記第１の秘密鍵で前記暗号化されたセッション鍵の正当性を示す情報を作成するセッション鍵正当情報生成手段と、
前記暗号化されたセッション鍵と前記セッション鍵の正当性を示す情報とを前記通信装置に送信する暗号化セッション鍵送信制御手段とを備え、
前記鍵情報保持装置は、
前記第２の公開鍵および第２の秘密鍵を格納する鍵情報保持装置記憶手段と、
前記第２の公開鍵を前記通信装置に送信する第２の公開鍵送信制御手段と、

前記通信装置から受信する前記暗号化されたセッション鍵を、前記第２の秘密鍵で復号する暗号化セッション鍵復号手段とを備え、
前記通信装置は、
前記サーバー装置に前記第１の公開鍵を送信するよう要求し、前記鍵情報保持装置に前記第２の公開鍵を送信するよう要求する公開鍵要求手段と、
前記第２の公開鍵を前記鍵情報保持装置から受信し、該第２の公開鍵を前記サーバー装置に送信する公開鍵中継送信手段と、
前記サーバー装置から受信する前記暗号化されたセッション鍵の正当性を示す情報が正当か否かを前記サーバー装置の公開鍵で検証するセッション鍵正当情報検証手段と、
前記サーバー装置から受信する前記暗号化されたセッション鍵を前記鍵情報保持装置に送信する暗号化セッション鍵送信手段と
を備えることを特徴とする秘密情報送受信システム。
【請求項５】
ネットワークに接続したサーバー装置及び前記サーバー装置とセッションを確立しデータを送受信する通信装置と、鍵情報を格納し、前記通信装置に組み込まれる鍵情報保持装置とを有する秘密情報送受信システムにおけるサーバー装置であって、
第１の公開鍵および第１の秘密鍵と、前記第１の公開鍵の正当性を保障する証明書と、セッション鍵を格納するサーバー記憶手段と、
前記第１の公開鍵の正当性を保障する証明書を前記通信装置に送信する第１の証明書送信制御手段と、
前記通信装置から受信する第２の公開鍵の正当性を保障する証明書が正当か否かを検証する第１の証明書検証手段と、
前記第２の公開鍵の正当性を保障する証明書から前記第２の公開鍵を取り出し、前記セッション鍵を前記第２の公開鍵で暗号化するセッション鍵暗号化手段と、
前記第１の秘密鍵で前記暗号化されたセッション鍵の正当性を示す情報を作成するセッション鍵正当情報生成手段と、
前記暗号化されたセッション鍵と前記暗号化されたセッション鍵の正当性を示す情報とを前記通信装置に送信する暗号化セッション鍵送信制御手段とを備えることを特徴とするサーバー装置。
【請求項６】
ネットワークに接続し、第１の公開鍵及び第１の秘密鍵と、前記第１の公開鍵の正当性を保障する証明書とセッション鍵とが格納された前記サーバー装置と、前記ネットワークに接続し、前記サーバー装置とセッションを確立しデータを送受信する通信装置と、前記通信装置に組み込まれ、第２の公開鍵と前記第２の公開鍵の正当性を保障する証明書とが格納された鍵情報保持装置とを有する秘密情報送受信システムにおいて、
前記サーバー装置のコンピュータに、
前記前記第１の公開鍵の正当性を保障する証明書を前記通信装置に送信するステップと、
前記鍵情報保持装置から受信する前記第２の公開鍵の正当性を保障する証明書が正当か否かを検証するステップと、
前記前記第２の公開鍵の正当性を保障する証明書から前記第２の公開鍵を取り出し、前記セッション鍵を前記第２の公開鍵で暗号化するステップと、
前記第１の秘密鍵で前記暗号化されたセッション鍵の正当性を示す情報を作成するステップと、
前記暗号化されたセッション鍵と前記暗号化されたセッション鍵の正当性を示す情報とを前記通信装置に送信するステップとを実行させるためのプログラム。
【請求項７】
ネットワークに接続したサーバー装置及び前記サーバー装置とセッションを確立しデータを送受信する通信装置と、鍵情報を格納し、前記通信装置に組み込まれる鍵情報保持装置とを有する秘密情報送受信システムにおける鍵情報保持装置であって、

前記鍵情報保持装置は、
公開鍵および秘密鍵と、前記公開鍵の正当性を保障する証明書とを格納する鍵情報保持装置記憶手段と、
前記証明書を前記通信装置に送信するよう要求する証明書送信制御手段と、
前記通信装置から受信する前記暗号化されたセッション鍵を前記秘密鍵で復号する暗号化セッション鍵復号手段とを備えることを特徴とする鍵情報保持装置。
【請求項８】
ネットワークに接続し、第１の公開鍵及び第１の秘密鍵と前記第１の公開鍵の正当性を保障する証明書とセッション鍵とが格納された前記サーバー装置と、前記ネットワークに接続し、前記サーバー装置とセッションを確立しデータを送受信する通信装置と、前記通信装置に組み込まれ、第２の公開鍵及び第２の秘密鍵と前記第２の公開鍵の正当性を保障する証明書とが格納された鍵情報保持装置とを有する秘密情報送受信システムにおいて、
前記サーバー装置が、前記第１の公開鍵の正当性を保障する証明書を前記通信装置に送信し、
前記通信装置が、前記サーバー装置から送信された前記第１の公開鍵の正当性を保障する証明書の正当性を検証し、
前記鍵情報保持装置が、前記第２の公開鍵の正当性を保障する証明書を前記通信装置に送信し、
前記通信装置が、前記鍵情報保持装置から送信された前記第２の公開鍵の正当性を保障する証明書を前記サーバー装置に送信し、
前記サーバー装置が、
前記通信装置から送信された前記第２の公開鍵の正当性を保障する証明書が正当か否かを検証し、
前記セッション鍵を暗号化し、
前記サーバー装置の秘密鍵で前記暗号化されたセッション鍵の正当性を示す情報を作成し、
前記暗号化されたセッション鍵と前記暗号化されたセッション鍵の正当性を示す情報とを前記通信装置に送信し、
前記通信装置が、
前記第１の公開鍵の正当性を保障する証明書から前記第１の公開鍵を取り出し、前記暗号化されたセッション鍵の正当性を示す情報が正当か否かを前記第１の公開鍵で検証し、
前記暗号化されたセッション鍵を前記鍵情報保持装置に送信し、
前記鍵情報保持装置が、
前記通信装置から受信する前記暗号化されたセッション鍵を前記通信装置の秘密鍵で復号することを特徴とする秘密情報送受信方法。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、秘密情報送受信システム及び方法、サーバー装置及びプログラム、並びに鍵情報保持装置に関する。
【背景技術】
【０００２】
近年において、インターネットを利用した音楽配信システムや、企業・学校内でイントラネットを利用した教育講座の受講システム等が普及している。有料の音楽データや教育講座のデータ等（以下、コンテンツという）は、そのコンテンツを購入した購入者のみが受信できるものである必要がある。例えば、不特定多数の人間が使用する端末（学校や企業の教育施設内、或いはインターネットカフェ等の共有端末等）を利用してコンテンツを受信する場合には、図７で示すように、購入者が個々に持つICカード４００を、ＩＣカードリーダライタ３２０を経由してPC３００に接続し、PC３００がICカード４００内の情報

をサーバー２００に送信してサーバー２００から認証されることで、その後、コンテンツを受信する。

【０００３】

しかしながら、サーバー２００から送信されるコンテンツは、インターネット上の通信を暗号化する従来技術であり、サーバー２００とPC３００間のみでしか使用できないSSL（Secure Socket Layer）を利用して配信されるため、PC３００とＩＣカードリーダライタ３２０間、或いはICカード４００とＩＣカードリーダライタ３２０間では、暗号化されていないデータがやり取りされる場合があり、悪意ある第３者にデータを盗聴されてしまう、或いは改竄されるという問題がある。

【０００４】

上記のICカード４００とＩＣカードリーダライタ３２０間で、安全にデータをやり取りする技術として、特許文献1の技術が公開されている。この技術は、ICカード４００がＩＣカードリーダライタ３２０と相互に公開鍵を交換し、その後のICカード４００とＩＣカードリーダライタ３２０間のデータを全て公開鍵暗号方式で暗号化する技術である。しかしながら、この技術を利用すると、本来サーバーが直接確認すべきICカード４００の情報が、一旦ＩＣカードリーダライタ３２０によってデータ変換されることとなり、セキュリティが必ずしも確保されないという問題点がある。

【特許文献１】特開2004－38445号公報

【発明の開示】

【発明が解決しようとする課題】

【０００５】

この発明は上記の点を鑑みてなされたもので、鍵情報保持装置（ICカード）とサーバー装置の間で安全な通信経路を確立する秘密情報送受信システム及び方法、サーバー装置及びプログラム、並びに鍵情報保持装置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】

【０００６】

上記の課題を解決するために、本発明は、ネットワークに接続したサーバー装置及び前記サーバー装置とセッションを確立しデータを送受信する通信装置と、鍵情報を格納し、前記通信装置に組み込まれる鍵情報保持装置とを有する秘密情報送受信システムにおいて、前記サーバー装置は、第１の公開鍵および第１の秘密鍵と、前記第１の公開鍵の正当性を保障する証明書と、セッション鍵を格納するサーバー記憶手段と、前記第１の公開鍵の正当性を保障する証明書を前記通信装置に送信する第１の証明書送信制御手段と、前記通信装置から受信する、前記第２の公開鍵の正当性を保障する証明書が正当か否かを検証する第１の証明書検証手段と、前記第２の公開鍵の正当性を保障する証明書から前記通信装置の公開鍵を取り出し、前記セッション鍵を前記通信装置の公開鍵で暗号化するセッション鍵暗号化手段と、前記サーバー装置の秘密鍵で前記暗号化されたセッション鍵の正当性を示す情報を作成するセッション鍵正当情報生成手段と、前記暗号化されたセッション鍵と前記セッション鍵の正当性を示す情報とを前記通信装置に送信する暗号化セッション鍵送信制御手段とを備え、前記鍵情報保持装置は、第２の公開鍵および第２の秘密鍵と、前記第２の公開鍵の正当性を保障する証明書とを格納する鍵情報保持装置記憶手段と、前記第２の公開鍵の正当性を保障する証明書を前記通信装置に送信する第２の証明書送信制御手段と、前記通信装置から受信する前記暗号化されたセッション鍵を、前記第２の秘密鍵で復号する暗号化セッション鍵復号手段とを備え、前記通信装置は、前記サーバー装置に前記第１の公開鍵の正当性を保障する証明書を送信するよう要求し、前記鍵情報保持装置に前記第２の公開鍵の正当性を保障する証明書を送信するよう要求する証明書要求手段と、前記サーバー装置から受信する前記第１の公開鍵の正当性を保障する証明書が正当か否かを検証する第２の証明書検証手段と、前記鍵情報保持装置から受信する前記第２の公開鍵の正当性を保障する証明書を前記サーバー装置に送信する証明書中継送信手段と、前記第１の公開鍵の正当性を保障する証明書から前記第１の公開鍵を取り出し、前記サーバー装置から受信する前記暗号化されたセッション鍵の正当性を示す情報が正当か否かを前記

第１の公開鍵で検証するセッション鍵正当情報検証手段と、前記サーバー装置から受信する前記暗号化されたセッション鍵を前記鍵情報保持装置に送信する暗号化セッション鍵送信手段とを備えることを特徴とする秘密情報送受信システムである。

これにより、ネットワーク上にあるサーバー装置が生成するセッション鍵を安全に鍵情報保持装置に送信するため、サーバー装置と鍵情報保持装置間で、安全な通信を行うことができる。

【０００７】

また、本発明は、ネットワークに接続したサーバー装置及び前記サーバー装置とセッションを確立しデータを送受信する通信装置と、鍵情報を格納し、前記通信装置に組み込まれる鍵情報保持装置とを有する秘密情報送受信システムにおいて、前記サーバー装置は、第１の公開鍵および第１の秘密鍵と、前記第１の公開鍵の正当性を保障する証明書を格納するサーバー記憶手段と、前記第１の公開鍵の正当性を保障する証明書を前記通信装置に送信する第１の証明書送信制御手段と、前記通信装置から受信する第２の公開鍵の正当性を保障する証明書が正当か否かを検証する第１の証明書検証手段と、前記通信装置から受信する前記第２の公開鍵の正当性を保障する証明書から前記第２の公開鍵を取り出し、前記通信装置から受信する暗号化されたセッション鍵の正当性を示す情報が正当か否かを前記第２の公開鍵で検証するセッション鍵正当情報検証手段と、前記暗号化されたセッション鍵を前記第１の秘密鍵で復号する暗号化セッション鍵復号手段とを備え、前記鍵情報保持装置は、前記第２の公開鍵および第２の秘密鍵と、前記第２の公開鍵の正当性を保障する証明書と、セッション鍵を格納する鍵情報保持装置記憶手段と、前記第２の公開鍵の正当性を保障する証明書を前記通信装置に送信する第２の証明書送信制御手段と、前記通信装置から前記第１の公開鍵を受信する公開鍵受信手段と、前記セッション鍵を読み出し、前記受信した第１の公開鍵で暗号化するセッション鍵暗号化手段と、前記第２の秘密鍵で前記暗号化されたセッション鍵の正当性を示す情報を作成するセッション鍵正当情報生成手段と、前記暗号化されたセッション鍵と前記暗号化されたセッション鍵の正当性を示す情報とを前記通信装置に送信する暗号化セッション鍵送信制御手段とを備え、前記通信装置は、前記サーバー装置に前記第１の公開鍵の正当性を保障する証明書を送信するよう要求し、前記鍵情報保持装置に前記第２の公開鍵の正当性を保障する証明書を送信するよう要求する証明書要求手段と、前記サーバー装置から受信する前記第１の公開鍵の正当性を保障する証明書が正当か否かを検証する第２の証明書検証手段と、前記鍵情報保持装置から受信する前記第２の公開鍵の正当性を保障する証明書を前記サーバー装置に送信する証明書中継送信手段と、前記第１の公開鍵の正当性を保障する証明書から前記第１の公開鍵を取り出し、前記第１の公開鍵を前記鍵情報保持装置に送信する公開鍵送信手段と、前記鍵情報保持装置から受信する前記暗号化されたセッション鍵を前記サーバー装置に送信するよう要求する暗号化セッション鍵送信手段とを備えることを特徴とする秘密情報送受信システムである。

これにより、鍵情報保持装置が生成するセッション鍵を安全にネットワーク上にあるサーバー装置に送信するため、サーバー装置と鍵情報保持装置間で、安全な通信を行うことができる。

【０００８】

好ましくは、本発明の秘密情報送受信システムは、前記セッション鍵は、セッションごとに異なる。

これにより、ネットワーク上のサーバー装置と、鍵情報保持装置の間で確立されるセッションごとに、セッション鍵を更新するため、通信経路をより安全にすることができる。

【０００９】

また、本発明は、ネットワークに接続したサーバー装置及び前記サーバー装置とセッションを確立しデータを送受信する通信装置と、鍵情報を格納し、前記通信装置に組み込まれる鍵情報保持装置とを有する秘密情報送受信システムにおいて、前記サーバー装置は、前記第１の公開鍵および第１の秘密鍵と、セッション鍵を格納するサーバー記憶手段と、前記第１の公開鍵を前記通信装置に送信する第１の公開鍵送信制御手段と、前記通信装置

から前記第２の公開鍵を受信し、前記セッション鍵を前記第２の公開鍵で暗号化するセッション鍵暗号化手段と、前記第１の秘密鍵で前記暗号化されたセッション鍵の正当性を示す情報を作成するセッション鍵正当情報生成手段と、前記暗号化されたセッション鍵と前記セッション鍵の正当性を示す情報とを前記通信装置に送信する暗号化セッション鍵送信制御手段とを備え、前記鍵情報保持装置は、前記第２の公開鍵および第２の秘密鍵を格納する鍵情報保持装置記憶手段と、前記第２の公開鍵を前記通信装置に送信する第２の公開鍵送信制御手段と、前記通信装置から受信する前記暗号化されたセッション鍵を、前記第２の秘密鍵で復号する暗号化セッション鍵復号手段とを備え、前記通信装置は、前記サーバー装置に前記第１の公開鍵を送信するよう要求し、前記鍵情報保持装置に前記第２の公開鍵を送信するよう要求する公開鍵要求手段と、前記第２の公開鍵を前記鍵情報保持装置から受信し、該第２の公開鍵を前記サーバー装置に送信する公開鍵中継送信手段と、前記サーバー装置から受信する前記暗号化されたセッション鍵の正当性を示す情報が正当か否かを前記サーバー装置の公開鍵で検証するセッション鍵正当情報検証手段と、前記サーバー装置から受信する前記暗号化されたセッション鍵を前記鍵情報保持装置に送信する暗号化セッション鍵送信手段とを備えることを特徴とする秘密情報送受信システムである。

これにより、証明書を使用せずに鍵情報保持装置が生成するセッション鍵をネットワーク上にあるサーバー装置に送信するため、証明書生成、管理等の処理を行う認証局を必要としないため、システム構築が容易になる。

【００１０】

また、本発明は、ネットワークに接続したサーバー装置及び前記サーバー装置とセッションを確立しデータを送受信する通信装置と、鍵情報を格納し、前記通信装置に組み込まれる鍵情報保持装置とを有する秘密情報送受信システムにおけるサーバー装置であって第１の公開鍵および第１の秘密鍵と、前記第１の公開鍵の正当性を保障する証明書と、セッション鍵を格納するサーバー記憶手段と、前記第１の公開鍵の正当性を保障する証明書を前記通信装置に送信する第１の証明書送信制御手段と、前記通信装置から受信する第２の公開鍵の正当性を保障する証明書が正当か否かを検証する第１の証明書検証手段と、前記第２の公開鍵の正当性を保障する証明書から前記第２の公開鍵を取り出し、前記セッション鍵を前記第２の公開鍵で暗号化するセッション鍵暗号化手段と、前記第１の秘密鍵で前記暗号化されたセッション鍵の正当性を示す情報を作成するセッション鍵正当情報生成手段と、前記暗号化されたセッション鍵と前記暗号化されたセッション鍵の正当性を示す情報とを前記通信装置に送信する暗号化セッション鍵送信制御手段とを備えることを特徴とするサーバー装置である。

【００１１】

また、本発明は、ネットワークに接続し、第１の公開鍵及び第１の秘密鍵と、前記第１の公開鍵の正当性を保障する証明書とセッション鍵とが格納された前記サーバー装置と、前記ネットワークに接続し、前記サーバー装置とセッションを確立しデータを送受信する通信装置と、前記通信装置に組み込まれ、第２の公開鍵と前記第２の公開鍵の正当性を保障する証明書とが格納された鍵情報保持装置とを有する秘密情報送受信システムにおいて、前記サーバー装置のコンピュータに、前記前記第１の公開鍵の正当性を保障する証明書を前記通信装置に送信するステップと、前記鍵情報保持装置から受信する前記第２の公開鍵の正当性を保障する証明書が正当か否かを検証するステップと、前記前記第２の公開鍵の正当性を保障する証明書から前記第２の公開鍵を取り出し、前記セッション鍵を前記第２の公開鍵で暗号化するステップと、前記第１の秘密鍵で前記暗号化されたセッション鍵の正当性を示す情報を作成するステップと、前記暗号化されたセッション鍵と前記暗号化されたセッション鍵の正当性を示す情報とを前記通信装置に送信するステップとを実行させるためのプログラムである。

【００１２】

また、本発明は、ネットワークに接続したサーバー装置及び前記サーバー装置とセッションを確立しデータを送受信する通信装置と、鍵情報を格納し、前記通信装置に組み込まれる鍵情報保持装置とを有する秘密情報送受信システムにおける鍵情報保持装置であって

、前記鍵情報保持装置は、公開鍵および秘密鍵と、前記公開鍵の正当性を保障する証明書とを格納する鍵情報保持装置記憶手段と、前記証明書を前記通信装置に送信するよう要求する証明書送信制御手段と、前記通信装置から受信する前記暗号化されたセッション鍵を前記秘密鍵で復号する暗号化セッション鍵復号手段とを備えることを特徴とする鍵情報保持装置である。

【００１３】

また、本発明は、ネットワークに接続し、第１の公開鍵及び第１の秘密鍵と前記第１の公開鍵の正当性を保障する証明書とセッション鍵とが格納された前記サーバー装置と、前記ネットワークに接続し、前記サーバー装置とセッションを確立しデータを送受信する通信装置と、前記通信装置に組み込まれ、第２の公開鍵及び第２の秘密鍵と前記第２の公開鍵の正当性を保障する証明書とが格納された鍵情報保持装置とを有する秘密情報送受信システムにおいて、前記サーバー装置が、前記第１の公開鍵の正当性を保障する証明書を前記通信装置に送信し、前記通信装置が、前記サーバー装置から送信された前記第１の公開鍵の正当性を保障する証明書の正当性を検証し、前記鍵情報保持装置が、前記第２の公開鍵の正当性を保障する証明書を前記通信装置に送信し、前記通信装置が、前記鍵情報保持装置から送信された前記第２の公開鍵の正当性を保障する証明書を前記サーバー装置に送信し、前記サーバー装置が、前記通信装置から送信された前記第２の公開鍵の正当性を保障する証明書が正当か否かを検証し、前記セッション鍵を暗号化し、前記サーバー装置の秘密鍵で前記暗号化されたセッション鍵の正当性を示す情報を作成し、前記暗号化されたセッション鍵と前記暗号化されたセッション鍵の正当性を示す情報とを前記通信装置に送信し、前記通信装置が、前記第１の公開鍵の正当性を保障する証明書から前記第１の公開鍵を取り出し、前記暗号化されたセッション鍵の正当性を示す情報が正当か否かを前記第１の公開鍵で検証し、前記暗号化されたセッション鍵を前記鍵情報保持装置に送信し、前記鍵情報保持装置が、前記通信装置から受信する前記暗号化されたセッション鍵を前記通信装置の秘密鍵で復号することを特徴とする秘密情報送受信方法である。

【発明の効果】

【００１４】

本発明によれば、ネットワーク上にあるサーバーが生成するセッション鍵を安全にセキュリティチップに送信するようにしたので、サーバーとセキュリティチップの間における通信経路全般に渡って、セキュリティを確保することができ、これによりサーバーとセキュリティチップ間で、安全な通信を行うことができる。

【発明を実施するための最良の形態】

【００１５】

本発明の鍵情報保持装置（以下、セキュリティチップという）とは、秘密情報の送信、受信及びその両方を行うデバイスのことであり、ＩＣカードやＳＤカードのような着脱可能な筐体で機器に組み込まれるものや、予め機器の中に組み込まれるものである。なお、セキュリティチップは、耐タンパ性を持っても良い。以下では、本発明を適用した一実施形態である、ＩＣカード４００とインターネットＮ上のサーバー２００（サーバー装置）での安全な通信経路（以下、セキュアチャネルという）の確保方法を説明する。図１はセキュアチャネルの概要図である。ＩＣカード４００は、ＩＣカードリーダライタ３２０と通信を行い、データを送受信する。ＩＣカードリーダライタ３２０は、インターネットＮに接続可能なＰＣ３００（通信装置）に接続されており、ＰＣ３００から受信したデータをＩＣカード４００に送信し、またＩＣカード４００から受信したデータをＰＣ３００に送信する。ＰＣ３００はインターネットＮを介してＩＣカードリーダライタ３２０から受信したデータをサーバー２００へ送信し、またサーバー２００からデータを受信する。サーバー２００はインターネットＮを介してＰＣ３００とデータを送受信することで、サーバー２００はＩＣカード４００のデータを受信する。本実施形態では、図１のように接続されたシステムにおいて、サーバー２００がＩＣカード４００へ、秘密データであるセッション鍵を送信する方法を説明する。

【００１６】

図２は、本実施形態に用いられるＩＣカード４００に搭載されるセキュリティチップの構成の一部を示すブロック図である。１２０は記憶部であり、セキュリティチップ１００とサーバー３００の間でセッションを確立するのに必要となるクライアント公開鍵１２１（第２の公開鍵）とクライアント秘密鍵１２２（第２の秘密鍵）、クライアント証明書１２３（第２の公開鍵の正当性を保障する証明書）を格納する。なお、記憶部１２０は、フラッシュメモリ等の不揮発性メモリ、または不揮発性メモリとＲＡＭ（Random Access Memory）との組み合わせによって構成される。１１０は制御部であり、クライアント証明書１２３をＰＣ３００に送信するよう通信部１３０に指示するクライアント証明書送信制御部１１１（第２の証明書送信制御部）、ＰＣ３００から送信される暗号化されたセッション鍵を復号する暗号化セッション鍵復号部１１２を含む。なお、通信部は、ＰＣ３００に接続されたＩＣカードリーダライタ３２０とデータの送受信を行う。

【００１７】

図３は、本実施形態に用いられるサーバー２００の構成の一部を示すブロック図である。２２０は記憶部であり、セキュリティチップ１００とサーバー３００の間でセッションを確立するのに必要となるサーバー公開鍵２２１（第１の公開鍵）、サーバー秘密鍵２２２（第２の秘密鍵）、サーバー証明書２２３（第１の公開鍵の正当性を保障する証明書）、セッション鍵２２４、セキュリティチップ１００に送信する送信データベース２２５を格納する。２１０は制御部であり、サーバー証明書送信制御部２１１（第１の証明書巣新制御部）、クライアント証明書検証部２１２（第１の証明書検証部）、セッション鍵生成部２１３、セッション鍵暗号化部２１４、セッション鍵正当情報生成部２１５、暗号化セッション鍵送信制御部２１６を含む。

【００１８】

サーバー証明書送信制御部２１１は、ＰＣ３００へサーバー証明書２２１を送信するよう通信部２３０に指示する制御を行う。クライアント証明書検証部２１２は、ＰＣ３００から受信したクライアント証明書の正当性を検証する処理を行う。セッション鍵生成部２１３は、セッション確立後のデータの暗号化、及び復号に用いるセッション鍵を生成し、記憶部２２０に格納する。セッション鍵暗号化部２１３は、記憶部２２０のセッション鍵２２４を、ＰＣ３００から受信するクライアント証明書内のクライアント公開鍵で暗号化する処理を行う。セッション鍵正当情報生成部２１５は、セッション鍵生成部２１３によって生成されたセッション鍵の正当性を示す情報を生成する。暗号化セッション鍵送信制御部２１６は、暗号化されたセッション鍵をクライアントに送信するよう通信部２３０を制御する。なお、通信部２３０は、無線または有線でインターネットに接続している。３４０は、ＣＲＴ（Cathode Ray Tube）や液晶ディスプレイ等で構成される表示部である。

【００１９】

図４は、本実施形態に用いられるクライアントとしてのＰＣ３００の構成の一部を示すブロック図である。３１０は制御部であり、証明書要求部３１１、サーバー証明書検証部３１２（第２の証明書検証部）、クライアント証明書中継送信部３１３（証明書中継送信部）、セッション鍵正当情報検証部３１４、暗号化セッション鍵送信制御部３１５を含む。

【００２０】

証明書要求部３１１は、サーバー２００に対してサーバー証明書２２３の送信要求を、通信部３３０からサーバー２００へ送信させ、また、セキュリティチップに対してクライアント証明書１２３の送信要求を、通信部３３０からサーバー２００へ送信させる。サーバー証明書検証部３１２は、サーバー２００から受信したサーバー証明書２２３の正当性を検証する処理を行う。クライアント証明書中継送信部３１３は、セキュリティチップ１００から受信したクライアント証明書１２３をサーバー２００へ送信するよう通信部に指示する。セッション鍵正当情報検証部３１４は、サーバー２００から送信された暗号化されたセッション鍵の正当性を検証する。暗号化セッション鍵送信制御部３１５は、サーバー２００から送信された暗号化セッション鍵をセキュリティチップ１００へ送信するよう通信部３３０を制御する。なお、通信部３３０は、無線または有線でインターネットに接

続している。３２０はＩＣカードリーダライタである。３５０はキーボード、マウス等で構成される入力部である。

【００２１】

上述したセキュリティチップ１００、サーバー２００、ＰＣ３００の各制御部はメモリ及びＣＰＵ（中央演算装置）により構成され、各制御部の機能を実現するためのプログラム（図示せず）をメモリにロードして実行することによりその機能を実現する。

なお、これらの各制御部は専用のハードウェアにより実現されるものであっても良い。

また、上述したサーバー２００、ＰＣ３００の各記憶部は、ハードディスク装置や光磁気ディスク装置、フラッシュメモリ等の不揮発性メモリ、ＲＡＭのような揮発性メモリ、あるいはこれらの組み合わせにより構成されるものとする。

【００２２】

以下では、サーバー２００からコンテンツを配信する際に、セキュリティチップとインターネットＮ上のサーバー２００との間でセキュアチャネルを確立する動作を、図５のフローチャートを参照して説明する。

【００２３】

まず、ユーザーがＰＣ３００の入力部３３０から、コンテンツ配信を要求するデータを入力する。このデータを証明書要求部３１１が検知すると、サーバー２００とセッション確立のために、サーバー２００に対してサーバー証明書を要求するデータを送信するよう通信部３３０を制御する（ステップＳ１）。これを受けて、サーバー２００のサーバー証明書送信制御部２１１は、記憶部２２０からサーバー証明書２２３を読み出し、ＰＣ３００へ送信するよう通信部２３０を制御する（ステップＳ２）。なお、図５のステップＳ２のように、サーバー２００のサーバー証明書送信制御部２１１は、サーバー証明書の他に、サーバーの署名を生成して更に送信しても良い。

【００２４】

次にＰＣ２００のサーバー証明書検証部３１２が、通信部３３０からサーバー証明書を受信すると、サーバー証明書の正当性を検証する（ステップＳ３）。なお、サーバー証明書の他に、サーバーから署名を受信した場合、その正当性を検証する処理を行う。これらの、証明書・署名の検証方法は、任意の既存の証明書・署名の検証技術を適用することも可能である。

【００２５】

その後、ＰＣ３００の証明書要求部３１１は、セキュリティチップ１００に対してクライアント証明書１２３を要求するデータを送信するよう、ＩＣカードリーダライタ３２０を制御する。この時、ＩＣカードリーダライタ３２０がＩＣカード４００を検出しなかった場合、証明書要求部３１１はユーザーに対して、ＩＣカード４００をＩＣカードリーダライタ３２０に検出させる指示を表示部３６０に表示させる。そしてＩＣカードリーダライタ３２０がＩＣカード４００を検出すると、前述のクライアント証明書の送信要求をセキュリティチップに送信する（ステップＳ４）。これを受けて、セキュリティチップ１００のクライアント証明書送信制御部１１１は、記憶部１２０からクライアント証明書１２３を読み出し、ＰＣ３００へ送信するよう通信部１３０を制御する（ステップＳ５）。その後、ＰＣ３００は、ＩＣカードリーダライタ３２０から受信したクライアント証明書を、サーバー２００へ送信するよう通信部３３０を制御する（ステップＳ６）。

【００２６】

サーバー２００のクライアント証明書検証部２１２は、通信部２３０からクライアント証明書を受信すると、クライアント証明書の正当性を検証する（ステップＳ７）。なお、クライアント証明書の他に、クライアントから署名を受信した場合、その正当性を検証する処理を行う。この検証方法は、任意の既存の証明書・署名の検証技術を適用することも可能である。

【００２７】

上記の検証処理の結果、正当性を確認すると、サーバー２００のセッション鍵生成部２１３は、セッション鍵を生成し、記憶部２２０に格納する。その後、サーバー２００のセ

ッション鍵暗号化部２１４が、ＰＣ３００から受信した前述のクライアント証明書からクライアント公開鍵を読み出し、これを用いて記憶部２２０に格納されたセッション鍵２２４を暗号化する。次に、セッション鍵正当情報生成部２１５が、記憶部２２０のサーバー秘密鍵２２２で署名を生成する（ステップＳ８）。

その後、前述の暗号化したセッション鍵と、生成した署名を、ＰＣ３００へ送信するよう通信部２３０を制御する（ステップＳ９）。

【００２８】

次に、ＰＣ３００のセッション鍵正当情報検証部は、受信した前述のサーバー証明書からサーバーの公開鍵を読み出し、これを用いて、サーバーから受信した署名を検証する（ステップＳ１０）。その後、暗号化セッション鍵送信制御部３１５が、セキュリティチップ１００へ、暗号化したセッション鍵を送信するようＩＣカードリーダライタ３２０を制御する（ステップＳ１１）。

【００２９】

これを受けて、セキュリティチップ１００は、記憶部１２０からクライアント秘密鍵を読み出し、これを用いて暗号化されたセッション鍵を復号し（ステップＳ１２）、記憶部１２０へ格納する。その後、処理が終了し、セッションが確立したことを示すデータをＰＣ３００へ送信するよう、通信部１３０を制御する。これを受けてＰＣ３００はセッションが確立したことを示すデータをサーバー２００へ送信する（ステップＳ１４）。

【００３０】

これにより、セキュリティチップを搭載したＩＣカード４００と、サーバーの間でセキュアチャネルが確保でき、セッション鍵を用いて互いにデータを暗号化・復号することで秘密データを送受信することができる。

【００３１】

なお、上述した実施形態においては、セッション鍵をサーバー２００で生成したが、サーバーの公開鍵をセキュリティチップ１００の記憶部１２０に格納し、上述の実施形態におけるサーバー２００の搭載するセッション鍵生成部２１３、セッション鍵暗号化部２１４、セッション鍵正当情報生成部２１５、暗号化セッション鍵送信制御部２１６と同等の処理能力を持つ機能を制御部２１０に搭載し、更にＰＣ３００がサーバー公開鍵をセキュリティチップ１００へ送信する手段及びセキュリティチップがこれを受信する手段を搭載することで、セッション鍵をセキュリティチップに生成させても良い。その場合の動作を以下に示す。

【００３２】

まず、図５のステップＳ１～Ｓ７の処理を同様に行う。次に、サーバー２００は、クライアント証明書の検証が終了したことをＰＣ３００へ通知する。これを受けて、ＰＣ３００はサーバー証明書からサーバー公開鍵を読み出し、セキュリティチップ１００へ送信する。これを受けてセキュリティチップ１００は、上述の実施形態におけるサーバー２００の搭載するセッション鍵生成部２１３、セッション鍵暗号化部２１４、セッション鍵正当情報生成部２１５、暗号化セッション鍵送信制御部２１６と同様の処理を行い、暗号化セッション鍵と、暗号化セッション鍵の正当性を示す情報を、ＰＣ３００へ送信するよう通信部１３０を制御する。ＰＣ３００は、ＩＣカードリーダライタ３２０から受信したデータを、そのままサーバー２００へ送信するよう通信部３３０を制御する。これにより、セッション鍵がセキュリティチップ１００からサーバー２００へ送信される。

【００３３】

なお、図６に、サーバー２００からセキュリティチップ１００へ、コンテンツ配信に必要な秘密データを送信する具体例を示す。サーバー２００の制御部２１０が、記憶部２２０の送信データベース２２５からライセンスデータを読み出し、上述のセッション鍵で暗号化し、ＰＣ３００へ送信するよう通信部２３０を制御する（ステップＳａ）。ＰＣ３００の制御部３１０は通信部３３０から受信した、暗号化されたライセンスデータをそのままセキュリティチップへ送信するようＩＣカードリーダライタ３２０を制御する。セキュリティチップ１００は通信部１３０から暗号化されたライセンスデータを受信し、上述に

て記憶部１２０へ格納したセッション鍵で復号し（ステップＳｂ）、復号したライセンスデータを、記憶部１２０の不揮発性メモリで構成される領域に格納する（ステップＳｃ）。その後、セキュリティチップの制御部１１０は、ライセンスデータの書き込み処理が終了したことを通知するデータを、ＰＣ３００に送信するよう通信部１３０を制御する。ＰＣ３００は、ＩＣカードリーダライタ３２０から受信した、セキュリティチップからの通知データを、そのままサーバー２００へ送信するよう通信部２３０を制御する。

【００３４】

なお、上述の実施形態において、サーバー２００が保持するサーバー証明書２２３と、セキュリティチップ１００が保持するクライアント証明書１２３を送受信し、証明書の検証処理を行ったが、これらの証明書を送受信する代わりに、セキュリティチップ１００が保持するクライアント公開鍵１２１をセキュリティチップ１００へ送信し、次に、サーバー２００がセッション鍵を生成し、受信したクライアント公開鍵で暗号化してセキュリティチップ１００に送信し、セキュリティチップ１００がこれを受信して前述のサーバー公開鍵で復号することで、セッション確立としても良い。

【００３５】

なお、上述の実施形態において、セッション鍵は、セッションの確立ごとにサーバー２００またはセキュリティチップ１００によって生成されるとしたが、予め１つまたは複数のセッション鍵を、サーバー２００の記憶部２２０またはセキュリティチップ１００の記憶部１２０に格納し、使用しても良い。

【００３６】

このように、セキュリティチップ１００がサーバー２００にクライアント公開鍵を送信し、サーバー２００がセッション鍵を生成し、受信したクライアント公開鍵で暗号化してセキュリティチップ１００に送信し、これをセキュリティチップ１００はクライアント秘密鍵で復号してセッション鍵を読み出すので、サーバー２００及びセキュリティチップ１００は、互いに、秘密データをセッション鍵で暗号化して送信すること、またその逆に、送信された前述の暗号化秘密データを復号することができるようになり、安全な通信経路を確保することが可能となる。また、サーバー２００がセキュリティチップ１００にサーバー公開鍵を送信し、セキュリティチップ１００がセッション鍵を生成し、受信したサーバー公開鍵で暗号化してサーバー２００に送信し、これをサーバー２００はサーバー秘密鍵で復号してセッション鍵を読み出す場合も同様に、サーバー２００及びセキュリティチップ１００は、互いに、秘密データをセッション鍵で暗号化して送信すること、またその逆に、送信された前述の暗号化秘密データを復号することができるようになり、安全な通信経路を確保することが可能となる。

【００３７】

また、サーバー証明書を利用して、セキュリティチップ１００を認証し、また、クライアント証明書を利用して、サーバー２００を認証するようにしたので、サーバー２００とセキュリティチップ１００の間に他の機器が介在するシステムであっても、その機器等においてデータの改竄を防止することができ、これにより、サーバー２００からセキュリティチップ１００に渡って連続した、安全な通信経路を確保することができる。

【００３８】

以上、この発明の一実施形態を、図面を参照して詳述してきたが、具体的な構成はこの実施形態に限られるものではなく、この発明の要旨を逸脱しない範囲の設計等も含まれる。

【図面の簡単な説明】

【００３９】

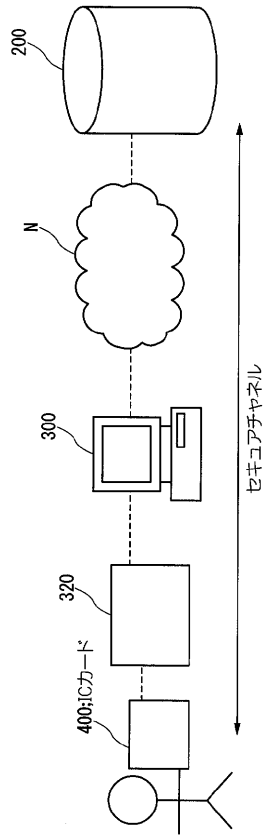
【図１】本発明の一の実施形態による、セキュアチャネルの概要図である。

【図２】同実施形態に用いられる、ＩＣカードに搭載されるセキュリティチップの構成の一部を示すブロック図である。

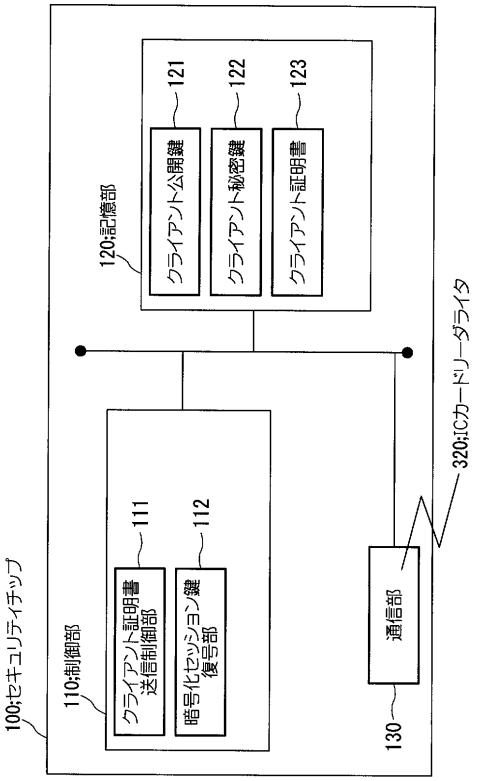
【図３】同実施形態に用いられる、インターネット上のサーバーの構成の一部を示すブロック図である。

【図４】同実施形態に用いられる、ＰＣの構成の一部を示すブロック図である。
【図５】同実施形態による、セキュリティチップとインターネット上のサーバーとの間でセキュアチャネルを確立する動作を示すフローチャートである。
【図６】同実施形態による、サーバーからセキュリティチップへ、コンテンツ配信に必要な秘密データを送信するフローチャートである。
【図７】従来の、ＳＳＬ技術を利用した、インターネット上のサーバーとＰＣ間で秘密データを送受信する際に用いられるシステムの概要図である。
【符号の説明】
【００４０】
１００…セキュリティチップ
１１０…制御部
１１１…クライアント証明書送信制御部
１１２…暗号化セッション鍵復号部
１２０…記憶部
１２１…クライアント公開鍵
１２２…クライアント秘密鍵
１２３…クライアント証明書
１３０…通信部
２００…サーバー
２１０…制御部
２１１…サーバー証明書送信制御部
２１２…クライアント証明書検証部
２１３…セッション鍵生成部
２１４…セッション鍵暗号化部
２１５…セッション鍵正当情報生成部
２１６…暗号化セッション鍵送信制御部
２２０…記憶部
２２１…サーバー公開鍵
２２２…サーバー秘密鍵
２２３…サーバー証明書
２２４…セッション鍵
２２５…送信データベース
２３０…通信部
３００…ＰＣ
３１０…制御部
３１１…証明書要求部
３１２…サーバー証明書検証部
３１３…クライアント証明書中継送信部
３１４…セッション鍵正当情報検証部
３１５…暗号化セッション鍵送信制御部
３２０…ＩＣカードリーダライタ
３３０…通信部
３４０…表示部
３５０…入力部
４００…ＩＣカード
Ｎ…インターネット網

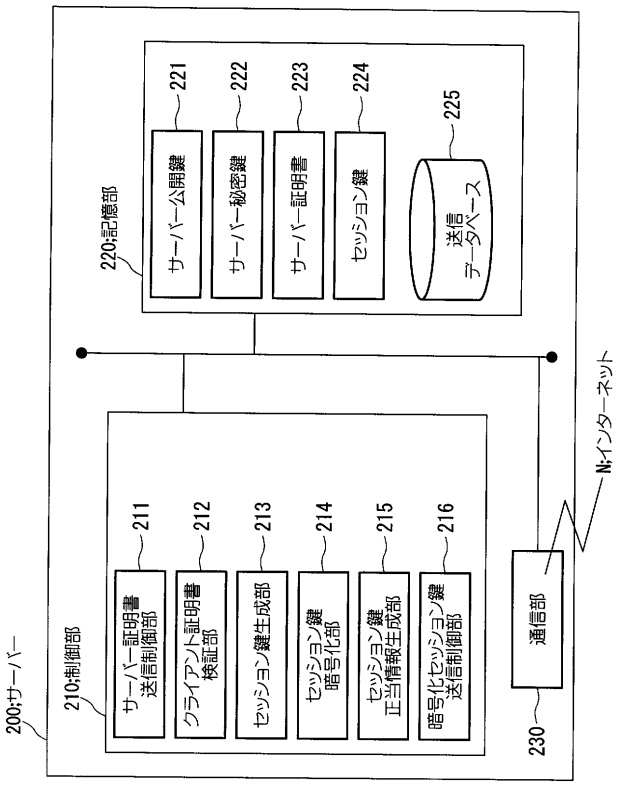
【図１】


200
N
300
320
400;ICカード
セキュアチャネル

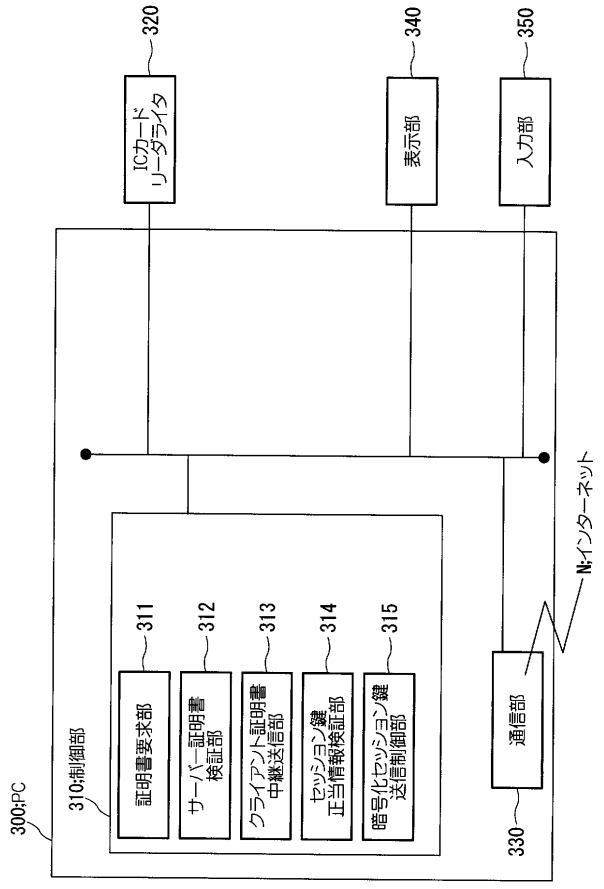
【図２】


100;セキュリティチップ
110;制御部
クライアント証明書送信制御部
111
暗号化セッション鍵復号部
112
120;記憶部
クライアント公開鍵
121
クライアント秘密鍵
122
クライアント証明書
123
通信部
130
320;ICカードリーダライタ

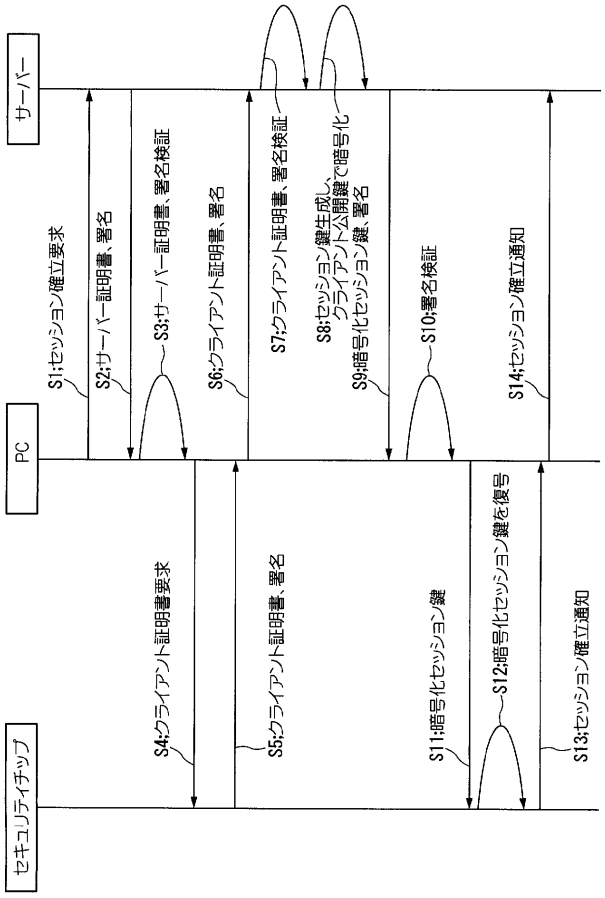
【図３】


200;サーバー
210;制御部
サーバー証明書送信制御部
211
クライアント証明書検証部
212
セッション鍵生成部
213
セッション鍵暗号化部
214
セッション鍵正当情報生成部
215
暗号化セッション鍵送信制御部
216
220;記憶部
サーバー公開鍵
221
サーバー秘密鍵
222
サーバー証明書
223
セッション鍵
224
送信データベース
225
通信部
230
N;インターネット

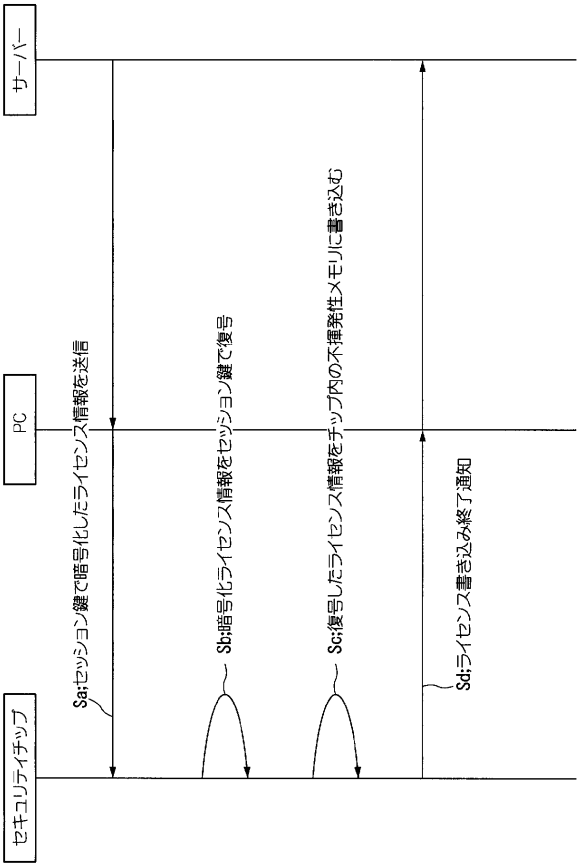
【図４】


300;PC
310;制御部
証明書要求部
311
サーバー証明書検証部
312
クライアント証明書中継送信部
313
セッション鍵正当情報検証部
314
暗号化セッション鍵送信制御部
315
ICカードリーダライタ
320
表示部
340
入力部
350
通信部
330
N;インターネット

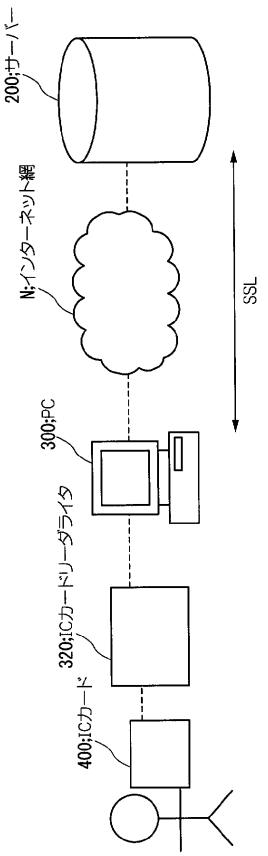
【図５】


サーバー
PC
セキュリティチップ
S1;セッション確立要求
S2;サーバー証明書、署名
S3;サーバー証明書、署名検証
S4;クライアント証明書要求
S5;クライアント証明書、署名
S6;クライアント証明書、署名
S7;クライアント証明書、署名検証
S8;セッション鍵生成、
クライアント公開鍵で暗号化
S9;暗号化セッション鍵、署名
S10;署名検証
S11;暗号化セッション鍵
S12;暗号化セッション鍵を復号
S13;セッション確立通知
S14;セッション確立通知

【図６】


サーバー
PC
セキュリティチップ
Sa;セッション鍵で暗号化したライセンス情報を送信
Sb;暗号化ライセンス情報をセッション鍵で復号
Sc;復号したライセンス情報をチップ内の不揮発性メモリに書き込む
Sd;ライセンス書き込み終了通知

【図７】


200;サーバー
N;インターネット網
SSL
300;PC
320;ICカードリーダライタ
400;ICカード

フロントページの続き

(72)発明者　三露　学
東京都台東区台東１丁目５番１号　凸版印刷株式会社内
(72)発明者　増永　優作
東京都台東区台東１丁目５番１号　凸版印刷株式会社内
(72)発明者　本谷　佳代
東京都台東区台東１丁目５番１号　凸版印刷株式会社内
(72)発明者　林　奈津子
東京都台東区台東１丁目５番１号　凸版印刷株式会社内

Ｆターム(参考) 5J104 AA09　AA16　EA04　EA05　EA15　EA16　EA17　EA19　JA03　JA21
LA03　LA06　NA02　NA37