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

特許第5170648号
(P5170648)

(45)発行日　平成25年3月27日(2013.3.27)　(24)登録日　平成25年1月11日(2013.1.11)

(51)Int.Cl.		F I		
G06F 21/41	(2013.01)	G06F	21/20	141
G06F 21/33	(2013.01)	G06F	21/20	133
G06F 21/34	(2013.01)	G06F	21/20	134
H04L 9/32	(2006.01)	H04L	9/00	675D

請求項の数 9　(全 32 頁)

(21)出願番号　特願2008-45784(P2008-45784)
(22)出願日　平成20年2月27日(2008.2.27)
(65)公開番号　特開2009-205342(P2009-205342A)
(43)公開日　平成21年9月10日(2009.9.10)
審査請求日　平成23年1月14日(2011.1.14)

(73)特許権者　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(73)特許権者　504132272
国立大学法人京都大学
京都府京都市左京区吉田本町３６番地１
(74)代理人　100089118
弁理士　酒井　宏明
(74)代理人　100112656
弁理士　宮田　英毅
(72)発明者　橋本　正一
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

最終頁に続く

(54)【発明の名称】権限委譲システム、権限委譲方法および権限委譲プログラム

(57)【特許請求の範囲】
【請求項１】
アプリケーションサーバ各々を利用する利用者の本人性を認証サーバが認証する構成の下、所定のアプリケーションサーバを利用する権限を他の利用者から委譲された利用者について当該利用者の権限を判定し、当該利用者による当該アプリケーションサーバの利用を制御する権限委譲システムであって、
利用者の本人性を確認可能な情報を格納する格納媒体に、当該格納媒体を利用する利用者が他の利用者から委譲された権限に関する権限委譲情報を格納する格納手段を備え、
前記認証サーバは、
所定のアプリケーションサーバへアクセスすることを要求するアクセス要求を利用者が利用する利用者端末から受け付けた際に、当該利用者が利用する格納媒体に格納されている情報に基づいて当該利用者の本人性を認証するとともに、前記格納手段によって当該格納媒体に格納された権限委譲情報もしくは当該権限委譲情報から導出される情報を、当該アクセス要求にて指定されたアプリケーションサーバに転送する権限委譲情報転送手段を備え、
前記アプリケーションサーバ各々は、
前記権限委譲情報転送手段によって転送された前記権限委譲情報もしくは前記情報を受け付けると、当該権限委譲情報もしくは当該情報から、委譲された権限の内容を抽出し、抽出した当該内容を確認することで、当該権限委譲情報を格納する格納媒体の利用者の権限を判定する判定手段と、

を備えたことを特徴とする権限委譲システム。
【請求項２】
前記権限委譲情報は、委譲の対象となるアプリケーションの種別、および／または、委譲の範囲により、複数のパターンで定義されるものであって、
前記格納手段は、前記複数のパターンの内のいずれかのパターンを、前記権限委譲情報として前記格納媒体に格納することを特徴とする請求項１に記載の権限委譲システム。
【請求項３】
前記格納手段は、権限を他の利用者に委譲する権限委譲者を識別する利用者ＩＤと、権限を委譲される被権限委譲者を識別する利用者ＩＤと、委譲の対象となるアプリケーションの種別および／または委譲の範囲により定義される権限委譲情報のパターンと、当該委譲が有効である有効期限とを、当該権限委譲者によって指定されることで、前記権限委譲情報として前記格納媒体に格納することを特徴とする請求項１または２に記載の権限委譲システム。
【請求項４】
前記権限委譲システムは、発行局サーバと登録局サーバと失効リストリポジトリサーバと登録端末とから構成されるものであって、
前記発行局サーバは、
利用者の本人性を確認するための利用者証明書を発行する利用者証明書発行手段と、
前記権限委譲情報を確認するための権限委譲証明書を発行する権限委譲証明書発行手段とを備え、
前記登録局サーバは、
前記利用者証明書および前記権限委譲証明書の発行申請を受け付ける申請受付手段と、
前記申請受付手段によって受け付けた利用者証明書の発行を前記発行局サーバに要求する利用者証明書発行要求手段と、
前記申請受付手段によって受け付けた権限委譲証明書の発行を前記発行局サーバに要求する権限委譲証明書発行要求手段と、
前記利用者証明書発行手段によって発行された利用者証明書を取得し、当該利用者証明書を申請した利用者が利用する前記登録端末に対して、当該利用者証明書を送信する利用者証明書送信手段と、
前記権限委譲証明書発行手段によって発行された権限委譲証明書を取得し、当該権限委譲証明書によって権限を委譲された利用者が利用する所定の端末に対して、当該権限委譲証明書を送信する権限委譲証明書送信手段とを備え、
前記失効リストリポジトリサーバは、
前記利用者証明書および／または前記権限委譲証明書が失効しているか否かをアプリケーションサーバに通知する通知手段を備え、
前記登録端末は、
前記利用者証明書送信手段によって送信された利用者証明書を取得する利用者証明書取得手段を備え、
前記所定の端末は、
前記権限委譲証明書送信手段によって送信された権限委譲証明書を取得する権限委譲証明書取得手段を備えたことを特徴とする請求項１～３のいずれか一つに記載の権限委譲システム。
【請求項５】
前記登録端末は、
権限を他の利用者に委譲する権限委譲者を識別する利用者ＩＤ、権限を委譲される被権限委譲者を識別する利用者ＩＤ、委譲の対象となるアプリケーションの種別および／または委譲の範囲により定義される権限委譲情報のパターン、および当該委譲が有効である有効期限の指定を権限委譲者から受け付け、前記登録局サーバに送信することで、権限委譲証明書の発行申請を行う権限委譲証明書申請手段を備え、
前記登録局サーバは、

前記権限委譲者の本人性を、当該権限委譲者が利用する格納媒体に格納された利用者証明書により認証する第１の利用者認証手段と、
前記第１の利用者認証手段によって前記権限委譲者の本人性が認証されたことを条件として、前記権限委譲証明書申請手段によって申請された権限委譲証明書の発行を、前記発行局サーバに送信する権限委譲証明書発行要求手段と、
前記被権限委譲者の本人性を、当該被権限委譲者が利用する格納媒体に格納された利用者証明書により認証する第２の利用者認証手段と、
前記第２の利用者認証手段によって前記被権限委譲者の本人性が認証されたことを条件として、当該被権限委譲者が利用する所定の端末に権限委譲証明書を送信する権限委譲証明書送信手段とを備え、
前記発行局サーバの権限委譲証明書発行手段は、前記権限委譲証明書申請手段によって受け付けられた情報に基づいて、前記権限委譲証明書を発行することを特徴とする請求項４に記載の権限委譲システム。
【請求項６】
前記認証サーバは、
他の利用者から権限を委譲された被権限委譲者の本人性を、当該被権限委譲者が利用する格納媒体に格納された利用者証明書により認証する認証手段を備え、
前記アプリケーションサーバは、
前記認証手段によって前記被権限委譲者の本人性が確認されたことを条件として、当該被権限委譲者が利用する格納媒体に格納された権限委譲証明書を要求する権限委譲証明書要求手段と、
前記権限委譲証明書要求手段によって要求した権限委譲証明書を取得すると、前記被権限委譲者に委譲された権限が有効期限を経過しているか否か、および、当該権限が失効しているか否かを確認する第１の確認手段と、
前記第１の確認手段によって、権限の有効期限を経過していないこと、および、当該権限が失効していないことが確認されたことを条件として、当該委譲の対象および委譲の範囲を確認し、前記被権限委譲者に対して当該アプリケーションサーバを利用する権限を認可するか否かを決定する第２の確認手段と、
を備えたことを特徴とする請求項１～５のいずれか一つに記載の権限委譲システム。
【請求項７】
アプリケーションサーバ各々を利用する利用者の本人性を認証サーバが認証する構成の下、所定のアプリケーションサーバを利用する権限を他の利用者から委譲された利用者について当該利用者の権限を判定し、当該利用者による当該アプリケーションサーバの利用を制御する権限委譲方法であって、
利用者の本人性を確認可能な情報を格納する格納媒体に、当該格納媒体を利用する利用者が他の利用者から委譲された権限に関する権限委譲情報を格納する格納工程を含み、
前記認証サーバは、
所定のアプリケーションサーバへアクセスすることを要求するアクセス要求を利用者が利用する利用者端末から受け付けた際に、当該利用者が利用する格納媒体に格納されている情報に基づいて当該利用者の本人性を認証するとともに、前記格納工程によって当該格納媒体に格納された権限委譲情報もしくは当該権限委譲情報から導出される情報を、当該アクセス要求にて指定されたアプリケーションサーバに転送する権限委譲情報転送工程を含み、
前記アプリケーションサーバ各々は、
前記権限委譲情報転送工程によって転送された前記権限委譲情報もしくは前記情報を受け付けると、当該権限委譲情報もしくは当該情報から、委譲された権限の内容を抽出し、抽出した当該内容を確認することで、当該権限委譲情報を格納する格納媒体の利用者の権限を判定する判定工程と、
を含んだことを特徴とする権限委譲方法。
【請求項８】

アプリケーションサーバ各々を利用する利用者の本人性を認証サーバが認証する構成の下、所定のアプリケーションサーバを利用する権限を他の利用者から委譲された利用者について当該利用者の権限を判定し、当該利用者による当該アプリケーションサーバの利用を制御する権限委譲方法をコンピュータに実行させる権限委譲プログラムであって、

利用者の本人性を確認可能な情報を格納する格納媒体に、当該格納媒体を利用する利用者が他の利用者から委譲された権限に関する権限委譲情報を格納する格納手順をコンピュータに実行させ、

前記認証サーバとしてのコンピュータに、

所定のアプリケーションサーバへアクセスすることを要求するアクセス要求を利用者が利用する利用者端末から受け付けた際に、当該利用者が利用する格納媒体に格納されている情報に基づいて当該利用者の本人性を認証するとともに、前記格納手順によって当該格納媒体に格納された権限委譲情報もしくは当該権限委譲情報から導出される情報を、当該アクセス要求にて指定されたアプリケーションサーバに転送する権限委譲情報転送手順を実行させ、

前記アプリケーションサーバ各々としてのコンピュータに、

前記権限委譲情報転送手順によって転送された前記権限委譲情報もしくは前記情報を受け付けると、当該権限委譲情報もしくは当該情報から、委譲された権限の内容を抽出し、抽出した当該内容を確認することで、当該権限委譲情報を格納する格納媒体の利用者の権限を判定する判定手順と、

を実行させることを特徴とする権限委譲プログラム。

【請求項９】

アプリケーションサーバ各々を利用する利用者の本人性を認証サーバが認証する構成の下、所定のアプリケーションサーバを利用する権限を他の利用者から委譲された利用者について当該利用者の権限を判定し、当該利用者による当該アプリケーションサーバの利用を制御する権限委譲方法であって、

利用者の本人性を確認可能な情報を格納する格納媒体に、当該格納媒体を利用する利用者が他の利用者から委譲された権限に関する権限委譲情報であって、前記アプリケーションサーバにおいて委譲された権限の内容が抽出され、抽出された当該内容が確認されることで、当該格納媒体の利用者の権限が判定される権限委譲情報を格納する格納工程を含んだことを特徴とする権限委譲方法。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、権限委譲システム、権限委譲方法および権限委譲プログラムに関する。

【背景技術】

【０００２】

教育機関や企業等でのサービス・業務の電子化は急速に進展しつつあり、クライアント－サーバによるＷＥＢアプリケーションが利用されている。これらのサービス・業務のアプリケーションリソースに利用者がアクセスするには、アクセスしようとする本人性の確認が必要なことから、ＩＤとパスワード、ＩＣカード、電子証明書、バイオメトリックスを用いた本人性の確認行為、すなわち、個人認証が行われている（非特許文献１、非特許文献２を参照）。

【０００３】

図１４に、従来のサービス・業務のアプリケーションごとの認証処理の概要を示す。個人認証は、通常、サービスや業務ごとに行われることから、それぞれの認証サーバが、ＩＤ払い出し機能によりＩＤおよび初期パスワードを発行し、認証情報を管理するためのディレクトリデータベースにこれらの情報を格納するとともに、これらの情報を利用者に電子メールや通知書等により通知する。利用者は、なりすましを防止するため、各認証サーバに対して初期パスワードの変更登録を実施し、以降、自己責任によりこれを管理・運用しなければならない。

【０００４】
一方、アプリケーション側が利用者に対して、サービス・業務アプリケーションのリソース使用を許可する認可処理については、個人認証処理が認可と等価であったため、認証と認可は一体として扱われ、利用者およびアプリケーション側は認可を意識することはなかった。
【０００５】
ところが、利用者の立場で、複数のＩＤやパスワードを管理・運用することは繁雑であり、せっかくの電子化のメリットとなるべき利便性を損なっている。このため、利用者の利便性向上、ＩＤとパスワードの漏洩等によるなりすましリスクの抑制、アプリケーション側の視点からは、ＩＤとパスワードの管理コストの低減、および、認証システムの設備投資や運用作業量の抑制などを実現するため、個人認証を複数のサービス・業務で一括して行うシングルサインオンといった認証方式が導入されつつある。
【０００６】
シングルサインオン認証は、一度の認証で、複数のサービス・業務を収容するポータル画面に遷移し、以降、シングルログアウトするまで、ポータルに提示されたサービス・業務のアプリケーションにアクセスできるという認証方式である。図１５に、ＩＤおよびパスワードによるシングルサインオン認証処理の流れを示す。利用者は、ポータルのＵＲＬ（Uniform Resource Locator）をクライアント端末に入力し、クライアント端末は、認証サーバへポータルへのアクセス要求を行う。すると、認証サーバは、クライアント端末へ認証情報を要求し、利用者は、ＩＤおよびパスワードをクライアント端末に入力する。そして、クライアント端末は、ＩＤおよびパスワードを認証サーバへ送信し、認証サーバは、ディレクトリデータベースの認証情報とマッチングを行い、本人性を判定する。この結果、正しいと判定されれば、認証サーバは、クライアント端末へポータルのＵＲＬアクセスを許可し、シングルサインオン認証処理が完了する。
【０００７】
この機能により、利用者は、複数のサービス・業務ごとにＩＤおよびパスワードを覚えることから解放され、利便性が著しく向上する。一方、バックエンドのアプリケーション側も、ＩＤの発行やそれに伴うＩＤのライフサイクル管理が一元化される。また、サービス・業務ごとに行っていたサービス・業務の個人認証という行為は大幅に軽減され、認証システムの開発・保守におけるコストや運用稼動の分割損も大きく改善される。
【０００８】
【非特許文献１】“ベリサインマネージドＰＫＩ”、［online］、［平成２０年２月６日検索］、インターネット＜http://www.verisign.co.jp/mpki/solution/authdevice/companyid.html＞
【非特許文献２】“ＩＤ管理システム「GreenOffice Directory」”、［online］、［平成２０年２月６日検索］、インターネット＜http://www.kccs.co.jp/products/directory/index.html＞
【発明の開示】
【発明が解決しようとする課題】
【０００９】
ところで、上記した従来の技術では、権限を他の利用者に委譲する権限委譲者から、権限を他の利用者から委譲される被権限委譲者に対して、権限を適切に委譲することができないという課題があった。
【００１０】
すなわち、上記してきたように、利用者やアプリケーションサーバ側にとっての利便性向上、ＩＤライフサイクル管理の軽減、認証機能の開発・運用などのコスト低減の観点から、シングルサインオン認証は非常に有効である。ところが、例えば、教育機関や企業における予算権限あるいは業務権限を有する教職員あるいは部課長以上の利用者は、多忙なため、バックエンドアプリケーションへアクセスする権限を、部下あるいは秘書などへ委譲しているという実態があるが、その多くは、ＩＤおよびパスワードを被権限委譲者に教

えるといったレベルであり、ミスや不正利用に対して非常にリスクの高いものであった。
【００１１】
また、適切な権限委譲の一つの方法として、個別のサービス・業務のアプリケーションに対して、利用者が被権限委譲者を決め、対象業務、委譲範囲、有効期限を通知するといった処理が必要であった。この方法は、権限を委譲する利用者の負担が大きいことと同時に、アプリケーションサーバ側の審査などの負担が大きくなるといった課題があった。別の方法として、シングルサインオン認証に利用するディレクトリデータベースに権限委譲に関わる認可情報を登録する方法もあるが、権限を委譲する利用者の負担が大きいことに加えて、ディレクトリデータベースを更新する作業が増えるとともに、アプリケーション側と連携して内容を確認するといった作業も増えるなど、トータルな仕事量が増えるといった課題があった。
【００１２】
さらに、権限を委譲した利用者本人の異動や委譲された人が異動した際には、異動した利用者本人が、失効をアプリケーションサーバ側あるいはディレクトリデータベースに対して迅速に申請しなければならない。これらの更新処理も、アプリケーションサーバ側あるいはディレクトリデータベースにとって大きな負担となっていた。
【００１３】
そこで、この発明は、上記した従来技術の課題を解決するためになされたものであり、権限を適切に委譲することが可能な権限委譲システム、権限委譲方法および権限委譲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】
【００１４】
上述した課題を解決し、目的を達成するため、本発明は、アプリケーションサーバ各々を利用する利用者の本人性を認証サーバが認証する構成の下、所定のアプリケーションサーバを利用する権限を他の利用者から委譲された利用者について当該利用者の権限を判定し、当該利用者による当該アプリケーションサーバの利用を制御する権限委譲システムであって、利用者の本人性を確認可能な情報を格納する格納媒体に、当該格納媒体を利用する利用者が他の利用者から委譲された権限に関する権限委譲情報を格納する格納手段を備え、前記認証サーバは、所定のアプリケーションサーバへアクセスすることを要求するアクセス要求を利用者が利用する利用者端末から受け付けた際に、当該利用者が利用する格納媒体に格納されている情報に基づいて当該利用者の本人性を認証するとともに、前記格納手段によって当該格納媒体に格納された権限委譲情報もしくは当該権限委譲情報から導出される情報を、当該アクセス要求にて指定されたアプリケーションサーバに転送する権限委譲情報転送手段を備え、前記アプリケーションサーバ各々は、前記権限委譲情報転送手段によって転送された前記権限委譲情報もしくは前記情報を受け付けると、当該権限委譲情報もしくは当該情報から、委譲された権限の内容を抽出し、抽出した当該内容を確認することで、当該権限委譲情報を格納する格納媒体の利用者の権限を判定する判定手段と、を備えたことを特徴とする。
【００１５】
また、本発明は、上記の発明において、前記権限委譲情報は、委譲の対象となるアプリケーションの種別、および／または、委譲の範囲により、複数のパターンで定義されるものであって、前記格納手段は、前記複数のパターンの内のいずれかのパターンを、前記権限委譲情報として前記格納媒体に格納することを特徴とする。
【００１６】
また、本発明は、上記の発明において、前記格納手段は、権限を他の利用者に委譲する権限委譲者を識別する利用者ＩＤと、権限を委譲される被権限委譲者を識別する利用者ＩＤと、委譲の対象となるアプリケーションの種別および／または委譲の範囲により定義される権限委譲情報のパターンと、当該委譲が有効である有効期限とを、当該権限委譲者によって指定されることで、前記権限委譲情報として前記格納媒体に格納することを特徴とする。

【００１７】
また、本発明は、上記の発明において、前記権限委譲システムは、発行局サーバと登録局サーバと失効リストリポジトリサーバと登録端末とから構成されるものであって、前記発行局サーバは、利用者の本人性を確認するための利用者証明書を発行する利用者証明書発行手段と、前記権限委譲情報を確認するための権限委譲証明書を発行する権限委譲証明書発行手段とを備え、前記登録局サーバは、前記利用者証明書および前記権限委譲証明書の発行申請を受け付ける申請受付手段と、前記申請受付手段によって受け付けた利用者証明書の発行を前記発行局サーバに要求する利用者証明書発行要求手段と、前記申請受付手段によって受け付けた権限委譲証明書の発行を前記発行局サーバに要求する権限委譲証明書発行要求手段と、前記利用者証明書発行手段によって発行された利用者証明書を取得し、当該利用者証明書を申請した利用者が利用する前記登録端末に対して、当該利用者証明書を送信する利用者証明書送信手段と、前記権限委譲証明書発行手段によって発行された権限委譲証明書を取得し、当該権限委譲証明書によって権限を委譲された利用者が利用する所定の端末に対して、当該権限委譲証明書を送信する権限委譲証明書送信手段とを備え、前記失効リストリポジトリサーバは、前記利用者証明書および／または前記権限委譲証明書が失効しているか否かをアプリケーションサーバに通知する通知手段を備え、前記登録端末は、前記利用者証明書送信手段によって送信された利用者証明書を取得する利用者証明書取得手段を備え、前記所定の端末は、前記権限委譲証明書送信手段によって送信された権限委譲証明書を取得する権限委譲証明書取得手段を備えたことを特徴とする。
【００１８】
また、本発明は、上記の発明において、前記登録端末は、権限を他の利用者に委譲する権限委譲者を識別する利用者ＩＤ、権限を委譲される被権限委譲者を識別する利用者ＩＤ、委譲の対象となるアプリケーションの種別および／または委譲の範囲により定義される権限委譲情報のパターン、および当該委譲が有効である有効期限の指定を権限委譲者から受け付け、前記登録局サーバに送信することで、権限委譲証明書の発行申請を行う権限委譲証明書申請手段を備え、前記登録局サーバは、前記権限委譲者の本人性を、当該権限委譲者が利用する格納媒体に格納された利用者証明書により認証する第１の利用者認証手段と、前記第１の利用者認証手段によって前記権限委譲者の本人性が認証されたことを条件として、前記権限委譲証明書申請手段によって申請された権限委譲証明書の発行を、前記発行局サーバに送信する権限委譲証明書発行要求手段と、前記被権限委譲者の本人性を、当該被権限委譲者が利用する格納媒体に格納された利用者証明書により認証する第２の利用者認証手段と、前記第２の利用者認証手段によって前記被権限委譲者の本人性が認証されたことを条件として、当該被権限委譲者が利用する所定の端末に権限委譲証明書を送信する権限委譲証明書送信手段とを備え、前記発行局サーバの権限委譲証明書発行手段は、前記権限委譲証明書申請手段によって受け付けられた情報に基づいて、前記権限委譲証明書を発行することを特徴とする。
【００１９】
また、本発明は、上記の発明において、前記認証サーバは、他の利用者から権限を委譲された被権限委譲者の本人性を、当該被権限委譲者が利用する格納媒体に格納された利用者証明書により認証する認証手段を備え、前記アプリケーションサーバは、前記認証手段によって前記被権限委譲者の本人性が確認されたことを条件として、当該被権限委譲者が利用する格納媒体に格納された権限委譲証明書を要求する権限委譲証明書要求手段と、前記権限委譲証明書要求手段によって要求した権限委譲証明書を取得すると、前記被権限委譲者に委譲された権限が有効期限を経過しているか否か、および、当該権限が失効しているか否かを確認する第１の確認手段と、前記第１の確認手段によって、権限の有効期限を経過していないこと、および、当該権限が失効していないことが確認されたことを条件として、当該委譲の対象および委譲の範囲を確認し、前記被権限委譲者に対して当該アプリケーションサーバを利用する権限を認可するか否かを決定する第２の確認手段と、を備えたことを特徴とする。
【００２０】

また、本発明は、アプリケーションサーバ各々を利用する利用者の本人性を認証サーバが認証する構成の下、所定のアプリケーションサーバを利用する権限を他の利用者から委譲された利用者について当該利用者の権限を判定し、当該利用者による当該アプリケーションサーバの利用を制御する権限委譲方法であって、利用者の本人性を確認可能な情報を格納する格納媒体に、当該格納媒体を利用する利用者が他の利用者から委譲された権限に関する権限委譲情報を格納する格納工程を含み、前記認証サーバは、所定のアプリケーションサーバへアクセスすることを要求するアクセス要求を利用者が利用する利用者端末から受け付けた際に、当該利用者が利用する格納媒体に格納されている情報に基づいて当該利用者の本人性を認証するとともに、前記格納工程によって当該格納媒体に格納された権限委譲情報もしくは当該権限委譲情報から導出される情報を、当該アクセス要求にて指定されたアプリケーションサーバに転送する権限委譲情報転送工程を含み、前記アプリケーションサーバ各々は、前記権限委譲情報転送工程によって転送された前記権限委譲情報もしくは前記情報を受け付けると、当該権限委譲情報もしくは当該情報から、委譲された権限の内容を抽出し、抽出した当該内容を確認することで、当該権限委譲情報を格納する格納媒体の利用者の権限を判定する判定工程と、を含んだことを特徴とする。

【００２１】

また、本発明は、アプリケーションサーバ各々を利用する利用者の本人性を認証サーバが認証する構成の下、所定のアプリケーションサーバを利用する権限を他の利用者から委譲された利用者について当該利用者の権限を判定し、当該利用者による当該アプリケーションサーバの利用を制御する権限委譲方法をコンピュータに実行させる権限委譲プログラムであって、利用者の本人性を確認可能な情報を格納する格納媒体に、当該格納媒体を利用する利用者が他の利用者から委譲された権限に関する権限委譲情報を格納する格納手順をコンピュータに実行させ、前記認証サーバとしてのコンピュータに、所定のアプリケーションサーバへアクセスすることを要求するアクセス要求を利用者が利用する利用者端末から受け付けた際に、当該利用者が利用する格納媒体に格納されている情報に基づいて当該利用者の本人性を認証するとともに、前記格納手順によって当該格納媒体に格納された権限委譲情報もしくは当該権限委譲情報から導出される情報を、当該アクセス要求にて指定されたアプリケーションサーバに転送する権限委譲情報転送手順を実行させ、前記アプリケーションサーバ各々としてのコンピュータに、前記権限委譲情報転送手順によって転送された権限委譲情報もしくは前記情報を受け付けると、当該権限委譲情報もしくは当該情報から、委譲された権限の内容を抽出し、抽出した当該内容を確認することで、当該権限委譲情報を格納する格納媒体の利用者の権限を判定する判定手順と、を実行させることを特徴とする。

【００２２】

また、本発明は、アプリケーションサーバ各々を利用する利用者の本人性を認証サーバが認証する構成の下、所定のアプリケーションサーバを利用する権限を他の利用者から委譲された利用者について当該利用者の権限を判定し、当該利用者による当該アプリケーションサーバの利用を制御する権限委譲方法であって、利用者の本人性を確認可能な情報を格納する格納媒体に、当該格納媒体を利用する利用者が他の利用者から委譲された権限に関する権限委譲情報であって、前記アプリケーションサーバにおいて委譲された権限の内容が抽出され、抽出された当該内容が確認されることで、当該格納媒体の利用者の権限が判定される権限委譲情報を格納する格納工程を含んだことを特徴とする。

【発明の効果】

【００２３】

本発明によれば、格納媒体に権限委譲情報を格納し、アプリケーションサーバが、当該権限委譲情報に基づいて被権限委譲者の権限を判定するので、権限を適切に委譲することが可能になる。

【発明を実施するための最良の形態】

【００２４】

以下に添付図面を参照して、この発明に係る権限委譲システム、権限委譲方法および権

限委譲プログラムの実施例を詳細に説明する。なお、以下では、前提技術、実施例１に係る権限委譲システムの概要および特徴、実施例１に係る権限委譲システムの構成、実施例１に係る権限委譲システムによる処理の手順、実施例１の効果について順に説明し、次に、他の実施例について説明する。

【実施例１】

【００２５】

［前提技術］

従来のシングルサインオン認証は、サービスや業務のアプリケーションを提供する提供者にとって、認証した利用者全てにサービス・業務のリソースへのアクセスを許可する場合には問題ないが、個人認証をパスした一部の人にリソースへのアクセス権限を設定する場合には、バックエンドのアプリケーション側が、対象とするリソースへのアクセスを許可するか否かといった認可をしなくてはならない。その具体的方法として、次のようなことが行われる。

【００２６】

（１）特定のアプリケーションのリソースにアクセスできる人のＩＤをアプリケーションの利用者管理サーバに格納し、個人認証時に確認したＩＤを基に、アクセスの許可（認可）を与え、利用者にリソースを提示する。もし、アクセス権が無い人であれば、個人認証処理後に、「○○業務に登録されていません」といった注意文がメッセージとして表示される。

【００２７】

（２）認証を行う際に利用されるディレクトリデータベースに、ＩＤおよびパスワード以外の情報として、アプリケーション側の認可に必要な情報を付加し、認証判定後にバックエンドアプリケーション側にこれらの認可情報を提示し、アプリケーション側で認可判定する。この認可情報で判定条件が満たさなければ、「○○業務に登録されていません」といった注意文がメッセージとして表示される。

【００２８】

最近、サービス・業務の効率化に大きく貢献する電子化が進むにつれ、発生源入力が求められ、教育機関の教職員や企業の部課長などの予算権限や業務権限を有した利用者も、多忙に関わらず自分で入力することが求められる。しかし、多忙のため入力処理ができず、結果として、電子的な組織内処理の遅れによるビジネスなど機会損失が発生することが危惧されている。それゆえ、秘書や部下などによる代行入力によって対応されているが、情報セキュリティの観点からの適切な権限委譲はあまり行われていない。具体的には、アクセス権限を保有している利用者が、ＩＤおよびパスワードを部下や秘書に教えて対応していることが多い。これは、一種の「なりすまし」であり、不正利用やミスがあった場合の対応ができなくなるという問題がある。

【００２９】

従って、本来、電子的な方法で、(1)誰に（権限委譲される人）、(2)どのサービス・業務に対して（対象業務）、(3)申請だけかあるいは決裁も含めるかといった内容（委譲範囲）、(4)いつまで委譲するのか（有効期限）、などを明確にした上で、アクセス権限を適正な人へ委譲しなければならない。また、(5)委譲した利用者が異動等によりその権限を失効した場合には、委譲された利用者の権限も同時に失効するといった仕組み（失効処理）が必要となる。

【００３０】

「なりすまし」でない権限委譲は、基本的に、権限を有した利用者が、委譲先の利用者登録を新たに申請することで行われる。この時、サービス・業務のアプリケーション側は、申請者の本人確認および権限委譲先の本人確認を行った上で、申請内容について審査しなければならない。シングルサインオン認証では、複数のサービス・業務の収容を前提としているため、権限を委譲しようとする利用者は、対象とするサービス・業務のアプリケーションすべてに対して、権限を委譲される人、権限委譲範囲、有効期限などを申請しなければならず、多忙ゆえに権限委譲を行おうとするのに反して、一層多忙になるといった

問題があった。また、異なったサービス・業務に対して、それぞれ異なった複数の人に委譲した場合、あるいは、一つのサービス・業務のアクセス権限を複数の人に委譲する場合には処理が一層増えるといった問題が発生した。さらに、権限を有する本人が異動した場合、あるいは、委譲された利用者が異動した場合など、委譲した権利を失効させる作業を申請ベースでタイムリーに行うことは困難な場合が多かった。

【００３１】

一方、認証のディレクトリデータベースに権限委譲を登録する場合、該当するデータベースの一元的な集中管理が前提となる。この場合でも、権限委譲のフラグを追記したりなどの作業は、人事異動などによるデータベースの更新に加えて行われることが多いため、権限委譲の処理が遅れたり、認可に必要な情報をアプリケーション側と連携しつつ審査するといった処理により、管理コストと作業量が膨大になってしまうといった問題があった。

【００３２】

権限を委譲する立場の利用者と委譲された利用者とに関わる繁雑な処理を、サービス・業務のアプリケーション全てに対して行わなければならない。加えて、サービス・業務のアプリケーション側は、申請された処理に対して、申請者の本人確認、権限委譲先の本人確認、申請内容の審査を行わなければならない。一方、ディレクトリデータベースに権限委譲による認可情報を付加する場合でも、予算権限やアクセス権限を認識している利用者が申請し、データベース管理者もアプリケーション側と確認の上、データ追記を行う必要があり、通常の更新作業に加えて、非常に多くの作業負荷が発生していた。

【００３３】

このような方法では、権限を委譲する利用者の数が多いほど、あるいは、対象となるアプリケーションの数が多いほど、これらの権限委譲処理に関する作業量は急激に増え、登録および失効に関するミスやトラブルが発生するといった問題もあった。特に、シングルサインオン認証では、複数のサービス・業務の利用が前提となっているため、このような負担の著しい増加は明らかであった。

【００３４】

上記してきたように、シングルサインオン認証は、複数のサービス・業務について、一度だけ認証することにより、許可されたサービス・業務に対してアクセスでき、利用者にとって利便性が大きく向上している。一方、バックエンドのアプリケーション側にとっても、利用者のＩＤ管理を一元化でき、ライフサイクル管理を容易にしており、認証システムの開発・運用・保守を軽減するといった大きなメリットがある。

【００３５】

このような状況の中、発生源入力といったサービス・業務の効率化の観点から、予算権限や業務権限を有した教職員や部課長以上の利用者も電子的な入力が必要であるが、多忙なためその権限を部下あるいは秘書などへ適切に委譲するには、利用者本人の作業量が増えたり、アプリケーション側の負荷が増大したり、データベース更新の作業量が増えるなど、大きな問題となっていた。そのため、シングルサインオン認証とアプリケーション側の認可において、利用者およびアプリケーション側のメリットを低下させず、予算権限や業務権限に精通している利用者が安全に安心して権限を委譲できる方式が強く望まれていた。

【００３６】

［実施例１に係る権限委譲システムの概要および特徴］

まず、図１を用いて、実施例１に係る権限委譲システムの概要および特徴を説明する。図１は、実施例１に係る権限委譲システムの概要および特徴を説明するための図である。

【００３７】

シングルサインオン認証における個人認証の手法として、ＩＣカード等の格納媒体に格納した利用者証明書によって利用者の本人性を確認する手法がある（サービス・業務のシングルサインオン認証において、通常、ＩＤおよびパスワードを使って認証するが、複数のサービス・業務が利用できることもあり、よりセキュアなＩＣカードとＰＩＮによる多

要素認証を利用する例が増えてきつつある）。かかる手法による場合、利用者は、利用者のみの操作によって利用者証明書の発行を受け、ＩＣカード等の格納媒体に格納する。

【００３８】

ここで、実施例１に係る権限委譲システムは、利用者証明書をＩＣカード等の格納媒体に格納する手順をそのまま踏襲する。すなわち、権限を委譲する利用者は、当該利用者のみの操作によって権限委譲証明書（権限を委譲する利用者のＩＤ、権限を委譲される利用者のＩＤ、権限委譲の対象となるサービス・業務、権限委譲の作業範囲、権限委譲の有効期限等の権限委譲情報を含む）の発行を受け、権限を委譲される利用者の利用者証明書を格納したＩＣカード等の格納媒体に、当該権限委譲証明書を併せて格納する。そして、シングルサインオン認証後のバックエンドアプリケーション側の認可判定の際、バックエンドアプリケーションサーバは、ＩＣカード等の格納媒体に格納された権限委譲情報に基づいて、権限を委譲される利用者の権限を判定する。

【００３９】

図１を用いて簡単に説明する。実施例１において、権限を委譲する利用者のことを「権限委譲者」と呼び、権限を委譲される利用者のことを「被権限委譲者」と呼ぶ。図１に示すように、実施例１における認証用ＩＣカード１２（特許請求の範囲に記載の「格納媒体」に対応する）は、権限委譲者、被権限委譲者各々が保持するものである。また、認証用ＩＣカード１２各々は、権限委譲者、被権限委譲者各々の利用者証明書（利用者の本人性を確認可能な情報を含む）を格納する。

【００４０】

ここで、利用者証明書を認証用ＩＣカード１２に格納する手順を簡単に説明すると、実施例１においては、図１に示すように、プライベート発行局サーバ７と、登録局（ＲＡ）サーバ８と、ＲＡ端末１０と、カード発行機（図示を省略）とから主に構成されるシステムを想定する。このようなシステムにおいて、ＲＡ端末１０は、利用者によって操作されることで登録局（ＲＡ）サーバ８にアクセスし、利用者証明書の発行申請情報を送信する。続いて、登録局（ＲＡ）サーバ８は、ＲＡ端末１０から送信された発行申請情報の正当性を確認し、プライベート発行局サーバ７に対して利用者証明書の発行を要求する。すると、プライベート発行局サーバ７は、利用者証明書を発行し、登録局（ＲＡ）サーバ８に送信する。次に、登録局（ＲＡ）サーバ８は、ＲＡ端末１０から利用者証明書ダウンロード要求を受け付け、ＲＡ端末１０に対して利用者証明書を送信する。すると、ＲＡ端末１０は、カード発行機に対して利用者証明書を送信し、カード発行機は、認証用ＩＣカード１２に利用者証明書を書き込む。

【００４１】

ところで、実施例１に係る権限委譲システムは、権限委譲情報についても、上記した手順をそのまま踏襲して、認証用ＩＣカード１２に格納する（図１の（１）を参照）。権限委譲証明書を認証用ＩＣカード１２に格納する手順を簡単に説明すると、実施例１に係る権限委譲システムは、利用者証明書を発行する際のシステムと同じシステムにおいて、ＲＡ端末１０は、権限委譲者によって操作されることで登録局（ＲＡ）サーバ８にアクセスし、権限委譲証明書の発行申請情報を送信する。続いて、登録局（ＲＡ）サーバ８は、ＲＡ端末１０から送信された発行申請情報の正当性を確認し、プライベート発行局サーバ７に対して権限委譲証明書の発行を要求する。すると、プライベート発行局サーバ７は、権限委譲証明書を発行し、登録局（ＲＡ）サーバ８に送信する。次に、登録局（ＲＡ）サーバ８は、被権限委譲者が操作するＲＡ端末１０から権限委譲証明書ダウンロード要求を受け付け、被権限委譲者が操作するＲＡ端末１０に対して権限委譲証明書を送信する。すると、当該ＲＡ端末１０は、リーダライタ１３に対して権限委譲証明書を送信し、リーダライタ１３は、被権限委譲者の認証用ＩＣカード１２に、権限委譲証明書を書き込む。

【００４２】

さて、実施例１に係る権限委譲システムは、被権限委譲者の認証用ＩＣカード１２に格納された権限委譲情報に基づいて、被権限委譲者の権限を判定する。具体的には、まず、クライアント端末１が、バックエンドアプリケーションサーバ５へアクセスすることを要

求するアクセス要求を認証サーバ３に送信すると（図１の（２）を参照）、認証サーバ３は、被権限委譲者の認証用ＩＣカード１２に格納されている利用者証明書に基づいて、当該被権限委譲者の本人性を認証するとともに、当該認証用ＩＣカード１２に格納された権限委譲情報を、当該アクセス要求にて指定されたバックエンドアプリケーションサーバ５に転送する（図１の（３）を参照）。

【００４３】

すると、バックエンドアプリケーションサーバ５は、認証サーバ３から転送された権限委譲情報を受け付けると、当該権限委譲情報に基づいて、認証用ＩＣカード１２の利用者の権限を判定する（図１の（４）を参照）。

【００４４】

このように、実施例１に係る権限委譲システムは、認証用ＩＣカード１２に権限委譲情報を格納し、バックエンドアプリケーションサーバ５が、当該権限委譲情報に基づいて被権限委譲者の権限を判定するので、権限を適切に委譲することが可能になる。

【００４５】

［実施例１に係る権限委譲システムの構成］

次に、図２および図３を用いて、実施例１に係る権限委譲システムの構成を説明する。図２および図３は、実施例１に係る権限委譲システムの構成を示すブロック図である。なお、以下では、ＲＡ端末１０、ＩＣカード発行機１１、登録局（ＲＡ）サーバ８、プライベート発行局サーバ７、クライアント端末１、認証サーバ３、バックエンドアプリケーションサーバ５を順に説明する。

【００４６】

［ＲＡ端末１０］

図２に示すように、実施例１におけるＲＡ端末１０は、本発明に特に密接に関連するものとして、登録局サーバアクセス部１０ａと、利用者認証部１０ｂと、証明書発行申請情報投入部１０ｃと、利用者証明書ダウンロード部１０ｄと、証明書データ送信部１０ｅと、権限委譲証明書ダウンロード部１０ｆとを備える。

【００４７】

登録局サーバアクセス部１０ａは、登録局（ＲＡ）サーバ８にアクセスする機能を備えた部である。具体的には、登録局サーバアクセス部１０ａは、利用者（権限委譲者、被権限委譲者など）によってＲＡ端末１０が操作されることで登録局（ＲＡ）サーバ８にアクセスする。例えば、登録局（ＲＡ）サーバ８がＷｅｂサーバとしての機能を備えている場合、登録局サーバアクセス部１０ａは、ＲＡ端末１０上のブラウザソフト（以下、ブラウザ）で実現可能であり、登録局（ＲＡ）サーバ８に対してＨＴＴＰ（HyperText Transfer Protocol）通信を行うことで、登録局（ＲＡ）サーバ８にアクセスすることができる。

【００４８】

利用者認証部１０ｂは、登録局（ＲＡ）サーバ８との間で利用者認証を行う機能を備えた部である。具体的には、利用者認証部１０ｂは、登録局（ＲＡ）サーバ８の利用者認証部８ａとの間で、ＲＡ端末１０を操作している利用者の本人性を認証することを目的として利用者認証を行う。例えば、利用者認証部１０ｂは、ブラウザとＷｅｂサーバとの間における既存のＩＤ／パスワード認証や、証明書を用いたＳＳＬ（Secure Socket Layer）相互認証等により実現可能である。

【００４９】

証明書発行申請情報投入部１０ｃは、登録局（ＲＡ）サーバ８に対して、証明書を発行する際に必要な申請情報を投入する機能を備えた部である。具体的には、証明書発行申請情報投入部１０ｃは、登録局（ＲＡ）サーバ８の申請情報検証部８ｂに対して、申請情報を投入する。例えば、証明書発行申請情報投入部１０ｃは、ブラウザ上に表示された申請情報の登録フォーマットに、利用者によって、会社名、名前、利用者ＩＤ等の必要情報が投入され、利用者によって、ブラウザ上に用意された送信ボタンが押下されることなどによって実現可能である。

【００５０】
利用者証明書ダウンロード部１０ｄは、登録局（ＲＡ）サーバ８から利用者証明書をダウンロードする機能を備えた部である。具体的には、利用者証明書ダウンロード部１０ｄは、利用者証明書をダウンロードすることを要求するダウンロード要求を登録局（ＲＡ）サーバ８へ送信し、登録局（ＲＡ）サーバ８から送信される利用者証明書データをＲＡ端末１０に保存する。例えば、利用者証明書ダウンロード部１０ｄは、利用者によって、ブラウザ上に表示されたダウンロードボタンが押下されることなどによって、ダウンロード要求を登録局（ＲＡ）サーバ８へ送信し、登録局（ＲＡ）サーバ８から送信される利用者証明書データをＲＡ端末１０の記憶部に格納することで実現可能である。
【００５１】
証明書データ送信部１０ｅは、利用者証明書や権限委譲証明書をＩＣカード発行機１１に送信する機能を備えた部である。具体的には、証明書データ送信部１０ｅは、利用者証明書ダウンロード部１０ｄによってダウンロードされＲＡ端末１０に保存された利用者証明書や、権限委譲証明書ダウンロード部１０ｆによってダウンロードされＲＡ端末１０に保存された権限委譲証明書を、ＩＣカード発行機１１のＩＣカードデータ書込部１１ａに送信する。例えば、証明書データ送信部１０ｅは、既存のコンピュータシステムが所持するデータ通信機能や、ファイルアクセス機能を用いて実現可能である。
【００５２】
権限委譲証明書ダウンロード部１０ｆは、登録局（ＲＡ）サーバ８から権限委譲証明書をダウンロードする機能を備えた部である。具体的には、権限委譲証明書ダウンロード部１０ｆは、権限委譲証明書をダウンロードすることを要求するダウンロード要求を登録局（ＲＡ）サーバ８へ送信し、登録局（ＲＡ）サーバ８から送信される権限委譲証明書データをＲＡ端末１０に保存する。例えば、権限委譲証明書ダウンロード部１０ｆは、利用者（被権限委譲者）によって、ブラウザ上に表示されたダウンロードボタンが押下されることなどによって、ダウンロード要求を登録局（ＲＡ）サーバ８へ送信し、登録局（ＲＡ）サーバ８から送信される証明書データを利用者（被権限委譲者）の認証用ＩＣカード１２に格納することで実現可能である。
【００５３】
例えば、権限委譲証明書ダウンロード部１０ｆは、利用者（被権限委譲者）によって、ブラウザ上に表示されたダウンロードボタンが押下されることなどによって、ダウンロード要求を登録局（ＲＡ）サーバ８へ送信し、登録局（ＲＡ）サーバ８から送信される権限委譲証明書データを受信し、ＲＡ端末１０に接続されたリーダライタ１３を介して、ＰＫＣＳ（Public Key Cryptography Standards）＃１１やＭＳ－ＣＡＰＩ（Microsoft Crypto API）等の標準的なＩＣカードアクセスインタフェース機能により、受信した権限委譲証明書データを認証用ＩＣカード１２へ書き込むことにより実現可能である。
【００５４】
［ＩＣカード発行機１１］
図２に示すように、実施例１におけるＩＣカード発行機１１は、本発明に特に密接に関連するものとして、ＩＣカードデータ書込部１１ａを備える。
【００５５】
ＩＣカードデータ書込部１１ａは、認証用ＩＣカード１２に利用者証明書データを書き込む機能を備えた部である。具体的には、ＩＣカードデータ書込部１１ａは、ＲＡ端末１０の証明書データ送信部１０ｅによって送信された利用者証明書データを、認証用ＩＣカード１２に書き込む。例えば、ＩＣカードデータ書込部１１ａは、既存のＩＣカード発行システムを用いて実現可能である。
【００５６】
［登録局（ＲＡ）サーバ８］
図２に示すように、実施例１における登録局（ＲＡ）サーバ８は、本発明に特に密接に関連するものとして、利用者認証部８ａと、申請情報検証部８ｂと、鍵対生成部８ｃと、証明書発行要求部８ｄと、証明書管理部８ｅと、利用者証明書送信部８ｆと、権限委譲証

明書発行要求部８ｇと、権限委譲証明書管理部８ｈと、権限委譲証明書送信部８ｉと、権限委譲証明書失効要求部８ｊとを備える。

【００５７】

利用者認証部８ａは、ＲＡ端末１０との間で利用者認証を行う機能を備えた部である。具体的には、利用者認証部８ａは、ＲＡ端末１０の利用者認証部１０ｂとの間で、ＲＡ端末１０を操作している利用者の本人性を認証することを目的として利用者認証を行う。例えば、利用者認証部８ａは、ブラウザとＷｅｂサーバとの間における既存のＩＤ／パスワード認証や、証明書を用いたＳＳＬ相互認証等により実現可能である。

【００５８】

申請情報検証部８ｂは、申請情報を検証する機能を備えた部である。具体的には、申請情報検証部８ｂは、ＲＡ端末１０の証明書発行申請情報投入部１０ｃによって投入された申請情報を検証し、検証結果を鍵対生成部８ｃに伝達する。例えば、申請情報検証部８ｂは、ＲＡ端末１０から送信された申請情報を受信し、データの過不足や形式チェック等を実施するものであり、既存のＷｅｂサーバソフト等により実現可能である。

【００５９】

鍵対生成部８ｃは、鍵対を生成する機能を備えた部である。具体的には、鍵対生成部８ｃは、申請情報検証部８ｂから申請情報が正当であるとの検証結果を伝達されると、鍵対を生成する。例えば、鍵対生成部８ｃは、公開鍵暗号方式における秘密鍵および公開鍵のペアを生成するものであり、既存のＰＫＩ（Public Key Infrastructure）アプリケーション等により実現可能である。

【００６０】

証明書発行要求部８ｄは、利用者証明書の発行を要求する機能を備えた部である。具体的には、証明書発行要求部８ｄは、プライベート発行局サーバ７の証明書発行部７ａに対して、鍵対生成部８ｃによって生成された公開鍵に対する利用者証明書の発行を要求する。例えば、証明書発行要求部８ｄは、ＰＫＣＳ＃１０等の標準化されたデータ形式で証明書発行申請データをプライベート発行局サーバ７へ送信するものであり、既存のＰＫＩアプリケーション等により実現可能である。

【００６１】

証明書管理部８ｅは、利用者証明書を管理する機能を備えた部である。具体的には、証明書管理部８ｅは、プライベート発行局サーバ７の証明書発行部７ａから送信された利用者証明書データを受信し、登録局（ＲＡ）サーバ８の記憶部に格納する。例えば、証明書管理部８ｅは、既存のコンピュータシステムが保持するデータ通信機能、データ保存機能を用いて実現可能である。

【００６２】

利用者証明書送信部８ｆは、利用者証明書を送信する機能を備えた部である。具体的には、利用者証明書送信部８ｆは、証明書管理部８ｅによって管理されている利用者証明書データを、ＲＡ端末１０に送信する。例えば、利用者証明書送信部８ｆは、既存のＷｅｂサーバソフトや、これと連携するＲＤＢＭＳ（Relational DataBase Management System）等により実現可能である。

【００６３】

権限委譲証明書発行要求部８ｇは、権限委譲証明書の発行を要求する機能を備えた部である。具体的には、権限委譲証明書発行要求部８ｇは、プライベート発行局サーバ７の権限委譲証明書発行部７ｂに対して、権限委譲証明書の発行を要求する。例えば、権限委譲証明書発行要求部８ｇは、ＰＫＣＳ＃１０等の標準化されたデータ形式で証明書発行申請データをプライベート発行局サーバ７へ送信するものであり、既存のＰＫＩアプリケーション等により実現可能である。

【００６４】

権限委譲証明書管理部８ｈは、権限委譲証明書を管理する機能を備えた部である。具体的には、権限委譲証明書管理部８ｈは、プライベート発行局サーバ７の権限委譲証明書発行部７ｂから送信された権限委譲証明書データを受信し、登録局（ＲＡ）サーバ８の記憶

部に格納する。例えば、権限委譲証明書管理部８ｈは、既存のコンピュータシステムが保持するデータ通信機能、データ保存機能を用いて実現可能である。

【００６５】

権限委譲証明書送信部８ｉは、権限委譲証明書を送信する機能を備えた部である。具体的には、権限委譲証明書送信部８ｉは、権限委譲証明書管理部８ｈによって管理されている権限委譲証明書データを、ＲＡ端末１０に送信する。例えば、権限委譲証明書送信部８ｉは、既存のＷｅｂサーバソフトや、これと連携するＲＤＢＭＳ等により実現可能である。

【００６６】

権限委譲証明書失効要求部８ｊは、権限委譲証明書を失効させることを要求する機能を備えた部である。具体的には、権限委譲証明書失効要求部８ｊは、権限委譲証明書に対する失効を要求する権限委譲証明書失効要求データをプライベート発行局サーバ７の権限委譲証明書失効部７ｃへ送信する。例えば、権限委譲証明書失効要求部８ｊは、既存の認証局アプリケーション等により実現可能である。

【００６７】

［プライベート発行局サーバ７］

図２に示すように、実施例１におけるプライベート発行局サーバ７は、本発明に特に密接に関連するものとして、証明書発行部７ａと、権限委譲証明書発行部７ｂと、権限委譲証明書失効部７ｃと、失効リスト公開部７ｄとを備える。

【００６８】

証明書発行部７ａは、利用者証明書を発行する機能を備えた部である。具体的には、証明書発行部７ａは、登録局（ＲＡ）サーバ８の証明書発行要求部８ｄから利用者証明書の発行要求を受け付け、利用者証明書を発行する。例えば、証明書発行部７ａは、既存のＰＫＩアプリケーションあるいは認証局アプリケーションにより実現可能である。

【００６９】

権限委譲証明書発行部７ｂは、権限委譲証明書を発行する機能を備えた部である。具体的には、権限委譲証明書発行部７ｂは、登録局（ＲＡ）サーバ８の権限委譲証明書発行要求部８ｇから権限委譲証明書の発行要求を受け付け、権限委譲証明書を発行する。なお、例えば、権限委譲証明書は、既存のＸ．５０９等で規定された証明書の標準形式に準じた証明書であるため、権限委譲証明書発行部７ｂは、既存のＰＫＩアプリケーションあるいは認証局アプリケーションにより実現可能である。

【００７０】

権限委譲証明書失効部７ｃは、権限委譲証明書を失効させる機能を備えた部である。具体的には、権限委譲証明書失効部７ｃは、登録局（ＲＡ）サーバ８の権限委譲証明書失効要求部８ｊから権限委譲証明書の失効要求を受け付け、該当する権限委譲証明書の情報を証明書失効リスト（ＣＲＬ：Certificate Revocation List）に登録する。例えば、権限委譲証明書失効部７ｃは、既存のＸ．５０９等で規定されており、その標準形式に従った失効リストデータの作成は、既存のＰＫＩアプリケーションあるいは認証局アプリケーションにより実現可能である。

【００７１】

失効リスト公開部７ｄは、証明書失効リストを公開する機能を備えた部である。具体的には、失効リスト公開部７ｄは、権限委譲証明書失効部７ｃによって登録された証明書失効リストを、失効リストリポジトリサーバ９へ登録し、公開する。例えば、失効リスト公開部７ｄは、既存のＬＤＡＰ（Lightweight Directory Access Protocol）等のリポジトリサーバへのアクセス機能を用いることで実現可能である。

【００７２】

［クライアント端末１］

図３に示すように、実施例１におけるクライアント端末１は、本発明に特に密接に関連するものとして、証明書一覧部１ａと、ＩＣカードアクセス部１ｂと、権限委譲証明書送信部１ｃとを備える。

【００７３】
証明書一覧部１ａは、利用可能な証明書の一覧を出力部に表示する機能を備えた部である。具体的には、証明書一覧部１ａは、認証サーバ３の権限委譲証明書要求画面部３ａによる画面情報を受信すると、リーダライタ１３を介して認証用ＩＣカード１２内に格納された権限委譲証明書等の情報を出力部に表示し、利用者による選択（一覧の中から権限委譲証明書を選択）を受け付ける。例えば、証明書一覧部１ａは、既存のブラウザ等により実現可能である。
【００７４】
ＩＣカードアクセス部１ｂは、認証用ＩＣカード１２にアクセスする。具体的には、ＩＣカードアクセス部１ｂは、リーダライタ１３を介して認証用ＩＣカード１２にアクセスし、当該認証用ＩＣカード１２に格納されている権限委譲証明書を受信する。例えば、ＩＣカードアクセス部１ｂのＰＩＮによるアクセス制御機能やＩＣカード内の情報の読み書きに関する機能は、既存のＩＣカードアプリケーションによって実現可能である。
【００７５】
権限委譲証明書送信部１ｃは、権限委譲証明書を送信する機能を備えた部である。具体的には、権限委譲証明書送信部１ｃは、ＩＣカードアクセス部１ｂによって受信された権限委譲証明書を、認証サーバ３の権限委譲証明書検証部３ｂに送信する。例えば、権限委譲証明書送信部１ｃは、既存のブラウザと、Ｗｅｂサーバとの間の送受信機能を用いることで実現可能である。
【００７６】
［認証サーバ３］
図３に示すように、認証サーバ３は、本発明に特に密接に関連するものとして、権限委譲証明書要求画面部３ａと、権限委譲証明書検証部３ｂと、権限委譲証明書転送部３ｃと、認可結果画面表示部３ｄとを備える。
【００７７】
権限委譲証明書要求画面部３ａは、権限委譲証明書を要求する画面情報をクライアント端末１に送信する。具体的には、権限委譲証明書要求画面部３ａは、バックエンドアプリケーションサーバ５の権限委譲証明書要求部５ａから権限委譲証明書要求を受け付けると、権限委譲証明書の送信を要求する画面情報を、クライアント端末１に送信する。例えば、権限委譲証明書要求画面部３ａの画面表示させるための電文生成や送信機能は、通常のＷｅｂアプリケーションシステムにおいて実現可能である。
【００７８】
権限委譲証明書検証部３ｂは、権限委譲証明書を検証する。具体的には、権限委譲証明書検証部３ｂは、クライアント端末１の権限委譲証明書送信部１ｃによって送信された権限委譲証明書を検証し、検証結果を権限委譲証明書転送部３ｃに伝達する。例えば、権限委譲証明書検証部３ｂは、既存のＷｅｂサーバにおけるＳＳＬ送受信機能や、証明書パース機能を用いることで実現可能である。
【００７９】
権限委譲証明書転送部３ｃは、権限委譲証明書を転送する。具体的には、権限委譲証明書転送部３ｃは、権限委譲証明書検証部３ｂによって正当であることが検証された権限委譲証明書を、バックエンドアプリケーションサーバ５の権限委譲証明書確認部５ｂに送信する。例えば、権限委譲証明書転送部３ｃは、既存のサーバ間通信機能を用いることで実現可能である。
【００８０】
認可結果画面表示部３ｄは、認可結果の画面情報を送信する。具体的には、認可結果画面表示部３ｄは、バックエンドアプリケーションサーバ５の認可結果通知部５ｄから通知された認可結果の画面情報を、クライアント端末１に送信する。例えば、認可結果画面表示部３ｄの画面表示させるための電文生成や送信機能は、通常のＷｅｂアプリケーションシステムにおいて実現可能である。
【００８１】

［バックエンドアプリケーションサーバ５］
図３に示すように、バックエンドアプリケーションサーバ５は、本発明に特に密接に関連するものとして、権限委譲証明書要求部５ａと、権限委譲証明書確認部５ｂと、失効情報確認部５ｃと、認可結果通知部５ｄとを備える。
【００８２】
権限委譲証明書要求部５ａは、権限委譲証明書を要求する。具体的には、権限委譲証明書要求部５ａは、認可の否決情報とあわせて権限委譲証明書を要求する電文を、認証サーバ３に送信する。例えば、権限委譲証明書要求部５ａは、通常のコンピュータシステムにおける電文生成機能、電文送信機能により実現可能である。
【００８３】
権限委譲証明書確認部５ｂは、権限委譲証明書を確認する。具体的には、権限委譲証明書確認部５ｂは、認証サーバ３の権限委譲証明書転送部３ｃから転送された権限委譲証明書内に格納された権限委譲情報を確認する。例えば、権限委譲証明書確認部５ｂは、既存のＰＫＩアプリケーションにおける証明書パース機能等を用いることで実現可能である。
【００８４】
失効情報確認部５ｃは、失効情報を確認する。具体的には、失効情報確認部５ｃは、失効リストリポジトリサーバ９を参照し、該当する利用者ＩＤの利用者証明書や権限委譲証明書が失効していないかを確認する。例えば、失効情報確認部５ｃは、既存のＰＫＩアプリケーションにおいて、ＬＤＡＰ等のリポジトリへのアクセスプロトコルを用いた失効リスト情報の照会機能を用いることで実現可能である。
【００８５】
認可結果通知部５ｄは、認可結果を通知する。具体的には、認可結果通知部５ｄは、権限委譲証明書確認部５ｂや失効情報確認部５ｃによって確認された認可結果を、認証サーバ３の認可結果画面表示部３ｄに送信する。例えば、認可結果通知部５ｄは、通常のコンピュータシステムにおける電文生成機能、電文送受信機能により実現可能である。
【００８６】
［実施例１に係る権限委譲システムによる処理の手順］
次に、図４～図１３－２を用いて、実施例１に係る権限委譲システムによる処理の手順を詳細に説明する。なお、以下では、認証用ＩＣカードの発行と認証情報の格納の流れ、権限委譲証明書を認証用ＩＣカードに格納するまでの流れ、本発明におけるシングルサインオン認証処理の流れ、権限を有した利用者での認可処理の流れ、権限を委譲された利用者での認可処理の流れ、権限を委譲された利用者が権限変更を行う認可処理の流れを順に説明する。
【００８７】
［認証用ＩＣカードの発行と認証情報の格納の流れ］
図４は、認証用ＩＣカードの発行と認証情報の格納の流れを説明するための図である。実施例１に係る権限委譲システムは、図４に示すように、利用者証明書を発行するプライベート発行局サーバ７、利用者の本人性を確認した上でＲＡ端末１０からの利用者証明書発行要求を受け付け、プライベート発行局サーバ７に利用者証明書発行を要求する登録局サーバ８、登録局サーバ８に対して利用者証明書発行要求を申請するためのＲＡ端末１０、および、認証用ＩＣカード１２に利用者証明書を含む認証情報を格納するためのカード発行機１１から構成され、各構成機器は、ネットワークで通信可能な状態になっている。
【００８８】
まず、オペレータは、各部門などに設置されたＲＡ端末１０における登録局サーバアクセス機能（登録局サーバアクセス部１０ａ）を用いて登録局サーバ８へネットワークを介してアクセスし、登録局サーバ１０との間で利用者認証機能（利用者認証部１０ｂ）を用いて利用者認証を実施後、証明書発行申請情報投入機能（証明書発行申請情報投入部１０ｃ）を用いて利用者証明書の発行申請情報を送信する（図４の（１）を参照）。
【００８９】
次に、登録局サーバ８は、申請情報検証機能（申請情報検証部８ｂ）を用いて、ＲＡ端

末１０から申請された利用者証明書発行申請情報の正当性を確認し、鍵対生成機能（鍵対生成部８ｃ）により、秘密鍵および公開鍵の鍵対を生成後、証明書発行要求機能（証明書発行要求部８ｄ）を用いてプライベート発行局サーバ７に対して当該公開鍵に対する証明書の発行を要求する（図４の（１）を参照）。なお、利用者証明書発行申請データには、ＲＡ端末１０から送信された申請情報の中から、利用者証明書に格納すべき情報を含めて送信される。例えば、会社名や名前、利用者ＩＤ等が該当する。

【００９０】

そして、プライベート発行局サーバ７は、証明書発行機能（証明書発行部７ａ）を用いて、登録局サーバ８からの利用者証明書発行要求データを受信し、当該データに基づく利用者証明書を作成し、登録局サーバ８へ利用者証明書を送信する（図４の（２）を参照）。なお、発行された利用者証明書内には、証明書発行申請データに含まれていた会社名や名前等の認証情報が含まれている。

【００９１】

すると、登録局サーバ８は、証明書管理機能（証明書管理部８ｅ）を用いて、プライベート発行局サーバ７から送信された利用者証明書データを受信し、登録局サーバ８内に格納する（図４の（２）を参照）。

【００９２】

次に、ＲＡ端末１０は、登録局サーバアクセス機能（登録局サーバアクセス部１０ａ）を用いて、登録局（ＲＡ）サーバ８へネットワークを介してアクセスし、利用者認証機能（利用者認証部８ａ）を用いて、登録局（ＲＡ）サーバ８との間で利用者認証を実施後、利用者証明書ダウンロード機能（利用者証明書ダウンロード部１０ｄ）を用いて、登録局（ＲＡ）サーバ８から利用者証明書をダウンロードする（図４の（２）を参照）。

【００９３】

一方、登録局サーバ８では、利用者認証機能（利用者認証部８ａ）を用いて利用者認証を実施後、利用者証明書送信機能（利用者証明書送信部８ｆ）を用いて、ＲＡ端末１０からの利用者証明書ダウンロード要求を受け付け、さらにその後、登録局サーバ８内に格納された対象の利用者証明書を検索して取得し、ＲＡ端末１０に対してこれを送信する（図４の（２）を参照）。

【００９４】

続いて、ＲＡ端末１０は、証明書データ送信機能（証明書データ送信部１０ｅ）を用いてカード発行機１１に対してダウンロードした利用者証明書データを送信する（図４の（３）を参照）。また、この利用者証明書データの送信の完了と同時に、ＲＡ端末１０上の利用者証明書データは自動消去する。ＩＣカード発行機１１側では、事前に書き込み対象の初期化された認証用ＩＣカード１２をＩＣカード発行機１１にセットした後、ＩＣカードデータ書込機能（ＩＣカードデータ書込部１１ａ）を用いて、ＲＡ端末１０からの利用者証明書データを受信後、認証用ＩＣカード１２の不揮発性のメモリ領域に利用者証明書データを書き込む（図４の（４）を参照）。

【００９５】

以上の機能および手順により、会社名や氏名等の認証に必要な情報を含む利用者証明書が格納された認証用ＩＣカード１２を作成し、シングルサインオン認証への利用を実現した。

【００９６】

［権限委譲証明書を認証用ＩＣカードに格納するまでの流れ］

次に、図５は、権限委譲証明書に必要な構成要素を説明するための図である。実施例１に係る権限委譲システムは、利用者が権限委譲証明書の申請を入力するＲＡ端末１０、利用者の本人性を確認した上で申請を受け付ける登録局サーバ８、権限委譲証明書を生成するプライベート発行局サーバ７、認証に必要な利用者証明書および権限委譲証明書の失効を受け付け、そのリストを公開する失効リストリポジトリサーバ９から主に構成される。また、ＲＡ端末１０には、利用者が利用者証明書で本人確認を行う場合、権限を委譲される人が自分の利用者証明書で本人確認を行う場合、さらに、自分の認証用ＩＣカードに権

限委譲証明書をダウンロードする場合等に利用するリーダライタ１３が接続され、認証用ＩＣカード１２の読み書きをつかさどる。

【００９７】

次に、権限委譲情報パターンについて説明する。利用者が有している権限を委譲するには、いくつかのパターンに集約できる。図６に、このパターン例を示す。もちろん、本人の意思確認や責任内規の整備が必要であるが、この例は、権限を有する利用者が指示して電子処理を行うことを前提としている。基本的に、権限を委譲する内容や範囲として、申請と決裁の場合がほとんどである。これらの対象業務と内容とをパターン化することにより、権限を委譲する利用者が申請を行う際の入力の簡素化が可能になる。

【００９８】

図７に、権限委譲証明書を申請する際の申請内容の例を示す。上記した権限委譲情報パターン（番号の選択）に加えて、権限を委譲する人のＩＤ番号、権限を委譲される人のＩＤ番号、委譲する期限だけであり、同じような情報を、サービス・業務のアプリケーションごとに入力するのに比べ、はるかに短時間に、簡単に申請することが可能になる。

【００９９】

図８は、権限委譲証明書を認証用ＩＣカードに格納するまでの流れを説明するための図である。バックエンドアプリケーションサーバにアクセスできる権限を有した利用者が、他者にその権限を委譲したい場合、まず、権限委譲利用者は、ＲＡ端末１０において、自分の認証用ＩＣカード１２をリーダライタ１３に挿入する（図８の（１）を参照）。ＲＡ端末１０は、登録局サーバアクセス機能（登録局サーバアクセス部１０ａ）を用いて登録局サーバ８へアクセス後、利用者認証機能（利用者認証部１０ｂ）を用いて認証用ＩＣカード１２内の利用者証明書を用いた利用者認証を実施する。続いて、ＲＡ端末１０は、申請情報投入機能（証明書発行申請情報投入部１０ｃ）を用いて、図７に示した権限委譲される人のＩＤ、権限委譲情報パターン、権限委譲の有効期限等の情報の指定を受け付け、これを登録局（ＲＡ）サーバ８へ送信する（図８の（２）を参照）。

【０１００】

なお、認証用ＩＣカード１２内の利用者証明書を用いた利用者認証の実施は、例えば、ブラウザとＷｅｂサーバ間におけるＳＳＬ相互認証において、認証用ＩＣカード１２内に格納された秘密鍵情報や証明書情報に対して、ＰＫＣＳ＃１１やＭＳ－ＣＡＰＩ等の標準的なＩＣカードアクセスインタフェース機能を用いてアクセスし、これらを用いて、クライアント側での認証情報生成や登録局（ＲＡ）サーバ８への認証情報の送信を実施することで実現可能である。

【０１０１】

続いて、登録局（ＲＡ）サーバ８は、申請情報検証機能（申請情報検証部８ｂ）を用いてＲＡ端末１０から申請された権限委譲証明書発行申請情報の正当性を確認し、鍵対生成機能（鍵対生成部８ｃ）により秘密鍵および公開鍵の鍵対を生成後、権限委譲証明書発行要求機能（権限委譲証明書発行要求部８ｇ）を用いてプライベート発行局サーバ７に対して当該公開鍵に対する権限委譲証明書の発行を要求する（図８の（２）を参照）。なお、権限委譲証明書発行申請データには、ＲＡ端末１０から送信された申請情報の中から、図７に示すような権限委譲証明書に格納すべき情報を含めて送信される。

【０１０２】

次に、プライベート発行局サーバ７は、権限委譲証明書発行機能（権限委譲証明書発行部７ｂ）を用いて、登録局サーバ８からの権限委譲証明書発行要求データを受信し、当該データに基づく権限委譲証明書を作成し、登録局サーバ８へ権限委譲証明書を送信する（図８の（４）を参照）。なお、発行された権限委譲証明書内には、権限委譲証明書発行申請データに含まれる権限委譲する人のＩＤ、権限委譲される人のＩＤ、権限委譲情報のパターン、権限委譲の有効期限等の権限委譲を証明する情報が含まれている。

【０１０３】

続いて、登録局サーバ８は、権限委譲証明書管理機能（権限委譲証明書管理部８ｈ）を用いて、プライベート発行局サーバ７から送信された権限委譲証明書データを受信し、登

録局（ＲＡ）サーバ８内に格納する（図８の（４）を参照）。
【０１０４】
次に、権限を委譲される利用者がシステムにログインした。この際も、権限を委譲される本人の認証用ＩＣカード１２をリーダライタ１３に挿入し（図８の（３）を参照）、被権限委譲者が利用するＲＡ端末１０は、登録局サーバアクセス機能（登録局サーバアクセス部１０ａ）を用いて登録局サーバ８へアクセス後、利用者認証機能（利用者認証部１０ｂ）を用いて認証用ＩＣカード１２内の利用者証明書を用いた利用者認証を実施する。
【０１０５】
そして、被権限委譲者が利用するＲＡ端末１０は、権限委譲証明書ダウンロード機能（権限委譲証明書ダウンロード部１０ｆ）を用いて、登録局（ＲＡ）サーバ８から権限委譲証明書を、権限を委譲される本人の認証用ＩＣカード１２内にダウンロードする。この時、登録局サーバ８では、利用者認証機能（利用者認証部８ａ）を用いて利用者認証を実施後、権限委譲証明書送信機能（権限委譲証明書送信部８ｉ）を用いて、被権限委譲者が利用するＲＡ端末１０からの権限委譲証明書ダウンロード要求を受け付け、さらにその後、登録局サーバ８内に格納された対象の権限委譲証明書を検索して取得し、被権限委譲者が利用するＲＡ端末１０に対してこれを送信する。
【０１０６】
以上の機能および手順により、権限委譲証明書を、権限の委譲を依頼された利用者の認証用ＩＣカード１２内に格納することを実現した。さらに、この一連の操作は非常に簡単である。なお、実施例１においては、被権限委譲者が、自ら操作するＲＡ端末１０によって登録局サーバ８へアクセスし、自身向けに発行された権限委譲証明書をＩＣカードに格納する手法を説明したが、本発明はこれに限られるものではない。例えば、被権限委譲者が利用するクライアント端末１が登録局サーバ８に通信可能に接続されている環境であれば、当該被権限委譲者は、当該クライアント端末１によって登録局サーバ８へアクセスし、自身向けに発行された権限委譲証明書をＩＣカードに格納してもよい。言い換えると、権限委譲者が関与することなく被権限委譲者が権限委譲証明書を取得することが可能な手法であれば、どの端末を用いて登録局サーバ８へアクセスするかは任意に変更し得る。
【０１０７】
［失効リポジトリサーバへの登録］
また、権限委譲証明書の内容変更、利用者や権限を委譲された利用者が異動した際には、権限委譲証明書の発行を申請した利用者、つまりは、権限委譲を希望した利用者が、ＲＡ端末１０を通して、失効リストリポジトリサーバ９に登録することで、権限委譲証明書を失効させることが可能である。利用者証明書の失効も失効リストリポジトリサーバ９に登録することで、利用者が異動した後も権限委譲証明書が使われることができないように二重のブロックをかけるのである。以上を実現する機能および手順は、以下の通りである。
【０１０８】
まず、権限委譲を希望した利用者は、ＲＡ端末１０において自分の認証用ＩＣカード１２をリーダライタ１３に挿入する。ＲＡ端末１０は、登録局サーバアクセス機能（登録局サーバアクセス部１０ａ）を用いて登録局サーバ８へアクセス後、利用者認証機能（利用者認証部１０ｂ）を用いて認証用ＩＣカード１２内の利用者証明書を用いた利用者認証を実施する。続いて、ＲＡ端末１０は、申請情報投入機能（証明書発行申請情報投入部１０ｃ）を用いて、失効を希望する対象の権限委譲証明書の識別情報を含む失効申請情報を入力し、これを登録局（ＲＡ）サーバ８へ送信する。
【０１０９】
続いて、登録局サーバ８は、申請情報検証機能（申請情報検証部８ｂ）を用いてＲＡ端末１０から申請された権限委譲証明書失効申請情報の正当性を確認し、権限委譲証明書失効要求機能（権限委譲証明書失効要求部８ｊ）を用いてプライベート発行局サーバ７に対して権限委譲証明書に対する失効を要求する。
【０１１０】

そして、プライベート発行局サーバ７は、権限委譲証明書失効機能（権限委譲証明書失効部７ｃ）を用いて、登録局サーバ８からの権限委譲証明書失効要求データを受信し、該当の権限委譲証明書の情報を証明書失効リストに登録し、失効リスト公開機能（失効リスト公開部７ｄ）を用いて、証明書失効リストを失効リストリポジトリサーバ９へ登録、公開する。

【０１１１】

［本発明におけるシングルサインオン認証処理の流れ］

図９は、本発明におけるシングルサインオン認証およびバックエンドアプリケーションサーバ５での認可のシステム構成例を示す図である。通常のシングルサインオン認証でＩＣカードを利用する場合と同様の構成となっている。図１０は、本発明におけるシングルサインオン認証処理の流れを説明するための図である。なお、図１０に示す処理の流れは、権限を委譲する利用者および権限を委譲された利用者ともに同じであり、認証用ＩＣカード１２（利用者証明書）を使ったシングルサインオン認証と同様の流れとなっている。

【０１１２】

まず、クライアント端末１が、認証サーバ３に対して、ポータルへのアクセス要求を送信する（ステップＳ１０１）。次に、認証サーバ３は、クライアント端末１に対して、認証情報要求を送信する（ステップＳ１０２）。すると、クライアント端末１は、認証用ＩＣカード１２に対して、リーダライタ１３を介して認証情報要求を送信する（ステップＳ１０３）。

【０１１３】

ここで、利用者は、認証用ＩＣカード１２内に格納された利用者証明書を選択し（ステップＳ１０４）、ＩＤ、パスワード入力の代わりに、認証用ＩＣカード１２を利用してＰＩＮ入力する（ステップＳ１０５およびステップＳ１０６）。なお、認証用ＩＣカード１２へのＰＩＮ入力は、クライアント端末１上に表示されたＰＩＮ入力画面からＰＩＮが投入され、これをリーダライタ１３を介して認証用ＩＣカード１２へ送信することにより実現可能であり、既存のＩＣカード利用アプリケーションにて実装されているものである。

【０１１４】

すると、クライアント端末１と認証サーバ３との間で、ＳＳＬ等の暗号通信路を介して、認証用ＩＣカード１２内に格納された秘密鍵および利用者証明書を用いたクライアント認証が実施される（ステップＳ１０７）。なお、クライアント端末１と認証サーバ３との間でのＳＳＬによる暗号通信路の構築や、ＳＳＬにおける利用者証明書を用いたクライアント認証の実施等についても、既存のブラウザおよびＷｅｂサーバソフトを用いることで実現可能である。

【０１１５】

続いて、認証サーバ３は、そのクライアント認証に用いた利用者証明書の識別名（ＤＮ）を抽出し（ステップＳ１０８）、ディレクトリデータベース４に格納した識別名とマッチングさせ（ステップＳ１０９）、認証の判定を行う（ステップＳ１１０）。なお、利用者証明書の識別名を取得する機能については、既存のＰＫＩアプリケーション機能が有する証明書パース機能で実現可能であり、さらに、ディレクトリデータベースに格納した識別名とのマッチングについても、既存のＷｅｂアプリケーションとＲＤＢＭＳとの連携機能により実現可能である。

【０１１６】

こうして、認証の結果、認証ＯＫ（利用者の本人性を確認）であれば、認証サーバ３は、クライアント端末１に対して、ポータルのＵＲＬを提示する（ステップＳ１１１）。

【０１１７】

［権限を有した利用者での認可処理の流れ］

図１１は、権限を有した利用者での認可処理を説明するための図である。ここでは、クライアント端末１の操作者は、すでに図１０のシングルサインオン認証処理を完了し、本人認証が済みの状態となった後の流れを示している。

【０１１８】

まず、対象とするアプリケーションへアクセスする権限を有する利用者の場合、クライアント端末１から認証サーバ３を経由して、対象となるバックエンドアプリケーションサーバ５へアクセス要求を送信する（ステップＳ１２０およびＳ１２１）。

【０１１９】

すると、バックエンドアプリケーションサーバ５は、これを受けて利用者ＩＤを要求する（ステップＳ１２２）。認証サーバ３は、認証をパスした利用者ＩＤ情報をバックエンドアプリケーションサーバ５へ提示し（ステップＳ１２３）、バックエンドアプリケーションサーバ５は、利用者管理のデータベースと照合して認可判定を行い（ステップＳ１２４）、設定されたアクセス権限に従って、認可結果およびリソースＵＲＬを認証サーバ３経由にてクライアント端末１に表示させる（ステップＳ１２５およびＳ１２６）。

【０１２０】

このように、権限を有する利用者は、バックエンドアプリケーションサーバ５側の利用者データベースに利用者ＩＤおよびアクセス権限が格納されているので、特別な処理無しにサービス・業務を行うことができる。

【０１２１】

［権限を委譲された利用者での認可処理の流れ］

図１２－１および図１２－２は、権限を委譲された利用者での認可処理の流れを説明するための図である。この実施例は、利用者が、元来、アクセス権限を持たない人が、アクセス権限を委譲された利用者の場合である。

【０１２２】

まず、バックエンドアプリケーションサーバ５側に利用者ＩＤを登録していないので、通常の処理では認可は否決される。従って、通常は、「○○サービスに利用登録がされていません」といったエラーメッセージがクライアント端末に表示される。

【０１２３】

実施例１に係る権限委譲システムでは、クライアント端末１から認証サーバ３に対して、バックエンドアプリケーションサーバ５へのアクセス要求が送信され、認証サーバ３からバックエンドアプリケーションサーバ５に対して当該アクセス要求が送信され、バックエンドアプリケーションサーバ５において認可判定が行われ、これが否決となった場合（ステップＳ２０１～Ｓ２０５）、バックエンドアプリケーションサーバ５は、権限委譲証明書要求機能（権限委譲証明書要求部５ａ）を用いて、認可の否決情報とあわせて権限委譲証明書を要求する電文を認証サーバ３に返す（ステップＳ２０６）。認証サーバ３は、権限委譲証明書の要求電文を受信すると、権限委譲証明書要求画面機能（権限委譲証明書要求画面部３ａ）を用いて、権限委譲証明書の送信を要求する画面情報をクライアント端末１へ送信する（ステップＳ２０７）。

【０１２４】

クライアント端末１は、画面情報を受信すると、証明書一覧機能（証明書一覧部１ａ）によりクライアント端末１からアクセス可能な証明書の一覧を表示する（ステップＳ２０８）。なお、リーダライタ１３を介して認証用ＩＣカード１２内に格納された権限委譲証明書の情報も、その一覧に含められて表示される。利用者が、その一覧の中から権限委譲証明書を選択すると（ステップＳ２０９）、クライアント端末１は、ＩＣカードアクセス機能（ＩＣカードアクセス部１ｂ）を用いて、認証用ＩＣカード１２へアクセスするためのＰＩＮ入力画面をクライアント端末１上に表示し、利用者により入力されたＰＩＮ情報を認証用ＩＣカード１２へ送信し（ステップＳ２１０およびＳ２１１）、認証用ＩＣカード１２におけるＰＩＮ照合が完了後、認証用ＩＣカード１２内に格納された権限委譲証明書を受信する。

【０１２５】

クライアント端末１は、さらに、権限委譲証明書送信機能（権限委譲証明書送信部１ｃ）を用いて、図１０において確立したＳＳＬ等の暗号通信路を介し、認証用ＩＣカード１２内から取得した権限委譲証明書を認証サーバ３へ送信する（ステップＳ２１２）。

【０１２６】

認証サーバ３では、権限委譲証明書検証機能（権限委譲証明書検証部３ｂ）を用いて、暗号通信路において暗号化された権限委譲証明書を復号して、権限委譲証明書内に格納された権限委譲された利用者の識別情報を取得し、これを先に実施済みのシングルサインオン認証にて認証済みの利用者と一致していることを確認する（ステップＳ２１３）。この確認が完了後、認証サーバ３は、権限委譲証明書転送機能（権限委譲証明書転送部３ｃ）を用いて、権限委譲証明書をバックエンドアプリケーションサーバ５へ送信する（ステップＳ１２４）。なお、実施例１においては、認証サーバ３が、権限委譲証明書自体をバックエンドアプリケーションサーバ５へ送信する手法を説明したが、本発明はこれに限られるものではない。認証サーバ３が送信する情報は、利用者が権限委譲に基づいてバックエンドアプリケーションサーバ５にアクセス（ログイン）するものであることを示す情報であれば、権限委譲証明書から導出された他の形態の情報であってもよい。

【０１２７】

バックエンドアプリケーションサーバ５では、権限委譲情報確認機能（権限委譲証明書確認部５ｂ）を用いて、受信した権限委譲証明書内に格納された権限委譲者の識別情報、権限委譲の有効期限、図７に示した権限委譲の対象業務や委譲範囲を示す委譲パターンの情報を抽出し、その権限委譲者の有するアクセス権限との整合性の確認、権限委譲の有効期限が切れていないことを確認する。また、失効情報確認機能（失効情報確認部５ｃ）を用いて、失効リストリポジトリサーバ９を参照し、該当する利用者ＩＤの利用者証明書や権限委譲証明書が失効していないかを確認する（ステップＳ２１５）。なお、有効期限と失効とを先に確認した上で、その他の情報を確認し、認可判定を行ってもよい。

【０１２８】

最後に、バックエンドアプリケーションサーバ５は、認可結果通知機能（認可結果通知部５ｄ）を用いて、委譲により、アクセス可能なリソースのＵＲＬ情報を認証サーバ３へ通知し（ステップＳ２１６）、認証サーバ３は、認可結果画面表示機能（認証結果画面表示部３ｄ）を用いてこれをクライアント端末１に表示させる（ステップＳ２１７）。

【０１２９】

［権限を委譲された利用者が権限変更を行う認可処理の流れ］

図１３－１および図１３－２は、権限を委譲された利用者が権限変更を行う認可処理の流れを説明するための図である。この場合、特定アプリケーションへのアクセス権限があるが、その作業可能な範囲が異なる。

【０１３０】

例えば、図６のパターン２の権限を有していた人が、パターン４の権限を委譲される。結果として、一部の業務に対して、申請や決裁の権限が追加されたことになる。この場合、権限を委譲された利用者は、バックエンドアプリケーションサーバ５（例えば、旅費申請）側に利用者ＩＤを登録しているので、認可は可決される。しかし、パターン２の権限であるので、旅費の決裁処理はできなかった。

【０１３１】

実施例１に係る権限委譲システムでは、権限を委譲された利用者が、一度認可された後（ステップＳ３０１～Ｓ３０７）、クライアント端末１は、権限の変更を、認証サーバ３経由で、旅費アプリケーションサーバ５に対して要求した（ステップＳ３０８およびＳ３０９）。

【０１３２】

旅費アプリケーションサーバ５は、権限変更を否決し（ステップＳ３１０）、権限委譲証明書要求機能（権限委譲証明書要求部５ａ）を用いて認証サーバ３に対して権限委譲証明書を要求する（ステップＳ３１１）。

【０１３３】

以降、認証サーバ３が権限委譲証明書の要求電文を受信後の処理は、図１２において述べたものと同様の処理が行われ、旅費アプリケーションサーバ５に対して権限委譲証明書が送信される（ステップＳ３１２からＳ３１９）。

【０１３４】

旅費アプリケーションサーバ５は、権限委譲情報確認機能（権限委譲証明書確認部５ｂ）および失効情報確認部（失効情報確認部５ｃ）を用いて、図１２と同様に受信した権限委譲証明書の内容およびその有効性を確認後、認可結果通知機能（認可結果通知部５ｄ）を用いて、委譲によりアクセス可能なリソースのＵＲＬ情報を認証サーバ３へ通知し（ステップＳ３２１）、認証サーバ３は、認証結果画面表示機能を用いてこれをクライアント端末１に表示させる（ステップＳ３２２）。

【０１３５】

こうして、実施例１においては、委譲により旅費業務の決裁処理が新たに可能となり、決裁ボタンをアクティブにしたリソースのＵＲＬをクライアント端末１に表示させた。

【０１３６】

以上が、認証用ＩＣカード１２の利用者証明書を使ってシングルサインオン認証し、権限を委譲された利用者が、権限委譲証明書を使って、サービス・業務のアプリケーションサーバ５で認可されるまでの流れである。本発明による認可処理の流れは、認証用ＩＣカード１２の利用者証明書を使った個人認証と同じ操作であるので、利用者にとっても抵抗感無く操作することができる。また、バックエンドアプリケーションサーバ５での認可判定時に、失効リストリポジトリサーバ９を参照することで、利用者の異動など権限失効に対しても自動的に対処できる。

【０１３７】

［実施例１の効果］

上記してきたように、実施例１によれば、予算や業務に対する権限を有した多忙な教職員や部課長などの利用者にとっても、一度、権限委譲証明書を申請し、その証明書を秘書や部下のＩＣカードに格納することにより、有効期限の範囲でアクセス権限を適切に委譲することができる。また、シングルサインオン認証およびアプリケーション側の認可処理において、利用者、アプリケーション側あるいはディレクトリサーバ側の負担を大幅に増大させずに、権限委譲を安全、安心に行うことができる。

【０１３８】

少なくとも、従来のように「なりますまし」による処理のようなセキュリティリスクの高い状況から解放され、ミスや不正利用に対してトレースできるといった効果がある。また、従来の権限委譲の方法に比べ、各サービス・業務のアプリケーションに対する申請処理あるいはディレクトリデータベースへの権限委譲情報の追加も必要なく、利用者の処理も大幅に軽減でき、安心して代行入力などが実施できる。

【０１３９】

さらに、バックエンドアプリケーションサーバ側あるいはディレクトリデータベースも申請ごとに処理することはなく、大きな作業量の負担は発生しなくなる。

【０１４０】

権限委譲された利用者の認可についても、シングルサインオン認証は従来通りであり、認可否決処理に権限委譲証明書要求が追加された程度であったため、従来の認可処理に比べて負担とは感じられない。従って、シングルサインオン認証のメリットを活かしつつ、権限委譲証明書による認可処理が行えるというメリットがある。

【０１４１】

実施例１においては、権限委譲証明書をバックエンドアプリケーションサーバ側が読み込み、それを条件として認可判定し、リソースへのアクセスを許可する。権限委譲情報は、複数の典型的なパターンを準備し、それらの一つを選択することにより、権限委譲証明書を発行させる。したがって、権限内容をよく理解している利用者本人が特定のパターンを選択して申請するため、アプリケーション側で行う審査が必要なく、ミスも大幅に抑制できる。

【０１４２】

また、権限委譲証明書の発行処理は、利用者が、各バックエンドアプリケーションサーバ側、あるいは、ディレクトリデータベースに行う代わりに、利用者証明書を発行した同じ手順にて行うため、処理に必要となる本人確認などの負担が大きく軽減でき、安心、安

全に権限委譲の処理を行うことができる。

【０１４３】

また、シングルサインオン認証後、バックエンドアプリケーションサーバ側が利用者の権限委譲証明書を読み込み、さらに、失効リストリポジトリサーバを参照した上で、認可の判定を自動的に行う。したがって、バックエンドアプリケーションサーバ側での認可時点で、権限委譲証明書の利用者ＩＤ（権限を委譲した利用者および委譲された利用者のＩＤ）が登録されているため、リポジトリに提示された失効証明書リストを参照することによって、失効を検知でき、認可を拒否できるため、安心して認可処理を行うことができる。

【０１４４】

従来の技術では、権限を有する利用者が、アプリケーションごとに利用者申請を行い、アプリケーションサーバ側は、本人性を確認した上で申請の都度審査を行っていた。あるいは、権限を有する利用者がディレクトリデータベースに対して、権限委譲による認可情報を追加するように申請しなければならず、ディレクトリデータベース側は、その都度更新などの作業が増えていた。特に、シングルサインオン認証は、多数のサービス・業務を収容することが前提であるため、これら申請の際の本人確認や権限を委譲された人の本人確認および審査などに関る繁雑な処理は極めて膨大となり、シングルサインオン認証のメリットを損なっていた。また、申請と同様に、権限を有した利用者や権限を委譲された人が異動した場合、繁雑な失効申請を迅速に行うことが必要であり、これも作業が増える原因であった。

【実施例２】

【０１４５】

［他の実施例］

さて、これまで本発明の実施例について説明したが、本発明は上述した実施例以外にも、種々の異なる形態にて実施されてよいものである。

【０１４６】

［システム構成等］

実施例１において説明した各処理のうち、自動的におこなわれるものとして説明した処理の全部または一部を手動的におこなうこともでき、あるいは、手動的におこなわれるものとして説明した処理の全部または一部を公知の方法で自動的におこなうこともできる。この他、上記文書中や図面中で示した処理手順、制御手順、具体的名称、各種のデータやパラメータを含む情報については、特記する場合を除いて任意に変更することができる。

【０１４７】

また、図示した各装置の各構成要素は機能概念的なものであり、必ずしも物理的に図示の如く構成されていることを要しない。すなわち、各装置の分散・統合の具体的形態は図示のものに限られず、その全部または一部を、各種の負荷や使用状況などに応じて、任意の単位で機能的または物理的に分散・統合して構成することができる。さらに、各装置にて行なわれる各処理機能は、その全部または任意の一部が、ＣＰＵおよび当該ＣＰＵにて解析実行されるプログラムにて実現され、あるいは、ワイヤードロジックによるハードウェアとして実現され得る。

【０１４８】

なお、本実施例で説明した権限委譲方法は、あらかじめ用意されたプログラムをパーソナルコンピュータやワークステーションなどのコンピュータで実行することによって実現することができる。このプログラムは、インターネットなどのネットワークを介して配布することができる。また、このプログラムは、ハードディスク、フレキシブルディスク（ＦＤ）、ＣＤ－ＲＯＭ、ＭＯ、ＤＶＤなどのコンピュータで読み取り可能な記録媒体に記録され、コンピュータによって記録媒体から読み出されることによって実行することもできる。

【産業上の利用可能性】

【０１４９】

以上のように、本発明に係る権限委譲システム、権限委譲方法および権限委譲プログラムは、アプリケーションサーバを利用する利用者の権限を判定して当該アプリケーションサーバの利用を制御することに有用であり、特に、権限を適切に委譲することに適する。

【図面の簡単な説明】

【０１５０】

【図１】実施例１に係る権限委譲システムの概要および特徴を説明するための図である。

【図２】実施例１に係る権限委譲システムの構成を示すブロック図である。

【図３】実施例１に係る権限委譲システムの構成を示すブロック図である。

【図４】認証用ＩＣカードの発行と認証情報の格納の流れを説明するための図である。

【図５】権限委譲証明書に必要な構成要素を説明するための図である。

【図６】権限委譲情報パターンについて説明するための図である。

【図７】権限委譲証明書を申請する際の申請内容を説明するための図である。

【図８】権限委譲証明書を認証用ＩＣカードに格納するまでの流れを説明するための図である。

【図９】本発明におけるシングルサインオン認証およびバックエンドアプリケーションサーバ５での認可のシステム構成例を示す図である。

【図１０】本発明におけるシングルサインオン認証処理の流れを説明するための図である。

【図１１】権限を有した利用者での認可処理を説明するための図である。

【図１２－１】権限を委譲された利用者での認可処理の流れを説明するための図である。

【図１２－２】権限を委譲された利用者での認可処理の流れを説明するための図である。

【図１３－１】権限を委譲された利用者が権限変更を行う認可処理の流れを説明するための図である。

【図１３－２】権限を委譲された利用者が権限変更を行う認可処理の流れを説明するための図である。

【図１４】従来技術を説明するための図である。

【図１５】従来技術を説明するための図である。

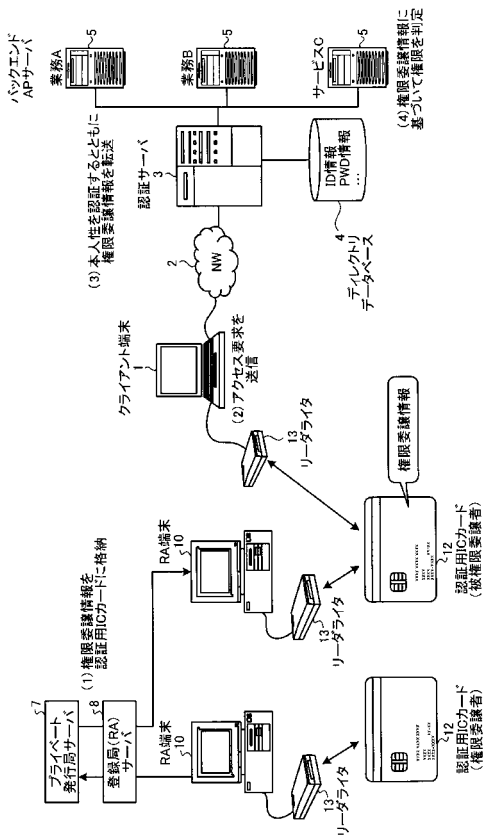
【符号の説明】

【０１５１】

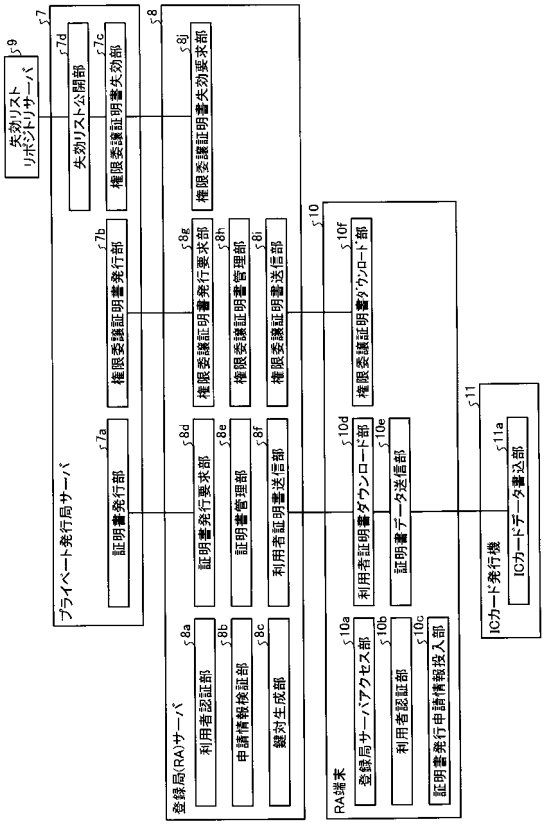
１　クライアント端末
１ａ　証明書一覧部
１ｂ　ＩＣカードアクセス部
１ｃ　権限委譲証明書送信部
２　ネットワーク
３　認証サーバ
３ａ　権限委譲証明書要求画面部
３ｂ　権限委譲証明書検証部
３ｃ　権限委譲証明書転送部
３ｄ　認可結果画面表示部
４　ディレクトリデータベース
５　バックエンドアプリケーションサーバ
５ａ　権限委譲証明書要求部
５ｂ　権限委譲証明書確認部
５ｃ　失効情報確認部
５ｄ　認可結果通知部
７　プライベート発行局サーバ
７ａ　証明書発行部
７ｂ　権限委譲証明書発行部
７ｃ　権限委譲証明書失効部
７ｄ　失効リスト公開部

８　登録局（ＲＡ）サーバ
８ａ　利用者認証部
８ｂ　申請情報検証部
８ｃ　鍵対生成部
８ｄ　証明書発行要求部
８ｅ　証明書管理部
８ｆ　利用者証明書送信部
８ｇ　権限委譲証明書発行要求部
８ｈ　権限委譲証明書管理部
８ｉ　権限委譲証明書送信部
８ｊ　権限委譲証明書失効要求部
９　失効リストリポジトリサーバ
１０　ＲＡ端末
１０ａ　登録局サーバアクセス部
１０ｂ　利用者認証部
１０ｃ　証明書発行申請情報投入部
１０ｄ　利用者証明書ダウンロード部
１０ｅ　証明書データ送信部
１０ｆ　権限委譲証明書ダウンロード部
１１　ＩＣカード発行機
１１ａ　ＩＣカードデータ書込部
１２　認証用ＩＣカード
１３　リーダライタ

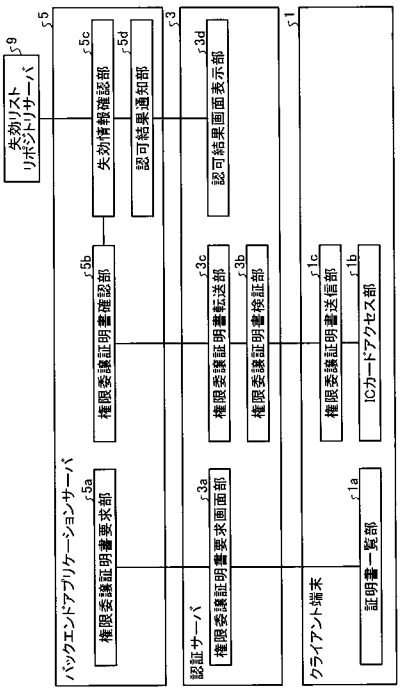
【図１】



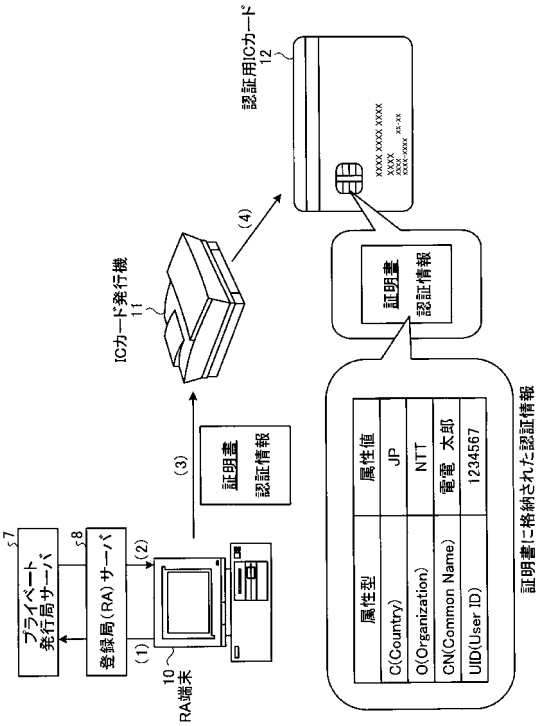
【図２】



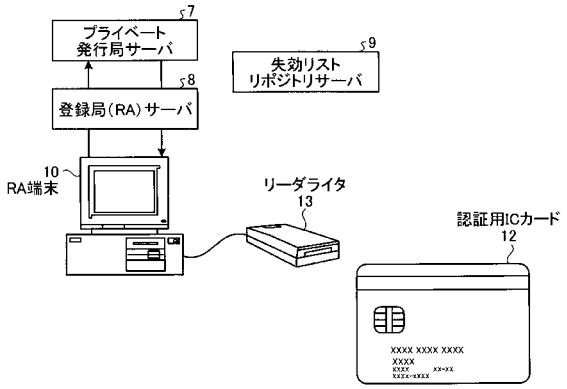
【図３】



【図４】



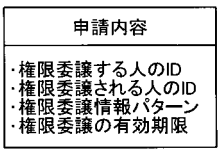
【図５】



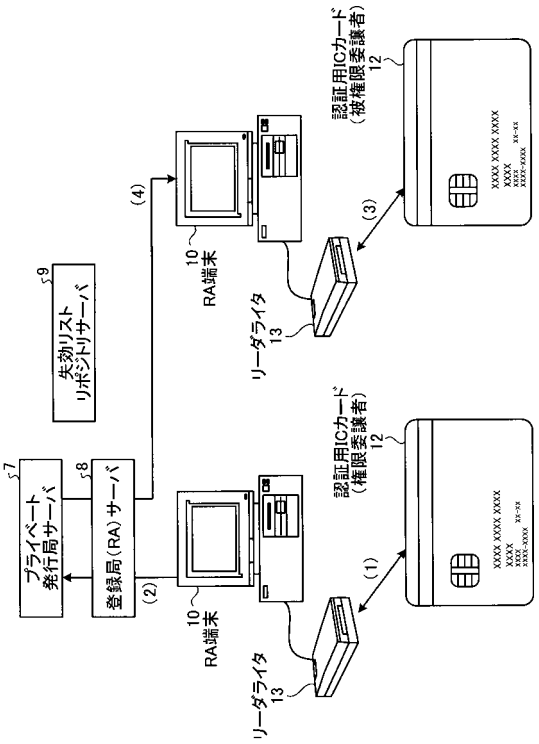
【図６】

権限を委譲する人	権限を委譲される人	対象業務	委譲範囲	パターン 1	2	3	4	5
管理者（部課長以上）	秘書 部下	社内稟議	申請	×	×	○	○	○
			決済	×	×	×	×	○
		物品購入	申請	×	×	○	○	○
			決済	×	×	×	×	○
		社内各種処理	申請	×	×	○	○	○
			決済	×	×	×	×	○
		旅費	申請	×	○	×	○	○
			決済	×	×	×	×	○
		休暇等願	申請	×	○	○	○	○
			決済	×	×	×	×	○
		スケジュール	登録	○	○	○	○	○

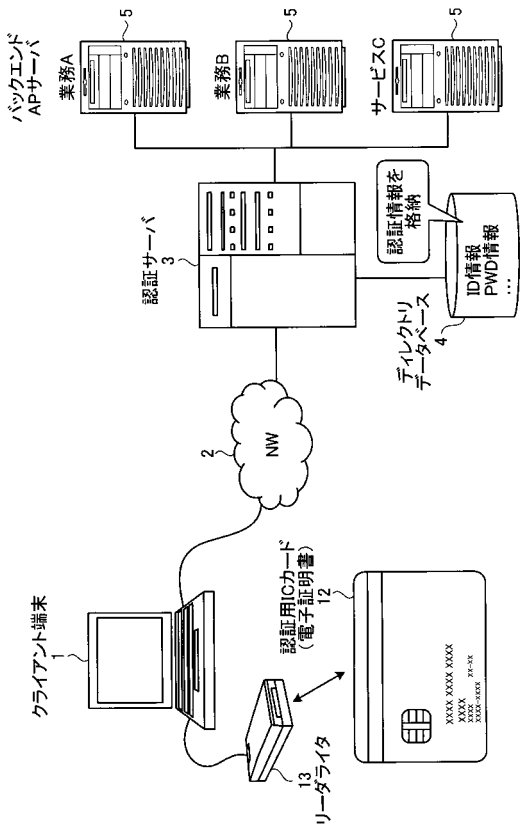
【図７】


申請内容
・権限委譲する人のID
・権限委譲される人のID
・権限委譲情報パターン
・権限委譲の有効期限

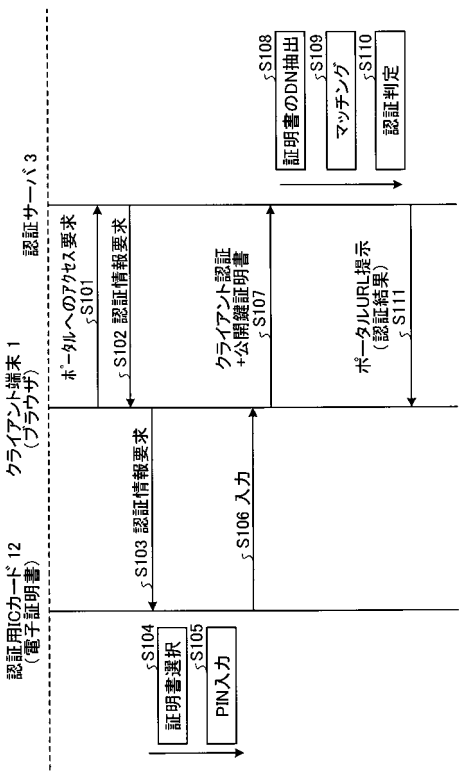
【図８】


認証用ICカード
（被権限委譲者）
12
失効リスト
リポジトリサーバ
9
RA端末
10
リーダライタ
13
プライベート
発行局サーバ
7
登録局(RA)サーバ
8
(1)
(2)
(3)
(4)

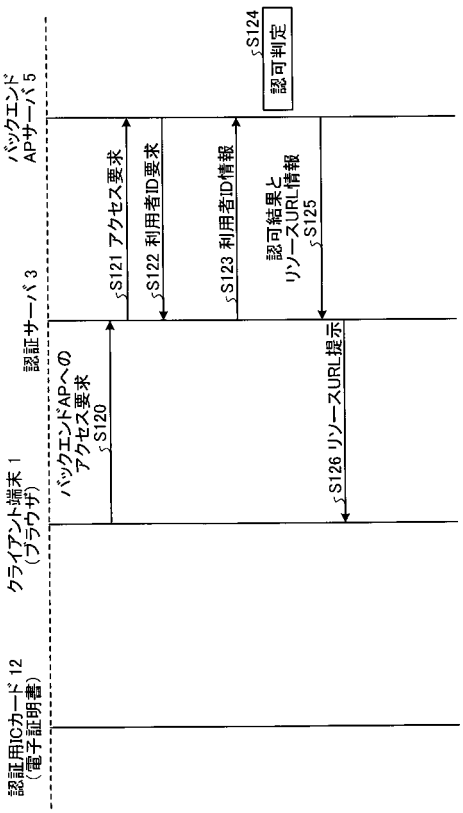
【図９】


バックエンド
APサーバ
業務A
業務B
サービスC
5
認証サーバ
3
認証情報を
格納
ID情報
PWD情報
…
ディレクトリ
データベース
4
NW
2
クライアント端末
1
認証用ICカード
（電子証明書）
12
リーダライタ
13

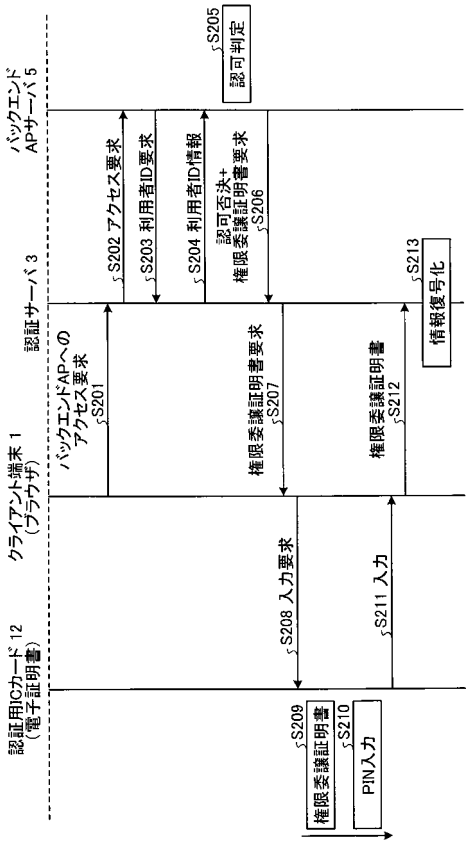
【図１０】


認証用ICカード 12
（電子証明書）
クライアント端末 1
（ブラウザ）
認証サーバ 3
ポータルへのアクセス要求
S101
S102 認証情報要求
S103 認証情報要求
S104
証明書選択
S105
PIN入力
S106 入力
クライアント認証
+公開鍵証明書
S107
ポータルURL提示
（認証結果）
S111
S108
証明書のDN抽出
S109
マッチング
S110
認証判定

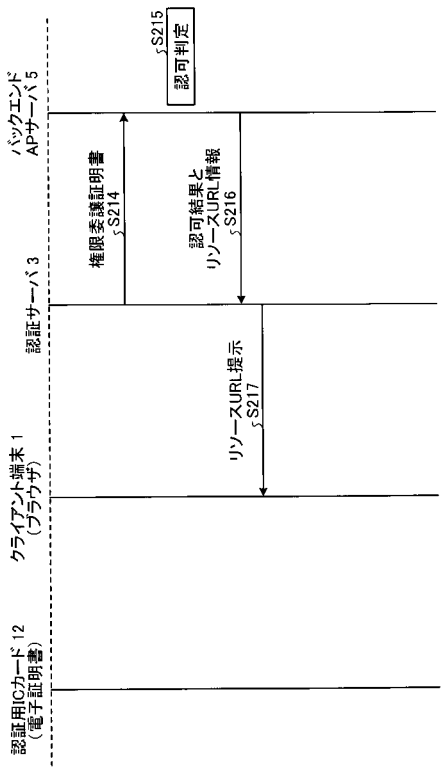
【図１１】



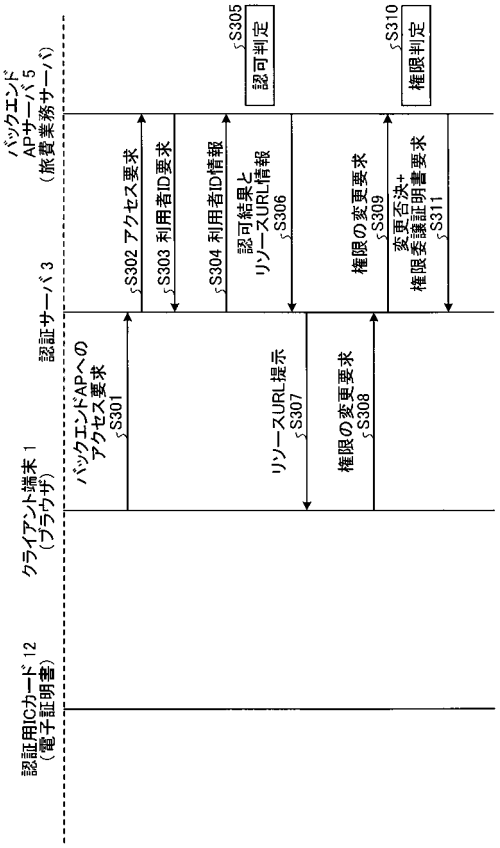
【図１２－１】



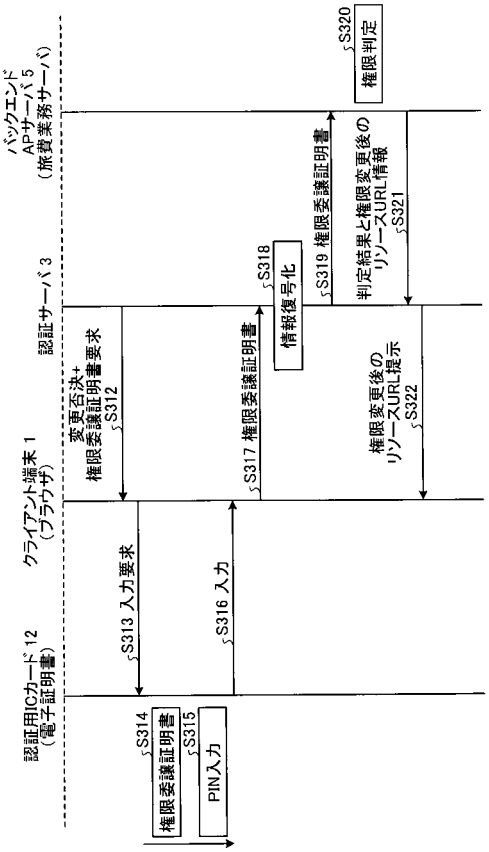
【図１２－２】



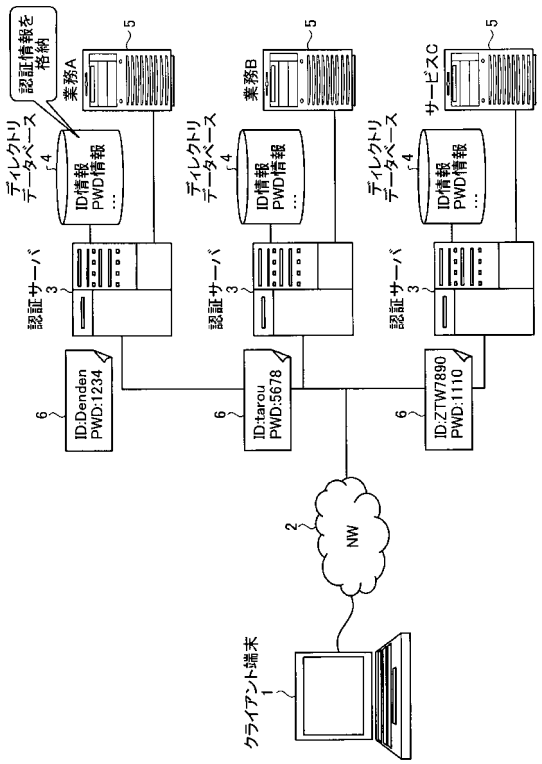
【図１３－１】



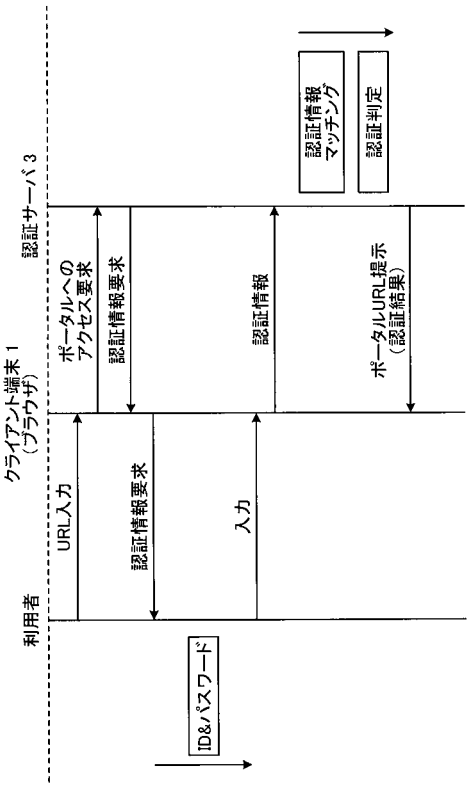
【図１３－２】


認証用ICカード 12
(電子証明書)
クライアント端末 1
(ブラウザ)
認証サーバ 3
バックエンド
APサーバ 5
(旅費業務サーバ)
S314
権限委譲証明書
S315
PIN入力
S313 入力要求
S316 入力
変更否決+
権限委譲証明書要求
S312
S317 権限委譲証明書
S318
情報復号化
S319 権限委譲証明書
S320
権限判定
判定結果と権限変更後の
リソースURL情報
S321
権限変更後の
リソースURL提示
S322

【図１４】


認証情報を格納
ディレクトリデータベース 4
ID情報
PWD情報
…
業務A
業務B
サービスC
5
認証サーバ 3
6
ID:Denden
PWD:1234
ID:tarou
PWD:5678
ID:ZTW7890
PWD:1110
2
NW
クライアント端末 1

【図１５】


利用者
クライアント端末 1
(ブラウザ)
認証サーバ 3
URL入力
ポータルへの
アクセス要求
認証情報要求
認証情報
ポータルURL提示
(認証結果)
認証情報要求
入力
ID&パスワード
認証情報
マッチング
認証判定

フロントページの続き

(72)発明者　青柳　真紀子
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　永井　靖浩
京都府京都市左京区吉田本町　国立大学法人京都大学大学院情報学研究科内
(72)発明者　古村　隆明
京都府京都市左京区吉田本町　国立大学法人京都大学大学院情報学研究科内

審査官　▲吉▼田　耕一

(56)参考文献　特開２００４－２０６１８７（ＪＰ，Ａ）
特開２００１－２４３５１７（ＪＰ，Ａ）
特開平０６－１８８９０５（ＪＰ，Ａ）
特開２００６－００４３１４（ＪＰ，Ａ）
特開２００６－２２１５０６（ＪＰ，Ａ）
特開２００５－０１０３０１（ＪＰ，Ａ）

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