(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2005-20580
(P2005-20580A)
(43)公開日　平成17年1月20日(2005.1.20)

(51)Int.Cl.[7]	F I		テーマコード（参考）
H04L 9/08	H04L 9/00	601B	5B017
G06F 12/14	G06F 12/14	310K	5J104
	G06F 12/14	320B	
	H04L 9/00	601F	

審査請求 未請求　請求項の数 11　OL　（全 17 頁）

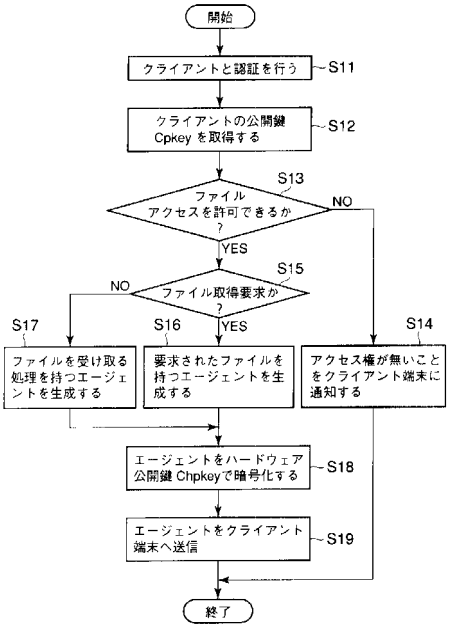
(21)出願番号　特願2003-185142(P2003-185142)
(22)出願日　平成15年6月27日(2003.6.27)

(71)出願人　000003562
東芝テック株式会社
東京都千代田区神田錦町１丁目１番地
(74)代理人　100058479
弁理士　鈴江　武彦
(74)代理人　100091351
弁理士　河野　哲
(74)代理人　100088683
弁理士　中村　誠
(74)代理人　100108855
弁理士　蔵田　昌俊
(74)代理人　100084618
弁理士　村松　貞男
(74)代理人　100092196
弁理士　橋本　良郎

最終頁に続く

(54)【発明の名称】ネットワークシステム

(57)【要約】
【課題】正規のクライアント端末からのみファイル管理サーバへのアクセスを可能とし、これにより、セキュリティの向上を図る。
【解決手段】ファイル管理サーバは、先ず、クライアントとの間の認証を行い、認証が確認されその後クライアント端末からファイル取得要求を受信すると、アクセスを許可できるか否かを判断し、許可できる場合は許可通知を行う。そして、クライアント端末からサーバ公開鍵で暗号化されたハードウェア公開鍵を受信するとこれを復号化する。また、要求されたファイルを持ったエージェントを生成する。そして、生成されたエージェントをクライアント端末から受信したハードウェア公開鍵で暗号化し、該当するクライアント端末に送信する。クライアント端末は、エージェントを受信すると、このエージェントをハードウェア秘密鍵で復号化しファイルを取り出す。
【選択図】　図６



【特許請求の範囲】
【請求項１】
クライアント端末とファイル管理サーバを接続したネットワークシステムにおいて、
前記クライアント端末は、少なくともハードウェア公開鍵とハードウェア秘密鍵等のユニークな鍵を保管した端末情報格納部と、前記ファイル管理サーバにファイル取得要求を送信する要求送信手段と、前記ファイル管理サーバからアクセス許可を受けると前記端末情報格納部のハードウェア公開鍵を前記ファイル管理サーバへ送信するハードウェア公開鍵送信手段と、前記ファイル管理サーバからファイル通信に関する処理を行うエージェントを受信するとこのエージェントを前記端末情報格納部のハードウェア秘密鍵で復号化してファイルを受け取るファイル受取手段とを備え、
前記ファイル管理サーバは、前記クライアント端末からファイル取得要求を受信するとそのクライアント端末に対してアクセス許可を送信し、続いて前記クライアント端末からハードウェア公開鍵を取得すると前記エージェントを生成するエージェント生成手段と、この生成されたエージェントに要求されたファイルを持たせ、このエージェントを受信したハードウェア公開鍵で暗号化し、該当するクライアント端末に送信するエージェント送信手段とを備えたことを特徴とするネットワークシステム。
【請求項２】
クライアント端末とファイル管理サーバを接続したネットワークシステムにおいて、
さらに、クライアントの証明書及び公開鍵を管理する認証サーバを接続し、
前記認証サーバは、前記ファイル管理サーバからクライアントの証明書を受信すると、その証明書が管理しているクライアントの証明書と一致しているか否かを確認し、一致していれば該当するクライアントの公開鍵を前記ファイル管理サーバに送信する手段を備え、
前記クライアント端末は、少なくともハードウェア公開鍵とハードウェア秘密鍵等のユニークな鍵を保管した端末情報格納部と、クライアントの証明書を前記ファイル管理サーバに送信するクライアント証明書送信手段と、前記ファイル管理サーバからサーバの公開鍵を取得するサーバ公開鍵取得手段と、前記ファイル管理サーバにファイル取得要求を送信する要求送信手段と、前記ファイル管理サーバからアクセス許可を受けると前記端末情報格納部のハードウェア公開鍵を、取得したサーバの公開鍵で暗号化して前記ファイル管理サーバへ送信するハードウェア公開鍵送信手段と、前記ファイル管理サーバからファイル通信に関する処理を行うエージェントを受信するとこのエージェントを前記端末情報格納部のハードウェア秘密鍵で復号化してファイルを受け取るファイル受取手段とを備え、
前記ファイル管理サーバは、前記クライアント端末からクライアントの証明書を受信すると、その証明書を確認のために前記認証サーバに送信するクライアント証明書送信手段と、前記認証サーバからクライアントの公開鍵を取得すると、該当するクライアント端末にサーバの公開鍵を送信するサーバ公開鍵送信手段と、前記クライアント端末からファイル取得要求を受信するとそのクライアント端末に対してアクセス許可を送信し、続いて前記クライアント端末から暗号化されたハードウェア公開鍵を受信しそれをサーバの秘密鍵で復号化して取得すると前記エージェントを生成するエージェント生成手段と、この生成されたエージェントに要求されたファイルを持たせ、このエージェントを受信したハードウェア公開鍵で暗号化し、該当するクライアント端末に送信するエージェント送信手段とを備えたことを特徴とするネットワークシステム。
【請求項３】
クライアント端末とファイル管理サーバを接続したネットワークシステムにおいて、
前記クライアント端末は、少なくともハードウェア公開鍵とハードウェア秘密鍵等のユニークな鍵を保管した端末情報格納部と、前記ファイル管理サーバにファイル取得要求を送信する要求送信手段と、前記ファイル管理サーバからアクセス許可を受けると前記端末情報格納部のハードウェア公開鍵を前記ファイル管理サーバへ送信するハードウェア公開鍵送信手段と、前記ファイル管理サーバからファイル通信に関する処理を行うエージェントを受信するとこのエージェントを前記端末情報格納部のハードウェア秘密鍵で復号化する復号化手段と、この復号化したエージェントから乱数を取り出し、この乱数と自己のハー

ドウェア公開鍵とから共通鍵暗号方式により共通鍵を生成する共通鍵生成手段と、復号化したエージェントからファイルを、前記共通鍵生成手段が生成する共通鍵で復号化して受け取るファイル受取手段とを備え、
前記ファイル管理サーバは、乱数を保持したエージェントを格納したエージェント格納部と、前記クライアント端末からファイル取得要求を受信するとそのクライアント端末に対してアクセス許可を送信し、続いて前記クライアント端末から暗号化されたハードウェア公開鍵を受信しそれをサーバの秘密鍵で復号化して取得すると前記エージェント格納部から該当するエージェントを取り出すエージェント取出手段と、この取り出したエージェントに取得要求のあった共通鍵を使用して暗号化されたファイルを持たせ、このエージェントを受信したハードウェア公開鍵で暗号化し、該当するクライアント端末に送信するエージェント送信手段とを備えたことを特徴とするネットワークシステム。

【請求項４】
クライアント端末とファイル管理サーバを接続したネットワークシステムにおいて、
前記クライアント端末は、少なくともハードウェア公開鍵とハードウェア秘密鍵等のユニークな鍵を保管した端末情報格納部と、前記ファイル管理サーバにファイル保管要求を送信する要求送信手段と、前記ファイル管理サーバからアクセス許可を受けると前記端末情報格納部のハードウェア公開鍵を前記ファイル管理サーバへ送信するハードウェア公開鍵送信手段と、前記ファイル管理サーバからファイル通信に関する処理を行うエージェントを受信するとこのエージェントを前記端末情報格納部のハードウェア秘密鍵で復号化する復号化手段と、この復号化したエージェントに保管すべきファイルを格納するファイル格納手段と、このファイルを格納したエージェントを前記ファイル管理サーバから取得したサーバの公開鍵で暗号化してそのファイル管理サーバへ送信するエージェント送信手段とを備え、
前記ファイル管理サーバは、前記クライアント端末からファイル保管要求を受信するとそのクライアント端末に対してアクセス許可を送信し、続いて前記クライアント端末から暗号化されたハードウェア公開鍵を取得すると前記エージェントを生成するエージェント生成手段と、この生成されたエージェントを受信したハードウェア公開鍵で暗号化し、該当するクライアント端末に送信するエージェント送信手段と、前記クライアント端末からエージェントを受信すると、そのエージェントをサーバの秘密鍵で復号化し、このエージェントからファイルを受取って保管するファイル保管手段とを備えたことを特徴とするネットワークシステム。

【請求項５】
クライアント端末とファイル管理サーバを接続したネットワークシステムにおいて、
さらに、クライアントの証明書及び公開鍵を管理する認証サーバを接続し、
前記認証サーバは、前記ファイル管理サーバからクライアントの証明書を受信すると、その証明書が管理しているクライアントの証明書と一致しているか否かを確認し、一致していれば該当するクライアントの公開鍵を前記ファイル管理サーバに送信する手段を設け、
前記クライアント端末は、少なくともハードウェア公開鍵とハードウェア秘密鍵等のユニークな鍵を保管した端末情報格納部と、クライアントの証明書を前記ファイル管理サーバに送信するクライアント証明書送信手段と、前記ファイル管理サーバからサーバの公開鍵を取得するサーバ公開鍵取得手段と、前記ファイル管理サーバにファイル保管要求を送信する要求送信手段と、前記ファイル管理サーバからアクセス許可を受けると前記端末情報格納部のハードウェア公開鍵を、取得したサーバの公開鍵で暗号化して前記ファイル管理サーバへ送信するハードウェア公開鍵送信手段と、前記ファイル管理サーバからファイル通信に関する処理を行うエージェントを受信するとこのエージェントを前記端末情報格納部のハードウェア秘密鍵で復号化する復号化手段と、この復号化したエージェントに保管すべきファイルを格納するファイル格納手段と、このファイルを格納したエージェントを前記ファイル管理サーバから取得したサーバの公開鍵で暗号化してそのファイル管理サーバへ送信するエージェント送信手段とを備え、
前記ファイル管理サーバは、前記クライアント端末からクライアントの証明書を受信する

と、その証明書を確認のために前記認証サーバに送信するクライアント証明書送信手段と、前記認証サーバからクライアントの公開鍵を取得すると、該当するクライアント端末にサーバの公開鍵を送信するサーバ公開鍵送信手段と、前記クライアント端末からファイル保管要求を受信するとそのクライアント端末に対してアクセス許可を送信し、続いて前記クライアント端末から暗号化されたハードウェア公開鍵を受信しそれをサーバの秘密鍵で復号化して取得すると前記エージェントを生成するエージェント生成手段と、この生成されたエージェントを受信したハードウェア公開鍵で暗号化し、該当するクライアント端末に送信するエージェント送信手段と、前記クライアント端末からエージェントを受信すると、そのエージェントをサーバの秘密鍵で復号化し、この復号化したエージェントからファイルを受取って保管するファイル保管手段とを備えたことを特徴とするネットワークシステム。

【請求項６】

クライアント端末のファイル格納手段は、エージェントに格納するファイルを自己のハードウェア公開鍵で暗号化することを特徴とする請求項５記載のネットワークシステム。

【請求項７】

クライアント端末は、さらに、乱数を発生する乱数発生手段と、この乱数発生手段から発生する乱数と自己のハードウェア公開鍵とから共通鍵暗号方式により共通鍵を生成する共通鍵生成手段とを設け、ファイル格納手段は、前記共通鍵生成手段が生成する共通鍵を用いてエージェントに格納するファイルを暗号化するとともに使用した乱数を前記エージェントに格納し、

ファイル管理サーバは、さらに、ファイルを取り出した後の乱数を保持したエージェントを保管するエージェント保管手段を備えたことを特徴とする請求項５記載のネットワークシステム。

【請求項８】

共通鍵生成手段が生成する共通鍵をファイル毎に動的に変更することを特徴とする請求項７記載のネットワークシステム。

【請求項９】

さらに、クライアントの証明書及びファイル管理サーバの証明書を管理する認証サーバを接続してネットワークシステムを形成し、

前記認証サーバは、前記ファイル管理サーバからクライアントの証明書を受信すると、その証明書が管理しているクライアントの証明書と一致しているか否かを確認して前記ファイル管理サーバに通知し、前記クライアント端末からファイル管理サーバの証明書を受信すると、その証明書が管理しているファイル管理サーバの証明書と一致しているか否かを確認して前記クライアント端末に通知する手段を設け、

前記クライアント端末は、さらに、前記ファイル管理サーバからそのサーバの証明書を取得すると、その証明書を確認のために前記認証サーバに送信するサーバ証明書送信手段を設け、要求送信手段は、前記認証サーバからファイル管理サーバの証明書の一致が通知されると、前記ファイル管理サーバにファイル取得やファイル保管の通信要求を送信し、

前記ファイル管理サーバは、前記クライアント端末からクライアントの証明書を受信すると、その証明書を確認のために前記認証サーバに送信するクライアント証明書送信手段と、前記認証サーバからクライアントの証明書の一致が通知されると、該当するクライアント端末に対してアクセス許可を送信する許可送信手段とを備えたことを特徴とする請求項１又は４記載のネットワークシステム。

【請求項１０】

ファイル管理サーバは、ファイル通信のアクセスを許可するクライアント端末のハードウェア公開鍵を予め登録する登録手段と、前記クライアント端末から取得したハードウェア公開鍵が予め登録したクライアント端末のハードウェア公開鍵と一致しているか否かを判断する判断手段とを備え、エージェント生成手段は、前記判断手段が一致を判断するとエージェントを生成することを特徴とする請求項２又は５記載のネットワークシステム。

【請求項１１】

クライアント端末は、端末情報格納部のハードウェア公開鍵のハッシュ値を求め、このハッシュ値を前記ファイル管理サーバに予め送信するハッシュ値送信手段を設け、
前記ファイル管理サーバは、前記クライアント端末から受信したハッシュ値を予め登録する登録手段と、前記クライアント端末からハードウェア公開鍵を取得するとそのハードウェア公開鍵のハッシュ値を求め、そのハッシュ値が予め登録したクライアント端末のハードウェア公開鍵のハッシュ値と一致しているか否かを判断する判断手段とを備え、エージェント生成手段は、前記判断手段が一致を判断するとエージェントを生成することを特徴とする請求項２又は５記載のネットワークシステム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、クライアント端末とファイル管理サーバを接続したネットワークシステムに関する。

【０００２】

【従来の技術】

この種のネットワークシステムでは、ファイル管理サーバのファイルにクライアントユーザが端末を使用してアクセスする場合は、クライアントユーザの認証を行ってからファイルをそのクライアントユーザに送信するものが知られている。また、逆にクライアントユーザが端末からファイルをファイル管理サーバに送信する場合も同様である。

【０００３】

通常の認証は、ファイル管理サーバがクライアントユーザを正しいと判断するために行う認証で、そのクライアントユーザに対してアクセス権のあるファイルに対してアクセスを許可するものである。また、認証サーバを使用し、ファイル管理サーバとクライアントユーザの電子証明書を用いて認証を行い、暗号化通信を行いファイルのやり取りを行う方法も知られている。例えば、ＳＳＬ（ｓｅｃｕｒｅ　ｓｏｃｋｅｔｓ　ｌａｙｅｒ）のようなセキュアプロトコルＨＴＴＰＳを用いたものである。

【０００４】

また、セキュアな暗号化通信の例として、ファイル管理サーバの公開鍵と秘密鍵を用いたものが知られている。すなわち、クライアントユーザとサーバのファイル通信において、サーバがファイルを配信するエージェントを生成し、このエージェントを使用してクライアントユーザにファイルを送信するようになっている。この従来例ではサーバが公開鍵と秘密鍵を保有しており、サーバが各クライアントにサーバの公開鍵を送り、この公開鍵を受け取った各クライアントはサーバと暗号化通信を行うためのそれぞれクライアント独自の共通鍵をサーバに送るようになっている。この共通鍵はサーバがファイルを送信するために用いるエージェントを暗号化するために用いる。そして、サーバはクライアントにファイルを送るためにエージェントを生成し、この生成したエージェントにファイルを添付し、クライアントから受け取った共通鍵でエージェントを暗号化して電子メールでクライアントに送るようになっている。エージェントを受け取ったクライアントは共通鍵でそのエージェントを復号化し、要求したファイルを受け取るというものである（例えば、特許文献１参照）。

【０００５】

【特許文献１】

特開２００２－３０５５１３号公報

【０００６】

【発明が解決しようとする課題】

しかしながら、このように、クライアントユーザとファイル管理サーバの認証のみを行うものでは、クライアント端末の認証は行われないので、例えば、ＩＤとパスワードだけでクライアントユーザの認証を行うと、ＩＤとパスワードを何らかの方法で知った第三者が、クライアントユーザが所持している端末と全く別の端末を使用してファイル管理サーバにアクセスすることが可能であった。従って、成り済ましをして不正にファイル管理サー

バのファイルにアクセスすることが可能であった。
【０００７】
そこで、本発明は、正規のクライアント端末からのみファイル管理サーバへのアクセスを可能とし、これにより、第三者による別の端末からの成り済ましによるファイル管理サーバへのアクセスを防止でき、セキュリティの向上できるネットワークシステムを提供する。
【０００８】
【課題を解決するための手段】
本発明は、クライアント端末とファイル管理サーバを接続したネットワークシステムにおいて、クライアント端末は、少なくともハードウェア公開鍵とハードウェア秘密鍵等のユニークな鍵を保管した端末情報格納部と、ファイル管理サーバにファイル取得要求を送信する要求送信手段と、ファイル管理サーバからアクセス許可を受けると端末情報格納部のハードウェア公開鍵をファイル管理サーバへ送信するハードウェア公開鍵送信手段と、ファイル管理サーバからファイル通信に関する処理を行うエージェントを受信するとこのエージェントを端末情報格納部のハードウェア秘密鍵で復号化してファイルを受け取るファイル受取手段とを備え、ファイル管理サーバは、クライアント端末からファイル取得要求を受信するとそのクライアント端末に対してアクセス許可を送信し、続いてクライアント端末からハードウェア公開鍵を取得するとエージェントを生成するエージェント生成手段と、この生成されたエージェントに要求されたファイルを持たせ、このエージェントを受信したハードウェア公開鍵で暗号化し、該当するクライアント端末に送信するエージェント送信手段とを備えたことにある。
【０００９】
【発明の実施の形態】
以下、本発明の実施の形態を、図面を参照して説明する。
（第１の実施の形態）
図１に示すように、例えばインターネットからなるネットワーク１にファイル管理サーバ２、認証サーバ３及び複数のクライアント端末４を接続してネットワークシステムを形成している。
【００１０】
このネットワークシステムは、ファイル管理サーバ２がクライアント端末４からの要求によって所定のファイルを保管する処理やクライアント端末４からの要求によってファイル管理サーバ２からクライアント端末４に所定のファイルを配信する処理を行うようになっている。そして、ファイル管理サーバ２とクライアント端末４との間でのファイルの送受信を行うためにファイル通信に関する処理を行うエージェントを生成し、そのエージェントに要求されたファイルを持たせ、暗号化して送受信するものである。
【００１１】
前記認証サーバ３は、クライアントユーザの証明書とクライアントユーザの公開鍵及びサーバの証明書とサーバの公開鍵を管理するようになっている。そして、前記認証サーバ３は、ファイル管理サーバ２がクライアント端末４からクライアントユーザの証明書を受け取り、それを送ってきたときに、そのクライアントユーザの証明書が正しいかを管理しているクライアントユーザの証明書との一致の有無によって判断し、一致した場合にクライアントユーザの証明書が正しいことを確認しファイル管理サーバ２にそのクライアントユーザに該当する公開鍵を配布する手段を備えている。
【００１２】
また、前記認証サーバ３は、クライアント端末４がファイル管理サーバ２からサーバの証明書を受け取り、それを送ってきたときに、そのサーバの証明書が正しいかを管理しているサーバの証明書との一致の有無によって判断し、一致した場合にサーバの証明書が正しいことを確認し該当するクライアント端末４にそれを通知する手段を備えている。
前記認証サーバ３は、ＣＰＵ、ＲＯＭ、ＲＡＭ、ハードディスク、通信インターフェース等で構成されている。

【００１３】
前記ファイル管理サーバ２は、図２に示すように、全体を制御する制御部本体２１、クライアントユーザとの認証に利用するサーバ自身の公開鍵と秘密鍵とサーバの証明書を保管したサーバ情報格納部２２、認証を行ったクライアントユーザのクライアント証明書を格納するクライアント証明書格納部２３、クライアント端末４のファイルに関する要求に対してファイル通信を行う場合にエージェントを暗号化するのに用いる前記クライアント端末４から取得したハードウェア公開鍵や前記認証サーバ３から受け取ったクライアントの公開鍵を格納するクライアント公開鍵格納部２４を備えている。
【００１４】
また、前記ファイル管理サーバ２は、図２に示すように、暗号化したファイルを格納するファイル管理データベース２５、このファイル管理データベース２５で管理しているクライアント端末４のファイルを暗号化するファイル暗号化手段２６、このファイル暗号化手段２６が暗号化に用いる鍵を格納した暗号鍵格納部２７、クライアント端末４とファイル通信を行うためにエージェントを生成するエージェント生成手段２８、クライアント端末３とファイル通信をするエージェントを管理するか否かを判断することや管理のための処理を行うエージェント管理手段２９、管理するエージェントを保管するエージェント格納部３０、クライアント端末４のハードウェア公開鍵でエージェントを暗号化するエージェント暗号化手段３１、自己（サーバ）の秘密鍵でエージェントを復号化するエージェント復号化手段３２を備えている。
前記ファイル管理サーバ２は、ＣＰＵ、ＲＯＭ、ＲＡＭ、ハードディスク、通信インターフェース等で構成されている。
【００１５】
前記クライアント端末４は、図３に示すように、全体を制御する制御部本体４１、前記ファイル管理サーバ２との認証に使用するクライアントユーザの公開鍵及び秘密鍵とクライアント証明書を保管するクライアント情報格納部４２、前記ファイル管理サーバ２とのファイル通信を行うためのエージェントの暗号化及び復号化に使用するハードウェア公開鍵とハードウェア秘密鍵を格納した端末情報格納部４３、ハードウェア公開鍵から独自の共通鍵を生成するための動的鍵生成手段４４、動的な共通鍵を生成するための情報として乱数を発生する乱数発生手段４５を備えている。前記端末情報格納部４３は、アクセスが非常に困難なＥＥＰＲＯＭやＩＣチップによって構成されている。
【００１６】
また、前記クライアント端末４は、例えば、パーソナルコンピュータからなり、図３に示すように、前記ファイル管理サーバ２とファイルの通信を行うためにエージェントを暗号化するエージェント暗号化手段４６、前記ファイル管理サーバ２とファイルの通信を行うためにエージェントを復号化するエージェント復号化手段４７、前記ファイル管理サーバ２から取得したサーバの公開鍵及びサーバの証明書を格納するサーバ情報格納部４８、前記ファイル管理サーバ２から送られる暗号化されたサーバの公開鍵及びサーバの証明書を復号化して前記サーバ情報格納部４８に格納する認証復号化手段４９を備えている。
【００１７】
前記ファイル管理サーバ２のエージェント生成手段２８によって生成されるエージェントは、図４に示すように、クライアント宛先情報５１と、ファイルの配布や受け取り処理などのファイルに関する処理情報５２、エージェントが持っているファイルを復号化するために利用する乱数を格納する乱数情報格納部５３、ファイルを格納するファイル格納部５４によって構成されている。
【００１８】
前記ファイル管理サーバ２は、クライアント端末４のファイルを保管したり、管理しているファイルを正規のクライアント端末４に配信したり、ソフトウェアカスタマイズやオートアップデートなどに用いるファイルを格納したり、それらをクライアント端末４に配信する目的を担う。
【００１９】

前記ファイル管理サーバ２の制御部本体２１は、クライアント端末４におけるクライアントユーザとのユーザ認証を行うときに、クライアントユーザの証明書が正規のものであるか前記認証サーバ３に問い合わせ、正しいことが判明した場合、その認証サーバ３からクライアント公開鍵を受け取り、そのクライアント公開鍵をクライアント公開鍵格納部２４に格納し、また、クライアントユーザの証明書をクライアント証明書格納部２３に格納する処理を行う。また、クライアントユーザが正しいと判明し、クライアント端末４側に自己のサーバ証明書をサーバ情報格納部２２から取り出し、そのサーバ証明書をクライアント端末４に送信する処理を行う。

【００２０】

前記ファイル管理サーバ２は、ファイル暗号化手段２６により内部で独自に生成されたファイルを暗号化する処理やクライアント端末４から受け取ったファイルを暗号化する処理を行う。暗号化するために用いる暗号鍵は暗号鍵格納部２７に格納されており、この格納部２７から読み出して使用する。

【００２１】

前記ファイル管理サーバ２は、認証したクライアントユーザから内部に保管されているファイルの取得要求やファイルを保管したい保管要求があった場合には、要求されたファイルがそのクライアントユーザに許可できるか、また、そのクライアントユーザが指定したファイルの保管が可能かどうかを判断し、可能ならば、クライアント端末４からそのクライアント端末４のハードウェア公開鍵を受け取る処理を行う。

【００２２】

なお、予めクライアント端末４のハードウェア公開鍵を登録しておき、そのハードウェア公開鍵と一致するかを確かめて端末認証を行い、許可することを要求することも可能である。

【００２３】

要求を許可したクライアント端末４にファイルを渡すための処理を持つエージェントをエージェント生成手段２８により生成する。もし、要求がファイルの取得要求ならば、指定したファイルをファイル管理データベース２５から取り出し、もし、このファイルが暗号化されていれば、エージェント復号化手段３２で復号化を行い、エージェントにそのファイルを格納し（ファイル格納手段）、そのエージェントを該当するクライアント端末４のハードウェア公開鍵で暗号化してそのクライアント端末４に送る。また、もし、要求がファイル管理サーバ２にファイルを保管したい保管要求ならば、ファイルをファイル管理データベース２５に格納し、必要に応じてクライアント端末４の情報を持っているエージェントをエージェント管理手段２９によりエージェント格納部３０に格納する。

【００２４】

前記クライアント端末４は、ファイル管理サーバ２との認証を行うときに、クライアント情報格納部４２からクライアント証明書を取り出し、そのクライアント証明書をファイル管理サーバ２に送信する。

【００２５】

また、クライアントユーザがファイル管理サーバ２と認証を行った場合において、その認証が確認されると、ファイル管理サーバ２からそのサーバ２の証明書とサーバ公開鍵がクライアントの公開鍵で暗号化されてクライアント端末４に送られることになる。前記クライアント端末４は、これを受け取ると認証復号化手段４９によって復号化してサーバ証明書とサーバ公開鍵を受け取り、そのサーバ証明書を前記認証サーバ３に送信して確認を行う。そして、サーバ証明書が確認されると、サーバ証明書とサーバ公開鍵をサーバ情報格納部４８に格納する。

【００２６】

クライアントユーザはファイル管理サーバ２に保管されているファイルを取得したい場合は、クライアント端末４を操作する。クライアント端末４は、先ず、端末情報格納部４３に格納されている端末４のハードウェア公開鍵を取り出し、ファイルの取得要求とそのハードウェア公開鍵をファイル管理サーバ２に送る。また、クライアント端末４は、ファイ

ル管理サーバ２からエージェントを受け取ると、そのエージェントをエージェント復号化手段４７で復号化する。このとき、端末情報格納部４３に格納されているハードウェア公開鍵を使用してエージェントを復号化する。

【００２７】

また、クライアント端末４からファイル管理サーバ２にファイルを保管する場合は、ファイル管理サーバ２からクライアント端末４にファイルを要求するエージェントが送信される。クライアント端末４は、このエージェントを受信すると、そのエージェントにファイルを格納し（ファイル格納手段）、このファイルを格納したエージェントをエージェント暗号化手段４６にてファイル管理サーバ２の公開鍵を使用して暗号化しファイル管理サーバ２に送る（エージェント送信手段）。

【００２８】

また、クライアント端末４からファイル管理サーバ２にファイルを保管する場合においてそのファイルを暗号化して保管する場合は乱数発生手段４５が発生する乱数を使用する。このとき、ファイル毎に別々の鍵で暗号化するために乱数発生手段４５から動的に変化する乱数を発生させ、その乱数とクライアント端末のハードウェア公開鍵をもとに動的鍵生成手段４４で動的に変更される新しい共通鍵を作り（共通鍵生成手段）、この共通鍵を使用してファイルを暗号化する。そして、この暗号化されたファイルと使用した乱数をエージェントに格納してファイル管理サーバ２に送信する。

【００２９】

ファイル管理サーバ２は、暗号化されたファイルと使用した乱数を格納したエージェントを受信すると、そのエージェントをサーバ情報格納部２２に格納されているサーバの秘密鍵を使用して復号化し、この復号化したエージェントからファイルを受け取ってファイル管理データベース２５に保管する（ファイル保管手段）。そして、ファイルを取り出したエージェントには乱数が格納されており、上記において保管したファイルをクライアント端末４に送信するときにはこの乱数が必要となる。このため、乱数を保持したこのエージェントをエージェント格納部３０に保管する（エージェント保管手段）。

【００３０】

その後、ファイル管理サーバ２が、クライアント端末４から上記において保管したファイルの取得要求を受信すると、そのクライアント端末４に対してアクセス許可を送信し、続いてそのクライアント端末４から暗号化されたハードウェア公開鍵を受信し、それをサーバの秘密鍵で復号化して取得するとエージェント格納部３０から該当する乱数を保持したエージェントを取り出す（エージェント取出手段）。そして、この取り出したエージェントに取得要求のあったファイルをファイル管理データベース２５から読み出して格納する（ファイル格納手段）。このときのファイルはクライアント端末４において共通鍵を使用して暗号化されている。そして、このエージェントを受信したハードウェア公開鍵で暗号化し、該当するクライアント端末４に送信する（エージェント送信手段）。

【００３１】

このような構成のネットワークシステムにおいては、クライアントユーザがクライアント端末４を使用してファイル管理サーバ２からファイルを取得する場合と、クライアントユーザがクライアント端末４を使用してファイル管理サーバ２にファイルを保管させる場合の２通りの処理がある。

【００３２】

クライアント端末４は、図５に示す流れ図に基づく処理を行い、ファイル管理サーバ２は、図６に示す流れ図に基づく処理を行う。

【００３３】

先ず、クライアント端末４は、Ｓ１にて、ファイル管理サーバ２との認証を行う。すなわち、クライアント情報格納部４２からクライアント証明書を取り出してファイル管理サーバ２に送信する（クライアント証明書送信手段、図９のＲ１）。

【００３４】

ファイル管理サーバ２は、Ｓ１１にて、クライアント端末４からのクライアント証明書を

受信すると、そのクライアント証明書を認証サーバ３に送信する（クライアント証明書送信手段、図９のＲ２）。

【００３５】

認証サーバ３はファイル管理サーバ２から送信されたクライアント証明書を予め登録されているクライアント証明書と比較し、一致していれば認証確認とそのクライアント証明書に設定されているクライアントの公開鍵Ｃｐｋｅｙをファイル管理サーバ２に送信する（図９のＲ３）。

【００３６】

ファイル管理サーバ２は、Ｓ１２にて、クライアントの公開鍵Ｃｐｋｅｙを取得する。そして、クライアント端末４に対してサーバの証明書と公開鍵Ｓｐｋｅｙを送信する（サーバ公開鍵送信手段、図９のＲ４）。この送信時においてはサーバ証明書とサーバ公開鍵Ｓｐｋｅｙはクライアント認証で得たクライアント端末の公開鍵Ｃｐｋｅｙを用いて暗号化する。

【００３７】

クライアント端末４は、Ｓ２にて、ファイル管理サーバ２から送信されるサーバの証明書と公開鍵Ｓｐｋｅｙを取得する（サーバ公開鍵取得手段）。そのとき、クライアントの公開鍵で暗号化されている場合は、クライアントの秘密鍵で復号を行い、取り出すことができる。

【００３８】

そして、サーバの証明書を認証サーバ３に送信して証明書が正しいか否かを確認してもらう（サーバ証明書送信手段、図９のＲ５）。この結果、証明書が正しければ、サーバの証明書と公開鍵Ｓｐｋｅｙをサーバ情報格納部４８に格納する。

【００３９】

続いて、クライアント端末４は、Ｓ３にて、端末情報格納部４３に格納されている端末独自のハードウェア公開鍵Ｃｈｐｋｅｙを読み出し、このハードウェア公開鍵Ｃｈｐｋｅｙをサーバ情報格納部４８に格納されているファイル管理サーバ２の公開鍵Ｓｐｋｅｙで暗号化し、Ｓｐｋｅｙ＿Ｃｈｐｋｅｙを生成する。なお、サーバ２にハードウェア公開鍵を暗号化して送らない場合は、この処理は行わない。

【００４０】

続いて、クライアント端末４は、Ｓ４にて、ファイル通信要求をファイル管理サーバ２に送信する（要求送信手段）。すなわち、ファイル取得要求或はファイル保管要求を送信する。

これに対し、ファイル管理サーバ２は、Ｓ１３にて、ファイル通信要求を受信すると、この要求に対してファイルアクセスを許可できるか否かを判断する。許可できないと判断した時には、Ｓ１４にて、アクセス権が無いことをクライアント端末４に通知して処理を終了する。また、許可できることを判断すると、クライアント端末４に対して許可通知を行う（許可送信手段）。

【００４１】

クライアント端末４は、ファイル管理サーバ２から許可通知を受けると、Ｓ５にて、ハードウェア公開鍵Ｃｈｐｋｅｙをファイル管理サーバ２の公開鍵Ｓｐｋｅｙで暗号化した鍵Ｓｐｋｅｙ＿Ｃｈｐｋｅｙをファイル管理サーバ２に送信する（ハードウェア公開鍵送信手段）。

【００４２】

ファイル管理サーバ２は、Ｓ１５にて、受信した要求がファイル取得要求か、ファイル保管要求かを確認する。そして、ファイル取得要求であれば、Ｓ１６にて、エージェント生成手段２８はクライアント端末４の宛先情報とファイルをこのクライアント端末に渡す処理機能を有し、要求されたファイルを持ったエージェントを生成する。また、ファイル保管要求であれば、Ｓ１７にて、エージェント生成手段２８はクライアント端末４の宛先情報とファイルを受け取る処理機能を有するエージェントを生成する。

【００４３】

続いて、ファイル管理サーバ２は、Ｓ１８にて、エージェント暗号化手段３１により生成されたエージェントをハードウェア公開鍵Ｃｈｐｋｅｙで暗号化し、Ｓ１９にて、要求を受けたクライアント端末４に送信する（エージェント送信手段）。この場合、ハードウェア公開鍵Ｃｈｐｋｅｙがファイル管理サーバ２の公開鍵Ｓｐｋｅｙで暗号化されている鍵Ｓｐｋｅｙ＿Ｃｈｐｋｅｙであれば、ファイル管理サーバ２の秘密鍵Ｓｓｋｅｙで鍵Ｓｐｋｅｙ＿Ｃｈｐｋを復号化し、ハードウェア公開鍵Ｃｈｐｋｅｙを取り出してからエージェントの暗号化を行う。

【００４４】

なお、ファイルが乱数を使用したクライアント端末独自の暗号で暗号化されている場合はその乱数情報を保持することになる。この乱数情報はファイルを暗号化するときにクライアント端末のハードウェア公開鍵Ｃｈｐｋｅｙから共通鍵を生成する場合に用いるものである。この場合、ファイル管理サーバ２内で保管しておいた乱数情報を持ったエージェントを呼び出し、そのエージェントに指定のファイルを持たせ、クライアント端末４のハードウェア公開鍵Ｃｈｐｋｅｙで暗号化する。

【００４５】

クライアント端末４は、ファイル管理サーバ２からエージェントを受信すると、図７に示す流れ図に基づく処理を行い、ファイル管理サーバ２は、クライアント端末４からエージェントを受信すると、図８に示す流れ図に基づく処理を行う。

【００４６】

すなわち、クライアント端末４は、図７に示すように、Ｓ２１にて、エージェントを受信すると、Ｓ２２にて、このエージェントがクライアント端末４のハードウェア公開鍵Ｃｈｐｋｅｙで暗号化されているので、エージェント復号化手段４７により端末情報格納部４３からクライアント端末４のハードウェア秘密鍵Ｃｈｓｋｅｙを読み出し、このハードウェア秘密鍵Ｃｈｓｋｅｙを使用して復号化する（復号化手段）。

【００４７】

続いて、クライアント端末４は、Ｓ２３にて、クライアントユーザがファイル管理サーバ２に指定のファイルを保管させる処理であるか、それともファイル管理サーバ２にあるファイルを取得する処理であるかを判断する。そして、ファイル管理サーバ２にあるファイルを取得する処理であることを判断すると、Ｓ２４にて、エージェントからファイルを受け取る（ファイル受取手段）。エージェントはクライアント端末４にファイルを渡したことをファイル管理サーバ２に報告する。

【００４８】

このような処理を行うことで、エージェントが他のクライアント端末に渡っても他のクライアント端末ではこのエージェントを復号することができない。また、エージェントからのファイルを渡した旨のファイル管理サーバへの報告もされない。また、ファイルがクライアント端末独自の暗号によって暗号化されていた場合にはその暗号鍵の素である乱数をクライアント端末４に渡し、クライアント端末４はその暗号鍵の素とハードウェア公開鍵で共通鍵を作り、ファイルの復号化を行う。これによりエージェントに対する適切なファイルの入出が可能となる。

【００４９】

また、ファイル管理サーバ２に指定のファイルを保管させる処理の場合は、Ｓ２５にて、エージェントに指定したファイルを持たせる。すなわち、エージェントに指定したファイルを格納する（ファイル格納手段）。そして、Ｓ２６にて、エージェント暗号化手段４６により認証で得たファイル管理サーバ２の公開鍵Ｓｐｋｅｙでエージェントを暗号化し、Ｓ２７にて、その暗号化したエージェントをファイル管理サーバ２に送信し（エージェント送信手段）、一連の処理を終了する。なお、ファイルがクライアント端末４による独自の暗号鍵で暗号化されていた場合は、そのときに利用した乱数をエージェントに保持させる。

【００５０】

ファイル管理サーバ２は、図８に示すように、Ｓ３１にて、クライアント端末４から送信

されるエージェントを受信し、Ｓ３２にて、受信したエージェントをエージェント復号化手段３２によりサーバ情報格納部２２に格納されているファイル管理サーバ２の秘密鍵Ｓｓｋｅｙを使用して復号化し、エージェントに格納されているファイルを取り出して保管する（ファイル保管手段）。また、このエージェントはサーバ２がファイルを保管したことをクライアント端末４に通知する。

【００５１】

そして、Ｓ３３にて、エージェントを保管する必要が有るか否かを判断する。すなわち、乱数を保持したエージェントは指定したファイルが要求されたときにその応答に対応するので、このようなエージェントは保管しておく必要がある。従って、エージェントがこのようなエージェントの場合は、Ｓ３４にて、保管する（エージェント保管手段）。

【００５２】

このように、クライアント端末４に、その端末特有のハードウェア公開鍵Ｃｈｐｋｅｙ及びハードウェア秘密鍵Ｃｈｓｋｅｙを格納した端末情報格納部４３を設け、クライアントとサーバとの間の認証が終了すると、クライアント端末４からファイル管理サーバ２にハードウェア公開鍵Ｃｈｐｋｅｙを送信し、ファイル管理サーバ２はファイル通信を行うエージェントを、受信したハードウェア公開鍵Ｃｈｐｋｅｙで暗号化してクライアント端末４に送信するようにしているので、正規のクライアント端末からのみファイル管理サーバへのアクセスしてファイルを取得したり、ファイルを保管させたりでき、これにより、第三者による別の端末からの成り済ましによるファイル管理サーバへのアクセスを防止でき、セキュリティの向上できる。

【００５３】

また、クライアント端末４からファイル管理サーバ２にハードウェア公開鍵Ｃｈｐｋｅｙを送信する場合に、このハードウェア公開鍵Ｃｈｐｋｅｙをファイル管理サーバ２から受信したサーバの公開鍵Ｓｐｋｅｙで暗号化して送信するようにしているので、ハードウェア公開鍵Ｃｈｐｋｅｙが第３者に読み取られるのをさらに防止することができ、よりセキュリティの向上できる。

【００５４】

また、クライアント端末４はファイル管理サーバ２からエージェントを受信すると、そのエージェントをハードウェア秘密鍵Ｃｈｓｋｅｙで復号化している。従って、ハードウェア秘密鍵Ｃｈｓｋｅｙを持っている正規の端末でしかエージェントを復号化することができない。しかも、通信するファイルはエージェントに格納されている。このようにエージェントの復号化及びエージェントが保持しているファイルの取り出しが正規の端末でしかできないので、第三者によるエージェントの復号化及びエージェントが保持しているファイルの取り出しは不可能であり、セキュリティをさらに向上できる。

【００５５】

また、クライアント端末４からのファイル取得要求時に、ファイル管理サーバ２から送信されるエージェントをクライアント端末４が受信してエージェントからファイルを受け取ると、エージェントは正規のクライアントにファイルを渡した結果をファイル管理サーバ２に報告するようにしているので、ファイル管理サーバ２は該当するクライアント端末４にファイルが正しく届けられたか否かを確認することができる。従って、エージェントから応答がなければ誤ったクライアント端末に送信したか、通信が切断されたか、あるいは盗まれたか等に異変に気づくことができる。

【００５６】

さらに、クライアント端末４がファイル管理サーバ２にファイルを保管する場合に、クライアント端末のハードウェア公開鍵と乱数発生手段４５からの乱数によって共通鍵を生成し、その共通鍵を、乱数を変化させることでファイル毎に変更し、それぞれファイルを異なる共通鍵で暗号化するようにしている。また、その乱数情報を対応するエージェントが保管するようにしている。従って、クライアント端末４が共通鍵を保存しなくてもファイルを要求したとき、エージェントがその乱数をクライアントに渡し、その乱数とハードウェア公開鍵とから共通鍵を生成してファイルを復号化することができる。これにより、た

とえファイル管理サーバ２に保管しているクライアント端末４のファイルが盗まれてもファイルが解読されるのを防止することができる。

【００５７】

なお、この実施の形態において、ファイル管理サーバ２に予めクライアント端末４のハードウェア公開鍵を登録し（登録手段）、クライアント端末４からのハードウェア公開鍵を受信した時にこのハードウェア公開鍵を登録されているハードウェア公開鍵と比較して一致しているか否かを判断し（判断手段）、この一致判断によって端末の認証を行ってもよい。

【００５８】

また、ハードウェア公開鍵ではなく、ハードウェア公開鍵のハッシュ値を予めファイル管理サーバ２に送って登録する方法でもよい。すなわち、クライアント端末４は、端末情報格納部４３からハードウェア公開鍵を読み出してそのハッシュ値を求め、このハッシュ値をファイル管理サーバ２に送信する（ハッシュ値送信手段）。

【００５９】

ファイル管理サーバ２はクライアント端末４からハッシュ値を受信すると、そのハッシュ値を保管用メモリに登録する（登録手段）。その後、クライアント端末４からファイル取得要求やファイル保管要求が送信され、そのときにクライアント端末４からハードウェア公開鍵を受信すると、この受信したハードウェア公開鍵のハッシュ値を求め、予め登録していたハッシュ値を比較して一致の有無を判断する（判断手段）。

【００６０】

このように、ハードウェア公開鍵に代えて、そのハッシュ値を使用して端末の確認を行ってもよい。

このように、ハードウェア公開鍵やそのハッシュ値をファイル管理サーバ２に予め登録することで、ファイル通信を許可するクライアント端末４を予め特定することができる。

【００６１】

このようなネットワークシステムは、例えば、ソフトウェアやプログラムの配信システムに容易に適用することができる。すなわち、ソフトウェア配信に適用する場合はファイル管理サーバ２をソフトウェア配信サーバに変更すればよい。ソフトウェア配信サーバはクライアント端末に対してソフトウェアを配信する。この場合にソフトウェアをエージェントに格納して送信させることになる。この場合もエージェントをハードウェア公開鍵で暗号化してクライアント端末に送信するので、ソフトウェアを配信するときの改ざん防止に対処できる。また、常に正規のクライアント端末に配信するのでライセンス違反の防止に対処できる。

【００６２】

例えば、有料のソフトウェア（ＯＳやアプリケーション）の起動コードを各クライアント端末（ソフトウェアを購入したユーザがインストールするマシン）のハードウェア秘密鍵で実行させる。すなわち、ユーザは有料のソフトウェアパッケージをお店で購入し、あるいはネットワークからダウンロードする。そして、そのソフトウェアを起動する場合に、途中までは起動するようになっており、その途中からの起動はソフトウェア配信サーバからコードを受け取って行う。このときにユーザのクライアント端末はそのソフトウェアの製品番号とクライアント端末のハードウェア公開鍵をソフトウェア配信サーバに送信する。その要求を受け取ったソフトウェア配信サーバはその要求を受け取ったクライアント端末でしか動かない起動コードを生成し該当するクライアント端末に配信する。

【００６３】

具体的には、起動コードの一部を、要求を受けたクライアント端末のハードウェア公開鍵で暗号化しておき、起動コードを完全に実行する場合においてクライアント端末のハードウェア秘密鍵で復号化する。すなわち、毎回起動するに当たりその端末のハードウェア秘密鍵にアクセスし復号化を行いそのソフトウェアを起動させるものである。

【００６４】

これは一つのソフトウェアを一つの端末にしか対応させない方式であり、ソフトウェアの

起動コードをクライアントのハードウェア公開鍵で暗号化し、製品番号を対応するハードウェア公開鍵でマッピングさせ管理させておく。ソフトウェアのパッケージを別の端末にインストールする場合を想定すると、起動コードをもらうためにはハードウェア公開鍵と製品番号を送る必要が有る。しかし、その製品番号がすでに別のハードウェア公開鍵とマッチしているために、そのＯＳはライセンス違反をしているということが判明し、不正なライセンス違反を防ぐことに利用できる。また、このソフトウェアを他の端末にコピーしても対応するハードウェア秘密鍵が必要になるため、他の端末では起動することができない。

【００６５】

（第２の実施の形態）

なお、この実施の形態は、本発明をＰＯＳシステムに適用したものについて述べる。

図１０に示すように、ＬＡＮからなるネットワーク６１にファイル管理サーバであるストア管理サーバ６２、認証サーバ６３及びクライアント端末として４台のＰＯＳ端末６４－１，６４－２，６４－３，６４－４を接続してＰＯＳシステムと呼ばれるネットワークシステムを形成している。

【００６６】

このＰＯＳシステムにおいては各ＰＯＳ端末６４－１～６４－４のデータをストア管理サーバ６２で収集し管理するが、各ＰＯＳ端末６４－１～６４－４とストア管理サーバ６２との間では売上データなどの機密データの送受信が行われる。そして、このＰＯＳシステムにおいては接続されるＰＯＳ端末６４－１～６４－４が予め分かっているので、ストア管理サーバ６２は、接続されている各ＰＯＳ端末６４－１～６４－４に設定されている端末独自のハードウェア公開鍵のハッシュ値を予め登録する。なお、ハッシュ値は、ハッシュ関数から生成されるものであり、ストア管理サーバ６２もＰＯＳ端末６４－１～６４－４も同じハッシュ関数を使用する。

【００６７】

例えば、ＰＯＳ端末６４－１とストア管理サーバ６２とでファイル通信を行う場合に、先ず、ＰＯＳ端末６４－１を操作するオペレータ（クライアント）とストア管理サーバ６２との認証を認証サーバ６３により行う。そして、ＰＯＳ端末６４－１からストア管理サーバ６２にファイル取得要求を行う時には、ＰＯＳ端末６４－１からそのＰＯＳ端末のハードウェア公開鍵と指定したファイルの取得要求をストア管理サーバ６２に送信する。

【００６８】

ストア管理サーバ６２は、受け取ったハードウェア公開鍵をＰＯＳ端末６４－１が利用しているのと同じハッシュ関数でハッシュ化を行い事前にそのＰＯＳ端末から受け取っていたハッシュ値と比較する。そして、正しければＰＯＳ端末が正規のものであると判断し、要求されたファイルとＰＯＳ端末６４－１にそのファイルを渡す処理等を持つエージェントを生成し、このエージェントにファイルを保管させ、このエージェントを受け取ったＰＯＳ端末６４－１のハードウェア公開鍵で暗号化する。そして、暗号化したエージェントをＰＯＳ端末６４－１に送信する。

【００６９】

ＰＯＳ端末６４－１は、エージェントを受信すると、そのエージェントをハードウェア秘密鍵で復号化しファイルを得る。

【００７０】

このシステムではネットワーク６１に予めハードウェア公開鍵のハッシュ値がストア管理サーバ６２に登録されていないＰＯＳ端末が接続されていたとしても、このＰＯＳ端末からのユーザ認証では端末認証されないためファイル通信は行えない。

これにより登録されていないＰＯＳ端末からファイルを受け取ることやファイルが盗まれるのを防止することができる。

【００７１】

なお、本発明は、上記実施の形態そのままに限定されるものではなく、実施段階ではその要旨を逸脱しない範囲で構成要素を変形して具体化できる。また、例えば、実施の形態に

示される全構成要素から幾つかの構成要素を削除してもよい。

【００７２】

【発明の効果】

以上詳述したように、本発明によれば、正規のクライアント端末からのみファイル管理サーバへのアクセスを可能とし、これにより、第三者による別の端末からの成り済ましによるファイル管理サーバへのアクセスを防止でき、セキュリティの向上できるネットワークシステムを提供できる。

【図面の簡単な説明】

【図１】本発明の、第１の実施の形態に係るネットワークシステムの構成を示すブロック図。

【図２】同実施の形態におけるファイル管理サーバの機能構成を示すブロック図。

【図３】同実施の形態におけるクライアント端末の機能構成を示すブロック図。

【図４】同実施の形態におけるエージェントの構成を示す図。

【図５】同実施の形態におけるクライアント端末の処理を示す流れ図。

【図６】同実施の形態におけるファイル管理サーバの処理を示す流れ図。

【図７】同実施の形態におけるクライアント端末の処理を示す流れ図。

【図８】同実施の形態におけるファイル管理サーバの処理を示す流れ図。

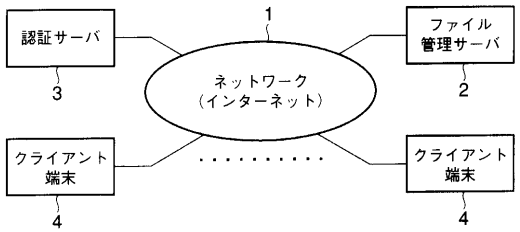
【図９】同実施の形態における証明書による認証を説明するための図。

【図１０】本発明の、第２の実施の形態に係るネットワークシステムの構成を示すブロック図。

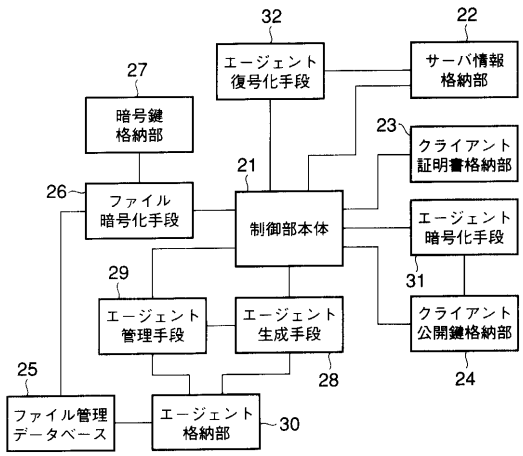
【符号の説明】

１…ネットワーク、２…ファイルサーバ、４…クライアント端末、２１…制御部本体、２８…エージェント生成手段、３１…エージェント暗号化手段、４１…制御部本体、４３…端末情報格納部、４７…エージェント復号化手段。

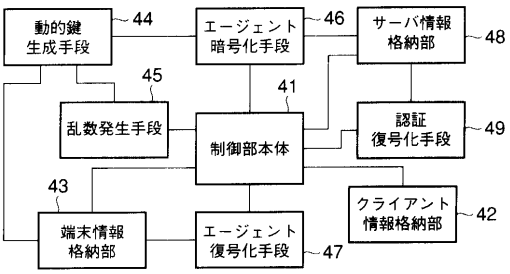
【図１】



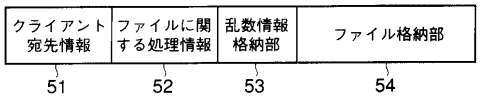
【図２】



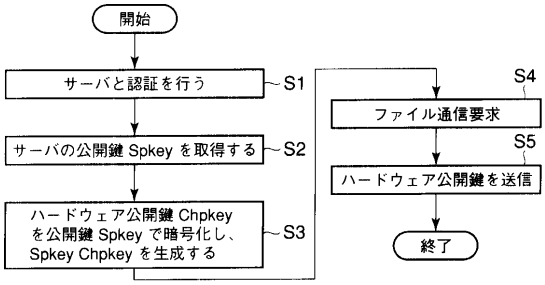
【図３】



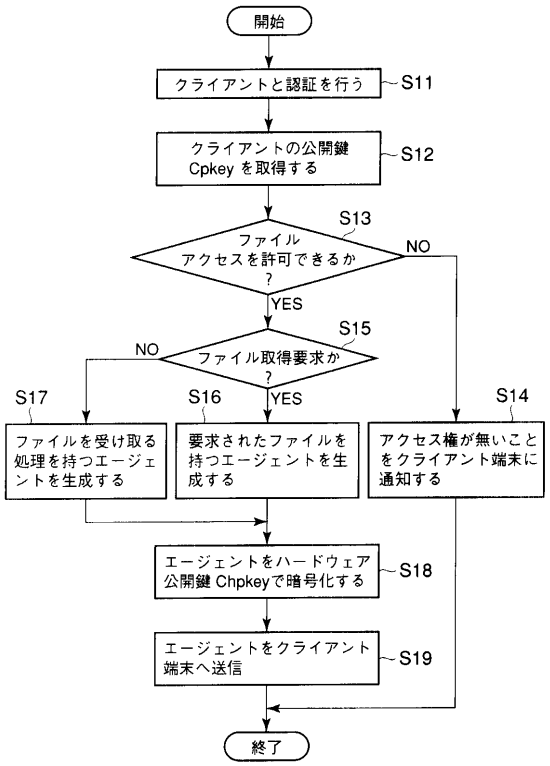
【図４】



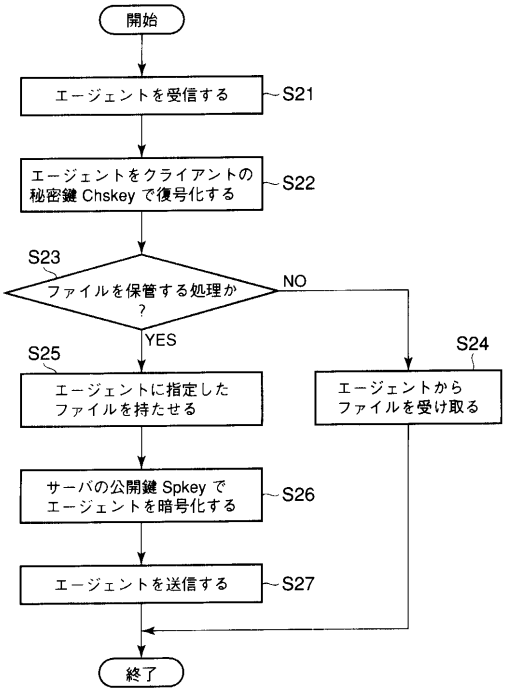
【図５】



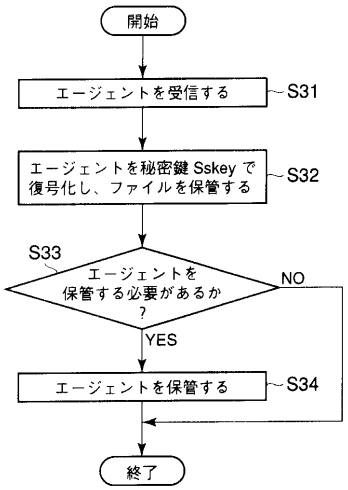
【図６】



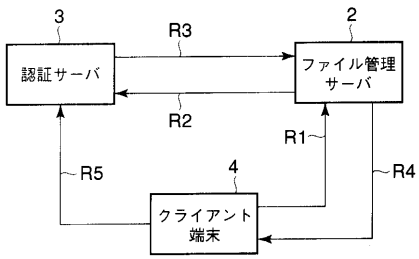
【図７】



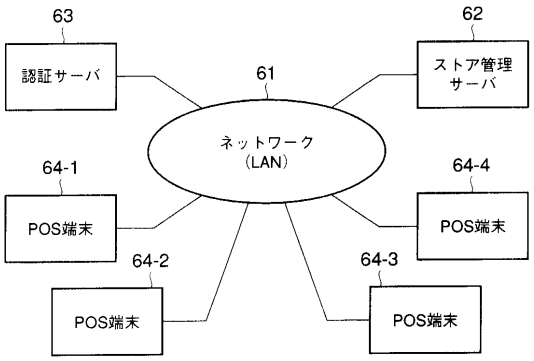
【図８】



【図９】



【図１０】



フロントページの続き

(72)発明者　村形　健太郎
静岡県三島市南町６番７８号　東芝テック株式会社三島事業所内

Ｆターム(参考) 5B017 AA03　BA06　BA07　CA16
5J104 EA17　EA19