(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
2019年4月18日(18.04.2019)

WIPO | PCT

(10) 国際公開番号
WO 2019/074127 A1

(51) 国際特許分類:
G06F 21/31 (2013.01) *G06F 13/00* (2006.01)

(21) 国際出願番号： PCT/JP2018/038234

(22) 国際出願日： 2018年10月1日(01.10.2018)

(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 2017-198703 2017年10月12日(12.10.2017) JP
特願 2018-148913 2018年7月21日(21.07.2018) JP

(72) 発明者；および
(71) 出願人：川村 宜浩(**KAWAMURA Yoshihiro**) [JP/JP]; 〒4091502 山梨県北杜市大泉町谷戸４３２７－１ Yamanashi (JP).

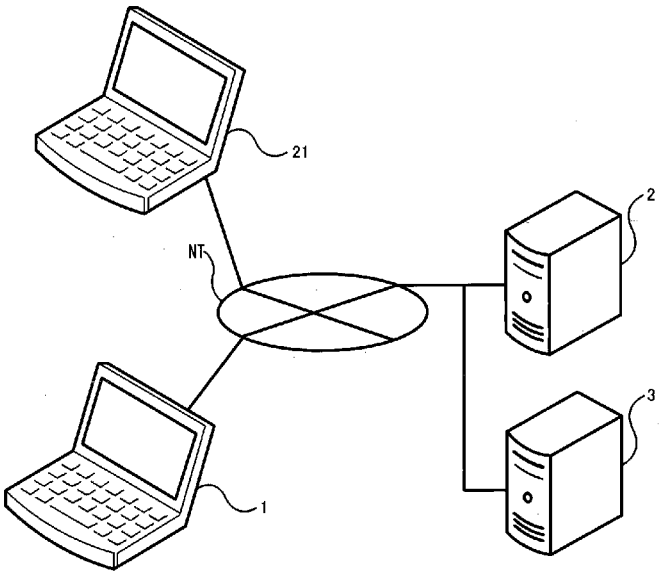
(81) 指定国(表示のない限り、全ての種類の国内保護が可能)：AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL,

WO 2019/074127 A1

(54) **Title:** CLIENT SERVER SYSTEM

(54) 発明の名称： クライアントサーバシステム

［図５］



(57) **Abstract:** Provided is a client server system in which a terminal device (1) comprises a data acquisition unit (113) which transmits an access request to a one-time URL indicated by URL information received from an operation server (2), and acquires data from the operation server (2). The operation server (2) comprises: a URL generation unit (212) which generates a one-time URL; a validity period setting unit (213) which sets a validity period for the one-time URL; an authentication processing unit (216) which authenticates the terminal device (1); and a state setting unit (215) which

［続葉有］

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, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, 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, KM, ML, MR, NE, SN, TD, TG).

添付公開書類:

一 国際調査報告(条約第21条(3))

sets an authentication function enabled state or an authentication function disabled state during the validith period of the one-time URL. The authentication processing unit (216), upon receipt of an access request, starts an authentication process if the authentication function enabled state is set, or avoids implementation of an authentication process if the authentication function disabled state is set.

(57) 要約:端末装置(1)は、業務サーバ(2)から受信したＵＲＬ情報が示すワンタイムＵＲＬへアクセス要求を送信することにより、業務サーバ(2)からデータを取得するデータ取得部(１１３)を有する。業務サーバ(2)は、ワンタイムＵＲＬを生成するＵＲＬ生成部(２１２)と、ワンタイムＵＲＬの有効期限を設定する有効期限設定部(２１３)と、端末装置(1)を認証する認証処理部(２１６)と、ワンタイムＵＲＬの有効期限内において、認証機能アクティブ状態と認証機能非アクティブ状態とのいずれかの状態に設定する状態設定部(２１５)と、を有する。認証処理部(２１６)は、アクセス要求を受信した場合、認証機能アクティブ状態に設定されているとき、認証処理を開始し、認証機能非アクティブ状態に設定されているとき、認証処理の実行を回避する。

明細書

発明の名称

クライアントサーバシステム

技術分野

本発明は、クライアントサーバシステムに関する。

背景技術

モバイル端末と、コンテンツプロバイダと、を備えるネットワークシステムが提案されている（例えば特許文献１参照）。ここで、モバイル端末は、自端末の電話番号を含む発呼信号を生成して、コンテンツプロバイダへ送信する。また、モバイル端末は、コンテンツプロバイダからメールを受信して該メールに含まれたパスワードを用いてコンテンツプロバイダにアクセスを行う。コンテンツプロバイダは、発呼信号を受信して発呼信号に含まれる電話番号を抽出し、契約しているユーザの電話番号と発呼信号に含まれる電話番号とを比較してモバイル端末を認証したとき、パスワードを生成して登録すると共に該パスワードを含むＵＲＬ（Uniform Resource Locator）を記述したメールを発呼信号に含まれる電話番号を用いてモバイル端末へ送信する。コンテンツプロバイダは、モバイル端末からからＵＲＬを含むアクセス要求情報を受信したとき、該ＵＲＬに含まれたパスワードを登録されているパスワードと比較し、一致しているときにモバイル端末に対してアクセスを許可して所定のコンテンツを供給する。

先行技術文献

特許文献

特許文献１：特開２００３－３０１４６号公報

発明の概要

発明が解決しようとする課題

しかしながら、特許文献１に記載されたネットワークシステムでは、メールに記述されたＵＲＬが盗聴された場合、コンテンツプロバイダへの不正アクセスが生じる虞がある。

本発明は、上記事由に鑑みてなされたものであり、サーバへの不正アクセスを抑制できるクライアントサーバシステム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

上記目的を達成するために、本発明に係るクライアントサーバシステムは、

第１端末装置と、第２端末装置と、サーバと、を備えるクライアントサーバシステムであって、

前記第１端末装置は、

前記サーバから受信した第１アクセス情報に基づいて、アクセス要求を前記サーバへ送信することにより、前記サーバからデータを取得するデータ取得部を有し、

前記第２端末装置は、

前記サーバから受信した第２アクセス情報に基づいて、前記サーバの状態を切り替える切替リクエストを前記サーバへ送信することにより、前記サーバの状態を切り替えるリクエスト送信部を有し、

前記サーバは、

前記第１アクセス情報および前記第２アクセス情報を生成するアクセス情報生成部と、

前記第１アクセス情報および前記第２アクセス情報の有効期限を設定する有効期限設定部と、

前記第１アクセス情報を前記第１端末装置へ送信するとともに、前記第２アクセス情報を前記第２端末装置へ送信するアクセス情報送信部と、

前記アクセス要求の送信元を認証するための認証処理を実行する認証処理部と、

前記切替リクエストを受信すると、前記認証処理部による認証処理の実行が許可される第１状態と、前記認証処理部による認証処理の実行が禁止される第２状態とのいずれかの状態に設定する状態設定部と、を有し、

前記認証処理部は、前記データ取得部から前記アクセス要求を受信した場合、前記第１状態に設定されているとき、前記認証処理を開始し、前記第２状態に設定されているとき、前記認証処理の実行を回避する。

発明の効果

本発明によれば、状態設定部が、切替リクエストを受信すると、認証処理の実行が許可される第１状態と、認証処理の実行が禁止される第２状態とのいずれかの状態に設定する。そして、認証処理部が、データ取得部からアクセス要求を受信した場合、第１状態に設定されているとき、認証処理を開始し、第２状態に設定されているとき、認証処理の実行を回避する。これにより、例えば状態設定部が、端末装置に対応する認証処理を一度実行した後第２状態に切り替えれば、その後、アクセス情報が盗聴されて他の端末装置からアクセス要求を受信しても認証処理部による認証が実行されない。従って、サーバへの不正アクセスが抑制されセキュリティを強化できる。また、本発明によれば、第１アクセス情報が第１端末装置へ送信されるとともに、第２アクセス情報が第２端末装置へ送信される。そして、第２端末装置にが、第２アクセス情報に基づいて、切替リクエストをサーバへ送信することにより、サーバの状態を切り替えることができる。

図面の簡単な説明

[図１] 本発明の実施の形態に係るクライアントサーバシステムの概略図である。

[図２] 実施の形態に係るクライアントサーバシステムのブロック図である。

[図３] 実施の形態に係るクライアントサーバシステムの動作を示すシーケンス図である。

[図４] 変形例に係るクライアントサーバシステムの動作を示すシーケンス図である。

[図５] 変形例に係るクライアントサーバシステムの概略図である。

[図６] 変形例に係る端末装置のブロック図である。

[図７] 変形例に係るクライアントサーバシステムの動作を示すシーケンス図である。

[図８] 変形例に係るクライアントサーバシステムの動作を示すシーケンス図である。

発明を実施するための形態

以下、本発明の一実施の形態に係るクライアントサーバシステムについて図面を参照して詳細に説明する。

本実施の形態に係るクライアントサーバシステムでは、サーバが端末装置から認証リクエストを受信すると、端末装置へワンタイムＵＲＬを示すＵＲＬ情報を送信する。そして、端末装置は、ユーザによるＵＲＬ情報が示すワンタイムＵＲＬへアクセスするための操作を受け付けると、アクセス要求をサーバへ送信する。サーバは、端末装置からアクセス要求を受信すると、認証処理の実行が許可された状態の場合、端末装置の認証処理を実行す

る。ここで、ワンタイムＵＲＬは、ネットワーク情報と認証情報とを含むアクセス情報である。認証情報としては、例えばログイン情報、トークンがある。

本実施の形態に係るクライアントサーバシステムは、図１に示すように、ユーザが所有する端末装置１と、例えばウェブコンテンツを提供する会社が所有する業務サーバ２および認証サーバ３とを備える。端末装置１と業務サーバ２、認証サーバ３とは、ネットワークＮＴを介して接続されている。ネットワークＮＴには、ＬＡＮ（Local Area Network）およびインターネットが含まれる。

端末装置１は、例えば通信機能を備えた汎用のパーソナルコンピュータであり、図２に示すように、ＣＰＵ（Central Processing Unit）１０１とＲＡＭ（Random Access Memory）（図示せず）とＲＯＭ（Read Only Memory）（図示せず）とストレージ１０２と入力部１０５と表示部１０３と通信部１０４とを備える。ＲＡＭは揮発性メモリから構成され、ＣＰＵ１０１の作業領域として使用される。ＲＯＭは、磁気ディスク、半導体メモリ等の不揮発性メモリから構成され、入力部１０５は、例えばキーボードであり、ユーザが入力する各種操作情報を受け付けて、受け付けた操作情報をＣＰＵ１０１へ出力する。表示部１０３は、例えば液晶ディスプレイであり、ＣＰＵ１０１から入力された各種情報を表示する。

端末装置１のＲＯＭは、端末装置１の各種機能を実現するためのプログラムを記憶する。そして、ＣＰＵ１０１は、このプログラムをＲＯＭからＲＡＭに読み出して実行することにより、ログイン受付部１１１、リクエスト送信部１１２およびデータ取得部１１３として機能する。ログイン受付部１１１は、表示部１０３にログイン画面を表示させるとともに、ユーザが入力部１０５を介して入力したユーザ識別情報およびパスワードを示すログイン情報を受け付ける。

リクエスト送信部１１２は、ログイン受付部１１１がログイン情報を受け付けると、業務サーバ２へ端末装置１の認証を要求する認証リクエストを送信する。この認証リクエストには、ログイン受付部１１１が受け付けた、ユーザ識別情報、パスワードを示す情報を含むログイン情報が含まれる。

データ取得部１１３は、業務サーバ２からワンタイムＵＲＬを示すＵＲＬ情報を受信した後、ユーザにより入力部１０５を介してワンタイムＵＲＬへアクセスするための操作を受け付けると、ワンタイムＵＲＬへのアクセス要求を業務サーバ２へ送信する。そして、データ取得部１１３は、ワンタイムＵＲＬへのアクセス要求を送信した後、業務サーバ２とのセッションが確立すると、業務サーバ２からデータを取得する。データ取得部１１３は、業務サーバ２から受信したデータを、ストレージに記憶させる。

業務サーバ２は、例えば通信機能を備えた汎用のパーソナルコンピュータであり、ＣＰＵ２０１とＲＡＭ（図示せず）とストレージ２０２と通信部２０４とを備える。ストレージ２０２は、端末装置１のユーザへ提供するデータを記憶する業務データベース（以下、「業務ＤＢ」と称する）２２１と、ログイン情報を記憶するログインＤＢ２２２と、を有する。

また、ストレージ２０２は、ワンタイムＵＲＬを生成して端末装置へ送信する機能、データを端末装置１への送信する機能および端末装置１の業務サーバ２へのアクセス権限を認証サーバ３への問い合わせる機能を実現するためのプログラムを記憶する。そして、ＣＰＵ２０１は、このプログラムをストレージ２０２からＲＡＭに読み出して実行することにより、リクエスト受信部２１１、アクセス情報生成部であるＵＲＬ生成部２１２、有効期限設定部２１３、アクセス情報送信部であるＵＲＬ送信部２１４、状態設定部２１５、認証処理部２１６およびデータ送信部２１７として機能する。リクエスト受信部２１１は、端末装置１から認証リクエストを受信する。リクエスト受信部２１１は、認証リクエストの送信元である端末装置１の識別情報を抽出して、ＵＲＬ送信部２１４へ通知する。

ＵＲＬ生成部２１２は、ワンタイムＵＲＬを生成する。有効期限設定部２１３は、ＵＲＬ生成部２１２により生成されるワンタイムＵＲＬの有効期限を設定する。

ＵＲＬ送信部２１４は、ＵＲＬ生成部２１２が生成するワンタイムＵＲＬを示すＵＲＬ情報を生成し、リクエスト受信部２１１から通知される送信元の端末装置１の識別情報に基づいて、ＵＲＬ情報を端末装置１へ送信する。

認証処理部２１６は、データ取得要求の送信元である端末装置１を認証するための認証処理を実行する。認証処理部２１６は、認証処理において、まず、端末装置１の業務サーバ２へのアクセス権限の有無を問い合わせる問い合わせ情報を、通信部２０４を介して認証サーバ３へ送信する。この問い合わせ情報には、対象となる端末装置１に対応するユーザ識別情報およびパスワードを示す情報が含まれる。そして、認証処理部２１６は、認証サーバ３から通信部２０４を介して、問い合わせ情報に対応する端末装置１に業務サーバ２へのアクセス権限があることを示す応答情報を受信すると、認証成功と判定し、端末装置１とのセッションを確立する。一方、認証処理部２１６は、認証サーバ３から通信部２０４を介して、問い合わせ情報に対応する端末装置１に業務サーバ２へのアクセス権限が無いことを示す応答情報を受信すると、認証失敗と判定し、端末装置１とのセッションの確立を回避する。また、認証処理部２１６は、端末装置１から認証リクエストを受信すると、受信した認証リクエストに含まれるログイン情報を抽出してログインＤＢ２２２に記憶させる。

状態設定部２１５は、ワンタイムＵＲＬの有効期限内において、認証処理部２１６による認証処理の実行が許可される認証機能アクティブ状態（第１状態）と、認証処理部２１６による認証処理の実行が禁止される認証機能非アクティブ状態（第２状態）とのいずれかの状態に設定する。そして、認証処理部２１６は、データ取得部１１３からアクセス要求を受信した場合、認証機能アクティブ状態に設定されているとき、認証処理を開始する。一方、認証処理部２１６は、認証機能非アクティブ状態に設定されているとき、認証処理の実行を回避する。状態設定部２１５は、受信したアクセス要求の送信元の端末装置１のＩＰアドレス、アクセス要求を受信した時間帯、送信元の端末装置１が存在する場所に応じて、認証機能アクティブ状態と認証機能非アクティブ状態とのいずれかに設定するものであってもよい。

データ送信部２１７は、端末装置１と業務サーバ２との間でセッションが確立すると、業務ＤＢ２２１が記憶するデータを端末装置１へ通信部２０４を介して送信する。

認証サーバ３は、業務サーバ２と同様に、例えば通信機能を備えた汎用のパーソナルコンピュータであり、ＣＰＵ３０１とＲＡＭ（図示せず）とストレージ３０２と通信部３０４とを備える。ストレージ３０２は、端末装置１のアクセス権限に関する情報が登録されたリポジトリ３２１を有する。

また、ストレージ３０２は、リポジトリ３２１を参照して、業務サーバ２から受信した問い合わせ情報に対応する端末装置１に業務サーバ２へのアクセス権限があるか否かを判定し、判定結果を業務サーバ２へ応答する機能を実現するためのプログラムを記憶する。そして、ＣＰＵ３０１が、このプログラムをストレージ３０２からＲＡＭに読み出して実行することにより、アクセス権限判定部３１１および権限有無通知部３１２として機能する。アクセス権限判定部３１１は、リポジトリ３２１を参照して、業務サーバ２から受信した問い合わせ情報に対応する端末装置１に業務サーバ２へのアクセス権限があるか否かを判定する。具体的には、アクセス権限判定部３１１は、問い合わせ情報に含まれるユーザ識別情報、パスワードを示す情報がリポジトリ３２１に登録されているか否かを判定する。アクセス権限判定部３１１は、問い合わせ情報に含まれるユーザ識別情報、パスワードを示す情報がリポジトリ３２１に登録されている場合、対応する端末装置１にアクセス権限があると判定する。

権限有無通知部３１２は、アクセス権限判定部３１１によるアクセス権限の有無の判定結果を示す応答情報を、業務サーバ２へ通信部３０４を介して送信する。

次に、本実施の形態に係るクライアントサーバシステムの動作について図３を参照しながら説明する。まず、業務サーバ2において、ＵＲＬ生成部２１２が、ワンタイムＵＲＬを生成する（ステップＳ１）。次に、業務サーバ２の有効期限設定部２１３は、ＵＲＬ生成部２１２が生成したワンタイムＵＲＬの有効期限を設定する（ステップＳ２）。

続いて、ＵＲＬ生成部２１２が生成したＵＲＬを示すＵＲＬ情報が、業務サーバ2から端末装置１へ送信される（ステップＳ３）。ＵＲＬ情報は、例えばＵＲＬ生成部２１２が生成したＵＲＬの記述を含むメールの形で業務サーバ2から端末装置１へ送信される。

一方、端末装置１では、ＵＲＬ情報を受信すると、データ取得部１１３が、ＵＲＬ情報が示すワンタイムＵＲＬを表示部１０３に表示させる（ステップＳ４）。ここで、データ取得部１１３は、ブラウザとして機能する場合、ワンタイムＵＲＬの記述を含むブラウザ画面を表示部１０３に表示させる。

続いて、端末装置１のデータ取得部１１３は、表示部１０３に表示されるワンタイムＵＲＬが選択された状態で、ユーザが入力部１０５を介してワンタイムＵＲＬをクリックする操作を行うと、そのワンタイムＵＲＬクリック操作を受け付ける（ステップＳ５）。

その後、ワンタイムＵＲＬへアクセスすることを要求するアクセス要求が、端末装置１から業務サーバ2へ送信される（ステップＳ６）。

次に、ワンタイムＵＲＬで指定されるログイン入力情報が、業務サーバ2から端末装置１へ送信される（ステップＳ７）。このログイン入力情報は、例えば端末装置１の表示部１０３にログイン画面を表示させるための情報である。

続いて、端末装置１の表示部１０３にログイン画面が表示された状態で、ユーザが入力部１０５を介してログイン操作を行うと、端末装置１のログイン受付部１１１が、ログイン操作を受け付ける（ステップＳ８）。ここで、ログイン操作としては、例えばユーザによるユーザ識別情報、パスワード等の入力操作である。

続いて、端末装置１の認証を業務サーバ2へ要求する認証リクエストが、端末装置１から業務サーバ2へ送信される（ステップＳ９）。このとき、業務サーバ2では、認証処理部２１６が、受信した認証リクエストに含まれるログイン操作により入力されたユーザ識別情報、パスワード等を含むログイン情報を抽出してログインＤＢ２２２に記憶させる。

その後、業務サーバ2では、状態設定部２１５が、業務サーバ2を、認証処理部２１６による認証処理が許可される認証機能アクティブ状態に設定する（ステップＳ１０）。次に、認証処理部２１６が、認証処理を開始する（ステップＳ１１）。

続いて、業務サーバ2の認証処理部２１６は、認証が成功したと判定すると（ステップＳ１２）、端末装置１と業務サーバ2との間のセッションを確立する（ステップＳ１３）。続いて、アクセス要求に対応するデータが、業務サーバ2から端末装置１へ送信される（ステップＳ１４）。一方、端末装置１では、データを受信すると、データ取得部１１３が、受信したデータをストレージに記憶させる（ステップＳ１５）。これにより、端末装置１において、業務サーバ2から取得したデータを利用することが可能となる。

また、業務サーバ2において、状態設定部２１５が、ワンタイムＵＲＬの有効期限内において、業務サーバ2を認証機能非アクティブ状態に設定したとする（ステップＳ１６）。ここで、端末装置１において、データ取得部１１３が、ＵＲＬ情報が示すワンタイムＵＲＬを表示部１０３に表示させた後（ステップＳ１７）、そのワンタイムＵＲＬクリック操作を受け付けたとする（ステップＳ１８）。この場合、ワンタイムＵＲＬへアクセスすることを要求するアクセス要求が、端末装置１から業務サーバ2へ送信される（ステップＳ１９）。このとき、業務サーバ2が認証機能非アクティブ状態に設定されているので、認証処理部２１６は、認証処理の実行を回避する。

また、ワンタイムＵＲＬの有効期限が到来すると、業務サーバ２では、ＵＲＬ生成部２１２が、ワンタイムＵＲＬを失効させる（ステップＳ２０）。

以上説明したように、本実施の形態に係るクライアントサーバシステムによれば、状態設定部２１５が、ワンタイムＵＲＬの有効期限内において、認証処理の実行が許可される認証機能アクティブ状態と、認証処理の実行が禁止される認証機能非アクティブ状態とのいずれかの状態に設定する。そして、認証処理部２１６が、データ取得部１１３からアクセス要求を受信した場合、認証機能アクティブ状態に設定されているとき、認証処理を開始する。一方、認証処理部２１６は、認証機能非アクティブ状態に設定されているとき、認証処理の実行を回避する。これにより、例えば状態設定部２１５が、端末装置１に対応する認証処理を一度実行した後、認証機能非アクティブ状態に切り替えれば、その後、ＵＲＬ情報が盗聴されて他の端末装置からアクセス要求を受信しても認証処理部２１６による認証が実行されない。従って、業務サーバ２への不正アクセスが抑制される。

以上、本発明の実施の形態について説明したが、本発明は前述の実施の形態の構成に限定されるものではない。例えば、アクセス要求が、端末装置１から業務サーバ２へ送信された後、業務サーバ２において他のワンタイムＵＲＬを生成し、生成したワンタイムＵＲＬの記述を含むいわゆるＣメール（ＳＭＳ（Short Mail Service）メール）が、業務サーバ２から端末装置１へ送信されるようにしてもよい。そして、端末装置１の表示部１０３にＣメールの内容が表示された状態で、ユーザが入力部１０５を介してＣメールに記述されたワンタイムＵＲＬをクリックすると、認証リクエストが、端末装置１から業務サーバ２へ送信されてもよい。その後、業務サーバ２において、状態設定部２１５が、業務サーバ２を認証機能アクティブ状態に設定すればよい。

本構成によれば、端末装置１にブラウザが実装されていなくてもワンタイムＵＲＬを用いた認証処理が実現できる。

実施の形態では、ワンタイムＵＲＬを利用して認証処理を実行するクライアントサーバシステムの例について説明したが、これに限らず、例えばワンタイムトークンとワンタイムＵＲＬとの両方を利用して認証処理を実行するものであってもよい。この場合、業務サーバ２は、ワンタイムトークンを生成するトークン生成部を備えており、有効期限設定部２１３が、ワンタイムトークンの有効期限を設定する構成とすればよい。また、端末装置１が、業務サーバ２のＵＲＬ生成部２１２と同じ方法でワンタイムＵＲＬを生成するアクセス情報生成部であるＵＲＬ生成部と、生成されたＵＲＬの有効期限を設定する有効期限設定部と、を備えていてもよい。

ここで、本変形例に係るクライアントサーバシステムの動作について図４を参照しながら説明する。まず、ログイン入力情報が、業務サーバ２から端末装置１へ送信される（ステップＳ２０１）。次に、端末装置１の表示部１０３にログイン画面が表示された状態で、ユーザがログイン操作を行うと、端末装置１のログイン受付部１１１が、ログイン操作を受け付ける（ステップＳ２０２）。続いて、第１認証リクエストが、端末装置１から業務サーバ２へ送信される（ステップＳ２０３）。一方、業務サーバ２では、端末装置１から第１認証リクエストを受信すると、ワンタイムトークン生成部が、ワンタイムトークンを生成する（ステップＳ２０４）。その後、業務サーバ２の有効期限設定部２１３が、ワンタイムトークンの有効期限を設定する（ステップＳ２０５）。

次に、トークン生成部が生成したワンタイムトークンを示すトークン情報が、業務サーバ２から端末装置１へ送信される（ステップＳ２０６）。トークン情報は、例えばワンタイムトークンの記述を含むｈｔｍｌファイルの形で業務サーバ２から端末装置１へ送信される。続いて、端末装置１の表示部１０３にワンタイムトークンを含む画面が表示された状態で、ユーザがトークンを入力する操作を行うと、端末装置１のログイン受付部１１１が、トークンの入力操作を受け付ける（ステップＳ２０７）。続いて、第２認証リクエ

ストが、端末装置１から業務サーバ２へ送信される（ステップＳ２０８）。その後、端末装置１では、ＵＲＬ生成部が、ワンタイムＵＲＬを生成し（ステップＳ２０９）、有効期限設定部が、ＵＲＬ生成部が生成したワンタイムＵＲＬの有効期限を設定する（ステップＳ２１０）。

一方、業務サーバ２では、端末装置１から第２認証リクエストを受信すると、ＵＲＬ生成部２１２が、ワンタイムＵＲＬを生成する（ステップＳ２１１）。次に、業務サーバ２の有効期限設定部２１３は、ＵＲＬ生成部２１２が生成したワンタイムＵＲＬの有効期限を設定する（ステップＳ２１２）。

一方、端末装置１では、データ取得部１１３が、ＵＲＬ生成部が生成したワンタイムＵＲＬを表示部１０３に表示させる（ステップＳ２１３）。その後、端末装置１のデータ取得部１１３は、表示部１０３に表示されるワンタイムＵＲＬが選択された状態で、ユーザが入力部１０５を介してワンタイムＵＲＬをクリックする操作を行うと、そのワンタイムＵＲＬクリック操作を受け付ける（ステップＳ２１４）。次に、ワンタイムＵＲＬへのアクセス要求が、端末装置１から業務サーバ２へ送信される（ステップＳ２１５）。一方、業務サーバ２では、アクセス要求を受信すると、状態設定部２１５が、業務サーバ２を認証機能アクティブ状態に設定する（ステップＳ２１６）。その後、ステップＳ２１７乃至Ｓ２２６の処理が実行される。ステップＳ２１７乃至Ｓ２２６の処理は、実施の形態で説明したステップＳ１１乃至Ｓ２０の処理と同様である。

本構成によれば、ログイン情報、ワンタイムトークンおよびワンタイムＵＲＬを用いた３つのステップが正常に行われて初めて認証処理が実行される。従って、実施の形態に比べてセキュリティの向上を図ることができる。

実施の形態では、ユーザがワンタイムＵＲＬをクリックすると、端末装置１の表示部１０３にログイン画面が表示され、ユーザがログイン操作を行うと、認証リクエストが、端末装置１から業務サーバ２へ送信され、その後、業務サーバ２が認証機能アクティブ状態に設定される例について説明した。但し、これに限らず、例えば、端末装置１が、ワンタイムＵＲＬを生成するＵＲＬ生成部を備えており、ユーザがワンタイムＵＲＬをクリックすると、端末装置１のＵＲＬ生成部が他のワンタイムＵＲＬを生成して表示部１０３に表示するものであってもよい。そして、ユーザにより、端末装置１の表示部１０３に表示されたワンタイムＵＲＬがクリックされると、認証リクエストが、端末装置１から業務サーバ２へ送信され、業務サーバ２が認証機能アクティブ状態に設定されるようにしてもよい。

或いは、端末装置１の表示部１０３にログイン画面が表示された状態で、ユーザがログイン操作を行うと、端末装置１のＵＲＬ生成部が他のワンタイムＵＲＬを生成して表示部１０３に表示するものであってもよい。この場合、業務サーバ２は、エージェント情報記憶部と、エージェント情報判定部と、を備える構成とすればよい。エージェント情報記憶部は、業務サーバ２とのセクション確立が許容される端末装置に対応する複数のユーザエージェント情報を記憶する。また、エージェント情報判定部は、端末装置１から受信した認証リクエストに含まれるユーザエージェント情報がエージェント情報記憶部に記憶されているユーザエージェント情報のいずれかに一致するか否かを判定する。

本変形例では、ユーザにより、端末装置１の表示部１０３に表示されたワンタイムＵＲＬがクリックされると、端末装置１に付与されたユーザエージェント情報を含む認証リクエストが、端末装置１から業務サーバ２へ送信される。そして、業務サーバ２において、エージェント情報判定部が、認証リクエストに含まれるユーザエージェント情報がエージェント情報記憶部に記憶されているユーザエージェント情報のいずれかとが一致するか否か判定する。エージェント情報判定部が、認証リクエストに含まれるユーザエージェント情報がエージェント情報記憶部に記憶されているユーザエージェント情報のいずれか

に一致していると判定すると、状態設定部２１５が、業務サーバ２を認証機能アクティブ状態に設定する。

また、業務サーバ２が、認証リクエストを受信すると、認証リクエストを受信した旨を通知するリクエスト通知情報を他の端末装置へ送信するリクエスト通知部を備えるものであってもよい。この場合、ユーザがワンタイムＵＲＬをクリックすることにより、アクセス要求が端末装置１から業務サーバ２へ送信されると、業務サーバ２のリクエスト通知部が、リクエスト通知情報を、例えば管理者の所持する他の端末装置へ送信する。そして、他の端末装置において、リクエスト通知情報に対して応答するための操作を行うと、応答情報が、他の端末装置から業務サーバ２へ送信される。そして、業務サーバ２において、状態設定部２１５が、応答情報を受信すると、業務サーバ２を認証機能アクティブ状態に設定するようにすればよい。

実施の形態において、状態設定部２１５が、認証機能アクティブ状態に設定した後、ワンタイムＵＲＬの有効期限の到来前に、業務サーバ２への不正アクセスが検出されると、業務サーバ２を認証機能非アクティブ状態に設定するものであってもよい。

実施の形態において、端末装置１が、複数存在し、業務サーバ２が、１の端末装置１と業務サーバ２との間でセッションが確立すると、他の端末装置１からのワンタイムＵＲＬへのアクセスを禁止するアクセス制限部を更に備えるものであってもよい。

実施の形態では、ログイン情報が、ユーザ識別情報とパスワードを示す情報とを含む場合について説明したが、ログイン情報に含まれる情報はこれらに限定されるものではない。例えばログイン情報が、ユーザを特定できる乱数列（トークン）を含むものであってもよい。

実施の形態では、状態設定部２１５が、ワンタイムＵＲＬの有効期限の到来前に、業務サーバ２の状態を一度だけ認証機能アクティブ状態から認証機能非アクティブ状態へ切り替える例について説明した。但し、これに限らず、状態設定部２１５が、業務サーバ２の状態を認証機能アクティブ状態から認証機能非アクティブ状態へ、或いは、認証機能非アクティブの状態から認証機能アクティブの状態へ複数回切り替えてもよい。

実施の形態において、端末装置１が業務サーバとしての機能を有するものであってもよい。

実施の形態では、端末装置１がワンタイムＵＲＬを表示部１０３に表示される例について説明したが、これに限らず、例えば端末装置１がワンタイムＵＲＬを表示部１０３に表示しないものであってもよい。この場合、端末装置１は、例えばＵＲＬ情報を受信すると、表示部１０３にアイコンを表示させ、そのアイコンがクリックされると、ＵＲＬ情報が示すワンタイムＵＲＬに基づいて、業務サーバ２へアクセスする構成であってもよい。

実施の形態では、図３のステップＳ１３において、業務サーバ２が端末装置１とのセッションを確立する例について説明したが、これに限らない。例えば、業務サーバ２が、図３のステップＳ１３のタイミングにおいて、トークンを端末装置１へ送信するものであってもよい。

実施の形態に係るクライアントサーバシステムでは、業務サーバ２と認証サーバ３とが各別の機器である例について説明した。但し、これに限定されるものではなく、業務サーバ２の機能と認証サーバ３の機能との両方を有する機器を備えたクライアントサーバシステムであってもよい。

本実施の形態に係るクライアントサーバシステムにおいて、例えば、ユーザが端末装置を用いて、業務サーバ２を、認証機能アクティブ状態または認証機能非アクティブ状態に設定することができるものであってもよい。本変形例に係るクライアントサーバシステムは、例えば図５に示すように、データの提供を受けるユーザが所持する端末装置１と、業務サーバ２と、認証サーバ３と、業務サーバ２の管理者が所持する端末装置２１と、を備

える。なお、図５において、実施の形態と同様の構成については図１と同一の符号を付している。また、端末装置２１のハードウェア構成は、実施の形態で説明した端末装置１と同様である。以下、実施の形態と同様の構成については、図１または図２と同一の符号を用いて説明する。

端末装置２１のＣＰＵ１０１は、ストレージ１０２からＲＡＭに読み出して実行することにより、図６に示すように、受付部２１１１およびリクエスト送信部２１１２として機能する。受付部２１１１は、業務サーバ２からアクセス制御用ワンタイムＵＲＬを指定する操作または業務サーバ２の認証機能を切り替えるための操作を受け付ける。リクエスト送信部２１１２は、受付部２１１１が切替操作を受け付けると、業務サーバ２へ業務サーバ２の認証機能を切り替えることを要求する切替リクエストを送信する。この認証リクエストには、業務サーバ２の認証機能をアクティブにするか非アクティブにするかを示す情報が含まれる。

ＵＲＬ生成部２１２は、第１ワンタイムＵＲＬであるログイン用ワンタイムＵＲＬと第２ワンタイムＵＲＬであるアクセス制御用ワンタイムＵＲＬとを生成する。ここで、ログイン用ワンタイムＵＲＬは、例えばデータの提供を受けるユーザの所持する端末装置１へログイン情報を送信する際に使用されるものであり、アクセス制御用ワンタイムＵＲＬは、管理者が端末装置２１を介して業務サーバ２から切替情報を受信するための使用されるものである。この切替情報は、例えば端末装置２１の表示部１０３に業務サーバ２の認証機能を切り替えるための切替操作画面を表示させるための情報である。また、ＵＲＬ生成部２１２は、ログイン用ワンタイムＵＲＬ毎に、それに対応するアクセス制御用ワンタイムＵＲＬを同時または同一の実行プロセス時に生成する。ここで、アクセス制御用ワンタイムＵＲＬは、１つのログイン用ワンタイムＵＲＬに対して１つだけ生成されてもよいし、複数生成されてもよい。

ＵＲＬ送信部２１４は、ログイン用ワンタイムＵＲＬを示す第１ＵＲＬ情報であるログイン用ＵＲＬ情報と、アクセス制御用ワンタイムＵＲＬを示す第２ＵＲＬ情報であるアクセス制御用ＵＲＬ情報を生成する。そして、ＵＲＬ送信部２１４は、リクエスト受信部２１１から通知される送信元の端末装置１の識別情報に基づいて、ログイン用ＵＲＬ情報を端末装置１へ送信する。また、ＵＲＬ送信部２１４は、リクエスト受信部２１１から通知される送信元の端末装置２１の識別情報に基づいて、アクセス制御用ＵＲＬ情報を端末装置２１へ送信する。

認証処理部２１６は、実施の形態と同様に、データ取得要求の送信元である端末装置１を認証するための認証処理を実行する。状態設定部２１５は、アクセス制御用ワンタイムＵＲＬの有効期限内において、端末装置２１から受信した切替リクエストに基づいて、認証機能アクティブ状態（第１状態）と、認証機能非アクティブ状態（第２状態）とのいずれかの状態に設定する。そして、認証処理部２１６は、アクセス要求を受信した場合、認証機能アクティブ状態に設定されているとき、認証処理を開始する。一方、認証処理部２１６は、認証機能非アクティブ状態に設定されているとき、認証処理の実行を回避する。

有効期限設定部２１３およびデータ送信部２１７の機能は、実施の形態と同様である。

次に、本実施の形態に係るクライアントサーバシステムの動作について図７および図８を参照しながら説明する。まず、業務サーバ２において、ＵＲＬ生成部２１２が、ログイン用ワンタイムＵＲＬを生成するとともに（ステップＳ３０１）、アクセス制御用ワンタイムＵＲＬを生成する（ステップＳ３０２）。即ち、ＵＲＬ生成部２１２は、ログイン用ワンタイムＵＲＬとアクセス制御用ワンタイムＵＲＬとを同時または同一の実行プロセス時に生成する。次に、業務サーバ２の有効期限設定部２１３は、ＵＲＬ生成部２１２が生成したログイン用ワンタイムＵＲＬの有効期限を設定する（ステップＳ３０３）。

続いて、ＵＲＬ生成部２１２が生成したログイン用ワンタイムＵＲＬを示すログイン用

ＵＲＬ情報が、業務サーバ２から端末装置１へ送信され（ステップＳ３０４）、ＵＲＬ生成部２１２が生成したアクセス制御用ワンタイムＵＲＬを示すログイン用ＵＲＬ情報が、業務サーバ２から端末装置２１へ送信され（ステップＳ３０５）。ログイン用ＵＲＬ情報およびアクセス制御用ＵＲＬ情報は、例えばＵＲＬ生成部２１２が生成したログイン用ワンタイムＵＲＬ、アクセス制御用ワンタイムＵＲＬの記述を含むメールの形で業務サーバ２から端末装置１へ送信される。但し、この時点では、業務サーバ２が認証機能非アクティブであるため、端末装置１は、業務サーバ２からデータを取得できない。また、アクセス制御用ワンタイムＵＲＬは、管理者（例えば、上位権限者、上司、保護者等）が所持する端末装置２１へ例えばメールにより送信される。

一方、端末装置１では、ログイン用ＵＲＬ情報を受信すると、データ取得部１１３が、ログイン用ＵＲＬ情報が示すログイン用ワンタイムＵＲＬを表示部１０３に表示させる（ステップＳ３０６）。ここで、データ取得部１１３は、ブラウザとして機能する場合、ワンタイムＵＲＬの記述を含むブラウザ画面を表示部１０３に表示させる。また、端末装置２１では、アクセス制御用ＵＲＬ情報を受信すると、リクエスト送信部２１１２が、アクセス制御用ＵＲＬ情報が示すアクセス制御用ワンタイムＵＲＬを表示部１０３に表示させる（ステップＳ３０７）。

続いて、端末装置２１のリクエスト送信部２１１２は、表示部１０３に表示されるアクセス制御用ワンタイムＵＲＬが選択された状態で、ユーザが入力部１０５を介してアクセス制御用ワンタイムＵＲＬをクリックする操作を行うと、そのアクセス制御用ワンタイムＵＲＬクリック操作を受け付ける（ステップＳ３０８）。

その後、アクセス制御用ワンタイムＵＲＬへアクセスすることを要求するアクセス要求が、端末装置２１から業務サーバ２へ送信される（ステップＳ３０９）。

次に、アクセス制御用ワンタイムＵＲＬで指定される切替情報が、業務サーバ２から端末装置２１へ送信される（ステップＳ３１０）。この切替情報は、例えば端末装置２１の表示部１０３に業務サーバ２の認証機能を切り替えるための切替操作画面を表示させるための情報である。

続いて、端末装置２１の表示部１０３に切替操作画面が表示された状態で、ユーザが入力部１０５を介して切替操作を行うと、端末装置１の受付部２１１１が、切替操作を受け付ける（ステップＳ３１１）。その後、業務サーバ２の認証機能の切替を要求する切替リクエストが、端末装置２１から業務サーバ２へ送信される（ステップＳ３１２）。

一方、業務サーバ２では、状態設定部２１５が、切替リクエストを受信すると、業務サーバ２を、認証処理部２１６による認証処理が許可される認証機能アクティブ状態に設定する（ステップＳ３１３）。つまり、管理者が、端末装置２１を使用してアクセス制御用ワンタイムＵＲＬにアクセスすることにより、業務サーバ２が認証機能アクティブとなり、端末装置１が業務サーバ２からデータを取得することが可能となる。ここで、状態設定部２１５は、受信した切替リクエストに対応するアクセス制御用ワンタイムＵＲＬに対応付けて生成されたログイン用ワンタイムＵＲＬへのアクセス要求についての認証機能のみをアクティブ状態にする。例えば、ログイン用ワンタイムＵＲＬとして「ＬＵＲＬ－Ａ」、「ＬＵＲＬ－Ｂ」が生成され、これらそれぞれに対応付けられたアクセス制御用ワンタイムＵＲＬとして「ＡＵＲＬ－Ａ」、「ＡＵＲＬ－Ｂ」が生成されているとする。この場合、状態設定部２１５は、切替リクエストがアクセス制御用ワンタイムＵＲＬ「ＡＵＲＬ－Ａ」に対応するものである場合、ログイン用ワンタイムＵＲＬ「ＬＵＲＬ－Ａ」へのアクセス要求についての認証機能のみをアクティブにし、ログイン用ワンタイムＵＲＬ「ＬＵＲＬ－Ａ」へのアクセス要求についての認証機能は非アクティブの状態で維持する。

次に、端末装置１のデータ取得部１１３は、表示部１０３に表示されるログイン用ワン

タイムＵＲＬが選択された状態で、ユーザが入力部１０５を介してログイン用ワンタイムＵＲＬをクリックする操作を行うと、そのログイン用ワンタイムＵＲＬのクリック操作を受け付ける（ステップＳ３１４）。

続いて、ログイン用ワンタイムＵＲＬへアクセスすることを要求するアクセス要求が、端末装置１から業務サーバ２へ送信される（ステップＳ３１５）。

その後、ログイン用ワンタイムＵＲＬで指定されるログイン入力情報が、業務サーバ２から端末装置１へ送信される（ステップＳ３１６）。このログイン入力情報は、例えば端末装置１の表示部１０３にログイン画面を表示させるための情報である。ここで、業務サーバ２は、ステップＳ３１３において認証機能がアクティブになっているログイン用ワンタイムＵＲＬへのアクセス要求を受信したときのみ、そのログイン用ワンタイムＵＲＬで指定されるログイン情報を端末装置１へ送信する。例えば、ログイン用ワンタイムＵＲＬとして「ＬＵＲＬ－Ａ」、「ＬＵＲＬ－Ｂ」が生成され、ログイン用ワンタイムＵＲＬ「ＬＵＲＬ－Ａ」へのアクセス要求に対応する認証機能のみがアクティブになっているとする。この場合、業務サーバ２は、ログイン用ワンタイムＵＲＬ「ＬＵＲＬ－Ａ」へのアクセス要求を受信した場合、ログイン情報を端末装置１へ送信するが、ログイン用ワンタイムＵＲＬ「ＬＵＲＬ－Ｂ」へのアクセス要求を受信した場合、ログイン情報の端末装置１への送信を回避する。

次に、端末装置１の表示部１０３にログイン画面が表示された状態で、ユーザが入力部１０５を介してログイン操作を行うと、端末装置１のログイン受付部１１１が、ログイン操作を受け付ける（ステップＳ３１７）。ここで、ログイン操作としては、例えばユーザによるユーザ識別情報、パスワード等の入力操作である。

続いて、端末装置１の認証を業務サーバ２へ要求する認証リクエストが、端末装置１から業務サーバ２へ送信される（ステップＳ３１８）。このとき、業務サーバ２では、認証処理部２１６が、受信した認証リクエストに含まれるログイン操作により入力されたユーザ識別情報、パスワード等を含むログイン情報を抽出してログインＤＢ２２２に記憶させる。

その後、業務サーバ２では、認証処理部２１６が、認証処理を開始する（ステップＳ３１９）。次に、業務サーバ２の認証処理部２１６は、認証が成功したと判定すると（ステップＳ３２０）、端末装置１と業務サーバ２との間のセッションを確立する（ステップＳ３２１）。続いて、アクセス要求に対応するデータが、業務サーバ２から端末装置１へ送信される（ステップＳ３２２）。一方、端末装置１では、データを受信すると、データ取得部１１３が、受信したデータをストレージに記憶させる（ステップＳ３２３）。

また、端末装置２１のリクエスト送信部２１１２が、アクセス制御用ＵＲＬ情報が示すアクセス制御用ワンタイムＵＲＬを表示部１０３に表示させているとする（ステップＳ３２４）。このとき、受付部２１１１は、表示部１０３に表示されるアクセス制御用ワンタイムＵＲＬが選択された状態で、ユーザが入力部１０５を介してアクセス制御用ワンタイムＵＲＬをクリックする操作を行うと、そのアクセス制御用ワンタイムＵＲＬクリック操作を受け付ける（ステップＳ３２５）。

その後、図８に示すように、アクセス制御用ワンタイムＵＲＬへアクセスすることを要求するアクセス要求が、端末装置２１から業務サーバ２へ送信される（ステップＳ３２６）。次に、アクセス制御用ワンタイムＵＲＬで指定される切替情報が、業務サーバ２から端末装置２１へ送信される（ステップＳ３２７）。

続いて、端末装置２１の表示部１０３に切替操作画面が表示された状態で、ユーザが入力部１０５を介して切替操作を行うと、端末装置１の受付部２１１１が、切替操作を受け付ける（ステップＳ３２８）。その後、業務サーバ２の認証機能の切替を要求する切替リクエストが、端末装置２１から業務サーバ２へ送信される（ステップＳ３２９）。

一方、業務サーバ２では、状態設定部２１５が、切替リクエストを受信すると、業務サーバ２を、認証処理部２１６による認証処理が許可される認証機能非アクティブ状態に設定する（ステップＳ３３０）。

その後、端末装置１において、データ取得部１１３が、ＵＲＬ情報が示すワンタイムＵＲＬを表示部１０３に表示させた後（ステップＳ３３１）、そのワンタイムＵＲＬクリック操作を受け付けたとする（ステップＳ３３２）。この場合、ワンタイムＵＲＬへアクセスすることを要求するアクセス要求が、端末装置１から業務サーバ２へ送信される（ステップＳ３３３）。このとき、業務サーバ２が認証機能非アクティブ状態に設定されているので、認証処理部２１６は、認証処理の実行を回避する。

また、ログイン用ワンタイムＵＲＬおよびアクセス制御用ワンタイムＵＲＬの有効期限が到来すると、業務サーバ２では、ＵＲＬ生成部２１２が、ログイン用ワンタイムＵＲＬおよびアクセス制御用ワンタイムＵＲＬを失効させる（ステップＳ３３４）。

ここで、例えばステップＳ３２１において業務サーバ２と端末装置１との間でセッションが確立している状態で、端末装置２１から切替リクエストが業務サーバ２へ送信されたとする。この場合、業務サーバ２が強制的に認証機能非アクティブ状態に設定されると、強制的にセッションが無効化される。

このように、本構成によれば、ログイン用ワンタイムＵＲＬが一度生成されると、ログイン用ワンタイムＵＲＬが再度端末装置１へ送信されなくても、同一のログイン用ワンタイムＵＲＬを用いたアクセス制御ができる。

また、本構成によれば、管理者が所持する端末装置２１から業務サーバ２の認証機能を切り替えることができるので、業務サーバ２の管理者の利便性が向上する。また、本構成によれば、ログイン用ワンタイムＵＲＬを通知した後、ユーザ認証が行われる。そして、第２端末装置からアクセス制御用ワンタイムＵＲＬへアクセスすることにより、業務サーバ２の認証機能をアクティブまたは非アクティブに切替えることができる。

なお、本変形例において、アクセス制御用ワンタイムＵＲＬとして、業務サーバ２を認証機能アクティブにするためのものと、認証機能非アクティブにするためのものとの２つが存在してもよい。或いは、アクセス制御用ワンタイムＵＲＬは、３種類以上あってもよいし、業務サーバ２を認証機能アクティブにするためのアクセス制御用ワンタイムＵＲＬと、認証機能非アクティブにするためのアクセス制御用ワンタイムＵＲＬとが、それぞれ２種類以上存在してもよい。

或いは、ＵＲＬ生成部２１２が、アクセス制御用ワンタイムＵＲＬの有効状態と無効状態とを切り替えるための第３ワンタイムＵＲＬを生成するものであってもよい。

前述の変形例において、業務サーバ２の状態設定部２１５が、端末装置２１からアクセス要求を受信すると、業務サーバ２を、認証処理部２１６による認証処理が許可される認証機能アクティブ状態または非アクティブ状態に設定するものであってもよい。即ち、端末装置２１から送信されるアクセス要求が、切替リクエストとして機能する構成であってもよい。この場合、図７のステップＳ３１０乃至Ｓ３１２および図８のステップＳ３２７乃至Ｓ３２９の処理が省略されるので、処理の簡素化が図られる。

また、本発明に係る端末装置１、業務サーバ２の各種機能は、専用のシステムによらず、通常のコンピュータシステムを用いて実現可能である。例えば、ネットワークに接続されているコンピュータに、上記動作を実行するためのプログラムを、コンピュータシステムが読み取り可能な非一時的な記録媒体（ＣＤ－ＲＯＭ(Compact Disc Read Only Memory)等）に格納して配布し、当該プログラムをコンピュータシステムにインストールすることにより、上述の処理を実行する端末装置１、業務サーバ２を構成してもよい。

また、コンピュータにプログラムを提供する方法は任意である。例えば、プログラムは、通信回線の掲示版（ＢＢＳ (Bulletin Board System)）にアップロードされ、通信回線

を介してコンピュータに配信されてもよい。そして、コンピュータは、このプログラムを起動して、ＯＳ(Operating System)の制御の下、他のアプリケーションと同様に実行する。これにより、コンピュータは、上述の処理を実行する端末装置１、業務サーバ２として機能する。

以上、本発明の各実施の形態および変形例（なお書きに記載したものを含む。以下、同様。）について説明したが、本発明はこれらに限定されるものではない。本発明は、実施の形態及び変形例が適宜組み合わされたもの、それに適宜変更が加えられたものを含む。

産業上の利用可能性

本発明は、シングルサインオンを実行するクライアントサーバシステムに好適である。

符号の説明

１：端末装置、２：業務サーバ、３：認証サーバ、１０１，２０１，３０１：ＣＰＵ、１０２，２０２，３０２：ストレージ、１０３：表示部、１０４，２０４，３０４：通信部、１０５：入力部、１１１：ログイン受付部、１１２，２１１２：リクエスト送信部、１１３：データ取得部、２０２，３０２：ストレージ、２１１：リクエスト受信部、２１２：ＵＲＬ生成部、２１３：有効期限設定部、２１４：ＵＲＬ送信部、２１５：状態設定部、２１６：認証処理部、２１７：データ送信部、２２１：業務ＤＢ、２２２：ログインＤＢ、３１１：アクセス権限判定部、３１２：権限有無通知部、３２１：リポジトリ、２１１１：受付部、ＮＴ：ネットワーク

請求の範囲

[請求項１]

第１端末装置と、第２端末装置と、サーバと、を備えるクライアントサーバシステムであって、

前記第１端末装置は、

前記サーバから受信した第１アクセス情報に基づいて、アクセス要求を前記サーバへ送信することにより、前記サーバからデータを取得するデータ取得部を有し、

前記第２端末装置は、

前記サーバから受信した第２アクセス情報に基づいて、前記サーバの状態を切り替える切替リクエストを前記サーバへ送信することにより、前記サーバの状態を切り替えるリクエスト送信部を有し、

前記サーバは、

前記第１アクセス情報および前記第２アクセス情報を生成するアクセス情報生成部と、

前記第１アクセス情報および前記第２アクセス情報の有効期限を設定する有効期限設定部と、

前記第１アクセス情報を前記第１端末装置へ送信するとともに、前記第２アクセス情報を前記第２端末装置へ送信するアクセス情報送信部と、

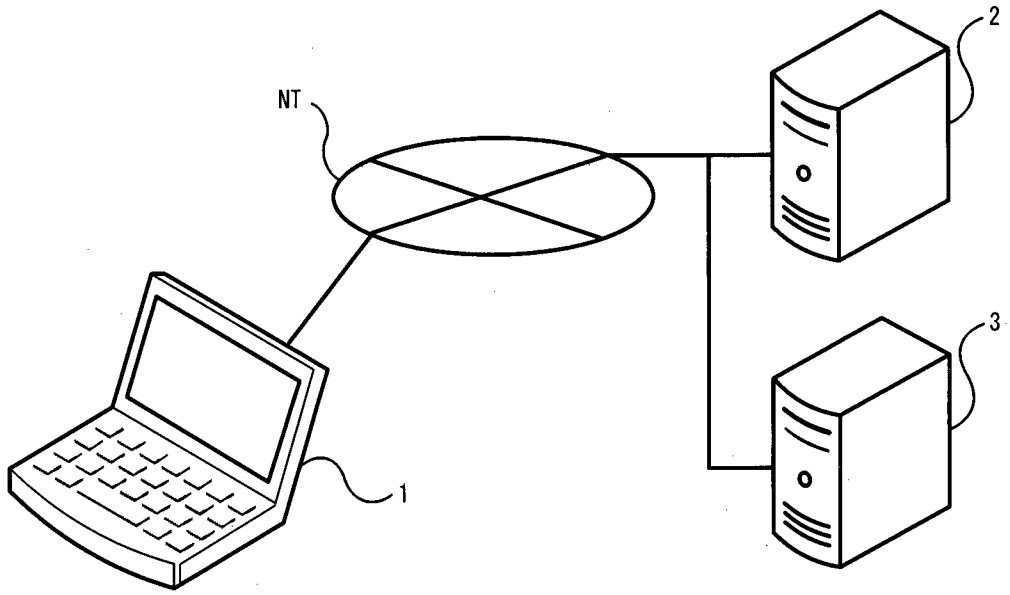
前記アクセス要求の送信元を認証するための認証処理を実行する認証処理部と、

前記切替リクエストを受信すると、前記認証処理部による認証処理の実行が許可される第１状態と、前記認証処理部による認証処理の実行が禁止される第２状態とのいずれかの状態に設定する状態設定部と、を有し、

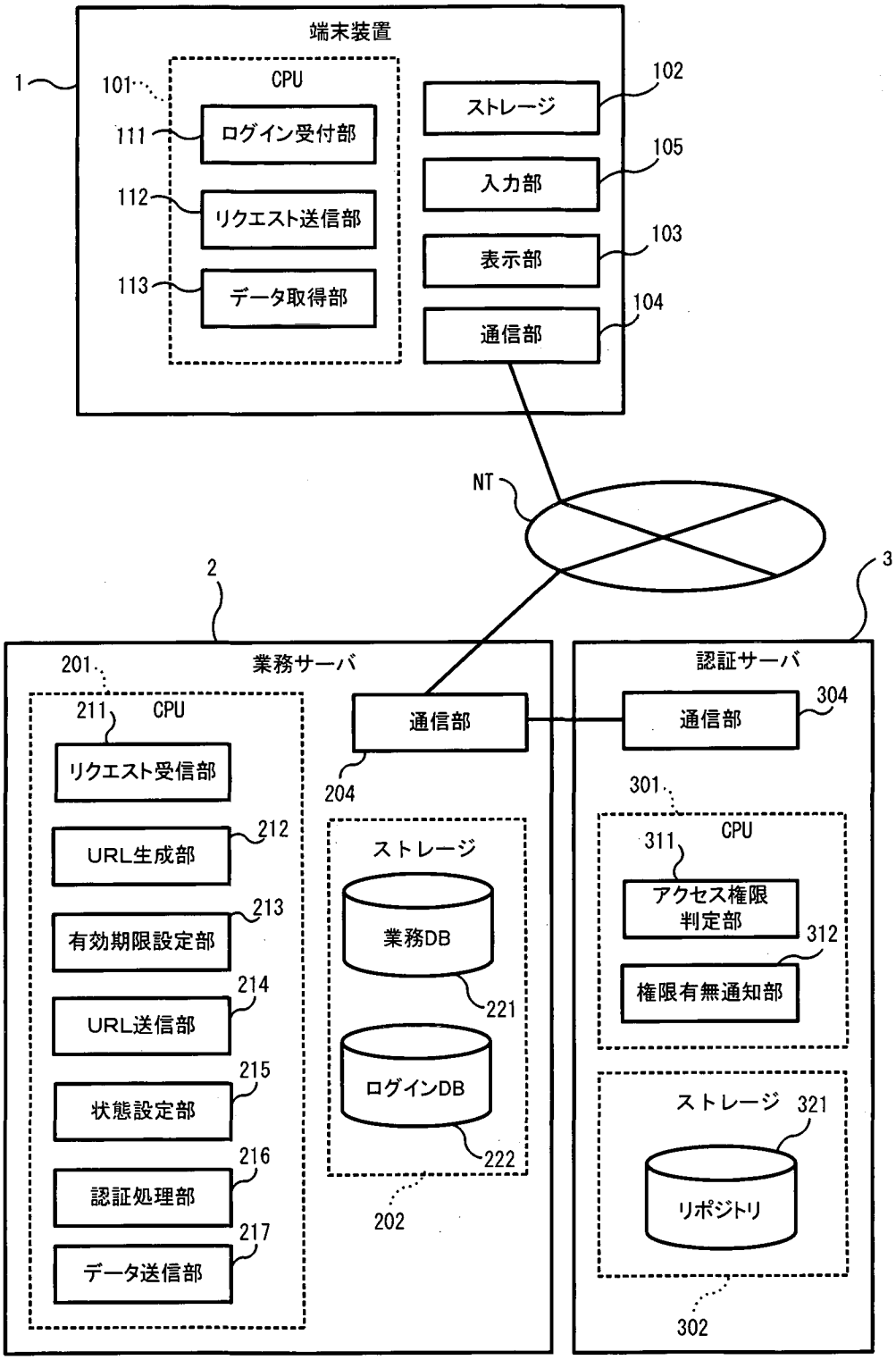
前記認証処理部は、前記データ取得部から前記アクセス要求を受信した場合、前記第１状態に設定されているとき、前記認証処理を開始し、前記第２状態に設定されているとき、前記認証処理の実行を回避する、

クライアントサーバシステム。

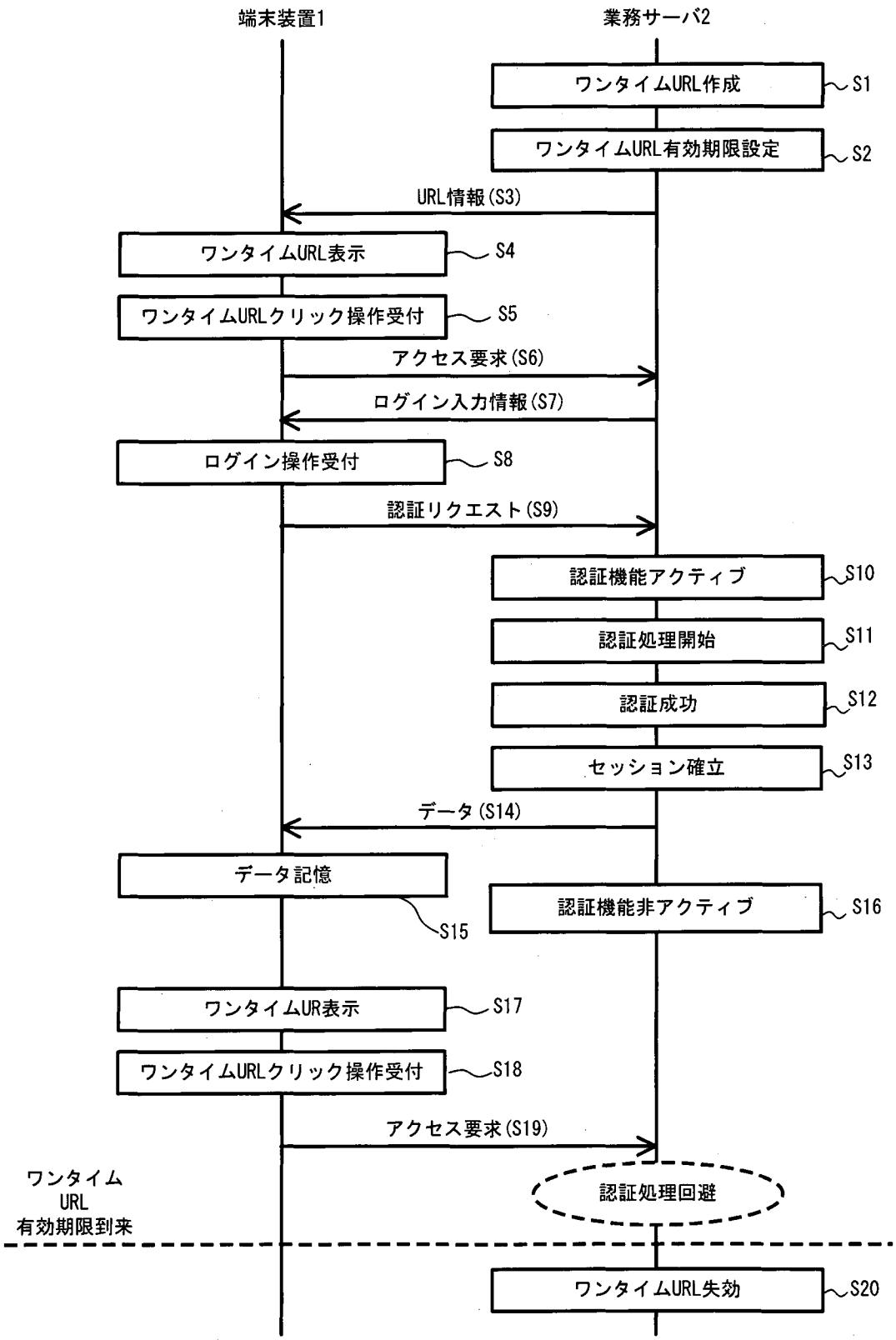
[図１]



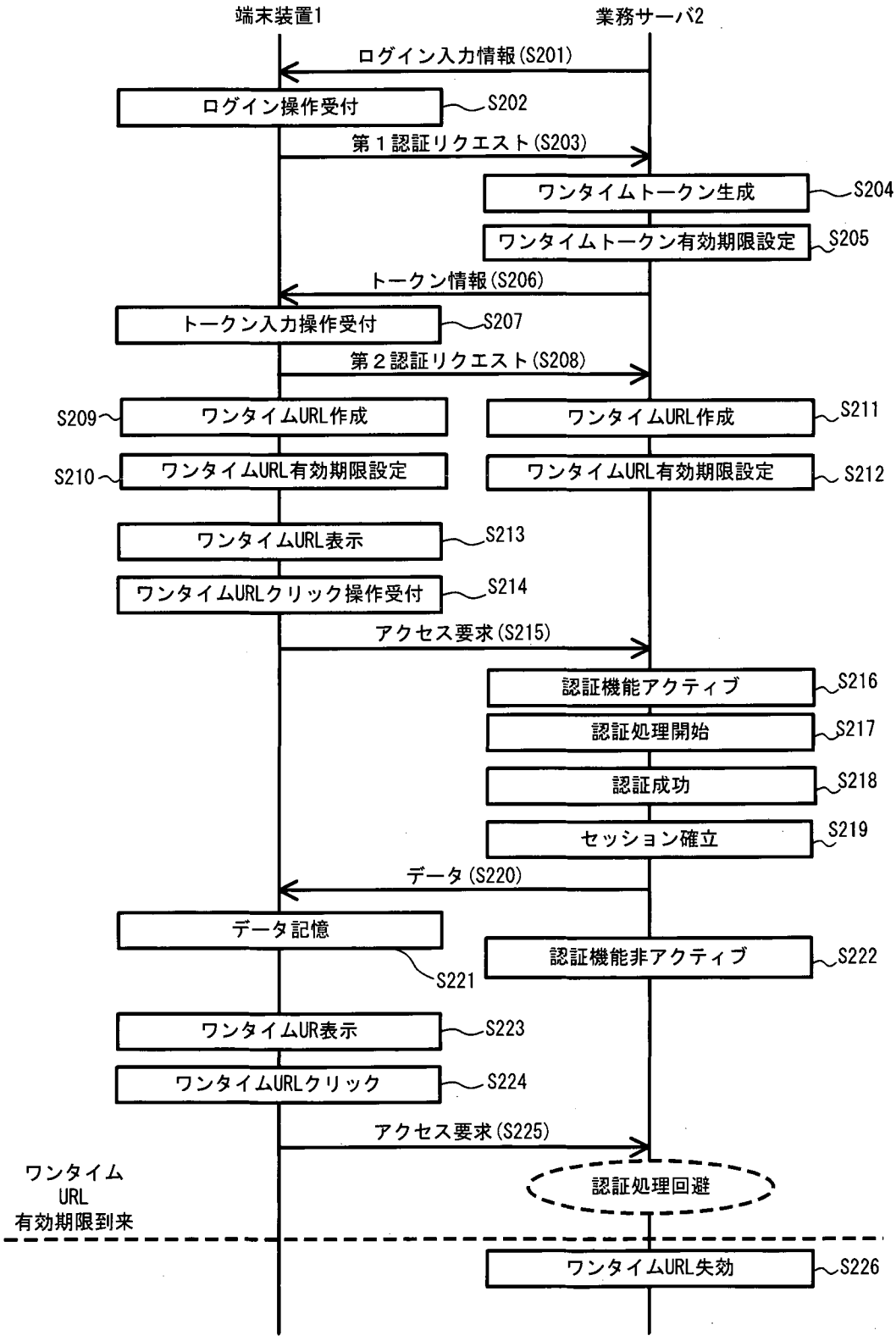
[図２]


端末装置
1
101
CPU
111
ログイン受付部
112
リクエスト送信部
113
データ取得部
102
ストレージ
105
入力部
103
表示部
104
通信部
NT
2
3
201
業務サーバ
211
CPU
リクエスト受信部
212
URL生成部
213
有効期限設定部
214
URL送信部
215
状態設定部
216
認証処理部
217
データ送信部
通信部
204
ストレージ
業務DB
221
ログインDB
222
202
認証サーバ
通信部
304
301
CPU
311
アクセス権限判定部
312
権限有無通知部
ストレージ
321
リポジトリ
302

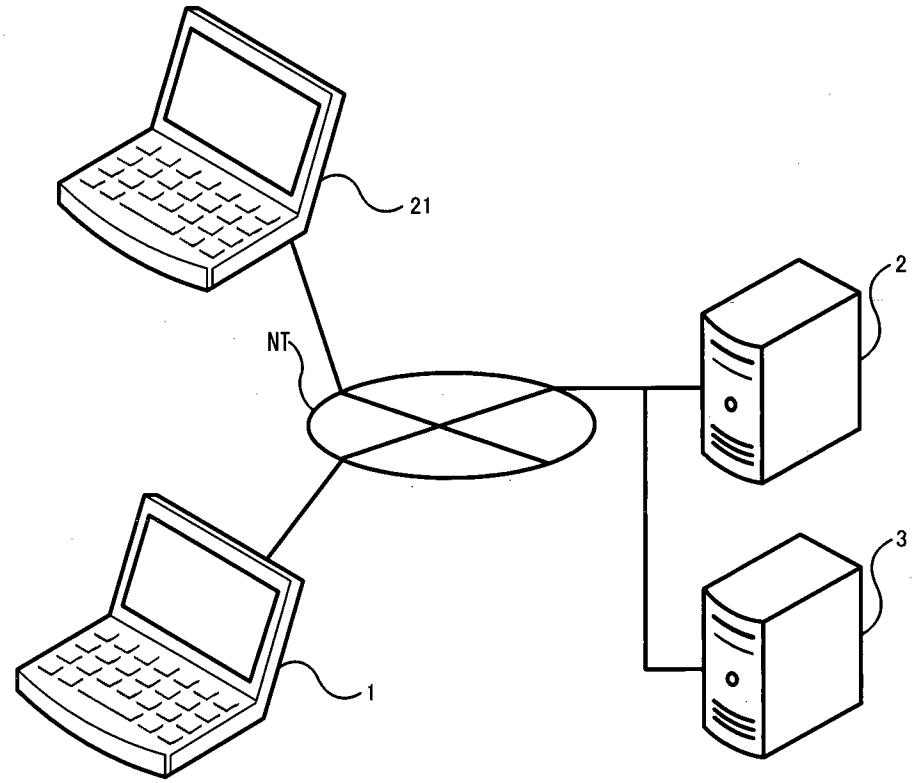
[図３]


端末装置1
業務サーバ2
ワンタイムURL作成
S1
ワンタイムURL有効期限設定
S2
URL情報(S3)
ワンタイムURL表示
S4
ワンタイムURLクリック操作受付
S5
アクセス要求(S6)
ログイン入力情報(S7)
ログイン操作受付
S8
認証リクエスト(S9)
認証機能アクティブ
S10
認証処理開始
S11
認証成功
S12
セッション確立
S13
データ(S14)
データ記憶
S15
認証機能非アクティブ
S16
ワンタイムUR表示
S17
ワンタイムURLクリック操作受付
S18
アクセス要求(S19)
ワンタイム
URL
有効期限到来
認証処理回避
ワンタイムURL失効
S20

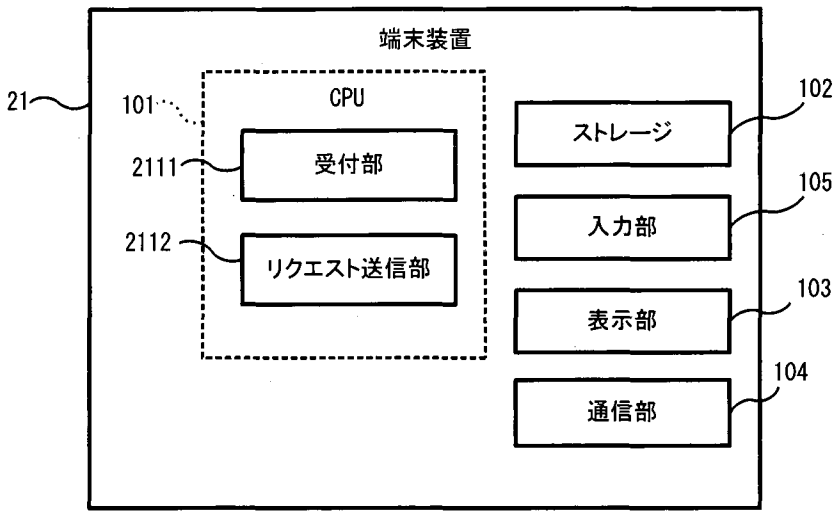
[図４]


端末装置1
業務サーバ2
ログイン入力情報(S201)
ログイン操作受付
S202
第１認証リクエスト(S203)
ワンタイムトークン生成
S204
ワンタイムトークン有効期限設定
S205
トークン情報(S206)
トークン入力操作受付
S207
第２認証リクエスト(S208)
S209
ワンタイムURL作成
ワンタイムURL作成
S211
S210
ワンタイムURL有効期限設定
ワンタイムURL有効期限設定
S212
ワンタイムURL表示
S213
ワンタイムURLクリック操作受付
S214
アクセス要求(S215)
認証機能アクティブ
S216
認証処理開始
S217
認証成功
S218
セッション確立
S219
データ(S220)
データ記憶
S221
認証機能非アクティブ
S222
ワンタイムUR表示
S223
ワンタイムURLクリック
S224
アクセス要求(S225)
ワンタイム
URL
有効期限到来
認証処理回避
ワンタイムURL失効
S226

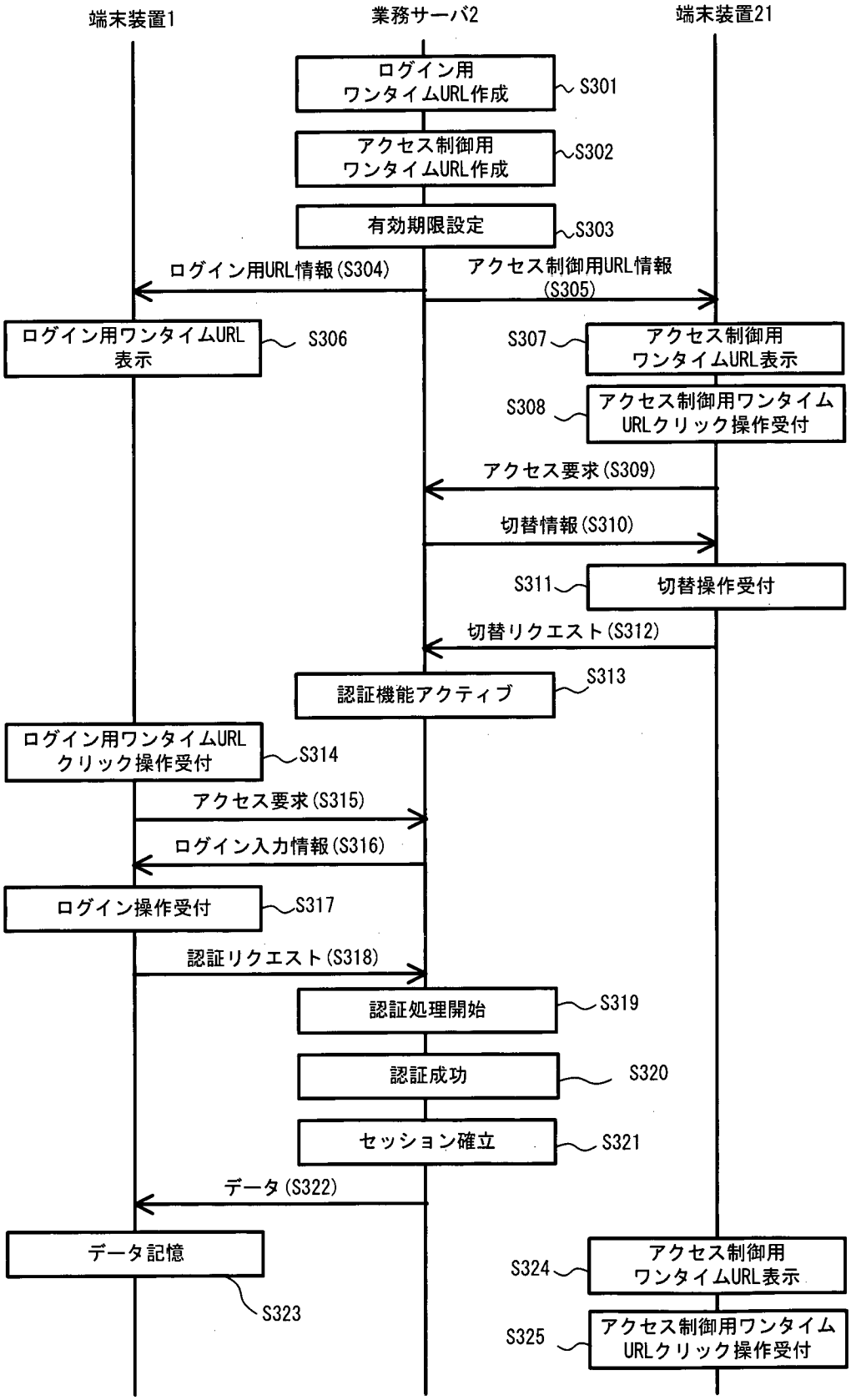
[図５]



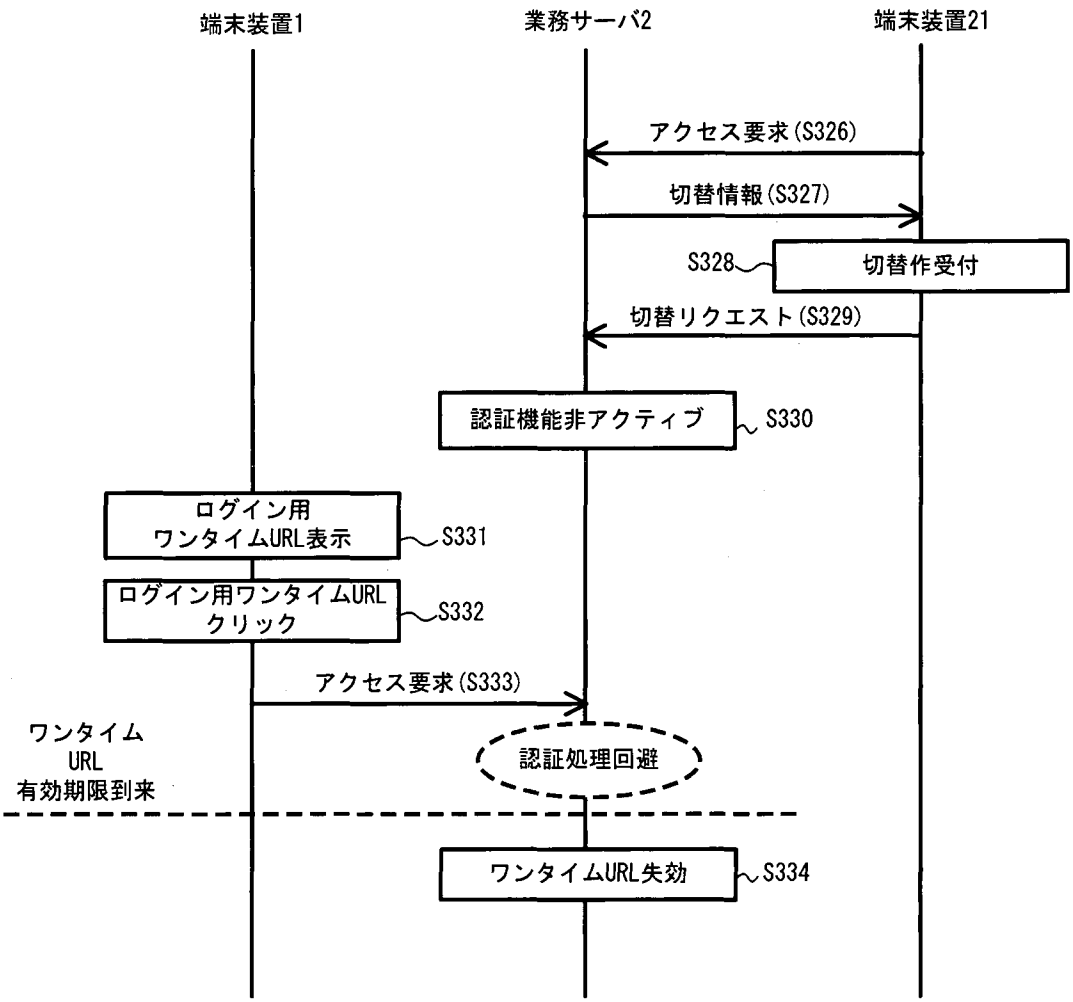
[図６]


端末装置
21
101
CPU
2111
受付部
2112
リクエスト送信部
ストレージ
102
入力部
105
表示部
103
通信部
104

[図７]


端末装置1
業務サーバ2
端末装置21
ログイン用
ワンタイムURL作成
S301
アクセス制御用
ワンタイムURL作成
S302
有効期限設定
S303
ログイン用URL情報(S304)
アクセス制御用URL情報
(S305)
ログイン用ワンタイムURL
表示
S306
S307
アクセス制御用
ワンタイムURL表示
S308
アクセス制御用ワンタイム
URLクリック操作受付
アクセス要求(S309)
切替情報(S310)
S311
切替操作受付
切替リクエスト(S312)
認証機能アクティブ
S313
ログイン用ワンタイムURL
クリック操作受付
S314
アクセス要求(S315)
ログイン入力情報(S316)
ログイン操作受付
S317
認証リクエスト(S318)
認証処理開始
S319
認証成功
S320
セッション確立
S321
データ(S322)
データ記憶
S323
S324
アクセス制御用
ワンタイムURL表示
S325
アクセス制御用ワンタイム
URLクリック操作受付

[図８]


端末装置1
業務サーバ2
端末装置21
アクセス要求(S326)
切替情報(S327)
S328
切替作受付
切替リクエスト(S329)
認証機能非アクティブ
S330
ログイン用
ワンタイムURL表示
S331
ログイン用ワンタイムURL
クリック
S332
アクセス要求(S333)
ワンタイム
URL
有効期限到来
認証処理回避
ワンタイムURL失効
S334

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2018/038234

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl. G06F21/31(2013.01)i, G06F13/00(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)
Int.Cl. G06F21/31, G06F13/00

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

Published examined utility model applications of Japan	1922-1996
Published unexamined utility model applications of Japan	1971-2018
Registered utility model specifications of Japan	1996-2018
Published registered utility model applications of Japan	1994-2018

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 2015-231177 A (NIPPON TELEGRAPH AND TELEPHONE CORP.) 21 December 2015, paragraphs [0021]-[0025], [0043]-[0048], fig. 1-3, 8-9 (Family: none)	1
A	JP 2015-103194 A (CANON INC.) 04 June 2015, paragraphs [0015]-[0019], [0024], [0033]-[0038], [0049]-[0056], fig. 1, 3-4, 6 (Family: none)	1
A	JP 2012-99912 A (OLYMPUS CORP.) 24 May 2012, paragraphs [0105]-[0106], [0112]-[0114], [0117]-[0119], fig. 13, 15 & US 2012/0106449 A1, paragraphs [0136]-[0137], [0143]-[0145], [0148]-[0149], fig. 13, 15	1
A	KR 2003-0092920 A (HYUNDAI SYSCOMM INC.) 06 December 2003, page 1, lines 2-8, page 6, lines 30-35 (Family: none)	1

☐ 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 06 December 2018 (06.12.2018)	Date of mailing of the international search report 18 December 2018 (18.12.2018)
Name and mailing address of the ISA/ Japan Patent Office 3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan	Authorized officer Telephone No.

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１８／０３８２３４

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　G06F21/31(2013.01)i, G06F13/00(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.　G06F21/31, G06F13/00

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	１９７１－２０１８年
日本国実用新案登録公報	１９９６－２０１８年
日本国登録実用新案公報	１９９４－２０１８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 2015-231177 A（日本電信電話株式会社）2015.12.21, 段落［００２１］－［００２５］、［００４３］－［００４８］、図１－３、８－９（ファミリーなし）	1
Ａ	JP 2015-103194 A（キヤノン株式会社）2015.06.04, 段落［００１５］－［００１９］、［００２４］、［００３３］－［００３８］、［００４９］－［００５６］、図１、３－４、６（ファミリーなし）	1

☑　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 ０６．１２．２０１８	国際調査報告の発送日 １８．１２．２０１８
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　４２２９ 青木　重徳 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
Ａ	JP 2012-99912 A (オリンパス株式会社) 2012.05.24, 段落［０１０５］－［０１０６］、［０１１２］－［０１１４］、［０１１７］－［０１１９］、図１３、１５ & US 2012/0106449 A1, 段落［０１３６］－［０１３７］、［０１４３］－［０１４５］、［０１４８］－［０１４９］、ＦＩＧ．１３、１５	1
Ａ	KR 2003-0092920 A (HYUNDAI SYSCOMM INC.) 2003.12.06, 第１頁第２－８行、第６頁第３０－３５行（ファミリーなし）	1