

明 細 書

発明の名称： 認証連携システムおよびＩＤプロバイダ装置

技術分野

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

背景技術

[0002] 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認証連携を行うための技術として、シングルサインオン（Single Sign On、以下ＳＳＯという）がある。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い。

[0003] しかし、最近では、異なるドメイン間（異なるWWWサーバ間の意味であり、以下、クロスドメインという）でのＳＳＯが求められている。その理由として、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。

[0004] しかしながら、クロスドメインのＳＳＯを実現するためには、認証結果を共有するために大きな手間が発生するという問題がある。主な問題点としては以下の２点が挙げられる。

[0005] 第１の問題点は、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。第２の問題点は、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、単純に導入することはできず、別途施策を用意する必要があることである。

[0006] これらの問題点を解消するため、ＳＳＯの標準化の要望がある。この要望に応じる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 St

structured Information Standards) が策定した SAML (Security Assertion Markup Language) がある。

[0007] 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、以下、IDP、もしくは ID プロバイダという)、サービス提供者 (Service Provider、以下、SP もしくは 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。

[0008] ユーザが 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 (以下、アカウント連携という) である。これら信頼関係の構築およ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ユーザが SSO を開始することはできない。

[0009] 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、ユーザ端末を介した、サービスプロバイダ開始モデルの SSO の手順を説明する。

[0010] (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。

[0011] (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、ユーザ側の端末を介して、認証リクエストを ID プロバイダに送る。

[0012] (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。

[0013] (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、ユーザ端末を介してサービスプロバイダに返信する。

[0014] (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。

[0015] (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。

[0016] なお、ユーザがSSO要求をしたときの起点として、SAMLではサービスプロバイダ開始モデル（以下、SP開始モデルという）とIDプロバイダ開始モデル（以下、IDP開始モデル）の2つが定義されている。SP開始モデルは、前述したSSO手順の通りであり、ユーザがSPにアクセスし、SPがSAMLに基づいた認証リクエストを送信するところから、SSO要求が始まるモデルである。

[0017] IDP開始モデルは、前述のSSO手順（1）において、ユーザ端末からIDプロバイダに対して、サービスプロバイダのサービス提供を要求するところから始まるモデルである。したがって、SSO手順（2）は行われず、手順（1）に続いて（3）～（6）の処理を行う。

[0018] 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、複数のサービスを使用可能となる。

[0019] 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。

- [0020] 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 S P M L (S e r v i c e P r o v i s i o n i n g M a r k u p L a n g u a g e) がある。
- [0021] 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 S S O 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 S S O 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。
- [0022] 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 S S O 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 I D プロバイダにユーザ属性を要求し、I D 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、S S O の過程でアカウント登録および連携を実行する。
- [0023] しかしながら、例えば企業において所定のユーザが S a a S を利用する場合、管理部門がサービスプロバイダに対して、事前のアカウント登録やアカウント連携を一括して行う必要がある。もしくは各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サービスプロバイダ利用申請手続きを経た後、管理部門がサービスプロバイダに対して、申請したユーザに関する事前のアカウント登録や連携を行うことになる。このような事前処理を経た後にユーザは、サービスプロバイダが提供するサービスを利用可能となる。
- [0024] ここで、前者の事前処理を行う場合は、S S O の過程でアカウント登録および連携を実行する必要がないので、前述したデータ処理システムとは無関係である。一方、後者の承認フローを通す場合は、ユーザだけでなく、ユーザ所属先の上長や管理部門など多くの人手を介すことになり、手間暇を要す

る。更に、管理部門が行うアカウント登録や連携を一括して行なわない場合、人手による作業が発生し、負担も大きい。そのため、効率が悪く、利便性も悪い。

[0025] SaaSなどにおいては、使いたいときに素早く使える点がメリットの1つである。しかし、後者の承認フローを通す場合には、人手による作業が発生し、負担も大きいため、このメリットを生かすことができない。そのため、SSOの過程でアカウント登録およ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。

[0026] しかしながら、この仕組みを実現するためには上記のSAML機能を実装したIDプロバイダの改造が必要であり、その導入コストは大きい。

先行技術文献

特許文献

[0027] 特許文献1：特表2008-538247号公報

非特許文献

[0028] 非特許文献1：“Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0”, OASIS Standard, 15 March 2005, <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

[0029] 本発明が解決しようとする課題は、ＩＤプロバイダ装置を改造する必要がないため導入が容易であり、かつ、ＳＳＯの過程でアカウント登録および連携を実行する際に入手を介さないでサービス利用可否の決定を行うことができる認証連携システムおよび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

[0030] 実施形態のＩＤプロバイダ装置は、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ポリシー情報を記憶するポリシー情報記憶部と、認証連携要求を受信した場合に、ユーザ端末のログイン状態に応じたタイミングでポリシー評価処理とアカウント連携処理とを行なう認証連携要求事前処理部と、サービスプロバイダ装置から認証連携要求を受信した場合に、当該認証連携要求を認証連携要求事前処理部に転送する認証連携要求転送部と、を備える。

図面の簡単な説明

[0031] [図1]第１の実施形態に係る認証連携システムのハードウェア構成の一例を示すブロック図。

[図2]第１の実施形態に係るＩＤプロバイダ装置の転送先ＵＲＬ管理テーブルの一例を示す図。

[図3]第１の実施形態に係るＩＤプロバイダ装置のＩＤＰ認証連携部の機能構成の一例を示すブロック図。

[図4]第１の実施形態に係るＩＤプロバイダ装置のＩＤＰユーザストアの一例を示す図。

[図5]第１の実施形態に係るＩＤプロバイダ装置の認証アサーションの一例を示す図。

[図6]第１の実施形態に係るＩＤプロバイダ装置の認証連携制御システムの機能構成の一例を示すブロック図。

[図7]第１の実施形態に係るＩＤプロバイダ装置の認証セッション一時記憶装置の一例を示すブロック図。

[図8]第1の実施形態に係るIDプロバイダ装置のポリシストアの一例を示す図。

[図9]第1の実施形態に係るサービスプロバイダ装置のSPユーザストアの一例を示すブロック図。

[図10]第1の実施形態に係るサービスプロバイダ装置のサービスデータストアの一例を示すブロック図。

[図11]第1の実施形態に係るサービスプロバイダ装置の検証ポリシストアの一例を示すブロック図。

[図12]第1の実施形態に係るサービスプロバイダ装置の一時記憶装置の一例を示す図。

[図13]第1の実施形態に係る認証連携システムの動作の一例を示すシーケンス図。

[図14]第1の実施形態に係る認証連携システムの動作の一例を示すシーケンス図。

[図15]第1の実施形態に係る認証連携システムの動作の一例を示すシーケンス図。

[図16]第2の実施形態に係る認証連携システムの機能構成の一例を示すブロック図。

[図17]第2の実施形態に係る認証連携システムの動作の一例を示すシーケンス図。

[図18]第2の実施形態に係る認証連携システムの動作の一例を示すシーケンス図。

[図19]第2の実施形態に係る認証連携システムの動作の一例を示すシーケンス図。

[図20]第3の実施形態に係る認証連携システムの機能構成の一例を示すブロック図。

[図21]第3の実施形態に係る認証連携システムの機能構成の一例を示すブロック図。

[図22]第3の実施形態に係る認証連携システムの動作の一例を示すシーケンス図。

[図23]第3の実施形態に係る認証連携システムの動作の一例を示すシーケンス図。

[図24]第3の実施形態に係る認証連携システムの動作の一例を示すシーケンス図。

[図25]第4の実施形態に係る認証連携システムの機能構成の一例を示すブロック図。

[図26]第4の実施形態に係る認証連携システムの動作の一例を示すシーケンス図。

発明を実施するための形態

[0032] 以下、図面を参照して本発明の実施形態に係る認証連携システムについて説明する。

[0033] (第1の実施形態)

以下、図1乃至図15を参照して本実施形態の認証連携システムについて説明する。

[0034] 図1は、本実施形態の認証連携システムの基本構成を示すブロック図である。この認証連携システムは、ユーザが操作するユーザ端末100に対してログイン処理を実行可能なIDプロバイダ装置200と、ログイン処理が成功した場合にユーザ端末100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、複数台あってもよいが、ここでは1台のみを図示している。また、ユーザ端末100と、IDプロバイダ装置200と、サービスプロバイダ装置300とは、それぞれネットワークを介して接続されても良い。

[0035] ユーザ端末100は、通常のコンピュータ機能を有し、IDプロバイダ装置200およびサービスプロバイダ装置300と通信可能な装置であり、ユーザの操作に応じて、サービスプロバイダ装置300の利用を要求するSP利用要求をサービスプロバイダ装置300に送信する機能と、ユーザ端末1

００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、ユーザインタフェース機能と、を備える。

[0036] ＩＤプロバイダ装置２００は、ログイン処理、すなわちサービスプロバイダ装置３００が提供するサービスを利用するユーザの認証を行う。また、ＩＤプロバイダ装置２００は、後述するポリシ情報に基づき、サービスプロバイダへのユーザのアカウント登録とアカウント連携とを行う。

[0037] ＩＤプロバイダ装置２００は、ポータルサーバ２１０、Ｗｅｂサーバ２２０、ＩＤＰ認証連携部２３０、認証連携制御システム２４０、ＩＤＰユーザストア２５０、ポリシストア２６０、認証セッション一時記憶装置（第１メモリ）２７０、および鍵記憶装置２８０を備えている。

[0038] ポータルサーバ２１０はユーザに、アクセス先のサービスプロバイダを表示する。

[0039] Ｗｅｂサーバ２２０は、リバースプロキシ装置（第１のメッセージ転送部）２２１と転送先ＵＲＬ記憶装置２２２を備え、ユーザ端末１００からのメッセージを受信する。

[0040] すなわち、Ｗｅｂサーバ２２０がメッセージを受信すると、リバースプロキシ装置２２１は、転送先ＵＲＬ記憶装置２２２を参照して受信したメッセージを転送する。

[0041] 図２は転送先ＵＲＬ記憶装置２２２に記憶された転送先ＵＲＬ管理テーブル２２３の一例である。図２に示すように本実施形態の転送先ＵＲＬ管理テーブル２２３は、インターネット公開ＵＲＬと転送先ＵＲＬとが対応付けられて記憶され、各インターネット公開ＵＲＬと転送先ＵＲＬにはＩＤが付与されている。すなわち、リバースプロキシ装置２２１は、ユーザ端末１００からｗｅｂサーバ２２０が受信したメッセージに対応するインターネット公開ＵＲＬを検索し、検索結果に対応する転送先ＵＲＬに当該メッセージを転

送する。

[0042] IDP認証連携部230は、SSOのIDプロバイダ機能を有する。ここで、図3を参照して、IDP認証連携部230の構成の一例について説明する。

[0043] 図3に示すように、本実施形態のIDプロバイダ装置200のIDP認証連携部230は、認証連携要求メッセージ受信部232、ログイン要求メッセージ送信部233、ログイン応答メッセージ受信部234、および認証連携応答メッセージ送信部235を備える。

[0044] 認証連携要求メッセージ受信部232は、後述するサービスプロバイダ装置300のSP認証連携部330から認証連携要求メッセージを受信する。認証連携要求メッセージは例えば、HTTPリクエストの形態であり、サービスプロバイダ装置300がユーザ端末100からサービス利用要求を受信した場合に、IDプロバイダ装置200に認証連携を要求するために発行するメッセージである。また、認証連携要求メッセージ受信部232は、ユーザ端末のログイン状態を確認し、ログイン完了状態であれば、後述する認証連携応答メッセージ送信部235にユーザを認証したことを示す認証連携応答メッセージの作成を依頼する。

[0045] ログイン要求メッセージ送信部233は、ログイン未完了のユーザ端末100にログイン要求メッセージを送信する。

[0046] ログイン応答メッセージ受信部234は、ログイン要求メッセージへの応答情報として、ユーザ端末100によって入力されたログイン応答メッセージを受信し、ユーザのログイン処理を行う。

[0047] 具体的には、ログイン応答メッセージ受信部234は、当該ユーザ端末100から、ログイン要求メッセージへの応答情報としてユーザIDおよびユーザ認証情報を含むログイン応答メッセージを受信した場合に、IDプロバイダユーザストア250（以下、IDPユーザストア250という）内のユーザIDおよび参照情報に基づいて認証する処理である。ここで、図4を参照して、IDPユーザストア250について説明する。

- [0048] IDプロバイダ装置200は、IDユーザストア250は、IDプロバイダ装置200に所属するユーザに関する属性情報（以下、ユーザ属性情報という）を記憶する。
- [0049] 図4に示すように、IDユーザストア250は、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251を記憶する。ユーザ属性情報251は、例えばユーザを識別するユーザIDと、ユーザの氏名と、ユーザの従業員番号と、ユーザの所属部と、ユーザの所属課と、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をした際に参照する参照情報と、ユーザの電話番号と、を項目名に含む。なお、IDユーザストア250にユーザ属性情報251は複数記憶されているが、図4にはその一例を示している。
- [0050] すなわち、ユーザ属性情報251は個人の情報を特徴付ける情報の集合体である。なお、ユーザ属性情報251はこれらには限らず、例えば勤務状態といった任意の項目名と項目値とを更に含んでもよい。また、ユーザのログイン処理をした際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。
- [0051] 認証連携応答メッセージ送信部235は、認証連携要求メッセージ受信部232から認証連携応答メッセージ作成依頼を受信した場合に、IDプロバイダ装置200でユーザを認証したことを示す認証アサーションを含む認証連携応答メッセージを作成する。認証アサーションとは、サービスプロバイダ装置300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。
- [0052] ここで、図5に本実施形態のIDP認証連携部230が作成する認証アサーション231の一例を示す。
- [0053] 図5に示すように、認証アサーション231は、認証連携IDと、ログイン処理の認証方式名を含むアサーション本文と、デジタル署名と含む。認証連携IDとは、IDプロバイダ装置200とサービスプロバイダ装置300の双方で、それぞれのユーザID（ユーザIDとSP側ユーザID）を紐付

けるためのIDであり、後述するアカウントプロビジョニング部247によって発行される。認証連携IDは、例えば、新規に発行してもよいし、IDプロバイダ装置200のユーザIDを指定してもよいし、IDプロバイダ装置200とサービスプロバイダ装置300間で共通のユーザ属性情報251であるメールアドレスを指定してもよい。なお、認証連携IDは、後述の認証連携応答確認処理で、サービスプロバイダ装置300が、利用要求してきたユーザを識別するために使用する。デジタル署名は、IDP認証連携部230によって当該アサーション本文に対して鍵記憶装置280内の署名生成鍵に基づいて生成される。

[0054] なお、鍵記憶装置280は、IDプロバイダ装置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。

[0055] また、認証連携応答メッセージ送信部235は、作成した認証連携応答メッセージをSP認証連携部330に対して送信する。

[0056] 続いて、図6を参照して、認証連携制御システム240の構成の一例について説明する。

[0057] 図6に示すように、認証連携制御システム240は、認証連携要求メッセージ事前処理部241と、ポリシ評価情報取得部245と、ポリシ評価部246と、アカウントプロビジョニング部247とを備える。

[0058] 認証連携要求メッセージ事前処理部241は、ログイン状態判定部242と、ユーザID取得部243と、認証連携要求メッセージ転送部（第2のメッセージ転送部）244とを備え、ユーザ端末100からIDプロバイダ装置200が認証連携要求メッセージを受信した場合に事前処理を行う。事前処理については後述する。

[0059] ログイン状態判定部242はユーザ端末100から、例えばHTTPリクエストの形態である認証連携要求メッセージを受信した場合に、HTTPリクエストに含まれるCookieに格納されたIDP認証トークンを参照してログイン状態を判定する。IDP認証トークンは、後述するログイン処

理が行われるとIDプロバイダ装置200が発行する。すなわち、HTTPリクエスト中のCookieにIDP認証トークンが含まれる場合、IDプロバイダ装置200においてユーザがログイン完了状態である。なお、このCookieには当該IDP認証トークンが発行されたユーザを示すユーザIDが含まれる。

[0060] このCookieは、例えばIDプロバイダ装置に備えられたRAMのようなメモリに格納される。以下、Cookieが格納されたメモリを認証セッション一時記憶装置270という。図7に認証セッション一時記憶装置270の一例を示す。

[0061] ユーザID取得部243は、ログイン状態判定部242がログイン完了状態であると判定した場合に、当該認証連携要求メッセージからIDP認証トークンに対応したユーザIDを取得する。

[0062] 認証連携要求メッセージ転送部244は、IDプロバイダ装置200内には存在しないURL（以下、ダミーURLという）に認証連携要求メッセージを転送する。転送先のダミーURLはあらかじめ設定されており、ここではダミー（1）URLであるとする。

[0063] ポリシ評価情報取得部245は、IDPユーザストア250と、後述するサービス利用状況データストア320とからポリシ評価情報を取得する。ポリシ評価情報とはIDPユーザストア250に記憶されたユーザ属性情報251と後述するSPサービスストア320に記憶されたユーザのサービス利用状況情報321～324を含む情報である。

[0064] ポリシ評価部246は、ポリシ評価情報取得部245が取得したポリシ評価情報と、ポリシストア260で管理されるポリシ情報とに基づいて、サービスプロバイダ300を利用しようとするユーザの利用可否を判断する。

[0065] 本実施形態のポリシストア260は、通信が許可される対象となるユーザを示す複数のポリシ情報を記憶する。図8にポリシストア260の一例を示す。

[0066] 図8に示すように、ポリシストア260は、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および役職を示す複数の認証連携ポリシー（以下、ポリシー情報という）261（262、263、264、・・・）を記憶する。

[0067] なお、ポリシーストア260は、ユーザの所属および役職といった静的なポリシー（例えば、図8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8中のCの[4]）を含んでもよい。

[0068] 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8中のBの[4]の[責務条件]）。

[0069] アカウントプロビジョニング部247は、ポリシー評価部246の利用可否の判断結果に基づき、IDPユーザストア250からユーザ属性情報251を取得し、取得したユーザ属性情報251を用いて、SPユーザストア310に対してアカウント登録を行う。すなわち、アカウントプロビジョニング部247は、認証連携IDを発行する。また、アカウントプロビジョニング部247は、IDPユーザストア250とSPユーザストア310の両方に対して、アカウント連携を行う。

[0070] 上述のような構成によって、認証連携制御システム240は、ユーザがSSOを要求したときもしくはSSO処理の途中で行われるログインのタイミングで、ポリシー情報に基づき後述するアカウント登録処理とアカウント連携処理を行う。

- [0071] ここでポリシ情報とは、誰（どのユーザ）が、どのサービスプロバイダ装置に、どのような操作（アクション）を行うことができるか否かが定義された、ユーザのサービスプロバイダ利用可否条件の集合体を指す。言い換えると、ポリシ情報とは、サービスプロバイダ装置300に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。また、ポリシ情報には、オプションとして環境条件や責務条件についても定義されるものもある。
- [0072] 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る。サービスプロバイダ装置300は、サービスプロバイダ（以下、SPと記載する）ユーザストア310、サービス利用状況データストア320、SP認証連携部330、検証ポリシストア340、一時記憶装置（第2メモリ）350を備えている。
- [0073] SPユーザストア310は、ユーザ属性部分情報記憶手段として機能する。なお、ユーザ属性部分情報とは、IDPユーザストア250内のユーザ属性情報251内のユーザ属性の項目名および項目値のうちの一部の項目名と項目値とである。このユーザ属性部分情報とサービスプロバイダ装置300におけるユーザID（以下、SP側ユーザIDという）と関連付けた情報をアカウント登録情報という311という。
- [0074] すなわち、SPユーザストア310は、サービスプロバイダ300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。なお、SPユーザストア310は、ユーザ属性部分情報ではなく、ユーザ属性情報251すべてをSP側ユーザIDに関連付けて記憶しても良い。
- [0075] 具体的には、SPユーザストア310は、図9に示すように、認証連携IDと氏名とアドレス情報と電話番号などのユーザ属性情報の一部と、サービスプロバイダ装置300内でユーザを識別するSP側ユーザIDとを関連付けたアカウント登録情報311記憶している。
- [0076] サービス利用状況データストア320は、図10に示すように、サービスプロバイダ装置300ごとの、ユーザ利用管理テーブル321と、利用数管理テーブル322と、ディスク使用量管理テーブル323と、課金料金管理

テーブル 3 2 4 とを記憶し、ユーザのサービス利用状況を監視している。

[0077] ユーザ利用管理テーブル 3 2 1 は、S P 側ユーザ I D 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、また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。

[0078] 利用数管理テーブル 3 2 2 は、ユーザ利用管理テーブル 3 2 1 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。

[0079] ディスク使用量管理テーブル 3 2 3 は、ユーザ利用管理テーブル 3 2 1 内のサービス利用状況が示すサービス利用中のサービスデータが使用しているディスク容量と、サービスプロバイダ装置 3 0 0 におけるディスク容量の上限値とを関連付けて書き込まれる。課金料金管理テーブル 3 2 4 は、ユーザ利用管理テーブル 3 2 1 内のサービス利用状況が示すサービス利用中のサービスに課金された料金の合計と、サービスプロバイダ装置 3 0 0 における課金料金上限値とを関連付けて書き込まれる。サービスデータストア 3 2 2 には、これらの管理テーブル 3 2 1 ~ 3 2 4 の他に、例えばライセンス数を管理するテーブルを記憶しても良い。

[0080] S P 認証連携部 3 3 0 は、S S O のサービスプロバイダ機能を有する。S P 認証連携部 3 3 0 は、具体的には、認証連携応答確認処理と、S P 利用応答処理を行う。

[0081] 認証連携応答確認処理は、後述する検証ポリシーストア 3 4 0 内の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、I D プロバイダ装置 2 0 0 の I D P 認証連携部 2 3 0 が作成する認証アサーション 2 3 1 の認証方式名とデジタル署名とをそれぞれ検証し、検証した結果がいずれも正当のとき、S P 認証トークンを発行し、この S P 認証トークンを認証連携 I D および S P 側ユーザ I D に関連付けて一時記憶装置 3 5 0 に書き込む処理である。

[0082] S P 利用応答処理は、この認証連携応答確認処理において S P 認証トーク

ンが発行された場合に、ユーザ端末１００にサービスプロバイダ装置３００が利用可能であると応答する処理である。

[0083] 図１１に示すように検証ポリシストア３４０は、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、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３４１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。

[0084] 一時記憶装置３５０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、登録されたアカウント登録情報３１１内の認証連携ＩＤと、ＳＰ側のユーザＩＤと、発行されたＳＰ認証トークンとを関連付けて記憶する。

[0085] ここで、本実施形態の認証連携システムの認証連携処理について図１３乃至図１５を参照して説明する。

[0086] なお、本実施形態では、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ＳＳＯ処理が可能な状態であり、かつ当該ＩＤプロバイダ側の組織に所属するユーザが当該サービスプロバイダ装置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、ユーザのログイン状態と、ユーザからのＳＳＯ要求起点にはさまざまな組み合わせがあるが、本実施形態ではユーザのログイン状態は完了状態であり、かつユーザからのＳＳＯ要求起点がサービスプロバイダ装置３００から開始とする。

[0087] また、本実施形態の認証連携システムにおいては、ＳＳＯは上述した（１）～（６）の手順で行なわれるとする。

[0088] この状態において、ユーザがサービスプロバイダ装置３００にサービス利用要求をしたときに、ＳＳＯ処理を実行し、サービスプロバイダ装置３００のサービスを利用可能とする本実施形態の認証連携システムの動作について説明する。

[0089] 図１３乃至図１５は本実施形態の認証連携システムの動作の一例を示すシ

ーケンス図である。なお、シーケンス図にはステップ番号を付与しており、小さい番号から順に処理が行われるとする。

- [0090] 図13に示すように、ステップS1では、ユーザが、アカウントが未登録のサービスプロバイダ装置300のサービスを利用するために、ユーザ端末100を操作し所望のサービスプロバイダ装置300にサービス要求を行なう。サービスプロバイダ装置300へのサービス要求は、例えば、ユーザ端末100の表示部（図示しない）に表示されたサービス公開URLのリンクのうち、ユーザの所望のリンクを、入力部（図示しない）を用いてクリックする。
- [0091] ステップS2ではユーザ端末100は、ユーザの操作により、サービスプロバイダ装置300にサービス要求（以下、SP利用要求メッセージという）を送信する。サービスプロバイダ装置300は、アクセス管理を担うSP認証連携部330がSP利用要求メッセージを受信する。
- [0092] ステップS3では、SP利用要求メッセージを受信したSP認証連携部330が、ユーザの認証連携状態を確認する。認証連携状態の確認は、例えば、ユーザからのSP利用要求メッセージが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、SP認証連携部330が発行したSP認証トークンが存在するかどうかで判断する。
- [0093] 当該SP認証トークンが存在すれば、SP認証連携部330は、ユーザ端末100の認証連携が完了した状態とみなす。一方、当該SP認証トークンが存在しない場合は、SP認証連携部330は、ユーザ端末100の認証連携が未完了の状態とみなし、ユーザ端末のアドレス情報を含む認証連携要求メッセージを作成する。本実施形態では、認証連携が未完了状態とする。
- [0094] ステップS4では、SP認証連携部330が、ステップS3での認証連携状態の確認結果、認証連携が未完了状態であるため、「IDP認証連携部230の認証連携要求メッセージ受信部232」を宛先とした認証連携要求メッセージを発行し、ユーザ端末100に送信する。
- [0095] ステップS5では、ユーザ端末100が、認証連携要求メッセージを受信

すると、指定された宛先（ここでは、IDP認証連携部230の認証連携要求メッセージ受信部232）にリダイレクトする。

[0096] ステップS6では、ステップS5においてユーザ端末100によってリダイレクトされた認証連携要求メッセージを、一旦Webサーバ220が受信する。Webサーバ220が認証連携要求メッセージを受信すると、リバースプロキシ装置221が、転送先URL記憶装置222に記憶された転送先URL管理テーブル223に基づいて、メッセージ転送の可否判定を行う。判定方法は、転送先URL管理テーブル223のインターネット公開URLフィールドの中に、受信した認証連携要求メッセージの宛先と適合するURLを検索する。ここでは、No. 1のID「1-A」が適合するため、転送先はID「1-B」の「認証連携制御システム240の認証連携要求メッセージ事前処理部241」となる。

[0097] ステップS7では、Webサーバ220が、リバースプロキシ装置221を通じて、前ステップの判定において転送先と判定されたID「1-B」の「認証連携制御システム240の認証連携要求メッセージ事前処理部241」を宛先として、認証連携要求メッセージを転送する。続いて、図14の処理に進む。

[0098] 図14のステップS8では、転送された認証連携要求メッセージを受信した認証連携要求メッセージ事前処理部241のログイン状態判定部242が、ユーザのログイン状態を判定する。ログイン状態の確認は、認証セッション一時記憶装置270におけるIDP認証トークンの有無によって確認する。本実施形態によると、ログイン完了状態であるため、認証セッション一時記憶装置270にIDP認証トークンが存在する。したがって、ログイン状態判定部242はログイン完了状態と判定し、判定結果をユーザID取得部243に送信する。

[0099] 続いて、ステップS9では、ユーザID取得部243が、認証セッション一時記憶装置270から、ステップS8において確認されたIDP認証トークンと対応付けられたユーザIDを取得する。

- [0100] ステップS 1 0では、認証連携要求メッセージ事前処理部2 4 1が、ポリシ評価情報取得部2 4 5に対し、ポリシ評価情報の取得を依頼する。このとき、ステップS 9で取得したユーザIDもポリシ評価情報取得部2 4 5に送信する。
- [0101] ステップS 1 1では、ポリシ評価情報取得部2 4 5が、サービスプロバイダ装置3 0 0のサービス利用状況データストア3 2 0にアクセスし、サービス利用状況情報3 2 1～3 2 4を取得する（以下、サービス利用状況情報取得処理という）。
- [0102] ステップS 1 2では、ポリシ評価情報取得部2 4 5が、認証連携要求メッセージ事前処理部2 4 1から受信したユーザIDを検索キーとして、図4に示したIDPユーザストア2 5 0から、ユーザ属性情報2 5 1を取得する（以下、ユーザ属性情報取得処理という）。
- [0103] ステップS 1 3では、認証連携要求メッセージ事前処理部2 4 1は、ポリシ評価部2 4 6に対し、ポリシ評価の実行を依頼する。このとき、ステップS 1 1の実行によって得られたサービス利用状況情報3 2 1～3 2 4と、ステップS 1 2の実行によって得られたユーザ属性情報2 5 1を、ポリシ評価情報としてまとめ、それをポリシ評価部2 4 6に引き渡す。
- [0104] ステップS 1 4では、ポリシ評価部2 4 6は、図8のポリシストア2 6 0から、ユーザが指定したサービスプロバイダ装置3 0 0に関するポリシ情報2 6 1を取得する。
- [0105] ステップS 1 5では、ポリシ評価部2 4 6が、ステップS 1 3で取得されたポリシ評価情報と、ステップS 1 4で取得したポリシ情報を使って、ポリシ評価を行う。以下、ステップS 1 3～ステップS 1 5の処理をポリシ評価処理という。
- [0106] ポリシ評価処理の結果、当該ユーザのサービス利用可否が決定する。本実施形態では、サービス利用が許可されたとする。
- [0107] ステップS 1 6では、サービス利用が許可の場合、認証連携要求メッセージ事前処理部2 4 1のアカウントプロビジョニング部2 4 7が、当該ユーザ

に関するアカウントプロビジョニングを実施する。このとき、ステップS 12で取得されたユーザIDも送信する。

[0108] ステップS 17では、アカウントプロビジョニング部247が、ステップS 16で受信したユーザIDを検索キーとして、IDPユーザストア250から当該ユーザのユーザ属性情報251の一部の属性情報であるユーザ属性部分情報を取得する。

[0109] ステップS 18では、アカウントプロビジョニング部247が、当該ユーザのSP側ユーザIDを作成し、取得したユーザ属性部分情報と対応付けてSPユーザストア310に登録するとともに、IDプロバイダ装置200とサービスプロバイダ装置300の両アカウントを紐付ける認証連携IDも登録する。本実施形態では、認証連携IDとして、IDプロバイダ装置200のユーザIDを指定する。

[0110] 以下、ステップS 16～ステップS 18の処理をアカウントプロビジョニング処理（アカウント連携処理）という。続いて、図15のステップS 19の処理に進む。

[0111] 図15のステップS 19では、認証連携要求メッセージ事前処理部241の認証連携要求メッセージ転送部244が、IDプロバイダ装置200内には存在しないダミーのURLを宛先として、ユーザ端末100に向けて認証連携要求メッセージを転送する。ここでは、ダミーのURLはダミー（1）URLであるとする。

[0112] ステップS 20では、認証連携要求メッセージを受信したユーザ端末100が、指定のURL、すなわち、ダミー（1）URLに認証連携要求メッセージをリダイレクトする。

[0113] ステップS 21では、Webサーバ220が、ユーザ端末100によってリダイレクトされた認証連携要求メッセージを一旦受信する。Webサーバ220のリバースプロキシ装置221は、転送先URL記憶装置222に保存された転送先URL管理テーブル223に基づいたメッセージ転送の要否判定を行う。なお、判定方法は、転送先URL管理テーブル223のインタ

ーネット公開URLフィールドの中から、ステップS20で受信した認証連携要求メッセージの宛先と適合するURLを検索する。ここでは、ID「1-C」が適合するため、転送先はID「1-D」、すなわちIDP認証連携部230の認証連携要求メッセージ受信部232となる。続いて、メッセージ転送処理が行われる。

[0114] ステップS22では、Webサーバ220のリバースプロキシ装置221が、ステップS21の判定結果に基づいて、IDP認証連携部230の認証連携要求メッセージ受信部232を宛先として、認証連携要求メッセージを転送する。

[0115] ステップS23では、IDP認証連携部230の認証連携要求メッセージ受信部232が、認証連携要求メッセージを受信後、ユーザのログイン状態を確認する。ログイン状態の確認は、例えば認証セッション一時記憶装置270にユーザに発行されたIDP認証トークンが記憶されているか否かを確認することによって行なう。本実施形態ではログイン完了状態としているためIDP認証トークンが存在する。

[0116] ステップS24では、IDP認証連携部230の認証連携要求メッセージ受信部232が、ログイン状態の確認後、ログイン完了状態であるため、認証連携応答メッセージ送信部235に対し、認証連携応答メッセージの送信を要求する。認証連携応答メッセージとは、サービスプロバイダ300に、IDプロバイダ装置200でユーザを認証したことを示す認証アサーションを含む。

[0117] ステップS25では、認証連携応答メッセージ送信部235が、IDプロバイダ装置200側でユーザを認証したことを証明する認証アサーションを作成し、作成した認証アサーションを含める認証連携応答メッセージを作成する。作成した認証連携応答メッセージはSP認証連携部330を宛先として、ユーザ端末100に送信する。

[0118] ステップS26では、ユーザ端末100が、指定の宛先であるSP認証連携部330に対し、受信した認証連携応答メッセージをリダイレクトする。

- [0119] ステップS 2 7 では、認証連携応答メッセージを受信した S P 認証連携部 3 3 0 が、認証連携応答確認処理を行い、確認結果に基づいて認証連携を行う。
- [0120] 認証連携応答確認処理では、具体的には、S P 認証連携部 3 3 0 は、受信したメッセージに含まれる認証アサーションの検証を行う。なお、認証アサーションの検証は、図 1 1 に示した検証ポリシストア 3 4 0 の認証アサーション検証ポリシーに従って行う。
- [0121] 検証の結果、問題がなければ、S P 認証連携部 3 3 0 は認証連携を完了し、S P 認証トークンを発行する。S P 認証連携部 3 3 0 が発行した S P 認証トークンは、例えば、H T T P C o o k i e やセッション情報に格納する。なお、ステップS 2 4 ~ S 2 7 の処理を認証連携応答処理という。
- [0122] ステップS 2 8 では、認証連携を完了した S P 認証連携部 3 3 0 が、ユーザ端末 1 0 0 に当該 S P 認証トークンとサービスデータとを含む S P 利用応答メッセージを送信し、ユーザに利用可能である旨を通知する S P 利用応答処理を行う。これによって、I D プロバイダ装置 2 0 0 所属のユーザとサービスプロバイダ装置 3 0 0 との間での S S O 処理が終了する。
- [0123] 上述のように、本実施形態の認証連携システムによると、I D プロバイダ装置 2 0 0 の組織に所属するユーザが、サービスプロバイダ装置 3 0 0 にアカウントが登録されていない状態であり、ユーザのログイン状態は完了状態であり、かつユーザからの S S O 要求起点がサービスプロバイダ装置 3 0 0 から開始する場合において、S S O の過程でアカウント登録および連携を実行する際の手を介さないサービス利用可否の決定を行うことが可能となる。
- [0124] 具体的には、本実施形態の認証連携システムは、S S O 処理手順（2）と（3）の間に、ポリシストア 2 6 0 に事前に記憶されたサービス利用に関するポリシー情報 2 6 1 とサービス利用状況データストア 3 2 0 の利用状況 3 2 1 ~ 3 2 4 に基づき、サービスプロバイダ装置 3 0 0 が提供するサービスを、認証連携要求を行なったユーザが利用可能か否かを評価した後、サービスプロバイダ装置 3 0 0 へのアカウント登録とアカウント連携を行う処理を割

り込ませることで、ユーザ端末１００を介したサービスプロバイダ装置３００が提供するサービスの利用申請からＳＳＯに至る一連の処理を自動化させることができる。したがって、本実施形態の認証連携システムによって、ユーザ所属の上長やＩＳ部門など人手を介することなく、ユーザがスムーズにサービス利用を開始できる。

[0125] また、本実施形態の認証連携システムによると、ＩＤプロバイダ装置２００の認証連携サーバ２３０が、ＳＳＯ手順（２）～（４）の処理を連続して行う中で、ＳＳＯ手順（３）の直前に、ポリシ評価、およびアカウント登録・アカウント連携を行なうアカウントプロビジョニング処理の割り込みをＩＤプロバイダ装置の認証連携サーバ製品を直接改造することなく実現することが可能となる。このため、導入コストも低く、容易に、かつ人手を介さずにサービス利用可否を決定できる認証連携システムの提供が可能となる。

[0126] また、本実施形態の認証連携システムによると、ユーザがＳＳＯを要求したときの起点が、サービスプロバイダ装置３００の動作が開始したときであって、ユーザのログインが完了である場合に、適切なタイミングで、ポリシ評価とアカウントプロビジョニングを実施できる。

[0127] （第２の実施形態）

第２の実施形態の認証連携システムについて図１６乃至図１９を参照して説明する。

[0128] 本実施形態は第１の実施形態と同様に、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ＳＳＯ処理が可能な状態であり、かつ当該ＩＤプロバイダ装置２００が設置された組織に所属するユーザが当該サービスプロバイダ装置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、本実施形態の認証連携システムは第１の実施形態と同様に、ＳＳＯは上述した（１）～（６）の手順で行なわれるとする。

[0129] また、ユーザのログイン状態と、ユーザからのＳＳＯ要求起点にはさまざまな組み合わせがあるが、本実施形態ではユーザのログイン状態は未完了状態であり、かつユーザからのＳＳＯ要求起点がサービスプロバイダ装置３０

0から開始とする。

[0130] ここで、図16を参照して、本実施形態の認証連携システムの機能構成について説明する。なお、第1の実施形態と同一の構成には同一の符号を付し、説明は省略する。

[0131] 図16は本実施形態の認証連携制御システム240の機能構成の一例を示す図である。図16に示すように、本実施形態の認証連携制御システム240は、ポリシー評価情報取得部245と、ポリシー評価部246と、アカウントプロビジョニング部247と、ログイン応答メッセージ事前処理部290を備える。

[0132] ログイン応答メッセージ事前処理部290は、認証情報抽出部291と、認証識別部292と、ログイン応答メッセージ転送部293とを備える。

[0133] 認証情報抽出部291は、ユーザ端末100からログイン応答メッセージを受信した場合に、ログイン応答メッセージに含まれるユーザIDとパスワードとを認証情報として抽出する。なお、ログイン応答メッセージは、ユーザがログイン未完了の場合にIDプロバイダ装置200から送信されるログイン要求メッセージに応答するために、ユーザ端末100によって入力される。ログイン応答メッセージは、例えば、ユーザがログイン未完了の場合にユーザ端末100に表示されるログイン画面を介して入力される。ログイン画面には、具体的には、ユーザIDとパスワードを入力する欄が表示される。

[0134] 認証識別部292は、認証情報抽出部291によって抽出された認証情報と、図4に示したIDPユーザストア250に含まれるユーザIDおよび参照情報に基づいてユーザの認証と識別を行う。

[0135] 具体的に、認証識別部292は、認証情報抽出部291が抽出したユーザIDに基づいてIDPユーザストア250を検索し、ユーザIDが一致するユーザ属性情報に含まれる参照情報と認証情報抽出部291が抽出したパスワードが一致するかを判定する。

[0136] ログイン応答メッセージ転送部293は、ダミーURLにログイン応答メ

ッセージを転送する。

[0137] 図 17 乃至図 19 を参照して、ユーザがサービスプロバイダ装置 300 にサービス利用要求をしたときに、SSO 処理を実行し、サービスプロバイダ装置 300 のサービスを利用可能とする、本実施形態の認証連携システムの認証連携処理について説明する。図 17 乃至図 19 は、本実施形態の認証連携処理の一例を示すシーケンス図である。

[0138] なお、本実施形態の認証連携処理は、図 13 に示したステップ S1 ～ステップ S7 の処理に続いて、図 17 乃至図 19 に示したステップ S30 ～ステップ S50 の処理を行う。

[0139] ステップ S1 ～ステップ S7 の処理は第 1 の実施形態と同様であるため省略し、図 17 のステップ S30 から説明する。

[0140] ステップ S30 では、本実施形態のログイン状態判定部 242 がログイン状態は未完了状態であると判定し、判定結果を認証連携要求メッセージ転送部 244 に送信する。

[0141] ステップ S31 では、認証連携要求メッセージ転送部 244 が、認証連携要求メッセージをダミー URL 宛に転送する。ここでは、ダミーの URL はダミー (1) URL であるとする。

[0142] ステップ S32 では、認証連携要求メッセージを受信したユーザ端末 100 が、指定の URL、すなわち、ダミー (1) URL に認証連携要求メッセージをリダイレクトする。

[0143] ステップ S33 では、Web サーバ 220 が、ユーザ端末 100 によってリダイレクトされた認証連携要求メッセージを一旦受信する。Web サーバ 220 のリバースプロキシ装置 221 は、転送先 URL 記憶装置 222 に保存された転送先 URL 管理テーブル 223 に基づいたメッセージ転送の要否判定を行う。ここでは、ID「1-C」が適合するため、転送先は ID「1-D」、すなわち IDP 認証連携部 230 の認証連携要求メッセージ受信部 232 となる。続いて、メッセージ転送処理が行われる。

[0144] ステップ S34 では、Web サーバ 220 のリバースプロキシ装置 221

が、ステップS 3 3の判定結果に基づいて、IDP認証連携部230の認証連携要求メッセージ受信部232を宛先として、認証連携要求メッセージを転送する。

[0145] ステップS 3 5では、IDP認証連携部230の認証連携要求メッセージ受信部232が、認証連携要求メッセージを受信後、ユーザのログイン状態を確認する。ログイン状態の確認は図14のステップS 8と同様の処理であるため、説明は省略する。本実施形態では、ログイン未完了である。

[0146] ステップS 3 6では、ステップS 3 5の判定結果に基づいて、ログイン要求メッセージ送信部233が、ユーザ端末100にログイン要求メッセージを送信する。

[0147] ステップS 3 7では、ログイン要求メッセージを受信したユーザ端末100に、ログイン画面が表示され、ユーザが当該ログイン画面を介してユーザIDとパスワードとを入力する。

[0148] ステップS 3 8では、ユーザ端末100が、ステップS 3 7で入力された当該ユーザIDとパスワードとを含むログイン応答メッセージをIDP認証連携部230のログイン応答メッセージ受信部234を宛先として送信する。

[0149] 続いて図18のステップS 3 9に進む。

[0150] 図18のステップS 3 9ではWebサーバ220が、ステップS 3 8でユーザ端末100によって送信されたログイン応答メッセージを一旦受信する。また、Webサーバ220のリバースプロキシ装置221は、転送先URL記憶装置222に保存された転送先URL管理テーブル223に基づいて、当該ログイン応答メッセージの転送制御の要否判定を行う。なお、判定方法は、転送先URL管理テーブル223のインターネット公開URLフィールドの中から、受信したログイン応答メッセージの宛先と適合するURLを検索する。ここでは、ID「3-A」が適合するため、メッセージ転送要と判定される。なお、転送先URL管理テーブル223に一致するURLが存在しない場合は転送制御不要と判定される。

- [0151] ここでは、転送先はID「3-B」、すなわち認証連携システム240のログイン応答メッセージ事前処理部290となる。続いて、メッセージ転送処理が行われる。
- [0152] ステップS40では、Webサーバ220のリバースプロキシ装置221が、ステップS39の判定結果に基づいて、ログイン応答メッセージ事前処理部290を宛先として、ログイン応答メッセージを転送する。
- [0153] ステップS41では、ログイン応答メッセージ事前処理部291の認証情報抽出部291が、受信したログイン応答メッセージから、ユーザIDとパスワードを認証情報として抽出する。
- [0154] ステップS42では、ログイン応答メッセージ事前処理部291の認証識別部292が、ステップS41で抽出されたユーザIDを検索キーとして、IDPユーザストア250のユーザ属性情報を検索し、パスワードを取得する。
- [0155] ステップS43では、ログイン応答メッセージ事前処理部291の認証識別部292が、取得したパスワードと、ログイン応答メッセージから抽出されたパスワードとを照合し、ユーザの認証を行うとともに、ユーザIDによるユーザの識別を行う。本実施形態では、ユーザを認証できたとする。
- [0156] ステップS44では、ログイン応答メッセージ事前処理部291が、ポリシ評価情報取得部245に、ポリシ評価情報の取得要求を送信する。このとき、ログイン応答メッセージから取得されたユーザIDもともに送信する。
- [0157] ステップS44の処理に引き続いて、図14のステップS11のサービスデータ取得処理、図14のステップS12のユーザ属性情報取得処理、ステップS13～S15のポリシ評価処理、およびステップS16～S18のアカウントプロビジョニング処理は行われる。これらの処理は第1の実施形態で説明済みであるため省略する。
- [0158] 続いて、図19のステップS45では、ログイン応答メッセージ事前処理部291のログイン応答メッセージ転送部293が、IDプロバイダ装置200内には存在しないダミーのURLを宛先として、ユーザ端末100に向

けてログイン応答メッセージを転送する。なお、本実施形態ではログイン応答メッセージ転送部293が転送するダミーのURLはあらかじめ設定されており、「ダミー(3)URL」であるとする。

[0159] ステップS46では、ログイン応答メッセージを受信したユーザ端末100が、宛先であるダミー(3)URLにログイン応答メッセージをリダイレクトする。

[0160] ステップS47では、Webサーバ220が、ユーザ端末100によってリダイレクトされたログイン応答メッセージを一旦受信する。ここで、Webサーバ220のリバースプロキシ装置221が、転送先URL記憶装置222に記憶された転送先URL管理テーブル223に基づき、メッセージ転送の要否判定を行う。

[0161] 判定方法は、転送先URL管理テーブル223のインターネット公開URLフィールドの中の受信したログイン応答メッセージの宛先と一致するURLを検索し、一致するURLが存在する場合に「転送要」とする。ここでは、ID「3-C」が適合するため、転送先は対応する転送先URLのID「3-D」である。すなわち、リバースプロキシ装置221は、IDP認証連携部230のログイン応答メッセージ受信部234にログイン応答メッセージの転送が必要であると判定する。

[0162] ステップS48では、Webサーバ220のリバースプロキシ装置221が、ステップS47での判定結果に基づいて、IDP認証連携部230のログイン応答メッセージ受信部234を宛先として、ログイン応答メッセージを転送する。

[0163] ステップS49では、IDP認証連携部230のログイン応答メッセージ受信部234が、受信したログイン応答メッセージに基づいてログイン処理を行う。ログイン処理は、具体的には、ログイン応答メッセージ受信部234が、受信したログイン応答メッセージログインからユーザIDとパスワードを取得する。取得したユーザIDを検索キーとして、ログイン応答メッセージ受信部234がIDPユーザストア250からパスワードを取得し、ロ

グイン応答メッセージから抽出したパスワードと照合してユーザの認証を行う。なお、本実施形態では、ユーザの認証が確認できたとする。

[0164] ステップS50では、ログイン応答メッセージ受信部234が、IDプロバイダ装置200においてログインが完了したことを示すIDP認証トークンを発行し、ユーザIDとともに認証セッション一時記憶装置270に格納する。

[0165] ステップS50に続いて、図15のステップS24～ステップS27における認証連携応答処理とステップS28におけるSP利用応答処理を行い、本実施形態の認証連携処理は終了する。

[0166] 上述のように、本実施形態の認証連携システムによると、IDプロバイダ装置200の組織に所属するユーザがサービスプロバイダ装置300にアカウントが登録されていない状態であり、ユーザのログイン状態は未完了状態であり、かつユーザからのSSO要求起点がサービスプロバイダ装置300から開始する場合において、SSOの過程でアカウント登録および連携を実行する際の手を介さないサービス利用可否の決定を行うことが可能となる。

[0167] また、本実施形態の認証連携システムによると、IDプロバイダ装置200の組織に所属するユーザがサービスプロバイダ装置300にアカウントが登録されていない状態であり、ユーザのログイン状態は未完了状態であり、かつユーザからのSSO要求起点がサービスプロバイダ装置300から開始する場合において、適切なタイミングで、ポリシ評価とアカウントプロビジョニングを実施できる。

[0168] (第3の実施形態)

第3の実施形態の認証連携システムについて図20乃至図24を参照して説明する。

[0169] 本実施形態は第1の実施形態と同様に、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SSO処理が可能な状態であり、かつ当該IDプロバイダ装置200側の組織に所属するユーザが当該サービスプロバイダ装置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。

[0170] また、ユーザのログイン状態と、ユーザからのＳＳＯ要求起点にはさまざまな組み合わせがあるが、本実施形態ではユーザのログイン状態は完了状態であり、かつユーザからのＳＳＯ要求起点がＩＤプロバイダ装置２００から開始される（ＩＤＰ開始モデル）とする。

[0171] ＩＤＰ開始モデルは、前述のＳＳＯ手順（１）において、ユーザ端末からＩＤプロバイダに対して、サービスプロバイダのサービス提供を要求するところから始まるモデルである。したがって、本実施形態ではＳＳＯ手順（２）は行われず、手順（１）に続いて（３）～（６）の処理を行う。

[0172] ここで、図２０および図２１を参照して、本実施形態の認証連携システムの機能構成について説明する。なお、第１の実施形態および第２の実施形態と同一の構成には同一の符号を付し、説明は省略する。

[0173] 図２０は本実施形態のＩＤＰ認証連携部２３０の機能構成の一例を示す図である。

[0174] 図２０に示すように、本実施形態のＩＤＰ認証連携部２３０は、ログイン要求メッセージ送信部２３３と、ログイン応答メッセージ受信部２３４と、認証連携応答メッセージ送信部２３５と、認証連携応答発行要求メッセージ受信部２３６とを備える。

[0175] 認証連携応答発行要求メッセージ受信部２３６は、認証連携応答発行要求メッセージを受信する。なお、認証連携応答発行要求メッセージとは、ＩＤＰ開始モデルにおいて発行されるサービスプロバイダ装置３００への認証連携要求メッセージのことである。すなわち、ユーザ端末１００からサービス利用要求を受信したＩＤプロバイダ装置２００がサービスプロバイダ装置３００に認証連携を要求するために発行するメッセージである。

[0176] サービスプロバイダ装置３００が発行する認証連携要求メッセージをＳＰ認証連携要求メッセージといい、ＩＤプロバイダ装置２００が発行する認証連携要求メッセージ（認証連携応答発行要求メッセージ）をＩＤＰ認証連携要求メッセージとしてもよい。

[0177] 図２１は本実施形態の認証連携制御システム２４０の機能構成の一例を示

す図である。図 2 1 に示すように、本実施形態の認証連携制御システム 2 4 0 は、認証連携応答発行要求メッセージ事前処理部 2 9 4 を備える。

[0178] 認証連携応答発行要求メッセージ事前処理部 2 9 4 は、認証連携応答発行要求メッセージ転送部 2 9 5 を備え、受信した認証連携応答発行要求メッセージの転送処理を行う。

[0179] ここで、図 2 2 乃至図 2 4 を参照して、本実施形態における認証連携システムの認証連携処理について説明する。図 2 2 乃至図 2 4 は、本実施形態における認証連携処理の一例を示すシーケンス図である。

[0180] まず、ステップ S 6 1 では、ユーザが、サービスプロバイダ装置 3 0 0 のサービスを利用するために、ポータルサーバ 2 1 0 によってユーザ端末 1 0 0 に表示されたポータルメニュー画面を介して、サービスプロバイダ装置 3 0 0 が提供するサービス公開 URL のリンクのうち所望のリンクをクリックすることにより、ユーザ端末 1 0 0 に S P 利用要求が入力される。

[0181] ステップ S 6 2 では、ユーザ端末 1 0 0 がポータルサーバ 2 1 0 に S P 利用要求メッセージを送信する。

[0182] ステップ S 6 3 では、Webサーバ 2 2 0 が、ユーザ端末 1 0 0 から送信された S P 利用要求メッセージを受信し、受信した S P 要求メッセージの転送要否判定処理を行う。

[0183] 転送要否判定処理は、具体的には、Webサーバ 2 2 0 が備えるリバースプロキシ装置 2 2 1 が、転送先 URL 記憶装置 2 2 2 に記憶された転送先 URL 管理テーブル 2 2 3 に基づいて行う。例えば、図 2 の転送先 URL 管理テーブル 2 2 3 のインターネット公開 URL フィールドの中に、受信した S P 利用要求メッセージの宛先と適合する URL を検索する。ここでは宛先はポータルサーバ 2 2 0 であるが、図 2 のインターネット公開 URL フィールドの中に適合するものがないため、リバースプロキシ装置 2 2 1 は転送処理が不要であると判定する。

[0184] ステップ S 6 4 では、リバースプロキシ装置 2 2 1 が、ステップ S 6 3 での判定結果に基づいて、元々の宛先であるポータルサーバ 2 2 0 に S P 利用

要求メッセージを転送する。

- [0185] ステップS 6 5では、S P利用要求メッセージを受信したポータルサーバ2 2 0が、I D P認証連携部2 3 0の認証連携応答発行要求メッセージ受信部2 3 6を宛先とした認証連携応答発行要求メッセージを作成し、ユーザ端末1 0 0に送信する。すなわち、ポータルサーバ2 2 0は認証連携応答発行要求機能を備える。
- [0186] ステップS 6 6では、認証連携応答発行要求メッセージを受信したユーザ端末1 0 0が、指定された宛先である認証連携応答発行要求メッセージ受信部2 9 4にリダイレクトする。
- [0187] ステップS 6 7では、W e bサーバ2 2 0が、リダイレクトされた認証連携応答発行要求メッセージを受信し、受信したメッセージの転送要否判定処理を行う。
- [0188] 転送要否判定処理はステップS 6 3における処理と同様である。ここでは、宛先が、図2に示した転送先URL管理テーブル2 2 3のインターネット公開URLのI D「2 - A」と一致するため、リバースプロキシ装置2 2 1は転送要と判定する。また、転送先URLは、I D「2 - A」に対応するI D「2 - B」の転送先URLである。すなわち、転送先URLは、認証連携制御システム2 4 0の認証連携応答発行要求メッセージ事前処理部2 9 4である。
- [0189] ステップS 6 8では、リバースプロキシ装置2 2 1が、ステップS 6 7の判定結果に基づいて、認証連携制御システム2 4 0の認証連携応答発行要求メッセージ事前処理部2 9 4を宛先として、認証連携応答発行要求メッセージを転送する。
- [0190] 図2 3のステップS 6 9では、認証連携応答発行要求メッセージを受信した認証連携応答発行要求メッセージ事前処理部2 9 4のログイン状態判定部2 4 2が、ユーザのログイン状態を判定する。ログイン状態の確認は、認証セッション一時記憶装置2 7 0にユーザに発行されたI D P認証トークンが記憶されているか否かによって確認する。本実施形態では、認証セッション

一時記憶装置 270 に IDP 認証トークンが記憶されており、ログイン完了状態と判定される。

[0191] ステップ S70 では、ユーザ ID 取得部 243 が、認証セッション一時記憶装置 270 から、ステップ S69 における IDP 認証トークンに対応づけられたユーザ ID を取得する。

[0192] ステップ S71 では、認証連携応答発行要求メッセージ事前処理部 294 が、ポリシー評価情報取得部 245 にポリシー評価情報の取得を要求する。このとき、ステップ S70 で取得されたユーザ ID もポリシー評価情報取得部 245 に引き渡される。

[0193] ステップ S71 に引き続いて、図 14 のステップ S11 のサービスデータ取得処理、図 14 のステップ S12 のユーザ属性情報取得処理、ステップ S13～S15 のポリシー評価処理、およびステップ S16～S18 のアカウントプロビジョニング処理が行われる。これらの処理は第 1 の実施形態で説明済みであるため省略する。

[0194] 続いて、図 24 のステップ 72 の処理を行う。ステップ S72 では、ステップ S18 のアカウントプロビジョニング終了後に、認証連携応答発行要求メッセージ受信部 294 が、宛先がダミー URL である認証連携応答発行要求メッセージをユーザ端末 100 に送信する。なお、認証連携応答発行要求メッセージ受信部 294 が送信するダミー URL はあらかじめ設定されており、本実施形態では「ダミー（2）URL」である。

[0195] ステップ S73 では、認証連携応答発行要求メッセージを受信したユーザ端末 100 が、認証連携応答発行要求メッセージの宛先であるダミー（2）URL に、認証連携応答発行要求メッセージをリダイレクトする。

[0196] ステップ S74 では、リバースプロキシ装置 221 が、転送先 URL 記憶装置 223 に記憶された転送先 URL 管理テーブル 223 に基づいて、ユーザ端末 100 によってリダイレクトされた認証連携応答発行要求メッセージの転送要否判定処理を行う。

[0197] ここでは、転送先 URL 管理テーブル 223 に含まれるインターネット公

開URLのID「2-C」が適合するため、メッセージ転送制御が必要であると判定する。

[0198] 転送先は、ID「2-C」に対応した転送先URLである。すなわち、ID「2-D」のIDP認証連携部230の認証連携応答発行要求メッセージ受信部236である。

[0199] ステップS75では、リバースプロキシ装置221が、ステップS74の判定結果に基づいて、IDP認証連携部230の認証連携応答発行要求メッセージ受信部236を宛先として、認証連携応答発行要求メッセージを転送する。

[0200] ステップS76では、IDP認証連携部230の認証連携応答発行要求メッセージ受信部236が、認証連携応答発行要求メッセージを受信後、ユーザのログイン状態を判定する。ログイン状態判定結果は、例えば認証セッション時記憶装置270にユーザに発行されたIDP認証トークンが記憶されているか否かを確認することによって行なう。本実施形態ではログイン完了状態としているためIDP認証トークンが存在する。

[0201] ステップS77では、IDP認証連携部230の認証連携応答発行要求メッセージ受信部236が、ログイン状態の判定結果がログイン完了状態であるため、認証連携応答メッセージ送信部235に対し、認証連携応答メッセージの送信を要求する。認証連携応答メッセージ送信部235は、IDP側でユーザを認証したことを証明する認証アサーションを作成する。

[0202] ステップS77の処理に引き続き、図15のステップS25～ステップS28の処理が行われ、本実施形態の認証連携処理は終了する。ステップS25～S28の処理については第1の実施形態で説明しているため、省略する。

[0203] 上述のように、本実施形態の認証連携システムによると、IDプロバイダ装置200の組織に所属するユーザがサービスプロバイダ装置300にアカウントが登録されていない状態であり、ユーザのログイン状態は完了状態であり、かつユーザからのSSO要求起点がIDプロバイダ装置200から開始

する場合において、SSOの過程でアカウント登録および連携を実行する際の手人を介さないサービス利用可否の決定を行うことが可能となる。

[0204] また、本実施形態の認証連携システムによると、IDプロバイダ装置200の認証連携サーバ230が、SSO手順(2)～(4)の処理を連続して行う中で、SSO手順(3)の直前に、ポリシ評価、およびアカウント登録・アカウント連携を行なうアカウントプロビジョニング処理の割り込みをIDプロバイダ装置の認証連携サーバ製品を直接改造することなく実現することが可能となる。このため、導入コストも低く、かつ手人を介さずにサービス利用可否を決定できる認証連携システムの提供が可能となる。

[0205] また、本実施形態の認証連携システムによると、IDプロバイダ装置200の組織に所属するユーザがサービスプロバイダ装置300にアカウントが登録されていない状態であり、ユーザのログイン状態は完了状態でありかつユーザからのSSO要求起点がIDプロバイダ装置200から開始する場合において、適切なタイミングで、ポリシ評価とアカウントプロビジョニングを実施できる。

[0206] (第4の実施形態)

第4の実施形態の認証連携システムについて図25乃至図26を参照して説明する。

[0207] 本実施形態は第1の実施形態と同様に、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SSO処理が可能な状態であり、かつ当該IDプロバイダ側の組織に所属するユーザが当該サービスプロバイダ装置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、本実施形態の認証連携システムは第1の実施形態と同様に、SSOは上述した(1)～(6)の手順で行なわれるとする。

[0208] また、本実施形態ではユーザのログイン状態は未完了状態であり、かつユーザからのSSO要求起点がIDプロバイダ装置200から開始とする。

[0209] ここで、図25を参照して、本実施形態の認証連携システムの機能構成について説明する。なお、第1の実施形態乃至第3の実施形態と同一の構成に

は同一の符号を付し、説明は省略する。

[0210] 図 25 は、本実施形態の認証連携制御システム 240 の機能構成の一例を示す図である。図 25 に示すように、本実施形態の認証連携制御システム 240 は、ポリシー評価情報取得部 245 と、ポリシー評価部 246 と、アカウントプロビジョニング部 247 と、ログイン応答メッセージ事前処理部 290 と、認証連携応答発行要求メッセージ事前処理部 294 とを備える。すなわち、本実施形態の認証連携制御システム 240 は、第 2 の実施形態の認証連携制御システム 240 の認証連携要求メッセージ事前処理部 241 を第 3 の実施形態の認証連携制御システム 240 の認証連携応答発行要求メッセージ事前処理部 294 に置き換えて構成されている。

[0211] ここで、図 22、図 24、および図 26 を参照して、本実施形態の認証連携システムにおける認証連携処理の一例について説明する。図 26 は、本実施形態の認証連携処理の一例を示すシーケンス図である。

[0212] まず、本実施形態の認証連携システムは、図 22 のステップ S61 の SP 利用要求からステップ S68 の認証連携応答発行要求メッセージの転送までの処理を行なう。これらの処理は第 3 の実施形態で説明したため、省略する。

[0213] ステップ S68 に続いて、ステップ S81 では、携応答発行要求メッセージを受信した認証連携応答発行要求メッセージ事前処理部 294 のログイン状態判定部 242 が、ユーザのログイン状態を判定する。ログイン状態の確認は、認証セッション一時記憶装置 270 に、ユーザに発行された IDP 認証トークンが記憶されているか否かによって確認する。本実施形態では、認証セッション一時記憶装置 270 に IDP 認証トークンが記憶されておらず、ログイン未完了状態と判定される。

[0214] ステップ S81 でログイン未完了状態と判定されたため、続いて、図 24 に示したステップ S72～ステップ S75 の処理を行う。これらの処理も第 3 の実施形態で説明したため、省略する。

[0215] ステップ S75 に引き続いて、図 17 のステップ S35～図 19 のステッ

プS 2 8までの処理を行い、本実施形態の認証連携処理は終了する。図1 7のステップS 3 5～図1 9のステップS 2 8までの処理は、第2の実施形態で説明したため省略する。

[0216] 上述のように、本実施形態の認証連携システムによると、IDプロバイダ装置2 0 0の組織に所属するユーザがサービスプロバイダ装置3 0 0にアカウントが登録されていない状態であり、ユーザのログイン状態は未完了状態であり、かつユーザからのSSO要求起点がIDプロバイダ装置2 0 0から開始する場合において、SSOの過程でアカウント登録および連携を実行する際の人手を介さないサービス利用可否の決定を行うことが可能となる。

[0217] また、本実施形態の認証連携システムによると、IDプロバイダ装置2 0 0の組織に所属するユーザがサービスプロバイダ装置3 0 0にアカウントが登録されていない状態であり、ユーザのログイン状態は未完了状態でありかつユーザからのSSO要求起点がIDプロバイダ装置2 0 0から開始する場合において、適切なタイミングで、ポリシ評価とアカウントプロビジョニングを実施できる。

[0218] また、本実施形態の認証連携システムによると、IDプロバイダ装置2 0 0の認証連携サーバ2 3 0が、SSO手順(2)～(4)の処理を連続して行う中で、SSO手順(3)の直前に、ポリシ評価、およびアカウント登録・アカウント連携を行なうアカウントプロビジョニング処理の割り込みをIDプロバイダ装置の認証連携サーバ製品を直接改造することなく実現することが可能となる。このため、導入コストも低く、かつ人手を介さずにサービス利用可否を決定できる認証連携システムの提供が可能となる。

[0219] 以上、本発明のいくつかの実施形態を説明したが、これら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

[0220] 100…ユーザ端末、200…IDプロバイダ、210…ポータルサーバ、
220…Webサーバ、221…リバースプロキシ装置、222…転送URL記憶装置、
230…IDP認証連携部、240…認証連携制御システム、
250…IDPユーザストア、260…ポリシーストア、270…認証セッション一時記憶装置、
280…鍵記憶装置、290…ログイン応答メッセージ事前処理部、
300…サービスプロバイダ装置、310…SPユーザストア、
320…サービス利用状況データストア、330…一時記憶装置、340…
検証ポリシーストア、350…SP認証連携部

請求の範囲

[請求項1]

ユーザが操作するユーザ端末のログイン処理を行うＩＤプロバイダ装置と、前記ログイン処理が完了した場合に前記ユーザ端末にサービスデータを送信するサービスプロバイダ装置とを備え、前記ユーザ端末は前記サービスプロバイダ装置にサービス利用要求を行なう認証連携システムであって、

前記ＩＤプロバイダ装置は、

前記ユーザを識別するユーザ識別子含む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ＩＤＰユーザ属性情報を記憶するＩＤＰユーザ属性情報記憶部と、

前記ユーザＩＤと前記ユーザのログイン状態がログイン完了状態であることを示す認証トークンとを対応付けて記憶するＩＤＰ認証セッション記憶部と、

前記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ポリシー情報を記憶するポリシー情報記憶部と、

前記ＩＤプロバイダ装置の署名生成鍵を記憶する鍵記憶部と、

前記ユーザ端末のログイン処理が未完了状態である場合には、前記ユーザ端末にログイン要求を行い、前記ユーザ端末のログイン処理が完了状態である場合には、前記サービス利用要求を受信した前記サービスプロバイダ装置から発行されるＳＰ認証連携要求を受信し、前記ログイン処理の認証方式名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し、前記認証アサーション含む認証連携応答を前記サービスプロバイダ装置に送信するＩＤＰ認証連携部と、

前記ユーザ端末から前記ＳＰ認証連携要求を受信した場合に、前記認証セッション記憶部に当該ユーザに発行された認証トークンが記憶されているか否かを確認するログイン状態確認処理を行うログイン状

態判定部と、前記ログイン状態確認処理の結果がログイン未完了の状態であれば、前記ＳＰ認証連携要求を前記ＩＤＰ認証連部に転送する認証連携要求転送部と、前記ユーザ端末から、前記ＩＤＰ認証連部からの前記ログイン要求に基づいて送信された前記ユーザの認証情報を受信し、受信した前記認証情報に基づいて前記ログイン処理を行う認証識別部と、前記ログイン状態確認処理の結果がログイン完了状態である場合に、前記認証セッション記憶部に当該ユーザに発行された認証トークンに対応付けて記憶されたユーザＩＤに基づいて前記ＩＤＰユーザ属性情報記憶部から取得したＩＤＰユーザ属性情報と前記ポリシー情報とに基づいて前記ユーザ端末を操作するユーザがサービスデータの送信が許可される対象となるユーザであるか否かを評価し、前記ログイン状態確認処理の結果がログイン未完了の状態である場合に、前記認証情報に含まれるユーザＩＤに基づいて前記ＩＤＰユーザ属性情報記憶部から取得したＩＤＰユーザ属性情報と前記ポリシー情報とに基づいて前記ユーザ端末を操作するユーザがサービスデータの送信が許可されるユーザであるか否かを評価するポリシー評価部と、前記ポリシー評価部による評価結果が許可である場合に、前記取得されたＩＤＰユーザ属性情報を参照して前記サービスプロバイダ装置とのアカウント連携処理を行い、前記サービスプロバイダ装置における前記ユーザの識別子であるＳＰ側ユーザＩＤを作成するアカウント連携部と、前記アカウント連携処理後に前記ＳＰ認証連携要求を前記ＩＤＰ認証連部に送信する認証連携要求転送部とを具備する認証連携制御部と、

を備え、

前記サービスプロバイダ装置は、

前記認証連携応答を受信した場合に前記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検証ポリシーを記憶する検証ポリシー記憶部と、

前記アカウント連携処理において発行される前記ＳＰ側ユーザＩＤと、前記ユーザ属性情報に含まれるユーザ属性の項目名および項目値のうちの少なくとも一つの項目名と項目値とであるユーザ属性部分情報とを関連付けたアカウント登録を記憶するＳＰユーザ属性情報記憶部と、

前記サービス利用要求を受信した場合、当該サービス利用要求が認証トークンを含むか否かを判定し、前記サービス利用要求が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とを前記ユーザ端末に送信し、前記サービス利用要求が前記認証トークンを含まない場合には、前記ユーザ端末のアドレス情報を含む前記ＩＤプロバイダ装置に対する前記ＳＰ認証連携要求を発行し、

前記認証連携応答を受信した場合、前記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、前記認証トークンと前記サービスデータとを前記ユーザ端末に送信するＳＰ認証連携部と、

前記ＳＰ側ユーザＩＤと、前記認証トークンとを関連付けて記憶するＳＰ認証セッション記憶部と、

を備える認証連携システム。

[請求項２]

ユーザが操作するユーザ端末のログイン処理を行うＩＤプロバイダ装置と、前記ログイン処理が完了した場合に前記ユーザ端末にサービスデータを送信するサービスプロバイダ装置とを備え、前記ユーザ端末は前記ＩＤプロバイダ装置にサービス利用要求を行なう認証連携システムであって、

前記ＩＤプロバイダ装置は、

前記ユーザを識別するユーザ識別子含む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ＩＤＰユーザ属性情報を記憶するＩＤＰユーザ属性情報記憶部と、

前記ユーザIDと前記ユーザのログイン状態がログイン完了状態であることを示す認証トークンとを対応付けて記憶するIDP認証セッション記憶部と、

前記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ポリシー情報を記憶するポリシー情報記憶部と、

前記IDプロバイダ装置の署名生成鍵を記憶する鍵記憶部と、

前記ユーザ端末からサービス利用要求を受信した場合に、前記サービスプロバイダ装置に対するIDP認証連携要求を発行するIDP認証連携要求部と、

前記ユーザ端末のログイン処理が未完了状態である場合には、前記ユーザ端末にログイン要求を行い、前記ユーザ端末のログイン処理が完了状態である場合には、前記IDP認証連携要求を受信し、前記ログイン処理の認証方式名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し、前記認証アサーション含む認証連携応答を前記サービスプロバイダ装置に送信するIDP認証連携部と、

前記IDP認証連携要求を受信した場合に、前記認証セッション記憶部に当該ユーザに発行された認証トークンが記憶されているか否かを確認するログイン状態確認処理を行うログイン状態判定部と、前記ログイン状態確認処理の結果がログイン未完了の状態であれば、前記IDP認証連携要求を前記IDP認証連部に転送する認証連携要求転送部と、前記ユーザ端末から、前記IDP認証連携部からの前記ログイン要求に基づいて送信された前記ユーザの認証情報を受信し、受信した前記認証情報に基づいて前記ログイン処理を行う認証識別部と、前記ログイン状態確認処理の結果がログイン完了状態である場合に、前記認証セッション記憶部に当該ユーザに発行された認証トークンに対応付けて記憶されたユーザIDに基づいて前記IDPユーザ属性情

報記憶部から取得したＩＤＰユーザ属性情報と前記ポリシー情報とに基づいて前記ユーザ端末を操作するユーザがサービスデータの送信が許可される対象となるユーザであるか否かを評価し、前記ログイン状態確認処理の結果がログイン未完了の状態である場合に、前記認証情報に含まれるユーザＩＤに基づいて前記ＩＤＰユーザ属性情報記憶部から取得したＩＤＰユーザ属性情報と前記ポリシー情報とに基づいて前記ユーザ端末を操作するユーザがサービスデータの送信が許可されるユーザであるか否かを評価するポリシー評価部と、前記ポリシー評価部による評価結果が許可である場合に、前記取得されたＩＤＰユーザ属性情報を参照して前記サービスプロバイダ装置とのアカウント連携処理を行い、前記サービスプロバイダ装置における前記ユーザの識別子であるＳＰ側ユーザＩＤを作成するアカウント連携部と、前記アカウント連携処理後に前記ＩＤＰ認証連携要求を前記ＩＤＰ認証連携部に送信する認証連携要求転送部とを具備する認証連携制御部と、

を備え、

前記サービスプロバイダ装置は、

前記認証連携応答を受信した場合に前記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検証ポリシーを記憶する検証ポリシー記憶部と、

前記アカウント連携処理において発行される前記ＳＰ側ユーザＩＤと、前記ユーザ属性情報に含まれるユーザ属性の項目名および項目値のうちの少なくとも一つの項目名と項目値とであるユーザ属性部分情報とを関連付けたアカウント登録を記憶するＳＰユーザ属性情報記憶部と、

前記ＩＤＰ認証連携部から前記認証連携応答を受信した場合、前記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、前記認証トークンと前記サービ

スデータとを前記ユーザ端末に送信するＳＰ認証連携部と、

前記ＳＰ側ユーザＩＤと、前記認証トークンとを関連付けて記憶するＳＰ認証セッション記憶部と、

を備える認証連携システム。

[請求項３]

ユーザが操作するユーザ端末にサービスデータを送信するサービスプロバイダ装置と接続され認証連携システムを構成する、前記サービスプロバイダ装置にサービス利用要求を行なう前記ユーザ端末のログイン処理を行うＩＤプロバイダ装置であって、

前記ユーザを識別するユーザ識別子含む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ＩＤＰユーザ属性情報を記憶するＩＤＰユーザ属性情報記憶部と、

前記ユーザＩＤと前記ユーザのログイン状態がログイン完了状態であることを示す認証トークンとを対応付けて記憶するＩＤＰ認証セッション記憶部と、

前記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ポリシー情報を記憶するポリシー情報記憶部と、

前記ＩＤプロバイダ装置の署名生成鍵を記憶する鍵記憶部と、

前記ユーザ端末のログイン処理が未完了状態である場合には、前記ユーザ端末にログイン要求を行い、前記ユーザ端末のログイン処理が完了状態である場合には、前記サービス利用要求を受信した前記サービスプロバイダ装置から発行されるＳＰ認証連携要求を受信し、前記ログイン処理の認証方式名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し、前記認証アサーション含む認証連携応答を前記サービスプロバイダ装置に送信するＩＤＰ認証連携部と、

前記ユーザ端末から前記ＳＰ認証連携要求を受信した場合に、前記認証セッション記憶部に当該ユーザに発行された認証トークンが記憶

されているか否かを確認するログイン状態確認処理を行うログイン状態判定部と、前記ログイン状態確認処理の結果がログイン未完了の状態であれば、前記ＳＰ認証連携要求を前記ＩＤＰ認証連部に転送する認証連携要求転送部と、前記ユーザ端末から、前記ＩＤＰ認証連携部からの前記ログイン要求に基づいて送信された前記ユーザの認証情報を受信し、受信した前記認証情報に基づいて前記ログイン処理を行う認証識別部と、前記ログイン状態確認処理の結果がログイン完了状態である場合に、前記認証セッション記憶部に当該ユーザに発行された認証トークンに対応付けて記憶されたユーザＩＤに基づいて前記ＩＤＰユーザ属性情報記憶部から取得したＩＤＰユーザ属性情報と前記ポリシー情報とに基づいて前記ユーザ端末を操作するユーザがサービスデータの送信が許可されるユーザであるか否かを評価し、前記ログイン状態確認処理の結果がログイン未完了の状態である場合に、前記認証情報に含まれるユーザＩＤに基づいて前記ＩＤＰユーザ属性情報記憶部から取得したＩＤＰユーザ属性情報と前記ポリシー情報とに基づいて前記ユーザ端末を操作するユーザがサービスデータの送信が許可される対象となるユーザであるか否かを評価するポリシー評価部と、前記ポリシー評価部による評価結果が許可である場合に、前記取得されたＩＤＰユーザ属性情報を参照して前記サービスプロバイダ装置とのアカウント連携処理を行い、前記サービスプロバイダ装置における前記ユーザの識別子であるＳＰ側ユーザＩＤを作成するアカウント連携部と、前記アカウント連携処理後に前記ＳＰ認証連携要求を前記ＩＤＰ認証連携部に送信する認証連携要求転送部とを具備する認証連携制御部と、

前記サービスプロバイダ装置から送信された前記認証連携要求を前記認証連携制御部に転送する転送装置と、

を備えるＩＤプロバイダ装置。

[請求項４]

ユーザが操作するユーザ端末にサービスデータを送信するサービス

プロバイダ装置と接続され認証連携システムを構成し、ユーザ端末のログイン処理を行うＩＤプロバイダ装置であって、

前記ユーザを識別するユーザ識別子含む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ＩＤＰユーザ属性情報を記憶するＩＤＰユーザ属性情報記憶部と、

前記ユーザＩＤと前記ユーザのログイン状態がログイン完了状態であることを示す認証トークンとを対応付けて記憶するＩＤＰ認証セッション記憶部と、

前記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ポリシー情報を記憶するポリシー情報記憶部と、

前記ＩＤプロバイダ装置の署名生成鍵を記憶する鍵記憶部と、

前記ユーザ端末からサービス利用要求を受信した場合に、前記サービスプロバイダ装置に対するＩＤＰ認証連携要求を発行するＩＤＰ認証連携要求部と、

前記ユーザ端末のログイン処理が未完了状態である場合には、前記ユーザ端末にログイン要求を行い、前記ユーザ端末のログイン処理が完了状態である場合には、前記ＩＤＰ認証連携要求を受信し、前記ログイン処理の認証方式名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し、前記認証アサーション含む認証連携応答を前記サービスプロバイダ装置に送信するＩＤＰ認証連携部と、

前記ＩＤＰ認証連携要求を受信した場合に、前記認証セッション記憶部に当該ユーザに発行された認証トークンが記憶されているか否かを確認するログイン状態確認処理を行うログイン状態判定部と、前記ログイン状態確認処理の結果がログイン未完了の状態であれば、前記ＩＤＰ認証連携要求を前記ＩＤＰ認証連部に転送する認証連携要求転送部と、前記ユーザ端末から、前記ＩＤＰ認証連携部からの前記ログ

イン要求に基づいて送信された前記ユーザの含む認証情報を受信し、受信した前記認証情報に基づいて前記ログイン処理を行う認証識別部と、前記ログイン状態確認処理の結果がログイン完了状態である場合に、前記認証セッション記憶部に当該ユーザに発行された認証トークンに対応付けて記憶されたユーザIDに基づいて前記IDPユーザ属性情報記憶部から取得したIDPユーザ属性情報と前記ポリシー情報とに基づいて前記ユーザ端末を操作するユーザがサービスデータの送信が許可される対象となるユーザであるか否かを評価し、前記ログイン状態確認処理の結果がログイン未完了の状態である場合に、前記認証情報に含まれるユーザIDに基づいて前記IDPユーザ属性情報記憶部から取得したIDPユーザ属性情報と前記ポリシー情報とに基づいて前記ユーザ端末を操作するユーザがサービスデータの送信が許可されるユーザであるか否かを評価するポリシー評価部と、前記ポリシー評価部による評価結果が許可である場合に、前記取得されたIDPユーザ属性情報を参照して前記サービスプロバイダ装置とのアカウント連携処理を行い、前記サービスプロバイダ装置における前記ユーザの識別子であるSP側ユーザIDを作成するアカウント連携部と、前記アカウント連携処理後に前記IDP認証連携要求を前記IDP認証連携部に送信する認証連携要求転送部とを具備する認証連携制御部と、を備えるIDプロバイダ装置。

[請求項5]

前記ユーザIDと、前記各サービスプロバイダ装置のサービス利用状況とを関連付けたサービス利用状況情報を記憶するサービス利用状況記憶部を備え、

前記認証連携要求事前処理部は、前記サービス利用状況記憶部に記憶された前記サービス利用状況情報と前記ポリシー情報記憶部に記憶された前記ポリシー情報とを参照して前記ユーザ端末を操作するユーザがサービスデータの送信が許可されるユーザであるか否かを評価する請求項3に記載のIDプロバイダ装置。