(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6071847号
(P6071847)
(45)発行日　平成29年2月1日(2017.2.1)　(24)登録日　平成29年1月13日(2017.1.13)

(51)Int.Cl.　F I
G06F 21/41 (2013.01)　G06F 21/41

請求項の数 6　(全 34 頁)

(21)出願番号　特願2013-230647(P2013-230647)
(22)出願日　平成25年11月6日(2013.11.6)
(65)公開番号　特開2015-90620(P2015-90620A)
(43)公開日　平成27年5月11日(2015.5.11)
審査請求日　平成28年9月27日(2016.9.27)

(73)特許権者　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(73)特許権者　301063496
東芝ソリューション株式会社
神奈川県川崎市幸区堀川町７２番地３４
(74)代理人　100108855
弁理士　蔵田　昌俊
(74)代理人　100109830
弁理士　福原　淑弘
(74)代理人　100103034
弁理士　野河　信久
(74)代理人　100075672
弁理士　峰　隆司

最終頁に続く

(54)【発明の名称】認証システム、方法及びプログラム

(57)【特許請求の範囲】
【請求項１】
ユーザに操作されるユーザ端末に通信可能なサービス提供者装置、ＩＤａａＳ事業者装置及び認証代行装置を備えた認証システムであって、
前記サービス提供者装置は、
当該サービス提供者装置が提供するサービスのアカウントを識別するサービスアカウント識別子及び第１連携ＩＤを含むサービスアカウント情報を記憶するサービスアカウント情報記憶手段、
を備え、
前記ＩＤａａＳ事業者装置は、
前記ユーザを識別するユーザＩＤに一致するＳＳＯ（シングルサインオン）アカウント識別子、前記第１連携ＩＤに一致する第１連携ＩＤ及び前記第１連携ＩＤとは異なる第２連携ＩＤを含むＳＳＯアカウント情報を記憶するＳＳＯアカウント情報記憶手段、
を備え、
前記認証代行装置は、
前記ユーザに対する認証処理のアカウントを識別する認証アカウント識別子、前記第２連携ＩＤに一致する第２連携ＩＤ及び当該認証処理の方式を示す認証クラスを含む認証アカウント情報を記憶する認証アカウント情報記憶手段、
を備え、
前記ユーザ端末から送信されたユーザＩＤ及びＳＳＯ要求に基づいて、当該ユーザＩＤ

に一致するＳＳＯアカウント識別子を含むＳＳＯアカウント情報に第２連携ＩＤを介して関連付けられた認証アカウント情報をもつ前記認証代行装置が、前記ユーザ端末を操作するユーザの認証処理を実行し、
前記認証処理の結果が成功のとき、当該認証処理されたユーザのユーザＩＤに一致するＳＳＯアカウント識別子を含むＳＳＯアカウント情報をもつＩＤｓｓＳ事業者装置が、当該ＳＳＯアカウント情報に第１連携ＩＤを介して関連付けられたサービスアカウント情報に含まれるサービスアカウント識別子で識別されるサービスに対するＳＳＯ認証を許可し、
前記ＳＳＯ認証が許可されたサービスを提供する前記サービス提供装置が、前記ユーザＩＤ及び前記ＳＳＯ要求を送信したユーザ端末に対し、前記サービスに関する情報を送信することを特徴とする認証システム。
【請求項２】
請求項１に記載の認証システムにおいて、
前記認証代行装置は、
前記認証処理の方式を示す認証クラス、及び当該認証処理のレベルを示す認証レベルを関連付けて記述した認証クラス管理テーブルを記憶した第１テーブル記憶手段、
を備え、
前記ＳＳＯアカウント情報記憶手段は、前記認証レベルを含んでおり、
前記認証処理に問題が生じ、当該認証処理のレベルが低下する場合、前記認証代行装置が、当該認証処理の認証レベルを低下させるように前記認証クラス管理テーブルを更新し、前記低下させた認証レベルとこの認証レベルに前記認証アカウント情報内で関連付けられた認証クラスとを前記ＩＤａａＳ事業者装置に送信し、
前記ＩＤａａＳ事業者装置が、前記認証代行装置から認証レベルと認証クラスとを受信すると、当該受信した認証クラスに基づいて前記ＳＳＯアカウント情報を検索し、当該検索により得られた認証レベルを、当該受信した認証レベルに低下させるように前記ＳＳＯアカウント情報を更新する
ことを特徴とする認証システム。
【請求項３】
請求項１に記載の認証システムにおいて、
前記認証代行装置は、
前記認証処理の方式を示す認証クラス、当該認証処理のレベルを示す認証レベル、及び当該認証クラスの認証代行事業者名を含む認証クラスインデックスを関連付けて記述した認証クラス管理テーブルを記憶した第１テーブル記憶手段、
を備え、
前記ＳＳＯアカウント情報記憶手段は、前記認証レベルを含まず、前記認証クラスインデックスを含んでおり、
前記ＩＤａａＳ事業者装置は、
前記認証レベル及び前記認証クラスインデックスを関連付けて記述した認証レベル管理テーブルを記憶した第２テーブル記憶手段、
を備え、
前記認証処理に問題が生じ、当該認証処理のレベルが低下する場合、前記認証代行装置が、当該認証処理の認証レベルを低下させるように前記認証クラス管理テーブルを更新し、前記認証クラス管理テーブル内で低下させた認証レベルとこの認証レベルに関連付けた認証クラスインデックスとを前記ＩＤａａＳ事業者装置に送信し、
前記ＩＤａａＳ事業者装置が、前記認証代行装置から認証レベルと認証クラスインデックスとを受信すると、当該受信した認証クラスインデックスに基づいて前記認証レベル管理テーブルを検索し、当該検索により得られた認証レベルを、当該受信した認証レベルに低下させるように前記認証レベル管理テーブルを更新する
ことを特徴とする認証システム。
【請求項４】

ユーザに操作されるユーザ端末及び前記ユーザにサービスを提供するためのサービス提供者装置にそれぞれ通信可能なＩＤａａＳ事業者装置及び認証代行装置を備えた認証システムであって、
前記サービス提供者装置は、
前記サービスのアカウントを識別するサービスアカウント識別子及び第１連携ＩＤを含むサービスアカウント情報を記憶しており、
前記ＩＤａａＳ事業者装置は、
前記ユーザを識別するユーザＩＤに一致するＳＳＯ（シングルサインオン）アカウント識別子、前記第１連携ＩＤに一致する第１連携ＩＤ及び前記第１連携ＩＤとは異なる第２連携ＩＤを含むＳＳＯアカウント情報を記憶するＳＳＯアカウント情報記憶手段、
を備え、
前記認証代行装置は、
前記ユーザに対する認証処理のアカウントを識別する認証アカウント識別子、前記第２連携ＩＤに一致する第２連携ＩＤ及び当該認証処理の方式を示す認証クラスを含む認証アカウント情報を記憶する認証アカウント情報記憶手段、
を備え、
前記ユーザ端末から送信されたユーザＩＤ及びＳＳＯ要求に基づいて、当該ユーザＩＤに一致するＳＳＯアカウント識別子を含むＳＳＯアカウント情報に第２連携ＩＤを介して関連付けられた認証アカウント情報をもつ前記認証代行装置が、前記ユーザ端末を操作するユーザの認証処理を実行し、
前記認証処理の結果が成功のとき、当該認証処理されたユーザのユーザＩＤに一致するＳＳＯアカウント識別子を含むＳＳＯアカウント情報をもつＩＤｓｓＳ事業者装置が、当該ＳＳＯアカウント情報に第１連携ＩＤを介して関連付けられたサービスアカウント情報に含まれるサービスアカウント識別子で識別されるサービスに対するＳＳＯ認証を許可し、
前記ＳＳＯ認証が許可されたサービスを提供する前記サービス提供装置が、前記ユーザＩＤ及び前記ＳＳＯ要求を送信したユーザ端末に対し、前記サービスに関する情報を送信することを特徴とする認証システム。

【請求項５】

ユーザ端末を操作するユーザに提供するサービスのアカウントを識別するサービスアカウント識別子及び第１連携ＩＤを含むサービスアカウント情報を記憶するサービスアカウント情報記憶手段を備えたサービス提供装置と、
前記ユーザを識別するユーザＩＤに一致するＳＳＯ（シングルサインオン）アカウント識別子、前記第１連携ＩＤに一致する第１連携ＩＤ及び前記第１連携ＩＤとは異なる第２連携ＩＤを含むＳＳＯアカウント情報を記憶するＳＳＯアカウント情報記憶手段を備えたＩＤａａＳ事業者装置と、
前記ユーザに対する認証処理のアカウントを識別する認証アカウント識別子、前記第２連携ＩＤに一致する第２連携ＩＤ及び当該認証処理の方式を示す認証クラスを含む認証アカウント情報を記憶する認証アカウント情報記憶手段を備えた認証代行装置と
を備えた認証システムが実行する認証方法であって、
前記ＩＤａａＳ事業者装置が、前記ユーザ端末から送信されたユーザＩＤ及びＳＳＯ要求に基づいて、当該ユーザＩＤに一致するＳＳＯアカウント識別子を含むＳＳＯアカウント情報に第２連携ＩＤを介して関連付けられた認証アカウント情報をもつ前記認証代行装置に認証要求を送信するステップと、
前記認証代行装置が、前記ＩＤａａＳ事業者装置から受けた認証要求に基づいて、前記ユーザ端末を操作するユーザの認証処理を実行し、当該認証処理の結果を前記ＩＤａａＳ事業者装置に送信するステップと、
前記ＩＤａａＳ事業者装置が、前記認証処理の結果が成功のとき、当該認証処理されたユーザのユーザＩＤに一致するＳＳＯアカウント識別子を含むＳＳＯアカウント情報に第１連携ＩＤを介して関連付けられたサービスアカウント情報に含まれるサービスアカウン

ト識別子で識別されるサービスに対するＳＳＯ認証を許可し、当該許可を前記サービス提供者装置に送信するステップと、
前記サービス提供者装置が、前記ユーザＩＤ及び前記ＳＳＯ要求を送信したユーザ端末に対し、前記ＳＳＯ認証が許可されたサービスに関する情報を送信するステップと、
を備えたことを特徴とする認証方法。
【請求項６】
ユーザ端末を操作するユーザに提供するサービスのアカウントを識別するサービスアカウント識別子及び第１連携ＩＤを含むサービスアカウント情報を記憶したサービス提供装置と、
前記ユーザを識別するユーザＩＤに一致するＳＳＯ（シングルサインオン）アカウント識別子、前記第１連携ＩＤに一致する第１連携ＩＤ及び前記第１連携ＩＤとは異なる第２連携ＩＤを含むＳＳＯアカウント情報を記憶するＳＳＯアカウント情報記憶手段を備えたＩＤａａＳ事業者装置と、
前記認証処理のアカウントを識別する認証アカウント識別子、前記第２連携ＩＤに一致する第２連携ＩＤ及び当該認証処理の方式を示す認証クラスを含む認証アカウント情報を記憶した認証代行装置と
を備えた認証システム内で前記ＩＤａａＳ事業者装置に用いられるプログラムであって、
前記ＩＤａａＳ事業者装置に、
前記ユーザ端末から送信されたユーザＩＤ及びＳＳＯ要求に基づいて、当該ユーザＩＤに一致するＳＳＯアカウント識別子を含むＳＳＯアカウント情報に第２連携ＩＤを介して関連付けられた認証アカウント情報をもつ前記認証代行装置に認証要求を送信する手段、
前記認証代行装置が前記認証要求に基づいて前記ユーザの認証処理を実行した場合に、前記認証処理の結果が成功のとき、当該認証処理されたユーザのユーザＩＤに一致するＳＳＯアカウント識別子を含むＳＳＯアカウント情報に第１連携ＩＤを介して関連付けられたサービスアカウント情報に含まれるサービスアカウント識別子で識別されるサービスに対するＳＳＯ認証を許可し、当該許可を前記サービス提供者装置に送信する手段、
を実現させ、
前記ユーザＩＤ及び前記ＳＳＯ要求を送信したユーザ端末に対し、前記ＳＳＯ認証が許可されたサービスに関する情報を前記サービス提供者装置に送信させる
ことを特徴とするプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明の実施形態は、認証システム、方法及びプログラムに関する。
【背景技術】
【０００２】
近年、企業又はプロバイダ等のサービス提供者は、ユーザのＩＤ及びパスワードを認証し、ユーザにサービスを提供している。
【０００３】
このため、ユーザは、サービス毎に、ＩＤ及びパスワードを管理する必要がある。また、ユーザは、セキュリティ強化の観点から、パスワードの定期的な更新や、複雑で長いパスワードの使用が各サービス提供者から要求される。
【０００４】
ここで、オンラインで金融機関を利用する場合には、本人確認のために乱数カードの利用やワンタイムパスワードの利用などが推奨されている。この場合、ユーザは、サービス毎に、ワンタイムパスワードのデバイスや乱数表を管理する必要がある。
【０００５】
一方、サービス提供者は、ユーザ毎に、ＩＤ及びパスワードを管理及び認証し、サービスを提供する。また、サービス提供者は、コストや運用面から、ワンタイムパスワードの

デバイスや乱数表の利用等により、ユーザ毎のセキュリティ強度を維持している。これらワンタイムパスワードのデバイスや乱数表は、セキュリティ強度を維持するため、他のサービス提供者と共同で利用されることはない。

【０００６】

以上のように、ユーザ及びサービス提供者は、パスワード、ワンタイムパスワードのデバイス又は乱数表などを管理する必要がある。この種の管理は、ユーザとサービスとの組合せ毎に管理対象が増えるため、煩雑になり、利便性を低下させる。このような利便性の低下を阻止する観点から、１回の認証で複数のサービスを利用可能とするシングルサインオン（ＳＳＯ）による認証連携（フェデレーション）が実現されてきている。

【０００７】

このようなシングルサインオンを用いるためには、複数のサービス提供者が互いに信頼関係を結ぶと共に、各サービス提供者のシステム間で認証連携をする必要がある。

【先行技術文献】

【特許文献】

【０００８】

【特許文献１】特許第４９５６０９６号公報

【特許文献２】特開２００１－２７３４２１号公報

【特許文献３】特開２００１－１９７０５５号公報

【発明の概要】

【発明が解決しようとする課題】

【０００９】

しかしながら、以上のような認証連携は、各サービス提供者が他のサービス提供者のシステムを監視する必要が生じるため、運用が複雑化し、サービス提供者の利便性が低下してしまう。

【００１０】

また、以上のような認証連携は、システム間で認証の強度が異なる場合に、シングルサインオンをユーザが安全に利用することが難しくなり、ユーザの利便性を低下させてしまう。

【００１１】

また、サービス提供者は、生体認証などの高セキュアな環境を容易に準備できないため、一旦、構築した環境を利用し続ける可能性が高い。そのため、ユーザに対して提供する認証方法が固定になってしまう。

【００１２】

また、サービス提供者からユーザのＩＤ管理を請け負うＩＤａａＳ（Identity as a Service）事業者が知られている。

【００１３】

本発明が解決しようとする課題は、ユーザ及びサービス提供者の利便性を向上させつつ、認証方式を容易に変更し得る認証システム、方法及びプログラムを提供することである。

【課題を解決するための手段】

【００１４】

実施形態の認証システムは、ユーザに操作されるユーザ端末に通信可能なサービス提供者装置、ＩＤａａＳ事業者装置及び認証代行装置を備えている。

【００１５】

前記サービス提供者装置は、サービスアカウント情報記憶手段を備えている。

【００１６】

前記サービスアカウント情報記憶手段は、当該サービス提供者装置が提供するサービスのアカウントを識別するサービスアカウント識別子及び第１連携ＩＤを含むサービスアカウント情報を記憶する。

【００１７】

前記ＩＤａａＳ事業者装置は、ＳＳＯアカウント情報記憶手段を備えている。

【００１８】

前記ＳＳＯアカウント情報記憶手段は、前記ユーザを識別するユーザＩＤに一致するＳＳＯ（シングルサインオン）アカウント識別子、前記第１連携ＩＤに一致する第１連携ＩＤ及び前記第１連携ＩＤとは異なる第２連携ＩＤを含むＳＳＯアカウント情報を記憶する。

【００１９】

前記認証代行装置は、認証アカウント情報記憶手段を備えている。

【００２０】

前記認証アカウント情報記憶手段は、前記ユーザに対する認証処理のアカウントを識別する認証アカウント識別子、前記第２連携ＩＤに一致する第２連携ＩＤ及び当該認証処理の方式を示す認証クラスを含む認証アカウント情報を記憶する。

【００２１】

前記ユーザ端末から送信されたユーザＩＤ及びＳＳＯ要求に基づいて、当該ユーザＩＤに一致するＳＳＯアカウント識別子を含むＳＳＯアカウント情報に第２連携ＩＤを介して関連付けられた認証アカウント情報をもつ前記認証代行装置は、前記ユーザ端末を操作するユーザの認証処理を実行する。

【００２２】

前記認証処理の結果が成功のとき、当該認証処理されたユーザのユーザＩＤに一致するＳＳＯアカウント識別子を含むＳＳＯアカウント情報をもつＩＤｓｓＳ事業者装置は、当該ＳＳＯアカウント情報に第１連携ＩＤを介して関連付けられたサービスアカウント情報に含まれるサービスアカウント識別子で識別されるサービスに対するＳＳＯ認証を許可する。

【００２３】

前記ＳＳＯ認証が許可されたサービスを提供する前記サービス提供装置は、前記ユーザＩＤ及び前記ＳＳＯ要求を送信したユーザ端末に対し、前記サービスに関する情報を送信する。

【図面の簡単な説明】

【００２４】

【図１】第１の実施形態に係る認証システムの構成を示す模式図である。
【図２】同実施形態における各装置のアカウント情報等を説明するための模式図である。
【図３】同実施形態における各アカウント情報を説明するための模式図である。
【図４】同実施形態における動作の一例を説明するための模式図である。
【図５】同実施形態における業務シーケンスの一例を示すシーケンス図である。
【図６】同実施形態における業務シーケンスの一例を示すシーケンス図である。
【図７】同実施形態における動作の一例を説明するためのフローチャートである。
【図８】同実施形態における動作の一例を説明するためのフローチャートである。
【図９】同実施形態における動作の一例を説明するための模式図である。
【図１０】第２の実施形態に係る認証システムに適用される各管理テーブルを説明するための模式図である。
【図１１】同実施形態における各アカウント情報を説明するための模式図である。
【図１２】同実施形態における動作の一例を説明するための模式図である。
【図１３】同実施形態における認証レベルの管理例を示す模式図である。
【図１４】同実施形態における動作の一例を説明するためのフローチャートである。
【図１５】同実施形態における動作の一例を説明するためのフローチャートである。
【図１６】同実施形態における動作の一例を説明するためのフローチャートである。
【図１７】同実施形態における動作の一例を説明するためのフローチャートである。
【図１８】同実施形態における動作の一例を説明するためのフローチャートである。
【図１９】同実施形態における動作の一例を説明するためのフローチャートである。
【図２０】同実施形態における認証レベル変更時の方針の一例を示す模式図である。

【図２１】同実施形態における認証レベル変更時の方針の一例を示す模式図である。
【発明を実施するための形態】
【００２５】
以下、各実施形態について図面を用いて説明するが、その前に各実施形態の概要を述べる。
【００２６】
第１の実施形態は、ユーザに操作されるユーザ端末に通信可能なサービス提供者装置、ＩＤａａＳ事業者装置及び認証代行装置を備えた認証システムに関する。なお、認証システムは、ユーザに操作されるユーザ端末及び当該ユーザにサービスを提供するためのサービス提供者装置にそれぞれ通信可能なＩＤａａＳ事業者装置及び認証代行装置を備えた構成としてもよい。
【００２７】
サービス提供者装置は、当該サービス提供者装置が提供するサービスのアカウントを識別するサービスアカウント識別子及び第１連携ＩＤを含むサービスアカウント情報を記憶するサービスアカウント情報記憶手段を備えている。
【００２８】
ＩＤａａＳ事業者装置は、ユーザを識別するユーザＩＤに一致するＳＳＯ（シングルサインオン）アカウント識別子、第１連携ＩＤに一致する第１連携ＩＤ及び第１連携ＩＤとは異なる第２連携ＩＤを含むＳＳＯアカウント情報を記憶するＳＳＯアカウント情報記憶手段を備えている。
【００２９】
認証代行装置は、ユーザに対する認証処理のアカウントを識別する認証アカウント識別子、第２連携ＩＤに一致する第２連携ＩＤ及び当該認証処理の方式を示す認証クラスを含む認証アカウント情報を記憶する認証アカウント情報記憶手段を備えている。
【００３０】
ここで、ユーザ端末から送信されたユーザＩＤ及びＳＳＯ要求に基づいて、当該ユーザＩＤに一致するＳＳＯアカウント識別子を含むＳＳＯアカウント情報に第２連携ＩＤを介して関連付けられた認証アカウント情報をもつ認証代行装置は、ユーザ端末を操作するユーザの認証処理を実行する。
【００３１】
認証処理の結果が成功のとき、当該認証処理されたユーザのユーザＩＤに一致するＳＳＯアカウント識別子を含むＳＳＯアカウント情報をもつＩＤｓｓＳ事業者装置は、当該ＳＳＯアカウント情報に第１連携ＩＤを介して関連付けられたサービスアカウント情報に含まれるサービスアカウント識別子で識別されるサービスに対するＳＳＯ認証を許可する。
【００３２】
ＳＳＯ認証が許可されたサービスを提供するサービス提供装置は、ユーザＩＤ及びＳＳＯ要求を送信したユーザ端末に対し、サービスに関する情報を送信する。
【００３３】
以上のような第１の実施形態によれば、各サービス提供者が他のサービス提供者のシステムを監視する必要がなく、運用が容易化し、サービス提供者の利便性が向上する。
【００３４】
また、以上のような認証連携は、ＩＤａａＳ事業者装置に連携した認証代行装置が認証を実行するので、シングルサインオンをユーザが安全に利用することが容易になり、ユーザの利便性が向上する。
【００３５】
また、サービス提供者は、生体認証などの高セキュアな環境を準備する必要が無いため、ユーザに対して提供する認証方法を容易に変更できる。
【００３６】
このように第１の実施形態によれば、ユーザ及びサービス提供者の利便性を向上させつつ、認証方式を容易に変更可能となっている。

【００３７】
また、第１の実施形態においては、認証代行装置は、認証処理の方式を示す認証クラス、及び当該認証処理のレベルを示す認証レベルを関連付けて記述した認証クラス管理テーブルを記憶した第１テーブル記憶手段を備えている。
【００３８】
ＳＳＯアカウント情報記憶手段は、認証レベルを含んでいる。
【００３９】
ここで、認証処理に問題が生じ、当該認証処理のレベルが低下する場合、認証代行装置が、当該認証処理の認証レベルを低下させるように認証クラス管理テーブルを更新し、当該低下させた認証レベルとこの認証レベルに認証アカウント情報内で関連付けられた認証クラスとをＩＤａａＳ事業者装置に送信する。
【００４０】
ＩＤａａＳ事業者装置は、認証代行装置から認証レベルと認証クラスとを受信すると、当該受信した認証クラスに基づいてＳＳＯアカウント情報を検索し、当該検索により得られた認証レベルを、当該受信した認証レベルに低下させるようにＳＳＯアカウント情報を更新する。
【００４１】
従って、第１の実施形態によれば、認証処理に問題が生じ、当該認証処理のレベルが低下する場合に、認証レベルを低下させることができるため、認証処理の信頼性を維持することができる。
【００４２】
次に、第２の実施形態においては、認証代行装置は、認証処理の方式を示す認証クラス、当該認証処理のレベルを示す認証レベル、及び当該認証クラスの認証代行事業者名を含む認証クラスインデックスを関連付けて記述した認証クラス管理テーブルを記憶した第１テーブル記憶手段を備えている。
【００４３】
ＩＤａａＳ事業者装置は、認証レベル及び認証クラスインデックスを関連付けて記述した認証レベル管理テーブルを記憶した第２テーブル記憶手段を備えている。
【００４４】
ここで、認証処理に問題が生じ、当該認証処理のレベルが低下する場合、認証代行装置が、当該認証処理の認証レベルを低下させるように認証クラス管理テーブルを更新し、当該認証クラス管理テーブル内で低下させた認証レベルとこの認証レベルに関連付けた認証クラスインデックスとをＩＤａａＳ事業者装置に送信する。
【００４５】
ＩＤａａＳ事業者装置は、認証代行装置から認証レベルと認証クラスインデックスとを受信すると、当該受信した認証クラスインデックスに基づいて認証レベル管理テーブルを検索し、当該検索により得られた認証レベルを、当該受信した認証レベルに低下させるように認証レベル管理テーブルを更新する。
【００４６】
従って、第２の実施形態によれば、認証処理に問題が生じ、当該認証処理のレベルが低下する場合に、認証レベルを低下させることができるため、認証処理の信頼性を維持することができる。また、第２の実施形態によれば、認証レベルを低下させる際に、ＩＤａａＳ事業者装置は、ユーザＩＤ毎のＳＳＯアカウント情報を更新する必要が無く、認証レベル管理テーブルを更新すればよいので、認証レベルの低下に必要な負荷を大幅に軽減させることができる。
【００４７】
以上が各実施形態の概要である。続いて、各実施形態を具体的に説明する。
【００４８】
＜第１の実施形態＞
図１は第１の実施形態に係る認証システムの構成を示す模式図であり、図２及び図３は

各装置のアカウント情報等を説明するための模式図である。

【００４９】

この認証システムは、ユーザＵに操作されるユーザ端末１０と、サービス提供者装置２０と、ＩＤａａＳ事業者装置３０と、認証代行装置４０とが通信可能となっている。これらのユーザＵ、ユーザ端末１０、サービス提供者装置２０、ＩＤａａＳ事業者装置３０及び認証代行装置４０は、多重に存在するが、図面では１台ずつ示している。また、各装置１０，２０，３０，４０は、それぞれハードウェア構成、又はハードウェア資源とソフトウェアとの組合せ構成のいずれでも実施可能となっている。組合せ構成のソフトウェアとしては、予めネットワーク又は記憶媒体からコンピュータにインストールされ、当該コンピュータのプロセッサに実行されて各装置１０，２０，３０，４０の各機能を実現させるためのプログラムが用いられる。

【００５０】

ユーザＵは、サービスを利用する個人ユーザ又は企業ユーザである。当該図では、ログイン認証することによりサービスを受けるものを前提としている。ユーザＵは、個人／企業／公共等の利用者を表す。

【００５１】

ユーザ端末１０は、例えば、Ｗｅｂブラウザを用いて他の装置２０，３０，４０にアクセス可能な通常のコンピュータ機能を有する端末装置であり、例えば、ノートＰＣ（personal computer）、デスクトップＰＣ又はモバイル端末などの任意の端末装置が使用可能となっている。

【００５２】

ここでは、ユーザ端末１０は、例えば、メモリ１１、Ｗｅｂブラウザ部１２及び認証クライアント部１３を備えている。なお、Ｗｅｂブラウザ部１２は、ユーザ端末１０内のプロセッサ（図示せず）がメモリ１１内のブラウザ用アプリケーションプログラムを実行することにより、実現される機能部である。同様に、認証クライアント部１３は、ユーザ端末１０内のプロセッサ（図示せず）がメモリ１１内の認証用アプリケーションプログラムを実行することにより、実現される機能部である。

【００５３】

サービス提供者装置２０は、サービス提供者に運営される装置であり、公共や企業のサービスサイトがある。サービス提供者装置２０は、ユーザ端末１０から受けた要求に基づいて、サービスを提供する一般的なＷｅｂサービスの提供元である。

【００５４】

ここでは、サービス提供者装置２０は、例えば、メモリ２１及びセキュアなＷｅｂ処理部２２を備えている。Ｗｅｂ処理部２２は、サービス提供者装置２０内のプロセッサ（図示せず）が、メモリ２１内のセキュア処理用アプリケーションプログラムを実行することにより、実現される機能部である。メモリ２１は、図２及び図３に示す如き、サービスアカウント情報ａｃ１等の情報を記憶する記憶装置である。

【００５５】

サービスアカウント情報ａｃ１は、図３に示すように、サービスアカウント識別子及び第１ＩＤａａＳ連携情報を含んでいる。なお、サービスアカウント情報ａｃ１は、サービス履歴などのサービスに関わる属性情報を更に含んでもよい。

【００５６】

サービスアカウント識別子は、サービス提供者によるユーザ毎のサービスのアカウントを識別する識別子である。

【００５７】

第１ＩＤａａＳ連携情報は、連携先のＩＤａａＳ事業者を示す連携先ＩＤａａＳ名と、サービス提供者装置２０とＩＤａａＳ事業者装置３０とが連携のために共有する識別情報である第１連携ＩＤとを含んでいる。

【００５８】

なお、ユーザＵから見たユーザＩＤの管理者はサービス提供者であるが、サービス提供

者はユーザＩＤの管理をＩＤａａＳ事業者にアウトソーシングしている。このため、ユーザＩＤの実体はＩＤａａＳ事業者の管理する領域に存在する。

【００５９】

ＩＤａａＳ事業者装置３０は、サービス提供者からユーザのＩＤ管理を請け負うＩＤａａＳ事業者に運営される装置である。なお、「ＩＤａａＳ事業者」は、「ＩＤプロバイダ」と読み替えてもよい。

【００６０】

ここでは、ＩＤａａＳ事業者装置３０は、図１に示すように、例えば、メモリ３１、認証サービス部３２及びＩＤ管理部３３を備えている。認証サービス部３２は、ＩＤａａＳ事業者装置３０内のプロセッサ（図示せず）が、メモリ３１内の認証サービス用アプリケーションプログラムを実行することにより、実現される機能部である。ＩＤ管理部３３は、ＩＤａａＳ事業者装置３０内のプロセッサ（図示せず）が、メモリ３１内の認証サービス用アプリケーションプログラムを実行することにより、実現される機能部である。ＩＤ管理部３３は、図２及び図３に示す如き、ＳＳＯアカウント情報ａｃ２を作成し、ＩＤとの関連付けを行う。また、ＩＤ管理部３３は、ＳＳＯアカウント情報ａｃ２で認証する方法を設定させることも可能である。メモリ３１は、ＳＳＯ（Single Sign-On）アカウント情報ａｃ２等の情報を記憶する記憶装置である。

【００６１】

ＳＳＯアカウント情報ａｃ２は、図３に示すように、ＳＳＯアカウント識別子、ＳＰ連携情報及びＡＰ連携情報を含んでいる。なお、ＳＳＯアカウント情報ａｃ２は、ＳＳＯアカウント識別子の値としてのユーザＩＤに関連付けられたユーザ管理情報（例、ユーザＵの名前、住所、年齢、メールアドレス、電話番号、パスワードなど）を更に含んでもよい。また、ＳＰはサービス提供者（Service Provider）の略語であり、ＡＰは認証代行事業者（Authentication Provider）の略語である。

【００６２】

ＳＳＯアカウント識別子は、ＩＤａａＳ事業者によるユーザ毎のシングルサインオンのアカウントを識別する識別子であり、値としてユーザＩＤが用いられる。

【００６３】

ＳＰ連携情報は、連携先のサービス提供者を示す連携先ＳＰ名と、連携のためにサービス提供者装置２０と共有する識別情報である第１連携ＩＤとを含んでいる。

【００６４】

ＡＰ連携情報は、連携先の認証代行事業者を示す連携先ＡＰ名と、連携のために認証代行装置４０と共有する識別情報である第２連携ＩＤと、認証代行装置４０による認証処理のレベルを示す認証レベルとを含んでいる。

【００６５】

認証代行装置４０は、ＩＤａａＳ事業者から認証を請け負う認証代行事業者に運営される装置である。例えば、ＩＳＯ／ＩＥＣ ２４７６１に規定されたＡＣＢｉｏ（Authentication Context for Biometrics）技術により、ネットワーク上に生体認証を流さずに本人認証をする認証代行サービスを提供可能となっている。

【００６６】

ここでは、認証代行装置４０は、図１に示すように、例えば、メモリ４１、認証代行部４２及び証明書発行部４３を備えている。認証代行部４２は、認証代行装置４０内のプロセッサ（図示せず）が、メモリ４１内の認証代行用アプリケーションプログラムを実行することにより、実現される機能部である。認証代行部４２は、ここではＡＣＢｉｏ認証を代行する。証明書発行部４３は、認証代行装置４０内のプロセッサ（図示せず）が、メモリ４１内の証明書発行用アプリケーションプログラムを実行することにより、実現される機能部である。証明書発行部４３は、認証代行部４２が検証する時に確認するＢＲＴ証明書（Biometric Reference Template Certificate）を予め発行する。なお、ＢＲＴ証明書は、ＡＣＢｉｏ認証で使用するクライアントから生体認証の結果とともに送付される証明書である。メモリ４１は、図３及び図２に示す如き、認証アカウント情報ａｃ３及び認証

クラス管理テーブルＴ１を記憶する記憶装置である。

【００６７】

認証アカウント情報ａｃ３は、図３に示すように、認証アカウント識別子、第２ＩＤａａＳ連携情報及び認証情報を含んでいる。

【００６８】

認証アカウント識別子は、認証代行事業者によるユーザ毎の認証のアカウントを識別する識別子である。

【００６９】

第２ＩＤａａＳ連携情報は、連携先のＩＤａａＳ事業者を示す連携先ＩＤａａＳ名と、認証代行装置４０とＩＤａａＳ事業者装置３０とが連携のために共有する識別情報である第２連携ＩＤとを含んでいる。

【００７０】

認証情報は、認証代行装置４０による認証処理の実行に必要な情報を特定する認証クラスと、当該認証処理に用いられるユーザ毎のクレデンシャル情報とを含んでいる。

【００７１】

認証クラスは、各ユーザで共通して認証処理の実行に必要な情報を特定する情報であり、例えば、認証処理の方式を含んでいる。例えば、図示した情報“acbio-finger-vein”は、認証処理の方式が、ＡＣＢｉｏ技術の指静脈(finger-vein)認証であることを示している。

【００７２】

クレデンシャル情報は、ユーザ毎に認証処理の実行に必要な情報であり、例えば、ＡＣＢｉｏ技術の場合には、ＢＲＴ証明書又はＢＲＴ証明書の識別情報を含んでいる。なお、ＢＲＴ証明書は、生体参照情報のハッシュ値に対して発行者（例、ＩＤａａＳ事業者又は第三者機関）のデジタル署名を施したデータである。生体参照情報（Biometric Reference Template）は、ユーザの生体認証の真正性の基準となるクレデンシャルである。

【００７３】

認証クラス管理テーブルＴ１は、認証代行装置４０による認証処理のレベルを示す認証レベルと、認証代行装置４０による認証処理の実行に必要な情報を特定する認証クラスとが関連付けられて記述されている。

【００７４】

次に、以上のように構成された認証システムの動作について図４乃至図９を用いて説明する。

【００７５】

始めに、事前準備として、図４に示すように、各アカウント情報ａｃ１～ａｃ３等を保存するステップＳＴ１～ＳＴ４を予め実行しておく。なお、ステップＳＴ２～ＳＴ４は、認証処理の一例であるＡＣＢｉｏ認証に関する処理であり、他の認証処理を用いる場合には適宜、変更される。

【００７６】

ステップＳＴ１では、ＩＤａａＳ事業者装置内のＩＤ管理部３３がＳＳＯアカウント情報ａｃ２を作成し、当該ＳＳＯアカウント情報ａｃ２をメモリ３１に保存する。ＩＤ管理部３３は、ＳＳＯアカウント情報とユーザＩＤとを関連付けている。同様に、ＩＤ管理部３３は、サービスアカウント情報ａｃ１を作成し、当該サービスアカウント情報ａｃ１をメモリ２１に保存する。

【００７７】

ステップＳＴ２では、ＩＤ管理部３３が、認証アカウント情報ａｃ３を作成し、当該認証アカウント情報ａｃ３をメモリ４１に保存する。認証アカウント情報ａｃ３は、ＳＳＯアカウント情報ａｃ２に関連付けられている。

【００７８】

ステップＳＴ３では、ユーザ端末１０内の認証クライアント部１３と、認証代行装置４０内の証明書発行部４３との間でＢＲＴ証明書の発行手続きを実行する。

【００７９】
ステップＳＴ４では、証明書発行部４３から、発行したＢＲＴ証明書を認証アカウント情報ａｃ３に登録する。
【００８０】
事前準備の終了後、以下のステップＳＴ１０～ＳＴ１９に示すように、シングルサインオン（ＳＳＯ）認証が可能となる。
【００８１】
ステップＳＴ１０では、ユーザ端末１０内のＷｅｂブラウザ部１２が、ユーザＩＤ及びＳＳＯ要求をＩＤａａＳ事業者装置３０に送信する。
【００８２】
ステップＳＴ１１では、ＩＤａａＳ事業者装置３０内の認証サービス部３２が、メモリ内のＳＳＯアカウント情報ａｃ２から、シングルサインオンのアカウントや、認証レベルを確認する。
【００８３】
ステップＳＴ１２では、認証サービス部３２が、Ｗｅｂブラウザ部１２に認証用のログイン画面データを送信し、認証情報を要求する。
【００８４】
ステップＳＴ１３では、Ｗｅｂブラウザ部１２が、ＡＣＢｉｏ認証依頼を認証クライアント部１３に送出する。
【００８５】
ステップＳＴ１４では、認証クライアント部１３が、ＡＣＢｉｏ認証要求を認証代行装置４０に送信する。認証代行装置４０内の認証代行部４２は、メモリ４１内の認証アカウント情報ａｃ３に登録されたＢＲＴ証明書から情報を取り出し、ＡＣＢｉｏ認証要求に基づいて、ＡＣＢｉｏ認証を実行する。
【００８６】
このようなステップＳＴ１４においては、ユーザ端末１０から送信されたユーザＩＤ及びＳＳＯ要求に基づいて、当該ユーザＩＤに一致するＳＳＯアカウント識別子を含むＳＳＯアカウント情報に第２連携ＩＤを介して関連付けられた認証アカウント情報ａｃ３をもつ認証代行装置４０が、ユーザ端末１０を操作するユーザの認証処理を実行している。
【００８７】
ステップＳＴ１５では、認証クライアント部１３が、ステップＳＴ１５のＡＣＢｉｏ認証要求の送信後に、Ｗｅｂブラウザ部１２に制御を戻す。
【００８８】
ステップＳＴ１６では、Ｗｅｂブラウザ部１２が、認証結果を認証サービス部３２に送信する。
【００８９】
ステップＳＴ１７では、認証サービス部３２が、認証代行部４２から認証結果を確認する。
【００９０】
ステップＳＴ１８では、認証サービス部３２が、認証結果が正しいことを確認し、ＳＳＯ認証の許可をＷｅｂブラウザ部１２に返信する。
【００９１】
このようなステップＳＴ１８では、認証処理の結果が成功のとき、当該認証処理されたユーザのユーザＩＤに一致するＳＳＯアカウント識別子を含むＳＳＯアカウント情報ａｃ２をもつＩＤｓｓＳ事業者装置３０が、当該ＳＳＯアカウント情報ａｃ２に第１連携ＩＤを介して関連付けられたサービスアカウント情報ａｃ１に含まれるサービスアカウント識別子で識別されるサービスに対するＳＳＯ認証を許可している。
【００９２】
ステップＳＴ１９では、シングルサインオン認証により、Ｗｅｂブラウザ部１２が、ＳＳＯで連携するサービス提供者装置２０へ、シングルサインオンする。

【００９３】
ステップＳＴ１９の後、ＳＳＯ認証が許可されたサービスを提供するサービス提供装置２０は、ステップＳＴ１０でユーザＩＤ及びＳＳＯ要求を送信したユーザ端末１０に対し、サービスに関する情報を送信する。
【００９４】
図５は、サービス提供者が、ＩＤａａＳ事業者へＩＤのアウトソースおよび、ＳＳＯの対応を要求した場合の業務シーケンスの一例を示すシーケンス図である。この業務シーケンスは、オンライン、オフライン又はその両者を混在させた形態のいずれとしても実現可能となっている。
【００９５】
ステップＳＴ２０では、サービス提供者装置が、ＩＤのアウトソースの業務を依頼（打診）するＩＤアウトソース要求をＩＤａａＳ事業者装置に送信する。
【００９６】
ステップＳＴ２１では、ＩＤａａＳ事業者装置が、このＩＤアウトソース要求に応じて、ＩＤａａＳサービスの内容、価格等を示す利用メニューをサービス提供者装置２０に送信する。
【００９７】
ステップＳＴ２２では、サービス提供者装置２０が、この利用メニューからサービス提供者が選択したＩＤａａＳサービスをＩＤａａＳ事業者に通知する。
【００９８】
ステップＳＴ２３では、通知されたＩＤａａＳサービスに相当する認証代行サービスの利用申請を認証代行装置４０に送信する。
【００９９】
ステップＳＴ２４では、認証代行装置４０が、この利用申請に基づき、ＩＤａａＳ事業者装置３０に対して契約を締結する処理を実行する。
【０１００】
ステップＳＴ２５では、ＩＤａａＳ事業者装置３０が、ステップＳＴ２４の処理に基づき、サービス提供者装置２０に対して、契約を締結する処理を実行する。
【０１０１】
ステップＳＴ２６では、サービス提供者装置２０が、ＳＳＯサービスの利用開始をユーザ端末１０に通知する。この通知は、例えば、ＳＳＯ可能なサービスと、ＳＳＯの認証方法とを含んでいる。
【０１０２】
ステップＳＴ２７では、ユーザ端末１０が、ステップＳＴ２６の通知から選択したＳＳＯ可能なサービスと、当該選択した認証方法とを含むＳＳＯ利用申請をサービス提供者装置２０に送信する。
【０１０３】
ステップＳＴ２８では、サービス提供者装置２０が、このＳＳＯ利用申請をＩＤａａＳ事業者装置３０に送信する。
【０１０４】
ステップＳＴ２９では、ＩＤａａＳ事業者装置３０が、このＳＳＯ利用申請に基づいて、認証を代行する認証代行申請を認証代行装置４０に送信する。
【０１０５】
図６は、サービス提供者が、ＩＤａａＳ事業者へＩＤのアウトソースおよび、ＳＳＯの対応を要求した場合の業務シーケンスの一例を示す模式図である。この業務シーケンスは、オンライン、オフライン又はその両者を混在させた形態のいずれとしても実現可能となっている。
【０１０６】
ステップＳＴ３０では、サービス提供者装置２０が、サービス利用料を請求するサービス利用料請求をユーザ端末１０に送信する。このサービス利用料請求は、ステップＳＴ２

７のＳＳＯ利用申請などで申請したサービスの利用料金を含めた費用（サービス利用料）を請求する請求書データである。

【０１０７】

ステップＳＴ３１では、ユーザ端末１０のユーザが、このサービス利用料請求に基づいてサービス利用料をサービス提供者に支払う。支払い方法としては、例えば、銀行引き落としなどの如き、任意の支払い方法が適用可能となっている。

【０１０８】

ステップＳＴ３２では、ＩＤａａＳ事業者装置３０が、ユーザＩＤの管理料を含む費用（ＩＤ管理費）を請求するＩＤ管理費請求をサービス提供者装置２０に送信する。

【０１０９】

ステップＳＴ３３では、サービス提供者装置２０を運営するサービス提供者が、このＩＤ管理費請求に基づいて、ＩＤ管理費をＩＤａａＳ事業者に支払う。

【０１１０】

ステップＳＴ３４では、認証代行装置４０が、認証代行サービスの利用料を含む費用（認証代行料）を請求する認証代行料請求をＩＤａａＳ事業者装置３０に送信する。

【０１１１】

ステップＳＴ３５では、ＩＤａａＳ事業者装置３０を運営するＩＤａａＳ事業者が、この認証代行料請求に基づいて、認証代行料を認証代行事業者に支払う。

【０１１２】

図７及び図８は、ユーザが、サービス提供者のＷｅｂサイトにログインを要求してから、ログインするまでの動作の一例を説明するためのフローチャートである。この例では、サービス提供者は、ＩＤａａＳ事業者にＩＤ管理をアウトソーシングする、ＩＤａａＳ事業者は、認証代行事業者を用いる。また、認証代行事業者は、生体情報をネットワーク上に流さないオンライン認証ＡＣＢｉｏを用いることを前提としている。

【０１１３】

ステップＳＴ４１では、ユーザ端末１０が、ユーザＵの操作に応じて、Ｗｅｂサイトへ接続するＷｅｂ接続を要求する。

【０１１４】

ステップＳＴ４２では、ステップＳＴ４１で動作するＷｅｂアプリケーションが、Ｗｅｂサイトに接続するユーザＩＤと、接続要求とをＩＤａａＳ事業者装置３０に送信する。なお、接続要求は、ＳＳＯ要求と読み替えてもよい。

【０１１５】

ステップＳＴ４３では、ＩＤａａＳ事業者装置３０が、ユーザＩＤ及び接続要求を受信する。

【０１１６】

ステップＳＴ４４では、ＩＤａａＳ事業者装置３０が、接続要求を受信すると、メモリ３１からＳＳＯアカウント情報ａｃ２を読み出す。

【０１１７】

ステップＳＴ４５では、ＩＤａａＳ事業者装置３０が、当該読み出したＳＳＯアカウント情報に基づいて、ステップＳＴ４３で受信したユーザＩＤが正であるか否を判定するＩＤ認証を実行する。

【０１１８】

ステップＳＴ４６では、ステップＳＴ４５の判定の結果、否の場合、ＩＤａａＳ事業者装置３０が、エラー処理を実行する。

【０１１９】

ステップＳＴ４７では、ステップＳＴ４５の判定の結果、正の場合、ＩＤａａＳ事業者装置３０が、ＳＳＯアカウント情報ａｃ２に基づいて、当該ユーザＩＤが示すユーザが、オンライン生体認証の対象であるか否かを判定する。この例では、当該ユーザがオンライン生体認証の対象であるとする。そのため、ステップＳＴ４７の判定結果が否の場合については、記載を省略する。

【０１２０】
ステップＳＴ４８では、ＩＤａａＳ事業者装置３０が、オンライン生体認証要求及びＳＳＯアカウント情報ａｃ２を認証代行装置４０に送信する。
【０１２１】
このようなステップＳＴ４３～ＳＴ４８においては、ＩＤａａＳ事業者装置３０が、ユーザ端末１０から送信されたユーザＩＤ及びＳＳＯ要求に基づいて、当該ユーザＩＤに一致するＳＳＯアカウント識別子を含むＳＳＯアカウント情報ａｃ２に第２連携ＩＤを介して関連付けられた認証アカウント情報ａｃ３をもつ認証代行装置４０に認証要求を送信するステップを実行している。
【０１２２】
ステップＳＴ４９では、認証代行装置４０が、このオンライン生体認証要求及びアカウントを受信する。
【０１２３】
ステップＳＴ５０では、認証代行装置４０が、このＳＳＯアカウント情報ａｃ２に基づいて、メモリ４１からＡＰアカウント情報ａｃ３を読み出す。
【０１２４】
ステップＳＴ５１では、認証代行装置４０が、ステップＳＴ５０でＡＰアカウント情報ａｃ３が確認された後、ＡＣＢｉｏ認証に必要なチャレンジコードを生成する。
【０１２５】
ステップＳＴ５２では、認証代行装置４０が、このチャレンジコードと共に、ＡＣＢｉｏの認証要求をユーザ端末１０に送信する。
【０１２６】
ステップＳＴ５３では、ユーザ端末１０が、チャレンジコード及び認証要求を受信する。
【０１２７】
ステップＳＴ５４では、ユーザ端末１０が、認証クライアント部１３として搭載されている生体認証連携のＡＣＢｉｏアプリケーションプログラムにより、ＡＣＢｉｏインスタンスを生成する。ＡＣＢｉｏインスタンスは、生体認証の結果情報、チャレンジコード及びＢＲＴ証明書等を含んでいる。
【０１２８】
ステップＳＴ５５では、ユーザ端末１０が、当該生成されたＡＣＢｉｏインスタンスを認証代行装置４０に送信する。
【０１２９】
ステップＳＴ５６では、認証代行装置４０が、このＡＣＢｉｏインスタンスを受信する。
【０１３０】
ステップＳＴ５７では、認証代行装置４０が、当該受信されたＡＣＢｉｏインスタンスを検証する。ここでは、例えば、ＡＣＢｉｏインスタンスに含まれる生体認証の結果情報、チャレンジコード及びＢＲＴ証明書等が検証される。
【０１３１】
ステップＳＴ５８では、認証代行装置４０が、ＡＣＢｉｏインスタンスの検証結果と、ステップＳＴ４９で受信したＳＳＯアカウント情報ａｃ２とをＩＤａａＳ事業者装置３０に送信する。
【０１３２】
このようなステップＳＴ４９～ＳＴ５２，ＳＴ５６～ＳＴ５８においては、認証代行装置４０が、ＩＤａａＳ事業者装置３０から受けた認証要求に基づいて、ユーザ端末１０を操作するユーザの認証処理を実行し、当該認証処理の結果をＩＤａａＳ事業者装置３０に送信するステップを実行している。
【０１３３】
ステップＳＴ５９では、ＩＤａａＳ事業者装置３０が、認証代行装置４０からＡＣＢｉ

ｏインスタンスの検証結果と、ＳＳＯアカウント情報ａｃ２とを受信する。
【０１３４】
ステップＳＴ６０では、ＩＤａａＳ事業者装置３０が、ＡＣＢｉｏの認証結果が成功か否かを判定する。
【０１３５】
ステップＳＴ６１では、ステップＳＴ６０の判定の結果、否の場合、ＩＤａａＳ事業者装置３０が、エラー処理を実行する。
【０１３６】
ステップＳＴ６２では、ステップＳＴ６０の判定の結果、成功の場合、ＩＤａａＳ事業者装置３０が、ステップＳＴ５９で受信したＳＳＯアカウント情報ａｃ２からユーザＩＤを抽出し、当該ユーザＩＤ及び認証成功を示す認証情報をサービス提供者装置２０に通知する。
【０１３７】
このようなステップＳＴ５９～ＳＴ６２においては、ＩＤａａＳ事業者装置３０が、認証処理の結果が成功のとき、当該認証処理されたユーザのユーザＩＤに一致するＳＳＯアカウント識別子を含むＳＳＯアカウント情報ａｃ２に第１連携ＩＤを介して関連付けられたサービスアカウント情報ａｃ３に含まれるサービスアカウント識別子で識別されるサービスに対するＳＳＯ認証を許可し、当該許可をサービス提供者装置２０に送信するステップを実行している。
【０１３８】
ステップＳＴ６３では、サービス提供者装置２０が、ユーザＩＤ及び認証情報を受信し、ユーザＩＤに基づく認証を許可する。
【０１３９】
ステップＳＴ６４では、サービス提供者装置２０が、ステップＳＴ４３で受信したユーザＩＤ及び接続要求に基づいて、Ｗｅｂページへの接続及び表示をそれぞれ許可する。
【０１４０】
このようなステップＳＴ６３～ＳＴ６４においては、サービス提供者装置２０が、ステップＳＴ４２でユーザＩＤ及びＳＳＯ要求を送信したユーザ端末１０に対し、ＳＳＯ認証が許可されたサービスに関する情報を送信するステップを実行している。
【０１４１】
ステップＳＴ６５では、ユーザ端末１０が、ログインの成功により、接続できるＷｅｂページを表示する。
【０１４２】
次に、脆弱性報告など外部要因により、認証代行プロバイダの管理者が特定の認証方式のレベルを変更する場合について説明する。なお、認証代行装置４０は、認証処理の方式を示す認証クラス、及び当該認証処理のレベルを示す認証レベルを関連付けて記述した認証クラス管理テーブルＴ１をメモリ４１に記憶している。また、ＳＳＯアカウント情報ａｃ２は、認証レベルを含んでいる。
【０１４３】
認証処理に問題が生じ、当該認証処理のレベルが低下する場合、認証代行装置４０が、当該認証処理の認証レベルを低下させるように認証クラス管理テーブルＴ１を更新し、当該低下させた認証レベルとこの認証レベルに認証アカウント情報ａｃ３内で関連付けられた認証クラスとをＩＤａａＳ事業者装置３０に送信する。
【０１４４】
ＩＤａａＳ事業者装置３０は、認証代行装置４０から認証レベルと認証クラスとを受信すると、当該受信した認証クラスに基づいてＳＳＯアカウント情報ａｃ２を検索し、当該検索により得られた認証レベルを、当該受信した認証レベルに低下させるようにＳＳＯアカウント情報ａｃ２を更新する。
【０１４５】
例えば図９に示すように、認証クラス管理テーブルＴ１内の認証クラス“acbio-finger

-vein”の認証レベル“LEVEL 4”を“LEVEL 3”に変更する場合、認証代行装置４０は、変更後の認証レベル“LEVEL 3”及び連携ＩＤ“f7asiiu218j8”を含む認証レベル変更通知をＩＤａａＳ事業者装置３０に送信する。

【０１４６】

ＩＤａａＳ事業者装置３０は、この認証レベル変更通知に基づいて、ユーザＩＤ毎のＳＳＯアカウント情報ａｃ２に含まれるＡＰ連携情報内の認証レベル“LEVEL 4”を“LEVEL 3”に変更する。

【０１４７】

上述したように第１の実施形態によれば、ユーザ端末１０から送信されたユーザＩＤ及びＳＳＯ要求に基づいて、当該ユーザＩＤに一致するＳＳＯアカウント識別子を含むＳＳＯアカウント情報ａｃ２に第２連携ＩＤを介して関連付けられた認証アカウント情報ａｃ３をもつ認証代行装置４０は、ユーザ端末１０を操作するユーザの認証処理を実行する。

【０１４８】

認証処理の結果が成功のとき、当該認証処理されたユーザのユーザＩＤに一致するＳＳＯアカウント識別子を含むＳＳＯアカウント情報ａｃ２をもつＩＤｓｓＳ事業者装置３０は、当該ＳＳＯアカウント情報ａｃ２に第１連携ＩＤを介して関連付けられたサービスアカウント情報ａｃ３に含まれるサービスアカウント識別子で識別されるサービスに対するＳＳＯ認証を許可する。

【０１４９】

ＳＳＯ認証が許可されたサービスを提供するサービス提供装置２０は、ユーザＩＤ及びＳＳＯ要求を送信したユーザ端末１０に対し、サービスに関する情報を送信する。

【０１５０】

第１の実施形態は、このような構成により、ユーザ及びサービス提供者の利便性を向上させつつ、認証方式を容易に変更可能となっている。

【０１５１】

また、第１の実施形態によれば、認証処理に問題が生じ、当該認証処理のレベルが低下する場合、認証代行装置４０が、当該認証処理の認証レベルを低下させるように認証クラス管理テーブルＴ１を更新し、当該低下させた認証レベルとこの認証レベルに認証アカウント情報ａｃ３内で関連付けられた認証クラスとをＩＤａａＳ事業者装置３０に送信する。また、ＩＤａａＳ事業者装置３０が、認証代行装置４０から認証レベルと認証クラスとを受信すると、当該受信した認証クラスに基づいてＳＳＯアカウント情報ａｃ２を検索し、当該検索により得られた認証レベルを、当該受信した認証レベルに低下させるようにＳＳＯアカウント情報ａｃ２を更新する。第１の実施形態は、このような構成により、認証処理に問題が生じ、当該認証処理のレベルが低下する場合に、認証レベルを低下させることができるため、認証処理の信頼性を維持することができる。

【０１５２】

以上のような第１の実施形態の効果について補足的に説明する。

【０１５３】

本実施形態では、ＩＤａａＳ事業者に対して、認証サービスを認証代行したことにより、ＩＤａａＳにて、オプションとして認証方式をサービス提供者のユーザが選択することができる。

【０１５４】

これにより、当初の目的であるユーザおよびサービス提供者の利便性を向上し、ユーザ、サービス提供者に、セキュリティサービスの選択の自由度をもたせることができる。

【０１５５】

また、ＩＤａａＳはＩＤを管理、認証代行は認証のみでＩＤを管理しないという方法で疎結合することにより、認証の管理・運用方法をシンプルにする。

【０１５６】

また、本実施形態では、認証サービスをＩＤａａＳと切り離すことにより、以下の効果（ａ）～（ｄ）を得ることができる。

【０１５７】
（ａ）サービス提供者に対する効果
サービス提供者は、ＩＤ管理をＩＤａａＳ事業者にアウトソーシングすることにより、運用面で以下のような効果を得ることができる。
【０１５８】
すなわち、サービス提供者は、ＩＤプロバイダや他のサービス提供者と信頼関係を結んでユーザ情報を連携、管理する必要がない。
【０１５９】
また、サービス提供者は、ＩＤ管理の状況についてタイムリな監視が不要である。
【０１６０】
これは、一般に信頼関係を結んでいるシステムが複数になると個々に、設定が必要となりシステムや運用の複雑さが増すが、システムや運用を含めた複雑な管理をアウトソースできるためである。
【０１６１】
また、サービス提供者は、ＩＤ管理をアウトソーシングしたことにより、自社のＩＤ管理による、ＩＤ情報の漏えいリスクを無くすことができる。
【０１６２】
また、サービス提供者は、ＩＤａａＳ事業者がオプション提供する認証方法を選択することができる。ここで、サービス提供者は、自社で準備するには多大な準備や運用検討が必要な生体認証を簡単に導入することができる。サービス提供者は、自社でセキュアな管理環境を整える必要がない。
【０１６３】
また、サービス提供者は、生体認証を導入した場合、ユーザの認証情報忘れにより、サービス利用の機会を損失することを低減することができる。
【０１６４】
また、サービス提供者は、自サービスではセキュリティの高い認証が必要なユーザが一部の場合でも、ＳＳＯ認証においてＩＤａａＳを利用する他のサービス提供者のユーザ全体の数が多い場合に、セキュリティの高い認証（生体認証等）をユーザに提供することができる。
【０１６５】
（ｂ）ＩＤａａＳ事業者に対する効果
ＩＤａａＳ事業者は、認証代行サービスを認証代行事業者にアウトソーシングすることにより、サービス提供者及びユーザに対し、利用サービスを向上させる効果を得ることができる。
【０１６６】
ＩＤａａＳ事業者は、認証方式をアウトソースすることにより、ＩＤに対する認証方法の選択肢を増やすとともに、疎結合により切り離しを可能とすることで、ユーザおよびサービス提供者の要求に応じたよりセキュアな認証方法を選定することができる。同様に、ＩＤａａＳ事業者は、セキュリティ効果の高い認証方式に迅速に対応していくことが可能になる。
【０１６７】
ＩＤａａＳ事業者は、生体認証などのように、認証方式や管理の難易度の高い管理方法を用いるリソースについても自ら準備するのではなく、すでに完成しているリソースを利用できる。
【０１６８】
ＩＤａａＳ事業者は、複数のサービス提供者からの要求で認証を実施するので、小規模なサービス提供者のグループに対しても高セキュリティなサービスを提供することができる。
【０１６９】
（ｃ）認証代行事業者に対する効果

認証代行事業者は、ＩＤａａＳ事業者の認証代行サービスをすることにより、専門性に特化したセキュアな認証を提供する効果を得ることができる。

【０１７０】

また、認証代行事業者は、ＩＤに付随するユーザ情報については、ＩＤａａＳ事業者がもつため管理する必要がない。

【０１７１】

認証代行事業者は、サービス提供者だけでなく、ＩＤａａＳから不特定多数の希望者に対して、認証代行サービスを提供できる。

【０１７２】

（ｄ）ユーザに対する効果

ユーザは、以下のように、利便性が向上する効果を得ることができる。すなわち、ユーザは、ＩＤａａＳが提供する認証サービスを利用することができる。また、ユーザは、セキュアにしたい場合に、生体認証を利用する等、選択肢が増える。更に、ユーザは、ＩＤａａＳを利用してシングルサインオン（ＳＳＯ）することで、サービス提供者毎に登録するユーザＩＤを個々に覚える必要がない。

【０１７３】

＜第２の実施形態＞

次に、第２の実施形態に係る認証システムについて図１を参照しながら説明する。

【０１７４】

第２の実施形態は、第１の実施形態の変形例であり、認証レベルの変更に要する負荷を軽減する形態となっている。

【０１７５】

例えば、第１の実施形態では、認証レベルを変更する場合、全てのユーザのＳＳＯアカウント情報ａｃ２の属性（サポート認証レベル）を変更しなくてはならない。このため、第１の実施形態は、アカウント数が大きくなると、認証レベルの変更による負荷が大きい。

【０１７６】

これに対し、第２の実施形態では、図１０に示すように、ＩＤａａＳ事業者装置３０が、認証レベルと、認証クラスインデックスとを関連付けて記述した認証レベル管理テーブルＴ２をメモリ３１に記憶している。ここで、認証クラスインデックスは、認証代行事業者名（ＡＰ名）と認証クラスとを表現するインデックスである。

【０１７７】

また、認証代行装置４０は、認証処理の方式を示す認証クラス、当該認証処理のレベルを示す認証レベル、及び当該認証クラスの認証代行事業者名を含む認証クラスインデックスを関連付けて記述した認証クラス管理テーブルＴ１をメモリ４１に記憶している。

【０１７８】

これに伴い、図１１に示すように、ＩＤａａＳ事業者装置３０が管理するＳＳＯアカウント情報ａｃ２では、ＡＰ連携情報が認証レベルに代えて、認証クラスインデックスを含む構成となっている。

【０１７９】

このような第２の実施形態では、図１２に示すように、認証レベルを変更する場合、両テーブルＴ１，Ｔ２を書き換えればよく、ＳＳＯアカウント情報ａｃ２の書き換えが不要である。

【０１８０】

詳しくは、認証処理に問題が生じ、当該認証処理のレベルが低下する場合、認証代行装置４０が、当該認証処理の認証レベルを低下させるように認証クラス管理テーブルＴ１を更新し、当該認証クラス管理テーブルＴ１内で低下させた認証レベルとこの認証レベルに関連付けた認証クラスインデックスとをＩＤａａＳ事業者装置３０に送信する。

【０１８１】

ＩＤａａＳ事業者装置３０は、認証代行装置４０から認証レベルと認証クラスインデッ

クスとを受信すると、当該受信した認証クラスインデックスに基づいて認証レベル管理テーブルＴ２を検索し、当該検索により得られた認証レベルを、当該受信した認証レベルに低下させるように認証レベル管理テーブルＴ２を更新する。

【０１８２】

このようにして、両テーブルＴ１，Ｔ２の書き換えが実行される。なお、両テーブルＴ１，Ｔ２の書き換えは、ＩＤａａＳ事業者装置３０が認証レベル管理テーブルＴ２を書き換えた後、認証代行装置４０が認証クラス管理テーブルＴ１を書き換えるように変形してもよい。後述するステップＳＴ９１－３では、この変形例について述べる。

【０１８３】

認証処理は、第１の実施形態と同様に実行される。

【０１８４】

次に、以上のように構成された認証システムの動作について説明する。

【０１８５】

図１３は、ＩＤａａＳ事業者による認証レベルの管理例を示す模式図である。

【０１８６】

ユーザ端末１０、サービス提供者装置２０、ＩＤａａＳ事業者装置３０及び認証代行装置４０は複数存在するが、図１３中においては、説明を簡潔にする観点から、各装置１０～４０が１台ずつ記載されている。

【０１８７】

図１３に示す例の場合、ユーザＵ１，Ｕ２は、ＳＳＯ認証を利用したいサービス毎に、所望の認証レベルをもっている。

【０１８８】

ユーザ端末１０は、ユーザＵ１，Ｕ２の操作に応じて、サービス提供者装置２０から提供されるサービスの認証レベルを自由に選択できる。

【０１８９】

サービス提供者装置２０は、サービス毎に、提供可能な認証レベルをユーザに提示できる。また、サービス提供者装置２０は、サービス毎に、提示する認証レベルに合わせた認証レベルをＩＤａａＳ事業者装置３０から選択、決定できる。

【０１９０】

ＩＤａａＳ事業者装置３０では、認証代行装置４０により代行可能な認証処理における複数の認証レベルをサービス提供者装置２０に提示できる。

【０１９１】

ＩＤａａＳ事業者装置３０では、ユーザＩＤ毎に、サービス提供装置３０のサービスと、認証クラスインデックスとを管理できる。ＩＤａａＳ事業者装置３０では、認証レベル管理テーブルＴ２により、認証レベルと、認証クラスインデックスとを関連付けて管理できる。

【０１９２】

認証代行装置４０では、認証クラス管理テーブルＴ１により、認証レベルと、認証クラスと、認証クラスインデックスとを関連付けて管理できる。

【０１９３】

このため、ＩＤａａＳ事業者装置３０で統合管理されている範囲で、ユーザ端末１０を利用するユーザＵ１，Ｕ２は、ＳＳＯ認証により、サービス毎のＩＤを意識することがない。

【０１９４】

また、ネットワーク上で問題が発生した場合、両テーブルＴ１，Ｔ２内の認証レベルを下げることにより、サービス提供者装置２０へのアクセスを制限できる。問題が解決した場合には、両テーブルＴ１，Ｔ２内の認証レベルを上げることができる。

【０１９５】

認証代行装置４０による認証を一時的に停止する等の緊急措置も可能となる。

【０１９６】

ＩＤａａＳ事業者装置３０は、サービス提供者装置２０やユーザ端末１０に提供する認証処理を実行する認証装置として、認証代行装置４０を利用できる。そのため、ＩＤａａＳ事業者装置３０は、生体認証などの環境を自己で構築する必要がない。

【０１９７】

認証代行装置４０は、代行する認証毎に、認証レベルをもっている。

【０１９８】

認証代行装置４０は、ユーザＩＤ及びユーザ情報を管理しない。

【０１９９】

全ての装置１０～４０は、多重化し、疎結合で認証される。

【０２００】

図１４は、ＩＤａａＳ事業者装置３０によるＳＳＯ連携の動作の一例を説明するためのフローチャートである。図１４左方のステップＳＴ７１～ＳＴ７５は、既存のＳＳＯ連携の動作を示している。

【０２０１】

ステップＳＴ７１では、ＳＳＯを作成する。

【０２０２】

ステップＳＴ７２では、ＳＳＯを連携する。

【０２０３】

ステップＳＴ７３では、ＳＳＯを利用する。

【０２０４】

ステップＳＴ７４では、ＳＳＯの連携を解除する。

【０２０５】

ステップＳＴ７５では、ＳＳＯを削除する。

【０２０６】

図１４右方のステップＳＴ８１～ＳＴ９４は、本実施形態におけるＳＳＯ連携の動作の一例を示している。

【０２０７】

ステップＳＴ８１では、ＩＤａａＳ事業者が、ＳＳＯの認定レベルを選定する。

【０２０８】

ステップＳＴ８２は、ＩＤａａＳ事業者装置３０が、ＳＳＯ連携先の確定（審査）をする。

【０２０９】

ステップＳＴ８３では、認証システムがＳＳＯを作成する。

【０２１０】

ステップＳＴ８４では、認証システムがＳＳＯを連携する。

【０２１１】

ステップＳＴ８５では、ユーザが，初回に接続するＳＰ（サービス提供者）を利用する。なお、２回目に接続するＳＰを利用する場合には、ステップ８５ではなく、ステップＳＴ８８に進む。

【０２１２】

ステップＳＴ８６では、ユーザが初回はＳＳＯ以外で、ＳＰサイトの認証をうける。

【０２１３】

ステップＳＴ８７では、ユーザがＳＰで認証された場合、ＳＳＯの利用を開始する。

【０２１４】

ステップＳＴ８９では、ユーザがＳＳＯを利用する。

【０２１５】

ステップＳＴ９０では、認証方式に問題が発生したことにより、認証方式のレベルが下がったとＩＤａａＳ事業者に判定される。

【０２１６】

ステップＳＴ９１では、ＩＤａａＳ事業者装置３０及び認証代行装置４０が、認証レベ

ルを下げる。
【０２１７】
ステップＳＴ９２では、認証方式の問題が解決したことにより、ＩＤａａＳ事業者装置３０及び認証代行装置４０が、認証方式のレベルを復旧させ、認証レベルを元に戻す。
【０２１８】
ステップＳＴ９３では、認証システムがＳＳＯを解除する。
【０２１９】
ステップＳＴ９４では、認証システムがＳＳＯを削除する。
【０２２０】
次に、以上のような本実施形態におけるステップＳＴ８１～ＳＴ９２について、図１５～図１９のフローチャートを用いて説明する。なお、図１５及び図１６はステップＳＴ８１～ＳＴ８４の説明に用い、図１７はステップＳＴ８５～ＳＴ８７，ＳＴ８９の説明に用いる。図１８はステップＳＴ８８～ＳＴ８９の説明に用い、図１９はステップＳＴ９０～ＳＴ９２の説明に用いる。
【０２２１】
ステップＳＴ８１－１では、ＩＤａａＳ事業者が、ＳＰ向けＳＳＯ認証のオプションサービス（通常のパスワード以外に、ワンタイムパスワード（ＯＴＰ）、生体認証、生体認証＋ＡＣＢｉｏ等）を選定する。このとき、ＩＤａａＳ事業者は認証レベルを確定し、当該認証レベルを認証レベル管理テーブルＴ１に登録する。
【０２２２】
ステップＳＴ８２－１では、ＩＤａａＳ事業者装置３０が、ＩＤａａＳ事業者が連携を希望するサービス提供者に関して、ＳＰ向けＳＳＯ連携を招待（募集）する。
【０２２３】
ステップＳＴ８２－２では、サービス提供者装置２０が、ＳＳＯの連携要求をＩＤａａＳ事業者装置３０に送信する。
【０２２４】
ステップＳＴ８２－３では、ＩＤａａＳ事業者装置３０が、このＳＳＯの連携要求を受け付ける。
【０２２５】
ステップＳＴ８２－４では、ＩＤａａＳ事業者装置３０が、ＳＳＯの連携要求を受け付けた結果をサービス提供者装置２０に回答する。ＩＤａａＳ事業者装置３０は、ＳＳＯで連携するＳＰ間の安全性のために、連携先を精査する。
【０２２６】
ステップＳＴ８２－５では、サービス提供者装置２０が、ＳＳＯの連携要求の結果を受け取る。
【０２２７】
ステップＳＴ８２－６では、ＩＤａａＳ事業者装置３０が、ＳＰ連携情報をメモリ３１へ登録する。
【０２２８】
ステップＳＴ８２－７では、ＩＤａａＳ事業者装置３０が、ユーザ向けにＳＳＯサービス開始の連絡、広告処理を実行する。
【０２２９】
ステップＳＴ８３－１では、ユーザ端末１０が、ユーザの操作に応じて、ＩＤａａＳ事業者装置３０にＳＳＯのＩＤ登録依頼を送信する。ＩＤａａＳ事業者のＩＤや元のＩＤを利用することも運用として可能である。
【０２３０】
ステップＳＴ８３－２では、ＩＤａａＳ事業者装置３０が、このＳＳＯのＩＤ登録依頼を受け付け、新規ＩＤを登録する。
【０２３１】
ステップＳＴ８３－３では、ＩＤａａＳ事業者装置３０が、認証方法をユーザに確認す

るためのメニュー情報をユーザ端末１０に送信する。
【０２３２】
ステップＳＴ８３－４では、ユーザ端末１０が、ユーザの操作に応じて、このメニュー情報から、認証方法を選び、指定する。当該例では、ユーザは、ＩＤａａＳ事業者装置３０の提供する認証代行装置４０の提供するＡＣＢｉｏ認証を選択、指定する。
【０２３３】
ステップＳＴ８３－５では、ＩＤａａＳ事業者装置３０が、ユーザ端末１０から認証方法を受け付ける。
【０２３４】
ステップＳＴ８３－６では、当該受け付けた認証方法が認証代行装置４０を利用する場合、ＩＤａａＳ事業者装置３０が、認証代行装置４０に認証利用申請を送信する。
【０２３５】
※ＩＤａａＳ事業者装置３０は、認証代行装置４０に向けたＳＳＯに紐づくアカウントを合わせて発行して渡す。
【０２３６】
ステップＳＴ８３－７では、認証代行装置４０が、ＩＤａａＳ事業者装置３０から受けたアカウント情報により、認証情報の登録要求をユーザ端末１０に送信する。この認証情報の登録要求は、チャレンジコードを含んでいる。
【０２３７】
ステップＳＴ８３－８では、ユーザ端末１０が、この認証情報の登録要求に基づいて、ユーザの生体情報を採取し、当該生体情報のハッシュ値と、登録要求内のチャレンジコードとを含むＡＣＢｉｏインスタンスを生成する。また、ユーザ端末１０は、生成したＡＣＢｉｏインスタンスを認証代行装置４０に送信する。
【０２３８】
ステップＳＴ８３－９では、認証代行装置４０が、このＡＣＢインスタンスに基づいて、ＡＣＢｉｏのＢＲＴ証明書を発行し、当該ＢＲＴ証明書をユーザ端末１０に送信する。
【０２３９】
ステップＳＴ８３－１０では、ユーザ端末１０が、このＢＲＴ証明書を含む認証情報を登録し、登録完了通知を認証代行装置４０に送信する。
【０２４０】
ステップＳＴ８３－１１では、認証代行装置４０が、この登録完了通知を受け付ける。
ステップＳＴ８３－１２では、認証代行装置４０が、ＢＲＴ証明書を含む認証情報を登録し、アカウントと連携する。アカウントの連携確認後、認証代行装置４０は、認証登録の結果をＩＤａａＳ事業者装置３０に送信する。この例では、認証登録の結果が正常であるとする。なお、異常の場合には、例えば、ステップＳＴ８３－７～ＳＴ８３－１１の処理を再試行すればよい。
【０２４１】
ステップＳＴ８３－１３では、ＩＤａａＳ事業者装置３０が、認証登録の結果を受け付け、認証の利用申請が受付けられたことを確認し、ＳＳＯ　ＩＤの登録完了をユーザ端末１０に通知する。
【０２４２】
ステップＳＴ８３－１４では、ユーザ端末１０が、このＳＳＯ　ＩＤの登録完了の通知を受け付ける。
【０２４３】
ステップＳＴ８４－１では、ＩＤａａＳ事業者装置３０が、メモリ３１にＳＳＯ　ＩＤの情報を登録し、該当するユーザのユーザ管理情報を更新する。
【０２４４】
ステップＳＴ８５－１では、ユーザ端末１０が、ユーザの操作に応じて、ＳＳＯ　ＩＤを用いてログインする。
【０２４５】

ステップＳＴ８５－２では、ＩＤａａＳ事業者装置３０が、ユーザ端末１０から受けたＳＳＯ　ＩＤを認証する。

【０２４６】

ステップＳＴ８５－３では、ＩＤａａＳ事業者装置３０が、パスワード認証要求又はＡＣＢｉｏ認証要求を認証代行装置４０に送信する。ここでは、オンライン生体認証ＡＣＢｉｏの認証要求を送信する場合を例に挙げて述べる。

【０２４７】

ステップＳＴ８５－４では、認証代行装置４０が、この認証要求を受け付ける。

【０２４８】

ステップＳＴ８５－５では、認証代行装置４０が、当該受け付けた認証要求に基づいて、ユーザ端末１０に認証要求を送信する。

【０２４９】

ステップＳＴ８５－６では、ユーザ端末１０が、この認証要求を受信する。

【０２５０】

ステップＳＴ８５－７では、ユーザ端末１０が、当該受信した認証要求に応じて、ユーザの生体認証を実行し、認証結果を含むＡＣＢｉｏインスタンスを生成する。

【０２５１】

ステップＳＴ８５－８では、当該生成したＡＣＢｉｏインスタンスを認証代行装置４０に送信する。

【０２５２】

ステップＳＴ８５－９では、認証代行装置４０が、ＡＣＢｉｏインスタンスを受信する。

【０２５３】

ステップＳＴ８５－１０では、認証代行装置４０が、このＡＣＢｉｏインスタンスの内容を検証し、検証結果をＩＤａａＳ事業者装置３０に送信する。

【０２５４】

ステップＳＴ８５－１１では、ＩＤａａＳ事業者装置３０が、認証代行装置４０から検証結果を受信する。

【０２５５】

ステップＳＴ８６－１では、ＩＤａａＳ事業者装置３０が、ＳＳＯで初回時にサービス提供者装置２０に接続する場合の初回認証要求をサービス提供者装置２０に送信する。

【０２５６】

ステップＳＴ８６－２では、サービス提供者装置２０が、この初回認証要求に基づいて、ＳＳＯによるサービス提供者装置２０への初回接続であることを示す情報を含む初回の認証要求をユーザ端末１０に送信する。

【０２５７】

ステップＳＴ８６－３では、ユーザ端末１０が、サービス提供者装置２０から初回の認証要求を受信する。

【０２５８】

ステップＳＴ８６－４では、ユーザ端末１０が、サービス提供者装置２０への認証情報の入力をユーザに促し、入力された認証情報をサービス提供者装置２０に送信する。

【０２５９】

ステップＳＴ８６－５では、サービス提供者装置２０が、ステップＳＴ８６－２の認証要求に対する応答として、認証情報をユーザ端末１０から受信する。

【０２６０】

ステップＳＴ８６－６では、サービス提供者装置２０が、当該受信した認証情報を検証する。この例では、検証が成功したとする。

【０２６１】

ステップＳＴ８７－１では、サービス提供者装置２０が、初回の認証が成功したことを示す検証結果をＩＤａａＳ事業者装置３０に送信する。

【０２６２】
ステップＳＴ８７－２では、ＩＤａａＳ事業者装置３０が、サービス提供者装置２０から検証結果を受信する。
【０２６３】
ステップＳＴ８７－３では、ＩＤａａＳ事業者装置３０が、当該受信した検証結果に基づいて、メモリ３１内のＳＳＯアカウント情報及びユーザ管理情報を更新する。
【０２６４】
ステップＳＴ８９－１では、ステップＳＴ８６－６の検証の完了後、サービス提供者装置２０が、ユーザへのサービスの提供を開始する。
【０２６５】
ステップＳＴ８９－２では、ユーザ端末１０が、サービス提供者装置２０からサービスの提供が開始され、継続操作が許可される。
【０２６６】
図１８は、ＳＳＯで２回目以降にサービス提供者装置２０に接続する場合の流れを示す模式図である。
【０２６７】
ステップＳＴ８８－１～ＳＴ８８－１０の処理は、前述したステップＳＴ８５－１～ＳＴ８５－１０と同様に実行される。なお、ステップＳＴ８８－１０では、認証代行装置４０が、このＡＣＢｉｏインスタンスの内容を検証し、検証結果をＩＤａａＳ事業者装置３０に送信する。
【０２６８】
ステップＳＴ８８－１１ａでは、ＩＤａａＳ事業者装置３０が、認証代行装置４０から検証結果を受信し、ステップＳＴ８８－１０の検証の完了をサービス提供者装置２０に送信する。
【０２６９】
ステップＳＴ８９－１ａでは、ステップＳＴ８８－１０の検証の完了後、サービス提供者装置２０が、ユーザへのサービスの提供を開始する。
【０２７０】
ステップＳＴ８９－２では、ユーザ端末１０が、サービス提供者装置２０からサービスの提供が開始され、継続操作が許可される。
【０２７１】
図１９は、ＩＤａａＳの認証レベルをダウンする動作と、認証レベルを復旧する動作とを説明するためのフローチャートである。
【０２７２】
ステップＳＴ９０－１では、ＩＤａａＳ事業者が、外部要因による問題認知を受け付ける。
【０２７３】
ステップＳＴ９１－１では、ＩＤａａＳ事業者がセキュリティの状況を確認し、ＩＤａａＳ事業者装置３０を操作する。ＩＤａａＳ事業者装置３０は、ＩＤａａＳ事業者の操作に応じて、認証レベルをダウンする通知を認証代行装置４０に送信する。
【０２７４】
ステップＳＴ９１－２では、認証代行装置４０が認証レベルをダウンする通知を表示し、認証代行事業者に状況の確認を促す。認証代行事業者は、この状況を確認し、認証レベルをダウンすることを確認する。なお、ステップＳＴ９１－１～ＳＴ９１－２の処理は、予め定められた操作により実行される。
【０２７５】
ステップＳＴ９１－３では、ＩＤａａＳ事業者装置３０が、認証代行装置４０の対象の認証クラスに対応する認証クラス管理テーブルＴ１内の認証レベルを下げる。また、ＩＤａａＳ事業者装置３０は、対象の認証クラスに対応する認証レベル管理テーブルＴ２内の認証レベルを下げる。この例では、認証レベル“LEVEL2”を“LEVEL1”に低下させる。ま

た、ＩＤａａＳ事業者装置３０は、認証レベルを変更（ダウン）したことを示す認証レベル変更通知をサービス提供者装置２０に送信する。

【０２７６】

このようなステップＳＴ９１－３においては、認証処理に問題が生じ、当該認証処理のレベルが低下する場合、ＩＤａａＳ事業者装置３０が、当該認証処理の認証レベルを低下させるように認証レベル管理テーブルＴ２を更新し、当該認証レベル管理テーブルＴ２内で低下させた認証レベルとこの認証レベルに関連付けた認証クラスインデックスとを認証代行装置４０に送信する。

【０２７７】

認証代行装置４０は、ＩＤａａＳ事業者装置３０から認証レベルと認証クラスインデックスとを受信すると、当該受信した認証クラスインデックスに基づいて認証クラス管理テーブルＴ１を検索し、当該検索により得られた認証レベルを、当該受信した認証レベルに低下させるように認証クラス管理テーブルＴ１を更新している。

【０２７８】

また、ＩＤａａＳ事業者装置３０は、認証レベル変更通知をサービス提供者装置２０に送信している。

【０２７９】

ステップＳＴ９１－４では、サービス提供者装置２０が、認証レベル変更通知を受け付ける。この認証レベル変更通知は、例えば、図示しないサービス提供者端末に送信され、当該サービス提供者端末から表示出力される。

【０２８０】

ステップＳＴ９１－５では、サービス提供者は、この認証レベル変更通知を視認し、例えば図２０に示す方針ｐ１に沿って、対策処置の手続きを進める。

【０２８１】

ステップＳＴ９１－５の後、認証レベルをダウンさせた問題が解消され、セキュリティ状況が復旧したとする。

【０２８２】

ステップＳＴ９２－１では、ＩＤａａＳ事業者が、外部要因による問題復旧を受け付ける。

【０２８３】

ステップＳＴ９２－２では、ＩＤａａＳ事業者がセキュリティの状況を確認し、ＩＤａａＳ事業者装置３０を操作する。ＩＤａａＳ事業者装置３０は、ＩＤａａＳ事業者の操作に応じて、認証レベルを復旧させる通知を認証代行装置４０に送信する。

【０２８４】

ステップＳＴ９２－３では、認証代行装置４０が認証レベルを復旧する通知を表示し、認証代行事業者に状況の確認を促す。認証代行事業者は、この状況を確認し、認証レベルを復旧させることを確認する。なお、ステップＳＴ９２－２～ＳＴ９２－３の処理は、予め定められた操作により実行される。

【０２８５】

ステップＳＴ９２－４では、ＩＤａａＳ事業者装置３０が、認証代行装置４０の対象の認証クラスに対応する認証クラス管理テーブルＴ１内の認証レベルを元に戻す（復旧させる）。また、ＩＤａａＳ事業者装置３０は、対象の認証クラスに対応する認証レベル管理テーブルＴ２内の認証レベルを元に戻す（復旧させる）。この例では、認証レベル“LEVEL1”を“LEVEL2”に戻す。また、ＩＤａａＳ事業者装置３０は、認証レベルを復旧（変更）したことを示す認証レベル復旧通知をサービス提供者装置２０に送信する。

【０２８６】

ステップＳＴ９２－５では、サービス提供者装置２０が、認証レベル復旧通知を受け付ける。この認証レベル復旧通知は、例えば、図示しないサービス提供者端末に送信され、当該サービス提供者端末から表示出力される。

【０２８７】

ステップＳＴ９２－６では、サービス提供者は、この認証レベル復旧通知を視認し、例えば図２１に示す方針ｐ２に沿って、復旧処置の手続きを進める。

【０２８８】

上述したように第２の実施形態によれば、認証処理に問題が生じ、当該認証処理のレベルが低下する場合、認証代行装置４０が、当該認証処理の認証レベルを低下させるように認証クラス管理テーブルＴ１を更新し、当該低下させた認証レベルとこの認証レベルに関連付けた認証クラスインデックスとをＩＤａａＳ事業者装置３０に送信する。

【０２８９】

ＩＤａａＳ事業者装置３０は、認証代行装置４０から認証レベルと認証クラスインデックスとを受信すると、当該受信した認証クラスインデックスに基づいて認証レベル管理テーブルＴ１を検索し、当該検索により得られた認証レベルを、当該受信した認証レベルに低下させるように認証レベル管理テーブルＴ１を更新する。

【０２９０】

第２の実施形態は、このような構成により、第１の実施形態の効果に加え、認証レベルを低下させる際に、ＩＤａａＳ事業者装置３０が、ユーザＩＤ毎のＳＳＯアカウント情報を更新する必要が無く、認証レベル管理テーブルＴ２を更新すればよいので、認証レベルの低下に必要な負荷を大幅に軽減させることができる。

【０２９１】

以上説明した少なくとも一つの実施形態によれば、各アカウント情報ａｃ１～ａｃ３内の各連携ＩＤを介してサービス提供者装置２０、ＩＤａａＳ事業者装置３０及び認証代行装置４０を連携させた構成により、ユーザ及びサービス提供者の利便性を向上させつつ、認証方式を容易に変更可能となっている。

【０２９２】

なお、上記の各実施形態に記載した手法は、コンピュータに実行させることのできるプログラムとして、磁気ディスク（フロッピー（登録商標）ディスク、ハードディスクなど）、光ディスク（ＣＤ－ＲＯＭ、ＤＶＤなど）、光磁気ディスク（ＭＯ）、半導体メモリなどの記憶媒体に格納して頒布することもできる。

【０２９３】

また、この記憶媒体としては、プログラムを記憶でき、かつコンピュータが読み取り可能な記憶媒体であれば、その記憶形式は何れの形態であっても良い。

【０２９４】

また、記憶媒体からコンピュータにインストールされたプログラムの指示に基づきコンピュータ上で稼働しているＯＳ（オペレーティングシステム）や、データベース管理ソフト、ネットワークソフト等のＭＷ（ミドルウェア）等が上記実施形態を実現するための各処理の一部を実行しても良い。

【０２９５】

さらに、各実施形態における記憶媒体は、コンピュータと独立した媒体に限らず、ＬＡＮやインターネット等により伝送されたプログラムをダウンロードして記憶又は一時記憶した記憶媒体も含まれる。

【０２９６】

また、記憶媒体は１つに限らず、複数の媒体から上記の各実施形態における処理が実行される場合も本発明における記憶媒体に含まれ、媒体構成は何れの構成であっても良い。

【０２９７】

なお、各実施形態におけるコンピュータは、記憶媒体に記憶されたプログラムに基づき、上記の各実施形態における各処理を実行するものであって、パソコン等の１つからなる装置、複数の装置がネットワーク接続されたシステム等の何れの構成であっても良い。

【０２９８】

また、各実施形態におけるコンピュータとは、パソコンに限らず、情報処理機器に含まれる演算処理装置、マイコン等も含み、プログラムによって本発明の機能を実現することが可能な機器、装置を総称している。

【０２９９】

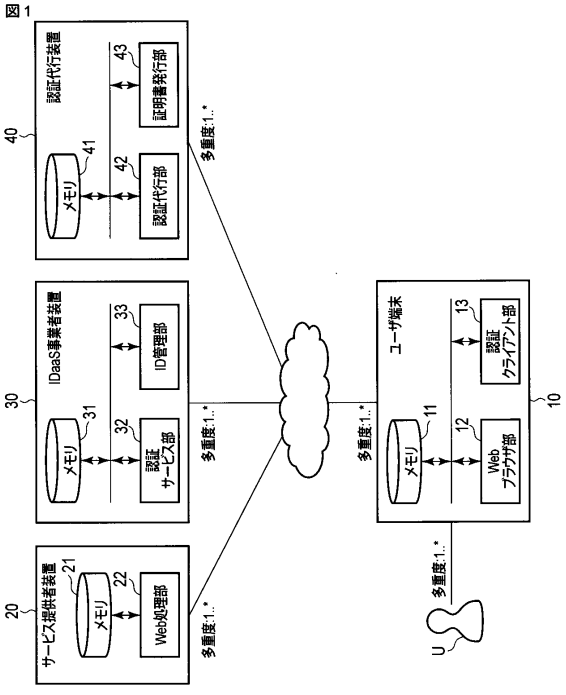
なお、本発明のいくつかの実施形態を説明したが、これらの実施形態は、例として提示したものであり、発明の範囲を限定することは意図していない。これら新規な実施形態は、その他の様々な形態で実施されることが可能であり、発明の要旨を逸脱しない範囲で、種々の省略、置き換え、変更を行うことができる。これら実施形態やその変形は、発明の範囲や要旨に含まれるとともに、特許請求の範囲に記載された発明とその均等の範囲に含まれる。

【符号の説明】

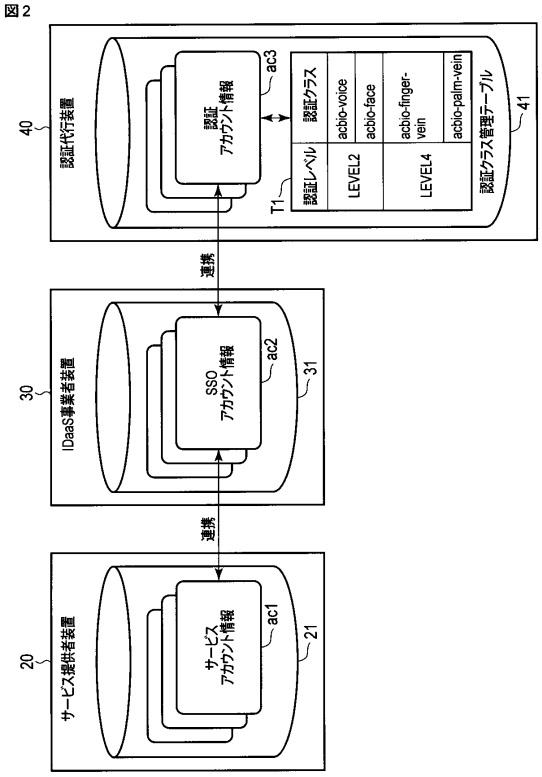
【０３００】

１０…ユーザ端末、１１，２１，３１，４１…メモリ、１２…Ｗｅｂブラウザ部、１３…認証クライアント部、２０…サービス提供者装置、２２…Ｗｅｂ処理部、３０…ＩＤａａＳ事業者装置、３２…認証サービス部、３３…ＩＤ管理部、４０…認証代行装置、４２…認証代行部、４３…証明書発行部、ａｃ１…サービスアカウント情報、ａｃ２…ＳＳＯアカウント情報、ａｃ３…認証アカウント情報、Ｔ１…認証クラス管理テーブル、Ｔ２…認証レベル管理テーブル。

【図１】



【図２】



【図３】

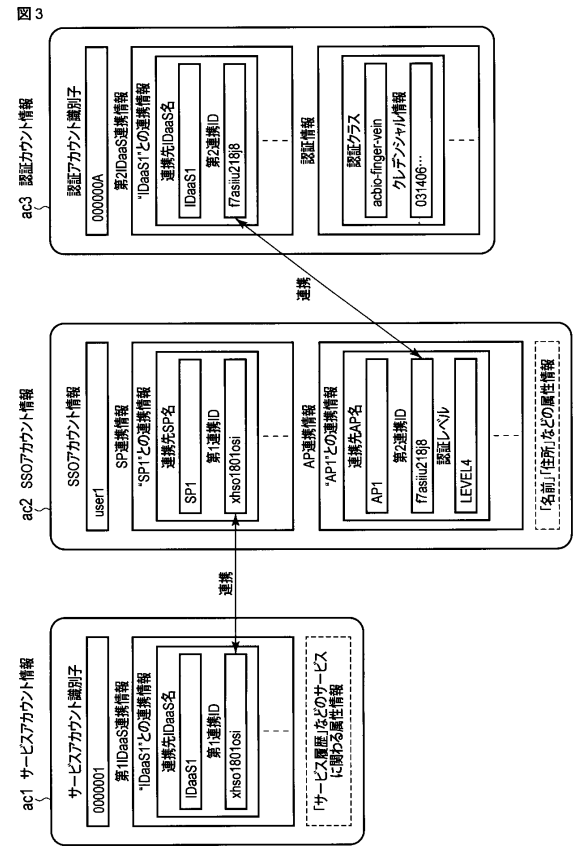


図3
ac3 認証アカウント情報
認証アカウント識別子
0000000A
第2IDaaS連携情報
"IDaaS1"との連携情報
連携先IDaaS名
IDaaS1
第2連携ID
f7asiiu218j8
認証情報
認証クラス
acbio-finger-vein
クレデンシャル情報
031406…
連携
ac2 SSOアカウント情報
SSOアカウント情報
user1
SP連携情報
"SP1"との連携情報
連携先SP名
SP1
第1連携ID
xhso1801osi
AP連携情報
"AP1"との連携情報
連携先AP名
AP1
第2連携ID
f7asiiu218j8
認証レベル
LEVEL4
「名前」「住所」などの属性情報
連携
ac1 サービスアカウント情報
サービスアカウント識別子
0000001
第1IDaaS連携情報
"IDaaS1"との連携情報
連携先IDaaS名
IDaaS1
第1連携ID
xhso1801osi
「サービス履歴」などのサービスに関わる属性情報

【図４】

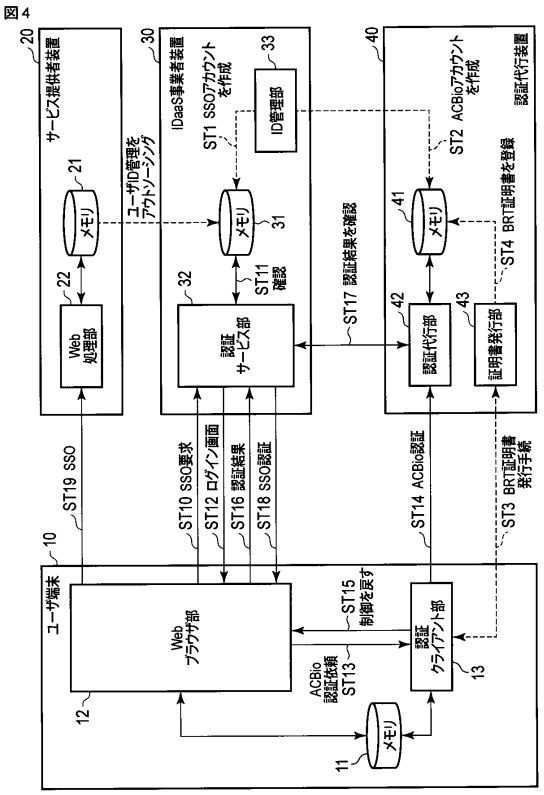


図4
20 サービス提供装置
21 メモリ
22 Web処理部
30 IDaaS事業者装置
ST1 SSOアカウントを作成
33 ID管理部
31 メモリ
32 認証サービス部
ST11 確認
40 認証代行装置
41 メモリ
ST2 ACBioアカウントを作成
42 認証代行部
43 証明書発行部
ST4 BRT証明書を登録
ユーザのID管理をアウトソーシング
ST17 認証結果を確認
ST19 SSO
ST10 SSO要求
ST12 ログイン画面
ST16 認証結果
ST18 SSO認証
ST14 ACBio認証
ST3 BRT証明書発行手続
10 ユーザ端末
Webブラウザ部
12
ST15 制御を戻す
ACBio認証依頼 ST13
認証クライアント部
13
11 メモリ

【図５】

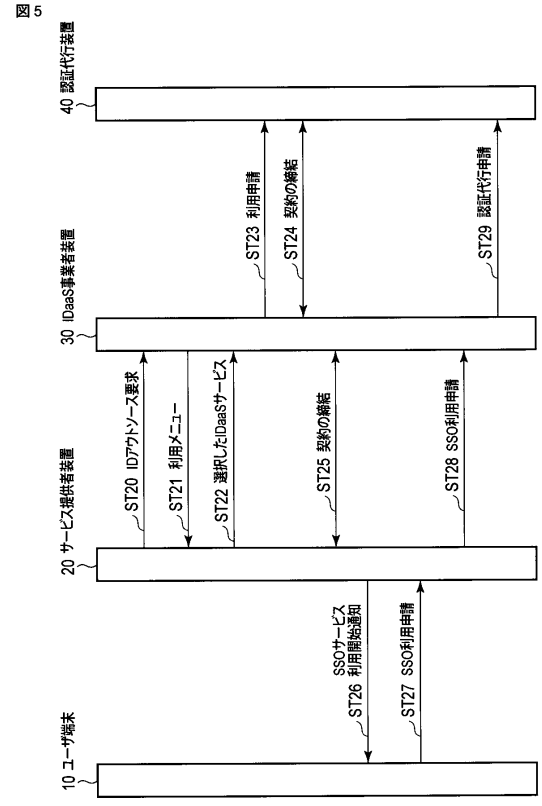


図5
40 認証代行装置
30 IDaaS事業者装置
20 サービス提供装置
10 ユーザ端末
ST20 IDアウトソース要求
ST21 利用メニュー
ST22 選択したIDaaSサービス
ST23 利用申請
ST24 契約の締結
ST25 契約の締結
ST26 SSOサービス利用開始通知
ST27 SSO利用申請
ST28 SSO利用申請
ST29 認証代行申請

【図６】

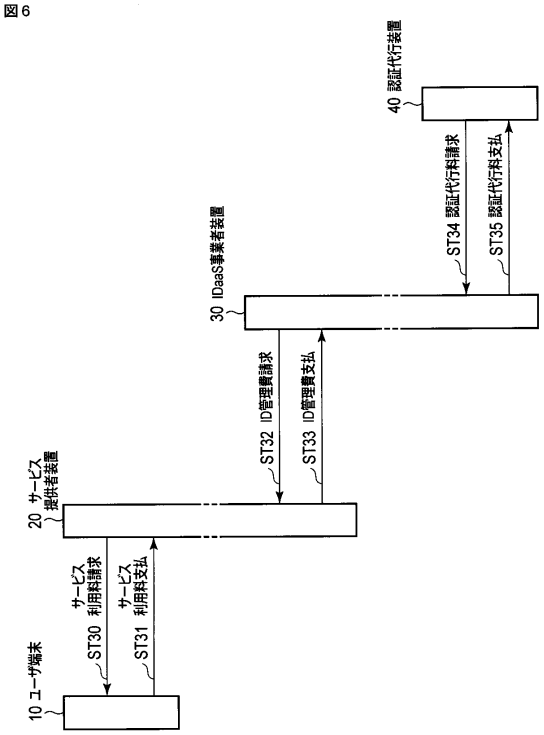


図6
40 認証代行装置
30 IDaaS事業者装置
20 サービス提供装置
10 ユーザ端末
ST30 サービス利用料請求
ST31 サービス利用料支払
ST32 ID管理費請求
ST33 ID管理費支払
ST34 認証代行料請求
ST35 認証代行料支払

【図７】

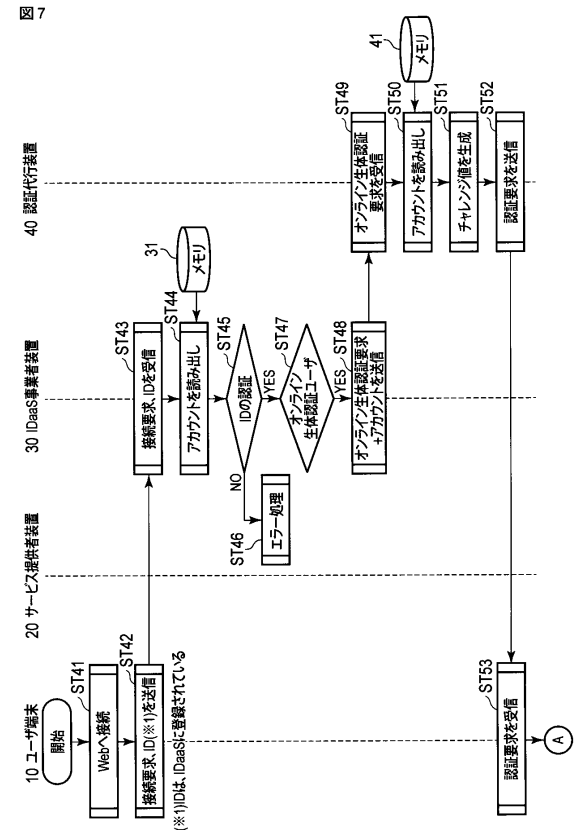


図7
10 ユーザ端末
20 サービス提供者装置
30 IDaaS事業者装置
40 認証代行装置
開始
Webへ接続
接続要求、ID(※1)を送信
(※1)IDは、IDaaSに登録されている
接続要求、IDを受信
アカウントを読み出し
IDの認証
NO
エラー処理
YES
オンライン生体認証ユーザ
YES
オンライン生体認証要求+アカウントを送信
オンライン生体認証要求を受信
アカウントを読み出し
チャレンジ値を生成
認証要求を送信
認証要求を受信
メモリ
ST41
ST42
ST43
ST44
ST45
ST46
ST47
ST48
ST49
ST50
ST51
ST52
ST53
31
41

【図８】

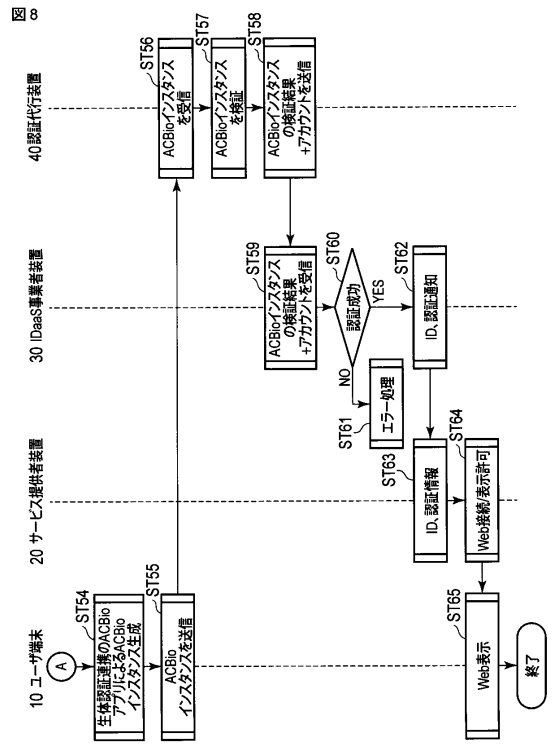


図8
10 ユーザ端末
20 サービス提供者装置
30 IDaaS事業者装置
40 認証代行装置
生体認証連携のACBioアプリによるACBioインスタンス生成
ACBioインスタンスを送信
ACBioインスタンスを受信
ACBioインスタンスを検証
ACBioインスタンスの検証結果+アカウントを送信
ACBioインスタンスの検証結果+アカウントを受信
認証成功
NO
YES
エラー処理
ID、認証通知
ID、認証情報
Web接続(表示許可)
Web表示
終了
ST54
ST55
ST56
ST57
ST58
ST59
ST60
ST61
ST62
ST63
ST64
ST65

【図９】

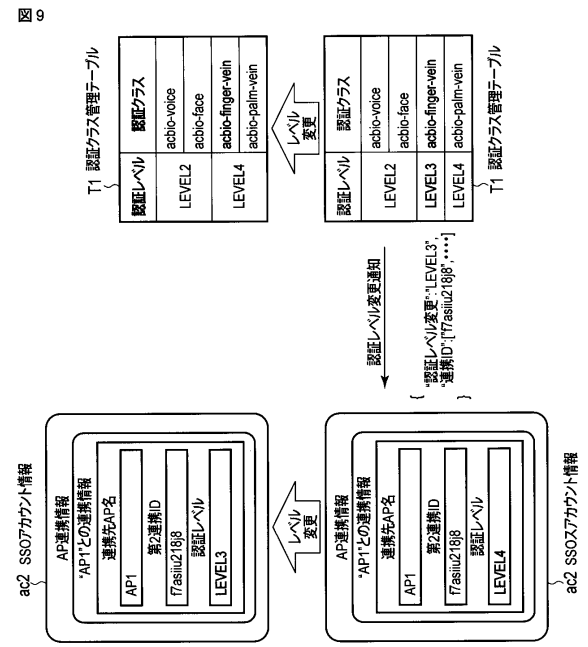


図9
T1 認証クラス管理テーブル
認証レベル
認証クラス
LEVEL2
acbio-voice
acbio-face
LEVEL4
acbio-finger-vein
acbio-palm-vein
レベル変更
LEVEL3
認証レベル変更通知
{
"認証レベル変更":"LEVEL3",
"連携ID":[f7asiiu218j8",・・・]
}
ac2 SSOアカウント情報
AP連携情報
"AP1"との連携情報
連携先AP名
AP1
第2連携ID
f7asiiu218j8
認証レベル

【図１０】

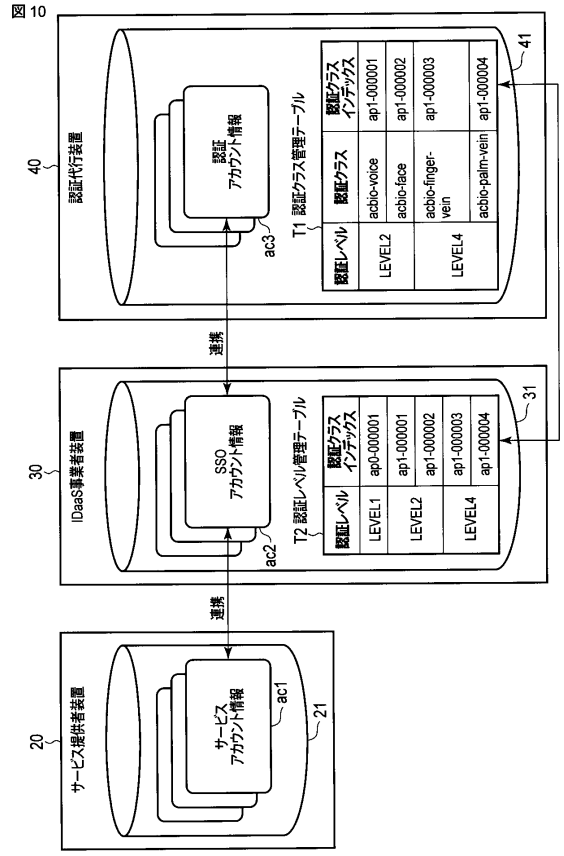
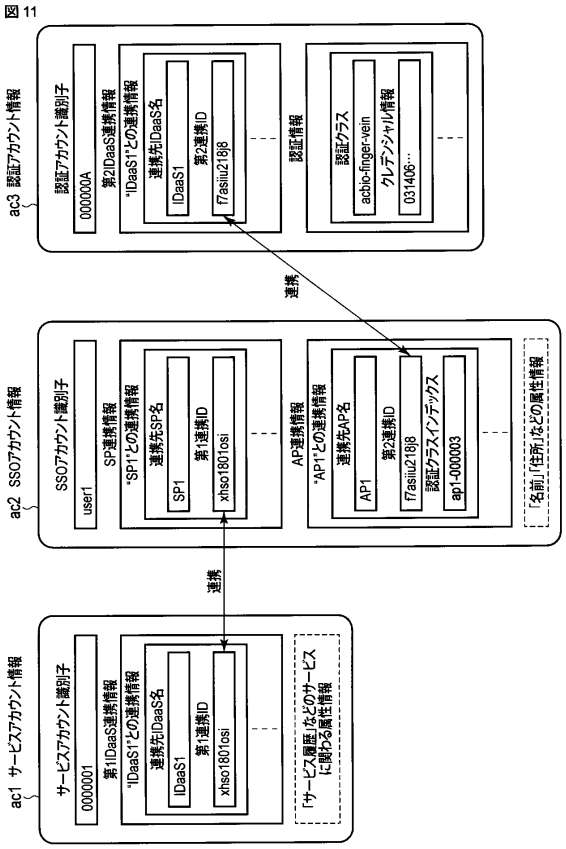
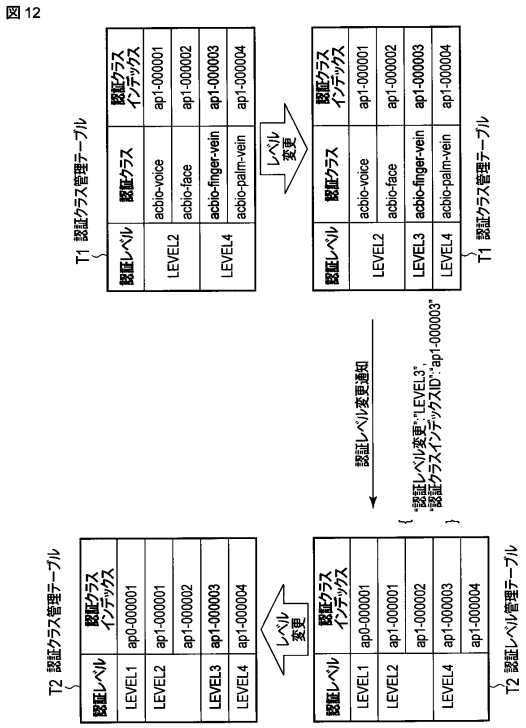


図10
20
サービス提供者装置
サービス
アカウント情報
ac1
21
連携
30
IDaaS事業者装置
SSO
アカウント情報
ac2
T2 認証レベル管理テーブル
認証レベル
認証クラス
インデックス
LEVEL1
ap0-000001
LEVEL2
ap1-000001
ap1-000002
LEVEL4
ap1-000003
ap1-000004
31
40
認証代行装置
認証
アカウント情報
ac3
T1 認証クラス管理テーブル
認証レベル
認証クラス
インデックス
LEVEL2
acbio-voice
ap1-000001
acbio-face
ap1-000002
LEVEL4
acbio-finger-vein
ap1-000003
acbio-palm-vein
ap1-000004
41

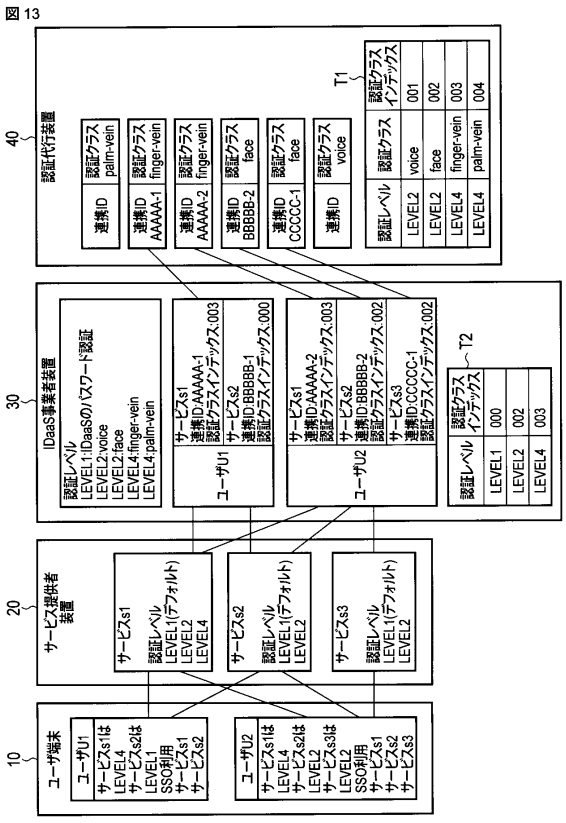
【図１１】



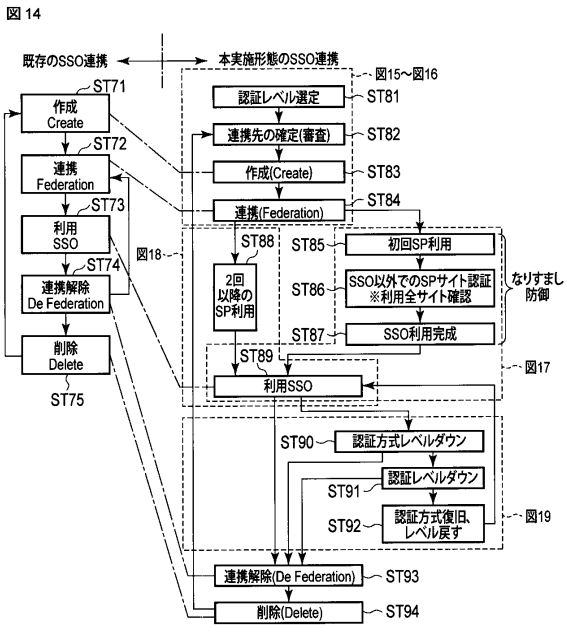
【図１２】



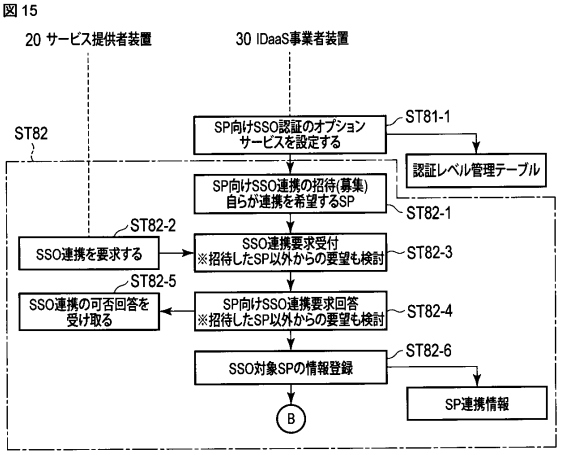
【図１３】



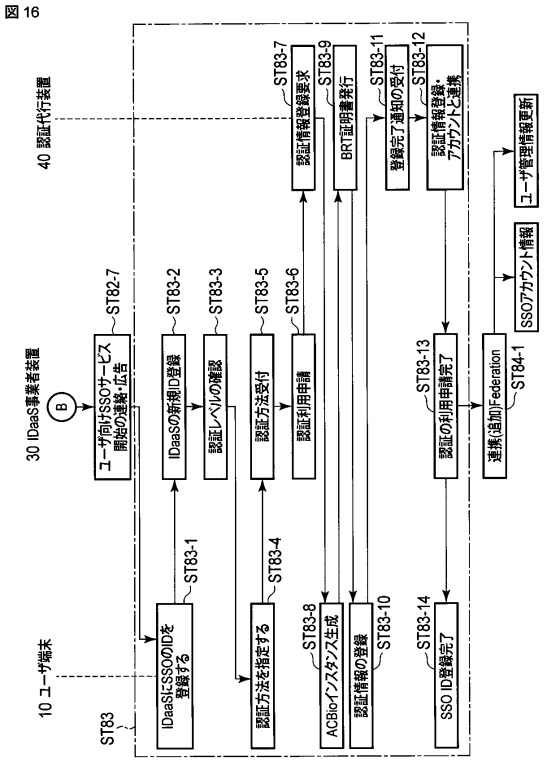
【図１４】



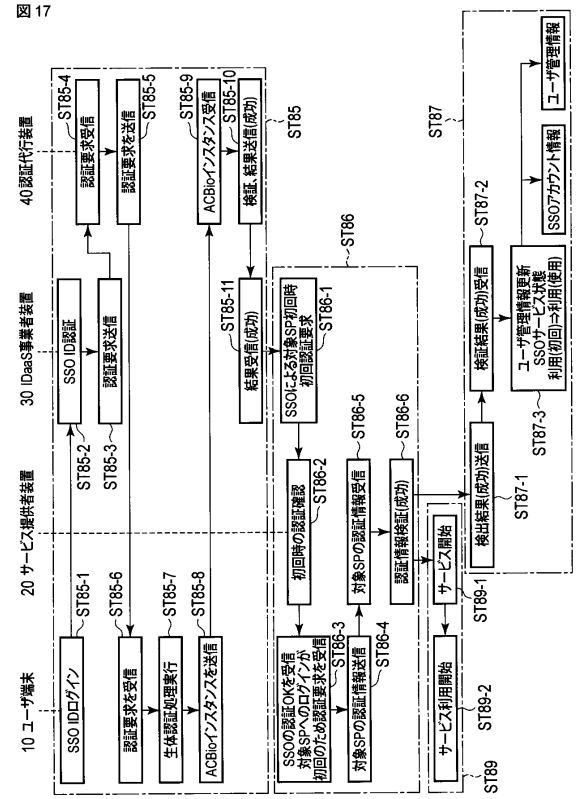
【図１５】



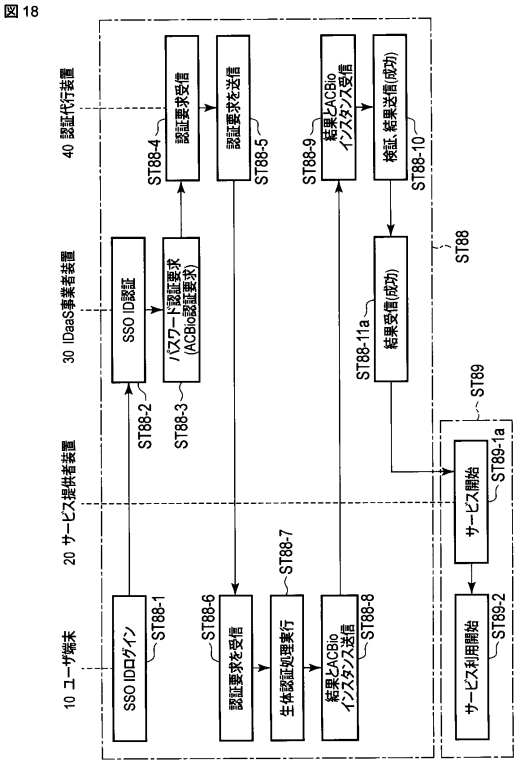
【図１６】



【図１７】

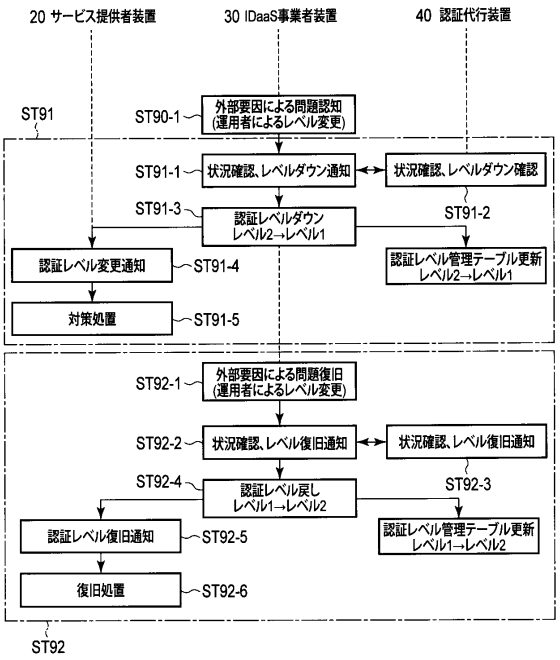


【図１８】



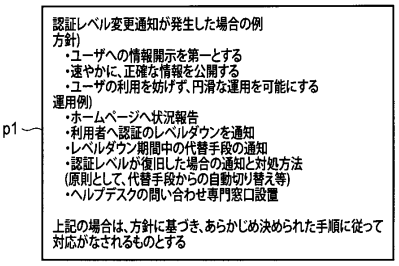
【図１９】

図19



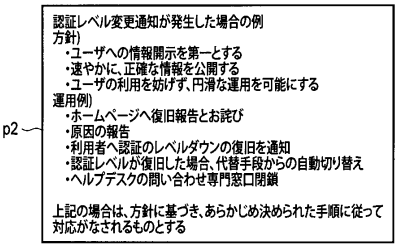
【図２０】

図20



【図２１】

図21



フロントページの続き

(74)代理人 100153051
弁理士 河野 直樹
(74)代理人 100140176
弁理士 砂川 克
(74)代理人 100158805
弁理士 井関 守三
(74)代理人 100172580
弁理士 赤穂 隆雄
(74)代理人 100179062
弁理士 井上 正
(74)代理人 100124394
弁理士 佐藤 立志
(74)代理人 100112807
弁理士 岡田 貴志
(74)代理人 100111073
弁理士 堀内 美保子
(72)発明者 鶴見 理恵子
東京都港区芝浦一丁目１番１号 東芝ソリューション株式会社内
(72)発明者 西村 明夫
東京都港区芝浦一丁目１番１号 東芝ソリューション株式会社内
(72)発明者 池田 竜朗
東京都港区芝浦一丁目１番１号 東芝ソリューション株式会社内

審査官 岸野 徹

(56)参考文献 特開２０１３－１７１３４９（ＪＰ，Ａ）
特開２００７－２５７４２６（ＪＰ，Ａ）
米国特許出願公開第２０１１／０２０９２０２（ＵＳ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ ２１／４１