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

特許第5289480号
(P5289480)

(45)発行日　平成25年9月11日(2013.9.11)　(24)登録日　平成25年6月14日(2013.6.14)

(51)Int.Cl.		F I		
G06F 21/41	(2013.01)	G06F	21/20	141
G06F 21/31	(2013.01)	G06F	21/20	131A
H04L 9/32	(2006.01)	H04L	9/00	673A

請求項の数 7　(全 19 頁)

(21)出願番号　特願2011-29995(P2011-29995)
(22)出願日　平成23年2月15日(2011.2.15)
(65)公開番号　特開2012-168795(P2012-168795A)
(43)公開日　平成24年9月6日(2012.9.6)
審査請求日　平成24年2月16日(2012.2.16)

(73)特許権者　000001007
キヤノン株式会社
東京都大田区下丸子３丁目３０番２号
(74)代理人　100126240
弁理士　阿部　琢磨
(74)代理人　100124442
弁理士　黒岩　創吾
(72)発明者　田村　存
東京都大田区下丸子３丁目３０番２号キヤノン株式会社内

審査官　▲吉▼田　耕一

最終頁に続く

(54)【発明の名称】情報処理システム、情報処理装置の制御方法、およびそのプログラム。

(57)【特許請求の範囲】
【請求項１】
クライアント、および認証情報の入力を要求し認証処理を行う認証サービスを提供する少なくとも１つ以上の認証装置と通信可能な、Ｗｅｂサービスを提供する情報処理システムであって、
前記認証サービスによる認証処理が成功したことを信頼し、認証処理に必要な認証情報の入力を要求することなくＷｅｂサービスを提供する提供手段と、
何れかの前記認証サービスを受けさせる際に必要となる認証装置を決定するためのキー情報と、前記認証装置のアドレス情報とを関連付けて保存する保存手段と、
前記Ｗｅｂサービスを受けるために前記クライアントがアクセスを行い、前記クライアントからのアクセスが前記認証サービスを受けていない未認証のアクセスだった場合は、前記アクセスが行われることで取得したキー情報に対応する前記保存手段により保存されたキー情報を特定し、特定された該キー情報と関連づけて保存された前記認証装置のアドレス情報を前記クライアントへ送信するとともに、前記クライアントに前記認証サービスを受けさせるために前記認証装置へアクセスするようリダイレクトの指示を出す指示手段と、を有し、
前記指示手段は、前記キー情報とは異なる情報であって、指定の認証装置で認証を受けるための情報が、前記クライアントが前記情報処理システムにアクセスする際に使用したＵＲＬに含まれている場合、または前記キー情報の入力を要求する画面に含まれる項目であって、指定の認証装置で認証を受けるための項目が前記クライアントにおいて有効とさ

れた場合、取得したキー情報に関わらず、指定の認証装置へアクセスするようリダイレクトの指示を出すことを特徴とする情報処理システム。
【請求項２】
前記キー情報の入力を要求する画面を前記クライアントへ送信する送信手段と、前記クライアントが前記情報処理システムにアクセスする際に使用したＵＲＬにキー情報が含まれているか否かを判断する判断手段と、を有し、
前記指示手段は、前記判断手段によりキー情報が含まれていると判断された場合は、前記ＵＲＬから取得したキー情報を前記取得したキー情報として利用し、
前記判断手段によりキー情報が含まれていないと判断された場合は、前記送信手段により送信された画面を介して入力されたキー情報を前記取得したキー情報として利用することを特徴とする請求項１に記載の情報処理システム。
【請求項３】
ＵＲＬから前記キー情報を抽出する抽出手段を有し、
前記判断手段は、前記抽出手段によりキー情報が抽出された場合に、前記ＵＲＬにキー情報が含まれていると判断することを特徴とする請求項２に記載の情報処理システム。
【請求項４】
前記提供手段は、前記指示手段による指示に応じて認証装置へアクセスし該認証装置からアサーションを取得したクライアントから前記アサーションを取得し、前記アサーションの検証を行い、前記アサーションが妥当だった場合にはＷｅｂサービスを前記クライアントへ提供することを特徴とする請求項３に記載の情報処理システム。
【請求項５】
前記キー情報とは、テナントＩＤであることを特徴とする請求項１に記載の情報処理システム。
【請求項６】
クライアント、および認証情報の入力を要求し認証処理を行う認証サービスを提供する少なくとも１つ以上の認証装置、および前記認証サービスによる認証処理が成功したことを信頼し、認証処理に必要な認証情報の入力を要求することなくＷｅｂサービスを提供するサービス提供装置と通信可能な情報処理装置を制御する制御方法であって、
保存手段は、何れかの前記認証サービスを受けさせる際に必要となる認証装置を決定するためのキー情報と、前記認証装置のアドレス情報とを関連付けて保存し、
指示手段は、前記Ｗｅｂサービスを受けるために前記クライアントがアクセスを行い、前記クライアントからのアクセスが前記認証サービスを受けていない未認証のアクセスだった場合は、前記アクセスが行われることで取得したキー情報に対応する前記保存手段により保存されたキー情報を特定し、特定された該キー情報と関連づけて保存された前記認証装置のアドレス情報を前記クライアントへ送信するとともに、前記クライアントに前記認証サービスを受けさせるために前記認証装置へアクセスするようリダイレクトの指示を出し、
更に、前記指示手段は、前記キー情報とは異なる情報であって、指定の認証装置で認証を受けるための情報が、前記クライアントが前記情報処理システムにアクセスする際に使用したＵＲＬに含まれている場合、または前記キー情報の入力を要求する画面に含まれる項目であって、指定の認証装置で認証を受けるための項目が前記クライアントにおいて有効とされた場合、取得したキー情報に関わらず、指定の認証装置へアクセスするようリダイレクトの指示を出すことを特徴とする制御方法
【請求項７】
請求項６に記載の制御方法をコンピュータに実行させるためのプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、シングルサインオンを提供する情報処理システム、情報処理装置の制御方法、およびそのプログラムに関する。

【背景技術】
【０００２】
従来複数のサービス間で認証を連携させる技術として、ＳＡＭＬ（Ｓｅｃｕｒｉｔｙ Ａｓｓｅｒｔｉｏｎ Ｍａｒｋｕｐ Ｌａｎｇｕａｇｅ）によるシングルサインオン（以下ＳＳＯ） の仕組みがある。ＳＡＭＬのＳＳＯにおいて、ユーザは、認証サービスを提供する側（Ｉｄｅｎｔｉｔｙ Ｐｒｏｖｉｄｅｒ、以下 ＩｄＰ）、および認証サービスの認証結果を信頼してサービスを提供する側（Ｓｅｒｖｉｃｅ Ｐｒｏｖｉｄｅｒ、以下 ＳＰ）の両方のＩＤを保有している。ユーザがＩｄＰで認証を受けると、ＳＰはその認証結果を信頼して、そのアクセスをＳＰ内で管理するＩＤとして認証する（ＩｄＰ先行）。また、ＩｄＰで認証を受けていない未認証のユーザがＳＰにアクセスしてきた場合、ＳＰは、未認証のユーザユーザを適切なＩｄＰへと誘導し、ＩｄＰで認証させる必要がある（ＳＰ先行）。このようなフローをＳＰ－ｉｎｉｔｉａｔｅｄ ＳＳＯと呼ぶことがある。
【０００３】
また、未認証ユーザがＳＰにアクセスした時点で、そのユーザをどのＩｄＰへ誘導させて認証を受けさせるかを特定することができない。そこで従来のＳＰ－ｉｎｉｔｉａｔｅｄ ＳＳＯには、ＳＰが認証を連携させているＩｄＰの一覧を表示してユーザに選択させる方式があった。また、ユーザがアクセスするＳＰが要求するであろう認証レベル、およびユーザ属性に従って、ＳＰの要求を満たすＩｄＰを決定してユーザをリダイレクトさせる方式が特許文献１に開示されている。
【先行技術文献】
【特許文献】
【０００４】
【特許文献１】特開２０１０－１２８７１９
【発明の概要】
【発明が解決しようとする課題】
【０００５】
しかしながら従来の方法には以下の問題があった。企業のイントラネット内のＩｄＰを利用したいユーザがいたとする。そのユーザはイントラネット内のＩｄＰを指定する手段が必要だが、セキュリティの観点から見たとき、ＳＰはＩＤＰの一覧表示を行う際に、そのＩｄＰを一覧に表示すべきでない。なぜなら、例えば、そのユーザとは関係のない第三者によりそのＩＤＰが見えてしまう可能性があり、その場合、そのユーザに関する個人情報が漏れてしまうからである。
【０００６】
また、特許文献１では、ＳＰがユーザに対しリダイレクトさせた相手先のＩｄＰに、そのユーザのＩＤが登録されていない可能性もあり、ユーザが認証を受けることができない。
【課題を解決するための手段】
【０００７】
本発明の一実施系に係る情報処理システムは、ライアント、および認証情報の入力を要求し認証処理を行う認証サービスを提供する少なくとも１つ以上の認証装置と通信可能な、Ｗｅｂサービスを提供する情報処理システムであって、前記認証サービスによる認証処理が成功したことを信頼し、認証処理に必要な認証情報の入力を要求することなくＷｅｂサービスを提供する提供手段と、何れかの前記認証サービスを受けさせる際に必要となる認証装置を決定するためのキー情報と、前記認証装置のアドレス情報とを関連付けて保存する保存手段と、前記Ｗｅｂサービスを受けるために前記クライアントがアクセスを行い、前記クライアントからのアクセスが前記認証サービスを受けていない未認証のアクセスだった場合は、前記アクセスが行われることで取得したキー情報に対応する前記保存手段により保存されたキー情報を特定し、特定された該キー情報と関連づけて保存された前記認証装置のアドレス情報を前記クライアントへ送信するとともに、前記クライアントに前

記認証サービスを受けさせるために前記認証装置へアクセスするようリダイレクトの指示を出す指示手段と、を有し、前記指示手段は、前記キー情報とは異なる情報であって、指定の認証装置で認証を受けるための情報が、前記クライアントが前記情報処理システムにアクセスする際に使用したＵＲＬに含まれている場合、または前記キー情報の入力を要求する画面に含まれる項目であって、指定の認証装置で認証を受けるための項目が前記クライアントにおいて有効とされた場合、取得したキー情報に関わらず、指定の認証装置へアクセスするようリダイレクトの指示を出すことを特徴とする。

【発明の効果】

【０００８】

本発明によれば、未認証のユーザからアクセスを行われたＳＰが、ユーザのアクセスに応じて取得したキー情報を基に適切なＩｄＰに誘導させるため、そのユーザは適切なＩｄＰで認証を受けられるようになる。

【図面の簡単な説明】

【０００９】

【図１】ネットワーク構成を示す図である。

【図２】本発明の実施の形態に係るモジュール構成図である。

【図３】本発明の実施の形態に係る認証サービス決定サービス３００のモジュール構成図である。

【図４】本発明の実施の形態に係る第２の管理モジュール３１１が管理する情報である。

【図５】本発明の実施の形態に係るサービス提供サーバ５００のフローである。

【図６】本発明の実施の形態に係る認証サービス決定サービス３００のフローである。

【図７】本発明の実施の形態に係るＳＳＯを実現する際の認証サービスＢ４５０におけるフローである。

【図８】本発明の実施の形態に係るＳＳＯを実現する際の認証サービスＡ４００におけるフローである。

【図９】本発明の実施の形態に係るＳＳＯを実施しない際の認証サービスＡ４００におけるフローである。

【図１０】本発明の実施の形態に係る認証情報の入力画面である。

【図１１】本発明の第２の実施の形態に係る認証サービス決定サービス３００のモジュール構成図である。

【図１２】本発明の第２の実施の形態に係る第３の管理モジュール３２１が管理する情報である。

【図１３】本発明の第２の実施の形態に係る認証サービス決定サービス３００のフローである。

【図１４】本発明の第３の実施の形態に係る認証サービス決定サービス３００のモジュール構成図である。

【図１５】本発明の第３の実施の形態に係る認証サービス決定サービス３００のフローである。

【図１６】本発明の第３の実施の形態に係る企業ＩＤの入力画面である。

【図１７】本発明の第４の実施の形態に係る認証サービス決定サービス３００のモジュール構成図である。

【図１８】本発明の第４の実施の形態に係る認証サービス決定サービス３００のフローである。

【図１９】本発明の第４の実施の形態に係る企業ＩＤの入力画面である。

【図２０】本発明の実施の形態に係るハードウェア構成図。

【発明を実施するための形態】

【００１０】

本発明の目的は、認証を連携させたＳＳＯシステムにおいて、未認証のユーザアクセスを適切なＩｄＰに誘導させることである。

以降、本発明を実施するための最良の形態について図面を用いて説明する。

【実施例１】
【００１１】
本実施の形態に係る権限委譲システムは、図１に示すような構成のネットワーク上に実現される。
【００１２】
１００は、Ｗｉｄｅ　Ａｒｅａ　Ｎｅｔｗｏｒｋ（ＷＡＮ１００）であり、本発明ではＷｏｒｌｄ　Ｗｉｄｅ　Ｗｅｂ（ＷＷＷ）システムが構築されている。１０１は各構成要素を接続するＬｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ（ＬＡＮ１０１）である。ＬＡＮ１０１は、ＷＡＮ１００を介すること互いの装置は通信可能になる。
【００１３】
２００はユーザが操作するクライアントＰＣであり、３００はユーザのアクセスを適切なＩｄＰへと誘導する認証サービス決定サービスである。４００および４５０はそれぞれ認証を行う認証サービスＡ，Ｂであり、ともにＩｄＰ（アイデンティティプロバイダ装置）として動作する。なお認証サービスは２つに限定されるものではない。どのＩｄＰが実際の認証を行うかはアクセスしてきたユーザによって異なる。５００はサービス提供サービスであり、認証されたユーザに対してサービスを提供する。
【００１４】
またクライアントＰＣ２００、認証サービス決定サービス３００、認証サービスＡ４００、認証サービスＢ４５０、サービス提供サービス５００はそれぞれＷＡＮネットワーク１００およびＬＡＮ１０１を介して接続されている。なおクライアントＰＣ２００およびそれぞれのサービスはそれぞれ個別のＬＡＮ上に構成されていてもよいし同一のＬＡＮ上に構成されていてもよい。また同一のＰＣ上に構成されていてもよい。認証サービス決定サービス３００、認証サービスＡ４００、サービス提供サービス５００は同じネットワーク内（イントラネット内）に構築されたサーバ群となる。
【００１５】
クライアントＰＣ２００はまずＷｅｂサービスを受けるためサービス提供サービス５００にアクセスする。サービス提供サービスは未認証のユーザアクセスを受け付けると、アクセスを認証サービス決定サービス３００にリダイレクトさせる。認証サービス決定サービス３００は未認証アクセスを適切な認証サービスＡ４００または認証サービスＢ４５０にリダイレクトさせる。認証サービスＡ４００または認証サービスＢ４５０はユーザを認証すると、再度ユーザをサービス提供サービス５００にリダイレクトさせ、サービス提供サービス５００がユーザにサービスを提供する。
【００１６】
図２０は本実施の形態に係るクライアントＰＣ２００の構成を示す図である。また認証サービス決定サービス３００、認証サービスＡ４００、認証サービスＢ４５０、サービス提供サービス５００を提供するサーバコンピューターの構成も同様である。これらサービスはサーバであり、図２０に示されるハードウェアブロック図の構成を有する。このように、本実施形態のクライアントＰＣ２００およびサーバには一般的な情報処理装置のハードウェア構成を適用できる。
【００１７】
図２０において、ＣＰＵ２０１は、ＲＯＭ２０３のプログラム用ＲＯＭに記憶された、或いはハードディスク２１１からＲＡＭ２０２にロードされたＯＳやアプリケーション等のプログラムを実行する。ここでＯＳとはコンピュータ上で稼動するオペレーティングシステムの略語であり、以下オペレーティングシステムのことをＯＳと呼ぶ。後述する各フローチャートの処理はこのプログラムの実行により実現できる。ＲＡＭ２０２は、ＣＰＵ２０１の主メモリ、ワークエリア等として機能する。キーボードコントローラ（ＫＢＣ）２０５は、キーボード（ＫＢ）２０９や不図示のポインティングデバイスからのキー入力を制御する。ＣＲＴコントローラ（ＣＲＴＣ）２０６は、ＣＲＴディスプレイ２１０の表示を制御する。ディスクコントローラ（ＤＫＣ）２０７は各種データを記憶するハードディスク（ＨＤ）２１１やフロッピー（登録商標）ディスク（ＦＤ）等におけるデータアク

セスを制御する。ＮＣ２１２はネットワークに接続されて、ネットワークに接続された他の機器との通信制御処理を実行する。

【００１８】

尚、後述の全ての説明においては、特に断りのない限り実行のハード上の主体はＣＰＵ２０１であり、ソフトウェア上の主体はハードディスク（ＨＤ）２１１にインストールされたアプリケーションプログラムである。

【００１９】

図２は本実施の形態に係るモジュール構成図である。３００は認証サービス決定サービスで、４００は認証サービスＡ、４５０は認証サービスＢである。２つの認証サービスはいずれもＩｄＰとして機能するが、ＩｄＰが１つであっても良い。少なくとも１つ以上のＩｄＰが存在すれば、本発明は実施可能である。また、５００はサービス提供サービスである。また、実施例１においては、認証サービス決定サービス３００、または認証サービスＡ４００、またはサービス提供サービス５００がＳＰ（サービスプロバイダ装置）となる。ＳＰは、ＩｄＰとシングルサインオン連携を行う。

【００２０】

図２（Ａ）は本実施の形態に係る認証サービス決定サービス３００のモジュール構成図である。認証サービス決定サービス３００は管理モジュール３０１、キー取り出しモジュール３０２、取得モジュール３０３、アクセス誘導モジュール３０４を備える。管理モジュール３０１は認証装置を決定するキーとなる情報と、認証装置の情報とを紐付けて記憶する。認証サービス決定サービス３００が未認証のユーザからのアクセスを受け付けると、キー取り出しモジュール３０２は認証装置を決定するキーとなる情報を、ユーザがアクセスした際に提供される情報から取り出す。取得モジュール３０３は取り出したキーとなる情報を用いて、管理モジュール３０１から認証装置の情報を取得する。アクセス誘導モジュール３０４は取り出した認証装置の情報に従い、ユーザを適切な認証サービスにアクセスするように誘導する。

【００２１】

図２（Ｂ）は本実施の形態に係る認証サービスＡ４００のモジュール構成図である。認証サービスＡ４００はサービスＡ認証モジュール４０１とアサーション検証モジュール４０２を備える。

【００２２】

認証サービスＡ４００が未認証のアクセスを受け付けると、図１０（Ａ）に示すような画面を提示し、ユーザにユーザＩＤとパスワードの入力を促し認証を行う。またＳＳＯを実現させるために、認証サービスＡ４００が他認証サービスにより提供された認証の証拠をユーザのアクセスから受け取ると、アサーション検証モジュール４０２が証拠、即ち認証結果の妥当性を検証し、ユーザのアクセスを承認するか否かを決定する。なお本実施例において認証の証拠はＳＡＭＬアサーションを想定するが、本発明のＳＳＯはＳＡＭＬおよびＳＡＭＬアサーションを用いたものに限定されるものではない。

【００２３】

図２（Ｃ）は本実施の形態に係る認証サービスＢ４５０のモジュール構成図である。認証サービスＢ４５０は、サービスＢ認証モジュール４５１とアサーション発行モジュール４５２を備える。

【００２４】

認証サービスＢ４５０が未認証のアクセスを受け付けると、図１０（Ｂ）に示すような画面を提示し、ユーザにユーザＩＤとパスワードの入力を促し認証を行う。認証に成功するとアサーション発行モジュール４５２が認証の証拠となるＳＡＭＬアサーションを生成し、アサーションの検証を行うことが可能な認証サービスへ、ユーザのアクセスをリダイレクトさせる。なお本実施例において前記認証の証拠はＳＡＭＬアサーションを想定するが、本発明のＳＳＯはＳＡＭＬおよびＳＡＭＬアサーションを用いたものに限定されるものではない。

【００２５】

図２（Ｄ）は本実施の形態に係るサービス提供サービス５００のモジュール構成図である。サービス提供サービス５００はアクセス拒否モジュール５０１とサービス提供モジュール５０２を備える。サービス提供サービス５００がアクセスを受け付けると、ユーザのアクセスが認証済みであるか否かをアクセス拒否モジュール５０１が判断し、未認証のアクセスを認証サービス決定サービス３００へリダイレクトさせる。またアクセスが認証済みであればサービス提供モジュール５０２がサービスを提供する。ここでサービス提供モジュール５０２が提供するサービスとしては、たとえばインターネット上の共有ストレージに文書を蓄積する、文書蓄積サービスなどがある。なおサービス提供モジュール５０２が提供するサービスは文書蓄積サービスに限定されるものではない。

【００２６】

図３は本実施の形態に係る、認証装置を決定するキーとなる情報としてユーザＩＤを利用する場合の認証サービス決定サービス３００のモジュール構成図である。認証サービス決定サービス３００は第２の管理モジュール３１１、キー取り出しモジュール３０２、取得モジュール３０３、アクセス誘導モジュール３０４を備える。第２の管理モジュール３１１はユーザＩＤと、そのユーザが認証を受ける認証装置の情報とを紐付けて記憶する。図４は本実施の形態に係る、第２の管理モジュール３１１が管理する情報である。管理情報６００はユーザＩＤと、そのユーザが認証を受ける認証装置の情報（各ＩｄＰのアドレス情報）とを関連付けて保存・管理を行う。ここではたとえばユーザＩＤ「ｕｓｅｒ００１」と「ｕｓｅｒ００３」は認証サービスＢ４５０と、ユーザＩＤ「ｕｓｅｒ００２」は認証サービスＡ４００とそれぞれ紐付けられている様子を示している。なお、認証サービスＢ４５０は、認証サービスＡ４００とＳＳＯを実現していることを想定している。図５は本実施の形態に係る、サービス提供サービス５００が実行するフローである。本フローは、サービスを受けようとするユーザがサービス提供サーバ５００にアクセスすることによって始まる。

【００２７】

ステップＳ１１０１でサービス提供サーバ５００はユーザのアクセスを受け付ける。ステップＳ１１０２でサービス拒否モジュール５０１はステップＳ１１０１で受け付けたアクセスが認証済みであるか否かを判断する。認証済みであればステップＳ１１０３に遷移し、未認証であればステップＳ１１５１に遷移する。

【００２８】

ステップＳ１１０３でサービス提供モジュール５０２は、ステップＳ１１０２で認証済みと判断されたアクセスに対してサービスを提供し、フローを終了する。ステップＳ１１５１でアクセス拒否モジュール５０１は、ステップＳ１１０２で未認証と判断されたアクセスを、認証サービス決定サービス３００へとリダイレクトさせる。なおその際、認証の完了後に再度サービス提供サービス５００にアクセスするよう情報を付加しておく。情報を付加してリダイレクトが済むと、フローが終了する。図６は本実施の形態に係る、認証サービス決定サービス３００が実行するフローである。本フローは、ユーザが直接認証サービス決定サービスにアクセスするか、ユーザのアクセスがサービス提供サービス５００からリダイレクトされることによって始まる。なおアクセスのリダイレクト元はサービス提供サービス５００に限定されるものではない。

【００２９】

ステップＳ１２０１で認証サービス決定サービス３００は、未認証のユーザアクセスを受け付ける。ステップＳ１２０２でキー取り出しモジュール３０２は、未認証のユーザアクセスのＵＲＬパラメーターからユーザＩＤを抽出する。なおユーザＩＤはＵＲＬパラメーター以外の情報から取得してもよい。また、ＵＲＬの前半部分は夫々のサーバへアクセスするためのＵＲＬになっており、ＵＲＬの後半部分がユーザＩＤ、または後述する企業ＩＤを特定するためのキー情報となっている。このＵＲＬの特性を活かし、後半部分のキー情報のみ変更し、変更したＵＲＬを使用することで、アクセス先を変更せずに、認証先のみを変更することも可能となる。

【００３０】

ステップＳ１２０３で取得モジュール３０３は、ステップＳ１２０２で取得したユーザＩＤを用い、第２の管理モジュール３１１から、前記ユーザＩＤに紐付けられた認証装置のアドレス情報を取得する。ここでたとえば、ステップＳ１２０２で取り出したユーザＩＤが「ｕｓｅｒ００１」であれば、認証サービス決定サービス３００は、それと一致するユーザＩＤを検索し、そのユーザＩＤに関連した認証サービスＢ４５０のＵＲＬ「ｈｔｔｐ：／／ｓｅｒｖｉｃｅ＿ｂ／？ｓｐ＝ｈｔｔｐ％３Ａ％２Ｆ％２Ｆｓｅｒｖｉｃｅ＿ａ％２Ｆ」を特定する。この例のＵＲＬは認証サービスＢ４５０と認証サービスＡ４００がＳＳＯする場合を想定している。ステップＳ１２０４でアクセス誘導モジュール３０４は、ステップＳ１２０３で取得した装置情報に従い、未認証のユーザのアクセスをリダイレクトさせるため、クライアントへＰＣ１００へ特定したＵＲＬを送信する。なおその際、ステップＳ１２０１で認証完了後のアクセス先情報を受け取っていれば、ここでも前記情報を付加してリダイレクトさせる。リダイレクトが済むとフローが終了する。図７は本実施の形態に係る、ＳＳＯを実現する際の認証サービスＢ４５０におけるフローである。本フローはユーザのアクセスが認証サービス決定サービス３００からリダイレクトされることによって始まる。

【００３１】

ステップＳ１５０１で認証サービスＢ４５０は、認証サービス決定サービス３００からリダイレクトされた認証要求を受け付ける。また認証成功時のリダイレクト先をＵＲＬから取得する。この例では「？ｓｐ＝ｈｔｔｐ％３Ａ％２Ｆ％２Ｆｓｅｒｖｉｃｅ＿ａ％２Ｆ」の部分がリダイレクト先を表している。ステップＳ１５０２でサービスＢ認証モジュール４５１は、図１０（Ｂ）で示されるような認証画面７５０を表示させる。ステップＳ１５０３でサービスＢ認証モジュール４５１は、認証画面７５０で入力された認証情報が正しいか確認する。認証情報が正しければステップＳ１５０４に遷移し、正しくなければステップＳ１５５１に遷移する。

【００３２】

ステップＳ１５０４でアサーション発行モジュール４５２は、ステップ１５０３で正しいと判断された認証情報に対応するアサーションを発行する。なお、アサーションをクレデンシャルと称する場合もある。アサーションを発行するとステップＳ１５０１で取得したリダイレクト先ＵＲＬにユーザのアクセスをリダイクトさせる。なおその際、ステップＳ１５０１で認証完了後のアクセス先情報を受け取っていれば、ここでも前記情報を付加してリダイレクトさせる。リダイレクトが済むとフローが終了する。

【００３３】

ステップＳ１５５１でサービスＢ認証モジュール４５１は、認証画面７５０で入力された認証情報が正しくないため認証失敗した旨を通知する画面を表示させ、フローを終了する。ここでクライアントＰＣ２００は、サービスＢ認証モジュール４５１から送信された認証失敗画面を表示する。この画面は再度ステップＳ１５０２に遷移させユーザから認証情報を受け付ける画面であってもよく、また単に認証に失敗したことを示すだけの画面であってもよい。またそのいずれかに限定されるものでもない。この時点ではユーザのアクセスは未認証状態であるため、ユーザが継続してサービス提供サービス５００にアクセスしようとしても、アクセスできない。その場合は図５に示されるフローが実施される

図８は本実施の形態に係る、ＳＳＯを実現する際の認証サービスＡ４００におけるフローである。本フローはユーザのアクセスが認証サービスＢ４５０で認証に成功し、リダイレクトされることによって始まる。

【００３４】

ステップＳ１６０１で認証サービスＡ４００は、認証サービスＢ４５０からのリダイレクトを受け付ける。ステップＳ１６０２でアサーション検証モジュール４０２は、ステップＳ１６０１で受け付けたリダイレクトに含まれるアサーションが妥当なものか検証する。検証の結果、妥当であると判断された場合はステップＳ１６０３に遷移する。また妥当でないと判断された場合はステップＳ１６５１に遷移する。

【００３５】

ステップＳ１６０３でサービスＡ認証モジュール４０１は、ステップＳ１６０１で受け付けたリダイレクトを認証し、サービスへのアクセスを許可する。ここで、ステップＳ１６０１で認証完了後のアクセス先情報を受け取っていれば、その情報にもとづいてユーザのアクセスをリダイレクトさせる。たとえば認証完了後のリダイレクト先としてサービス提供サービス５００が指定されていた場合は、ユーザのアクセスをサービス提供サービス５００にリダイレクトさせる。このとき、すでにユーザのアクセスは認証が済んでいるため、ユーザはサービス提供サービス５００が提供するサービスを受けることができる。リダイレクトが済むとフローが終了する。ステップＳ１６５１でサービスＡ認証モジュール４０１は、アサーションが妥当でなかったため認証失敗した旨を通知する画面を表示させ、フローを終了する。

【００３６】

図９は本実施の形態に係る、ＳＳＯを実施しない際の認証サービスＡ４００におけるフローである。本フローはユーザのアクセスが認証サービス決定サービス３００からリダイレクトされることによって始まる。なお本フローにおいては、サービス提供サービス５００と同一セキュリティードメインに存在する認証サービスＡ４００がユーザのアクセスを認証する。ここでは認証サービスＢ４５０はユーザのアクセスの認証を行わない。

【００３７】

ステップＳ１７０１で認証サービスＡ４００は、認証サービス決定サービス３００からリダイレクトされた認証要求を受け付ける。ステップＳ１７０２でサービスＡ認証モジュール４０１は、図１０（Ａ）で示されるような認証画面７００を表示させる。ステップＳ１７０３でサービスＡ認証モジュール４０１は、認証画面７００で入力された認証情報が正しいか確認する。認証情報が正しければステップＳ１７０４に遷移し、正しくなければステップＳ１７５１に遷移する。

【００３８】

ステップＳ１７０４でサービスＡ認証モジュール４０１は、ステップＳ１７０１で受け付けたリダイレクトを認証し、サービスへのアクセスを許可する。ここで、ステップＳ１７０１で認証完了後のアクセス先情報を受け取っていれば、その情報にもとづいてユーザのアクセスをリダイレクトさせる。たとえば認証完了後のリダイレクト先としてサービス提供サービス５００が指定されていた場合は、ユーザのアクセスをサービス提供サービス５００にリダイレクトさせる。このとき、すでにユーザのアクセスは認証が済んでいるため、ユーザはサービス提供サービス５００が提供するサービスを受けることができる。リダイレクトが済むとフローが終了する。ステップＳ１７５１でサービスＡ認証モジュール４０１は、認証画面７００で入力された認証情報が正しくないため認証失敗した旨を通知する画面を表示させ、フローを終了する。

【００３９】

図１０は本実施の形態に係る、認証情報の入力画面である。図１０（Ａ）は認証サービスＡ４００がユーザのアクセスを認証するための認証情報入力画面であり、ユーザＩＤ入力欄およびパスワード入力欄を持つ。図１０（Ｂ）は認証サービスＢ４５０がユーザのアクセスを認証するための認証情報入力画面であり、ユーザＩＤ入力欄およびパスワード入力欄を持つ。

【００４０】

本実施の形態によれば、未認証のユーザアクセスを、ユーザＩＤに従い適切なＩｄＰに誘導させ、ユーザが認証を受けられるようになる。なおＳＳＯ連携しているＩｄＰの一覧表示や共通リポジトリは必要ない。

【実施例２】

【００４１】

次に、本発明を実施するための第２の形態について図面を用いて説明する。なお第１の実施の形態と共通の部分については説明を省略し、以下では差異部分のみ説明する。

【００４２】

図１１は本実施の第２の形態に係る、認証装置を決定するキーとなる情報としてユーザ

のグループ識別子を利用する場合の認証サービス決定サービス３００のモジュール構成図である。なおここでユーザのグループ識別子として企業ＩＤを用いているが、ユーザのグループ識別子は企業ＩＤに限定されるものではない。認証サービス決定サービス３００は第３の管理モジュール３２１、キー取り出しモジュール３０２、取得モジュール３０３、アクセス誘導モジュール３０４を備える。企業ＩＤは、本システムを利用する法人単位に一意に割り当てられた固有情報であり、テナントＩＤとも称する。第３の管理モジュール３２１は企業ＩＤと、そのユーザが認証を受ける認証装置の情報とを紐付けて記憶する。

【００４３】

図１２は本実施の第２の形態に係る、第３の管理モジュール３２１が管理する情報である。管理情報６５０は企業ＩＤと、その企業ＩＤに関連する企業に属しているユーザが認証を受ける認証サーバの情報とが紐付けられている。ここではたとえば企業ＩＤ「１１１１１１１１」と「３３３３３３３３」は認証サービスＢ４５０と、ユーザＩＤ「２２２２２２２２」は認証サービスＡ４００とそれぞれ紐付けられている様子を示す。なおここで認証サービスＢ４５０は、認証サービスＡ４００とＳＳＯを実現していることを想定している。

【００４４】

図１３は本実施の第２の形態に係る、認証サービス決定サービス３００が実行するフローである。本フローは、ユーザが直接認証サービス決定サービスにアクセスするか、ユーザのアクセスがサービス提供サービス５００からリダイレクトされることによって始まる。なおアクセスのリダイレクト元はサービス提供サービス５００に限定されるものではない。

【００４５】

ステップＳ１２１１で認証サービス決定サービス３００は、未認証のユーザアクセスを受け付ける。ステップＳ１２１２でキー取り出しモジュール３０２は未認証のユーザアクセスのＵＲＬパラメーターから企業ＩＤを抽出する。なお企業ＩＤはＵＲＬパラメーター以外の情報から取得してもよい。この抽出した企業ＩＤがキー情報となる。

【００４６】

ステップＳ１２１３で取得モジュール３０３は、ステップＳ１２１２で取得した企業ＩＤを用い、第３の管理モジュール３２１から、企業ＩＤに紐付けられた認証装置の情報を取得する。ここでたとえば、ステップＳ１２１２で取り出した企業ＩＤが「１１１１１１１１」であれば取得できる装置情報は認証サービスＢ４５０のＵＲＬ「ｈｔｔｐ：／／ｓｅｒｖｉｃｅ＿ｂ／？ｓｐ＝ｈｔｔｐ％３Ａ％２Ｆ％２Ｆｓｅｒｖｉｃｅ＿ａ％２Ｆ」である。この例のＵＲＬは認証サービスＢ４５０と認証サービスＡ４００がＳＳＯする場合を想定している。

【００４７】

ステップＳ１２１４でアクセス誘導モジュール３０４は、ステップＳ１２１３で取得した装置情報に従い、未認証のユーザアクセスをリダイレクトさせる。なおその際、ステップＳ１２１１で認証完了後のアクセス先情報を受け取っていれば、ここでも前記情報を付加してリダイレクトさせる。リダイレクトが済むとフローが終了する。

【００４８】

本実施の第２の形態によれば、未認証のユーザアクセスを、ユーザのグループ識別子に従い適切なＩｄＰに誘導させ、ユーザが認証を受けられるようになる。なおＳＳＯ連携しているＩｄＰの一覧表示や共通リポジトリは必要ない。

【実施例３】

【００４９】

次に、本発明を実施するための第３の形態について図面を用いて説明する。
なお第２の実施の形態と共通の部分については説明を省略し、以下では差異部分のみ説明する。

【００５０】

図１４は本実施の第３の形態に係る認証サービス決定サービス３００のモジュール構成

図である。なおここで第３の管理モジュール３２１を用い、認証装置を決定するキーとなる情報として企業ＩＤを用いている。しかし認証装置を決定するキーとなる情報は企業ＩＤに限定されるものではない。認証サービス決定サービス３００は第３の管理モジュール３２１、キー取り出しモジュール３０２、取得モジュール３０３、アクセス誘導モジュール３０４を備える。また、判断モジュール３３１、要求モジュール３３２、第２のキー取り出しモジュール３３３、第２の取得モジュール３３４、第２のアクセス誘導モジュール３３５を備える。

【００５１】

認証サービス決定サービス３００が未認証のユーザからのアクセスを受け付けると、判断モジュール３３１はユーザアクセスのパラメーターに企業ＩＤが含まれるか否かを判断し、含まれない場合は要求モジュール３３２が企業ＩＤを要求する画面を表示させる。第２のキー取り出しモジュール３３３は画面で入力された企業ＩＤを取り出す。第２の取得モジュール３３４は前記取り出した企業ＩＤを用いて、第３の管理モジュール３２１から認証装置の情報を取得する。第２のアクセス誘導モジュール３３５は前記取り出した認証装置の情報に従い、認証サービス決定サービス３００に対するユーザのアクセスを適切な認証サービスに誘導する。

【００５２】

図１５は本実施の第３の形態に係る、認証サービス決定サービス３００が実行するフローである。なお、図１３と同様のフローにおいては、同じ符号を付与しており、以下、差異部分のみ説明する。本フローは、ユーザが直接認証サービス決定サービスにアクセスするか、ユーザのアクセスがサービス提供サービス５００からリダイレクトされることによって始まる。なおアクセスのリダイレクト元はサービス提供サービス５００に限定されるものではない。

【００５３】

ステップＳ１３０１で認証サービス決定サービス３００は、未認証のユーザアクセスを受け付ける。ステップＳ１３０２で判断モジュール３３１は、未認証のユーザアクセスのＵＲＬパラメーターに企業ＩＤが含まれるか判断する。企業ＩＤが含まれていると判断された場合はステップＳ１２１２に遷移し、含まれていないと判断された場合はステップＳ１３０３に遷移する。なお企業ＩＤはＵＲＬパラメーター以外の情報から取得してもよい。ステップＳ１３０３で要求モジュール３３２は、図１６に示されるような企業ＩＤ入力画面８００を表示させる。

【００５４】

ステップＳ１３０４で第２の取り出しモジュール３３３は、企業ＩＤ入力画面８００で入力された企業ＩＤを取り出す。ステップＳ１３０５で第２の取得モジュール３３４は、ステップＳ１３０４で取得した企業ＩＤを用い、第３の管理モジュール３２１から、前記企業ＩＤに紐付けられた認証装置の情報を取得する。ここでたとえば、ステップＳ１３０４で取り出した企業ＩＤが「１１１１１１１１」であれば取得できる装置情報は認証サービスＢ４５０のＵＲＬ「ｈｔｔｐ：／／ｓｅｒｖｉｃｅ＿ｂ／？ｓｐ＝ｈｔｔｐ％３Ａ％２Ｆ％２Ｆｓｅｒｖｉｃｅ＿ａ％２Ｆ」である。この例のＵＲＬは認証サービスＢ４５０と認証サービスＡ４００がＳＳＯする場合を想定している。

【００５５】

ステップＳ１３０６で第２のアクセス誘導モジュール３３５は、ステップＳ１３０５で取得した装置情報に従い、未認証のユーザアクセスをリダイレクトさせる。なおその際、ステップＳ１３０１で認証完了後のアクセス先情報を受け取っていれば、ここでも前記情報を付加してリダイレクトさせる。リダイレクトが済むとフローが終了する。図１６は本実施の第３の形態に係る、企業ＩＤの入力画面である。ユーザは本画面で、自身が所属する企業の企業ＩＤを入力することができる。

【００５６】

本実施の第３の形態によれば、未認証のユーザアクセスに認証装置を決定するキーとなる情報が含まれなかった場合でも、認証装置を決定するキーとなる情報の入力をユーザに

促すことができる。したがって、未認証のユーザアクセスを適切なＩｄＰに誘導させ、ユーザが認証を受けられるようになる。

【実施例４】

【００５７】

次に、本発明を実施するための第４の形態について図面を用いて説明する。なお第３の実施の形態と共通の部分については説明を省略し、以下では差異部分のみ説明する。図１７は本実施の第４の形態に係る認証サービス決定サービス３００のモジュール構成図である。なおここで第３の管理モジュール３２１を用い、認証装置を決定するキーとなる情報として企業ＩＤを用いている。しかし認証装置を決定するキーとなる情報は企業ＩＤに限定されるものではない。認証サービス決定サービス３００は第３の管理モジュール３２１、キー取り出しモジュール３０２、取得モジュール３０３、アクセス誘導モジュール３０４を備える。また判断モジュール３３１、要求モジュール３３２、第２のキー取り出しモジュール３３３、第２の取得モジュール３３４、第２のアクセス誘導モジュール３３５を備える。また指示受付モジュール３４１と第３のアクセス誘導モジュール３４２を備える。

【００５８】

認証サービス決定サービス３００が未認証のユーザからのアクセスを受け付けると、指示受付モジュール３４１はユーザアクセスのパラメーターに認証サービスの指定を有効にしているか否かを確認する。確認の結果指定されていた場合は第３のアクセス誘導モジュール３４２がユーザのアクセスを指定の認証サービスに誘導する。

【００５９】

図１８は本実施の第４の形態に係る、認証サービス決定サービス３００が実行するフローである。なお、図１５と同様のフローにおいては、同じ符号を付与しており、以下、差異部分のみ説明する。本フローは、ユーザが直接認証サービス決定サービスにアクセスするか、ユーザのアクセスがサービス提供サービス５００からリダイレクトされることによって始まる。なおアクセスのリダイレクト元はサービス提供サービス５００に限定されるものではない。本フローは特に、次のケースを想定している。すなわち、そのユーザが所属する企業では認証サービスＢ４５０で認証を受け、ＳＳＯで認証サービスＡ４００の認証を受けることになっている。しかしなんらかの事情により認証サービスＢ４５０側にアカウントを持たず、したがって認証サービスＡ４００でＳＳＯによる認証を受けられないユーザが、認証サービスＡで直接認証を受ける必要がある場合である。例えば、企業の中の管理者がこれに当てはまる。管理者は、認証サービスＢ４５０のサービスを受ける必要がないため、認証サービスＢ４５０に認証情報を登録しておかない場合もある。

【００６０】

ステップＳ１４０１で認証サービス決定サービス３００は、未認証のユーザアクセスを受け付ける。ステップＳ１４０２で指示受付モジュール３４１は、未認証のユーザアクセスのＵＲＬパラメーターに認証サービスの指定が含まれるか否かを判断する。含まれていないと判断した場合はステップＳ１４０３に遷移し、含まれていると判断した場合はステップＳ１４１１に遷移する。

【００６１】

ステップＳ１４０３で判断モジュール３３１は、未認証のユーザアクセスのＵＲＬパラメーターにキー情報となる企業ＩＤが含まれているか否かを判断する。企業ＩＤが含まれていると判断された場合はステップＳ１２１２に遷移し、含まれていないと判断された場合はステップＳ１４０４に遷移する。なお企業ＩＤはＵＲＬパラメーター以外の情報から取得してもよい。ステップＳ１４０４で要求モジュール３３２は、図１９に示されるような企業ＩＤ入力画面８５０を表示させる。

【００６２】

ステップＳ１４０５で指示受付モジュール３４１は、企業ＩＤ入力画面８５０で特定の認証サービスが指定されていたか判断する。たとえばここでは、「認証サービスＡで認証を受ける」のチェックボックスがＯＮであったか判断する。特定の認証サービスが指定さ

れていないと判断された場合はステップＳ１３０４に遷移し、指定されていると判断した場合はステップＳ１４１１に遷移する。

【００６３】

ステップＳ１４１１で第３のアクセス誘導モジュール３４２は、ステップＳ１４０２またはステップＳ１４０４の指定に従い、未認証のユーザアクセスをリダイレクトさせる。なおその際、ステップＳ１４０１で認証完了後のアクセス先情報を受け取っていれば、ここでも前記情報を付加してリダイレクトさせる。リダイレクトが済むとフローが終了する。

【００６４】

図１９は本実施の第４の形態に係る、企業ＩＤの入力画面である。ユーザは本画面で、自身が所属する企業の企業ＩＤを入力することができる。また、なんらかの事情により認証サービスＡ４００で認証を受けたいユーザは、「認証サービスAで認証を受ける」のチェックボックスをＯＮにすることができる。すると入力した企業ＩＤに紐付けられた認証サービスの設定に関わらず、認証サービスAで認証を受けることができるようになる。

【００６５】

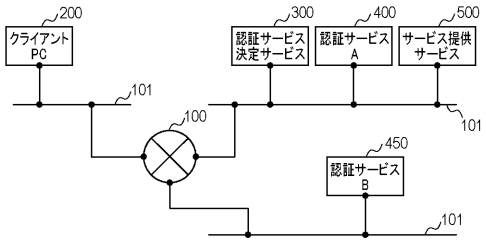
本実施の第４の形態によれば、ユーザが特定の認証サービスでの認証を希望する場合、認証装置を決定するキーとなる情報に関わらず、ユーザのアクセスを指定されたＩｄＰに誘導させ、ユーザが認証を受けられるようになる。

【符号の説明】

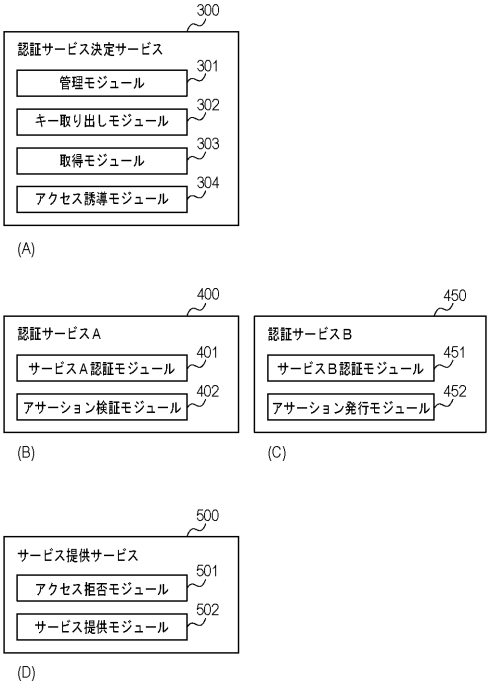
【００６６】

１００　ＷＡＮ
１０１　ＬＡＮ
２００　クライアントＰＣ
３００　認証サービス決定サービス
４００　認証サービスＡ
４５０　認証サービスＢ
５００　サービス提供サービス

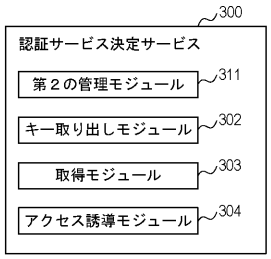
【図１】



【図２】



【図３】

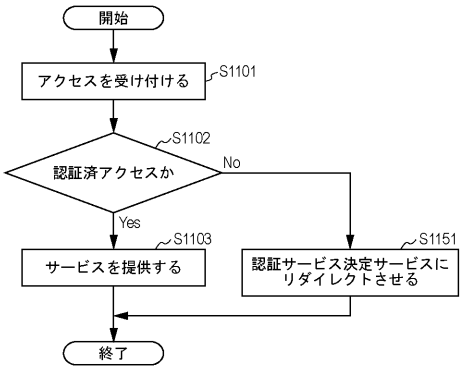


【図４】

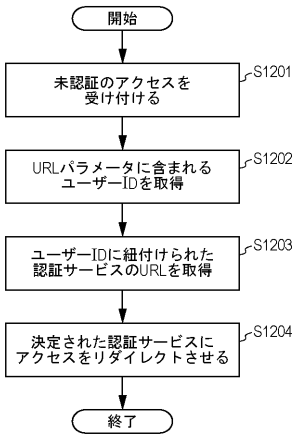
600

ユーザID	IdPのURL
user001	http://service_b/?sp=http%3A%2F%2Fservice_a%2F
user002	http://service_a/
user003	http://service_b/?sp=http%3A%2F%2Fservice_a%2F
:	:

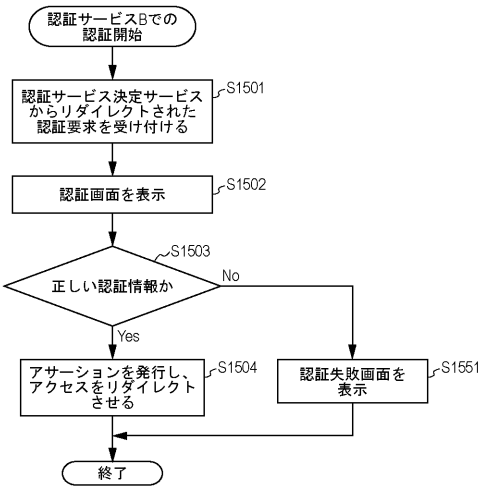
【図５】


開始
アクセスを受け付ける
S1101
認証済アクセスか
S1102
No
Yes
サービスを提供する
S1103
認証サービス決定サービスに
リダイレクトさせる
S1151
終了

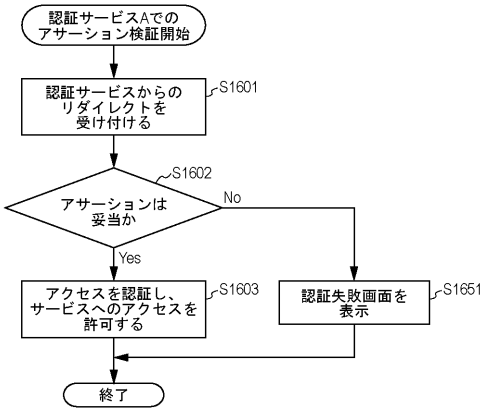
【図６】


開始
未認証のアクセスを
受け付ける
S1201
URLパラメータに含まれる
ユーザーIDを取得
S1202
ユーザーIDに紐付けられた
認証サービスのURLを取得
S1203
決定された認証サービスに
アクセスをリダイレクトさせる
S1204
終了

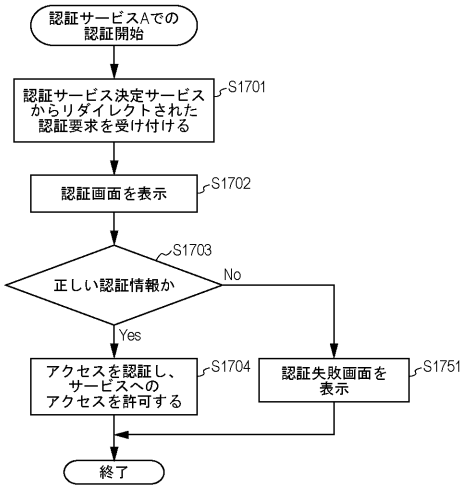
【図７】


認証サービスBでの
認証開始
認証サービス決定サービス
からリダイレクトされた
認証要求を受け付ける
S1501
認証画面を表示
S1502
正しい認証情報か
S1503
No
Yes
アサーションを発行し、
アクセスをリダイレクト
させる
S1504
認証失敗画面を
表示
S1551
終了

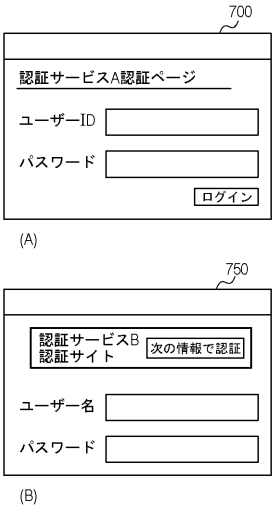
【図８】


認証サービスAでの
アサーション検証開始
認証サービスからの
リダイレクトを
受け付ける
S1601
アサーションは
妥当か
S1602
No
Yes
アクセスを認証し、
サービスへのアクセスを
許可する
S1603
認証失敗画面を
表示
S1651
終了

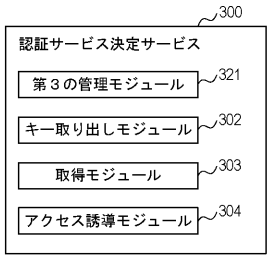
【図９】



【図１０】



【図１１】

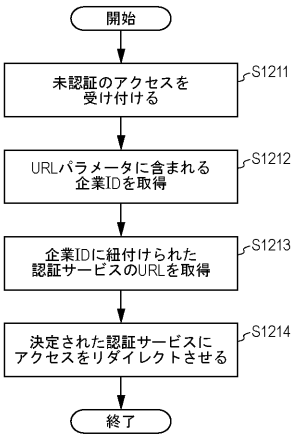


【図１２】

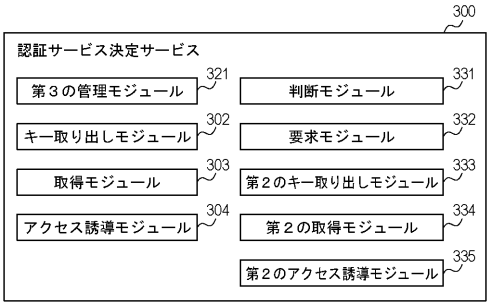
650

企業ID	IdPのURL
11111111	http://service_b/?sp=http%3A%2F%2Fservice_a%2F
22222222	http://service_a/
33333333	http://service_b/?sp=http%3A%2F%2Fservice_a%2F
:	:

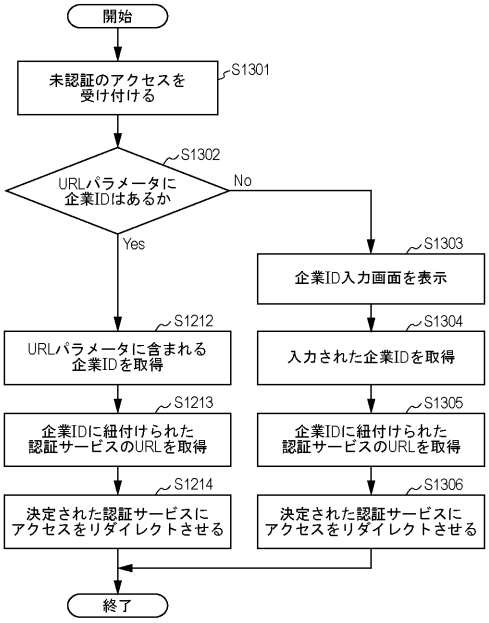
【図１３】



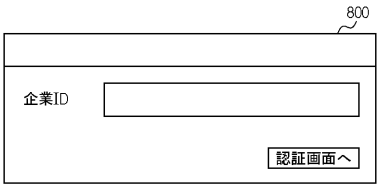
【図１４】



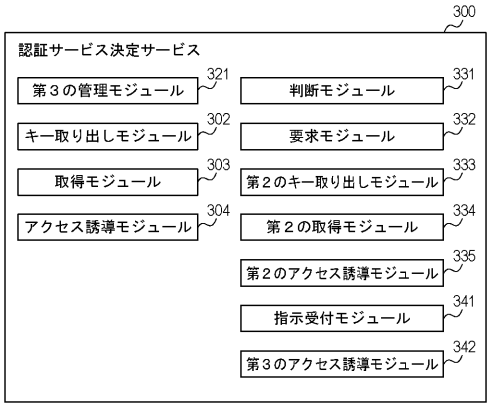
【図１５】



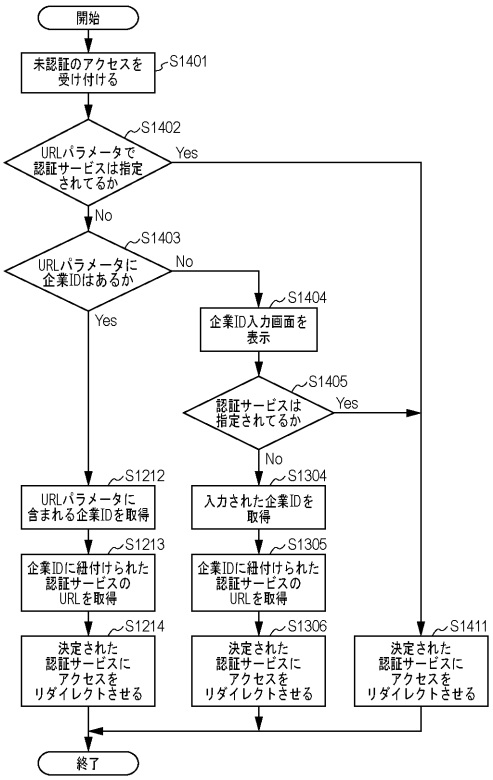
【図１６】



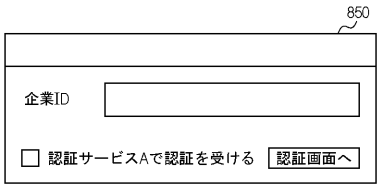
【図１７】



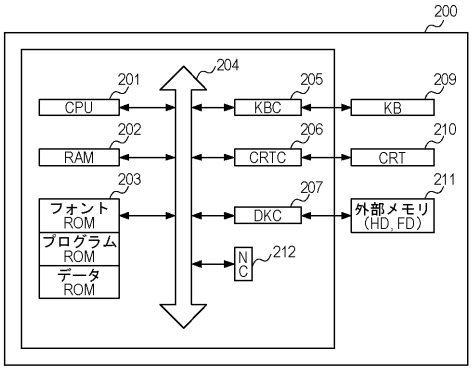
【図１８】



【図１９】



【図２０】



フロントページの続き

(56)参考文献 特開２００７－３１０５１２（ＪＰ，Ａ）
特開２０１０－１２８７１９（ＪＰ，Ａ）
特開２００１－２２２５０８（ＪＰ，Ａ）
特開２００７－２１９９３５（ＪＰ，Ａ）
特開平１１－２８２８０４（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／４１
Ｇ０６Ｆ　２１／３１
Ｈ０４Ｌ　９／３２