

明 細 書

発明の名称：

電子承認システム、電子承認サーバ、電子承認プログラム、及びコンピュータ可読記憶媒体

技術分野

[0001] 本発明の実施形態は、電子承認システム、電子承認サーバ、電子承認プログラム、及びコンピュータ可読記憶媒体に関する。

背景技術

[0002] 電子印鑑装置によって、電子文書に印影データを挿入する電子印鑑システムが実用化されている。電子印鑑装置は、手指生体特徴などにより生体認証を行い、生体認証の結果に応じて、電子文書に印影データを挿入する。このように、電子印鑑装置は、電子印鑑装置を本人（登録者）以外が使用することを防ぐように構成されている。

[0003] しかしながら、電子印鑑装置は、電子印鑑装置の登録者に対応付けられた印影データを電子文書に挿入するように構成されており、組織、部門、及び団体などに対応付けられた印影データを電子文書に挿入するケースに対応することができないという課題がある。

[0004] また、印鑑の誤押印及び虚偽の押印などによる電子文書の変更を防止する電子印鑑システムがある。しかしながら、このようなシステムでは、電子印鑑装置の為の端末（電子文書の表示を行う端末）が専用端末になる為、汎用性が低いという課題がある。

先行技術文献

特許文献

[0005] 特許文献1：日本国特開2004-214792号公報
特許文献2：日本国特開2007-066212号公報

発明の概要

発明が解決しようとする課題

[0006] 本発明が解決しようとする課題は、利便性の高い電子承認システム、電子承認サーバ、電子承認プログラム、及びコンピュータ可読記憶媒体を提供することである。

課題を解決するための手段

[0007] 一実施形態に係る電子承認システムは、少なくとも1つ以上の電子承認装置と、電子承認サーバとを備える。前記電子承認装置は、第1通信部と、生体認証部と、セキュリティチップと、を具備する。前記電子承認サーバは、第2通信部と、プロセッサと、を具備する。第1通信部は、情報処理装置を介して前記電子承認サーバと通信する。生体認証部は、生体認証を行う。セキュリティチップは、前記生体認証の結果が正常である場合、予め記憶された秘密鍵を用いて信頼性確認情報を生成し、前記情報処理装置を介して前記信頼性確認情報を前記電子承認サーバに送信する。第2通信部は、前記情報処理装置を介して前記電子承認装置と通信する。プロセッサは、前記秘密鍵に対応する公開鍵と、前記信頼性確認情報と、に基づいて、前記電子承認装置における承認が正常に実行されたことを示す電子承認記録を保存する。

図面の簡単な説明

[0008] [図1]図1は、第1実施形態に係る電子承認システムの概略的な構成例について説明する為の説明図である。

[図2]図2は、第1実施形態に係る電子承認システムの各構成の例について説明する為の説明図である。

[図3]図3は、第1実施形態に係る電子承認システムのサーバに記憶されているデータの例について説明する為の説明図である。

[図4]図4は、第1実施形態に係る電子承認システムの電子印鑑装置に記憶されているデータの例について説明する為の説明図である。

[図5]図5は、第1実施形態に係る電子承認システムの動作の例について説明する為の説明図である。

[図6]図6は、第1実施形態に係る電子承認システムの動作の他の例について

説明する為の説明図である。

[図7]図7は、第2実施形態に係る電子承認システムの動作の例について説明する為の説明図である。

[図8]図8は、第3実施形態に係る電子承認システムの動作の例について説明する為の説明図である。

[図9]図9は、第3実施形態に係る電子承認システムのサーバに記憶されているデータの例について説明する為の説明図である。

[図10]図10は、第3実施形態に係る電子承認システムの電子署名装置に記憶されているデータの例について説明する為の説明図である。

[図11]図11は、第3実施形態に係る電子承認システムの動作の例について説明する為の説明図である。

実施形態

[0009] 以下、実施形態について、図面を参照して説明する。なお、各図面は、実施形態の理解を促すための模式図である。各図面で示された構成の形状、寸法、及び比などは、実施する場合の仕様に応じて適時変更可能である。

[0010] (第1実施形態)

図1は、第1実施形態に係る電子印鑑システム1の概略的な構成例について説明する為の説明図である。図2は、第1実施形態に係る電子印鑑システム1の各構成の例について説明する為の説明図である。

[0011] 電子印鑑システム1は、電子文書(文書データ)に対して、承認の記録を電子的に付与する(電子承認記録を付与する)電子承認システムの一形態である。電子印鑑システム1は、文書データに対して、電子承認記録として電子印影イメージを付与するシステムである。電子印鑑システム1は、電子印鑑システムサーバ11、管理サーバ12、情報処理装置13、及び少なくとも1つ以上の電子印鑑装置14などを備える。電子印鑑システムサーバ11は電子承認サーバの一例であり、電子印鑑装置14は電子承認装置の一例である。

[0012] 電子印鑑システム1では、電子印鑑装置14において承認の為の操作(例

例えば生体認証)が行われた場合、電子印鑑システムサーバ11及び管理サーバ12が、電子印鑑装置14における操作が正常であるか否か判断する。電子印鑑装置14における操作が正常であると判断した場合、電子印鑑システムサーバ11が文書データに対して電子印影イメージを挿入する。

[0013] 電子印鑑システムサーバ11、管理サーバ12、及び情報処理装置13は、ネットワーク15を介して通信する。ネットワーク15は、例えば公衆回線である。また、電子印鑑装置14は、情報処理装置13と通信可能に構成されている。電子印鑑装置14は、情報処理装置13を介して、電子印鑑システムサーバ11と通信可能に構成されている。

[0014] まず、電子印鑑システムサーバ11及び管理サーバ12の構成例について説明する。

電子印鑑システムサーバ11は、電子承認に関する処理を行う電子承認サーバである。電子印鑑システムサーバ11は、プロセッサ21、メモリ22、及び通信部23を備える。

[0015] プロセッサ21は、演算処理を実行する演算素子である。プロセッサ21は、例えばCentral Processing Unit(CPU)として構成される。プロセッサ21は、メモリ22に記憶されているプログラムに基づいて種々の処理を行う。プロセッサ21は、通信部23及びネットワーク15などを介して、管理サーバ12及び情報処理装置13とデータを送受信する。

[0016] メモリ22は、プログラム及びデータを記憶する記憶装置である。メモリ22は、例えば、読み出し専用の不揮発性メモリであるROM、データを一時的に記憶するRAM、及びデータを記憶するストレージのいずれか、または複数を備える。

[0017] 通信部23は、他の機器と通信する為の構成である。通信部23は、ネットワーク15を介して、管理サーバ12及び情報処理装置13と通信する。

[0018] プロセッサ21は、メモリ22に記憶されているプログラム(電子承認プログラム)に基づいて、後述する電子承認に関する種々の処理を実行する。

[0019] 管理サーバ12は、電子承認に関する処理を行う電子承認サーバである。

管理サーバ１２は、プロセッサ３１、メモリ３２、及び通信部３３を備える。

[0020] プロセッサ３１は、演算処理を実行する演算素子である。プロセッサ３１は、例えばCentral Processing Unit（CPU）として構成される。プロセッサ３１は、メモリ３２に記憶されているプログラムに基づいて種々の処理を行う。プロセッサ３１は、通信部３３及びネットワーク１５などを介して、電子印鑑システムサーバ１１とデータを送受信する。

[0021] メモリ３２は、プログラム及びデータを記憶する記憶装置である。メモリ３２は、例えば、読み出し専用の不揮発性メモリであるROM、データを一時的に記憶するRAM、及びデータを記憶するストレージのいずれか、または複数を備える。

[0022] 通信部３３は、他の機器と通信する為の構成である。通信部３３は、ネットワーク１５を介して、電子印鑑システムサーバ１１と通信する。なお、管理サーバ１２の通信部３３は、ネットワーク１５を介して電子印鑑システムサーバ１１と通信するのではなく、専用回線によって電子印鑑システムサーバ１１と直接通信するように構成されていてもよい。

[0023] プロセッサ３１は、メモリ３２に記憶されているプログラム（電子承認プログラム）に基づいて、後述する電子承認に関する種々の処理を実行する。

[0024] 次に、情報処理装置１３の構成例について説明する。

情報処理装置１３は、電子印鑑システムサーバ１１と電子印鑑装置１４との中継、電子印鑑装置１４のユーザに対する情報の出力、及び電子印鑑装置１４のユーザからの操作入力の受付などを行う。情報処理装置１３は、プロセッサ４１、メモリ４２、通信部４３、ディスプレイ４４、及び操作インタフェース４５を備える。

[0025] プロセッサ４１は、演算処理を実行する演算素子である。プロセッサ４１は、例えばCentral Processing Unit（CPU）として構成される。プロセッサ４１は、メモリ４２に記憶されているプログラムに基づいて種々の処理を行う。プロセッサ４１は、通信部４３及びネットワーク１５などを介して、

電子印鑑システムサーバ１１とデータを送受信する。また、プロセッサ４１は、通信部４３を介して電子印鑑装置１４とデータを送受信する。

[0026] メモリ４２は、プログラム及びデータを記憶する記憶装置である。メモリ４２は、例えば、読み出し専用の不揮発性メモリであるＲＯＭ、データを一時的に記憶するＲＡＭ、及びデータを記憶するストレージのいずれか、または複数を備える。

[0027] 通信部４３は、他の機器と通信する為の構成である。通信部４３は、ネットワーク１５を介して、電子印鑑システムサーバ１１と通信する。また、通信部４３は、電子印鑑装置１４と無線通信を行う。なお、通信部４３は、例えばＵＳＢなどを介して電子印鑑装置１４と有線による通信を中継するＵＳＢコネクタを備える構成であってもよい。

[0028] ディスプレイ４４は、プロセッサ４１または図示されないグラフィックコントローラなどの表示制御部から入力される映像信号に応じて画面を表示する。

[0029] 操作インタフェース４５は、情報処理装置１３を操作するユーザ（例えば電子印鑑装置１４のユーザ）による操作入力を受け付ける為の構成である。操作インタフェース４５は、種々の操作部材を有する。操作インタフェース４５は、操作部材の操作に応じた操作信号をプロセッサ４１に供給する。操作部材は、例えば、タッチセンサ、テンキー、電源キー、用紙フィードキー、種々のファンクションキー、マウス、またはキーボードなどである。また、タッチセンサは、ディスプレイ４４と一体にタッチパネルとして構成されていてもよい。

[0030] 次に、電子印鑑装置１４の構成例について説明する。

電子印鑑装置１４は、文書データに電子印影イメージを挿入する為にユーザが操作する装置である。電子印鑑装置１４は、ユーザの生体情報（例えば指紋、静脈パターン、虹彩、顔特徴など）に基づいて生体認証を行う。電子印鑑装置１４は、プロセッサ５１、メモリ５２、通信部５３、生体センサ５４、セキュリティチップ５５、及びバッテリー５６を備える。また、電子印鑑

装置 1 4 は、図示されないインジケータ、またはスピーカなどを備えていてもよい。

- [0031] プロセッサ 5 1 は、演算処理を実行する演算素子である。プロセッサ 5 1 は、例えば Central Processing Unit (CPU) として構成される。プロセッサ 5 1 は、メモリ 5 2 に記憶されているプログラムに基づいて種々の処理を行う。プロセッサ 5 1 は、通信部 5 3 を介して、情報処理装置 1 3 とデータを送受信する。
- [0032] メモリ 5 2 は、プログラム及びデータを記憶する記憶装置である。メモリ 5 2 は、例えば、読み出し専用の不揮発性メモリである ROM、データを一時的に記憶する RAM、及びデータを記憶するストレージのいずれか、または複数を備える。
- [0033] 通信部 5 3 は、他の機器と通信する為の構成である。通信部 5 3 は、情報処理装置 1 3 と無線通信を行う。
- [0034] 生体センサ 5 4 は、ユーザの生体情報を取得する。本実施形態では、生体センサ 5 4 は、ユーザの指紋を画像として取得する。
- [0035] セキュリティチップ 5 5 は、生体認証に関する処理と、電子印鑑システムサーバ 1 1 に送信するデータ（後述の信頼性確認情報）の生成とを行う。セキュリティチップ 5 5 は、セキュアエレメントと呼ばれることもある。セキュリティチップ 5 5 は、例えば、プロセッサ、メモリ、乱数生成器、及び暗号回路などを有する。
- [0036] プロセッサは、所定の処理を実行する演算素子である。プロセッサは、入力された信号に応じて、生体認証を実行する。また、プロセッサは、乱数生成器による乱数生成を制御する。また、プロセッサは、暗号回路による暗号化処理を制御する。
- [0037] メモリは、上記の生体認証に用いられる生体情報（本例では、予めユーザの指紋の画像から特徴点などが抽出されて生成されたもの）を記憶する。なお、メモリは、暗号化された生体情報を記憶する構成であってもよい。また、メモリは、暗号回路において用いられる暗号鍵（秘密鍵）を予め記憶する

。

- [0038] 乱数生成器は、プロセッサの制御に応じて、乱数を生成する構成である。
乱数生成器は、例えば、ランダムな長さの乱数を生成し、生成したランダム長の乱数をパディングし、出力する。
- [0039] 暗号回路は、プロセッサの制御に応じて、データを暗号化する暗号化処理を実行する。暗号回路は、入力された暗号鍵を用いて、入力されたデータを暗号化し、暗号化されたデータ（暗号化データ）を出力する。例えば、暗号回路には、プロセッサがメモリから読み出した秘密鍵が暗号鍵として入力される。また、暗号回路には、暗号化の対象のデータとして、乱数生成器により生成された乱数が入力される。また、暗号回路は、例えば、暗号化処理としてハッシュ計算を行い、ハッシュ値を暗号化データとして出力する。即ち、暗号回路は、秘密鍵と乱数とに基づいてハッシュ計算を行い、ハッシュ値を暗号化データとして出力するように構成されている。
- [0040] バッテリ 56 は、電子印鑑装置 14 の各部に電力を供給する構成である。
バッテリ 56 は、例えばリチウムイオン二次電池などの蓄電池及び DC-DC コンバータなどを有する。DC-DC コンバータは、蓄電池の出力端子の直流電圧を電子印鑑装置 14 の各部の構成の定格電圧に応じた電圧に変換し、供給する。
- [0041] なお、電子印鑑装置 14 は、情報処理装置 13 と有線による通信を行うように構成されていてもよい。例えば、電子印鑑装置 14 は、情報処理装置 13 と USB により通信を行うように構成されていてもよい。この場合、電子印鑑装置 14 は、USB ケーブルが接続されるコネクタ（USB コネクタ）を備える。
- [0042] また、電子印鑑装置 14 は、USB ケーブルを介して情報処理装置 13 から給電される直流電力によって動作する。この為、電子印鑑装置 14 は、バッテリ 56 が省略されてもよい。
- [0043] 次に、電子印鑑システムサーバ 11 及び管理サーバ 12 に記憶されている情報について説明する。

図3は、電子印鑑システムサーバ11のメモリ22、または管理サーバ12のメモリ32に記憶されている情報について説明する為の説明図である。

[0044] 電子印鑑システムサーバ11のメモリ22、または管理サーバ12のメモリ32には、電子承認記録を付与する対象の文書データ（図3の例では「契約書A」）が記憶されている。

[0045] また、電子印鑑システムサーバ11のメモリ22、または管理サーバ12のメモリ32には、種々の電子印影に関するデータが記憶されている。図3の例では、「電子印影イメージ」、「電子印影ID」、「電子印鑑ID」、及び「公開鍵」が対応付けられて記憶されている。

[0046] 電子印影イメージは、文書データに付与される電子承認記録の一形態である。電子印影イメージは、例えば文書データ上に重ねられて表示される（挿入される）画像として構成されている。

[0047] 電子印影IDは、電子印影イメージを識別する為の識別情報である。

[0048] 電子印鑑IDは、電子印鑑装置14を識別する為の識別情報である。

[0049] 公開鍵は、電子印鑑装置14に記憶された秘密鍵に対応する暗号鍵である。公開鍵は、後述する信頼性確認情報の確認に用いられる。

[0050] 本実施形態では、電子印影イメージ及び電子印影IDが対応付けられて電子印鑑システムサーバ11のメモリ22に記憶されており、電子印影ID、電子印鑑ID、及び公開鍵が対応付けられて管理サーバ12のメモリ32に記憶されているものとして説明する。また、電子印鑑システムサーバ11のメモリ22には、電子承認記録を付与する対象の文書データも記憶されている。

[0051] 図3に示されるように、「契約書A」の文書データには、電子印影#1及び電子印影#2が関連付けられている。電子印影#1及び電子印影#2は、「契約書A」の文書データへの挿入する必要がある電子印影イメージの識別情報である。

[0052] 電子印影#1には、電子印鑑#1及び公開鍵#1が対応付けられている。

[0053] また、電子印影#2には、電子印鑑#2、電子印鑑#3、及び電子印鑑#

4などの電子印鑑IDと、公開鍵#2、公開鍵#3、及び公開鍵#4と、が対応付けられている。

[0054] なお、1つの電子印鑑装置14が、複数の電子印影IDに対応付けられていてもよい。

[0055] 次に、電子印鑑装置14に記憶されている情報について説明する。

図4は、電子印鑑装置14のセキュリティチップ55に記憶されている情報について説明する為の説明図である。

[0056] 図4に示されるように、電子印鑑装置14のセキュリティチップ55には、「電子印鑑ID」、「秘密鍵」、及び「生体情報」などが対応付けられて記憶されている。なお、電子印鑑装置14は、メモリ52に「電子印鑑ID」、「秘密鍵」、及び「生体情報」のいずれかまたは複数が記憶される構成であってもよい。

[0057] 秘密鍵は、管理サーバ12において、電子印鑑装置14の電子印鑑IDに対応付けられた公開鍵に対応する暗号鍵である。秘密鍵は、後述する信頼性確認情報の生成に用いられる。

[0058] 生体情報は、生体認証に用いられる情報である。生体情報は、例えば予めユーザの指紋の画像から特徴点などが抽出されて生成されたものである。

[0059] 図4に示されるように、電子印鑑IDが「電子印鑑#1」である電子印鑑装置14をユーザXYZが所持しているとする。この場合、ユーザXYZの生体情報である「生体情報#1」と、「秘密鍵#1」が、セキュリティチップ55のメモリに記憶されている。「秘密鍵#1」は、管理サーバ12において、「電子印鑑#1」に対応付けられた「公開鍵#1」に対応する暗号鍵である。

[0060] また、電子印鑑IDが「電子印鑑#2」である電子印鑑装置14をユーザAが所持しているとする。この場合、ユーザAの生体情報である「生体情報#2」と、「秘密鍵#2」が、セキュリティチップ55のメモリに記憶されている。「秘密鍵#2」は、管理サーバ12において、「電子印鑑#2」に対応付けられた「公開鍵#2」に対応する暗号鍵である。

- [0061] また、電子印鑑IDが「電子印鑑#3」である電子印鑑装置14をユーザBが所持しているとする。この場合、ユーザBの生体情報である「生体情報#3」と、「秘密鍵#3」が、セキュリティチップ55のメモリに記憶されている。「秘密鍵#3」は、管理サーバ12において、「電子印鑑#3」に対応付けられた「公開鍵#3」に対応する暗号鍵である。
- [0062] また、電子印鑑IDが「電子印鑑#4」である電子印鑑装置14が未登録（ユーザが登録されていない）とする。この場合、「秘密鍵#4」が、セキュリティチップ55のメモリに記憶され、生体情報がブランクとなっている。なお、「秘密鍵#4」は、管理サーバ12において、「電子印鑑#4」に対応付けられた「公開鍵#4」に対応する暗号鍵である。
- [0063] 電子印鑑システム1では、少なくとも1つ以上の電子印鑑装置14がユーザ（権限者）に対して提供される。権限者は、情報処理装置13により電子印鑑装置14の登録用WEBページにアクセスする。権限者は、電子印鑑装置14と情報処理装置13とを接続させ、電子印鑑装置14の生体センサ54により自身、もしくは、権限を与える者の生体情報（指紋画像）を読み取らせることにより、生体情報を電子印鑑装置14のセキュリティチップ55に登録させることができる。生体情報の登録が完了すると、電子印鑑装置14は、情報処理装置13を介して生体情報の登録が完了した旨を電子印鑑システムサーバ11に送信する。これにより、電子印鑑システムサーバ11において、電子印鑑装置14が無効から有効に切り替わる。
- [0064] 次に、電子印鑑システム1の動作の例について説明する。
- 図5は、電子印鑑システム1の動作について説明する為のシーケンス図である。なお、図5は、1人の権限者の承認によって文書データへの挿入が可能な電子印影に関する処理の例を示す。具体的には、図3の「電子印影#1」のようなケースである。
- [0065] 電子印鑑システムサーバ11のプロセッサ21は、文書データと、文書データに関連付けられた電子印影IDとに基づいて、承認用のURLを生成する（ステップS11）。例えば、承認用URLのWEBページには、文書デ

ータに基づく表示と、必要な電子印影イメージを示す情報（例えば電子印影 I D）と、承認が必要な電子印鑑装置 1 4 を示す情報（電子印鑑 I D）とを示す承認画面が表示される。

[0066] 例えば、電子印鑑システムサーバ 1 1 のプロセッサ 2 1 は、電子承認を必要とするユーザ（権限者または他のユーザ）が操作する端末から送信された情報に基づいて、承認用 URL の生成を行う。端末から送信された情報には、少なくとも電子印影 I D を示す情報が含まれている。プロセッサ 2 1 は、電子承認の対象のユーザ（電子印鑑装置 1 4 の所持者）の操作する情報処理装置 1 3 に承認用 URL を送信する（ステップ S 1 2）。なお、送信先を示す情報が、電子印鑑装置 1 4（または電子印鑑 I D）に対応付けられていてもよい。

[0067] 情報処理装置 1 3 のプロセッサ 4 1 は、操作インタフェース 4 5 の操作に基づいて承認用 URL にアクセスし、承認画面をディスプレイ 4 4 に表示する（ステップ S 1 3）。電子印鑑装置 1 4 の所持者、即ち権限者は、ディスプレイ 4 4 に表示された承認画面を視認することにより、自身が電子承認の対象のユーザであることを確認する。電子印鑑装置 1 4 の所持者は、電子承認の為の操作を操作インタフェース 4 5 により入力する。

[0068] プロセッサ 4 1 は、承認画面において操作を受け付けた場合（ステップ S 1 4）、電子印鑑装置 1 4 との間で通信を確立する（ステップ S 1 5）。

[0069] 電子印鑑システムサーバ 1 1 のプロセッサ 2 1 は、情報処理装置 1 3 と電子印鑑装置 1 4 との間で通信が確立された場合、情報処理装置 1 3 を介して電子印鑑装置 1 4 に対して承認要求を送信する（ステップ S 1 6）。

[0070] 電子印鑑装置 1 4 は、承認要求を受信すると、生体認証（本実施形態では指紋認証）を実行する（ステップ S 1 7）。例えば、電子印鑑装置 1 4 のプロセッサ 5 1 は、図示されないインジケータ、スピーカ、または情報処理装置 1 3 のディスプレイ 4 4 などに指紋認証の実行を権限者に対して促す表示を行う。プロセッサ 5 1 は、生体センサ 5 4 を起動する。プロセッサ 5 1 は、生体センサ 5 4 によって権限者の指紋の画像を取得する。プロセッサ 5 1

は、指紋画像をセキュリティチップ55に入力する。セキュリティチップ55は、予め設定されている生体情報（指紋から抽出された特徴点）と、入力された指紋画像とに基づいて、生体認証を行い、結果をプロセッサ51に出力する。

[0071] 電子印鑑装置14は、生体認証結果が正常である場合、セキュリティチップ55の乱数生成器により乱数を生成する（ステップS18）。例えば、プロセッサ51は、生体認証結果が正常である場合、乱数の生成をセキュリティチップ55に指示する。セキュリティチップ55は、乱数生成器により乱数を生成し、乱数をプロセッサ51に出力する。

[0072] さらに、電子印鑑装置14は、セキュリティチップ55の暗号回路により乱数を暗号化する（ステップS19）。具体的には、セキュリティチップ55は、予め記憶されている秘密鍵と、乱数とを暗号回路に入力し、乱数を秘密鍵によって暗号化した暗号化データを取得する。より具体的には、セキュリティチップ55は、秘密鍵と乱数とに基づいてハッシュ計算を行い、ハッシュ値を暗号化データとして取得する。セキュリティチップ55は、暗号化データ（ハッシュ値）をプロセッサ51に出力する。

[0073] 電子印鑑装置14のプロセッサ51は、乱数及び暗号化データを信頼性確認情報として、情報処理装置13を介して電子印鑑システムサーバ11に送信する（ステップS20）。即ち、電子印鑑装置14は、生体認証結果が正常である場合に、自身が記憶している秘密鍵を用いて生成した信頼性確認情報を電子印鑑システムサーバ11に送信する。

[0074] 電子印鑑システムサーバ11のプロセッサ21は、電子印鑑装置14から信頼性確認情報を受け取ると、信頼性確認情報と既に登録されている情報とに基づいて、電子印鑑装置14において正規の所持者（権限者）が承認したか否かを判定する。即ち、プロセッサ21は、既に登録されている「電子印影イメージ」、「電子印影ID」、「電子印鑑ID」、及び「公開鍵」などの情報と、信頼性確認情報と、に基づいて、電子印影イメージを文書データに付与するか否かを判断する。なお、電子印影イメージを付与するか否かを判断

する対象となる文書データ及び電子印影イメージは、ステップS 1 1で承認用URLの生成に用いた電子印影IDの電子印影イメージ及び文書データである。

[0075] まず、電子印鑑システムサーバ1 1のプロセッサ2 1は、電子印鑑装置1 4から受け取った信頼性確認情報と、電子印影IDとを管理サーバ1 2に対して送信する（ステップS 2 1）。

[0076] 管理サーバ1 2のプロセッサ3 1は、電子印鑑システムサーバ1 1から送信された電子印影IDに対応付けられている公開鍵をメモリ3 2から取得する（ステップS 2 2）。

[0077] プロセッサ3 1は、取得した公開鍵を用いて、信頼性確認情報の暗号化データ（ハッシュ値）を復号する（ステップS 2 3）。

[0078] プロセッサ3 1は、暗号化データを復号した値と、信頼性確認情報の乱数とを照合する（ステップS 2 4）。プロセッサ3 1は、暗号化データを復号した値と、信頼性確認情報の乱数とが一致する場合、照合結果が正常であると判断する。また、プロセッサ3 1は、暗号化データを復号した値と、信頼性確認情報の乱数とが一致しない場合、照合結果が異常であると判断する。なお、上述した例では、信頼性確認を行うためのデータとして乱数を用いたが、乱数以外のデータを秘密鍵で暗号化し、それらを信頼性確認情報とし利用することもできる。また、以下の実施例でも同様である。

[0079] プロセッサ3 1は、照合結果を電子印鑑システムサーバ1 1に送信する（ステップS 2 5）。

[0080] 電子印鑑システムサーバ1 1のプロセッサ2 1は、管理サーバ1 2からの照合結果に基づいて、承認記録を保存する（ステップS 2 6）。プロセッサ2 1は、管理サーバ1 2から受信した照合結果が正常である場合、電子承認記録として電子印影イメージを文書データに対応付けて保存する。

[0081] プロセッサ2 1は、承認結果を示す承認結果画面を生成し、情報処理装置1 3に送信する（ステップS 2 7）。例えば、プロセッサ2 1は、文書データの表示に電子印影イメージを重ねて表示させた画面を承認結果画面として

生成する。

[0082] 情報処理装置 1 3 のプロセッサ 4 1 は、受け取った承認結果を示す画面をディスプレイ 4 4 に表示させる（ステップ S 2 8）。これにより、情報処理装置 1 3 を操作する権限者は、電子承認記録が電子印鑑システムサーバ 1 1 において正常に記録されたことを確認することができる。

[0083] 上記したように、電子印鑑システム 1 の電子印鑑システムサーバ 1 1 のプロセッサ 2 1 は、電子印鑑装置 1 4 において秘密鍵を用いて生成された信頼性確認情報と、秘密鍵に対応する公開鍵とに基づく照合結果に基づいて、電子承認記録を保存する。これにより、電子印鑑システム 1 は、電子印鑑装置 1 4 に対応付けられた権限者が承認したという記録を文書データと対応付けて保存することができる。

[0084] このような構成によると、電子印影イメージの権限者が予め登録された人物であるものの、電子印影イメージが個人を示す印影に限定されない。また、電子印鑑装置 1 4 の所持者が操作する端末として、電子印鑑装置 1 4 及び電子印鑑システムサーバ 1 1 と通信可能な汎用的な情報処理装置 1 3 を用いることができる。

[0085] また、上記のような構成によると、電子印鑑システムサーバ 1 1 は、電子印鑑装置 1 4 から受け取った信頼性確認情報と電子印影 I D を外部サーバである管理サーバ 1 2 に送信し、管理サーバ 1 2 から照合結果を受け取る。即ち、電子印鑑システムサーバ 1 1 が、秘密鍵に対する公開鍵などの機密情報を管理する必要がなくなる。これにより、電子印鑑システムサーバ 1 1 のセキュリティに要するコストを削減することができる。

[0086] 次に、第 1 実施形態に係る電子印鑑システム 1 の動作の他の例について説明する。

図 6 は、電子印鑑システム 1 の動作の他の例について説明する為の説明図である。図 6 は、複数の権限者の承認によって文書データへの挿入が可能な電子印影に関する処理の例を示す。具体的には、図 3 の「電子印影 # 2」のようなケースである。

- [0087] 電子印鑑システムサーバ11のプロセッサ21は、文書データと、文書データに関連付けられた電子印影IDとに基づいて、承認用のURLを生成する（ステップS31）。例えば、承認用URLのWEBページには、文書データに基づく表示と、必要な電子印影イメージを示す情報（例えば電子印影ID）と、承認が必要な複数の電子印鑑装置14を示す情報（電子印鑑ID）とを示す承認画面が表示される。なお、電子印鑑装置14毎に、異なる承認画面（異なる承認用URL）が生成されてもよい。
- [0088] 電子印鑑システムサーバ11のプロセッサ21は、電子印鑑装置14毎に情報処理装置13に承認用URLを送信する（ステップS32）。なお、送信先を示す情報が、電子印鑑装置14（または電子印鑑ID）に対応付けられていてもよい。即ち、プロセッサ21は、電子印影IDに対応付けられた複数の電子印鑑IDに対応付けられた送信先に承認用URLを送信する。
- [0089] 電子印鑑装置14の所持者（権限者）は、情報処理装置13及び電子印鑑装置14によって、図5のステップS15乃至ステップS20の処理を行うことにより、電子印鑑システムサーバ11に対して信頼性確認情報を送信する。
- [0090] 電子印鑑システムサーバ11のプロセッサ21は、電子印鑑装置14から信頼性確認情報を受け取る（ステップS33）。プロセッサ21は、電子印鑑装置14から信頼性確認情報を受け取ると、信頼性確認情報と、電子印影IDとを管理サーバ12に対して送信する。
- [0091] 管理サーバ12のプロセッサ31は、電子印鑑システムサーバ11から送信された電子印影IDに対応付けられている1つの公開鍵をメモリ32から取得する（ステップS34）。
- [0092] プロセッサ31は、取得した公開鍵を用いて、信頼性確認情報の暗号化データ（ハッシュ値）を復号する（ステップS35）。
- [0093] プロセッサ31は、暗号化データを復号した値と、信頼性確認情報の乱数とを照合する（ステップS36）。プロセッサ31は、照合結果が正常であるか否か判断する（ステップS37）。プロセッサ31は、暗号化データを

復号した値と、信頼性確認情報の乱数とが一致する場合、照合結果が正常であると判断する。また、プロセッサ31は、暗号化データを復号した値と、信頼性確認情報の乱数とが一致しない場合、照合結果が異常であると判断する。

[0094] プロセッサ31は、照合結果が正常ではない（異常である）と判断した場合、未確認の公開鍵があるか否か判断する（ステップS38）。即ち、プロセッサ31は、電子印影IDに対応付けられた公開鍵のなかで、まだ照合に用いていない公開鍵が存在するか否か判断する。

[0095] プロセッサ31は、未確認の公開鍵があると判断した場合（ステップS38、YES）、ステップS34の処理を再度実行する。これにより、プロセッサ31は、他の公開鍵を取得し、照合を行う。

[0096] また、プロセッサ31は、未確認の公開鍵がないと判断した場合（ステップS38、NO）、異常を示す照合結果を電子印鑑システムサーバ11に送信する（ステップS39）。

[0097] また、プロセッサ31は、ステップS37において、照合結果が正常であると判断した場合（ステップS37、YES）、正常を示す照合結果を電子印鑑システムサーバ11に送信する（ステップS40）。また、プロセッサ31は、照合結果が正常であると判断した場合、暗号化データの複合に使用した公開鍵に対応する電子印鑑IDを、照合結果とともに電子印鑑システムサーバ11に送信する。

[0098] 電子印鑑システムサーバ11のプロセッサ21は、正常を示す照合結果を受信した場合、承認が行われた電子印鑑装置14を特定する（ステップS41）。例えば、プロセッサ21は、正常を示す照合結果とともに管理サーバ12から送信された電子印鑑IDに基づいて、承認が行われた電子印鑑装置14を特定する。即ち、電子印鑑システムサーバ11及び管理サーバ12は、どの公開鍵で照合結果が正常になったのかに基づいて、どの電子印鑑装置14で承認が行われたのかを判断することができる。さらに、プロセッサ21は、特定した結果に基づいて、ステップS31で承認用URLの生成に用

いた電子印影 I D に対応付けられた電子印鑑 I D の消し込みを行う。即ち、プロセッサ 2 1 は、承認用 U R L の生成に用いた電子印影 I D に対応付けられた複数の電子印鑑 I D から、正常を示す照合結果とともに管理サーバ 1 2 から送信された電子印鑑 I D を消し込む処理を行う。

[0099] プロセッサ 2 1 は、全ての照合が完了したか否か判断する（ステップ S 4 2）。即ち、プロセッサ 2 1 は、管理サーバ 1 2 に送信した電子印影 I D に対応付けられた複数の電子印鑑 I D のうち、正常を示す照合結果を受信しておらず、消し込みが行われていない電子印鑑 I D が存在するか否か判断する。プロセッサ 2 1 は、電子印影 I D に対応付けられた全ての電子印鑑 I D の消し込みが行われている場合、全ての照合が完了していると判断する。即ち、プロセッサ 2 1 は、電子印影 I D に対応付けられた全ての電子印鑑装置 1 4 において、権限者による承認が行われたと判断する。

[0100] プロセッサ 2 1 は、全ての照合が完了していないと判断した場合（ステップ S 4 2、N O）、ステップ S 3 3 の処理に移行する。これにより、プロセッサ 2 1 は、他の電子印鑑装置 1 4 からの信頼性確認情報の送信を待つ。

[0101] また、プロセッサ 2 1 は、全ての照合が完了したと判断した場合（ステップ S 4 2、Y E S）、承認記録を保存し（ステップ S 4 3）、図 6 の処理を終了する。即ち、プロセッサ 2 1 は、電子印影 I D に対応付けられた全ての電子印鑑装置 1 4 の照合が正常に完了した場合、電子印影イメージを文書データに対応付けて保存する。

[0102] 上記したように、電子印鑑システム 1 の電子印鑑システムサーバ 1 1 のプロセッサ 2 1 は、複数の電子印鑑装置 1 4 において秘密鍵を用いて生成された信頼性確認情報と、秘密鍵に対応する公開鍵とに基づく照合結果に基づいて、電子承認記録を保存する。これにより、電子印鑑システム 1 は、複数の電子印鑑装置 1 4 にそれぞれ対応付けられた権限者が承認したという記録を文書データと対応付けて保存することができる。

[0103] このような構成によると、電子印鑑システム 1 は、複数の権限者の承認に基づき、複数の権限者がそれぞれ所持する電子印鑑装置 1 4 に対応付けられ

た電子承認記録を保存することができる。

[0104] なお、上記の例では、電子印鑑システムサーバ11が管理サーバ12に対して、信頼性確認情報及び電子印影IDを送信する。さらに、管理サーバ12が、電子印影IDに対応付けられた公開鍵を総当たりで信頼性確認情報の照合に用いると説明したが、この構成に限定されない。電子印鑑システムサーバ11は管理サーバ12に対して、信頼性確認情報のみを送信する構成であってもよい。この場合、管理サーバ12は、管理している公開鍵を総当たりで信頼性確認情報の照合に用いる。さらに、管理サーバ12は、照合結果が正常である公開鍵に対応付けられた電子印影IDと、照合結果とを電子印鑑システムサーバ11に対して送信する。このような構成によっても、電子印鑑システム1は、複数の権限者の承認に基づき、複数の権限者がそれぞれ所持する電子印鑑装置14に対応付けられた電子承認記録を保存することができる。

[0105] また、管理サーバ12は、公開鍵との照合結果を照合を行う毎に電子印鑑システムサーバ11に対して送信してもよい。この場合、電子印鑑システムサーバ11は、電子印鑑装置14から受信した信頼性確認情報と、電子印鑑装置14の電子印鑑IDと、電子印影IDとを管理サーバ12に対して送信する。また、この場合、管理サーバ12は、電子印影IDと、電子印鑑IDと、公開鍵とを対応付けてメモリ32に記憶している。管理サーバ12は、受信した電子印影IDに対応し、且つ受信した電子印鑑IDに対応付けられている公開鍵と、受信した信頼性確認情報に基づいて、照合を行う。管理サーバ12は、照合結果（正常または異常）を電子印鑑システムサーバ12に送信する。このような構成によっても、電子印鑑システム1は、複数の権限者の承認に基づき、複数の権限者がそれぞれ所持する電子印鑑装置14に対応付けられた電子承認記録を保存することができる。このような構成によると、管理サーバ12が保持している公開鍵を総当たりで照合する必要がなくなる。この為、管理サーバ12の処理負荷を軽減することができる。

[0106] なお、上記の例では、電子印鑑システム1は、電子印影IDに対応付けら

れた全ての電子印鑑装置 1 4 の所持者（権限者）の承認に基づき、電子承認記録を保存すると説明したが、この構成に限定されない。電子印鑑システム 1 は、電子印影 I D に対応付けられた複数の電子印鑑装置 1 4 の所持者（権限者）のいずれかの承認に基づき、電子承認記録を保存する構成であってもよい。この場合、電子印鑑システムサーバ 1 1 のプロセッサ 2 1 は、図 6 のステップ S 4 2 を省略することにより、上記構成を実現することができる。

[0107] （第 2 実施形態）

図 7 は、第 2 の実施形態に係る電子印鑑システム 1 について説明する為の説明図である。第 2 の実施形態に係る電子印鑑システム 1 は、管理サーバ 1 2 の機能を電子印鑑システムサーバ 1 1 が備える点が第 1 の実施形態と異なる。なお、電子印鑑システムサーバ 1 1 のハードウェアの構成は第 1 実施形態と同様である為、同じ参照符号を付し、構成の説明を省略する。また、本例では、電子印鑑システムサーバ 1 1 のメモリ 2 2 に、電子印影イメージの挿入対象の文書データ、「電子印影イメージ」、「電子印影 I D」、「電子印鑑 I D」、及び「公開鍵」が対応付けられて記憶されている。

[0108] 電子印鑑システムサーバ 1 1 のプロセッサ 2 1 は、文書データと、文書データに関連付けられた電子印影 I D とに基づいて、承認用の URL を生成する（ステップ S 5 1）。

[0109] プロセッサ 2 1 は、電子承認の対象のユーザ（電子印鑑装置 1 4 の所持者）の操作する情報処理装置 1 3 に承認用 URL を送信する（ステップ S 5 2）。

[0110] 情報処理装置 1 3 のプロセッサ 4 1 は、操作インタフェース 4 5 の操作に基づいて承認用 URL にアクセスし、承認画面をディスプレイ 4 4 に表示する（ステップ S 5 3）。

[0111] プロセッサ 4 1 は、承認画面において操作を受け付けた場合（ステップ S 5 4）、電子印鑑装置 1 4 との間で無線通信を確立する（ステップ S 5 5）。

[0112] 電子印鑑システムサーバ 1 1 のプロセッサ 2 1 は、情報処理装置 1 3 と電

子印鑑装置 1 4 との間で無線通信が確立された場合、情報処理装置 1 3 を介して電子印鑑装置 1 4 に対して承認要求を送信する（ステップ S 5 6）。

[0113] 電子印鑑装置 1 4 は、承認要求を受信すると、生体認証（本実施形態では指紋認証）を実行する（ステップ S 5 7）。

[0114] 電子印鑑装置 1 4 は、生体認証結果が正常である場合、セキュリティチップ 5 5 の乱数生成器により乱数を生成する（ステップ S 5 8）。

[0115] さらに、電子印鑑装置 1 4 は、セキュリティチップ 5 5 の暗号回路により乱数を暗号化する（ステップ S 5 9）。

[0116] 電子印鑑装置 1 4 のプロセッサ 5 1 は、乱数及び暗号化データを信頼性確認情報として、情報処理装置 1 3 を介して電子印鑑システムサーバ 1 1 に送信する（ステップ S 6 0）。

[0117] 電子印鑑システムサーバ 1 1 のプロセッサ 2 1 は、電子印鑑装置 1 4 から信頼性確認情報を受け取ると、信頼性確認情報と既に登録されている情報とに基づいて、電子印鑑装置 1 4 において正規の所持者（権限者）が承認したか否かを判定する。

[0118] まず、電子印鑑システムサーバ 1 1 のプロセッサ 2 1 は、ステップ S 5 1 で承認用 URL の生成に用いた電子印影 ID に対応付けられている公開鍵をメモリ 2 2 から取得する（ステップ S 6 1）。

[0119] プロセッサ 2 1 は、取得した公開鍵を用いて、信頼性確認情報の暗号化データ（ハッシュ値）を復号する（ステップ S 6 2）。

[0120] プロセッサ 2 1 は、暗号化データを復号した値と、信頼性確認情報の乱数とを照合する（ステップ S 6 3）。プロセッサ 2 1 は、暗号化データを復号した値と、信頼性確認情報の乱数とが一致する場合、照合結果が正常であると判断する。また、プロセッサ 2 1 は、暗号化データを復号した値と、信頼性確認情報の乱数とが一致しない場合、照合結果が異常であると判断する。

[0121] プロセッサ 2 1 は、照合結果に基づいて、承認記録を保存する（ステップ S 6 4）。プロセッサ 2 1 は、照合結果が正常である場合、電子承認記録として電子印影イメージを文書データに対応付けて保存する。

[0122] プロセッサ 21 は、承認結果を示す承認結果画面を生成し、情報処理装置 13 に送信する（ステップ S65）。

[0123] 情報処理装置 13 のプロセッサ 41 は、受け取った承認結果を示す画面をディスプレイ 44 に表示させる（ステップ S66）。これにより、情報処理装置 13 を操作する権限者は、電子承認記録が電子印鑑システムサーバ 11 において正常に記録されたことを確認することができる。

[0124] 上記したように、電子印鑑システム 1 の管理サーバ 12 を省略することができる。これにより、電子印鑑システム 1 の構成を簡略化することができる。

[0125] （第 3 実施形態）

図 8 は、第 3 実施形態に係る電子承認システムである電子署名システム 2 について説明する為の説明図である。第 3 の実施形態に係る電子署名システム 2 は、電子印鑑装置 14 の代わりにペン型の電子署名装置を用いる点が第 1 実施形態と異なる。なお、第 1 実施形態と同様の構成の詳細な説明を省略し、異なる点について説明する。

[0126] 電子署名システム 2 は、電子署名システムサーバ 16、管理サーバ 12、情報処理装置 13、及び少なくとも 1 つ以上の電子署名装置 17などを備える。

[0127] 電子署名システムサーバ 16 は、電子承認に関する処理を行う電子承認サーバである。電子署名システムサーバ 16 は、プロセッサ 21、メモリ 22、及び通信部 23 を備える。即ち、電子署名システムサーバ 16 は、電子印鑑システムサーバ 11 と同様の構成を備える。

[0128] 電子署名装置 17 は、文書データに電子署名イメージを挿入する為にユーザが操作する装置である。電子署名装置 17 は、ユーザの生体情報（例えば指紋、静脈パターン、虹彩、顔特徴など）に基づいて生体認証を行う。

[0129] 電子署名装置 17 は、プロセッサ 51、メモリ 52、通信部 53、生体センサ 54、セキュリティチップ 55、及びバッテリー 56 を備える。また、電子印鑑装置 14 は、図示されないインジケータ、またはスピーカなどを備え

ていてもよい。即ち、電子署名装置 1 7 は、電子印鑑装置 1 4 と同様の構成を備える。

[0130] さらに、電子署名装置 1 7 は、後述する電子署名イメージを生成する機能を有する。

[0131] 例えば、電子署名装置 1 7 は、タッチパネルとして構成された情報処理装置 1 3 に対して操作信号を与えるポインティングデバイスとして構成される。この場合、電子署名装置 1 7 のユーザが、電子署名装置 1 7 を用いて情報処理装置 1 3 のディスプレイ 4 4 上で署名操作を行う。情報処理装置 1 3 のプロセッサ 4 1 は、電子署名装置 1 7 の軌跡に基づいて、電子署名イメージを生成する。

[0132] また、例えば、電子署名装置 1 7 は、単体で電子署名イメージを生成するように構成されていてもよい。例えば、電子署名装置 1 7 は、照明と照明からの反射光を読み取るセンサとを備え、センサの出力に基づいて、電子署名装置 1 7 の軌跡を判断し、電子署名イメージを生成してもよい。

[0133] 次に、電子署名システムサーバ 1 6 のメモリ 2 2、または管理サーバ 1 2 のメモリ 3 2 に記憶されている情報について説明する。

図 9 は、電子署名システムサーバ 1 6 のメモリ 2 2、または管理サーバ 1 2 のメモリ 3 2 に記憶されている情報について説明する為の説明図である。

[0134] 本例では、電子署名システムサーバ 1 6 のメモリ 2 2、または管理サーバ 1 2 のメモリ 3 2 に、電子承認記録を付与する対象の文書データ、「電子署名装置 ID」、及び「公開鍵」が対応付けられて記憶されている。また、電子署名システムサーバ 1 6 のメモリ 2 2、または管理サーバ 1 2 のメモリ 3 2 には、「電子署名 ID」及び「電子署名イメージ」が記憶される記憶領域が「電子署名装置 ID」と対応付けられて設けられている。「電子署名 ID」及び「電子署名イメージ」は、後述する登録処理によって、電子署名システムサーバ 1 6 のメモリ 2 2、または管理サーバ 1 2 のメモリ 3 2 に記憶される。

[0135] 電子署名イメージは、文書データに付与される電子承認記録の一形態であ

る。電子署名イメージは、例えば文書データ上に重ねられて表示される（挿入される）画像として構成されている。電子署名イメージは、上記の電子署名装置 17 によって生成された画像である。

- [0136] 電子署名 ID は、電子署名イメージを識別する為の識別情報である。
- [0137] 電子署名装置 ID は、電子署名装置 17 を識別する為の識別情報である。
- [0138] 本実施形態では、電子署名イメージ及び電子署名 ID の記憶領域が電子署名システムサーバ 16 のメモリ 22 に設けられており、電子署名 ID の記憶領域、電子署名装置 ID、及び公開鍵が対応付けられて管理サーバ 12 のメモリ 32 に記憶されているものとして説明する。また、電子署名システムサーバ 16 のメモリ 22 には、電子承認記録を付与する対象の文書データも記憶されている。
- [0139] 図 9 に示されるように、「契約書 B」の文書データには、電子署名 # 1 が関連付けられている。電子印影 # 1 は、「契約書 B」の文書データへの挿入する必要がある電子署名イメージの識別情報である。
- [0140] 電子署名 # 1 には、電子署名装置 # 1 及び公開鍵 # 1 が対応付けられている。
- [0141] なお、1 つの電子署名装置 17 が、複数の電子署名 ID に対応付けられていてもよい。
- [0142] 次に、電子署名装置 17 に記憶されている情報について説明する。
- 図 10 は、電子署名装置 17 のセキュリティチップ 55 に記憶されている情報について説明する為の説明図である。
- [0143] 図 10 に示されるように、電子署名装置 17 のセキュリティチップ 55 には、「電子署名装置 ID」、「秘密鍵」、及び「生体情報」などが対応付けられて記憶されている。なお、電子署名装置 17 は、メモリ 52 に「電子署名装置 ID」、「秘密鍵」、及び「生体情報」のいずれかまたは複数記憶される構成であってもよい。
- [0144] 秘密鍵は、管理サーバ 12 において、電子署名装置 17 の電子署名装置 ID に対応付けられた公開鍵に対応する暗号鍵である。秘密鍵は、信頼性確認

情報の生成に用いられる。

[0145] 図10に示されるように、電子署名装置IDが「電子署名装置#1」である電子署名装置17をユーザDEFが所持しているとする。この場合、ユーザDEFの生体情報である「生体情報#1」と、「秘密鍵#1」が、セキュリティチップ55のメモリに記憶されている。「秘密鍵#1」は、管理サーバ12において、「電子署名装置#1」に対応付けられた「公開鍵#1」に対応する暗号鍵である。

[0146] 電子署名システム2では、少なくとも1つ以上の電子署名装置17がユーザ（権限者）に対して提供される。権限者は、情報処理装置13により電子署名装置17の登録用WEBページにアクセスする。権限者は、電子署名装置17と情報処理装置13とを接続させる。権限者は、電子署名装置17及び情報処理装置13によって、電子署名装置17の操作に応じた電子署名イメージを生成させる。さらに、電子署名装置17の生体センサ54により自身の生体情報（指紋画像）を読み取らせることにより、生体情報を電子署名装置17のセキュリティチップ55に登録させることができる。生体情報の登録が完了すると電子署名装置17は、情報処理装置13を介して生体情報の登録が完了した旨、電子署名イメージ、及び電子署名装置IDを電子署名システムサーバ16に送信する。これにより、電子署名システムサーバ16において、電子署名装置17が無効から有効に切り替わる。

[0147] 図11は、電子署名システム2の動作について説明する為のシーケンス図である。なお、図11は、1人の権限者の承認によって文書データへの挿入が可能な電子署名に関する処理の例を示す。

[0148] 電子署名システムサーバ16のプロセッサ21は、文書データと、文書データに関連付けられた電子署名IDとに基づいて、承認用のURLを生成する（ステップS71）。例えば、承認用URLのWEBページには、文書データに基づく表示と、電子署名が必要な旨を示す情報とを示す承認画面が表示される。

[0149] 例えば、電子署名システムサーバ16のプロセッサ21は、電子承認の対

象のユーザ（電子署名装置１７の所持者）の操作する情報処理装置１３に承認用ＵＲＬを送信する（ステップＳ７１）。

[0150] 情報処理装置１３のプロセッサ４１は、操作インタフェース４５の操作に基づいて承認用ＵＲＬにアクセスし、承認画面をディスプレイ４４に表示する（ステップＳ７３）。電子署名装置１７の所持者、即ち権限者は、ディスプレイ４４に表示された承認画面を視認することにより、自身が電子承認の対象のユーザであることを確認する。電子署名装置１７の所持者は、電子承認の為の操作を操作インタフェース４５により入力する。

[0151] プロセッサ４１は、承認画面において操作を受け付けた場合（ステップＳ７４）、電子署名装置１７との間で無線通信を確立する（ステップＳ７５）。

[0152] 電子署名装置１７の所持者は、情報処理装置１３及び電子署名装置１７により電子署名イメージを生成する為の操作を行う（ステップＳ７６）。即ち、権限者は、電子署名装置１７及び情報処理装置１３によって、電子署名装置１７の操作に応じた電子署名イメージを生成させる。

[0153] また、電子署名システムサーバ１６のプロセッサ２１は、情報処理装置１３と電子署名装置１７との間で無線通信が確立された場合、情報処理装置１３を介して電子署名装置１７に対して承認要求を送信する（ステップＳ７７）。

[0154] 電子署名装置１７は、承認要求を受信すると、生体認証（本実施形態では指紋認証）を実行する（ステップＳ７８）。例えば、電子署名装置１７のプロセッサ５１は、図示されないインジケータ、スピーカ、または情報処理装置１３のディスプレイ４４などに指紋認証の実行を権限者に対して促す表示を行う。プロセッサ５１は、生体センサ５４を起動する。プロセッサ５１は、生体センサ５４によって権限者の指紋の画像を取得する。プロセッサ５１は、指紋画像をセキュリティチップ５５に入力する。セキュリティチップ５５は、予め設定されている生体情報（指紋から抽出された特徴点）と、入力された指紋画像とに基づいて、生体認証を行い、結果をプロセッサ５１に出

力する。

- [0155] 電子署名装置 17 は、生体認証結果が正常である場合、セキュリティチップ 55 の乱数生成器により乱数を生成する（ステップ S79）。例えば、プロセッサ 51 は、生体認証結果が正常である場合、乱数の生成をセキュリティチップ 55 に指示する。セキュリティチップ 55 は、乱数生成器により乱数を生成し、乱数をプロセッサ 51 に出力する。
- [0156] さらに、電子署名装置 17 は、セキュリティチップ 55 の暗号回路により乱数を暗号化する（ステップ S80）。具体的には、セキュリティチップ 55 は、予め記憶されている秘密鍵と、乱数とを暗号回路に入力し、乱数を秘密鍵によって暗号化した暗号化データを取得する。より具体的には、セキュリティチップ 55 は、秘密鍵と乱数とに基づいてハッシュ計算を行い、ハッシュ値を暗号化データとして取得する。セキュリティチップ 55 は、暗号化データ（ハッシュ値）をプロセッサ 51 に出力する。
- [0157] 電子署名装置 17 のプロセッサ 51 は、乱数及び暗号化データを信頼性確認情報として、情報処理装置 13 を介して電子署名システムサーバ 16 に送信する（ステップ S81）。電子署名装置 17 のプロセッサ 51 は、生成した電子署名イメージと、電子署名装置 ID とを信頼性確認情報とともに送信する。即ち、電子署名装置 17 は、生体認証結果が正常である場合に、自身が記憶している秘密鍵を用いて生成した信頼性確認情報と、電子署名イメージと、電子署名装置 ID とを電子署名システムサーバ 16 に送信する。なお、情報処理装置 13 が、ステップ S76 で生成された電子署名イメージを一時的に保存しておき、電子署名システムサーバ 16 に送信する構成であってもよい。
- [0158] 電子署名システムサーバ 16 のプロセッサ 21 は、電子署名装置 17 から信頼性確認情報を受け取ると、信頼性確認情報と既に登録されている情報とに基づいて、電子署名装置 17 において正規の所持者（権限者）が承認したか否かを判定する。即ち、プロセッサ 21 は、既に登録されている「電子署名装置 ID」、及び「公開鍵」などの情報と、信頼性確認情報と、に基づい

て、電子署名イメージを文書データに付与するか否か判断する。

- [0159] まず、電子署名システムサーバ16のプロセッサ21は、電子署名装置17から受け取った信頼性確認情報と、電子署名装置IDとを管理サーバ12に対して送信する（ステップS82）。
- [0160] 管理サーバ12のプロセッサ31は、電子署名システムサーバ16から送信された電子署名装置IDに対応付けられている公開鍵をメモリ32から取得する（ステップS83）。
- [0161] プロセッサ31は、取得した公開鍵を用いて、信頼性確認情報の暗号化データ（ハッシュ値）を復号する（ステップS84）。
- [0162] プロセッサ31は、暗号化データを復号した値と、信頼性確認情報の乱数とを照合する（ステップS85）。
- [0163] プロセッサ31は、照合結果を電子署名システムサーバ16に送信する（ステップS86）。
- [0164] 電子署名システムサーバ16のプロセッサ21は、管理サーバ12からの照合結果に基づいて、承認記録を保存する（ステップS87）。プロセッサ21は、管理サーバ12から受信した照合結果が正常である場合、電子承認記録として、情報処理装置13及び電子署名装置17から送信された電子署名イメージを文書データに対応付けて保存する。
- [0165] また、電子署名システムサーバ16のプロセッサ21は、管理サーバ12からの照合結果に基づいて、電子署名イメージ及び電子署名IDをメモリ22に保存する（ステップS88）。即ち、プロセッサ21は、管理サーバ12から受信した照合結果が正常である場合、ステップS81で情報処理装置13及び電子署名装置17から送信された電子署名イメージと電子署名IDと電子署名装置IDとを対応付けてメモリ22に保存する登録処理を行う。また、プロセッサ21は、電子署名IDと電子署名装置IDとを対応付け、管理サーバ12に送信する。管理サーバ12のプロセッサ31は、電子署名IDと電子署名装置IDとを対応付け、メモリ32に保存する。
- [0166] さらに、電子署名システムサーバ16のプロセッサ21は、承認結果を示

す承認結果画面を生成し、情報処理装置 13 に送信する（ステップ S 89）。例えば、プロセッサ 21 は、文書データの表示に電子署名イメージを重ねて表示させた画面を承認結果画面として生成する。

[0167] 情報処理装置 13 のプロセッサ 41 は、受け取った承認結果を示す画面をディスプレイ 44 に表示させる（ステップ S 90）。これにより、情報処理装置 13 を操作する権限者は、電子承認記録が電子署名システムサーバ 16 において正常に記録されたことを確認することができる。

[0168] 上記したように、電子署名システム 2 の電子署名システムサーバ 16 のプロセッサ 21 は、電子署名装置 17 において秘密鍵を用いて生成された信頼性確認情報と、秘密鍵に対応する公開鍵とに基づく照合結果に基づいて、電子承認記録を保存する。これにより、電子署名システム 2 は、電子署名装置 17 に対応付けられた権限者が承認したという記録を文書データと対応付けて保存することができる。

[0169] このような構成によると、第 1 の実施形態のように、電子印影イメージが予め登録されていない場合であっても、権限者の署名の画像を電子承認記録として登録することができる。

[0170] なお、上述の各実施の形態で説明した機能は、ハードウェアを用いて構成するに留まらず、ソフトウェアを用いて各機能を記載したプログラムをコンピュータに読み込ませて実現することもできる。また、各機能は、適宜ソフトウェア、ハードウェアのいずれかを選択して構成するものであっても良い。また、本実施形態に係るプログラムは、電子機器に記憶された状態で譲渡されてもよいし、電子機器に記憶されていない状態で譲渡されてもよい。後者の場合は、プログラムは、ネットワークを介して譲渡されてよいし、記憶媒体に記憶された状態で譲渡されてもよい。記憶媒体は、非一時的な有形の媒体である。記憶媒体は、コンピュータ可読媒体であり、電子印鑑システムサーバ 11 及び電子印鑑装置 14 等により読み取られ、実行される。記憶媒体は、CD-ROM、メモリカード等のプログラムを記憶可能かつコンピュータで読取可能な媒体であればよく、その形態は問わない。

[0171] 本発明のいくつかの実施形態を説明したが、これらの実施形態は、例として提示したものであり、発明の範囲を限定することは意図していない。これら新規な実施形態は、その他の様々な形態で実施されることが可能であり、発明の要旨を逸脱しない範囲で、種々の省略、置き換え、変更を行うことができる。これら実施形態やその変形は、発明の範囲や要旨に含まれるとともに、特許請求の範囲に記載された発明とその均等の範囲に含まれる。

請求の範囲

- [請求項1] 少なくとも1つ以上の電子承認装置と、電子承認サーバとを備える電子承認システムであって、
- 前記電子承認装置は、
- 情報処理装置を介して前記電子承認サーバと通信する第1通信部と、
- 、
- 生体認証を行う生体認証部と、
- 前記生体認証の結果が正常である場合、予め記憶された秘密鍵を用いて信頼性確認情報を生成し、前記情報処理装置を介して前記信頼性確認情報を前記電子承認サーバに送信するセキュリティチップと、
- を具備し、
- 前記電子承認サーバは、
- 前記情報処理装置を介して前記電子承認装置と通信する第2通信部と、
- 、
- 前記秘密鍵に対応する公開鍵と、前記信頼性確認情報と、に基づいて、前記電子承認装置における承認が正常に実行されたことを示す電子承認記録を保存するプロセッサと、
- を具備する電子承認システム。
- [請求項2] 前記プロセッサは、前記電子承認記録に対応付けられた異なる秘密鍵がそれぞれ設定された複数の前記電子承認装置において生成された信頼性確認情報と、前記電子承認装置毎の前記秘密鍵にそれぞれ対応した公開鍵と、に基づいて、前記電子承認記録を保存する請求項1に記載の電子承認システム。
- [請求項3] 前記プロセッサは、
- 前記電子承認記録に対応付けられた全ての前記電子承認装置において承認が正常に実行された場合、前記電子承認記録を保存する、
- 請求項2に記載の電子承認システム。
- [請求項4] 前記電子承認記録は、電子印影イメージであり、

前記プロセッサは、文書データに前記電子印影イメージを挿入することにより、前記電子承認記録を保存する請求項 1 乃至 3 のいずれか 1 項に記載の電子承認システム。

[請求項5]

前記プロセッサは、

前記電子承認装置から受け取った前記信頼性確認情報及び前記電子承認記録を識別する為の電子承認記録識別情報を外部サーバに送信し、

前記電子承認装置における承認が正常に実行されたか否かを示す情報を前記外部サーバから受け取る請求項 1 乃至 4 のいずれか 1 項に記載の電子承認システム。

[請求項6]

前記電子承認記録は、電子署名イメージであり、

前記プロセッサは、文書データに前記電子署名イメージを挿入することにより、前記電子承認記録を保存する請求項 1 乃至 3 のいずれか 1 項に記載の電子承認システム。

[請求項7]

前記信頼性確認情報は、乱数と、前記乱数が秘密鍵によって暗号化された暗号化データであり、

前記プロセッサは、前記公開鍵によって復号した前記暗号化データと前記乱数とが一致する場合、前記電子承認記録を保存する請求項 1 乃至 6 のいずれか 1 項に記載の電子承認システム。

[請求項8]

生体認証を行う生体認証部と、前記生体認証の結果が正常である場合、予め記憶された秘密鍵を用いて信頼性確認情報を生成するセキュリティチップと、を備える電子承認装置と情報処理装置を介して通信する通信部と、

前記秘密鍵に対応する公開鍵と、前記信頼性確認情報と、に基づいて、前記電子承認装置における承認が正常に実行されたことを示す電子承認記録を保存するプロセッサと、

を具備する電子承認サーバ。

[請求項9]

少なくとも 1 つ以上の電子承認装置と、電子承認サーバとにおいて

実行される電子承認プログラムであって、

前記電子承認プログラムを実行することにより、前記電子承認装置は、

情報処理装置を介して前記電子承認サーバと通信し、

生体認証を行い、

前記生体認証の結果が正常である場合、予め記憶された秘密鍵を用いて信頼性確認情報を生成し、

前記情報処理装置を介して前記信頼性確認情報を前記電子承認サーバに送信し、

前記電子承認プログラムを実行することにより、前記電子承認サーバは、

前記情報処理装置を介して前記電子承認装置と通信し、

前記秘密鍵に対応する公開鍵と、前記信頼性確認情報と、に基づいて、前記電子承認装置における承認が正常に実行されたことを示す電子承認記録を保存する、

電子承認プログラム。

[請求項10]

電子承認装置に、

情報処理装置を介して電子承認サーバと通信させることと、

生体認証を行わせることと、

前記生体認証の結果が正常である場合、予め記憶された秘密鍵を用いて信頼性確認情報を生成させることと、

前記情報処理装置を介して前記信頼性確認情報を前記電子承認サーバに送信させることと、を実行させ

前記電子承認サーバに、

前記情報処理装置を介して前記電子承認装置と通信させることと、

前記秘密鍵に対応する公開鍵と、前記信頼性確認情報と、に基づいて、前記電子承認装置における承認が正常に実行されたことを示す電子承認記録を保存させることと、を実行させる電子承認プログラムを

記憶したコンピュータ可読記憶媒体。