(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第5153591号
(P5153591)

(45)発行日　平成25年2月27日(2013.2.27)　(24)登録日　平成24年12月14日(2012.12.14)

(51)Int.Cl.　　F I
G06F 21/31 (2013.01)　　G06F 21/20 131A
H04L 9/32 (2006.01)　　H04L 9/00 673A

請求項の数 18　(全 44 頁)

(21)出願番号　特願2008-301659(P2008-301659)
(22)出願日　平成20年11月26日(2008.11.26)
(65)公開番号　特開2010-128719(P2010-128719A)
(43)公開日　平成22年6月10日(2010.6.10)
審査請求日　平成23年1月25日(2011.1.25)

(出願人による申告)国等の委託研究の成果に係る特許出願(平成１９年度　独立行政法人情報通信研究機構「次世代ネットワーク(ＮＧＮ)基板技術の研究開発」委託研究、産業技術力強化法第１９条の適用を受ける特許出願)

(73)特許権者　000005108
株式会社日立製作所
東京都千代田区丸の内一丁目６番６号
(74)代理人　110000198
特許業務法人湘洋内外特許事務所
(72)発明者　山本　暖
神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所　システム開発研究所内
(72)発明者　鍛　忠司
神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所　システム開発研究所内

最終頁に続く

(54)【発明の名称】認証仲介サーバ、プログラム、認証システム及び選択方法

(57)【特許請求の範囲】
【請求項１】
端末装置がサービス提供サーバからサービスの提供を受ける際に、前記端末装置のユーザが認証を受ける認証サーバを選択する認証仲介サーバであって、
サービス提供サーバＩＤ、および、当該サービス提供サーバＩＤが認証に要求する要求条件、を特定するサービス提供サーバ要求情報を記憶する記憶部と、制御部と、を備え、
前記制御部は、
前記サービス提供サーバより、サービス提供サーバＩＤを特定した情報取得要求を取得すると、前記情報取得要求で特定されるサービス提供サーバＩＤに対応する要求条件を前記サービス提供サーバ要求情報より取得し、取得した要求条件を満たす前記認証サーバを選択する処理と、
選択した認証サーバを特定する情報を、前記サービス提供サーバに通知する処理と、を行うこと、
を特徴とする認証仲介サーバ。
【請求項２】
請求項１に記載の認証仲介サーバであって、
前記記憶部には、
ユーザＩＤ、および、当該ユーザＩＤで特定されるユーザが認証を受けた最新の認証レベルである現在認証レベル、を特定する認証レベル情報と、
認証サーバＩＤ、当該認証サーバＩＤで特定される認証サーバが提供する認証方法、お

よび、当該認証方法の認証強度、を特定する提供認証強度情報と、
認証レベル、および、当該認証レベルで要求される認証強度、を特定する認証レベル定義情報と、が記憶されており、
前記要求条件には、前記サービス提供サーバが要求する認証レベルである要求認証レベルが含まれており、
前記情報取得要求には、ユーザＩＤが含まれており、
前記制御部は、
前記情報取得要求で特定されるユーザＩＤに対応する現在認証レベルを前記認証レベル情報から特定する処理と、
前記情報取得要求で特定されるサービス提供サーバＩＤに対応する要求認証レベルを前記要求条件から特定する処理と、
前記認証レベル情報から特定した現在認証レベルが、前記要求条件から特定した要求認証レベルに満たない場合には、前記認証レベル情報から特定した現在認証レベルに対応する認証強度と、前記要求条件から特定した要求認証レベルに対応する認証強度と、を前記認証レベル定義情報より特定し、前記要求条件から特定した要求認証レベルに対応する認証強度に対して、前記認証レベル情報から特定した現在認証レベルに対応する認証強度で不足する認証強度を特定する処理と、
前記不足する認証強度を満たす認証方法を提供する認証サーバの認証サーバＩＤを前記提供認証強度情報より特定する処理と、を行い、
前記制御部は、前記提供認証強度情報より特定された認証サーバＩＤで特定される前記認証サーバの中から、前記端末装置のユーザが認証を受ける認証サーバを選択すること、
を特徴とする認証仲介サーバ。
【請求項３】
請求項１又は２に記載の認証仲介サーバであって、
前記記憶部には、
認証サーバＩＤ、および、当該認証サーバＩＤで特定される認証サーバが保有するユーザの属性情報である保有属性情報、を特定する認証サーバ情報、が記憶されており、
前記要求条件には、前記サービス提供サーバが要求する認証で使用するユーザの属性情報である要求属性情報が含まれており、
前記制御部は、前記情報取得要求で特定されるサービス提供サーバＩＤに対応する要求属性情報を前記要求条件から特定し、前記要求条件から特定した要求属性情報を、前記保有属性情報に有する認証サーバを選択すること、
を特徴とする認証仲介サーバ。
【請求項４】
請求項１～３のいずれか一項に記載の認証仲介サーバであって、
前記要求条件には、前記サービス提供サーバが連携している認証サーバを特定する連携認証サーバＩＤ情報が含まれており、
前記制御部は、前記情報取得要求で特定されるサービス提供サーバＩＤに対応する連携認証サーバＩＤ情報を前記要求条件から特定し、前記要求条件から特定した連携認証サーバＩＤ情報で特定される認証サーバを選択すること、
を特徴とする認証仲介サーバ。
【請求項５】
請求項１～４のいずれか一項に記載の認証仲介サーバであって、
前記記憶部には、ユーザＩＤ、当該ユーザＩＤで特定されるユーザの認証を行うことのできる認証サーバ、当該認証サーバを最後に選択した日時、および、当該認証サーバを選択する条件、を特定するユーザポリシ情報が記憶されており、
前記情報取得要求には、ユーザＩＤが含まれており、
前記制御部は、
前記ユーザポリシ情報より、前記情報取得要求に含まれるユーザＩＤで特定されるユーザの認証を行うことのできる認証サーバであって、前記選択する条件を満たし、前記最後

に選択した日時が最も古い認証サーバを選択すること、
を特徴とする認証仲介サーバ。
【請求項６】
請求項５に記載の認証仲介サーバであって、
前記選択する条件には、前記ユーザの状況を特定するプレゼンス情報が含まれており、
前記制御部は、前記情報取得要求で特定されるユーザＩＤに対応するプレゼンス情報を取得する処理を行い、取得したプレゼンス情報を前記選択する条件に含む認証サーバを選択すること、
を特徴とする認証仲介サーバ。
【請求項７】
請求項５又は６に記載の認証仲介サーバであって、
前記選択する条件には、サービス提供サーバＩＤが含まれており、
前記情報取得要求には、前記端末装置からサービスの提供を要求されたサービス提供サーバＩＤが特定されており、
前記制御部は、前記情報取得要求で特定されるサービス提供サーバＩＤを前記選択する条件に含む認証サーバを選択すること、
を特徴とする認証仲介サーバ。
【請求項８】
請求項５～７のいずれか一項に記載の認証仲介サーバであって、
前記ユーザポリシ情報には、前記認証サーバを選択する優先度を特定する情報が含まれており、
前記制御部は、前記優先度の高いものから前記認証サーバを選択すること、
を特徴とする認証仲介サーバ。
【請求項９】
コンピュータを、端末装置がサービス提供サーバからサービスの提供を受ける際に、前記端末装置のユーザが認証を受ける認証サーバを選択する認証仲介サーバとして機能させるプログラムであって、
前記コンピュータを、サービス提供サーバＩＤ、および、当該サービス提供サーバＩＤが認証に要求する要求条件、を特定するサービス提供サーバ要求情報を記憶する記憶手段、制御手段、として機能させ、
前記制御手段に、
前記サービス提供サーバより、サービス提供サーバＩＤを特定した情報取得要求を取得すると、前記情報取得要求で特定されるサービス提供サーバＩＤに対応する要求条件を前記サービス提供サーバ要求情報より取得し、取得した要求条件を満たす前記認証サーバを選択する処理と、
選択した認証サーバを特定する情報を、前記サービス提供サーバに通知する処理と、を行わせること、
を特徴とするプログラム。
【請求項１０】
請求項９に記載のプログラムであって、
前記記憶手段には、
ユーザＩＤ、および、当該ユーザＩＤで特定されるユーザが認証を受けた最新の認証レベルである現在認証レベル、を特定する認証レベル情報と、
認証サーバＩＤ、当該認証サーバＩＤで特定される認証サーバが提供する認証方法、および、当該認証方法の認証強度、を特定する提供認証強度情報と、
認証レベル、および、当該認証レベルで要求される認証強度、を特定する認証レベル定義情報と、が記憶されており、
前記要求条件には、前記サービス提供サーバが要求する認証レベルである要求認証レベルが含まれており、
前記情報取得要求には、ユーザＩＤが含まれており、

前記制御手段に、
前記情報取得要求で特定されるユーザＩＤに対応する現在認証レベルを前記認証レベル情報から特定する処理と、
前記情報取得要求で特定されるサービス提供サーバＩＤに対応する要求認証レベルを前記要求条件から特定する処理と、
前記認証レベル情報から特定した現在認証レベルが、前記要求条件から特定した要求認証レベルに満たない場合には、前記認証レベル情報から特定した現在認証レベルに対応する認証強度と、前記要求条件から特定した要求認証レベルに対応する認証強度と、を前記認証レベル定義情報より特定し、前記要求条件から特定した要求認証レベルに対応する認証強度に対して、前記認証レベル情報から特定した現在認証レベルに対応する認証強度で不足する認証強度を特定する処理と、
前記不足する認証強度を満たす認証方法を提供する認証サーバの認証サーバＩＤを前記提供認証強度情報より特定する処理と、を行わせ、
前記制御手段に、前記提供認証強度情報より特定された認証サーバＩＤで特定される前記認証サーバの中から、前記端末装置のユーザが認証を受ける認証サーバを選択させること、
を特徴とするプログラム。
【請求項１１】
請求項９又は１０に記載のプログラムであって、
前記記憶手段には、
認証サーバＩＤ、および、当該認証サーバＩＤで特定される認証サーバが保有するユーザの属性情報である保有属性情報、を特定する認証サーバ情報、が記憶されており、
前記要求条件には、前記サービス提供サーバが要求する認証で使用するユーザの属性情報である要求属性情報が含まれており、
前記制御手段に、前記情報取得要求で特定されるサービス提供サーバＩＤに対応する要求属性情報を前記要求条件から特定し、前記要求条件から特定した要求属性情報を、前記保有属性情報に有する認証サーバを選択させること、
を特徴とするプログラム。
【請求項１２】
請求項９～１１のいずれか一項に記載のプログラムであって、
前記要求条件には、前記サービス提供サーバが連携している認証サーバを特定する連携認証サーバＩＤ情報が含まれており、
前記制御手段に、前記情報取得要求で特定されるサービス提供サーバＩＤに対応する連携認証サーバＩＤ情報を前記要求条件から特定し、前記要求条件から特定した連携認証サーバＩＤ情報で特定される認証サーバを選択させること、
を特徴とするプログラム。
【請求項１３】
請求項９～１２のいずれか一項に記載のプログラムであって、
前記記憶手段には、ユーザＩＤ、当該ユーザＩＤで特定されるユーザの認証を行うことのできる認証サーバ、当該認証サーバを最後に選択した日時、および、当該認証サーバを選択する条件、を特定するユーザポリシ情報が記憶されており、
前記情報取得要求には、ユーザＩＤが含まれており、
前記制御手段に、
前記ユーザポリシ情報より、前記情報取得要求に含まれるユーザＩＤで特定されるユーザの認証を行うことのできる認証サーバであって、前記選択する条件を満たし、前記最後に選択した日時が最も古い認証サーバを選択させること、
を特徴とするプログラム。
【請求項１４】
請求項１３に記載のプログラムであって、
前記選択する条件には、前記ユーザの状況を特定するプレゼンス情報が含まれており、

前記制御手段に、前記情報取得要求で特定されるユーザＩＤに対応するプレゼンス情報を取得する処理を行い、取得したプレゼンス情報を前記選択する条件に含む認証サーバを選択させること、
を特徴とするプログラム。
【請求項１５】
請求項１３又は１４に記載のプログラムであって、
前記選択する条件には、サービス提供サーバＩＤが含まれており、
前記情報取得要求には、前記端末装置からサービスの提供を要求されたサービス提供サーバＩＤが特定されており、
前記制御手段に、前記情報取得要求で特定されるサービス提供サーバＩＤを前記選択する条件に含む認証サーバを選択させること、
を特徴とするプログラム。
【請求項１６】
請求項１３～１５のいずれか一項に記載のプログラムであって、
前記ユーザポリシ情報には、前記認証サーバを選択する優先度を特定する情報が含まれており、
前記制御手段に、前記優先度の高いものから前記認証サーバを選択させること、
を特徴とするプログラム。
【請求項１７】
端末装置と、当該端末装置にサービスを提供するサービス提供サーバと、当該端末装置が当該サービス提供サーバからサービスの提供を受ける際に当該端末装置のユーザが認証を受ける認証サーバと、当該認証サーバの選択を行う認証仲介サーバと、を備える認証システムであって、
前記認証仲介サーバは、
サービス提供サーバＩＤ、および、当該サービス提供サーバＩＤが認証に要求する要求条件、を特定するサービス提供サーバ要求情報を記憶する記憶部と、制御部と、を備え、
前記認証仲介サーバの制御部は、
前記サービス提供サーバより、サービス提供サーバＩＤを特定した情報取得要求を取得すると、前記情報取得要求で特定されるサービス提供サーバＩＤに対応する要求条件を前記サービス提供サーバ要求情報より取得し、取得した要求条件を満たす前記認証サーバを選択する処理と、
選択した認証サーバを特定する情報を、前記サービス提供サーバに通知する処理と、を行うこと、
を特徴とする認証システム。
【請求項１８】
サービス提供サーバＩＤ、および、当該サービス提供サーバＩＤが認証に要求する要求条件、を特定するサービス提供サーバ要求情報を記憶する記憶部と、制御部と、を備える認証仲介サーバにおいて、端末装置がサービス提供サーバからサービスの提供を受ける際に、前記端末装置のユーザが認証を受ける認証サーバを選択する選択方法であって、
前記制御部が、前記サービス提供サーバより、サービス提供サーバＩＤを特定した情報取得要求を取得すると、前記情報取得要求で特定されるサービス提供サーバＩＤに対応する要求条件を前記サービス提供サーバ要求情報より取得し、取得した要求条件を満たす前記認証サーバを選択する処理を行う過程と、
前記制御部が、選択した認証サーバを特定する情報を、前記サービス提供サーバに通知する処理を行う過程と、を有すること、
を特徴とする選択方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、端末装置がサービス提供サーバからサービスの提供を受ける際に、端末装置

のユーザが認証を受ける認証サーバを選択する技術に関する。

【背景技術】

【０００２】

インターネットの普及により、動画又は音声の配信、Ｗｅｂアプリケーション又はＷｅｂサイトの公開等、多種多様なサービスがネットワークを介してユーザに提供されており、これらのサービスの提供を受ける際に、サービスの提供者がサービスを利用するユーザの認証を行う場合がある。

【０００３】

そして、各々のサービス提供者が独自にユーザ認証方式を実装した場合、ユーザは各サービスを享受する度に、各々のサービス提供者が任意に選択した認証方式による認証を要求されることとなり、ユーザの利便性が損なわれ、また、ユーザは各サービスの利用に先立って、各々のサービス提供者等に自らの属性情報を登録しなければならず、属性情報が漏洩する可能性を高め、ユーザのプライバシ侵害につながるおそれもある。

【０００４】

このような問題を解決するものとして、一度の認証操作で複数のサービス享受を可能とする、シングルサインオンと呼ばれる技術が知られている。例えば、非特許文献１及び非特許文献２に記載されたＳＡＭＬ（Security Assertion Markup Language）や、非特許文献３に記載されたＯｐｅｎＩＤ Ａｕｔｈｅｎｔｉｃａｔｉｏｎでは、サービス提供者（非特許文献１および非特許文献２ではＳｅｒｖｉｃｅ Ｐｒｏｖｉｄｅｒと呼ばれ、また、非特許文献３ではＲｅｌｙｉｎｇ Ｐａｒｔｙとして参照される）が認証サーバ（非特許文献１および非特許文献２ではＩｄｅｎｔｉｔｙ Ｐｒｏｖｉｄｅｒと呼ばれ、また、非特許文献３ではＯｐｅｎＩＤ Ｐｒｏｖｉｄｅｒとして参照される）へユーザの認証を委託することで、ユーザがサービスを利用する度に認証操作を行わなければならないこと、および、ユーザの属性情報を各々のサービス提供者が保持すること、を防止している。

【０００５】

【非特許文献１】ＯＡＳＩＳ、Ａｓｓｅｒｔｉｏｎｓ ａｎｄ Ｐｒｏｔｏｃｏｌｓ ｆｏｒ ｔｈｅ ＯＡＳＩＳ Ｓｅｃｕｒｉｔｙ Ａｓｓｅｒｔｉｏｎ Ｍａｒｋｕｐ Ｌａｎｇｕａｇｅ（ＳＡＭＬ）Ｖ２．０、［平成２０年８月２０日検索］、インターネット＜URL: http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf＞

【非特許文献２】ＯＡＳＩＳ、Ｐｒｏｆｉｌｅｓ ｆｏｒ ｔｈｅ ＯＡＳＩＳ Ｓｅｃｕｒｉｔｙ Ａｓｓｅｒｔｉｏｎ Ｍａｒｋｕｐ Ｌａｎｇｕａｇｅ（ＳＡＭＬ）Ｖ２．０、［平成２０年８月２０日検索］、インターネット＜URL: http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf＞

【非特許文献３】ＯｐｅｎＩＤ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ ２．０ － Ｆｉｎａｌ、［平成２０年８月２０日検索］、インターネット＜URL: http://openid.net/specs/openid-authentication-2_0.html＞

【発明の開示】

【発明が解決しようとする課題】

【０００６】

上述した従来技術においては、ユーザが複数の認証方式を利用する場合に、以下のような問題が存在する。

【０００７】

非特許文献１および非特許文献２に記載されるＳＡＭＬにおいては、基本的には、サービス提供者が信頼関係を結んでいる認証サーバとの間でしか、認証の委託が実行されない。信頼関係を結んでいる認証サーバが複数存在する場合には、Ｉｄｅｎｔｉｔｙ Ｐｒｏｖｉｄｅｒ Ｄｉｓｃｏｖｅｒｙ Ｐｒｏｆｉｌｅとして記載されている手段を用いて、ユーザが認証済みの認証サーバを動的に選択することは可能だが、ユーザの状況（例えばプレゼンス情報）やポリシを反映することができない、という問題がある。

【０００８】

また、非特許文献３に記載されるＯｐｅｎＩＤ Ａｕｔｈｅｎｔｉｃａｔｉｏｎにおい

ては、ユーザがサービス提供サーバに対して、ＯｐｅｎＩＤと呼ばれるＵＲＬを提示することで、認証に利用される認証サーバを指定することが可能であるが、複数の認証サーバを使い分ける場合には、認証サーバの数だけＯｐｅｎＩＤを用意する必要があり、ユーザの利便性を低下させる、という問題がある。

【０００９】

そこで、本発明は、ユーザの状況、ユーザが利用するサービスの種類及びユーザの利便性を考慮して、認証サーバを動的に変更できるようにすることを目的とする。

【課題を解決するための手段】

【００１０】

以上の課題を解決するため、本発明は、ユーザが予め設定した選択条件を満たす認証サーバを選択する。

【００１１】

例えば、本発明は、端末装置がサービス提供サーバからサービスの提供を受ける際に、前記端末装置のユーザが認証を受ける認証サーバを選択する認証仲介サーバであって、サービス提供サーバＩＤ、および、当該サービス提供サーバＩＤが認証に要求する要求条件、を特定するサービス提供サーバ要求情報を記憶する記憶部と、制御部と、を備え、前記制御部は、前記サービス提供サーバより、サービス提供サーバＩＤを特定した情報取得要求を取得すると、前記情報取得要求で特定されるサービス提供サーバＩＤに対応する要求条件を前記サービス提供サーバ要求情報より取得し、取得した要求条件を満たす前記認証サーバを選択する処理と、選択した認証サーバを特定する情報を、前記サービス提供サーバに通知する処理と、を行うこと、を特徴とする。

【発明の効果】

【００１２】

以上のように、本発明によれば、ユーザの状況、ユーザが利用するサービスの種類及びユーザの利便性を考慮して、認証サーバを動的に変更することができる。

【発明を実施するための最良の形態】

【００１３】

以下の実施形態において使用しているドメイン名、ＵＲＬ、ＵＲＩ、ＩＰアドレス等の情報は、説明のために用いる架空のものであり、実在のものとは無関係である。

【００１４】

図１は、本発明の一実施形態である認証システム１０の概略図である。

【００１５】

図示するように、認証システム１０は、端末装置１と、複数のサービス提供サーバ２Ａ、２Ｂ、・・・（以下、各々を区別しない場合には、サービス提供サーバ２という）と、複数の認証サーバ３Ａ、３Ｂ、・・・（以下、各々を区別しない場合には、認証サーバ３という）と、認証仲介サーバ４と、プレゼンスサーバ５と、を備える。そして、これらは、ネットワーク６を介して相互に情報を送受信することができるようにされている。

【００１６】

図２は、端末装置１の一例を示す概略図である。図示するように、端末装置１は、記憶部１０１と、制御部１０５と、入力部１１５と、出力部１１６と、送受信部１１７と、音声入出力部１１８と、を備える。

【００１７】

記憶部１０１は、セッション情報記憶領域１０２と、プレゼンス情報記憶領域１０３と、を備える。

【００１８】

セッション情報記憶領域１０２には、ネットワーク６を介して他の装置との間で確立したセッションを特定するセッション情報が記憶される。ここで、本実施形態では、セッションは、装置間で行われる一連のデータ通信シーケンスをさすものとする。

【００１９】

例えば、本実施形態においては、図３（セッション情報テーブル１０２ａの概略図）に

示すようなセッション情報テーブル１０２ａがセッション情報記憶領域１０２に記憶される。

【００２０】

セッション情報記憶テーブル１０２ａは、接続先ＩＤ欄１０２ｂと、セッションＩＤ欄１０２ｃと、を有する。

【００２１】

接続先ＩＤ欄１０２ｂには、接続先の装置を特定する情報が格納される。ここでは、接続先の装置を特定する情報として、各々の装置（サービス提供サーバ２又は認証サーバ３）を一意に識別するための識別情報であるサービス提供サーバＩＤ又は認証サーバＩＤが格納される。例えば、接続先の装置がＷｅｂサーバである場合、接続先ＩＤ欄の値として、ｈｔｔｐ：／／ｗｗｗ．ｈｉｔａｃｈｉ．ｃｏｍ／のようなＵＲＬを利用することができる。

【００２２】

セッションＩＤ欄１０２ｃには、接続先ＩＤ欄１０２ｂで特定される装置との間のセッションを特定する情報が格納される。ここでは、セッションを特定する情報として、各々のセッションに一意となるように割り振られた識別情報であるセッションＩＤが格納される。例えば、接続先の装置がＷｅｂサーバである場合、セッションＩＤ欄の値としては、ＷｅｂサーバからのＨＴＴＰレスポンス内でＳｅｔ－Ｃｏｏｋｉｅヘッダの値として渡された文字列を格納することができる。

【００２３】

図２に戻り、プレゼンス情報記憶領域１０３には、端末装置１を利用するユーザのプレゼンス情報が記憶される。

【００２４】

例えば、本実施形態においては、プレゼンス情報として、端末装置１を利用するユーザが「自宅」にいるのか「職場」にいるのか、を特定する情報（予め入力部１１５を介してユーザが入力しておけばよい）、および、端末装置１を利用するユーザが後述する音声入出力部１１８を介して「通話中」か否かを特定する情報（後述する音声通信部１１２で通話中か否かを特定すればよい）、とが記憶されているが、このような態様に限定されるわけではない。

【００２５】

制御部１０５は、サービス利用部１０６と、サービス要求生成部１０７と、サービス通信部１０８と、認証処理部１０９と、セッション管理部１１０と、プレゼンス情報処理部１１１と、音声通信部１１２と、ユーザポリシ処理部１１３と、を有する。

【００２６】

サービス利用部１０６は、入力部１１５及び出力部１１６を介してユーザに対してサービスを利用するための入出力インタフェースを提供し、必要な情報の入力を受け付ける処理を行う。

【００２７】

サービス要求生成部１０７は、入力部１１５及び出力部１１６を介して、サービス利用部１０６が入力を受け付けた情報に基づいて、サービス提供サーバ２に対して、サービスを要求するためのメッセージ（サービス要求メッセージ）を生成する処理を行う。

【００２８】

サービス通信部１０８は、送受信部１１７及びネットワーク６を介した情報の送受信処理を制御する。例えば、サービス通信部１０８としては、ＷｅｂサイトやＷｅｂアプリケーションを利用するためのＨＴＴＰ通信を可能とするプロトコルスタックなどが考えられる。

【００２９】

また、サービス通信部１０８は、認証仲介サーバ４及びサービス提供サーバ２との間でやりとりするメッセージの転送処理を行う。

【００３０】

認証処理部１０９は、認証サーバ３が実行する認証に際し、ユーザへの入出力要求及び認証に必要な情報の計算処理を行う。例えば、認証サーバ３が実行する認証方式がＴＬＳクライアント認証であった場合、認証処理部１０９は、必要であれば出力部１１６を介して、ユーザへＰＩＮ（Personal Identification Number）の入力を要求し、スマートカード等の可搬性の記憶媒体又は記憶部１０１に記憶されたユーザの秘密鍵を取得し、認証サーバ３から送信されてきた情報と合わせて、本人性を証明するための情報を計算し、送受信部１１７を介して計算した情報を認証サーバ３へ送信する処理を行う。

【００３１】

セッション管理部１１０は、端末装置１が他の装置との間で確立したセッションを管理する処理を行う。例えば、端末装置１がサービス提供サーバ２又は認証サーバ３との間でセッションを確立すると、セッション情報テーブル１０２ａに新たなレコードを生成し、接続先の装置のＩＤとセッションＩＤとを生成した新たなレコードに格納し、確立されたセッションが終了する（切断される）と、当該セッションに対応するレコードを削除する。

【００３２】

プレゼンス情報処理部１１１は、端末装置１のユーザのプレゼンス情報を管理する処理を行う。例えば、端末装置１のユーザより入力部１１５を介して、ユーザが「自宅」にいるのか、「職場」にいるのか、を特定する情報の入力を受け付け、入力された「自宅」又は「職場」を特定する情報を記憶部１０１のプレゼンス情報記憶領域１０３に記憶する処理を行う。

【００３３】

また、プレゼンス情報処理部１１１は、後述する音声通信部１１２が音声通信を実行している場合には、端末装置１のユーザが音声通話を行っていることを特定する情報（「通話中」であることを特定する情報）を記憶部１０１のプレゼンス情報記憶領域１０３に記憶する。

【００３４】

さらに、プレゼンス情報処理部１１１は、予め定められた時、または、プレゼンスサーバ２からの要求があったときに、送受信部１１７及びネットワーク６を介して、プレゼンス情報記憶領域１０３に記憶されているプレゼンス情報を送信する処理を制御する。

【００３５】

音声通信部１１２は、ＳＩＰ（Session Initiation Protocol）等に従った呼制御を行うとともに、ＲＴＰ（Real Time Protocol）等に従った音声通信を制御する。

【００３６】

ユーザポリシ処理部１１３は、端末装置１のユーザより、入力部１１５を介して、ユーザＩＤ、使用する認証サーバ３の認証サーバＩＤ、当該認証サーバ３の優先度、当該認証サーバ３を使用する際の使用条件（プレゼンス情報に対する条件）、当該認証サーバ３を使用するサービス提供サーバ２を特定する情報（サービス提供サーバＩＤ）、を特定するポリシ情報の入力を受け付ける。

【００３７】

そして、ユーザポリシ処理部１１３は、入力を受け付けたポリシ情報を、送受信部１１７及びネットワーク６を介して、認証仲介サーバ４に送信する処理を行う。

【００３８】

入力部１１５は、情報の入力を受け付ける。

【００３９】

出力部１１６は、情報を出力する。

【００４０】

送受信部１１７は、ネットワーク６を介した情報の送受信を行う。

【００４１】

音声入出力部１１８は、音声の入力及び出力を行う。

【００４２】

以上に記載した端末装置１は、例えば、図４（コンピュータ９の概略図）に示すような、ＣＰＵ（Central Processing Unit）９０１と、メモリ９０２と、ＨＤＤ（Hard Disk Drive）等の外部記憶装置９０３と、ＣＤ（Compact Disk）やＤＶＤ（Digital Versatile Disk）などの可搬性を有する記憶媒体９０４に対して情報を読み書きする読書装置９０５と、キーボードやマウス等の入力装置９０６と、ディスプレイなどの出力装置９０７と、通信ネットワークに接続するためのＮＩＣ（Network Interface Card）などの送受信装置９０８と、を備えた一般的なコンピュータ９にマイク及びスピーカを備えるハンドセット（図示せず）を利用可能に接続することで実現できる。

【００４３】

例えば、記憶部１０１は、ＣＰＵ９０１がメモリ９０２又は外部記憶装置９０３を利用することにより実現可能であり、制御部１０５は、外部記憶装置９０３に記憶されている所定のプログラムをメモリ９０２にロードしてＣＰＵ９０１で実行することで実現可能であり、入力部１１５は、ＣＰＵ９０１が入力装置９０６を利用することで実現可能であり、出力部１１６は、ＣＰＵ９０１が出力装置９０７を利用することで実現可能であり、送受信部１１７は、ＣＰＵ９０１が送受信装置９０８を利用することで実現可能であり、音声入出力部１１８は、ＣＰＵ９０１がハンドセット（図示せず）を利用することで実現可能である。

【００４４】

この所定のプログラムは、読書装置９０５を介して記憶媒体９０４から、あるいは、送受信装置９０８を介してネットワークから、外部記憶装置９０３にダウンロードされ、それから、メモリ９０２上にロードされてＣＰＵ９０１により実行されるようにしてもよい。また、読書装置９０５を介して記憶媒体９０４から、あるいは、送受信装置９０８を介してネットワークから、メモリ９０２上に直接ロードされ、ＣＰＵ９０１により実行されるようにしてもよい。

【００４５】

図５は、サービス提供サーバ２の一例を示す概略図である。図示するように、サービス提供サーバ２は、記憶部２０１と、制御部２０４と、入力部２１１と、出力部２１２と、送受信部２１３と、を備える。

【００４６】

記憶部２０１は、セッション情報記憶領域２０２を備える。

【００４７】

セッション情報記憶領域２０２には、サービス提供サーバ２が、ネットワーク６を介して他の装置との間で確立したセッションを特定するセッション情報が記憶される。例えば、本実施形態においては、図６（セッション情報テーブル２０２ａの概略図）に示すようなセッション情報テーブル２０２ａがセッション情報記憶領域２０２に記憶される。

【００４８】

セッション情報記憶テーブル２０２ａは、接続先ＩＤ欄２０２ｂと、セッションＩＤ欄２０２ｃと、を有する。

【００４９】

接続先ＩＤ欄２０２ｂには、接続先の装置を特定する情報が格納される。ここでは、接続先の装置を特定する情報として、各々の装置（端末装置１）に一意となるように割り振られた識別情報が格納される。例えば、接続先の装置が端末装置１である場合には、端末装置１を使用するユーザのユーザＩＤを利用することができる。

【００５０】

セッションＩＤ欄２０２ｃには、接続先ＩＤ欄２０２ｂで特定される装置との間のセッションを特定する情報が格納される。ここでは、セッションを特定する情報として、各々のセッションを一意錦別するための識別情報であるセッションＩＤが格納される。例えば、接続先の装置がＷｅｂクライアントである場合、セッションＩＤ欄の値としては、当該ＷｅｂクライアントからのＨＴＴＰリクエスト内でＣｏｏｋｉｅヘッダの値として渡される文字列を格納することができる。

【００５１】
図５に戻り、制御部２０４は、サービス提供部２０５と、セッション管理部２０６と、認証サーバ情報取得部２０７と、認証要求処理部２０８と、サービス通信部２０９と、を備える。
【００５２】
サービス提供部２０５は、端末装置１から要求されたサービスを、端末装置１へ提供する処理を行う。
【００５３】
セッション管理部２０６は、サービス提供サーバ２が他の装置との間で確立したセッションを管理する処理を行う。例えば、サービス提供サーバ２が端末装置１との間でセッションを確立すると、セッション情報テーブル２０２ａに新たなレコードを生成し、接続先の装置のＩＤとセッションＩＤとを生成した新たなレコードに格納し、確立されたセッションが終了すると、当該セッションに対応するレコードを削除する。
【００５４】
認証サーバ情報取得部２０７は、端末装置１から特定のサービスを要求された際に、当該端末装置１のユーザに対する認証を実行する認証サーバ３を特定する認証サーバ情報を、送受信部２１３及びネットワーク６を介して、認証仲介サーバ４から直接、もしくは端末装置１を介して間接的に、取得する処理を行う。
【００５５】
例えば、認証仲介サーバ４が、非特許文献３に記載されるＯｐｅｎＩＤ Ａｕｔｈｅｎｔｉｃａｔｉｏｎのように、認証サーバ情報をＸＲＤＳ文書で通知する場合、サービス提供サーバ２は、当該認証仲介サーバ４に対して、ＨＴＴＰまたはＨＴＴＰＳを用いて直接、認証サーバ情報を要求して、取得することができる。
【００５６】
また、サービス提供サーバ２は、非特許文献２に記載されているＩｄｅｎｔｉｔｙ Ｐｒｏｖｉｄｅｒ Ｄｉｓｃｏｖｅｒｙ Ｐｒｏｆｉｌｅに従い、ＨＴＴＰリダイレクトを利用して、端末装置１を介して間接的に認証仲介サーバ４に認証サーバ情報を要求して、取得するようにしてもよい。
【００５７】
認証要求処理部２０８は、認証仲介サーバ４から認証サーバ情報を受信した際に、送受信部２１３及びネットワーク６を介して、当該認証サーバ情報によって指定される認証サーバ３に対し、端末装置１を介して間接的に、ユーザの認証を要求する認証要求メッセージを送信する処理を行う。例えば、端末装置１と、サービス提供サーバ２と、認証サーバ３とが、ＨＴＴＰまたはＨＴＴＰＳを用いた通信が可能である場合には、ＨＴＴＰリダイレクトを利用して、端末装置１を介して間接的に認証要求メッセージを送信することができる。
【００５８】
サービス通信部２０９は、送受信部２１３及びネットワーク６を介して、端末装置１に対してサービスを提供するのに必要な情報を送受信する処理を行う。例えば、サービス通信部２０９としては、ＷｅｂサイトやＷｅｂアプリケーションを利用するためのＨＴＴＰ通信を可能とするプロトコルスタック等として構成することができる。
【００５９】
入力部２１１は、情報の入力を受け付ける。
【００６０】
出力部２１２は、情報を出力する。
【００６１】
送受信部２１３は、ネットワーク６を介した情報の送受信を行う。
【００６２】
以上に記載したサービス提供サーバ２は、例えば、図４に示すようなコンピュータ９により実現できる。

【００６３】
例えば、記憶部２０１は、ＣＰＵ９０１がメモリ９０２又は外部記憶装置９０３を利用することにより実現可能であり、制御部２０４は、外部記憶装置９０３に記憶されている所定のプログラムをメモリ９０２にロードしてＣＰＵ９０１で実行することで実現可能であり、入力部２１１は、ＣＰＵ９０１が入力装置９０６を利用することで実現可能であり、出力部２１２は、ＣＰＵ９０１が出力装置９０７を利用することで実現可能であり、送受信部２１３は、ＣＰＵ９０１が送受信装置９０８を利用することで実現可能である。
【００６４】
この所定のプログラムは、読書装置９０５を介して記憶媒体９０４から、あるいは、送受信装置９０８を介してネットワークから、外部記憶装置９０３にダウンロードされ、それから、メモリ９０２上にロードされてＣＰＵ９０１により実行されるようにしてもよい。また、読書装置９０５を介して記憶媒体９０４から、あるいは、送受信装置９０８を介してネットワークから、メモリ９０２上に直接ロードされ、ＣＰＵ９０１により実行される
ようにしてもよい。
【００６５】
図７は、認証サーバ３の一例を示す概略図である。図示するように、認証サーバ３は、記憶部３０１と、制御部３０５と、入力部３１２と、出力部３１３と、送受信部３１４と、を備える。
【００６６】
記憶部３０１は、セッション情報記憶領域３０２と、ユーザ属性情報記憶領域３０３と、を備える。
【００６７】
セッション情報記憶領域３０２には、認証サーバ３が、ネットワーク６を介して他の装置との間で確立したセッションを特定するセッション情報が記憶される。例えば、本実施形態においては、図８（セッション情報テーブル３０２ａの概略図）に示すようなセッション情報テーブル３０２ａがセッション情報記憶領域３０２に記憶される。
【００６８】
セッション情報記憶テーブル３０２ａは、接続先ＩＤ欄３０２ｂと、セッションＩＤ欄３０２ｃと、を有する。
【００６９】
接続先ＩＤ欄３０２ｂには、接続先の装置を特定する情報が格納される。ここでは、接続先の装置を特定する情報として、各々の装置（端末装置１）を一意に識別するための識別情報が格納される。例えば、接続先の装置が端末装置１である場合には、端末装置１を使用するユーザのユーザＩＤを利用することができる。
【００７０】
セッションＩＤ欄３０２ｃには、接続先ＩＤ欄３０２ｂで特定される装置との間のセッションを特定する情報が格納される。ここでは、セッションを特定する情報として、各々のセッションに一意となるように割り振られた識別情報であるセッションＩＤが格納される。例えば、接続先の装置がＷｅｂクライアントである場合、セッションＩＤ欄の値としては、当該ＷｅｂクライアントからのＨＴＴＰリクエスト内でＣｏｏｋｉｅヘッダの値として渡される文字列を格納することができる。
【００７１】
図７に戻り、ユーザ属性情報記憶領域３０３には、認証サーバ３が認証するユーザの属性を特定するユーザ属性情報が記憶される。例えば、本実施形態においては、図９（ユーザ属性情報テーブル３０３ａの概略図）に示すようなユーザ属性情報テーブル３０３ａがユーザ属性情報記憶領域３０３に記憶される。
【００７２】
ユーザ属性情報テーブル３０３ａは、ユーザＩＤ欄３０３ｂと、属性欄３０３ｃと、を有する。

【００７３】
ユーザＩＤ欄３０３ｂには、端末装置１のユーザを特定する情報が格納される。ここでは、ユーザを特定する情報として、各々のユーザを一意に識別するための識別情報であるユーザＩＤが格納される。
【００７４】
属性欄３０３ｃには、ユーザＩＤ欄３０３ｂで特定されるユーザの属性を特定する情報が格納される。ここでは、ユーザの属性を特定する情報として、例えば、ユーザの氏名、ユーザのメールアドレス、ユーザの住所、ユーザの電子証明書等を特定する情報のうち、認証サーバ３で行う認証方式に対応した情報が格納される。
【００７５】
このユーザ属性情報は、サービス提供サーバ２からの要求を受け、ユーザの設定したポリシの範囲内でサービス提供サーバ２へ送信される。また、ユーザ属性記憶領域３０３には、認証に必要であれば、ユーザのパスワードを格納することもできる。
【００７６】
制御部３０５は、認証要求処理部３０６と、認証実行部３０７と、認証結果生成部３０８と、セッション管理部３０９と、ユーザ属性管理部３１０と、を備える。
【００７７】
認証要求処理部３０６は、サービス提供サーバ２から直接的に、または、端末装置１を介して間接的に、送信された認証要求メッセージを受信し、受信した認証要求メッセージに含まれるパラメータ（セッションＩＤ、ユーザＩＤ等）を取得する処理を行う。例えば、端末装置１と、サービス提供サーバ２と、認証サーバ３とが、ＨＴＴＰまたはＨＴＴＰＳを用いた通信が可能である場合には、認証サーバ３は、ＨＴＴＰリダイレクトを利用して、サービス提供サーバ２から端末装置１を介して間接的に送信される認証要求メッセージを受信することができる。
【００７８】
認証実行部３０７は、ユーザの認証に必要な処理を実行する。本実施形態においては、認証実行部３０７は、送受信部３１４及びネットワーク６を介して、端末装置１へ本人性を証明するための情報を要求する。例えば、認証サーバ３の実行する認証方式がＴＬＳクライアント認証であった場合、認証実行部３０７は、端末装置１へ乱数列を送信し、当該端末装置１から返却された情報が、端末装置１の保有する秘密鍵で計算されたものであることを、ユーザ属性記憶領域３０３に格納された端末装置１の電子証明書を用いて検証することで、ユーザの認証を実行することができる。
【００７９】
認証結果生成部３０８は、認証実行部３０７によって実行されたユーザ認証の結果を特定する認証結果情報を生成する。当該認証結果情報としては、例えば、非特許文献１に記載されるＳＡＭＬ　Ａｓｓｅｒｔｉｏｎと呼ばれるＸＭＬ文書を利用することが可能である。
【００８０】
セッション管理部３０９は、認証サーバ３が他の装置との間で確立したセッションを管理する処理を行う。例えば、認証サーバ３が端末装置１との間でセッションを確立すると、セッション情報テーブル３０２ａに新たなレコードを生成し、接続先の装置のＩＤとセッションＩＤとを生成した新たなレコードに格納し、確立されたセッションが終了すると、当該セッションに対応するレコードを削除する。
【００８１】
ユーザ属性管理部３１０は、端末装置１から要求を受け、ユーザ属性記憶領域３０３に記憶されているユーザ属性情報を作成、更新又は削除する処理を行う。
【００８２】
また、ユーザ属性管理部３１０は、送受信部３１４及びネットワーク６を介して、サービス提供サーバ２から属性取得要求メッセージを受信すると、ユーザの設定したポリシの範囲内で、要求されたユーザ属性情報をサービス提供サーバ２へ送信する処理を行う。

【００８３】
入力部３１２は、情報の入力を受け付ける。
【００８４】
出力部３１３は、情報を出力する。
【００８５】
送受信部３１４は、ネットワーク６を介した情報の送受信を行う。
【００８６】
以上に記載した認証サーバ３は、例えば、図４に示すようなコンピュータ９により実現できる。
【００８７】
例えば、記憶部３０１は、ＣＰＵ９０１がメモリ９０２又は外部記憶装置９０３を利用することにより実現可能であり、制御部３０５は、外部記憶装置９０３に記憶されている所定のプログラムをメモリ９０２にロードしてＣＰＵ９０１で実行することで実現可能であり、入力部３１２は、ＣＰＵ９０１が入力装置９０６を利用することで実現可能であり、出力部３１３は、ＣＰＵ９０１が出力装置９０７を利用することで実現可能であり、送受信部３１４は、ＣＰＵ９０１が送受信装置９０８を利用することで実現可能である。
【００８８】
この所定のプログラムは、読書装置９０５を介して記憶媒体９０４から、あるいは、送受信装置９０８を介してネットワークから、外部記憶装置９０３にダウンロードされ、それから、メモリ９０２上にロードされてＣＰＵ９０１により実行されるようにしてもよい。また、読書装置９０５を介して記憶媒体９０４から、あるいは、送受信装置９０８を介してネットワークから、メモリ９０２上に直接ロードされ、ＣＰＵ９０１により実行されるようにしてもよい。
【００８９】
図１０は、認証仲介サーバ４の構成の一例を示す概略図である。
【００９０】
図示するように、認証仲介サーバ４は、記憶部４０１と、制御部４１１と、入力部４１８と、出力部４１９と、送受信部４２０と、を備える。
【００９１】
記憶部４０１は、ユーザポリシ情報記憶領域４０２と、認証サーバ情報記憶領域４０３と、サービス提供サーバ要求情報記憶領域４０４と、認証レベル情報記憶領域４０５と、提供認証強度情報記憶領域４０６と、認証レベル定義情報記憶領域４０７と、ＩＤ情報記憶領域４０８と、属性情報記憶領域４０９と、を備える。
【００９２】
ユーザポリシ情報記憶領域４０２には、ユーザ毎に、認証サーバ３を選択する選択指針を特定するユーザポリシ情報が格納される。例えば、本実施形態においては、図１１（ユーザポリシ情報テーブル４０２ａの概略図）に示すようなユーザポリシ情報テーブル４０２ａがユーザポリシ情報記憶領域４０２に記憶される。
【００９３】
ユーザポリシ情報テーブル４０２ａは、ユーザＩＤ欄４０２ｂと、認証サーバＩＤ欄４０２ｃと、最終認証時刻欄４０２ｄと、優先度欄４０２ｅと、使用条件欄４０２ｆと、サービス提供サーバＩＤ条件欄４０２ｇと、を有する。
【００９４】
ユーザＩＤ欄４０２ｂには、端末装置１のユーザを特定する情報が格納される。ここでは、ユーザを特定する情報として、各々のユーザに一意に割り当てられている識別情報であるユーザＩＤが格納される。
【００９５】
ここで、一つのユーザＩＤには、一つ以上の認証サーバ関連情報がレコード（テーブルの行）の形で関連付けられる。認証サーバ関連情報は、認証サーバＩＤと、最終認証時刻と、優先度と、選択条件と、を有する。

【００９６】
認証サーバＩＤ欄４０２ｃには、ユーザＩＤ欄４０２ｂで特定されるユーザを認証可能な認証サーバ３を特定する情報（ここでは、認証サーバＩＤ）が格納される。例えば、認証サーバ３がＨＴＴＰによる接続を受け入れる場合、認証サーバＩＤ欄４０２ｃの値として、ｈｔｔｐ：／／ｗｗｗ．ｈｉｔａｃｈｉ．ｃｏｍ／のようなＵＲＬを利用することができる。
【００９７】
最終認証時刻欄４０２ｄには、ユーザＩＤ欄４０２ｂで特定されるユーザの認証に、認証サーバＩＤ欄４０２ｃで特定される認証サーバ３が、最後に選択された際の時刻を特定する情報（ここでは、年月日時間）が格納される。
【００９８】
優先度欄４０２ｅには、ユーザＩＤ欄４０２ｂで特定されるユーザの認証に、認証サーバＩＤ欄４０２ｃで特定される認証サーバ３を選択する際の優先度を特定する情報が格納される。本実施形態においては、優先度欄４０２ｅに格納されている数値が小さいほど、選択する際の優先度（優先的に選択される度合い）が高くなるようにされているが、このような態様に限定されるわけではない。
【００９９】
使用条件欄４０２ｆには、ユーザＩＤ欄４０２ｂで特定されるユーザの認証に、認証サーバＩＤ欄４０２ｃで特定される認証サーバ３を選択する際の条件を特定する情報が格納される。ここで、認証サーバ３を使用する際の条件を特定する情報として、例えば、ユーザのプレゼンス情報、ユーザが使用する端末装置１のプレゼンス情報、ユーザが使用する端末装置１の種類などを利用することができる。
【０１００】
なお、使用条件欄４０２ｆに「＊」の記号が格納されている場合には、認証サーバＩＤ欄４０２ｃで特定される認証サーバ３が使用される場合に満たすべき条件は存在しないこと（条件が課せられていないこと）を示すものとする。
【０１０１】
サービス提供サーバＩＤ条件欄４０２ｇには、ユーザＩＤ欄４０２ｂで特定されるユーザの認証に、認証サーバＩＤ欄４０２ｃで特定される認証サーバを選択するサービス提供サーバ２を特定する情報（ここでは、サービス提供サーバＩＤ）が格納される。例えば、ユーザＩＤ欄４０２ｂで特定されるユーザの認証に、認証サーバＩＤ欄４０２ｃで特定される認証サーバを使用するのは、サービス提供サーバＩＤ条件欄４０２ｇで特定されるサービス提供サーバ２より認証要求を受けた場合に、制限することができる。
【０１０２】
なお、サービス提供サーバＩＤ条件欄４０２ｇに「＊」の記号が格納されている場合には、当該サービス提供サーバＩＤ条件欄が、全てのサービス提供サーバＩＤを含むこと（特定のサービス提供サーバ２に限定されないこと）を示すものとする。
【０１０３】
図１０に戻り、認証サーバ情報記憶領域４０３には、認証仲介サーバ４がサービス提供サーバ２に対して紹介可能な認証サーバ３と、当該認証サーバ３が対応する認証方式と、当該認証サーバ３が保有するユーザの属性情報と、を特定する認証サーバ情報が記憶される。例えば、本実施形態においては、図１２（認証サーバ情報テーブル４０３ａの概略図）に示すような認証サーバ情報テーブル４０３ａが認証サーバ情報記憶領域４０３に記憶される。
【０１０４】
認証サーバ情報テーブル４０３ａは、認証サーバＩＤ欄４０３ｂと、対応認証方式欄４０３ｃと、保有属性情報欄４０３ｄと、を有する。
【０１０５】
認証サーバＩＤ欄４０３ｂには、認証サーバ３を特定する情報が格納される。ここでは、各々の認証サーバ３を一意に識別するための識別情報である認証サーバＩＤが格納され

る。
【０１０６】
一つの認証サーバＩＤには、一つ以上の対応認証方式と、一つ以上の保有属性情報が、レコード（テーブルの行）の形で関連付けられる。
【０１０７】
対応認証方式欄４０３ｃには、認証サーバＩＤ欄４０３ｂで特定される認証サーバ３によって実行可能な認証方式の種類を特定する情報が格納される。ここで、認証方式の種類を特定する情報として、各々の認証方式を一意に識別するための識別情報である認証方式名が格納される。
【０１０８】
保有属性情報欄４０３ｄには、認証サーバＩＤ欄４０３ｂによって特定される認証サーバ３が保有するユーザの属性情報の種類を特定する情報が格納される。ここで、ユーザ属性情報種類を特定する情報として、氏名、住所、メールアドレス、クレジットカード番号等のようなユーザ属性の名称が格納される。
【０１０９】
図１０に戻り、サービス提供サーバ要求情報記憶領域４０４には、サービス提供サーバ２毎に、認証サーバ３を選択する選択指針を特定するサービス提供サーバ要求情報が記憶される。例えば、本実施形態においては、図１３（サービス提供サーバ要求情報テーブル４０４ａの概略図）に示すようなサービス提供サーバ要求情報テーブル４０４ａがサービス提供サーバ要求情報記憶領域４０４に記憶される。
【０１１０】
サービス提供サーバ要求情報テーブル４０４ａは、サービス提供サーバＩＤ欄４０４ｂと、連携認証サーバＩＤ欄４０４ｃと、要求認証レベル欄４０４ｄと、要求属性情報欄４０４ｅと、を有する。
【０１１１】
サービス提供サーバＩＤ欄４０４ｂには、サービス提供サーバ２を特定する情報が格納される。ここでは、サービス提供サーバ２を特定する情報として、各々のサービス提供サーバ２を一意に識別するための識別情報であるサービス提供サーバＩＤが格納される。
【０１１２】
一つのサービス提供サーバＩＤには、一つ以上の連携認証サーバＩＤと、一つ以上の要求認証方式と、一つ以上の要求属性情報と、が、レコード（テーブルの行）の形で関連付けられる。
【０１１３】
連携認証サーバＩＤ欄４０４ｃには、サービス提供サーバＩＤ欄４０４ｂで特定されるサービス提供サーバ２が、認証を委託するために事前に連携処理を行っている認証サーバ３を特定する情報が格納される。ここでは、認証サーバ３を特定する情報として、各々の認証サーバ３を一意に識別するための識別情報である認証サーバＩＤが格納される。なお、連携認証サーバＩＤ欄４０４ｃに「＊」の記号が格納されている場合には、サービス提供サーバＩＤ欄４０４ｂで特定されるサービス提供サーバ２は、認証サーバ３との間で事前の連携処理を必要としないことを示す。
【０１１４】
要求認証レベル欄４０４ｄには、サービス提供サーバＩＤ欄４０４ｂで特定されるサービス提供サーバ２が、サービスを提供する際に要求する認証の安全性（強度）のレベル（要求認証レベル）を特定する情報が格納される。
【０１１５】
要求属性情報欄４０４ｅには、サービス提供サーバＩＤ欄４０４ｂで特定されるサービス提供サーバ２が、認証サーバ３に開示を要求するユーザの属性情報の種類を特定する情報が格納される。なお、要求属性情報欄４０４ｅに「＊」の記号が格納されている場合には、サービス提供サーバＩＤ欄４０４ｂで特定されるサービス提供サーバ２は、認証サーバ３に対して特定の属性情報を要求しないことを示す。

【０１１６】
図１０に戻り、認証レベル情報記憶領域４０５には、ユーザが受けた最新の認証レベル（現在認証レベル）を特定する認証レベル情報が格納される。例えば、本実施形態においては、図１４（認証レベル情報テーブル４０５ａの概略図）に示すような認証レベル情報テーブル４０５ａが認証レベル情報記憶領域４０５に記憶される。
【０１１７】
認証レベル情報テーブル４０５ａは、ユーザＩＤ欄４０５ｂと、現在認証レベル欄４０５ｃと、を有する。
【０１１８】
ユーザＩＤ欄４０５ｂには、ユーザを特定する情報が格納される。ここでは、各々のユーザを一意に識別するための識別情報であるユーザＩＤが格納される。
【０１１９】
現在認証レベル欄４０５ｃには、ユーザＩＤ欄４０５ｂで特定されるユーザが認証を受けた最新の認証レベル（現在受けている認証レベル）を特定する情報が格納される。
【０１２０】
図１０に戻り、提供認証強度情報記憶領域４０６には、認証サーバ３で提供する認証方式と、当該認証方式の認証強度と、を特定する提供認証強度情報が記憶される。例えば、本実施形態においては、図１５（提供認証強度情報テーブル４０６ａの概略図）に示すような提供認証強度情報テーブル４０６ａが提供認証強度情報記憶領域４０６に記憶される。
【０１２１】
提供認証強度情報テーブル４０６ａは、認証サーバＩＤ欄４０６ｂと、提供認証方式欄４０６ｃと、認証強度欄４０６ｄと、提供ＵＲＩ欄４０６ｅと、を有する。
【０１２２】
認証サーバＩＤ欄４０６ｂには、認証サーバ３を特定する情報が格納される。ここでは、各々の認証サーバ３を一意に識別するための識別情報である認証サーバＩＤが格納される。
【０１２３】
提供認証方式欄４０６ｃには、認証サーバＩＤ欄４０６ｂで特定される認証サーバ３が提供する認証方式を特定する情報が格納される。
【０１２４】
認証強度欄４０６ｄには、認証サーバＩＤ欄４０６ｂで特定される認証サーバ３が、提供認証方式欄４０６ｃで特定される認証方式で行う認証の認証強度を特定する情報が格納される。ここで、本実施形態においては、認証強度欄４０６ｄに格納される数値が大きいほど、認証強度が高いこと（認証の安全性が高いこと）を示すものとする。
【０１２５】
提供ＵＲＩ欄４０６ｅには、認証サーバＩＤ欄４０６ｂで特定される認証サーバ３が、提供認証方式欄４０６ｃで特定される認証方式による認証を提供するＵＲＩを特定する情報が格納される。
【０１２６】
図１０に戻り、認証レベル定義情報記憶領域４０７には、認証レベルの定義を特定する認証レベル定義情報が記憶される。例えば、本実施形態においては、図１６（認証レベル定義情報テーブル４０７ａの概略図）に示すような認証レベル定義情報テーブル４０７ａが認証レベル定義情報記憶領域４０７ａに記憶される。
【０１２７】
認証レベル定義情報テーブル４０７ａは、認証レベル欄４０７ｂと、定義欄４０７ｃと、を有する。
【０１２８】
認証レベル欄４０７ｂには、認証レベルを特定する情報が格納される。
【０１２９】

定義欄４０７ｃには認証レベル欄４０７ｂで特定される認証レベルを満足するために実施する必要のある認証の方法を特定する情報が格納される。ここで、本実施形態においては、定義欄４０７ｃにおいて、認証強度と、認証の回数と、の組合せにより、各々認証レベルに応じた認証の方式を特定している。

【０１３０】

なお、本実施形態の認証レベル定義では、サービス提供者がある認証レベルを要求している場合、ユーザがそれよりも大きな数字の認証レベルを満足している場合には、要求認証レベルを満足する、と判定するようにしている。

【０１３１】

図１０に戻り、ＩＤ情報記憶領域４０８には、ユーザが各々のサービス提供サーバ２で使用する固有のユーザＩＤを特定するＩＤ情報が記憶される。例えば、本実施形態においては、図１７（ＩＤ情報テーブル４０８ａの概略図）に示すようなＩＤ情報テーブル４０８ａがＩＤ情報記憶領域４０８に記憶される。

【０１３２】

ＩＤ情報テーブル４０８ａは、ユーザＩＤ欄４０８ｂと、サーバＩＤ欄４０８ｃと、サービス固有ユーザＩＤ欄４０８ｄと、を有する。

【０１３３】

ユーザＩＤ欄４０８ｂには、ユーザを特定する情報が格納される。ここでは、各々のユーザを一意に識別するための識別情報であるユーザＩＤが格納される。

【０１３４】

サーバＩＤ欄４０８ｃには、ユーザＩＤ欄４０８ｂで特定されるユーザがサービスの提供を受けるサービス提供サーバ２を特定する情報が格納される。ここでは、各々のサービス提供サーバ２を一意に識別するための識別情報であるサービス提供サーバＩＤが格納される。

【０１３５】

サービス固有ユーザＩＤ欄４０８ｄには、ユーザＩＤ欄４０８ｂで特定されるユーザが、サーバＩＤ欄４０８ｃで特定されるサービス提供サーバ２において使用している識別情報（サービス固有ユーザＩＤ）を特定する情報が格納される。

【０１３６】

図１０に戻り、属性情報記憶領域４０９には、ユーザの属性を特定する属性情報が格納される。例えば、本実施形態においては、図１８（属性情報テーブル４０９ａの概略図）に示すような属性情報テーブル４０９ａが属性情報記憶領域４０９に記憶される。

【０１３７】

属性情報テーブル４０９ａは、ユーザＩＤ欄４０９ｂと、属性型欄４０９ｃと、属性値欄４０９ｄと、を有する。

【０１３８】

ユーザＩＤ欄４０９ｂには、ユーザを特定する情報が格納される。ここでは、各々のユーザを一意に識別するための識別情報であるユーザＩＤが格納される。

【０１３９】

属性型欄４０９ｃには、ユーザＩＤ欄４０９ｂで特定されるユーザの属性の種類を特定する情報が格納される。

【０１４０】

属性値欄４０９ｄには、ユーザＩＤ欄４０９ｂで特定されるユーザが、属性型欄４０９ｃで特定される属性の種類において使用する属性の値を特定する情報が格納される。

【０１４１】

図１０に戻り、制御部４１１は、情報取得要求処理部４１２と、認証サーバ選択部４１３と、ユーザポリシ管理部４１４と、ユーザ情報取得部４１５と、アイデンティティ変換部４１６と、を有する。

【０１４２】

情報取得要求処理部４１２は、送受信部４２０及びネットワーク６を介して、サービス

提供サーバ２から直接、もしくは端末装置１を介して間接的に、情報取得要求メッセージを受信すると、受信した情報取得要求メッセージに含まれるユーザＩＤ及びサービス提供サーバＩＤを取得し、認証サーバ選択部４１３に出力する。

【０１４３】

なお、受信した当該情報取得要求メッセージにユーザＩＤが含まれていない場合には、端末装置１に対して、送受信部４２０及びネットワーク６を介して、ユーザＩＤの入力を要求する応答メッセージ（例えばｆｏｒｍタグを含むＨＴＴＰレスポンス）を返信し、ユーザＩＤを取得するようにすることも可能である。

【０１４４】

認証サーバ選択部４１３は、情報取得要求処理部４１２から、ユーザＩＤ及びサービス提供サーバＩＤを取得すると、記憶部４０１のユーザポリシ情報記憶領域４０２に記憶されているユーザポリシ情報と、認証サーバ情報記憶領域４０３に記憶されている認証サーバ情報と、サービス提供サーバ要求情報記憶領域４０４に記憶されているサービス提供サーバ要求情報と、から取得したユーザＩＤ及びサービス提供サーバＩＤに該当する情報を取得するとともに、後述するユーザ情報取得部４１５が取得したユーザのプレゼンス情報などを参照して、ユーザの認証に使用すべき認証サーバ３を選択する。

【０１４５】

また、認証サーバ選択部４１３は、選択した認証サーバ３を特定する認証サーバ情報を、サービス提供サーバ２に対して直接、もしくは端末装置１を介して間接的に送信する。例えば、非特許文献３に記載されるＯｐｅｎＩＤ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎのように、認証サーバ３の情報をＸＲＤＳ文書として表現し、サービス提供サーバ２に送信することができる。また、非特許文献２に記載されているＩｄｅｎｔｉｔｙ　Ｐｒｏｖｉｄｅｒ　Ｄｉｓｃｏｖｅｒｙ　Ｐｒｏｆｉｌｅに従い、ＨＴＴＰリダイレクトを利用して、端末装置１を介して間接的に認証サーバ情報をサービス提供サーバ２へ送信してもよい。

【０１４６】

ユーザポリシ管理部４１４は、送受信部４２０及びネットワーク６を介して、端末装置１からユーザＩＤ、当該ユーザＩＤによって特定されるユーザが使用する認証サーバ３の認証サーバＩＤ、当該認証サーバ３の優先度、当該認証サーバ３を選択する条件（使用条件、サービス提供サーバＩＤ条件）、を特定する情報を取得し、記憶部４０１のユーザポリシ情報記憶領域４０２に記憶されたユーザポリシ情報テーブル４０２ａに対して、レコードを作成、更新、もしくは削除する。

【０１４７】

ユーザ情報取得部４１５は、送受信部４２０及びネットワーク６を介して、プレゼンスサーバ５に対してユーザＩＤを特定したプレゼンス情報取得要求を送信することで、プレゼンスサーバ５から、当該ユーザＩＤに対応するユーザのプレゼンス情報を取得する。また、ネットワーク６上に、プレゼンスに類するユーザの情報を管理するサーバが存在する場合には、当該サーバからユーザ情報を取得する。

【０１４８】

アイデンティティ変換部４１６は、ＩＤ情報記憶領域４０８に記憶されているＩＤ情報及び属性情報記憶領域４０９に記憶されている属性情報を管理する処理を行う。

【０１４９】

また、アイデンティティ変換部４１６は、サービス提供サーバ２が要求する要求属性情報を、属性情報記憶領域４０９から取得して、送受信部４２０及びネットワーク６を介して、直接、または、端末装置１を介して間接的に、サービス提供サーバ２に送信する処理を行う。

【０１５０】

入力部４１８は、情報の入力を受け付ける。

【０１５１】

出力部４１９は、情報を出力する。

【０１５２】

送受信部４２０は、ネットワーク６を介した情報の送受信を行う。

【０１５３】

以上に記載した認証仲介サーバ４は、例えば、図４に示すようなコンピュータ９により実現できる。

【０１５４】

例えば、記憶部４０１は、ＣＰＵ９０１がメモリ９０２又は外部記憶装置９０３を利用することにより実現可能であり、制御部４１１は、外部記憶装置９０３に記憶されている所定のプログラムをメモリ９０２にロードしてＣＰＵ９０１で実行することで実現可能であり、入力部４１８は、ＣＰＵ９０１が入力装置９０６を利用することで実現可能であり、出力部４１９は、ＣＰＵ９０１が出力装置９０７を利用することで実現可能であり、送受信部４２０は、ＣＰＵ９０１が送受信装置９０８を利用することで実現可能である。

【０１５５】

この所定のプログラムは、読書装置９０５を介して記憶媒体９０４から、あるいは、送受信装置９０８を介してネットワークから、外部記憶装置９０３にダウンロードされ、それから、メモリ９０２上にロードされてＣＰＵ９０１により実行されるようにしてもよい。また、読書装置９０５を介して記憶媒体９０４から、あるいは、送受信装置９０８を介してネットワークから、メモリ９０２上に直接ロードされ、ＣＰＵ９０１により実行されるようにしてもよい。

【０１５６】

図１９は、プレゼンスサーバ５の一例を示す概略図である。図示するように、プレゼンスサーバ５は、記憶部５０１と、制御部５０４と、入力部５０８と、出力部５０９と、送受信部５１０と、を備える。

【０１５７】

記憶部５０１は、プレゼンス情報記憶領域５０２を備える。

【０１５８】

プレゼンス情報記憶領域５０２には、端末装置１のユーザの状況を特定するプレゼンス情報が記憶される。例えば、本実施形態においては、図２０（プレゼンス情報テーブル５０２ａの概略図）に示すようなプレゼンス情報テーブル５０２ａがプレゼンス情報記憶領域５０２に記憶される。

【０１５９】

プレゼンス情報テーブル５０２ａは、ユーザＩＤ欄５０２ｂと、プレゼンス情報欄５０２ｃと、を有する。

【０１６０】

ユーザＩＤ欄５０２ｂには、ユーザを特定する情報が格納される。ここでは、各々のユーザを一意に識別するための識別情報であるユーザＩＤが格納される。

【０１６１】

プレゼンス情報欄５０２ｃには、ユーザＩＤ欄５０２ｂで特定されるユーザの状況（プレゼンス）を特定するプレゼンス情報が格納される。

【０１６２】

図１９に戻り、制御部５０４は、情報取得要求処理部５０５と、情報更新要求処理部５０６と、を備える。

【０１６３】

情報取得要求処理部５０５は、送受信部５１０及びネットワーク６を介して、認証仲介サーバ４から情報取得要求メッセージを受信すると、取得した情報取得要求メッセージに含まれるユーザＩＤを取得し、当該ユーザＩＤをキーとしてプレゼンス情報記憶領域５０２に記憶されているプレゼンス情報を検索する。検索の結果、当該ユーザＩＤによって特定されるユーザのプレゼンス情報を取得すると、送受信部５１０及びネットワーク６を介して、情報取得要求メッセージを送信してきた認証仲介サーバ４に返信する。

【０１６４】

情報更新要求処理部５０６は、送受信部５１０及びネットワーク６を介して、端末装置

１から情報更新要求メッセージを受信すると、受信した情報更新要求メッセージに含まれるユーザＩＤおよびプレゼンス情報を取得し、プレゼンス情報記憶領域５０２内の、当該ユーザＩＤに対応するレコードを作成もしくは更新する。

【０１６５】

入力部５０８は、情報の入力を受け付ける。

【０１６６】

出力部５０９は、情報を出力する。

【０１６７】

送受信部５１０は、ネットワーク６を介した情報の送受信を行う。

【０１６８】

以上に記載したプレゼンスサーバ５は、例えば、図４に示すようなコンピュータ９により実現できる。

【０１６９】

例えば、記憶部５０１は、ＣＰＵ９０１がメモリ９０２又は外部記憶装置９０３を利用することにより実現可能であり、制御部５０４は、外部記憶装置９０３に記憶されている所定のプログラムをメモリ９０２にロードしてＣＰＵ９０１で実行することで実現可能であり、入力部５０８は、ＣＰＵ９０１が入力装置９０６を利用することで実現可能であり、出力部５０９は、ＣＰＵ９０１が出力装置９０７を利用することで実現可能であり、送受信部５１０は、ＣＰＵ９０１が送受信装置９０８を利用することで実現可能である。

【０１７０】

この所定のプログラムは、読書装置９０５を介して記憶媒体９０４から、あるいは、送受信装置９０８を介してネットワークから、外部記憶装置９０３にダウンロードされ、それから、メモリ９０２上にロードされてＣＰＵ９０１により実行されるようにしてもよい。また、読書装置９０５を介して記憶媒体９０４から、あるいは、送受信装置９０８を介してネットワークから、メモリ９０２上に直接ロードされ、ＣＰＵ９０１により実行されるようにしてもよい。

【０１７１】

図２１及び図２２は、認証システム１０で認証を行う際の処理の一例を示すシーケンスである。

【０１７２】

本シーケンスにおいては、ユーザＩＤ“ｕｓｅｒ００１”により識別されるユーザが、端末装置１を使用して、サービス提供サーバＩＤ“ｓｐ００１”により識別されるサービス提供サーバ２Ａと、サービス提供サーバＩＤ“ｓｐ００２”により識別されるサービス提供サーバ２Ｂと、に対してサービスの提供を要求した場合における、各装置における処理を示す。なお、端末装置１とその他の装置との間でセッションは確立されていないことを前提とする。

【０１７３】

また、認証サーバ３Ａは認証サーバＩＤ“ｉｄｐ００１”により識別され、認証サーバ３Ｂは認証サーバＩＤ“ｉｄｐ００２”によって識別されるものとする。

【０１７４】

さらに、“ｓｐ００１”のサービス提供サーバＩＤで特定されるサービス提供サーバ２Ａは、認証仲介サーバ４に対して認証サーバ３の取得（選択）を要求する際、端末装置１を介して間接的に要求メッセージを送信するものとし、一方、サービス提供サーバＩＤ“ｓｐ００２”で特定されるサービス提供サーバ２Ｂは、認証仲介サーバ４に対して認証サーバ３の取得（選択）を要求する際、端末装置１を介さず、要求メッセージを直接送信するものとする。

【０１７５】

図２１では、端末装置１のユーザが、サービスサーバ２Ａからサービスの提供を受ける場合のシーケンスを示す。

【０１７６】

まず、端末装置１のユーザが、入力部１１５を介して、サービス提供サーバ２Ａからサービスの提供を受けるためのサービス要求操作を実行した場合、端末装置１のサービス要求生成部１０７は、端末装置１のユーザのユーザＩＤ“ｕｓｅｒ００１”を特定したサービス要求メッセージを生成し、送受信部１１７及びネットワーク６を介して、生成したサービス要求メッセージをサービス提供サーバ２Ａへ送信する（Ｓ１０）。ここで、本実施形態においては、サービス要求メッセージは、ＨＴＴＰのＧＥＴリクエストやＰＯＳＴリクエスト等を用いて記述されるが、このような態様に限定されるわけではない。

【０１７７】

サービス提供サーバ２Ａでは、送受信部２１１及びネットワーク６を介してサービス要求メッセージを受信すると、サービス通信部２０９が、当該サービス要求メッセージにセッション情報が含まれているか否かを確認し（本シーケンスではセッション情報が含まれていないものとして説明する）、セッション情報が存在しないことが判明すると、認証サーバ情報取得部２０７が、ユーザＩＤ“ｕｓｅｒ００１”及びサービス提供サーバＩＤ“ｓｐ００１”を特定した情報取得要求メッセージを生成し、送受信部２１３及びネットワーク６を介して、端末装置１を経由する形で、認証仲介サーバ４へ送信する（Ｓ１１、Ｓ１２）。

【０１７８】

認証仲介サーバ４は、送受信部４１２及びネットワーク６を介して情報取得要求メッセージを受信すると、情報取得要求処理部４１２が、受信した情報取得要求メッセージに含まれるユーザＩＤ及びサービス提供サーバＩＤを取得して、認証サーバの候補を選択する処理に移る。ここでは、ユーザＩＤとして“ｕｓｅｒ００１”が取得され、サービス提供サーバＩＤとして“ｓｐ００１”が取得される。

【０１７９】

そして、ユーザ情報取得部４１５が、情報取得要求処理部４１２で取得したユーザＩＤを特定したプレゼンス情報取得要求メッセージを生成し、送受信部４２０及びネットワーク６を介して、生成したプレゼンス情報取得要求メッセージをプレゼンスサーバ５に送信する（Ｓ１３）。

【０１８０】

このようなプレゼンス情報取得要求メッセージを受信したプレゼンスサーバ５では、情報取得要求処理部５０５が、受信したプレゼンス情報取得要求メッセージに含まれるユーザＩＤ（ここでは、“ｕｓｅｒ００１”）に対応するプレゼンス情報をプレゼンス情報記憶領域５０２から取得し、取得したプレゼンス情報を含む応答メッセージを認証仲介サーバ４に返信する（Ｓ１４）。例えば、図２０に示すプレゼンス情報テーブル５０２では、ユーザＩＤ“ｕｓｅｒ００１”に対応するプレゼンス情報として「自宅」を特定する情報が取得される。

【０１８１】

次に、認証サーバ選択部４１３が、認証サーバ３の選択処理を行う（Ｓ１５）。

【０１８２】

例えば、まず、認証サーバ選択部４１３は、ユーザＩＤ“ｕｓｅｒ００１”をキーとして、ユーザポリシ情報記憶領域４０２に記憶されているユーザポリシ情報テーブル４０２ａからポリシ情報（認証サーバＩＤ、最終認証時刻、優先度、使用条件、サービス提供サーバＩＤ条件）の集合（レコードの集合）を取得し、認証サーバ３の候補群として記憶部４０１に記憶する。例えば、図１１に示すユーザポリシ情報テーブル４０２ａでは、ユーザＩＤ“ｕｓｅｒ００１”に対応するユーザポリシ情報として、テーブル４０２ａの上から４レコード（認証サーバＩＤ“ｉｄｐ００１”、“ｉｄｐ００２”、“ｉｄｐ００３”、“ｉｄｐ００４”に対応する４レコード）、が取得される。

【０１８３】

次に、認証サーバ選択部４１３は、サービス提供サーバＩＤ“ｓｐ００１”をキーとして、サービス提供サーバ要求情報記憶領域４０４に記憶されているサービス提供サーバ要求情報テーブル４０４ａからサービス提供サーバ要求情報（連携認証サーバＩＤ、要求認

証レベル、要求属性情報）を取得する。例えば、図１２に示すサービス提供サーバ要求情報テーブル４０４ａでは、サービス提供サーバＩＤ“ｓｐ００１”に対応するサービス提供サーバ要求情報として、最も上のレコードに格納されている連携認証サーバＩＤが「＊」、要求認証レベルが「２」、要求属性情報が「メールアドレス」、となっている情報が取得される。

【０１８４】

続いて、認証サーバ選択部４０７は、不足している認証強度を判定する処理を行う。

【０１８５】

まず、認証サーバ選択部４１３は、認証レベル情報記憶領域４０５に記憶されている認証レベル情報テーブル４０５ａより、ユーザＩＤ“ｕｓｅｒ００１”に対応する最新（現在）の認証レベルを取得する。ここでは、ユーザＩＤ“ｕｓｅｒ００１”で識別されるユーザはまだ認証を受けていないため、現在の認証レベルは「０」であるとする。

【０１８６】

上述のように、サービス提供サーバ要求情報テーブル４０４ａから取得したサービス提供サーバ要求情報では、要求認証レベルが「２」であるため、認証サーバ選択部４１３は、認証強度が不足していると判定する。

【０１８７】

そして、認証サーバ選択部４１３は、認証レベル定義テーブル４０７ａを参照して、ユーザＩＤ“ｕｓｅｒ００１”で識別されるユーザの現在の認証レベル「０」と、要求認証レベル「２」と、を比較して、要求認証レベル「２」を満足するために必要な認証強度を判定する。例えば、図１６に示す認証レベル定義テーブル４０７ａでは、認証レベル「０」は「認証を受けていない」状態であり、認証レベル「２」は「認証強度が２の認証方式で１回認証を受ける」状態であるため、不足している認証強度は「２」であり、この認証強度「２」の認証を一回行えば、要求認証レベル「２」を満足することができると判定する。

【０１８８】

続いて、認証サーバ選択部４０７は、認証サーバ３の候補を絞り込む処理を行う。

【０１８９】

まず、認証サーバ選択部４０７は、サービス提供サーバＩＤ“ｓｐ００１”をキーとしてサービス提供サーバ要求情報テーブル４０４ａから取得したサービス提供サーバ要求情報に含まれる連携認証サーバＩＤと一致する認証サーバＩＤを有するものを、記憶部４０１に記憶された認証サーバ３の候補群から選択する。ここではサービス提供サーバ“ｓｐ００１”の連携認証サーバの値が「＊」であるため、認証サーバ３の候補群内の全ての認証サーバ３が候補として残される。

【０１９０】

次に、認証サーバ選択部４０７は、認証サーバ３の候補群から、サービス提供サーバＩＤ条件の値が、情報取得要求メッセージの送信元であるサービス提供サーバ２のサービス提供サーバＩＤを含むものだけを選択し、それ以外のものを候補群から削除する。ここでは、情報取得要求メッセージの送信元であるサービス提供サーバのＩＤ“ｓｐ００１”は各レコードのサービス提供サーバＩＤ条件に含まれるため、候補群内の全ての認証サーバ３が候補として残される。

【０１９１】

次に、認証サーバ選択部４０７は、認証サーバ情報記憶領域４０３に記憶されている認証サーバ情報テーブル４０３ａから、認証サーバ３の候補群に残った認証サーバ３の認証サーバＩＤに対応する認証サーバ情報（要求認証レベル、保有属性情報）を取得し、記憶部４０１内の候補群の各々に追加する（各々に関連付ける）。

【０１９２】

次に、認証サーバ選択部４０７は、認証サーバ３の候補群内の認証サーバ３において、認証強度情報記憶領域４０６に記憶されている認証強度情報テーブル４０６ａから、認証強度が上述のようにして判定した不足している認証強度と一致し、かつ、保有属性情報が

要求属性情報と一致するものだけを選択する。

【０１９３】

ここでは、不足している認証強度が「２」で、要求属性情報として「メールアドレス」が指定されているため、認証強度情報テーブル４０６ａ及び認証サーバ情報テーブル４０３ａにおいてこれらに適合するものとして、“ｉｄｐ００１”及び“ｉｄｐ００２”が候補群に残される。認証サーバ“ｉｄｐ００４”については認証強度が「１」であるため、また、認証サーバ“ｉｄｐ００３”については、保有属性情報が「クレジットカード番号」のみに限られ、要求属性情報「メールアドレス」を含まないため、それぞれ候補群から削除される。

【０１９４】

次に、認証サーバ選択部４０７は、候補群に残った認証サーバ３の内、使用条件の値がステップＳ１４で取得したユーザのプレゼンス情報と一致するものだけを残し、一致しないものを候補群から削除する。ここでは、プレゼンス情報として「自宅」を特定する情報が得られているため、候補群の内、使用条件が「自宅」もしくは「＊」（使用条件を指定していないことを示す）に一致する“ｉｄｐ００１”と“ｉｄｐ００２”が候補群に残される。

【０１９５】

次に、認証サーバ選択部４０７は、候補群の中で最も優先度が高い候補を残し、その他の候補を候補群から削除する。図１１に示すユーザポリシ情報テーブル４０２ａでは、これらの候補群“ｉｄｐ００１”及び“ｉｄｐ００２”はともに同じ優先度「１０」をもつため、候補群の絞り込みは行われない。

【０１９６】

次に、認証サーバ選択部４０７は、候補群内で最終認証時刻が最も古い候補を選択する。図１１に示すユーザポリシ情報テーブル４０２ａでは、“ｉｄｐ００１”の最終認証時刻が「２００８－０８－１９Ｔ１０：０３：２８」で、“ｉｄｐ００２”の最終認証時刻が「２００８－０７－３０Ｔ１７：３２：１５」であるため、最終認証時刻の最も古いものとして、“ｉｄｐ００２”が候補として選ばれる。

【０１９７】

この段階で候補として選択された認証サーバ３について、ユーザポリシ記憶領域４０２に記憶されているユーザポリシ情報テーブル４０２ａの最終認証時刻欄４０２ｄの値を、現在の時刻で置き換える。ここでは、“ｉｄｐ００２”の最終認証時刻欄が現在時刻（例えば、２００８－０８－２２Ｔ１６：５０：３６とする）で書き換えられる。

【０１９８】

以上で、ステップＳ１５の認証サーバ３の選択処理が終了する。

【０１９９】

次に、認証サーバ選択部４１３は、候補として選択された認証サーバ３Ｂが提供する認証方式（認証強度の不足に対応するもの）の提供ＵＲＩを提供認証強度情報記憶領域４０６に記憶されている提供認証強度情報テーブル４０６ａの提供ＵＲＩ欄４０６ｅより取得して、取得した提供ＵＲＩを特定する情報を含む応答メッセージ（情報取得要求メッセージに対する）を生成して、サービス提供サーバ２Ａへ、端末装置１を介して間接的に送信する（Ｓ１６、Ｓ１７）。ここでは、認証サーバＩＤ“ｉｄｐ００２”が提供する電子証明書型認証方式の提供ＵＲＩ“ｈｔｔｐｓ：／／ｉｄｐ００２／”が、端末装置１を介して間接的に、サービス提供サーバ２Ａへ送信される。

【０２００】

サービス提供サーバ２Ａは、認証仲介サーバ４から情報取得メッセージに対する応答メッセージを受信すると、認証サーバ情報取得部２０７が、受信した応答メッセージから提供ＵＲＩを取得して、認証要求処理部２０８が、提供ＵＲＩに対して端末装置１を介して認証要求メッセージを送信する（Ｓ１８、Ｓ１９）。

【０２０１】

認証サーバ３Ｂは、認証実行部３０７が、ユーザが使用する端末装置１との間で認証処

理を実行する（Ｓ２０）。ここでは、図１２の認証サーバ情報テーブル４０３ａに示されるように、認証サーバＩＤ“ｉｄｐ００２”で特定される認証サーバ３は電子証明書型認証方式にのみ対応しているため、認証実行部３０７は、送受信部３１４及びネットワーク６を介して、端末装置１に対してユーザの電子証明書を要求し、取得する。

【０２０２】

そして、認証実行部３０７は、取得した電子証明書の正当性を確認し（ここでは、電子証明書が正当なものであるとして説明する）、認証結果生成部３０８が、ユーザが認証に成功したことを示す認証結果メッセージを生成し、端末装置１を介して間接的に、サービス提供サーバ２Ａに送信する（Ｓ２１、Ｓ２２）。

【０２０３】

サービス提供サーバ２Ａでは、認証サーバ３Ｂより認証結果メッセージを受信すると、認証要求処理部２０８が、受信した認証結果メッセージより認証結果を特定する情報を取得し、認証結果の正当性を確認する（Ｓ２３）。

【０２０４】

認証結果を検証した結果、ユーザの正当性が確認できると、認証サーバ情報取得部２０７が、前記提供ＵＲＩが提供している認証方式での認証が成功したことを伝える情報取得要求メッセージを生成し、送受信部２１３及びネットワーク６を介して、端末装置１を経由する形で、認証仲介サーバ４へ送信する（Ｓ２４、Ｓ２５）。

【０２０５】

そして、認証仲介サーバ４では、送受信部４２０及びネットワーク６を介して情報取得要求メッセージを受信すると、情報取得要求処理部４１２が、受信した情報取得要求メッセージに含まれるユーザＩＤ及びサービス提供サーバＩＤを取得し、認証サーバの候補を選択する処理に移る（Ｓ２６）。

【０２０６】

ここで、認証サーバ選択部４１３では、上述のステップＳ１５において、ユーザＩＤ“ｕｓｅｒ００１”で識別されるユーザの現在認証レベルが「２」に更新された結果、追加的な認証は不要であると判定し、提供ＵＲＩを含まず、ユーザＩＤ“ｕｓｅｒ００１”を含む応答メッセージを作成し、送受信部４２０及びネットワーク６を介して、端末装置１を経由する形で、サービス提供サーバ２Ａへ送信する（Ｓ２７、Ｓ２８）。

【０２０７】

なお、ステップＳ２７、Ｓ２８で送信する応答メッセージには、ＩＤ情報記憶領域４０８に記憶されているＩＤ情報（サービス提供サーバ２Ａに対するサービス固有ユーザＩＤ）と、属性情報記憶領域４０９に記憶されている属性情報（サービス提供サーバ２Ａが要求する要求属性情報に対応するもの）を含める。

【０２０８】

サービス提供サーバ２Ａでは、認証仲介サーバ４から応答メッセージを受信すると、認証要求処理部２０８が、当該応答メッセージからユーザＩＤを取得するとともに、セッション管理部２０６が新規にセッションＩＤを生成し、セッション情報記憶領域２０２に記憶されているセッション情報テーブル２０２ａに当該ユーザＩＤと当該セッションＩＤの組を格納して、サービス提供部２０５が端末装置１に対して要求されたサービスを提供する（Ｓ２９）。

【０２０９】

なお、サービス提供サーバ２Ａでは、ステップＳ２７、Ｓ２８で送信されてきたＩＤ情報及び属性情報を、サービスを提供する際に使用することができる。例えば、サービス提供サーバ２Ａで提供するサービスに必要なログイン処理や検証処理等にこれらの情報を使用したり、サービス提供サーバ２Ａを介して購入した物品の支払いに属性情報に含まれるクレジットカード番号を用いたり、サービス提供サーバ２Ａからの情報提供に属性情報に含まれるメールアドレスを使用したり、といった使用方法がある。

【０２１０】

次に、図２２では、図２１に示したシーケンスに引き続いて、端末装置１のユーザが、

サービス提供サーバ２Ｂからサービスの提供を受ける場合のシーケンスを示す。

【０２１１】

まず、端末装置１のユーザが、端末装置１の入力部１１５を介して、サービス提供サーバ２Ｂからサービス提供を受けるためのサービス要求操作を実行した場合、端末装置１のサービス要求生成部１０７は、端末装置１のユーザのユーザＩＤ“ｕｓｅｒ００１”を特定したサービス要求メッセージを生成し、送受信部１１７及びネットワーク６を介して、生成したサービス要求メッセージをサービス提供サーバ２Ｂへ送信する（Ｓ３０）。

【０２１２】

サービス提供サーバ２Ｂでは、送受信部２１３及びネットワーク６を介してサービス要求メッセージを受信すると、サービス通信部２０８が、受信したサービス要求メッセージにセッション情報が含まれるか否かを確認し（ここでは、セッション情報が含まれていないものとして説明を行う）、セッション情報が含まれていない場合には、認証サーバ情報取得部２０７が、ユーザＩＤ及びサービス提供サーバＩＤを特定した情報取得要求メッセージを生成し、送受信部２１３及びネットワーク６を介して、認証仲介サーバ４へ送信する（Ｓ３１）。

【０２１３】

認証仲介サーバ４では、送受信部４２０及びネットワーク６を介して情報取得要求メッセージを受信すると、情報取得要求処理部４１２が、受信したメッセージに含まれるユーザＩＤ及びサービス提供サーバＩＤを取得し、認証サーバ３の候補を選択する処理に移る。ここでは、ユーザＩＤとして“ｕｓｅｒ００１”が取得され、サービス提供サーバＩＤとしては“ｓｐ００２”が取得される。

【０２１４】

次に、ユーザ情報取得部４１５は、情報取得要求処理部４１２で取得したユーザＩＤを特定したプレゼンス情報取得要求メッセージを生成し、送受信部４２０及びネットワーク６を介して、生成したプレゼンス情報取得要求メッセージをプレゼンスサーバ５に送信する（Ｓ３２）。

【０２１５】

このようなプレゼンス情報取得要求メッセージを受信したプレゼンスサーバ５では、情報取得要求処理部５０５が、受信したプレゼンス情報取得要求メッセージに含まれるユーザＩＤ（ここでは、“ｕｓｅｒ００１”）に対応するプレゼンス情報をプレゼンス情報記憶領域５０２から取得し、取得したプレゼンス情報を含む応答メッセージを認証仲介サーバ４に返信する（Ｓ３３）。例えば、図２０に示すプレゼンス情報テーブル５０２では、ユーザＩＤ“ｕｓｅｒ００１”に対応するプレゼンス情報として「自宅」を特定する情報が取得される。

【０２１６】

次に、認証サーバ選択部４１３が、認証サーバ３の選択処理を行う（Ｓ３４）。

【０２１７】

例えば、まず、認証サーバ選択部４１３は、ユーザＩＤ“ｕｓｅｒ００１”をキーとして、ユーザポリシ情報記憶領域４０２に記憶されているユーザポリシ情報テーブル４０２ａからポリシ情報（認証サーバＩＤ、最終認証時刻、優先度、使用条件、サービス提供サーバＩＤ条件）の集合（レコードの集合）を取得し、認証サーバ３の候補群として記憶部４０１に記憶する。例えば、図１１に示すユーザポリシ情報テーブル４０２ａでは、ユーザＩＤ“ｕｓｅｒ００１”に対応するユーザポリシ情報として、テーブル４０２ａの上から４レコード（認証サーバＩＤ“ｉｄｐ００１”、“ｉｄｐ００２”、“ｉｄｐ００３”、“ｉｄｐ００４”に対応する４レコード）、が取得される。

【０２１８】

次に、認証サーバ選択部４１３は、サービス提供サーバＩＤ“ｓｐ００２”をキーとして、サービス提供サーバ要求情報記憶領域４０４に記憶されているサービス提供サーバ要求情報テーブル４０４ａからサービス提供サーバ要求情報（連携認証サーバＩＤ、要求認証レベル、要求属性情報）を取得する。例えば、図１２に示すサービス提供サーバ要求情

報テーブル４０４ａでは、サービス提供サーバＩＤ“ｓｐ００２”に対応するサービス提供サーバ要求情報として、上から二番目のレコードに格納されている連携認証サーバＩＤが「＊」、要求認証レベルが「３」、要求属性情報が「＊」、となっている情報が取得される。

【０２１９】

続いて、認証サーバ選択部４０７は、不足している認証強度を判定する処理を行う。

【０２２０】

まず、認証サーバ選択部４１３は、認証レベル情報記憶領域４０５に記憶されている認証レベル情報テーブル４０５ａより、ユーザＩＤ“ｕｓｅｒ００１”に対応する最新（現在）の認証レベルを取得する。ここでは、ユーザＩＤ“ｕｓｅｒ００１”で識別されるユーザは図２１で示す処理により、“ｉｄｐ００２”の電子証明書型認証方式での認証を受けているため、現在の認証レベルは「２」であるとする。

【０２２１】

上述のように、サービス提供サーバ要求情報テーブル４０４ａから取得したサービス提供サーバ要求情報では、要求認証レベルが「４」であるため、認証サーバ選択部４１３は、認証強度が不足していると判定する。

【０２２２】

そして、認証サーバ選択部４１３は、認証レベル定義テーブル４０７ａを参照して、ユーザＩＤ“ｕｓｅｒ００１”で識別されるユーザの現在の認証レベル「２」と、要求認証レベル「４」と、を比較して、要求認証レベル「４」を満足するために必要な認証強度を判定する。例えば、図１６に示す認証レベル定義テーブル４０７ａでは、認証レベル「２」は「認証強度が２の認証方式で１回認証を受ける」状態であり、認証レベル「４」は「認証強度が１の認証方式と認証強度が２の認証方式でそれぞれ１回以上認証を受ける」状態であるため、不足している認証強度は「１」であり、この認証強度「１」の認証を一回行えば、要求認証レベル「４」を満足することができると判定する。

【０２２３】

続いて、認証サーバ選択部４０７は、認証サーバ３の候補を絞り込む処理を行う。

【０２２４】

まず、認証サーバ選択部４０７は、サービス提供サーバＩＤ“ｓｐ００２”をキーとしてサービス提供サーバ要求情報テーブル４０４ａから取得したサービス提供サーバ要求情報に含まれる連携認証サーバＩＤと一致する認証サーバＩＤを有するものを、記憶部４０１に記憶された認証サーバ３の候補群から選択する。ここではサービス提供サーバ“ｓｐ００２”の連携認証サーバの値が「＊」であるため、認証サーバ３の候補群内の全ての認証サーバ３が候補として残される。

【０２２５】

次に、認証サーバ選択部４０７は、認証サーバ３の候補群から、サービス提供サーバＩＤ条件の値が、情報取得要求メッセージの送信元であるサービス提供サーバ２のサービス提供サーバＩＤを含むものだけを選択し、それ以外のものを候補群から削除する。ここでは、情報取得要求メッセージの送信元であるサービス提供サーバのＩＤ“ｓｐ００２”は“ｉｄｐ００３”を除く各レコードのサービス提供サーバＩＤ条件に含まれるため、“ｉｄｐ００１”と、“ｉｄｐ００２”と、“ｉｄｐ００４”と、が候補群に残される。これは、ユーザ“ｕｓｅｒ００１”が、サービス提供サーバ“ｓｐ００２”のサービス利用に際しては、認証サーバ“ｉｄｐ００３”の利用を望んでいないことを示している。

【０２２６】

次に、認証サーバ選択部４０７は、認証サーバ情報記憶領域４０３に記憶されている認証サーバ情報テーブル４０３ａから、認証サーバ３の候補群に残った認証サーバ３の認証サーバＩＤに対応する認証サーバ情報（要求認証レベル、保有属性情報）を取得し、記憶部４０１内の候補群の各々に追加する（各々に関連付ける）。

【０２２７】

次に、認証サーバ選択部４０７は、認証サーバ３の候補群内の認証サーバ３において、

認証強度情報記憶領域４０６に記憶されている認証強度情報テーブル４０６ａから、認証強度が上述のようにして判定した不足している認証強度と一致し、かつ、保有属性情報が要求属性情報と一致するものだけを選択する。

【０２２８】

ここでは、不足している認証強度が「１」で、要求属性情報として「＊」が指定されているため、認証強度情報テーブル４０６ａ及び認証サーバ情報テーブル４０３ａにおいてこれらに適合するものとして、“ｉｄｐ００１”及び“ｉｄｐ００４”が候補群に残される。認証サーバ“ｉｄｐ００２”については認証強度が「２」であるため、候補群から削除される。

【０２２９】

次に、認証サーバ選択部４０７は、候補群に残った認証サーバ３の内、使用条件の値がステップＳ３３で取得したユーザのプレゼンス情報と一致するものだけを残し、一致しないものを候補群から削除する。ここでは、プレゼンス情報として「自宅」を特定する情報が得られているため、候補群の内、使用条件が「自宅」もしくは「＊」（使用条件を指定していないことを示す）に一致する“ｉｄｐ００１”が候補群に残される。

【０２３０】

次に、認証サーバ選択部４０７は、候補群の中で最も優先度が高い候補を残し、その他の候補を候補群から削除する。ここでは、候補が“ｉｄｐ００１”のみのため、候補群の絞り込みは行われない。

【０２３１】

次に、認証サーバ選択部４０７は、候補群内で最終認証時刻が最も古い候補を選択する。ここでは、候補が“ｉｄｐ００１”のみのため、候補群の絞り込みは行われない。

【０２３２】

この段階で候補として選択された認証サーバ３について、ユーザポリシ記憶領域４０２に記憶されているユーザポリシ情報テーブル４０２ａの最終認証時刻欄４０２ｄの値を、現在の時刻で置き換える。ここでは、“ｉｄｐ００１”の最終認証時刻欄が現在時刻で書き換えられる。

【０２３３】

以上で、ステップＳ１５の認証サーバ３の選択処理が終了する。

【０２３４】

次に、認証サーバ選択部４１３は、候補として選択された認証サーバ３Ａが提供する認証方式の提供ＵＲＩを提供認証強度情報記憶領域４０６に記憶されている提供認証強度情報テーブル４０６ａの提供ＵＲＩ欄４０６ｅより取得して、取得した提供ＵＲＩを特定する情報を含む応答メッセージ（情報取得要求メッセージに対する）を生成して、サービス提供サーバ２Ｂへ送信する（Ｓ３５）。ここでは、認証サーバＩＤ”ｉｄｐ００１”が提供するＩＤ／ＰＷ認証方式の提供ＵＲＩ“ｈｔｔｐｓ：／／ｉｄｐ００１／ｐａｓｓｗｄ／”が、サービス提供サーバ２Ｂへ送信される。

【０２３５】

サービス提供サーバ２Ｂは、認証仲介サーバ４から情報取得メッセージに対する応答メッセージを受信すると、認証サーバ情報取得部２０７が、受信した応答メッセージから提供ＵＲＩを取得して、認証要求処理部２０８が、提供ＵＲＩに対して端末装置１を介して認証要求メッセージを送信する（Ｓ３７、Ｓ３８）。

【０２３６】

認証サーバ３Ａは、認証実行部３０７が、ユーザが使用する端末装置１との間で認証処理を実行する（Ｓ３８）。ここでは、認証実行部３０７は、送受信部３１４及びネットワーク６を介して、端末装置１に対してユーザＩＤ及びパスワードを要求し、取得する。

【０２３７】

そして、認証実行部３０７は、取得したユーザＩＤをキーとして、ユーザ属性情報記憶領域３０３に記憶されているユーザ属性情報テーブル３０３ａを検索し、対応する属性欄３０３ｃに格納されているパスワードと、取得したパスワードと、が対応するか否かによ

り取得したユーザＩＤ及びパスワードの正当性を確認し（ここでは、ユーザＩＤ及びパスワードが正当なものであるとして説明する）、認証結果生成部３０８が、ユーザが認証に成功したことを示す認証結果メッセージを生成し、端末装置１を介して間接的に、サービス提供サーバ２Ｂに送信する（Ｓ３９、Ｓ４０）。

【０２３８】

サービス提供サーバ２Ｂでは、認証サーバ３Ａより認証結果メッセージを受信すると、認証要求処理部２０８が、受信した認証結果メッセージより認証結果を特定する情報を取得し、認証結果の正当性を確認する（Ｓ４１）。

【０２３９】

認証結果を検証した結果、ユーザの正当性が確認できると、認証サーバ情報取得部２０７が、前記提供ＵＲＩが提供している認証方式での認証が成功したことを伝える情報取得要求メッセージを生成し、送受信部２１３及びネットワーク６を介して、認証仲介サーバ４へ送信する（Ｓ４２）。

【０２４０】

そして、認証仲介サーバ４では、送受信部４２０及びネットワーク６を介して情報取得要求メッセージを受信すると、情報取得要求処理部４１２が、受信した情報取得要求メッセージに含まれるユーザＩＤ及びサービス提供サーバＩＤを取得し、認証サーバ３の候補を選択する処理に移る（Ｓ４３）。

【０２４１】

ここで、認証サーバ選択部４１３では、上述のステップＳ１５において、ユーザＩＤ“ｕｓｅｒ００１”で識別されるユーザの現在認証レベルが「４」に更新された結果、追加的な認証は不要であると判定し、提供ＵＲＩを含まず、ユーザＩＤ“ｕｓｅｒ００１”を含む応答メッセージを作成し、送受信部４２０及びネットワーク６を介して、サービス提供サーバ２Ｂへ送信する（Ｓ４４）。

【０２４２】

なお、ステップＳ４４で送信する応答メッセージには、ＩＤ情報記憶領域４０８に記憶されているＩＤ情報（サービス提供サーバ２Ｂに対するサービス固有ユーザＩＤ）と、属性情報記憶領域４０９に記憶されている属性情報（サービス提供サーバ２Ｂが要求する要求属性情報に対応するもの）を含める。

【０２４３】

サービス提供サーバ２Ｂでは、認証仲介サーバ４から応答メッセージを受信すると、認証要求処理部２０８が、当該応答メッセージからユーザＩＤを取得するとともに、セッション管理部２０６が新規にセッションＩＤを生成し、セッション情報記憶領域２０２に記憶されているセッション情報テーブル２０２ａに当該ユーザＩＤと当該セッションＩＤの組を格納して、サービス提供部２０５が端末装置１に対して要求されたサービスを提供する（Ｓ４５）。

【０２４４】

なお、サービス提供サーバ２Ｂでは、ステップＳ４４で送信されてきたＩＤ情報及び属性情報を、サービスを提供する際に使用することができる。

【０２４５】

図２３は、サービス提供サーバ２の処理を示すフローチャートである。

【０２４６】

まず、サービス提供サーバ２のサービス通信部２０９が、送受信部２１３及びネットワーク６を介して、端末装置１からサービス要求メッセージを受信すると（Ｓ５０でＹｅｓ）、セッション管理部２０６が、受信したサービス要求メッセージにセッションＩＤが含まれるか否かを確認する（Ｓ５１）。そして、セッションＩＤが含まれている場合には（Ｓ５１でＹｅｓ）ステップＳ５２に進み、セッションＩＤが含まれていない場合には（Ｓ５１でＮｏ）ステップＳ５３に進む。

【０２４７】

ステップＳ５２では、セッション管理部２０５が、セッション情報記憶領域２０２に記

憶されているセッション情報テーブル２０２ａに、ステップＳ５１で確認されたセッションＩＤに対応するレコードがあるか否かを確認する。このようなレコードがある場合には（Ｓ５２でＹｅｓ）ステップＳ６５に進み、このようなレコードがない場合には（Ｓ５２でＮｏ）ステップＳ５３に進む。

【０２４８】

ステップＳ６５では、セッション管理部２０６は、取得されたセッションＩＤに対応するセッションが有効であると判断して、サービス提供部２０４が、サービス要求メッセージの送信元である端末装置１に対してサービスを提供する。

【０２４９】

一方、ステップＳ５３では、セッション管理部２０６は、セッションが無効であると判断して、認証サーバ情報取得部２０７が、ステップＳ５０で受信したサービス要求メッセージに含まれるユーザＩＤと、自装置のサービス提供サーバＩＤと、を特定した情報取得メッセージを作成する。

【０２５０】

そして、認証サーバ情報取得部２０７は、作成した情報取得メッセージを、認証仲介サーバ４へ送信し（Ｓ５４）、応答を待ち受ける（Ｓ５５）。

【０２５１】

認証仲介サーバ４から情報取得メッセージに対する応答を受信すると（Ｓ５５でＹｅｓ）、認証サーバ情報取得部２０７が、受信した応答メッセージに提供ＵＲＩが含まれているか否かを確認する（Ｓ５６）。そして、受信した応答メッセージに提供ＵＲＩが含まれている場合には（Ｓ５６でＹｅｓ）ステップＳ５７に進み、受信した応答メッセージに提供ＵＲＩが含まれていない場合には（Ｓ５６でＮｏ）ステップＳ６３に進む。

【０２５２】

ステップＳ５７では、認証要求処理部２０８は、さらなる認証が必要であると判断して、ステップＳ５６で確認された提供ＵＲＩで特定される認証サーバ３に対して、端末装置１を介して認証要求メッセージを送信し（Ｓ５７）、応答を待ち受ける（Ｓ５８）。

【０２５３】

認証サーバ３から認証要求メッセージに対する応答メッセージを受信すると（Ｓ５８でＹｅｓ）、認証要求処理部２０８は、受信した応答メッセージから認証結果を特定する情報を取得し（Ｓ５９）、認証結果の正当性を確認する（Ｓ６０）。

【０２５４】

認証結果を検証した結果、ユーザの正当性を確認できた場合（Ｓ６０のＹｅｓ）には、ユーザの正当性が確認できたことを認証仲介サーバ４に通知するため、ステップＳ５６で確認した提供ＵＲＩと、認証成功を意味する情報と、ステップＳ５９で取得した認証結果に含まれるユーザの属性情報と、を含む情報取得メッセージを作成し（ステップＳ６１）、ステップＳ５４に戻り、処理を繰り返す。

【０２５５】

一方、認証結果を検証した結果、ユーザの正当性が確認できなかった場合（Ｓ６０でＮｏ）、ユーザの正当性が確認できなかったことを認証仲介サーバ４に通知するため、ステップＳ５６で確認した提供ＵＲＩと、認証失敗を意味する情報と、を含む情報取得メッセージを作成し（Ｓ６２）、ステップＳ５４に戻り、処理を繰り返す。

【０２５６】

また、ステップＳ５６で提供ＵＲＩが含まれていない場合には、認証サーバ情報取得部２０７は、ステップＳ５５で受信した応答メッセージがエラーメッセージであるか否かを確認する（Ｓ６３）。ステップＳ５５で受信した応答メッセージがエラーメッセージである場合には（Ｓ６３でＹｅｓ）、端末装置１にサービスを提供することなく処理を終了し、ステップＳ５５で受信した応答メッセージがエラーメッセージではない場合には（Ｓ６３でＮｏ）、ステップＳ６４に進む。

【０２５７】

ステップＳ６４では、認証サーバ情報取得部２０７は、さらなる認証は不要であると判

断して、認証要求処理部２０８が、情報取得メッセージに対する応答メッセージからサービス提供サーバ２におけるユーザの識別情報（サービス固有ユーザＩＤ）と、属性情報と、を取得するとともに、セッション管理部２０６が新規にセッションＩＤを生成し、セッション情報記憶領域２０２に記憶されているセッション情報テーブル２０２ａに、当該識別情報（ユーザＩＤ）と、当該セッションＩＤと、の組を格納する。

【０２５８】

そして、サービス提供部２０５が端末装置１に対してサービスを提供する（Ｓ６５）。ここで、サービス提供部２０５は、サービスを提供する際に、ステップＳ６４において、取得したユーザの識別情報（サービス固有ユーザＩＤ）及び属性情報を使用してサービスを提供することができる。

【０２５９】

図２４は、認証サーバ３の処理を示すフローチャートである。

【０２６０】

まず、認証サーバ３では、送受信部３１４及びネットワーク６を介してユーザ認証要求メッセージを受信すると（Ｓ７０でＹｅｓ）、セッション管理部３０８が、受信したユーザ認証要求メッセージにセッションＩＤが含まれるか否かを確認する（Ｓ７１）。そして、セッションＩＤが含まれる場合には（ステップＳ７１でＹｅｓ）ステップＳ７２に進み、セッションＩＤが含まれない場合には（ステップＳ７１でＮｏ）ステップＳ７３に進む。

【０２６１】

ステップＳ７２では、セッション管理部３０８は、セッション情報記憶領域３０２に記憶されているセッション情報テーブル３０２ａに、ステップＳ７１で確認されたセッションＩＤに対応するレコードがあるか否かを確認することで、セッションが有効か否かを判断する。

【０２６２】

そして、セッション管理部３０８は、ユーザ認証要求メッセージに含まれるセッションＩＤに関連付けられる接続先ＩＤをセッション情報テーブル３０２ａより取得できた場合には、セッションが有効であると判断し(Ｓ７２でＹｅｓ）ステップＳ７６に進み、ユーザ認証要求メッセージに含まれるセッションＩＤに関連付けられる接続先ＩＤをセッション情報テーブル３０２ａより取得できなかった場合には、セッションが無効であると判断し(Ｓ７２でＮｏ）ステップＳ７３に進む。

【０２６３】

ステップＳ７３では、認証実行部３０７が、端末装置１に対して認証処理を実行する。例えば、認証実行部３０７は、端末装置１に対してユーザＩＤとパスワードの組を要求し、ユーザ属性情報記憶領域３０３に記憶されているユーザ属性情報テーブル３０３ａに格納されたユーザＩＤ及びパスワードと比較することで、ユーザの本人性（正当性）を確認することができる。

【０２６４】

また、別の例として、認証実行部３０７は、端末装置１へ乱数列を送信し、当該端末装置１から返却された情報が、端末装置１の保有する秘密鍵で計算されたものであることを、ユーザ属性記憶領域３０３に格納された端末装置１の電子証明書（公開鍵）を用いて検証することで、ユーザ認証を実現してもよい。

【０２６５】

次に、認証実行部３０７は、ステップＳ７３での認証処理で、認証が成功したか否かを確認する（Ｓ７４）。そして、認証が成功した場合には（ステップＳ７４でＹｅｓ）ステップＳ７５に進み、認証が失敗した場合には（ステップＳ７４でＮｏ）ステップＳ７７に進む。

【０２６６】

ステップＳ７５では、セッション管理部３０９が、新規にセッションＩＤを生成し、セッション情報記憶領域３０２に記憶されているセッション情報テーブル３０２ａに、ステ

ップＳ７３の認証の結果得られたユーザＩＤと、生成したセッションＩＤと、の組を格納する（Ｓ７５）。

【０２６７】

そして、ステップＳ７６では、認証結果生成部３０８が、ユーザの認証が成功したことを示す認証結果メッセージを生成し、送受信部３１４及びネットワーク６を介して、生成した認証結果メッセージを、端末装置１を経由して間接的に、ユーザ認証要求メッセージの送信元であるサービス提供サーバ２へ送信する。ここで送信される認証結果メッセージには、セッションＩＤに関連付けられる接続先ＩＤがユーザＩＤとして格納される。また、当該認証結果メッセージには、当該認証サーバ３で管理している、前記ユーザＩＤで識別されるユーザの属性情報が含まれる。

【０２６８】

一方、ステップＳ７７では、認証結果生成部３０８が、ユーザ認証が失敗に終わったことを示す認証結果メッセージを生成し、送受信部３１４及びネットワーク６を介して、当該認証結果メッセージを、端末装置１を経由して間接的に、ユーザ認証要求メッセージの送信元であるサービス提供サーバ２へ送信する。

【０２６９】

上記の処理においては、認証を行う前（Ｓ７３の前）か、もしくは認証結果を送信する前（Ｓ７６の前）に、端末装置１に対して、サービス提供サーバ２へ認証結果を送信することを通知する旨を通知してもよい。

【０２７０】

図２５は、端末装置１の処理を示すフローチャートである。

【０２７１】

まず、端末装置１のサービス利用部１０６が、入力部１１５を介して、ユーザからサービス提供サーバ２に対するサービスの利用要求を受け付けると（Ｓ８０でＹｅｓ）、サービス要求生成部１０７が、ユーザＩＤを特定したサービス要求メッセージを生成し、サービス通信部１０８が、送受信部１１７及びネットワーク６を介して、生成したサービス要求メッセージをサービス提供サーバ２へ送信し（Ｓ８１）、応答を待ち受ける（Ｓ８２）。ここで、サービス要求メッセージには、ユーザが利用を希望する認証仲介サーバ４のＩＤを含めても良い。

【０２７２】

サービス提供サーバ２から、サービス利用要求メッセージに対する応答メッセージを受信すると（Ｓ８２でＹｅｓ）、サービス通信部１０８は、当該応答メッセージの内容を確認し、当該応答メッセージが、認証仲介サーバ４に対して転送されるべき情報取得メッセージであるか否かを確認する（Ｓ８３）。ここで、非特許文献２に記載されるＳＡＭＬ Ｗｅｂ ＳＳＯ Ｐｒｏｆｉｌｅや、非特許文献３に記載されるＯｐｅｎＩＤ Ａｕｔｈｅｎｔｉｃａｔｉｏｎのように、端末装置１と、サービス提供サーバ２と、認証仲介サーバ４と、がＨＴＴＰまたはＨＴＴＰＳを用いて通信可能である場合には、ＨＴＴＰリダイレクトの機能を利用し、当該応答メッセージが情報取得メッセージであるかを判定することなく、応答メッセージ内のＬｏｃａｔｉｏｎヘッダで示されるＵＲＬへＨＴＴＰリクエストを送信するだけで良い。この場合、当該応答メッセージが情報取得メッセージであるか否かは、当該Ｌｏｃａｔｉｏｎヘッダで示されるＵＲＬが認証仲介サーバのＵＲＬに等しいか否か、と等価であると考えられる。

【０２７３】

そして、ステップＳ８２で取得した応答メッセージが情報取得メッセージでなかった場合には（Ｓ８３でＮｏ）ステップＳ８９に進む。一方、当該応答メッセージが情報取得メッセージであった場合には（Ｓ８３のＹｅｓ）、ステップＳ８４に進む。

【０２７４】

ステップＳ８４では、サービス通信部１０８は、当該応答メッセージ（情報取得メッセージ）を認証仲介サーバ４へ転送し（Ｓ８４）、応答を待ち受ける（Ｓ８５）。

【０２７５】

そして、サービス通信部１０８は、認証仲介サーバ４から応答メッセージを受信すると（Ｓ８５でＹｅｓ）、当該応答メッセージをサービス提供サーバへ転送する（Ｓ８６）。

【０２７６】

そして、サービス通信部１０８は、ステップＳ８６で転送した応答メッセージがエラーメッセージであった場合には（Ｓ８７でＹｅｓ）処理を終了し、エラーメッセージでなかった場合には（Ｓ８７でＮｏ）、ステップＳ８６で転送したメッセージへの応答を待ち受ける（Ｓ８８）。

【０２７７】

そして、サービス提供サーバ２から応答を受信すると（Ｓ８８でＹｅｓ）、ステップＳ８９に進む。

【０２７８】

ステップＳ８９では、サービス通信部１０８は、応答メッセージが認証サーバ３に対して転送されるべき認証要求メッセージであるか否かを確認する。ここで、非特許文献２に記載されるＳＡＭＬ Ｗｅｂ ＳＳＯ Ｐｒｏｆｉｌｅや、非特許文献３に記載されるＯｐｅｎＩＤ Ａｕｔｈｅｎｔｉｃａｔｉｏｎのように、端末装置１と、サービス提供サーバ２と、認証サーバ３と、がＨＴＴＰまたはＨＴＴＰＳを用いて通信可能である場合には、ＨＴＴＰリダイレクトの機能を利用し、当該応答メッセージが認証要求メッセージであるかを判定することなく、応答メッセージ内のＬｏｃａｔｉｏｎヘッダで示されるＵＲＬへＨＴＴＰリクエストを送信するだけで良い。この場合、当該応答メッセージが認証要求メッセージであるか否かは、当該Ｌｏｃａｔｉｏｎヘッダで示されるＵＲＬが認証サーバのＵＲＬに等しいか否か、と等価であると考えられる。

【０２７９】

応答メッセージが認証要求メッセージでなかった場合には（Ｓ８９でＮｏ）、サービス提供サーバ２からのサービスを享受する（Ｓ９０）。なお、サービス提供サーバ２からサービスの提供を受ける際に必要とされる情報（サービス固有ユーザＩＤや属性情報）は、認証仲介サーバ４に登録しておくことで、サービスの提供を受ける際に追加して取得を要求されることがないようにすることができる。

【０２８０】

一方、応答メッセージが認証要求メッセージであった場合には（Ｓ８９でＹｅｓ）当該応答メッセージ（認証要求メッセージ）を認証サーバ３へ転送する（Ｓ９１）。

【０２８１】

そして、認証サーバ３から認証処理の実行を要求されると認証処理部１０９が、入力部１１５及び出力部１１６を適宜利用して、対応する認証処理を実行する（Ｓ９２）。例えば、認証サーバ３からユーザＩＤとパスワードの組を要求された場合は、認証処理部１０９がユーザに対してユーザＩＤとパスワードの組を入力するよう要求し、取得したユーザＩＤとパスワードの組を、送受信部１１７及びネットワーク６を介して認証サーバ３へ送信する。

【０２８２】

そして、認証処理部１０９は、ステップＳ９２での認証処理が成功したか否かを判断し（Ｓ９３）、成功しなかった場合には（Ｓ９３でＮｏ）、すなわち、認証サーバ３に対してユーザの本人性を証明できなかった場合には、サービス利用部１０６が、出力部１１６にユーザに対して認証に失敗したことを示すエラーメッセージを表示し（Ｓ９４）、サービスを享受することなく、処理を終了する。

【０２８３】

一方、認証処理に成功した場合には（Ｓ９３でＹｅｓ）、すなわち、認証サーバ３に対してユーザの本人性を証明できた場合には、セッション管理部１１０が、認証サーバ３から応答として返される認証結果メッセージに含まれるセッションＩＤを、認証サーバ３のＩＤと関連付け、セッション情報記憶領域１０２に記憶されているセッション情報テーブル１０２ａに格納する（Ｓ９５）。

【０２８４】

そして、認証処理部１０９は、認証サーバ３から応答として返された認証結果メッセージを、サービス提供サーバ２へ転送し（Ｓ９６）、ステップＳ８２に戻り、処理を繰り返す。

【０２８５】

図２６は、認証仲介サーバ４の処理を示すフローチャートである。

【０２８６】

まず、認証仲介サーバ４が、送受信部４２０及びネットワーク６を介して情報取得要求メッセージを受信すると（Ｓ１００でＹｅｓ）、情報取得要求処理部４１２が、取得した情報取得要求メッセージに含まれるユーザＩＤ及びサービス提供サーバＩＤを取得する（Ｓ１０１）。ここで、ユーザＩＤについては、必ずしも情報取得要求メッセージのパラメータとして含まれている必要はなく、非特許文献３におけるＯｐｅｎＩＤのように、当該メッセージを受信した認証仲介サーバのＵＲＬをユーザＩＤとして利用しても良いし、端末装置１に対して入力を要求しても良い。

【０２８７】

次に、ユーザ情報取得部４１５が、ステップＳ１０１で取得したユーザＩＤを特定したユーザ情報取得要求を、送受信部２１１及びネットワーク６を介して、プレゼンスサーバ５に送信することで、プレゼンスサーバ５より、当該ユーザＩＤで特定されるユーザのプレゼンス情報を取得する（Ｓ１０２）。なお、ネットワーク６上に、プレゼンスに類するユーザの情報を管理するサーバが存在する場合には、当該サーバからユーザ情報を取得するようにしてもよい。

【０２８８】

次に、認証サーバ選択部４１３が、ステップＳ１０１で取得したユーザＩＤをキーとして、ユーザポリシ情報記憶領域４０２に記憶されているユーザポリシ情報テーブル４０２ａから、当該ユーザＩＤによって特定されるユーザのポリシ情報（認証サーバＩＤ、最終認証時刻、優先度、使用条件、サービス提供サーバＩＤ条件）のレコードの集合を取得し、当該ポリシ情報の集合を、認証サーバ３の候補群として記憶部４０１に記憶する（Ｓ１０３）。

【０２８９】

次に、認証サーバ選択部４１３は、ステップＳ１０１で取得したサービス提供サーバＩＤをキーとして、サービス提供サーバ要求情報記憶領域４０４に記憶されているサービス提供サーバ要求情報テーブル４０４ａを検索し、当該サービス提供サーバＩＤによって特定されるサービス提供サーバ要求情報（連携認証サーバＩＤ、要求認証レベル、要求属性情報）のレコードを取得する（Ｓ１０４）。

【０２９０】

次に、認証サーバ選択部４１３は、ステップＳ１００で受信した情報提供要求メッセージに提供ＵＲＩが含まれているかどうかを確認する（Ｓ１０５）。そして、情報提供要求メッセージに提供ＵＲＩが含まれている場合には（Ｓ１０５でＹｅｓ）、ステップＳ１０６に進み、情報提供要求メッセージに提供ＵＲＩが含まれていない場合には（Ｓ１０５でＮｏ）、ステップＳ１１０に進む。

【０２９１】

ステップＳ１０６では、認証サーバ選択部４１３は、情報提供要求メッセージに認証成功を意味する情報が含まれているか否かを確認する。そして、情報提供要求メッセージに認証成功を意味する情報が含まれている場合には（ステップＳ１０６でＹｅｓ）ステップ１０７に進み、情報提供要求メッセージに認証成功を意味する情報が含まれていない場合には（ステップＳ１０６でＮｏ）ステップＳ１０９に進む。

【０２９２】

ステップＳ１０７では、認証サーバ選択部４１３は、認証レベル情報記憶領域４０５の認証レベル情報テーブル４０５ａを更新する。すなわち、ステップＳ１０１で取得したユーザＩＤをキーとして認証レベル情報テーブル４０５ａを検索し、当該ユーザＩＤによって特定されるレコードの認証レベルを取得し、ステップＳ１０５で確認した提供ＵＲＩを

キーとして提供認証強度情報記憶領域４０６に記憶されている提供認証強度情報テーブル４０６ａから当該提供ＵＲＩが提供している認証方式の認証強度を取得し、認証レベル定義情報記憶領域４０７に記憶されている認証レベル定義情報テーブル４０７ａの定義を参照して新しい認証レベルを特定し、認証レベル情報テーブル４０５ａのステップＳ１０１で取得したユーザＩＤに対応する認証レベル欄４０５ｃを更新する。

【０２９３】

次に、アイデンティティ変換部４１６が、属性情報記憶領域４０９に記憶されている属性情報テーブル４０９ａを更新する（Ｓ１０８）。すなわち、ステップ１００で取得した情報提供要求メッセージに含まれている属性値をステップＳ１０１で取得したユーザＩＤをキーとして属性情報テーブル４０９ａを検索し、当該ユーザＩＤによって特定されるユーザの属性値として格納する。

【０２９４】

ステップＳ１０９では、認証サーバ選択部４１３は、ステップＳ１０３で記憶した認証サーバ３の候補群から、ステップ１０５で確認された提供ＵＲＩに対応する認証サーバ３を削除する。

【０２９５】

ステップＳ１１０では、認証サーバ選択部４１３は、追加的な認証が必要か否かを判断する（Ｓ４１０）。まず、認証サーバ選択部４１３は、ステップＳ１０１で取得したユーザＩＤをキーとして認証レベル情報テーブル４０５ａから当該ユーザＩＤによって特定されるユーザの現在認証レベルを取得する。次に、取得した現在認証レベルと、ステップＳ１０４で取得したサービス提供サーバ要求情報に含まれる要求認証レベルと、を比較し、認証強度が不足しているかどうかを確認する。

【０２９６】

ここで、認証強度が不足していない場合には、ステップＳ１１０において追加的な認証が必要ではないと判断し（ステップＳ１１０でＮｏ）、ステップＳ１１１に進む。一方、認証強度が不足している場合には、ステップＳ１１０において追加的な認証が必要と判断し（ステップＳ１１０でＹｅｓ）、ステップＳ１１２に進む。

【０２９７】

ステップＳ１１１では、アイデンティティ変換部４１６が、ステップＳ１０１で取得したユーザＩＤ及びサービス提供サーバＩＤをキーとしてＩＤ情報記憶領域４０８に記憶されているＩＤ情報テーブル４０８ａを検索し、当該サービス提供サーバＩＤで特定されるサービス提供サーバ２において、当該ユーザＩＤで特定されるユーザが使用しているユーザの識別情報（サービス固有ユーザＩＤ）を取得する。そして、アイデンティティ変換部４１６は、Ｓ１０１で取得したサービス提供サーバＩＤをキーとしてサービス提供サーバ要求情報テーブル４０４ａを検索し、当該サービス提供サーバＩＤで特定されるサービス提供サーバ２が必要とする要求属性情報を取得する。続いて、アイデンティティ変換部４１６は、取得した要求属性情報と、Ｓ１０１で取得したユーザＩＤと、をキーとして、属性情報テーブル４０９ａを検索し、当該ユーザＩＤで特定されるユーザの属性情報を取得する。さらに、アイデンティティ変換部４１６は、取得したサービス固有ユーザ情報と、属性情報と、を含む情報取得応答メッセージを作成すると、認証サーバ選択部４１３がサービス提供サーバ２へ直接、もしくは端末装置１を介して間接的に情報取得応答メッセージを送信し、処理を終了する。

【０２９８】

一方、ステップＳ１１２では、認証サーバ選択部４１３は、認証サーバ３の候補群を絞り込む処理を行う。

【０２９９】

まず、認証サーバ選択部４１３は、ステップＳ１０３で記憶した認証サーバ３の候補群から、認証サーバＩＤが連携認証サーバＩＤ（ステップＳ１０４でサービス提供サーバ２の情報として取得したもの）と一致するものだけを残し、一致しないものを候補群から削除する。当該連携認証サーバＩＤの値が「＊」であった場合には、候補群内の全ての認証

サーバが候補として残される。

【０３００】

続いて、認証サーバ選択部４１３は、認証サーバ３の候補群から、サービス提供サーバＩＤ条件の値が、情報取得要求メッセージの送信元であるサービス提供サーバ２のサービス提供サーバＩＤを含むものだけを選択し、それ以外のものを候補群から削除する。当該サービス提供サーバＩＤ条件の値が「＊」であった場合には、候補群内の全ての認証サーバが候補として残される。

【０３０１】

さらに、認証サーバ選択部４１３は、認証サーバの候補群に残った候補のそれぞれについて、認証サーバ情報記憶領域４０３に記憶されている認証サーバ情報テーブル４０３ａから、認証サーバ情報（対応認証方式、保有属性情報）を取得し、記憶部４０１内の候補群に追加する。

【０３０２】

そして、認証サーバ選択部４１３は、認証サーバ３の候補群に残った候補のそれぞれについて、記憶部４０１内の提供認証強度情報テーブル４０６ａから、それぞれの候補に対応する認証強度、提供ＵＲＩを取得し、記憶部４０１内の候補群に追加する。

【０３０３】

次に、認証サーバ選択部４１３は、候補群内の認証サーバ３の内、不足している認証強度（ステップＳ１１０で特定したもの）を提供する認証方式を含み、かつ保有属性情報が要求属性情報（ステップＳ１０４でサービス提供サーバ要求情報として取得したもの）を含むものだけを残し、一致しないものを候補群から削除する。同様に、要求属性情報の値が「＊」であった場合には、保有属性情報の値は候補群の絞り込みに影響を与えない。

【０３０４】

次に、認証サーバ選択部４１３は、候補群内の認証サーバの内、使用条件の値が、ステップＳ１０２で取得したプレゼンス情報に合致するものだけを残し、そうでないものを候補群から削除する。当該使用条件の値が「＊」であった場合には、候補群内の全ての認証サーバが候補として残される。

【０３０５】

そして、認証サーバ選択部４１３は、候補群内に認証サーバの候補が残されているか否かを確認する（Ｓ１１３）。そして、候補が残されていない場合には（ステップＳ１１２でＮｏ）ステップＳ１１４に進み、候補が残されている場合には（ステップＳ１１２でＹｅｓ）ステップＳ１１５に進む。

【０３０６】

ステップＳ１１４では、認証サーバ選択部４１３は、使用できる認証サーバ３が存在しなかったことを示すエラーメッセージをサービス提供サーバ２へ直接、もしくは端末装置１を介して間接的に送信し、処理を終了する。

【０３０７】

一方、ステップＳ１１５では、認証サーバ選択部４１３は、候補群内に残っている認証サーバ３の中で最も優先度が高い候補を選択する。

【０３０８】

次に、認証サーバ選択部４１３は、ステップＳ１１５で選択した認証サーバ３が複数あるか否かを確認し（Ｓ１１６）、複数ある場合には（ステップＳ１１６でＹｅｓ）ステップＳ１１７に進み、複数ない場合には（ステップＳ１１６でＮｏ）ステップＳ１１８に進む。

【０３０９】

ステップＳ１１７では、認証サーバ選択部４１３は、候補群内で最終認証時刻が最も古い候補を選択する。

【０３１０】

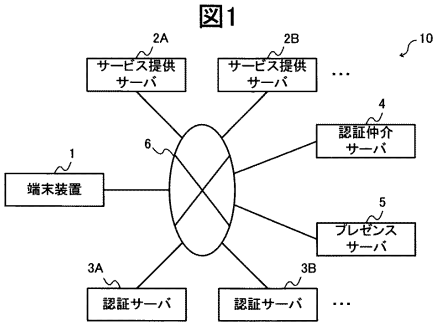
そして、ユーザポリシ管理部４１４は、選択された認証サーバ３について、ユーザポリシ情報記憶領域４０２に記憶されているユーザポリシ情報テーブル４０２ａの最終認証時

刻欄４０２ｄの値を、現在の時刻で置き換える（Ｓ１１８）。
【０３１１】
そして、認証サーバ選択部４１３は、候補として選択された認証サーバ３のＩＤを、サービス提供サーバへ直接、もしくは端末装置１を介して間接的に送信し（Ｓ１１９）、処理を終了する。
【０３１２】
以上に記載したように、本発明によれば、ユーザは端末装置１に同一のユーザＩＤを入力するだけで、ユーザのポリシと、サービス提供サーバ２の要求認証方式および要求属性情報と、ユーザのプレゼンス情報と、に基づいて、最適な認証サーバ３が動的に選択され、認証に利用される。
【０３１３】
また、最終的に認証サーバ３の候補を絞り込む際、認証サーバ３が最後に利用された時刻を元に絞り込みを行うため、同じ認証サーバ３が連続して使用される可能性が低減される。これにより、同一認証サーバ３を連続して使用する場合に比較して、認証サーバ３によるユーザのサービス利用履歴の追跡が困難となる。
【０３１４】
以上に記載した実施形態においては、図２１のステップＳ１５、図２２のステップＳ３４、および、図２６のステップＳ１１２～Ｓ１１７に記載されているように、認証サーバ３を選択する際に、サービス提供サーバ２が連携している認証サーバであること、ユーザが特定のサービス提供サーバ２で処理を受ける際に選択することを特定している認証サーバ３であること、サービス提供サーバ２が要求する認証レベルを満たすために必要な認証方式を提供している認証サーバ３であること、サービス提供サーバ２が要求するユーザの属性情報を保有する認証サーバ３であること、ユーザのプレゼンス情報で選択される認証サーバ３であること、ユーザが定める優先度の高いものから選択された認証サーバ３であること、最終認証時刻が古いものから選択された認証サーバ３であること、の条件を満たすように選択されるようになっているが、このような態様に限定されず、これらの条件のうちの少なくとも一つ以上、これらの条件のうちの任意の組合せ、を満たすものを選択するようにすることも可能である。
【０３１５】
以上に記載した実施形態においては、図１４に示すように、認証レベル情報テーブル４０５ａにおいて、ユーザＩＤと、当該ユーザＩＤで特定されるユーザが既に認証を受けた最新の認証レベル（現在認証レベル）と、特定する情報が格納されているが、このような態様に限定されず、例えば、当該ユーザＩＤで特定されるユーザが、現在認証レベルにおいて、認証を受けた認証方式の認証強度と、当該認証強度を有する認証方式による認証を受けた回数と、を特定する情報も格納するようにしてもよい。これらの情報を格納しておくことで、特定の認証強度を有する認証方式による認証を、特に三回以上受けなければならないような場合でも、強度不足を判定可能となる。
【０３１６】
以上に記載した実施形態においては、認証仲介サーバ４と、プレゼンスサーバ５と、が別々の装置として記載されているが、このような態様に限定されず、これらの装置が行っている処理を一つの装置にまとめることも可能である。
【図面の簡単な説明】
【０３１７】
【図１】認証システムの概略図。
【図２】端末装置の一例を示す概略図。
【図３】セッション情報テーブルの概略図。
【図４】コンピュータの概略図。
【図５】サービス提供サーバの一例を示す概略図。
【図６】セッション情報テーブルの概略図。
【図７】認証サーバの一例を示す概略図。

【図８】セッション情報テーブルの概略図。
【図９】ユーザ属性情報テーブルの概略図。
【図１０】認証仲介サーバの構成の一例を示す概略図。
【図１１】ユーザポリシ情報テーブルの概略図。
【図１２】認証サーバ情報テーブルの概略図。
【図１３】サービス提供サーバ要求情報テーブルの概略図。
【図１４】認証レベル情報テーブルの概略図。
【図１５】提供認証強度情報テーブルの概略図。
【図１６】認証レベル定義情報テーブルの概略図。
【図１７】ＩＤ情報テーブルの概略図。
【図１８】属性情報テーブルの概略図。
【図１９】プレゼンスサーバの構成の一例を示す概略図。
【図２０】プレゼンス情報テーブルの概略図。
【図２１】認証システムで認証を行う際の処理の一例を示すシーケンス。
【図２２】認証システムで認証を行う際の処理の一例を示すシーケンス。
【図２３】サービス提供サーバの処理を示すフローチャート。
【図２４】認証サーバの処理を示すフローチャート。
【図２５】端末装置の処理を示すフローチャート。
【図２６】認証仲介サーバの処理を示すフローチャート。
【符号の説明】
【０３１８】
１０　認証システム
１　端末装置
１０１　記憶部
１０５　制御部
２　サービス提供サーバ
２０１　記憶部
２０４　制御部
３　認証サーバ
３０１　記憶部
３０５　制御部
４　認証仲介サーバ
４０１　記憶部
４０２　ユーザポリシ情報記憶領域
４０３　認証サーバ情報記憶領域
４０４　サービス提供サーバ要求情報記憶領域
４０５　認証レベル情報記憶領域
４０６　提供認証強度情報記憶領域
４０７　認証レベル定義情報記憶領域
４０８　ＩＤ情報記憶領域
４０９　属性情報記憶領域
４１１　制御部
４１２　情報取得要求処理部
４１３　認証サーバ選択部
４１４　ユーザポリシ管理部
４１５　ユーザ情報取得部
４１６　アイデンティティ変換部
５　プレゼンスサーバ
５０１　記憶部
５０４　制御部

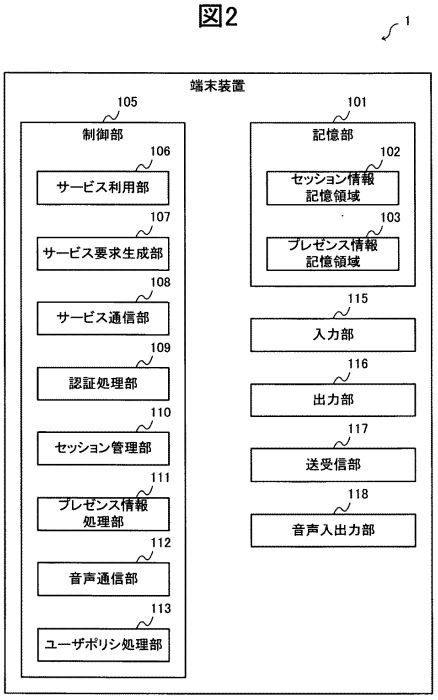
【図１】

図1



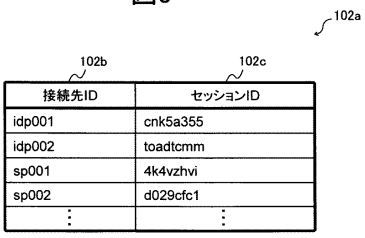
【図２】

図2



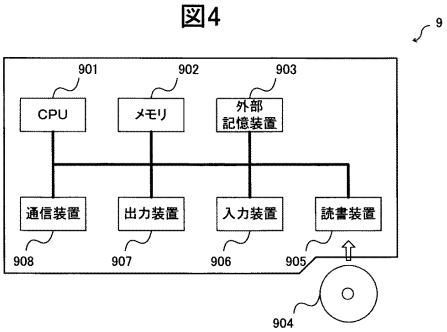
【図３】

図3



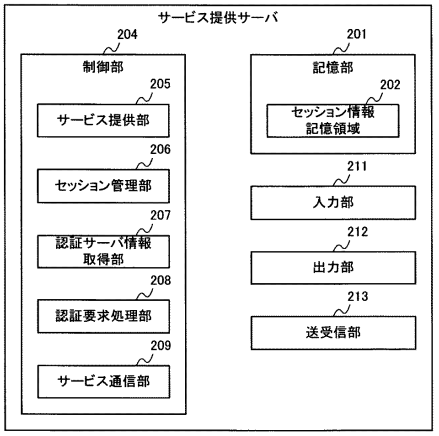
【図４】

図4



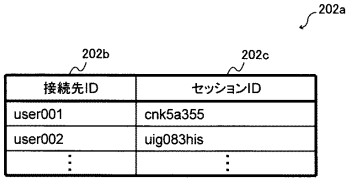
【図５】

図5



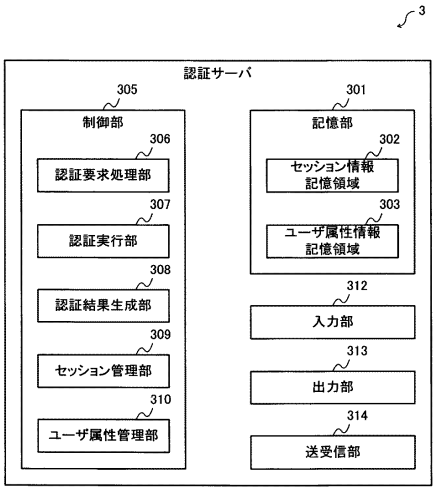
【図６】

図6



【図７】

図7



【図８】

図8

302a

302b 接続先ID	302c セッションID
user001	cnk5a355
user002	uig083his
⋮	⋮

【図９】

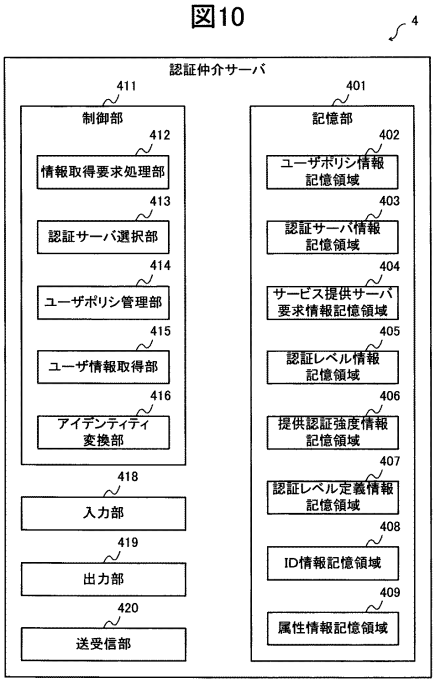
図9

303a

303b ユーザID	303c 属性
user001	AAAA
user002	BBBB
user003	CCCC
⋮	⋮

【図１０】

図10



【図１１】

図11

402a

402b ユーザID	402c 認証サーバID	402d 最終認証時刻	402e 優先度	402f 使用条件	402g サービス提供サーバID条件
user001	idp001	2008-08-19T10:03:28	10	*	*
	idp002	2008-07-30T17:32:15	10	自宅	sp001, sp002
	idp003	2008-08-01T01:17:04	10	職場	sp001
	idp004	2008-07-15T09:29:30	30	職場	*
user002	idp001	2008-08-03T12:22:57	10	*	*
	idp005	2008-08-04T15:10:31	10	*	*
	idp006	2008-08-01T02:11:01	10	*	*
…	…	…	…	…	…

【図１２】

図12

403a

403b 認証サーバID	403c 対応認証方式	403d 保有属性情報
idp001	ID/PW型認証方式、 電子証明書型認証方式	氏名、住所、メールアドレス、 クレジットカード番号
idp002	電子証明書型認証方式	メールアドレス
idp003	電子証明書型認証方式	クレジットカード番号
idp004	ID/PW型認証方式	なし
⋮	⋮	⋮

【図１３】

図13

404a

404b サービス提供サーバID	404c 連携認証サーバID	404d 要求認証レベル	404e 要求属性情報
sp001	*	2	メールアドレス
sp002	*	4	*
sp003	idp003, idp004	3	クレジットカード番号
⋮	⋮	⋮	⋮

【図１４】

図14

405a

405b ユーザID	405c 現在認証レベル
user001	1
user002	2
⋮	⋮

【図１５】

図15

406a

406b 認証サーバID	406c 提供認証方式	406d 認証強度	406e 提供URI
idp001	ID/PW型認証方式	1	http://idp001/passwd/
	電子証明書型認証方式	2	https://idp002/pkc/
idp002	電子証明書型認証方式	2	https://idp002/
idp003	電子証明書型認証方式	2	https://idp003/
idp004	ID/PW型認証方式	1	http://idp004/
⋮	⋮	⋮	⋮

【図１６】

図16

407a

407b 認証レベル	407c 定義
0	認証なし
1	認証強度が1の認証方式で1回認証を受ける
2	認証強度が2の認証方式で1回認証を受ける
3	認証レベル1の認証を2回以上組み合わせて認証を受ける
4	認証レベル1の認証と認証レベル2の認証をそれぞれ1回以上組み合わせて認証を受ける

【図１７】

図17

408a

408b ユーザID	408c サーバID	408d サービス固有ユーザID
user001	sp001	user001@hitachi.com
user001	sp003	Usr.001@sp003
user002	sp001	user002@hitachi.com
user002	sp002	user002
⋮	⋮	⋮

【図１８】

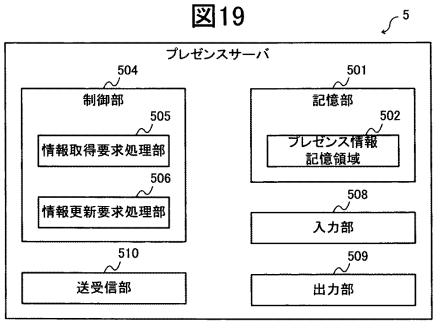
図18

409a

409b ユーザID	409c 属性型	409d 属性値
user001	メールアドレス	user001@hitachi.com
user001	クレジットカード番号	0000-0000-0000-0000
user001	氏名	Hitachi Taro
user002	メールアドレス	user002@hitachi.com
⋮	⋮	⋮

【図１９】

図19



【図２０】

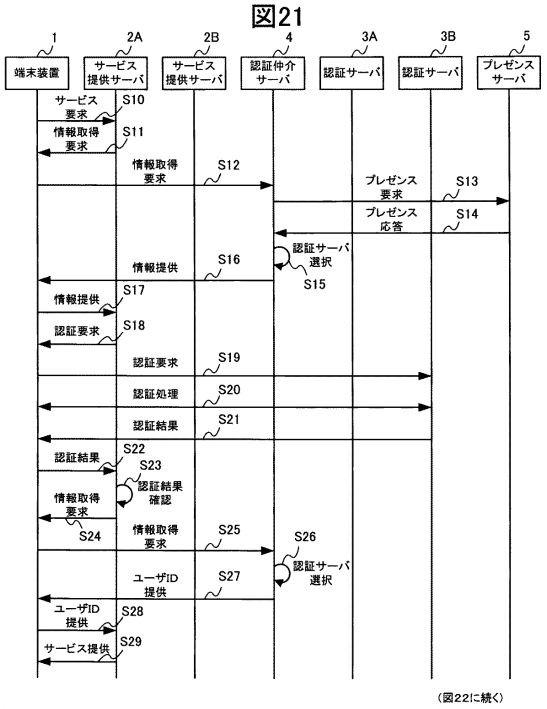
図20

502a

502b ユーザID	502c プレゼンス
user001	自宅
user002	職場
user003	職場、通話中
⋮	⋮

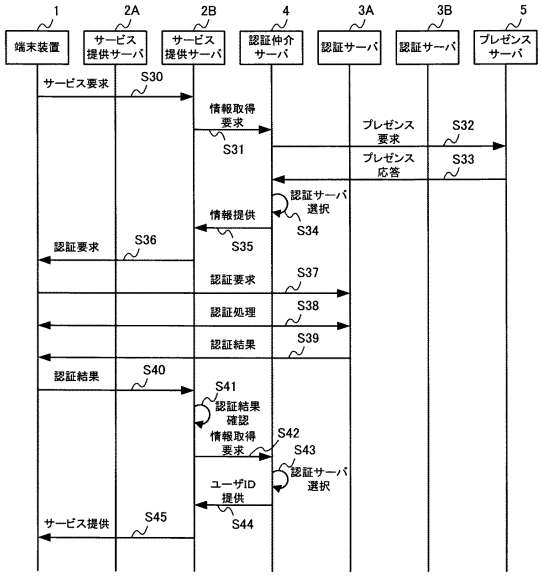
【図２１】

図21



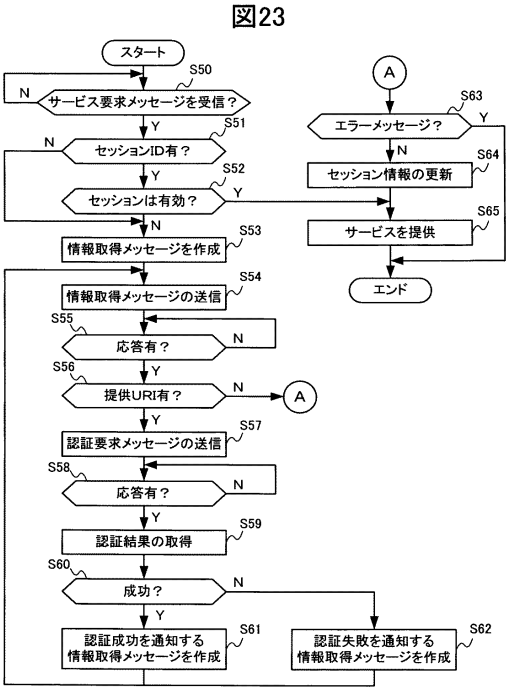
【図２２】

図22



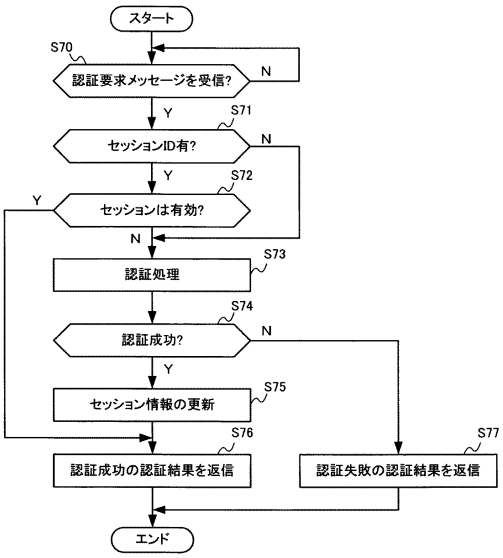
【図２３】

図23



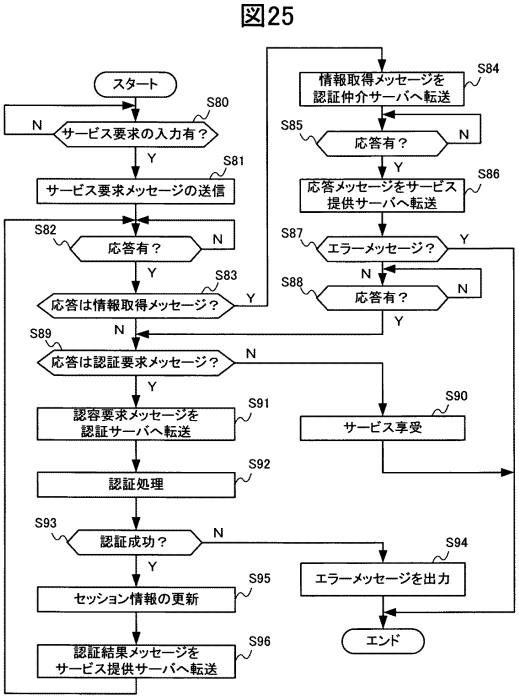
【図２４】

図24



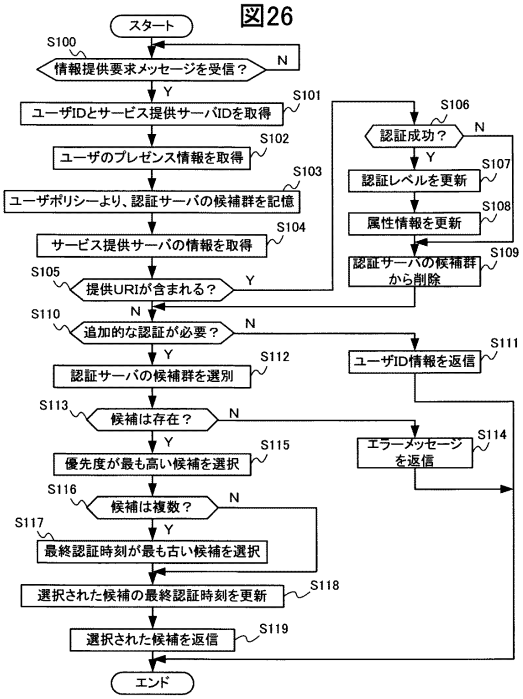
【図２５】

図25



【図２６】

図26



フロントページの続き

(72)発明者　藤城　孝宏
神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所　システム開発研究所内
(72)発明者　入部　真一
神奈川県川崎市幸区鹿島田８９０番地　株式会社日立製作所　ネットワークソリューション事業部内

審査官　宮司　卓佳

(56)参考文献　特開２００７－２５７４２６（ＪＰ，Ａ）
特開２００８－１１７３２６（ＪＰ，Ａ）
特開２００７－１５７００２（ＪＰ，Ａ）
特開２００７－３２８４１１（ＪＰ，Ａ）
特開２００４－３４２０８８（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／２０
Ｈ０４Ｌ　９／３２