(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3622789号
(P3622789)
(45)発行日　平成17年2月23日(2005.2.23)　(24)登録日　平成16年12月3日(2004.12.3)

(51)Int.Cl.[7]	F I		
G06F 15/00	G06F	15/00	330B
G06F 17/60	G06F	17/60	140
H04L 9/32	H04L	9/00	675Z

請求項の数 8　(全 18 頁)

(21)出願番号　特願2004-512005(P2004-512005)
(86)(22)出願日　平成14年6月11日(2002.6.11)
(86)国際出願番号　PCT/JP2002/005813
(87)国際公開番号　WO2003/105002
(87)国際公開日　平成15年12月18日(2003.12.18)
審査請求日　平成15年5月20日(2003.5.20)

早期審査対象出願

(73)特許権者　399009239
株式会社帝国データバンク
東京都港区南青山二丁目５番２０号
(74)代理人　100112601
弁理士　金原　正道
(72)発明者　渡辺　秀明
東京都港区南青山２－５－２０　株式会社帝国データバンク内
(72)発明者　浅海　輝一
東京都港区南青山２－５－２０　株式会社帝国データバンク内
(72)発明者　和田　宗樹
東京都港区南青山２－５－２０　株式会社帝国データバンク内

最終頁に続く

(54)【発明の名称】汎用的組織内個人認証システム

(57)【特許請求の範囲】
【請求項１】
入力手段、制御手段、表示手段、出力手段、記憶手段等を備えるコンピュータ等の端末において操作により情報処理が行われるシステムであって、
ユーザー端末からアクセスされるＷＥＢサーバーなどのオンラインデータ処理システムと、
ネットワークを介して前記のオンラインデータ処理システムと接続される認証機関システムとから構成され、
前記のオンラインデータ処理システムは、ユーザー端末から送信される、汎用的な企業コード等の組織識別データ、または個人を識別するシリアルナンバーが組み込まれた電子証明書を受信する電子証明書受信手段と、認証機関システムとの間でデータ送受信を行い、ユーザーの認証処理を行う認証手段とを少なくとも含み、
前記の認証機関システムには、認証データベースが備えられ、前記認証データベースが記憶するデータには、企業コード等の組織識別データと、組織内の個人を認証するために個人を識別するシリアルナンバーと、組織内の個人の権限情報を少なくとも含む個人認証データとが関連付けられており、
前記認証データベースから抽出された、組織内の個人の権限情報を少なくとも含む個人認証データに基づき、前記の認証手段がオンラインデータ処理システムにおいて、組織内の個人の権限情報の認証を少なくとも含むユーザー認証を行うことを特徴とする、汎用的組織内個人認証システム。

【請求項２】
前記の認証機関システムは、複数のオンラインデータ処理システムからアクセス可能に備えられ、異なる複数のＷＥＢサーバーなどのオンラインデータ処理システムにアクセスするユーザー認証を同一の電子証明書を用いて行うことが可能なことを特徴とする、請求項１に記載の汎用的組織内個人認証システム。
【請求項３】
前記認証データベースにはさらに、企業コード等の組織識別データで識別される企業ごとの企業基本情報を含むデータが記憶されたことを特徴とする、請求項１または２のいずれかに記載の汎用的組織内個人認証システム。
【請求項４】
前記の認証機関システムには、企業等の組織の所定の権限を有する者が、組織に所属する電子証明書を保有する個人ごとに、組織内の個人の権限を設定する組織権限設定手段が備えられ、
認証データベースから抽出された、組織内の個人の権限情報を少なくとも含む個人認証データに基づき、前記の認証手段がオンラインデータ処理システムにおいて、組織内の個人の権限情報の認証を少なくとも含むユーザー認証を行うことを特徴とする、請求項１～３のいずれかに記載の汎用的組織内個人認証システム。
【請求項５】
前記の認証機関システムには、前記のオンラインデータ処理システムの所定の権限を有する者が、どの電子証明書保有者であれば当該オンラインデータ処理システムにアクセスして利用可能とするかを設定する利用権限設定手段が備えられ、
認証データベースから抽出された、組織内の個人の権限情報を少なくとも含む個人認証データに基づき、前記の認証手段がオンラインデータ処理システムにおいて、組織内の個人の権限情報の認証を少なくとも含むユーザー認証を行い、当該オンラインデータ処理システムにアクセスして利用可能か否かを判定することを特徴とする、請求項１～４のいずれかに記載の汎用的組織内個人認証システム。
【請求項６】
前記の認証手段がオンラインデータ処理システムにおいて行われる、組織内の個人の権限情報の認証を少なくとも含むユーザー認証は、システムやサービスの利用等の利用可否についてのユーザー認証、取引や商談・契約等に対する権限の有無についてのユーザー認証、入札参加や各種申請・審査等に対する資格の有無についてのユーザー認証のいずれかであることを特徴とする、請求項１～５のいずれかに記載の汎用的組織内個人認証システム。
【請求項７】
汎用的な企業コード等の組織識別データと、個人を識別するシリアルナンバーとが組み込まれた電子証明書を所有するユーザーがユーザー端末からアクセスして、前記の利用権限設定手段に対しオンラインデータ処理システムにおける利用権限の設定申請を行う利用権限申請手段が、前記の認証機関システムに備えられたことを特徴とする、請求項１～６のいずれかに記載の汎用的組織内個人認証システム。
【請求項８】
前記の認証機関システムに備えられる認証データベースは、組織識別データをキーとして関連付けられた企業情報などの組織情報を記憶・蓄積・更新する組織情報データベースと連携して備えられ、企業等の組織情報の更新・変動を反映して、認証データベースから抽出された、組織内の個人の権限情報を少なくとも含む個人認証データに基づき、前記の認証手段がオンラインデータ処理システムにおいて、組織内の個人の権限情報の認証を少なくとも含むユーザー認証を行うことを特徴とする、請求項１～７のいずれかに記載の汎用的組織内個人認証システム。
【発明の詳細な説明】
【技術分野】
【０００１】

本発明は、企業などの組織に所属する個人を認証するための、汎用的に利用可能な組織内個人認証システムに関する。

【背景技術】

【０００２】

近年、コンピュータ・ネットワークや通信環境の発達に伴い、インターネットに代表される商業活動などのビジネスが活発になってきている。ショッピング・モールやオークションなどの消費者対企業の取引のためのＷｅｂサイトのほか、資材調達などの企業間取引のためのサイトなども多数存在し、それらに伴う決済方法などの技術も様々なものが開発されている。

また、電子調達をはじめとする電子商取引にあっては、商品等を売り込み販売をしたい販売者が取引情報をネットワークを通じて送信するなど、売り込みや入札参加などをする場合に、商品等の調達者との間で互いに顔を見ることなく、調達する側にとっては販売者が本当に実在するのかどうか、あるいは信用があるかどうかなどの点において不安がある。このため、本当に信用がある取引先であっても、上記のような問題のために商取引の機会を失ってしまうことが起きる。

【発明の開示】

【発明が解決しようとする課題】

【０００３】

与信情報・信用情報・取引履歴情報・人物情報・地域や価格あるいは支払条件その他の取引条件情報・その他の情報を見極める必要が生ずる。

また、上記では電子商取引の例をあげたが、企業などに関する情報を判断する場面は、これ以外にも多々生ずる。

たとえば、企業等が参加する国や地方自治体などによる物品購入や工事などの入札に際しての判断や、企業等との提携、契約に際しての判断、企業合併や合弁事業の立上げ時等における判断、その他の場面でも、これらの情報を正確に客観的な観点から見極める必要が生ずる。

たとえば、建設業においては、経営事項審査による客観的な工事施工能力評価にて、入札制限やスクリーニングが可能だが、他業種においては、経営事項審査に代わる仕組みはない。物品調達や申請をオープンな環境で電子化を推進していくためには、入札・申請企業の状態を把握し、判断していくための企業情報を入手できるシステムとの連携が必要となる。

【０００４】

ところで今日、インターネット等のコンピューター技術を用いた取引や入札等において、認証をするための電子署名、電子証明書が様々に開発されている。

電子署名法では、法人を認証して電子証明書を発行できるのは法務省の商業登記認証局で、民間の特定認証局は純然たる個人（自然人）の認証を行うと規定されている。

しかしながら、電子証明書は、自然人である個人に対して発行されるものである。したがって、個人の認証が行われ実在する個人であることが証明できた場合にも、下記のような重大な問題が残っている。

すなわち、たとえば地方自治体の入札や申請といった手続き業務や、民間の資材調達などで、担当者レベルの証明書が必要となるケースが大半である。その際、自然人に対して発行した電子証明書では証明書所有者がどの企業に属するのかが判別できない。また、商業登記認証局は企業の代表者印鑑証明のような位置づけで、企業に対し一つの証明書しか発行されず、個人事業者への証明書発行も行われない。これらの理由により、入札・申請受付後の業務や資材調達の業務が円滑に進まないこととなる。

その個人が本当に企業等の組織に所属しているのか否か、あるいは所属をしていたとしても取引や入札等において参加・判断・決定の権限があるか否かなどは、従来の電子証明書だけでは判断ができないからである。また企業等を退職したり、部署や役職が変動することがあり、これらの更新・変動に対応しなければならない。さらに、企業そのものが合併や、倒産、信用情報の変動、その他の変動を受けることも多い。

【０００５】
そこで、上記の様々な課題を解決し、本発明においては、インターネット等の電子空間での取引や入札、契約などにおいて、個人を認証する際に、その個人が本当に企業等の組織に所属しているのか否か、あるいは所属をしていたとしても取引や入札等において参加・判断・決定の権限があるか否かなどを認証することの可能なシステムを提供することを目的とする。
そのため、電子証明書に汎用企業コードまたはシリアルナンバー等を組み込み、認証データベースに、企業コード、シリアルナンバー、企業内個人情報、企業基本情報、権限情報等を入れることにより、企業と個人の情報とを関連付けて認証することが可能となり、また個人事業者の認証を可能にする。
さらに本発明においては、運営者が違う複数の認証サイトなど、複数の認証システムにおいても、１枚の証明書でユーザーが対応可能なシステムを提供することを目的とする。
【０００６】
従来の電子証明書であれば、認証システムごとの証明書が必要となる。たとえば電子入札を行う自治体ごとの複数の証明書であり、サービスサイトごとの複数の証明書である。結果として、ユーザーはそれぞれについての専用の証明書を有さねばならず、煩雑かつ不便であり、トラブルも予想され、また運営者にとっても、コストをかけて自前の証明書の発行をしなければならなかった。
ここで、電子証明書に汎用的企業コードが組み込まれ、認証データベースの活用がオープンとなれば、自治体や企業などの運営者などの認証サイド、入札者などのユーザーの被認証サイド共に、１つの汎用電子証明書で認証作業が済まされることを可能にする。
さらに本発明においては、電子証明書を用いた認証のための認証データベースと、企業等の組織情報データベースとを連携させることにより、認証に際して随時最新の更新されたデータに基づき認証等の処理が可能なシステムを提供することをも目的とする。企業等からの退職、部署や役職が変動、さらに企業そのものが合併や、倒産、信用情報の変動、その他の変動に対応することにより、適格な認証処理を行うことができる。
しかも、データは認証機関が収集・蓄積・更新を行うようにすることで、それぞれの認証を行うＷＥＢサイトなどが個々にデータベースを構築することなく、本発明の認証システムを利用することが可能になる。
【課題を解決するための手段】
【０００７】
上記課題を解決するため、請求項１に記載の発明においては、
入力手段、制御手段、表示手段、出力手段、記憶手段等を備えるコンピュータ等の端末において操作により情報処理が行われるシステムであって、
ユーザー端末からアクセスされるＷＥＢサーバーなどのオンラインデータ処理システムと、
ネットワークを介して前記のオンラインデータ処理システムと接続される認証機関システムとから構成され、
前記のオンラインデータ処理システムは、ユーザー端末から送信される、汎用的な企業コード等の組織識別データ、または個人を識別するシリアルナンバーとが組み込まれた電子証明書を受信する電子証明書受信手段と、認証機関システムとの間でデータ送受信を行い、ユーザーの認証処理を行う認証手段とを少なくとも含み、
前記の認証機関システムには、認証データベースが備えられ、前記認証データベースが記憶するデータには、企業コード等の組織識別データと、組織内の個人を認証するために個人を識別するシリアルナンバーと、組織内の個人の権限情報を少なくとも含む個人認証データとが関連付けられており、
前記認証データベースから抽出された、組織内の個人の権限情報を少なくとも含む個人認証データに基づき、前記の認証手段がオンラインデータ処理システムにおいて、組織内の個人の権限情報の認証を少なくとも含むユーザー認証を行う、汎用的組織内個人認証システムであることを特徴としている。

【０００８】
また、上記課題を解決するため、請求項２に記載の発明においては、
前記の認証機関システムは、複数のオンラインデータ処理システムからアクセス可能に備えられ、異なる複数のＷＥＢサーバーなどのオンラインデータ処理システムにアクセスするユーザー認証を同一の電子証明書を用いて行うことが可能な、請求項１に記載の汎用的組織内個人認証システムであることを特徴としている。
【０００９】
また、上記課題を解決するため、請求項３に記載の発明においては、
前記認証データベースにはさらに、企業コード等の組織識別データで識別される企業ごとの企業基本情報を含むデータが記憶された、請求項１または２のいずれかに記載の汎用的組織内個人認証システムであることを特徴としている。
【００１０】
また、上記課題を解決するため、請求項４に記載の発明においては、
前記の認証機関システムには、企業等の組織の所定の権限を有する者が、組織に所属する電子証明書を保有する個人ごとに、組織内の個人の権限を設定する組織権限設定手段が備えられ、
認証データベースから抽出された、組織内の個人の権限情報を少なくとも含む個人認証データに基づき、前記の認証手段がオンラインデータ処理システムにおいて、組織内の個人の権限情報の認証を少なくとも含むユーザー認証を行う、請求項１～３のいずれかに記載の汎用的組織内個人認証システムであることを特徴としている。
【００１１】
また、上記課題を解決するため、請求項５に記載の発明においては、
前記の認証機関システムには、前記のオンラインデータ処理システムの所定の権限を有する者が、どの電子証明書保有者であれば当該オンラインデータ処理システムにアクセスして利用可能とするかを設定する利用権限設定手段が備えられ、
認証データベースから抽出された、組織内の個人の権限情報を少なくとも含む個人認証データに基づき、前記の認証手段がオンラインデータ処理システムにおいて、組織内の個人の権限情報の認証を少なくとも含むユーザー認証を行い、当該オンラインデータ処理システムにアクセスして利用可能か否かを判定する、請求項１～４のいずれかに記載の汎用的組織内個人認証システムであることを特徴としている。
【００１２】
また、上記課題を解決するため、請求項６に記載の発明においては、
前記の認証手段がオンラインデータ処理システムにおいて行われる、組織内の個人の権限情報の認証を少なくとも含むユーザー認証は、システムやサービスの利用等の利用可否についてのユーザー認証、取引や商談・契約等に対する権限の有無についてのユーザー認証、入札参加や各種申請・審査等に対する資格の有無についてのユーザー認証のいずれかである、請求項１～５のいずれかに記載の汎用的組織内個人認証システムであることを特徴としている。
【００１３】
また、上記課題を解決するため、請求項７に記載の発明においては、
汎用的な企業コード等の組織識別データと、個人を識別するシリアルナンバーとが組み込まれた電子証明書を所有するユーザーがユーザー端末からアクセスして、前記の利用権限設定手段に対しオンラインデータ処理システムにおける利用権限の設定申請を行う利用権限申請手段が、前記の認証機関システムに備えられた、請求項１～６のいずれかに記載の汎用的組織内個人認証システムであることを特徴としている。
【００１４】
また、上記課題を解決するため、請求項８に記載の発明においては、
前記の認証機関システムに備えられる認証データベースは、組織識別データをキーとして関連付けられた企業情報などの組織情報を記憶・蓄積・更新する組織情報データベースと連携して備えられ、企業等の組織情報の更新・変動を反映して、認証データベースから抽

出された、組織内の個人の権限情報を少なくとも含む個人認証データに基づき、前記の認証手段がオンラインデータ処理システムにおいて、組織内の個人の権限情報の認証を少なくとも含むユーザー認証を行う、請求項１～７のいずれかに記載の汎用的組織内個人認証システムであることを特徴としている。

【００２２】

【発明の効果】

【００２３】

【発明を実施するための最良の形態】

【００２４】

以下、本発明の実施の形態について図面を参照して説明する。

本発明の個人認証システムは、入力手段、制御手段、表示手段、出力手段、記憶手段等を備えるコンピュータ等の端末において操作により情報処理が行われるシステムである。

図１は、本発明のシステムの基本的な構成の一例を示すシステム構成図である。

ユーザー端末からアクセスされるＷＥＢサーバーなどのオンラインデータ処理システムと、ネットワークを介して前記のオンラインデータ処理システムと接続される認証機関システムとから構成される。

認証機関システムは、電子証明書を用いて、本発明において特徴的な、企業等の組織識別データと個人認証データとを結びつけた認証処理を行い、認証の結果をＷＥＢサイトの運営などを行うオンラインデータ処理システムに返す機能を備える。また企業等の組織識別データと、組織等に所属する個人情報とを結びつけ、データの保守・管理などを行う。

【００２５】

オンラインデータ処理システムは、ＷＥＢサイトにおいてユーザー端末からのアクセスを受け付け、電子商取引や、商談、入札、契約、その他のデータ処理を行う。データ処理の際のユーザーの個人認証のために、前記の認証機関システムと連携してデータ処理を行うように備えられ、認証機関システムとの間で個人認証のためのデータの送受信を行う。

オンラインデータ処理システムに接続するためのユーザー端末としては、通常、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端末が用いられる。この他、利用者端末には、インターネット等に接続可能なブラウザ機能を搭載した携帯電話をはじめとする無線通信端末、携帯情報端末や、インターネットＴＶ、ゲーム機器、テレビ会議システム、その他のネットワーク接続機能を備えた家電製品などの機器を広く含む。

コンピュータ端末は、制御手段、記憶手段、入力手段、出力手段、表示手段などを備える。またインターネットに代表されるコンピュータネットワークに接続詞、データの送受信を行う機能を備え、ブラウザや電子メールソフトウェア、ワードプロセッサなどのアプリケーションプログラムや、オペレーティングシステム（ＯＳ）を備えることが通常の形態である。

【００２６】

オンラインデータ処理システムは、通常はサーバーシステムから構成されて、インターネットに代表される通信手段に接続されて備えられ、通信手段に接続するユーザー端末からアクセスされる。

ここで通信手段には、インターネットをはじめとして、専用線により接続されたネットワーク形態や、企業内ＬＡＮ、企業間ＬＡＮ、ＷＡＮなどの形態を広く含む。またここで用いられる通信回線の形態には、有線通信、無線通信の形態を広く含み、衛星通信や、Ｂｌｕｅｔｏｏｔｈなどを用いた形態を含む。

次に、オンラインデータ処理しステムの構成の一例としては、アプリケーションサーバー、データベースサーバー、認証サーバー、ＷＥＢサーバー、その他必要に応じメールサーバー、その他の各種装置により構成することができるが、このような形態に限定されるものではない。

また、これらの各サーバーは、物理的に同一の装置に設けられる形態や、物理的に複数の装置からなる形態、あるいはネットワークを介して接続される物理的に複数の装置からなる形態などを含み、機能的に同様の機能が実現されるならば、様々な形態を含む。

【００２７】
オンラインデータ処理システムは、インターネットを介してＷＥＢサイト等においてユーザーからのアクセスを受け付ける場合には、ユーザー端末からアクセスするためのコンテンツデータ及びプログラムを記憶するＷＥＢサーバーを備えている。
コンテンツデータには、ＨＴＭＬファイル、ＸＭＬファイルなどのＷＥＢ上に表示されるデータファイルや、Ｃ－ＨＴＭＬファイルなどのＷＥＢサイトにアクセス可能な携帯電話等に表示されるデータファイルなどが含まれる。
また、これらのファイルに挿入されるなどして表示又は出力される、文字データファイル、音声データファイル、画像データファイル、動画像データファイル、アニメーションデータファイル，その他の様々なコンテンツデータを記憶することができる。
【００２８】
オンラインデータ処理システムのより具体的な一例を列挙すれば、たとえば次のようなシステムである。
企業等の組織に属するユーザーからアクセスされて、企業間取引その他の電子商取引の受発注・契約などを行うシステムである。このような場合において、アクセスしたユーザーが該当する企業等の組織に所属する個人であるか否か、あるいは所属する個人であって取引・契約等の権限を有する個人であるか否かの認証が必要な場合に、認証機関システムとの連携によって個人認証を行う。
あるいは、企業等の組織に属するユーザーからアクセスされて、物品の納入やサービスの提供、工事の受注や見積参加などの入札を行うシステムである。たとえば国や地方自治体などの入札参加を受け付けるような場合が一例である。このような場合においても、アクセスしたユーザーが該当する企業等の組織に所属する個人であるか否か、あるいは所属する個人であって入札参加・見積提出等の権限を有する個人であるか否かの認証が必要な場合に、認証機関システムとの連携によって個人認証を行う。
あるいは、組織は企業には限定されない。たとえば一例をあげれば、弁護士・税理士などの有資格者がユーザーである場合において、これら有資格者の所属する管理団体（弁護士会・税理士会）等が組織である場合などが想定される。電子データを用いた各種申請書類、申告書類の提出などのような場合において、アクセスしたユーザーが該当する資格者の組織に所属する個人であるか否か、権限を有する個人であるか否かの認証が必要な場合に、認証機関システムとの連携によって個人認証を行う。
これらはいずれも、オンラインデータ処理システムの一例であって、これ以外の様々な形態において本発明の個人認証システムを利用することが可能である。
また、オンラインデータ処理システムは、ＷＥＢサーバーにより構成されるＷＥＢサイトには限定されない。ＦＴＰその他の方法によるアクセスや、電子メール、ピアツーピア方式のアクセス、その他の方法において利用することもできる。
【００２９】
前記のオンラインデータ処理システムは、ユーザー端末から送信される、汎用的な企業コード等の組織識別データ、または個人を識別するシリアルナンバーが組み込まれた電子証明書を受信する電子証明書受信手段を備えている。
電子証明書受信手段は、ユーザー端末からのアクセスにおいて、電子商取引の申込み、契約の申込み、入札参加の申込み、その他の個人認証が必要な際に、必要なデータと共にユーザー端末から送信された電子証明書を受信するものである。受信された電子証明書はオンラインデータ処理システムにおいて記憶手段に、関連するデータと共に記憶される。電子証明書は、認証機関システムに対し組織内個人認証のための照会をするために用いられる。
前記のオンラインデータ処理システムは、認証機関システムとの間でデータ送受信を行い、ユーザーの認証処理を行う認証手段を備えている。
ユーザー端末からオンラインデータ処理システムに対する電子証明書の送信は、
電子証明書を保有したユーザー端末が、前記のような電子商取引や入札サイト等のオンラインデータ処理システム宛に商取引や入札などの必要な所定の情報（何を送信して呈示す

る。所定の情報には電子証明書が添付され、あるいは電子証明書により、暗号化された上で送信される。
受信したＷＥＢサイト等のオンラインデータ処理システムにおいては、認証手段が、ユーザー端末から送信された電子証明書に中に含まれる企業コード等の組織識別情報、あるいは個人ごとのシリアルナンバー等の個人識別情報を抽出し、受信した必要な所定事項のデータと共に記憶する。認証処理に必要な組織識別情報あるいは個人識別情報を、後述する認証機関システムに送信し、認証データベースに照会することにより、認証処理を行う。
送信される取引条件情報１件１件については、企業コードが付加された電子証明書による暗号化通信によりセキュアに守られている。
【００３０】
ここで、企業コードが付加された電子証明書による認証は、取引や入札、その他の各オンラインデータ処理システムにアクセスしてデータをを送信する企業等の組織に所属する個人が汎用的な企業コード等の組織識別データ、または個人を識別するシリアルナンバーが組み込まれた電子証明書の交付を受けて行うものである。
図２は、認証機関システムが、複数のオンラインデータ処理システムからアクセス可能に備えられた形態の一例を示すシステム構成図である。異なる複数のＷＥＢサーバーなどのオンラインデータ処理システムにアクセスするユーザー認証を同一の電子証明書を用いて行うことが可能にされている。
本発明の個人認証システムは、汎用的な企業コードなどの組織識別データを用いて認証処理を行うので、様々なオンラインデータ処理システムにおいて汎用的に利用することができる。電子商取引サイト、入札サイトなどの各オンラインデータ処理システムは、独自に認証データベースを設ける必要がない。
【００３１】
次に、認証機関システムには、認証データベースが備えられている。
認証データベースが記憶するデータには、企業コード等の組織識別データと、組織と個人とを関連付けることにより組織内の個人を認証するための個人認証データとが少なくとも含まれている。企業コード等の組織識別データと、組織内の個人を認証するために個人を識別するシリアルナンバーと、組織内の個人の権限情報を少なくとも含む個人認証データとが関連付けられている。
組織識別データは、汎用的な企業コード等の組織識別データであって、望ましい形態の一例としては電子証明書に組み込まれ、これに対応して、組織と個人とを関連付けたデータが認証データベースに記憶される。
また、認証データベースにはさらに、企業基本情報などを記憶管理しておくことが望ましい。
認証データベースに記憶されるデータのさらに別の形態としては、電子証明書として企業コードなどの組織識別データが組み込まれていない、個人のシリアルナンバーが組み込まれた電子証明書を用いる場合の形態があげられる。
この場合には、認証データベースには、個人のシリアルナンバーと企業コード等の組織識別データとの対応テーブルを設けることにより、組織と個人とを関連付けることが必要になる。
認証データベースに記憶される権限情報は、第一には、認証される個人が該当する企業等に所属する者であるか否か、あるいは所属していても所定の権限を有しているか否かといった組織内における権限情報がある。
【００３２】
こうした権限情報を登録・管理するために、認証機関システムには、企業等の組織の所定の権限を有する者が、組織に所属する電子証明書を保有する個人の権限を設定する組織権限設定手段が備えられる。組織に所属する電子証明書を保有する個人ごとに、組織内の個人の権限を設定する。
企業等の組織の管理者・責任者等が、組織内の電子証明書保有者の職務権限を設定する機能を構築し、電子証明書保有者が認証システムにアクセスした際に、認証システムからの

要求に応じて、結びつけられた「企業」における権限情報を提供する。認証データベースから抽出された、組織内の個人の権限情報を含む認証情報に基づき、前記の認証手段がオンラインデータ処理システムにおけるユーザー認証を行うことを特徴とする。
また、権限情報の第二の形態は、電子商取引や入札などを行うＷＥＢサイト等のオンラインデータ処理システムが、企業等の組織あるいはそれらに所属する個人に対して、取引や入札等への申込みや参加等の権限を与えるか否かの権限を付与しておくものである。
【００３３】
こうした権限情報を付与する場合に、認証機関システムには、前記のオンラインデータ処理システムの所定の権限を有する者が、どの電子証明書保有者であれば当該オンラインデータ処理システムにアクセスして利用可能とするかを設定する利用権限設定手段が備えられる。
オンラインデータ処理システムの管理者・運営者が、自社のシステムにどの電子証明書保有者であれば利用可能とするかを設定する機能を構築し、電子証明書保有者が認証システムにアクセスした際に、認証システムからの要求に応じて、設定した利用権限情報を提供する。認証データベースから抽出された、組織内の個人の権限情報を少なくとも含む個人認証データに基づき、前記の認証手段がオンラインデータ処理システムにおいて、組織内の個人の権限情報の認証を少なくとも含むユーザー認証を行い、当該オンラインデータ処理システムにアクセスして利用可能か否かを判定する。
こうした権限情報の設定により、自然人である個人に対して発行されている汎用的な電子証明書を利用して、企業、官公庁、団体、学校などの組織に属している人間としての属性情報の利用、権限情報の有無による認証を行うことができる。企業対政府の電子入札、電子申請や企業間電子商取引において、電子証明書を利用する場合には、「企業人」に対して電子証明書を発行する必要があるためである。「企業人」に対して電子証明書を発行し利用されるためには、「本人」の存在証明と同時に、所属する「企業」の存在証明やその属性情報を認識する機能が実現される。
【００３４】
ここで用いられる電子証明書の一例としては、例えば下記のようなものであり、ネットワークに接続された認証機関システム等により発行される。認証機関システムは、中立的な第三者機関の認証局である形態が望ましく、本発明のシステムにおいては、後述する認証機関システム又はこれと連携するサーバなどにおいて発行処理を行うことができる。
電子証明書としては知られている様々な方式のものを採用することができるが、代表的な形態としては公開鍵暗号方式による電子署名方式があげられる。
公開鍵暗号方式とは、１組の鍵ペア（公開鍵と秘密鍵）を用いて、暗号化、復号（解読）を行う暗号方式である。秘密鍵で暗号化したものは、公開鍵でなければ復号ができないものである。公開鍵が間違いなく本人のものであるという証明を、信頼される第三者機関である認証機関システムが行う。認証機関は、公開鍵の持ち主を証明する電子的な証明書（電子証明書）を発行する。
【００３５】
本発明の個人認証システムにおいては、自然人であり電子証明書を保有する個人と、個人所属する企業等の組織との対応付けを、汎用的な企業コード等の組織識別データを用いて行うため、望ましい方式としては次の要件を満たす必要がある。
第一に、電子証明書発行先である個人の所属する企業等の組織が、一般に流通している組織情報（企業情報）データベースの中で、どの識別コードに当たるかを正確に特定できることである。
第二に、電子証明書発行先である個人の所属する企業等の組織が、一般に流通している企業情報データベースに収録していない際に、識別コードを新規設定することである。当然ながら、識別コードは業種・業態を横断したものであり、正確に管理、運用されている必要がある。
第三に、組織識別コードを利用する際に、最低限必要な情報が無料公開されていることにより、認証を利用するオンラインデータ処理システムにおいて、情報の有用な活用をする

ことができる。
【００３６】
次に、認証機関システムが行う電子証明書の発行形態の一例について説明する。
初めに、ユーザー端末から認証機関システムにアクセスし、公開鍵を認証機関システムへ届け出て、電子証明書の発行を請求する。
例えば企業Ａに所属するユーザーが会員として登録するためには、まず企業Ａのユーザーは認証機関システムに対して、会社名、氏名、ローマ字氏名、電子メールアドレス等を記載の上、入会の申込を行う。
認証機関は、本人からの請求によるものであること等を確認する。入会申込があると、認証機関システムにおいては企業Ａの審査を行うが、審査においては既存の企業情報データベースなどを用いて企業Ａの審査を行ったり、本人確認等を併用して審査することができる。
審査をパスした場合には、認証機関システムにおいて、認証データベースに対して、当該申込企業Ａの申請者ユーザーの情報等を認証機関システム内の認証データベースに登録する。
認証データベースへの登録に際しては、所属組織（企業等）からの申込みにより電子証明書を発行する際に、「本人」と所属する「企業」の結びつけを行う。
企業等の組織との結びつけには、一般に流通している企業情報データベースの識別コードを用いる。
電子証明書に一般的な企業識別コードを組み込む。
または、企業識別キーを組み込めない電子証明書については、シリアルナンバー等の電子証明書に格納された固有の情報と当該企業の企業識別コードとの対応テーブルを用いる。
登録が済むと、請求したユーザーに、電子証明書（公開鍵入り）を送付する。
以上の電子証明書、及び電子証明書の発行の処理及びそのための構成は、望ましい形態の一例を示したものであって、本発明のシステムにおいては電子証明書の他の形態のものを使用することができる。
【００３７】
以下、本発明の基本的な処理の流れについて、図３を参照して説明する。
図３は、本発明のシステムの基本的な処理の流れの一例を示すシステム概要図である。
初めに、認証処理の前提として、電子商取引や入札などを行うＷＥＢサイト等のオンラインデータ処理システムから、企業等の組織あるいはそれらに所属する個人に対して、取引や入札等への申込みや参加等の利用権限を与えるか否かの権限を付与するために認証機関システムにアクセスし、権限情報（利用権限情報）を登録する（Ｓ１００）。
権限情報（利用権限情報）は、アクセスしてきたユーザーである個人が、該当する企業等の組織に所属しているか否かの実在の判定をすることにより、実在すれば電子商取引や入札などの認証処理により利用許可がされるといったような情報である。
また、あらかじめ企業等の組織の管理者などが、組織に所属する個人の内、誰に権限を与えるかの権限情報（組織権限情報）を付与しておく場合には、権限情報（組織権限情報）が付与されているか否かの判定をすることにより、実在すれば電子商取引や入札などの認証処理により利用許可がされるといったような情報である。
【００３８】
次に、オンラインデータ処理システムにおけるユーザー認証処理について説明するが、ユーザー認証の内容はたとえば、システムやサービスの利用等の利用可否についてのユーザー認証、取引や商談・契約等に対する権限の有無についてのユーザー認証、入札参加や各種申請・審査等に対する資格の有無についてのユーザー認証、などである。
ユーザー端末からオンラインデータ処理システムにアクセスし、電子商取引の申込みや、入札参加申込みなどの、オンラインデータ処理システムがデータ入力・送信を要求する所定のデータ項目のデータを入力し、入力された電子文書を送信する。この際に電子証明書を併せて送信する（Ｓ１０１）が、電子証明書が秘密鍵方式の場合にはこれを用いて電子文書を暗号化（電子署名）する。電子証明書には企業コード等の組織識別データ、あるい

は個人を識別するシリアルナンバーが含まれている。電子文書、暗号文、公開鍵を送信する。

【００３９】

次にオンラインデータ処理システムにおいては、ユーザー端末から送信されたデータを電子証明書受信手段が受信し、添付された公開鍵を用いて暗号文を復号し、署名の検証を行う。元の電子文書と照合することで、不正な改ざんがなされていないことを確認できる。同時に、認証手段が、公開鍵に対応する秘密鍵の持ち主が電子署名したことを確認するために、認証機関システムの認証データベースに対して照会を行う（Ｓ１０２）。認証データベースから抽出された、組織内の個人の権限情報を少なくとも含む認証情報に基づき、前記の認証手段が所定の権限情報があるか否かを判定し、オンラインデータ処理システムにおけるユーザー認証を行う。

認証データベースには、あらかじめ前記のオンラインデータ処理システムの所定の権限を有する者が、どの電子証明書保有者であれば利用可能とするかの設定が記憶されている場合には、電子証明書を所有する登録済のユーザーは、認証機関システムへ照会するユーザー認証を経ることにより、個々のオンラインデータ処理システムにおけるユーザー登録が不要となる。

認証機関システムは、オンラインデータ処理システムからの照会要求に応じて、結びつけられた「企業」の属性情報を提供することが望ましい。

認証が完了すると、その結果がユーザー端末に通知されると共に（Ｓ１０３）、データ処理に必要な所定のデータの送受信などが行われる。

以上、本発明の基本的な実施形態により、企業等の組織内における個人認証が可能となる。

また、複数の認証システム（運営者が違う複数の認証サイト）でも、ユーザーは１枚の証明書で済む。また、電子証明書に汎用的企業コードが組み込まれ、認証データベースの活用がオープンとなることにより、認証サイド（自治体や企業などの運営者)、被認証サイド（入札者、ユーザー等）共に１つの汎用電子証明書で認証作業が済まされることとなる。

【００４０】

次に、図４を参照して、本発明のシステムの別の実施形態における処理の流れの一例について説明する。

電子証明書を用いた通常の認証作業では、ユーザーの登録があらかじめ行われ、かつ認証データベースに入力されていなければならない。新規の申請者は、登録をした後でなければ、証明書の利用ができず、かつ複数の自治体に入札する場合や、複数のサービスを利用する際、それぞれ登録作業を行う必要がある。

そこで、図４に示すように、電子証明書を所有するユーザーがユーザー端末からアクセスして、前記の利用権限設定手段に対しオンラインデータ処理システムにおける利用権限の設定申請を行う利用権限申請手段が、前記の認証機関システムに備えられることが望ましい。

ここで、汎用的企業コードが組み込まれた電子証明書が流通し、権限情報が入力された認証データベース（あらかじめ、利用を許可する相手の情報が登録されている）があれば、最初の登録を済ませて証明書を得たユーザーは、その後、新たに登録する必要なく、各自治体への入札やサービスサイトの利用が可能となる。ＷＥＢサイト側も、自前の電子認証システムを構築しないで済む。

【００４１】

次に、図４を再度参照して本実施形態における処理の流れの一例について説明する。

証明書ホルダー（電子証明書を所有する人）が、自身の手により、他のサイトへの登録も行うことができる汎用申請システムである。

オンラインデータ処理システムにおける利用権限の設定申請が承認され、利用権限設定手段に記憶された場合には、該当する電子証明書を所有する個人が所属する組織に属する所定の条件を満たす個人に対するユーザー認証が認められる。

例えば、ある自治体（Ａ）で入札参加資格を得て、電子証明書で電子入札している証明書ホルダー企業（甲）が、他の自治体（Ｂ）でも入札資格を得ようとする場合に、サイト運営者が権限情報を渡すアクションをしなくても、ユーザーである証明書ホルダー自体が最初にアクションを起こすケースである。
自治体Ａの入札参加資格を得て、認証機関システムにアクセスし（Ｓ２００）、証明書の発行を受けた企業甲は、自治体Ｂに申請する際に
利用申請サイトへ登録申請する（Ｓ２０１）。
その利用申請サイトから自治体Ｂの入札サイトへと企業甲の情報が伝えられ（Ｓ２０２）、内容が確認されて、資格付与の審査がなされる。ＯＫであれば、企業甲は直接自治体Ｂに対して入札に参加することができる（Ｓ２０３）。このシステムは、サイト運営者側に各企業の事前データがない場合に有効な手段となりうる。

【００４２】

次に、図５を参照して、本発明のシステムの別の実施形態における処理の流れの一例について説明する。
図５においては、電子証明書受信手段および認証手段を少なくとも備えるオンラインデータ処理システムにおいて、インターネットを介してデータ送受信、データ処理を行うＷＥＢサイト等に接続されて、データ処理システムが備えられる。データ処理システムは、ＷＥＢサイト等を管理・運営する管理者が、その組織内等におけるデータ処理を行う基幹システムである。たとえば、受信したデータを記憶したり、取引、請求、経理その他のデータ処理を行うシステムや、ユーザーの顧客管理などを行うシステムなどがその一例である。
ユーザー認証後の各種データ処理を行うデータ処理システムは、前記の認証データベースに用いられる企業コード等の組織識別データを利用することを特徴とする。
これにより、電子申請（受付)、電子契約（取引開始)、さらに基幹システム（取引～請求など）へとシームレスな業務連携が可能となる
通常の電子証明書はあくまでも認証に特化したものでしかない。サイト運営者は認証終了後、基幹の業務システム（実際の商取引）へと進めるために、当該ユーザーの顧客情報を呼び出して取引情報と結びつけるなど新たな作業を強いられるが、汎用的企業コードが組み込まれた電子証明書が流通し、企業情報が入力された認証データベースの利用がオープンとなれば、認証後、当該企業の情報は企業コードをキーとして連動していくので、シームレスに基幹業務へと進めることが可能となる。

【００４３】

次に、図６を参照して、本発明のシステムの別の実施形態における処理の流れの一例について説明する。
本実施形態においては、図６に示すように、認証機関システムに備えられる認証データベースは、組織識別データをキーとして関連付けられた企業情報などの組織情報を記憶・蓄積・更新する組織情報データベースと連携して備えられる。
企業は生き物であり、吸収合併、倒産、休眠など、様々な変化が起きる可能性がある。しかしながら、たとえば、自治体の入札の場合、倒産企業や合併による被合併企業などは入札参加資格を失うが、これらの変動情報と電子証明書とが連動した仕組みが商業登記認証局や通常の民間認証局にはなく、そのような事態が発生した際にスピーディな対応が取れない。また、商業登記に基づいた電子証明書では、企業の休眠や登記の不正利用などにも対応できない。
ここで、企業の変動情報を反映した組織情報（企業情報）データベースと認証データベースとを結びつけることにより、企業等の情報が更新される場合には、認証データベースがリアルタイムまたはそれに近いタイミングで随時更新され反映される（Ｓ３００）。
倒産や被合併などによって電子申請や電子入札にアクセス不可となった企業等に関してのデータの更新があった場合には、認証機関システムからオンラインデータ処理システムに対し、無効処理リスト（ＣＲＬ）を送信するなどして提供する（Ｓ３０１）。無効処理リストはオンラインデータ処理システムにおいて記憶される。

ユーザー端末からオンラインデータ処理システムにアクセスし、電子商取引の申込みや、入札参加申込みなどの、オンラインデータ処理システムがデータ入力・送信を要求する所定のデータ項目のデータを入力し、入力された電子文書を送信する（Ｓ３０２）。この際に電子証明書を併せて送信し、オンラインデータ処理システムにおいては、ユーザー端末から送信されたデータを電子証明書受信手段が受信する。
次いで署名の検証を行う際に、無効処理リストと照合することで、認証システム上で警告することができる（Ｓ３０３）。無効処理リストにない場合には、通常の認証処理を行う。
これにより、サイト運営者は、適格なユーザーとのみ、やりとりを行うことが可能となる。企業等の組織情報の更新・変動を反映したユーザー認証が可能にされている。

【００４４】
次に、図７を参照して、本発明のシステムの別の実施形態における処理の流れの一例について説明する。
本実施形態においては、オンラインデータ処理システムには顧客等のユーザーデータベースが備えられている。
商号変更、住所変更など企業は変動するものであるが、通常の認証システムでは、そのメンテナンスが煩雑（あるいは不可能）であり、登録時の情報がそのままになっているケースが多い。
ここで、企業の変動情報を反映した組織情報（企業情報）データベースと認証データベースとを結びつけることにより、データの更新があった場合には認証データベースがリアルタイムまたはそれに近いタイミングで随時更新され反映される（Ｓ４００）。データの更新があった場合には、認証機関システムからオンラインデータ処理システムに対し、更新されたデータを送信するなどして提供し（Ｓ４０１）、ユーザーデータベースを更新する（Ｓ４０２）。商号変更、住所変更などの情報を提供でき、サイト運営者側の顧客データベースがメンテナンスすることができる。
前記の認証データベースと連携して備えられる企業情報などの組織情報を記憶・蓄積・更新する組織情報データベースの更新・変動を、前記のユーザーデータベースの更新・変動に利用可能なことを特徴とする。
顧客データベースがメンテナンスでき、ユーザー端末からオンラインデータ処理システムにアクセスして（Ｓ４０３）、認証処理を行う場合などにも、最新のデータを参照することができる。
次に、図８を参照して、本発明のシステムの別の実施形態における処理の流れの一例について説明する。
たとえば、建設業においては、経営事項審査による客観的な工事施工能力評価にて、入札制限やスクリーニングが可能だが、他業種においては、経営事項審査に代わる仕組みはない。物品調達や申請をオープンな環境で電子化を推進していくためには、入札・申請企業の状態を把握し、判断していくための企業情報を入手できるシステムとの連携が必要となる。

【００４５】
ここで、企業の信用情報を備えた組織情報（企業情報）データベースと認証データベースとを結びつけておくことにより、サイト運営者側は各ユーザーの信用状態を確認することができる。また、あらかじめ権限情報としての適格スクリーニング情報が認証データベースに入力されていれば、自動的な企業選定が可能となる。
本実施形態において、組織情報データベースに記憶されるデータには、企業の信用情報などの組織信用情報が含まれている。
組織信用情報はたとえば、第三者である調査員が、企業等の基本情報、組織情報、取引高や支払実績、納品実績その他の取引情報、財務情報、構成員情報、その他の重要事項情報を含む、定量的あるいは定性的情報などを含むことができる。またこのような情報に基づき、信用情報を示す指数、評点、ランク付け、その他の信用情報として記憶・蓄積・更新をすることができる。

また本実施形態においては、認証データベースにあらかじめ記憶されている権限情報には、信用情報に基づく適格スクリーニング情報が含まれていることが望ましい。
適格スクリーニング情報は、それぞれのオンラインデータ処理システムが、取引や入札等の相手の適格性を判定するために、前記の組織信用情報に基づきスクリーニング処理を行うための基準となるデータである。あらかじめ、企業情報から基準値または格付値のテーブルなどを判断の元になるデータを作成しておくことにより、取引可否、入札可否、あるいは優先順位による判断などを行い有望先を絞り込むことを特徴とする。
この場合には初めに、あらかじめ、企業情報から基準値または格付値のテーブルなどを判断の元になるデータを作成しておく。
基準値とは例えば、評点５０点以上は取引をしないなどの基準となる数値などの値であり、格付値とは例えば、評点７０点以上がＡランクなどの、判断基準となるランク分けである。
なお本発明のシステムにおいては、上記の基準値、あるいは格付値以外にも、判断の基準となる様々な尺度などをあらかじめ設定しておくことができる。
また判断の元となるデータについては、案件単位で許容値の変更を行うことができる。
これにより、オンラインデータ処理システムにおけるデータ処理において、信用情報に基づくスクリーニング処理が可能なことを特徴とする。

【００４６】

次に、前記の企業情報取得エージェントは、企業コードが付加された取引条件情報から企業情報を取得するための情報（企業コードなど）を抽出し、企業情報提供サーバに対し、検索依頼を行う。検索依頼は、リアルタイム、または、バッチ処理にて、マージしたデータを企業情報取得のために企業情報取得サーバ向けに送信する。
図８を参照すれば、組織情報データベースに記憶されている組織信用情報は、認証データベースに記憶されるデータと企業コード等の組織識別データと関連付けられて記憶されており、企業コード等を用いて抽出・参照可能にされている（Ｓ５００）。
自動的なスクリーニング処理を行う場合には、あらかじめオンラインデータ処理システムから認証データベースに対して、適格スクリーニング情報を設定し、記憶させておく（Ｓ５０１）。
ユーザー端末からオンラインデータ処理システムにアクセスし、電子商取引の申込みや、入札参加申込みなどの、オンラインデータ処理システムがデータ入力・送信を要求する所定のデータ項目のデータを入力し、入力された電子文書を送信する（Ｓ５０２）。この際に電子証明書を併せて送信し、オンラインデータ処理システムにおいては、ユーザー端末から送信されたデータを電子証明書受信手段が受信する。
次いで、認証データベースに照会を行い（Ｓ５０３）、企業コード等を用いて該当する企業等の組織の信用情報を含む情報を抽出する（Ｓ５０４）。企業コードをキーにして、検索、抽出されるデータは、企業情報や、売上高や評点などの情報である。返却するデータが、判断そのもの（ＹＥＳ・ＮＯなど）のみの場合もある。
このようにして取得された信用情報を用いて、取引可否、入札可否や優先順位の判断を行う。以上のような処理により、格付値または限界値のテーブルなどを元にして、取引可否、優先順位による判断などを行い有望先を絞り込む。
次に認証期間システムから取得した結果のデータから、オンラインデータ処理システムにおいて得られた前記の判断結果は、情報を送信して取引申込等をした企業等に対してその結果を通知する。

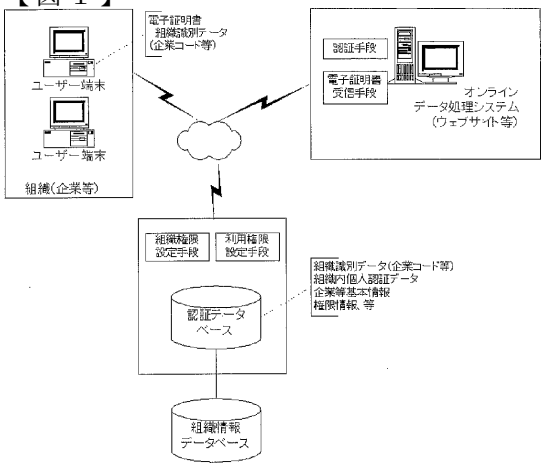
【産業上の利用可能性】

【００４７】

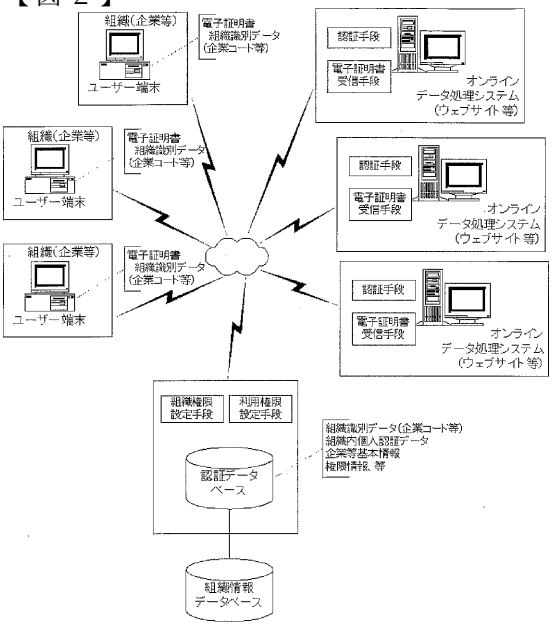
以上詳細に説明したように、本発明によれば、インターネット等の電子空間での取引や入札、契約などにおいて、個人を認証する際に、その個人が本当に企業等の組織に所属しているのか否か、あるいは所属をしていたとしても取引や入札等において参加・判断・決定の権限があるか否かなどを認証することの可能なシステムを提供することができる。
そのため、電子証明書に汎用企業コードまたはシリアルナンバー等を組み込み、認証デー

タベースに、企業コード、シリアルナンバー、企業内個人情報、企業基本情報、権限情報等を入れることにより、企業と個人の情報とを関連付けて認証することが可能となり、また個人事業者の認証が可能になる。
さらに本発明においては、運営者が違う複数の認証サイトなど、複数の認証システムにおいても、１枚の証明書でユーザーが対応可能なシステムを提供することができる。電子証明書に汎用的企業コードが組み込まれ、認証データベースの活用がオープンとなれば、自治体や企業などの運営者などの認証サイド、入札者などのユーザーの被認証サイド共に、１つの汎用電子証明書で認証作業が済まされることが可能になる。
さらに本発明によれば、電子証明書を用いた認証のための認証データベースと、企業等の組織情報データベースとを連携させることにより、認証に際して随時最新の更新されたデータに基づき認証等の処理が可能なシステムを提供することができる。企業等からの退職、部署や役職が変動、さらに企業そのものが合併や、倒産、信用情報の変動、その他の変動に対応することにより、適格な認証処理を行うことができる。
しかも、データは認証機関が収集・蓄積・更新を行うようにすることで、それぞれの認証を行うＷＥＢサイトなどが個々にデータベースを構築することなく、本発明の認証システムを利用することが可能になる。
【図面の簡単な説明】
【００４４】
【図１】本発明のシステムの基本的な構成の一例を示すシステム構成図である。
【図２】認証機関システムが、複数のオンラインデータ処理システムからアクセス可能に備えられた形態の一例を示すシステム構成図である。
【図３】本発明のシステムの基本的な処理の流れの一例を示すシステム概要図である。
【図４】本発明のシステムの一実施形態の基本的な処理の流れの一例を示すシステム概要図である。
【図５】本発明のシステムの一実施形態の基本的な処理の流れの一例を示すシステム概要図である。
【図６】本発明のシステムの一実施形態の基本的な処理の流れの一例を示すシステム概要図である。
【図７】本発明のシステムの一実施形態の基本的な処理の流れの一例を示すシステム概要図である。
【図８】本発明のシステムの一実施形態の基本的な処理の流れの一例を示すシステム概要図である。

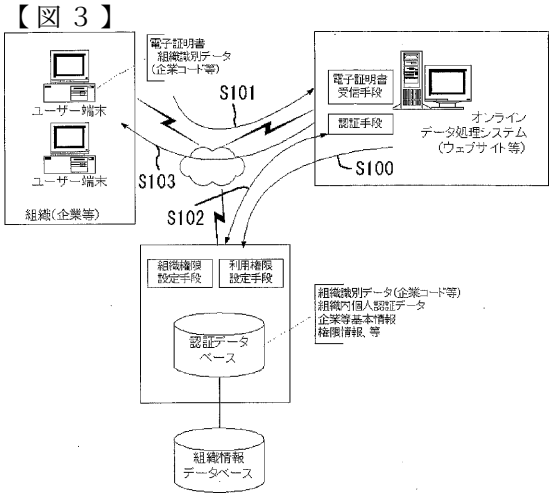
【図１】


電子証明書
組織識別データ
(企業コード等)
ユーザー端末
ユーザー端末
組織(企業等)
認証手段
電子証明書
受信手段
オンライン
データ処理システム
(ウェブサイト等)
組織権限
設定手段
利用権限
設定手段
認証データ
ベース
組織識別データ(企業コード等)
組織内個人認証データ
企業等基本情報
権限情報、等
組織情報
データベース

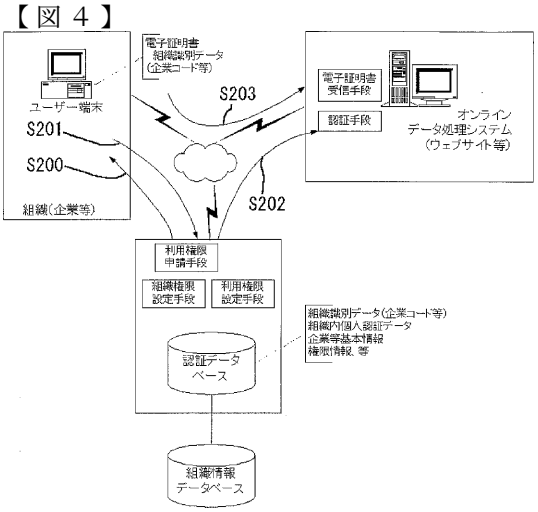
【図２】


組織(企業等)
ユーザー端末
電子証明書
組織識別データ
(企業コード等)
認証手段
電子証明書
受信手段
オンライン
データ処理システム
(ウェブサイト等)
組織権限
設定手段
利用権限
設定手段
認証データ
ベース
組織識別データ(企業コード等)
組織内個人認証データ
企業等基本情報
権限情報、等
組織情報
データベース

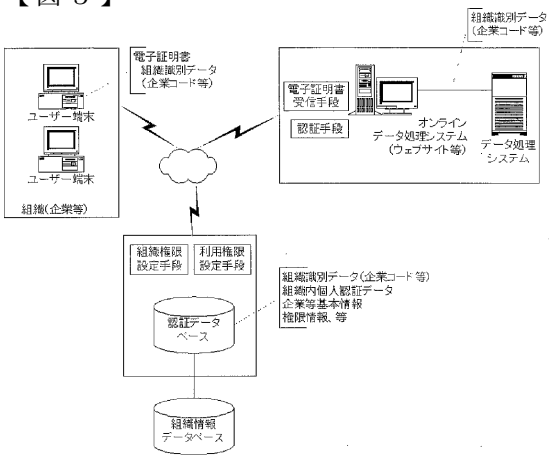
【図３】


電子証明書
組織識別データ
(企業コード等)
ユーザー端末
ユーザー端末
組織(企業等)
S101
S103
S102
S100
電子証明書
受信手段
認証手段
オンライン
データ処理システム
(ウェブサイト等)
組織権限
設定手段
利用権限
設定手段
認証データ
ベース
組織識別データ(企業コード等)
組織内個人認証データ
企業等基本情報
権限情報、等
組織情報
データベース

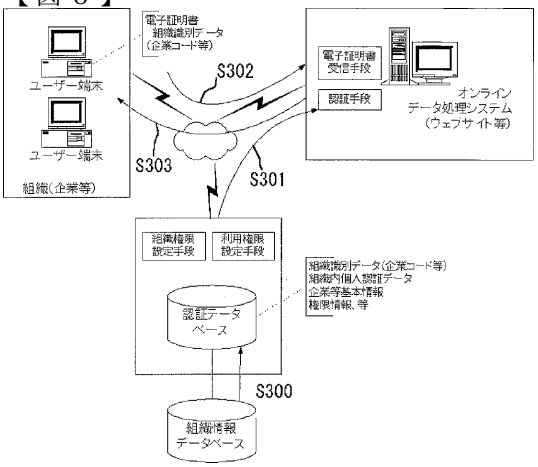
【図４】


電子証明書
組織識別データ
(企業コード等)
ユーザー端末
S201
S200
組織(企業等)
S203
S202
電子証明書
受信手段
認証手段
オンライン
データ処理システム
(ウェブサイト等)
利用権限
申請手段
組織権限
設定手段
利用権限
設定手段
認証データ
ベース
組織識別データ(企業コード等)
組織内個人認証データ
企業等基本情報
権限情報、等
組織情報
データベース

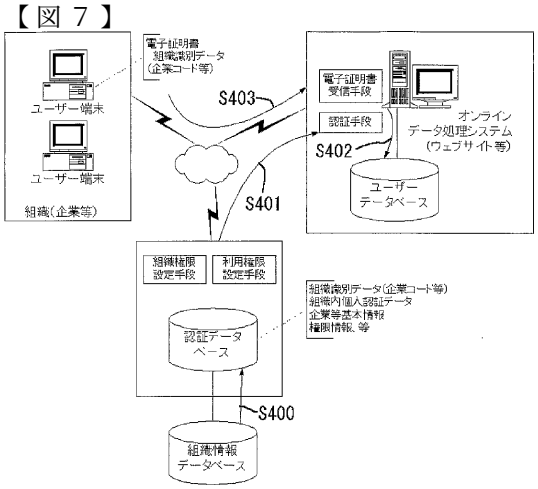
【図５】


組織識別データ
(企業コード等)
電子証明書
組織識別データ
(企業コード等)
ユーザー端末
ユーザー端末
組織(企業等)
電子証明書
受信手段
認証手段
オンライン
データ処理システム
(ウェブサイト等)
データ処理
システム
組織権限
設定手段
利用権限
設定手段
認証データ
ベース
組織識別データ(企業コード等)
組織内個人認証データ
企業等基本情報
権限情報、等
組織情報
データベース

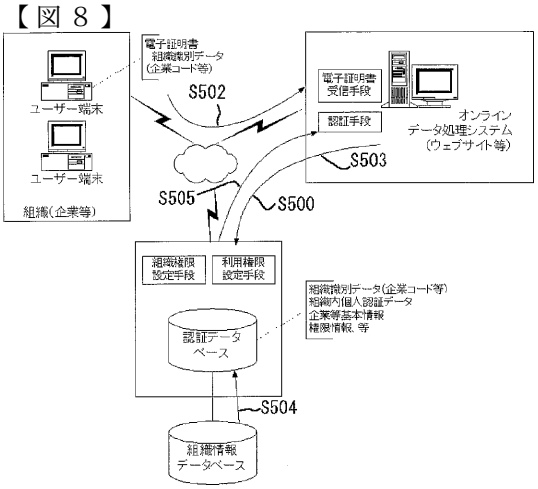
【図６】


電子証明書
組織識別データ
(企業コード等)
ユーザー端末
ユーザー端末
組織(企業等)
S302
S303
S301
電子証明書
受信手段
認証手段
オンライン
データ処理システム
(ウェブサイト等)
組織権限
設定手段
利用権限
設定手段
認証データ
ベース
組織識別データ(企業コード等)
組織内個人認証データ
企業等基本情報
権限情報、等
S300
組織情報
データベース

【図７】


電子証明書
組織識別データ
(企業コード等)
ユーザー端末
ユーザー端末
組織(企業等)
S403
S402
S401
電子証明書
受信手段
認証手段
オンライン
データ処理システム
(ウェブサイト等)
ユーザー
データベース
組織権限
設定手段
利用権限
設定手段
認証データ
ベース
組織識別データ(企業コード等)
組織内個人認証データ
企業等基本情報
権限情報、等
S400
組織情報
データベース

【図８】


電子証明書
組織識別データ
(企業コード等)
ユーザー端末
ユーザー端末
組織(企業等)
S502
S505
S500
S503
電子証明書
受信手段
認証手段
オンライン
データ処理システム
(ウェブサイト等)
組織権限
設定手段
利用権限
設定手段
認証データ
ベース
組織識別データ(企業コード等)
組織内個人認証データ
企業等基本情報
権限情報、等
S504
組織情報
データベース

フロントページの続き

(72)発明者　浅野　敬
東京都港区南青山２－５－２０　株式会社帝国データバンク内

審査官　宮司　卓佳

(56)参考文献　特開２００１－２１６４００（ＪＰ，Ａ）
特開２０００－０２０３７７（ＪＰ，Ａ）
特開２００２－００７９３０（ＪＰ，Ａ）
特開平１１－２９８４６９（ＪＰ，Ａ）
特開２００２－１４９６０９（ＪＰ，Ａ）
特開２００２－０２６９６２（ＪＰ，Ａ）
特開２００１－２１６３７１（ＪＰ，Ａ）
特開２００１－３０６５２５（ＪＰ，Ａ）
河井保博，山崎洋一，特集１　ディジタル署名時代がやってくる　法整備で加速する電子文書活用への道，日経インターネットテクノロジー，２００１年　5月２２日，p.159-p.163
岩野英一，奥澤慎哉，浅田隆介，ＥＣビジネスの具体的展開　総合ネット与信・金融サービスサイト，ＮＴＴ技術ジャーナル，２００１年　6月　1日，第１３巻，第6号，p.20-p.22

(58)調査した分野(Int.Cl.^{7}，ＤＢ名)
G06F15/00
G06F17/60
H04L 9/32