

明 細 書

発明の名称：

認証連携システム、ＩＤプロバイダ装置およびプログラム

技術分野

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

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、近年、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（ユーザＩＤ）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] アイデンティティ管理技術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という）がある。SSOは、一度の認証手続きだけで、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。

[0005] 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。

- [0006] さらに、最近では、異なるドメイン間（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。
- [0007] 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。
- [0008] 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。
- [0009] これらの問題点を解消するため、ベンダ間でのSSOの標準化という要望がある。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 Structured Information Standards）が策定したSAML（Security Assertion Markup Language）がある。
- [0010] 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）、ユーザの三者であり、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。
- [0011] 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後にＳＳＯを行なうことができる。

[0012] 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。以下の手順では、特に断りのない限り、基本的に昇順で順番に処理を行う。

[0013] （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。

[0014] （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。

[0015] （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。

[0016] （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。

[0017] （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。

[0018] （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。

[0019] 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。現在、多くのベンダが、ＳＡＭＬのＩＤＰおよびＳＰ

の機能を実装したアクセス管理製品や、SAMLのSP機能を実装したSaaSサービスの提供を行っている。

[0020] 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。

[0021] 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。

[0022] 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。

[0023] 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および連携を実行する。

[0024] 以上で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およ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、企業内での情報システムを統括する I S (I n f o r m a t i o n S y s t e m) 部門がサービスプロバイダに対して、アカウント登録および連携を行う。

[0027] I S 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じ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および連携を行う。

[0028] 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ずる場合は、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、I S 部門など多くの人手を介することになり、大量の手間暇を要する。更に、I S 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、S a a S 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、S S O 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。

先行技術文献

特許文献

[0031] 特許文献1：特表2008-538247号公報

発明の概要

発明が解決しようとする課題

[0032] 本発明が解決しようとする課題は、S S O の過程でアカウント登録および

連携を実行する際に、ユーザの負荷が少なく、かつ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認証連携システム、ＩＤプロバイダ装置およ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

[0033] 実施形態のＩＤプロバイダ装置のポリシ記憶部は、サービスプロバイダＩＤ毎に、サービスデータの送信が許可されるユーザを示すポリシ情報と、サービスデータの送信許可が削除される対象となるユーザを示すポリシ情報を記憶する。ＩＤプロバイダ装置は、所定の周期が到来した場合、もしくはサービスプロバイダ装置の利用状況が変化した場合に、サービスプロバイダ装置から送信される当該サービスプロバイダ装置の利用状況を取得し、取得した利用状況に基づいてサービス利用状況記憶部を更新する。ＩＤプロバイダ装置は、サービス利用状況記憶部が更新された場合、サービスプロバイダＩＤ毎の削除対象アカウントの決定を行なう。

図面の簡単な説明

[0034] [図1]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]実施形態に係るＩＤＰユーザリポジトリを説明するための模式図。

[図3]実施形態に係るＩＤＰサービス利用状況ストアを説明するための模式図。

[図4]実施形態に係る認証連携ポリシストアを説明するための模式図。

[図5]実施形態に係るＳＰユーザ設定ルールストアを説明するための模式図。

[図6]実施形態に係る削除対象決定ポリシストアを説明するための模式図。

[図7]実施形態に係る削除対象アカウントストアを説明するための模式図。

[図8]実施形態に係る認証アサーションを説明するための模式図。

[図9]実施形態に係るＳＰユーザリポジトリを説明するための模式図。

[図10]実施形態に係るサービスデータストアを説明するための模式図。

[図11]実施形態に係るＳＰサービス利用状況ストアを説明するための模式図。

[図12]実施形態に係る検証ポリシーストアを説明するための模式図。

[図13]実施形態に係る全体動作の概要を示す模式図。

[図14]実施形態に係る利用状況取得の処理フローを示すシーケンス図。

[図15]実施形態に係る利用状況取得の処理に必要な構成要素の一例を示すブロック図。

[図16]実施形態に係るユーザ認証の処理フローを示すシーケンス図。

[図17]実施形態に係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。

[図18]実施形態に係る認証連携ポリシー評価の処理フローを示すシーケンス図である。

[図19]実施形態に係る認証連携ポリシー評価の処理に必要な構成要素の一例を示すブロック図。

[図20]実施形態に係るアカウント連携の処理フローを示すシーケンス図。

[図21]実施形態に係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。

[図22]実施形態に係る認証連携の処理フローを示すシーケンス図。

[図23]実施形態に係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。

発明を実施するための形態

[0035] (第1の実施形態)

以下、図1乃至図23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。

[0036] 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、IDプロバイダ装置200とサービスプロバイダ装置300は、それぞれ複数台あってもよいが、ここでは1

台ずつを図示している。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。

[0037] 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る。ユーザ端末１００は、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、ユーザ端末１００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。

[0038] 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、ＩＤＰユーザリポジトリ２０１、ＩＤＰ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、鍵記憶部２０５、削除対象決定ポリシーストア２０６、削除対象アカウントストア２０７、ＩＤＰ認証連携部２０８、認証連携ハンドリング部２０９、認証連携ポリシー評価部２１０、ＩＤＰアカウントプロビジョニング部２１１、サービス利用状況管理部２１２、およびトリガ２１３を備える。

[0039] ＩＤＰ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、ＩＤＰユーザリポジトリ（ユーザ属性情報記憶部）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２０１ａであって、ユーザを識別するユーザＩＤと、ユーザのログイン処理時に参照するパスワードと、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、認証連携ＩＤなどを項目名に含む複数のユーザ属性情報２０１ａを記憶する。認証連携ＩＤは、サービスプロバイダ装置３０

０と自装置２００との間で共有するＩＤであり、本実施形態では後述するアカウント連携処理において発行される。なお、サービスプロバイダとの認証連携が行われていない場合、認証連携ＩＤは空である。

[0040] ユーザ属性情報２０１ａは個人の情報を特徴付ける情報の集合体である。ユーザ属性情報２０１ａは上述したに限らず、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値とを更に含んでもよい。また、ユーザのログイン処理時に、参照するパスワードは、例えばユーザの指紋等の生体認証情報であってもよい。

[0041] ＩＤＰサービス利用状況ストア（第１のサービス利用状況記憶部）２０２は、認証連携ポリシー評価部２１０から参照され、ユーザごとのサービス利用状況情報２０２ａを記憶する。なお、サービス利用状況情報２０２ａは、ユーザＩＤ毎の、各サービスプロバイダ装置３００が提供するサービスの利用状況である。

[0042] すなわち、ＩＤＰサービス利用状況ストア２０２は、ＩＤプロバイダ装置２００側においてユーザごとのサービス利用状況を記憶する。図３に示すように、ＩＤＰサービス利用状況ストア２０２は、サービス利用状況情報２０２ａとしてユーザ利用管理テーブル２０２ａＡと、利用数管理テーブル２０２ａＢとを記憶している。ユーザ利用管理テーブル２０２ａＡ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、サービスプロバイダＩＤごとの「サービス利用状況」とを関連付けて記憶する。

[0043] サービス利用状況は、例えば、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」、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」、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データの送信の許可の一時停止を示す「サービス利用停止」、およびユーザ端末１００から受けた利用終了要求に基づく「サービス利用終了」である。なお、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む

。また、サービス利用状況は、ユーザがサービスを利用した最終の日時（最終のログイン日時）である最終利用日時およびディスク利用量も関連付けて記憶される。

[0044] 例えば、図3のユーザIDが「USER__A」のサービス利用状況は、SP(1)はサービス未利用の状態、SP(2)はサービス利用中、SP(N)はサービス未利用の状態である。さらに、SP(2)では、最終利用日時が2011/02/10で、ディスク利用量が4Gバイトである。

[0045] 利用数管理テーブル202aBは、図3に示すように、ユーザ利用管理テーブル202aA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、あらかじめ設定された利用数の上限値とをサービスプロバイダIDごとに関連付けて書き込まれる。

[0046] 認証連携ポリシーストア（認証連携ポリシー記憶部）203は、認証連携ポリシー評価部210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および役職を示す複数の認証連携ポリシー（認証連携ポリシー情報）203a（203aA, 203aB, 203aC, …）を記憶する。

[0047] なお、認証連携ポリシー203a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。

[0048] 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。

[0049] 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（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209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Aの[4]の[責務条件]）。

[0050] SPユーザ設定ルールストア（一部項目名記憶部）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

鍵記憶部205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。

[0051] 削除対象決定ポリシストア（削除対象ポリシ記憶部）206は、図6に示すように、サービス利用状況管理部212から参照され、削除対象決定ポリシを記憶する。具体的には、削除対象決定ポリシストア（削除対象決定ポリシ記憶部）206は、図6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において、サービスデータの送信許可を削除されるユーザの条件（削除対象条件）を示す削除対象決定ポリシ（削除対象決定ポリシ情報）206a（206aA、206aB、206aC…）を記憶する。

[0052] 例えば、削除対象決定ポリシ206aは、サービスプロバイダSP（1）に登録されたユーザの最終利用日時が半年以上前であること、ディスク利用量が5GB異常であること、ユーザの所属する部がXであることを削除対象条件として記述する。サービスプロバイダSP（2）とサービスプロバイダ

S P (3) の削除対象決定ポリシも同様に記述する。サービスデータの送信許可の削除は、例えば後述する S P ユーザリポジトリから削除対象アカウントを削除してもよいし、サービスデータ送信許可上体を一時停止状態に変更してもよい。

[0053] 削除対象アカウントストア（削除対象アカウント記憶部）207は、図7に示すように、後述するサービス利用状況管理部212が、削除対象決定ポリシ206aと、サービス利用状況202aと、ユーザ属性情報201aとに基づいて決定した削除対象アカウント（削除対象アカウント情報）207aを記憶する。削除対象アカウント情報207aは各サービスプロバイダ装置200における削除対象のユーザIDである。

[0054] IDP認証連携部208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208は、具体的には例えば、以下の機能（f208-1）～（f208-3）をもっている。

[0055] （f208-1） 後述する認証連携ハンドリング部209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およ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およびパスワードに基づいて認証するログイン処理を実行する機能。

[0056] （f208-2） 後述するIDPアカウントプロビジョニング部211が発行した認証連携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205内の署名生成鍵に基づくデジタル署名を生成し、図8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208aを作成する機能。

[0057] （f208-3） 作成した認証アサーション208a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。

[0058] 認証連携ハンドリング部209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、後述するポリシ評価処理とアカウント連携処理とIDP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209は、具体的には、以下の機能（f209-1）～（f209-4）をもっている。

[0059]（f209-1） 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208に送出する機能。

[0060]（f209-2） IDP認証連携部208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210に送出する機能。

[0061]（f209-3） 認証連携ポリシ評価部210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211に送出する機能。

[0062]（f209-4） IDPアカウントプロビジョニング部211から送出されたアカウント連携応答内の操作完了に含まれるサービスプロバイダIDおよびユーザIDを含むIDP認証連携実行要求をIDP認証連携部208に送出する機能。

[0063] 認証連携ポリシ評価部210は、認証連携ハンドリング部209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203aとユーザ利用管理テーブル202aAとに基づいてポリシ評価を行う。認証連携ポリシ評価部210は、具体的には、以下の機能（f210-1）～（f210-5）をもっている。

[0064]（f210-1） 認証連携ハンドリング部209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201aを読み出す機能。

[0065]（f210-2） 認証連携ハンドリング部209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情報203aを読み出す機能。

[0066] (f210-3) 認証連携ハンドリング部209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サービス利用状況ストア202からサービス利用状況情報202aを読み出す機能。

[0067] (f210-4) 読み出した認証連携ポリシ203aに示される所属および役職に対し、当該読み出したユーザ属性情報201a内の所属や役職、および当該読み出したサービス利用状況情報202a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。

[0068] (f210-5) 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209に送出する機能。

[0069] IDPアカウントプロビジョニング部211は、認証連携ハンドリング部209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211は、具体的には例えば、以下の機能(f212-1)～(f212-8)をもっている。

[0070] (f211-1) 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。

[0071] (f211-2) 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、削除対象アカウントストア207から削除対象アカウント情報207aを読み出す機能。

[0072] (f211-3) 当該読み出した一部の項目名とアカウント連携要求メッセージ内のユーザ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およ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。

[0073] (f211-4) 当該アカウント連携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 を発行する機能。

- [0074] (f 2 1 1 - 5) 取得したユーザ属性部分情報に操作指示として「アカウント登録」を付加し、取得した削除対象アカウント情報 207 a に操作指示として「アカウント削除」を付加すると共に、発行された認証連携 ID を付加し、アカウントプロビジョニング要求（アカウント連携要求メッセージ）を作成する機能。
- [0075] (f 2 1 1 - 6) 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。
- [0076] (f 2 1 1 - 7) 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 SP ユーザリポジトリ 302 の操作完了が通知されると、当該操作完了に含まれるサービスプロバイダ ID およびユーザ ID に基づいて、IDP ユーザリポジトリ 201 内のユーザ属性情報 201 a に認証連携 ID を登録する機能。
- [0077] (f 2 1 1 - 8) 当該登録完了とユーザリポジトリの操作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 209 に送出する機能。
- [0078] サービス利用状況管理部 212 は、サービス利用状況取得部 214 と削除対象アカウント決定部 215 とを備える。
- [0079] サービス利用状況取得部 214 は、サービスプロバイダ装置 300 に利用状況取得要求を送信する。また、サービス利用状況取得部 214 は、当該利用状況取得要求に基づいてサービスプロバイダ装置 300 から送信される当該サービスプロバイダ装置 300 の利用状況を取得し、取得した利用状況に基づいて SP IDP サービス利用状況ストア 202 を更新する。
- [0080] 削除対象アカウント決定部 215 は、取得した利用状況と、ユーザ属性情報 201 a と、削除対象決定ポリシ 206 a A とに基づいて削除対象アカウントの決定を行なう。
- [0081] トリガ 213 は、あらかじめ定められた時刻が到来した場合に、サービス

利用状況管理部 211 のサービス利用状況取得部 212 にサービスプロバイダ装置 300 の利用状況取得を行なうよう要求する。すなわち、トリガ 213 は、サービス利用状況取得部 212 に利用状況取得実行要求を送信する。

[0082] サービス利用状況取得部 214 は、この利用状況取得実行要求を受信すると、サービスプロバイダ装置 300 からサービス利用状況を取得する。トリガ 213 は、例えば、周期によって設定してもよい。すなわち、トリガ 213 は、ID プロバイダ装置 200 とサービスプロバイダ装置 300 との認証セッションの張り直しのアクションのように一定時間ごとに動作するアクションとしてもよい。

[0083] 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、サービスデータ通信部 301、SP ユーザリポジトリ 302、サービスデータストア 303、SP サービス利用状況ストア 304、検証ポリシーストア 305、SP 認証連携部 306、サービス利用状況提供部 307、および SP アカウントプロビジョニング部 308 を備えている。

[0084] サービスデータ通信部 301 は、後述する SP 認証連携部 306 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後述する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 に送信する機能をもっている。

[0085] SP ユーザリポジトリ 302 は、サービスデータ通信部 301 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部）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および項目値のうち、SP ユーザ設定ルール 204a に基づく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。

[0086] 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。

[0087] SP サービス利用状況ストア（第 2 のサービス利用状況記憶部）304 は、ユーザごとの当該サービスプロバイダ装置 300 が提供するサービスの利用状況であるサービス利用状況情報 304 a を記憶する。

[0088] すなわち、SP サービス利用状況ストア 304 は、サービスプロバイダ装置 300 側においてユーザごとのサービス利用状況を記憶するユーザ利用管理テーブル 202 a A と、利用数管理テーブル 202 a B とを記憶している。

[0089] 図 11 に示すように、SP サービス利用状況ストア 304 は、ユーザ利用管理テーブル 304 a A と、利用数管理テーブル 304 a B とを記憶している。ユーザ利用管理テーブル 304 a A は、サービスデータ 303 a の送信が許可された場合を示す「サービス利用中」、サービスデータ 303 a の送信が許可されていない場合を示す「サービス未利用」、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データの送信の許可の一時停止を示す「サービス利用停止」、もしくはユーザ端末 100 から受けた利用終了要求に基づく「サービス利用終了」のいずれかを示す、当該サービスプロバイダ装置 300 の利用状況と、ユーザ ID とを関連付けて書き込まれる。

[0090] また、サービスプロバイダ装置 300 の利用状況は、ユーザの最終利用日時およびディスク利用量も関連付けて記憶される。なお、ユーザ利用管理テーブル 304 a A は、ID プロバイダ装置 200 が複数ある場合は、ユーザ ID と ID プロバイダ装置の ID ごとの利用状況が書き込まれる。

[0091] 利用数管理テーブル 202 a B は、図 11 に示すように、ユーザ利用管理テーブル 304 a A 内の利用状況が示すサービス利用中の個数を示す利用数と、あらかじめ設定された利用数の上限値とを関連付けて書き込まれる。

[0092] 検証ポリシストア 305 は、図 12 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 303 a 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ーを記憶する。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。

[0093] SP認証連携部306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306は、具体的には例えば、以下の機能(f306-1)～(f306-4)をもっている。

[0094] (f306-1) 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。

[0095] (f306-2) IDプロバイダ装置200から認証連携応答を受けると、検証ポリシーストア305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、当該認証アサーション208a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。

[0096] (f306-3) 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する機能。

[0097] (f306-4) 発行された認証トークンと、IDプロバイダ装置200から受けた認証連携応答に含まれるユーザのアドレス情報とを含むサービス実行要求をサービスデータ通信部301に送出する機能。

[0098] サービス利用状況提供部307は、IDプロバイダ装置200のサービス利用状況取得部214から利用状況取得要求を受けると、この利用状況送信要求に含まれるユーザIDに基づいてSPサービス利用状況ストア304を検索し、当該検索により得られたサービスプロバイダ装置300の利用状況を送信する機能をもっている。

[0099] SPアカウントプロビジョニング部308は、IDプロバイダ装置200のIDPアカウントプロビジョニング部211から受けたアカウント連携要

求メッセージに基づき、SPユーザリポジトリ302に対してアカウントプロビジョニングを行う。また、SPアカウントプロビジョニング部308は、当該アカウント連携要求メッセージに基づき、SPサービス利用状況ストア304を更新する。

[0100] SPアカウントプロビジョニング部308は、具体的には例えば、以下の機能（f308-1）～（f308-5）をもっている。

[0101] （f308-1） IDプロバイダ装置200のIDPアカウントプロビジョニング部211からアカウント連携要求メッセージを受信すると、アカウント連携要求メッセージに含まれる操作情報を確認し、操作情報が「アカウント登録」である場合に新規の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302aとを関連付けてSPユーザリポジトリ302に登録する機能。

[0102] （f308-2） アカウント連携要求メッセージに含まれる操作情報が「削除」である場合に、当該アカウント連携要求メッセージに含まれるユーザID（削除対象アカウント）に基づいてSPユーザリポジトリ302を検索し、検索結果のユーザ属性部分情報302aを削除する機能。

[0103] （f308-3） アカウント連携要求メッセージに含まれる操作情報が「更新」である場合に、当該アカウント連携要求メッセージに含まれるユーザIDに基づいてSPユーザリポジトリ302を検索し、検索結果のユーザ属性部分情報302aを更新する機能。なお、操作情報「更新」は例えばアカウントの無効であり、このとき、SPアカウントプロビジョニング部308は、当該アカウント連携要求メッセージに含まれるユーザIDに基づいてSPユーザリポジトリ302を検索し、検索結果のユーザ属性部分情報302aに含まれる有効フラグ（図示しない）を「false」に変更する。

[0104] なお、アカウントの無効を操作情報「削除」に含めても良い。

[0105] （f308-4） ユーザリポジトリの操作の後、アカウント連携要求メッセージに含まれるユーザIDと、操作情報とに基づいてSPサービス利用状況ストア304を更新する機能。

- [0106] 例えば、操作情報が「アカウント登録」の場合、ユーザ利用管理テーブル 304 a A に新規の利用状況として当該ユーザ ID と、利用状況「サービス利用中」とを書き込む。このときユーザ利用管理テーブル 304 a A に当該ユーザ ID が存在する場合は、利用状況の更新を行なう。
- [0107] また、操作情報が「削除」の場合、ユーザ利用管理テーブル 304 a A に書き込まれた当該ユーザ ID の利用状況を「サービス未利用」に変更する。
- [0108] (f 308-5) SP ユーザリポジトリ 302 の操作および SP サービス利用状況ストア 304 の更新 (SP アカウント操作) 後、操作したユーザ属性部分情報 302 a 内のユーザ ID と自装置 300 のサービスプロバイダ ID とを含む操作完了と、ストア更新完了と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 に通知する機能。
- [0109] 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 13 乃至図 23 を参照して説明する。以下の説明は、ID プロバイダ装置 200 とサービスプロバイダ装置 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ない、かつ認証未連携である状態から開始される。
- [0110] この状態において、ユーザがサービス要求をした時に、ID プロバイダ装置 200 が認証連携ポリシー 203 a を満たすか否かを判定し、満たす場合にサービスプロバイダ装置 300 側へのユーザのアカウント登録を行うことにより、ID プロバイダ装置 200 とサービスプロバイダ装置 300 間の SSO が実行され、サービスプロバイダ装置 300 からサービスデータ 303 a が送信される典型的な処理を例に挙げて述べる。
- [0111] 以降、図 13 に示す如き、ステップ S10 のサービス利用状況取得 (S11~S19)、ステップ S20 のユーザ認証 (S21~S27)、ステップ S30 の認証連携ポリシー評価 (S31~S36)、ステップ S40 のアカウント連携 (S41~S49) およびステップ S50 の認証連携 (S51~S58) に分けて説明する。

まず、図１４のシーケンス図および図１５の模式図を参照して、図１３のステップＳ１０のサービス利用状況取得について説明する。

- [0112] ステップＳ１１では、ＩＤプロバイダ装置２００のトリガ２１３が、あらかじめ設定された時刻が到来すると、サービス利用状況管理部２１２に対して、利用状況取得の実行を要求する。本実施形態では、トリガ２１３を２０１１年４月１日の１２時に設定する。
- [0113] ステップＳ１２では、サービス利用状況管理部２１２のサービス利用状況取得部２１４は、トリガ２１３から利用状況取得実行要求を受信すると、サービスプロバイダ装置３００のサービス利用状況提供部３０７に、利用状況の取得を要求する。本実施形態では、ＳＰ（１）というサービスプロバイダＩＤのサービスプロバイダ装置３００のみに利用状況の取得要求を送るとする。
- [0114] ステップＳ１３では、サービス利用状況提供部３０７は、各サービスプロバイダ装置３００のＳＰサービス利用状況ストア３０４からサービス利用状況情報３０４ａを取得し、ＩＤプロバイダ装置２００のサービス利用状況管理部２１２に送信する。
- [0115] ステップＳ１４では、サービス利用状況管理部２１２のサービス利用状況取得部２１４は、受信したサービスプロバイダ装置３００ごとのサービス利用状況情報３０４ａに基づいてＩＤＰサービス利用状況ストア２０２を更新する。
- [0116] ステップＳ１５では、サービス利用状況取得部２１４は、受信したサービス利用状況情報３０４ａに基づいてＳＰＩＤＰサービス利用状況ストア２０２を更新すると、削除対象アカウント決定部２１５に削除対象決定要求を送信する。
- [0117] ステップＳ１６では、削除対象アカウント決定部２１５は、削除対象決定要求を受信すると、削除対象決定ポリシストア２０６から削除対象決定ポリシ２０６ａを取得する。
- [0118] ステップＳ１７では、削除対象アカウント決定部２１５は、ＩＤＰユーザ

リポジトリ 201 からユーザ属性情報 201 a を取得する。

[0119] ステップ S 18 では、削除対象アカウント決定部 215 は、ステップ S 14 で更新されたユーザ利用管理テーブル 202 a A と利用数管理テーブル 202 a B と、ステップ S 16 で取得した削除対象決定ポリシー 206 a と、ステップ S 17 で取得したユーザ属性情報 201 a とに基づいて、削除対象のアカウントを決定する。具体的には、削除対象アカウント決定部 215 は、所定のユーザに関するユーザ属性情報 201 a とユーザ利用管理テーブル 202 a A と利用数管理テーブル 202 a B に記憶された当該ユーザのサービス利用状況とに基づいて、削除対象決定ポリシー 206 a の示す削除条件を満たすユーザを判定する。

[0120] 例えば、削除対象アカウント決定部 215 が、図 6 の削除対象決定ポリシー 206 a A と、図 3 のユーザ利用管理テーブル 202 a A と、利用数管理テーブル 202 a B とに基づいて削除対象決定ポリシー 206 a の示す削除条件を満たすユーザを判定する場合について具体的に説明する。まず、削除対象決定ポリシー 206 a A の S P (1) における削除条件 [1] 「最終利用日時が半年以上前であること」を満たすのは、USER__B および USER__N である。

[0121] 続いて、削除対象決定ポリシー 206 a A の S P (1) における削除条件 [2] 「ディスク利用量が、5 GB 以上であること」を満たすのは、USER__B および USER__N である。続いて、削除対象決定ポリシー 206 a A の S P (1) における削除条件 [3] 「ユーザの所属する部が X であること」を満たすのは、USER__B である。したがって、USER__B が削除対象決定ポリシー 206 a の示す削除条件を全て満たすため、削除対象アカウントと決定される。なお、削除対象アカウントが複数存在する場合は、それら全てを削除対象アカウントと決定する。

[0122] ステップ S 19 では、削除対象アカウント決定部 215 は、決定した削除対象アカウントを削除対象アカウントストア 207 に記憶する。

[0123] ここで、図 16 のシーケンス図および図 17 の模式図を参照して、図 13

のステップS 2 0のユーザ認証について説明する。ステップS 2 0のユーザ認証は、ユーザがサービスプロバイダ装置3 0 0側のサービスを利用するためにユーザ端末を操作すると開始される。

[0124] ステップS 2 1では、ユーザが、サービスプロバイダ装置3 0 0側のサービスを利用するために、ユーザ端末1 0 0を操作すると、ユーザ端末1 0 0はサービス要求をサービスプロバイダ装置3 0 0に送信する。サービスプロバイダ装置3 0 0は、アクセス管理を担うS P認証連携部3 0 6がサービス要求をキャッチする。

[0125] ステップS 2 2では、S P認証連携部3 0 6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否かを判定する。例えば、ユーザからのサービス要求がH T T Pリクエストの形態の場合、そのH T T Pリクエストに含まれるC o o k i eの中に、サービスプロバイダ装置3 0 0が発行した認証トークンが存在することを確認する。

[0126] なお、認証トークンの存在が確認できた場合、すなわち認証連携済みの場合、サービスプロバイダ装置3 0 0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、S P認証連携部3 0 6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3 0 1により、当該認証トークンとサービスデータストア3 0 3内のサービスデータ3 0 3 aとをサービス要求元のユーザ端末1 0 0に送信する。具体的には、S P認証連携部3 0 6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関連付けられたユーザI Dを含むサービス実行要求をサービスデータ通信部3 0 1に送出する。

[0127] 一方、ステップS 2 2での判定の結果、サービス要求が認証トークンを含まない場合には、すなわち認証未連携の場合には、ステップS 2 3が実行される。

[0128] ステップS 2 3では、サービスプロバイダ装置3 0 0は、I Dプロバイダ装置2 0 0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3 0 0から直接I Dプロバイダ装置2 0 0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。また、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。

[0129] ここでは、サービスプロバイダ装置３００が１つのＩＤプロバイダであるＩＤプロバイダ装置２００としか連携しないため、ＩＤプロバイダの選択が不要である。サービスプロバイダ装置３００が１つのＩＤプロバイダであるＩＤプロバイダ装置２００と連携しており、ＩＤプロバイダの選択が必要な場合には、ＳＰ認証連携部３０６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（図示しない）をユーザ端末１００に送信してもよい。このとき、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。

[0130] ステップＳ２４では、ＩＤプロバイダ装置２００の認証連携ハンドリング部２０９が、ＩＤプロバイダ装置２００宛の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２０８に送信する。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２０９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。

[0131] ステップＳ２５では、ＩＤＰ認証連携部２０８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２０８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およびユーザ認証情報をＩＤＰユーザリポジトリ２

01内のユーザIDおよびパスワードに基づいて認証する。本実施形態では、当該ユーザ端末100から受けたユーザID「USER__A」、パスワード「PASS__A」、に基づいて認証を行い、ユーザ認証は成功したとする。

[0132] ステップS26では、IDP認証連携部208は、ログインに成功したユーザのアカウント情報が、削除対象アカウントストア207に存在するかどうかを判定し、ログインに成功したアカウントの情報が存在する場合、当該アカウントを削除対象アカウントストア207から削除する。本実施形態では、削除対象アカウントストア207に、「USER__A」が登録されていないため、削除対象アカウントストア207は更新されない。

[0133] ステップS27では、IDP認証連携部208は、ステップS25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と認証成功の旨を含むユーザ認証完了（ログイン完了）のメッセージを認証連携ハンドリング部209に通知する。

[0134] 以上により、ステップS20のユーザ認証（S21～S27）が終了する。

[0135] 続いて、ステップS30の認証連携ポリシー評価においては、ユーザ認証終了後、ユーザ利用管理テーブル202aA、利用数管理テーブル202aB、ユーザ属性情報201a、認証連携ポリシー203a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18のシーケンス図および図19の模式図を参照してステップS30の認証連携ポリシー評価について説明する。

[0136] ステップS31では、認証連携ハンドリング部209は、ステップS27にて送信され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209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210に送出する。ポリシー評価要求は、ステップS25のログイン処理過程で取得したユーザID、すなわちユーザのIDP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。

[0137] 以降、ステップS32～S34を通じて、認証連携ポリシー評価部208は、認証連携ポリシー203aの評価に必要な情報を収集する。

[0138] ステップS32では、認証連携ポリシー評価部210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IDPサービス利用状況ストア202からサービス利用状況202aを読み出す。但し、ステップS32は、静的なポリシー評価を実行する場合には省略される。

[0139] 以降、ステップS32で読み出されるユーザIDはUSER__A、ユーザが要求するサービスプロバイダ装置300はSP(1)とする。

[0140] ステップS33では、認証連携ポリシー評価部210は、ポリシー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201aを読み出す。

[0141] ステップS34では、認証連携ポリシー評価部210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ー203aを読み出す。本実施形態では、図4の各認証連携ポリシー203aのうち、図中Aに関連付けられた第1の認証連携ポリシー(SP(1)利用時のポリシー)203aAが検索結果として読み出される。

[0142] ステップS35では、認証連携ポリシー評価部210は、静的なポリシー評価を実行する場合、ステップS34で読み出した認証連携ポリシー203aAに示される所属および役職に対し、ステップS33で読み出したユーザ属性情報201a内の所属およ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ポリシー評価処理を行う。

[0143] 但し、ステップS32のユーザ利用管理テーブル202aAも用いる動的なポリシー評価を実行する場合には、ステップS32, S33, S34を通じて取得したサービス利用状況202a、ユーザ属性情報201aおよび認証連携ポリシー203aAに基づいて、ポリシー評価を実行する。

[0144] 例えば、認証連携ポリシー203aAに示すSP(1)の利用に関する、ステップS35におけるポリシー評価を説明する。認証連携ポリシー203aAに

は、事前に〔１〕～〔４〕のサービス利用条件が定義されており（静的なポリシー評価の場合には〔４〕は未定義）、収集したユーザ利用管理テーブル２０２ａＡ、ユーザ属性情報２０１ａ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。

[0145] 認証連携ポリシー２０３ａＡの〔１〕：認証連携ポリシー２０３ａ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、ユーザ属性情報２０１ａにおけるUSER__Aの所属部が「Ｘ部門」である。従って、USER__Aは認証連携ポリシー２０３ａにおける〔１〕の条件を満たす。

[0146] 認証連携ポリシー２０３ａＡの〔２〕：認証連携ポリシー２０３ａ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、ユーザ属性情報２０１ａにおけるUSER__Aの所属課が「Ｙ課」である。従って、USER__Aは認証連携ポリシー２０３ａにおける〔２〕の条件を満たす。

[0147] 認証連携ポリシー２０３ａＡの〔３〕：認証連携ポリシー２０３ａ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、ユーザ属性情報２０１ａにおけるUSER__A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。

[0148] 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、利用数管理テーブル２０２ａＢにおけるＳＰ（１）の現在の利用数が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。

[0149] 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、ユーザ利用管理テーブル２０２ａＡ、利用数管理テーブル２０２ａＢ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。

[0150] すなわち、認証連携ポリシー評価部210は、読み出した認証連携ポリシー203aに対して、読み出したユーザ属性情報201a、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、サービスデータの送信を許可するか否かを判定する。

[0151] ステップS36では、認証連携ポリシー評価部210は、ステップS35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209に送出する。以上により、ステップS30の認証連携ポリシー評価（S31～S36）が終了する。

[0152] ステップS40のアカウント連携では、ステップS30の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20のシーケンス図および図21の模式図を用いて述べる。

[0153] ステップS41では、認証連携ハンドリング部209は、ステップS36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、ポリシー評価応答が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211に依頼する。なお、ポリシー評価応答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、ポリシー評価応答が許可の場合を例に挙げ、以降のステップS42～49を説明する。

[0154] ステップS42では、IDPアカウントプロビジョニング部211は、受信したアカウント連携要求内のサービスプロバイダID（ここでは、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 204 a を読み出す。ユーザ設定ルール 204 a は、例えば、ID プロバイダ装置 200 が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）などである。ここでは、IDP アカウントプロビジョニング部 211 は、ユーザ設定ルール 204 a 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。

[0155] ステップ S43 では、IDP アカウントプロビジョニング部 211 は、削除対象アカウントストア 207 から SP (1) に関する削除対象のアカウントを検索する。

[0156] なお、ステップ S43 の検索は、ステップ S32 で認証連携ポリシー評価部 210 が IDP サービス利用状況ストア 202 から取得したサービス利用状況情報において、受信したアカウント連携内のサービスプロバイダ ID（ここでは、SP (1)）の利用者数が上限に達しているかを判定し、SP (1) の利用者数が上限に達している場合に行なうようにしてもよい。このとき、ステップ S32 において、静的なポリシー評価が実行され、サービス利用状況取得が省略された場合は、ステップ S43 の前に IDP プロビジョニング部 210 が IDP サービス利用状況ストア 202 からサービス利用状況を取得する。

[0157] 本実施形態では、図 7 に示すように、削除対象アカウントストア 207 には SP (1) に関する削除対象のアカウントとして USER__B が登録されているため、ここでは USER__B が検索結果である。なお、複数の削除対象アカウントが存在する場合は、1 つのユーザ ID のみを削除してもよいし、全て削除してもよい。

[0158] ステップ S44 では、IDP アカウントプロビジョニング部 211 は、ステップ S42 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 201 a のうち、当該一部の項目名に一致する項目名およびこの項目名に関連付けられた項目値からなる必要なユ

ーザ属性情報（以下、ユーザ属性部分情報という）を取得する。

[0159] ステップS 4 5では、I D Pアカウントプロビジョニング部2 1 1は、ステップS 4 4で取得したユーザ属性部分情報に、操作指示として「アカウント登録」を付加し、ステップS 4 3で取得した削除対象アカウントに操作指示として「削除」指示を付加してS Pアカウント連携要求メッセージを作成し、作成したアカウント連携要求メッセージをサービスプロバイダ装置3 0 0のS Pアカウントプロビジョニング部3 0 9に送信する。また、I D Pアカウントプロビジョニング部2 1 1は、認証連携I Dを発行しアカウント連携要求メッセージに含める。

[0160] アカウント連携要求メッセージに含まれる操作指示は、例えば、S Pアカウントプロビジョニング部3 0 8が公開する操作インタフェースに基づくS Pユーザリポジトリ3 0 2の操作の種類であり、削除、アカウント登録、アカウント更新などがある。本実施形態では、サービスプロバイダ装置3 0 0側にユーザのアカウントが登録されてないため、ステップS 4 5では、操作指示として「アカウント登録」を指定する。

[0161] また、I D Pアカウントプロビジョニング部2 1 1は、S Pアカウント連携要求メッセージを送信する先のサービスプロバイダ装置3 0 0と自装置2 0 0との間で共有する認証連携I Dを発行し、この認証連携I DをS Pアカウント連携要求メッセージに含める。

[0162] ステップS 4 6では、S Pアカウントプロビジョニング部3 0 8は、受信したアカウント連携要求メッセージに基づき、S Pユーザリポジトリ3 0 2の操作を行なう。具体的には、S Pアカウントプロビジョニング部3 0 8は、受信したアカウント連携要求メッセージに含まれる操作指示が「アカウント登録」である場合、S P側ユーザI D（サービスプロバイダ装置3 0 0側のユーザI D）を新規発行し、当該S P側ユーザI Dと、S P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S Pユーザリポジトリ3 0 2に登録する。このとき、S Pアカウントプロビジョニング部3 0 8は、アカウント連携要求メッセージ内の認証連携I Dも登録する。

- [0163] また、ステップS 4 6においてS Pアカウントプロビジョニング部3 0 8は、操作指示が「削除」である場合、当該アカウント連携要求メッセージ内の削除対象アカウントに基づいて、S Pユーザリポジトリ3 0 2内のユーザ属性部分情報3 0 2 a検索し、削除対象アカウントと一致するユーザIDを含むユーザ属性部分情報3 0 2 aを削除する。
- [0164] ステップS 4 7では、S Pアカウントプロビジョニング部3 0 8は、受信したアカウント連携要求メッセージに基づき、S Pサービス利用状況ストア3 0 4を更新する。具体的には、S Pアカウントプロビジョニング部3 0 8は、受信したアカウント連携要求メッセージに含まれる操作指示が「アカウント登録」である場合、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に含まれるユーザIDとサービス利用状況「サービス利用中」と、最終利用日時と、ディスク利用量と関連づけてS Pサービス利用状況ストア3 0 4のユーザ利用管理テーブル3 0 4 a Aに登録するとともに、「サービス利用中」のユーザID数をカウントして利用数管理テーブル3 0 4 a Bの現在の利用数を更新する。
- [0165] また、S Pアカウントプロビジョニング部3 0 8は、受信したアカウント連携要求メッセージに含まれる操作指示が「削除」である場合、当該アカウント連携要求メッセージに含まれる削除対象アカウントに基づいてS Pサービス利用状況ストア3 0 4を検索し、検索結果のユーザ利用情報3 0 4 aに含まれるサービス利用状況を「サービス利用停止」に変更する。
- [0166] ステップS 4 6のユーザリポジトリ操作とステップS 4 7のサービス利用状況ストア2 0 2更新後、S Pアカウントプロビジョニング部3 0 8は、登録したユーザ属性部分情報3 0 2 a内のユーザIDと自装置のサービスプロバイダIDとを含む操作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2 0 0に通知する。具体的には、操作完了は、IDプロバイダ装置2 0 0内のID Pアカウントプロビジョニング部2 1 1に通知される。
- [0167] ステップS 4 8では、ID Pアカウントプロビジョニング部2 1 1は、ス

ステップS 4 5で発行された認証連携IDをIDPユーザリポジトリ2 0 1 aのUSER__Aのレコードに登録する。

[0168] ステップS 4 9では、IDPアカウントプロビジョニング部2 1 1は、ステップS 4 7で通知された操作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2 0 9に送出する。

[0169] 以上により、ステップS 4 0のアカウント連携（S 4 1～S 4 9）が終了する。

[0170] ステップS 5 0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2 0 0とサービスプロバイダ装置3 0 0との間で認証連携、すなわちSSOを行う。以下、図2 2のシーケンス図および図2 3の模式図を用いてステップS 5 0の認証連携について説明する。

[0171] ステップS 5 1では、認証連携ハンドリング部2 0 9は、ステップS 4 9にて通知されたアカウント連携応答に含まれる認証結果を解析する。その結果に問題がなければ、認証連携ハンドリング部2 0 9は、アカウント連携応答内の操作完了に含まれるサービスプロバイダIDおよびユーザIDを含む認証連携実行要求をIDP認証連携部2 0 8に送出する。

[0172] ステップS 5 2では、IDP認証連携部2 0 8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ユーザIDに基づいてIDPユーザリポジトリを検索し、認証連携IDを取得する。

[0173] ステップS 5 3では、IDP認証連携部2 0 8は、ステップS 5 2で取得された認証連携IDと、ステップS 2 5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2 0 8は、アサーション本文に対して鍵記憶部2 0 5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2 0 8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2 0 8 aを作成する。

[0174] ステップS 5 4では、IDP認証連携部2 0 8は、作成した認証アサーション2 0 8 aと、受信した認証連携実行要求内のユーザID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3 0 0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 S P 認証連携部 306 に受信される。

[0175] ステップ S 55 では、S P 認証連携部 306 は、認証アサーション検証ポリシー 306 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 208 a 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、S P 認証連携部 306 は、I D プロバイダ装置 200 が発行した認証アサーション 208 a から、I D 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。

[0176] ステップ S 56 では、S P 認証連携部 306 は、ステップ S 55 で許可と決定されたとき、認証トークンを発行する。この認証トークンは認証連携 I D とユーザ I D とに関連付けてサービスプロバイダ装置 300 の一時記憶部（図示しない）に記憶されても良い。

[0177] ステップ S 57 では、S P 認証連携部 306 は、ステップ S 56 で発行された認証トークンと、当該認証トークンに認証連携 I D を介して関連付けられたユーザ I D とを含むサービス実行要求をサービスデータ通信部 301 に送出する。

[0178] ステップ S 58 では、サービスデータ通信部 301 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 303 a とをユーザ端末 100 に送信する。

[0179] 上述したように本実施形態の認証連携システムによれば、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、I D 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ー 203 a に基づき、サービスデータ 303 a の送信可否を判定する。そして、判定結果が許可の場合、I D プロバイダ装置 200 内で管理さ

れる当該ユーザ属性情報 201 a 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。

[0180] 補足すると、従来の認証連携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。一方、本実施形態の認証連携システムは、前述した予め認証連携ポリシー 203 a 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。

[0181] また、本実施形態の認証連携システムは、一般的に時間がかかる、ID プロバイダ装置 200 がサービスプロバイダ装置 300 の利用状況を取得する利用状況取得処理を、SSO のタイミングで行うのではなく事前に行なっているため、ユーザのログイン時の待ち時間が長くなることなく、ユーザの負荷を軽減できる。また、削除対象アカウントの決定も事前に行なっているため、よりユーザの負荷を軽減できる。

[0182] 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。

[0183] また、本実施形態の認証連携システムによれば、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。

[0184] 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。

[0185] 例えば、本実施形態ではＩＤプロバイダ装置２００側が利用状況取得処理を要求するトリガを備えるが、サービスプロバイダ装置３００側が備えても良い。サービスプロバイダ装置３００側がトリガを備える場合、図１３のステップＳ１０におけるステップＳ１０のサービスにおいて、トリガは、例えばＳＰサービス利用状況ストア３０４に登録されたサービス利用状況が変化したか否かを判定し、サービス利用状況が変化した場合に、サービス利用状況取得実行要求をサービス利用状況提供部３０７送信する（ステップＳ１１）。ステップＳ１２は省略され、ステップＳ１３において、利用状況取得実行要求を受信したサービス利用状況提供部３０７がＳＰサービス利用状況ストア３０４からサービス利用状況を取得する。その後、ステップＳ１４～ステップＳ１９の処理が行われる。

[0186] この場合、ＳＰサービス利用状況ストア３０４とＩＤＰサービス利用状況ストア２０２との間に差異が生じないため、サービス利用状況に基づいた正確なポリシ評価を行なうことが可能となる。

[0187] また、本実施形態の認証連携システムは、トリガ２１３によって開始されるステップＳ１０のサービス利用状況取得において、ステップＳ１５で削除対象アカウントの決定を行ない、削除対象アカウントを削除するのは、ステップＳ４０のアカウント連携において行っている。これは、アカウントの削除という操作を極力遅らせるためである。

[0188] しかし、ＳＳＯ時のレスポンスタイムの改善を優先するために、ステップＳ１０のサービス利用状況取得に削除対象アカウントの削除を行なっても良い。すなわち、ステップＳ１５の削除対象アカウント決定後にサービスプロ

バイダ装置300にアカウント削除のメッセージを送ってもよい。この場合、ステップS40のアカウント連携では、アカウントの登録のみを行うことになる。

[0189] また、ステップS47のSPサービス利用状況ストア304の更新は、例えば一定周期毎にSPユーザリポジトリ302に記憶されたユーザ属性部分情報302aを参照して行なうなど、SSO処理中に行なわないようにしても良い。これにより、ユーザのログイン待ち時間が軽減できる。このときSPサービス利用状況ストア304の更新の一定周期は、サービス利用状況取得を開始するトリガに設定された一定周期より短くする。

[0190] なお、上記の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。

[0191] ここで、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。

[0192] 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）等が本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。

[0193] さらに、本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。

[0194] また、記憶媒体は1つに限らず、複数の媒体から本実施形態における処理が実行される場合も本実施形態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。

[0195] なお、本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、本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。

[0196] また、本実施形態の各記憶部は1つの記憶装置で実現しても良いし、複数の記憶装で実現しても良い。

[0197] そして、本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実施形態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。

符号の説明

[0198] 100…ユーザ端末、200…IDプロバイダ装置、201…IDPユーザリポジトリ、202…IDPサービス利用状況ストア、203…認証連携ポリシストア、204…SPユーザ設定ルールストア、205…鍵記憶部、206…削除対象決定ポリシストア、207…削除対象アカウントストア、208…IDP認証連携部、209…認証連携ハンドリング部、210…認証連携ポリシ評価部、211…IDPアカウントプロビジョニング部、212…サービス利用状況管理部、213…トリガ、214…サービス利用状況取得部、215…削除対象アカウント決定部、300…サービスプロバイダ装置、301…サービスデータ通信部、302…SPユーザリポジトリ、303…サービスデータストア、304…SPサービス利用状況ストア、305…検証ポリシストア、306…SP認証連携部、307…サービス利用状況提供部、308…SPアカウントプロビジョニング部

請求の範囲

[請求項1]

ユーザが操作するユーザ端末に対して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、前記ユーザ端末はサービス利用要求を前記サービスプロバイダ装置に送信する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ＩＤを含み、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を記憶するユーザ属性情報記憶部と、

前記ユーザＩＤと、前記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、当該サービスプロバイダ装置の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第１のサービス利用状況記憶部と、

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認証連携ポリシー情報を記憶する認証連携ポリシー記憶部と、

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部と、

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おけるサービスデータの送信許可が削除される対象となるユーザを示す削除対象決定ポリシー情報を記憶する削除対象決定ポリシー記憶部と、

所定の周期が到来した場合、もしくは前記サービスプロバイダ装置の利用状況が変化した場合に、前記サービスプロバイダ装置から送信されるサービス利用状況情報を取得し、取得した当該サービス利用状

況情報に基づいて前記第 1 のサービス利用状況記憶部を更新する手段と、

前記ユーザ属性情報と、前記サービス利用状況情報と、前記削除対象決定ポリシー情報とに基づいて、前記サービス利用状況情報に含まれる前記サービスプロバイダ ID 毎の削除対象アカウントの決定を行なう手段と、

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、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信すると、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信する手段と、

前記送信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部内のユーザ ID 及びパスワード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信する手段と、

前記送信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部からユーザ属性情報を読み出す手段と、

前記送信されたポリシー評価要求内のサービスプロバイダ ID に基づいて前記認証連携ポリシー記憶部から認証連携ポリシー情報を読み出す手段と、

前記読み出した認証連携ポリシー情報と、前記読み出したユーザ属性情報とに基づいて、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

に送信する手段と、 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信する手段と、

前記送信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部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部内で当該ユーザ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、

前記送信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、前記削除対象アカウント決定部が決定した前記削除対象アカウントから削除対象アカウントを取得する手段と、

前記取得したユーザ属性部分情報に操作指示としてアカウント登録指示を付加し、前記取得した削除対象アカウントに操作指示としてアカウント削除指示もしくはアカウント無効指示を付加し、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当該ユーザ端末のアドレス情報とを含む更新完了が通知されると、当該更新完了を示すアカウント連携応答を送信する手段と、

前記送信されたアカウント連携応答内の更新完了に含まれるサービスプロバイダID及び前記ユーザIDを含む認証連携実行要求を送信する手段と、

前記認証連携実行要求を受信すると、当該認証連携実行要求内のユーザID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、

前記サービスプロバイダ装置は、

前記ユーザ属性情報記憶部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、当該サービスプロバイダ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部と、

前記サービスデータを記憶するサービスデータ記憶部と、

前記ユーザIDと、当該サービスプロバイダ装置の利用状況とを関連付けて記憶する第2のサービス利用状況記憶部と

前記サービス利用状況記憶部から当該サービスプロバイダ装置の利用状況を取得し、取得した前記利用状況を前記IDプロバイダ装置に送信する手段と、

前記ユーザ端末から前記サービス要求を受信すると、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部内のサービスデータとを当該ユーザ端末に送信し、否の場合には前記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、当該前記アカウント連携要求メッセージに含まれる前記操作指示が前記アカウント登録の場合に新規の前記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部に登録する手段と、当該前記アカウント連携要求メッセージに含まれる前記操作指示が前記アカウント削除の場合に、当該アカウント連携要求メッセー

ジ内の削除対象アカウントに基づいて前記ユーザ属性部分情報記憶部を検索し、当該削除対象アカウントと一致するユーザIDを含む前記ユーザ属性部分情報を削除する手段と、

前記登録もしくは削除の後、登録したユーザ属性部分情報内のユーザIDもしくは削除したユーザ属性部分情報内のユーザIDと、当該サービスプロバイダ装置のサービスプロバイダIDとを含む更新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前記認証連携応答を受信すると、当該認証連携応答の検証を行い、検証結果が許可のとき、前記認証トークンを発行し、前記認証連携応答に含まれるユーザIDと、当該認証トークンとを含むサービス実行要求を送信する手段と、

前記送信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部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

を備える認証連携システム。

[請求項2] 前記サービス利用状況情報に基づいて、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を備える請求項1に記載の認証連携システム。

[請求項3] 前記削除対象アカウントと前記ユーザ属性部分情報に含まれるユーザIDとが一致する場合、当該ユーザ属性部分情報を無効とする手段を備える請求項1及び請求項2のいずれか1項に記載の認証連携システム。

[請求項4] 前記第2のサービス利用状況記憶部に記憶される前記サービスプロバイダ装置の利用状況が変化した場合に、当該利用状況を前記IDプロバイダ装置に送信する手段を備える請求項1乃至請求項3のいずれか1項に記載の認証連携システム。

[請求項5] 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するとともに前記ユーザ端末に対して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ＩＤを含み、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を記憶するユーザ属性情報記憶部と、

前記ユーザＩＤと、前記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、当該サービスプロバイダ装置の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第１のサービス利用状況記憶部と、

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認証連携ポリシー情報を記憶する認証連携ポリシー記憶部と、

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部と、

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おけるサービスデータの送信許可が削除される対象となるユーザを示す削除対象決定ポリシー情報を記憶する削除対象決定ポリシー記憶部と、

前記サービスプロバイダ装置に利用状況取得要求を送信し、当該利用状況取得要求に基づいて前記サービスプロバイダ装置から送信されるサービス利用状況情報を取得し、取得した前記サービス利用状況情報に基づいて前記サービス利用状況記憶部を更新する手段と、

前記ユーザ属性情報と、前記サービス利用状況情報と、前記削除対象決定ポリシー情報とに基づいて、前記サービス利用状況情報に含まれる前記サービスプロバイダＩＤ毎の削除対象アカウントの決定を行な

う手段と、

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、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信すると、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信する手段と、

前記送信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部のユーザID及びパスワード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信する手段と、

前記送信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部からユーザ属性情報を読み出す手段と、

前記送信されたポリシー評価要求内のサービスプロバイダIDに基づいて前記認証連携ポリシー記憶部から認証連携ポリシー情報を読み出す手段と、

前記読み出した認証連携ポリシー情報と、前記読み出したユーザ属性情報とに基づいて、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信する手段と、 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信する手段と、

前記送信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部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部内で当該ユーザ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、

前記送信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、前記削除対象アカウント決定部が決定した前記削除対象アカウントから削除対象アカウントを取得する手段と、

前記取得したユーザ属性部分情報に操作指示としてアカウント登録指示を付加し、前記取得した削除対象アカウントに操作指示としてアカウント削除指示もしくはアカウント無効指示を付加し、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当該ユーザ端末のアドレス情報とを含む更新完了が通知されると、当該更新完了を示すアカウント連携応答を送信する手段と、

前記送信されたアカウント連携応答内の更新完了に含まれるサービスプロバイダID及び前記ユーザIDを含む認証連携実行要求を送信する手段と、

前記認証連携実行要求を受信すると、当該認証連携実行要求内のユーザID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、

を備えるIDプロバイダ装置。

[請求項6]

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するとともに前記ユーザ端末に対してログイン処理を行うＩＤプロバイダ装置のプログラムであって、

前記ＩＤプロバイダ装置を構成するコンピュータに、

前記ユーザを識別するユーザＩＤを含み、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を記憶する機能と、

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認証連携ポリシー情報を記憶する機能と、

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機能と、

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おけるサービスデータの送信許可が削除される対象となるユーザを示す削除対象決定ポリシー情報を記憶する機能と、

前記サービスプロバイダ装置に利用状況取得要求を送信し、当該利用状況取得要求に基づいて前記サービスプロバイダ装置から送信されるサービス利用状況を取得し、取得した前記サービス利用状況情報に基づいて、前記ユーザＩＤと、前記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、サービスプロバイダ装置の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機能と、

前記ユーザ属性情報と、前記サービス利用状況情報と、前記削除対象決定ポリシー情報とに基づいて、前記サービス利用状況情報に含まれる前記サービスプロバイダＩＤ毎の削除対象アカウントの決定を行なう機能と、

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、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信すると、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信する機能と、

前記送信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のユーザID及びパスワードに基づいて認証するログイン処理を実行する機能と、

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信する機能と、

前記送信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情報を読み出す機能と、

前記送信されたポリシ評価要求内のサービスプロバイダIDに基づいて前記認証連携ポリシ情報を読み出す機能と、

前記読み出した認証連携ポリシ情報と、前記読み出したユーザ属性情報とに基づいて、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機能と、

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信する機能と、 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信する機能と、

前記送信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、前記ユーザ属性の一部の項目名を読み出す機能と、

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、当該ユーザIDに一致するユーザIDを含む前記

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機能と、

前記送信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、前記決定された削除対象アカウントから削除対象アカウントを取得する機能と、

前記取得したユーザ属性部分情報に操作指示としてアカウント登録指示を付加し、前記取得した削除対象アカウントに操作指示としてアカウント削除指示もしくはアカウント無効指示を付加し、アカウント連携要求メッセージを作成する機能と、

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機能と、

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当該ユーザ端末のアドレス情報とを含む更新完了が通知されると、当該更新完了を示すアカウント連携応答を送信する機能と、

前記送信されたアカウント連携応答内の更新完了に含まれるサービスプロバイダID及び前記ユーザIDを含む認証連携実行要求を送信する機能と、

前記認証連携実行要求を受信すると、当該認証連携実行要求内のユーザID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機能と、

を実行させるプログラム。