(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5429912号
(P5429912)
(45)発行日　平成26年2月26日(2014.2.26)　(24)登録日　平成25年12月13日(2013.12.13)

(51)Int.Cl.　　F I
H04L 9/32 (2006.01)　　H04L 9/00 673A
G06F 21/31 (2013.01)　　G06F 21/20 131A

請求項の数 10　(全 21 頁)

(21)出願番号　特願2012-548721 (P2012-548721)
(86)(22)出願日　平成23年11月30日 (2011.11.30)
(86)国際出願番号　PCT/JP2011/077692
(87)国際公開番号　WO2012/081404
(87)国際公開日　平成24年6月21日 (2012.6.21)
審査請求日　平成25年5月20日 (2013.5.20)
(31)優先権主張番号　特願2010-280637 (P2010-280637)
(32)優先日　平成22年12月16日 (2010.12.16)
(33)優先権主張国　日本国(JP)

(73)特許権者　000164449
九州日本電気ソフトウェア株式会社
福岡市早良区百道浜２丁目４－１　ＮＥＣ九州システムセンター
(74)代理人　110000682
特許業務法人ワンディーＩＰパートナーズ
(72)発明者　吉垣　伸介
福岡県福岡市早良区百道浜二丁目４番１号　ＮＥＣ九州システムセンター　九州日本電気ソフトウェア株式会社内
(72)発明者　塩谷　幸治
福岡県福岡市早良区百道浜二丁目４番１号　ＮＥＣ九州システムセンター　九州日本電気ソフトウェア株式会社内

最終頁に続く

(54)【発明の名称】認証システム、認証サーバ、サービス提供サーバ、認証方法、及びプログラム

(57)【特許請求の範囲】
【請求項１】
ユーザに対して端末を介して認証を行う認証サーバと、前記ユーザに前記端末を介してサービスを提供するサービス提供サーバとを備え、
前記認証サーバは、前記ユーザが前記端末を介して前記認証を要求すると、前記ユーザに前記端末を介してログイン情報を入力させ、そして、入力された前記ログイン情報を前記サービス提供サーバに送信すると共に、前記ログイン情報からハッシュ関数を用いて第１のハッシュ値を算出し、
前記サービス提供サーバは、前記認証サーバから送信された前記ログイン情報が、予め登録されている情報と一致しているかどうかを判定し、一致している場合に、前記ハッシュ関数と同一のハッシュ関数を用いて、前記ログイン情報から第２のハッシュ値を算出し、
前記第１のハッシュ値と前記第２のハッシュ値とが一致する場合に、前記認証サーバが前記端末との間でセッションを確立する、
ことを特徴とする認証システム。
【請求項２】
前記ログイン情報が、第１の識別子とパスワードとを含み、
前記サービス提供サーバが、
予め、前記第１の識別子毎に、当該第１の識別子に対応するパスワードと、当該第１の識別子に関連付けられた第２の識別子とを記憶し、

前記ログイン情報として送信されてきた第１の識別子が、記憶されている前記第２の識別子と関連付けられており、且つ、前記ログイン情報として送信されてきたパスワードが、記憶されているパスワードと一致する場合に、予め登録されている情報と一致していると判定する、請求項１に記載の認証システム。
【請求項３】
前記認証サーバが、前記ログイン情報を記憶し、記憶した前記ログイン情報から前記第１のハッシュ値を算出し、そして、前記第１のハッシュ値を算出すると同時に、または算出した後に、記憶した前記ログイン情報を削除する、
請求項１または２に記載の認証システム。
【請求項４】
前記認証サーバが、前記ログイン情報を示す電子メール作成し、作成した前記電子メールによって、前記ログイン情報を前記サービス提供サーバに送信する、請求項１から３のいずれかに記載の認証システム。
【請求項５】
前記認証サーバが、前記ユーザが前記端末を介して前記認証を要求すると、前記端末に対して、予め設定されたサービスＩＤを送信し、前記ログイン情報と共に前記サービスＩＤを返信させ、更に、前記サービス提供サーバに、前記ログイン情報に加えて前記サービスＩＤを送信し、そして、前記ログイン情報及び前記サービスＩＤから前記第１のハッシュ値を算出し、
前記サービス提供サーバが、前記ログイン情報及び前記サービスＩＤから前記第２のハッシュ値を算出する、請求項１～４のいずれかに記載の認証システム。
【請求項６】
サービス提供サーバにサービスの提供を求めるユーザに対して端末を介して認証を行う認証サーバであって、
前記ユーザが前記端末を介して前記認証を要求すると、前記ユーザに前記端末を介してログイン情報を入力させる、情報入力部と、
入力された前記ログイン情報を前記サービス提供サーバに送信する、送信部と、
前記ログイン情報からハッシュ関数を用いて第１のハッシュ値を算出する、ハッシュ処理部と、
前記端末との間にセッションを確立する、セッション確立部とを備え、
前記ハッシュ処理部は、
前記サービス提供サーバが、送信された前記ログイン情報に基づいて、それが予め登録されている情報と一致していることを条件に、前記ハッシュ関数と同一のハッシュ関数を用いて、第２のハッシュ値を算出すると、
前記第１のハッシュ値と前記第２のハッシュ値とが一致しているかどうかを判定し、
前記セッション確立部は、前記ハッシュ処理部が一致していると判定する場合に、前記セッションを確立する、
ことを特徴とする認証サーバ。
【請求項７】
認証サーバが端末との間にセッションを確立した場合に、前記端末を介してユーザにサービスを提供するサービス提供サーバであって、
前記認証サーバから、前記端末を介して入力されたログイン情報が送信されると、前記ログイン情報が、予め登録されている情報と一致しているかどうかを判定する、ログイン情報判定部と、
前記ログイン情報判定部が一致していると判定した場合に、前記ログイン情報からハッシュ関数を用いてハッシュ値を算出する、ハッシュ値算出部と、
前記認証サーバによって、それが前記ハッシュ関数と同一のハッシュ関数を用いて前記ログイン情報から算出したハッシュ値と、前記ハッシュ値算出部が算出したハッシュ値とが一致することを条件にして、前記端末との間にセッションが確立されると、前記端末を介して前記ユーザにサービスを提供する、サービス提供部と、を備えている、

ことを特徴とするサービス提供サーバ。
【請求項８】
ユーザに対して端末を介して認証を行う認証サーバと、前記ユーザに前記端末を介してサービスを提供するサービス提供サーバとを用いる認証方法であって、
（ａ）前記ユーザが前記端末を介して前記認証を要求すると、前記認証サーバが、前記ユーザに前記端末を介してログイン情報を入力させる、ステップと、
（ｂ）前記認証サーバが、入力された前記ログイン情報を前記サービス提供サーバに送信する、ステップと、
（ｃ）前記認証サーバが、入力された前記ログイン情報からハッシュ関数を用いて第１のハッシュ値を算出する、ステップと、
（ｄ）前記サービス提供サーバが、前記ログイン情報が、予め登録されている情報と一致しているかどうかを判定し、一致している場合に、前記ハッシュ関数と同一のハッシュ関数を用いて、前記ログイン情報から第２のハッシュ値を算出する、ステップと、
（ｅ）前記認証サーバが、前記（ｃ）のステップで算出された前記第１のハッシュ値と前記（ｄ）のステップで算出された前記第２のハッシュ値とが一致する場合に、前記端末との間でセッションを確立する、ステップと、を有することを特徴とする認証方法。
【請求項９】
サービス提供サーバにサービスの提供を求めるユーザに対する、端末を介した認証を、コンピュータによって行うための、プログラムであって、
前記コンピュータに、
（ａ）前記ユーザが前記端末を介して前記認証を要求すると、前記ユーザに前記端末を介してログイン情報を入力させる、ステップと、
（ｂ）前記（ａ）のステップで入力された前記ログイン情報を前記サービス提供サーバに送信する、ステップと、
（ｃ）前記（ａ）のステップで入力された前記ログイン情報からハッシュ関数を用いて第１のハッシュ値を算出する、ステップと、
（ｄ）前記サービス提供サーバが、送信された前記ログイン情報に基づいて、それが予め登録されている情報と一致していることを条件に、前記ハッシュ関数と同一のハッシュ関数を用いて、第２のハッシュ値を算出すると、前記（ｃ）のステップで算出した前記第１のハッシュ値と前記サービス提供サーバが算出した前記第２のハッシュ値とが一致しているかどうかを判定する、ステップと、
（ｅ）前記（ｄ）のステップで一致していると判定する場合に、前記端末との間にセッションを確立する、ステップと、
を実行させる、プログラム。
【請求項１０】
認証サーバが端末との間にセッションを確立した場合に、コンピュータによって、前記端末を介してユーザにサービスを提供するための、プログラムであって、
前記コンピュータに、
（ａ）前記認証サーバから、前記端末を介して入力されたログイン情報が送信されると、前記ログイン情報が、予め登録されている情報と一致しているかどうかを判定する、ステップと、
（ｂ）前記（ａ）のステップで一致していると判定した場合に、前記ログイン情報からハッシュ関数を用いてハッシュ値を算出する、ステップと、
（ｃ）前記認証サーバが、それが前記ハッシュ関数と同一のハッシュ関数を用いて前記ログイン情報から算出したハッシュ値と、前記（ｂ）のステップで算出されたハッシュ値とが一致することを条件にして、前記端末との間にセッションを確立すると、前記端末を介して前記ユーザにサービスを提供する、ステップと、
を実行させる、プログラム。
【発明の詳細な説明】
【技術分野】

【０００１】
本発明は、クラウドコンピューティングに用いられる、認証システム、認証サーバ、サービス提供サーバ、認証方法、及びこれらを実現するためのプログラムに関する。
【背景技術】
【０００２】
近年、「クラウドコンピューティング」と呼ばれるコンピュータの利用形態が増加している。クラウドコンピューティングでは、ユーザに対して、インターネットの向こう側から、各種アプリケーションサービス、サーバなどのハードウェアリーソースが、提供される。
【０００３】
ユーザは、インターネットに接続できる環境にあれば、クラウドコンピューティングが提供するサービス（クラウドコンピューティング・サービス）を受けることができ、その際、サービスインフラを意識する必要がない。特許文献１は、クラウドコンピューティング・サービスを提供するシステム（以下「クラウドシステム」という。）を開示している。
【０００４】
特許文献１に開示されたクラウドシステムは、認証サーバと、複数のサービス提供サーバとを備えている。特許文献１に開示されたクラウドシステムによれば、ユーザは、一度ログインを行うと、各サーバを意識することなく、各サービス提供サーバが提供するサービスを受けることができる。以下に説明する。
【０００５】
先ず、ユーザが、ログインを行うと、認証サーバによる認証処理が行われる。具体的には、ユーザは、端末を用いてサービス要求を示す依頼文を作成し、これを暗号化した後、認証サーバに送信する。そして、認証サーバは、ユーザの端末のＩＤを復号鍵とする復号化処理を行い、復号化できた場合に、端末からのログインを認める。次に、認証サーバは、ユーザによるログインを認めた場合は、ツアーの予約サービスを提供するサーバ（以下「ツアー予約サーバ」とする。）を呼び出す。
【０００６】
呼び出されたツアー予約サーバは、ユーザの画面に、ツアー予約画面を表示させ、予約を行わせる。そして、ユーザが予約を行うと、ツアー予約サーバは、ホテルの予約サービスを提供するサーバ、及びレストランの予約サービスを提供するサーバを呼び出し、ホテル及びレストランの予約を行わせる。このように、ユーザは、一度のログインで各サービスを受けることができる。
【０００７】
また、企業では、クラウドコンピューティングの導入により、導入しない場合に比べて、極めて短期間で、しかも低コストで、必要な環境を整えることができる。このため、クラウドコンピューティングの導入は企業においても増加している。
【先行技術文献】
【特許文献】
【０００８】
【特許文献１】特開２０１０－１９１８０１号公報
【発明の概要】
【発明が解決しようとする課題】
【０００９】
ところで、企業では、他社に管理されたくないデータについては、自社で管理を行う必要があるため、セキュリティを確保しつつ、企業内システムとクラウドシステムとを連携させる必要がある。例えば、特許文献１に開示された技術を利用し、認証サーバによる認証が行われた場合に、クラウドシステムから企業内システムへのアクセスが許可される仕組みとすることが考えられる。
【００１０】

しかしながら、特許文献１に開示されたクラウドシステムでは、認証の際の復号鍵として、ユーザの端末のＩＤが利用されており、企業内システムのセキュリティとしては不十分である。また、認証サーバが企業の外に存在することからも、企業内システムとクラウドシステムとを連携させる場合は、セキュリティが十分に確保されたシステムとすることが求められている。

【００１１】

本発明の目的の一例は、上記問題を解消し、認証サーバと、サービスを提供するサーバとの間のセキュリティを高め得る、認証システム、それに用いられる認証サーバ、サービス提供サーバ、認証方法、及びプログラムを提供することにある。

【課題を解決するための手段】

【００１２】

上記目的を達成するため、本発明の一側面における認証システムは、ユーザに対して端末を介して認証を行う認証サーバと、前記ユーザに前記端末を介してサービスを提供するサービス提供サーバとを備え、

前記認証サーバは、前記ユーザが前記端末を介して前記認証を要求すると、前記ユーザに前記端末を介してログイン情報を入力させ、そして、入力された前記ログイン情報を前記サービス提供サーバに送信すると共に、前記ログイン情報からハッシュ関数を用いて第１のハッシュ値を算出し、

前記サービス提供サーバは、前記認証サーバから送信された前記ログイン情報が、予め登録されている情報と一致しているかどうかを判定し、一致している場合に、前記ハッシュ関数と同一のハッシュ関数を用いて、前記ログイン情報から第２のハッシュ値を算出し、

前記第１のハッシュ値と前記第２のハッシュ値とが一致する場合に、前記認証サーバが前記端末との間でセッションを確立する、

ことを特徴とする。

【００１３】

上記目的を達成するため、本発明の一側面における認証サーバは、サービス提供サーバにサービスの提供を求めるユーザに対して端末を介して認証を行う認証サーバであって、

前記ユーザが前記端末を介して前記認証を要求すると、前記ユーザに前記端末を介してログイン情報を入力させる、情報入力部と、

入力された前記ログイン情報を前記サービス提供サーバに送信する、送信部と、

前記ログイン情報からハッシュ関数を用いて第１のハッシュ値を算出する、ハッシュ処理部と、

前記端末との間にセッションを確立する、セッション確立部とを備え、

前記ハッシュ処理部は、

前記サービス提供サーバが、送信された前記ログイン情報に基づいて、それが予め登録されている情報と一致していることを条件に、前記ハッシュ関数と同一のハッシュ関数を用いて、第２のハッシュ値を算出すると、

前記第１のハッシュ値と前記第２のハッシュ値とが一致しているかどうかを判定し、

前記セッション確立部は、前記セッション処理部が一致していると判定する場合に、前記セッションを確立する、

ことを特徴とする。

【００１４】

上記目的を達成するため、本発明の一側面におけるサービス提供サーバは、認証サーバが端末との間にセッションを確立した場合に、前記端末を介してユーザにサービスを提供するサービス提供サーバであって、

前記認証サーバから、前記端末を介して入力されたログイン情報が送信されると、前記ログイン情報が、予め登録されている情報と一致しているかどうかを判定する、ログイン情報判定部と、

前記ログイン情報判定部が一致していると判定した場合に、前記ログイン情報からハッ

シュ関数を用いてハッシュ値を算出する、ハッシュ値算出部と、
前記認証サーバによって、それが前記ハッシュ関数と同一のハッシュ関数を用いて前記ログイン情報から算出したハッシュ値と、前記ハッシュ値算出部が算出したハッシュ値とが一致することを条件にして、前記端末との間にセッションが確立されると、前記端末を介して前記ユーザにサービスを提供する、サービス提供部と、を備えている、
ことを特徴とする。
【００１５】
上記目的を達成するため、本発明の一側面における認証方法は、ユーザに対して端末を介して認証を行う認証サーバと、前記ユーザに前記端末を介してサービスを提供するサービス提供サーバとを用いる認証方法であって、
（ａ）前記ユーザが前記端末を介して前記認証を要求すると、前記認証サーバが、前記ユーザに前記端末を介してログイン情報を入力させる、ステップと、
（ｂ）前記認証サーバが、入力された前記ログイン情報を前記サービス提供サーバに送信する、ステップと、
（ｃ）前記認証サーバが、入力された前記ログイン情報からハッシュ関数を用いて第１のハッシュ値を算出する、ステップと、
（ｄ）前記サービス提供サーバが、前記ログイン情報が、予め登録されている情報と一致しているかどうかを判定し、一致している場合に、前記ハッシュ関数と同一のハッシュ関数を用いて、前記ログイン情報から第２のハッシュ値を算出する、ステップと、
（ｅ）前記認証サーバが、前記（ｃ）のステップで算出された前記第１のハッシュ値と前記（ｄ）のステップで算出された前記第２のハッシュ値とが一致する場合に、前記端末との間でセッションを確立する、ステップと、を有することを特徴とする。
【００１６】
上記目的を達成するため、本発明の一側面における第１のプログラムは、サービス提供サーバにサービスの提供を求めるユーザに対する、端末を介した認証を、コンピュータによって行うための、プログラムであって、
前記コンピュータに、
（ａ）前記ユーザが前記端末を介して前記認証を要求すると、前記ユーザに前記端末を介してログイン情報を入力させる、ステップと、
（ｂ）前記（ａ）のステップで入力された前記ログイン情報を前記サービス提供サーバに送信する、ステップと、
（ｃ）前記（ａ）のステップで入力された前記ログイン情報からハッシュ関数を用いて第１のハッシュ値を算出する、ステップと、
（ｄ）前記サービス提供サーバが、送信された前記ログイン情報に基づいて、それが予め登録されている情報と一致していることを条件に、前記ハッシュ関数と同一のハッシュ関数を用いて、第２のハッシュ値を算出すると、前記（ｃ）のステップで算出した前記第１のハッシュ値と前記サービス提供サーバが算出した前記第２のハッシュ値とが一致しているかどうかを判定する、ステップと、
（ｅ）前記（ｄ）のステップで一致していると判定する場合に、前記端末との間にセッションを確立する、ステップと、
を実行させる、ことを特徴とする。
【００１７】
上記目的を達成するため、本発明の一側面における第２のプログラムは、認証サーバが端末との間にセッションを確立した場合に、コンピュータによって、前記端末を介してユーザにサービスを提供するための、プログラムであって、
前記コンピュータに、
（ａ）前記認証サーバから、前記端末を介して入力されたログイン情報が送信されると、前記ログイン情報が、予め登録されている情報と一致しているかどうかを判定する、ステップと、
（ｂ）前記（ａ）のステップで一致していると判定した場合に、前記ログイン情報からハ

ッシュ関数を用いてハッシュ値を算出する、ステップと、
（ｃ）前記認証サーバが、それが前記ハッシュ関数と同一のハッシュ関数を用いて前記ログイン情報から算出したハッシュ値と、前記（ｂ）のステップで算出されたハッシュ値とが一致することを条件にして、前記端末との間にセッションを確立すると、前記端末を介して前記ユーザにサービスを提供する、ステップと、
を実行させる、ことを特徴とする。
【発明の効果】
【００１８】
以上の特徴により、本発明によれば、認証サーバと、サービスを提供するサーバとの間のセキュリティを高めることができる。
【図面の簡単な説明】
【００１９】
【図１】図１は、本発明の実施の形態における認証システム、認証サーバ、及びサービス提供サーバの構成を示すブロック図である。
【図２】図２は、本実施の形態で用いられる、サービスＩＤ、ユーザＩＤ、及びセッションＩＤを紐付けて管理するテーブルの一例を示す図である。
【図３】図３は、本実施の形態で用いられる、ユーザＩＤ、パスワード、及び別のＩＤを管理するテーブルの一例を示す図である。
【図４】図４は、本実施の形態における認証サーバの動作を示すフロー図である。
【図５】図５は、本実施の形態におけるサービス提供用サーバの動作を示すフロー図である。
【図６】図６は、本発明の実施の形態における認証サーバ及びサービス提供サーバを実現するコンピュータの一例を示すブロック図である。
【発明を実施するための形態】
【００２０】
（実施の形態）
以下、本発明の実施の形態における、認証システム、認証サーバ、サービス提供サーバ、認証方法、及びプログラムについて、図１～図４を参照しながら説明する。
【００２１】
［システム構成］
最初に、本実施の形態における、認証システム、認証サーバ及びサービス提供サーバの構成について図１～図３を用いて説明する。図１は、図１は、本発明の実施の形態における認証システム、認証サーバ、及びサービス提供サーバの構成を示すブロック図である。
【００２２】
図１に示すように、本実施の形態における認証システム１００は、認証サーバ１０と、サービス提供サーバ２０とを備えている。認証サーバ１０とサービス提供サーバ２０とは、互いに、インターネットなどのネットワーク（図１において図示せず）を介して接続されている。また、認証サーバ１０には、ネットワークを介して、ユーザの端末３０が接続される。なお、図１の例では、単一の端末３０のみが図示されているが、本実施の形態において端末の数は限定されるものではない。
【００２３】
また、図１に示すように、認証サーバ１０は、情報入力部１１と、送信部１２と、ハッシュ処理部１３と、セッション確立部１４とを備えている。認証サーバ１０は、このような構成により、サービス提供サーバ２０にサービスの提供を求めるユーザに対して端末３０を介して認証を行う。
【００２４】
情報入力部１１は、ユーザが端末３０を介して認証を要求すると、ユーザに端末３０を介してログイン情報を入力させる。本実施の形態では、情報入力部１１は、端末３０の表示画面にログインページ３１を表示させ、ユーザに、ログインページ３１上で、ログイン情報として、ユーザの識別子（ユーザＩＤ）とパスワードとを入力させる。

【００２５】
送信部１２は、入力されたログイン情報をサービス提供サーバ２０に送信する。ハッシュ処理部１３は、ログイン情報から、ハッシュ関数を用いて第１のハッシュ値を算出する。そして、ログイン情報がサービス提供サーバ２０に送信された後、後述するように、サービス提供サーバ２０が、第２のハッシュ値を算出すると、ハッシュ処理部１３は、それ自身が算出した第１のハッシュ値と第２のハッシュ値とが一致しているかどうかを判定する。
【００２６】
ハッシュ処理部１３が、第１のハッシュ値と第２のハッシュ値とが一致していると判定すると、セッション確立部１４は、セッションＩＤを発行し、端末３０との間にセッションを確立する。また、セッション確立部１４は、セッションＩＤを端末３０に送信する。端末３０は、セッションＩＤを用いることで、サービス提供サーバ２０からサービスを受けることができる。
【００２７】
また、図１に示すように、サービス提供サーバ２０は、ログイン情報判定部２１と、ハッシュ値算出部２２と、サービス提供部２３とを備えている。サービス提供サーバ２０は、このような構成により、認証サーバ１０が端末３０との間にセッションを確立すると、端末３０を介してユーザにサービスを提供する。
【００２８】
ログイン情報判定部２１は、認証サーバ１０から、端末３０を介して入力されたログイン情報が送信されると、ログイン情報が、予め登録されている情報と一致しているかどうかを判定する。
【００２９】
ハッシュ値算出部２２は、ログイン情報判定部２１が一致していると判定した場合に、ログイン情報からハッシュ関数を用いて第２のハッシュ値を算出する。なお、第１のハッシュ値の算出に用いられたハッシュ関数と、第２のハッシュ値の算出に用いられたハッシュ関数とは、同一のハッシュ関数であれば良い。本実施の形態において、用いられるハッシュ関数は特に限定されるものではない。
【００３０】
サービス提供部２３は、認証サーバ１０のセッション確立部１４が、第１のハッシュ値と第２のハッシュ値とが一致することを条件に、端末３０との間にセッションを確立すると、端末３０を介してユーザにサービスを提供する。提供されるサービスの例としては、在庫管理情報、社内情報といった各種情報の情報提供サービスなどが挙げられる。
【００３１】
以上のように、本実施の形態における認証システム１００では、認証サーバ１０及びサービス提供サーバ２０のそれぞれにおいて、別々に、ログイン情報に基づいてハッシュ値が算出される。そして、両者のハッシュ値が一致して初めて、端末３０は、サービス提供サーバ２０から、サービスを受けることができる。従って、本実施の形態によれば、認証サーバ１０と、サービス提供サーバ２０との間のセキュリティの向上が図られる。
【００３２】
ここで、図１に加えて図２及び図３を用いて、本実施の形態における認証システム１００、認証サーバ１０、及びサービス提供サーバ２０の構成を更に具体的に説明する。
【００３３】
まず、本実施の形態において、ユーザが利用する端末３０は、パーソナルコンピュータ、携帯電話、スマートフォンといった通信機能を備えた情報機器であれば良く、特に限定されるものではない。更に、以下の説明では、サービス提供サーバ２０は、企業の社内サーバ（例えばＡ社のサーバ）であり、認証サーバ１０はクラウドコンピューティングを行うサーバ（Ａ社とは別の企業が提供するサーバ）であるとする。ユーザは、Ａ社の社員であるとする。
【００３４】

また、図１に示すように、本実施の形態では、認証サーバ１０は、記憶部１５を備えており、情報入力部１１は、入力されたログイン情報を記憶部１５に記憶させる。ハッシュ処理部１３は、記憶部１５に記憶されているログイン情報から第１のハッシュ値を算出する。

【００３５】

そして、ハッシュ処理部１３は、第１のハッシュ値を算出すると、それと同時に、またはその後に、記憶されているログイン情報を記憶部１５から削除する。これは、認証サーバ１０からのログイン情報の漏洩を抑制するためである。

【００３６】

なお、「算出の後」にログイン情報が削除されるタイミングは、特に限定されるものではないが、第１のハッシュ値の算出時を起点とした経過時間が長すぎると、認証サーバ１０からログイン情報が漏洩する可能性が高くなる。よって、経過時間は出来る限り短くなるようにするのが良い。また、本実施の形態では、「算出の後」にログイン情報が削除されるタイミングは、サービス提供サーバ２０によって指定されても良い。

【００３７】

送信部１２は、本実施の形態では、ログイン情報を示す電子メール１６作成し、作成した電子メール１６によって、ログイン情報をサービス提供サーバ２０に送信する。本実施の形態において、送信部１２によるログイン情報の送信方式は、特に限定されるものではないが、電子メール１６による場合は、認証子システム１００の構築にかかるコストの低減を図ることができる。また、送信部１２は、電子メール１６を暗号化した状態で送信するのが好ましい。

【００３８】

また、本実施の形態では、ユーザが端末３０を介して認証を要求すると、情報入力部１１が、端末３０に対して、予め設定されたサービスＩＤを送信し、ログイン情報と共にサービスＩＤを返信させることができる。具体的には、情報入力部１１は、サービスＩＤが埋め込まれたログインページ３１を表示させる。そして、ユーザがログインページ３１上のログインボタンをクリックすると、入力されたＩＤ及びパスワードと共にサービスＩＤが返信される。

【００３９】

サービスＩＤが用いられる場合、記憶部１５は、図２に示すように、サービスＩＤ、ユーザＩＤ、及びセッションＩＤを紐付けて管理する。図２は、本実施の形態で用いられる、サービスＩＤ、ユーザＩＤ、及びセッションＩＤを紐付けて管理するテーブルの一例を示す図である。そして、送信部１２は、サービス提供サーバに、ログイン情報に加えてサービスＩＤを送信する。また、ハッシュ処理部１３は、ログイン情報及びサービスＩＤから第１のハッシュ値を算出する。更に、サービス提供サーバ２０のハッシュ値算出部２２は、ログイン情報及びサービスＩＤから第２のハッシュ値を算出する。

【００４０】

また、サービスＩＤが用いられる場合、認証サーバ１０は、使用するサービスＩＤを、予め、サービス提供サーバ２０に送信する。サービス提供サーバ２０は、本実施の形態では、記憶部２４を備えており、予め送信されてきたサービスＩＤを記憶部２４に登録する。なお、記憶部２４は、サービス提供サーバ２０に接続されたデータベースによって実現されていても良い。

【００４１】

そして、サービス提供サーバ２０は、ユーザによる認証の際に、認証サーバ１０からサービスＩＤが送信されてくると、送信されてきたサービスＩＤが登録されているかどうかを判定する。判定の結果、サービス提供サーバ２０は、送信されてきたサービスＩＤが登録されていない場合は、認証を認めず、端末３０へのサービスの提供を拒否する。これにより、なりすましメールによる攻撃が回避される。

【００４２】

また、本実施の形態では、記憶部２４には、ログイン情報としてのユーザＩＤ毎に、各

ユーザＩＤに対応するパスワードと、各ユーザＩＤに関連付けられた別のＩＤとが記憶されても良い。この場合、ログイン情報判定部２１は、まず、ログイン情報として送信されてきたユーザＩＤが、記憶部２４に記憶されている別のＩＤと関連付けられているか判定する。続いて、ログイン情報判定部２１は、ログイン情報として送信されてきたパスワードが、記憶部２４に記憶されているパスワードと一致するかどうかも判定する。

【００４３】

そして、ログイン情報判定部２１が、ユーザＩＤが別のＩＤと関連付けられており、且つ、パスワードが、記憶されているパスワードと一致している、と判定すると、ハッシュ値算出部２２は、ログイン情報からハッシュ関数を用いて第２のハッシュ値を算出する。

【００４４】

ここで、図３を用いて具体例を説明する。本例では、記憶部２４は、図３に示すテーブルを記憶している。図３は、本実施の形態で用いられる、ユーザＩＤ、パスワード、及び別のＩＤを管理するテーブルの一例を示す図である。

【００４５】

図３の例では、ユーザＩＤとして、ユーザのニックネームなどが用いられ、別のＩＤとして、Ａ社の社員であるユーザの社員ＩＤが用いられている。この場合は、ユーザは、ニックネームなどによってログインし、このニックネームなどが社員ＩＤと紐付けられている場合は、サービスの提供を受けることができる。このように、ユーザは、社員ＩＤといった極めて重要なＩＤを社外から入力することなく、社内のサーバにアクセスすることができる。この結果、社内サーバのセキュリティを確保しつつ、社内サーバと社外サーバとの連携を強化できる。

【００４６】

［システム動作］

次に、本発明の実施の形態における認証システム１００、認証サーバ１０、サービス提供サーバ２０の動作について図４及び図５を用いて説明する。図４は、本実施の形態における認証サーバの動作を示すフロー図である。図５は、本実施の形態におけるサービス提供用サーバの動作を示すフロー図である。以下の説明においては、適宜図１～図３を参酌する。

【００４７】

また、本実施の形態では、認証システム１００を構成する認証サーバ１０及びサービス提供サーバ２０を動作させることによって、認証方法が実施される。よって、本実施の形態における認証方法の説明は、以下の認証サーバ１０及びサービス提供サーバ２０の動作説明に代える。また、以下においては、まず、図４を用いて認証サーバの動作を説明し、続いて、図５を用いてサービス提供サーバの動作を説明する。

【００４８】

［認証サーバの動作］

図４に示すように、最初に、認証サーバ１０において、情報入力部１１は、ユーザから端末３０を介して認証が要求されているかどうかを判定する（ステップＡ１）。ステップＡ１の判定の結果、認証が要求されていない場合は、情報入力部１１は待機状態となる。一方、ステップＡ１の判定の結果、認証が要求されている場合は、情報入力部１１は、更に、ステップＡ１において認証を要求したユーザが既にログインしているかどうかを判定する（ステップＡ２）。

【００４９】

ステップＡ２の判定の結果、ユーザが既にログインしている場合は、情報入力部１１は、その旨を端末３０の画面に表示させ、処理を終了する。一方、ステップＡ２の判定の結果、ユーザが未だログインしていない場合は、情報入力部１１は、端末３０の画面にログインページ３１を表示させる（ステップＡ３））。また、ステップＡ３において、情報入力部１１は、ログインページ３１に任意のサービスＩＤを埋め込ませる。

【００５０】

次に、ユーザが、ログインページ３１上で、ユーザＩＤとパスワードとを入力し、ログ

インボタンをクリックすると、情報入力部１１は、ユーザＩＤ、パスワード及びサービスＩＤを受け取り、これらを記憶部１５に記憶させる（ステップＡ４）。

【００５１】

次に、ステップＡ４が実行されると、送信部１２は、情報入力部１１が受け取った、ユーザＩＤ、パスワード及びサービスＩＤをサービス提供サーバ２０に送信する（ステップＡ５）。

【００５２】

次に、ハッシュ処理部１３は、記憶部１５に記憶されているユーザＩＤ、パスワード及びサービスＩＤを取得し、これらを、予め設定されているハッシュ関数に代入して、ハッシュ値（第１のハッシュ値）を算出する（ステップＡ６）。また、ハッシュ処理部１３は、ステップＡ６の実行と同時に、または実行後に、記憶部１５に記憶されているユーザＩＤ、パスワード及びサービスＩＤを削除する。

【００５３】

ステップＡ６の実行後、ハッシュ処理部１３は、サービス提供サーバ２０から、ハッシュ値（第２のハッシュ値）が送信されているかどうかを判定する（ステップＡ７）。ステップＡ７の判定の結果、サービス提供サーバ２０からハッシュ値が送信されていない場合は、ハッシュ処理部１３は、サービス提供サーバ２０が認証失敗の通知を送信していることを条件に、処理を終了する。

【００５４】

一方、ステップＡ７の判定の結果、サービス提供サーバ２０からハッシュ値が送信されている場合は、ハッシュ処理部１３は、送信されてきたハッシュ値と、ステップＡ６で算出したハッシュ値とが一致するかどうかを判定する（ステップＡ８）。ステップＡ８の判定の結果、一致する場合は、ハッシュ処理部１３は、セッション確立部１４にステップＡ９を実行するように指示する。一方、ステップＡ８の判定の結果、一致しない場合は、ハッシュ処理部１３は、セッション確立部１４にステップＡ１０を実行するように指示する。

【００５５】

ステップＡ９では、セッション確立部１４は、セッションＩＤを発行し、端末３０との間にセッションを確立する。また、セッション確立部１４は、セッションＩＤを、記憶部１５に格納されているテーブル（図２参照）に書き込むと共に、端末３０に送信する。

【００５６】

また、セッションに有効期限が設定されている場合は、ステップＡ９の実行後、セッション確立部１４は、有効期限のチェックを実行する。そして、セッション確立からの経過時間が有効期限に到達した場合は、セッション確立部１４は、セッションを終了し、記憶部１５に格納されているテーブルからセッションＩＤを削除する。

【００５７】

一方、ステップＡ１０では、セッション確立部１４は、認証が失敗である旨を、端末３０に通知する。これにより、端末３の画面には、認証が失敗である旨が表示される。ステップＡ９またはステップＡ１０の実行後、認証サーバ１０における処理は終了する。

【００５８】

［サービス提供サーバの動作］

図５に示すように、最初に、サービス提供サーバ２０において、ログイン情報判定部２１は、認証サーバ１０が送信した、ユーザＩＤ、パスワード及びサービスＩＤを受信する（ステップＢ１）。

【００５９】

次に、ログイン情報判定部２１は、ステップＢ１で受信した、ユーザＩＤ、パスワード及びサービスＩＤが登録されている情報と一致しているかどうかを判定する（ステップＢ２）。

【００６０】

具体的には、ログイン情報判定部２１は、まず、記憶部２４に格納されているテーブル

（図３）を抽出する。そして、ログイン情報判定部２１は、受信したユーザＩＤに関連付けられている社員ＩＤがテーブルに登録されているか、受信したパスワードがテーブルに登録されているパスワードと一致しているか、について判定する。更に、ログイン情報判定部２１は、受信したサービスＩＤが予め記憶部２４に登録されているサービスＩＤと一致するかどうかについても判定する。

【００６１】

ステップＢ２の判定の結果、ユーザＩＤ、パスワード及びサービスＩＤが登録されている情報と一致している場合は、ログイン情報判定部２１は、ハッシュ値算出部２２にステップＢ３を実行させる。一方、ステップＢ２の判定の結果、ユーザＩＤ、パスワード及びサービスＩＤが登録されている情報と一致していない場合は、ログイン情報判定部２１は、認証が失敗である旨を認証サーバ１０に通知する（ステップＢ７）。

【００６２】

ステップＢ３では、ハッシュ値算出部２２は、ステップＢ１で受信した、ユーザＩＤ、パスワード及びサービスＩＤを、予め設定されているハッシュ関数に代入して、ハッシュ値（第２のハッシュ値）を算出する。次に、ハッシュ値算出部２２は、算出したハッシュ値を認証サーバ１０へと送信する（ステップＢ４）。これにより、認証サーバでは、ハッシュ値の一致判定（図４に示したステップＡ８）が行われる。

【００６３】

次に、ステップＢ４が実行されると、サービス提供部２３が、認証サーバ１０においてセッションＩＤが発行されているかどうかを判定する（ステップＢ５）。ステップＢ５の判定の結果、セッションＩＤが発行されている場合は、サービス提供部２３は、ユーザからの指示に応じてサービスを提供する（ステップＢ６）。そして、サービス提供部２３によるサービスの提供が終了すると、サービス提供サーバ２０における処理も終了する。一方、ステップＢ５の判定の結果、セッションＩＤが発行されていない場合は、そのまま、サービス提供サーバ２０における処理は終了する。

【００６４】

以上のように本実施の形態では、認証サーバ１０とサービス提供サーバ２０とで、別々にハッシュ値が算出され、二つのハッシュ値の一致を条件にセッションが確立されるので、認証サーバ１０とサービス提供サーバ２０との間のセキュリティの向上が図られる。また、認証サーバ上でのログイン情報の保持は、ハッシュ値の算出に要する時間だけで済み、更に、認証サーバには、重要な情報を保持させないようにもできるため、これらの点からもセキュリティの向上が図られる。

【００６５】

従って、サービス提供サーバ２０が企業の社内サーバであり、認証サーバ１０が社外のサーバである場合に、ユーザである社員が社外から端末３０を介して社内サーバにアクセスした際においても、十分なセキュリティが確保される。

【００６６】

本発明の実施の形態におけるプログラムとしては、コンピュータに、図４に示すステップＡ１～Ａ１０を実行させるプログラムと、図５に示すステップＢ１～Ｂ６を実行させるプログラムとが挙げられる。

【００６７】

前者のプログラムをコンピュータにインストールし、実行することによって、本実施の形態における認証サーバ１０を実現することができる。この場合、コンピュータのＣＰＵ（Central Processing Unit）は、情報入力部１１、送信部１２、ハッシュ処理部１３、セッション確立部１４として機能し、処理を行なう。また、コンピュータに備えられた、メモリ、ハードディスク等の記憶装置が記憶部１５として機能する。

【００６８】

また、後者のプログラムをコンピュータにインストールし、実行することによって、本実施の形態におけるサービス提供サーバ２０を実現することができる。この場合、コンピュータのＣＰＵは、ログイン情報判定部２１、ハッシュ値算出部２２、サービス提供部２

３として機能し、処理を行なう。また、コンピュータに備えられた、メモリ、ハードディスク等の記憶装置が記憶部２４として機能する。

【００６９】

ここで、実施の形態におけるプログラムを実行することによって、認証サーバ及びサービス提供サーバを実現するコンピュータについて図６を用いて説明する。図６は、本発明の実施の形態における認証サーバ及びサービス提供サーバを実現するコンピュータの一例を示すブロック図である。

【００７０】

図６に示すように、コンピュータ１１０は、ＣＰＵ１１１と、メインメモリ１１２と、記憶装置１１３と、入力インターフェイス１１４と、表示コントローラ１１５と、データリーダ／ライタ１１６と、通信インターフェイス１１７とを備える。これらの各部は、バス１２１を介して、互いにデータ通信可能に接続される。

【００７１】

ＣＰＵ１１１は、記憶装置１１３に格納された、本実施の形態におけるプログラム（コード）をメインメモリ１１２に展開し、これらを所定順序で実行することにより、各種の演算を実施する。メインメモリ１１２は、典型的には、ＤＲＡＭ（Dynamic Random Access Memory）等の揮発性の記憶装置である。また、本実施の形態におけるプログラムは、コンピュータ読み取り可能な記録媒体１２０に格納された状態で提供される。なお、本実施の形態におけるプログラムは、通信インターフェイス１１７を介して接続されたインターネット上で流通するものであっても良い。

【００７２】

また、記憶装置１１３の具体例としては、ハードディスクの他、フラッシュメモリ等の半導体記憶装置が挙げられる。入力インターフェイス１１４は、ＣＰＵ１１１と、キーボード及びマウスといった入力機器１１８との間のデータ伝送を仲介する。表示コントローラ１１５は、ディスプレイ装置１１９と接続され、ディスプレイ装置１１９での表示を制御する。データリーダ／ライタ１１６は、ＣＰＵ１１１と記録媒体１２０との間のデータ伝送を仲介し、記録媒体１２０からのプログラムの読み出し、及びコンピュータ１１０における処理結果の記録媒体１２０への書き込みを実行する。通信インターフェイス１１７は、ＣＰＵ１１１と、他のコンピュータとの間のデータ伝送を仲介する。

【００７３】

また、記録媒体１２０の具体例としては、ＣＦ（Compact Flash）及びＳＤ（Secure Digital）等の汎用的な半導体記憶デバイス、フレキシブルディスク（Flexible Disk）等の磁気記憶媒体、又はＣＤ－ＲＯＭ（Compact Disk Read Only Memory）などの光学記憶媒体が挙げられる。

【００７４】

上述した実施の形態の一部又は全部は、以下に記載する（付記１）～（付記２２）によって表現することができるが、以下の記載に限定されるものではない。

【００７５】

（付記１）

ユーザに対して端末を介して認証を行う認証サーバと、前記ユーザに前記端末を介してサービスを提供するサービス提供サーバとを備え、

前記認証サーバは、前記ユーザが前記端末を介して前記認証を要求すると、前記ユーザに前記端末を介してログイン情報を入力させ、そして、入力された前記ログイン情報を前記サービス提供サーバに送信すると共に、前記ログイン情報からハッシュ関数を用いて第１のハッシュ値を算出し、

前記サービス提供サーバは、前記認証サーバから送信された前記ログイン情報が、予め登録されている情報と一致しているかどうかを判定し、一致している場合に、前記ハッシュ関数と同一のハッシュ関数を用いて、前記ログイン情報から第２のハッシュ値を算出し、

前記第１のハッシュ値と前記第２のハッシュ値とが一致する場合に、前記認証サーバが

前記端末との間でセッションを確立する、
ことを特徴とする認証システム。
【００７６】
（付記２）
前記ログイン情報が、第１の識別子とパスワードとを含み、
前記サービス提供サーバが、
予め、前記第１の識別子毎に、当該第１の識別子に対応するパスワードと、当該第１の識別子に関連付けられた第２の識別子とを記憶し、
前記ログイン情報として送信されてきた第１の識別子が、記憶されている前記第２の識別子と関連付けられており、且つ、前記ログイン情報として送信されてきたパスワードが、記憶されているパスワードと一致する場合に、予め登録されている情報と一致していると判定する、付記１に記載の認証システム。
【００７７】
（付記３）
前記認証サーバが、前記ログイン情報を記憶し、記憶した前記ログイン情報から前記第１のハッシュ値を算出し、そして、前記第１のハッシュ値を算出すると同時に、または算出した後に、記憶した前記ログイン情報を削除する、
付記１または２に記載の認証システム。
【００７８】
（付記４）
前記認証サーバが、前記ログイン情報を示す電子メール作成し、作成した前記電子メールによって、前記ログイン情報を前記サービス提供サーバに送信する、付記１から３のいずれかに記載の認証システム。
【００７９】
（付記５）
前記認証サーバが、前記ユーザが前記端末を介して前記認証を要求すると、前記端末に対して、予め設定されたサービスＩＤを送信し、前記ログイン情報と共に前記サービスＩＤを返信させ、更に、前記サービス提供サーバに、前記ログイン情報に加えて前記サービスＩＤを送信し、そして、前記ログイン情報及び前記サービスＩＤから前記第１のハッシュ値を算出し、
前記サービス提供サーバが、前記ログイン情報及び前記サービスＩＤから前記第２のハッシュ値を算出する、付記１～４のいずれかに記載の認証システム。
【００８０】
（付記６）
サービス提供サーバにサービスの提供を求めるユーザに対して端末を介して認証を行う認証サーバであって、
前記ユーザが前記端末を介して前記認証を要求すると、前記ユーザに前記端末を介してログイン情報を入力させる、情報入力部と、
入力された前記ログイン情報を前記サービス提供サーバに送信する、送信部と、
前記ログイン情報からハッシュ関数を用いて第１のハッシュ値を算出する、ハッシュ処理部と、
前記端末との間にセッションを確立する、セッション確立部とを備え、
前記ハッシュ処理部は、
前記サービス提供サーバが、送信された前記ログイン情報に基づいて、それが予め登録されている情報と一致していることを条件に、前記ハッシュ関数と同一のハッシュ関数を用いて、第２のハッシュ値を算出すると、
前記第１のハッシュ値と前記第２のハッシュ値とが一致しているかどうかを判定し、
前記セッション確立部は、前記ハッシュ処理部が一致していると判定する場合に、前記セッションを確立する、
ことを特徴とする認証サーバ。

【００８１】
（付記７）
前記ログイン情報を記憶する記憶部を更に備え、
前記ハッシュ処理部が、前記記憶部に記憶されている前記ログイン情報から前記第１のハッシュ値を算出し、そして、前記第１のハッシュ値を算出すると同時に、または算出した後に、記憶されている前記ログイン情報を前記記憶部から削除する、
付記６に記載の認証サーバ。
【００８２】
（付記８）
前記送信部が、前記ログイン情報を示す電子メール作成し、作成した前記電子メールによって、前記ログイン情報を前記サービス提供サーバに送信する、付記６または７に記載の認証サーバ。
【００８３】
（付記９）
前記情報入力部が、前記ユーザが前記端末を介して前記認証を要求すると、前記端末に対して、予め設定されたサービスＩＤを送信し、前記ログイン情報と共に前記サービスＩＤ返信させ、
前記送信部が、前記サービス提供サーバに、前記ログイン情報に加えて前記サービスＩＤを送信し、
前記ハッシュ処理部が、前記ログイン情報及び前記サービスＩＤから前記第１のハッシュ値を算出し、そして、前記サービス提供サーバが、前記ログイン情報及び前記サービスＩＤから前記第２のハッシュ値を算出すると、前記第１のハッシュ値と前記第２のハッシュ値とが一致しているかどうかを判定する、
付記６～８のいずれかに記載の認証サーバ。
【００８４】
（付記１０）
認証サーバが端末との間にセッションを確立した場合に、前記端末を介してユーザにサービスを提供するサービス提供サーバであって、
前記認証サーバから、前記端末を介して入力されたログイン情報が送信されると、前記ログイン情報が、予め登録されている情報と一致しているかどうかを判定する、ログイン情報判定部と、
前記ログイン情報判定部が一致していると判定した場合に、前記ログイン情報からハッシュ関数を用いてハッシュ値を算出する、ハッシュ値算出部と、
前記認証サーバによって、それが前記ハッシュ関数と同一のハッシュ関数を用いて前記ログイン情報から算出したハッシュ値と、前記ハッシュ値算出部が算出したハッシュ値とが一致することを条件にして、前記端末との間にセッションが確立されると、前記端末を介して前記ユーザにサービスを提供する、サービス提供部と、を備えている、
ことを特徴とするサービス提供サーバ。
【００８５】
（付記１１）
前記ログイン情報が、第１の識別子とパスワードとを含み、
当該サービス提供サーバが、前記第１の識別子毎に、当該第１の識別子に対応するパスワードと、当該第１の識別子に関連付けられた第２の識別子とを記憶する、記憶部を更に備え、
前記ログイン情報判定部は、前記ログイン情報として送信されてきた第１の識別子が、前記記憶部に記憶されている前記第２の識別子と関連付けられており、且つ、前記ログイン情報として送信されてきたパスワードが、前記記憶部に記憶されているパスワードと一致する場合に、予め登録されている情報と一致していると判定する、付記１０に記載のサービス提供サーバ。
【００８６】

（付記１２）
ユーザに対して端末を介して認証を行う認証サーバと、前記ユーザに前記端末を介してサービスを提供するサービス提供サーバとを用いる認証方法であって、
（ａ）前記ユーザが前記端末を介して前記認証を要求すると、前記認証サーバが、前記ユーザに前記端末を介してログイン情報を入力させる、ステップと、
（ｂ）前記認証サーバが、入力された前記ログイン情報を前記サービス提供サーバに送信する、ステップと、
（ｃ）前記認証サーバが、入力された前記ログイン情報からハッシュ関数を用いて第１のハッシュ値を算出する、ステップと、
（ｄ）前記サービス提供サーバが、前記ログイン情報が、予め登録されている情報と一致しているかどうかを判定し、一致している場合に、前記ハッシュ関数と同一のハッシュ関数を用いて、前記ログイン情報から第２のハッシュ値を算出する、ステップと、
（ｅ）前記認証サーバが、前記（ｃ）のステップで算出された前記第１のハッシュ値と前記（ｄ）のステップで算出された前記第２のハッシュ値とが一致する場合に、前記端末との間でセッションを確立する、ステップと、を有することを特徴とする認証方法。
【００８７】
（付記１３）
前記ログイン情報が、第１の識別子とパスワードとを含み、
（ｆ）前記サービス提供サーバが、前記第１の識別子毎に、当該第１の識別子に対応するパスワードと、当該第１の識別子に関連付けられた第２の識別子とを記憶するステップを更に有し、
前記（ｄ）のステップにおいて、前記サービス提供サーバが、
前記ログイン情報として送信されてきた第１の識別子が、記憶されている前記第２の識別子と関連付けられており、且つ、前記ログイン情報として送信されてきたパスワードが、記憶されているパスワードと一致する場合に、予め登録されている情報と一致していると判定する、付記１２に記載の認証方法。
【００８８】
（付記１４）
前記（ａ）のステップにおいて、前記認証サーバが、前記ログイン情報を記憶し、
前記（ｃ）のステップにおいて、前記認証サーバが、前記（ａ）のステップで記憶した前記ログイン情報から前記第１のハッシュ値を算出し、そして、前記第１のハッシュ値を算出すると同時に、または算出した後に、記憶した前記ログイン情報を削除する、
付記１２または１３に記載の認証方法。
【００８９】
（付記１５）
前記（ｂ）のステップにおいて、前記認証サーバが、前記ログイン情報を示す電子メール作成し、作成した前記電子メールによって、前記ログイン情報を前記サービス提供サーバに送信する、付記１２から１４のいずれかに記載の認証方法。
【００９０】
（付記１６）
前記（ａ）のステップにおいて、前記認証サーバが、前記ユーザが前記端末を介して前記認証を要求すると、前記端末に対して、予め設定されたサービスＩＤを送信し、前記ログイン情報と共に前記サービスＩＤを返信させ、
前記（ｂ）のステップにおいて、前記認証サーバが、前記サービス提供サーバに、前記ログイン情報に加えて前記サービスＩＤを送信し、
前記（ｃ）のステップにおいて、前記認証サーバが、前記ログイン情報及び前記サービスＩＤから前記第１のハッシュ値を算出し、
前記（ｄ）のステップにおいて、前記サービス提供サーバが、前記ログイン情報及び前記サービスＩＤから前記第２のハッシュ値を算出する、
付記１２～１５のいずれかに記載の認証方法。

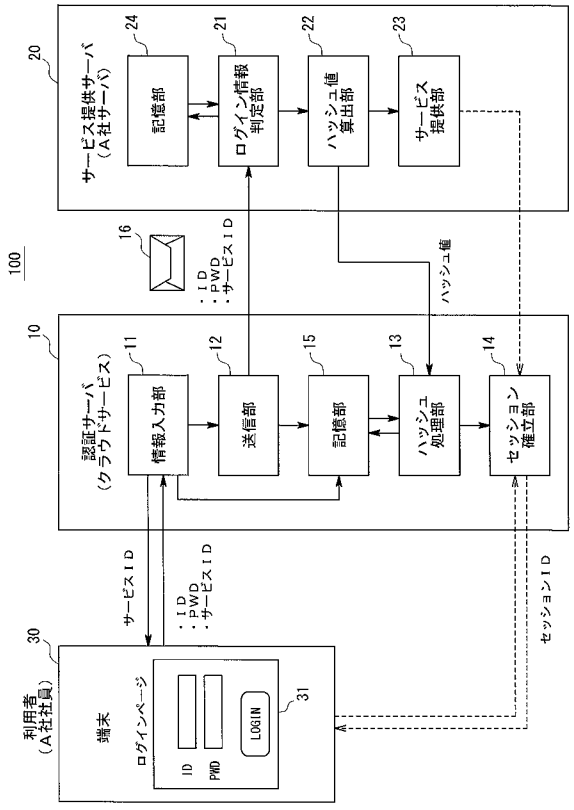
【００９１】
（付記１７）
サービス提供サーバにサービスの提供を求めるユーザに対する、端末を介した認証を、コンピュータによって行うための、プログラムであって、
前記コンピュータに、
（ａ）前記ユーザが前記端末を介して前記認証を要求すると、前記ユーザに前記端末を介してログイン情報を入力させる、ステップと、
（ｂ）前記（ａ）のステップで入力された前記ログイン情報を前記サービス提供サーバに送信する、ステップと、
（ｃ）前記（ａ）のステップで入力された前記ログイン情報からハッシュ関数を用いて第１のハッシュ値を算出する、ステップと、
（ｄ）前記サービス提供サーバが、送信された前記ログイン情報に基づいて、それが予め登録されている情報と一致していることを条件に、前記ハッシュ関数と同一のハッシュ関数を用いて、第２のハッシュ値を算出すると、前記（ｃ）のステップで算出した前記第１のハッシュ値と前記サービス提供サーバが算出した前記第２のハッシュ値とが一致しているかどうかを判定する、ステップと、
（ｅ）前記（ｄ）のステップで一致していると判定する場合に、前記端末との間にセッションを確立する、ステップと、
を実行させる、プログラム。
【００９２】
（付記１８）
前記（ａ）のステップにおいて、前記ログイン情報を記憶し、
前記（ｃ）のステップにおいて、記憶されている前記ログイン情報から前記第１のハッシュ値を算出し、そして、前記第１のハッシュ値を算出すると同時に、または算出した後に、記憶されている前記ログイン情報を削除する、
付記１７に記載のプログラム。
【００９３】
（付記１９）
前記（ｂ）のステップにおいて、前記ログイン情報を示す電子メール作成し、作成した前記電子メールによって、前記ログイン情報を前記サービス提供サーバに送信する、付記１７または１８に記載のプログラム。
【００９４】
（付記２０）
前記（ａ）のステップにおいて、前記ユーザが前記端末を介して前記認証を要求すると、前記端末に対して、予め設定されたサービスＩＤを送信し、前記ログイン情報と共に前記サービスＩＤを返信させ、
前記（ｂ）のステップにおいて、前記サービス提供サーバに、前記ログイン情報に加えて前記サービスＩＤを送信し、
前記（ｃ）のステップにおいて、前記ログイン情報及び前記サービスＩＤから前記第１のハッシュ値を算出し、
前記（ｄ）のステップにおいて、前記サービス提供サーバが、前記ログイン情報及び前記サービスＩＤから前記第２のハッシュ値を算出すると、前記第１のハッシュ値と前記第２のハッシュ値とが一致しているかどうかを判定する、
付記１７～１９のいずれかに記載のプログラム。
【００９５】
（付記２１）
認証サーバが端末との間にセッションを確立した場合に、コンピュータによって、前記端末を介してユーザにサービスを提供するための、プログラムであって、
前記コンピュータに、
（ａ）前記認証サーバから、前記端末を介して入力されたログイン情報が送信されると、

前記ログイン情報が、予め登録されている情報と一致しているかどうかを判定する、ステップと、
（ｂ）前記（ａ）のステップで一致していると判定した場合に、前記ログイン情報からハッシュ関数を用いてハッシュ値を算出する、ステップと、
（ｃ）前記認証サーバが、それが前記ハッシュ関数と同一のハッシュ関数を用いて前記ログイン情報から算出したハッシュ値と、前記（ｂ）のステップで算出されたハッシュ値とが一致することを条件にして、前記端末との間にセッションを確立すると、前記端末を介して前記ユーザにサービスを提供する、ステップと、
を実行させる、プログラム。
【００９６】
（付記２２）
前記ログイン情報が、第１の識別子とパスワードとを含み、
（ｄ）前記第１の識別子毎に、当該第１の識別子に対応するパスワードと、当該第１の識別子に関連付けられた第２の識別子とを記憶する、ステップを、更に前記コンピュータに実行させ、
前記（ａ）のステップにおいて、前記ログイン情報として送信されてきた第１の識別子が、前記（ｄ）のステップで記憶されている前記第２の識別子と関連付けられており、且つ、前記ログイン情報として送信されてきたパスワードが、前記（ｄ）のステップで記憶されているパスワードと一致する場合に、予め登録されている情報と一致していると判定する、付記２１に記載のプログラム。

【００９７】
以上、実施の形態を参照して本願発明を説明したが、本願発明は上記実施の形態に限定されるものではない。本願発明の構成や詳細には、本願発明のスコープ内で当業者が理解し得る様々な変更をすることができる。
【００９８】
この出願は、２０１０年１２月１６日に出願された日本出願特願２０１０－２８０６３７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】
【００９９】
以上のように本発明によれば、認証サーバと、サービスを提供するサーバとの間のセキュリティを高めることができる。従って、本発明は、特に、企業などが、クラウドコンピューティングを利用するため、社外サーバと社内サーバとを連携させる場合に有用である。
【符号の説明】
【０１００】
１０　認証サーバ
１１　情報入力部
１２　送信部
１３　ハッシュ処理部
１４　セッション確立部
１５　記憶部
１６　電子メール
２０　サービス提供サーバ
２１　ログイン情報判定部
２２　ハッシュ値算出部
２３　サービス提供部
２４　記憶部
３０　端末

１００　認証システム
１１０　コンピュータ
１１１　ＣＰＵ
１１２　メインメモリ
１１３　記憶装置
１１４　入力インターフェイス
１１５　表示コントローラ
１１６　データリーダ／ライタ
１１７　通信インターフェイス
１１８　入力機器
１１９　ディスプレイ装置
１２０　記録媒体
１２１　バス

【図１】



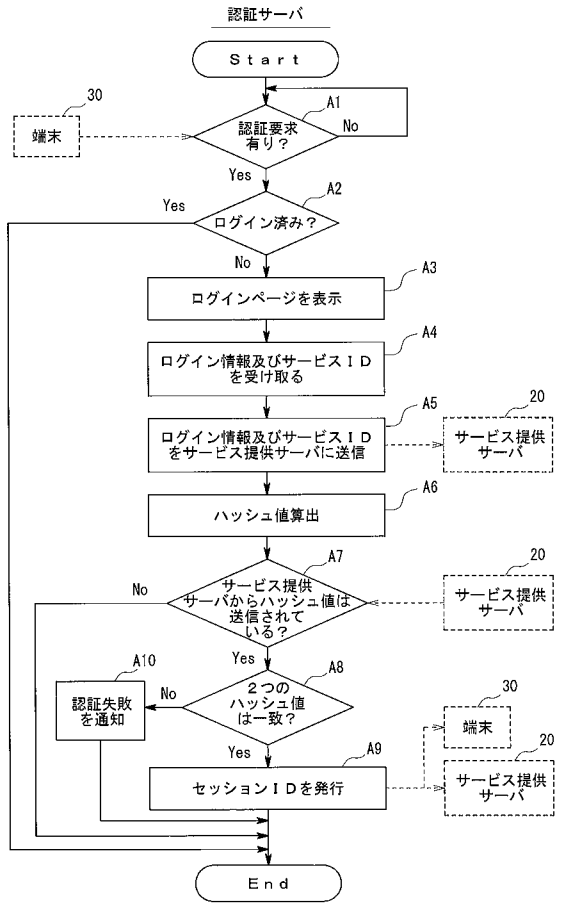
【図２】

ユーザＩＤ	サービスＩＤ	セッションＩＤ
Blackbird	S11AY001	SS000231
Yassy	S22BY001	SS000232
Redstone	S33CY001	SS000233
・・・	・・・	・・・

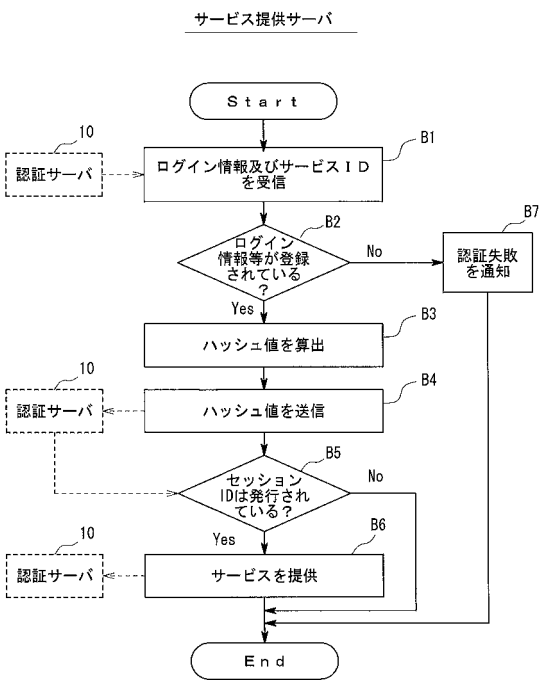
【図３】

ユーザＩＤ	社員ＩＤ	パスワード
Blackbird	104045	AAA11
Yassy	104085	ABB34
Redstone	104063	B1C69
・・・	・・・	・・・

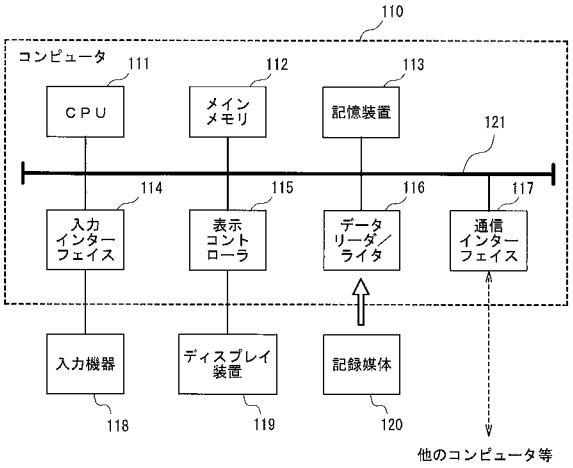
【図４】


認証サーバ
Ｓｔａｒｔ
30
端末
A1
認証要求有り？
No
Yes
A2
Yes
ログイン済み？
No
A3
ログインページを表示
A4
ログイン情報及びサービスＩＤを受け取る
A5
20
ログイン情報及びサービスＩＤをサービス提供サーバに送信
サービス提供サーバ
A6
ハッシュ値算出
A7
20
No
サービス提供サーバからハッシュ値は送信されている？
サービス提供サーバ
Yes
A10
A8
No
認証失敗を通知
２つのハッシュ値は一致？
30
端末
Yes
A9
20
セッションＩＤを発行
サービス提供サーバ
Ｅｎｄ

【図５】


サービス提供サーバ
Ｓｔａｒｔ
10
認証サーバ
B1
ログイン情報及びサービスＩＤを受信
B7
B2
No
ログイン情報等が登録されている？
認証失敗を通知
Yes
B3
ハッシュ値を算出
10
認証サーバ
B4
ハッシュ値を送信
B5
No
セッションIDは発行されている？
Yes
B6
10
認証サーバ
サービスを提供
Ｅｎｄ

【図６】


110
コンピュータ
111
ＣＰＵ
112
メインメモリ
113
記憶装置
121
114
入力インターフェイス
115
表示コントローラ
116
データリーダ／ライタ
117
通信インターフェイス
入力機器
ディスプレイ装置
記録媒体
118
119
120
他のコンピュータ等

フロントページの続き

審査官　金木　陽一

(56)参考文献　特開２００３－３３８８２３（ＪＰ，Ａ）
特開２００８－０８３８５９（ＪＰ，Ａ）
特開２００９－１３０４４７（ＪＰ，Ａ）
特開２００９－２５８９１７（ＪＰ，Ａ）
特開２００９－２８２５６１（ＪＰ，Ａ）
特開２０１０－０６１３０２（ＪＰ，Ａ）
特開２０１０－０６８４６０（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／３２
Ｇ０６Ｆ　２１／３１