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

特許第5126968号
(P5126968)

(45)発行日　平成25年1月23日(2013.1.23)　(24)登録日　平成24年11月9日(2012.11.9)

(51)Int.Cl.		F I		
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	675Z

請求項の数 4　(全 14 頁)

(21)出願番号　特願2008-44093(P2008-44093)
(22)出願日　平成20年2月26日(2008.2.26)
(65)公開番号　特開2009-205230(P2009-205230A)
(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　100121706
弁理士　中尾　直樹
(74)代理人　100128705
弁理士　中村　幸雄
(74)代理人　100147773
弁理士　義村　宗洋
(74)代理人　100066153
弁理士　草野　卓

最終頁に続く

(54)【発明の名称】認証・認可システム、認証・認可方法

(57)【特許請求の範囲】
【請求項１】
ユーザの本人認証に用いられるルート認証局またはこのルート認証局を上位に持つ中間認証局が発行した電子証明書（利用者証明書）と、ユーザのアプリケーションサーバ装置へのアクセス認可の判定に用いられる上記ルート認証局または上記ルート認証局を上位に持つ中間認証局が発行した電子証明書（資格証明書）とを記録した、耐タンパー性を持つ耐タンパーデバイスと、
上記耐タンパーデバイスに記録された上記利用者証明書および上記資格証明書の入力を受け付ける受付手段と、上記利用者証明書または上記資格証明書を認証サーバ装置に送信可能な送信手段とを備えるクライアント装置と、
上記クライアント装置から上記利用者証明書または上記資格証明書を受信する受信手段と、上記利用者証明書を用いて本人認証を行う認証手段と、上記資格証明書をアプリケーションサーバ装置に送信する送信手段とを備える認証サーバ装置と、
上記認証サーバ装置から上記資格証明書を受信する受信手段と、上記資格証明書を用いてアクセス認可の判定を行う認可判定手段とを備えるアプリケーションサーバ装置とを備える認証・認可システム。
【請求項２】
上記利用者証明書はユーザに唯一つ発行され、
上記資格証明書はユーザのアプリケーションサーバ装置へのアクセス権限に基づいて一つまたは複数発行されている

ことを特徴とする請求項１に記載の認証・認可システム。
【請求項３】
耐タンパー性を持つ耐タンパーデバイスには、ユーザの本人認証に用いられるルート認証局またはこのルート認証局を上位に持つ中間認証局が発行した電子証明書（利用者証明書）と、ユーザのアプリケーションサーバ装置へのアクセス認可の判定に用いられる上記ルート認証局または上記ルート認証局を上位に持つ中間認証局が発行した電子証明書（資格証明書）が記録されており、
クライアント装置の受付手段が、上記耐タンパーデバイスに記録された上記利用者証明書および上記資格証明書の入力を受け付ける受付ステップと、
クライアント装置の送信手段が、上記利用者証明書を認証サーバ装置に送信する利用者証明書送信ステップと、
認証サーバ装置の受信手段が、上記クライアント装置から上記利用者証明書を受信する利用者証明書受信ステップと、
認証サーバ装置の認証手段が、上記利用者証明書を用いて本人認証を行う認証ステップと、
クライアント装置の送信手段が、上記本人認証に成功した場合に上記資格証明書を認証サーバ装置に送信する資格証明書送信ステップと、
認証サーバ装置の受信手段が、上記クライアント装置から上記資格証明書を受信する資格証明書受信ステップと、
認証サーバ装置の送信手段が、アプリケーションサーバ装置に上記資格証明書を送信する送信ステップと、
アプリケーションサーバ装置の受信手段が、上記認証サーバ装置から上記資格証明書を受信する受信ステップと、
アプリケーションサーバ装置の認可判定手段が、上記資格証明書を用いてアクセス認可の判定を行う認可判定ステップと
を有する認証・認可方法。
【請求項４】
上記利用者証明書はユーザに唯一つ発行されており、
上記資格証明書はユーザのアプリケーションサーバ装置へのアクセス権限に基づいて一つまたは複数発行されており、
上記資格証明書送信ステップでは、一つまたは複数発行されている上記資格証明書の中から一つ選択して認証サーバ装置に送信される
ことを特徴とする請求項３に記載の認証・認可方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、利用者（ユーザ）が複数の属性を有し、この属性ごとにアプリケーションサーバのリソースへのアクセス権限を有する場合に、本人認証を行うと共に、その属性の選択によってアプリケーションサーバのリソース利用の認可を行う技術に関する。
【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、クライアントーサーバによってＷＥＢアプリケーションサーバが利用されている。サービス・業務ごとのアプリケーションサーバのリソースにアクセスするには、アクセスしようとするユーザの本人確認が必要であることが多い。このため、ユーザＩＤ（ユーザアカウント）とパスワード、ＩＣカード、電子証明書、バイオメトリックスなどを用いたユーザの本人確認行為、すなわち本人認証が行われている。
【０００３】
本人認証は通常、サービスや業務毎に行われるため、それぞれのユーザＩＤが同一ユーザに発行される。ユーザは第三者によるなりすましを防止するため、各ユーザＩＤに対し

て異なったパスワードを設定し、自己責任で管理・運用しなければならない。

【０００４】

一方、アプリケーションサーバ側がユーザに対してサービス・業務に関するアプリケーションサーバのリソース使用を許可する認可処理は、本人認証が各サービス・業務毎に行われてきたこともあり、本人認証処理と等価に扱われている（例えば非特許文献１、２参照）。このため、ユーザおよびアプリケーションサーバ側は認可を意識することはなかった。

【０００５】

ところで、ユーザの立場で複数のユーザ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、ユーザの利便性向上、ユーザ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、アプリケーションサーバ側の視点から、ユーザ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、本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う認証技術が導入されつつある（例えば非特許文献３参照）。

【０００６】

シングルサインオン認証は、例えば、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、認証サーバ装置と連携しているサービス・業務のアプリケーションサーバ装置にアクセスできるという認証方式である。図１に、ユーザＩＤとパスワードによるシングルサインオン認証処理の流れの一例を示す。ユーザはクライアント装置でポータルのＵＲＬ（Uniform Resource Locator）を入力し、認証サーバ装置に対してポータルへのアクセス要求を行う。認証サーバ装置はクライアント装置へ認証情報を要求し、ユーザはユーザＩＤとパスワードを入力する。クライアント装置はユーザＩＤとパスワードを認証サーバへ送信し、認証サーバ装置ではデータベースの認証情報とマッチングを行い、ユーザの同一性を判定する。この結果、正しいと判定されればクライアント装置へポータルのＵＲＬアクセスを許可し、シングルサインオン認証が完了する。

【０００７】

この機能により、ユーザは複数のサービス・業務毎にユーザＩＤとパスワードを覚える事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サーバ側もユーザＩＤの発行やそれに伴うユーザＩＤのライフサイクル管理が一元化される。また、サービス・業務毎に行っていたサービス・業務の本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】

シングルサインオン認証は、一度の認証でポータルに入り、登録されているバックエンドのＷＥＢアプリケーションサーバにアクセスすることができ、ユーザにとって非常に利便性の高い方式である。一方、最初に認証されれば、特定のアプリケーションサーバのリソースに自由にアクセスできることから、最初の認証をセキュアに行う必要がある。このため、シングルサインオン認証では、ＩＤとパスワードだけでなく、ＩＣカード利用といったより高セキュリティな多要素認証を用いることが望ましい。この時、ＩＣカードに格納されるのは、ユーザ本人を証明する利用者証明書（電子証明書）である。

【０００９】

ＩＣカードには利用者証明書を記録し、利用者証明書には会社名、名前、ユーザＩＤ、パスワードなどが含まれる。通常、ユーザが業務を行う業務組織に対応した発行局に対して、各部門などに設置した登録端末を使って電子申請し、発行された利用者証明書をダウンロードし、カード発行機へデータを送って、認証用ＩＣカードを作成する。登録局端末にダウンロードした利用者証明書は、ＩＣカードへ記録した段階で登録端末から自動的に消去される。このＩＣカードには認証に必要な情報を利用者証明書というデータで記録し、シングルサインオン認証に利用する。

【００１０】

図２はＩＣカード（利用者証明書）を使ったシングルサインオン認証の流れの一例である。ユーザＩＤとパスワードを用いた認証と異なるのは、ユーザ側でユーザＩＤおよびパスワードの入力の代わりに、ＩＣカードを利用してＰＩＮ入力することであり、認証に必要な識別名（ＤＮ：Domain Name）を暗号化してこれを認証サーバへ送信し、認証サーバ装置ではこれを復号化した後にデータベースに格納した識別名とマッチングさせて、認証の判定を行っている。認証ＯＫであれば、クライアント装置へポータルのＵＲＬを提示する。

【００１１】

図３はアクセス権限を有するユーザに対する認可処理の流れの一例を示す。まず、対象とするアプリケーションサーバ（ＡＰサーバ）へアクセスする権限を有するユーザの場合、クライアント装置から認証サーバ装置を経由して、対象となるアプリケーションサーバへアクセス要求を送る。バックエンドアプリケーションサーバはこれを受けてユーザＩＤを要求する。認証サーバ装置は認証をパスしたユーザＩＤをバックエンドアプリケーションサーバへ提示し、アプリケーションサーバはユーザデータベースと照合し、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を認証サーバ装置経由にてクライアント装置に表示させる。

【非特許文献１】京セラコミュニケーションシステム（株）、ＩＤ管理システム「GreenOffice Directory」, [平成20年2月6日検索], インターネット <URL : http://www.kccs.co.jp/products/directory/index.html>

【非特許文献２】Liberty Alliance ID-FF, [平成20年2月6日検索], インターネット <URL : http://www.projectliberty.org/resource_center/specifications/liberty_alliance_id_ff_1_2_specifications>

【非特許文献３】OASIS (Organization for the Advancement of Structured Information Standards), "Security Assertion Markup Language(SAML) v2.0", [平成20年2月6日検索], インターネット <URL : http://www.oasis-open.org/specs/index.php#samlv2.0>

【発明の開示】

【発明が解決しようとする課題】

【００１２】

上述のような認証方式で問題となるのは、今後一層、認証と認可を別々に扱うことが必要になるという点である。シングルサインオン認証は、複数のサービス・業務のリソースへアクセスする前段での本人確認である。一方、認可は、サービス・業務側が特定のユーザに対して、そのリソースを提供するか否かを判定することであり、本人認証に用いる情報とは異なった情報が必要になる。そのため通常は、（１）サービス・業務側のユーザデータベースに特定のユーザＩＤを登録し、シングルサインオン認証で得られたユーザＩＤとユーザデータベースのユーザＩＤとを比較し、認可判定を行う方式、（２）シングルサインオン認証サーバ側にサービス・業務毎にユーザＩＤ単位でのアクセスリストを作成し、そのリストに基づきサービス・業務側の認可を代行して行う方式があり、これらに基づいて認可を行っている。このような（１）または（２）の方式は、ユーザの属する業務組織からの申請に基づき、情報管理部門やサービス担当部門がデータを設定することにより実施されてきている。

【００１３】

一方、近年のダイナミックな人的リソースの活用に伴い、個人は会社に帰属するが、固定的な下位の業務組織（例えば、事業部や部門など）だけでなく、組織横断的なプロジェクトにも属するなど仕事のやり方が多様になってきている。また、企業も持株組織を多く採用しており、傘下のグループ企業は別会社となっていることが多い。さらには、教育機関などは独立法人化され、従来は人事異動といった扱いが退職と就職を繰り返す処理に代わり、従来以上に人的なリソースの流動が激しくなってきている。このような社会的な環境変化を受けて、個人の同一性は上位の持株組織で保証するが、よりダイナミックな人的リソース活用の観点から、プロジェクトといった下位の業務組織での役割や資格は上位組織では把握せず、下位の業務組織に任せるといった運用が始まりつつある。

【００１４】
このような状況で特に問題となるのは、或る特定のユーザＩＤを持つユーザが同一のアプリケーションに対して異なる立場（ユーザ属性）からのアクセス権限を有している場合であり、教育機関での兼担、企業での兼務に相当する。また、教育機関あるいは企業の組織をまたがってのプロジェクトでの業務の例でも同様であり、どの役割（ユーザ属性）でサービス・業務といったリソースにアクセスできるかが重要となる。
【００１５】
これらの問題に対する最も簡便な第１の方法は、プロジェクトなどの業務組織毎に、つまりアクセス権限等資格が異なる「ユーザ属性」毎に、ユーザＩＤを発行することである。現実に各会社単位で職員番号やユーザＩＤを発行し、会社内のリソースへのアクセスをコントロールしていることが多い。しかしこの方法は、例えばグループ企業内で会社を跨ったプロジェクトの場合、一人のユーザが複数のユーザＩＤを保持しなければならず、ユーザにとって煩雑な管理を強いられ、認証・認可のシステム側から見るとユーザＩＤ管理やライセンス費用負担が膨大になる。
【００１６】
総じて、人的リソースの流動が激しくなかった従来の組織では、アクセス権限等の認可判定に使うユーザＩＤは、サービス・業務を扱う会社内で管理運用されるものであり、その会社が他会社に跨ったユーザＩＤを発行するといった概念はなかった。
【００１７】
第２の方法として、ＩＣカード（利用者証明書）で認証・認可する場合、ＩＣカードはユーザ個人に対して発行され、基本証明書となる利用者証明書は所属する会社で発行され、兼務やプロジェクトで「ユーザ属性」が追加・更新される度毎に、利用者証明書を更新し、それをＩＣカードに入れなおすという方法がある。しかし、人的リソースの活用の観点から、兼務やプロジェクトの「ユーザ属性」が高頻度に更新されることを考えれば、ユーザや電子証明書の管理者にとって、その作業は膨大となり多くのミスも危惧される。また、社内に閉じていないプロジェクトの場合、社内で管理しているＩＣカード（利用者証明書）に社外も含めたプロジェクトの「ユーザ属性」を追加することは困難である。
【００１８】
第３の方法として、ユーザのユーザ属性が組織を跨って複数あり、かつユーザ属性が頻繁に更新されるような場合、前述した認可判定の方式（１）、（２）に従って、組織やプロジェクト毎に認証やサービス・業務システムの設定データの更新を繰り返すことが考えられる。
（１）サービス・業務側のユーザデータベースに特定のユーザＩＤを登録し、シングルサインオン認証で得られたＩＤとユーザデータベースのユーザＩＤとを比較し、認可判定を行う方式
（２）シングルサインオン認証側にサービス・業務毎にアクセスリストを作成し、そのリストに基づきサービス・業務側の認可を代行して行う方式
【００１９】
これらの方法は、認可に必要な「ユーザ属性」を設定・更新するといった作業が必要で、兼務やプロジェクトがその性格上頻繁に更新される事を考えると、管理運営のスタッフの負荷は非常に大きい。また、特定のプロジェクトは組織と扱われない場合も多く、組織内に閉じた、表面化しないプロジェクトもあり、それらに対するアクセス権限の設定、同一性確認やアクセス権限の妥当性などセキュリティの観点からも困難であった。
【００２０】
以上説明したように、人的なリソースを有効に活用している最近の教育機関や企業の環境では、単一の業務組織だけでなく、別の業務組織の兼務あるいは組織を跨ったプロジェクトで業務を行うことも多く、これら異なった「ユーザ属性」でのサービス・業務のリソースに対するアクセス権限は異なっている。
【００２１】
従来、人的なリソースを一つの業務組織で閉じて活用してきたため、「ユーザ属性」毎

の対応は、（１）ユーザ属性毎のユーザＩＤをユーザに付与する、（２）ＩＣカードの利用者証明書をユーザ属性毎に追加・更新する、（３）認証システムあるいはサービス・業務システムのユーザデータベースに「ユーザ属性」に応じた認可情報を必要が生じた時点で追加登録するといった方法がとられていた。しかし、（１）の方法ではユーザＩＤ管理の繁雑さやセキュリティリスクの問題、（２）の方法では作業の繁雑さと更新費用の問題、（３）の方法では登録の作業負担の問題があった。また近年のように、人的なリソースを有効活用する観点から、頻繁に業務組織が変わったり、異なる業務組織で兼務したりする場合、人的なリソースが流動的であるほど、集中管理の方式は向いていないと云える。従って、本人認証に加えて、「ユーザ属性」に応じたアプリケーションサーバへのアクセス権限を判定する認可を行う認証・認可方式が望まれている。

【課題を解決するための手段】

【００２２】

本発明では、ルート認証局またはこのルート認証局を上位に持つ中間認証局（例えば持株会社の人事部対応の認証局）が発行した電子証明書（利用者証明書）を本人認証に利用し、このルート認証局またはこのルート認証局を上位に持つ中間認証局（例えばプロジェクトなど業務組織対応の認証局）が発行した電子証明書（資格証明書）を認可に利用する。利用者証明書からルート認証局の下位認証局に対する証明書までの信頼のパスと、資格証明書からルート認証局の下位認証局に対する証明書までの信頼のパスとが別個に形成され、それぞれの信頼のパスの起点がルート認証局で同一となっている。利用者証明書と資格証明書は、耐タンパー性を持つ耐タンパーデバイスに記録される。利用者証明書はユーザに唯一つ発行されており、資格証明書はユーザのアプリケーションサーバ装置へのアクセス権限に基づいて一つまたは複数発行される。認可は、一つまたは複数発行されている資格証明書の中から一つ選択して行われる。

【発明の効果】

【００２３】

本発明に拠れば、本人認証用の電子証明書（利用者証明書）とアクセス認可用の電子証明書（資格証明書）を分離しているから、利用者証明書を用いて本人認証が可能である共に、ユーザ属性に応じた資格証明書を発行することで、ユーザ属性に応じたアプリケーションサーバへのアクセス権限を判定する認可を行うことができる。

【発明を実施するための最良の形態】

【００２４】

本発明は、複数の組織で構成された組織体における認証・認可に有用である。このような組織体として、持株会社を頂点とし、Ａ会社からＺ会社までを傘下企業とする企業形態を例に採り、この企業形態における認証局（ＣＡ局）の階層構造を図４に示す。認証局は、コンピュータで実現される。

【００２５】

持株会社のプライベート認証局（ルート認証局）を頂点に、その下位に各会社の中間認証局が並び、さらに各会社の中間認証局の下位に部、課、プロジェクトなどの中間認証局が配置され、階層構造を形成している。各認証局は、自身の担当する電子証明書を発行する。

【００２６】

この企業形態での構成員（ユーザ）は、持株会社傘下のＡ会社からＺ会社のいずれかにあるいは複数に跨って所属する。各構成員は、グループ全体でユニークな個人番号（ユーザＩＤ）を割り当てられている。本人認証に用いる利用者証明書（会社名、構成員の氏名、ユーザＩＤなどを含む。）は、職員証などの名目の例えばＩＣカードに記録され、このＩＣカードが持株会社から構成員に渡される。

【００２７】

図５に利用者証明書の信頼パスの一例を示す。この例は構成員「鈴木太郎」の利用者証明書の階層例であり、個人番号、グループでユニークなコモンネームなどが利用者証明書に格納される。利用者証明書の信頼を保証するのは持株会社の中間認証局（ルート認証局

の下位の認証局）である人事認証局が発行した人事証明書であり、さらに人事証明書の信頼を保証するのは持株会社のルート認証局が発行したルート証明書である。このように図５に示す階層構造に基づいた信頼のパスを構成することによって、グループ内のいずれの会社や部、課等の組織に異動しても、組織毎にＩＣカード（利用者証明書）を発行する必要は無く、人的リソースの効率的な活用とグループ内の人事流動性が担保される。なお、ＩＣカード（利用者証明書）の発行は持株会社で行うため、構成員本人が直接操作することは無く、例えば持株会社傘下のいずれかのグループ会社に配属した段階で構成員に渡せばよい。なお、この利用者証明書のＩＣカードへの記録の処理は従前と同じである。

【００２８】

次に、構成員「鈴木太郎」がＢ会社に入社し、プロジェクトＰで業務を行う場合を想定して、利用者証明書を記録したＩＣカードに資格証明書（電子証明書）を記録する処理を説明する。

資格証明書の登録、発行、資格証明書ダウンロードなどに必要な構成要素は、構成員が資格証明書の登録申請を入力し資格証明書を受信するクライアント装置、プロジェクトＰの資格証明書を発行する管理者装置、利用者証明書によって本人確認した上で申請や審査結果を受け付けるＢ会社の登録局サーバ装置、企画証明書の認証を行うＢ会社の認証局である。また、端末装置には利用者証明書で本人確認を行う場合などに利用するリーダライタが接続されている。

【００２９】

図６に資格証明書の信頼パスの一例を示す。構成員「鈴木太郎」が自らのＩＣカードにダウンロードする資格証明書は、図５に示した利用者証明書の信頼パスと階層が異なり、プロジェクトＰに固有の資格証明書となっている。この資格証明書の信頼を保証するのは、Ｂ会社内部の中間認証局（ルート認証局から見た中間認証局）であるプロジェクトＰ認証局が発行した企画証明書であり、この企画証明書の信頼を保証するのはＢ会社のプライベート認証局（持株会社のルート認証局から見た中間認証局）が発行したＢ会社証明書であり、このＢ会社証明書の信頼を保証するのは持株会社のルート認証局が発行したルート証明書である。資格証明書の信頼の起点となるルート証明書は、利用者証明書の信頼の起点となるルート証明書を発行する持株会社のルート認証局から発行されたものである。このような信頼のパスに基づく資格証明書を用いて、プロジェクトＰで使えるサービス・業務のアプリケーションリソースへのアクセス認可を行う。

【００３０】

ここで資格証明書の内実である情報設定テンプレートについて説明する。ここで説明する資格証明書の例では、業務を行う業務組織（ここではプロジェクトＰ）、「ユーザ属性」、対象となるサービス・業務と権限の組合せパターン、ユーザＩＤおよび有効期限を設定できるようにした。

【００３１】

図７に資格証明書の情報設定テンプレートの例を示す。構成員（ここでは「鈴木太郎」）は、資格証明書登録申請時に、ユーザ属性を１～６（１：部長、２：担当部長、３：課長、４：担当課長、５：プロジェクトリーダ、６：補佐）の中から選択し、対象業務と権限範囲の組合せパターンＡ～Ｅ（各パターンでは、図７に示すように、対象業務とその業務での権限の有無を示す○×が割り当てられている。）の中から選択する。さらに、構成員のユーザＩＤ（持株会社で提供された個人番号）および想定される資格証明書の有効期限を入力する。例えば、ユーザＩＤが「００９８７」で、担当課長、業務と権限の組合せパターンが「Ｃ」で、暫定有効期限を「２００８年４月」とすれば、「４，Ｃ，００９８７，２００８０４」といった入力を行えばよい。勿論、入力様式は、実装するユーザインターフェース次第で変わりうる。「ユーザ属性」は必要な種類を準備すればよく、業務と権限との組み合わせパターンは教育機関や企業などの組織体のニーズに合わせて設定すればよい。

【００３２】

資格証明書をＩＣカードに記録するまでの処理を説明する。

（１）構成員「鈴木太郎」はプロジェクトＰの業務に必要なサービス・業務のアプリケーションリソースにアクセスできるようにするため、まず、例えば自分の端末装置に接続されたリーダライタにＩＣカードを読み取らせて、ＩＣカードに記録された「利用者証明書」を使った資格証明書の登録申請を行う。
（２）登録申請を受け付けたＢ会社の登録局サーバ装置は、プロジェクトＰの管理者装置へ審査処理を依頼する情報を送り、管理者装置は「利用者証明書」で本人確認などの審査を行った上で、プロジェクトＰ認証局から発行された企画証明書付きの資格証明書を発行する。
（３）登録局サーバ装置は資格証明書（企画証明書を含む。）を管理者装置から受けるとＢ会社の認証局へ認証要求情報を送り、Ｂ会社の認証局は、企画証明書に対するＢ会社証明書を発行する。
（４）構成員「鈴木太郎」は登録局サーバ装置からの発行通知メールを受けると、該当するＵＲＬへアクセスして、再度「利用者証明書」で本人確認を行った上、リーダライタを用いて申請した資格証明書を自分のＩＣカードへ記録する。

【００３３】
ここで説明した資格証明書をＩＣカードに記録する処理は、プロジェクトＰに配属された構成員「鈴木太郎」の例で示したが、他のプロジェクトや業務組織に所属している場合や兼務している場合などでも同様である。複数の組織やプロジェクトに所属する場合、該当の管理者装置から資格証明書の発行を受けることで、必要な複数の資格証明書をＩＣカードに記録する。

【００３４】
本人を確認する本人認証は或る人事組織（ここでは持株会社）の発行した利用者証明書で行うことにより、人的なリソースの流動性を担保した上で、具体的なサービス・業務のアプリケーションリソースのアクセス認可は業務組織が発行した資格証明書によって認可判定する。従って、本人認証に必要な利用者証明書は一つだけＩＣカードに記録され、一方、資格証明書は所属している業務組織の数だけＩＣカードに記録されることになる。

【００３５】
次に、本発明による認証・認可システムにおける本人認証およびサービス・業務のアプリケーションリソースに対する認可の処理を説明する。
図８は、本発明の認証・認可システム１００の実施形態を示している。認証・認可システム１００はクライアント装置１１０、認証サーバ装置１２０、アプリケーションサーバ装置１３０から構成される。これらは相互に通信可能に接続されている。また、クライアント装置１１０にはリーダライタ１４０が接続しており、リーダライタ１４０を介してＩＣカード１５０に記録された情報がクライアント装置１１０に提供される。クライアント装置１１０、認証サーバ装置１２０およびアプリケーションサーバ装置１３０はコンピュータで実現され、各装置が発揮する機能構成部は各装置にインストールされたプログラムをＣＰＵが解釈・実行することで実現される。

【００３６】
図９－１、図９－２は、特定の業務組織に配属された構成員が特定のアプリケーションリソースにアクセスしようとする際の認証・認可の処理の一例を示している。なお、アプリケーションサーバ装置のユーザデータベースに、該当する業務組織のアクセス許可が登録されていることを前提条件としている。

【００３７】
ここでは、本人認証をシングルサインオン認証で説明する。
まず、構成員（ユーザ）の入力操作によってクライアント装置１１０から認証サーバ装置１２０のポータルへのアクセス要求があると（ステップＳ１）、認証情報を要求する情報（認証情報要求）がクライアント装置１１０へ送信される（ステップＳ２）。

【００３８】
クライアント装置１１０が認証情報要求を受信すると、その受付部１１２が、クライアント装置１１０に接続されているリーダライタ１４０を制御してＩＣカード１５０から識

別名と利用者証明書を読み込む（ステップＳ３）。そして、クライアント装置１１０の制御部１１１が識別名（ＤＮ）を暗号化してから、クライアント装置１１０の送信部１１３は、暗号化された識別名と利用者証明書を認証サーバ装置１２０へ送信する（ステップＳ４）。

【００３９】

認証サーバ装置１２０の受信部１２４が、クライアント装置１１０から暗号化された識別名と利用者証明書を受信すると（ステップＳ５）、認証サーバ装置１２０の認証部１２１が、識別名を復号した後、利用者証明書とその信頼のパスから構成員（ここでは「鈴木太郎」）が持株会社によって保証されたグループ構成員であることを確認し、ユーザデータベース（図示しない。）に格納した識別名とマッチングさせて本人認証を行う（ステップＳ６）。

【００４０】

認証に成功すると、認証サーバ装置１２０の送信部１２３は、クライアント装置１１０に対して認証完了情報を通知すると共にアプリケーションサーバ装置の一覧が示されるポータルへのアクセス許可（ポータルのＵＲＬを含む。）を通知する（ステップＳ７）。このとき、この後に続く認可処理のために、資格証明書の入力を促す。

【００４１】

ここから、必要なアプリケーションリソースにアクセスするための認可判定の処理に移行する。

【００４２】

構成員は、クライアント装置１１０の入力手段（図示しない。）を操作して、その出力手段たるディスプレイ（図示しない。）に表示されたポータル画面に表示されているアプリケーションサーバ装置の一覧の中からアクセスしたいアプリケーションサーバ装置を選択する。このポータル画面には、ＩＣカード１５０から読み込まれた資格証明書の一覧も表示されている。そこで、構成員は、クライアント装置１１０の入力手段を操作して、選択したアプリケーションサーバ装置へのアクセス権限に相応しい資格証明書を「ユーザ属性」に基づいて選択する（ステップＳ８）。選択された資格証明書は受付部１１２によってＩＣカード１５０からリーダライタ１４０を介して読み込まれる（ステップＳ９）。クライアント装置１１０の制御部１１１が、選択された資格証明書を暗号化してから、クライアント装置１１０の送信部１１３が、暗号化された資格証明書と選択したアプリケーションサーバ装置を示す情報（ＡＰ指示情報）を認証サーバ装置１２０へ送信する（ステップＳ１０）。

【００４３】

認証サーバ装置１２０の受信部１２４がクライアント装置１１０から暗号化された資格証明書とＡＰ指示情報を受信すると（ステップＳ１１）、認証サーバ装置１２０の復号部１２２が資格証明書を復号するとともに、署名検証して改竄の無いことを確認した上でユーザＩＤを保持するとともに（ステップＳ１２）、認証サーバ装置１２０の制御部が、ＡＰ指示情報に基づき構成員が選択したアプリケーションサーバ装置１３０に対してアクセス要求を行う（ステップＳ１３）。

【００４４】

アプリケーションサーバ装置１３０の受信部１３２が認証サーバ装置１２０からアクセス要求を受けると、アプリケーションサーバ装置１３０の送信部１３１がユーザＩＤ（持株会社から付与されたＩＤ）を認証サーバ装置１２０に対して要求する（ステップＳ１４）。

【００４５】

アプリケーションサーバ装置１３０からユーザＩＤ要求を受けると、認証サーバ装置１２０の送信部１２３は、利用者証明書から得たユーザＩＤと資格証明書をアプリケーションサーバ装置１３０へ送信する（ステップＳ１５）。なお、認証サーバ装置１２０とアプリケーションサーバ装置１３０との間の通信は例えばＳＳＬ通信によって行う。

【００４６】

アプリケーションサーバ装置１３０の受信部１３２が認証サーバ装置１２０からユーザＩＤと資格証明書を受けると（ステップＳ１６）、アプリケーションサーバ装置１３０の認可判定部１３３は、（１）構成員のユーザＩＤと資格証明書のユーザＩＤが一致することを確認した上で、（２）第５図に示した信頼のパスをたどり資格証明書が信頼できるかどうかを検証し、（３）資格証明書の有効期限を検証し、（４）資格証明書に記載された組織とアプリケーションサーバ装置１３０のユーザデータベース（図示しない。）に登録された組織が一致するかを確認することで認可判定を行う（ステップＳ１７）。これらの判定に全て合格したならばアクセス要求が認可されたものとして、アプリケーションサーバ装置１３０の送信部１３１は、第７図に示すように資格証明書に格納された「ユーザ属性」の種類に従って要求されたアプリケーションリソースへのアクセスを許可する情報（リソースのＵＲＬを含む。）を認証サーバ装置１２０に送信する（ステップＳ１８）。

【００４７】

このアクセス許可情報を受けた認証サーバ装置１２０は、その送信部１２３によって、当該アクセス許可情報をクライアント装置１１０に転送し、クライアント装置１１０の受信部１１４が当該アクセス許可情報を取得する（ステップＳ１９）ことでクライアント装置１１０からアプリケーションリソースへのアクセスが可能となる。

【００４８】

構成員のユーザ属性が複数の業務組織に跨っている場合であっても、必要な資格証明書を選択することで認可判定が行われる。

【００４９】

本発明に拠れば、認証サーバ装置のアクセスリストやアプリケーションサーバ装置のユーザデータベースにユーザＩＤを個別に追加・更新する方式に比べ、現行の認証サーバ装置の軽微なシステム変更とアプリケーションサーバ装置のユーザデータベースにアクセス許可する業務組織を設定するだけで実現が可能であり、設定等運用の負担も大きく軽減できる。

【００５０】

なお、上述の実施形態ではＩＣカードを用いるものとしたが、ＵＳＢトークン（登録商標）、ＣＰＵ搭載のセキュアなメモリーカードなどＩＣカード以外の耐タンパーデバイスでも同様な機能を有しているため、本発明を実施できる。

【００５１】

これまでの説明では、本発明が適用される組織体として、グループ企業での持株会社を上位組織とし、傘下のグループ会社の下位組織（部、課、プロジェクトなど）で実務業務を行うところを業務組織とする組織体とした。本発明は、このような会社組織に限定されず、例えば一行政部門を上位組織とし、当該行政部門が所管の独立行政法人やその部局を業務組織としても同様である。また、地方公共団体での都道府県を上位組織とし、市町村の組織を業務組織としても扱うことができる。このように、社会の様々な階層の組織でも適用可能であることはもちろんである。

【図面の簡単な説明】

【００５２】

【図１】従来の、ユーザＩＤとパスワードによるシングルサインオン認証の処理フロー。

【図２】従来の、ＩＣカード（利用者証明書）を使ったシングルサインオン認証の処理フロー。

【図３】従来の、アクセス権限を有するユーザに対する認可処理の処理フロー。

【図４】本発明の適用に好適な一例として、持株会社を頂点とし、Ａ会社からＺ会社までを傘下企業とする企業形態における認証局（ＣＡ局）の階層構造を示す図。

【図５】利用者証明書の信頼パスを例示する図。

【図６】資格証明書の信頼パスを例示する図。

【図７】資格証明書の情報設定テンプレートを例示する図。

【図８】本発明の認証・認可システムの実施形態の一例。

【図９－１】本発明の認証・認可方法の実施形態の処理フロー（主に認証処理を示す。）

。
【図９－２】本発明の認証・認可方法の実施形態の処理フロー（主に認可処理を示す。）
。
【符号の説明】
【００５３】
１００　　認証・認可システム
１１０　　クライアント装置
１２０　　認証サーバ装置
１３０　　アプリケーションサーバ装置
１５０　　ＩＣカード

【図１】

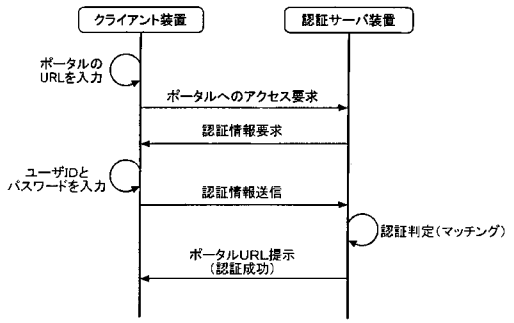

図1

【図２】

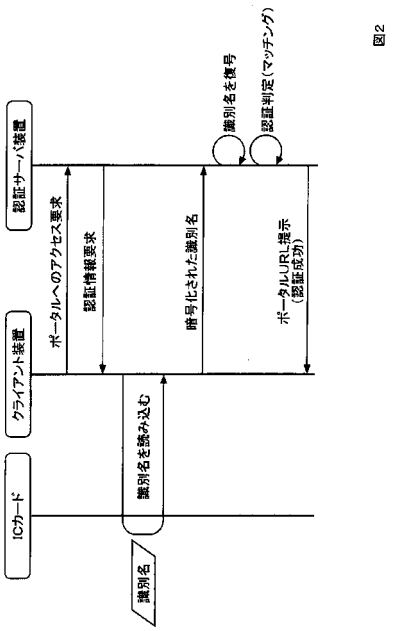

図2

【図３】

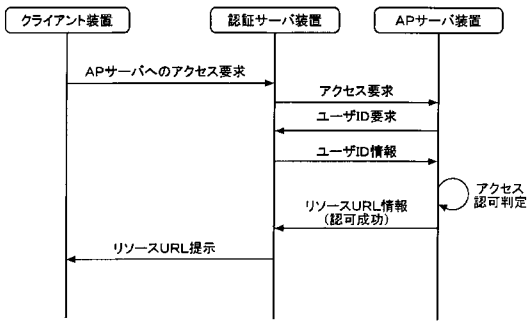

図3

【図４】

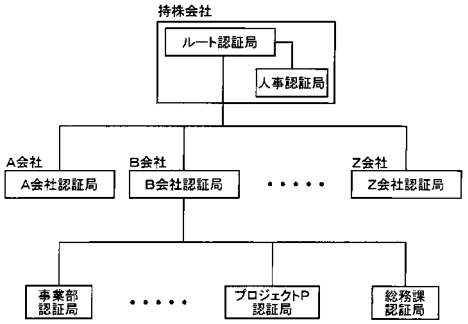

図4

【図５】

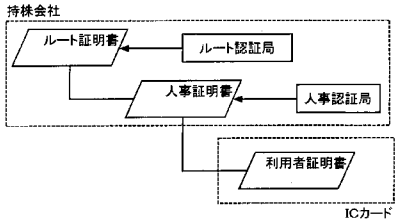

図5

【図６】

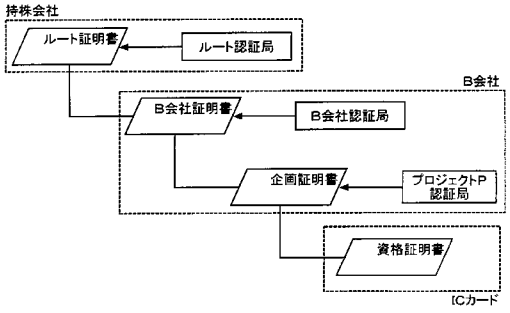

図6

【図７】

組織 役割	対象業務	権限範囲	パターン A	B	C	D	E	ユーザID	有効期限
組織 1. 部長 2. 担当部長 3. 課長 4. 担当課長 5. プロジェクトリーダ 6. 補佐	人事処理	申請・登録	○	○	○	○	○		
		決裁	×	×	×	×	○		
	社内稟議	申請・登録	×	○	○	○	○		
		決裁	×	×	×	○	○		
	リソース管理	申請・登録	×	×	○	○	○		
		決裁	×	×	○	○	○		
	データベースアクセス	閲覧	○	○	○	○	○		
		書換え	×	○	○	○	○		

図7

【図８】

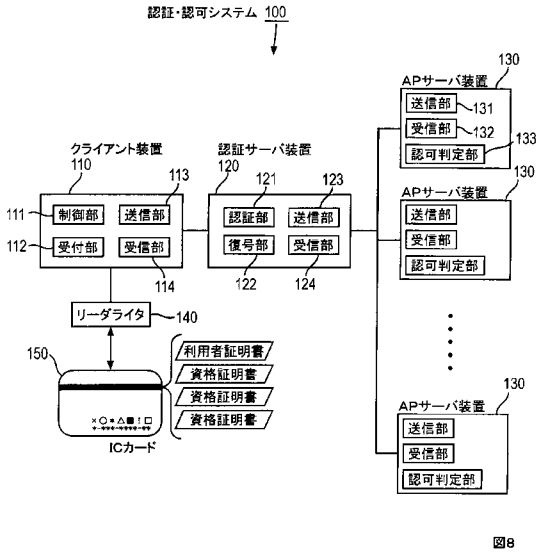

図8

【図９－１】

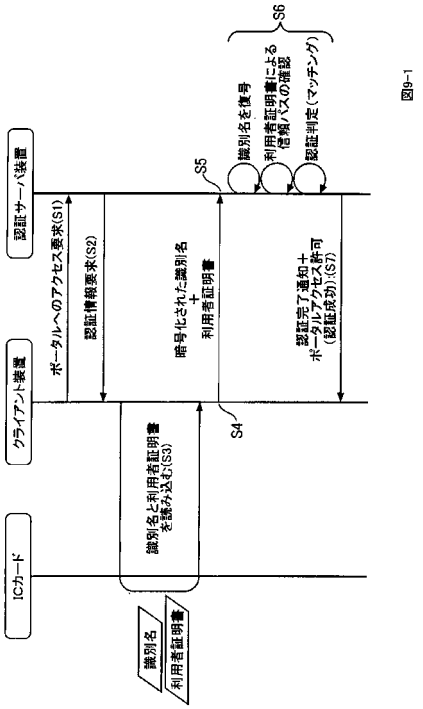

図9-1

【図９－２】

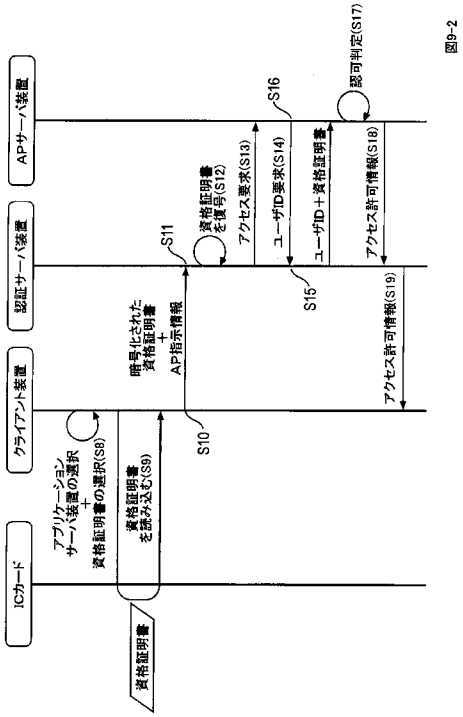

図9-2

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　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
(72)発明者　高橋　健司
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２００３－３４５７５２（ＪＰ，Ａ）
特開２００５－０５０３０８（ＪＰ，Ａ）
特開２００５－２３５１５９（ＪＰ，Ａ）
特開２００１－２１１１６９（ＪＰ，Ａ）

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