

明 細 書

発明の名称： ポリシ更新システム及びポリシ更新装置

技術分野

[0001] 本発明の実施形態は、ポリシ更新システム及びポリシ更新装置に関する。

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

特許文献２：特開２００７－３２３３５７号公報

非特許文献

- [0025] 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>

発明の概要

発明が解決しようとする課題

- [0026] 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。
- [0027] 通常、企業では、組織変更や人事異動が行われると、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が更新される。これに伴い、ポリシーの更新作業やシステム環境の更新作業を行う必要があり、一般的に、これら作業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やシステム環境更新作業を行う）。
- [0028] 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。
- [0029] 本発明が解決しようとする課題は、人手を介さずに、ポリシー更新作業及びシステム環境更新作業を実現し得るポリシー更新システム及びポリシー更新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] 実施形態のポリシー更新システムは、ユーザに複数のサービスを提供可能なサーバ装置であって、前記各サービスを利用可能なユーザを識別する第1ユーザIDを前記サービス毎に少なくとも記憶する記憶手段を有したサーバ装置と、前記ユーザに関するアイデンティティ情報であり、前記第1ユーザIDに対応した第2ユーザIDを少なくとも含む複数の項目が関連付けられたユーザ属性情報を記述した少なくとも1つの条件から成り、前記ユーザ属性情報の値が前記条件を満足するときに前記サービスの利用を許可する前記各サービスの利用権限を規定した複数のポリシーを記憶するポリシー記憶装置と、前記ユーザ属性情報が変更されたときに前記記憶された各ポリシーを更新可能なポリシー更新装置と、変更後のユーザ属性情報と、変更前のユーザ属性情報

と変更後のユーザ属性情報との間で異なる値を示す変更内容であって、変更前のユーザ属性情報の値と変更後のユーザ属性情報の値とを含む前記第2ユーザID毎の変更内容とを記憶するユーザ属性情報記憶装置とを含む。

[0031] 前記ポリシ更新装置は、検出手段、作成手段、収集手段、評価手段、特定手段、更新手段及び削除手段を備えている。

[0032] 前記検出手段は、前記ユーザ属性情報記憶装置に記憶された変更内容に基づいて、前記ポリシ記憶装置に記憶された各ポリシのうち、修正が必要となる修正対象ポリシを検出する。

[0033] 前記作成手段は、前記検出された修正対象ポリシに記述されたユーザ属性情報の値を、前記記憶された変更内容内の変更前のユーザ属性情報の値から変更後のユーザ属性情報の値に修正した修正ポリシを作成する。

[0034] 前記収集手段は、前記サーバ装置により提供されるサービスを利用可能なユーザの第2ユーザIDを含む変更後のユーザ属性情報をポリシ評価用ユーザ属性情報として前記ユーザ属性情報記憶装置から収集する。

[0035] 前記評価手段は、前記ポリシ記憶装置に記憶された各ポリシのうち、前記作成された修正ポリシを除くポリシと、前記作成された修正ポリシとに基づいて、前記収集されたポリシ評価用ユーザ属性情報を前記第2ユーザID毎に評価する。

[0036] 前記特定手段は、前記評価手段による評価結果のうち、前記ユーザ属性情報記憶装置に記憶された変更内容内の変更前のユーザ属性情報の値ではポリシを満足するが、前記収集されたポリシ評価用ユーザ属性情報の値ではポリシ及び／または修正ポリシを満足しない旨の評価結果を示す第2ユーザIDを特定する。

[0037] 前記更新手段は、前記ポリシ記憶装置に記憶された各ポリシのうち、前記作成した修正ポリシに対応するポリシを当該修正ポリシに更新する。

[0038] 前記削除手段は、前記特定された第2ユーザIDに対応する第1ユーザIDを前記サーバ装置内の前記記憶手段から削除する。

図面の簡単な説明

[0039] [図1]図 1 は一実施形態に係るポリシ更新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ユーザストアに記憶されるユーザ関連情報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ユーザストアに記憶されるユーザ関連情報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ユーザストアに記憶されるユーザ関連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ユーザストアに記憶されるユーザ関連情報の一例を示す模式図である。

[図6]図 6 は同実施形態に係るユーザストアに記憶されるユーザ関連情報の一例を示す模式図である。

[図7]図 7 は同実施形態に係るユーザストアに記憶されるユーザ関連情報の一例を示す模式図である。

[図8]図 8 は同実施形態に係るユーザストアに記憶されるユーザ関連情報の一例を示す模式図である。

[図9]図 9 は同実施形態に係るユーザストアに記憶されるユーザ関連情報の一例を示す模式図である。

[図10]図 10 は同実施形態に係る 1D 記憶装置に記憶される 1D 登録情報の一例を示す模式図である。

[図11]図 11 は同実施形態に係る 1D 記憶装置に記憶される 1D 登録情報の一例を示す模式図である。

[図12]図 12 は同実施形態に係る 1D 記憶装置に記憶される 1D 登録情報の一例を示す模式図である。

[図13]図 13 は同実施形態に係るポリシ記憶装置に記憶されるポリシの一例を示す模式図である。

[図14]図 14 は同実施形態に係る削除ユーザ一時記憶装置に記憶される削除対象ユーザ情報の一例を示す模式図である。

[図15]図15は同実施形態に係る修正ポリシ作成装置の動作の一例を示すフローチャートである。

[図16]図16は同実施形態に係るポリシ評価用ユーザ属性情報の一例を示す模式図である。

[図17]図17は同実施形態に係る評価結果情報の一例を示す模式図である。
[図18]図18は同実施形態に係る削除ユーザ特定装置の動作の一例を示すフローチャートである。

[図19]図19は同実施形態に係るユーザ削除承認装置の動作の一例を示す模式図である。

[図20]図20は同実施形態に係る修正ポリシの一例を示す模式図である。

発明を実施するための形態

[0040] 図1は一実施形態に係るポリシ更新システムの構成例を示す模式図であり

、図2乃至図9は同実施形態に係るユーザストアに記憶されるユーザ関連情報の一例を示す模式図であり、図10乃至図12は同実施形態に係るID記憶装置に記憶されるID登録情報の一例を示す模式図であり、図13は同実施形態に係るポリシ記憶装置に記憶されるポリシの一例を示す模式図であり、図14は同実施形態に係る削除ユーザ一時記憶装置に記憶される削除対象ユーザ情報の一例を示す模式図であり、図15は同実施形態に係る修正ポリシ作成装置の動作の一例を示すフローチャートであり、図16は同実施形態に係るポリシ評価用ユーザ属性情報の一例を示す模式図であり、図17は同実施形態に係る削除ユーザ特定装置の動作の一例を示すフローチャートであり、図19は同実施形態に係るユーザ削除承認装置の動作の一例を示す模式図であって、図20は同実施形態に係る修正ポリシの一例を示す模式図である。

[0041] ポリシ更新システム1は、図1に示すように、ユーザストア10、クラウドサーバ装置20、ポリシ記憶装置30及びポリシ更新装置40を備えており、なお、ポリシ更新装置40と、ユーザストア10、クラウドサーバ装置20及びポリシ記憶装置30とは、有線又は無線を介して通信可能である。

- [0042] ユーザストア 10 は、図 1 に示すように、変更前ユーザストア 10A 及び変更後ユーザストア 10B を更に備えている。
- [0043] 変更前ユーザストア 10A は、図 2 乃至図 6 に示すように、変更前のユーザ関連情報を記憶する記憶装置である。ユーザ関連情報とは、クラウドサーバ装置 20 により提供される SaaS (Software as a Service) を利用し、且つポリシ更新装置 40 が配置される組織に所属するユーザに関する情報であり、具体的には、ユーザ属性情報、部情報、課情報、役職情報及び SaaS 情報などの情報である。なお、ユーザ関連情報は、上記したユーザ属性情報、部情報、課情報、役職情報及び SaaS 情報に限定されるものでない。
- [0044] ユーザ属性情報とは、上記ユーザに関するアイデンティティ情報であり、例えば、図 2 に示すように、ユーザ Id (userId)、ユーザ名、部 Id、課 Id、役職 Id 及びメールアドレスが関連付けられた情報、つまり、個人の情報を特徴付ける情報の集合体である。ユーザ Id はユーザを識別するための識別情報である。部 Id はポリシ更新装置 40 が配置される組織を構成する部を識別するための識別情報である。課 Id はポリシ更新装置 40 が配置される組織を構成する課を識別するための識別情報である。役職 Id はポリシ更新装置 40 が配置される組織に所属するユーザの役職を識別するための識別情報である。
- [0045] 部情報とは、ポリシ更新装置 40 が配置される組織を構成する部に関する情報であり、例えば、図 3 に示すように、部 Id、部名及び削除フラグが関連付けられた情報である。部名は、例えば、総務部、営業部、研究部及び開発部など、部 Id で識別される部の名称を示す。削除フラグは当該削除フラグを含む情報、この場合、部情報が削除対象の情報であるか否かを示すものであり、「true」又は「false」のどちらか一方を示す。具体的には、削除フラグが「true」を示す場合は、当該削除フラグを含む情報が削除対象の情報であることを示し、削除フラグが「false」を示す場合は、当該削除フラグを含む情報が非削除対象の情報であることを示す。なお、削除フラグが「true」を示したとしても、当該削除フラグを含む情報は削除されたわけではなく

、あくまで削除フラグは当該削除フラグを含む情報が削除対象であるか否かを示す情報である。

[0046] 課情報とは、ポリシー更新装置40が配置される組織を構成する課に関する情報であり、例えば、図4に示すように、課Ｉｄ、課名及び削除フラグが関連付けられた情報である。課名は、例えば、〇〇技術課、××技術課及び開発支援技術課など、課Ｉｄで識別される課の名称を示す。

[0047] 役職情報とは、ポリシー更新装置40が配置される組織に存在する役職に関する情報であり、例えば、図5に示すように、役職Ｉｄ、役職名及び削除フラグが関連付けられた情報である。役職名は、例えば、部長、課長及び担当など、役職Ｉｄで識別される役職の名称を示す。

[0048] ＳａａＳ情報とは、ポリシー更新装置40が配置される組織が利用可能なＳａａＳに関する情報であり、例えば、図6に示すように、ＳａａＳＩｄ、ＳａａＳ名及び管理者Ｉｄが関連付けられた情報である。ＳａａＳＩｄは、クラウドサーバ装置20により提供されるＳａａＳのうち、ポリシー更新装置40が配置される組織が利用可能なＳａａＳを識別するための識別情報である。ＳａａＳ名は、例えば、ＳａａＳ1乃至ＳａａＳ3など、ＳａａＳＩｄで識別されるＳａａＳの名称を示す。管理者Ｉｄは、ポリシー更新装置40が配置される組織において、関連付けられたＳａａＳＩｄで識別されるＳａａＳの利用者を管理するユーザのユーザＩｄを示す情報である。

[0049] なお、本実施形態では、変更前ユーザストア10Aには、変更前のユーザ属性情報が図2に示すような形式で記憶されたとしたが、これに限定されず、例えば、変更前のユーザ属性情報と変更後のユーザ属性情報との間で異なる値を示す変更内容であって、変更前のユーザ属性情報の値と変更後のユーザ属性情報の値とを含むユーザＩｄ毎の変更内容のみを示す形式で記憶されとしてもよい。

[0050] 変更後ユーザストア10Bは、図7乃至図9に示すように、変更前ユーザストア10Aに記憶されたユーザ関連情報から変更されたユーザ関連情報を記憶する記憶装置である。なお、変更後のユーザ関連情報は、変更前のユー

ザ関連情報と同様な形式の情報であるため、ここでは詳細な説明は省略する。また、本実施形態では、役職情報及びSaaS情報は変更されないとして変更後の役職情報及びSaaS情報を図示しないが、別の態様において、図5及び図6と同様な形式の変更後の役職情報及びSaaS情報が変更後ユーザストア10Bに記憶されてもよいことは明白なことである。

[0051] クラウドサーバ装置20は、複数のSaaSをユーザに対して提供する装置である。クラウドサーバ装置20は、複数のID記憶装置20Aを備えており、これらID記憶装置20Aは、例えば、図10乃至図12に示すように、SaaSを利用可能なユーザのユーザIDとユーザ名とが関連付けられたID登録情報を、クラウドサーバ装置20が提供可能なSaaS毎に記憶する記憶装置である。本実施形態では、SaaS1乃至SaaS3にそれぞれ対応したID記憶装置20Aがクラウドサーバ装置20内に設けられる。

[0052] なお、本実施形態では、ユーザストア10に記憶されるユーザ関連情報、この場合、ユーザ属性情報内のユーザIDと、各ID記憶装置20Aに記憶されるID登録情報内のユーザIDとが同様な形式のユーザIDであるとして説明するが、これに限定されず、ユーザ属性情報内のユーザIDとID登録情報内のユーザIDとは対応付けられていれば、必ずしも同様な形式のユーザIDでなくとも構わない。

[0053] ポリシ記憶装置30は、例えば、図13に示すようにクラウドサーバ装置20により提供されるSaaSの現行の利用権限を規定した少なくとも1つの条件から成るポリシを記憶する記憶装置である。より詳細には、ポリシとは、ユーザ関連情報を用いた少なくとも1つの条件から成り、SaaSを利用する際に通知されるユーザ関連情報が当該条件を満足する場合に許可、つまり、SaaSの利用を許可し、許可を示さない場合にはSaaSの利用を拒否するもの（禁止型ポリシ）である。図13では、クラウドサーバ装置20により提供される3つのSaaS、つまり、SaaS1乃至SaaS3に関するポリシの一例を示す。例えば、SaaS1に関するポリシは、ユーザ関連情報が「部IDがdept3であり、且つ役職IDがpost1またはpost2である

」という条件を満足する場合に、S a a S 1の利用を許可し、それ以外はS a a S 1の利用を拒否するポリシーである。なお、ポリシーの記述形式は、図13に示す記述形式に限定されるものでなく、例えば、各種名称（部名、課名及び役職名など）を用いて記述するなど、任意の記述形式で構わない。

[0054] ここで、ポリシー更新装置40は、図1に示すように、修正ポリシー時記憶装置41、削除ユーザー時記憶装置42、修正ポリシー作成装置43、削除ユーザー特定装置44、ユーザー削除承認装置45、ポリシー更新装置46及びユーザー削除装置47を備えている。

[0055] 修正ポリシー時記憶装置41は、修正ポリシー作成装置43により作成される修正ポリシーを含む複数のポリシーを一時的に記憶する記憶装置である。

[0056] 削除対象ユーザー時記憶装置42は、例えば、図14に示すように、削除ユーザー特定装置により生成される削除対象ユーザー情報を一時的に記憶する記憶装置である。削除対象ユーザー情報とは、ユーザーID及び削除対象S a a Sが関連付けられた情報である。

[0057] 修正ポリシー作成装置43は、図1に示すように、修正対象ポリシー検出部43A、修正ポリシー作成部43B及び修正ポリシー保存部43Cを更に備えている。

[0058] 修正対象ポリシー検出部43Aは、変更前ユーザーストア10A及び変更後ユーザーストア10Bに各々記憶されたユーザー関連情報と、ポリシー記憶装置30に記憶されたポリシーとに基づいて、修正が必要なポリシー（以下、修正対象ポリシーと表記）を検出する。具体的には、修正対象ポリシー検出部43Aは、以下の各機能(f43A-1)乃至(f43A-4)をもっている。

[0059] (f43A-1) 変更前ユーザーストア10A及び変更後ユーザーストア10Bに記憶されたユーザー関連情報を参照しながら、変更前のユーザー関連情報と変更後のユーザー関連情報、この場合、変更前のユーザー属性情報 U_B と変更後のユーザー属性情報 U_A とを比較して、変更前のユーザー属性情報 U_B と変更後のユーザー属性情報 U_A とで異なる内容、つまり、変更前の値と変更後の値とを含む変更内容をユーザーID毎に検出する機能。

- [0060] なお、上記したように、変更前ユーザストア 10A に記憶された変更前のユーザ属性情報が変更内容のみを示す形式である場合、当該 (f43-1) の機能は省略される。
- [0061] (f43A-2) 変更前ユーザストア 10A 及び変更後ユーザストア 10B に記憶されたユーザ関連情報を参照して、(f43A-1) の機能により検出した変更内容に含まれる変更後の値が変更前のユーザ関連情報、この場合、変更前の部情報 D_B 、課情報 S_B 及び役職情報 P_B に含まれる値 (I_d) のみから成るか否かを変更内容毎に判定する機能。
- [0062] なお、(f43-1) の機能が省略される場合、当該 (f43-2) の機能は、変更前ユーザストア 10A 及び変更後ユーザストア 10B に記憶されたユーザ関連情報を参照して、変更前ユーザストア 10A に記憶された変更内容内の変更後の値が変更前の部情報 D_B 、課情報 S_B 及び役職情報 P_B に含まれる値 (I_d) のみから成るか否かを変更内容毎に検出する機能となる。
- [0063] (f43A-3) (f43A-2) の機能による判定結果が変更前のユーザ関連情報のみから成る旨を示す場合、当該変更内容がポリシーに影響を及ぼすものでないとした上で、ポリシー記憶装置 30 に記憶されたポリシーを参照して、当該変更内容に関連付けられたユーザ I_d で識別される変更前のユーザ関連情報、この場合、変更前のユーザ属性情報 U_B が満足するポリシーを修正対象ポリシーとして検出しない機能。
- [0064] (f43A-4) (f43A-2) の機能による判定結果が否を示す場合、当該変更内容がポリシーに影響を及ぼすものであるとした上で、ポリシー記憶装置 30 に記憶されたポリシーを参照して、当該変更内容に関連付けられたユーザ I_d で識別される変更前のユーザ関連情報、この場合、変更前のユーザ属性情報 U_B が満足するポリシーを修正対象ポリシーとして検出する機能。
- [0065] 修正ポリシー作成部 43B は、修正ポリシー検出部 43A により検出された修正対象ポリシーに記述されたユーザ関連情報を、検出した変更内容に含まれる変更前の値から変更後の値に修正した修正ポリシーを作成する。
- [0066] 修正ポリシー保存部 43C は、修正対象ポリシー検出部 43A により検出され

た修正対象ポリシ以外のポリシ（即ち、修正対象ポリシとして検出されなかったポリシ）と、修正ポリシ作成部43Bにより作成された修正ポリシとを修正ポリシ一時記憶装置41に書込む。

[0067] ここで、以上のように構成された修正ポリシ作成装置の動作の一例について、図2乃至図9、図13の模式図と、図15のフローチャートとを参照しながら説明する。

[0068] 始めに、修正対象ポリシ検出部43Aは、変更前ユーザストア10A及び変更後ユーザストア10Bに記憶されたユーザ関連情報を参照しながら、変更前のユーザ属性情報 U_B と変更後のユーザ属性情報 U_A とを比較して、変更前のユーザ属性情報 U_B と変更後のユーザ属性情報 U_A とで異なる値を示す変更内容をユーザID毎に検出する（ステップS1）。

[0069] 具体的には、修正対象ポリシ検出部43Aは、user03の「sect1-sect2」、user06の「sect2-sect1」、user08の「dept3, sect3, post2-dept5, sect4, post1」、user09の「dept3, sect3, post3-dept5, sect4, post2」、user10の「dept3, sect3-dept5, sect4」を変更内容（以下、順に変更内容A乃至Eと表記）として検出する。なお、ここでは、“（ユーザID）の「（変更前の値）-（変更後の値）」”の形式を用いて変更内容を示している。

[0070] 続いて、修正対象ポリシ検出部43Aは、変更前ユーザストア10A及び変更後ユーザストア10Bに記憶されたユーザ関連情報を参照して、検出した変更内容A乃至Eに含まれる変更後の値が変更前の部情報 D_B 、課情報 S_B 及び役職情報 P_B に含まれる値（ID）のみから成るか否かを変更内容A乃至E毎に判定する（ステップS2）。

[0071] 具体的には、変更内容A及びBの変更後の値は、sect2またはsect1であり、これらsect2またはsect1は、図4に示すように、変更前の課情報 S_B に含まれるため、変更内容A及びBは、修正対象ポリシ検出部43Aにより変更前のユーザ関連情報（課情報 S_B ）のみから成ると判定される。また、変更内容C乃至Eの変更後の値は、dept5やsect4を含んでおり、これらdept5やsect4は、図3及び図4に示すように、変更前の部情報 D_B 及び課情報 S_B には含ま

れていないため、変更内容C乃至Eは、修正対象ポリシ検出部43Aにより変更前のユーザ関連情報（部情報D_B及び課情報S_B）のみから成らないと判定される。

[0072] ステップS2の処理による判定結果が変更前のユーザ関連情報のみから成る旨を示す場合（ステップS2のYes）には、修正対象ポリシ検出部43Aは、当該変更内容A及びBがポリシに影響を及ぼすものでないとした上で、ポリシ記憶装置30に記憶されたポリシを参照して、当該変更内容A及びBに関連付けられたユーザId「user03」及び「user06」で識別される変更前のユーザ属性情報U_{B3}、U_{B6}が満足するポリシP₁、P₂を修正対象ポリシとして検出しない（ステップS3）。

[0073] ステップS2の処理による判定結果が否を示す場合（ステップS2のNo）には、修正対象ポリシ検出部43Aは、当該変更内容C乃至Eがポリシに影響を及ぼすものであるとした上で、ポリシ記憶装置30に記憶されたポリシを参照して、当該変更内容C乃至Eに関連付けられたユーザId「user08」、「user09」及び「user10」で識別される変更前のユーザ属性情報U_{B8}乃至U_{B10}が満足するポリシP₃を修正対象ポリシとして検出する（ステップS4）。

[0074] 次に、修正ポリシ作成部44Bは、ステップS4の処理において検出された修正対象ポリシP₃に記述されたユーザ属性情報「dept3」及び「sect3」を、当該変更内容C乃至Eに含まれる変更後の値「dept5」及び「sect4」に修正した修正ポリシを作成する（ステップS5）。

[0075] しかる後、修正ポリシ保存部43Cは、ステップS3の処理において修正対象ポリシとして検出されなかったポリシP₁、P₂と、ステップS5の処理において作成された修正ポリシとを修正ポリシ一時記憶装置41に書込む（ステップS6）。

[0076] 削除ユーザ特定装置44は、図1に示すように、ユーザ属性情報収集部44A、ポリシ評価部44B及び削除ユーザ保存部44Cを更に備えている。

[0077] ユーザ属性情報収集部44Aは、例えば、図16に示すように、クラウド

サーバ装置 20 より提供される SaaS を利用可能なユーザの変更後のユーザ属性情報をポリシー評価に必要な情報（以下、ポリシー評価用ユーザ属性情報と表記）として収集する。具体的には、ユーザ属性情報収集部 44A は、以下の各機能(f44A-1)及び(f44A-2)をもっている。

[0078] (f44A-1) クラウドサーバ装置 20 内の各 ID 記憶装置 20A に記憶された ID 登録情報を参照しながら、ID 登録情報内のユーザ ID を含む変更後のユーザ関連情報、この場合、変更後のユーザ属性情報 U_A をポリシー評価用ユーザ属性情報として変更後ユーザストア 10B から収集する機能。

[0079] (f44A-2) (f44A-1)の機能により収集されたポリシー評価用ユーザ属性情報を図示しない一時メモリに書込む機能。

[0080] ポリシー評価部 44B は、修正ポリシー時記憶装置 41 に記憶されたポリシー及び修正ポリシーに基づいて、ユーザ属性情報収集部 44A により収集されたポリシー評価用ユーザ属性情報を評価する。具体的には、ポリシー評価部 44B は、以下の各機能(f44B-1)及び(f44B-2)をもっている。

[0081] (f44B-1) 修正ポリシー時記憶装置 41 に記憶されたポリシー及び修正ポリシーに基づいて、ユーザ属性情報収集部 44A により収集されたポリシー評価用ユーザ属性情報を評価する、つまり、ポリシー評価用ユーザ属性情報がポリシー及び修正ポリシーを満足するか否かを評価する機能。

[0082] (f44B-2) (f44B-1)の機能による評価結果を示す評価結果情報を生成した後に、当該生成した評価結果情報を図示しない一時メモリに書込む機能。

[0083] なお、評価結果情報は、例えば、図 17 に示すように、ユーザ ID、ユーザ名及び SaaS 利用権限が関連付けられた情報である。SaaS 利用権限はポリシー更新装置 40 が配置される組織に対してクラウドサーバ装置 20 が提供可能な SaaS に対応しており、ここでは、SaaS 1 乃至 SaaS 3 の利用権限に関する評価結果を示す。具体的には、SaaS 利用権限は、図 17 に示すように、「許可」、「拒否」または「-」のいずれかの値を用いて表す。「許可」は、ポリシー評価用ユーザ属性情報が当該 SaaS に関するポリシー及び／または修正ポリシーを満足した旨の評価結果を示す。「拒否」は

、変更前のユーザ属性情報 U_B では当該 $SaaS$ に関するポリシーを満足するが、ポリシー評価用ユーザ属性情報では当該 $SaaS$ に関するポリシー及び／または修正ポリシーを満足しない旨の評価結果を示す。「－」は、変更前のユーザ属性情報 U_B とポリシー評価用ユーザ属性情報とが共に当該 $SaaS$ に関するポリシー及び／または修正ポリシーを満足しない旨の評価結果を示す。

[0084] 削除ユーザ保存部44Cは、ポリシー評価部44Bにより生成された評価結果情報に基づいて、削除対象ユーザ情報を生成した後に、当該生成した削除対象ユーザ情報を削除対象ユーザー一時記憶装置42に書込む。

[0085] なお、削除対象ユーザ情報は、例えば、図14に示すように、ユーザID及び削除対象 $SaaS$ が関連付けられた情報である。削除対象 $SaaS$ はポリシー更新装置40が配置される組織に対してクラウドサーバ装置20が提供可能な $SaaS$ に対応しており、ここでは、 $SaaS1$ 乃至 $SaaS3$ に対応する各ID記憶装置20Aに記憶されたID登録情報の削除に関する。具体的には、削除対象 $SaaS$ は、図14に示すように、「○」、「×」及び「－」のいずれかの値を用いて表す。「○」は、ポリシー評価部44Bにより生成された評価結果情報内の $SaaS$ 利用権限の「拒否」に対応し、当該 $SaaS$ に対応するID記憶装置20Aに記憶され、当該削除対象 $SaaS$ に関連付けられたユーザIDを含むID登録情報が削除対象である旨を示す。

「×」は、ポリシー評価部44Bにより生成された評価結果情報内の $SaaS$ 利用権限の「許可」に対応し、当該 $SaaS$ に対応するID記憶装置20Aに記憶され、当該削除対象 $SaaS$ に関連付けられたユーザIDを含むID登録情報が非削除対象である旨を示す。「－」は、ポリシー評価部44Bにより生成された評価結果情報内の $SaaS$ 利用権限の「－」に対応し、当該 $SaaS$ に対応するID記憶装置20Aに当該削除対象 $SaaS$ に関連付けられたユーザIDを含むID登録情報が記憶されていない旨を示す。

[0086] ここで、以上のように構成された削除ユーザ特定装置の動作の一例について、図7、図10乃至図12、図14、図17の模式図と、図18のフローチャートとを参照しながら説明する。但し、本動作例では、修正ポリシー作成

装置 4 3 により上記したステップ S 1 乃至 S 6 の処理が実行され、修正ポリシー時記憶装置 4 1 には、ポリシー P₁、P₂とポリシー P₃に対応する修正ポリシーが記憶されているものとする。

[0087] ステップ S 6 の処理に続いて、ユーザ属性情報収集部 4 4 A は、クラウドサーバ装置 2 0 内の各 I D 記憶装置 2 0 A に記憶された I D 登録情報 R₁乃至 R₃を参照しながら、I D 登録情報 R₁乃至 R₃内のユーザ I D を含む変更後のユーザ関連情報、この場合、変更後のユーザ属性情報 U_{A1}乃至 U_{A3}、U_{A8}乃至 U_{A10}をポリシー評価用ユーザ属性情報 M として変更後ユーザストア 1 0 B から収集する（ステップ S 7）。

[0088] 次に、ポリシー評価部 4 4 B は、修正ポリシー時記憶装置 4 1 に記憶されたポリシー P₁、P₂及び修正ポリシーに基づいて、ステップ S 7 の処理において収集されたポリシー評価用ユーザ属性情報 M を評価する、つまり、ポリシー評価用ユーザ属性情報 M がポリシー P₁、P₂及び修正ポリシーを満足するか否かを評価する（ステップ S 8）。

[0089] 続いて、ポリシー評価部 4 4 B は、図 1 7 に示すように、ステップ S 8 の処理による評価結果を示す評価結果情報 N を生成する（ステップ S 9）。

[0090] しかる後、削除ユーザ保存部 4 4 C は、ステップ S 9 の処理により生成された評価結果情報 N に基づいて、図 1 4 に示すような削除対象ユーザ情報 T を生成した後に、当該生成した削除対象ユーザ情報 T を削除ユーザ一時記憶装置 4 2 に書込む（ステップ S 1 0）。

[0091] ユーザ削除承認装置 4 5 は、図 1 に示すように、承認依頼部 4 5 A、削除対象ユーザ削除部 4 5 B 及び修正ポリシー修正部 4 5 C を備えている。

[0092] 承認依頼部 4 5 A は、削除対象ユーザ一時記憶装置 4 2 に記憶された削除対象ユーザ情報内の削除対象 S a a S が削除対象である旨の値を示す S a a S に関して、変更前ユーザストア 1 0 A に記憶された変更前のユーザ関連情報、この場合、当該 S a a S に関する S a a S 情報内の管理者 I D で識別されるユーザ（の管理者端末）に対して、当該削除対象 S a a S に関連付けられたユーザ I D を含む I D 登録情報を当該 S a a S に対応した I D 記憶装置

20Aから削除することに関する承認／却下を依頼する。

[0093] なお、管理者端末は承認依頼部45Aからの依頼を受けると、ユーザ（管理者）の操作に応じて、当該依頼を承認するまたは却下する旨のメッセージとユーザIDとを含む応答メッセージをユーザ削除承認装置45に送信する。

[0094] 削除対象ユーザ削除部45Bは、管理者端末から送信された却下する旨のメッセージを含む応答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応答メッセージ内のユーザIDを含む削除対象ユーザ情報を削除ユーザ一時記憶装置42から削除する。

[0095] 修正ポリシ修正部45Cは、削除対象ユーザ削除部45Bで入力を受け付けた応答メッセージ内のユーザIDで識別されるユーザが、削除対象ユーザ情報内の当該ユーザIDに関連付けられた削除対象SaaSが削除対象である旨の値を示すSaaSを継続して利用できるよう、当該SaaSに関するポリシを修正した修正ポリシを作成し、修正ポリシ一時記憶装置41に記憶された当該SaaSに関するポリシを当該作成した修正ポリシに更新する（書き換える）。

[0096] ここで、以上のように構成されたユーザ削除承認装置の動作の一例について、図6、図10乃至図12、図20の模式図と、図19のフローチャートとを参照しながら説明する。但し、本動作例では、修正ポリシ作成装置43により上記したステップS1乃至S6の処理が実行され、修正ポリシ一時記憶装置41には、ポリシP₁、P₂とポリシP₃に対応する修正ポリシとが記憶されているものとし、また、削除ユーザ特定装置44により上記したステップS7乃至S10の処理が実行され、削除ユーザ一時記憶装置42には、図14に示す削除対象ユーザ情報が記憶されているものとする。

[0097] ステップS10の処理に続いて、承認依頼部45Aは、削除対象ユーザ一時記憶装置42に記憶された削除対象ユーザ情報T内の削除対象SaaSが削除対象である旨の値を示すSaaS1及びSaaS2に関して、変更前ユーザストア10Aに記憶された当該SaaS1及びSaaS2に関するSaaS

a S 情報 S a₁, S a₂内の管理者 I D 「user01」 及び「user02」で識別されるユーザ（の管理者端末）に対して、当該削除対象 S a a S に関連付けられたユーザ I D 「user08」 及び「user03」を含む I D 登録情報 R 1₃, R 2₂を当該 S a a S 1 及び S a a S 2 に対応した各 I D 記憶装置 2 0 A から削除することに関する承認／却下を依頼する（ステップ S 1 1）。

[0098] なお、ここでは、管理者端末は承認依頼部 4 5 A からの依頼に対して、ユーザ I D 「user08」を含む I D 登録情報 R 1₃の削除を却下する旨のメッセージと、ユーザ I D 「user03」を含む I D 登録情報 R 2₂の削除を承認する旨のメッセージとを応答メッセージとして削除対象ユーザ削除部 4 5 B に送信する。

[0099] 次に、削除対象ユーザ削除部 4 5 B は、管理者端末から送信された応答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応答メッセージ内のメッセージに従った処理を実行する（ステップ S 1 2）。

[0100] ここでは、削除対象ユーザ削除部 4 5 B は、ユーザ I D 「user08」を含む I D 登録情報 R 1₃の削除を却下する旨のメッセージを含む応答メッセージに関して、当該ユーザ I D 「user08」を含む削除対象ユーザ情報を削除ユーザ一時記憶装置 4 2 から削除する。

[0101] また、削除対象ユーザ削除部 4 5 B は、ユーザ I D 「user03」を含む I D 登録情報 R 2₂の削除を承認する旨のメッセージを含む応答メッセージに関して、I D 登録情報 R 2₂を削除するよう要求する削除要求メッセージを後述するユーザ削除装置 4 7 に送信する。そして、ユーザ削除装置 4 7 において、I D 登録情報 R 2₂の削除が実行される。

[0102] しかる後、修正ポリシ修正部 4 5 C は、削除対象ユーザ削除部 4 5 B で入力を受け付けた応答メッセージ内のユーザ I D 「user08」で識別されるユーザが、削除対象ユーザ情報内の当該ユーザ I D に関連付けられた削除対象 S a a S が削除対象である旨の値を示す S a a S 1 を継続して利用できるように、当該 S a a S 1 に関するポリシ P₁を修正した修正ポリシを作成し、修正ポリシー時記憶装置 4 1 に記憶された当該 S a a S 1 に関するポリシ P₁を当該

作成した修正ポリシに更新する（ステップS 13）。

- [0103] 具体的には、修正ポリシ修正部45Cは、ユーザID「user08」を含む変更後のユーザ関連情報、この場合、ユーザ属性情報 U_{B8} を参照して、図20に示すように、当該ユーザ属性情報 U_{B8} に含まれる部IDと役職IDとを用いた「部IDがdept5であり、且つ役職IDがpost1である」旨の条件を追加する。なお、ここでは、ポリシP1がユーザ属性情報内の部ID及び役職IDを用いた条件から成るため、部IDと役職IDとを用いた条件が追加される、つまり、対応するポリシを構成する条件に用いられたユーザ属性情報に対応するようにして、条件の追加は行われる。
- [0104] ポリシ更新装置46は、修正ポリシー時記憶装置41に記憶されたポリシ及び修正ポリシに従って、ポリシ記憶装置30に記憶されたポリシを更新する。
- [0105] ユーザ削除装置47は、ユーザ削除承認装置45により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に従って、クラウドサーバ装置20内のID記憶装置20Aに記憶されたID登録情報を削除する。
- [0106] 以上説明した一実施形態によれば、人手を介さずに、ポリシ更新作業及びシステム環境更新作業を実現することができる。
- [0107] 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。
- [0108] 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。
- [0109] 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。

[0110] 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。

[0111] 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。

[0112] 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。

[0113] 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。

[0114] 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]

ユーザに複数のサービスを提供可能なサーバ装置であって、前記各サービスを利用可能なユーザを識別する第1ユーザIDを前記サービス毎に少なくとも記憶する記憶手段を有したサーバ装置と、前記ユーザに関するアイデンティティ情報であり、前記第1ユーザIDに対応した第2ユーザIDを少なくとも含む複数の項目が関連付けられたユーザ属性情報を記述した少なくとも1つの条件から成り、前記ユーザ属性情報の値が前記条件を満足するときに前記サービスの利用を許可する前記各サービスの利用権限を規定した複数のポリシーを記憶するポリシー記憶装置と、前記ユーザ属性情報が変更されたときに前記記憶された各ポリシーを更新可能なポリシー更新装置と、変更後のユーザ属性情報と、変更前のユーザ属性情報と変更後のユーザ属性情報との間で異なる値を示す変更内容であって、変更前のユーザ属性情報の値と変更後のユーザ属性情報の値とを含む前記第2ユーザID毎の変更内容とを記憶するユーザ属性情報記憶装置とを含むポリシー更新システムであって、

前記ポリシー更新装置は、

前記ユーザ属性情報記憶装置に記憶された変更内容に基づいて、前記ポリシー記憶装置に記憶された各ポリシーのうち、修正が必要となる修正対象ポリシーを検出する検出手段と、

前記検出された修正対象ポリシーに記述されたユーザ属性情報の値を、前記記憶された変更内容内の変更前のユーザ属性情報の値から変更後のユーザ属性情報の値に修正した修正ポリシーを作成する作成手段と、

前記サーバ装置により提供されるサービスを利用可能なユーザの第2ユーザIDを含む変更後のユーザ属性情報をポリシー評価用ユーザ属性情報として前記ユーザ属性情報記憶装置から収集する収集手段と、

前記ポリシー記憶装置に記憶された各ポリシーのうち、前記作成された

修正ポリシを除くポリシと、前記作成された修正ポリシとに基づいて、前記収集されたポリシ評価用ユーザ属性情報を前記第2ユーザID毎に評価する評価手段と、

前記評価手段による評価結果のうち、前記ユーザ属性情報記憶装置に記憶された変更内容内の変更前のユーザ属性情報の値ではポリシを満足するが、前記収集されたポリシ評価用ユーザ属性情報の値ではポリシ及び／または修正ポリシを満足しない旨の評価結果を示す第2ユーザIDを特定する特定手段と、

前記ポリシ記憶装置に記憶された各ポリシのうち、前記作成した修正ポリシに対応するポリシを当該修正ポリシに更新する更新手段と、

前記特定された第2ユーザIDに対応する第1ユーザIDを前記サーバ装置内の前記記憶手段から削除する削除手段と

を備えたことを特徴とするポリシ更新システム。

[請求項2]

請求項1に記載のポリシ更新システムにおいて、

前記ポリシ更新装置は、

前記特定された第2ユーザIDに対応する第1ユーザIDの削除に関して、前記サーバ装置により提供される各サービスを管理する管理者が操作する管理者端末に当該第1ユーザIDの削除の承認を依頼する依頼手段と、

前記依頼手段により依頼された削除の承認に対する前記管理者端末からの応答に応じて、前記第1ユーザIDの削除を実行する削除実行手段と

を更に備えたことを特徴とするポリシ更新システム。

[請求項3]

ユーザに複数のサービスを提供可能なサーバ装置であって、前記各サービスを利用可能なユーザを識別する第1ユーザIDを前記サービス毎に少なくとも記憶する記憶手段を有したサーバ装置と、前記ユーザに関するアイデンティティ情報であり、前記第1ユーザIDに対応した第2ユーザIDを少なくとも含む複数の項目が関連付けられたユ

ーザ属性情報を記述した少なくとも1つの条件から成り、前記ユーザ属性情報の値が前記条件を満足するときに前記サービスの利用を許可する前記各サービスの利用権限を規定した複数のポリシを記憶するポリシ記憶装置と、前記ユーザ属性情報が変更される場合に、変更後のユーザ属性情報と、変更前のユーザ属性情報と変更後のユーザ属性情報との間で異なる値を示す変更内容であって、変更前のユーザ属性情報の値と変更後のユーザ属性情報の値とを含む前記第2ユーザID毎の変更内容とを記憶するユーザ属性情報記憶装置と接続可能なポリシ更新装置であって、

前記ユーザ属性情報記憶装置に記憶された変更内容に基づいて、前記ポリシ記憶装置に記憶された各ポリシのうち、修正が必要となる修正対象ポリシを検出する検出手段と、

前記検出された修正対象ポリシに記述されたユーザ属性情報の値を、前記記憶された変更内容内の変更前のユーザ属性情報の値から変更後のユーザ属性情報の値に修正した修正ポリシを作成する作成手段と、

前記サーバ装置により提供されるサービスを利用可能なユーザの第2ユーザIDを含む変更後のユーザ属性情報をポリシ評価用ユーザ属性情報として前記ユーザ属性情報記憶装置から収集する収集手段と、

前記ポリシ記憶装置に記憶された各ポリシのうち、前記作成された修正ポリシを除くポリシと、前記作成された修正ポリシとに基づいて、前記収集されたポリシ評価用ユーザ属性情報を前記第2ユーザID毎に評価する評価手段と、

前記評価手段による評価結果のうち、前記ユーザ属性情報記憶装置に記憶された変更内容内の変更前のユーザ属性情報の値ではポリシを満足するが、前記収集されたポリシ評価用ユーザ属性情報の値ではポリシ及び／または修正ポリシを満足しない旨の評価結果を示す第2ユーザIDを特定する特定手段と、

前記ポリシ記憶装置に記憶された各ポリシのうち、前記作成した修正ポリシに対応するポリシを当該修正ポリシに更新する更新手段と、
前記特定された第2ユーザIDに対応する第1ユーザIDを前記サーバ装置内の前記記憶手段から削除する削除手段と
を備えたことを特徴とするポリシ更新装置。

[請求項4]

請求項3に記載のポリシ更新装置において、
前記特定された第2ユーザIDに対応する第1ユーザIDの削除に関して、前記サーバ装置により提供される各サービスを管理する管理者が操作する管理者端末に当該第1ユーザIDの削除の承認を依頼する依頼手段と、
前記依頼手段により依頼された削除の承認に対する前記管理者端末からの応答に応じて、前記第1ユーザIDの削除を実行する削除実行手段と
を更に備えたことを特徴とするポリシ更新装置。