

明 細 書

発明の名称：

ポリシ管理システム、ＩＤプロバイダシステム及びポリシ評価装置

技術分野

[0001] 本発明の実施形態は、ポリシ管理システム、ＩＤプロバイダシステム及びポリシ評価装置に関する。

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] ところで、SAMLに基づくSSOでは、上述したように、事前のアカウント連携及び登録が必要である。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。

[0019] 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。

[0020] 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。

[0021] 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。

[0022] 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。

[0023] このため、SSOの手順の(2)と(3)との間に、事前に定義したサービス利用に関するポリシーとサービスの利用状況とに基づき、サービスプロバイダが提供するサービスの利用可否を評価した後に、アカウント連携及び登録を実行する処理を割り込ませることで、サービスプロバイダ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技術がある。

先行技術文献

特許文献

[0024] 特許文献1：特許第4892093号公報

発明の概要

発明が解決しようとする課題

- [0025] 以上説明した技術は、通常、問題ない。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、企業では、組織変更や人事異動が行われると、セキュリティの観点からポリシーを更新する。しかしながら、組織変更や人事異動が行われる場合、組織変更や人事異動に伴う引き継ぎ作業を行う必要があり、人手を介さずにすぐにポリシーが更新されてしまうと、当該引き継ぎ作業に利用するサービスが利用できないといった不都合が生じ得る。このため、一般的に、組織変更や人事異動によるポリシーの更新は人手を介して行われる（つまり、ユーザがポリシー更新作業を行う）。
- [0027] しかしながら、人手による作業はユーザへの負担が大きい上、作業ミス（ヒューマンエラー）が生じる恐れがある。
- [0028] 本発明が解決しようとする課題は、人手を介さずに、ポリシー更新作業を実現し得るポリシー管理システム、IDプロバイダシステム及びポリシー評価装置を提供することである。

課題を解決するための手段

- [0029] 実施形態のポリシー管理システムは、ユーザ端末と、前記ユーザ端末を操作するユーザのアイデンティティを管理するIDプロバイダシステムと、前記ユーザ端末にサービスデータを提供するサービスプロバイダシステムとを含む。
- [0030] 前記ユーザ端末は、ログイン実行手段、第1送信手段及び再生手段を備えている。
- [0031] 前記ログイン実行手段は、ユーザの操作に応じて、前記IDプロバイダシステムとの間でログイン処理を実行する。
- [0032] 前記第1送信手段は、前記ログイン処理時に発行され、当該ユーザを識別するユーザIDを含むIDプロバイダ認証トークンと、前記サービスプロバイダシステムを識別するサービスプロバイダIDとを含むアクセス要求メッ

セージを前記 I D プロバイダシステムに送信する。

[0033] 前記再生手段は、前記サービスプロバイダシステムから送信されるサービスデータを受信し、当該受信したサービスデータを再生する。

[0034] 前記 I D プロバイダシステムは、第 1 格納手段、第 2 格納手段、第 3 格納手段、第 1 取得手段、第 1 判定手段、第 2 取得手段、確認手段、通知受領手段、ポリシー評価手段、第 2 判定手段、第 3 取得手段、決定手段、実行要求手段、第 2 送信手段及び第 3 送信手段を備えている。

[0035] 前記第 1 格納手段は、前記ユーザを特定するためのユーザの属性の項目名と項目値とを関連付けたユーザ属性情報であって、ユーザ I D を少なくとも含むユーザ属性情報を格納する。

[0036] 前記第 2 格納手段は、前記サービスプロバイダ I D 毎に、当該サービスプロバイダ I D で識別されるサービスプロバイダシステムによるサービスデータの送信を許可するための判定条件であって、判定 I D で識別される複数の条件を含み、当該各条件は更に複数の詳細条件及び責務を含む判定条件と、旧ポリシーから新ポリシーに移行するにあたり、新ポリシーだけでなく、旧ポリシーの判定条件による判定結果も参照する期間を示す移行期間とを少なくとも定義する一対の旧ポリシー及び新ポリシーを格納する。

[0037] 前記第 3 格納手段は、前記サービスプロバイダ I D 毎に、前記送信されたアクセス要求メッセージの送信日付が前記移行期間内であるときに参照される第 1 差分判定条件と、前記送信されたアクセス要求メッセージの送信日付が前記移行期間外であるときに参照される第 2 差分判定条件であって、差分対応 I D で識別される条件及び責務を含む第 2 差分判定条件とを少なくとも定義する差分対応定義情報を格納する。

[0038] 前記第 1 取得手段は、前記送信されたアクセス要求メッセージを受けると、当該アクセス要求メッセージ内のサービスプロバイダ I D に対応した新ポリシーを取得する。

[0039] 前記第 1 判定手段は、当該アクセス要求メッセージの送信日付が前記取得された新ポリシーに定義された移行期間に含まれるか否かを判定する。

- [0040] 前記第2取得手段は、前記第1判定手段による判定結果が含まれる旨を示すとき、前記取得された新ポリシに対応する旧ポリシを取得する。
- [0041] 前記確認手段は、当該アクセス要求メッセージ内のIDプロバイダ認証トークンに含まれるユーザIDに基づいて、前記第1格納手段に格納されたユーザ属性情報を取得すると共に、当該ユーザIDが当該アクセス要求メッセージ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システムに格納されているか否かを確認する。
- [0042] 前記通知受領手段は、前記サービスプロバイダシステムから送信され、前記確認手段に対する通知であって、前記ユーザIDが格納されている旨または格納されていない旨を示す通知を受領する。
- [0043] 前記ポリシ評価手段は、前記取得されたユーザ属性情報に基づいて、前記取得された新ポリシまたは前記取得された新ポリシ及び旧ポリシを評価する。
- [0044] 前記第2判定手段は、前記ポリシ評価手段による評価結果と、前記通知受領手段により受領された通知とに基づいて、前記差分対応定義情報を取得する必要があるか否かを判定する。
- [0045] 前記第3取得手段は、前記第2判定手段による判定結果が必要である旨を示すとき、前記差分対応定義情報を取得する。
- [0046] 前記決定手段は、前記評価結果に少なくとも基づいて（但し、前記第3取得手段により差分対応定義情報が取得された場合は当該差分対応定義情報も参照して）、適応する判定IDを決定する。
- [0047] 前記実行要求手段は、前記決定された判定IDで識別される条件内の責務を実行するよう要求する（但し、前記決定手段により前記差分対応定義情報に定義された第2差分判定条件が参照された場合は当該第2差分判定条件内の責務も実行するよう要求する）。
- [0048] 前記第2送信手段は、前記実行要求手段からの要求に応じて、当該アクセス要求メッセージ内の前記IDプロバイダ認証トークンに含まれるユーザIDを少なくとも含む認証連携メッセージを、当該アクセス要求メッセージ内

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システムに送信する。

[0049] 前記第3送信手段は、前記実行要求手段からの要求に応じて、当該アクセス要求メッセージ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によるサービスデータの送信が拒否された旨を表示させる拒否画面情報を前記ユーザ端末に送信する。

[0050] 前記サービスプロバイダシステムは、第4格納手段、発行手段及び第4送信手段を備えている。

[0051] 前記第4格納手段は、サービスデータを利用するユーザを特定するためのユーザの属性の項目名と項目値とを関連付けたユーザ属性情報を格納する。

[0052] 前記発行手段は、前記送信された認証連携要求メッセージを受けると、当該認証連携要求メッセージ内のユーザIDに基づいて当該認証連携要求メッセージの正当性を検証し、当該検証の結果が正当である場合に、当該検証に用いたユーザIDを含むサービスプロバイダ認証トークンを発行する。

[0053] 前記第4送信手段は、前記発行されたサービスプロバイダ認証トークン内のユーザIDで識別されるユーザ端末にサービスデータを送信する。

図面の簡単な説明

[0054] [図1]図1は一実施形態に係るポリシー管理システムの構成例を示す模式図である。

[図2]図2は同実施形態に係るポリシー格納装置に格納される旧ポリシーの一例を示す模式図である。

[図3]図3は同実施形態に係るポリシー格納装置に格納される新ポリシーの一例を示す模式図である。

[図4]図4は同実施形態に係る差分対応定義格納装置に格納される差分対応定義情報の一例を示す模式図である。

[図5]図5は同実施形態に係るポリシー評価装置の構成例を示す模式図である。

[図6]図6は同実施形態に係るポリシー管理システムの動作の一例を示すシーケンス図である。

[図7]図7は同実施形態に係るポリシー管理システムの動作の一例を示すシーケンス図である。

[図8]図8は同実施形態の変形例に係るポリシー管理システムの動作の一例を示すシーケンス図である。

発明を実施するための形態

[0055] 図1は一実施形態に係るポリシー管理システムの構成例を示す模式図であり、図2は同実施形態に係るポリシー格納装置に格納される旧ポリシーの一例を示す模式図であり、図3は同実施形態に係るポリシー格納装置に格納される新ポリシーの一例を示す模式図であり、図4は同実施形態に係るポリシー差分対応定義格納装置に格納されるポリシー差分対応定義情報の一例を示す模式図であって、図5は同実施形態に係るポリシー評価装置の構成例を示す模式図であり、

ポリシー管理システム1は、図1に示すように、ユーザが操作するユーザ端末100、IDプロバイダシステム200及び複数のサービスプロバイダシステム300を備えている。なお、サービスプロバイダシステム300は、通常複数台あるが、ここでは1台のみを図示している。以下、各装置100乃至300の詳細な機能について説明する。

[0056] ユーザ端末100は、通常のコンピュータ機能を有してIDプロバイダシステム200及び各サービスプロバイダシステム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、サービスプロバイダシステム300によって提供されるサービスの利用を希望する旨のアクセス要求メッセージを送信する機能と、IDプロバイダシステム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システム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。また、ユーザ端末100は、IDプロバイダシステム200及び各サービスプロバイダシステム300から送信される各種メッセージをリダイレクト（返信）する機能をもっている。

[0057] ここで、IDプロバイダシステム200は、ユーザのアイデンティティを

管理するものであり、ユーザ属性情報格納装置 201、ポリシー格納装置 202、ポリシー差分対応定義格納装置 203、認証連携装置 204、企業ポータル装置 205、ポリシー評価装置 206、IDプロビジョニング装置 207 及び拒否画面表示装置 208 を備えている。

[0058] ユーザ属性情報格納装置 201 は、IDプロバイダシステム 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であるユーザ属性情報を格納する。具体的には、ユーザ属性情報格納装置 201 は、ユーザを特定するためのユーザの属性の項目名と項目値とを関連付けたユーザ属性情報であって、ユーザを識別するためのユーザ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を格納する。

[0059] なお、ユーザ属性情報は個人の情報を特徴付ける情報の集合体であり、ユーザ属性情報の例としては、上述したように、ユーザの氏名、ユーザの所属、ユーザの役職、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が、これらに限られず、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参照情報は、通常パスワードを用いるが、これに限られず、例えばユーザの指紋等の生体認証情報であってもよい。

[0060] ポリシ格納装置 202 は、図 2 及び図 3 に示すように、サービスプロバイダシステム 300 を識別するサービスプロバイダID毎に、一対の旧ポリシ 202a 及び新ポリシ 202b を格納する。具体的には、ポリシ格納装置 202 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システム 300 によるユーザ端末 100 へのサービスデータの送信を許可するための判定条件と、当該判定条件による判定の結果を有効とする有効期間と、旧ポリシ 202a から新ポリシ 202b に移行するにあたり、旧ポリシの判定条件による判定の結果も参照する移行期間（移行猶予期間とも呼ぶ）とを含む一対の旧ポリシ 202a 及び新ポリシ 202b を格納する。なお、判定条件は判定IDで識別される複数の条件を含

んでおり、これら条件は更に複数の詳細条件及び責務を含んでいる。

[0061] ここでポリシとは、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）が定義されたものであり、オプションとして責務についても定義されるものである。

[0062] ポリシ差分対応定義格納装置 203 は、図 4 に示すように、サービスプロバイダシステム 300 を識別するサービスプロバイダ ID 毎に、ポリシ差分対応定義情報 203a を格納する。具体的には、ポリシ差分対応定義格納装置 203 は、ユーザ端末 100 から送信されたアクセス要求メッセージの送信日付が移行期間内であるときに参照される第 1 差分判定条件と、ユーザ端末 100 から送信されたアクセス要求メッセージの送信日付が移行期間外であるときに参照される第 2 差分判定条件とを含むポリシ差分対応定義情報 203a を格納する。なお、第 1 差分判定条件は差分対応 ID で識別される複数の条件を含んでおり、これら条件は更に複数の詳細条件と適応する判定 ID の示唆とを含んでいる。また、第 2 差分対応判定条件は差分対応 ID で識別される条件と責務とを含んでいる。

[0063] 認証連携装置 204 は、シングルサインオンの ID プロバイダ機能を有する。具体的には、認証連携装置 204 は、以下の各機能 (f204-1) 乃至 (f204-4) をもっている。

[0064] (f204-1) ユーザ端末 100 から送信されたユーザ ID 及びユーザ認証情報をユーザ属性情報格納装置 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。

[0065] (f204-2) 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 を含む ID プロバイダ認証トークンをユーザ端末 100 に発行する機能。

[0066] (f204-3) ID プロビジョニング装置 207 から認証連携要求を受けると、ID プロバイダ認証トークン内のユーザ ID を含むアサーション本文に対して、図示しない鍵記憶装置内の署名生成鍵（秘密鍵）に基づく署名を生成

し、当該アサーション本文と、当該デジタル署名と、当該署名生成鍵に対応した署名検証鍵（公開鍵）とを含む認証アサーションを作成する機能。

[0067] (f204-4) 作成した認証アサーションを含む認証連携要求メッセージを、ユーザ端末100を介してサービスプロバイダシステム300内の認証連携装置302に送信する機能、つまり、認証連携要求メッセージをユーザ端末100のリダイレクト機能を用いてサービスプロバイダシステム300内の認証連携装置302に送信する機能。

[0068] 企業ポータル装置205は、ユーザ端末100からのアクセス要求メッセージの入力を受け付けると、当該入力を受け付けたアクセス要求メッセージをポリシ評価装置206に転送する。なお、アクセス要求メッセージには、認証連携装置204により発行されたIDプロバイダ認証トークンと、ユーザが利用を希望するサービスデータを提供可能なサービスプロバイダシステム300を示すサービスプロバイダIDとが含まれる。

[0069] ポリシ評価装置206は、企業ポータル装置205からのアクセス要求メッセージの入力を受け付けると、ポリシ格納装置202に格納された旧ポリシ202a及び／または新ポリシ202bに基づいて、当該入力を受け付けたアクセス要求メッセージ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システム300によるユーザ端末100へのサービスデータの送信を許可するか否かを判定する。なお、ポリシ評価装置206の詳細については後述する。

[0070] IDプロビジョニング装置207は、ポリシ評価装置206からの指示に応じて、認証連携要求を認証連携装置204に送信する他、サービスプロバイダシステム300内のユーザ属性情報格納装置301に格納されたユーザ属性情報に関して、ユーザ属性情報の登録要求処理、更新要求処理、削除要求処理及び検索要求処理を実行する。

[0071] 拒否画面表示装置208は、ポリシ評価装置206からの指示に応じて、アクセス要求メッセージ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システム300によるサービスデータの送信が拒否された旨を示

す拒否画面情報をユーザ端末１００に送信する、つまり、ユーザ端末１００に拒否画面を表示させる。

[0072] ここで、図５を参照しながら、ポリシ評価装置２０６について詳細に説明する。ポリシ評価装置２０６は、図２に示すように、ポリシ評価要求部２１１、新ポリシ取得部２１２、旧ポリシ要否判定部２１３、旧ポリシ取得部２１４、属性情報収集部２１５、ポリシ評価部２１６、ポリシ差分対応判定部２１７、ポリシ差分対応定義取得部２１８及びＩＤプロビジョニング実行要求部２１９を備えている。

[0073] ポリシ評価要求部２１１は、企業ポータル装置２０５からのアクセス要求メッセージの入力を受け付けると、当該入力を受け付けたアクセス要求メッセージ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システム３００によるユーザ端末１００へのサービスデータの送信を許可するための判定条件を定義したポリシのうち新ポリシ２０２ｂを、新ポリシ取得部２１２を介して取得する。

[0074] 旧ポリシ要否判定部２１３は、ポリシ評価要求部２１１により取得された新ポリシに定義される移行期間を用いて、ユーザ端末１００によるアクセス要求メッセージの送信日付が当該移行期間に含まれているか否かを判定する。この判定の結果が含まれる旨を示すとき、旧ポリシ要否判定部２１３は、ポリシ評価要求部２１１により取得された新ポリシ２０２ｂに対応した旧ポリシ２０２ａを、旧ポリシ取得部２１４を介して取得する。また判定の結果が否を示すとき、旧ポリシ要否判定部２１３は、旧ポリシ２０２ａを取得する必要はないと判断し、旧ポリシを取得しない。

[0075] 属性情報収集部２１５は、アクセス要求メッセージ内のＩＤプロバイダ認証トークンに含まれるユーザＩＤを用いて、ユーザ属性情報格納装置２０１からユーザ属性情報を取得する。属性情報収集部２１５は、取得したユーザ属性情報がサービスプロバイダシステム３００内のユーザ属性情報格納装置３０１に格納されているか否かを、ＩＤプロビジョニング装置２０７を介して確認する、つまり、取得したユーザ属性情報を用いてサービスプロバイダ

システム 300 内のユーザ属性情報格納装置 301 を検索するよう ID プロビジョニング装置 207 に指示する。

[0076] ポリシ評価部 216 は、属性情報収集部 215 により取得されたユーザ属性情報を用いて、取得されたポリシを評価する、具体的には、旧ポリシ 202 a 及び新ポリシ 202 b の双方を評価する、または新ポリシ 202 b のみを評価する。

[0077] ポリシ差分対応判定部 217 は、ポリシ評価部 216 による評価結果（即ち、ポリシに定義された複数の条件のうちのいずれかの条件の成立）に基づいて、ポリシ差分対応定義格納装置 203 に格納されたポリシ差分対応定義情報 203 a を取得する必要があるか否かを判定する。具体的には、ポリシ差分対応判定部 217 は、以下の各機能(f217-1)乃至(f217-7)をもっている。

[0078] (f217-1) ポリシ評価部 216 により旧ポリシ 202 a 及び新ポリシ 202 b の双方について評価が行われたか、または新ポリシ 202 b のみについて評価が行われたかのどちらであることを判定する機能。

[0079] (f217-2) (f217-1)による判定の結果が、双方について評価が行われた旨を示すとき、ポリシ差分対応判定部 217 は、ポリシ評価部 216 による旧ポリシ 202 a の評価結果と新ポリシ 202 b の評価結果とが一致しているか否かを判定する機能。

[0080] (f217-3) (f217-2)による判定の結果が一致している旨を示すとき、ポリシ差分対応定義情報 203 a を取得する必要があると判断する機能。

[0081] (f217-4) (f217-2)による判定の結果が否を示すとき、ポリシ差分対応定義情報 203 a を取得する必要があると判断し、ポリシ差分対応定義情報 203 a を、差分対応定義取得部 218 を介して取得する機能。

[0082] (f217-5) (f217-1)による判定の結果が新ポリシ 202 b についてのみ評価が行われた旨を示すとき、新ポリシ 202 b の評価結果が拒否（つまり、図 3 に示す NEW-DENY-3 が成立）であり、且つ属性情報収集部 215 によりユーザ属性情報が格納されていることが確認されているか否かを判定する機能

。

[0083] (f217-6) (f217-5)による判定の結果が新ポリシ202bの評価結果が拒否であり且つユーザ属性情報の格納が確認されている旨を示すとき、ポリシ差分対応定義情報203aを取得する必要があると判断し、ポリシ差分対応定義情報203aを、差分対応定義取得部218を介して取得する機能。

[0084] (f217-7) (f217-5)による判定の結果が否を示すとき、ポリシ差分対応定義情報203aを取得する必要がないと判断する機能。

[0085] IDプロビジョニング実行要求部219は、ポリシ差分対応判定部217によりポリシ差分対応定義情報203aが取得されている場合、当該取得されたポリシ差分対応定義情報203aの定義にしたがって優先されるポリシに定義された条件内の責務に従う処理を実行する。また、IDプロビジョニング実行要求部219は、ポリシ差分対応判定部217によりポリシ差分対応定義情報203aが取得されていない場合、ポリシ評価部216による評価結果に基づいて、成立した条件内の責務に従う処理を実行する。なお、IDプロビジョニング実行要求部219により実行される処理の一例としては、IDプロビジョニング装置207に認証連携要求を送信させるために認証連携送信要求をIDプロビジョニング装置207に送信する処理、サービスプロバイダシステム300内のユーザ属性情報格納装置301に格納されたユーザ属性情報を削除させる削除要求を送信させるために削除送信要求をIDプロビジョニング装置207に送信する処理、拒否画面表示装置208に拒否画面情報を送信させるために拒否画面情報送信要求を拒否画面表示装置208に送信する処理等が挙げられる。

[0086] また、サービスプロバイダシステム300は、ユーザ端末100にサービスデータを提供するものであり、図1に示すように、ユーザ属性情報格納装置301、認証連携装置302、サービス提供装置303及びIDプロビジョニング装置304を備えている。

[0087] ユーザ属性情報格納装置301は、当該サービスプロバイダシステム300によ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であるユ

ーザ属性情報を格納する。このユーザ属性情報は、ＩＤプロバイダシステム２００内のユーザ属性情報格納装置２０１に格納されるユーザ属性情報と同様な項目名から構成されてもよいし、ユーザ属性情報格納装置２０１に格納されるユーザ属性情報の一部の項目名から構成されてもよい。

[0088] 認証連携装置３０２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。具体的には、認証連携装置３０２は、以下の各機能(f302-1)乃至(f302-3)をもっている。

[0089] (f302-1) ＩＤプロバイダシステム２００内の認証連携装置２０４からの認証連携要求メッセージの入力を受け付けると、当該入力を受け付けた認証連携要求メッセージ内の認証アサーションに含まれるデジタル署名を、当該認証アサーションに含まれる署名検証鍵を用いて検証する機能。

[0090] 具体的には、まず、認証アサーションに含まれる署名検証鍵を用いてデジタル署名に対応したアサーション本文を復号する。その後、復号したアサーション本文に含まれるユーザＩＤが、ユーザ属性情報格納装置３０１内に格納されているか否かを判定することで、認証連携要求メッセージの正当性を検証する。

[0091] (f302-2) (f302-1)の機能による検証の結果が正当である旨を示すとき、当該検証に用いたユーザＩＤを含むサービスプロバイダ認証トークンを発行する機能。なお、発行したサービスプロバイダ認証トークンは、ユーザからのアクセス要求メッセージが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の中に格納される。

[0092] (f302-3) (f302-2)の機能により発行されたサービスプロバイダ認証トークンを含むサービス提供要求メッセージをユーザ端末１００に送信する機能。

[0093] サービス提供装置３０３は、ユーザ端末１００のリダイレクト機能により返信されたサービス提供要求メッセージの入力を受け付けると、当該サービスプロバイダシステム３００により提供可能なサービスデータをユーザ端末１００に送信する。

- [0094] IDプロビジョニング装置304は、IDプロバイダシステム200内のIDプロビジョニング装置207からの要求に従って、ユーザ属性情報格納装置301に格納されたユーザ属性情報の登録処理、更新処理、削除処理及び検索処理を実行する。
- [0095] 次に、以上のように構成されたポリシー管理システムの動作の一例について、図2乃至4の模式図と、図6及び図7のシーケンス図とを参照しながら説明する。但し、本動作例では、認証連携装置204の(f204-1)及び(f204-2)の機能を用いた事前処理（ログイン処理）が予め実行され、既に、IDプロバイダ認証トークンが発行されているものとする。また、本動作例では、ユーザ端末を操作するユーザの所属が“X部門”であり、役職が“主任”であり、ユーザ端末によってアクセス要求メッセージが送信された日付（送信日付）が“2011/10/10”であるものとする。
- [0096] 始めに、ユーザ端末100は、ユーザの操作に応じて、事前処理時に発行されたIDプロバイダ認証トークンと、ユーザが利用を希望するサービスデータを提供可能なサービスプロバイダシステム300を示すサービスプロバイダIDとを含むアクセス要求メッセージをIDプロバイダシステム200に送信する（ステップS1）。
- [0097] 続いて、IDプロバイダシステム200内の企業ポータル装置205は、ユーザ端末100からのアクセス要求メッセージの入力を受け付けると、当該入力を受け付けたアクセス要求メッセージをポリシー評価装置206に転送する（ステップS2）。
- [0098] 次に、ポリシー評価装置206内のポリシー評価要求部211は、企業ポータル装置205からのアクセス要求メッセージの入力を受け付けると、当該入力を受け付けたアクセス要求メッセージ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システム300によるユーザ端末100へのサービスデータの送信を許可するための判定条件を定義したポリシーのうち新ポリシー202bを、新ポリシー取得部212を介して取得する（ステップS3）。ここでは、図3に示す新ポリシー202bが取得されたものとする。

- [0099] 続いて、旧ポリシ要否判定部 213 は、ステップ S3 の処理において取得された新ポリシ 202b に定義される移行期間を用いて、ユーザ端末 100 によるアクセス要求メッセージの送信日付が当該移行期間に含まれているか否かを判定する（ステップ S4）。この場合、アクセス要求メッセージの送信日付が“2011/10/10”であり、新ポリシ 202b に定義される移行期間が“2011/10/1～2011/10/30”であるので、当該アクセス要求メッセージの送信日付が当該移行期間に含まれていると判定される。
- [0100] なお、ステップ S4 の判定の結果が否を示す場合には、後述するステップ S6 の処理に進む。
- [0101] ステップ S4 の判定の結果が移行期間に含まれる旨を示す場合には、旧ポリシ要否判定部 213 は、ステップ S3 の処理において取得された新ポリシ 202b に対応した旧ポリシ 202a を、旧ポリシ取得部 214 を介して取得する（ステップ S5）。ここでは、図 2 に示す旧ポリシ 202a が取得されたものとする。
- [0102] 次に、属性情報収集部 215 は、当該アクセス要求メッセージ内の ID プロバイダ認証トークンに含まれるユーザ ID を用いて、ユーザ属性情報格納装置 201 からユーザ属性情報を取得する。その後、属性情報収集部 215 は、当該取得したユーザ属性情報がユーザ属性情報格納装置 301 に格納されているか否かを確認するために、当該取得したユーザ属性情報内のユーザ ID（ユーザの氏名やユーザ属性情報自体でもよい）を含む確認要求メッセージを、ID プロビジョニング装置 207 を介して ID プロビジョニング装置 304 に送信する。ID プロビジョニング装置 304 は、属性情報収集部 215 から送信された確認要求メッセージの入力を受け付けると、当該入力を受け付けた確認要求メッセージ内のユーザ ID がユーザ属性情報格納装置 301 に含まれているか否かを判定（検索）し、当該判定の結果を ID プロバイダシステム 200 に通知する（ステップ S6）。ここでは、ID プロバイダシステム 200 は、属性情報収集部 215 により取得されたユーザ属性情報内のユーザ ID がユーザ属性情報格納装置 301 に格納されている旨の

通知を受けたものとする。

[0103] 続いて、ポリシー評価部 216 は、ステップ S6 の処理において取得されたユーザ属性情報を用いて、当該処理までに取得されたポリシーを評価する、つまり、新ポリシー 202b 及び旧ポリシー 202a の双方を評価する、または新ポリシー 202b のみを評価する（ステップ S7）。ここでは、新ポリシー 202b 及び旧ポリシー 202a の双方を評価する。新ポリシー 202b の評価では、ユーザの所属が“X 部門”であり、役職が“主任”であり、“サービスプロバイダシステムのユーザ ID が登録済み”であるため、図 3 に示す新ポリシー 202b の判定 ID “NEW-DENY-3” の判定条件を満足する（つまり、判定 ID “NEW-DENY-3” が成立する）。また、旧ポリシー 202a の評価では、同様に、ユーザの所属が“X 部門”であり、役職が“主任”であり、“サービスプロバイダシステムのユーザ ID が登録済み”であるため、図 2 に示す旧ポリシー 202a の判定 ID “OLD-PERMIT-2” の判定条件を満足する（つまり、判定 ID “OLD-PERMIT-2” が成立する）。

[0104] 次に、ポリシー差分対応判定部 217 は、上述した(f217-1)乃至(f217-7)の機能を用いて、ポリシー差分対応定義格納装置 203 に格納されたポリシー差分対応定義情報 203a を取得する必要があるか否かを判定する（ステップ S8）。ここでは、ステップ S7 の処理において、新ポリシー 202b 及び旧ポリシー 202a の双方を評価し、新ポリシー 202b では判定 ID “NEW-DENY-3” が成立（つまり、拒否）し、旧ポリシー 202a では判定 ID “OLD-PERMIT-2” が成立（つまり、許可）しているため、ポリシー差分対応判定部 217 は、ポリシー差分対応定義情報 203a を取得する必要があると判断して、図 4 に示すポリシー差分対応定義情報 203a をポリシー差分対応定義取得部 218 を介して取得する。

[0105] 続いて、ID プロビジョニング実行要求部 219 は、適応される判定 ID で識別される条件内の責務に従う処理を実行する（ステップ S9）。ここでは、ステップ S8 の処理において、ポリシー差分対応定義情報 203a が取得されたため、ID プロビジョニング実行要求部 219 は当該ポリシー差分対応

定義情報 203 a を参照した上で、差分対応 ID “DIFF-2” で識別される条件に従って、判定 ID “OLD-PERMIT-2” で識別される条件内の責務 “認証連携要求の実行” を行う、つまり、認証連携送信要求を ID プロビジョニング装置 207 に送信する。

[0106] 次に、ID プロビジョニング装置 207 は、ID プロビジョニング実行要求部 219 から認証連携送信要求を受けると、認証連携要求を認証連携装置 204 に送信する（ステップ S10）。

[0107] 続いて、認証連携装置 204 は、ID プロビジョニング装置 207 から認証連携要求を受けると、ID プロバイダ認証トークン内のユーザ ID を含むアサーション本文に対して、図示しない鍵記憶装置内の署名生成鍵（秘密鍵）に基づく署名を生成し、当該アサーション本文と、当該デジタル署名と、当該署名生成鍵に対応した署名検証鍵（公開鍵）とを含む認証アサーションを作成する（ステップ S11）。

[0108] 次に、認証連携装置 204 は、ステップ S11 の処理において作成した認証アサーションを含む認証連携要求メッセージを、ユーザ端末 100 を介して認証連携装置 302 に送信する（ステップ S12）。

[0109] 続いて、サービスプロバイダシステム 300 内の認証連携装置 302 は、認証連携装置 204 から送信された認証連携要求メッセージの入力を受け付けると、当該入力を受け付けた認証連携要求メッセージ内の認証アサーションに含まれるデジタル署名を、当該認証アサーションに含まれる署名検証鍵を用いて検証する。具体的には、認証連携装置 302 は、認証アサーションに含まれる署名検証鍵を用いてデジタル署名に対応したアサーション本文を復号し、その後、復号したアサーション本文に含まれるユーザ ID が、ユーザ属性情報格納装置 301 内に格納されているか否かを判定することで、認証連携要求メッセージの正当性を検証する（ステップ S13）。ここでは、ステップ S6 の処理において、ユーザ ID がユーザ属性情報格納装置 301 内に格納されていることは確認済みであるので、認証連携装置 302 は当該認証連携要求メッセージは正当であると判断して、当該ユーザ ID を含むサ

ービスプロバイダ認証トークンを発行する。

[0110] 次に、認証連携装置 302 は、ステップ S 13 の処理において発行したサービスプロバイダ認証トークンを含むサービス提供要求メッセージをユーザ端末 100 に送信する（ステップ S 14）。

[0111] 続いて、ユーザ端末 100 は、認証連携装置 302 から送信されたサービス提供要求メッセージの入力を受け付けると、当該入力を受け付けたサービス提供要求メッセージをサービスプロバイダシステム 300 にリダイレクト（返信）する（ステップ S 15）。

[0112] 次に、サービスプロバイダシステム 300 内のサービス提供装置 303 は、ユーザ端末 100 から返信されたサービス提供要求メッセージの入力を受け付けると、当該サービスプロバイダシステム 300 により提供可能なサービスデータをユーザ端末 100 に送信する（ステップ S 16）。

[0113] しかる後、ユーザ端末 100 は、サービスプロバイダシステム 300 から送信されたサービスデータの入力を受け付けると、当該入力を受け付けたサービスデータを再生する（ステップ S 17）。

[0114] 以上説明した一実施形態によれば、差分対応定義情報格納装置 203 及びポリシー評価装置 206 を含む ID プロバイダシステム 200 を備えた構成により、人手を介さずに、ポリシー更新作業を実現することができる。

[0115] 以下に、上述した一実施形態の変形例について説明する。

[0116] [変形例]

ここでは、ポリシー管理システムの動作の変形例について、図 2 及び図 4 の模式図と、図 6 及び図 8 のシーケンス図とを参照しながら説明する。但し、本動作例では、認証連携装置 204 の (f204-1) 及び (f204-2) の機能を用いた事前処理（ログイン処理）が予め実行され、既に、ID プロバイダ認証トークンが発行されているものとする。また、本動作例では、ユーザ端末を操作するユーザの所属が“X 部門”であり、役職が“主任”であり、ユーザ端末によってアクセス要求メッセージが送信された日付（送信日付）が“2011/11/1”であるものとする。

[0117] ステップS 1 乃至 S 3 の処理は、上述した一実施形態と同様に実行される。

[0118] ステップS 4 の処理では、アクセス要求メッセージの送信日付が“2011/11/1”であり、新ポリシ 2 0 2 b に定義される移行期間が“2011/10/1~2011/10/30”であるので、当該アクセス要求メッセージの送信日付が当該移行期間に含まれていないと判定される（つまり、移行期間外であると判定される）。このため、ステップS 5 の処理は省略され、ステップS 6 の処理に進む。

[0119] また、ステップS 6 の処理は、上述した一実施形態と同様に実行される。

[0120] ステップS 7 の処理では、ポリシ評価部 2 1 6 は新ポリシ 2 0 2 b のみを評価する。この場合、ユーザの所属が“X 部門”であり、役職が“主任”であり、“サービスプロバイダシステムのユーザIDが登録済み”であるため、図 3 に示す新ポリシ 2 0 2 b の判定ID “NEW-DENY-3” の判定条件を満足する（つまり、判定ID “NEW-DENY-3” が成立する）。

[0121] ステップS 8 の処理では、ステップS 7 の処理において新ポリシ 2 0 2 b のみを評価し、新ポリシ 2 0 2 b では判定ID “NEW-DENY-3” が成立（つまり、拒否）し、且つ（上述したステップS 6 の処理により）属性情報収集部 2 1 5 によりユーザ属性情報が格納されていることが確認されているため、ポリシ差分対応判定部 2 1 7 は、ポリシ差分対応定義情報 2 0 3 a を取得する必要があると判断して、図 4 に示すポリシ差分対応定義情報 2 0 3 a をポリシ差分対応定義取得部 2 1 8 を介して取得する。

[0122] ステップS 9 の処理では、ステップS 8 の処理において、ポリシ差分対応定義情報 2 0 3 a が取得されたため、IDプロビジョニング実行要求部 2 1 9 は、当該ポリシ差分対応定義情報 2 0 3 a を参照した上で、差分対応ID “DIFF-5” で識別される条件に従って、判定ID “NEW-DENY-3” で識別される条件内の責務“拒否画面表示の実行”を行うと共に、責務“サービスプロバイダシステムのユーザIDの削除を実行”を行う。つまり、IDプロビジョニング実行要求部 2 1 9 は、拒否画面情報送信要求を拒否画面表示装置 2 0 8 に送信すると共に、削除送信要求をIDプロビジョニング装置 2 0 7 に

送信する。

[0123] 続いて、IDプロビジョニング装置207は、IDプロビジョニング実行要求部219から削除送信要求を受けると、IDプロバイダ認証トークン内のユーザIDを含む削除要求メッセージをIDプロビジョニング装置304に送信する（ステップS18）。

[0124] 次に、サービスプロバイダシステム300内のIDプロビジョニング装置304は、IDプロビジョニング装置207から送信された削除要求メッセージの入力を受け付けると、当該入力を受け付けた削除要求メッセージ内のユーザID（ユーザ属性情報）をユーザ属性情報格納装置301から削除する（ステップS19）。

[0125] また、拒否画面表示装置208は、ステップS9の処理において送信された拒否画面情報送信要求を受けると、拒否画面情報をユーザ端末100に送信する（ステップS20）。

[0126] しかる後、ユーザ端末100は、拒否画面表示装置208から送信された拒否画面情報の入力を受け付けると、当該入力を受け付けた拒否画面情報に従って、拒否画面を表示する（ステップS21）。

[0127] 上記した変形例によれば、ポリシ更新に伴うシステム環境の更新作業（つまり、ユーザ属性情報格納装置301に格納されたユーザID（ユーザ属性情報）の削除）も人手を介さずに実現することができる。

[0128] 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。

[0129] 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。

[0130] 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。

[0131] 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。

[0132] 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。

[0133] 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。

[0134] 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。

[0135] 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]

ユーザ端末と、前記ユーザ端末を操作するユーザのアイデンティティを管理するIDプロバイダシステムと、前記ユーザ端末にサービスデータを提供するサービスプロバイダシステムとを含むポリシ管理システムであって、

前記ユーザ端末は、

ユーザの操作に応じて、前記IDプロバイダシステムとの間でログイン処理を実行するログイン実行手段と、

前記ログイン処理時に発行され、当該ユーザを識別するユーザIDを含むIDプロバイダ認証トークンと、前記サービスプロバイダシステムを識別するサービスプロバイダIDとを含むアクセス要求メッセージを前記IDプロバイダシステムに送信する第1送信手段と、

前記サービスプロバイダシステムから送信されるサービスデータを受信し、当該受信したサービスデータを再生する再生手段と

を備え、

前記IDプロバイダシステムは、

前記ユーザを特定するためのユーザの属性の項目名と項目値とを関連付けたユーザ属性情報であって、ユーザIDを少なくとも含むユーザ属性情報を格納する第1格納手段と、

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システムによるサービスデータの送信を許可するための判定条件であって、判定IDで識別される複数の条件を含み、当該各条件は更に複数の詳細条件及び責務を含む判定条件と、旧ポリシから新ポリシに移行するにあたり、新ポリシだけでなく、旧ポリシの判定条件による判定結果も参照する期間を示す移行期間とを少なくとも定義する一対の旧ポリシ及び新ポリシを格納する第2格納手段と、

前記サービスプロバイダID毎に、前記送信されたアクセス要求メ

ッセージの送信日付が前記移行期間内であるときに参照される第1差分判定条件と、前記送信されたアクセス要求メッセージの送信日付が前記移行期間外であるときに参照される第2差分判定条件であって、差分対応IDで識別される条件及び責務を含む第2差分判定条件とを少なくとも定義する差分対応定義情報を格納する第3格納手段と、

前記送信されたアクセス要求メッセージを受けると、当該アクセス要求メッセージ内のサービスプロバイダIDに対応した新ポリシーを取得する第1取得手段と、

当該アクセス要求メッセージの送信日付が前記取得された新ポリシーに定義された移行期間に含まれるか否かを判定する第1判定手段と、

前記第1判定手段による判定結果が含まれる旨を示すとき、前記取得された新ポリシーに対応する旧ポリシーを取得する第2取得手段と、

当該アクセス要求メッセージ内のIDプロバイダ認証トークンに含まれるユーザIDに基づいて、前記第1格納手段に格納されたユーザ属性情報を取得すると共に、当該ユーザIDが当該アクセス要求メッセージ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システムに格納されているか否かを確認する確認手段と、

前記サービスプロバイダシステムから送信され、前記確認手段に対する通知であって、前記ユーザIDが格納されている旨または格納されていない旨を示す通知を受領する通知受領手段と、

前記取得されたユーザ属性情報に基づいて、前記取得された新ポリシーまたは前記取得された新ポリシー及び旧ポリシーを評価するポリシー評価手段と、

前記ポリシー評価手段による評価結果と、前記通知受領手段により受領された通知とに基づいて、前記差分対応定義情報を取得する必要があるか否かを判定する第2判定手段と、

前記第2判定手段による判定結果が必要である旨を示すとき、前記差分対応定義情報を取得する第3取得手段と、

前記評価結果に少なくとも基づいて（但し、前記第3取得手段により差分対応定義情報が取得された場合は当該差分対応定義情報も参照して）、適応する判定IDを決定する決定手段と、

前記決定された判定IDで識別される条件内の責務を実行するよう要求する（但し、前記決定手段により前記差分対応定義情報に定義された第2差分判定条件が参照された場合は当該第2差分判定条件内の責務も実行するよう要求する）実行要求手段と、

前記実行要求手段からの要求に応じて、当該アクセス要求メッセージ内の前記IDプロバイダ認証トークンに含まれるユーザIDを少なくとも含む認証連携メッセージを、当該アクセス要求メッセージ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システムに送信する第2送信手段と、

前記実行要求手段からの要求に応じて、当該アクセス要求メッセージ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によるサービスデータの送信が拒否された旨を表示させる拒否画面情報を前記ユーザ端末に送信する第3送信手段と

を備え、

前記サービスプロバイダシステムは、

サービスデータを利用するユーザを特定するためのユーザの属性の項目名と項目値とを関連付けたユーザ属性情報を格納する第4格納手段と、

前記送信された認証連携要求メッセージを受けると、当該認証連携要求メッセージ内のユーザIDに基づいて当該認証連携要求メッセージの正当性を検証し、当該検証の結果が正当である場合に、当該検証に用いたユーザIDを含むサービスプロバイダ認証トークンを発行する発行手段と、

前記発行されたサービスプロバイダ認証トークン内のユーザIDで識別されるユーザ端末にサービスデータを送信する第4送信手段と

を備えたことを特徴とするポリシー管理システム。

[請求項2]

ユーザを識別するユーザIDを含むIDプロバイダ認証トークンと、サービスプロバイダシステムを識別するサービスプロバイダIDとを含むアクセス要求メッセージを送信するユーザ端末と、前記ユーザ端末にサービスデータを提供し、当該サービスデータを利用するユーザを特定するためのユーザの属性の項目名と項目値とを関連付けたユーザ属性情報を格納する格納手段を含むサービスプロバイダシステムと通信可能なIDプロバイダシステムであって、

前記ユーザを特定するためのユーザの属性の項目名と項目値とを関連付けたユーザ属性情報であって、ユーザIDを少なくとも含むユーザ属性情報を格納する第1格納手段と、

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システムによるサービスデータの送信を許可するための判定条件であって、判定IDで識別される複数の条件を含み、当該各条件は更に複数の詳細条件及び責務を含む判定条件と、旧ポリシーから新ポリシーに移行するにあたり、新ポリシーだけでなく、旧ポリシーの判定条件による判定結果も参照する期間を示す移行期間とを少なくとも定義する一対の旧ポリシー及び新ポリシーを格納する第2格納手段と、

前記サービスプロバイダID毎に、前記送信されたアクセス要求メッセージの送信日付が前記移行期間内であるときに参照される第1差分判定条件と、前記送信されたアクセス要求メッセージの送信日付が前記移行期間外であるときに参照される第2差分判定条件であって、差分対応IDで識別される条件及び責務を含む第2差分判定条件とを少なくとも定義する差分対応定義情報を格納する第3格納手段と、

前記送信されたアクセス要求メッセージを受けると、当該アクセス要求メッセージ内のサービスプロバイダIDに対応した新ポリシーを取得する第1取得手段と、

当該アクセス要求メッセージの送信日付が前記取得された新ポリシに定義された移行期間に含まれるか否かを判定する第 1 判定手段と、

前記第 1 判定手段による判定結果が含まれる旨を示すとき、前記取得された新ポリシに対応する旧ポリシを取得する第 2 取得手段と、

当該アクセス要求メッセージ内の ID プロバイダ認証トークンに含まれるユーザ ID に基づいて、前記第 1 格納手段に格納されたユーザ属性情報を取得すると共に、当該ユーザ ID が当該アクセス要求メッセージ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システムに格納されているか否かを確認する確認手段と、

前記サービスプロバイダシステムから送信され、前記確認手段に対する通知であって、前記ユーザ ID が格納されている旨または格納されていない旨を示す通知を受領する通知受領手段と、

前記取得されたユーザ属性情報に基づいて、前記取得された新ポリシまたは前記取得された新ポリシ及び旧ポリシを評価するポリシ評価手段と、

前記ポリシ評価手段による評価結果と、前記通知受領手段により受領された通知とに基づいて、前記差分対応定義情報を取得する必要があるか否かを判定する第 2 判定手段と、

前記第 2 判定手段による判定結果が必要である旨を示すとき、前記差分対応定義情報を取得する第 3 取得手段と、

前記評価結果に少なくとも基づいて（但し、前記第 3 取得手段により差分対応定義情報が取得された場合は当該差分対応定義情報も参照して）、適応する判定 ID を決定する決定手段と、

前記決定された判定 ID で識別される条件内の責務を実行するよう要求する（但し、前記決定手段により前記差分対応定義情報に定義された第 2 差分判定条件が参照された場合は当該第 2 差分判定条件内の責務も実行するよう要求する）実行要求手段と、

前記実行要求手段からの要求に応じて、当該アクセス要求メッセー

ジ内の前記IDプロバイダ認証トークンに含まれるユーザIDを少なくとも含む認証連携メッセージを、当該アクセス要求メッセージ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システムに送信する第1送信手段と、

前記実行要求手段からの要求に応じて、当該アクセス要求メッセージ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によるサービスデータの送信が拒否された旨を表示させる拒否画面情報を前記ユーザ端末に送信する第2送信手段と

を備えたことを特徴とするIDプロバイダシステム。

[請求項3]

ユーザを識別するユーザIDを含むIDプロバイダ認証トークンと、サービスプロバイダシステムを識別するサービスプロバイダIDとを含むアクセス要求メッセージを送信するユーザ端末と、前記ユーザ端末にサービスデータを提供し、当該サービスデータを利用するユーザを特定するためのユーザの属性の項目名と項目値とを関連付けたユーザ属性情報を格納する格納手段を含むサービスプロバイダシステムと通信可能であり、前記ユーザを特定するためのユーザの属性の項目名と項目値とを関連付けたユーザ属性情報であって、ユーザIDを少なくとも含むユーザ属性情報を格納する第1格納手段と、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システムによるサービスデータの送信を許可するための判定条件であって、判定IDで識別される複数の条件を含み、当該各条件は更に複数の詳細条件及び責務を含む判定条件と、旧ポリシーから新ポリシーに移行するにあたり、新ポリシーだけでなく、旧ポリシーの判定条件による判定結果も参照する期間を示す移行期間とを少なくとも定義する一対の旧ポリシー及び新ポリシーを格納する第2格納手段と、前記サービスプロバイダID毎に、前記送信されたアクセス要求メッセージの送信日付が前記移行期間内であるときに参照される第1差分判定条件と、前記送信されたアクセス要求メッセージの送信日付が前

記移行期間外であるときに参照される第2差分判定条件であって、差分対応IDで識別される条件及び責務を含む第2差分判定条件とを少なくとも定義する差分対応定義情報を格納する第3格納手段とを含むIDプロバイダシステムに用いられるポリシ評価装置であって、

前記送信されたアクセス要求メッセージを受けると、当該アクセス要求メッセージ内のサービスプロバイダIDに対応した新ポリシを取得する第1取得手段と、

当該アクセス要求メッセージの送信日付が前記取得された新ポリシに定義された移行期間に含まれるか否かを判定する第1判定手段と、

前記第1判定手段による判定結果が含まれる旨を示すとき、前記取得された新ポリシに対応する旧ポリシを取得する第2取得手段と、

当該アクセス要求メッセージ内のIDプロバイダ認証トークンに含まれるユーザIDに基づいて、前記第1格納手段に格納されたユーザ属性情報を取得すると共に、当該ユーザIDが当該アクセス要求メッセージ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システムに格納されているか否かを確認する確認手段と、

前記サービスプロバイダシステムから送信され、前記確認手段に対する通知であって、前記ユーザIDが格納されている旨または格納されていない旨を示す通知を受領する通知受領手段と、

前記取得されたユーザ属性情報に基づいて、前記取得された新ポリシまたは前記取得された新ポリシ及び旧ポリシを評価するポリシ評価手段と、

前記ポリシ評価手段による評価結果と、前記通知受領手段により受領された通知とに基づいて、前記差分対応定義情報を取得する必要があるか否かを判定する第2判定手段と、

前記第2判定手段による判定結果が必要である旨を示すとき、前記差分対応定義情報を取得する第3取得手段と、

前記評価結果に少なくとも基づいて（但し、前記第3取得手段によ

り差分対応定義情報が取得された場合は当該差分対応定義情報も参照して)、適応する判定IDを決定する決定手段と、

前記決定された判定IDで識別される条件内の責務を実行するよう要求する(但し、前記決定手段により前記差分対応定義情報に定義された第2差分判定条件が参照された場合は当該第2差分判定条件内の責務も実行するよう要求する)実行要求手段と

を備えたことを特徴とするポリシ評価装置。