(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4256100号
(P4256100)
(45)発行日　平成21年4月22日(2009.4.22)　(24)登録日　平成21年2月6日(2009.2.6)

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

請求項の数 8　(全 19 頁)

(21)出願番号　特願2002-24585(P2002-24585)
(22)出願日　平成14年1月31日(2002.1.31)
(65)公開番号　特開2003-223366(P2003-223366A)
(43)公開日　平成15年8月8日(2003.8.8)
審査請求日　平成16年8月25日(2004.8.25)

(73)特許権者　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(74)代理人　100074099
弁理士　大菅　義之
(74)代理人　100067987
弁理士　久木元　彰
(72)発明者　秋山　良太
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

審査官　平井　誠

最終頁に続く

(54)【発明の名称】正当媒体管理システム

(57)【特許請求の範囲】
【請求項１】
原本保存手段のＩＤ番号に対応する鍵を記憶する記憶手段と、
記録媒体の発行要求元の原本保存手段から送信される前記ＩＤ番号を使用して前記記憶手段から前記鍵を取得し、該鍵を使用して記録媒体の改竄不可能領域に前記記録媒体固有の媒体番号とともに、原本格納用であることを示す原本媒体証明書を暗号化して書き込み、該記録媒体を記録媒体の発行要求元の前記原本保存手段に発行する媒体発行手段と、を有し、
前記原本保存手段は、前記記録媒体の前記改竄不可能領域から暗号化された情報を読み出し、自己が所有する前記鍵と同じ鍵を使用して復号し、該復号結果の媒体番号が前記記録媒体の媒体番号と一致することを確認するとともに、前記記録媒体が前記媒体発行手段に発行を要求した原本媒体であることを確認した後に、前記記録媒体に原本文書を記録することを特徴とする記録媒体管理システム。
【請求項２】
文書の謄本又は副本を保存する謄本・副本保存手段と、
記録媒体の発行要求元の謄本・副本保存手段のＩＤ番号に対応する鍵を記憶する記憶手段と、
記録媒体の発行要求元の前記謄本・副本保存手段から送信される前記ＩＤ番号を使用して前記記憶手段から前記鍵を取得し、該鍵を使用して記録媒体の改竄不可能領域に前記記録媒体固有の媒体番号を暗号化して書き込むとともに、謄本・副本格納用であることを示

す謄本・副本媒体証明書を暗号化して書き込み、該記録媒体を記録媒体の発行要求元の前記謄本・副本保存手段に発行する媒体発行手段と、を有し、
前記謄本・副本保存手段は、前記記録媒体の前記改竄不可能領域から暗号化された情報を読み出し、自己が所有する前記鍵と同じ鍵を使用して復号し、該復号結果の媒体番号が前記記録媒体の媒体番号と一致することを確認するとともに、前記記録媒体が前記媒体発行手段に発行を要求した謄本・副本媒体であることを確認した後に、該記録媒体に謄本又は副本文書を記録することを特徴とする記録媒体管理システム。
【請求項３】
記録媒体の発行要求元の原本保存手段のＩＤ番号に基づいて該原本保存手段の鍵を記憶装置から読み出す読出手段と、
前記鍵を使用して記録媒体の改竄不可能領域に前記記録媒体固有の媒体番号とともに、原本格納用であることを示す原本媒体証明書を暗号化して書き込み、該記録媒体を記録媒体の発行要求元の前記原本保存手段に発行する媒体発行手段と、を有し、
記録媒体の発行要求元の前記原本保存手段に対して前記記録媒体が前記媒体発行手段に発行要求した原本媒体であることの確認を可能にしたことを特徴とする記録媒体発行装置。
【請求項４】
記録媒体の発行要求元の謄本・副本保存手段のＩＤ番号に基づいて前記謄本・副本保存手段の鍵を記憶装置から読み出す読出手段と、
該鍵を使用して記録媒体の改竄不可能領域に前記記録媒体固有の媒体番号とともに、謄本・副本格納用であることを示す謄本・副本媒体証明書を暗号化して書き込み、該記録媒体を記録媒体の発行要求元の前記謄本・副本保存手段に発行する媒体発行手段と、を有し、
前記謄本・副本保存手段に対して前記記録媒体が前記媒体発行手段に発行要求した謄本・副本媒体であることの確認を可能にしたことを特徴とする記録媒体発行装置。
【請求項５】
前記媒体発行手段は、固有の媒体番号が付され、改竄不可能な領域を有する記録媒体の供給を工場から受けることを特徴とする請求項１、又は２記載の媒体管理システム。
【請求項６】
前記改竄不可能領域には、前記媒体発行手段が前記記録媒体を発行したことを示す証明も含まれることを特徴とする請求項１、又は２記載の媒体管理システム。
【請求項７】
原本文書を記録する原本保存手段に記録媒体を供給する媒体発行手段は、
記録媒体の発行要求元の原本保存手段のＩＤ番号に基づいて、該原本保存手段の鍵を記憶手段から読み出す処理と、
該鍵を使用して記録媒体の改竄不可能領域に前記記録媒体固有の媒体番号とともに、原本格納用であることを示す原本媒体証明書を暗号化して書き込み、該記録媒体を記録媒体の発行要求元の前記原本保存手段に発行する処理とを行い、
前記原本保存手段は、
前記記録媒体の前記改竄不可能領域から暗号化された情報を読み出し、自己が所有する前記鍵と同じ鍵を使用して前記媒体番号を復号し、該復号結果の媒体番号が前記記録媒体の媒体番号と一致することを確認するとともに、前記記録媒体が前記媒体発行手段に発行要求した原本媒体であることを確認した後に、前記記録媒体に原本文書を記録する処理を行う、
ことを特徴とする記録媒体管理方法。
【請求項８】
謄本文書又は副本文書を記録する謄本・副本保存手段に記録媒体を供給する媒体発行手段は、
記録媒体の発行要求元の謄本・副本保存手段のＩＤ番号に基づいて前記謄本・副本保存手段の鍵を記憶手段から読み出す処理と、

該鍵を使用して記録媒体の改竄不可能領域に前記記録媒体固有の媒体番号とともに、謄本・副本格納用であることを示す謄本・副本媒体証明書を暗号化して書き込み、該記録媒体を記録媒体の発行要求元の前記謄本・副本保存手段に発行する処理とを行い、

謄本・副本保存手段は、

前記記録媒体の前記改竄不可能領域から暗号化された情報を読み出し、自己が所有する前記鍵と同じ鍵を使用して復号し、該復号結果の媒体番号が前記記録媒体の媒体番号に一致することを確認するとともに、前記記録媒体が前記媒体発行手段に発行要求した謄本・副本媒体であることを確認した後に、該記録媒体に謄本又は副本文書を記録する処理を行う、

ことを特徴とする記録媒体管理方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は文書の原本や、謄本又は副本を記録した光磁気ディスク等の記録媒体の正当性を管理する正当媒体管理システムに関する。

【０００２】

【従来の技術】

今日多くの文書が作成され、光磁気ディスク等の記録媒体に記録されている。また、記録媒体に記録される書類もあらゆる分野に及んでおり、例えば会社の設計部門や営業部門で作成する開発計画書や企画書、市役所や区役所等が作成する戸籍や住民に関する書類、更には会社間や組織間で遣り取りする書類など、様々な書類が存在する。

【０００３】

また、このような書類のセキュリティーは重要であり、例えば書類の内容が改竄されないよう保存し、また原本は原本として、謄本は謄本として確実に保存する必要がある。特に、原本性、謄本性等を確実に確保するためには、原本又は謄本等に対して、それらの書類が原本である、又は謄本であると定める権限者が必要である。

【０００４】

そして、権限者であるためには、当該権限者しか持ち得ない資格印、例えば電子鍵が必要である。すなわち、対象となる文書を原本であると認定し、対象となる文書を謄本であると認定し、当該認定者の署名鍵で電子署名されることが必要である。また、第三者による複製や改竄を防止するため、重要な文書は複製が不可能な媒体領域に記録することも要求される。

【０００５】

【発明が解決しようとする課題】

しかしながら、従来の場合、例えば原本作成者が無意識のうちに複数の記録媒体に原本を書き込んだ場合、唯一であるはずの原本が複数作成されることになる。また、誤って原本用の記録媒体に副本文書が記録され、又は副本用の記録媒体に原本文書が記録された場合、混乱を招き、原本文書に対して統一した変更処理や追加処理を行うこともできない。

【０００６】

一方、最近記録媒体に対して固有番号を付加して管理する方式が提案されている。その理由は、今日のマルチメディア化に伴って記録媒体個々に固有番号を付加し、記録媒体に関する著作権を確実に保護しようとするものである。そして、このような情報は一般ユーザが書き込み困難な領域に記録され、改竄不可能な情報となる。

【０００７】

そこで、本発明は記録媒体の改竄不可能領域に正当媒体である旨の署名を行い、更に記録媒体に対して媒体発行機関の認証を行い、記録媒体の原本性、唯一性を確実に確保する正当媒体管理システムを提供するものである。

【０００８】

【課題を解決するための手段】

上記課題は請求項１記載の発明によれば、原本保存手段のＩＤ番号に対応する鍵を記憶

する記憶手段と、記録媒体の発行要求元の原本保存手段から送信される前記ＩＤ番号を使用して前記記憶手段から前記鍵を取得し、該鍵を使用して記録媒体の改竄不可能領域に前記記録媒体固有の媒体番号とともに、原本格納用であることを示す原本媒体証明書を暗号化して書き込み、該記録媒体を記録媒体の発行要求元の前記原本保存手段に発行する媒体発行手段とを有し、前記原本保存手段は、前記記録媒体の前記改竄不可能領域から暗号化された情報を読み出し、自己が所有する前記鍵と同じ鍵を使用して復号し、該復号結果の媒体番号が前記記録媒体の媒体番号と一致することを確認するとともに、前記記録媒体が前記媒体発行手段に発行を要求した原本媒体であることを確認した後に、前記記録媒体に原本文書を記録する記録媒体管理システムを提供することによって達成できる。

【０００９】

ここで、記録媒体とは例えば光磁気ディスクのように特定の記録エリアに一般ユーザがアクセス不可能な領域を有する媒体であり、例えば上記領域に記録媒体固有の媒体番号を記録し、また正当媒体であることの証明を記録し、上記原本保存手段の鍵を使用して署名を行う。また、この署名には正当媒体発行機関が正当に発行した旨の認証も含める。

【００１０】

このように構成することにより、上記署名が行われた記録媒体が送られた原本保存手段では自己が保有する上記鍵と同じ鍵を使用して上記署名を復号し、例えば記録された記録媒体の固有の媒体番号を確認し、原本用の記録媒体であることを確認した場合のみ原本文書を記録することによって、確実に唯一存在する原本記憶媒体に原本文書を保存する。

【００１１】

上記構成は文書の原本に限らず、請求項２に記載するように、例えば文書の謄本や副本を記録する場合でも同様であり、正当媒体発行機関によって署名が行われた記録媒体に、対応する謄本・副本保存手段が自己の保有する上記鍵と同じ鍵を使用して上記署名を復号し、謄本又は副本文書を当該記録媒体に記録することで、確実に謄本又は副本用の記録媒体に謄本又は副本書類を保存することができる。

【００１２】

また、上記原本、又は謄本や副本を記録する記録媒体には、時刻情報を付加した履歴情報も含めて署名を行い、記録する。このように構成することにより、唯一存在する原本媒体としての機能を向上させ、謄本又は副本媒体としての機能を向上させることができる。

【００１３】

さらに、上記課題は請求項３記載の発明によれば、記録媒体の発行要求元の原本保存手段のＩＤ番号に基づいて該原本保存手段の鍵を記憶装置から読み出す読出手段と、前記鍵を使用して記録媒体の改竄不可能領域に前記記録媒体固有の媒体番号とともに、原本格納用であることを示す原本媒体証明書を暗号化して書き込み、該記録媒体を記録媒体の発行要求元の前記原本保存手段に発行する媒体発行手段とを有し、記録媒体の発行要求元の前記原本保存手段に対して前記記録媒体が前記媒体発行手段に発行要求した原本媒体であることの確認を可能にした記録媒体発行装置を提供することによって達成できる。

【００１４】

この場合、正当媒体発行装置は署名が行われた記録媒体を原本保存装置に送付してもよく、又電子的手法によって原本保存装置に送ってもよく、上記記録媒体が供給された原本保存装置では原本文書を記録する。

【００１５】

また、上記構成は文書の原本に限らず、請求項４に記載するように、例えば文書の謄本や副本を記録する場合でも同様であり、上記記録媒体の供給を受けた謄本・副本保存装置では謄本又は副本に関する情報を記録する。

【００１６】

【発明の実施の形態】

以下、本発明の実施形態を図面を用いて詳細に説明する。

＜第１の実施形態＞

図１は本実施形態の正当媒体管理システムのシステム構成図である。

【００１７】
同図において、原本保存機関１は、文書の原本を保存する機関であり、例えば区役所や市役所、又は会社の営業部や開発部などが対応し、戸籍や住民票の原本を保持し、又は開発計画書や企画書などの原本を保持する。
【００１８】
正当媒体発行機関２は記録媒体が原本であることを証明する機関であり、ＬＡＮやインターネット等のネットワークを介して上記原本保存機関１に接続されている。また、正当媒体発行機関２は鍵管理簿３ａを構築する記憶装置３に接続され、鍵管理簿３ａからＩＤ番号に対応する鍵を読み出す。また、正当媒体発行機関２は工場４とネットワークを介して接続され、記録媒体固有の媒体番号が付与された記録媒体の出荷を受ける。
【００１９】
正当媒体発行機関２は鍵管理簿３ａから取得した鍵を使用して記録媒体の発行処理を行い、工場４から出荷された記録媒体に正当媒体の署名を行い、原本保存機関１に運搬する。原本保存機関１は運搬された記録媒体に対し、復号処理を行い、書類の原本を記録する。尚、この復号及び記録処理については後述する。
【００２０】
謄本・副本保存機関５は、書類の謄本又は副本を保存する機関であり、正当媒体発行機関２とネットワークを介して接続されている。例えば、役所の出張所や支所、会社の営業所や支店などが対応する。この謄本・副本保存機関５も上記正当媒体発行機関２によって証明された記録媒体に文書の謄本又は副本を保存する。
【００２１】
以下、具体的な処理方法についてフローチャートを用いて説明する。
図２は本例の処理を説明するフローチャートである。先ず、原本保存機関１は、正当媒体発行機関２に対して文書の原本を保存するための記録媒体の発行を要求する（ステップ（以下、Ｓで示す）１）。この時、同時に原本保存機関１は原本保存機関１を証明するＩＤコード（ＩＤａ）も正当媒体発行機関２に送る。
【００２２】
正当媒体発行機関２は記録媒体の発行要求を受信すると、同時に受信するＩＤコード（ＩＤａ）に従って鍵管理簿３ａをアクセスし、鍵管理簿３ａから対応する鍵Ｋａを読み出す（Ｓ２）。鍵管理簿３ａには、図１に示すようにＩＤコードに対応した鍵が予め登録され、鍵管理簿３ａはＩＤコード（ＩＤａ）に基づいて検索を行い、鍵Ｋａを読み出し、正当媒体発行機関２に渡す。
【００２３】
正当媒体発行機関２は鍵管理簿３ａから取り出した鍵Ｋａを使用し、正当媒体発行機関２の証明書付きの記録媒体を作成する。この為、先ず工場４からＩＤ書き込み済みの記録媒体の出荷を受ける。ここで、工場４から出荷される記録媒体は、例えば光磁気ディスク（ＭＯディスク・magneto-optical disk）であり、記録媒体には個々の媒体番号が記録されている。本例の場合、この媒体番号として、「ＭＩＤ－Ａ」が記録されている。
【００２４】
次に、正当媒体発行機関２は工場４から出荷された記録媒体「ＭＩＤ－Ａ」を使用し、正当媒体証明書付きの記録媒体を作成する。図３はこの処理を説明する模式図である。
【００２５】
先ず、正当媒体発行機関２は工場４から出荷された記録媒体に対してパスワード（ＰＷＭ）を使用して媒体のＳＡ領域（secure area）にアクセスし、媒体番号の情報を読み出す（Ｓ３、図３に示す▲１▼及び▲２▼）。ここで、上記媒体の媒体番号は「ＭＩＤ－Ａ」であり、上記処理によって「ＭＩＤ－Ａ」の媒体番号が読み出される。尚、このＳＡ領域へのアクセスは、上記パスワード（ＰＷＭ）を使用しなければ不可能であり、ＳＡ領域は所謂改竄不可能な領域である。
【００２６】
次に、媒体番号「ＭＩＤ－Ａ」の情報と共に、「原本媒体証明書」、及び「発行機関証明

書」を正当媒体発行機関２の鍵Ｋｃによって暗号化した「ＥＫｃ（発行機関証明書）」を原本保存機関１の鍵Ｋａを使用して暗号化する（Ｓ４、図３に示す▲３▼）。ここで、「原本媒体証明書」は本媒体が原本文書の格納用であることを証明するものであり、例えば“本媒体は原本格納用である、番号は「ＭＩＤ－Ａ」”の記述文とする。

【００２７】

また、上記暗号化処理は、例えば図４に示すようにデータ（ＤＡＴＡ）を演算器を通して暗号処理部に送り、ＤＥＳ（data encryption standard）のアルゴリズムに従って鍵Ｋａでデータ（ＤＡＴＡ）を暗号化し、暗号文ＥＫａ（ＤＡＴＡ）を得る。尚、本例では上記データ（ＤＡＴＡ）は、媒体番号「ＭＩＤ－Ａ」、「原本媒体証明書」、「ＥＫｃ（発行機関証明書）」であり、暗号出力ＥＫａ（ＤＡＴＡ）は以下のようになる。

【００２８】

ＥＫａ（ＤＡＴＡ）＝ＥＫａ（「ＭＩＤ－Ａ」、「原本媒体証明書」、「ＥＫｃ（発行機関証明書））」

また、上記「ＥＫｃ（発行機関証明書）」は「発行機関証明書」を正当媒体発行機関２の鍵Ｋｃで暗号化したものであり、この暗号化の手法も上記と同様である。

【００２９】

次に、上記のようにして暗号化したＥＫａ（ＤＡＴＡ）を前述の原本媒体に書き込む（Ｓ５、図３に示す▲４▼）。この処理によって、原本媒体（ＭＯ）６のＳＡ領域７には暗号化したＥＫａ（ＤＡＴＡ）が書き込まれる。尚、この暗号化したＥＫａ（ＤＡＴＡ）を原本証明書シールとも言う。

【００３０】

正当媒体発行機関２は上記ＳＡ領域７に暗号文「ＥＫａ（ＤＡＴＡ）」が書き込まれた原本媒体（ＭＯ）６を原本保存機関１に運搬する（Ｓ６、図３に示す▲５▼）。このようにして正当媒体発行機関２から送られた原本媒体（ＭＯ）６には原本保存機関１によって文書の原本が記録される。

【００３１】

次に、原本保存機関１が行う原本媒体（ＭＯ）６への原本文書の書き込み処理について説明する。図５はこの処理を説明するフローチャートであり、図６は原本書き込み処理を模式的に示す図である。

【００３２】

先ず、原本保存機関１はホストコンピュータ１０のドライバに原本媒体（ＭＯ）６を挿入し、原本媒体（ＭＯ）６のＳＡ領域７をアクセスし、原本保存機関１の鍵Ｋａを使用して前述の原本証明書シールを復号する（Ｓ７、図６に示す▲１▼）。尚、図７はこの復号処理を模式的に示す図である。復号処理は上記暗号化処理の逆であり、ＳＡ領域７からＥＫａ（ＤＡＴＡ）を読み出し、ＤＥＳのアルゴリズムに従って復号する。

【００３３】

次に、上記復号化の結果得られるデータ、即ち鍵Ｋａで暗号化された情報、「ＭＩＤ－Ａ」、「原本媒体証明書」、「ＥＫｃ（発行機関証明書）」と、平文を比較し、一致を判断する（Ｓ８、図６に示す▲２▼）。具体的には、例えば平文「ＭＩＤ－Ａ」と、上記復号処理の結果得られる「ＭＩＤ－Ａ」とを比較する。

【００３４】

ここで、両データが一致すれば、原本のアクセス条件を示すと共に、原本に対するライトアクセスを許可する（Ｓ９、図６に示す▲３▼）。また、「原本媒体証明書」の記述内容、即ち前述の“本媒体は原本格納用である、番号は「ＭＩＤ－Ａ」”の記述文をホストコンピュータ１０のディスプレイに表示する。

【００３５】

また、原本のアクセス条件とは、データの編集は許可するが、データを削除することは禁止する等の条件である。この原本のアクセス条件もホストコンピュータ１０のディスプレイに表示される。

【００３６】

尚、上記判断がＮＯである場合、ディスプレイにエラー表示を行い、原本媒体（ＭＯ）６へのライト許可を与えない。このように構成することにより、原本保存機関１は必ず正当媒体発行機関２によって正当媒体であることが認証された原本媒体（ＭＯ）６に原本書類を書き込むことになる。

【００３７】

次に、原本媒体（ＭＯ）６であることが確認された場合、ライト許可が付与され、原本保存機関１はメッセージｍの書き込みを行う（Ｓ１０、図６に示す▲４▼）。ここで、メッセージｍは、原本媒体（ＭＯ）６に記録する原本文書である。

【００３８】

次に、時刻生成装置から時刻データ（ｔｏｒ）を読み出し、原本媒体（ＭＯ）６に書き込み、所謂タイムスタンプを生成する（Ｓ１１、図６に示す▲５▼）。尚、このタイムスタンプは原本書類の書き込み時刻を記録する処理である。

【００３９】

次に、履歴管理プログラムを駆動し、履歴情報Ｈを書き込む（Ｓ１２、図６に示す▲６▼）。例えば、上記履歴情報Ｈの内容として、例えば“時刻（ｔｏｒ）に原本保存機関１によって書類番号○○の文書ｍが保管された”等の記述が行われる。

【００４０】

次に、上記一連の書込み情報、「ＭＩＤ－Ａ」、「メッセージｍ」、「時刻データ（ｔｏｒ）」、「履歴情報Ｈ」を基に署名を行い（Ｓ１３）、認証子（ＣＳor）を生成する（Ｓ１３、図６に示す▲７▼）。この場合、原本保存機関１が有する他の鍵Korsを使用して行う。

【００４１】

最後に、ハードディスク上の一連の情報組、「ＭＩＤ－Ａ」、「メッセージｍ」、「時刻データ（ｔｏｒ）」、「履歴情報Ｈ」、「認証子（ＣＳor）」を原本媒体（ＭＯ）６に保管する（Ｓ１４、図６に示す▲８▼）。この処理によって、原本媒体（ＭＯ）６には原本書類が保管される。

【００４２】

以上のように、原本保存機関１は原本媒体を作成する際、必ず記録媒体をドライバにセットして復号処理を行うので、前述の原本証明書シールが確認され、例えば原本証明書シールが無い場合や、異なる媒体番号の場合にはエラー表示が行われる。したがって、誤って原本媒体（ＭＯ）６と異なる記録媒体に原本文書を記録することがない。

【００４３】

また、ディスプレイには「原本媒体証明書」が前述の記述文として表示され、セットされた記録媒体が原本記録用の媒体（原本媒体（ＭＯ）６）であることが確認できる。

【００４４】

また、正当媒体証明書の発行機関である正当媒体発行機関２の「発行機関証明書」も添付されており、必要に応じて復号することによって、認証機関の証明も可能である。

【００４５】

さらに、本例の正当媒体の認証は記録媒体のＳＡ領域７に記録され、第三者による改竄不可能な領域に電子署名が行われ、更に原本媒体（ＭＯ）６の正当性が確実に確保される。

＜第２の実施形態＞

次に、本発明の第２の実施形態について説明する。

【００４６】

本実施形態は、謄本又は副本書類に対する正当媒体管理システムについて説明するものである。また、この処理は前述の正当媒体発行機関２と謄本・副本保存機関５で行われる処理であり、図８は本例の処理を説明するフローチャートであり、本例の説明においても前述の図１のシステム図も使用する。

【００４７】

先ず、謄本・副本保存機関５は謄本又は副本を記録するための記録媒体の発行を正当媒体発行機関２に要求する（ステップ（以下、ＳＴで示す）１）。この時、同時に謄本・副本

保存機関５を証明するＩＤコード（ＩＤｂ）も送付する。

【００４８】

正当媒体発行機関２は記録媒体の発行要求を受信すると、上記ＩＤコード（ＩＤｂ）を使用して鍵管理簿３ａにアクセスし、鍵管理簿３ａから対応する鍵Ｋｂを取り出す（ＳＴ２）。

【００４９】

次に、正当媒体発行機関２は取り出した鍵Ｋｂを使用して、正当媒体発行機関２の証明書付きの記録媒体を作成する。この処理は、前述と同様、工場４から出荷されたＩＤ書き込み済みの記録媒体に対し、パスワード（ＰＷＭ）を使用してＳＡ領域にアクセスし、記録媒体の媒体番号（例えば、「ＭＩＤ－Ｂ」）の情報を読み出す（ＳＴ３）。

【００５０】

次に、この媒体番号「ＭＩＤ－Ｂ」の情報と共に、「謄本又は副本媒体証明書」、及び「発行機関証明書」を正当媒体発行機関２の鍵Ｋｃによって暗号化した「ＥＫｃ（発行機関証明書）」を謄本・副本保存機関５の鍵Ｋｂを使用して暗号化する（ＳＴ４）。この場合、「謄本又は副本媒体証明書」は本媒体が原本の謄本又は副本の格納用であることを証明するものであり、例えば“本媒体は謄本又は副本格納用である、番号は「ＭＩＤ－Ｂ」”の記述を行う。

【００５１】

また、上記暗号化処理は原本の作成と同様、以下のＥＫｂ（ＤＡＴＡ）を生成する。

ＥＫｂ（ＤＡＴＡ）＝ＥＫｂ（「ＭＩＤ－Ｂ」、「謄本又は副本媒体証明書」、「ＥＫｃ（発行機関証明書））」

次に、上記のようにして暗号化したＥＫｂ（ＤＡＴＡ）を記録媒体（謄本・副本媒体（ＭＯ）８）「ＭＩＤ－Ｂ」のＳＡ領域９に書き込み、謄本・副本証明書シールとする（ＳＴ５）。そして、この謄本・副本証明書シールが書き込まれた謄本又は副本媒体（ＭＯ）８は謄本・副本保存機関５に配布され（ＳＴ６）、以後原本に対する謄本又は副本書き込み用として使用される。

【００５２】

次に、上記謄本又は副本記録媒体（ＭＯ）８に謄本又は副本データを記録する場合、以下の処理を行う。図９はこの処理を説明するフローチャートであり、図１０はその処理を模式的に説明する図である。

【００５３】

先ず、鍵Ｋｂを使用して暗号化された謄本・副本証明書シールを復号する（ＳＴ７、図１０に示す▲１▼）。この場合、謄本・副本保存機関５の鍵Ｋｂを使用し、謄本・副本媒体（ＭＯ）８のＳＡ領域９からＥＫｂａ（ＤＡＴＡ）を読み出し、ＤＥＳのアルゴリズムを使用して、暗号データを復号する。そして、復号処理の結果得られるデータ、即ち鍵Ｋｂで復号された情報「ＭＩＤ－Ｂ」と、平文「ＭＩＤ－Ｂ」を比較し、一致を判断する（ＳＴ８、図１０に示す▲２▼）。

【００５４】

ここで、両データが一致していればホストコンピュータ１２のディスプレイに謄本又は副本のアクセス条件を示すと共に、ライトアクセスを許可する（ＳＴ９、図１０に示す▲３▼）。尚、この場合のアクセス条件は、例えばデータの編集は不可であるが、データの削除は許可する等の条件である。また、ディスプレイにセットされた記録媒体（謄本・副本媒体（ＭＯ）８）が謄本又は副本作成用である旨の表示を行う。一方、上記判断が不一致である場合、ディスプレイにエラー表示を行う。

【００５５】

次に、謄本・副本媒体（ＭＯ）８が正当媒体であると判断した場合、リードアクセスが許可され、謄本・副本保存機関５に必要な情報を記録する。

先ず、原本情報を読み出し、記録する（ＳＴ１０、図１０に示す▲４▼）。この原本情報は前述の原本保存機関１に記録する「ＭＩＤ－Ａ」、「メッセージｍ」、「時刻データ（ｔｏｒ）」、「履歴情報Ｈ」、「認証子（ＣＳｏｒ）」であり、例えばネットワークを介し

て原本保存機関１から送信を受け、使用する。また、メディアを介して供給を受けてもよい。

【００５６】

次に、メッセージｍ’の書き込み処理を行う（ＳＴ１１、図１０に示す▲５▼）。例えば、メッセージｍ’として、“これは副本である”等の記述を行う。次に、時刻生成装置から時刻データ（ｔco）を読み出し、謄本・副本媒体（ＭＯ）８に書き込み、所謂タイムスタンプを生成する（ＳＴ１２、図１０に示す▲６▼）。

【００５７】

次に、履歴管理プログラムを駆動し、履歴情報Ｈ’を書き込む（ＳＴ１３、図１０に示す▲７▼）。この場合、上記履歴情報Ｈ’の内容として、例えば“時刻（ｔco）に謄本・副本保存機関５により○○番の原本データから副本を作成した”等の記述を行う。

【００５８】

次に、上記一連の情報、「ＭＩＤ－Ｂ」、「ＭＩＤ－Ａ」、「メッセージｍ」、「時刻データ（ｔor）」、「履歴情報Ｈ」、「認証子（ＣＳor）」、「メッセージｍ’」、「時刻データ（ｔco）」、「履歴情報Ｈ’」を基に署名を行い（ＳＴ１４）、認証子（ＣＳco）を生成する（ＳＴ１４、図１０に示す▲８▼）。さらに、ハードディスク上の一連の情報組を記録媒体「ＭＩＤ－Ｂ」に保管する（ＳＴ１５、図１０に示す▲９▼）。

【００５９】

以上のように処理することによって、正当媒体発行機関２が認証した謄本又は副本媒体（ＭＯ）８に原本の謄本又は副本が作成され、謄本・副本保存機関５に保存される。

【００６０】

従ってこの場合も、謄本・副本保存機関５は謄本・副本媒体（ＭＯ）８に謄本又は副本の情報を記録する際、必ず記録媒体をドライバにセットして復号処理を行うので、前述の謄本・副本証明書シールが確認され、例えば謄本・副本証明書シールが無い場合や、異なる媒体番号の場合にはエラー表示が行われ、確実に正当な記録媒体に謄本又は副本書類を記録することができる。

【００６１】

また、正当媒体証明書の発行機関である正当媒体発行機関２の「発行機関証明書」も添付されており、必要に応じて認証機関を確認を行うことができる。

さらに、本例の正当媒体の認証は記録媒体のＳＡ領域９に記録され、第三者による改竄不可能な領域に行われ、謄本・副本媒体（ＭＯ）８の正当性が確実に確保される。

＜第３の実施形態＞

次に、本発明の第３の実施形態について説明する。

【００６２】

上記第１の実施形態では、工場４から出荷された記録媒体に対して正当媒体発行機関２が正当媒体の署名を行い、原本媒体（ＭＯ）６を原本保存機関１に送り、原本の記録を行った。しかし、本実施形態では、原本保存機関１が予めＩＤ書き込み済みの記録媒体を保有している場合の処理を説明するものである。

【００６３】

以下、具体的に説明する。

図１１は本実施形態を説明する正当媒体管理システムのシステム図である。本実施形態においても、原本保存機関２１、正当媒体発行機関２２、謄本・副本保存機関２５はＬＡＮやインターネット等のネットワークで接続され、原本保存機関２１は区役所や市役所、会社のセクションであり、文書の原本を保存する。また、正当媒体発行機関２２は文書が記憶された媒体が原本であることを証明する機関であり、謄本・副本保存機関２５は謄本又は副本文書を保存する機関であり、例えば役所の支所や、企業の営業所や支店等が対応する。

【００６４】

図１２は本例の処理を説明するフローチャートである。

先ず、原本保存機関２１は正当媒体発行機関２２に対して正当媒体証明書の配送を要求す

る（ステップ（以下、ＳＴＰで示す）１）。この場合も、同時に原本保存機関２１はＩＤコード（ＩＤａ）を正当媒体発行機関２２に送る。

【００６５】

正当媒体発行機関２２は原本媒体証明書の配送要求を受信すると、前述と同様記憶装置２３（鍵管理簿２３ａ）をアクセスし、鍵管理簿２３ａからＩＤコード（ＩＤａ）に対応する鍵Ｋａを読み出す（ＳＴＰ２）。

【００６６】

本例においては、原本保存機関２１がＩＤ書き込み済みの記録媒体を保有し、原本保存機関２１が記録媒体への原本媒体証明書の書き込みを行うため、正当媒体発行機関２２は上記鍵Ｋａを使用して認証のためのデータを作成し、原本保存機関２１に送る。このため、先ず正当媒体発行機関２２は上記鍵Ｋａで署名した送信データＺＯを作成する。この送信データＺＯは、「ＩＤｃ」、「ＰＷＭ」、「ＯＭＬ」、「ＴＯ」、「ＥＫｃ（ＴＯ、ＰＯＬ）」の各情報である。

【００６７】

ここで、「ＩＤｃ」は正当媒体発行機関２２のＩＤ番号であり、「ＰＷＭ」は原本媒体（ＭＯ）１６のＳＡ領域１７にアクセスするためのパスワードであり、「ＯＭＬ」は正当媒体であることを証明する証明書である。また、「ＰＯＬ」は正当媒体発行機関２２の証明書であり、「ＥＫｃ（ＴＯ、ＰＯＬ）」は、該証明書「ＰＯＬ」を時刻情報「ＴＯ」と共に、鍵Ｋｃで暗号化したデータである。そして、上記各データは、原本保存機関２１の鍵Ｋａによって暗号化され、送信データＺＯとして原本保存機関２１に送られる（ＳＴＰ３）。

【００６８】

原本保存機関２１は正当媒体発行機関２２から送信された上記送信データＺＯを使用して証明書付きの媒体を作成する。

図１３は証明書付きの媒体の作成処理を模式的に示す図である。原本保存機関２１はパスワード「ＰＷＭ」を使用して原本媒体（ＭＯ）１６のＳＡ領域１７にアクセスし、媒体名「ＭＩＤ－Ａ」の情報を読み出す（ＳＴＰ４、図１３に示す▲１▼、▲２▼）。

【００６９】

次に、読み出した媒体番号「ＭＩＤ－Ａ」と、正当媒体発行機関２２から送付された送信データＺＯの情報、即ち正当媒体証明書「ＯＭＬ」、及び正当媒体発行機関２２によって暗号化された発行機関証明書「ＥＫｃ（ＴＯ、ＰＯＬ）」を鍵Ｋａを使用して暗号化し、原本媒体（ＭＯ）１６のＳＡ領域１７に書き込む（ＳＴＰ５、図１３に示す▲３▼）。

【００７０】

上記処理によって、ＥＫａ（ＤＡＴＡ）＝ＥＫａ（「ＭＩＤ－Ａ」、「原本媒体証明書（ＯＭＬ）」、「ＥＫｃ（時刻ＴＯ）、（発行機関証明書ＰＯＬ）」の情報が原本媒体（ＭＯ）１６のＳＡ領域１７に記録され、発行証明シールとなる。

【００７１】

次に、上記のようにして作成された原本媒体（ＭＯ）１６に原本書類を記録する場合、前述の図５に示す処理が行われる。尚、この場合にも、原本保存機関１はホストコンピュータ１０のドライバに原本媒体（ＭＯ）１６を挿入し、鍵Ｋａを使用して原本媒体（ＭＯ）１６から原本証明書シールを復号する。

【００７２】

そして、上記復号の結果によって得られる媒体番号「ＭＩＤ－Ａ」と平文「ＭＩＤ－Ａ」を比較し、両データが一致していれば原本媒体（ＭＯ）１６のアクセス条件を示すと共に、原本媒体（ＭＯ）１６に対するライトアクセスを許可する。そして、前述と同様、メッセージｍの書き込みを行い、更に時刻データ（ｔｏｒ）、及び履歴情報Ｈの書き込み処理を行う。さらに、前述と同様認証子（ＣＳｏｒ）を生成し、最後に一連の情報組のデータを原本媒体（ＭＯ）１６に記録する。

【００７３】

以上のように構成することによって、原本保存機関２１にＩＤ書き込み済みの媒体が用意

されている場合でも、前述と同様に正当媒体発行機関２２の署名を原本媒体（ＭＯ）１６に記憶することができ、原本媒体（ＭＯ）１６に確実に原本データを保存することができる。

＜第４の実施形態＞

次に、本発明の第４の実施形態について説明する。

【００７４】

本実施形態は、正当媒体発行機関が証明する謄本又は副本の作成処理について説明する。尚、この場合もＩＤ書き込み済みの記録媒体は工場４から出荷されるのではなく、謄本・副本保存機関２５が予め保有しているものであり、前述の図１１のシステム図を使用する。以下、具体的に説明する。

【００７５】

先ず、謄本・副本保存機関２５は謄本又は副本の作成に使用する正当媒体証明書の発行を正当媒体発行機関２２に要求し、同時にＩＤコード（ＩＤｂ）を送信する。正当媒体発行機関２２は正当媒体証明書の発行要求を受信すると、供給されたＩＤコード（ＩＤｂ）を使用して鍵管理簿２３ａをアクセスし、鍵管理簿２３ａから対応する鍵Ｋｂを読み出す。そして、前述と同様、正当媒体発行機関２２は送信データＺＣを作成する。この送信データＺＣは「ＩＤｃ」、「ＰＷＭ」、「ＣＭＬ」、「ＴＣ」、「ＥＫｃ（ＴＣ、ＰＯＬ）」を含む。

【００７６】

ここで、前述と同様「ＩＤｃ」は正当媒体発行機関２２のＩＤ番号であり、「ＰＷＭ」は謄本又は副本媒体（ＭＯ）１８のＳＡ領域１９にアクセスするためのパスワードであり、「ＣＭＬ」は正当媒体であることを証明する証明書である。また、「ＰＯＬ」は正当媒体発行機関２２の証明書であり、「ＥＫｃ（ＴＣ、ＰＯＬ）」は、該証明書「ＰＯＬ」を時刻「ＴＣ」と共に、鍵Ｋｃで暗号化した情報である。そして、上記送信データＺＣは謄本・副本保存機関２５に送られる。

【００７７】

謄本・副本保存機関２５では、前述と同様、鍵Ｋｂを使用して謄本・副本媒体（ＭＯ）１８を作成する。その後、暗号化された謄本・副本証明書シールを復号し、謄本・副本媒体（ＭＯ）１８のＳＡ領域１９から暗号化された情報「ＭＩＤ－Ｂ」を読み出し、平文「ＭＩＤ－Ｂ」と比較し、一致判断を行う。そして、両データが一致していればホストコンピュータ１２のディスプレイに謄本又は副本のアクセス条件を示すと共に、謄本又は副本に対するライトアクセスを許可し、不一致であればディスプレイにエラー表示を行う。

【００７８】

その後、謄本・副本媒体（ＭＯ）１８が正当媒体であると判断された場合、謄本・副本保存機関２５は謄本又は副本の情報を記録する。すなわち、例えばネットワークを介して原本情報（「ＭＩＤ－Ａ」、「メッセージｍ」、「時刻データ（ｔｏｒ）」、「履歴情報Ｈ」、「認証子（ＣＳｏｒ）」）を受信し、原本情報を記録し、メッセージｍ’の書き込み処理を行い、更に時刻データ（ｔｏｒ）を読み出し、履歴情報Ｈを書き込む。さらに、認証子（ＣＳｏｒ）を生成し、最後にハードディスク上の一連の情報組を謄本・副本媒体（ＭＯ）１８に記録する。

【００７９】

以上のように処理することによって、謄本・副本保存機関２５にＩＤ書き込み済みの媒体が用意されている場合でも、謄本・副本媒体（ＭＯ）１８に確実に謄本又は副本データを保存することができる。

【００８０】

（付記１）　原本を保存する原本保存機関と、

該原本保存機関を特定するＩＤ番号に対応した鍵を記憶する記憶手段と、

前記記憶手段から前記ＩＤ番号に対応する鍵を取得し、該鍵を使用して記録媒体の改竄不可能な領域に正当媒体の署名を行う正当媒体発行機関とを有し、

前記原本保存機関は、前記改竄不可能領域から該正当媒体の署名を復号し、該記録媒体に

原本書類を記録することを特徴とする正当媒体管理システム。
【００８１】
（付記２）　文書の謄本又は副本を保存する謄本・副本保存機関と、
該謄本・副本保存機関を特定するＩＤ番号に対応した鍵を記憶する記憶手段と、
前記記憶手段から前記ＩＤ番号に対応する鍵を取得し、該鍵を使用して記録媒体の改竄不可能領域に正当媒体の署名を行う正当媒体発行機関とを有し、
前記謄本・副本発行機関は、前記改竄不可能領域から該正当媒体の署名を自己が所有する前記鍵と同じ鍵を使用して復号し、該記録媒体に謄本又は副本書類を記録することを特徴とする正当媒体管理システム。
【００８２】
（付記３）　前記正当媒体発行機関は、固有の媒体番号が付され、改竄不可能領域を有する記録媒体の供給を工場から受けることを特徴とする付記１、又は付記２記載の正当媒体管理システム。
【００８３】
（付記４）　前記改竄不可能領域に記録される正当媒体の署名は、前記固有の媒体番号、及び正当媒体証明書であることを特徴とする付記３記載の正当媒体管理システム。
【００８４】
（付記５）　改竄不可能領域に記録される正当媒体の署名は、前記正当媒体発行機関の発行を証明する署名も含まれることを特徴とする付記４記載の正当媒体管理システム。
【００８５】
（付記６）　前記正当媒体の署名を復号し、前記記録媒体に原本文書を記録する際、時刻情報と履歴情報も記録することを特徴とする付記１記載の正当媒体管理システム。
【００８６】
（付記７）　前記正当媒体の署名を復号し、前記記録媒体に謄本又は副本文書を記録する際、謄本又は副本である旨を記録し、時刻情報及び履歴情報を記録することを特徴とする付記２記載の正当媒体管理システム。
【００８７】
（付記８）　書類の原本を保存する原本保存手段と、
該原本保存手段を特定するＩＤ番号に対応した鍵を記憶する記憶手段と、
前記記憶手段から前記ＩＤ番号に対応する鍵を取得し、該鍵を使用して記録媒体の改竄不可能領域に正当媒体の署名を行うための情報を前記原本保存手段に送信する正当媒体発行手段とを有し、
前記原本保存手段は、該正当媒体発行手段から送信される正当媒体の署名を行うための情報に従って、前記改竄不可能領域に正当媒体の署名を行い、更に自己が所有する前記鍵と同じ鍵を使用して該文書を復号し、該記録媒体に原本文書を記録することを特徴とする正当媒体管理システム。
【００８８】
（付記９）　文書の謄本又は副本を保存する謄本・副本保存手段と、
該謄本・副本保存手段を特定するＩＤ番号に対応した鍵を記憶する記憶手段と、
前記記憶手段から前記ＩＤ番号に対応する鍵を取得し、該鍵を使用して記録媒体の改竄不可能領域に正当媒体の署名を行うための情報を前記謄本・副本保存手段に送信する正当媒体発行手段とを有し、
前記謄本・副本保存手段は、前記正当媒体発行手段から送信される正当媒体の署名を行うための情報に基づいて、前記改竄不可能領域に正当媒体の署名を行い、更に自己が所有する前記鍵と同じ鍵を使用して該文書を復号し、該記録媒体に謄本又は副本文書を記録することを特徴とする正当媒体管理システム。
【００８９】
（付記１０）　前記原本保存機関は、固有の媒体番号が付され、改竄不可能な領域を有する記録媒体の供給を工場から受けることを特徴とする付記８記載の正当媒体管理システム。

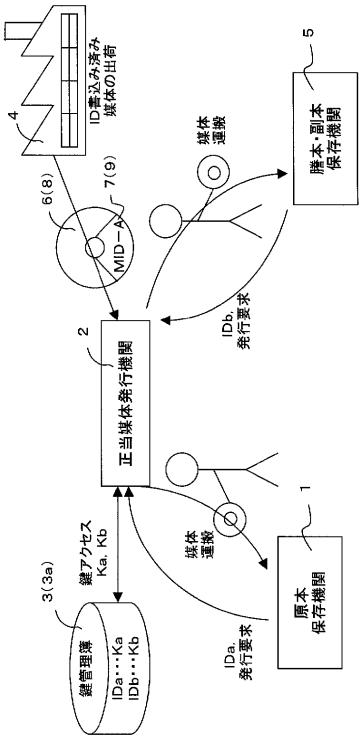
【００９０】
（付記１１） 前記謄本・副本保存機関は、固有の媒体番号が付され、改竄不可能な領域を有する記録媒体の供給を工場から受けることを特徴とする付記９記載の正当媒体管理システム。
【００９１】
（付記１２） 改竄不可能な領域に記録される正当媒体の署名は、前記固有の媒体番号、及び正当媒体証明書であることを特徴とする付記１０、又は１１記載の正当媒体管理システム。
【００９２】
（付記１３） 改竄不可能な領域に記録される正当媒体の署名は、前記正当媒体発行機関の発行を証明する署名も含まれることを特徴とする付記１０、又は１１記載の正当媒体管理システム。
【００９３】
（付記１４） 原本保存手段のＩＤ番号に基づいて該原本保存手段の鍵を記憶手段から読み出し、該鍵を使用して記録媒体の改竄不可能領域に正当媒体証明書の署名を行う署名処理と、
該署名が行われた記録媒体が送付され、該署名を前記鍵を使用して復号し、前記記録媒体に原本文書の記録を行う原本記録処理と、
を行うことを特徴とする正当媒体管理方法。
【００９４】
（付記１５） 謄本・副本保存手段のＩＤ番号に基づいて前記謄本・副本保存手段の鍵を記憶手段から読み出し、該鍵を使用して記録媒体の改竄不可能領域に正当媒体証明書の署名を行う署名処理と、
該署名が行われた記録媒体が送付され、該署名を前記鍵を使用して復号し、前記記録媒体に謄本又は副本文書の記録を行う謄本・副本記録処理と、
を行うことを特徴とする正当媒体管理方法。
【００９５】
（付記１６） 前記改竄不可能領域に行う正当媒体証明書の署名には前記正当媒体発行機関の発行証明の署名も含まれることを特徴とする請求項１４記載の正当媒体管理方法。
【００９６】
（付記１７） 原本保存手段のＩＤ番号に基づいて該原本保存手段の鍵を記憶手段から読み出し、該鍵を使用して記録媒体の改竄不可能領域に正当媒体証明書の署名を行う署名処理と、
該署名が行われた記録媒体が送付され、該署名を前記鍵を使用して復号し、前記記録媒体に原本文書の記録を行う原本記録処理と、
を行うプログラムであって、制御装置が処理可能な正当媒体管理プログラム。
【００９７】
（付記１８） 謄本・副本保存手段のＩＤ番号に基づいて前記謄本・副本保存手段の鍵を記憶手段から読み出し、該鍵を使用して記録媒体の改竄不可能領域に正当媒体証明書の署名を行う署名処理と、
該署名が行われた記録媒体が送付され、該署名を前記鍵を使用して復号し、前記記録媒体に謄本又は副本文書の記録を行う謄本・副本記録処理と、
を行うプログラムであって、制御装置が処理可能な正当媒体管理プログラム。
【００９８】
（付記１９） 原本保存手段のＩＤ番号に基づいて該原本保存手段の鍵を記憶装置から読み出す読出手段と、
前記鍵を使用して記録媒体の改竄不可能領域に正当媒体の署名を行う署名手段と、
を有することを特徴とする正当媒体発行装置。
【００９９】
（付記２０） 謄本・副本保存手段のＩＤ番号に基づいて前記謄本・副本保存手段の鍵を

記憶装置から読み出す読出手段と、
該鍵を使用して記録媒体の改竄不可能領域に正当媒体である署名を行う署名手段と、
を有することを特徴とする正当媒体発行装置。
【０１００】
（付記２１） 前記改竄不可能領域に記録する正当媒体の署名には、前記記録媒体の固有番号、及び正当媒体証明書を含むことを特徴とする付記１９、又は２０記載の正当媒体発行装置。
【０１０１】
（付記２２） 前記改竄不可能領域に記録する正当媒体の署名には、発行機関の発行であることを証明する署名も含まれることを特徴とする付記２１記載の正当媒体発行装置。
【０１０２】
【発明の効果】
以上説明したように、本発明によれば原本媒体に原本文書を記録する際、必ず正当媒体発行機関によって署名された原本証明書シールを復号し、原本媒体の媒体番号を確認するので、確実に原本媒体に原本文書を記録することができる。
【０１０３】
また、原本証明書シールの発行機関である正当媒体発行機関の発行機関証明書も添付されており、記録媒体の原本性がより確実になる。
また、正当媒体の認証は記録媒体の改竄不可能な領域に記録され、より確実な正当媒体の管理を行うことができる。
【０１０４】
さらに、原本保存機関や謄本・副本保存機関側でも正当媒体発行機関の署名が可能であり、何れの機関においても原本媒体の作成、謄本・副本媒体の作成を行うことができる。
【図面の簡単な説明】
【図１】第１の実施形態の正当媒体管理システムのシステム構成図である。
【図２】第１の実施形態の正当媒体管理システムにおける処理動作を説明するフローチャートである。
【図３】原本媒体（ＭＯ）へのデータ書き込み処理を示す図である。
【図４】暗号化処理を説明する図である。
【図５】復号化処理を説明するフローチャートである。
【図６】復号化処理を説明する模式図である。
【図７】復号化処理を説明する模式図である。
【図８】謄本・副本媒体（ＭＯ）を作成するフローチャートである。
【図９】第２の実施形態の正当媒体管理システムにおける処理動作を説明するフローチャートである。
【図１０】謄本・副本媒体（ＭＯ）を作成する模式図である。
【図１１】第３の実施形態の正当媒体管理システムのシステム構成図である。
【図１２】第３の実施形態の正当媒体管理システムにおける処理動作を説明するフローチャートである。
【図１３】暗号化処理を説明する図である。
【符号の説明】
１　原本保存機関
２　正当媒体発行機関
３　記憶装置
３ａ　鍵管理簿
４　工場
５　謄本・副本保存機関
６　原本媒体（ＭＯ）
７　ＳＡ領域
８　謄本・副本媒体（ＭＯ）

９　ＳＡ領域
１０、１２　ホストコンピュータ
１６　原本媒体（ＭＯ）
１７　ＳＡ領域
１８　謄本・副本媒体（ＭＯ）
１９　ＳＡ領域
２１　原本保存機関
２２　正当媒体発行機関
２３　記憶装置
２３ａ　鍵管理簿
２５　謄本・副本保存機関

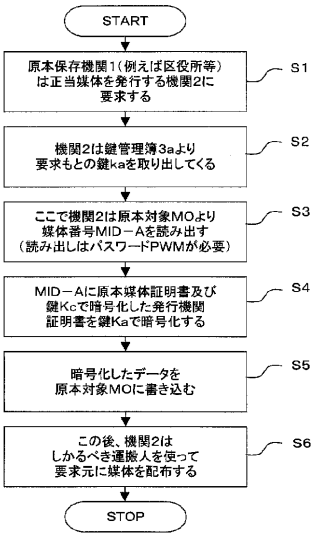
【図１】

第1の実施形態の
正当媒体管理システムのシステム構成図



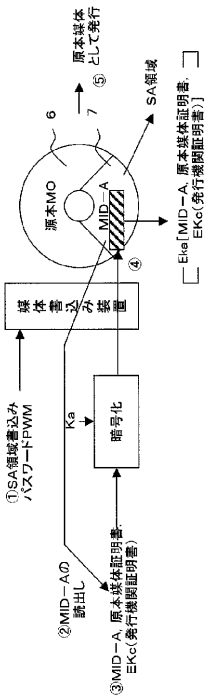
【図２】

第1の実施形態の正当媒体管理システムにおける
処理動作を説明するフローチャート



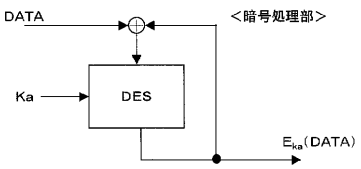
【図３】

原本媒体（MO）へのデータ書き込み処理を示す図



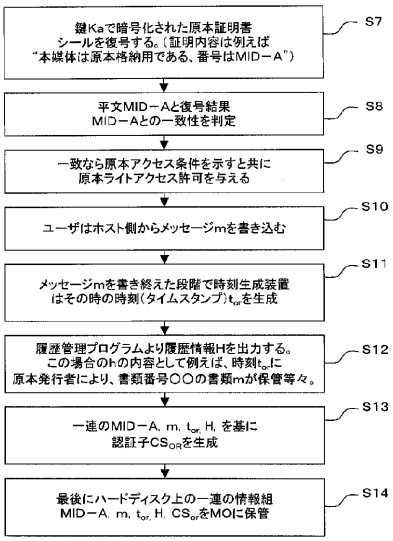
【図４】

暗号化処理を説明する図



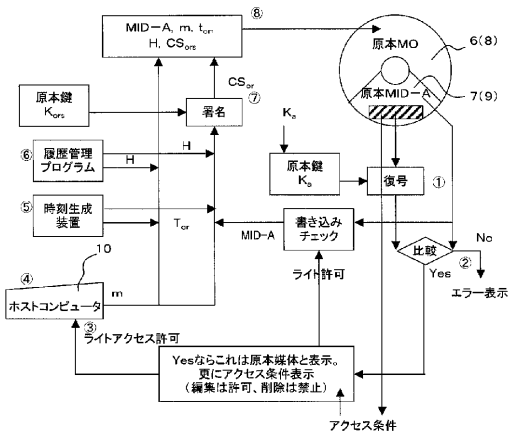
【図５】

復号化処理を説明するフローチャート



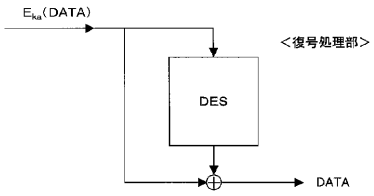
【図６】

復号化処理を説明する模式図



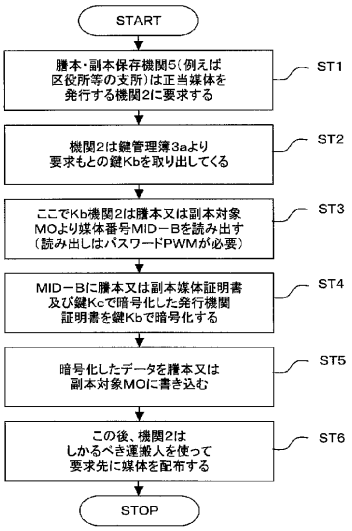
【図７】

復号化処理を説明する模式図



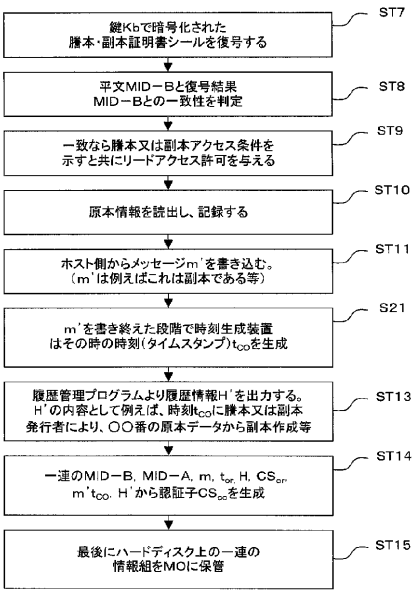
【図８】

謄本・副本媒体(MO)を作成するフローチャート



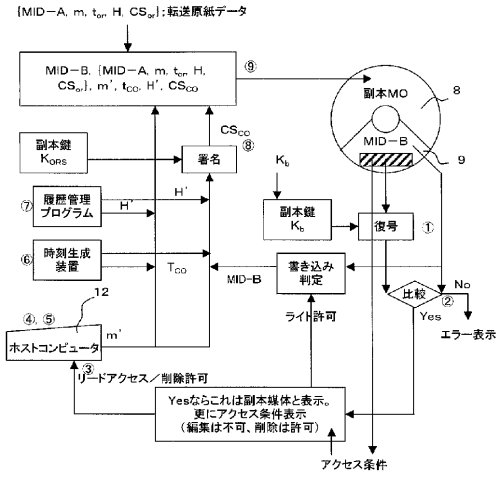
【図９】

第2の実施形態の正当媒体管理システムにおける処理動作を説明するフローチャート



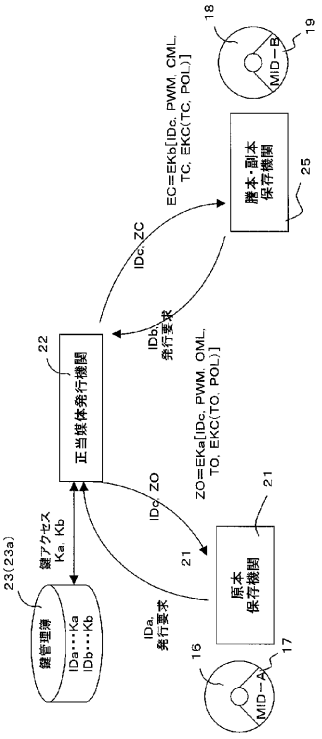
【図１０】

謄本・副本媒体(MO)を作成する模式図



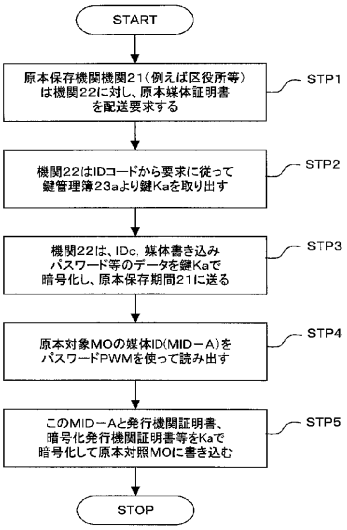
【図１１】

第3の実施形態の
正当媒体管理システムのシステム構成図



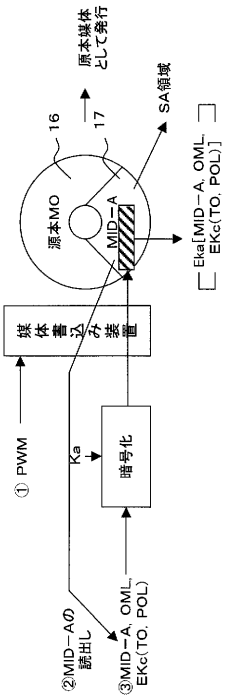
【図１２】

第3の実施形態の正当媒体管理システムにおける
処理動作を説明するフローチャート



【図１３】

暗号化処理を説明する図



フロントページの続き

(56)参考文献 国際公開第００／０４６８０４（WO，Ａ１）
特開２００１－０５２４３１（ＪＰ，Ａ）
特開２００２－１３２４５７（ＪＰ，Ａ）
特開２００１－３１３６３６（ＪＰ，Ａ）
特開２０００－０７６１３８（ＪＰ，Ａ）
特開２０００－０７６１４１（ＪＰ，Ａ）
国際公開第９７／０１４１４４（WO，Ａ１）
特開２０００－２６０１２１（ＪＰ，Ａ）
特開平１１－１９６０８４（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F 21/24