(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4132530号
(P4132530)
(45)発行日　平成20年8月13日(2008.8.13)　(24)登録日　平成20年6月6日(2008.6.6)

(51)Int.Cl.　F I
G06F 21/24 (2006.01)　G06F 12/14 560B
G06F 12/14 560C
G06F 12/14 540B

請求項の数 9　(全 16 頁)

(21)出願番号　特願2000-15092(P2000-15092)
(22)出願日　平成12年1月24日(2000.1.24)
(65)公開番号　特開2001-209582(P2001-209582A)
(43)公開日　平成13年8月3日(2001.8.3)
審査請求日　平成16年5月17日(2004.5.17)

(73)特許権者　000006747
株式会社リコー
東京都大田区中馬込１丁目３番６号
(74)代理人　100104190
弁理士　酒井　昭徳
(72)発明者　金井　洋一
東京都大田区中馬込１丁目３番６号　株式会社リコー内
(72)発明者　谷内田　益義
東京都大田区中馬込１丁目３番６号　株式会社リコー内

審査官　小林　秀和

最終頁に続く

(54)【発明の名称】電子保存装置

(57)【特許請求の範囲】
【請求項１】
記録媒体に格納した保存データの内容を確定的なものとして最初に作成した文書であることを保証する原本の電子データを内部記録媒体に保存し、障害発生時においても前記内部記録媒体に保存された前記電子データの保存時の状態を保証する電子保存装置において、
前記内部記憶媒体に格納され、装置設定ファイル、媒体認証コードリストファイル、内部タイマ設定履歴ファイル、アカウント管理リストファイルを含む管理情報を一括して内部管理情報一括データとして生成し、当該内部管理情報一括データを暗号化してバックアップ情報を生成するバックアップ情報生成手段と、
前記内部記憶媒体に格納した管理情報を喪失した場合に、前記暗号化されたバックアップ情報を復号化して前記管理情報を前記内部記憶媒体にリストアするリストア手段と、
を備えたことを特徴とする電子保存装置。
【請求項２】
前記バックアップ情報生成手段は、外部システムからバックアップ要求を受け付けた場合に、前記内部記憶媒体に格納した管理情報を第１の暗号鍵で暗号化したバックアップ情報を作成し、作成したバックアップ情報を出力することを特徴とする請求項１に記載の電子保存装置。
【請求項３】
前記バックアップ情報生成手段は、装置本体に装着したＩＣカードの内部に保持した第

１の暗号鍵および第１の復号鍵を用いて前記バックアップ情報の作成または復号をおこなうことを特徴とする請求項２に記載の電子保存装置。

【請求項４】

前記バックアップ情報生成手段は、

外部システムからバックアップ要求を受け付けた場合に、前記内部記憶媒体に格納した管理情報を所定の乱数により暗号化する第１の暗号化手段と、

前記第１の暗号化手段による暗号化に用いた前記乱数を前記第１の暗号鍵により暗号化する第２の暗号化手段と、

前記第１の暗号化手段により暗号化された暗号化管理情報および前記第２の暗号化手段により暗号化された暗号化乱数を前記バックアップ情報として出力する出力手段と、

を備えたことを特徴とする請求項１に記載の電子保存装置。

【請求項５】

前記リストア手段は、

前記バックアップ情報に含まれる暗号化乱数を前記第１の復号鍵で復号化する第１の復号化手段と、

前記第１の復号化手段により復号化された乱数で前記暗号化管理情報を復号化する第２の復号化手段と、

前記第２の復号化手段により復号化された管理情報を前記内部記憶媒体に記録する記録手段と、

を備えたことを特徴とする請求項４に記載の電子保存装置。

【請求項６】

前記出力手段は、

前記第１の暗号化手段により暗号化された暗号化管理情報に前記第２の暗号化手段により暗号化された暗号化乱数を付与して暗号化内部情報を作成する暗号化内部情報作成手段と、前記暗号化内部情報作成手段により作成された暗号化内部情報のハッシュ値を算定する第１のハッシュ値算定手段とを備え、

前記ハッシュ値算定手段により算定されたハッシュ値を前記暗号化内部情報作成手段により作成された暗号化内部情報とともに前記バックアップ情報として出力することを特徴とする請求項４に記載の電子保存装置。

【請求項７】

前記リストア手段は、

前記バックアップ情報に含まれる暗号化内部情報のハッシュ値を算定する第２のハッシュ値算定手段と、

前記第２のハッシュ値算定手段により算定されたハッシュ値と前記バックアップ情報に含まれるハッシュ値とを比較する比較手段と、

前記比較手段により両ハッシュ値が一致すると判断された場合に、前記暗号化乱数を前記第１の暗号鍵に対応する第１の復号鍵で復号化する第１の復号化手段と、

前記第１の復号化手段により復号化された乱数を用いて前記暗号化管理情報を復号化する第２の復号化手段と、

を備えたことを特徴とする請求項６に記載の電子保存装置。

【請求項８】

前記出力手段は、前記ハッシュ値算定手段により算定されたハッシュ値を第２の暗号鍵を用いて暗号化した暗号化ハッシュ値を前記暗号化内部情報作成手段により作成された暗号化内部情報とともに前記バックアップ情報として出力し、

前記比較手段は、前記第２の暗号鍵に対応する第２の復号鍵を用いて前記暗号化ハッシュ値を復号化したハッシュ値と前記第２のハッシュ値算定手段により算定されたハッシュ値とを比較することを特徴とする請求項７に記載の電子保存装置。

【請求項９】

前記第１の暗号鍵および前記第２の復号鍵は公開鍵暗号系の公開鍵であり、前記第２の暗号鍵および前記第１の復号鍵は前記公開鍵暗号系の秘密鍵であることを特徴とする請求

項８に記載の電子保存装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
この発明は、内部記憶媒体に保存された電子データを所定の管理情報に基づいて保存状態を保証する電子保存装置に関し、特に、なんらかの障害が発生した場合であっても、内部記憶媒体に記憶した内部管理情報を迅速に復旧し、もって電子データの保存時の状態を保証できる電子保存装置に関する。
【０００２】
【従来の技術】
近年のコンピュータ技術の進展に伴うペーパーレス化の進展に伴って、紙によって原本書類として保存されていた情報が電子データの形式で保存される場合が増えてきたため、かかる電子データの原本性を保証する従来技術が知られている。
【０００３】
たとえば、「金井他：原本性保証電子保存システムの開発－システムの構築－, Medical Imaging Technology, Vol.16, No.4, Proceedings of JAMIT Annual Meeting'98(1998)」や、「国分他：原本性保証電子保存システムの開発, （特）情報処理振興事業協会発行　創造的ソフトウエア育成事業およびエレクトロニック・コマース推進事業　最終成果発表会論文集　創造的ソフトウエア育成事業編(1998)」には、電子データの原本性を保証するシステムの一例が開示されている。
【０００４】
かかる従来技術を用いると、電子データの原本性を保証することが可能となり、これにより原本書類を電子データの形式で保存し、もって高度情報化社会の推進並びに社会全体の生産性向上に寄与することができる。
【０００５】
【発明が解決しようとする課題】
しかしながら、これらの従来技術は、原本となる電子データを格納する大容量記憶媒体以外は、あるレベルの耐タンパー性を持った筐体に格納されていることを前提とするため、原本性保証電子保存装置になんらかの障害が生じた場合に、その障害対処に時間を要する。
【０００６】
具体的には、電子データの原本性を保証するためには、内部記憶媒体に記憶した内部管理情報を通常利用することとなるが、この内部記憶媒体に記憶した内部管理情報が障害などによって失われると、耐タンパー性が保持されているためにかえってその復旧に時間を要する結果となる。
【０００７】
このため、なんらかの障害が発生した場合であっても、内部記憶媒体に記憶した内部管理情報を迅速に復旧し、もって電子データの原本性を迅速かつ効率良く保証することができる原本性保証電子保存装置をいかに実現するかが極めて重要な課題となっている。
【０００８】
この発明は、上記問題（課題）に鑑みてなされたものであり、なんらかの障害が発生した場合であっても、内部記憶媒体に記憶した内部管理情報を迅速に復旧し、もって電子データの保存時の状態を保証することができる電子保存装置を提供することを目的とする。
【０００９】
【課題を解決するための手段】
上記目的を達成するために、この発明は、記録媒体に格納した保存データの内容を確定的なものとして最初に作成した文書であることを保証する原本の電子データを内部記録媒体に保存し、障害発生時においても前記内部記録媒体に保存された前記電子データの保存時の状態を保証する電子保存装置において、前記内部記憶媒体に格納され、装置設定ファイル、媒体認証コードリストファイル、内部タイマ設定履歴ファイル、アカウント管理リ

ストファイルを含む管理情報を一括して内部管理情報一括データとして生成し、当該内部管理情報一括データを暗号化してバックアップ情報を生成するバックアップ情報生成手段と、前記内部記憶媒体に格納した管理情報を喪失した場合に、前記暗号化されたバックアップ情報を復号化して前記管理情報を前記内部記憶媒体にリストアするリストア手段と、を備えたことを特徴とする。

【００１０】

この発明によれば、内部記憶媒体に格納した管理情報のバックアップ情報を生成しておき、この内部記憶媒体に格納した管理情報を喪失した場合に、生成されたバックアップ情報を内部記憶媒体にリストアすることとしたので、なんらかの障害が発生した場合であっても、内部記憶媒体に記憶した内部管理情報を迅速に復旧し、もって電子データの保存時の状態を迅速かつ効率良く保証することができる。また、暗号化されたバックアップ情報を正しく復号化して内部記憶媒体にリストアすることができる。

【００１１】

また、前記バックアップ情報生成手段は、外部システムからバックアップ要求を受け付けた場合に、前記内部記憶媒体に格納した管理情報を第１の暗号鍵で暗号化したバックアップ情報を作成し、作成したバックアップ情報を出力することを特徴とする。

【００１２】

この発明によれば、外部システムからバックアップ要求を受け付けた場合に、内部記憶媒体に格納した管理情報を第１の暗号鍵で暗号化したバックアップ情報を作成し、作成したバックアップ情報を出力することとしたので、バックアップ情報の暗号強度を高めることができる。

【００１３】

また、前記バックアップ情報生成手段は、装置本体に装着したＩＣカードの内部に保持した第１の暗号鍵および第１の復号鍵を用いて前記バックアップ情報の作成または復号をおこなうことを特徴とする。

【００１４】

この発明によれば、装置本体に装着したＩＣカードの内部に保持した第１の暗号鍵および第１の復号鍵を用いてバックアップ情報の作成または復号をおこなうこととしたので、ＩＣカードに応じて暗号鍵および復号鍵を自在に変更することができる。

【００１５】

また、前記バックアップ情報生成手段は、外部システムからバックアップ要求を受け付けた場合に、前記内部記憶媒体に格納した管理情報を所定の乱数により暗号化する第１の暗号化手段と、前記第１の暗号化手段による暗号化に用いた前記乱数を前記第１の暗号鍵により暗号化する第２の暗号化手段と、前記第１の暗号化手段により暗号化された暗号化管理情報および前記第２の暗号化手段により暗号化された暗号化乱数を前記バックアップ情報として出力する出力手段と、を備えたことを特徴とする。

【００１６】

この発明によれば、外部システムからバックアップ要求を受け付けた場合に、内部記憶媒体に格納した管理情報を所定の乱数により暗号化し、暗号化に用いた乱数を第１の暗号鍵により暗号化し、暗号化した暗号化管理情報および暗号化乱数をバックアップ情報として出力することとしたので、単に管理情報を暗号化するだけでなく、この暗号化に用いた乱数についても暗号化して出力することができる。

【００１７】

また、前記リストア手段は、前記バックアップ情報に含まれる暗号化乱数を前記第１の復号鍵で復号化する第１の復号化手段と、前記第１の復号化手段により復号化された乱数で前記暗号化管理情報を復号化する第２の復号化手段と、前記第２の復号化手段により復号化された管理情報を前記内部記憶媒体に記録する記録手段と、を備えたことを特徴とする。

【００１８】

この発明によれば、バックアップ情報に含まれる暗号化乱数を第１の復号鍵で復号化し

、復号化した乱数で暗号化管理情報を復号化し、この復号化された管理情報を内部記憶媒体に記録することとしたので、暗号化された管理情報を正しく復号化して内部記憶媒体にリストアすることができる。

【００１９】

また、前記出力手段は、前記第１の暗号化手段により暗号化された暗号化管理情報に前記第２の暗号化手段により暗号化された暗号化乱数を付与して暗号化内部情報を作成する暗号化内部情報作成手段と、前記暗号化内部情報作成手段により作成された暗号化内部情報のハッシュ値を算定する第１のハッシュ値算定手段とを備え、前記ハッシュ値算定手段により算定されたハッシュ値を前記暗号化内部情報作成手段により作成された暗号化内部情報とともに前記バックアップ情報として出力することを特徴とする。

【００２０】

この発明によれば、暗号化された暗号化管理情報に暗号化乱数を付与して暗号化内部情報を作成し、作成した暗号化内部情報のハッシュ値を算定し、算定したハッシュ値を暗号化内部情報とともにバックアップ情報として出力することとしたので、暗号化内部情報の改ざんを効率良く防止することができる。

【００２１】

また、前記リストア手段は、前記バックアップ情報に含まれる暗号化内部情報のハッシュ値を算定する第２のハッシュ値算定手段と、前記第２のハッシュ値算定手段により算定されたハッシュ値と前記バックアップ情報に含まれるハッシュ値とを比較する比較手段と、前記比較手段により両ハッシュ値が一致すると判断された場合に、前記暗号化乱数を前記第１の暗号鍵に対応する第１の復号鍵で復号化する第１の復号化手段と、前記第１の復号化手段により復号化された乱数を用いて前記暗号化管理情報を復号化する第２の復号化手段と、を備えたことを特徴とする。

【００２２】

この発明によれば、バックアップ情報に含まれる暗号化内部情報のハッシュ値を算定し、算定したハッシュ値とバックアップ情報に含まれるハッシュ値とを比較し、両ハッシュ値が一致すると判断された場合に、暗号化乱数を第１の暗号鍵に対応する第１の復号鍵で復号化し、復号化した乱数を用いて暗号化管理情報を復号化することとしたので、バックアップ情報が改ざんされているか否かを効率良く判断し、改ざんされていないことを条件として内部記憶媒体への管理情報の設定をおこなうことができる。

【００２３】

また、前記出力手段は、前記ハッシュ値算定手段により算定されたハッシュ値を第２の暗号鍵を用いて暗号化した暗号化ハッシュ値を前記暗号化内部情報作成手段により作成された暗号化内部情報とともに前記バックアップ情報として出力し、前記比較手段は、前記第２の暗号鍵に対応する第２の復号鍵を用いて前記暗号化ハッシュ値を復号化したハッシュ値と前記第２のハッシュ値算定手段により算定されたハッシュ値とを比較することを特徴とする。

【００２４】

この発明によれば、算定されたハッシュ値を第２の暗号鍵を用いて暗号化した暗号化ハッシュ値を暗号化内部情報とともにバックアップ情報として出力し、この第２の暗号鍵に対応する第２の復号鍵を用いて暗号化ハッシュ値を復号化したハッシュ値と算定されたハッシュ値とを比較することとしたので、暗号化ハッシュ値を用いてバックアップ情報の改ざんを防止することができる。

【００２５】

また、前記第１の暗号鍵および前記第２の復号鍵は公開鍵暗号系の公開鍵であり、前記第２の暗号鍵および前記第１の復号鍵は前記公開鍵暗号系の秘密鍵であることを特徴とする。

【００２６】

この発明によれば、第１の暗号鍵および第２の復号鍵を公開鍵暗号系の公開鍵とし、第２の暗号鍵および第１の復号鍵を公開鍵暗号系の秘密鍵としたので、公開鍵暗号系を用い

てバックアップ情報の暗号強度を高めることができる。

【００２７】

【発明の実施の形態】

以下に添付図面を参照して、この発明にかかる電子保存装置の好適な実施の形態を詳細に説明する。以下の説明において電子データの原本性とは、大容量記憶媒体に保存した電子データの保存状態を維持することを意味する。

【００２８】

図１は、本実施の形態において用いる原本性保証電子保存装置の構成を示すブロック図である。同図に示す原本性保証電子保存装置１００は、原本の電子データを大容量記憶媒体１０１上に保存しておき、内部記憶媒体１０４に格納した管理情報などを用いてこの電子データの保存時の状態を保証することようにした装置である。

【００２９】

ここで、この原本性保証電子保存装置１００になんらかの障害が発生した場合には、内部記憶媒体１０４に格納した情報が失われてしまい、電子データの原本性を保証することができなくなる。特に、大容量記憶媒体１０１以外は耐タンパー性を持った筐体に格納されるため、管理情報を簡易に再設定することは難しい。

【００３０】

このため、この原本性保証電子保存装置１００では、内部記憶媒体１０４に格納した管理情報をバックアップするとともに、この原本性保証電子保存装置１００になんらかの障害が発生した場合には、バックアップした管理情報を内部記憶媒体１０４にリストアするよう構成している。

【００３１】

ただし、かかる管理情報は、そもそも原本となる電子データの原本性を保証するために用いるものであり、むやみに装置外部に保持すべきものではないので、その暗号強度を高めることで、本来の原本性保証に影響を与えないようにしている。

【００３２】

同図に示すように、この原本性保証電子保存装置１００は、大容量記憶媒体１０１と、通信ポート１０２と、プログラム格納媒体１０３と、内部記憶媒体１０４と、内部タイマ１０５と、バックアップ処理部１０６と、リストア処理部１０７と、制御部１０８とからなる。

【００３３】

大容量記憶媒体１０１は、原本となる電子データなどを記憶する大容量の二次記憶装置であり、たとえば光磁気ディスクやＣＤ－Ｒなどからなる。この大容量記憶媒体１０１は、図中に破線で示したように原本性保証電子保存装置１００から取り外し可能としても良いが、その他の構成部位については原本性保証電子保存装置１００と物理的に一体化し、通信ポート１０２以外からのアクセスを受け付けない耐タンパー性を有する構成にする。

【００３４】

ただし、この耐タンパー性には、筐体を開けられないようにシールを貼る程度のレベルから、筐体を開けた場合に装置が動作しなくなるレベルまで様々なものがあるが、本発明はこの耐タンパー性のレベルには特段の制限を受けない。

【００３５】

通信ポート１０２は、ネットワークを介して外部システム１１０との通信をおこなうためのインターフェース部であり、たとえばＬＡＮカードなどの通信モデムなどからなる。

【００３６】

プログラム格納媒体１０３は、主制御プログラム、ハッシュプログラム、鍵生成プログラム、暗号化プログラムおよび復号化プログラムなどの各種プログラムを格納したメモリであり、たとえば書換可能なＥＥＰＲＯＭや読み出し専用のＲＯＭなどからなる。

【００３７】

内部記憶媒体１０４は、各種プログラムの実行に必要となるパラメータを記憶するＥＥＰＲＯＭなどからなるメモリであり、具体的には、装置暗号鍵、装置復号鍵、媒体認証コ

ードリスト、最新データ識別番号、タイマ設定履歴ファイルおよびアカウント管理リストなどを記憶する。内部タイマ１０５は、制御部１０８の本体をなすプロセッサがプログラムの実行時に所得する時刻を計時するタイマである。

【００３８】

バックアップ処理部１０６は、乱数および公開鍵などを用いて内部記憶媒体１０４に格納した管理情報のバックアップ情報を生成する処理部であり、具体的には、内部記憶媒体１０４から装置設定ファイルなどの後述する各種ファイルを読み出して内部管理情報一括データとする。その後、装置内部で乱数を生成してこの乱数を公開鍵で暗号化して、暗号化乱数を作成するとともに、該乱数で内部管理情報一括データを一括して暗号化し、これに暗号化乱数を付与して内部管理情報一括暗号化データとする。

【００３９】

その後、この内部管理情報一括暗号化データについてのハッシュ値を計算し、このハッシュ値を秘密鍵で暗号化してプログラム署名を作成し、このプログラム署名を内部管理情報一括暗号化データに付与して、内部管理情報一括パッケージデータを作成して、外部システム１１０に送出する。

【００４０】

リストア処理部１０７は、内部記憶媒体１０４に格納した管理情報を喪失した場合に、バックアップ処理部１０６により生成されたバックアップ情報に含まれる管理情報を内部記憶媒体１０４にリストアする処理部である。

【００４１】

具体的には、外部システム１１０から内部管理情報一括パッケージデータを受け取ったならば、この内部管理情報一括パッケージデータを内部管理情報一括暗号化データとプログラム署名とに分離し、内部管理情報一括暗号化データのハッシュ値を計算するとともに、プログラム署名を公開鍵で復号化する。

【００４２】

そして、両ハッシュ値が一致する場合には、内部管理情報一括暗号化データに含まれる暗号化乱数を秘密鍵で復号化して乱数を取得し、この乱数で内部管理情報一括暗号化データを復号化して内部管理情報一括データを取得し、この内部管理情報一括データを形成する各ファイルを内部記憶媒体１０４に格納する。

【００４３】

制御部１０８は、その実体はプロセッサであり、プログラム格納媒体１０３に格納された主制御プログラム、ハッシュプログラム、鍵生成プログラム、暗号化プログラム、復号化プログラムおよびバックアップ制御プログラムなどの各種プログラムを読み出して実行することになる。

【００４４】

具体的には、この制御部１０８では、外部システム１１０などから内部管理情報のバックアップ作成要求を受け付けた際に、バックアップの作成をバックアップ１０６に対して指示するとともに、外部システム１１０などからリストア要求を受け付けた際に、リストア処理部１０７に対してリストア指示をおこなう。

【００４５】

なお、本実施の形態では、説明の便宜上外部システム１１０などからの要求に応答してバックアップ並びにリストアをおこなうよう制御することとしたが、内部タイマ１０５の計時に基づいて定期的にバックアップ指示をおこなうとともに、内部記憶媒体１０４の異常を検知してリストア指示をおこなうよう構成することもできる。

【００４６】

上記構成を有する原本性保証電子保存装置１００を用いることにより、内部記憶媒体１０４に格納した管理情報を効率良くバックアップするとともに、状況に応じてバックアップ情報を内部記憶媒体１０４に迅速にリストアし、もって大容量記憶媒体１０１に格納した原本の電子データの原本性を継続的に保証することができる。

【００４７】

つぎに、図１に示した大容量記憶媒体１０１に保持したファイル並びに内部記憶媒体１０４に保持したファイルについて説明する。図２は、図１に示した大容量記憶媒体１０１上に保持した電子データ並びに内部記憶媒体１０４に保持した管理情報を説明するための説明図である。

【００４８】

同図に示すように、大容量記憶媒体１０１には、原本としての各電子データが保存データとして格納されるとともに、その保存データを管理するための保存データリストファイルと、媒体ごとに管理するための媒体管理情報ファイルが格納されている。

【００４９】

具体的には、この保存データリストファイルは、保存データごとに設けられた複数の保存データエントリからなり、各保存データエントリは、保存データ識別番号、保存データ名、作成情報、最終更新情報、廃棄情報および最新のバージョン番号などで形成される。また、媒体管理情報ファイルは、媒体識別番号、媒体名および媒体初期化日時情報などで形成される。

【００５０】

これに対して、内部記憶媒体１０４には、電子署名の計算などに使用する装置固有の装置暗号鍵（公開鍵暗号系の場合には秘密鍵）、電子署名の検証などに用いる装置固有の装置復号鍵（公開鍵暗号系の場合には公開鍵）、保存データ識別番号や媒体識別番号を生成する際に用いる装置識別番号、つぎの保存データに付与する保存データ識別番号、つぎにフォーマットする媒体に付与するつぎの媒体識別番号、大容量記憶媒体１０１の真正性を検証するための媒体認証コードリスト、内部タイマ設定履歴、外部システム１１０のアカウントを管理するアカウント管理リスト並びに装置アクセスログなどを格納する。

【００５１】

具体的には、図中に示した装置設定ファイルには、上記装置暗号鍵、装置復号鍵、装置識別情報、つぎの保存データ識別番号およびつぎの媒体識別番号などが記録され、また、媒体認証コードリストファイルには、媒体識別番号および媒体認証コードなどが記録される。さらに、内部タイマ設定履歴ファイルには内部タイマ設定履歴が記録され、装置アクセス履歴ファイルには装置アクセス履歴が記録され、アカウント管理リストファイルにはアカウント管理リストが記録されている。

【００５２】

つぎに、図１に示した外部システム１１０からの原本性保証電子保存装置１００へのログイン手順について説明する。図３は、図１に示した外部システム１１０からの原本性保証電子保存装置１００へのログイン手順を示すフローチャートである。

【００５３】

まず、内部管理情報のバックアップをおこなう際には、管理者などが外部システム１１０を用いて原本性保証電子保存装置１００に対してログインをしなければならない。なお、ここではパスワードによる一般的なチャレンジレスポンス認証処理をおこなうこととする。

【００５４】

同図に示すように、外部システム１１０が、原本性電子保存装置１００に対してアカウント名とログイン要求を送信すると（ステップＳ３０１）、原本性保証電子保存装置１００は、このアカウント名とログイン要求を受信し（ステップＳ３０２）、内部記憶媒体１０４からアカウント管理テーブルを取得し（ステップＳ３０３）、このアカウント管理テーブルから該当するアカウントエントリを取得する（ステップＳ３０４）。

【００５５】

そして、該当するエントリが存在するか否かを確認し（ステップＳ３０５）、該当するエントリが存在しない場合（ステップＳ３０５否定）は、エラーの終了コードを外部システム１１０のクライアントに送信し（ステップＳ３０６）、エラー処理をおこなって（ステップＳ３１８）、処理を終了する。

【００５６】

これに対して、該当するエントリが存在する場合（ステップＳ３０５肯定）は、乱数を生成し（ステップＳ３０７）、この乱数を外部システム１１０のクライアントに送信するとともに（ステップＳ３０８）、該乱数とアカウントエントリに格納されているユーザ側内部認証鍵を合わせたものに対してハッシュ値を計算する（ステップＳ３０９）。

【００５７】

また、外部システム１１０がこの乱数を受信したならば（ステップＳ３１０）、この乱数とパスワードを合わせたものに対してハッシュ値を計算し（ステップＳ３１１）、計算したハッシュ値を原本性保証電子保存装置１００に対して送信する（ステップＳ３１２）。

【００５８】

そして、原本性保証電子保存装置１００が、このハッシュ値を受信すると（ステップＳ３１３）、受信したハッシュ値が計算したハッシュ値と一致するか否かを確認し（ステップＳ３１４）、両者が一致しない場合（ステップＳ３１４否定）は、エラーの結果コードをクライアントに送信し（ステップＳ３１５）、エラー処理をおこなって（ステップＳ３１８）、処理を終了する。

【００５９】

一方、両者が一致する場合（ステップＳ３１４肯定）には、成功した結果コードを外部システム１１０のクライアントに送信し（ステップＳ３１６）、ログインしたアカウントのアカウントエントリを内部に保持する（ステップＳ３１７）。

【００６０】

なお、外部システム１１０が結果コードを受信したならば（ステップＳ３１９）、この結果コードがエラーコードであるか否かを確認し（ステップＳ３２０）、エラーコードである場合（ステップＳ３２０肯定）は、エラー処理をおこなう（ステップＳ３２１）。

【００６１】

上記一連の処理をおこなうことにより、外部システム１１０からクライアントがバックアップ要求をおこなうに際して、原本性保証電子保存装置１００に対して正常にログインすることができる。

【００６２】

つぎに、図１に示したバックアップ処理部１０６などによるバックアップ手順について説明する。図４は、図１に示したバックアップ処理部１０６などによるバックアップ手順を示すフローチャートである。

【００６３】

同図に示すように、原本性保証電子保存装置１００がバックアップ要求を受け付けたならば、内部に保持しているアカウントエントリのアカウント権限を参照し（ステップＳ４０１）、装置管理者のアカウント権限があるか否かを確認する（ステップＳ４０２）。そして、アカウント権限がない場合（ステップＳ４０２否定）は、エラー処理をおこなった後に（ステップＳ４１２）、処理を終了する。

【００６４】

これに対して、アカウント権限がある場合（ステップＳ４０２肯定）は、内部記憶媒体１０４から装置設定ファイル、媒体認証コードリストファイル、内部タイマ設定履歴ファイル、アカウント管理リストファイルを読み出し（ステップＳ４０３）、読み出したファイルを一括して内部管理情報一括データとする（ステップＳ４０４）。

【００６５】

なお、内部記憶媒体１０４に記憶する装置アクセス履歴ファイルについては、外部システム１１０から原本性保証電子保存装置１００へのアクセスが生ずるたびに頻繁に変更されるファイルであるため、ここではこの装置アクセス履歴ファイルのバックアップはおこなわないものとする。

【００６６】

その後、装置内部で乱数を生成し（ステップＳ４０５）、この乱数をプログラム内部のプログラム公開鍵で暗号化して暗号化乱数を作成し（ステップＳ４０６）、該乱数により

内部管理情報一括データを暗号化し、これに暗号化乱数を付与して内部管理情報一括暗号化データとする（ステップＳ４０７）。

【００６７】

その後、この内部管理情報一括暗号化データについてのハッシュ値を計算し（ステップＳ４０８）、このハッシュ値を秘密鍵で暗号化してプログラム署名を作成し（ステップＳ４０９）、このプログラム署名を内部管理情報一括暗号化データに付与して、内部管理情報一括パッケージデータを作成して（ステップＳ４１０）、外部システム１１０に送出する（ステップＳ４１１）。

【００６８】

つぎに、図１に示したリストア処理部１０７などによるリストア手順について説明する。図５は、図１に示したリストア処理部１０７などによるリストア手順を示すフローチャートである。なお、ここでは全く新しい原本性保証電子保存装置１００に内部管理情報をリストアする場合を示すこととする。

【００６９】

同図に示すように、原本性保証電子保存装置１００がリストア要求を受け付けたならば、内部に保持しているアカウントエントリのアカウント権限を参照し（ステップＳ５０１）、装置管理者のアカウント権限があるか否かを確認する（ステップＳ５０２）。そして、アカウント権限がない場合（ステップＳ５０２否定）は、エラー処理をおこなった後に（ステップＳ５１７）、すべての処理を終了する。

【００７０】

これに対して、アカウント権限がある場合（ステップＳ５０２肯定）は、完全に新しい原本性保証電子保存装置１００であるか否かについても確認し（ステップＳ５０３）、新しい原本性保証電子保存装置１００でない場合（ステップＳ５０３否定）は、エラー処理をおこなった後に（ステップＳ５１７）、すべての処理を終了する。

【００７１】

一方、新しい原本性保証電子保存装置１００である場合（ステップＳ５０３肯定）は、外部システム１１０から内部管理情報一括パッケージデータを受け取り（ステップＳ５０４）、この内部管理情報一括パッケージデータを内部管理情報一括暗号化データとプログラム署名とに分離し（ステップＳ５０５）、内部管理情報一括暗号化データのハッシュ値を計算するとともに（ステップＳ５０６）、プログラム署名をプログラム内部に保持しているプログラム公開鍵で復号化する（ステップＳ５０７）。

【００７２】

そして、復号化したものが先のハッシュ値と一致するか否かを確認し（ステップＳ５０８）、両ハッシュ値が一致しない場合（ステップＳ５０８否定）には、エラー処理をおこない（ステップＳ５１７）、その後、すべての処理を終了する。

【００７３】

これに対して、両ハッシュ値が一致する場合（ステップＳ５０８肯定）は、内部管理情報一括暗号化データから暗号化乱数を取得し（ステップＳ５０９）、この暗号化乱数をプログラム内部に保持しているプログラム秘密鍵で復号化して乱数を取得し（ステップＳ５１０）、この乱数で内部管理情報一括暗号化データを復号化して内部管理情報一括データを取得し（ステップＳ５１１）、この内部管理情報一括データを分解して、装置設定ファイル、媒体認証コードリストファイル、内部タイマ設定履歴ファイル、アカウント管理リストファイルとして内部記憶媒体１０４に記録する（ステップＳ５１２）。

【００７４】

そして、外部システム１１０から受け取った現在時刻で内部タイマ１０５を設定し（ステップＳ５１３）、設定前の日時情報を不明とし、設定後の日時情報を先に受け取った現在時刻に設定したタイマ設定エントリを作成する（ステップＳ５１４）。そして、内部設定履歴ファイルに新しいタイマ設定エントリを追加し（ステップＳ５１５）、装置アクセス履歴ファイルに、リストアしたことを示すログを記録して（ステップＳ５１６）、処理を終了する。

【００７５】
ところで、上記処理では、全く新しい原本性保証電子保存装置１００に内部管理情報をリストアすることとしたが、すでに使用している原本性保証電子保存装置１００に相乗りする形で内部管理情報をリストアする場合もある。
【００７６】
そこで、つぎに、使用している原本性保証電子保存装置１００に相乗りする形で内部管理情報をリストアする場合のリストア手順について説明する。図６は、図１に示したリストア処理部１０７などが、使用している原本性保証電子保存装置１００に相乗りする形で内部管理情報をリストアする場合のリストア手順を示すフローチャートである。
【００７７】
同図に示すように、この場合にも、原本性保証電子保存装置１００がリストア要求を受け付けたならば、内部に保持しているアカウントエントリのアカウント権限を参照し（ステップＳ６０１）、装置管理者のアカウント権限があるか否かを確認する（ステップＳ６０２）。そして、アカウント権限がない場合（ステップＳ６０２否定）は、エラー処理をおこなった後に（ステップＳ６１６）、処理を終了する。
【００７８】
これに対して、アカウント権限がある場合（ステップＳ６０２肯定）は、外部システム１１０から内部管理情報一括パッケージデータを受け取り（ステップＳ６０３）、この内部管理情報一括パッケージデータを内部管理情報一括暗号化データとプログラム署名とに分離し（ステップＳ６０４）、内部管理情報一括暗号化データのハッシュ値を計算するとともに（ステップＳ６０５）、プログラム署名をプログラム内部に保持しているプログラム公開鍵で復号化する（ステップＳ６０６）。
【００７９】
そして、復号化したものが先のハッシュ値と一致するか否かを確認し（ステップＳ６０７）、両ハッシュ値が一致しない場合（ステップＳ６０７否定）には、エラー処理をおこなった後に（ステップＳ６１６）、処理を終了する。
【００８０】
これに対して、両ハッシュ値が一致する場合（ステップＳ６０７肯定）は、内部管理情報一括暗号化データから暗号化乱数を取得し（ステップＳ６０８）、この暗号化乱数をプログラム内部に保持しているプログラム秘密鍵で復号化して乱数を取得し（ステップＳ６０９）、この乱数で内部管理情報一括暗号化データを復号化して内部管理情報一括データを取得し（ステップＳ６１０）、この内部管理情報一括データを分解して（ステップＳ６１１）、分解して得られた装置設定ファイルから装置識別番号を取得する（ステップＳ６１２）。
【００８１】
そして、装置識別番号を名前とするフォルダを内部記憶媒体１０４に作成し（ステップＳ６１３）、そのフォルダの下に、分解して得られた装置設定ファイル、媒体認証コードリストファイル、内部タイマ設定履歴ファイル、アカウント管理リストファイルとして内部記憶媒体１０４に記録するとともに（ステップＳ６１４）、装置アクセス履歴ファイルに、リストアしたことを示すログを記録して（ステップＳ６１５）、処理を終了する。
【００８２】
上述してきたように、本実施の形態にかかる原本性保証電子保存装置１００では、外部システム１１０からバックアップ要求を受け付けた際に、バックアップ処理手段１０６が、内部記憶媒体１０４に格納した管理情報についてのバックアップを作成し、また、外部システム１１０からリストア要求を受け付けた際に、リストア処理部１０７が、バックアップ処理部１０６によって生成されたバックアップ情報を内部記憶媒体１０４にリストアするよう構成したので、内部記憶媒体１０４に格納した管理情報を効率良くバックアップするとともに、状況に応じてバックアップ情報を内部記憶媒体１０４に迅速にリストアし、もって大容量記憶媒体１０１に格納した原本の電子データの原本性を継続的に保証することができる。

【００８３】
なお、本実施の形態で説明した障害復旧方法は、あらかじめ用意されたプログラムをパーソナルコンピュータやワークステーション等のコンピュータまたはマイコン内蔵のプリンタ、ディジタル複写機等で実行することにより実現される。このプログラムは、ＲＡＭ、ＲＯＭ、ハードディスク、フロッピーディスク、ＣＤ－ＲＯＭ、ＭＯ、ＤＶＤ等のコンピュータで読み取り可能な記録媒体に記録され、コンピュータによって記録媒体から読み出されることによって実行される。またこのプログラムは、上記記録媒体を介して、あるいは伝送媒体としてネットワークを介して配布することができる。
【００８４】
【発明の効果】
以上説明したように、この発明によれば、内部記憶媒体に格納した管理情報のバックアップ情報を生成しておき、この内部記憶媒体に格納した管理情報を喪失した場合に、生成されたバックアップ情報を内部記憶媒体にリストアすることとしたので、なんらかの障害が発生した場合であっても、内部記憶媒体に記憶した内部管理情報を迅速に復旧し、もって電子データの保存時の状態を迅速かつ効率良く保証することができるという効果を奏する。また、暗号化されたバックアップ情報を正しく復号化して内部記憶媒体にリストアすることができるという効果を奏する。
【００８５】
また、この発明によれば、外部システムからバックアップ要求を受け付けた場合に、内部記憶媒体に格納した管理情報を第１の暗号鍵で暗号化したバックアップ情報を作成し、作成したバックアップ情報を出力することとしたので、バックアップ情報の暗号強度を高めることができるという効果を奏する。
【００８６】
また、この発明によれば、装置本体に装着したＩＣカードの内部に保持した第１の暗号鍵および第１の復号鍵を用いてバックアップ情報の作成または復号をおこなうよう構成したので、ＩＣカードに応じて暗号鍵および復号鍵を自在に変更することができるという効果を奏する。
【００８７】
また、この発明によれば、外部システムからバックアップ要求を受け付けた場合に、内部記憶媒体に格納した管理情報を所定の乱数により暗号化し、暗号化に用いた乱数を第１の暗号鍵により暗号化し、暗号化した暗号化管理情報および暗号化乱数をバックアップ情報として出力するよう構成したので、単に管理情報を暗号化するだけでなく、この暗号化に用いた乱数についても暗号化して出力することができるという効果を奏する。
【００８８】
また、この発明によれば、バックアップ情報に含まれる暗号化乱数を第１の復号鍵で復号化し、復号化した乱数で暗号化管理情報を復号化し、この復号化された管理情報を内部記憶媒体に記録するよう構成したので、暗号化された管理情報を正しく復号化して内部記憶媒体にリストアすることができるという効果を奏する。
【００８９】
また、この発明によれば、暗号化された暗号化管理情報に暗号化乱数を付与して暗号化内部情報を作成し、作成した暗号化内部情報のハッシュ値を算定し、算定したハッシュ値を暗号化内部情報とともにバックアップ情報として出力するよう構成したので、暗号化内部情報の改ざんを効率良く防止することができるという効果を奏する。
【００９０】
また、この発明によれば、バックアップ情報に含まれる暗号化内部情報のハッシュ値を算定し、算定したハッシュ値とバックアップ情報に含まれるハッシュ値とを比較し、両ハッシュ値が一致すると判断された場合に、暗号化乱数を第１の暗号鍵に対応する第１の復号鍵で復号化し、復号化した乱数を用いて暗号化管理情報を復号化するよう構成したので、バックアップ情報が改ざんされているか否かを効率良く判断し、改ざんされていないことを条件として内部記憶媒体への管理情報の設定をおこなうことができるという効果を奏

する。

【００９１】

また、この発明によれば、算定されたハッシュ値を第２の暗号鍵を用いて暗号化した暗号化ハッシュ値を暗号化内部情報とともにバックアップ情報として出力し、この第２の暗号鍵に対応する第２の復号鍵を用いて暗号化ハッシュ値を復号化したハッシュ値と算定されたハッシュ値とを比較するよう構成したので、暗号化ハッシュ値を用いてバックアップ情報の改ざんを防止することができるという効果を奏する。

【００９２】

また、この発明によれば、第１の暗号鍵および第２の復号鍵を公開鍵暗号系の公開鍵とし、第２の暗号鍵および第１の復号鍵を公開鍵暗号系の秘密鍵とするよう構成したので、公開鍵暗号系を用いてバックアップ情報の暗号強度を高めることができるという効果を奏する。

【図面の簡単な説明】

【図１】　この実施の形態で用いる原本性保証電子保存装置の構成を示すブロック図である。

【図２】　図１に示した大容量記憶媒体に保持したファイル並びに内部記憶媒体に保持したファイルを説明するための説明図である。

【図３】　図１に示した外部システムからの原本性保証電子保存装置へのログイン手順を示すフローチャートである。

【図４】　図１に示したバックアップ処理部によるバックアップ手順を示すフローチャートである。

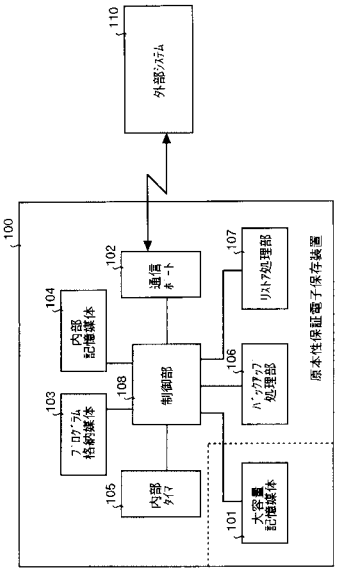
【図５】　図１に示したリストア処理部によるリストア手順を示すフローチャートである。

【図６】　図１に示したリストア処理部が、使用している原本性保証電子保存装置に相乗りする形で内部管理情報をリストアする場合のリストア手順を示すフローチャートである。

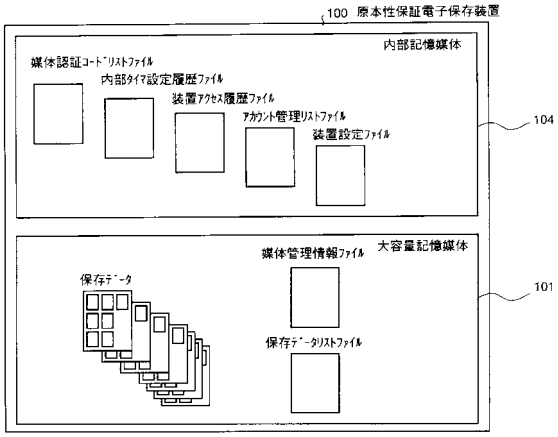
【符号の説明】

１００　原本性保証電子保存装置
１０１　大容量記憶媒体
１０２　通信ポート
１０３　プログラム格納媒体
１０４　内部記録媒体
１０５　内部タイマ
１０６　バックアップ処理部
１０７　リストア処理部
１０８　制御部
１１０　外部システム

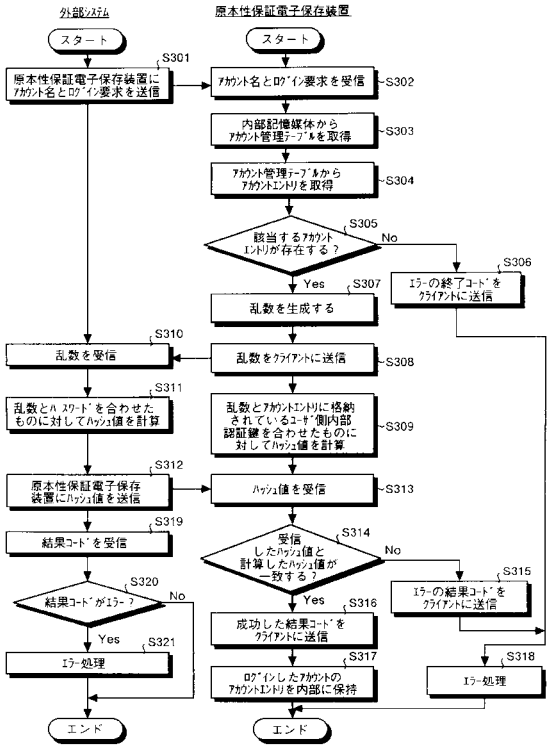
【図１】


110
外部ｼｽﾃﾑ
100
原本性保証電子保存装置
102
通信ﾈｯﾄ
107
ﾘｽﾄｱ処理部
104
内部記憶媒体
106
ﾊﾞｯｸｱｯﾌﾟ処理部
108
制御部
103
ﾌﾟﾛｸﾞﾗﾑ格納媒体
105
内部ﾀｲﾏ
101
大容量記憶媒体

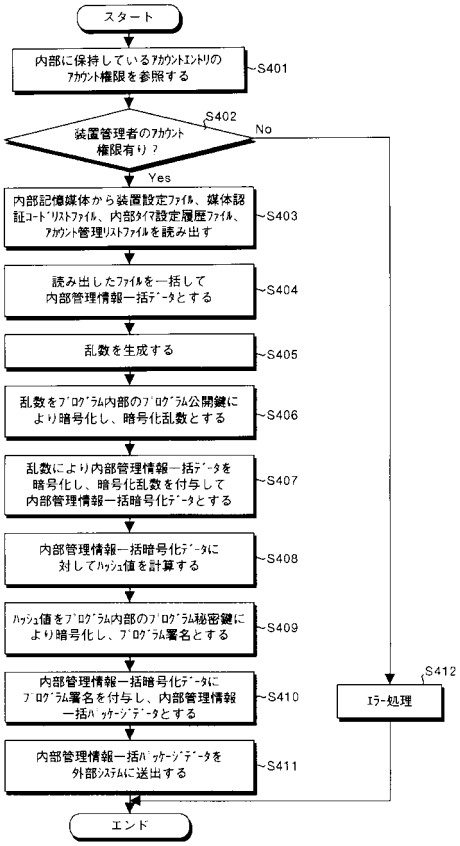
【図２】


100 原本性保証電子保存装置
内部記憶媒体
媒体認証ｺｰﾄﾞﾘｽﾄﾌｧｲﾙ
内部ﾀｲﾏ設定履歴ﾌｧｲﾙ
装置ｱｸｾｽ履歴ﾌｧｲﾙ
ｱｶｳﾝﾄ管理ﾘｽﾄﾌｧｲﾙ
装置設定ﾌｧｲﾙ
104
大容量記憶媒体
媒体管理情報ﾌｧｲﾙ
保存ﾃﾞｰﾀ
保存ﾃﾞｰﾀﾘｽﾄﾌｧｲﾙ
101

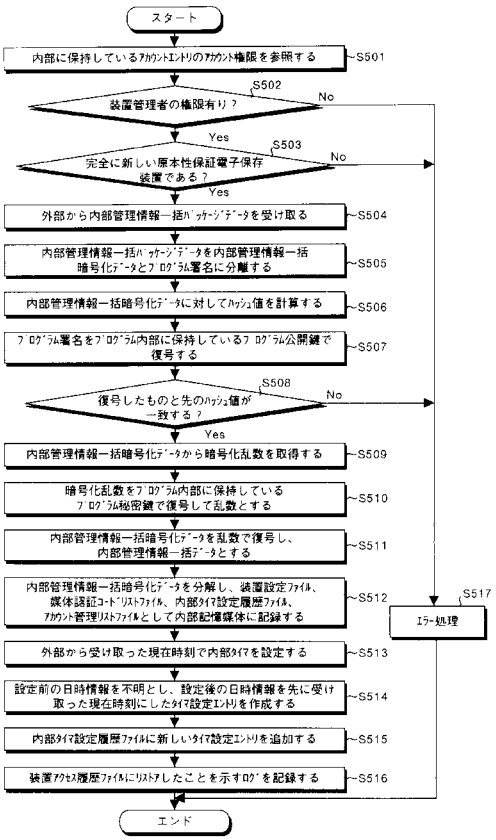
【図３】


外部ｼｽﾃﾑ
原本性保証電子保存装置
スタート
スタート
S301
原本性保証電子保存装置にｱｶｳﾝﾄ名とﾛｸﾞｲﾝ要求を送信
S302
ｱｶｳﾝﾄ名とﾛｸﾞｲﾝ要求を受信
S303
内部記憶媒体からｱｶｳﾝﾄ管理ﾃｰﾌﾞﾙを取得
S304
ｱｶｳﾝﾄ管理ﾃｰﾌﾞﾙからｱｶｳﾝﾄｴﾝﾄﾘを取得
S305
該当するｱｶｳﾝﾄｴﾝﾄﾘが存在する？
No
Yes
S306
ｴﾗｰの終了ｺｰﾄﾞをｸﾗｲｱﾝﾄに送信
S307
乱数を生成する
S308
乱数をｸﾗｲｱﾝﾄに送信
S309
乱数とｱｶｳﾝﾄｴﾝﾄﾘに格納されているﾕｰｻﾞ側内部認証鍵を合わせたものに対してﾊｯｼｭ値を計算
S310
乱数を受信
S311
乱数とﾊﾟｽﾜｰﾄﾞを合わせたものに対してﾊｯｼｭ値を計算
S312
原本性保証電子保存装置にﾊｯｼｭ値を送信
S313
ﾊｯｼｭ値を受信
S314
受信したﾊｯｼｭ値と計算したﾊｯｼｭ値が一致する？
No
Yes
S315
ｴﾗｰの結果ｺｰﾄﾞをｸﾗｲｱﾝﾄに送信
S316
成功した結果ｺｰﾄﾞをｸﾗｲｱﾝﾄに送信
S317
ﾛｸﾞｲﾝしたｱｶｳﾝﾄのｱｶｳﾝﾄｴﾝﾄﾘを内部に保持
S318
ｴﾗｰ処理
S319
結果ｺｰﾄﾞを受信
S320
結果ｺｰﾄﾞがｴﾗｰ？
No
Yes
S321
ｴﾗｰ処理
エンド
エンド

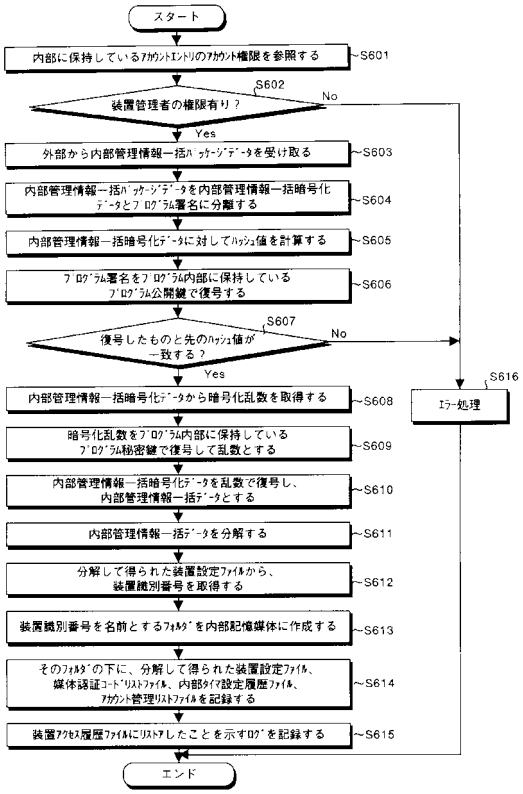
【図４】


スタート
内部に保持しているｱｶｳﾝﾄｴﾝﾄﾘのｱｶｳﾝﾄ権限を参照する
S401
装置管理者のｱｶｳﾝﾄ権限有り？
S402
No
Yes
内部記憶媒体から装置設定ﾌｧｲﾙ、媒体認証ｺｰﾄﾞﾘｽﾄﾌｧｲﾙ、内部ﾀｲﾏ設定履歴ﾌｧｲﾙ、ｱｶｳﾝﾄ管理ﾘｽﾄﾌｧｲﾙを読み出す
S403
読み出したﾌｧｲﾙを一括して内部管理情報一括ﾃﾞｰﾀとする
S404
乱数を生成する
S405
乱数をﾌﾟﾛｸﾞﾗﾑ内部のﾌﾟﾛｸﾞﾗﾑ公開鍵により暗号化し、暗号化乱数とする
S406
乱数により内部管理情報一括ﾃﾞｰﾀを暗号化し、暗号化乱数を付与して内部管理情報一括暗号化ﾃﾞｰﾀとする
S407
内部管理情報一括暗号化ﾃﾞｰﾀに対してﾊｯｼｭ値を計算する
S408
ﾊｯｼｭ値をﾌﾟﾛｸﾞﾗﾑ内部のﾌﾟﾛｸﾞﾗﾑ秘密鍵により暗号化し、ﾌﾟﾛｸﾞﾗﾑ署名とする
S409
内部管理情報一括暗号化ﾃﾞｰﾀにﾌﾟﾛｸﾞﾗﾑ署名を付与し、内部管理情報一括ﾊﾟｯｹｰｼﾞﾃﾞｰﾀとする
S410
内部管理情報一括ﾊﾟｯｹｰｼﾞﾃﾞｰﾀを外部ｼｽﾃﾑに送出する
S411
ｴﾗｰ処理
S412
エンド

【図５】


スタート
内部に保持しているｱｶｳﾝﾄｴﾝﾄﾘのｱｶｳﾝﾄ権限を参照する
S501
装置管理者の権限有り？
S502
No
Yes
完全に新しい原本性保証電子保存装置である？
S503
No
Yes
外部から内部管理情報一括ﾊﾟｯｹｰｼﾞﾃﾞｰﾀを受け取る
S504
内部管理情報一括ﾊﾟｯｹｰｼﾞﾃﾞｰﾀを内部管理情報一括暗号化ﾃﾞｰﾀとﾌﾟﾛｸﾞﾗﾑ署名に分離する
S505
内部管理情報一括暗号化ﾃﾞｰﾀに対してﾊｯｼｭ値を計算する
S506
ﾌﾟﾛｸﾞﾗﾑ署名をﾌﾟﾛｸﾞﾗﾑ内部に保持しているﾌﾟﾛｸﾞﾗﾑ公開鍵で復号する
S507
復号したものと先のﾊｯｼｭ値が一致する？
S508
No
Yes
内部管理情報一括暗号化ﾃﾞｰﾀから暗号化乱数を取得する
S509
暗号化乱数をﾌﾟﾛｸﾞﾗﾑ内部に保持しているﾌﾟﾛｸﾞﾗﾑ秘密鍵で復号して乱数とする
S510
内部管理情報一括暗号化ﾃﾞｰﾀを乱数で復号し、内部管理情報一括ﾃﾞｰﾀとする
S511
内部管理情報一括暗号化ﾃﾞｰﾀを分解し、装置設定ﾌｧｲﾙ、媒体認証ｺｰﾄﾞﾘｽﾄﾌｧｲﾙ、内部ﾀｲﾏ設定履歴ﾌｧｲﾙ、ｱｶｳﾝﾄ管理ﾘｽﾄﾌｧｲﾙとして内部記憶媒体に記録する
S512
外部から受け取った現在時刻で内部ﾀｲﾏを設定する
S513
設定前の日時情報を不明とし、設定後の日時情報を先に受け取った現在時刻にしたﾀｲﾏ設定ｴﾝﾄﾘを作成する
S514
内部ﾀｲﾏ設定履歴ﾌｧｲﾙに新しいﾀｲﾏ設定ｴﾝﾄﾘを追加する
S515
装置ｱｸｾｽ履歴ﾌｧｲﾙにﾘｽﾄｱしたことを示すﾛｸﾞを記録する
S516
ｴﾗｰ処理
S517
エンド

【図６】


スタート
内部に保持しているｱｶｳﾝﾄｴﾝﾄﾘのｱｶｳﾝﾄ権限を参照する
S601
装置管理者の権限有り？
S602
No
Yes
外部から内部管理情報一括ﾊﾟｯｹｰｼﾞﾃﾞｰﾀを受け取る
S603
内部管理情報一括ﾊﾟｯｹｰｼﾞﾃﾞｰﾀを内部管理情報一括暗号化ﾃﾞｰﾀとﾌﾟﾛｸﾞﾗﾑ署名に分離する
S604
内部管理情報一括暗号化ﾃﾞｰﾀに対してﾊｯｼｭ値を計算する
S605
ﾌﾟﾛｸﾞﾗﾑ署名をﾌﾟﾛｸﾞﾗﾑ内部に保持しているﾌﾟﾛｸﾞﾗﾑ公開鍵で復号する
S606
復号したものと先のﾊｯｼｭ値が一致する？
S607
No
Yes
内部管理情報一括暗号化ﾃﾞｰﾀから暗号化乱数を取得する
S608
暗号化乱数をﾌﾟﾛｸﾞﾗﾑ内部に保持しているﾌﾟﾛｸﾞﾗﾑ秘密鍵で復号して乱数とする
S609
内部管理情報一括暗号化ﾃﾞｰﾀを乱数で復号し、内部管理情報一括ﾃﾞｰﾀとする
S610
内部管理情報一括ﾃﾞｰﾀを分解する
S611
分解して得られた装置設定ﾌｧｲﾙから、装置識別番号を取得する
S612
装置識別番号を名前とするﾌｫﾙﾀﾞを内部記憶媒体に作成する
S613
そのﾌｫﾙﾀﾞの下に、分解して得られた装置設定ﾌｧｲﾙ、媒体認証ｺｰﾄﾞﾘｽﾄﾌｧｲﾙ、内部ﾀｲﾏ設定履歴ﾌｧｲﾙ、ｱｶｳﾝﾄ管理ﾘｽﾄﾌｧｲﾙを記録する
S614
装置ｱｸｾｽ履歴ﾌｧｲﾙにﾘｽﾄｱしたことを示すﾛｸﾞを記録する
S615
ｴﾗｰ処理
S616
エンド

フロントページの続き

(56)参考文献 特開平０５－００２５１８（ＪＰ，Ａ）
特開平１１－１４３３６１（ＪＰ，Ａ）
特開平１０－１３３９２５（ＪＰ，Ａ）
特開平０７－１３１４５２（ＪＰ，Ａ）
特開平０９－１６７２２０（ＪＰ，Ａ）
五十嵐 幸雄，富士通研，戸籍抄本を電子化するシステム試作，日経エレクトロニクス 第７１２号 NIKKEI ELECTRONICS，日本，日経ＢＰ社 Nikkei Business Publications，Inc.，１９９８年 3月２３日，p.31，p.32
金井洋一，原本性保証電子保存システムについて，行政＆ＡＤＰ，社団法人行政情報システム研究所，１９９８年，１９９８年８月号，p.10-p.17

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F 21/24