(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2008-293399
(P2008-293399A)
(43)公開日　平成20年12月4日(2008.12.4)

(51)Int.Cl.		F I		テーマコード（参考）
G06F 21/20	(2006.01)	G06F 15/00	330C	5B285

審査請求 未請求　請求項の数 15　ＯＬ　（全 19 頁）

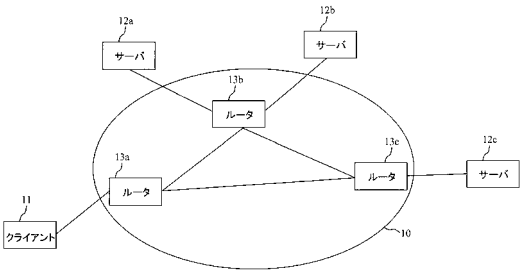
(21)出願番号　特願2007-140088 (P2007-140088)
(22)出願日　平成19年5月28日 (2007.5.28)

(71)出願人　899000057
学校法人日本大学
東京都千代田区九段南四丁目８番２４号
(71)出願人　899000079
学校法人慶應義塾
東京都港区三田２丁目１５番４５号
(74)代理人　100119677
弁理士　岡田　賢治
(74)代理人　100115794
弁理士　今下　勝博
(72)発明者　木原　雅巳
東京都千代田区九段南四丁目８番２４号
学校法人日本大学内

最終頁に続く

(54)【発明の名称】端末認証システム及び端末認証方法及びプログラム及び記録媒体

(57)【要約】
【課題】本発明は、特別な認証情報を用いずに短時間で正規ユーザを認証することを目的とする。
【解決手段】本発明は、通信ネットワーク１０上の仮想地図を形成し、サーバ１２ａ、１２ｂ、１２ｃ側又はクライアント１１側からの接続要求コマンドの伝搬時間を測定することで、アクセスの要求やサービスの要求をしてきたクライアント１１に対して予め登録されているクライアント１１かどうかを認証することを特徴とする。さらに、複数のサーバ１２ａ、１２ｂ、１２ｃとクライアント１１との間の仮想の距離によって仮想地図上の位置を特定し、予め特定した位置からのクライアント１１かどうかを認証することを特徴とする。
【選択図】図１



【特許請求の範囲】
【請求項１】
クロック周波数の同期がとれたサーバ及びクライアントが通信ネットワークで接続されている端末認証システムであって、
前記サーバは、
前記クライアントと前記サーバとの間の転送遅延時間を予め記憶している認証情報記憶手段と、
前記クライアントと前記サーバとの間の転送遅延時間を取得する転送遅延時間取得手段と、
前記転送遅延時間取得手段の取得した転送遅延時間を、前記認証情報記憶手段に記憶されている転送遅延時間と照合する認証情報照合手段と、
を備えることを特徴とする端末認証システム。
【請求項２】
前記サーバは、それぞれ、前記転送遅延時間を予め定められたタイミングで取得し、前記認証情報記憶手段に記憶されている転送遅延時間を、取得した転送遅延時間に更新する認証情報更新手段をさらに備えることを特徴とする請求項１に記載の端末認証システム。
【請求項３】
前記転送遅延時間取得手段は、前記転送遅延時間を複数回取得し、
前記認証情報照合手段は、前記転送遅延時間取得手段の取得する転送遅延時間の平均値を算出し、当該平均値を、前記認証情報記憶手段に記憶されている転送遅延時間と照合することを特徴とする請求項１又は２に記載の端末認証システム。
【請求項４】
前記認証情報照合手段は、さらに、前記転送遅延時間取得手段の取得する転送遅延時間の分散を算出し、前記平均値を中心とする当該分散の範囲を、前記認証情報記憶手段に記憶されている転送遅延時間と照合することを特徴とする請求項３に記載の端末認証システム。
【請求項５】
クロック周波数の同期がとれた２以上のサーバ及びクライアントが通信ネットワークで接続されている端末認証システムであって、
前記サーバは、それぞれ、
前記クライアントと前記サーバとの間の転送遅延時間を取得する転送遅延時間取得手段と、
前記転送遅延時間取得手段の取得した転送遅延時間を、前記サーバのうちの予め定められた認証用サーバへ送信する認証情報送信手段と、を備え、
前記認証用サーバは、さらに、
前記認証情報送信手段の送信する転送遅延時間を受信する転送遅延時間受信手段と、
前記通信ネットワーク内に接続されている前記サーバ及び前記クライアントの通信ネットワーク上の仮想位置を、前記サーバごとに記憶する認証情報記憶手段と、
前記転送遅延時間受信手段の受信した転送遅延時間を、前記サーバごとに蓄積する認証情報蓄積手段と、
前記認証情報蓄積手段の蓄積した転送遅延時間が２つ以上になった場合に、前記認証情報記憶手段を参照して前記認証情報蓄積手段の蓄積しているサーバの位置を抽出し、抽出した位置と転送遅延時間とから、前記認証情報蓄積手段の蓄積しているクライアントの位置を算出し、前記認証情報記憶手段に記憶されている位置と照合する認証情報照合手段と、
を備えることを特徴とする端末認証システム。
【請求項６】
前記サーバは、それぞれ、さらに、
前記転送遅延時間を予め定められたタイミングで取得する最新転送遅延時間取得手段と、

前記最新転送遅延時間取得手段の取得した転送遅延時間を前記認証用サーバへ送信する最新転送遅延時間送信手段と、を備え、
前記認証用サーバは、さらに、
前記最新転送遅延時間送信手段の送信した転送遅延時間と、前記認証情報記憶手段に記憶されている前記サーバの位置を用いて、前記クライアントの位置を算出し、前記認証情報記憶手段に記憶されている前記クライアントの位置を、算出したクライアントの位置に更新する認証情報更新手段を備えることを特徴とする請求項５に記載の端末認証システム。
【請求項７】
前記転送遅延時間取得手段は、前記転送遅延時間を複数回取得し、取得した転送遅延時間の平均値を算出し、
前記認証情報送信手段は、前記転送遅延時間取得手段の算出する平均値を、前記転送遅延時間として前記サーバのうちの予め定められた認証用サーバへ送信することを特徴とする請求項５又は６に記載の端末認証システム。
【請求項８】
前記転送遅延時間取得手段は、前記クライアントの時刻を送信する指示を前記クライアントに送信し、前記クライアントから受信する前記クライアントの時刻と前記サーバの時刻との時間差を測定し、当該時間差を前記クライアントから前記サーバまでの転送遅延時間として取得し、
前記クライアントは、前記クライアントの時刻を送信する指示を前記転送遅延時間取得手段から受信すると、当該転送遅延時間取得手段へ前記クライアントの時刻を送信するクライアント応答信号送信手段を備えることを特徴とする請求項１から７のいずれかに記載の端末認証システム。
【請求項９】
前記転送遅延時間取得手段は、前記サーバの時刻を送信する指示を前記クライアントから受信すると、前記クライアントに前記サーバの時刻を送信し、前記クライアントの受信した前記サーバの時刻と前記クライアントの時刻との時間差を前記クライアントに送信させ、当該時間差から前記サーバから前記クライアントまでの転送遅延時間として取得し、
前記クライアントは、
前記サーバの時刻を送信する指示を前記サーバに送信するクライアント測定指示送信手段と、
前記サーバから前記サーバの時刻を受信し、前記サーバの時刻と前記クライアントの時刻との時間差を測定し、当該時間差を前記サーバへ送信するクライアント認証情報送信手段と、
を備えることを特徴とする請求項１から７のいずれかに記載の端末認証システム。
【請求項１０】
前記サーバと前記クライアントとの間にはＴＣＰレイヤでの通信が行われ、肯定応答信号（ＡＣＫ）に、ＴＣＰレイヤのタイムスタンプを含むことを特徴とする請求項８又は９に記載の端末認証システム。
【請求項１１】
前記サーバ及び前記クライアントは時刻の同期がとれていることを特徴とする請求項１から１０のいずれかに記載の端末認証システム。
【請求項１２】
クロック周波数の同期がとれたサーバ及びクライアントが通信ネットワークで接続されている端末認証システムに用いられる端末認証方法であって、
前記サーバが、前記サーバと前記クライアントとの間の転送遅延時間を取得する転送遅延時間取得ステップと、
それぞれの前記サーバが、前記転送遅延時間取得ステップで取得した転送遅延時間を、前記サーバとクライアントとの間の転送遅延時間が予め記憶されている認証情報記憶手段に記憶されている転送遅延時間と照合する認証情報照合ステップと、

を順に有することを特徴とする端末認証方法。
【請求項１３】
クロック周波数の同期がとれた２以上のサーバ及びクライアントが通信ネットワークで接続されている端末認証システムに用いられる端末認証方法であって、
前記サーバのうちの予め定められた認証用サーバが、それぞれの前記サーバによって取得された前記サーバと前記クライアントとの間の転送遅延時間を受信する転送遅延時間受信ステップと、
前記転送遅延時間受信ステップで受信した転送遅延時間を、前記認証情報送信手段を備える前記サーバごとに蓄積する認証情報蓄積ステップと、
前記認証情報蓄積手段の蓄積した転送遅延時間が２つ以上になった場合に、前記通信ネットワーク内に接続されている前記サーバ及び前記クライアントの通信ネットワーク上の仮想位置が前記サーバごとに記憶されている認証情報記憶手段を参照して前記認証情報蓄積ステップで蓄積したサーバごとに位置を抽出し、抽出した位置と転送遅延時間とから、前記認証情報蓄積手段の蓄積しているクライアントの位置を算出し、前記認証情報記憶手段に記憶されている位置と照合する認証情報照合ステップと、
を順に有することを特徴とする端末認証方法。
【請求項１４】
請求項１２又は１３に記載の端末認証方法をコンピュータに実行させるための端末認証プログラム。
【請求項１５】
請求項１４に記載の端末認証プログラムを記録したコンピュータ読出可能な記憶媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、サーバとクライアントとを備える通信ネットワークの認証方式に関し、特に、端末認証システム及び端末認証方法及びプログラム及び記録媒体に関する。
【背景技術】
【０００２】
映像、静止画、音楽などのコンテンツを、通信ネットワーク経由で配信するサービスにおいて、コンテンツの配信を希望する個人もしくは端末が、正規の利用者であるかどうかを確認する技術が提案されている（例えば、特許文献１乃至３参照。）。
【０００３】
アクセスされる側の端末にユーザの位置情報を蓄積しておき、ユーザが衛星測位システムによって取得した位置情報を、アクセスされる側の端末が照合することで、認証を行っていた。この方法では、正確な位置の取得には、複数の衛星からの電波信号を受信することが必須である。屋外の受信でも、都心の高層ビルの陰などでは受信が妨げられ、位置精度が落ちる。さらに地下や屋内では、電波受信が完全に途絶え、位置情報が得られない場合があった。
【特許文献１】特開２００７－４２４３号公報
【特許文献２】特開２００６－１０８８３４号公報
【特許文献３】特開２００６－２５２０１６号公報
【発明の開示】
【発明が解決しようとする課題】
【０００４】
上記のように、従来は、ユーザを特定する認証情報を、衛星などの外部から取得して、認証情報を送受信する必要があるため、認証を受けるまでに時間を要し、さらに、認証情報を取得できないために正規ユーザであっても認証が受けられない場合があった。
【０００５】
本発明は、特別な認証情報を用いずに短時間で正規ユーザを認証することを目的とする。

【課題を解決するための手段】
【０００６】
本発明は、上記目的を達成するため、クライアントとサーバとの間の通信ネットワーク上の時間的な位置関係を利用して正規ユーザを認証することを特徴とする。クライアントとサーバとの間で通信を行う際に必ず発生する転送遅延時間を利用するので、特別な認証情報を用いずに短時間で正規ユーザを認証することができる。
【０００７】
具体的には、本発明に係る端末認証システムは、クロック周波数の同期がとれたサーバ及びクライアントが通信ネットワークで接続されている端末認証システムであって、前記サーバは、前記クライアントと前記サーバとの間の転送遅延時間を予め記憶している認証情報記憶手段と、前記クライアントと前記サーバとの間の転送遅延時間を取得する転送遅延時間取得手段と、前記転送遅延時間取得手段の取得した転送遅延時間を、前記認証情報記憶手段に記憶されている転送遅延時間と照合する認証情報照合手段と、を備える。
【０００８】
サーバとクライアントとの間の転送遅延時間を認証情報に利用するので、特別な認証情報を用いずに短時間で正規ユーザを認証することができる。さらに、サーバが同一のクライアントまでの転送遅延時間を取得するので、認証の確度を高めることができる。
【０００９】
クロック周波数の同期がとれているとは、サーバ又はクライアントの有するクロックのカウントする周波数が同期していることをいう。この結果、クロック周波数の同期がとれているサーバ又はクライアントは同じ周期でクロックが刻まれることになる。
時刻の同期がとれているとは、サーバ又はクライアントの有するクロックの絶対時刻が一致していることをいう。この結果、時刻の同期がとれたサーバ又はクライアントは同じ時刻を刻むことになる。
【００１０】
本発明に係る端末認証システムでは、前記サーバは、それぞれ、前記転送遅延時間を予め定められたタイミングで取得し、前記認証情報記憶手段に記憶されている転送遅延時間を、取得した転送遅延時間に更新する認証情報更新手段をさらに備えることが好ましい。認証情報照合手段の照合先を最新の情報に更新することで、第三者のなりすましを防ぐことができる。
【００１１】
本発明に係る端末認証システムでは、前記転送遅延時間取得手段は、前記転送遅延時間を複数回取得し、
前記認証情報照合手段は、前記転送遅延時間取得手段の取得する転送遅延時間の平均値を算出し、当該平均値を、前記認証情報記憶手段に記憶されている転送遅延時間と照合することが好ましい。往復転送遅延時間の平均値を算出することで、登録時のルートとは異なったルートでクライアントとサーバの間のコネクションが確立された場合でも、登録されたクライアントであることを判定することができる。
【００１２】
本発明に係る端末認証システムでは、前記認証情報照合手段は、さらに、前記転送遅延時間取得手段の取得する転送遅延時間の分散を算出し、前記平均値を中心とする当該分散の範囲を、前記認証情報記憶手段に記憶されている転送遅延時間と照合することが好ましい。認証の確度を高めることができる。
【００１３】
具体的には、本発明に係る端末認証システムは、クロック周波数の同期がとれた２以上のサーバ及びクライアントが通信ネットワークで接続されている端末認証システムであって、前記サーバは、それぞれ、前記クライアントと前記サーバとの間の転送遅延時間を取得する転送遅延時間取得手段と、前記転送遅延時間取得手段の取得した転送遅延時間を、前記サーバのうちの予め定められた認証用サーバへ送信する認証情報送信手段と、を備え、前記認証用サーバは、さらに、前記認証情報送信手段の送信する転送遅延時間を受信す

る転送遅延時間受信手段と、前記通信ネットワーク内に接続されている前記サーバ及び前記クライアントの通信ネットワーク上の仮想位置を、前記サーバごとに記憶する認証情報記憶手段と、前記転送遅延時間受信手段の受信した転送遅延時間を、前記サーバごとに蓄積する認証情報蓄積手段と、前記認証情報蓄積手段の蓄積した転送遅延時間が２つ以上になった場合に、前記認証情報記憶手段を参照して前記認証情報蓄積手段の蓄積しているサーバの位置を抽出し、抽出した位置と転送遅延時間とから、前記認証情報蓄積手段の蓄積しているクライアントの位置を算出し、前記認証情報記憶手段に記憶されている位置と照合する認証情報照合手段と、を備える。

【００１４】

通信ネットワーク上の仮想的な位置を利用している。サーバの位置と転送遅延時間によって、通信ネットワーク上の仮想的な位置を特定することができる。転送遅延時間を取得しておき、認証情報記憶手段にこの位置を予め記憶させておくことで、認証情報照合手段はクライアントの通信ネットワーク上の仮想的な位置を特定し、予め登録されているクライアントか否かを判定することができる。このように、通信ネットワーク上に形成される仮想的な地図上にマッピングされたクライアントの位置を認証情報として利用するので、特別な認証情報を用いずに短時間で正規ユーザを認証することができる。

【００１５】

本発明に係る端末認証システムでは、前記サーバは、それぞれ、さらに、前記転送遅延時間を予め定められたタイミングで取得する最新転送遅延時間取得手段と、前記最新転送遅延時間取得手段の取得した転送遅延時間を前記認証用サーバへ送信する最新転送遅延時間送信手段と、を備え、前記認証用サーバは、さらに、前記最新転送遅延時間送信手段の送信した転送遅延時間と、前記認証情報記憶手段に記憶されている前記サーバの位置を用いて、前記クライアントの位置を算出し、前記認証情報記憶手段に記憶されている前記クライアントの位置を、算出したクライアントの位置に更新する認証情報更新手段を備えることが好ましい。認証情報照合手段の照合先を最新の情報に更新することで、第三者のなりすましを防ぐことができる。

【００１６】

本発明に係る端末認証システムでは、前記転送遅延時間取得手段は、前記転送遅延時間を複数回取得し、取得した転送遅延時間の平均値を算出し、前記認証情報送信手段は、前記転送遅延時間取得手段の算出する平均値を、前記転送遅延時間として前記サーバのうちの予め定められた認証用サーバへ送信することが好ましい。転送遅延時間の平均値を算出することで、登録時のルートとは異なったルートでクライアントとサーバの間のコネクションが確立された場合でも、登録されたクライアントであることを判定することができる。

【００１７】

本発明に係る端末認証システムでは、前記転送遅延時間取得手段は、前記クライアントの時刻を送信する指示を前記クライアントに送信し、前記クライアントから受信する前記クライアントの時刻と前記サーバの時刻との時間差を測定し、当該時間差を前記クライアントから前記サーバまでの転送遅延時間として取得し、前記クライアントは、前記クライアントの時刻を送信する指示を前記転送遅延時間取得手段から受信すると、当該転送遅延時間取得手段へ前記クライアントの時刻を送信するクライアント応答信号送信手段を備えることが好ましい。クライアントとサーバとの間ではクロック周波数の同期がとれているので、転送遅延時間の測定値の再現性がよい。

【００１８】

本発明に係る端末認証システムでは、前記転送遅延時間取得手段は、前記サーバの時刻を送信する指示を前記クライアントから受信すると、前記クライアントに前記サーバの時刻を送信し、前記クライアントの受信した前記サーバの時刻と前記クライアントの時刻との時間差を前記クライアントに送信させ、当該時間差から前記サーバから前記クライアントまでの転送遅延時間として取得し、前記クライアントは、前記サーバの時刻を送信する指示を前記サーバに送信するクライアント測定指示送信手段と、前記サーバから前記サー

バの時刻を受信し、前記サーバの時刻と前記クライアントの時刻との時間差を測定し、当該時間差を前記サーバへ送信するクライアント認証情報送信手段と、を備えることが好ましい。クライアントとサーバとの間ではクロック周波数の同期がとれているので、転送遅延時間の測定値の再現性がよい。

【００１９】

本発明に係る端末認証システムでは、前記サーバと前記クライアントとの間にはＴＣＰレイヤでの通信が行われ、肯定応答信号（ＡＣＫ）に、ＴＣＰレイヤのタイムスタンプを含むことが好ましい。ＴＣＰレイヤのタイムスタンプを用いることで、ＴＣＰコネクションの確立時に、転送遅延時間を測定することができる。

【００２０】

本発明に係る端末認証システムでは、前記サーバ及び前記クライアントは時刻の同期がとれていることが好ましい。時刻の同期がとれていると、絶対時刻での転送遅延時間が保証される。

【００２１】

本発明に係る端末認証方法は、クロック周波数の同期がとれたサーバ及びクライアントが通信ネットワークで接続されている端末認証システムに用いられる端末認証方法であって、前記サーバが、前記サーバと前記クライアントとの間の転送遅延時間を取得する転送遅延時間取得ステップと、それぞれの前記サーバが、前記転送遅延時間取得ステップで取得した転送遅延時間を、前記サーバとクライアントとの間の転送遅延時間が予め記憶されている認証情報記憶手段に記憶されている転送遅延時間と照合する認証情報照合ステップと、を順に有する。

【００２２】

サーバとクライアントとの間の転送遅延時間を認証情報に利用しているので、特別な認証情報を用いずに短時間で正規ユーザを認証することができる。さらに、サーバが同一のクライアントまでの転送遅延時間を取得するので、認証の確度を高めることができる。

【００２３】

本発明に係る端末認証方法は、クロック周波数の同期がとれた２以上のサーバ及びクライアントが通信ネットワークで接続されている端末認証システムに用いられる端末認証方法であって、前記サーバのうちの予め定められた認証用サーバが、それぞれの前記サーバによって取得された前記サーバと前記クライアントとの間の転送遅延時間を受信する転送遅延時間受信ステップと、前記転送遅延時間受信ステップで受信した転送遅延時間を、前記認証情報送信手段を備える前記サーバごとに蓄積する認証情報蓄積ステップと、前記認証情報蓄積手段の蓄積した転送遅延時間が２つ以上になった場合に、前記通信ネットワーク内に接続されている前記サーバ及び前記クライアントの通信ネットワーク上の仮想位置が前記サーバごとに記憶されている認証情報記憶手段を参照して前記認証情報蓄積ステップで蓄積したサーバごとに位置を抽出し、抽出した位置と転送遅延時間とから、前記認証情報蓄積手段の蓄積しているクライアントの位置を算出し、前記認証情報記憶手段に記憶されている位置と照合する認証情報照合ステップと、を順に有する。

【００２４】

通信ネットワーク上の仮想的な位置を利用している。サーバの位置と転送遅延時間によって、通信ネットワーク上の仮想的な位置を特定することができる。転送遅延時間を取得しておき、認証情報記憶手段にこの位置を予め記憶させておくことで、認証情報照合手段はクライアントの通信ネットワーク上の仮想的な位置を特定し、予め登録されているクライアントか否かを判定することができる。このように、通信ネットワーク上に形成される仮想的な地図上にマッピングされたクライアントの位置を認証情報として利用するので、特別な認証情報を用いずに短時間で正規ユーザを認証することができる。

【００２５】

本発明に係る端末認証プログラムは、本発明に係る端末認証方法をコンピュータに実行させるための端末認証プログラムである。端末認証プログラムをコンピュータに実行させることで、特別な認証情報を用いずに短時間で正規ユーザを認証することができる。

【００２６】
本発明に係る記憶媒体は、本発明に係る端末認証プログラムを記録したコンピュータ読出可能な記憶媒体である。端末認証プログラムをコンピュータに読み取らせ、コンピュータに実行させることで、特別な認証情報を用いずに短時間で正規ユーザを認証することができる。
【発明の効果】
【００２７】
本発明は、サーバ及びクライアント間の通信ネットワークが確保できれば、どこからでもクライアントの認証を行うことができるので、特別な認証情報を用いずに短時間で正規ユーザを認証することができる。
【発明を実施するための最良の形態】
【００２８】
添付の図面を参照して本発明の実施の形態を説明する。以下に説明する実施の形態は本発明の構成の例であり、本発明は、以下の実施の形態に制限されるものではない。
（実施形態１）
図１は、実施形態１に係る端末認証システムの概略構成図である。図１に示す端末認証システムは、サーバ１２ａ、１２ｂ、１２ｃがクライアント１１と通信ネットワーク１０で接続されている。本実施形態では、クライアント１１のみを示したが、クライアントの数はこれに限らない。例えば２以上であってもよい。また、サーバ１２ａ、１２ｂ、１２ｃは、本実施形態では３台のみを示したが、２台以下であってもよいし、４台以上であってもよい。
【００２９】
通信ネットワーク１０は、クライアント１１と複数のサーバ１２ａ、１２ｂ、１２ｃとを接続する通信網である。通信ネットワーク１０は、広域網又は構内網のいずれであってもよいし、有線又は無線のいずれを用いていてもよいし、公衆回線又は専用回線のいずれを用いていてもよい。本実施形態では、通信ネットワーク１０の一例として、通信ネットワーク１０を構成する一部のルータ１３ａ、１３ｂ、１３ｃのみを示して他を省略した。
【００３０】
ルータ１３ａ、１３ｂ、１３ｃは、クライアント１１の送信する情報をサーバ１２ａ、１２ｂ又は１２ｃへ転送する。例えば、クライアント１１とサーバ１２ａとが送受信する際に、ルータ１３ａ及びルータ１３ｂが情報を転送する。
【００３１】
クライアント１１は、通信ネットワーク１０を介してサーバ１２ａから情報を取得する端末である。クライアント１１は、サーバ１２ａ、１２ｂ及び１２ｃからの情報の提供が許可されており、サーバ１２ａ、１２ｂ及び１２ｃへの登録が完了している端末である。クライアント１１は、固定端末又は無線端末のいずれであってもよい。
【００３２】
サーバ１２ａ、１２ｂ、１２ｃは、クライアント１１との間の認証情報を記憶しており、認証情報との照合が成立すると、クライアント１１へサービスを提供する。本実施形態では、サーバ１２ａ、１２ｂ及び１２ｃのいずれもクライアント１１を照合する機能を有しているが、一例として、サーバ１２ａが、クライアント１１を認証する場合について説明する。
【００３３】
図２は、サーバの機能の一例を示す概略構成図である。サーバ１２ａは、認証情報記憶手段２１と、転送遅延時間取得手段２２と、認証情報照合手段２３と、を備える。サーバ１２ａは、さらに、認証情報更新手段３４を備えることが好ましい。なお、図２では、サーバ１２ａとクライアント１１とを接続する通信ネットワーク（図１の符号１０）は省略した。
【００３４】
また、本実施形態に係る端末認証方法は、本実施形態に係る端末認証システムに用いら

れる端末認証方法であって、転送遅延時間取得手段２２として機能させるための転送遅延時間取得ステップと、認証情報照合手段２３として機能させるための認証情報照合ステップと、を順に有する。端末認証方法において、さらに、認証情報更新手段３４として機能させるための最新転送遅延時間更新ステップを、転送遅延時間取得ステップの前にさらに有することが好ましい。また、本実施形態に係る端末認証プログラムは、本実施形態に係る端末認証方法をコンピュータに実行させるための端末認証プログラムである。端末認証プログラムは、コンピュータ読出可能な記憶媒体に記録されていてもよい。

【００３５】

認証情報記憶手段２１は、サーバ１２ａとクライアント１１との間の転送遅延時間が予め記憶されている。クライアント１１への情報提供サービスを開始する際に、サーバ１２ａはクライアント１１との間の転送遅延時間を取得して認証情報記憶手段２１に記憶する。本実施形態ではクライアント１１が１つだが、２以上の場合は、認証情報記憶手段２１は、各クライアント１１との間の転送遅延時間を記憶しておく。また、サーバ１２ａがさらに認証情報更新手段３４を備える場合は、認証情報記憶手段２１の記憶する転送遅延時間は最新の情報に更新される。

【００３６】

転送遅延時間取得手段２２は、認証情報更新手段３４と同じルートを介してクライアント１１との間の転送遅延時間を取得する。例えば、クライアント１１からサーバ１２ａへアクセスがあると、転送遅延時間取得手段２２はクライアント１１との間の転送遅延時間を取得する。ここで、転送遅延時間は、サーバ１２ａが取得した時間又はクライアント１１が取得した時間である。クライアント１１からサーバ１２ａへのコネクション設定時に転送遅延時間取得手段２２が転送遅延時間を取得する。

【００３７】

さらに、転送遅延時間取得手段２２は、クライアント１１との間の転送遅延時間を複数回取得することが好ましい。さらに、転送遅延時間取得手段２２は、取得した転送遅延時間の平均値を算出することが好ましい。転送遅延時間の平均値を算出することで、登録時のルートとは異なったルートでクライアント１１とサーバとの間のコネクションが確立された場合でも、認証情報照合手段２３は、登録されたクライアント１１であることを判定することができる。

【００３８】

図３は、転送遅延時間の測定方法の第１例を示すシーケンス図である。転送遅延時間の測定方法の第１例では、クライアント１１はクライアント応答信号送信手段を備える。通常のＴＣＰコネクション確立における３ウェイハンドシェークの一例について説明する。クライアント１１がＳＹＮ（接続要求）をサーバ１２ａに送信する。

【００３９】

サーバ１２ａの転送遅延時間取得手段は、クライアント１１からＳＹＮを受信すると、クライアント１１の時刻を送信する指示をクライアント１１に送信する。クライアント１１の時刻を送信する指示は、例えば、クライアント１１からのＳＹＮに対するＡＣＫ（肯定応答）でもよい。この場合、サーバ１２ａの転送遅延時間取得手段は、クライアント１１からのＳＹＮに対するＡＣＫ（肯定応答）と、サーバ１２ａからのＳＹＮをクライアント１１に送信する。

【００４０】

クライアント１１のクライアント応答信号送信手段は、サーバ１２ａの転送遅延時間取得手段からクライアント１１の時刻を送信する指示を受信すると、サーバ１２ａの転送遅延時間取得手段へクライアント１１の時刻を送信する。あるいは、クライアント１１のクライアント応答信号送信手段は、サーバ１２ａからのＡＣＫを受信し、サーバ１２ａからのＳＹＮに対するＡＣＫとクライアント１１の時刻をサーバ１２ａの転送遅延時間取得手段に送信する。

【００４１】

サーバ１２ａの転送遅延時間取得手段は、クライアント１１からのＡＣＫとクライアン

ト１１の時刻を受信する。そして、クライアント１１の時刻とサーバ１２ａの時刻との時間差を測定して転送遅延時間として取得する。クライアント１１とサーバ１２ａとの間で時刻同期がとれていなくても、クライアント１１とサーバ１２ａはクロック周波数の同期がとれているので、転送遅延時間は再現性よく取得することができる。クライアント１１とサーバ１２ａとの間で時刻同期がとれていれば、サーバ１２ａで測定しても、クライアント１１で測定しても、同じ転送遅延時間が保証されることになる。

【００４２】

図４は、転送遅延時間の測定方法の第２例を示すシーケンス図である。転送遅延時間の測定方法の第２例では、クライアント１１はクライアント測定指示送信手段と、クライアント認証情報送信手段と、を備える。転送遅延時間の測定方法の第２例では、時刻情報を含むＴＣＰコネクション確立における３ウェイハンドシェークの一例を示す。

【００４３】

クライアント１１のクライアント測定指示送信手段は、サーバの時刻を送信する指示をサーバに送信する。例えば、クライアント１１がＳＹＮとサーバの時刻を送信する指示をサーバに送信してもよいし、ＳＹＮをサーバの時刻を送信する指示として利用してもよい。

【００４４】

サーバ１２ａの転送遅延時間取得手段は、サーバの時刻を送信する指示をクライアント測定指示送信手段から受信すると、クライアント測定指示送信手段へサーバ１２ａの時刻を送信する。あるいは、サーバ１２ａは、クライアント１１からのＳＹＮに対するＡＣＫと、サーバ１２ａからのＳＹＮと、サーバ１２ａの時刻と、をクライアント１１に送信する。

【００４５】

クライアント１１のクライアント認証情報送信手段は、サーバ１２ａからサーバの時刻を受信し、クライアント測定指示送信手段がサーバ１２ａの時刻とクライアント１１の時刻との時間差を測定して、測定した時間差をサーバへ送信する。あるいは、クライアント１１は、サーバ１２ａからのＡＣＫ、ＳＹＮ及びサーバ１２ａの時刻を受信する。クライアント１１は、ＡＣＫを受信することで、クライアント１１からサーバ１２ａへのコネクションが確立する。そして、サーバ１２ａからのＳＹＮに対するＡＣＫ及びサーバ１２ａの時刻とクライアント１１の時刻との時間差をサーバ１２ａへ送信する。

【００４６】

サーバ１２ａの転送遅延時間取得手段は、クライアント認証情報送信手段から時間差を受信する。あるいは、サーバ１２ａは、クライアント１１からＡＣＫと時間差を受信する。サーバ１２ａは時間差をサーバ１２ａからクライアント１１までの転送遅延時間として取得する。クライアント１１とサーバ１２ａとの間で時刻同期がとれていなくても、クライアント１１とサーバ１２ａはクロック周波数の同期がとれているので、転送遅延時間は再現性よく取得することができる。クライアント１１とサーバ１２ａとの間で時刻同期がとれていれば、サーバ１２ａで測定しても、クライアント１１で測定しても、同じ転送遅延時間が保証されることになる。

【００４７】

ここで、図３及び図４にて説明した転送遅延時間の測定方法の第１例及び第２例において、前記サーバと前記クライアントとの間の応答信号（ＡＣＫ）に、ＴＣＰレイヤのタイムスタンプを含むことが好ましい。従来の転送遅延時間の測定では、測定用のパケットを送出し、そのパケットを受信することで転送遅延時間を測定していた。この場合、測定頻度を上げていくと、測定用パケットのトラフィックがその回線容量に無視できなくなることがある。本実施形態では、一般的なインターネット上で不可欠なＴＣＰ／ＩＰ動作の中で使用されるプロトコルに、転送遅延時間測定機能を埋め込むこともできる。このプロトコルをほとんど変更することなく、そのパケットに時刻情報を埋め込むことで、ＴＣＰコネクションの伝送時間測定とクライアント１１からの時間測定とを、１つのＴＣＰコネクション確立時に同時に完了することができる。ＴＣＰレイヤのタイムスタンプを用いるこ

とで、ＴＣＰコネクションの確立時に、転送遅延時間を測定することができる。

【００４８】

図２に示す認証情報照合手段２３は、転送遅延時間取得手段２２の取得した転送遅延時間を、認証情報記憶手段２１に記憶されている転送遅延時間と照合する。転送遅延時間は通信ネットワークの通信環境に応じて変化するので、認証情報照合手段２３は、例えば、通信ネットワーク１０の通信環境ごとに予め誤差の範囲を定め、その誤差の範囲内にあることで照合を行う。認証の確度を高めるため、認証情報照合手段２３は、転送遅延時間を複数回測定してその平均値を求め、その平均値を照合することが好ましい。さらに、認証情報照合手段２３は、転送遅延時間取得手段２２の取得する転送遅延時間の分散を算出し、その平均値を中心とする当該分散の範囲を、認証情報記憶手段２１に記憶されている転送遅延時間と照合することが好ましい。転送遅延時間を認証情報として利用するので、特別な認証情報を用いずに短時間で正規ユーザを認証することができる。さらに、サーバが同一のクライアント１１との間の転送遅延時間を測定するので、認証の確度を高めることができる。

【００４９】

図２に示す認証情報更新手段３４は、クライアント１１との間の転送遅延時間を予め定められたタイミングで取得し、認証情報記憶手段２１に記憶されている転送遅延時間を、取得した転送遅延時間に更新する。通信ネットワーク１０の状況によってはルータ１３ａ及び１３ｂの転送先は変わる可能性がある。この場合に、認証情報更新手段３４が、認証情報記憶手段２１に記憶されている転送遅延時間を最新のものに更新することで、認証情報照合手段２３の照合する確度を高めることができる。これにより、第三者のなりすましを防ぐことができる。

【００５０】

（実施形態２）

本実施形態に係る端末認証システムは、図１に示す端末認証システムにおいて、３以上のサーバ１２ａ、１２ｂ、１２ｃを備え、そのうちの少なくとも１つのサーバ１２ｂが認証用サーバとして予め定められている。ここで、認証用サーバは１つに限られず、２つ以上であってもよい。例えば、認証用サーバは、複数のサーバによって構成されるグループごとに定められていてもよい。

【００５１】

図５は、サーバの機能の一例を示す概略構成図である。本実施形態においては、サーバ１２ａは、転送遅延時間取得手段２２と、認証情報送信手段２４と、を備える。認証用サーバ１２ｂは、認証情報記憶手段２５と、転送遅延時間受信手段２６と、認証情報蓄積手段２７と、認証情報照合手段２８と、を備える。ここで、認証用サーバ１２ｂは、転送遅延時間取得手段２２及び認証情報送信手段２４などのサーバ１２ａと同様の構成を備えるが、図５では簡単のため省略した。これらの構成によって、本実施形態に係る端末認証システムは、サーバ１２ａ、１２ｂ、１２ｃの取得した転送遅延時間に基づいてクライアント１１を認証する。なお、図５では、サーバ１２ａとクライアント１１とを接続する通信ネットワーク（図１の符号１０）は省略した。

【００５２】

さらに、サーバ１２ａは、最新転送遅延時間取得手段３５と、最新転送遅延時間送信手段３６と、をさらに備えることが好ましい。この場合、認証用サーバ１２ｂは、認証情報更新手段３７をさらに備えることが好ましい。これらの構成をさらに備えることによって、端末認証システムは、認証情報照合手段２８の照合先を最新の情報に更新することで、第三者のなりすましを防ぐことができる。

【００５３】

本実施形態に係る端末認証方法は、本実施形態に係る端末認証システムとして機能させる。また、本実施形態に係る端末認証プログラムは、本実施形態に係る端末認証方法をコンピュータに実行させるための端末認証プログラムである。端末認証プログラムは、コンピュータ読出可能な記憶媒体に記憶されていてもよい。本実施形態に係る端末認証方法は

、例えば、認証情報記憶手段２５として機能させるための認証情報記憶ステップと、転送遅延時間取得手段２２として機能させるための転送遅延時間取得ステップと、認証情報送信手段２４として機能させるための認証情報送信ステップと、転送遅延時間受信手段２６として機能させるための転送遅延時間受信ステップと、認証情報蓄積手段２７として機能させるための認証情報蓄積ステップと、認証情報照合手段２８として機能させるための認証情報照合ステップと、転送遅延時間取得手段２２として機能させるための転送遅延時間取得ステップと、を順に有する。

【００５４】

さらに、端末認証方法は、最新転送遅延時間取得手段３５として機能させるための最新転送遅延時間取得ステップと、最新転送遅延時間送信手段３６として機能させるための最新転送遅延時間送信ステップと、認証情報更新手段３７として機能させるための認証情報更新ステップと、を転送遅延時間取得ステップの前に有することが好ましい。

【００５５】

クライアント１１からサーバ１２ａへアクセスがあると、サーバ１２ａの転送遅延時間取得手段２２はクライアント１１との間の転送遅延時間を取得する。ここで、転送遅延時間は、サーバ１２ａの時刻とサーバ１２ａが取得したクライアント１１の時刻との時間差又はサーバ１２ａが取得したクライアント１１の時刻とサーバ１２ａの時刻との時間差である。クライアント１１からサーバ１２ａへのコネクション設定時に転送遅延時間取得手段２２が転送遅延時間を取得する。そして、認証情報送信手段２４は、転送遅延時間取得手段２２の取得した転送遅延時間を、サーバ１２ａ、１２ｂ、１２ｃのうちの予め定められた認証用サーバ１２ｂへ送信する。

【００５６】

クライアント１１からサーバ１２ａへアクセスがあった場合、サーバ１２ａは、認証用サーバ１２ｂ及びサーバ１２ｃの転送遅延時間取得手段２２も、クライアント１１の転送遅延時間を取得する。そして、それぞれのサーバ１２ａ、１２ｂ、１２ｃは、取得した転送遅延時間を認証用サーバ１２ｂへ送信する。なお、クライアント１１からサーバ１２ａへアクセスがあった旨の他のサーバ１２ｂ及び１２ｃへの通知は、サーバ１２ａがサーバ１２ｂ及び１２ｃへ直接通知してもよいし、一旦サーバ１２ａから認証用サーバ１２ｂへ通知した後に認証用サーバ１２ｂがサーバ１２ｃへ通知してもよい。

【００５７】

一方、認証用サーバ１２ｂの認証情報記憶手段２５は、クライアント１１との間の転送遅延時間が通信ネットワーク内に接続されているサーバごとに予め記憶されている。例えば、認証情報記憶手段２５は、サーバ１２ａとクライアント１１との間の転送遅延時間と、サーバ１２ｂとクライアント１１との間の転送遅延時間と、サーバ１２ｃとクライアント１１との間の転送遅延時間と、を記憶している。記憶している内容は、実施形態１の認証情報記憶手段２１と同様に、クライアント１１への情報提供サービスを開始する際に、各サーバ１２ａ、１２ｂ、１２ｃがクライアント１１との間の転送遅延時間を取得したものである。

【００５８】

認証用サーバ１２ｂの転送遅延時間受信手段２６は、認証情報送信手段２４からの転送遅延時間を受信する。そして、認証用サーバ１２ｂの認証情報蓄積手段２７は、転送遅延時間受信手段２６の受信した転送遅延時間を、認証情報送信手段２４を備えるサーバ１２ａ、１２ｂ、１２ｃごとに蓄積する。例えば、サーバ１２ａから送信された転送遅延時間を、サーバ１２ａの識別情報と関連付けて記憶する。

【００５９】

認証用サーバ１２ｂの認証情報照合手段２８は、認証情報蓄積手段２７の蓄積する転送遅延時間が３つ以上になった場合に、認証情報記憶手段２５を参照して認証情報蓄積手段２７の蓄積しているサーバの転送遅延時間を抽出し、抽出した転送遅延時間の分散を算出する。例えば、認証情報照合手段２８は、サーバ１２ａ、１２ｂ、１２ｃの転送遅延時間を蓄積すると、認証情報記憶手段２５を参照し、サーバ１２ａ、１２ｂ及び１２ｃの転送

遅延時間を抽出する。認証情報照合手段２８は、認証情報蓄積手段２７の蓄積している転送遅延時間の分散を算出する。そして、認証情報照合手段２８は、算出した２つの分散の差異が一定範囲内にあることを判定する。

【００６０】

それぞれのサーバ１２ａ、１２ｂ、１２ｃとクライアント１１の転送遅延時間のばらつきが、予め登録されているクライアントとの転送遅延時間のばらつきの一定範囲内であれば、それぞれのサーバ１２ａ、１２ｂ、１２ｃとクライアント１１の通信ネットワーク上の相対的な位置関係がある範囲内であることを判定することができる。転送遅延時間を認証情報として利用するので、特別な認証情報を用いずに短時間で正規ユーザを認証することができる。さらに、サーバの取得した転送遅延時間の分散によって、予め登録されているクライアント１１であるか否かを判定するので、認証の確度を高めることができる。

【００６１】

サーバ１２ａの最新転送遅延時間取得手段３５は、クライアント１１との間の転送遅延時間を予め定められたタイミングで取得する。サーバ１２ａの最新転送遅延時間送信手段３６は、最新転送遅延時間取得手段３５の取得した転送遅延時間を認証用サーバ１２ｂへ送信する。認証用サーバ１２ｂの転送遅延時間受信手段２６は、サーバ１２ａの最新転送遅延時間送信手段３６の送信した転送遅延時間を受信する。認証用サーバ１２ｂの認証情報更新手段３７は、最新転送遅延時間送信手段３６が送信して転送遅延時間受信手段２６が受信した転送遅延時間を取得すると、認証情報記憶手段２５に記憶されている転送遅延時間を、最新転送遅延時間送信手段３６の送信した転送遅延時間に更新する。

【００６２】

（実施形態３）

図５に示す端末認証システムでは３以上のサーバ１２ａ、１２ｂ、１２ｃを必要としたが、本実施形態に係る端末認証システムでは、２以上のサーバを必要とする。また、図５に示す端末認証システムと、認証情報記憶手段２５と、認証情報照合手段２８と、認証情報更新手段３７と、について異なる。

【００６３】

図６は、本実施形態に係る端末認証システムの説明図である。図１に示したシステムにおいて、複数のサーバ１２ａ、１２ｂ、１２ｃとクライアント１１との間の転送遅延時間を測定すると、さらに通信ネットワーク１０上の仮想位置が限定される。本実施形態に係る端末認証システムは、この仮想位置を認証情報として利用していることを特徴としている。

【００６４】

通信機器を特定することで、特定の機能を利用することが可能となるようなサービス、例えば、サーバからコンテンツをダウンロードするサービスなどでは、正規のユーザのみにサービスを提供する必要があり、さらに、ダウンロードされたコンテンツが、正規のユーザでのみ利用されていることが保証される必要がある。このようなサービスでは、コンテンツをダウンロードする機器が登録されている必要があり、さらにその機器が別の許可されていない不正なユーザによって利用されていること（本実施形態では、別の場所でコンテンツが利用されること。）を防止することが要求される。

【００６５】

本実施形態は、このようなユーザ機器（クライアント１１）の通信ネットワーク上の位置を、サービス利用開始時に特定し、そのデータを登録し保存する。その後、クライアント１１がサービスを利用してコンテンツをダウンロードするときに、再度、通信ネットワーク上の位置を再計算し、この利用時の位置と登録された位置を比較することで、そのクライアント１１が正規のユーザかどうかを判断することができる。

【００６６】

具体的には、本実施形態においては、サーバ１２ａは、転送遅延時間取得手段２２と、認証情報送信手段２４と、を備える。認証用サーバ１２ｂは、認証情報記憶手段２５と、転送遅延時間受信手段２６と、認証情報蓄積手段２７と、認証情報照合手段２８と、を備

える。ここで、認証用サーバ１２ｂは、認証情報記憶手段２１及び認証情報送信手段２４を備えるが、図５では簡単のため省略した。また、転送遅延時間取得手段２２は、最新転送遅延時間取得手段３５と同じルートを介してクライアント１１との間の転送遅延時間を取得する。これらの構成によって、本実施形態に係る端末認証システムは、サーバ１２ａ、１２ｂ、１２ｃのうちの少なくとも２つのサーバの取得した転送遅延時間によって特定される通信ネットワーク上の仮想位置に基づいてクライアント１１を認証する。

【００６７】

また、転送遅延時間取得手段２２は、クライアント１１との間の転送遅延時間を複数回取得し、取得した転送遅延時間の平均値を算出することが好ましい。この場合、認証情報送信手段２４は、転送遅延時間取得手段２２の算出する平均値を、転送遅延時間としてサーバ１２ａ、１２ｂ、１２ｃのうちの予め定められた認証用サーバへ送信する。転送遅延時間の平均値を算出することで、登録時のルートとは異なったルートでクライアントとサーバの間のコネクションが確立された場合でも、登録されたクライアントであることを判定することができる。

【００６８】

本実施形態に係る端末認証方法は、本実施形態に係る端末認証システムとして機能させる。また、本実施形態に係る端末認証プログラムは、本実施形態に係る端末認証方法をコンピュータに実行させるための端末認証プログラムである。端末認証プログラムは、コンピュータ読出可能な記憶媒体に記憶されていてもよい。本実施形態に係る端末認証方法は、例えば、認証情報記憶手段２５として機能させるための認証情報記憶ステップと、転送遅延時間取得手段２２として機能させるための転送遅延時間取得ステップと、認証情報送信手段２４として機能させるための認証情報送信ステップと、転送遅延時間受信手段２６として機能させるための転送遅延時間受信ステップと、認証情報蓄積手段２７として機能させるための認証情報蓄積ステップと、認証情報照合手段２８として機能させるための認証情報照合ステップと、転送遅延時間取得手段２２として機能させるための転送遅延時間取得ステップと、を順に有する。

【００６９】

さらに、端末認証方法は、最新転送遅延時間取得手段３５として機能させるための最新転送遅延時間取得ステップと、最新転送遅延時間送信手段３６として機能させるための最新転送遅延時間送信ステップと、認証情報更新手段３７として機能させるための認証情報更新ステップと、を転送遅延時間取得ステップの前に有することが好ましい。

【００７０】

認証用サーバ１２ｂの認証情報記憶手段２５は、通信ネットワーク内に接続されているサーバ１２ａ、１２ｂ、１２ｃ及びクライアント１１の通信ネットワーク上の仮想位置を記憶する。通信ネットワーク上の仮想位置は、サーバ１２ａ、１２ｂ、１２ｃなどの地図上の位置が固定されている位置を基準とした仮想地図上に、クライアント１１との間の転送遅延時間によって特定されている位置である。サーバ１２ａ、１２ｂ、１２ｃの仮想位置は、例えば、サーバ１２ａ、１２ｂ、１２ｃの配置されているネットワーク上の位置である。クライアント１１の仮想位置の登録時に、それぞれのサーバ１２ａ、１２ｂ、１２ｃとクライアント１１との間の転送遅延時間を測定し、サーバ１２ａ、１２ｂ、１２ｃからの転送遅延時間によって特定される位置を、クライアント１１の位置として登録する。仮想位置は、例えば、緯度経度などの２次元平面上の位置又は３次元空間上の位置である。

【００７１】

認証用サーバ１２ｂの認証情報照合手段２８は、認証情報蓄積手段２７の蓄積した転送遅延時間が２つ以上になった場合に、認証情報記憶手段２５を参照して認証情報蓄積手段２７の蓄積しているサーバ１２ａ、１２ｂ、１２ｃの位置を抽出し、抽出した位置と転送遅延時間とから、認証情報蓄積手段２７の蓄積しているクライアント１１の位置を算出する。例えば、認証情報照合手段２８は、サーバ１２ａ、１２ｂ及び１２ｃの転送遅延時間から距離を算出して、サーバ１２ａ、１２ｂ及び１２ｃのそれぞれの位置と算出したそれ

ぞれの距離とからクライアント１１の位置を特定する。ここで、転送遅延時間から距離への変換は、転送速度一定として時間積分を行ってもよいし、予め定めた関数によって定義される速度を時間積分してもよい。認証情報照合手段２８は、算出したサーバ１２ａ、１２ｂ及び１２ｃの位置を、認証情報記憶手段２５に記憶されている位置と照合する。転送遅延時間は通信ネットワーク１０の通信環境に応じて変化するので、認証情報照合手段２８は、例えば、通信ネットワーク１０の通信環境ごとに予め誤差の範囲を定め、その誤差の範囲内にあることで照合を行う。

【００７２】

サーバの位置と転送遅延時間によって、通信ネットワーク上の仮想的な位置を特定することができる。転送遅延時間を取得しておき、認証情報記憶手段２５にこの位置を予め記憶させておくことで、認証情報照合手段２８はクライアント１１の通信ネットワーク上の仮想的な位置を特定し、予め登録されているクライアント１１か否かを判定することができる。この方式では、サーバ及びクライアント間の通信ネットワークが確保できれば、屋外、屋内を問わないため、どこからでもクライアント１１の認証を行うことができる。また、ＧＰＳ受信機のような特別なハードウェアは必要なく、通常のソフトウェアを機器へインストールすればよい。

【００７３】

サーバ１２ａ、１２ｂ及び１２ｃは、最新転送遅延時間取得手段３５と、最新転送遅延時間送信手段３６と、をさらに備えることが好ましい。この場合、認証用サーバ１２ｂは、認証情報更新手段３７をさらに備えることが好ましい。これらの構成をさらに備えることによって、端末認証システムは、認証情報照合手段２８の参照先を最新の情報に更新することで、第三者のなりすましを防ぐことができる。認証用サーバ１２ｂの認証情報更新手段３７は、最新転送遅延時間送信手段の送信した転送遅延時間と、認証情報記憶手段に記憶されているサーバの位置を用いて、クライアント１１の位置を算出し、認証情報記憶手段２５に記憶されているクライアント１１の位置を、算出したクライアント１１の位置に更新する。サーバ１２ａ、１２ｂ及び１２ｃとの間の転送遅延時間からのクライアント１１の位置の算出方法は、認証情報照合手段２８と同様の方法を用いることができる。

【実施例】

【００７４】

転送遅延時間は、基本的に１回の測定で求めることはできない。ネットワークの状態が時間的に変化するので、統計的な数値から転送遅延時間を求めることが好ましい。このため、複数回の測定が要求され、この測定方式（アルゴリズム）は一種類ではないので、実施例としてはいくつか考えられる。

【００７５】

（転送遅延時間測定方式の実施例１）

サーバ１２ａとクライアント１１との間の転送遅延時間測定方式の第１実施例について図１を用いて説明する。サーバ１２ａから、認証プロセスを実施するときに、転送遅延時間を複数回測定してから認証プロセスに反映する方式。この場合、転送遅延時間をサーバが測定する方式と、クライアント１１が転送遅延時間を測定して、結果をサーバ１２ａに転送する方式がある。

【００７６】

（転送遅延時間測定方式の実施例２）

サーバ１２ａとクライアント１１との間の転送遅延時間測定方式の第２実施例について説明する。サーバ１２ａから、認証プロセスを実施するタイミングとは関係なく、ある一定の時間間隔で、転送遅延を複数回測定し、その結果を認証プロセスに反映する。例えば、サーバ１２ａは、１時間に１回、又は、１０分間に１回ずつ測定するなどである。この場合、転送遅延時間をサーバ１２ａが測定する方式と、クライアント１１が転送遅延時間を測定して、結果をサーバ１２ａに転送する方式とがある。

【００７７】

（転送遅延時間測定方式の実施例３）

サーバ１２ａとクライアント１１との間の転送遅延時間測定方式の第３実施例について説明する。サーバ１２ａから、認証プロセスを実施するタイミングとは関係なく、サーバ１２ａとクライアント１１の間のトラフィック状態を計測し、トラフィックが予め設定された状態のときに、１回もしくは複数回、転送遅延時間を測定し、その結果を認証プロセスに反映する。例えば、トラフィックが、ある一定値以下になり、通信ネットワークが空いている状態のときに、転送遅延時間を測定する。この場合、転送遅延時間をサーバ１２ａが測定する方式と、クライアント１１が転送遅延時間を測定して、結果をサーバ１２ａに転送する方式がある。

【００７８】

（システム認証の実施例１）

複数のサーバ１２ａ、１２ｂ及び１２ｃとクライアント１１との間の転送遅延時間測定とシステム認証の第１実施例について説明する。転送遅延時間測定方式の実施例１、２及び３で、複数のサーバ１２ａ、１２ｂ及び１２ｃが順番に、サーバ１２ａ、１２ｂ及び１２ｃのそれぞれとクライアント１１との間の転送遅延時間を測定し、認証に必要な数のサーバ１２ａ、１２ｂ又は１２ｃで、転送遅延時間測定が終了した時点で、最終的にシステム全体の認証をする。

【００７９】

（システム認証の実施例２）

複数のサーバ１２ａ、１２ｂ及び１２ｃとクライアント１１との間の転送遅延時間測定とシステム認証の第２実施例について説明する。転送遅延時間測定方式の実施例３をベースに転送遅延時間を測定する方式において、認証に必要な数以上のサーバ１２ａ、１２ｂ又は１２ｃを使用して、サーバ１２ａ、１２ｂ及び１２ｃのそれぞれとクライアント１１間のトラフィックを順次測定しながら、トラフィックが予め設定された状態になったサーバ１２ａ、１２ｂ及び１２ｃのそれぞれとクライアント１１との間の転送遅延時間から測定し、転送遅延時間測定が終了したサーバ１２ａ、１２ｂ又は１２ｃが、認証に必要な数になった時点で認証を完了する方式。

【００８０】

（システム認証の実施例３）

複数のサーバ１２ａ、１２ｂ及び１２ｃとクライアント１１との間の転送遅延時間測定とシステム認証の第３実施例について説明する。転送遅延時間測定方式の実施例２と同様な方式で、クライアント１１を認証する。システム認証の実施例２と異なるのは、認証が終了しても、サーバ１２ａ、１２ｂ及び１２ｃのそれぞれとクライアント１１との間のトラフィックを順次測定しながら、トラフィックが予め設定された状態になったサーバ１２ａ、１２ｂ及び１２ｃのそれぞれとクライアント１１との間の転送遅延時間を測定し続ける点である。これを続けることで、通信ネットワーク１０に接続されているクライアント１１を、認証に必要なサーバ数以上のサーバ１２ａ、１２ｂ又は１２ｃで、常にサーバ１２ａ、１２ｂ及び１２ｃのそれぞれとクライアント１１間の転送遅延時間測定を実施することができ、常に認証することができる。

【産業上の利用可能性】

【００８１】

サーバからコンテンツをダウンロードするサービスなどでは、正規のユーザのみにサービスを提供するための正規のユーザの認証に利用することができる。

【図面の簡単な説明】

【００８２】

【図１】実施形態１に係る端末認証システムの概略構成図である。

【図２】サーバの機能の一例を示す概略構成図である。

【図３】転送遅延時間の測定方法の第１例を示すシーケンス図である。

【図４】転送遅延時間の測定方法の第２例を示すシーケンス図である。

【図５】サーバの機能の一例を示す概略構成図である。

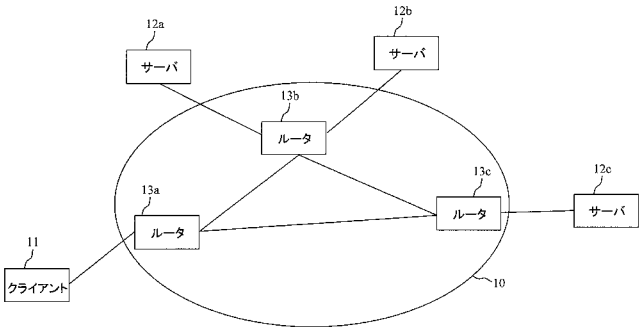
【図６】本実施形態に係る端末認証システムの説明図である。

【符号の説明】

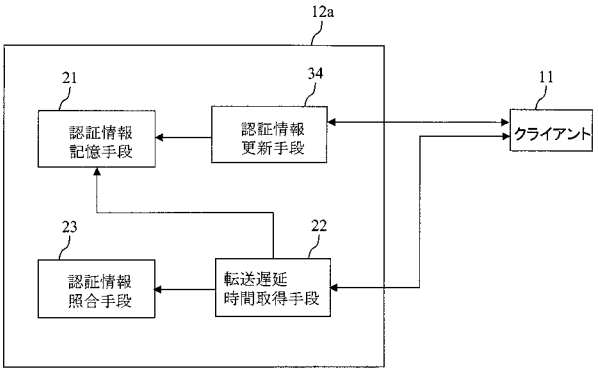
【００８３】

１０　通信ネットワーク
１１　クライアント
１２　サーバ
１３　ルータ
２１　認証情報記憶手段
２２　転送遅延時間取得手段
２３　認証情報照合手段
２４　認証情報送信手段
２５　認証情報記憶手段
２６　転送遅延時間受信手段
２７　認証情報蓄積手段
２８　認証情報照合手段
３４　認証情報更新手段
３５　最新転送遅延時間取得手段
３６　最新転送遅延時間送信手段
３７　認証情報更新手段

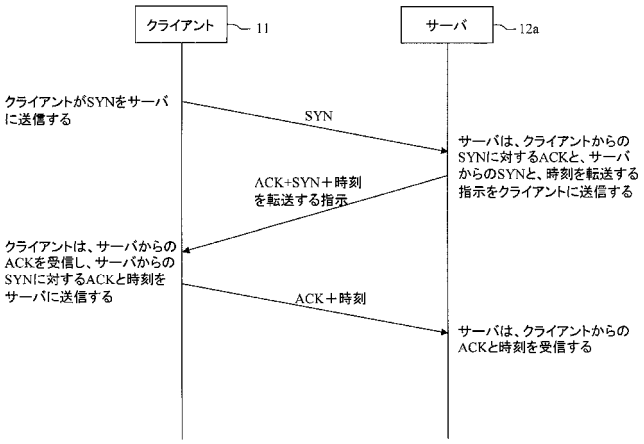
【図１】



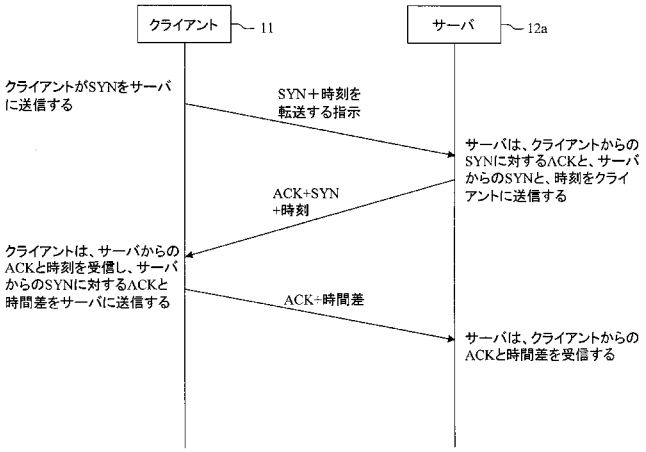
【図２】



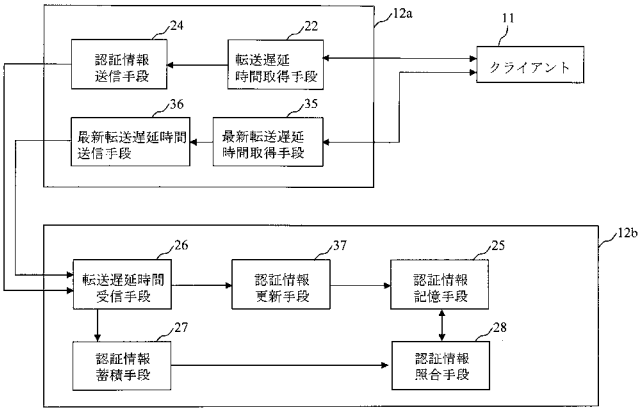
【図３】



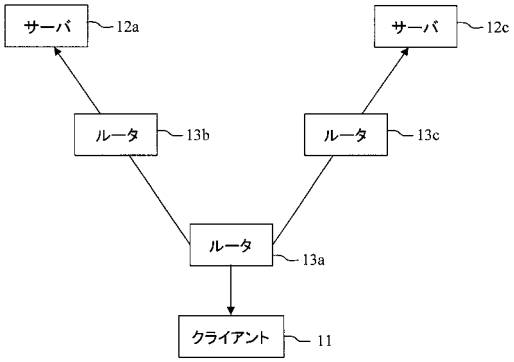
【図４】


クライアント
11
サーバ
12a
クライアントがSYNをサーバに送信する
SYN＋時刻を転送する指示
サーバは、クライアントからのSYNに対するACKと、サーバからのSYNと、時刻をクライアントに送信する
ACK+SYN+時刻
クライアントは、サーバからのACKと時刻を受信し、サーバからのSYNに対するACKと時間差をサーバに送信する
ACK+時間差
サーバは、クライアントからのACKと時間差を受信する

【図５】


12a
11
24
認証情報送信手段
22
転送遅延時間取得手段
クライアント
36
最新転送遅延時間送信手段
35
最新転送遅延時間取得手段
12b
26
転送遅延時間受信手段
37
認証情報更新手段
25
認証情報記憶手段
27
認証情報蓄積手段
28
認証情報照合手段

【図６】


サーバ
12a
サーバ
12c
ルータ
13b
ルータ
13c
ルータ
13a
クライアント
11

フロントページの続き

(72)発明者　小野　定康
東京都港区三田２丁目１５番４５号　慶應義塾大学デジタルメディア・コンテンツ統合研究機構内

Ｆターム(参考) 5B285 AA01　BA09　CB41　CB49　CB50　CB62　CB72