(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第6918576号
(P6918576)

(45)発行日　令和3年8月11日(2021.8.11)　(24)登録日　令和3年7月27日(2021.7.27)

(51)Int.Cl.		F I		
G06F 21/33	(2013.01)	G06F	21/33	
G06F 21/31	(2013.01)	G06F	21/31	
G06F 21/32	(2013.01)	G06F	21/32	
H04L 9/32	(2006.01)	H04L	9/00	673D
H04L 9/10	(2006.01)	H04L	9/00	675B

請求項の数 13　(全 25 頁)　最終頁に続く

(21)出願番号　特願2017-102857(P2017-102857)
(22)出願日　平成29年5月24日(2017.5.24)
(65)公開番号　特開2018-197997(P2018-197997A)
(43)公開日　平成30年12月13日(2018.12.13)
審査請求日　令和2年5月21日(2020.5.21)

(73)特許権者　000001007
キヤノン株式会社
東京都大田区下丸子３丁目３０番２号
(74)代理人　100126240
弁理士　阿部　琢磨
(74)代理人　100124442
弁理士　黒岩　創吾
(72)発明者　船山　弘孝
東京都大田区下丸子３丁目３０番２号キヤノン株式会社内

審査官　平井　誠

最終頁に続く

(54)【発明の名称】システム、情報処理装置、方法及びプログラム

(57)【特許請求の範囲】
【請求項１】
第１認証モジュールと耐タンパー性を備える第１記憶手段とを有し、該第１認証モジュールによるユーザーの認証のための認証情報と該認証情報に関連付けて秘密鍵とを前記第１記憶手段に格納し、前記秘密鍵に対応する公開鍵をサービス提供システムに登録済みの第１情報処理装置と、
前記公開鍵を登録し、前記第１情報処理装置を介して前記ユーザーに機能を提供する際に前記第１情報処理装置から受け付けた前記秘密鍵で暗号化されたデータを前記登録された公開鍵により検証するサービス提供システムと、
第２認証モジュールと耐タンパー性を備える第２記憶手段とを有する第２情報処理装置と、を含むシステムであって、
前記第２情報処理装置における、前記サービス提供システムで発行された第１検証用データを受信した場合に、当該第１検証用データを含む認証要求を、前記第１情報処理装置に対して送信する第１送信手段と、
前記第１情報処理装置における、前記第２情報処理装置からの前記認証要求の受信に応じて、ユーザーにより入力された認証情報を用いた、前記第１認証モジュールを介した認証処理を実行する認証手段と、
前記第１情報処理装置における、前記第１認証モジュールを介した認証処理が成功した際に、前記第１記憶手段に格納された前記秘密鍵を用いて前記認証要求に含まれる第１検証用データを暗号化する第１暗号化手段と、

前記第１情報処理装置における、前記第１記憶手段に格納された前記秘密鍵を用いて前記暗号化されたデータを、前記第２情報処理装置に対して返却する返却手段と、
前記第２情報処理装置における、前記第１情報処理装置から返却された前記暗号化されたデータを、前記サービス提供システムに送信する第２送信手段と、
前記サービス提供システムにおける、前記暗号化されたデータを前記登録された公開鍵により復号した結果、前記第１検証用データであると検証できた場合に、第２検証用データを前記第２情報処理装置に対して提供する提供手段と、
前記第２情報処理装置における、前記第２認証モジュールによる前記ユーザーの認証情報の登録の際に秘密鍵と公開鍵を生成し、該認証情報と該秘密鍵とを前記第２記憶手段に格納する格納手段と、
前記第２情報処理装置における、前記第２記憶手段に格納された前記秘密鍵を用いて前記第２検証用データを暗号化する第２暗号化手段と、
前記第２情報処理装置における、前記第２記憶手段に格納された前記秘密鍵に対応する前記公開鍵と、前記第２記憶手段に格納された前記秘密鍵を用いて前記暗号化されたデータとを、前記サービス提供システムに送信する第３送信手段と、
前記サービス提供システムにおける、前記第３送信手段により送信されてきた前記暗号化されたデータを前記公開鍵により復号した結果、前記第２検証用データであると検証できた場合に、当該公開鍵を登録する登録手段と、
を有することを特徴とするシステム。

【請求項２】

第１認証モジュールと、該第１認証モジュールにより認証処理を行う際に必要なユーザーの認証情報と、該認証情報の登録の際に生成された秘密鍵とを格納した耐タンパー性を備える第１記憶手段と、を有する第１情報処理装置と接続できる通信機能、第２認証モジュール、及び、耐タンパー性を備える第２記憶手段、を有する第２情報処理装置であって、
前記第１情報処理装置の前記秘密鍵に対応する公開鍵が登録されているサービス提供システムで発行された第１検証用データを受信した場合に、当該第１検証用データを含む認証要求を、前記第１情報処理装置に対して送信する第１送信手段と、
前記第１情報処理装置における前記第１認証モジュールを介した前記ユーザーの認証処理の成功に応じて前記第１記憶手段に格納された前記秘密鍵を用いて暗号化された前記第１検証用データが、前記第１情報処理装置から返却された場合に、該暗号化されたデータを前記サービス提供システムに送信する第２送信手段と、
前記第２認証モジュールによる前記ユーザーの認証情報の登録の際に秘密鍵と公開鍵を生成され、該認証情報と該秘密鍵とが前記第２記憶手段に格納され、かつ、前記サービス提供システムにおける前記暗号化されたデータの前記登録された前記公開鍵による検証に従い前記サービス提供システムから第２検証用データが提供された場合に、前記提供された第２検証用データに対する応答として、前記第２記憶手段に格納された前記秘密鍵に対応する前記公開鍵と、前記第２記憶手段に格納された前記秘密鍵を用いて前記暗号化されたデータとを、前記サービス提供システムに送信する第３送信手段と、
を有することを特徴とする第２情報処理装置。

【請求項３】

前記第１情報処理装置から、前記サービス提供システムの移行用情報を取得する取得手段を、さらに、有し、
前記移行用情報を用いて前記サービス提供システムにアクセスすることで、前記サービス提供システムから前記第１検証用データが受信されることを特徴とする請求項２に記載の第２情報処理装置。

【請求項４】

前記第１情報処理装置が複数の異なるサービス提供システムに対してそれぞれ公開鍵を登録しており、
前記取得手段が前記第１情報処理装置から前記複数のサービス提供システムの移行用情

報を取得した場合には、各サービス提供システムに対して、前記第１送信手段、前記第２送信手段、及び前記第３送信手段による処理を繰り返し実行することを特徴とする請求項３に記載の第２情報処理装置。

【請求項５】

前記第１送信手段は、前記ユーザーの選択に応じて、前記第１検証用データを含む認証要求を、前記第１情報処理装置に対して送信することを特徴とする請求項２乃至４のいずれか１項に記載の第２情報処理装置。

【請求項６】

前記認証情報は、前記ユーザーの生体情報に基づく情報であることを特徴とする請求項２乃至５のいずれか１項に記載の第２情報処理装置。

【請求項７】

前記生体情報は、前記ユーザーの指紋、顔、虹彩、静脈、及び声紋の少なくともいずれかの情報であることを特徴とする請求項６に記載の第２情報処理装置。

【請求項８】

第１認証モジュールと、該第１認証モジュールにより認証処理を行う際に必要なユーザーの認証情報と、該認証情報の登録の際に生成された秘密鍵とを格納した耐タンパー性を備える第１記憶手段と、を有する第１情報処理装置と接続できる通信機能、第２認証モジュール、及び、耐タンパー性を備える第２記憶手段、を有する第２情報処理装置における方法であって、

前記第１情報処理装置の前記秘密鍵に対応する公開鍵が登録されているサービス提供システムで発行された第１検証用データを受信した場合に、当該第１検証用データを含む認証要求を、前記第１情報処理装置に対して送信する第１送信ステップと、

前記第１情報処理装置における前記第１認証モジュールを介した前記ユーザーの認証処理の成功に応じて前記第１記憶手段に格納された前記秘密鍵を用いて暗号化された前記第１検証用データが、前記第１情報処理装置から返却された場合に、該暗号化されたデータを前記サービス提供システムに送信する第２送信ステップと、

前記第２認証モジュールによる前記ユーザーの認証情報の登録の際に秘密鍵と公開鍵を生成され、該認証情報と該秘密鍵とが前記第２記憶手段に格納され、かつ、前記サービス提供システムにおける前記暗号化されたデータの前記登録された前記公開鍵による検証に従い前記サービス提供システムから第２検証用データが提供された場合に、前記提供された第２検証用データに対する応答として、前記第２記憶手段に格納された前記秘密鍵に対応する前記公開鍵と、前記第２記憶手段に格納された前記秘密鍵を用いて前記暗号化されたデータとを、前記サービス提供システムに送信する第３送信ステップと、

を有することを特徴とする方法。

【請求項９】

請求項２乃至７のいずれか１項に記載の各手段としてコンピュータを機能させるためのプログラム。

【請求項１０】

第１認証モジュールと耐タンパー性を備える第１記憶手段とを有し、該第１認証モジュールによるユーザーの認証のための認証情報と該認証情報に関連付けて第１秘密鍵とを前記第１記憶手段に格納し、前記第１秘密鍵に対応する第１公開鍵をサービス提供システムに登録済みの第１情報処理装置と、

前記第１公開鍵が登録されたサービス提供システムと、

第２認証モジュールと耐タンパー性を備える第２記憶手段とを有する第２情報処理装置と、を含むシステムであって、

前記第１情報処理装置は、前記サービス提供システムに前記第２情報処理装置を新規に登録するために、前記第１認証モジュールで管理された前記サービス提供システムに対応するＵＲＬ情報を用いたアクセスを実行する実行手段と、

前記アクセスに従い前記サービス提供システムで発行された検証用データを受信し、前記ユーザーによる認証情報の入力に応じた前記第１認証モジュールでの認証が成功した場

合に、前記第１秘密鍵と前記検証用データとを用いて作成された署名データを前記サービス提供システムに送信する送信手段と、を有し、
前記サービス提供システムでの前記署名データの前記第１公開鍵による検証に従う前記第２情報処理装置の登録処理に際して、前記第２認証モジュールを外部オーセンティケータとして用いることで、当該第２認証モジュールが前記第２記憶手段で管理する第２秘密鍵に対応する第２公開鍵が前記サービス提供システムに登録されることを特徴とするシステム。
【請求項１１】
前記第１認証モジュールは、前記第１情報処理装置で動作する内部オーセンティケータであることを特徴とする請求項１０に記載のシステム。
【請求項１２】
前記実行手段は、前記第１認証モジュールとは異なるアプリケーションとして実現されることを特徴とする請求項１０または１１に記載のシステム。
【請求項１３】
第１認証モジュールと耐タンパー性を備える第１記憶手段とを有し、該第１認証モジュールによるユーザーの認証のための認証情報と該認証情報に関連付けて第１秘密鍵とを前記第１記憶手段に格納し、前記第１秘密鍵に対応する第１公開鍵をサービス提供システムに登録済みの第１情報処理装置と、
前記第１公開鍵が登録されたサービス提供システムと、
第２認証モジュールと耐タンパー性を備える第２記憶手段とを有する第２情報処理装置と、を含むシステムにおける方法であって、
前記第１情報処理装置は、
前記サービス提供システムに前記第２情報処理装置を新規に登録するために、前記第１認証モジュールで管理された前記サービス提供システムに対応するＵＲＬ情報を用いたアクセスを実行する実行ステップと、
前記アクセスに従い前記サービス提供システムで発行された検証用データを受信し、前記ユーザーによる認証情報の入力に応じた前記第１認証モジュールでの認証が成功した場合に、前記第１秘密鍵と前記検証用データとを用いて作成された署名データを前記サービス提供システムに送信する送信ステップと、を有し、
前記サービス提供システムでの前記署名データの前記第１公開鍵による検証に従う前記第２情報処理装置の登録処理に際して、前記第２認証モジュールを外部オーセンティケータとして用いることで、当該第２認証モジュールが前記第２記憶手段で管理する第２秘密鍵に対応する第２公開鍵が前記サービス提供システムに登録されることを特徴とする方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、デスクトップＰＣや、タブレットやスマートフォンなどの携帯端末のような情報処理装置の特殊なデータを別の装置に移行する際の技術に関する。
【背景技術】
【０００２】
近年、生体認証を含む新たな認証システムとして、ＦＩＤＯ（Ｆａｓｔ　Ｉｄｅｎｔｉｔｙ　Ｏｎｌｉｎｅ）が注目されている。生体認証で用いられる指紋や静脈といった生体情報は、外部に情報が流出してしまった場合に、ＩＤ／パスワード認証におけるパスワードと異なり情報を書き換えることができないため、情報漏洩が致命的になる。これに対して、ＦＩＤＯで想定される仕組みの１つでは、インターネットなどネットワーク上のサービスを利用するための認証作業自体を、ネットワークを経由してサーバー上で行うのではなく、ユーザーの手元にある端末上で行う。サービス上でのユーザーの確認はその認証成功に従う別の方法で保障される。そのため、生体情報がネットワーク上に流れることがなく、情報漏洩のリスクが少ないと言える。

【０００３】
ここで、上述のＦＩＤＯの仕組みなど、生体情報での認証を行う仕組みにおいて、認証に必要な情報は、端末内の耐タンパー性のあるセキュアな領域に格納される。従って、認証に必要な情報はセキュアに管理される一方で容易に取り出すことができないため、ユーザーが利用する情報処理装置を変更する時などには、データ移行が比較的難しいといえる。多くの場合は、新たな情報処理装置側で、ユーザーによる登録作業の完全なやり直しを求められる。
【０００４】
データ移行に関する技従来技術としては特許文献１がある。特許文献１では、まず、端末間でのデータ移行時に移行元端末から出力した移行データが端末依存情報だった場合に、端末非依存情報に書き換える。そして、移行先端末が、移行元端末が出力したその移行データを取り込む際には、移行先端末で使用できる端末依存情報に復元する技術が開示されている。
【先行技術文献】
【特許文献】
【０００５】
【特許文献１】特開２０１４－２３５５８３号公報
【発明の概要】
【発明が解決しようとする課題】
【０００６】
ユーザーが利用する情報処理装置を変更する時（買い替えなど）に上述のような仕組みを採用するサービスを変更後の装置でも利用したい場合がある。しかしながら、そのようなサービスを利用するために情報処理装置で管理される情報には上述した認証に必要な情報も含まれるため、特許文献１に記載の技術のような新旧の装置間での簡単なデータ移行でサービスを継続利用できるようになるわけではない。
【課題を解決するための手段】
【０００７】
本発明におけるシステムは、
第１認証モジュールと耐タンパー性を備える第１記憶手段とを有し、該第１認証モジュールによるユーザーの認証のための認証情報と該認証情報に関連付けて秘密鍵とを前記第１記憶手段に格納し、前記秘密鍵に対応する公開鍵をサービス提供システムに登録済みの第１情報処理装置と、
前記公開鍵を登録し、前記第１情報処理装置を介して前記ユーザーに機能を提供する際に前記第１情報処理装置から受け付けた前記秘密鍵で暗号化されたデータを前記登録された公開鍵により検証するサービス提供システムと、
第２認証モジュールと耐タンパー性を備える第２記憶手段とを有する第２情報処理装置と、を含むシステムであって、
前記第２情報処理装置における、前記サービス提供システムで発行された第１検証用データを受信した場合に、当該第１検証用データを含む認証要求を、前記第１情報処理装置に対して送信する第１送信手段と、前記第１情報処理装置における、前記第２情報処理装置からの前記認証要求の受信に応じて、ユーザーにより入力された認証情報を用いた、前記第１認証モジュールを介した認証処理を実行する認証手段と、前記第１情報処理装置における、前記第１認証モジュールを介した認証処理が成功した際に、前記第１記憶手段に格納された前記秘密鍵を用いて前記認証要求に含まれる第１検証用データを暗号化する第１暗号化手段と、前記第１情報処理装置における、前記第１記憶手段に格納された前記秘密鍵を用いて前記暗号化されたデータを、前記第２情報処理装置に対して返却する返却手段と、前記第２情報処理装置における、前記第１情報処理装置から返却された前記暗号化されたデータを、前記サービス提供システムに送信する第２送信手段と、前記サービス提供システムにおける、前記暗号化されたデータを前記登録された公開鍵により復号した結果、前記第１検証用データであると検証できた場合に、第２検証用データを前記第２情報

処理装置に対して提供する提供手段と、前記第２情報処理装置における、前記第２認証モジュールによる前記ユーザーの認証情報の登録の際に秘密鍵と公開鍵を生成し、該認証情報と該秘密鍵とを前記第２記憶手段に格納する格納手段と、前記第２情報処理装置における、前記第２記憶手段に格納された前記秘密鍵を用いて前記第２検証用データを暗号化する第２暗号化手段と、前記第２情報処理装置における、前記第２記憶手段に格納された前記秘密鍵に対応する前記公開鍵と、前記第２記憶手段に格納された前記秘密鍵を用いて前記暗号化されたデータとを、前記サービス提供システムにおける、前記第３送信手段により送信されてきた前記暗号化されたデータを前記公開鍵により復号した結果、前記第２検証用データであると検証できた場合に、当該公開鍵を登録する登録手段と、を有することを特徴とする。

【発明の効果】

【０００８】

本発明によれば、利用する情報処理装置を変更する際などに、生体認証などを用いた認証の仕組みを利用するサービスを、変更後の端末でも利用する際に必要となる登録作業を簡略化できる。

【図面の簡単な説明】

【０００９】

【図１】本発明のシステム構成の例を示す図である。

【図２】本発明における情報処理装置のハードウェア構成例を示す図である。

【図３】本発明における情報処理装置のソフトウェア構成例を示す図である。

【図４】実施例１における移行作業全体を示すシーケンス。

【図５】移行作業において各端末で表示される画面の例を示す図である。

【図６】実施例１における移行元端末、移行先端末における処理を説明するためのフローチャート。

【図７】移行作業において扱われるデータの構成例を示す図である。

【図８】実施例１で利用されるデータテーブルの例を示す図である。

【図９】実施例２における移行作業全体を示すシーケンス。

【図１０】実施例２における移行先端末での表示制御処理を説明するためのフローチャート。

【図１１】実施例２における移行元端末での表示制御処理を説明するためのフローチャート。

【発明を実施するための形態】

【００１０】

以下、本発明を実施するための形態について図面を用いて説明する。

【００１１】

（実施例１）

図１は、本発明のシステムの全体構成の例を示す図である。

【００１２】

図１において、例えばスマートフォンなどである端末１２１、１２２、連携サービス１１１、１１２はネットワーク１０１～１０４を介して、有線、無線などの通信を利用して、接続されている。ネットワーク１０１～１０４は、例えば、インターネット等のＬＡＮ、ＷＡＮ、電話回線、専用デジタル回線、ＡＴＭやフレームリレー回線、ケーブルテレビ回線、データ放送用無線回線等のいずれであり。またはこれらの組み合わせにより実現される、いわゆる通信ネットワークである。ネットワーク１０１～１０４は、データの送受信が可能であればよい。本明細書ではネットワーク１０１はインターネット、ネットワーク１０１～１０４は企業内ネットワークやサービスプロバイダーのネットワークである。

【００１３】

端末１２１、１２２は、プログラムの実行環境が内蔵された携帯電話、スマートフォン、タブレット端末などの情報処理装置である。端末１２１、１２２は、ウェブブラウザーなどのアプリケーションが実行可能である。また、端末１２１、１２２は、個人を認証す

るための生体情報を取得するためのセンサーやカメラなどを備え、生体情報を検証し、認証するためのプログラムも動作する。

【００１４】

本実施例では、端末１２１、１２２を区別して、端末１２１を移行元端末１２１と呼び、端末１２２を移行先端末１２２と呼ぶことで区別する場合がある。例えば、端末買い替えや追加購入の際の旧端末が移行元端末１２１であり、旧端末の環境が移行されるべき新端末が移行先端末１２２である。本発明では、端末１２１、１２２の接続はＢｌｕｅｔｏｏｔｈ（登録商標）通信を想定しているが、ＵＳＢやＷｉＦｉなど、他の有線、または無線の接続を利用することも可能である。

【００１５】

連携サービス１１１、１１２は、それぞれが機能を提供するサービス提供システムである。サービス提供システムは、１以上のサーバーコンピュータ（仮想マシンも含む）上にて実行され、端末１２１、１２２内で動作するアプリケーションに対してＡｐｐｌｉｃａｔｉｏｎ　Ｐｒｏｇｒａｍ　Ｉｎｔｅｒｆａｃｅ（ＡＰＩ）を公開する。端末１２１、１２２にインストールされているアプリケーションは、連携サービス１１１、１１２が提供する各種ＡＰＩを呼び出すことで、端末１２１、１２２の利用者に連携サービス１１１、１１２を利用した各種機能を提供する。端末１２１、１２２のユーザーは連携サービス１１１、１１２にアカウントを持ち、連携サービス１１１、１１２に対してユーザー自身のアカウントで認証することで、連携サービス１１１、１１２内のユーザー自身のデータにアクセスすることができる。Ｆａｓｔ　Ｉｄｅｎｔｉｔｙ　Ｏｎｌｉｎｅ（ＦＩＤＯ）が適用されたシステムにおいては、連携サービス１１１、１１２は、Ｒｅｌｙｉｎｇ　Ｐａｒｔｙ（ＲＰ）サーバー及びＦＩＤＯサーバーに対応する。

【００１６】

図２は、本発明に係る端末１２１、１２２などを含む情報処理装置のハードウェア構成の例を示す図である。

【００１７】

図２において、Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ（ＣＰＵ）２０２は装置全体の制御を行う。ＣＰＵ２０２はＨａｒｄ　Ｄｉｓｃ　Ｄｒｉｖｅ（ＨＤＤ）２０５に格納されているアプリケーションプログラム、ＯＳ等を実行し、Ｒａｎｄａｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ（ＲＡＭ）２０３にプログラムの実行に必要な情報、ファイル等を一時的に格納する制御を行う。Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ（ＲＯＭ）２０４はフラッシュメモリなどの記憶手段であり、内部には、基本Ｉ／Ｏプログラム等の各種データを記憶する。ＲＡＭ２０３は一時記憶手段であり、ＣＰＵ２０２の主メモリ、ワークエリア等として機能する。ＨａｒｄＤｉｓｃＤｒｉｖｅ（ＨＤＤ）２０５は補助記憶装置の一つであり、大容量メモリとして機能し、Ｗｅｂブラウザ等のアプリケーションプログラム、サービスサーバー群のプログラム、ＯＳ、後述する本発明特有の処理の関連プログラム等を格納している。補助記憶装置はＳＳＤやＳＤカードなどで実現してもよい。Ｔｒｕｓｔｅｄ　Ｐｌａｔｆｏｒｍ　Ｍｏｄｕｌｅ（ＴＰＭ）２１０は、機密情報を処理したり格納したりする目的で、格納したデータを外部から読み取られることを防ぐ耐タンパー性を備えた記憶手段（チップ）である。耐タンパー性を備えた記憶手段の具体例としては、業界標準であるＴＰＭ２．０（もしくはそれ以上のバージョン）の仕様に準拠したものを想定している。本発明では、オーセンティケータ（Ａｕｔｈｅｎｔｉｃａｔｏｒ）３０５が、認証に用いる生体情報の特徴量や後述の秘密鍵を格納するために用いる。

【００１８】

タッチパネル２０６は表示と入力の２つの機能を備えており、アプリケーションの画面やキーボードなどを表示したりするとともに、ユーザーが画面に手や専用のペンで圧力を加えることにより、触れられた画面位置情報を外部へ情報信号として出力する。出力された信号情報をアプリケーションが利用することで、ユーザーはタッチパネル２０６を通じてアプリケーションを操作することができる。

【００１９】

生体情報センサー２０７は、ユーザーの生体情報を読取るセンサーである。生体情報としては、例えば、ユーザーの指紋、虹彩、静脈、顔画像、声紋などの情報を読み取り信号に変換する。複数のセンサーを用いて、複数の種類の生体情報を組み合わせて、それらのデータの特徴量を認証情報として扱ってもよい。本特許では、生体情報センサー２０７として指紋読み取りセンサーを想定しているが、カメラなど他の生体情報センサーであってもよい。また、タッチパネル２０６と重ねて生体情報センサーを実現し、タッチパネル２０６に触れたり、入力を行ったりすると同時に指紋情報などを読み取って、電気信号に変更するといった構成であってもよい。

【００２０】

Ｂｌｕｅｔｏｏｔｈ２０８は、Ｂｌｕｅｔｏｏｔｈ通信を行う送受信機であり、他のＢｌｕｅｔｏｏｔｈ対応端末と接続することで相互に通信を行うことができる通信機能である。システムバス２０１は、装置内におけるデータの流れを司るものである。Ｎｅｔｗｏｒｋ Ｉｎｔｅｒｆａｃｅ Ｃａｒｄ（ＮＩＣ）２０９は、該インターフェース２０９、ネットワーク１０１～１０４を介して外部装置とのデータのやり取りを行う。なお、上記コンピュータの構成はその一例であり、図２の構成例に限定されるものではない。例えば、データやプログラムの格納先は、その特徴に応じてＲＯＭ２０４、ＲＡＭ２０３、ＨＤＤ２０５などで変更することも可能である。また、ＵＳＢインターフェースを備えることもできる。生体情報センサー２０７やＢｌｕｅｔｏｏｔｈは、ＵＳＢ接続された外付けハードウェアで実現することもできる。また、携帯電話などであった場合には通話機能のためのハードウェアなど、他に不図示の構成を備えることも可能である。

【００２１】

加えて、ＣＰＵ２０２がＨＤＤ２０５に記憶されている関連プログラムに基づき処理を実行することによって、図３に示されるようなソフトウェア構成及び図６のフローチャートの各ステップの処理が実現される。

【００２２】

図３は、端末１２１、１２２を含む情報処理装置のソフトウェアのモジュール構成例を示す図である。

【００２３】

端末１２１は、連携アプリケーション３０２、移行アプリケーション３０３、認証クライアント３０４、オーセンティケータ（Ａｕｔｈｅｎｔｉｃａｔｏｒ）３０５の各機能から構成される。

【００２４】

なお、本発明において、オーセンティケータ（Ａｕｔｈｅｎｔｉｃａｔｏｒ）は、認証器としての生体情報センサー２０７と連携して、とくに生体情報である認証情報を情報処理装置内で管理したり、生体情報センサー２０７を制御したりするための認証モジュールである。各端末では、複数のオーセンティケータを接続することができ、１つのオーセンティケータに対して複数の生体情報センサーに関する情報を管理させることもできる。また、端末に無線などで外部接続される生体情報センサーを持つ別の認証端末を外部オーセンティケータとして利用することも可能である。

【００２５】

連携アプリケーション３０２は、連携サービス１１１、１１２が提供する各種ＡＰＩと通信してユーザーに機能を提供するアプリケーションである。ユーザーが連携アプリケーション３０２を用いて連携サービス１１１、１１２にアクセスする場合は、オーセンティケータ３０５の認証情報格納部３３３により格納された認証情報を用いて、連携サービス１１１、１１２に対する認証を行う必要がある。なお、連携サービスごとに連携アプリケーションが用意されているような場合には、複数の連携アプリケーションが端末上にインストールされることになる。

【００２６】

移行アプリケーション３０３は、移行元端末１２１内で管理される、連携サービス１１１、１１２に対する認証などに必要な情報を移行先端末である端末１２２に移行する際に

利用するアプリケーションである。移行アプリケーション３０３は、移行先端末１２２で実行されることになり、移行に係る両端末間で行われるデータ移行のための処理を制御する端末移行制御部３１１と、移行の対象となる連携サービスの情報を一覧で扱うサービス管理部３１２から構成される。移行先端末１２２の移行アプリケーション３０３が移行元端末１２１のＯＳを経由して通信する場合には、移行元端末１２１に移行アプリケーション３０３は必須ではない。

【００２７】

認証クライアント３０４は、登録制御部３２１、認証制御部３２２、オーセンティケータ管理部３２３から構成され、連携サービス１１１、１１２との連携に必要な認証に必要な情報や、１以上のオーセンティケータの管理を行う。ＦＩＤＯが適用されたシステムにおいては、認証クライアント３０４はＦＩＤＯクライアントに対応する。

【００２８】

オーセンティケータ３０５は、おもに生体情報を用いた端末内での認証処理を制御したり、連携サービスとの認証に必要な情報を管理したりする。オーセンティケータ３０５は、生体情報登録処理部３３１、生体情報認証処理部３３２、認証情報格納部３３３、生体情報要求部３３４から構成される。ここで、認証情報格納部３３３は、ＴＰＭ２１０に認証に必要な情報として、例えば、連携サービスに対して登録する公開鍵のペアとなる秘密鍵などの情報を格納する。

【００２９】

なお、この移行アプリケーション３０３、認証クライアント３０４、オーセンティケータ３０５の少なくともいずれかは、端末１２１上で動作するオペレーティングシステム（ＯＳ）とともに同梱されるソフトウェアや、ＯＳの機能として実現することも可能である。

【００３０】

次に、本発明の前提となる移行元端末１２１における連携サービスの利用に必要となる生体情報などの登録処理について説明する。

【００３１】

移行元端末１２１の連携アプリケーション３０２は、連携サービスにアクセスし、生体情報登録処理を開始する。なお、連携アプリケーション３０２がウェブブラウザーであり、連携サービスがウェブブラウザーによってアクセスされるウェブアプリケーションであった場合は、この登録処理はｊａｖａ　ｓｃｒｉｐｔによって実現されても良い。処理を開始すると、連携サービスは、連携アプリケーション３０２にユーザーＩＤ、パスワードの入力を要求し、ユーザーからの入力を待機する。ＩＤ、パスワードが正しく入力された場合、連携サービスを起点にして、移行元端末１２１の連携アプリケーション３０２を経由した、認証クライアント３０４及びオーセンティケータ３０５による生体情報入力処理へ移行する。

【００３２】

生体情報要求部３３４は、生体情報センサー２０７を介して、ユーザーから指紋情報などの生体情報入力を受付ける。生体情報が入力された後、入力された生体情報に１対１に対応する特徴量情報はユニークなＩＤを割り当てられてＴＰＭ２１０に格納される。続いて、生体情報登録処理部３３１は公開鍵、秘密鍵を作成する。その後、認証情報格納部３３３は、連携サービスを識別するためのサービスＩＤ、ユーザーＩＤ、パスワード、作成された秘密鍵、および入力された生体情報に１対１に対応する特徴量情報に対応するＩＤを紐付けて、ＴＰＭ２１０に格納する。ここで、認証情報格納部３３３により格納される情報の一部の例を、表Ａに示す。

【００３３】

【表１】

表Ａ

認証情報ＩＤ	サービスＩＤ	秘密鍵	生体情報ＩＤ
407c-8841-79d	service-a.com	1faea2da-a269-4fa7-812a-509470d9a0cb	d493a744
4c04-428b-a7a2	service-a.com	d7ae30c8-3775-4706-8597-aaf681bc30f5	dcc97daa
92b2-498d-bea6	twitter.com	36ae5eed-732b-4b05-aa7b-4dddb4be3267	51caacaa
：	：	：	

【００３４】

表Ａで、認証情報ＩＤ列は、各認証情報に対して一意なＩＤである。サービスＩＤ列は、連携サービスのトップレベルドメイン、セカンドレベルドメインの情報を格納する。秘密鍵列は、前述のように作成された秘密鍵を格納する。生体情報ＩＤ列は移行元端末１２１の認証情報格納部３３３に格納されている、生体情報の特徴量に対応するＩＤを格納する。

【００３５】

生体情報登録処理部３３１は、認証クライアント３０４にＴＰＭ２１０に格納された秘密鍵とペアで作成された公開鍵と、該秘密鍵に対応する認証情報ＩＤを渡す。登録制御部３２１は、連携サービスに対して、認証情報ＩＤと公開鍵とを送信する。

【００３６】

連携サービスでは、ユーザーＩＤ、パスワードに、送信されてきた認証情報ＩＤと公開鍵を紐付けて保存し、管理する。表Ｂは、連携サービスで管理されるデータテーブルの一部の例である。

【００３７】

【表２】

表Ｂ

認証情報ＩＤ	公開鍵	ユーザーＩＤ
407c-8841-79d	AC43C5FB-BFA2-48D1-A71B-FB04ACDA347A	user001
4c04-428b-a7a2	8143CA9F-35C9-4333-948F-BFCE66A74310	user002
：	：	

【００３８】

ユーザーＩＤに紐付けて、認証情報ＩＤ列、公開鍵列には、認証クライアント３０４から送信されてきた認証情報ＩＤ、公開鍵が格納される。

【００３９】

以降、連携サービスを利用する場合には、まず、生体情報認証処理部３３２による生体情報による端末上での認証が行われ、それにより特定された生体情報ＩＤに対応する秘密鍵で連携サービスから提供されたデータが暗号化される。そして、連携アプリケーション３０２が、その暗号化されたデータ（後述の署名７２３）を連携サービスに送信する。連携サービスでは、受信したデータを登録済みの公開鍵で復号し、データの正当性を検証できた際に個人の認証が成功したとみなし、サービスを提供する。

【００４０】

なお、本発明の特徴でもある、移行先端末１２２で上述の表Ａと同等の情報を格納する手順、及び公開鍵を連携サービスに登録する手順については、図６などを用いて後述する。

【００４１】

図４は、移行先端末１２２でユーザーが操作を開始して、移行元端末１２１から認証に

必要な情報を移行する際の処理全体の流れについて説明したシーケンス図である。データ移行処理では、移行対象となる連携サービスごとに、移行元端末１２１を用いた認証処理（Ｓ８０２～Ｓ８１５）と移行先端末１２２における登録処理（Ｓ８２０～Ｓ８２７）とが連続して実行されることになる。

【００４２】

まず、ユーザーは、移行先端末１２２のデータ移行ウィザードなどに従い、移行元端末１２１からのデータ移行を開始する。その際には、ユーザーによって、移行元端末１２１と移行先端末１２２とがＢｌｕｅｔｏｏｔｈ２０８などを介して接続される。データ移行ウィザードに従う処理の中で、移行元端末１２１にインストールされている連携アプリケーション３０２を起動する。なお、移行先端末１２２の認証クライアント３０４は、接続された移行元端末１２１のオーセンティケータ３０５を外部オーセンティケータとして認識できるようになっている。従って、接続された移行元端末１２１内のオーセンティケータは、移行先端末１２２のオーセンティケータ管理部３２３にて管理されることになる。よって、図４で示すシーケンスにおいては、移行元端末１２１と移行先端末１２２との間の通信は、移行元端末１２１のオーセンティケータ３０５と、移行先端末１２２の認証クライアント３０４とにより、各端末のＯＳなどを経由して行われることになる。

【００４３】

なお、本発明では、移行先端末１２２の認証クライアント３０４から見て、移行先端末１２２内のオーセンティケータ３０５は同じ端末内にあるため内部オーセンティケータと呼び、移行元端末１２１のオーセンティケータ３０５は外部オーセンティケータと呼ぶ。

【００４４】

以降では、特に断りのない限りは、ハードウェアやソフトウェアモジュールの表記について、例えば、移行先端末１２２の端末移行制御部３１１を表す場合は単に「端末移行制御部３１１」と記載する。また、同様に、移行先端末１２２のＴＰＭ２１０は、単に「ＴＰＭ２１０」と記載する。

【００４５】

一方で、移行元端末１２１の端末移行制御部３１１を表す場合は、「移行元端末１２１の端末移行制御部３１１」というように、移行元端末１２１である点を明記する。

【００４６】

次に、移行先端末１２２の連携アプリケーション３０２は、移行元端末１２１からアプリケーションデータを取得して、補助記憶手段に格納する。その際に、Ｓ８０１で、移行元端末１２１に保存されている以下の図８（ａ）（サービスリスト）で示す連携サービスの移行用情報も取得し、移行先端末１２２の補助記憶手段に格納する。

【００４７】

サービスＩＤ列には、連携サービスのトップレベルドメイン、セカンドレベルドメインの情報を格納する。例えば連携サービスのＵＲＬが“ｈｔｔｐ：／／ｗｗｗ．ｓｅｒｖｉｃｅ－ａ．ｃｏｍ”であった場合に、サービスＩＤ列には“ｓｅｒｖｉｃｅ－ａ．ｃｏｍ”が格納される。移行用ＵＲＬ列は、認証に必要な情報を移行するためにサービスＩＤに対応する連携サービスが公開しているＡＰＩのＵＲＬである。連携サービスによっては移行用ＵＲＬが存在しないサービスもあるので、その場合は移行用ＵＲＬカラムをｎｕｌｌにする。移行用ＵＲＬは、移行元端末１２１が予め連携サービスから取得する。

【００４８】

なお、サービスリストに示す移行用情報は、各端末のＯＳが管理していてもよいし、オーセンティケータ３０５が管理していてもよく、全く別のモジュールが管理していてもよい。いずれの場合も、移行先端末１２２の連携アプリケーション３０２は、移行元端末１２１のＯＳを経由して、移行用情報を取得することになる。

【００４９】

続いて、移行先端末１２２の連携アプリケーション３０２は、サービスリストに登録されている、移行用ＵＲＬがｎｕｌｌではない連携サービスについて、データ移行におけるループ処理（Ｓ８０２～Ｓ８２７）を繰り返して実行する。連携サービスが予め提供する

移行用ＵＲＬへのアクセスによって、本実施例では、移行先端末用の連携サービス上での認証のために必要な情報の簡単な登録のための処理が実行されることになる。なお、移行用ＵＲＬが無くても、連携サービスのホームページなどで移行用サービスを提供するリンクなどを用意して、ユーザーがそのリンクを指定することで、本処理を実行するように実現してもよい。

【００５０】

Ｓ８０２にて、端末移行制御部３１１は、連携サービスに対して認証するために、サービスリストにおける移行先ＵＲＬにアクセスする。

【００５１】

Ｓ８０３にて、連携サービスは、図７（Ａ）に示す認証用パラメータ７０１を生成する。認証用パラメータ７０１はアサーションチャレンジ７０２とアサーション拡張領域７０３から構成される。アサーションチャレンジ７０２はチャレンジレスポンス認証をするために利用する検証用データである。アサーション拡張領域７０３は、連携サービスが認証クライアント３０４やオーセンティケータ３０５の動作を制御するために、連携サービスが指定可能な拡張パラメータが格納される。続いて、Ｓ８０４にて、連携サービスは、Ｓ８０３で生成した認証用パラメータ７０１を、端末移行制御部３１１に対して送信する。

【００５２】

Ｓ８１０にて、端末移行制御部３１１は認証用パラメータ７０１を認証制御部３２２に渡す。認証制御部３２２は、図５（ａ－１）で示す移行元端末の選択画面５０１を、移行先端末１２２のタッチパネル２０６に表示する。ユーザーが移行先端末１２２のタッチパネル２０６を介して移行元端末１２１を選択する。ここで、移行元端末の選択画面５０１には接続済みの端末に係る情報が表示される。または、移行元端末の選択画面５０１には接続済みの端末のオーセンティケータを含む、オーセンティケータ管理部３２３にて管理されているオーセンティケータが、選択候補として表示される。

【００５３】

選択画面５０１を介して移行元端末１２１が選択された場合には、認証制御部３２２は、タッチパネル２０６に、図５（ａ－２）で示す移行元端末での生体認証を促す画面５１１を表示する。キャンセルボタンが押下された場合には、データ移行処理が中止される。

【００５４】

Ｓ８１１にて、認証制御部３２２は、Ｓ８１０で選択された移行元端末１２１の生体情報認証処理部３３２に対して、図７（Ｂ）で示す認証要求データ７１１による認証要求を行う。ここで認証要求データ７１１は、認証用パラメータ７０１と連携サービスＩＤ７１２とＷｅｂＯｒｉｇｉｎ７１３を含む。ＷｅｂＯｒｉｇｉｎ７１３、連携サービスＩＤ７１２は、それぞれサービスリストにおける移行用ＵＲＬ、連携サービスＩＤ７１２である。

【００５５】

Ｓ８１２にて、移行元端末１２１の生体情報認証処理部３３２は、生体情報による認証処理を実行する。ここで、図６（Ａ）は、移行元端末１２１における生体情報による認証処理の詳細を説明するためのフローチャートである。

【００５６】

Ｓ６０１にて、移行元端末１２１の生体情報認証処理部３３２は、図５（ｂ）に示す生体情報の入力要求画面５４１を移行元端末１２１のタッチパネル２０６に表示して、ユーザーに対して生体情報センサー２０７への生体情報の入力を促す。Ｓ６０２にて、移行元端末１２１の生体情報認証処理部３３２は、移行元端末１２１の生体情報要求部３３４を介して移行元端末１２１の生体情報センサー２０７で読み取ったユーザーの生体情報の特徴量を取得する。ここで取得した特徴量は、指紋のパターン・虹彩の模様・静脈の形など個人に対してユニークであるものを、ユニーク性を損なわないような値に変換したものである。

【００５７】

Ｓ６０３にて、移行元端末１２１の生体情報認証処理部３３２は、ここで取得した特徴

量と、移行元端末１２１のＴＰＭ２１０に格納済みの生体情報の特徴量とを比較することで生体情報認証を実行する。所定の一致度を示す特徴量が特定された場合には、認証が成功したことになる。移行元端末１２１の生体情報認証処理部３３２は、認証が成功した特徴量に対応する生体情報ＩＤから、移行元端末１２１のＴＰＭ２１０に格納されている秘密鍵を特定する。

【００５８】

Ｓ６０４で、移行元端末１２１の生体情報認証処理部３３２は、特定した秘密鍵を用いて、認証用パラメータ７０１に含まれるアサーションチャレンジ７０２を暗号化して、署名７２３を作成する。

【００５９】

図４で示すシーケンスの説明に戻る。

【００６０】

Ｓ８１３にて、移行元端末１２１の生体情報認証処理部３３２は、Ｓ８１２の生体情報による認証処理で生成した署名７２３を含むアサーション（Ａｓｓｅｒｔｉｏｎ）７２１（図７（Ｃ））を生成し、移行先端末１２２の認証制御部３２２経由で、端末移行制御部３１１に返却する。アサーション７２１は認証情報ＩＤ７２２と署名７２３から構成される。認証情報ＩＤ７２２は、前述のＳ６０４にて署名作成に利用した生体情報ＩＤに紐付けて表Ａで管理されていた認証情報ＩＤである。

【００６１】

Ｓ８１４にて、端末移行制御部３１１は、連携サービスに対してアサーション７２１を送信する。

【００６２】

Ｓ８１５にて、連携サービスは、アサーション７２１の署名７２３を検証する。具体的には、連携サービスは、前述の表Ｂから、認証情報ＩＤ７２２に対応する公開鍵を特定し、署名７２３を復号する。連携サービスは、復号したデータと、Ｓ８０４で送信済みの認証用パラメータ７０１に含まれていたアサーションチャレンジ７０２とを比較して、両者が一致するかを判断する。一致した場合には、登録済みのユーザーのオーセンティケータによる正当な要求であることが検証されたことになる。よって、本移行処理を実行しようとするユーザーに対応するユーザーＩＤが、表Ｂの中から特定されることになる。

【００６３】

なお、この検証処理は、本シーケンスで説明するデータ移行処理に限らず、端末が連携サービスを利用する際の認証においても同様に行われる処理である。つまり、ここでの検証処理は、本データ移行処理を実行しようとしているユーザーを認証するために行われる。

【００６４】

また、Ｓ８１２の認証処理の中で、Ｓ６０３にて生体情報による認証処理に失敗した場合にはＳ６０４で署名が作成されず、移行元端末１２１の生体情報認証処理部３３２から移行先端末１２２の端末移行制御部３１１に対して認証エラーが送信される。この場合には、図４に戻り、次の連携サービスに対するループ処理が実行されることになる。処理すべき連携サービスが無ければ、図４のシーケンスが終了する。

【００６５】

次に、移行先端末１２２のオーセンティケータ３０５を用いた、連携サービスに対する登録処理が行われる。

【００６６】

Ｓ８２０にて、連携サービスは、図７（Ｄ）で示す登録用パラメータ７３１を生成する。Ｓ８２１にて、連携サービスは、生成した登録用パラメータ７３１を移行先端末１２２の端末移行制御部３１１に対して送信する。

【００６７】

登録用パラメータ７３１は、アカウント情報７３２、暗号化パラメータ７３３、ａｔｔｅｓｔａｔｉｏｎチャレンジ７３４、認証拡張領域７３５から構成される。アカウント情

報７３２はＳ８１５で特定したユーザーＩＤや、そのユーザーＩＤと紐づくユーザー名などの属性情報が設定される。暗号化パラメータ７３３は、連携サービスがサポートしている暗号化アルゴリズムなど、登録する認証情報に関する属性情報が設定される。ａｔｔｅｓｔａｔｉｏｎチャレンジ７３４は、チャレンジレスポンス認証をするために連携サービスが発行する検証用データ（パラメータ値）である。認証拡張領域７３５は連携サービスが認証クライアント３０４やオーセンティケータ３０５の動作を制御するために指定可能な拡張パラメータが格納される。

【００６８】

図８（ｂ）は、連携サービスにより管理される、ａｔｔｅｓｔａｔｉｏｎチャレンジの発行状況を管理するためのテーブルの例である。図８（ｂ）によれば、どのユーザーＩＤに対してどのａｔｔｅｓｔａｔｉｏｎチャレンジを発行したかを特定できる。

【００６９】

ａｔｔｅｓｔａｔｉｏｎチャレンジ列は、発行済みのａｔｔｅｓｔａｔｉｏｎチャレンジであるデータを格納する。ユーザーＩＤ列はａｔｔｅｓｔａｔｉｏｎチャレンジを発行したユーザーＩＤの情報を格納する。ここでは、Ｓ８１５にて特定したユーザーＩＤに紐付けてａｔｔｅｓｔａｔｉｏｎチャレンジ７３４が管理されることになる。

【００７０】

Ｓ８２２にて、移行先端末１２２の登録制御部３２１は、端末移行制御部３１１からの登録用パラメータ７３１を用いた生体情報登録要求に応じて、図５（ａ－３）で示す移行先選択画面５２１を移行先端末１２２のタッチパネル２０６に表示する。この選択画面５２１を介して、ユーザーに移行先を選択させることになる。ここで、移行先として選択されるのは、内部または外部のオーセンティケータのいずれかである。続いて、登録制御部３２１は、移行先として選択された移行先端末１２２のオーセンティケータ３０５の生体情報登録処理部３３１に対して、図７（Ｅ）で示す登録要求データ７４１を渡す。ここで登録要求データ７４１は、登録用パラメータ７３１と連携サービスＩＤ７４２とＷｅｂＯｒｉｇｉｎ７４３を含む。ＷｅｂＯｒｉｇｉｎ７４３、連携サービスＩＤ７４２は、それぞれサービスリストにおける移行用ＵＲＬ列の値、連携サービスＩＤ列の値である。

【００７１】

Ｓ８２３にて、オーセンティケータ３０５は、移行先端末１２２における生体情報による認証処理及び登録処理を実行する。図６（Ｂ）は、移行先端末１２２におけるＳ８２３における処理の詳細を説明するためのフローチャートである。

【００７２】

Ｓ６１１にて、生体情報要求部３３４は、認証クライアント３０４からオーセンティケータ３０５に対する登録要求（生体情報登録処理部３３１が登録要求データ７４１を受け取ったこと）に応じて、タッチパネル２０６に図５（ａ－４）で示す生体情報の入力要求画面５３１を表示する。この表示により、ユーザーに対して生体情報センサー２０７への生体情報の入力を促す。Ｓ６１２にて、生体情報登録処理部３３１は、生体情報センサー２０７に対して入力された生体情報の特徴量を受け付ける。

【００７３】

Ｓ６１３にて、認証情報格納部３３３は、Ｓ６１２で取得した生体情報の特徴量と、その特徴量情報に割り当てられたユニークなＩＤ（生体情報ＩＤ）を、移行先端末１２２のＴＰＭ２１０に格納する。同時に、生体情報登録処理部３１１は、生体情報ＩＤに対応する、秘密鍵と公開鍵、認証情報ＩＤをそれぞれ作成する。そして、認証情報格納部３３３は、作成された認証情報ＩＤ、登録要求データ７４１に含まれる連携サービスＩＤ７４２、作成された秘密鍵、生体情報ＩＤを紐付けてＴＰＭ２１０に格納する。ここで格納される情報は、前述した移行元端末１２１の表Ａと同様の形式で格納され、管理されることになる。

【００７４】

Ｓ６１４にて、生体情報登録処理部３３１は、図７（Ｆ）で示すクレデンシャル情報７５１を作成する。クレデンシャル情報７５１は、認証情報ＩＤ７５２とアルゴリズム７５

３と公開鍵７５４とａｔｔｅｓｔａｔｉｏｎ７５５から構成される。
【００７５】
認証情報ＩＤ７５２には、Ｓ６１３にて作成した公開鍵に対応する認証情報ＩＤが設定される。アルゴリズム７５３には、Ｓ６１３における鍵生成に利用したアルゴリズムが設定される。公開鍵７５４には、Ｓ６１３にて作成した公開鍵が設定される。また、ａｔｔｅｓｔａｔｉｏｎ７５５には、ａｔｔｅｓｔａｔｉｏｎチャレンジ７３４をＳ６１３にて生成した秘密鍵を用いて暗号化したデータが設定される。
【００７６】
続いて、図４のシーケンスの説明に戻る。
【００７７】
Ｓ８２４にて、端末移行制御部３１１は、生体情報登録処理部３３１で作成されたクレデンシャル情報７５１を、登録制御部３２１を介して取得して、そのクレデンシャル情報７５１を連携サービスに送信する。クレデンシャル情報７５１の送信は、連携サービスからＳ８２１で送信されてきた登録用パラメータ７３１に対する応答となる。
【００７８】
Ｓ８２５にて、連携サービスは、クレデンシャル情報７５１に含まれるａｔｔｅｓｔａｔｉｏｎ７５５の検証処理を実行する。具体的には、クレデンシャル情報７５１に含まれる公開鍵で、クレデンシャル情報７５１に含まれるａｔｔｅｓｔａｔｉｏｎ７５５を復号する。そして、復号されたデータと前述の図８（ｂ）のテーブル内の発行済みのａｔｔｅｓｔａｔｉｏｎチャレンジとを比較する。図８（ｂ）のテーブル内で復号されたデータと一致するａｔｔｅｓｔａｔｉｏｎチャレンジに紐付くユーザーＩＤが、クレデンシャル情報７５１を用いた登録処理を行いたいユーザーのＩＤであることが特定されることになる。
【００７９】
Ｓ８２６にて、連携サービスは、特定されたユーザーＩＤに紐付けて、クレデンシャル情報７５１に含まれる認証情報７５２、公開鍵７５４を、前述の表Ｂに追加で登録する。
【００８０】
Ｓ８２７にて、連携サービスは、端末移行制御部３１１に対して、正常に登録処理が完了したことを通知する。
【００８１】
移行先端末１２２の端末移行制御部３１１は、サービスリスト（図８（ａ））に登録されている移行用ＵＲＬがｎｕｌｌではない全ての連携サービスに対するループ処理が完了した場合に、Ｓ８２８に進む。
【００８２】
Ｓ８２８では、移行先端末１２２の端末移行制御部３１１は、図５（ａ－５）で示す移行結果についての通知画面５５１を表示する。本図では、移行元端末１２１のサービスリストに登録されていた２つのサービスが移行先端末１２１で同様に利用できるよう、データ移行が成功したことを通知している。
【００８３】
（本実施例におけるメリット）
本発明を適用しない場合には、移行先端末１２２で、移行対象の各連携サービスにアクセスして、ユーザーＩＤ、パスワードを用いて認証（ログイン）した上で、再度、生体認証をしたうえで、サービスに認証情報ＩＤと公開鍵の再登録を行う必要があった。
【００８４】
それに対して、本発明では、移行先端末１２２での移行対象の各連携サービスに対するユーザーＩＤ、パスワードを用いた認証（ログイン）を省略できる。
【００８５】
これにより、例えば、スマートフォンの機種変更時などに、携帯電話会社のキャリア窓口などで簡単に各サービスへの認証に必要な情報の移行作業が行えるようになる。また、そういったキャリア窓口などの第３者が多い場所におけるユーザーＩＤ、パスワードの入

力を回避した上での、移行作業が可能となる。
【００８６】
（変形例）
本実施例では、移行作業のトリガは、移行先端末１２２の移行アプリケーション３０３に対するユーザー操作であった。この場合、連携サービス１１１、１１２に対する認証処理（Ｓ８１２）は外部オーセンティケータとして移行元端末１２１を用い、登録処理（Ｓ８２３）は移行先端末１２２内の内部オーセンティケータを用いていた。
【００８７】
一方で、移行作業のトリガは、移行元端末１２１の移行アプリケーション３０３に対するユーザー操作であってもよい。この場合、連携サービス１１１、１１２に対する認証処理（Ｓ８１２）は移行元端末１２１内の内部オーセンティケータを用い、登録処理（Ｓ８２３）は外部オーセンティケータとしての移行先端末１２２のものを用いることになる。
【００８８】
なお、表Ｂに相当する情報を連携サーバー１１１、１１２に登録する手段として、Ｓ８０２～Ｓ８１５までの連携サービス１１１、１１２に対する認証処理をＢａｓｉｃ認証などの生体認証を使わない方法で行うことも可能である。
【００８９】
（実施例２）
実施例１では、連携サービスごとに、移行元端末１２１での生体認証と移行先端末１２２での生体認証を繰り返しユーザーに行わせることで移行作業をおこなった。顔画像認証や虹彩認証など、カメラなどで撮影することで生体認証を行う場合には、両端末を固定して、常に認証対象が撮影できる状態であれば、とくに煩雑さはない。しかしながら、指紋情報を読み取る生体情報センサー２０７を採用した場合には、各端末の表示に従い、２つの端末に対して交互に指をかざすといった作業が発生し、連携サービスが多い場合にはユーザーが煩雑さを感じる可能性がある。実施例２では、そのような点を改善するための処理を説明する。
【００９０】
実施例２が実施例１と異なる点は、図９で示すように、連携サービスが複数存在する場合に、まずは実施例１における図４のＳ８０２～Ｓ８２１の処理を連携サービスの全てに対して行う。その後に、Ｓ８２２～Ｓ８２７の処理を連携サービスの全てに対して行うようにした。つまり、図９で示すように、連携サービスごとのループ処理を、第１ループ処理（９００）と、第２ループ処理（９１０）に分割したところがポイントである。これによって、移行対象の連携サービスが多い場合でも、各端末での生体認証作業をまとめて行えるようになる。
【００９１】
具体的には、本実施例において、Ｓ８０２～Ｓ８２１の処理を繰り返し実行している間、移行元端末１２１は、指紋センサーとしての生体情報センサー２０７に対してユーザーに指をかざした状態を維持させることで、連続的に生体情報の入力を受け付けるように構成する。同様に、本実施例において、Ｓ８２２～Ｓ８２７の処理を繰り返し実行している間、移行先端末１２２も、生体情報センサー２０７に対してユーザーに指をかざした状態を維持させることで、連続的に生体情報の入力を受け付けるように構成する。
【００９２】
図９で示す処理における、実施例１の図４で示す処理との違いについて説明する。移行アプリケーション３０３の端末移行制御部３１１が、連携サービスから受信した認証用パラメータ７０１のアサーション拡張領域７０３の中に、下記の拡張情報を追記する。
｛’’ｓｅｓｓｉｏｎｉｄ’：’ａｂ１２－１２７ｄ－０１２ｂ－２ｂｅ５’，‘ｒｅｐｅａｔｎｕｍ’：２｝
【００９３】
拡張情報に含まれる‘ｓｅｓｓｉｏｎｉｄ’は、図９のシーケンス単位で一意となるＩＤである。また、拡張情報に含まれる‘ｒｅｐｅａｔｎｕｍ’は、サービスリストに登録

されている連携サービスのうち移行用ＵＲＬが存在するものの総数である。ここでは、図８（ａ）にある通り有効な移行用ＵＲＬが登録された連携サービスが２つなので、拡張情報にも“２”という値が設定されている。

【００９４】

端末移行制御部３１１は、１度の移行処理で連携サービス数分行われる第１ループ処理９００においては、それぞれの連携サービスから受信する認証用パラメータの全てに、同じ‘ｓｅｓｓｉｏｎｉｄ’の値が指定された拡張情報として追記することになる。

【００９５】

拡張情報が追記された認証用パラメータ７０１は、端末移行制御部３１１から認証制御部３２２を経由して、最終的にはＳ８１１にて認証要求データとして移行元端末１２１の生体情報認証処理部３３２に渡る。

【００９６】

この拡張情報を用いて、図９で示すシーケンスにおけるＳ８１０～Ｓ８１２までの間の、移行先端末１２２での画面５０１及び画面５１１の表示を行うか否かが制御（図１０（ａ）で後述）される。さらに、移行元端末１２１では、Ｓ８１２内の処理であるＳ６０１における画面５４１の表示を行うか否かが制御（図１１で後述）される。

【００９７】

さらに、図９で示す処理における、実施例１の図４で示す処理との他の違いについて説明する。移行アプリケーション３０３の端末移行制御部３１１が、連携サービスから受信した登録用パラメータ７３１の認証拡張領域７３５の中に、下記の拡張情報を追記する。

{’’ｓｅｓｓｉｏｎｉｄ’：’ａｂ１２－１２７ｄ－０１２ｂ－２ｂｅ５’,‘ｒｅｐｅａｔｎｕｍ’：２}

【００９８】

拡張情報に含まれる‘ｓｅｓｓｉｏｎｉｄ’は、図９のシーケンス単位で一意となるＩＤである。また、拡張情報に含まれる‘ｒｅｐｅａｔｎｕｍ’は、サービスリストに登録されている連携サービスのうち移行用ＵＲＬが存在するものの総数である。

【００９９】

端末移行制御部３１１は、１度の移行処理で連携サービス数分行われる第２ループ処理９１０においては、それぞれの連携サービスからＳ８２１で受信する登録用パラメータの全てに、同じ‘ｓｅｓｓｉｏｎｉｄ’の値が指定された拡張情報として追記することになる。ここで追記される拡張情報の例として、上述の認証用パラメータ７０１のアサーション拡張領域７０３の中に追記した拡張情報と同じものを利用している。第２ループ処理９１０ように別の拡張情報を利用してもよい。

【０１００】

この拡張情報を用いて、Ｓ８２２における移行先端末１２２での画面５２１の表示を行うか否かが制御（図１０（ａ）で後述）される。さらに、移行先端末１２２では、Ｓ８２３内の処理であるＳ６１１における画面５３１の表示を行うか否かが制御（図１０（ｂ）で後述）される。

【０１０１】

図１０（ａ）は、移行先端末１２２における、図９で示すＳ８１０、Ｓ８２２で提供される画面の表示制御のための拡張処理を説明するためのフローチャートである。

【０１０２】

まず、図９のＳ８１０での制御を説明する。Ｓ８１０では、図４を用いて前述した通り、認証制御部３２２が、端末移行制御部３１１から認証用パラメータ７０１を受け取る。この認証用パラメータ７０１のアサーション拡張領域７０３には、上述した拡張情報が追記されている。

【０１０３】

Ｓ１００１にて、認証制御部３２２は、アサーション拡張領域７０３の中の拡張情報のｓｅｓｓｉｏｎｉｄが、既にメモリに保存済みの判定用のｓｅｓｓｉｏｎｉｄと一致するか否かを判定する。ここで、一致しない場合にはＳ１００２に進む。判定後には、今回の

判定で新たに端末移行制御部３１１から受け取った認証用パラメータ７０１に拡張情報として含まれるｓｅｓｓｉｏｎｉｄを、認証制御部３２２が、次回のＳ１００１での判定処理用に、移行先端末１２２のメモリに保存する。なお、Ｓ１００１で一致しないと判定されるのは、連携サービスごとに行われる第１ループ処理９００における１回目のＳ８１０での処理であることが想定される。

【０１０４】

Ｓ１００２にて、認証制御部３２２は、移行元端末の選択画面５０１を生成する。生成された画面５０１は、Ｓ８１０で説明した通り、移行先端末１２２のタッチパネル２０６に表示されることになる。その後、選択画面５０１を介して移行元端末が選択された場合には、認証制御部３２２は、タッチパネル２０６に、図５（ａ－２）で示す移行元端末での生体認証を促す画面５１１を表示する。ここでは、さらに、認証制御部３２２は、選択画面５０１を介して選択された移行元端末（オーセンティケータ）の情報をメモリに一時保存する。

【０１０５】

その後、Ｓ８１１にて、認証制御部３２２は、Ｓ８１０で選択された移行元端末１２１の生体情報認証処理部３３２に対して、図７（Ｂ）で示す認証要求データ７１１による認証要求を行う。

【０１０６】

ここで、Ｓ１００１にて一致しないとの判定が行われていた場合には、認証制御部３２２により移行元端末の選択画面５０１が生成されない。つまり、Ｓ１００２の処理後に表示されている図５（ａ－２）で示す画面５１１の表示が維持されることになる。その後、Ｓ８１１にて、認証制御部３２２は、既にメモリに一時保存されている移行元端末（オーセンティケータ）の情報に基づき、移行元端末１２１の生体情報認証処理部３３２に対して、図７（Ｂ）で示す認証要求データ７１１による認証要求を行う。

【０１０７】

なお、図９のＳ８２２においても、認証制御部３２２は、登録用パラメータ７３１の認証拡張領域７３５の中に追記された拡張情報を用いて、Ｓ１００１～Ｓ１００２と同様の処理が実行される。Ｓ８２２では、認証制御部３２２は、第１ループ処理９００によって、各連携サービスから登録用パラメータ７３１を受信した状態で開始され、それらを順番に処理していく。

【０１０８】

Ｓ１００１にて、登録制御部３２１は、認証拡張領域７３５の中の拡張情報のｓｅｓｓｉｏｎｉｄが、既にメモリに保存済みの判定用のｓｅｓｓｉｏｎｉｄと一致するか否かを判定する。ここで、一致しない場合にはＳ１００２に進む。判定後には、今回の判定で新たに処理した登録用パラメータ７３１に拡張情報として含まれるｓｅｓｓｉｏｎｉｄを、登録制御部３２１が、次回のＳ１００１での判定処理用に、移行先端末１２２のメモリに保存する。

【０１０９】

Ｓ１００２にて、登録制御部３２１は、移行先の選択画面５２１を生成する。生成された画面５２２は、Ｓ８２２で説明した通り、移行先端末１２２のタッチパネル２０６に表示されることになる。その後、選択画面５２２を介して移行先が選択された場合には、登録制御部３２１は、移行先として選択された端末（オーセンティケータ）の情報をメモリに一時保存する。選択された移行先端末１２２のオーセンティケータ３０５の生体情報登録処理部３３１に対して、図７（Ｅ）で示す登録要求データ７４１を渡す。

【０１１０】

ここで、Ｓ１００１にて一致しないとの判定が行われていた場合には、登録制御部３２１は、選択画面５２２を生成しない。つまりは、その表示をスキップして、既にメモリに一時保存されている移行先の情報に基づき、オーセンティケータ３０５の生体情報登録処理部３３１に対して、図７（Ｅ）で示す登録要求データ７４１を渡す。

【０１１１】

図１０（ｂ）は、移行先端末１２２における、図９のＳ８２３の処理内のＳ６１１及びＳ６１２に対応して実行される要求画面５３１に係る表示制御処理を具体的に説明するためのフローチャートである。本処理は、認証クライアント３０４からのオーセンティケータ３０５に対する登録要求として、生体情報登録処理部３３１が登録要求データ７４１を受け取ったことに応じて、開始される。

【０１１２】

Ｓ１０１１にて、生体情報要求部３３４は、登録要求データ７４１に追記されている拡張情報のｓｅｓｓｉｏｎｉｄと、既にメモリに保存済みの判定用のｓｅｓｓｉｏｎｉｄと一致するか否かを判定する。ここで、一致しない場合にはＳ１０１２に進み、一致する場合にはＳ１０１６に進む。

【０１１３】

Ｓ１０１２にて、生体情報要求部３３４は、要求画面５３１を生成する。生成された画面５３１は、Ｓ６１１で説明した通り、移行先端末１２２のタッチパネル２０６に表示されることになる。

【０１１４】

Ｓ１０１３にて、生体情報要求部３３４は、登録要求データ７４１に追記されている拡張情報に含まれるパラメータ‘ｒｅｐｅａｔｎｕｍ’の値が１であるか否かを判定する。ここで、‘ｒｅｐｅａｔｎｕｍ’の値が１であると判定された場合にはＳ１０１４に進む。

【０１１５】

Ｓ１０１４では、生体情報要求部３３４は、生体情報センサー２０７に対して入力された生体情報の特徴量を受け付け（Ｓ６１２）に応じて、タッチパネル２０６に表示中の要求画面５３１を削除する。つまりは、生体情報を受け付けて連携サービスにクレデンシャル情報を応答（Ｓ８２４）するまでの間に、要求画面５３１がタッチパネル２０６上から消えることになる。

【０１１６】

Ｓ１０１３で‘ｒｅｐｅａｔｎｕｍ’の値が１でない、つまりは２以上の整数であると判定された場合には、タッチパネル２０６上の要求画面５３１の表示が維持されることになる。さらに、Ｓ１０１５にて、生体情報要求部３３４は、呼出回数として“１”を、メモリに一時保存する。

【０１１７】

Ｓ１０１６にて、生体情報要求部３３４は、呼出回数の値を１だけインクリメントして、ｓｅｓｓｉｏｎｉｄが同じ登録要求データ７４１による登録要求の回数をカウントする。Ｓ１０１７にて、生体情報要求部３３４は、呼出回数の値が、登録要求データ７４１に追記されている拡張情報に含まれるパラメータ‘ｒｅｐｅａｔｎｕｍ’の値まで達したかを判定する。呼出回数の値が‘ｒｅｐｅａｔｎｕｍ’の値まで達したと判定された場合にはＳ１０１８に進む。

【０１１８】

Ｓ１０１８にて、生体情報要求部３３４は、生体情報センサー２０７に対して入力された生体情報の特徴量を受け付け（Ｓ６１２）に応じて、タッチパネル２０６に表示中の要求画面５３１を削除する。つまりは、生体情報を受け付けて連携サービスにクレデンシャル情報を応答（Ｓ８２４）するまでの間に、要求画面５３１がタッチパネル２０６上から消えることになる。

【０１１９】

Ｓ１０１７にて、‘ｒｅｐｅａｔｎｕｍ’の値に達していない、つまりは、まだ他に第２ループ処理（９１０）で処理すべき連携サービスがある場合には、タッチパネル２０６上の要求画面５３１の表示が維持されることになる。

【０１２０】

図１１は、移行元端末１２１における、図９のＳ８１２の処理内のＳ６０１及びＳ６０２に対応して実行される要求画面５４１に係る表示制御処理を具体的に説明するためのフ

ローチャートである。

【０１２１】

本処理は、移行先端末１２２の認証クライアント３０４からの移行元端末１２１のオーセンティケータ３０５に対する認証要求として、移行元端末１２１の生体情報認証処理部３３２が認証要求データ７１１を受け取ったことに応じて、開始される。

【０１２２】

Ｓ１１０１にて、移行元端末１２１の生体情報認証処理部３３２は、認証要求データ７１１に追記されている拡張情報のｓｅｓｓｉｏｎｉｄと、既にメモリに保存済みの判定用のｓｅｓｓｉｏｎｉｄと一致するか否かを判定する。ここで、一致しない場合にはＳ１０１２に進み、一致する場合にはＳ１０１６に進む。

【０１２３】

Ｓ１１０２にて、移行元端末１２１の生体情報認証処理部３３２は、要求画面５４１を生成する。生成された画面５４１は、Ｓ６０１で説明した通り、移行元端末１２１のタッチパネル２０６に表示されることになる。

【０１２４】

Ｓ１１０３にて、移行元端末１２１の生体情報認証処理部３３２は、認証要求データ７１１に追記されている拡張情報に含まれるパラメータ‘ｒｅｐｅａｔｎｕｍ’の値が１であるか否かを判定する。ここで、‘ｒｅｐｅａｔｎｕｍ’の値が１であると判定された場合にはＳ１１０４に進む。

【０１２５】

Ｓ１１０４では、移行元端末１２１の生体情報認証処理部３３２は、移行元端末１２１の生体情報センサー２０７に対して入力された生体情報の特徴量を受け付け（Ｓ６０２）に応じて、移行元端末１２１のタッチパネル２０６に表示中の要求画面５４１を削除する。つまりは、生体情報を受け付けて、移行先端末１２２にアサーションを返却（Ｓ８１３）するまでの間に、要求画面５４１が移行元端末１２１のタッチパネル２０６上から消えることになる。

【０１２６】

Ｓ１１０３で‘ｒｅｐｅａｔｎｕｍ’の値が１でない、つまりは２以上の整数であると判定された場合には、移行元端末１２１のタッチパネル２０６上の要求画面５４１の表示が維持されることになる。さらに、Ｓ１１０５にて、移行元端末１２１の生体情報認証処理部３３２は、呼出回数として“１”を、メモリに一時保存する。

【０１２７】

Ｓ１１０６にて、移行元端末１２１の生体情報認証処理部３３２は、呼出回数の値を１だけインクリメントして、ｓｅｓｓｉｏｎｉｄが同じ認証要求データ７１１による認証要求の回数をカウントする。Ｓ１１０７にて、移行元端末１２１の生体情報認証処理部３３２は、呼出回数の値が、認証要求データ７１１に追記されている拡張情報に含まれるパラメータ‘ｒｅｐｅａｔｎｕｍ’の値まで達したかを判定する。呼出回数の値が‘ｒｅｐｅａｔｎｕｍ’の値まで達したと判定された場合にはＳ１１０８に進む。

【０１２８】

Ｓ１１０８にて、移行元端末１２１の生体情報認証処理部３３２は、生体情報センサー２０７に対して入力された生体情報の特徴量を受け付け（Ｓ６０２）に応じて、移行元端末１２１のタッチパネル２０６に表示中の要求画面５４１を削除する。つまりは、生体情報を受け付けて移行先端末１２２にアサーションを返却（Ｓ８１３）するまでの間に、要求画面５４１が移行元端末１２１のタッチパネル２０６上から消えることになる。

【０１２９】

Ｓ１１０７にて、‘ｒｅｐｅａｔｎｕｍ’の値に達していない、つまりは、まだ他に第１ループ処理（９００）で処理すべき連携サービスがある場合には、移行元端末１２１のタッチパネル２０６上の要求画面５４１の表示が維持されることになる。

【０１３０】

（他の実施例）

本発明は、上述した実施形態（実施例１、２、応用例１，２，３）を適宜組み合わせることにより構成された装置あるいはシステムやその方法も含まれるものとする。

【０１３１】

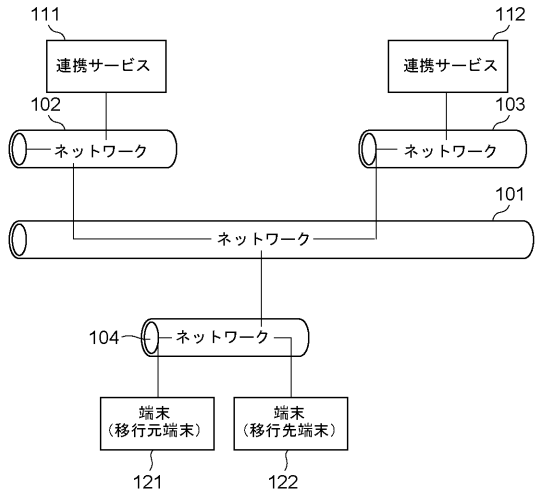
ここで、本発明は、上述した実施形態の機能を実現する１以上のソフトウェア（プログラム）を実行する主体となる装置あるいはシステムである。また、その装置あるいはシステムで実行される上述した実施形態を実現するための方法も本発明の一つである。また、そのプログラムは、ネットワーク又は各種記憶媒体を介してシステム或いは装置に供給され、そのシステム或いは装置の１以上のコンピュータ（ＣＰＵやＭＰＵ等）によりそのプログラムが読み出され、実行される。つまり、本発明の一つとして、さらにそのプログラム自体、あるいは該プログラムを格納したコンピュータにより読み取り可能な各種記憶媒体も含むものとする。また、上述した実施形態の機能を実現する回路（例えば、ＡＳＩＣ）によっても、本発明は実現可能である。

【符号の説明】

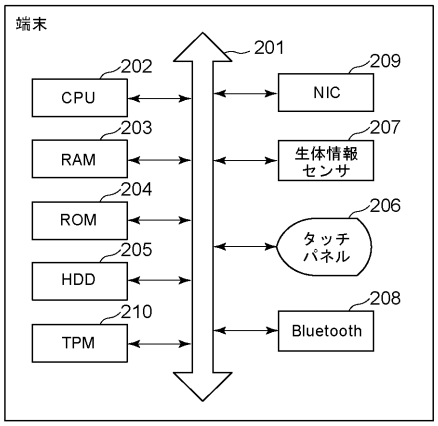
【０１３２】

１１１、１１２　連携サービス
１２１、１２２　端末
３０３　移行アプリケーション
３０４　認証クライアント
３０５　オーセンティケータ（Ａｕｔｈｅｎｔｉｃａｔｏｒ）

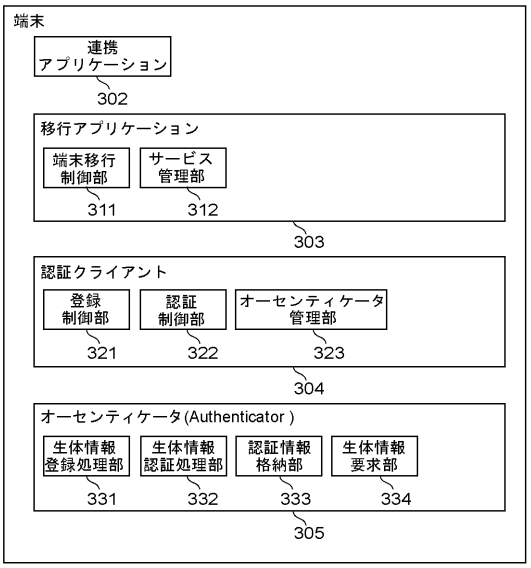
【図１】



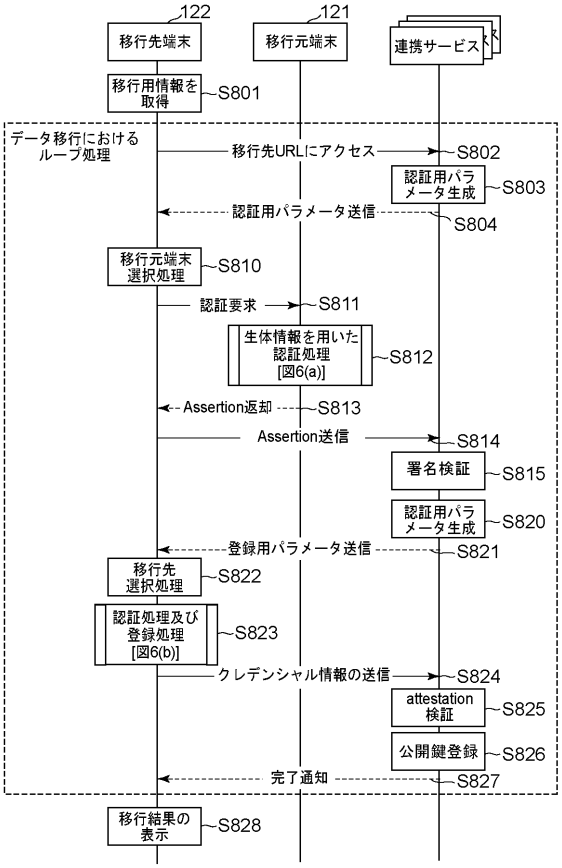
【図２】



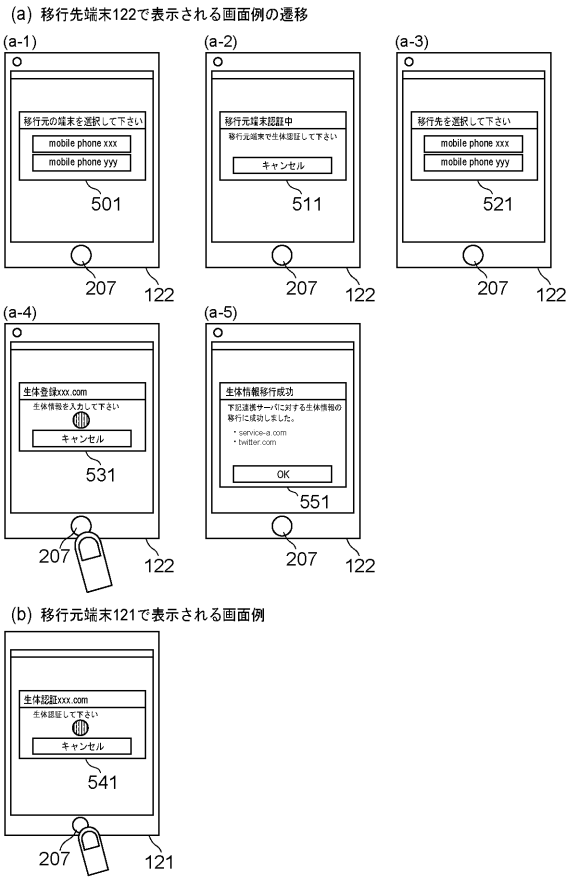
【図３】


端末
連携
アプリケーション
302
移行アプリケーション
端末移行
制御部
311
サービス
管理部
312
303
認証クライアント
登録
制御部
321
認証
制御部
322
オーセンティケータ
管理部
323
304
オーセンティケータ(Authenticator)
生体情報
登録処理部
331
生体情報
認証処理部
332
認証情報
格納部
333
生体情報
要求部
334
305

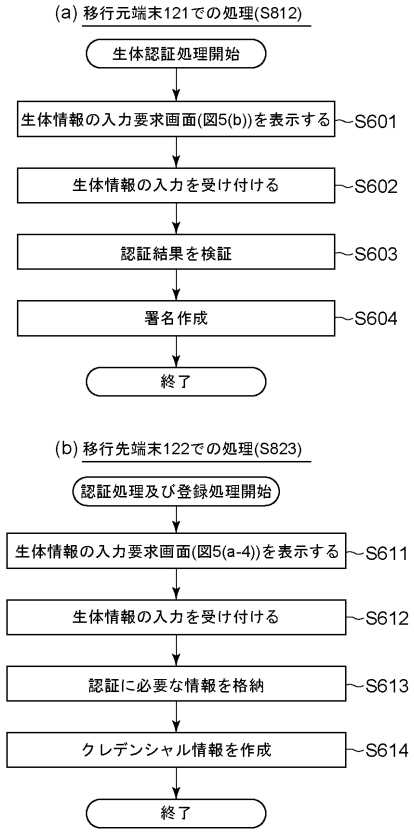
【図４】


122
移行先端末
121
移行元端末
連携サービス
移行用情報を
取得
S801
データ移行における
ループ処理
移行先URLにアクセス
S802
認証用パラ
メータ生成
S803
認証用パラメータ送信
S804
移行元端末
選択処理
S810
認証要求
S811
生体情報を用いた
認証処理
[図6(a)]
S812
Assertion返却
S813
Assertion送信
S814
署名検証
S815
認証用パラ
メータ生成
S820
登録用パラメータ送信
S821
移行先
選択処理
S822
認証処理及び
登録処理
[図6(b)]
S823
クレデンシャル情報の送信
S824
attestation
検証
S825
公開鍵登録
S826
完了通知
S827
移行結果の
表示
S828

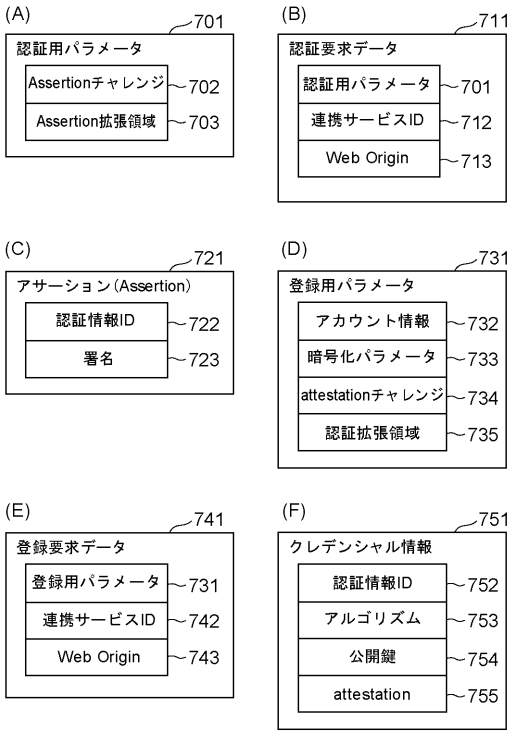
【図５】


(a) 移行先端末122で表示される画面例の遷移
(a-1)
移行元の端末を選択して下さい
mobile phone xxx
mobile phone yyy
501
207
122
(a-2)
移行元端末認証中
移行元端末で生体認証して下さい
キャンセル
511
207
122
(a-3)
移行先を選択して下さい
mobile phone xxx
mobile phone yyy
521
207
122
(a-4)
生体登録xxx.com
生体情報を入力して下さい
キャンセル
531
207
122
(a-5)
生体情報移行成功
下記連携サーバに対する生体情報の
移行に成功しました。
・service-a.com
・twitter.com
OK
551
207
122
(b) 移行元端末121で表示される画面例
生体認証xxx.com
生体認証して下さい
キャンセル
541
207
121

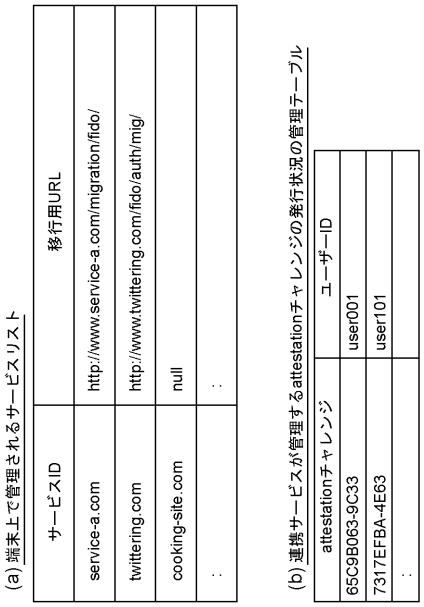
【図６】


(a) 移行元端末121での処理(S812)
生体認証処理開始
生体情報の入力要求画面(図5(b))を表示する
S601
生体情報の入力を受け付ける
S602
認証結果を検証
S603
署名作成
S604
終了
(b) 移行先端末122での処理(S823)
認証処理及び登録処理開始
生体情報の入力要求画面(図5(a-4))を表示する
S611
生体情報の入力を受け付ける
S612
認証に必要な情報を格納
S613
クレデンシャル情報を作成
S614
終了

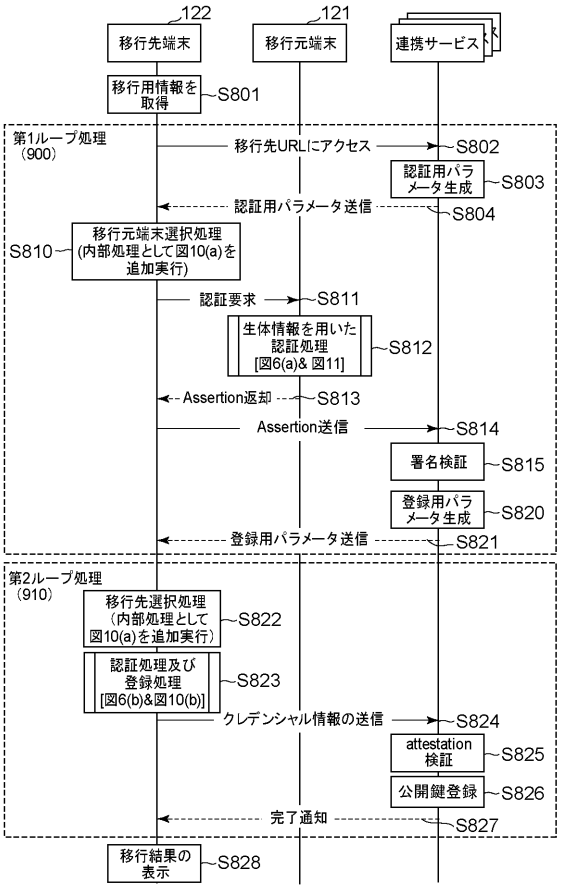
【図７】


(A)
701
認証用パラメータ
Assertionチャレンジ
702
Assertion拡張領域
703
(B)
711
認証要求データ
認証用パラメータ
701
連携サービスID
712
Web Origin
713
(C)
721
アサーション(Assertion)
認証情報ID
722
署名
723
(D)
731
登録用パラメータ
アカウント情報
732
暗号化パラメータ
733
attestationチャレンジ
734
認証拡張領域
735
(E)
741
登録要求データ
登録用パラメータ
731
連携サービスID
742
Web Origin
743
(F)
751
クレデンシャル情報
認証情報ID
752
アルゴリズム
753
公開鍵
754
attestation
755

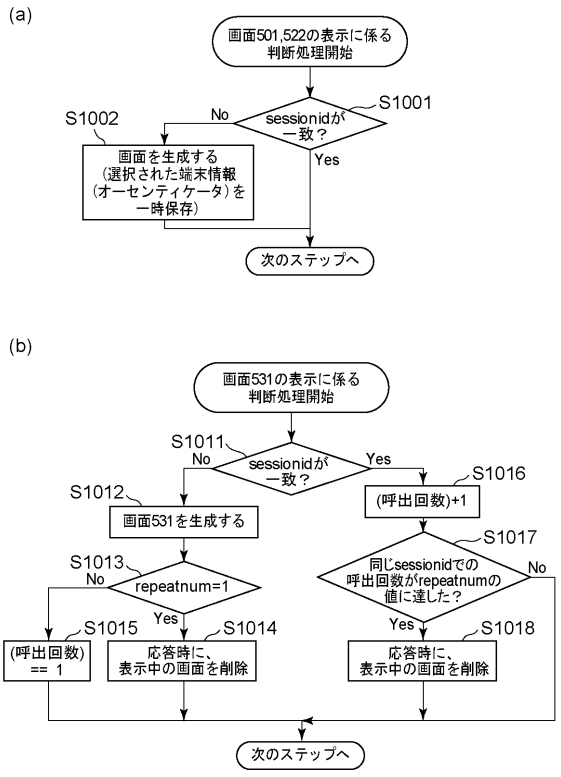
【図８】


(a) 端末上で管理されるサービスリスト
サービスID
移行用URL
service-a.com
http://www.service-a.com/migration/fido/
twittering.com
http://www.twittering.com/fido/auth/mig/
cooking-site.com
null
(b) 連携サービスが管理するattestationチャレンジの発行状況の管理テーブル
attestationチャレンジ
ユーザーID
65C9B063-9C33
user001
7317EFBA-4E63
user101

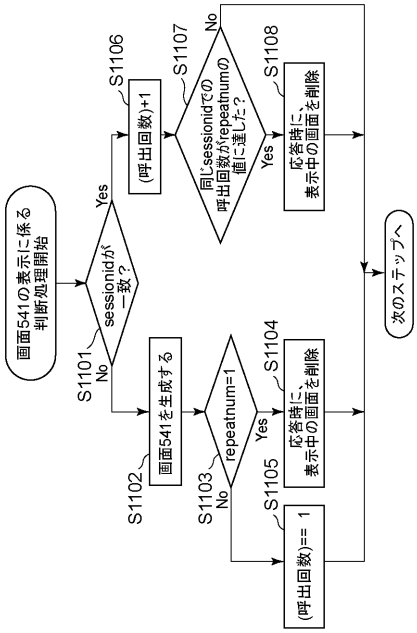
【図９】


122
移行先端末
121
移行元端末
連携サービス
移行用情報を取得
S801
第1ループ処理
(900)
移行先URLにアクセス
S802
認証用パラメータ生成
S803
認証用パラメータ送信
S804
S810
移行元端末選択処理
(内部処理として図10(a)を追加実行)
認証要求
S811
生体情報を用いた認証処理
[図6(a)& 図11]
S812
Assertion返却
S813
Assertion送信
S814
署名検証
S815
登録用パラメータ生成
S820
登録用パラメータ送信
S821
第2ループ処理
(910)
移行先選択処理
(内部処理として図10(a)を追加実行)
S822
認証処理及び登録処理
[図6(b)&図10(b)]
S823
クレデンシャル情報の送信
S824
attestation検証
S825
公開鍵登録
S826
完了通知
S827
移行結果の表示
S828

【図１０】


(a)
画面501,522の表示に係る判断処理開始
S1001
sessionidが一致？
No
Yes
S1002
画面を生成する(選択された端末情報(オーセンティケータ)を一時保存)
次のステップへ
(b)
画面531の表示に係る判断処理開始
S1011
sessionidが一致？
No
Yes
S1012
画面531を生成する
S1013
repeatnum=1
No
Yes
S1015
(呼出回数) == 1
S1014
応答時に、表示中の画面を削除
S1016
(呼出回数)+1
S1017
同じsessionidでの呼出回数がrepeatnumの値に達した？
No
Yes
S1018
応答時に、表示中の画面を削除
次のステップへ

【図１１】


画面541の表示に係る
判断処理開始
S1101
sessionidが
一致？
Yes
No
S1102
画面541を生成する
S1103
repeatnum=1
No
Yes
S1104
応答時に、
表示中の画面を削除
S1105
(呼出回数)== 1
S1106
(呼出回数)+1
S1107
同じsessionidでの
呼出回数がrepeatnumの
値に達した？
No
Yes
S1108
応答時に、
表示中の画面を削除
次のステップへ

フロントページの続き

(51)Int.Cl. FI
H04L 9/00 621A

(56)参考文献 特開２００８－２５７３６５（ＪＰ，Ａ）
特開２０１７－０７３８３５（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ ２１／００－８８
Ｈ０４Ｌ ９／００－３８