

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第5166177号

(P5166177)

(45) 発行日 平成25年3月21日 (2013. 3. 21)

(24) 登録日 平成24年12月28日 (2012. 12. 28)

(51) Int. Cl.

F I

G 0 6 F 21/62 (2013. 01)

G 0 6 F 21/24 1 6 5 F

G 0 6 F 21/31 (2013. 01)

G 0 6 F 21/20 1 3 1 A

G 0 6 F 21/34 (2013. 01)

G 0 6 F 21/20 1 3 4

G 0 9 C 1/00 (2006. 01)

G 0 9 C 1/00 6 4 0 D

G 0 6 T 7/00 (2006. 01)

G 0 6 T 7/00 5 9 0

請求項の数 12 (全 20 頁)

(21) 出願番号 特願2008-229031 (P2008-229031)
 (22) 出願日 平成20年9月5日 (2008. 9. 5)
 (65) 公開番号 特開2010-61580 (P2010-61580A)
 (43) 公開日 平成22年3月18日 (2010. 3. 18)
 審査請求日 平成23年8月24日 (2011. 8. 24)

(73) 特許権者 000104652
 キヤノン電子株式会社
 埼玉県秩父市下影森 1 2 4 8 番地
 (74) 代理人 100076428
 弁理士 大塚 康徳
 (74) 代理人 100112508
 弁理士 高柳 司郎
 (74) 代理人 100115071
 弁理士 大塚 康弘
 (74) 代理人 100116894
 弁理士 木村 秀二
 (74) 代理人 100130409
 弁理士 下山 治
 (74) 代理人 100134175
 弁理士 永川 行光

最終頁に続く

(54) 【発明の名称】 認証処理装置、認証処理方法、管理サーバ装置、管理サーバ装置の制御方法

(57) 【特許請求の範囲】

【請求項 1】

認証処理装置であって、

前記認証処理装置に接続可能な電子デバイスの識別子により、前記認証処理装置の使用を許可する手段と、

前記電子デバイスの識別子と、印影画像を含む印影ファイルと、をセットにして保持する保持手段と、

前記電子デバイスが接続され且つ前記使用が許可されると、この接続された電子デバイスの識別子に対応する、前記保持手段に保持されている印影ファイルを取得する取得手段と、

前記取得手段が取得した印影ファイルに含まれている印影画像を、電子文書と合成する合成手段と

前記合成手段により得られた合成画像を出力する出力手段と

を備えることを特徴とする認証処理装置。

【請求項 2】

更に、

前記合成手段により得られた合成画像に対して、セキュリティ情報を付加する手段を備えることを特徴とする請求項 1 に記載の認証処理装置。

【請求項 3】

前記合成手段は、

前記電子文書を前記印影画像に合成可能な電子文書に変換する変換手段を備えることを特徴とする請求項 1 又は 2 に記載の認証処理装置。

【請求項 4】

更に、前記取得手段が取得した印影ファイルに含まれている印影画像を表示する表示手段を備えることを特徴とする請求項 1 乃至 3 の何れか 1 項に記載の認証処理装置。

【請求項 5】

前記合成手段は更に、前記合成手段による合成処理における時刻情報を押印時刻を示す情報として取得し、取得した時刻情報を前記合成画像に対して合成することを特徴とする請求項 1 乃至 4 の何れか 1 項に記載の認証処理装置。

【請求項 6】

10

更に、

前記印影画像を作成する作成手段と

前記作成手段により作成された印影画像を、前記印影ファイルに登録する登録手段とを備えることを特徴とする請求項 1 乃至 5 の何れか 1 項に記載の認証処理装置。

【請求項 7】

ユーザ端末装置と、管理サーバ装置と、で構成されている認証処理装置であって、

前記ユーザ端末装置は、

前記ユーザ端末装置に接続可能な電子デバイスの識別子により、前記ユーザ端末装置の使用を許可する手段と、

前記電子デバイスが接続され且つ前記使用が許可されると、前記電子デバイスの識別子を取得する取得手段と、

20

前記取得手段が取得した識別子を前記管理サーバ装置に送信する第 1 の送信手段と、

前記管理サーバ装置から、電子文書と、前記識別子に対応する印影画像と、が合成された画像を受信する手段と

を備え、

前記管理サーバ装置は、

前記ユーザ端末装置に接続可能な電子デバイスの識別子と、前記印影画像を含む印影ファイルと、をセットにして保持する保持手段と、

前記第 1 の送信手段により送信された識別子を受信し、受信した識別子とセットになって前記保持手段に保持されている印影ファイルを取得する取得手段と、

30

前記取得手段が取得した印影ファイルに含まれている印影画像を、前記電子文書と合成する合成手段と、

前記合成手段により得られた画像を前記ユーザ端末装置に送信する手段と

を備えることを特徴とする認証処理装置。

【請求項 8】

ユーザ端末装置に接続可能な電子デバイスの識別子により該ユーザ端末装置の使用を許可する前記ユーザ端末装置と、ネットワークを介して接続された管理サーバ装置であって、

前記電子デバイスの識別子と、印影画像を含む印影ファイルと、をセットにして保持する保持手段と、

40

前記電子デバイスの識別子を前記ユーザ端末装置から取得し、取得した識別子に対応する前記保持手段に保持されている印影ファイルを取得する取得手段と、

前記取得手段が取得した印影ファイルに含まれている印影画像と、電子文書と、を合成する合成手段と

前記合成手段により得られた画像を前記ユーザ端末装置に送信する手段と

を備えることを特徴とする管理サーバ装置。

【請求項 9】

認証処理装置が行う認証処理方法であって、

前記認証処理装置に接続可能な電子デバイスの識別子により、前記認証処理装置の使用を許可する工程と、

50

前記電子デバイスが接続され且つ前記使用が許可されると、前記電子デバイスの識別子と、印影画像を含む印影ファイルと、をセットにして保持する保持手段において、この接続された電子デバイスの識別子に対応する印影ファイルを取得する取得工程と、

前記取得工程で取得した印影ファイルに含まれている印影画像を、電子文書と合成する合成工程と

前記合成工程で得られた合成画像を出力する出力工程と

を備えることを特徴とする認証処理方法。

【請求項 10】

ユーザ端末装置に接続可能な電子デバイスの識別子により該ユーザ端末装置の使用を許可する前記ユーザ端末装置と、ネットワークを介して接続された管理サーバ装置の制御方法であって、

10

前記電子デバイスの識別子を前記ユーザ端末装置から取得し、前記電子デバイスの識別子と、印影画像を含む印影ファイルと、をセットにして保持する保持手段において、取得した識別子に対応する印影ファイルを取得する取得工程と、

前記取得工程で取得した印影ファイルに含まれている印影画像と、電子文書と、を合成する合成工程と

前記合成工程で得られた画像を前記ユーザ端末装置に送信する工程と

を備えることを特徴とする管理サーバ装置の制御方法。

【請求項 11】

コンピュータを、請求項 1 乃至 7 の何れか 1 項に記載の認証処理装置の各手段として機能させるためのコンピュータプログラム。

20

【請求項 12】

コンピュータを、請求項 8 に記載の管理サーバ装置の各手段として機能させるためのコンピュータプログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、印影画像を文章画像上に配置するための技術に関するものである。

【背景技術】

【0002】

30

パスワードやスマートカード、生体情報などを用いて認証を行う個人認証システムはすでに数多く存在している。しかし、そのようなシステムは概して認証による個人の特定や認証の自動化作業にとどまっており、認証を通過した後にその情報を活用するということとはあまり考えられていなかった。

【0003】

一方、日本では従来、印鑑が個人を特定するための道具として使用されている。印鑑はその所有者と結び付けられており、公的な文書においても間違いなく本人であることを証明する為に用いられている。近年では端末上で印鑑を使用する感覚で電子文書に印影画像を埋め込む電子印鑑システムも普及している。ただし、電子端末上では印影画像を偽造することが容易であるため、誰がその印影を埋め込んだかということが重要になる。しかし、従来の方法ではそれを識別する為に、押印するための個人を認証するパスワードの入力が必要であったり、タブレットに印鑑を模した特殊な専用デバイスを使用する必要があったりと、手軽に使用できるものではなかった。

40

【0004】

特許文献 1 には、利用者端末から電子印鑑を管理している管理端末にログインし、そこから印影画像と電子証明書を選択し、利用者端末上で電子文書上の任意の位置にそれを貼り付けるといったシステムが開示されている。

【0005】

特許文献 2 には、次のようなシステムが開示されている。即ち、データを一つのまとまりとして取り扱い可能な所定フォーマット形式に変換されている電子文書と、電子文書の

50

捺印領域情報とを管理している。そして、アプリケーションソフトを閉じた状態で、電子文書に印影データを対応付けて印影画像付きの電子文書を作成する。

【0006】

特許文献3には、次のような技術が開示されている。利用者端末に接続されたUSBメモリ装置に、電子文書上に添付するための印影画像と、印影画像を登録するための固有の登録番号と、を格納している。そして、固有の登録番号をキーにして、USBメモリに格納された印影画像を照合するために、サーバデータベースから、印影画像を取り出す。

【特許文献1】特開2003-169051号公報

【特許文献2】特開2007-304812号公報

【特許文献3】特開2005-352851号公報

10

【発明の開示】

【発明が解決しようとする課題】

【0007】

しかしながら、特許文献1、2に開示されているシステムでは、電子文書に電子印鑑を押印するために、利用者がユーザ名等、個人を特定できるユーザ情報を入力し、印影情報を取得する必要がある、という問題がある。

【0008】

また、特許文献3に開示されているシステムでは、USBメモリ装置に格納された登録番号をキーにしてサーバから印影画像を取り出せる。そのため、USBメモリ装置を保持する利用者の端末装置に限定されず、他の端末装置からでも簡単に印影画像を取得できる、という問題がある。

20

【0009】

本発明は以上の問題に鑑みてなされたものであり、セキュリティを確保しつつ、印鑑が押印された文書の電子データをより容易に取得するための技術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】

【0010】

本発明の目的を達成するために、例えば、本発明の認証処理装置は以下の構成を備える。

【0011】

30

即ち、認証処理装置であって、

前記認証処理装置に接続可能な電子デバイスの識別子により、前記認証処理装置の使用を許可する手段と、

前記電子デバイスの識別子と、印影画像を含む印影ファイルと、をセットにして保持する保持手段と、

前記電子デバイスが接続され且つ前記使用が許可されると、この接続された電子デバイスの識別子に対応する、前記保持手段に保持されている印影ファイルを取得する取得手段と、

前記取得手段が取得した印影ファイルに含まれている印影画像を、電子文書と合成する合成手段と

40

前記合成手段により得られた合成画像を出力する出力手段と

を備えることを特徴とする。

【0012】

本発明の目的を達成するために、例えば、本発明の認証処理装置は以下の構成を備える。

【0013】

即ち、ユーザ端末装置と、管理サーバ装置と、で構成されている認証処理装置であって、

、

前記ユーザ端末装置は、

前記ユーザ端末装置に接続可能な電子デバイスの識別子により、前記ユーザ端末装置

50

の使用を許可する手段と、

前記電子デバイスが接続され且つ前記使用が許可されると、前記電子デバイスの識別子を取得する取得手段と、

前記取得手段が取得した識別子を前記管理サーバ装置に送信する第1の送信手段と、
前記管理サーバ装置から、電子文書と、前記識別子に対応する印影画像と、が合成された画像を受信する手段と

を備え、

前記管理サーバ装置は、

前記ユーザ端末装置に接続可能な電子デバイスの識別子と、前記印影画像を含む印影ファイルと、をセットにして保持する保持手段と、

前記第1の送信手段により送信された識別子を受信し、受信した識別子とセットになって前記保持手段に保持されている印影ファイルを取得する取得手段と、

前記取得手段が取得した印影ファイルに含まれている印影画像を、前記電子文書と合成する合成手段と、

前記合成手段により得られた画像を前記ユーザ端末装置に送信する手段と

を備えることを特徴とする。

【0014】

本発明の目的を達成するために、例えば、本発明の管理サーバ装置は以下の構成を備える。

【0015】

即ち、ユーザ端末装置に接続可能な電子デバイスの識別子により該ユーザ端末装置の使用を許可する前記ユーザ端末装置と、ネットワークを介して接続された管理サーバ装置であって、

前記電子デバイスの識別子と、印影画像を含む印影ファイルと、をセットにして保持する保持手段と、

前記電子デバイスの識別子を前記ユーザ端末装置から取得し、取得した識別子に対応する前記保持手段に保持されている印影ファイルを取得する取得手段と、

前記取得手段が取得した印影ファイルに含まれている印影画像と、電子文書と、を合成する合成手段と

前記合成手段により得られた画像を前記ユーザ端末装置に送信する手段と

を備えることを特徴とする。

【0016】

本発明の目的を達成するために、例えば、本発明の認証処理方法は以下の構成を備える。

【0017】

即ち、認証処理装置が行う認証処理方法であって、

前記認証処理装置に接続可能な電子デバイスの識別子により、前記認証処理装置の使用を許可する工程と、

前記電子デバイスが接続され且つ前記使用が許可されると、前記電子デバイスの識別子と、印影画像を含む印影ファイルと、をセットにして保持する保持手段において、この接続された電子デバイスの識別子に対応する印影ファイルを取得する取得工程と、

前記取得工程で取得した印影ファイルに含まれている印影画像を、電子文書と合成する合成工程と

前記合成工程で得られた合成画像を出力する出力工程と

を備えることを特徴とする。

【0018】

本発明の目的を達成するために、例えば、本発明の管理サーバ装置の制御方法は以下の構成を備える。

【0019】

即ち、ユーザ端末装置に接続可能な電子デバイスの識別子により該ユーザ端末装置の使

10

20

30

40

50

用を許可する前記ユーザ端末装置と、ネットワークを介して接続された管理サーバ装置の制御方法であって、

前記電子デバイスの識別子を前記ユーザ端末装置から取得し、前記電子デバイスの識別子と、印影画像を含む印影ファイルと、をセットにして保持する保持手段において、取得した識別子に対応する印影ファイルを取得する取得工程と、

前記取得工程で取得した印影ファイルに含まれている印影画像と、電子文書と、を合成する合成工程と

前記合成工程で得られた画像を前記ユーザ端末装置に送信する工程と

を備えることを特徴とする。

【発明の効果】

10

【0020】

本発明の構成によれば、セキュリティを確保しつつ、印鑑が押印された文書の電子データをより容易に取得することができる。

【発明を実施するための最良の形態】

【0021】

以下、添付図面を参照し、本発明の好適な実施形態について説明する。なお、以下説明する実施形態は、本発明を具体的に実施した場合の一例を示すもので、特許請求の範囲に記載の構成の具体的な実施例の1つである。

【0022】

〔第1の実施形態〕

20

図1は、本実施形態に係るシステム（認証処理装置）の機能構成例を示すブロック図である。図1に示す如く、本実施形態に係るシステムは、管理サーバ装置1とユーザ端末装置6とで構成されており、それぞれは、LANなどのネットワーク10に接続されている。更にユーザ端末装置6には、認証デバイス5（電子デバイス）を接続することができる。

【0023】

管理サーバ装置1、ユーザ端末装置6は何れも、一般のパーソナルコンピュータであることを前提にしている。しかし、一般的なパーソナルコンピュータと同等以上、若しくはそれに準ずる演算処理能力を有する装置であれば、如何なる装置を管理サーバ装置1、ユーザ端末装置6に適用しても良い。

30

【0024】

先ず、ユーザ端末装置6について説明する。図1に示す如く、ユーザ端末装置6は、文書変換部7、押印位置指示部8、を有する。

【0025】

文書変換部7は、テキスト文書等の特定の形式に依存しないデータを、PDF等の画像情報を合成可能な文書データに変換する。

【0026】

押印位置指示部8は、文書変換部7により変換されたデータである電子文書において、押印する位置を指定し、指定した位置を示す情報を生成する。

【0027】

40

また、上述の取り、ユーザ端末装置6には、認証デバイス5が脱着可能に接続される。

【0028】

次に、管理サーバ装置1について説明する。図1に示す如く、管理サーバ装置1は、認証情報データベース2、電子印鑑データベース3、押印部4、管理データベース9を有する。

【0029】

認証情報データベース2には、認証デバイス5の識別子と、この認証デバイス5を操作するユーザのパスワードと、がセットになって登録されている（第2の保持）。なお、認証デバイス5を操作するユーザが複数人である場合、それぞれのユーザについてこのセットが認証情報データベース2に登録されていることになる。

50

【0030】

例えば、認証デバイスCを操作できるユーザとしてAさんとBさんの二人いた場合、認証デバイスCの識別子とAさんのパスワードのセットと、認証デバイスCの識別子とBさんのパスワードのセットとが、認証情報データベース2に登録されることになる。

【0031】

また、認証デバイス5が複数存在する場合には、それぞれの認証デバイス5についてこのセットが登録されていることになる。例えば、ユーザFが、認証デバイスDと、認証デバイスEとを所持している場合、認証デバイスDの識別子とFさんのパスワードのセットと、認証デバイスEの識別子とFさんのパスワードのセットとが、認証情報データベース2に登録されることになる。

10

【0032】

電子印鑑データベース3には、認証デバイス5の識別子と、複数の印影画像を含む印影ファイルと、がセットになって登録されている。

【0033】

なお、後述する管理データベース9に、印影画像のテンプレートを記憶させておき、ユーザ端末装置6からの入力情報とテンプレートとを合成することにより、印影画像を作成、登録することも可能である。

【0034】

例えば、ユーザ端末装置6において、ユーザの名前・部署名を入力し、その入力された名前・部署名（入力情報）と、テンプレートとを合成することで、ユーザの名前・部署名入りの、ユーザ固有の印影画像を作成することができる。

20

【0035】

更に、人事異動等により、ユーザの名前・部署名を修正したい場合、ユーザ端末装置6からの再入力情報により、ユーザ端末装置6からの再入力情報とテンプレートとを合成し、印影画像を修正、再登録することも可能である。

【0036】

また、電子印鑑データベース3に、認証デバイス5の識別子に対するユーザ名を予め登録しておき、登録されたユーザ名とテンプレートとを合成することにより、ユーザ名入りの印影画像を作成、登録することも可能である。

【0037】

30

また、管理サーバ装置1、またはユーザ端末装置6で計時されている日付・時刻情報を読み出し、読み出された日付・時刻情報と、テンプレートとを合成することも可能である。この場合、合成された印影画像は、読み出された日時・時刻情報が異なる毎に、修正、再登録されることは言うまでもない。

【0038】

押印部4は、ユーザ端末装置6から送信されてきた電子文書、押印位置情報、印影画像を受信すると、この電子文書上の、押印位置情報が示す位置に、この印影画像を配置する（押印する）ことで、印影が押印された電子文書を作成する。

【0039】

管理データベース9には、印影画像のテンプレート等、様々な情報を登録することができる。

40

【0040】

図5は、管理サーバ装置1、ユーザ端末装置6、に適用可能なコンピュータのハードウェア構成例を示すブロック図である。

【0041】

CPU51は、ROM52やRAM53に格納されているコンピュータプログラムやデータを用いてコンピュータ全体の制御を行う。本コンピュータを管理サーバ装置1に適用した場合、CPU51は、管理サーバ装置1が行うものとして後述する各処理を実行する。また、本コンピュータをユーザ端末装置6に適用した場合には、CPU51は、ユーザ端末装置6が行うものとして後述する各処理を実行する。

50

【0042】

ROM 52には、本コンピュータの設定データや、ブートプログラムなどが格納されている。

【0043】

RAM 53は、HDD（ハードディスクドライブ）54からロードされたコンピュータプログラムやデータ、インターフェース57を介して外部から受信したデータなどを一時的に記憶するためのエリアを有する。更に、RAM 53は、CPU 51が各種の処理を実行する際に用いるワークエリアを有する。即ち、RAM 53は、各種のエリアを適宜提供することができる。

【0044】

HDD 54には、OS（オペレーティングシステム）や、本コンピュータを適用した装置が行う各種の処理をCPU 51に実行させるためのコンピュータプログラムやデータが保存されている。

【0045】

本コンピュータを管理サーバ装置1に適用した場合、係るコンピュータプログラムには、押印部4等、管理サーバ装置1が行うものとして後述する各処理をCPU 51に実行させるためのコンピュータプログラムが含まれている。また、認証情報データベース2、電子印鑑データベース3、管理データベース9についてもこのHDD 54内に設けられている。

【0046】

また、本コンピュータをユーザ端末装置6に適用した場合、係るコンピュータプログラムには、文書変換部7、押印位置指示部8等、ユーザ端末装置6が行うものとして後述する各処理をCPU 51に実行させるためのコンピュータプログラムが含まれている。

【0047】

HDD 54に保存されているコンピュータプログラムやデータは、CPU 51による制御に従って適宜RAM 53にロードされ、CPU 51による処理対象となる。

【0048】

入力装置55は、キーボードやマウスなどにより構成されており、本コンピュータの操作者は、この入力装置55を操作することで、各種の指示をCPU 51に対して入力することができる。

【0049】

表示装置56は、CRTや液晶画面などにより構成されており、CPU 51による処理結果を画像や文字などでもって表示することができる。

【0050】

インターフェース57は、様々なインターフェースで構成されている。例えば、本コンピュータをユーザ端末装置6に適用した場合、インターフェース57は、本コンピュータをネットワーク10に接続する為のネットワークインターフェース、本コンピュータに認証デバイス5を接続する為のデバイスインターフェースを含む。また、本コンピュータを管理サーバ装置1に適用した場合、インターフェース57は、本コンピュータをネットワーク10に接続する為のネットワークインターフェースにより構成されている。

【0051】

58は上述の各部を繋ぐバスである。

【0052】

本実施形態では説明を簡単にするために、管理サーバ装置1、ユーザ端末装置6の何れも図5に示した構成を有するコンピュータであるものとして説明するが、コンピュータの構成については係る構成に限定するものではない。また、管理サーバ装置1とユーザ端末装置6とで異なる構成を有するコンピュータを適用しても良い。

【0053】

図6は、本実施形態に係るシステムを構成する認証デバイス5、管理サーバ装置1、ユーザ端末装置6のそれぞれの装置間の処理のシーケンスを示す図である。

【0054】

認証デバイス5がユーザ端末装置6に接続されたことをユーザ端末装置6が検知すると、ユーザ端末装置6は認証デバイス5に対して、識別子の送信要求を行う（ステップS61）。

【0055】

認証デバイス5はこの送信要求を受信すると、自身に固有の識別子をユーザ端末装置6に対して返信する（ステップS62）。

【0056】

ユーザ端末装置6は、認証デバイス5から識別子を受信すると、ユーザ端末装置6上でユーザが入力したパスワードと、この受信した識別子と、を管理サーバ装置1に送信する（ステップS63）。

10

【0057】

ステップS64では先ず、管理サーバ装置1は、ユーザ端末装置6から識別子とパスワードとを受信すると、受信した識別子とパスワードのセットが、認証情報データベース2に登録されているかを判断すべく、この認証情報データベース2内を検索する。係る検索の結果、ユーザ端末装置6から受信した識別子とパスワードとのセットが認証情報データベース2に登録されていた場合には、認証成功を示す認証情報をユーザ端末装置6に送信する。一方、ユーザ端末装置6から受信した識別子とパスワードとのセットが認証情報データベース2に登録されていなかった場合には、認証失敗を示す認証情報をユーザ端末装置6に送信する。

20

【0058】

ステップS65では、ユーザ端末装置6は、管理サーバ装置1から受信した認証情報を参照する。そしてユーザ端末装置6は、この認証情報が認証成功を示している場合には、ログイン成功であるので、ステップS66では、ユーザ端末装置6は、パスワードを入力したユーザに対して、ユーザ端末装置6の使用（処理の開始）を許可する。

【0059】

次に、ユーザ端末装置6のユーザは、押印したい文書データを選択する。係る文書データは予め作成され、ユーザ端末装置6内に保存されたものから1つをユーザが選択したものであっても良いし、現在作成した文書データであっても良い。

【0060】

30

この文書データは、テキストデータなど、特定の形式に依存しないデータであるので、ユーザ端末装置6は、この文書データを、画像情報を合成することが可能な文書データ（電子文書）に変換する。なお、係る電子文書が予め選択されていても良い。

【0061】

従ってステップS67では、ユーザ端末装置6は、ユーザによる文書データの選択操作を受け付け、係る選択操作により選択された文書データを、画像情報を合成可能な電子文書に変換する処理を行う。また、ユーザ端末装置6のユーザは、この変換した電子文書上で、押印する位置（領域）を指定するので、ユーザ端末装置6は、この指定された位置（指定位置、配置位置）を示す情報である押印位置情報（配置位置情報）を生成する。

【0062】

40

そして次に、ステップS68では、ユーザ端末装置6は、認証デバイス5に対して識別子の送信要求を行う。

【0063】

ステップS69では、認証デバイス5は、この送信要求を受信すると、自身に固有の識別子をユーザ端末装置6に対して送信する。

【0064】

そしてステップS70では、ユーザ端末装置6は、認証デバイス5から識別子を受信すると、この受信した識別子を管理サーバ装置1に送信する（第1の送信）。

【0065】

ステップS71では、管理サーバ装置1は、ユーザ端末装置6から識別子を受信すると

50

、電子印鑑データベース3において、この識別子とセットになって登録されている印影ファイルを検索する。

【0066】

そしてステップS72では、管理サーバ装置1は、係る検索により得られた印影ファイルをユーザ端末装置6に送信する。

【0067】

ユーザ端末装置6は、管理サーバ装置1から送信された識別子に対応する印影ファイル（返信結果）を受信すると、受信した印影ファイルに含まれているそれぞれの印影画像を選択可能に一覧表示し、何れか1つをユーザに選択させる。ユーザによる印影画像の選択が完了すると、ステップS73においてユーザ端末装置6は、ユーザにより選択された印影画像（選択印影画像）、上記変換済み電子文書、押印位置情報、を管理サーバ装置1に送信する（第2の送信）。

10

【0068】

ステップS74において、管理サーバ装置1は、ユーザ端末装置6から受信した電子文書上の、ユーザ端末装置6から受信した押印位置情報が示す位置に、ユーザ端末装置6から受信した選択印影画像を配置（合成）する（合成処理）。これにより、選択印影画像が示す印影が押印された電子文書（合成画像）を作成することができる。

【0069】

そしてステップS75において管理サーバ装置1は、ステップS74で作成した合成画像（送信応答、押印済み電子文書）を、ユーザ端末装置6に送信（出力）する。

20

【0070】

以下、図6に示した各処理についてより詳細に説明する。

【0071】

図2は、ユーザ端末装置6がログインするための、ユーザ端末装置6、管理サーバ装置1のそれぞれが行う処理のフローチャートである。なお、図6においてステップS21、S22、S24はユーザ端末装置6側の処理で、ステップS23は管理サーバ装置1側の処理である。

【0072】

ユーザ端末装置6は、ユーザ端末装置6のインターフェース57に認証デバイス5が接続されているか否かをチェックする（ステップS21）。ここで、認証デバイス5とは、例えば、USBキー、非接触ICカード、スマートメディア等、ユーザ端末装置6に接続可能なものであって、識別子を取得できるものであれば、どのようなデバイスであっても構わない。なお、認証デバイス5の識別子は、例えば、シリアル番号、デバイスID等、認証デバイス5を固有に識別できるものであれば良い。

30

【0073】

インターフェース57は、認証デバイス5が接続されるとその旨をCPU51に通知するので、CPU51はこの通知があった場合には、インターフェース57に認証デバイス5が接続されたと判断する。係る判断の結果、認証デバイス5がインターフェース57に接続された場合には処理をステップS22に進め、接続されていない場合には処理をステップS21に戻す。

40

【0074】

ステップS22では、CPU51は、インターフェース57を介して認証デバイス5に識別子の送信要求を送信する。認証デバイス5はこの送信要求を受信すると、自身に固有の識別子をユーザ端末装置6に対して返信するので、ユーザ端末装置6のCPU51は、この送信された識別子をインターフェース57を介してRAM53に取得する。

【0075】

次に、ユーザ端末装置6のユーザは、入力装置55を用いてパスワードを入力するので、CPU51はこの入力されたパスワードをRAM53に一時的に取得する。

【0076】

そしてCPU51は、RAM53にパスワード、識別子を取得する（第3の取得）と、

50

この取得したパスワード、識別子を、インターフェース 57 を介して管理サーバ装置 1 に送信する。

【0077】

管理サーバ装置 1 の CPU 51 は、ユーザ端末装置 6 から送信されたパスワード、識別子をインターフェース 57 を介して RAM 53 に取得する。そしてステップ S23 では、管理サーバ装置 1 は、この取得したパスワードと識別子のセットが、HDD 54 内に保存されている認証情報データベース 2 内に登録されているか否かをチェックする。即ち、認証情報データベース 2 内を検索する。係る検索の結果、ユーザ端末装置 6 から受信したパスワードと識別子のセットが認証情報データベース 2 内に登録されていた場合には、処理をステップ S24 に進める。一方、ユーザ端末装置 6 から受信したパスワードと識別子の

10

【0078】

ステップ S24 では、管理サーバ装置 1 は、認証成功を示す認証情報をユーザ端末装置 6 に送信するので、ユーザ端末装置 6 は、管理サーバ装置 1 から受信した認証情報を参照する。そしてユーザ端末装置 6 は、この認証情報が認証成功を示している場合には、ログイン成功であるので、パスワードを入力したユーザに対して、ユーザ端末装置 6 の使用を許可する。

【0079】

以上説明した処理により、ユーザは、ユーザ端末装置 6 の使用が許可される。なお、認証デバイス 5 は、ユーザがログインしている間は常にユーザ端末装置 6 に接続されているものとする。従って、例えば、ユーザ端末装置 6 から認証デバイス 5 が抜かれるなど、認証デバイス 5 とユーザ端末装置 6 との間の接続が解除された場合、ユーザ端末装置 6 の CPU 51 は、例えば、入力装置 55 からの指示の受付を禁止するなどの処理を行う。これにより、第三者によるユーザ端末装置 6 の不正な利用を防止する。

20

【0080】

なお、本実施形態では、ログインのためには、パスワードと識別子の両方を管理サーバ装置 1 に送信するものとしているが、パスワードを必要としないシステムの構築も可能である。この場合、パスワードの入力は行わないし、パスワードの送信も行わない。また、管理サーバ装置 1 側では、認証情報データベース 2 には識別子のみを登録しておき、ユーザ端末装置 6 から送信された識別子が認証情報データベース 2 内に登録されていれば認証成功とする。

30

【0081】

さらに、認証情報データベース 2 がユーザ端末装置 6 の HDD 54 内に納められている構成も可能である。この場合、パスワードと識別子のセットは管理サーバ装置 1 に送信しない。ユーザ端末装置 6 の CPU 51 がパスワードと識別子を取得すると、そのセットがユーザ端末装置 6 の HDD 54 内に保存されている認証情報データベース 2 内に登録されているか否かをチェックし、登録されていれば認証成功とする。

【0082】

また、認証情報データベース 2 がユーザ端末装置 6 の HDD 54 内に納められている構成においても、パスワードを必要としないシステムの構築が可能であることは言うまでもない。

40

【0083】

次に、ログイン後に、押印された電子文書を取得するためにユーザ端末装置 6 が行う処理について、同処理のフローチャートを示す図 3 を用いて説明する。

【0084】

ユーザ端末装置 6 のユーザは、押印したい文書データを入力装置 55 を用いて選択指示する。例えば、予め HDD 54 に保存している文書データ群のファイル名などを表示装置 56 の表示画面上に一覧表示し、ユーザはこの一覧表示された中から 1 つを入力装置 55 を用いて選択する。従ってステップ S31 では、ユーザ端末装置 6 の CPU 51 は、選択

50

指示された文書データをHDD 54からRAM 53に読み出す。

【0085】

次に、ステップS 32では、CPU 51は、この読み出した文書データをPDF等の画像情報を合成可能なデータである電子文書に変換する。また、プリンタドライバ方式の変換システムを用いることにより、ユーザ端末装置6上で印刷可能な任意の文書を押印可能な文書に変換することも可能である。

【0086】

次に、ステップS 33では、CPU 51は、認証デバイス5に対して識別子の送信要求を行うので、認証デバイス5は、自身に固有の識別子をユーザ端末装置6に送信する。ユーザ端末装置6は、認証デバイス5から識別子を受信すると、この受信した識別子を管理サーバ装置1に送信する。

10

【0087】

上述の通り、管理サーバ装置1は、ユーザ端末装置6から識別子を受信すると、この識別子に対応する印影ファイルを管理サーバ装置1のHDD 54内の電子印鑑データベース3から取得し、ユーザ端末装置6に送信する。従ってステップS 34では、CPU 51は、インターフェース57を介してこの印影ファイルをRAM 53に取得する。

【0088】

次に、ステップS 35では、ユーザ端末装置6のCPU 51は、取得した印影ファイルに含まれているそれぞれの印影画像を選択可能に表示装置56の表示画面上に一覧表示し、何れか1つをユーザに選択させる。

20

【0089】

ここで、ユーザは一覧表示された印影画像に加え、所定の画像形式の印影画像を読み込み、その画像を選択印影画像として使用することも可能である。その場合、読み込まれた印影画像は管理サーバ装置1に送信され、管理サーバ装置1のHDD 54内の電子印鑑データベース3に識別子と関連付けられて登録される。ここで登録された印影画像は、次回以降、ユーザ端末装置6からの要求に応じて印影ファイルとしてユーザ端末装置6に送信され、ユーザ端末装置6の表示装置56の表示画面上に一覧表示され、選択可能となる。

【0090】

また、ユーザは、一覧表示された印影画像を削除することも可能である。その場合、削除された印影画像を示す情報は管理サーバ装置1に送信され、電子印鑑データベース3内で識別子と関連付けられた、この情報が示す印影画像が削除される。

30

【0091】

次に、ステップS 36では、ユーザ端末装置6のCPU 51は、変換した電子文書を表示装置56の表示画面上に表示するので、ユーザは入力装置55を用いて、この電子文書上で押印する位置（領域）を指定する。ユーザ端末装置6のCPU 51は、この指定された位置（指定位置）を示す情報である押印位置情報を生成する。

【0092】

なお、押印する位置は、電子文書上であれば、自由に押印する位置を指定することが可能である。

【0093】

40

なお、押印位置情報の指定については、電子文書が得られれば、ステップS 37までの間にいつ行っても良いし、選択印影画像の選択については、印影ファイルが得られれば、ステップS 37までの間にいつ行っても良い。即ち、それぞれの処理は、上記の順番で行うことに限定するものでもない。

【0094】

次に、ステップS 37では、ユーザ端末装置6は、ユーザにより選択された印影画像（選択印影画像）、上記変換済み電子文書、押印位置情報、を管理サーバ装置1に送信する。

【0095】

管理サーバ装置1は、ユーザ端末装置6から受信した電子文書上の、ユーザ端末装置6

50

から受信した押印位置情報が示す位置に、ユーザ端末装置 6 から受信した選択印影画像を配置（合成）することで、押印済み電子文書を作成する。なお、合成とは、電子文書を透過させて表示させることも可能である。例えば、印鑑の丸い枠と、氏名等の文字以外の部分は、透過されている為、電子文書の文字が表示される。そして管理サーバ装置 1 は、この作成した押印済み電子文書をネットワーク 10 を介してユーザ端末装置 6 に送信する。

【0096】

従ってステップ S 38 では、ユーザ端末装置 6 の CPU 51 は、インターフェース 57 を介してこの押印済み電子文書を RAM 53 に取得する。取得した押印済み電子文書の取り扱いについては本実施形態では特に触れないが、HDD 54 に保存するようにしても良いし、表示装置 56 の表示画面上に表示するようにしても良い。なお、HDD 54 に保存する場合、ユーザによって指示された、押印したい文書データ（例えば Word 等）に上書き保存をされるわけではなく、画像情報を合成可能な電子文書に変換された文書データ（例えば PDF 等）を保存する。また、ユーザ端末装置 6 に印刷装置を接続し、この印刷装置に押印済み電子文書を印刷させても良い。

10

【0097】

また、ユーザ端末装置 6 の所定のアプリケーションソフトを用いて、押印済み電子文書を他のユーザ端末装置 6 に通信（メール）しても良い。

【0098】

なお、電子印鑑データベース 3 には、認証デバイス 5 の識別子と、複数の印影画像を含む印影ファイルと、がセットになって登録されているが、これに限定されず、印影画像を含まない印影ファイルが登録されている構成とすることも可能である。

20

【0099】

この場合、ステップ S 33 で、管理サーバ装置 1 から識別子に対応する印影画像を含まない印影ファイルを取得後に、ユーザ端末装置 6 にて、所定の画像作成ソフトを用いて印影画像を作成する。そして、作成された印影画像を、管理サーバ装置 1 に送信し、識別子と関連付けられた印影ファイルに登録する。印影ファイルに登録後、ユーザ端末装置 6 は、識別子の取得、管理サーバ装置 1 への送信を再度行い（ステップ S 33）、ステップ S 34 以降の処理を行う。

【0100】

また、管理サーバ装置 1 は、識別子とセットになっている印影ファイルをユーザ端末装置 6 へ送信後（ステップ S 43）に、ユーザ端末装置 6 から印影画像を受信した場合、受信した印影画像を、識別子と関連付けられた印影ファイルに登録する。そして、ステップ S 33 においてユーザ端末装置 6 が送信した識別子を受信し（ステップ S 41）、ステップ S 42 以降の処理を行う。

30

【0101】

次に、ログイン後に、押印された電子文書を取得するために管理サーバ装置 1 が行う処理について、同処理のフローチャートを示す図 4 を用いて説明する。

【0102】

まず、ステップ S 41 では、管理サーバ装置 1 の CPU 51 は、上記ステップ S 33 においてユーザ端末装置 6 が送信した識別子を受信する。

40

【0103】

次に、ステップ S 42 では、管理サーバ装置 1 の CPU 51 は、ステップ S 41 で受信した識別子とセットになって登録されている印影ファイルを、HDD 54 内の電子印鑑データベース 3 から検索する。

【0104】

そしてステップ S 43 では、管理サーバ装置 1 の CPU 51 は、係る検索により得られた印影ファイルをユーザ端末装置 6 に送信する。

【0105】

次に、ステップ S 44 では、管理サーバ装置 1 の CPU 51 は、上記ステップ S 37 においてユーザ端末装置 6 から送信された選択印影画像、変換済み電子文書、押印位置情報

50

、を受信し、RAM 53に取得する。

【0106】

次に、ステップS45では、管理サーバ装置1のCPU51は、ユーザ端末装置6から受信した電子文書上の、ユーザ端末装置6から受信した押印位置情報が示す位置に、ユーザ端末装置6から受信した選択印影画像を配置（合成）する。なお、本ステップにおいて管理サーバ装置1のCPU51は、選択印影画像の合成時における時刻情報をCPU51内部のタイマにより計時し、計時した時刻情報を、HDD54内の管理データベース9に登録するようにしても良い。

【0107】

そしてステップS46では、管理サーバ装置1のCPU51は、ステップS45で作成した合成画像（押印済み電子文書）を、ユーザ端末装置6に送信する。

10

【0108】

以上の説明により、本実施形態によれば、電子文書に押印する場合に従来では生じていた煩わしい作業を軽減させることができる。また、利用者が電子文書に押印したい文書の形式やフォーマットに捉われることなく押印が可能となる。

【0109】

なお、本実施形態では、電子文書に対しては選択印影画像を指示された位置に配置するのみの処理を行っていたが、これ以外の処理を電子文書に対して行うようにしても良い。例えば、閲覧、編集、文書内の文字列や図のコピー、印刷の可否等を制御するためのセキュリティ情報を、この電子文書に付加するようにしても良い。なお、係るセキュリティ情報は、ユーザ端末装置6側で設定したものを、電子文書、選択印影画像、押印位置情報と共に管理サーバ装置1に送信するようにしても良いし、予め管理サーバ装置1側のHDD54に保持させておいても良い。

20

【0110】

但し、このセキュリティ情報（属性）を付加させることができるかどうかは、変換された電子文書のフォーマットに依存する。例えば、上で挙げたPDFには、上述したようなセキュリティ情報を付加することが可能である。

【0111】

また、管理サーバ装置1がタイムサーバと接続されていれば、電子文書上に選択印影画像を合成した時刻情報をこのタイムサーバから取得し、この取得した時刻情報もこの電子文書に合成しても良い。すなわち、時差が生じる地域においても時刻の同期を取る事ができる。

30

【0112】

また、この時刻情報に対しても、上述したようなセキュリティ情報を付加させてもよい。

【0113】

これにより、印影画像の正当性や押印時刻を保証することや、押印済み電子文書の統括的な管理が可能になるため、押印ログや文書のデータベース化も容易となる。

【0114】

また、本実施形態では説明を簡単にするために図1には管理サーバ装置1、ユーザ端末装置6をそれぞれ1台ずつ示しているが、これに限定するものではない。即ち、ユーザの数だけユーザ端末装置6をネットワーク10上に接続しても良いし、処理を分散させるために管理サーバ装置1を複数台ネットワーク10に接続するようにしても良い。

40

【0115】

管理サーバ装置1が複数台ネットワーク10に接続されている場合、それぞれの管理サーバ装置1は同じ情報を保持しておく。そして、ユーザ端末装置6からのアクセスがあった場合には、より処理負荷の小さい管理サーバ装置1にアクセスするようにシステムを構築する。係る技術については一般のネットワーク技術であるので、これ以上の説明は省略する。

【0116】

50

また、管理サーバ装置 1、ユーザ端末装置 6 の各構成は、上述した構成に限定されず、適宜組み合わせた構成とすることも可能である。

【0117】

例えば、電子印鑑データベース 3、押印部 4、管理データベース 9 を、ユーザ端末装置 6 が有するようにしても良い。

【0118】

また、管理サーバ装置 1 が特定の形式に依存しないデータを認識できるのであれば、文書変換部 7 を管理サーバ装置 1 が有するようにしても良い。

【0119】

また、認証デバイス 5 に、電子印鑑データベース 3 を保持させるようにしても良い。この場合、印影ファイルを取得するためにユーザ端末装置 6 が認証デバイス 5 に識別子を要求した後、認証デバイス 5 は識別子と印影ファイルをユーザ端末装置 6 に送信すれば、ユーザ端末装置 6 側では印影画像を選択可能に一覧表示できる。

【0120】

[第 2 の実施形態]

本実施形態では、管理サーバ装置 1 とユーザ端末装置 6 とを 1 つの装置内にまとめたものを認証処理装置とする。即ち、第 1 の実施形態では、押印済み電子文書を取得するためには、ネットワーク 10 を介してユーザ端末装置 6 と管理サーバ装置 1 との間でのデータ通信を行っていた。本実施形態では、これらの装置をまとめた 1 つの認証処理装置を動作させることで、押印済み電子文書を取得する。

【0121】

図 7 は、本実施形態に係る認証処理装置の機能構成例を示すブロック図である。即ち、図 2 に示したユーザ端末装置 6 が有する各部と、管理サーバ装置 1 が有する各部とが、1 つの装置（認証処理装置）700 内に納められている。また、この認証処理装置 700 についても、図 5 に示した構成例を有するコンピュータを適用することができる。

【0122】

即ち、本実施形態に係る認証処理装置 700 の動作については、第 1 の実施形態で説明した一連の処理において、通信処理がないだけで、それぞれの装置が行っているものとして第 1 の実施形態で説明した各処理を認証処理装置 700 が行うことになる。

【0123】

例えば、認証処理装置 700 がログインするために行う処理については以下の通りである。

【0124】

まず、インターフェース 57 に認証デバイス 5 が接続されているか否かをチェックする。認証デバイス 5 がインターフェース 57 に接続された場合にはインターフェース 57 を介して認証デバイス 5 の識別子をインターフェース 57 を介して RAM 53 に取得する。

【0125】

次に、認証処理装置 700 のユーザは、入力装置 55 を用いてパスワードを入力するので、この入力されたパスワードを RAM 53 に一時的に取得する。

【0126】

そして、RAM 53 にパスワード、識別子を取得すると、この取得したパスワードと識別子のセットが、HDD 54 内に保存されている認証情報データベース 2 内に登録されているか否かをチェックする。そして、パスワードと識別子のセットが認証情報データベース 2 内に登録されていた場合には、認証成功となり、パスワードを入力したユーザに対して、認証処理装置 700 の使用を許可（ログイン）する。

【0127】

次に、ログイン後に、押印された電子文書を取得するために認証処理装置 700 が行う処理について、同処理のフローチャートを示す図 8 を用いて説明する。

【0128】

認証処理装置 700 のユーザは、押印したい文書データを入力装置 55 を用いて選択指

10

20

30

40

50

示する。例えば、予めHDD54に保存している文書データ群のファイル名などを表示装置56の表示画面上に一覧表示し、ユーザはこの一覧表示された中から1つを入力装置55を用いて選択する。従ってステップS81では、認証処理装置700のCPU51は、選択指示された文書データをHDD54からRAM53に読み出す。

【0129】

次に、ステップS82では、CPU51は、この読み出した文書データをPDF等の画像情報を合成可能な電子文書に変換する。また、プリンタドライバ方式の変換システムを用いることにより、ユーザ端末装置6上で印刷可能な任意の文書を押印可能な文書に変換することも可能である。

【0130】

次に、ステップS83では、CPU51は、認証デバイス5に対して識別子の送信要求を行うので、認証デバイス5は、自身に固有の識別子を認証処理装置700に送信する。従ってステップS83では、認証デバイス5から送信された識別子を取得する。

【0131】

次に、ステップS84では、CPU51は、ステップS83で取得した識別子とセットになって登録されている印影ファイルを、HDD54内の電子印鑑データベース3から検索する。

【0132】

そしてステップS85では、CPU51は、係る検索により得られた印影ファイルを取得する。

【0133】

次に、ステップS86では、CPU51は、取得した印影ファイルに含まれているそれぞれの印影画像を選択可能に表示装置56の表示画面上に一覧表示し、何れか1つを選択印影画像としてユーザに選択させる。

次に、ステップS87では、CPU51は、変換した電子文書を表示装置56の表示画面上に表示するので、ユーザは入力装置55を用いて、この電子文書上で押印する位置（領域）を指定する。CPU51は、この指定された位置（指定位置）を示す情報である押印位置情報を生成する。

【0134】

なお、押印位置情報の指定については、電子文書が得られれば、ステップS88までの間にいつ行っても良いし、選択印影画像の選択については、印影ファイルが得られれば、ステップS88までの間にいつ行っても良い。即ち、それぞれの処理は、上記の順番で行うことに限定するものでもない。

【0135】

次に、ステップS88では、CPU51は、電子文書上の押印位置情報が示す位置に、選択印影画像を配置（合成）することで、押印済み電子文書を取得する。なお、本ステップにおいてCPU51は、選択印影画像の合成時における時刻情報を、HDD54内の管理データベース9に登録するようにしても良い。また、取得した押印済み電子文書の取り扱いについては本実施形態では特には触れないが、HDD54に保存するようにしても良いし、表示装置56の表示画面上に表示するようにしても良い。また、認証処理装置700に印刷装置を接続し、この印刷装置に押印済み電子文書を印刷させても良い。

【0136】

以上の説明により、本実施形態によれば、第1の実施形態のようにデータ通信を行うための時間を省略できるし、1台の装置のみで同様の目的を達成することができるので、コストや設置スペース、設置の手間の問題を解消することができる。

【0137】

なお、本実施形態では、電子文書に対しては選択印影画像を指示された位置に配置するのみの処理を行っていたが、これ以外の処理を電子文書に対して行うようにしても良い。例えば、閲覧、編集、文書内の文字列や図のコピー、印刷の可否等を制御するためのセキュリティ情報を、この電子文書に付加するようにしても良い。なお、係るセキュリティ情

10

20

30

40

50

報は、認証処理装置 700 においてユーザが入力装置 55 を用いて設定したものを用いても良いし、予め HDD 54 に保持させておいたものを用いても良い。

【0138】

但し、このセキュリティ情報を付加させることができるかどうかは、変換された電子文書のフォーマットに依存する。例えば、上で挙げた PDF には、上述したようなセキュリティ情報を付加することが可能である。

【0139】

また、認証処理装置 700 がタイムサーバと接続されていれば、電子文書上に選択印影画像を合成した時刻情報をこのタイムサーバから取得し、この取得した時刻情報もこの電子文書に合成しても良い。すなわち、時差が生じる地域においても時刻の同期を取る事が

10

【0140】

また、この時刻情報に対しても、上述したようなセキュリティ情報を付加させてもよい。

【0141】

これにより、印影画像の正当性や押印時刻を保証することや、押印済み電子文書の統括的な管理が可能になるため、押印ログや文書のデータベース化も容易となる。

【0142】

なお、上記各実施形態は適宜組み合わせ用いても良い。

【0143】

20

[その他の実施形態]

また、本発明の目的は、以下のようにすることによって達成されることはいうまでもない。即ち、前述した実施形態の機能を実現するソフトウェアのプログラムコード（コンピュータプログラム）を記録した記録媒体（または記憶媒体）を、システムあるいは装置に供給する。係る記憶媒体は言うまでもなく、コンピュータ読み取り可能な記憶媒体である。そして、そのシステムあるいは装置のコンピュータ（または CPU や MPU）が記録媒体に格納されたプログラムコードを読み出し実行する。この場合、記録媒体から読み出されたプログラムコード自体が前述した実施形態の機能を実現することになり、そのプログラムコードを記録した記録媒体は本発明を構成することになる。

【0144】

30

また、コンピュータが読み出したプログラムコードを実行することにより、そのプログラムコードの指示に基づき、コンピュータ上で稼働しているオペレーティングシステム（OS）などが実際の処理の一部または全部を行う。その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【0145】

さらに、記録媒体から読み出されたプログラムコードが、コンピュータに挿入された機能拡張カードやコンピュータに接続された機能拡張ユニットに備わるメモリに書込まれたとする。その後、そのプログラムコードの指示に基づき、その機能拡張カードや機能拡張ユニットに備わる CPU などが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

40

【0146】

本発明を上記記録媒体に適用する場合、その記録媒体には、先に説明したフローチャートに対応するプログラムコードが格納されることになる。

【0147】

また、本発明が通信手段を持つ場合、ネットワークを介して前述した実施形態の機能を実現するソフトウェアのプログラムコードをシステムあるいは装置に供給することも可能である。

【図面の簡単な説明】

【0148】

【図1】本発明の第1の実施形態に係るシステム（認証処理装置）の機能構成例を示すブ

50

ロック図である。

【図2】 ユーザ端末装置6がログインするための、ユーザ端末装置6、管理サーバ装置1のそれぞれが行う処理のフローチャートである。

【図3】 ログイン後に、押印された電子文書を取得するためにユーザ端末装置6が行う処理のフローチャートである。

【図4】 ログイン後に、押印された電子文書を取得するために管理サーバ装置1が行う処理のフローチャートである。

【図5】 管理サーバ装置1、ユーザ端末装置6、に適用可能なコンピュータのハードウェア構成例を示すブロック図である。

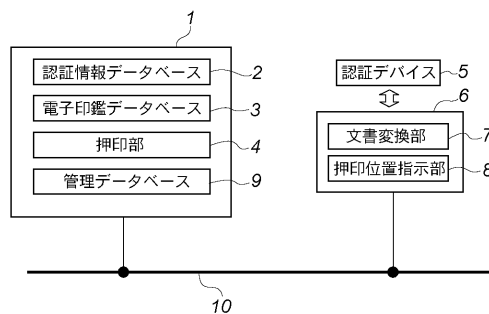
【図6】 本発明の第1の実施形態に係るシステムを構成する認証デバイス5、管理サーバ装置1、ユーザ端末装置6のそれぞれの装置間の処理のシーケンスを示す図である。

10

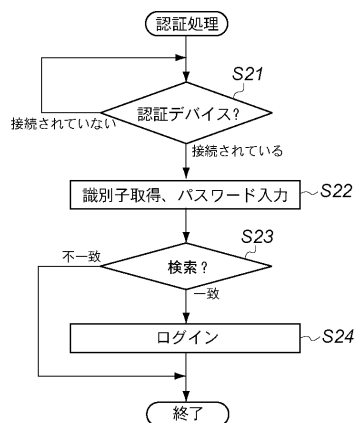
【図7】 本発明の第2の実施形態に係る認証処理装置の機能構成例を示すブロック図である。

【図8】 ログイン後に、押印された電子文書を取得するために認証処理装置700が行う処理のフローチャートである。

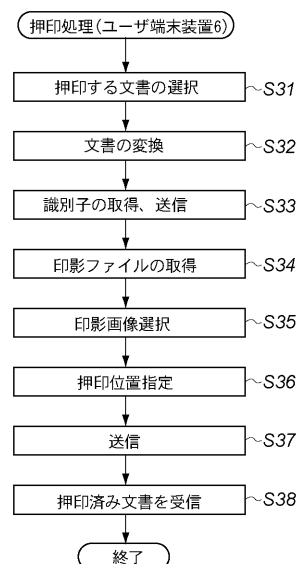
【図1】



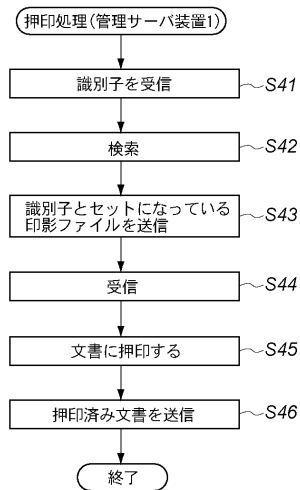
【図2】



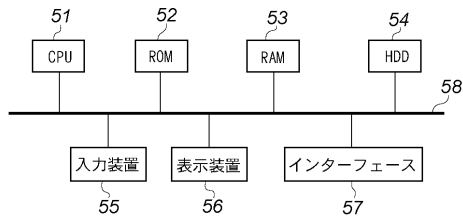
【図3】



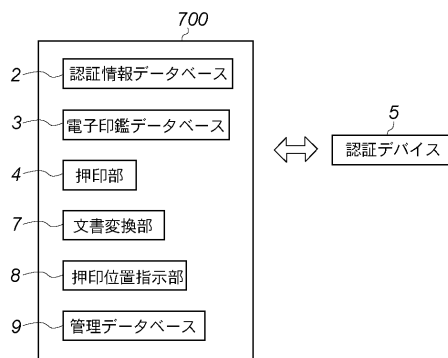
【図 4】



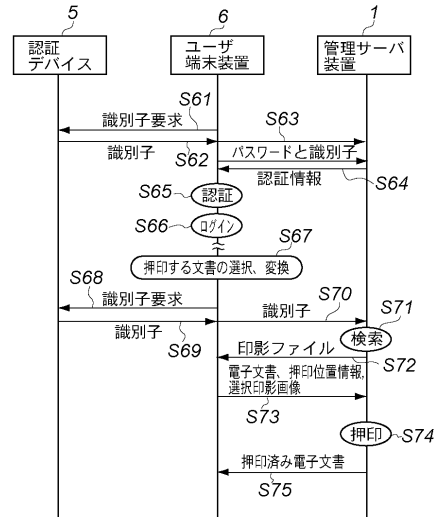
【図 5】



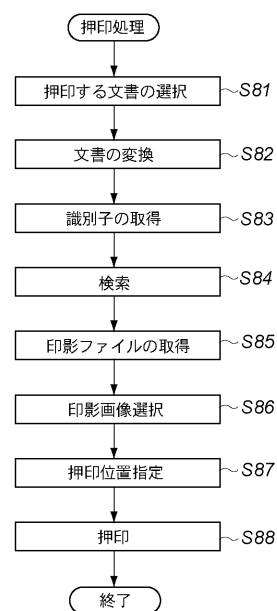
【図 7】



【図 6】



【図 8】



フロントページの続き

(72)発明者 佐藤 智規
埼玉県秩父市下影森1248番地 キヤノン電子株式会社内

審査官 石田 信行

(56)参考文献 特開2007-128515 (JP, A)
特開2005-276000 (JP, A)
特開2005-141565 (JP, A)
特開2003-304243 (JP, A)
特開2003-169051 (JP, A)
特開2005-217610 (JP, A)
特開2008-134769 (JP, A)
特開2007-066212 (JP, A)
特開2007-036316 (JP, A)
特開2004-062214 (JP, A)
特開2001-229323 (JP, A)

(58)調査した分野(Int.Cl., DB名)
G06F 21/24
G06F 21/20
G06K 19/10
G06T 7/00
G09C 1/00
H04L 9/32