

【公報種別】特許法第17条の2の規定による補正の掲載

【部門区分】第6部門第3区分

【発行日】平成17年9月22日(2005.9.22)

【公開番号】特開2003-308304(P2003-308304A)

【公開日】平成15年10月31日(2003.10.31)

【出願番号】特願2002-110455(P2002-110455)

【国際特許分類第7版】

G 06 F 15/00

H 04 L 9/08

H 04 L 9/32

【F I】

G 06 F 15/00 3 3 0 G

H 04 L 9/00 6 7 5 D

H 04 L 9/00 6 0 1 C

【手続補正書】

【提出日】平成17年4月8日(2005.4.8)

【手続補正1】

【補正対象書類名】明細書

【補正対象項目名】発明の名称

【補正方法】変更

【補正の内容】

【発明の名称】通信端末及び通信システム

【手続補正2】

【補正対象書類名】明細書

【補正対象項目名】特許請求の範囲

【補正方法】変更

【補正の内容】

【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ホームアドレスを含む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を構成し、上記ホームアドレスを用いて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

を備えることを特徴とする通信端末。

【請求項2】

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上記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、

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、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、

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4】

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5】

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を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6】

上記通信処理手段は、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7に記載の通信端末。

【請求項7】

上記情報ファイル構成手段は、上記通信処理手段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5に記載の通信端末。

【請求項8】

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のパスワード及びパス情報の入力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9】

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10】

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11】

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通信システム。

#### 【請求項12】

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11に記載の通信システム。

#### 【手続補正3】

【補正対象書類名】明細書

【補正対象項目名】0001

【補正方法】変更

【補正の内容】

【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システムに関する。

#### 【手続補正4】

【補正対象書類名】明細書

【補正対象項目名】0008

【補正方法】変更

【補正の内容】

【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システムを提供することを目的とする。

#### 【手続補正5】

【補正対象書類名】明細書

【補正対象項目名】0009

【補正方法】変更

【補正の内容】

【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としてのホームアドレス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を構成し、上記ホームアドレスを用いて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を備える。

【手続補正6】

【補正対象書類名】明細書

【補正対象項目名】0010

【補正方法】削除

【補正の内容】

【手続補正7】

【補正対象書類名】明細書

【補正対象項目名】0011

【補正方法】削除

【補正の内容】

【手続補正8】

【補正対象書類名】明細書

【補正対象項目名】0012

【補正方法】削除

【補正の内容】

【手続補正9】

【補正対象書類名】明細書

【補正対象項目名】0013

【補正方法】変更

【補正の内容】

【0013】

本発明に係る通信システムでは、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。

【手続補正10】

【補正対象書類名】明細書

【補正対象項目名】0078

【補正方法】削除

【補正の内容】

【手続補正11】

【補正対象書類名】明細書

【補正対象項目名】0079

【補正方法】削除

【補正の内容】

**【手続補正12】****【補正対象書類名】**明細書**【補正対象項目名】**0080**【補正方法】**変更**【補正の内容】****【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。また、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、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。

**【手続補正13】****【補正対象書類名】**明細書**【補正対象項目名】**0081**【補正方法】**変更**【補正の内容】****【0081】**

請求項2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。

**【手続補正14】****【補正対象書類名】**明細書**【補正対象項目名】**0082**【補正方法】**変更**【補正の内容】****【0082】**

請求項3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。

**【手続補正15】****【補正対象書類名】**明細書**【補正対象項目名】**0083**【補正方法】**変更**【補正の内容】****【0083】**

請求項4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。

**【手続補正16】****【補正対象書類名】**明細書

【補正対象項目名】0084

【補正方法】変更

【補正の内容】

【0084】

請求項5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る、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。

【手続補正17】

【補正対象書類名】明細書

【補正対象項目名】0085

【補正方法】変更

【補正の内容】

【0085】

請求項6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。

【手続補正18】

【補正対象書類名】明細書

【補正対象項目名】0086

【補正方法】変更

【補正の内容】

【0086】

請求項7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。

【手続補正19】

【補正対象書類名】明細書

【補正対象項目名】0087

【補正方法】変更

【補正の内容】

【0087】

請求項8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。

【手続補正20】

【補正対象書類名】明細書

【補正対象項目名】0088

【補正方法】変更

【補正の内容】

【0088】

請求項9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る、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。

【手続補正21】

【補正対象書類名】明細書

【補正対象項目名】0089

【補正方法】変更

【補正の内容】

【0089】

請求項10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。

【手続補正22】

【補正対象書類名】明細書

【補正対象項目名】0090

【補正方法】削除

【補正の内容】

【手続補正23】

【補正対象書類名】明細書

【補正対象項目名】0091

【補正方法】削除

【補正の内容】

【手続補正24】

【補正対象書類名】明細書

【補正対象項目名】0092

【補正方法】削除

【補正の内容】

【手続補正25】

【補正対象書類名】明細書

【補正対象項目名】0093

【補正方法】削除

【補正の内容】

【手続補正26】

【補正対象書類名】明細書

【補正対象項目名】0094

【補正方法】削除

【補正の内容】

【手続補正27】

【補正対象書類名】明細書

【補正対象項目名】0095

【補正方法】削除

【補正の内容】

【手続補正28】

【補正対象書類名】明細書

【補正対象項目名】0096

【補正方法】削除

【補正の内容】

【手続補正29】

【補正対象書類名】明細書

【補正対象項目名】0097

【補正方法】削除

【補正の内容】

【手続補正30】

【補正対象書類名】明細書

【補正対象項目名】0098

【補正方法】削除

【補正の内容】

【手続補正31】

【補正対象書類名】明細書

【補正対象項目名】0099

【補正方法】削除

【補正の内容】

【手続補正32】

【補正対象書類名】明細書

【補正対象項目名】0100

【補正方法】削除

【補正の内容】

【手続補正33】

【補正対象書類名】明細書

【補正対象項目名】0101

【補正方法】削除

【補正の内容】

【手続補正34】

【補正対象書類名】明細書

【補正対象項目名】0102

【補正方法】削除

【補正の内容】

【手続補正35】

【補正対象書類名】明細書

【補正対象項目名】0103

【補正方法】削除

【補正の内容】

**【手続補正36】****【補正対象書類名】**明細書**【補正対象項目名】**0104**【補正方法】**変更**【補正の内容】****【0104】**

請求項11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にならなく、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。また、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／不許可を判定でき、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。

**【手続補正37】****【補正対象書類名】**明細書**【補正対象項目名】**0105**【補正方法】**削除**【補正の内容】****【手続補正38】****【補正対象書類名】**明細書**【補正対象項目名】**0106**【補正方法】**変更**【補正の内容】****【0106】**

請求項12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。