





---

本発明は、認証サーバ側から利用者の携帯端末へ送る情報とそのタイミングを、利用者ごとに変えることに加え、認証サーバ側で制御するタイミング情報を、利用者の携帯端末から送り返すことで、認証サーバ側でタイミングの一致を確認する手法を採用する。本発明に係る携帯端末の認証システムは、通信ネットワークで接続された携帯端末2を認証サーバ1が認証する認証システムであって、携帯端末2は、認証サーバ1からタイミング信号を受信する度に、認証サーバ1へ返送用信号を返信し、認証サーバ1は、タイミング信号を携帯端末2に複数回送信して各送信時刻を記録し、返送用信号を受信して各返信時刻を記録し、各送信時刻の時間間隔と各返送用信号の返信時刻の時間間隔とが略一致している場合に、認証成功と判定する。

## 明 細 書

**発明の名称：** 携帯端末の認証システム及びその方法

### 技術分野

[0001] 本発明は、携帯端末の認証システム及びその方法に関する。

### 背景技術

[0002] 現在、携帯電話認証には契約者固有番号が使用されている。利用者自身がパスワードのように記憶しておく必要がないことが特長のひとつである。使用方法が簡単のためインターネットサービスでの利用者認証に使われている。

[0003] 携帯電話を用いた認証方法が提案されている（例えば、特許文献 1 及び 2 参照。）。特許文献 1 の発明は、返信のタイミングを秘匿にしておき、その秘匿のタイミングに送信されたことをもって認証を行う。特許文献 2 の発明は、携帯電話に電話をかけて所定の操作入力を指示し、音声メッセージに沿った操作入力がなされることをもって認証を行う。

### 先行技術文献

#### 特許文献

[0004] 特許文献1：特開 2 0 0 7 - 1 4 9 0 2 6 号公報

特許文献2：特開 2 0 0 6 - 3 3 0 8 5 6 号公報

### 発明の概要

#### 発明が解決しようとする課題

[0005] 契約者固有番号は利便性の高い認証方法であるが、現在、販売台数が伸びているスマートフォンでは使用できない欠点がある。スマートフォンでは、より一般的なコンピュータのような機器構成とネットワーク構成になることが原因である。

[0006] 特許文献 1 及び 2 の発明は、利用者が携帯端末に入力するため、正規利用者が不正利用者に転送すれば正規ユーザであるとして認証される問題がある。

[0007] 本発明は、スマートフォンでも利用できかつ認証サーバ側から利用者を特定することのできる携帯端末の認証システム及び携帯端末の認証方法を提供することを目的とする。

### 課題を解決するための手段

[0008] 上記目的を達成するために、本発明は、認証サーバ側から利用者の携帯端末へ信号を送るタイミングを利用者ごとに変え、その信号に合わせて携帯端末から返信させて、返信のタイミングの一致を認証サーバ側で確認する。

[0009] 具体的には、本発明に係る携帯端末の認証システムは、通信ネットワークで接続された携帯端末を認証サーバが認証する認証システムであって、前記携帯端末は、前記認証サーバからタイミング信号を受信する度に、前記認証サーバへ返送用信号を返信し、前記認証サーバは、前記タイミング信号を前記携帯端末に複数回送信して各送信時刻を記録し、前記返送用信号を受信して各返信時刻を記録し、前記各送信時刻の時間間隔と前記各返送用信号の返信時刻の時間間隔とが略一致している場合に、認証成功と判定する。

[0010] 本発明に係る携帯端末の認証システムは、携帯端末と認証サーバとの送受信タイミングを用いて認証を行うため、スマートフォンでも利用することができる。また、本発明に係る携帯端末の認証システムは、携帯端末からの返送用信号の返信タイミングを用いて認証を行うため、利用者が携帯端末に入力することなく認証サーバ側から利用者を特定することができる。したがって、本発明に係る携帯端末の認証システムは、スマートフォンでも利用できかつ認証サーバ側から利用者を特定することのできる携帯端末の認証システム及び携帯端末の認証方法を提供することができる。

[0011] 本発明に係る携帯端末の認証システムでは、前記認証サーバは、前記各送信時刻の時間間隔と前記各返送用信号の返信時刻の時間間隔との差が一定時間内である場合に、認証成功と判定してもよい。

[0012] 本発明に係る携帯端末の認証システムでは、前記携帯端末は、前記認証サーバからの電話着信によって、前記タイミング信号を受信し、前記認証サーバは、前記携帯端末に向けて電話発信を行うことによって前記タイミング信

号を送信し、前記認証成功と判定する際に、電話発信時刻の時間間隔と前記各返送用信号の返信時刻の時間間隔とが略一致している場合に、認証成功と判定してもよい。

[0013] 本発明に係る携帯端末の認証システムでは、前記携帯端末は、前記認証サーバからの電話着信の停止によって、前記タイミング信号を受信し、前記認証サーバは、前記携帯端末に向けて電話発信の停止を行うことによって前記タイミング信号を送信し、前記認証成功と判定する際に、電話発信の停止時刻の時間間隔と前記各返送用信号の返信時刻の時間間隔とが略一致している場合に、認証成功と判定してもよい。

[0014] 本発明に係る携帯端末の認証システムでは、前記携帯端末は、前記認証サーバからの電話着信又は電話着信の停止によって、前記タイミング信号を受信し、前記認証サーバは、前記携帯端末に向けて電話発信及び電話発信の停止を行うことによって前記タイミング信号を送信し、前記認証成功と判定する際に、電話発信から電話発信の停止までの時間間隔と電話発信に対する前記各返送用信号の返信時刻から電話発信の停止に対する前記各返送用信号の返信時刻までの時間間隔とが略一致している場合に、認証成功と判定してもよい。

[0015] 本発明に係る携帯端末の認証システムでは、前記認証サーバは、さらに、前記携帯端末へ認証用電話番号を事前に通知しておき、前記認証用電話番号を用いて前記携帯端末に向けて電話発信し、前記携帯端末は、着信番号が前記認証用電話番号であるか否かを判定し、前記認証用電話番号である場合に前記返送用信号を返信してもよい。

[0016] 本発明に係る携帯端末の認証システムでは、前記認証サーバは、前記認証用電話番号を暗号化して通知し、前記携帯端末は、暗号化された前記認証用電話番号を受信し、予め付与されている暗号鍵を用いて前記認証用電話番号を復号化してもよい。

[0017] 本発明に係る携帯端末の認証システムでは、前記携帯端末は、自端末の識別情報を前記認証サーバに送信し、前記認証サーバは、前記携帯端末からの

識別情報を受信し、当該識別情報が予め記憶されているか否かを判定し、前記識別情報が予め記憶されている場合に、予め記憶されている携帯端末の電話番号に電話発信を行ってもよい。

[0018] 本発明に係る携帯端末の認証システムでは、前記認証サーバは、HTML (HyperText Markup Language) ファイルに包含されるデータ要素を前記携帯端末に向けて送信することによって前記タイミング信号を送信し、前記携帯端末は、前記データ要素を要求する要求信号を前記認証サーバへ送信することによって前記返信を行ってもよい。

[0019] 本発明に係る携帯端末の認証システムでは、前記認証サーバは、前記タイミング信号を送信する際に、前記携帯端末に格納されている秘匿情報を読み出させる命令を前記携帯端末へ送信し、前記認証成功と判定する際に、さらに、前記携帯端末から受信した秘匿情報と予め記憶されている秘匿情報とが一致している場合に、認証成功と判定し、前記携帯端末は、前記命令を受信すると、命令のあった前記秘匿情報を読み出して前記認証サーバに送信してもよい。

[0020] 本発明に係る携帯端末の認証システムでは、前記認証サーバは、前記タイミング信号の送信時刻の後でありかつ前記返送用信号の受信の前に、電話回線を通じて前記携帯端末へ発呼し、前記携帯端末からの前記返送用信号の返信があるか否かを判定し、前記認証成功と判定する際に、さらに、前記返送用信号の返信がない場合に、認証成功と判定し、前記携帯端末は、前記タイミング信号の受信の後に前記認証サーバからの着信を受けてもよい。

[0021] 具体的には、本発明に係る携帯端末の認証方法は、認証サーバから携帯端末にタイミングを通知し、タイミングの通知時刻を記録するタイミング通知手順と、前記タイミング通知手順におけるタイミングの通知を契機に、携帯端末から認証サーバへ返信を行い、当該返信時刻を記録する返信手順と、をランダムなタイミングで順に複数回繰り返し、前記タイミング通知手順において記録した前記通知時刻の時間間隔と前記返信手順において記録した前記返信時刻の時間間隔とが略一致している場合に、認証成功と判定する認証判

定手順と、を順に有する。

[0022] 本発明に係る携帯端末の認証方法は、携帯端末と認証サーバとの送受信タイミングを用いて認証を行うため、スマートフォンでも利用することができる。また、本発明に係る携帯端末の認証方法は、携帯端末からの返送用信号の返信タイミングを用いて認証を行うため、利用者が携帯端末に入力することなく認証サーバ側から利用者を特定することができる。したがって、本発明に係る携帯端末の認証方法は、スマートフォンでも利用できかつ認証サーバ側から利用者を特定することのできる携帯端末の認証システム及び携帯端末の認証方法を提供することができる。

[0023] 本発明に係る携帯端末の認証方法では、前記認証判定手順において、さらに、前記各送信時刻の時間間隔と前記各返送用信号の返信時刻の時間間隔との差が一定時間内である場合に、認証成功と判定してもよい。

[0024] 本発明に係る携帯端末の認証方法では、前記タイミング通知手順において、認証サーバから携帯端末に向けて電話発信を行うことによってタイミングを通知し、前記返信手順における前記契機は、認証サーバからの電話着信であり、前記認証判定手順において、前記電話発信の時間間隔と前記返信時刻の時間間隔とが略一致している場合に、認証成功と判定してもよい。

[0025] 本発明に係る携帯端末の認証方法では、前記タイミング通知手順において、認証サーバから携帯端末に向けて電話発信の停止を行うことによってタイミングを通知し、前記返信手順における前記契機は、認証サーバからの電話着信の停止であり、前記認証判定手順において、前記電話発信の停止の時間間隔と前記返信時刻の時間間隔とが略一致している場合に、認証成功と判定してもよい。

[0026] 本発明に係る携帯端末の認証方法では、前記タイミング通知手順において、認証サーバから携帯端末に向けて電話発信を行い、認証サーバから携帯端末に向けて電話発信の停止を行い、前記返信手順における前記契機は、認証サーバからの電話着信又は電話着信の停止であり、前記認証判定手順において、前記電話発信から前記電話発信の停止までの時間間隔と電話発信に対す

る前記返信時刻から電話発信の停止に対する前記返信時刻までの時間間隔とが略一致している場合に、認証成功と判定してもよい。

[0027] 本発明に係る携帯端末の認証方法では、認証サーバから携帯端末へ認証用電話番号を通知する認証用電話番号通知手順を、前記タイミング通知手順の前にさらに有し、前記タイミング通知手順において、前記認証用電話番号通知手順で通知した認証用電話番号を用いて認証サーバから携帯端末に向けて電話発信し、前記返信手順において、前記認証用電話番号からの着信を契機に、携帯端末から認証サーバへ返信を行ってもよい。

[0028] 本発明に係る携帯端末の認証方法では、携帯端末から認証サーバに携帯端末の識別情報を通知し、当該識別情報が認証サーバに記憶されているか否かを判定する識別情報判定手順を、前記タイミング通知手順又は前記認証用電話番号通知手順の前にさらに有し、前記識別情報が認証サーバに記憶されている場合に、前記タイミング通知手順において、認証サーバの記憶している携帯端末の電話番号に電話発信を行ってもよい。

[0029] 本発明に係る携帯端末の認証方法では、前記タイミング通知手順において、前記返信手順から前記タイミング通知手順までの間に、ランダムに変化する任意の時間間隔を有してもよい。

[0030] 本発明に係る携帯端末の認証方法では、前記返信手順において、前記タイミング通知手順から前記返信手順までの間に、ランダムに変化する任意の時間間隔を有してもよい。

[0031] 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

[0032] 本発明によれば、スマートフォンでも利用できかつ認証サーバ側から利用者を特定することのできる携帯端末の認証システム及び携帯端末の認証方法を提供することができる。本発明は、認証サーバ側から利用者を特定するため、利用者側での秘密情報の不正な利用や、正規の認証プロセス変えてしまうような不正なアクセスによる認証を防止することができる。

## 図面の簡単な説明

[0033] [図1]実施形態 1 に係る認証システムの一例を示す。

[図2]実施形態 1 に係るタイミング信号の送信時刻と返送用信号の返信時刻の一例を示す。

[図3]実施形態 2 に係る認証システムの一例を示す。

[図4]実施形態 2 に係るタイミング信号の送信時刻と返送用信号の返信時刻の一例を示す。

[図5]実施形態 3 に係るタイミング信号の送信時刻と返送用信号の返信時刻の一例を示す。

[図6]実施形態 4 に係るタイミング信号の送信時刻と返送用信号の返信時刻の一例を示す。

[図7]実施形態 5 に係る認証方法のシーケンス図を示す。

[図8]実施形態 6 に係る認証システムの一例を示す。

[図9]データ取得部に準備されているウェブページの一例を示す。

[図10]HTMLによるWebページのダウンロードプロセスを示す。

[図11]携帯端末がパイプライン処理を行う場合の送信時刻の時間間隔及び返信時刻の時間間隔の測定方法の一例を示す。

[図12]送信時刻の時間間隔及び返信時刻の時間間隔の測定方法の他の一例を示す。

## 発明を実施するための形態

[0034] 添付の図面を参照して本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。

[0035] (実施形態 1)

図 1 に、本実施形態に係る認証システムの一例を示す。本実施形態の認証システムは、認証に使用する利用者ごと秘密情報は時間である。本実施形態の認証システムは、通信ネットワークで接続された携帯端末 2 を認証サーバ 1 が認証する認証システムである。本実施形態に係る認証方法は、タイミン

グ通知手順及び返信手順をランダムなタイミングで順に複数回繰り返す、その後、認証判定手順を実行する。

[0036] タイミング通知手順では、認証サーバ1は、タイミング信号を携帯端末2に複数回送信して各送信時刻を記録する。返信手順では、携帯端末2は、認証サーバ1からタイミング信号を受信する度に、認証サーバ1へ返送用信号を返信する。認証サーバ1は、返送用信号を受信して各返信時刻を記録する。認証判定手順では、タイミング通知手順において記録した各送信時刻の時間間隔と返信手順において記録した返信時刻の時間間隔とが略一致している場合に、認証成功と判定する。タイミング信号及び返送用信号は、データ通信を用いて伝送される信号であってもよいし、電話回線を用いて伝送される信号であってもよい。

[0037] ここで、本実施形態に係る認証方法は、タイミング通知手順及び返信手順をランダムなタイミングで順に複数回繰り返す。例えば、タイミング通知手順において、返信手順からタイミング通知手順までの間に、ランダムに変化する任意の時間間隔を有してもよい。また、返信手順において、タイミング通知手順から返信手順までの間に、ランダムに変化する任意の時間間隔を有してもよい。

[0038] タイミング通知手順から返信手順までの間に、ランダムに変化する任意の時間間隔を有する場合、認証サーバ1から携帯端末2へ返送用信号を送信する返信時間を指定し、携帯端末2は指定された返信時間に返送用信号を返信する。返信時間の指定は、タイミング信号を受信後の経過時間を指定してもよいし、時刻を指定してもよい。また、認証サーバ1が返信時間を暗号化して携帯端末2へ送信し、携帯端末2が返信時間を復号化してもよい。この場合の暗号鍵は、携帯端末2に予め格納されている携帯端末2固有の情報であってもよいし、認証サーバ1から携帯端末2へ予め付与しておいてもよい。携帯端末2固有の情報は、例えば、SIM (Subscriber Identity Module) カードにIMSI (International Mobile Subscriber Identity) 若しくはI

MEI (International Mobile Equipment Identifier)、MAC (Media Access Control) アドレス、IP (Internet Protocol) アドレス又は電話番号である。暗号鍵を認証サーバ1から携帯端末2へ付与する場合は、認証サーバ1から携帯端末2へ暗号鍵を認証の度に付与することで、認証の度に異なる暗号鍵を用いて復号化することが好ましい。また、携帯端末2の利用者が返信時間を見ることができないよう、携帯端末2に返信時間が表示されないようなプログラムを携帯端末2に組み込むことが好ましい。

[0039] 図2に、実施形態1に係るタイミング信号の送信時刻と返送用信号の返信時刻の一例を示す。

(1) 携帯端末2が認証サーバ1に最初にアクセスすると、それに対するレスポンスとして、認証サーバ1は携帯端末2の一意な番号に任意な情報を送り、その送信時刻  $t_{s1}$  を記録する。

(2) 携帯端末2は、任意な情報を返送用信号として認証サーバ1に返送する。

(3) 認証サーバ1では、送信した任意な情報と同じものが返送されることをまず確認し、返送用信号を受信した時刻を返信時刻  $t_{r1}$  として記録する。

(4) 認証サーバ1は、任意な情報の送出を繰り返し、その送出間隔をランダムに変更する。

(5) その結果、認証サーバ1には、任意な情報の送信時刻  $t_{s1}$ 、 $t_{s2}$ 、 $t_{s3}$ 、・・・と、その返信時刻  $t_{r1}$ 、 $t_{r2}$ 、 $t_{r3}$ 、・・・が記録される。

[0040] (6) 原理的には、携帯端末2が正規の利用者であり、登録されている一意な番号で認証サーバ1からの情報を受信していれば、任意な情報の送出時間間隔  $T_{s1}$  と返信時刻の時間間隔  $T_{r1}$  は同じであり、任意な情報の送出時間間隔  $T_{s2}$  と返信時刻の時間間隔  $T_{r2}$  は同じであり、任意な情報の送出時間間隔  $T_{s3}$  と返信時刻の時間間隔  $T_{r3}$  は同じになる。

[0041] 実際の認証処理では、返信時刻の時間間隔  $T_{r1}$ 、 $T_{r2}$ 、 $T_{r3}$ 、・・・

・に、認証サーバ1から携帯端末2までの往復遅延時間の変動と、携帯端末2内での処理時間の変動を考慮する必要がある。そこで、認証判定手順において、認証サーバ1は、各送信時刻の時間間隔 $T_{s1}$ 、 $T_{s2}$ 、 $T_{s3}$ 、 $\dots$ と各返送用信号の返信時刻の時間間隔 $T_{r1}$ 、 $T_{r2}$ 、 $T_{r3}$ 、 $\dots$ との差が一定時間内である場合に、認証成功と判定する。

[0042] 例えば、本実施形態では、変動による誤差 $\Delta$ を考慮すると、以下のような関係となる。

$$T_{r1} = T_{s1} \pm \Delta 1$$

$$T_{r2} = T_{s2} \pm \Delta 2$$

$$T_{r3} = T_{s3} \pm \Delta 3$$

[0043] この $\Delta 1$ 、 $\Delta 2$ 、 $\Delta 3$ 、 $\dots$ は、実験的に求める必要がある。実際の認証フローでは、実験的に求めた $\Delta$ の最大値 $\Delta_{max}$ に認証判断のしきい値となる一定時間を設定する。認証は、任意な情報の送出をランダムな時間間隔で繰り返し、

$$|T_{r_n} - T_{s_n}| \leq \Delta_{max}$$

であることが確認されれば、その利用者は正規の利用者と認証される。

[0044] 本実施形態に係る認証方法を用いることで、複数の携帯端末2が同時にアクセスしてきた場合は認証失敗になるため、複数人同時のなりすましを防ぐことができる。また、 $\Delta_{max}$ を、正規の利用者の携帯端末2であれば $\Delta_{max}$ 以内であるけれども、正規の利用者以外の者であれば $\Delta_{max}$ 超となる値に設定することで、正規の利用者以外の者によるなりすましを防ぐことができる。

[0045] 本実施形態では、タイミング通知手順において、認証サーバ1は、携帯端末2に格納されている秘匿情報を読み出させる命令を携帯端末2へ送信してもよい。秘匿情報は、予め携帯端末2に付与した情報であり、暗号であってもよいし、携帯端末固有の情報であってもよい。この場合、返信手順において、携帯端末2は、命令を受信すると、命令のあった秘匿情報を読み出して認証サーバ1に送信する。そして、認証判定手順において、さらに、携帯端

末 2 から受信した秘匿情報と予め記憶されている秘匿情報とが一致している場合に、認証成功と判定する。これにより、認証要素が増えるため、認証精度を高めることができる。

[0046] (実施形態 2)

図 3 に、実施形態 2 に係る認証システムの一例を示す。本実施形態に係る認証システムは、認証サーバ 1 が電話発信部 1 1 及び認証判定部 1 2 を備え、携帯端末 2 が電話着信部 2 1 及びタイミング検出部 2 2 を備える。本実施形態では、タイミング信号を送信するために電話発信部 1 1 が電話発信を行い、タイミング検出部 2 2 が返送用信号として着信時刻情報を送信する。

[0047] 図 4 に、実施形態 2 に係るタイミング信号の送信時刻と返送用信号の返信時刻の一例を示す。

タイミング通知手順において、電話発信部 1 1 が携帯端末 2 に向けて電話発信を行うことによってタイミングを通知する。そして、認証判定部 1 2 は、電話発信部 1 1 の電話発信時刻  $t_{s1}$ 、 $t_{s2}$ 、 $\dots$  を記録する。

[0048] 返信手順において、電話着信部 2 1 が認証サーバ 1 からの電話を着信することによって、タイミング信号を受信する。タイミング検出部 2 2 は、電話着信部 2 1 の着信時刻  $t_{n1}$ 、 $t_{n2}$ 、 $\dots$  を検出して記録する。そして、タイミング検出部 2 2 は、電話着信部 2 1 の着信時刻情報を返送用信号として認証サーバ 1 に返信する。返送用信号の返信方法は、データ通信を行うことによって返信してもよいし、電話発信することによって返信してもよい。認証判定部 1 2 は、タイミング検出部 2 2 から着信時刻情報を受信し、その受信時刻を返信時刻  $t_{r1}$ 、 $t_{r2}$ 、 $\dots$  として記録する。

[0049] 認証判定手順において、認証判定部 1 2 が、電話発信部 1 1 の電話発信時刻  $t_{s1}$ 、 $t_{s2}$ 、 $\dots$  の時間間隔  $T_{s1}$ 、 $T_{s2}$ 、 $\dots$  と着信時刻情報の受信時刻  $t_{r1}$ 、 $t_{r2}$ 、 $\dots$  の時間間隔  $T_{r1}$ 、 $T_{r2}$ 、 $\dots$  とが略一致している場合に、認証成功と判定する。例えば、時間間隔  $T_{s1}$  と時間間隔  $T_{r1}$  が一致し、かつ、時間間隔  $T_{s2}$  と時間間隔  $T_{r2}$  が一致し、かつ、時間間隔  $T_{s3}$  と時間間隔  $T_{r3}$  が一致する場合に、認証成功と判定す

る。

[0050] 認証判定部 12 は、着信時刻情報に含まれる着信時刻  $t_{n1}$ 、 $t_{n2}$ 、 $\dots$  を用いて、予想される標準的な遅延時間内に電話着信部 21 が電話を着信したか否かを判断してもよい。予想される標準的な遅延時間は、利用者の初期登録時などで測定した結果と、他の同様な携帯端末でのデータとを考慮して決定する。この場合、着信停止時刻情報の受信時刻である返信時刻の時間間隔  $T_{r1}$ 、 $T_{r2}$ 、 $\dots$  に代えて、電話着信部 21 の着信時刻  $t_{n1}$ 、 $t_{n2}$ 、 $\dots$  の時間間隔  $T_{n1}$ 、 $T_{n2}$ 、 $\dots$  を用いる。すなわち、認証サーバ 1 が電話発信する送信時刻の時間間隔  $T_{s1}$ 、 $T_{s2}$ 、 $\dots$  と、電話着信部 21 の着信時刻の時間間隔  $T_{n1}$ 、 $T_{n2}$ 、 $\dots$  と、を比較し、時間間隔  $T_{s1}$  と時間間隔  $T_{n1}$  がしきい値以内であり、時間間隔  $T_{s2}$  と時間間隔  $T_{n2}$  がしきい値以内であり、時間間隔  $T_{s3}$  と時間間隔  $T_{n3}$  がしきい値以内であれば、認証成功と判定する。しきい値は、利用者の初期登録時などで測定した結果と、他の同様な携帯電話でのデータとを考慮して決定する。

[0051] (実施形態 3)

本実施形態に係る認証システム及び認証方法は、携帯端末 2 が、着信による呼び出しが停止したときに、認証サーバ 1 に返送用信号を送信する。

[0052] 図 5 に、実施形態 3 に係るタイミング信号の送信時刻と返送用信号の返信時刻の一例を示す。

タイミング通知手順において、電話発信部 11 が携帯端末 2 への電話発信の停止を行うことによってタイミングを通知する。そして、認証判定部 12 は、電話発信部 11 の発信停止時刻  $t_{s1}$ 、 $t_{s2}$ 、 $\dots$  を記録する。

[0053] 返信手順において、電話着信部 21 が、認証サーバ 1 からの電話の着信の停止を検出することによって、タイミング信号を受信する。タイミング検出部 22 は、電話着信部 21 の着信停止時刻  $t_{n1}$ 、 $t_{n2}$ 、 $\dots$  を検出して記録する。そして、タイミング検出部 22 は、電話着信部 21 の着信停止時刻を含む着信停止時刻情報を、返送用信号として認証サーバ 1 に返信する。

認証判定部 12 が、タイミング検出部 22 からの着信停止時刻情報を受信し、着信停止時刻情報の受信時刻を返信時刻として記録する。

[0054] 認証判定手順において、認証判定部 12 が、電話発信部 11 の発信停止時刻の時間間隔  $T_{s1}$ 、 $T_{s2}$ 、・・・と着信停止時刻情報の受信時刻の時間間隔  $T_{r1}$ 、 $T_{r2}$ 、・・・とが略一致している場合に、認証成功と判定する。

[0055] 認証判定部 12 は、着信停止時刻情報を用いて、予想される標準的な遅延時間内に電話着信部 21 の電話の着信が停止したか否かを判断してもよい。この場合、着信停止時刻情報の受信時刻の時間間隔  $T_{r1}$ 、 $T_{r2}$ 、・・・に代えて、電話着信部 21 の着信停止時刻の時間間隔  $T_{n1}$ 、 $T_{n2}$ 、・・・を用いる。すなわち、認証サーバ 1 の発信停止時刻の時間間隔  $T_{s1}$ 、 $T_{s2}$ 、・・・と、電話着信部 21 の着信停止時刻の時間間隔  $T_{n1}$ 、 $T_{n2}$ 、・・・と、を比較し、時間間隔  $T_{s1}$  と時間間隔  $T_{n1}$  がしきい値以内であり、時間間隔  $T_{s2}$  と時間間隔  $T_{n2}$  がしきい値以内であれば、認証成功と判定する。しきい値は、利用者の初期登録時などで測定した結果と、他の同様な携帯電話でのデータとを考慮して決定する。

[0056] (実施形態 4)

本実施形態では、認証サーバからの電話発信から電話発信停止までの時間間隔を時間間隔  $T_{s1}$ 、 $T_{s2}$ 、 $T_{s3}$ 、・・・として用い、電話発信に対する各返送用信号の返信時刻から電話発信停止に対する各返送用信号の返信時刻までの時間間隔を時間間隔  $T_{r1}$ 、 $T_{r2}$ 、 $T_{r3}$ 、・・・として用いる。

[0057] 図 6 に、実施形態 4 に係るタイミング信号の送信時刻と返送用信号の返信時刻の一例を示す。

第 1 のタイミング通知手順において、電話発信部 11 が携帯端末 2 に向けて電話発信を行うことによってタイミングを通知する。認証判定部 12 は、電話発信部 11 の電話発信時刻  $t_{s1}$  を記録する。

第 1 の返信手順において、電話着信部 21 が認証サーバ 1 からの電話を着

信することによって、タイミング信号を受信する。タイミング検出部 22 は、電話着信部 21 の着信時刻  $t_{n1}$  を検出して記録する。そして、タイミング検出部 22 は、電話着信部 21 の着信時刻情報を返送用信号として認証サーバ 1 に返信する。認証判定部 12 は、タイミング検出部 22 から着信時刻情報を受信し、受信時刻  $t_{r1}$  を記録する。

[0058] 第 2 のタイミング通知手順において、電話発信部 11 が携帯端末 2 に向けて電話発信の停止を行うことによってタイミングを通知する。認証判定部 12 は、電話発信部 11 の発信停止時刻  $t_{s2}$  を記録する。

第 2 の返信手順において、電話着信部 21 が認証サーバ 1 からの電話着信の停止によって、タイミング信号を受信する。タイミング検出部 22 は、電話着信部 21 の着信停止時刻  $t_{n2}$  を検出して記録する。そして、タイミング検出部 22 は、電話着信部 21 の着信停止時刻情報を返送用信号として認証サーバ 1 に返信する。認証判定部 12 は、タイミング検出部 22 から着信停止時刻情報を受信し、受信時刻  $t_{r2}$  を記録する。

[0059] 第 1 のタイミング通知手順、第 1 の返信手順、第 2 のタイミング通知手順及び第 2 の返信手順を順に実行する。第 1 のタイミング通知手順、第 1 の返信手順、第 2 のタイミング通知手順及び第 2 の返信手順を 1 度以上行った後に、認証判定手順を行う。

[0060] 認証判定手順において、認証判定部 12 が、電話発信時刻  $t_{s1}$  から発信停止時刻  $t_{s2}$  までの時間間隔  $T_{s1}$  と電話発信に対する各返送用信号の返信時刻である受信時刻  $t_{r1}$  から電話発信の停止に対する各返送用信号の返信時刻である受信時刻  $t_{r2}$  までの時間間隔  $T_{r1}$  とが略一致している場合に、認証成功と判定する。

[0061] このように、認証サーバ 1 が電話をかけて呼び出し、呼び出しを停止するまでの呼び出し時間間隔  $T_{s1}$ 、 $T_{s2}$ 、 $T_{s3}$ 、・・・と、利用者携帯電話が受信した時間と呼び出しが停止した時間から求められる呼び出し時間間隔  $T_{r1}$ 、 $T_{r2}$ 、 $T_{r3}$ 、・・・を比較し、しきい値以内であれば、利用者携帯電話を認証する。しきい値は、利用者の初期登録時などで測定した結

果と、他の同様な携帯電話でのデータとを考慮して決定する。

[0062] 認証サーバ1による呼び出し時間は、認証サーバ1側でランダムに変化させる。これにより不正に認証サーバ1側に電話着信による情報を送信されることを防ぐことができる。

[0063] (実施形態5)

図7に、実施形態5に係る認証方法のシーケンス図を示す。本実施形態に係る認証方法は、タイミング通知手順の前に、識別情報判定手順及び認証用電話番号通知手順を更に順に有する。

[0064] 識別情報判定手順では、ステップS101～ステップS104を行う。

ステップS101では、携帯端末2が認証サーバ1に認証要求を行う。

ステップS102では、認証サーバ1が、携帯端末2の識別情報を携帯端末2に要求する。識別情報は、例えばID及びパスワード(PW)である。

ステップS103では、携帯端末2が、ID及びパスワード(PW)を認証サーバ1に送信する。

ステップS104では、認証サーバ1が、ID及びパスワード(PW)が予め登録された正規のものであるか確認し、正規のものである場合は、認証用電話番号通知手順を行う。認証用電話番号通知手順では、認証サーバ1から携帯端末2へ認証用電話番号を通知する。

[0065] ステップS105では、タイミング通知手順において、認証サーバ1が、発信者番号を表示して電話をかける。このとき、認証サーバ1は、認証用電話番号通知手順で通知した認証用電話番号からだけでなく、他の電話番号からも電話をかける。

[0066] ステップS106では、携帯端末2が、通知された認証用電話番号から電話がかかってきたときにだけ返信手順を行う。すなわち、携帯端末2は、通知された認証用電話番号から電話がかかってきたときにだけ、返送用信号を認証サーバ1に送信する。

[0067] ステップS105及びステップS106を繰り返す。このとき、認証用電話番号ランダムに変更する。そして、認証判定手順を行い(ステップS10

7)、認証判定手順において認証が成功した場合、認証サーバ1は正規の利用者である旨を通知する(ステップS108)。

[0068] このように、本実施形態では、認証サーバ1が利用者の携帯端末2に電話をかける前に、認証サーバ1側から携帯端末2に認証サーバ1側の認証用電話番号を通知し、その後利用者の携帯端末2に電話をかける。これにより、認証要素を増やすことができるため、認証精度を高めることができる。

[0069] さらに、利用者の携帯端末2は、認証サーバ1から通知される認証用電話番号を表示しないことが好ましい。例えば、専用のソフトウェアを用いる。これにより、不正に認証サーバ1から情報を得ている場合には、電話着信を選択することができないようにすることができる。ID及びPWを送受信する端末と、認証サーバ1から電話を受ける端末を分けるような、携帯端末2のなりすましが行われた場合、認証精度を向上する効果がある。

[0070] 本実施形態では、ステップS106において、携帯端末2は、認証用電話番号を認証サーバ1に送信してもよい。この場合、ステップS107の認証判定手順において、認証サーバ1は、さらに、携帯端末2に通知した認証用電話番号と携帯端末2から受信した認証用電話番号とが一致している場合に、認証成功と判定してもよい。

[0071] 本実施形態では、ステップS104の認証用電話番号通知手順において、認証用電話番号を暗号化して通知してもよい。例えば、認証サーバ1と携帯端末2の間のデータ通信を、たとえばSSL(Secure Socket Layer)/TLS(Transport Layer Security)などで、インターネット上のデータ通信を暗号化する。この場合、携帯端末2は、暗号化された認証用電話番号を受信し、予め付与されている暗号鍵を用いて認証用電話番号を復号化する。これにより、認証サーバ1から通知される認証用電話番号を、携帯端末2の利用者に悪用されることなく、携帯端末2のソフトウェアに通知することができる。

[0072] ここで、認証用電話番号、暗号化アルゴリズム及び暗号鍵は、利用者ごとなわち携帯端末2ごとに異なることが好ましい。また、認証サーバ1は、

携帯端末 2 に搭載されるソフトウェアを定期的に変更することが好ましく、この場合は各携帯端末 2 の使用しているソフトウェアのバージョンを管理することが好ましい。携帯端末 2 は、認証の度に、使用するソフトウェアのバージョン情報を認証サーバ 1 へ送信することが好ましく、この際にバージョン情報を暗号化して送信することが好ましい。

[0073] 本実施形態では、認証用電話番号通知手順において、認証サーバ 1 から携帯端末 2 へ通知する認証用電話番号又は認証用電話番号を暗号化するアルゴリズム若しくは暗号鍵のいずれかを、予め定められた携帯端末 2 のグループごとに変化させてもよい。

[0074] なお、実施形態 2 ～実施形態 5 において、タイミング信号が電話回線を用いて伝送される信号であり、返送用信号がデータ通信を用いて伝送される信号である場合について説明したが、返送用信号に電話回線を用いて伝送される信号を用いてもよい。

[0075] (実施形態 6)

図 8 に、実施形態 6 に係る認証システムの一例を示す。本実施形態に係る認証システムは、認証サーバ 1 が電話発信部 1 1 と、認証判定部 1 2 と、データ取得部 1 3 と、を備え、携帯端末 2 が送受信部 2 3 を備える。本実施形態では、タイミング信号及び返送用信号がデータの送受信である。

[0076] 具体的には、タイミング通知手順において、認証サーバ 1 は、HTML ファイルに包含されるデータ要素を携帯端末 2 に向けて送信することによってタイミング信号を送信する。返信手順において、携帯端末 2 は、データ要素を要求する要求信号を認証サーバ 1 へ送信することによって返送用信号の返信を行う。

[0077] 図 9 に、データ取得部 1 3 に準備されているウェブページの一例を示す。携帯端末 2 を認証するために、携帯端末 2 が認証サーバ 1 に接続すると、携帯端末 2 は、図 9 に示すような web ページにアクセスする。このページには、複数個の画像などのデータ要素  $e_1 \sim e_N$  が埋め込まれている。携帯端末 2 のブラウザが、このページをダウンロードすると、データ要素  $e_1 \sim e_N$  を

要求する複数の要求信号が発生することになる。

[0078] 図10は、HTMLによるWebページのダウンロードプロセスを示す。HTTPによるWebページのダウンロードでは、最初にそのページのHTMLファイルがダウンロードされる。このときに、リクエストGET1が携帯端末2から送信され、データ取得部13はレスポンス1を携帯端末2に送信する。携帯端末2は、レスポンス1によって取得したHTMLファイルを解析後、Webページに含まれている各データ要素 $e_1 \sim e_N$ をダウンロードする。

[0079] 携帯端末2がGETコマンドを使ってWebページ内のデータ要素をダウンロードすると、データ取得部13は、ある時間間隔で要求信号を受信することになる。このとき、データ取得部13で、要求信号の時間間隔を測定する。図10に示すように、レスポンス1からレスポンス2までを送信時刻の時間間隔 $T_{s1}$ として測定し、リクエストGET2からリクエストGET3までを返信時刻の時間間隔 $T_{r1}$ として測定する。

[0080] 携帯端末2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11に示すように、携帯端末2が、画像ファイル $e_1$ の要求信号であるリクエストGET2と、画像ファイル $e_2$ の要求信号であるリクエストGET3と、画像ファイル $e_3$ 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端末2の場合、携帯端末2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、返信時刻の時間間隔 $T_{r1}$ 、 $T_{r2}$ 、 $T_{r3}$ 、・・・を測定することができない。そこで、認証サーバ1のデータ取得部13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。

[0081] 例えば、データ取得部13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 2 を携帯端末 2 に送信し、その後に 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 3 及びレスポンス 4 を送信しない。これにより、携帯端末 2 は、レスポンス 2 の受信後に、改めてリクエスト GET 3 を送信する。

[0082] データ取得部 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間隔を返信時刻の時間間隔  $T_{r1}$  として測定する。

[0083] また、パイプライン処理を行う携帯端末 2 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 を受信したデータ取得部 13 は、パイプライン処理に対応していない旨の情報を携帯端末 2 に送信し、携帯端末 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 (HyperText Transfer Protocol) / 1.0 又は HTTP / 0.9 の仕様の HTTP である旨を携帯端末 2 に送信する。こうすることで、図 10 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測定を行うことができる。

[0084] 図 12 に、データ取得部 13 における他の送信時刻の時間間隔  $T_{s1}$ 、 $T_{s2}$ 、 $T_{s3}$ 、・・・及び返信時刻の時間間隔  $T_{r1}$ 、 $T_{r2}$ 、 $T_{r3}$ 、・・・の測定方法の一例を示す。携帯端末 2 は、画像ファイル  $e_2$  を受信すると、TCP (Transmission Control Protocol) のクローズ信号 (FIN)  $C_2$  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 の要求信号の時間間隔を送信時刻の時間間隔  $T_{s1}$ 、 $T_{s2}$ 、 $T_{s3}$ 、・・・として用い、データ要素を送信後のクローズ信号を受信する時間間隔を返信時刻の時間間隔  $T_{r1}$ 、 $T_{r2}$ 、 $T_{r3}$ 、・・・として測定する。

[0085] 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、同時に送信時刻の時間間隔  $T_{s1}$ 、 $T_{s2}$ 、 $T_{s3}$ 、・・・及び返信時刻

の時間間隔  $T_{r1}$ 、 $T_{r2}$ 、 $T_{r3}$ 、 $\dots$  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、送信時刻の時間間隔  $T_{s1}$ 、 $T_{s2}$ 、 $T_{s3}$ 、 $\dots$  及び返信時刻の時間間隔  $T_{r1}$ 、 $T_{r2}$ 、 $T_{r3}$ 、 $\dots$  が長くなることが予想されるが、処理データとして使用することができる。

[0086] 本実施形態では、タイミング通知手順と前記返信手順の間に、認証サーバ 1 から電話回線を通じて携帯端末 2 へ発呼する認証サーバ発呼手順をさらに有してもよい。認証サーバ発呼手順では、認証サーバ 1 が、タイミング信号の送信時刻  $t_{s1}$ 、 $t_{s2}$ 、 $t_{s3}$ 、 $\dots$  の後でありかつ返送用信号の受信時刻  $t_{r1}$ 、 $t_{r2}$ 、 $t_{r3}$ 、 $\dots$  の前に、電話発信部 11 が電話回線を通じて携帯端末 2 へ発呼する。たとえば、データ取得部 13 がリクエスト GET 4 を受信した直後に、電話発信部 11 が携帯端末 2 へ電話をかける。この場合、携帯端末 2 は、タイミング信号の受信の後に認証サーバ 1 からの着信を受け、リクエスト GET 5 の送信が停止する。このため、データ取得部 13 はリクエスト GET 5 の受信ができなくなる。そこで、認証判定部 12 が、携帯端末 2 からの要求信号があるか否かを判定し、認証成功と判定する際に、さらに、返送用信号の返信がない場合に、認証成功と判定する。ここで、携帯端末 2 からの要求信号がないことは、リクエスト GET 5 の受信予定時刻にリクエスト GET 5 を受信しないことによって判定することができる。

[0087] なお、実施形態 1 ～実施形態 6 に係る発明は、いずれも組み合わせが可能である。例えば、1 度目のタイミング信号と返送用信号の送受信は実施形態 2 ～実施形態 5 のいずれかの発明を用い、2 度目以降のタイミング信号と返送用信号の送受信は実施形態 6 の発明を用いる。このように、タイミング信号と返送用信号の送受信において実施形態 1 ～実施形態 6 に係る発明を組み合わせることで、認証精度を高めることができる。

**産業上の利用可能性**

[0088] 本発明は情報通信産業に適用することができる。

### 符号の説明

[0089] 1 : 認証サーバ

2 : 携帯端末

1 1 : 電話発信部

1 2 : 認証判定部

1 3 : データ取得部

2 1 : 電話着信部

2 2 : タイミング検出部

2 3 : 送受信部

## 請求の範囲

- [請求項1]           通信ネットワークで接続された携帯端末を認証サーバが認証する認証システムであって、
- 前記携帯端末は、前記認証サーバからタイミング信号を受信する度に、前記認証サーバへ返送用信号を返信し、
- 前記認証サーバは、前記タイミング信号を前記携帯端末に複数回送信して各送信時刻を記録し、前記返送用信号を受信して各返信時刻を記録し、前記各送信時刻の時間間隔と前記各返送用信号の返信時刻の時間間隔とが略一致している場合に、認証成功と判定する、
- 携帯端末の認証システム。
- [請求項2]           前記認証サーバは、前記各送信時刻の時間間隔と前記各返送用信号の返信時刻の時間間隔との差が一定時間内である場合に、認証成功と判定することを特徴とする請求項1に記載の携帯端末の認証システム。
- [請求項3]           前記携帯端末は、前記認証サーバからの電話着信によって、前記タイミング信号を受信し、
- 前記認証サーバは、前記携帯端末に向けて電話発信を行うことによって前記タイミング信号を送信し、前記認証成功と判定する際に、電話発信時刻の時間間隔と前記各返送用信号の返信時刻の時間間隔とが略一致している場合に、認証成功と判定する、
- ことを特徴とする請求項1又は2に記載の携帯端末の認証システム。
- [請求項4]           前記携帯端末は、前記認証サーバからの電話着信の停止によって、前記タイミング信号を受信し、
- 前記認証サーバは、前記携帯端末に向けて電話発信の停止を行うことによって前記タイミング信号を送信し、前記認証成功と判定する際に、電話発信の停止時刻の時間間隔と前記各返送用信号の返信時刻の時間間隔とが略一致している場合に、認証成功と判定する、

ことを特徴とする請求項 1 又は 2 に記載の携帯端末の認証システム。  
。

[請求項5] 前記携帯端末は、前記認証サーバからの電話着信又は電話着信の停止によって、前記タイミング信号を受信し、

前記認証サーバは、前記携帯端末に向けて電話発信及び電話発信の停止を行うことによって前記タイミング信号を送信し、前記認証成功と判定する際に、電話発信から電話発信の停止までの時間間隔と電話発信に対する前記各返送用信号の返信時刻から電話発信の停止に対する前記各返送用信号の返信時刻までの時間間隔とが略一致している場合に、認証成功と判定する、

ことを特徴とする請求項 1 又は 2 に記載の携帯端末の認証システム。  
。

[請求項6] 前記認証サーバは、さらに、前記携帯端末へ認証用電話番号を事前に通知しておき、前記認証用電話番号を用いて前記携帯端末に向けて電話発信し、

前記携帯端末は、着信番号が前記認証用電話番号であるか否かを判定し、前記認証用電話番号である場合に前記返送用信号を返信する、

ことを特徴とする請求項 3 から 5 のいずれかに記載の携帯端末の認証システム。

[請求項7] 前記認証サーバは、前記認証用電話番号を暗号化して通知し、

前記携帯端末は、暗号化された前記認証用電話番号を受信し、予め付与されている暗号鍵を用いて前記認証用電話番号を復号化する、

ことを特徴とする請求項 6 に記載の携帯端末の認証システム。

[請求項8] 前記携帯端末は、自端末の識別情報を前記認証サーバに送信し、

前記認証サーバは、前記携帯端末からの識別情報を受信し、当該識別情報が予め記憶されているか否かを判定し、前記識別情報が予め記憶されている場合に、予め記憶されている携帯端末の電話番号に電話発信を行う、

ことを特徴とする請求項 3 から 7 のいずれかに記載の携帯端末の認証システム。

[請求項9] 前記認証サーバは、HTML (HyperText Markup Language) ファイルに包含されるデータ要素を前記携帯端末に向けて送信することによって前記タイミング信号を送信し、

前記携帯端末は、前記データ要素を要求する要求信号を前記認証サーバへ送信することによって前記返信を行う、

ことを特徴とする請求項 1 又は 2 に記載の携帯端末の認証システム。

[請求項10] 前記認証サーバは、前記タイミング信号を送信する際に、前記携帯端末に格納されている秘匿情報を読み出させる命令を前記携帯端末へ送信し、前記認証成功と判定する際に、さらに、前記携帯端末から受信した秘匿情報と予め記憶されている秘匿情報とが一致している場合に、認証成功と判定し、

前記携帯端末は、前記命令を受信すると、命令のあった前記秘匿情報を読み出して前記認証サーバに送信する、

ことを特徴とする請求項 1 から 9 のいずれかに記載の携帯端末の認証システム。

[請求項11] 前記認証サーバは、前記タイミング信号の送信時刻の後でありかつ前記返送用信号の受信の前に、電話回線を通じて前記携帯端末へ発呼し、前記携帯端末からの前記返送用信号の返信があるか否かを判定し、前記認証成功と判定する際に、さらに、前記返送用信号の返信がない場合に、認証成功と判定し、

前記携帯端末は、前記タイミング信号の受信の後に前記認証サーバからの着信を受ける、

ことを特徴とする請求項 1 から 10 のいずれかに記載の携帯端末の認証システム。

[請求項12] 認証サーバから携帯端末にタイミングを通知し、タイミングの通知

時刻を記録するタイミング通知手順と、

前記タイミング通知手順におけるタイミングの通知を契機に、携帯端末から認証サーバへ返信を行い、当該返信時刻を記録する返信手順と、

をランダムなタイミングで順に複数回繰り返し、

前記タイミング通知手順において記録した前記通知時刻の時間間隔と前記返信手順において記録した前記返信時刻の時間間隔とが略一致している場合に、認証成功と判定する認証判定手順と、

を順に有する携帯端末の認証方法。

[請求項13] 前記認証判定手順において、さらに、前記各送信時刻の時間間隔と前記各返送用信号の返信時刻の時間間隔との差が一定時間内である場合に、認証成功と判定することを特徴とする請求項12に記載の携帯端末の認証方法。

[請求項14] 前記タイミング通知手順において、認証サーバから携帯端末に向けて電話発信を行うことによってタイミングを通知し、

前記返信手順における前記契機は、認証サーバからの電話着信であり、

前記認証判定手順において、前記電話発信の時間間隔と前記返信時刻の時間間隔とが略一致している場合に、認証成功と判定する、

ことを特徴とする請求項12又は13に記載の携帯端末の認証方法。

[請求項15] 前記タイミング通知手順において、認証サーバから携帯端末に向けて電話発信の停止を行うことによってタイミングを通知し、

前記返信手順における前記契機は、認証サーバからの電話着信の停止であり、

前記認証判定手順において、前記電話発信の停止の時間間隔と前記返信時刻の時間間隔とが略一致している場合に、認証成功と判定する、

ことを特徴とする請求項 1 2 又は 1 3 に記載の携帯端末の認証方法。  
。

[請求項16] 前記タイミング通知手順において、認証サーバから携帯端末に向けて電話発信を行い、認証サーバから携帯端末に向けて電話発信の停止を行い、

前記返信手順における前記契機は、認証サーバからの電話着信又は電話着信の停止であり、

前記認証判定手順において、前記電話発信から前記電話発信の停止までの時間間隔と電話発信に対する前記返信時刻から電話発信の停止に対する前記返信時刻までの時間間隔とが略一致している場合に、認証成功と判定する、

ことを特徴とする請求項 1 2 又は 1 3 に記載の携帯端末の認証方法。  
。

[請求項17] 認証サーバから携帯端末へ認証用電話番号を通知する認証用電話番号通知手順を、前記タイミング通知手順の前にさらに有し、

前記タイミング通知手順において、前記認証用電話番号通知手順で通知した認証用電話番号を用いて認証サーバから携帯端末に向けて電話発信し、

前記返信手順において、前記認証用電話番号からの着信を契機に、携帯端末から認証サーバへ返信を行う、

ことを特徴とする請求項 1 4 から 1 6 のいずれかに記載の携帯端末の認証方法。

[請求項18] 携帯端末から認証サーバに携帯端末の識別情報を通知し、当該識別情報が認証サーバに記憶されているか否かを判定する識別情報判定手順を、前記タイミング通知手順又は前記認証用電話番号通知手順の前にさらに有し、

前記識別情報が認証サーバに記憶されている場合に、前記タイミング通知手順において、認証サーバの記憶している携帯端末の電話番号

に電話発信を行う、

ことを特徴とする請求項 1 4 から 1 7 のいずれかに記載の携帯端末の認証方法。

[請求項19]

前記タイミング通知手順において、前記返信手順から前記タイミング通知手順までの間に、ランダムに変化する任意の時間間隔を有する、

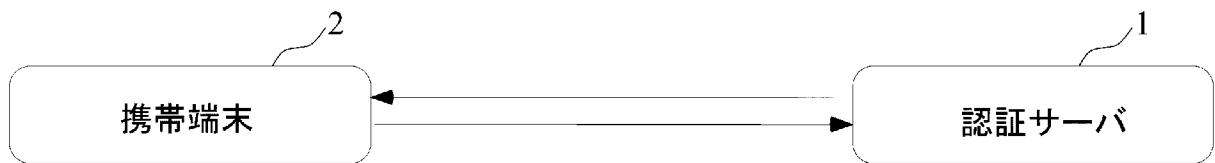
ことを特徴とする請求項 1 2 から 1 8 のいずれかに記載の携帯端末の認証方法。

[請求項20]

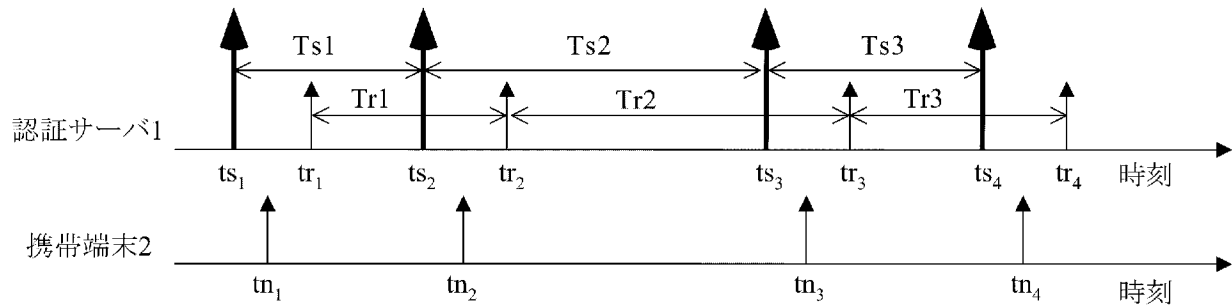
前記返信手順において、前記タイミング通知手順から前記返信手順までの間に、ランダムに変化する任意の時間間隔を有する、

ことを特徴とする請求項 1 2 から 1 8 のいずれかに記載の携帯端末の認証方法。

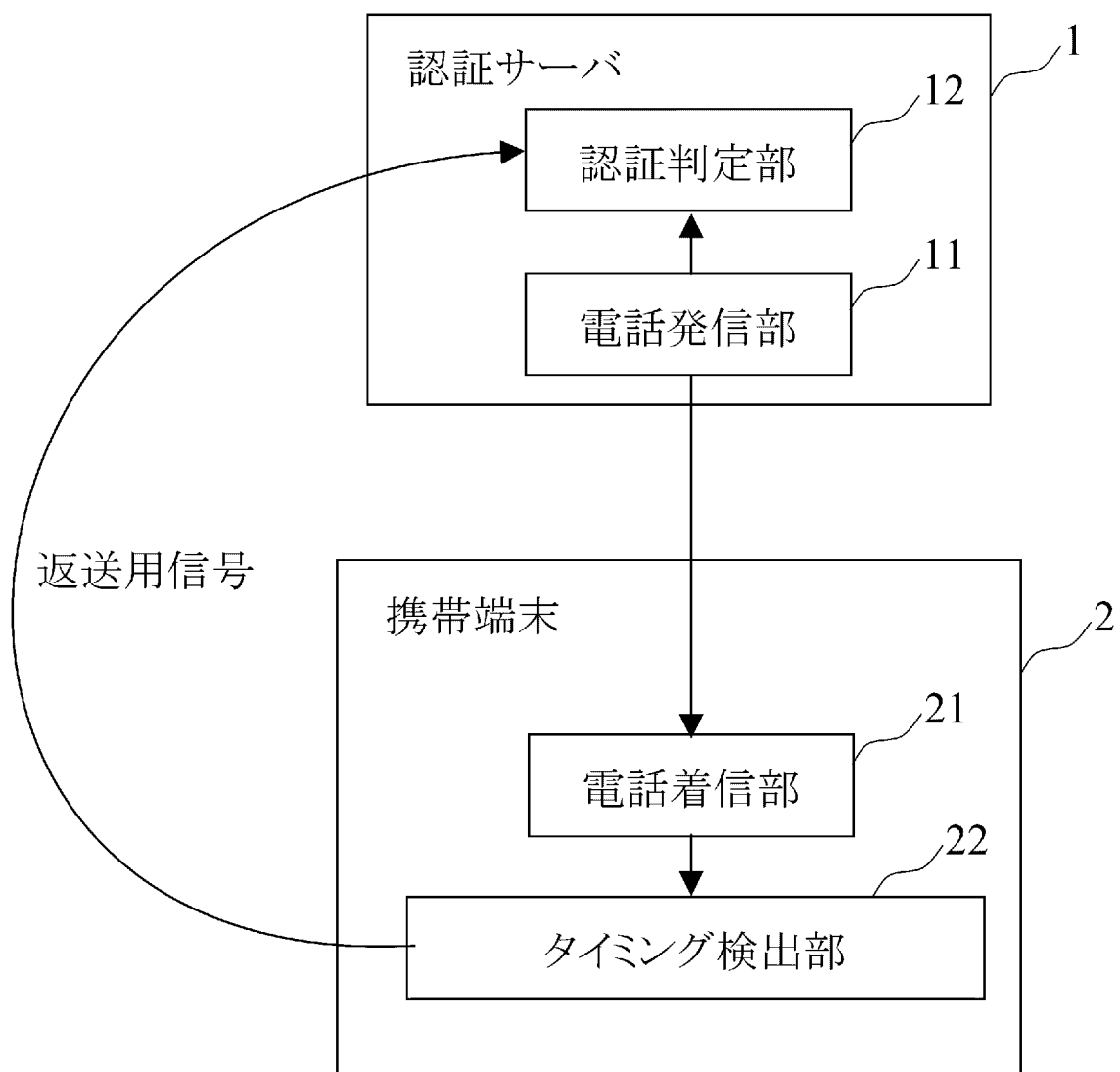
[図1]



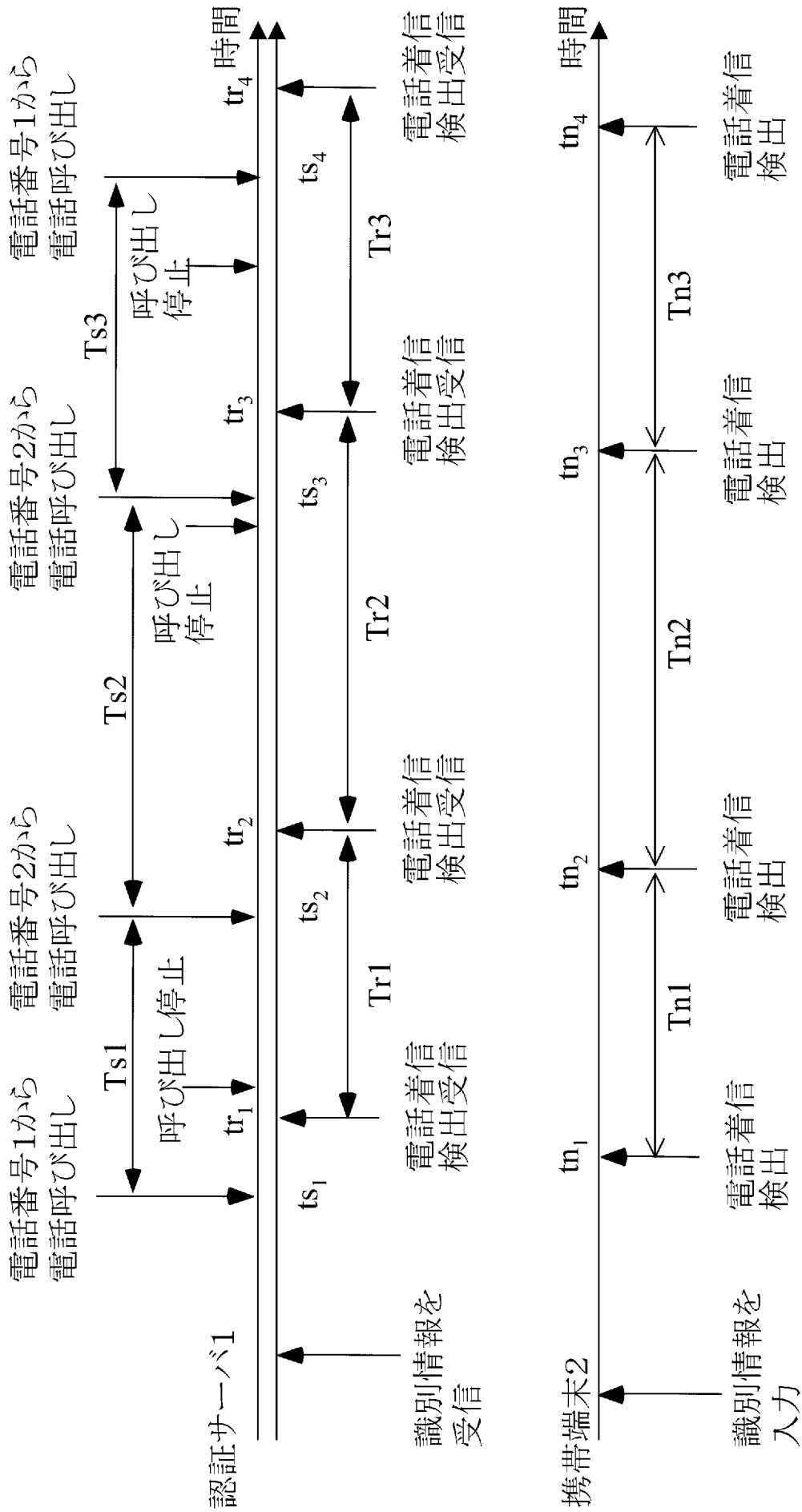
[図2]



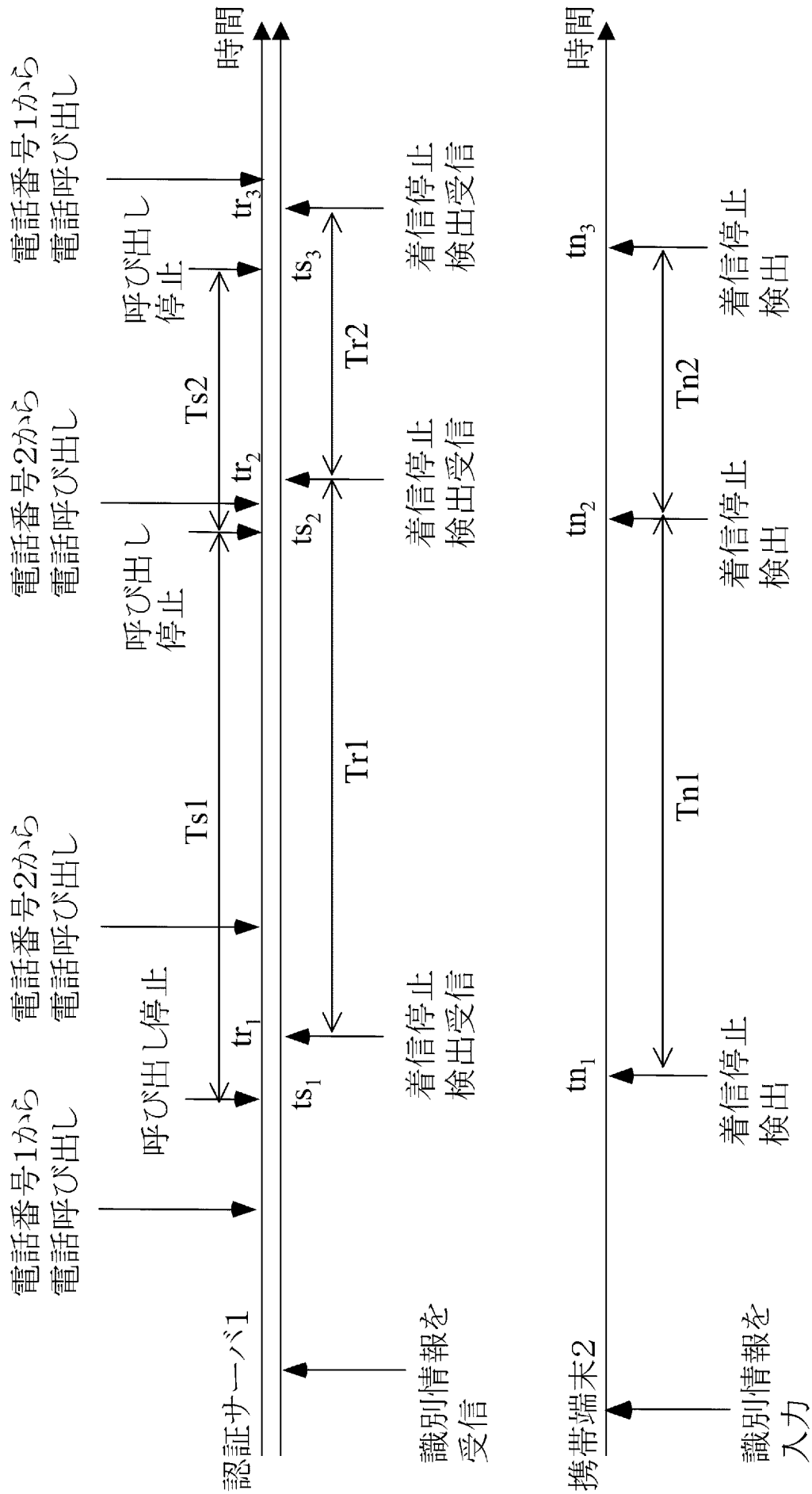
[図3]



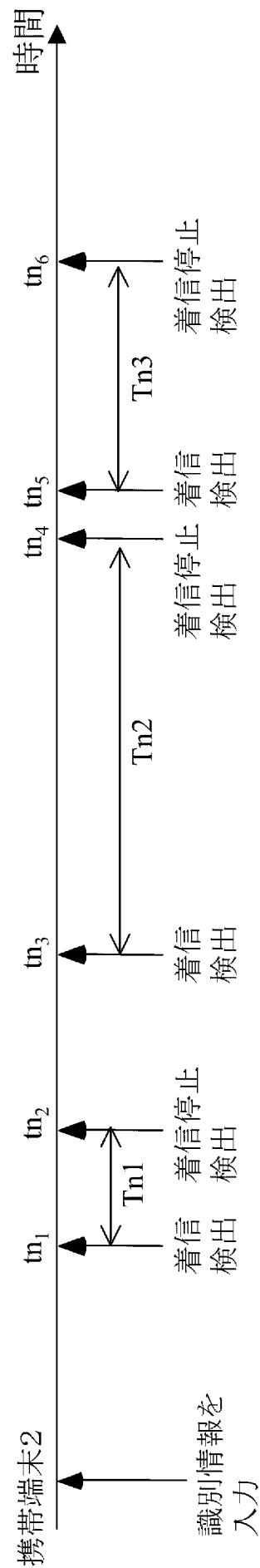
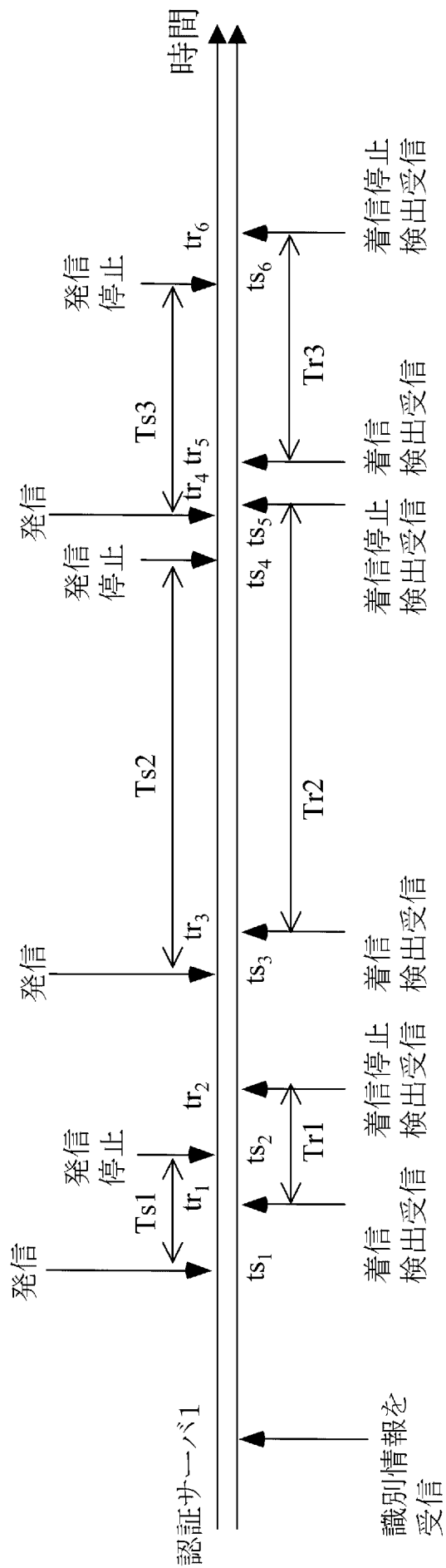
[図4]



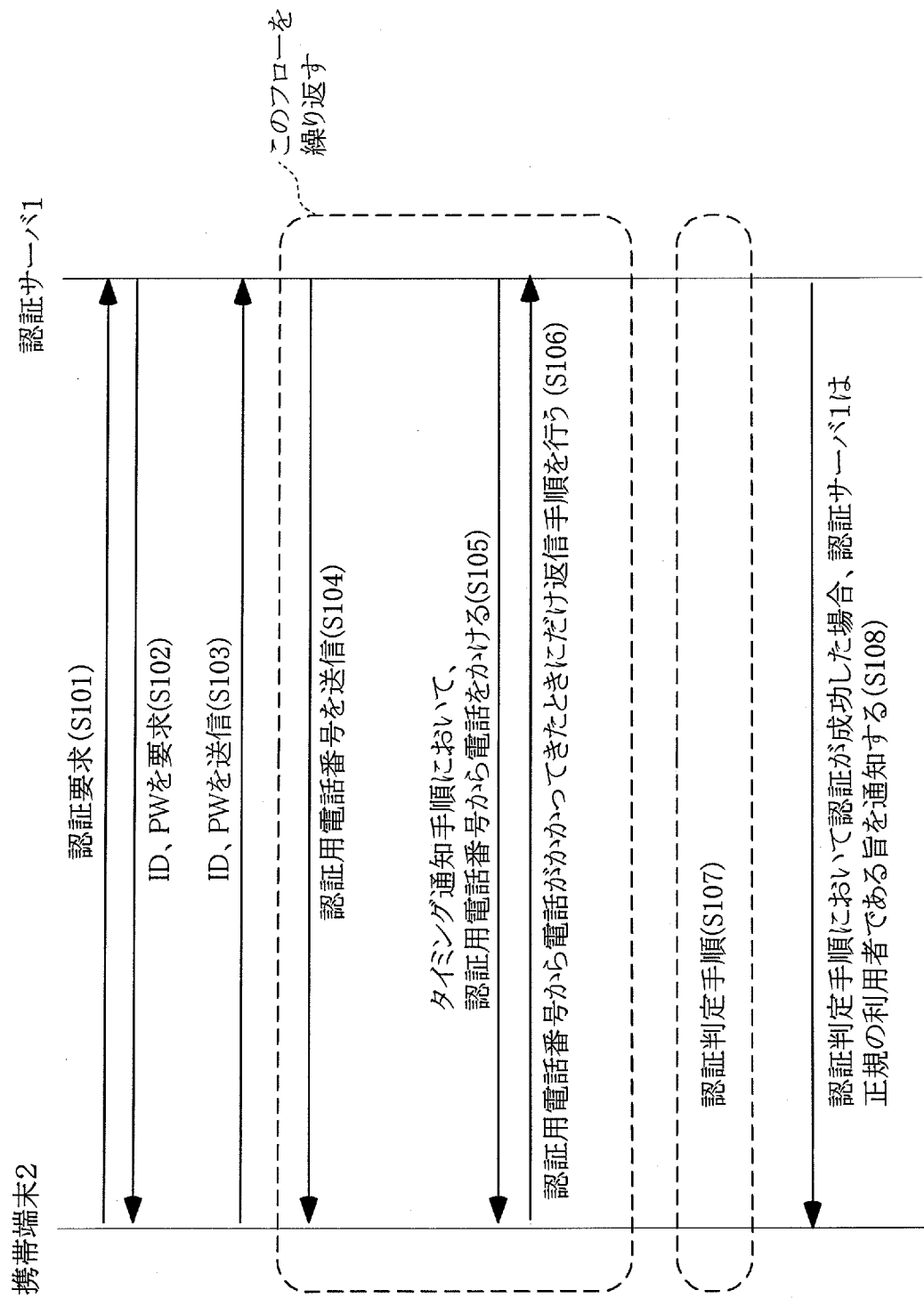
[図5]



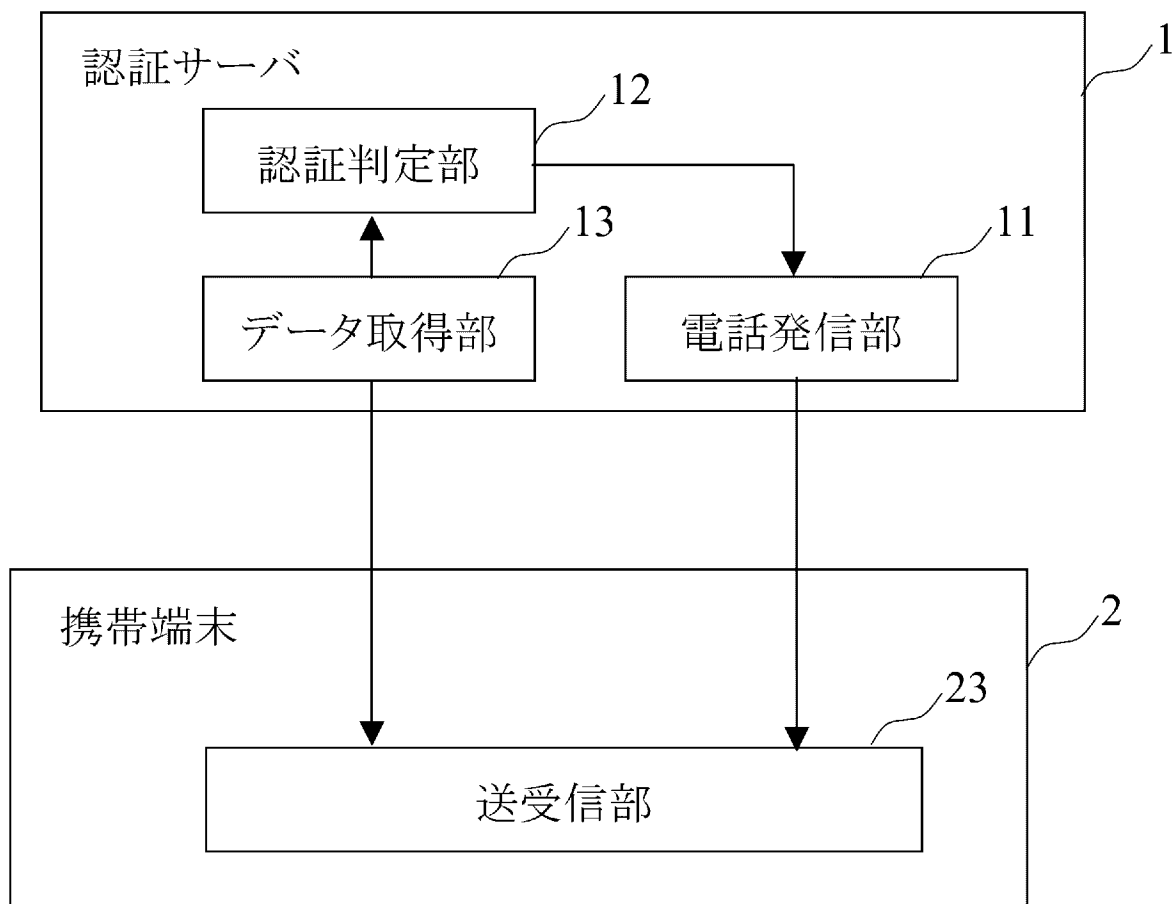
[図6]



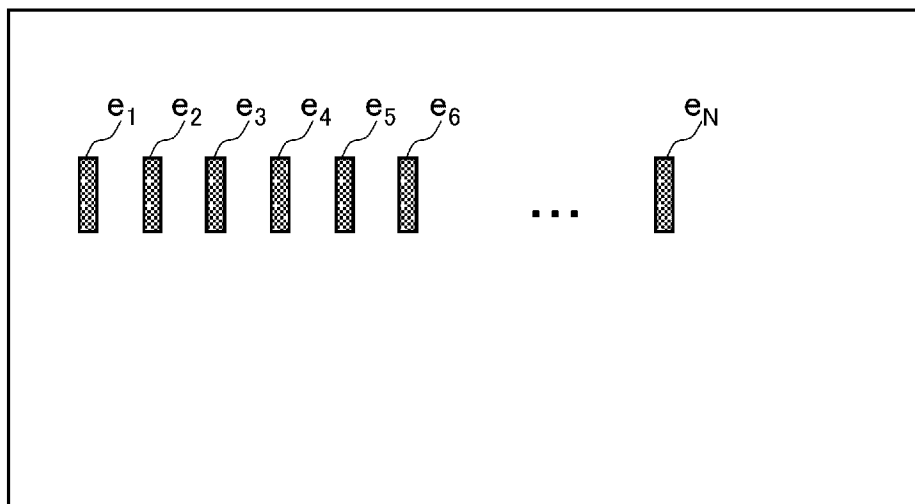
[図7]



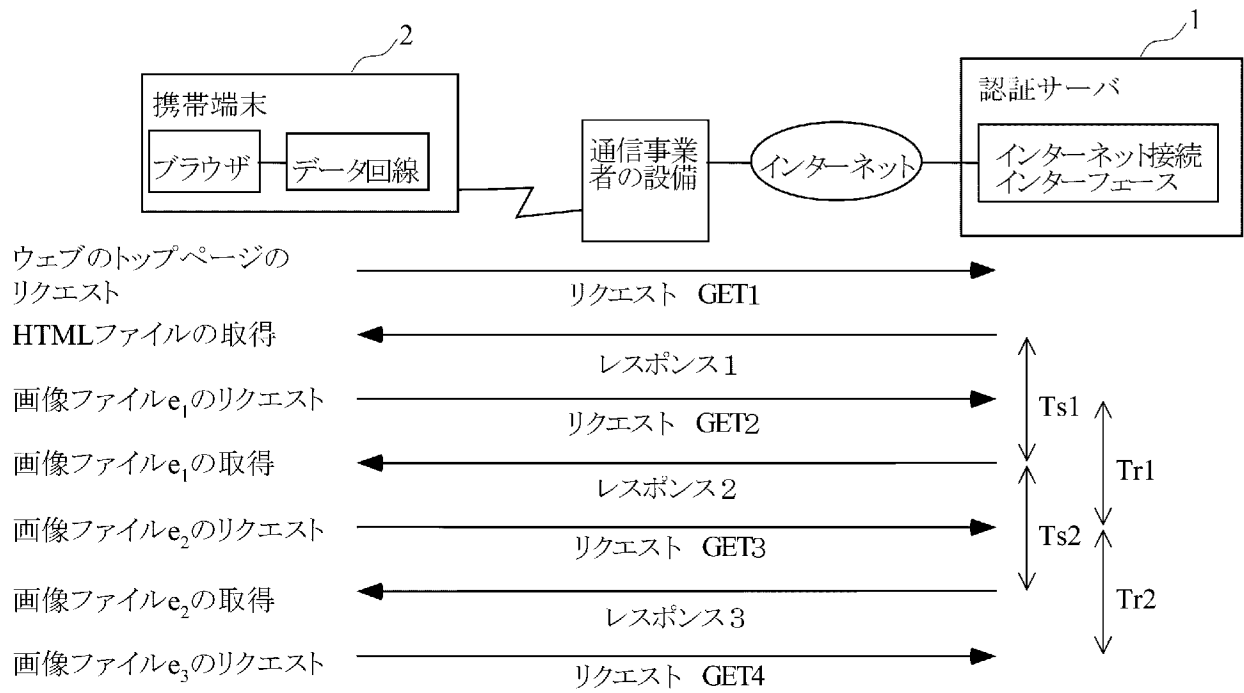
[図8]



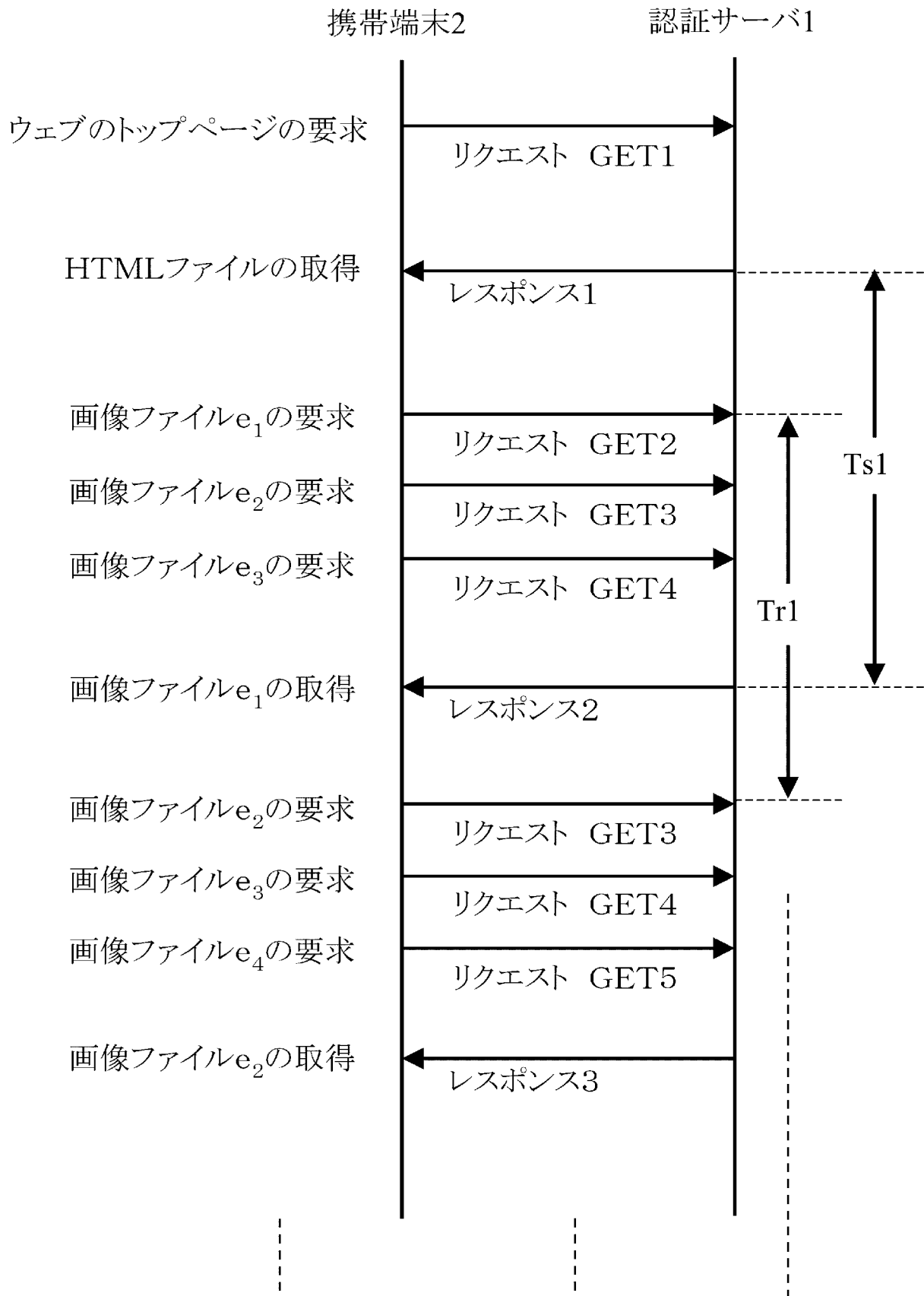
[図9]



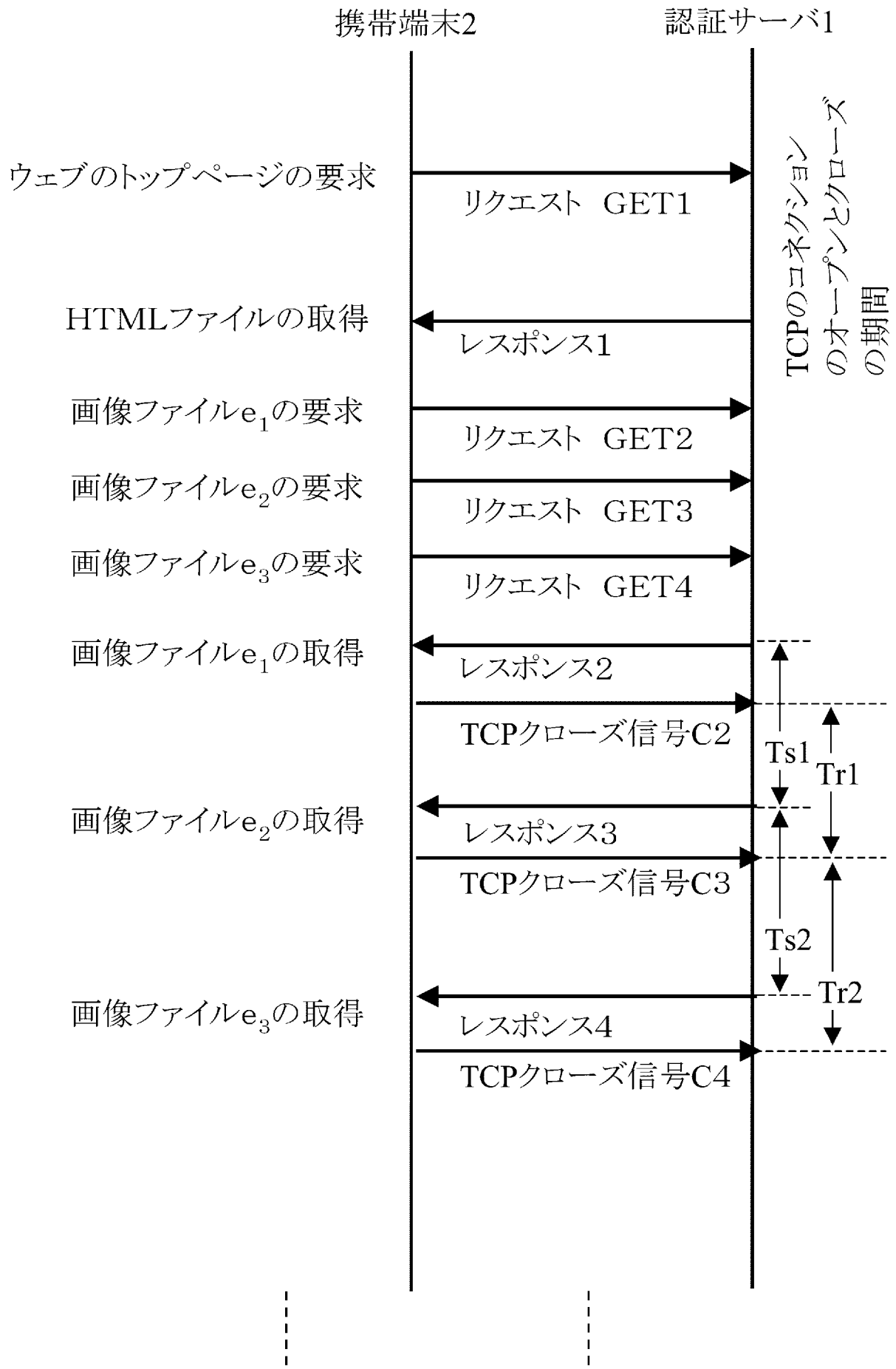
[図10]



[図11]



[図12]



# INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2011/076948

## A. CLASSIFICATION OF SUBJECT MATTER

G06F21/20 (2006.01) 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)

G06F21/20

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 2007-149026 A (NTT Docomo Inc.),<br>14 June 2007 (14.06.2007),<br>entire text; all drawings<br>(Family: none)                                | 1-20                  |
| A         | JP 2006-129083 A (Canon Inc.),<br>18 May 2006 (18.05.2006),<br>paragraph [0069]<br>& US 2008/0184345 A1 & WO 2006/046720 A1<br>& CN 101091355 A | 1-20                  |

☐ 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  
05 January, 2012 (05.01.12)

Date of mailing of the international search report  
17 January, 2012 (17.01.12)

Name and mailing address of the ISA/  
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

## A. 発明の属する分野の分類 (国際特許分類 (I P C))

Int.Cl. G06F21/20 (2006.01) 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. G06F21/20

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<br>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<br>請求項の番号 |
|-----------------|-----------------------------------------------------------------------------------------------------------------|----------------|
| A               | JP 2007-149026 A (株式会社エヌ・ティ・ティ・ドコモ)<br>2007.06.14, 全文、全図<br>(ファミリーなし)                                           | 1-20           |
| A               | JP 2006-129083 A (キヤノン株式会社)<br>2006.05.18, 段落 0069<br>& US 2008/0184345 A1 & WO 2006/046720 A1 & CN 101091355 A | 1-20           |

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

0 5 . 0 1 . 2 0 1 2

国際調査報告の発送日

1 7 . 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)

田中 慎太郎

5 S

3 2 4 4

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