

明 細 書

発明の名称： 認証連携システム及びＩＤプロバイダ装置

技術分野

[0001] 本発明の実施形態は、認証連携システム及びＩＤプロバイダ装置に関する。

背景技術

[0002] 社会、経済、生活のオンラインサービスへの依存度が増す情勢を背景に、個人や組織に関する情報を管理するアイデンティティ管理の重要性が高まっている。アイデンティティ管理とは、様々なサービスやシステムにおいて、個人や組織に関する情報の安全性と利便性を図り、登録から変更、削除までのアイデンティティのライフサイクル全体を管理する技術である。

[0003] ここで、アイデンティティとは、ある状況で個人やグループ、組織・企業を特定する情報の総体であり、識別子やクレデンシャル、属性が含まれる。識別子とは、アイデンティティを識別するための情報であり、アカウントや社員番号などに相当する。クレデンシャルとは、ある情報内容の正当性を示すための情報であり、パスワードなどがある。属性とは、アイデンティティを特徴付ける情報であり、氏名や住所、生年月日などを指す。

[0004] このようなアイデンティティ管理を利用した技術の代表例として、シングルサインオン（Single Sign-On、以降ＳＳＯと略す）がある。ＳＳＯは、一度の認証手続きで複数のアプリケーションやサービスを利用できる技術である。ＳＳＯは、一つの企業のイントラネットのようなシングルドメインにおいて、複数のアプリケーションが備える認証を統合させる場合が多かった。この場合、ＳＳＯは、一般的にＨＴＴＰ Ｃｏｏｋｉｅに認証結果を含め、アプリケーション間で認証結果を共有させる方式によって実現される。また、このようなＳＳＯ方式をＳＩ（System Integration）ベンダやミドルウェアベンダが個別にアクセス管理製品として製造していた。

[0005] 近年、シングルドメインを超えた異なるドメイン間（以下、クロスドメイ

ンともいう)でのSSOが求められてきた。理由としては、企業統合や合併、海外展開などの活発化、および台頭してきたクラウドコンピューティングのSaaS (Software as a Service) 等によるアウトソーシングが挙げられる。例えば、SaaS等は、使いたいときに素早く使える点がメリットの一つである。

[0006] しかしながら、クロスドメインのSSOを実現する場合、認証結果の共有に大きな手間が発生していた。主な原因としては2点ある。1点目は、HTTP Cookieの利用がシングルドメインに限定されているため、ドメイン間でHTTP Cookieを利用して認証結果を共有できないことである。2点目は、ドメインごとに採用しているアクセス管理製品のSSO方式がベンダ間で異なるため、単純に導入できず、別途、施策を用意する必要があったためである。

[0007] このような原因を解消するため、SSOの標準化の要望が高まるようになった。このような要望に応じた代表的な標準技術の一つとして、非営利団体OASIS (Organization for the Advancement of Structured Information Standards) が策定したSAML (Security Assertion Markup Language) がある。

[0008] SAMLは認証・認可・属性に関する情報の表現形式、および送受信手順が定義された仕様であり、目的に応じて様々な実装形態を可能にするように体系的に規定されている。主体の構成はアイデンティティ提供者 (Identity Provider、以降、IdPと略し、IDプロバイダという)、サービス提供者 (Service Provider、以降SPと略し、サービスプロバイダという)、ユーザの3者であり、IDプロバイダが発行する認証結果をサービスプロバイダが信頼することでSSOを実現している。

[0009] SAMLに基づくSSOを開始する場合、一般的に次の2点について事前に準備する必要がある。1点目は、サービスプロバイダとIDプロバイダとの間でビジネスや技術面での情報交換や合意形成を通じて、信頼関係を構築しておくことである。2点目では、一人のユーザがサービスプロバイダごと

に個別のアカウントを持ち、これらの個別のＳＰアカウントとＩＤプロバイダのアカウントを事前に連携させておくことである。これら信頼関係の構築及び事前のアカウント連携といった事前準備を終えた状態でないとＳＳＯを開始することはできない。

[0010] このような事前準備の後、ＳＳＯは以下のような手順（１）～（６）に沿って実現される。ここでは、Ｗｅｂブラウザを介したＳＳＯの手順を説明する。

[0011] （１）ユーザがサービスプロバイダに対してサービス提供を要求する。

[0012] （２）サービスプロバイダは、まだユーザの認証をしていないため、ユーザ側のＷｅｂブラウザを介して、認証リクエストをＩＤプロバイダに送る。

[0013] （３）ＩＤプロバイダは何らかの手段でユーザを認証し、認証アサーションを作成する。なお、ＳＡＭＬは、認証手段を規定せず、認証アサーションをサービスプロバイダに伝える仕組みを規定している。認証アサーションとは、サービスプロバイダが認証結果を信用できるかを判断するため、認証手段の種類やクレデンシャルがどのように作成されたかなどの情報が含まれる。

[0014] （４）ＩＤプロバイダは、作成した認証アサーションを含む認証結果を、ユーザ側のＷｅｂブラウザを介してサービスプロバイダに返信する。

[0015] （５）サービスプロバイダは、ＩＤプロバイダの認証結果に基づき、サービス提供の可否を決定する。

[0016] （６）ユーザは、サービスプロバイダからサービス提供を受ける。

[0017] このように、ＳＡＭＬに基づくＳＳＯでは、ユーザが一度の認証手続きをＩＤプロバイダに行うだけで更なる認証手続きを実行せずに、複数のサービスが使用可能となる。現在では、個別のＳＳＯ方式を実装していたミドルウェアベンダは、クロスドメインの相互運用性を確保するために、ＳＡＭＬのＩＤプロバイダ・サービスプロバイダ機能を実装したアクセス管理製品の販売や、ＳＡＭＬのサービスプロバイダ機能を実装した商用のＷｅｂサービスへの導入を実行している。

[0018] 但し、SAMLに基づくSSOは、アイデンティティのライフサイクル全体のうち、アイデンティティの「利用」という一部分でしかない。前述したように、SSOを開始する場合、アカウント連携を行う必要があり、アカウント連携を行うには、サービスプロバイダとIDプロバイダ間にアイデンティティの登録、変更、削除、再発行、一時停止などの管理を包括的に連携する技術が求められる。

[0019] アイデンティティの登録、変更、削除、再発行、一時停止などを自動化する技術としてアカウントプロビジョニングがあり、その標準技術としてSPML (Service Provisioning Markup Language) がある。

[0020] ところで、前述したアカウント連携の事前準備を終えていない状態から、アカウント連携をSSOの一部として動的に実行するデータ処理システムが知られている。通常、サービスプロバイダ側にユーザのアカウントが登録されてない状態、すなわち、アカウント連携が行われてない状態でSSOを開始しようとした場合、エラーが発生することになっていた。

[0021] しかしながら、このデータ処理システムによれば、前述した状態でもアカウント連携をSSOの一部として動的に実行できる。具体的には、サービスプロバイダがユーザからのサービス要求を受けた後、サービスプロバイダがユーザのアカウントを登録するための十分な情報を保持していないことを確認する。確認後、サービスプロバイダはIDプロバイダにユーザ属性を要求し、IDプロバイダはサービスプロバイダに所望のユーザ属性を提供する。これにより、データ処理システムは、SSOの過程でアカウント登録及び連携を実行する。

先行技術文献

特許文献

[0022] 特許文献1：特表2008-538247号公報

非特許文献

[0023] 非特許文献1：“Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0”，OASIS Standard, 15 March 2005, h

<http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf>

非特許文献2：“OASIS Service Provisioning Markup Language (SPML) Version 2”，OASIS Standard, 1 April 2006, <http://www.oasis-open.org/committees/provision/docs/pstc-spml2-os.pdf>

発明の概要

発明が解決しようとする課題

- [0024] 以上説明したデータ処理システムは、個々のユーザのアカウント登録に必要なユーザ属性の要求及び提供という軽量の処理で実現でき、多数のユーザに対する大量の事前処理を必要としないことから、通常、問題ない。
- [0025] しかしながら、本発明者の検討によれば、以下に述べるように、改良の余地がある。
- [0026] 通常、企業において、サービスプロバイダが提供するサービスを利用する場合、ＩＳ（Information System）部門がサービスプロバイダに対して、アカウント登録及び連携を行う。
- [0027] ＩＳ部門は、企業に所属する多数のユーザに応じた大量の事前処理を一括して行うか、又はユーザによる任意のタイミングで一連の承認フローを通した手続きを経た後に当該ユーザに対するアカウント登録及び連携を行う。
- [0028] ここで、前者の事前処理を行う場合は、ＳＳＯの過程でアカウント登録及び連携を実行する必要があるため、前述したデータ処理システムとは無関係である。
- [0029] 一方、後者の承認フローを通す場合は、ユーザだけでなく、ユーザが所属する組織階層ごとの上長や調達部門、ＩＳ部門など多くの人手を介すことになり、大量の手間暇を要する。更に、ＩＳ部門が事前処理を一括して行わないことから、人手による作業が発生し、負担が大きい上、効率や利便性も悪い。例えば、ＳaaS等における素早く使えるメリットを生かすことができない。
- [0030] 従って、ＳＳＯの過程でアカウント登録及び連携を実行するシステムでは、人手を介さずにサービス利用可否を決定するシームレスな仕組みを備えて

いることが望ましい。

- [0031] 本発明が解決しようとする課題は、SSOの過程でアカウント登録及び連携を実行する際に、人手を介さずにサービス利用可否を決定し得る認証連携システム及びIDプロバイダ装置を提供することである。

課題を解決するための手段

- [0032] 実施形態の認証連携システムは、ユーザが操作するユーザ端末にログイン処理を実行可能で第1メモリを有するIDプロバイダ装置と、前記ログイン処理が成功した場合に前記ユーザ端末にサービスデータを送信可能で第2メモリを有する複数のサービスプロバイダ装置とを備えている。
- [0033] 前記IDプロバイダ装置のユーザ属性情報記憶手段は、前記ユーザを特定するためのユーザ属性の項目名と前記ユーザ属性の項目値とを関連付けたユーザ属性情報であって、少なくとも前記ユーザを識別するユーザIDを前記項目名に含む複数の前記ユーザ属性情報を記憶する。
- [0034] 前記IDプロバイダ装置のサービス利用状況記憶手段は、前記ユーザIDと、前記各サービスプロバイダ装置を識別するサービスプロバイダIDと、前記サービスデータの送信が許可された場合を示すサービス利用中、又は前記サービスデータの送信が許可されていない場合を示すサービス未利用のいずれかを示すサービス利用状況とを関連付けて記憶する。
- [0035] 前記IDプロバイダ装置のポリシー記憶手段は、前記サービスプロバイダID毎に、当該サービスプロバイダIDで識別されるサービスプロバイダ装置によるサービスデータの送信が許可される対象となるユーザを示す複数のポリシー情報を記憶する。
- [0036] 前記IDプロバイダ装置の一部項目名記憶手段は、前記サービスプロバイダIDと、前記ユーザ属性情報内のユーザ属性の項目名のうち、一部の項目名とを関連付けて記憶する。
- [0037] 前記IDプロバイダ装置の鍵記憶手段は、自装置の署名生成鍵を記憶する。
- [0038] 前記IDプロバイダ装置は、いずれかの前記サービスプロバイダ装置から

送信されて当該サービスプロバイダ装置のサービスプロバイダIDと前記ユーザ端末のアドレス情報とを含む認証連携要求を受けると、当該認証連携要求内のユーザ端末のアドレス情報を含むユーザ認証要求を送出する。

[0039] 前記IDプロバイダ装置は、前記送出されたユーザ認証要求内のユーザ端末のアドレス情報に基づいて、当該ユーザ端末にログイン要求を送信し、当該ユーザ端末から受けたユーザID及びユーザ認証情報を前記ユーザ属性情報記憶手段内のユーザID及び参照情報に基づいて認証するログイン処理を実行する。

[0040] 前記IDプロバイダ装置は、前記ログイン処理が成功したとき、当該ログイン処理に用いたユーザIDと前記認証連携要求内のサービスプロバイダIDとを含むポリシ評価要求を送出する。

[0041] 前記IDプロバイダ装置は、前記送出されたポリシ評価要求内のユーザIDに基づいて前記ユーザ属性記憶手段からユーザ属性情報を読み出す。

[0042] 前記IDプロバイダ装置は、前記送出されたポリシ評価要求内のサービスプロバイダIDに基づいて前記ポリシ記憶手段からポリシ情報を読み出す。

[0043] 前記IDプロバイダ装置の送信許可判定手段は、前記読み出したポリシ情報に対し、前記読み出したユーザ属性情報、ユーザが利用したいサービスの種類、ユーザが行いたいサービスへの操作、サービスを実行するに際してのユーザの環境条件に適合するか否かと、当該読み出したポリシ情報に示される利用料金の上限値に対して前記受信した利用料金応答内の利用料金が適合するか否かとに応じて、前記サービスデータの送信を許可するか否かを判定する。

[0044] 前記IDプロバイダ装置は、この判定結果を含むポリシ評価応答を前記ポリシ評価要求の送信元に送出する。

[0045] 前記IDプロバイダ装置は、前記ポリシ評価応答内の判定結果が許可を示す場合、前記ポリシ評価要求内のユーザIDとサービスプロバイダIDとを含むアカウント連携要求を送出する。

[0046] 前記IDプロバイダ装置は、前記送出されたアカウント連携要求内のサー

ビスプロバイダIDに基づいて、前記一部項目名記憶手段からユーザ属性の一部の項目名を読み出す。

[0047] 前記IDプロバイダ装置は、当該読み出した一部の項目名と前記アカウント連携要求内のユーザIDとに基づいて、前記ユーザ属性記憶手段内で当該ユーザIDに一致するユーザIDを含むユーザ属性情報のうち、当該一部の項目名に一致する項目名及びこの項目名に関連付けられた項目値からなるユーザ属性部分情報を取得する。

[0048] 前記IDプロバイダ装置は、前記取得したユーザ属性部分情報にアカウント登録指示を付加してアカウント連携要求メッセージを作成する。

[0049] 前記IDプロバイダ装置は、前記アカウント連携要求メッセージを前記認証連携要求の送信元のサービスプロバイダ装置に送信する。

[0050] 前記IDプロバイダ装置は、前記アカウント連携要求メッセージの送信先のサービスプロバイダ装置から当該サービスプロバイダ装置のサービスプロバイダIDと前記ユーザ属性部分情報内のユーザIDとを含む登録完了が通知されると、当該登録完了を示すアカウント連携応答を送出する。

[0051] 前記IDプロバイダ装置は、前記送出されたアカウント連携応答内の登録完了に含まれるサービスプロバイダID及びユーザIDに基づいて、前記サービス利用状況記憶手段内のサービス利用状況をサービス未利用からサービス利用中に更新する。

[0052] 前記IDプロバイダ装置は、前記送出されたアカウント連携応答内の登録完了に含まれるサービスプロバイダID及びユーザIDを含む認証連携実行要求を送出する。

[0053] 前記IDプロバイダ装置は、前記認証連携実行要求を受けると、当該認証連携実行要求内のサービスプロバイダIDで識別されるサービスプロバイダ装置と自装置との間で共有する認証連携IDを発行し、この認証連携IDと当該認証連携実行要求内のユーザIDとを関連付けて前記第1メモリに書き込む。

[0054] 前記IDプロバイダ装置は、前記発行した認証連携IDと、前記ログイン

処理の認証方式名とを含むアサーション本文に対して前記署名生成鍵に基づくデジタル署名を生成し、当該アサーション本文と当該デジタル署名とを含む認証アサーションを作成する。

[0055] 前記ＩＤプロバイダ装置は、前記作成した認証アサーションを含む認証連携応答を前記認証連携要求の送信元のサービスプロバイダ装置に送信する。

[0056] 前記各サービスプロバイダ装置のユーザ属性部分情報記憶手段は、前記ユーザ属性情報記憶手段内のユーザ属性情報内のユーザ属性の項目名及び項目値のうちの一部の項目名と項目値とを関連付けたユーザ属性部分情報と、自装置内でユーザを識別するＳＰ側ユーザＩＤとを関連付けて記憶する。

[0057] 前記各サービスプロバイダ装置の検証ポリシ記憶手段は、前記ログイン処理が成功した場合にサービスデータの送信を許可するログイン処理の認証方式名と、前記署名生成鍵に対応する署名検証鍵とを含む認証アサーション検証ポリシを記憶する。

[0058] 前記各サービスプロバイダ装置のサービスデータ記憶手段は、前記サービスデータを記憶する。

[0059] 前記各サービスプロバイダ装置は、前記ユーザ端末からサービス要求を受けると、当該サービス要求が認証トークンを含むか否かを判定し、前記認証トークンを含む場合には当該認証トークンと前記サービスデータ記憶手段内のサービスデータとを当該ユーザ端末に送信し、否の場合には自装置のサービスプロバイダＩＤと当該ユーザ端末のアドレス情報とを含む認証連携要求を前記ＩＤプロバイダ装置に送信する。

[0060] 前記各サービスプロバイダ装置は、前記アカウント連携要求メッセージを受信すると、新規の前記ＳＰ側ユーザＩＤを発行し、当該発行したＳＰ側ユーザＩＤと、当該アカウント連携要求メッセージ内のユーザ属性部分情報とを関連付けて前記ユーザ属性部分情報記憶手段に登録する。

[0061] 前記各サービスプロバイダ装置は、この登録の後、登録したユーザ属性部分情報内のユーザＩＤと自装置のサービスプロバイダＩＤとを含む登録完了を前記アカウント連携要求メッセージの送信元のＩＤプロバイダ装置に通知

する。

[0062] 前記各サービスプロバイダ装置は、前記IDプロバイダ装置から認証連携応答を受けると、当該認証連携応答内の認証アサーションから認証連携IDを抽出し、当該抽出した認証連携IDと、前記登録されたユーザ属性部分情報内のユーザIDとを関連付けて前記第2メモリに書き込む。

[0063] 前記各サービスプロバイダ装置は、前記認証アサーション検証ポリシー内の認証方式名と署名検証鍵とに基づいて、前記認証アサーション内の認証方式名とデジタル署名とをそれぞれ検証する。

[0064] 前記各サービスプロバイダ装置は、前記検証した結果がいずれも正当のとき、認証トークンを発行し、この認証トークンを前記認証連携IDに関連付けて前記第2メモリに書き込む。

[0065] 前記各サービスプロバイダ装置は、前記書き込まれた認証トークンと、当該認証トークンに前記第2メモリ内で前記認証連携IDを介して関連付けられたユーザIDとを含むサービス実行要求を送出する。

[0066] 前記各サービスプロバイダ装置は、前記送出されたサービス実行要求に基づいて、当該サービス実行要求内の認証トークンと前記サービスデータ記憶手段内のサービスデータとを前記ユーザ端末に送信する。

図面の簡単な説明

[0067] [図1]図1は、第1の実施形態に係る認証連携システム及びその周辺構成を示す模式図である。

[図2]図2は、同実施形態におけるIDPユーザリポジトリを説明するための模式図である。

[図3]図3は、同実施形態におけるサービス利用状況データストアを説明するための模式図である。

[図4]図4は、同実施形態における認証連携ポリシーストアを説明するための模式図である。

[図5]図5は、同実施形態におけるSPユーザ設定ルールストアを説明するための模式図である。

[図6]図6は、同実施形態における一時記憶部を説明するための模式図である。

[図7]図7は、同実施形態における認証アサーションを説明するための模式図である。

[図8]図8は、同実施形態における信頼ＩｄＰストアを説明するための模式図である。

[図9]図9は、同実施形態におけるＳＰユーザリポジトリを説明するための模式図である。

[図10]図10は、同実施形態におけるサービスデータストアを説明するための模式図である。

[図11]図11は、同実施形態における利用状況ストアを説明するための模式図である。

[図12]図12は、同実施形態における一時記憶部を説明するための模式図である。

[図13]図13は、同実施形態における検証ポリシストアを説明するための模式図である。

[図14]図14は、同実施形態における全体動作の概要を示す模式図である。

[図15]図15は、同実施形態におけるユーザ認証の処理フローを示すシーケンス図である。

[図16]図16は、同実施形態におけるユーザ認証の処理に必要な構成要素の一例を示すブロック図である。

[図17]図17は、同実施形態における認証連携ポリシ評価の処理フローを示すシーケンス図である。

[図18]図18は、同実施形態における認証連携ポリシ評価の処理に必要な構成要素の一例を示すブロック図である。

[図19]図19は、同実施形態におけるアカウント連携の処理フローを示すシーケンス図である。

[図20]図20は、同実施形態におけるアカウント連携の処理に必要な構成要

素の一例を示すブロック図である。

[図21]図 2 1 は、同実施形態における認証連携の処理フローを示すシーケンス図である。

[図22]図 2 2 は、同実施形態における認証連携の処理に必要な構成要素の一例を示すブロック図である。

[図23]図 2 3 は、第 2 の実施形態における利用状況ストアを説明するための模式図である。

[図24]図 2 4 は、同実施形態におけるサービス利用状況ストアを説明するための模式図である。

[図25]図 2 5 は、第 3 の実施形態における利用状況ストアを説明するための模式図である。

[図26]図 2 6 は、同実施形態におけるサービス利用状況ストアを説明するための模式図である。

発明を実施するための形態

[0068] 以下、各実施形態について図面を用いて説明する。なお、各実施形態では、既に ID プロバイダとサービスプロバイダ間で信頼関係が確立された状態、ユーザは ID プロバイダ側の組織に所属する状態、認証連携ポリシーは事前に定義済みであることを前提条件としている。また、各装置は、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対応する装置のコンピュータにインストールされ、対応する装置の機能を実現させるためのプログラムが用いられる。

[0069] <第 1 の実施形態>

図 1 は第 1 の実施形態に係る認証連携システム及びその周辺構成を示す模式図であり、図 2 乃至図 1 3 は同実施形態におけるリポジトリ、ストア又は記憶部等を説明するための模式図である。この認証連携システムは、ユーザが操作するユーザ端末 1 0 0 に対してログイン処理を実行可能な ID プロバイダ装置 2 0 0 と、ログイン処理が成功した場合にユーザ端末 1 0 0 にサー

ビスデータを送信可能なサービスプロバイダ装置 300 とを備えている。なお、サービスプロバイダ装置 300 は、複数台あるが、ここでは 1 台のみを図示している。

[0070] ここで、ユーザ端末 100 は、通常のコンピュータ機能を有して ID プロバイダ装置 200 及び各サービスプロバイダ装置 300 と通信可能な装置であり、例えば、ユーザの操作に応じて、サービス要求をサービスプロバイダ装置 300 に送信する機能と、ID プロバイダ装置 200 との間でログイン処理を実行する機能と、サービスプロバイダ装置 300 からサービスデータを受信する機能と、予めメモリに記憶したサービス利用アプリケーションプログラムを CPU が実行することにより、当該受信したサービスデータを再生する機能とを備えている。

[0071] ID プロバイダ装置 200 は、ユーザのアイデンティティを管理するものであり、ID ユーザリポジトリ 201、サービス利用状況ストア 202、認証連携ポリシーストア 203、SP ユーザ設定ルールストア 204、一時記憶部 205、鍵記憶部 206、ID 認証連携部 207、認証連携ハンドリング部 208、認証連携ポリシー評価部 209 及び ID アカウントプロビジョニング部 210 を備えている。

[0072] ここで、ID ユーザリポジトリ 201 は、ID プロバイダ装置 200 が配置される組織のユーザに関するアイデンティティ情報（以下、「ユーザ属性情報」という）を記憶する。具体的には、ID ユーザリポジトリ（ユーザ属性情報記憶手段）201 は、図 2 に示すように、ユーザを特定するためのユーザ属性の項目名とユーザ属性の項目値とを関連付けたユーザ属性情報 201 a であって、ユーザを識別するユーザ ID と、ユーザの氏名と、ユーザの所属と、ユーザの役職と、ユーザ端末のアドレス情報と、ユーザのログイン処理時に参照する参照情報とを項目名に含む複数のユーザ属性情報 201 a を記憶する。

[0073] なお、ユーザ属性情報 201 a は個人の情報を特徴付ける情報の集合体であり、ユーザ属性情報 201 a の例としては、ユーザの氏名、ユーザの所属

、ユーザの役職、ユーザ端末のアドレス情報、ユーザのログイン処理時に参照する参照情報などが挙げられる。しかし、これらには限られず、例えば電話番号や勤務状態といった任意の項目名と項目地とを更に含んでもよい。また、ユーザのログイン処理時に参照する参照情報は、本実施形態ではパスワードを用いるが、これには限られず、例えばユーザの指紋等の生体認証情報であってもよい。

[0074] サービス利用状況ストア202は、認証連携ポリシー評価部209から参照され、サービスの利用状況を記憶する。具体的には、サービス利用状況ストア（サービス利用状況記憶手段）202は、図3に示すように、ユーザ利用管理テーブル202aと、利用数管理テーブル202bとを記憶している。ユーザ利用管理テーブル202aは、ユーザIDと、各サービスプロバイダ装置300を識別するサービスプロバイダID（SP（1）～SP（N））と、サービスデータの送信が許可された場合を示すサービス利用中、又はサービスデータの送信が許可されていない場合を示すサービス未利用のいずれかを示すサービス利用状況とを関連付けて書き込まれる。なお、サービス利用状況は、サービス利用中及びサービス未利用に限らず、例えばユーザ端末100から受けた一時停止要求に基づくサービス一時停止中、及び／又はユーザ端末100から受けた利用終了要求に基づくサービス利用終了を含んでもよい。また、サービス利用終了は、現在の利用数が上限値を超えた場合に、IDプロバイダ装置200が遊休ユーザの利用を無効化した場合を含んでもよい。さらに、利用数管理テーブル202bは、図3に示すように、ユーザ管理テーブル202a内のサービス利用状況が示すサービス利用中の個数を示す利用数と、利用数の上限値とを関連付けて書き込まれる。

[0075] 認証連携ポリシーストア203は、認証連携ポリシー評価部209から参照され、認証連携ポリシーを記憶する。具体的には、認証連携ポリシーストア（ポリシー記憶手段）203は、図4に示すように、サービスプロバイダID毎に、当該サービスプロバイダIDで識別されるサービスプロバイダ装置300によるサービスデータの送信が許可されるユーザの所属及び役職を示す複数の

認証連携ポリシー（ポリシー情報）203a（203aA, 203aB, 203aC, …）を記憶する。

[0076] なお、認証連携ポリシー203aは、ユーザの所属及び役職といった静的なポリシー（例えば、図4中のA～Cの[1]～[3]）に加え、更に、サービスの利用数、従量制課金の合計といった動的なポリシー（例えば、図4中のCの[4]）を含んでもよい。

[0077] ここでポリシーとは、一般的に誰（サブジェクト）が、どのシステム資源（リソース）に対して、どのような操作（アクション）を行うことができるか（つまり、許可または拒否）が定義されたアクセス可否条件の集合体を指す。またオプションで、環境条件や責務条件についても定義されるものである。

[0078] 例えば、上述したポリシーの各要素について、「サブジェクト」は氏名や役職、所属など、「リソース」はサービスプロバイダIDやURLなど、「アクション」は利用開始や利用再開など、「環境条件」は何らかの要求を行なうユーザのIPアドレスやアクセス可能な期間や時刻などが該当する。また、「責務条件」はポリシー（アクセス可否条件）評価の結果を受けて、認証連携ハンドリング部208が認証連携の実行に際して課す作業になる。例えば、“「新規利用者を登録する」要求は許可するが、その代わりに「遊休者のIDを削除する」ことは確実に実行せよ”というような指示になるのである（例えば、図4中のBの[4]の[責務条件]）。

[0079] SPユーザ設定ルールストア（一部項目名記憶手段）204は、図5に示すように、ユーザ設定ルール204aを記憶する。ユーザ設定ルール204aは、サービスプロバイダIDと、IDPユーザリポジトリ201に記憶されたユーザ属性情報201a内のユーザ属性の項目名のうち、一部の項目名とを関連付けて書き込まれている。

[0080] 一時記憶部（第1メモリ）205は、RAM等のような一時的なメモリであり、図6に示すように、例えば、認証連携IDとユーザIDとを関連付けて記憶する。

- [0081] 鍵記憶部206は、自装置200の署名生成鍵を記憶する。署名生成鍵としては、例えば、公開鍵暗号方式における公開鍵と秘密鍵との鍵ペアのうちの秘密鍵が使用可能となっている。
- [0082] IDP認証連携部207は、シングルサインオンのIDプロバイダ機能を有する。IDP認証連携部207は、具体的には例えば、以下の機能(f207-1)～(f207-4)をもっている。
- [0083] (f207-1) 認証連携ハンドリング部208から送出されたユーザ認証要求内のユーザ端末100のアドレス情報に基づいて、当該ユーザ端末100にログイン要求を送信し、当該ユーザ端末100から受けたユーザID及びユーザ認証情報をIDPユーザリポジトリ201内のユーザID及び参照情報に基づいて認証するログイン処理を実行する機能。
- [0084] (f207-2) 認証連携ハンドリング部208から認証連携実行要求を受けると、当該認証連携実行要求内のサービスプロバイダIDで識別されるサービスプロバイダ装置300と自装置200との間で共有する認証連携IDを発行し、この認証連携IDと当該認証連携実行要求内のユーザIDとを関連付けて一時記憶部205に書き込む機能。
- [0085] (f207-4) 発行した認証連携IDと、ログイン処理の認証方式名とを含むアサーション本文に対して鍵記憶部206内の署名生成鍵に基づくデジタル署名を生成し、図7に示すように、当該アサーション本文と当該デジタル署名とを含む認証アサーション207aを作成する機能。
- [0086] (f207-4) 作成した認証アサーション207aを含む認証連携応答を認証連携要求の送信元のサービスプロバイダ装置300に送信する機能。
- [0087] 認証連携ハンドリング部208は、サービスプロバイダ装置300からの認証連携要求を受信した後、ポリシ評価処理とアカウント連携処理とIDプロバイダ認証連携処理で構成される一連の処理をハンドリングする。認証連携ハンドリング部208は、具体的には例えば、以下の機能(f208-1)～(f208-5)をもっている。
- [0088] (f208-1) いずれかのサービスプロバイダ装置300から送信されて当該

サービスプロバイダ装置 300 のサービスプロバイダ ID とユーザ端末 100 のアドレス情報とを含む認証連携要求を受けると、当該認証連携要求内のユーザ端末 100 のアドレス情報を含むユーザ認証要求を IDP 認証連携部 207 に送出する機能。

[0089] (f208-2) IDP 認証連携部 207 によるログイン処理が成功したとき、当該ログイン処理に用いたユーザ ID と認証連携要求内のサービスプロバイダ ID とを含むポリシ評価要求を認証連携ポリシ評価部 209 に送出する機能。

[0090] (f208-3) 認証連携ポリシ評価部 209 から受けたポリシ評価応答内の判定結果が許可を示す場合、ポリシ評価要求内のユーザ ID とサービスプロバイダ ID とを含むアカウント連携要求を IDP アカウントプロビジョニング部 210 に送出する機能。

[0091] (f208-4) 送出されたアカウント連携応答内の登録完了に含まれるサービスプロバイダ ID 及びユーザ ID に基づいて、サービス利用状況ストア 202 内のサービス利用状況をサービス未利用からサービス利用中に更新する機能。

[0092] (f208-5) IDP アカウントプロビジョニング部 210 から送出されたアカウント連携応答内の登録完了に含まれるサービスプロバイダ ID 及びユーザ ID を含む認証連携実行要求を IDP 認証連携部 207 に送出する機能。

[0093] 認証連携ポリシ評価部 209 は、認証連携ハンドリング部 208 からのポリシ評価要求を受けて、事前に定義された認証連携ポリシ 203 a とサービス利用状況に基づいてポリシ評価を行う。認証連携ポリシ評価部 209 は、具体的には例えば、以下の機能 (f209-1) ~ (f209-4) をもっている。

[0094] (f209-1) 認証連携ハンドリング部 208 から送出されたポリシ評価要求内のユーザ ID に基づいて IDP ユーザリポジトリ 201 からユーザ属性情報 201 a を読み出す機能。

[0095] (f209-2) 認証連携ハンドリング部 208 から送出されたポリシ評価要求内のサービスプロバイダ ID に基づいて認証連携ポリシストア 203 から認

証連携ポリシ（ポリシ情報）203aを読み出す機能。

[0096] (f209-3) 読み出した認証連携ポリシ203aに示される所属及び役職に対し、当該読み出したユーザ属性情報201a内の所属及び役職が適合するか否かに応じて、サービスデータの送信を許可するか否かを判定する送信許可判定機能。

[0097] (f209-4) この判定結果を含むポリシ評価応答をポリシ評価要求の送信元の認証連携ハンドリング部208に送出する機能。

[0098] IdPアカウントプロビジョニング部210は、認証連携ハンドリング部208からのアカウント連携要求を受けて、サービスプロバイダ装置300に対してアカウントプロビジョニングを実行する。IdPアカウントプロビジョニング部210は、具体的には例えば、以下の機能(f210-1)～(f210-5)をもっている。

[0099] (f210-1) 送出されたアカウント連携要求内のサービスプロバイダIDに基づいて、SPユーザ設定ルールストア204からユーザ属性の一部の項目名を読み出す機能。

[0100] (f210-2) 当該読み出した一部の項目名とアカウント連携要求内のユーザIDとに基づいて、IdPユーザリポジトリ201内で当該ユーザIDに一致するユーザIDを含むユーザ属性情報201aのうち、当該一部の項目名に一致する項目名及びこの項目名に関連付けられた項目値からなるユーザ属性部分情報を取得する機能。

[0101] (f210-3) 取得したユーザ属性部分情報にアカウント登録指示を付加してアカウント連携要求メッセージを作成する機能。

[0102] (f210-4) アカウント連携要求メッセージを認証連携要求の送信元のサービスプロバイダ装置300に送信する機能。

[0103] (f210-5) アカウント連携要求メッセージの送信先のサービスプロバイダ装置300から当該サービスプロバイダ装置のサービスプロバイダIDとユーザ属性部分情報内のユーザIDとを含む登録完了が通知されると、当該登録完了を示すアカウント連携応答を認証連携ハンドリング部208に送出す

る機能。

[0104] 一方、サービスプロバイダ装置300は、ユーザが利用するサービスを提供するものであり、信頼IDストア301、SPユーザリポジトリ302、サービスデータストア303、利用状況ストア304、一時記憶部305、検証ポリシーストア306、SP認証連携部307、利用状況提供部308、SPアカウントプロビジョニング部309及びサービスデータ通信部310を備えている。

[0105] 信頼IDストア301は、図8に示すように、IDプロバイダ装置200を識別するIDプロバイダIDのリストからなるIDプリスト（IDプロバイダリスト）301aを記憶する。

[0106] SPユーザリポジトリ302は、サービスデータ通信部310が送信するサービスデータを利用するユーザのアイデンティティ情報を記憶する。具体的には、SPユーザリポジトリ（ユーザ属性部分情報記憶手段）302は、図9に示すように、IDPユーザリポジトリ201内のユーザ属性情報201a内のユーザ属性の項目名及び項目値のうちの一部の項目名と項目値とを関連付けたユーザ属性部分情報302aと、自装置300内でユーザを識別するSP側ユーザIDとを関連付けて記憶している。

[0107] サービスデータストア303は、図10に示すように、サービスデータ303aを記憶している。サービスデータ303aは、サービスプロバイダ装置300によるサービス提供（サービスデータ送信）の対象として、ユーザ端末100に送信される任意のデータである。

[0108] 利用状況ストア304は、図11に示すように、ユーザ利用管理テーブル304aと、利用数管理テーブル304bとを記憶している。ユーザ利用管理テーブル304aは、ユーザIDと、サービスデータ303aの送信が許可された場合を示すサービス利用中、又はサービスデータ303aの送信が許可されていない場合を示すサービス未利用のいずれかを示すサービス利用状況とを関連付けて書き込まれる。利用数管理テーブル304bは、ユーザ管理テーブル内のサービス利用状況が示すサービス利用中の個数を示す利用

数と、利用数の上限値とを関連付けて書き込まれる。

- [0109] 一時記憶部（第２メモリ）３０５は、ＲＡＭ等のような一時的なメモリであり、図１２に示すように、例えば、認証アサーション２０７ａから抽出した認証連携ＩＤと、登録されたユーザ属性部分情報３０２ａ内のユーザＩＤと、発行された認証トークンとを関連付けて記憶する。
- [0110] 検証ポリシストア３０６は、図１３に示すように、ログイン処理が成功した場合にサービスデータ３０３ａの送信を許可するログイン処理の認証方式名と、ＩＤプロバイダ装置２００の署名生成鍵に対応する署名検証鍵とを含む認証アサーション検証ポリシを記憶する。署名検証鍵としては、例えば、公開鍵暗号方式における公開鍵と秘密鍵との鍵ペアのうちの公開鍵が使用可能となっている。
- [0111] ＳＰ認証連携部３０７は、シングルサインオンのサービスプロバイダ機能を有する。ＳＰ認証連携部３０７は、具体的には例えば、以下の機能(f307-1)～(f307-5)をもっている。
- [0112] (f307-1) ユーザ端末１００からサービス要求を受けると、当該サービス要求が認証トークンを含むか否かを判定し、認証トークンを含む場合には当該認証トークンとサービスデータストア３０３内のサービスデータ３０３ａとを当該ユーザ端末１００に送信し、否の場合には自装置３００のサービスプロバイダＩＤと当該ユーザ端末１００のアドレス情報とを含む認証連携要求をＩＤプロバイダ装置２００に送信する機能。
- [0113] (f307-2) ＩＤプロバイダ装置２００から認証連携応答を受けると、当該認証連携応答内の認証アサーション２０７ａから認証連携ＩＤを抽出し、当該抽出した認証連携ＩＤと、登録されたユーザ属性部分情報３０２ａ内のユーザＩＤとを関連付けて一時記憶部３０５に書き込む機能。
- [0114] (f307-3) 検証ポリシストア３０６内の認証アサーション検証ポリシ内の認証方式名と署名検証鍵とに基づいて、当該認証アサーション２０７ａ内の認証方式名とデジタル署名とをそれぞれ検証する検証機能。
- [0115] (f307-4) 検証した結果がいずれも正当のとき、認証トークンを発行し、

この認証トークンを認証連携IDに関連付けて一時記憶部305に書き込む機能。

[0116] (f307-5) 書き込まれた認証トークンと、当該認証トークンに一時記憶部305内で認証連携IDを介して関連付けられたユーザーIDを含むサービス実行要求をサービスデータ通信部310に送出する機能。

[0117] 利用状況提供部308は、IDプロバイダ装置200の認証連携ポリシ評価部209から利用状況送信要求を受けると、この利用状況送信要求に含まれるユーザーIDに基づいて利用状況ストア304を検索し、当該検索により得られたサービス利用状況を送信する機能をもっている。

[0118] SPアカウンストプロビュニオン部309は、IDプロバイダ装置200のIDPアカウンストプロビュニオン部210から受けたアカウンストプロビュニオン部210からアカウンスト連携要求メッセージを受信すると、新規のSP側ユーザーIDを発行し、当該発行したSP側ユーザーIDと、当該アカウンスト連携要求メッセージ内のユーザー属性部分情報302aとを関連付けてSPユーザーIDと自装置300のサービスプロバイダIDとを含む登録完了をアカウンスト連携要求メッセージの送信元のIDプロバイダ装置200に通知する機能。

[0119] (f309-1) IDプロバイダ装置200のIDPアカウンストプロビュニオン部210からアカウンスト連携要求メッセージを受信すると、新規のSP側ユーザーIDを発行し、当該発行したSP側ユーザーIDと、当該アカウンスト連携要求メッセージ内のユーザー属性部分情報302aとを関連付けてSPユーザーIDと自装置300のサービスプロバイダIDとを含む登録完了をアカウンスト連携要求メッセージの送信元のIDプロバイダ装置200に通知する機能。

[0120] (f309-2) この登録の後、登録したユーザー属性部分情報302a内のユーザーIDと自装置300のサービスプロバイダIDとを含む登録完了をアカウンスト連携要求メッセージの送信元のIDプロバイダ装置200に通知する機能。

[0121] サービスデータ通信部310は、SP認証連携部307から送出されたサービス実行要求に基づいて、当該サービス実行要求内の認証トークンとサービスデータストア303内のサービスデータ303aとをユーザー端末100に送信する機能をもっている。

[0122] 次に、以上のように構成された認証連携システムの動作について図 14乃至図 22を参照して説明する。以下の説明は、IDプロバイタ装置 200とサービスプロバイタ装置 300間でSSOが可能なシステム環境にあり、且つIDプロバイタ側の組織に所属するユーザが当該サービスプロバイタ装置 300にアカウントが登録されていない状態から開始される。また、この状態において、ユーザがサービス要求をした時に、IDプロバイタ装置 200が認証連携ポリシー 203aを満たすかを判定し、満たす場合にサービスプロバイタ装置 300側へのユーザのアカウント登録を行うことにより、IDプロバイタ装置 200とサービスプロバイタ装置 300間のSSOが実行され、サービスプロバイタ装置 300からサービスデータ 303aが送信される典型的な処理を例に挙げて述べる。

[0123] 以降、図 14に示す如き、ステップ ST10のユーザ認証 (ST11～ST18)、ステップ ST20の認証連携ポリシー評価 (ST21～ST27)、ステップ ST30のアカウント連携 (ST31～ST37) 及びステップ ST40の認証連携 (ST41～ST49) に分けて説明する。

[0124] ステップ ST10のユーザ認証の処理においては、IDプロバイタ側の組織に所属するユーザが、ユーザのアカウントがサービスプロバイタ装置 300に未登録の状態、ユーザ端末 100からサービス要求をサービスプロバイタ装置 300に送信し、IDプロバイタ装置 200がサービスプロバイタ装置 300に代わってユーザの認証を行う。以下、図 15のシーケンス図及び図 16の模式図を用いて述べる。

[0125] ステップ ST11では、ユーザは、サービスプロバイタ装置 300側のサービスを利用するために、ユーザ端末 100を操作する。ユーザ端末 100は、ユーザの操作により、サービス要求をサービスプロバイタ装置 300に送信する。サービスプロバイタ装置 300は、アクセス管理を担うSP認証連携部 307がサービス要求をキャッチする。

[0126] ステップ ST12では、SP認証連携部 307は、ユーザからのサービス要求を受けると、そのサービス要求が認証トークンを含むかを判定する

。例えば、ユーザからのサービス要求がＨＴＴＰリクエストの形態の場合、そのＨＴＴＰリクエストに含まれるＣｏｏｋｉｅの中に、サービスプロバイダ装置３００が発行した認証トークンが存在することを確認する。

[0127] 認証トークンの存在が確認できたら、サービスプロバイダ装置３００は、サービス要求により要求されたサービスをユーザに対して提供する。すなわち、ＳＰ認証連携部３０７は、サービス要求が認証トークンを含む旨を判定すると、サービスデータ通信部３１０により、当該認証トークンとサービスデータ記憶部３０３内のサービスデータ３０３ａとをユーザ端末１００に送信する。具体的には、ＳＰ認証連携部３０７は、サービス要求内の認証トークンと、当該認証トークンに一時記憶部３０５内で認証連携ＩＤを介して関連付けられたユーザＩＤとを含むサービス実行要求をサービスデータ通信部３１０に送出する。

[0128] 一方、判定の結果、サービス要求が認証トークンを含まない場合には、ステップＳＴ１３を実行する。なお、後述するようにステップＳＴ１３，ＳＴ１４が省略される場合にはステップＳＴ１５を実行する。

[0129] ステップＳＴ１３では、ＳＰ認証連携部３０７は、ユーザが所属するＩＤプロバイダを当該ユーザに選択させるため、事前に信頼関係を確立したＩＤプロバイダを示すＩＤプロバイダＩＤを列挙したＩｄＰリスト３０１ａを信頼ＩｄＰストア３０１から読み出してユーザ端末１００に送信する。なお、ＩｄＰリスト３０１ａはＩＤプロバイダリストと呼んでもよい。

[0130] ステップＳＴ１４では、ユーザ端末１００は、サービスプロバイダ装置３００から受信したＩｄＰリスト３０１ａを表示し、ユーザに対して、自身が所属するＩＤプロバイダの選択を促す。しかる後、ユーザ端末１００は、ユーザの操作により、選択されたＩＤプロバイダＩＤをサービスプロバイダ装置３００に送信する。なお、サービス要求がＩＤプロバイダの指定を含む場合や、サービスプロバイダ装置３００が一つのＩＤプロバイダのＩＤプロバイダ装置２００としか連携しない場合などのように、ＩＤプロバイダの選択が不要な場合には、ステップＳＴ１３～ＳＴ１４が省略される。

- [0131] ステップST15では、サービスプロバイダ装置300は、ユーザ端末100から受信したIDプロバイダIDに基づいて、当該IDプロバイダIDに識別されるIDプロバイダ装置200に認証連携要求を依頼する。このとき、認証連携要求は、サービスプロバイダ装置300から直接IDプロバイダ装置200に向けて送信してもよいし、ユーザ端末100を一旦経由して、リダイレクトする形で送信されてもよい。認証連携要求は、自装置300のサービスプロバイダIDとユーザ端末100のアドレス情報とを含んでいる。
- [0132] ステップST16では、IDプロバイダ装置200の認証連携ハンドリング部208が、IDプロバイダ装置200宛のメッセージをインターセプトする。認証連携ハンドリング部208は、メッセージを解析し、そのメッセージが認証連携要求であることを確認した場合、認証連携の処理を開始し、認証連携要求内のユーザ端末100のアドレス情報を含むユーザ認証要求をIDP認証連携部207に送出する。なお、認証連携要求以外のメッセージであることを確認した場合は、認証連携ハンドリング部208が仲介する形で、サービスプロバイダ装置300が所望する宛先へ再送信する。
- [0133] ステップST17では、IDP認証連携部207は、ユーザ認証要求を受けると、このユーザ認証要求に基づいて、ユーザの識別と認証のためのログイン処理を実行する。このログイン処理においては、IDP認証連携部207は、送出されたユーザ認証要求内のユーザ端末100のアドレス情報に基づいて、当該ユーザ端末100にログイン要求を送信し、当該ユーザ端末100から受けたユーザID及びユーザ認証情報をIDPユーザリポジトリ201内のユーザID及び参照情報に基づいて認証する。
- [0134] ステップST18では、IDP認証連携部207は、ステップST17のログイン処理が成功したとき、ログイン処理に用いたユーザIDと認証成功の旨とを含むユーザ認証完了のメッセージを認証連携ハンドリング部208に通知する。
- [0135] 以上により、ステップST10のユーザ認証(ST11～ST18)が終

了する。

[0136] ステップS T 2 0の認証連携ポリシー評価においては、ユーザ認証終了後、サービス利用状況やユーザ属性情報2 0 1 a、認証連携ポリシー2 0 3 aを入力値として、認証連携ポリシー評価を行い、ユーザのサービス要求に対して許可を下す。以下、図1 7のシーケンス図及び図1 8の模式図を用いて述べる。

[0137] ステップS T 2 1では、認証連携ハンドリング部2 0 8は、ステップS T 1 8にて受信したユーザ認証完了のメッセージを解析し、ログイン処理が成功したことを確認する。ログイン処理が成功したとき、認証連携ハンドリング部2 0 8は、ユーザのサービス要求に対するポリシー評価要求を認証連携ポリシー評価部2 0 9に送出する。ポリシー評価要求は、ステップS T 1 7の過程で取得したユーザID、すなわちユーザのID Pアカウントと、認証連携要求内のサービスプロバイダIDとを含んでいる。

[0138] 以降、ステップS T 2 2～S T 2 5を通じて、認証連携ポリシー評価部2 0 8は、認証連携ポリシー2 0 3 aの評価に必要な情報を収集する。

[0139] ステップS T 2 2では、認証連携ポリシー評価部2 0 9は、ポリシー評価要求内のユーザIDとサービスプロバイダIDに基づいてサービス利用状況ストア2 0 2からユーザのサービス利用状況を読み出す。但し、ステップS T 2 2は、後述するように静的なポリシー評価を実行する場合には省略される。このことは、ステップS T 2 3も同様である。

[0140] ここで、サービス利用状況ストア2 0 2は、図3に示すような2つの情報群を管理している。例えば、図3の上段に示すように、ユーザ単位でIDプロバイダ装置2 0 0が連携する単一もしくは複数のサービスプロバイダ装置3 0 0に関する利用状況の情報が記憶されている。例えば、図1 0のユーザIDがuser_0020のレコードについては、S P (1) はサービス未利用の状態、S P (2) はサービス利用中、S P (3) はサービス一時停止中、S P (N) はサービス利用終了の状態を表している。また、図3の下段に示すように、サービスプロバイダ装置3 0 0単位で、それぞれのサービスプロバイダ

装置 300 を利用するユーザ数、およびそのサービスプロバイダ装置 300 を利用できるユーザ数の上限値が記憶されている。

[0141] 以降、本実施形態では、図 3 を使って、ユーザ ID は user_0001、ユーザが要求するサービスプロバイダ装置 300 は SP (1) と仮定する。

[0142] ステップ ST 23 では、認証連携ポリシー評価部 209 は、ポリシー評価要求内のユーザ ID に基づいて、利用状況提供部 308 から、サービスプロバイダ装置 300 が管理するユーザの利用状況を取得する。

[0143] ただし、ステップ ST 23 は、ユーザが希望するサービスプロバイダ装置 300 以外に、本実施形態のような他の全サービスプロバイダ装置 300 の利用状況がサービス未利用のケースでは実行されない。図 3 によると、ユーザ ID が user_0001 のレコードがこれに該当する。

[0144] ステップ ST 23 が実行されるケースは、図 3 のユーザ ID が、user_0020 と user_1000 である。このようなケースが起こる状況は、認証連携ポリシー 203 a の評価指標として、ID プロバイダ側でなく、他のサービスプロバイダ装置 300 側で管理する情報も含めたいときである。他のサービスプロバイダ装置 300 側で管理する情報の一例としては、ユーザがサービス利用時に課される費用、つまり従量制課金がある。このように、時間に応じて変化する情報をも認証連携ポリシー 203 a の評価指標として含めることで、ユーザのサービス利用に関してダイナミックなアクセス制御（＝動的なポリシー評価）が可能となる。なお、ダイナミックなアクセス制御を実行する場合には、前述した従量制課金に限らず、例えば、サービスの現在の利用数とその上限値とを管理してもよい。

[0145] ステップ ST 24 では、認証連携ポリシー評価部 209 は、ポリシー評価要求内のユーザ ID に基づいて ID P ユーザリポジトリ 201 からユーザ属性情報 201 a を読み出す。本実施形態では、図 2 に示すようなユーザの属性情報となる。

[0146] ステップ ST 25 では、認証連携ポリシー評価部 209 は、ポリシー評価要求内のサービスプロバイダ ID に基づいて認証連携ポリシーストア 203 から認

証連携ポリシ 203 a を読み出す。本実施形態では、図 4 の各認証連携ポリシ 203 a のうち、図中 A に関連付けられた第 1 の認証連携ポリシ（SP（1）利用時のポリシ）203 a A が検索結果として読み出される。

[0147] ステップ ST 26 では、認証連携ポリシ評価部 209 は、静的なポリシ評価を実行する場合、ステップ ST 25 で読み出した認証連携ポリシ 203 a A に示される所属及び役職に対し、ステップ ST 24 で読み出したユーザ属性情報 201 a 内の所属及び役職が適合するか否かに応じて、サービスデータ 303 a の送信を許可するか否かを判定する。

[0148] 但し、ステップ ST 22 のサービス利用状況をも用いる動的なポリシ評価を実行する場合には、ステップ ST 22，ST 24，ST 25 を通じて取得したサービス利用状況、ユーザ属性情報 201 a 及び認証連携ポリシ 203 a A に基づいて、ポリシ評価を実行する。

[0149] 例えば、認証連携ポリシ 203 a A に示す SP（1）の利用に関するポリシ評価を例に説明する。認証連携ポリシ 203 a A には、事前に [1] ～ [4] のサービス利用条件が定義されており（静的なポリシ評価の場合には [4] は未定義）、収集したサービス利用状況、ユーザ属性情報 201 a が、これらのサービス利用条件を全て満たすことを以下のように確認する。その結果として、ユーザのサービス要求に対して、許可を下す。

[0150] 認証連携ポリシ 203 a A の [1]：認証連携ポリシ 203 a は、ユーザの所属する部が X であることを示す。これに対し、図 2 に示すように、ユーザ属性における当該ユーザの所属部が「X 部門」である。従って、認証連携ポリシ 203 a における [1] の条件を満たす。

[0151] 認証連携ポリシ 203 a A の [2]：認証連携ポリシ 203 a は、ユーザの所属する課が Y であることを示す。これに対し、図 2 に示すように、ユーザ属性における当該ユーザの所属課が「Y 課」である。従って、認証連携ポリシ 203 a における [2] の条件を満たす。

[0152] 認証連携ポリシ 203 a A の [3]：認証連携ポリシ 203 a は、ユーザの役職が Z 以上の役職であることを示す。これに対し、図 2 に示すように、

ユーザ属性における当該ユーザの役職が「Z職」である。従って、認証連携ポリシー203aにおける[3]の条件を満たす。

[0153] 認証連携ポリシー203aAの[4]：認証連携ポリシー203aは、利用中のアカウント数が上限値を超えないことを示す。これに対し、図3に示すように、当該サービスの利用数が10であり、上限値100を超えていない。従って、認証連携ポリシー203aにおける[4]の条件を満たす。

[0154] 以上のように、事前に定義した認証連携ポリシー203aに基づき、収集したサービス利用状況とユーザ属性情報201aを使って、ユーザのサービス要求に対する認証連携ポリシー評価を行う。なお、上記の条件において、一つでも条件を満たさないことが確認できたら、認証連携ポリシー評価の結果は拒否となる。

[0155] ステップST27では、認証連携ポリシー評価部209は、ステップST26の判定結果からなるポリシー評価結果をポリシー評価応答として、認証連携ハンドリング部208に送出する。

[0156] 以上により、ステップST20の認証連携ポリシー評価(ST21～ST27)が終了する。

[0157] ステップST30のアカウント連携では、認証連携ポリシー評価により得られたポリシー評価応答（サービスデータ送信の許可を示す場合）に基づき、サービスプロバイダ装置300のSPユーザリポジトリ302に対して、ユーザのアカウントを作成することで、SSOの事前準備として必要なIDプロバイダ装置200とサービスプロバイダ装置300間でのアカウント連携を実現する。以下、図19のシーケンス図及び図20の模式図を用いて述べる。

[0158] ステップST31では、認証連携ハンドリング部208は、ステップST27で送出されたポリシー評価応答に含まれるポリシー評価結果を確認し、サービス要求を許可する場合は、ポリシー評価要求内のユーザIDとサービスプロバイダIDとを含むアカウント連携要求をIDPアカウントプロビジョニング部210に依頼する。なお、ポリシー評価結果がサービス利用の拒否を示す

場合、サービス利用拒否の旨をユーザ端末１００に通知する。ここでは、ボ
リシ評価結果が許可の場合を例に挙げ、以降のステップ３２～３７を説
明する。

[0159] ステップ３２では、ＩＤＰアカウントプロビジョニング部２１０は、

送出されたアカウント連携内のサービスプロバイダ（例、ＳＰ（１））
に基づいて、ＳＰユーザ設定ルールストア２０４からユーザ設定ルール２０
４ａを読み出す。ユーザ設定ルール２０４ａは、例えば、サービスプロバイ
ダ装置３００に対してアカウント登録を行う際、サービスプロバイダ装置
３００ごとに求められる必要なユーザ属性の項目名（ユーザ属性の一部の項目
名）などがある。ここでは、ＩＤＰアカウントプロビジョニング部２１０は
、ユーザ設定ルール２０４ａとして、ユーザ属性の一部の項目名を読み出し
たものとする。

[0160] ステップ３３では、ＩＤＰアカウントプロビジョニング部２１０は、

ステップ３２で読み出した一部の項目名とアカウント連携要求内のユー
ザＩＤとに基づいて、ＩＤＰユーザリポジトリ２０１内で当該ユーザＩＤに
一致するユーザＩＤを含むユーザ属性情報２０１ａのうち、当該一部の項目
名に一致する項目名及びこの項目名に関連付けられた項目値から必要な
ユーザ属性情報（ユーザ属性部分情報）を取得する。

[0161] ステップ３４では、ＩＤＰアカウントプロビジョニング部２１０は、

取得したユーザ属性部分情報にアカウント登録指示を付加してアカウント連
携要求メッセージを作成する。例えば、ＩＤＰアカウントプロビジョニング
部２１０は、ＳＰアカウントプロビジョニング部３０９が公開する操作イン
タフェースに基づき、ＳＰユーザリポジトリ３０２の操作の種類と、その操
作が対象とするステップ３３で取得したユーザ属性部分情報に対応付け
て、ＳＰアカウント連携要求メッセージを作成する。なお、本実施形態では
、サービスプロバイダ装置３００側にユーザのアカウントが登録されてない
ため、操作の種類としてアカウント登録を指定する。

[0162] ステップ３５では、ＩＤＰアカウントプロビジョニング部２１０は、

作成したＳＰアカウント連携要求メッセージを、認証連携要求の送信元のサービスプロバイダ装置３００に送信する。ＳＰアカウント連携要求メッセージは、サービスプロバイダ装置３００内のＳＰアカウントプロビジョニング部３０９に受信される。

[0163] ステップＳＴ３６では、ＳＰアカウントプロビジョニング部３０９は、受信したＳＰアカウント連携要求メッセージに基づき、ＳＰ側ユーザＩＤ（サービスプロバイダ装置３００側のユーザＩＤ）を新規発行し、当該ＳＰ側ユーザＩＤと、アカウント連携要求メッセージ内のユーザ属性部分情報３０２aとを関連付けてＳＰユーザリポジトリ３０２に登録する。登録後、ＳＰアカウントプロビジョニング部３０９は、登録したユーザ属性部分情報３０２a内のユーザＩＤと自装置のサービスプロバイダＩＤとを含む登録完了をアカウント連携要求メッセージの送信元のＩＤプロバイダ装置２００に通知する。具体的には、登録完了は、ＩＤプロバイダ装置２００内のＩｄＰアカウントプロビジョニング部２１０に通知される。

[0164] ステップＳＴ３７では、ＩｄＰアカウントプロビジョニング部２１０は、登録完了が通知されると、当該登録完了を示すアカウント連携応答を認証連携ハンドリング部２０８に送出する。

[0165] 以上により、ステップＳＴ３０のアカウント連携（ＳＴ３１～ＳＴ３７）が終了する。

[0166] ステップＳＴ４０の認証連携では、アカウント連携終了後、ＩＤプロバイダ装置２００とサービスプロバイダ装置３００との間で認証連携、すなわちＳＳＯを行う。以下、図２１のシーケンス図及び図２２の模式図を用いて述べる。

[0167] ステップＳＴ４１では、認証連携ハンドリング部２０８は、ステップＳＴ３７にて通知されたアカウント連携応答に含まれる結果を解析する。その結果に問題がなければ、認証連携ハンドリング部２０８は、送出されたアカウント連携応答内の登録完了に含まれるサービスプロバイダＩＤ及びユーザＩＤに基づいて、サービス利用状況ストア２０２内のサービス利用状況をサー

ビス未利用からサービス利用中に更新する。これにより、サービス利用状況ストア202において、当該ユーザが要求したサービスプロバイダ装置300の利用状況がサービス未利用の状態からサービス利用中の状態に変更される。

[0168] ステップST42では、認証連携ハンドリング部208は、アカウント連携応答内の登録完了に含まれるサービスプロバイダID及びユーザIDを含む認証連携実行要求をIDP認証連携部207に送出する。

[0169] ステップST43では、IDP認証連携部207は、認証連携実行要求を受けると、当該認証連携実行要求内のサービスプロバイダIDで識別されるサービスプロバイダ装置300と自装置200との間で共有する認証連携IDを発行し、この認証連携IDと当該認証連携実行要求内のユーザIDとを関連付けて一時記憶部205に書き込む。

[0170] ステップST44では、IDP認証連携部207は、発行した認証連携IDと、ステップST17で行ったログイン処理の認証方式名とを含むアサーション本文を作成する。また、IDP認証連携部207は、アサーション本文に対して鍵記憶部206内の署名生成鍵に基づくデジタル署名を生成する。さらに、IDP認証連携部207は、当該アサーション本文と当該デジタル署名とを含む認証アサーション207aを作成する。

[0171] ステップST45では、IDP認証連携部207は、作成した認証アサーション207aを含む認証連携応答を、認証連携要求の送信元のサービスプロバイダ装置300に送信する。この認証連携応答は、当該サービスプロバイダ装置300のSP認証連携部307に受信される。

[0172] ステップST46では、SP認証連携部307は、認証連携応答を受けると、当該認証連携応答内の認証アサーション207aから認証連携IDを抽出し、当該抽出した認証連携IDと、ステップST36でSPユーザリポジトリ302に登録されたユーザ属性部分情報302a内のユーザIDとを関連付けて一時記憶部305に書き込む。

[0173] ステップST47では、SP認証連携部307は、認証アサーション検証

ポリシ内の認証方式名と署名検証鍵とに基づいて、認証アサーション207a内の認証方式名とデジタル署名とをそれぞれ検証する。これにより、SP認証連携部307は、IDプロバイダ装置200が発行した認証アサーション207aから、IDプロバイダ装置200の認証結果を信頼できるかを判断し、ユーザへのサービスデータ送信（サービス提供）の可否を決定する。本実施形態では、検証した結果がいずれも正当であるとし、サービスデータ送信を許可として決定する。

[0174] ステップST48では、SP認証連携部307は、ステップST47で許可と決定されたとき、認証トークンを発行し、この認証トークンを認証連携IDに関連付けて一時記憶部305に書き込む。

[0175] ステップST49では、SP認証連携部307は、書き込まれた認証トークンと、当該認証トークンに一時記憶部305内で認証連携IDを介して関連付けられたユーザIDとを含むサービス実行要求をサービスデータ通信部310に送出する。サービスデータ通信部310は、送出されたサービス実行要求に基づいて、当該サービス実行要求内の認証トークンとサービスデータストア303内のサービスデータ303aとをユーザ端末100に送信する。

[0176] 上述したように本実施形態によれば、ユーザからのサービスプロバイダ装置300へのサービス要求に対し、IDプロバイダ装置200内に配備された認証連携ハンドリング部208がサービスプロバイダ装置300からの認証連携要求をインターセプトし、事前に定義された認証連携ポリシ203aに基づき、サービスデータ303aの送信可否を判定する。そして、判定結果が許可の場合、IDプロバイダ装置200内で管理される当該ユーザ属性情報201aを使って、サービスプロバイダ装置300内で管理されるSPユーザリポジトリ302に対して、当該ユーザのアカウントを作成する。その後、IDプロバイダ装置200とサービスプロバイダ装置300の各々が、従来の認証連携処理を行い、当該ユーザに対してサービスプロバイダ装置300から所望のサービスが提供される。

[0177] 従って、サービスプロバイダ装置 300 側に当該ユーザのアカウントが登録されていない状態でも、当該ユーザのサービス要求、すなわち SSO の実施タイミングで、ID プロバイダ装置 200 側に事前に定義した認証連携ポリシー 203 a に基づき、サービスデータ 303 a の送信可否を自動判定することで、人手を介することなく、且つ時間を要することなく、当該ユーザに対してシームレスなサービス利用を提供することができる。

[0178] また、インターネットなどの分散環境下で提供されるサービス利用において、事前に定義したサービス利用のポリシーとサービスの利用状況に基づいて、サービスの利用申請からシングルサインオンまでの一連の処理を自動化し、ユーザのスムーズなサービス利用の開始を実現することができる。

[0179] <第 2 の実施形態>

次に、第 2 の実施形態について前述した図面を参照しながら説明する。

[0180] 第 2 の実施形態は、第 1 の実施形態のステップ S T 2 3 を実行する場合の具体例である。ここでは、サービス要求を送信したユーザ端末 100 のユーザが、既に他の様々なサービスプロバイダを利用している状況下であって、別のサービスプロバイダを新規利用する場合を例に挙げて述べる。

[0181] この場合、第 1 の実施形態のステップ S T 2 3 において、ユーザが利用中の各サービスプロバイダの利用料金を認証連携ポリシー評価の指標として利用し、認証連携ポリシー 203 a に対して、利用料金の上限値を事前に定義することで（例、図 4 の C の [4] ）、別のサービスプロバイダの新規利用を拒否可能としている。

[0182] これに伴い、サービスプロバイダ装置 300 の利用状況ストア 304 は、図 23 に示すように、ユーザ利用管理テーブル 304 a において、ユーザ ID と、サービス利用中の状態に対して累積した利用料金とを関連付けて記憶する。

[0183] また、利用状況提供部 308 は、ID プロバイダ装置 200 からユーザ ID を含む利用料金送信要求を受けると、この利用料金送信要求内のユーザ ID に基づいて利用状況ストア 304 を検索し、当該検索により得られた利用

料金及び当該ユーザIDを含む利用料金応答を当該IDプロバイダ装置200に送信する機能をもっている。

[0184] 一方、IDプロバイダ装置200においては、認証連携ポリシーストア203内の各認証連携ポリシー203aのうちのいずれかの認証連携ポリシー203aは、サービスプロバイダIDに関連付けて、当該サービスプロバイダIDで識別されるサービスプロバイダ装置300によるサービスデータ303aの送信が許可されるユーザの所属及び役職と、当該ユーザの利用料金の上限値（例、図4のCの[4]）とを示している。

[0185] また、認証連携ポリシー評価部209は、認証連携ハンドリング部208から送出されたポリシー評価要求内のユーザIDとサービスプロバイダIDとに基づいて、当該サービスプロバイダIDで識別されるサービスプロバイダ装置300に対し、当該ユーザIDを含む利用料金送信要求を送信し、当該サービスプロバイダ装置300から当該ユーザID及び利用料金を含む利用料金応答を受信する機能を更に備えている。なお、受信した利用料金は、図24に示すように、ユーザIDとサービスプロバイダIDとに関連付けてサービス状況ストア202内のユーザ利用管理テーブル202aに書き込んでもよいが、必ずしも書き込まなくてもよい。

[0186] また、認証連携ポリシー評価部209の前述した送信許可判定機能は、認証連携ポリシーストア203から読み出した認証連携ポリシー203aにユーザの所属及び役職と利用料金の上限値とが含まれる場合、読み出したポリシー情報に示される所属及び役職に対してIDPユーザリポジトリ201から読み出したユーザ属性情報201a内の所属及び役職が適合するか否かと、当該読み出したポリシー情報に示される利用料金の上限値に対してサービスプロバイダ装置300から受信した利用料金応答内の利用料金が適合するか否かとに応じて、サービスデータ303aの送信を許可するか否かを判定する機能となっている。

[0187] ここで、本明細書においては、上述したような読み出したポリシー情報に示される所属及び役職には限られず、読み出したポリシー情報に対して、読み出

したユーザ属性情報、ユーザが利用したいサービスの種類、ユーザが行いたいサービスへの操作、サービスを実行するに際してのユーザの環境条件に適合するか否かと、当該読み出したポリシー情報に示される利用料金の上限値に対して、受信した利用料金応答内の利用料金が適合するか否かに応じて、サービスデータ 303a の送信を許可するか否かを判定しても良い。

[0188] 次に、以上のように構成された認証連携システムの動作について前述した図 17 を主に参照して説明する。

[0189] 今、ステップ ST10 のユーザ認証 (ST11 ~ ST18) は、前述した通りに実行される。

[0190] 続いて、ステップ ST20 の認証連携ポリシー評価においては、ステップ ST21 (ポリシー評価要求) 及びステップ ST22 (サービス利用状況の検索) が前述した通りに実行される。

[0191] ステップ ST23 では、認証連携ポリシー評価部 209 は、認証連携ハンドリング部 208 から送出されたポリシー評価要求内のユーザ ID とサービスプロバイダ ID とに基づいて、当該サービスプロバイダ ID で識別されるサービスプロバイダ装置 300 に対し、当該ユーザ ID を含む利用料金送信要求を送信する。

[0192] サービスプロバイダ装置 300 の利用状況提供部 308 は、この利用料金送信要求内のユーザ ID に基づいて利用状況ストア 304 を検索し、当該検索により得られた利用料金及び当該ユーザ ID を含む利用料金応答を当該 ID プロバイダ装置 200 に送信する。

[0193] ID プロバイダ装置 200 の認証連携ポリシー評価部 209 は、この利用料金応答を受信する。

[0194] 次に、ステップ ST24 (ユーザ属性情報 201a の検索) 及びステップ ST25 (認証連携ポリシー 203a の検索) が前述同様に実行される。但し、認証連携ポリシー 203a は、利用料金の上限値を含んでいるものとする。

[0195] ステップ ST26 では、認証連携ポリシー評価部 209 は、認証連携ポリシーストア 203 から読み出した認証連携ポリシー 203a にユーザの所属及び役

職と利用料金の上限值とが含まれる場合、読み出したポリシー情報に示される所属及び役職に対してＩｄＰユーザリポジトリ２０１から読み出したユーザ属性情報２０１ａ内の所属及び役職が適合するか否かと、当該読み出したポリシー情報に示される利用料金の上限值に対してサービスプロバイダ装置３００から受信した利用料金応答内の利用料金が適合するか否かとに応じて、サービスデータ３０３ａの送信を許可するか否かを判定する。

[0196] 以降のステップＳＴ２７（ポリシー評価応答）、ステップＳＴ３０のアカウント連携（ＳＴ３１～ＳＴ３７）及びステップＳＴ４０の認証連携（ＳＴ４１～ＳＴ４９）の処理は、前述した通りに実行される。

[0197] 上述したように本実施形態によれば、第１の実施形態の効果に加え、ユーザの利用料金にも応じて、サービスデータ送信の可否を判定することができる。

[0198] 従って、認証連携ポリシー２０３ａを導入し、ＩＤプロバイダ装置２００やサービスプロバイダ装置３００側で管理する動的に変化するサービス利用状況も、ユーザ単位でなく、ＩＤプロバイダ単位で取り扱うことで、厳密な認証連携およびサービス利用の制御が可能となる。

[0199] 補足すると、第１の実施形態においてスムーズなサービス利用が可能になることで利便性が向上する反面、企業などの営利組織にとって無駄なサービス利用は好ましくない。従って、ユーザや組織レベルでのサービス利用状況に応じて、ダイナミック且つ柔軟に利用管理をコントロールする仕組みを備えていることが望ましい。本実施形態及び第３の実施形態はこのような仕組みを備えた認証連携システムを実現することができる。

[0200] <第３の実施形態>

次に、第３の実施形態について前述した図面を参照しながら説明する。

[0201] 第３の実施形態は、第１の実施形態のステップＳＴ２３を実行する場合の他の具体例である。ここでは、サービスプロバイダ装置３００では、サービスを利用するユーザの数が上限値にある状況において、新たにサービス要求を受けた場合を例に挙げて述べる。

[0202] すなわち、サービスプロバイダの利用数を認証連携ポリシ評価の指標とし

て利用し、認証連携ポリシ203aに対して、利用数が上限値を超過した場合の追加条件を事前に定義しておく(図4のBの[4])。事前に定義する場合の追加条件には、IDプロバイダ装置200内で管理する遊休状態のユーザが存在すれば、サービスプロバイダ装置300内で管理する遊休状態ユーザのプロカウントを削除もしくは無効化し、新規ユーザのプロカウント登録の責務条件を定義する(図4のBの[4]の[責務条件])。このように、利用数が上限を超えた場合に、遊休ユーザのプロカウントを無効化して空いた枠を申請ユーザのプロカウントに割り当てる旨の責務条件を備えた認証連携ポリシ203aにより、利用数が上限を超えた場合でも、IDプロバイダ内の利用状況3aに合わせて、必要に応じた素早いサービス利用が開始可能となっている。

[0203] 換言すると、認証連携ポリシ203内の各認証連携ポリシ203aのうちのいずれかの認証連携ポリシ203aは、サービスプロバイダIDに関連付けて、当該サービスプロバイダIDで識別されるサービスプロバイダ装置300によるサービスデータ303aの送信が許可されるユーザの所属及び役職と、当該ユーザの人数が上限値を超えた場合には当該ユーザの中で最終利用日から現在までの期間が所定期間以上であるユーザが存在することと、当該存在するユーザのユーザ属性部分情報302aを無効化すること(例、図4のBの[4])とを示している。なお、ここでいう「ユーザの人数」は、サービス利用状況ストリーム202内の「現在の利用数」に等しい値を意味している。

[0204] これに伴い、サービスプロバイダ装置300の利用状況ストリーム304は、図25に示すように、ユーザ利用管理テーブル304aにおいて、前述した記憶内容に加え、ユーザIDと、サービスデータ303aを送信した最終の日付を示す最終利用日とを含む最終利用日情報とを記憶する。

[0205] また、利用状況提供部308は、IDプロバイダ装置200から最終利用日送信要求を受けると、利用状況ストリーム304内の最終利用日情報当該IDプロバイダ装置200に送信する機能をもっている。

一方、ＩＤプロバイダ装置２００の認証連携ポリシ評価部２０９は、前述した機能に加え、認証連携ハンドリング部２０８から送出されたポリシ評価要求内のサービスプロバイダＩＤに基づいてサービス利用状況ストア２０２から利用数及び上限値を読み出す機能と、当該送出されたポリシ評価要求内のサービスプロバイダＩＤに基づいて、当該サービスプロバイダＩＤで識別されるサービスプロバイダ装置３００に対し、最終利用日送信要求を送信し、当該サービスプロバイダ装置３００から最終利用日情報を受信する機能とをもっている。なお、受信した最終利用日情報は、図２６に示すように、ユーザＩＤとサービスプロバイダＩＤとに関連付けてサービス状況ストア２０２内のユーザ利用管理テーブル２０２ａに書き込んでもよいが、必ずしも書き込まなくてもよい。

[0206] また、認証連携ポリシ評価部２０９の前述した送信許可判定機能は、認証連携ポリシストア２０３から読み出した認証連携ポリシ２０３ａにユーザの所属及び役職と利用数の上限値を超えた場合に所定期間以上であるユーザが存在することと当該存在するユーザのユーザ属性部分情報３０２ａを無効化することとが含まれる場合、当該読み出した認証連携ポリシ２０３ａに示される所属及び役職に対してＩｄＰユーザリポジトリ２０１から読み出したユーザ属性情報２０１ａ内の所属及び役職が適合するか否かと、サービス利用状況ストア２０２から読み出した利用数が当該サービス利用状況ストア２０２から読み出した上限値を超えた場合に最終利用日送信要求をサービスプロバイダ装置２００に送信して当該サービスプロバイダ装置２００から受けた最終利用日情報内の最終利用日が読み出した認証連携ポリシ２０３ａ内の所定期間以上に適合するか否かとに応じてサービスデータ３０３ａの送信を許可するか否かを判定する機能とをもっている。

[0207] 次に、以上のように構成された認証連携システムの動作について前述した図１７を主に参照して説明する。

[0208] 今、ステップＳＴ１０のユーザ認証（ＳＴ１１～ＳＴ１８）は、前述した通りに実行される。

- [0209] 続いて、ステップS T 2 0の認証連携ポリシー評価においては、ステップS T 2 1（ポリシー評価要求）及びステップS T 2 2（サービス利用状況の検索）が前述同様に実行される。このステップS T 2 2では、ポリシー評価要求内のサービスプロバイダIDに基づいてサービス利用状況ストア2 0 2から利用数及び上限値が読み出される。
- [0210] ステップS T 2 3では、認証連携ポリシー評価部2 0 9は、認証連携ハンドリング部2 0 8から送出されたポリシー評価要求内のユーザIDとサービスプロバイダIDとに基づいて、当該サービスプロバイダIDで識別されるサービスプロバイダ装置3 0 0に対し、最終利用日送信要求を送信する。
- [0211] サービスプロバイダ装置3 0 0の利用状況提供部3 0 8は、この最終利用日送信要求を受けると、利用状況ストア3 0 4内の最終利用日情報をIDプロバイダ装置2 0 0に送信する。
- [0212] IDプロバイダ装置2 0 0の認証連携ポリシー評価部2 0 9は、この最終利用日情報を受信する。
- [0213] 次に、ステップS T 2 4（ユーザ属性情報2 0 1 aの検索）及びステップS T 2 5（認証連携ポリシー2 0 3 aの検索）が前述同様に実行される。但し、認証連携ポリシー2 0 3 aは、サービスプロバイダIDに関連付けて、当該サービスプロバイダIDで識別されるサービスプロバイダ装置3 0 0によるサービスデータ3 0 3 aの送信が許可されるユーザの所属及び役職と、当該ユーザの人数が上限値を超えた場合には当該ユーザの中で最終利用日から現在までの期間が所定期間以上であるユーザが存在することと、当該存在するユーザのユーザ属性部分情報3 0 2 aを無効化すること（例、図4のBの[4]）とを示しているものとする。
- [0214] ステップS T 2 6では、認証連携ポリシー評価部2 0 9が、図4の2 0 3 a Bで示す認証連携ポリシーに基づいて、連携の可否を決定する。認証連携ポリシーストア2 0 3から読み出した認証連携ポリシー2 0 3 aにユーザの所属及び役職と利用数の上限値を超えた場合に所定期間以上であるユーザが存在することと当該存在するユーザのユーザ属性部分情報3 0 2 aを無効化すること

とが含まれる場合、当該読み出した認証連携ポリシ２０３aに示される所属及び役職に対してＩｄＰユーザーゾトリ２０１から読み出したユーザー属性情報２０１a内の所属及び役職が適合するか否かと、サービス利用状況ストア２０２から読み出した上限値を超えた場合に最終利用日送信要求をサービスプロバイダ装置２００に送信して当該サービスプロバイダ装置２００から受けた最終利用日情報内の最終利用日が読み出した認証連携ポリシ２０３a内の所定期間以上に適合するか否かとに応じてサービスデータ３０３aの送信を許可するか否かを判定する。

[0215] ストップＳＴ２７（ポリシ評価応答）では、認証連携ポリシ評価部２０９が下した許可に加えて、図４の認証連携ポリシ２０３aにおけるＢ〔４〕からの「半年以上に渡ってサービス未使用のユーザーのＳＰアカウントを無効化する」との責務条件付きの評価結果を、認証連携ポリシ評価部２０９が認証連携ハンドリング部２０８に返す。このとき、無効化対象ユーザーのユーザＩＤも当該評価結果には付与される。

[0216] 以降のストップＳＴ３０のアカウント連携（ＳＴ３１～ＳＴ３７）及びストップＳＴ４０の認証連携（ＳＴ４１～ＳＴ４９）の処理は、前述した通り実行される。なお、本実施形態では、認証連携ポリシの評価結果として条件が含まれるため、ストップＳＴ３３（ユーザー属性情報の検索）とストップＳＴ３４（ＳＰアカウント連携要求メッセージ送信）において、次のような処理が加わる。

[0217] まず、ストップＳＴ３３においては、ＩｄＰアカウントプロビジョニング部２１０が、当該ユーザーの属性部分情報とアカウント登録指示に加えて、更に無効化対象ユーザーのアカウントを無効化するアカウント更新指示も付加して、アカウント連携要求メッセージを作成する。

- [0218] 上述したように本実施形態によれば、第１の実施形態の効果に加え、利用数が上限を超えた場合に、遊休ユーザのアカウントを無効化して空いた枠を申請ユーザのアカウントに割り当てる旨の責務条件を認証連携ポリシー２０３aに加えた構成により、利用数が上限を超えた場合でも、ＩＤプロバイダ内の利用状況に合わせて、素早くサービス利用を開始することができる。
- [0219] 以上説明した少なくとも一つの実施形態によれば、サービスプロバイダＩＤ毎に、サービスデータ３０３aの送信が許可されるユーザの所属及び役職を示す複数の認証連携ポリシー２０３aを記憶する認証連携ポリシーストア２０３と、読み出した認証連携ポリシー２０３aに示される所属及び役職に対し、読み出したユーザ属性情報２０１a内の所属及び役職が適合するか否かに応じて、サービスデータ３０３aの送信を許可するか否かを判定する認証連携ポリシー評価部２０９とを備えた構成により、ＳＳＯの過程でアカウント登録及び連携を実行する際に、人手を介さずにサービス利用可否を決定することができる。
- [0220] 補足すると、従来のデータ処理システムにおいては、サービスプロバイダがアカウントを登録するための十分な情報を保持していないことを確認し、不足したユーザ属性をＩＤプロバイダに要求する手間がかかり、このような確認や要求に人手を介していた。
- [0221] 一方、少なくとも一つの実施形態では、前述した予め認証連携ポリシー２０３aを記憶した構成により、従来のような確認や要求に人手を介することがない。
- [0222] 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。
- [0223] 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。

[0224] 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。

[0225] 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または一時記憶した記憶媒体も含まれる。

[0226] 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。

[0227] 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。

[0228] 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。

[0229] 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。

請求の範囲

[請求項1]

ユーザが操作するユーザ端末にログイン処理を実行可能で第1メモリを有するIDプロバイダ装置と、前記ログイン処理が成功した場合に前記ユーザ端末にサービスデータを送信可能で第2メモリを有する複数のサービスプロバイダ装置とを備えた認証連携システムであって、

前記IDプロバイダ装置は、

前記ユーザを特定するためのユーザ属性の項目名と前記ユーザ属性の項目値とを関連付けたユーザ属性情報であって、少なくとも前記ユーザを識別するユーザIDを前記項目名に含む複数の前記ユーザ属性情報を記憶するユーザ属性情報記憶手段と、

前記ユーザIDと、前記各サービスプロバイダ装置を識別するサービスプロバイダIDと、前記サービスデータの送信が許可された場合を示すサービス利用中、又は前記サービスデータの送信が許可されていない場合を示すサービス未利用のいずれかを示すサービス利用状況とを関連付けて記憶するサービス利用状況記憶手段と、

前記サービスプロバイダID毎に、当該サービスプロバイダIDで識別されるサービスプロバイダ装置によるサービスデータの送信が許可される対象となるユーザを示す複数のポリシー情報を記憶するポリシー記憶手段と、

前記サービスプロバイダIDと、前記ユーザ属性情報内のユーザ属性の項目名のうち、一部の項目名とを関連付けて記憶する一部項目名記憶手段と、

自装置の署名生成鍵を記憶する鍵記憶手段と、

いずれかの前記サービスプロバイダ装置から送信されて当該サービスプロバイダ装置のサービスプロバイダIDと前記ユーザ端末のアドレス情報とを含む認証連携要求を受けると、当該認証連携要求内のユーザ端末のアドレス情報を含むユーザ認証要求を送出する手段と、

前記送出されたユーザ認証要求内のユーザ端末のアドレス情報に基づいて、当該ユーザ端末にログイン要求を送信し、当該ユーザ端末から受けたユーザID及びユーザ認証情報を前記ユーザ属性情報記憶手段内のユーザID及び参照情報に基づいて認証するログイン処理を実行する手段と、

前記ログイン処理が成功したとき、当該ログイン処理に用いたユーザIDと前記認証連携要求内のサービスプロバイダIDとを含むポリシ評価要求を送出する手段と、

前記送出されたポリシ評価要求内のユーザIDに基づいて前記ユーザ属性記憶手段からユーザ属性情報を読み出す手段と、

前記送出されたポリシ評価要求内のサービスプロバイダIDに基づいて前記ポリシ記憶手段からポリシ情報を読み出す手段と、

前記読み出したポリシ情報に対して、前記読み出したユーザ属性情報、ユーザが利用したいサービスの種類、ユーザが行いたいサービスへの操作、サービスを実行するに際してのユーザの環境条件に適合するか否かに応じて、前記サービスデータの送信を許可するか否かを判定する送信許可判定手段と、

この判定結果を含むポリシ評価応答を前記ポリシ評価要求の送信元に送出する手段と、

前記ポリシ評価応答内の判定結果が許可を示す場合、前記ポリシ評価要求内のユーザIDとサービスプロバイダIDとを含むアカウント連携要求を送出する手段と、

前記送出されたアカウント連携要求内のサービスプロバイダIDに基づいて、前記一部項目名記憶手段からユーザ属性の一部の項目名を読み出す手段と、

当該読み出した一部の項目名と前記アカウント連携要求内のユーザIDとに基づいて、前記ユーザ属性記憶手段内で当該ユーザIDに一致するユーザIDを含むユーザ属性情報のうち、当該一部の項目名に

一致する項目名及びこの項目名に関連付けられた項目値からなるユーザ属性部分情報を取得する手段と、

前記取得したユーザ属性部分情報にアカウント登録指示を付加してアカウント連携要求メッセージを作成する手段と、

前記アカウント連携要求メッセージを前記認証連携要求の送信元のサービスプロバイダ装置に送信する手段と、

前記アカウント連携要求メッセージの送信先のサービスプロバイダ装置から当該サービスプロバイダ装置のサービスプロバイダIDと前記ユーザ属性部分情報内のユーザIDとを含む登録完了が通知されると、当該登録完了を示すアカウント連携応答を送出する手段と、

前記送出されたアカウント連携応答内の登録完了に含まれるサービスプロバイダID及びユーザIDに基づいて、前記サービス利用状況記憶手段内のサービス利用状況をサービス未利用からサービス利用中に更新する手段と、

前記送出されたアカウント連携応答内の登録完了に含まれるサービスプロバイダID及びユーザIDを含む認証連携実行要求を送出する手段と、

前記認証連携実行要求を受けると、当該認証連携実行要求内のサービスプロバイダIDで識別されるサービスプロバイダ装置と自装置との間で共有する認証連携IDを発行し、この認証連携IDと当該認証連携実行要求内のユーザIDとを関連付けて前記第1メモリに書き込む手段と、

前記発行した認証連携IDと、前記ログイン処理の認証方式名とを含むアサーション本文に対して前記署名生成鍵に基づくデジタル署名を生成し、当該アサーション本文と当該デジタル署名とを含む認証アサーションを作成する手段と、

前記作成した認証アサーションを含む認証連携応答を前記認証連携要求の送信元のサービスプロバイダ装置に送信する手段と

を備え、

前記各サービスプロバイダ装置は、

前記ユーザ属性情報記憶手段内のユーザ属性情報内のユーザ属性の項目名及び項目値のうちの一部の項目名と項目値とを関連付けたユーザ属性部分情報と、自装置内でユーザを識別するＳＰ側ユーザＩＤとを関連付けて記憶するユーザ属性部分情報記憶手段と、

前記ログイン処理が成功した場合にサービスデータの送信を許可するログイン処理の認証方式名と、前記署名生成鍵に対応する署名検証鍵とを含む認証アサーション検証ポリシーを記憶する検証ポリシー記憶手段と、

前記サービスデータを記憶するサービスデータ記憶手段と、

前記ユーザ端末からサービス要求を受けると、当該サービス要求が認証トークンを含むか否かを判定し、前記認証トークンを含む場合には当該認証トークンと前記サービスデータ記憶手段内のサービスデータとを当該ユーザ端末に送信し、否の場合には自装置のサービスプロバイダＩＤと当該ユーザ端末のアドレス情報とを含む認証連携要求を前記ＩＤプロバイダ装置に送信する手段と、

前記アカウント連携要求メッセージを受信すると、新規の前記ＳＰ側ユーザＩＤを発行し、当該発行したＳＰ側ユーザＩＤと、当該アカウント連携要求メッセージ内のユーザ属性部分情報とを関連付けて前記ユーザ属性部分情報記憶手段に登録する手段と、

この登録の後、登録したユーザ属性部分情報内のユーザＩＤと自装置のサービスプロバイダＩＤとを含む登録完了を前記アカウント連携要求メッセージの送信元のＩＤプロバイダ装置に通知する手段と、

前記ＩＤプロバイダ装置から認証連携応答を受けると、当該認証連携応答内の認証アサーションから認証連携ＩＤを抽出し、当該抽出した認証連携ＩＤと、前記登録されたユーザ属性部分情報内のユーザＩＤとを関連付けて前記第２メモリに書き込む手段と、

前記認証アサーション検証ポリシー内の認証方式名と署名検証鍵とに基づいて、前記認証アサーション内の認証方式名とデジタル署名とをそれぞれ検証する検証手段と、

前記検証した結果がいずれも正当のとき、認証トークンを発行し、この認証トークンを前記認証連携IDに関連付けて前記第2メモリに書き込む手段と、

前記書き込まれた認証トークンと、当該認証トークンに前記第2メモリ内で前記認証連携IDを介して関連付けられたユーザIDとを含むサービス実行要求を送出する手段と、

前記送付されたサービス実行要求に基づいて、当該サービス実行要求内の認証トークンと前記サービスデータ記憶手段内のサービスデータとを前記ユーザ端末に送信する手段と

を備えたことを特徴とする認証連携システム。

[請求項2]

請求項1に記載の認証連携システムにおいて、

前記各サービスプロバイダ装置は、

前記ユーザIDと、前記サービス利用中の状態に対して累積した利用料金とを関連付けて記憶する利用料金記憶手段と、

前記IDプロバイダ装置からユーザIDを含む利用料金送信要求を受けると、この利用料金送信要求内のユーザIDに基づいて前記利用料金記憶手段を検索し、当該検索により得られた利用料金及び当該ユーザIDを含む利用料金応答を当該IDプロバイダ装置に送信する手段と

を更に備え、

前記IDプロバイダ装置は、

前記各ポリシー情報のうちのいずれかのポリシー情報は、前記サービスプロバイダIDに関連付けて、当該サービスプロバイダIDで識別されるサービスプロバイダ装置によるサービスデータの送信が許可される対象となるユーザの環境条件と、当該ユーザの利用料金の上限値と

を示しており、

前記送出されたポリシー評価要求内のユーザIDとサービスプロバイダIDとに基づいて、当該サービスプロバイダIDで識別されるサービスプロバイダ装置に対し、当該ユーザIDを含む利用料金送信要求を送信し、当該サービスプロバイダ装置から当該ユーザID及び利用料金を含む利用料金応答を受信する手段と

を更に備え、

前記送信許可判定手段は、前記読み出したポリシー情報に対して前記読み出したユーザ属性情報、ユーザが利用したいサービスの種類、ユーザが行いたいサービスへの操作、サービスを実行するに際してのユーザの環境条件に適合するか否かと、当該読み出したポリシー情報に示される利用料金の上限値に対して前記受信した利用料金応答内の利用料金が適合するか否かとに応じて、前記サービスデータの送信を許可するか否かを判定することを特徴とする認証連携システム。

[請求項3]

請求項1に記載の認証連携システムにおいて、

前記各ポリシー情報のうちのいずれかのポリシー情報は、前記サービスプロバイダIDに関連付けて、当該サービスプロバイダIDで識別されるサービスプロバイダ装置によるサービスデータの送信が許可される対象となるユーザの環境条件と、当該ユーザの人数が上限値を超えた場合には当該ユーザの中で最終利用日から現在までの期間が所定期間以上であるユーザが存在することと、当該存在するユーザのユーザ属性部分情報を無効化することとを示しており、

前記各サービスプロバイダ装置は、

前記ユーザIDと、前記サービスデータを送信した最終の日付を示す最終利用日とを含む最終利用日情報を記憶する最終利用日記憶手段と、

前記IDプロバイダ装置から最終利用日送信要求を受けると、前記最終利用日記憶手段内の最終利用日情報を当該IDプロバイダ装置に

送信する手段と、

を更に備え、

前記ＩＤプロバイダ装置は、

前記サービスプロバイダＩＤと、当該サービスプロバイダＩＤに関連付けられた前記サービス利用状況が示す前記サービス利用中の個数
を示していて前記ユーザの人数に等しい利用数と、前記利用数の上限
値とを関連付けて記憶するサービス利用数記憶手段と、

前記送出されたポリシー評価要求内のサービスプロバイダＩＤに基づ
いて前記サービス利用数記憶手段から利用数及び上限値を読み出す手
段と、

前記送出されたポリシー評価要求内のサービスプロバイダＩＤに基づ
いて、当該サービスプロバイダＩＤで識別されるサービスプロバイダ
装置に対し、前記最終利用日送信要求を送信し、当該サービスプロバ
イダ装置から前記最終利用日情報を受信する手段と

を更に備え、

前記送信許可判定手段は、

前記読み出したポリシー情報にユーザの利用数の上限値を超えた場合
に前記所定期間以上であるユーザが存在することと当該存在するユー
ザのユーザ属性部分情報を無効化することとが含まれる場合、前記読
み出したポリシー情報に対して前記読み出したユーザ属性情報、ユーザ
が利用したいサービスの種類、ユーザが行いたいサービスへの操作、
サービスを実行するに際してのユーザの環境条件に適合するか否かと
、前記サービス利用数記憶手段から読み出した利用数が当該サービス
利用数記憶手段から読み出した上限値を超えた場合に前記最終利用日
送信要求をサービスプロバイダ装置に送信して当該サービスプロバイ
ダ装置から受けた最終利用日情報内の最終利用日が前記読み出したポ
リシ情報内の所定期間以上に適合するか否かとに応じて、前記サービ
スデータの送信を許可するか否かを判定する手段と、

この判定の結果が許可を示す場合、当該判定に用いた所定期間以上のユーザのユーザIDを含む無効化要求を前記サービスプロバイダ装置に送信する手段と

を備えたことを特徴とする認証連携システム。

[請求項4]

ユーザが操作するユーザ端末にログイン処理を実行可能で第1メモリを有するIDプロバイダ装置における前記ログイン処理が成功した場合に前記ユーザ端末にサービスデータを送信可能で第2メモリを有する複数のサービスプロバイダ装置に通信可能な前記IDプロバイダ装置であって、

前記ユーザを特定するためのユーザ属性の項目名と前記ユーザ属性の項目値とを関連付けたユーザ属性情報であって、少なくとも前記ユーザを識別するユーザIDを前記項目名に含む複数の前記ユーザ属性情報を記憶するユーザ属性情報記憶手段と、

前記ユーザIDと、前記各サービスプロバイダ装置を識別するサービスプロバイダIDと、前記サービスデータの送信が許可された場合を示すサービス利用中、又は前記サービスデータの送信が許可されていない場合を示すサービス未利用のいずれかを示すサービス利用状況とを関連付けて記憶するサービス利用状況記憶手段と、

前記サービスプロバイダID毎に、当該サービスプロバイダIDで識別されるサービスプロバイダ装置によるサービスデータの送信が許可される対象となるユーザの環境条件を示す複数のポリシー情報を記憶するポリシー記憶手段と、

前記サービスプロバイダIDと、前記ユーザ属性情報内のユーザ属性の項目名のうち、一部の項目名とを関連付けて記憶する一部項目名記憶手段と、

自装置の署名生成鍵を記憶する鍵記憶手段と、

いずれかの前記サービスプロバイダ装置から送信されて当該サービスプロバイダ装置のサービスプロバイダIDと前記ユーザ端末のアド

レス情報とを含む認証連携要求を受けると、当該認証連携要求内のユーザ端末のアドレス情報を含むユーザ認証要求を送出する手段と、

前記送付されたユーザ認証要求内のユーザ端末のアドレス情報に基づいて、当該ユーザ端末にログイン要求を送信し、当該ユーザ端末から受けたユーザID及びユーザ認証情報を前記ユーザ属性情報記憶手段内のユーザID及び参照情報に基づいて認証するログイン処理を実行する手段と、

前記ログイン処理が成功したとき、当該ログイン処理に用いたユーザIDと前記認証連携要求内のサービスプロバイダIDとを含むポリシー評価要求を送出する手段と、

前記送付されたポリシー評価要求内のユーザIDに基づいて前記ユーザ属性記憶手段からユーザ属性情報を読み出す手段と、

前記送付されたポリシー評価要求内のサービスプロバイダIDに基づいて前記ポリシー記憶手段からポリシー情報を読み出す手段と、

前記読み出したポリシー情報に対し、前記読み出したユーザ属性情報、ユーザが利用したいサービスの種類、ユーザが行いたいサービスへの操作、サービスを実行するに際してのユーザの環境条件に適合するか否かに応じて、前記サービスデータの送信を許可するか否かを判定する送信許可判定手段と、

この判定結果を含むポリシー評価応答を前記ポリシー評価要求の送信元に送付する手段と、

前記ポリシー評価応答内の判定結果が許可を示す場合、前記ポリシー評価要求内のユーザIDとサービスプロバイダIDとを含むアカウント連携要求を送付する手段と、

前記送付されたアカウント連携要求内のサービスプロバイダIDに基づいて、前記一部項目名記憶手段からユーザ属性の一部の項目名を読み出す手段と、

当該読み出した一部の項目名と前記アカウント連携要求内のユーザ

ＩＤとに基づいて、前記ユーザ属性記憶手段内で当該ユーザＩＤに一致するユーザＩＤを含むユーザ属性情報のうち、当該一部の項目名に一致する項目名及びこの項目名に関連付けられた項目値からなるユーザ属性部分情報を取得する手段と、

前記取得したユーザ属性部分情報にアカウント登録指示を付加してアカウント連携要求メッセージを作成する手段と、

前記アカウント連携要求メッセージを前記認証連携要求の送信元のサービスプロバイダ装置に送信する手段と、

前記アカウント連携要求メッセージの送信先のサービスプロバイダ装置から当該サービスプロバイダ装置のサービスプロバイダＩＤと前記ユーザ属性部分情報内のユーザＩＤとを含む登録完了が通知されると、当該登録完了を示すアカウント連携応答を送出する手段と、

前記送出されたアカウント連携応答内の登録完了に含まれるサービスプロバイダＩＤ及びユーザＩＤに基づいて、前記サービス利用状況記憶手段内のサービス利用状況をサービス未利用からサービス利用中に更新する手段と、

前記送出されたアカウント連携応答内の登録完了に含まれるサービスプロバイダＩＤ及びユーザＩＤを含む認証連携実行要求を送出する手段と、

前記認証連携実行要求を受けると、当該認証連携実行要求内のサービスプロバイダＩＤで識別されるサービスプロバイダ装置と自装置との間で共有する認証連携ＩＤを発行し、この認証連携ＩＤと当該認証連携実行要求内のユーザＩＤとを関連付けて前記第１メモリに書き込む手段と、

前記発行した認証連携ＩＤと、前記ログイン処理の認証方式名とを含むアサーション本文に対して前記署名生成鍵に基づくデジタル署名を生成し、当該アサーション本文と当該デジタル署名とを含む認証アサーションを作成する手段と、

前記作成した認証アサーションを含む認証連携応答を前記認証連携要求の送信元のサービスプロバイダ装置に送信する手段と

を備え、

前記各サービスプロバイダ装置は、

前記ユーザ端末からサービス要求を受けると、当該サービス要求が認証トークンを含むか否かを判定し、前記認証トークンを含む場合には当該認証トークンと前記サービスデータ記憶手段内のサービスデータとを当該ユーザ端末に送信し、否の場合には自装置のサービスプロバイダIDと当該ユーザ端末のアドレス情報とを含む認証連携要求を前記IDプロバイダ装置に送信し、

前記アカウント連携要求メッセージを受信すると、新規の前記SP側ユーザIDを発行し、当該発行したSP側ユーザIDと、当該アカウント連携要求メッセージ内のユーザ属性部分情報とを関連付けて登録し、

この登録の後、登録したユーザ属性部分情報内のユーザIDと自装置のサービスプロバイダIDとを含む登録完了を前記アカウント連携要求メッセージの送信元のIDプロバイダ装置に通知し、

前記IDプロバイダ装置から認証連携応答を受けると、当該認証連携応答内の認証アサーションから認証連携IDを抽出し、当該抽出した認証連携IDと、前記登録されたユーザ属性部分情報内のユーザIDとを関連付けて前記第2メモリに書き込むと、予め記憶した認証アサーション検証ポリシー内の認証方式名と署名検証鍵とに基づいて、前記認証アサーション内の認証方式名とデジタル署名とをそれぞれ検証し、

前記検証した結果がいずれも正当のとき、認証トークンを発行し、この認証トークンを前記認証連携IDに関連付けて前記第2メモリに書き込むと、前記書き込まれた認証トークンと、当該認証トークンに前記第2メモリ内で前記認証連携IDを介して関連付けられたユーザ

ＩＤとを含むサービス実行要求を送出し、前記送出されたサービス実行要求に基づいて、当該サービス実行要求内の認証トークンと予め記憶したサービスデータとを前記ユーザ端末に送信することを特徴とするＩＤプロバイダ装置。