(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7238558号
(P7238558)

(45)発行日　令和5年3月14日(2023.3.14)

(24)登録日　令和5年3月6日(2023.3.6)

(51)国際特許分類
Ｇ０６Ｆ　21/45　(2013.01)

ＦＩ
Ｇ０６Ｆ　21/45

請求項の数　7　（全14頁）

(21)出願番号　特願2019-73617(P2019-73617)
(22)出願日　平成31年4月8日(2019.4.8)
(65)公開番号　特開2020-173507(P2020-173507A)
(43)公開日　令和2年10月22日(2020.10.22)
審査請求日　令和4年2月28日(2022.2.28)

(73)特許権者　000005496
富士フイルムビジネスイノベーション株式会社
東京都港区赤坂九丁目７番３号
(74)代理人　110001519
弁理士法人太陽国際特許事務所
(72)発明者　時得　克司
神奈川県横浜市西区みなとみらい六丁目１番　富士ゼロックス株式会社内
審査官　小林　秀和

最終頁に続く

(54)【発明の名称】　認証仲介装置及び認証仲介プログラム

(57)【特許請求の範囲】
【請求項１】
サービスを提供するサービス提供装置から認証要求があった場合に、利用者がサービスを利用するための利用者ＩＤを管理するＩＤ管理装置の中から、認証要求があった前記サービス提供装置の認証に関する認証要件を充足するＩＤ管理装置を抽出する抽出部と、
前記抽出部により抽出された前記ＩＤ管理装置にアクセスするためのリンク情報を、前記サービス提供装置に送信する送信部と、
前記サービス提供装置の認証に関する認証要件と、前記ＩＤ管理装置が前記認証要件を充足するか否かを示す充足要件と、が登録された要件充足リストを取得する取得部と、
前記認証要件を前記要件充足リストに登録することを受け付ける受付部と、
を備え、
前記抽出部は、前記サービス提供装置から認証要求があった場合に、前記要件充足リストに基づいて、認証要求があった前記サービス提供装置の認証要件を充足する前記ＩＤ管理装置を抽出し、
前記受付部は、前記認証要件を満たすことが必須及び任意を含む複数の条件のうち何れの条件であるかを受け付ける
認証仲介装置。
【請求項２】
前記受付部は、前記任意として受け付けた認証要件のうち、予め定めた数又は割合以上の認証要件を満たすことを必須の条件とすることを受け付ける

請求項１記載の認証仲介装置。
【請求項３】
前記受付部は、前記要件充足リストへの前記認証要件の登録パターンを複数受け付ける
請求項１又は請求項２記載の認証仲介装置。
【請求項４】
前記抽出部は、複数の登録パターンの各々について前記ＩＤ管理装置を抽出する
請求項３記載の認証仲介装置。
【請求項５】
前記取得部は、認証要求があった前記サービス提供装置の認証に関する保証レベルと、前記ＩＤ管理装置の認証に関する保証レベルと、を取得する
請求項１～４の何れか１項に記載の認証仲介装置。
【請求項６】
サービスを提供するサービス提供装置から認証要求があった場合に、利用者がサービスを利用するための利用者ＩＤを管理するＩＤ管理装置の中から、認証要求があった前記サービス提供装置の認証に関する認証要件を充足するＩＤ管理装置を抽出する抽出部と、
前記抽出部により抽出された前記ＩＤ管理装置にアクセスするためのリンク情報を、前記サービス提供装置に送信する送信部と、
前記サービス提供装置の認証に関する認証要件と、前記ＩＤ管理装置が前記認証要件を充足するか否かを示す充足要件と、が登録された要件充足リストと、認証要求があった前記サービス提供装置の認証に関する保証レベルと、前記ＩＤ管理装置の認証に関する保証レベルと、を取得する取得部と、
を備え、
前記抽出部は、前記サービス提供装置から認証要求があった場合に、前記要件充足リストに基づいて、前記サービス提供装置の認証に関する保証レベルと異なる保証レベルを有する前記ＩＤ管理装置の中から、認証要求があった前記サービス提供装置の認証要件を充足する前記ＩＤ管理装置を抽出する
認証仲介装置。
【請求項７】
コンピュータを、請求項１～６の何れか１項に記載の認証仲介装置の各部として機能させるための認証仲介プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、認証仲介装置及び認証仲介プログラムに関する。
【背景技術】
【０００２】
特許文献１には、サービスデータの送信が許可される対象となるユーザを示すポリシ情報を記憶するポリシ情報記憶部と、認証連携要求を受信した場合に、ユーザ端末のログイン状態に応じたタイミングでポリシ評価処理とアカウント連携処理とを行なう認証連携要求事前処理部とサービスプロバイダ装置から認証連携要求を受信した場合に、当該認証連携要求を認証連携要求事前処理部に転送する認証連携要求転送部と、を備えたＩＤプロバイダ装置が開示されている。
【０００３】
特許文献２には、クラウドサービスと接続する認証システムであって、ユーザＩＤが登録された複数の認証基盤サーバと、入力されたユーザＩＤと一致するユーザＩＤの登録された認証基盤サーバを特定する情報を、前記クラウドサービスから取得し、前記特定する情報に基づき、前記認証基盤サーバから前記入力されたユーザＩＤの登録情報を取得するデータ連携サーバとを備えたことを特徴とする認証システムが開示されている。
【先行技術文献】
【特許文献】

【０００４】
【文献】特開２０１３－１３７５８８号公報
特開２０１７－４２９６号公報
【発明の概要】
【発明が解決しようとする課題】
【０００５】
従来は１つのシステム内で行われていたサービスの提供及び利用者ＩＤの管理を別個に行う例が多くなっている。また、サービス提供装置とＩＤ管理装置との間で認証処理を仲介する認証仲介装置を設け、１つの利用者ＩＤで複数のサービスの提供が受けられるシングルサインオンを可能とする認証連携（フェデレーション）の仕組みが知られている。
【０００６】
しかしながら、認証仲介装置は、サービス提供装置の認証要件と異なる認証要件を有するＩＤ管理装置については、認証処理を仲介することはできない。例えばサービス提供装置の認証要件よりも緩い認証要件のＩＤ管理装置に認証処理を仲介してしまうと、セキュリティ上の問題が生じる可能性があるためである。
【０００７】
本発明は、サービス提供装置から認証要求があった場合に、サービス提供装置の認証要件を充足するＩＤ管理装置に認証処理を仲介することができる認証仲介装置及び認証仲介プログラムを提供することを目的とする。
【課題を解決するための手段】
【０００８】
第１態様に係る認証仲介装置は、サービスを提供するサービス提供装置から認証要求があった場合に、利用者がサービスを利用するための利用者ＩＤを管理するＩＤ管理装置の中から、認証要求があった前記サービス提供装置の認証に関する認証要件を充足するＩＤ管理装置を抽出する抽出部と、前記抽出部により抽出された前記ＩＤ管理装置にアクセスするためのリンク情報を、前記サービス提供装置に送信する送信部と、を備える。
【０００９】
第２態様に係る認証仲介装置は、第１態様に係る認証仲介装置において、前記サービス提供装置の認証に関する認証要件と、前記ＩＤ管理装置が前記認証要件を充足するか否かを示す充足要件と、が登録された要件充足リストを取得する取得部を備え、前記抽出部は、前記サービス提供装置から認証要求があった場合に、前記要件充足リストに基づいて、認証要求があった前記サービス提供装置の認証要件を充足する前記ＩＤ管理装置を抽出する。
【００１０】
第３態様に係る認証仲介装置は、第２態様に係る認証仲介装置において、前記認証要件を前記要件充足リストに登録することを受け付ける受付部を備える。
【００１１】
第４態様に係る認証仲介装置は、第３態様に係る認証仲介装置において、前記受付部は、前記認証要件を満たすことが必須及び任意を含む複数の条件のうち何れの条件であるかを受け付ける。
【００１２】
第５態様に係る認証仲介装置は、第４態様に係る認証仲介装置において、前記受付部は、前記任意として受け付けた認証要件のうち、予め定めた数又は割合以上の認証要件を満たすことを必須の条件とすることを受け付ける。
【００１３】
第６態様に係る認証仲介装置は、第３態様～第５態様の何れかの態様に係る認証仲介装置において、前記受付部は、前記要件充足リストへの前記認証要件の登録パターンを複数受け付ける。
【００１４】
第７態様に係る認証仲介装置は、第６態様に係る認証仲介装置において、前記抽出部は

、複数の登録パターンの各々について前記ＩＤ管理装置を抽出する。
【００１５】
第８態様に係る認証仲介装置は、第２態様～第７態様の何れかの態様に係る認証仲介装置において、前記取得部は、認証要求があった前記サービス提供装置の認証に関する保証レベルと、前記ＩＤ管理装置の認証に関する保証レベルと、を取得する。
【００１６】
第９態様に係る認証仲介装置は、第８態様に係る認証仲介装置において、前記抽出部は、前記要件充足リストに基づいて、前記サービス提供装置の認証に関する保証レベルと異なる保証レベルを有する前記ＩＤ管理装置の中から、認証要求があった前記サービス提供装置の認証要件を充足する前記ＩＤ管理装置を抽出する。
【００１７】
第１０態様に係る認証仲介プログラムは、第１～第９態様の何れかの態様に係る認証仲介装置の各部として機能させるためのプログラムである。
【発明の効果】
【００１８】
第１、第１０態様によれば、サービス提供装置から認証要求があった場合に、サービス提供装置の認証要件を充足するＩＤ管理装置に認証処理を仲介することができる、という効果を有する。
【００１９】
第２態様によれば、サービス提供装置の認証に関する認証要件と、ＩＤ管理装置が認証要件を充足するか否かを示す充足要件と、が登録された要件充足リストを用いずにサービス提供装置の認証要件を充足するＩＤ管理装置を抽出する場合と比較して、サービス提供装置の認証要件を充足するＩＤ管理装置を容易に抽出することができる、という効果を有する。
【００２０】
第３態様によれば、認証要件を要件充足リストに登録することを受け付けない場合と比較して、認証要件を容易に変更することができる、という効果を有する。
【００２１】
第４態様によれば、認証要件を満たすことが必須及び任意を含む複数の条件のうち何れの条件であるかを受け付けない場合と比較して、柔軟に認証要件を設定することができる、という効果を有する。
【００２２】
第５態様によれば、様々なパターンの認証要件を設定することができる、という効果を有する。
【００２３】
第６態様によれば、要件充足リストへの認証要件の登録パターンを１つしか受け付けない場合と比較して、提供するサービスの内容を登録パターンに応じて異ならせることができる、という効果を有する。
【００２４】
第７態様によれば、登録パターンに応じたＩＤ管理装置を抽出することができる、という効果を有する。
【００２５】
第８態様によれば、認証要求があったサービス提供装置の認証に関する保証レベルと同じ保証レベルのＩＤ管理装置を抽出することができる、という効果を有する。
【００２６】
第９態様によれば、サービス提供装置の認証に関する保証レベルと同じ保証レベルを有するＩＤ管理装置については、サービス提供装置の認証要件を充足するか否かを判定する必要がない、という効果を有する。
【図面の簡単な説明】
【００２７】

【図１】認証仲介装置の構成図である。
【図２】認証仲介装置の電気的構成を示すブロック図である。
【図３】認証仲介装置の機能構成を示すブロック図である。
【図４】認証仲介プログラムの処理の流れの一例を示すフローチャートである。
【図５】認証仲介システムの具体的な接続関係を示す図である。
【図６】要件充足リストの一例を示す図である。
【図７】保証レベル情報の一例を示す図である。
【図８】リンク情報の一例を示す図である。
【発明を実施するための形態】
【００２８】
以下、図面を参照して、本発明を実施するための形態を詳細に説明する。
【００２９】
図１は、本実施形態に係る認証仲介システム１の構成図である。認証仲介システム１は、認証仲介装置１０、複数のサービス提供装置２０、及び複数のＩＤ管理装置３０がネットワークＮを介して接続された構成である。
【００３０】
認証仲介装置１０は、サービス提供装置２０を利用する利用者についての認証処理をサービス提供装置２０から要求された場合に、サービス提供装置２０に対して、認証処理を実行するＩＤ管理装置３０を仲介する。
【００３１】
サービス提供装置（ＲＰ：Ｒｅｌｙｉｎｇ　Ｐａｒｔｙ）２０は、利用者にサービスを提供する。ここで、サービスとは、利用者に提供する電子的な処理であり、例えばドキュメント管理に関する処理、ストレージ管理に関する処理、及びメールの送受信に関する処理等が挙げられるが、これらに限られるものではない。
【００３２】
サービス提供装置２０が提供するサービスを利用する利用者は、例えば利用者ＩＤ及びパスワードを含む利用者情報をサービス提供装置２０に入力し、サービスの利用を指示する。サービス提供装置２０は、サービスの利用が指示されると、利用者情報を認証仲介装置１０に送信し、認証処理を要求する。
【００３３】
ＩＤ管理装置（ＩｄＰ：Ｉｄｅｎｔｉｔｙ　Ｐｒｏｖｉｄｅｒ）３０は、利用者がサービスを利用するための利用者ＩＤを管理し、サービス提供装置２０から認証要求があった場合に認証処理を実行する。
【００３４】
図２は、認証仲介装置１０の構成図である。認証仲介装置１０は、一般的なコンピュータを含む装置で構成される。
【００３５】
図２に示すように、認証仲介装置１０は、コントローラ１２を備える。コントローラ１２は、ＣＰＵ（Central Processing Unit）１２Ａ、ＲＯＭ（Read Only Memory）１２Ｂ、ＲＡＭ（Random Access Memory）１２Ｃ、不揮発性メモリ１２Ｄ、及び入出力インターフェース（Ｉ／Ｏ）１２Ｅを備える。そして、ＣＰＵ１２Ａ、ＲＯＭ１２Ｂ、ＲＡＭ１２Ｃ、不揮発性メモリ１２Ｄ、及びＩ／Ｏ１２ＥがバスＢ１２Ｆを介して各々接続されている。
【００３６】
また、Ｉ／Ｏ１２Ｅには、通信部１４及び記憶部１６が接続されている。
【００３７】
通信部１４は、外部装置とデータ通信を行うためのインターフェースである。
【００３８】
記憶部１６は、ハードディスク等の不揮発性の記憶装置で構成され、後述する認証仲介プログラム１６Ａ、要件充足リスト１６Ｂ、及び保証レベル情報１６Ｃ、及びリンク情報

１６Ｄ等を記憶する。ＣＰＵ１２Ａは、記憶部１６に記憶された認証仲介プログラム１６Ａを読み込んで実行する。

【００３９】

次に、認証仲介装置１０が認証仲介プログラム１６Ａを実行する場合におけるＣＰＵ１２Ａの機能構成について説明する。

【００４０】

図３に示すように、ＣＰＵ１２Ａは、機能的には、取得部４０、抽出部４２、送信部４４、及び受付部４６を備える。

【００４１】

取得部４０は、サービスを提供するサービス提供装置２０の認証に関する認証要件と、利用者がサービスを利用するための利用者ＩＤを管理するＩＤ管理装置３０が認証要件を充足するか否かを示す充足要件と、が登録された要件充足リスト１６Ｂを記憶部１６から読み出すことにより取得する。

【００４２】

抽出部４２は、サービスを提供するサービス提供装置２０から認証要求があった場合に、利用者がサービスを利用するための利用者ＩＤを管理するＩＤ管理装置３０の中から、認証要求があったサービス提供装置２０の認証に関する認証要件を充足するＩＤ管理装置３０を抽出する。具体的には、サービス提供装置２０から認証要求があった場合に、取得部４０が取得した要件充足リスト１６Ｂに基づいて、認証要求があったサービス提供装置２０の認証要件を充足するＩＤ管理装置３０を抽出する。

【００４３】

送信部４４は、抽出部４２により抽出されたＩＤ管理装置３０にアクセスするためのリンク情報を、サービス提供装置２０に送信する。

【００４４】

受付部４６は、サービス提供装置２０から、認証要件を満たすことが必須及び任意の何れの条件であるかを受け付ける。

【００４５】

また、受付部４６は、認証要件を満たすことが必須及び任意の何れの条件であるかを受け付けてもよい。

【００４６】

また、受付部４６は、任意として受け付けた認証要件のうち、予め定めた数又は割合以上の認証要件を満たすことを必須の条件とすることを受け付けてもよい。

【００４７】

また、受付部４６は、要件充足リスト１６Ｂへの認証要件の登録パターンを複数受け付けてもよい。この場合、抽出部４２は、複数の登録パターンの各々についてＩＤ管理装置３０を抽出する。

【００４８】

また、取得部４０は、認証要求があったサービス提供装置２０の認証に関する保証レベルと、ＩＤ管理装置３０の認証に関する保証レベルと、を保証レベル情報１６Ｃから取得してもよい。この場合、抽出部４２は、要件充足リスト１６Ｂに基づいて、サービス提供装置２０の認証に関する保証レベルと異なる保証レベルを有するＩＤ管理装置３０の中から、認証要求があったサービス提供装置２０の認証要件を充足するＩＤ管理装置３０を抽出する。ここで、保証レベルとは、所謂ＬｏＡ（Ｌｅｖｅｌ ｏｆ Ａｓｓｕｒａｎｃｅ）のことであり、利用者の認証に関する保証の度合いを表す。

【００４９】

次に、本実施の形態に係る認証仲介装置１０の作用を説明する。図２に示すように、認証仲介プログラム１６Ａは記憶部１６に記憶されている。ＣＰＵ１２Ａが認証仲介プログラム１６Ａを読み出して実行することにより、図４に示す認証仲介処理が実行される。なお、図４に示す認証仲介処理は、予め定めた時間毎に繰り返し実行される。

【００５０】

以下では、図５に示すように、認証仲介システム１が、認証仲介装置１０としてのＩｄＰ＿Ｂｒと、サービス提供装置２０としてのＲＰ＿Ａ、ＲＰ＿Ｂ、及びＲＰ＿Ｃと、ＩＤ管理装置３０としてのＩｄＰ＿Ａ及びＩｄＰ＿Ｃと、で構成される場合について説明する。なお、ＲＰ＿Ａ、ＲＰ＿Ｂ、及びＲＰ＿Ｃを区別しない場合は、単にＲＰと称する場合がある。また、ＩｄＰ＿Ａ及びＩｄＰ＿Ｃを区別しない場合は、単にＩｄＰと称する場合がある。

【００５１】

また、各装置は、認証に関する保証レベルに応じて２つのグループに分けられる。図５の例では、ＲＰ＿Ａ及びＩｄＰ＿ＡがグループＸに属し、ＩｄＰ＿ｂｒ、ＩｄＰ＿Ｃ、ＲＰ＿Ｂ、及びＲＰ＿ＣがグループＹに属する。ここで、グループＸ内の各装置の保証レベルは同一であり、グループＹ内の各装置の保証レベルも同一であるものとする。また、グループＹに属する装置の保証レベルは、グループＸに属する装置の保証レベルよりも高いものとする。

【００５２】

グループＸに属するかグループＹに属するかは、本実施形態では一例としてトラストフレームワークに参加しているか不参加であるかで分けられる。ここで、トラストフレームワークとは、利用者認証の信頼性を保証し合う枠組みである。図５の例では、例えばグループＹに属する装置はトラストフレームワークに参加しており、グループＸに属する装置はトラストフレームワークに不参加の装置である。

【００５３】

また、図５の例では、ＩｄＰ＿Ａは、利用者Ｕｓｅｒ＿Ａ、Ｕｓｅｒ＿Ｂの利用者情報を保持しており、ＩｄＰ＿Ｃは、利用者Ｕｓｅｒ＿Ｃ、Ｕｓｅｒ＿Ｄの利用者情報を保持しており、ＩｄＰ＿ｂｒは、利用者Ｕｓｅｒ＿Ａ、Ｕｓｅｒ＿Ｂ、Ｕｓｅｒ＿Ｃ、Ｕｓｅｒ＿Ｄの利用者情報を保持しているものとする。

【００５４】

利用者は、サービスの提供を受けたいＲＰに対して利用者情報を入力し、サービスの利用を要求する。

【００５５】

ＩｄＰ＿ｂｒは、Ｕｓｅｒ＿Ａ～Ｕｓｅｒ＿Ｄの何れかによりＲＰ＿Ａから認証要求があった場合、ＲＰ＿Ａと保証レベルが同一のＩｄＰ＿Ａについては、ＲＰ＿Ａに対して問題無く認証処理を仲介可能である。一方、Ｕｓｅｒ＿Ａ～Ｕｓｅｒ＿Ｄの何れかによりＲＰ＿Ａから認証要求があった場合、ＲＰ＿Ａと保証レベルが異なるＩｄＰ＿Ｃについては、本来はＲＰ＿Ａに対して認証処理を仲介できないが、ＩｄＰ＿ＣがＲＰ＿Ａの認証要件を充足する場合は認証処理を仲介する。

【００５６】

また、ＩｄＰ＿ｂｒは、Ｕｓｅｒ＿Ａ～Ｕｓｅｒ＿Ｄの何れかによりＲＰ＿Ｂから認証要求があった場合、ＲＰ＿Ｂと保証レベルが同一のＩｄＰ＿Ｃについては、ＲＰ＿Ｂに対して問題無く認証処理を仲介可能である。一方、Ｕｓｅｒ＿Ａ～Ｕｓｅｒ＿Ｄの何れかによりＲＰ＿Ｂから認証要求があった場合、ＲＰ＿Ｂと保証レベルが異なるＩｄＰ＿Ａについては、本来はＲＰ＿Ｂに対して認証処理を仲介できないが、ＩｄＰ＿ＡがＲＰ＿Ｂの認証要件を充足する場合は認証処理を仲介する。

【００５７】

また、ＲＰ＿Ｃは、ＩｄＰ＿ｂｒとは接続されていない。このため、ＲＰ＿Ｃは、保証レベルが異なるＩｄＰ＿Ａ及びＲＰ＿Ａの影響を受けない。従って、Ｕｓｅｒ＿Ｃ又はＵｓｅｒ＿ＤによりＲＰ＿Ｃから認証要求があった場合は、ＩｄＰ＿Ｃが認証処理を実行する。

【００５８】

ステップＳ１００では、ＲＰから認証要求があったか否かを判定する。すなわち、ＲＰから利用者情報を受信したか否かを判定する。そして、ＲＰから利用者情報を受信した場合はステップＳ１０２へ移行し、ＲＰから利用者情報を受信していない場合はステップＳ

１０８へ移行する。
【００５９】
ステップＳ１０２では、ＲＰの認証に関する認証要件と、ＩｄＰが認証要件を充足するか否かを示す充足要件と、が登録された要件充足リスト１６Ｂを記憶部１６から読み出すことにより取得する。また、各ＲＰ及び各ＩｄＰの保証レベルが登録された保証レベル情報１６Ｃを記憶部１６から読み出すことにより取得する。
【００６０】
図６に示すように、要件充足リスト１６Ｂは、ＲＰの認証に関する認証要件と、ＩｄＰが認証要件を充足するか否かを示す充足要件と、が登録されたリストである。
【００６１】
図６に示すように、要件充足リスト１６Ｂには、各ＲＰの認証要件について「必須」、「任意」、「不可」、及び「不要」の何れかが登録されている。ここで、認証要件が「必須」とは、その認証要件が必ず必要であることを表す。また、認証要件が「任意」とは、その認証要件を用いて認証しても良いし、その認証要件を用いなくても良いことを表す。認証要件が「不可」とは、その認証要件を用いて認証してはいけないことを表す。また、認証要件が「不要」とは、その認証要件を用いて認証する必要がないことを表す。
【００６２】
また、要件充足リスト１６Ｂには、各ＩｄＰが充足する認証要件が登録されている。図６では、ＩｄＰが充足する認証要件を「○」で示し、充足しない認証要件は空欄としている。各ＲＰは、各認証要件が「必須」、「任意」、「不可、及び「不要」の何れであるのかを予めＩｄＰ＿ｂｒに通知することにより、要件充足リスト１６Ｂに登録しておく。また、各ＩｄＰは、各認証要件を充足するか否かを予めＩｄＰ＿ｂｒに通知することにより、要件充足リスト１６Ｂに登録しておく。
【００６３】
また、図７に示すように、保証レベル情報１６Ｃは、各ＲＰ及び各ＩｄＰの保証レベルが登録されている。図７の例では、ＲＰ＿Ａ及びＩｄＰ＿Ａの保証レベルがＬ１に設定され、ＲＰ＿Ｂ及びＩｄＰ＿Ｃの保証レベルがＬ２に設定されている。なお、本実施形態では一例としてＬ２＞Ｌ１である。すなわち、ＲＰ＿Ｂ及びＩｄＰ＿Ｃの保証レベルの方が、ＲＰ＿Ａ及びＩｄＰ＿Ａの保証レベルよりも高く設定されている。
【００６４】
ステップＳ１０４では、ステップＳ１０２で取得した要件充足リスト１６Ｂ及び保証レベル情報１６Ｃに基づいて、認証要求があったＲＰの認証要件を充足するＩｄＰを抽出する。具体的には、まず保証レベル情報１６Ｃを参照し、認証要求があったＲＰの保証レベルと同じ保証レベルを有するＩｄＰを抽出する。
【００６５】
更に、要件充足リスト１６Ｂに基づいて、認証要求があったＲＰの保証レベルと異なる保証レベルを有するＩｄＰの中から、認証要求があったＲＰの認証要件を充足するＩｄＰを抽出する。ここで、認証要求があったＲＰの認証要件を充足するＩｄＰとは、ＲＰの認証要件のうち「必須」が設定された認証要件を全て充足するＩｄＰである。すなわち、ＲＰの認証要件のうち「必須」が設定された認証要件を１つでも充足しない場合は、ＲＰの認証要件を充足するとはいえない。
【００６６】
具体的には、例えばＵｓｅｒ＿Ａ～Ｕｓｅｒ＿Ｄの何れかによりＲＰ＿Ａから認証要求があった場合、ＲＰ＿Ａと保証レベルが同一のＩｄＰ＿Ａは無条件に抽出される。一方、ＲＰ＿Ａと保証レベルが異なるＩｄＰ＿Ｃについては、ＲＰ＿Ａの認証要件を充足するか否かによる。ここで、図６に示すように、ＲＰ＿Ａの認証要件のうち「必須」が設定された認証要件は、「写真無公的身分証明書１種類」、「単要素認証」、及び「弱中間者攻撃対策」である。そして、ＩｄＰ＿Ｃは、認証要件として「弱中間者攻撃対策」は充足するものの、「写真無公的身分証明書１種類」及び「単要素認証」については充足していない。従って、ＩｄＰ＿Ｃは抽出されない。

【００６７】
　また、例えばＵｓｅｒ＿Ａ～Ｕｓｅｒ＿Ｄの何れかによりＲＰ＿Ｂから認証要求があった場合、ＲＰ＿Ｂと保証レベルが同一のＩｄＰ＿Ｃは無条件に抽出される。一方、ＲＰ＿Ｂと保証レベルが異なるＩｄＰ＿Ａについては、ＲＰ＿Ｂの認証要件を充足するか否かによる。ここで、図６に示すように、ＲＰ＿Ｂの認証要件のうち「必須」が設定された認証要件は、「写真付公的身分証明書１種類」、「電話番号提示」、「多要素認証」、及び「弱中間者攻撃対策」である。そして、ＩｄＰ＿Ａは、これら全ての認証要件を充足する。従って、ＩｄＰ＿Ａも抽出される。
【００６８】
　なお、保証レベル情報１６Ｃを取得せずに、要件充足リスト１６Ｂのみに基づいて、認証要求があったＲＰの認証要件を充足するＩｄＰを抽出するようにしてもよい。すなわち、保証レベルに関係無く、全てのＩｄＰに対して認証要求があったＲＰの認証要件を充足するか否かを判定してもよい。
【００６９】
　ステップＳ１０６では、記憶部１６からリンク情報１６Ｄを読み出し、読み出したリンク情報１６Ｄから、ステップＳ１０４で抽出したＩｄＰのリンク先を取得する。図８に示すように、リンク情報１６Ｄには、各ＲＰ及び各ＩｄＰのリンク先が登録されている。図８の例では、リンク先はＵＲＬ（Uniform Resource Locator）で表されるが、これに限られるものではない。そして、取得したリンク先を、認証要求があったＲＰにリンク情報として送信する。これにより、ＲＰでは、抽出された全てのＩｄＰのリンク先が表示され、認証処理を実行可能なＩｄＰへのアクセスが可能となる。
【００７０】
　ところで、ＲＰ及びＩｄＰの管理者は、例えばＲＰに認証要件を入力して要件充足リスト１６ＢにＲＰ及びＩｄＰの少なくとも一方の認証要件を登録するよう要求可能である。この場合、ＲＰは、受け付けた認証要件をＩｄＰ＿ｂｒに送信し、要件充足リスト１６Ｂに登録するよう要求する。
【００７１】
　そこで、ステップＳ１０８では、ＲＰ又はＩｄＰから、認証要件を要件充足リスト１６Ｂに登録することを受け付けたか否かを判定する。そして、認証要件を要件充足リスト１６Ｂに登録することを受け付けた場合はステップＳ１１０へ移行し、認証要件を要件充足リスト１６Ｂに登録することを受け付けていない場合は本ルーチンを終了する。
【００７２】
　ＩｄＰについては、ＲＰの各認証要件を充足するか否かを受け付ける。
【００７３】
　また、ＲＰについては、各認証要件について、認証要件を満たすことが必須及び任意を含む複数の条件のうち何れの条件であるかを受け付ける。本実施形態では、一例として「必須」、「任意」、「不可」、及び「不要」の何れかを受け付ける。
【００７４】
　また、ＲＰの認証要件を受け付ける場合、「任意」として受け付けた認証要件のうち、予め定めた数又は割合以上の認証要件を満たすことを必須の条件とすることを受け付けてもよい。例えば、図６の例では、ＲＰ＿Ａの認証要件として「任意」が設定された「単要素認証」、「フィッシング／ファーミング対策」、「盗聴対策」、及び「強中間者攻撃対策」の４個の認証要件のうち、例えば予め定めた数として２個以上（５０％以上）の認証要件を満たすことを必須の条件としてもよい。この場合、「フィッシング／ファーミング対策」、「盗聴対策」、及び「強中間者攻撃対策」のうち２個以上の認証要件を充足するＩｄＰが抽出対象となる。
【００７５】
　また、ＲＰの認証要件を受け付ける場合、要件充足リスト１６Ｂへの認証要件の登録パターンを複数受け付けてもよい。この場合、複数の登録パターンの各々についてＩｄＰを抽出する。この場合、ＲＰは、例えば第１の登録パターンの認証要件を第２の登録パター

ンの認証要件よりも厳しくし、第１の登録パターンの認証要件を満たす利用者には全ての機能についてサービスを提供し、第２の登録パターンの認証要件を満たす利用者には一部の機能についてサービスを提供することが可能となる。

【００７６】

また、ＲＰから、要件充足リスト１６Ｂに登録されていない新たな認証要件を追加することを受け付けても良い。

【００７７】

ステップＳ１１０では、ステップＳ１０８で受け付けた認証要件を要件充足リスト１６Ｂに登録する。

【００７８】

以上、実施の形態を説明したが、本発明の技術的範囲は上記実施の形態に記載の範囲には限定されない。発明の要旨を逸脱しない範囲で上記実施の形態に多様な変更又は改良を加えることができ、該変更又は改良を加えた形態も本発明の技術的範囲に含まれる。

【００７９】

例えば、本実施形態では、ＲＰ及びＩｄＰがグループＸ及びグループＹの何れに属するかは、トラストフレームワークへの参加及び不参加の何れであるかによって分けられる場合について説明したが、これに限られない。例えば、グループＸ及びグループＹの何れに属するかが、装置の機微度の違いで分けられてもよい。ここで、機微度とは、各装置が扱う情報の重要度である。例えば機微度が相対的に低い装置をグループＸ、機微度が相対的に高い装置をグループＹに属する装置とした場合、トラストフレームワークへの参加及び不参加の何れであるかによってグループ分けした場合と同様となる。

【００８０】

また、上記実施の形態は、クレーム（請求項）にかかる発明を限定するものではなく、また実施の形態の中で説明されている特徴の組み合わせの全てが発明の解決手段に必須であるとは限らない。前述した実施の形態には種々の段階の発明が含まれており、開示される複数の構成要件の組み合わせにより種々の発明が抽出される。実施の形態に示される全構成要件から幾つかの構成要件が削除されても、効果が得られる限りにおいて、この幾つかの構成要件が削除された構成が発明として抽出され得る。

【００８１】

また、上記実施の形態では、サービス仲介プログラムがＲＯＭ１０２に予めインストールされている場合について説明したが、本発明はこれに限定されるものではない。例えば、サービス仲介プログラムが、ＣＤ－ＲＯＭ（Compact Disc Read Only Memory）等の記憶媒体に格納されて提供される形態、又はネットワークを介して提供される形態としてもよい。

【００８２】

さらに、上記実施の形態では、サービス仲介処理を、プログラムを実行することにより、コンピュータを利用してソフトウェア構成により実現する場合について説明したが、本発明はこれに限定されるものではない。例えば、サービス仲介処理を、ハードウェア構成や、ハードウェア構成とソフトウェア構成の組み合わせによって実現する形態としてもよい。

【００８３】

その他、上記実施の形態で説明した認証仲介装置１０の構成（図２参照。）は一例であり、本発明の主旨を逸脱しない範囲内において不要な部分を削除したり、新たな部分を追加したりしてもよいことは言うまでもない。

【００８４】

また、上記実施の形態で説明したサービス仲介プログラムの処理の流れ（図４参照）も一例であり、本発明の主旨を逸脱しない範囲内において不要なステップを削除したり、新たなステップを追加したり、処理順序を入れ替えたりしてもよいことは言うまでもない。

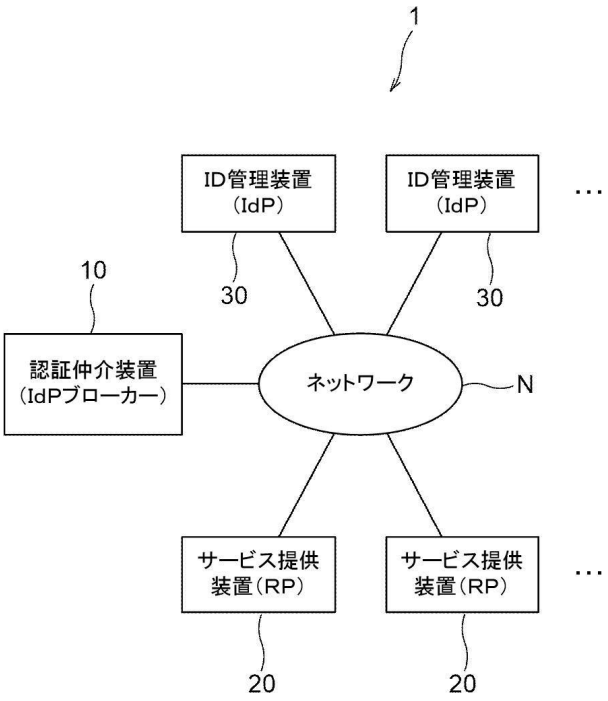
【符号の説明】

【００８５】

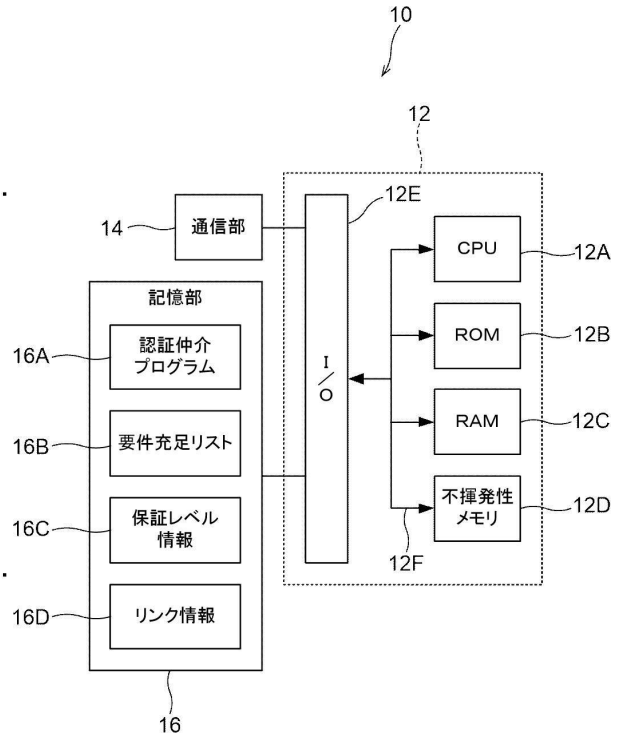
１　　認証仲介システム
１０　認証仲介装置
１２　コントローラ
１４　通信部
１６　記憶部
１６Ａ 認証仲介プログラム
１６Ｂ 要件充足リスト
１６Ｃ 保証レベル情報
１６Ｄ リンク情報
２０　サービス提供装置
３０　ＩＤ管理装置
４０　取得部
４２　抽出部
４４　送信部
４６　受付部

【図面】

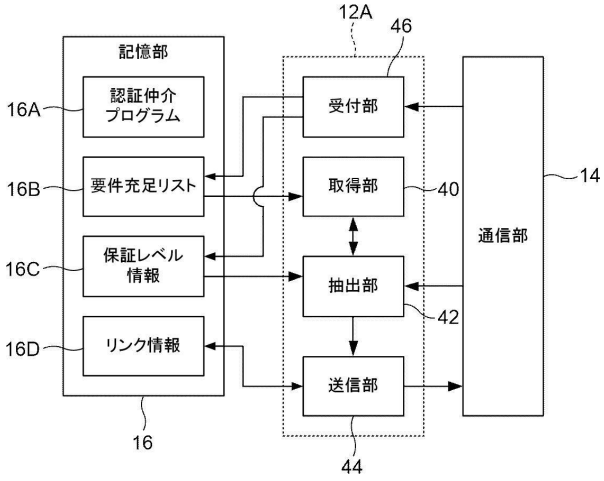
【図１】



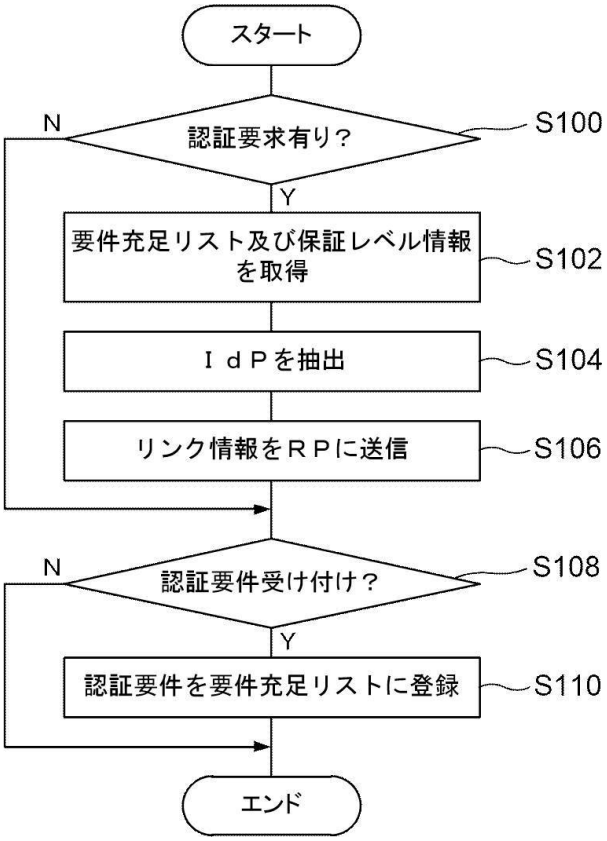
【図２】



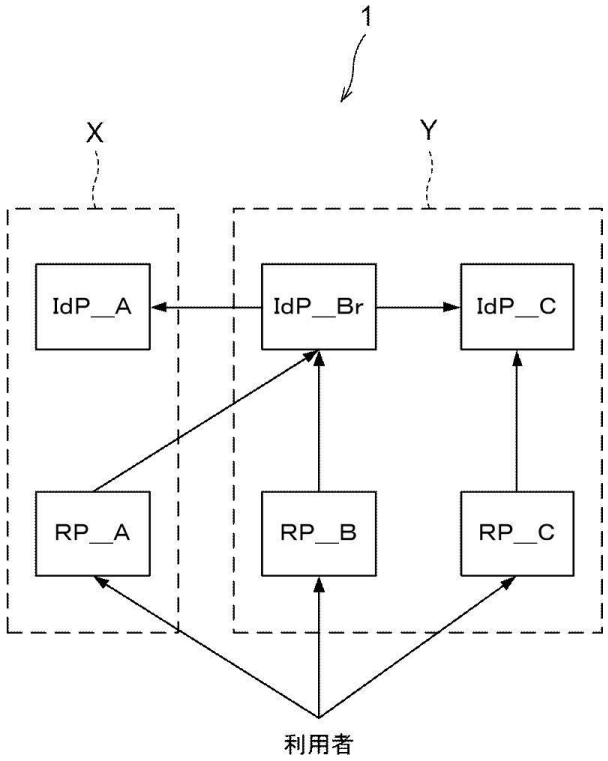
【図３】



【図４】



【図５】



【図６】

16B

認証要件	RP__A	RP__B	IdP__A	IdP__C
写真付公的身分証明書2種類	不要	不要		
写真付公的身分証明書1種類	任意	必須	○	○
写真無公的身分証明書1種類	必須	不要		
金融個別番号表示	不要	不要		
電話番号提示	任意	必須	○	○
多要素認証	任意	必須	○	○
単要素認証	必須	不可		
フィッシング／ファーミング対策	任意	任意		○
盗聴対策	任意	任意		○
強中間者攻撃対策	任意	任意		○
弱中間者攻撃対策	必須	必須	○	○

【図７】

16C

装置	保証レベル
RP__A	L1
RP__B	L2
IdP__A	L1
IdP__C	L2

【図８】

16D

装置	リンク先
RP__A	RP_A.com
RP__B	RP_B.com
IdP__A	IdP_A.com
IdP__C	IdP_C.com

フロントページの続き

(56)参考文献 特表２０１５－５０７２８５（ＪＰ，Ａ）
特開２０１１－１９１８８２（ＪＰ，Ａ）
国際公開第２０１０／１１０１８２（WO，Ａ１）
特表２０１６－５１１８４９（ＪＰ，Ａ）

(58)調査した分野 (Int.Cl.，ＤＢ名)
Ｇ０６Ｆ ２１／４５
Ｇ０６Ｆ ２１／４１