(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2006-18335
(P2006-18335A)
(43)公開日　平成18年1月19日(2006.1.19)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/24	(2006.01)	G06F	12/14	540C	5B017
H04L 9/08	(2006.01)	G06F	12/14	530C	5J104
		H04L	9/00	601C	
		H04L	9/00	601E	

審査請求 未請求　請求項の数 22　ＯＬ　（全 22 頁）

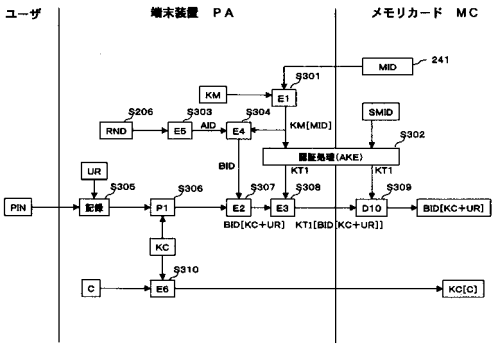
(21)出願番号　特願2004-192399 (P2004-192399)
(22)出願日　平成16年6月30日 (2004.6.30)

(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(74)代理人　100109900
弁理士　堀口　浩
(72)発明者　佐藤　順
東京都青梅市末広町２丁目９番地　株式会社東芝青梅事業所内
(72)発明者　寺内　亨
東京都青梅市末広町２丁目９番地　株式会社東芝青梅事業所内

Ｆターム(参考)　5B017 AA07 BA05
5J104 AA01 AA12 AA16 AA32 EA04 EA15 EA16 JA03 NA02 NA27 NA37 PA14

(54)【発明の名称】コンテンツ記憶準備方法、コンテンツ記憶方法、コンテンツ使用方法、端末システム及び記憶媒体接続可能端末装置

(57)【要約】
【課題】　追加ＩＤを用いてコンテンツを暗号化し、パスワードバインドする場合において、直接追加ＩＤを操作することの困難なコンテンツ記憶方法及びコンテンツ使用方法を提供する。
【解決手段】　予め、ＭＩＤによってバインドされ、メモリカードMCに記憶された乱数ＲＮＤを端末装置ＰＡが呼び出し、乱数ＲＮＤを復号化する。そして、乱数ＲＮＤによって生成された追加ＩＤ（ＡＩＤ）およびＭＩＤによってバインドキー（ＢＩＤ）を生成し、ユーザに使用する際のパスワードを記憶したことを条件に、コンテンツ暗号鍵ＫＣおよびコンテンツ使用方法に関する情報ＵＲをバインドキー（ＢＩＤ）によって暗号化し、更に、記憶するコンテンツをコンテンツ暗号鍵ＫＣによって暗号化し、暗号化されたコンテンツ暗号鍵ＫＣ、コンテンツ使用方法に関する情報ＵＲ及び、暗号化されたコンテンツを



【特許請求の範囲】
【請求項１】
暗号化したコンテンツを端末装置から記憶媒体へ記憶する際に必要な乱数を予め前記記憶媒体に記憶するコンテンツ記憶準備方法であって、
前記記憶媒体から前記記憶媒体を特定する固有情報を読み出し、
乱数を発生させ、
前記乱数を前記コンテンツの使用の際に必要な情報を含むコンテンツ使用情報に書き込み、
前記固有情報を用いて前記コンテンツ使用情報を暗号化し、
前記暗号化したコンテンツ使用情報を前記記憶媒体に記憶する
ことを特徴とするコンテンツ記憶準備方法。
【請求項２】
端末装置から暗号化された第１のコンテンツ使用情報が予め記憶された記憶媒体へコンテンツを記憶するコンテンツ記憶方法であって、
前記記憶媒体から暗号化された前記第１のコンテンツ使用情報を読み出し、
前記記憶媒体を特定する固有情報を用いて読み出した前記第１のコンテンツ使用情報を復号し、
少なくとも前記固有情報と復号した前記第１のコンテンツ使用情報に含まれる乱数とを用いてバインドキーを生成し、
入力されたパスワードを第２のコンテンツ使用情報に書き込み、
前記バインドキーを用いて前記コンテンツを暗号化するためのコンテンツ暗号鍵と前記第２のコンテンツ使用情報とを暗号化すると共に、前記コンテンツ暗号鍵を用いて前記コンテンツを暗号化し、
暗号化した前記コンテンツ暗号鍵、前記第２のコンテンツ使用情報、及び前記コンテンツを前記記憶媒体に記憶する
ことを特徴とするコンテンツ記憶方法。
【請求項３】
記憶媒体から読み出した暗号化された第１のコンテンツ使用情報を復号して得られた乱数と前記記憶媒体を特定する固有情報とから算出されたバインドキーを用いてコンテンツを暗号化するためのコンテンツ暗号鍵と記憶時のパスワードを含む第２のコンテンツ使用情報とが暗号化されて記憶されると共に、前記コンテンツ暗号鍵を用いて前記コンテンツが暗号化されて記憶された前記記憶媒体から前記コンテンツを使用するコンテンツ使用方法であって、
前記記憶媒体から暗号化された前記第１のコンテンツ使用情報を読み出し、
前記固有情報を用いて読み出した前記第１のコンテンツ使用情報を復号し、
前記固有情報と復号した前記第１のコンテンツ使用情報に含まれる乱数とを用いてバインドキーを生成し、
前記バインドキーを用いて前記記憶媒体から読み出した暗号化された前記コンテンツ暗号鍵と第２のコンテンツ使用情報とを復号し、
復号した前記第２のコンテンツ使用情報に含まれる前記パスワードと使用時の入力パスワードとが一致する場合、復号した前記コンテンツ暗号鍵を用いて前記記憶媒体から読み出した暗号化された前記コンテンツを解読して使用する
ことを特徴とするコンテンツ使用方法。
【請求項４】
前記第１のコンテンツ使用情報及び前記第２のコンテンツ使用情報は、それぞれに対応する前記コンテンツの使用の際に必要な情報を含んでいることを特徴とする請求項２に記載のコンテンツ記憶方法または請求項３に記載のコンテンツ使用方法。
【請求項５】
暗号化したコンテンツを端末装置から記憶媒体へ記憶する際に必要な乱数を予め前記記憶媒体に記憶するコンテンツ記憶準備方法であって、

前記記憶媒体から前記記憶媒体を特定する固有情報を読み出し、
前記乱数および入力されたパスワードを前記コンテンツの使用の際に必要な情報を含むコンテンツ使用情報に書き込み、
前記固有情報を用いて前記コンテンツ使用情報を暗号化し、
前記暗号化したコンテンツ使用情報を前記記憶媒体に記憶する
ことを特徴とするコンテンツ記憶準備方法。
【請求項６】
端末装置から暗号化された第１のコンテンツ使用情報が予め記憶された記憶媒体へコンテンツを記憶するコンテンツ記憶方法であって、
前記記憶媒体から暗号化された前記第１のコンテンツ使用情報を読み出し、
前記記憶媒体を特定する固有情報を用いて読み出した前記第１のコンテンツ使用情報を復号し、
入力されたパスワードと復号した前記第１のコンテンツ使用情報に含まれる設定パスワードとが一致する場合、復号した前記第１のコンテンツ使用情報に含まれる乱数を取得し、
少なくとも取得した前記乱数と前記固有情報とを用いてバインドキーを生成し、
前記コンテンツの使用の際に必要な情報を含む第２のコンテンツ使用情報と前記コンテンツを暗号化するためのコンテンツ暗号鍵を統合して統合情報を生成し、
前記バインドキーを用いて前記統合情報を暗号化すると共に、前記コンテンツ暗号鍵を用いて前記コンテンツを暗号化し、
暗号化した前記統合情報及び暗号化した前記コンテンツを前記記憶媒体に記憶する
ことを特徴とするコンテンツ記憶方法。
【請求項７】
記憶媒体から読み出した暗号化された第１のコンテンツ使用情報を復号して得られた乱数と前記記憶媒体を特定する固有情報とから算出されたバインドキーを用いてコンテンツを暗号化するためのコンテンツ暗号鍵と前記コンテンツの使用の際に必要な情報を含む第２のコンテンツ使用情報とが暗号化されて記憶されると共に、前記コンテンツ暗号鍵を用いて前記コンテンツが暗号化されて記憶された前記記憶媒体から前記コンテンツを使用するコンテンツ使用方法であって、
前記記憶媒体から暗号化された前記第１のコンテンツ使用情報を読み出し、
前記固有情報を用いて読み出した前記第１のコンテンツ使用情報を復号し、
前記入力されたパスワードと復号した前記第１のコンテンツ使用情報に含まれる設定パスワードが一致した場合、復号した前記第１のコンテンツ使用情報に含まれる乱数を取得し、
少なくとも前記固有情報と取得した前記乱数とを用いてバインドキーを生成し、
前記バインドキーを用いて前記記憶媒体から読み出した暗号化された第２のコンテンツ使用情報を復号し、
復号した前記第２のコンテンツ使用情報に含まれる前記コンテンツ暗号鍵を用いて前記記憶媒体から読み出した暗号化された前記コンテンツを解読して使用する
ことを特徴とするコンテンツ使用方法。
【請求項８】
前記第１のコンテンツ使用情報は、前記コンテンツの使用の際に必要な情報を含んでいることを特徴とする請求項６に記載のコンテンツ記憶方法または請求項７に記載のコンテンツ使用方法。
【請求項９】
前記設定パスワードは、ディレクトリ毎に設定されることを特徴とする請求項６乃至請求項８のいずれか１項に記載のコンテンツ記憶方法又はコンテンツ使用方法。
【請求項１０】
暗号化したコンテンツを記憶媒体へ記憶する前に、当該記憶媒体から前記記憶媒体を特定する固有情報を読み出し、乱数を前記コンテンツの使用の際に必要な情報を含むコンテンツ使用情報に書き込み、前記固有情報を用いて前記コンテンツ使用情報を暗号化して前

記記憶媒体に出力する端末装置と、
前記端末装置からの前記コンテンツ使用情報を秘匿された特定手続でしかアクセスすることができない記憶領域に記憶する記憶媒体と
を有することを特徴とする端末システム。
【請求項１１】
暗号化された第１のコンテンツ使用情報が予め記憶された記憶媒体へコンテンツを記憶するに際し、前記記憶媒体から暗号化された前記第１のコンテンツ使用情報を読み出し、前記記憶媒体を特定する固有情報を用いて読み出した前記第１のコンテンツ使用情報を復号し、少なくとも前記固有情報と復号した前記第１のコンテンツ使用情報に含まれる乱数とを用いてバインドキーを生成し、入力されたパスワードを第２のコンテンツ使用情報に書き込み、前記バインドキーを用いて前記コンテンツを暗号化するためのコンテンツ暗号鍵と前記第２のコンテンツ使用情報とを暗号化すると共に、前記コンテンツ暗号鍵を用いて前記コンテンツを暗号化し、暗号化した前記コンテンツ暗号鍵、前記第２のコンテンツ使用情報、及び前記コンテンツを前記記憶媒体に出力する端末装置と、
前記第１のコンテンツ使用情報、前記コンテンツ暗号鍵、及び前記第２のコンテンツ使用情報を秘匿された特定手続でしかアクセスすることができない記憶領域に記憶し、前記コンテンツを通常の手続でアクセスすることができる第２の記憶領域に記憶する記憶媒体と
を有することを特徴とする端末システム。
【請求項１２】
記憶媒体から読み出した暗号化された第１のコンテンツ使用情報を復号して得られた乱数と前記記憶媒体を特定する固有情報とから算出されたバインドキーを用いてコンテンツを暗号化するためのコンテンツ暗号鍵と記憶時のパスワードを含む第２のコンテンツ使用情報とが暗号化されて記憶されると共に、前記コンテンツ暗号鍵を用いて前記コンテンツが暗号化されて記憶された前記記憶媒体から前記コンテンツを使用するに際し、前記記憶媒体から暗号化された前記第１のコンテンツ使用情報を読み出し、前記固有情報を用いて読み出した前記第１のコンテンツ使用情報を復号し、前記固有情報と復号した前記第１のコンテンツ使用情報に含まれる乱数とを用いてバインドキーを生成し、前記バインドキーを用いて前記記憶媒体から読み出した暗号化された前記コンテンツ暗号鍵と第２のコンテンツ使用情報を復号し、復号した前記第２のコンテンツ使用情報に含まれる前記パスワードと使用時の入力パスワードとが一致する場合、復号した前記コンテンツ暗号鍵を用いて前記記憶媒体から読み出した暗号化された前記コンテンツを解読して使用する端末装置と、
前記第１のコンテンツ使用情報、前記コンテンツ暗号鍵、及び前記第２のコンテンツ使用情報を秘匿された特定手続でしかアクセスすることができない記憶領域に記憶し、前記コンテンツを通常の手続でアクセスすることができる第２の記憶領域に記憶する記憶媒体と
を有することを特徴とする端末システム。
【請求項１３】
暗号化された第１のコンテンツ使用情報が予め記憶された記憶媒体へコンテンツを記憶するに際し、前記記憶媒体から暗号化された前記第１のコンテンツ使用情報を読み出し、前記記憶媒体を特定する固有情報を用いて読み出した前記第１のコンテンツ使用情報を復号し、入力されたパスワードと復号した前記第１のコンテンツ使用情報に含まれる設定パスワードとが一致する場合、復号した前記第１のコンテンツ使用情報に含まれる乱数を取得し、少なくとも取得した前記乱数と前記固有情報とを用いてバインドキーを生成し、前記コンテンツの使用の際に必要な情報を含む第２のコンテンツ使用情報と前記コンテンツを暗号化するためのコンテンツ暗号鍵を統合して統合情報を生成し、前記バインドキーを用いて前記統合情報を暗号化すると共に、前記コンテンツ暗号鍵を用いて前記コンテンツを暗号化し、暗号化した前記統合情報及び暗号化した前記コンテンツを前記記憶媒体に出力する端末装置と、
前記第１のコンテンツ使用情報、前記統合情報を秘匿された特定手続でしかアクセスすることができない記憶領域に記憶し、前記コンテンツを通常の手続でアクセスすることがで

きる第２の記憶領域に記憶する記憶媒体と
を有することを特徴とする端末システム。
【請求項１４】
記憶媒体から読み出した暗号化された第１のコンテンツ使用情報を復号して得られた乱数と前記記憶媒体を特定する固有情報とから算出されたバインドキーを用いてコンテンツを暗号化するためのコンテンツ暗号鍵と前記コンテンツの使用の際に必要な情報を含む第２のコンテンツ使用情報とが暗号化されて記憶されると共に、前記コンテンツ暗号鍵を用いて前記コンテンツが暗号化されて記憶された前記記憶媒体から前記コンテンツを使用するに際し、前記記憶媒体から暗号化された前記第１のコンテンツ使用情報を読み出し、前記固有情報を用いて読み出した前記第１のコンテンツ使用情報を復号し、前記入力されたパスワードと復号した前記第１のコンテンツ使用情報に含まれる設定パスワードが一致した場合、復号した前記第１のコンテンツ使用情報に含まれる乱数を取得し、少なくとも前記固有情報と取得した前記乱数とを用いてバインドキーを生成し、前記バインドキーを用いて前記記憶媒体から読み出した暗号化された第２のコンテンツ使用情報を復号し、復号した前記第２のコンテンツ使用情報に含まれる前記コンテンツ暗号鍵を用いて前記記憶媒体から読み出した暗号化された前記コンテンツを解読して使用する端末装置と、
前記第１のコンテンツ使用情報、前記コンテンツ暗号鍵、及び前記第２のコンテンツ使用情報を秘匿された特定手続でしかアクセスすることができない記憶領域に記憶し、前記コンテンツを通常の手続でアクセスすることができる第２の記憶領域に記憶する記憶媒体とを有することを特徴とする端末システム。
【請求項１５】
ＲＡＭと、データの読み出し書きこみを行うメモリインタフェースと、データを暗号化及び復号化する暗号化手段及び復号化手段と、乱数を発生する乱数発生手段とを有する端末装置と、
秘匿された特定手続でしかアクセスすることができない第１の記憶領域と、通常の手続でアクセスすることができる第２の記憶領域とを有する記憶媒体とを有し、
前記端末装置と前記記憶媒体が接続され、前記端末装置から前記第２の記憶領域へコンテンツを記録する場合、記録する前に
前記メモリインタフェースによって前記第１の記憶領域に記憶された前記記憶媒体を特定する固有情報を読み出し、
前記乱数発生手段で乱数を発生し、
前記乱数を前記ＲＡＭに記録された前記コンテンツを使用する際に必要な情報を含むコンテンツ使用情報へ記録し、
前記暗号化手段によって前記固有情報を用いて前記コンテンツ使用情報を暗号化し、
前記暗号化したコンテンツ使用情報を前記第１の記憶領域に記憶する
ことを特徴とする記憶媒体接続可能端末装置。
【請求項１６】
ＲＡＭと、データの読み出し書きこみを行うメモリインタフェースと、データを暗号化及び復号化する暗号化手段及び復号化手段と、乱数を発生する乱数発生手段とを有する端末装置と、
秘匿された特定手続でしかアクセスすることができない第１の記憶領域と、通常の手続でアクセスすることができる第２の記憶領域とを有する記憶媒体とを有し、
コンテンツを前記第２の記憶領域へ記憶する場合、
前記メモリインタフェースによって前記第１の記憶領域から前記記憶媒体を特定する固有情報を用いて前記暗号化手段によって暗号化して前記第１の記憶領域に記憶された前記乱数発生手段によって発生させた乱数を含む第１のコンテンツ使用情報を読み出し、
前記復号化手段によって前記固有情報を用いて前記暗号化第１のコンテンツ使用情報を復号して前記乱数を含む前記第１のコンテンツ使用情報を生成し、
少なくとも前記固有情報と前記第１のコンテンツ使用情報に含まれる前記乱数とを用いてバインドキーを生成し、

入力されたパスワードを前記ＲＡＭに記憶された第２のコンテンツ使用情報に記憶し、
前記暗号化部によって前記コンテンツを暗号化するためのコンテンツ暗号鍵と前記第２のコンテンツ使用情報とを前記バインドキーを用いて暗号化すると共に、前記コンテンツ暗号鍵を用いて前記コンテンツを暗号化し、
暗号化した前記コンテンツ暗号鍵と前記第２のコンテンツ使用情報を第１の記憶領域へ記憶し、
暗号化した前記コンテンツを前記第２の記憶領域に記憶する
ことを特徴とした記憶媒体接続可能端末装置。
【請求項１７】
請求項１６に記載の記憶媒体接続可能端末装置であって、
更に使用手段を有し、
前記第２の記憶領域に記憶されたコンテンツを使用する際、
前記メモリインタフェースによって前記第１の記憶領域から暗号化された前記乱数を含む第１のコンテンツ使用情報を読み出し、
前記復号化手段によって前記固有情報を用いて前記乱数を含む第１のコンテンツ使用情報を復号して前記乱数を生成し、
前記固有情報と復号した前記乱数とを用いてバインドキーを生成し、
前記第１の記憶領域から読み出された暗号化された前記コンテンツ暗号鍵と前記パスワードを含む第２のコンテンツ使用情報とを前記復号化手段によって前記バインドキーを用いて復号して前記コンテンツ暗号鍵と前記パスワードを含む第２のコンテンツ使用情報を生成し、
復号した前記パスワードを含む第２のコンテンツ使用情報の前記パスワードと使用時のパスワードが一致する場合、復号した前記コンテンツ暗号鍵を用いて前記第２の記憶領域から読み出された暗号化された前記コンテンツを前記復号化手段によって解読して、
前記使用手段によって使用する
ことを特徴とする請求項１６に記載の記憶媒体接続可能端末装置。
【請求項１８】
ＲＡＭと、
データの読み出し書きこみを行うメモリインタフェースと、
データを暗号化及び復号化する暗号化手段及び復号化手段と、
乱数を発生する乱数発生手段と
を有する端末装置と、
秘匿された特定手続でしかアクセスすることができない第１の記憶領域と、
通常の手続でアクセスすることができる第２の記憶領域と
を有する記憶媒体とを有し、
前記端末装置と前記記憶媒体が接続され、前記端末装置から前記第２の記憶領域へコンテンツを記憶する場合、記憶する前に
前記メモリインタフェースによって前記第１の記憶領域から前記記憶媒体を特定する固有情報を読み出し、
前記乱数発生手段によって乱数を発生し、
前記乱数および前記端末装置へ入力されたパスワードを前記ＲＡＭに記憶された前記コンテンツを使用する際に必要な情報を含むコンテンツ使用情報へ記憶し、
前記暗号化手段によって前記固有情報を用いて前記コンテンツ使用情報を暗号化し、
前記暗号化したコンテンツ使用情報を前記第１の記憶領域に記憶する
ことを特徴とする記憶媒体接続可能端末装置。
【請求項１９】
ＲＡＭと、
データの読み出し書きこみを行うメモリインタフェースと、
データを暗号化及び復号化する暗号化手段及び復号化手段と、
乱数を発生する乱数発生手段と

を有する端末装置と、
秘匿された特定手続でしかアクセスすることができない第１の記憶領域と、
通常の手続でアクセスすることができる第２の記憶領域と
を有する記憶媒体とを有し、
前記第２の記憶領域へコンテンツを記憶する場合、
前記記憶媒体から前記記憶媒体を特定する固有情報を用いて前記乱数発生部で発生した乱数と設定パスワードとを含む第１のコンテンツ使用情報が前記暗号化手段によって暗号化され前記第１の領域へ記憶された暗号化第１のコンテンツ使用情報を前記メモリインタフェースによって読み出し、
前記復号化手段によって前記固有情報を用いて前記暗号化第１のコンテンツ使用情報を復号して前記乱数と前記設定パスワードを含む前記第１のコンテンツ使用情報を生成し、
入力されたパスワードと復号した前記設定パスワードとが一致する場合、復号した前記第１のコンテンツ使用情報から前記乱数を取得し、少なくともこの取得した乱数と前記固有情報とを用いてバインドキーを生成し、
前記コンテンツを使用する際に必要な情報を含む第２のコンテンツ使用情報と前記コンテンツを暗号化するための暗号鍵を統合して統合情報を生成し、
前記暗号化手段によって前記バインドキーを用いて前記統合情報を暗号化すると共に、前記コンテンツ暗号鍵を用いて前記コンテンツを暗号化し、
暗号化した前記統合情報を前記第１の記憶領域へ記憶し、
暗号化した前記コンテンツを前記第２の記憶領域へ記憶する
ことを特徴とする記憶媒体接続可能端末装置。
【請求項２０】
請求項１９に記載の記憶媒体接続可能端末装置であって、
更にコンテンツ使用手段を有し、
前記第２の記憶領域に記憶されたコンテンツを使用する際、
前記メモリインタフェースによって前記第１の記憶領域から暗号化された前記乱数と前記設定パスワードを含む第１のコンテンツ使用情報を読み出し、
前記復号化手段によって前記固有情報を用いて前記乱数と前記設定パスワードを含む第１のコンテンツ使用情報を復号し、
前記入力されたパスワードと前記設定パスワードが一致した場合、前記乱数と前記設定パスワードを含む第１のコンテンツ使用情報より前記乱数を生成し、
前記固有情報と復号した前記乱数とを用いてバインドキーを生成し、
前記第１の記憶領域から読み出された暗号化された前記コンテンツ暗号鍵を含む第２のコンテンツ使用情報を前記復号化手段によって前記バインドキーを用いて復号して前記コンテンツ暗号鍵を含む第２のコンテンツ使用情報を生成し、
復号した前記コンテンツ暗号鍵を用いて前記第２の記憶領域から読み出された暗号化された前記コンテンツを前記復号化手段によって解読して、
前記使用手段によって使用する
ことを特徴とする請求項１９に記載の記憶媒体接続可能端末装置。
【請求項２１】
前記第１のコンテンツ使用情報は前記コンテンツを使用する際に必要な情報を含んでいることを特徴とする請求項１９または請求項２０に記載の記憶媒体接続可能端末装置。
【請求項２２】
前記設定パスワードはディレクトリ毎に設定されることを特徴とする請求項１９乃至請求項２１のいずれか１項に記載の記憶媒体接続可能端末装置。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、コンテンツ記憶準備方法、コンテンツ記憶方法、コンテンツ使用方法、端末

システム及び記憶媒体接続可能端末装置に関する。
【背景技術】
【０００２】
近年、パーソナルコンピュータや携帯電話機、ＰＤＡ（Personal Digital Assistants）、オーディオプレーヤ、電子カメラ等の装置では、メモリカード等の記憶メディアを使用してコンテンツを記憶／再生するものが多くなっており、更にこのような装置で使用される記憶メディアには著作権保護機能を備えたものが増えている。
【０００３】
記憶メディアに適用される著作権保護の種類には、主にメディアバインド、セットバインド、及びユーザバインド等がある。
【０００４】
メディアバインドは、コンテンツを暗号化もしくは復号するための鍵（以下、コンテンツ解読鍵と記す。）を、記憶メディアの製造番号やロット番号等のメディア固有の情報（以下、ＭＩＤと記す。）により暗号化し、記憶メディアの特殊な記憶領域に保存しておく。そして、コンテンツを再生する場合に、上記特殊記憶領域からＭＩＤを読み出してコンテンツ解読鍵を復号し、この復号されたコンテンツ解読鍵によりコンテンツを復号するものである。従って、コンテンツが他のメモリカード等に不正にコピーされたとしても、オリジナルのＭＩＤとコピー先の記憶メディア（例えば、メモリカード等）のＭＩＤが異なることから、コンテンツ解読鍵を適切に取得することができないため、結果的にコンテンツの不正コピーを防止することができる。
【０００５】
また、セットバインドは、ＭＩＤと、搭載する端末装置の製造番号等の機器固有の情報（以下、セットＩＤと記す）とを組み合わせてコンテンツ解読鍵を暗号化し、これにより記憶メディアに保存されたコンテンツの再生を搭載する端末装置に限定するものである。
【０００６】
同様に、ユーザバインドは、ＭＩＤと、コンテンツを使用するユーザの固有情報（以下、ユーザＩＤと記す。）とを組み合わせてコンテンツ解読鍵を暗号化し、これにより記憶メディアに保存されたコンテンツの再生を使用するユーザに限定するものである。なお、ユーザＩＤとしては、ユーザの会員番号、電話番号等が使用される。
【０００７】
その他、記憶メディアの著作権保護機能には、上記ＭＩＤ、セットＩＤ、及びユーザＩＤからなる３種類のＩＤを組み合わせてコンテンツ解読鍵を暗号化するものもある。このような任意のＩＤを組み合わせて作ったＩＤを使用してコンテンツ解読鍵を暗号化することで、目的に応じてコンテンツの著作権を保護することが可能となる。なお、複数のＩＤを組み合わせて作ったＩＤを一般にバインドＩＤ（以下、ＢＩＤと記す。）と呼んでいる。
【０００８】
そして、以上に述べた著作権保護技術においては、ＢＩＤによりコンテンツ解読鍵を暗号化している。このため、例えば端末装置の故障などによって買い換えた場合に、セットＩＤが変化してＢＩＤを正しく生成できなくなり、この結果コンテンツの再生を行えなくなるという問題があった。そして、この問題を解決するためにＭＩＤと１つ乃至複数の追加ＩＤ（以下、ＡＩＤという。）を用いてセットバインド及びユーザバインドを実現するものがある（例えば、特許文献１参照。）。ここで用いるＡＩＤとしては、端末装置を特定するＩＤやユーザを特定するＩＤや、ユーザが所属するグループを特定するＩＤなどが用いられている。
【特許文献１】特開２００４－１３９４３３号公報（１１頁乃至２２頁、図５）
【発明の開示】
【発明が解決しようとする課題】
【０００９】
従来のセットバインド及びユーザバインド等に用いられるＡＩＤは、更にセキュリティ

を高めるため、ＡＩＤにユーザが設定した暗証番号もしくはパスワードを単純に当てはめることで、パスワードバインドを実現することができる。しかし、読み取り時にユーザがパスワードを変更することなどにより、ＡＩＤの値を直接操作できることになるため、セキュリティはある程度高まるものの、セキュリティの脆弱さが発生するという問題点がある。

【００１０】

本発明は上記問題点を解決するためになされたものであり、ＡＩＤの値を直接操作しないパスワードバインドを実現したコンテンツ記憶準備方法、コンテンツ記憶方法、コンテンツ使用方法、端末システム及び記憶媒体接続可能端末装置を提供することを目的とする。

【課題を解決するための手段】

【００１１】

本発明のコンテンツ記憶準備方法は、暗号化したコンテンツを端末装置から記憶媒体へ記憶する際に必要な乱数を予め前記記憶媒体に記憶するコンテンツ記憶準備方法であって、前記記憶媒体から前記記憶媒体を特定する固有情報を読み出し、前記乱数を前記コンテンツの使用の際に必要な情報を含むコンテンツ使用情報に書き込み、前記固有情報を用いて前記コンテンツ使用情報を暗号化し、前記暗号化したコンテンツ使用情報を前記記憶媒体に記憶することを特徴とする。

【００１２】

また、本発明のコンテンツ記憶方法は、端末装置から暗号化された第１のコンテンツ使用情報が予め記憶された記憶媒体へコンテンツを記憶するコンテンツ記憶方法であって、前記記憶媒体から暗号化された前記第１のコンテンツ使用情報を読み出し、前記記憶媒体を特定する固有情報を用いて読み出した前記第１のコンテンツ使用情報を復号し、少なくとも前記固有情報と復号した前記第１のコンテンツ使用情報に含まれる乱数とを用いてバインドキーを生成し、入力されたパスワードを第２のコンテンツ使用情報に書き込み、前記バインドキーを用いて前記コンテンツを暗号化するためのコンテンツ暗号鍵と前記第２のコンテンツ使用情報とを暗号化すると共に、前記コンテンツ暗号鍵を用いて前記コンテンツを暗号化し、暗号化した前記コンテンツ暗号鍵、前記第２のコンテンツ使用情報、及び前記コンテンツを前記記憶媒体に記憶することを特徴とする。

【００１３】

また、本発明のコンテンツ使用方法は、記憶媒体から読み出した暗号化された第１のコンテンツ使用情報を復号して得られた乱数と前記記憶媒体を特定する固有情報とから算出されたバインドキーを用いてコンテンツを暗号化するためのコンテンツ暗号鍵と記憶時のパスワードを含む第２のコンテンツ使用情報とが暗号化されて記憶されると共に、前記コンテンツ暗号鍵を用いて前記コンテンツが暗号化されて記憶された前記記憶媒体から前記コンテンツを使用するコンテンツ使用方法であって、前記記憶媒体から暗号化された前記第１のコンテンツ使用情報を読み出し、前記固有情報を用いて読み出した前記第１のコンテンツ使用情報を復号し、前記固有情報と復号した前記第１のコンテンツ使用情報に含まれる乱数とを用いてバインドキーを生成し、前記バインドキーを用いて前記記憶媒体から読み出した暗号化された前記コンテンツ暗号鍵と第２のコンテンツ使用情報とを復号し、復号した前記第２のコンテンツ使用情報に含まれる前記パスワードと使用時の入力パスワードとが一致する場合、復号した前記コンテンツ暗号鍵を用いて前記記憶媒体から読み出した暗号化された前記コンテンツを解読して使用することを特徴とする。

【発明の効果】

【００１４】

本発明によれば、コンテンツの秘密管理を強化するためＡＩＤの値を直接操作しないパスワードバインドを実現したコンテンツ記憶準備方法、コンテンツ記憶方法、コンテンツ使用方法、端末システム及び記憶媒体接続可能端末装置を提供することができる。

【発明を実施するための最良の形態】

【００１５】

以下に、本発明の実施の形態を説明する。

【実施例１】

【００１６】

本発明の第１の実施の形態を図面を用いて説明する。図１は、本発明の第１の実施の形態にかかわる端末装置ＰＡの回路構成を示すブロック図である。

【００１７】

端末装置ＰＡは、例えばマイクロプロセッサを使用したＣＰＵ１１を備え、このＣＰＵ１１が接続されるバス１０には、ＲＡＭ１２、ＲＯＭ１３、デコーダ１４、メモリインタフェース１６、及び暗号化・復号化部１７、乱数発生部１８がそれぞれ接続されている。

【００１８】

また、デコーダ１４には表示部１５が接続されている。更に、ＲＡＭ１２には端末装置ＰＡのデータ処理に必要な各種のプログラム及びデータの他にコンテンツ使用に関する情報ＵＲ１２０が記憶される。また、データ処理に必要な各種のプログラムはＲＯＭ１３にも記憶されている。

【００１９】

そして、メモリインタフェース１６には、メモリカードＭＣが着脱時自在に接続される。メモリインタフェース１６は、ＣＰＵ１１の制御に基づいてメモリカードＭＣとの間でデータの書き込み及び読み出し処理を行う。メモリカードＭＣには、図示しないコンテンツサーバＣＳＶからネットワークを介してダウンロードされたコンテンツや、ＲＡＭ１２又はＲＯＭ１３に格納されているコンテンツ等が記憶される。ここで、コンテンツとは、音楽、静止画、テキストデータ及びプログラムなどのユーザに提供するあらゆるコンテンツであり、さらには電子メールやブックマーク、電話帳などの個人情報もコンテンツの概念に含まれる。

【００２０】

デコーダ１４は、上記コンテンツサーバＣＳＶからダウンロードされたコンテンツや、メモリカードＭＣに記憶されているコンテンツをデコードして表示部１５に表示するものである。表示部１５には、例えばＬＣＤが使用される。また、暗号化・復号化部１７は、コンテンツや、コンテンツを解読する解読鍵などを暗号化したり、復号したりする。なお、本発明における端末装置ＰＡの構成はこれに限定されることなく、発明を実施できる範囲内において応用可能である。例えば、ＣＰＵ１１がＣＰＵ１１ａとＣＰＵ１１ｂの２つが存在し、ＣＰＵ１１ｂと暗号化・復号化部１７と、メモリインタフェース１６と、乱数発生部１８を１つの半導体チップで実現するように設計することも可能である。

【００２１】

次に、メモリカードＭＣの詳細な構成を説明する。図２は、メモリカードＭＣの構成を示すブロック図である。図２のように、メモリカードＭＣは、コントローラ２１と、秘匿領域２２及び公開領域２３からなる記憶部とから構成される。

【００２２】

秘匿領域２２は、コントローラ２１を通して非公開の手順、つまり秘匿された特定手続でしかアクセスすることができない論理的な記憶領域であり、コンテンツの復号に必要な情報を記憶するために用いられる。そして、この秘匿領域２２は、秘密の定数が記憶される秘匿ＲＯＭ領域２４と、秘密の変数が記憶される秘匿Ｒ／Ｗ（リードライト）領域２５とから構成される。物理的には、秘匿ＲＯＭ領域２４は、例えば内蔵するＲＯＭ（読み出し専用不揮発メモリ）上に確保され、秘匿Ｒ／Ｗ領域２５は、例えば内蔵するフラッシュメモリ（書き換え可能な不揮発メモリ）の特定領域に確保される。

【００２３】

図３は、この秘匿領域２２の構成と記憶内容を示している。秘匿ＲＯＭ領域２４には、ＭＩＤ（メディアＩＤ）２４１が記憶されている。ＭＩＤは、メモリカードＭＣ毎に固有に割り当てられた番号であり、シリアル番号や製造番号等の様々な識別情報が使用される。

【００２４】

秘匿Ｒ／Ｗ領域２５には、秘匿管理ファイル２５１が記憶される。この秘匿管理ファイル２５１は、コンテンツを復号するための鍵データやコンテンツのライセンス情報等を格納するためのもので、第１のフィールド２５１０には暗号管理データ数＝ｎが格納され、それに続く暗号管理データ（１）２５１１～暗号管理データ（ｎ）２５１ｎにはそれぞれ上記暗号管理データ数＝ｎにより示されるｎ個の暗号管理データが格納される。暗号管理データは、コンテンツを復号するための鍵データや、コンテンツのライセンス情報を暗号化したものである。

【００２５】

一方、メモリカードＭＣの公開領域２３は、秘匿領域２２以外の通常の手順でアクセス可能な論理的な記憶領域であり、読み出し専用の公開ＲＯＭ領域２６と、書き換え可能な公開Ｒ／Ｗ（リードライト）領域２７とから構成される。

【００２６】

図４は、この公開Ｒ／Ｗ領域２７の構成と記憶内容を示している。公開Ｒ／Ｗ領域２７には、コンテンツ管理ファイル２７１と、バインド管理データを管理するためのバインド管理ファイル２７２と、任意の数のコンテンツＡ，Ｂ‥を格納する領域２７３Ａ，２７３Ｂ‥とを有する。なお、任意のディレクトリＡの下にコンテンツＣ（領域２７３Ｃ）を格納することも可能である。

【００２７】

そして、コンテンツ管理ファイル２７１は、メモリカードＭＣ内に格納されているコンテンツと暗号管理データとを関連付けるためのファイルであり、第１のフィールド２７１０にはコンテンツ管理データ数（＝ｎ）が格納される。また、それに続くコンテンツ管理データ（１）２７１１～コンテンツ管理データ（ｎ）２７１ｎには、それぞれ上記コンテンツ管理データ数（＝ｎ）により示されるｎ個のコンテンツ管理データが格納される。

【００２８】

更に、各コンテンツのコンテンツ管理データ（１）～（ｎ）は、それぞれ２種類のフィールドにより構成され、その第１のフィールド２７１ａには、コンテンツのファイル名が記憶される。なお、コンテンツがディレクトリに格納されているときには、コンテンツのファイル名にはルートディレクトリのパスも含まれる。また、第２のフィールド２７１ｂには、暗号管理データ番号が格納される。この暗号管理データ番号は、該当するコンテンツに対応した暗号管理データが、秘匿Ｒ／Ｗ領域２５の秘匿管理ファイル２５１に格納されている先頭の暗号管理データから何番目の暗号管理データなのかを示すものである。例えば、暗号管理データ番号がｎであったとすると、該当するコンテンツの暗号管理データは秘匿管理ファイル２５１のｎ番目の暗号管理データ２５１ｎとなる。

【００２９】

次に、以上のように構成された端末装置ＰＡ及びメモリカードＭＣによるコンテンツの著作権保護処理動作を図５乃至図８を用いて説明する。なお、この明細書・特許請求の範囲において、メモリカードＭＣに記憶されたコンテンツを端末装置ＰＡで「使用する」とは、メモリカードＭＣに記憶されたコンテンツを端末装置ＰＡで再生すること、メモリカードＭＣに記憶されたコンテンツを端末装置ＰＡへコピーすること、及びメモリカードＭＣに記憶されたコンテンツを端末装置ＰＡへ移動することなどの概念を意味する。

【００３０】

（メモリカードＭＣに乱数値ＲＮＤを記憶）

まず、コンテンツを端末装置ＰＡからメモリカードＭＣに記憶する際、及びメモリカードＭＣに記憶されたコンテンツを使用する際に必要な乱数値ＲＮＤを、メモリカードＭＣへ記憶する場合について述べる。図５は、その場合の端末装置ＰＡとメモリカードＭＣの処理手順と処理内容を示すシーケンス図である。

【００３１】

まず、端末装置ＰＡのＣＰＵ１１は、メモリインタフェース１６を介してメモリカードＭＣの秘匿ＲＯＭ領域２４に格納されているＭＩＤ２４１を取得する。そして、このＭＩＤ２４１と端末装置ＰＡによって決まる情報ＫＭとを計算して相互認証処理（ＡＫＥ）に

用いる情報ＫＭ［ＭＩＤ］を生成する（Ｓ１０１、図５のＥ１）。例えば、情報ＫＭ［ＭＩＤ］は、端末装置ＰＡのデバイスＩＤ（ＫＭ）とメモリカードＭＣのＭＩＤ２４１から計算する。

【００３２】

次に、端末装置ＰＡのＣＰＵ１１は、Ｓ１０１で生成した情報ＫＭ［ＭＩＤ］を用いて相互認証処理（ＡＫＥ）を実行する。また、このときメモリカードＭＣのコントローラ２１においても、ＭＩＤ２４１を暗号化した秘匿メディアＩＤ（ＳＭＩＤ）を用いて相互認証処理（ＡＫＥ）を実行する（Ｓ１０２、図５のＡＫＥ）。なお、秘匿メディアＩＤ（ＳＭＩＤ）とは、メモリカードＭＣを端末装置ＰＡに初めて装着したときに決められる値であって、端末装置ＰＡのデバイスＩＤ（ＫＭ）とメモリカードＭＣのＭＩＤ２４１を用いて計算された値である。

【００３３】

この相互認証処理（ＡＫＥ）では、端末装置ＰＡ及びメモリカードＭＣが同じ関数ｇ（ｘ、ｙ）、ｈ（ｘ、ｙ）を共有しており、端末装置ＰＡで生成された情報ＫＭ［ＭＩＤ］が当該メモリカードＭＣの秘匿メディアＩＤ（ＳＭＩＤ）とを端末装置ＰＡのＣＰＵ１１及びメモリカードＭＣのコントローラ２１において、それぞれ入力レベルで比較し、同じならば、相互認証処理（ＡＫＥ）により互いに一方が他方を正当であると確認できるようになっている。この相互認証処理（ＡＫＥ）は、例えば特開２００１－２３３５３号公報、特開２００１－２２６４７号公報等に記載された方式を用いて処理すれば良い。この相互認証処理（ＡＫＥ）において、それぞれ一方が他方を正当であると確認できた場合には、端末装置ＰＡ及びメモリカードＭＣとも鍵情報ＫＴ１を生成し、相互認証されなかった場合には処理を終了する。

【００３４】

一方、端末装置ＰＡの乱数発生部１８は乱数値ＲＮＤを発生する（Ｓ１０３、図５の「ＲＮＤ発生」）。そして、ＣＰＵ１１は、ＲＡＭ１２に記憶されるコンテンツ使用に関する情報ＵＲ１２０の拡張部に乱数値ＲＮＤを記憶する（Ｓ１０４、図５の「ＵＲへＲＮＤを記憶」）。暗号化・復号化部１７は、乱数値ＲＮＤを含む情報ＵＲとＳ１０１で計算したＫＭ［ＭＩＤ］とを受信して、暗号化を行う（Ｓ１０５、図５のＥ２）。ここで、コンテンツ使用に関する情報ＵＲ１２０は、当該コンテンツの複製・移動の可・不可、並びに回数の情報等、主にコンテンツを使用する際に必要な情報が記載されており、その中の一つにコンテンツの使用を拡張する際の情報を記憶する拡張部がある。そして、情報ＵＲ１２０はコンテンツ毎にそれぞれ設定され、ＲＡＭ１２に記憶されるが、メモリカードＭＣへの記憶後にＲＡＭ１２から消去される。

【００３５】

次に、暗号化・復号化部１７は、Ｓ１０５で暗号化した乱数値ＭＩＤ［ＵＲ］とＳ１０２の相互認証処理（ＡＫＥ）で生成された鍵情報ＫＴ１とを用いて、更に暗号化を行う（Ｓ１０６、図５のＥ３）。そして、暗号化・復号化部１７は、こうして二重に暗号化を施した情報ＫＴ１［ＭＩＤ［ＵＲ］］をメモリインタフェース１７からメモリカードＭＣへ送る。

【００３６】

メモリカードＭＣのコントローラ２１は、端末装置ＰＡから送られた二重に暗号化を施した情報ＫＴ１［ＭＩＤ［ＵＲ］］を、Ｓ１０２の相互認証処理（ＡＫＥ）で生成した鍵情報ＫＴ１を用いて復号する（Ｓ１０７、図５のＤ１０）。そして、一つ目の暗号を復号した暗号化情報ＭＩＤ［ＵＲ］を秘匿管理ファイル２５１の例えば暗号管理データ（１）２５１１として格納する。また、その暗号管理データ（１）の番号をコンテンツ管理ファイル２７１の例えばコンテンツ管理データ（１）２７１１に暗号管理データ番号２７１ｂとして格納する。

【００３７】

更に、上記のＳ１０３からＳ１０７の処理と並行して、端末装置ＰＡからメモリカードＭＣへコンテンツの代わりとなるダミー情報が送られ、メモリカードＭＣのコントローラ

２１は、そのダミー情報を公開Ｒ／Ｗ領域２７のコンテンツＡ（２７３Ａ）へ格納する（Ｓ１０８）。

【００３８】

（乱数値ＲＮＤをメモリカードＭＣから読み出す）

次に、コンテンツを端末装置ＰＡからメモリカードＭＣに記憶する際、及びメモリカードＭＣに記憶されたコンテンツを使用する際に必要な乱数ＲＮＤを、メモリカードＭＣから読み出す場合について述べる。図６は、その場合の端末装置ＰＡとメモリカードＭＣの処理手順と処理内容を示すシーケンス図である。

【００３９】

まず、端末装置ＰＡのＣＰＵ１１は、メモリインタフェース１６を介してメモリカードＭＣの秘匿ＲＯＭ領域２４よりＭＩＤ２４１を取得する。そして、このＭＩＤ２４１と端末装置ＰＡの例えばデバイスＩＤの情報ＫＭとを計算して、相互認証処理（ＡＫＥ）に出力する情報ＫＭ［ＭＩＤ］を生成する（Ｓ２０１、図６のＥ１）。

【００４０】

次に、端末装置ＰＡのＣＰＵ１１は、Ｓ２０１で生成した情報ＫＭ［ＭＩＤ］を用いて相互認証処理（ＡＫＥ）を実行する。また、このときメモリカードＭＣのコントローラ２１においても、ＭＩＤ２４１を暗号化した秘匿メディアＩＤ（ＳＭＩＤ）を用いて相互認証処理（ＡＫＥ）を実行する（Ｓ２０２、図６のＡＫＥ）。この相互認証処理（ＡＫＥ）において、相互認証された場合には、端末装置ＰＡ及びメモリカードＭＣとも鍵情報ＫＴ１を生成し、相互認証されなかった場合には処理を終了する。

【００４１】

次に、メモリカードＭＣのコントローラ２１は、秘匿Ｒ／Ｗ領域２５の例えば暗号管理データ（１）２５１１から暗号化された情報ＭＩＤ［ＵＲ］を読み出し、この情報ＭＩＤ［ＵＲ］をＳ２０２で生成した鍵情報ＫＴ１を用いて暗号化する（Ｓ２０３、図６のＥ１０）。そして、コントローラ２１は、この二重に暗号化が施された情報ＫＴ１［ＭＩＤ［ＵＲ］］を端末装置ＰＡへ送る。

【００４２】

端末装置ＰＡのＣＰＵ１１は、メモリカードＭＣから送られた暗号化情報ＫＴ１［ＭＩＤ［ＵＲ］］を受信して暗号化・復号化部１７に送信する。そして暗号化・復号化部１７は、Ｓ２０２で生成された鍵情報ＫＴ１によって二重に暗号化が施された情報ＫＴ１［ＭＩＤ［ＵＲ］］を復号する（Ｓ２０４、図６のＤ３）。暗号化・復号化部１７は更に、この一つ目の暗号を復号した暗号化された情報ＭＩＤ［ＵＲ］を、Ｓ２０１で計算した情報ＫＭ［ＭＩＤ］によって復号する（Ｓ２０５、図６のＤ２）。これにより、コンテンツ使用に関する情報ＵＲ１２０が得られる。その後、コンテンツを記憶または使用する際、この情報ＵＲの拡張部に記載された乱数値ＲＮＤを読み出して（Ｓ２０６）、暗号化や復号などが行われる。

【００４３】

（コンテンツを端末装置ＰＡからメモリカードＭＣに記憶）

次に、コンテンツを端末装置ＰＡからメモリカードＭＣに記憶する場合について述べる。なお、コンテンツをメモリカードＭＣに記憶する際においては、メモリカードＭＣから乱数値ＲＮＤを読み出す処理（図６のＳ２０６を得る処理）が先に実行されなければならないが、ここでは図６の処理が先に実行されたものとして説明する。図７は、コンテンツを端末装置ＰＡからメモリカードＭＣに記憶する場合の処理手順と処理内容を示すシーケンス図である。

【００４４】

まず、端末装置ＰＡのＣＰＵ１１は、メモリインタフェース１６を介してメモリカードＭＣの秘匿ＲＯＭ領域２４よりＭＩＤ２４１を取得する。そして、このＭＩＤ２４１と端末装置ＰＡの例えばデバイスＩＤの情報ＫＭとを計算して相互認証処理（ＡＫＥ）に用いる情報ＫＭ［ＭＩＤ］を生成する（Ｓ３０１、図７のＥ１）。

【００４５】

次に、端末装置ＰＡのＣＰＵ１１は、Ｓ３０１で生成した情報ＫＭ［ＭＩＤ］を用いて相互認証処理（ＡＫＥ）を実行する。また、このときメモリカードＭＣのコントローラ２１においても、ＭＩＤを暗号化した秘匿メディアＩＤ（ＳＭＩＤ）を用いて相互認証処理（ＡＫＥ）を実行する（Ｓ３０２、図７のＡＫＥ）。この相互認証処理（ＡＫＥ）において、相互認証された場合には、端末装置ＰＡ及びメモリカードＭＣとも鍵情報ＫＴ１を生成し、相互認証されなかった場合には処理を終了する。

【００４６】

また、端末装置ＰＡのＣＰＵ１１はこのＳ３０１の処理と並行して、先に図６の処理で復号した情報ＵＲの拡張部に記憶された乱数値ＲＮＤを用いて追加ＩＤ（ＡＩＤ）を生成する（Ｓ３０３、図７のＥ５）。更にＣＰＵ１１は、Ｓ３０１で計算したＫＭ［ＭＩＤ］の値とこの追加ＩＤ（ＡＩＤ）とからバインドキーＢＩＤを生成する（Ｓ３０４、図７のＥ４）。なお、この処理において、Ｓ３０３を省略して情報ＵＲの拡張部に記憶された乱数ＲＮＤをそのまま追加ＩＤ（ＡＩＤ）としてＳ３０４を実行して、バインドキーＢＩＤを求めても良い。

【００４７】

また、このＳ３０４の処理と並行して、端末装置ＰＡのユーザからパスワード（ＰＩＮ）が入力されると、ＣＰＵ１１は復号した上記情報ＵＲの拡張部にそのパスワードを記憶する（Ｓ３０５、図７の「記憶」）。そして、パスワード（ＰＩＮ）の記憶が行われると、ＣＰＵ１１は記憶したいコンテンツの暗号鍵ＫＣと、コンテンツ使用に関する情報ＵＲとを統合する（Ｓ３０６、図７のＰ１）。そして、暗号化・復号化部１７は、このＳ３０６で統合された情報（ＫＣ＋ＵＲ）をＳ３０４で生成されたバインドキーＢＩＤによって暗号化する（Ｓ３０７、図７のＥ２）。暗号化・復号化部１７は更に、Ｓ３０７で生成した暗号化情報ＢＩＤ［ＫＣ＋ＵＲ］を、Ｓ３０２で生成された鍵情報ＫＴ１によって更に暗号化する（Ｓ３０８、図７のＥ３）。そして、ここで生成された二重に暗号化が施された情報ＫＴ１［ＢＩＤ［ＫＣ＋ＵＲ］］は、暗号化・復号化部１７からメモリインタフェース１６を介してメモリカードＭＣへ送られる。

【００４８】

メモリカードＭＣのコントローラ２１は、端末装置ＰＡから送られた暗号化情報ＫＴ１［ＢＩＤ［ＫＣ＋ＵＲ］］をＳ３０２で生成した鍵情報ＫＴ１を用いて一つ目の暗号を復号する（Ｓ３０９、図７のＤ１０）。そして、Ｓ３０９で復号された暗号化情報ＢＩＤ［ＫＣ＋ＵＲ］を秘匿管理ファイル２５１の例えば暗号管理データ（２）２５１２に格納する。また、コントローラ２１は、暗号管理データ（２）の番号をコンテンツ管理ファイル２７１の例えばコンテンツ管理データ（２）２７１２に暗号管理データ番号として格納する。

【００４９】

また、暗号化情報ＢＩＤ［ＫＣ＋ＵＲ］をメモリカードＭＣへ格納すると、端末装置ＰＡの暗号化・復号化部１７は、記憶したいコンテンツＣをコンテンツ暗号鍵ＫＣで暗号化する（Ｓ３１０、図７のＥ６）。そして、コンテンツ暗号鍵ＫＣで暗号化したコンテンツＣの暗号化情報ＫＣ［Ｃ］をメモリインタフェース１６からメモリカードＭＣへ送る。メモリカードＭＣのコントローラ２１は、受信したコンテンツＣの暗号化情報ＫＣ［Ｃ］を公開Ｒ／Ｗ領域２７のコンテンツＢ（２７３Ｂ）へ格納する。また、コントローラ２１はこの格納処理と同時にコンテンツ名を生成して、コンテンツ管理ファイル２７１のコンテンツ管理データ（２）にコンテンツ名２７１ａとして格納する。

【００５０】

（メモリカードＭＣに記憶されたコンテンツを端末装置ＰＡで使用）

次に、コンテンツＣをメモリカードＭＣから読み出し、それを端末装置ＰＡにおいて使用する場合について述べる。なお、コンテンツＣを使用する場合においても、乱数値ＲＮＤをメモリカードＭＣから読み出す処理（図６のＳ２０６を得る処理）が先に実行されなければならないが、ここでもその説明は省略する。図８は、コンテンツＣをメモリカードＭＣから読み出し、端末装置ＰＡで使用する場合の処理手順と処理内容を示すシーケンス

図である。この図８において、処理Ｓ４０１～Ｓ４０４は、図７の処理Ｓ３０１～Ｓ３０４と同じ処理であるので、その説明は省略する。

【００５１】

次に、メモリカードＭＣのコントローラ２１は、端末装置ＰＡからの使用するコンテンツＣの読み出し要求に従い秘匿Ｒ／Ｗ領域２５の例えば暗号管理データ（２）２５１２からその要求に対応する例えば暗号管理データＢＩＤ［ＫＣ＋ＵＲ］を読み出す。そして、この読み出した情報ＢＩＤ［ＫＣ＋ＵＲ］をＳ４０２の相互認証処理（ＡＫＥ）によって生成した鍵情報ＫＴ１を用いて暗号化する（Ｓ４０５、図８のＥ１０）。そして、二重に暗号化が施された暗号化情報ＫＴ１［ＢＩＤ［ＫＣ＋ＵＲ］］がメモリカードＭＣからの応答として端末装置ＰＡへ送られる。

【００５２】

その後、端末装置ＰＡの暗号化・復号化部１７は、メモリカードＭＣから受信した暗号化情報ＫＴ１［ＢＩＤ［ＫＣ＋ＵＲ］］をＳ４０２の相互認証処理によって生成された鍵情報ＫＴ１を用いて一つ目の暗号を復号する（Ｓ４０６、図８のＤ３）。そして、Ｓ４０４で生成されたバインドキー（ＢＩＤ）を用いて更に二つ目の暗号を復号する（Ｓ４０７、図８のＤ２）。その後、暗号化・復号化部１７は復号された情報ＫＣ＋ＵＲをコンテンツ暗号鍵ＫＣとコンテンツ使用に関する情報ＵＲとにそれぞれ分ける（Ｓ４０８、図８のＰ'１）。

【００５３】

次に、端末装置ＰＡのユーザから使用するコンテンツのパスワードが入力されると、ＣＰＵ１１は、そのパスワードとＳ４０８で分けられた情報ＵＲの拡張部に記憶したパスワードとが一致するかの認証を行う（Ｓ４０９、図８の「認証」）。ここで、パスワードが一致せず認証出来なかった場合は、Ｓ４０８によって生成されたコンテンツ暗号鍵ＫＣが無効になるように処理される。

【００５４】

また、パスワードが一致し認証が完了した場合は、メモリカードＭＣの例えばコンテンツＢ（２７３Ｂ）から暗号化されたコンテンツＫＣ［Ｃ］が読み出され、端末装置ＰＡに送信される。そして、暗号化・復号化部１７はコンテンツＫＣ［Ｃ］をＳ４０８で得たコンテンツ暗号鍵ＫＣによって復号する（Ｓ４１０、図８のＤ６）。この復号により得られたコンテンツＣは、端末装置ＰＡ内のＲＡＭ１２に一旦保存され、その後、例えばデコーダ１４により復号された後、表示部１５に表示される。

【００５５】

本発明の第１の実施例によれば、追加ＩＤ（ＡＩＤ）を使用して著作権保護を行い、かつ追加ＩＤ（ＡＩＤ）のパスワードバインドを行う場合、その追加ＩＤ（ＡＩＤ）を直接操作しない方法で各コンテンツ毎にパスワードを設定できるため、よりセキュリティに強い著作権保護及びパスワードバインドを実現することができる。

【実施例２】

【００５６】

本発明の第２の実施の形態を、図面を用いて説明する。第２の実施の形態において、端末装置ＰＡ及びメモリカードＭＣの構造は第１の実施の形態と同じであるため、その説明を省略する。以下、本発明の第２の実施の形態のコンテンツの著作権保護処理動作を図９乃至図１２を用いて説明する。

【００５７】

（メモリカードＭＣに乱数値ＲＮＤを記憶）

まず、コンテンツを端末装置ＰＡからメモリカードＭＣに記憶する際、及びメモリカードＭＣに記憶されたコンテンツを使用する際に必要な乱数ＲＮＤを、メモリカードＭＣへ記憶する場合について述べる。図９は、その場合の端末装置ＰＡとメモリカードＭＣの処理手順と処理内容を示すシーケンス図である。

【００５８】

第２の実施形態の図９に示した処理Ｓ５０１～Ｓ５０２は、第１の実施形態の図５に示

した処理Ｓ１０１～Ｓ１０２と同じであるので、その説明は省略する。

【００５９】

そして、Ｓ５０２の相互認証が出来た場合、端末装置ＰＡのＣＰＵ１１は、ユーザから入力されたパスワード（ＰＩＮ）と、乱数発生部１８から発生された乱数値ＲＮＤとをコンテンツ使用に関する情報ＵＲの拡張部に記憶し（Ｓ５０３）、その情報ＵＲをＳ５０１で計算したＫＭ［ＭＩＤ］を用いて暗号化する（Ｓ５０４、図９のＥ２）。

【００６０】

次に、Ｓ５０４で暗号化された乱数値ＲＮＤ（ＭＩＤ［ＵＲ］）をＳ５０２の相互認証処理（ＡＫＥ）で生成された鍵情報ＫＴ１を用いて、更に暗号化する（Ｓ５０５、図９のＥ３）。そして、Ｓ５０５において二重に暗号化が施された情報ＫＴ１［ＭＩＤ［ＵＲ］］をメモリインタフェース１７からメモリカードＭＣへ送る。

【００６１】

メモリカードＭＣのコントローラ２１は、端末装置ＰＡから受信した暗号化情報ＫＴ１［ＭＩＤ［ＵＲ］］を、Ｓ５０２の相互認証処理（ＡＫＥ）で生成された鍵情報ＫＴ１を用いて復号する（Ｓ５０６、図９のＤ１０）。そして、一つ目の暗号が復号された暗号化情報ＭＩＤ［ＵＲ］を秘匿管理ファイル２５１の例えば暗号管理データ（１）２５１１として格納する。またコントローラ２１は、その暗号管理データ（１）の番号をコンテンツ管理ファイル２７１の例えばコンテンツ管理データ（１）２７１１に暗号管理データ番号２７１ｂとして格納する。

【００６２】

更に、上記の処理と並行して、端末装置ＰＡからメモリカードＭＣへコンテンツの代わりとなるダミー情報が送られ、メモリカードＭＣのコントローラ２１は、そのダミー情報を公開Ｒ／Ｗ領域２７のコンテンツＡ（２７３Ａ）へ格納する（Ｓ５０７）。

【００６３】

（乱数値ＲＮＤをメモリカードＭＣから読み出す）

次に、コンテンツを端末装置ＰＡからメモリカードＭＣに記憶する際、及びメモリカードＭＣに記憶されたコンテンツを使用する際に必要な乱数ＲＮＤを、メモリカードＭＣから読み出す場合について述べる。図１０は、その場合の端末装置ＰＡとメモリカードＭＣの処理手順と処理内容を示すシーケンス図である。

【００６４】

第２の実施形態の図１０に示した処理Ｓ６０１～Ｓ６０５は、第１の実施形態の図６に示した処理Ｓ２０１～Ｓ２０５と同じであるので、その説明は省略する。

【００６５】

処理Ｓ６０４及び処理Ｓ６０５により、二重に暗号化されていた情報ＫＴ１［ＭＩＤ［ＵＲ］］が復号された情報ＵＲが得られると、次に、ユーザから入力されたパスワード（ＰＩＮ）と情報ＵＲの拡張部に記憶されているパスワード（ＰＩＮ）とを比較して、認証を行う（Ｓ６０６、図１０の「認証」）。そして、この認証によりパスワード（ＰＩＮ）が一致しなかった場合は、処理Ｓ６０５によって復号された情報ＵＲの値を無効にする。

【００６６】

一方、パスワード（ＰＩＮ）が一致した場合には、情報ＵＲの拡張部に記憶されている乱数値ＲＮＤを取得する（Ｓ６０７）。この乱数値ＲＮＤはその後、コンテンツを記憶または使用される際に使用される。

【００６７】

（コンテンツを端末装置ＰＡからメモリカードＭＣに記憶）

次に、コンテンツを端末装置ＰＡからメモリカードＭＣに記憶する場合について述べる。なお、コンテンツをメモリカードＭＣに記憶する際においては、メモリカードＭＣから乱数値ＲＮＤを読み出す処理（図１０のＳ６０７を得る処理）が先に実行されなければならないが、ここでは図１０の処理が先に実行されているものとして説明する。図１１は、コンテンツを端末装置ＰＡからメモリカードＭＣに記憶する場合の処理手順と処理内容を示すシーケンス図である。

【００６８】
第２の実施形態の図１１に示した処理Ｓ７０１～Ｓ７０４は、第１の実施形態の図７に示した処理Ｓ３０１～Ｓ３０４と同じであるので、その説明は省略する。
【００６９】
処理Ｓ７０４でバインドキー（ＢＩＤ）を生成する処理と並行して、端末装置のＣＰＵ１１は記憶したいコンテンツの暗号鍵ＫＣと、コンテンツ使用に関する情報ＵＲとを統合する（Ｓ７０５、図１１のＰ１）。そして、暗号化・復号化部１７は、Ｓ７０５で統合された情報（ＫＣ＋ＵＲ）をＳ７０４で生成されたバインドキーＢＩＤによって暗号化する（Ｓ７０６、図１１のＥ２）。暗号化・復号化部１７は更に、Ｓ７０６で生成した暗号化情報ＢＩＤ［ＫＣ＋ＵＲ］を、Ｓ７０２で生成された鍵情報ＫＴ１によって更に暗号化する（Ｓ７０７、図１１のＥ３）。そして、ここで生成二重に暗号化が施された暗号化情報ＫＴ１［ＢＩＤ［ＫＣ＋ＵＲ］］は、暗号化・復号化部１７からメモリカードＭＣへ送られる。
【００７０】
メモリカードＭＣのコントローラ２１は、端末装置ＰＡから送られた暗号化情報ＫＴ１［ＢＩＤ［ＫＣ＋ＵＲ］］をＳ７０２で生成した鍵情報ＫＴ１を用いて一つ目に暗号を復号する（Ｓ７０８、図１１のＤ１０）。そして、Ｓ７０８で復号された暗号化情報ＢＩＤ［ＫＣ＋ＵＲ］を秘匿管理ファイル２５１の例えば暗号管理データ（２）２５１２に格納する。また、コントローラ２１は、暗号管理データ（２）の番号をコンテンツ管理ファイル２７１の例えばコンテンツ管理データ（２）２７１２に暗号管理データ番号として格納する。
【００７１】
また、暗号化情報ＢＩＤ［ＫＣ＋ＵＲ］をメモリカードＭＣへ格納すると、端末装置ＰＡの暗号化・復号化部１７は、記憶したいコンテンツＣをコンテンツ暗号鍵ＫＣで暗号化する（Ｓ７０９、図１１のＥ６）。そして、コンテンツ暗号鍵ＫＣで暗号化したコンテンツＣの情報ＫＣ［Ｃ］をメモリインタフェース１６からメモリカードＭＣへ送る。メモリカードＭＣのコントローラ２１は、受信したコンテンツＣの暗号化情報ＫＣ［Ｃ］を公開Ｒ／Ｗ領域２７のコンテンツＢ（２７３Ｂ）へ格納する。また、コントローラ２１はこの格納処理と同時にコンテンツ名を生成して、コンテンツ管理ファイル２７１のコンテンツ管理データ（２）２７１２にコンテンツ名２７１ａとして格納する。
【００７２】
（メモリカードＭＣに記憶されたコンテンツを端末装置ＰＡで使用）
次に、コンテンツＣをメモリカードＭＣから読み出し、それを端末装置ＰＡにおいて使用する場合について述べる。なお、コンテンツを使用する場合においても、乱数値ＲＮＤをメモリカードＭＣから読み出す処理（図１０のＳ６０７を得る処理）が先に実行されなければならないが、ここでもその説明は省略する。図１２は、コンテンツをメモリカードＭＣから読み出し、端末装置ＰＡで使用する場合の処理手順と処理内容を示すシーケンス図である。
【００７３】
第２の実施形態の図１２に示した処理Ｓ８０１～Ｓ８０７は、第１の実施形態の図８に示した処理Ｓ４０１～Ｓ４０７と同じであるので、その説明は省略する。
【００７４】
処理Ｓ８０７及び処理Ｓ８０６により、二重に暗号化されていた情報ＫＴ１［ＢＩＤ［ＫＣ＋ＵＲ］］が復号された情報（ＫＣ＋ＵＲ）が得られると、暗号化・復号化部１７はコンテンツ暗号鍵ＫＣとコンテンツ使用に関する情報ＵＲとにそれぞれ分ける（Ｓ８０８、図１２のＰ'１）。
【００７５】
次に、端末装置ＰＡの暗号化・復号化部１７は、メモリカードＭＣの例えばコンテンツＢ（２７３Ｂ）から暗号化されたコンテンツＫＣ［Ｃ］を受信すると、コンテンツ暗号鍵ＫＣによって復号する（Ｓ８０９、図１２のＤ６）。この復号により得られたコンテンツ

Ｃは、端末装置ＰＡ内のＲＡＭ１２に一旦保存され、その後、例えばデコーダ１４により復号された後、表示部１５に表示される。

【００７６】

以上の第２の実施例によると、例えば、３つのコンテンツの記憶を行う場合、メモリカードＭＣの秘匿Ｒ／Ｗ領域２５の秘匿管理ファイル２５１、及び公開Ｒ／Ｗ領域２７は次のようになる。

【００７７】

図１３（Ａ）は３つのコンテンツをメモリカードＭＣへ記憶した場合における秘匿管理ファイル２５１のブロック図の一例である。まず秘匿管理ファイル２５１には、ＭＩＤでバインドされた情報ＵＲが格納され、その情報ＵＲの拡張部には乱数値ＲＮＤ及びパスワード（ＰＩＮ）が記憶されている（図１３（Ａ）の２５１１）。そして、その下にそれぞれ３つのコンテンツの暗号化された解読鍵ＢＩＤ［ＫＣ１＋ＵＲ１］～ＢＩＤ［ＫＣ３＋ＵＲ３］がそれぞれ格納されている。

【００７８】

また図１３（Ｂ）は、３つのコンテンツを記憶した場合の公開Ｒ／Ｗ領域２７のブロック図の一例である。図１３（Ｂ）のように、コンテンツ管理ファイル２７１やバインド管理ファイル２７２が記憶されており、更にダミーファイル２７３Ａや、コンテンツ１乃至３が記憶されている。

【００７９】

なお、以上の第２の実施例では、図１３（Ａ）、（Ｂ）のように１つのメモリカードＭＣに対し、それぞれのコンテンツを１つの乱数ＲＮＤ、１つのパスワード（ＰＩＮ）を用いてバインドしたが、これに限定されることなく図１３（Ｃ）、（Ｄ）のように、ディレクトリ毎に乱数値ＲＮＤおよびパスワード（ＰＩＮ）を設定して、パスワードバインドを実現するなど、数々の応用が可能である。

【００８０】

本発明の第２の実施例によれば、追加ＩＤ（ＡＩＤ）を使用して著作権保護を行い、かつＡＩＤのパスワードバインドを行う場合、ＡＩＤを直接操作しない方法でカード毎またはディレクトリ毎にパスワードを設定できるため、よりセキュリティに強い著作権保護・パスワードバインドを行うことができる。

【図面の簡単な説明】

【００８１】

【図１】本発明の実施の形態に係る端末装置ＰＡの回路構成を示すブロック図。

【図２】本発明の実施の形態に係るメモリカードＭＣの構成を示すブロック図。

【図３】本発明の実施の形態に係るメモリカードＭＣの秘匿領域の構成と記憶データのフォーマットの一例を示す図。

【図４】本発明の実施の形態に係るメモリカードＭＣの公開Ｒ／Ｗ領域の構成と記憶データフォーマットの一例を示す図。

【図５】実施例１における乱数値をメモリカードＭＣへ記憶する処理手順を示したシーケンス図。

【図６】実施例１における乱数値をメモリカードＭＣから読み出す処理手順を示したシーケンス図。

【図７】実施例１におけるコンテンツを端末装置ＰＡからメモリカードＭＣへ記憶する処理手順を示したシーケンス図。

【図８】実施例１におけるコンテンツをメモリカードＭＣから呼び出して、端末装置ＰＡで使用する処理手順を示したシーケンス図。

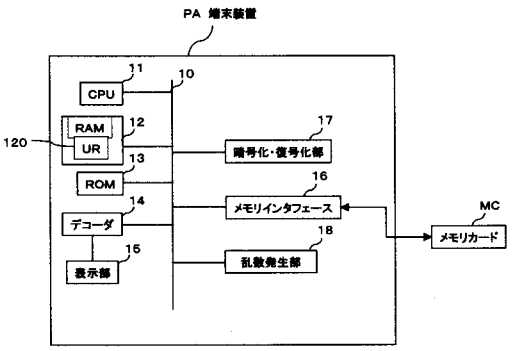
【図９】実施例２における乱数値をメモリカードＭＣへ記憶する処理手順を示したシーケンス図。

【図１０】実施例２における乱数値をメモリカードＭＣから読み出す処理手順を示したシーケンス図。

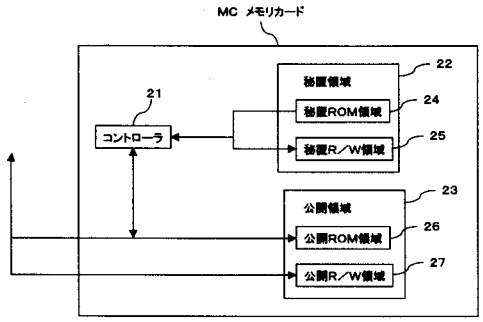
【図１１】実施例２におけるコンテンツを端末装置ＰＡからメモリカードＭＣへ記憶する

処理手順を示したシーケンス図。
【図１２】実施例２におけるコンテンツをメモリカードＭＣから呼び出して、端末装置ＰＡで使用する処理手順を示したシーケンス図。
【図１３】実施例２において、コンテンツを３つ記憶する場合の秘匿管理ファイル２５１及び公開Ｒ／Ｗ領域２７の一例を示した図。
【符号の説明】
【００８２】
１０　バス
１１　ＣＰＵ
１２　ＲＡＭ
１３　ＲＯＭ
１４　デコーダ
１５　表示部
１６　メモリインタフェース
１７　暗号化・復号化部
１８　乱数発生部
２１　コントローラ
２２　秘匿領域
２３　公開領域
２４　秘匿ＲＯＭ領域
２５　秘匿Ｒ／Ｗ領域
２６　公開ＲＯＭ領域
２７　公開Ｒ／Ｗ領域

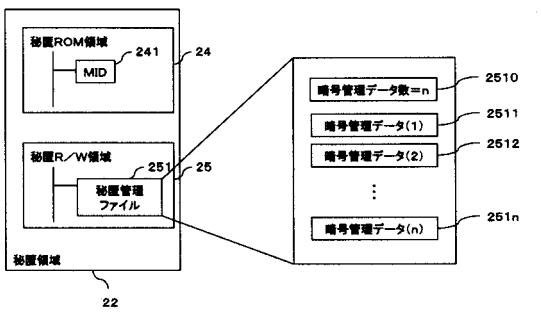
【図１】



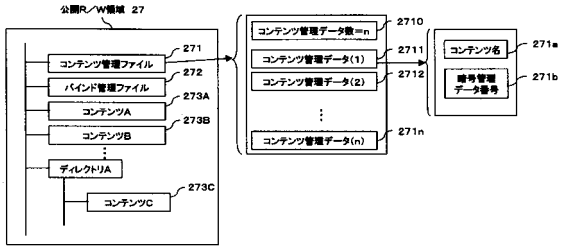
【図２】



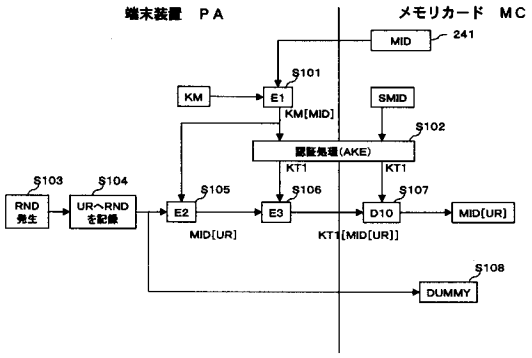
【図３】



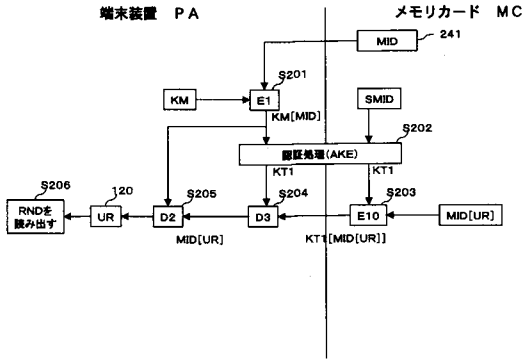
【図４】



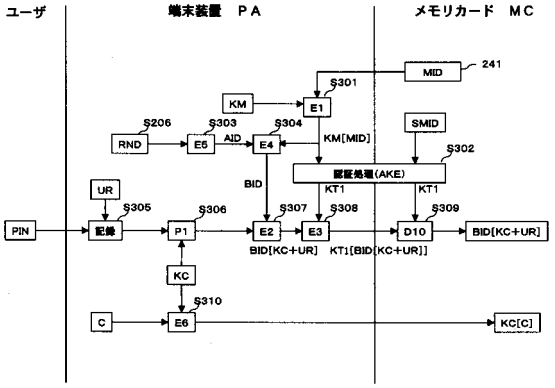
【図５】



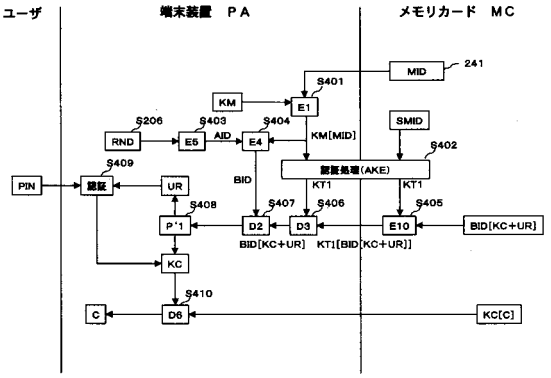
【図６】



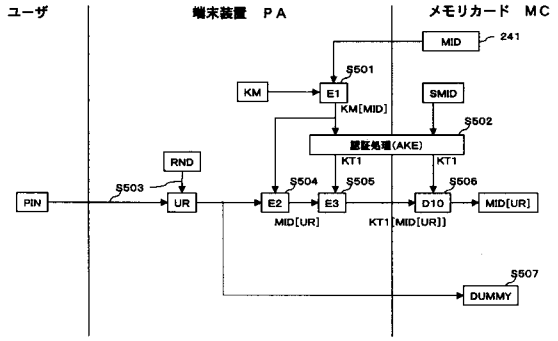
【図７】



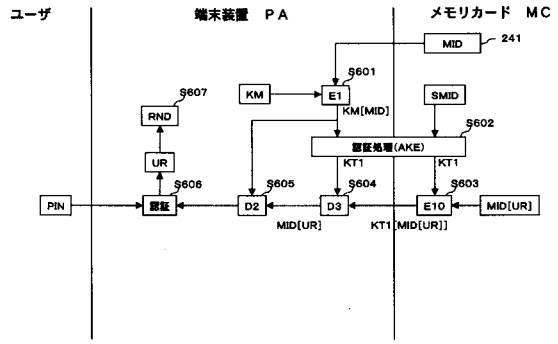
【図８】



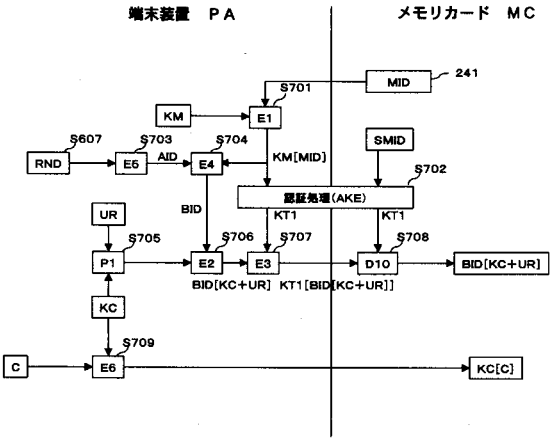
【図９】



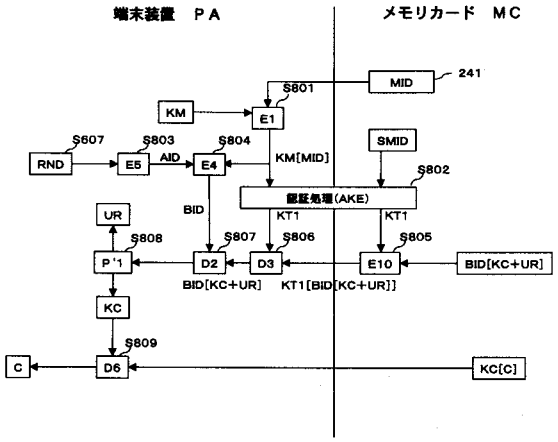
【図１０】



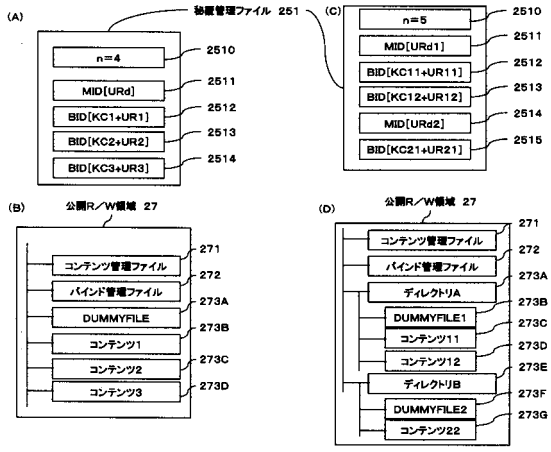
【図１１】



【図１２】


端末装置 PA
メモリカード MC
MID
241
S801
KM
E1
S607
S803
S804
SMID
RND
E5
AID
E4
KM[MID]
S802
認証処理(AKE)
BID
KT1
KT1
UR
S808
S807
S806
S805
P'1
D2
D3
E10
BID[KC+UR]
BID[KC+UR]
KT1[BID[KC+UR]]
KC
S809
C
D6
KC[C]

【図１３】


(A)
秘匿管理ファイル 251
n=4
2510
MID[URd]
2511
BID[KC1+UR1]
2512
BID[KC2+UR2]
2513
BID[KC3+UR3]
2514
(C)
n=5
2510
MID[URd1]
2511
BID[KC11+UR11]
2512
BID[KC12+UR12]
2513
MID[URd2]
2514
BID[KC21+UR21]
2515
(B)
公開R／W領域 27
コンテンツ管理ファイル
271
バインド管理ファイル
272
DUMMYFILE
273A
コンテンツ1
273B
コンテンツ2
273C
コンテンツ3
273D
(D)
公開R／W領域 27
コンテンツ管理ファイル
271
バインド管理ファイル
272
ディレクトリA
273A
DUMMYFILE1
273B
コンテンツ11
273C
コンテンツ12
273D
ディレクトリB
273E
DUMMYFILE2
273F
コンテンツ22
273G

フロントページの続き

【要約の続き】
、メモリカードＭＣに記憶する。
【選択図】　図７