

(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局



(43) 国際公開日
2012年5月18日(18.05.2012)

PCT

(10) 国際公開番号
WO 2012/063699 A1

- (51) 国際特許分類:
H04L 9/32 (2006.01) H04W 12/06 (2009.01)
G06F 21/20 (2006.01)
- (21) 国際出願番号: PCT/JP2011/075277
- (22) 国際出願日: 2011年11月2日(02.11.2011)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願 2010-250290 2010年11月8日(08.11.2010) JP
特願 2010-250292 2010年11月8日(08.11.2010) JP
特願 2011-117429 2011年5月25日(25.05.2011) JP
- (71) 出願人(米国を除く全ての指定国について): 学校法人日本大学(NIHON UNIVERSITY) [JP/JP]; 〒1028275 東京都千代田区九段南四丁目8番24号 Tokyo (JP).
- (72) 発明者; および
- (75) 発明者/出願人(米国についてのみ): 木原 雅巳(KIHARA, Masami) [JP/JP]; 〒1028275 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 Tokyo (JP). 土屋 貴寛(TSUCHIYA, Takahiro) [JP/JP]; 〒1028275 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 Tokyo (JP).

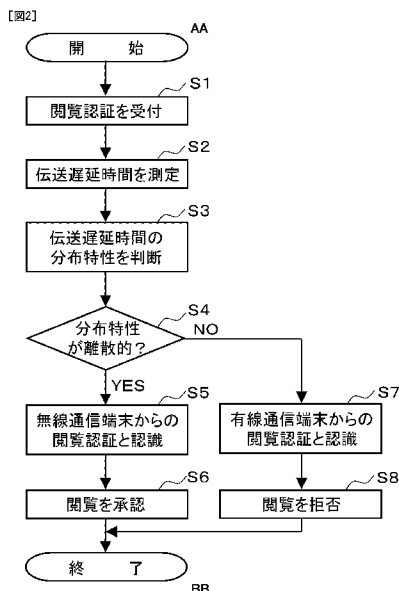
(74) 代理人: 岡田 賢治, 外(OKADA, Kenji et al.); 〒1050003 東京都港区西新橋二丁目12番5号瀬戸ロビル3階アイル知財事務所 Tokyo (JP).

(81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

[続葉有]

(54) Title: AUTHENTICATION SERVER AND AUTHENTICATION METHOD BY AUTHENTICATION SERVER

(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



AA START
S1 ACCEPT BROWSING AUTHENTICATION
S2 MEASURE TRANSMISSION DELAY TIME
S3 DETERMINE DISTRIBUTION CHARACTERISTIC OF TRANSMISSION DELAY TIME
S4 IS DISTRIBUTION CHARACTERISTIC DISCRETE?
S5 RECOGNIZE BROWSING AUTHENTICATION FROM WIRELESS COMMUNICATION TERMINAL
S6 APPROVE BROWSING
BB END
S7 RECOGNIZE BROWSING AUTHENTICATION FROM WIRED COMMUNICATION TERMINAL
S8 DENY BROWSING

(57) Abstract: The purpose of this first invention is to provide an authentication server capable of securely and accurately determining whether an access source is a portable phone or a computer when the browsing of contents is limited to portable phone users. This first invention is an authentication server (1) characterized by being provided with a transmission delay time measurement unit (13) which measures the transmission delay time between the authentication server (1) and a communication terminal (2) multiple times, a transmission delay time distribution characteristic determination unit (14) which determines whether the distribution characteristic of the transmission delay time measured multiple times is discrete, and a content browsing authentication unit (15) which recognizes the communication terminal (2) to be a wireless communication terminal and approves browsing when it is determined that the distribution characteristic of the transmission delay time is discrete and recognizes the communication terminal (2) to be a wired communication terminal and denies the browsing when it is determined that the distribution characteristic of the transmission delay time is not discrete.

(57) 要約: 本第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を提供することを目的とする。本第1の発明は、認証サーバ1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測定部13と、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伝送遅延時間分布特性判断部14と、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閲覧を拒否するコンテンツ閲覧認証部15と、を備えることを特徴とする認証サーバ1である。

- (84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).
- 規則 4.17 に規定する申立て:
- 不利にならない開示又は新規性喪失の例外に関する申立て (規則 4.17(v))
- 添付公開書類:
- 国際調査報告 (条約第 21 条(3))

明 細 書

発明の名称： 認証サーバ及び認証サーバによる認証方法

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は判断されたときに、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は判断されたときに、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接続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は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は判定するか又は

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接続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は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する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

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接続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、通信端末との接続を用いるため、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は判断されたときに、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 1 4 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 S 3 及び S 4）。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 1 5 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 S 4 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 S 5）、コンテンツの閲覧を承認する（ステップ S 6）。そして、データ通信部 1 2 は、コンテンツの閲覧の承認を携帯電話 2 A に通知するとともに、コンテンツ格納部 1 1 の格納するコンテンツを携帯電話 2 A に提供する。ただし、データ通信部 1 2 は、コンテンツの閲覧の承認に代えて、コンテンツ格納部 1 1 の格納するコンテンツのみを携帯電話 2 A に提供してもよい。コンテンツ閲覧認証部 1 5 は、伝送遅延時間の分布特性が離散的でないとは判断されたときに（ステップ S 4 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 S 7）、コンテンツの閲覧を拒否する（ステップ S 8）。そして、データ通信部 1 2 は、コンテンツの閲覧の拒否をコンピュータ 2 B に通知する。

[0077] 携帯電話 2 A 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 2 A 及びコンピュータ 2 B 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 2 B 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 GET 1 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 1 2 は、レスポンス RES 1 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 ファイルに含ま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 Δt_1 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 Δt_2 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 2 A 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 e 1 の要求信号であるリクエスト GET 2 と、画像ファイル e 2 の要求信号であるリクエスト GET 3 と、画像ファイル e 3 の要求信号であるリクエスト GET 4 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 2 A の場合、携帯電話 2 A がリクエスト GET 2 及びリクエスト GET 3 をほぼ同時に送信するため、リクエスト GET 2 からリクエスト GET 3 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 GET 2、リクエスト GET 3 及びリクエスト GET 4 をまとめて受信すると、リクエスト GET 2 に対するレスポンス RES 2 を通信端末 2 に送信し、その後にレスポンス RES 2 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 GET 3 及びリクエスト GET 4 に対してはレスポンス RES 3 及びレスポンス RES 4 を送信しない。これにより、通信端末 2 は、レスポンス RES 2 の受信後に、改めてリクエスト GET 3 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 GET 2、リクエスト GET 3 及びリクエスト GET 4 のうちのリクエスト GET 2 を受信してから、再送させたリクエスト GET 3 を受信するまでの時間 Δt_1 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 2 A 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GET 1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 Δt_1 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 $M_{\min}$ 及び最大値 $M_{\max}$ を検索する（ステップS12）。最小値 $M_{\min}$ から最大値 $M_{\max}$ 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 $M_{\text{mode } 0}$ を検索し、最頻値 $M_{\text{mode } 0}$ 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 $M_{\text{mode } 0}$ が10msの自然数倍であれば、最頻値 $M_{\text{mode } 0}$ 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Mode 0が10msの自然数倍の周辺であれば、最頻値Mode 0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Mode 0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Mode 0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Mode 0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Mode 0での頻度C₀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] $T_{+n} = \text{Mode} + 10n$ 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 S 18）。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 S 19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 S 20）。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 S 19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 S 21）。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もあり、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 S 22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 S 25）。 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 S 22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 S 23）。条件 X が成立するときには（ステップ S 23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 S 25）。条件 X が成立しないときには（ステップ S 23において NO）、例外として、所定の閾値の半

分 $\text{Threshold} / 2$ を新たな F_n としたうえで (ステップ S 2 4)、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 S 2 5)。

[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 S 1 8 から S 2 5 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 S 2 6)。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 S 2 6 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 S 2 8)。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 S 2 6 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 S 3 0)。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 2 B 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もあり、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 2 A は電話回線を使用することができるが、コンピュータ 2 B 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 2 A 及びコンピュータ 2 B 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 1 2 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 1 5 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 2 A 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 2 B 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 2 A 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 2 A 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 2 A 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 2 A 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 S 2 6 において Y E S）、電話通信に対して着信応答があったときには（ステップ S 2 7 において Y E S）、原則どおり、閲覧認証は携帯電話 2 A からであると識別する（ステップ S 2 8）。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 S 2 6 において Y E S）、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 S 2 7 において N O）、例外として、閲覧認証はコンピュータ 2 B のデータモジュールからであると識別する（ステップ S 3 0）。

[0106] 無線通信端末からの閲覧認証時でも、数 m s 又は 1 0 数 m s 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 *Mode 0* 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 *Mode 0* 以外で再び最頻値 *Mode 0* 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 S 2 6 において N O）、パラメータ *r* が 0 でないときには（ステップ S 2 9 において N O）、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 S 3 0）。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 S 2 6 において N O）、パラメータ *r* が 0 であるときには（ステップ S 2 9 において Y E S）、例外として、再識別を行うためにステップ S 3 1 及び S 3 2 に進む。

[0108] ステップ S 3 1 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Mode 0での頻度C₀を0にセットする。ステップS 3 2では、最頻値Mode 0及び最頻値Modeを0にリセットする。ステップS 3 1及びS 3 2を行ったうえで、ステップS 1 4及びS 1 5に進む。ステップS 1 5では、パラメータrが1でありかつ最頻値Mode 0が10msより小さくかつ最頻値Mode 0での頻度C₀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S 1 5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S 3 0）。条件Yが成立しないときには（ステップS 1 5においてNO）、ステップS 1 6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S 2 6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S 2 6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 *Threshold* 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 2 A に提供すればよい。

[0116] 本実施形態では、携帯電話 2 A 又はコンピュータ 2 B 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 2 A 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 2 A 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 2 A に認証要求を発行し、携帯電話 2 A 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 2 A 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 1 2 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 1 5 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 1 5 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 S 2 7 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 2 A 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 2 B 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 2 0 0 が携帯電話 2 A 又はコンピュータ 2 B 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 2 A からであると識別し（ステップ S 2 8）、分布特性が変化しない場合にはステップ S 3 0 に移行する。

[0120] また、図 7 に示すステップ S 2 7 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 S 2 8 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 2 B のデータモジュールからであると識別する（ステップ S 3 0）。これにより、通信端末が携帯電話 2 A 又はコンピュータ 2 B 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 1 0 3 は、通信端末 2 0 0 にコンテンツを提供するに際し、通信端末 2 0 0 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 1 0 3 は、通信端末 2 0 0 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 2 0 0 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 1 0 3 は、コンテンツ格納部 3 1 と、データ通信部 3 2 と、伝送遅延時間測定部 3 3 と、抽出部 3 5 と、分布特性算出部 3 4 と、分布特性判定部 3 6 と、コンテンツ閲覧認証部 3 7 と、通話判定部 3 8 と、を備える。コンテンツ格納部 3 1 は、通信端末 2 0 0 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 が離散的でないとして判定すると（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ファイルに含ま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ファイルに含ま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 Δt_1 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 Δt_2 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ファイルに含ま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 $M_{\min}$ 及び最大値 $M_{\max}$ を検索する（ステップS12）。最小値 $M_{\min}$ から最大値 $M_{\max}$ 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 $M_{\text{mode } 0}$ を検索し、最頻値 $M_{\text{mode } 0}$ 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S 1 5においてN O）、ステップS 1 6に進む。ステップS 1 5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1 0 m sの自然数倍又は1 0 m sの自然数倍の周辺となることが多い。ここで、最頻値M o d e 0が1 0 m sの自然数倍であれば、最頻値M o d e 0から1 0 m s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M o d e 0が1 0 m sの自然数倍の周辺であれば、最頻値M o d e 0から1 0 m s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M o d e 0の1の位を四捨五入し新たな最頻値M o d eとする。ただし、伝送遅延時間が1 0 m sの自然数倍又は1 0 m sの自然数倍の周辺となることが少ないU s e r A g e n tがある。そのU s e r A g e n tを会社Aとする。そこで、U s e r A g e n tが会社Aであるときには、例外として、最頻値M o d e 0を新たな最頻値M o d eとし、U s e r A g e n t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M o d e 0の1の位を四捨五入して新たな最頻値M o d eとする（ステップS 1 6）。

[0145] ここで、U s e r A g e n tは、通信端末2 0 0のI D、パスワード、携帯電話会社に固有なI D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I D及び電話番号が改竄されにくいことを考慮すれば、U s e r A g e n tは、携帯電話会社に固有なI D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I Dを付与しない会社が存在することを考慮すれば、U s e r A g e n t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M o d eから1 0 m s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M o d e 0での頻度C₀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 $T o t a l$ を 0 にリセットする（ステップ S 1 7）。自然数 n が 1、2、3 及び 4 である場合について、ステップ S 1 8 から S 2 5 までを繰り返す。

[0148] $T_{+n} = M o d e + 1 0 n$ に対して、 $[T_{+n} - 2, T_{+n} + 2]$ の範囲の最大頻度 C_{+n} を計算し、 $T_{-n} = M o d e - 1 0 n$ 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 S 1 8）。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 S 1 9 において Y E S）、最大頻度 C_n を最大頻度 C_{+n} にセットする（ステップ S 2 0）。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 S 1 9 において N O）、最大頻度 C_n を最大頻度 C_{-n} にセットする（ステップ S 2 1）。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もあり、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 $U s e r \ A g e n t$ 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 $U s e r \ A g e n t$ を会社 B とする。そこで、 $U s e r \ A g e n t$ 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 $T h r e s h o l d / 2$ より小さいときには（ステップ S 2 2 において N O）、原則どおり、最大頻度の合計 $T o t a l$ 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 S 2 5）。 F_n が所定の閾値の半分 $T h r e s h o l d / 2$ より大きいと

きには（ステップS 2 2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S 2 3）。条件Xが成立するときには（ステップS 2 3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S 2 5）。条件Xが成立しないときには（ステップS 2 3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S 2 4）、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S 2 5）。

[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S 1 8からS 2 5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S 2 6）。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S 2 6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S 2 8）。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S 2 6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S 3 0）。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もあり、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S 2 6においてN O）、パラメータ r が0でないときには（ステップS 2 9においてN O）、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S 3 0）。最大頻度の合計 $T o t a l$ が所定の閾値 $T h r e s h o l d$ より小さいところ（ステップS 2 6においてN O）、パラメータ r が0であるときには（ステップS 2 9においてY E S）、例外として、再識別を行うためにステップS 3 1及びS 3 2に進む。

[0158] ステップS 3 1では、通信端末2 0 0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 $M o d e 0$ での頻度 C_0 を0にセットする。ステップS 3 2では、最頻値 $M o d e 0$ 及び最頻値 $M o d e$ を0にリセットする。ステップS 3 1及びS 3 2を行ったうえで、ステップS 1 4及びS 1 5に進む。ステップS 1 5では、パラメータ r が1でありかつ最頻値 $M o d e 0$ が1 0 m s より小さくかつ最頻値 $M o d e 0$ 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S 1 5においてY E S）、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S 3 0）。条件Yが成立しないときには（ステップS 1 5においてN O）、ステップS 1 6に進む。このように、数m s 又は1 0 数m s 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 $T h r e s h o l d$ 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2 0 0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2 0 0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 $T h r e s h o l d$ が大きいほど、最大頻度の合計 $T o t a l$ は所定の閾値 $T h r e s h o l d$ を越えにくい（ステップS 2 6においてN

0)。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場合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S 1 0 3)、その電話番号を利用した電話通信を実行する(ステップS 1 0 4)。

[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5 6は、電話通信部5 4が電話通信を実行しているときに、電話通信部5 4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5 5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S 1 0 5)。伝送遅延時間変化判断ステップについては、図1 8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5 7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ときに(ステップS 1 0 5においてYES)、その通信端末2が正規の携帯電話3 Aであると判断し(ステップS 1 0 6)、コンテンツの閲覧を承認する(ステップS 1 0 7)。そして、データ通信部5 2は、コンテンツの閲覧の承認を正規の携帯電話3 Aに通知するとともに、コンテンツ格納部5 1の格納するコンテンツを正規の携帯電話3 Aに提供する。ただし、データ通信部5 2は、コンテンツの閲覧の承認に代えて、コンテンツ格納部5 1の格納するコンテンツのみを正規の携帯電話3 Aに提供してもよい。

[0187] コンテンツ閲覧認証部5 7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ないと判断したときに(ステップS 1 0 5においてNO)、その通信端末2が携帯電話3 Cになりすました非正規の携帯電話3 Bであると判断し(ステップS 1 0 8)、コンテンツの閲覧を拒否する(ステップS 1 0 9)。そして、データ通信部5 2は、コンテンツの閲覧の拒否を非正規の携帯電話3 B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 GET 1 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 RES 1 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 ファイルに含ま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 GET 2 を認証サーバ 1 に送信し、画像ファイル e 1 を要求する。データ通信部 52 は、レスポンス RES 2 を通信端末 2 に送信し、画像ファイル e 1 を提供する。通信端末 2 は、リクエスト GET 3 を認証サーバ 1 に送信し、画像ファイル e 2 を要求する。データ通信部 52 は、レスポンス RES 3 を通信端末 2 に送信し、画像ファイル e 2 を提供する。通信端末 2 は、リクエスト GET 4 を認証サーバ 1 に送信し、画像ファイル e 3 を要求する。データ通信部 52 は、レスポンス RES 4 を通信端末 2 に送信し、画像ファイル e 3 を提供する。通信端末 2 が HTML ファイルに含ま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 GET 2 を通信端末 2 から受信してから次にリクエスト GET 3 を通信端末 2 から受信するまでの時間 Δt_1 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 GET 3 を通信端末 2 から受信してから次にリクエスト GET 4 を通信端末 2 から受信するまでの時間 Δt_2 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 ファイルに含ま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 GET 1 を通信端末 2 から受信してから次にリクエスト GET 2 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 5 2 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 3 A 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 3 A 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 e 1 の要求信号であるリクエスト GET 2 と、画像ファイル e 2 の要求信号であるリクエスト GET 3 と、画像ファイル e 3 の要求信号であるリクエスト GET 4 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 3 A の場合、携帯電話 2 A がリクエスト GET 2 及びリクエスト GET 3 をほぼ同時に送信するため、リクエスト GET 2 からリクエスト GET 3 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 5 2 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 5 3 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 5 2 は、リクエスト GET 2、リクエスト GET 3 及びリクエスト GET 4 をまとめて受信すると、リクエスト GET 2 に対するレスポンス RES 2 を通信端末 2 に送信し、その後にレスポンス RES 2 の送信後にデータ通信部 5 2 が TCP のコネクションを close する。このように、リクエスト GET 3 及びリクエスト GET 4 に対してはレスポンス RES 3 及びレスポンス RES 4 を送信しない。これにより、通信端末 2 は、レスポンス RES 2 の受信後に、改めてリクエスト GET 3 を送信する。

[0196] 伝送遅延時間測定部 5 3 は、まとめて受信したリクエスト GET 2、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 Δt_1 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 Δt_1 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 3 A 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 1 8 に示し、非正規の携帯電話 3 B 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 1 9 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 5 6 は、図 1 8 及び図 1 9 に示したように、電話通信部 5 4 が電話通信を実行しているときに、電話通信部 5 4 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 5 5 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 5 7 は、図 1 8 に示したように、伝送遅延時間変化判断部 5 6 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 3 A 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 5 7 は、図 1 9 に示したように、伝送遅延時間変化判断部 5 6 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 3 B 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 5 6 は、電話通信部 5 4 が電話通信を実行しているときに、電話通信部 5 4 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 5 2 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 1 7 に示したリクエスト GET 2、GET 3、GET 4、・・・である。

[0205] コンテンツ閲覧認証部 5 7 は、伝送遅延時間変化判断部 5 6 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 3 A 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 5 7 は、伝送遅延時間変化判断部 5 6 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 3 B 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 5 6 は、電話通信部 5 4 が電話通信を実行しているときに、電話通信部 5 4 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 5 5 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 3 A 又は非正規の携帯電話 3 B 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 5 7 は、伝送遅延時間変化判断部 5 6 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 3 A 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 5 7 は、伝送遅延時間変化判断部 5 6 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 3 B 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 3 A 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 3 A 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 3 A 毎に設定されないときには、伝送遅延時間変化判断部 5 6 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 5 7 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 5 7 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 5 7 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 3 A 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 5 7 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 3 C になりすました非正規の携帯電話 3 B 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 5 1 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 5 2 は、コンテンツの閲覧の承認を正規の携帯電話 3 A 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 3 A に提供すればよい。

[0214] 本実施形態では、正規の携帯電話 3 A 又は非正規の携帯電話 3 B 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 3 A 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 3 A 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 3 A に認証要求を発行し、正規の携帯電話 3 A 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 3 A 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
2 A : 携帯電話
2 B : コンピュータ
1 1 : コンテンツ格納部
1 2 : データ通信部
1 3 : 伝送遅延時間測定部
1 4 : 伝送遅延時間分布特性判断部
1 5 : コンテンツ閲覧認証部
3 1 : コンテンツ格納部
3 2 : データ通信部
3 3 : 伝送遅延時間測定部
3 4 : 分布特性算出部
3 5 : 抽出部
3 6 : 分布特性判定部
3 7、4 2 : コンテンツ閲覧認証部
3 8 : 通話判定部
4 1 : 通話変化判定部
1 0 3、1 0 4 : 認証サーバ
2 0 0 : 通信端末
1 : 認証サーバ

- 2 : 通信端末
- 3 A、3 B、3 C : 携帯電話
- 5 1 : コンテンツ格納部
- 5 2 : データ通信部
- 5 3 : I D / 電話番号対応テーブル
- 5 4 : 電話通信部
- 5 5 : 伝送遅延時間測定部
- 5 6 : 伝送遅延時間変化判断部
- 5 7 : コンテンツ閲覧認証部

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は判断されたときに、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

ース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接続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接続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は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接続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は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。

[請求項25]

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

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26] 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25に記載の認証サーバ。

[請求項27] 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26に記載の認証サーバ。

[請求項28] 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接続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25に記載の認証サーバ。

[請求項29] 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、請求項 25 から 28 のいずれかに記載の認証サーバ。

[請求項30] 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、請求項 25 から 29 のいずれかに記載の認証サーバ。

[請求項31] 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、請求項 25 から 30 のいずれかに記載の認証サーバ。

[請求項32] 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。

[請求項33] 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、請求項32に記載の認証サーバによる認証方法。

[請求項34] 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することを特徴とする、請求項33に記載の認証サーバによる認証方法。

[請求項35] 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接続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ことを特徴とする、請求項32に記載の認証サーバによる認証方法。

[請求項36] 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、請求項 3 2 から 3 5 のいずれかに記載の認証サーバによる認証方法。

[請求項37]

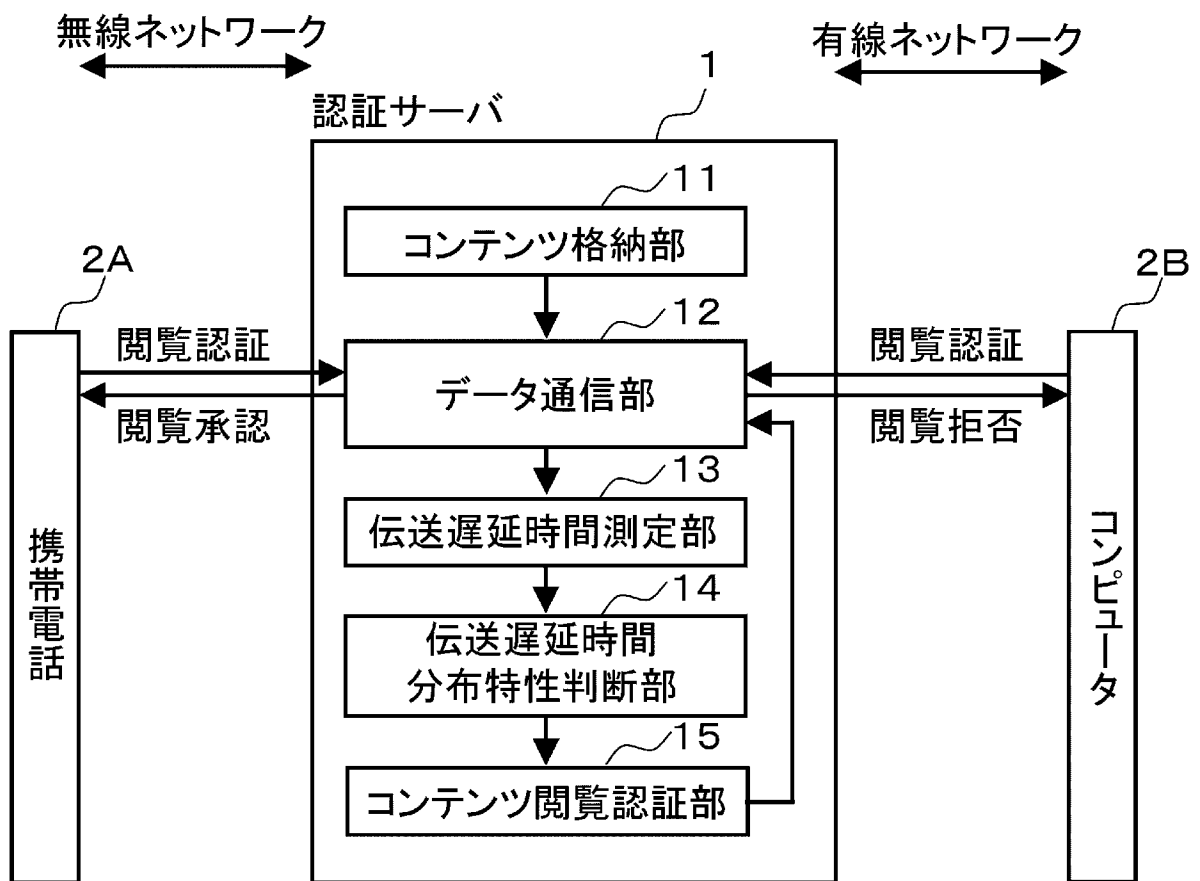
前記伝送遅延時間変化判断ステップは、電話通信を実行しているときに、電話通信を実行していないときと比べて、前記通信端末から前記伝送遅延時間の測定用のパケットを受信していないかどうかを判断し、

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、請求項 3 2 から 3 6 のいずれかに記載の認証サーバによる認証方法。

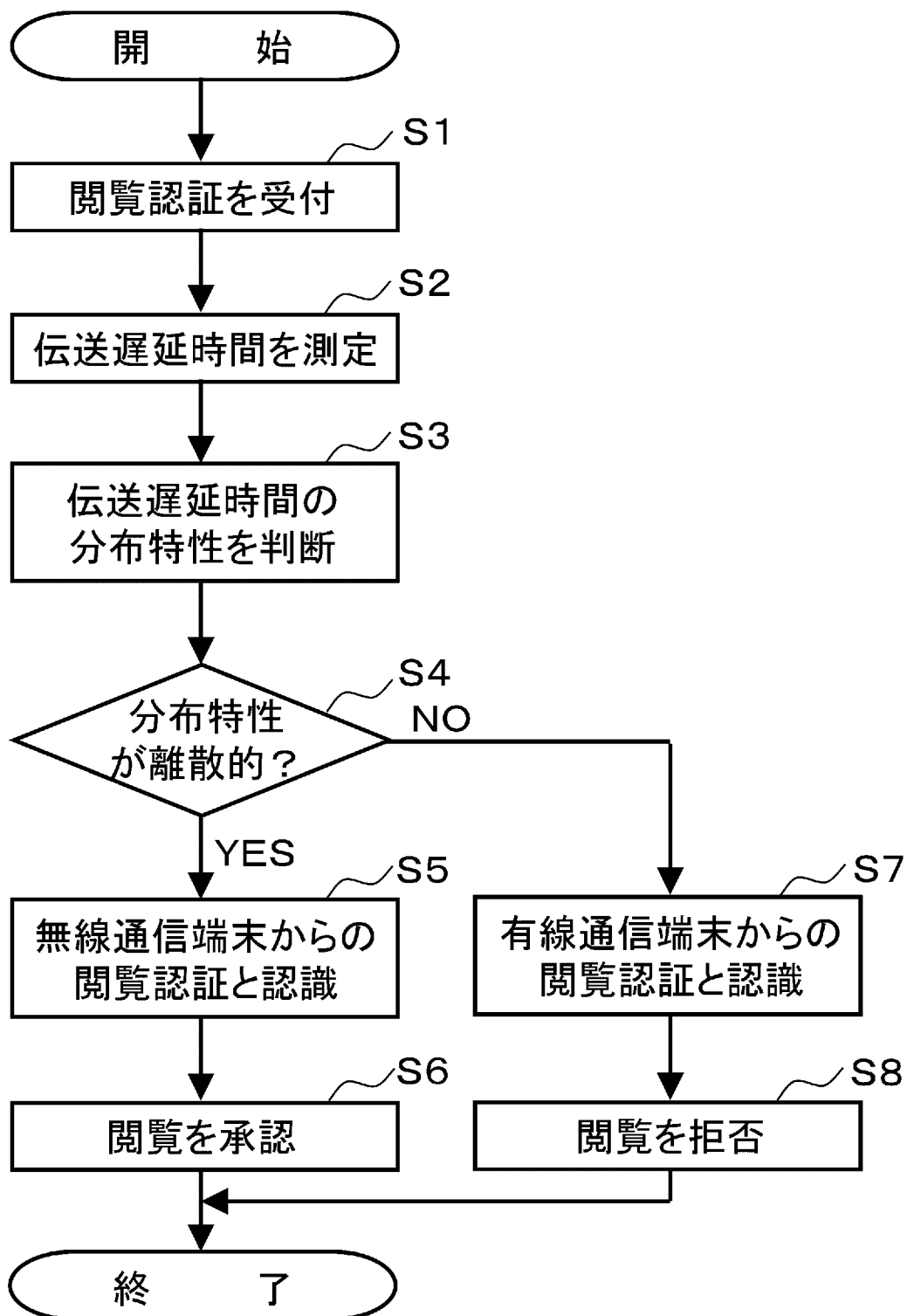
[請求項38]

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、請求項 3 2 から 3 7 のいずれかに記載の認証サーバによる認証方法。

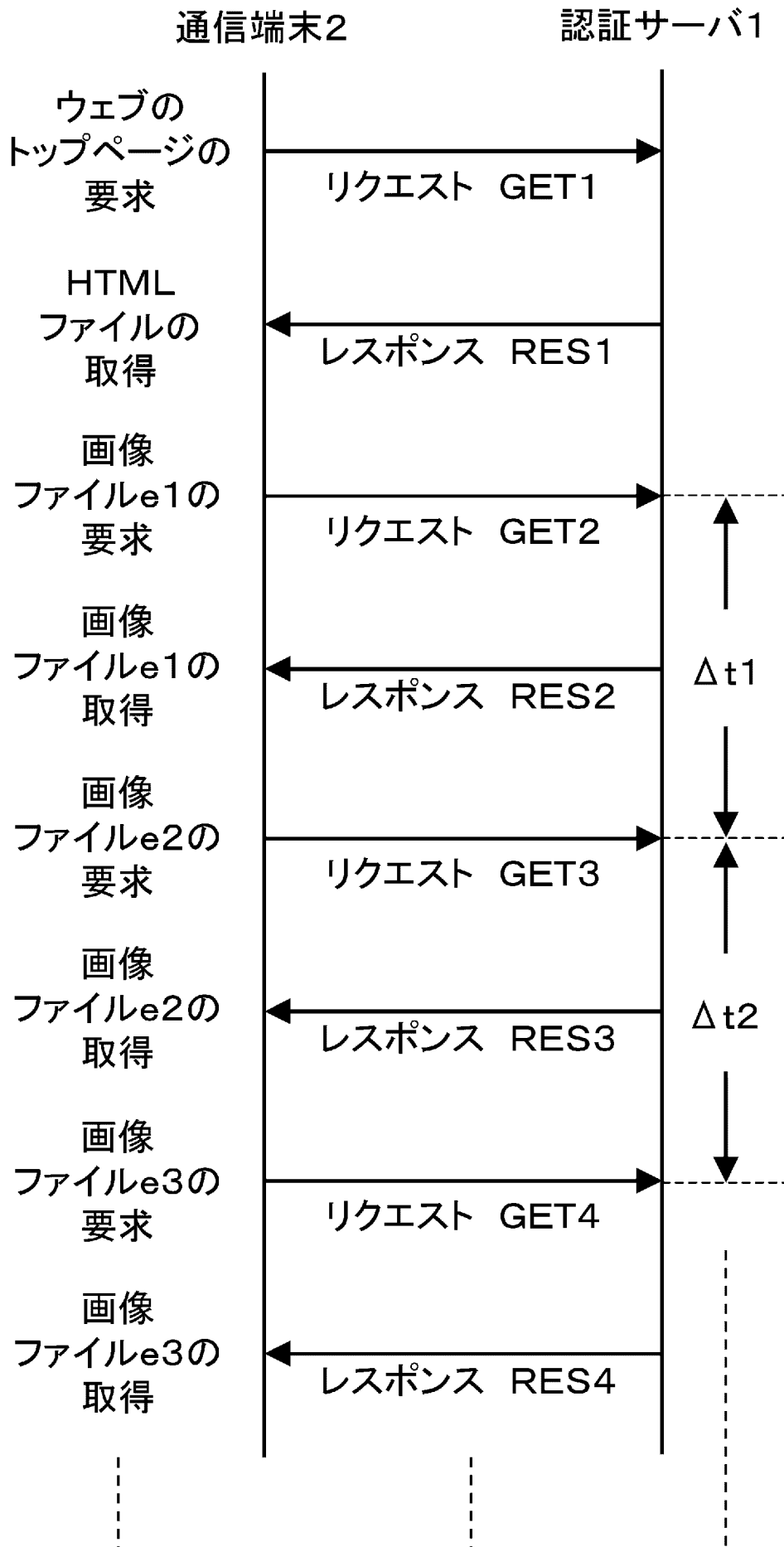
[図1]



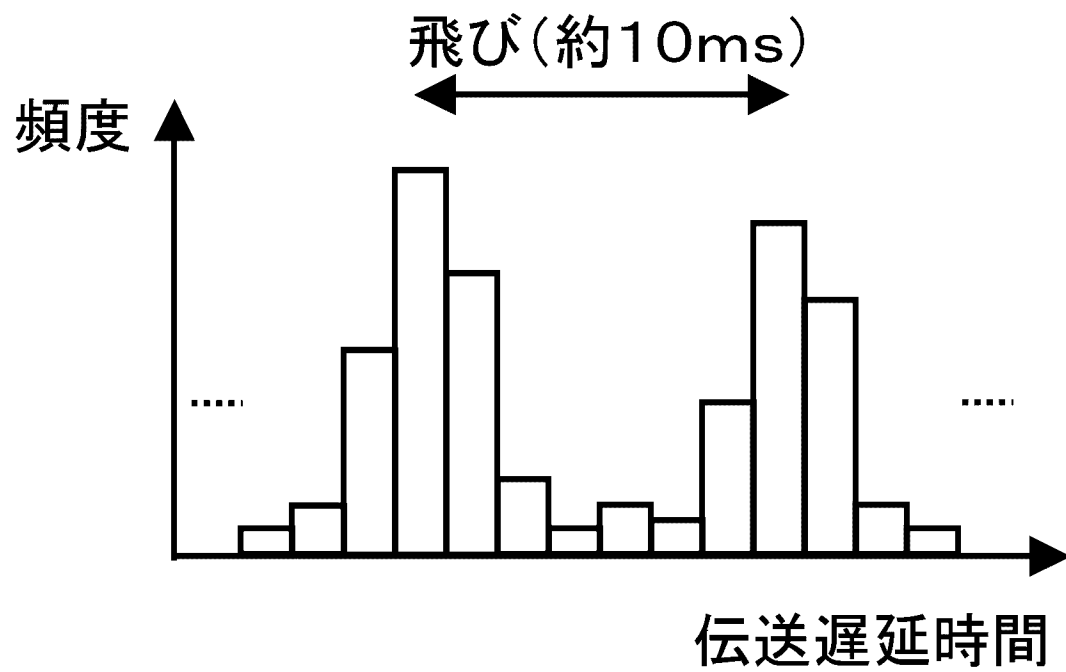
[図2]



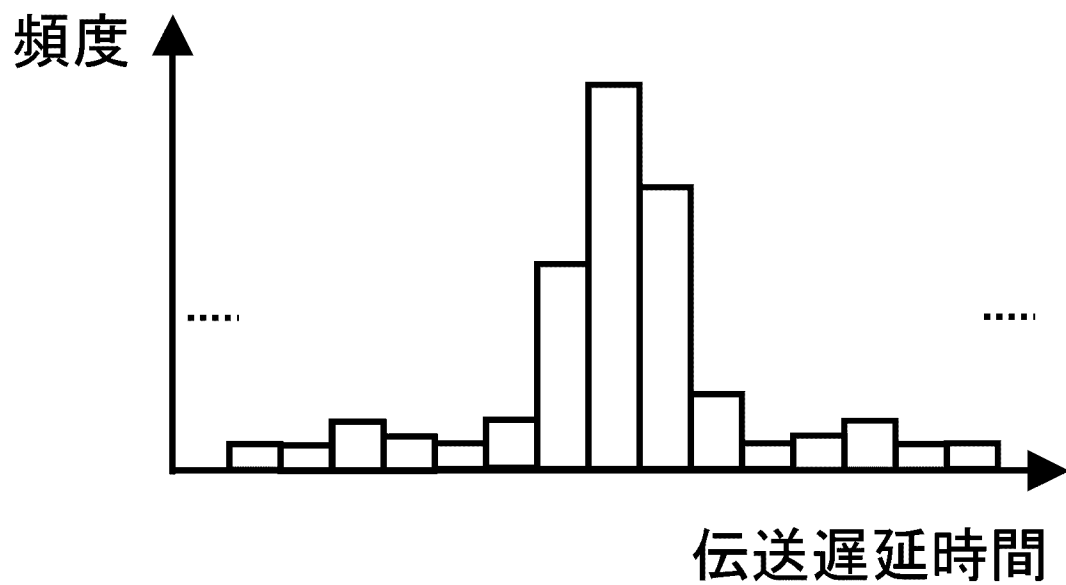
[図3]



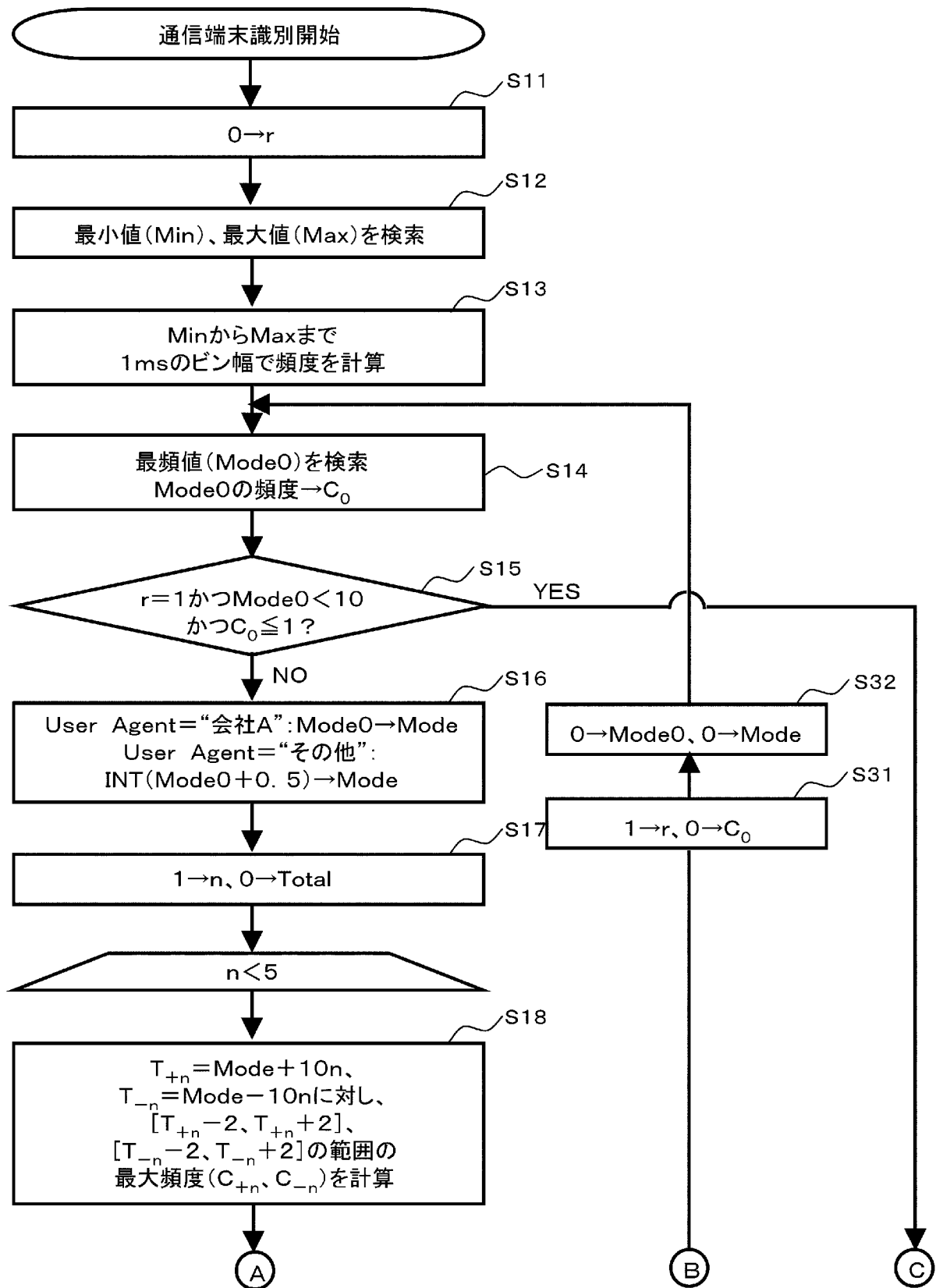
[図4]



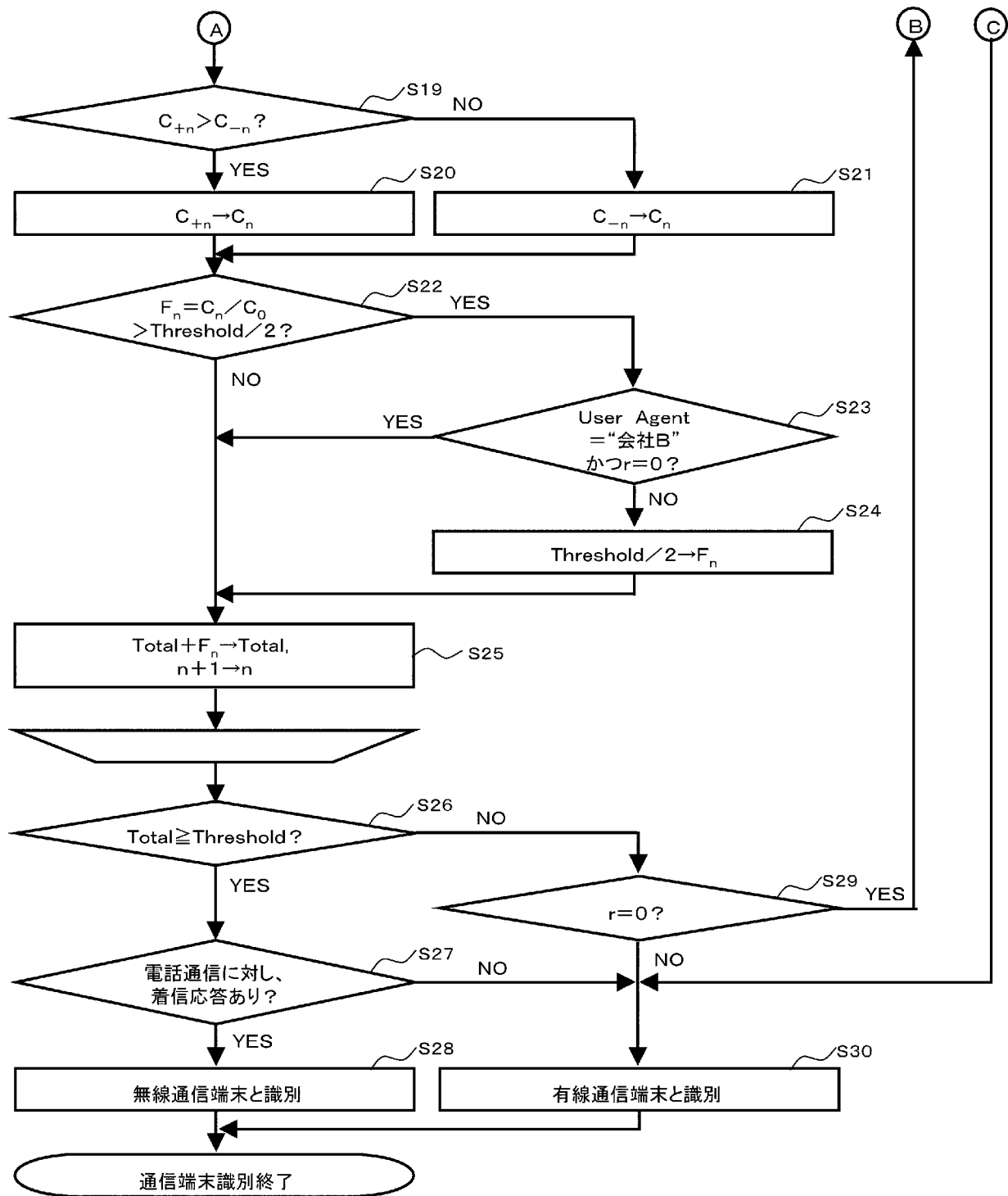
[図5]



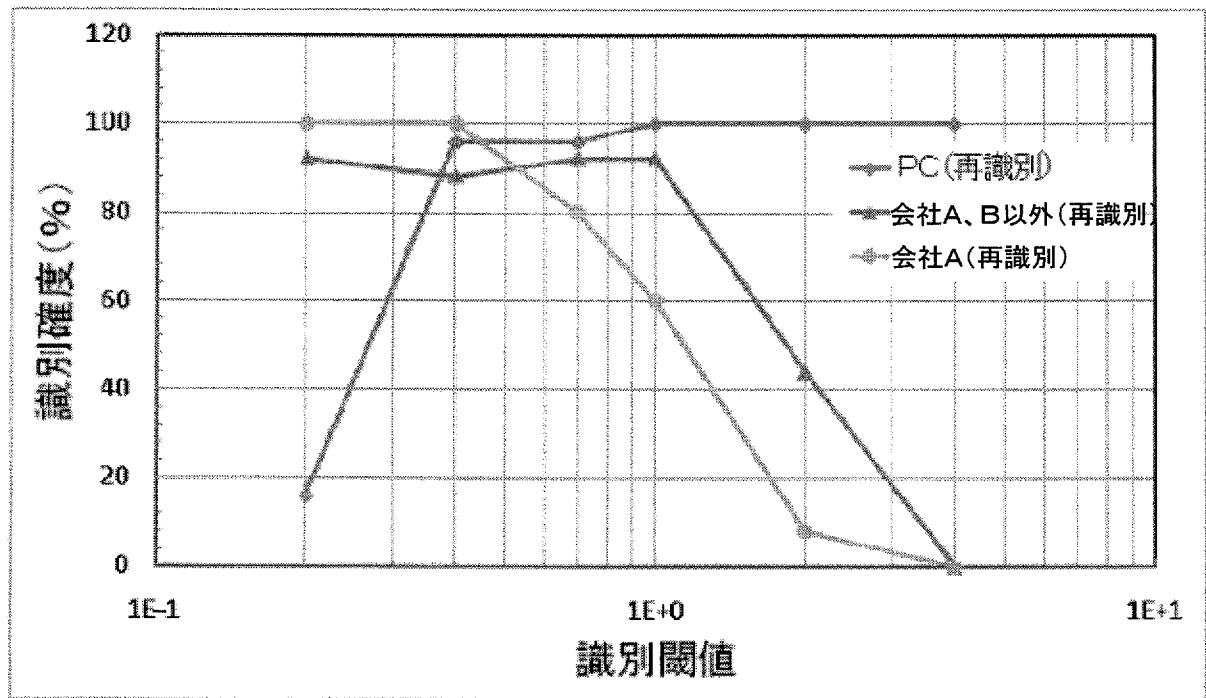
[図6]



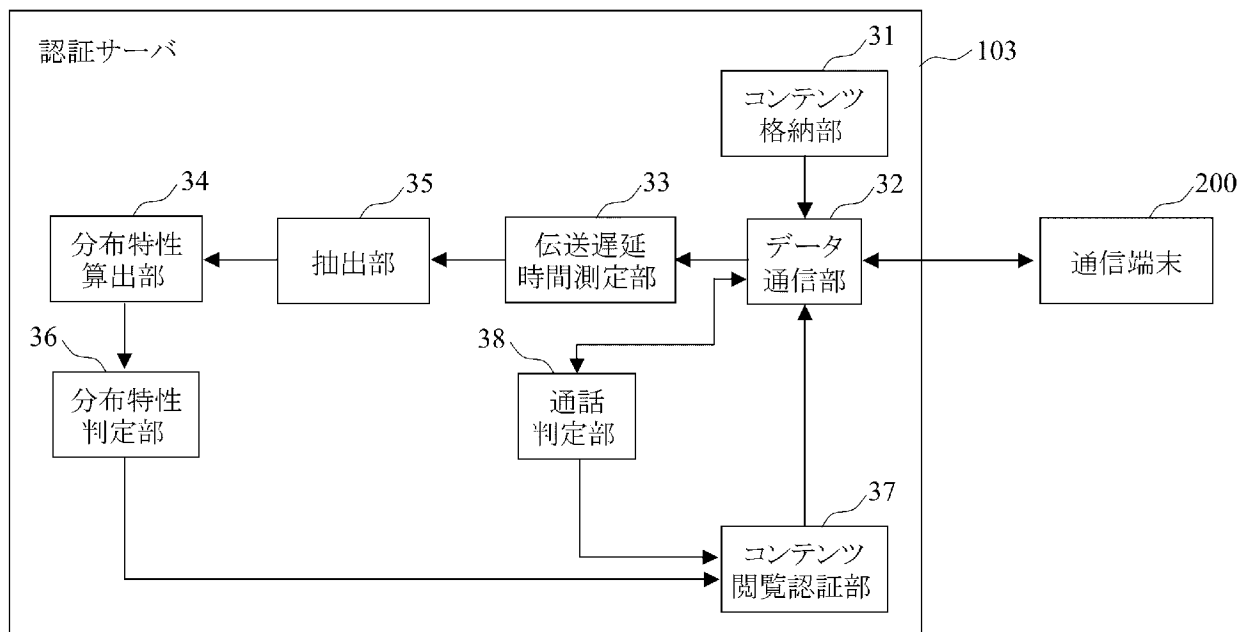
[図7]



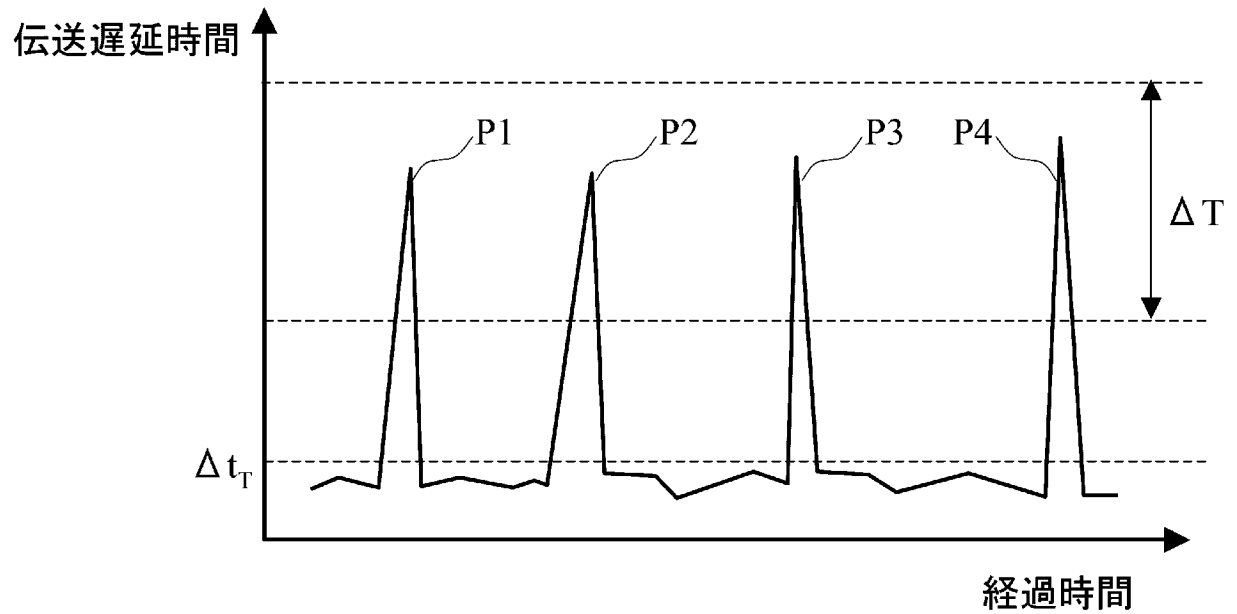
[図8]



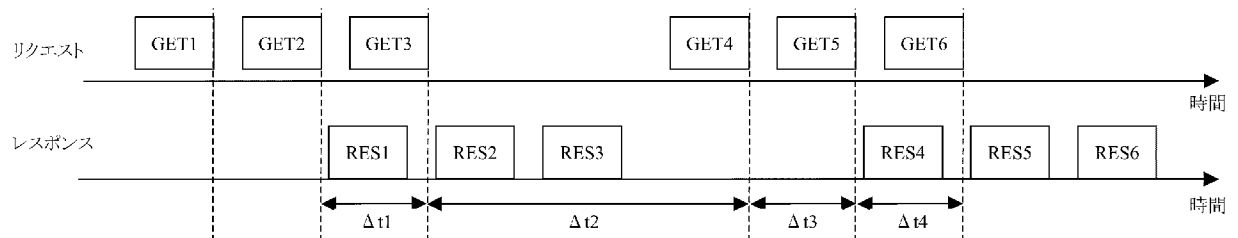
[図9]



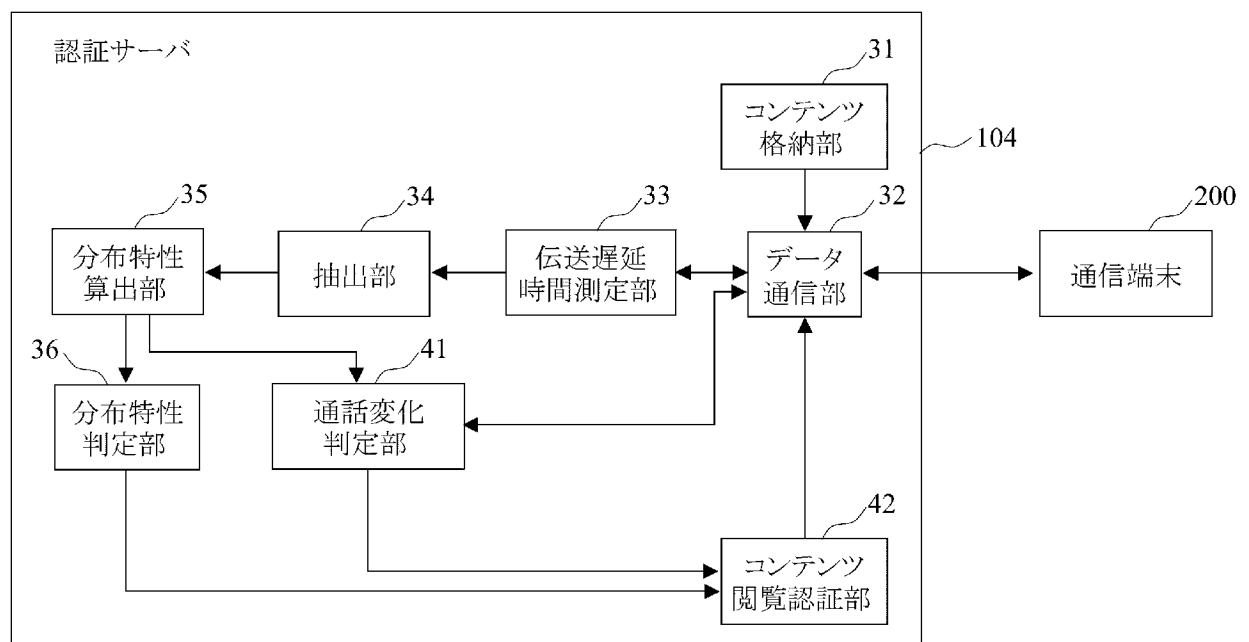
[図10]



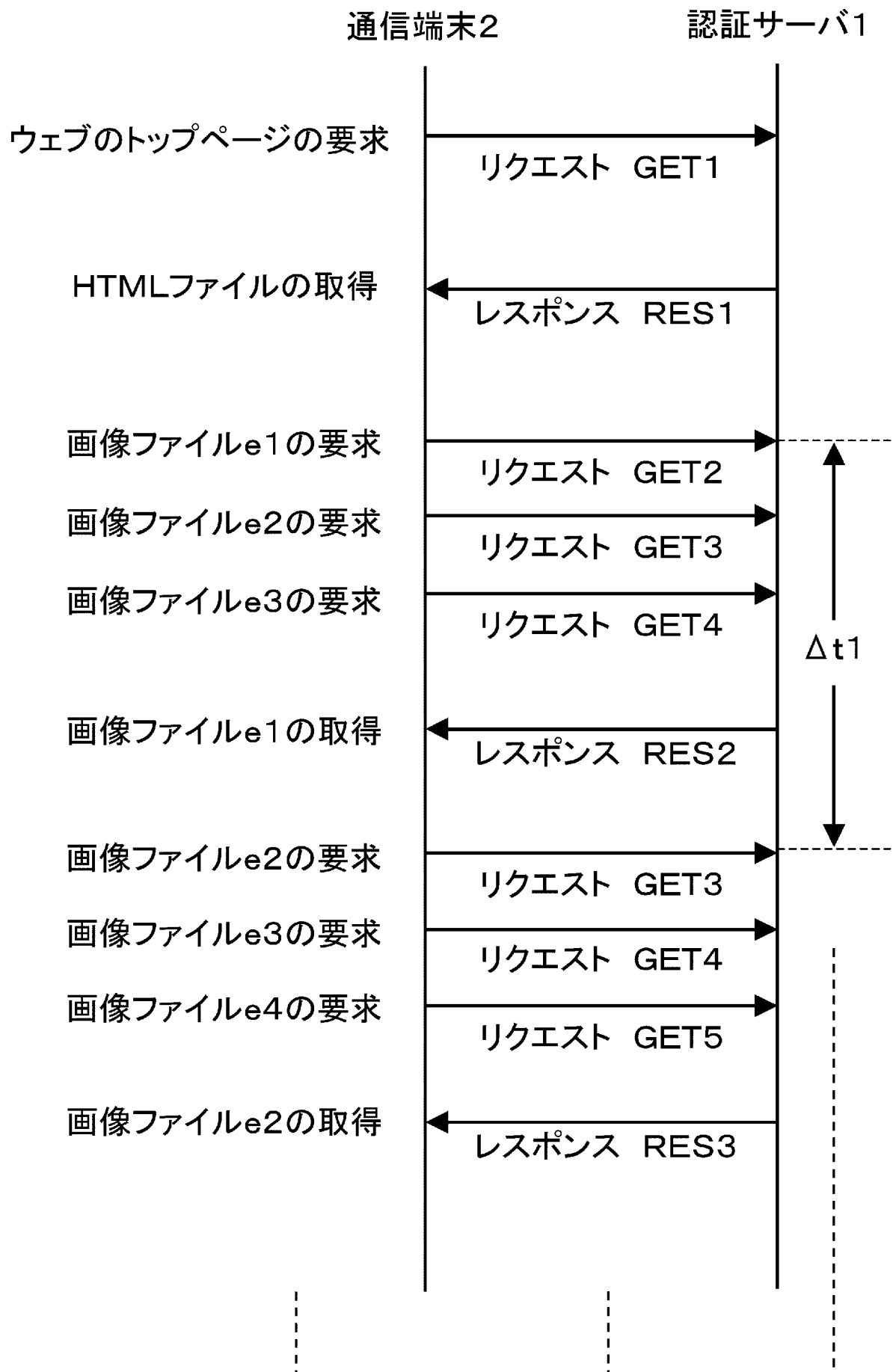
[図11]



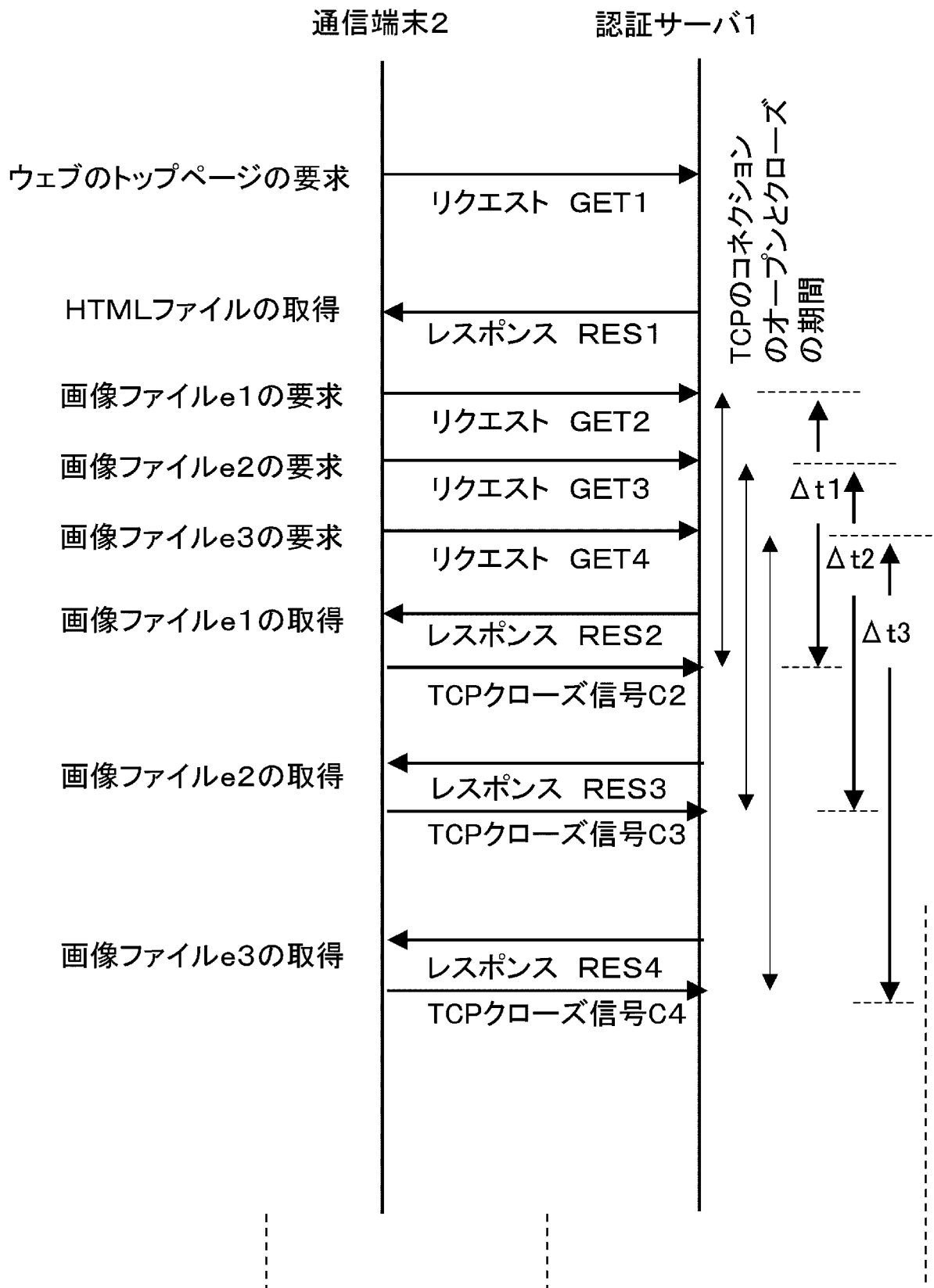
[図12]



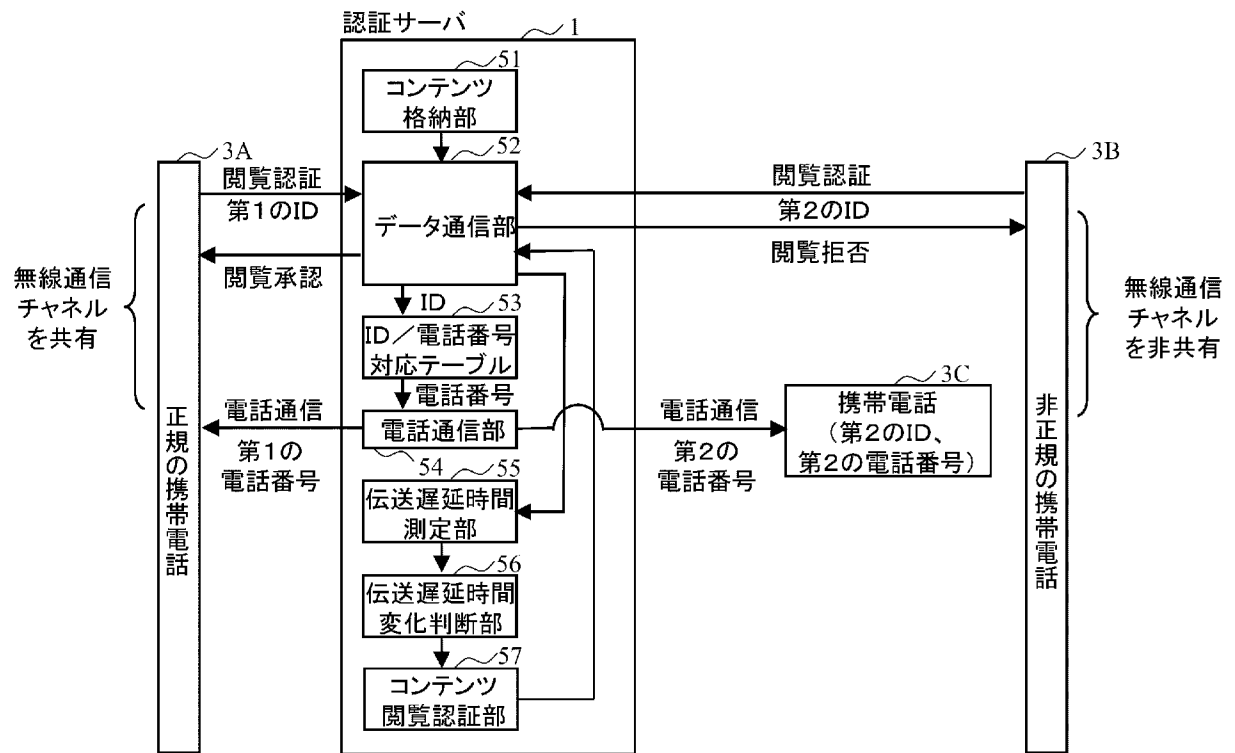
[図13]



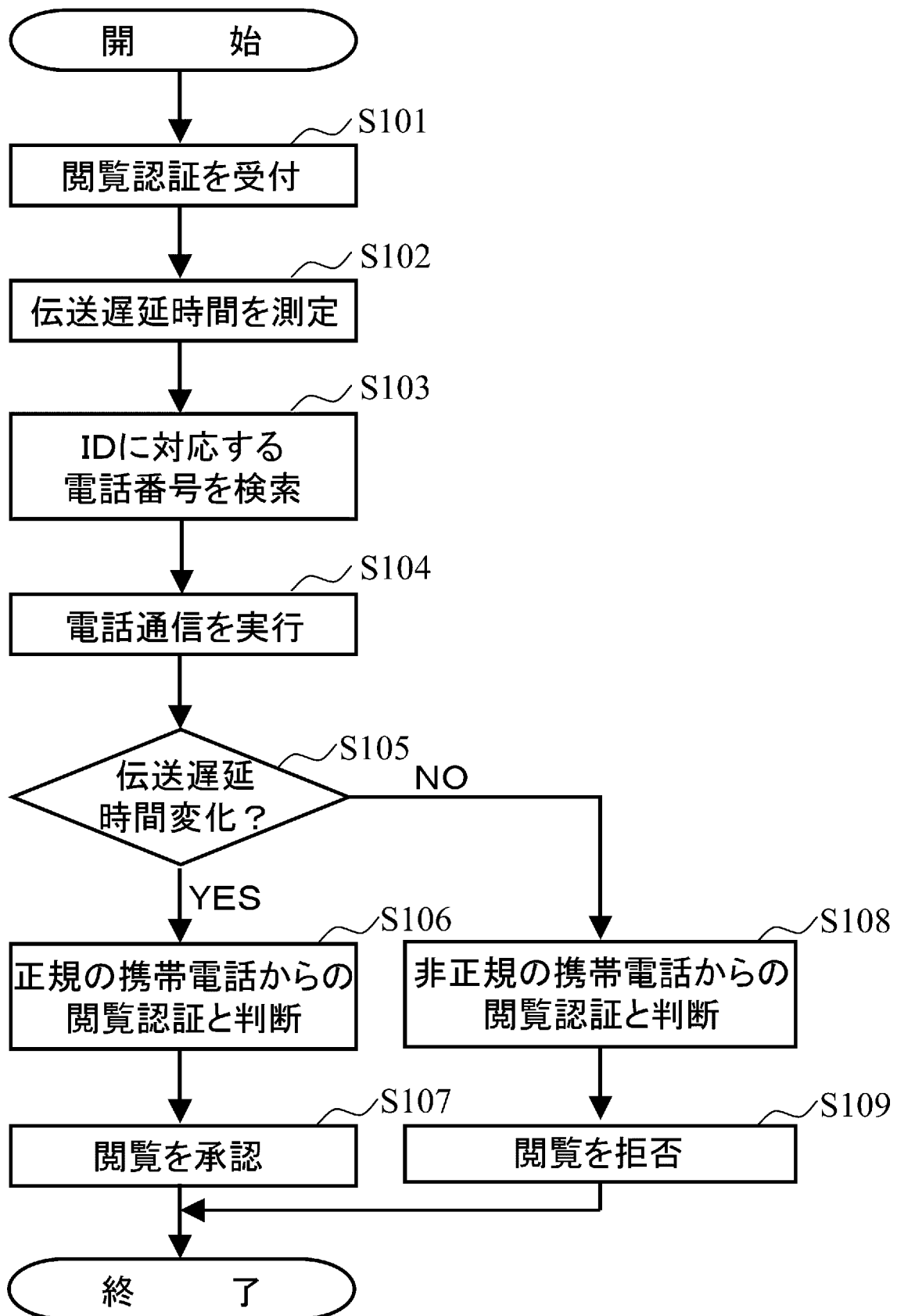
[図14]



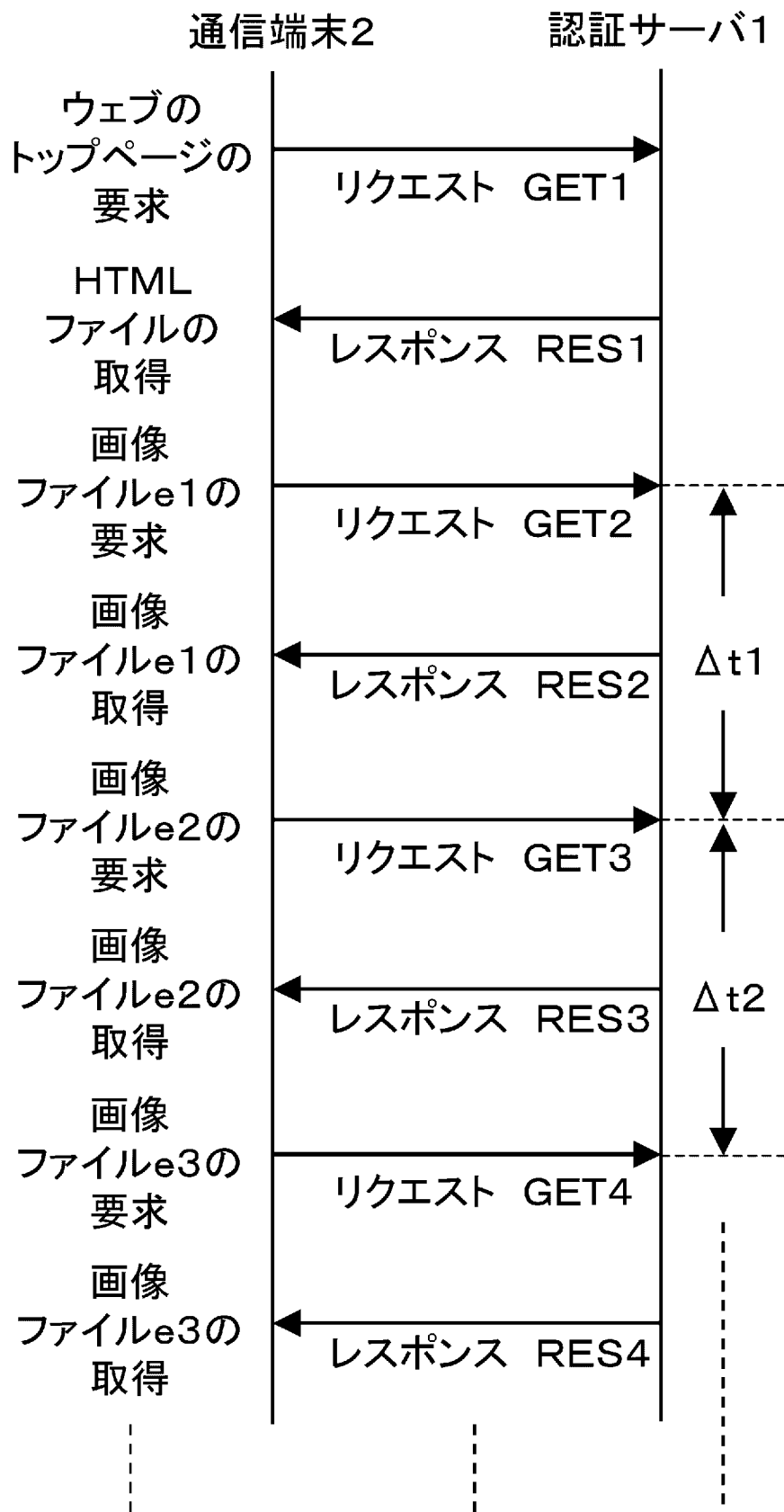
[図15]



[図16]



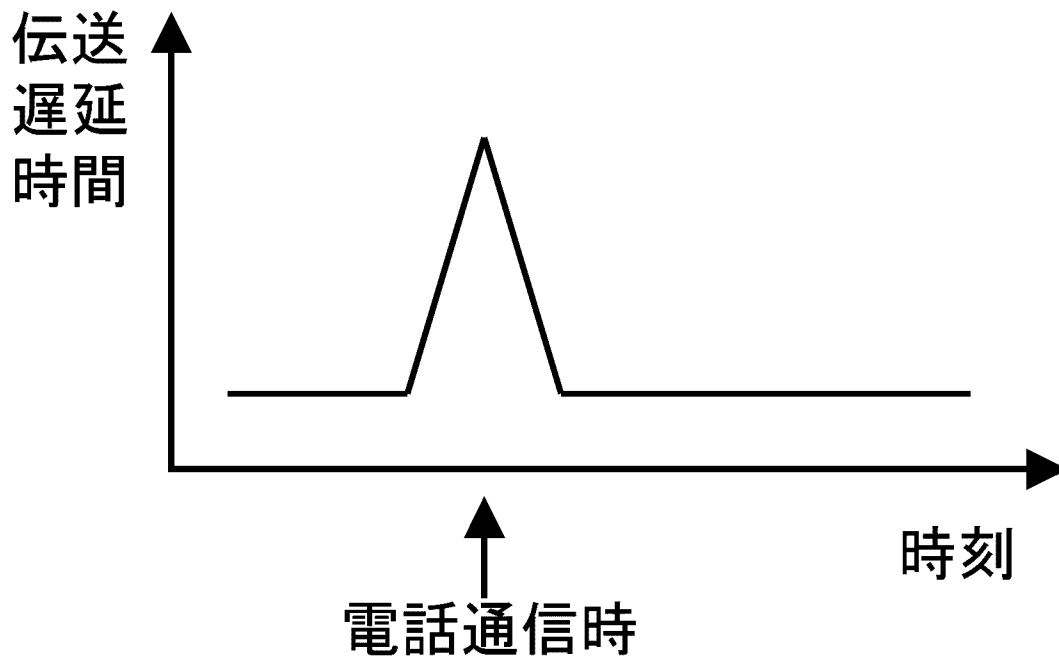
[図17]



[図18]

正規の携帯電話からの閲覧認証

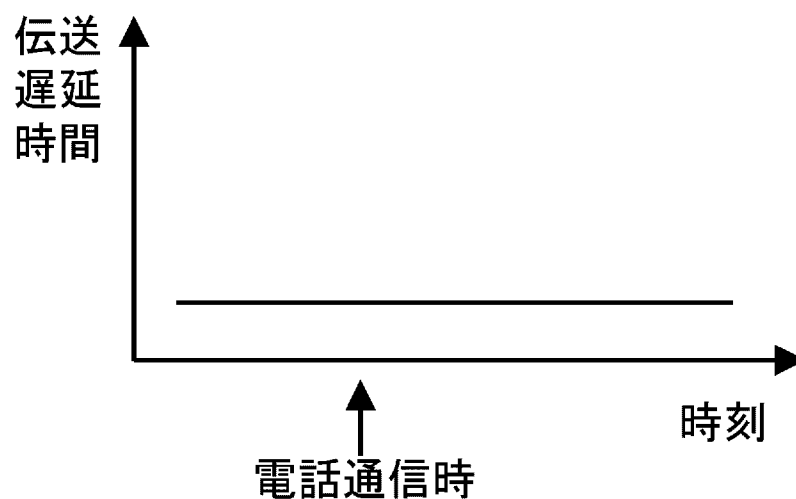
→伝送遅延時間が電話通信時に増加する



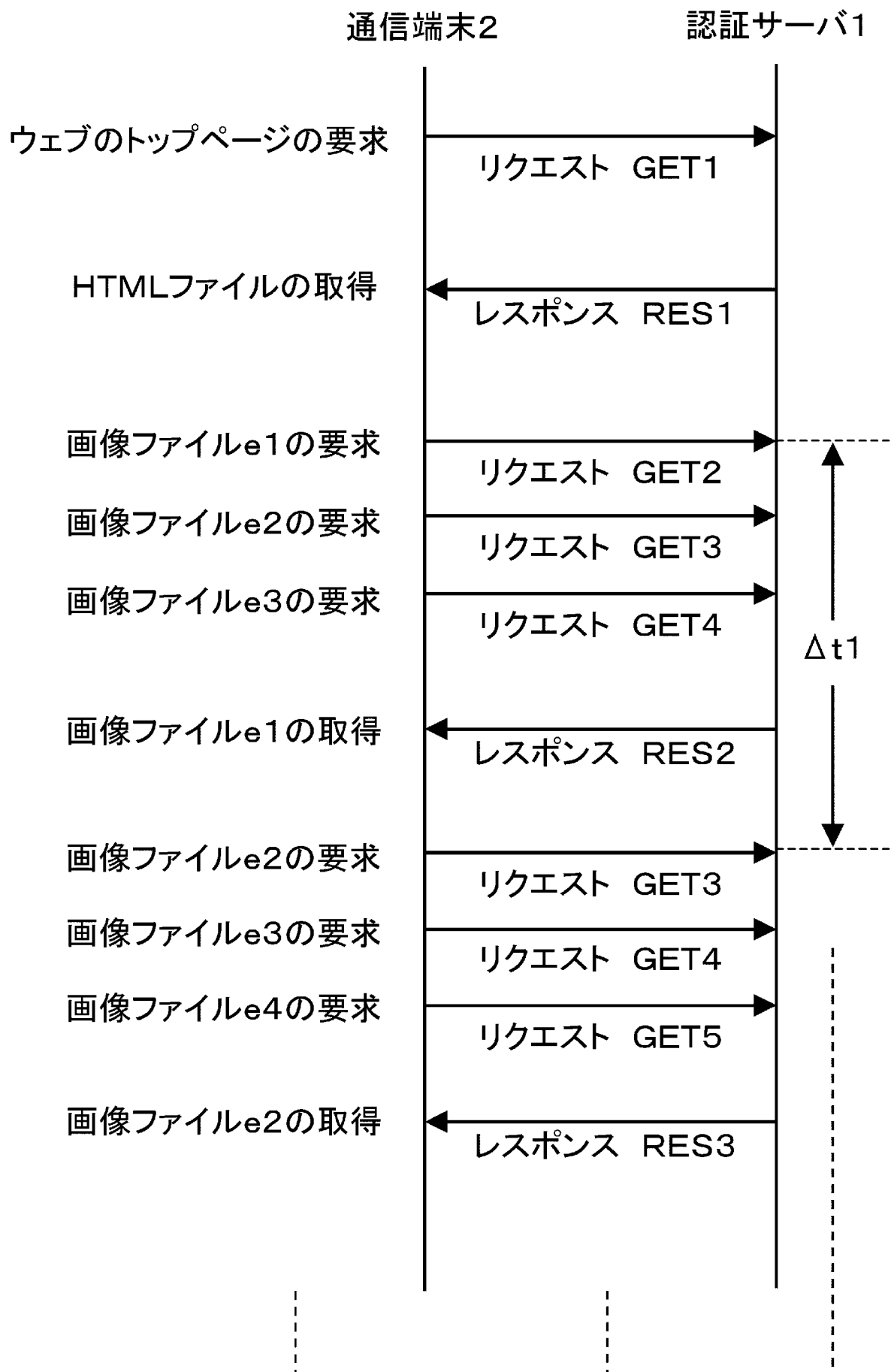
[図19]

非正規の携帯電話からの閲覧認証

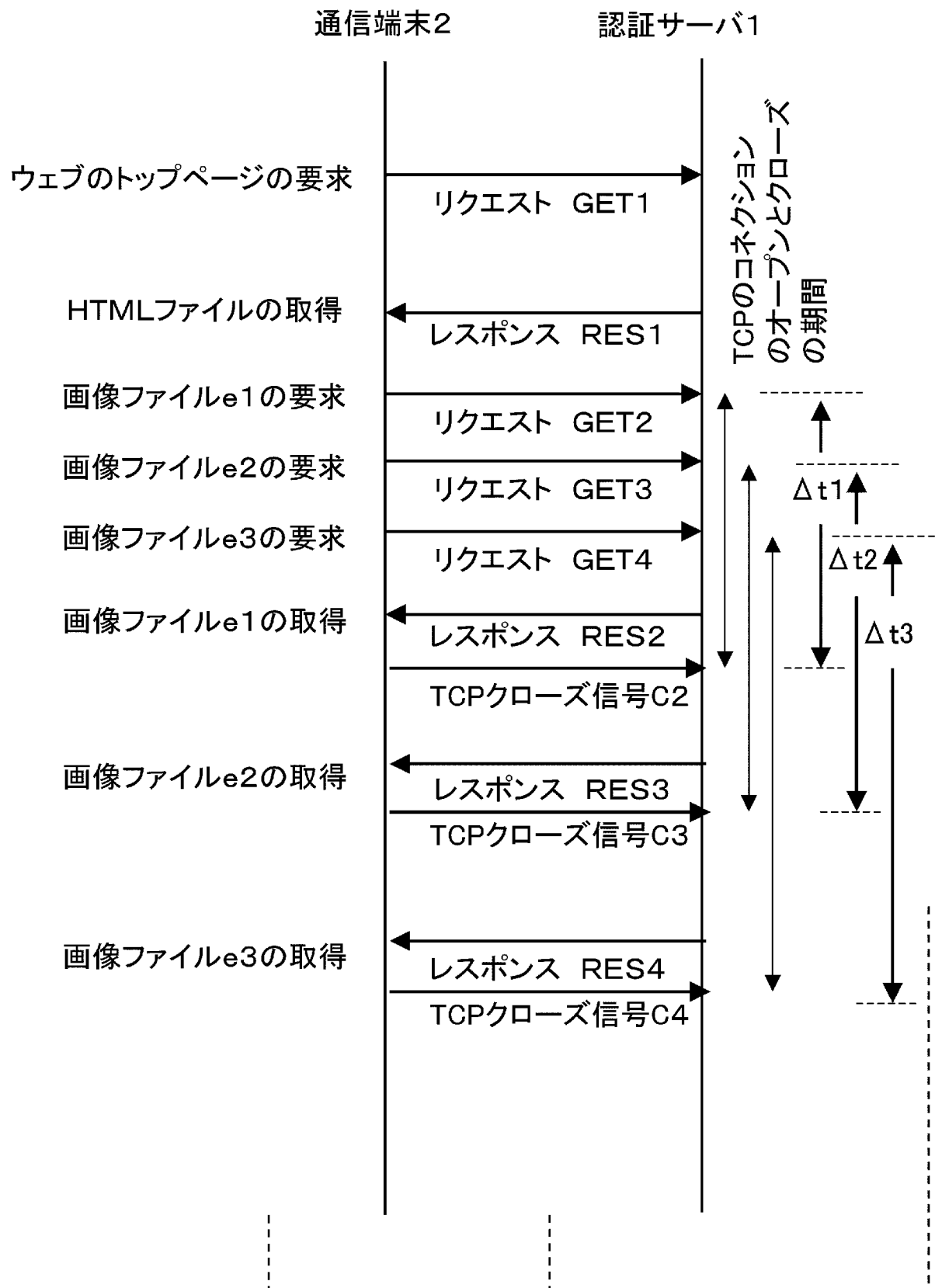
→伝送遅延時間が電話通信時に増加しない



[図20]



[図21]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2011/075277

A. CLASSIFICATION OF SUBJECT MATTER

H04L9/32(2006.01)i, G06F21/20(2006.01)i, H04W12/06(2009.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L9/32, G06F21/20, H04W12/06

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2012

Kokai Jitsuyo Shinan Koho 1971-2012 Toroku Jitsuyo Shinan Koho 1994-2012

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2008-287542 A (Nihon University, Keio University), 27 November 2008 (27.11.2008), paragraphs [0026] to [0047] (Family: none)	1-24
A	JP 2008-524681 A (International Business Machines Corp.), 10 July 2008 (10.07.2008), paragraphs [0015], [0016] & US 2006/0233372 A1 & EP 1832082 B1 & WO 2006/063972 A1 & CN 101069406 A & AT 488943 T	1-24



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T"

later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X"

document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y"

document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&"

document member of the same patent family

Date of the actual completion of the international search

13 January, 2012 (13.01.12)

Date of mailing of the international search report

24 January, 2012 (24.01.12)

Name and mailing address of the ISA/

Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2011/075277

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2004-222270 A (NTT Docomo Inc.), 05 August 2004 (05.08.2004), paragraph [0046] & US 2004/0176947 A1 & EP 1435704 A2 & CN 1512709 A	1-24
A	T. Tsuchiya, M. Kihara and A. J. P. Berena, "Transmission Time-based Authentication Scheme Using 3G Mobile Device for DRM System", [online], Proceedings of the 2009 IEEE European Frequency and Time Forum & International Frequency Control Symposium, 2009.04, pp. 706- 710. [retrieved on 2011.11.24]. Retrieved from the Internet: <URL: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5168275 >	1-24
P,X	Takahiro TSUCHIYA, Suguru HOSHINO, Masami KIHARA, "A Method for Distinguishing Between Cellular Phone and PC Using Transmission Delay in Internet Access", 2011 Nen The Institute of Electronics, Information and Communication Engineers Sogo Taikai Koen Ronbunshu, Tsushin 2, 28 February 2011 (28.02.2011), page 231	1-4,7-10, 13-16,19-22
P,A		5,6,11,12, 17,18,23,24

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2011/075277

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:
See extra sheet.

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:
1-24

Remark on Protest

- ☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.
- ☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.
- ☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2011/075277

Continuation of Box No.III of continuation of first sheet (2)

The technical feature common to the invention in claim 1 and the invention in claim 25 is

an authentication server characterized by being provided with a data communication unit which performs data communication with a communication terminal that performs authentication for browsing contents, a transmission delay time measurement unit which measures the transmission delay time between the data communication unit and the communication terminal multiple times, and a contents browsing authentication unit which approves the browsing of the contents or denies the browsing of the contents.

However, since this technical feature makes no contribution over the prior art in the light of the disclosure of document 1 (JP 2008-287542 A (Nihon University, Keio University), 27 November 2008 (27.11.2008), paragraphs [0026] to [0047]), this technical feature cannot be a special technical feature.

Further, these inventions have no other same or corresponding special technical feature.

The following two inventions (groups) are contained in the claims.

(Invention 1) The inventions in claims 1-24

An authentication server, wherein it is determined whether the distribution characteristic of the transmission delay time is discrete or not, the browsing of the contents is approved when it is determined that the distribution characteristic is discrete, and the browsing of the contents is denied when it is determined that the distribution characteristic is not discrete.

(Invention 2) The inventions in claims 25-38

An authentication server, wherein when telephone communication using a telephone number associated with the identifier or password of a communication terminal is being executed, it is determined whether there is a change in transmission delay time compared to when the telephone communication is not executed, the browsing of the contents is approved when it is determined that there is a change, and the browsing of the contents is denied when it is determined that there is no change.

A. 発明の属する分野の分類 (国際特許分類 (I P C))

Int.Cl. H04L9/32(2006.01)i, G06F21/20(2006.01)i, H04W12/06(2009.01)i

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (I P C))

Int.Cl. H04L9/32, G06F21/20, H04W12/06

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1 9 2 2 - 1 9 9 6 年
日本国公開実用新案公報	1 9 7 1 - 2 0 1 2 年
日本国実用新案登録公報	1 9 9 6 - 2 0 1 2 年
日本国登録実用新案公報	1 9 9 4 - 2 0 1 2 年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
A	JP 2008-287542 A (学校法人日本大学、学校法人慶應義塾) 2008.11.27, 段落【0026】 - 【0047】 (ファミリーなし)	1-24
A	JP 2008-524681 A (インターナショナル・ビジネス・マシーンズ・ コーポレーション) 2008.07.10, 段落【0015】, 【0016】 & US 2006/0233372 A1 & EP 1832082 B1 & WO 2006/063972 A1 & CN 101069406 A & AT 488943 T	1-24

☒ C 欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日

1 3 . 0 1 . 2 0 1 2

国際調査報告の発送日

2 4 . 0 1 . 2 0 1 2

国際調査機関の名称及びあて先

日本国特許庁 (I S A / J P)

郵便番号 1 0 0 - 8 9 1 5

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

金沢 史明

5 S

4 5 3 8

電話番号 0 3 - 3 5 8 1 - 1 1 0 1 内線 3 5 4 6

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
A	JP 2004-222270 A (株式会社エヌ・ティ・ティ・ドコモ) 2004.08.05, 段落【0046】 & US 2004/0176947 A1 & EP 1435704 A2 & CN 1512709 A	1-24
A	T. Tsuchiya, M. Kihara and A. J. P. Berena, "Transmission Time-based Authentication Scheme Using 3G Mobile Device for DRM System", [online], Proceedings of the 2009 IEEE European Frequency and Time Forum & International Frequency Control Symposium, 2009.04, pp. 706-710. [retrieved on 2011.11.24]. Retrieved from the Internet: <URL: http://ieeexplore.ieee.org/xpls/abs_all.jsp? arnumber=5168275 >	1-24
P, X	土屋貴寛, 星野卓, 木原雅巳, "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,	1-4, 7-10, 13-16, 19-22
P, A	2011.02.28, p. 231	5, 6, 11, 12, 17, 18, 23, 24

第Ⅱ欄 請求の範囲の一部の調査ができないときの意見（第1ページの2の続き）

法第8条第3項（P C T 17条(2)(a)）の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1. ☐ 請求項 _____ は、この国際調査機関が調査をすることを要しない対象に係るものである。
つまり、
2. ☐ 請求項 _____ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、
3. ☐ 請求項 _____ は、従属請求の範囲であってP C T規則6.4(a)の第2文及び第3文の規定に従って記載されていない。

第Ⅲ欄 発明の単一性が欠如しているときの意見（第1ページの3の続き）

次に述べるようにこの国際出願に二以上の発明があるところの国際調査機関は認めた。
特別ページ参照

1. ☐ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求項について作成した。
2. ☐ 追加調査手数料を要求するまでもなく、すべての調査可能な請求項について調査することができたので、追加調査手数料の納付を求めなかった。
3. ☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったため、この国際調査報告は、手数料の納付のあった次の請求項のみについて作成した。
4. ☒ 出願人が必要な追加調査手数料を期間内に納付しなかったため、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求項について作成した。

請求項 1-24

追加調査手数料の異議の申立てに関する注意

- ☐ 追加調査手数料及び、該当する場合には、異議申立手数料の納付と共に、出願人から異議申立てがあった。
- ☐ 追加調査手数料の納付と共に出願人から異議申立てがあったが、異議申立手数料が納付命令書に示した期間内に支払われなかった。
- ☐ 追加調査手数料の納付はあったが、異議申立てはなかった。

(第Ⅲ欄のつづき)

請求項 1 に係る発明と請求項 2 5 に係る発明とは、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、前記コンテンツの閲覧を承認するか、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という共通の技術的特徴を有している。

しかしながら、当該技術的特徴は、文献 1 (JP 2008-287542 A (学校法人日本大学、学校法人慶應義塾) 2008. 11. 27, 段落【0026】 - 【0047】) の開示内容に照らして、先行技術に対する貢献をもたらすものではないから、当該技術的特徴は、特別な技術的特徴であるとはいえない。

また、これらの発明の間には、ほかに同一の又は対応する特別な技術的特徴は存在しない。そして、請求の範囲には以下に示す 2 の発明 (群) が含まれる。

(発明 1) 請求項 1 - 2 4 に係る発明

伝送遅延時間の分布特性が離散的であるか否かを判断して、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、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認証サーバ。

(発明 2) 請求項 2 5 - 3 8 に係る発明

通信端末の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、伝送遅延時間に変化があるかどうかを判断し、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、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認証サーバ。