

明 細 書

発明の名称：

V P N接続認証システム、ユーザ端末、認証サーバ、生体認証結果証拠情報検証サーバ、V P N接続サーバ、およびプログラム

技術分野

[0001] 本発明の実施形態は、V P N接続認証システム、ユーザ端末、認証サーバ、生体認証結果証拠情報検証サーバ、V P N接続サーバ、およびプログラムに関する。

背景技術

[0002] モバイルコンピューティングにおける企業内ネットワークへの接続においては、V P N (Virtual Private network) 接続が利用される。ユーザは、V P N接続において、当該ユーザが接続できる権限を有する者であるか否かの認証としてのユーザ認証を求められる。当該ユーザ認証には、第1または第2の認証機能だけを使うことができる。第1の認証機能はV P N製品が提供する認証機能である。第2の認証機能は、V P N製品以外の製品が提供する認証機能で、V P N製品が連携を可能にする認証機能である。

[0003] V P N製品では、パスワード認証、P K I (Public Key Infrastructure) を使った認証が提供される。V P N製品と連携する認証機能を持つ製品では、ワンタイムパスワードを生成する認証用装置を使う。この装置は、認証用装置に表示されたワンタイムパスワードをV P N製品のパスワードとしてV P N接続クライアントからV P N接続サーバに送信する。この装置は、V P N接続サーバが認証機能を持つ製品に、パスワードとして送信されたワンタイムパスワードを検証させる。

[0004] また、生体情報を用いてユーザを特定する生体認証を行なう生体認証製品もある。この製品は、V P Nのユーザ認証用パスワードを格納し、生体認証が成功した場合に生体認証製品がV P Nのユーザ認証用パスワードを取り出して、V P N接続クライアントに渡してV P N接続のユーザ認証を行う。

先行技術文献

特許文献

- [0005] 特許文献1：特開 2 0 0 1 － 1 4 2 7 6 号公報
特許文献2：特開 2 0 0 5 － 3 1 6 6 6 0 号公報
特許文献3：特開 2 0 0 6 － 2 1 5 8 7 5 号公報

発明の概要

発明が解決しようとする課題

- [0006] ユーザ認証においては、セキュリティとユーザ利便性との両立が望まれる。しかしながら、パスワード認証にはパスワード盗難などの多くのセキュリティ脅威が存在しており、セキュリティ面での問題がある。PKIを使った認証を用いた場合は、ネットワーク上のセキュリティは向上する。しかし、PKIを使った認証では、格納された秘密鍵を利用可能にするために暗証番号などが利用される。このため、クライアントにおけるセキュリティはパスワード認証と同様である。
- [0007] ワンタイムパスワードを生成する認証用装置を使った認証では、ワンタイムパスワードを用いるため、セキュリティの強度は向上する。しかし、ワンタイムパスワードは通常のパスワードより文字数が多い。また、ユーザは認証用装置に表示されたワンタイムパスワードを入力しなければならない。このため、ユーザ利便性が低下するという問題があった。
- [0008] 生体認証製品は、VPNのユーザ認証用パスワードを格納する。生体認証製品は、生体認証が成功した場合に生体認証製品がVPNのユーザ認証用パスワードを取り出して、VPN接続クライアントに渡してVPN接続のユーザ認証を行う。この場合には、ユーザの利便性は向上する。しかし、ネットワーク上のセキュリティはパスワード認証と同様である。

課題を解決するための手段

- [0009] 本発明が解決しようとする課題は、ワンタイムパスワードを生成する認証用装置を使った場合のようなワンタイムパスワードの入力を不要とし、パス

ワード認証よりもセキュリティを向上させることができ、ユーザの本人確認を実行し得るV P N接続認証システム、ユーザ端末、認証サーバ、生体認証結果証拠情報検証サーバ、およびV P N接続サーバを提供することである。

[0010] 実施形態のV P N接続認証システムは、ユーザが用いるユーザ端末と、前記ユーザ端末と通信可能に接続する認証サーバと、前記認証サーバに内蔵され又は通信可能に接続する生体認証結果証拠情報検証サーバと、前記認証サーバから書き込み可能である認証情報管理D Bと、前記ユーザ端末とV P Nで通信可能に接続するV P N接続サーバとを有する。

[0011] 前記ユーザ端末は、前記認証サーバ及び前記V P N接続サーバの間で通信する通信部を有する

前記ユーザ端末は、前記ユーザに前記認証サーバへのV P N接続要求を表示する表示部を有する。

[0012] 前記ユーザ端末は、前記表示部によって表示された前記認証サーバへのV P N接続要求を前記ユーザが決定する入力部を有する。

[0013] 前記ユーザ端末は、前記認証サーバからのチャレンジ値を受け取り、前記ユーザの生体認証を実行して生体認証結果証拠情報を生成し、前記認証サーバへ返却する生体認証処理部を有する。

[0014] 前記ユーザ端末は、前記認証サーバでの認証が成功した場合に、前記認証サーバから受信するI D、トークンから、前記I D及び前記トークンを前記V P N接続サーバへの認証を要求するための形式を持った情報に生成する送信内容生成部を有する。

[0015] 前記ユーザ端末は、前記認証サーバ又は前記V P N接続サーバと前記ユーザ端末との間の通信内容に応じた処理を、前記表示部、前記入力部、前記生体認証処理部、前記送信内容生成部、前記V P N接続部によって実行させ、それらの実行の結果を必要に応じて、前記認証サーバ又は前記V P N接続サーバに送信する制御部を有する。

[0016] 前記認証サーバは、前記ユーザ端末及び前記生体認証結果証拠情報検証サーバと前記認証サーバとの間で通信する通信部有する。

- [0017] 前記認証サーバは、前記ユーザ端末からのVPN接続要求に対して、前記ユーザ端末に送信する前記チャレンジ値を生成するチャレンジ値生成部を有する。
- [0018] 前記認証サーバは、前記生体認証結果証拠情報検証サーバでの検証が成功した場合に、前記トークンを生成するトークン生成部を有する。
- [0019] 前記認証サーバは、前記認証情報管理DBへ前記トークンを書き込むDB処理部を有する。
- [0020] 前記認証サーバは、制御部を有する。この制御部は、前記ユーザ端末又は前記生体認証結果証拠情報検証サーバと前記認証サーバとの間の通信内容に応じた処理を、前記チャレンジ値生成部、前記トークン生成部、前記DB処理部によって実行させ、それらの実行の結果を必要に応じて、前記認証サーバ又は前記VPN接続サーバに送信する。
- [0021] 前記生体認証結果証拠情報検証サーバは、前記認証サーバと前記生体認証結果証拠情報検証サーバとの間で通信する通信部を有する。
- [0022] 前記生体認証結果証拠情報検証サーバは、生体認証結果証拠情報検証部を有する。この生体認証結果証拠情報検証部は、前記ユーザ端末の前記生体認証処理部によって生成され、前記認証サーバを経由して受信する生体認証結果証拠情報を検証して、この検証が成功した場合に、前記検証の結果と生体認証結果証拠情報に含まれるユーザ識別子とを前記認証サーバに返却する。
- [0023] 前記認証情報管理DBは、各前記ユーザに対応して、生体認証処理に係るユーザ識別子、前記VPN接続サーバを利用するユーザの前記ID及び前記トークンを格納する
- 前記VPN接続サーバは、前記ユーザ端末と前記VPN接続サーバとの間で通信する通信部を有する。
- [0024] 前記VPN接続サーバは、前記認証情報管理DBから前記IDと前記トークンとの対を読み出すDB処理部を有する。
- [0025] 前記VPN接続サーバは、前記ユーザ端末から受信した前記IDと前記トークンのうちの前記トークンと、前記IDをキーとして前記認証情報管理DB

Bから読み出したトークンとの一致を判定するトークン判定部を有する。

[0026] 前記V P N接続サーバは、前記ユーザ端末と前記V P N接続サーバとの間のV P N通信を可能にするV P N接続部を有する。

[0027] 前記V P N接続サーバは、前記ユーザ端末から前記IDと前記トークンを受信すると、前記DB処理部、前記トークン判定部、前記V P N接続部を実行させて、それらの実行の結果を必要に応じて前記ユーザ端末に送信する制御部を有する。

図面の簡単な説明

[0028] [図1]図1は、実施形態に係るV P N接続認証システムの構成を示す模式図である。

[図2]図2は、同実施形態における処理フローセアを説明するための模式図である。

[図3]図3は、同実施形態におけるステップST1乃至ST15の動作を説明するためのフローチャートである。

[図4]図4は、同実施形態におけるステップST16乃至ST33の動作を説明するためのフローチャートである。

[図5]図5は、同実施形態における認証情報管理DB40を説明するための模式図である。

発明を実施するための形態

[0029] 以下、実施形態について図面を用いて説明する。なお、以下の各装置は、

装置毎に、ハードウェア構成、又はハードウェア資源とソフトウェアとの組合せ構成のいずれでも実施可能である。組合せ構成のソフトウェアとしては、予めネットワーク又は記憶媒体から対応する装置のコンピュータにインストールされ、対応する装置の機能を実現させるためのプログラムが用いられる。

[0030] 図1は、実施形態に係るV P N接続認証システムの構成を示す模式図である。図2は、同システムにおける処理フローセアを説明するための模式図である。処理フローセアは、図2に示すように、V P N接続要求、第1の認証フロ

セス、第2の認証プロセス、VPN接続から構成される。

[0031] 認証処理とは、認証したい対象（人、装置等）が正当である事を確認するための処理である。また、正当である事とは、検証者が正しいと認めるための基準を、認証したい対象が満たした場合を意味する。

[0032] 以下においては、ユーザは、生体認証処理に係るユーザ識別子、及びVPN接続サーバを利用するユーザのIDを持つものとする。ユーザ識別子とIDとは別であってもよいし、同一であってもよい。

[0033] 実施形態に係るVPN接続認証システムは、ユーザ端末10、認証サーバ20、生体認証結果証拠情報検証サーバ30、認証情報管理DB（Data Base）40、VPN接続サーバ50を備える。

[0034] ユーザ端末10は、ユーザが用いる端末であり、認証サーバ20及びVPN接続サーバ50と接続して通信可能である。

認証サーバ20は、ユーザ端末10及び認証情報管理DB40と接続する。また、認証サーバ20は、生体認証結果証拠情報検証サーバ30を内蔵してもよいし、又は、図1に示すように、生体認証結果証拠情報検証サーバ30と外部で接続して通信可能としてもよい。

生体認証結果証拠情報検証サーバ30は、認証サーバ20に内蔵されてもよいし、又は、図1に示すように、認証サーバ20と外部で接続して通信可能としてもよい。

[0035] 認証情報管理DB40は、認証サーバ20及びVPN接続サーバ50に接続して通信可能である。

VPN接続サーバ50は、ユーザ端末10及び認証情報管理DB40と接続して通信可能である。

[0036] ここで、ユーザ端末10は、通常のコンピュータ機能を有する。ユーザ端末10は、例えば、通信部11、制御部12、表示部13、入力部14、生体認証処理部15、送信内容生成部16及びVPN接続クライアント機能部17を備える。そして、ユーザ端末10は、例えば、携帯電話（フィーチャフォン）、スマートフォン、タブレット端末であってもよい。以下では、

ユーザ端末 10 の各構成を説明する。

[0037] 通信部 11 は、ユーザ端末 10 と認証サーバ 20、VPN 接続サーバ 50 との間の通信インタフェースである。以下の説明では、全ての場合に当てはまるため、通信のときに通信部 11 を経由する旨の記述を省略する。

[0038] 制御部 12 は、認証サーバ 20 又は VPN 接続サーバ 50 との通信内容に応じた 1 つまたは複数の処理を、表示部 13、入力部 14、生体認証処理部 15、送信内容生成部 16、VPN 接続クライアント機能部 17 に実行させる。そして、制御部 12 は、それらの処理の結果を必要に応じて認証サーバ 20 又は VPN 接続サーバ 50 に送信する。制御部 12 は、例えば、以下の機能(f12-1)～(f12-4)を有する。

[0039] (f12-1) 認証サーバ 20 に対して、VPN 接続認証の要求を送信する VPN 接続要求送信機能。

(f12-2) ユーザに対して、認証サーバ 20 により生成された要求としての生体認証の実行を要求する認証要求と認証サーバ 20 により生成されたランダムなチャレンジ値とを当該認証サーバ 20 から受け取ると、チャレンジ値に対応して生体認証処理部 15 が生成する生体認証結果証拠情報に基づいて、送信内容生成部 16 が生成した送信内容を生体認証結果証拠情報として認証サーバ 20 に送信する生体認証結果証拠情報送信機能。

[0040] (f12-3) 認証サーバ 20 からの認証結果、ID、及びトークンを受け取ると、送信内容生成部 16 が当該 ID 及び当該トークンに基づいて送信内容生成部 16 が生成した送信内容を VPN 接続サーバ 50 に送信する ID・トークン送信機能。

[0041] (f12-4) ID 及びトークンを VPN 接続サーバ 50 へ送信した結果、VPN 接続が VPN 接続サーバ 50 で許可された場合に、この VPN 接続サーバ 50 との VPN 通信のための送受信内容の処理を実行する処理結果としての、VPN 接続クライアント機能部 17 での処理結果を送信する VPN 接続通信機能。

ここで、トークンとは上記で実施する生体認証に利用する情報である。ト

ークンは、一時的に生成されるワンタイムパスワードなどを含む。

[0042] 表示部 13 は、表示機能を有する。この表示機能は、例えば、認証サーバ 20 への VPN 接続要求、認証サーバ 20 からの認証要求、生体認証処理部 15 からの操作指示、認証サーバ 20 での認証結果、VPN 接続サーバ 50 との VPN 接続状況を表示する。

入力部 14 は、例えば、表示部 13 に表示された認証サーバ 20 への VPN 接続要求をユーザが決定するための入力機能を有する。

[0043] 生体認証処理部 15 は、例えば、指紋センサや CCD カメラ等の生体認証に用いる機器が適宜使用可能である。認証サーバ 20 への VPN 接続要求があった場合には、この認証サーバ 20 からのチャレンジ値をユーザ端末 10 が受信すると、生体認証処理部 15 は、当該チャレンジ値とともに、ユーザ端末 10 内での生体認証の実行を要求する実行要求を制御部 12 から受け取り、生体認証処理を実行する。そして、生体認証処理部 15 は、当該チャレンジ値を含む生体認証結果証拠情報を生成し、生成結果を制御部 12 に返す。

[0044] 送信内容生成部 16 は、認証サーバ 20 から受信した認証結果、ID、トークンに基づいて、当該 ID 及び当該トークンを VPN 接続サーバ 50 への認証要求のための形式の情報を生成する。

VPN 接続クライアント機能部 17 は、VPN 接続サーバ 50 で認証が成功した後に、VPN 接続サーバ 50 との間の VPN 接続を実行する。

[0045] 認証サーバ 20 は、通信部 21、制御部 22、チャレンジ値生成部 23、トークン生成部 24、DB 処理部 25 を備える。以下では、認証サーバ 20 の各構成を説明する。

通信部 21 は、認証サーバ 20 との間、ユーザ端末 10 との間、及び生体認証結果証拠情報検証サーバ 30 との間の通信インタフェースである。以下の説明では、全ての場合に当てはまるため、通信のときに通信部 21 を経由する旨の記述を省略する。

[0046] 制御部 22 は、ユーザ端末 10 又は生体認証結果証拠情報検証サーバ 30

との通信内容に応じた処理を、チャレンジ値生成部 23、トークン生成部 24、DB 処理部 25 に実行させる。そして、制御部 22 は、それらの結果を必要に応じてユーザ端末 10 又は生体認証結果証拠情報検証サーバ 30 に送信する。制御部 22 は、例えば、以下の機能(f22-1)～(f22-4)を有する。

[0047] (f22-1) ユーザ端末 10 からの VPN 接続要求に対して、チャレンジ値生成部 23 にチャレンジ値を生成させ、この生成したチャレンジ値をユーザ端末 10 に送信するチャレンジ値送信機能。

[0048] (f22-2) ユーザ端末 10 から送信された生体認証結果証拠情報の検証を、生体認証結果証拠情報検証サーバ 30 に対して要求する生体認証結果証拠情報検証要求機能。

(f22-3) 生体認証結果証拠情報の内容に不整合がなく正しいと生体認証結果証拠情報検証サーバ 30 により判断され、その結果、生体認証が正しく実行されて成功した場合に、生体認証結果証拠情報検証サーバ 30 から送信される検証結果及びユーザ識別子に対して、トークン生成部 24 にトークンを生成させるとともに、認証情報管理 DB 40 の当該ユーザ識別子のレコードに対して、当該トークンを DB 処理部 25 に書き込ませるトークン書き込み機能。

[0049] (f22-4) (f22-2)が終了した後に、(f22-2)による検証結果をユーザ端末 10 に対して送信し、併せて、(f22-2)による生体認証結果証拠情報の検証が成功した場合で、さらに(f22-3)も終了した後に、(f22-2)の検証結果に加えて、ユーザ識別子に対応する ID を DB 処理部 25 に検索させて得られた ID とトークンとをユーザ端末 10 に対して送信する検証結果送信機能。

[0050] チャレンジ値生成部 23 は、ユーザ端末 10 から認証サーバ 20 が VPN 接続要求を受け取ると、制御部 22 からの処理要求によって、ユーザ端末 10 に送信するためのチャレンジ値を生成する機能を有する。

[0051] トークン生成部 24 は、生体認証結果証拠情報検証サーバ 30 からの検証結果が成功である事を示す場合に、制御部 22 からの処理要求によってトークンを生成する機能を有する。このトークンは、認証情報管理 DB 40 へ書

き込まれた後にユーザ端末 10 に送信される。

[0052] DB処理部 25 は、トークン生成部 24 によって生成されたトークンを、生体認証結果証拠情報検証サーバ 30 から検証結果とともに返されたユーザ識別子に対応づけて認証情報管理DB 40 に書き込む機能を有する。

[0053] 生体認証結果証拠情報検証サーバ 30 は、通信部 31 と生体認証結果証拠情報検証部 32 とを備える。

通信部 31 は、認証サーバ 20 との間の通信インタフェースである。以下の説明では、全ての場合に当てはまるため、通信のときに通信部 31 を経由する旨の記述を省略する。

[0054] 生体認証結果証拠情報検証部 32 は、ユーザ端末 10 の生体認証処理部 15 で生成された生体認証結果証拠情報を検証する。生体認証結果証拠情報検証部 32 は、生体認証結果証拠情報の内容に不整合がなく正しいと判断し、その結果、生体認証が正しく実行されて検証が成功した場合に、検証結果とともに認証サーバ 20 へ送信するための識別子としての、生体認証結果証拠情報に含まれるユーザ識別子を抽出する機能を有する。

[0055] 図 5 に示すように、認証情報管理DB 40 は、認証情報 40a を格納する。認証情報 40a は、各ユーザに対応して、生体認証処理に係るユーザ識別子、VPN接続サーバを利用するユーザのID及びトークンを格納する。この認証情報管理DB 40 は、ユーザ識別子及びIDのそれぞれをキーとして、認証サーバ 20 によってトークンが書き込まれる機能を有する。同じく、認証情報管理DB 40 は、VPN接続サーバ 50 によりトークンが読み出される機能を有する。なお、認証情報管理DB 40 は、通信機能を有するDB管理サーバであってもよいし、LDAP (Lightweight Directory Access Protocol) サーバであってもよい。

[0056] VPN接続サーバ 50 は、通信部 51、制御部 52、DB処理部 53、トークン判定部 54、VPN接続サーバ機能部 55 を備える。以下では、VPN接続サーバ 50 の各構成を説明する。

[0057] 通信部 51 は、ユーザ端末 10 との間の通信を行なうための通信インタフ

ケースである。以下の説明では、全ての場合に当てはまるため、通信のときに通信部 5 1 を経由する旨の記述を省略する。

[0058] 制御部 5 2 は、ユーザ端末 1 0 からの I D とトークンとを受信すると、D B 処理部 5 3、トークン判定部 5 4、V P N 接続サーバ機能部 5 5 を実行させ、それらの結果を必要に応じてユーザ端末 1 0 に送信する。制御部 5 2 は、例えば、以下の機能(f52-1)～(f52-4)を有する。

[0059] (f52-1) ユーザ端末 1 0 から I D とトークンとを受信すると、認証情報管理 D B 4 0 の中のトークン読出しを、当該 I D をキーとして D B 処理部 5 3 に実行させるトークン読出し機能。

[0060] (f52-2) ユーザ端末 1 0 から受信したトークンと(f52-1)で読み出したトークンとが一致するか否かの判定をトークン判定部 5 4 に実行させるトークン判定機能。

(f52-3) (f52-2)での判定の結果、トークン同士が一致した場合に、ユーザ端末 1 0 と V P N 接続サーバ 5 0 との間の V P N 接続を許可すると共に、ユーザ端末 1 0 との間で V P N による通信を行なうための送受信内容の処理を実行する V P N 接続サーバ機能部 5 5 での処理結果を送信する V P N 接続通信機能。

[0061] 送受信内容の処理を実行する事とは、ユーザ端末 1 0 と V P N 接続サーバ 5 0 との間の通信データの授受の前後（送る場合は前、受ける場合は後）で行なう暗号化等の処理を実行する事である。この事は、V P N 接続サーバ機能部 5 5 の機能でもあるし、翻って、V P N 接続クライアント機能部 1 7 の機能でもある。なお、通信自体は通信部 5 1 が実行する。

[0062] D B 処理部 5 3 は、ユーザ端末 1 0 から受信した I D をキーとして認証情報管理 D B 4 0 の中のトークンを読み出す機能を有する。

トークン判定部 5 4 は、ユーザ端末 1 0 から受信したトークンと D B 処理部 5 3 が認証情報管理 D B 4 0 から読み出したトークンとが一致するか否かを判定する機能を有する。

[0063] V P N 接続サーバ機能部 5 5 は、V P N 接続サーバ 5 0 で認証が成功した

後に、ユーザ端末１０のＶＰＮ接続クライアント機能部１７との間のＶＰＮ接続を実行する機能をも有する。

[0064] 次に、以上のように構成されたＶＰＮ接続認証システムの動作を図２乃至図４のフローチャートを用いて説明する。

ユーザ端末１０においては、図３に示すように、表示部１３に表示された画面に従い、ユーザが入力部１４からＶＰＮ接続要求を選択することによって（ＳＴ２）、ユーザ端末１０から認証サーバ２０にＶＰＮ接続要求が送信される（ＳＴ３）。これにより、第１の認証プロセスが開始される。

[0065] 認証サーバ２０においては、通信部２１がＶＰＮ接続要求を受信すると（ＳＴ４）、制御部２２が、予め決められた又はＶＰＮ接続要求で指定された認証方法に従い、以後の認証処理を実行する。

[0066] 制御部２２は、乱数等からなるチャレンジ値をチャレンジ値生成部２３に生成させて（ＳＴ５）、チャレンジ値を保持するとともに、このチャレンジ値と認証要求とをユーザ端末１０に送信する（ＳＴ６）。ここで、認証要求には、例えば、認証処理を指定する情報や、いくつかの照合アルゴリズムを指定する情報が含まれてもよい。

ユーザ端末１０では、チャレンジ値と認証要求とを受信すると（ＳＴ７）、制御部１２が生体認証処理部１５にチャレンジ値及び生体認証処理実行要求を渡す（ＳＴ８）。

[0067] 生体認証処理部１５は、チャレンジ値及び生体認証処理実行要求を受けると、生体認証処理を実行し、チャレンジ値を含む生体認証結果証拠情報を生成し（ＳＴ８）、当該生体認証結果証拠情報を認証サーバ２０に送信する（ＳＴ９）。ここで、「生体認証結果証拠情報」とは、生体認証で使用された生体認証製品の情報や、予め登録されて使用された生体情報の証明書等である。

[0068] 認証サーバ２０は、ユーザ端末１０から生体認証結果証拠情報を受信すると（ＳＴ１０）、当該生体認証結果証拠情報を生体認証結果証拠情報検証サーバ３０へ送信する（ＳＴ１１）。

[0069] 生体認証結果証拠情報検証サーバ30は、認証サーバ20から生体認証結果証拠情報を受信すると（ST12）、生体認証結果証拠情報検証部32に生体認証結果証拠情報を検証させる。

[0070] 生体認証結果証拠情報検証部32は、生体認証結果証拠情報を検証すると共に、生体認証結果証拠情報に含まれるユーザ識別子を抽出する（ST13）。

生体認証結果証拠情報検証サーバ30は、生体認証結果証拠情報の検証結果を認証サーバ20に送信する。生体認証結果証拠情報検証部32での検証に成功した場合は、生体認証結果証拠情報検証サーバ30は、検証結果と併せて、ユーザ識別子も認証サーバ20に送信する（ST14）。

[0071] 認証サーバ20は、生体認証結果証拠情報検証部32での検証結果を生体認証結果証拠情報検証サーバ30から受信する（ST15）。そして、この検証に成功した場合には、トークン生成部24は、トークンを生成する（ST16）。これにより、第2の認証プロセスが開始される。

[0072] DB処理部25は、生体認証結果証拠情報検証サーバ30から認証サーバ20へ検証結果と共に返されたユーザ識別子に対して、認証情報管理DB40に当該トークンを書き込む。この書き込みと共に、DB処理部25は、トークンに対応するIDを認証情報管理DB40に問い合わせる（ST17）。

[0073] 認証情報管理DB40は、DB処理部25を通じて認証サーバ20から指定されたユーザ識別子に対応するトークンを書き込む（ST18）。そして、認証情報管理DB40は、ユーザ識別子に対応するIDを検索し、この検索したIDをトークンの書き込み結果とともに認証サーバ20に返す（ST19）。

[0074] 認証サーバ20は、認証情報管理DB40から返却された、トークンの書き込み結果とIDとを受け取る（ST20）。そして、認証サーバ20は、当該IDとST16で生成されたトークンとをユーザ端末10に送信する（ST21）。

- [0075] ユーザ端末10は、IDとトークンを認証サーバ20から受け取る (S T 22)。そして、送信内容生成部16は、当該IDと当該トークンに基づいてV P N接続サーバ50に送信する内容を生成して、この生成結果を通信部21を通じてV P N接続サーバ50に送信する (S T 23)。
- [0076] V P N接続サーバ50は、ユーザ端末10からのIDとトークンを受信する (S T 24)。すると、DB処理部53は、認証情報管理DB40に格納されたIDに対するトークンの読出しを認証情報管理DB40に対して要求する (S T 25)。
- [0077] 認証情報管理DB40は、V P N接続サーバ50からの読出し要求に対し、指定されたIDに対するトークンを読み出し (S T 26)、この読み出したトークンをV P N接続サーバ50返却する (S T 27)。
- [0078] V P N接続サーバ50は、認証情報管理DB40からトークンを受け取る (S T 28)。すると、トークン判定部54は、このトークンがS T 24でユーザ端末10から受け取ったトークンと一致するか否かを判定する (S T 29)。そして、双方のトークンが一致した場合は、V P N接続サーバ50は認証成功を示す信号をユーザ端末10に送信する。また、双方のトークンが一致しなかった場合は、V P N接続サーバ50は認証失敗を示す信号をユーザ端末10に送信する (S T 30)。
- [0079] ユーザ端末10は、V P N接続サーバ50から認証結果を受信する (S T 31)。受信した認証結果が成功の場合は、V P N接続クライアント機能部17は、V P N接続サーバ50のV P N接続サーバ機能部55との間のV P N接続を確立して (S T 32)、V P N接続認証の処理を終了する (S T 33)。
- [0080] なお、上記の各実施形態に記載した手法は、コンピュータに実行させることができるプログラムとして、磁気ディスク (フロッピー (登録商標) ディスク、ハードディスクなど)、光ディスク (CD-ROM、DVDなど)、光磁気ディスク (MO)、半導体メモリなどの記憶媒体に格納して頒布することもできる。

また、この記憶媒体としては、プログラムを記憶でき、かつコンピュータが読み取り可能な記憶媒体であれば、その記憶形式は何れの形態であっても良い。

また、記憶媒体からコンピュータにインストールされたプログラムの指示に基づきコンピュータ上で稼働しているOS（オペレーティングシステム）や、データベース管理ソフト、ネットワークソフト等のMW（ミドルウェア）等が上記実施形態を実現するための各処理の一部を実行しても良い。

さらに、各実施形態における記憶媒体は、コンピュータと独立した媒体に限らず、LANやインターネット等により伝送されたプログラムをダウンロードして記憶または一時記憶した記憶媒体も含まれる。

また、記憶媒体は1つに限らず、複数の媒体から上記の各実施形態における処理が実行される場合も本発明における記憶媒体に含まれ、媒体構成は何れの構成であっても良い。なお、各実施形態におけるコンピュータは、記憶媒体に記憶されたプログラムに基づき、上記の各実施形態における各処理を実行するものであって、パソコン等の1つからなる装置、複数の装置がネットワーク接続されたシステム等の何れの構成であっても良い。

また、各実施形態におけるコンピュータとは、パソコンに限らず、情報処理機器に含まれる演算処理装置、マイコン等も含み、プログラムによって本発明の機能を実現することが可能な機器、装置を総称している。

ここまでで実施形態を説明したが、これらの実施形態は、例として提示したものであり、発明の範囲を限定することは意図していない。この新規な実施形態は、その他の様々な形態で実施されることが可能であり、発明の要旨を逸脱しない範囲で、種々の省略、置き換え、変更を行うことができる。この実施形態やその変形は、発明の範囲や要旨に含まれるとともに、特許請求の範囲に記載された発明とその均等の範囲に含まれる。

符号の説明

[0081] 10…ユーザ端末、20…認証サーバ、30…生体認証結果証拠情報検証サーバ、40…認証情報管理DB、50…VPN接続サーバ、11, 21,

3 1, 5 1…通信部、1 2, 2 2, 5 2…制御部、1 3…入力部、1 4…表示部、1 5…生体認証処理部、1 6…送信内容生成部、1 7…V P N接続クライアント機能部、2 3…チャレンジ値生成部、2 4…トークン生成部、2 5…D B処理部、3 2…生体認証結果証拠情報検証部、5 3…D B処理部、5 4…トークン生成部、5 5…V P N接続サーバ機能部、4 0 a…認証情報。

請求の範囲

- [請求項1] ユーザが用いるユーザ端末（１０）と、前記ユーザ端末（１０）と通信可能に接続する認証サーバ（２０）と、前記認証サーバ（２０）に内蔵され又は通信可能に接続する生体認証結果証拠情報検証サーバ（３０）と、前記認証サーバ（２０）から書き込み可能である認証情報管理ＤＢ（４０）と、前記ユーザ端末（１０）とＶＰＮ（Virtual Private network）で通信可能に接続するＶＰＮ接続サーバ（５０）とを備えたＶＰＮ接続認証システムであって、
- 前記ユーザ端末（１０）は、
- 前記認証サーバ（２０）及び前記ＶＰＮ接続サーバ（５０）の間で通信する通信部（１１）と、
- 前記認証サーバ（２０）へのＶＰＮ接続要求を表示する表示部（１３）と、
- 前記表示部（１３）によって表示されたＶＰＮ接続要求を決定するための入力を受け付ける入力部（１４）と、
- 前記認証サーバ（２０）からのチャレンジ値を受け取り、このチャレンジ値に対応して、前記ユーザの生体認証を実行して生体認証結果証拠情報を生成して前記認証サーバ（２０）へ返却する生体認証処理部（１５）と、
- 前記認証サーバ（２０）での認証が成功した場合に、前記認証サーバ（２０）から受信するＩＤ及びトークンに基づいて、これらＩＤ及びトークンが前記ＶＰＮ接続サーバ（５０）への認証を要求するための形式を有する情報を生成する送信内容生成部（１６）と、
- 前記認証サーバ（２０）又は前記ＶＰＮ接続サーバ（５０）と前記ユーザ端末（１０）との間の通信内容に応じた処理を、前記表示部（１３）、前記入力部（１４）、前記生体認証処理部（１５）、前記送信内容生成部（１６）、前記ＶＰＮ接続部（１７）によって実行させ、それらの実行の結果を必要に応じて、前記認証サーバ（２０）又は

前記VPN接続サーバ（50）に送信する制御部（12）と、
を備え、

前記認証サーバ（20）は、

前記ユーザ端末（10）及び前記生体認証結果証拠情報検証サーバ（30）との間で通信する通信部（21）と、

前記ユーザ端末（10）からのVPN接続要求に対して、前記ユーザ端末（10）に送信するためのチャレンジ値を生成するチャレンジ値生成部（23）と、

前記生体認証結果証拠情報検証サーバ（30）での検証が成功した場合に、前記トークンを生成するトークン生成部（24）と、

前記認証情報管理DB（40）へ前記トークンを書き込むDB処理部（25）と、

前記ユーザ端末（10）又は前記生体認証結果証拠情報検証サーバ（30）と前記認証サーバ（20）との間の通信内容に応じた処理を、前記チャレンジ値生成部（23）、前記トークン生成部（24）、前記DB処理部（25）によって実行させ、これらの実行の結果を必要に応じて前記認証サーバ（20）又は前記VPN接続サーバ（50）に送信する制御部（22）と、
を備え、

前記生体認証結果証拠情報検証サーバ（30）は、

前記認証サーバ（20）との間で通信する通信部（31）と、

前記ユーザ端末（10）の前記生体認証処理部（15）によって生成され、前記認証サーバ（20）を経由して受信する生体認証結果証拠情報を検証して、この検証が成功した場合に、前記検証の結果と生体認証結果証拠情報に含まれるユーザ識別子とを前記認証サーバ（20）に返却する生体認証結果証拠情報検証部（32）と、
を備え、

前記認証情報管理DB（40）は、

各ユーザに対応して、生体認証処理に係るユーザ識別子、前記VPN接続サーバ（50）を利用するユーザのID及びトークンを格納し、

前記VPN接続サーバ（50）は、

前記ユーザ端末（10）との間で通信する通信部（51）と、

前記認証情報管理DB（40）から前記IDと前記トークンとの対を読み出すDB処理部（53）と、

前記ユーザ端末（10）から受信したトークンと、前記IDをキーとして前記認証情報管理DB（40）から読み出したトークンとが一致するか否かを判定するトークン判定部（54）と、

前記ユーザ端末（10）と前記VPN接続サーバ（50）との間でのVPN通信を可能にするVPN接続部（55）と、

前記ユーザ端末（10）から前記IDと前記トークンとを受信すると、前記DB処理部（53）、前記トークン判定部（54）、前記VPN接続部（55）を実行させて、それらの実行の結果を必要に応じて前記ユーザ端末（10）に送信する制御部（52）と、
を備えたことを特徴とするVPN接続認証システム。

[請求項2]

ユーザが用いるユーザ端末と、前記ユーザ端末と通信可能に接続する認証サーバ（20）と、前記認証サーバ（20）に内蔵され又は通信可能に接続する生体認証結果証拠情報検証サーバ（30）と、前記認証サーバ（20）から書き込み可能である認証情報管理DB（40）と、前記ユーザ端末とVPN（Virtual Private network）で通信可能に接続するVPN接続サーバ（50）とを備えて、

前記認証サーバ（20）は、

前記ユーザ端末からのVPN接続要求に対して、前記ユーザ端末に送信するためのチャレンジ値を生成するチャレンジ値生成部（23）と、

前記生体認証結果証拠情報検証サーバ（30）での検証が成功した

場合に、トークンを生成するトークン生成部（２４）と、

前記認証情報管理ＤＢ（４０）へ前記トークンを書き込むＤＢ処理部（２５）と、

前記ユーザ端末又は前記生体認証結果証拠情報検証サーバ（３０）と前記認証サーバ（２０）との間の通信内容に応じた処理を、前記チャレンジ値生成部（２３）、前記トークン生成部（２４）、前記ＤＢ処理部（２５）によって実行させ、これらの実行の結果を必要に応じて前記ＶＰＮ接続サーバ（５０）に送信する制御部（２２）と、
を備え、

前記生体認証結果証拠情報検証サーバ（３０）は、

前記認証サーバ（２０）との間で通信する通信部（３１）と、

前記ユーザ端末によって生成され、前記認証サーバ（２０）を経由して受信する生体認証結果証拠情報を検証して、この検証が成功した場合に、前記検証の結果と生体認証結果証拠情報に含まれるユーザ識別子とを前記認証サーバ（２０）に返却する生体認証結果証拠情報検証部（３２）と、

を備え、

前記認証情報管理ＤＢ（４０）は、

各ユーザに対応して、生体認証処理に係るユーザ識別子、前記ＶＰＮ接続サーバ（５０）を利用するユーザのＩＤ及びトークンを格納し、

前記ＶＰＮ接続サーバ（５０）は、

前記ユーザ端末との間で通信する通信部（５１）と、

前記認証情報管理ＤＢ（４０）から前記ＩＤと前記トークンとの対を読み出すＤＢ処理部（５３）と、

前記ユーザ端末から受信したトークンと、前記ＩＤをキーとして前記認証情報管理ＤＢ（４０）から読み出したトークンとが一致するかどうかを判定するトークン判定部（５４）と、

前記ユーザ端末と前記VPN接続サーバ（５０）との間でのVPN通信を可能にするVPN接続部（５５）と、

前記ユーザ端末から前記IDと前記トークンとを受信すると、前記DB処理部（５３）、前記トークン判定部（５４）、前記VPN接続部（５５）を実行させて、それらの実行の結果を必要に応じて前記ユーザ端末に送信する制御部（５２）と、

を有するVPN接続認証システムに用いられるユーザ端末であって、

前記認証サーバ（２０）及び前記VPN接続サーバ（５０）の間で通信する通信部（１１）と、

前記認証サーバ（２０）へのVPN接続要求を表示する表示部（１３）と、

前記表示部（１３）によって表示されたVPN接続要求を決定するための入力を受け付ける入力部（１４）と、

前記認証サーバ（２０）からのチャレンジ値を受け取り、このチャレンジ値に対応して、前記ユーザの生体認証を実行して生体認証結果証拠情報を生成して前記認証サーバ（２０）へ返却する生体認証処理部（１５）と、

前記認証サーバ（２０）での認証が成功した場合に、前記認証サーバ（２０）から受信するID及びトークンに基づいて、これらID及びトークンが前記VPN接続サーバ（５０）への認証を要求するための形式を有する情報を生成する送信内容生成部（１６）と、

前記認証サーバ（２０）又は前記VPN接続サーバ（５０）との間の通信内容に応じた処理を、前記表示部（１３）、前記入力部（１４）、前記生体認証処理部（１５）、前記送信内容生成部（１６）、前記VPN接続部（１７）によって実行させ、それらの実行の結果を必要に応じて、前記認証サーバ（２０）又は前記VPN接続サーバ（５０）に送信する制御部（１２）と、

を備えたことを特徴とするユーザ端末。

[請求項3]

ユーザが用いるユーザ端末（１０）と、前記ユーザ端末（１０）と通信可能に接続する認証サーバと、前記認証サーバに内蔵され又は通信可能に接続する生体認証結果証拠情報検証サーバ（３０）と、前記認証サーバから書き込み可能である認証情報管理ＤＢ（４０）と、前記ユーザ端末（１０）とＶＰＮ（Virtual Private network）で通信可能に接続するＶＰＮ接続サーバ（５０）とを備えて、

前記ユーザ端末（１０）は、

前記認証サーバ及び前記ＶＰＮ接続サーバ（５０）の間で通信する通信部（１１）と、

前記認証サーバへのＶＰＮ接続要求を表示する表示部（１３）と、

前記表示部（１３）によって表示されたＶＰＮ接続要求を決定するための入力を受け付ける入力部（１４）と、

前記認証サーバからのチャレンジ値を受け取り、このチャレンジ値に対応して、前記ユーザの生体認証を実行して生体認証結果証拠情報を生成して前記認証サーバへ返却する生体認証処理部（１５）と、

前記認証サーバでの認証が成功した場合に、前記認証サーバから受信するＩＤ及びトークンに基づいて、これらＩＤ及びトークンが前記ＶＰＮ接続サーバ（５０）への認証を要求するための形式を有する情報を生成する送信内容生成部（１６）と、

前記認証サーバ又は前記ＶＰＮ接続サーバ（５０）と前記ユーザ端末（１０）との間の通信内容に応じた処理を、前記表示部（１３）、前記入力部（１４）、前記生体認証処理部（１５）、前記送信内容生成部（１６）、前記ＶＰＮ接続部（１７）によって実行させ、それらの実行の結果を必要に応じて、前記認証サーバ又は前記ＶＰＮ接続サーバ（５０）に送信する制御部（１２）と、
を備え、

前記生体認証結果証拠情報検証サーバ（３０）は、

前記認証サーバとの間で通信する通信部（３１）と、

前記ユーザ端末（１０）の前記生体認証処理部（１５）によって生成され、前記認証サーバを経由して受信する生体認証結果証拠情報を検証して、この検証が成功した場合に、前記検証の結果と生体認証結果証拠情報に含まれるユーザ識別子とを前記認証サーバに返却する生体認証結果証拠証拠情報検証部（３２）と、

を備え、

前記認証情報管理ＤＢ（４０）は、

各ユーザに対応して、生体認証処理に係るユーザ識別子、前記ＶＰＮ接続サーバ（５０）を利用するユーザのＩＤ及びトークンを格納し、

前記ＶＰＮ接続サーバ（５０）は、

前記ユーザ端末（１０）との間で通信する通信部（５１）と、

前記認証情報管理ＤＢ（４０）から前記ＩＤと前記トークンとの対を読み出すＤＢ処理部（５３）と、

前記ユーザ端末（１０）から受信したトークンと、前記ＩＤをキーとして前記認証情報管理ＤＢ（４０）から読み出したトークンとが一致するか否かを判定するトークン判定部（５４）と、

前記ユーザ端末（１０）と前記ＶＰＮ接続サーバ（５０）との間で

のＶＰＮ通信を可能にするＶＰＮ接続部（５５）と、

前記ユーザ端末（１０）から前記ＩＤと前記トークンを受信する

と、前記ＤＢ処理部（５３）、前記トークン判定部（５４）、前記ＶＰＮ接続部（５５）を実行させて、それらの実行の結果を必要に応じて

て前記ユーザ端末（１０）に送信する制御部（５２）と、

を有するＶＰＮ接続認証システムに用いられる認証サーバであって、

前記ユーザ端末（１０）及び前記生体認証結果証拠情報検証サーバ（３０）との間で通信する通信部（２１）と、

前記ユーザ端末（１０）からのＶＰＮ接続要求に対して、前記ユーザ端末（１０）に送信するためのチャレンジ値を生成するチャレンジ

値生成部（２３）と、

前記生体認証結果証拠情報検証サーバ（３０）での検証が成功した場合に、前記トークンを生成するトークン生成部（２４）と、

前記認証情報管理ＤＢ（４０）へ前記トークンを書き込むＤＢ処理部（２５）と、

前記ユーザ端末（１０）又は前記生体認証結果証拠情報検証サーバ（３０）との間の通信内容に応じた処理を、前記チャレンジ値生成部（２３）、前記トークン生成部（２４）、前記ＤＢ処理部（２５）によって実行させ、これらの実行の結果を必要に応じて前記ＶＰＮ接続サーバ（５０）に送信する制御部（２２）と、

を備えたことを特徴とする認証サーバ。

[請求項４]

ユーザが用いるユーザ端末（１０）と、前記ユーザ端末（１０）と通信可能に接続する認証サーバ（２０）と、前記認証サーバ（２０）に内蔵され又は通信可能に接続する生体認証結果証拠情報検証サーバと、前記認証サーバ（２０）から書き込み可能である認証情報管理ＤＢ（４０）と、前記ユーザ端末（１０）とＶＰＮ（Virtual Private network）で通信可能に接続するＶＰＮ接続サーバ（５０）とを備えて、

前記ユーザ端末（１０）は、

前記認証サーバ（２０）及び前記ＶＰＮ接続サーバ（５０）の間で通信する通信部（１１）と、

前記認証サーバ（２０）へのＶＰＮ接続要求を表示する表示部（１３）と、

前記表示部（１３）によって表示されたＶＰＮ接続要求を決定するための入力を受け付ける入力部（１４）と、

前記認証サーバ（２０）からのチャレンジ値を受け取り、このチャレンジ値に対応して、前記ユーザの生体認証を実行して生体認証結果証拠情報を生成して前記認証サーバ（２０）へ返却する生体認証処理

部（１５）と、

前記認証サーバ（２０）での認証が成功した場合に、前記認証サーバ（２０）から受信するＩＤ及びトークンに基づいて、これらＩＤ及びトークンが前記ＶＰＮ接続サーバ（５０）への認証を要求するための形式を有する情報を生成する送信内容生成部（１６）と、

前記認証サーバ（２０）又は前記ＶＰＮ接続サーバ（５０）と前記ユーザ端末（１０）との間の通信内容に応じた処理を、前記表示部（１３）、前記入力部（１４）、前記生体認証処理部（１５）、前記送信内容生成部（１６）、前記ＶＰＮ接続部（１７）によって実行させ、それらの実行の結果を必要に応じて、前記認証サーバ（２０）又は前記ＶＰＮ接続サーバ（５０）に送信する制御部（１２）と、
を備え、

前記認証サーバ（２０）は、

前記ユーザ端末（１０）及び前記生体認証結果証拠情報検証サーバとの間で通信する通信部（２１）と、

前記ユーザ端末（１０）からのＶＰＮ接続要求に対して、前記ユーザ端末（１０）に送信するためのチャレンジ値を生成するチャレンジ値生成部（２３）と、

前記生体認証結果証拠情報検証サーバでの検証が成功した場合に、前記トークンを生成するトークン生成部（２４）と、

前記認証情報管理ＤＢ（４０）へ前記トークンを書き込むＤＢ処理部（２５）と、

前記ユーザ端末（１０）又は前記生体認証結果証拠情報検証サーバと前記認証サーバ（２０）との間の通信内容に応じた処理を、前記チャレンジ値生成部（２３）、前記トークン生成部（２４）、前記ＤＢ処理部（２５）によって実行させ、これらの実行の結果を必要に応じて前記認証サーバ（２０）又は前記ＶＰＮ接続サーバ（５０）に送信する制御部（２２）と、

を備え、

前記認証情報管理DB（40）は、

各ユーザに対応して、生体認証処理に係るユーザ識別子、前記VPN接続サーバ（50）を利用するユーザのID及びトークンを格納し、

前記VPN接続サーバ（50）は、

前記ユーザ端末（10）との間で通信する通信部（51）と、

前記認証情報管理DB（40）から前記IDと前記トークンとの対を読み出すDB処理部（53）と、

前記ユーザ端末（10）から受信したトークンと、前記IDをキーとして前記認証情報管理DB（40）から読み出したトークンとが一致するか否かを判定するトークン判定部（54）と、

前記ユーザ端末（10）と前記VPN接続サーバ（50）との間でのVPN通信を可能にするVPN接続部（55）と、

前記ユーザ端末（10）から前記IDと前記トークンとを受信すると、前記DB処理部（53）、前記トークン判定部（54）、前記VPN接続部（55）を実行させて、それらの実行の結果を必要に応じて前記ユーザ端末（10）に送信する制御部（52）と、

を備えたVPN接続認証システムに用いられる生体認証結果証拠情報検証サーバであって、

前記認証サーバ（20）との間で通信する通信部（31）と、

前記ユーザ端末（10）の前記生体認証処理部（15）によって生成され、前記認証サーバ（20）を経由して受信する生体認証結果証拠情報を検証して、この検証が成功した場合に、前記検証の結果と生体認証結果証拠情報に含まれるユーザ識別子とを前記認証サーバ（20）に返却する生体認証結果証拠情報検証部（32）と、

を備えたことを特徴とする生体認証結果証拠情報検証サーバ。

[請求項5]

ユーザが用いるユーザ端末（10）と、前記ユーザ端末（10）と

通信可能に接続する認証サーバ（２０）と、前記認証サーバ（２０）に内蔵され又は通信可能に接続する生体認証結果証拠情報検証サーバ（３０）と、前記認証サーバ（２０）から書き込み可能である認証情報管理ＤＢ（４０）と、前記ユーザ端末（１０）とＶＰＮ（Virtual Private network）で通信可能に接続するＶＰＮ接続サーバとを備えて、

前記ユーザ端末（１０）は、

前記認証サーバ（２０）及び前記ＶＰＮ接続サーバの間で通信する通信部（１１）と、

前記認証サーバ（２０）へのＶＰＮ接続要求を表示する表示部（１３）と、

前記表示部（１３）によって表示されたＶＰＮ接続要求を決定するための入力を受け付ける入力部（１４）と、

前記認証サーバ（２０）からのチャレンジ値を受け取り、このチャレンジ値に対応して、前記ユーザの生体認証を実行して生体認証結果証拠情報を生成して前記認証サーバ（２０）へ返却する生体認証処理部（１５）と、

前記認証サーバ（２０）での認証が成功した場合に、前記認証サーバ（２０）から受信するＩＤ及びトークンに基づいて、これらＩＤ及びトークンが前記ＶＰＮ接続サーバへの認証を要求するための形式を有する情報を生成する送信内容生成部（１６）と、

前記認証サーバ（２０）又は前記ＶＰＮ接続サーバと前記ユーザ端末（１０）との間の通信内容に応じた処理を、前記表示部（１３）、前記入力部（１４）、前記生体認証処理部（１５）、前記送信内容生成部（１６）、前記ＶＰＮ接続部（１７）によって実行させ、それらの実行の結果を必要に応じて、前記認証サーバ（２０）又は前記ＶＰＮ接続サーバに送信する制御部（１２）と、

を備え、

前記認証サーバ（２０）は、

前記ユーザ端末（１０）及び前記生体認証結果証拠情報検証サーバ（３０）との間で通信する通信部（２１）と、

前記ユーザ端末（１０）からのＶＰＮ接続要求に対して、前記ユーザ端末（１０）に送信するためのチャレンジ値を生成するチャレンジ値生成部（２３）と、

前記生体認証結果証拠情報検証サーバ（３０）での検証が成功した場合に、前記トークンを生成するトークン生成部（２４）と、

前記認証情報管理ＤＢ（４０）へ前記トークンを書き込むＤＢ処理部（２５）と、

前記ユーザ端末（１０）又は前記生体認証結果証拠情報検証サーバ（３０）と前記認証サーバ（２０）との間の通信内容に応じた処理を、前記チャレンジ値生成部（２３）、前記トークン生成部（２４）、前記ＤＢ処理部（２５）によって実行させ、これらの実行の結果を必要に応じて前記認証サーバ（２０）又は前記ＶＰＮ接続サーバに送信する制御部（２２）と、

を備え、

前記生体認証結果証拠情報検証サーバ（３０）は、

前記認証サーバ（２０）との間で通信する通信部（３１）と、

前記ユーザ端末（１０）の前記生体認証処理部（１５）によって生成され、前記認証サーバ（２０）を経由して受信する生体認証結果証拠情報を検証して、この検証が成功した場合に、前記検証の結果と生体認証結果証拠情報に含まれるユーザ識別子とを前記認証サーバ（２０）に返却する生体認証結果証拠情報検証部（３２）と、

を備え、

前記認証情報管理ＤＢ（４０）は、

各ユーザに対応して、生体認証処理に係るユーザ識別子、前記ＶＰＮ接続サーバを利用するユーザのＩＤ及びトークンを格納するＶＰＮ

接続認証システムに用いられるVPN接続サーバであって

前記ユーザ端末（１０）との間で通信する通信部（５１）と、

前記認証情報管理DB（４０）から前記IDと前記トークンとの対を読み出すDB処理部（５３）と、

前記ユーザ端末（１０）から受信したトークンと、前記IDをキーとして前記認証情報管理DB（４０）から読み出したトークンとが一致するか否かを判定するトークン判定部（５４）と、

前記ユーザ端末（１０）の間でのVPN通信を可能にするVPN接続部（５５）と、

前記ユーザ端末（１０）から前記IDと前記トークンとを受信すると、前記DB処理部（５３）、前記トークン判定部（５４）、前記VPN接続部（５５）を実行させて、それらの実行の結果を必要に応じて前記ユーザ端末（１０）に送信する制御部（５２）と、
を備えたことを特徴とするVPN接続サーバ。

[請求項6]

ユーザが用いるユーザ端末と、前記ユーザ端末と通信可能に接続する認証サーバ（２０）と、前記認証サーバ（２０）に内蔵され又は通信可能に接続する生体認証結果証拠情報検証サーバ（３０）と、前記認証サーバ（２０）から書き込み可能である認証情報管理DB（４０）と、前記ユーザ端末とVPN（Virtual Private network）で通信可能に接続するVPN接続サーバ（５０）とを備えて、

前記認証サーバ（２０）は、

前記ユーザ端末からのVPN接続要求に対して、前記ユーザ端末に送信するためのチャレンジ値を生成するチャレンジ値生成部（２３）と、

前記生体認証結果証拠情報検証サーバ（３０）での検証が成功した場合に、トークンを生成するトークン生成部（２４）と、

前記認証情報管理DB（４０）へ前記トークンを書き込むDB処理部（２５）と、

前記ユーザ端末又は前記生体認証結果証拠情報検証サーバ（３０）と前記認証サーバ（２０）との間の通信内容に応じた処理を、前記チャレンジ値生成部（２３）、前記トークン生成部（２４）、前記ＤＢ処理部（２５）によって実行させ、これらの実行の結果を必要に応じて前記ＶＰＮ接続サーバ（５０）に送信する制御部（２２）と、を備え、

前記生体認証結果証拠情報検証サーバ（３０）は、

前記認証サーバ（２０）との間で通信する通信部（３１）と、

前記ユーザ端末によって生成され、前記認証サーバ（２０）を経由して受信する生体認証結果証拠情報を検証して、この検証が成功した場合に、前記検証の結果と生体認証結果証拠情報に含まれるユーザ識別子とを前記認証サーバ（２０）に返却する生体認証結果証拠情報検証部（３２）と、

を備え、

前記認証情報管理ＤＢ（４０）は、

各ユーザに対応して、生体認証処理に係るユーザ識別子、前記ＶＰＮ接続サーバ（５０）を利用するユーザのＩＤ及びトークンを格納し、

前記ＶＰＮ接続サーバ（５０）は、

前記ユーザ端末との間で通信する通信部（５１）と、

前記認証情報管理ＤＢ（４０）から前記ＩＤと前記トークンとの対を読み出すＤＢ処理部（５３）と、

前記ユーザ端末から受信したトークンと、前記ＩＤをキーとして前記認証情報管理ＤＢ（４０）から読み出したトークンとが一致するかどうかを判定するトークン判定部（５４）と、

前記ユーザ端末と前記ＶＰＮ接続サーバ（５０）の間でのＶＰＮ通信を可能にするＶＰＮ接続部（５５）と、

前記ユーザ端末から前記ＩＤと前記トークンとを受信すると、前記

DB処理部（５３）、前記トークン判定部（５４）、前記VPN接続部（５５）を実行させて、それらの実行の結果を必要に応じて前記ユーザ端末に送信する制御部（５２）と、

を有するVPN接続認証システムに用いられるユーザ端末としてのコンピュータを、

前記認証サーバ（２０）及び前記VPN接続サーバ（５０）の間で通信する通信部（１１）、

前記認証サーバ（２０）へのVPN接続要求を表示する表示部（１３）、

前記表示部（１３）によって表示されたVPN接続要求を決定するための入力を受け付ける入力部（１４）、

前記認証サーバ（２０）からのチャレンジ値を受け取り、このチャレンジ値に対応して、前記ユーザの生体認証を実行して生体認証結果証拠情報を生成して前記認証サーバ（２０）へ返却する生体認証処理部（１５）、

前記認証サーバ（２０）での認証が成功した場合に、前記認証サーバ（２０）から受信するID及びトークンに基づいて、これらID及びトークンが前記VPN接続サーバ（５０）への認証を要求するための形式を有する情報を生成する送信内容生成部（１６）、

前記認証サーバ（２０）又は前記VPN接続サーバ（５０）との間の通信内容に応じた処理を、前記表示部（１３）、前記入力部（１４）、前記生体認証処理部（１５）、前記送信内容生成部（１６）、前記VPN接続部（１７）によって実行させ、それらの実行の結果を必要に応じて、前記認証サーバ（２０）又は前記VPN接続サーバ（５０）に送信する制御部（１２）

として機能させるためのプログラム。

[請求項7]

ユーザが用いるユーザ端末（１０）と、前記ユーザ端末（１０）と通信可能に接続する認証サーバ（２０）と、前記認証サーバ（２０）

に内蔵され又は通信可能に接続する生体認証結果証拠情報検証サーバと、前記認証サーバ（２０）から書き込み可能である認証情報管理ＤＢ（４０）と、前記ユーザ端末（１０）とＶＰＮ（Virtual Private network）で通信可能に接続するＶＰＮ接続サーバ（５０）とを備えて、

前記ユーザ端末（１０）は、

前記認証サーバ（２０）及び前記ＶＰＮ接続サーバ（５０）の間で通信する通信部（１１）と、

前記認証サーバ（２０）へのＶＰＮ接続要求を表示する表示部（１３）と、

前記表示部（１３）によって表示されたＶＰＮ接続要求を決定するための入力を受け付ける入力部（１４）と、

前記認証サーバ（２０）からのチャレンジ値を受け取り、このチャレンジ値に対応して、前記ユーザの生体認証を実行して生体認証結果証拠情報を生成して前記認証サーバ（２０）へ返却する生体認証処理部（１５）と、

前記認証サーバ（２０）での認証が成功した場合に、前記認証サーバ（２０）から受信するＩＤ及びトークンに基づいて、これらＩＤ及びトークンが前記ＶＰＮ接続サーバ（５０）への認証を要求するための形式を有する情報を生成する送信内容生成部（１６）と、

前記認証サーバ（２０）又は前記ＶＰＮ接続サーバ（５０）と前記ユーザ端末（１０）との間の通信内容に応じた処理を、前記表示部（１３）、前記入力部（１４）、前記生体認証処理部（１５）、前記送信内容生成部（１６）、前記ＶＰＮ接続部（１７）によって実行させ、それらの実行の結果を必要に応じて、前記認証サーバ（２０）又は前記ＶＰＮ接続サーバ（５０）に送信する制御部（１２）と、を備え、

前記認証サーバ（２０）は、

前記ユーザ端末（１０）及び前記生体認証結果証拠情報検証サーバとの間で通信する通信部（２１）と、

前記ユーザ端末（１０）からのＶＰＮ接続要求に対して、前記ユーザ端末（１０）に送信するためのチャレンジ値を生成するチャレンジ値生成部（２３）と、

前記生体認証結果証拠情報検証サーバでの検証が成功した場合に、前記トークンを生成するトークン生成部（２４）と、

前記認証情報管理ＤＢ（４０）へ前記トークンを書き込むＤＢ処理部（２５）と、

前記ユーザ端末（１０）又は前記生体認証結果証拠情報検証サーバと前記認証サーバ（２０）との間の通信内容に応じた処理を、前記チャレンジ値生成部（２３）、前記トークン生成部（２４）、前記ＤＢ処理部（２５）によって実行させ、これらの実行の結果を必要に応じて前記認証サーバ（２０）又は前記ＶＰＮ接続サーバ（５０）に送信する制御部（２２）と、

を備え、

前記認証情報管理ＤＢ（４０）は、

各ユーザに対応して、生体認証処理に係るユーザ識別子、前記ＶＰＮ接続サーバ（５０）を利用するユーザのＩＤ及びトークンを格納し、

前記ＶＰＮ接続サーバ（５０）は、

前記ユーザ端末（１０）との間で通信する通信部（５１）と、

前記認証情報管理ＤＢ（４０）から前記ＩＤと前記トークンとの対を読み出すＤＢ処理部（５３）と、

前記ユーザ端末（１０）から受信したトークンと、前記ＩＤをキーとして前記認証情報管理ＤＢ（４０）から読み出したトークンとが一致するか否かを判定するトークン判定部（５４）と、

前記ユーザ端末（１０）と前記ＶＰＮ接続サーバ（５０）との間で

のVPN通信を可能にするVPN接続部（55）と、

前記ユーザ端末（10）から前記IDと前記トークンとを受信すると、前記DB処理部（53）、前記トークン判定部（54）、前記VPN接続部（55）を実行させて、それらの実行の結果を必要に応じて前記ユーザ端末（10）に送信する制御部（52）と、

を備えたVPN接続認証システムに用いられる生体認証結果証拠情報検証サーバとしてのコンピュータを、

前記認証サーバ（20）との間で通信する通信部（31）、

前記ユーザ端末（10）の前記生体認証処理部（15）によって生成され、前記認証サーバ（20）を経由して受信する生体認証結果証拠情報を検証して、この検証が成功した場合に、前記検証の結果と生体認証結果証拠情報に含まれるユーザ識別子とを前記認証サーバ（20）に返却する生体認証結果証拠情報検証部（32）

として機能させるためのプログラム。