(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2013-243667
(P2013-243667A)
(43)公開日　平成25年12月5日(2013.12.5)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/08	(2006.01)	H04L	9/00	601B	5J104
G06F 21/62	(2013.01)	H04L	9/00	601E	
		G06F	21/24	166C	

審査請求 未請求　請求項の数 31　OL　（全 35 頁）

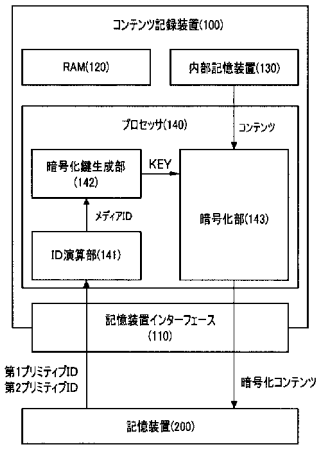
(21)出願番号　特願2013-103826 (P2013-103826)
(22)出願日　平成25年5月16日 (2013.5.16)
(31)優先権主張番号　10-2012-0052576
(32)優先日　平成24年5月17日 (2012.5.17)
(33)優先権主張国　韓国 (KR)

(71)出願人　390019839
三星電子株式会社
Ｓａｍｓｕｎｇ　Ｅｌｅｃｔｒｏｎｉｃｓ　Ｃｏ．，Ｌｔｄ．
大韓民国京畿道水原市霊通区三星路１２９　１２９，Ｓａｍｓｕｎｇ－ｒｏ，Ｙｅｏｎｇｔｏｎｇ－ｇｕ，Ｓｕｗｏｎ－ｓｉ，Ｇｙｅｏｎｇｇｉ－ｄｏ，Ｒｅｐｕｂｌｉｃ　ｏｆ　Ｋｏｒｅａ
(74)代理人　100089037
弁理士　渡邊　隆
(74)代理人　100110364
弁理士　実広　信哉

最終頁に続く

(54)【発明の名称】記憶装置の識別子を基盤とするコンテンツの暗復号化装置及び方法

(57)【要約】
【課題】暗号化コンテンツが他の記録装置に無断複製されることを防止する暗号化方法及び装置を提供する。
【解決手段】本発明によるコンテンツ記憶装置は、記録装置に備えられた第１パート及び第２パートそれぞれを識別するための第１プリミティブＩＤ及び第２プリミティブＩＤを前記記憶装置から提供される記憶装置インターフェースと、前記第１プリミティブＩＤ及び第２プリミティブＩＤを用いて前記記憶装置の固有識別子であるメディアＩＤを生成し、前記メディアＩＤを用いて生成した暗号化鍵でコンテンツを暗号化するプロセッサとを含み、前記記憶装置インターフェースは、前記プロセッサによって暗号化したコンテンツを前記記憶装置に提供する。
【選択図】図２



【特許請求の範囲】
【請求項１】
記憶装置に備えられた第１パート及び第２パートそれぞれを識別するための第１プリミティブＩＤ及び第２プリミティブＩＤを前記記憶装置から提供される記憶装置インターフェースと、
前記第１プリミティブＩＤ及び第２プリミティブＩＤを用いて前記記憶装置の固有識別子であるメディアＩＤを生成し、前記メディアＩＤを用いて生成した暗号化鍵でコンテンツを暗号化するプロセッサと
を含み、
前記記憶装置インターフェースは、前記プロセッサによって暗号化したコンテンツを前記記憶装置に提供するコンテンツ記録装置。
【請求項２】
前記第１プリミティブＩＤは、前記記憶装置に備えられたコントローラの固有識別子であるコントローラＩＤであり、
前記第２プリミティブＩＤは、前記記憶装置に備えられたメモリ装置の固有識別子であるメモリＩＤを暗号化した暗号化メモリＩＤである請求項１に記載のコンテンツ記録装置。
【請求項３】
前記プロセッサは、
前記メモリ暗号化ＩＤを復号化して前記メモリＩＤを取得し、前記メモリＩＤを用いて前記メディアＩＤ生成に用いるメモリ装置の他の固有識別子であるメモリ派生ＩＤを生成し、前記コントローラＩＤ及び前記メモリ派生ＩＤを用いて前記メディアＩＤを演算するＩＤ演算部と、
前記メディアＩＤを用いて前記暗号化鍵を生成する暗号化鍵生成部と、
前記暗号化鍵で前記コンテンツを暗号化する暗号化部と
を含む請求項２に記載のコンテンツ記録装置。
【請求項４】
前記記憶装置インターフェースは、前記記憶装置から第１認証情報をさらに提供され、
前記プロセッサは、
前記暗号化メモリＩＤを復号化して前記メモリＩＤを生成し、前記メモリＩＤを用いて第２認証情報を生成する認証情報生成部と、
前記第１認証情報と前記第２認証情報が一致すると、前記メモリＩＤを用いて前記メモリ派生ＩＤを演算する派生ＩＤ生成部と
を含む請求項２に記載のコンテンツ記録装置。
【請求項５】
前記プロセッサは、
前記派生ＩＤ演算部によって演算された前記メモリ派生ＩＤ及び前記コントローラＩＤのうち少なくとも一つを用いて前記メディアＩＤを演算するＩＤ演算部をさらに含む請求項４に記載のコンテンツ記録装置。
【請求項６】
前記記憶装置インターフェースは、前記記憶装置と前記コンテンツ記録装置との間の公開鍵基盤の相互認証をするための第３認証情報をさらに提供され、
前記プロセッサは、
前記第３認証情報を用いて前記相互認証を行い、前記第３認証情報から前記コントローラＩＤを取得する相互認証部と、
前記派生ＩＤ演算部によって演算された前記メモリ派生ＩＤ及び前記相互認証部によって取得された前記コントローラＩＤのうち少なくとも一つを用いて前記メディアＩＤを演算するＩＤ演算部と
をさらに含む請求項４に記載のコンテンツ記録装置。
【請求項７】

前記記憶装置インターフェースは、前記暗号化鍵の生成に用いるランダムナンバーを前記記憶装置にさらに提供する請求項１に記載のコンテンツ記録装置。
【請求項８】
前記プロセッサは、
前記プリミティブ識別子を用いて前記記憶装置の固有識別子を演算するＩＤ演算部と、
前記ランダムナンバーを生成するランダムナンバー生成部と、
前記固有識別子及び前記ランダムナンバーを用いて前記暗号化鍵を生成する暗号化鍵生成部と、
前記暗号化鍵で前記コンテンツを暗号化する暗号化部と、
を含む請求項７に記載のコンテンツ記録装置。
【請求項９】
前記暗号化鍵生成部は、ＣＭＡＣアルゴリズムに前記固有識別子及び前記ランダムナンバーを入力して前記暗号化鍵を生成する請求項８に記載のコンテンツ記録装置。
【請求項１０】
前記記憶装置インターフェースは、前記暗号化鍵の生成に前記メディアＩＤと共に用いる前記コンテンツの識別子を前記記憶装置にさらに提供する請求項１に記載のコンテンツ記録装置。
【請求項１１】
前記プロセッサは、一つの入力パラメータ及び一つの出力を有する所定のルーチンに前記メディアＩＤを前記入力パラメータに設定して前記ルーチンを実行し、その結果として出力データを前記暗号化鍵として用いる請求項１に記載のコンテンツ記録装置。
【請求項１２】
前記ルーチンは、一方向性関数である請求項１１に記載のコンテンツ記録装置。
【請求項１３】
メディアＩＤを用いて生成した復号化鍵で復号化する暗号化コンテンツ及びプリミティブＩＤを格納するメモリ装置と、
前記メモリ装置を制御するコントローラと、
を含み、
前記プリミティブＩＤは、前記コントローラの固有識別子であるコントローラＩＤ及び前記メモリ装置の固有識別子であるメモリＩＤを暗号化した暗号化メモリＩＤを含み、
前記メディアＩＤは、前記メモリ装置及び前記コントローラを含む記憶装置の固有識別子であり、前記メモリＩＤを用いて生成したメモリ派生ＩＤ及び前記コントローラＩＤを用いて生成される記憶装置。
【請求項１４】
前記メモリ装置は、前記メモリＩＤを第１領域に、前記暗号化コンテンツを前記第１領域と異なる第３領域にそれぞれ格納し、
前記第１領域は、前記第３領域に対するアクセス方法によってはアクセスでされない領域である請求項１３に記載の記憶装置。
【請求項１５】
前記メモリ装置は、前記コントローラＩＤ及び前記暗号化メモリＩＤを前記第１領域及び第３領域と異なる第２領域に格納し、
前記第２領域は、読み取り専用アクセスのみ可能な領域である請求項１４に記載の記憶装置。
【請求項１６】
前記メモリ装置は、前記復号化鍵を格納しない請求項１３に記載の記憶装置。
【請求項１７】
前記メモリ装置は、前記復号化鍵の生成に用いるランダムナンバーをさらに格納する請求項１３に記載の記憶装置。
【請求項１８】
前記メモリ装置は、前記復号化鍵の生成に用いるコンテンツ識別子をさらに格納する請

求項１３に記載の記憶装置。
【請求項１９】
記憶装置から前記記憶装置に格納された暗号化コンテンツと前記記憶装置に備えられた第１パート及び第２パートそれぞれを識別するための第１プリミティブＩＤ及び第２プリミティブＩＤを提供される記憶装置インターフェースと、
前記第１プリミティブＩＤ及び第２プリミティブＩＤを用いて前記記憶装置の固有識別子であるメディアＩＤを生成し、前記メディアＩＤを用いて生成した復号化鍵で前記暗号化コンテンツを復号化して再生するプロセッサと、
を含むコンテンツ再生装置。
【請求項２０】
前記第２プリミティブＩＤは、前記記憶装置に備えられたメモリ装置の固有識別子であるメモリＩＤを暗号化した暗号化メモリＩＤであり、
前記プロセッサは、前記暗号化メモリＩＤを用いて前記コンテンツ再生装置と前記記憶装置との間の第１認証のための第２認証情報を生成する請求項１９に記載のコンテンツ再生装置。
【請求項２１】
前記記憶装置インターフェースは、前記第１認証のための第１認証情報を前記記憶装置からさらに提供され、
前記プロセッサは、前記第１認証情報及び前記第２認証情報を比較し、二つの認証情報が一致する場合に限り、前記メディアＩＤを生成する請求項２０に記載のコンテンツ再生装置。
【請求項２２】
前記第１プリミティブＩＤは、前記記憶装置に備えられたコントローラの固有識別子であるコントローラＩＤであり、
前記記憶装置インターフェースは、前記コンテンツ再生装置と前記記憶装置との間の第２認証のための第３認証情報を前記記憶装置から提供され、前記第３認証情報は、前記コントローラＩＤを含む請求項１９に記載のコンテンツ再生装置。
【請求項２３】
前記記憶装置インターフェースは、前記記憶装置から前記記憶装置に格納されたランダムナンバーをさらに提供され
前記プロセッサは、前記メディアＩＤ及び前記ランダムナンバーをＣＭＡＣアルゴリズムに入力して前記復号化鍵を生成する請求項１９に記載のコンテンツ再生装置。
【請求項２４】
前記記憶装置インターフェースは、前記記憶装置から前記記憶装置に格納されたコンテンツ識別子をさらに提供され
前記プロセッサは、前記メディアＩＤ及び前記コンテンツ識別子をＣＭＡＣアルゴリズムに入力して前記復号化鍵を生成する請求項１９に記載のコンテンツ再生装置。
【請求項２５】
第１記憶装置に接続され、前記第１記憶装置に格納された暗号化コンテンツと前記第１記憶装置に備えられた第１パート及び第２パートそれぞれを識別するための第１プリミティブＩＤ及び第２プリミティブＩＤを提供される記憶装置インターフェースと、
前記第１プリミティブＩＤ及び第２プリミティブＩＤを用いて前記第１記憶装置の固有識別子の第１メディアＩＤを生成し、前記第１メディアＩＤを用いて生成した復号化鍵で前記暗号化コンテンツを復号化することを試みた結果、復号化を失敗するプロセッサと
を含み、
前記第１記憶装置に格納された暗号化コンテンツは、前記第１記憶装置と異なる第２記憶装置の固有識別子の第２メディアＩＤを用いて生成した暗号化鍵で暗号化されるコンテンツ再生装置。
【請求項２６】
第１端末からコンテンツ及びメモリＩＤを用いて生成したメモリ派生ＩＤを提供される

受信部であって、前記メモリＩＤは、前記第１端末に接続された記憶装置に備えられたメモリ装置の固有な識別子である、受信部と、
格納部と、
前記メモリ派生ＩＤを用いて前記コンテンツを暗号化し、暗号化したコンテンツを前記格納部に格納する暗号化部と、
前記格納部に格納された前記暗号化したコンテンツを第２端末に送信する送信部と、
を含み、
前記第１端末と前記第２端末は一つの端末グループに属するコンテンツ記憶サーバ。
【請求項２７】
前記格納部は、前記コンテンツは記憶せず、前記暗号化したコンテンツのみ格納する請求項２６に記載のコンテンツ記憶サーバ。
【請求項２８】
前記暗号化部は、前記メモリ派生ＩＤ及びサーバセキュリティ鍵を用いて生成した暗号化鍵を用いて前記コンテンツを暗号化する請求項２６に記載のコンテンツ記憶サーバ。
【請求項２９】
前記送信部は、前記第２端末に前記暗号化したコンテンツ及び前記暗号化したコンテンツの復号化鍵を送信する請求項２６に記載のコンテンツ記憶サーバ。
【請求項３０】
前記暗号化したコンテンツは、前記記憶装置に接続された前記第２端末によって復号化される請求項２６に記載のコンテンツ記憶サーバ。
【請求項３１】
前記コンテンツ記憶サーバは、前記暗号化したコンテンツを、前記メモリ派生ＩＤを用いて復号化し、復号化したコンテンツを前記送信部に提供した後に削除する復号化部をさらに含み、
前記送信部は、前記第２端末に前記復号化したコンテンツを送信する請求項２６に記載のコンテンツ記憶サーバ。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、コンテンツの暗号化装置及び方法とこれに対応する復号化装置及び方法に関するものである。より詳細には、記憶装置に暗号化したコンテンツを格納し、前記コンテンツの無断複製及び再生などを防止することにおいて、前記コンテンツを暗号化及び復号化するための鍵生成に前記記憶装置の固有識別子を用いる装置及び方法に関するものである。
【背景技術】
【０００２】
近年様々な形態の移動式記憶装置が紹介されている。最近の移動式記憶装置は、大容量化、小型化の傾向にある。移動式記憶装置のインターフェースは、ホスト装置からの取り外しが可能な方式で実現されており、移動式記憶装置の利便性がさらに高まっている。例えば、フラッシュメモリを記憶手段として用いるメモリカードまたはＵＳＢ（Ｕｎｉｖｅｒｓａｌ　Ｓｅｒｉａｌ　Ｂｕｓ）ポートに接続可能なＵＳＢメモリが紹介されており、最近ではＳＳＤ（Ｓｏｌｉｄ　Ｓｔａｔｅ　Ｄｒｉｖｅ）の登場により次代に広く使われている。また、安価な記憶装置の一つとして評価されるハードディスクも外装型ハードディスクが登場し、従来の固定式ハードディスクとは異なって移動性を提供する。
【０００３】
前記移動式記憶装置だけではなく、前記移動式記憶装置に接続できるホスト装置も小型化されている。このように、いつ、いかなる所でも移動式記憶装置に格納したデジタルコンテンツは移動式ホスト装置を介して楽しめる環境が整えられており、コンテンツの流通方式はデジタルデータの形態で流通するものに変化しつつある。これに伴い、デジタルコンテンツの不正コピーを防止する技術の重要性はさらに高まっている。

【０００４】
デジタルコンテンツの不正コピーを防止するため、前記デジタルコンテンツは原本そのままではなく暗号化した状態で移動式記憶装置に格納した方が好ましい。前記暗号化には特定暗号化鍵を用いて行う。
【０００５】
例えば、対称型暗号化技術を用いてコンテンツを暗号化する場合、前記暗号化鍵は復号化鍵としても用いることができる。したがって、前記暗号化鍵が流出した場合、暗号化したコンテンツと暗号化鍵が同時に配布されると誰でも暗号化したコンテンツを復号化して再生できる。したがって、暗号化したコンテンツと暗号化鍵が同時に配布されても復号化できないように、前記暗号化したコンテンツが前記許可された記憶装置以外の記憶装置に不正コピーされる場合、復号化できないようにする暗号化及び復号化方法の提供が要求される。
【発明の概要】
【発明が解決しようとする課題】
【０００６】
本発明が解決しようとする技術的課題は、記憶装置の識別子を、前記記憶装置に格納されるコンテンツの暗号化鍵として用いるか、または前記識別子を用いて前記暗号化鍵を生成するコンテンツの暗復号化方法及び装置を提供するものである。
【０００７】
本発明が解決しようとする別の技術的課題は、記憶装置の識別子を、前記記憶装置に格納されるコンテンツの暗号化鍵として用いることにおいて、前記記憶装置の識別子が流出しないようにするコンテンツ記録装置及び方法を提供するものである。
【０００８】
本発明が解決しようとするさらに別の技術的課題は、記憶装置の識別子を、前記記憶装置に格納された暗号化コンテンツの復号化鍵として用いるコンテンツ再生装置及び方法を提供するものである。
【０００９】
本発明が解決しようとするさらに別の技術的課題は、記憶装置の識別子を、前記記憶装置に格納された暗号化コンテンツの復号化鍵として用いることにおいて、前記記憶装置の識別子が流出しないようにするコンテンツ記録装置及び方法を提供するものである。
【００１０】
本発明が解決しようとする技術的課題は、記憶装置の識別子を前記記憶装置に格納されるコンテンツの暗号化鍵として用い、前記識別子を用いて前記記憶装置に格納された暗号化コンテンツを復号化するコンテンツ暗復号化装置を提供するものである。
【００１１】
本発明の技術的課題は、以上で言及した技術的課題に限定されず、言及されていないその他の技術的課題は、次の記載から当業者に明確に理解されるものである。
【課題を解決するための手段】
【００１２】
前記技術的課題を達成するための本発明の一実施態様によるコンテンツ記録装置は、前記記憶装置から記憶装置に備えられた第１パート及び第２パートそれぞれを識別するための第１プリミティブＩＤ及び第２プリミティブＩＤを提供される記憶装置インターフェースと、前記第１プリミティブＩＤ及び第２プリミティブＩＤを用いて前記記憶装置の固有識別子であるメディアＩＤを生成し、前記メディアＩＤを用いて生成した暗号化鍵でコンテンツを暗号化するプロセッサとを含む。前記記憶装置インターフェースは、前記プロセッサによって暗号化したコンテンツを前記記憶装置に提供する。
【００１３】
前記技術的課題を達成するための本発明の別の実施態様による記憶装置は、メディアＩＤを用いて生成した復号化鍵で復号化する暗号化コンテンツ及びプリミティブＩＤを格納するメモリ装置と、前記メモリ装置を制御するコントローラと、を含む。前記プリミティ

ブＩＤは、前記コントローラの固有識別子であるコントローラＩＤ及び前記メモリ装置の固有識別子であるメモリＩＤを暗号化した暗号化メモリＩＤを含み、前記メディアＩＤは、前記メモリ装置及び前記コントローラを含む記憶装置の固有識別子であり、前記メモリＩＤを用いて生成したメモリ派生ＩＤ及び前記コントローラＩＤを用いて生成したものである。

【００１４】

前記技術的課題を達成するための本発明のさらに別の実施態様によるコンテンツ再生装置は、記憶装置から前記記憶装置に格納された暗号化コンテンツと前記記憶装置に備えられた第１パート及び第２パートそれぞれを識別するための第１プリミティブＩＤ及び第２プリミティブＩＤを提供される記憶装置インターフェースと、前記第１プリミティブＩＤ及び第２プリミティブＩＤを用いて前記記憶装置の固有識別子であるメディアＩＤを生成し、前記メディアＩＤを用いて生成した復号化鍵で前記暗号化コンテンツを復号化して再生するプロセッサと、を含む。

【００１５】

前記技術的課題を達成するための本発明のさらに別の実施態様によるコンテンツ再生装置は、第１記憶装置に接続され、前記第１記憶装置に格納された暗号化コンテンツと前記第１記憶装置に備えられた第１パート及び第２パートそれぞれを識別するための第１プリミティブＩＤ及び第２プリミティブＩＤを提供される記憶装置インターフェースと、前記第１プリミティブＩＤ及び第２プリミティブＩＤを用いて前記第１記憶装置の固有識別子の第１メディアＩＤを生成し、前記第１メディアＩＤを用いて生成した復号化鍵で前記暗号化コンテンツの復号化を試みた結果、復号化を失敗するプロセッサとを含む。前記第１記憶装置に格納された暗号化コンテンツは、前記第１記憶装置と異なる第２記憶装置の固有識別子の第２メディアＩＤを用いて生成した暗号化鍵で暗号化される。

【００１６】

前記技術的課題を達成するための本発明のさらに別の実施態様によるコンテンツ記憶サーバは、第１端末からコンテンツ及びメモリＩＤを用いて生成したメモリ派生ＩＤを提供される受信部であって、前記メモリＩＤは、前記第１端末に接続された記憶装置に備えられたメモリ装置の固有な識別子である、受信部と、格納部と、前記メモリ派生ＩＤを用いて前記コンテンツを暗号化し、暗号化したコンテンツを前記格納部に格納する暗号化部と、前記格納部に格納された前記暗号化したコンテンツを第２端末に送信する送信部と、を含む。前記第１端末と前記第２端末は一つの端末グループに属する。

【００１７】

前記技術的課題を達成するための本発明のさらに別の実施態様によるコンテンツ暗号化記憶方法は、記憶装置から前記記憶装置に格納されたプリミティブＩＤを提供され、前記プリミティブＩＤから前記記憶装置の固有識別子であるメディアＩＤを演算し、前記メディアＩＤを用いて暗号化鍵を生成し、前記暗号化鍵を用いてコンテンツを暗号化することによって暗号化コンテンツを生成し、前記暗号化コンテンツが前記記憶装置に格納されるように、前記暗号化コンテンツを前記記憶装置に提供することを含む。

【００１８】

前記技術的課題を達成するための本発明のさらに別の実施態様によるコンテンツ復号化方法は、記憶装置から前記記憶装置に格納されたプリミティブＩＤを提供され、前記プリミティブＩＤから前記記憶装置の固有識別子であるメディアＩＤを演算し、前記記憶装置に格納された暗号化コンテンツを提供され、前記メディアＩＤを用いてコンテンツ復号化鍵を生成し、前記コンテンツ復号化鍵を用いて前記暗号化コンテンツを復号化することを含む。

【００１９】

前記技術的課題を達成するための本発明のさらに別の態様によるコンピュータで読み取り可能な記録媒体は、前記コンテンツ暗号化／復号化方法を実行するためのコンピュータプログラムを格納する。

【発明の効果】

【００２０】
前記本発明によれば、記憶装置に格納された暗号化コンテンツを復号化するための復号化鍵は前記記憶装置の識別子から求められるものであり、前記記憶装置の識別子は復号化時点で前記記憶装置から求めなければならないため、暗号化コンテンツを他の記憶装置に無断複製されても復号化できない効果がある。
【００２１】
すなわち、特定暗号化コンテンツを特定記憶装置に格納されているときのみ復号化できるようにし、特定暗号化コンテンツの復号化鍵が流出しても他の記憶装置では前記流出した復号化鍵を利用できないようにする効果がある。
【図面の簡単な説明】
【００２２】
【図１】本発明の一実施形態によるコンテンツ暗復号化システムの構成図である。
【図２】本発明の一実施形態によるコンテンツ記録装置の構成図である。
【図３】本発明の一実施形態によるコンテンツ記録装置の構成図である。
【図４】本発明の一実施形態によるコンテンツ記録装置の構成図である。
【図５】本発明の一実施形態による記憶装置の構成図である。
【図６】本発明の一実施形態によるコンテンツ再生装置の構成図である。
【図７】本発明の一実施形態による記憶装置の構成図である。
【図８】本発明の一実施形態による記憶装置の構成図である。
【図９】本発明の一実施形態によるコンテンツ暗復号化システムの動作を説明するための図である。
【図１０】本発明の一実施形態によるコンテンツ暗復号化システムの動作を説明するための図である。
【図１１】本発明の一実施形態によるコンテンツ暗復号化システムの動作を説明するための図である。
【図１２】本発明の一実施形態によるコンテンツ暗復号化システムの動作を説明するための図である。
【図１３】本発明の一実施形態によるコンテンツ暗復号化システムの動作を説明するための図である。
【図１４】本発明の一実施形態によるコンテンツ暗復号化システムの動作を説明するための図である。
【図１５】本発明の一実施形態による記憶装置の構成図である。
【図１６】本発明の一実施形態によるコンテンツを暗号化する方法を示す順序図である。
【図１７】本発明の一実施形態によるメディアＩＤを演算する方法を示す順序図である。
【図１８】本発明の一実施形態によるメディアＩＤを演算する方法を示す順序図である。
【図１９】本発明の一実施形態によるメディアＩＤを演算する方法を示す順序図である。
【図２０】本発明の一実施形態によるメディアＩＤを演算する方法を示す順序図である。
【図２１】本発明の一実施形態によるメディアＩＤからコンテンツ暗号化鍵を生成する方法を示す順序図である。
【図２２】本発明の一実施形態によるメディアＩＤからコンテンツ暗号化鍵を生成する方法を示す順序図である。
【図２３】本発明の一実施形態によるメディアＩＤからコンテンツ暗号化鍵を生成する方法を示す順序図である。
【図２４】本発明の一実施形態によるメディアＩＤからコンテンツ暗号化鍵を生成する方法を示す順序図である。
【図２５】本発明の一実施形態によるコンテンツ復号化方法を示す順序図である。
【図２６】本発明の一実施形態によるコンテンツ無断複製する際のコンテンツ復号化方法を示す順序図である。
【図２７】本発明の一実施形態によるコンテンツ復号化方法を示す順序図である。
【発明を実施するための形態】

【００２３】
本発明の利点及び特徴、これらを達成する方法は添付する図面と共に詳細に後述する実施形態において明確になるであろう。しかしながら、本発明は、以下で開示する実施形態に限定されるものではなく、互いに異なる多様な形態で実現されるものであり、本実施形態は、単に本発明の開示を完全にし、本発明が属する技術分野で通常の知識を有する者に発明の範疇を完全に知らせるために提供されるものであり、本発明は、請求項の範囲によってのみ定義される。図面に表示する構成要素のサイズ及び相対的なサイズは説明を明瞭するため、誇張したものであり得る。明細書全体にかけて同一参照符号は同一構成要素を指称し、「及び／または」は、言及されたアイテムのそれぞれ及び一つ以上のすべての組合せを含む。

【００２４】
本明細書で使用された用語は、実施形態を説明するためのものであり、本発明を限定しようとするものではない。本明細書で、単数型はその文脈で特に言及しない限り複数型も含む。明細書で使用される「含む（ｃｏｍｐｒｉｓｅ）」及び／または「含む（ｃｏｍｐｒｉｓｉｎｇ）」は言及された構成要素以外の一つ以上の他の構成要素の存在または追加を排除しない。

【００２５】
第１、第２などが多様な素子、構成要素を叙述するために使用されるが、これら素子、構成要素はこれらの用語によって限定されないことはいうまでもない。これらの用語は、単にある構成要素を他の構成要素と区別するために用いるものである。したがって、以下で言及される第１素子または構成要素は本発明の技術的思想内で第２素子または構成要であり得ることは勿論である。

【００２６】
本明細書で記述する実施形態は本発明の理想的な構成図を参考にして説明する。したがって、製造技術などによって構成図の形態や構造を変形する場合がある。したがって、本発明の実施形態は図示する特定形態に限定されるものではなく、それから変形した形態も含む。すなわち、図示する構成は本発明の特定形態を例示するためであり、発明の範疇を限定するためではない。

【００２７】
他に定義されなければ、本明細書で使用されるすべての用語（技術及び科学的用語を含む）は、本発明が属する技術分野で通常の知識を有する者が共通に理解できる意味として使用され得る。また一般に使用される辞典に定義されている用語は明白に特別に定義されていない限り理想的にまたは過度に解釈しない。

【００２８】
図１を参照して本発明の一実施形態によるコンテンツ暗復号化システムの構成を説明する。

【００２９】
コンテンツ記録装置１００は、記憶装置２００に格納されるコンテンツや、コンテンツ記録装置１００の内部に備えられた格納部（図示せず）に格納されているコンテンツ、またはネットワークを介して受信したコンテンツを暗号化して記憶装置２００に格納する。コンテンツ記録装置１００は、記憶装置２００に格納されたプリミティブＩＤを記憶装置２００から提供され、前記プリミティブＩＤを用いて暗号化鍵を生成し、前記暗号化鍵を用いて前記コンテンツを暗号化する。記憶装置２００は、コンテンツ記録装置１００及びコンテンツ再生装置３００のうち少なくとも一つと無線通信できる通信インターフェースを備えることができる。記憶装置２００は、取り外しできるようにコンテンツ記録装置１００の接続ポートまたはコンテンツ再生装置３００の接続ポートに接続する接続ポートをさらに備えることもできる。記憶装置２００はコンテンツ記録装置１００またはコンテンツ再生装置３００の内部に設置されたものであり得る。

【００３０】
コンテンツ再生装置３００は記憶装置２００に格納された暗号化コンテンツを復号化し

て再生する。コンテンツ再生装置３００は記憶装置２００から記憶装置２００に格納されたプリミティブＩＤを提供され、前記プリミティブＩＤを用いて復号化鍵を生成して前記暗号化コンテンツを復号化する。

【００３１】

コンテンツ記録装置１００及びコンテンツ再生装置３００は、コンピュータ、ＵＭＰＣ（Ｕｌｔｒａ ＭｏｂｉｌｅＰＣ）、ワークステーション、ネットブック（ｎｅｔ－ｂｏｏｋ）、ＰＤＡ（Ｐｅｒｓｏｎａｌ Ｄｉｇｉｔａｌ Ａｓｓｉｓｔａｎｔｓ）、ポータブル（ｐｏｒｔａｂｌｅ）コンピュータ、ウェブタブレット（ｗｅｂ ｔａｂｌｅｔ）、携帯電話（ｍｏｂｉｌｅ ｐｈｏｎｅ）、スマートフォン（ｓｍａｒｔ ｐｈｏｎｅ）、ｅ－ブック（ｅ－ｂｏｏｋ）、ＰＭＰ（ｐｏｒｔａｂｌｅ ｍｕｌｔｉｍｅｄｉａ ｐｌａｙｅｒ）、携帯用ゲーム機、ナビゲーション（ｎａｖｉｇａｔｉｏｎ）装置、ブラックボックス（ｂｌａｃｋ ｂｏｘ）、デジタルカメラ（ｄｉｇｉｔａｌ ｃａｍｅｒａ）、３次元テレビ受像機（３－ｄｉｍｅｎｓｉｏｎａｌ ｔｅｌｅｖｉｓｉｏｎ）、デジタル音声録音機（ｄｉｇｉｔａｌ ａｕｄｉｏ ｒｅｃｏｒｄｅｒ）、デジタル音声再生機（ｄｉｇｉｔａｌ ａｕｄｉｏ ｐｌａｙｅｒ）、デジタル画像録画機（ｄｉｇｉｔａｌ ｐｉｃｔｕｒｅ ｒｅｃｏｒｄｅｒ）、デジタル画像再生機（ｄｉｇｉｔａｌ ｐｉｃｔｕｒｅ ｐｌａｙｅｒ）、デジタルビデオレコーダ（ｄｉｇｉｔａｌ ｖｉｄｅｏ ｒｅｃｏｒｄｅｒ）、デジタルビデオプレーヤ（ｄｉｇｉｔａｌ ｖｉｄｅｏ ｐｌａｙｅｒ）の情報を無線環境で送受信できる装置、ホームネットワークを構成する多様な電子装置中の一つ、コンピュータネットワークを構成する多様な電子装置中の一つ、テレマティックスネットワークを構成する多様な電子装置中の一つ、コンピュータシステムを構成する多様な構成要素中の一つなどのような電子装置の多様な構成要素中の一つであり得る。

【００３２】

前記暗号化に用いる暗号化アルゴリズム及び暗号化鍵は特定したものに限定されないが、暗号化鍵と復号化鍵が同一になるように対称鍵暗号化方式によるアルゴリズム、例えばＡＥＳ（Ａｄｖａｎｃｅｄ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ）標準に従う暗号化アルゴリズムを用いることができる。前記対称鍵暗号化方式を用いる場合、コンテンツ記録装置１００が前記プリミティブＩＤから前記暗号化鍵を生成する方法とコンテンツ再生装置３００が前記プリミティブＩＤから前記復号化鍵を生成する方法は同一である。

【００３３】

図１に図示するように、前記プリミティブＩＤは第１プリミティブＩＤ及び第２プリミティブＩＤを含み得る。コンテンツ記録装置１００及びコンテンツ再生装置３００いずれも前記第１プリミティブＩＤ及び前記第２プリミティブＩＤのうち少なくとも一つを用いて記憶装置２００の固有識別子であるメディアＩＤを生成し、前記メディアＩＤを用いて暗号化鍵または復号化鍵を生成することができる。前記プリミティブＩＤは前記メディアＩＤ演算に利用される一つ以上の識別用データであって、前記メディアＩＤとは異なるデータであり得る。

【００３４】

図２は、本発明の一実施形態によるコンテンツ記録装置１００の構成図を図示する。図２に図示するように、本実施形態によるコンテンツ記録装置１００はプロセッサ１４０及び記憶装置インターフェース１１０を含み得る。コンテンツ記録装置１００はプロセッサ１４０が実行する命令セットを一時的に格納するＲＡＭ（Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）１２０及び内部記憶装置１３０をさらに含み得る。

【００３５】

記憶装置インターフェース１１０はコンテンツ記録装置１００と記憶装置２００との間のデータ送受信を仲介する。記憶装置インターフェース１１０は記憶装置２００に備えられた第１パート及び第２パートそれぞれを識別するための第１プリミティブＩＤ及び第２プリミティブＩＤを記憶装置２００から提供され、プロセッサ１４０によって暗号化したコンテンツを記憶装置２００に提供する。前記第１プリミティブＩＤは前記記憶装置に備えられたコントローラの固有識別子であるコントローラＩＤであり、前記第２プリミティ

ブＩＤは前記記憶装置に備えられたメモリ装置の固有識別子であるメモリＩＤを暗号化した暗号化メモリＩＤであり得る。記憶装置２００の前記第１パート及び第２パートはそれぞれコントローラ及びメモリ装置を意味し得るが、一実施例に過ぎず、記憶装置２００の前記第１パート及び第２パートは記憶装置２００のそれぞれ他のパートを示すものと理解できるであろう。

【００３６】

プロセッサ１４０はＲＡＭ１２０に一時的に格納される命令を実行し、実行される命令はその機能によってＩＤ演算部１４１、暗号化鍵生成部１４２及び暗号化部１４３にグループ分けすることができる。

【００３７】

ＩＤ演算部１４１は前記メモリ暗号化ＩＤを復号化して前記メモリＩＤを取得し、前記メモリＩＤを用いて前記メディアＩＤ生成に用いるメモリ装置の他の固有識別子であるメモリ派生ＩＤを生成し、前記コントローラＩＤ及び前記メモリ派生ＩＤのうち少なくとも一つを用いて前記メディアＩＤを演算する。例えば、ＩＤ演算部１４１は前記コントローラＩＤ及び前記メモリ派生ＩＤを２進演算（ｂｉｎａｒｙ　ｏｐｅｒａｔｉｏｎ）して前記メディアＩＤを演算するか、または前記コントローラＩＤ及び前記メモリ派生ＩＤを文字列連結演算して前記メディアＩＤを演算することができる。前記文字列連結演算において、コントローラＩＤの後に前記メモリ派生ＩＤが連結され得、前記メモリ派生ＩＤの後に前記コントローラＩＤが連結され得る。

【００３８】

暗号化鍵生成部１４２は前記メディアＩＤを用いて前記暗号化鍵を生成し、暗号化部１４３は前記暗号化鍵で前記コンテンツを暗号化する。前記コンテンツは内部記憶装置（ｉｎｔｅｒｎａｌ　ｓｔｏｒａｇｅ）１３０に格納されたものであるが、記憶装置２００に格納されたものであり得る。暗号化鍵生成部１４２は一つの入力パラメータ及び一つの出力を有する所定のルーチンに前記メディアＩＤを前記入力パラメータとして設定し、前記ルーチンを実行し、その結果、出力したデータを前記暗号化鍵として暗号化部１４３に提供することができる。前記ルーチンは一方向性関数（ｏｎｅ－ｗａｙ　ｆｕｎｃｔｉｏｎ）であり得る。

【００３９】

図３も本発明の一実施形態によるコンテンツ記録装置１００の構成図を図示する。

【００４０】

図３に図示するように、プロセッサ１４０はランダムナンバー生成器（Ｒａｎｄｏｍ　Ｎｕｍｂｅｒ　Ｇｅｎｅｒａｔｏｒ、ＲＮＧ）１４４をさらに含み得る。ランダムナンバー生成器はランダムナンバーを生成して暗号化鍵生成部１４２に提供する。

【００４１】

暗号化鍵生成部１４２はＩＤ生成部１４１が生成したメディアＩＤ及び前記ランダムナンバーから提供されたランダムナンバーを用いて暗号化鍵を生成することができる。例えば、暗号化鍵生成部１４２はＣＭＡＣ（Ｃｉｐｈｅｒ－ｂａｓｅｄ　Ｍｅｓｓａｇｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｃｏｄｅ）アルゴリズムに前記固有識別子及び前記ランダムナンバーを入力して前記暗号化鍵を生成することができる。暗号化コンテンツを復号化するための復号化鍵を生成する際にも前記ランダムナンバーが必要であるため、前記ランダムナンバーは前記暗号化コンテンツと共に記憶装置２００に格納され得る。暗号化鍵生成部１４２が前記メディアＩＤ及びコンテンツの固有識別子を用いて暗号化鍵を生成する実施例については図１０を参照して詳細に説明する。

【００４２】

暗号化鍵生成部１４２は前記メディアＩＤ及びコンテンツの固有識別子を用いて暗号化鍵を生成することもできる。前記ランダムナンバーの場合と同様に暗号化コンテンツを復号化するための復号化鍵を生成する際にもコンテンツ固有識別子が必要であるため、前記コンテンツの固有識別子は前記暗号化コンテンツと共に記憶装置２００に格納され得る。暗号化鍵生成部１４２が前記メディアＩＤ及びコンテンツの固有識別子を用いて暗号化鍵

を生成する実施例については図１１を参照して詳細に説明する。

【００４３】

図４も本発明の一実施形態によるコンテンツ記録装置１００の構成図を図示する。

【００４４】

図４に図示するように、本実施形態によるコンテンツ記録装置１００はプロセッサ１４０及び記憶装置インターフェース１１０を含み得、プロセッサ１４０はＩＤ演算部１４１、暗号化鍵生成部１４２及び暗号化部１４３の他に認証情報生成部１４５、派生ＩＤ生成部１４６及び相互認証部１４７をさらに含み得る。

【００４５】

本実施形態によるコンテンツ記録装置１００は記憶装置２００と二回の相互認証、すなわち第１認証及び第２認証を行う。前記第１認証は記憶装置２００のメモリ装置２０６を認証するための認証であり、前記第２認証は記憶装置２００のコントローラ２０８を認証するための認証である。

【００４６】

前記第１認証は派生ＩＤ生成部１４６が第１認証情報を記憶装置２００から提供され、認証情報生成部１４５から第２認証情報を提供され、前記第１認証情報及び前記第２認証情報を比較することによって行う。前記比較の結果、前記第１認証情報と前記第２認証情報が一致する場合に限って派生ＩＤ生成部１４６が前記メモリＩＤを用いて前記メモリ派生ＩＤを生成する。派生ＩＤ生成部１４６は前記メモリＩＤを認証情報生成部１４５から提供され、認証情報生成部１４５は記憶装置２００から提供された暗号化メモリＩＤを復号化して前記メモリＩＤを生成した後派生ＩＤ生成部１４６に提供する。派生ＩＤ生成部１４６が生成した前記メモリ派生ＩＤはＩＤ演算部１４１に提供される。

【００４７】

前記第２認証は、相互認証部１４７によって行う。相互認証部１４７は前記第２認証のために記憶装置２００から第３認証情報を提供される。前記第２認証は公開鍵基盤の相互認証であり得、前記第３認証情報には記憶装置２００の認証書データ及び記憶装置２００に備えられたコントローラの固有の識別子であるコントローラプリミティブＩＤが含まれ得、相互認証部１４７は前記認証書データに含まれた認証書ＩＤ及び前記コントローラプリミティブＩＤを用いて前記コントローラのまた他の固有識別子であるコントローラＩＤを取得することができる。例えば、相互認証部１４７は前記認証書ＩＤ及び前記コントローラプリミティブＩＤを文字列連結演算（ｓｔｒｉｎｇ　ｃｏｎｃａｔｅｎａｔｉｏｎ）して前記コントローラＩＤを取得することができる。

【００４８】

整理すると、相互認証部１４７はコンテンツ記録装置１００と記憶装置２００との間の公開鍵基盤の相互認証を行うために記憶装置２００と認証書を相互交換し、この過程で記憶装置２００から提供される前記第３認証情報から前記コントローラＩＤを取得する。相互認証部１４７は前記コントローラＩＤをＩＤ演算部１４１に提供する。前述したように、ＩＤ演算部１４１は前記コントローラＩＤ及び前記メモリ派生ＩＤのうち少なくとも一つを用いて前記メディアＩＤを演算することができる。暗号化鍵生成部１４２は前記メディアＩＤを用いて暗号化鍵を生成し、暗号化部１４３は前記暗号化鍵を用いてコンテンツを暗号化した後、記憶装置２００に提供する。

【００４９】

図５は、本発明の一実施形態による記憶装置２００の構成を図示する。図５に図示するように、本実施形態による記憶装置２００はメモリ装置２０６及びメモリ装置２０６を制御するコントローラ２０８を含み得る。

【００５０】

メモリ装置２０６は不揮発性メモリとして、ＮＡＮＤ－ＦＬＡＳＨメモリ、ＮＯＲ－ＦＬＡＳＨメモリ、相変化メモリ（ＰＲＡＭ：Ｐｈａｓｅ　ｃｈａｎｇｅ　Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）、磁気固体メモリ（ＭＲＡＭ：Ｍａｇｎｅｔｉｃ　Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）、抵抗メモリ（ＲｅＲＡＭ：Ｒｅｓｉｓｔｉｖｅ

Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）を記憶手段として使用したチップまたはパッケージであり得る。

【００５１】

また、前記パッケージ方式と関連し、メモリ装置２０６はＰｏＰ（Ｐａｃｋａｇｅ ｏｎ Ｐａｃｋａｇｅ）、Ｂａｌｌ ｇｒｉｄ ａｒｒａｙｓ（ＢＧＡｓ）、Ｃｈｉｐ ｓｃａｌｅ ｐａｃｋａｇｅｓ（ＣＳＰｓ）、Ｐｌａｓｔｉｃ Ｌｅａｄｅｄ Ｃｈｉｐ Ｃａｒｒｉｅｒ（ＰＬＣＣ）、Ｐｌａｓｔｉｃ Ｄｕａｌ Ｉｎ Ｌｉｎｅ Ｐａｃｋａｇｅ（ＰＤＩＰ）、Ｄｉｅ ｉｎ Ｗａｆｆｌｅ Ｐａｃｋ、Ｄｉｅ ｉｎ Ｗａｆｅｒ Ｆｏｒｍ、Ｃｈｉｐ Ｏｎ Ｂｏａｒｄ（ＣＯＢ）、Ｃｅｒａｍｉｃ Ｄｕａｌ Ｉｎ Ｌｉｎｅ Ｐａｃｋａｇｅ（ＣＥＲＤＩＰ）、Ｐｌａｓｔｉｃ Ｍｅｔｒｉｃ Ｑｕａｄ Ｆｌａｔ Ｐａｃｋ（ＭＱＦＰ）、Ｔｈｉｎ Ｑｕａｄ Ｆｌａｔｐａｃｋ（ＴＱＦＰ）、Ｓｍａｌｌ Ｏｕｔｌｉｎｅ（ＳＯＩＣ）、Ｓｈｒｉｎｋ Ｓｍａｌｌ Ｏｕｔｌｉｎｅ Ｐａｃｋａｇｅ（ＳＳＯＰ）、Ｔｈｉｎ Ｓｍａｌｌ Ｏｕｔｌｉｎｅ（ＴＳＯＰ）、Ｔｈｉｎ Ｑｕａｄ Ｆｌａｔｐａｃｋ（ＴＱＦＰ）、Ｓｙｓｔｅｍ Ｉｎ Ｐａｃｋａｇｅ（ＳＩＰ）、Ｍｕｌｔｉ Ｃｈｉｐ Ｐａｃｋａｇｅ（ＭＣＰ）、Ｗａｆｅｒ－ｌｅｖｅｌ Ｆａｂｒｉｃａｔｅｄ Ｐａｃｋａｇｅ（ＷＦＰ）、Ｗａｆｅｒ－Ｌｅｖｅｌ Ｐｒｏｃｅｓｓｅｄ Ｓｔａｃｋ Ｐａｃｋａｇｅ（ＷＳＰ）などのような方式でパッケージ化して実装することができる。

【００５２】

メモリ装置２０６は暗号化コンテンツ及びプリミティブＩＤを格納する。前記暗号化コンテンツは前記メディアＩＤを用いて生成した復号化鍵で復号化するデータであり、前記プリミティブＩＤは前記メディアＩＤ演算に利用する一つ以上の識別用データであり、前記メディアＩＤとは異なるデータである。前記プリミティブＩＤは前記コントローラの固有識別子であるコントローラＩＤ及び前記メモリ装置の固有識別子であるメモリＩＤを暗号化した暗号化メモリＩＤを含む。

【００５３】

前記メディアＩＤは前記メモリ装置及び前記コントローラを含む記憶装置の固有識別子であり、前記メモリＩＤを用いて生成したメモリ派生ＩＤ及び前記コントローラＩＤを用いて生成したものである。

【００５４】

メモリ装置２０６は、記憶領域が第１領域、第２領域及び第３領域に分けられたものであり得る。

【００５５】

メモリ装置２０６は、前記メモリＩＤを前記第１領域に、前記コントローラＩＤ及び前記暗号化メモリＩＤを前記第２領域に、前記暗号化コンテンツを前記第３領域にそれぞれ格納することができる。

【００５６】

前記第１領域は前記第３領域のアクセス方法によってはアクセスされない領域である。例えば、前記第３領域はＲＥＡＤ／ＷＲＩＴＥのアクセスが可能な領域であり、前記第１領域はメモリ装置２０６の内部のセキュリティロジック（図示せず）によってのみアクセス可能な領域であり得る。また、前記第２領域は読み取り専用アクセスのみ可能な領域であり得る。前記セキュリティロジックは前記メモリＩＤに対するリード要請に応答して前記第２領域に格納された暗号化メモリＩＤをコントローラ２０８を介して出力することができる。

【００５７】

図４を参照して説明したように、メモリ装置２０６は前記復号化鍵の生成に用いるランダムナンバー及びコンテンツ識別子中の一つをさらに格納することもできる。

【００５８】

復号化鍵と暗号化コンテンツが共に複製されることを防止するため、メモリ装置２０６は復号化鍵そのものを格納しない方が好ましい。すなわち、本実施形態による記憶装置２

００に格納された前記暗号化コンテンツを再生しようとする装置は記憶装置２００から前記プリミティブＩＤを提供され、前記メディアＩＤを生成した後、前記メディアＩＤを用いて前記暗号化コンテンツに対する復号化鍵を直接生成しなければならない。

【００５９】

図６は本発明の一実施形態によるコンテンツ再生装置３００の構成を図示する。図６に図示するように、本実施形態によるコンテンツ再生装置３００はプロセッサ３４０及び記憶装置インターフェース３６０を含み、プロセッサ３４０が実行する命令セットを一時的に格納するＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）３２０をさらに含み得る。

【００６０】

記憶装置インターフェース３６０は、記憶装置２００に格納された暗号化コンテンツと記憶装置２００に備えられた第１パート及び第２パートそれぞれを識別するための第１プリミティブＩＤ及び第２プリミティブＩＤを記憶装置２００から提供される。

【００６１】

プロセッサ３４０は前記第１プリミティブＩＤ及び第２プリミティブＩＤを用いて前記記憶装置の固有識別子であるメディアＩＤを生成し、前記メディアＩＤを用いて生成した復号化鍵で前記暗号化コンテンツを復号化して再生する。

【００６２】

前記第２プリミティブＩＤは、前記記憶装置に備えられたメモリ装置の固有識別子であるメモリＩＤを暗号化した暗号化メモリＩＤであり得る。プロセッサ３４０は前記暗号化メモリＩＤを用いてコンテンツ再生装置３００と記憶装置１００との間の第１認証のための第２認証情報を生成することができる。プロセッサ３４０は前記暗号化メモリＩＤを復号化して前記メモリＩＤを生成し、前記メモリＩＤに基づいて前記第２認証情報を生成することができる。

【００６３】

前述したように、前記第１認証は記憶装置１００のメモリ装置２０６を認証するための認証である。記憶装置インターフェース３６０は前記第１認証のための第１認証情報を記憶装置２００からさらに提供されてプロセッサ３４０に提供する。プロセッサ３４０は前記第１認証情報及び前記第２認証情報を比較して二つの認証情報が一致する場合に限って前記メディアＩＤを生成する。

【００６４】

前記第１プリミティブＩＤは記憶装置２００に備えられたコントローラ２０８の固有識別子であるコントローラＩＤであり得る。記憶装置インターフェース３６０はコンテンツ再生装置３００と記憶装置２００との間の第２認証のための第３認証情報を記憶装置２００から提供されるが、前記第３認証情報は前記コントローラＩＤを含む。

【００６５】

記憶装置インターフェース３６０は記憶装置２００に格納されたランダムナンバーを記憶装置２００からさらに提供され、前記ランダムナンバーをプロセッサ３４０に提供することができる。プロセッサ３４０は前記メディアＩＤ及び前記ランダムナンバーをＣＭＡＣアルゴリズムに入力して前記復号化鍵を生成することができる。記憶装置インターフェース３６０は記憶装置２００に格納されたコンテンツ識別子を記憶装置２００からさらに提供され、前記ランダムナンバーをプロセッサ３４０に提供することもできる。プロセッサ３４０は前記メディアＩＤ及び前記コンテンツ識別子をＣＭＡＣアルゴリズムに入力して前記復号化鍵を生成することもできる。

【００６６】

図７ないし８を参照して本発明の一実施形態によるコンテンツ記憶サーバの構成及び動作について説明する。本実施形態によるコンテンツ記憶サーバ４００はクラウド（ＣＬＯＵＤ）サービスを提供するサーバであり得る。すなわち、コンテンツ記憶サーバ４００は特定ユーザが所有した複数の端末間にコンテンツの同期化が自動的に行われるようにサポートするサーバであり得る。また、コンテンツ記憶サーバ４００はコンテンツ記録装置１

００、記憶装置２００及びコンテンツ再生装置３００のうち少なくとも２つの組合せで構成され得る。

【００６７】

例えば、第１端末５０２及び第２端末５０４が一つの端末グループ５００に属するものであり、第１端末５０２が新規コンテンツを生成して前記新規コンテンツがコンテンツ記憶サーバ４００にアップロードされる場合、コンテンツ記憶サーバ４００はアップロードされたコンテンツを第２端末５０４に送信することによって前記同期化が自動的に行われるようにサポートするサーバであり得る。

【００６８】

コンテンツ記憶サーバ４００は前記同期化が自動的に、ユーザの操作なしで行われるようにサポートした方が望ましいが、本発明の一部実施形態によれば、前記同期化は手動で、ユーザの操作によって行われることもできる。例えば、コンテンツのアップロード及びダウンロードのうち少なくとも一つはユーザの命令または確認を条件として行われ得る。

【００６９】

以下、本実施形態によるコンテンツ記憶サーバ４００の構成及び動作について説明する。図７ないし８で第１端末５０２及び第２端末５０４は一つの端末グループ５００に属するものである。例えば、第１端末５０２及び第２端末５０４は一人のユーザが所有するものであり得る。第１端末５０２及び第２端末５０４は、例えば、移動通信端末であり得、記憶装置５２２は例えばＰＣカード（ＰＣＭＣＩＡ、ｐｅｒｓｏｎａｌ ｃｏｍｐｕｔｅｒ ｍｅｍｏｒｙ ｃａｒｄ ｉｎｔｅｒｎａｔｉｏｎａｌ ａｓｓｏｃｉａｔｉｏｎ）、コンパクトフラッシュ（登録商標）カード（ＣＦ）、スマートメディアカード（ＳＭ、ＳＭＣ）、メモリスティック、マルチメディアカード（ＭＭＣ、ＲＳ－ＭＭＣ、ＭＭＣｍｉｃｒｏ）、ＳＤカード（ＳＤ、ｍｉｎｉＳＤ、ｍｉｃｒｏＳＤ、ＳＤＨＣ）、ユニバーザルフラッシュ記憶装置（ＵＦＳ）などのようなメモリカードであり得る。

【００７０】

図７は、コンテンツがアップロードされる場合のコンテンツ記憶サーバ４００の動作を図示する。アップロード対象コンテンツは第１端末５０２が生成したものであり得、第１端末５０２に接続された記憶装置５２２に格納されたものであり得る。

【００７１】

第１端末５０２はメモリ派生ＩＤを生成し、アップロード対象コンテンツを前記メモリ派生ＩＤと共にコンテンツ記憶サーバ４００にアップロードする。前記メモリ派生ＩＤは流出を防ぐために暗号化した状態でアップロードされる。

【００７２】

コンテンツ記憶サーバ４００の受信部４０２は前記コンテンツ及び前記メモリ派生ＩＤを受信して暗号化部４０４に提供する。暗号化部４０４は前記メモリ派生ＩＤを暗号化鍵として用いて前記コンテンツを暗号化する。暗号化部４０４は対称型暗号化アルゴリズムを用いて前記メモリ派生ＩＤが復号化鍵としても使用できるようにした方が好ましい。暗号化部４０４によって暗号化が完了した後にはコンテンツ原本は削除した方が好ましい。

【００７３】

暗号化部４０４によって暗号化したコンテンツは格納部４０５に格納される。一部実施形態によれば、格納部４０５はコンテンツ記憶サーバ４００とは別のサーバ（図示せず）に備えられ得る。

【００７４】

図８を参照して第２端末５０４が暗号化されたコンテンツをダウンロードする動作について説明する。送信部４０６は格納部４０５に格納された暗号化コンテンツを第２端末５０４に送信する。前記送信は第２端末５０４を操作せず、自動的に実行され得、第２端末５０４介してユーザを確認した後に実行され得る。前記送信は第１端末５０２と第２端末５０４との間のコンテンツ同期化のためのものであるため、第２端末５０４に同一コンテンツがすでに格納されていれば、前記送信は実行しない方が好ましい。

【００７５】

前述したように、第２端末５０４はコンテンツ記憶サーバ４００から暗号化コンテンツのみダウンロードする。したがって、第２端末５０４が復号化鍵を生成するためには第１端末がコンテンツをアップロードする際、第１端末に接続されていた記憶装置５２２が第２端末５０４に接続されなければならない。第２端末５０４は記憶装置５２２から前記暗号化メモリＩＤを提供され、前記第１認証を行うことによって前記メモリ派生ＩＤを生成し、前記メモリ派生ＩＤを用いてコンテンツ記憶サーバ４００からダウンロードした暗号化コンテンツを復号化することができる。

【００７６】

第２端末５０４は、ユーザが前記ダウンロードした暗号化コンテンツの再生命令を入力する時点で前記メモリ派生ＩＤ生成及び復号化を行うこともできるが、前記再生命令がなくても、ダウンロード完了時に前記メモリ派生ＩＤ生成及び復号化を行うこともできる。

【００７７】

本発明による一実施形態によれば、コンテンツ記憶サーバ４００は第２端末５０４に復号化したコンテンツを送信することもできる。すなわち、コンテンツ記憶サーバ４００は前記暗号化したコンテンツを第１端末５０２から提供されたメモリ派生ＩＤを用いて復号化し、復号化したコンテンツを送信部４０６に提供した後、削除する復号化部（図示せず）をさらに含むことができる。

【００７８】

このような実施形態で、コンテンツ記憶サーバ４００は前記メモリ派生ＩＤを格納部４０５のセキュリティ領域に格納し、前記メモリ派生ＩＤが流出することを防止することができる。

【００７９】

本発明による一実施形態によれば、コンテンツ記憶サーバ４００は前記メモリ派生ＩＤに基づき前記メモリ派生ＩＤとは異なる暗号化鍵を用いてアップロードされたコンテンツを暗号化することもできる。この際、暗号化部４０４は前記メモリ派生ＩＤに基づき前記メモリ派生ＩＤとは異なる暗号化鍵を生成し、送信部４０６は第２端末５０４に前記暗号化したコンテンツ及び前記暗号化したコンテンツの復号化鍵を共に送信することができる。

【００８０】

本実施形態によるコンテンツ記憶サーバ４００は、第１端末５０２に接続された記憶装置５２２のメモリ派生ＩＤを用いて前記アップロードしたコンテンツを暗号化し、暗号化したコンテンツのみ格納する。前記メモリ派生ＩＤは記憶装置５２２に備えられたメモリ装置の固有識別子であるメモリＩＤに基づき生成したものである。

【００８１】

従来技術によるクラウドサービスはアップロードしたコンテンツにアクセスするためのユーザ認証を経るが、このような認証が無力化されるとサービスユーザの個人情報に関するコンテンツが流出する危険性があった。

【００８２】

反面、本実施形態によるコンテンツ記憶サーバ４００はアップロードされたコンテンツを暗号化した後に格納し、暗号化鍵はコンテンツアップロード端末に接続された記憶装置のメモリ派生ＩＤを用いて生成する。また、コンテンツ記憶サーバ４００は前記暗号化鍵を格納しない。暗号化鍵と復号化する鍵は同一であるため、コンテンツダウンロード端末は前記暗号化したコンテンツの復号化鍵を直接生成しなければならない。すなわち、コンテンツアップロード端末に接続されていた記憶装置を備えていなければ、コンテンツの復号化が不可能である。

【００８３】

すなわち、ユーザ認証が無力化されても、各コンテンツの復号化鍵を得るためには前記メモリ派生ＩＤを知らなければならず、前記メモリ派生ＩＤを知るためにはコンテンツアップロード端末に接続された記憶装置に物理的に接続されなければならない。したがって、本実施形態によれば、クラウドサーバにアップロードするコンテンツに対する保安性を

強化する効果がある。例えば、個人情報に関するコンテンツも安心してクラウドサービスにより同期化できる効果がある。

【００８４】

図９ないし図１５を参照して本発明の実施形態によるコンテンツ記録装置、記憶装置及びコンテンツ再生装置の構成及び動作について説明する。

【００８５】

図９は、本発明の一実施形態によるコンテンツ記録装置１００、記憶装置２００及びコンテンツ再生装置３００をそれぞれ図示する。

【００８６】

本実施形態によるコンテンツ記録装置１００は、図９に図示するように記憶装置２００から記憶装置２００に格納されたプリミティブＩＤを提供され、前記プリミティブＩＤから記憶装置２００の固有識別子であるメディアＩＤを演算する記憶装置識別子演算部１０２、前記メディアＩＤを用いてコンテンツ暗号化鍵を生成する暗号化鍵生成部１０４、前記コンテンツ暗号化鍵を用いてコンテンツ１０８を暗号化することによって暗号化コンテンツを生成する暗号化部１０６及び前記暗号化コンテンツが記憶装置２００に格納されるように記憶装置２００を制御する記憶装置制御部（図示せず）を含み得る。

【００８７】

記憶装置２００は、メモリ装置２０６及び前記記憶装置制御部の命令に応じてメモリ装置２０６を制御するメモリ装置コントローラ２０８を含み得る。メモリ装置２０６はプリミティブＩＤ２６０及び暗号化コンテンツ２６８を格納することができる。

【００８８】

コンテンツ再生装置３００は記憶装置２００から記憶装置２００に格納されたプリミティブＩＤを提供され、前記プリミティブＩＤから記憶装置２００のメディアＩＤを演算する記憶装置識別子演算部３０２、記憶装置２００に格納された暗号化コンテンツ２６８が出力されるように前記記憶装置を制御する制御部（図示せず）、前記メディアＩＤを用いてコンテンツ復号化鍵を生成する復号化鍵生成部３０４、前記コンテンツ復号化鍵を用いて記憶装置２００から出力される暗号化コンテンツ２６８を復号化する復号化部３０６を含む。また、復号化したコンテンツを再生する再生部３０８をさらに含み得る。

【００８９】

図１０は、本発明の一実施形態によるコンテンツ記録装置１００、記憶装置２００及びコンテンツ再生装置３００をそれぞれ図示する。本実施形態による記憶装置２００にはランダムデータ２６６がさらに格納される。以下、図９に図示するコンテンツ記録装置１００、記憶装置２００及びコンテンツ再生装置３００と図１０に図示するコンテンツ記録装置１００、記憶装置２００及びコンテンツ再生装置３００の動作の異なる点を中心に説明する。

【００９０】

本実施形態による記憶装置２００はメモリ装置２０６にプリミティブＩＤ２６０、メモリＩＤ２６２、ランダムデータ２６６、暗号化コンテンツ２６８をそれぞれ格納することができる。メモリＩＤ２６２は暗号化コンテンツ２６８が格納されるユーザ領域に対するアクセス方法によりリードされないのが好ましい。

【００９１】

プリミティブＩＤ２６０はコントローラＩＤ２６１及び暗号化メモリＩＤ２６４を含み得る。暗号化メモリＩＤ２６４はメモリ装置２０６の固有な識別子であるメモリＩＤ２６２が暗号化されたものである。

【００９２】

本実施形態によるコンテンツ記録装置１００はランダムナンバー生成器１０３をさらに含み得る。暗号化鍵生成部１０４は記憶装置識別子演算部１０２によって生成されたメディアＩＤ及びランダムナンバー生成器１０３によって生成されたランダムナンバーを用いて暗号化鍵を生成することができる。暗号化鍵生成部１０４は例えば、ＣＭＡＣ（Ｃｉｐｈｅｒ－ｂａｓｅｄ Ｍｅｓｓａｇｅ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｃｏｄｅ）アル

ゴリズムに前記メディアＩＤと前記提供されたランダムナンバーを入力して算出するデータを前記コンテンツ暗号化鍵として生成することができる。

【００９３】

本実施形態によるコンテンツ再生装置３００は記憶装置２００に格納されたランダムナンバー２６６を提供され、記憶装置識別子演算部３０２によって演算されたメディアＩＤ及びランダムナンバー２６６を用いてコンテンツ暗号化鍵を生成する復号化鍵生成部３０４を含み得る。例えば、復号化鍵生成部３０４はＣＭＡＣ（Ｃｉｐｈｅｒ－ｂａｓｅｄ Ｍｅｓｓａｇｅ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｃｏｄｅ）アルゴリズムに前記メディアＩＤとランダムナンバー２６６を入力して算出するデータを前記コンテンツ復号化鍵として用いることができる。

【００９４】

図１１は、図１０におけるランダムナンバー２６６の代わりに、コンテンツ識別子２６７を用いて暗号化鍵を生成するコンテンツ記録装置１００及びコンテンツ識別子２６７を用いて復号化鍵を生成するコンテンツ再生装置３００を図示する。以下、図１１に図示するコンテンツ記録装置１００、記憶装置２００及びコンテンツ再生装置３００と図９に図示するコンテンツ記録装置１００、記憶装置２００及びコンテンツ再生装置３００の動作の異なる点を中心に説明する。

【００９５】

図１１に図示するように、本実施形態によるコンテンツ記録装置１００はコンテンツ１０８の識別子を取得するコンテンツ識別子取得部１１０をさらに含む。コンテンツ識別子取得部１１０はコンテンツ１０８のヘッダーに含まれたコンテンツ識別子を取得するか、またはコンテンツ１０８の識別用情報をコンテンツ１０８から生成した後、前記識別用情報を利用して照会することによりコンテンツ識別子提供サーバ（図示せず）からコンテンツ１０８のコンテンツ識別子を提供され得る。コンテンツ識別子取得部１１０は前記コンテンツ識別子を暗号化鍵生成部１０４に提供し、記憶装置２００に提供する。

【００９６】

本実施形態によるコンテンツ記録装置１００は前記コンテンツ識別子及び前記メディアＩＤを用いて暗号化鍵を生成する暗号化鍵生成部１０４を含み得る。

【００９７】

本実施形態による記憶装置２００はコンテンツ記録装置１００から提供されたコンテンツ識別子２６７を格納する。

【００９８】

本実施形態によるコンテンツ再生装置３００は記憶装置２００に格納されたコンテンツ識別子２６７を提供され、前記メディアＩＤ及びコンテンツ識別子２６７を用いて復号化鍵を生成する復号化鍵生成部３０４を含み得る。

【００９９】

一方、本実施形態によるコンテンツ記録装置１００はコンテンツ識別子２６７を記憶装置２００に格納しない場合もある。この場合、コンテンツ再生装置３００は暗号化コンテンツの識別用情報を生成した後、前記識別用情報を利用して照会することによりコンテンツ識別子提供サーバ（図示せず）からコンテンツ１０８のコンテンツ識別子を提供され得る。

【０１００】

図１２は、本発明の一実施形態によるコンテンツ記録装置１００、記憶装置２００及びコンテンツ再生装置３００をそれぞれ図示する。以下、図９に図示するコンテンツ記録装置１００、記憶装置２００及びコンテンツ再生装置３００と図１２に図示するコンテンツ記録装置１００、記憶装置２００及びコンテンツ再生装置３００の動作を比較して異なる点を中心に説明する。

【０１０１】

図１２に図示するように、暗号化鍵を生成して復号化鍵を生成することにおいて、メディアＩＤを所定の関数に入力して出力されたデータを暗号化鍵または復号化鍵として生成

することができる。前記所定の関数は、例えば一方向性関数（ｏｎｅ－ｗａｙ　ｆｕｎｃｔｉｏｎ）であり得る。

【０１０２】

すなわち、図１２に図示する暗号化鍵生成部１０４及び復号化鍵生成部３０４は暗号化鍵及び復号化鍵をそれぞれ生成することにおいて、ランダムナンバー２６６、パスワードまたはコンテンツ識別子２６７を必要としない。

【０１０３】

図１３は本発明の一実施形態によるコンテンツ記録装置１００、記憶装置２００及びコンテンツ再生装置３００をそれぞれ図示する。以下、図９に図示するコンテンツ記録装置１００、記憶装置２００及びコンテンツ再生装置３００と図１３に図示するコンテンツ記録装置１００、記憶装置２００及びコンテンツ再生装置３００を比較して動作が異なる点を中心に説明する。

【０１０４】

図１３に図示するように、コンテンツ記録装置１００及びコンテンツ再生装置３００はそれぞれ暗号化鍵を生成して復号化鍵を生成することにおいて、メディアＩＤをそのまま暗号化鍵または復号化鍵として用いることができる。したがって、図１３に図示するコンテンツ記録装置１００の暗号化鍵生成部１０４及びコンテンツ再生装置３００の復号化鍵生成部３０４は特別な動作を行わず、入力されたメディアＩＤをそのまま暗号化鍵または復号化鍵として出力する。

【０１０５】

図１４は、本発明の一実施形態によるコンテンツ記録装置１００、記憶装置２００及びコンテンツ再生装置３００をそれぞれ図示する。以下、図１０に図示するコンテンツ記録装置１００、記憶装置２００及びコンテンツ再生装置３００と図１４に図示するコンテンツ記録装置１００、記憶装置２００及びコンテンツ再生装置３００を比較して動作が異なる点を中心に説明する。

【０１０６】

図１４に図示するように、メディアＩＤを演算することにおいて、メディアＩＤから提供されたプリミティブＩＤ２６０をそのままメディアＩＤとして用いることができる。したがって、図１４に図示するコンテンツ記録装置１００の記憶装置識別子演算部１０２及びコンテンツ再生装置３００の記憶装置識別子演算部３０２は特別な動作を実行せず、入力されたプリミティブＩＤ２６０をそのままメディアＩＤとして出力することができる。

【０１０７】

図１ないし１４の各構成要素はソフトウェア（ｓｏｆｔｗａｒｅ）または、ＦＰＧＡ（ｆｉｅｌｄ－ｐｒｏｇｒａｍｍａｂｌｅ　ｇａｔｅ　ａｒｒａｙ）やＡＳＩＣ（ａｐｐｌｉｃａｔｉｏｎ－ｓｐｅｃｉｆｉｃ　ｉｎｔｅｇｒａｔｅｄ　ｃｉｒｃｕｉｔ）のようなハードウェア（ｈａｒｄｗａｒｅ）を意味する。しかしながら、前記構成要素はソフトウェアまたはハードウェアに限定されることを意図せず、アドレッシング（ａｄｄｒｅｓｓｉｎｇ）できる記憶媒体に位置するように構成することもでき、一つまたはそれ以上のプロセッサを実行させるように構成することもできる。前記構成要素から提供される機能はさらに細分化した構成要素によって実現され得、複数の構成要素を合わせて特定の機能を実行する一つの構成要素として実現することもできる。

【０１０８】

図１５を参照して本発明のいくつかの実施形態による記憶装置について説明する。図１５を参照すると、記憶装置２００は不揮発性メモリ装置２０７及びコントローラ２０８を含む。前述した記憶装置２００は図１５に図示する形態で構成することができる。

【０１０９】

ここで不揮発性メモリ装置２０７は前述した少なくとも一つのメモリ装置２０６を含み得る。

【０１１０】

コントローラ２０８はホスト（Ｈｏｓｔ）及び不揮発性メモリ装置２０７に接続される

。コントローラ２０８はホストからの要請に応答して不揮発性メモリ装置２０７をアクセスするように構成される。例えば、コントローラ２０８は不揮発性メモリ装置２０７の読み取り、書き込み、消去、そして背景（ｂａｃｋｇｒｏｕｎｄ）の動作を制御するように構成される。コントローラ２０８は不揮発性メモリ装置２０７とホスト（Ｈｏｓｔ）との間にインターフェースを提供するように構成される。コントローラ２０８は不揮発性メモリ装置２０７を制御するためのファームウェア（ｆｉｒｍｗａｒｅ）を駆動するように構成される。

【０１１１】

例示的に、コントローラ２０８はＲＡＭ（Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）、プロセシングユニット（ｐｒｏｃｅｓｓｉｎｇ ｕｎｉｔ）、ホストインターフェース（ｈｏｓｔ ｉｎｔｅｒｆａｃｅ）、またメモリインターフェース（ｍｅｍｏｒｙ ｉｎｔｅｒｆａｃｅ）のようなよく知られている構成要素をさらに含む。ＲＡＭはプロセシングユニットの動作メモリ、不揮発性メモリ装置２０７とホストとの間のキャッシューメモリ、また不揮発性メモリ装置２０７とホストとの間のバッファメモリのうち少なくとも一つとして利用される。プロセシングユニットはコントローラ２０８の諸般動作を制御する。

【０１１２】

ホストインターフェースはホストとコントローラ２０８との間のデータ交換を行うためのプロトコルを含む。例示的に、コントローラ２０８はＵＳＢ（Ｕｎｉｖｅｒｓａｌ Ｓｅｒｉａｌ Ｂｕｓ）プロトコル、ＭＭＣ（ｍｕｌｔｉｍｅｄｉａ ｃａｒｄ）プロトコル、ＰＣＩ（ｐｅｒｉｐｈｅｒａｌ ｃｏｍｐｏｎｅｎｔ ｉｎｔｅｒｃｏｎｎｅｃｔｉｏｎ）プロトコル、ＰＣＩ－Ｅ（ＰＣＩ－ｅｘｐｒｅｓｓ）プロトコル、ＡＴＡ（Ａｄｖａｎｃｅｄ Ｔｅｃｈｎｏｌｏｇｙ Ａｔｔａｃｈｍｅｎｔ）プロトコル、Ｓｅｒｉａｌ－ＡＴＡプロトコル、Ｐａｒａｌｌｅｌ－ＡＴＡプロトコル、ＳＣＳＩ（ｓｍａｌｌ ｃｏｍｐｕｔｅｒ ｓｍａｌｌ ｉｎｔｅｒｆａｃｅ）プロトコル、ＥＳＤＩ（ｅｎｈａｎｃｅｄ ｓｍａｌｌ ｄｉｓｋ ｉｎｔｅｒｆａｃｅ）プロトコル、またＩＤＥ（Ｉｎｔｅｇｒａｔｅｄ Ｄｒｉｖｅ Ｅｌｅｃｔｒｏｎｉｃｓ）プロトコルなどのような多様なインターフェースプロトコルのうち少なくとも一つにより外部（ホスト）と通信するように構成される。メモリインターフェースは不揮発性メモリ装置２０７とインターフェーシングする。例えば、メモリインターフェースはＮＡＮＤインターフェースまたはＮＯＲインターフェースを含む。

【０１１３】

記憶装置２００はエラー訂正ブロックを追加して含むように構成され得る。エラー訂正ブロックはエラー訂正コード（ＥＣＣ）を用いて不揮発性メモリ装置２０７から読み取ったデータのエラーを検出して訂正するように構成される。例示的に、エラー訂正ブロックはコントローラ２０８の構成要素として提供される。エラー訂正ブロックは不揮発性メモリ装置２０７の構成要素として提供され得る。

【０１１４】

コントローラ２０８及び不揮発性メモリ装置２０７は一つの半導体装置に集積され得る。例示的に、コントローラ２０８及び不揮発性メモリ装置２０７は一つの半導体装置に集積され、メモリカードを構成することができる。

【０１１５】

例えば、コントローラ２０８及び不揮発性メモリ装置２０７は一つの半導体装置に集積され、ＰＣカード（ＰＣＭＣＩＡ、ｐｅｒｓｏｎａｌ ｃｏｍｐｕｔｅｒ ｍｅｍｏｒｙ ｃａｒｄ ｉｎｔｅｒｎａｔｉｏｎａｌ ａｓｓｏｃｉａｔｉｏｎ）、コンパクトフラッシュカード（ＣＦ）、スマートメディアカード（ＳＭ、ＳＭＣ）、メモリスティック、マルチメディアカード（ＭＭＣ、ＲＳ－ＭＭＣ、ＭＭＣｍｉｃｒｏ）、ＳＤカード（ＳＤ、ｍｉｎｉＳＤ、ｍｉｃｒｏＳＤ、ＳＤＨＣ）、ユニバーザルフラッシュ記憶装置（ＵＦＳ）などのようなメモリカードを構成する。

【０１１６】

コントローラ２０８及び不揮発性メモリ装置２０７は一つの半導体装置に集積され、半導体ドライブ（ＳＳＤ、Ｓｏｌｉｄ　Ｓｔａｔｅ　Ｄｒｉｖｅ）を構成することができる。半導体ドライブ（ＳＳＤ）は半導体メモリにデータを格納するように構成されるメモリ装置を含む。記憶装置２００が半導体ドライブ（ＳＳＤ）として利用される場合、記憶装置２００に接続されたホスト（Ｈｏｓｔ）の動作速度は画期的に改善される。前記ホストは記憶装置２００に一つ以上のコンテンツを暗号化するための及び暗号化されたコンテンツを格納するためのコンテンツ記録装置１００またはコンテンツ記憶サーバ４００であり得る。

【０１１７】

図１６を参照して本発明の一実施形態によるコンテンツを暗号化する方法について説明する。

【０１１８】

本実施形態によるコンテンツを暗号化する方法はコンテンツ記録装置１００がコンテンツを暗号化した後、暗号化コンテンツを記憶装置２００に格納することに要約される。

【０１１９】

記憶装置２００はメモリ装置を備え、前記メモリ装置に暗号化したコンテンツデータを格納することができる。

【０１２０】

記憶装置２００は磁気記憶装置を備え、前記磁気記憶装置に暗号化したコンテンツデータを格納することもできる。前記磁気記憶装置は、例えばハードディスクであり得る。

【０１２１】

記憶装置２００は光学記憶装置を備え、前記光学記憶装置に暗号化したコンテンツデータを格納することもできる。前記光学記憶装置は、例えばコンパクトディスクまたはＤＶＤディスクであり得る。

【０１２２】

記憶装置２００はプリミティブＩＤ（ｐｒｉｍｉｔｉｖｅ　ＩＤ）を格納する。一実施形態によれば、前記プリミティブＩＤはメディアＩＤを演算するために用いる基礎データであり得る。この際、前記プリミティブＩＤは前記メディアＩＤとは異なるデータである。別の実施形態によれば、前記プリミティブＩＤをそのまま前記メディアＩＤとして用いることもできる。

【０１２３】

コンテンツ記録装置１００は前記プリミティブＩＤを提供され（Ｓ１０２）、前記プリミティブＩＤから記憶装置２００の固有識別子であるメディアＩＤを演算することができる。

【０１２４】

前記プリミティブＩＤは第１プリミティブＩＤ及び第２プリミティブＩＤを含み、前記第２プリミティブＩＤが変換された第２識別子と第１プリミティブＩＤが結合することによって前記メディアＩＤが演算され得る。前記メディアＩＤを演算する方法については図１７ないし２０を参照してより詳細に説明する。

【０１２５】

コンテンツ記録装置１００は前記メディアＩＤを用いてコンテンツ暗号化鍵を生成する（Ｓ１０６）。コンテンツ暗号化鍵の生成に前記メディアＩＤを利用するということは、コンテンツ暗号化鍵生成において、前記メディアＩＤが少なくとも一度は入力されることを意味する。コンテンツ暗号化鍵の生成については図２０ないし図２４を参照して詳細に説明する。

【０１２６】

コンテンツ記録装置１００は前記コンテンツ暗号化鍵を用いてコンテンツを暗号化して前記コンテンツ原本をそのまま置いて暗号化コンテンツを追加して生成するか、または前記コンテンツ原本を暗号化コンテンツに変換することができる（Ｓ１０８）。

【０１２７】

前記暗号化コンテンツは記憶装置２００に提供され（Ｓ１１０）、記憶装置２００は前記暗号化コンテンツを格納する。図１に図示するように、コンテンツ記録装置１００は前記プリミティブＩＤを提供した記憶装置２００に前記暗号化コンテンツを格納した方が好ましい。前記暗号化コンテンツの復号化鍵は前記暗号化コンテンツが格納されている記憶装置のプリミティブＩＤから演算されるため、プリミティブＩＤを提供した記憶装置と暗号化コンテンツを格納する記憶装置が互いに異なってはならない。

【０１２８】

図１６に図示するように、コンテンツ記録装置１００は前記コンテンツ暗号化鍵を記憶装置２００に提供せず、前記暗号化コンテンツに含めることもない。したがって、前記暗号化コンテンツの復号化鍵を取得するためには前記暗号化コンテンツが格納された記憶装置２００のプリミティブＩＤを取得し、前記プリミティブＩＤから前記暗号化コンテンツが格納された記憶装置２００のメディアＩＤを演算し、前記メディアＩＤから復号化鍵を生成しなければならない。前記暗号化コンテンツを再生しようとするコンテンツ再生装置３００は前記暗号化コンテンツの復号化鍵を記憶装置２００から直接取得することはできない。したがって、図１６に図示するコンテンツを暗号化する方法によれば、暗号化コンテンツが異なる記憶装置に無断複製されても前記暗号化コンテンツが復号化されることを防止できる効果がある。このような効果については図２６を参照して後述する。

【０１２９】

コンテンツ記録装置１００が前記プリミティブＩＤから前記メディアＩＤを演算（Ｓ１０４）する方法について図１７ないし１９を参照してより詳細に説明する。

【０１３０】

図１７は記憶装置２００が第１パート及び第２パートを含み、記憶装置２００に第１パートを識別するための第１プリミティブＩＤ及び第２パート２０２を識別するための第２プリミティブＩＤが格納される場合のメディアＩＤを演算する方法について図示する。

【０１３１】

第１パート及び第２パートはそれぞれ記憶装置２００に備えられる素子またはモジュールを意味し、それぞれ特定機能を実行する素子グループまたはモジュールグループであり得る。例えば、第２パートはメモリ装置であり得、第１パートは前記メモリ装置を制御するコントローラであり得る。また、記憶装置２００に複数個のメモリ装置が備えられている場合、第１パートは前記複数個のメモリ装置中の一つを、第２パートは前記複数個のメモリ装置中の他の一つを意味し得る。

【０１３２】

図１７に図示するように、コンテンツ記録装置１００は記憶装置２００に格納された前記第１プリミティブＩＤ及び前記第２プリミティブＩＤを記憶装置２００から提供される（Ｓ１１４）。

【０１３３】

コンテンツ記録装置１００は前記第１プリミティブＩＤ及び前記第２プリミティブＩＤのうち少なくとも一つを用いて前記メディアＩＤを演算する（Ｓ１１６）。コンテンツ記録装置１００が前記第１プリミティブＩＤのみを用いて前記メディアＩＤを演算する場合、前記メディアＩＤは第１パートによって特定され、コンテンツ記録装置１００が前記第２プリミティブＩＤのみを用いて前記メディアＩＤを演算する場合、前記メディアＩＤは第２パート２０２によって特定され、コンテンツ記録装置１００が前記第１プリミティブＩＤ及び前記第２プリミティブＩＤを何れも用いて前記メディアＩＤを演算する場合、前記メディアＩＤは第１パート及び第２パート何れによって識別される。

【０１３４】

図１８は、記憶装置２００がコンテンツ記録装置１００に提供する第２プリミティブＩＤは第２パートの識別子が暗号化されたデータである場合を図示する。

【０１３５】

図１８に図示するように、コンテンツ記録装置１００は記憶装置２００に格納された前記第１プリミティブＩＤ及び前記第２プリミティブＩＤを記憶装置２００から提供され（

Ｓ１１４）、前記第２プリミティブＩＤを第２識別子に変換することができる（Ｓ１１８）。コンテンツ記録装置１００は前記メディアＩＤの演算において、前記第２プリミティブＩＤではない前記第２識別子を用いることができる。すなわち、コンテンツ記録装置１００は前記第１プリミティブＩＤ及び前記第２識別子のうち少なくとも一つを用いて前記メディアＩＤを演算することができる（Ｓ１２０）。

【０１３６】

前記第２プリミティブＩＤが第２パートの暗号化した識別子である理由は、第２パートの識別子が流出することを防止するためである。

【０１３７】

図１９ないし２０を参照して前記メディアＩＤを演算する方法について説明する。第２パートはメモリ装置であり得、第１パートはメモリ装置を制御するコントローラであり得る。

【０１３８】

メモリ装置２０６はコンテンツ記録装置１００を含む外部装置のデータ出力要請にもかかわらずデータを出力されない保護領域にメモリＩＤ（ＭＥＭＯＲＹ　ＩＤ）を格納することができる。前記メモリＩＤはメモリ装置２０６に付与した固有識別子である。

【０１３９】

メモリ装置２０６は前記メモリＩＤを暗号化した暗号化メモリＩＤ（ＥＮＣＲＹＰＴＥＤ　ＭＥＭＯＲＹ　ＩＤ）をさらに格納することができる。外部装置からのデータ出力要請にもかかわらず、データが出力されないメモリＩＤとは異なって、記憶装置２００はコンテンツ記録装置１００の要請に応じて前記暗号化メモリＩＤをコンテンツ記録装置１００に提供することができる（Ｓ１２２）。前記暗号化メモリＩＤは図１８を参照して説明した前記第２プリミティブＩＤと同一なものと理解することができる。

【０１４０】

先ず、メモリ装置２０６の他の識別子として使用できるメモリ派生ＩＤを生成する方法（Ｓ１０）について説明する。前記メモリ派生ＩＤは図１８を参照して説明した前記第２識別子と同一なものと理解することができる。

【０１４１】

コンテンツ記録装置１００は記憶装置２００から前記暗号化メモリＩＤを提供され（Ｓ１２２）、前記暗号化メモリＩＤを復号化して前記メモリＩＤを生成する（Ｓ１２４）。コンテンツ記録装置１００は記憶装置２００に格納された暗号化補助鍵を提供され、コンテンツ記録装置１００に格納された第２補助鍵で前記暗号化補助鍵を復号化して補助鍵を生成した後、前記補助鍵を用いて前記暗号化メモリＩＤをメモリＩＤで復号化することができる。

【０１４２】

コンテンツ記録装置１００は前記メモリＩＤを用いて第２認証情報を生成する（Ｓ１２６）。コンテンツ記録装置１００はランダムナンバーを生成し、前記ランダムナンバーを暗号化してセッション鍵を生成し、前記メモリＩＤと前記セッション鍵を所定の一方向性関数（ｏｎｅ－ｗａｙ　ｆｕｎｃｔｉｏｎ）に入力して前記第２認証情報を生成することができる。前記一方向性関数は、出力値から入力値を演算することができないものであって、例えば２個の演算子（ｏｐｅｒａｎｄ）を入力されるビット演算中の排他的論理合（ＸＯＲ）であり得る。

【０１４３】

一方、記憶装置２００も前記メモリＩＤを用いて第１認証情報を生成する（Ｓ１２８）。メモリ装置２０６には前記メモリＩＤ及び前記暗号化メモリＩＤ以外にも複数の補助鍵で構成された補助鍵セットがさらに格納されている場合もあり得、記憶装置２００は前記補助鍵セットの補助鍵中の一つの補助鍵を暗号化し、前記暗号化した補助鍵を、前記コンテンツ記録装置１００によって生成したランダムナンバーを暗号化鍵として再暗号化してセッション鍵を生成することができる。記憶装置２００は前記セッション鍵及び前記メモリＩＤを所定の一方向性関数に入力して前記第１認証情報を生成することができる。

【０１４４】
コンテンツ記録装置１００は前記第１認証情報を記憶装置２００から提供され（Ｓ１３０）前記第２認証情報と一致するかどうかを検証する（Ｓ１３２）。検証（Ｓ１３２）の結果、第１、２認証情報が一致しない場合、認証失敗として処理する（Ｓ１３４）。
【０１４５】
検証（Ｓ１３２）の結果、第１、２認証情報が一致する場合、前記メモリＩＤを用いてメモリ派生ＩＤを生成する（Ｓ１３６）。前記メモリ派生ＩＤは前記メモリＩＤとアプリケーション固有鍵（Ａｐｐｌｉｃａｔｉｏｎ Ｓｐｅｃｉｆｉｃ Ｓｅｃｒｅｔ Ｖａｌｕｅ：ＡＳＳＶ）を所定の一方向性関数に入力して生成することができる。
【０１４６】
前記アプリケーション固有鍵はコンテンツ記録装置１００で実行する各アプリケーションに対して固有な鍵が付与することである。例えば、音楽記録アプリケーション、映像記録アプリケーション、ソフトウェア記録アプリケーションごとに互いに異なる固有鍵を付与することができる。前記アプリケーション固有鍵は暗号化される前記コンテンツのタイプによって固有値を有するか、または暗号化される前記コンテンツの提供者識別情報によって固有値を有することができる。
【０１４７】
好ましくは、前記アプリケーション固有鍵は暗号化される前記コンテンツのタイプによって固有値を有することができる。前記コンテンツのタイプは、例えば動画、音楽、文書、ソフトウェアなどから一つを選択することができる。
【０１４８】
次に、図２０を参照してコンテンツ記録装置１００が記憶装置２００からコントローラ２０２の識別子を提供される（Ｓ２０）ことについて説明する。
【０１４９】
先ず、コンテンツ記録装置１００が記憶装置２００から第３認証情報を提供される（Ｓ１４０）。前述したように前記第３認証情報は記憶装置２００の認証書及び記憶装置２００に備えられたコントローラのプリミティブＩＤを含み得る。
【０１５０】
次に、コンテンツ記録装置１００と記憶装置２００との間に相互認証が行われる（Ｓ１４１）。前記相互認証は公開鍵基盤の認証であり得る。相互認証（Ｓ１４１）に失敗した場合、コンテンツ記録装置１００は認証失敗として処理する（Ｓ１４４）。コンテンツ記録装置１００は前記第３認証情報から前記コントローラＩＤ（ＣＯＮＴＲＯＬＬＥＲ ＩＤ）を取得することができる（Ｓ１４８）。
【０１５１】
コンテンツ記録装置１００は前記メモリ派生ＩＤ及び前記コントローラＩＤのうち少なくとも一つを用いてメディアＩＤを演算する。好ましくは、コンテンツ記録装置１００は前記メモリ派生ＩＤ及び前記コントローラＩＤを何れも用いてメディアＩＤを演算する。
【０１５２】
コンテンツ記録装置１００は前記メモリ派生ＩＤ及び前記コントローラＩＤを２進演算した結果データを前記メディアＩＤとして使用することができる。例えば、前記メモリ派生ＩＤ及び前記コントローラＩＤをＡＮＤ、ＯＲ、ＸＯＲなど２個の被演算子を要する２進演算した結果が前記メディアＩＤであり得る。
【０１５３】
コンテンツ記録装置１００は前記メモリ派生ＩＤ後に前記コントローラＩＤを文字列連結演算（ｓｔｒｉｎｇ ｃｏｎｃａｔｅｎａｔｉｏｎ）した結果データを前記メディアＩＤとして使用することもできる。前記メディアＩＤは前記コントローラＩＤ後に前記メモリ派生ＩＤを文字列連結演算した結果であり得る。
【０１５４】
次に、コンテンツ記録装置１００が前記メディアＩＤを用いてコンテンツ暗号化鍵を生成する動作（Ｓ１０６）について図２１ないし２４を参照して詳細に説明する。

【０１５５】
本発明による一実施形態によれば、コンテンツ記録装置１００は図２１に図示するように前記メディアＩＤ及びランダムナンバーを用いて前記コンテンツ暗号化鍵を生成することができる。すなわち、コンテンツ記録装置１００は予め定義したビット数のランダムナンバーを生成し（Ｓ１６０）、所定の関数またはアルゴリズムに前記ランダムナンバー及び前記メディアＩＤを入力して前記コンテンツ暗号化鍵を生成することができる（Ｓ１６２）。例えば、コンテンツ記録装置１００はＣＭＡＣ（Ｃｉｐｈｅｒ－ｂａｓｅｄ Ｍｅｓｓａｇｅ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｃｏｄｅ）アルゴリズムに前記メディアＩＤと前記ランダムナンバーを入力して算出するデータを前記コンテンツ暗号化鍵として使用することができる。
【０１５６】
前述したように、前記コンテンツ暗号化鍵は記憶装置２００に提供しない方が好ましい。
【０１５７】
ただし、コンテンツ記録装置１００は前記ランダムナンバーを記憶装置２００に提供して記憶装置２００に格納するようにする（Ｓ１０７）。前記ランダムナンバーを記憶装置２００に入力する理由は、コンテンツ復号化鍵の生成に前記ランダムナンバーが必要であるからである。
【０１５８】
本発明による一実施形態によれば、コンテンツ記録装置１００は図２２に図示するように前記メディアＩＤ及びコンテンツ識別子を用いて前記コンテンツ暗号化鍵を生成することもできる（Ｓ１６３）。前記コンテンツ識別子は各コンテンツと１対１に対応するデータであり得る。また、前記コンテンツ識別子と前記コンテンツは１対Ｎ（Ｎは２以上の自然数）の対応であり得る。例えば、コンテンツ種類によって前記コンテンツ識別子が割り当てられる。
【０１５９】
コンテンツ記録装置１００は所定の関数またはアルゴリズムに前記コンテンツ識別子及び前記メディアＩＤを入力して前記コンテンツ暗号化鍵を生成することができる（Ｓ１６３）。例えば、前記アルゴリズムはＣＭＡＣアルゴリズムであり得る。
【０１６０】
前述したように、前記コンテンツ暗号化鍵は記憶装置２００に提供しない方が好ましい。ただし、コンテンツ記録装置１００は前記コンテンツ識別子を記憶装置２００に提供して（Ｓ１１１）、記憶装置２００に格納するようにすることができる。前記コンテンツ識別子を記憶装置２００に入力する理由は、コンテンツ復号化鍵の生成に前記コンテンツ識別子が必要であるからである。
【０１６１】
一方、コンテンツ記録装置１００は前記コンテンツ識別子も記憶装置２００に提供しないことができる。すなわち、記憶装置２００はコンテンツ暗号化鍵だけでなく、コンテンツ識別子も格納しないことができる。この場合、記憶装置２００に格納した暗号化コンテンツを再生しようとする再生装置はコンテンツ識別子提供サーバ（図示せず）から前記暗号化コンテンツのコンテンツ識別子を提供され、前記提供されたコンテンツ識別子及び記憶装置２００の識別子を所定の関数またはアルゴリズムに入力してコンテンツ復号化鍵を生成することができる。
【０１６２】
本発明による一実施形態によれば、コンテンツ記録装置１００は図２３に図示するように、前記メディアＩＤのみ所定の関数に入力し、前記関数の出力データを前記コンテンツ暗号化鍵として使用することもできる。前記所定の関数は例えば一方向性関数であり得る。この場合、コンテンツ記録装置１００は記憶装置２００に復号化鍵を生成するためのいかなる値も伝送しない。記憶装置２００に格納された暗号化コンテンツを復号化しようとする装置はコンテンツ記録装置１００と同一に前記メディアＩＤのみ前記所定の関数に入

力し、前記関数の出力データを復号化鍵として用いることができる。すなわち、暗号化コンテンツを復号化しようとする装置は前記所定の関数を知っている場合、記憶装置２００のメディアＩＤから復号化鍵を取得することができる。

【０１６３】

本発明による一実施形態によれば、コンテンツ記録装置１００は図２４に図示するように前記メディアＩＤをそのまま前記コンテンツ暗号化鍵として用いることもできる（Ｓ１６７）。

【０１６４】

以下、本発明の一実施形態によるコンテンツ復号化方法について図２５ないし２７を参照して説明する。

【０１６５】

図２５は、本実施形態により、コンテンツ再生装置３００が記憶装置２００に格納された暗号化コンテンツを復号化する方法を示す順序図である。

【０１６６】

記憶装置２００には記憶装置２００のプリミティブＩＤ及び暗号化コンテンツがそれぞれ格納されている（Ｓ２００，Ｓ２０２）。

【０１６７】

コンテンツ再生装置３００は前記プリミティブＩＤを記憶装置２００から提供される。図２５には図示していないが、コンテンツ再生装置３００は前記プリミティブＩＤの提供を記憶装置２００に要請し、前記要請に対する応答として前記プリミティブＩＤを提供され得る。例えば、コンテンツ再生装置３００は前記暗号化コンテンツに対する再生命令がユーザから入力される場合、前記プリミティブＩＤの提供要請を行うことができる。

【０１６８】

コンテンツ再生装置３００は前記プリミティブＩＤを用いてメディアＩＤを演算する（Ｓ２０６）。コンテンツ再生装置３００がメディアＩＤを演算する動作は図１７ないし図２０を参照して説明したコンテンツ記録装置１００のメディアＩＤ演算動作と同様であり得る。

【０１６９】

コンテンツ再生装置３００は前記メディアＩＤを用いてコンテンツ復号化鍵を生成する（Ｓ２０８）。

【０１７０】

図２１に図示するコンテンツ記録装置１００によって記憶装置２００に格納された暗号化コンテンツを暗号化した場合、コンテンツ再生装置３００は記憶装置２００からランダムナンバーを読み込み、前記ランダムナンバー及び前記メディアＩＤを所定の関数またはアルゴリズムに入力してコンテンツ復号化鍵を生成することができる（Ｓ２０８）。

【０１７１】

図２２に図示するコンテンツ記録装置１００によって記憶装置２００に格納された暗号化コンテンツを暗号化した場合、コンテンツ再生装置３００は記憶装置２００からコンテンツ識別子を読み込むかまたは前記コンテンツ識別子提供サーバ（図示せず）からコンテンツ識別子を提供され、前記コンテンツ識別子及び前記メディアＩＤを所定の関数またはアルゴリズムに入力してコンテンツ復号化鍵を生成することができる（Ｓ２０８）。

【０１７２】

図２３に図示するコンテンツ記録装置１００によって記憶装置２００に格納された暗号化コンテンツを暗号化した場合、前記メディアＩＤを所定の関数またはアルゴリズムに入力してコンテンツ復号化鍵を生成することができる（Ｓ２０８）。

【０１７３】

図２４に図示するコンテンツ記録装置１００によって記憶装置２００に格納された暗号化コンテンツを暗号化した場合、コンテンツ再生装置３００は前記メディアＩＤをそのままコンテンツ復号化鍵として用いることができる（Ｓ２０８）。

【０１７４】

再び、図２５を参照してコンテンツ再生装置３００の復号化鍵を生成（Ｓ２０８）した後の動作について説明する。コンテンツ再生装置３００は記憶装置３００に格納された暗号化コンテンツを読み込んだ後（Ｓ２１０）、前記コンテンツ復号化鍵を用いて前記暗号化コンテンツを復号化し（Ｓ２１２）、復号化したコンテンツを再生する（Ｓ２１４）。

【０１７５】

図２６を参照して記憶装置Ｘ　２００に格納されていた暗号化コンテンツが他の記憶装置Ｙ　２０１に無断複製される場合、コンテンツ再生装置３００が記憶装置Ｙ　２０１に格納された暗号化コンテンツの復号化を失敗する動作について説明する。

【０１７６】

記憶装置Ｙ　２０１は記憶装置Ｘ　２００のプリミティブＩＤ　Ｘとは異なるプリミティブＩＤ　Ｙを格納している（Ｓ２０１）。

【０１７７】

また、記憶装置Ｘ　２００は図１に図示するコンテンツを暗号化する方法によって暗号化した暗号化コンテンツを格納している（Ｓ２０２）。以下、ユーザが記憶装置Ｘ　２００から記憶装置Ｙ　２０１に前記暗号化コンテンツを無断複製した状況（Ｓ２０３）と仮定する。

【０１７８】

ユーザがコンテンツ再生装置３００に前記記憶装置Ｙ　２０１を接続して前記コンテンツ再生装置３００に前記暗号化コンテンツの再生命令を入力する場合、コンテンツ再生装置３００は記憶装置Ｙ　２０１に格納されたプリミティブＩＤ　Ｙを提供される（Ｓ２０５）。

【０１７９】

コンテンツ再生装置３００は前記プリミティブＩＤ　Ｙを用いて記憶装置Ｙ　２０１のメディアＩＤを生成する（Ｓ２０７）。

【０１８０】

コンテンツ再生装置３００は前記メディアＩＤを用いて復号化鍵を生成する（Ｓ２０９）。

【０１８１】

コンテンツ再生装置３００は生成された復号化鍵を用いて記憶装置Ｙ　２０１から提供（Ｓ２１０）された暗号化コンテンツの復号化を試みる（Ｓ２１３）。しかしながら、生成（Ｓ２０９）した復号化鍵が前記暗号化コンテンツの復号化鍵と異なるため、コンテンツ再生装置３００は前記暗号化コンテンツを復号化することができない。

【０１８２】

したがって、コンテンツ再生装置３００は記憶装置Ｘ　２００から無断複製され、記憶装置Ｙ　２０１に格納された暗号化コンテンツを再生することができない（Ｓ２１５）。

【０１８３】

図２７は、コンテンツを暗号化する装置及びコンテンツを復号化する装置が何れもホスト装置１５０である場合のコンテンツ暗号化及び復号化方法について説明する。

【０１８４】

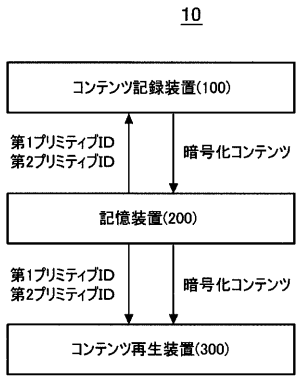
本実施形態によるホスト装置１５０は記憶装置２００に格納されたプリミティブＩＤを記憶装置２００から提供され（Ｓ１０２）、記憶装置２００のメディアＩＤを演算し（Ｓ１０４）、メディアＩＤから暗号化鍵を生成し（Ｓ１０６）、前記暗号化鍵を用いてコンテンツを暗号化し（Ｓ１０８）、及び暗号化したコンテンツを記憶装置２００に格納（Ｓ１１０）する。

【０１８５】

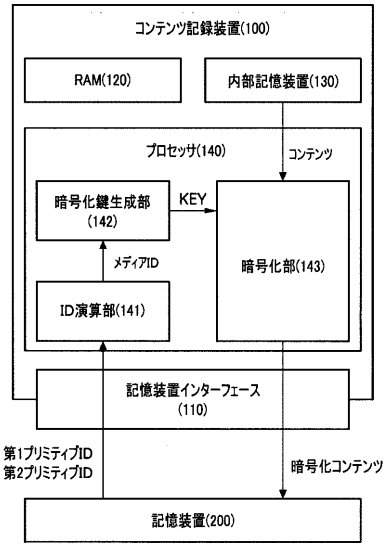
ホスト装置１５０は記憶装置２００に格納された暗号化コンテンツを復号化した後に再生するため、記憶装置２００に格納されたプリミティブＩＤを記憶装置２００から提供され（Ｓ２０４）、記憶装置２００のメディアＩＤを演算し（Ｓ２０６）、メディアＩＤから復号化鍵を生成し（Ｓ２０８）、前記暗号化鍵を用いて暗号化コンテンツを復号化し（Ｓ２１２）復号化したコンテンツを再生する（Ｓ２１４）。

【０１８６】
図２７は、ホスト装置１５０が図１６に図示する暗号化方法及び図２５に図示する復号化方法を実行することについてのみ図示しているが、本実施形態によるホスト装置１５０が実行する暗号化方法及び復号化方法は図１６、図２５に図示する暗号化、復号化方法に限定されない。すなわち、ホスト装置１５０は図１６ないし図２４を参照して説明した本発明の実施形態による暗号化方法を実行することができ、実行した暗号化方法に対応する復号化方法を実行することができる。
【０１８７】
図１６ないし２７の各ステップは、ソフトウェア（ｓｏｆｔｗａｒｅ）または、ＦＰＧＡ（ｆｉｅｌｄ－ｐｒｏｇｒａｍｍａｂｌｅ ｇａｔｅ ａｒｒａｙ）やＡＳＩＣ（ａｐｐｌｉｃａｔｉｏｎ－ｓｐｅｃｉｆｉｃ ｉｎｔｅｇｒａｔｅｄ ｃｉｒｃｕｉｔ）のようなハードウェア（ｈａｒｄｗａｒｅ）を介して行うことができる。しかしながら、前記構成要素はソフトウェアまたはハードウェアに限定されることを意図せず、アドレッシング（ａｄｄｒｅｓｓｉｎｇ）できる記憶媒体に位置するように構成され得、一つまたはそれ以上のプロセッサを実行させるように構成され得る。前記構成要素から提供する機能はさらに細分化した構成要素によって実現することができ、複数の構成要素を合わせて特定の機能を遂行する一つの構成要素として実現することもできる。
【０１８８】
本発明の概念はコンピュータ読み取りが可能な媒体上にコンピュータ読み取り可能なコードで実現することができる。前記コンピュータ読み取り可能な媒体はコンピュータ読み取りが可能な記憶媒体及びコンピュータ読み取り可能な伝送媒体を含み得る。前記コンピュータ読み取り可能な記憶媒体はデータを格納し、格納されたデータは今後コンピュータシステムによってリード（ｒｅａｄ）するデータ記憶装置であり得、例えば、ＲＯＭ、ＲＡＭ、ＣＤ－ＲＯＭ、磁気テープ、フロッピー（登録商標）ディスク、その他の光記憶装置であり得る。前記コンピュータ読み取り可能な記憶媒体はネットワークで連結されたコンピュータシステムに分散され、プログラムコードが記憶されて実行されることを分散処理方式によって行うようにすることができる。前記コンピュータ読み取り可能な伝送媒体は有無線インターネットに接続することにより搬送波または搬送信号（ｃａｒｒｉｅｒ ｗａｖｅ、ｃａｒｒｉｅｒ ｓｉｇｎａｌ）を送信するものであり得る。
【０１８９】
以上添付する図面を参照して本発明の実施形態について説明したが、本発明が属する技術分野で通常の知識を有する者は、本発明がその技術的思想や必須の特徴を変更しない範囲で他の具体的な形態で実施され得るということを理解することができる。したがって、上記実施形態はすべての面で例示的なものであり、限定的なものではないと理解しなければならない。
【符号の説明】
【０１９０】
１００　コンテンツ記録装置
１５０　ホスト装置
２００　記憶装置
３００　コンテンツ再生装置

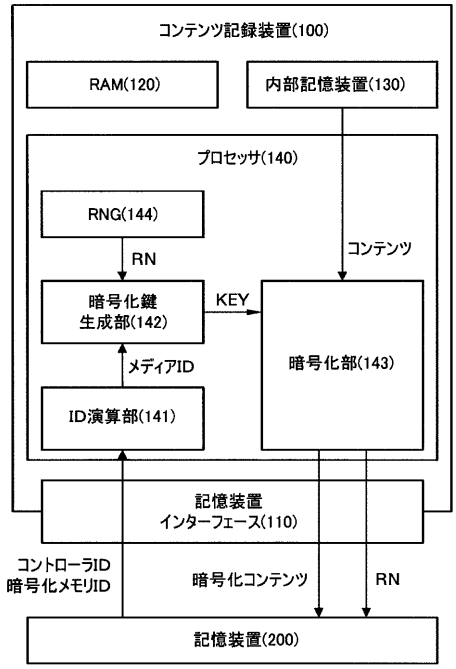
【図１】


10
コンテンツ記録装置(100)
第1プリミティブID
第2プリミティブID
暗号化コンテンツ
記憶装置(200)
第1プリミティブID
第2プリミティブID
暗号化コンテンツ
コンテンツ再生装置(300)

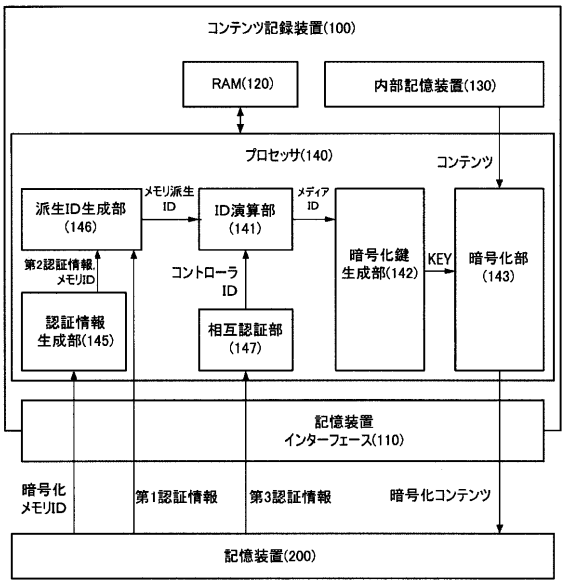
【図２】


コンテンツ記録装置(100)
RAM(120)
内部記憶装置(130)
プロセッサ(140)
コンテンツ
暗号化鍵生成部
(142)
KEY
メディアID
暗号化部(143)
ID演算部(141)
記憶装置インターフェース
(110)
第1プリミティブID
第2プリミティブID
暗号化コンテンツ
記憶装置(200)

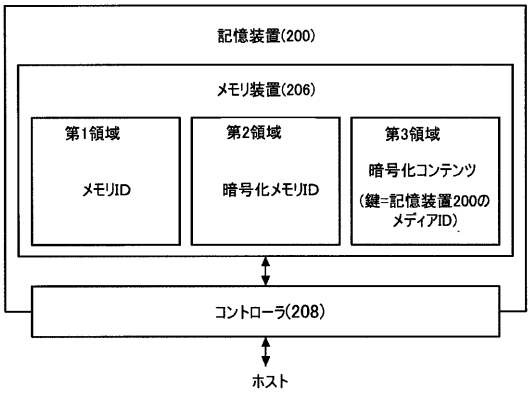
【図３】


コンテンツ記録装置(100)
RAM(120)
内部記憶装置(130)
プロセッサ(140)
RNG(144)
RN
コンテンツ
暗号化鍵
生成部(142)
KEY
メディアID
暗号化部(143)
ID演算部(141)
記憶装置
インターフェース(110)
コントローラID
暗号化メモリID
暗号化コンテンツ
RN
記憶装置(200)

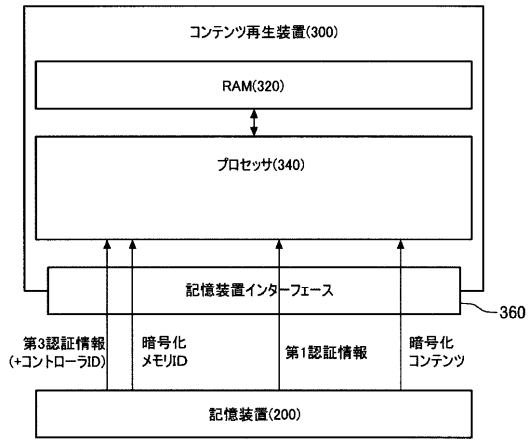
【図４】


コンテンツ記録装置(100)
RAM(120)
内部記憶装置(130)
プロセッサ(140)
コンテンツ
派生ID生成部
(146)
メモリ派生
ID
ID演算部
(141)
メディア
ID
暗号化鍵
生成部(142)
KEY
暗号化部
(143)
第2認証情報
メモリID
コントローラ
ID
認証情報
生成部(145)
相互認証部
(147)
記憶装置
インターフェース(110)
暗号化
メモリID
第1認証情報
第3認証情報
暗号化コンテンツ
記憶装置(200)

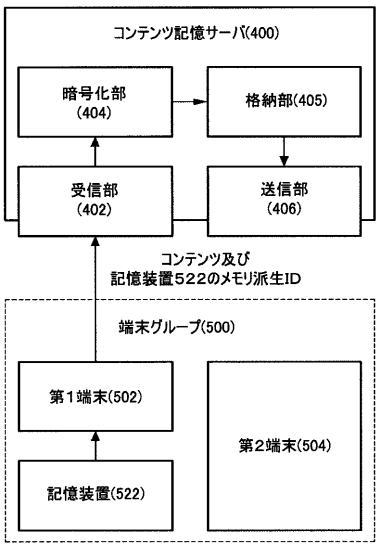
【図５】


記憶装置(200)
メモリ装置(206)
第1領域
メモリID
第2領域
暗号化メモリID
第3領域
暗号化コンテンツ
(鍵=記憶装置200のメディアID)
コントローラ(208)
ホスト

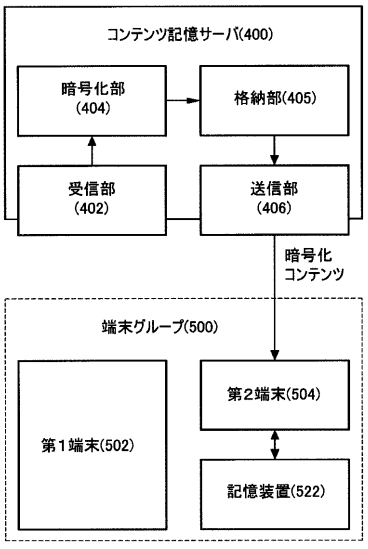
【図６】


コンテンツ再生装置(300)
RAM(320)
プロセッサ(340)
記憶装置インターフェース
360
第3認証情報
(+コントローラID)
暗号化
メモリID
第1認証情報
暗号化
コンテンツ
記憶装置(200)

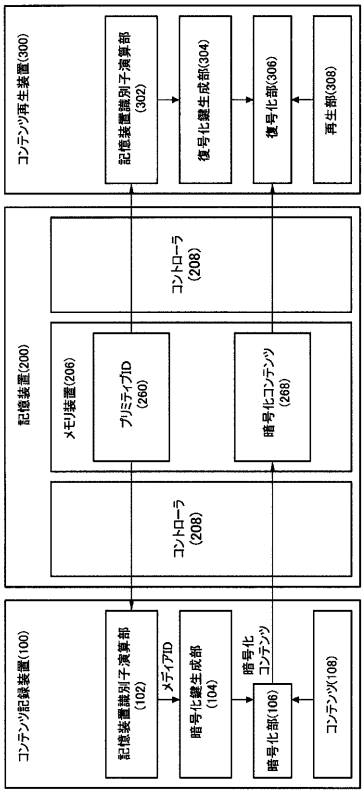
【図７】


コンテンツ記憶サーバ(400)
暗号化部
(404)
格納部(405)
受信部
(402)
送信部
(406)
コンテンツ及び
記憶装置522のメモリ派生ID
端末グループ(500)
第1端末(502)
記憶装置(522)
第2端末(504)

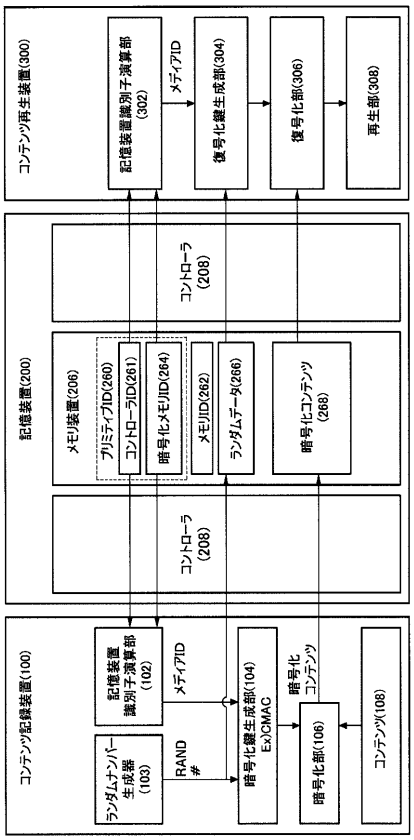
【図８】


コンテンツ記憶サーバ(400)
暗号化部
(404)
格納部(405)
受信部
(402)
送信部
(406)
暗号化
コンテンツ
端末グループ(500)
第1端末(502)
第2端末(504)
記憶装置(522)

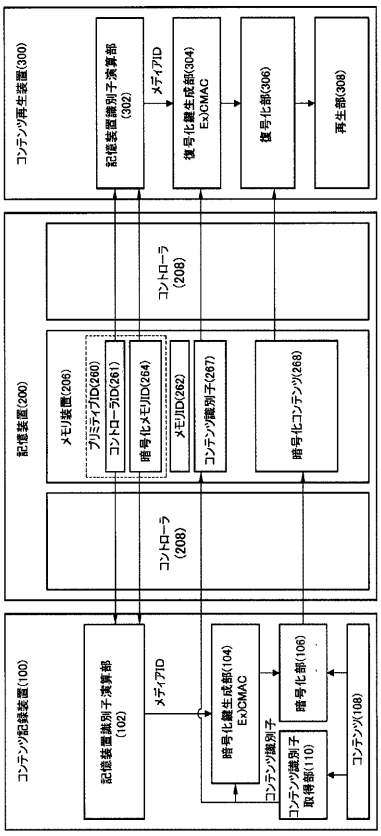
【図９】



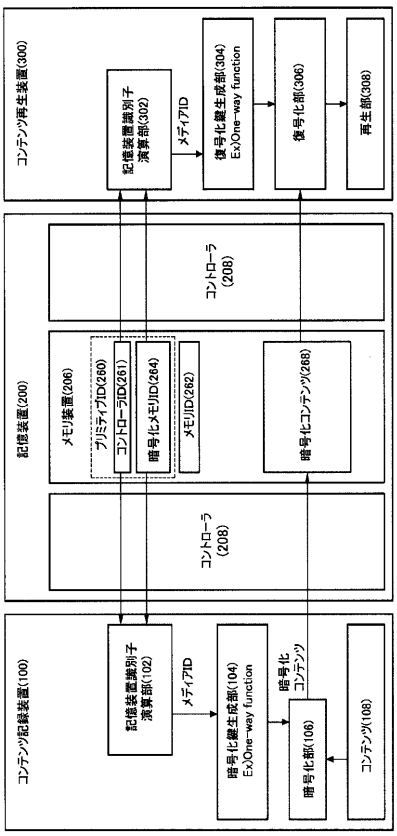
【図１０】



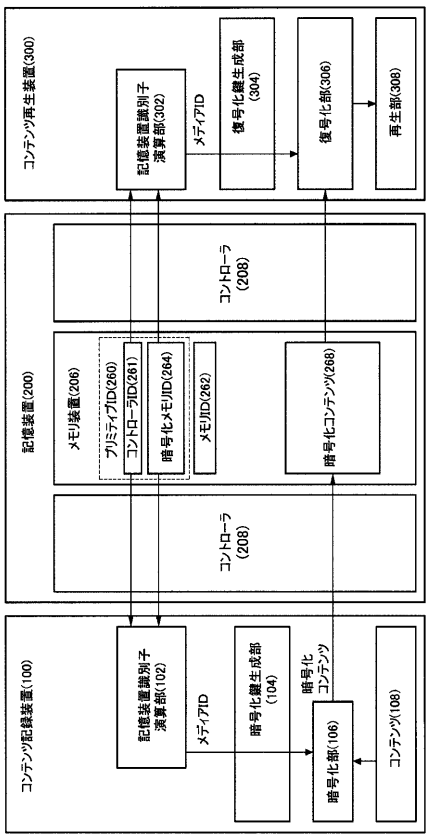
【図１１】



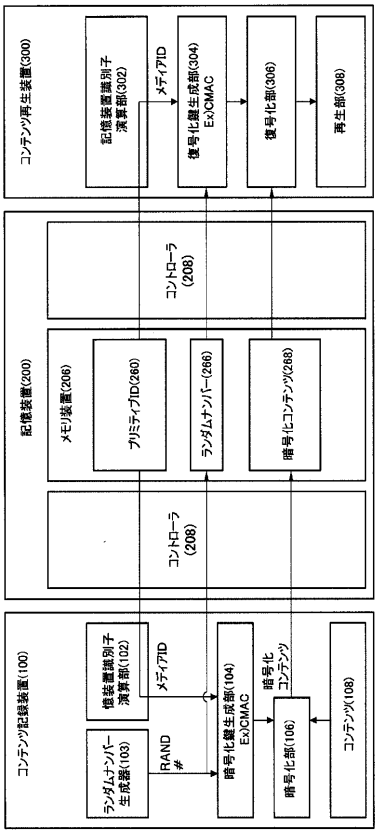
【図１２】



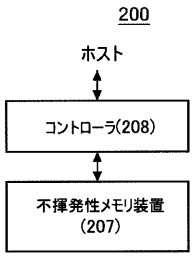
【図１３】



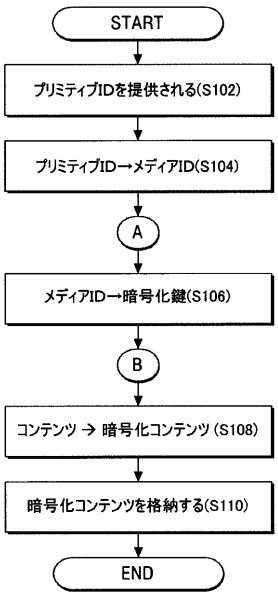
【図１４】



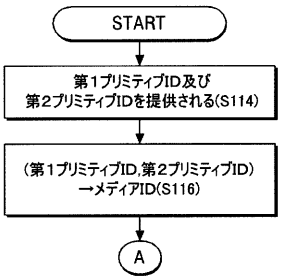
【図１５】



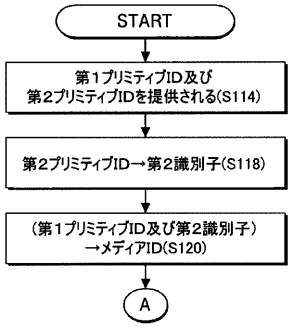
【図１６】



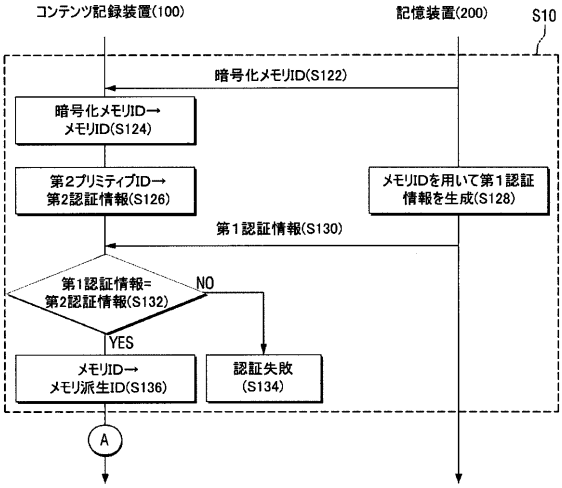
【図１７】



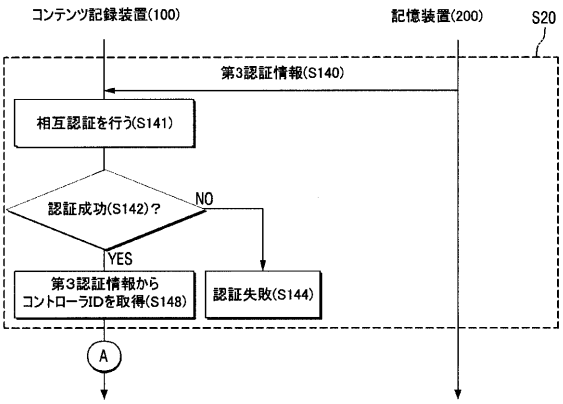
【図１８】



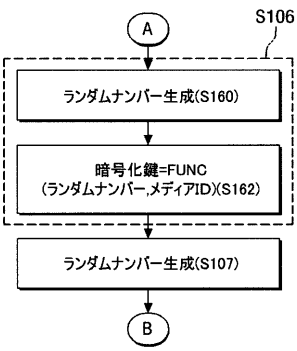
【図１９】



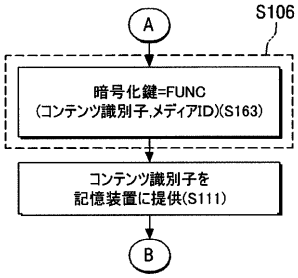
【図２０】



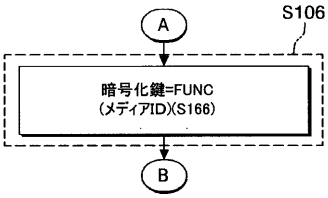
【図２１】



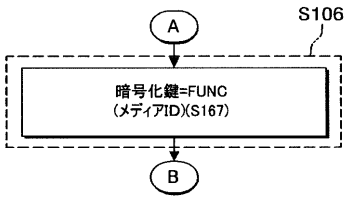
【図２２】



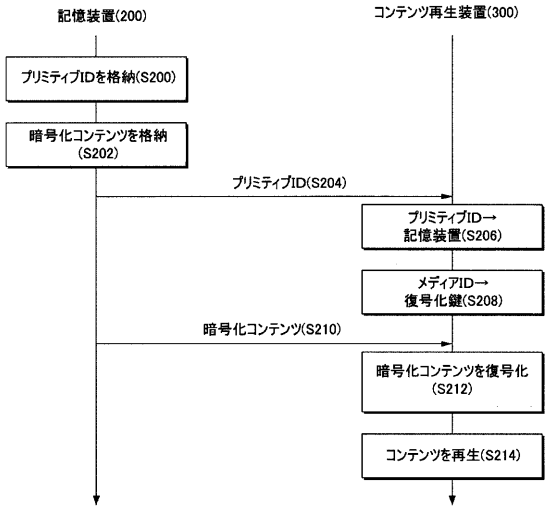
【図２３】



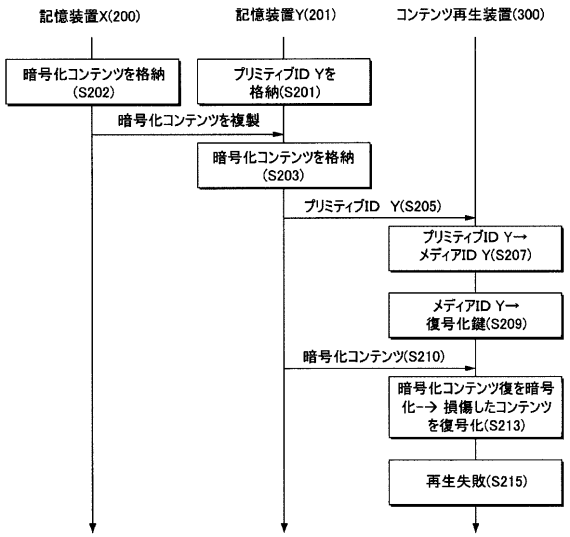
【図２４】



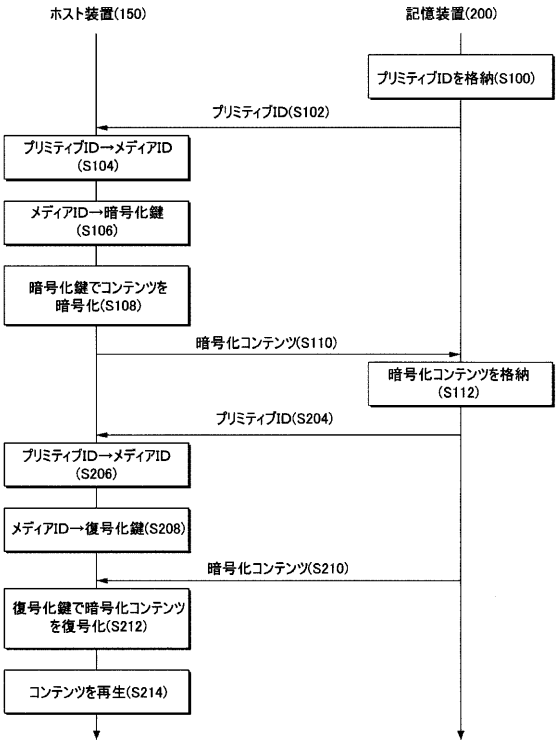
【図２５】


記憶装置(200)
コンテンツ再生装置(300)
プリミティブIDを格納(S200)
暗号化コンテンツを格納
(S202)
プリミティブID(S204)
プリミティブID→
記憶装置(S206)
メディアID→
復号化鍵(S208)
暗号化コンテンツ(S210)
暗号化コンテンツを復号化
(S212)
コンテンツを再生(S214)

【図２６】


記憶装置X(200)
記憶装置Y(201)
コンテンツ再生装置(300)
暗号化コンテンツを格納
(S202)
プリミティブID Yを
格納(S201)
暗号化コンテンツを複製
暗号化コンテンツを格納
(S203)
プリミティブID Y(S205)
プリミティブID Y→
メディアID Y(S207)
メディアID Y→
復号化鍵(S209)
暗号化コンテンツ(S210)
暗号化コンテンツ復を暗号
化→ 損傷したコンテンツ
を復号化(S213)
再生失敗(S215)

【図２７】


ホスト装置(150)
記憶装置(200)
プリミティブIDを格納(S100)
プリミティブID(S102)
プリミティブID→メディアID
(S104)
メディアID→暗号化鍵
(S106)
暗号化鍵でコンテンツを
暗号化(S108)
暗号化コンテンツ(S110)
暗号化コンテンツを格納
(S112)
プリミティブID(S204)
プリミティブID→メディアID
(S206)
メディアID→復号化鍵(S208)
暗号化コンテンツ(S210)
復号化鍵で暗号化コンテンツ
を復号化(S212)
コンテンツを再生(S214)

フロントページの続き

(72)発明者　王　▲衛▼新
大韓民国京畿道水原市靈通區靈通１洞（番地なし）　水原メールセンターピーオーボックス１２０
(72)発明者　趙　熙昌
大韓民国ソウル特別市瑞草區良才洞３１２－４　江南パークヴィル２０１號
(72)発明者　張　炯碩
大韓民国京畿道水原市靈通區網浦洞（番地なし）　ドンスウォンエルジーヴィレッジ２次アパート２０２棟１８０２號

Ｆターム(参考) 5J104 EA26　JA03　NA43　PA07　PA10