(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5875051号
(P5875051)
(45)発行日　平成28年3月2日(2016.3.2)　(24)登録日　平成28年1月29日(2016.1.29)

(51)Int.Cl.　　F I
H04L 9/32 (2006.01)　　H04L 9/00 673D
H04W 12/06 (2009.01)　　H04W 12/06

請求項の数 24　(全 42 頁)

(21)出願番号	特願2012-542884 (P2012-542884)
(86)(22)出願日	平成23年11月2日 (2011.11.2)
(86)国際出願番号	PCT/JP2011/075277
(87)国際公開番号	WO2012/063699
(87)国際公開日	平成24年5月18日 (2012.5.18)
審査請求日	平成26年10月27日 (2014.10.27)
(31)優先権主張番号	特願2011-117429 (P2011-117429)
(32)優先日	平成23年5月25日 (2011.5.25)
(33)優先権主張国	日本国(JP)
(31)優先権主張番号	特願2010-250290 (P2010-250290)
(32)優先日	平成22年11月8日 (2010.11.8)
(33)優先権主張国	日本国(JP)
(31)優先権主張番号	特願2010-250292 (P2010-250292)
(32)優先日	平成22年11月8日 (2010.11.8)
(33)優先権主張国	日本国(JP)

(73)特許権者　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
(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
(72)発明者　土屋　貴寛
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
審査官　金沢　史明

最終頁に続く

(54)【発明の名称】認証サーバ及び認証サーバによる認証方法

(57)【特許請求の範囲】
【請求項１】
コンテンツの閲覧のための認証を行う通信端末とデータ通信を行うデータ通信部と、
前記データ通信部及び前記通信端末の間の伝送遅延時間を複数回にわたり測定する伝送遅延時間測定部と、
複数回にわたり測定された前記伝送遅延時間の分布特性が離散的であるかどうかを判断する伝送遅延時間分布特性判断部と、
前記伝送遅延時間の分布特性が離散的であると判断されたときに、前記コンテンツの閲覧を承認し、前記伝送遅延時間の分布特性が離散的でないと判断されたときに、前記コンテンツの閲覧を拒否するコンテンツ閲覧認証部と、
を備えることを特徴とする認証サーバ。
【請求項２】
前記データ通信部は、前記通信端末に複数のデータ要素を包含するＨＴＭＬファイルを送信し、前記通信端末から各データ要素を要求する要求信号を受信し、
前記伝送遅延時間測定部は、前記通信端末から各データ要素を要求する要求信号が受信された間隔を測定することにより、前記データ通信部から前記通信端末までの伝送遅延時間及び前記通信端末から前記データ通信部までの伝送遅延時間の合計を測定することを特徴とする、請求項１に記載の認証サーバ。
【請求項３】
前記データ通信部は、１つの前記要求信号の受信と１つの前記データ要素の送信を順に

繰り返し、
前記伝送遅延時間測定部は、各々の前記要求信号が受信された間隔を測定することにより前記伝送遅延時間の合計を測定することを特徴とする、請求項２に記載の認証サーバ。
【請求項４】
前記データ通信部は、前記データ要素を受信した前記通信端末からコネクションのクローズ信号を受信し、
前記伝送遅延時間測定部は、前記要求信号を受信してから前記クローズ信号を受信するまでの時間間隔を測定することにより、前記データ通信部から前記通信端末までの伝送遅延時間及び前記通信端末から前記データ通信部までの伝送遅延時間の合計を測定することを特徴とする、請求項１に記載の認証サーバ。
【請求項５】
前記データ通信部は、前記通信端末に対して電話通信を行い、
前記コンテンツ閲覧認証部は、前記伝送遅延時間の分布特性が離散的であると判断されたうえに、前記電話通信に対し前記通信端末から着信応答がなされたときに、前記コンテンツの閲覧を承認し、前記伝送遅延時間の分布特性が離散的であると判断されたところ、前記電話通信に対し前記通信端末から着信応答がなされなかったときに、前記コンテンツの閲覧を拒否することを特徴とする、請求項１から４のいずれかに記載の認証サーバ。
【請求項６】
前記データ通信部は、前記通信端末に対して電話通信を行い、
前記コンテンツ閲覧認証部は、前記伝送遅延時間の分布特性が離散的であると判断されたうえに、前記電話通信に対し前記伝送遅延時間の分布特性が変化したときに、前記コンテンツの閲覧を承認し、前記伝送遅延時間の分布特性が離散的であると判断されたところ、前記電話通信に対し前記伝送遅延時間の分布特性が変化しなかったときに、前記コンテンツの閲覧を拒否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認証サーバ。
【請求項７】
通信端末の行うコンテンツの閲覧のための認証を受け付けるコンテンツ閲覧認証受付ステップと、
前記通信端末との間の伝送遅延時間を複数回にわたり測定する伝送遅延時間測定ステップと、
複数回にわたり測定された前記伝送遅延時間の分布特性が離散的であるかどうかを判断する伝送遅延時間分布特性判断ステップと、
前記伝送遅延時間の分布特性が離散的であると判断されたときに、前記コンテンツの閲覧を承認し、前記伝送遅延時間の分布特性が離散的でないと判断されたときに、前記コンテンツの閲覧を拒否するコンテンツ閲覧認証ステップと、
を順に備えることを特徴とする認証サーバによる認証方法。
【請求項８】
前記伝送遅延時間測定ステップは、前記通信端末に複数のデータ要素を包含するＨＴＭＬファイルを送信し、前記通信端末から各データ要素を要求する要求信号を受信し、前記通信端末から各データ要素を要求する要求信号が受信された間隔を測定することにより、前記認証サーバから前記通信端末までの伝送遅延時間及び前記通信端末から前記認証サーバまでの伝送遅延時間の合計を測定することを特徴とする、請求項７に記載の認証サーバによる認証方法。
【請求項９】
前記伝送遅延時間測定ステップは、１つの前記要求信号の受信と１つの前記データ要素の送信を順に繰り返し、各々の前記要求信号が受信された間隔を測定することにより前記伝送遅延時間の合計を測定することを特徴とする、請求項８に記載の認証サーバによる認証方法。
【請求項１０】
前記伝送遅延時間測定ステップは、前記データ要素を受信した前記通信端末からコネク

ションのクローズ信号を受信し、前記要求信号を受信してから前記クローズ信号を受信するまでの時間間隔を測定することにより、前記データ通信部から前記通信端末までの伝送遅延時間及び前記通信端末から前記データ通信部までの伝送遅延時間の合計を測定することを特徴とする、請求項７に記載の認証サーバによる認証方法。

【請求項１１】

前記コンテンツ閲覧認証ステップは、前記通信端末に対して電話通信を行い、前記伝送遅延時間の分布特性が離散的であると判断されたうえに、前記電話通信に対し前記通信端末から着信応答がなされたときに、前記コンテンツの閲覧を承認し、前記伝送遅延時間の分布特性が離散的であると判断されたところ、前記電話通信に対し前記通信端末から着信応答がなされなかったときに、前記コンテンツの閲覧を拒否することを特徴とする、請求項７から１０のいずれかに記載の認証サーバによる認証方法。

【請求項１２】

前記コンテンツ閲覧認証ステップは、前記通信端末に対して電話通信を行い、前記伝送遅延時間の分布特性が離散的であると判断されたうえに、前記電話通信に対し前記伝送遅延時間の分布特性が変化したときに、前記コンテンツの閲覧を承認し、前記伝送遅延時間の分布特性が離散的であると判断されたところ、前記電話通信に対し前記伝送遅延時間の分布特性が変化しなかったときに、前記コンテンツの閲覧を拒否することを特徴とする、請求項７から１１のいずれかに記載の認証サーバによる認証方法。

【請求項１３】

コンテンツの閲覧のための認証を行う通信端末とデータ通信を行うデータ通信部と、

前記データ通信部及び前記通信端末の間の伝送遅延時間を複数回にわたり測定する伝送遅延時間測定部と、

前記伝送遅延時間測定部の測定した伝送遅延時間を蓄積して伝送遅延時間のピーク値を検出し、各ピーク値を含む一定範囲内の伝送遅延時間を抽出する抽出部と、

前記抽出部の抽出した伝送遅延時間の分布特性を算出する分布特性算出部と、

前記分布特性算出部の算出した伝送遅延時間の分布特性が離散的であるか否かを判定する分布特性判定部と、

前記分布特性判定部が離散的であると判定すると前記コンテンツの閲覧を承認し、前記分布特性判定部が離散的でないと判定すると前記コンテンツの閲覧を拒否するコンテンツ閲覧認証部と、

を備えることを特徴とする認証サーバ。

【請求項１４】

前記データ通信部は、前記通信端末に複数のデータ要素を包含するＨＴＭＬファイルを送信し、前記通信端末から各データ要素を要求する要求信号を受信し、

前記伝送遅延時間測定部は、前記通信端末から各データ要素を要求する要求信号が受信された間隔を測定することにより、前記データ通信部から前記通信端末までの伝送遅延時間を測定することを特徴とする、請求項１３に記載の認証サーバ。

【請求項１５】

前記データ通信部は、１つの前記要求信号の受信と１つの前記データ要素の送信を順に繰り返し、

前記伝送遅延時間測定部は、各々の前記要求信号が受信された間隔を測定することにより前記伝送遅延時間の合計を測定することを特徴とする、請求項１４に記載の認証サーバ。

【請求項１６】

前記データ通信部は、前記データ要素を受信した前記通信端末からコネクションのクローズ信号を受信し、

前記伝送遅延時間測定部は、前記要求信号を受信してから前記クローズ信号を受信するまでの時間間隔を測定することにより、前記データ通信部から前記通信端末までの伝送遅延時間及び前記通信端末から前記データ通信部までの伝送遅延時間の合計を測定することを特徴とする、請求項１３に記載の認証サーバ。

【請求項１７】
前記データ通信部は、前記通信端末に対して電話通信を行い、
前記データ通信部が前記通信端末から着信応答を受信したか否かを判定する通話判定部をさらに備え、
前記コンテンツ閲覧認証部は、前記分布特性判定部において離散的であると判定しかつ前記通話判定部において着信応答を受信したと判定した場合に前記コンテンツの閲覧を承認し、前記分布特性判定部において離散的でないと判定するか又は前記通話判定部において着信応答を受信しないと判定した場合に前記コンテンツの閲覧を拒否することを特徴とする、請求項１３から１６のいずれかに記載の認証サーバ。
【請求項１８】
前記データ通信部は、前記通信端末に対して電話通信を行い、
前記データ通信部による電話通信を検出すると、前記分布特性算出部の算出する伝送遅延時間の分布特性が変化したか否かを判定する通話変化判定部をさらに備え、
前記コンテンツ閲覧認証部は、前記分布特性判定部において離散的であると判定しかつ前記通話変化判定部において伝送遅延時間の分布特性が変化したと判定した場合に前記コンテンツの閲覧を承認し、前記分布特性判定部において離散的でないと判定するか又は前記通話変化判定部において伝送遅延時間の分布特性が変化しなかったと判定した場合に前記コンテンツの閲覧を拒否することを特徴とする、請求項１３から１７のいずれかに記載の認証サーバ。
【請求項１９】
データ通信部が、コンテンツの閲覧のための認証を行う通信端末とデータ通信を行い、伝送遅延時間測定部が、前記通信端末との間の伝送遅延時間を複数回にわたり測定し、抽出部が、伝送遅延時間を蓄積して伝送遅延時間のピーク値を検出し、各ピーク値を含む一定範囲内の伝送遅延時間を抽出し、分布特性算出部が、抽出された伝送遅延時間の分布特性を算出し、分布特性判定部が、算出した分布特性が離散的であるか否かを判定する分布特性判定ステップと、
前記分布特性判定ステップにおいて離散的であると判定されると前記コンテンツの閲覧を承認し、前記分布特性判定ステップにおいて離散的でないと判定されると前記コンテンツの閲覧を拒否するコンテンツ閲覧認証ステップと、
を順に有することを特徴とする認証サーバによる認証方法。
【請求項２０】
前記分布特性判定ステップにおいて、前記伝送遅延時間測定部が、前記通信端末に複数のデータ要素を包含するＨＴＭＬファイルを送信し、前記通信端末から各データ要素を要求する要求信号を受信し、前記通信端末から各データ要素を要求する要求信号が受信された間隔を測定することにより、前記認証サーバから前記通信端末までの伝送遅延時間を測定することを特徴とする、
請求項１９に記載の認証サーバによる認証方法。
【請求項２１】
前記分布特性判定ステップにおいて、１つの前記要求信号の受信と１つの前記データ要素の送信を順に繰り返し、各々の前記要求信号が受信された間隔を測定することにより前記伝送遅延時間の合計を測定することを特徴とする、請求項２０に記載の認証サーバによる認証方法。
【請求項２２】
前記分布特性判定ステップにおいて、前記データ要素を受信した前記通信端末からコネクションのクローズ信号を受信し、前記要求信号を受信してから前記クローズ信号を受信するまでの時間間隔を測定することにより、前記データ通信部から前記通信端末までの伝送遅延時間及び前記通信端末から前記データ通信部までの伝送遅延時間の合計を測定することを特徴とする、請求項１９に記載の認証サーバによる認証方法。
【請求項２３】
前記データ通信部が、前記通信端末に対して電話通信を行い、通話判定部が、前記デー

タ通信部が前記通信端末から着信応答を受信したか否かを判定する通話判定ステップを、前記分布特性判定ステップの前、前記分布特性判定ステップと同時又は前記分布特性判定ステップと前記コンテンツ閲覧認証ステップの間にさらに有し、

前記コンテンツ閲覧認証ステップにおいて、前記コンテンツ閲覧認証部は、前記分布特性判定ステップにおいて離散的であると判定しかつ前記通話判定ステップにおいて着信応答を受信したと判定した場合に前記コンテンツの閲覧を承認し、前記分布特性判定ステップにおいて離散的でないと判定するか又は前記通話判定ステップにおいて着信応答を受信しないと判定した場合に前記コンテンツの閲覧を拒否することを特徴とする、

請求項１９から２２のいずれかに記載の認証サーバによる認証方法。

【請求項２４】

前記データ通信部が、前記通信端末に対して電話通信を行い、通話変化判定部が、前記データ通信部による電話通信の後に、前記分布特性算出部の算出する伝送遅延時間の分布特性が変化したか否かを判定する通話変化判定ステップを、前記分布特性判定ステップの前、前記分布特性判定ステップと同時又は前記分布特性判定ステップと前記コンテンツ閲覧認証ステップの間にさらに有し、

前記コンテンツ閲覧認証ステップにおいて、前記コンテンツ閲覧認証部は、前記分布特性判定ステップにおいて離散的であると判定しかつ前記通話変化判定ステップにおいて伝送遅延時間の分布特性が変化したと判定した場合に前記コンテンツの閲覧を承認し、前記分布特性判定ステップにおいて離散的でないと判定するか又は前記通話変化判定ステップにおいて伝送遅延時間の分布特性が変化しなかったと判定した場合に前記コンテンツの閲覧を拒否することを特徴とする、請求項１９から２３のいずれかに記載の認証サーバによる認証方法。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、携帯電話のユーザに限定してコンテンツを閲覧させるにあたり、コンピュータから閲覧させることを防止し、携帯電話から閲覧させることを承認する認証サーバ及び認証サーバによる認証方法に関する。

【背景技術】

【０００２】

携帯電話のユーザに限定してコンテンツを閲覧させるにあたり、コンピュータから閲覧させることを防止し、携帯電話から閲覧させることを承認する必要がある。従来技術では、アクセス元のＩＰアドレスを参照することにより、アクセス元が携帯電話及びコンピュータのうちいずれであるかを判断している。

【先行技術文献】

【特許文献】

【０００３】

【特許文献１】特開２００５－２９５２９７号公報

【特許文献２】特開２００７－８９０６５号公報

【発明の概要】

【発明が解決しようとする課題】

【０００４】

しかし、ＩＰアドレスは、コンピュータにより偽装される可能性があり、携帯電話会社により変更される可能性がある。よって、アクセス元が携帯電話及びコンピュータのうちいずれであるかを、安全にかつ正確に判断することができなかった。

【０００５】

特許文献１及び特許文献２では、２個の通信端末の間での伝送遅延時間を測定し、当該２個の通信端末の間の距離を測定することにより、当該２個の通信端末のうち一方の通信端末が他方の通信端末を認証している。しかし、他方の通信端末が携帯電話及びコンピュータのうちいずれであるかを判断しているわけではない。

【０００６】
そこで、本課題を解決するために、第１の発明は、携帯電話のユーザに限定してコンテンツを閲覧させるにあたり、アクセス元が携帯電話及びコンピュータのうちいずれであるかを、安全にかつ正確に判断することができる認証サーバ及び認証サーバによる認証方法を提供することを第１の目的とする。
【０００７】
一方、近年では、コンピュータと同様な機能を有するスマートフォンと呼ばれる携帯電話が普及しており、スマートフォンは通常のインターネットを利用している。しかし、通常のインターネット内で生成されるＩＤを参照することによっては、通常のインターネット内で生成されるＩＤは安全性の高い固有のＩＤではないため、携帯電話のユーザが正規のユーザであるかどうかを安全にかつ正確に判断することができなかった。
【０００８】
特許文献１及び特許文献２では、２個の通信端末の間での伝送遅延時間を測定し、当該２個の通信端末の間の距離を測定することにより、当該２個の通信端末のうち一方の通信端末が他方の通信端末を認証している。しかし、当該２個の通信端末の間の距離によらず、他方の通信端末のユーザが正規のユーザであるかどうかを判断しているわけではない。
【０００９】
そこで、本課題を解決するために、第２の発明は、携帯電話のユーザに限定してコンテンツを閲覧させるときに、携帯電話のユーザが正規のユーザであるかどうかを安全にかつ正確に判断することができる認証サーバ及び認証サーバによる認証方法を提供することを第２の目的とする。
【課題を解決するための手段】
【００１０】
上記第１の目的を達成するために、認証サーバ及び通信端末の間の伝送遅延時間の分布特性が離散的であるかどうかに基づいて、通信端末が携帯電話などの無線通信端末であるかコンピュータなどの有線通信端末であるかを判断することとした。
【００１１】
具体的には、本第１の発明は、コンテンツの閲覧のための認証を行う通信端末とデータ通信を行うデータ通信部と、前記データ通信部及び前記通信端末の間の伝送遅延時間を複数回にわたり測定する伝送遅延時間測定部と、複数回にわたり測定された前記伝送遅延時間の分布特性が離散的であるかどうかを判断する伝送遅延時間分布特性判断部と、前記伝送遅延時間の分布特性が離散的であると判断されたときに、前記コンテンツの閲覧を承認し、前記伝送遅延時間の分布特性が離散的でないと判断されたときに、前記コンテンツの閲覧を拒否するコンテンツ閲覧認証部と、を備えることを特徴とする認証サーバである。
【００１２】
この構成によれば、携帯電話のユーザに限定してコンテンツを閲覧させるにあたり、アクセス元が携帯電話及びコンピュータのうちいずれであるかを、安全にかつ正確に判断することができる。上述の判断はアクセス元が行うのではなく認証サーバが行うため、コンピュータにより上述の分布特性が偽装されるおそれがない。
【００１３】
また、本第１の発明は、前記データ通信部は、前記通信端末に複数のデータ要素を包含するＨＴＭＬファイルを送信し、前記通信端末から各データ要素を要求する要求信号を受信し、前記伝送遅延時間測定部は、前記通信端末から各データ要素を要求する要求信号が受信された間隔を測定することにより、前記データ通信部から前記通信端末までの伝送遅延時間及び前記通信端末から前記データ通信部までの伝送遅延時間の合計を測定することを特徴とする認証サーバである。
【００１４】
この構成によれば、アクセス元は、ウェブブラウザを有していればよく、伝送遅延時間の測定用のソフトウェアを有していなくてもよい。
【００１５】

ここで、前記データ通信部は、１つの前記要求信号の受信と１つの前記データ要素の送信を順に繰り返し、前記伝送遅延時間測定部は、各々の前記要求信号が受信された間隔を測定することにより前記伝送遅延時間の合計を測定してもよい。

この構成によれば、パイプライン処理を行う通信端末であっても、通信端末から各データ要素を要求する要求信号が受信された間隔を測定することにより、前記データ通信部から前記通信端末までの伝送遅延時間及び前記通信端末から前記データ通信部までの伝送遅延時間の合計を測定することができる。

【００１６】

また、本第１の発明は、前記データ通信部は、前記データ要素を受信した前記通信端末からコネクションのクローズ信号を受信し、前記伝送遅延時間測定部は、前記要求信号を受信してから前記クローズ信号を受信するまでの時間間隔を測定することにより、前記データ通信部から前記通信端末までの伝送遅延時間及び前記通信端末から前記データ通信部までの伝送遅延時間の合計を測定する認証サーバである。

この構成によれば、専用のソフトウェアを用いずに伝送遅延時間の測定を行うことができる。さらに、通信端末とのコネクションを用いるため、複数の通信端末との伝送遅延時間を平行して測定することができる。

【００１７】

また、本第１の発明は、前記データ通信部は、前記通信端末に対して電話通信を行い、前記コンテンツ閲覧認証部は、前記伝送遅延時間の分布特性が離散的であると判断されたうえに、前記電話通信に対し前記通信端末から着信応答がなされたときに、前記コンテンツの閲覧を承認し、前記伝送遅延時間の分布特性が離散的であると判断されたところ、前記電話通信に対し前記通信端末から着信応答がなされなかったときに、前記コンテンツの閲覧を拒否することを特徴とする認証サーバである。

【００１８】

この構成によれば、実際にはアクセス元がコンピュータのデータモジュールであるところ、アクセス元が携帯電話であると判断することを確実に防止することができる。

【００１９】

また、本第１の発明は、通信端末の行うコンテンツの閲覧のための認証を受け付けるコンテンツ閲覧認証受付ステップと、前記通信端末との間の伝送遅延時間を複数回にわたり測定する伝送遅延時間測定ステップと、複数回にわたり測定された前記伝送遅延時間の分布特性が離散的であるかどうかを判断する伝送遅延時間分布特性判断ステップと、前記伝送遅延時間の分布特性が離散的であると判断されたときに、前記コンテンツの閲覧を承認し、前記伝送遅延時間の分布特性が離散的でないと判断されたときに、前記コンテンツの閲覧を拒否するコンテンツ閲覧認証ステップと、を順に備えることを特徴とする認証サーバによる認証方法である。

【００２０】

この構成によれば、携帯電話のユーザに限定してコンテンツを閲覧させるにあたり、アクセス元が携帯電話及びコンピュータのうちいずれであるかを、安全にかつ正確に判断することができる。上述の判断はアクセス元が行うのではなく認証サーバが行うため、コンピュータにより上述の分布特性が偽装されるおそれがない。

【００２１】

また、本第１の発明は、前記伝送遅延時間測定ステップは、前記通信端末に複数のデータ要素を包含するＨＴＭＬファイルを送信し、前記通信端末から各データ要素を要求する要求信号を受信し、前記通信端末から各データ要素を要求する要求信号が受信された間隔を測定することにより、前記認証サーバから前記通信端末までの伝送遅延時間及び前記通信端末から前記認証サーバまでの伝送遅延時間の合計を測定することを特徴とする認証サーバによる認証方法である。

【００２２】

この構成によれば、アクセス元は、ウェブブラウザを有していればよく、伝送遅延時間の測定用のソフトウェアを有していなくてもよい。

【００２３】
ここで、前記伝送遅延時間測定ステップは、１つの前記要求信号の受信と１つの前記データ要素の送信を順に繰り返し、各々の前記要求信号が受信された間隔を測定することにより前記伝送遅延時間の合計を測定してもよい。
本発明により、パイプライン処理を行う通信端末であっても、通信端末から各データ要素を要求する要求信号が受信された間隔を測定することにより、前記データ通信部から前記通信端末までの伝送遅延時間及び前記通信端末から前記データ通信部までの伝送遅延時間の合計を測定することができる。
【００２４】
また、本第１の発明は、前記伝送遅延時間測定ステップは、前記データ要素を受信した前記通信端末からコネクションのクローズ信号を受信し、前記要求信号を受信してから前記クローズ信号を受信するまでの時間間隔を測定することにより、前記データ通信部から前記通信端末までの伝送遅延時間及び前記通信端末から前記データ通信部までの伝送遅延時間の合計を測定する認証サーバによる認証方法である。
この構成によれば、専用のソフトウェアを用いずに伝送遅延時間の測定を行うことができる。さらに、通信端末とのコネクションを用いるため、複数の通信端末との伝送遅延時間を平行して測定することができる。
【００２５】
また、本第１の発明は、前記コンテンツ閲覧認証ステップは、前記通信端末に対して電話通信を行い、前記伝送遅延時間の分布特性が離散的であると判断されたうえに、前記電話通信に対し前記通信端末から着信応答がなされたときに、前記コンテンツの閲覧を承認し、前記伝送遅延時間の分布特性が離散的であると判断されたところ、前記電話通信に対し前記通信端末から着信応答がなされなかったときに、前記コンテンツの閲覧を拒否することを特徴とする認証サーバによる認証方法である。
【００２６】
この構成によれば、実際にはアクセス元がコンピュータのデータモジュールであるところ、アクセス元が携帯電話であると判断することを確実に防止することができる。
【００２７】
本第１の発明に係る認証サーバでは、前記データ通信部は、前記通信端末に対して電話通信を行い、前記コンテンツ閲覧認証部は、前記伝送遅延時間の分布特性が離散的であると判断されたうえに、前記電話通信に対し前記伝送遅延時間の分布特性が変化したときに、前記コンテンツの閲覧を承認し、前記伝送遅延時間の分布特性が離散的であると判断されたところ、前記電話通信に対し前記伝送遅延時間の分布特性が変化しなかったときに、前記コンテンツの閲覧を拒否してもよい。
コンテンツ閲覧認証部が電話通信に対し伝送遅延時間の分布特性が変化したか否かを判定するため、本第１の発明に係る認証サーバは、通信端末が通話機能を有する無線通信端末であることを確認することができる。そして、コンテンツ閲覧認証部が通信端末が通話機能を有する無線通信端末であることを確認した上でコンテンツの提供の認証を行うため、アクセス元が移動通信端末及びコンピュータのうちいずれであるかを、より安全にかつ正確に判断することができる。
【００２８】
本第１の発明に係る認証サーバによる認証方法では、前記コンテンツ閲覧認証ステップは、前記通信端末に対して電話通信を行い、前記伝送遅延時間の分布特性が離散的であると判断されたうえに、前記電話通信に対し前記伝送遅延時間の分布特性が変化したときに、前記コンテンツの閲覧を承認し、前記伝送遅延時間の分布特性が離散的であると判断されたところ、前記電話通信に対し前記伝送遅延時間の分布特性が変化しなかったときに、前記コンテンツの閲覧を拒否してもよい。
コンテンツ閲覧認証ステップにおいて電話通信に対し伝送遅延時間の分布特性が変化したか否かを判定するため、本第１の発明に係る認証サーバによる認証方法は、通信端末が通話機能を有する無線通信端末であることを確認することができる。そして、コンテンツ

閲覧認証ステップにおいて通信端末が通話機能を有する無線通信端末であることを確認した上でコンテンツの提供の認証を行うため、アクセス元が移動通信端末及びコンピュータのうちいずれであるかを、より安全にかつ正確に判断することができる。

【００２９】

具体的には、本第１の発明に係る認証サーバは、コンテンツの閲覧のための認証を行う通信端末とデータ通信を行うデータ通信部と、前記データ通信部及び前記通信端末の間の伝送遅延時間を複数回にわたり測定する伝送遅延時間測定部と、前記伝送遅延時間測定部の測定した伝送遅延時間を蓄積して伝送遅延時間のピーク値を検出し、各ピーク値を含む一定範囲内の伝送遅延時間を抽出する抽出部と、前記抽出部の抽出した伝送遅延時間の分布特性を算出する分布特性算出部と、前記分布特性算出部の算出した伝送遅延時間の分布特性が離散的であるか否かを判定する分布特性判定部と、前記分布特性判定部が離散的であると判定すると前記コンテンツの閲覧を承認し、前記分布特性判定部が離散的でないと判定すると前記コンテンツの閲覧を拒否するコンテンツ閲覧認証部と、を備える。

【００３０】

本第１の発明に係る認証サーバは、データ通信部と、伝送遅延時間測定部と、抽出部と、分布特性算出部と、分布特性判定部と、を備えるため、通信端末が無線通信端末であるのか又は有線通信端末であるのかを判定することができる。本第１の発明に係る認証サーバは、コンテンツ閲覧認証部を備えるため、通信端末が無線通信端末である場合には通信端末へのコンテンツの提供を可能にし、通信端末が有線通信端末である場合には通信端末へのコンテンツの提供を阻止することができる。これにより、本第１の発明に係る認証サーバは、アクセス元が移動通信端末及びコンピュータのうちいずれであるかを判断することができる。ここで、本第１の発明に係る認証サーバは、認証を認証サーバが行うため、判断を安全にかつ正確に行うことができる。したがって、本第１の発明は、移動通信端末のユーザに限定してコンテンツを閲覧させるにあたり、アクセス元が移動通信端末及びコンピュータのうちいずれであるかを、安全にかつ正確に判断することができる。

【００３１】

本第１の発明に係る認証サーバでは、前記データ通信部は、前記通信端末に複数のデータ要素を包含するＨＴＭＬファイルを送信し、前記通信端末から各データ要素を要求する要求信号を受信し、前記伝送遅延時間測定部は、前記通信端末から各データ要素を要求する要求信号が受信された間隔を測定することにより、前記データ通信部から前記通信端末までの伝送遅延時間を測定してもよい。

本第１の発明によれば、通信端末にウェブブラウザへのアクセスを行わせるだけで認証を行うことができるため、伝送遅延時間の測定用の特別なソフトウェアを通信端末に搭載させる必要がない。このため、容易に認証を行うことができる。

【００３２】

ここで、前記データ通信部は、１つの前記要求信号の受信と１つの前記データ要素の送信を順に繰り返し、前記伝送遅延時間測定部は、各々の前記要求信号が受信された間隔を測定することにより前記伝送遅延時間の合計を測定してもよい。

本発明により、パイプライン処理を行う通信端末であっても、通信端末から各データ要素を要求する要求信号が受信された間隔を測定することにより、前記データ通信部から前記通信端末までの伝送遅延時間及び前記通信端末から前記データ通信部までの伝送遅延時間の合計を測定することができる。

【００３３】

また、本第１の発明は、前記データ通信部は、前記データ要素を受信した前記通信端末からコネクションのクローズ信号を受信し、前記伝送遅延時間測定部は、前記要求信号を受信してから前記クローズ信号を受信するまでの時間間隔を測定することにより、前記データ通信部から前記通信端末までの伝送遅延時間及び前記通信端末から前記データ通信部までの伝送遅延時間の合計を測定する認証サーバである。

この構成によれば、専用のソフトウェアを用いずに伝送遅延時間の測定を行うことができる。さらに、通信端末とのコネクションを用いるため、複数の通信端末との伝送遅延時

間を平行して測定することができる。

【００３４】

本第１の発明に係る認証サーバでは、前記データ通信部は、前記通信端末に対して電話通信を行い、前記データ通信部が前記通信端末から着信応答を受信したか否かを判定する通話判定部をさらに備え、前記コンテンツ閲覧認証部は、前記分布特性判定部において離散的であると判定しかつ前記通話判定部において着信応答を受信したと判定した場合に前記コンテンツの閲覧を承認し、前記分布特性判定部において離散的でないと判定するか又は前記通話判定部において着信応答を受信しないと判定した場合に前記コンテンツの閲覧を拒否してもよい。

本第１の発明に係る認証サーバは、通話判定部を備えるため、通信端末が通話機能を有していることを確認することができる。そして、コンテンツ閲覧認証部が通信端末が通話機能を有していることを確認した上でコンテンツの提供の認証を行うため、アクセス元が移動通信端末及びコンピュータのうちいずれであるかを、より安全にかつ正確に判断することができる。

【００３５】

本第１の発明に係る認証サーバでは、前記データ通信部は、前記通信端末に対して電話通信を行い、前記データ通信部による電話通信を検出すると、前記分布特性算出部の算出する伝送遅延時間の分布特性が変化したか否かを判定する通話変化判定部をさらに備え、前記コンテンツ閲覧認証部は、前記分布特性判定部において離散的であると判定しかつ前記通話変化判定部において伝送遅延時間の分布特性が変化したと判定した場合に前記コンテンツの閲覧を承認し、前記分布特性判定部において離散的でないと判定するか又は前記通話変化判定部において伝送遅延時間の分布特性が変化しなかったと判定した場合に前記コンテンツの閲覧を拒否してもよい。

本第１の発明に係る認証サーバは、通話変化判定部を備えるため、通信端末が通話機能を有する無線通信端末であることを確認することができる。そして、コンテンツ閲覧認証部が通信端末が通話機能を有する無線通信端末であることを確認した上でコンテンツの提供の認証を行うため、アクセス元が移動通信端末及びコンピュータのうちいずれであるかを、より安全にかつ正確に判断することができる。

【００３６】

具体的には、本第１の発明に係る認証サーバによる認証方法は、データ通信部が、コンテンツの閲覧のための認証を行う通信端末とデータ通信を行い、伝送遅延時間測定部が、前記通信端末との間の伝送遅延時間を複数回にわたり測定し、抽出部が、伝送遅延時間を蓄積して伝送遅延時間のピーク値を検出し、各ピーク値を含む一定範囲内の伝送遅延時間を抽出し、分布特性算出部が、抽出された伝送遅延時間の分布特性を算出し、分布特性判定部が、算出した分布特性が離散的であるか否かを判定する分布特性判定ステップと、前記分布特性判定ステップにおいて離散的であると判定されると前記コンテンツの閲覧を承認し、前記分布特性判定ステップにおいて離散的でないと判定されると前記コンテンツの閲覧を拒否するコンテンツ閲覧認証ステップと、を順に有する。

【００３７】

本第１の発明に係る認証サーバによる認証方法は、分布特性判定ステップを有するため、通信端末が無線通信端末であるのか又は有線通信端末であるのかを判定することができる。本第１の発明に係る認証サーバによる認証方法は、コンテンツ閲覧認証ステップを有するため、通信端末が無線通信端末である場合には通信端末へのコンテンツの提供を可能にし、通信端末が有線通信端末である場合には通信端末へのコンテンツの提供を阻止することができる。これにより、本第１の発明に係る認証サーバは、アクセス元が移動通信端末及びコンピュータのうちいずれであるかを判断することができる。ここで、本第１の発明に係る認証サーバによる認証方法は、認証を認証サーバが行うため、判断を安全にかつ正確に行うことができる。したがって、本第１の発明は、移動通信端末のユーザに限定してコンテンツを閲覧させるにあたり、アクセス元が移動通信端末及びコンピュータのうちいずれであるかを、安全にかつ正確に判断することができる。

【００３８】
本第１の発明に係る認証サーバによる認証方法では、前記分布特性判定ステップにおいて、前記伝送遅延時間測定部が、前記通信端末に複数のデータ要素を包含するＨＴＭＬファイルを送信し、前記通信端末から各データ要素を要求する要求信号を受信し、前記通信端末から各データ要素を要求する要求信号が受信された間隔を測定することにより、前記認証サーバから前記通信端末までの伝送遅延時間を測定してもよい。
本第１の発明によれば、通信端末にウェブブラウザへのアクセスを行わせるだけで認証を行うことができるため、伝送遅延時間の測定用の特別なソフトウェアを通信端末に搭載させる必要がない。このため、容易に認証を行うことができる。
【００３９】
ここで、前記分布特性判定ステップにおいて、１つの前記要求信号の受信と１つの前記データ要素の送信を順に繰り返し、各々の前記要求信号が受信された間隔を測定することにより前記伝送遅延時間の合計を測定してもよい。
本発明により、パイプライン処理を行う通信端末であっても、通信端末から各データ要素を要求する要求信号が受信された間隔を測定することにより、前記データ通信部から前記通信端末までの伝送遅延時間及び前記通信端末から前記データ通信部までの伝送遅延時間の合計を測定することができる。
【００４０】
また、本第１の発明は、前記分布特性判定ステップにおいて、前記データ要素を受信した前記通信端末からコネクションのクローズ信号を受信し、前記要求信号を受信してから前記クローズ信号を受信するまでの時間間隔を測定することにより、前記データ通信部から前記通信端末までの伝送遅延時間及び前記通信端末から前記データ通信部までの伝送遅延時間の合計を測定する認証サーバによる認証方法である。
この構成によれば、専用のソフトウェアを用いずに伝送遅延時間の測定を行うことができる。さらに、通信端末とのコネクションを用いるため、複数の通信端末との伝送遅延時間を平行して測定することができる。
【００４１】
本第１の発明に係る認証サーバによる認証方法では、前記データ通信部が、前記通信端末に対して電話通信を行い、通話判定部が、前記データ通信部が前記通信端末から着信応答を受信したか否かを判定する通話判定ステップを、前記分布特性判定ステップの前、前記分布特性判定ステップと同時又は前記分布特性判定ステップと前記コンテンツ閲覧認証ステップの間にさらに有し、前記コンテンツ閲覧認証ステップにおいて、前記コンテンツ閲覧認証部は、前記分布特性判定ステップにおいて離散的であると判定しかつ前記通話判定ステップにおいて着信応答を受信したと判定した場合に前記コンテンツの閲覧を承認し、前記分布特性判定ステップにおいて離散的でないと判定するか又は前記通話判定ステップにおいて着信応答を受信しないと判定した場合に前記コンテンツの閲覧を拒否してもよい。
本第１の発明に係る認証サーバによる認証方法は、通話判定ステップを有するため、通信端末が通話機能を有していることを確認することができる。そして、コンテンツ閲覧認証ステップにおいて通信端末が通話機能を有していることを確認した上でコンテンツの提供の認証を行うため、アクセス元が移動通信端末及びコンピュータのうちいずれであるかを、より安全にかつ正確に判断することができる。
【００４２】
本第１の発明に係る認証サーバによる認証方法では、前記データ通信部が、前記通信端末に対して電話通信を行い、通話変化判定部が、前記データ通信部による電話通信の後に、前記分布特性算出部の算出する伝送遅延時間の分布特性が変化したか否かを判定する通話変化判定ステップを、前記分布特性判定ステップの前、前記分布特性判定ステップと同時又は前記分布特性判定ステップと前記コンテンツ閲覧認証ステップの間にさらに有し、前記コンテンツ閲覧認証ステップにおいて、前記コンテンツ閲覧認証部は、前記分布特性判定ステップにおいて離散的であると判定しかつ前記通話変化判定ステップにおいて伝送

遅延時間の分布特性が変化したと判定した場合に前記コンテンツの閲覧を承認し、前記分布特性判定ステップにおいて離散的でないと判定するか又は前記通話変化判定ステップにおいて伝送遅延時間の分布特性が変化しなかったと判定した場合に前記コンテンツの閲覧を拒否してもよい。

本第１の発明に係る認証サーバによる認証方法は、通話変化判定ステップを有するため、通信端末が通話機能を有する無線通信端末であることを確認することができる。そして、コンテンツ閲覧認証ステップにおいて通信端末が通話機能を有する無線通信端末であることを確認した上でコンテンツの提供の認証を行うため、アクセス元が移動通信端末及びコンピュータのうちいずれであるかを、より安全にかつ正確に判断することができる。

【００４３】

上記第２の目的を達成するために、認証サーバ及び通信端末の間の伝送遅延時間が、認証サーバから通信端末への電話通信の実行前後で変化するかどうかに基づいて、通信端末のユーザが正規のユーザであるかどうかを判断することとした。

【００４４】

具体的には、本第２の発明は、コンテンツの閲覧のための認証を行う通信端末とデータ通信を行うデータ通信部と、前記通信端末の識別子又はパスワードを前記通信端末の電話番号と対応付ける対応テーブルと、前記データ通信部が前記識別子又は前記パスワードを利用した前記コンテンツの閲覧のための認証を前記通信端末から行われたときに、前記対応テーブルで前記識別子又は前記パスワードと対応付けられた前記電話番号を利用した電話通信を実行する電話通信部と、前記データ通信部及び前記通信端末の間の伝送遅延時間を複数回にわたり測定する伝送遅延時間測定部と、前記電話通信部が電話通信を実行しているときに、前記電話通信部が電話通信を実行していないときと比べて、前記伝送遅延時間測定部が測定している前記伝送遅延時間に変化があるかどうかを判断する伝送遅延時間変化判断部と、前記伝送遅延時間変化判断部が前記伝送遅延時間に変化があると判断したときに、前記コンテンツの閲覧を承認し、前記伝送遅延時間変化判断部が前記伝送遅延時間に変化がないと判断したときに、前記コンテンツの閲覧を拒否するコンテンツ閲覧認証部と、を備えることを特徴とする認証サーバである。

【００４５】

この構成によれば、認証を行った通信端末及び電話通信を受けた通信端末が同一の通信端末であるかどうかを確認することができる。そのため、携帯電話のユーザに限定してコンテンツを閲覧させるときに、携帯電話のユーザが正規のユーザであるかどうかを安全にかつ正確に判断することができる。

【００４６】

また、本第２の発明は、前記データ通信部は、前記通信端末に複数のデータ要素を包含するＨＴＭＬファイルを送信し、前記通信端末から各データ要素を要求する要求信号を受信し、前記伝送遅延時間測定部は、前記通信端末から各データ要素を要求する要求信号が受信された間隔を測定することにより、前記データ通信部から前記通信端末までの伝送遅延時間及び前記通信端末から前記データ通信部までの伝送遅延時間の合計を測定することを特徴とする認証サーバである。

【００４７】

この構成によれば、携帯電話は、ウェブブラウザを有していればよく、伝送遅延時間の測定用のソフトウェアを有していなくてもよい。

【００４８】

ここで、前記データ通信部は、１つの前記要求信号の受信と１つの前記データ要素の送信を順に繰り返し、前記伝送遅延時間測定部は、各々の前記要求信号が受信された間隔を測定することにより前記伝送遅延時間の合計を測定してもよい。

本発明により、パイプライン処理を行う通信端末であっても、通信端末から各データ要素を要求する要求信号が受信された間隔を測定することにより、前記データ通信部から前記通信端末までの伝送遅延時間及び前記通信端末から前記データ通信部までの伝送遅延時間の合計を測定することができる。

【００４９】
また、本第２の発明は、前記データ通信部は、前記データ要素を受信した前記通信端末からコネクションのクローズ信号を受信し、前記伝送遅延時間測定部は、前記要求信号を受信してから前記クローズ信号を受信するまでの時間間隔を測定することにより、前記データ通信部から前記通信端末までの伝送遅延時間及び前記通信端末から前記データ通信部までの伝送遅延時間の合計を測定する認証サーバである。
この構成によれば、専用のソフトウェアを用いずに伝送遅延時間の測定を行うことができる。さらに、通信端末とのコネクションを用いるため、複数の通信端末との伝送遅延時間を平行して測定することができる。
【００５０】
また、本第２の発明は、前記伝送遅延時間変化判断部は、前記電話通信部が電話通信を実行しているときに、前記電話通信部が電話通信を実行していないときと比べて、前記伝送遅延時間測定部が測定している前記伝送遅延時間に増加があるかどうかを判断し、前記コンテンツ閲覧認証部は、前記伝送遅延時間変化判断部が前記伝送遅延時間に増加があると判断したときに、前記コンテンツの閲覧を承認し、前記伝送遅延時間変化判断部が前記伝送遅延時間に増加がないと判断したときに、前記コンテンツの閲覧を拒否することを特徴とする認証サーバである。
【００５１】
この構成によれば、伝送遅延時間の変化内容を、携帯電話毎に様々に設定できる。
【００５２】
また、本第２の発明は、前記伝送遅延時間変化判断部は、前記電話通信部が電話通信を実行しているときに、前記電話通信部が電話通信を実行していないときと比べて、前記データ通信部が前記通信端末から前記伝送遅延時間の測定用のパケットを受信していないかどうかを判断し、前記コンテンツ閲覧認証部は、前記伝送遅延時間変化判断部が前記伝送遅延時間の測定用のパケットの受信がないと判断したときに、前記コンテンツの閲覧を承認し、前記伝送遅延時間変化判断部が前記伝送遅延時間の測定用のパケットの受信があると判断したときに、前記コンテンツの閲覧を拒否することを特徴とする認証サーバである。
【００５３】
この構成によれば、伝送遅延時間の変化内容を、携帯電話毎に様々に設定できる。
【００５４】
また、本第２の発明は、前記コンテンツ閲覧認証部は、前記伝送遅延時間変化判断部が前記伝送遅延時間に変化があると判断したうえに、前記電話通信に対し前記通信端末から着信応答がなされたときに、前記コンテンツの閲覧を承認し、前記伝送遅延時間変化判断部が前記伝送遅延時間に変化があると判断したところ、前記電話通信に対し前記通信端末から着信応答がなされなかったときに、前記コンテンツの閲覧を拒否することを特徴とする認証サーバである。
【００５５】
この構成によれば、携帯電話のユーザが正規のユーザであるかどうかをより安全にかつ正確に判断することができる。
【００５６】
また、本第２の発明は、通信端末の行うコンテンツの閲覧のための認証を受け付けるコンテンツ閲覧認証受付ステップと、前記通信端末との間の伝送遅延時間を複数回にわたり測定する間に、前記コンテンツの閲覧のための認証に利用された識別子又はパスワードに対応付けられた電話番号を利用した電話通信を実行する電話通信実行ステップと、電話通信を実行しているときに、電話通信を実行していないときと比べて、測定している前記伝送遅延時間に変化があるかどうかを判断する伝送遅延時間変化判断ステップと、前記伝送遅延時間に変化があると判断したときに、前記コンテンツの閲覧を承認し、前記伝送遅延時間に変化がないと判断したときに、前記コンテンツの閲覧を拒否するコンテンツ閲覧認証ステップと、を順に備えることを特徴とする認証サーバによる認証方法である。

【００５７】
この構成によれば、認証を行った通信端末及び電話通信を受けた通信端末が同一の通信端末であるかどうかを確認することができる。そのため、携帯電話のユーザに限定してコンテンツを閲覧させるときに、携帯電話のユーザが正規のユーザであるかどうかを安全にかつ正確に判断することができる。
【００５８】
また、本第２の発明は、前記電話通信実行ステップは、前記通信端末に複数のデータ要素を包含するＨＴＭＬファイルを送信し、前記通信端末から各データ要素を要求する要求信号を受信し、前記通信端末から各データ要素を要求する要求信号が受信された間隔を測定することにより、前記認証サーバから前記通信端末までの伝送遅延時間及び前記通信端末から前記認証サーバまでの伝送遅延時間の合計を測定することを特徴とする認証サーバによる認証方法である。
【００５９】
この構成によれば、通信端末は、ウェブブラウザを有していればよく、伝送遅延時間の測定用のソフトウェアを有していなくてもよい。
【００６０】
ここで、前記電話通信実行ステップは、１つの前記要求信号の受信と１つの前記データ要素の送信を順に繰り返し、各々の前記要求信号が受信された間隔を測定することにより前記伝送遅延時間の合計を測定してもよい。
本発明により、パイプライン処理を行う通信端末であっても、通信端末から各データ要素を要求する要求信号が受信された間隔を測定することにより、前記データ通信部から前記通信端末までの伝送遅延時間及び前記通信端末から前記データ通信部までの伝送遅延時間の合計を測定することができる。
【００６１】
また、本第２の発明は、前記電話通信実行ステップは、前記データ要素を受信した前記通信端末からコネクションのクローズ信号を受信し、前記要求信号を受信してから前記クローズ信号を受信するまでの時間間隔を測定することにより、前記認証サーバから前記通信端末までの伝送遅延時間及び前記通信端末から前記認証サーバまでの伝送遅延時間の合計を測定する認証サーバによる認証方法である。
この構成によれば、専用のソフトウェアを用いずに伝送遅延時間の測定を行うことができる。さらに、通信端末とのコネクションを用いるため、複数の通信端末との伝送遅延時間を平行して測定することができる。
【００６２】
また、本第２の発明は、前記伝送遅延時間変化判断ステップは、電話通信を実行しているときに、電話通信を実行していないときと比べて、測定している前記伝送遅延時間に増加があるかどうかを判断し、前記コンテンツ閲覧認証ステップは、前記伝送遅延時間に増加があると判断したときに、前記コンテンツの閲覧を承認し、前記伝送遅延時間に増加がないと判断したときに、前記コンテンツの閲覧を拒否することを特徴とする認証サーバによる認証方法である。
【００６３】
この構成によれば、伝送遅延時間の変化内容を、携帯電話毎に様々に設定できる。
【００６４】
また、本第２の発明は、前記伝送遅延時間変化判断ステップは、電話通信を実行しているときに、電話通信を実行していないときと比べて、前記通信端末から前記伝送遅延時間の測定用のパケットを受信していないかどうかを判断し、前記コンテンツ閲覧認証ステップは、前記伝送遅延時間の測定用のパケットの受信がないと判断したときに、前記コンテンツの閲覧を承認し、前記伝送遅延時間の測定用のパケットの受信があると判断したときに、前記コンテンツの閲覧を拒否することを特徴とする認証サーバによる認証方法である。
【００６５】

この構成によれば、伝送遅延時間の変化内容を、携帯電話毎に様々に設定できる。

【００６６】

また、本第２の発明は、前記コンテンツ閲覧認証ステップは、前記伝送遅延時間変化判断ステップで前記伝送遅延時間に変化があると判断したうえに、前記電話通信に対し前記通信端末から着信応答がなされたときに、前記コンテンツの閲覧を承認し、前記伝送遅延時間変化判断ステップで前記伝送遅延時間に変化があると判断したところ、前記電話通信に対し前記通信端末から着信応答がなされなかったときに、前記コンテンツの閲覧を拒否することを特徴とする認証サーバによる認証方法である。

【００６７】

この構成によれば、携帯電話のユーザが正規のユーザであるかどうかをより安全にかつ正確に判断することができる。

【００６８】

なお、上記各発明は、可能な限り組み合わせることができる。

【発明の効果】

【００６９】

本第１の発明によれば、移動通信端末のユーザに限定してコンテンツを閲覧させるにあたり、アクセス元が移動通信端末及びコンピュータのうちいずれであるかを、安全にかつ正確に判断することができる認証サーバ及び認証サーバによる認証方法を提供することができる。

【００７０】

本第２の発明は、携帯電話のユーザに限定してコンテンツを閲覧させるときに、携帯電話のユーザが正規のユーザであるかどうかを安全にかつ正確に判断することができる認証サーバ及び認証サーバによる認証方法を提供することができる。

【図面の簡単な説明】

【００７１】

【図１】認証サーバの構成を示す図である。

【図２】認証サーバの処理を示す図である。

【図３】伝送遅延時間の測定方法を示す図である。

【図４】無線通信端末から閲覧認証を行った場合の伝送遅延時間の分布特性を示す図である。

【図５】有線通信端末から閲覧認証を行った場合の伝送遅延時間の分布特性を示す図である。

【図６】通信端末の識別方法を示す図である。

【図７】通信端末の識別方法を示す図である。

【図８】識別閾値及び識別確度の関係を示す図である。

【図９】実施形態３に係るコンテンツ提供システムの一例を示す。

【図１０】通信端末２００が真のスマートフォンである場合の伝送遅延時間の推移の一例を示す。

【図１１】伝送遅延時間の算出方法の一例を示す。

【図１２】実施形態４に係るコンテンツ提供システムの一例を示す。

【図１３】パイプライン処理を行う場合の伝送遅延時間の測定方法を示す図である。

【図１４】伝送遅延時間の測定方法の他の一例を示す図である。

【図１５】実施形態５に係る認証サーバの構成を示す図である。

【図１６】実施形態５に係る認証サーバの処理を示す図である。

【図１７】伝送遅延時間の測定方法を示す図である。

【図１８】正規の携帯電話が閲覧認証を行った場合の伝送遅延時間の変化内容を示す図である。

【図１９】非正規の携帯電話が閲覧認証を行った場合の伝送遅延時間の変化内容を示す図である。

【図２０】パイプライン処理を行う場合の伝送遅延時間の測定方法を示す図である。

【図２１】伝送遅延時間の測定方法の他の一例を示す図である。
【発明を実施するための形態】
【００７２】
添付の図面を参照して本第１の発明の実施形態を説明する。以下に説明する実施形態は本発明の実施の例であり、本発明は、以下の実施形態に制限されるものではない。なお、本明細書及び図面において符号が同じ構成要素は、相互に同一のものを示すものとする。
【００７３】
（実施形態１）
認証サーバの構成を図１に示す。認証サーバ１は、通信端末２から閲覧認証を受け付けたときに、通信端末２が無線ネットワークを介した携帯電話２Ａであれば、閲覧を承認し、通信端末２が有線ネットワークを介したコンピュータ２Ｂであれば、閲覧を拒否する。認証サーバ１は、コンテンツ格納部１１、データ通信部12、伝送遅延時間測定部１３、伝送遅延時間分布特性判断部１４及びコンテンツ閲覧認証部１５から構成される。
【００７４】
コンテンツ格納部１１は、コンテンツを格納する。データ通信部１２は、コンテンツの閲覧のための認証を行う通信端末２とデータ通信を行う。伝送遅延時間測定部１３は、データ通信部１２及び通信端末２の間の伝送遅延時間を複数回にわたり測定する。伝送遅延時間分布特性判断部１４は、複数回にわたり測定された伝送遅延時間の分布特性が離散的であるかどうかを判断する。コンテンツ閲覧認証部１５は、伝送遅延時間の分布特性が離散的であると判断されたときに、その通信端末２が無線通信端末であると認識し、コンテンツの閲覧を承認し、伝送遅延時間の分布特性が離散的でないと判断されたときに、その通信端末２が有線通信端末であると認識し、コンテンツの閲覧を拒否する。
【００７５】
認証サーバの処理を図２に示す。コンテンツ閲覧認証受付ステップでは、データ通信部１２は、通信端末２の行うコンテンツの閲覧のための認証を受け付ける（ステップＳ１）。伝送遅延時間測定ステップでは、伝送遅延時間測定部１３は、通信端末２との間の伝送遅延時間を複数回にわたり測定する（ステップＳ２）。伝送遅延時間測定ステップについては、図３を用いて後に詳述する。伝送遅延時間分布特性判断ステップでは、伝送遅延時間分布特性判断部１４は、複数回にわたり測定された伝送遅延時間の分布特性が離散的であるかどうかを判断する（ステップＳ３及びＳ４）。伝送遅延時間分布特性判断ステップについては、図４から図７までを用いて後に詳述する。
【００７６】
コンテンツ閲覧認証ステップについて説明する。コンテンツ閲覧認証部１５は、伝送遅延時間の分布特性が離散的であると判断されたときに（ステップＳ４において「ＹＥＳ」）、その通信端末２が無線通信端末であると認識し（ステップＳ５）、コンテンツの閲覧を承認する（ステップＳ６）。そして、データ通信部１２は、コンテンツの閲覧の承認を携帯電話２Ａに通知するとともに、コンテンツ格納部１１の格納するコンテンツを携帯電話２Ａに提供する。ただし、データ通信部１２は、コンテンツの閲覧の承認に代えて、コンテンツ格納部１１の格納するコンテンツのみを携帯電話２Ａに提供してもよい。コンテンツ閲覧認証部１５は、伝送遅延時間の分布特性が離散的でないと判断されたときに（ステップＳ４において「ＮＯ」）、その通信端末２が有線通信端末であると認識し（ステップＳ７）、コンテンツの閲覧を拒否する（ステップＳ８）。そして、データ通信部１２は、コンテンツの閲覧の拒否をコンピュータ２Ｂに通知する。
【００７７】
携帯電話２Ａのユーザに限定して認証サーバ１のコンテンツを閲覧させるにあたり、通信端末２が携帯電話２Ａ及びコンピュータ２Ｂのうちいずれであるかを、安全にかつ正確に判断することができる。上述の判断は通信端末２が行うのではなく認証サーバ１が行うため、コンピュータ２Ｂにより分布特性が偽装されるおそれがない。
【００７８】
次に、伝送遅延時間測定ステップの詳細について説明する。伝送遅延時間の測定方法を

図３に示す。通信端末２は、リクエストＧＥＴ１を認証サーバ１に送信し、ウェブのトップページを要求する。データ通信部１２は、レスポンスＲＥＳ１を通信端末２に送信し、ＨＴＭＬファイルを提供する。通信端末２は、ＨＴＭＬファイルを解析し、ＨＴＭＬファイルに包含される複数の画像ファイルを以下のように要求する。

【００７９】

通信端末２は、リクエストＧＥＴ２を認証サーバ１に送信し、画像ファイルｅ１を要求する。データ通信部１２は、レスポンスＲＥＳ２を通信端末２に送信し、画像ファイルｅ１を提供する。通信端末２は、リクエストＧＥＴ３を認証サーバ１に送信し、画像ファイルｅ２を要求する。データ通信部１２は、レスポンスＲＥＳ３を通信端末２に送信し、画像ファイルｅ２を提供する。通信端末２は、リクエストＧＥＴ４を認証サーバ１に送信し、画像ファイルｅ３を要求する。データ通信部１２は、レスポンスＲＥＳ４を通信端末２に送信し、画像ファイルｅ３を提供する。通信端末２がＨＴＭＬファイルに包含される全ての画像ファイルを取得するまで、以上の処理が繰り返される。

【００８０】

伝送遅延時間測定部１３は、リクエストＧＥＴ２を通信端末２から受信してから次にリクエストＧＥＴ３を通信端末２から受信するまでの時間Δｔ１を、データ通信部１２から通信端末２までの伝送遅延時間及び通信端末２からデータ通信部１２までの伝送遅延時間の合計として測定する。伝送遅延時間測定部１３は、リクエストＧＥＴ３を通信端末２から受信してから次にリクエストＧＥＴ４を通信端末２から受信するまでの時間Δｔ２を、データ通信部１２から通信端末２までの伝送遅延時間及び通信端末２からデータ通信部１２までの伝送遅延時間の合計として測定する。データ通信部１２がＨＴＭＬファイルに包含される全ての画像ファイルを提供するまで、以上の処理が繰り返される。

【００８１】

ここで、伝送遅延時間測定部１３は、リクエストＧＥＴ１を通信端末２から受信してから次にリクエストＧＥＴ２を通信端末２から受信するまでの時間を測定しないことが好ましい。これは、当該時間が、データ通信部１２から通信端末２までの伝送遅延時間及び通信端末２からデータ通信部１２までの伝送遅延時間を含むのみならず、通信端末２でのＨＴＭＬファイルの解析時間をさらに含むためである。

【００８２】

携帯電話２Ａは、ウェブブラウザを有していればよく、伝送遅延時間の測定用のソフトウェアを有していなくてもよく、新しいソフトウェアの開発は不要である。

【００８３】

携帯電話２Ａによってはパイプライン処理を行うものがある。パイプライン処理は、要求信号をまとめて送信することで、ページのアクセスを高速にすることができる処理である。例えば、図１３に示すように、通信端末２が、画像ファイルｅ１の要求信号であるリクエストＧＥＴ２と、画像ファイルｅ２の要求信号であるリクエストＧＥＴ３と、画像ファイルｅ３の要求信号であるリクエストＧＥＴ４と、をまとめて送信する。このようなパイプライン処理を行う携帯電話２Ａの場合、携帯電話２Ａがリクエスト ＧＥＴ２及びリクエストＧＥＴ３をほぼ同時に送信するため、リクエストＧＥＴ２からリクエストＧＥＴ３までの時間を測定しても、伝送遅延時間の合計を測定することができない。そこで、認証サーバ１のデータ通信部１２は、１つの要求信号の受信と１つのデータ要素の送信を順に繰り返す。そして、伝送遅延時間測定部１３は、各々の要求信号が受信された間隔を測定することにより伝送遅延時間の合計を測定する。

【００８４】

例えば、データ通信部１２は、リクエストＧＥＴ２、リクエストＧＥＴ３及びリクエストＧＥＴ４をまとめて受信すると、リクエストＧＥＴ２に対するレスポンスＲＥＳ２を通信端末２に送信し、その後にレスポンスＲＥＳ２の送信後にデータ通信部１２がＴＣＰのコネクションをｃｌｏｓｅする。このように、リクエストＧＥＴ３及びリクエストＧＥＴ４に対してはレスポンスＲＥＳ３及びレスポンスＲＥＳ４を送信しない。これにより、通信端末２は、レスポンスＲＥＳ２の受信後に、改めてリクエストＧＥＴ３を送信する。

【００８５】
伝送遅延時間測定部１３は、まとめて受信したリクエストＧＥＴ２、リクエストＧＥＴ３及びリクエストＧＥＴ４のうちのリクエストＧＥＴ２を受信してから、再送させたリクエストＧＥＴ３を受信するまでの時間Δｔ１を、データ通信部１２から通信端末２までの伝送遅延時間及び通信端末２からデータ通信部１２までの伝送遅延時間の合計として測定する。
【００８６】
また、パイプライン処理を行う携帯電話２Ａに対応するために、ウェブのトップページを要求するリクエストＧＥＴ１を受信したデータ通信部１２は、パイプライン処理に対応していない旨の情を通信端末２に送信し、通信端末２のパイプライン処理を停止させてもよい。具体的には、ＨＴＴＰ／１．０又はＨＴＴＰ／０．９の仕様のＨＴＴＰである旨を通信端末２に送信する。こうすることで、図３に示すような、１つの要求信号の受信と１つのデータ要素の送信を順に繰り返す伝送遅延時間の測定を行うことができる。
【００８７】
図１４に、伝送遅延時間測定部１３における他の伝送遅延時間測定方法の一例を示す。通信端末２は、画像ファイルｅ２を受信すると、ＴＣＰのクローズ信号（ＦＩＮ）Ｃ２を認証サーバ１に送信する。本方式は、このＴＣＰのクローズ信号（ＦＩＮ）を利用し、認証サーバ１が要求信号を受信してから、データ要素を送信後のクローズ信号を受信するまでの間隔を、伝送遅延時間として測定する。例えば、伝送遅延時間測定部１３は、認証サーバ１がリクエストＧＥＴ２を受信してから、クローズ信号Ｃ２を通信端末２から受信するまでの間隔を、伝送遅延時間Δｔ１として測定する。
【００８８】
この方式は、パイプライン方式ではなく、ＴＣＰのコネクションを同時に複数確立する場合に適用できる。このため、複数のコネクションの数分だけ、同時に伝送遅延時間を測定することができるとともに、画像のダウンロードの高速化を図ることができる。画像のサイズが大きい場合には、後から送られたＧＥＴに対するクローズ時間が遅くなるので、伝送遅延時間が長くなることが予想されるが、通信端末２と認証サーバ１間の伝送遅延特性は含まれているので、処理データとして使用することができる。
【００８９】
次に、伝送遅延時間分布特性判断ステップの詳細について説明する。伝送遅延時間の分布特性を図４及び図５に示す。伝送遅延時間が複数回にわたり測定されており、所定の範囲の伝送遅延時間が測定された頻度がヒストグラムの形式で計測される。無線通信端末からの閲覧認証時の伝送遅延時間の分布特性を図４に示す。無線ネットワークを介した携帯電話２Ａからの閲覧認証があったときには、伝送遅延時間の分布特性が離散的になる。つまり、伝送遅延時間に対して約１０ｍｓ間隔で頻度のピークが出現する。有線通信端末からの閲覧認証時の伝送遅延時間の分布特性を図５に示す。有線ネットワークを介したコンピュータ２Ｂからの閲覧認証があったときには、伝送遅延時間の分布特性が非離散的になる。つまり、伝送遅延時間に対して頻度のピークが１つしか出現しない。
【００９０】
伝送遅延時間分布特性判定部１４は、伝送遅延時間の分布特性が離散的であるかどうかを判断するために、以下のように処理を実行する。まず、最頻値から約１０ｍｓの自然数倍だけ離れた伝送遅延時間での頻度を加算する。次に、加算値を最頻値での頻度で除算し除算値を所定の閾値と比較する。除算値が所定の閾値より大きいときには、伝送遅延時間に対して約１０ｍｓ間隔で頻度のピークが出現していると判断し、無線ネットワークを介した携帯電話２Ａからの閲覧認証があったと判断する。除算値が所定の閾値より小さいときには、伝送遅延時間に対して頻度のピークが１つしか出現していないと判断し、有線ネットワークを介したコンピュータ２Ｂからの閲覧認証があったと判断する。ここで、所定の閾値は、判断精度を高くするべく設定される。
【００９１】
通信端末の識別方法を図６及び図７に示す。通信端末２の識別処理の全回数は、何回で

あってもよく、識別精度の高低に応じて設定される。まず、通信端末２の識別処理の回数を表すパラメータｒを０にリセットする（ステップＳ１１）。

【００９２】

伝送遅延時間の最小値Ｍｉｎ及び最大値Ｍａｘを検索する（ステップＳ１２）。最小値Ｍｉｎから最大値Ｍａｘまで、１ｍｓのビン幅で頻度を計算する（ステップＳ１３）。伝送遅延時間の最頻値Ｍｏｄｅ０を検索し、最頻値Ｍｏｄｅ０での頻度を$Ｃ_{0}$とおく（ステップＳ１４）。パラメータｒは０にリセットされており（ステップＳ１５においてＮＯ）、ステップＳ１６に進む。ステップＳ１５については後述する。

【００９３】

無線通信端末からの閲覧認証時には、伝送遅延時間は１０ｍｓの自然数倍又は１０ｍｓの自然数倍の周辺となることが多い。ここで、最頻値Ｍｏｄｅ０が１０ｍｓの自然数倍であれば、最頻値Ｍｏｄｅ０から１０ｍｓの自然数倍だけ離れた伝送遅延時間において頻度のピークを認めやすく、離散的な分布特性を認めやすい。しかし、最頻値Ｍｏｄｅ０が１０ｍｓの自然数倍の周辺であれば、最頻値Ｍｏｄｅ０から１０ｍｓの自然数倍だけ離れた伝送遅延時間において頻度のピークを認めにくく、離散的な分布特性を認めにくい。

【００９４】

そこで、原則として、最頻値Ｍｏｄｅ０の１の位を四捨五入し新たな最頻値Ｍｏｄｅとする。ただし、伝送遅延時間が１０ｍｓの自然数倍又は１０ｍｓの自然数倍の周辺となることが少ないＵｓｅｒ　Ａｇｅｎｔがある。そのＵｓｅｒ　Ａｇｅｎｔを会社Ａとする。そこで、Ｕｓｅｒ　Ａｇｅｎｔが会社Ａであるときには、例外として、最頻値Ｍｏｄｅ０を新たな最頻値Ｍｏｄｅとし、Ｕｓｅｒ　Ａｇｅｎｔが会社Ａ以外のその他の会社であるときには、原則どおり、最頻値Ｍｏｄｅ０の１の位を四捨五入して新たな最頻値Ｍｏｄｅとする（ステップＳ１６）。

【００９５】

ここで、Ｕｓｅｒ　Ａｇｅｎｔは、通信端末２のＩＤ、パスワード、携帯電話会社に固有なＩＤ及び電話番号などを用いて判定すればよい。ただし、携帯電話会社に固有なＩＤ及び電話番号が改竄されにくいことを考慮すれば、Ｕｓｅｒ　Ａｇｅｎｔは、携帯電話会社に固有なＩＤ及び電話番号を用いて判定することが望ましい。さらに、携帯電話会社に固有なＩＤを付与しない会社が存在することを考慮すれば、Ｕｓｅｒ　Ａｇｅｎｔは、電話番号を用いて判定することがなお望ましい。

【００９６】

最頻値Ｍｏｄｅから１０ｍｓの自然数倍だけ離れた伝送遅延時間の周辺での最大頻度を計算し、自然数が様々である場合について最大頻度を加算する。加算値を最頻値Ｍｏｄｅ０での頻度$Ｃ_{0}$で除算し除算値を所定の閾値と比較する。

【００９７】

自然数が様々である場合について最大頻度を加算するにあたり、自然数ｎを１にセットし最大頻度の合計Ｔｏｔａｌを０にリセットする（ステップＳ１７）。自然数ｎが１、２、３及び４である場合について、ステップＳ１８からＳ２５までを繰り返す。

【００９８】

$Ｔ_{+n}$＝Ｍｏｄｅ＋１０ｎに対して、［$Ｔ_{+n}$－２，$Ｔ_{+n}$＋２］の範囲の最大頻度$Ｃ_{+n}$を計算し、$Ｔ_{-n}$＝Ｍｏｄｅ－１０ｎに対して、［$Ｔ_{-n}$－２，$Ｔ_{-n}$＋２］の範囲の最大頻度$Ｃ_{-n}$を計算する（ステップＳ１８）。最大頻度$Ｃ_{+n}$が最大頻度$Ｃ_{-n}$より大きいときには（ステップＳ１９においてＹＥＳ）、最大頻度$Ｃ_{n}$を最大頻度$Ｃ_{+n}$にセットする（ステップＳ２０）。最大頻度$Ｃ_{-n}$が最大頻度$Ｃ_{+n}$より大きいときには（ステップＳ１９においてＮＯ）、最大頻度$Ｃ_{n}$を最大頻度$Ｃ_{-n}$にセットする（ステップＳ２１）。そして、原則として、最大頻度$Ｃ_{n}$を加算対象とする。

【００９９】

有線通信端末からの閲覧認証時でも、最大頻度$Ｃ_{n}$が所定値より大きくなったときには、上述の除算値が所定の閾値より大きくなることがあり、無線通信端末からの閲覧認証と誤認されることがある。そこで、最大頻度$Ｃ_{n}$が所定値より大きくなったときには、例外

として、最大頻度C_nより小さい頻度を加算対象とする。

【０１００】

無線通信端末からの閲覧認証時でも、伝送遅延時間に対して頻度のピークが１つ又は２つしか出現しないことがあるＵｓｅｒ　Ａｇｅｎｔがあり、最大頻度C_nより小さい頻度を加算対象としてしまえば、有線通信端末からの閲覧認証と誤認されることがある。そのＵｓｅｒ　Ａｇｅｎｔを会社Ｂとする。そこで、Ｕｓｅｒ　Ａｇｅｎｔが会社Ｂであるときには、原則どおり、最大頻度C_nを加算対象とする。

【０１０１】

$F_n=C_n/C_0$を計算する。F_nが所定の閾値の半分Ｔｈｒｅｓｈｏｌｄ／２より小さいときには（ステップＳ２２においてＮＯ）、原則どおり、最大頻度の合計Ｔｏｔａｌとして、現状値にF_nを加算した値にセットする（ステップＳ２５）。F_nが所定の閾値の半分Ｔｈｒｅｓｈｏｌｄ／２より大きいときには（ステップＳ２２においてＹＥＳ）、Ｕｓｅｒ　Ａｇｅｎｔが会社Ｂでありかつパラメータｒが０であること（条件Ｘという）が成立するかどうかを判断する（ステップＳ２３）。条件Ｘが成立するときには（ステップＳ２３においてＹＥＳ）、原則どおり、最大頻度の合計Ｔｏｔａｌとして、現状値にF_nを加算した値にセットする（ステップＳ２５）。条件Ｘが成立しないときには（ステップＳ２３においてＮＯ）、例外として、所定の閾値の半分Ｔｈｒｅｓｈｏｌｄ／２を新たなF_nとしたうえで（ステップＳ２４）、最大頻度の合計Ｔｏｔａｌとして、現状値に新たなF_nを加算した値にセットする（ステップＳ２５）。

【０１０２】

自然数ｎが１、２、３及び４である場合について、ステップＳ１８からＳ２５までを繰り返し、最大頻度の合計Ｔｏｔａｌが所定の閾値Ｔｈｒｅｓｈｏｌｄより大きいかどうかを判断する（ステップＳ２６）。最大頻度の合計Ｔｏｔａｌが所定の閾値Ｔｈｒｅｓｈｏｌｄより大きいときには（ステップＳ２６においてＹＥＳ）、原則として、閲覧認証は無線通信端末からであると識別する（ステップＳ２８）。最大頻度の合計Ｔｏｔａｌが所定の閾値Ｔｈｒｅｓｈｏｌｄより小さいときには（ステップＳ２６においてＮＯ）、原則として、閲覧認証は有線通信端末からであると識別する（ステップＳ３０）。ここで、所定の閾値Ｔｈｒｅｓｈｏｌｄは、Ｕｓｅｒ　Ａｇｅｎｔに応じて設定してもよい。

【０１０３】

有線通信端末からの閲覧認証時でも、閲覧認証がコンピュータ２Ｂ用のデータモジュールからであるときには、最大頻度の合計Ｔｏｔａｌが所定の閾値Ｔｈｒｅｓｈｏｌｄより大きくなることがあり、無線通信端末からの閲覧認証であると誤認されることがある。しかし、携帯電話２Ａは電話回線を使用することができるが、コンピュータ２Ｂ用のデータモジュールは電話回線を使用できないため、このことを利用して携帯電話２Ａ及びコンピュータ２Ｂ用のデータモジュールからの閲覧認証を区別することができる。

【０１０４】

つまり、データ通信部１２は、通信端末２に対して電話通信を行う。なお、この電話通信は、人間の音声のデータのみならず、あらゆるデータをも伝送する。そして、コンテンツ閲覧認証部１５は、電話通信に対し通信端末２から着信応答がなされたときに、その通信端末２が電話回線を使用する携帯電話２Ａであると認識し、コンテンツの閲覧を承認し、電話通信に対し通信端末２から着信応答がなされなかったときに、その通信端末２が電話回線を使用しないコンピュータ２Ｂのデータモジュールであると認識し、コンテンツの閲覧を拒否する。ここで、認証サーバ１は、通信端末２の電話番号のデータを格納していればよい。そして、携帯電話２Ａがユーザの音声を検知することにより、着信応答を返してもよく、携帯電話２Ａが自己にインストールされたソフトウェアを用いて自動音声を出力することにより、着信応答を返してもよい。さらに、携帯電話２Ａがユーザの受信ボタン押下を検知することにより、着信応答を返してもよく、携帯電話２Ａが自己にインストールされたソフトウェアを用いて信号を送出することにより、着信応答を返してもよい。

【０１０５】

最大頻度の合計Ｔｏｔａｌが所定の閾値Ｔｈｒｅｓｈｏｌｄより大きいうえに（ステッ

プＳ２６においてＹＥＳ）、電話通信に対して着信応答があったときには（ステップＳ２７においてＹＥＳ）、原則どおり、閲覧認証は携帯電話２Ａからであると識別する（ステップＳ２８）。最大頻度の合計Ｔｏｔａｌが所定の閾値Ｔｈｒｅｓｈｏｌｄより大きいところ（ステップＳ２６においてＹＥＳ）、電話通信に対して着信応答がなかったときには（ステップＳ２７においてＮＯ）、例外として、閲覧認証はコンピュータ２Ｂのデータモジュールからであると識別する（ステップＳ３０）。

【０１０６】

無線通信端末からの閲覧認証時でも、数ｍｓ又は１０数ｍｓの伝送遅延時間で頻度のピークが出現することがあり、その場合にその伝送遅延時間を最頻値Ｍｏｄｅ０とすれば離散的な分布特性を認めにくい。そこで、最初に検索した最頻値Ｍｏｄｅ０以外で再び最頻値Ｍｏｄｅ０を検索し再識別を行う。

【０１０７】

最大頻度の合計Ｔｏｔａｌが所定の閾値Ｔｈｒｅｓｈｏｌｄより小さいうえに（ステップＳ２６においてＮＯ）、パラメータｒが０でないときには（ステップＳ２９においてＮＯ）、原則どおり、閲覧認証は有線通信端末からであると識別する（ステップＳ３０）。最大頻度の合計Ｔｏｔａｌが所定の閾値Ｔｈｒｅｓｈｏｌｄより小さいところ（ステップＳ２６においてＮＯ）、パラメータｒが０であるときには（ステップＳ２９においてＹＥＳ）、例外として、再識別を行うためにステップＳ３１及びＳ３２に進む。

【０１０８】

ステップＳ３１では、通信端末２の識別処理の回数を表すパラメータｒを１にセットし、最初に検索した最頻値Ｍｏｄｅ０での頻度C_0を０にセットする。ステップＳ３２では、最頻値Ｍｏｄｅ０及び最頻値Ｍｏｄｅを０にリセットする。ステップＳ３１及びＳ３２を行ったうえで、ステップＳ１４及びＳ１５に進む。ステップＳ１５では、パラメータｒが１でありかつ最頻値Ｍｏｄｅ０が１０ｍｓより小さくかつ最頻値Ｍｏｄｅ０での頻度C_0が１以下であること（条件Ｙという）が成立するかどうかを判断する。条件Ｙが成立するときには（ステップＳ１５においてＹＥＳ）、閲覧認証は有線通信端末からであると識別する（ステップＳ３０）。条件Ｙが成立しないときには（ステップＳ１５においてＮＯ）、ステップＳ１６に進む。このように、数ｍｓ又は１０数ｍｓの伝送遅延時間で頻度のピークが出現することがある無線通信端末からの閲覧認証を有線通信端末からの閲覧認証と区別することができる。

【０１０９】

識別閾値及び識別確度の関係を図８に示す。横軸は所定の閾値Ｔｈｒｅｓｈｏｌｄを示し、縦軸は識別の確度を示す。矩形のデータポイントはコンピュータ２Ｂからの閲覧認証について識別確度を示し、三角のデータポイントは会社Ａ及び会社Ｂ以外の会社の携帯電話２Ａからの閲覧認証について識別確度を示し、円形のデータポイントは会社Ａの携帯電話２Ａからの閲覧認証について識別確度を示す。いずれのデータポイントも再識別を考慮に入れている。

【０１１０】

所定の閾値Ｔｈｒｅｓｈｏｌｄが大きいほど、最大頻度の合計Ｔｏｔａｌは所定の閾値Ｔｈｒｅｓｈｏｌｄを越えにくい（ステップＳ２６においてＮＯ）。よって、有線通信端末からの閲覧認証が無線通信端末からの閲覧認証と誤認されることは少ないが、無線通信端末からの閲覧認証が有線通信端末からの閲覧認証と誤認されることが多い。

【０１１１】

所定の閾値Ｔｈｒｅｓｈｏｌｄが小さいほど、最大頻度の合計Ｔｏｔａｌは所定の閾値Ｔｈｒｅｓｈｏｌｄを越えやすい（ステップＳ２６においてＹＥＳ）。よって、無線通信端末からの閲覧認証が有線通信端末からの閲覧認証と誤認されることは少ないが、有線通信端末からの閲覧認証が無線通信端末からの閲覧認証と誤認されることが多い。

【０１１２】

そこで、所定の閾値Ｔｈｒｅｓｈｏｌｄを、大き過ぎもせず小さ過ぎもしない値に設定することが好ましい。具体的には、図８の場合においては、所定の閾値Ｔｈｒｅｓｈｏｌ

ｄを、０．４程度の値に設定することが好ましい。

【０１１３】

本実施形態では、最大頻度の合計Ｔｏｔａｌが所定の閾値Ｔｈｒｅｓｈｏｌｄより大きいときには、無線通信端末からの閲覧認証があったと識別し、最大頻度の合計Ｔｏｔａｌが所定の閾値Ｔｈｒｅｓｈｏｌｄより小さいときには、有線通信端末からの閲覧認証があったと識別している。他の実施形態では、最大頻度の合計Ｔｏｔａｌが所定の閾値Ｔｈｒｅｓｈｏｌｄより大きいほど、無線通信端末からの閲覧認証があった確率が高いと判定し、最大頻度の合計Ｔｏｔａｌが所定の閾値Ｔｈｒｅｓｈｏｌｄより小さいほど、有線通信端末からの閲覧認証があった確率が高いと判定してもよい。

【０１１４】

他の実施形態では、識別確度をより向上させるために、通信端末２のＩＤ、携帯電話会社のネットワーク内で生成される固有のＩＤ、通信端末２のパスワード及び通信端末２の位置情報などの識別要素を、伝送遅延時間の分布特性及び電話通信への着信応答と複合的に併用してもよい。本実施形態を利用して、無線通信端末からの閲覧認証が相当高い確率でなされたと判定したときには、少ない個数の識別要素さえ満足すれば、無線通信端末からの閲覧認証が確実になされたと判定してもよい。本実施形態を利用して、無線通信端末からの閲覧認証が若干低い確率でなされたと判定したときには、多い個数の識別要素を満足して初めて、無線通信端末からの閲覧認証が確実になされたと判定してもよい。

【０１１５】

本実施形態では、認証サーバ１がコンテンツ格納部１１においてコンテンツを格納している。他の実施形態では、認証サーバ１はコンテンツを格納しておらず、認証サーバ１以外のコンテンツサーバがコンテンツを格納してもよい。このとき、データ通信部１２は、コンテンツの閲覧の承認を携帯電話２Ａに通知するとともに、認証サーバ１以外のコンテンツサーバの格納するコンテンツを携帯電話２Ａに提供すればよい。

【０１１６】

本実施形態では、携帯電話２Ａ又はコンピュータ２Ｂが、閲覧要求を発行し閲覧可否を通知されている。他の実施形態では、携帯電話２Ａ以外の他の装置が、閲覧要求を発行し閲覧承認を通知されてもよい。ただし、本実施形態及び他の実施形態の両方において、携帯電話２Ａが閲覧認証を行うことに変わりはない。つまり、他の実施形態では、他の装置が閲覧要求を発行し、認証サーバ１が携帯電話２Ａに認証要求を発行し、携帯電話２Ａが閲覧認証を行い、認証サーバ１が他の装置に閲覧承認を通知しコンテンツを提供する。ただし、認証サーバ１が閲覧承認に代えてコンテンツのみを提供してもよい。このとき、認証サーバ１は、他の装置及び携帯電話２Ａに関する情報を対応付けて記憶している。なお、他の装置は、無線ネットワークを介してもよく、有線ネットワークを介してもよい。

【０１１７】

（実施形態２）

本実施形態に係る認証サーバによる認証方法は、実施形態１で説明したコンテンツ閲覧認証ステップにおいて電話通信を用いることを特徴とする。そのため、コンテンツ閲覧認証ステップの前に、図１に示すデータ通信部１２は、通信端末に対して電話通信を行う。そして、コンテンツ閲覧認証ステップにおいて、本実施形態に係る認証サーバは以下のように動作する。

【０１１８】

コンテンツ閲覧認証部１５は、伝送遅延時間の分布特性が離散的であると判断されたうえに、電話通信に対し伝送遅延時間の分布特性が変化したときに、コンテンツの閲覧を承認する。一方、コンテンツ閲覧認証部１５は、伝送遅延時間の分布特性が離散的であると判断されたところ、電話通信に対し伝送遅延時間の分布特性が変化しなかったときに、コンテンツの閲覧を拒否する。

【０１１９】

例えば、図７に示すステップＳ２７において、着信応答があるか否かに代えて、伝送遅延時間の分布特性が変化したか否かを判定する。通信端末が携帯電話２Ａである場合、通

信端末は、電話通信を行うと、伝送遅延時間が一時的又は継続的に長くなったり、認証を行うための通信を中断したりする。そうすると、長い伝送遅延時間の分布が増えたり、伝送遅延時間の分布が全体的に減ったりといった変化が生じる。一方、通信端末がコンピュータ２Ｂである場合、通信端末は、電話通話を行っても、伝送遅延時間が一時的又は継続的に長くなったり、認証を行うための通信を中断したりすることもない。このため、電話通話を行ったときの伝送遅延時間の分布特性の変化を検出することで、通信端末２００が携帯電話２Ａ又はコンピュータ２Ｂのいずれであるのかを判別することができる。そして、分布特性が変化した場合には閲覧認証は携帯電話２Ａからであると識別し（ステップＳ２８）、分布特性が変化しない場合にはステップＳ３０に移行する。

【０１２０】

また、図７に示すステップＳ２７において、着信応答があるか否かに加えて、さらに伝送遅延時間の分布特性が変化したか否かを判定してもよい。この場合、着信応答がありかつ分布特性が変化した場合にはステップＳ２８に移行し、着信応答がないか又は分布特性が変化しない場合には閲覧認証はコンピュータ２Ｂのデータモジュールからであると識別する（ステップＳ３０）。これにより、通信端末が携帯電話２Ａ又はコンピュータ２Ｂのいずれであるかをさらに正確に判定することができる。

【０１２１】

（実施形態３）

図９に、実施形態３に係るコンテンツ提供システムの一例を示す。認証サーバ１０３は、通信端末２００にコンテンツを提供するに際し、通信端末２００が真のスマートフォンであるのか、又はコンピュータがスマートフォンに成りすました偽のスマートフォンであるかを判定する。そして、認証サーバ１０３は、通信端末２００が真のスマートフォンであればコンテンツを提供し、通信端末２００が偽のスマートフォンであればコンテンツを提供しない。

【０１２２】

認証サーバ１０３は、コンテンツ格納部３１と、データ通信部３２と、伝送遅延時間測定部３３と、抽出部３５と、分布特性算出部３４と、分布特性判定部３６と、コンテンツ閲覧認証部３７と、通話判定部３８と、を備える。コンテンツ格納部３１は、通信端末２００に提供するコンテンツを格納する。

【０１２３】

図２に、実施形態３に係る認証サーバによる認証方法の一例を示す。本実施形態に係る認証サーバによる認証方法は、閲覧認証受け付けステップと、分布特性判定ステップと、コンテンツ閲覧認証ステップと、を順に有する。閲覧認証受け付けステップでは、データ通信部３２は、通信端末２００の行うコンテンツの閲覧のための認証を受け付ける（図２に示す符号Ｓ１）。分布特性判定ステップでは、ステップＳ２～Ｓ４を実行する。コンテンツ閲覧認証ステップでは、ステップＳ５～Ｓ８を実行する。

【０１２４】

以下、分布特性判定ステップについて説明する。

データ通信部３２は、コンテンツの閲覧のための認証を行う通信端末２００とデータ通信を行う。伝送遅延時間測定部３３は、データ通信部３２及び通信端末２００の間の伝送遅延時間を複数回にわたり測定する（図２に示す符号Ｓ２）。この結果、通信端末２００が真のスマートフォンである場合、図１０に示すように、伝送遅延時間に鋭いピークＰ１～Ｐ４が現れる。

【０１２５】

抽出部３５は、伝送遅延時間測定部３３の測定した伝送遅延時間を蓄積して各ピークＰ１～Ｐ４のピーク値である伝送遅延時間を検出し、各ピーク値を含む一定範囲ΔＴ内の伝送遅延時間を抽出する。ここで、一定範囲ΔＴは、伝送遅延時間のピークとバックグラウンドとを分離可能な閾値Δt_Tを超えかつ複数のピーク値を含む任意の範囲である。

【０１２６】

そして、分布特性算出部３４は、抽出部３５の抽出した伝送遅延時間を蓄積して伝送遅

延時間の分布特性を算出する。そうすると、通信端末２００が真のスマートフォンである場合は図４に示すような離散的な分布となり、通信端末２００が偽のスマートフォンである場合は図５に示すような非離散的な分布となる。

【０１２７】

分布特性判定部３６は、分布特性算出部３４の算出した分布特性が離散的であるか否かを判定する（図２に示す符号Ｓ４）。これにより、通信端末２００が真のスマートフォンであるのか偽のスマートフォンであるのかを判定することができる。

【０１２８】

以下、コンテンツ閲覧認証ステップについて説明する。

コンテンツ閲覧認証部３７は、分布特性判定部３６が離散的であると判定すると（ステップＳ４において「ＹＥＳ」）、真のスマートフォンからの閲覧認証と認識し（図２に示す符号Ｓ５）、コンテンツの閲覧を承認する（図２に示す符号Ｓ６）。すると、データ通信部３２は、コンテンツの閲覧の承認を通信端末２００に通知するとともに、コンテンツ格納部３１の格納するコンテンツを通信端末２００に提供する。ただし、データ通信部３２は、コンテンツの閲覧の承認に代えて、コンテンツ格納部３１の格納するコンテンツのみを通信端末２００に提供してもよい。

一方、コンテンツ閲覧認証部３７は、分布特性判定部３６が離散的でないと判定すると（図２に示す符号Ｓ４において「ＮＯ」）、偽のスマートフォンからの閲覧認証と認識し（図２に示す符号Ｓ７）、コンテンツの閲覧を拒否する（図２に示す符号Ｓ８）。すると、データ通信部３２は、コンテンツ格納部３１の格納するコンテンツを通信端末２００に送信せず、コンテンツの閲覧の拒否を通信端末２００に通知する。

【０１２９】

真のスマートフォンのユーザに限定して認証サーバ１０３のコンテンツを閲覧させるにあたり、通信端末２００が真のスマートフォンであるのか又は偽のスマートフォンであるかを、安全にかつ正確に判断することができる。上述の判断は通信端末２００が行うのではなく認証サーバ１０３が行うため、コンピュータにより分布特性が偽装されるおそれがない。

【０１３０】

本実施形態では、通話判定ステップ（不図示）を有していても良い。通話判定ステップは、閲覧認証受け付けステップと分布特性判定ステップの間、分布特性判定ステップと同時又は分布特性判定ステップとコンテンツ閲覧認証ステップの間に実行される。

【０１３１】

通話判定ステップでは、本実施形態に係るコンテンツ提供システムは、以下のように動作する。データ通信部３２は、通信端末に対して電話通信を行う。通話判定部３８は、データ通信部３２が通信端末２００から着信応答を受信したか否かを判定する。通信端末２００から着信応答を受信することによって、通信端末２００が携帯電話やスマートフォンなどの電話機能を有する端末であることを確認することができる。通信端末２００から着信応答を受信できなかった場合は、通信端末２００がコンピュータなどの電話機能を有さない成りすましの端末であることを確認することができる。

【０１３２】

通話判定ステップを有する場合、コンテンツ閲覧認証ステップにおいて、本実施形態に係るコンテンツ提供システムは、以下のように動作する。

コンテンツ閲覧認証部３７は、分布特性判定部３６において離散的であると判定しかつ通話判定部３８において着信応答を受信したと判定した場合、コンテンツの閲覧を承認する。すると、データ通信部３２は、コンテンツの閲覧の承認を通信端末２００に通知するとともに、コンテンツ格納部３１の格納するコンテンツを通信端末２００に提供する。

一方、コンテンツ閲覧認証部３７は、分布特性判定部３６において離散的でないと判定するか又は通話判定部３８において着信応答を受信しないと判定した場合、コンテンツの閲覧を拒否する。すると、データ通信部３２は、コンテンツ格納部３１の格納するコンテンツを通信端末２００に送信せず、コンテンツの閲覧の拒否を通信端末２００に通知する

。

【０１３３】

次に、ステップＳ２における伝送遅延時間の測定の詳細について説明する。データ通信部３２は、通信端末２００に複数のデータ要素を包含するＨＴＭＬファイルを送信し、通信端末２００から各データ要素を要求する要求信号を受信する。そして、伝送遅延時間測定部３３は、通信端末２００から各データ要素を要求する要求信号が受信された間隔を測定することにより、データ通信部３２から通信端末２００までの伝送遅延時間及び通信端末２００からデータ通信部３２までの伝送遅延時間の合計を測定する。ここで、データ要素は、例えば、画像ファイルである。

【０１３４】

図３に、データ要素が画像ファイルである場合における伝送遅延時間の測定方法の一例を示す。

通信端末２００は、リクエストＧＥＴ１を認証サーバ１０３に送信し、ウェブのトップページを要求する。データ通信部３２は、レスポンスＲＥＳ１を通信端末２００に送信し、ＨＴＭＬファイルを提供する。通信端末２００は、ＨＴＭＬファイルを解析し、ＨＴＭＬファイルに包含される複数の画像ファイルｅ１、ｅ２、ｅ３・・・を以下のように要求する。

【０１３５】

通信端末２００は、リクエストＧＥＴ２を認証サーバ１０３に送信し、画像ファイルｅ１を要求する。データ通信部３２は、レスポンスＲＥＳ２を通信端末２００に送信し、画像ファイルｅ１を提供する。通信端末２００は、リクエストＧＥＴ３を認証サーバ１０３に送信し、画像ファイルｅ２を要求する。データ通信部３２は、レスポンスＲＥＳ３を通信端末２００に送信し、画像ファイルｅ２を提供する。通信端末２００は、リクエストＧＥＴ４を認証サーバ１０３に送信し、画像ファイルｅ３を要求する。データ通信部３２は、レスポンスＲＥＳ４を通信端末２００に送信し、画像ファイルｅ３を提供する。通信端末２００がＨＴＭＬファイルに包含される全ての画像ファイルを取得するまで、以上の処理が繰り返される。

【０１３６】

図１１に、伝送遅延時間の算出方法の一例を示す。伝送遅延時間測定部３３は、リクエストＧＥＴ２を通信端末２００から受信してから次にリクエストＧＥＴ３を通信端末２００から受信するまでの時間Δｔ１を、データ通信部３２から通信端末２００までの伝送遅延時間として測定する。伝送遅延時間測定部３３は、リクエストＧＥＴ３を通信端末２００から受信してから次にリクエストＧＥＴ４を通信端末２００から受信するまでの時間Δｔ２を、データ通信部３２から通信端末２００までの伝送遅延時間として測定する。データ通信部３２がＨＴＭＬファイルに包含される全ての画像ファイルを提供するまで、以上の処理が繰り返される。これにより、図１０に示す伝送遅延時間が得られる。

【０１３７】

なお、通信端末２００は、ウェブブラウザを有していればよく、伝送遅延時間の測定用のソフトウェアを有していなくてもよく、新しいソフトウェアの開発は不要である。

【０１３８】

また、パイプライン処理を行う携帯電話２Ａの対応は実施形態１で説明したとおりである。

【０１３９】

次に、図４及び図５を参照しながら伝送遅延時間分布特性判断ステップの詳細について説明する。伝送遅延時間が複数回にわたり測定されており、所定の範囲の伝送遅延時間が測定された頻度がヒストグラムの形式で計測される。無線ネットワークを介した通信端末２００からの閲覧認証があったときには、図４に示すように、伝送遅延時間の分布特性が離散的になる。例えば、伝送遅延時間に対して約１０ｍｓ間隔で頻度のピークが出現する。偽のスマートフォンである有線ネットワークを介した通信端末２００からの閲覧認証があったときには、図５に示すように、伝送遅延時間の分布特性が非離散的になる。つまり

、伝送遅延時間に対して頻度のピークが１つしか出現しない。

【０１４０】

分布特性判定部３４は、伝送遅延時間の分布特性が離散的であるかどうかを判断するために、以下のように処理を実行する。まず、最頻値から約１０ｍｓの自然数倍だけ離れた伝送遅延時間での頻度を加算する。次に、加算値を最頻値での頻度で除算し除算値を所定の閾値と比較する。除算値が所定の閾値より大きいときには、伝送遅延時間に対して約１０ｍｓ間隔で頻度のピークが出現していると判断し、無線ネットワークを介したスマートフォンからの閲覧認証があったと判断する。除算値が所定の閾値より小さいときには、伝送遅延時間に対して頻度のピークが１つしか出現していないと判断し、偽のスマートフォンからの閲覧認証があったと判断する。ここで、所定の閾値は、判断精度を高くするべく設定される。

【０１４１】

図６及び図７に、通信端末の識別方法の一例を示す。通信端末２００の識別処理の全回数は、何回であってもよく、識別精度の高低に応じて設定される。まず、通信端末２００の識別処理の回数を表すパラメータｒを０にリセットする（ステップＳ１１）。

【０１４２】

伝送遅延時間の最小値Ｍｉｎ及び最大値Ｍａｘを検索する（ステップＳ１２）。最小値Ｍｉｎから最大値Ｍａｘまで、１ｍｓのビン幅で頻度を計算する（ステップＳ１３）。伝送遅延時間の最頻値Ｍｏｄｅ０を検索し、最頻値Ｍｏｄｅ０での頻度をC_0とおく（ステップＳ１４）。パラメータｒは０にリセットされており（ステップＳ１５においてＮＯ）、ステップＳ１６に進む。ステップＳ１５については後述する。

【０１４３】

真のスマートフォンからの閲覧認証時には、伝送遅延時間は１０ｍｓの自然数倍又は１０ｍｓの自然数倍の周辺となることが多い。ここで、最頻値Ｍｏｄｅ０が１０ｍｓの自然数倍であれば、最頻値Ｍｏｄｅ０から１０ｍｓの自然数倍だけ離れた伝送遅延時間において頻度のピークを認めやすく、離散的な分布特性を認めやすい。しかし、最頻値Ｍｏｄｅ０が１０ｍｓの自然数倍の周辺であれば、最頻値Ｍｏｄｅ０から１０ｍｓの自然数倍だけ離れた伝送遅延時間において頻度のピークを認めにくく、離散的な分布特性を認めにくい。

【０１４４】

そこで、原則として、最頻値Ｍｏｄｅ０の１の位を四捨五入し新たな最頻値Ｍｏｄｅとする。ただし、伝送遅延時間が１０ｍｓの自然数倍又は１０ｍｓの自然数倍の周辺となることが少ないＵｓｅｒ　Ａｇｅｎｔがある。そのＵｓｅｒ　Ａｇｅｎｔを会社Ａとする。そこで、Ｕｓｅｒ　Ａｇｅｎｔが会社Ａであるときには、例外として、最頻値Ｍｏｄｅ０を新たな最頻値Ｍｏｄｅとし、Ｕｓｅｒ　Ａｇｅｎｔが会社Ａ以外のその他の会社であるときには、原則どおり、最頻値Ｍｏｄｅ０の１の位を四捨五入して新たな最頻値Ｍｏｄｅとする（ステップＳ１６）。

【０１４５】

ここで、Ｕｓｅｒ　Ａｇｅｎｔは、通信端末２００のＩＤ、パスワード、携帯電話会社に固有なＩＤ及び電話番号などを用いて判定すればよい。ただし、携帯電話会社に固有なＩＤ及び電話番号が改竄されにくいことを考慮すれば、Ｕｓｅｒ　Ａｇｅｎｔは、携帯電話会社に固有なＩＤ及び電話番号を用いて判定することが望ましい。さらに、携帯電話会社に固有なＩＤを付与しない会社が存在することを考慮すれば、Ｕｓｅｒ　Ａｇｅｎｔは、電話番号を用いて判定することがなお望ましい。

【０１４６】

最頻値Ｍｏｄｅから１０ｍｓの自然数倍だけ離れた伝送遅延時間の周辺での最大頻度を計算し、自然数が様々である場合について最大頻度を加算する。加算値を最頻値Ｍｏｄｅ０での頻度C_0で除算し除算値を所定の閾値と比較する。

【０１４７】

自然数が様々である場合について最大頻度を加算するにあたり、自然数ｎを１にセット

し最大頻度の合計Ｔｏｔａｌを０にリセットする（ステップＳ１７）。自然数ｎが１、２、３及び４である場合について、ステップＳ１８からＳ２５までを繰り返す。

【０１４８】

T_{+n}＝Ｍｏｄｅ＋１０ｎに対して、［T_{+n}－２，T_{+n}＋２］の範囲の最大頻度C_{+n}を計算し、T_{-n}＝Ｍｏｄｅ－１０ｎに対して、［T_{-n}－２，T_{-n}＋２］の範囲の最大頻度C_{-n}を計算する（ステップＳ１８）。最大頻度C_{+n}が最大頻度C_{-n}より大きいときには（ステップＳ１９においてＹＥＳ）、最大頻度C_nを最大頻度C_{+n}にセットする（ステップＳ２０）。最大頻度C_{-n}が最大頻度C_{+n}より大きいときには（ステップＳ１９においてＮＯ）、最大頻度C_nを最大頻度C_{-n}にセットする（ステップＳ２１）。そして、原則として、最大頻度C_nを加算対象とする。

【０１４９】

偽のスマートフォンからの閲覧認証時でも、最大頻度C_nが所定値より大きくなったときには、上述の除算値が所定の閾値より大きくなることがあり、真のスマートフォンからの閲覧認証と誤認されることがある。そこで、最大頻度C_nが所定値より大きくなったときには、例外として、最大頻度C_nより小さい頻度を加算対象とする。

【０１５０】

真のスマートフォンからの閲覧認証時でも、伝送遅延時間に対して頻度のピークが１つ又は２つしか出現しないことがあるＵｓｅｒ　Ａｇｅｎｔがあり、最大頻度C_nより小さい頻度を加算対象としてしまえば、偽のスマートフォンからの閲覧認証と誤認されることがある。そのＵｓｅｒ　Ａｇｅｎｔを会社Ｂとする。そこで、Ｕｓｅｒ　Ａｇｅｎｔが会社Ｂであるときには、原則どおり、最大頻度C_nを加算対象とする。

【０１５１】

F_n＝C_n／C_0を計算する。F_nが所定の閾値の半分Ｔｈｒｅｓｈｏｌｄ／２より小さいときには（ステップＳ２２においてＮＯ）、原則どおり、最大頻度の合計Ｔｏｔａｌとして、現状値にF_nを加算した値にセットする（ステップＳ２５）。F_nが所定の閾値の半分Ｔｈｒｅｓｈｏｌｄ／２より大きいときには（ステップＳ２２においてＹＥＳ）、Ｕｓｅｒ　Ａｇｅｎｔが会社Ｂでありかつパラメータｒが０であること（条件Ｘという）が成立するかどうかを判断する（ステップＳ２３）。条件Ｘが成立するときには（ステップＳ２３においてＹＥＳ）、原則どおり、最大頻度の合計Ｔｏｔａｌとして、現状値にF_nを加算した値にセットする（ステップＳ２５）。条件Ｘが成立しないときには（ステップＳ２３においてＮＯ）、例外として、所定の閾値の半分Ｔｈｒｅｓｈｏｌｄ／２を新たなF_nとしたうえで（ステップＳ２４）、最大頻度の合計Ｔｏｔａｌとして、現状値に新たなF_nを加算した値にセットする（ステップＳ２５）。

【０１５２】

自然数ｎが１、２、３及び４である場合について、ステップＳ１８からＳ２５までを繰り返し、最大頻度の合計Ｔｏｔａｌが所定の閾値Ｔｈｒｅｓｈｏｌｄより大きいかどうかを判断する（ステップＳ２６）。最大頻度の合計Ｔｏｔａｌが所定の閾値Ｔｈｒｅｓｈｏｌｄより大きいときには（ステップＳ２６においてＹＥＳ）、原則として、閲覧認証は真のスマートフォンからであると識別する（ステップＳ２８）。最大頻度の合計Ｔｏｔａｌが所定の閾値Ｔｈｒｅｓｈｏｌｄより小さいときには（ステップＳ２６においてＮＯ）、原則として、閲覧認証は偽のスマートフォンからであると識別する（ステップＳ３０）。ここで、所定の閾値Ｔｈｒｅｓｈｏｌｄは、Ｕｓｅｒ　Ａｇｅｎｔに応じて設定してもよい。

【０１５３】

偽のスマートフォンからの閲覧認証時でも、閲覧認証がコンピュータ用のデータモジュールからであるときには、最大頻度の合計Ｔｏｔａｌが所定の閾値Ｔｈｒｅｓｈｏｌｄより大きくなることがあり、真のスマートフォンからの閲覧認証であると誤認されることがある。しかし、通信端末２００がスマートフォンの場合は電話回線を使用することができるが、通信端末２００がコンピュータ用のデータモジュールは電話回線を使用できないため、このことを利用してスマートフォンであるかコンピュータ用のデータモジュールから

の閲覧認証を区別することができる。

【０１５４】

つまり、データ通信部３２は、通信端末２００に対して電話通信を行う。なお、この電話通信は、人間の音声のデータのみならず、あらゆるデータをも伝送する。そして、コンテンツ閲覧認証部１５は、電話通信に対し通信端末２００から着信応答がなされたときに、その通信端末２００が電話回線を使用する通信端末２００であると認識し、コンテンツの閲覧を承認し、電話通信に対し通信端末２００から着信応答がなされなかったときに、その通信端末２００が電話回線を使用しないコンピュータのデータモジュールであると認識し、コンテンツの閲覧を拒否する。ここで、認証サーバ１０３は、通信端末２００の電話番号のデータを格納していればよい。そして、通信端末２００がユーザの音声を検知することにより、着信応答を返してもよく、通信端末２００が自己にインストールされたソフトウェアを用いて自動音声を出力することにより、着信応答を返してもよい。さらに、通信端末２００がユーザの受信ボタン押下を検知することにより、着信応答を返してもよく、通信端末２００が自己にインストールされたソフトウェアを用いて信号を送出することにより、着信応答を返してもよい。

【０１５５】

最大頻度の合計Ｔｏｔａｌが所定の閾値Ｔｈｒｅｓｈｏｌｄより大きいうえに（ステップＳ２６においてＹＥＳ）、電話通信に対して着信応答があったときには（ステップＳ２７においてＹＥＳ）、原則どおり、閲覧認証はスマートフォンからであると識別する（ステップＳ２８）。最大頻度の合計Ｔｏｔａｌが所定の閾値Ｔｈｒｅｓｈｏｌｄより大きいところ（ステップＳ２６においてＹＥＳ）、電話通信に対して着信応答がなかったときには（ステップＳ２７においてＮＯ）、例外として、閲覧認証はコンピュータのデータモジュールからであると識別する（ステップＳ３０）。

【０１５６】

真のスマートフォンからの閲覧認証時でも、数ｍｓ又は１０数ｍｓの伝送遅延時間で頻度のピークが出現することがあり、その場合にその伝送遅延時間を最頻値Ｍｏｄｅ０とすれば離散的な分布特性を認めにくい。そこで、最初に検索した最頻値Ｍｏｄｅ０以外で再び最頻値Ｍｏｄｅ０を検索し再識別を行う。

【０１５７】

最大頻度の合計Ｔｏｔａｌが所定の閾値Ｔｈｒｅｓｈｏｌｄより小さいうえに（ステップＳ２６においてＮＯ）、パラメータｒが０でないときには（ステップＳ２９においてＮＯ）、原則どおり、閲覧認証は偽のスマートフォンからであると識別する（ステップＳ３０）。最大頻度の合計Ｔｏｔａｌが所定の閾値Ｔｈｒｅｓｈｏｌｄより小さいところ（ステップＳ２６においてＮＯ）、パラメータｒが０であるときには（ステップＳ２９においてＹＥＳ）、例外として、再識別を行うためにステップＳ３１及びＳ３２に進む。

【０１５８】

ステップＳ３１では、通信端末２００の識別処理の回数を表すパラメータｒを１にセットし、最初に検索した最頻値Ｍｏｄｅ０での頻度$Ｃ_{0}$を０にセットする。ステップＳ３２では、最頻値Ｍｏｄｅ０及び最頻値Ｍｏｄｅを０にリセットする。ステップＳ３１及びＳ３２を行ったうえで、ステップＳ１４及びＳ１５に進む。ステップＳ１５では、パラメータｒが１でありかつ最頻値Ｍｏｄｅ０が１０ｍｓより小さくかつ最頻値Ｍｏｄｅ０での頻度$Ｃ_{0}$が１以下であること（条件Ｙという）が成立するかどうかを判断する。条件Ｙが成立するときには（ステップＳ１５においてＹＥＳ）、閲覧認証は偽のスマートフォンからであると識別する（ステップＳ３０）。条件Ｙが成立しないときには（ステップＳ１５においてＮＯ）、ステップＳ１６に進む。このように、数ｍｓ又は１０数ｍｓの伝送遅延時間で頻度のピークが出現することがある真のスマートフォンからの閲覧認証を偽のスマートフォンからの閲覧認証と区別することができる。

【０１５９】

図８に、識別閾値及び識別確度の関係を示す。横軸は所定の閾値Ｔｈｒｅｓｈｏｌｄを示し、縦軸は識別の確度を示す。矩形のデータポイントはコンピュータからの閲覧認証に

ついて識別確度を示し、三角のデータポイントは会社Ａ及び会社Ｂ以外の会社の通信端末２００からの閲覧認証について識別確度を示し、円形のデータポイントは会社Ａの通信端末２００からの閲覧認証について識別確度を示す。いずれのデータポイントも再識別を考慮に入れている。

【０１６０】

所定の閾値Ｔｈｒｅｓｈｏｌｄが大きいほど、最大頻度の合計Ｔｏｔａｌは所定の閾値Ｔｈｒｅｓｈｏｌｄを越えにくい（ステップＳ２６においてＮＯ）。よって、偽のスマートフォンからの閲覧認証が真のスマートフォンからの閲覧認証と誤認されることは少ないが、真のスマートフォンからの閲覧認証が偽のスマートフォンからの閲覧認証と誤認されることが多い。

【０１６１】

所定の閾値Ｔｈｒｅｓｈｏｌｄが小さいほど、最大頻度の合計Ｔｏｔａｌは所定の閾値Ｔｈｒｅｓｈｏｌｄを越えやすい（ステップＳ２６においてＹＥＳ）。よって、真のスマートフォンからの閲覧認証が偽のスマートフォンからの閲覧認証と誤認されることは少ないが、偽のスマートフォンからの閲覧認証が真のスマートフォンからの閲覧認証と誤認されることが多い。

【０１６２】

そこで、所定の閾値Ｔｈｒｅｓｈｏｌｄを、大き過ぎもせず小さ過ぎもしない値に設定することが好ましい。具体的には、図８の場合においては、所定の閾値Ｔｈｒｅｓｈｏｌｄを、０．４程度の値に設定することが好ましい。

【０１６３】

本実施形態では、最大頻度の合計Ｔｏｔａｌが所定の閾値Ｔｈｒｅｓｈｏｌｄより大きいときには、真のスマートフォンからの閲覧認証があったと識別し、最大頻度の合計Ｔｏｔａｌが所定の閾値Ｔｈｒｅｓｈｏｌｄより小さいときには、偽のスマートフォンからの閲覧認証があったと識別している。他の実施形態では、最大頻度の合計Ｔｏｔａｌが所定の閾値Ｔｈｒｅｓｈｏｌｄより大きいほど、真のスマートフォンからの閲覧認証があった確率が高いと判定し、最大頻度の合計Ｔｏｔａｌが所定の閾値Ｔｈｒｅｓｈｏｌｄより小さいほど、偽のスマートフォンからの閲覧認証があった確率が高いと判定してもよい。

【０１６４】

他の実施形態では、識別確度をより向上させるために、通信端末２００のＩＤ、携帯電話会社のネットワーク内で生成される固有のＩＤ、通信端末２００のパスワード及び通信端末２００の位置情報などの識別要素を、伝送遅延時間の分布特性及び電話通信への着信応答と複合的に併用してもよい。本実施形態を利用して、真のスマートフォンからの閲覧認証が相当高い確率でなされたと判定したときには、少ない個数の識別要素さえ満足すれば、真のスマートフォンからの閲覧認証が確実になされたと判定してもよい。本実施形態を利用して、真のスマートフォンからの閲覧認証が若干低い確率でなされたと判定したときには、多い個数の識別要素を満足して初めて、真のスマートフォンからの閲覧認証が確実になされたと判定してもよい。

【０１６５】

本実施形態では、通信端末２００が真のスマートフォンであるか否かである例について説明したが、通信端末２００はスマートフォンでなくともよい。例えば、携帯電話などの無線通信によって通話を行うとともにデータ通信を行うことが可能な端末であればよい。

【０１６６】

また、本実施形態では、認証サーバ１０３がコンテンツ格納部３１においてコンテンツを格納している。他の実施形態では、認証サーバ１０３はコンテンツを格納しておらず、認証サーバ１０３以外のコンテンツサーバがコンテンツを格納してもよい。このとき、データ通信部３２は、コンテンツの閲覧の承認を通信端末２００に通知するとともに、認証サーバ１０３以外のコンテンツサーバの格納するコンテンツを通信端末２００に提供すればよい。

【０１６７】

本実施形態では、通信端末２００が、閲覧要求を発行し閲覧可否を通知されている。他の実施形態では、通信端末２００以外の他の装置が、閲覧要求を発行し閲覧承認を通知されてもよい。ただし、本実施形態及び他の実施形態の両方において、通信端末２００が閲覧認証を行うことに変わりはない。つまり、他の実施形態では、他の装置が閲覧要求を発行し、認証サーバ１０３が通信端末２００に認証要求を発行し、通信端末２００が閲覧認証を行い、認証サーバ１０３が他の装置に閲覧承認を通知しコンテンツを提供する。ただし、認証サーバ１０３が閲覧承認に代えてコンテンツのみを提供してもよい。このとき、認証サーバ１０３は、他の装置及び通信端末２００に関する情報を対応付けて記憶している。なお、他の装置は、無線ネットワークを介してもよく、有線ネットワークを介してもよい。

【０１６８】

（実施形態４）

図１２に、実施形態４に係るコンテンツ提供システムの一例を示す。本実施形態に係るコンテンツ提供システムは、図９に示す認証サーバ１０３に代えて認証サーバ１０４を備える。認証サーバ１０４は、通話判定部３８及びコンテンツ閲覧認証部３７を備えず、通話変化判定部４１及びコンテンツ閲覧認証部４２を備える。

【０１６９】

本実施形態に係る認証サーバによる認証方法は、実施形態３にて説明した閲覧認証受け付けステップと、分布特性判定ステップと、コンテンツ閲覧認証ステップと、を順に有する。そして、閲覧認証受け付けステップと分布特性判定ステップの間、分布特性判定ステップと同時又は分布特性判定ステップとコンテンツ閲覧認証ステップの間に、通話変化判定ステップを有する。

【０１７０】

通話変化判定ステップでは、本実施形態に係るコンテンツ提供システムは、以下のように動作する。データ通信部３２は、通信端末２００に対して電話通信を行い、電話通信を行った旨を通話変化判定部４１に出力する。通話変化判定部４１は、分布特性算出部３４の算出する伝送遅延時間の分布特性が変化したか否かを判定する。そして、通話変化判定部４１は、データ通信部３２から電話通信を行った旨を取得する前後における伝送遅延時間の分布特性を比較する。そして、通話変化判定部４１は、データ通信部３２が電話通信を行った後に伝送遅延時間の分布特性が変化したか否かを判定する。

【０１７１】

通信端末２００が真のスマートフォンである場合、通信端末２００は、電話通話を行うと、伝送遅延時間が一時的又は継続的に長くなったり、認証を行うための通信を中断したりする。そうすると、長い伝送遅延時間の分布が増えたり、伝送遅延時間の分布が全体的に減ったりといった変化が生じる。一方、通信端末２００が偽のスマートフォンである場合、通信端末２００は、電話通話を行っても、伝送遅延時間が一時的又は継続的に長くなったり、認証を行うための通信を中断したりすることもない。このため、電話通話を行ったときの伝送遅延時間の分布特性の変化を検出することで、通信端末２００がスマートフォン又は有線のコンピュータのいずれであるのかを判別することができる。

【０１７２】

通話変化判定ステップを有する場合、コンテンツ閲覧認証ステップにおいて、本実施形態に係るコンテンツ提供システムは、以下のように動作する。

コンテンツ閲覧認証部４２は、分布特性判定部３６において離散的であると判定しかつ通話変化判定部４１において伝送遅延時間の分布特性が変化したと判定した場合、コンテンツの閲覧を承認する。すると、データ通信部３２は、コンテンツの閲覧の承認を通信端末２００に通知するとともに、コンテンツ格納部３１の格納するコンテンツを通信端末２００に提供する。

一方、コンテンツ閲覧認証部４２は、分布特性判定部３６において離散的でないと判定するか又は通話変化判定部４１において伝送遅延時間の分布特性が変化なかったと判定した場合、コンテンツの閲覧を拒否する。すると、データ通信部３２は、コンテンツ格納部

３１の格納するコンテンツを通信端末２００に送信せず、コンテンツの閲覧の拒否を通信端末２００に通知する。

【０１７３】

また、通話変化判定ステップの直前、直後又はこれと同時に、通話判定ステップをさらに有していても良い。この場合、認証サーバ１０４は、通話判定部３８をさらに備え、コンテンツ閲覧認証ステップにおいて、本実施形態に係るコンテンツ提供システムは、以下のように動作する。

コンテンツ閲覧認証部４２は、分布特性判定部３６において離散的であると判定しかつ通話変化判定部４１において伝送遅延時間の分布特性が変化したと判定しかつ通話判定部３８において着信応答を受信したと判定した場合、コンテンツの閲覧を承認する。すると、データ通信部３２は、コンテンツの閲覧の承認を通信端末２００に通知するとともに、コンテンツ格納部３１の格納するコンテンツを通信端末２００に提供する。

一方、コンテンツ閲覧認証部４２は、分布特性判定部３６において離散的でないと判定するか、通話変化判定部４１において伝送遅延時間の分布特性が変化なかったと判定するか又は通話判定部３８において着信応答を受信しないと判定した場合、コンテンツの閲覧を拒否する。すると、データ通信部３２は、コンテンツ格納部３１の格納するコンテンツを通信端末２００に送信せず、コンテンツの閲覧の拒否を通信端末２００に通知する。これにより、通信端末がスマートフォン又はコンピュータのいずれであるかをさらに正確に判定することができる。

【０１７４】

添付の図面を参照して本第２の発明の実施形態を説明する。以下に説明する実施形態は本発明の実施の例であり、本発明は、以下の実施形態に制限されるものではない。なお、本明細書及び図面において符号が同じ構成要素は、相互に同一のものを示すものとする。

【０１７５】

（実施形態５）

実施形態５に係る認証サーバの構成を図１５に示す。認証サーバ１は、通信端末２から閲覧認証を受け付けたときに、通信端末２が正規の携帯電話３Ａであれば、閲覧を承認し、通信端末２が携帯電話３Ｃになりすました非正規の携帯電話３Ｂであれば、閲覧を拒否する。

【０１７６】

認証サーバ１は、コンテンツ格納部５１、データ通信部５２、識別子（ＩＤ）／電話番号対応テーブル５３、電話通信部５４、伝送遅延時間測定部５５、伝送遅延時間変化判断部５６及びコンテンツ閲覧認証部５７から構成される。

【０１７７】

コンテンツ格納部５１は、コンテンツを格納する。データ通信部５２は、コンテンツの閲覧のための認証を行う通信端末２とデータ通信を行う。ＩＤ／電話番号対応テーブル５３は、通信端末２のＩＤ及び電話番号を対応付ける。電話通信部５４は、データ通信部５２がＩＤを利用したコンテンツの閲覧のための認証を通信端末２から行われたときに、ＩＤ／電話番号対応テーブル５３でそのＩＤと対応付けられた電話番号を利用した電話通信を実行する。なお、この電話通信は、人間の音声のデータのみならず、あらゆるデータをも伝送する。ここで、不図示の対応テーブルが、通信端末２のパスワード及び電話番号を対応付けてもよい。以下は、通信端末２のＩＤ及び電話番号を対応付ける場合を説明する。

【０１７８】

伝送遅延時間測定部５５は、データ通信部５２及び通信端末２の間の伝送遅延時間を複数回にわたり測定する。伝送遅延時間変化判断部５６は、電話通信部５４が電話通信を実行しているときに、電話通信部５４が電話通信を実行していないときと比べて、伝送遅延時間測定部５５が測定している伝送遅延時間に変化があるかどうかを判断する。

【０１７９】

コンテンツ閲覧認証部５７は、伝送遅延時間変化判断部５６が伝送遅延時間に変化があ

ると判断したときに、その通信端末２が正規の携帯電話３Ａであると判断し、コンテンツの閲覧を承認する。

【０１８０】

正規の携帯電話３ＡのＩＤ及び電話番号は、それぞれ第１のＩＤ及び第１の電話番号であり、ＩＤ／電話番号対応テーブル５３で対応付けられている。つまり、データ通信及び電話通信は、正規の携帯電話３Ａ及び認証サーバ１の間で実行されており、無線通信チャネルを共有している。よって、電話通信が実行されたときには、データ通信に割り込みが発生して、伝送遅延時間に変化が発生する。

【０１８１】

コンテンツ閲覧認証部５７は、伝送遅延時間変化判断部５６が伝送遅延時間に変化がないと判断したときに、その通信端末２が携帯電話３Ｃになりすました非正規の携帯電話３Ｂであると判断し、コンテンツの閲覧を拒否する。

【０１８２】

携帯電話３ＣのＩＤ及び電話番号は、それぞれ第２のＩＤ及び第２の電話番号であり、ＩＤ／電話番号対応テーブル５３で対応付けられている。ここで、携帯電話３Ｃになりすました非正規の携帯電話３Ｂは、ＩＤを改竄することはできても、電話番号を改竄することはできない。つまり、データ通信は、非正規の携帯電話３Ｂ及び認証サーバ１の間で実行されていても、電話通信は、携帯電話３Ｃ及び認証サーバ１の間で実行されており、両通信は、無線通信チャネルを共有していない。よって、電話通信が実行されたときでも、データ通信に割り込みが発生せず、伝送遅延時間に変化が発生しない。

【０１８３】

認証サーバの処理を図１６に示す。コンテンツ閲覧認証受付ステップでは、データ通信部５２は、通信端末２の行うコンテンツの閲覧のための認証を受け付ける（ステップＳ１０１）。

【０１８４】

電話通信実行ステップでは、伝送遅延時間測定部５５が、通信端末２との間の伝送遅延時間を複数回にわたり測定する間に（ステップＳ１０２）、電話通信部５４が、コンテンツの閲覧のための認証に利用されたＩＤに対応付けられた電話番号をＩＤ／電話番号対応テーブル５３により検索し（ステップＳ１０３）、その電話番号を利用した電話通信を実行する（ステップＳ１０４）。

【０１８５】

伝送遅延時間変化判断ステップでは、伝送遅延時間変化判断部５６は、電話通信部５４が電話通信を実行しているときに、電話通信部５４が電話通信を実行していないときと比べて、伝送遅延時間測定部５５が測定している伝送遅延時間に変化があるかどうかを判断する（ステップＳ１０５）。伝送遅延時間変化判断ステップについては、図１８で詳述する。

【０１８６】

コンテンツ閲覧認証ステップでは、コンテンツ閲覧認証部５７は、伝送遅延時間変化判断部５６が伝送遅延時間に変化があると判断したときに（ステップＳ１０５においてＹＥＳ）、その通信端末２が正規の携帯電話３Ａであると判断し（ステップＳ１０６）、コンテンツの閲覧を承認する（ステップＳ１０７）。そして、データ通信部５２は、コンテンツの閲覧の承認を正規の携帯電話３Ａに通知するとともに、コンテンツ格納部５１の格納するコンテンツを正規の携帯電話３Ａに提供する。ただし、データ通信部５２は、コンテンツの閲覧の承認に代えて、コンテンツ格納部５１の格納するコンテンツのみを正規の携帯電話３Ａに提供してもよい。

【０１８７】

コンテンツ閲覧認証部５７は、伝送遅延時間変化判断部５６が伝送遅延時間に変化がないと判断したときに（ステップＳ１０５においてＮＯ）、その通信端末２が携帯電話３Ｃになりすました非正規の携帯電話３Ｂであると判断し（ステップＳ１０８）、コンテンツの閲覧を拒否する（ステップＳ１０９）。そして、データ通信部５２は、コンテンツの閲

覧の拒否を非正規の携帯電話３Ｂに通知する。

【０１８８】

本第２の発明によれば、認証を行った通信端末及び電話通信を受けた通信端末が同一の通信端末であるかどうかを確認することができる。そのため、携帯電話のユーザに限定してコンテンツを閲覧させるときに、携帯電話のユーザが正規のユーザであるかどうかを安全にかつ正確に判断することができる。

【０１８９】

次に、電話通信実行ステップの詳細について説明する。伝送遅延時間の測定方法を図１７に示す。通信端末２は、リクエストＧＥＴ１を認証サーバ１に送信し、ウェブのトップページを要求する。データ通信部５２は、レスポンスＲＥＳ１を通信端末２に送信し、ＨＴＭＬファイルを提供する。通信端末２は、ＨＴＭＬファイルを解析し、ＨＴＭＬファイルに包含される複数の画像ファイルを以下のように要求する。

【０１９０】

通信端末２は、リクエストＧＥＴ２を認証サーバ１に送信し、画像ファイルｅ１を要求する。データ通信部５２は、レスポンスＲＥＳ２を通信端末２に送信し、画像ファイルｅ１を提供する。通信端末２は、リクエストＧＥＴ３を認証サーバ１に送信し、画像ファイルｅ２を要求する。データ通信部５２は、レスポンスＲＥＳ３を通信端末２に送信し、画像ファイルｅ２を提供する。通信端末２は、リクエストＧＥＴ４を認証サーバ１に送信し、画像ファイルｅ３を要求する。データ通信部５２は、レスポンスＲＥＳ４を通信端末２に送信し、画像ファイルｅ３を提供する。通信端末２がＨＴＭＬファイルに包含される全ての画像ファイルを取得するまで、以上の処理が繰り返される。

【０１９１】

伝送遅延時間測定部５５は、リクエストＧＥＴ２を通信端末２から受信してから次にリクエストＧＥＴ３を通信端末２から受信するまでの時間Δｔ１を、データ通信部５２から通信端末２までの伝送遅延時間及び通信端末２からデータ通信部５２までの伝送遅延時間の合計として測定する。伝送遅延時間測定部５５は、リクエストＧＥＴ３を通信端末２から受信してから次にリクエストＧＥＴ４を通信端末２から受信するまでの時間Δｔ２を、データ通信部５２から通信端末２までの伝送遅延時間及び通信端末２からデータ通信部５２までの伝送遅延時間の合計として測定する。データ通信部５２がＨＴＭＬファイルに包含される全ての画像ファイルを提供するまで、以上の処理が繰り返される。

【０１９２】

ここで、伝送遅延時間測定部５５は、リクエストＧＥＴ１を通信端末２から受信してから次にリクエストＧＥＴ２を通信端末２から受信するまでの時間を測定しないことが好ましい。これは、当該時間が、データ通信部５２から通信端末２までの伝送遅延時間及び通信端末２からデータ通信部５２までの伝送遅延時間を含むのみならず、通信端末２でのＨＴＭＬファイルの解析時間をさらに含むためである。

【０１９３】

正規の携帯端末３Ａは、ウェブブラウザを有していればよく、伝送遅延時間の測定用のソフトウェアを有していなくてもよく、新しいソフトウェアの開発は不要である。

【０１９４】

携帯電話３Ａによってはパイプライン処理を行うものがある。パイプライン処理は、要求信号をまとめて送信することで、ページのアクセスを高速にすることができる処理である。例えば、図２０に示すように、通信端末２が、画像ファイルｅ１の要求信号であるリクエストＧＥＴ２と、画像ファイルｅ２の要求信号であるリクエストＧＥＴ３と、画像ファイルｅ３の要求信号であるリクエストＧＥＴ４と、をまとめて送信する。このようなパイプライン処理を行う携帯電話３Ａの場合、携帯電話２Ａがリクエスト ＧＥＴ２及びリクエストＧＥＴ３をほぼ同時に送信するため、リクエストＧＥＴ２からリクエストＧＥＴ３までの時間を測定しても、伝送遅延時間の合計を測定することができない。そこで、認証サーバ１のデータ通信部５２は、１つの要求信号の受信と１つのデータ要素の送信を順に繰り返す。そして、伝送遅延時間測定部５３は、各々の要求信号が受信された間隔を測定

することにより伝送遅延時間の合計を測定する。

【０１９５】

例えば、データ通信部５２は、リクエストＧＥＴ２、リクエストＧＥＴ３及びリクエストＧＥＴ４をまとめて受信すると、リクエストＧＥＴ２に対するレスポンスＲＥＳ２を通信端末２に送信し、その後にレスポンスＲＥＳ２の送信後にデータ通信部５２がＴＣＰのコネクションをｃｌｏｓｅする。このように、リクエストＧＥＴ３及びリクエストＧＥＴ４に対してはレスポンスＲＥＳ３及びレスポンスＲＥＳ４を送信しない。これにより、通信端末２は、レスポンスＲＥＳ２の受信後に、改めてリクエストＧＥＴ３を送信する。

【０１９６】

伝送遅延時間測定部５３は、まとめて受信したリクエストＧＥＴ２、リクエストＧＥＴ３及びリクエストＧＥＴ４のうちのリクエストＧＥＴ２を受信してから、再送させたリクエストＧＥＴ３を受信するまでの時間Δｔ１を、データ通信部５２から通信端末２までの伝送遅延時間及び通信端末２からデータ通信部５２までの伝送遅延時間の合計として測定する。

【０１９７】

また、パイプライン処理を行う携帯電話３Ａに対応するために、ウェブのトップページを要求するリクエストＧＥＴ１を受信したデータ通信部５２は、パイプライン処理に対応していない旨の情を通信端末２に送信し、通信端末２のパイプライン処理を停止させてもよい。具体的には、ＨＴＴＰ／１．０又はＨＴＴＰ／０．９の仕様のＨＴＴＰである旨を通信端末２に送信する。こうすることで、図１７に示すような、１つの要求信号の受信と１つのデータ要素の送信を順に繰り返す伝送遅延時間の測定を行うことができる。

【０１９８】

図２１に、伝送遅延時間測定部５３における他の伝送遅延時間測定方法の一例を示す。通信端末２は、画像ファイルｅ２を受信すると、ＴＣＰのクローズ信号（ＦＩＮ）Ｃ２を認証サーバ１に送信する。本方式は、このＴＣＰのクローズ信号（ＦＩＮ）を利用し、認証サーバ１が要求信号を受信してから、データ要素を送信後のクローズ信号を受信するまでの間隔を、伝送遅延時間として測定する。例えば、伝送遅延時間測定部５３は、認証サーバ１がリクエストＧＥＴ２を受信してから、クローズ信号Ｃ２を通信端末２から受信するまでの間隔を、伝送遅延時間Δｔ１として測定する。

【０１９９】

この方式は、パイプライン方式ではなく、ＴＣＰのコネクションを同時に複数確立する場合に適用できる。このため、複数のコネクションの数分だけ、同時に伝送遅延時間を測定することができるとともに、画像のダウンロードの高速化を図ることができる。画像のサイズが大きい場合には、後から送られたリクエストＧＥＴに対するクローズ時間が遅くなるので、伝送遅延時間が長くなることが予想されるが、通信端末２と認証サーバ１間の伝送遅延特性は含まれているので、処理データとして使用することができる。

【０２００】

次に、伝送遅延時間変化判断ステップの詳細について説明する。伝送遅延時間の変化内容を図１８及び図１９に示す。伝送遅延時間の変化内容の一例として、正規の携帯電話３Ａからの閲覧認証時における伝送遅延時間の時間変化を図１８に示し、非正規の携帯電話３Ｂからの閲覧認証時における伝送遅延時間の時間変化を図１９に示す。

【０２０１】

まず、伝送遅延時間の時間変化の第１の例について説明する。伝送遅延時間変化判断部５６は、図１８及び図１９に示したように、電話通信部５４が電話通信を実行しているときに、電話通信部５４が電話通信を実行していないときと比べて、伝送遅延時間測定部５５が測定している伝送遅延時間に増加があるかどうかを判断する。

【０２０２】

コンテンツ閲覧認証部５７は、図１８に示したように、伝送遅延時間変化判断部５６が伝送遅延時間に増加があると判断したときに、その通信端末２が正規の携帯電話３Ａであると判断し、コンテンツの閲覧を承認する。電話通信が中止された後に、電話通信が開始

される前のように、伝送遅延時間が元に戻る。

【０２０３】

コンテンツ閲覧認証部５７は、図１９に示したように、伝送遅延時間変化判断部５６が伝送遅延時間に増加がないと判断したときに、その通信端末２が非正規の携帯電話３Ｂであると判断し、コンテンツの閲覧を拒否する。

【０２０４】

次に、伝送遅延時間の時間変化の第２の例について説明する。伝送遅延時間変化判断部５６は、電話通信部５４が電話通信を実行しているときに、電話通信部５４が電話通信を実行していないときと比べて、データ通信部５２が通信端末２から伝送遅延時間の測定用のパケットを受信していないかどうかを判断する。ここで、伝送遅延時間の測定用のパケットは、例えば図１７に示したリクエストＧＥＴ２、ＧＥＴ３、ＧＥＴ４、・・・である。

【０２０５】

コンテンツ閲覧認証部５７は、伝送遅延時間変化判断部５６が伝送遅延時間の測定用のパケットの受信がないと判断したときに、その通信端末２が正規の携帯電話３Ａであると判断し、コンテンツの閲覧を承認する。電話通信が中止された後に、伝送遅延時間の測定用のパケットが再送されてもされなくてもよい。

【０２０６】

コンテンツ閲覧認証部５７は、伝送遅延時間変化判断部５６が伝送遅延時間の測定用のパケットの受信があると判断したときに、その通信端末２が非正規の携帯電話３Ｂであると判断し、コンテンツの閲覧を拒否する。

【０２０７】

次に、伝送遅延時間の時間変化の第３の例について説明する。伝送遅延時間変化判断部５６は、電話通信部５４が電話通信を実行しているときに、電話通信部５４が電話通信を実行していないときと比べて、伝送遅延時間測定部５５が測定している伝送遅延時間に減少があるかどうかを判断する。ここで、伝送遅延時間が減少する可能性があるのは、電話通信がデータ通信に割り込んだときに、正規の携帯電話３Ａ又は非正規の携帯電話３Ｂが処理能力を増大させる可能性があるためである。

【０２０８】

コンテンツ閲覧認証部５７は、伝送遅延時間変化判断部５６が伝送遅延時間に減少があると判断したときに、その通信端末２が正規の携帯電話３Ａであると判断し、コンテンツの閲覧を承認する。電話通信が中止された後に、電話通信が開始される前のように、伝送遅延時間が元に戻る。

【０２０９】

コンテンツ閲覧認証部５７は、伝送遅延時間変化判断部５６が伝送遅延時間に減少がないと判断したときに、その通信端末２が非正規の携帯電話３Ｂであると判断し、コンテンツの閲覧を拒否する。

【０２１０】

伝送遅延時間の変化内容は、正規の携帯電話３Ａ毎に様々に設定されてもされなくてもよい。正規の携帯電話３Ａ毎に設定されるときには、認証サーバ１の不図示の記憶部が変化内容を記憶すればよい。正規の携帯電話３Ａ毎に設定されないときには、伝送遅延時間変化判断部５６が何らかの変化があるかどうかを判断すればよい。

【０２１１】

本実施形態では、コンテンツ閲覧認証部５７は、伝送遅延時間に変化があるかどうかに応じて、コンテンツの閲覧を承認するかどうかを判断する。他の実施形態では、コンテンツ閲覧認証部５７は、伝送遅延時間に変化があるかどうか及び電話通信に対し通信端末２から着信応答がなされたかどうかに応じて、コンテンツの閲覧を承認するかどうかを判断する。

【０２１２】

つまり、他の実施形態では、コンテンツ閲覧認証部５７は、伝送遅延時間変化判断部５

６が伝送遅延時間に変化があると判断したうえに、電話通信に対し通信端末２から着信応答がなされたときに、その通信端末２が正規の携帯電話３Ａであると判断し、コンテンツの閲覧を承認する。そして、コンテンツ閲覧認証部５７は、伝送遅延時間変化判断部５６が伝送遅延時間に変化があると判断したところ、電話通信に対し通信端末２から着信応答がなされなかったときに、その通信端末２が携帯電話３Ｃになりすました非正規の携帯電話３Ｂであると判断し、コンテンツの閲覧を拒否する。これにより、携帯電話のユーザが正規のユーザであるかどうかをより安全にかつ正確に判断することができる。ここで、通信端末２がユーザの音声を検知することにより、着信応答を返してもよく、通信端末２が自己にインストールされたソフトウェアを用いて自動音声を出力することにより、着信応答を返してもよい。さらに、通信端末２がユーザの受信ボタン押下を検知することにより、着信応答を返してもよく、通信端末２が自己にインストールされたソフトウェアを用いて信号を送出することにより、着信応答を返してもよい。

【０２１３】

本実施形態では、認証サーバ１がコンテンツ格納部５１においてコンテンツを格納している。他の実施形態では、認証サーバ１はコンテンツを格納しておらず、認証サーバ１以外のコンテンツサーバがコンテンツを格納してもよい。このとき、データ通信部５２は、コンテンツの閲覧の承認を正規の携帯電話３Ａに通知するとともに、認証サーバ１以外のコンテンツサーバの格納するコンテンツを正規の携帯電話３Ａに提供すればよい。

【０２１４】

本実施形態では、正規の携帯電話３Ａ又は非正規の携帯電話３Ｂが、閲覧要求を発行し閲覧可否を通知されている。他の実施形態では、正規の携帯電話３Ａ以外の他の装置が、閲覧要求を発行し閲覧承認を通知されてもよい。ただし、本実施形態及び他の実施形態の両方において、正規の携帯電話３Ａが閲覧認証を行うことに変わりはない。つまり、他の実施形態では、他の装置が閲覧要求を発行し、認証サーバ１が正規の携帯電話３Ａに認証要求を発行し、正規の携帯電話３Ａが閲覧認証を行い、認証サーバ１が他の装置に閲覧承認を通知しコンテンツを提供する。ただし、認証サーバ１が閲覧認証に代えてコンテンツのみを提供してもよい。このとき、認証サーバ１は、他の装置及び正規の携帯電話３Ａに関する情報を対応付けて記憶している。

【産業上の利用可能性】

【０２１５】

本第１の発明は情報通信産業に適用することができる。

【０２１６】

本第２の発明に係る認証サーバ及び認証サーバによる認証方法は、携帯電話のユーザに限定してコンテンツを閲覧させるときに利用することができる。

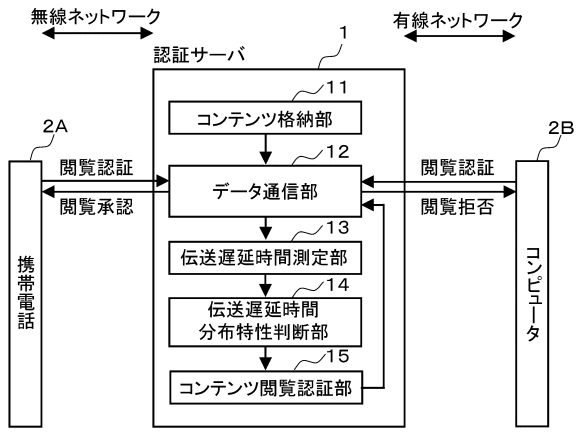
【符号の説明】

【０２１７】

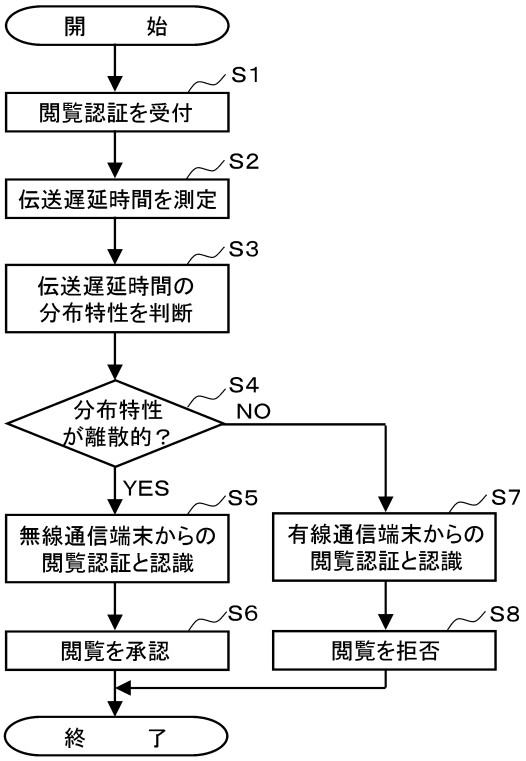
１：認証サーバ
２：通信端末
２Ａ：携帯電話
２Ｂ：コンピュータ
１１：コンテンツ格納部
１２：データ通信部
１３：伝送遅延時間測定部
１４：伝送遅延時間分布特性判断部
１５：コンテンツ閲覧認証部
３１：コンテンツ格納部
３２：データ通信部
３３：伝送遅延時間測定部
３４：分布特性算出部
３５：抽出部

３６：分布特性判定部
３７、４２：コンテンツ閲覧認証部
３８：通話判定部
４１：通話変化判定部
１０３、１０４：認証サーバ
２００：通信端末
１：認証サーバ
２：通信端末
３Ａ、３Ｂ、３Ｃ：携帯電話
５１：コンテンツ格納部
５２：データ通信部
５３：ＩＤ／電話番号対応テーブル
５４：電話通信部
５５：伝送遅延時間測定部
５６：伝送遅延時間変化判断部
５７：コンテンツ閲覧認証部

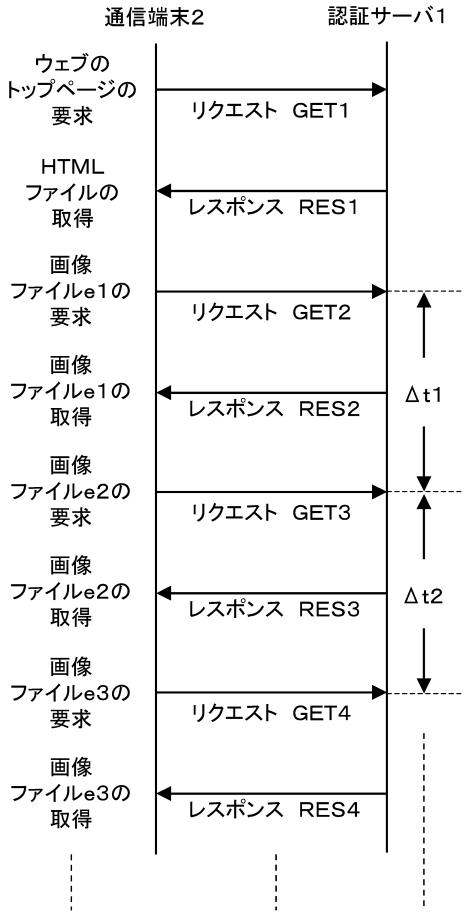
【図１】



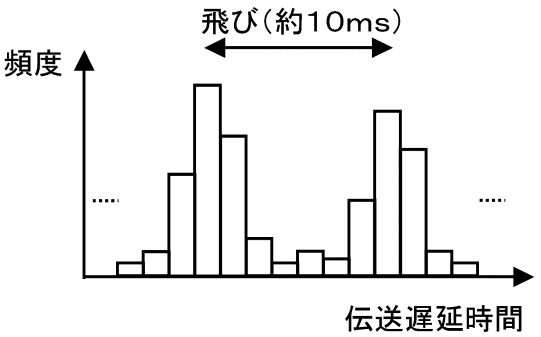
【図２】



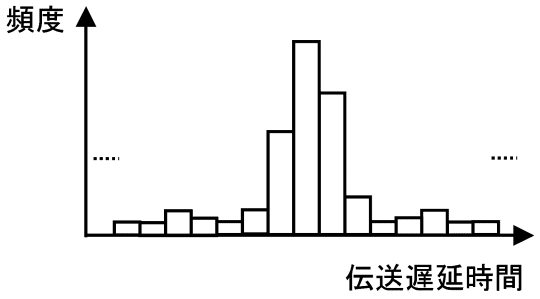
【図３】


通信端末2
認証サーバ1
ウェブの
トップページの
要求
リクエスト GET1
HTML
ファイルの
取得
レスポンス RES1
画像
ファイルe1の
要求
リクエスト GET2
Δt1
画像
ファイルe1の
取得
レスポンス RES2
画像
ファイルe2の
要求
リクエスト GET3
Δt2
画像
ファイルe2の
取得
レスポンス RES3
画像
ファイルe3の
要求
リクエスト GET4
画像
ファイルe3の
取得
レスポンス RES4

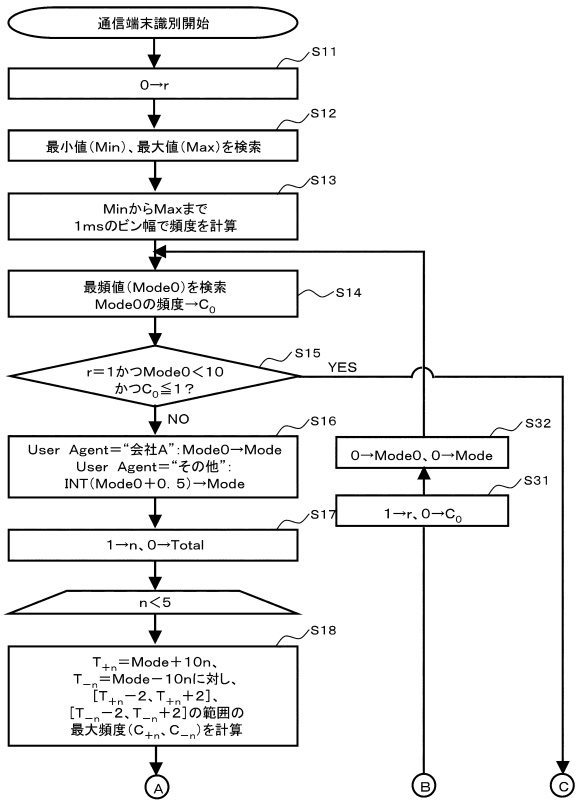
【図４】


飛び（約10ms）
頻度
伝送遅延時間

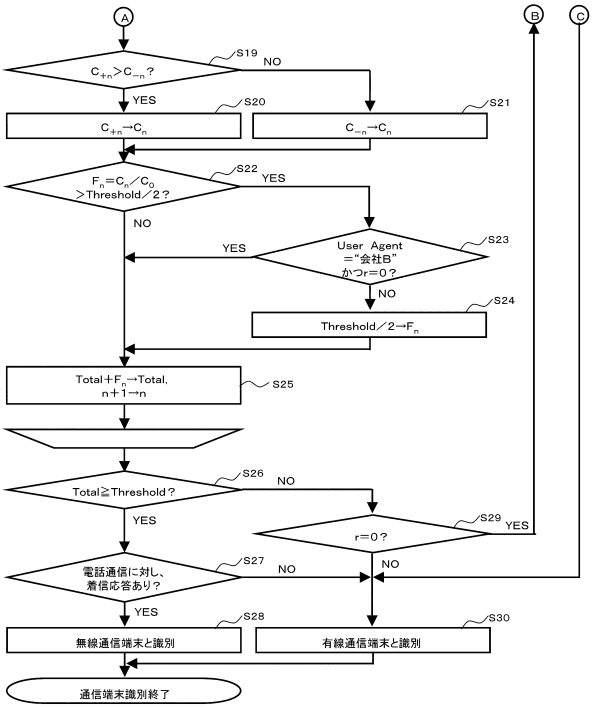
【図５】


頻度
伝送遅延時間

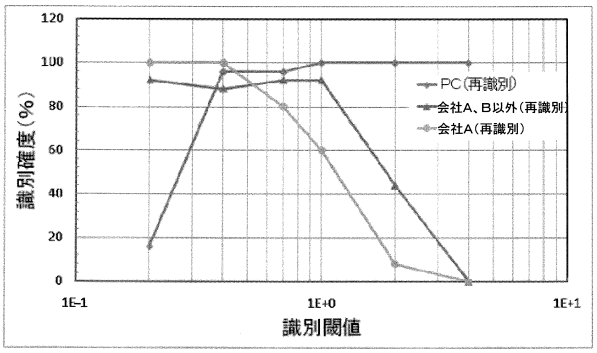
【図６】


通信端末識別開始
S11
0→r
S12
最小値（Min）、最大値（Max）を検索
S13
MinからMaxまで
1msのビン幅で頻度を計算
最頻値（Mode0）を検索
Mode0の頻度→C0
S14
S15
r＝1かつMode0＜10
かつC0≦1？
YES
NO
S16
User Agent＝“会社A”：Mode0→Mode
User Agent＝“その他”：
INT（Mode0＋0．5）→Mode
S17
1→n、0→Total
n＜5
S18
T+n＝Mode＋10n、
T−n＝Mode−10nに対し、
[T+n−2、T+n＋2]、
[T−n−2、T−n＋2]の範囲の
最大頻度（C+n、C−n）を計算
A
S32
0→Mode0、0→Mode
S31
1→r、0→C0
B
C

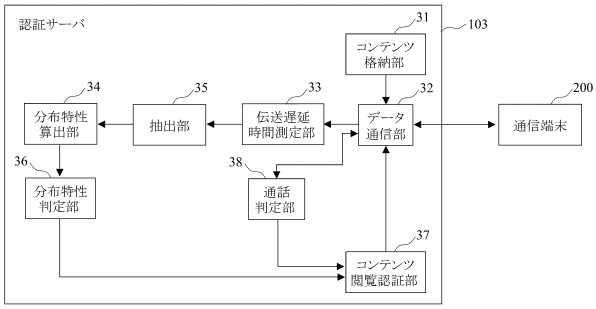
【図７】


A
B
C
S19
C+n＞C−n？
NO
YES
S20
C+n→Cn
S21
C−n→Cn
S22
Fn＝Cn／C0
＞Threshold／2？
YES
NO
S23
User Agent
＝“会社B”
かつr＝0？
YES
NO
S24
Threshold／2→Fn
S25
Total＋Fn→Total、
n＋1→n
S26
Total≧Threshold？
NO
YES
S29
r＝0？
YES
NO
S27
電話通信に対し、
着信応答あり？
NO
YES
S28
無線通信端末と識別
S30
有線通信端末と識別
通信端末識別終了

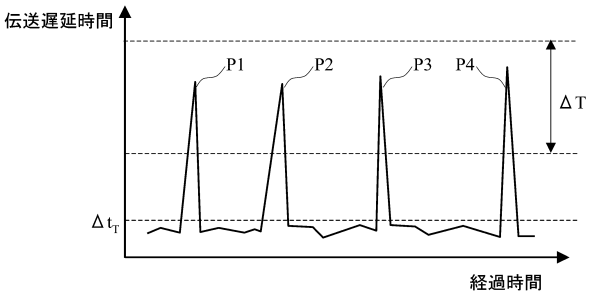
【図８】



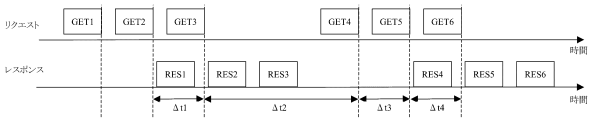
【図９】



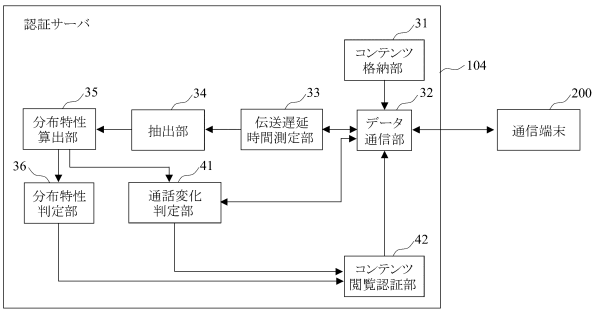
【図１０】



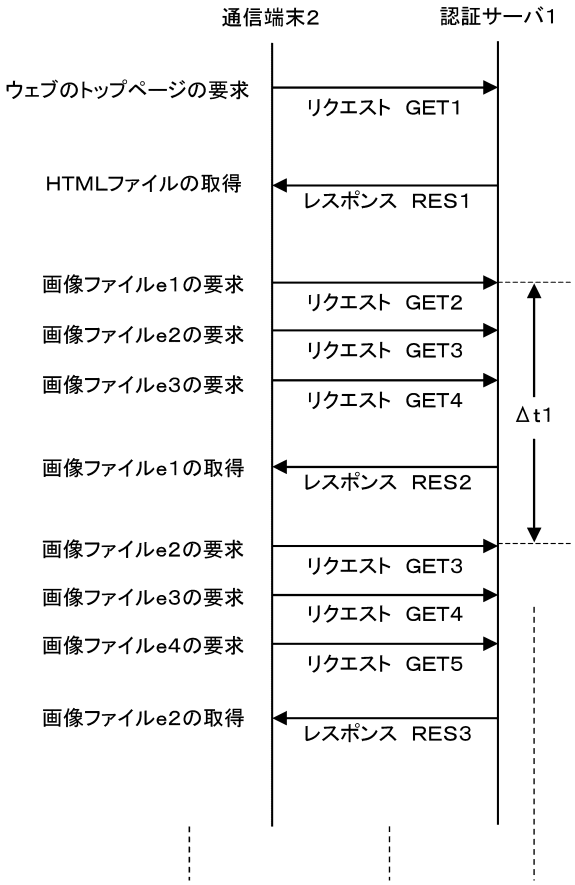
【図１１】



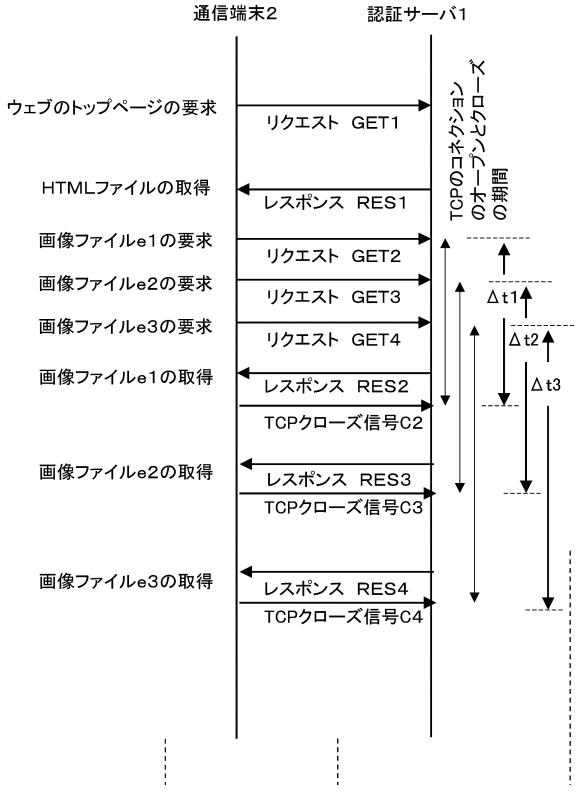
【図１２】



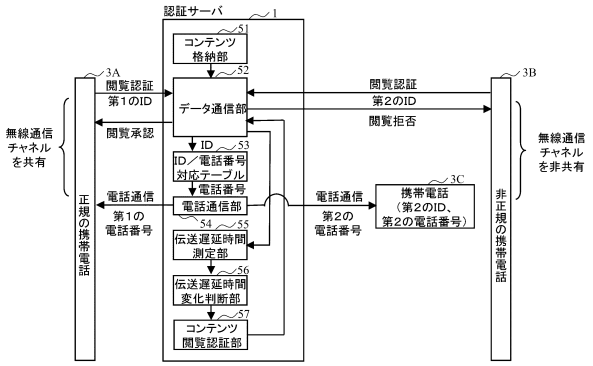
【図１３】



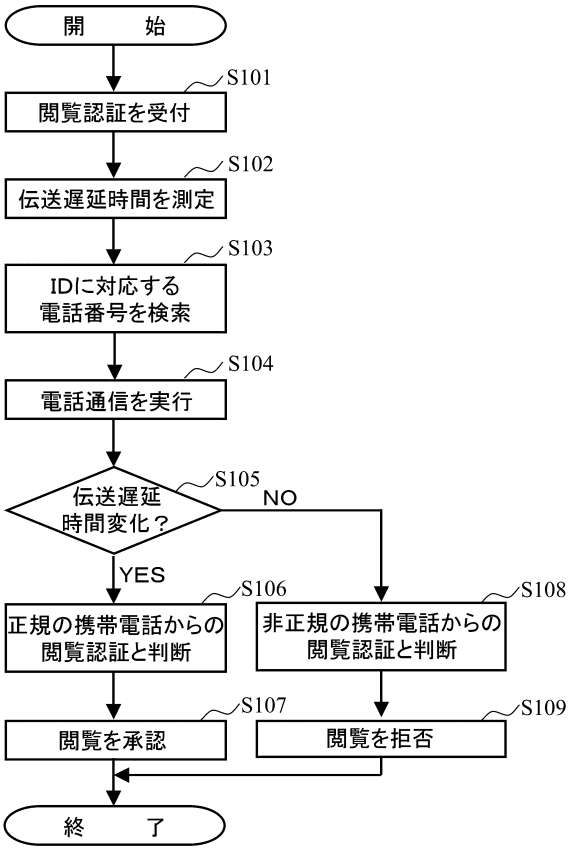
【図１４】



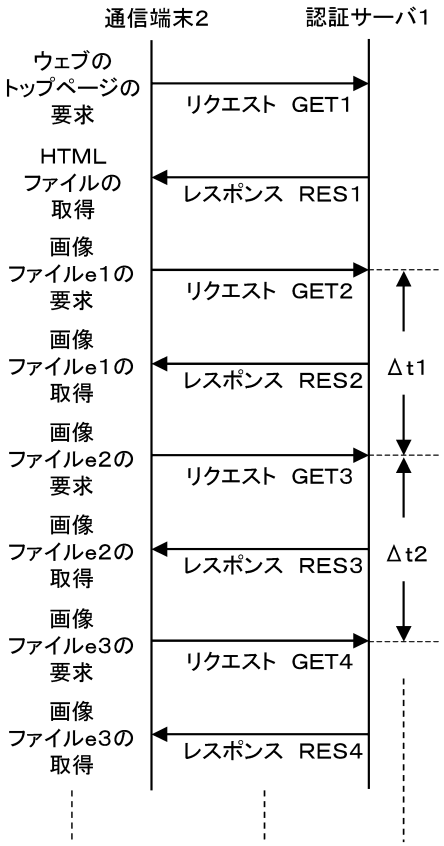
【図１５】



【図１６】

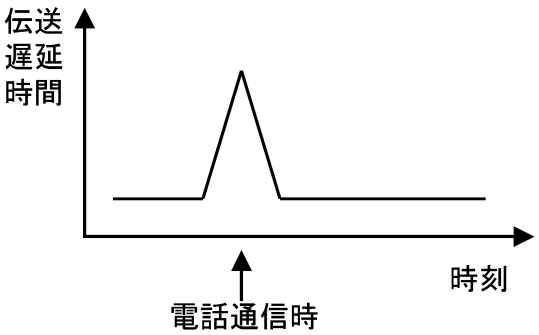


【図１７】

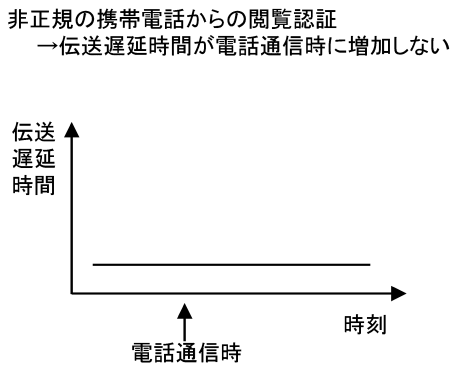


【図１８】

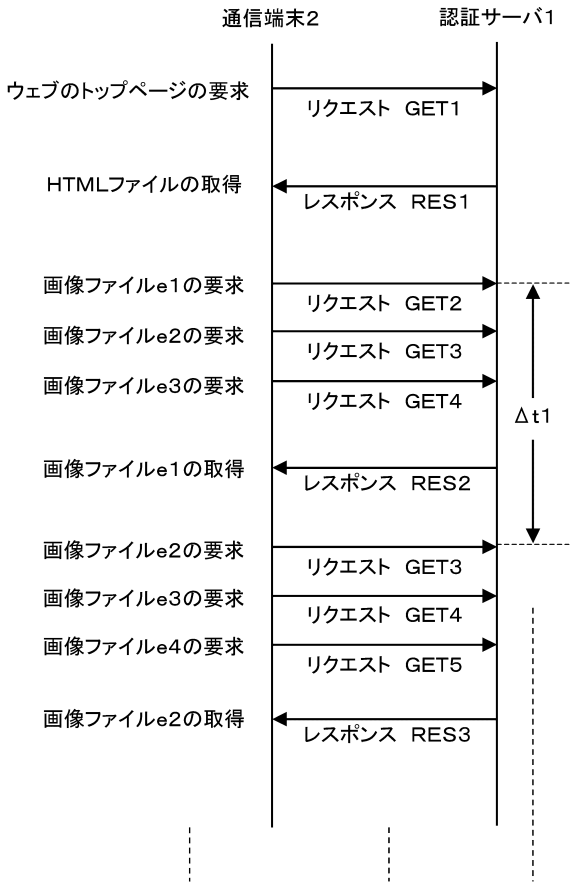
正規の携帯電話からの閲覧認証
　→伝送遅延時間が電話通信時に増加する



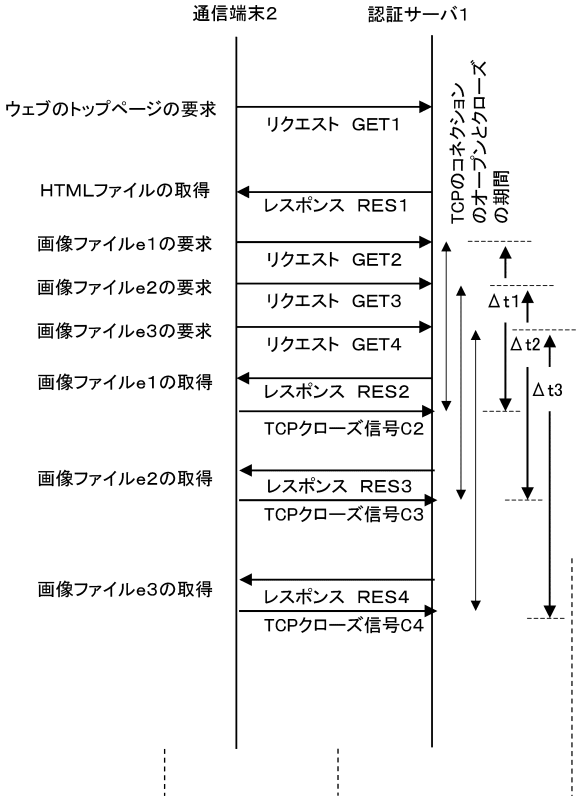
【図１９】


非正規の携帯電話からの閲覧認証
→伝送遅延時間が電話通信時に増加しない
伝送
遅延
時間
時刻
電話通信時

【図２０】


通信端末2
認証サーバ1
ウェブのトップページの要求
リクエスト GET1
HTMLファイルの取得
レスポンス RES1
画像ファイルe1の要求
リクエスト GET2
画像ファイルe2の要求
リクエスト GET3
画像ファイルe3の要求
リクエスト GET4
Δt1
画像ファイルe1の取得
レスポンス RES2
画像ファイルe2の要求
リクエスト GET3
画像ファイルe3の要求
リクエスト GET4
画像ファイルe4の要求
リクエスト GET5
画像ファイルe2の取得
レスポンス RES3

【図２１】


通信端末2
認証サーバ1
ウェブのトップページの要求
リクエスト GET1
HTMLファイルの取得
レスポンス RES1
画像ファイルe1の要求
リクエスト GET2
画像ファイルe2の要求
リクエスト GET3
画像ファイルe3の要求
リクエスト GET4
画像ファイルe1の取得
レスポンス RES2
TCPクローズ信号C2
画像ファイルe2の取得
レスポンス RES3
TCPクローズ信号C3
画像ファイルe3の取得
レスポンス RES4
TCPクローズ信号C4
TCPのコネクション
のオープンとクローズ
の期間
Δt1
Δt2
Δt3

フロントページの続き

特許法第３０条第１項適用　第５４回日本大学理工学部学術講演会論文集（平成２２年１１月２７日）学校法人日本大学理工学部発行第４９９ページ～第５００ページに発表

(56)参考文献　特開２００８－２８７５４２（ＪＰ，Ａ）
特開２００４－２２２２７０（ＪＰ，Ａ）
特表２００８－５２４６８１（ＪＰ，Ａ）
土屋貴寛，他，インターネットアクセスにおける伝送遅延を用いた携帯電話とＰＣの識別方法，２０１１年電子情報通信学会総合大会講演論文集 通信2，電子情報通信学会，２０１１年　２月２８日，p. 231
T. Tsuchiya et al., Transmission Time-based Authentication Scheme Using 3G Mobile Device for DRM System, Proceedings of the 2009 IEEE European Frequency and Time Forum & International Frequency Control Symposium, IEEE, ２００９年　4月, pp. 706-710, ［２０１１年１１月２４日検索］，インターネット，ＵＲＬ，http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5168275

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／５５
Ｈ０４Ｌ　９／３２
Ｈ０４Ｗ　１２／０６