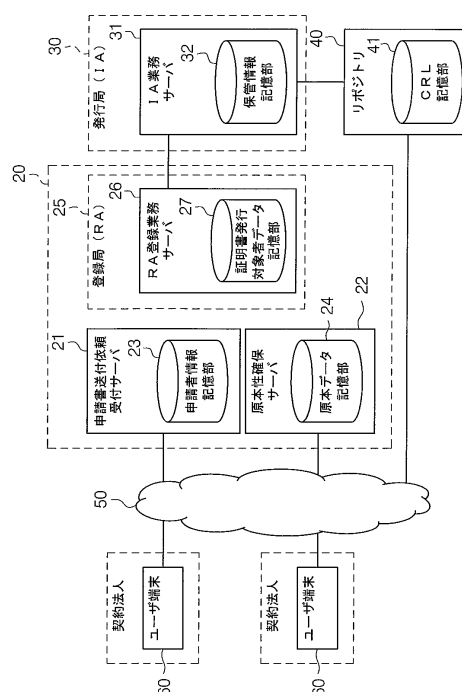




【特許請求の範囲】

【請求項 1】

商業登記簿謄本に基づいて確認された電子証明書の申請者が所属する法人の商号に関する情報と、

前記法人の代表者の印鑑登録証明書により前記申請者についての前記法人の証明の意思が確認された前記申請者に関する情報と

を含むことを特徴とする電子証明書。

【請求項 2】

前記法人の代表者の印鑑登録証明書により前記申請者についての前記法人の証明の意思が確認された、前記法人における前記申請者が所属する部署名に関する情報又は前記法人における前記申請者の役職名に関する情報をさらに含むことを特徴とする請求項 1 に記載の電子証明書。

10

【請求項 3】

前記第 1 のユーザに対して発行された電子証明書を用いた前記第 1 のユーザの電子署名が施された電子文書を受信した第 2 のユーザの端末が、

前記電子文書の内容を表示する段階と、

前記電子証明書に含まれる、商業登記簿謄本に基づいて確認された電子証明書の申請者である第 1 のユーザが所属する法人の商号に関する情報と、前記法人の代表者の印鑑登録証明書により前記第 1 のユーザについての前記法人の証明の意思が確認された前記第 1 のユーザに関する情報とを表示する段階と

20

を備えたことを特徴とする認証方法。

【請求項 4】

前記認証方法において、

前記電子証明書は、前記法人における前記申請者が所属する部署名に関する情報、又は、前記法人における前記申請者の役職名に関する情報を含み、

前記第 2 のユーザの端末が、

前記電子証明書に含まれる、前記第 1 のユーザが所属する法人における前記第 1 のユーザが所属する部署名に関する情報、又は、前記第 1 のユーザが所属する法人における前記第 1 のユーザの役職名に関する情報をさらに表示する段階

をさらに備えたことを特徴とする請求項 3 に記載の認証方法。

30

【請求項 5】

第 1 のユーザと第 2 のユーザとの間で取り交わす電子文書を管理するコンピュータを用いて電子文書を認証する認証方法であって、

前記コンピュータが、

商業登記簿謄本に基づいて確認された電子証明書の申請者である第 1 のユーザが所属する法人の商号に関する情報と、前記第 1 のユーザが所属する法人の代表者の印鑑登録証明書により前記第 1 のユーザについての前記第 1 のユーザが所属する法人の証明の意思が確認された前記第 1 のユーザに関する情報とを含む、前記第 1 のユーザに対して発行された電子証明書を用いて前記第 1 のユーザの電子署名が施された電子文書を原本性を確保して電子文書を保管する原本性確保電子文書保存装置に保存する段階と、

40

第 2 のユーザの端末に前記原本性確保電子文書保存装置に保存された電子文書を提供する段階と、

前記第 2 のユーザの端末に前記第 1 のユーザの電子証明書に含まれる前記第 1 のユーザが所属する法人に関する情報と前記第 1 のユーザに関する情報とを表示する段階と、

商業登記簿謄本に基づいて確認された電子証明書の申請者である第 2 のユーザが所属する法人の商号に関する情報と、前記第 2 のユーザが所属する法人の代表者の印鑑登録証明書により前記第 2 のユーザについての前記第 2 のユーザが所属する法人の証明の意思が確認された前記第 2 のユーザに関する情報とを含む、前記第 2 のユーザに対して発行された電子証明書を用いて前記第 2 のユーザの電子署名が施された電子文書を前記原本性確保電子文書保存装置に保存する段階と

50

を備えたことを特徴とする認証方法。

【請求項 6】

前記第 1 のユーザの電子証明書は、前記第 1 のユーザが所属する法人における前記第 1 のユーザが所属する部署名に関する情報、又は、前記第 1 のユーザが所属する法人における前記第 1 のユーザの役職名に関する情報を含み、

前記コンピュータが、

前記第 2 のユーザの端末に、前記第 1 のユーザの電子証明書に含まれる、前記第 1 のユーザが所属する法人における前記第 1 のユーザが所属する部署名に関する情報、又は、前記第 1 のユーザが所属する法人における前記第 1 のユーザの役職名に関する情報を表示させる段階

10

をさらに備えたことを特徴とする請求項 5 に記載の認証方法。

【請求項 7】

前記電子文書は P D F 形式であって、前記電子文書の表示において前記電子署名と連携した印影を表示させることを特徴とする請求項 3 ～ 6 のいずれか 1 つに記載の認証方法。

【請求項 8】

第 1 のユーザと第 2 のユーザとの間で取り交わす電子文書を管理するコンピュータを用いて電子文書を認証する認証プログラムであって、

コンピュータを、

商業登記簿謄本に基づいて確認された電子証明書の申請者である第 1 のユーザが所属する法人の商号に関する情報と、前記第 1 のユーザが所属する法人の代表者の印鑑登録証明書により前記第 1 のユーザについての前記第 1 のユーザが所属する法人の証明の意思が確認された前記第 1 のユーザに関する情報とを含む、前記第 1 のユーザに対して発行された電子証明書を用いて前記第 1 のユーザの電子署名が施された電子文書を原本性を確保して電子文書を保管する原本性確保電子文書保存装置に保存する手段と、

20

第 2 のユーザの端末に前記原本性確保電子文書保存装置に保存された電子文書を提供する手段と、

前記第 2 のユーザの端末に前記第 1 のユーザの電子証明書に含まれる前記第 1 のユーザが所属する法人に関する情報と前記第 1 のユーザに関する情報とを表示する手段と、

商業登記簿謄本に基づいて確認された電子証明書の申請者である第 2 のユーザが所属する法人の商号に関する情報と、前記第 2 のユーザが所属する法人の代表者の印鑑登録証明書により前記第 2 のユーザについての前記第 2 のユーザが所属する法人の証明の意思が確認された前記第 2 のユーザに関する情報とを含む、前記第 2 のユーザに対して発行された電子証明書を用いて前記第 2 のユーザの電子署名が施された電子文書を前記原本性確保電子文書保存装置に保存する手段と

30

として機能させるための認証プログラム。

【請求項 9】

前記第 1 のユーザの電子証明書は、前記第 1 のユーザが所属する法人における前記第 1 のユーザが所属する部署名に関する情報、又は、前記第 1 のユーザが所属する法人における前記第 1 のユーザの役職名に関する情報を含み、

前記コンピュータを、

40

前記第 2 のユーザの端末に、前記電子証明書に含まれる、前記第 1 のユーザが所属する法人における前記第 1 のユーザが所属する部署名に関する情報、又は、前記第 1 のユーザが所属する法人における前記第 1 のユーザの役職名に関する情報を表示させる手段

として機能させることを特徴とする請求項 8 に記載の認証プログラム。

【請求項 10】

前記電子文書は P D F 形式であって、前記電子文書の表示において前記電子署名と連携した印影を表示させることを特徴とする請求項 8 又は 9 に記載の認証プログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

50

本発明は、公開鍵暗号方式に基づく電子証明書、その電子証明書を用いた認証方法及び認証プログラムに関するものである。

【0002】

【従来の技術】

電子署名法においては、電子署名とその電子署名を検証するための電子証明書及び電子証明書の失効情報を発行する認証業務について一定の要件を満たす場合に特定認証業務の認定を受け得る。そして、特定認証業務の認定を受けた認証業務によって管理されている電子証明書のみが、実社会における実印と同等の扱いを受けることができることとなり、法的に一定の効果が期待できる証明書となる（例えば、非特許文献1参照。）。

【0003】

一方、法人の認証については、法人認証局が法人登記簿に基づいて各法人について1つだけ発行した電子証明書が用いられる。法人認証局は商業登記簿の記載内容に基づいて法人に対して電子証明書を発行するもので、電子証明書の発行を受けた法人は、その電子証明書を電子申請や電子商取引等における企業の認証情報として利用できる。

【0004】

【非特許文献1】

情報処理振興事業協会 セキュリティセンター著、“PKI関連技術解説 8.5 特定認証業務機関”、[online]、平成14年12月12日、情報処理振興事業協会セキュリティセンター、[平成15年4月21日検索]、インターネット<URL: <http://www.ipa.go.jp/security/pki/085.html>>

【0005】

【発明が解決しようとする課題】

しかし、電子署名法は、個人を認証するためのものであり、電子署名法に対応した特定認証業務においては、その個人の所属する法人や所属部署等については、電子署名法の認定制度における認定の対象外である。このため、電子署名法における特定認証業務の認定を受けた電子証明書を用いたとしても、個人の特定はできるが、その個人が所属する法人やその法人における役職等は特定できない。従って、電子署名法による特定認証業務により発行された電子証明書を用いたとしても、個人の意思が確認できるのみで、その個人が所属する法人の意思を確認することはできない。

【0006】

一方、法人認証局による電子証明書は各法人に対して1つだけしか発行されない。このため、法人間での契約において、必ず、法人認証局が発行した電子証明書を用いなければならないとすると、法人内で権限を委譲された担当者が契約を行うという取引実情に合わず不便である。

【0007】

本発明は、上記問題点を解決するためになされたものであり、その目的は、法人から権限を委譲された個人の電子証明書を用いて、その法人の意思を証明できる電子証明書、認証方法及び認証プログラムを提供することにある。

【0008】

【課題を解決するための手段】

上記問題点を解決するために、請求項1に記載の発明は、商業登記簿謄本に基づいて確認された電子証明書の申請者が所属する法人の商号に関する情報と、前記法人の代表者の印鑑登録証明書により前記申請者についての前記法人の証明の意思が確認された前記申請者に関する情報とを含むことを要旨とする。

【0009】

請求項2に記載の発明は、請求項1に記載の電子証明書において、前記法人の代表者の印鑑登録証明書により前記申請者についての前記法人の証明の意思が確認された、前記法人における前記申請者が所属する部署名に関する情報又は前記法人における前記申請者の役職名に関する情報をさらに含むことを要旨とする。

10

20

30

40

50

【0010】

請求項3に記載の発明は、前記第1のユーザに対して発行された電子証明書を用いた前記第1のユーザの電子署名が施された電子文書を受信した第2のユーザの端末が、前記電子文書の内容を表示する段階と、前記電子証明書に含まれる、商業登記簿謄本に基づいて確認された電子証明書の申請者である第1のユーザが所属する法人の商号に関する情報と、前記法人の代表者の印鑑登録証明書により前記第1のユーザについての前記法人の証明の意思が確認された前記第1のユーザに関する情報とを表示する段階とを備えたことを要旨とする。

【0011】

請求項4に記載の発明は、請求項3に記載の認証方法において、前記認証方法において、前記電子証明書は、前記法人における前記申請者が所属する部署名に関する情報、又は、前記法人における前記申請者の役職名に関する情報を含み、前記第2のユーザの端末が、前記電子証明書に含まれる、前記第1のユーザが所属する法人における前記第1のユーザが所属する部署名に関する情報、又は、前記第1のユーザが所属する法人における前記第1のユーザの役職名に関する情報をさらに表示する段階をさらに備えたことを要旨とする。

【0012】

請求項5に記載の発明は、第1のユーザと第2のユーザとの間で取り交わす電子文書を管理するコンピュータを用いて電子文書を認証する認証方法であって、前記コンピュータが、商業登記簿謄本に基づいて確認された電子証明書の申請者である第1のユーザが所属する法人の商号に関する情報と、前記第1のユーザが所属する法人の代表者の印鑑登録証明書により前記第1のユーザについての前記第1のユーザが所属する法人の証明の意思が確認された前記第1のユーザに関する情報とを含む、前記第1のユーザに対して発行された電子証明書を用いて前記第1のユーザの電子署名が施された電子文書を原本性を確保して電子文書を保管する原本性確保電子文書保存装置に保存する段階と、第2のユーザの端末に前記原本性確保電子文書保存装置に保存された電子文書を提供する段階と、前記第2のユーザの端末に前記第1のユーザの電子証明書に含まれる前記第1のユーザが所属する法人に関する情報と前記第1のユーザに関する情報とを表示する段階と、商業登記簿謄本に基づいて確認された電子証明書の申請者である第2のユーザが所属する法人の商号に関する情報と、前記第2のユーザが所属する法人の代表者の印鑑登録証明書により前記第2のユーザについての前記第2のユーザが所属する法人の証明の意思が確認された前記第2のユーザに関する情報とを含む、前記第2のユーザに対して発行された電子証明書を用いて前記第2のユーザの電子署名が施された電子文書を前記原本性確保電子文書保存装置に保存する段階とを備えたことを要旨とする。

【0013】

請求項6に記載の発明は、請求項5に記載の認証方法において、前記第1のユーザの電子証明書は、前記第1のユーザが所属する法人における前記第1のユーザが所属する部署名に関する情報、又は、前記第1のユーザが所属する法人における前記第1のユーザの役職名に関する情報を含み、前記コンピュータが、前記第2のユーザの端末に、前記第1のユーザの電子証明書に含まれる、前記第1のユーザが所属する法人における前記第1のユーザが所属する部署名に関する情報、又は、前記第1のユーザが所属する法人における前記第1のユーザの役職名に関する情報を表示させる段階をさらに備えたことを要旨とする。

【0014】

請求項7に記載の発明は、請求項3～6のいずれか1つに記載の認証方法において、前記電子文書はPDF形式であって、前記電子文書の表示において前記電子署名と連携した印影を表示させることを要旨とする。

【0015】

請求項8に記載の発明は、第1のユーザと第2のユーザとの間で取り交わす電子文書を管理するコンピュータを用いて電子文書を認証する認証プログラムであって、コンピュータを、商業登記簿謄本に基づいて確認された電子証明書の申請者である第1のユーザが所属

する法人の商号に関する情報と、前記第 1 のユーザが所属する法人の代表者の印鑑登録証明書により前記第 1 のユーザについての前記第 1 のユーザが所属する法人の証明の意思が確認された前記第 1 のユーザに関する情報とを含む、前記第 1 のユーザに対して発行された電子証明書を用いて前記第 1 のユーザの電子署名が施された電子文書を原本性を確保して電子文書を保管する原本性確保電子文書保存装置に保存する手段と、第 2 のユーザの端末に前記原本性確保電子文書保存装置に保存された電子文書を提供する手段と、前記第 2 のユーザの端末に前記第 1 のユーザの電子証明書に含まれる前記第 1 のユーザが所属する法人に関する情報と前記第 1 のユーザに関する情報とを表示する手段と、商業登記簿謄本に基づいて確認された電子証明書の申請者である第 2 のユーザが所属する法人の商号に関する情報と、前記第 2 のユーザが所属する法人の代表者の印鑑登録証明書により前記第 2 のユーザについての前記第 2 のユーザが所属する法人の証明の意思が確認された前記第 2 のユーザに関する情報とを含む、前記第 2 のユーザに対して発行された電子証明書を用いて前記第 2 のユーザの電子署名が施された電子文書を前記原本性確保電子文書保存装置に保存する手段ととして機能させることを要旨とする。 10

【0016】

請求項 9 に記載の発明は、請求項 8 に記載の認証プログラムにおいて、前記第 1 のユーザの電子証明書は、前記第 1 のユーザが所属する法人における前記第 1 のユーザが所属する部署名に関する情報、又は、前記第 1 のユーザが所属する法人における前記第 1 のユーザの役職名に関する情報を含み、前記コンピュータを、前記第 2 のユーザの端末に、前記電子証明書に含まれる、前記第 1 のユーザが所属する法人における前記第 1 のユーザが所属する部署名に関する情報、又は、前記第 1 のユーザが所属する法人における前記第 1 のユーザの役職名に関する情報を表示させる手段として機能させることを要旨とする。 20

【0017】

請求項 10 に記載の発明は、請求項 8 又は 9 に記載の認証プログラムにおいて、前記電子文書は P D F 形式であって、前記電子文書の表示において前記電子署名と連携した印影を表示させることを要旨とする。

【0018】

(作用)

請求項 1 に記載の発明によれば、電子証明書は、商業登記簿謄本に基づいて確認された電子証明書の申請者が所属する法人の商号に関する情報と、その法人の代表者の印鑑登録証明書により申請者についてのその法人の証明の意思が確認された申請者に関する情報とを含む。このため、個人の申請者に対して発行された電子証明書を用いて、その個人が所属する法人の商号に関する情報を証明できる。従って、法人から権限を委譲された個人に対して発行された電子証明書を用いて、その法人の意思を証明できる。 30

【0019】

請求項 2 に記載の発明によれば、電子証明書は、法人の代表者の印鑑登録証明書により申請者についての法人の証明の意思が確認された、その法人における申請者が所属する部署名に関する情報又はその法人における申請者の役職名に関する情報をさらに含む。このため、電子証明書に記載された部署名又は役職名に関する情報を確認することで、電子証明書の所有者である個人が所属する部署名又はその個人の役職名を確認できる。 40

【0020】

請求項 3 に記載の発明によれば、第 2 のユーザは、電子文書に署名を行った第 1 のユーザが所属する法人の商号を確認できる。従って、第 2 のユーザは、第 1 のユーザが所属する法人から権限を委譲された第 1 のユーザに対して発行された電子証明書により、受信した電子文書が、第 1 のユーザが所属する法人の意思によるものことを確認できる。

【0021】

請求項 4 に記載の発明によれば、第 2 のユーザは、第 1 のユーザの電子証明書に記載された部署名又は役職名に関する情報を確認することで、第 1 のユーザが所属する部署名又は第 1 のユーザの役職名を確認できる。

【0022】

請求項 5 又は 8 に記載の発明によれば、第 2 のユーザが、第 1 のユーザの電子証明書における第 1 のユーザが所属する法人の商号を確認した上で、第 2 のユーザの電子署名を施して電子文書を原本性確保電子文書保存装置で保存できる。従って、それぞれが所属する法人から権限を委譲された第 1 のユーザと第 2 のユーザとの間で、それぞれが所属する法人の意思を明確にしながら、契約書として取り扱うことが可能な電子文書を取り交わすことができる。そして、その電子文書を原本性を確保して保存できる。このため、ネットワークを介して契約を締結することが可能となり、文書作成から契約の締結までの効率を上げることができる。さらに、紙の契約書を使用しないため、紙の契約書を保管する場所が不要となる。

【0023】

10

請求項 6 又は 9 に記載の発明によれば、第 2 のユーザは、第 1 のユーザの電子証明書に記載された部署名又は役職名に関する情報を確認することで、第 1 のユーザが所属する部署名又はその第 1 のユーザの役職名を確認できる。

【0024】

請求項 7 又は 10 に記載の発明によれば、PDF 形式の電子文書を用いるとともに、電子文書の表示において電子署名と連携した印影を表示させることで、紙の契約書と同様に視覚される電子文書を用いることが可能となる。また、PDF 形式の電子文書を用いることで、電子媒体に保存された内容を必要に応じて肉眼で見読可能な状態にすることが可能となる。

【0025】

20

【発明の実施の形態】

以下、本発明を具体化した一実施形態を図 1 ～図 9 に従って説明する。本実施形態では、電子証明書の所有者である利用者の所属する法人の実在と、その法人における利用者の所属とを保証する電子証明書、認証方法及び認証プログラムとして説明する。本実施形態では、契約支援システム 20 の契約法人に所属する従業者に対して電子証明書を発行する際に、その契約法人の実在と、その契約法人におけるその従業者の所属とを確認する。そして、発行する電子証明書に、契約法人の商号、その従業者の所属部署及び役職を電子証明書の利用者に関する情報として含める。本実施形態における認証業務は、電子署名法における特定認証業務の認定の要件を満たすものとする。

【0026】

30

なお、本実施形態では、電子証明書の所有者を利用者といい、電子証明書の検証をする者を検証者というものとする。また、利用者及び検証者が所属する法人は、契約支援システム 20 と契約支援サービスについての契約を結んでおり、契約支援サービスの提供を受ける法人を契約法人というものとする。そして、この契約法人に所属する個人（利用者）に対して、本実施形態における認証局が電子証明書を発行する。

【0027】

図 1 に示すように、契約支援システム 20 には、申請書送付依頼受付サーバ 21 及び原本性確保電子文書保存装置としての原本性確保サーバ 22 が備えられ、インターネット 50 を介して契約法人のユーザ端末 60 に接続されている。さらに、契約支援システム 20 には、登録局（RA: Registration Authority）25 が設けられ、この登録局 25 には、RA 登録業務サーバ 26 が備えられている。この RA 登録業務サーバ 26 は、発行局（IA: Issuing Authority）30 に備えられた IA 業務サーバ 31 に接続されている。そして、IA 業務サーバ 31 は、リポジトリ 40 に接続されており、このリポジトリ 40 は、インターネット 50 を介して、ユーザ端末 60 に接続されている。そして、本実施形態では、登録局（RA: Registration Authority）25、発行局（IA: Issuing Authority）30 及びリポジトリ 40 が、認証局（CA: Certification Authority）を構成する。

40

【0028】

申請書送付依頼受付サーバ 21 は、申請者情報記憶部 23 を備えている。そして、申請書

50

送付依頼受付サーバ２１は、ユーザ端末６０から送信された電子証明書の発行申請書の送付依頼情報を受信して、申請者情報記憶部２３に保存する。このため、申請書送付依頼受付サーバ２１は、図示しない制御手段（ＣＰＵ）、記憶手段（ＲＡＭ、ＲＯＭ、ハードディスク等）、通信手段等を備えている。

【００２９】

原本性確保サーバ２２は、電子文書の原本性を確保して保管するための諸機能を有している。この原本性確保サーバ２２は、原本データを記憶する原本データ記憶部２４を備えている。この原本性確保サーバ２２は、図示しない制御手段（ＣＰＵ）、記憶手段（ＲＡＭ、ＲＯＭ、ハードディスク等）、通信手段等を備えている。

【００３０】

登録局２５は、ＲＡ認証業務とＲＡ登録業務とを行う。ＲＡ認証業務は、電子証明書の利用申込に係る申込受付、審査及び発行承認と、電子証明書の失効申請の受付、審査及び承認に関する業務を含む。ＲＡ登録業務は、ＩＡ業務への電子証明書の発行依頼、電子証明書と利用者署名鍵とが格納されたＩＣカードの利用者への送付、ＩＡ業務への電子証明書の発行依頼等に関する業務を含む。

【００３１】

ＲＡ登録業務サーバ２６は、利用者の鍵ペア（利用者署名鍵と利用者署名検証鍵）をＩＣカード内で生成させ、ＩＡ業務サーバ３１に対して電子証明書の発行指示を行う。そして、ＲＡ登録業務サーバ２６は、ＩＡ業務サーバ３１から受信した電子証明書をＩＣカードに格納する。また、ＲＡ登録業務サーバ２６は、電子証明書の失効についての入力に従って、ＩＡ業務サーバ３１に対して電子証明書の失効指示を行う。このため、ＲＡ登録業務サーバ２６は、図示しない制御手段（ＣＰＵ）、記憶手段（ＲＡＭ、ＲＯＭ、ハードディスク等）、通信手段等を備えている。ＲＡ登録業務サーバ２６は、証明書発行対象者データ記憶部２７を備えている。この証明書発行対象者データ記憶部２７には、電子証明書の発行対象者に関するデータが記録される。

【００３２】

発行局３０は、電子認証局の鍵の管理、ＲＡ業務からの要求に従った電子証明書の発行、失効等のＩＡ業務を行う。

ＩＡ業務サーバ３１は、ＲＡ登録業務サーバ２６からの電子証明書の発行指示に従って電子証明書を生成し、その電子証明書をＲＡ登録業務サーバ２６に送信する。また、ＲＡ認証業務に基づく失効指示に従って電子証明書の失効を行い、証明書廃棄リスト（ＣＲＬ：Certificate Revocation List）をリポジトリ４０に登録する。このため、ＩＡ業務サーバ３１は、図示しない制御手段（ＣＰＵ）、記憶手段（ＲＡＭ、ＲＯＭ、ハードディスク等）、通信手段等を備えている。

【００３３】

発行局３０は、保管情報記憶部３２を備えている。この保管情報記憶部３２には、電子証明書３３及びその作成に関する記録、本認証局についての認証局証明書であるＣＡ電子証明書３４、電子証明書の失効に関する情報及びその作成に関する記録等が記録される。

【００３４】

電子証明書３３は、電子証明書の発行申請に従って発行し、ＩＣカードに格納して申請を行った利用者に対して提供する電子証明書である。電子証明書３３は、電子証明書を発行した場合に記録される。ＣＡ電子証明書３４は、本認証局に対して発行した認証局証明書である。ＣＡ電子証明書３４は、本認証局に対してＣＡ電子証明書を発行した場合に記録される。このＣＡ電子証明書３４は、後述するように、リポジトリ４０にて公開される。

【００３５】

図２は、電子証明書３３のデータ構成を示す。電子証明書３３は、基本部３３１と拡張部３３２とから構成される。基本部３３１は、バージョン３３ａ、シリアル番号３３ｂ、署名アルゴリズム３３ｃ、発行者情報３３ｄ、有効期間情報３３ｅ、利用者情報３３ｆ、利用者署名検証鍵情報３３ｇに関するデータを含んで構成されている。拡張部３３２は、鍵の用途３３ｈ、基本制約３３ｉ、認証局鍵識別子３３ｊ、主体者鍵識別子３３ｋ、証明書

10

20

30

40

50

ポリシー 331、CRLのリポジトリ登録先 33mを含んで構成されている。

【0036】

バージョン 33aの領域には、X.509証明書のバージョンに関するデータが記録される。シリアル番号 33bの領域には、電子証明書を一意に識別するための番号に関するデータが記録される。署名アルゴリズム 33cの領域には、発行者が証明書に署名する際に用いるアルゴリズムに関するデータが記録される。本実施形態では、「`sha1withRSAEncryption`」を示すデータが記録される。発行者情報 33dは、発行者組織名、発行者認証業務名とを含む。発行者組織名領域には、証明書を発行した発行者の組織名に関するデータが記録される。本実施形態では、本認証局の組織名を示すデータが記録される。発行者認証業務名領域には、発行者の認証業務名に関するデータが記録される。本実施形態では、本認証局の認証業務名を示すデータが記録される。有効期間情報 33eは、電子証明書の有効期間の開始日と終了日とを含む。開始日領域には、電子証明書の有効期間の開始日（時刻）に関するデータが記録される。終了日領域には、電子証明書の有効期間の終了日（時刻）に関するデータが記録される。なお、本実施形態では、電子証明書の有効期間は3年間である。

10

【0037】

利用者情報 33fは、利用者国名、利用者組織名、利用者認証局名、利用者契約法人の商号、利用者所属部署名、利用者役職名及び利用者固有名称を含む。利用者国名領域には、利用者の国名に関するデータが記録される。本実施形態では、「日本国」を示す「JP」が記録される。

20

【0038】

利用者組織名領域には、本認証局の運用組織名として発行者組織名と同様のデータが記録される。本実施形態では、本認証局の組織名を示すデータが記録される。なお、組織名の証明は電子署名法の認定制度における認定の対象外である。

【0039】

利用者認証局名領域には、本認証局の名称として発行者認証業務名と同様のデータが記録される。本実施形態では、本認証局の認証業務名を示すデータが記録される。なお、認証局名の証明は電子署名法の認定制度における認定の対象外である。

【0040】

利用者契約法人の商号領域には、利用者の属性情報として、利用者の契約法人の商号のアルファベット表記に関するデータが記録される。具体的には、「`Company - 契約法人の商号（アルファベット表記）`」のように記録される。この利用者契約法人の商号は、利用者の発行申請書に記載された契約法人の商号を電子証明書に転記する。なお、契約法人の商号の証明は電子署名法の認定制度における認定の対象外である。

30

【0041】

利用者所属部署名領域には、利用者の属性情報として、利用者の契約法人における所属部署に関するデータが記録される。具体的には、「`Department - 所属部署名（アルファベット表記）`」のように記録される。この利用者所属部署名は、利用者の発行申請書に記載された所属部署名を電子証明書に転記する。なお、所属部署名の証明は電子署名法の認定制度における認定の対象外である。

40

【0042】

利用者役職名領域には、利用者の契約法人における役職に関するデータが記録される。具体的には、「`Title - 役職名（アルファベット表記）`」のように記録される。この利用者役職名は、利用者の発行申請書に記載された役職名を電子証明書に転記する。なお、役職名の証明は電子署名法の認定制度における認定の対象外である。

【0043】

利用者固有名称領域には、利用者の氏名に関するデータが記録される。この利用者の氏名は、発行申請書に記入されている利用者の日本語呼称のローマ字表記をそのまま転記する。なお、利用者の固有名称の証明は電子署名法の認定制度における認定の対象である。

【0044】

50

利用者署名検証鍵情報 3 3 g は、利用者署名検証鍵の暗号方式及び利用者署名検証鍵を含む。利用者署名検証鍵の暗号方式領域には、利用者署名検証鍵の暗号方式に関するデータが記録される。本実施形態では、「rsaEncryption」を示すデータが記録される。利用者署名検証鍵領域には、1024bit 以上の利用者署名検証鍵が記録される。

【0045】

鍵の用途 3 3 h の領域には、鍵の用途に関するデータとして、「digitalSignature, nonRepudiation」及び「KeyEncryption」を示すデータが記録される。なお、「digitalSignature」は、この鍵は認証の保証等の用途で一般データに署名するために使用できることを示す。「nonRepudiation」は、この鍵は後に否認できないメッセージに署名するために使用できることを示す。「KeyEncryption」は、この鍵はセッション鍵を交換するために使用できることを示す。基本制約 3 3 i の領域には、本電子証明書 3 3 の利用者が認証局ではないことを示すデータが記録される。認証局鍵識別子 3 3 j の領域には、CA 署名検証鍵の sha-1 ハッシュ値を設定する。主体者鍵識別子 3 3 k の領域には、利用者署名検証鍵の sha-1 ハッシュ値を設定する。証明書ポリシー 3 3 l の領域には、本認証局の認証局運営規定 (CPS: Certification Practice Statement) を公開した URL、電子署名法で認定された特定認証業務であることを示すデータ等が記録される。CRL のリポジトリ登録先 3 3 m の領域には、CRL を公開した URL に関するデータが記録される。

【0046】

図 3 は、CA 電子証明書 3 4 のデータ構成を示す。CA 電子証明書 3 4 は、基本部 3 4 1 と拡張部 3 4 2 とから構成される。基本部 3 4 1 は、バージョン 3 4 a、シリアル番号 3 4 b、署名アルゴリズム 3 4 c、発行者情報 3 4 d、有効期間情報 3 4 e、利用者情報 3 4 f、CA 署名検証鍵情報 3 4 g に関するデータを含んで構成されている。拡張部 3 4 2 は、鍵の用途 3 4 h、基本制約 3 4 i、認証局鍵識別子 3 4 j、主体者鍵識別子 3 4 k に関するデータを含んで構成されている。

【0047】

項目 3 4 a ~ 3 4 e の各領域には、項目 3 3 a ~ 3 3 e の各領域と同様のデータが記録される。なお、本実施形態では、CA 電子証明書の有効期間は 10 年間である。

【0048】

利用者情報 3 4 f は、利用者組織名と利用者名称とを含む。利用者組織名領域には、発行者情報 3 4 d の発行者組織名と同様のデータが記録される。本実施形態では、本認証局の組織名を示すデータが記録される。利用者名称領域には、発行者情報 3 4 d の発行者認証業務名と同様のデータが記録される。本実施形態では、本認証局の認証業務名を示すデータが記録される。

【0049】

CA 署名検証鍵情報 3 4 g は、CA 署名検証鍵の暗号方式及び CA 署名検証鍵を含む。CA 署名検証鍵の暗号方式領域には、CA 署名検証鍵の暗号方式に関するデータが記録される。本実施形態では、「rsaEncryption」を示すデータが記録される。CA 署名検証鍵領域には、1024bit 以上の本認証局の CA 署名検証鍵が記録される。

【0050】

鍵の用途 3 4 h の領域には、鍵の用途に関するデータとして、「KeyCertSign, cRLSign」を示すデータが記録される。なお、「KeyCertSign」は、当該鍵は証明書に署名するために使用できることを示す。「cRLSign」は、当該鍵は CRL に署名するために使用できることを示す。基本制約 3 4 i の領域には、本 CA 電子証明書 3 4 の利用者が認証局であることを示すデータが記録される。認証局鍵識別子 3 4 j の領域には、CA 署名検証鍵の sha-1 ハッシュ値を設定する。主体者鍵識別子 3 4 k の領域には、本認証局の CA 署名検証鍵の sha-1 ハッシュ値を設定する。

【0051】

リポジトリ40は、利用者や署名検証者等に対する情報を提供することを目的に失効情報等を保管するWebサーバの総称である。リポジトリ40は、検証者が電子証明書の有効性を検証できるようにCRLを常時公開する。具体的には、リポジトリ40は、CRL記憶部41を備えており、IA業務サーバ31から通知されたCRLをCRL記憶部41に保存し、これを公開する。また、リポジトリ40は、CPS及びCA電子証明書を公開する。このため、リポジトリ40は、図示しない制御手段(CPU)、記憶手段(RAM、ROM、ハードディスク等)、通信手段等を備えている。

【0052】

CRL記憶部41には、図4に示すように、失効した電子証明書についてのCRL410が記録されている。CRL410は、バージョン、署名アルゴリズム、発行者情報、今回更新日時、次回更新日時、失効される電子証明書のシリアル番号、失効日時、理由コード及び認証局鍵識別子に関するデータを含んで構成されている。 10

【0053】

バージョンデータ領域には、CRLのバージョンに関するデータが記録される。署名アルゴリズム領域には、CRL発行者の署名アルゴリズムの識別子に関するデータが記録される。本実施形態では、「sha1withRSAEncryption」を示すデータが記録される。

【0054】

発行者情報は、発行者組織名、発行者認証業務名とを含む。発行者組織名領域には、CRL発行者の組織名に関するデータが記録される。本実施形態では、本認証局の組織名を示すデータが記録される。発行者認証業務名領域には、CRL発行者の認証業務名に関するデータが記録される。本実施形態では、本認証局の認証業務名を示すデータが記録される。 20

【0055】

今回更新日時領域には、CRL記憶部41の更新が行われた日時に関するデータが記録される。次回更新日時領域には、次回、CRL記憶部41の更新を行う予定の日時に関するデータが記録される。失効される電子証明書領域には、失効される電子証明書のシリアル番号に関するデータが記録される。失効日時領域には、その電子証明書の失効日時が記録される。理由コード領域には、その電子証明書の失効の理由を示すコードが記録される。 30
認証局鍵識別子領域には、認証局公開鍵のsha-1ハッシュ値に関するデータが記録される。

【0056】

ユーザ端末60は、契約法人の従業員である契約支援システム20の利用者が使用するコンピュータ端末である。このユーザ端末60は、電子証明書の申請書の送付を申し込む場合や、契約支援システム20の利用者が、他の契約法人の担当者との間で契約の締結のための処理を行う場合に使用される。このため、ユーザ端末60は、ネットワークを介してデータを送信する機能や、受信したデータを表示する機能等を有する。また、このユーザ端末60は、図示しないCPU、RAM、ROMの他、キーボード、マウス等の入力手段、ディスプレイ等の出力手段、モデム等の通信手段等を有する。また、ユーザ端末60には、ICカード読み取り装置が接続されている。 40

【0057】

次に、上記のように構成されたシステムを用いて、契約支援業務を行う場合の手順を説明する。以下、電子証明書発行処理と、電子証明書の失効処理と、契約支援処理とに分けて説明する。

【0058】

(電子証明書発行処理)

まず、電子証明書を発行する場合の処理手順を図5を用いて説明する。契約支援サービスでは、契約支援サービスの提供を受けることを契約している契約企業に所属する個人(利用者)に対して電子証明書を発行する。

【0059】

図5に示すように、利用者は、ユーザ端末60を用いて、インターネット50を介して申請書送付依頼受付サーバ21にアクセスする。申請書送付依頼受付サーバ21は、電子証明書の発行申請のためのウェブページ（証明書発行申請画面）をユーザ端末60に送信し、利用者は、その証明書発行申請画面において、利用者情報を入力する。具体的には、利用者情報には、利用者の所属する企業、利用者の氏名等に関する情報が含まれる。そして、ユーザ端末60は、入力された利用者情報を申請書送付依頼受付サーバ21に送信する（ステップS1-1）。申請書送付依頼受付サーバ21は、この利用者情報を申請者情報記憶部23に記録する（ステップS1-2）。そして、申請書送付依頼受付サーバ21は、R A認証業務担当者に、利用者情報の登録が行われた旨の電子メールを送信して、電子証明書の発行申請を受け付けた旨を通知する（ステップS1-3）。 10

【0060】

この通知を受けたR A認証業務担当者は、事実確認の照会書、照会書受領書、電子証明書発行申請書及び利用者規約を利用者の自宅住所宛に本人限定受取郵便にて送付する（ステップS1-4）。

【0061】

電子証明書発行申請書は、利用者情報記入欄と利用者所属確認欄とを含む。利用者情報記入欄は、発行申請日、利用者氏名（カナ、漢字、ローマ字）、利用者押印、自宅住所、生年月日、電話番号、電子メールアドレス、勤務先、所属部署名及び役職名を含む。ここで、勤務先、所属部署名及び役職名については、英文又はローマ字表記と漢字との双方を記載する。利用者所属確認欄は、利用者所属確認日、法人名、代表者氏名及び代表者印を含む。利用者所属確認欄には、利用者が所属する契約法人の代表者が記入、押印することで、利用者が契約法人に所属していることを本認証局に保証する。ここで、代表者印には、代表者の印鑑登録証明書の印鑑と同じ印鑑を用いる。 20

【0062】

そして、利用者は、必要事項を記入した申請書類（発行申請書、住民票の写し、照会書受領書、商業登記簿謄本及び法人代表者の印鑑登録証明書）を登録局25に提出する（ステップS1-5）。住民票の写しは、利用者の居住所を証明する書類として提出が必須である。なお、日本国籍を持たない外国人については住民票の写しに代えて登録原票記載事項証明書を用いる。照会書受領書は、本人限定受取郵便により利用者に送付された申請の事実を確認する照会書に対する受領書として、利用者の本人性の確認のために提出が必須である。商業登記簿謄本は、法人の実在性の確認のために提出が必須である。法人代表者の印鑑登録証明書は、法人代表者による利用者の所属証明の意思確認のために提出が必須である。 30

【0063】

申請書類を受領した登録局25は、証明書発行書類の審査を行う（ステップS1-6）。具体的には、まず、R A認証業務担当者が一次審査を行う。ここでは、R A認証業務担当者が、必要書類の確認、照会書受領書の確認、利用者規約の確認、住民票との住所の照合、企業代表者印・企業名の電子契約サービス契約書の確認を行う。ここで、発行申請書類がすべて提出されていること、記入漏れがないこと、住民票の写しが発行日から3か月以内であること、及び、利用者の自筆署名及び利用者の印が押印されていることにより、利用者の意思を確認する。また、住民票の写しを用いて、電子証明書発行申請書に記載されている氏名及び住所が住民票の写しに記載されている氏名及び住所と同一であることを確認することにより、利用者の実在性を確認する。また、本人限定郵便に対する照会書受領書を用いて、利用者の本人性を確認する。 40

【0064】

契約法人への所属確認は、以下のようにして行う。すなわち、発行申請書に記載されている法人の商号、法人代表者名が、添付された商業登記簿謄本に記載されている法人の商号、法人代表者名と同一であることを確認する。また、発行申請書に押印されている契約法人の代表者印の印影と、添付された印鑑登録証明書の印影とを照合し、同じであることを 50

確認する。さらに、発行申請書に記載された法人の商号が契約支援サービスの利用契約法人であることを確認する。

【0065】

R A 認証業務担当者による一次審査を通過した発行申請については、R A 認証業務責任者が二次審査として再審査を行う。そして、二次審査の終了後、R A 認証業務責任者は、その発行申請を承認する。発行申請が承認された場合、R A 認証業務担当者は、証明書発行準備を行う。具体的には、R A 認証担当者が証明書発行対象者リストを作成し、証明書発行対象者データを作成して記録媒体に記録する。さらに、R A 認証業務担当者は、利用者名及び企業名を記述した I C カードを準備して、その I C カード、証明書発行対象者データを記録した記録媒体、及び、証明書発行対象者リストを安全に R A 登録業務担当者のもとに搬送する。 10

【0066】

R A 登録業務担当者は、これらを受け取ると、電子証明書発行のための作業を行う（ステップ S 1 - 7）。まず、R A 登録業務担当者は、電子証明証書発行準備作業を行う。具体的には、R A 登録業務担当者は、証明書発行対象者データを記録した記録媒体、I C カード等を確認し、記録媒体に記録された証明書発行対象者データを R A 登録業務サーバ 2 6 に登録するための作業を行う。

【0067】

R A 登録業務サーバ 2 6 は、証明書を発行対象者についての証明書発行対象者データを証明書発行対象者データ記憶部 2 7 に登録する（ステップ S 1 - 8）。さらに、R A 登録業務サーバ 2 6 は、I C カードを活性化させる P I N を生成し、利用者以外が容易に知り得ない方法で印刷する。 20

【0068】

次に、R A 登録業務担当者は、R A 登録業務サーバ 2 6 に接続された端末の表示手段に表示される発行指示画面にて P I N 等を入力して電子証明書の発行指示を行う。これに応じて、R A 登録業務サーバ 2 6 は、I C カード内で利用者鍵ペア（利用者署名鍵と利用者署名検証鍵）を生成させる（ステップ S 1 - 9）。そして、R A 登録業務サーバ 2 6 は、生成した利用者署名検証鍵と電子証明書記載情報とを電子証明書発行リクエストファイルに変換し、証明書発行依頼とともに I A 業務サーバ 3 1 に送信する（ステップ S 1 - 1 0）。 30

【0069】

これを受信した I A 業務サーバ 3 1 は、電子証明書を生成し（ステップ S 1 - 1 1）、その電子証明書を R A 登録業務サーバ 2 6 に返信する（ステップ S 1 - 1 2）。電子証明書を受信した R A 登録業務サーバ 2 6 は、I C カード内に電子証明書を格納する（S 1 - 1 3）。そして、R A 登録業務サーバ 2 6 は、P I N と証明書発行対象者データ記憶部 2 7 に記録した証明書発行対象者データとを削除する。

【0070】

R A 登録業務担当者及び R A 登録業務責任者は、P I N を利用者以外が容易に知り得ない安全な方法で印刷した印刷物を配達記録郵便で利用者本人に送付する。また、I C カードと受領書とを本人限定受取郵便を使用して郵送する（ステップ S 1 - 1 4）。 40

【0071】

これらを受領した利用者は、I C カード内の電子証明書と利用者署名鍵とを確認し（ステップ S 1 - 1 5）、受領書に記入をして登録局 2 5 に送付する（ステップ S 1 - 1 6）。これを受け取ると、R A 認証業務担当者は、受領書の受領を記録する（ステップ S 1 - 1 7）。

【0072】

（電子証明書の失効処理）

次に、電子証明書を失効させる場合の処理手順を説明する。本実施形態の契約支援サービスは、契約法人に所属する個人である利用者について、その利用者の所属する契約法人の商号、その利用者の所属部署、及び、利用者の役職名についても、電子証明書に含まれる 50

。そして、これらの情報は、電子証明書の発行時に、商業登記簿謄本を用いて法人の実在性を確認し、法人代表者の印鑑登録証明書を用いて、法人代表者による利用者の所属証明の意思確認を行ったものである。このため、この契約支援サービスにおいては、電子証明書における利用者の所属する契約法人の商号、その利用者の所属部署、及び、利用者の役職名は、保証されたものとなっている。

【0073】

しかし、利用者の所属部署や利用者の役職名は、電子証明書の有効期間が終了する前に変更される可能性が高い。また、電子証明書の有効期間が経過する前に、利用者がその契約法人に所属しなくなる場合もある。このような場合は、電子証明書の記載事項が変更された場合に該当するため、電子証明書を失効させる必要がある。

10

【0074】

利用者の所属部署や利用者の役職名が変更になった場合や利用者が契約法人に所属しなくなった場合には、利用者又は契約法人は、登録局25に対し、電子証明書の失効申請を行う。利用者本人が失効申請を行う場合、電子証明書の失効申請書には、その利用者の氏名、住所、生年月日、利用者の氏名のローマ字表記、契約法人の商号、利用者の署名及び押印、失効の理由等が含まれる。契約法人が失効申請を行う場合、電子証明書の失効申請書には、契約法人の連絡担当者の氏名、連絡先、利用者の氏名及びそのローマ字表記、契約法人の商号、契約法人の代表者名、契約法人代表者の押印、失効申請の理由等が含まれる。

【0075】

失効申請書を受領すると、RA認証業務は、複数人により失効申請者と失効申請書とを確認する。そして、RA認証業務は、失効申請者が利用者本人又は利用者が所属する契約法人であり、かつ、失効申請書の記述が適切である場合に失効を承認し、RA登録業務に失効指示を行う。RA登録業務は、RA認証業務の指示に従い、複数人の管理の下、専用端末で発行局30に対して失効指示を行う。発行局30は、正当なRA登録業務担当者からの失効指示であることを確認して、当該電子証明書を失効する。そして、失効処理が完了すると、当該利用者に失効通知を郵送する。

20

【0076】

そして、IA業務サーバ31は、CRL記憶部41を定期的（例えば、24時間毎）に更新し、CRL410をリポジトリ40で公開する。

30

（契約支援処理）

次に、契約企業の間で契約を行う場合の処理手順を図6～図8に従って説明する。ここでは、A社とB社との間で契約を締結する場合を想定する。

【0077】

まず、A社とB社との間で契約を締結する場合、インターネット50を介して、A社の担当者とB社の担当者との間で、電子契約書の記載内容について合意を得る。そして、A社の担当者が、A社のユーザ端末60において電子契約書を作成してPDF化するための作業を行う。これにより、ユーザ端末60は、電子契約書のPDFファイルを作成する（ステップS2-1）。そして、A社の担当者は、その電子契約書を原本性確保サーバ22にアップロードするための操作を行う。この場合、A社のユーザ端末60は、その電子契約書を原本性確保サーバ22にアップロードする（ステップS2-2）。原本性確保サーバ22は、この電子契約書を、原本性確保サーバ22の専用の電子署名を施して原本データ記憶部24に格納する（ステップS2-3）。

40

【0078】

次に、A社の担当者は、電子証明書の識別情報を用いて原本性確保サーバ22から電子契約書を取り出すための操作を行う。この場合、この担当者の使用するユーザ端末60は、原本性確保サーバ22に電子契約書の取り出し要求を送信する（ステップS2-4）。これに応じて、原本性確保サーバ22は、要求された電子契約書をそのユーザ端末60にダウンロードする（ステップS2-5）。

【0079】

50

そして、A社の担当者は、本認証局により発行された自分の電子証明書を用いて、電子契約書に表示される印影と連動した電子署名を施すための操作を行う。この場合、A社の担当者のユーザ端末60は、電子契約書に印影と連動させA社の担当者の電子署名を施す（ステップS2-6）。電子署名については、具体的には、電子契約書のダイジェストを生成し、そのダイジェストを、担当者の利用者署名鍵（秘密鍵）を用いて暗号化して電子署名を生成する。ここで、ダイジェストとは、一方向ハッシュ関数を使った演算により、もとのデータから生成した特定長（例えば、128ビット）のデータである。

【0080】

そして、A社の担当者は、その担当者の電子署名が施された電子契約書を原本性確保サーバ22にアップロードするための操作を行う。この場合、A社のユーザ端末60は、その担当者の電子署名が施された電子契約書を原本性確保サーバ22にアップロードする（ステップS2-7）。原本性確保サーバ22は、この電子契約書を、独自の電子署名を施して原本データ記憶部24に格納する（ステップS2-8）。 10

【0081】

そして、A社の担当者は、契約の相手方であるB社に、電子契約書への署名を依頼する旨の電子メールを送信するための操作を行う。この場合、A社のユーザ端末60は、B社のユーザ端末60に電子契約書への署名を依頼する旨の電子メールを送信する（ステップS2-9）。この依頼を受けたB社の担当者は、B社のユーザ端末60により、その電子契約書の識別情報を入力し、原本性確保サーバ22から電子契約書を取り出すための操作を行う。この場合、B社のユーザ端末60は、原本性確保サーバ22にアクセスし、その電子契約書の取り出し要求を行う（ステップS2-10）。これに応じて、原本性確保サーバ22は、その電子契約書をB社のユーザ端末60にダウンロードする（ステップS2-11）。これを受信すると、B社の担当者は、ダウンロードした電子契約書に付された電子署名について、電子証明書の有効性確認のための操作を行う。これにより、B社のユーザ端末60は、電子証明書の有効性確認処理を実行する（ステップS2-12）。 20

【0082】

この電子証明書の有効性確認処理において、まず、B社の担当者は、ダウンロードした電子契約書のファイルを開く。すると、図9に示す表示画面70が表示される。表示画面70の右側には、PDF形式の電子契約書72が表示される。この電子契約書72には、契約者甲として、A社の住所、法人名、代表者名の記載74と、A社の担当者の電子署名と連動した印影75とが表示される。また、契約者乙として、B社の住所、法人名、代表者名の記載76が表示される。この記載76の右側には、捺印欄77が設けられている。 30

【0083】

ここで、B社の担当者が、印影75をクリックすると、ユーザ端末60は、図8に示す電子証明書の有効性の確認処理を実行する。この処理では、まず、ユーザ端末60は、電子署名のチェックを実行する（ステップS3-1）。このチェック処理では、まず、B社のユーザ端末60は、電子証明書からA会社の担当者の利用者署名検証鍵（公開鍵）を抽出する。次に、B社のユーザ端末60は、この利用者署名検証鍵を用いて電子契約書に付された電子署名を復号化することにより、電子契約書のダイジェストを抽出する。次に、B社のユーザ端末60は、ダウンロードした電子契約書のダイジェストを生成する。そして、このダイジェストと電子署名から抽出したダイジェストとが一致するかどうかを確認する。ここで、生成したダイジェストと電子署名から抽出したダイジェストとが一致しない場合、電子契約書又は電子署名のいずれかが改竄されていることとなる。 40

【0084】

さらに、B社のユーザ端末60は、電子証明書の開始日及び終了日をチェックすることにより、電子証明書が有効期限内であるかどうかをチェックする。そして、電子契約書及び電子署名が改竄されておらず、電子証明書が有効期限内である場合、B社のユーザ端末60は、「署名は有効です。文書のこのバージョンは署名されてから変更されていません。」と表示する。なお、生成したダイジェストと電子署名から抽出したダイジェストとが一致しない場合、文書が変更されている旨が表示される。また、電子証明書の有効期限を経 50

過している場合、その旨が表示される。

【0085】

次に、B社のユーザ端末60は、利用者のチェック処理を行う（ステップS3-2）。このチェック処理では、まず、B社のユーザ端末60は、電子証明書の利用者のチェックを促すメッセージと、利用者に問題がない場合にその旨を入力するための利用者確認ボタンとを有するウィンドウを表示する。これに応じて、B社の担当者は、電子証明書の利用者をチェックする。具体的には、B社の担当者は、まず、表示画面70において署名の表示を選択する。これにより、表示画面70の左側のフレームに電子証明書の内容を表示する署名表示画面71が表示される。ここで、A社の署名についての「署名A」をクリックすると、A社の担当者によってされた電子証明書の内容が表示される。ここで、電子署名を施したA社の担当者が利用者として利用者表示73が表示される。具体的には、利用者の表示として、A社の担当者の電子証明書の利用者契約法人の商号、利用者所属部署名、利用者役職名及び利用者固有名称に基づいて、契約法人の商号、所属部署名、役職名及び氏名がそれぞれ表示される。ここでは、契約法人の商号として「XXXX COMPANY, LTD.」が表示される。この「XXXX COMPANY, LTD.」は、記載74に法人名として表示されるA社の商号「〇〇株式会社」のアルファベット表記である。また、ここでは、所属部署名として「Production division」が表示される。役職名として「Manager」が表示される。氏名として「Taroxxxxxx」が表示される。ここで表示される所属部署名、役職名及び氏名は、電子署名を施したA社の担当者の所属部署名、役職名及び氏名である。B社の担当者は、利用者表示73の契約法人の商号が、記載74の法人名のアルファベット表記であることを確認することにより、電子契約書72の記載74の法人名として記載された法人の意思により電子署名がされたことを確認する。B社の担当者は、利用者表示73の所属部署名、役職名及び氏名を確認することにより、実際に電子署名を行ったA社の担当者の所属部署、役職名及び氏名を把握する。そして、これらの確認ができた場合、B社の担当者は、利用者に問題がない旨を上記の利用者確認ボタンを用いて入力する。

【0086】

次に、B社のユーザ端末60は、CA電子証明書のチェックのための処理を行う（ステップS3-3）。具体的には、B社のユーザ端末60は、CA電子証明書のチェックを促すメッセージと、CA電子証明書に問題がない場合にその旨を入力するためのCA電子証明書確認ボタンとを有するウィンドウを表示する。さらに、B社のユーザ端末60は、リポジトリ40にアクセスし、リポジトリ40に公開されているCA電子証明書を表示する。B社の担当者は、表示されたCA電子証明書に基づいて、電子証明書が改竄されていないことを確認する。そして、電子証明書が改竄されていないことが確認できた場合、B社の担当者は、その旨を上記の利用者確認ボタンを用いて入力する。

【0087】

次に、B社のユーザ端末60は、CRLによる電子証明書の破棄のチェックのための処理を行う（ステップS3-4）。具体的には、B社のユーザ端末60は、CRLによる電子証明書の破棄のチェックを促すメッセージと、電子証明書が破棄されていない場合にその旨を入力するための存在確認ボタンとを有するウィンドウを表示する。さらに、B社のユーザ端末60は、リポジトリ40のCRL記憶部41に記憶され公開されたCRL410を表示する。これに応じて、B社の担当者は、CRL410を参照して、A社の担当者の電子証明書についてのCRL410が公開されていないことを確認する。A社の担当者の電子証明書のCRL410が公開されていないことを確認した場合、B社の担当者は、電子証明書が破棄されていないことを確認した旨を上記の存在確認ボタンを用いて入力する。

【0088】

次に、B社のユーザ端末60は、電子契約書の内容の審査を促すための処理を行う（ステップS2-13）。具体的には、B社のユーザ端末60は、電子契約書の内容の審査を促す旨のメッセージと、電子契約書の内容を承認した旨を入力するための承認ボタンとを有

するウィンドウを表示する。これに応じて、B社の担当者は、電子契約書の内容の審査を行う。具体的には、B社の担当者は、表示画面70において電子契約書72の内容を審査する。そして、審査の結果、電子契約書72による契約を行ってよいと判断した場合、B社の担当者は、上記の承認ボタンを用いてその旨を入力する。

【0089】

次に、B社のユーザ端末60は、電子署名を促す旨のメッセージを出力する。これに応じて、B社の担当者は、本認証局により発行された自分の電子証明書を用いて、電子契約書に表示される印影と連動した電子署名を施すための操作を行う。これにより、B社の担当者のユーザ端末60は、電子契約書に、印影と連動したB社の担当者の電子署名を施す（ステップS2-14）。電子署名については、具体的には、電子契約書のダイジェストを生成し、そのダイジェストを、担当者の利用者署名鍵（秘密鍵）を用いて暗号化して電子署名を生成する。ここで、ダイジェストとは、一方向ハッシュ関数を使った演算により、もとのデータから生成した特定長（例えば、128ビット）のデータである。本実施形態では、電子署名を印影と連動させる。

【0090】

そして、B社の担当者は、その担当者の電子署名が施された電子契約書を原本性確保サーバ22にアップロードするための操作を行う。これにより、B社のユーザ端末60は、その担当者の電子署名が施された電子契約書を原本性確保サーバ22にアップロードする（ステップS2-15）。原本性確保サーバ22は、この電子契約書を、原本性確保サーバ22の専用の電子署名を施して原本データ記憶部24に格納する（ステップS2-16）。

【0091】

そして、B社の担当者は、A社に対して契約書に署名をした旨を電子メールにより通知するための操作を行う。これにより、B社のユーザ端末60は、契約書に署名をした旨を通知する電子メールをA社のユーザ端末60に送信する（ステップS2-17）。

【0092】

この通知を受けたA社の担当者は、ユーザ端末60により、原本性確保サーバ22から電子契約書を取り出すための操作を行う。A社のユーザ端末60は、原本性確保サーバ22にアクセスし、その電子契約書の識別情報を入力し、その電子契約書の取り出し要求を行う（ステップS2-18）。これに応じて、原本性確保サーバ22は、その電子契約書をA社のユーザ端末60にダウンロードする（ステップS2-19）。これを受信すると、A社の担当者は、ダウンロードした電子契約書に付された電子署名について、電子証明書の有効性確認のための操作を行う。これにより、A社のユーザ端末60は、電子証明書の有効性確認処理を実行する（ステップS2-20）。具体的には、A社のユーザ端末60は、上記の電子証明書の有効性確認処理と同様に、ステップS3-1～S3-4に従って、電子証明書の有効性を確認のための処理を実行する。そして、A社の担当者は、A社のユーザ端末60の表示に従って、電子証明書の有効性の確認を行う。

【0093】

そして、電子証明書の有効性が確認された場合、A社の担当者は、電子契約書の内容の審査を行う（ステップS2-21）。具体的には、A社の担当者は、表示画面70において電子契約書72の内容を審査する。

【0094】

B社の担当者の電子証明書の有効性が確認された場合、A社のユーザ端末60は、電子契約書の内容の審査を促すための処理を行う（ステップS2-21）。具体的には、A社のユーザ端末60は、電子契約書の内容の審査を促す旨のメッセージと、電子契約書の内容を承認した旨を入力するための承認ボタンとを有するウィンドウを表示する。これに応じて、A社の担当者は、電子契約書の内容の審査を行う。そして、審査の結果、電子契約書の内容に問題がないと判断した場合は、上記の承認ボタンを用いてその旨を入力する。

【0095】

これに応じて、A社のユーザ端末60は、契約が成立した旨を原本性確保サーバ22に通

知する。この通知を受けた原本性確保サーバ２２は、その時点で原本データ記憶部２４に格納されている電子契約書を契約成立時の原本として管理する。

【００９６】

以上、本実施形態によれば、以下に示す効果を得ることができる。

・ 上記実施形態では、電子証明書は、商業登記簿謄本に基づいて確認された電子証明書の申請者が所属する法人の商号に関する情報を含む。また、この電子証明書は、その法人の代表者の印鑑登録証明書により利用者についての法人の証明の意思が確認された利用者固有名称（利用者の氏名）に関する情報を含む。このため、法人が実在することが、商業登記簿謄本により証明される。また、法人の代表者により、その法人に利用者が所属していることが証明されたことが確認される。そして、このような電子証明書を用いることで、個人に対して発行された電子証明書を用いて、その個人が所属する法人の商号に関する情報を証明できる。従って、法人から権限を委譲された個人に対して発行された電子証明書を用いて、その法人の意思を証明できる。

10

【００９７】

・ 上記実施形態では、発行申請書は、法人における申請者が所属する部署名、又は、法人における申請者の役職名に関する記載を含む。そして、電子証明書は、発行申請書の部署名に関する記載に基づく法人における申請者が所属する部署名に関する情報、又は、発行申請書の役職名に関する記載に基づく法人における申請者の役職名に関する情報を含む。このため、電子証明書を発行された個人が所属する部署名、又は、その個人の役職名に関する情報として、その個人が所属する法人によって承認された情報を電子証明書に記載することができる。従って、電子証明書に記載された部署名又は役職名に関する情報を確認することで、電子証明書の所有者である個人が所属する部署名、又は、その個人の役職名を確認できる。

20

【００９８】

・ 上記実施形態では、Ａ社の担当者の電子証明書を用いたＡ社の担当者の電子署名が施された電子文書を原本性確保サーバ２２に保管する。そして、その電子文書をＢ社の担当者のユーザ端末６０にダウンロードし、Ｂ社の担当者のユーザ端末６０が、Ａ社の担当者の電子証明書におけるＡ社の担当者が所属する法人の商号（Ａ社の商号）に関する情報を利用者表示７３に表示する。このため、Ｂ社の担当者は、Ａ社の担当者が所属する法人の商号（Ａ社の商号）に関する情報を確認できる。従って、Ｂ社の担当者は、Ａ社の担当者が所属する法人（Ａ社）から権限を委譲されたＡ社の担当者に対して発行された電子証明書により、電子文書が、Ａ社の担当者が所属する法人（Ａ社）の意思によるものことを確認できる。また、同様にして、Ａ社の担当者は、Ｂ社の担当者が所属する法人（Ｂ社）から権限を委譲されたＢ社の担当者に対して発行された電子証明書により、電子文書が、Ｂ社の担当者が所属する法人（Ｂ社）の意思によるものことを確認できる。

30

【００９９】

・ 上記実施形態では、Ｂ社の担当者のユーザ端末６０は、Ａ社の担当者の電子証明書におけるＡ社の担当者が所属する部署に関する情報又はＡ社の担当者の役職名に関する情報を利用者表示７３に表示する。このため、Ｂ社の担当者は、Ａ社の担当者の電子証明書に記載された部署名又は役職名に関する情報を確認することで、Ａ社の担当者が所属する部署名、又は、Ａ社の担当者の役職名を確認できる。また、同様にして、Ａ社の担当者は、Ｂ社の担当者の電子証明書に記載された部署名又は役職名に関する情報を確認することで、Ｂ社の担当者が所属する部署名、又は、Ｂ社の担当者の役職名を確認できる。

40

【０１００】

・ 上記実施形態では、電子契約書を原本性確保サーバ２２にアップロードし、電子署名を行う法人の担当者は、原本性確保サーバ２２から電子証明書を取り出して、電子署名を施す。このため、インターネット５０を介して電子契約書により契約を締結することが可能となり、文書作成から契約の締結までの効率を上げることができる。また、電子文書の原本性を確保して保存できる原本性確保サーバ２２にて電子契約書を保管することで、電子契約書を安全に保管できる。さらに、紙の契約書を使用しないため、紙の契約書を保管

50

する場所が不要となる。

【0101】

・ 上記実施形態では、電子契約書には、PDF形式のファイルを用い、電子契約書の表示において電子署名と連携した印影を表示させる。このため、紙の契約書と同様に視覚される電子契約書を用いることが可能となる。また、PDF形式のファイルを用いることで、電子媒体に保存された内容を必要に応じて肉眼で見読可能な状態にすることが可能となる。

【0102】

・ 上記実施形態では、利用者が電子証明書に記載の法人に所属しなくなった場合や、部署や役職名が変更になった場合には、利用者又は契約法人からの通知に基づいて電子証明書 10
を失効し、CRL410を公開する。このため、検証者は、CRL410により電子証明書が破棄されていないことを確認することにより、使用されている電子証明書が破棄されたものでないことを確認できる。

【0103】

・ 上記実施形態では、電子署名法における特定認証業務の認定の要件を満たすとともに、電子証明書に記載する固有名称（氏名）を除く利用者の属性（契約法人の商号、所属部署名、役職名）を証明する。このため、電子署名法による認定要件を満たすことが可能となり、特定認証業務の認定を受けることで、電子証明書を実印と同等の扱いを受けることが可能となる。

【0104】

・ 上記実施形態では、ユーザ端末60が、電子署名のチェック、電子証明書の利用者のチェック、CA電子証明書の利用者のチェック、CRLによる電子証明書の破棄のチェックを促すためのメッセージを出力する。このため、検証者は、そのメッセージに従って、電子契約書を取り交わした相手と電子契約書の内容を確認できる。

【0105】

なお、上記実施形態は、以下の態様に変更してもよい。

・ 上記実施形態では、法人間で電子契約書により契約を締結する場合について本発明を具体化した。本発明はこれに限られるものではなく、法人の意思を確認しながら、その法人に所属する利用者による電子署名を許容する場合であれば、他の場面で使用してもよい。このようにすることで、法人に対する電子証明書を使用するまでもない場合について、 30
法人に所属する個人に対する電子証明書を用いて法人の意思を確認することができ、法人の意思を明確にしながら複数の電子証明書を使用できる。

【0106】

・ 上記実施形態では、検証者が、CA電子証明書の内容の確認、CRLの確認を行ったが、これらの確認を自動化してもよい。このようにすることで、人間による確認のミスを防止できる。

【0107】

【発明の効果】

以上詳述したように、本発明によれば、法人から権限を委譲された個人の電子証明書を用いて、その法人の意思を証明できる。

【図面の簡単な説明】

【図1】 本発明の一実施形態のシステム概略図。

【図2】 電子証明書の説明図。

【図3】 CA電子証明書の説明図。

【図4】 CRL記憶部に記憶されたデータの説明図。

【図5】 本発明の一実施形態の処理手順の説明図。

【図6】 本発明の一実施形態の処理手順の説明図。

【図7】 本発明の一実施形態の処理手順の説明図。

【図8】 本発明の一実施形態の処理手順の説明図。

【図9】 ユーザ端末に表示される表示画面の説明図。

10

20

30

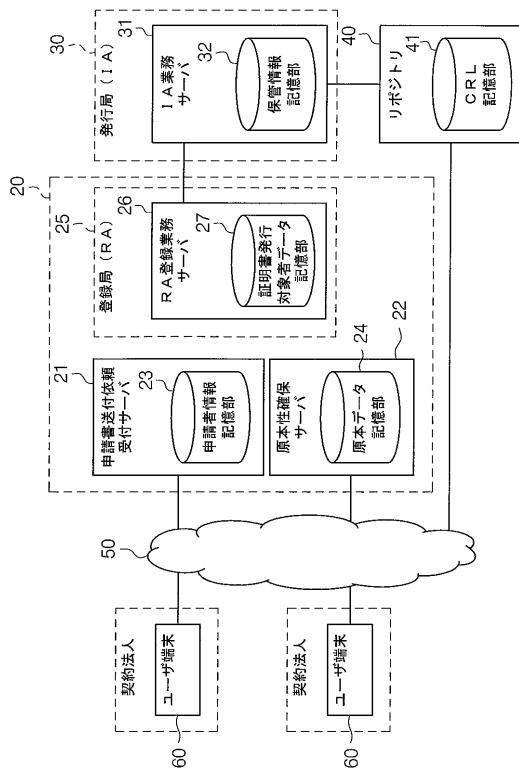
40

50

【符号の説明】

2 2 …コンピュータ及び原本性確保電子文書保存装置としての原本性確保サーバ、3 3 …電子証明書、7 5 …印影。

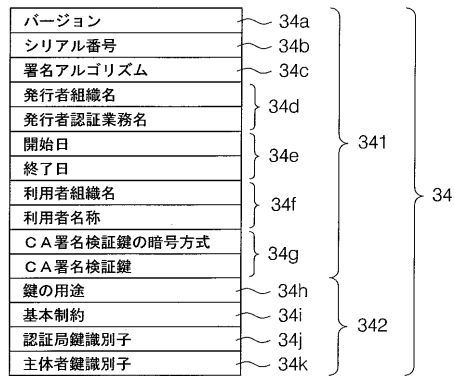
【図 1】



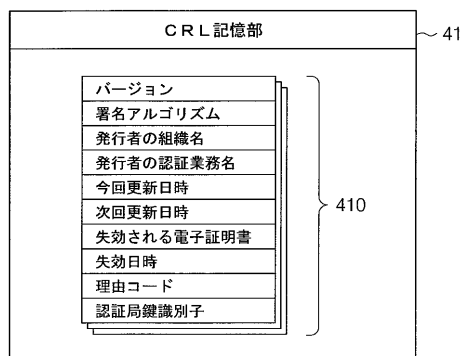
【図 2】

バージョン	33a	331	33
シリアル番号	33b		
署名アルゴリズム	33c		
発行者組織名	33d		
発行者認証業務名			
開始日	33e		
終了日			
利用者国名	33f		
利用者組織名			
利用者認証局名			
利用者契約法人の商号	33g		
利用者所属部署名			
利用者役職名			
利用者固有名称	33h		
利用者署名検証鍵の暗号方式			
利用者署名検証鍵	332		
鍵の用途			
基本制約			
認証局鍵識別子			
主体者鍵識別子			
証明書ポリシー			
CRLのリポジトリ登録先	33m		

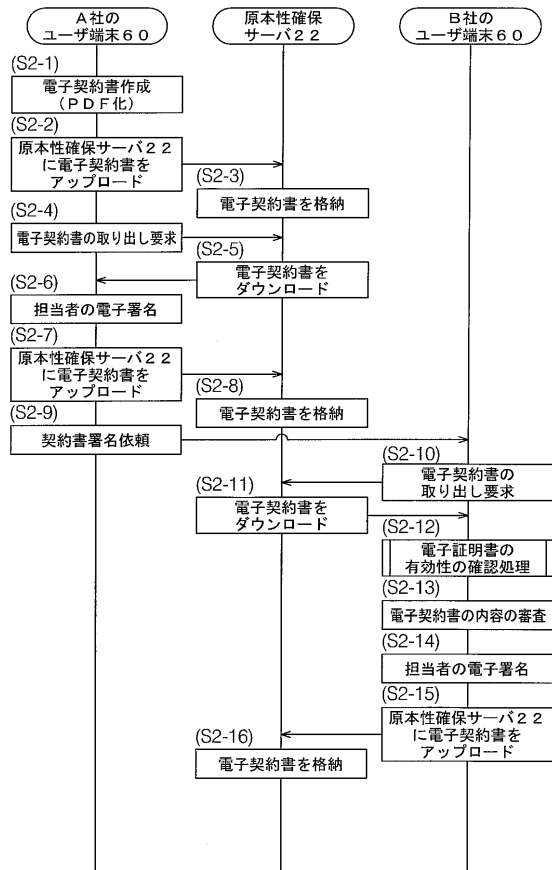
【図 3】



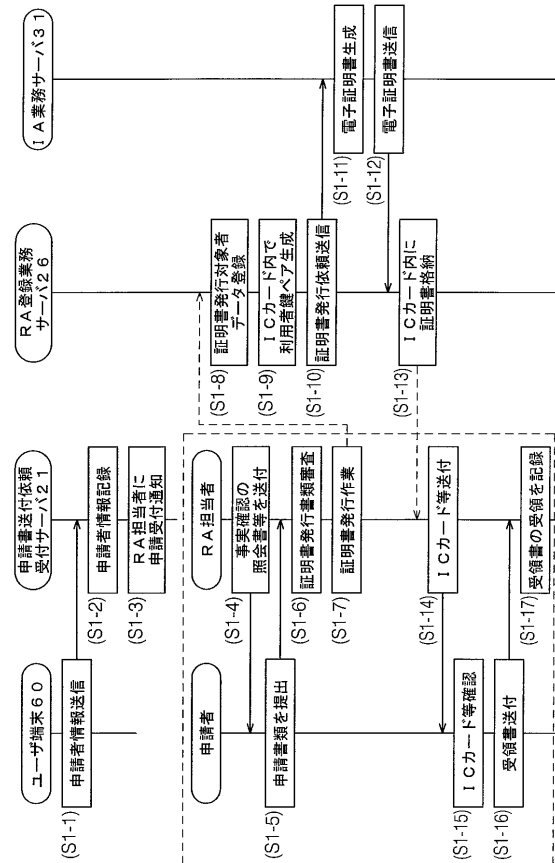
【図 4】



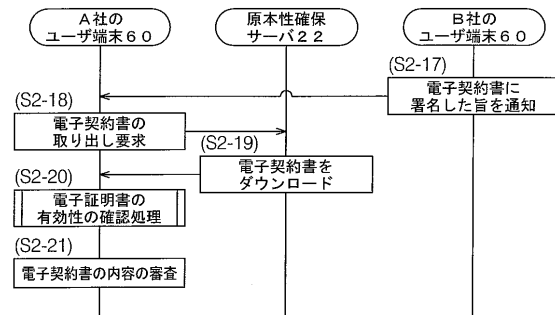
【図 6】



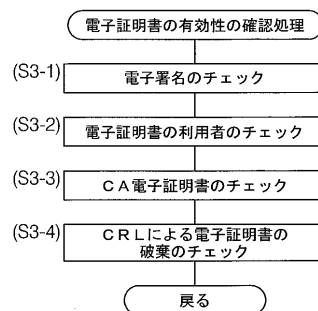
【図 5】



【図 7】



【図 8】



【図 9】

71	署名▼	署名A 契約法人の商号:XXXX COMPANY, LTD. 所属部署名:Production Division 役職名:Manager 氏名:Taro Xxxxxx
	署名▼	

70	72	<契約書>
----	----	--

71	署名▼	署名A 契約法人の商号:XXXX COMPANY, LTD. 所属部署名:Production Division 役職名:Manager 氏名:Taro Xxxxxx
----	-----	--

70	72	<契約書>
----	----	--

70	72	<契約書>
----	----	--

70	72	<契約書>
----	----	--

70	72	<契約書>
----	----	--

70	72	<契約書>
----	----	--

70	72	<契約書>
----	----	--

70	72	<契約書>
----	----	--

70	72	<契約書>
----	----	--

フロントページの続き

(72)発明者 前谷 英一郎

東京都中央区銀座7丁目16番3号 リコーリース 株式会社内

Fターム(参考) 5J104 EA05 PA10