

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第4410858号
(P4410858)

(45) 発行日 平成22年2月3日(2010.2.3)

(24) 登録日 平成21年11月20日(2009.11.20)

(51) Int. Cl. F I
G07B 17/00 (2006.01) G O 7 B 17/00
G09C 1/00 (2006.01) G O 9 C 1/00 6 6 O Z

請求項の数 23 外国語出願 (全 16 頁)

<p>(21) 出願番号 特願平8-359645 (22) 出願日 平成8年12月19日(1996.12.19) (65) 公開番号 特開平9-319907 (43) 公開日 平成9年12月12日(1997.12.12) 審査請求日 平成15年12月19日(2003.12.19) 審判番号 不服2007-27617(P2007-27617/J1) 審判請求日 平成19年10月9日(2007.10.9) (31) 優先権主張番号 08/575107 (32) 優先日 平成7年12月19日(1995.12.19) (33) 優先権主張国 米国(US)</p>	<p>(73) 特許権者 592006866 ビットニイ ボウズ インコーポレイテッド PITNEY BOWES INCORPORATED アメリカ合衆国 コネチカット州 069 26-0700 スタムフォード ワン エルムクロフト ワールド ヘッドクワ ーターズ (番地なし) (74) 代理人 100059959 弁理士 中村 稔 (74) 代理人 100067013 弁理士 大塚 文昭 (74) 代理人 100065189 弁理士 穴戸 嘉一</p>
---	---

最終頁に続く

(54) 【発明の名称】 オープンシステムのメータにおけるデジタルトークン発行方法

(57) 【特許請求の範囲】

【請求項1】

郵便証印を印刷するためにコンピュータシステムを動作させる方法であって、
デジタルトークンに対するリクエスト、及び郵便料金額及び受取人の情報を含む所定の郵便情報を、前記コンピュータシステムから、認証や会計されずに郵便のための印刷が行なわれることや記憶された郵便資金額が変化することを防ぐセキュリティ機能を備えた安全な郵便会計モジュールに送るステップと、

前記デジタルトークンに対するリクエストに回答して前記所定の郵便情報の少なくともいくつかを暗号化することにより生成されたデジタルトークンを前記安全な郵便会計モジュールから受け取るステップと、

受け取ったデジタルトークンを前記コンピュータシステム中の記憶装置に記憶するステップと、

前記コンピュータシステム中の前記記憶装置から前記デジタルトークンを検索するステップと、

安全でない非専用プリンタで印刷するために使用される前記郵便証印のグラフィックスイメージを、前記検索されたデジタルトークン及び前記所定の郵便情報を固定のグラフィックスイメージと組み合わせることによって生成するステップと、を有することを特徴とする方法。

【請求項2】

前記郵便証印のグラフィックスイメージを生成する前記ステップは、最初の証印印刷動

作がうまく終了しなかった場合に、もう1回、前記コンピュータシステムの記憶装置から前記トークンを検索するステップを含むことを特徴とする請求項1に記載の方法。

【請求項3】

前記コンピュータシステム中の前記記憶装置に前記郵便証印の前記グラフィックイメージを記憶するステップ、を含むことを特徴とする請求項1に記載の方法。

【請求項4】

前記コンピュータシステム中に前記受け取ったデジタルトークンを記憶する前記ステップは、

受け取ったデジタルトークンを取引記録として記憶するステップと、

郵便物カウントによって前記取引記録に索引を付けるステップと、を含むことを特徴とする請求項1に記載の方法。

10

【請求項5】

前記コンピュータシステムは、パーソナルコンピュータを含み、及び

当該コンピュータシステム中の記憶装置は、当該パーソナルコンピュータのハードディスクを含むことを特徴とする請求項1に記載の方法。

【請求項6】

記憶する前記ステップは、前記デジタルトークンを、前記パーソナルコンピュータのハードディスク上のダイナミックリンクライブの部分として隠しファイル中に記憶するステップを含むことを特徴とする請求項5に記載の方法。

【請求項7】

20

郵便証印のバッチを印刷するためにコンピュータシステムを動作させる方法であって、

デジタルトークンに対する少なくとも1つのリクエスト、及び複数の郵便料金額及び複数の受取人についての対応する情報を含む所定の郵便情報を、前記コンピュータシステムから、認証や会計されずに郵便のための印刷が行なわれることや記憶された郵便資金額が変化することを防ぐセキュリティ機能を備えた安全な郵便会計モジュールに送るステップと、

前記デジタルトークンに対するリクエストに回答して前記所定の郵便情報の少なくともいくつかを暗号化することにより生成された複数のデジタルトークンを前記安全な郵便会計モジュールから受け取るステップと、

受け取ったデジタルトークンを前記コンピュータシステム中の記憶装置に記憶するステップと、

30

前記デジタルトークンを前記コンピュータ中の前記記憶装置から検索するステップと、

安全でない非専用プリンタで印刷するために使用される複数の前記郵便証印のグラフィックイメージを、前記検索されたデジタルトークン及び前記所定の郵便情報を固定のグラフィックイメージと組み合わせることによって生成するステップと、を有することを特徴とする方法。

【請求項8】

コンピュータ読み取り可能な媒体、及び

前記コンピュータ読み取り可能な媒体上の実行可能コードを含む製品であって、

前記実行可能コードは、読み出されて実行されるとプロセッサにステップを実行させるものであり、当該ステップは、

40

デジタルトークンに対するリクエスト、及び郵便料金及び受取人の情報を含む所定の郵便情報を、プログラム可能なプロセッサに結合された安全な郵便会計モジュールに送るステップと、

前記デジタルトークンに対するリクエストに回答して前記所定の郵便情報の少なくともいくつかを暗号化することにより生成されたデジタルトークンを前記安全な郵便会計モジュールから受け取るステップと、

前記プログラム可能なプロセッサに関連するメモリ中に受け取ったデジタルトークンを記憶するステップと、

50

前記メモリから前記デジタルトークンを検索するステップと、
安全でない非専用プリンタで印刷するために使用される前記郵便証印のグラフィックス
イメージを、前記検索されたデジタルトークン及び前記所定の郵便情報を固定のグラフィ
ックスイメージと組み合わせることによって生成するステップと、を有することを特徴
とする製品。

【請求項 9】

前記コンピュータ中に前記受け取ったデジタルトークンを記憶する前記ステップは、
前記デジタルトークンをダイナミックリンクライブラリの部分として隠しファイル中に
記憶するステップを有することを特徴とする請求項 8 に記載の製品。

【請求項 10】

前記郵便証印のグラフィックスイメージを生成する前記ステップは、当該郵便証印を印
刷するためのプログラム可能なプロセッサに結合した安全でないプリンタを駆動するステ
ップを含むことを特徴とする請求項 8 に記載の製品。

【請求項 11】

前記安全な郵便会計モジュールとして使用するためのポータブルユニットをさらに含む
請求項 8 に記載の製品であって、

プロセッサと、

会計情報を記憶するための、前記ポータブルユニットのプロセッサに結合された不揮発
性メモリと、

前記ポータブルユニットを前記プログラム可能プロセッサに結合させるためのインター
フェースと、を有することを特徴とする製品。

【請求項 12】

前記ポータブルユニットは、前記デジタルトークンを生成することに関する暗号化機
能を実行するための前記ポータブルユニットのプロセッサに結合した暗号化モジュールを
更に含むことを特徴とする請求項 11 に記載の製品。

【請求項 13】

前記コンピュータ読み取り可能媒体は、前記プログラム可能プロセッサのメモリデバイ
スを含むことを特徴とする請求項 8 に記載の製品。

【請求項 14】

前記メモリデバイスは記憶ディスクを含むことを特徴とする請求項 13 に記載の製品。

【請求項 15】

前記記憶ディスクはハードディスクを含むことを特徴とする請求項 14 に記載の製品。

【請求項 16】

郵便資金管理、デジタルトークン生成、会計機能に対する暗号化装置である安全な取
引会計電子金庫に結合したホストコンピュータと共に使用するためのシステムであって、

前記ホストコンピュータと前記安全な取引会計電子金庫の間の通信を実行するための安
全な通信モジュールであって、当該通信は、特定の価値と受信者の情報に関する取引に対
するリクエストを前記ホストコンピュータから前記安全な取引会計電子金庫に送ること、
及び前記安全な取引会計電子金庫から前記ホストコンピュータへの、前記リクエストに
応答して前記特定の価値及び前記受取人の情報の少なくともいくつかを暗号化すること
により生成されたデジタルトークンを含む対応する応答メッセージを受け取ることを含む通
信モジュールと、

前記ホストコンピュータ中のメモリデバイス中に、前記安全な取引会計電子金庫から受
け取ったデジタルトークンを取得して記憶するための取引取得モジュールと、

前記システムが、前記ホストコンピュータ上で実行されるアプリケーションプログラム
と通信できるようにし、当該アプリケーションプログラムは前記システムが取引リクエ
ストを開始できるようにするアプリケーションプログラムインターフェースと、

安全でない非専用プリンタで印刷するために使用される郵便証印のグラフィックスイメ
ージを、前記デジタルトークン、前記特定の価値、及び前記受信者の情報を固定のグラ
フィックスイメージと組み合わせることによって生成するための安全な証印モジュールと

10

20

30

40

50

を有することを特徴とするシステム。

【請求項 17】

ユーザインターフェースモジュールを更に有することを特徴とする請求項 16 に記載のシステム。

【請求項 18】

前記アプリケーションプログラムインターフェースは、データリンクライブラリを含むことを特徴とする請求項 16 に記載のシステム。

【請求項 19】

前記取引取得モジュールは、コンピュータ読み取り可能媒体中の命令を含み、当該命令は、前記ホストコンピュータ内のプログラム可能プロセッサによって実行されることを特徴とする請求項 16 に記載のシステム。

10

【請求項 20】

前記安全な通信モジュールは、コンピュータ読み取り可能媒体中の命令を含み、当該命令は、前記ホストコンピュータ内のプログラム可能プロセッサによって実行されることを特徴とする請求項 16 に記載のシステム。

【請求項 21】

前記取引取得モジュールは、前記郵便証印のグラフィックイメージを前記メモリデバイス中に記憶することを特徴とする請求項 20 に記載のシステム。

【請求項 22】

20

前記アプリケーションプログラムインターフェースは、コンピュータ読み取り可能媒体中に命令を含んでおり、当該命令は、前記ホストコンピュータ内のプログラム可能なプロセッサによって実行されることを特徴とする請求項 16 に記載のシステム。

【請求項 23】

前記安全な通信モジュール及び前記取引取得モジュールは、前記プログラム可能プロセッサによって実行される、前記媒体中の命令を含むことを特徴とする請求項 22 に記載のシステム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

30

本発明は、改良された郵便料金支払システムに関し、特に、予め計算された郵便料金支払情報を有する改良された郵便料金支払システムに関する。

【0002】

【従来の技術】

米国郵便サービスは、現在のところ、クローズドシステムとオープンシステムの2つのタイプの料金メータに対する要求に注目している。クローズドシステムにおいては、このシステム機能が、全く料金メータ機能に専用である。クローズドシステムの料金計器メータの例は、郵便料金証明装置(PEDs)と呼ばれ、専用プリンタがメータすなわち会計機能に安全に結合される従来のデジタルおよびアナログ郵便料金メータを含む。クローズドシステムにおいては、プリンタが、安全にこのメータに接続され、しかもこのメータに専用のものであるため、会計をせずに、印刷されることはない。また、会計が終了した直後に、印刷が行われる。

40

【0003】

オープンシステムにおいては、プリンタが、料金メータ機能に専用なものではなく、料金メータ機能に加えて、多くの異なった用途に関するシステム機能に解放される。例えば、オープンシステム料金メータ装置は、単一/マルチ-タスクオペレーティングシステム、マルチユーザアプリケーション、およびデジタルプリンタを備えたパーソナルコンピュータ(PC)ベースの装置を備える。オープンシステム料金メータ装置は、セキュリティ会計モジュールに安全に接続されていない非専用プリンタを備えたPEDである。

PEDが郵便物に郵便料金証印を印刷するとき、PED内の会計レジスタは、印刷が行

50

われたことを常に示さなければならない。郵便機関は、一般に、郵便料金の印刷またはメータに記憶される郵便資金額の変化が認証されず会計されないことを防ぐセキュリティ特徴を備えた安全な方法で、会計情報が郵便料金メータ内に記憶されることを必要とする。クロードシステムにおいては、メータおよびプリンタが組み合わされたユニットであり、すなわち郵便料金証印の印刷が、会計されなければ確実に行われないようにインタロックされる。

【 0 0 0 4 】

オープンシステム P E D が、郵便料金支払証明を印刷するためのみには用いられないプリンタを利用するため、付加的なセキュリティ手段が、郵便料金支払証明の認証されない印刷を防ぐために必要とされる。このようなセキュリティ手段は、オープンおよびクロードメータシステムにおいて、P E D s による郵便料金支払の暗号証明を備える。郵便物に対する郵便資金額は、別のデータとともに暗号化され、デジタルトークンを生成することができる。デジタルトークンは、郵便物上に刻印された郵便資金額を含んだ情報を認証する暗号化された情報である。

デジタルトークンを生成し使用するシステムの例が、米国特許第 4,757,537号、4,831,555号、4,775,246号、4,873,645号および 4,725,718号に開示されており、この全体の開示内容が、本明細書の一部として組み込まれる。これらのシステムは、暗号アルゴリズムを利用して選択された情報を暗号化し、各郵便物に対して少なくとも1つのデジタルトークンを生成する。この情報の暗号化は、トークンの誤用が適切な検証手続により検出できるように、印刷された情報の改竄を防止するセキュリティを与える。

【 0 0 0 5 】

デジタルトークンの一部として暗号化される代表的な情報は、出所郵便コード、ベンダ I D、P E D 識別データ、郵便物カウント、郵便資金額、日付、およびオープンシステムに対しては送付先郵便コードを含む。これらの項目の情報は、まとめて郵便データと呼ばれ、秘密鍵で暗号化されて郵便物上に印刷されるときに、郵便収入ブロックまたは送付先郵便コードに行われるいかなる改竄の検出をも可能にする非常に高レベルのセキュリティを提供する。郵便収入ブロックは、郵便料金支払証明を与えるために用いられるデジタルトークンを含む、郵便物上に印刷されるイメージである。郵便データは、郵便収入ブロックにおいて暗号化された形態とされていない形態の両方で印刷されてもよい。郵便データは、デジタルトークンを生成するために秘密鍵を用いる暗号化変換計算であるデジタルトークン変換に対する入力として使える。デジタルトークン変換の結果すなわちデジタルトークンは、会計プロセスが終了した後でのみ利用可能である。

【 0 0 0 6 】

デジタルトークンは、オープンおよびクロードメータシステムの両方で利用される。しかしながら、オープンメータシステムに関しては、非専用プリンタが、郵便収入ブロックに加えて別の情報を印刷するために用いられてもよく、また郵便料金証明以外の機能において用いられてもよい。オープンシステム P E D においては、受取人情報が、デジタルトークンの生成に際して用いられる郵便データに含まれる。受取人情報のこのような使用は、郵便物と郵便収入ブロックとの間にセキュリティリンクを生成し、郵便物の明確な認証を可能にする。

2つのデジタルトークンが、郵便データおよび郵便料金支払を認証するために用いられるのが好ましい。第1のトークンは、郵便サービスおよび郵送者の P E D により保持される秘密鍵を用いるデジタルトークン変換により生成される。第2のトークンは、P E D ベンダおよび郵送者の P E D により保持される秘密鍵を用いるデジタルトークン変換により生成される。2つの独立した実体が異なる検証秘密を保持するという事実が、郵便サービスおよびベンダに郵便収入ブロックを認証し且つ郵便料金支払を検証するための独立した手段を与えるために、システムのセキュリティを非常に向上させる。ベンダの秘密鍵を用いる第2デジタルトークン変換の使用が、特定のベンダの装置による郵便料金支払を認証するセキュリティの任意の一部である。2つのデジタルトークン（郵便およびベンダ）の使用が、米国特許第 5,390,251号、および1994年5月13日に出願された係属中

10

20

30

40

50

の米国特許出願第08/242,564号(米国特許第5,655,023号)に開示されており、両方とも本発明の譲受人に譲渡され、これらの全体の内容は本明細書の一部として組み込まれる。

【0007】

【発明が解決しようとする課題】

前述したように、クローズドメータシステムとオープンメータシステムの本質的な違いは、プリンタである。クローズドメータシステムにおけるプリンタは、郵便料金の証明を印刷するために専用とされる安全な装置である。従って、クローズドメータシステムにおける印刷機能は、メータ機能に依存する。このことは、セキュリティのない非専用プリンタであるオープンメータシステムのプリンタに対照的であって、このプリンタは、郵便料金証明を印刷することに加えて、通常のPC関連ドキュメントを印刷する。従って、オープンメータシステムにおける印刷機能は、メータ機能から独立している。本発明は、オープンシステムにおいて、1つ以上の証印イメージを後に生成する際に用いられる1つ以上のデジタルトークンをリクエストし、計算し、記憶し且つ発行するプロセスを提供する。

10

【0008】

本発明に従うと、従来の郵便料金メータの金庫において典型的に行われていた機能のいくつかは、PCベースのオープンメータシステムの金庫から除かれて、PCにおいて行われる。処理される情報が受取人情報を含んでいるために、金庫からPCへの機能の移転が、メータのセキュリティに影響しないことが分かった。PCベースのオープンメータシステムにおいて、後で証印を生成し印刷するために、トークンが発行され記憶されることが可能であることも分かった。さらに、トークンが未だ印刷されていないか、トークンを有する証印の印刷が妨げられる問題が発生した場合に、トークンが再発行されることが分かった。

20

【0009】

【課題を解決するための手段】

本発明は、PCの特別なウィンドウズベースのソフトウェア、プリンタ、および郵便資金を記憶する金庫としての差し込み式周辺装置を備えるPCベースのメータシステムのようなオープンメータシステムに対してトークン生成プロセスを提供する。PCメータは、パーソナルコンピュータと、安全でない非専用プリンタを用いて、デジタルトークンを生成し、後に受取人アドレスを印刷すると同時に、封筒およびラベル上に郵便料金証明を印刷する。

30

本発明は、改竄および郵便料金支払の不正な証明を防ぐセキュリティを有するオープンメータシステムに対してトークン生成プロセスを提供する。本発明は、さらに、デジタルトークンのバッチ処理を行う能力を有するトークン生成プロセスを提供する。

【0010】

本発明によると、オープンシステムメータにおいてデジタルトークンを発行する方法は、デジタルトークンおよび受取人情報を含んだ所定の郵便情報に対するリクエストを、ホストプロセッサからホストプロセッサに作動的に結合する金庫に送り、そのトークンに対するリクエストに回答して、所定の郵便情報を用いて少なくとも1つのデジタルトークンを金庫内で計算し、金庫内で郵便資金を借方に記入し、デジタルトークンをホストプロセッサに発行し、続いて証印を生成し印刷するために、そのデジタルトークンおよび所定の郵便情報をホストプロセッサ内に取引記録として記憶するステップを有する。この方法は、さらに、デジタルトークンおよび所定の郵便情報のグラフィックイメージを含んだ証印をホストプロセッサにおいて生成し、リクエストされるときには郵便物に証印を印刷するステップを含む。

40

より具体的には、本願発明は、デジタルトークンを使用して、セキュリティ会計モジュールに安全に接続されていない非専用プリンタを備えたオープンシステム料金メータ装置をパーソナルコンピュータ(PC)ベースの装置で構成することを目的とするものである。このために本発明は、郵便資金を記憶する金庫としての差し込み式周辺装置等を使用して、PCベースのメータシステムのようなオープンメータシステムに対してトークン生

50

成プロセスを与える。

デジタルトークンとは、郵便物上に刻印された郵便料金額を含んだ情報を認証する暗号化された情報である。郵便物に対する郵便料金額は、別のデータとともに暗号化され、デジタルトークンを生成することができ、これにより郵便料金支払証明の認証されない印刷を防ぐことができる。デジタルトークンの一部として暗号化される代表的な情報は、出所郵便コード、ベンダID、PED識別データ、郵便物カウント、郵便料金額、日付、およびオープンシステムに対しては送付先郵便コードを含む。これらの項目の情報は、まとめて郵便データと呼ばれ、秘密鍵で暗号化されて郵便物上に印刷されるときに、郵便収入ブロックまたは送付先郵便コードに行われるいかなる改竄の検出をも可能にする非常に高レベルのセキュリティを提供する。ここで、郵便収入ブロックは、郵便料金支払証明を与えるために用いられるデジタルトークンを含む、郵便物上に印刷されるイメージである。デジタルトークンは、オープンおよびクローズドメータシステムの両方で利用されるものである。オープンメータシステムに関しては、非専用プリンタが、郵便収入ブロックに加えて別の情報を印刷するために用いられてもよく、また郵便料金証明以外の機能において用いられてもよい。また、オープンシステムPEDにおいては、受取人情報が、デジタルトークンの生成に際して用いられる郵便データに含まれ、受取人情報のこのような使用は、郵便物と郵便収入ブロックとの間にセキュリティリンクを生成し、郵便物の明確な認証を可能にするという効果をもたらす。

【0011】

本発明を説明するにあたって、図1～4に示される図面を参照すると、PCメータシステムとして示されるオープンシステムPCベースの郵便料金メータ10が全体として示されており、これにより本発明がデジタルトークンプロセスを実行する。PCメータシステム10が、郵便資金が記憶される取外し可能メータ装置すなわち電子金庫20に対してホストとして作動するように構成される従来のパーソナルコンピュータを備える。PCメータシステム10が、パーソナルコンピュータおよびそのプリンタを使用して、受取人のアドレスを印刷すると同時に、封筒に郵便料金を印刷し、または予め住所を書いた返信用封筒または大きな郵便物用のラベルを印刷する。本発明の好適な具体例が、郵便料金メータシステムに関して説明されるが、本発明は、取引証明を含む価値メータシステムに応用することができることを理解されたい。

【0012】

ここで使用される用語パーソナルコンピュータは、総称的に用いられ、ディスプレイおよびキーボードのようなユーザインタフェース手段と記憶媒体に作動的に結合される少なくとも1つのプロセッサを備えた現在および未来のマイクロプロセッシングシステムを示す。パーソナルコンピュータは、1人以上のユーザによりアクセス可能なワークステーションであってもよい。

PCベースの郵便料金メータ10は、パーソナルコンピュータ(PC)12、ディスプレイ14、キーボード16、およびレーザ又はインクジェットプリンタが好ましいセキュリティのないデジタルプリンタ18を有する。PC12が、インテル社により製造される80486およびペンティアムプロセッサのような従来のプロセッサ22と、従来のハードドライブ24、フロッピードライブ26およびメモリ28を備える。PCMCIAカード30のような取外し可能カードに収容される電子金庫20は、郵便資金管理、デジタルトークン生成および伝統的な会計機能に対するセキュリティのある暗号化装置である。PCメータシステム10が、PC12に配備されるのが好ましい任意のモデム29を備えてもよい。モデム29は、郵便サービス、または資金(借方または貸方)を再充填するための郵便認証ベンダとの通信のために用いられることができる。別の具体例においては、モデムが、PCMCIAカード30に備えられてもよい。

【0013】

PCメータシステム10が、従来のウィンドウズベースのワードプロセッシング、データベースおよび表計算アプリケーションプログラム36からアクセス可能なウィンドウズベースのPCソフトウェアモジュール34(図3および4)を更に備える。PCソフトウェ

アモジュール34は、金庫動的リンクライブラリ(DLL)40、ユーザインタフェースモジュール42、およびメータ機能を制御する複数のサブモジュールを備える。DLLモジュール40は、安全に金庫20と通信し、ユーザインタフェースモジュール42を通じてマイクロソフトウィンドウズベースのアプリケーションプログラム36にオープンインタフェースを提供する。DLLモジュール40は、証印イメージと、金庫の郵便資金の使用の写しを安全に記憶する。ユーザインタフェースモジュール42は、封筒またはラベルのようなドキュメント上に郵便収入ブロックを印刷するために、アプリケーションプログラム36にDLLモジュール40からの電子証印イメージのアクセスを与える。ユーザインタフェースモジュール42は、アプリケーションプログラムに、離れた位置からの再充填を行い、管理機能を実現する能力を与える。

10

【0014】

従って、PCベースメータシステム10は、ユーザリクエストに応じて郵便料金メータとなる取り付けられたプリンタを有する従来のパーソナルコンピュータとして作動する。プリンタ18は、手紙の印刷および封筒の宛名書きを含んだパーソナルコンピュータにより通常印刷される全てのドキュメントを印刷し、本発明の場合は、郵便料金証印を印刷する。

金庫は、PC12におけるPCMCIAコントローラ32を通じてアクセスされるPCMCIA I/O装置すなわちカード30に收容される。PCMCIAカードは、パーソナルコンピュータメモ리카ード国際協会の標準仕様に一致するクレジットカードサイズの周辺装置すなわちアダプタである。図2および3を参照すると、PCMCIAカード30は、マイクロプロセッサ44、冗長不揮発性メモリ(NVM)46、クロック48、暗号化モジュール50および会計モジュール52を含む。暗号化モジュール50は、NBSデータ暗号化標準(DES)、または別の適切な暗号化構成を実現する。好ましい具体例においては、暗号化モジュール50が、ソフトウェアモジュールである。暗号化モジュール50が、マイクロプロセッサ44に結合される別のチップのようなセパレータ装置であってもよいことを理解されたい。会計モジュール52は、出所ジップコード、ベンダID、PCベースの郵便料金メータ10を識別するデータ、PCベースの郵便料金メータ10により生成される郵便収入ブロックの連続的な郵便物カウント、郵便料金額および郵便サービスに付託した日付のような郵便データと、昇順レジスタおよび降順レジスタを組み込んだEEPROMであってよい。知られているように、メータユニットにおける昇順レジスタは、全ての取引において、支払われた、すなわち金庫により発行された郵便料金額を記録し、降順レジスタは、郵便料金が発行されるときに価値が減少するメータユニットに残っている郵便料金額を記録する。

20

30

【0015】

金庫のハードウェア設計が、PCMCIAコントローラ32を通じてホストプロセッサ22と通信するインタフェース56を備える。好ましくは、物理的なセキュリティを付加するために、暗号化を行い暗号鍵を記憶する金庫20のコンポーネント(マイクロプロセッサ44、ROM47およびNVM46)が、改竄のおそれのないように製造された同一の集積回路装置/チップにおいてパッケージングされる。このようなパッケージングは、NVM46の内容が、暗号化プロセッサによってのみ読み取られ、集積回路装置の外側でアクセス不能であることを保証する。代わりに、カード30全体が、改竄のおそれのないように製造されてもよい。

40

各NVM46のメモリが、セクションに組織される。各セクションは、金庫20が行った取引の履歴データを含む。このタイプの取引の例として、郵便料金の支払、トークンの発行、再充填、パラメータ構成、および郵便およびベンダの識別が含まれる。次に、各セクションは、取引記録に分割される。セクション内で、取引記録の長さは同一である。取引記録の構造は、金庫がデータの完全性を照合することができるものである。

【0016】

DLL40の機能は、PCベースのメータ10の鍵コンポーネントである。DLL40は、PC12のハードドライブ24に常駐する実行可能コードおよびデータ記憶領域41の両方を備える。ウィンドウズ環境においては、ワードプロセッシングおよび表計算プロ

50

グラムのような非常に多くのアプリケーションプログラム36が、1つ以上の動的リンクライブラリを用いて互いに通信する。PCベースのメータ10は、メータ処理に含まれる全てのプロセスをカプセル化し、動的リンクライブラリを使用できる全てのウィンドウズベースのアプリケーションから金庫20にオープンインタフェースを供給する。いかなるアプリケーションプログラム36も、DLL40を通じてPCMCIAカード30内の金庫マイクロプロセッサ44と通信することができる。

【0017】

DLL40は、以下のソフトウェアサブモジュールを含む。セキュリティのある通信サブモジュール80が、PC12と金庫20の間の通信を制御する。取引捕獲サブモジュール82が、PC12内に取引記録を記憶する。セキュリティのある証印イメージ生成および記憶サブモジュール84が、証印ビットマップイメージを生成し、後続の印刷に対するイメージを記憶する。アプリケーションインタフェースサブモジュール86が、非メータ処理アプリケーションプログラムにインタフェースし、非メータ処理アプリケーションプログラムによる証印に対するリクエストにตอบสนองして、デジタルトークンに対するリクエストを発行する。

PCメータシステム10のより詳細な説明が、本願と同時に出願された米国特許出願第08/575,112号に開示されており、これは本明細書の一部として組み込まれる。

【0018】

プリンタ18がメータ機能専用のものではないために、後に、ユーザの判断で対応する証印が生成され印刷されるときに使用するために、発行されるデジタルトークンが、PC12において要求され、計算されて、記憶されてもよい。このようなディレド印刷およびバッチ処理は、係属中の米国特許出願第08/575,104号(米国特許第5,835,689号)に開示されており、これは、本明細書の一部として組み込まれる。

デジタルトークン生成プロセス

本発明によると、デジタルトークンに対するリクエストがPC12から受け取られるとき、金庫20が、このリクエストに応じて、少なくとも1つのデジタルトークンを計算し、PC12に発行する。発行されたデジタルトークンは、後に印刷するためにPC12における取引記録の一部として記憶される。本発明の好ましい具体例においては、取引記録が、ハードドライブ24上のDLL記憶領域41内の隠蔽ファイルにおいて記憶される。各取引記録は、受取人情報に従って、隠蔽ファイルにおいて索引を付けられる。デジタルトークンを発行して記憶する方法は、トークンが印刷されなかった場合はいつでも、またはトークンを有する証印の印刷が妨げられる問題が生じた場合には、1つ以上のデジタルトークンが再発行できるという利点を与える。

【0019】

デジタルトークンをPC12において取引記録の一部として記憶することによって、デジタルトークンが、PC12において行われる証印の生成および印刷に対して、後にアクセスされることができる。さらに、デジタルトークンがない場合、すなわち郵便物上に適切に印刷されなかった場合には、デジタルトークンが、金庫20からというよりはDLL40から再発行されることができる。各取引の終了時の金庫の状態を含む取引記録の記憶が、発行されたトークンの記録と同様に会計情報に関しても金庫に対してバックアップを提供する。ハードドライブ24に記憶される取引記録の数は、好ましくは金庫20を最後に再充填してから全ての取引を含んだ所定の数に制限されてよい。

図5~7を参照すると、ステップ200で、金庫20に対して電源が入れられ、すなわちカード30がコントローラ32に挿入されるとき、金庫が自身をイニシャライズする。ステップ202で、金庫20が、冗長NVM46に記憶された資金の完全性を照合する。悪い場合には、ステップ204で、金庫20が自身をディスエーブル状態に設定する。NVMデータが正しい場合には、ステップ206で、郵便資金に関連するレジスタ、すなわち昇順、降順および郵便物カウトレジスタが、RAM45に対してロードされ、直前の取引記録が、RAM45にロードされる。NVM46のデータ完全性を検証し、最近の取引記録を金庫のRAM45に複写した後、ステップ208で、金庫20がイニシャライズさ

10

20

30

40

50

れ、その後外部コマンドを待つ。

【 0 0 2 0 】

ステップ 2 1 0 で状態コマンドが受け取られると、金庫 2 0 は、ステップ 2 1 2 で P C 1 2 にその現在の状態を応え、ステップ 2 0 8 で他のコマンドを受け取るのを待つ。ステップ 2 1 4 で、金庫 2 0 の機能にアクセスするためにパスワードが要求される場合には、ステップ 2 1 6 で、入力されたパスワードが正確かどうかを照合される。パスワードが要求されない場合、又は正しいパスワードがステップ 2 1 6 で検出された場合は、金庫は日付コマンドを確認する。ステップ 2 1 6 で正しくないパスワードが入力された場合は、金庫 2 0 は P C 1 2 にその現在の状況を応答し、ステップ 2 0 8 で他のコマンドを受け取るのを待つ。

10

ステップ 2 1 8 で、日付を設定するコマンドが受け取られたときは、ステップ 2 2 0 で、特定の月の最初に、金庫が日付を設定し、金庫の N V M 4 6 に記憶されたマスター鍵から、その月に関するトークン生成鍵を得て、そしてステップ 2 1 2 で D L L 4 0 を介してユーザアプリケーションプログラム 3 6 に状態メッセージを送り、ステップ 2 0 8 で他のコマンドを受け取るのを待つ。この金庫は、それから自身をイネーブル状態にし、トークンリクエストコマンドを受け入れる準備をする。日付が一旦設定され、別の日付設定コマンドが同じ月で受け取られるとき、この金庫は、単純にこのコマンドを承認し、このトークン生成鍵を再計算することなく日付を設定する。ステップ 2 1 8 で日付コマンドが受け取られないと、ステップ 2 2 4 で、郵便料金コマンドが受け取られ、ステップ 2 2 6 で、例えば 32 ドルの郵便料金額が設定される。

20

【 0 0 2 1 】

ステップ 2 2 8 で、送付先郵便コードを含むトークンリクエストコマンドが、金庫 2 0 により受け取られたとき、ステップ 2 3 4 ~ 2 4 0 で、リクエストの評価のフォーマットおよび範囲が金庫によって照合される。リクエストが不適切な場合には、金庫 2 0 が、リクエストを拒絶し、ステップ 2 3 0 で問い合わせのような他のコマンドを処理し、ステップ 2 0 8 でコマンドを受信するのを待つ。ステップ 2 2 8 でリクエストが適切であると判断されると、金庫 2 0 はステップ 2 3 4 でそのリクエストの日付を照合し、日付が設定されると金庫はステップ 2 3 6 でリクエストされた郵便料金額を 2 つの警告値、すなわち高い値の警告値及び郵便料金限度額と比較する。ステップ 2 3 4 で日付が設定されない場合、ステップ 2 1 2 で D L L 4 0 を介してユーザアプリケーションプログラム 3 6 に送られる。ステップ 2 3 6 で、リクエストされた郵便料金額が警告値を超える場合には、このリクエストは拒絶され、状態メッセージは、ステップ 2 1 2 で D L L 4 0 を介してユーザアプリケーションプログラム 3 6 に状態メッセージを送る。次に金庫 2 0 は、ステップ 2 3 8 で、リクエストされた郵便料金額を、降順レジスタにおいて利用可能な郵便資金と比較する。利用可能な郵便資金額がリクエストされた額よりも小さければ、この金庫は、トークンリクエストコマンドを拒絶し、ステップ 2 1 2 で D L L 4 0 を介してユーザアプリケーションプログラム 3 6 に適切なメッセージを送る。利用可能な郵便資金額が、リクエストされた額に等しいか又はそれよりも多いときには、金庫 2 0 が、ステップ 2 4 0 で送付先情報を照合する。ステップ 2 4 0 で郵便番号のフォーマットが適切であれば、ステップ 2 4 2 で会計プロセスが開始される。それが適切でなければ、ステップ 2 1 2 で、状態メッセージが D L L 4 0 を介してユーザアプリケーションプログラム 3 6 に送られる。

30

40

【 0 0 2 2 】

最終的に、ステップ 2 4 2 で、金庫 2 0 が、デジタルトークンを発行する会計プロセスを開始する。金庫 2 0 は、利用可能な郵便資金からリクエストされた郵便料金額を差し引き、すなわち R A M において、その額を昇順レジスタに加え、その額を降順レジスタから引く。ステップ 2 4 4 で、デジタルトークンが、受取人情報を含むオープンシステムアルゴリズムを用いて計算される。ステップ 2 4 6 で、金庫 2 0 が、R A M 4 5 において、郵便物カウントおよび計算されたトークンを含む取引記録を構成し、冗長 N V M 4 6 の索引付きファイルに取引記録を記憶する。好ましい具体例においては、N V M 取引ファイルが、郵便物カウントにより索引を付けられる。N V M に記憶した後は、ステップ 2 4

50

8で、金庫20が、NVM46の完全性を照合し、データが正確に記憶されていることを確認する。このプロセス中にエラーが生じた場合には、トークンは発行されず、エラーメッセージが、PC12内のホストプロセッサに報告される。エラーが発生しない場合には、取引記録を含む伝送バッファがアセンブルされ、ステップ250で、金庫20がPC12内のDLL40に取引記録を送る。ステップ252で、取引記録がDLL40中及びDLL記憶領域41中に記憶される。金庫20がPC12から肯定的な承認を受け取らない場合には、金庫20が、メッセージを再送信する。

【0023】

従来の郵便料金メータは、メータ内に取引を記憶する。本発明に従うと、取引捕獲サブモジュール82が、金庫20から受け取られる各取引記録を捕獲し、履歴記録用に、DLL40およびハードドライブ24上のDLL記憶領域41に取引記録を記録する。ハードドライブ24上に十分な空きがある場合には、このような取引捕獲が、複数の異なる金庫に対して記憶されることが可能である。図8を参照すると、通信セッションが達成される瞬間から、ステップ120で、取引捕獲サブモジュール82がメッセージトラフィックをモニターし、トークンの生成および再充填に対して各取引記録を選択的に捕獲し、ステップ124で、DLL40内にこの取引記録を記憶し、ステップ126で、DLL記憶領域41内の内密のライトプロテクトされたファイル83に記憶する。各取引記録に対して記憶された情報は、例えば、金庫連続番号、日付、郵便物カウント、郵便料金、利用可能郵便資金（降順レジスタ）、トークン、送付先郵便コード、およびブロックチェックキャラクタ（BCC）を含む。PC12により開始される所定の数の最近の記録が、郵便物カウントに従って索引を付けられる履歴ファイルであるファイル83に記憶される。ファイル83は、暗号鍵および構成パラメータを除いた取引時の金庫20の鏡像を表す。取引記録をハードドライブ24上に記憶することが、以下に説明されるバックアップ機能を与える。本発明によると、取引記録が、所定の時間またはカウントに関して、複数の発行されたデジタルトークンに対して維持される。

【0024】

本発明によると、図10に示される証印92の全体の固定グラフィックスイメージ90が、DLL記憶領域41内に圧縮データ94として記憶されている。郵便物カウント93a、ペндаID93b、郵便料金額93c、シリアルナンバ93d、日付93e、および出所ジップ93f、およびトークン93gを含んだ郵便データ情報が、証印イメージ生成モジュール84によって固定のグラフィックスイメージ90に組み合わされる。

図9を参照すると、ステップ142で、証印に対するリクエストがPC12内のアプリケーションプログラムから生成されるとき、証印イメージ生成モジュール84が、ステップ144で、金庫20からのデジタルトークンを照合し、ステップ146で、ビットマップ証印イメージ96を生成し、ステップ148で固定グラフィックスイメージの圧縮データ94を伸長し、ステップ150で、証印の固定グラフィックスイメージ90を、金庫20から受け取られる郵便データ情報およびトークンのいくつか又は全てに組み合わせる。ステップ152で、証印イメージが、印刷するためにDLL40に記憶される。サブモジュール84が、PC12のリクエストするアプリケーションプログラム36に、印刷する準備のできた生成されたビットマップ証印イメージ96を送り、デジタルトークンと関連する郵便データを含んだ取引記録をDLL記憶領域41内に記憶する。この時、証印が、すぐに又はその後印刷されることが可能である。

【0025】

従って、ビットマップ証印イメージ96が、DLL40内に記憶され、それは、DLL40内の実行可能コードによってのみアクセス可能である。さらに、DLL40の実行可能コードだけが、生成されたビットマップ証印イメージ96に対する証印の固定グラフィックスイメージ90にアクセスできる。通常のユーザが、意図的に又はそれとは別に、証印の固定グラフィックスイメージ90およびビットマップ証印イメージ96にアクセスすることが非常に困難であるために、このことは、証印が不慮に変更されることを阻止する。本発明は、受取人のリストを一度に入力するというよりは、郵送リストに受取人に関する

10

20

30

40

50

トークンのバッチを生成するのに適する。トークンのバッチは、D L L 記憶領域 4 1 内の取引ファイルに索引を付けられた取引記録のバッチの一部であり、郵送リストに関して封筒に印刷するときに、後に証印イメージを生成するために用いられる。このようなバッチ処理は、例えば郵便を生成するためのアドレスのデータベースを有するプロダクション郵送者に対して有用である。これらのデータベースは、通常は前処理されてソートされ、直接の市場販売の機会に対して、郵便料の割引や受取人のプロフィールを利用する。

【 0 0 2 6 】

別の具体例においては、P C ベースのオープンメータシステムが、サーバ P C に接続された金庫と、ユーザ P C からユーザがリクエストする郵便料金を備えたネットワークの一部である。トークン生成プロセスは、トークン生成を含む金庫の機能がサーバ P C 又は接続された金庫カードにおいて生じることを除いては、前述したように進んでいく。サーバ P C は、バックアップおよび災難に対する回復のために、全ての取引の記録を記憶する。ユーザ P C は、発行されたトークンを含む取引記録を、そのハードドライブに記憶し、それに対応する証印を生成する。この構成は、多くのユーザが、トークンの生成を禁止されずに、同一の受取人に手紙を送ることが可能となる。

本発明は、1つの具体例に関連して開示され説明されてきたが、上述したように、様々な変更および修正が本発明の範囲内でなされてもよいことは明らかであろう。従って、特許請求の範囲に記載した事項は、本発明の真の精神および範囲内の各々の変更および修正を含むものとして意図される。

【 図面の簡単な説明 】

【 図 1 】 本発明が作動する P C ベースのメータシステムのブロック図である。

【 図 2 】 取外し可能金庫カードおよび P C 内の D L L を含んだ図 1 の P C ベースのメータシステムの構成概略図である。

【 図 3 】 デジタルトークンを発行し記憶する金庫との相互作用を含んだ図 1 の P C ベースのメータシステムにおける D L L の構成概略図である。

【 図 4 】 図 1 の P C ベースのメータシステムにおける D L L サブモジュールのブロック図である。

【 図 5 】 本発明のデジタルトークン生成プロセスのフローチャートである。

【 図 6 】 本発明のデジタルトークン生成プロセスのフローチャートである。

【 図 7 】 本発明のデジタルトークン生成プロセスのフローチャートである。

【 図 8 】 図 1 の P C ベースのメータシステムに、発行されたデジタルトークンを含んだ取引記録を記憶する P C のフローチャートである。

【 図 9 】 図 1 の P C ベースのメータシステムにおいてデジタルトークンに対する証印イメージを生成する P C のフローチャートである。

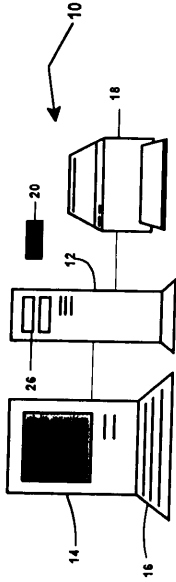
【 図 1 0 】 図 1 の P C ベースのメータシステムにより生成され印刷された証印を示す。

10

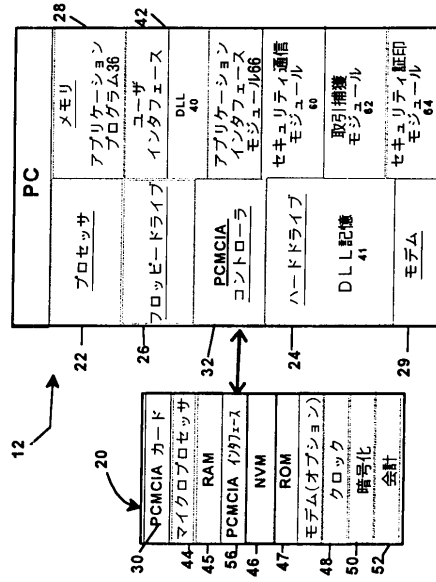
20

30

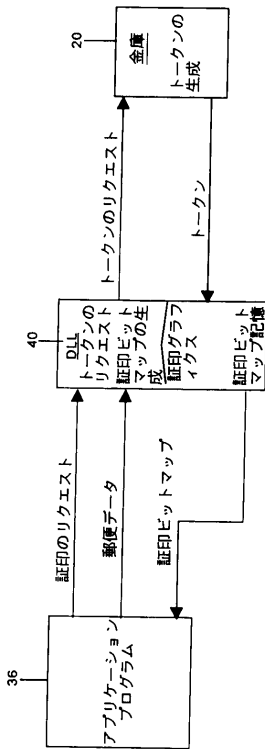
【図1】



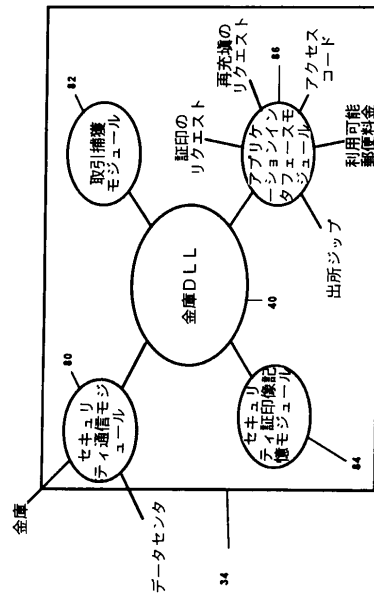
【図2】



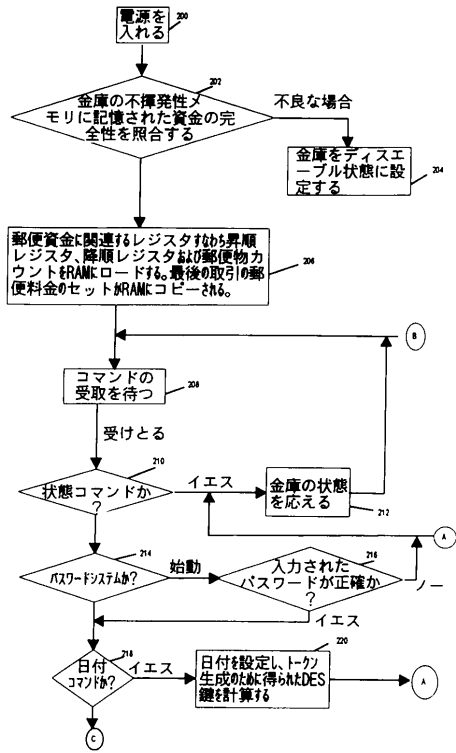
【図3】



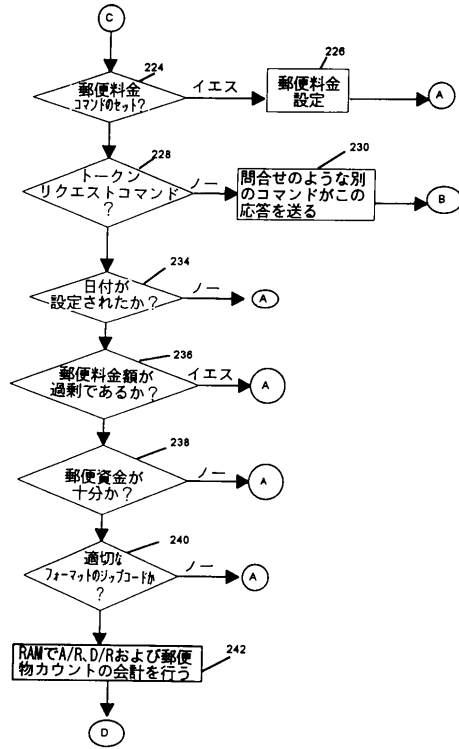
【図4】



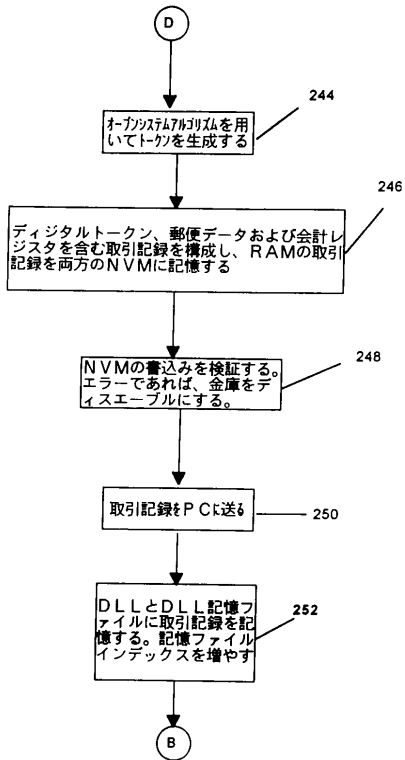
【図5】



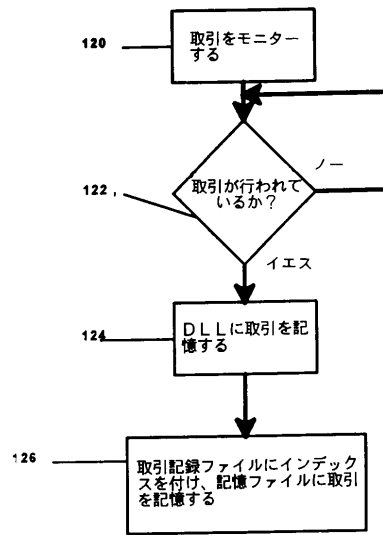
【図6】



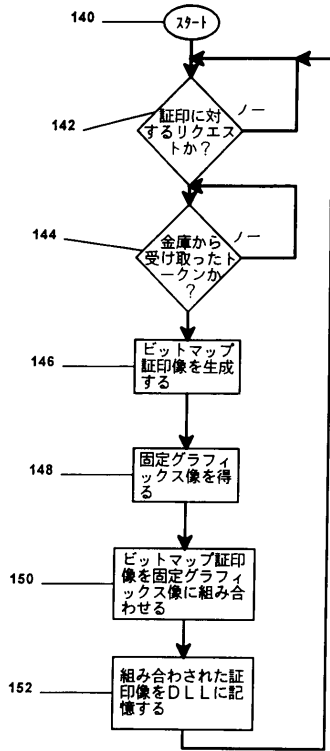
【図7】



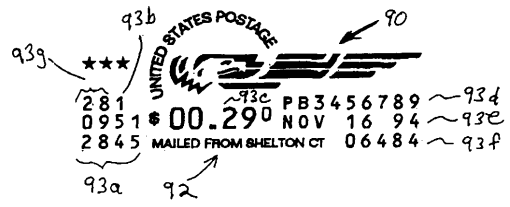
【図8】



【 図 9 】



【 図 10 】



フロントページの続き

(74)代理人 100084009

弁理士 小川 信夫

(72)発明者 ディヴィッド ケイ リー

アメリカ合衆国 コネチカット州 06468 モンロー アルパイン ロード 12

(72)発明者 ディヴィッド ダブリュー ライリー

アメリカ合衆国 コネチカット州 06612 イーストン ウッドランド ドライヴ 31

(72)発明者 フレデリック ダブリュー ライアン ジュニア

アメリカ合衆国 コネチカット州 06478 オックスフォード ネイブルズ レーン 4

合議体

審判長 千葉 成就

審判官 菅澤 洋二

審判官 佐々木 一浩

(56)参考文献 国際公開第95/19016(WO, A1)

(58)調査した分野(Int.Cl., DB名)

G07B17/00