

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第5093649号
(P5093649)

(45) 発行日 平成24年12月12日(2012.12.12)

(24) 登録日 平成24年9月28日(2012.9.28)

| | | | | | |
|--------------|--------------|------------------|------|-------|------|
| (51) Int.Cl. | | F I | | | |
| G06F | 21/20 | (2006.01) | G06F | 21/20 | 144C |
| H04L | 9/32 | (2006.01) | H04L | 9/00 | 673A |
| H04L | 12/56 | (2006.01) | H04L | 12/56 | 400Z |

請求項の数 12 (全 19 頁)

| | | | |
|-----------|-------------------------------|-----------|---------------------|
| (21) 出願番号 | 特願2007-132478 (P2007-132478) | (73) 特許権者 | 899000057 |
| (22) 出願日 | 平成19年5月18日 (2007.5.18) | | 学校法人日本大学 |
| (65) 公開番号 | 特開2008-287542 (P2008-287542A) | | 東京都千代田区九段南四丁目8番24号 |
| (43) 公開日 | 平成20年11月27日 (2008.11.27) | (74) 代理人 | 100119677 |
| 審査請求日 | 平成22年5月14日 (2010.5.14) | | 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 |
| | | (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 |

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) 【特許請求の範囲】

【請求項1】

サーバがクライアントと1以上のルータを含む通信ネットワークで接続され、コンテンツを前記通信ネットワーク経由で前記クライアントに配信するサービスにおいて、前記クライアントが正規の利用者であるかどうかを認証する端末認証システムであって、

前記サーバは、

前記クライアントまでの往復転送遅延時間が予め記憶されている認証情報記憶手段と、

前記クライアントまでの往復転送遅延時間を取得する往復転送遅延時間取得手段と、

前記往復転送遅延時間取得手段の取得した往復転送遅延時間が、前記認証情報記憶手段に記憶されている往復転送遅延時間の誤差範囲内にあることで照合を行う認証情報照合手段と、

前記クライアントまでの往復転送遅延時間をあらかじ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往復転送遅延時間を、取得した往復転送遅延時間に更新する認証情報更新手段と、を備え、

前記認証情報照合手段によって照合できたクライアントを正規の利用者であると認証してコンテンツを提供することを特徴とする端末認証システム。

【請求項2】

前記往復転送遅延時間取得手段は、前記クライアントまでの往復転送遅延時間を複数回取得し、

前記認証情報照合手段は、前記往復転送遅延時間取得手段の取得する往復転送遅延時間

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往復転送遅延時間と照合す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】

前記認証情報照合手段は、さらに、前記往復転送遅延時間取得手段の取得する往復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往復転送遅延時間と照合することを特徴とする請求項 2 に記載の端末認証システム。

【請求項 4】

2 以上のサーバがクライアントと 1 以上のルータを含む通信ネットワークで接続され、コンテンツを前記通信ネットワーク経由で前記クライアントに配信するサービスにおいて、前記クライアントが正規の利用者であるかどうかを認証する端末認証システムであって

10

前記サーバは、それぞれ、

前記クライアントまでの往復転送遅延時間を取得する往復転送遅延時間取得手段と、

前記往復転送遅延時間取得手段の取得した往復転送遅延時間を、前記サーバのうちあらかじ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、

前記クライアントまでの往復転送遅延時間をあらかじ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往復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、

20

前記認証用サーバは、

前記認証情報送信手段の送信する往復転送遅延時間を受信する往復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、

前記往復転送遅延時間受信手段の受信した往復転送遅延時間を、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往復転送遅延時間が 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、抽出した位置と往復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、

30

前記最新転送遅延時間送信手段の送信した往復転送遅延時間と、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と、を備え、

前記認証情報照合手段によって照合できたクライアントを正規の利用者であると認証してコンテンツを提供することを特徴とする端末認証システム。

【請求項 5】

前記往復転送遅延時間取得手段は、前記クライアントまでの往復転送遅延時間を複数回取得し、取得した往復転送遅延時間の平均値を算出し、

40

前記認証情報送信手段は、前記往復転送遅延時間取得手段の算出する平均値を、前記往復転送遅延時間として前記サーバのうちあらかじ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 4 に記載の端末認証システム。

【請求項 6】

前記クライアントは、さらに、前記往復転送遅延時間取得手段の送信する転送遅延時間測定指示を受信すると、当該往復転送遅延時間取得手段へ応答信号を送信するクライアント応答信号送信手段を備え、

前記往復転送遅延時間取得手段は、さらに、転送遅延時間の測定を指示する転送遅延時間測定指示を前記クライアントに送信し、前記クライアント応答信号送信手段の送信する

50

応答信号を受信すると、転送遅延時間測定指示を送信してから応答信号を受信するまでの時間を測定することを特徴とする請求項 1 から 5 のいずれかに記載の端末認証システム。

【請求項 7】

前記クライアントは、

転送遅延時間の測定を指示する転送遅延時間測定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、

前記サーバの送信する応答信号を受信し、前記クライアント測定指示送信手段が転送遅延時間測定指示を送信してから応答信号を受信するまでの時間を測定し、測定した時間を転送遅延時間として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、をさらに備え、

前記往復転送遅延時間取得手段は、さらに、前記クライアント測定指示送信手段の送信する転送遅延時間測定指示を受信すると、前記クライアント測定指示送信手段へ応答信号を送信し、前記クライアント認証情報送信手段の送信する転送遅延時間を受信することを特徴とする請求項 1 から 5 のいずれかに記載の端末認証システム。

【請求項 8】

前記転送遅延時間測定指示及び応答信号が、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 6 又は 7 に記載の端末認証システム。

【請求項 9】

サーバがクライアントと 1 以上のルータを含む通信ネットワークで接続され、コンテンツを前記通信ネットワーク経由で前記クライアントに配信するサービスにおいて、前記クライアントが正規の利用者であるかどうかを認証す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、前記クライアントまでの往復転送遅延時間をあらかじめ定められたタイミングで取得する往復転送遅延時間取得ステップと、

前記サーバが、前記往復転送遅延時間取得ステップで取得した往復転送遅延時間が、前記クライアントまでの往復転送遅延時間が予め認証情報記憶手段に記憶されている往復転送遅延時間の誤差範囲内にあることで照合を行う認証情報照合ステップと、を順に有し、

前記認証情報照合ステップにおいて照合できたクライアントを正規の利用者であると認証してコンテンツを提供することを特徴とする端末認証方法。

【請求項 10】

2 以上のサーバがクライアントと 1 以上のルータを含む通信ネットワークで接続され、コンテンツを前記通信ネットワーク経由で前記クライアントに配信するサービスにおいて、前記クライアントが正規の利用者であるかどうかを認証す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あらかじ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クライアントまでの往復転送遅延時間をあらかじめ定められたタイミングで受信する往復転送遅延時間受信ステップと、

前記往復転送遅延時間受信ステップで受信した往復転送遅延時間と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、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往復転送遅延時間が 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、抽出した位置と往復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の誤差範囲内にあることで照合を行う認証情報照合ステップと、

を順に有し、

10

20

30

40

50

前記認証情報照合ステップにおいて照合できたクライアントを正規の利用者であると認証してコンテンツを提供することを特徴とする端末認証方法。

【請求項 1 1】

請求項 9 又は 1 0 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 1 2】

請求項 1 1 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】

【0 0 0 1】

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】

【0 0 0 2】

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。 ）。

【0 0 0 3】

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 2 0 0 7 - 4 2 4 3 号公報

【特許文献 2】特開 2 0 0 6 - 1 0 8 8 3 4 号公報

【特許文献 3】特開 2 0 0 6 - 2 5 2 0 1 6 号公報

【発明の開示】

【発明が解決しようとする課題】

【0 0 0 4】

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。

【0 0 0 5】

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】

【0 0 0 6】

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。

【0 0 0 7】

具体的には、本発明に係る端末認証システムは、サーバがクライアントと 1 以上のルータを含む通信ネットワークで接続され、コンテンツを前記通信ネットワーク経由で前記クライアントに配信するサービスにおいて、前記クライアントが正規の利用者であるかどうかを認証する端末認証システムであって、前記サーバは、前記クライアントまでの往復転送遅延時間が予め記憶されている認証情報記憶手段と、前記クライアントまでの往復転送遅延時間を取得する往復転送遅延時間取得手段と、前記往復転送遅延時間取得手段の取得した往復転送遅延時間が、前記認証情報記憶手段に記憶されている往復転送遅延時間の誤

10

20

30

40

50

差範囲内にあることで照合を行う認証情報照合手段と、前記クライアントまでの往復転送遅延時間をあらかじ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往復転送遅延時間を、取得した往復転送遅延時間に更新する認証情報更新手段と、を備え、前記認証情報照合手段によって照合できたクライアントを正規の利用者であると認証してコンテンツを提供する。

【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往復転送時間を取得するので、認証の確度を高めることができる。

また、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。

10

【0010】

本発明に係る端末認証システムでは、前記往復転送遅延時間取得手段は、前記クライアントまでの往復転送遅延時間を複数回取得し、前記認証情報照合手段は、前記往復転送遅延時間取得手段の取得する往復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往復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。

【0011】

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、前記往復転送遅延時間取得手段の取得する往復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往復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。

20

【0012】

具体的には、本発明に係る端末認証システムは、2以上のサーバがクライアントと1以上のルータを含む通信ネットワークで接続され、コンテンツを前記通信ネットワーク経由で前記クライアントに配信するサービスにおいて、前記クライアントが正規の利用者であるかどうかを認証する端末認証システムであって、前記サーバは、それぞれ、前記クライアントまでの往復転送遅延時間を取得する往復転送遅延時間取得手段と、前記往復転送遅延時間取得手段の取得した往復転送遅延時間を、前記サーバのうちのあらかじ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、前記クライアントまでの往復転送遅延時間をあらかじ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往復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、前記認証情報送信手段の送信する往復転送遅延時間を受信する往復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、前記往復転送遅延時間受信手段の受信した往復転送遅延時間を、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往復転送遅延時間が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、抽出した位置と往復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、前記最新転送遅延時間送信手段の送信した往復転送遅延時間と、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と、を備え、前記認証情報照合手段によって照合できたクライアントを正規の利用者であると認証してコンテンツを提供する。

30

40

【0013】

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

50

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。

【0014】

また、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。

【0015】

本発明に係る端末認証システムでは、前記往復転送遅延時間取得手段は、前記クライアントまでの往復転送遅延時間を複数回取得し、取得した往復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、前記往復転送遅延時間取得手段の算出する平均値を、前記往復転送遅延時間として前記サーバのうちのあらかじめ定められた認証用サーバへ送信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と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。

【0016】

本発明に係る端末認証システムでは、前記クライアントは、さらに、前記往復転送遅延時間取得手段の送信する転送遅延時間測定指示を受信すると、当該往復転送遅延時間取得手段へ応答信号を送信するクライアント応答信号送信手段を備え、前記往復転送遅延時間取得手段は、さらに、転送遅延時間の測定を指示する転送遅延時間測定指示を前記クライアントに送信し、前記クライアント応答信号送信手段の送信する応答信号を受信すると、送遅延時間測定指示を送信してから応答信号を受信するまでの時間を測定することが好ましい。クライアントが転送遅延時間測定指示を送信してから応答信号を受信するまでの往復時間を測定するので、クライアントとサーバとの間で絶対時刻が保証されていなくても、クライアントとサーバの時計の誤差が相殺し、認証情報としての確度が損なわれない。

【0017】

本発明に係る端末認証システムでは、前記クライアントは、転送遅延時間の測定を指示する転送遅延時間測定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、前記サーバの送信する応答信号を受信し、前記クライアント測定指示送信手段が転送遅延時間測定指示を送信してから応答信号を受信するまでの時間を測定し、測定した時間を転送遅延時間として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、をさらに備え、前記往復転送遅延時間取得手段は、さらに、前記クライアント測定指示送信手段の送信する転送遅延時間測定指示を受信すると、前記クライアント測定指示送信手段へ応答信号を送信し、前記クライアント認証情報送信手段の送信する転送遅延時間を受信することが好ましい。サーバが転送遅延時間測定指示を送信してから応答信号を受信するまでの往復時間を測定するので、クライアントとサーバとの間で絶対時刻が保証されていなくても、クライアントとサーバの時計の誤差が相殺し、認証情報としての確度が損なわれない。

【0018】

本発明に係る端末認証システムでは、前記転送遅延時間測定指示及び応答信号が、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、往復転送遅延時間を測定することができる。

【0019】

本発明に係る端末認証方法は、サーバがクライアントと1以上のルータを含む通信ネットワークで接続され、コンテンツを前記通信ネットワーク経由で前記クライアントに配信するサービスにおいて、前記クライアントが正規の利用者であるかどうかを認証す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、前記クライアントまでの往復転送遅延時間をあらかじめ定められたタイミングで取得する往復転送遅延時間取得ステップと、前記サーバが、前記往復転送遅延時間取得ステップで取得した往復転送遅延

10

20

30

40

50

時間が、前記クライアントまでの往復転送遅延時間が予め認証情報記憶手段に記憶されている往復転送遅延時間の誤差範囲内にあることで照合を行う認証情報照合ステップと、順に有し、前記認証情報照合ステップにおいて照合できたクライアントを正規の利用者であると認証してコンテンツを提供する。

【0020】

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ため、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往復転送時間を取得するので、認証の確度を高めることができる。

【0021】

本発明に係る端末認証方法は、2以上のサーバがクライアントと1以上のルータを含む通信ネットワークで接続され、コンテンツを前記通信ネットワーク経由で前記クライアントに配信するサービスにおいて、前記クライアントが正規の利用者であるかどうかを認証す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あらかじ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クライアントまでの往復転送遅延時間をあらかじめ定められたタイミングで受信する往復転送遅延時間受信ステップと、前記往復転送遅延時間受信ステップで受信した往復転送遅延時間と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、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往復転送遅延時間が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、抽出した位置と往復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の誤差範囲内にあることで照合を行う認証情報照合ステップと、順に有し、前記認証情報照合ステップにおいて照合できたクライアントを正規の利用者であると認証してコンテンツを提供する。

【0022】

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。

【0023】

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。

【0024】

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】

【0025】

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】

【0026】

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。

10

【0027】

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もよいし、公衆回線又は専用回線のいずれを用いてもよい。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。

【0028】

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。従来は、それぞれのルータ13a、13b、13cの処理能力が低かったため、クライアント11と特定のサーバ、例えばサーバ12aとの間で送受信を行う際に通過するルータが異なることが多かった。しかし、ルータの処理速度が高くなったことで、通過するルータが自ずと決まるようになってきた。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が情報を転送する確率が多く、ルータ13cを経由する確率は少ない場合がある。

20

【0029】

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。

【0030】

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。

30

【0031】

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、往復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。

40

【0032】

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、往復転送遅延時間取得手段22として機能させるための往復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、往復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。

50

【 0 0 3 3 】

認証情報記憶手段 2 1 は、クライアント 1 1 までの往復転送遅延時間が予め記憶されている。クライアント 1 1 への情報提供サービスを開始する際に、サーバ 1 2 a はクライアント 1 1 までの転送遅延時間を取得して認証情報記憶手段 2 1 に記憶する。本実施形態ではクライアント 1 1 が 1 つだが、2 以上の場合は、認証情報記憶手段 2 1 は、各クライアント 1 1 との転送遅延時間を記憶しておく。また、サーバ 1 2 a がさらに認証情報更新手段 3 4 を備える場合は、認証情報記憶手段 2 1 の記憶する転送遅延時間は最新の情報に更新される。

【 0 0 3 4 】

往復転送遅延時間取得手段 2 2 は、認証情報更新手段 3 4 と同じルートを介してクライアント 1 1 までの往復転送遅延時間を取得する。例えば、クライアント 1 1 からサーバ 1 2 a へアクセスがあると、往復転送遅延時間取得手段 2 2 はクライアント 1 1 の往復転送遅延時間を取得する。ここで、往復転送遅延時間は、サーバ 1 2 a が取得した時間又はクライアント 1 1 が取得した時間である。クライアント 1 1 からサーバ 1 2 a へのコネクション設定時に往復転送遅延時間取得手段 2 2 が往復転送遅延時間を取得する。

10

【 0 0 3 5 】

さらに、往復転送遅延時間取得手段 2 2 は、クライアント 1 1 までの往復転送遅延時間を複数回取得することが好ましい。さらに、往復転送遅延時間取得手段 2 2 は、取得した往復転送遅延時間の平均値を算出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 1 1 とサーバ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 2 3 は、登録されたクライアント 1 1 であることを判定することができる。

20

【 0 0 3 6 】

図 3 は、往復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。往復転送遅延時間の測定方法の第 1 例では、クライアント 1 1 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 ウェイハンドシェイクの一例について説明する。クライアント 1 1 が SYN (接続要求) をサーバ 1 2 a に送信する。

【 0 0 3 7 】

サーバ 1 2 a 往復転送遅延時間取得手段は、クライアント 1 1 から SYN を受信すると、転送遅延時間の測定を指示する転送遅延時間測定指示をクライアント 1 1 に送信する。転送遅延時間の測定を指示する転送遅延時間測定指示は、例えば、クライアント 1 1 からの SYN に対する ACK (肯定応答) である。この場合、サーバ 1 2 a の往復転送遅延時間取得手段は、クライアント 1 1 からの SYN に対する ACK (肯定応答) と、サーバ 1 2 a からの SYN をクライアント 1 1 に送信する。

30

【 0 0 3 8 】

クライアント 1 1 のクライアント応答信号送信手段は、サーバ 1 2 a の往復転送遅延時間取得手段の送信する転送遅延時間測定指示を受信すると、サーバ 1 2 a の往復転送遅延時間取得手段へ応答信号を送信する。例えば、クライアント 1 1 のクライアント応答信号送信手段は、サーバ 1 2 a からの ACK を受信し、サーバ 1 2 a からの SYN に対する ACK をサーバ 1 2 a の往復転送遅延時間取得手段に送信する。

40

【 0 0 3 9 】

サーバ 1 2 a の往復転送遅延時間取得手段は、クライアント応答信号送信手段の送信する応答信号を受信する。例えば、サーバ 1 2 a の往復転送遅延時間取得手段は、クライアント 1 1 からの ACK を受信する。そして、転送遅延時間測定指示を送信してから応答信号を受信するまでの時間を測定する。クライアント 1 1 が転送遅延時間測定指示を送信してから応答信号を受信するまでの往復時間を測定するので、クライアント 1 1 とサーバとの間で絶対時刻が保証されていなくても、クライアント 1 1 とサーバの時計の誤差が相殺し、認証情報としての確度が損なわれない。

【 0 0 4 0 】

図 4 は、往復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。往復転送遅

50

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。往復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ウェイハンドシェイクの一例を示す。

【0041】

クライアント11のクライアント測定指示送信手段は、転送遅延時間の測定を指示する転送遅延時間測定指示をサーバに送信する。例えば、クライアント11がSYNとTime1(時刻)をサーバに送信する。

【0042】

サーバ12aの往復転送遅延時間取得手段は、クライアント測定指示送信手段の送信する転送遅延時間測定指示を受信すると、クライアント測定指示送信手段へ応答信号を送信する。例えば、サーバ12aは、クライアント11からのSYNとTime1に対するACKと、サーバ12aからのSYNと、Time2(時刻)と、をクライアント11に送信する。

10

【0043】

クライアント11のクライアント認証情報送信手段は、サーバの送信する応答信号を受信し、クライアント測定指示送信手段が転送遅延時間測定指示を送信してから応答信号を受信するまでの時間を測定し、測定した時間を転送遅延時間としてサーバへ送信する。例えば、クライアント11は、サーバ12aからのACKとTime2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と、Time3(時刻)をサーバ12aへ送信する。

20

【0044】

サーバ12aの往復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の送信する転送遅延時間を受信する。例えば、サーバ12aは、クライアント11からACKとTime3を受信する。なお、Time1、Time2及びTime3は、例えば、SYNを送信又は受信する際のタイムスタンプである。サーバ12aは、Time1、Time2及びTime3を取得することで、サーバ12a及びクライアント11間の伝送時間を測定することができる。サーバが転送遅延時間測定指示を送信してから応答信号を受信するまでの往復時間を測定するので、クライアント11とサーバとの間で絶対時刻が保証されていなくても、クライアント11とサーバの時計の誤差が相殺し、認証情報としての確度が損なわれない。

30

【0045】

ここで、図3及び図4にて説明した往復転送遅延時間の測定方法の第1例及び第2例において、転送遅延時間測定指示及び応答信号が、TCPレイヤのタイムスタンプを含むことが好ましい。従来の伝送時間の測定では、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伝送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、伝送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、図4のように、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、往復転送遅延時間を測定することができる。

40

【0046】

図2に示す認証情報照合手段23は、往復転送遅延時間取得手段22の取得した往復転送遅延時間を、認証情報記憶手段21に記憶されている往復転送遅延時間と照合する。往復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

50

、往復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、往復転送遅延時間取得手段22の取得する往復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に記憶されている往復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までの往復転送時間を測定するので、認証の確度を高めることができる。

【0047】

図2に示す認証情報更新手段34は、クライアント11までの往復転送遅延時間をあらかじめ定められたタイミングで取得し、認証情報記憶手段21に記憶されている往復転送遅延時間を、取得した往復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。

【0048】

(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。

【0049】

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、往復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、往復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、往復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の取得した往復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。

【0050】

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。

【0051】

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、往復転送遅延時間取得手段22として機能させるための往復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、往復転送遅延時間受信手段26として機能させるための往復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、往復転送遅延時間取得手段22として機能させるための往復転送遅延時間取得ステップと、を順に有する。

10

20

30

40

50

【 0 0 5 2 】

さらに、端末認証方法は、最新転送遅延時間取得手段 3 5 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 3 6 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 3 7 として機能させるための認証情報更新ステップと、を往復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。

【 0 0 5 3 】

クライアント 1 1 からサーバ 1 2 a へアクセスがあると、サーバ 1 2 a の往復転送遅延時間取得手段 2 2 はクライアント 1 1 の往復転送遅延時間を取得する。ここで、往復転送遅延時間は、サーバ 1 2 a が取得した時間又はクライアント 1 1 が取得した時間である。クライアント 1 1 からサーバ 1 2 a へのコネクション設定時に往復転送遅延時間取得手段 2 2 が往復転送遅延時間を取得する。そして、認証情報送信手段 2 4 は、往復転送遅延時間取得手段 2 2 の取得した往復転送遅延時間を、サーバ 1 2 a、1 2 b、1 2 c のうちのあらかじめ定められた認証用サーバ 1 2 b へ送信する。

10

【 0 0 5 4 】

クライアント 1 1 からサーバ 1 2 a へアクセスがあった場合、サーバ 1 2 a は、認証用サーバ 1 2 b 及びサーバ 1 2 c の往復転送遅延時間取得手段 2 2 も、クライアント 1 1 の往復転送遅延時間を取得する。そして、それぞれのサーバ 1 2 a、1 2 b、1 2 c は、取得した往復転送遅延時間を認証用サーバ 1 2 b へ送信する。なお、クライアント 1 1 からサーバ 1 2 a へアクセスがあった旨の他のサーバ 1 2 b 及び 1 2 c への通知は、サーバ 1 2 a がサーバ 1 2 b 及び 1 2 c へ直接通知してもよいし、一旦サーバ 1 2 a から認証用サーバ 1 2 b へ通知した後に認証用サーバ 1 2 b がサーバ 1 2 c へ通知してもよい。

20

【 0 0 5 5 】

一方、認証用サーバ 1 2 b の認証情報記憶手段 2 5 は、クライアント 1 1 までの往復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 2 5 は、サーバ 1 2 a からクライアント 1 1 までの往復転送遅延時間と、サーバ 1 2 b からクライアント 1 1 までの往復転送遅延時間と、サーバ 1 2 c からクライアント 1 1 までの往復転送遅延時間と、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 2 1 と同様に、クライアント 1 1 への情報提供サービスを開始する際に、各サーバ 1 2 a、1 2 b、1 2 c がクライアント 1 1 までの転送遅延時間を取得したものである。

30

【 0 0 5 6 】

認証用サーバ 1 2 b の往復転送遅延時間受信手段 2 6 は、認証情報送信手段 2 4 の送信する往復転送遅延時間を受信する。そして、認証用サーバ 1 2 b の認証情報蓄積手段 2 7 は、往復転送遅延時間受信手段 2 6 の受信した往復転送遅延時間を、認証情報送信手段 2 4 を備えるサーバ 1 2 a、1 2 b、1 2 c ごとに蓄積する。例えば、サーバ 1 2 a から送信された往復転送遅延時間を、サーバ 1 2 a の識別情報と関連付けて記憶する。

【 0 0 5 7 】

認証用サーバ 1 2 b の認証情報照合手段 2 8 は、認証情報蓄積手段 2 7 の蓄積する往復転送遅延時間が 3 つ以上になった場合に、認証情報記憶手段 2 5 を参照して認証情報蓄積手段 2 7 の蓄積しているサーバの往復転送遅延時間を抽出し、抽出した往復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 2 8 は、サーバ 1 2 a、1 2 b、1 2 c の往復転送遅延時間を蓄積すると、認証情報記憶手段 2 5 を参照し、サーバ 1 2 a、1 2 b 及び 1 2 c の往復転送遅延時間を抽出する。認証情報照合手段 2 8 は、認証情報蓄積手段 2 7 の蓄積している往復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 2 8 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。

40

【 0 0 5 8 】

それぞれのサーバ 1 2 a、1 2 b、1 2 c とクライアント 1 1 の往復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往復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 1 2 a、1 2 b、1 2 c とクライアント 1 1 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

50

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、サーバの取得した往復転送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。

【0059】

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までの往復転送遅延時間をあらかじ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の取得した往復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の往復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の送信した往復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が送信して往復転送遅延時間受信手段26が受信した往復転送遅延時間を取得すると、認証情報記憶手段25に記憶されている往復転送遅延時間を、最新転送遅延時間送信手段36の送信した往復転送遅延時間に更新する。

10

【0060】

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12a、12b、12c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。

【0061】

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からのクライアント11までの往復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。

20

【0062】

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る。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る。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。

30

【0063】

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。

【0064】

具体的には、本実施形態においては、サーバ12aは、往復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、往復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、往復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と同じルートを紹介してクライアント11までの往復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のうちのすくなくとも2つのサーバの取得した往復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。

40

50

【 0 0 6 5 】

また、往復転送遅延時間取得手段 2 2 は、クライアント 1 1 までの往復転送遅延時間を複数回取得し、取得した往復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 2 4 は、往復転送遅延時間取得手段 2 2 の算出する平均値を、往復転送遅延時間としてサーバ 1 2 a、1 2 b、1 2 c のうちのあらかじめ定められた認証用サーバへ送信する。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。

【 0 0 6 6 】

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 2 5 として機能させるための認証情報記憶ステップと、往復転送遅延時間取得手段 2 2 として機能させるための往復転送遅延時間取得ステップと、認証情報送信手段 2 4 として機能させるための認証情報送信ステップと、往復転送遅延時間受信手段 2 6 として機能させるための往復転送遅延時間受信ステップと、認証情報蓄積手段 2 7 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 2 8 として機能させるための認証情報照合ステップと、往復転送遅延時間取得手段 2 2 として機能させるための往復転送遅延時間取得ステップと、を順に有する。

【 0 0 6 7 】

さらに、端末認証方法は、最新転送遅延時間取得手段 3 5 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 3 6 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 3 7 として機能させるための認証情報更新ステップと、を往復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。

【 0 0 6 8 】

認証用サーバ 1 2 b の認証情報記憶手段 2 5 は、通信ネットワーク内に接続されているサーバ 1 2 a、1 2 b、1 2 c 及びクライアント 1 1 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 1 2 a、1 2 b、1 2 c 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 1 1 との往復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 1 2 a、1 2 b、1 2 c の仮想位置は、例えば、サーバ 1 2 a、1 2 b、1 2 c の配置されている実際の地図上の位置である。クライアント 1 1 の仮想位置の登録時に、それぞれのサーバ 1 2 a、1 2 b、1 2 c からクライアント 1 1 までの往復転送遅延時間を測定し、サーバ 1 2 a、1 2 b、1 2 c からの往復転送遅延時間によって特定される位置を、クライアント 1 1 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。

【 0 0 6 9 】

認証用サーバ 1 2 b の認証情報照合手段 2 8 は、認証情報蓄積手段 2 7 の蓄積した往復転送遅延時間が 2 つ以上になった場合に、認証情報記憶手段 2 5 を参照して認証情報蓄積手段 2 7 の蓄積しているサーバ 1 2 a、1 2 b、1 2 c の位置を抽出し、抽出した位置と往復転送遅延時間とから、認証情報蓄積手段 2 7 の蓄積しているクライアント 1 1 の位置を算出する。例えば、認証情報照合手段 2 8 は、サーバ 1 2 a、1 2 b 及び 1 2 c の往復転送遅延時間から距離を算出して、サーバ 1 2 a、1 2 b 及び 1 2 c 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 1 1 の位置を特定する。ここで、往復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、予め定められ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 2 8 は、算出したサーバ 1 2 a、1 2 b 及び 1 2 c の位置を、認証情報記憶手段 2 5 に記憶されている位置と照合する。往復転送遅延時間は通信ネットワーク 1 0 の通信環境に応じて変化するので、認証情報照合手段 2 8 は、例えば、通信ネットワーク 1 0 の通信環境ごとに予め誤差の

10

20

30

40

50

範囲を定め、その誤差の範囲内にあることで照合を行う。

【0070】

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しておくことで、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が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。

10

【0071】

さらに、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往復転送遅延時間と、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の往復転送遅延時間からのク

20

【実施例】

【0072】

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。

【0073】

(転送遅延時間測定方式の実施例1)

30

サーバ12aとクライアント11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、転送遅延をサーバから測定する方式と、クライアント11から転送遅延を測定して、結果をサーバ12aに転送する方式がある。

【0074】

(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、転送遅延をサーバ12aから測定する方式と、クライアント11から転送遅延を測定して、結果をサーバ12aに転送する方式とがある。

40

【0075】

(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、トラフィックがあらかじ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

50

いる状態のときに、転送遅延を測定する。この場合、転送遅延をサーバ12aから測定する方式と、クライアント11から転送遅延を測定して、結果をサーバ12aに転送する方式がある。

【0076】

(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。

10

【0077】

(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、トラフィックがあらかじ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。

20

【0078】

(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間のトラフィックを順次測定しながら、トラフィックがあらかじ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。

30

【産業上の利用可能性】

【0079】

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】

【0080】

【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。

40

【図2】サーバの機能の一例を示す概略構成図である。

【図3】往復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】往復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】

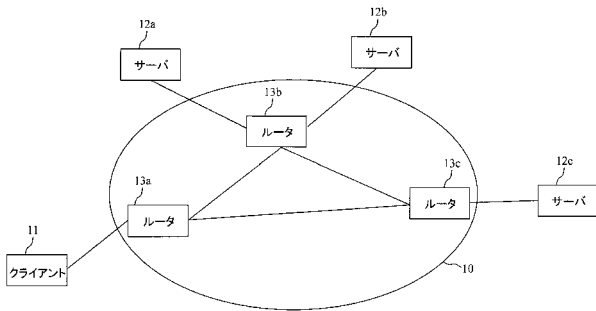
【0081】

- 10 通信ネットワーク
- 11 クライアント
- 12 サーバ

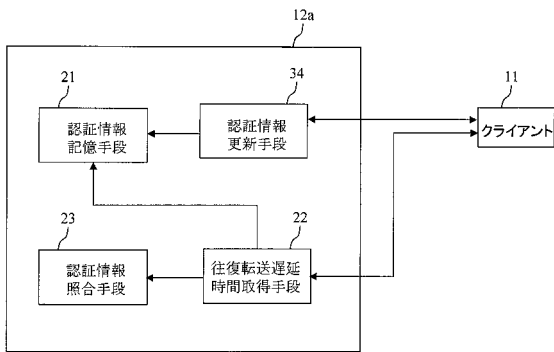
50

- 1 3 ルー タ
- 2 1 認 証 情 報 記 憶 手 段
- 2 2 往 復 転 送 遅 延 時 間 取 得 手 段
- 2 3 認 証 情 報 照 合 手 段
- 2 4 認 証 情 報 送 信 手 段
- 2 5 認 証 情 報 記 憶 手 段
- 2 6 往 復 転 送 遅 延 時 間 受 信 手 段
- 2 7 認 証 情 報 蓄 積 手 段
- 2 8 認 証 情 報 照 合 手 段
- 3 4 認 証 情 報 更 新 手 段
- 3 5 最 新 転 送 遅 延 時 間 取 得 手 段
- 3 6 最 新 転 送 遅 延 時 間 送 信 手 段
- 3 7 認 証 情 報 更 新 手 段

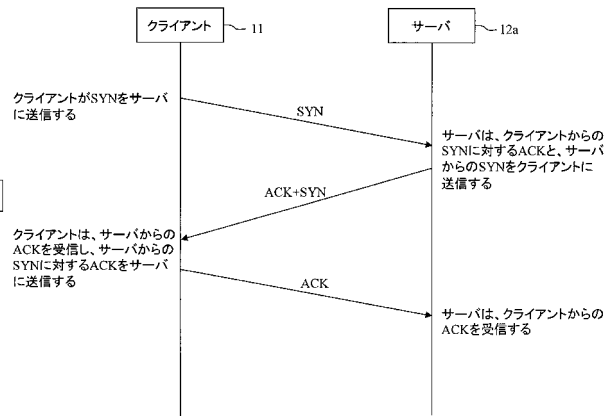
【 図 1 】



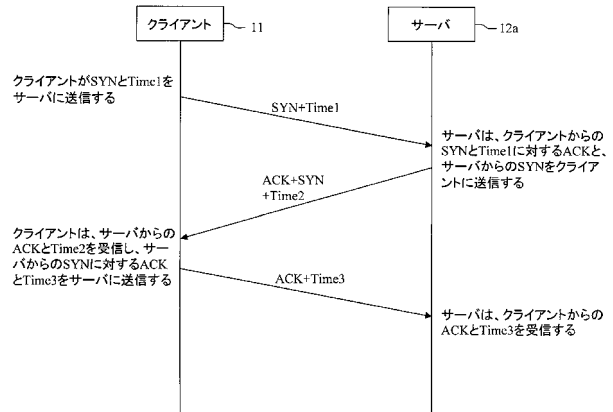
【 図 2 】



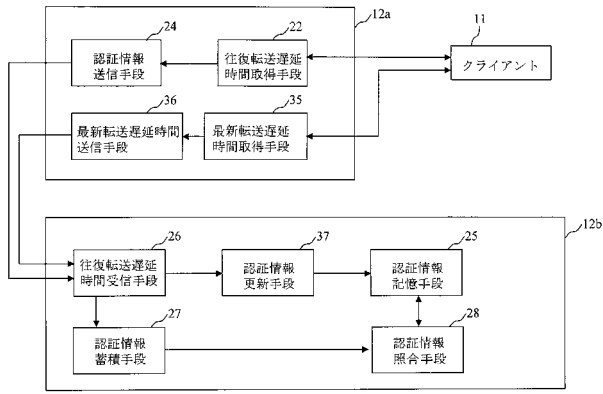
【 図 3 】



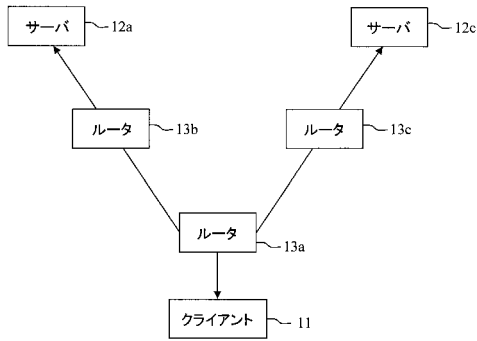
【 図 4 】



【図5】



【図6】



フロントページの続き

審査官 戸島 弘詩

- (56)参考文献 特開2004-295337(JP,A)
特開平10-032806(JP,A)
特開2005-295297(JP,A)
特開2003-215228(JP,A)
特開2006-197458(JP,A)
特表2003-533927(JP,A)
特開2004-304755(JP,A)
特開2006-324736(JP,A)

(58)調査した分野(Int.Cl., DB名)

G06F21/00-21/24
G09C1/00-5/00
H04K1/00
H04L9/00
H04N7/10, 7/14-7/173, 7/20-7/22
H04B7/24-7/26
H04L12/00-12/28, 12/44-12/66
H04W4/00-99/00