(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
2010 年 10 月 21 日(21.10.2010)

PCT

(10) 国際公開番号
WO 2010/119626 A1

(51) 国際特許分類:
G06F 21/20 (2006.01) *H04L 9/32* (2006.01)

(21) 国際出願番号: PCT/JP2010/002073

(22) 国際出願日: 2010 年 3 月 24 日(24.03.2010)

(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 2009-098998 2009 年 4 月 15 日(15.04.2009) JP

(71) 出願人 (米国を除く全ての指定国について): 日本電気株式会社 (NEC Corporation) [JP/JP]; 〒1088001 東京都港区芝五丁目７番１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): 才田好則 (SAIDA, Yoshinori) [JP/JP]; 〒1088001 東京都港区芝五丁目７番１号日本電気株式会社内 Tokyo (JP).

(74) 代理人: 家入健(IEIRI, Takeshi); 〒2210835 神奈川県横浜市神奈川区鶴屋町三丁目３３番８アサヒビルヂング１０階響国際特許事務所 Kanagawa (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, RO, RS, RU, 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.

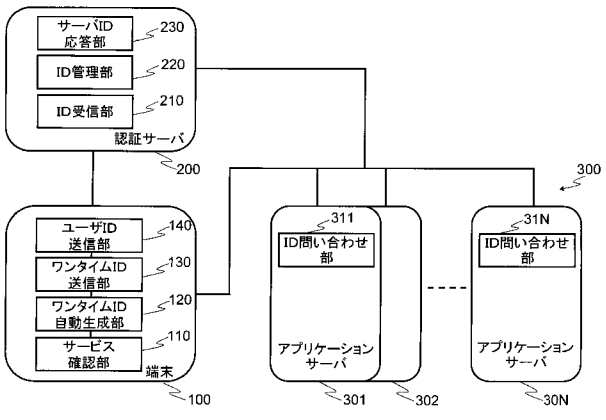
(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告（条約第 21 条(3)）

(54) **Title**: NONTEMPORARY COMPUTER-READABLE MEDIUM WHEREIN ID AUTHENTICATION SYSTEM, AND METHOD AND PROGRAM THEREOF ARE STORED

(54) 発明の名称 : ＩＤ認証システム、方法及びプログラムが格納された非一時的なコンピュータ可読媒体

[図1]



100 TERMINAL
110 UNIT FOR CONFIRMING THE SERVICES
120 AUTOMATIC ONE-TIME-ID GENERATING UNIT
130 ONE-TIME-ID TRANSMITTING UNIT
140 USER ID TRANSMITTING UNIT
200 AUTHENTICATION SERVER
210 ID RECEIVING UNIT
220 ID MANAGEMENT UNIT
230 UNIT FOR RESPONDING TO SERVERS WITH IDs
301/30N APPLICATION SERVER
311/31N UNIT FOR INQUIRING ABOUT IDs

(57) **Abstract**: Provided is an ID authentication system, wherein specifying and tracking of a terminal, spanning across multiple service providers, are prevented, when a user is utilizing multiple services. Provided in the ID authentication system is a terminal device, a service providing device, and authentication servers. The terminal device (100) is provided with; an automatic one-time-ID generating unit (120) that generates one-time IDs automatically; a one-time-ID transmitting unit (130) that transmits the one-time-IDs to the service providing devices; and a user ID transmitting unit (140) that transmits the one-time IDs and IDs for identifying the users uniquely, to the authentication server. The authentication server (200) is provided with an authentication information management unit (220) that stores the users' authentication information regarding the multiple service providing devices. The authentication server (200) transmits, to the service providing devices (300), authentication information regarding users capable of one-time IDs, for logging-in to the service providing devices (300).

(57) 要約:

[続葉有]

WO 2010/119626 A1

ユーザが複数のサービスを利用している場合に、複数のサービス提供者にまたがっての端末の特定、追跡を防止する。本発明にかかるＩＤ認証システムは端末装置と、サービス提供装置と、認証サーバとを備えるＩＤ認証システムである。端末装置１００は、ワンタイムＩＤを生成するワンタイムＩＤ自動生成部１２０と、サービス提供装置に当該ワンタイムＩＤを送信するワンタイムＩＤ送信部１３０と、認証サーバに対して、当該ワンタイムＩＤと、ユーザを一意に識別するためのＩＤとを送信するユーザＩＤ送信部１４０を備える。認証サーバ２００は、複数のサービス提供装置に対するユーザの認証情報を記憶する認証情報管理部２２０を備える。認証サーバ２００は、ワンタイムＩＤに対応する当該ユーザがサービス提供装置３００にログインするための認証情報をサービス提供装置３００に送信する。

明　細　書

発明の名称 ：

ＩＤ認証システム、方法及びプログラムが格納された非一時的なコンピュータ可読媒体

技術分野

[0001] 本発明はＩＤ認証システム、ＩＤ認証方法、ＩＤ認証プログラムが格納された非一時的なコンピュータ可読媒体に関し、特に複数のサービス提供装置に対する認証にかかるＩＤ認証システム、ＩＤ認証方法、ＩＤ認証プログラムが格納された非一時的なコンピュータ可読媒体に関する。

背景技術

[0002] ＰＣ（Personal Computer）や携帯電話といった端末から、ネットワークで接続されたサーバ上で提供されるサービスを利用する場合には、通常、ユーザを識別するためのＩＤおよびパスワードを用いてサービスにログインする。そのことにより、利用しようとしているユーザがサービス側に識別され、ユーザは、ユーザとサービス提供者との契約に応じたサービスを利用することが可能となる。

[0003] ユーザが複数のサーバ上でそれぞれ提供されるサービスを利用する場合には、通常はサービスごとに異なるＩＤとパスワードを用いてログインすることになる。ただしその場合、ログイン手続が煩雑になるため、シングルサインオンと呼ばれる仕組みが利用されることがある。シングルサインオンとは、ある一つのＩＤとパスワードを用いて一度サービスにログインすることにより、他のサービスへは再度のＩＤ及びパスワードの入力手続なしにログインできる仕組みである。このシングルサインオンの仕組みは、ユーザの識別情報が、最初にログインしたサービスと、次にログインするサービスとで共有されることで実現されている。

[0004] 各サービス提供者は各ユーザに対応するユーザ情報を保有する。ここで、ユーザ情報とは、ユーザがサービス提供者と契約した際に登録された、サー

ビスの利用コース等の契約情報、ユーザの氏名、住所、電話番号等の個人情報及び、サービス側でユーザを識別するための識別子等を含む情報である。サービス提供者はこれらのユーザ情報と、ユーザのＩＤ及びパスワードを互いに関連付けて管理している。以下、シングルサインオンに関連する技術を開示した例を挙げる。

[0005] 特許文献１に記載の認証システムは、利用者端末を識別するための識別情報を利用者端末が保持し、認証サーバがログイン認証済みの利用者端末の識別情報を格納するサインオン管理テーブルを備えるように構成されている。利用者端末からアプリケーションサーバにログイン要求があった場合には、アプリケーションサーバは利用者端末から送信された識別情報を基に、サインオン管理テーブルに当該利用者端末の識別情報が含まれているか否かを判定する。アプリケーションサーバは、当該識別情報が含まれている場合にはログイン認証成功とし、含まれていない場合にはログイン認証情報を利用者端末から取得するように動作する。このような処理により、特許文献１に記載の認証システムにおいてシングルサインオンを実現している。

[0006] 特許文献２に記載の認証システムは、複数のアプリケーションサーバに接続されたログイン代行システムであり、ログイン代行サーバと、認証サーバと、ログインテンプレートテーブル、ＵＲＬ変換テーブルからなるＤＢサーバとから構成されている。利用者は、あらかじめログイン代行システム内の認証サーバへのログインを行っておく。その後、利用者端末からユーザがアプリケーションサーバにログインする場合には、ログイン代行サーバが利用者端末から送信されるユーザのアプリケーションサーバへのログイン要求に応答して、当該ユーザの当該アプリケーションサーバに対するログイン認証情報を含む要求を、ＤＢサーバ及び認証サーバの認証情報を利用して生成し、当該ユーザに代わってアプリケーションサーバにログインする。アプリケーションサーバから返信されるレスポンスに対しては、その内容を当該利用者端末が当該アプリケーションサーバから直接受け取った場合と同様に機能するようにＤＢサーバを用いて変換し、当該利用者端末へと返信する。この

ような処理によって、特許文献２に記載の認証システムにおいてシングルサインオンを実現している。

先行技術文献

特許文献

[0007] 特許文献1：特開２００５－２６７５２９号公報

特許文献2：特開２００２－３３４０５６号公報

発明の概要

発明が解決しようとする課題

[0008] 本発明が解決しようとする課題は、特に特許文献１における問題点であるが、端末が一意な識別情報を複数のサービス提供装置（たとえばアプリケーションサーバ）に送信することに起因する問題が挙げられる。すなわち、ユーザが端末を通して複数のサービスを利用している場合に、単一のサービス提供者内において端末及びそれを利用しているユーザの特定が可能であるだけでなく、複数のサービス提供者にまたがって端末及びユーザの特定及び追跡が可能になる点である。

[0009] 具体的には、あるユーザがアプリケーションサーバＡ上のサービスを利用し、年齢、氏名、住所等の個人情報を入力したとする。その場合、特許文献１ではユーザの識別情報がアプリケーションサーバＡに送付されるため、アプリケーションサーバＡを管理するサービス提供者ａは、ユーザの識別情報と、ユーザの個人情報を関連づけて把握することが可能である。

[0010] 次にユーザがアプリケーションサーバＢやＣ上のサービスを利用し、それらで物品の購入をしたとする。この場合、アプリケーションサーバＢ及びＣを管理するサービス提供者ｂ及びｃは、ユーザの識別情報（これはアプリケーションサーバＡに送付されたものと同一である）と、ユーザの購入履歴を関連づけて把握することが可能である。

[0011] ここで、サービス提供者ｂ及びｃと、サービス提供者ａがお互いの情報を交換することにより、共通する識別情報を用いてユーザの個人情報と購入情

報等の履歴情報を結びつけて把握することが可能となり、ユーザのプライバシ保護の観点から問題である。

[0012] 本発明は、このような問題点を解決するためになされたものであり、複数のサービス提供装置間でのユーザの識別の防止、及びユーザの行動履歴情報等の共有を防止したシングルサインオンを実現することができるＩＤ認証システム、ＩＤ認証方法、及びＩＤ認証プログラムが格納された非一時的なコンピュータ可読媒体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

[0013] 本発明にかかるＩＤ認証システムの一態様は端末装置と、複数のサービス提供装置と、認証サーバとを備え、

前記端末装置は、

一時的に使用されるワンタイムＩＤを生成するワンタイムＩＤ生成手段と、

前記ワンタイムＩＤ生成手段により生成されたワンタイムＩＤを前記サービス提供装置に対して送信するワンタイムＩＤ送信手段と、

前記ワンタイムＩＤ送信手段により送信したワンタイムＩＤと、ユーザを一意に識別するユーザＩＤとを前記認証サーバに対して、送信するユーザＩＤ送信手段を有し、

前記サービス提供装置は、

前記端末装置から送信されたワンタイムＩＤを受信し、前記認証サーバに対して、受信したワンタイムＩＤに対応する認証情報を問い合わせるＩＤ問い合わせ手段を有し、

前記認証サーバは、

ユーザＩＤと、前記サービス提供装置において認証するための認証情報を互いに関連付けて記憶する認証情報管理手段と、

前記端末装置から送信された前記ワンタイムＩＤとユーザＩＤとを受信するＩＤ受信手段と、

前記サービス提供装置からの問い合わせに含まれるワンタイムＩＤに対応

する当該ユーザＩＤを、前記ＩＤ受信手段により受信された前記ワンタイムＩＤとユーザＩＤより取得し、さらに取得したユーザＩＤに基づいて前記認証情報管理手段において当該ユーザＩＤと関連づけられた認証情報を取得して、当該サービス提供装置に送信するサーバＩＤ応答手段を備えるものである。

[0014] 本発明にかかるＩＤ認証方法は、

端末装置においてワンタイムＩＤを生成し、

前記端末装置からサービス提供装置に対して前記ワンタイムＩＤを送信し、

前記端末装置から認証サーバに対して前記ワンタイムＩＤと、ユーザを一意に識別するためのユーザＩＤとを送信し、

前記サービス提供装置が、前記端末装置からワンタイムＩＤを受信し、そのワンタイムＩＤに基づいて前記認証サーバに一時的ＩＤに対応する認証情報を問い合わせる処理を実行し、

前記認証サーバが、前記端末装置から前記ワンタイムＩＤと前記ユーザＩＤとを受信し、

前記認証サーバが、前記サービス提供装置からの問い合わせに含まれるワンタイムＩＤに対応するユーザＩＤを取得し、さらに当該ユーザＩＤに対応する認証情報を取得して、当該サービス提供装置にその認証情報を送信するものである。

[0015] 本発明にかかるＩＤ認証プログラムが格納された非一時的なコンピュータ可読媒体は、

ユーザがサービス提供装置にログインするための認証を実行するＩＤ認証プログラムが格納された非一時的なコンピュータ可読媒体であって、

端末装置から送信されたワンタイムＩＤとユーザＩＤとを取得し、

前記端末装置から前記ワンタイムＩＤを受信したサービス提供装置からの問い合わせに含まれるワンタイムＩＤに対応するユーザＩＤを取得し、さらに当該ユーザＩＤに対応する認証情報を取得して、当該サービス提供装置に

する認証情報を送信し処理実行させる処理を認証サーバに対して実行させるものである。

発明の効果

[0016] 本発明により、複数のサービス提供装置間でのユーザの識別の防止、及びユーザの行動履歴情報等の共有を防止したシングルサインオンを実現できる。

図面の簡単な説明

[0017] [図1]実施の形態１にかかるＩＤ認証システムの構成図である。

[図2]実施の形態１にかかるＩＤ認証システムの処理を示すフローチャート図である。

[図3]実施の形態１にかかるＩＤ認証システムの処理を示すシーケンス図である。

[図4]実施の形態１にかかるワンタイムＩＤと端末ユーザＩＤの管理テーブルの図である。

[図5]実施の形態１にかかる端末ユーザＩＤとサーバユーザＩＤ、パスワードの管理テーブルの図である。

[図6]実施の形態２にかかるＩＤ認証システムの構成図である。

発明を実施するための形態

[0018] 実施の形態１

以下、図面を参照して本発明の実施の形態について説明する。

まず、図１を用いて、本発明の実施の形態１にかかるＩＤ認証システムの構成について説明する。このＩＤ認証システムは、図１に示されるように、端末１００、認証サーバ２００、複数のアプリケーションサーバ群３００（３０１～３０Ｎ）を備えている。これらは、ネットワークに接続され、相互に通信を行うことができる。

[0019] 上述の実施の形態では、端末１００、認証サーバ２００、複数のアプリケーションサーバ群３００をハードウェアの構成として説明したが、本発明は、これに限定されるものではない。本発明は、任意の処理を、ＣＰＵ（Centr

al Processing Unit）にコンピュータプログラムを実行させることにより実現することも可能である。この場合、コンピュータプログラムは、記録媒体に記録して提供することも可能であり、また、インターネットその他の通信媒体を介して伝送することにより提供することも可能である。また、非一時的なコンピュータ可読媒体には、例えば、フレキシブルディスク、ハードディスク、磁気ディスク、光磁気ディスク、ＣＤ－ＲＯＭ、ＤＶＤ、ＲＯＭカートリッジ、バッテリバックアップ付きＲＡＭメモリカートリッジ、フラッシュメモリカートリッジ、不揮発性ＲＡＭカートリッジ等が含まれる。また、通信媒体には、電話回線等の有線通信媒体、マイクロ波回線等の無線通信媒体等が含まれる。

[0020] 端末１００は、ＰＣ（Personal Computer）や携帯電話、ＰＤＡ(Personal Digital Assistant)などが該当する。アプリケーションサーバ群３００は、サービス提供装置の一例として例示したものであり、ネットワーク接続された何らかのサービスを提供する装置であればよい。

[0021] 端末１００はサービス確認部１１０と、ワンタイムＩＤ自動生成部１２０と、ワンタイムＩＤ送信部１３０と、ユーザＩＤ送信部１４０を備えている。認証サーバ２００は、ＩＤ受信部２１０と、ＩＤ管理部２２０と、サーバＩＤ応答部２３０とを含む。アプリケーションサーバ群３００は、ＩＤ問い合わせ部３１０（３１１～３１Ｎ）をそれぞれのアプリケーションサーバ上に含む。

[0022] サービス確認部１１０は、今回接続したアプリケーションサーバ及びその上で提供されるサービスが本ＩＤ認証システムに対応しているかどうかを確認する。なお、認証サーバ２００に接続するアプリケーションサーバ群３００全てが本ＩＤ認証システムに対応している状況下では、本処理部は必須の構成要件ではない。

[0023] ワンタイムＩＤ自動生成部１２０は、今回の接続用に、一時的な仮のＩＤであるワンタイムＩＤを生成する。ワンタイムＩＤ自動生成部１２０は接続毎に異なるワンタイムＩＤを生成する。

[0024] ワンタイムＩＤ送信部１３０は、今回の接続用に生成されたワンタイムＩＤを、今回接続しているアプリケーションサーバ３００に送信する。ユーザＩＤ送信部１４０は、ワンタイムＩＤと、認証サーバが当該ユーザを認識するために事前に発行していた端末ユーザＩＤを認証サーバ２００に送信する。この端末ユーザＩＤはユーザを一意に識別する識別情報であるが、ユーザ個人のみならず、グループを識別する識別情報も含む概念である。

[0025] ＩＤ受信部２１０は、端末１００から送信されたワンタイムＩＤ及び端末ユーザＩＤを受信し、それらの組を管理するテーブルに保存する。

[0026] ＩＤ管理部２２０は、認証サーバ２００が管理しているユーザ毎に、その端末ユーザＩＤと、当該ユーザの各アプリケーションサーバ３００の認証情報をテーブルで管理する認証情報管理部である。ここで、認証情報は各アプリケーションサーバ３００にログインするためのパスワードや身分情報等である。

[0027] サーバＩＤ応答部２３０は、アプリケーションサーバ３００から上述のワンタイムＩＤによる問い合わせを受信し、ＩＤ受信部２１０で管理しているワンタイムＩＤと端末ユーザＩＤの組から該当するワンタイムＩＤを検索し、組となっている端末ユーザＩＤを得る。その後、サーバＩＤ応答部２３０は、ＩＤ管理部２２０によって管理されている端末ユーザＩＤと、各アプリケーションサーバ３００のサーバユーザＩＤ及びパスワードの組の中から、問い合わせのあったアプリケーションサーバ及び、当該端末ユーザＩＤに対応した、サーバユーザＩＤとパスワードを取得し、それらをアプリケーションサーバ３００に返信する。

[0028] ＩＤ問い合わせ部３１０は、端末から送信されたワンタイムＩＤを受信し、そのワンタイムＩＤを使って認証サーバに該当ユーザの認証情報を問い合わせ、返答として当該ユーザのサーバユーザＩＤおよびパスワードを受信し、当該ユーザのログイン処理を実施する。

[0029] 続いて、図１及び、図２のフローチャート、図３のシーケンス図を参照して本発明の実施形態1にかかるＩＤ認証システムの処理について説明する。

[0030] ユーザが端末１００を用いて、複数のアプリケーションサーバ群３００上で提供される複数のサービスのうち、アプリケーションサーバ３０１上のサービスを利用する場合、本システムは次のような手順で動作する。

[0031] 端末１００がアプリケーションサーバ３０１上とネットワーク接続される（図２及び図３のステップＡ１）。接続方式としては、一例として、ＨＴＴＰ(HyperText Transfer Protocol)や、ＨＴＴＰＳ(HyperText Transfer Protocol Security)といったプロトコルを利用して接続することが想定される。

[0032] その場合、端末上のサービス確認部１１０は、接続されたサーバ及びサービスが、本発明のＩＤ認証システムに対応しているかどうかを判定する（図２及び図３のステップＡ２）。

[0033] この判定手順の一例としては、本システムに対応しているサーバ及びサービスのＵＲＬ(Uniform Resource Locator)やＩＰ(Internet Protocol)アドレス、及び接続時のポート番号等のリストを端末に保存しておき、そのリストと、今回接続したサーバ及びサービスの当該情報と比較してリストに含まれるかどうかを判定するというやり方が考えられる。

[0034] また他の例としては、ＨＴＴＰＳ接続時に行われるサーバのデジタル証明書の認証処理を利用するやり方が考えられる。具体的には、本発明の実施の形態にかかるＩＤ認証システムに対応したサーバ及びサービスの場合は、サーバのデジタル証明書内の特定のフィールドに、本システムに対応している識別子として特定の文字列をあらかじめ埋め込んでおき、接続したサーバから送信されたこのサーバのデジタル証明書を端末上で認証する場合に、その識別子が含まれているかどうかを判定するという方法が考えられる。

[0035] 他にもサーバのデジタル証明書の認証処理を利用した判定方法としては、本発明の実施の形態にかかるＩＤ認証システムに対応したサーバ及びサービスの場合は、サーバのデジタル証明書を発行する認証局を特定の認証局に限定するという方法がある。これによって、接続したサーバから送信されたデジタル証明書を端末上で認証する場合に、この特定の認証局によって発行された証明書であれば、本システムに対応していると判定することができる。

[0036] 本システムに対応していないサーバ及びサービスの場合は、本システムの認証機能は利用できない。しかし、端末上のユーザインタフェイスを通して当該サーバ及びサービス用のユーザＩＤ及びパスワードを入力する、通常のログイン方式にてサービスを利用することは可能である（図２のステップＡ３a）。一方、本システムに対応しているサーバ及びサービスであると判定された場合は、以降の手順で本システムのシングルサインオン処理を開始する（図２及び図３のステップＡ３b）。

[0037] サービス確認部１１０により接続されたサーバ及びサービスが本システムに対応していると判定された場合、ワンタイムＩＤ自動生成部１２０は今回のサーバ及びサービス接続用のワンタイムＩＤを新たに生成する(図２及び図３のステップＡ４)。

[0038] ワンタイムＩＤは、同一端末での複数回に渡るワンタイムＩＤの生成及び、他の端末におけるワンタイムＩＤと偶然同じものを生成しないように、十分な桁数を持ったＩＤにすることが望ましい。また必要に応じてＩＤの有効期限を設定することで、同じワンタイムＩＤが生成される可能性を減らすことも可能である。さらに、このワンタイムＩＤには、以降で述べるワンタイムＩＤの問い合わせ手順において必要な認証サーバ２００のアドレスが埋め込まれていてもよい。

[0039] ワンタイムＩＤの例として、「a323912z9dw0afcdsl@authentication.server.co.jp」のような形式が挙げられる。区切り文字として使用した「@」の前半部分「a323912z9dw0afcdsl」が、自動で生成されたランダムな文字列であり、「@」の後半部分「authentication.server.co.jp」が、このワンタイムＩＤを問い合わせる認証サーバのアドレスとなる。ここではワンタイムＩＤに認証サーバのアドレスを埋め込む実装例を示したが、認証サーバのアドレスはワンタイムＩＤに含めずに、別途送信するように実装してもよい。

[0040] 次にユーザＩＤ送信部１４０は、ステップＡ４で生成されたワンタイムＩＤと、認証サーバ２００が端末ユーザを認識するために事前に発行していた端末ユーザＩＤを認証サーバ２００に送信する(図２及び図３のステップＡ５

)。ここでは、ユーザＩＤ送信部１４０は、ワンタイムＩＤとして「a323912z9dw0afcdsl」、端末ユーザＩＤとして「user001」を認証サーバ２００に送信するものとする。

[0041] 端末ユーザは、認証サーバ２００に対して事前にユーザ登録を行い、認証サーバ２００が端末１００及び端末１００を利用しているユーザを認識するための端末ユーザＩＤを発行してもらっておく必要がある。さらに当該ユーザＩＤを端末１００上の端末ユーザＩＤ送信部に予め登録しておくことで、ユーザがユーザＩＤをこのステップＡ５において入力する手間が省け、自動で一連の処理を実行することが可能となる。また端末ユーザＩＤと同時に、パスワードも設定し、認証サーバ２００に送付してもよい。

[0042] 次に、端末１００上のワンタイムＩＤ送信部１３０は、ステップＡ４で生成されたワンタイムＩＤをアプリケーションサーバ３０１に送信する(図２及び図３のステップＡ６)。ここでは、ワンタイムＩＤ送信部１３０はワンタイムＩＤとして「a323912z9dw0afcdsl」をアプリケーションサーバ３０１に送信するものとする。

[0043] 端末１００からステップＡ５で認証サーバ２００に送信されたワンタイムＩＤ及び端末ユーザＩＤは、認証サーバ上のＩＤ受信部２１０によって受信され、ワンタイムＩＤとユーザＩＤが組としてＩＤ受信部２１０が管理するテーブルに保存される(図２及び図３のステップＡ７)。ここでは、ＩＤ受信部２１０は図４に示すように、ワンタイムＩＤ「a323912z9dw0afcdsl」と端末ユーザＩＤ「user001」の組をテーブルに格納し、管理する。本実施形態では、ワンタイムＩＤと端末ユーザＩＤをデータベースのテーブルで管理する例を示したが、サーバ内の主記憶装置等で管理してもよい。

[0044] なお、ユーザＩＤ送信部１４０による認証サーバ２００に対する処理(図２及び図３のステップＡ５、Ａ７)とワンタイムＩＤ送信部１３０によるアプリケーションサーバに対する処理(図２及び図３のステップＡ６)の処理順序はどちらが先でも構わず、同時に行われてもよい。

[0045] 端末１００からステップＡ６でアプリケーションサーバ３０１に送信され

たワンタイムＩＤは、アプリケーションサーバ３０１上のＩＤ問い合わせ部３１１によって受信され、このワンタイムＩＤを基に認証サーバ２００に対して現在接続中の端末ユーザの認証情報を問い合わせる（図２及び図３のステップＡ８）。ここでは、ＩＤ問い合わせ部３１１は、ワンタイムＩＤ「a323912z9dw0afcdsl」を基に認証サーバ２００に対して端末ユーザの認証情報を問い合わせるものとする。

[0046] ワンタイムＩＤ内に認証サーバのアドレスが埋め込まれている場合は、ＩＤ問い合わせ部３１１は、このアドレスが表す認証サーバに対して問い合わせを行う。一方ワンタイムＩＤと別に端末１００から認証サーバのアドレスが送信された場合は、そのアドレスを用いる。これらの方法を用いた、端末１００からの認証サーバの指定がない場合は、アプリケーションサーバ３０１は事前に既知の認証サーバのアドレスのリストを備えておき、これを用いてＩＤの問い合わせを行ってもよい。

[0047] 認証サーバ上のサーバＩＤ応答部２３０は、アプリケーションサーバ３０１からの、ワンタイムＩＤによる認証情報問い合わせを受信すると、ＩＤ受信部２１０が管理するワンタイムＩＤとユーザＩＤの組から該当するワンタイムＩＤを検索し、組となっている端末ユーザＩＤを取得する（図２及び図３のステップＡ９）。ここで、サーバＩＤ応答部２３０はワンタイムＩＤとして「a323912z9dw0afcdsl」を受信した場合、ワンタイムＩＤと端末ユーザＩＤが格納されたテーブル（図４）を検索し、端末ユーザＩＤとして「user001」を取得する。

[0048] 引き続きサーバＩＤ応答部２３０は、ＩＤ管理部２２０によって管理されている端末ユーザＩＤと、各アプリケーションサーバのサーバユーザＩＤ及びパスワードの組の中から、問い合わせのあったアプリケーションサーバ３０１及び、当該端末ユーザＩＤに対応した、サーバユーザＩＤとパスワードを取得し、それらをアプリケーションサーバ３０１に返信する（図２及び図３のステップＡ１０）。ここでは、アプリケーションサーバ３０１が「http://abcde.com」というアドレスを持つサーバであった場合、ＩＤ応答部２３０

は問い合わせに対し、ＩＤ管理部２２０が管理するテーブル（図５）から端末ユーザＩＤ「user001」に対応するサーバユーザＩＤ「yamada-taro」とパスワード「Xed241w」を取得する。その後、ＩＤ応答部２３０はアプリケーションサーバ３０１にサーバユーザＩＤ「yamada-taro」とパスワード「Xed241w」を送信する。

[0049] 認証サーバ上のＩＤ管理部２２０は、認証サーバが管理している端末ユーザ毎に端末ユーザＩＤと関連付けて、当該ユーザが各アプリケーションサーバ上のサービスにログインするためのサーバユーザＩＤとパスワードとの組を管理している（図５）。なお、これらの情報をデータベースのテーブルで管理する例を示したが、サーバ内の主記憶装置等で管理してもよい。このサーバユーザＩＤとパスワードの組は、アプリケーションサーバ毎に異なっており、これらは端末ユーザが事前に各アプリケーションサーバに対して登録等を行い発行してもらっておく必要がある。 本実施の形態の認証情報はＩＤとパスワードの組であるが、その他の認証情報であってもよい。

[0050] サーバユーザＩＤとパスワードを取得したアプリケーションサーバ３０１は、当該端末ユーザのログイン処理を行い、当該端末ユーザに対してサービスの提供を開始する(図２及び図３のステップＡ１１)。

[0051] 本実施形態では、端末１００はアプリケーションサーバ３００のそれぞれに対しては、それぞれ異なるワンタイムＩＤしか送信しないため、複数のアプリケーションサーバ３００をまたがって、ある特定の端末ユーザを識別し、その端末ユーザの各アプリケーションサーバ３００上での行動を追跡することを防止することができる。

[0052] また、ユーザがアプリケーションサーバ３００利用時に、認証サーバ２００側は、認証サーバ２００内で管理している当該アプリケーションサーバに対応した、当該ユーザのサーバユーザＩＤ及びパスワードをアプリケーションサーバのワンタイムＩＤを用いた問い合わせに応じて送信することで、各アプリケーションサーバに対するユーザの手動ログイン操作が不要な自動シングルサインオンを実現することができる。

[0053] 実施の形態２

本発明の実施の形態２は、図６に示すように認証サーバが複数個あることを特徴とするものである。この場合、端末ユーザは認証サーバ２００（２０１～２０Ｎ）のうちの任意の複数個の認証サーバに対してユーザ登録を行い、端末ユーザＩＤをあらかじめ発行してもらっておく。また各アプリケーションサーバ３００に対して、当該端末ユーザがログインするためのサーバユーザＩＤ及びパスワードは、端末ユーザがユーザ登録を実施した認証サーバのうちのいずれのＩＤ管理部において管理されていてもよい。

[0054] この構成における本発明のＩＤ認証システムの動作について、第１の実施の形態と異なる部分のみ説明する。

[0055] 図２及び図３のステップＡ４において端末１００上のワンタイムＩＤ自動生成部１２０がワンタイムＩＤを生成する場合には、複数の認証サーバ２００（２０１～２０Ｎ）のうち、今回問い合わせるべき認証サーバのアドレスを、ワンタイムＩＤに埋め込んでおく。 例えば今回認証サーバ２０５を利用するとして、認証サーバ２０５のアドレスが「authentication.server205.co.jp」であった場合は、この情報を第１の実施の形態で述べた手順でワンタイムＩＤに埋め込んでおく。別の手段として、同じく第１の実施の形態で説明したように、この認証サーバのアドレスをアプリケーションサーバにワンタイムＩＤと別に送信するようにしてもよい。

[0056] 図２及び図３のステップＡ８においてアプリケーションサーバがＩＤ問い合わせ部を用いて認証サーバにワンタイムＩＤの問い合わせを行う際には、アプリケーションサーバにて受信したワンタイムＩＤに埋め込まれた認証サーバのアドレス、もしくは別途受信した認証サーバのアドレスを用いて、問い合わせるべき認証サーバを決定し、当該認証サーバに問い合わせを行うように動作する。

[0057] このような一連の処理により、複数台認証サーバが存在する図６の構成においても、本発明のＩＤ認証システムは動作することができる。

[0058] なお、本発明は上記実施の形態に限られたものではなく、趣旨を逸脱しな

い範囲で適宜変更することが可能である。例えば、端末ユーザＩＤは認証サーバから提供されるものでなく、ＭＡＣアドレス（Media Access Control address）のように端末を一意に識別できるものであってもよい。

[0059] また、ユーザが複数の端末を保有する場合、各端末で同一の端末ユーザＩＤを共有してもよい。例えば、ユーザがＰＣと携帯電話、ＰＤＡを保有している場合、それらの端末で同一の端末ユーザＩＤを共有してもよい。

[0060] この出願は、２００９年４月１５日に出願された日本出願特願２００９－０９８９９８を基礎とする優先権を主張し、その開示の全てをここに取り込む。

産業上の利用可能性

[0061] 本発明は、例えば、ユーザ認証を要するインターネット上の電子商取引システムについて利用可能性を有する。

符号の説明

[0062] １００ 端末 ２００ 認証サーバ ３０１～３０Ｎ サービス提供装置 １１０ サービス確認部 １２０ ワンタイムＩＤ自動生成部 １３０ ワンタイムＩＤ送信部 １４０ ユーザＩＤ送信部 ２１０ ＩＤ受信部 ２２０ ＩＤ管理部 ２３０ サーバＩＤ応答部 ３１０ ＩＤ問い合わせ部

請求の範囲

[請求項1] 端末装置と、複数のサービス提供装置と、認証サーバとを備え、

前記端末装置は、

一時的に使用されるワンタイムＩＤを生成するワンタイムＩＤ生成手段と、

前記ワンタイムＩＤ生成手段により生成されたワンタイムＩＤを前記サービス提供装置に対して送信するワンタイムＩＤ送信手段と、

前記ワンタイムＩＤ送信手段により送信したワンタイムＩＤと、ユーザを一意に識別するユーザＩＤとを前記認証サーバに対して、送信するユーザＩＤ送信手段を有し、

前記サービス提供装置は、

前記端末装置から送信されたワンタイムＩＤを受信し、前記認証サーバに対して、受信したワンタイムＩＤに対応する認証情報を問い合わせるＩＤ問い合わせ手段を有し、

前記認証サーバは、

ユーザＩＤと、前記サービス提供装置において認証するための認証情報を互いに関連付けて記憶する認証情報管理手段と、

前記端末装置から送信された前記ワンタイムＩＤとユーザＩＤとを受信するＩＤ受信手段と、

前記サービス提供装置からの問い合わせに含まれるワンタイムＩＤに対応する当該ユーザＩＤを、前記ＩＤ受信手段により受信された前記ワンタイムＩＤとユーザＩＤより取得し、さらに取得したユーザＩＤに基づいて前記認証情報管理手段において当該ユーザＩＤと関連づけられた認証情報を取得して、当該サービス提供装置に送信するサーバＩＤ応答手段を有するＩＤ認証システム。

[請求項2] 前記端末装置のワンタイムＩＤ生成手段は、前記認証サーバのアドレス情報を含むワンタイムＩＤを生成し、

前記サービス提供装置は、当該ワンタイムＩＤに含まれるアドレス

情報により指定された認証サーバに対して問い合わせを行うことを特徴とする請求項１記載のＩＤ認証システム。

[請求項3] 前記認証サーバのアドレス情報を含むワンタイムＩＤは、一時的な識別情報である文字列とドメイン名から構成されることを特徴とする請求項２記載のＩＤ認証システム。

[請求項4] 前記ＩＤ認証システムは、複数の認証サーバを備えたことを特徴とする請求項２又は３記載のＩＤ認証システム。

[請求項5] 端末装置においてワンタイムＩＤを生成し、

前記端末装置からサービス提供装置に対して前記ワンタイムＩＤを送信し、

前記端末装置から認証サーバに対して前記ワンタイムＩＤと、ユーザを一意に識別するためのユーザＩＤとを送信し、

前記サービス提供装置が、前記端末装置からワンタイムＩＤを受信し、そのワンタイムＩＤに基づいて前記認証サーバに一時的ＩＤに対応する認証情報を問い合わせる処理を実行し、

前記認証サーバが、前記端末装置から前記ワンタイムＩＤと前記ユーザＩＤとを受信し、

前記認証サーバが、前記サービス提供装置からの問い合わせに含まれるワンタイムＩＤに対応するユーザＩＤを取得し、さらに当該ユーザＩＤに対応する認証情報を取得して、当該サービス提供装置にその認証情報を送信するＩＤ認証方法。

[請求項6] 前記ワンタイムＩＤは、前記認証サーバのアドレス情報を含み、

前記サービス提供装置は、当該ワンタイムＩＤに含まれるアドレス情報により指定された認証サーバに対して問い合わせを行うことを特徴とする請求項５記載のＩＤ認証方法。

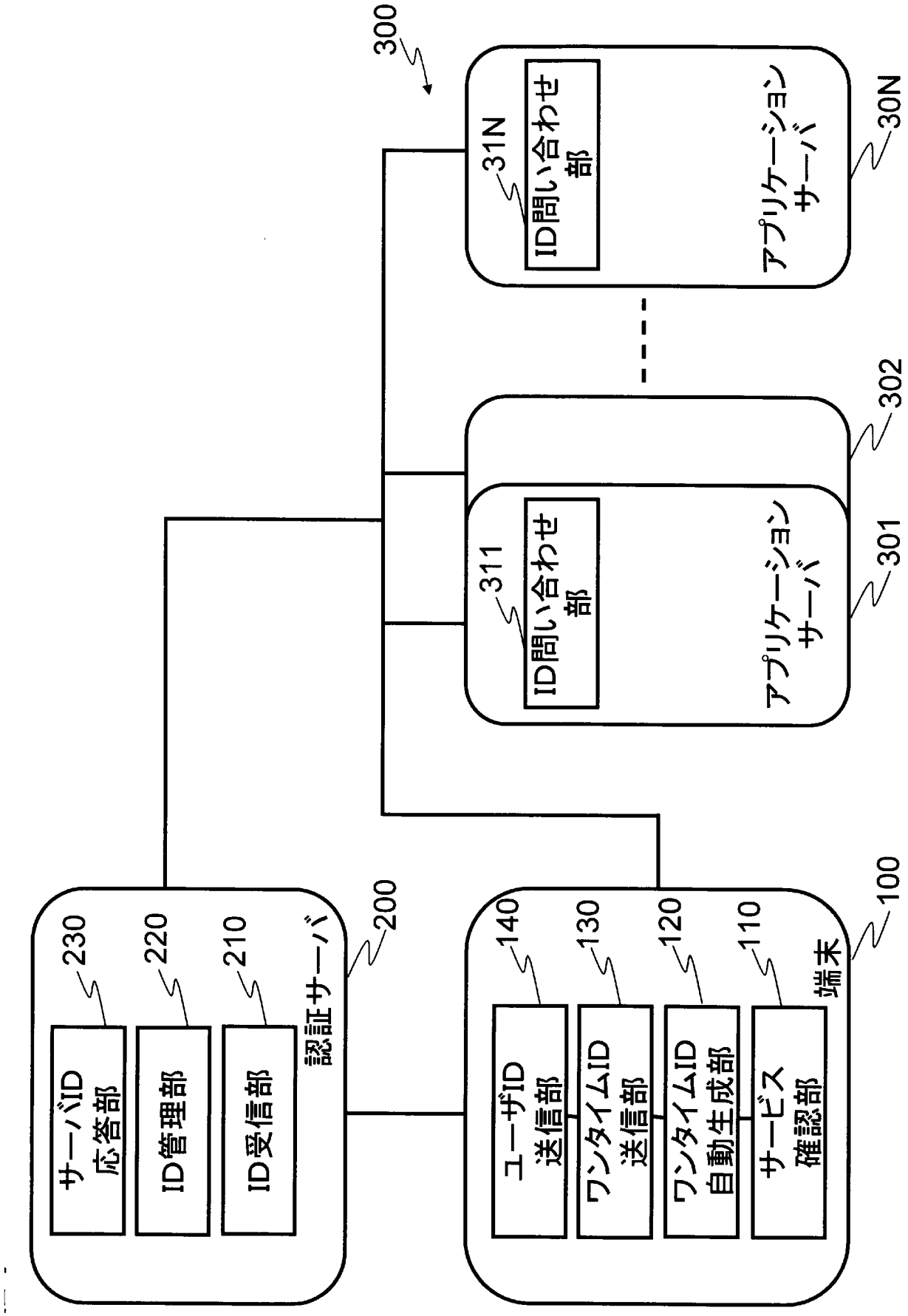
[請求項7] 前記認証サーバのアドレス情報を含むワンタイムＩＤは、一時的な識別情報である文字列とドメイン名から構成されることを特徴とする請求項６記載のＩＤ認証方法。

[請求項8] ユーザがサービス提供装置にログインするための認証を実行する処理をコンピュータに実行させるＩＤ認証プログラムが格納された非一時的なコンピュータ可読媒体であって、

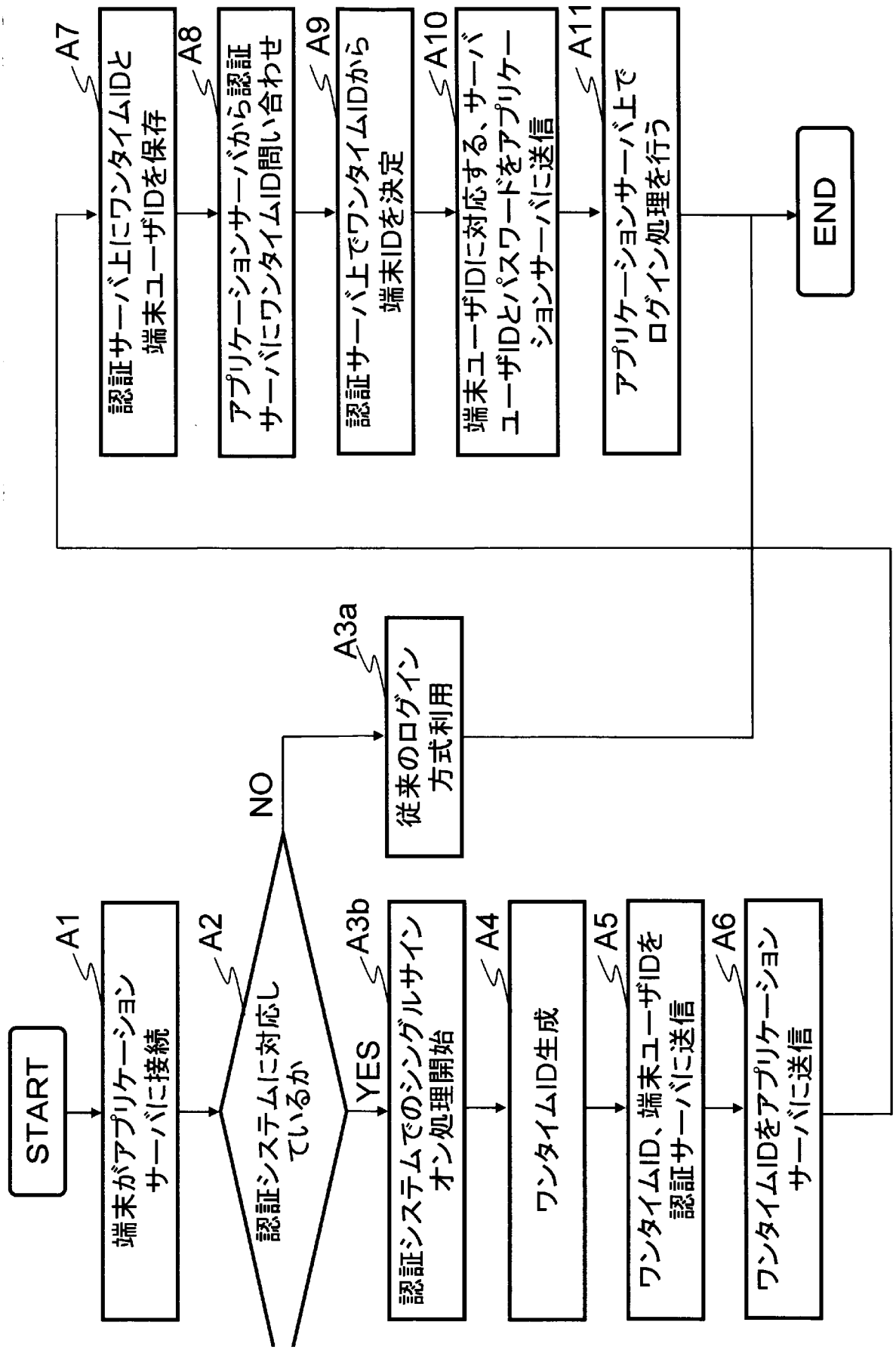
端末装置から送信されたワンタイムＩＤとユーザＩＤとを取得し、

前記端末装置から前記ワンタイムＩＤを受信したサービス提供装置からの問い合わせに含まれるワンタイムＩＤに対応するユーザＩＤを取得し、さらに当該ユーザＩＤに対応する認証情報を取得して、当該サービス提供装置にする認証情報を送信し処理実行させる処理を認証サーバに対して実行させるＩＤ認証プログラムが格納された非一時的なコンピュータ可読媒体。

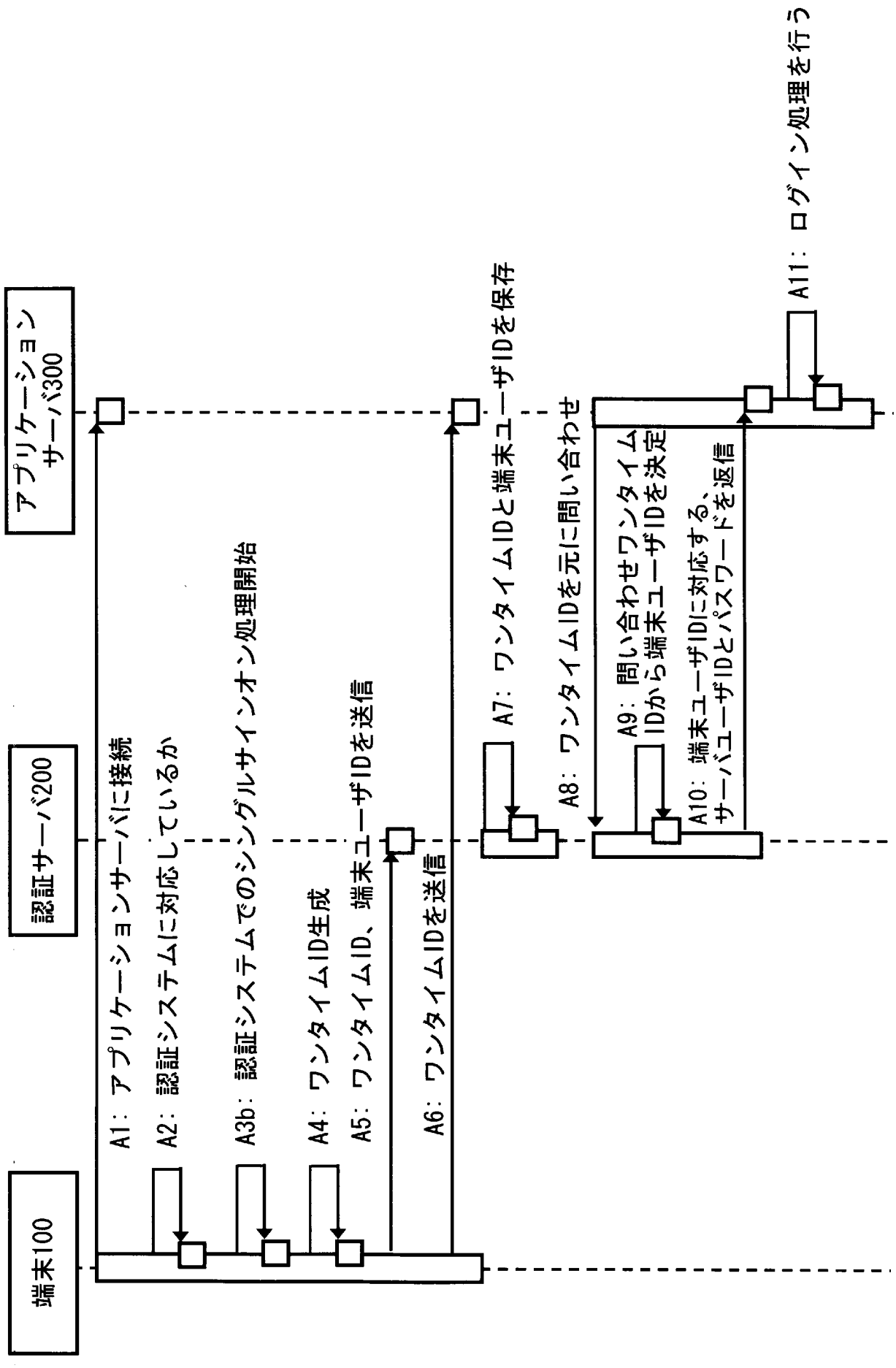
[図1]


300
31N
ID問い合わせ部
アプリケーションサーバ
30N
302
311
ID問い合わせ部
アプリケーションサーバ
301
230
220
210
サーバID応答部
ID管理部
ID受信部
認証サーバ
200
140
130
120
110
ユーザID送信部
ワンタイムID送信部
ワンタイムID自動生成部
サービス確認部
端末
100

[図2]


START
A1
端末がアプリケーション
サーバに接続
A2
認証システムに対応し
ているか
YES
NO
A3b
認証システムでのシングルサイン
オン処理開始
A4
ワンタイムID生成
A5
ワンタイムID、端末ユーザIDを
認証サーバに送信
A6
ワンタイムIDをアプリケーション
サーバに送信
A3a
従来のログイン
方式利用
A7
認証サーバ上にワンタイムIDと
端末ユーザIDを保存
A8
アプリケーションサーバから認証
サーバにワンタイムID問い合わせ
A9
認証サーバ上でワンタイムIDから
端末IDを決定
A10
端末ユーザIDに対応する、サーバ
ユーザIDとパスワードをアプリケー
ションサーバに送信
A11
アプリケーションサーバ上で
ログイン処理を行う
END

[図3]


端末100
認証サーバ200
アプリケーション
サーバ300
A1: アプリケーションサーバに接続
A2: 認証システムに対応しているか
A3b: 認証システムでのシングルサインオン処理開始
A4: ワンタイムID生成
A5: ワンタイムID、端末ユーザIDを送信
A6: ワンタイムIDを送信
A7: ワンタイムIDと端末ユーザIDを保存
A8: ワンタイムIDを元に問い合わせ
A9: 問い合わせワンタイム
IDから端末ユーザIDを決定
A10: 端末ユーザIDに対応する、
サーバユーザIDとパスワードを返信
A11: ログイン処理を行う

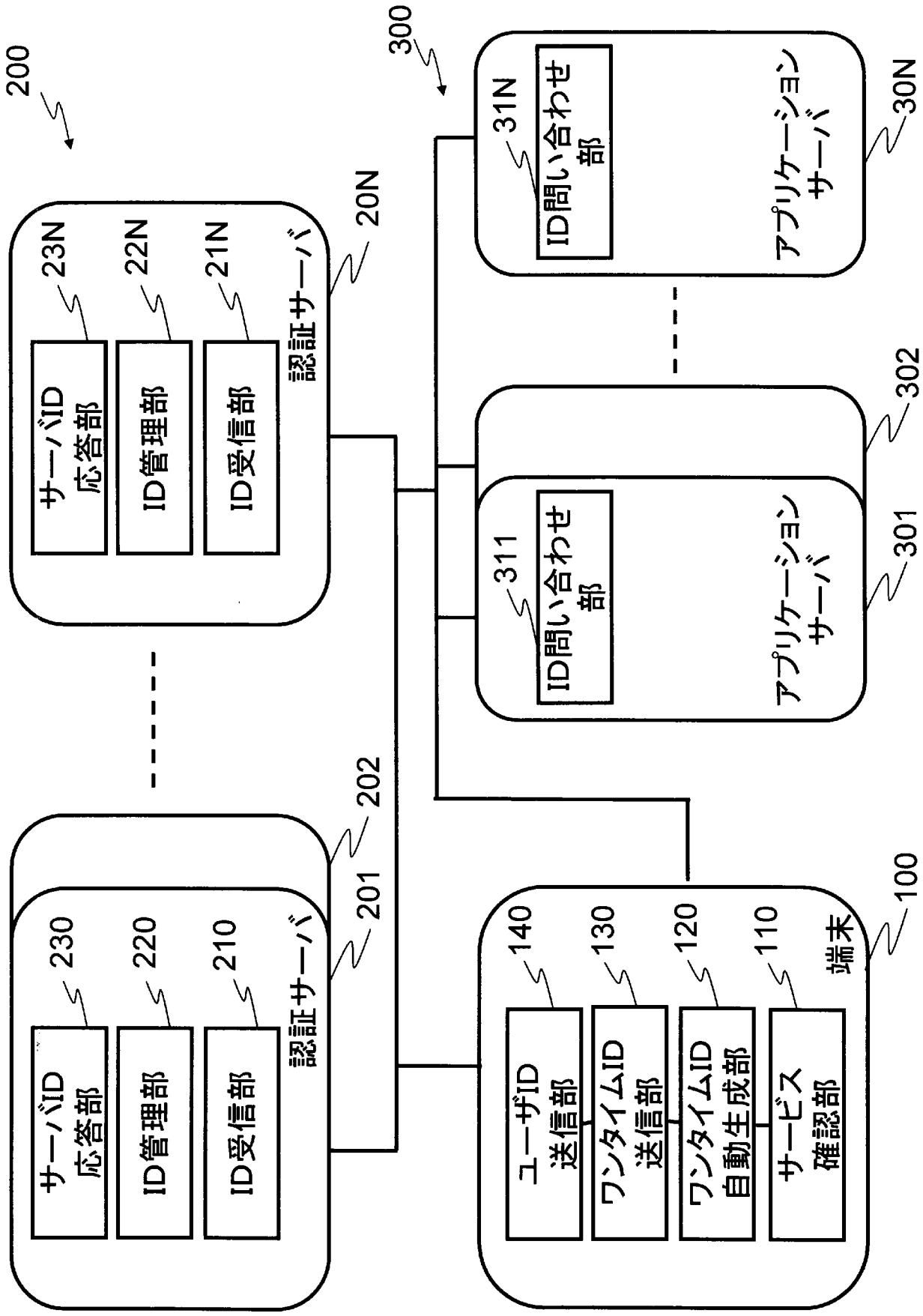
[図4]

ワンタイムID	端末ユーザID
a323912z9dw0afcdsl	user001
…	…

[図5]

端末ユーザID	アプリケーションサーバ識別子	サーバユーザID	パスワード
user001	http://abcde.com	yamada-taro	Xed241w
user001	http://fghij.com	yamada-t	E3vfgf36f
…	…	…	…

[図6]


200
300
認証サーバ
20N
23N
サーバID応答部
22N
ID管理部
21N
ID受信部
31N
ID問い合わせ部
アプリケーションサーバ
30N
302
311
ID問い合わせ部
アプリケーションサーバ
301
202
認証サーバ
201
230
サーバID応答部
220
ID管理部
210
ID受信部
100
端末
140
ユーザID送信部
130
ワンタイムID送信部
120
ワンタイムID自動生成部
110
サービス確認部

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2010/002073

A. CLASSIFICATION OF SUBJECT MATTER
G06F21/20(2006.01)i, *H04L9/32*(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, H04L9/32

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	1996-2010
Kokai Jitsuyo Shinan Koho	1971-2010	Toroku Jitsuyo Shinan Koho	1994-2010

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.
Y	JP 2006-004149 A (KDDI Corp.), 05 January 2006 (05.01.2006), paragraphs [0014] to [0033] (Family: none)	1-8
Y	JP 2005-519365 A (Telefonaktiebolaget LM Ericsson), 30 June 2005 (30.06.2005), paragraph [0041]; fig. 2 & US 2005/0154913 A1 & GB 2401509 A & EP 1497705 A & WO 2003/073242 A1 & DE 10392283 T & CA 2473793 A & SE 402099 A	1-8

☒ 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	Date of mailing of the international search report
23 April, 2010 (23.04.10)	11 May, 2010 (11.05.10)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2010/002073

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	"Jisedai Ninsho System SKIP9 Tsukaisute no One Time ID de Net Security no Gainen ga Kawaru One Time Password o Koeta Shin Solution", Nikkei System Kochiku no.145, no.145, Nikkei Business Publications, Inc., 26 April 2005 (26.04.2005), pages 170 to 171	1-8
Y	JP 2006-011989 A (NTT Docomo Inc.), 12 January 2006 (12.01.2006), paragraph [0046] & US 2005/0289643 A1 & EP 1613017 A1 & KR 10-2006-0048639 A & CN 1716856 A & KR 10-2007-0108337 A	2-4,6-7

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１０／００２０７３

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　G06F21/20(2006.01)i, H04L9/32(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（ＩＰＣ））

Int.Cl.　G06F21/20, H04L9/32

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	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２０１０年
日本国実用新案登録公報	１９９６－２０１０年
日本国登録実用新案公報	１９９４－２０１０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
Y	JP 2006-004149 A（ＫＤＤＩ株式会社）2006.01.05, 段落【００１４】－【００３３】（ファミリーなし）	1-8
Y	JP 2005-519365 A（テレフォンアクチーボラゲット　エル　エム　エリクソン）2005.06.30, 段落【００４１】、図２ & US 2005/0154913 A1 & GB 2401509 A & EP 1497705 A & WO 2003/073242 A1 & DE 10392283 T & CA 2473793 A & SE 402099 A	1-8

☑　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 ２３．０４．２０１０	国際調査報告の発送日 １１．０５．２０１０
国際調査機関の名称及びあて先 日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 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）　５Ｓ　４２２５ 本郷　彰 電話番号　０３－３５８１－１１０１　内線　３５４６

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
Y	次世代認証システムＳＫＩＰ９　使い捨てのワンタイムＩＤでネットセキュリティの概念が変わる　ワンタイムパスワードを超えた新ソリューション，日経システム構築　ｎｏ．１４５，第145号，日経ＢＰ社，2005.04.26，170～171	1-8
Y	JP 2006-011989 A (株式会社エヌ・ティ・ティ・ドコモ) 2006.01.12, 段落【００４６】 & US 2005/0289643 A1 & EP 1613017 A1 & KR 10-2006-0048639 A & CN 1716856 A & KR 10-2007-0108337 A	2-4,6-7