(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2007-184857
(P2007-184857A)
(43)公開日　平成19年7月19日(2007.7.19)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/32	(2006.01)	H04L	9/00	675Z	5J104
G06Q 50/00	(2006.01)	H04L	9/00	673D	
B65G 61/00	(2006.01)	G06F	17/60	114	
		G06F	17/60	140	
		B65G	61/00	520	

審査請求 有　請求項の数 9　ＯＬ　（全 22 頁）

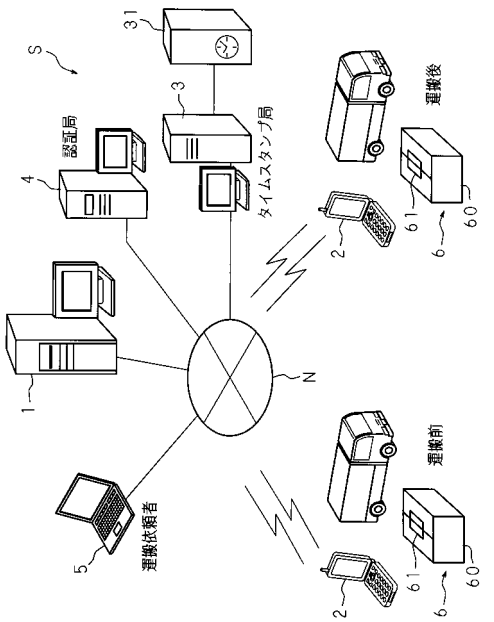
(21)出願番号　特願2006-2791 (P2006-2791)
(22)出願日　平成18年1月10日 (2006.1.10)

(71)出願人　503059884
有限会社カテナス
山口県宇部市南小羽山町２丁目４番１３号
(74)代理人　100078868
弁理士　河野　登夫
(74)代理人　100114557
弁理士　河野　英仁
(72)発明者　吉村　克生
山口県宇部市南小羽山町２丁目４番１３号
有限会社カテナス内

Ｆターム(参考)　5J104 AA11　MA01　PA07　PA10

(54)【発明の名称】認証方法、認証装置、認証システム及びコンピュータプログラム

(57)【要約】
【課題】運搬される物品が漏洩等されていないことを客観的に証明することが可能な認証方法を提供する。
【解決手段】携帯電話機２は運搬前の物品６の封止状況を撮像した画像データ及びタイムスタンプ生成装置３により生成されたタイムスタンプに関するデータをサーバコンピュータ１へ送信する。サーバコンピュータ１は、送信された画像データ及びタイムスタンプに関するデータを用いて、運搬前の画像データ及び時刻を認証する。認証が得られた場合、サーバコンピュータ１は識別情報を携帯電話機２へ送信する。携帯電話機２は、運搬後の画像データ、タイムスタンプに関するデータ、及び識別情報をサーバコンピュータ１へ送信する。サーバコンピュータ１は、識別情報、画像データ及びタイムスタンプに関するデータを用いて、運搬後の画像データ及び時刻を認証する。
【選択図】図１



【特許請求の範囲】
【請求項１】
運搬する物品の認証を行う認証装置を用いた認証方法において、
運搬前の物品の封止状況を撮像した画像データ及び該画像データに対するタイムスタンプに関するデータを前記認証装置の制御部により受信する運搬前受信ステップと、
前記制御部により前記画像データ及びタイムスタンプに関するデータを用いて運搬前の画像データ及び時刻を認証する運搬前認証ステップと、
認証が得られた場合に、識別情報を前記制御部により送信する識別情報送信ステップと、
運搬後の物品の封止状況を撮像した画像データ、該画像データに対するタイムスタンプに関するデータ及び識別情報を前記制御部により受信する運搬後受信ステップと、
受信した識別情報、画像データ及びタイムスタンプに関するデータを用いて、前記制御部により運搬後の画像データ及び時刻を認証する運搬後認証ステップと
を備えることを特徴とする認証方法。
【請求項２】
運搬する物品の認証を行う認証装置、該認証装置に通信網を介して接続された情報処理装置及びタイムスタンプ生成装置を用いた認証方法において、
撮像手段を有する情報処理装置の制御部により運搬前の物品の封止状況を撮像した画像データに関するデータを、前記タイムスタンプ生成装置へ送信するステップと、
タイムスタンプ生成装置により生成されたタイムスタンプに関するデータ及び運搬前の画像データを前記情報処理装置の制御部により前記認証装置へ送信するステップと、
前記送信された画像データ及びタイムスタンプに関するデータを用いて、前記認証装置の制御部により運搬前の画像データ及び時刻を認証する運搬前認証ステップと、
認証が得られた場合に、識別情報を前記認証装置の制御部により前記情報処理装置へ送信する識別情報送信ステップと、
前記認証装置から送信された識別情報を前記情報処理装置により受信するステップと、
前記撮像手段により運搬後の物品の封止状況を撮像した画像データに関するデータを、前記情報処理装置の制御部によりタイムスタンプ生成装置へ送信するステップと、
タイムスタンプ生成装置により生成されたタイムスタンプに関するデータ、運搬後の画像データ及び前記識別情報を前記情報処理装置の制御部により前記認証装置へ送信するステップと、
前記送信された識別情報、画像データ及びタイムスタンプに関するデータを用いて、前記認証装置の制御部により運搬後の画像データ及び時刻を認証する運搬後認証ステップと
を備えることを特徴とする認証方法。
【請求項３】
運搬する物品の認証を行う認証装置において、
運搬前の物品の封止状況を撮像した画像データ及び該画像データに対するタイムスタンプに関するデータを受信する運搬前受信手段と、
前記画像データ及びタイムスタンプに関するデータを用いて運搬前の画像データ及び時刻を認証する運搬前認証手段と、
認証が得られた場合に、識別情報を送信する識別情報送信手段と、
運搬後の物品の封止状況を撮像した画像データ、該画像データに対するタイムスタンプに関するデータ及び識別情報を受信する運搬後受信手段と、
受信した識別情報、画像データ及びタイムスタンプに関するデータを用いて運搬後の画像データ及び時刻を認証する運搬後認証手段と
を備えることを特徴とする認証装置。
【請求項４】
前記運搬前認証手段及び運搬後認証手段により認証が得られた場合に、デジタル署名付きの証明書を生成する生成手段
をさらに備えることを特徴とする請求項３に記載の認証装置。

【請求項５】
前記生成手段は、前記運搬前認証手段及び運搬後認証手段により認証が得られた場合に、デジタル証明書がさらに付属されたデジタル署名付きの証明書を生成するよう構成してあることを特徴とする請求項４に記載の認証装置。
【請求項６】
識別情報に対応付けて、認証済みの運搬前の画像データ及びタイムスタンプ、並びに、運搬後の画像データ及びタイムスタンプを記憶する手段
をさらに備えることを特徴とする請求項３乃至５のいずれか一つに記載の認証装置。
【請求項７】
前記運搬後認証手段は、受信した識別情報と前記識別情報送信手段により送信した識別情報とが一致するか否かを判断し、一致する場合に、画像データ及びタイムスタンプに関するデータを用いて運搬後の画像データ及び時刻を認証するよう構成してあることを特徴とする請求項３乃至６のいずれか一つに記載の認証装置。
【請求項８】
請求項３乃至７のいずれか一つに記載の認証装置に通信網を介して接続された情報処理装置及びタイムスタンプ生成装置を有する認証システムにおいて、
前記情報処理装置は、
撮像手段と、
撮像手段により運搬前の物品の封止状況を撮像した画像データに関するデータを、前記タイムスタンプ生成装置へ送信する手段と、
タイムスタンプ生成装置により生成されたタイムスタンプに関するデータ及び運搬前の画像データを前記認証装置へ送信する手段と、
前記認証装置から送信された識別情報を受信する手段と、
前記撮像手段により運搬後の物品の封止状況を撮像した画像データに関するデータを、通信網を介して接続されるタイムスタンプ生成装置へ送信する手段と、
タイムスタンプ生成装置により生成されたタイムスタンプに関するデータ、運搬後の画像データ及び前記識別情報を前記認証装置へ送信する手段と
を備えることを特徴とする認証システム。
【請求項９】
運搬する物品の認証を行うコンピュータに用いられるコンピュータプログラムにおいて、
コンピュータの制御部に、受信した運搬前の物品の封止状況を撮像した画像データ及び該画像データに対するタイムスタンプに関するデータを用いて運搬前の画像データ及び時刻を認証させる運搬前認証ステップと、
コンピュータの制御部に、認証が得られた場合に、識別情報を送信させる識別情報送信ステップと、
コンピュータの制御部に、受信した運搬後の物品の封止状況を撮像した画像データ、該画像データに対するタイムスタンプに関するデータ及び識別情報を用いて運搬後の画像データ及び時刻を認証させる運搬後認証ステップと
を備えることを特徴とする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、運搬する物品の認証を行う認証方法、認証装置、認証システム及びコンピュータを認証装置として機能させるためのコンピュータプログラムに関する。
【背景技術】
【０００２】
個人情報保護法の施行に伴い、個人情報取扱事業者は、情報主体（個人情報の提供者）からの要請に応えて、個人情報の入手、加工、訂正及び廃棄の全ての過程にわたってその経過を情報主体に説明する法的義務が生じた。そのため、個人情報取扱事業者またはこの

事業者の委託を受けた事業者が、個人情報を運搬または廃棄のため運搬する場合に、個人情報が漏洩することなく安全に運搬されたことを、客観的証拠をもって情報主体に説明する必要が生じていた。

【０００３】

産業廃棄物等を搬送または廃棄のため運搬する場合は、産業廃棄物管理票（マニフェスト）を用いることによって、これらの廃棄物が確実に廃棄されるシステムとなっている（例えば特許文献１乃至５）。特許文献１に開示された運搬回収システムは、運搬業者が回収地において回収情報入力端末装置を用いて、運搬車両の位置情報の送信を行い、回収管理センタは、この位置情報が適正であるかの認証を行う。

さらに、処理場においても運搬業者は同様に位置情報の送信を行い、回収管理センタ側で地点認証を行う。

【特許文献１】特開２００４－３４２０２８号公報
【特許文献２】特開２００２－２１５８２４号公報
【特許文献３】特開２００２－３１４５２８号公報
【特許文献４】特開２００４－３１８６１７号公報
【特許文献５】特開２００５－２０２７６８号公報

【発明の開示】

【発明が解決しようとする課題】

【０００４】

しかしながら、特許文献１乃至５に開示された技術は、物品を搬送または廃棄のため運搬する場合に、物品が確実に破棄されたことを示すものであり、運搬中に第３者による物品の不正取得、物品の内部情報の漏洩または改竄があった場合でもこれを把握することはできなかった。また、物品の不正取得、物品の内部情報の漏洩または改竄が無かったとしても、これを客観的に証明する術はなかった。特許文献１に開示された運搬管理システムは、運搬前に運搬業者を搬送業者ＩＤ及びパスワードで認証すると共に、運搬車両の位置認証を行っているが、運搬中の物品の盗難、漏洩または改竄が無かったことを客観的に証明することはできない。

【０００５】

本発明は斯かる事情に鑑みてなされたものであり、その目的は、物品の封止状況を撮像した画像データ及びタイムスタンプ生成装置により生成されたタイムスタンプに関するデータを、運搬前及び運搬後に認証装置により認証することにより、運搬される物品が運搬中に盗難、漏洩または改竄されていないことを客観的に証明することが可能な認証方法、認証装置、認証システム、コンピュータを認証装置として機能させるためのコンピュータプログラムを提供することにある。

【０００６】

また、本発明の他の目的は、運搬前の認証及び運搬後の認証双方による認証が得られた場合に、デジタル署名付きの証明書を生成、さらには認証機関が発行するデジタル証明書を付属することにより、客観的に運搬中に物品が盗難、漏洩または改竄されていないことを保証すると共に、この証明書自体の改竄及びなりすましを防止することが可能な認証装置等を提供することにある。

【課題を解決するための手段】

【０００７】

本発明に係る認証方法は、運搬する物品の認証を行う認証装置を用いた認証方法において、運搬前の物品の封止状況を撮像した画像データ及び該画像データに対するタイムスタンプに関するデータを前記認証装置の制御部により受信する運搬前受信ステップと、前記制御部により前記画像データ及びタイムスタンプに関するデータを用いて運搬前の画像データ及び時刻を認証する運搬前認証ステップと、認証が得られた場合に、識別情報を前記制御部により送信する識別情報送信ステップと、運搬後の物品の封止状況を撮像した画像データ、該画像データに対するタイムスタンプに関するデータ及び識別情報を前記制御部により受信する運搬後受信ステップと、受信した識別情報、画像データ及びタイムスタン

プに関するデータを用いて、前記制御部により運搬後の画像データ及び時刻を認証する運搬後認証ステップとを備えることを特徴とする。

【０００８】

本発明に係る認証方法は、運搬する物品の認証を行う認証装置、該認証装置に通信網を介して接続された情報処理装置及びタイムスタンプ生成装置を用いた認証方法において、撮像手段を有する情報処理装置の制御部により運搬前の物品の封止状況を撮像した画像データに関するデータを、前記タイムスタンプ生成装置へ送信するステップと、タイムスタンプ生成装置により生成されたタイムスタンプに関するデータ及び運搬前の画像データを前記情報処理装置の制御部により前記認証装置へ送信するステップと、前記送信された画像データ及びタイムスタンプに関するデータを用いて、前記認証装置の制御部により運搬前の画像データ及び時刻を認証する運搬前認証ステップと、認証が得られた場合に、識別情報を前記認証装置の制御部により前記情報処理装置へ送信する識別情報送信ステップと、前記認証装置から送信された識別情報を前記情報処理装置により受信するステップと、前記撮像手段により運搬後の物品の封止状況を撮像した画像データに関するデータを、前記情報処理装置の制御部によりタイムスタンプ生成装置へ送信するステップと、タイムスタンプ生成装置により生成されたタイムスタンプに関するデータ、運搬後の画像データ及び前記識別情報を前記情報処理装置の制御部により前記認証装置へ送信するステップと、前記送信された識別情報、画像データ及びタイムスタンプに関するデータを用いて、前記認証装置の制御部により運搬後の画像データ及び時刻を認証する運搬後認証ステップとを備えることを特徴とする。

【０００９】

本発明に係る認証装置は、運搬する物品の認証を行う認証装置において、運搬前の物品の封止状況を撮像した画像データ及び該画像データに対するタイムスタンプに関するデータを受信する運搬前受信手段と、前記画像データ及びタイムスタンプに関するデータを用いて運搬前の画像データ及び時刻を認証する運搬前認証手段と、認証が得られた場合に、識別情報を送信する識別情報送信手段と、運搬後の物品の封止状況を撮像した画像データ、該画像データに対するタイムスタンプに関するデータ及び識別情報を受信する運搬後受信手段と、受信した識別情報、画像データ及びタイムスタンプに関するデータを用いて運搬後の画像データ及び時刻を認証する運搬後認証手段とを備えることを特徴とする。

【００１０】

本発明に係る認証装置は、前記運搬前認証手段及び運搬後認証手段により認証が得られた場合に、デジタル署名付きの証明書を生成する生成手段をさらに備えることを特徴とする。

【００１１】

本発明に係る認証装置は、前記生成手段は、前記運搬前認証手段及び運搬後認証手段により認証が得られた場合に、デジタル証明書がさらに付属されたデジタル署名付きの証明書を生成するよう構成してあることを特徴とする。

【００１２】

本発明に係る認証装置は、識別情報に対応付けて、認証済みの運搬前の画像データ及びタイムスタンプ、並びに、運搬後の画像データ及びタイムスタンプを記憶する手段をさらに備えることを特徴とする。

【００１３】

本発明に係る認証装置は、前記運搬後認証手段は、受信した識別情報と前記識別情報送信手段により送信した識別情報とが一致するか否かを判断し、一致する場合に、画像データ及びタイムスタンプに関するデータを用いて運搬後の画像データ及び時刻を認証するよう構成してあることを特徴とする。

【００１４】

本発明に係る認証システムは、上述のいずれか一つの認証装置に通信網を介して接続された情報処理装置及びタイムスタンプ生成装置を有する認証システムにおいて、前記情報処理装置は、撮像手段と、撮像手段により運搬前の物品の封止状況を撮像した画像データ

に関するデータを、前記タイムスタンプ生成装置へ送信する手段と、タイムスタンプ生成装置により生成されたタイムスタンプに関するデータ及び運搬前の画像データを前記認証装置へ送信する手段と、前記認証装置から送信された識別情報を受信する手段と、前記撮像手段により運搬後の物品の封止状況を撮像した画像データに関するデータを、通信網を介して接続されるタイムスタンプ生成装置へ送信する手段と、タイムスタンプ生成装置により生成されたタイムスタンプに関するデータ、運搬後の画像データ及び前記識別情報を前記認証装置へ送信する手段とを備えることを特徴とする。

【００１５】

本発明に係るコンピュータプログラムは、運搬する物品の認証を行うコンピュータに用いられるコンピュータプログラムにおいて、コンピュータの制御部に、受信した運搬前の物品の封止状況を撮像した画像データ及び該画像データに対するタイムスタンプに関するデータを用いて運搬前の画像データ及び時刻を認証させる運搬前認証ステップと、コンピュータの制御部に、認証が得られた場合に、識別情報を送信させる識別情報送信ステップと、コンピュータの制御部に、受信した運搬後の物品の封止状況を撮像した画像データ、該画像データに対するタイムスタンプに関するデータ及び識別情報を用いて運搬後の画像データ及び時刻を認証させる運搬後認証ステップとを備えることを特徴とする。

【００１６】

本発明にあっては、認証システムは、運搬する物品の認証を行う認証装置、該認証装置に通信網を介して接続された情報処理装置及びタイムスタンプ生成装置により構成される。運搬前に、情報処理装置の撮像手段により、物品の封止状況を撮像する。情報処理装置の制御部は運搬前の物品の封止状況を撮像した画像データに関するデータを、タイムスタンプ生成装置へ送信する。情報処理装置は、タイムスタンプ生成装置により生成されたタイムスタンプに関するデータ及び運搬前の画像データを認証装置へ送信する。認証装置の制御部は、送信された画像データ及びタイムスタンプに関するデータを用いて、運搬前の画像データ及び時刻を認証する。認証が得られた場合、認証装置の制御部は識別情報を情報処理装置へ送信する。情報処理装置は、認証装置から送信された識別情報を受信する。

【００１７】

運搬後、情報処理装置の撮像手段により物品の封止状況を再び撮像する。情報処理装置は、運搬後の画像データに関するデータを、タイムスタンプ生成装置へ送信する。情報処理装置の制御部は、タイムスタンプ生成装置により生成されたタイムスタンプに関するデータ、運搬後の画像データ及び識別情報を認証装置へ送信する。そして認証装置の制御部は、送信された識別情報、画像データ及びタイムスタンプに関するデータを用いて、運搬後の画像データ及び時刻を認証する。このように、運搬前に封止状況を撮像した画像データに対するタイムスタンプに関するデータを取得し、これを認証装置で認証できた場合に、識別情報を付与し、運搬後には、同様に運搬後の封止状況を撮像した画像データ、タイムスタンプに関するデータさらには付与した識別情報に基づいて認証を行うこととしたので、運搬対象の物品が運搬前後において改竄不可能な画像データ及びタイムスタンプにより認証できる結果、客観的に運搬される物品が運搬中に盗難、漏洩または改竄されていないことを証明することが可能となる。

【００１８】

また、本発明にあっては、運搬前における認証及び運搬後における認証により認証が得られた場合に、デジタル署名付きの証明書を生成する。さらには、証明書にデジタル証明書を付属させる。このように認証装置において、物品が運搬中に盗難、漏洩または改竄されていないことを示す客観的な証明書を、認証機関による高い安全性をもって個人情報取扱事業者等に提供することが可能となる。

【発明の効果】

【００１９】

本発明にあっては、運搬前に封止状況を撮像した画像データに対するタイムスタンプに関するデータを取得し、これを認証装置で認証できた場合に、識別情報を付与し、運搬後には、同様に運搬後の封止状況を撮像した画像データ、タイムスタンプに関するデータさ

らには付与した識別情報に基づいて認証を行うこととしたので、運搬対象の物品が運搬前後において改竄不可能な画像データ及びタイムスタンプにより認証できる結果、客観的に運搬される物品が運搬中に盗難、漏洩または改竄されていないことを証明することが可能となる。

【００２０】

また、本発明にあっては、認証装置において、物品が運搬中に盗難、漏洩または改竄されていないことを示す客観的な証明書を、認証機関による高い安全性をもって個人情報取扱事業者等に提供することが可能となる。また個人情報取扱事業者は、自身で物品を運搬する場合または運搬を委託する場合においても、依頼者からの開示請求に応じて、本発明による証明書を高い信頼性、安全性及び客観性を伴って提供することができる等、本発明は優れた効果を奏する。

【発明を実施するための最良の形態】

【００２１】

実施の形態１

以下本発明の実施の形態を、図面を参照して説明する。図１は本発明に係る認証システムの概要を示す模式図である。図１においてＳは認証システムであり、認証を行う認証装置１、情報処理装置２、タイムスタンプ局のタイムスタンプ生成装置３、認証局の認証局コンピュータ４及び運搬依頼者のコンピュータ５等を含んで構成される。認証装置１は例えば、サーバコンピュータ（以下サーバコンピュータ１）が用いられ、インターネット及び携帯電話網を含む通信網Ｎに接続されている。情報処理装置２はカメラ機能（図３参照）及び通信機能等を有する装置であり、例えば携帯電話機、ＰＤＡまたはパーソナルコンピュータが用いられる。以下では情報処理装置２を携帯電話機２であるものとして説明する。

【００２２】

タイムスタンプ局におけるタイムスタンプ生成装置３は、通信網Ｎに接続され処理対象の画像データ等に対し、時刻源３１から得られる基準時間に基づいてタイムスタンプを付与し、画像データが「いつ」の時点で存在し、それ以降改ざんされずに証拠性を保っている事を第三者的に証明するものである。このタイムスタンプ生成装置３はアマノタイムビジネス株式会社のデジタルタイムスタンプサービスまたはセイコーインスツル株式会社のタイムスタンプサービスを利用すればよい。

【００２３】

認証局の認証局コンピュータ４は通信網Ｎを介して接続されており、例えば日本ベリサイン株式会社が運営するコンピュータを利用する。運搬依頼者のコンピュータ５も通信網Ｎを介して接続されており、サーバコンピュータ１から、物品６の運搬が適正に行われたことを示す証明書を取得することができる。物品６は例えば個人情報が記述された紙媒体、または個人情報が記録された記録媒体であり、物品収納箱６０に格納されている。物品収納箱６０には物品６の封止を行う封止部６１が設けられている。この封止部６１は、例えば、サンワサプライ株式会社のセキュリティシールを用いることができ、これはシールを剥がした場合に、その痕跡を視覚的に確認することができるものである。

【００２４】

本発明の概要を以下に説明する。まず運搬依頼者の立ち会いの下、運搬を行う作業者が、物品６を物品収納箱６０へ格納し、封止部６１にて封止する。そして作業者は携帯電話機２のカメラを用いて、物品６の封止状況を撮像する。これは、物品収納箱６０が封止部６１により、確実に封止されていることを認識することが可能な画像であれば良く、静止画または動画のいずれであっても良い。作業者はタイムスタンプ生成装置３へ画像データに関するデータ、例えば画像データのハッシュ値、を送信する。タイムスタンプ生成装置３はこのハッシュ値にタイムスタンプを付与し、生成したハッシュ値を含むタイムスタンプを携帯電話機２へ送信する。

【００２５】

その後作業者は、携帯電話機２からサーバコンピュータ１へアクセスし、撮像した画像

データ及びタイムスタンプに関するデータを送信する。サーバコンピュータ１は、送信された画像データ及びタイムスタンプに関するデータを用いて認証を行う。なお、タイムスタンプを用いた認証手順については後述する。そして認証が得られた場合に、この運搬作業に固有の識別情報を生成し、携帯電話機２へ送信する。

【００２６】

運搬作業者は運搬元から運搬先へ移動した場合、同様に携帯電話機２のカメラを用いて、必要に応じて運搬先の運搬依頼者の立ち会いの下、物品６の封止状況を撮像する。ここで、封止部６１に開封したことを示す印がついていた場合、または運搬収納箱６０が破壊されている場合などは、封止されているとはいえず、最終的な認証は行われない。運搬後の物品６０の封止状況を撮像した画像に関するデータは再びタイムスタンプ生成装置３へ送信され、タイムスタンプ生成装置３は生成したタイムスタンプに関するデータを携帯電話機２へ送信する。携帯電話機２はサーバコンピュータ１へ運搬後の画像データ及びタイムスタンプに関するデータ、そして送信された識別情報を送信する。

【００２７】

サーバコンピュータ１は、送信された識別情報がサーバコンピュータ１に存在するか否かを判断し、存在する場合、運搬後の画像データ及びタイムスタンプに関するデータを用いて認証を行う。識別情報がサーバコンピュータ１に存在し、かつ運搬前及び運搬後において画像データが存在しタイムスタンプによる認証が得られた場合に、デジタル署名付きの証明書を生成する。この場合、認証局コンピュータ４が発行するデジタル証明書をさらに付属しても良い。なお、この証明書には、運搬前の画像データ及びタイムスタンプ、並びに、運搬後の画像データ及びタイムスタンプを含ませても良い。運搬依頼者等は、情報が漏洩することなく運搬されたことを示す証明書を、コンピュータ５を用いてサーバコンピュータ１から受信することができ、その安全性は認証局コンピュータ４により確保される。

【００２８】

図２はサーバコンピュータ１のハードウェア構成を示すブロック図である。サーバコンピュータ１は、制御部としてのＣＰＵ(Central Processing Unit)１１、ＲＡＭ(Random Access Memory)１２、入力部１３、表示部１４、通信部１６及び記憶部１５を含んで構成される。ＣＰＵ１１は、バス１７を介してサーバコンピュータ１のハードウェア各部と接続されていて、それらを制御すると共に、記憶部１５に格納された制御プログラム１５３に従って、種々のソフトウェア的機能を実行する。制御プログラムは、Ｃ言語等のプログラミング言語で記述されている。

【００２９】

表示部１４は例えば液晶ディスプレイ等であり、入力部１３はキーボード及びマウス等から構成される。通信部１６はＬＡＮカード等であり、携帯電話機２との間で情報を送受信する。記憶部１５は例えばハードディスクで構成され、内部には上述した制御プログラム１５３、生体情報ファイル１５１、画像データベース１５２及びタイムスタンプ認証プログラム１５４等が記憶されている。なお、生体情報ファイル１５１及び画像データベース１５２の詳細については後述する。また、記憶部１５に記憶されている生体情報ファイル１５１及び画像データベース１５２は必ずしもサーバコンピュータ１内に設ける必要はなく図示しないデータベースコンピュータに記憶するようにしても良い。

【００３０】

図３は携帯電話機２のハードウェア構成を示すブロック図である。携帯電話機２は、制御部としてのＣＰＵ２１、ＲＡＭ２２、入力部２３、表示部２４、通信部２６、撮像手段であるカメラ２９、生体情報取得部２８、及び、タイムスタンプ認証プログラム２５１が記憶された記憶部２５を含んで構成される。ＣＰＵ２１は、バス２７を介して携帯電話機２のハードウェア各部と接続されていて、それらを制御すると共に、記憶部２５に格納された制御プログラムに従って、種々のソフトウェア的機能を実行する。

【００３１】

表示部２４は例えば液晶ディスプレイ等であり、入力部２３はプッシュボタン等により

構成される。なお、タッチパネルのように表示部２４と入力部２３とを一体的に構成するようにしても良い。カメラ２９は撮像した画像データをＣＰＵ２１へ出力し、ＣＰＵ２１は出力された画像データを記憶部２５に記憶する。通信部２６は高周波送受信部及びアンテナ等を備え、画像データ等を含む各種データの送受信を行う。生体情報取得部２８は、例えば指紋センサ等から構成され、入力された指紋等の生体情報をＣＰＵ２１へ出力する。なお、生体情報は指紋の他、声紋または眼球奥の虹彩等を利用すればよい。

【００３２】

図４はサーバコンピュータ１に記憶される生体情報ファイル１５１のレコードレイアウトを示す説明図である。生体情報ファイル１５１は作業者ＩＤフィールド、作業者氏名フィールド、作業者生体情報フィールド及びＭＡＣ（Media Access Control）アドレスフィールドを含んで構成される。作業者ＩＤフィールドには、運搬作業を行う作業者のＩＤが記憶されており、これに対応付けて、作業者氏名、作業者の生体情報、作業者が使用する携帯電話機２のＭＡＣアドレスが記憶されている。作業者ＩＤ、作業者氏名等の情報はサーバコンピュータ１の入力部１３から、オペレータが適宜入力すればよい。また生体情報及びＭＡＣアドレスは携帯電話機２から送信される情報を元に、生体情報ファイル１５１へ登録すればよい。

【００３３】

作業者氏名フィールドには、作業者の氏名が記憶されており、作業者生体情報フィールドには、各作業者の指紋データ等の生体情報が記憶されている。ＭＡＣアドレスフィールドには携帯電話機２固有の機器情報であるＭＡＣアドレスが記憶されている。なお本実施の形態においては情報処理装置である携帯電話機２を特定するための固有の情報としてＭＡＣアドレスを用いたが、これ以外にも携帯電話機２の電話番号、ＩＰ(Internet Protocol)アドレス等を利用しても良い。サーバコンピュータ１は携帯電話機２からアクセスがあった場合、作業者ＩＤ及びパスワードの他、作業者生体情報を用いたバイオメトリクス認証を行い、さらにＭＡＣアドレスを用いて機器の認証を行うことにより、運搬前後の作業者のなりすましを防止する。なお、図４においては図示しないが、作業者ＩＤに対応付けてパスワードも記憶しても良い。

【００３４】

図５は画像データベース１５２のレコードレイアウトを示す説明図である。画像データベース１５２は作業番号フィールド、識別情報フィールド、運搬前画像データフィールド、運搬前タイムスタンプフィールド、運搬後画像データフィールド及び運搬後タイムスタンプフィールドを含んで構成される。サーバコンピュータ１のＣＰＵ１１は各データベースのフィールドのキーを関連づけたスキーマにおいてＳＱＬ(Structured Query Language)を用いて対話することにより、必要な情報の記憶、検索等の処理を実行する。作業番号フィールドには、運搬作業毎に作業番号が付与されて記憶されており、各作業番号に対応付けて、識別情報、運搬前画像データ、運搬前タイムスタンプ、運搬後画像データ及び運搬後タイムスタンプが記憶されている。作業番号はサーバコンピュータ１の入力部１３から、オペレータが適宜番号を運搬作業毎に入力すればよい。

【００３５】

識別情報は、運搬前の画像データ及びタイムスタンプに関するデータを元に認証を得ることができた場合に、ＣＰＵ１１が生成する固有の識別情報である。この識別情報は例えば、作業番号等を含んだ他と重複しない識別情報を用いればよい。運搬前画像データフィールドには、作業者が携帯電話機２から送信した運搬前の物品６の封止状況を撮像した画像データが記憶されている。運搬前タイムスタンプフィールドには、運搬前の画像データに対応するタイムスタンプに関するデータが記憶されている。このタイムスタンプに関するデータはタイムスタンプ局の秘密鍵で暗号化されており、暗号化された画像データのハッシュ値及び時間情報が、運搬前タイムスタンプフィールドに記憶されている。

【００３６】

運搬後画像データフィールドには、作業者が携帯電話機２から送信した運搬後の物品６の封止状況を撮像した画像データが記憶されている。運搬前タイムスタンプフィールドに

は、運搬後の画像データに対応するタイムスタンプに関するデータが記憶されている。図５の例においては、作業番号「１０００」については、識別情報「ＸＸＸＸ１０００」が付与され、運搬前の画像データのタイムスタンプが、２００５年１２月８日１１時２５分００秒であり、さらに運搬後の画像データのタイムスタンプが２００５年１２月８日１５時１０分１０秒であることを示している。作業番号「２０００」については、識別情報「ＸＸＸＸ２０００」が付与され、運搬前の画像データのタイムスタンプが、２００５年１２月９日１６時０３分１０秒であるが、未だ運搬中で運搬後の画像データに関する認証が行われていないことが理解できる。また識別番号「３０００」に関しては、運搬前の画像データに関する認証が行われておらず、識別情報もＣＰＵ１１により付与されていない状態である。

【００３７】

以上のハードウェア構成において、本発明に係る認証処理手順を、フローチャートを用いて説明する。図６は運搬前の画像データのタイムスタンプに関するデータを取得する手順を示すフローチャートである。作業者は携帯電話機２のカメラ２９を用いて、運搬前の物品６の封止状況を撮像する（ステップＳ６１）。具体的には上述したように、物品６が格納された物品収納箱６０が封止部６１により封止された状態を運搬依頼者またはその代理人等の立ち会いのもと撮像する。撮像された運搬前の画像データは記憶部２５に記憶される。ＣＰＵ２１は記憶部２５に記憶したタイムスタンプ認証プログラム２５１を起動する（ステップＳ６２）。ＣＰＵ２１は撮像した画像データのハッシュ値を算出する（ステップＳ６３）。

【００３８】

ＣＰＵ２１は算出した画像データのハッシュ値を、画像データに関するデータとしてタイムスタンプ生成装置３へ送信する（ステップＳ６４）。タイムスタンプ生成装置３は画像データのハッシュ値が送信された時刻におけるタイムスタンプを生成する（ステップＳ６５）。タイムスタンプ生成装置３は、送信されたハッシュ値及びタイムスタンプをタイムスタンプ生成装置３が所有する秘密鍵で暗号化する（ステップＳ６６）。タイムスタンプ生成装置３は暗号化したハッシュ値及びタイムスタンプをタイムスタンプに関する情報として携帯電話機２へ送信する（ステップＳ６７）。携帯電話機２のＣＰＵ２１は暗号化されたハッシュ値及びタイムスタンプを受信し、記憶部２５に記憶する（ステップＳ６８）。

【００３９】

図７は運搬前の画像データ及びタイムスタンプに関する情報を送信する際の手順を示すフローチャートである。携帯電話機２のＣＰＵ２１はサーバコンピュータ１へアクセスし通信を確立する（ステップＳ７１）。サーバコンピュータ１は携帯電話機２へ本発明に係る認証システムへログインするためのログイン画面を、記憶部１５から読み出して送信する（ステップＳ７２）。図８は携帯電話機２の表示部２４に表示されるログイン画面のイメージを示す説明図である。図８に示すように、ログイン画面は例えばｃＨＴＭＬ（Compact HyperText Markup Language）形式等で記述されており、ＣＰＵ２１のブラウザはこれを解析して作業番号ボックス１３１、作業者ＩＤボックス１３２、パスワードボックス１３３、「生体情報を入力後、送信ボタンを操作してください」との情報及び送信ボタン１３４が表示されている。

【００４０】

作業者は、入力部２３を操作して作業番号を作業番号ボックス１３１へ、作業者ＩＤを作業者ＩＤボックス１３２へ、パスワードをパスワードボックス１３３へそれぞれ入力すると共に、生体情報取得部２８から生体情報を入力する（ステップＳ７３）。入力部２３及び生体情報取得部２８から入力されたこれらの情報はＣＰＵ２１へ出力され、送信ボタン１３４の操作をトリガーに、ＣＰＵ２１は出力された作業番号、作業者ＩＤ、パスワード及び生体情報をサーバコンピュータ１へ送信する（ステップＳ７４）。またＣＰＵ２１はサーバコンピュータ１との情報の送受信において携帯電話機２を特定するための固有の機器情報たるＭＡＣアドレスをサーバコンピュータ１へ送信する（ステップＳ７５）。こ

のＭＡＣアドレスの送信タイミングは、ステップＳ７１の直後であっても良い。

【００４１】

サーバコンピュータ１のＣＰＵ１１は送信された作業番号、作業者ＩＤ、パスワード、生体情報及びＭＡＣアドレスを受信し、これらをもとに、生体情報ファイル１５１を検索し、登録した作業者ＩＤ、パスワード、生体情報及びＭＡＣアドレスが、受信した作業者ＩＤ、パスワード、生体情報及びＭＡＣアドレスに一致するか否かを判断する（ステップＳ７６）。ＣＰＵ１１は一致しないと判断した場合は（ステップＳ７６でＮＯ）、不正アクセスであると判断し処理を終了する。一方ＣＰＵ１１は登録した作業者ＩＤ、パスワード、生体情報及びＭＡＣアドレスが、受信した作業者ＩＤ、パスワード、生体情報及びＭＡＣアドレスに一致すると判断した場合（ステップＳ７６でＹＥＳ）、画像データ及びタイムスタンプに関するデータの取得要求画面を記憶部１５から読み出して携帯電話機２へ送信する（ステップＳ７７）。

【００４２】

図９は画像データ及びタイムスタンプに関するデータを入力する際のイメージを示す説明図である。携帯電話機２の表示部２４には、作業番号、認証のため送信される画像データボックス１３５、画像データのサムネイルボックス１３６、撮像日時、タイムスタンプ取得の有無及び送信ボタン１３４等が表示される。ユーザはステップＳ６１において撮像した認証に供すべき画像データを選択する（ステップＳ７８）。ＣＰＵ２１は入力部２３の操作により画像データが選択された場合、画像データのファイル名またはパスを画像データボックス１３５に表示する。またＣＰＵ２１は記憶部２５に記憶した画像データを読み出すと共に、画像データのサムネイルをサムネイルボックス１３６に表示する（ステップＳ７９）。

【００４３】

さらに、ＣＰＵ２１は読み出した画像データの撮像日時を表示部２４へ出力する。また、ＣＰＵ２１は選択された画像データに対応するタイムスタンプが、ステップＳ６８の処理により記憶部２５に記憶されていると判断した場合、図９に示すようにＣＰＵ２１は「タイムスタンプ取得済」の表示を表示部２４に行う。作業者は表示部２４において認証に用いる画像データを確認し、またタイムスタンプが取得済みであることをも確認した上で、送信ボタン１３４を操作する。

【００４４】

ＣＰＵ２１は入力部２３から送信ボタン１３４の操作信号を受信した場合、選択された画像データに対応するタイムスタンプに関するデータ、すなわち画像データに対応する暗号化されたハッシュ値及びタイムスタンプを記憶部２５から読み出す（ステップＳ７１０）。ＣＰＵ２１は読み出した画像データ並びに暗号化されたハッシュ値及びタイムスタンプをサーバコンピュータ１へ送信する（ステップＳ７１１）。サーバコンピュータ１のＣＰＵ１１は、画像データベース１５２に、ステップＳ７４で送信された作業番号に対応付けて、ステップＳ７１１において送信された画像データ並びに暗号化されたハッシュ値及びタイムスタンプを記憶する（ステップＳ７１２）。

【００４５】

図１０は運搬前の画像データ及びタイムスタンプに関するデータの認証処理手順を示すフローチャートである。サーバコンピュータ１のＣＰＵ１１は画像データベース１５２から画像データ並びに暗号化されたハッシュ値及びタイムスタンプを読み出す（ステップＳ８１）。ＣＰＵ１１はタイムスタンプ認証プログラム１５４を起動する（ステップＳ８２）。ＣＰＵ１１はタイムスタンプ認証プログラム１５４に従い、読み出した運搬前の画像データのハッシュ値を算出する（ステップＳ８３）。ＣＰＵ１１はタイムスタンプ生成装置３の公開鍵を、例えば認証局の認証局コンピュータ４等から取得する（ステップＳ８４）。

【００４６】

ＣＰＵ１１は取得した公開鍵を用いて暗号化されたハッシュ値及びタイムスタンプの復号を行う（ステップＳ８５）。ＣＰＵ１１は復号したハッシュ値とステップＳ８３におい

て算出したハッシュ値とが一致するか否かを判断する（ステップＳ８６）。ＣＰＵ１１は一致しないと判断した場合（ステップＳ８６でＮＯ）、画像データに変更または改竄が加えられたと判断し、携帯電話機２または運搬依頼者のコンピュータ５へエラー信号を送信し処理を終了する。一方、ハッシュ値が一致するとＣＰＵ１１が判断した場合（ステップＳ８６でＹＥＳ）、タイムスタンプに記述された確定時刻に画像データが存在しており、かつ、画像データが確定時刻以降不正に改竄されていないと判断し、識別情報を生成する（ステップＳ８７）。ＣＰＵ１１はこの識別情報を画像データベース１５２に、作業番号に対応付けて記憶する。

【００４７】

ＣＰＵ１１はこの識別情報を携帯電話機２へ送信する（ステップＳ８８）。携帯電話機２のＣＰＵ２１は送信された識別情報を受信し（ステップＳ８９）、記憶部２５に識別情報を記憶する（ステップＳ８１０）。

【００４８】

作業者は運搬元から運搬先へ移動し、運搬後の物品６の封止状況を示す画像を撮像する。図１１は運搬後の画像データのタイムスタンプに関するデータを取得する手順を示すフローチャートである。作業者は携帯電話機２のカメラ２９を用いて、運搬後の物品６の封止状況を撮像する（ステップＳ１１１）。具体的には上述したように、物品６が格納された物品収納箱６０が封止部６１により封止された状態を必要に応じて運搬先の運搬依頼者またはその代理人等の立ち会いのもと運搬先で撮像する。撮像された運搬後の画像データは記憶部２５に記憶される。ＣＰＵ２１は記憶部２５に記憶したタイムスタンプ認証プログラム２５１を起動する（ステップＳ１１２）。ＣＰＵ２１は撮像した画像データのハッシュ値を算出する（ステップＳ１１３）。

【００４９】

ＣＰＵ２１は算出した画像データのハッシュ値を、画像データに関するデータとしてタイムスタンプ生成装置３へ送信する（ステップＳ１１４）。タイムスタンプ生成装置３は画像データのハッシュ値が送信された時刻におけるタイムスタンプを生成する（ステップＳ１１５）。タイムスタンプ生成装置３は、送信されたハッシュ値及びタイムスタンプをタイムスタンプ生成装置３が所有する秘密鍵で暗号化する（ステップＳ１１６）。タイムスタンプ生成装置３は暗号化したハッシュ値及びタイムスタンプをタイムスタンプに関するデータとして携帯電話機２へ送信する（ステップＳ１１７）。携帯電話機２のＣＰＵ２１は暗号化されたハッシュ値及びタイムスタンプを受信し、記憶部２５に記憶する（ステップＳ１１８）。

【００５０】

図１２及び図１３は運搬後の画像データ及びタイムスタンプに関する情報を送信する際の手順を示すフローチャートである。携帯電話機２のＣＰＵ２１はサーバコンピュータ１へアクセスし通信を確立する（ステップＳ１２１）。サーバコンピュータ１は携帯電話機２へ本発明に係る認証システムへログインするためのログイン画面を、記憶部１５から読み出して携帯電話機２へ送信する（ステップＳ１２２）。

【００５１】

作業者は、入力部２３を操作して作業番号を作業番号ボックス１３１へ、作業者ＩＤを作業者ＩＤボックス１３２へ、パスワードをパスワードボックス１３３へそれぞれ入力すると共に、生体情報取得部２８から生体情報を入力する（ステップＳ１２３）。入力部２３及び生体情報取得部２８から入力されたこれらの情報はＣＰＵ２１へ出力され、送信ボタン１３４の操作をトリガーに、ＣＰＵ２１は出力された作業番号、作業者ＩＤ、パスワード及び生体情報をサーバコンピュータ１へ送信する（ステップＳ１２４）。またＣＰＵ２１はサーバコンピュータ１との情報の送受信において携帯電話機２を特定するための固有の機器情報たるＭＡＣアドレスをサーバコンピュータ１へ送信する（ステップＳ１２５）。

【００５２】

サーバコンピュータ１のＣＰＵ１１は送信された作業番号、作業者ＩＤ、パスワード、

生体情報及びＭＡＣアドレスを受信し、これらをもとに、生体情報ファイル１５１を検索し、登録した作業者ＩＤ、パスワード、生体情報及びＭＡＣアドレスが、受信した作業者ＩＤ、パスワード、生体情報及びＭＡＣアドレスに一致するか否かを判断する（ステップＳ１２６）。ＣＰＵ１１は一致しないと判断した場合は（ステップＳ１２６でＮＯ）、不正アクセスであると判断し処理を終了する。一方ＣＰＵ１１は登録した作業者ＩＤ、パスワード、生体情報及びＭＡＣアドレスが、受信した作業者ＩＤ、パスワード、生体情報及びＭＡＣアドレスに一致すると判断した場合（ステップＳ１２６でＹＥＳ）、本作業番号に対応する識別情報の取得を携帯電話機２へ要求する（ステップＳ１２７）。

【００５３】

作業者は携帯電話機２の入力部２３からステップＳ８９において受信した識別情報を入力する（ステップＳ１２８）。なお識別情報は入力部２３から直接入力することのほか、ステップＳ８１０において記憶部２５に記憶した識別情報をＣＰＵ２１により読み出すようにしても良い。ＣＰＵ２１は入力されたまたは読み出された識別情報をサーバコンピュータ１へ送信する（ステップＳ１２９）。

【００５４】

サーバコンピュータ１のＣＰＵ１１は作業番号をもとに画像データベース１５２を検索し、記憶された識別情報と、送信された識別情報とが一致するか否かを判断する（ステップＳ１２１０）。ＣＰＵ１１は識別情報が一致しないと判断した場合（ステップＳ１２１０でＮＯ）、不正アクセス、運搬前の画像データが存在しない、または運搬前の画像データ及びタイムスタンプに対する認証が得られていないと判断し処理を終了する。一方、ＣＰＵ１１は識別情報が一致すると判断した場合（ステップＳ１２１０でＹＥＳ）、運搬後の画像データ及びタイムスタンプに関する情報の取得要求画面を記憶部１５から読み出して携帯電話機２へ送信する（ステップＳ１２１１）。

【００５５】

作業者はステップＳ１１１において撮像した認証に供すべき運搬後の画像データを選択する（ステップＳ１２１２）。ＣＰＵ２１は入力部２３の操作により画像データが選択された場合、画像データのファイル名またはパスを画像データボックス１３５に表示する。またＣＰＵ２１は記憶部２５に記憶した画像データを読み出すと共に、画像データのサムネイルをサムネイルボックス１３６に表示する（ステップＳ１２１３）。

【００５６】

さらに、ＣＰＵ２１は読み出した画像データの撮像日時を表示部２４へ出力する。また、ＣＰＵ２１は選択された画像データに対応するタイムスタンプが、ステップＳ１１８の処理により記憶部２５に記憶されていると判断した場合、図９に示すようにＣＰＵ２１は「タイムスタンプ取得済」の表示を表示部２４に行う。作業者は表示部２４において認証に用いる画像データを確認し、またタイムスタンプが取得済みであることをも確認した上で、送信ボタン１３４を操作する。

【００５７】

ＣＰＵ２１は入力部２３から送信ボタン１３４の操作信号を受信した場合、選択された画像データに対応するタイムスタンプに関するデータ、すなわち画像データに対応する暗号化されたハッシュ値及びタイムスタンプを記憶部２５から読み出す（ステップＳ１２１４）。ＣＰＵ２１は読み出した画像データ並びに暗号化されたハッシュ値及びタイムスタンプをサーバコンピュータ１へ送信する（ステップＳ１２１５）。サーバコンピュータ１のＣＰＵ１１は、画像データベース１５２に、ステップＳ７４で送信された作業番号に対応付けて、ステップＳ７１１において送信された運搬後の画像データ並びに暗号化されたハッシュ値及びタイムスタンプを記憶する（ステップＳ１２１６）。

【００５８】

図１４は運搬後の画像データ及びタイムスタンプに関するデータの認証処理手順を示すフローチャートである。サーバコンピュータ１のＣＰＵ１１は画像データベース１５２から運搬後の画像データ並びに暗号化されたハッシュ値及びタイムスタンプを読み出す（ステップＳ１４１）。ＣＰＵ１１はタイムスタンプ認証プログラム１５４を起動する（ステ

ップＳ１４２）。ＣＰＵ１１はタイムスタンプ認証プログラム１５４に従い、読み出した運搬後の画像データのハッシュ値を算出する（ステップＳ１４３）。ＣＰＵ１１は公開鍵を、例えば認証局の認証局コンピュータ４等から取得する（ステップＳ１４４）。

【００５９】

ＣＰＵ１１は取得した公開鍵を用いて暗号化されたハッシュ値及びタイムスタンプの復号を行う（ステップＳ１４５）。ＣＰＵ１１は復号したハッシュ値とステップ１４３において算出したハッシュ値とが一致するか否かを判断する（ステップＳ１４６）。ＣＰＵ１１は一致しないと判断した場合（ステップＳ１４６でＮＯ）、画像データに変更または改竄が加えられたと判断し、携帯電話機２または運搬依頼者のコンピュータ５へエラー信号を送信し処理を終了する。一方、ハッシュ値が一致するとＣＰＵ１１が判断した場合（ステップＳ１４６でＹＥＳ）、タイムスタンプに記述された確定時刻に画像データが存在しており、かつ、画像データが確定時刻以降不正に改竄されていないと判断し、認証が成功したことを示す認証成功フラグを画像データベース１５２に、作業番号に対応付けて記憶する（ステップＳ１４７）。このように、運搬前後の生体情報による認証及び機器固有の情報に基づく認証に加えて、運搬前の画像データ及びタイムスタンプに関するデータ、運搬前の画像データの認証成功に伴い発生する識別情報、並びに、運搬後の画像データ及びタイムスタンプに関するデータに基づいて、認証を行うこととしたので、運搬する物品６に関する情報の漏洩がないことを高い信頼性を持って保証することが可能となる。

【００６０】

続いてサーバコンピュータ１による証明書の生成処理及びコンピュータ１が生成された証明書を取得する際の処理について説明する。図１５は証明書生成処理及び証明書取得処理の手順を示すフローチャートである。運搬依頼者はコンピュータ５を用いてサーバコンピュータ１との間で通信を確立し、証明書の発行を希望する運搬作業にかかる作業番号を入力する。なお、コンピュータ５とサーバコンピュータ１との通信を確立する際にはＩＤ及びパスワードによる認証を行っても良い。コンピュータ５は入力された作業番号及び証明書の取得要求を示す情報をサーバコンピュータ１へ送信する（ステップＳ１５１）。

【００６１】

サーバコンピュータ１のＣＰＵ１１は送信された作業番号を元に、画像データベース１５２を検索し、作業番号に対応する認証成功フラグが記憶されているか判断する（ステップＳ１５２）。ＣＰＵ１１は認証成功フラグが記憶されていないと判断した場合（ステップＳ１５２でＮＯ）、上述した一連の認証が完了していないことから証明書の生成を中断し処理を終了する。ＣＰＵ１１は認証成功フラグが記憶されていると判断した場合（ステップＳ１５２でＹＥＳ）、画像データベース１５２から作業番号に対応する運搬前の画像データ及びタイムスタンプ、並びに運搬後の画像データ及びタイムスタンプを読み出す（ステップＳ１５３）。そしてＣＰＵ１１は、例えば「認証機関○○は、以下のとおり物品が漏洩することなく確実に下記日時に運搬元から運搬先へ運搬されたことを証明する」等の文章と共に、読み出した運搬前の画像データ及びタイムスタンプ、並びに運搬後の画像データ及びタイムスタンプを記述した証明書を生成する（ステップＳ１５４）。なお、作業番号に対応する識別情報をも記述するようにしても良い。

【００６２】

この生成した証明書はデジタル署名を付加させてコンピュータ５へ送信する。すなわち、サーバコンピュータ１のＣＰＵ１１は秘密鍵を用いて生成した証明書を暗号化する（ステップＳ１５５）。ＣＰＵ１１は暗号化された証明書のハッシュ値を算出する（ステップＳ１５６）。ＣＰＵ１１は暗号化された証明書及びハッシュ値をコンピュータ５へ送信する（ステップＳ１５７）。コンピュータ５は暗号化された証明書及びハッシュ値を受信する（ステップＳ１５８）。コンピュータ５は暗号化された証明書から算出されるハッシュ値と、ステップＳ１５８において受信したハッシュ値とが一致するか否かを判断する（ステップＳ１５９）。

【００６３】

コンピュータ５はハッシュ値が一致しないと判断した場合（ステップＳ１５９でＮＯ）

、証明書が改竄されたと判断し、その旨を運搬依頼者に提示するメッセージを表示し、処理を終了する。一方、ハッシュ値が一致するとコンピュータ５が判断した場合（ステップＳ１５９でＹＥＳ）、コンピュータ５は、認証局の認証局コンピュータ４等から公開鍵を取得し（ステップＳ１５１０）、暗号化された証明書の復号を行う（ステップＳ１５１１）。コンピュータ５は復号された証明書を図示しないハードディスク等に記憶し（ステップＳ１５１２）、必要に応じて図示しないモニタに表示またはプリントアウト等する。

【００６４】

サーバコンピュータ１はさらに証明書の信頼性を高めるために認証局の認証局コンピュータ４が発行するデジタル証明書を生成した証明書に付属するようにしても良い。以下にその内容を説明する。なお、ステップＳ１５４までの処理はデジタル証明書を付属しない場合と同じであるので説明を省略する。図１６はデジタル証明書を付属する場合の証明書の送信手順を示すフローチャートである。サーバコンピュータ１のＣＰＵ１１はステップＳ１５４において生成された証明書のハッシュ値を算出する（ステップＳ１６１）。ＣＰＵ１１はサーバコンピュータ１の個人鍵で証明書及び算出したハッシュ値を暗号化する（ステップＳ１６２）。

【００６５】

ＣＰＵ１１はサーバコンピュータ１の公開鍵、有効期限、登録者情報及び認証局名等を含む情報が記憶されたデジタル証明書を認証局の秘密鍵で暗号化する（ステップＳ１６３）。ＣＰＵ１１は暗号化された証明書、ハッシュ値及びデジタル証明書をコンピュータ５へ送信する（ステップＳ１６４）。コンピュータ５は暗号化された証明書、ハッシュ値及びデジタル証明書を受信する（ステップＳ１６５）。コンピュータ５は認証局の公開鍵を取得し（ステップＳ１６６）、取得した認証局の公開鍵でデジタル証明書を復号し、サーバコンピュータ１の公開鍵を取り出す（ステップＳ１６７）。

【００６６】

コンピュータ５は取り出したサーバコンピュータ１の公開鍵を用いて暗号化された証明書及びハッシュ値を復号する（ステップＳ１６８）。コンピュータ５は復号した証明書のハッシュ値を算出し（ステップＳ１６９）、算出したハッシュ値と、ステップＳ１６８において復号したハッシュ値とが一致するか否かを判断する（ステップＳ１６１０）。コンピュータ５はハッシュ値が一致しないと判断した場合（ステップＳ１６１０でＮＯ）、証明書が改竄されたと判断し、その旨を運搬依頼者に提示するメッセージを表示し、処理を終了する。一方、ハッシュ値が一致するとコンピュータ５が判断した場合（ステップＳ１６１０でＹＥＳ）、コンピュータ５は復号された証明書を図示しないハードディスク等に記憶し（ステップＳ１６１１）、必要に応じて図示しないモニタに表示またはプリントアウト等する。

【００６７】

実施の形態２

図１７は実施の形態２に係る封止部６１の構成を示す模式的斜視図である。実施の形態１においては封止部６１を、剥がしたことを識別することが可能なシールを用いて構成したが、センサ等を用いて構成しても良い。以下にその内容を説明する。運搬対象たる印刷物または記録媒体等の物品６は、ステンレススチールまたはアルミニウム等からなる物品収納箱６０に納められる。物品収納箱６０の上部には右蓋６０１及び左蓋６０２が開閉自在に取り付けられており、右蓋６０１と左蓋６０２と閉状態を維持するためのロック機構６０３，６０３が右蓋６０１及び左蓋６０２の上面にそれぞれ取り付けられている。

【００６８】

右蓋６０１及び左蓋６０２にはさらに実施の形態２に係る封止部６１が設けられている。封止部６１は、左蓋６０２下面に設けられる磁石６２、右蓋６０１下面に設けられる磁気センサ６３、及び、該磁気センサ６３に接続され右蓋６０１上面に設けられる表示パネル６４を含んで構成される。磁気センサ６３は、右蓋６０１及び左蓋６０２が閉状態へ移動した場合に、磁石６２による磁気を検出し、検出信号を表示パネル６４へ出力する。

【００６９】

表示パネル６４は、赤色ＬＥＤからなる開ランプ６４１及び緑色ＬＥＤからなる閉ランプ６４２を上面に備える。右蓋６０１及び左蓋６０２が開状態にある場合、表示パネル６４は、内部に備えるマイコン（図示せず）の指示により開ランプ６４１を点灯させる。一方、右蓋６０１及び左蓋６０２が閉状態へ移行し、磁気センサ６３が磁石６２による磁気を検知した場合は、検出信号が表示パネル６４へ出力される。表示パネル６４のマイコンは検出信号の出力をトリガーに、閉ランプ６４２を点灯させ、開ランプ６４１を消灯する。

【００７０】

表示パネル６４のマイコンは、この閉ランプ６４２の点灯後、右蓋６０１及び左蓋６０２が開状態となり再び閉状態へ移行した場合には、閉ランプ６４２の点灯を行わないようプログラミングされている。すなわち、物品収納箱６０の封止後、一端開封した場合、閉ランプ６４２は点灯しない。なお、このプログラムをリセットする場合、表示パネル６４の裏面に設けられる図示しないタッチパネルから、所定のパスワードを入力する。これにより、作業者は、閉状態にあり、閉ランプ６４２による緑色の発光が生じている画像を携帯電話機２から撮像できる。なお、本実施の形態においては、物品収納箱６０に、封止部６１を形成したが、トラック荷台の開閉扉に同様の封止部６１を形成するようにしても良い。

【００７１】

本実施の形態２は以上の如き構成としてあり、その他の構成及び作用は実施の形態１と同様であるので、対応する部分には同一の参照番号を付してその詳細な説明を省略する。

【００７２】

実施の形態３

図１８は実施の形態３に係るサーバコンピュータ１の構成を示すブロック図である。実施の形態１に係るサーバコンピュータ１を動作させるためのコンピュータプログラムは、本実施の形態３のように、ＣＤ－ＲＯＭ、ＭＯ、またはＤＶＤ－ＲＯＭ等の可搬型記録媒体１Ａで提供することも可能である。さらに、コンピュータプログラムを、通信網Ｎを介して図示しないサーバコンピュータからダウンロードすることも可能である。以下に、その内容を説明する。

【００７３】

図１８に示すサーバコンピュータ１の図示しないリーダ／ライタに、画像データ及び時刻を認証させ、識別情報を送信させ、並びに、画像データ及び時刻を認証させるコンピュータプログラムが記録された可搬型記録媒体１Ａ（ＣＤ－ＲＯＭ、ＭＯ又はＤＶＤ－ＲＯＭ等）を、挿入して記憶部１５の制御プログラム１５３内にこのプログラムをインストールする。または、かかるプログラムを、通信部１６を介して外部の図示しないサーバコンピュータからダウンロードし、記憶部１５にインストールするようにしても良い。かかるプログラムはＲＡＭ１２にロードして実行される。これにより、上述のような本発明のサーバコンピュータ１として機能する。

【００７４】

本実施の形態３は以上の如き構成としてあり、その他の構成及び作用は実施の形態１と同様であるので、対応する部分には同一の参照番号を付してその詳細な説明を省略する。

【図面の簡単な説明】

【００７５】

【図１】本発明に係る認証システムの概要を示す模式図である。

【図２】サーバコンピュータのハードウェア構成を示すブロック図である。

【図３】携帯電話機のハードウェア構成を示すブロック図である。

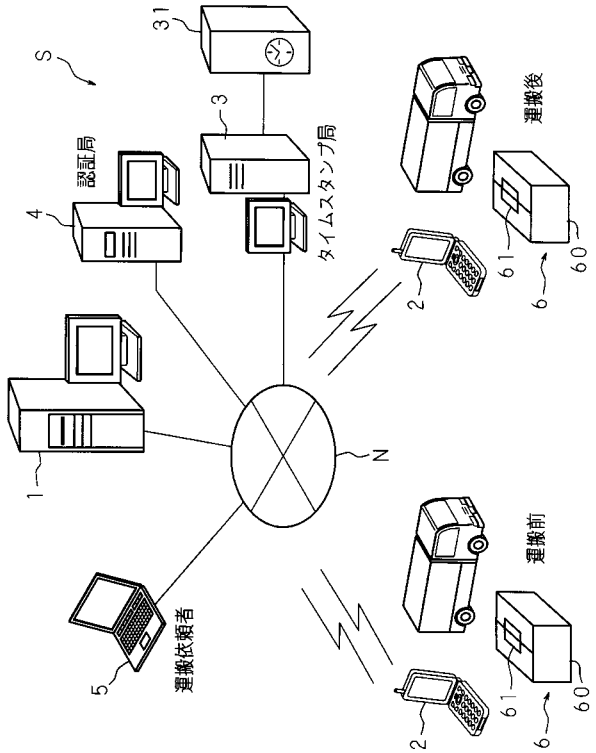
【図４】サーバコンピュータに記憶される生体情報ファイルのレコードレイアウトを示す説明図である。

【図５】画像データベースのレコードレイアウトを示す説明図である。

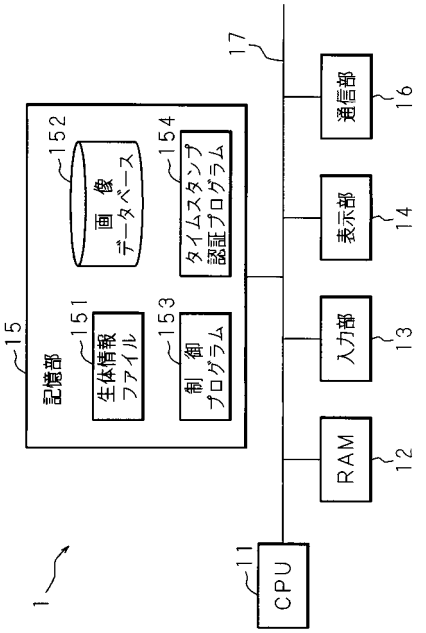
【図６】運搬前の画像データのタイムスタンプに関するデータを取得する手順を示すフローチャートである。

【図７】運搬前の画像データ及びタイムスタンプに関する情報を送信する際の手順を示すフローチャートである。
【図８】携帯電話機の表示部に表示されるログイン画面のイメージを示す説明図である。
【図９】画像データ及びタイムスタンプに関するデータを入力する際のイメージを示す説明図である。
【図１０】運搬前の画像データ及びタイムスタンプに関するデータの認証処理手順を示すフローチャートである。
【図１１】運搬後の画像データのタイムスタンプに関するデータを取得する手順を示すフローチャートである。
【図１２】運搬後の画像データ及びタイムスタンプに関する情報を送信する際の手順を示すフローチャートである。
【図１３】運搬後の画像データ及びタイムスタンプに関する情報を送信する際の手順を示すフローチャートである。
【図１４】運搬後の画像データ及びタイムスタンプに関するデータの認証処理手順を示すフローチャートである。
【図１５】証明書生成処理及び証明書取得処理の手順を示すフローチャートである。
【図１６】デジタル証明書を付属する場合の証明書の送信手順を示すフローチャートである。
【図１７】実施の形態２に係る封止部の構成を示す模式的斜視図である。
【図１８】実施の形態３に係るサーバコンピュータの構成を示すブロック図である。
【符号の説明】
【００７６】
１　サーバコンピュータ（認証装置）
２　携帯電話機（情報処理装置）
３　タイムスタンプ生成装置
４　認証局コンピュータ
５　コンピュータ
Ｎ　通信網
Ｓ　認証システム
６　物品
６０　物品収納箱
６１　封止部
１１　ＣＰＵ（制御部）
１２　ＲＡＭ
１３　入力部
１４　表示部
１５　記憶部
１５１　生体情報ファイル
１５２　画像データベース
２１　ＣＰＵ（制御部）
２３　入力部
２４　表示部
２５　記憶部
２９　カメラ（撮像手段）
２８　生体情報取得部
１Ａ　記録媒体

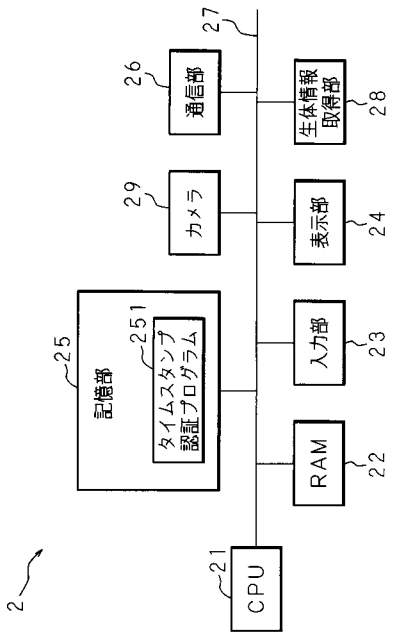
【図１】



【図２】



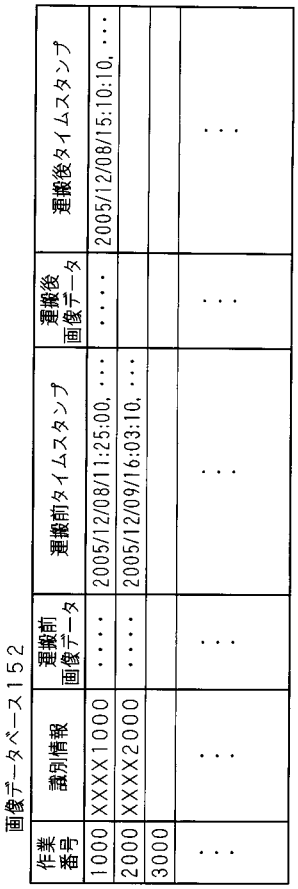
【図３】



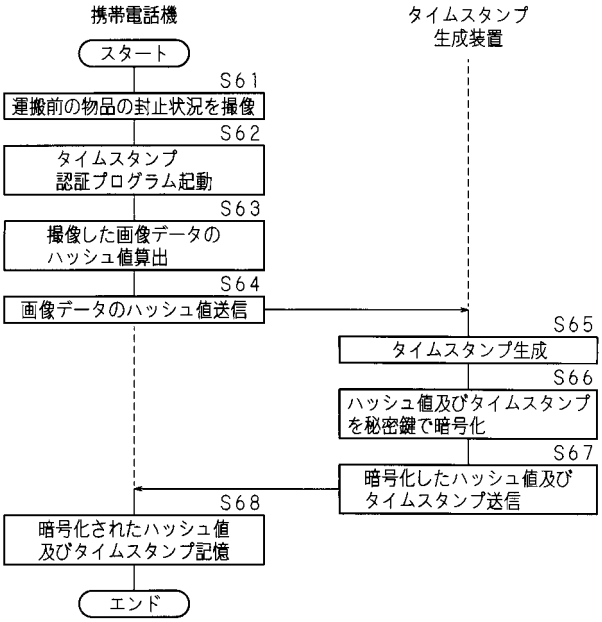
【図４】

作業者ＩＤ	作業者氏名	作業者生体情報	MACアドレス
001	AAA	・・・・・・	・・・・・・
002	BBB	・・・・・・	・・・・・・
003	CCC	・・・・・・	・・・・・・
・・・	・・・	・・・	・・・

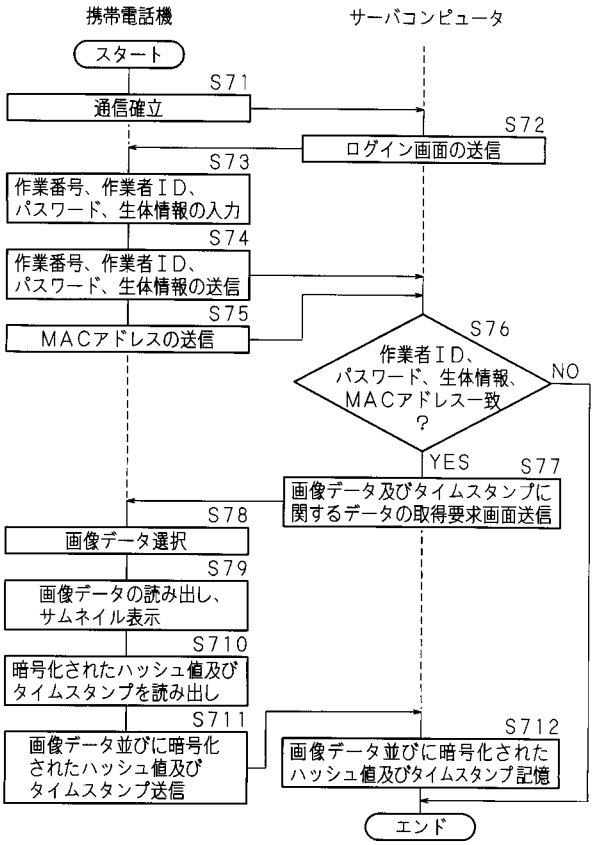
【図５】


画像データベース152
作業番号
識別情報
運搬前画像データ
運搬前タイムスタンプ
運搬後画像データ
運搬後タイムスタンプ
1000
2000
3000
XXXX1000
XXXX2000
2005/12/08/11:25:00, ・・・
2005/12/09/16:03:10, ・・・
2005/12/08/15:10:10, ・・・

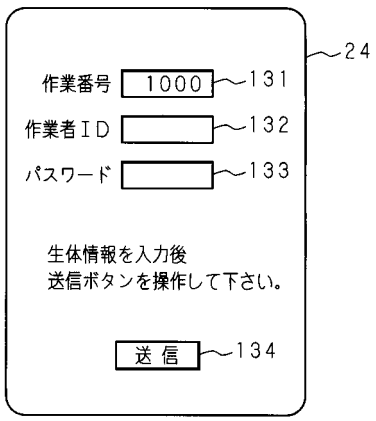
【図６】


携帯電話機
タイムスタンプ生成装置
スタート
S61
運搬前の物品の封止状況を撮像
S62
タイムスタンプ認証プログラム起動
S63
撮像した画像データのハッシュ値算出
S64
画像データのハッシュ値送信
S65
タイムスタンプ生成
S66
ハッシュ値及びタイムスタンプを秘密鍵で暗号化
S67
暗号化したハッシュ値及びタイムスタンプ送信
S68
暗号化されたハッシュ値及びタイムスタンプ記憶
エンド

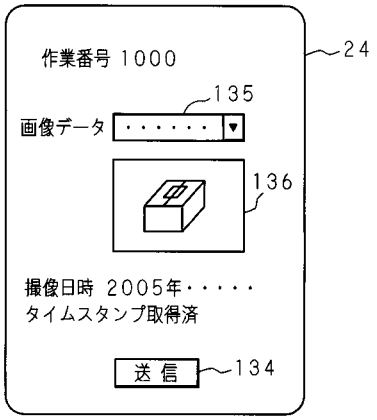
【図７】


携帯電話機
サーバコンピュータ
スタート
S71
通信確立
S72
ログイン画面の送信
S73
作業番号、作業者ＩＤ、パスワード、生体情報の入力
S74
作業番号、作業者ＩＤ、パスワード、生体情報の送信
S75
MACアドレスの送信
S76
作業者ＩＤ、パスワード、生体情報、MACアドレス一致？
NO
YES
S77
画像データ及びタイムスタンプに関するデータの取得要求画面送信
S78
画像データ選択
S79
画像データの読み出し、サムネイル表示
S710
暗号化されたハッシュ値及びタイムスタンプを読み出し
S711
画像データ並びに暗号化されたハッシュ値及びタイムスタンプ送信
S712
画像データ並びに暗号化されたハッシュ値及びタイムスタンプ記憶
エンド

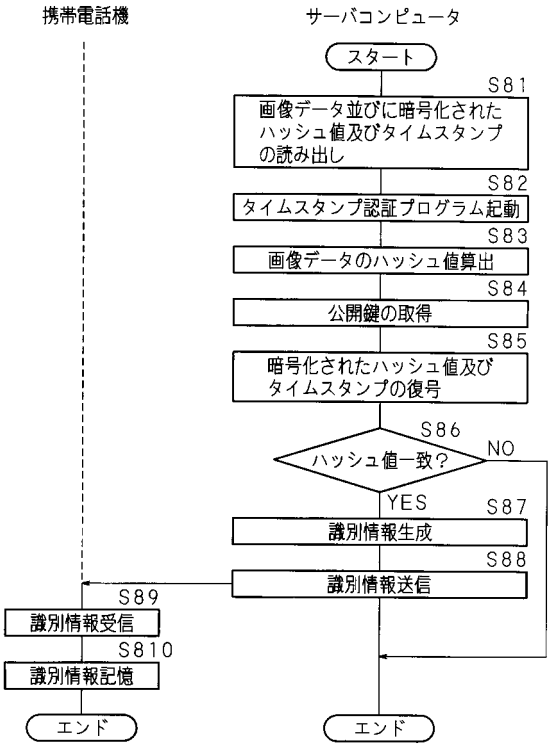
【図８】


24
作業番号
1000
131
作業者ＩＤ
132
パスワード
133
生体情報を入力後
送信ボタンを操作して下さい。
送 信
134

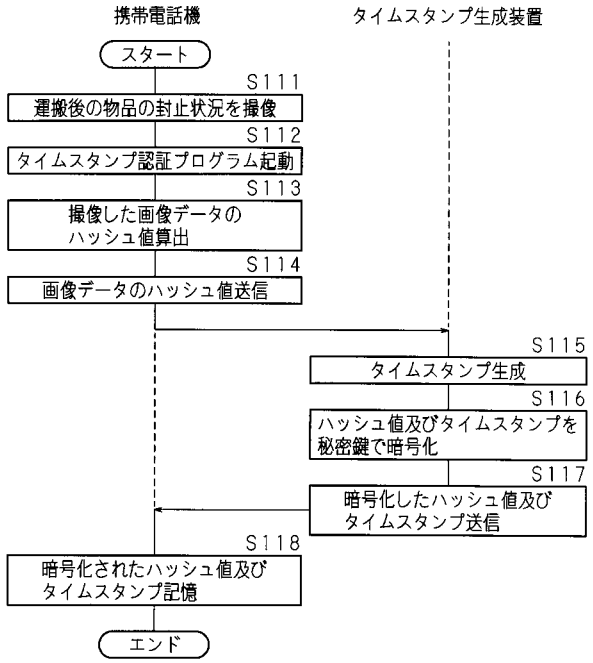
【図９】



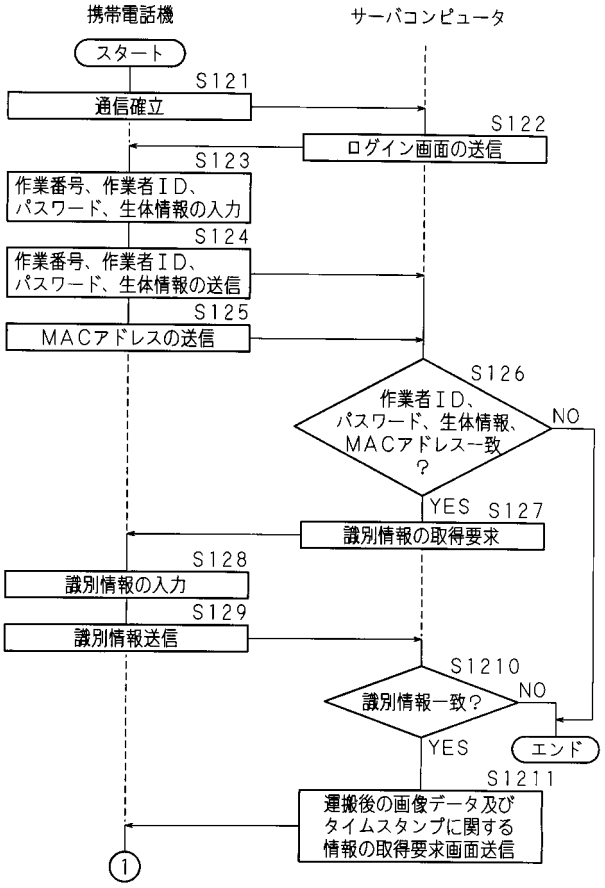
【図１０】



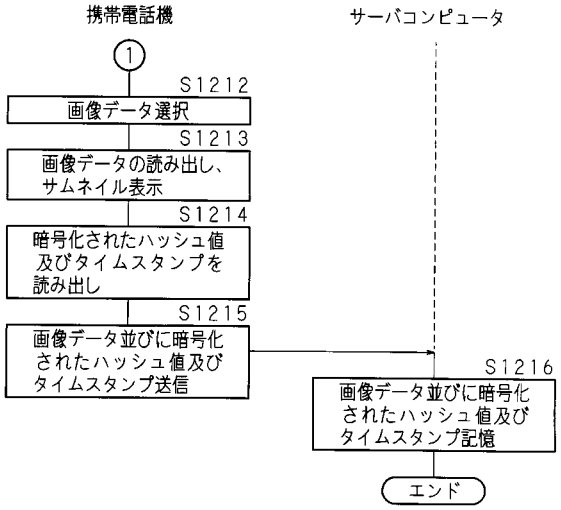
【図１１】



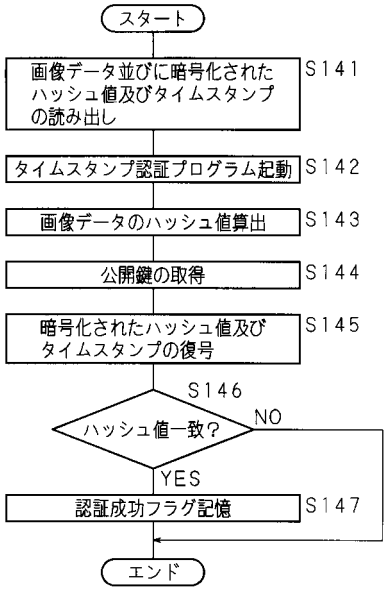
【図１２】



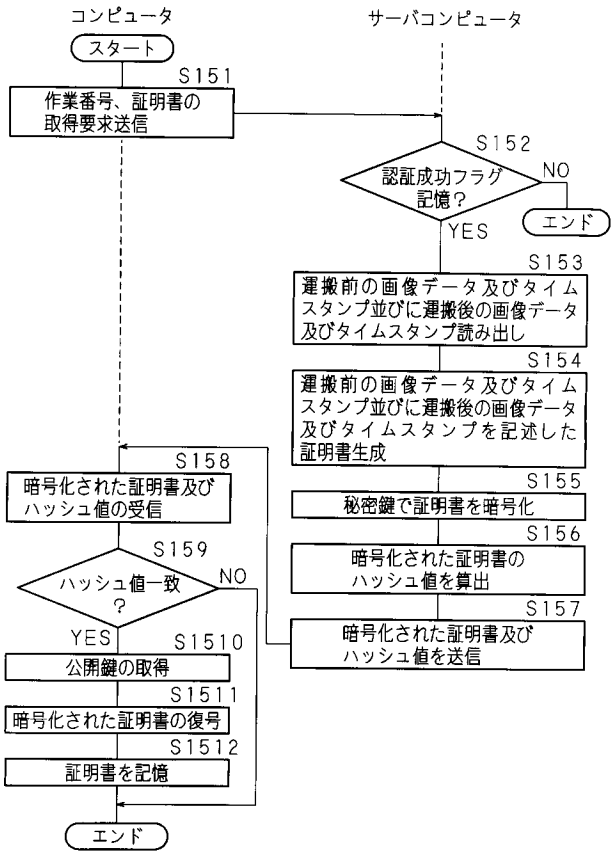
【図１３】



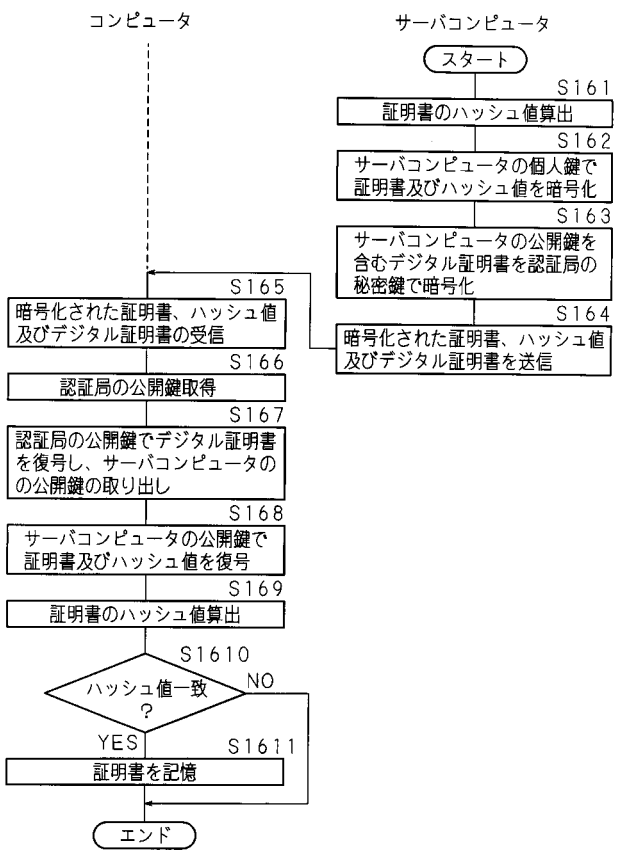
【図１４】



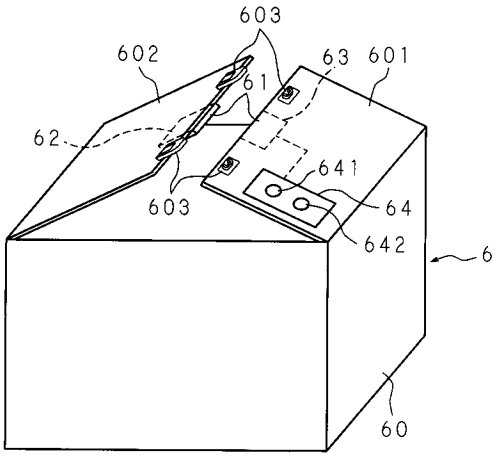
【図１５】



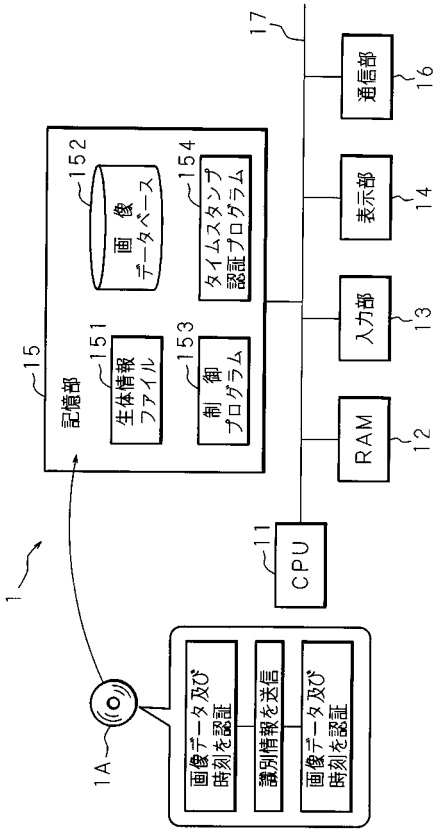
【図１６】



【図１７】


603
602
63
601
61
62
641
603
64
642
6
60

【図１８】


17
通信部
16
表示部
14
入力部
13
RAM
12
CPU
11
15
記憶部
151
生体情報ファイル
152
画像データベース
153
制御プログラム
154
タイムスタンプ認証プログラム
1
1A
画像データ及び時刻を認証
識別情報を送信
画像データ及び時刻を認証