(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2018-82244
(P2018-82244A)
(43)公開日　平成30年5月24日(2018.5.24)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/32	(2006.01)	H04L	9/00	675B	5J104
G06F 21/33	(2013.01)	G06F	21/33		
G09C 1/00	(2006.01)	G09C	1/00	640E	

審査請求 有　請求項の数 32　ＯＬ　（全 26 頁）

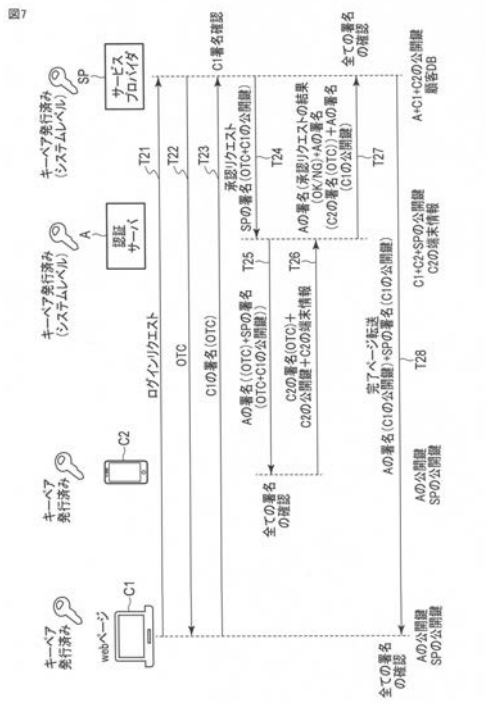
(21)出願番号　特願2016-221657 (P2016-221657)
(22)出願日　平成28年11月14日 (2016.11.14)

(71)出願人　516260888
ソラミツ株式会社
東京都千代田区二番町１４番地　日本テレビ麹町ビル西館４Ｆ
(71)出願人　501044644
楽天証券株式会社
東京都世田谷区玉川一丁目１４番１号　楽天クリムゾンハウス
(74)代理人　100108855
弁理士　蔵田　昌俊
(74)代理人　100103034
弁理士　野河　信久
(74)代理人　100153051
弁理士　河野　直樹

最終頁に続く

(54)【発明の名称】ログイン認証システム、ログイン認証システムにおけるサービスプロバイダ及び認証サーバ、ログイン認証システムにおけるサービスプロバイダ、認証サーバ、コンピュータ及び携帯端末のた

(57)【要約】　（修正有）
【課題】サービスプロバイダが認証サーバと共に、ユーザがＩＤおよびパスワードの入力の必要がなく、安全に機密性の高いサービスにログインすることができるログイン認証システムを提供する。
【解決手段】サービスプロバイダと認証サーバは第１のユーザ端末から受信したログインリクエストに基づいて、第１のユーザ端末による署名生成と検証、サービスプロバイダによる署名生成と検証、認証サーバによる署名生成と検証、第２のユーザ端末による署名生成と検証を順次行って、第１のユーザ端末のログイン認証を行なう。ログイン認証が成功した場合に、ログインが成功したことを示す画面情報が第１のユーザ端末に送信される。
【選択図】図７



【特許請求の範囲】
【請求項１】
サービスプロバイダと、認証サーバとを有するログイン認証システムにおいて、
前記サービスプロバイダは、
第１のユーザ端末からログインリクエストを受信するログインリクエスト受信手段と、
前記受信したログインリクエストに応答して、前記第１のユーザ端末に識別コードを送信する識別コード送信手段と、
前記第１のユーザ端末の署名がされた前記識別コードを受信する第１コード受信手段と、
前記受信した前記第１のユーザ端末の署名がされた前記識別コードの前記第１のユーザ端末の署名が確認された場合、前記認証サーバに、前記識別コードと前記第１のユーザ端末の公開鍵とに前記サービスプロバイダの署名がされた第１データを含む承認リクエストを前記認証サーバに送信する承認リクエスト送信手段と
を具備し、
前記認証サーバは、
前記承認リクエストを受信し、前記承認リクエストに含まれる第１データに含まれる前記サービスプロバイダの署名が確認された場合に、前記第１データ及び前記識別コードに前記認証サーバの署名を行ない、前記認証サーバの署名がされた前記第１データ及び前記識別コードを第２のユーザ端末に送信する第１データ送信手段と、
前記認証サーバの署名がされた前記第１データ及び前記識別コードの送信に応答して、前記第２のユーザ端末から、前記第２のユーザ端末の署名がされた前記識別コード、前記第２のユーザ端末の公開鍵及び前記第２のユーザ端末の端末情報を含む第２データを受信する第２データ受信手段と、
前記受信した第２データに含まれる前記第２のユーザ端末の署名及び前記端末情報が確認された場合に、前記認証サーバの署名がされた前記承認リクエストに対する結果を示す承認結果情報及び前記認証サーバの署名がされた前記第２のユーザ端末の署名が付された前記識別コードを含む第３データを前記サービスプロバイダに送信する第３データ送信手段と
を具備し、
前記サービスプロバイダは、
前記認証サーバから前記第３データを受信する第３データ受信手段と、
前記受信した前記第３データの前記認証サーバ及び前記第２のユーザ端末の署名が確認された場合、前記認証サーバの署名がされた前記第１のユーザ端末の公開鍵及び前記サービスプロバイダの署名がされた前記第１のユーザ端末の公開鍵を前記ログインリクエストの後の画面情報とともに前記第１のユーザ端末に送信する画面情報送信手段と
を具備するログイン認証システム。
【請求項２】
前記第１のユーザ端末から初期登録リクエストを受信する初期登録受信手段と、
前記初期登録リクエストを受信した場合に、前記第１のユーザ端末の公開鍵、前記第２のユーザ端末の公開鍵、前記サービスプロバイダの公開鍵、前記認証サーバの公開鍵及びユーザの識別情報を互いに関連付ける処理を行なう関連付け処理手段をさらに具備する請求項１記載のログイン認証システム。
【請求項３】
前記関連付け処理手段は、
前記サービスプロバイダが、
前記第１のユーザ端末から初期登録リクエストを受信した場合、前記認証サーバの署名が行なわれた初期識別コード及び前記サービスプロバイダの署名が付された初期識別コードを含む第１の初期登録データを前記第１のユーザ端末に送信する第１の初期登録データ送信手段を具備し、
前記認証サーバが、

前記第１の初期登録データの送信に応答して、前記第２のユーザ端末から第２のユーザ端末の署名が行なわれた前記第１のユーザ端末の署名が付された前記初期識別コード、暗号化されたユーザの識別情報、前記第１のユーザ端末の公開鍵、前記第２のユーザ端末の公開鍵及び前記第２のユーザ端末の端末情報を含む第２の初期登録データを受信する第１の初期登録データ受信手段と、

前記第２の初期登録データに含まれる前記第２のユーザ端末の署名が行なわれた前記第１のユーザ端末の署名が付された前記初期識別コードの前記第１のユーザ端末及び前記第２のユーザ端末の署名が確認され、かつ前記初期識別コードが確認された場合に、前記認証サーバの署名がされた前記第２のユーザ端末及び前記第１のユーザ端末の署名が付された前記初期識別コード、前記暗号化されたユーザの識別情報、前記第１のユーザ端末の公開鍵及び前記第２のユーザ端末の公開鍵を含む第３の初期登録データを前記サービスプロバイダに送信する第２の初期登録データ送信手段とを具備し、

前記サービスプロバイダが、

前記第３の初期登録データを前記認証サーバから受信する第２の初期登録データ受信手段と、

前記受信した第３の初期登録データに含まれる前記第１のユーザ端末、前記第２のユーザ端末及び認証サーバの署名及びユーザの識別情報が確認された場合、前記初期登録リクエストの後の初期登録完了画面情報とともに前記第１のユーザ端末に送信する初期登録完了画面情報送信手段とをさらに具備する、

請求項２記載のログイン認証システム。

【請求項４】

前記サービスプロバイダは、

前記第１のユーザ端末の公開鍵、前記第２のユーザ端末の公開鍵、前記認証サーバの公開鍵及びユーザの識別情報を互いに関連付けて記憶する記憶部を具備する請求項１記載のログイン認証システム。

【請求項５】

前記サービスプロバイダが提供するサービスに関するユーザ関連情報が、前記ユーザの識別情報にさらに関連付けられている、請求項４記載のログイン認証システム。

【請求項６】

前記認証サーバは、前記第１のユーザ端末の公開鍵、前記第２のユーザ端末の公開鍵、前記サービスプロバイダの公開鍵及び前記第２のユーザ端末の端末情報が互いに関連付けて記憶されている記憶部を具備する、請求項１記載のログイン認証システム。

【請求項７】

前記第３データは、前記認証サーバの署名がされた前記第１のユーザ端末の公開鍵を含む、請求項１記載のログイン認証システム。

【請求項８】

前記第３の初期登録データは、前記認証サーバの署名がされた前記第１のユーザ端末の公開鍵を含む、請求項３記載のログイン認証システム。

【請求項９】

第１のユーザ端末からログインリクエストを受信するログインリクエスト受信手段と、

前記受信したログインリクエストに応答して、前記第１のユーザ端末に識別コードを送信する識別コード送信手段と、

前記第１のユーザ端末の署名がされた前記識別コードを受信する第１コード受信手段と、

前記受信した前記第１のユーザ端末の署名がされた前記識別コードの前記第１のユーザ端末の署名が確認された場合に、前記識別コードと前記第１のユーザ端末の公開鍵とに前記サービスプロバイダの署名がされた第１データを含む承認リクエストを前記認証サーバに送信する承認リクエスト送信手段と、

前記第１データの送信に応答して、前記認証サーバから前記認証サーバの署名がされた前記承認リクエストに対する結果を示す承認結果情報、前記認証サーバの署名がされた前

記第２のユーザ端末の署名が付された前記識別コード及び前記第１のユーザ端末の公開鍵を含む第２データを受信する第２データ受信手段と、
前記受信した前記第２データの前記認証サーバ及び前記第２のユーザ端末の署名が確認された場合、前記認証サーバの署名がされた前記第１のユーザ端末の公開鍵及び前記サービスプロバイダの署名がされた前記第１のユーザ端末の公開鍵を前記ログインリクエストの後の画面情報とともに前記第１のユーザ端末に送信する画面情報送信手段と
を具備するログイン認証システムにおけるサービスプロバイダ。
【請求項１０】
前記第１のユーザ端末から初期登録リクエストを受信した場合、前記認証サーバの署名が行なわれた初期識別コード及び前記サービスプロバイダの署名が付された初期識別コードを含む第１の初期登録データを前記第１のユーザ端末に送信する第１の初期登録データ送信手段と、
前記第１の初期登録データの送信後、前記認証サーバの署名がされた前記第２のユーザ端末及び前記第１のユーザ端末の署名が付された前記初期識別コード、暗号化されたユーザの識別情報、前記第１のユーザ端末の公開鍵及び前記第２のユーザ端末の公開鍵を含む第２の初期登録データを前記認証サーバから受信する第２の初期登録データ受信手段と、
前記受信した第２の初期登録データに含まれる前記第１のユーザ端末、前記第２のユーザ端末及び認証サーバの署名及び前記ユーザの識別情報が確認された場合、前記初期登録リクエストの後の初期登録完了画面情報とともに前記第１のユーザ端末に送信する初期登録完了画面情報送信手段と
をさらに具備する請求項９記載のサービスプロバイダ。
【請求項１１】
前記第１のユーザ端末の公開鍵、前記第２のユーザ端末の公開鍵、前記認証サーバの公開鍵及びユーザの識別情報を互いに関連付けて記憶する記憶部を具備する請求項９記載のサービスプロバイダ。
【請求項１２】
前記サービスプロバイダが提供するサービスに関するユーザ関連情報が、前記ユーザの識別情報にさらに関連付けられている、請求項１１記載のサービスプロバイダ。
【請求項１３】
サービスプロバイダから承認リクエストを受信し、前記承認リクエストに含まれる第１データに含まれる前記サービスプロバイダの署名が確認された場合に、前記第１データ及び識別コードに認証サーバの署名を行ない、前記認証サーバの署名がされた前記第１データ及び前記識別コードを第２のユーザ端末に送信する第１データ送信手段と、
前記認証サーバの署名がされた前記第１データ及び前記識別コードに応答して、前記第２のユーザ端末から、前記第２のユーザ端末の署名がされた前記識別コード、前記第２のユーザ端末の公開鍵及び前記第２のユーザ端末の端末情報を含む第２データを受信する第２データ受信手段と、
前記受信した第２データに含まれる前記第２のユーザ端末の署名及び前記端末情報が確認された場合に、前記認証サーバの署名がされた前記承認リクエストに対する結果を示す承認結果情報及び前記認証サーバの署名がされた前記第２のユーザ端末の署名が付された前記識別コードを含む第３データを前記サービスプロバイダに送信する第３データ送信手段と
を具備する認証サーバ。
【請求項１４】
前記認証サーバの署名が行なわれた初期識別コード及び前記サービスプロバイダの署名が付された初期識別コードを含む第１の初期登録データの送信に応答して、前記第２のユーザ端末から第２のユーザ端末の署名が行なわれた第１のユーザ端末の署名が付された前記初期識別コード、暗号化されたユーザの識別情報、前記第１のユーザ端末の公開鍵、前記第２のユーザ端末の公開鍵及び前記第２のユーザ端末の端末情報を含む第２の初期登録データを受信する第１の初期登録データ受信手段と、

前記第２の初期登録データに含まれる前記第２のユーザ端末の署名が行なわれた前記第１のユーザ端末の署名が付された前記初期識別コードの前記第１のユーザ端末及び前記第２のユーザ端末の署名が確認され、かつ前記初期識別コードが確認された場合に、前記認証サーバの署名がされた前記第２のユーザ端末及び前記第１のユーザ端末の署名が付された前記初期識別コード、前記暗号化された前記ユーザの識別情報、前記第１のユーザ端末の公開鍵及び前記第２のユーザ端末の公開鍵を含む第３の初期登録データを前記サービスプロバイダに送信する第１の初期登録データ送信手段と
を具備する請求項１３記載の認証サーバ。
【請求項１５】
前記認証サーバは、第１のユーザ端末の公開鍵、前記第２のユーザ端末の公開鍵、前記サービスプロバイダの公開鍵及び前記第２のユーザ端末の端末情報が互いに関連付けて記憶されている記憶部を具備する、請求項１３記載の認証サーバ。
【請求項１６】
前記第３データは、前記認証サーバの署名がされた第１のユーザ端末の公開鍵を含む、請求項１３記載の認証サーバ。
【請求項１７】
前記第３の初期登録データは、前記認証サーバの署名がされた前記第１のユーザ端末の公開鍵を含む、請求項１４記載の認証サーバ。
【請求項１８】
第１のユーザ端末と、第２のユーザ端末とを具備し、前記第２のユーザ端末を使用して、前記第１のユーザ端末にログインを行なうログイン認証システムにおけるログイン処理の前記第２のユーザ端末におけるログイン認証方法において、
認証サーバの署名がされた第１データ及び識別コードを受信し、前記第１データは、前記識別コードと前記第１のユーザ端末の公開鍵とにサービスプロバイダの署名がされたデータであり、
前記受信した前記認証サーバの署名がされた前記第１データ及び前記識別コードの前記認証サーバ及び前記サービスプロバイダの署名が確認された場合に、前記第２のユーザ端末の署名がされた前記識別コード、前記第２のユーザ端末の公開鍵及び前記第２のユーザ端末の端末情報を含む第１データを前記認証サーバに送信し、
これにより、前記第１のユーザ端末のログインを行なうログイン認証方法。
【請求項１９】
前記ログイン認証システムの初期登録を行なう場合に、前記第１のユーザ端末の署名がされた初期識別コードと、前記第１のユーザ端末の前記公開鍵を読み込み、
前記第１のユーザ端末の署名が確認された場合に、前記第２のユーザ端末の署名が行なわれた前記第１のユーザ端末の署名が付された前記初期識別コード、暗号化されたユーザの識別情報、前記第１のユーザ端末の公開鍵、前記第２のユーザ端末の公開鍵及び前記第２のユーザ端末の端末情報を含む初期登録データを送信する、
請求項１８記載のログイン認証方法。
【請求項２０】
前記読み込みは、前記第１のユーザ端末の署名がされた初期識別コードと、前記第１のユーザ端末の前記公開鍵を含むＱＲコードを読み込む、請求項１９記載のログイン認証方法。
【請求項２１】
第１のユーザ端末と、第２のユーザ端末とを具備し、前記第２のユーザ端末を使用して、前記第１のユーザ端末にログインを行なうログイン認証システムにおけるログイン処理の前記第１のユーザ端末におけるログイン認証方法において、
ログインリクエストをサービスプロバイダに送信し、
前記送信したログインリクエストに応答して、前記サービスプロバイダから識別コードを受信し、
前記受信した識別コードに前記第１のユーザ端末の署名を行ない、前記第１のユーザ端

末の署名がされた前記識別コードを前記サービスプロバイダに送信し、
前記第１のユーザ端末の署名がされた前記識別コードを前記サービスプロバイダに送信した後に、前記サービスプロバイダから認証サーバの署名がされた前記第１のユーザ端末の公開鍵及び前記サービスプロバイダの署名がされた前記第１のユーザ端末の公開鍵を前記ログインリクエストの後の画面情報とともに受信する、
ログイン認証方法。
【請求項２２】
初期登録リクエストを前記サービスプロバイダに送信し、
前記初期登録リクエストの送信に応答して、前記認証サーバの署名が行なわれた初期識別コード及び前記サービスプロバイダの署名が付された初期識別コードを含む第１の初期登録データを含む第１の初期登録データを前記サービスプロバイダから受信し、
前記受信した前記第１の初期登録データの前記認証サーバ及び前記サービスプロバイダの署名が確認された場合に、前記第２のユーザ端末が読み込み可能なＱＲコードを表示し、前記ＱＲコードは、前記第１のユーザ端末の署名がされた前記初期識別コード、前記第１のユーザ端末の公開鍵を含み、
前記ＱＲコードを表示した後、前記サービスプロバイダから前記認証サーバの署名がされた前記第１のユーザ端末の公開鍵及び前記サービスプロバイダの署名がされた前記第１のユーザ端末の公開鍵を前記ログインリクエストの後の画面情報とともに受信し、
前記ログインリクエストの後の画面情報とともに受信した前記認証サーバの署名がされた前記第１のユーザ端末の公開鍵及び前記サービスプロバイダの署名がされた前記第１のユーザ端末の公開鍵の前記認証サーバ及び前記サービスプロバイダの署名が確認された場合に、前記ログインリクエストの後の初期登録完了画面情報を表示する、
請求項２１記載のログイン認証方法。
【請求項２３】
第１のユーザ端末からのログインリクエストを受信する手段と、
前記受信したログインリクエストに基づいて、前記第１のユーザ端末の公開鍵及び第２のユーザ端末の公開鍵を使用して、前記第１のユーザ端末のログイン認証を行なう手段と、
前記ログイン認証が成功した場合に、ログインが成功したことを示す画面情報を前記第１のユーザ端末に送信する送信手段と
を具備するログイン認証システム。
【請求項２４】
前記ログイン認証を行なう手段は、認証サーバ群における複数の認証サーバであり、
前記複数の認証サーバにおける認証用のデータは、ブロックチェーン技術により同一性が保たれている、請求項２３記載のログイン認証システム。
【請求項２５】
サービスプロバイダと、認証サーバとを有するログイン認証システムにおけるログイン認証方法において、
前記サービスプロバイダが、
第１のユーザ端末からログインリクエストを受信し、
前記受信したログインリクエストに応答して、前記第１のユーザ端末に識別コードを送信し、
前記第１のユーザ端末の署名がされた前記識別コードを受信し、
前記受信した前記第１のユーザ端末の署名がされた前記識別コードの前記第１のユーザ端末の署名が確認された場合、前記認証サーバに、前記識別コードと前記第１のユーザ端末の公開鍵とに前記サービスプロバイダの署名がされた第１データを含む承認リクエストを前記認証サーバに送信し、
前記認証サーバが、
前記承認リクエストを受信し、前記承認リクエストに含まれる第１データに含まれる前記サービスプロバイダの署名が確認された場合に、前記第１データ及び前記識別コードに

前記認証サーバの署名を行ない、前記認証サーバの署名がされた前記第１データ及び前記識別コードを第２のユーザ端末に送信し、
前記認証サーバの署名がされた前記第１データ及び前記識別コードの送信に応答して、前記第２のユーザ端末から、前記第２のユーザ端末の署名がされた前記識別コード、前記第２のユーザ端末の公開鍵及び前記第２のユーザ端末の端末情報を含む第２データを受信し、
前記受信した第２データに含まれる前記第２のユーザ端末の署名及び前記端末情報が確認された場合に、前記認証サーバの署名がされた前記承認リクエストに対する結果を示す承認結果情報及び前記認証サーバの署名がされた前記第２のユーザ端末の署名が付された前記識別コードを含む第３データを前記サービスプロバイダに送信し、
前記サービスプロバイダが、
前記認証サーバから前記第３データを受信し、
前記受信した前記第３データの前記認証サーバ及び前記第２のユーザ端末の署名が確認された場合、前記認証サーバの署名がされた前記第１のユーザ端末の公開鍵及び前記サービスプロバイダの署名がされた前記第１のユーザ端末の公開鍵を前記ログインリクエストの後の画面情報とともに前記第１のユーザ端末に送信する、
ログイン認証方法。
【請求項２６】
第１のユーザ端末からログインリクエストを受信し、
前記受信したログインリクエストに応答して、前記第１のユーザ端末に識別コードを送信し、
前記第１のユーザ端末の署名がされた前記識別コードを受信し、
前記受信した前記第１のユーザ端末の署名がされた前記識別コードの前記第１のユーザ端末の署名が確認された場合に、前記認証サーバに、前記識別コードと前記第１のユーザ端末の公開鍵とに前記サービスプロバイダの署名がされた第１データを含む承認リクエストを前記認証サーバに送信し、
前記第１データの送信に応答して、前記認証サーバから前記認証サーバの署名がされた前記承認リクエストに対する結果を示す承認結果情報、前記認証サーバの署名がされた前記第２のユーザ端末の署名が付された前記識別コード及び前記第１のユーザ端末の公開鍵を含む第２データを受信し、
前記受信した前記第２データの前記認証サーバ及び前記第２のユーザ端末の署名が確認された場合、前記認証サーバの署名がされた前記第１のユーザ端末の公開鍵及び前記サービスプロバイダの署名がされた前記第１のユーザ端末の公開鍵を前記ログインリクエストの後の画面情報とともに前記第１のユーザ端末に送信する、
ログイン認証システムにおけるサービスプロバイダのログイン認証方法。
【請求項２７】
サービスプロバイダから承認リクエストを受信し、前記承認リクエストに含まれる第１データに含まれる前記サービスプロバイダの署名が確認された場合に、前記第１データ及び識別コードに前記認証サーバの署名を行ない、前記認証サーバの署名がされた前記第１データ及び前記識別コードを第２のユーザ端末に送信し、
前記認証サーバの署名がされた前記第１データ及び前記識別コードに応答して、前記第２のユーザ端末から、前記第２のユーザ端末の署名がされた前記識別コード、前記第２のユーザ端末の公開鍵及び前記第２のユーザ端末の端末情報を含む第２データを受信し、
前記受信した第２データに含まれる前記第２のユーザ端末の署名及び前記端末情報が確認された場合に、前記認証サーバの署名がされた前記承認リクエストに対する結果を示す承認結果情報及び前記認証サーバの署名がされた前記第２のユーザ端末の署名が付された前記識別コードを含む第３データを前記サービスプロバイダに送信する、
ログイン認証システムにおける認証サーバのログイン認証方法。
【請求項２８】
第１のユーザ端末からのログインリクエストを受信し、

前記受信したログインリクエストに基づいて、前記第１のユーザ端末の公開鍵及び第２のユーザ端末の公開鍵を使用して、前記第１のユーザ端末のログイン認証を行ない、
前記ログイン認証が成功した場合に、ログインが成功したことを示す画面情報を前記第１のユーザ端末に送信する、
ログイン認証システムにおけるログイン認証方法。
【請求項２９】
ログイン認証システムのサービスプロバイダに、
第１のユーザ端末からログインリクエストを受信させ、
前記受信したログインリクエストに応答して、前記第１のユーザ端末に識別コードを送信させ、
前記第１のユーザ端末の署名がされた前記識別コードを受信させ、
前記受信した前記第１のユーザ端末の署名がされた前記識別コードの前記第１のユーザ端末の署名が確認された場合に、前記認証サーバに、前記識別コードと前記第１のユーザ端末の公開鍵とに前記サービスプロバイダの署名がされた第１データを含む承認リクエストを前記認証サーバに送信させ、
前記第１データの送信に応答して、前記認証サーバから前記認証サーバの署名がされた前記承認リクエストに対する結果を示す承認結果情報、前記認証サーバの署名がされた前記第２のユーザ端末の署名が付された前記識別コード及び前記第１のユーザ端末の公開鍵を含む第２データを受信させ、
前記受信した前記第２データの前記認証サーバ及び前記第２のユーザ端末の署名が確認された場合、前記認証サーバの署名がされた前記第１のユーザ端末の公開鍵及び前記サービスプロバイダの署名がされた前記第１のユーザ端末の公開鍵を前記ログインリクエストの後の画面情報とともに前記第１のユーザ端末に送信させる、
ログイン認証プログラム。
【請求項３０】
ログイン認証システムの認証サーバに、
サービスプロバイダから承認リクエストを受信し、前記承認リクエストに含まれる第１データに含まれる前記サービスプロバイダの署名が確認された場合に、前記第１データ及び識別コードに前記認証サーバの署名を行ない、前記認証サーバの署名がされた前記第１データ及び前記識別コードを第２のユーザ端末に送信させ、
前記認証サーバの署名がされた前記第１データ及び前記識別コードに応答して、前記第２のユーザ端末から、前記第２のユーザ端末の署名がされた前記識別コード、前記第２のユーザ端末の公開鍵及び前記第２のユーザ端末の端末情報を含む第２データを受信させ、
前記受信した第２データに含まれる前記第２のユーザ端末の署名及び前記端末情報が確認された場合に、前記認証サーバの署名がされた前記承認リクエストに対する結果を示す承認結果情報及び前記認証サーバの署名がされた前記第２のユーザ端末の署名が付された前記識別コードを含む第３データを前記サービスプロバイダに送信させる、
ログイン認証プログラム。
【請求項３１】
第１のユーザ端末と、第２のユーザ端末とを具備し、前記第２のユーザ端末を使用して、前記第１のユーザ端末にログインを行なうログイン認証システムにおける前記第２のユーザ端末に、
認証サーバの署名がされた第１データ及び識別コードを受信させ、前記第１データは、前記識別コードと前記第１のユーザ端末の公開鍵とにサービスプロバイダの署名がされたデータであり、
前記受信した前記認証サーバの署名がされた前記第１データ及び前記識別コードの前記認証サーバ及び前記サービスプロバイダの署名が確認された場合に、前記第２のユーザ端末の署名がされた前記識別コード、前記第２のユーザ端末の公開鍵及び前記第２のユーザ端末の端末情報を含む第１データを前記認証サーバに送信させ、
これにより、前記第１のユーザ端末のログインを行なうログイン認証プログラム。

【請求項３２】
第１のユーザ端末と、第２のユーザ端末とを具備し、前記第２のユーザ端末を使用して、前記第１のユーザ端末にログインを行なうログイン認証システムにおける前記第１のユーザ端末に、
ログインリクエストをサービスプロバイダに送信させ、
前記送信したログインリクエストに応答して、前記サービスプロバイダから識別コードを受信させ、
前記受信した識別コードに前記第１のユーザ端末の署名を行ない、前記第１のユーザ端末の署名がされた前記識別コードを前記サービスプロバイダに送信させ、
前記第１のユーザ端末の署名がされた前記識別コードを前記サービスプロバイダに送信した後に、前記サービスプロバイダから認証サーバの署名がされた前記第１のユーザ端末の公開鍵及び前記サービスプロバイダの署名がされた前記第１のユーザ端末の公開鍵を前記ログインリクエストの後の画面情報とともに受信させる、
ログイン認証プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ログイン認証システム、ログイン認証システムにおけるサービスプロバイダ及び認証サーバ、ログイン認証システムにおけるサービスプロバイダ、認証サーバ、コンピュータ及び携帯端末のためのログイン認証方法及びプログラムに関する。
【背景技術】
【０００２】
従来より、機密性の高いサービスのサイトにログインを行なう場合には、ユーザがＩＤ及びパスワード（ＰＷ）を入力してログインを行なうシステムが広く知られている。また、ユーザがＩＤ及びＰＷを盗み取られた場合には、第３者が当該ユーザになりすますことにより機密性の高いサービスのサイトにログインが可能となってしまう。
【０００３】
このような問題に対処するために、生体認証情報を使用してログインを行なう技術も良く知られている（例えば、特許文献１参照）。
【先行技術文献】
【特許文献】
【０００４】
【特許文献１】特開２０１３－１７４９５５号公報
【発明の概要】
【発明が解決しようとする課題】
【０００５】
しかしながら、生体認証情報を使用する方法は、生体認証情報を読み取るための特別な装置が必要である。そのため、そのような特別な装置を有しないユーザにとっては、このような生体認証情報を使用するログイン認証方法は不便である。
【０００６】
本発明は、上記実情に鑑みてなされたものであり、第１の端末及び第２の端末が公開鍵暗号方式を使用して、サービスプロバイダが認証サーバとともに提供するサービスへのログイン認証を行なうことにより、ユーザがＩＤ及びＰＷの入力を必要とすることなく、安全に機密性の高いサービスにログインすることができるログイン認証システム、ログイン認証システムにおけるサービスプロバイダ及び認証サーバ、ログイン認証システムにおけるサービスプロバイダ、認証サーバ、コンピュータ及び携帯端末のためのログイン認証方法及びプログラ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】
【０００７】
第１の発明によれば、サービスプロバイダと、認証サーバとを有するログイン認証シス

テムにおいて、前記サービスプロバイダは、第１のユーザ端末からログインリクエストを受信するログインリクエスト受信手段と、前記受信したログインリクエストに応答して、前記第１のユーザ端末に識別コードを送信する識別コード送信手段と、前記第１のユーザ端末の署名がされた前記識別コードを受信する第１コード受信手段と、前記受信した前記第１のユーザ端末の署名がされた前記識別コードの前記第１のユーザ端末の署名が確認された場合、前記認証サーバに、前記識別コードと前記第１のユーザ端末の公開鍵とに前記サービスプロバイダの署名がされた第１データを含む承認リクエストを前記認証サーバに送信する承認リクエスト送信手段とを具備し、前記認証サーバは、前記承認リクエストを受信し、前記承認リクエストに含まれる第１データに含まれる前記サービスプロバイダの署名が確認された場合に、前記第１データ及び前記識別コードに前記認証サーバの署名を行ない、前記認証サーバの署名がされた前記第１データ及び前記識別コードを第２のユーザ端末に送信する第１データ送信手段と、前記認証サーバの署名がされた前記第１データ及び前記識別コードの送信に応答して、前記第２のユーザ0端末から、前記第２のユーザ端末の署名がされた前記識別コード、前記第２のユーザ端末の公開鍵及び前記第２のユーザ端末の端末情報を含む第２データを受信する第２データ受信手段と、前記受信した第２データに含まれる前記第２のユーザ端末の署名及び前記端末情報が確認された場合に、前記認証サーバの署名がされた前記承認リクエストに対する結果を示す承認結果情報及び前記認証サーバの署名がされた前記第２のユーザ端末の署名が付された前記識別コードを含む第３データを前記サービスプロバイダに送信する第３データ送信手段とを具備し、前記サービスプロバイダは、前記認証サーバから前記第３データを受信する第３データ受信手段と、前記受信した前記第３データの前記認証サーバ及び前記第２のユーザ端末の署名が確認された場合、前記認証サーバの署名がされた前記第１のユーザ端末の公開鍵及び前記サービスプロバイダの署名がされた前記第１のユーザ端末の公開鍵を前記ログインリクエストの後の画面情報とともに前記第１のユーザ端末に送信する画面情報送信手段とを具備するログイン認証システム、である。

【０００８】

第２の発明によれば、第１の発明において、前記第１のユーザ端末から初期登録リクエストを受信する初期登録受信手段と、前記初期登録リクエストを受信した場合に、前記第１のユーザ端末の公開鍵、前記第２のユーザ端末の公開鍵、前記サービスプロバイダの公開鍵、前記認証サーバの公開鍵及び前記ユーザの識別情報を互いに関連付ける処理を行なう関連付け処理手段をさらに具備するログイン認証システム、である。

【０００９】

第３の発明によれば、第２の発明において、前記関連付け処理手段は、前記サービスプロバイダが、前記第１のユーザ端末から初期登録リクエストを受信した場合、前記認証サーバの署名が行なわれた初期識別コード及び前記サービスプロバイダの署名が付された初期識別コードを含む第１の初期登録データを前記第１のユーザ端末に送信する第１の初期登録データ送信手段を具備し、前記認証サーバが、前記第１の初期登録データの送信に応答して、前記第２のユーザ端末から第２のユーザ端末の署名が行なわれた前記第１のユーザ端末の署名が付された前記初期識別コード、暗号化されたユーザの識別情報、前記第１のユーザ端末の公開鍵、前記第２のユーザ端末の公開鍵及び前記第２のユーザ端末の端末情報を含む第２の初期登録データを受信する第１の初期登録データ受信手段と、前記第２の初期登録データに含まれる前記第２のユーザ端末の署名が行なわれた前記第１のユーザ端末の署名が付された前記初期識別コードの前記第１のユーザ端末及び前記第２のユーザ端末の署名が確認され、かつ前記初期識別コードが確認された場合に、前記認証サーバの署名がされた前記第２のユーザ端末及び前記第１のユーザ端末の署名が付された前記初期識別コード、前記暗号化された前記ユーザの識別情報、前記第１のユーザ端末の公開鍵及び前記第２のユーザ端末の公開鍵を含む第３の初期登録データを前記サービスプロバイダに送信する第２の初期登録データ送信手段とを具備し、前記サービスプロバイダが、前記第３の初期登録データを前記認証サーバから受信する第２の初期登録データ受信手段と、前記受信した第３の初期登録データに含まれる前記第１のユーザ端末、前記第２のユーザ

端末及び認証サーバの署名及び前記ユーザの識別情報が確認された場合、前記初期登録リクエストの後の初期登録完了画面情報とともに前記第１のユーザ端末に送信する初期登録完了画面情報送信手段とをさらに具備する、ログイン認証システム、である。

【００１０】

第４の発明によれば、第１のユーザ端末からログインリクエストを受信するログインリクエスト受信手段と、前記受信したログインリクエストに応答して、前記第１のユーザ端末に識別コードを送信する識別コード送信手段と、前記第１のユーザ端末の署名がされた前記識別コードを受信する第１コード受信手段と、前記受信した前記第１のユーザ端末の署名がされた前記識別コードの前記第１のユーザ端末の署名が確認された場合に、前記識別コードと前記第１のユーザ端末の公開鍵とに前記サービスプロバイダの署名がされた第１データを含む承認リクエストを前記認証サーバに送信する承認リクエスト送信手段と、前記第１データの送信に応答して、前記認証サーバから前記認証サーバの署名がされた前記承認リクエストに対する結果を示す承認結果情報、前記認証サーバの署名がされた前記第２のユーザ端末の署名が付された前記識別コード及び前記第１のユーザ端末の公開鍵を含む第２データを受信する第２データ受信手段と、前記受信した前記第２データの前記認証サーバ及び前記第２のユーザ端末の署名が確認された場合、前記認証サーバの署名がされた前記第１のユーザ端末の公開鍵及び前記サービスプロバイダの署名がされた前記第１のユーザ端末の公開鍵を前記ログインリクエストの後の画面情報とともに前記第１のユーザ端末に送信する画面情報送信手段とを具備するログイン認証システムにおけるサービスプロバイダ、である。

【００１１】

第５の発明によれば、サービスプロバイダから承認リクエストを受信し、前記承認リクエストに含まれる第１データに含まれる前記サービスプロバイダの署名が確認された場合に、前記第１データ及び識別コードに前記認証サーバの署名を行ない、前記認証サーバの署名がされた前記第１データ及び前記識別コードを第２のユーザ端末に送信する第１データ送信手段と、前記認証サーバの署名がされた前記第１データ及び前記識別コードに応答して、前記第２のユーザ端末から、前記第２のユーザ端末の署名がされた前記識別コード、前記第２のユーザ端末の公開鍵及び前記第２のユーザ端末の端末情報を含む第２データを受信する第２データ受信手段と、前記受信した第２データに含まれる前記第２のユーザ端末の署名及び前記端末情報が確認された場合に、前記認証サーバの署名がされた前記承認リクエストに対する結果を示す承認結果情報及び前記認証サーバの署名がされた前記第２のユーザ端末の署名が付された前記識別コードを含む第３データを前記サービスプロバイダに送信する第３データ送信手段とを具備する認証サーバ、である。

【００１２】

第６の発明によれば、第１のユーザ端末と、第２のユーザ端末とを具備し、前記第２のユーザ端末を使用して、前記第１のユーザ端末にログインを行なうログイン認証システムにおけるログイン処理の前記第２のユーザ端末におけるログイン認証方法において、認証サーバの署名がされた第１データ及び識別コードを受信し、前記第１データは、前記識別コードと前記第１のユーザ端末の公開鍵とにサービスプロバイダの署名がされたデータであり、前記受信した前記認証サーバの署名がされた前記第１データ及び前記識別コードの前記認証サーバ及び前記サービスプロバイダの署名が確認された場合に、前記第２のユーザ端末の署名がされた前記識別コード、前記第２のユーザ端末の公開鍵及び前記第２のユーザ端末の端末情報を含む第１データを前記認証サーバに送信し、これにより、前記第１のユーザ端末のログインを行なうログイン認証方法、である。

【００１３】

第７の発明によれば、第１のユーザ端末と、第２のユーザ端末とを具備し、前記第２のユーザ端末を使用して、前記第１のユーザ端末にログインを行なうログイン認証システムにおけるログイン処理の前記第１のユーザ端末におけるログイン認証方法において、ログインリクエストをサービスプロバイダに送信し、前記送信したログインリクエストに応答して、前記サービスプロバイダから識別コードを受信し、前記受信した識別コードに前記

第１のユーザ端末の署名を行ない、前記第１のユーザ端末の署名がされた前記識別コードを前記サービスプロバイダに送信し、前記第１のユーザ端末の署名がされた前記識別コードを前記サービスプロバイダに送信した後に、前記サービスプロバイダから前記認証サーバの署名がされた前記第１のユーザ端末の公開鍵及び前記サービスプロバイダの署名がされた前記第１のユーザ端末の公開鍵を前記ログインリクエストの後の画面情報とともに受信する、ログイン認証方法、である。

【００１４】

第８の発明によれば、第１のユーザ端末からのログインリクエストを受信する手段と、前記受信したログインリクエストに基づいて、前記第１のユーザ端末の公開鍵及び第２のユーザ端末の公開鍵を使用して、前記第１のユーザ端末のログイン認証を行なう手段と、前記ログイン認証が成功した場合に、ログインが成功したことを示す画面情報を前記第１のユーザ端末に送信する送信手段とを具備するログイン認証システム、である。

【発明の効果】

【００１５】

本発明によれば、第１の端末及び第２の端末が公開鍵暗号方式を使用して、サービスプロバイダが認証サーバとともに提供するサービスへのログイン認証を行なうことにより、ユーザがＩＤ及びＰＷの入力を必要とすることなく、安全に機密性の高いサービスにログインすることができるログイン認証システムを提供することができる。

【図面の簡単な説明】

【００１６】

【図１】実施形態のログイン認証を行なうためのログイン認証システムを説明するための図である。

【図２】コンピュータＣ１の構成を示す図である。

【図３】ログイン認証処理の初期登録処理前に各装置が保有している情報を示す図である。

【図４】ログイン認証処理の初期登録処理後に各装置が保有している情報を示す図である。

【図５】顧客情報の一例を示す図である。

【図６】ログイン認証システムの初期登録処理のタイミングチャートを示す図である。

【図７】ログイン認証システムのログイン認証処理のタイミングチャートを示す図である。

【図８】サービスプロバイダＳＰの初期登録処理を説明するためのフローチャートである。

【図９】認証サーバＡの初期登録処理を説明するためのフローチャートである。

【図１０】コンピュータＣ１の初期登録処理を説明するためのフローチャートである。

【図１１】ユーザ端末Ｃ２の初期登録処理を説明するためのフローチャートである。

【図１２】コンピュータＣ１のディスプレイ上に表示されるＱＲコード（登録商標）Ｃを示す図である。

【図１３】サービスプロバイダＳＰのログイン処理を説明するためのフローチャートである。

【図１４】認証サーバＡのログイン処理を説明するためのフローチャートである。

【図１５】コンピュータＣ１のログイン処理を説明するためのフローチャートである。

【図１６】ユーザ端末Ｃ２のログイン処理を説明するためのフローチャートである。

【図１７】セキュリティの観点から従来のログイン方式と実施形態のログイン方式とを説明するための図である。

【発明を実施するための形態】

【００１７】

以下、図面を参照して、本発明の実施形態に係るログイン認証システムについて説明する。なお、実施形態では、証券会社などの金融機関が提供する機密性の高いサービスにログインするためのログイン認証システムについて説明するが、ログインが必要なサービス

であれば、実施形態のログイン認証方法を適用することができる。

１　ログイン認証システムの構成

図１は、実施形態のログイン認証を行なうためのログイン認証システムを説明するための図である。

【００１８】

同図に示すように、インターネットなどのネットワーク１には、ユーザのコンピュータＣ１、ユーザの携帯端末Ｃ２、サービスプロバイダＳＰ、認証サーバ群ＡＣの認証サーバＡ－１～Ａ－４が接続されている。なお、認証サーバＡ－１～Ａ－４を区別する必要がない場合には、「認証サーバＡ」と省略して表記する。

【００１９】

コンピュータＣ１は、一般的なデスクトップコンピュータの他、モバイルコンピュータ、ラップトップコンピュータ、タブレット型端末などを含む。コンピュータＣ１上では、例えば、サービスプロバイダＳＰからダウンロードされ、ウェブブラウザ上で動作するＪａｖａＳｃｒｉｐｔ（登録商標）で記述されたコンピュータＣ１用のログイン認証プログラムによって、実施形態のログイン認証方法が実行される。

【００２０】

携帯端末Ｃ２は、スマートフォン、フィーチャー・フォン（ｆｅａｔｕｒｅ ｐｈｏｎｅ)などを含み、例えば、Ａｎｄｒｏｉｄ（登録商標）、ｉＯＳ（登録商標）などのＯＳ上で動作する携帯端末である。携帯端末Ｃ２上では、例えば、図示せぬアプリケーションプログラムダウンロードサーバからダウンロードされた携帯端末Ｃ２用のログイン認証プログラムによって、実施形態のログイン認証方法が実行される。

【００２１】

サービスプロバイダＳＰは、株式取引画面などのログイン認証が必要なサービス提供画面の提供などを行なうサービス提供プログラムの他、実施形態のログイン処理を行なうためのサービスプロバイダ用のログイン認証プログラムを有する。

【００２２】

認証サーバ群ＡＣは、認証サーバＡ－１～Ａ－４を有する。各認証サーバＡ－１～Ａ－４は相互に接続されるとともに、インターネット１にも接続されている。各認証サーバＡ－１～Ａ－４は、ユーザのコンピュータＣ１、携帯端末Ｃ２及びサービスプロバイダＳＰの公開鍵及び携帯端末Ｃ２の端末情報などを格納する記憶装置を有する。各認証サーバＡ－１～Ａ－４の記憶装置のデータは、ブロックチェーン技術により、データの同一性が保たれている。実施形態では、コンピュータＣ１、携帯端末Ｃ２及びサービスプロバイダＳＰと協働して、認証サーバＡがログイン認証処理を行なう。なお、認証サーバ群ＡＣに含まれる認証サーバの数は、４つに限られるものではない。

【００２３】

ユーザのコンピュータＣ１、携帯端末Ｃ２、サービスプロバイダＳＰ及び認証サーバ群ＡＣの認証サーバＡ－１～Ａ－４は、一般的な情報処理装置と同様の構成を有する。情報処理装置は、メモリ、ＣＰＵ、通信インターフェイス、記憶装置などを備え、実施形態に係るログイン認証処理は、ＣＰＵが各装置の記憶装置に記憶されたプログラムを実行することにより実現される。

【００２４】

すなわち、コンピュータＣ１の記憶装置には、コンピュータＣ１用のログイン認証プログラムが記憶され、携帯端末Ｃ２の記憶装置には、携帯端末Ｃ２用のログイン認証プログラムが記憶され、サービスプロバイダＳＰの記憶装置には、サービスプロバイダＳＰ用のログイン認証プログラムが記憶され、サービスプロバイダＳＰなどとともにログイン認証処理を行なう認証サーバＡには、認証サーバＡ用のログイン認証プログラムが記憶される。

【００２５】

例として、図２にコンピュータＣ１の構成を示す。

【００２６】

同図に示すように、コンピュータＣ１においては、バス１１にＣＰＵ１２、通信部１３、メモリ１４、入力部１５、記憶装置１６及び表示部１７が接続されている。

【００２７】

ＣＰＵ１２は、記憶装置１６に記憶された本発明の実施の形態に係るログイン認証プログラム２４と協働して、本実施形態に係るログイン認証処理を行なう他、コンピュータＣ１全体の制御を司るものである。

【００２８】

通信部１３は、ネットワーク１を介した認証サーバＡ、サービスプロバイダＳＰなどの外部装置との通信の制御を司る。

【００２９】

メモリ１４は、ログイン認証プログラム２４を実行する際に必要とされるワークエリアなどとして使用される。

【００３０】

入力部１５は、ログイン認証処理を行なう際に必要とされるデータなどを入力するためのインターフェイスであり、例えば、キーボード、マウス、タッチパネルなどである。

【００３１】

記憶装置１６は、ログイン認証処理に必要とされるプログラム、データを格納するためのものであり、例えば、ハードディスクドライブ（ＨＤＤ）、光ディスクドライブ、ＤＶＤ、ＭＯなどの大容量記憶装置である。この記憶装置１６には、ＯＳ（オペレーティングシステム）２１、鍵情報データベース２２、データベース２３及びログイン認証プログラム２４が格納されている。

表示部１７は、本実施形態に係るログイン認証プログラムによる処理のために必要な情報を表示するためのディスプレイであり、例えば、図１２に示すように、ログイン認証の際に必要となる初期登録用のＱＲコードを表示する。

【００３２】

ＯＳ２１は、コンピュータＣ１の基本的な機能を実現するためのプログラムである。

【００３３】

鍵情報データベース２２は、ログイン認証プログラム２４の初期登録処理によって発行されるコンピュータＣ１のキーペア（秘密鍵、公開鍵）を格納する。

【００３４】

データベース２３は、実施形態のログイン認証処理に関するデータや、ユーザ関連情報などを格納する。

【００３５】

ログイン認証プログラム２４は、ＯＳ２１上で動作するアプリケーションプログラムであって、ＣＰＵ１２と協働して、実施形態に係るログイン認証処理を実現するものであって、図６、図７及び図１０に示すコンピュータＣ１のフローチャートの処理を実現するものである。

【００３６】

なお、携帯端末Ｃ２の記憶装置に格納されるログイン認証プログラムは図６、図７及び図１１に示す携帯端末Ｃ２のフローチャートの処理、サービスプロバイダＳＰの記憶装置に格納されるログイン認証プログラムは図６、図７及び図８に示すサービスプロバイダＳＰのフローチャートの処理、認証サーバＡの記憶装置に格納されるログイン認証プログラムは図６、図７及び図９に示すサービスプロバイダＳＰのフローチャートの処理を実現する。

【００３７】

図３は、ログイン認証処理の初期登録処理前に各装置が保有している情報を示す図である。なお、図３及び図４においては、各装置が保有する秘密鍵については示していない。

【００３８】

同図に示すように、初期登録処理前には、コンピュータＣ１及び携帯端末Ｃ２は認証サーバＡの公開鍵及びサービスプロバイダＳＰの公開鍵を保有し、認証サーバＡはサービス

プロバイダＳＰの公開鍵を保有し、サービスプロバイダＳＰは認証サーバＡの公開鍵を保有している。

【００３９】

図４は、ログイン認証処理の初期登録処理後に各装置が保有している情報を示す図である。

【００４０】

同図に示すように、初期登録処理後には、コンピュータＣ１及び携帯端末Ｃ２は認証サーバＡの公開鍵及びサービスプロバイダＳＰの公開鍵を保有し、認証サーバＡはサービスプロバイダＳＰの公開鍵、コンピュータＣ１の公開鍵、携帯端末Ｃ２の公開鍵及び携帯端末Ｃ２の端末情報を保有し、サービスプロバイダＳＰは認証サーバＡの公開鍵、コンピュータＣ１の公開鍵、携帯端末Ｃ２の公開鍵及び顧客情報を保有している。

【００４１】

ここで、コンピュータＣ１のキーペア（秘密鍵及び公開鍵）は初期登録処理中にブラウザにより発行され、携帯端末Ｃ２のキーペアは、携帯端末Ｃ２にダウンロードされたログイン認証用のプログラムによって発行されているものとする。

【００４２】

顧客情報は、顧客ＤＢ（データベース）に保存されており、サービスプロバイダが提供するサービスに依存するが、例えば、顧客情報には、図５に示すように、顧客ごとにユーザＩＤ、ＰＷなどの情報が格納されている。

２　ログイン認証システムの動作

次に、実施形態に係るログイン認証システムの初期登録処理について、図６及び図７のタイミングチャート及び図８乃至図１１のフローチャートを参照して説明する。

２－１　ログイン認証処理の初期登録処理

実施形態のログイン認証方法を行なう場合、初期登録を行なう必要がある。コンピュータＣ１は、サービスプロバイダＳＰが提供するサービスにＩＤ及びＰＷを使用してログインを行ない、初期登録処理を行なう。

【００４３】

図６は、ログイン認証システムの初期登録処理のタイミングチャートを示す図である。図８はサービスプロバイダＳＰの初期登録処理を説明するためのフローチャート、図９は認証サーバＡの初期登録処理を説明するためのフローチャート、図１０はコンピュータＣ１の初期登録処理を説明するためのフローチャート及び図１１はユーザ端末Ｃ２の初期登録処理を説明するためのフローチャートである。

【００４４】

初期登録を行なう場合、コンピュータＣ１は、初期登録リクエストをサービスプロバイダＳＰに送信する（図６のＴ１、図１０のＳ４１）。サービスプロバイダＳＰは、コンピュータＣ１から初期登録リクエストを受信したかを判断し（図８のＳ１）、初期登録リクエストを受信した場合、初期登録用のワンタイムコード（ＯＴＣ）を生成し、生成したＯＴＣにサービスプロバイダＳＰの署名を行なう（図８のＳ２）。ＯＴＣは、例えば、ランダムに決定された数字である。次に、サービスプロバイダＳＰは、サービスプロバイダＳＰの署名がされたＯＴＣ（「ＳＰの署名（ＯＴＣ）」）を認証サーバＡに送信する（図６のＴ２、図８のＳ３）。図６のＴ１、Ｔ２により、認証サーバＡ及びサービスプロバイダＳＰでＯＴＣが共有される。

【００４５】

認証サーバＡは、サービスプロバイダＳＰの署名がされた初期登録用のＯＴＣを受信したかを判断し（図９のＳ２１）、サービスプロバイダＳＰの署名がされた初期登録用のＯＴＣを受信した場合、サービスプロバイダＳＰの署名を確認する（図９のＳ２２）。

【００４６】

認証サーバＡは、サービスプロバイダＳＰの署名が確認された場合、第１の初期登録データをサービスプロバイダＳＰに送信する（図６のＴ３、図９のＳ２３）。ここで、第１の初期登録データは、認証サーバＡの署名がされたＯＴＣ及びＳＰの書名（ＯＴＣ）（「

Ａの署名（（ＯＴＣ）＋ＳＰの署名（ＯＴＣ））」）である。
【００４７】
一方、認証サーバＡにおいて、サービスプロバイダＳＰの署名が確認されない場合、初期登録失敗処理が行なわれる（図９のＳ２４）。
【００４８】
サービスプロバイダＳＰは、認証サーバＡから第１の初期登録データを受信したか否かを判断し（図８のＳ４）、第１の初期登録データを受信した場合、認証サーバＡの署名の確認及びＯＴＣの確認を行なう（図８のＳ５）。
【００４９】
Ｓ５において、認証サーバＡの署名及びＯＴＣが確認された場合、第１の初期登録データをコンピュータＣ１に送信する（図６のＴ４、図８のＳ６）。サービスプロバイダＳＰにおいて、認証サーバＡの署名及びＯＴＣが確認されない場合、初期登録失敗処理が行なわれる（図８のＳ１１）。
【００５０】
コンピュータＣ１は、サービスプロバイダＳＰから第１の初期登録データを受信したか否かを判断し（図１０のＳ４２）、第１の初期登録データを受信した場合、認証サーバＡの署名及びサービスプロバイダＳＰの署名の確認を行なう（図１０のＳ４３）。認証サーバＡの署名及びサービスプロバイダＳＰの署名が確認された場合、コンピュータＣ１のブラウザ内で、新しいキーペア（コンピュータＣ１の秘密鍵及び公開鍵）を発行する（図１０のＳ４４）。コンピュータＣ１において、認証サーバＡの署名及びＯＴＣが確認されない場合、初期登録失敗処理が行なわれる（図１０のＳ４６）。
【００５１】
次に、コンピュータＣ１は、Ｃ１の署名がされたＯＴＣ及びコンピュータＣ１の公開鍵（「Ｃ１の署名（ＯＴＣ）＋Ｃ１の公開鍵」）を含むＱＲコードを作成し（図１０のＳ４５）、この作成されたＱＲコードをディスプレイ上に表示する（図１０のＳ４６）。図１２は、コンピュータＣ１のディスプレイ上に表示されるＱＲコードＣを示す図である。同図においては、ＱＲコードＣとともに、「初期登録用のＱＲコードを携帯端末で読み込んでください」のメッセージが表示される例を示している。
【００５２】
携帯端末Ｃ２は、コンピュータＣ１のディスプレイ上に表示されたＱＲコードを読み取り、Ｃ１の署名がされたＯＴＣ及びコンピュータＣ１の公開鍵（「Ｃ１の署名（ＯＴＣ）＋Ｃ１の公開鍵」）を取得する（図６のＴ５、図１１のＳ６１）。
【００５３】
携帯端末Ｃ２は、コンピュータＣ１の署名を確認し（図１１のＳ６２）、コンピュータＣ１の署名が確認された場合、第２の初期登録データを認証サーバＡに送信する（図６のＴ６、図１１のＳ６３）。ここで、第２の初期登録データは、下記のデータを含む。
・　携帯端末Ｃ２の署名が行なわれたコンピュータＣ１の署名が付されたＯＴＣ
・　暗号化されたユーザ情報（ＩＤ／ＰＷ）
・　コンピュータＣ１の公開鍵
・　携帯端末Ｃ２の公開鍵
・　携帯端末Ｃ２の端末情報
すなわち、
第２の初期登録データ　＝
　Ｃ２の署名（Ｃ１の署名（ＯＴＣ））＋サービスプロバイダＳＰ向けに暗号化したユーザ情報（ＩＤ／ＰＷ）＋　Ｃ１の公開鍵　＋　Ｃ２の公開鍵　＋　Ｃ２の端末情報
である。ここで、携帯端末Ｃ２の端末情報は、携帯端末Ｃの端末情報は、例えば、マックアドレスなどである。ユーザの携帯端末Ｃ２において、コンピュータＣ１の署名が確認されない場合、初期登録失敗処理が行なわれる（図１１のＳ６４）。
【００５４】
認証サーバＡは、第１の初期登録データをコンピュータＣ１に送信した後、第２の初期

登録データを受信したか否かを判断し（図９のＳ２５）、第２の初期登録データを受信した場合、第２の初期登録データのコンピュータＣ１及び携帯端末Ｃ２の署名及びＯＴＣの確認を行なう（図９のＳ２６）。認証サーバＡにおいて、コンピュータＣ１及び携帯端末Ｃ２の署名及びＯＴＣの確認がされない場合、初期登録失敗処理が行なわれる（図９のＳ２４）。

【００５５】

第２の初期登録データのコンピュータＣ１及び携帯端末Ｃ２の署名及びＯＴＣの確認がされた場合、携帯端末Ｃ２の端末情報を記憶装置に格納し（図９のＳ２７）、サービスプロバイダＳＰに第３の初期登録データを送信し（図６のＴ７、図９のＳ２８）、認証サーバＡにおける初期登録処理を終了する。

【００５６】

ここで、第３の初期登録データは、以下の情報を含む。

・　認証サーバＡの署名が行なわれ、かつ携帯端末Ｃ２の署名が行なわれたコンピュータＣ１の署名が付されたＯＴＣ
・　暗号化されたユーザ情報（ＩＤ／ＰＷ）
・　コンピュータＣ１の公開鍵
・　携帯端末Ｃ２の公開鍵
・　認証サーバＡの署名がされたコンピュータＣ１の公開鍵

すなわち、

第３の初期登録データ　＝

　Ａの署名（Ｃ２の署名（Ｃ１の署名（ＯＴＣ））　＋　ＳＰ向けに暗号化されたユーザ情報（ＩＤ／ＰＷ）　＋　Ｃ１の公開鍵　＋　Ｃ２の公開鍵　＋　Ａの署名（Ｃ１の公開鍵）

である。

【００５７】

サービスプロバイダＳＰは、第１の初期登録データをコンピュータＣ１に送信した後、認証サーバＡから第３の初期登録データを受信したか否かを判断し（図８のＳ７）、第３の初期登録データを受信した場合、認証サーバＡ、コンピュータＣ１、携帯端末Ｃ２、ＯＴＣ及びユーザ情報（ＩＤ／ＰＷ）の確認を行なう（図８のＳ８）。

【００５８】

Ｓ８において、認証サーバＡ、コンピュータＣ１及び携帯端末Ｃ２の署名、ＯＴＣ及びユーザ情報（ＩＤ／ＰＷ）の確認がされた場合、ログイン認証の初期登録の完了ページを認証サーバＡの署名がされたコンピュータＣ１の公開鍵（「Ａの署名（Ｃ１の公開鍵）」）とサービスプロバイダＳＰの署名がされたコンピュータＣ１の公開鍵（「ＳＰの署名（Ｃ１の公開鍵）」）とともにコンピュータＣ１に送信し（図６のＴ８、図８のＳ９）、サービスプロバイダＳＰにおける初期登録処理を終了する（図８のＳ１０）。サービスプロバイダＳＰにおいて、認証サーバＡ、コンピュータＣ１及び携帯端末Ｃ２の署名、ＯＴＣ及びユーザ情報（ＩＤ／ＰＷ）の確認がされない場合、初期登録失敗処理が行なわれる（図８のＳ１１）。

【００５９】

コンピュータＣ１は、Ｓ４７においてＱＲコードを表示した後、サービスプロバイダＳＰからログイン認証の初期登録の完了ページを受信したかを判断し（図１０のＳ４８）、完了ページを受信した場合、認証サーバＡ及びサービスプロバイダＳＰの署名を確認し（図１０のＳ４９）、認証サーバＡ及びサービスプロバイダＳＰの署名が確認された場合、初期登録の完了ページを表示し（図１０のＳ５０）、初期登録処理が終了する（図１０のＳ５２）。コンピュータＣ１において、認証サーバＡ及びサービスプロバイダＳＰの確認がされない場合、初期登録失敗処理が行なわれる（図１０のＳ４６）。

２－２　ログイン認証処理

次に、ログイン認証システムの初期登録が行なわれた後の通常ログイン認証処理について説明する。

【００６０】
図７は、ログイン認証システムのログイン認証処理のタイミングチャートを示す図である。図１３はサービスプロバイダＳＰのログイン処理を説明するためのフローチャート、図１４は認証サーバＡのログイン処理を説明するためのフローチャート、図１５はコンピュータＣ１のログイン処理を説明するためのフローチャート及び図１６はユーザ端末Ｃ２のログイン処理を説明するためのフローチャートである。
【００６１】
ログイン処理を行なう場合、コンピュータＣ１は、ログインリクエストをサービスプロバイダＳＰに送信する（図７のＴ２１、図１５のＳ１４１）。サービスプロバイダＳＰは、コンピュータＣ１からログインリクエストを受信したか否かを判断し（図１３のＳ１０１）、ログインリクエストを受信した場合、ログイン用のＯＴＣを生成し、生成したＯＴＣをコンピュータＣ１に送信する（図７のＴ２２、図１３のＳ１０２）。
【００６２】
コンピュータＣ１は、ログインリクエストをサービスプロバイダＳＰに送信後、サービスプロバイダＳＰからＯＴＣを受信したかを判断する（図１５のＳ１４２）。ＯＴＣを受信した場合、受信したＯＴＣにコンピュータＣ１の署名をして（「Ｃ１の署名（ＯＴＣ）」）、サービスプロバイダＳＰに送信する（図７のＴ２３、図１５のＳ１４３）。
【００６３】
サービスプロバイダＳＰはコンピュータＣ１からコンピュータＣ１の署名がされたＯＴＣを受信したか判断する（図１３のＳ１０３）。コンピュータＣ１の署名がされたＯＴＣを受信した場合、サービスプロバイダＳＰは、コンピュータＣ１の署名を確認する（図１３のＳ１０４）。サービスプロバイダＳＰにおいて、コンピュータＣ１の署名が確認されない場合、ログイン失敗処理が行なわれる（図１３のＳ１０６）。
【００６４】
サービスプロバイダＳＰは、コンピュータＣ１の署名が確認された場合、第１データを含む承認リクエストを認証サーバＡに送信する（図７のＴ２４、図１３のＳ１０５）。ここで、第１データは、下記のデータを含む。
・　サービスプロバイダＳＰの署名がされたＯＴＣ及びコンピュータＣ１の公開鍵
すなわち、
第１データ　＝
　サービスプロバイダＳＰの署名（ＯＴＣ＋コンピュータＣ１の公開鍵）
認証サーバＡは、サービスプロバイダＳＰから第１データを含む承認リクエストを受信したかを判断し（図１４のＳ１２１）、第１データを含む承認リクエストを受信した場合、サービスプロバイダＳＰの署名を確認する（図１４のＳ１２２）。
【００６５】
サービスプロバイダＳＰの署名が確認された場合、第１データ及びＯＴＣに認証サーバＡの署名をして（「Ａの署名（（ＯＴＣ）＋第１データ）」）、携帯端末Ｃ２に送信する（図６のＴ２５、図１４のＳ１２３）。
【００６６】
Ａの署名（（ＯＴＣ）＋第１データ）　＝
　　Ａの署名（（ＯＴＣ）　＋　ＳＰの署名（ＯＴＣ　＋　Ｃ１の公開鍵）
一方、認証サーバＡにおいて、サービスプロバイダＳＰの署名が確認されない場合、ログイン失敗処理が行なわれる（図１４のＳ１２９）。
【００６７】
携帯端末Ｃ２は、認証サーバＡの署名がされたＯＴＣ及び第１データを受信したかを判断し（図１６のＳ１６１）、認証サーバＡの署名がされたＯＴＣ及び第１データを受信した場合、認証サーバＡ及びサービスプロバイダＳＰの署名を確認する（図１６のＳ１６２）。
【００６８】
認証サーバＡ及びサービスプロバイダＳＰの署名が確認された場合、第２データを認証

サーバＡに送信する（図６のＴ２６、図１６のＳ１６３）。ここで、第２データは、下記のデータを含む。
・　携帯端末Ｃ２の署名がされたＯＴＣ
・　携帯端末Ｃ２の公開鍵
・　携帯端末Ｃの端末情報
すなわち、
第２データ　＝携帯端末Ｃの署名（ＯＴＣ）　＋　掲端末Ｃ２の公開鍵
＋　携帯端末Ｃ２の端末情報
である。

【００６９】
携帯端末Ｃにおいて、認証サーバＡ及びサービスプロバイダＳＰの署名が確認されない場合、ログイン処理失敗処理が行なわれる（図１６のＳ１６４）。

【００７０】
認証サーバＡは、Ｓ１２３において、認証サーバＡの署名がされた第１データ及びＯＴＣを送信した後、携帯端末Ｃ２から第２データを受信したかを判断し（図１４のＳ１２４）、第２データを受信した場合、携帯端末Ｃ２の署名及び端末情報を確認する（図１４のＳ１２５）。なお、携帯端末Ｃ２の署名の確認は、初期登録処理において記憶装置に格納された携帯端末の端末情報を使用して行なわれる。

【００７１】
Ｓ１２５において、携帯端末Ｃ２の署名及び端末情報を確認された場合、「承認リクエスト＝ＯＫ」とし、携帯端末Ｃ２の署名及び端末情報が確認されない場合、「承認リクエスト＝ＮＧ」として、第３データをサービスプロバイダＳＰに送信し（図７のＴ２８、図１４のＳ１２８）、認証サーバＡにおける処理を終了する。

【００７２】
ここで、第３データは、下記のデータを含む。
・　認証サーバＡの署名がされた承認リクエストの結果（ＯＫ／ＮＧ）
・　認証サーバＡの署名がされた携帯端末Ｃ２の署名が付されたＯＴＣ
・　認証サーバＡの署名がされた携帯端末Ｃ２の公開鍵
すなわち、
第３データ　＝
Ａの署名（承認リクエストの結果（ＯＫ／ＮＧ）　＋　Ａの署名（Ｃ２の署名（ＯＴＣ））　＋　Ａの署名（Ｃ１の公開鍵）
サービスプロバイダＳＰは、Ｓ１０５において承認リクエストを送信後、認証サーバＡから第３データを受信したかを判断し（図１３のＳ１０７）、認証サーバＡから第３データを受信した場合、認証サーバＡ、コンピュータＣ１及び携帯端末Ｃ２の署名及びＯＴＣを確認する（図１３のＳ１０８）。認証サーバＡ、コンピュータＣ１及び携帯端末Ｃ２の署名及びＯＴＣの確認がされた場合、「承認リクエスト　＝　ＯＫ」であるかを確認する（図１３のＳ１０９）。

【００７３】
Ｓ１０８及びＳ１０９において確認がされない場合、ログイン失敗処理が行なわれる（図１３のＳ１０６）。

【００７４】
Ｓ１０９において、「承認リクエスト　＝　ＯＫ」である場合、認証サーバＡの署名がされたコンピュータＣ１の公開鍵と、サービスプロバイダＳＰの署名がされたコンピュータＣ１の公開鍵をログイン完了ページとともにコンピュータＣ１に送信し（図７のＴ２８、図１３のＳ１０９）、サービスプロバイダＳＰにおけるログイン処理を完了する（図１３のＳ１１０）。

【００７５】
コンピュータＣ１は、Ｓ１４３においてコンピュータＣ１の署名がされたＯＴＣをサービスプロバイダＳＰに送信した後（図１５のＳ１４３）、サービスプロバイダＳＰからロ

グイン完了ページを受信したかを確認する（図１５のＳ１４４）。
【００７６】
ログイン完了ページを受信した場合、認証サーバＡ及びサービスプロバイダＳＰの署名を確認し（図１５のＳ１４５）、認証サーバＡ及びサービスプロバイダＳＰの署名が確認された場合、ログイン完了ページを表示して（図１５のＳ１４６）、ログイン認証処理を終了する（図１５のＳ１４７）。
【００７７】
Ｓ１４５において、認証サーバＡ及びサービスプロバイダＳＰの署名が確認がされない場合、ログインリクエスト失敗処理が行なわれる（図１５のＳ１４８）。
３　効果
従って、実施形態のログイン認証システムによれば、第１の端末（コンピュータＣ１）及び第２の端末（携帯端末Ｃ２）が公開鍵暗号方式を使用して、サービスプロバイダが認証サーバとともに提供するサービスへのログイン認証を行なうことにより、ユーザがＩＤ及びＰＷの入力を必要とすることなく、安全に機密性の高いサービスにログインすることができる。
【００７８】
実施形態のログイン認証システムによれば、ログインに必要な情報（コンピュータＣ１の秘密鍵、携帯端末Ｃ２の秘密鍵）をサービスプロバイダＳＰに記憶されたログイン認証情報（ユーザＩＤ／ＰＷ）と分離している。
【００７９】
従って、サービスプロバイダＳＰに記憶されたログイン認証情報（ユーザＩＤ／ＰＷ）がハッキングされてもログインに必要な情報（コンピュータＣ１の公開鍵、携帯端末Ｃ２の公開鍵）が漏れることがなくなる。
【００８０】
すなわち、実施形態のログイン認証システムによれば、ブロックチェーン技術を利用して、ログイン認証部分とコンテンツ提供部分を分離し、両方が同時にハッキングされない限り、ユーザのコンテンツの漏洩ができないようなセキュリティ性の高いサービスを提供することができる。
【００８１】
分離したログイン認証機能は、認証サーバ群ＡＣの認証サーバＡ－１～Ａ－４は、ブロックチェーン技術により構築される。これにより、認証サーバＡに格納される認証サーバのキーペア（公開鍵、秘密鍵）、サービスプロバイダＳＰの公開鍵、コンピュータＣ１の公開鍵、携帯端末Ｃ２の公開鍵及び端末情報の改ざんを防止することができる。
【００８２】
また、認証サーバ群ＡＣの認証サーバＡ－１～Ａ－４は、ブロックチェーン技術により構築されるため、認証サーバＡ－１～Ａ－４のうちの特定の認証サーバＡに障害が発生しても、他の認証サーバＡでサービスの冗長性を担保することができる。認証サーバＡ－１～Ａ－４の認証用のデータもブロックチェーン技術により構築されており、認証サーバＡ－１～Ａ－４の間で共有される。
【００８３】
中央管理型のログイン認証システムにおいて、セキュアであり、かつ可用性を担保するためには、システムの構築コストが増大してしまう。一方、実施形態のログイン認証システムのように、ブロックチェーン技術を使用した中央管理者不在の分散型認証システムによれば、可用性があり、低コストのログイン認証システムを提供することができる。
【００８４】
実施形態のログイン認証システムでは以下の特徴を有する。
・　３体認証
コンピュータＣ１、携帯端末Ｃ２、サービスプロバイダＳＰ及び認証サーバＡが相互に認証を行なうため、個別システムをハッキングすることにより不正行為を行なうことができない。

・　ゼロダウンタイム
　複数の会社が認証局（認証サーバＡ）になることで、特定の認証局が障害になっても認証サービスを継続することができる。
・　中央管理者不在
　認証機能及びデータを分散型台帳で管理することにより、データ改ざんのような不正行為の検知や防止が可能になる（中央認証局の内部不正も排除）。
・　相互扶助
　サービスプロバイダＳＰが認証サーバＡを兼ねることができる。通常、サービスプロバイダＳＰが認証サーバＡを兼ねると自己監査になるため、両方を兼ねることはできないが、サービスプロバイダＳＰ及び認証サーバＡが複数の場合、自己以外のサービスプロバイダＳＰのために認証サーバＡとしての機能を実行することができる。これにより、認証サービスを提供する側（認証サーバＡ）と受ける側（サービスプロバイダＳＰ）とでデータを共有することができる。

【００８５】
　図１７は、セキュリティの観点から従来のログイン方式と実施形態のログイン方式とを説明するための図である。
・　ＩＤ及びＰＷの漏れ
　従来のＩＤ及びＰＷを使用したログイン方式では、ＩＤ及びＰＷ漏れが発生した場合、ＩＤ及びＰＷを取得した人は、誰でも顧客のコンテンツのにアクセスが可能である。

【００８６】
　実施形態のログイン方式では、コンピュータＣ１及び携帯端末Ｃ２の鍵（公開鍵及び秘密鍵）を使用し、さらに顧客の秘密鍵へのアクセスは、実施形態では、生体認証でアクセスを許可するものとしているのでセキュアである。
・　サーバハッキングについて
　従来のログイン方式では、サーバに対してハッキングが発生し、顧客認証情報（ＩＤ及びＰＷ）が盗まれた場合、ＩＤ及びＰＷ漏れと同じ被害が発生する。

【００８７】
　実施形態のログイン方式では、ログイン認証に必要な顧客の秘密鍵をサーバ側で保持しないことで、サーバがハッキングされても認証情報が漏れることはない。
・　サイトのなりすまし
　従来のログイン方式では、顧客がなりすましサイトに接続し、ＩＤ及びＰＷを入力すると、ＩＤ及びＰＷが盗まれる恐れがある。

【００８８】
　実施形態のログイン方式では、署名付きの通信を行なうことにより、成りすましが不可能になる。

【００８９】
　本発明のいくつかの実施形態を説明したが、これらの実施形態は、例として提示したものであり、発明の範囲を限定することは意図していない。これら新規な実施形態は、その他の様々な形態で実施されることが可能であり、発明の要旨を逸脱しない範囲で、種々の省略、置き換え、変更を行うことができる。これら実施形態やその変形は、発明の範囲や要旨に含まれるとともに、特許請求の範囲に記載された発明とその均等の範囲に含まれる。

【００９０】
　また、実施形態に記載した手法は、計算機（コンピュータ）に実行させることができるプログラムとして、例えば磁気ディスク（フロッピー（登録商標）ディスク、ハードディスク等）、光ディスク（ＣＤ－ＲＯＭ、ＤＶＤ、ＭＯ等）、半導体メモリ（ＲＯＭ、ＲＡＭ、フラッシュメモリ等）等の記録媒体に格納し、また通信媒体により伝送して頒布することもできる。なお、媒体側に格納されるプログラムには、計算機に実行させるソフトウエア手段（実行プログラムのみならずテーブルやデータ構造も含む）を計算機内に構成させる設定プログラムをも含む。本装置を実現する計算機は、記録媒体に記録されたプログ

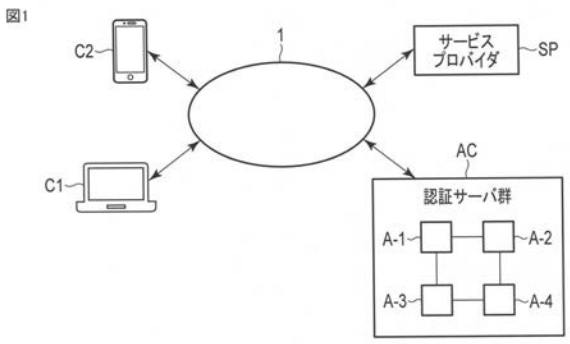
ラムを読み込み、また場合により設定プログラムによりソフトウエア手段を構築し、このソフトウエア手段によって動作が制御されることにより上述した処理を実行する。なお、本明細書でいう記録媒体は、頒布用に限らず、計算機内部あるいはネットワークを介して接続される機器に設けられた磁気ディスクや半導体メモリ等の記憶媒体を含むものである。

【符号の説明】

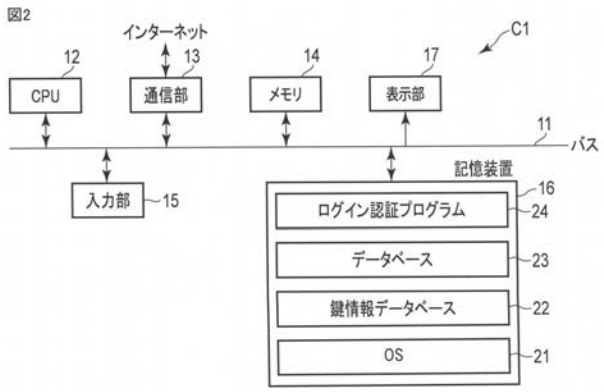
【００９１】

１…ネットワーク、Ｃ１…コンピュータ、Ｃ２…携帯端末、ＡＣ…認証サーバ群、Ａ、Ａ－１～Ａ－４…認証サーバ、ＳＰ…サービスプロバイダ。

【図１】



【図２】



【図３】

図3

コンピュータC1	携帯端末C2	認証サーバA	サービスプロバイダSP
Aの公開鍵	Aの公開鍵	SPの公開鍵	Aの公開鍵
SPの公開鍵	SPの公開鍵		

【図４】

図4

コンピュータC1	携帯端末C2	認証サーバA	サービスプロバイダSP
Aの公開鍵	Aの公開鍵	SPの公開鍵	Aの公開鍵
SPの公開鍵	SPの公開鍵	C1の公開鍵	C1の公開鍵
		C2の公開鍵	C2の公開鍵
		C2の端末情報	顧客情報

【図５】

図5

顧客DB

ユーザID － パスワード － 口座番号 － ……

【図６】

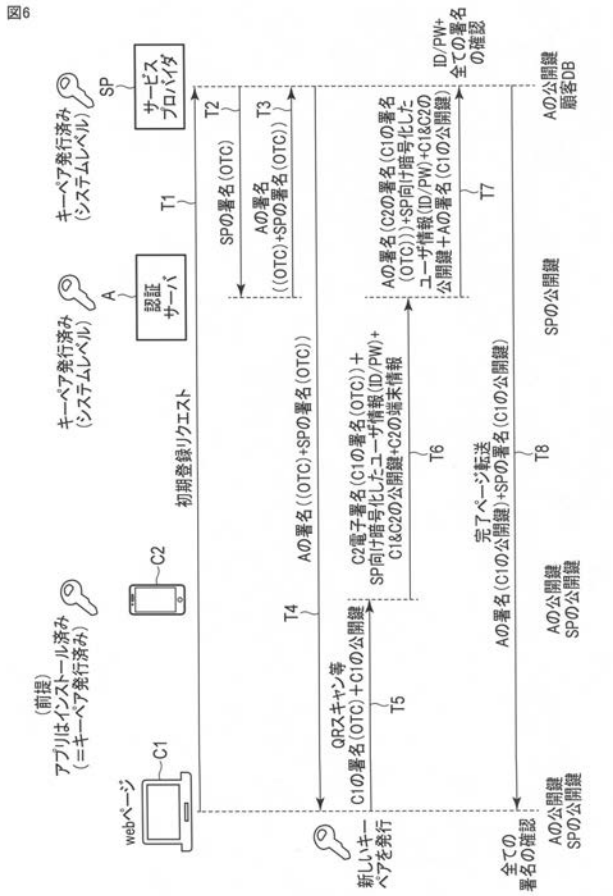


図6
サービスプロバイダ
SP
キーペア発行済み
(システムレベル)
認証サーバ
A
キーペア発行済み
(システムレベル)
C2
C1
webページ
(前提)
アプリはインストール済み
(=キーペア発行済み)
T1
T2
T3
T4
T5
T6
T7
T8
初期登録リクエスト
SPの署名(OTC)
Aの署名
((OTC)+SPの署名(OTC))
Aの署名((OTC)+SPの署名(OTC))
QRスキャン等
C1の署名(OTC)+C1の公開鍵
C2電子署名(C1の署名(OTC))+
SP向け暗号化したユーザ情報(ID/PW)+
C1&C2の公開鍵+C2の端末情報
Aの署名(C2の署名(C1の署名
(OTC)))+SP向け暗号化した
ユーザ情報(ID/PW)+C1&C2の
公開鍵+Aの署名(C1の公開鍵)
完了ページ転送
Aの署名(C1の公開鍵)+SPの署名(C1の公開鍵)
新しいキー
ペアを発行
全ての
署名の確認
ID/PW+
全ての署名
の確認
Aの公開鍵
顧客DB
SPの公開鍵
Aの公開鍵
SPの公開鍵
Aの公開鍵
SPの公開鍵

【図７】

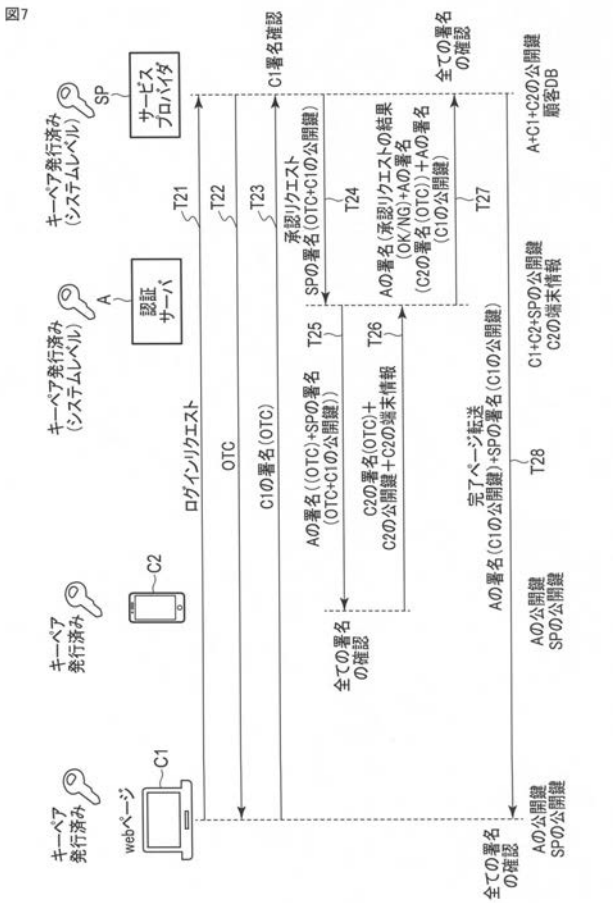


図7
サービスプロバイダ
SP
キーペア発行済み
(システムレベル)
認証サーバ
A
キーペア発行済み
(システムレベル)
C2
キーペア
発行済み
C1
webページ
キーペア
発行済み
T21
T22
T23
T24
T25
T26
T27
T28
ログインリクエスト
OTC
C1の署名(OTC)
C1署名確認
承認リクエスト
SPの署名(OTC+C1の公開鍵)
A署名((OTC)+SPの署名
(OTC+C1の公開鍵))
C2の署名(OTC)+
C2の公開鍵+C2の端末情報
Aの署名(承認リクエストの結果
(OK/NG)+Aの署名
(C2の署名(OTC))+Aの署名
(C1の公開鍵)
完了ページ転送
Aの署名(C1の公開鍵)+SPの署名(C1の公開鍵)
全ての署名
の確認
全ての署名
の確認
全ての署名
の確認
A+C1+C2の公開鍵
顧客DB
C1+C2+SPの公開鍵
C2の端末情報
Aの公開鍵
SPの公開鍵
Aの公開鍵
SPの公開鍵
Aの公開鍵
SPの公開鍵

【図８】

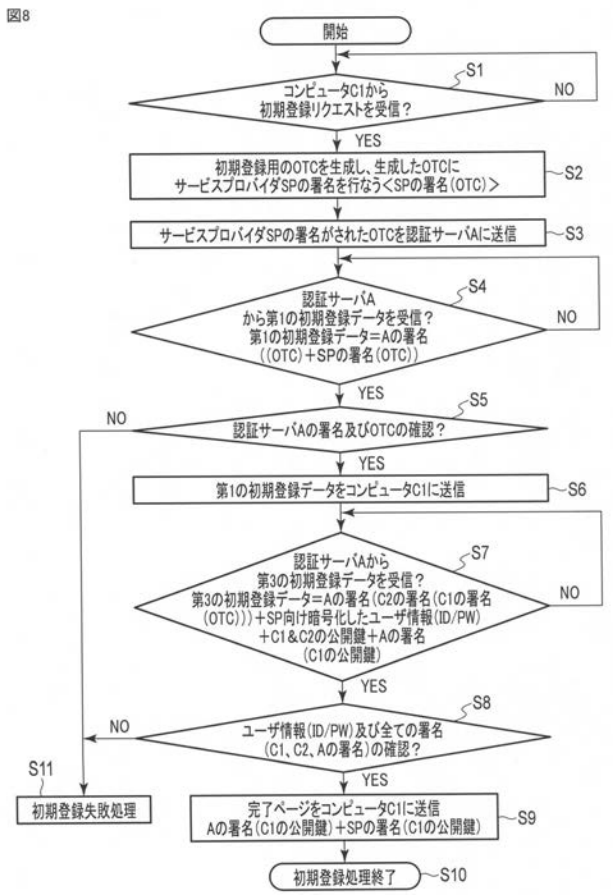


図8
開始
コンピュータC1から
初期登録リクエストを受信?
S1
NO
YES
初期登録用のOTCを生成し、生成したOTCに
サービスプロバイダSPの署名を行なう<SPの署名(OTC)>
S2
サービスプロバイダSPの署名がされたOTCを認証サーバAに送信
S3
認証サーバA
から第1の初期登録データを受信?
第1の初期登録データ=Aの署名
((OTC)+SPの署名(OTC))
S4
NO
YES
認証サーバAの署名及びOTCの確認?
S5
NO
YES
第1の初期登録データをコンピュータC1に送信
S6
認証サーバAから
第3の初期登録データを受信?
第3の初期登録データ=Aの署名(C2の署名(C1の署名
(OTC)))+SP向け暗号化したユーザ情報(ID/PW)
+C1&C2の公開鍵+Aの署名
(C1の公開鍵)
S7
NO
YES
ユーザ情報(ID/PW)及び全ての署名
(C1、C2、Aの署名)の確認?
S8
NO
YES
S11
初期登録失敗処理
完了ページをコンピュータC1に送信
Aの署名(C1の公開鍵)+SPの署名(C1の公開鍵)
S9
初期登録処理終了
S10

【図９】

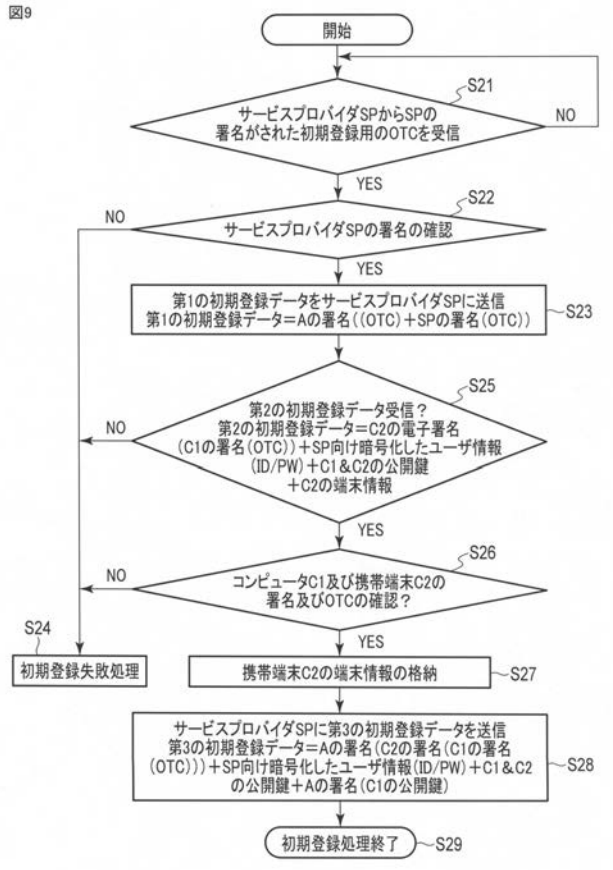
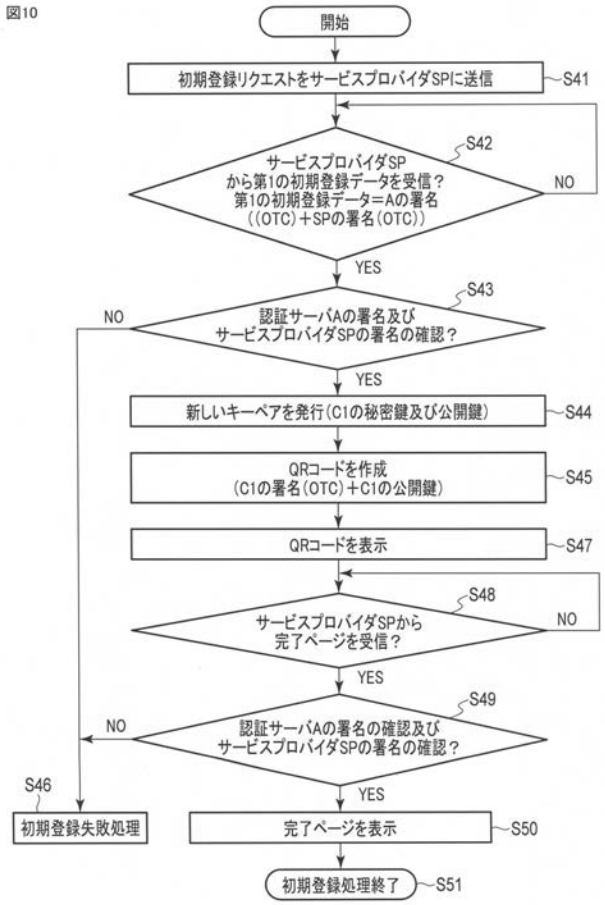
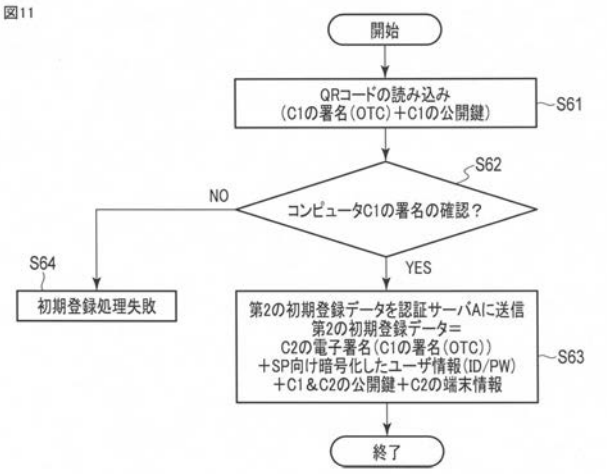


図9
開始
サービスプロバイダSPからSPの
署名がされた初期登録用のOTCを受信
S21
NO
YES
サービスプロバイダSPの署名の確認
S22
NO
YES
第1の初期登録データをサービスプロバイダSPに送信
第1の初期登録データ=Aの署名((OTC)+SPの署名(OTC))
S23
第2の初期登録データ受信?
第2の初期登録データ=C2の電子署名
(C1の署名(OTC))+SP向け暗号化したユーザ情報
(ID/PW)+C1&C2の公開鍵
+C2の端末情報
S25
NO
YES
コンピュータC1及び携帯端末C2の
署名及びOTCの確認?
S26
NO
YES
S24
初期登録失敗処理
携帯端末C2の端末情報の格納
S27
サービスプロバイダSPに第3の初期登録データを送信
第3の初期登録データ=Aの署名(C2の署名(C1の署名
(OTC)))+SP向け暗号化したユーザ情報(ID/PW)+C1&C2
の公開鍵+Aの署名(C1の公開鍵)
S28
初期登録処理終了
S29

【図１０】

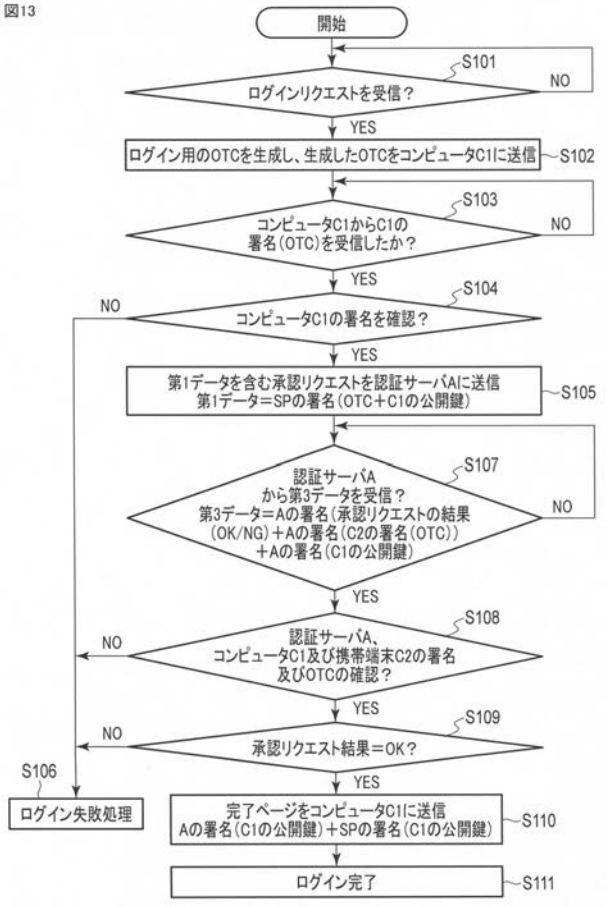


【図１１】

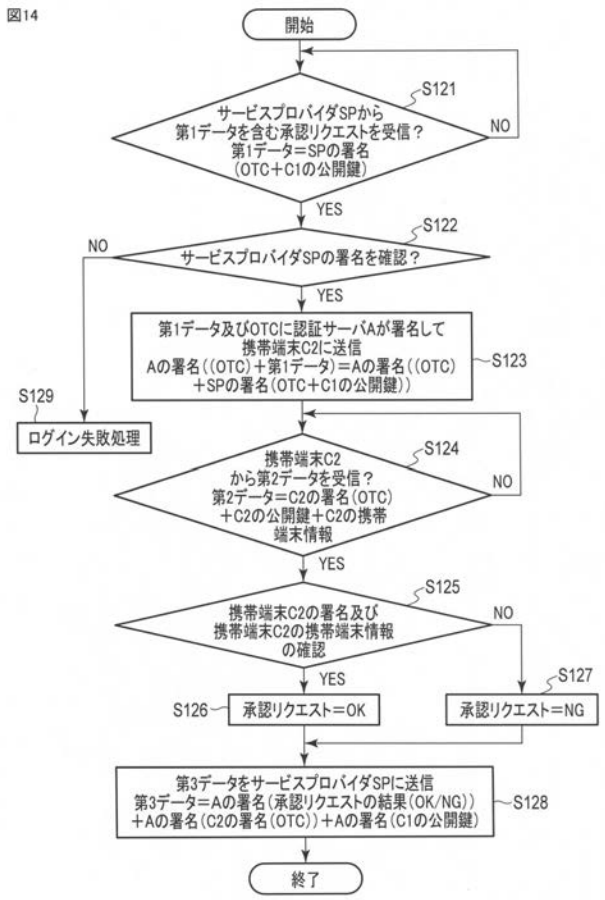


【図１２】

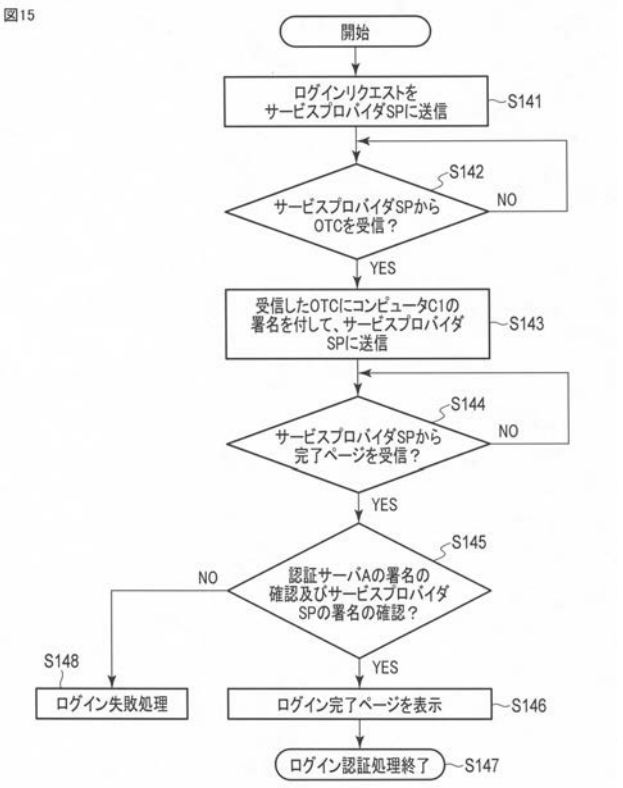
【図１３】



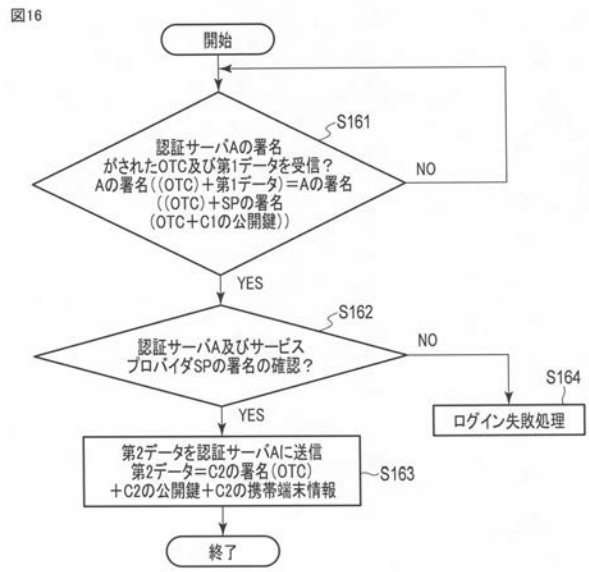
【図１４】



【図１５】



【図１６】



【図１７】

図17

	既存ログイン方式	新しいログイン方式
ID・PWD漏れ	・ID・PWD漏れが発生した場合、ID・PWDを取得した人は誰でも顧客のコンテンツにアクセスが可能	・ID・PWDを使わないことで根本的にID・PWDの漏れを防ぐ （顧客の秘密鍵へのアクセスは、生体認証付きでアクセスを許可する）
サーバハッキング	・サーバに対してハッキングが発生し、顧客認証情報（ID・PWD）が盗まれた場合、ID・PWD漏れと同じ被害が発生	・ログイン認証に必要な顧客の秘密鍵をサーバ側で保持しないことで、サーバがハッキングされても認証情報の漏れにならない
サイト成りすまし	・顧客が成りすましサイトに接続し、ID・PWDを入力すると、ID・PWDが盗まれる恐れがある	・署名付きの通信で成りすまし不可

フロントページの続き

(72)発明者　岡田　隆
東京都港区東麻布１－７－３　第二渡邊ビル７Ｆ　ソラミツ株式会社内
(72)発明者　武宮　誠
東京都港区東麻布１－７－３　第二渡邊ビル７Ｆ　ソラミツ株式会社内
(72)発明者　米津　武至
東京都港区東麻布１－７－３　第二渡邊ビル７Ｆ　ソラミツ株式会社内
(72)発明者　楠　雄治
東京都世田谷区玉川１－１４－１　楽天クリムゾンハウス　楽天証券株式会社内
(72)発明者　平山　忍
東京都世田谷区玉川１－１４－１　楽天クリムゾンハウス　楽天証券株式会社内
(72)発明者　矢田　耕一
東京都世田谷区玉川１－１４－１　楽天クリムゾンハウス　楽天証券株式会社内
(72)発明者　白崎　宏一
東京都世田谷区玉川１－１４－１　楽天クリムゾンハウス　楽天証券株式会社内
(72)発明者　石井　智晶
東京都世田谷区玉川１－１４－１　楽天クリムゾンハウス　楽天証券株式会社内
(72)発明者　南波　環樹
東京都世田谷区玉川１－１４－１　楽天クリムゾンハウス　楽天証券株式会社内
(72)発明者　沈　秀輔
東京都世田谷区玉川１－１４－１　楽天クリムゾンハウス　楽天証券株式会社内

Ｆターム(参考) 5J104 AA07　KA05　NA38　PA07

(54)【発明の名称】ログイン認証システム、ログイン認証システムにおけるサービスプロバイダ及び認証サーバ、ログイン認証システムにおけるサービスプロバイダ、認証サーバ、コンピュータ及び携帯端末のためのログイン認証方法及びプログラム