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

特許第4415527号
(P4415527)

(45)発行日　平成22年2月17日(2010.2.17)　(24)登録日　平成21年12月4日(2009.12.4)

(51)Int.Cl.		F I		
G06F 21/20	(2006.01)	G06F	15/00	330G
H04L 9/32	(2006.01)	H04L	9/00	675D
H04L 9/08	(2006.01)	H04L	9/00	601C

請求項の数 15　(全 21 頁)

(21)出願番号　特願2002-110455 (P2002-110455)
(22)出願日　平成14年4月12日 (2002.4.12)
(65)公開番号　特開2003-308304 (P2003-308304A)
(43)公開日　平成15年10月31日 (2003.10.31)
審査請求日　平成17年4月8日 (2005.4.8)

(73)特許権者　000005832
パナソニック電工株式会社
大阪府門真市大字門真１０４８番地
(74)代理人　100083806
弁理士　三好　秀和
(74)代理人　100108707
弁理士　中村　友之
(74)代理人　100101247
弁理士　高橋　俊一
(74)代理人　100108914
弁理士　鈴木　壯兵衛
(74)代理人　100112704
弁理士　伊藤　由布子

最終頁に続く

(54)【発明の名称】通信端末及び通信確立プログラム、通信システム

(57)【特許請求の範囲】
【請求項１】
ユーザが保有する記録媒体から認証サーバとの認証処理に必要な情報のうち、少なくともユーザごとの固有情報を読み出して入力する情報入力手段と、
上記情報入力手段にて入力した情報を用いて、認証処理に必要な認証用情報ファイル及び上記認証サーバとの通信に使用する通信用情報ファイルを構成する情報ファイル構成手段と、
上記情報ファイル構成手段にて構成された通信用情報ファイルを参照して上記認証サーバとの間で通信を行い、上記認証用情報ファイルを参照して上記認証サーバとの間で認証処理を行って、上記認証サーバとの間の通信を確立する通信処理手段と、
異なるユーザが保有する記録媒体に記憶された異なる固有情報に対して共通して使用される認証用共通情報及び通信用共通情報を記憶する共通情報記憶手段を更に備え、前記認証用共通情報は、上記認証サーバを区別する識別情報を含む認証処理に必要な情報であり、前記通信用共通情報は、上記認証サーバとの通信を可能にするために使用する情報であり、
上記情報入力手段は、通信利用の正当性を判定するためのパスワード、認証サーバとの間にて認証処理をするに際して使用する認証用固有情報、及び認証サーバとの間で通信処理をするに際して使用する通信用固有情報を上記記録媒体から読み出して入力し、
上記情報ファイル構成手段は、上記情報入力手段にて入力したパスワードから通信利用の正当性が判定された場合に、上記情報入力手段にて入力した認証用固有情報と上記共通

情報記憶手段に記憶された認証用共通情報とを用いて認証用情報ファイルを構成すると共に、上記情報入力手段にて入力した通信用固有情報と上記共通情報記憶手段に記憶された通信用共通情報とを用いて通信用情報ファイルを構成することを特徴とする通信端末。

【請求項２】

上記通信処理手段は、認証処理結果に基づいて上記認証サーバとの間で鍵交換処理をし、鍵交換処理の結果に従って暗号化処理をする鍵交換手段を更に備えることを特徴とする請求項１に記載の通信端末。

【請求項３】

上記情報入力手段は、上記固有情報としてホームアドレスを上記記録媒体から読み出して入力し、

上記情報ファイル構成手段は、上記情報入力手段にて入力したホームアドレスを用いて通信用情報ファイルを構成することを特徴とする請求項１に記載の通信端末。

【請求項４】

上記情報入力手段は、通信利用の正当性を判定するためのパスワード、認証サーバとの間にて認証処理をするに際して使用する認証用固有情報、及び認証サーバとの間で通信処理をするに際して使用する通信用固有情報、各通信端末にて共通した情報である認証用共通情報及び通信用共通情報を上記記録媒体から読み出して入力し、前記認証用共通情報及び前記通信用共通情報は異なるユーザが保有する記録媒体に記憶された異なる固有情報に対して共通して使用される情報であり、前記認証用共通情報は、上記認証サーバを区別する識別情報を含む認証処理に必要な情報であり、前記通信用共通情報は、上記認証サーバとの通信を可能にするために使用する情報であり、

上記情報ファイル構成手段は、上記情報入力手段にて入力した情報から認証用情報ファイル及び通信用情報ファイルを生成することを特徴とする請求項１に記載の通信端末。

【請求項５】

少なくとも上記情報ファイル構成手段に作成された認証用情報ファイル及び通信用情報ファイルを内部に保持して管理するファイル管理手段を更に備え、

上記通信処理手段は、上記情報ファイル構成手段からの指示に応じて、上記ファイル管理手段に保持された認証用情報ファイル及び通信用情報ファイルを読み出して認証処理を行うことを特徴とする請求項１に記載の通信端末。

【請求項６】

上記情報入力手段は、通信利用の正当性を判定するためのパスワードを上記固有情報として入力し、

上記情報ファイル構成手段は、上記認証用情報ファイル及び通信用情報ファイルを構成したことに応じて、上記情報入力手段にて入力したパスワード、上記認証用情報ファイル及び通信用情報ファイルについてのパス情報を一時記憶手段に記憶し、

上記通信処理手段は、上記一時記憶手段にパスワード及びパス情報が入力された場合に当該パスワード及びパス情報を読み出して、通信端末内での認証処理を開始することを特徴とする請求項１に記載の通信端末。

【請求項７】

上記通信処理手段は、通信端末内での認証処理の終了後に上記一時記憶手段に記憶されたパスワード及びパス情報を消去することを特徴とする請求項６に記載の通信端末。

【請求項８】

上記情報ファイル構成手段は、上記通信処理手段の通信端末内での認証処理の終了後に上記一時記憶手段に記憶された認証用情報ファイル及び通信用情報ファイルを消去することを特徴とする請求項６に記載の通信端末。

【請求項９】

上記情報入力手段は、通信利用の正当性を判定するためのパスワードを上記固有情報として入力し、

上記情報ファイル構成手段は、上記認証用情報ファイル及び通信用情報ファイルを構成したことに応じて、上記情報入力手段にて入力したパスワード、上記認証用情報ファイル

及び通信用情報ファイルについてのパス情報を、上記通信処理手段に送り、
上記通信処理手段は、上記情報ファイル構成手段からパスワード及びパス情報が入力されたことに応じて認証処理を開始することを特徴とする請求項１に記載の通信端末。
【請求項１０】
上記情報入力手段は、上記通信処理手段との間で認証処理をする認証サーバを識別する認証サーバ識別情報を上記記録媒体から読み出して入力し、
上記通信処理手段は、上記情報入力手段にて入力した認証サーバ識別情報により特定される認証サーバに接続して認証処理をして通信を確立することを特徴とする請求項１に記載の通信端末。
【請求項１１】
上記情報入力手段は、上記通信処理手段での認証処理によって通信を確立する各アプリケーションサーバに対応した各認証サーバを識別する認証サーバ識別情報を上記記録媒体から複数読み出して入力し、
上記通信処理手段は、上記情報入力手段にて入力した各認証サーバ識別情報により特定される各認証サーバとの間で認証処理をして、ユーザに選択されたアプリケーションサーバとの間の通信を確立することを特徴とする請求項１に記載の通信端末。
【請求項１２】
通信確立プログラムは、
コンピュータを、ユーザが保有する記録媒体から認証サーバとの認証処理に必要な情報のうち、少なくともユーザごとの固有情報を読み出して入力する情報入力手段、少なくともユーザごとの固有情報を読み出して入力した場合に、入力した情報を用いて、認証処理に必要な認証用情報ファイル及び上記認証サーバとの通信に使用する通信用情報ファイルを構成するファイル構成手段、として機能させる情報ファイル構成プログラムと、
コンピュータを、上記通信用情報ファイルを参照して上記認証サーバとの間で通信を行い、上記認証用情報ファイルを参照して上記認証サーバとの間で認証処理を行って、上記認証サーバとの間の通信を確立する通信処理手段として機能させる通信処理プログラムとを有し、
コンピュータが、異なるユーザが保有する記録媒体に記憶された異なる固有情報に対して共通して使用される認証用共通情報及び通信用共通情報を、上記情報入力手段が読み出し可能な記録媒体に記憶しておき、前記認証用共通情報は、上記認証サーバを区別する識別情報を含む認証処理に必要な情報であり、前記通信用共通情報は、上記認証サーバとの通信を可能にするために使用する情報であり、
上記情報入力手段は、通信利用の正当性を判定するためのパスワード、認証サーバとの間にて認証処理をするに際して使用する認証用固有情報、及び認証サーバとの間で通信処理をするに際して使用する通信用固有情報を上記記録媒体から読み出して入力し、
上記情報ファイル構成手段は、上記情報ファイル構成手段にて入力したパスワードから通信利用の正当性が判定された場合に、上記情報ファイル構成手段にて入力した認証用固有情報と上記認証用共通情報とを用いて認証用情報ファイルを構成すると共に、上記情報入力手段にて入力した通信用固有情報と上記通信用共通情報とを用いて通信用情報ファイルを構成すること
を特徴とする通信確立プログラム。
【請求項１３】
複数の通信端末との間で認証処理をして、認証処理の結果に応じてアプリケーションサーバと通信端末との間の通信を確立する認証サーバと、
ユーザが保有する記録媒体から上記認証サーバとの認証処理に必要な情報のうち、少なくともユーザごとの固有情報を読み出して入力し、入力した情報を用いて、認証処理に必要な認証用情報ファイル及び上記認証サーバとの通信に使用する通信用情報ファイルを構成し、上記通信用情報ファイルを参照して上記認証サーバとの間で通信を行い、上記認証用情報ファイルを参照して上記認証サーバとの間で認証処理を行う通信端末とを備え、
上記通信端末は、異なるユーザが保有する記録媒体に記憶された異なる固有情報に対し

て共通して使用される認証用共通情報及び通信用共通情報を記憶する共通情報記憶手段を更に備え、前記認証用共通情報は、上記認証サーバを区別する識別情報を含む認証処理に必要な情報であり、前記通信用共通情報は、上記認証サーバとの通信を可能にするために使用する情報であり、

上記情報入力手段は、通信利用の正当性を判定するためのパスワード、認証サーバとの間にて認証処理をするに際して使用する認証用固有情報、及び認証サーバとの間で通信処理をするに際して使用する通信用固有情報を上記記録媒体から読み出して入力し、

上記情報ファイル構成手段は、上記情報入力手段にて入力したパスワードから通信利用の正当性が判定された場合に、上記情報入力手段にて入力した認証用固有情報と上記共通情報記憶手段に記憶された認証用共通情報とを用いて認証用情報ファイルを構成すると共に、上記情報入力手段にて入力した通信用固有情報と上記共通情報記憶手段に記憶された通信用共通情報とを用いて通信用情報ファイルを構成すること

を特徴とする通信システム。

【請求項１４】

上記認証サーバは、アプリケーションサーバとのアクセス許可の程度を示すアクセス許可レベルと、認証処理に必要な情報との関係を予め設定しておき、上記通信端末との認証処理にて上記記録媒体に記録された認証処理に必要な情報を取得して、上記アクセス許可レベルを参照して上記各通信端末の上記アプリケーションサーバへのアクセスを制限することを特徴とする請求項１３に記載の通信システム。

【請求項１５】

上記記録媒体にはユーザ毎の固有情報としてホームアドレスが記憶され、

上記認証サーバは、上記アクセス許可レベルと上記ホームアドレスとの関係を予め設定しておくことを特徴とする請求項１３に記載の通信システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、例えばＩＰＳｅｃ（ＩＰ（Internet Protocol） security protocol）に準拠した認証処理及び暗号化処理をすることで、ＶＰＮ（virtual private network）を構築して通信データを送受信するための通信端末及び通信確立プログラム、通信システムに関する。

【０００２】

【従来の技術】

近年、クライアントーサーバシステムとして、ＩＰＳｅｃに準拠したプロトコルを実装することによりクライアント端末と認証サーバとの間にＶＰＮパスを構築して、認証サーバを介してクライアント端末とアプリケーションサーバとを接続するものが知られている。このようなシステムとしては、例えば特開２００２－４４１４１号公報にて開示されている。

【０００３】

このような従来の通信システムの一例を図１１に示す。この通信システムでは、クライアント端末１０１、認証サーバ１０２、アプリケーションサーバ１０３が通信回線を介して接続されることにより、クライアント端末１０１のアプリケーション処理部１１１とアプリケーションサーバ１０３との間での通信を実現している。また、この通信システムでは、クライアント端末１０１及び認証サーバ１０２にてＩＰ（Internet Protocol）を実装しており、ＲＦＣ（Request For Comments）２００２～ＲＦＣ２００５などに準拠したモバイルＩＰ、ＩＰＳｅｃに対応したＶＰＮパス１０４を構築する機能を有している。

【０００４】

このような通信システムにおけるクライアント端末１０１は、認証クライアント処理部１１２を起動して認証サーバ１０２との間でＶＰＮパス１０４を構築するに際して、入力装置１１３がユーザにより操作されると、起動情報取得部１２１においてログオン画面をユーザに提示してパスワードなどの入力を促す。そして、ユーザによりパスワード入力がな

されると、認証クライアント処理部１１２が起動し、予め設定されたファイルパスに従って情報ファイル管理部１１４にて保持しているネットワーク情報ファイル１３１及び認証情報ファイル１３２を認証・ネットワーク情報取得部１２２にて読み出す。

【０００５】

そして、この通信システムでは、ネットワーク情報ファイル１３１及び認証情報ファイル１３２を用いて、認証処理部１２３と認証サーバ１０２の認証処理部１４１との間で認証処理をし、鍵交換処理部１２４と認証サーバ１０２の鍵交換処理部１４２との間で鍵交換を行う。これにより、クライアント端末１０１の通信処理部１２５と認証サーバ１０２の通信処理部１４３との間で、アプリケーションサーバ１０３のＩＰアドレスを宛先アドレスとしたＩＰパケットを暗号化し、暗号化したデータを用いてＩＰＳｅｃパケットを作成し、更にＩＰヘッダを付加してカプセル化したパケットを用いた通信をすることで、ＶＰＮパス１０４を構築する。

【０００６】

このような通信システムでは、認証クライアント処理部１１２と認証サーバ１０２との間に機密保持性と信頼性の高いデータ通信を実現する。

【０００７】

【発明が解決しようとする課題】

しかしながら、従来の通信システムでは、認証クライアント処理部１１２を入力装置１１３にて起動する、すなわち認証クライアント処理部１１２へのログオンを手動で入力するパスワードのみから起動の判定をしており、且つ、ネットワーク情報ファイル１３１、認証情報ファイル１３２及びファイルパスをクライアント端末１０１内にて保持する構成となっていたので、パスワードが漏洩すると、システム内に侵入されて、不正な通信が行われるという危険性があった。

【０００８】

そこで、本発明は、上述した実情に鑑みて提案されたものであり、端末起動時のログオン処理を安全とすると共に、セキュリティに対する信頼性の高いシステムを構築することができる通信端末及び通信確立プログラム、通信システムを提供することを目的とする。

【０００９】

【課題を解決するための手段】

上述の課題を解決するために、本発明に係る通信端末では、ユーザが保有する記録媒体から認証サーバとの認証処理に必要な情報のうち、少なくともユーザごとの固有情報を読み出して入力する情報入力手段と、上記情報入力手段にて入力した情報を用いて、認証処理に必要な認証用情報ファイル及び上記認証サーバとの通信に使用する通信用情報ファイルを構成する情報ファイル構成手段と、　上記情報ファイル構成手段にて構成された通信用情報ファイルを参照して上記認証サーバとの間で通信を行い、上記認証用情報ファイルを参照して上記認証サーバとの間で認証処理を行って、上記認証サーバとの間の通信を確立する通信処理手段と、異なるユーザが保有する記録媒体に記憶された異なる固有情報に対して共通して使用される認証用共通情報及び通信用共通情報を記憶する共通情報記憶手段を更に備え、前記認証用共通情報は、上記認証サーバを区別する識別情報を含む認証処理に必要な情報であり、前記通信用共通情報は、上記認証サーバとの通信を可能にするために使用する情報であり、上記情報入力手段は、通信利用の正当性を判定するためのパスワード、認証サーバとの間にて認証処理をするに際して使用する認証用固有情報、及び認証サーバとの間で通信処理をするに際して使用する通信用固有情報を上記記録媒体から読み出して入力し、上記情報ファイル構成手段は、上記情報入力手段にて入力したパスワードから通信利用の正当性が判定された場合に、上記情報入力手段にて入力した認証用固有情報と上記共通情報記憶手段に記憶された認証用共通情報とを用いて認証用情報ファイルを構成すると共に、上記情報入力手段にて入力した通信用固有情報と上記共通情報記憶手段に記憶された通信用共通情報とを用いて通信用情報ファイルを構成する。

【００１１】

上述の課題を解決するために、本発明に係る通信確立プログラムでは、コンピュータを

、ユーザが保有する記録媒体から認証サーバとの認証処理に必要な情報のうち、少なくともユーザごとの固有情報を読み出して入力する情報入力手段、少なくともユーザごとの固有情報を読み出して入力した場合に、入力した情報を用いて、認証処理に必要な認証用情報ファイル及び上記認証サーバとの通信に使用する通信用情報ファイルを構成するファイル構成手段、として機能させる情報ファイル構成プログラムと、コンピュータを、上記通信用情報ファイルを参照して上記認証サーバとの間で通信を行い、上記認証用情報ファイルを参照して上記認証サーバとの間で認証処理を行って、上記認証サーバとの間の通信を確立する通信処理手段として機能させる通信処理プログラムとを有し、コンピュータが、異なるユーザが保有する記録媒体に記憶された異なる固有情報に対して共通して使用される認証用共通情報及び通信用共通情報を、上記情報入力手段が読み出し可能な記録媒体に記憶しておき、前記認証用共通情報は、上記認証サーバを区別する識別情報を含む認証処理に必要な情報であり、前記通信用共通情報は、上記認証サーバとの通信を可能にするために使用する情報であり、上記情報入力手段は、通信利用の正当性を判定するためのパスワード、認証サーバとの間にて認証処理をするに際して使用する認証用固有情報、及び認証サーバとの間で通信処理をするに際して使用する通信用固有情報を上記記録媒体から読み出して入力し、上記情報ファイル構成手段は、上記情報ファイル構成手段にて入力したパスワードから通信利用の正当性が判定された場合に、上記情報ファイル構成手段にて入力した認証用固有情報と上記認証用共通情報とを用いて認証用情報ファイルを構成すると共に、上記情報入力手段にて入力した通信用固有情報と上記通信用共通情報とを用いて通信用情報ファイルを構成する。

【００１３】

本発明に係る通信確立プログラムは、ユーザが保有する記録媒体から認証サーバとの認証処理に必要な情報のうち、少なくともユーザごとの固有情報を読み出して入力した場合に、入力した情報を用いて、認証処理に必要な認証用情報ファイル及び上記認証サーバとの通信に使用する通信用情報ファイルを構成する情報ファイル構成プログラムと、

上記通信用情報ファイルを参照して上記認証サーバとの間で通信を行い、上記認証用情報ファイルを参照して上記認証サーバとの間で認証処理を行って、上記認証サーバとの間の通信を確立する通信処理プログラムとを有し、異なるユーザが保有する記録媒体に記憶された異なる固有情報に対して共通して使用される認証用共通情報及び通信用共通情報を、上記情報ファイル構成プログラムが読み出し可能な記録媒体に記憶しておき、前記認証用共通情報は、上記認証サーバを区別する識別情報を含む認証処理に必要な情報であり、前記通信用共通情報は、上記認証サーバとの通信を可能にするために使用する情報であり、上記情報ファイル構成プログラムは、通信利用の正当性を判定するためのパスワード、認証サーバとの間にて認証処理をするに際して使用する認証用固有情報、及び認証サーバとの間で通信処理をするに際して使用する通信用固有情報を上記記録媒体から読み出して入力し、入力したパスワードから通信利用の正当性が判定された場合に、入力した認証用固有情報と上記共通情報記憶手段に記憶された認証用共通情報とを用いて認証用情報ファイルを構成すると共に、上記情報入力手段にて入力した通信用固有情報と上記共通情報記憶手段に記憶された通信用共通情報とを用いて通信用情報ファイルを構成するものである。

本発明に係る通信システムは、複数の通信端末との間で認証処理をして、認証処理の結果に応じてアプリケーションサーバと通信端末との間の通信を確立する認証サーバと、ユーザが保有する記録媒体から上記認証サーバとの認証処理に必要な情報のうち、少なくともユーザごとの固有情報を読み出して入力し、入力した情報を用いて、認証処理に必要な認証用情報ファイル及び上記認証サーバとの通信に使用する通信用情報ファイルを構成し、上記通信用情報ファイルを参照して上記認証サーバとの間で通信を行い、上記認証用情報ファイルを参照して上記認証サーバとの間で認証処理を行う通信端末とを備え、上記通信端末は、異なるユーザが保有する記録媒体に記憶された異なる固有情報に対して共通して使用される認証用共通情報及び通信用共通情報を記憶する共通情報記憶手段を更に備え、前記認証用共通情報は、上記認証サーバを区別する識別情報を含む認証処理に必要な情報であり、前記通信用共通情報は、上記認証サーバとの通信を可能にするために使用す

る情報であり、上記情報入力手段は、通信利用の正当性を判定するためのパスワード、認証サーバとの間にて認証処理をするに際して使用する認証用固有情報、及び認証サーバとの間で通信処理をするに際して使用する通信用固有情報を上記記録媒体から読み出して入力し、上記情報ファイル構成手段は、上記情報入力手段にて入力したパスワードから通信利用の正当性が判定された場合に、上記情報入力手段にて入力した認証用固有情報と上記共通情報記憶手段に記憶された認証用共通情報とを用いて認証用情報ファイルを構成すると共に、上記情報入力手段にて入力した通信用固有情報と上記共通情報記憶手段に記憶された通信用共通情報とを用いて通信用情報ファイルを構成するものである。

【００１４】

【発明の実施の形態】

以下、本発明の実施の形態について図面を参照して説明する。

【００１５】

本発明は、例えば図１に示すように構成された通信システムに適用される。

【００１６】

［通信システムの構成］

この通信システムは、例えばパーソナルコンピュータにて構成された通信端末１、認証サーバ２及びアプリケーションサーバ３が通信回線を介して接続されて構成されている。この通信システムでは、通信端末１と認証サーバ２との間でモバイルＩＰ及びＩＰＳｅｃに準拠したＶＰＮパス４を構築し、認証サーバ２を介して通信端末１とアプリケーションサーバ３との間でアプリケーションデータを伝送する。

【００１７】

通信端末１とアプリケーションサーバ３との間には、図示しない外部エージェント機能を有するルータや、ホームエージェント機能を有するルータが配設される。これらのルータは、通信端末１の移動先のＩＰアドレスであるＣ／ＯＩＰアドレス、通信端末１の本拠のホームＩＰアドレスを管理し、通信端末１とアプリケーションサーバ３との間でアプリケーションデータを中継する。これにより、通信端末１は、移動した場合であっても、ホームネットワークに接続されたアプリケーションサーバ３との間での通信を実現する。

【００１８】

通信端末１は、ユーザに保有される携帯型記録媒体であるＩＣ（Integrated Circuit）カード１０が挿入されるＩＣカード着脱機構を有するＩＣカードリーダ２１を備える。なお、本例では、携帯型記録媒体としてＩＣカード１０を使用した場合について説明するが、これに限らず、例えばＣＤ－Ｒ（Compact Disc-Recordable）やＦＤ（Floppy Disk）、記録機能を備えるＰＤＡ（Personal Digital Assistant）を接続した場合であっても良い。

【００１９】

このＩＣカード１０は、ＩＣにて構成された記憶機構を内蔵している。このＩＣカード１０には、通信端末１のＯＳ（Operation System）にログオンするためのＯＳログオン情報、認証クライアントログオンパスワード、ネットワーク情報、認証情報が少なくとも記憶されている。本例おいて、ＩＣカード１０に記憶される固有のネットワーク情報は、ホームＩＰアドレス情報などである。また、ＩＣカード１０に記憶される認証情報は、通信端末１と認証サーバ２との間で認証処理をするに際して使用する認証子である。

【００２０】

ＩＣカードリーダ２１は、ＩＣカード１０がユーザにより装着されると、その内容を読み出す。ＩＣカードリーダ２１は、ＯＳログオン情報をログオン用ＩＣカード読み取り部２２に出力する。このＯＳログオン情報は、ログオン用ＩＣカード読み取り部２２によってＩＣカードリーダ２１から読みとられてログオン部２３に送られる。ログオン部２３では、ＯＳログオン情報が送られると、図示しない表示部などを用いてユーザにＯＳのパスワード入力を促し、入力されたパスワードに応じてＯＳを起動させる。これにより、ＯＳによりＩＣカード監視部２４が起動される。

【００２１】

このとき、通信端末１では、ＯＳへのログオンが完了してＯＳが起動すると、ＯＳにより

図示しない記録媒体に格納されたＩＣカード監視プログラムを起動させることで、ＩＣカード監視部２４を起動させる。

【００２２】

ＩＣカード監視部２４は、その機能として、ＩＣカード読み取り部３１、情報ファイル構成部３２、起動部３３を有する。ＩＣカード監視部２４には、ＩＣカードリーダ２１により読み出して入力した認証クライアントログオンパスワード情報、ホームＩＰアドレス情報、認証情報が送られる。これらの情報が送られると、ＩＣカード読み取り部３１は、ネットワーク共通情報記憶部２５に予め記憶しておいた通信用共通情報及び認証用共通情報を読み出し、読み出した情報と共に認証クライアントログオンパスワード情報、ホームＩＰアドレス情報、認証情報を情報ファイル構成部３２に送る。

【００２３】

通信用共通情報及び認証用共通情報は、異なるユーザが保有するＩＣカード１０に記憶された異なる固有情報に対して共通して使用される情報である。この通信用共通情報及び認証用共通情報は、予め設定された情報であって、例えば、認証サーバ２を区別するための認証サーバ識別情報、パケット処理に関するパラメータ、モバイルＩＰに関するパラメータ、例えばＩＳＡＫＭＰ（internet security association key management）などの鍵交換プロトコル、ＩＰＳｅｃなどの暗号通信プロトコルに関するパラメータなどがある。これらの共通情報は、予めユーザの入力により生成される。

【００２４】

情報ファイル構成部３２では、ＩＣカード読み取り部３１及びネットワーク共通情報記憶部２５からの情報を用いて、通信端末１と認証サーバ２及びアプリケーションサーバ３との通信に必要なネットワーク情報ファイル４１を再構成すると共に、認証サーバ２との認証処理に必要な認証情報ファイル４２を再構成する。

【００２５】

ネットワーク情報ファイル４１及び認証情報ファイル４２は、情報ファイル管理部２６に送られ、情報ファイル管理部２６により保持されて管理される。このネットワーク情報ファイル４１及び認証情報ファイル４２のパス情報は、情報ファイル構成部３２により作成されて、一時記憶部２７に送られる。

【００２６】

また、情報ファイル構成部３２では、ＩＣカード読み取り部３１を介して送られた認証クライアントログオンパスワードを一時記憶部２７に送る処理をする。情報ファイル構成部３２にてネットワーク情報ファイル４１及び認証情報ファイル４２の再構成が完了し、認証クライアントログオンパスワード及びパス情報を一時記憶部２７に格納した状態となると、起動部３３では、認証クライアント２８を起動する。このとき、起動部３３では、ＯＳに認証クライアント２８の起動要求をすることで、ＯＳに認証クライアント２８を起動させる。

【００２７】

この認証クライアント２８は、その機能として、起動情報取得部５１、認証・ネットワーク情報取得部５２、認証処理部５３、鍵交換処理部５４、通信処理部５５を有している。この認証クライアント２８は、認証処理をすることで、通信端末１と認証サーバ２及びアプリケーションサーバ３との間の通信を確立する通信確立プログラムにて実現する機能にて構成される。

【００２８】

起動情報取得部５１では、起動部３３による起動要求に応じて、一時記憶部２７に記憶された認証クライアントログオンパスワードを読みだし、読み出した認証クライアントログオンパスワードの正当性を判定することで、通信利用の正当性を判定する。起動情報取得部５１は、認証クライアントログオンパスワードが正当であると判定した場合に一時記憶部２７からパス情報を読み出して認証・ネットワーク情報取得部５２に送り、以降の処理を実行させる。

【００２９】

また、起動情報取得部５１では、起動部３３による起動要求に応じて認証クライアント２８を起動させる場合のみならず、ＩＣカード監視部２４から直接認証クライアントログオンパスワード及びパス情報が送られたことを検知して認証クライアントログオンパスワードを読みだして認証クライアント２８を起動させても良い。

【００３０】

一方、起動情報取得部５１は、入力装置２９が手動にて操作されて認証クライアントログオンパスワードが入力された場合には、同様に正当性を判定して、正当と判定したときにデフォルトのパス情報を読み出して認証・ネットワーク情報取得部５２に送る。この場合は、ＩＣカード１０が挿入されたことによるＩＣカード監視部２４は起動せず、情報ファイル管理部２６に保持されているネットワーク情報ファイル４１及び認証情報ファイル４２を再構成せずに使用して以降の処理を実行することになる。

【００３１】

認証・ネットワーク情報取得部５２では、パス情報が送られると、パス情報に基づいて情報ファイル管理部２６にアクセスしてネットワーク情報ファイル４１及び認証情報ファイル４２を読み出して認証処理部５３、鍵交換処理部５４及び通信処理部５５に送る。

【００３２】

認証処理部５３では、ＲＦＣ（Request For Comments）２００２～ＲＦＣ２００５などに準拠したモバイルＩＰに基づいた処理を行うことで、通信端末１と認証サーバ２との間にモバイルＩＰ環境を実現する。このとき、認証処理部５３では、固有情報としてＩＣカード１０に格納されていた認証子及びホームＩＰアドレスを使用して登録要求パケットを認証サーバ２の認証処理部６１に送信し、認証処理部６１から登録応答パケットを受信することにより、認証サーバ２の認証処理部６１との間での認証処理をする。

【００３３】

このような認証処理の結果、認証処理部６１により認証サーバ２を介した通信が許可されると、鍵交換処理部５４では、認証サーバ２の鍵交換処理部６２との間で鍵交換処理をする。このとき、鍵交換処理部５４では、ＲＦＣ２４０１～ＲＦＣ２４１０などに準拠した処理をして、データを暗号化、復号するための暗号鍵を取得する。このような鍵交換処理の結果、暗号鍵、復号鍵の取得に成功することにより、通信端末１と認証サーバ２との間にＶＰＮパス４を構築したことになる。

【００３４】

通信処理部５５は、上述の認証処理及び鍵交換処理、アプリケーションサーバ３とのアプリケーションデータの伝送に際して、認証サーバ２との間でパケット通信をする。

【００３５】

アプリケーション処理部３０にて作成されたアプリケーションデータをアプリケーションサーバ３に送信する場合には、図２に示すように、ＯＳにより、アプリケーション処理部３０にて作成されたアプリケーションデータをデータ領域７２に格納し、このデータ領域７２の先頭に、ＩＰヘッダ情報領域７１を付加してＩＰパケットを作成する。このとき、ＯＳでは、アプリケーションサーバ３のＩＰアドレスであるサーバＩＰアドレスを宛先アドレス領域８２に格納し、更にホームＩＰアドレスを送信元アドレス領域８１に格納する。次いで、通信処理部５５では、ＯＳから送られたＩＰパケットを鍵交換処理により取得した暗号鍵を用いて暗号化して暗号化データを作成する。

【００３６】

次いで、通信処理部５５は、暗号化データをデータ領域７４に格納し、その先頭にＩＰＳｅｃヘッダ領域７３を付加してＩＰＳｅｃパケットを作成する。このとき、通信処理部５５では、認証サーバ２のＩＰアドレスであるサーバＩＰアドレスを認証情報ファイル４２から取得して宛先アドレス領域８４に格納し、更にホームＩＰアドレスを送信元アドレス領域８３に格納する。

【００３７】

次いで、通信処理部５５では、ＩＰＳｅｃパケットをデータ領域７６に格納し、その先頭にＩＰｉｎＩＰヘッダ領域７５を付加することでカプセル化してＩＰｉｎＩＰパケットを

作成する。このとき、通信処理部５５では、認証サーバ２のＩＰアドレスであるサーバＩＰアドレスを宛先アドレス領域８６に格納し、更に手動入力などによるＣ／ＯＩＰアドレス（case of IP address）を送信元アドレス領域８５に格納する。

【００３８】

通信システムでは、このように通信処理部５５によりＩＰｉｎＩＰパケットを作成して、ＶＰＮパス４を介してアプリケーションサーバ３との間でアプリケーションデータを伝送する。これに対し、認証サーバ２の通信処理部６３では、送信元アドレス領域８５に格納されたＣ／ＯＩＰアドレス、送信元アドレス領域８３の送信元アドレス領域８３に格納されたホームＩＰアドレスから通信端末１からのＩＰｉｎＩＰパケットが送信されたと判定し、カプセル化の開放、暗号化データの復号をしてＩＰパケットを復元して、アプリケーションサーバ３に送信する。

【００３９】

一方、宛先アドレス領域８２が通信端末１のホームＩＰアドレス、送信元アドレス領域８１がアプリケーションサーバ３のＩＰアドレスとなったＩＰパケットを認証サーバ２にて受信すると、認証サーバ２では、先ず、送信元アドレス領域８３に認証サーバ２のＩＰアドレスを格納し、宛先アドレス領域８４に通信端末１のホームＩＰアドレスを格納し、更にデータ領域７２のアプリケーションデータを暗号化してＩＰＳｅｃパケットを作成する。次に、通信処理部６３では、送信元アドレス領域８５に認証サーバ２のＩＰアドレス、宛先アドレス領域８６に通信端末１のＣ／ＯＩＰアドレスを格納したＩＰｉｎＩＰパケットを作成して通信端末１に送信する。

【００４０】

なお、上述した通信端末１では、ネットワーク情報ファイル４１及び認証情報ファイル４２を構成する情報の一部であって、ユーザ固有の固有情報をＩＣカード１０に格納しておき、ＩＣカード１０に記憶された固有情報とネットワーク共通情報記憶部２５に記憶された共通情報とを用いてネットワーク情報ファイル４１及び認証情報ファイル４２を再構成をする場合について説明したが、これに限らず、固有情報及び共通情報をＩＣカード１０に格納しておいても良い。このような場合、通信端末１では、ＩＣカード１０から読み出した情報のみを用いてネットワーク情報ファイル４１及び認証情報ファイル４２を再構成する。

【００４１】

このような通信端末１によれば、ネットワーク情報ファイル４１及び認証情報ファイル４２を再構成するための全情報をＩＣカード１０に記憶させるので、ＩＣカード１０に固有情報のみを記録する場合と比較して、セキュリティレベルを向上させることができる。

【００４２】

［通信端末１による通信確立処理］

つぎに、上述した通信システムにおいて、通信端末１により通信を開始するに際して行う通信確立処理について図３のフローチャートを参照して説明する。なお、以下の説明では、固有情報のみがＩＣカード１０に記憶され、共通情報がネットワーク共通情報記憶部２５に記憶されている場合について説明する。

【００４３】

通信端末１は、ＩＣカードリーダ２１にＩＣカード１０が挿入されることに応じてステップＳ１以降の処理を開始し、ＯＳログオン情報がログオン部２３に送られるとステップＳ２に処理を進める。

【００４４】

ステップＳ２では、ログオン部２３によりＯＳのパスワード入力を促すパスワード入力画面をユーザに提示してステップＳ３に処理を進め、正当なパスワード入力がなされていない場合にはステップＳ２の画面表示を維持し、正当なパスワード入力がなされた場合にステップＳ４に処理を進める。

【００４５】

ステップＳ４では、ログオン部２３により正当なパスワードが入力されたことを認識した

後にＯＳを起動してログインしてステップＳ５に処理を進め、更にＩＣカード監視プログラム（アプリケーション）を立ち上げてステップＳ６に処理を進める。

【００４６】

ステップＳ６では、通信端末１が前回に利用されたときに正常に終了していたか否かの判定をＩＣカード監視部２４により判定する。すなわち、ＩＣカード監視部２４では、前回の通信端末１の利用終了時にＩＣカード１０から読み出されて一時記憶部２７に記憶した認証クライアントログオンパスワード及びパス情報が削除されているか否かを判定し、認証クライアントログオンパスワード及びパス情報が正常に削除されておらず異常終了されていたときにはステップＳ７に処理を進め、正常に削除されていたときにはステップＳ８に処理を進める。これにより、以前に挿入されたＩＣカード１０内の固有情報を、今回の利用にて使用不可とする。

【００４７】

ステップＳ７では、一時記憶部２７に記憶されたままとなっている認証クライアントログオンパスワード及びパス情報を削除して、ステップＳ８に処理を進める。これにより、ＩＣカード監視部２４は、前回利用したＩＣカード１０に記憶された固有情報に対する第三者のアクセス可能性を除外する。

【００４８】

ステップＳ８では、ＩＣカードリーダ２１からＩＣカード１０に記憶されているユーザ固有の認証クライアントログオンパスワード、ホームＩＰアドレス情報、認証情報をＩＣカード読み取り部３１により取得して情報ファイル構成部３２に送ってステップＳ９に処理を進める。

【００４９】

ステップＳ９では、情報ファイル構成部３２によりＩＣカード読み取り部３１からの固有情報とネットワーク共通情報記憶部２５に記憶された共通情報とを用いてネットワーク情報ファイル４１及び認証情報ファイル４２を再構成して、情報ファイル管理部２６に送り、次いで、ステップＳ１０では、ネットワーク情報ファイル４１及び認証情報ファイル４２を再構成したことに応じて認証クライアントログオンパスワード及びパス情報を一時記憶部２７に格納して、ステップＳ１１に処理を進める。

【００５０】

ステップＳ１１では、起動部３３により認証クライアント２８を起動する処理をしてステップＳ１２に処理を進め、起動情報取得部５１により、今回の起動が手動起動か、ＩＣカード監視部２４が起動したことによる自動起動かの判定をする。このとき、起動情報取得部５１では、自動起動を判定するに際して、起動部３３による起動要求が発生したか否か、又は、一時記憶部２７に認証クライアント起動ログオンパスワード及びパス情報が一時記憶部２７に記憶されたか否かを判定する。起動情報取得部５１により自動起動であると判定した場合には、ステップＳ１３に処理を進め、認証・ネットワーク情報取得部５２により一時記憶部２７から認証クライアントログオンパスワード及びパス情報を取得してステップＳ１７に処理を進める。

【００５１】

一方、起動情報取得部５１により手動起動であると判定した場合には、ステップＳ１４に処理を進め、起動情報取得部５１によりパスワード入力画面をユーザに提示してステップＳ１５に処理を進め、正当な認証クライアントログオンパスワードの入力がなされた場合にステップＳ１６に処理を進める。ステップＳ１６では、予め設定されたデフォルトのネットワーク情報ファイル４１及び認証情報ファイル４２を取得するためのパス情報を認証・ネットワーク情報取得部５２にて取得してステップＳ１７に処理を進める。

【００５２】

ステップＳ１７において、認証・ネットワーク情報取得部５２は、ステップＳ１３又はステップＳ１６にて取得したパス情報に基づいて情報ファイル管理部２６からネットワーク情報ファイル４１及び認証情報ファイル４２を取得してネットワーク情報及び認証情報を認証処理部５３、鍵交換処理部５４及び通信処理部５５に送ってステップＳ１８に処理を

進める。
【００５３】
ステップＳ１８において、認証処理部５３は、認証情報を用いて認証サーバ２との間で認証処理を行い、ステップＳ１９において認証処理の結果、認証サーバ２にて認証されたか否かを判定して、認証されなかった場合にはステップＳ２０に処理を進めてエラー処理をして処理を終了する。一方、認証サーバ２に認証された場合にはステップＳ２１に処理を進める。
【００５４】
ステップＳ２１では、鍵交換処理部５４により認証サーバ２との鍵交換処理を行ってステップＳ２２に処理を進め、鍵交換が成功しなかったと判定したときにはステップＳ２３に処理を進めてエラー処理をして処理を終了する。一方、認証サーバ２との間での鍵交換処理が成功した場合にはステップＳ２４に処理を進める。
【００５５】
ステップＳ２４では、ステップＳ１８での認証処理、ステップＳ２１での鍵交換処理により、ＶＰＮパス４を構築したアプリケーションサーバ３との通信が確立し、ステップＳ２５において通信処理部５５により図２に示すようなＩＰｉｎＩＰパケットによる暗号化通信を開始する。
【００５６】
そして、ＶＰＮパス４を介した暗号化通信を終了するログオフ命令がＯＳにより発生した場合には、図４のステップＳ３１の処理を開始し、ＩＣカード監視部２４の情報ファイル構成部３２により、ネットワーク情報ファイル４１及び認証情報ファイル４２を削除するように情報ファイル管理部２６を制御して、ステップＳ３２に処理を進める。
【００５７】
ステップＳ３２では、情報ファイル構成部３２により、一時記憶部２７に記憶しておいた認証クライアントログオンパスワード及びパス情報を削除してステップＳ３３に処理を進めてＯＳからログオフして処理を終了する。
【００５８】
［通信端末１による他の通信確立処理］
つぎに、上述した通信システムにおいて、通信端末１により通信を開始するに際して行う他の通信確立処理について図５のフローチャートを参照して説明する。なお、上述と同じ処理については同一符号を付することによりその詳細な説明を省略する。
【００５９】
この通信確立処理では、ＩＣカード監視部２４を起動した後に、ステップＳ６及びステップＳ７の処理をせずにステップＳ８～ステップＳ１１の処理をし、自動起動された後のステップＳ１７の次のステップＳ４１において、認証・ネットワーク情報取得部５２によりネットワーク情報ファイル４１及び認証情報ファイル４２を削除してステップＳ４２に処理を進める。
【００６０】
ステップＳ４２では、一時記憶部２７によりステップＳ１０にて記憶した認証クライアントログオンパスワード及びパス情報を削除してステップＳ１８に処理を進める。
【００６１】
［実施形態の効果］
以上、詳細に説明したように、本実施形態に係る通信システムによれば、ＩＣカード１０からユーザごとの固有情報を読み出して入力した場合にネットワーク情報ファイル４１及び認証情報ファイル４２を再構成して、通信端末１と認証サーバ２との通信を確立するので、パスワードの漏洩により認証クライアント２８が起動することなく、ＩＣカード１０が挿入された場合のみに認証クライアント２８を起動するようにすることができ、通信端末１が起動する時のログオン処理を安全とすると共に、セキュリティに対する信頼性の高いシステムを構築することができる。
【００６２】

また、この通信システムによれば、共通情報を予めネットワーク共通情報記憶部２５に記憶しておき、ＩＣカード１０が挿入された場合に共通情報と固有情報とを用いてネットワーク情報ファイル４１及び認証情報ファイル４２を再構成するので、ＩＣカード１０に記録する情報量を少なくして、ＩＣカード１０のメモリ消費量を抑制することができる。

【００６３】

更に、この通信システムによれば、ＩＣカード１０が挿入された場合にはＩＣカード監視部２４を起動してＩＣカード１０の固有情報を用いて認証サーバ２と通信確立し、入力装置２９が操作されて起動した場合には通信端末１内の固有情報を用いて認証サーバ２と通信確立をするので、ＩＣカード１０が挿入されない場合でもデフォルトの動作をさせることができ、運用の柔軟性を確保することができる。

【００６４】

更にまた、この通信システムによれば、ＩＣカード１０に認証クライアントログオンパスワードを記録しておき、ネットワーク情報ファイル４１及び認証情報ファイル４２を再構成した後に、パス情報及び認証クライアントログオンパスワードを一時記憶部２７に記憶して認証処理を行うようにしたので、ＩＣカード監視プログラムと認証処理プログラムとの切り分けを容易とすることができる。したがって、この通信システムによれば、既存の認証クライアント２８のプログラム変更を少なくしてＩＣカード監視部２４による上述の処理を追加することができる。

【００６５】

更にまた、この通信システムによれば、起動部３３から直接認証クライアントログオンパスワード及びパス情報が送られたことを認証クライアント２８により検知して認証処理を行うので、一時記憶部２７に記憶することなく、固有情報に対するセキュリティをより向上させることができる。

【００６６】

更にまた、この通信システムによれば、一時記憶部２７に記憶した認証クライアントログオンパスワード及びパス情報を認証クライアント２８又はＩＣカード監視部２４により消去するので、通信が終了した後にネットワーク情報ファイル４１及び認証情報ファイル４２がそのまま保存されてＩＣカード１０に記憶された固有情報が漏洩することを防止することができる。

【００６７】

［通信システムの他の実施形態］

つぎに、通信システムの他の実施形態について説明する。なお、上述の実施形態と同様の部分については同一符号を付することによりその詳細な説明を省略する。

【００６８】

上述した通信システムは、図６に示すように、ＩＣカード１０に通信端末１と接続する認証サーバ２を識別するための認証サーバ識別情報を格納した場合、通信端末１は、認証情報として認証サーバ識別情報を読み出して認証情報ファイル４２を再構成する。これにより、この通信システムによれば、通信端末１の設定に拘わらず、ユーザが指定する認証サーバ２を介してアプリケーションサーバ３との接続を確立することができる。また、この通信システムによれば、ＩＣカード１０ごとに通信端末１の接続先を異なるものにすることができ、ＩＣカード１０を挿入させることで通信端末１の接続先を制限することができる。

【００６９】

これに対し、他の通信システムでは、図７に示すように、通信端末１との通信確立が可能な認証サーバ２Ａ、２Ｂ、２Ｃが存在し、各認証サーバ２Ａ、２Ｂ、２Ｃにそれぞれ異なるアプリケーションサーバ３Ａ、３Ｂ、３Ｃが接続されている場合、ＩＣカード１０に複数の認証サーバＡ識別情報、認証サーバＢ識別情報、認証サーバＣ識別情報を格納しておく。ここで、各アプリケーションサーバ３Ａ、３Ｂ、３Ｃは、通信端末１のアプリケーション処理部３０にて使用する複数のアプリケーションに対応しており、例えばそれぞれの用途が異なるものである。

【００７０】
そして、このＩＣカード１０が挿入された場合には、通信端末１は、複数の認証サーバ２と接続可能とするために、複数の認証サーバＡ識別情報、認証サーバＢ識別情報、認証サーバＣ識別情報を含む認証情報ファイル４２を情報ファイル構成部３２により再構成する。
【００７１】
認証処理をするときには、認証処理部５３は、接続する認証サーバ２の選択を促す認証サーバ選択入力表示などをして、入力装置２９からの命令に従って認証処理をする認証サーバ２を選択する。また、認証処理部５３は、接続する認証サーバ２の選択を促すに際して、通信確立を要求するアプリケーションサーバ３や、通信が確立した後に使用するアプリケーションの選択を促すことにより、アプリケーションサーバ３に接続された認証サーバ２を選択させても良い。
【００７２】
このような通信システムによれば、単一のＩＣカード１０に複数の認証サーバ識別情報を記憶したので、例えばユーザに接続を希望するアプリケーションサーバ３を選択させるのみで複数の認証サーバ２から接続先を指定させることができ、ユーザの利便性を向上させることができる。
【００７３】
更に他の通信システムは、図８に示すように、単一の認証サーバ２に対して複数の通信端末１Ａ、通信端末１Ｂ、通信端末１Ｃが接続され、更に認証サーバ２に複数のアプリケーションサーバ３Ａ、アプリケーションサーバ３Ｂ、アプリケーションサーバ３Ｃが接続されている場合、認証サーバ２により各通信端末１のアクセス制御を行う。
【００７４】
この認証サーバ２は、図９に示すような各通信端末１に対応する認証クライアント２８を識別する認証クライアント識別情報と、アクセス許可のレベルを示すアクセスレベルとを対応づけたテーブルを保持している。このアクセス許可レベルは、図１０に示すように、各アクセスレベル（１～３）に対応して、アプリケーションサーバ３Ａ、アプリケーションサーバ３Ｂ、アプリケーションサーバ３Ｃごとのアクセス許可／不許可を示す。認証サーバ２の認証処理部６１では、通信端末１の認証処理部５３からの登録要求及び接続先のアプリケーションサーバ３を示す情報を受け付けた場合に、図９のテーブルから認証クライアント識別情報を参照してアクセルレベルを認識し、図１０のテーブルからアクセスレベルに対するアクセス許可／不許可を認識する。
【００７５】
そして、認証サーバ２の認証処理部６１では、アクセス許可と判定した場合にはそのまま認証処理を進め、アクセス不許可と判定した場合にはその旨を通信端末１に通知する。
【００７６】
このような通信システムによれば、各通信端末１の認証クライアント２８ごとに、各アプリケーションサーバ３に対するアクセス許可／不許可を判定するので、通信端末１の各アプリケーションサーバ３へのアクセス制御をすることができる。
【００７７】
なお、上述の実施の形態は本発明の一例である。このため、本発明は、上述の実施形態に限定されることはなく、この実施の形態以外であっても、本発明に係る技術的思想を逸脱しない範囲であれば、設計等に応じて種々の変更が可能であることは勿論である。
【００８０】
【発明の効果】
請求項１に係る通信端末によれば、ユーザにより記録媒体が挿入された場合に、ユーザごとの固有情報を読み出して認証用情報ファイル及び通信用情報ファイルを構成して認証サーバとの間の通信を確立するので、パスワードなどの漏洩により認証処理を行うようなことがなく、記録媒体が挿入された場合のみに認証処理をするようにすることができ、起動時のログオン処理を安全とすると共に、セキュリティに対する信頼性の高いシステムを

構築することができる。請求項１に係る通信端末によれば、認証用共通情報及び通信用共通情報を予め記憶しておき、記憶したおいた共通情報と記録媒体から入力した認証用固有情報及び通信用固有情報を用いて認証用情報ファイル及び通信用情報ファイルを構成するので、記録媒体に記録する情報量を少なくして、記録媒体のメモリ消費量を抑制することができる。

【００８１】

請求項２に係る通信端末によれば、通信処理手段により認証サーバとの間で鍵交換処理をし、鍵交換処理の結果に従って暗号化処理をするので、請求項１と同様に、記録媒体が挿入された場合のみに認証処理及び鍵交換処理をするようにすることができ、起動時のログオン処理を安全とすると共に、セキュリティに対する信頼性の高いシステムを構築することができる。

【００８２】

請求項３に係る通信端末によれば、固有情報としてホームアドレスを記録媒体から読み出して入力した場合に、このホームアドレスを用いて通信用情報ファイルを構成するので、請求項１と同様に、ホームアドレスを用いた通信処理をするようにすることができ、起動時のログオン処理を安全とすると共に、セキュリティに対する信頼性の高いシステムを構築することができる。

【００８３】

請求項４に係る通信端末によれば、記録媒体からパスワード、認証用固有情報及び通信用固有情報、認証用共通情報及び通信用共通情報を読み出して入力した場合に、情報ファイル構成手段により認証用情報ファイル及び通信用情報ファイルを生成するようにしたので、記録媒体に固有情報のみを記録する場合と比較して、セキュリティレベルを向上させることができる。

【００８４】

請求項５に係る通信端末によれば、通信処理手段により、情報ファイル構成手段からの指示に応じて、ファイル管理手段に保持された認証用情報ファイル及び通信用情報ファイルを読み出して認証処理を行うので、記録媒体が挿入されない場合でもデフォルトの動作をさせることができ、運用の柔軟性を確保することができる。

【００８５】

請求項６に係る通信端末によれば、通信利用の正当性を判定するためのパスワードを固有情報として入力した場合、情報ファイル構成手段により認証用情報ファイル及び通信用情報ファイルを構成したことに応じてパスワード及び認証用情報ファイル及び通信用情報ファイルについてのパス情報を一時記憶手段に記憶して、通信処理手段による認証処理を開始するようにしたので、情報ファイルを構成するプログラムと認証処理をするプログラムとの切り分けを容易とすることができ、既存の認証処理をするプログラムの設計変更を少なくすることができる。

【００８６】

請求項７に係る通信端末によれば、認証処理の終了後に、一時記憶手段に記憶されたパスワード及びパス情報を通信処理手段により消去するようにしたので、通信が終了した後に通信用情報ファイル及び認証用情報ファイルがそのまま保存されて携帯用記録媒体に記憶された固有情報が漏洩することを防止することができる。

【００８７】

請求項８に係る通信端末によれば、通信処理手段の認証処理の終了後に、一時記憶手段に記憶された認証用情報ファイル及び通信用情報ファイルを情報ファイル構成手段により消去するようにしたので、通信が終了した後に通信用情報ファイル及び認証用情報ファイルがそのまま保存されて携帯用記録媒体に記憶された固有情報が漏洩することを防止することができる。

【００８８】

請求項９に係る通信端末によれば、通信利用の正当性を判定するためのパスワードを固有情報として入力した場合に、パスワード、認証用情報ファイル及び通信用情報ファイル

についてのパス情報を情報ファイル構成手段から通信処理手段に送って認証処理を開始するようにしたので、パスワード及びパス情報を一旦記憶する必要なく、セキュリティを向上させることができる。

【００８９】

請求項１０に係る通信端末によれば、認証サーバ識別情報を記録媒体から読み出して入力した場合に、認証サーバ識別情報により特定される認証サーバに接続を制限して認証処理をして通信を確立するので、既存の設定に拘わらず、ユーザが指定する認証サーバを介してアプリケーションサーバとの接続を確立することができ、更に、記録媒体ごとに通信端末の接続先を異なるものにすることができ、記録媒体を挿入させることで通信端末の接続先を制限することができる。

請求項１１に係る通信端末によれば、各アプリケーションサーバに対応した各認証サーバを識別する認証サーバ識別情報を記録媒体から複数読み出して入力した場合に、各認証サーバ識別情報により特定される各認証サーバとの間で認証処理をして、ユーザに選択されたアプリケーションサーバとの間の通信を確立するようにしたので、ユーザに接続を希望するアプリケーションサーバを選択させるのみで複数の認証サーバから接続先を指定させることができ、ユーザの利便性を向上させることができる。

【０１０４】

請求項１２に係る通信確立プログラムによれば、ユーザが保有する記録媒体から認証サーバとの認証処理に必要な情報のうち、少なくともユーザごとの固有情報を読み出して入力した場合に、入力した情報を用いて、認証処理に必要な認証用情報ファイル及び認証サーバとの通信に使用する通信用情報ファイルを構成する情報ファイル構成プログラムと、通信用情報ファイルを参照して認証サーバとの間で通信を行い、認証用情報ファイルを参照して認証サーバとの間で認証処理を行って、認証サーバとの間の通信を確立する通信処理プログラムとにて構成したので、パスワードなどの漏洩により認証処理を行うようなことがなく、記録媒体が挿入された場合のみに認証処理をするようにすることができ、起動時のログオン処理を安全とすると共に、セキュリティに対する信頼性の高いシステムを構築することができる。請求項１２に係る通信確立プログラムによれば、認証用共通情報及び通信用共通情報を予め記憶しておき、記憶したおいた共通情報と記録媒体から入力した認証用固有情報及び通信用固有情報を用いて認証用情報ファイル及び通信用情報ファイルを構成するので、記録媒体に記録する情報量を少なくして、記録媒体のメモリ消費量を抑制することができる。

請求項１３に係る通信システムによれば、複数の通信端末との間で認証処理をして、認証処理の結果に応じてアプリケーションサーバと通信端末との間の通信を確立する認証サーバと、ユーザが保有する記録媒体から認証サーバとの認証処理に必要な情報のうち、少なくともユーザごとの固有情報を読み出して入力し、入力した情報を用いて、認証処理に必要な認証用情報ファイル及び認証サーバとの通信に使用する通信用情報ファイルを構成し、通信用情報ファイルを参照して認証サーバとの間で通信を行い、認証用情報ファイルを参照して認証サーバとの間で認証処理を行う通信端末とからなるので、パスワードなどの漏洩により通信端末にて認証処理を行うようなことがなく、記録媒体が挿入された場合のみに認証処理をするようにすることができ、起動時のログオン処理を安全とすると共に、セキュリティに対する信頼性の高くすることができる。請求項１３に係る通信システムによれば、認証用共通情報及び通信用共通情報を予め記憶しておき、記憶したおいた共通情報と記録媒体から入力した認証用固有情報及び通信用固有情報を用いて認証用情報ファイル及び通信用情報ファイルを構成するので、記録媒体に記録する情報量を少なくして、記録媒体のメモリ消費量を抑制することができる。

【０１０６】

請求項１４に係る通信システムによれば、認証サーバにてアクセス許可レベルと、認証処理に必要な情報との関係を予め設定しておき、アクセス許可レベルを参照して各通信端末のアプリケーションサーバへのアクセスを制限するので、各通信端末ごとに、各アプリケーションサーバに対するアクセス許可／不許可を判定するので、通信端末の各アプリケ

ーションサーバへのアクセス制御をすることができる。
請求項１５に係る通信システムによれば、記録媒体にはユーザ毎の固有情報としてホームアドレスが記憶され、認証サーバは、アクセス許可レベルとホームアドレスとの関係を予め設定しておき、ホームアドレスに応じて通信端末のアプリケーションサーバへのアクセスを制限するので、通信端末の各アプリケーションサーバへのアクセス制御をすることができる。

【図面の簡単な説明】

【図１】本発明を適用した通信システム及び通信端末の構成を示す機能ブロック図である。

【図２】通信端末の通信処理部及び認証サーバの通信処理部によるパケット作成処理について説明するための図である。

【図３】本発明を適用した通信端末による通信確立処理において、ＩＣカードが挿入されてから暗号通信を開始するまでの処理手順を示すフローチャートである。

【図４】本発明を適用した通信端末による通信確立処理において、暗号通信を終了するときの処理手順を示すフローチャートである。

【図５】本発明を適用した通信端末による通信確立処理において、ＩＣカードが挿入されてから暗号通信を開始するまでの他の処理手順を示すフローチャートである。

【図６】本発明を適用した通信システムの他の実施形態について説明するためのブロック図である。

【図７】本発明を適用した通信システムの更に他の実施形態について説明するためのブロック図である。

【図８】本発明を適用した通信システムの更に他の実施形態について説明するためのブロック図である。

【図９】認証サーバにて保持している認証クライアント識別情報とアクセスレベルとを対応づけたテーブルについて説明するための図である。

【図１０】認証サーバにて保持している各アクセスレベルと各アプリケーションサーバごとのアクセス許可／不許可を示すテーブルについて説明するための図である。

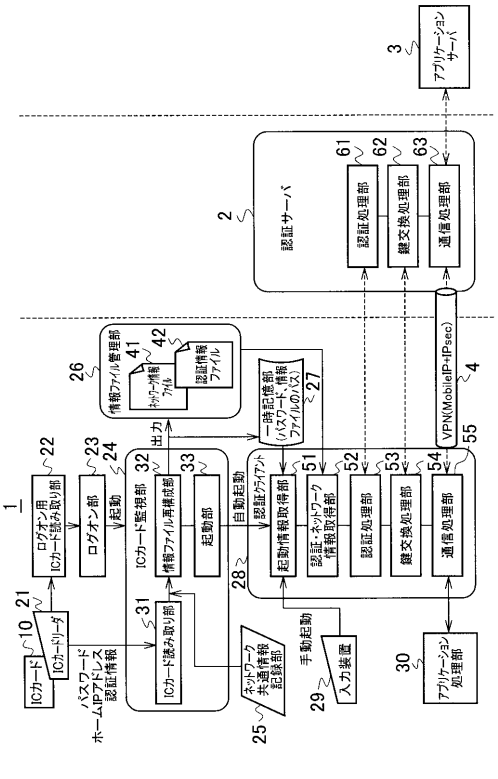
【図１１】従来の通信システムを示すブロック図である。

【符号の説明】

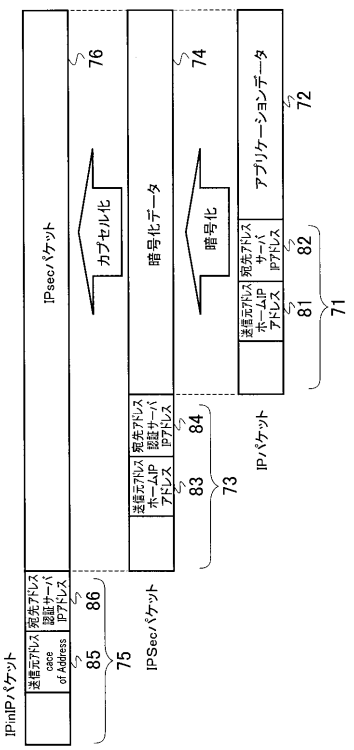
１　通信端末
２　認証サーバ
３　アプリケーションサーバ
４　ＶＰＮパス
１０　ＩＣカード
２１　ＩＣカードリーダ
２２　ログオン用ＩＣカード読み取り部
２３　ログオン部
２４　ＩＣカード監視部
２５　ネットワーク共通情報記憶部
２６　情報ファイル管理部
２７　一時記憶部
２８　認証クライアント
２９　入力装置
３０　アプリケーション処理部
３１　ＩＣカード読み取り部
３２　情報ファイル構成部
３３　起動部
４１　ネットワーク情報ファイル
４２　認証情報ファイル
５１　起動情報取得部

５２　認証・ネットワーク情報取得部
５３　認証処理部
５４　鍵交換処理部
５５　通信処理部
６１　認証処理部
６２　鍵交換処理部
６３　通信処理部
７１　ＩＰヘッダ情報領域
７２，７４，７６　データ領域
７３　ＩＰＳｅｃヘッダ領域
７５　ＩＰｉｎＩＰヘッダ領域
８１，８３，８５　送信元アドレス領域
８２，８４，８６　宛先アドレス領域

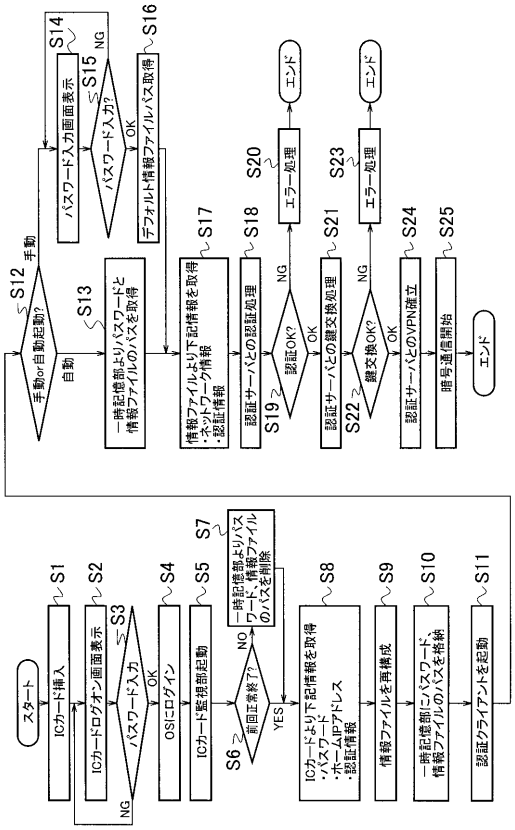
【図１】



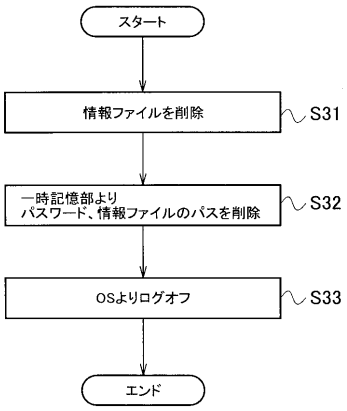
【図２】



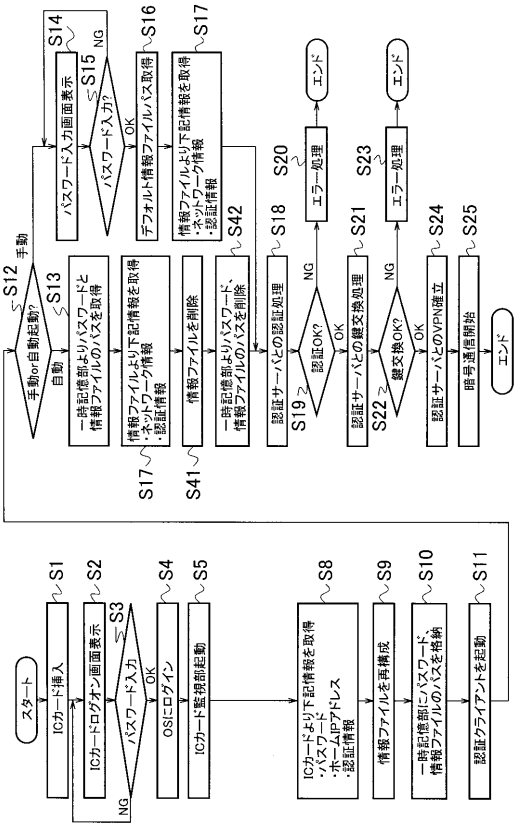
【図３】


スタート
ICカード挿入
ICカードログオン画面表示
パスワード入力
OSにログイン
ICカード監視部起動
前回正常終了?
一時記憶部よりパスワード、情報ファイルのパスを削除
ICカードより下記情報を取得
・パスワード
・ホームIPアドレス
・認証情報
情報ファイルを再構成
一時記憶部にパスワード、情報ファイルのパスを格納
認証クライアントを起動
手動or自動起動?
手動
自動
一時記憶部よりパスワードと情報ファイルのパスを取得
パスワード入力画面表示
パスワード入力?
デフォルト情報ファイルパス取得
情報ファイルより下記情報を取得
・ネットワーク情報
・認証情報
認証サーバとの認証処理
認証OK?
エラー処理
エンド
認証サーバとの鍵交換処理
鍵交換OK?
認証サーバとのVPN確立
暗号通信開始
S1
S2
S3
S4
S5
S6
S7
S8
S9
S10
S11
S12
S13
S14
S15
S16
S17
S18
S19
S20
S21
S22
S23
S24
S25

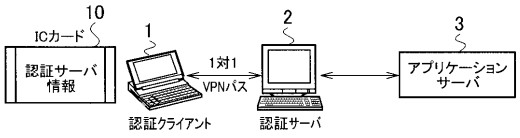
【図４】


スタート
情報ファイルを削除
S31
一時記憶部より
パスワード、情報ファイルのパスを削除
S32
OSよりログオフ
S33
エンド

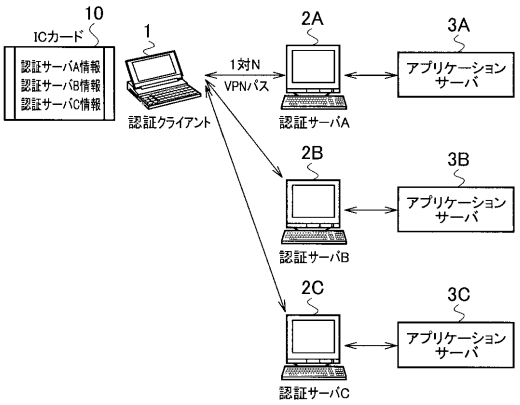
【図５】


スタート
ICカード挿入
ICカードログオン画面表示
パスワード入力
OSにログイン
ICカード監視部起動
ICカードより下記情報を取得
・パスワード
・ホームIPアドレス
・認証情報
情報ファイルを再構成
一時記憶部にパスワード、情報ファイルのパスを格納
認証クライアントを起動
手動or自動起動?
手動
自動
一時記憶部よりパスワードと情報ファイルのパスを取得
パスワード入力画面表示
パスワード入力?
デフォルト情報ファイルパス取得
情報ファイルより下記情報を取得
・ネットワーク情報
・認証情報
情報ファイルを削除
一時記憶部よりパスワード、情報ファイルのパスを削除
認証サーバとの認証処理
認証OK?
エラー処理
エンド
認証サーバとの鍵交換処理
鍵交換OK?
認証サーバとのVPN確立
暗号通信開始
S1
S2
S3
S4
S5
S8
S9
S10
S11
S12
S13
S14
S15
S16
S17
S18
S19
S20
S21
S22
S23
S24
S25
S41
S42

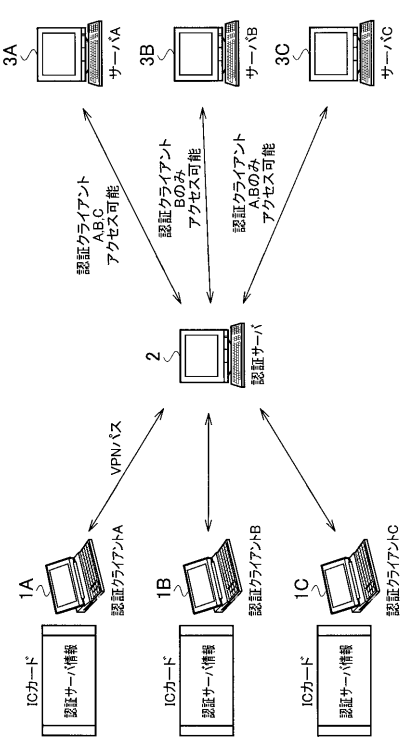
【図６】


10
ICカード
認証サーバ情報
1
認証クライアント
1対1
VPNパス
2
認証サーバ
3
アプリケーションサーバ

【図７】


10
ICカード
認証サーバA情報
認証サーバB情報
認証サーバC情報
1
認証クライアント
1対N
VPNパス
2A
認証サーバA
3A
アプリケーションサーバ
2B
認証サーバB
3B
アプリケーションサーバ
2C
認証サーバC
3C
アプリケーションサーバ

【図８】



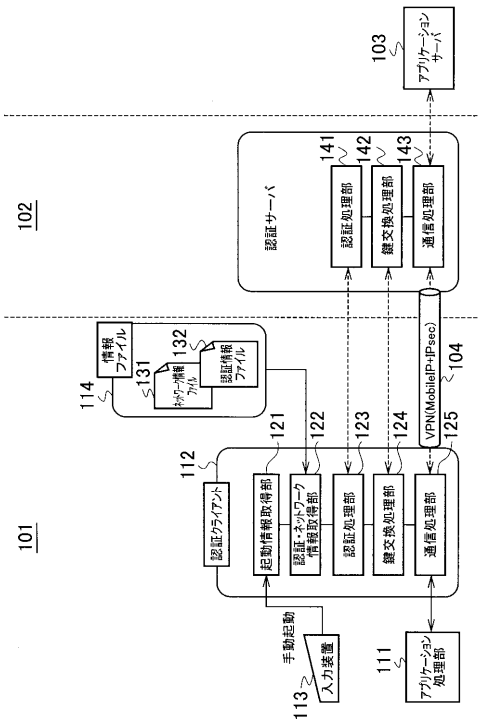
【図９】

認証クライアント	アクセスレベル
A	2
B	1
C	3

【図１０】

アクセスレベル	アクセス許可		
	サーバA	サーバB	サーバC
1	○	○	○
2	○	×	○
3	○	×	×

【図１１】



フロントページの続き

(72)発明者　石田　美津代
大阪府門真市大字門真１０４８番地　松下電工株式会社内
(72)発明者　中村　裕
大阪府門真市大字門真１０４８番地　松下電工株式会社内
(72)発明者　西園　賢治
大阪府門真市大字門真１０４８番地　松下電工株式会社内

審査官　鳥居　稔

(56)参考文献　特開２００１－３０６５０５（ＪＰ，Ａ）
特開２００１－０２２７０２（ＪＰ，Ａ）
特開平１１－３２８１８７（ＪＰ，Ａ）
特開２００１－０２２７００（ＪＰ，Ａ）
特開２００１－３５７０２０（ＪＰ，Ａ）
特開２０００－３２２３８３（ＪＰ，Ａ）
特開２００１－２１６２７１（ＪＰ，Ａ）
特開２００２－０５５９６１（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F　21/20