(19)日本国特許庁(JP)　(12)特　許　公　報(B1)　(11)特許番号

特許第6495996号
(P6495996)

(45)発行日　平成31年4月3日(2019.4.3)　(24)登録日　平成31年3月15日(2019.3.15)

(51)Int.Cl.		F I		
G06F 13/00	(2006.01)	G06F	13/00	510A
G06F 21/41	(2013.01)	G06F	21/41	
H04L 9/32	(2006.01)	H04L	9/00	673D

請求項の数 11　(全 14 頁)

(21)出願番号　特願2017-212729 (P2017-212729)
(22)出願日　平成29年11月2日 (2017.11.2)
審査請求日　平成29年11月2日 (2017.11.2)

(73)特許権者　592131906
みずほ情報総研株式会社
東京都千代田区神田錦町二丁目３番地
(73)特許権者　592052416
株式会社　みずほ銀行
東京都千代田区大手町一丁目５番５号
(74)代理人　100105957
弁理士　恩田　誠
(74)代理人　100068755
弁理士　恩田　博宣
(72)発明者　永井　哲也
東京都千代田区神田錦町二丁目３番地　みずほ情報総研　株式会社　内

最終頁に続く

(54)【発明の名称】ログイン管理システム、ログイン管理方法及びログイン管理プログラム

(57)【特許請求の範囲】
【請求項１】
引継情報を記憶する引継情報記憶部と、
ユーザ端末、関連サーバに接続される制御部とを備えたログイン管理システムであって、
前記制御部が、
前記ユーザ端末からログイン要求を受け付けた場合、前記ユーザ端末から取得した認証情報を用いて第１の認証処理を実行してログインを許可し、
前記ログインしたユーザ端末から前記関連サーバへの遷移要求を取得した場合、引継情報を生成し、前記引継情報記憶部に記録し、前記関連サーバに対して前記引継情報を提供し、
前記関連サーバから、前記引継情報を取得した場合、パスワードを生成して前記引継情報記憶部に記録して、前記関連サーバに提供し、
前記ユーザ端末から、再ログイン要求を受け付けた場合、前記引継情報及び前記パスワードを前記関連サーバから取得し、前記引継情報記憶部に記録された引継情報及びパスワードと、前記取得した引継情報及びパスワードとを用いて第２の認証処理を実行することを特徴とするログイン管理システム。
【請求項２】
引継情報を記憶する引継情報記憶部と、
ユーザ端末、関連サーバに接続される制御部とを備えたログイン管理システムであって

、
前記制御部が、
前記ユーザ端末からログイン要求を受け付けた場合、前記ユーザ端末から取得した認証情報を用いて第１の認証処理を実行して、ユーザＩＤを特定してログインを許可し、
前記ログインしたユーザ端末から前記関連サーバへの遷移要求を取得した場合、引継情報を生成し、前記ユーザＩＤに関連付けて前記引継情報記憶部に記録し、前記関連サーバに対して前記引継情報を提供し、
前記関連サーバから、前記引継情報を取得した場合、前記引継情報記憶部に記録されたユーザＩＤに関連付けられた個人情報を前記関連サーバで利用できるように提供し、
前記ユーザ端末から、再ログイン要求を受け付けた場合、前記引継情報を前記関連サーバから取得し、前記引継情報記憶部に記録された引継情報と、前記取得した引継情報とを用いて第２の認証処理を実行することを特徴とするログイン管理システム。
【請求項３】
前記再ログイン要求の受け付け時に、前記認証情報を、前記関連サーバから前記ユーザ端末を介してのリダイレクトにより取得することを特徴とする請求項１又は２に記載のログイン管理システム。
【請求項４】
前記認証情報は、有効期間が設定されているワンタイム認証情報であることを特徴とする請求項１～３の何れか一項に記載のログイン管理システム。
【請求項５】
前記制御部が、前記有効期間を、前記関連サーバの種類に応じて設定することを特徴とする請求項４に記載のログイン管理システム。
【請求項６】
前記制御部が、前記有効期間を、前記関連サーバにおける利用状況に応じて設定することを特徴とする請求項４又は５に記載のログイン管理システム。
【請求項７】
前記制御部が、前記有効期間を、前記ユーザ端末における前記関連サーバの利用履歴に応じて設定することを特徴とする請求項４～６のいずれか一項に記載のログイン管理システム。
【請求項８】
引継情報を記憶する引継情報記憶部と、
ユーザ端末、関連サーバに接続される制御部とを備えたログイン管理システムを用いてログインを管理する方法であって、
前記制御部が、
前記ユーザ端末からログイン要求を受け付けた場合、前記ユーザ端末から取得した認証情報を用いて第１の認証処理を実行してログインを許可し、
前記ログインしたユーザ端末から前記関連サーバへの遷移要求を取得した場合、引継情報を生成し、前記引継情報記憶部に記録し、前記関連サーバに対して前記引継情報を提供し、
前記関連サーバから、前記引継情報を取得した場合、パスワードを生成して前記引継情報記憶部に記録して、前記関連サーバに提供し、
前記ユーザ端末から、再ログイン要求を受け付けた場合、前記引継情報及び前記パスワードを前記関連サーバから取得し、前記引継情報記憶部に記録された引継情報及びパスワードと、前記取得した引継情報及びパスワードとを用いて第２の認証処理を実行することを特徴とするログイン管理方法。
【請求項９】
引継情報を記憶する引継情報記憶部と、
ユーザ端末、関連サーバに接続される制御部とを備えたログイン管理システムを用いてログインを管理する方法であって、
前記制御部が、

前記ユーザ端末からログイン要求を受け付けた場合、前記ユーザ端末から取得した認証情報を用いて第１の認証処理を実行して、ユーザＩＤを特定してログインを許可し、
前記ログインしたユーザ端末から前記関連サーバへの遷移要求を取得した場合、引継情報を生成し、前記ユーザＩＤに関連付けて前記引継情報記憶部に記録し、前記関連サーバに対して前記引継情報を提供し、
前記関連サーバから、前記引継情報を取得した場合、前記引継情報記憶部に記録されたユーザＩＤに関連付けられた個人情報を前記関連サーバで利用できるように提供し、
前記ユーザ端末から、再ログイン要求を受け付けた場合、前記引継情報を前記関連サーバから取得し、前記引継情報記憶部に記録された引継情報と、前記取得した引継情報とを用いて第２の認証処理を実行することを特徴とするログイン管理方法。

【請求項１０】
引継情報を記憶する引継情報記憶部と、
ユーザ端末、関連サーバに接続される制御部とを備えたログイン管理システムを用いてログインを管理するためのプログラムであって、
前記制御部を、
前記ユーザ端末からログイン要求を受け付けた場合、前記ユーザ端末から取得した認証情報を用いて第１の認証処理を実行してログインを許可し、
前記ログインしたユーザ端末から前記関連サーバへの遷移要求を取得した場合、引継情報を生成し、前記引継情報記憶部に記録し、前記関連サーバに対して前記引継情報を提供し、
前記関連サーバから、前記引継情報を取得した場合、パスワードを生成して前記引継情報記憶部に記録して、前記関連サーバに提供し、
前記ユーザ端末から、再ログイン要求を受け付けた場合、前記引継情報及び前記パスワードを前記関連サーバから取得し、前記引継情報記憶部に記録された引継情報及びパスワードと、前記取得した引継情報及びパスワードとを用いて第２の認証処理を実行する手段として機能させることを特徴とするログイン管理プログラム。

【請求項１１】
引継情報を記憶する引継情報記憶部と、
ユーザ端末、関連サーバに接続される制御部とを備えたログイン管理システムを用いてログインを管理するためのプログラムであって、
前記制御部を、
前記ユーザ端末からログイン要求を受け付けた場合、前記ユーザ端末から取得した認証情報を用いて第１の認証処理を実行して、ユーザＩＤを特定してログインを許可し、
前記ログインしたユーザ端末から前記関連サーバへの遷移要求を取得した場合、引継情報を生成し、前記ユーザＩＤに関連付けて前記引継情報記憶部に記録し、前記関連サーバに対して前記引継情報を提供し、
前記関連サーバから、前記引継情報を取得した場合、前記引継情報記憶部に記録されたユーザＩＤに関連付けられた個人情報を前記関連サーバで利用できるように提供し、
前記ユーザ端末から、再ログイン要求を受け付けた場合、前記引継情報を前記関連サーバから取得し、前記引継情報記憶部に記録された引継情報と、前記取得した引継情報とを用いて第２の認証処理を実行する手段として機能させることを特徴とするログイン管理プログラム。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、複数のサーバへのログインを管理するためのログイン管理システム、ログイン管理方法及びログイン管理プログラムに関する。
【背景技術】
【０００２】
特定のユーザに対してサービスを提供する場合、ログイン手続きによりユーザを認証す

ることがある。ここで、ログイン手続きが煩雑な場合、サービスの利用促進を図ることができない。そこで、予めユーザ名とパスワードを記憶しておき、必要な時に自動的にログインを行なうオートログイン方式が検討されている（例えば、特許文献１を参照。）。この文献に記載の技術では、ユーザ装置に接続されるアグリゲーションサーバは、サーバにログインするためのユーザ別ログイン情報を、ユーザの識別情報と対応付けて記憶するログイン情報記憶部を備える。ユーザ装置から入力されたユーザ識別情報に基づいて、ログイン情報記憶部のユーザ別ログイン情報を取得して暗号化を行ない、暗号情報を復号するための復号キーの入力を受け付けるための画面情報を、ユーザ装置に対して出力する。

【０００３】

また、関連する複数のサーバを利用する場合には、一度の利用者認証で複数のコンピュータやソフトウェア、サービスなどを利用できるようにするシングルサインオン方式も検討されている。このシングルサインオン技術では、複数のシステムから横断して利用できる認証基盤を用意し、利用者は一度の認証作業で連携するすべてのシステムにアクセスできるようにする。この場合、認証情報を動的に更新するシングルサインオンシステムも検討されている（例えば、特許文献２を参照。）。この文献に記載の技術では、複数のウェブサーバに対するユーザＩＤ及びパスワードを含む認証情報並びにパスワードの有効期限情報を格納するシングルサインオンデータベースと、シングルサイン機能を制御するシングルサインオンサーバとを備える。このシングルサインオンサーバが、利用者端末から任意のウェブサーバにアクセスするための認証情報を受け付けたとき、このパスワードが有効期限を越えているか否かを判定し、この有効期限を越えていると判定したとき、新たなパスワードを生成し、シングルサインオンデータベースの認証情報のパスワードを更新する。

【先行技術文献】

【特許文献】

【０００４】

【特許文献１】特開２００７－５８４８７号公報

【特許文献２】特開２０１２－３３０４２号公報

【発明の概要】

【発明が解決しようとする課題】

【０００５】

金融機関においても、決済系サービスを提供する決済サイトとともに、顧客とのコミュニケーション強化のために情報系サービスを提供する関連サイトを利用することがある。このような状況でオートログイン方式を用いると、ユーザによるパスワード事前登録や、パスワードを変更した場合に各サイトでの再登録が必要となる。更に、決済系サービス及び情報系サービスを、シームレスに利用することができず、サービスの一体感を実現できない場合もある。また、決済サイト及び関連サイトの管理形態に応じて、各サイトの認証強度が異なる場合もある。このような状況でシングルサインオンを許容した場合、複数のサイトに対する広いアクセス権が与えられることになる。このため、サイト間を行き来するシングルサインオン時の認証強度を高める必要がある。例えば、認証強度が低いサイトを踏み台にして、高い認証強度が求められるサイトを利用できると、全体の認証強度の低下を招く可能性がある。

【課題を解決するための手段】

【０００６】

上記課題を解決するために、ログイン管理システムは、引継情報を記憶する引継情報記憶部と、ユーザ端末、関連サーバに接続される制御部とを備える。そして、前記制御部が、前記ユーザ端末からログイン要求を受け付けた場合、前記ユーザ端末から取得した認証情報を用いて第１の認証処理を実行してログインを許可し、前記ログインしたユーザ端末から前記関連サーバへの遷移要求を取得した場合、引継情報を生成し、前記引継情報記憶部に記録し、前記関連サーバに対して前記引継情報を提供し、前記ユーザ端末から、再ログイン要求を受け付けた場合、前記引継情報を前記関連サーバから取得し、前記引継情報

記憶部に記録された引継情報と、前記取得した引継情報とを用いて第２の認証処理を実行する。

【発明の効果】

【０００７】

本発明によれば、連携する複数のサーバへの効率的なログインを的確に管理することができる。

【図面の簡単な説明】

【０００８】

【図１】本実施形態のシステム概略図。

【図２】本実施形態の情報記憶部の説明図であって、（ａ）は第１サーバのユーザ情報記憶部、（ｂ）は第１サーバの引継情報記憶部、（ｃ）は第２サーバのユーザ情報記憶部。

【図３】本実施形態の処理手順の説明図。

【図４】本実施形態の処理手順の説明図。

【発明を実施するための形態】

【０００９】

以下、図１～図４を用いて、ログイン管理システムの一実施形態を説明する。

図１に示すように、本実施形態では、インターネット等のネットワークを介してユーザ端末１０に接続された第１サーバ２０及び第２サーバ３０（関連サーバ）を用いる。第１サーバ２０及び第２サーバ３０は連携して、ユーザ端末１０に対するサービスを提供する。

【００１０】

ユーザ端末１０は、第１サーバ２０及び第２サーバ３０を利用するユーザのコンピュータ端末である。このユーザ端末１０は、ディスプレイ等の出力部、キーボード及びポインティングデバイス等の入力部を備えている。本実施形態では、ユーザ端末１０において起動されたブラウザ（アプリケーション）を用いて、第１サーバ２０及び第２サーバ３０にアクセスする。

【００１１】

第１サーバ２０は、ユーザに対して第１のサービスを提供するコンピュータシステムである。第１のサービスとしては、例えば、銀行が提供する決済サービスがある。この第１サーバ２０は、制御部２１、ユーザ情報記憶部２２、引継情報記憶部２４を備えている。

【００１２】

制御部２１は、制御手段（ＣＰＵ、ＲＡＭ、ＲＯＭ等）を備え、後述する処理（ユーザ認証段階、サービス管理段階、引継処理段階、サーバ認証段階等の各処理）を行なう。そのためのログイン管理プログラムを実行することにより、制御部２１は、ユーザ認証部２１１、サービス管理部２１２、引継処理部２１３、サーバ認証部２１４として機能する。

【００１３】

ユーザ認証部２１１は、第１サーバ２０にアクセスしてきたユーザを認証する処理を実行する。

サービス管理部２１２は、認証されたユーザに対してサービスを提供する処理を実行する。

【００１４】

引継処理部２１３は、第１サーバ２０から第２サーバ３０へのログイン(遷移)を支援するとともに、第２サーバ３０から第１サーバ２０へのログイン（戻り）を支援する処理を実行する。引継処理部２１３は、後述するワンタイムパスワードの有効時間（有効期間）に関するデータを保持している。

【００１５】

サーバ認証部２１４は、第１サーバ２０にアクセスしてきた他のサーバを認証する処理を実行する。このため、サーバ認証部２１４は、第１サーバ２０からの遷移を許容する第２サーバ３０のサーバＩＤを記録した関連サーバリストを保持する。

【００１６】

図２（ａ）に示すように、ユーザ情報記憶部２２には、サービスを提供するユーザを管理するためのユーザ管理レコード２２０が記録される。このユーザ管理レコード２２０は、ユーザ登録が行なわれた場合に記録される。このユーザ管理レコード２２０には、ユーザＩＤ、認証情報、ログイン状況、個人情報等に関する情報が記録される。

【００１７】

ユーザＩＤデータ領域には、第１サーバ２０において、各ユーザを特定するための識別子に関するデータが記録される。

認証情報データ領域には、第１サーバ２０において、このユーザを認証するための情報に関するデータが記録される。ユーザ認証情報としては、パスワードや生体情報を用いることができる。

【００１８】

ログイン状況データ領域には、このユーザにおける第１サーバ２０へのログイン状況を示すフラグ（ログイン済フラグ、ログアウトフラグ）が記録される。

個人情報データ領域には、このユーザの氏名や住所、連絡先、ユーザ属性等に関するデータが記録される。また、このデータ領域には、このユーザの口座情報等を記録することも可能である。

【００１９】

図２（ｂ）に示すように、引継情報記憶部２４には、連携する第２サーバ３０への遷移状況を管理するための引継管理レコード２４０が記録される。この引継管理レコード２４０は、ユーザが第１サーバ２０から第２サーバ３０に遷移する場合に記録される。この引継管理レコード２４０には、引継キー、ワンタイムパスワード、遷移日時、状況、ユーザＩＤ、遷移先に関する情報が記録される。

【００２０】

引継キーデータ領域には、サーバ間の遷移を特定するための識別子に関するデータが記録される。

ワンタイムパスワードデータ領域には、ランダムに生成した一時的なパスワード（ワンタイム認証情報）が記録される。このワンタイムパスワードは、所定の有効時間（本実施形態では１時間）のみ有効とする。

【００２１】

遷移日時データ領域には、ワンタイムパスワードを生成した年月日及び時刻に関するデータが記録される。

状況データ領域には、引継キー、ワンタイムパスワードの使用状況を特定するためのフラグが記録される。このデータ領域には、第２サーバ３０に遷移した場合には遷移済フラグが記録され、遷移先から戻った場合には、使用済フラグが記録される。

【００２２】

ユーザＩＤデータ領域には、第１サーバ２０から第２サーバ３０に遷移したユーザを特定するための識別子に関するデータが記録される。

遷移先データ領域には、ユーザの遷移先である第２サーバ３０を特定するための識別子（サーバＩＤ）に関するデータが記録される。

【００２３】

第２サーバ３０は、ユーザに対して第２のサービスを提供するコンピュータシステムである。第２のサービスとしては、例えば、銀行の決済サービスに関連する情報系サービスや、証券や保険等の金融関連サービスがある。この第２サーバ３０は、制御部３１、ユーザ情報記憶部３２を備えている。

制御部３１は、制御手段（ＣＰＵ、ＲＡＭ、ＲＯＭ等）を備え、後述する処理（ユーザ認証段階、サービス管理段階等の各処理）を行なう。そのためのログイン管理プログラムを実行することにより、制御部３１は、ユーザ認証部３１１、サービス管理部３１２として機能する。

【００２４】

ユーザ認証部３１１は、第２サーバ３０にアクセスしてきたユーザを認証する処理を実

行する。
サービス管理部３１２は、認証されたユーザに対してサービスを提供する処理を実行する。
【００２５】
図２（ｃ）に示すように、ユーザ情報記憶部３２には、サービスを提供するユーザを管理するためのユーザ管理レコード３２０が記録される。このユーザ管理レコード３２０は、ユーザ登録が行なわれた場合に記録される。このユーザ管理レコード３２０には、ユーザＩＤ、認証情報、ログイン状況、個人情報等に関する情報が記録される。
【００２６】
ユーザＩＤデータ領域には、第２サーバ３０において、各ユーザを特定するための識別子に関するデータが記録される。
認証情報データ領域には、第２サーバ３０において、このユーザを認証するための情報に関するデータが記録される。
【００２７】
ログイン状況データ領域には、このユーザにおける第２サーバ３０へのログイン状況を示すフラグ（ログイン済フラグ、ログアウトフラグ）が記録される。
個人情報データ領域には、このユーザの氏名や住所、連絡先、ユーザ属性等に関するデータが記録される。
【００２８】
（遷移処理）
図３、４を用いて、サービス利用処理を説明する。ここでは、第１サーバ２０が提供するサービスを利用していたユーザが、第２サーバ３０に遷移し、第２サーバ３０が提供するサービスを利用する場合を想定する。
【００２９】
図３に示すように、まず、ユーザ端末１０は、アクセス処理を実行する（ステップＳ１－１）。具体的には、ユーザが第１サーバ２０を利用する場合には、ユーザ端末１０を用いて、第１サーバ２０にアクセスする。この場合、ユーザ端末１０は、第１サーバ２０の制御部２１からログイン画面を取得し、出力部に出力する。このログイン画面には、ユーザＩＤ、認証情報を入力する。
【００３０】
次に、第１サーバ２０の制御部２１は、ユーザ認証処理を実行する（ステップＳ１－２）。具体的には、制御部２１のユーザ認証部２１１は、ログイン画面に入力されたユーザＩＤ、認証情報を取得する。ユーザ端末１０から取得したユーザＩＤ、認証情報が、ユーザ情報記憶部２２に記録されている場合には、ユーザ認証部２１１は、ユーザ認証（第１の認証処理）を完了し、ユーザ管理レコード２２０のログイン状況データ領域にログイン済フラグを記録する。なお、ユーザ端末１０から取得したユーザＩＤ、認証情報が、ユーザ情報記憶部２２に記録されていない場合には、ユーザ認証部２１１は、ログインを拒否する。
【００３１】
次に、第１サーバ２０の制御部２１は、サービス提供処理を実行する（ステップＳ１－３）。具体的には、制御部２１のサービス管理部２１２は、ユーザが希望するサービスについてのサービス画面を提供する。そして、ユーザは、ユーザ端末１０に出力されたサービス画面を用いて、所望のサービスを利用する。
【００３２】
次に、ユーザ端末１０は、遷移要求処理を実行する（ステップＳ１－４）。具体的には、ユーザが第２サーバ３０を利用する場合には、サービス画面において表示された第２サーバ３０へのリンクのボタンを選択する。この場合、ユーザ端末１０は、第１サーバ２０に対して、遷移先のサーバＩＤを含めた遷移要求電文を送信する。
【００３３】
遷移要求を取得した第１サーバ２０の制御部２１は、引継キーの生成処理を実行する（

ステップＳ１－５）。具体的には、制御部２１の引継処理部２１３は、遷移要求電文に対して、ユニークな引継キーを生成する。

【００３４】

次に、第１サーバ２０の制御部２１は、引継キーの登録処理を実行する（ステップＳ１－６）。具体的には、制御部２１の引継処理部２１３は、引継キーを記録した引継管理レコード２４０を生成し、引継情報記憶部２４に記録する。更に、引継処理部２１３は、この引継管理レコード２４０に、ログインしているユーザのユーザＩＤ、遷移先（第２サーバ３０のサーバＩＤ）を記録する。

【００３５】

次に、第１サーバ２０の制御部２１は、ログアウト処理を実行する（ステップＳ１－７）。具体的には、制御部２１の引継処理部２１３は、ユーザ管理レコード２２０のログイン状況データ領域に記録されたログイン済フラグを削除し、ログアウトフラグに更新する。

【００３６】

次に、第１サーバ２０の制御部２１は、リダイレクト応答処理を実行する（ステップＳ１－８）。具体的には、制御部２１のサービス管理部２１２は、ユーザ端末１０に対してリダイレクト要求電文を送信する。このリダイレクト要求電文には、トランザクション通番、遷移先、引継キーに関するデータを含める。このトランザクション通番は、第１サーバ２０から第２サーバ３０へのトランザクションを特定するための識別子である。

【００３７】

次に、ユーザ端末１０は、引継キーの保存処理を実行する（ステップＳ１－９）。具体的には、ユーザ端末１０は、リダイレクト要求電文に含まれる引継キーをブラウザに仮記憶する。

【００３８】

次に、ユーザ端末１０は、リダイレクト処理を実行する（ステップＳ１－１０）。具体的には、ユーザ端末１０は、遷移先である第２サーバ３０にリダイレクト電文を送信する。このリダイレクト電文には、トランザクション通番、遷移先、引継キーに関するデータを含める。

【００３９】

次に、第２サーバ３０の制御部３１は、ユーザ情報の要求処理を実行する（ステップＳ１－１１）。具体的には、制御部３１のユーザ認証部３１１は、第１サーバ２０に対して、ユーザ情報要求電文を送信する。ユーザ情報要求電文には、サーバＩＤ、サーバ認証情報を含める。更に、ユーザ情報要求電文には、ユーザ端末１０から取得したトランザクション通番、引継キーに関するデータを含める。

【００４０】

次に、第１サーバ２０の制御部２１は、クライアント認証処理を実行する（ステップＳ１－１２）。具体的には、制御部２１のサーバ認証部２１４は、関連サーバリストを用いて、遷移可能な第２サーバ３０を認証する。ユーザ情報要求電文に含まれるサーバＩＤが関連サーバリストに記録されている場合には、クライアント認証を完了する。

【００４１】

第２サーバ３０についてのクライアント認証を完了した場合、第１サーバ２０の制御部２１は、ユーザ情報の抽出処理を実行する（ステップＳ１－１３）。具体的には、制御部２１の引継処理部２１３は、ユーザ情報要求電文に含まれる引継キーが記録された引継管理レコード２４０を、引継情報記憶部２４から抽出する。そして、引継処理部２１３は、抽出した引継管理レコード２４０に記録されているユーザＩＤを取得する。この場合、引継処理部２１３は、ワンタイムパスワードを生成する。そして、引継処理部２１３は、引継管理レコード２４０に、ワンタイムパスワード、遷移済フラグ（状況）、現在日時（遷移日時）を記録する。

【００４２】

次に、第１サーバ２０の制御部２１は、ユーザ情報の送信処理を実行する（ステップＳ

１－１４）。具体的には、制御部２１の引継処理部２１３は、応答電文を第２サーバ３０に送信する。この応答電文には、トランザクション通番、引継キー、ワンタイムパスワード、ユーザＩＤ、個人情報に関するデータを含める。なお、クライアント認証を完了できなかった場合や、引継情報記憶部２４から引継管理レコード２４０を抽出できなかった場合には、引継処理部２１３は、エラー電文を第２サーバ３０に送信する。エラー電文を受信した第２サーバ３０は、エラーメッセージをユーザ端末１０の出力部に出力する。

【００４３】

次に、第２サーバ３０の制御部３１は、ログイン処理を実行する（ステップＳ１－１５）。具体的には、制御部３１のユーザ認証部３１１は、応答電文のユーザＩＤの認証処理を完了し、ユーザ管理レコード３２０のログイン状況データ領域にログイン済フラグを記録する。そして、制御部３１のサービス管理部３１２は、第１サーバ２０から取得した個人情報を利用して、ユーザが希望するサービスについてのサービス画面を提供する。

【００４４】

次に、ユーザ端末１０は、画面表示処理を実行する（ステップＳ１－１６）。具体的には、ユーザ端末１０は、出力部にサービス画面を表示する。このサービス画面により、ユーザは、第２サーバ３０が提供するサービスを利用する。

【００４５】

（戻り処理）

次に、図４を用いて、戻り処理を説明する。この戻り処理は、第２サーバ３０から第１サーバ２０に遷移する場合に実行される。

【００４６】

この場合、ユーザ端末１０は、戻り要求処理を実行する（ステップＳ２－１）。具体的には、ユーザ端末１０において、第１サーバ２０に戻るための操作が行なわれた場合や、第２サーバ３０におけるサービスを利用するために第１サーバ２０に戻る必要が生じた場合、ユーザ端末１０は、第２サーバ３０に対して、戻り要求を送信する。

【００４７】

次に、第２サーバ３０の制御部３１は、リダイレクト要求処理を実行する（ステップＳ２－２）。具体的には、制御部３１のサービス管理部３１２は、ユーザ端末１０に対してリダイレクト要求電文を送信する。このリダイレクト要求電文には、引継キー、サーバＩＤ、ユーザＩＤ、ワンタイムパスワードに関するデータを含める。

【００４８】

次に、ユーザ端末１０は、リダイレクト処理を実行する（ステップＳ２－３）。具体的には、ユーザ端末１０は、遷移先である第１サーバ２０にリダイレクト電文を送信する。このリダイレクト電文には、引継キー、サーバＩＤ、ユーザＩＤ、ワンタイムパスワードに関するデータを含める。

【００４９】

次に、第１サーバ２０の制御部２１は、引継情報の取得処理を実行する（ステップＳ２－４）。具体的には、制御部２１の引継処理部２１３は、ユーザ端末１０からリダイレクト電文を取得する。

【００５０】

次に、第１サーバ２０の制御部２１は、引継情報の整合性チェック処理を実行する（ステップＳ２－５）。具体的には、制御部２１の引継処理部２１３は、リダイレクト電文から引継キー、ワンタイムパスワードを取得する。次に、引継処理部２１３は、取得した引継キー、ワンタイムパスワードが記録された引継管理レコード２４０を、引継情報記憶部２４において検索する。引継情報記憶部２４から引継管理レコード２４０を抽出できた場合、引継処理部２１３は、引継管理レコード２４０に記録された遷移日時からの経過時間を算出する。経過時間が有効時間を経過していない場合には、引継情報が整合していると判定して、整合性チェック（第２の認証処理）を完了する。一方、引継管理レコード２４０を抽出できない場合や、経過時間が有効時間を経過している場合には、ログインできないことを示すメッセージをユーザ端末１０に返信する。この場合、ユーザ認証部２１１は

、ユーザ端末１０にログイン画面を出力し、ユーザ認証処理（ステップＳ１－２）をやり直す。

【００５１】

整合性チェックを完了した場合、第１サーバ２０の制御部２１は、引継情報の更新処理を実行する（ステップＳ２－６）。具体的には、制御部２１の引継処理部２１３は、引継情報記憶部２４に記録されている引継管理レコード２４０の状況データ領域に使用済フラグを記録する。

【００５２】

次に、第１サーバ２０の制御部２１は、ログイン処理を実行する（ステップＳ２－７）。具体的には、制御部２１の引継処理部２１３は、ユーザ情報記憶部２２のユーザ管理レコード２２０のログイン状況データ領域に、ログイン済フラグを記録する。

【００５３】

次に、第１サーバ２０の制御部２１は、リダイレクト応答処理を実行する（ステップＳ２－８）。具体的には、制御部２１のサービス管理部２１２は、サービス画面データをユーザ端末１０に送信する。

次に、ユーザ端末１０は、画面表示処理を実行する（ステップＳ２－９）。具体的には、ユーザ端末１０は、出力部にサービス画面を出力する。

【００５４】

以上、本実施形態によれば、以下のような効果を得ることができる。

（１）本実施形態によれば、遷移要求を取得した第１サーバ２０の制御部２１は、引継キーの生成処理（ステップＳ１－５）、引継キーの登録処理（ステップＳ１－６）、リダイレクト応答処理を実行する（ステップＳ１－８）。そして、第２サーバ３０の制御部３１は、ユーザ情報の要求処理を実行する（ステップＳ１－１１）。第１サーバ２０の制御部２１は、ユーザ情報の抽出処理（ステップＳ１－１３）、ユーザ情報の送信処理（ステップＳ１－１４）を実行する。これにより、第１サーバ２０で認証されたユーザは、第２サーバ３０に効率的に遷移でき、第２サーバ３０は、引継キーに基づいて、ユーザ情報を取得することができる。

【００５５】

（２）本実施形態によれば、第１サーバ２０の制御部２１は、クライアント認証処理（ステップＳ１－１２）、ユーザ情報の抽出処理（ステップＳ１－１３）を実行する。これにより、第１サーバ２０は、第２サーバ３０を確認してユーザ情報を提供することができる。そして、ユーザによるユーザＩＤ、パスワードの登録を不要とし、第２サーバ３０への遷移における利便性を向上させることができる。

【００５６】

（３）本実施形態によれば、第２サーバ３０の制御部３１は、ログイン処理を実行する（ステップＳ１－１５）。これにより、第１サーバ２０へのログインに基づいて、第２サーバ３０にログインすることができる。

【００５７】

（４）本実施形態によれば、第２サーバ３０の制御部３１は、リダイレクト要求処理を実行する（ステップＳ２－２）。そして、第１サーバ２０の制御部２１は、引継情報の取得処理（ステップＳ２－４）、引継情報の整合性チェック処理（ステップＳ２－５）、ログイン処理（ステップＳ２－７）を実行する。これにより、第２サーバ３０への遷移時に、第１サーバ２０をログアウトし、遷移先の第２サーバ３０から、再度、第１サーバ２０に戻る場合も円滑に遷移することができる。

【００５８】

（５）本実施形態によれば、第１サーバ２０の制御部２１は、引継情報の整合性チェック処理を実行する（ステップＳ２－５）。この場合、引継キーに関連付けられたワンタイムパスワードの有効期間の経過を確認する。これにより、第１サーバ２０から第２サーバ３０への有効期間の遷移を許容することができる。そして、ワンタイムパスワードの利用を一定時間内のみに制限することにより、第１サーバ２０への戻り時に用いる引継キーの

不正利用を抑制することができる。

【００５９】

また、上記実施形態は以下のように変更してもよい。

・上記実施形態では、第１サーバ２０の制御部２１は、引継情報の整合性チェック処理を実行する（ステップＳ２－５）。この場合、引継処理部２１３は、引継管理レコード２４０に記録された遷移日時からの経過時間が有効時間を経過していないかを判定する。この場合、有効時間は固定値に限定されるものではない。

【００６０】

例えば、遷移先や、遷移先で利用するサービスに応じて、有効時間を変更してもよい。この場合には、引継処理部２１３に、遷移先のサーバＩＤや、遷移先で利用するサービスＩＤに関連付けて有効時間を定める有効時間管理テーブルを保持させておく。そして、引継情報の整合性チェック処理（ステップＳ２－５）において、連係先のサーバＩＤやサービスＩＤに基づいて有効時間を特定する。

【００６１】

・上記実施形態では、ワンタイムパスワードの有効時間として１時間を用いる。有効時間は、これに限定されるものではない。例えば、サービスの利用履歴の統計情報に基づいて、有効時間を最適化するようにしてもよい。この場合には、第１サーバ２０の制御部２１は、第２サーバ３０においてサービスを利用する時間の長さの統計値を算出し、この統計値に基づいて有効時間を決定する。この場合、第２サーバ３０において利用するサービス毎に統計値を算出するようにしてもよい。そして、第１サーバ２０の制御部２１は、第２サーバ３０やサービスの利用状況に応じた有効時間を設定する。これにより、ログアウトから再ログインまでに時間を要する第２サーバ３０やサービスの所要時間に応じて、再ログインの利便性を図ることができる。

【００６２】

また、アクセス時期（アクセス曜日や時間帯）に基づいて、有効時間を最適化するようにしてもよい。この場合には、第１サーバ２０の制御部２１は、アクセス時期に関連付けて、第２サーバ３０のサービスの利用履歴情報を取得する。そして、制御部２１は、アクセス時期に関連付けて、サービス利用時間の統計値を算出する。アクセス時期によって、第２サーバ３０において利用するサービスの利用方法は異なるので、ユーザにおける第２サーバ３０やサービスの利用状況に応じて、再ログインの利便性を図ることができる。

【００６３】

また、ユーザ毎に、有効時間を最適化するようにしてもよい。この場合には、第１サーバ２０の制御部２１は、ユーザＩＤに関連付けて、第２サーバ３０のサービスの利用時間を取得する。そして、制御部２１は、ユーザＩＤに関連付けてサービス利用時間の統計値を算出する。これにより、ユーザにおける第２サーバ３０やサービスの利用状況に応じて、再ログインの利便性を図ることができる。

【００６４】

更に、ユーザにおける第２サーバ３０の利用状況（利用頻度）に基づいて、有効時間を最適化するようにしてもよい。この場合には、第１サーバ２０の制御部２１は、このユーザの第２サーバ３０の利用頻度を取得し、利用頻度に応じて、利用時間を調整する。例えば、第２サーバ３０の利用頻度が高いと判定した場合には、有効時間の初期値に対して所定割合で短くする。一方、第２サーバ３０の利用頻度が低いと判定した場合には、有効時間の初期値に対して所定割合で長くする。

【００６５】

また、サーバ状況に基づいて、有効時間を最適化するようにしてもよい。この場合には、第１サーバ２０の制御部２１は、第２サーバ３０のサーバ稼動状況を特定し、このサーバ稼動状況に基づいて有効時間を調整する。例えば、サーバ稼動状況において、第２サーバ３０が混雑していると判定した場合には、有効時間の初期値に対して所定割合で長くする。

【００６６】

・上記実施形態では、関連サーバとして第２サーバ３０を用いるが、関連サーバの数は限定されるものではない。また、第１サーバ２０から第２サーバ３０へ遷移し、第２サーバ３０から第１サーバ２０に戻る場合を想定したが、再ログインするサーバは第１サーバ２０に限定されない。

また、第１サーバ２０、第２サーバ３０が、予め停止時期が定められた計画停止や、突発的な障害発生による停止が生じた場合には、遷移や戻りを止めるようにしてもよい。この場合には、遷移元サーバにおいて、遷移先候補サーバの稼働状況を取得し、停止中には、遷移できないことを示すメッセージをユーザ端末１０に出力する。

【００６７】

また、第１サーバ２０から第２サーバ３０へ遷移し、この第２サーバ３０から、更に他のサーバ（第３サーバ）に遷移できるようにしてもよい。例えば、第２サーバ３０から第３サーバへの遷移を希望する場合、ユーザ端末１０を介してのリダイレクトにより、第２サーバ３０から第１サーバに戻る。この場合、第１サーバに対して、第２サーバ３０から第３サーバへの遷移要求を行なう。そして、再度、第１サーバから、ユーザ端末１０を介してのリダイレクトにより、第３サーバに遷移する。この場合には、第２サーバ３０への遷移時に生成した引継キーを、第３サーバへの遷移についても継続的に使用することが可能である。また、第３サーバへの遷移時に新たに引継キーを生成し、引継情報記憶部２４に登録するようにしてもよい。

【００６８】

また、第２サーバ３０から第３サーバに、ユーザ端末１０を介してのリダイレクトにより遷移させ、第２サーバ３０が、第１サーバに対して、第２サーバ３０から第３サーバに遷移したことを伝えるようにしてもよい。この場合には、第２サーバ３０への遷移時に生成した引継キーを、第３サーバから第１サーバ２０の戻り時にも継続して使用する。

そして、第３サーバから第１サーバ２０に戻る場合、上記実施形態と同様に、第１サーバ２０は、引継情報の取得処理（ステップＳ２－４）、引継情報の整合性チェック処理（ステップＳ２－５）を実行する。

【符号の説明】

【００６９】

１０…ユーザ端末、２０…第１サーバ、２１…制御部、２１１…ユーザ認証部、２１２…サービス管理部、２１３…引継処理部、２１４…サーバ認証部、２２…ユーザ情報記憶部、２４…引継情報記憶部、３０…第２サーバ、３１…制御部、３２…ユーザ情報記憶部、３１１…ユーザ認証部、３１２…サービス管理部。

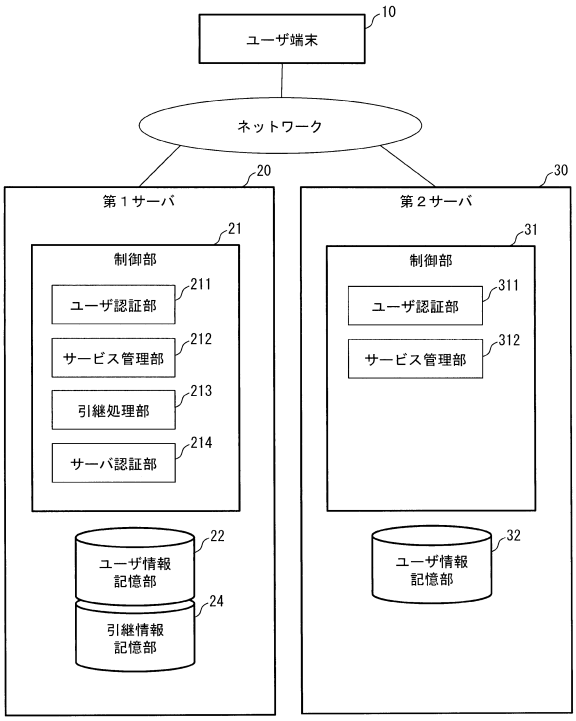
【要約】

【課題】複数のサーバへのログインを管理するためのログイン管理システム、ログイン管理方法及びログイン管理プログラムを提供する。

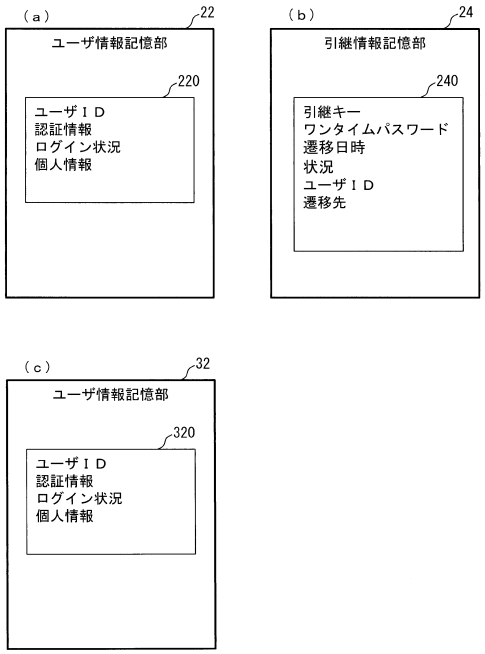
【解決手段】第１サーバ２０は、引継情報を記憶する引継情報記憶部２４と、ユーザ端末１０、第２サーバ３０に接続される制御部２１とを備える。そして、制御部２１が、ユーザ端末１０からログイン要求を受け付けた場合、ユーザ端末１０から取得した認証情報を用いて第１の認証処理を実行してログインを許可する。ログインしたユーザ端末１０から第２サーバ３０への遷移要求を取得した場合、引継情報を生成し、引継情報記憶部２４に記録し、第２サーバ３０に対して引継情報を提供する。そして、ユーザ端末１０から、再ログイン要求を受け付けた場合、引継情報を第２サーバ３０から取得し、引継情報記憶部２４に記録された引継情報と、取得した引継情報とを用いて第２の認証処理を実行する。

【選択図】図１

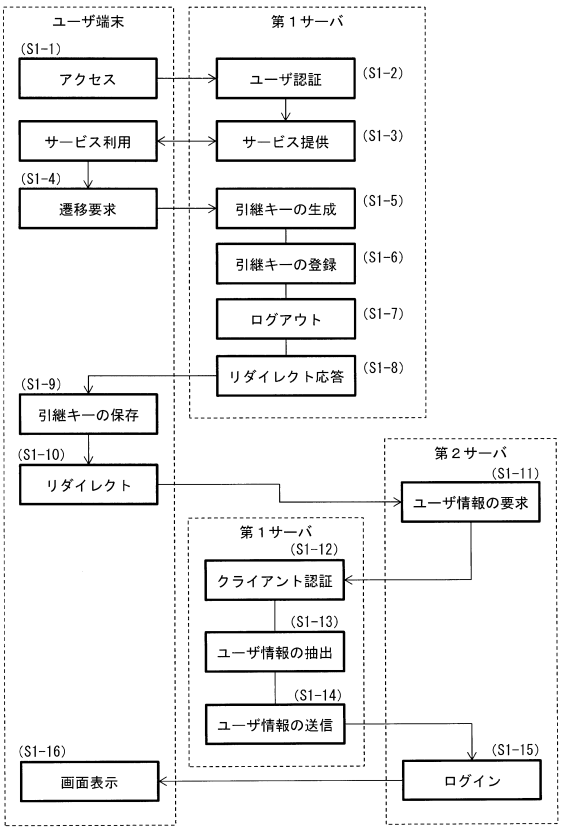
【図１】


ユーザ端末
10
ネットワーク
第１サーバ
20
第２サーバ
30
制御部
21
ユーザ認証部
211
サービス管理部
212
引継処理部
213
サーバ認証部
214
制御部
31
ユーザ認証部
311
サービス管理部
312
ユーザ情報記憶部
22
引継情報記憶部
24
ユーザ情報記憶部
32

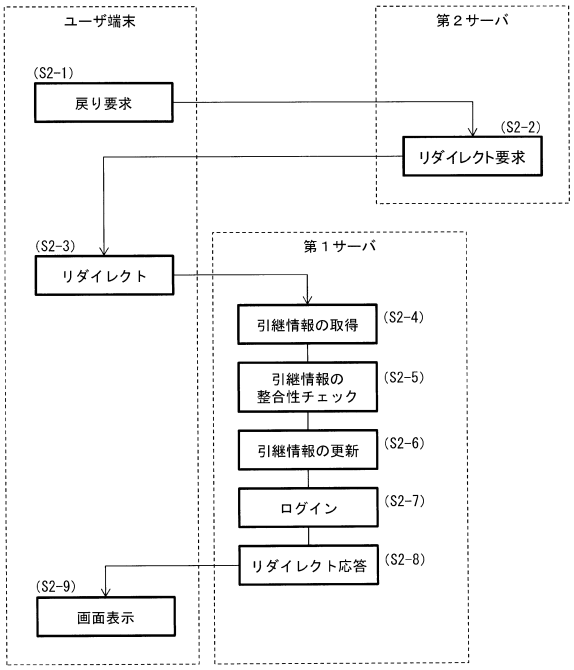
【図２】


（ａ）
ユーザ情報記憶部
22
220
ユーザＩＤ
認証情報
ログイン状況
個人情報
（ｂ）
引継情報記憶部
24
240
引継キー
ワンタイムパスワード
遷移日時
状況
ユーザＩＤ
遷移先
（ｃ）
ユーザ情報記憶部
32
320
ユーザＩＤ
認証情報
ログイン状況
個人情報

【図３】


ユーザ端末
第１サーバ
(S1-1)
アクセス
ユーザ認証
(S1-2)
サービス利用
サービス提供
(S1-3)
(S1-4)
遷移要求
引継キーの生成
(S1-5)
引継キーの登録
(S1-6)
ログアウト
(S1-7)
リダイレクト応答
(S1-8)
(S1-9)
引継キーの保存
(S1-10)
リダイレクト
第２サーバ
(S1-11)
ユーザ情報の要求
第１サーバ
(S1-12)
クライアント認証
(S1-13)
ユーザ情報の抽出
(S1-14)
ユーザ情報の送信
(S1-15)
ログイン
(S1-16)
画面表示

【図４】


ユーザ端末
第２サーバ
(S2-1)
戻り要求
(S2-2)
リダイレクト要求
(S2-3)
リダイレクト
第１サーバ
引継情報の取得
(S2-4)
引継情報の
整合性チェック
(S2-5)
引継情報の更新
(S2-6)
ログイン
(S2-7)
リダイレクト応答
(S2-8)
(S2-9)
画面表示

フロントページの続き

(72)発明者　赤荻　真由美
東京都千代田区神田錦町二丁目３番地　みずほ情報総研　株式会社　内
(72)発明者　高木　敏伸
東京都千代田区神田錦町二丁目３番地　みずほ情報総研　株式会社　内
(72)発明者　半田　勝也
東京都千代田区神田錦町二丁目３番地　みずほ情報総研　株式会社　内
(72)発明者　屋敷　圭志
東京都千代田区大手町一丁目５番５号　株式会社　みずほ銀行　内
(72)発明者　小野　佐保子
東京都千代田区大手町一丁目５番５号　株式会社　みずほ銀行　内
(72)発明者　南雲　友希
東京都千代田区大手町一丁目５番５号　株式会社　みずほ銀行　内
(72)発明者　須藤　泰自
東京都千代田区大手町一丁目５番５号　株式会社　みずほ銀行　内

審査官　北川　純次

(56)参考文献　特開２００１－２８２６７６（ＪＰ，Ａ）
特開２０１７－１７３８８９（ＪＰ，Ａ）
特開２０１６－００９２７６（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　１３／００
Ｇ０６Ｆ　２１／４１
Ｈ０４Ｌ　　９／００