

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2009-205342

(P2009-205342A)

(43) 公開日 平成21年9月10日(2009.9.10)

(51) Int.Cl.			F I			テーマコード (参考)		
G06F	21/20	(2006.01)	G06F	15/00	330D	5B285		
H04L	9/32	(2006.01)	G06F	15/00	330G	5J104		
			H04L	9/00	675D			

審査請求 未請求 請求項の数 9 O L (全 33 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)

(71) 出願人 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
 (71) 出願人 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 100114306
 弁理士 中辻 史郎
 (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

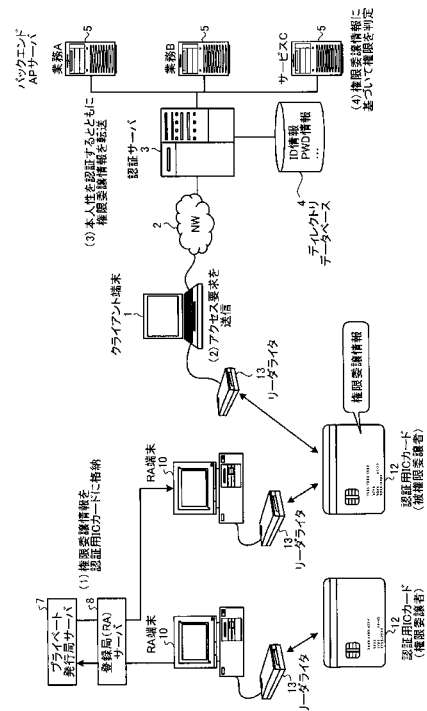
(54) 【発明の名称】 権限委譲システム、権限委譲方法および権限委譲プログラム

(57) 【要約】

【課題】 権限を適切に委譲することを課題とする。

【解決手段】 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。認証サーバは、アクセス要求を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、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し、アプリケーションサーバ各々は、転送された権限委譲情報等を受け付けると、当該権限委譲情報等に基づいて、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。

【選択図】 図1



【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、

10

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に基づいて、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。

20

【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、権限を他の利用者へ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。

30

【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、

40

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

50

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。

10

【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、

20

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。

30

【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、

40

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

50

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に基づいて、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に基づいて、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】

10

20

30

40

50

【 0 0 0 2 】

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）。

【 0 0 0 3 】

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。

10

【 0 0 0 4 】

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。

20

【 0 0 0 5 】

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、せつ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。

【 0 0 0 6 】

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。

30

【 0 0 0 7 】

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働の分割損も大きく改善される。

40

【 0 0 0 8 】

【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

50

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 】

【 0 0 0 9 】

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。

【 0 0 1 0 】

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。

【 0 0 1 1 】

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。

【 0 0 1 2 】

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。

【 0 0 1 3 】

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 】

【 0 0 1 4 】

上述した課題を解決し、目的を達成するため、請求項1に係る発明は、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

10

20

30

40

50

、当該権限委譲情報もしくは当該情報に基づいて、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、請求項2に係る発明は、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、請求項3に係る発明は、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。

10

【0017】

また、請求項4に係る発明は、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。

20

30

【0018】

また、請求項5に係る発明は、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

40

50

権限委譲証明書を発行することを特徴とする。

【0019】

また、請求項6に係る発明は、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。

10

【0020】

また、請求項7に係る発明は、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に基づいて、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。

20

30

【0021】

また、請求項8に係る発明は、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に基づいて、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。

40

【0022】

また、請求項9に係る発明は、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

50

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】

10

【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。

20

【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。

30

【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、発生源入力求められる、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。

40

【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

50

困)、(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ない。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。

10

【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。

20

【0032】

権限を委譲する立場の利用者と委譲された利用者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。

30

【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き、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。

40

【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

50

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。

【 0 0 3 6 】

[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。

【 0 0 3 7 】

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10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。

【 0 0 3 8 】

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10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。20

【 0 0 3 9 】

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 1 2（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 1 2 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。30

【 0 0 4 0 】

ここで、利用者証明書を認証用ICカード 1 2 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 1 0 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 1 0 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 1 0 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 1 0 から利用者証明書ダウンロード要求を受け付け、RA 端末 1 0 に対して利用者証明書を送信する。すると、RA 端末 1 0 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 1 2 に利用者証明書を書き込む。40

【 0 0 4 1 】

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 1 2 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 1 2 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 1 0 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50

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（R A）サーバ 8 は、R A 端末 1 0 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（R A）サーバ 8 に送信する。次に、登録局（R A）サーバ 8 は、被権限委譲者が操作する R A 端末 1 0 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 R A 端末 1 0 に対して権限委譲証明書を送信する。すると、当該 R A 端末 1 0 は、リーダライタ 1 3 に対して権限委譲証明書を送信し、リーダライタ 1 3 は、被権限委譲者の認証用 I C カード 1 2 に、権限委譲証明書を書き込む。

【 0 0 4 2 】

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 I C カード 1 2 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 I C カード 1 2 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 I C カード 1 2 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）。

10

【 0 0 4 3 】

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 I C カード 1 2 の利用者の権限を判定する（図 1 の（ 4 ）を参照）。

20

【 0 0 4 4 】

このように、実施例 1 に係る権限委譲システムは、認証用 I C カード 1 2 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。

【 0 0 4 5 】

[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、R A 端末 1 0、I C カード発行機 1 1、登録局（R A）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。

30

【 0 0 4 6 】

[R A 端末 1 0]

図 2 に示すように、実施例 1 における R A 端末 1 0 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 1 0 a と、利用者認証部 1 0 b と、証明書発行申請情報投入部 1 0 c と、利用者証明書ダウンロード部 1 0 d と、証明書データ送信部 1 0 e と、権限委譲証明書ダウンロード部 1 0 f とを備える。

【 0 0 4 7 】

登録局サーバアクセス部 1 0 a は、登録局（R A）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 1 0 a は、利用者（権限委譲者、被権限委譲者など）によって R A 端末 1 0 が操作されることで登録局（R A）サーバ 8 にアクセスする。例えば、登録局（R A）サーバ 8 が W e b 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 1 0 a は、R A 端末 1 0 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（R A）サーバ 8 に対して H T T P（HyperText Transfer Protocol）通信を行うことで、登録局（R A）サーバ 8 にアクセスすることができる。

40

【 0 0 4 8 】

利用者認証部 1 0 b は、登録局（R A）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 1 0 b は、登録局（R A）サーバ 8 の利用者認証

50

部 8 a との間で、R A 端末 1 0 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 1 0 b は、ブラウザと W e b サーバとの間における既存の I D / パスワード認証や、証明書を用いた S S L (Secure Socket Layer) 相互認証等により実現可能である。

【 0 0 4 9 】

証明書発行申請情報投入部 1 0 c は、登録局 (R A) 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 1 0 c は、登録局 (R A) サーバ 8 の申請情報検証部 8 b 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 1 0 c 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 I D 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。

10

【 0 0 5 0 】

利用者証明書ダウンロード部 1 0 d は、登録局 (R A) 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 1 0 d 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 (R A) サーバ 8 へ送信し、登録局 (R A) サーバ 8 から送信される利用者証明書データを R A 端末 1 0 に保存する。例えば、利用者証明書ダウンロード部 1 0 d 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 (R A) サーバ 8 へ送信し、登録局 (R A) サーバ 8 から送信される利用者証明書データを R A 端末 1 0 の記憶部に格納することで実現可能である。

20

【 0 0 5 1 】

証明書データ送信部 1 0 e は、利用者証明書や権限委譲証明書を I C カード発行機 1 1 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 1 0 e は、利用者証明書ダウンロード部 1 0 d によってダウンロードされ R A 端末 1 0 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 1 0 f によってダウンロードされ R A 端末 1 0 に保存された権限委譲証明書を、I C カード発行機 1 1 の I C カードデータ書込部 1 1 a に送信する。例えば、証明書データ送信部 1 0 e 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。

【 0 0 5 2 】

権限委譲証明書ダウンロード部 1 0 f は、登録局 (R A) 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 1 0 f 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 (R A) サーバ 8 へ送信し、登録局 (R A) サーバ 8 から送信される権限委譲証明書データを R A 端末 1 0 に保存する。例えば、権限委譲証明書ダウンロード部 1 0 f 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 (R A) サーバ 8 へ送信し、登録局 (R A) 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 I C カード 1 2 に格納することで実現可能である。

30

【 0 0 5 3 】

例えば、権限委譲証明書ダウンロード部 1 0 f 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 (R A) サーバ 8 へ送信し、登録局 (R A) 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、R A 端末 1 0 に接続されたリーダライタ 1 3 を介して、P K C S (Public Key Cryptography Standards) # 1 1 や M S - C A P I (Microsoft Crypto API) 等の標準的な I C 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 I C カード 1 2 へ書き込むことにより実現可能である。

40

【 0 0 5 4 】

[I C カード発行機 1 1]

図 2 に示すように、実施例 1 における I C カード発行機 1 1 は、本発明に特に密接に関

50

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。

10

【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。

20

【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。

30

【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。

40

【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 Syst

50

em)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。

10

【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。

20

【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。

30

【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。

40

【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

50

ションにより実現可能である。

【 0 0 7 1 】

失効リスト公開部 7 d 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 7 d は、権限委譲証明書失効部 7 c 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 7 d は、既存の L D A P (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。

【 0 0 7 2 】

[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 1 a と、IC カードアクセス部 1 b と、権限委譲証明書送信部 1 c とを備える。

10

【 0 0 7 3 】

証明書一覧部 1 a 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 1 a は、認証サーバ 3 の権限委譲証明書要求画面部 3 a による画面情報を受信すると、リーダライタ 1 3 を介して認証用 IC カード 1 2 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 1 a は、既存のブラウザ等により実現可能である。

【 0 0 7 4 】

20

IC カードアクセス部 1 b は、認証用 IC カード 1 2 にアクセスする。具体的には、IC カードアクセス部 1 b は、リーダライタ 1 3 を介して認証用 IC カード 1 2 にアクセスし、当該認証用 IC カード 1 2 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 1 b の P I N 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。

【 0 0 7 5 】

権限委譲証明書送信部 1 c 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 1 c は、IC カードアクセス部 1 b 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 3 b に送信する。例えば、権限委譲証明書送信部 1 c は、既存のブラウザと、W e b サーバとの間の送受信機能を用いること

30

【 0 0 7 6 】

[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 3 a と、権限委譲証明書検証部 3 b と、権限委譲証明書転送部 3 c と、認可結果画面表示部 3 d とを備える。

【 0 0 7 7 】

権限委譲証明書要求画面部 3 a 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 3 a 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 5 a 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 3 a の画面表示させるための電文生成や送信機能は、通常の W e b アプリケーションシステムにおいて実現可能である。

40

【 0 0 7 8 】

権限委譲証明書検証部 3 b 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 3 b は、クライアント端末 1 の権限委譲証明書送信部 1 c 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 3 c に伝達する。例えば、権限委譲証明書検証部 3 b は、既存の W e b サーバにおける S S L 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。

【 0 0 7 9 】

50

権限委譲証明書転送部 3 c 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 3 c は、権限委譲証明書検証部 3 b 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 5 b に送信する。例えば、権限委譲証明書転送部 3 c 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。

【 0 0 8 0 】

認可結果画面表示部 3 d 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 3 d 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 5 d 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 3 d 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。

10

【 0 0 8 1 】

[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 5 a と、権限委譲証明書確認部 5 b と、失効情報確認部 5 c と、認可結果通知部 5 d とを備える。

【 0 0 8 2 】

権限委譲証明書要求部 5 a 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 5 a 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 5 a 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。

20

【 0 0 8 3 】

権限委譲証明書確認部 5 b 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 5 b は、認証サーバ 3 の権限委譲証明書転送部 3 c 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 5 b 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。

【 0 0 8 4 】

失効情報確認部 5 c は、失効情報を確認する。具体的には、失効情報確認部 5 c 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 5 c 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。

30

【 0 0 8 5 】

認可結果通知部 5 d は、認可結果を通知する。具体的には、認可結果通知部 5 d は、権限委譲証明書確認部 5 b や失効情報確認部 5 c 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 3 d に送信する。例えば、認可結果通知部 5 d 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。

【 0 0 8 6 】

[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。

40

【 0 0 8 7 】

[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

50

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）。

10

【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。

20

【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）。

30

【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）。

40

【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】

50

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。

【 0 0 9 6 】

[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ーライタ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。

10

【 0 0 9 7 】

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手簡素化が可能になる。

20

【 0 0 9 8 】

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。

【 0 0 9 9 】

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をリーダーライタ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）。

30

【 0 1 0 0 】

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。

40

【 0 1 0 1 】

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、

50

権限委譲証明書発行申請データには、R A 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。

【 0 1 0 2 】

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 7 b）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。

【 0 1 0 3 】

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 8 h）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（R A）サーバ 8 内に格納する（図 8 の（4）を参照）。

【 0 1 0 4 】

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 R A 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 10 a）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 10 b）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。

【 0 1 0 5 】

そして、被権限委譲者が利用する R A 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 10 f）を用いて、登録局（R A）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 8 a）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 8 i）を用いて、被権限委譲者が利用する R A 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 R A 端末 10 に対してこれを送信する。

【 0 1 0 6 】

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 R A 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。

【 0 1 0 7 】

[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、R A 端末 10 を通して、失効リポジトリサーバ 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。

【 0 1 0 8 】

まず、権限委譲を希望した利用者は、R A 端末 10 において自分の認証用 IC カード 1

10

20

30

40

50

2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。

10

【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。

20

【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)。

30

【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。

40

【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

50

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、リーダー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

10

20

30

40

50

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）。 10

【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して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。 20

【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。 30

【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）。 40

【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。 40

【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 50

(ステップ S 3 0 1 ~ S 3 0 7)、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 S 3 0 8 および S 3 0 9)。

【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 S 3 1 0)、権限委譲証明書要求機能(権限委譲証明書要求部 5 a)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 S 3 1 1)。

【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 1 2 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 S 3 1 2 から S 3 1 9)。

10

【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 5 b)および失効情報確認部(失効情報確認部 5 c)を用いて、図 1 2 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 5 d)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 S 3 2 1)、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 S 3 2 2)。

【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。

20

【0136】

以上が、認証用 IC カード 1 2 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 1 2 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】

30

[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 of 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。

40

【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 of 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、

50

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。

【 0 1 4 1 】

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。

【 0 1 4 2 】

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く代わりに、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。

10

【 0 1 4 3 】

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。

20

【 0 1 4 4 】

従来技術では、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する複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、複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。

30

【 実施例 2 】

【 0 1 4 5 】

[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。

【 0 1 4 6 】

[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。

40

【 0 1 4 7 】

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

50

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。

10

【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。

20

【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。

30

【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。

40

【符号の説明】

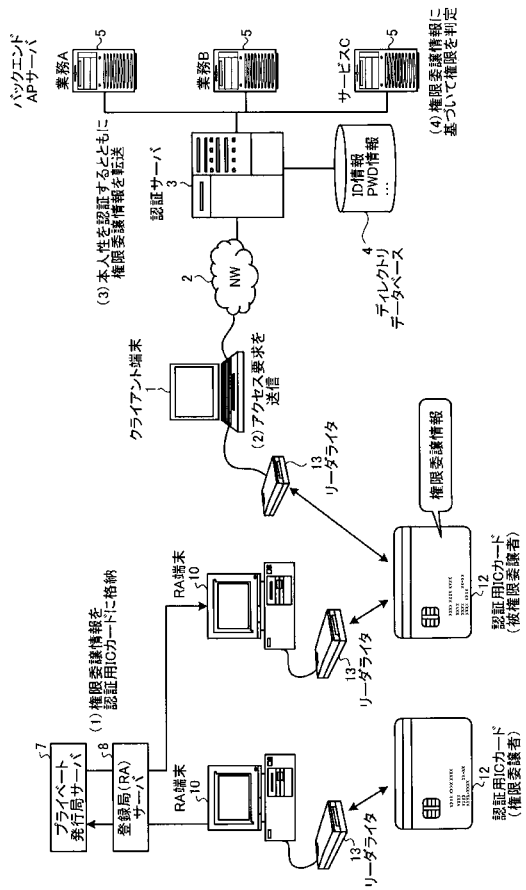
【0151】

- 1 クライアント端末
 - 1 a 証明書一覧部
 - 1 b ICカードアクセス部
 - 1 c 権限委譲証明書送信部
- 2 ネットワーク
- 3 認証サーバ
 - 3 a 権限委譲証明書要求画面部
 - 3 b 権限委譲証明書検証部
 - 3 c 権限委譲証明書転送部

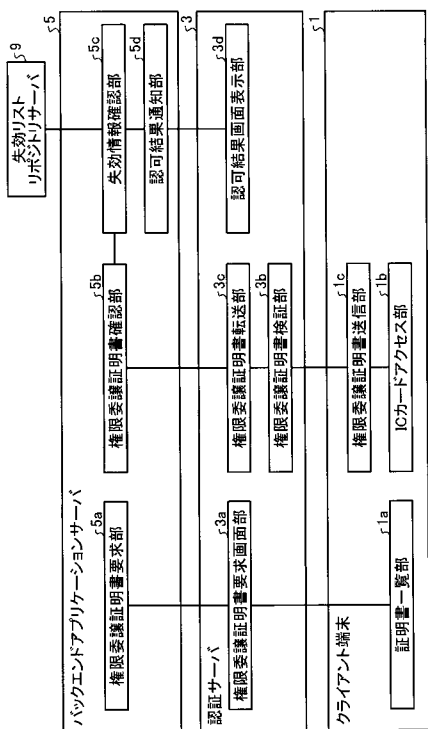
50

- 3 d 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
- 5 a 権限委譲証明書要求部
- 5 b 権限委譲証明書確認部
- 5 c 失効情報確認部
- 5 d 認可結果通知部
- 7 プライベート発行局サーバ
- 7 a 証明書発行部
- 7 b 権限委譲証明書発行部 10
- 7 c 権限委譲証明書失効部
- 7 d 失効リスト公開部
- 8 登録局(RA)サーバ
- 8 a 利用者認証部
- 8 b 申請情報検証部
- 8 c 鍵対生成部
- 8 d 証明書発行要求部
- 8 e 証明書管理部
- 8 f 利用者証明書送信部
- 8 g 権限委譲証明書発行要求部 20
- 8 h 権限委譲証明書管理部
- 8 i 権限委譲証明書送信部
- 8 j 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
- 10 a 登録局サーバアクセス部
- 10 b 利用者認証部
- 10 c 証明書発行申請情報投入部
- 10 d 利用者証明書ダウンロード部
- 10 e 証明書データ送信部 30
- 10 f 権限委譲証明書ダウンロード部
- 11 ICカード発行機
- 11 a 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

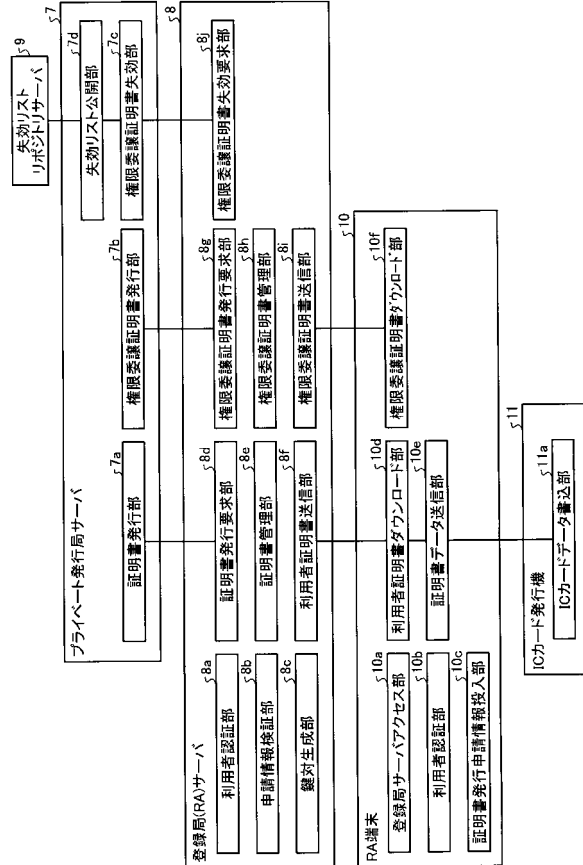
【図 1】



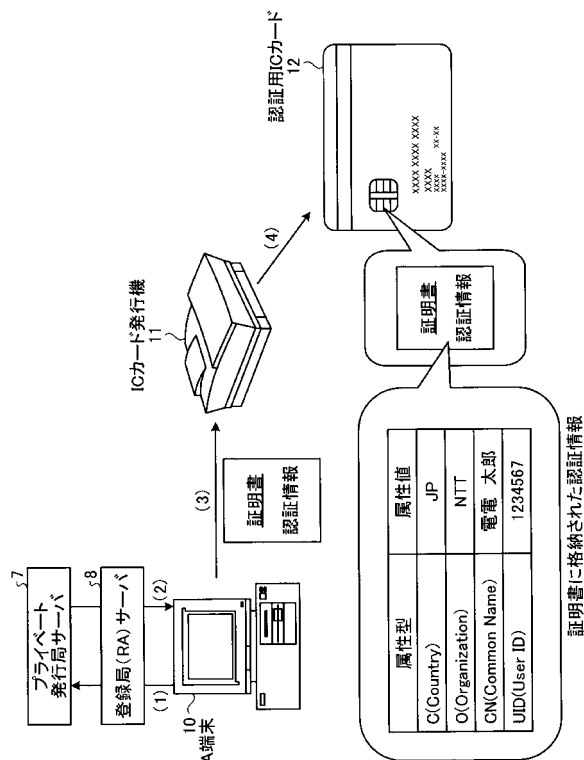
【図 3】



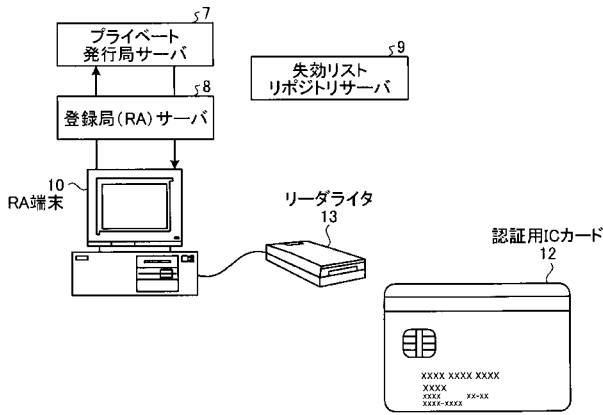
【図 2】



【図 4】



【 図 5 】



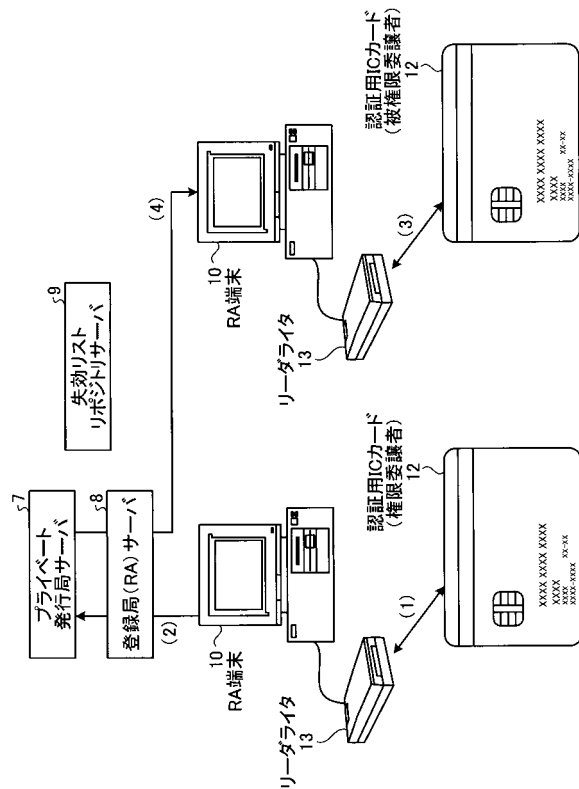
【 図 6 】

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 管理長以上 (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	○	○	○	○	○	○

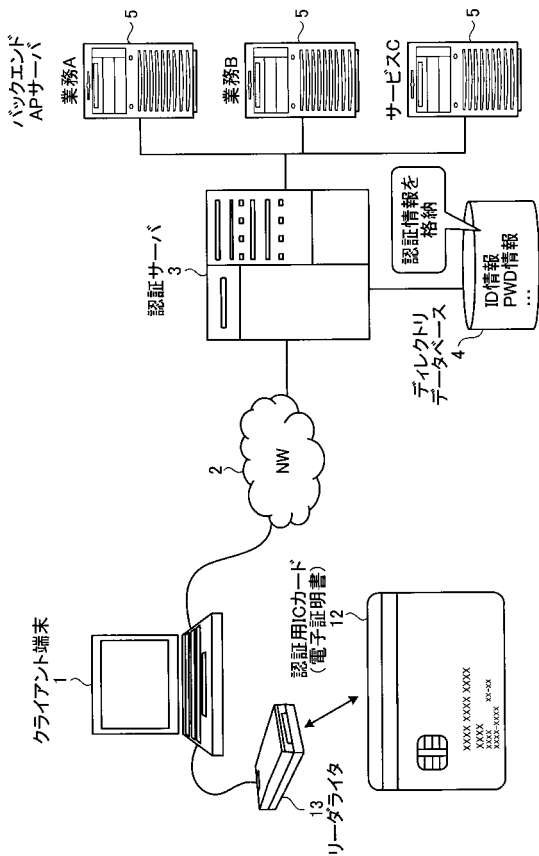
【 図 7 】

申請内容
<ul style="list-style-type: none"> 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

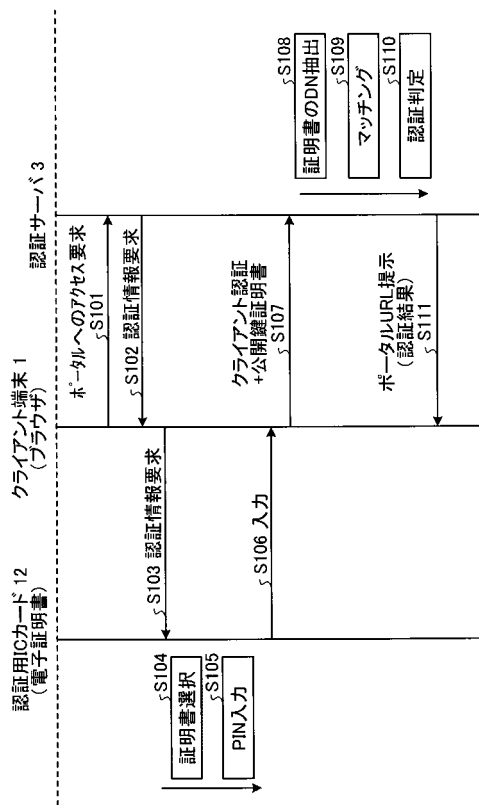
【 図 8 】



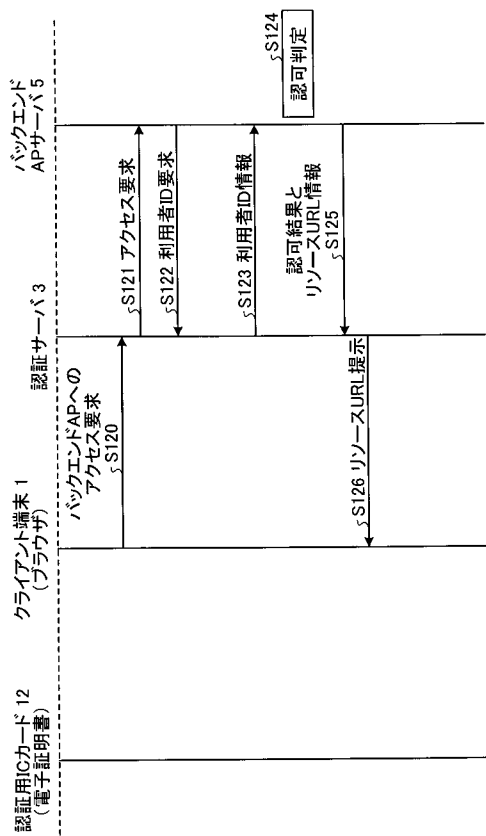
【 図 9 】



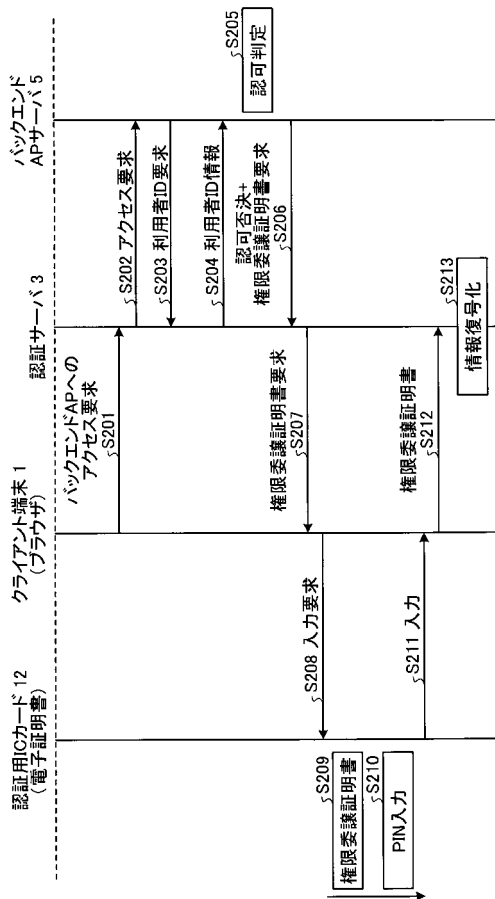
【 図 10 】



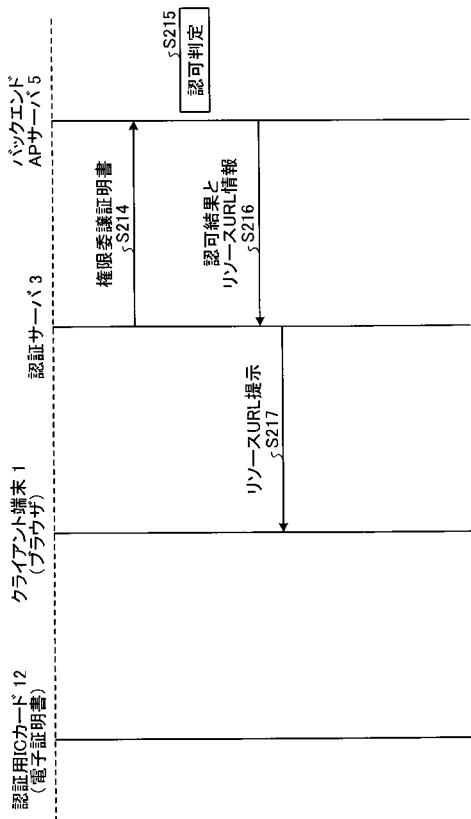
【 図 11 】



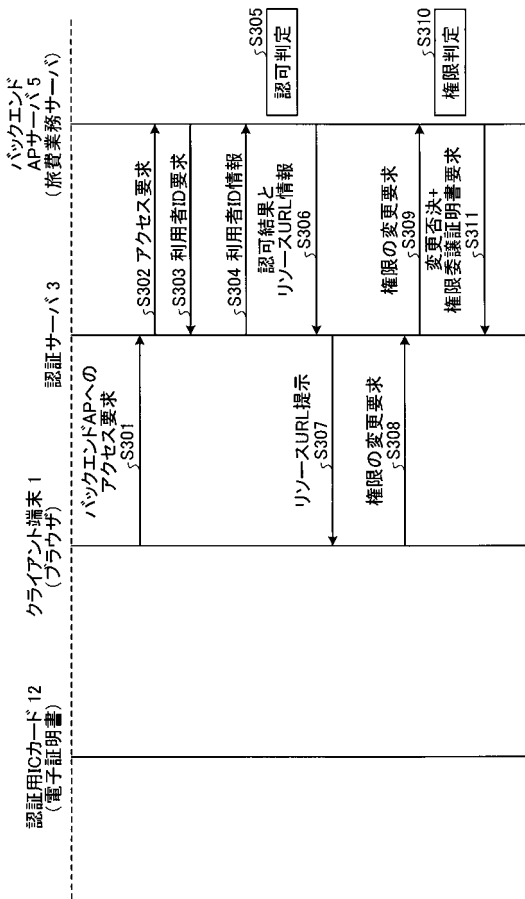
【 図 12 - 1 】



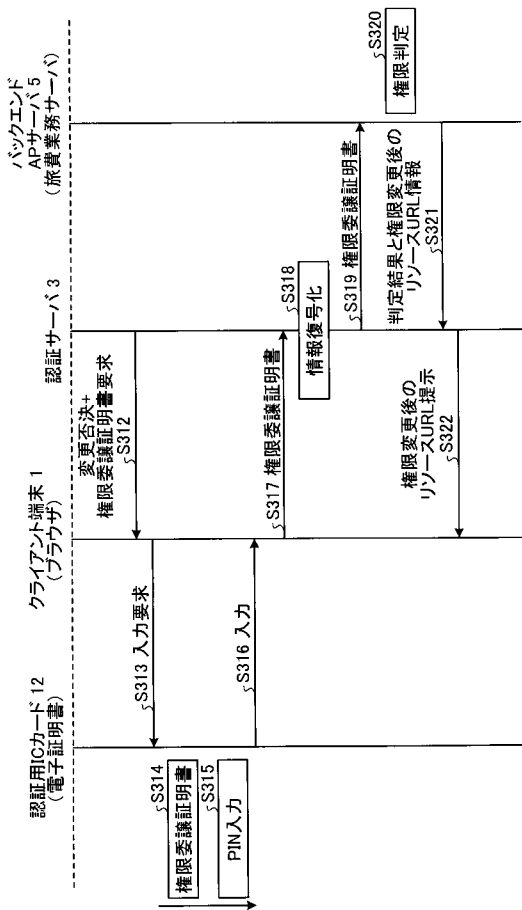
【 図 1 2 - 2 】



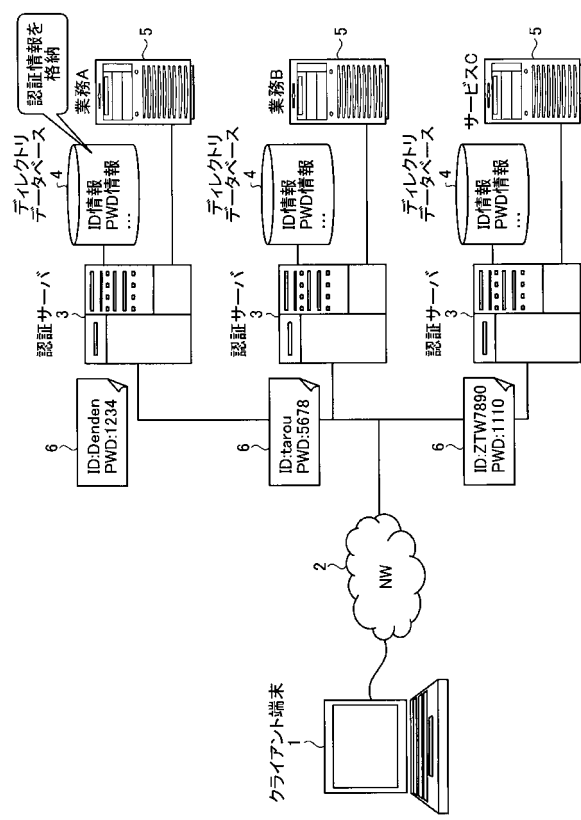
【 図 1 3 - 1 】



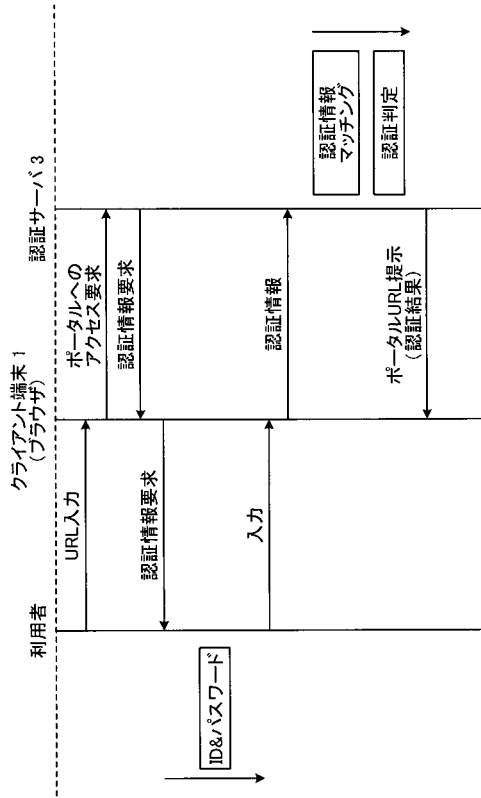
【 図 1 3 - 2 】



【 図 1 4 】



【 図 1 5 】



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所内

(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所内

Fターム(参考) 5B285 AA01 BA03 CA02 CA17 CA43 CB02 CB07 CB47 CB53 CB64

CB72 CB83 CB90 CB92

5J104 AA07 AA16 EA04 EA05 EA15 EA16 JA21 KA01 KA05 LA03

LA06 MA01 NA02 NA05 NA27 NA37 NA38