(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6144108号
(P6144108)
(45)発行日　平成29年6月7日(2017.6.7)　(24)登録日　平成29年5月19日(2017.5.19)

(51)Int.Cl.　　F I
H04L 9/08 (2006.01)　　H04L 9/00 601D
H04L 9/32 (2006.01)　　H04L 9/00 601E
　　H04L 9/00 675A

請求項の数 8　(全 30 頁)

(21)出願番号　特願2013-100918(P2013-100918)
(22)出願日　平成25年5月13日(2013.5.13)
(65)公開番号　特開2013-247676(P2013-247676A)
(43)公開日　平成25年12月9日(2013.12.9)
審査請求日　平成28年5月11日(2016.5.11)
(31)優先権主張番号　10-2012-0055527
(32)優先日　平成24年5月24日(2012.5.24)
(33)優先権主張国　韓国(KR)

(73)特許権者　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　100110364
弁理士　実広　信哉
(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

最終頁に続く

(54)【発明の名称】装置識別子とユーザ認証情報を基盤としたセキュア鍵生成装置

(57)【特許請求の範囲】
【請求項１】
第１記憶装置に格納された第１プリミティブＩＤを提供され、前記第１プリミティブＩＤから前記第１記憶装置の固有識別子である第１メディアＩＤを演算するＩＤ演算部と、
ユーザを認証するための認証情報をセキュア鍵生成部に提供する認証情報提供部と、
前記第１メディアＩＤ及び前記認証情報を全て用いてセキュア鍵を生成するセキュア鍵生成部を含み、
前記第１プリミティブＩＤは、前記第１記憶装置に備えられた第１メモリ素子の固有識別子である第１メモリＩＤを暗号化した第１暗号化メモリＩＤを含み、
前記ＩＤ演算部は、前記第１暗号化メモリＩＤを前記第１メモリＩＤに復号化し、前記第１メモリＩＤから第１メモリ派生ＩＤを演算し、前記第１メモリ派生ＩＤを用いて前記第１メディアＩＤを演算するセキュア鍵生成装置。
【請求項２】
前記第１プリミティブＩＤは、前記第１メディアＩＤ演算に用いる一つ以上の識別用データであり、前記第１メディアＩＤとは異なるデータである請求項１に記載のセキュア鍵生成装置。
【請求項３】
前記第１プリミティブＩＤは、前記第１記憶装置に備えられた第１コントローラの固有識別子である第１コントローラＩＤを含み、
前記ＩＤ演算部は、前記第１コントローラＩＤ及び前記第１メモリ派生ＩＤを全て用い

て前記第１メディアＩＤを演算する請求項１に記載のセキュア鍵生成装置。
【請求項４】
前記認証情報提供部は、前記ユーザから前記認証情報を入力され、
前記セキュア鍵生成部は、前記第１メディアＩＤとユーザから入力された認証情報を全て用いて前記セキュア鍵を生成する請求項１に記載のセキュア鍵生成装置。
【請求項５】
記憶装置に格納されたプリミティブＩＤを提供され、プロセッサに提供する記憶装置インターフェースと、
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及びユーザを認証するための認証情報を全て用いてセキュア鍵を生成するプロセッサを含み、
前記プリミティブＩＤは、前記記憶装置に備えられた第１メモリ素子の固有識別子である第１メモリＩＤを暗号化した第１暗号化メモリＩＤを含み、
前記プロセッサは、前記第１暗号化メモリＩＤを前記第１メモリＩＤに復号化し、前記第１メモリＩＤから第１メモリ派生ＩＤを演算し、前記第１メモリ派生ＩＤを用いて前記メディアＩＤを演算するセキュア鍵生成装置。
【請求項６】
メモリ素子の固有識別子であるメモリＩＤ及び前記メモリＩＤを暗号化した暗号化メモリＩＤを格納するメモリ素子と、
ホスト装置からユーザを認証するための認証情報を提供され、セキュア鍵生成部に提供し、前記ホスト装置からコンテンツを提供され、暗号化部に提供するホストインターフェースと、
前記メモリ素子から前記暗号化メモリＩＤを読み込み、前記暗号化メモリＩＤを復号化して前記メモリＩＤを取得し、前記メモリＩＤを用いて前記メモリ素子の他の固有識別子であるメモリ派生ＩＤを生成する派生ＩＤ演算部と、
前記認証情報及び前記前記メモリ派生ＩＤを全て用いてセキュア鍵を生成するセキュア鍵生成部と、
前記セキュア鍵を用いて前記コンテンツを暗号化して前記メモリ素子に格納する暗号化部を含む記憶装置。
【請求項７】
前記認証情報は、ＳＤカード規格（ＳＤ　Ｃａｒｄ　Ｓｔａｎｄａｒｄ）コマンドのパラメータとして含まれて前記ホスト装置から提供される請求項６に記載の記憶装置。
【請求項８】
記憶装置をセキュア鍵生成装置に電気的に接続し、
前記セキュア鍵生成装置が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、
前記セキュア鍵生成装置がユーザから前記ユーザを認証するための認証情報を直接入力されるか、またはネットワークを介して接続された他の装置から前記認証情報を提供され、
前記セキュア鍵生成装置が前記メディアＩＤ及び前記認証情報を全て用いてセキュア鍵を生成することを含み、
前記プリミティブＩＤは、前記記憶装置に備えられた第１メモリ素子の固有識別子である第１メモリＩＤを暗号化した第１暗号化メモリＩＤを含み、
前記演算は、前記第１暗号化メモリＩＤを前記第１メモリＩＤに復号化し、前記第１メモリＩＤから第１メモリ派生ＩＤを演算し、前記第１メモリ派生ＩＤを用いて前記メディアＩＤを演算するセキュア鍵の生成方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明はセキュア鍵生成装置に関するものである。より詳細には装置識別子とユーザ暗

号などユーザ認証情報をすべて使用してセキュア鍵を生成することによって特定装置及び特定ユーザに同時に従属するセキュア鍵を生成する装置、前記セキュア鍵を活用する記憶装置及びセキュア鍵の生成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、小型化の傾向である。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、安い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。前記暗号化は特定暗号化鍵を用いて行う。

【０００５】

一方、特定装置に対してのみ有効なセキュア鍵を利用した暗号化及び復号化技術は、前記特定装置を使用するとデータに対するセキュリティが解除するという問題点がある。

【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、特定装置及び特定ユーザに同時に従属するセキュア鍵を生成する装置、前記セキュア鍵を用いてコンテンツを自体暗号化格納する記憶装置及びセキュア鍵の生成方法を提供するものである。

【０００７】

本発明が解決しようとする他の技術的課題は、特定装置の識別子及びユーザによって入力されたユーザ認証情報を全て用いて演算したセキュア鍵を生成する装置、前記セキュア鍵を用いてコンテンツを自体暗号化格納する記憶装置及びセキュア鍵の生成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また他の技術的課題は、信頼できるコンピューティング（Ｔｒｕｓｔｅｄ　Ｃｏｍｐｕｔｉｎｇ）を支援するホスト装置で前記セキュア鍵を安全に生成する装置を提供するものである。

【０００９】

本発明が解決しようとするまた他の技術的課題は、セキュア鍵を生成することにおいて装置識別子及びユーザ認証情報及び生成されたセキュア鍵が流出しないように信頼できる実行環境でセキュア鍵を生成するホスト装置を提供するものである。

【００１０】

本発明の技術的課題は、以上で言及した技術的課題に制限されず、言及されていない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であろう。

【課題を解決するための手段】

【００１１】

前記技術的課題を達成するための本発明の一実施形態によるセキュア鍵生成装置は、第１記憶装置に格納された第１プリミティブＩＤを提供され、前記第１プリミティブＩＤから前記第１記憶装置の固有識別子である第１メディアＩＤを演算するＩＤ演算部と、ユーザを認証するための認証情報をセキュア鍵生成部に提供する認証情報提供部と、前記第１メディアＩＤ及び前記認証情報を全て用いてセキュア鍵を生成するセキュア鍵生成部を含む。前記プリミティブＩＤは、前記メディアＩＤ演算に用い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。前記認証情報提供部は、前記ユーザから前記認証情報を入力され得る。

【００１２】

一実施形態によれば、前記セキュア鍵生成装置が互いに異なる第１記憶装置に接続されるか、または第２記憶装置に接続され得る。前記セキュア鍵生成装置が前記第１記憶装置に接続される場合、前記ＩＤ演算部は第１記憶装置に格納された第１プリミティブＩＤを提供され、前記第１プリミティブＩＤから前記第１記憶装置の固有識別子である第１メディアＩＤを演算し、前記セキュア鍵生成部は、前記第１メディアＩＤ及び前記認証情報を全て用いてセキュア鍵を生成することができる。これに対し、前記セキュア鍵生成装置が前記第２記憶装置に接続される場合、前記ＩＤ演算部は第２記憶装置に格納された第２プリミティブＩＤを提供され、前記第２プリミティブＩＤから前記第２記憶装置の固有識別子である第２メディアＩＤを演算し、前記セキュア鍵生成部は、前記第２メディアＩＤ及び前記認証情報を全て用いて他のセキュア鍵を生成し、前記第２プリミティブＩＤは、前記第２メディアＩＤを生成するために使用するＩＤデータであり、前記第１プリミティブＩＤと異なる。

【００１３】

また、前記セキュア鍵生成装置が前記第１記憶装置に接続される場合、前記第１プリミティブＩＤは前記第１記憶装置に備えられた第１メモリ素子の固有識別子である第１メモリＩＤを暗号化した第１暗号化メモリＩＤであり、前記ＩＤ演算部は前記第１暗号化メモリＩＤを前記第１メモリＩＤで復号化し、前記第１メモリＩＤから第１メモリ派生ＩＤを演算し、前記第１メモリ派生ＩＤを前記第１メディアＩＤとして使用する。これに対し、前記セキュア鍵生成装置が前記第２記憶装置に接続される場合、前記ＩＤ演算部は第２記憶装置に格納された第２プリミティブＩＤを提供され、前記第２プリミティブＩＤから前記第２記憶装置の固有識別子である第２メディアＩＤを演算し、前記セキュア鍵生成部は、前記第２メディアＩＤ及び前記認証情報を全て用いて他のセキュア鍵を生成し、前記第２プリミティブＩＤは、前記第２記憶装置に備えられた第２メモリ素子の固有識別子である第２メモリＩＤを暗号化した第２暗号化メモリＩＤであり、前記ＩＤ演算部は、前記第２暗号化メモリＩＤを前記第２メモリＩＤで復号化し、前記第２メモリＩＤから第２メモリ派生ＩＤを演算し、前記第２メモリ派生ＩＤを前記第２メディアＩＤとして使用する。

【００１４】

一実施形態によれば、前記プリミティブＩＤは、前記記憶装置に備えられたメモリ素子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ＩＤ演算部は、前記暗号化メモリＩＤを前記メモリＩＤで復号化し、前記メモリＩＤからメモリ派生ＩＤを演算し、前記メモリ派生ＩＤを前記メディアＩＤとして使用することができる。また、前記ＩＤ演算部は、前記メモリ素子の認証プロセスを行い、前記認証プロセスの実行結果、メモリ素子の認証に成功した場合に限り、前記メモリＩＤから前記メモリ派生ＩＤを演算することができる。

【００１５】

一実施形態によれば、前記プリミティブＩＤは前記記憶装置に備えられたメモリ素子の固有識別子であるメモリＩＤであり得る。また、前記メディアＩＤは前記メモリＩＤと同一であり得る。したがって、本実施形態によれば、ＩＤ演算部は、前記記憶装置から前記メモリＩＤを提供され、前記メモリＩＤを前記メディアＩＤとして前記セキュア鍵生成部に提供することができる。

【００１６】

一実施形態によれば、前記プリミティブ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を含み、前記ＩＤ演算部は、前記コントローラＩＤを用いて前記メディアＩＤを演算することもできる。前記ＩＤ演算部は、前記コントローラと相互認証を行い、前記相互認証過程で前記コントローラＩＤを提供され得る。

【００１７】

一実施形態によれば、前記プリミティブＩＤは、前記記憶装置に備えられたメモリ素子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及び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を含み、前記ＩＤ演算部は、前記暗号化メモリＩＤを前記メモリＩＤで復号化し、前記メモリＩＤからメモリ派生ＩＤを演算し、前記コントローラＩＤ及び前記メモリ派生ＩＤを全て用いて前記メディアＩＤを演算することもできる。

【００１８】

前記技術的課題を達成するための本発明の他の実施形態によるセキュア鍵生成装置は、記憶装置に格納されたプリミティブＩＤを提供され、プロセッサに提供する記憶装置インターフェース、及び前記プリミティブ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及びユーザを認証するための認証情報を全て用いてセキュア鍵を生成するプロセッサを含む。

【００１９】

一実施形態によれば、前記プロセッサは、非セキュア実行モード及びセキュア実行モードのうち一つで動作し、前記認証情報は、前記プロセッサが非セキュア実行モードからセキュア実行モードに動作状態を切り替えるためのモード切り替え認証に使用され得る。前記プロセッサは、前記非セキュア実行モードでの命令実行を担う非セキュア仮想コア及び前記セキュア実行モードでの命令実行を担うセキュア仮想コアを含み、前記非セキュア仮想コアは前記認証情報を検証し、前記検証の成功時にインタラプト信号を生成し、前記プロセッサは、前記インタラプト信号に応答して動作モードを非セキュア実行モードからセキュア実行モードに切り替え、前記セキュア仮想コアは、前記セキュア鍵を生成することができる。前記セキュア鍵生成装置は、ＲＡＭをさらに含み、前記ＲＡＭは、前記非セキュア仮想コアで実行される命令によってアクセスできる第１領域及び前記セキュア仮想コアで実行される命令によってアクセスできる前記第１領域と重ならない第２領域を含み得る。前記非セキュア仮想コアで実行される命令は前記第２領域にアクセスできない方が好ましい。

【００２０】

一実施形態によれば、前記セキュア鍵生成装置は、前記認証情報を入力され前記プロセッサに提供する入力部をさらに含み、前記プロセッサは、非セキュア実行モード及びセキュア実行モードのうち一つで動作するものであり、前記セキュア実行モードで前記認証情報を前記入力部から提供されることと、前記セキュア鍵を生成することを実行することができる。前記セキュア鍵生成装置は、ＲＡＭをさらに含み、前記ＲＡＭは、前記プロセッサがセキュア実行モードで動作する時にのみアクセス可能なセキュア領域を含み、前記認証情報、プリミティブＩＤ、メディアＩＤ及びセキュア鍵は前記セキュア領域に格納され得る。

【００２１】

前記技術的課題を達成するための本発明のまた他の実施形態によるホスト装置は、記憶装置と接続され、前記プリミティブＩＤを前記記憶装置から提供され、システムオンチップ（Ｓｙｓｔｅｍ－ｏｎ－Ｃｈｉｐ、ＳｏＣ）に提供する記憶装置インターフェースと、前記記憶装置インターフェースと接続されたシステムオンチップを含む。前記システムオンチップは、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及びユーザを認証するための認証情報を全て用いてセキュア鍵を生成する周辺ロジック（ｐｈｅｒｉｐｅｒａｌ　ｌｏｇｉｃ）を含み得る。前記システムオンチップは、前記認証情報を提供され、前記周辺ロジックに提供するコア（Ｃｏｒｅ）をさらに含み得る。前記周辺ロジックは、前記記憶装置インターフェースと前記コアと

の間のデータパス（ｄａｔａ　ｐａｔｈ）上に接続されたものであり得る。前記ホスト装置は、前記システムオンチップによって制御され、ユーザから前記認証情報を入力され前記システムオンチップに提供する入力部をさらに含み得る。前記システムオンチップは、前記セキュア鍵を格納するレジスタをさらに含み得る。前記周辺ロジックは、前記セキュア鍵を用いてコンテンツを暗号化した後、前記記憶装置インターフェースを介して前記記憶装置に提供することができる。前記記憶装置インターフェースは、前記記憶装置から暗号化コンテンツを提供され、前記システムオンチップに提供し、前記周辺ロジックは、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及びユーザを認証するための認証情報を全て用いて前記暗号化コンテンツを復号化するためのセキュア鍵を生成することができる。

【００２２】

前記技術的課題を達成するための本発明のまた他の実施形態による記憶装置は、メモリＩＤ及び前記メモリＩＤを暗号化した暗号化メモリＩＤを格納するメモリ素子と、ホスト装置からユーザを認証するための認証情報を提供され、セキュア鍵生成部に提供し、前記ホスト装置からコンテンツを提供され、暗号化部に提供するホストインターフェースと、前記メモリ素子から前記暗号化メモリＩＤを読み込み、前記暗号化メモリＩＤを復号化し、前記メモリＩＤを取得し、前記メモリＩＤを用いて前記メモリ素子の他の固有識別子であるメモリ派生ＩＤを生成する派生ＩＤ演算部と、前記認証情報及び前記前記メモリ派生ＩＤを全て用いてセキュア鍵を生成するセキュア鍵生成部、及び前記セキュア鍵を用いて前記コンテンツを暗号化して前記メモリ素子に格納する暗号化部を含む。前記メモリＩＤは、前記メモリ素子の固有識別子であり得る。前記認証情報は、ＳＤカード規格（ＳＤ　Ｃａｒｄ　Ｓｔａｎｄａｒｄ）コマンドのパラメータに含まれ、前記ホスト装置から提供され得る。

【００２３】

一実施形態によれば、前記記憶装置は、ランダムナンバー生成器をさらに含み、前記セキュア鍵生成部は、前記ランダムナンバー生成器によって生成されたランダムナンバーをさらに用いて前記セキュア鍵を生成することができる。前記記憶装置は、ＴＣＧ（Ｔｒｕｓｔｅｄ　Ｃｏｍｐｕｔｉｎｇ　Ｇｒｏｕｐ）のＯＰＡＬ　ＳＳＣ（Ｏｐａｌ　Ｓｅｃｕｒｉｔｙ　Ｓｕｂｓｙｓｔｅｍ　Ｃｌａｓｓ）規格に従い動作するものであり得る。

【００２４】

前記技術的課題を達成するための本発明のまた他の実施形態によるセキュア鍵の生成方法は、記憶装置をセキュア鍵生成装置に電気的に接続し、前記セキュア鍵生成装置が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、前記セキュア鍵生成装置がユーザから前記ユーザを認証するための認証情報を直接入力されるか、または前記認証情報を、ネットワークを介して接続された他の装置から提供され、前記セキュア鍵生成装置が前記メディアＩＤ及び前記認証情報を全て用いてセキュア鍵を生成することを含む。

【発明の効果】

【００２５】

前記のような本発明によれば、装置及びユーザのいずれにも従属してセキュア性が優れたセキュア鍵を生成できる効果がある。例えば、本発明によるセキュア鍵生成装置によって生成されたセキュア鍵で暗号化したコンテンツは、前記セキュア鍵の生成と関連する特定ユーザが特定装置を使用する場合のみ復号化することができる。

【００２６】

また、前記セキュア鍵を生成する装置が信頼できるコンピューティングを支援する装置である場合、信頼できるコンピューティング環境を支援するセキュアモードで前記セキュア鍵の生成作業を行いユーザ認証情報、装置の識別子及び生成したセキュア鍵のような情報の流出を防げる効果がある。

【図面の簡単な説明】

【００２７】

【図１】本発明の一実施形態によるセキュア鍵生成装置の構成を示すブロック図である。
【図２】本発明の一実施形態によるセキュア鍵生成装置のＩＤ演算部と関連した構成を示すブロック図である。
【図３】本発明の一実施形態によるセキュア鍵生成装置のＩＤ演算部と関連した構成を示すブロック図である。
【図４】本発明の一実施形態によるセキュア鍵生成装置のＩＤ演算部の動作を説明するための参考図である。
【図５】本発明の一実施形態によるセキュア鍵生成装置の構成を示すブロック図である。
【図６】本発明の一実施形態によるセキュア鍵生成装置が信頼できるコンピューティングを支援する装置である場合の構成を示すブロック図である。
【図７】本発明の一実施形態によるセキュア鍵生成装置が信頼できるコンピューティングを支援する装置である場合の構成を示すブロック図である。
【図８】本発明の一実施形態によるセキュア鍵生成装置の構成を示すブロック図である。
【図９】図８に図示するセキュア鍵生成装置の周辺ロジックの配置を説明するための参考図である。
【図１０】図８に図示するセキュア鍵生成装置が暗号化・復号化を行う場合の構成を示すブロック図である。
【図１１】図８に図示するセキュア鍵生成装置が暗号化・復号化を行う場合の構成を示すブロック図である。
【図１２】本発明の一実施形態による記憶装置の構成を示すブロック図である。
【図１３】本発明の一実施形態による記憶装置の構成を示すブロック図である。
【図１４】本発明の一実施形態による記憶装置の構成を示すブロック図である。
【図１５】本発明の一実施形態によるセキュア鍵の生成方法を示す順序図である。
【図１６】本発明の一実施形態によるセキュア鍵の生成及び前記セキュア鍵を利用したコンテンツ暗号化方法を示す順序図である。
【図１７】本発明による一実施形態によりメディアＩＤを生成する方法を示す順序図である。
【図１８】本発明による一実施形態によりメディアＩＤを生成する方法を示す順序図である。
【図１９】本発明による一実施形態によりメディアＩＤを生成する方法を示す順序図である。
【図２０】本発明による一実施形態によりメディアＩＤを生成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セキュア鍵の生成及び前記セキュア鍵を利用したコンテンツ復号化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コンテンツを無断複製する際のコンテンツ復号化失敗の過程を示す順序図である。
【図２３】本発明の一実施形態によるユーザ認証情報の入力の際、誤りがある場合のコンテンツ復号化失敗過程を示す順序図である。
【発明を実施するための形態】
【００２８】
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、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。

【００２９】
本明細書で使用された用語は実施形態を説明するためであり、本発明を制限しようとするものではない。本明細書で、単数型は文句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（ｃｏｍｐｒｉｓｅｓ）」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。
【００３０】
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制限されないことはいうまでもない。これらの用語は、単に一つ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素子または構成要素であり得ることは勿論である。
【００３１】
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制限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、発明の範疇を制限するためではない。
【００３２】
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。
【００３３】
図１を参照して本発明の一実施形態によるセキュア鍵生成装置１０の構成及び動作について説明する。本実施形態によるセキュア鍵生成装置１０は記憶装置２００に接続され、記憶装置２００の固有識別子であるメディアＩＤとユーザ１を認証するための認証情報を用いてセキュア鍵を生成する。
【００３４】
セキュア鍵生成装置１０は、記憶装置２００に接続され、記憶装置２００からプリミティブＩＤを提供される。前記プリミティブＩＤは、記憶装置２００の固有識別子であるメディアＩＤ演算に用い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。セキュア鍵生成装置１０は、前記プリミティブＩＤから前記メディアＩＤを生成する。すなわち、セキュア鍵生成装置１０は、記憶装置２００から前記メディアＩＤを直接提供されるのではなく、前記メディアＩＤを生成できるソースデータであるプリミティブＩＤを提供される。前記メディアＩＤが露出することを防止するためのものとして、セキュア鍵生成装置１０は前記プリミティブＩＤから前記メディアＩＤの生成に使用するデータを格納することができる。
【００３５】
本実施形態によるセキュア鍵生成装置１０は、ＩＤ演算部１２、認証情報提供部１４及びセキュア鍵生成部１６を含み得る。ＩＤ演算部１２は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を演算する。
【００３６】
認証情報提供部１４は、ユーザ１を認証するための認証情報をセキュア鍵生成部１６に提供する。前記認証情報はユーザ１がセキュア鍵生成装置１０に直接入力することができる。また、ユーザ認証サーバ２がセキュア鍵生成装置１０にユーザ認証情報を提供することもできる。すなわち、認証情報提供部１４はユーザから入力されるか、またはユーザ認証サーバ２から提供された前記認証情報をセキュア鍵生成部１６に提供することができる。前記認証情報は、例えば、特定会員制サービスに使用するユーザ認証情報、ユーザ識別

情報または個人情報であり得る。前記個人情報は、個人の身上と関連する情報であり、例えば、誕生日、電話番号、メールアドレス、住民登録番号、ユーザ１が使用する金融セキュリティカードの特定番号に該当するコードまたは指紋、虹彩認識コードなどの生体情報であり得る。

【００３７】

セキュア鍵生成部１６は、前記メディアＩＤ及び前記認証情報を全て用いてセキュア鍵を生成する。セキュア鍵の生成に前記メディアＩＤを用いるということは、セキュア鍵の生成において、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。また、セキュア鍵の生成に前記認証情報を用いるということは、セキュア鍵の生成において、前記認証情報が少なくとも一度は入力されることを意味する。

【００３８】

セキュア鍵生成部１６は、前記メディアＩＤ及び前記認証情報を２進演算して前記セキュア鍵を生成することができる。前記２進演算には、例えばＡＮＤ、ＯＲ、ＮＯＲ、ＸＯＲ、ＮＡＮＤなどが使用される。セキュア鍵生成部１６は、前記メディアＩＤ及び前記認証情報を文字列連結演算（Ｓｔｒｉｎｇ　Ｃｏｎｃａｔｅｎａｔｉｏｎ、ＳＴＲＣＡＴ）して前記セキュア鍵を生成することもできる。前記文字列連結において前後関係は限定されない。すなわち、前記メディアＩＤ後に前記認証情報が連結されてもよく、前記認証情報の後に前記メディアＩＤが連結されてもよい。

【００３９】

セキュア鍵生成部１６は、前記メディアＩＤ及び前記認証情報のみを用いて前記セキュア鍵を生成することもでき、前記メディアＩＤ及び前記認証情報の他に一つ以上の可変データまたは固定データをさらに用いて前記セキュア鍵を生成することもできる。

【００４０】

前記セキュア鍵はユーザ認証情報、メディアＩＤ及びセキュア鍵演算式の３つをすべて知らなければ生成できない。セキュア鍵自体が流出しなければ、前記セキュア鍵演算式が知らされても前記ユーザ認証情報及び前記メディアＩＤの全てが分からない限り前記セキュア鍵は演算できない。しかし、前記メディアＩＤは外部に流出しない値であり、記憶装置２００が提供するプリミティブＩＤから得る他にはない値である。また前記認証情報も特定ユーザが外部に流出しないように管理するため簡単に外部に流出しない値である。したがって、本実施形態によるセキュア鍵生成装置１０は記憶装置２００に従属し、同時に特定ユーザに従属するセキュア鍵を生成する。

【００４１】

以下、図２ないし図３を参照してプリミティブＩＤからメディアＩＤを演算するＩＤ演算部１２の動作についてより詳細に説明する。

【００４２】

前述したように、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り、前記プリミティブＩＤも記憶装置２００の少なくとも１パートを識別するためのデータである。例えば、記憶装置２００が第１，２パートを備え、前記第１パートの識別子である第１プリミティブＩＤ及び前記第２パートの識別子である第２プリミティブＩＤは、それぞれ記憶装置２００からＩＤ演算部１２に提供され得る。この際、前記プリミティブＩＤ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を含む。

【００４３】

図２は、ＩＤ演算部１２が前記プリミティブＩＤのうち一つとして暗号化メモリＩＤ２６４を記憶装置２００から提供されることを図示する。暗号化メモリＩＤ２６４は、記憶装置２００に備えられたメモリ素子２０６の固有識別子であるメモリＩＤ２６２を暗号化したデータである。メモリＩＤ２６２は、メモリ素子２０６の製造時に製造業者によってプログラムされたデータであり得る。メモリＩＤ２６２はシステム領域に格納され、ユーザ領域に対するアクセスと同一な方式でアクセスされないことが好ましい。ユーザ領域に格納される場合、メモリＩＤ２６２が削除されたり変形され得、外部に流出できるからである。前記システム領域に格納されるメモリＩＤ２６２はユーザのアクセスによって削除

されたり、変更されたり流出しない。
【００４４】
また、図３は、ＩＤ演算部１２が前記プリミティブＩＤのうち他の一つとしてコントローラ認証情報を記憶装置２００から提供されることを図示する。セキュア鍵生成装置１０と記憶装置２００に備えられたメモリ素子２０６のコントローラ２０８は相互認証を行うことができ、前記コントローラ認証情報は前記相互認証のためにコントローラ２０８がセキュア鍵生成装置１０に提供する情報である。
【００４５】
図４は、ＩＤ演算部１２がメディアＩＤを生成することを説明するための参考図である。
【００４６】
ＩＤ演算部１２は、暗号化メモリＩＤ２６４を復号化してメモリＩＤ２６２を取得し、メモリＩＤ２６２からメモリ派生ＩＤを生成する。また、ＩＤ演算部１２は前記コントローラ認証情報からコントローラ２０８の固有識別子であるコントローラＩＤを取得する。
【００４７】
暗号化メモリＩＤ２６４を復号化するために使用する第１復号化鍵は暗号化された状態で記憶装置２００から提供され得る。また、暗号化第１復号化鍵を復号化するための第２復号化鍵はセキュア鍵生成装置１０に備えられた格納部（図示せず）に格納され得る。
【００４８】
すなわち、ＩＤ演算部１２は、暗号化第１復号化鍵を記憶装置２００から提供され、前記第２復号化鍵を用いて前記暗号化第１復号化鍵から第１復号化鍵を取得した後、前記第１復号化鍵を用いて暗号化メモリＩＤ２６４をメモリＩＤ２６２で復号化することができる。
【００４９】
前記メモリ派生ＩＤは、メモリ素子２０６の他の固有識別子である。すなわち、メモリ素子２０６は製造業者によってプログラムされた固有識別子であるメモリＩＤ２６２及びメモリＩＤ２６２を用いて生成されたメモリ派生ＩＤの２個の固有識別子を有することができる。メモリＩＤ２６２は、メモリ素子２０６に格納されるが、前記メモリ派生ＩＤはメモリ素子２０６に格納される値ではなく、記憶装置２００に接続されるセキュア鍵生成装置１０によって生成される値である。
【００５０】
ＩＤ演算部１２は、前記コントローラ認証情報を用いて前記コントローラＩＤを生成することができる。前記コントローラ認証情報にはコントローラ認証書ＩＤ及びコントローラ２０８の固有識別コードが含まれ得、ＩＤ演算部１２は前記コントローラ認証書ＩＤ及び前記固有識別コードを用いて前記コントローラＩＤを生成することができる。例えば、ＩＤ演算部１２は、前記コントローラ認証書ＩＤと前記固有識別コードを文字列連結演算（ｓｔｒｉｎｇ　ｃｏｎｃａｔｅｎａｔｉｏｎ　ｏｐｅｒａｔｉｏｎ）して前記コントローラＩＤを生成することができる。
【００５１】
ＩＤ演算部１２は、前記メモリ派生ＩＤ及び前記コントローラＩＤを用いて前記メディアＩＤを生成する。例えば、ＩＤ演算部１２は前記メモリ派生ＩＤ及び前記コントローラＩＤを２進演算に入力したり、文字列連結演算に入力して前記メディアＩＤを生成することができる。
【００５２】
図５ないし図７を参照して本発明の一実施形態によるセキュア鍵生成装置の構成及び動作について説明する。
【００５３】
本実施形態によるセキュア鍵生成装置２０は、図５に図示するようにプロセッサ１０２及び記憶装置インターフェース１０４を含み得る。セキュア鍵生成装置２０はプロセッサ１０２が実行する命令を一時的に格納するＲＡＭ１０６、ユーザ認証情報を入力される入

力部１０８をさらに含み得る。プロセッサ１０２、記憶装置インターフェース１０４、ＲＡＭ１０６及び入力部１０８はシステムバス１１０に接続され得る。

【００５４】

図５に図示するように、記憶装置インターフェース１０４はセキュア鍵生成装置２０と記憶装置２００との間のデータ送受信を仲介することができる。記憶装置インターフェース１０４は、記憶装置２００からプリミティブＩＤを提供され、システムバス１１０を介してプロセッサ１０２に提供することができる。

【００５５】

プロセッサ１０２は、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及びユーザを認証するための認証情報を全て用いてセキュア鍵を生成することができる。入力部１０８は、前記認証情報をユーザから入力されてプロセッサ１０２に提供することができる。プロセッサ１０２は前記セキュア鍵を多様な用途に使用することができる。例えば、前記セキュア鍵を高いセキュリティレベルでのユーザの認証情報として使用したり、記憶装置２００に格納されるコンテンツの暗号化鍵として使用することができる。

【００５６】

本発明の一実施形態によるセキュア鍵生成装置２０はセキュア実行環境（Ｓｅｃｕｒｅ Ｅｘｅｃｕｔｉｏｎ Ｅｎｖｉｒｏｎｍｅｎｔ）を支援するものであり得る。セキュア実行環境はプロセッサ、オペレーティングシステムなどの支援によりプログラムの安全な実行を保証する環境を意味する。安全な実行を保証する方法としては無欠性、機密性保証などがある。一般的にはハードウェアを基盤としたセキュア実行環境の接近方法がソフトウェアを基盤とした安全な実行環境の接近方法より安全であると知られている。本実施形態によるセキュア鍵生成装置２０もハードウェアを基盤としたセキュア実行環境を提供すると仮定する。

【００５７】

図６ないし図７に図示するように、セキュア鍵生成装置２０はプロセス実行環境を分離するために２個のコアを有するプロセッサ１０２を含み得る。プロセッサ１０２は物理的に別個の２個以上のコアを備えてセキュア実行モード及び非セキュア実行モードでそれぞれ使用することもでき、一つのコアを仮想分割し、セキュア実行モード及び非セキュア実行モード用途にそれぞれ使用することもできる。以下、図６及び図７ではプロセッサ１０２が２個の仮想コア（１２０，１２４）を有すると仮定して説明する。

【００５８】

セキュア鍵生成装置２０は、前記セキュア実行環境を提供するセキュア実行モードで実行されるプロセスによって生成されるデータを、前記セキュア実行環境を提供しない非セキュア実行モードで実行されるプロセスがアクセスできないようにすることが好ましい。すなわち、前記セキュア実行モードと前記非セキュア実行モードでのデータアクセスは互いに分離されることが好ましい。例えば、ＲＡＭ１０６は非セキュア仮想コア１２０で実行される命令によってアクセスできる第１領域及びセキュア仮想コア１２４で実行される命令によってアクセスできる前記第１領域と重ならない第２領域を含み得る。

【００５９】

プロセッサ１０２のコアがセキュア実行モードでのプロセス実行のためのセキュア仮想コア１２４及び非セキュア実行モードでのプロセス実行のための非セキュア仮想コア１２０に論理的に分割されて運用される場合、前記セキュア実行モードと前記仮想実行モードとの間の切り替えはコンテキストスイッチ（Ｃｏｎｔｅｘｔ Ｓｗｉｔｃｈｉｎｇ）方式により行われ得る。

【００６０】

以上説明したセキュア実行環境の提供に関する技術について、プロセッサ１０２はＡＲＭ社のＴＲＵＳＴＺＯＮＥ技術、ＩＮＴＥＬ社のＷｉｒｅｌｅｓｓ ＴＰＭ技術、Ｔｅｘａｓ Ｉｎｓｔｕｍｅｎｔ社のＭ－Ｓｈｉｅｌｄ技術、Ｆｒｅｅｓｃａｌｅ社のセキュリティ技術、ＳａｆｅＮｅｔ社のＳａｆｅＸｃｅｌ ＴＰＭ技術、ＳａｆｅＮｅｔ社のＳａ

ｆｅＺｏｎｅ技術、Ｄｉｓｃｒｅｔｉｘ社のＳｅｃｕｒｉｔｙ　ｐｌａｔｆｏｒｍ技術、Ｑｕａｌｃｏｍｍ社のＳｅｃｕｒｅＭＳＭ技術のうち少なくとも一つが適用されたものであり得る。

【００６１】

一方、特定プロセスがプロセッサ１０２のセキュア実行モードで実行されるためには所定の認証手続が必要である。前記認証手続は、ユーザ認証情報を入力され、前記認証情報が既に格納されているものと同一であるかを検証するものである。前記検証を通過した場合、プロセッサ１０２の動作モードを非セキュア実行モードから仮想実行モードに切り替えるためのインタラプト信号が生成され、プロセッサ１０２は前記インタラプト信号に応答して動作モードをセキュア実行モードに切り替えることができる。図６は非セキュア実行モードで動作していたプロセッサ１０２がセキュア実行モードに切り替えるためにユーザ認証を行い、前記ユーザ認証のためにユーザ認証情報を入力部１０８から提供され、前記ユーザ認証情報を利用した認証が成功する場合、非セキュア仮想コア１２０からモニタプロシジャ１２２を経てセキュア仮想コア１２４に活性化される仮想コアを交替することが記載されている。

【００６２】

すなわち、本実施形態によるセキュア鍵生成装置２０のプロセッサ１０２は非セキュア実行モードの状態で実行モード切り替えのためのユーザ認証情報を入力され、その結果、実行モードをセキュア実行モードに切り替え、前記セキュア実行モードでセキュア鍵を生成する。本実施形態によるセキュア鍵生成装置２０は、セキュア実行モードでセキュア鍵を生成するため、ユーザ認証情報、プリミティブＩＤ、メモリＩＤ、メディアＩＤなどが流出することを防止できる効果がある。

【００６３】

本発明の一実施形態によるセキュア鍵生成装置２０のプロセッサ１０２はセキュア実行モードに切り替えられた状態でユーザ認証情報及びプリミティブＩＤを提供され、前記セキュア鍵を生成することもできる。図７は、本実施形態によるセキュア鍵生成装置２０のプロセッサ１０２がセキュア実行モードに切り替えられた状態でユーザ認証情報及びプリミティブＩＤを提供され、前記セキュア鍵を生成することが図示されている。本実施形態によるセキュア鍵生成装置２０に備えられるＲＡＭ１０６は、プロセッサ１０２がセキュア実行モードで動作するときのみアクセス可能なセキュア領域を含み、プロセッサ１０２は前記認証情報、プリミティブＩＤ、メディアＩＤ及び前記セキュア鍵は前記セキュア領域に格納することができる。

【００６４】

本実施形態によれば、ユーザ認証情報を入力される時点で既にセキュア鍵生成装置２０はセキュア実行モードで動作する状態であるため、ユーザ認証情報、プリミティブＩＤ、メモリＩＤ、メディアＩＤなどが流出することを防止できる効果がある。

【００６５】

以下、図８ないし図１１を参照して本発明の一実施形態によるセキュア鍵生成装置の構成及び動作について説明する。

【００６６】

図８は、本実施形態によるセキュア鍵生成装置の構成を図示する。図８に図示するように、本実施形態によるセキュア鍵生成装置３０はシステムオンチップ（Ｓｙｓｔｅｍ　ｏｎ　Ｃｈｉｐ、ＳｏＣ）３０２及びシステムオンチップ３０２と接続された記憶装置インターフェース１０４を含み得る。本実施形態の記憶装置インターフェース１０４は、記憶装置２００と接続されて前記プリミティブＩＤを前記記憶装置から提供され、システムオンチップ３０２に提供する。

【００６７】

システムオンチップ３０２は、多様な機能を有するシステムを一つのチップとして実現したものであり、本実施形態によるシステムオンチップ３０２は前記プリミティブ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及びユーザ

を認証するための認証情報を全て用いてセキュア鍵を生成する周辺ロジック（ｐｅｒｉｐｈｅｒａｌ　ｌｏｇｉｃ）３２０を含む。

【００６８】

システムオンチップ３０２は命令演算を行うコア３２２をさらに含み得る。コア３２２はセキュア鍵生成装置３０に含まれたＲＡＭ（図示せず）に格納された命令を読み込んで実行することができる。前記ＲＡＭはシステムオンチップ３０２の内部に備えられ得、または外部に備えられ得る。コア３２２はセキュア鍵生成装置３０の入出力に関する動作を制御する。例えば、コア３２２は入力部１０８を介して入力されたユーザ認証情報を入力部１０８から提供される。コア３２２は前記ユーザ認証情報を周辺ロジック３２０に提供する。

【００６９】

周辺ロジック３２０は、前記ユーザ認証情報はコア３２２から提供されるが、前記プリミティブＩＤはコア３２２を経由せず、記憶装置インターフェース１０４から直接提供され得る。このため、図９に図示するように、周辺ロジック３２０は記憶装置インターフェース１０４とコア３２２との間のデータパス（ｄａｔａ　ｐａｔｈ）３２５上に接続されたものであり得る。周辺ロジック３２０は記憶装置２００から提供された前記プリミティブＩＤを、データパス３２５を介して提供され、コア３２２に伝達しなくてもよい。コア３２２はハッキングされやすく、コア３２２で前記プリミティブＩＤを利用した演算を行わないため、周辺ロジック３２０は前記プリミティブＩＤをコア３２２に伝達しないことが好ましい。

【００７０】

すなわち、周辺ロジック３２０はセキュア鍵を生成することにおいて、コア３２２と独立して動作する。コア３２２からユーザ認証情報を提供されること以外には前記セキュア鍵の生成と関連するすべての演算を周辺ロジック３２０が担う。また、周辺ロジック３２０は前記ＲＡＭに格納されているプログラムを実行せず、周辺ロジック３２０内に備えられたＲＯＭなどの不揮発性メモリに格納されているセキュア鍵生成専用プログラムのみ実行することができる。

【００７１】

周辺ロジック３２０は前記生成されたセキュア鍵をシステムオンチップ３０２内に備えられたレジスタ３２４に格納することができる。

【００７２】

セキュア鍵、メディアＩＤ、メモリＩＤなどを取り出すことを目的とするハッキングプログラムは通常コア３２２で実行される。したがって、コア３２２と独立した周辺ロジック３２０がセキュア鍵生成に関する演算を専用に担う本実施形態のセキュア鍵生成装置３０はセキュア鍵生成に関するデータが外部に流出することを効果的に防止することができる。

【００７３】

図１０に図示するように、本実施形態によるセキュア鍵生成装置３０は前記セキュア鍵を用いて内部記憶装置３０４に格納されたコンテンツを暗号化した後、セキュア鍵生成装置３０に接続され、前記セキュア鍵を生成に使用するメディアＩＤを生成するため、プリミティブＩＤを提供した記憶装置２００に、暗号化したコンテンツを格納することができる。セキュリティ性を高めるため、前記暗号化も周辺ロジック３２０が担うことができる。このため、周辺ロジック３２０は暗号化・復号化エンジン３２１を含み得る。暗号化・復号化エンジン３２１はレジスタ３２４に格納されたセキュア鍵を暗号化・復号化鍵として使用することができる。

【００７４】

図１１に図示するように、本実施形態によるセキュア鍵生成装置３０は記憶装置２００と接続され、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こともできる。セキュア鍵生成装置３０は前記暗号化コンテンツの復号化鍵を自ら生成しなければならないが、前記復号化鍵は記憶装置２００からプリミティブＩＤを提供され、セキュア鍵生成

装置３０のユーザから認証情報を入力された後、前記プリミティブＩＤから記憶装置２００のメディアＩＤを生成し、前記メディアＩＤ及び前記認証情報を用いて前記コンテンツの復号化鍵を生成することができる。

【００７５】

以上、セキュア鍵生成装置（１０，２０，３０）は、コンピュータ、ＵＭＰＣ（Ｕｌｔｒａ Ｍｏｂｉｌｅ ＰＣ）、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）、モバイルフォン（ｍｏｂｉｌｅ ｐｈｏｎｅ）、スマートフォン（ｓｍａｒｔ ｐｈｏｎｅ）、電子書籍（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）、三次元テレビ（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）、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のうち一つ、コンピュータネットワークを構成する多様な電子装置のうち一つ、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のうち一つ、コンピューティングシステムを構成する多様な構成要素のうち一つなどのような電子装置の多様な構成要素のうち一つであり得る。

【００７６】

以下、図１２ないし図１４を参照して本発明の一実施形態による記憶装置について説明する。本実施形態による記憶装置４０は自己暗号化する機能を備えたものである。すなわち、記憶装置４０がホスト装置に接続され、ホスト装置から格納するデータを提供されても前記データをそのまま格納せず、自己暗号化した後、格納する。

【００７７】

本実施形態による記憶装置４０は、前記自己暗号化する際に使用する暗号化鍵を前記ホスト装置から提供されたユーザ認証情報及び記憶装置４０に備えられたメモリ素子２０６のメモリ派生ＩＤを用いて生成する。

【００７８】

図１２を参照して本実施形態による記憶装置４０の構成及び動作について説明する。図１２に図示するように、本実施形態による記憶装置４０は、メモリ素子２０６、ホストインターフェース２１０、派生ＩＤ演算部２１２、セキュア鍵生成部２１４及び暗号化部２１６を含み得る。

【００７９】

ホストインターフェース２１０はホスト装置からユーザを認証するための認証情報を提供され、セキュア鍵生成部２１４に提供し、前記ホスト装置からコンテンツを提供され、暗号化部２１６に提供する。

【００８０】

メモリ素子２０６はメモリＩＤ２６２及びメモリＩＤ２６２を暗号化した暗号化メモリＩＤ２６４を格納する。メモリ素子２０６は、格納領域がユーザ領域及びシステム領域に区分されており、前記ユーザ領域に対するアクセス方法では前記システム領域にアクセスできないようにすることが好ましい。メモリＩＤ２６２及び暗号化メモリＩＤ２６４は前記システム領域に格納されることが好ましい。

【００８１】

メモリ素子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）、磁気ランダムアクセスメモリ（ＭＲＡＭ：Ｍａｇｎｅｔｉｃ Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）、抵抗メモリ（ＲＲＡＭ（登録商標）：Ｒｅｓｉｓｔｉｖｅ Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）を格納手段として使用あるチップまたはパッケージであり得る。また、前記パッケージ方式に関し、前記メモリ素子はＰｏＰ（Ｐａｃｋａｇｅ ｏｎ Ｐａｃｋａｇｅ）、ＢＧＡｓ（Ｂａｌｌ ｇｒｉｄ ａｒｒａｙｓ）、ＣＳＰｓ（Ｃｈｉｐ ｓｃａｌｅ ｐａｃｋａｇｅｓ）、ＰＬＣＣ（Ｐｌａｓｔｉｃ Ｌｅａｄｅｄ Ｃｈｉｐ Ｃａｒｒｉｅｒ）、ＰＤＩＰ（Ｐｌａｓｔｉｃ Ｄｕａｌ Ｉｎ Ｌｉｎｅ Ｐａｃｋａｇｅ）、Ｄｉｅ ｉｎ Ｗａｆｆｌｅ Ｐａｃｋ、Ｄｉｅ ｉｎ Ｗａｆｅｒ Ｆｏｒｍ、ＣＯＢ（Ｃｈｉｐ Ｏｎ Ｂｏａｒｄ）、ＣＥＲＤＩＰ（Ｃｅｒａｍｉｃ Ｄｕａｌ Ｉｎ Ｌｉｎｅ Ｐａｃｋａｇｅ）、ＭＱＦＰ（Ｐｌａｓｔｉｃ Ｍｅｔｒｉｃ Ｑｕａｄ Ｆｌａｔ Ｐａｃｋ）、ＴＱＦＰ（Ｔｈｉｎ Ｑｕａｄ Ｆｌａｔｐａｃｋ）、ＳＯＩＣ（Ｓｍａｌｌ Ｏｕｔｌｉｎｅ）、ＳＳＯＰ（Ｓｈｒｉｎｋ Ｓｍａｌｌ Ｏｕｔｌｉｎｅ Ｐａｃｋａｇｅ）、ＴＳＯＰ（Ｔｈｉｎ Ｓｍａｌｌ Ｏｕｔｌｉｎｅ）、ＴＱＦＰ（Ｔｈｉｎ Ｑｕａｄ Ｆｌａｔｐａｃｋ）、ＳＩＰ（Ｓｙｓｔｅｍ Ｉｎ Ｐａｃｋａｇｅ）、ＭＣＰ（Ｍｕｌｔｉ Ｃｈｉｐ Ｐａｃｋａｇｅ）、ＷＦＰ（Ｗａｆｅｒ－ｌｅｖｅｌ Ｆａｂｒｉｃａｔｅｄ Ｐａｃｋａｇｅ）、ＷＳＰ（Ｗａｆｅｒ－Ｌｅｖｅｌ Ｐｒｏｃｅｓｓｅｄ Ｓｔａｃｋ Ｐａｃｋａｇｅ）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。

【００８２】

派生ＩＤ演算部２１２はメモリ素子２０６から暗号化メモリＩＤ２６４を読み込み（ｒｅａｄ）、暗号化メモリＩＤ２６４を復号化してメモリＩＤ２６２を取得し、メモリＩＤ２６２を用いてメモリ素子２０６の他の固有識別子であるメモリ派生ＩＤを生成する。

【００８３】

セキュア鍵生成部２１４は、ユーザ認証情報及び前記前記メモリ派生ＩＤを全て用いてセキュア鍵を生成する。セキュア鍵生成部２１４が前記セキュア鍵を生成する方法はセキュア鍵生成装置１０のセキュア鍵生成部１６がセキュア鍵を生成する方法と同様である。

【００８４】

暗号化部２１６は前記セキュア鍵を用いて前記コンテンツを暗号化してメモリ素子２０６に格納する。

【００８５】

本実施形態による記憶装置４０は、ホスト装置から提供されたコンテンツを暗号化して格納することにおいて、記憶装置４０に備えられたメモリ素子２０６の固有識別子を反映して生成した暗号化鍵を用いるため、格納された暗号化コンテンツが無断複製されても復号化されることを防止できる効果がある。複製された後に暗号化コンテンツが格納された記憶装置では元の暗号化コンテンツが格納されていた記憶装置４０のメディアＩＤと同一メディアＩＤを取得できないからである。

【００８６】

本実施形態による記憶装置４０は、ユーザを認証できるユーザ認証情報をさらに反映して生成された暗号化鍵を用いるため、ユーザの認証情報を知らなければ記憶装置４０に格納されたコンテンツを復号化できなくなる。

【００８７】

本実施形態による記憶装置４０は、クラウドコンピューティングサービスのクラウドサーバに備えられる記憶装置として使用することができる。すなわち、クラウドコンピューティングサービスのユーザがアップロードするコンテンツまたはデータは前記ユーザ認証情報及び記憶装置４０のメディアＩＤを全て用いて暗号化した後に格納される。この場合、ユーザが記憶装置４０にアップロードしたコンテンツまたはデータがクラウドサービスサーバでハッキングされ、その結果、暗号化された状態で流出しても流出したコンテンツまたはデータが記憶装置４０に格納されておらず、ユーザ認証情報を入力しなければ復号化できない。したがって、本実施形態による記憶装置がクラウドコンピューティングサービスのクラウドサーバに備えられ、アップロードするコンテンツまたはデータの格納手段

として使用する場合、ユーザがアップロードするコンテンツまたはデータが流出する危険性を減らすことができる効果がある。

【００８８】

本実施形態による記憶装置４０はＳＤ協会（Ｓｅｃｕｒｅ Ｄｉｇｉｔａｌ Ａｓｓｏｃｉａｔｉｏｎ）のＳＤカード規格を満すものであり得る。この場合、ホストインターフェース２１０はＳＤカード規格に従うコマンドのパラメータとして受信した前記認証情報をセキュア鍵生成部２１４に提供することができる。

【００８９】

本実施形態による記憶装置４０は、ＳＳＤ（Ｓｏｌｉｄ Ｓｔａｔｅ Ｄｒｉｖｅ）、またはフラッシュメモリを内部に含むＨＤＤ（Ｈａｒｄ Ｄｉｓｋ Ｄｒｉｖｅ）規格であり得る。この場合、ホストインターフェース２１０は大容量記憶装置のための通信コマンドを支援するＡＴＡ、ＳＡＴＡ、ＳＣＳＩ、ＰＣＩｅ、ＵＳＢなどの物理的インターフェースであり得る。

【００９０】

本実施形態による記憶装置４０は、図１３に図示するようにランダムナンバー（Ｒａｎｄｏｍ Ｎｕｍｂｅｒ、ＲＮ）をさらに用いてセキュア鍵を生成することもできる。すなわち、セキュア鍵生成部２１４はランダムナンバー、前記認証情報及び前記メディアＩＤを全て用いてセキュア鍵を生成することができる。本実施形態による記憶装置４０は前記ランダムナンバーを生成してセキュア鍵生成部２１４に提供するランダムナンバー生成器２１７をさらに含み得る。本実施形態による記憶装置４０はＴＣＧ（Ｔｒｕｓｔｅｄ Ｃｏｍｐｕｔｉｎｇ Ｇｒｏｕｐ）のＯＰＡＬ ＳＳＣ（Ｏｐａｌ Ｓｅｃｕｒｉｔｙ Ｓｕｂｓｙｓｔｅｍ Ｃｌａｓｓ）規格に従い動作するものであり得る。

【００９１】

図１４を参照して本発明の一実施形態によるメモリシステムについて説明する。

【００９２】

図１４を参照すると、メモリシステム１０００は不揮発性メモリ装置１１００及びコントローラ１２００を含む。図１，図２または図３を参照して説明した記憶装置２００は図１４に図示するメモリシステム１０００形態で構成され得る。

【００９３】

ここで、不揮発性メモリ装置１１００は前述した少なくとも一つのメモリ素子２０６を含み得る。

【００９４】

コントローラ１２００は、ホスト装置及び不揮発性メモリ装置１１００に接続される。コントローラ１２００はホスト装置からの要請に応答して不揮発性メモリ装置１１００をアクセスするように構成される。例えば、コントローラ１２００は不揮発性メモリ装置１１００の読み取り、書き込み、消去、バックグラウンド（ｂａｃｋｇｒｏｕｎｄ）の動作を制御するように構成される。コントローラ１２００は、不揮発性メモリ装置１１００及びホスト装置１００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１２００は不揮発性メモリ装置１１００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。

【００９５】

例示的に、コントローラ１２００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）、及び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１１００及びホスト装置１００との間のキャッシュメモリ、及び不揮発性メモリ装置１１００及びホスト装置１００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１２００の諸般の動作を制御する。

【００９６】

ホストインターフェースは、ホスト装置及びコントローラ１２００との間のデータ交換を実行するためのプロトコルを含む。例示的に、コントローラ１２００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、及び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１１００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。

【００９７】

メモリシステム１０００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１１００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１２００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１１００の構成要素として提供され得る。

【００９８】

コントローラ１２００及び不揮発性メモリ装置１１００は一つの半導体装置に集積される。例示的に、コントローラ１２００及び不揮発性メモリ装置１１００は一つの半導体装置に集積され、メモリカードを構成され得る。例えば、コントローラ１２００及び不揮発性メモリ装置１１００は一つの半導体装置に集積されて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。

【００９９】

コントローラ１２００及び不揮発性メモリ装置１１００は、一つの半導体装置に集積されて半導体ドライブ（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素子を含む。メモリシステム１０００が半導体ドライブ（ＳＳＤ）として利用される場合、メモリシステム１０００に接続されたホスト装置の動作速度が画期的に改善される。

【０１００】

図１ないし図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）を介して行うことができる。しかし、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意味ではなく、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。

【０１０１】

図１５を参照して本発明の一実施形態によるセキュア鍵の生成方法について説明する。

【０１０２】
本実施形態によるセキュア鍵の生成方法は、ホスト装置が記憶装置のメディアＩＤを取得し、前記メディアＩＤ及びユーザ認証情報を全て用いてセキュア鍵を生成することに要約される。
【０１０３】
記憶装置はプリミティブＩＤ（ｐｒｉｍｉｔｉｖｅ　ＩＤ）を格納する（Ｓ１００）。前記プリミティブＩＤは記憶装置２００に備えられたメモリ素子に格納され得る。
【０１０４】
ホスト装置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（Ｓ１０４）。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を結合して前記メディアＩＤを演算できるが、前記プリミティブＩＤ自体が前記メディアＩＤであり得る。前記メディアＩＤを演算する方法については図１９ないし２２を参照して詳細に説明する。
【０１０５】
前記ホスト装置は、前記メディアＩＤとユーザ認証情報（例、パスワード）を全て用いてセキュア鍵を生成する（Ｓ１０６）。
【０１０６】
ホスト装置はユーザ認証情報を提供される。前記ユーザ認証情報はホスト装置に備えられた入力手段（図示せず）を介してユーザが入力したものであり得、ホスト装置以外の端末（図示せず）を介してユーザが入力したものをホスト装置が提供されたものであり得る。
【０１０７】
図１６は、本発明の一実施形態によるセキュア鍵の生成及び前記セキュア鍵を利用したコンテンツ暗号化方法を示す順序図である。図１８でセキュア鍵を生成する動作（Ｓ１００，Ｓ１０２，Ｓ１０４，Ｓ１０５，Ｓ１０６）までは図１７と同様である。
【０１０８】
本実施形態によるホスト装置は、前記セキュア鍵を用いてコンテンツを暗号化して暗号化コンテンツを生成するか、または前記コンテンツを暗号化コンテンツに変換する（Ｓ１０８）。前記暗号化に使用する暗号化アルゴリズム及び使用する暗号化鍵は特定のものに制限されないが、暗号化鍵と復号化鍵が同一であ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使用する。
【０１０９】
暗号化コンテンツは記憶装置に提供され（Ｓ１１０）、記憶装置は暗号化コンテンツを格納する（Ｓ１１２）。図１６に図示するように、ホスト装置は前記プリミティブＩＤを提供した記憶装置に前記暗号化コンテンツを格納することが好ましい。すなわち、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。
【０１１０】
図１６に図示するように、ホスト装置は前記セキュア鍵を記憶装置に提供せず、前記暗号化コンテンツに含めもしない。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のメディアＩＤを取得し、前記メディアＩＤから復号化鍵を生成しなければならず、前記暗号化コンテンツの復号化鍵を記憶装置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暗号化方法によれば、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復号化できない効果がある。
【０１１１】
ホスト装置が前記メディアＩＤを演算する方法について図１７ないし２０を参照してよ

り詳細に説明する。

【０１１２】

図１７は、記憶装置が第１パート及び第２パートを含み、記憶装置に第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。第１パート及び第２パートはそれぞれ記憶装置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行う素子グループまたはモジュールグループでもあり得る。例えば、第２パートはデータ格納機能を行う素子、モジュール、素子グループまたはモジュールグループであり得、第１パートは制御機能を実行する素子、モジュール、素子グループまたはモジュールグループであり得る。

【０１１３】

図１７に図示するように、ホスト装置は前記第１プリミティブＩＤ及び前記第２プリミティブＩＤを提供される（Ｓ１１４）。

【０１１４】

ホスト装置は、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）。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、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パートによって特定され、前記第１プリミティブＩＤ及び前記第２プリミティブＩＤを全て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パートすべてによって特定される。

【０１１５】

図１８に図示するように、前記第２プリミティブＩＤは第２識別子に変換され（Ｓ１１８）、前記メディアＩＤ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を演算することもできる（Ｓ１２０）。例えば、前記メディアＩＤは前記第１プリミティブＩＤ及び前記第２識別子全て用いて前記メディアＩＤを演算することができる。

【０１１６】

第２パートの固有識別子が外部に流出してはならない場合、前記第２パートの固有識別子の代わりに、前記第２パートの固有識別子を暗号化したデータが前記第２プリミティブＩＤとしてホスト装置に提供され得、ホスト装置は前記第２プリミティブＩＤを用いて第２パートのまた他の識別子として使用できる前記第２識別子を生成することができる。

【０１１７】

図１９ないし図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。

【０１１８】

図１９に図示するように、前記第２パートはメモリ素子であり得、第１パートはメモリ素子コントローラであり得る。メモリ素子は自身の固有識別子を格納する。前記メモリ素子コントローラの固有識別子もメモリ素子に格納され得る。

【０１１９】

先に、メモリ素子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第２識別子と同一なものと理解することができる。

【０１２０】

ホスト装置は、メモリ素子に格納された前記メモリ素子の固有識別子が暗号化された暗号化メモリＩＤを記憶装置から提供される（Ｓ１２２）。前記暗号化メモリＩＤもメモリ素子に格納されたものであり得る。前記暗号化メモリＩＤは図１８を参照して説明した第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。

【０１２１】

ホスト装置は、前記暗号化メモリＩＤを復号化して前記メモリ素子の固有識別子であるメモリＩＤを生成する（Ｓ１２４）。

【０１２２】
ホスト装置は、前記メモリＩＤを用いて第２認証情報を生成する（Ｓ１２６）。ホスト装置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、前記メモリ素子の固有識別子と前記セッション鍵を所定の一方向関数（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。前記一方向関数は、出力値から入力値を演算することが計算上不可能なものであって、例えば２個の演算子（ｏｐｅｒａｎｄ）を入力されるビット演算のうち排他的論理合（ＸＯＲ）であり得る。
【０１２３】
一方、記憶装置も前記メモリＩＤを用いて第１認証情報を生成する（Ｓ１２８）。メモリ素子にはメモリ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得るが、記憶装置は前記補助鍵セットの補助鍵のうち一つの補助鍵を暗号化し、前記暗号化した補助鍵を、前記ホスト装置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。記憶装置は前記セッション鍵及び前記メモリＩＤを所定の一方向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。
【０１２４】
ホスト装置は、前記第１認証情報を記憶装置から提供され（Ｓ１３０）、前記第２認証情報と一致するかを検証する（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）。
【０１２５】
検証（Ｓ１３２）結果、第１，２認証情報が一致する場合、前記メモリ素子の固有識別子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、前記メモリ素子の固有識別子とアプリケーション固有鍵（Ａｐｐｌｉｃａｔｉｏｎ　Ｓｐｅｃｉｆｉｃ　Ｓｅｃｒｅｔ　Ｖａｌｕｅ、ＡＳＳＶ）を所定の一方向関数に入力して生成され得る。
【０１２６】
前記アプリケーション固有鍵は、ホスト装置で行われる各アプリケーションに対して固有の鍵を付与するものであり得る。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別に互いに異なる固有の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、暗号化する前記コンテンツのタイプによって固有値を有したり、暗号化する前記コンテンツの提供者の識別情報によって固有値を有することができる。好ましくは、前記アプリケーション固有鍵は、暗号化する前記コンテンツのタイプにより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が選択され得る。
【０１２７】
次に、メモリ素子コントローラの固有識別子を提供されること（Ｓ２０）について説明する。
【０１２８】
図２０を参照してホスト装置が記憶装置からコントローラの識別子を提供されること（Ｓ２０）について説明する。
【０１２９】
先に、コンテンツ記録装置が記憶装置から第３認証情報を提供される（Ｓ１４０）。前記第３認証情報には前述したように、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識別コードが含まれ得る。
【０１３０】
次に、ホスト装置と記憶装置間に相互認証が行われる（Ｓ１４１）。前記相互認証は公開鍵を基盤とした認証であり得る。相互認証（Ｓ１４１）を失敗した際、ホスト装置は認証失敗として処理する（Ｓ１４４）。コンテンツ記録装置は前記第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）。
【０１３１】

ホスト装置は、前記メモリ派生ＩＤ及び前記コントローラ固有識別子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、ホスト装置は前記メモリ派生ＩＤ及び前記コントローラ固有識別子を全て用いてメディアＩＤを演算する。

【０１３２】

前記メディアＩＤは前記メモリ派生ＩＤ及び前記コントローラ固有識別子を２進演算した結果であり得る。例えば、前記メモリ派生ＩＤ及び前記コントローラ固有識別子をＡＮＤ、ＯＲ、ＸＯＲなどの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。

【０１３３】

前記メディアＩＤは、前記メモリ派生ＩＤ後に前記コントローラ固有識別子を文字列連結演算（ｓｔｒｉｎｇ　ｃｏｎｃａｔｅｎａｔｉｏｎ）した結果であり得る。前記メディアＩＤは前記コントローラ固有識別子の後に前記メモリ派生ＩＤを文字列連結演算した結果でもあり得る。

【０１３４】

以下、本発明の一実施形態によるセキュア鍵の生成及び前記セキュア鍵を利用したコンテンツ復号化方法について図２１を参照して説明する。

【０１３５】

コンテンツ記憶装置にはプリミティブＩＤ及び暗号化コンテンツがそれぞれ格納されている（Ｓ２００，Ｓ２０１）。前記暗号化コンテンツは、記憶装置のメディアＩＤ及びユーザパスワードＡを用いて生成された暗号化鍵を用いて暗号化したものと仮定する。

【０１３６】

ホスト装置は前記プリミティブＩＤを記憶装置から提供される（Ｓ２０２）。図８には図示していないが、ホスト装置は前記プリミティブＩＤの提供を記憶装置に要請し、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。ホスト装置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提供の要請を行うことができる。

【０１３７】

ホスト装置は前記プリミティブＩＤを用いてメディアＩＤを演算する（Ｓ２０３）。ホスト装置がメディア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ホスト装置のメディアＩＤ演算動作と同様であるため、重複する説明は省略する。

【０１３８】

ホスト装置はユーザから入力されたパスワードＡ認証情報を提供される（Ｓ２０４）。この際、入力された認証情報は前記暗号化コンテンツの暗号化鍵生成に使用したものと同一であり得、または異なるものでもあり得るが、説明の便宜上、同一なものと仮定する。

【０１３９】

ホスト装置は前記メディアＩＤ及び前記パスワードＡを用いて復号化鍵を生成する（Ｓ２０５）。

【０１４０】

復号化鍵の生成（Ｓ２０５）は前記メディアＩＤ及び前記ユーザ認証情報のみを用いることもでき、前記メディアＩＤ及び前記ユーザ認証情報の他に一つ以上の可変データまたは固定データをさらに用いることもできる。

【０１４１】

例えば、前記復号化鍵は前記メディアＩＤ及び前記認証情報を２進演算した結果として算出されるデータであり得る。前記復号化鍵は前記２進演算中でもＸＯＲ（ｅｘｃｌｕｓｉｖｅ　ＯＲ）演算の結果として算出されるデータであり得る。すなわち、前記復号化鍵は前記メディアＩＤ及び前記認証情報をＸＯＲ演算した結果のデータであり得る。

【０１４２】

例えば、前記復号化鍵は前記メディアＩＤ及び前記認証情報を文字列連結演算（Ｓｔｒｉｎｇ　Ｃｏｎｃａｔｅｎａｔｉｏｎ、ＳＴＲＣＡＴ）した結果として算出されるデータでもある。前記文字列連結において前後関係は限定されない。すなわち、前記メディアＩ

Ｄの後に前記認証情報が接続され得、前記認証情報の後に前記メディアＩＤが接続され得る。

【０１４３】

ホスト装置は記憶装置に格納された暗号化コンテンツを読み込んだ後（Ｓ２０６）、前記復号化鍵を用いて復号化し（Ｓ２０７）、コンテンツを再生する（Ｓ２０８）。

【０１４４】

図２２を参照してコンテンツ記憶装置Ｘ（２００）に格納されていた暗号化コンテンツがコンテンツ記憶装置Ｙ（２０１）に無断複製される場合、ホスト装置がコンテンツ記憶装置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。

【０１４５】

コンテンツ記憶装置Ｙ（２０１）にはコンテンツ記憶装置Ｘ（２００）とは異なるプリミティブＩＤ　Ｙが格納されている（Ｓ２１０）。

【０１４６】

また、コンテンツ記憶装置Ｘ（２００）は図１６に図示するコンテンツ暗号化方法によって暗号化された暗号化コンテンツが格納されている（Ｓ２０９）。前記暗号化鍵「ＸＡ」の生成に使用された認証情報を「Ａ」と仮定する。ユーザが記憶装置Ｘ（２００）からコンテンツ記憶装置Ｙ（２０１）に前記暗号化コンテンツを無断複製した状況（Ｓ２１１）を仮定する。前記無断複製の結果、コンテンツ記憶装置Ｙ（２０１）に暗号化鍵「ＸＡ」によって暗号化された暗号化コンテンツが格納される（Ｓ２１２）。

【０１４７】

ユーザがホスト装置にコンテンツ記憶装置Ｙ（２０１）を接続し、前記ホスト装置に前記暗号化コンテンツの再生命令を入力する場合、ホスト装置はコンテンツ記憶装置Ｙ（２０１）に格納されたプリミティブＩＤ　Ｙを提供される（Ｓ２１３）。

【０１４８】

ホスト装置は前記プリミティブＩＤ　Ｙを用いてコンテンツ記憶装置Ｙ（２０１）のメディアＩＤ　Ｙを生成する（Ｓ２１４）。

【０１４９】

ホスト装置はユーザ認証情報を入力される（Ｓ２１５）。前記ユーザ認証情報は前記暗号化コンテンツの暗号化鍵の生成に使用された認証情報と同じである「Ａ」と仮定する。

【０１５０】

ホスト装置は、メディアＩＤ　Ｙ及びユーザ認証情報「Ａ」を用いて復号化鍵「ＹＡ」を生成する（Ｓ２１６）。

【０１５１】

ホスト装置は生成された復号化鍵を用いてコンテンツ記憶装置Ｙ（２０１）から提供（Ｓ２１７）された暗号化コンテンツの復号化を試みる（Ｓ２１８）。しかし、生成（Ｓ２１６）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、ホスト装置は前記暗号化コンテンツを復号化できない。

【０１５２】

したがって、ホスト装置は無断複製されて記憶装置２０１に格納された暗号化コンテンツを再生できない（Ｓ２１９）。

【０１５３】

図２２にはホスト装置のユーザが正しい認証情報、すなわち暗号化鍵の生成に使用されたユーザ認証情報と同一なものを入力した場合を仮定したが、間違った認証情報、すなわち暗号化鍵の生成に使用されたユーザ認証情報と異なるものを入力する場合にも、ホスト装置は無断複製されて記憶装置２０１に格納された暗号化コンテンツを再生できない。

【０１５４】

すなわち、無断複製されて記憶装置２０１に格納された暗号化コンテンツは、ユーザ認証情報を正しく入力したかとは関係なく再生できない。

【０１５５】

図２３は、暗号化コンテンツの暗号化鍵を生成することに使用されたユーザ認証情報が正しくない場合、コンテンツ再生を失敗する実施形態を図示する。

【０１５６】

コンテンツ記憶装置Ｘ（２００）には記憶装置のメディアＩＤ及びユーザ認証情報「Ａ」を用いて生成された暗号化鍵「ＸＡ」を用いて暗号化された暗号化コンテンツが格納されている（Ｓ２０９）。

【０１５７】

ユーザがホスト装置にコンテンツ記憶装置Ｘ（２００）を接続し、ホスト装置に前記暗号化コンテンツの再生命令を入力する場合、ホスト装置はコンテンツ記憶装置Ｘ（２００）に格納されたプリミティブＩＤ　Ｘを提供される（Ｓ２２０）。

【０１５８】

ホスト装置は、前記プリミティブＩＤ　Ｘを用いてコンテンツ記憶装置Ｘ（２００）のメディアＩＤ　Ｘを生成する（Ｓ２２１）。

【０１５９】

ホスト装置はユーザ認証情報を入力される（Ｓ２２２）。前記ユーザ認証情報は、前記暗号化コンテンツの暗号化鍵の生成に使用された認証情報と異なる「Ｂ」と仮定する。

【０１６０】

ホスト装置は前記メディアＩＤ　Ｘ及び前記ユーザ認証情報「Ｂ」を用いて復号化鍵「ＸＢ」を生成する（Ｓ２２３）。

【０１６１】

ホスト装置は生成された復号化鍵を用いて記憶装置Ｘ（２００）から提供（Ｓ２２４）された暗号化コンテンツの復号化を試みる（Ｓ２２５）。しかし、生成された復号化鍵「ＸＢ」が前記暗号化コンテンツの復号化鍵「ＸＡ」と異なるため、ホスト装置は前記暗号化コンテンツを復号化できない。

【０１６２】

したがって、ホスト装置はコンテンツ記憶装置に格納された暗号化コンテンツを再生できない（Ｓ２１９）。

【０１６３】

図２３はホスト装置のユーザが正しくない認証情報、すなわち暗号化鍵の生成に使用したユーザ認証情報と異なることを入力した場合を仮定したが、正しい認証情報、すなわち暗号化鍵の生成に使用されたユーザ認証情報と同一なものを入力する場合は記憶装置に格納された暗号化コンテンツを再生することができる。

【０１６４】

以上添付された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せずに他の具体的な形態で実施され得る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、限定的でないものと理解しなければならない。

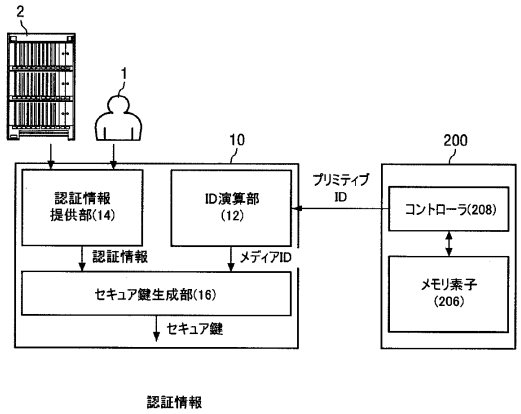
【符号の説明】

【０１６５】

１　ユーザ
２　ユーザ認証サーバ
１０　セキュア鍵生成装置
１２　ＩＤ演算部
１４　認証情報提供部
１６　セキュア鍵生成部
２０　セキュア鍵生成装置
３０　セキュア鍵生成装置
４０　記憶装置
１００　ホスト装置
１０２　プロセッサ

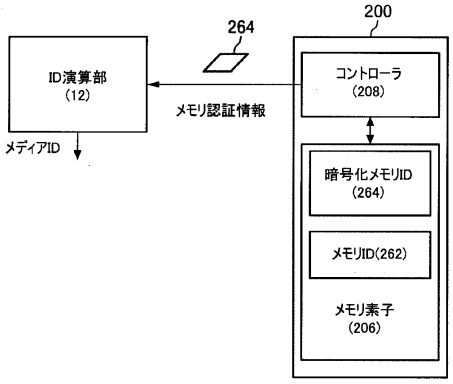
１０４　記憶装置インターフェース
１０６　ＲＡＭ
１０８　入力部
１１０　システムバス
１２０　非セキュア仮想コア
１２２　モニタプロシジャ
１２４　セキュア仮想コア
２００　記憶装置
２０６　メモリ素子
２０８　コントローラ
２１０　ホストインターフェース
２１２　派生ＩＤ演算部
２１４　セキュア鍵生成部
２１６　暗号化部
２１７　ランダムナンバー生成器
２６２　メモリＩＤ
２６４　暗号化メモリＩＤ
３０４　内部記憶装置
３２０　補助ロジック
３２１　暗・復号化エンジン
３２２　コア
３２４　レジスタ
３２５　データパス
１０００　メモリシステム
１１００　不揮発性メモリ装置
１２００　コントローラ

【図１】

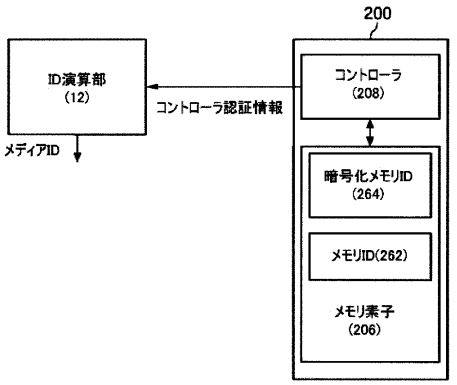


認証情報

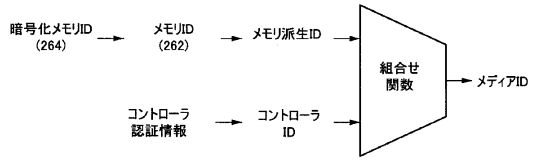
【図２】



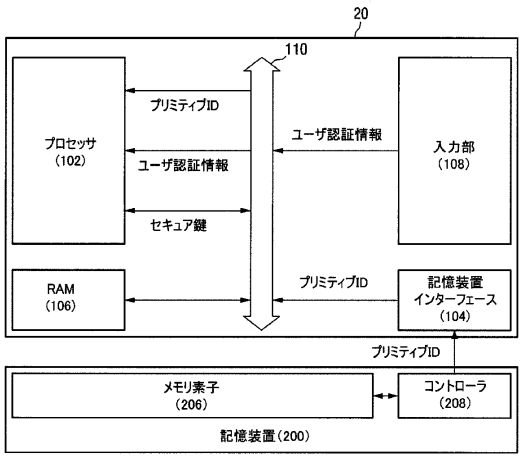
【図３】



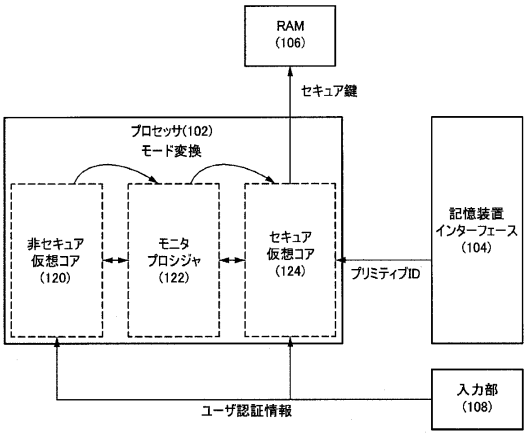
【図４】



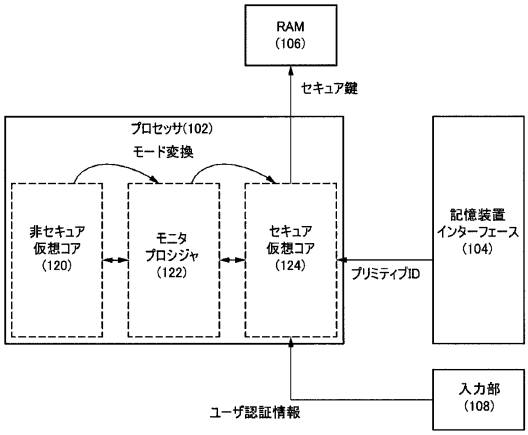
【図５】



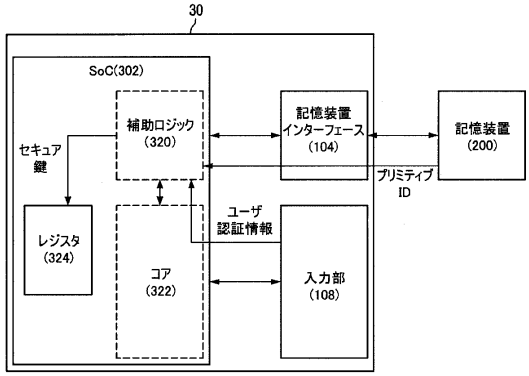
【図６】



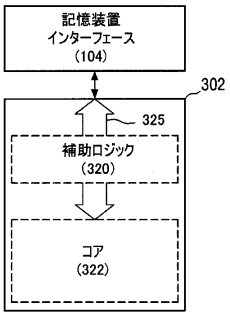
【図７】



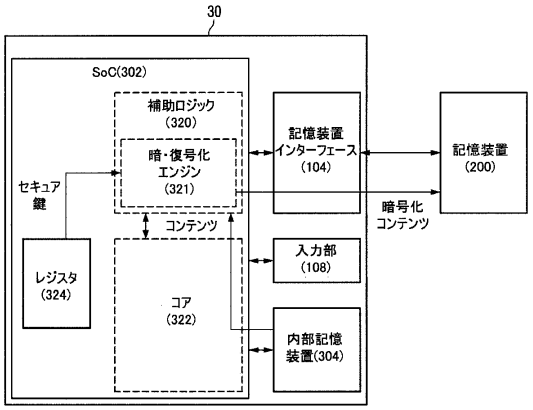
【図８】



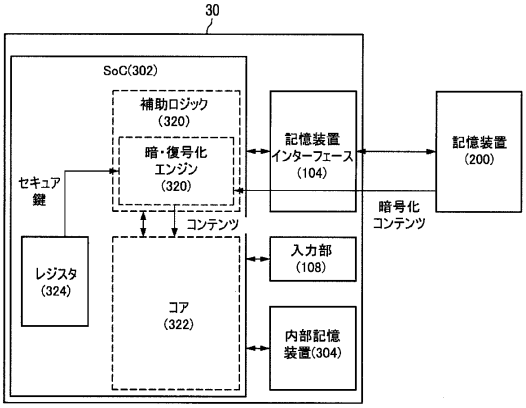
【図９】



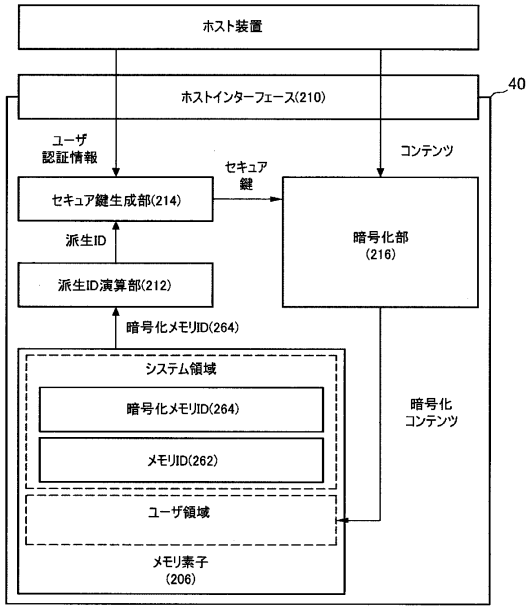
【図１０】



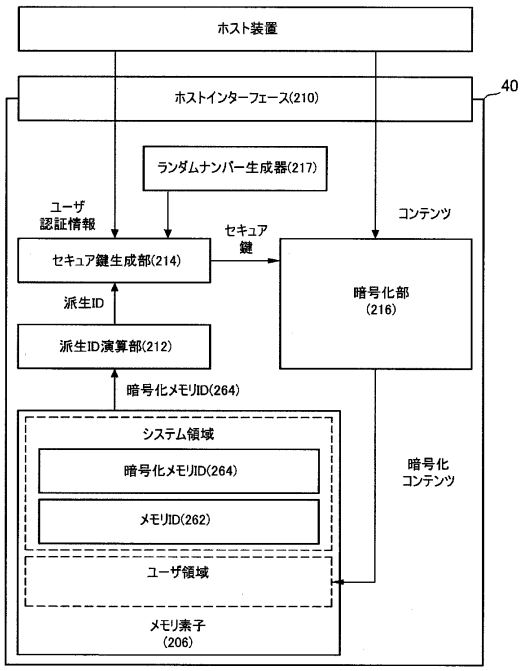
【図１１】



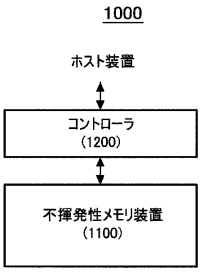
【図１２】



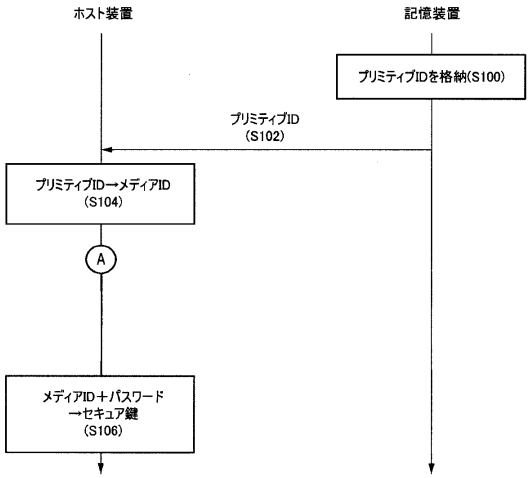
【図１３】



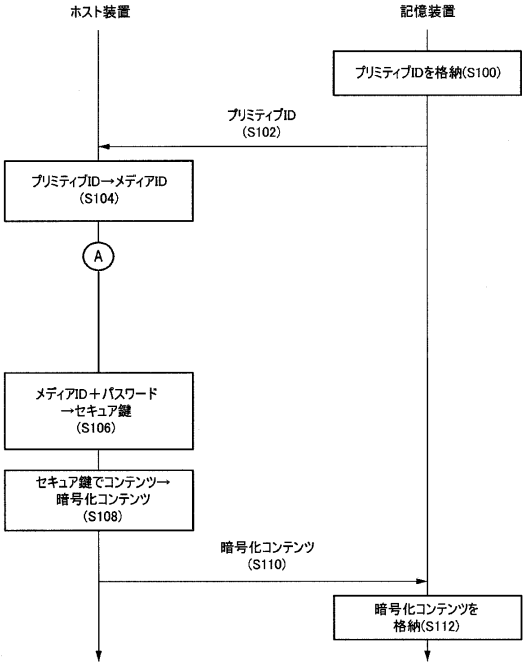
【図１４】



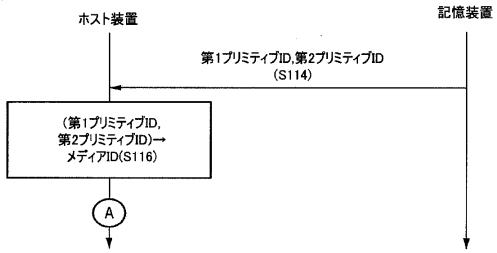
【図１５】



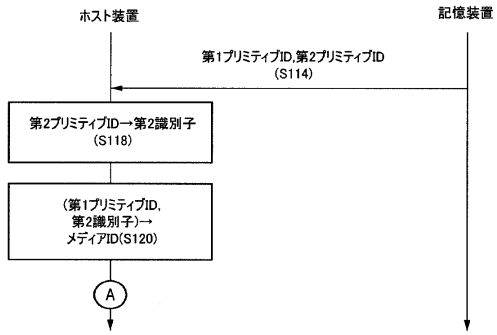
【図１６】



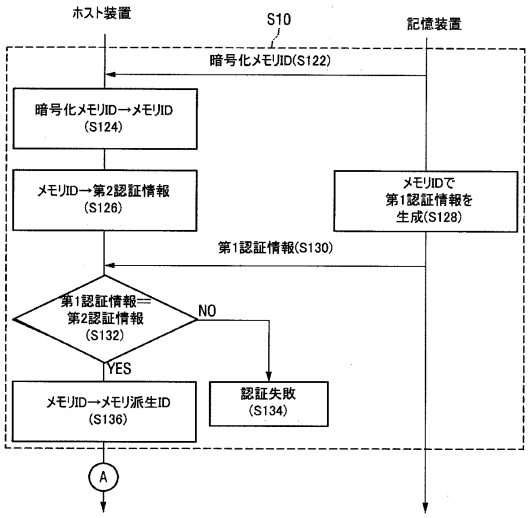
【図１７】



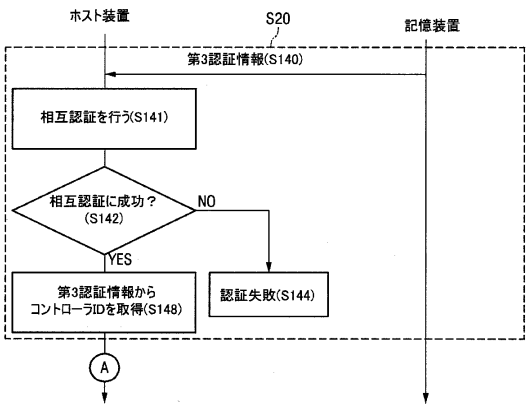
【図１８】



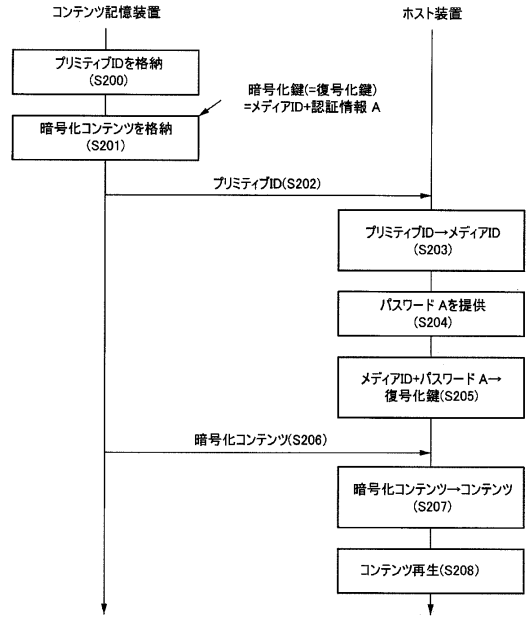
【図１９】



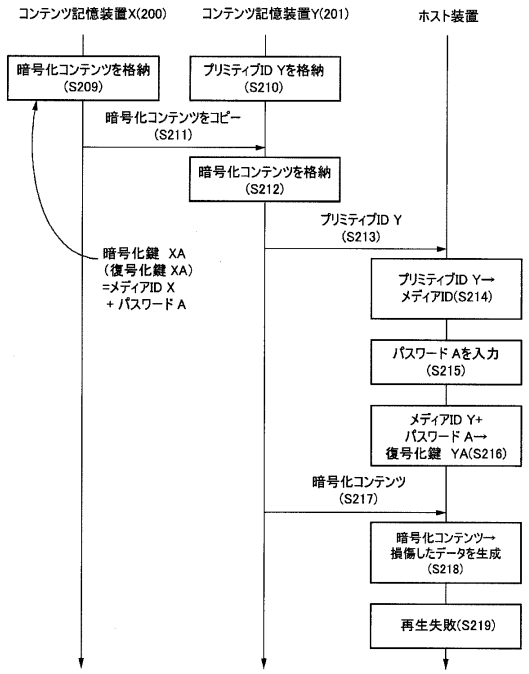
【図２０】



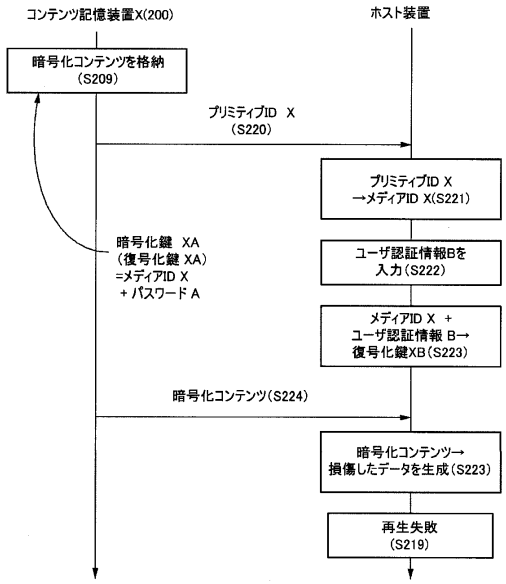
【図２１】



【図２２】



【図２３】


コンテンツ記憶装置X(200)
ホスト装置
暗号化コンテンツを格納
(S209)
プリミティブID X
(S220)
プリミティブID X
→メディアID X(S221)
暗号化鍵 XA
(復号化鍵 XA)
=メディアID X
+パスワード A
ユーザ認証情報Bを
入力(S222)
メディアID X +
ユーザ認証情報 B→
復号化鍵XB(S223)
暗号化コンテンツ(S224)
暗号化コンテンツ→
損傷したデータを生成(S223)
再生失敗
(S219)

フロントページの続き

(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　李　元▲ソク▼
大韓民国京畿道水原市靈通區靈通洞（番地なし）　サルグゴルドンガアパート７１５棟１３０２號
(72)発明者　金　▲ミン▼▲ウク▼
大韓民国ソウル特別市冠岳區幸運洞（番地なし）　ナクソンデヒュンダイホームタウンアパート３０１棟４０４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

審査官　中里　裕正

(56)参考文献　特開２００５－１７４３８８（ＪＰ，Ａ）
特開２００４－２０１０３８（ＪＰ，Ａ）
特開２０１０－０９２２０２（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／０８
Ｈ０４Ｌ　　９／３２