(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4957148号
(P4957148)
(45)発行日　平成24年6月20日(2012.6.20)　(24)登録日　平成24年3月30日(2012.3.30)

(51)Int.Cl.　F I
H04L 9/14 (2006.01)　H04L 9/00 641

請求項の数 4　(全 28 頁)

(21)出願番号　特願2006-260797(P2006-260797)
(22)出願日　平成18年9月26日(2006.9.26)
(65)公開番号　特開2008-85468(P2008-85468A)
(43)公開日　平成20年4月10日(2008.4.10)
審査請求日　平成21年6月9日(2009.6.9)

(73)特許権者　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(74)代理人　100089118
弁理士　酒井　宏明
(72)発明者　西口　直樹
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　長谷川　英司
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

審査官　青木　重徳

最終頁に続く

(54)【発明の名称】鍵管理機能を持つセキュア素子および情報処理装置

(57)【特許請求の範囲】
【請求項１】
コンテンツを複数のブロックに分割して入力する入力部と、
１つのブロックまたは複数のブロックを暗号化するための鍵を順次生成する鍵生成部と、
前記生成鍵を用いて前記１つのブロックまたは複数のブロックを暗号化するコンテンツ暗号部と、
前記暗号化に用いた生成鍵を復元するための鍵情報をその生成鍵から生成する鍵情報生成部と、
前記コンテンツ暗号部によって暗号化された各ブロックのコンテンツと、前記鍵情報生成部で生成された鍵情報とを外部記憶装置へ出力する記憶制御部と、
前記外部記憶装置に記憶されていた鍵情報を受信する復元制御部と、
前記生成鍵の復元状況を管理し、すでに復元された生成鍵の復元状況に基づいて、すでに復元された生成鍵の更新の可否および新たに復元すべき生成鍵の復元の可否を判断する鍵情報復元管理部と、
前記鍵情報復元管理部が前記生成鍵の復元を許可すると判断した場合には、前記復元制御部が受信した鍵情報から前記暗号化に用いた生成鍵を復元し、前記鍵情報復元管理部が前記生成鍵の復元を許可しないと判断した場合には、前記復元制御部が受信した鍵情報から前記暗号化に用いた生成鍵の復元を行わない鍵情報復元部と、
前記外部記憶装置に記憶された各ブロックのコンテンツを復号する情報処理機構に、前

記復元された生成鍵を出力する出力部とを備え、
前記鍵生成部が順次生成する鍵は、所定の条件を満たしたときに新たに生成され、１つのブロックまたは複数のブロックごとに異なることを特徴とする鍵管理機能を持つセキュア素子。
【請求項２】
前記鍵生成部が生成した生成鍵を記憶する鍵情報記憶部をさらに備え、前記鍵情報には、鍵情報記憶部に記憶された生成鍵を特定する鍵インデックスを含むことを特徴とする請求項１のセキュア素子。
【請求項３】
コンテンツを暗号化するための生成鍵の生成および復元と、コンテンツを前記生成鍵を用いて暗号化する機能を有するセキュア制御部と、
前記暗号化されたコンテンツと、前記コンテンツの暗号化に用いた生成鍵を復元することが可能なデータからなる鍵情報とを記憶したコンテンツ記憶部と、
コンテンツ記憶部に記憶されたコンテンツを再生する情報処理部とを備えた鍵管理機能を持つ情報処理装置であって、
前記セキュア制御部が、コンテンツを複数のブロックに分割して入力する入力部と、
所定の条件を満たしたときに、１つのブロックまたは複数のブロックを暗号化するための生成鍵を順次生成する鍵生成部と、前記生成鍵を用いて前記１つのブロックまたは複数のブロックを暗号化するコンテンツ暗号部と、前記暗号化に用いた生成鍵を復元するための鍵情報を、その生成鍵から生成する鍵情報生成部と、前記コンテンツ暗号部によって暗号化された各ブロックのコンテンツと、前記鍵情報生成部で生成された鍵情報とを、前記コンテンツ記憶部へ出力する記憶制御部と、前記情報処理部から、前記暗号化に用いた生成鍵を復元するための鍵情報を受信する復元制御部と、前記生成鍵の復元状況を管理し、すでに復元された生成鍵の復元状況に基づいて、すでに復元された生成鍵の更新の可否および新たに復元すべき生成鍵の復元の可否を判断する鍵情報復元管理部と、前記鍵情報復元管理部が前記生成鍵の復元を許可すると判断した場合には、前記復元制御部が受信した鍵情報から前記暗号化に用いた生成鍵を復元し、前記鍵情報復元管理部が前記生成鍵の復元を許可しないと判断した場合には、前記復元制御部が受信した鍵情報から前記暗号化に用いた生成鍵の復元を行わない鍵情報復元部と、前記復元した生成鍵を前記情報処理部へ出力する出力部とを備え、
前記情報処理部が、前記コンテンツ記憶部から、再生すべきブロックのコンテンツおよび鍵情報を取得する情報取得部と、取得された鍵情報を前記セキュア制御部に与えることにより、その鍵情報に対応する生成鍵をセキュア制御部から取得する鍵取得部と、前記セキュア制御部から取得した生成鍵を用いて、前記コンテンツ記憶部から取得したブロックのコンテンツを順次復元してコンテンツを再生するコンテンツ復元部とを備えたことを特徴とする鍵管理機能を持つ情報処理装置。
【請求項４】
前記請求項３に記載の情報処理装置の鍵管理機能を、コンピュータに実現させるためのプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
この発明は、コンテンツ保護に利用する鍵の管理機能を持つセキュア素子および情報処理装置に関し、特に、デジタル放送などにより取得したデジタルコンテンツを録画または再生するために用いる鍵管理機能を持つセキュア素子と、このセキュア素子を組み込んだ情報処理装置に関する。
【背景技術】
【０００２】
今日、デジタル放送により送られてくるデジタルコンテンツは大容量データであるため、デジタルコンテンツを記録する記録装置としては、ハードディスク（ＨＤＤと呼ぶ）等

が用いられている。しかし、デジタルコンテンツを単純にそのままＨＤＤに保存するだけでは、自由にデジタルコンテンツを複製し不正利用することも可能となる。

【０００３】

そこで、ＤＶＤレコーダなどのデジタルコンテンツの記録再生装置では、専用のハードウェア(LSI)を取りはずしできないように搭載し、ハードウェアに記録された固有の鍵を用いて、取得したデジタルコンテンツを暗号化した後、そのコンテンツをＨＤＤに保存するようにしている。

また、ＨＤＤに保存されたデジタルコンテンツは、ハードウェアによって復号された後、再生される。

【０００４】

これによれば、コンテンツが保存されているＨＤＤが盗まれたとしても、暗号化に使用したハードウェアがない場合には、そのコンテンツを再生することはできない。

PCのようなオープンなプラットフォーム上でデジタルコンテンツを記録再生する場合、コンテンツを録画または再生するためのアプリケーションソフトウェアは、ＬＳＩによって常に監視され、不正なアプリケーションプログラムが存在しても、不正なアプリケーションによる録画・再生処理ができないような保護機構が設けられている。

【０００５】

また、コンテンツを保存するＨＤＤのリストアやリカバリによる不正利用を防止するために、コンテンツリストやＨＤＤの利用状況などを含む管理情報（コンテンツ情報）は、取りはずしのできないＬＳＩの中に記録される。

この他にも、著作権保護等の観点から、デジタルコンテンツの不正利用や不正流出を防止するために、種々のセキュリティ対策が提案されている。

【特許文献１】特開２００３－１９８５２７号公報
【特許文献２】特開２００４－１２９２２７号公報
【特許文献３】特開２００４－３４２０４６号公報
【特許文献４】特開２００５－８５１８８号公報

【発明の開示】

【発明が解決しようとする課題】

【０００６】

しかし、従来技術では、搭載された１つのＬＳＩによって、デジタルコンテンツの暗号化と復号が行われる。

すなわち、ＬＳＩで暗号化されたデジタルコンテンツは、そのＬＳＩと１対１に関係付けられているので、デジタルコンテンツの再生処理やＤＶＤ媒体等への移動処理（ムーブ）、ＤＴＣＰ－ＩＰによる他の情報処理装置への配信処理等をする場合、同じＬＳＩを用いて復号をする必要がある。

ＬＳＩは、一般に、コンテンツの暗号化や復号等をする場合、１つのコンテンツについてのみ処理が可能であるので、自装置内でのコンテンツＡの再生処理と、他のコンテンツＢの他機器への配信処理を同時に行えない。

【０００７】

デジタルコンテンツは一般に大容量であるため、その配信処理に長時間かかることがあるが、配信処理中に、自装置でコンテンツの再生処理ができないのは、ユーザにとって不便である。すなわち、複数のコンテンツを同時に再生や配信したいという要求を満たす装置が望まれる。

一方、同時に処理できるコンテンツの数がＬＳＩの数と一致するとすれば、ＬＳＩを複数個搭載すれば、複数のコンテンツを同時に取り扱えるようになるとも考えられる。たとえば、１０個のＬＳＩを搭載すれば、１０個の異なる再生処理，録画処理および配信処理を、同時に処理できるようになる。

【０００８】

しかし、現在どのコンテンツがどのＬＳＩで使用されているか、再生中であるか、配信中であるかなどを管理する必要があり、各ＬＳＩにそれぞれ記録されているコンテンツ情

報を、ＬＳＩ間で互いに同期させることも必要となり、その情報管理や制御が非常に複雑化し、装置そのもののコストアップにもなる。

以上のように、従来と同様にデジタルコンテンツの不正利用防止などのセキュリティを確保した上で、複数のコンテンツの同時利用と、コストアップの防止および開発工程の複雑化の防止という要求を満たすことが望まれる。

【０００９】

そこで、本願発明は、以上のような事情を考慮してなされたものであり、コンテンツのセキュリティを十分に確保した上で、暗号化および復号に利用する鍵の管理を工夫することにより、コストアップの防止，ソフトウェア資産の有効活用および複数のコンテンツの同時利用を実現することのできる鍵管理機能を持つセキュア素子や情報処理装置を提供することを課題とする。

【課題を解決するための手段】

【００１０】

この発明は、コンテンツを複数のブロックに分割して入力する入力部と、１つのブロックまたは複数のブロックを暗号化するための鍵を順次生成する鍵生成部と、前記生成鍵を用いて前記１つのブロックまたは複数のブロックを暗号化するコンテンツ暗号部と、前記暗号化に用いた生成鍵を復元するための鍵情報をその生成鍵から生成する鍵情報生成部と、前記コンテンツ暗号部によって暗号化された各ブロックのコンテンツと、前記鍵情報生成部で生成された鍵情報とを外部記憶装置へ出力する記憶制御部とを備え、前記鍵生成部が順次生成する鍵は、所定の条件を満たしたときに新たに生成され、１つのブロックまたは複数のブロックごとに異なることを特徴とする鍵管理機能を持つセキュア素子を提供するものである。

これによれば、生成鍵を異ならせてコンテンツのブロックを暗号化しているので、生成鍵の漏洩によるコンテンツの不正利用の軽減を図ることができる。

【００１１】

この発明は、前記外部記憶装置に記憶されていた鍵情報を受信する復元制御部と、受信した鍵情報から前記暗号化に用いた生成鍵を復元する鍵情報復元部と、前記外部記憶装置に記憶された各ブロックのコンテンツを復号する情報処理機構に、前記復元された生成鍵を出力する出力部とをさらに備えたことを特徴とする。

これによれば、セキュア素子では、生成鍵の復元処理を行うが、コンテンツそのものの復号処理は行わないので、セキュア素子の処理負担を軽減でき、１つのセキュア素子を利用する場合でも、複数のコンテンツの同時利用が実質的に可能になる。

また、１つのセキュア素子を利用して複数のコンテンツの同時利用を実現できるので、複数のセキュア素子を用いて複数のコンテンツの同時利用をする場合に比べて、製造および開発のコストの低減と、ハードウェア及びソフトウェアの開発工数の軽減を図ることができる。

【００１２】

さらに、前記鍵情報復元部によって復元された生成鍵の復元状況を管理し、すでに復元された生成鍵の復元状況に基づいて、すでに復元された生成鍵の更新の可否および新たに復元すべき生成鍵の復元の可否を判断する鍵情報復元管理部をさらに備え、復元を許可しないと判断した場合には、前記鍵情報復元部はその許可されなかった生成鍵を復元しないことを特徴とする。

これによれば、生成鍵の復元状況を管理することで生成鍵の復元の可否を判断しているので、生成鍵の漏洩の危険性をより軽減でき、コンテンツの不正流出を防止することができる。

【００１３】

また、この発明は、コンテンツを暗号化するための生成鍵の生成および復元と、コンテンツを前記生成鍵を用いて暗号化する機能を有するセキュア制御部と、前記暗号化されたコンテンツと、前記コンテンツの暗号化に用いた生成鍵を復元することが可能なデータからなる鍵情報とを記憶したコンテンツ記憶部と、コンテンツ記憶部に記憶されたコンテン

ツを再生する情報処理部とを備えた鍵管理機能を持つ情報処理装置であって、前記セキュア制御部が、コンテンツを複数のブロックに分割して入力する入力部と、所定の条件を満たしたときに、１つのブロックまたは複数のブロックを暗号化するための生成鍵を順次生成する鍵生成部と、前記生成鍵を用いて前記１つのブロックまたは複数のブロックを暗号化するコンテンツ暗号部と、前記暗号化に用いた生成鍵を復元するための鍵情報を、その生成鍵から生成する鍵情報生成部と、前記コンテンツ暗号部によって暗号化された各ブロックのコンテンツと、前記鍵情報生成部で生成された鍵情報とを、前記コンテンツ記憶部へ出力する記憶制御部と、前記情報処理部から、前記暗号化に用いた生成鍵を復元するための鍵情報を受信する復元制御部と、受信した鍵情報から前記暗号化に用いた生成鍵を復元する鍵情報復元部と、前記復元した生成鍵を前記情報処理部へ出力する出力部とを備え、前記情報処理部が、前記コンテンツ記憶部から、再生すべきブロックのコンテンツおよび鍵情報を取得する情報取得部と、取得された鍵情報を前記セキュア制御部に与えることにより、その鍵情報に対応する生成鍵をセキュア制御部から取得する鍵取得部と、前記セキュア制御部から取得した生成鍵を用いて、前記コンテンツ記憶部から取得したブロックのコンテンツを順次復元してコンテンツを再生するコンテンツ復元部とを備えたことを特徴とする鍵管理機能を持つ情報処理装置を提供するものである。

【００１４】

これによれば、生成鍵を異ならせることにより生成鍵の漏洩の危険性の軽減とコンテンツの不正利用の軽減を図り、また、コンテンツ自体の復号は情報処理部で行い、セキュア制御部では比較的短時間で実施可能な鍵の復元処理を行うので、コンテンツの再生時におけるセキュア制御部の処理負担の軽減を図ることができ、１つのセキュア制御部を備えるだけで、複数のコンテンツの同時利用が実質的に可能となり、複数のコンテンツの同時利用を実現する場合のコストの低減と開発工数の軽減を図ることができる。

【００１５】

また、この発明は、コンピュータに、情報処理装置の鍵管理機能を実現させるためのプログラムを提供するものである。

この発明において、コンテンツとは、動画，静止画，音声などのマルチメディア情報やこれらのストリーミングデータを意味する。

コンテンツの暗号化は、受信と並行して行われ、所定の容量サイズのコンテンツごとに暗号化される。暗号化されるコンテンツの一単位をブロックと呼ぶ。

外部記憶装置とは、後述するようなコンテンツ記憶装置、具体的にはハードディスク（ＨＤＤ）のような不揮発性の書き換え可能な媒体である。

【００１６】

この発明のセキュア素子とは、後述するセキュア制御部（ＬＳＩ）に相当し、一般には、ＩＣチップのような半導体集積回路素子として提供されるものである。

情報処理部とは、コンテンツの再生や配信を担当する機能ブロックであり、後述するアプリケーションプログラムに相当する。

また、この発明において、前記鍵情報には、セキュア素子固有のマスタ鍵によって暗号化された生成鍵を含むことを特徴とする。

また、前記鍵情報には、前記生成鍵と、暗号化のためにその生成鍵を適用したコンテンツのブロックを特定する範囲情報とが含まれることを特徴とする。

【００１７】

さらに、前記鍵生成部が生成した生成鍵を記憶する鍵情報記憶部をさらに備え、前記鍵情報には、鍵情報記憶部に記憶された生成鍵を特定する鍵インデックスを含むことを特徴とする。

また、前記鍵情報に、前記鍵インデックスによって特定される生成鍵を適用したコンテンツのブロックを特定する範囲情報をさらに含むことを特徴とする。

また、前記鍵生成部は、鍵初期値を生成しその鍵初期値から所定の規則に基づいてその後の鍵を生成し、前記鍵情報には、鍵初期値を含むことを特徴とする。

生成鍵を生成するための所定の条件とは、生成鍵を生成するタイミングを決めるための

条件を意味し、後述するような種々のタイミングが考えられる。たとえば、暗号化処理の一単位である一ブロック分のコンテンツを受信するごとに、新たな鍵を生成してもよい。あるいは、所定の容量サイズに相当する複数のブロックを受信するごとに新たな鍵を生成してもよい。この生成タイミングについての詳細は後述する。

【発明の効果】

【００１８】

この発明によれば、コンテンツを暗号化するための生成鍵を異ならせてコンテンツのブロックを暗号化しているので、生成鍵の漏洩の危険性を軽減でき、たとえ生成鍵の１つが不正に流出したとしてもコンテンツ全体を不正利用することは困難であり、コンテンツ保護に必要かつ十分なセキュリティを確保することができる。

また、この発明のセキュア素子は、生成鍵の復元処理を担当し、コンテンツそのものの復元処理は行わないので、セキュア素子の処理負担を軽減できる。したがって、１つのセキュア素子を用いて複数のコンテンツの同時利用が実質的に可能となる。

【００１９】

さらに、１つのセキュア素子を用いて複数のコンテンツの同時利用を実現できるので、複数のセキュア素子を用いる場合に比べて、製造および開発のコストの低減と、ハードウェアおよびソフトウェアの開発工数の軽減を図ることができる。

また、コンテンツの再生をする場合、その再生に必要な生成鍵の復元状況を管理しながら生成鍵の復元の可否を判断しているので、不正な手段による生成鍵の漏洩の危険性を軽減でき、コンテンツの不正流出を防止できる。

【発明を実施するための最良の形態】

【００２０】

以下、図面を使用して本発明の実施の形態を説明する。なお、以下の実施例の記載によって、この発明が限定されるものではない。

＜この発明の情報処理装置の構成＞

図１に、この発明の情報処理装置の一実施例の構成ブロック図を示す。

この発明の情報処理装置は、主として、コンテンツ受信部１，セキュア制御部２，コンテンツ記憶装置３，および情報処理部４とから構成される。

コンテンツ受信部１は、画像，音声，文書などの種々の情報を受信する部分であり、たとえばデジタル放送によって送られてくる画像情報を受信するチューナに相当する。

【００２１】

セキュア制御部２は、取りはずしできないように基板等に固着されたＬＳＩチップであり、この中に、ＣＰＵ，ＲＯＭ，ＲＡＭ，Ｉ／Ｏコントローラ，タイマー等を含むマイクロコンピュータが搭載されている。

セキュア制御部２は、機能的に分類すると、主として鍵管理部とコンテンツ暗号部とを有する。

コンテンツ暗号部は、受信したコンテンツを、このセキュア制御部２で生成される鍵（Ｋ２）を用いて、暗号化する部分である。暗号化されたコンテンツは、コンテンツ記憶装置３に、後述するような鍵情報とともに格納される。

鍵管理部は、コンテンツを暗号化および復号するための鍵（Ｋ２）を生成し、記憶すると共に、情報処理部からの要求に基づいてその鍵（Ｋ２）を情報処理部４に与える処理をする部分である。その際、鍵（K2）は暗号化されて情報処理部４に与えられる。

【００２２】

コンテンツ記憶装置３は、コンテンツ，鍵情報およびコンテンツリストを記憶したメモリであり、主としてハードディスク（ＨＤＤ）などの大容量記憶装置が用いられる。ただし、不揮発性の書き換え可能な記録媒体を用いてもよい。たとえば、フラッシュメモリ，ＵＳＢメモリ，ＣＤ－ＲＷ，ＤＶＤ－ＲＷ，ＤＶＤ－ＲＡＭなどを用いてもよい。

ここで、コンテンツリストとは、ＨＤＤ３に記憶されるコンテンツと鍵情報とを関係付けた情報であり、このリストを見れば、コンテンツがどのような暗号化形式で、ＨＤＤ内のどこに保存されているかがわかる。

鍵情報とは、鍵管理部で生成された鍵（Ｋ２）の他に、その鍵を特定することのできるインデックス情報や、その鍵を適用するコンテンツを特定する範囲情報などを含む。鍵情報の具体例については、図７に示す。

【００２３】

情報処理部４とは、受信したコンテンツに対して特定の処理を実行する部分であり、アプリケーションプログラムに相当する。

たとえば、受信したコンテンツをＨＤＤ３に録画するための録画プログラム，ＨＤＤ３に保存されたコンテンツを再生するための再生プログラム，ＨＤＤ３に保存されたコンテンツを他の記録媒体（ＤＶＤ－Ｒなど）やネットワークを介して接続された他の情報機器に転送するための配信プログラムなどが、情報処理部４に相当する。

これらのアプリケーションプログラムは、前記したような情報取得部，鍵取得部およびコンテンツ復元部に相当する機能モジュールを含む。

【００２４】

この発明の情報処理装置は、たとえば、パソコンやワークステーションのような情報機器であり、この発明の主要な機能は、パソコン等に搭載されたマイクロコンピュータとセキュア制御部と、ＨＤＤなどに格納された制御プログラムおよびアプリケーションプログラムにより実現される。

【００２５】

この発明の情報処理装置の主要な機能には、コンテンツの録画機能と、コンテンツの再生（復元）機能とがある。以下、この発明の録画機能と再生機能の概略について説明する。

コンテンツの録画は、たとえば、アプリケーションプログラム４から録画要求がセキュア制御部２に与えられることにより開始する。この後セキュア制御部２では、鍵管理部が暗号化用の鍵（Ｋ２）を生成し、鍵（K２）をセキュア制御部２特有の鍵（Km）で暗号化し、コンテンツ暗号部が、受信されたコンテンツを鍵（Ｋ２）を用いて暗号化し、ＨＤＤ３へ格納する。ＨＤＤ３に格納されたコンテンツは鍵（K2）で暗号化されており、鍵（K2）はセキュア制御部２特有の鍵（Ｋｍ）で暗号化されている。

したがって、ＨＤＤ３が盗難され、ＨＤＤ３の中のコンテンツが読み出されたとしても、セキュア制御部特有の鍵（Ｋｍ）がわからなければ、コンテンツを復元することはできない。

【００２６】

コンテンツの受信は、チューナ１で連続的に受信されるが、受信されたコンテンツは所定容量ごとあるいは所定時間ごとに区切られ、区切られたブロックごとに、順次暗号化され、ＨＤＤへ格納される。

この発明では、暗号化のために用いる鍵（Ｋ２）を、１ブロックごと、あるいは数ブロックごとに生成する。たとえば、１つのブロックごとに暗号化の鍵（Ｋ２）を異ならせ、ブロックごとに異なる鍵（Ｋ２）で暗号化する。そして、暗号化されたブロックのコンテンツと、そのブロックを暗号化した鍵（Ｋ２）を特定する鍵情報とを対応づけて、ＨＤＤに格納する。

あるいは、たとえば１０秒間に受信される複数のブロックコンテンツは、同じ暗号化鍵Ｋ２－１で暗号化するが、次の１０秒間に受信されるブロックコンテンツについては新たに鍵Ｋ２－２を生成し、この新しく生成した鍵Ｋ２－２で暗号化する。

【００２７】

コンテンツの再生（復元）は、たとえば、アプリケーションプログラム４から再生（復号）要求がセキュア制御部２に与えられることにより開始する。再生要求には、ＨＤＤ３から読み出したコンテンツ情報（コンテンツIDなど）が含まれる。

セキュア制御部２では、再生要求に含まれるコンテンツ情報などから、どのコンテンツを再生するかを解釈し、再生すべきコンテンツに対応づけられた鍵情報を、ＨＤＤ３から読み出す。読み出した鍵情報やあるいはセキュア制御部２に記憶されている情報から、再生するコンテンツに対応づけられた鍵（Ｋ２）を復元し、アプリケーションプログラム４

に与える。
　また、再生要求されたコンテンツそのものは、セキュア制御部を介さずに、ＨＤＤ３から直接アプリケーションプログラム４に与えられる。
　アプリケーションプログラム４では、ＨＤＤ３から読み出したコンテンツを、セキュア制御部２から与えられた鍵（Ｋ２）を用いて復元する。復元されたコンテンツは、ＣＲＴやＬＣＤなどの表示装置で再生されたり、他の記録媒体へ移動されたり、ネットワークを介して他の情報機器へ配信される。
【００２８】
　以上のように、この発明では、コンテンツの録画時において、セキュア制御部にて複数の鍵（Ｋ２）を順次生成し、異なる鍵（Ｋ２）を用いてコンテンツを暗号化することを特徴とする。
　また、コンテンツ再生時において、コンテンツそのものについては、ＨＤＤに保存された状態の暗号化されたコンテンツを、ＨＤＤ３からアプリケーションプログラム４へ直接出力し、一方、暗号化されたコンテンツを復元するための鍵（Ｋ２）は、セキュア制御部２により復元し、セキュア制御部２からアプリケーションプログラム４へ出力する。
　このようにセキュア制御部で鍵（Ｋ２）の生成，復元，出力を管理することにより、コンテンツ保護，不正利用の防止というセキュリティを十分に確保し、セキュア制御部は、比較的短時間で処理可能な鍵の生成と復元のみを行うので、１つのセキュア制御部のみを用いても複数のコンテンツをほぼ同時に処理することができる。
【００２９】
＜セキュア制御部の構成ブロックの説明＞
　図２に、この発明で用いるセキュア制御部の構成ブロック図を示す。
　セキュア制御部２は、上記したように鍵管理部とコンテンツ暗号部２３とを備え、さらに、チューナ１とのインタフェースとなる入力部２１，アプリケーションプログラム４とのインタフェースとなる出力部２８，ＨＤＤ３とのインタフェースとなる記憶制御部２９および復元制御部３０とを備える。
　ここで、鍵管理部は、鍵生成部２２，鍵情報生成部２４，鍵情報復元部２６，鍵情報復元管理部２７，鍵情報記憶部２５とから構成される。
【００３０】
　この発明では、複数のＬＳＩを備えて複数のコンテンツに対して同時に再生や配信を行うのではなく、１つのＬＳＩのみを備え、複数のコンテンツの再生や配信処理をほぼ同時に行うようにすることを特徴とする。
　したがって、１つのＬＳＩのみを用いるので、複数のＬＳＩを用いた場合よりも、部品コストや製造コストを抑制することができ、複数のＬＳＩの同期をとって相互に動作させるためのハードウェアやソフトウェアも必要がなく、開発コストも低減することができる。
【００３１】
　入力部２１はチューナ１から与えられるコンテンツを、コンテンツ暗号部２３へ与える部分である。デジタル放送などの動画コンテンツは、連続して送られてくるので、たとえば所定のデータ量（１Ｍバイトなど）ごとにブロック化して、コンテンツ暗号部２３へ与えられる。１つのブロックが、暗号化処理の一単位となる。ブロック化は、一定時間ごと（たとえば、１０秒）に行ってもよい。
　また、１つのブロックあるいは所定数のブロックに相当するコンテンツが受信されるごとに、鍵生成部２２に対して鍵（Ｋ２）の生成が要求される。鍵生成部２２は、１つのブロックを暗号化するための鍵（Ｋ２）を生成する部分である。鍵（Ｋ２）を生成するタイミングは種々のものが考えられるが、後述する。
　セキュア制御部２の鍵情報記憶部２５に、マスタ鍵Ｋｍを、書き換えできないように予め格納しておく。鍵生成部２２で生成された鍵Ｋ２は、このマスタ鍵Ｋｍを用いて暗号化され、ＨＤＤ３に格納される。ただし、鍵Ｋ２をセキュア制御部の内部に記憶する場合は、鍵情報に鍵K2そのものは保存されないため、鍵K2を示す情報は暗号化せずにそのままHD

D3に格納してもよい。

【００３２】

コンテンツ暗号部２３は、鍵生成部２２によって生成された鍵Ｋ２を用いて、１ブロック分のコンテンツを暗号化する部分である。

ただし、一般的には、チューナ１から与えられるコンテンツ自体もすでに暗号化されている場合がある。この場合は、入力部２１で暗号化されたコンテンツを一旦取得した後、その暗号化に用いられている鍵（Ｋ１）を用いて暗号化されたコンテンツを復号した後、コンテンツ暗号部２３へ与える。この鍵Ｋ１は、チューナ１から与えられるか、または予めセキュア制御部に格納しておく。

すなわち、鍵Ｋ１で暗号化されていた受信コンテンツを、鍵Ｋ１で復号したものが、コンテンツ暗号部２３で、鍵Ｋ２を用いて暗号化される。鍵Ｋ２で暗号化されたコンテンツを、以下、Ｋ２（コンテンツ）と表記する。Ｋ２（コンテンツ）は、記憶制御部２９に与えられ、ＨＤＤ３へ格納される。

【００３３】

鍵情報生成部２４は、生成された鍵Ｋ２を用いて鍵情報ＫＪを生成する部分である。

鍵情報ＫＪとは、生成された鍵Ｋ２を特定するための情報であり、後述するように種々の形態が考えられる。たとえば、生成された鍵Ｋ２をマスタ鍵Ｋｍで暗号化したものの場合、鍵情報記憶部の鍵Ｋ２を示すインデックスとその鍵Ｋ２を適用するコンテンツの範囲を示す情報からなる場合などがある。

生成された鍵情報ＫＪは、記憶制御部２９に与えられ、ＨＤＤ３へ格納される。

【００３４】

記憶制御部２９は、暗号化されたコンテンツブロックと鍵情報ＫＪを、ＨＤＤ３へ記憶させる部分である。また、コンテンツブロックと鍵情報ＫＪを記憶する際には、両者を関係づける情報が、コンテンツリスト３５に記憶される。

コンテンツ記憶装置ＨＤＤ３は、主として、コンテンツリスト３５，鍵情報ＫＪ３６，コンテンツ３７を記憶するメモリである。ここで、コンテンツ３７は、生成された鍵Ｋ２で暗号化されたブロックのコンテンツである。

また、ＨＤＤ３に格納される鍵情報ＫＪ３６に鍵Ｋ２が含まれる場合は、鍵Ｋ２そのものではなく、マスタ鍵Ｋｍもしくはマスタ鍵以外にセキュア制御部に保持している固有の鍵（マスタ鍵から生成することも可能）で暗号化された鍵Ｋ２を記憶する。ここで、マスタ鍵Ｋｍで暗号化された鍵Ｋ２を、Ｋｍ（Ｋ２）と表記する。

【００３５】

図５に、コンテンツ記憶装置ＨＤＤ３に記憶される情報の一実施例の説明図を示す。

コンテンツ３７は、コンテンツごとに、１つのコンテンツファイル（ＣＦ０１，ＣＦ０２……）として記憶される。鍵情報ＫＪ３６は、コンテンツファイルにそれぞれ対応するファイル（ＫＪ０１，ＫＪ０２……）として記憶される。

コンテンツリスト３５は、コンテンツ名（ｃｔ－Ａ，ｃｔ－Ｂ……）と、コンテンツファイルの名称および格納場所と、鍵情報ファイルの名称および格納場所とを対応づけた状態で記憶したリストである。

コンテンツを鍵情報に対応付けて、複数のファイルで表現することも可能である。

【００３６】

鍵情報記憶部２５は、セキュア制御部２で利用する種々の情報を格納したものであり、固定記憶されたマスタ鍵Ｋｍの他に、生成された鍵Ｋ２，出力部２８から出力された鍵，鍵生成のための初期値、鍵生成の計算方法などを記憶する部分である。

復元制御部３０は、鍵情報復元部２６からの要求により、鍵情報ＫＪをＨＤＤ３から読み出す部分である。読み出した鍵情報ＫＪは、鍵情報復元部２６に与えられる。

鍵情報復元部２６は、鍵（Ｋ２）を復元する部分である。ここでは、復元制御部３０によって読み出された鍵情報ＫＪをもとに鍵（Ｋ２）を復元する。鍵情報KJに応じて鍵情報記憶部から情報を取得する。復元された鍵（Ｋ２）は、出力部２８が、再生要求や配信要求をしたアプリケーションプログラム４に対して、出力する。

【００３７】
鍵情報復元管理部２７は、復元された鍵の取得と更新の時刻や、復元の可否の判定フラグなどの情報を管理する部分である。
たとえば、アプリケーションに対して同時に出力できる鍵を一つとすると、ある鍵ＫＥＹをアプリケーションプログラムＡに出力した場合、その出力した時刻を記憶し、その出力した状態でアプリケーションプログラムAから異なる鍵ＫＥＹの出力（復元）要求があった場合、その鍵ＫＥＹの出力（復元）は認めないようにし、復元不可であることを、アプリケーションプログラムAに返信する。この場合は、鍵KEYの使用を止めることを通知した後、他の鍵を要求することで鍵の出力（復元）が可能になる。
【００３８】
以上がセキュア制御部２の主要構成モジュールであるが、各モジュールの機能は、ＬＳＩに内蔵されたマイクロコンピュータと、ＬＳＩ内部のＲＯＭ等やフラッシュメモリ等に格納された制御プログラムにより実現される。ＬＳＩ内部の鍵情報記憶部２５は、不揮発性の書き換え可能なメモリを用いることが好ましい。
【００３９】
このように、セキュア制御部２では主としてコンテンツの暗号化と鍵の生成および復元を行うが、暗号化されていたコンテンツの復号（復元）は、セキュア制御部の内部では行わない。コンテンツの復号をするために、コンテンツ自体をＨＤＤ３から読出す処理は、セキュア制御部を介さずに、図示しない別のロジックによって行われ、読み出されたコンテンツは、アプリケーションプログラムに直接与えられる。そして、アプリケーションプログラムが、読み出されたコンテンツの復号を行う。
【００４０】
＜この発明のコンテンツの暗号化と鍵管理の説明＞
図３に、この発明のコンテンツと鍵の暗号化処理などの概略説明図を示す。
また、図４に、従来から行われているコンテンツと鍵の暗号化処理などの概略説明図を示す。
まず、図４における従来の暗号化処理などについて、説明する。
ここで、「Ｋｎ」は鍵ｎを示し、「Ｋｍ」は、セキュア制御部特有のマスタ鍵を示す。また、「Ｋｎ（Ｄ）」は、鍵ｎによって暗号化されたＤを示す。ここでＤとは、暗号化する対象を意味し、たとえば、コンテンツや鍵が該当する。
【００４１】
図４の１１１において、チューナ１で受信されたコンテンツを入力する。ここで、入力されるコンテンツは、鍵Ｋ１で暗号化されたコンテンツ（Ｋ１（コンテンツ））とする。鍵Ｋ１は、予めセキュア制御部２に格納されるか、またはコンテンツと同様に暗号化された形式で入力される。入力されたコンテンツ（Ｋ１（コンテンツ））は、鍵Ｋ１で復号される（１１２）。
また、入力されたコンテンツに対して、１つの鍵Ｋ２０が生成される。その後、鍵Ｋ１で復号されたコンテンツは、生成鍵Ｋ２０を用いて暗号化される（１１３）。鍵Ｋ２０で暗号化されたコンテンツ（Ｋ２０（コンテンツ））は、ＨＤＤ３に記憶される（１１５）。
一方、生成鍵Ｋ２０は、マスタ鍵Ｋｍを用いて暗号化される（１１４）。暗号化された鍵（Ｋｍ（Ｋ２０））は、コンテンツと対応づけられて、ＨＤＤ３に記憶される（１１６）。
以上が、コンテンツの録画処理に相当する。
【００４２】
コンテンツの再生処理の場合は、ＨＤＤ３から、再生すべきコンテンツ（Ｋ２０（コンテンツ））と鍵（Ｋｍ（Ｋ２０））とが読み出される。すなわち、コンテンツと鍵が、どちらもセキュア制御部２に与えられる。
読み出された鍵は、マスタ鍵Ｋｍを用いて、セキュア制御部で復号される。その後、読み出されたコンテンツが、復号された鍵Ｋ２０を用いて、セキュア制御部で復号される（

１１７）。
次に、セキュア制御部内部で、鍵Ｋ３が生成され、この鍵Ｋ３を用いて、復号されたコンテンツを暗号化する（１１８）。この暗号化は、コンテンツをアプリケーションプログラムに与えるときに流出し不正利用されるのを防止するためである。
【００４３】
暗号化されたコンテンツ（Ｋ３（コンテンツ））と鍵Ｋ３とは、セキュア制御部から、再生要求をしたアプリケーションプログラム４に出力される。アプリケーションプログラム４では、鍵Ｋ３を用いて、暗号化されたコンテンツ（Ｋ３（コンテンツ））を復号する（１１９）。これにより、再生可能なコンテンツが生成され、その後表示装置などに表示される。
このように、従来のものでは、再生処理時において、鍵およびコンテンツの両方が、セキュア制御部２を介して、復元されかつアプリケーションプログラム４に与えられる。
【００４４】
一方、図３のこの発明の処理では、セキュア制御部２では、再生処理時には、鍵の復元とアプリケーションプログラム４への引き渡しが行われるが、コンテンツの復元は行われない。
図３において、コンテンツの受信処理については、従来と同様に、暗号化されたコンテンツ（Ｋ１（コンテンツ））の入力（１０１）が行われ、鍵Ｋ１を用いてそのコンテンツが復号される（１０２）。
次に、１つのブロックに相当するコンテンツが入力された場合、鍵Ｋ２が生成され、この鍵Ｋ２を用いて、復号されたコンテンツが暗号化される（１０３）。
暗号化されたコンテンツ（Ｋ２（コンテンツ））は、ＨＤＤ３に記憶される（１０５）。
【００４５】
また、生成された鍵Ｋ２は、マスタ鍵Ｋｍで暗号化される（１０４）。暗号化された鍵（Ｋｍ（Ｋ２））は、鍵情報としてＨＤＤ３に記憶される（１０６）。
また、鍵Ｋ２は、その後入力されるコンテンツの所定数のブロックごと、あるいは、所定時間内のブロックごとに新たに生成され、その入力されたブロックごとに新たに生成された鍵Ｋ２を用いて暗号化される。
さらに、ＨＤＤ３には、入力されたブロック数に相当する数の、コンテンツと、そのブロックを暗号化した鍵Ｋ２から生成した鍵情報ＫＪとが、対応づけて記憶される。このとき、コンテンツリストも作成される。
【００４６】
コンテンツの再生時においては、ＨＤＤ３から、再生すべきコンテンツ（Ｋ２（コンテンツ））と、これに対応する鍵情報ＫＪとが、直接アプリケーションプログラム４によって読み出される。
また、コンテンツに対応する鍵情報KJをセキュア制御部に渡す。これにより、再生すべきコンテンツと対応づけられて記憶されていた鍵（Ｋｍ（Ｋ２））が、セキュア制御部２に読み出される。読み出された鍵（Ｋｍ（Ｋ２））は、マスタ鍵Ｋｍを用いて復号される（１０７）。復号された鍵Ｋ２は、再生要求をしたアプリケーションプログラム４に与えられる。
再生要求をしたアプリケーションプログラム４は、直接与えられたコンテンツ（Ｋ２（コンテンツ））を、セキュア制御部２から与えられた鍵Ｋ２を用いて復号する（１０８）。復号されたコンテンツは、再生可能なコンテンツであり、表示装置などで再生される。
【００４７】
したがって、コンテンツそのものの復号処理は、アプリケーションプログラムで行われ、セキュア制御部２では行われない。再生時において、セキュア制御部２では、比較的短時間で処理できる鍵の復号処理のみが行われるので、セキュア制御部２が１つの再生処理に長時間拘束されてしまうことがない。よって、２つのアプリケーションプログラム４による再生要求処理と配信要求処理が同時間帯にあったとしても、セキュア制御部２では、

再生と配信のためのそれぞれの鍵の復元処理が短時間の間に行われるだけであり、１つの処理に長時間専有されることはないので、セキュア制御部が１つでも、その後の再生と配信処理をほぼリアルタイムで並行して行うことができる。

【００４８】

＜鍵の生成タイミングと、鍵情報および暗号化コンテンツの説明＞

ここでは、ブロックの暗号化に用いる生成鍵を生成するタイミングと、鍵情報生成部２４で生成される鍵情報ＫＪと、コンテンツ暗号部２３で暗号化されるコンテンツについて説明する。

入力されたコンテンツは、上記したように、ブロックに分けられ、そのブロックごとに鍵Ｋ２を用いて暗号化される。このとき、鍵Ｋ２は、１つのブロックごとあるいは数ブロックごとに異なるものが生成されるが、生成されるタイミングとしては、次のようなタイミングが考えられる。

【００４９】

（ａ）予め固定的に定められた暗号化処理の容量サイズに相当する数のブロックが入力されたとき。

この暗号化処理の容量サイズは、セキュア制御部に予め記憶される。

たとえば、予め定められた容量サイズが１メガバイトで、暗号化する１つのブロックのサイズが１メガバイトであれば、その１つのブロックごとに、異なる鍵Ｋ２が新たに生成される。

あるいは、予め定められた容量サイズが１メガバイトで、１つのブロックのサイズが２００キロバイトであれば、５つのブロックは同じ鍵Ｋ２－１で暗号化されるが、次の５つのブロックは、新たに生成された鍵Ｋ２－２で暗号化される。

【００５０】

（ｂ）暗号化処理の容量サイズを複数種類用意し、この中のいずれかの容量サイズに相当する複数のブロックが入力されたとき。

すなわち、暗号化処理の容量サイズが１つではなく可変的にいくつか設定される場合に相当する。コンテンツの種類、たとえば動画と静止画などの区別、圧縮率の高低の区別によって、暗号化処理する単位容量が異なる場合には、暗号化処理する容量サイズによって、鍵を生成するタイミングも異ならせる。この場合、暗号化処理の容量サイズは、セキュア制御部に、予め複数個記憶しておいてもよく、また、コンテンツの入力のときに、その都度、外部装置から指示入力してもよい。

たとえば、指示入力された容量サイズに相当する数のブロックが入力されるごとに、新たに鍵Ｋ２が生成される。

【００５１】

（ｃ）予め定められたコンテンツの暗号化処理時間

たとえば、固定的に予め定められた時間を１０秒とすると、この１０秒間に入力されたブロックに対しては同じ鍵Ｋ２を用いて暗号化するが、次の１０秒間は新たな鍵で暗号化する。すなわち、１０秒ごとに、異なる鍵Ｋ２を生成するようにする。この処理時間の値は、セキュア制御部に予め固定的に記憶しておくか、あるいは外部から設定入力してもよい。

【００５２】

（ｄ）可変的な複数個の暗号化処理時間

たとえば、コンテンツの種類などに対応させて、予め複数個の暗号化処理時間を記憶しておく。入力されたコンテンツの種類に対応して、どの暗号化処理時間を採用するかを決定し、その決定された処理時間ごとに、鍵Ｋ２を生成するようにする。あるいは、コンテンツを入力するときに、暗号化処理時間も入力し、入力された暗号化処理時間ごとに、新たに鍵Ｋ２を生成するようにしてもよい。

【００５３】

（ｅ）乱数により可変的に鍵生成のタイミングを決定する。たとえば、コンテンツの入力前に、乱数により、暗号化処理の容量サイズをランダムに決定する。決定された容量サ

イズに相当する数のブロックが入力されるごとに、新たに鍵Ｋ２を生成し、その生成鍵Ｋ２によってその容量サイズに達するまでの複数ブロックを暗号化してもよい。すなわち、鍵Ｋ２の生成タイミングを不定期としてもよい。

【００５４】

図６に、この発明で用いられるコンテンツと鍵と鍵情報の関係の説明図を示す。

上記したように、入力されたコンテンツは、所定サイズのブロックに分割されて暗号化される。この暗号化される単位である１つのブロックのコンテンツを、ＢＣｎ（ｎ＝１，２，……Ｚ）とする。

図６（ａ）は、１つのブロックを暗号化するごとに、新たな鍵Ｋ２を生成する場合を示している。すなわち、１つのブロックコンテンツＢＣに対応した鍵Ｋ２が生成され、その鍵Ｋ２を、Ｋ２－１，Ｋ２－２，……Ｋ２－Ｚとする。

さらに、生成された鍵Ｋ２に対応して、鍵情報生成部２４が鍵情報ＫＪを生成する。この鍵情報をＫＪｎ（ｎ＝１，２，……Ｚ）とする。

図６（ａ）に示すように、１つのコンテンツＣＴが、Ｚ個のブロック（ＢＣ１，ＢＣ２，……ＢＣｚ）に分割されて暗号化されるとすると、それぞれのブロックに対応した鍵Ｋ２と鍵情報ＫＪとが生成される。たとえば、ブロックコンテンツＢＣｉに対して、鍵Ｋ２－ｉ，鍵情報ＫＪｉが対応する。

【００５５】

一方、図６（ｂ）は、複数個のブロックごとに、新たな鍵Ｋ２を生成する場合を示している。

ここで、まず、２つのブロック（ＢＣ１，ＢＣ２）に対しては、同じ鍵Ｋ２－１を用いて暗号化することを示している。次の３つのブロック（ＢＣ３，ＢＣ４，ＢＣ５）に対しては、異なる鍵Ｋ２－２が新たに生成され、この鍵Ｋ２－２を用いて暗号化することを示している。

したがって、生成された鍵の数（ｒ）は、ブロック数（ｚ）よりも少ない。ただし、鍵情報ＫＪは、鍵Ｋｎごとに生成されるので、鍵の数（ｒ）と同じである。

【００５６】

ブロック化されたコンテンツＢＣおよび鍵情報ＫＪは、ＨＤＤ３へ与えられる。一実施例として、ブロックコンテンツＢＣと鍵情報ＫＪとを別々にＨＤＤ３へ与える形式の場合は、鍵情報ＫＪの中に、対応するコンテンツブロックを特定する情報（範囲情報）を含む。

たとえば、図６（ａ）の場合は、鍵情報ＫＪ１の中に、この鍵情報を適用するブロックはＢＣ１である旨の情報が含まれる。また、図６（ｂ）の場合は、鍵情報ＫＪ２の中に、この鍵情報を適用するブロックは、ＢＣ３，ＢＣ４，ＢＣ５である旨の情報が含まれる。

また、図６（ｃ）に示すような形式で、ＨＤＤ３へ与えてもよい。図６（ｃ）の形式１の場合は、記憶制御部２９が、ブロックコンテンツＢＣと、これに対応する鍵情報ＫＪとを対応づける処理をした後、両者を１つの対情報とした形式で、ＨＤＤ３へ与えることを示している。

図６（ｃ）の形式２の場合は、ブロックコンテンツＢＣと、鍵情報ＫＪと、両者の対応関係を示す範囲情報とを別々に分けて、ＨＤＤ３へ与えることを示している。

【００５７】

鍵情報ＫＪに範囲情報を含める場合は、セキュリティ確保のため、その範囲情報を、マスタ鍵Ｋｍで暗号化した後に含めてもよい。また、図６（ｃ）の形式２の場合も、セキュリティ確保のため、範囲情報の部分を、マスタ鍵Ｋｍで暗号化したものを、ＨＤＤ３へ与えてもよい。

【００５８】

次に、図７に、この発明の鍵情報の一実施例の説明図を示す。

図７において、鍵情報生成部２４によって生成される鍵情報ＫＪの内容の具体例を、いくつか示している。鍵情報ＫＪとしては、この中のいずれかを採用することができる。ただし、この具体例に限られるものではない。

鍵情報ＫＪとして、１つのコンテンツに対して図７のいずれか一つのみを採用してもよいが、複数個の形態で記憶してもよい。複数個の形態で記憶しておけば、いずれかの鍵情報からもとの鍵Ｋ２を復元できる。

また、図７には、１０種類の鍵情報ＫＪと対応して、セキュア制御部２の中の鍵情報記憶部２５に格納される情報を示している。

【００５９】

まず、１番目は、マスタ鍵で暗号化された鍵（Ｋｍ（Ｋ２））を、鍵情報としてＨＤＤ３に記憶することを示している。この場合、ＨＤＤ３が盗まれ、鍵（Ｋｍ（Ｋ２））が読み出されたとしても、マスタ鍵Ｋｍを知らなければ、生成鍵Ｋ２そのものを復元することは困難である。

また、鍵Ｋ２を復元する場合には、ＨＤＤ３からこの暗号化された鍵（Ｋｍ（Ｋ２））を読み出して、セキュア制御部に与える。鍵（Ｋｍ（Ｋ２））が与えられたセキュア制御部は、この鍵（Ｋｍ（Ｋ２））に、マスタ鍵Ｋｍを適用して生成鍵Ｋ２を復元することができる。

２番目は、マスタ鍵で暗号化された生成鍵（Km（Ｋ２））と、そのコンテンツの適用範囲情報とを、鍵情報ＫＪとしてＨＤＤ３に記憶する場合を示している。この場合も、セキュア制御部内部に、鍵Ｋ２を保存しなくてもよい。

【００６０】

３番目は、ｎ個の生成鍵Ｋ２－ｎそのものは、セキュア制御部の鍵情報記憶部２５に記憶しておき、その鍵Ｋ２－ｎを特定するインデックス番号からなる鍵インデックスｎを、ＨＤＤ３に記憶する場合を示している。

たとえば、３番目のブロックＢＣ３に対して鍵Ｋ２－３が生成された場合、鍵情報生成部２４において、その鍵Ｋ２－３を特定するインデックス番号（たとえば、３）を生成し、これを鍵インデックスｎとする。そして、生成鍵Ｋ２－３そのものは、セキュア制御部の鍵情報記憶部２５に記憶し、鍵インデックスｎ（＝３）を、ＨＤＤ３に記憶する。

これによれば、ＨＤＤ３の鍵インデックスｎが不正に読み出されたとしても、その鍵インデックスからセキュア制御部内部に記憶されている生成鍵Ｋ２を特定することはできない。

また、生成鍵Ｋ２を復元する場合、鍵インデックスｎをＨＤＤから読み出し、セキュア制御部に与える。鍵インデックスｎが与えられたセキュア制御部は、この鍵インデックスｎから対応する生成鍵Ｋ２－ｎを、鍵情報記憶部２５から読み出す。

【００６１】

４番目は、鍵インデックスｎに加えて、生成鍵の適用コンテンツを示す情報（コンテンツ範囲情報）を、ＨＤＤ３に記憶する場合を示している。この場合も、生成鍵Ｋ２そのものは、セキュア制御部に記憶される。

５番目は、１つのコンテンツを特定するＩＤ（コンテンツＩＤ）と、鍵インデックスｎとを、ＨＤＤ３に記憶する場合を示している。１つのコンテンツが、たとえば、ｎ個のブロックに分割されて暗号化された場合、鍵インデックスｎにより、何番目のブロックかを示すことができる。そのブロックを暗号化するのに利用した生成鍵Ｋ２そのものは、セキュア制御部に記憶される。

６番目は、５番目の鍵情報に対して、コンテンツ範囲情報を加えたものである。

【００６２】

７番目は、鍵初期値を、ＨＤＤ３に記憶することを示している。ここで、鍵初期値とは、ある規則に従って、鍵を生成するためのベースとなる値のことである。この場合、その後、順に生成される生成鍵Ｋ２は、ある規則に従って生成されるものとする。

たとえば、３番目に生成される生成鍵Ｋ２－３は、２番目の生成鍵Ｋ２－２に予め決められた特定値を加算したものとしてもよい。あるいは、それ以前に生成された生成鍵（Ｋ２－１，Ｋ２－２）をすべて加算したものとしてもよい。その他に、所定の鍵計算式を予め決めておき、その鍵計算式を用いて生成鍵を順次生成してもよい。

このような規則を予め決めておけば、鍵初期値を記憶しておくだけで、その後に生成さ

れた鍵Ｋ２をすべて記憶する必要はない。言いかえれば、鍵初期値のみを記憶しておくだけで、その後に生成された鍵Ｋ２をすべて再生させることができる。この場合も、生成鍵Ｋ２は、セキュア制御部に記憶してもしなくてもどちらでもよい。

【００６３】

８番目は、鍵初期値と、上記したような鍵計算式を含めて、ＨＤＤ３に記憶する場合を示している。この場合は、鍵計算式を１つに固定するのではなく、複数個の鍵計算式を用いることができる。すなわち、１つの鍵初期値に対して、異なる関係を持つ複数種類の鍵を生成することができる。

９番目は、鍵初期値と鍵計算式を対にした組の番号であるインデックスを、ＨＤＤ３に記憶する場合を示している。この場合、鍵初期値と鍵計算式とは、セキュア制御部の中に記憶される。

鍵Ｋ２を復元する場合は、このインデックスをＨＤＤ３から読み出してセキュア制御部に与えればよい。インデックスが与えられたセキュア制御部は、このインデックスから、鍵初期値と鍵計算式を特定し、さらにこれらから、各生成鍵Ｋ２を順に生成できる。

【００６４】

１０番目は、９番目の情報を組みかえたものであり、ＨＤＤ３に、鍵初期値とインデックスを記憶し、鍵計算式をセキュア制御部に記憶した場合を示している。この場合は、セキュア制御部に、ＨＤＤ３から読み出した鍵初期値とインデックスとを与えてやることにより、まず鍵情報記憶部２５から鍵計算式を読み出し、鍵初期値と鍵計算式とから生成鍵Ｋ２を復元することができる。

【００６５】

以上のように、ＨＤＤ３に記憶される鍵情報ＫＪは、種々の形態が考えられる。どの形態を採用するかは、予め固定的に決めてもよいが、セキュリティレベルの高低などの基準によって定めてもよい。

たとえば、１０段階のセキュリティレベルが設定可能な場合、レベル３のセキュリティレベルが設定された場合は、図７の３番目を採用することにしてもよい。

【００６６】

＜コンテンツの暗号化処理の具体例＞

図８に、コンテンツの録画時における暗号化処理の一実施例のフローチャートを示す。

ここでは、録画用のアプリケーションプログラムが、セキュア制御部に対して、コンテンツの暗号化を要求し、セキュア制御部が生成した鍵情報ＫＪと暗号化コンテンツとをＨＤＤ３に記憶する処理について説明する。

ユーザからの録画指示入力があると録画用アプリケーションが起動される。

録画用アプリケーションプログラムは、まず、ステップＳ１１において、セキュア制御部等のハードウェアを録画可能な状態に設定する。

次に、ステップＳ１２において、録画指示によって特定されるコンテンツの管理情報（コンテンツ名など）を、ＨＤＤ３のコンテンツリストに追加する。

【００６７】

ステップＳ１３において、セキュア制御部２に対して、録画要求のあったコンテンツの暗号化要求を送る。セキュア制御部２に与えられるこの暗号化要求には、たとえば、鍵の生成方法を含めてもよい。

暗号化要求を受けたセキュア制御部２は、図２に示す各機能ブロックによって、録画要求されたコンテンツの入力と暗号化処理を行い、暗号化に用いる鍵Ｋ２の生成と、鍵情報ＫＪの生成を行う。

ステップＳ１４において、セキュア制御部で暗号化されたコンテンツブロックと、生成された鍵情報ＫＪとを、セキュア制御部から取得する。ただし、鍵Ｋ２が新たに生成されず同じ鍵を継続して使用する場合は、暗号化されたコンテンツのみを取得し、鍵情報ＫＪは取得されない。言いかえれば、新たな鍵Ｋ２が生成された場合にのみ鍵情報ＫＪが取得される。

【００６８】

ステップＳ１５において、取得されたコンテンツブロックと鍵情報ＫＪとを、ＨＤＤ３へ格納する。
ステップＳ１６において、要求されたコンテンツ全体の録画が終了したか否か、チェックする。まだ終了していない場合は、ステップＳ１４へ戻り、再度コンテンツの暗号化とＨＤＤへの格納処理を繰り返す。
録画をすべて終了した場合は、処理を終了する。なお、鍵情報ＫＪの取得と格納は、図６に示したような形式のいずれかで行われ、図７に示したような情報からなる鍵情報ＫＪがセキュア制御部で生成されて、ＨＤＤ３に格納される。

【００６９】

図９に、録画時におけるセキュア制御部の暗号化処理のフローチャートを示す。
ステップＳ２１において、コンテンツの暗号化要求を、録画用アプリケーションプログラムから受信したか否かチェックし、受信した場合、その内容を解釈して、ステップＳ２２へ進む。
ステップＳ２２において、鍵Ｋ２を新たに生成するタイミングか否かチェックする。たとえば、前記したような５つのタイミングのいずれかに相当するタイミングか否か、チェックする。
新たに鍵Ｋ２を生成するタイミングにない場合は、ステップＳ２５へ進む。所定量のサイズに相当するブロックが入力された場合など、新たに鍵Ｋ２を生成するタイミングであると判断された場合、ステップＳ２３へ進む。

【００７０】

ステップＳ２３において、鍵生成部Ｓ２３が、暗号化のための鍵Ｋ２を新たに生成する。鍵Ｋ２の生成は、暗号アルゴリズムにより異なる可能性があるが、従来と同様に、乱数から生成する手法などを用いればよい。また、鍵初期値や鍵計算式が決められている場合、その値や式を基にして、鍵Ｋ２が生成される。
ステップＳ２４において、鍵情報生成部２４が、生成鍵Ｋ２を用いて、図７に示したような形態の鍵情報ＫＪを生成する。
ステップＳ２５において、コンテンツ暗号部２３が、生成鍵Ｋ２を用いて、ブロックごとにコンテンツを暗号化する。

【００７１】

ステップＳ２６において、記憶制御部２９が、暗号化されたブロックコンテンツＢＣと、鍵情報ＫＪとを、ＨＤＤ３へ格納する。
ただし、これらの情報（ＢＣ，ＫＪ）は、セキュア制御部が直接ＨＤＤに格納するのではなく、前記した図８のフローのように、一旦、これらの情報を録画用アプリケーションプログラムに与え、このアプリケーションプログラムが、ＨＤＤ３へ書き込むようにしてもよい。
ステップＳ２７において、暗号化要求されたコンテンツをすべて処理したか否かチェックする。暗号化処理が終了していない場合は、ステップＳ２２へ戻り、再度次のブロックコンテンツに対して、ステップＳ２２からＳ２６までの暗号化処理を繰り返す。

【００７２】

以上のように、所定のタイミングでブロックコンテンツを暗号化するための鍵Ｋ２を新たに生成しているので、複数の鍵Ｋ２のうち１つが漏洩したとしても、その鍵Ｋ２で暗号化した部分ブロックのみが復元されるだけであり、コンテンツ全体を復元（再生）することはできない。
すなわち、暗号化に使用する鍵Ｋ２を複数個生成することにより、十分なセキュリティを確保することができる。

【００７３】

＜コンテンツの復号処理の具体例＞

図１０に、コンテンツの再生（配信）時における復号処理の一実施例のフローチャートを示す。
ここでは、再生用あるいは配信用のアプリケーションプログラムが、セキュア制御部に

対して、コンテンツの復号要求を与え、セキュア制御部から復号のための鍵Ｋ２を取得し、要求されたコンテンツのブロックをＨＤＤから直接取得して、コンテンツを再生する処理について説明する。

【００７４】

まず、ステップＳ３１において、セキュア制御部などを、再生可能な状態に設定する。

ステップＳ３２において、再生するコンテンツのファイル名などの情報を、ＨＤＤのコンテンツリストから取得する。

ステップＳ３３において、コンテンツのファイル名に対応づけられてＨＤＤに記憶されていたコンテンツＢＣと、鍵情報ＫＪとを、ＨＤＤから直接読み出す。このとき、セキュア制御部は介在しない。

ステップＳ３４において、読み出した鍵情報ＫＪを、セキュア制御部に与える。すなわち、セキュア制御部に対して、鍵情報ＫＪに対応する鍵Ｋ２の復元要求をする。鍵情報ＫＪが与えられたセキュア制御部は、鍵情報ＫＪによって特定される鍵Ｋ２が復元可能か否かを判断し、可能であれば鍵Ｋ２を復元し、アプリケーションプログラムにその鍵Ｋ２を出力する。

【００７５】

ステップＳ３５において、セキュア制御部から、復元された鍵Ｋ２を取得する。

ステップＳ３６において、取得した鍵Ｋ２を用いて、ＨＤＤから読み出したコンテンツＢＣを復号し、再生する。

ステップＳ３７において、コンテンツの復号を終了した後、その鍵Ｋ２の使用が終了したことを、セキュア制御部に伝える。鍵の同時使用数により鍵復元の判断を行う場合には、使用終了により、同時使用数を減らす必要がある。これを行わないと同時使用数の限度に達し復元を許可されず、セキュア制御部は鍵K２を出力しない。

【００７６】

ステップＳ３８において、再生すべきコンテンツの再生がすべて終了したか否か、チェックする。再生を終了していない場合は、ステップＳ３３へ戻り、再度残りのコンテンツの復号処理を実行する。要求されたコンテンツの再生をすべて終了した場合は、処理を終了する。

【００７７】

図１１に、再生時におけるセキュア制御部の鍵の復元処理の一実施例のフローチャートを示す。

セキュア制御部は、アプリケーションプログラムからの復元要求あるいは更新依頼を受信して、鍵Ｋ２の復元の可否を判定した後、可能な場合に鍵Ｋ２を復元し、アプリケーションプログラムへ出力する。

ここで、更新依頼とは、アプリケーションプログラムが現在鍵Ｋ２を使用中の場合に、再度その鍵Ｋ２の継続使用を要求することや、現在使用中であることを定期的にセキュア制御部に対して通知することなどを意味する。たとえば、セキュア制御部は、鍵の使用を許可した後、一定時間（たとえば１０秒）以内に、使用を許可したアプリケーションプログラムから更新依頼を受理しなかった場合は、その後の鍵Ｋ２の復元をしないようにする。

【００７８】

また、鍵の復元が可能か否かは、鍵情報復元管理部２７が行う。

たとえば、セキュア制御部に復元要求があったとき、鍵情報復元部２６が、鍵情報復元管理部２７に復元可否の問合せを行い、鍵情報復元管理部２７が管理している復元状況情報をチェックすることにより復元可否を判断する。

【００７９】

図１２に、鍵情報復元管理部が管理保持する復元状況情報の一実施例の説明図を示す。

図１２には、２つのコンテンツの復元状況情報を示している。

コンテンツＩＤ＝２５のコンテンツに対しては、２つの鍵（１，３）が現在使用中であり、復元して２つの鍵をアプリケーションプログラムに出力したことを示している。

ここで、取得時間は、その鍵の復元要求を最初に受けた時間を示し、更新時間は、その後、アプリケーションプログラムから更新依頼を受けた時間を示す。

【００８０】

たとえば、鍵１については、１２時３４分２０秒に最初の復元依頼を受理した後、その３秒後に、復元された鍵１を現在使用中であることを示す更新依頼を受理したことを示す。鍵３についても同様である。

この２つの鍵については、どちらもアプリケーションプログラムからの更新依頼を受理しているので、その鍵（１，３）は、まだ使用可能（復元可能）である。

一方、コンテンツＩＤ＝５４３２のコンテンツに対しては、００時００分００秒に最初の復元要求を受理し、鍵５がアプリケーションプログラムに出力されたが、その後、そのアプリケーションプログラムから、更新依頼を受理していない状態であることを示している。この場合、一定時間経過しても、更新依頼を受理しない場合には、その後の使用（復元）は不可と判断する。

また、最初の復元要求後の経過時間によっては、更新依頼を受理しても復元を不可とすることも可能である。

このように、鍵情報復元管理部２７は、図１２に示すような鍵の復元状況情報を作成，確認，更新しながら、鍵の復元可否を判断する。

【００８１】

図１１のステップＳ５１において、鍵情報復元部２６が、アプリケーションプログラムから復元状況の更新依頼があるか否か、チェックする。

更新依頼がなければ、ステップＳ５２へ進み、鍵の復元可否を、鍵情報復元管理部２７へ問合わせる。更新依頼があれば、ステップＳ５６へ進み、その更新依頼を、鍵情報復元管理部２７へ通知する。

ステップＳ５２で、問合せを受けた鍵情報復元管理部２７は、ステップＳ５３において、復元状況情報を参照して復元の可否を判断する。

ただし、最初の鍵の復元依頼を受けた場合は、ステップＳ５３では、復元の可否は判断されず、ステップＳ５４でも復元可と判断される。

ステップＳ５３で復元可と判断された場合は、ステップＳ５５へ進む。

【００８２】

一方、復元不可と判断された場合は（ステップＳ５４）、その鍵の復元を行わずに処理を終了する。

ステップＳ５５において、復元が許可されたので、鍵情報復元部２６は、アプリケーションプログラムから与えられた鍵情報ＫＪを用いて、対応する鍵Ｋ２を復元し、さらに鍵Ｋ２を復元したことを鍵情報復元管理部２７へ通知する。

ステップＳ５７において、鍵情報復元管理部２７が、図１２の復元状況情報を更新または作成する。たとえば、最初の復元要求の場合は、その鍵についての復元状況情報を作成し、取得時間を記憶する。

ステップＳ５６で更新依頼の通知を受けた場合は、すでに作成されている鍵の復元状況情報の中の更新時間を変更する。

【００８３】

以上のように、復元要求を受けた鍵Ｋ２すべてについて無条件にアプリケーションプログラムに出力するのではなく、現在の復元状況をチェックし、復元可否を判断した後に、出力するようにする。これによれば、不正な鍵の復元要求があった場合に、不必要以上に鍵を出力することを防止することができ、コンテンツの不正な復元を防止できる。

【００８４】

図１２では、更新依頼を受理する時間間隔の経過で復元の可否を判断する例を示したが、これに限るものではない。

たとえば、１つのコンテンツにおいて、その再生要求があったときに同時に復元要求を受理する鍵Ｋ２の上限数を所定数（ｎ）に制限するようにしてもよい。

たとえば、１つのコンテンツが１００個のブロックコンテンツからなり、その鍵情報が

１０個存在する場合、アプリケーションプログラムから同時に受理できる鍵の復元要求は、５つまでとする。
すなわち、５つの鍵Ｋ２－１～Ｋ２－５は、同時にアプリケーションプログラムに出力されるが、この５つの鍵Ｋ２が出力（使用）されている状態では、６番目の鍵Ｋ２－６の復元要求は受理せず、６番目の鍵Ｋ２－６は復元しないようにする。

【００８５】

また、１つの鍵の復元要求を受理する時間間隔Ｔを決定し、その時間間隔Ｔ内に複数の鍵の復元要求を受理しても、１つの要求だけは受理するが、残りの要求は受理しないようにしてもよい。
この他にも、復元可否の判断には種々の方法が考えられるが、その判断方法を変更又は追加できるようにし、どの判断方法を使用するかの設定を、アプリケーションプログラムからできるようにしてもよい。
あるいは、コンテンツの種類や暗号化方式などのコンテンツの属性に対応して、どの復元可否の判断方法を使用するかを自動的に設定するようにしてもよい。

【００８６】

図１３に、鍵情報復元管理部の一実施例のフローチャートを示す。
ステップＳ７１において、復元状況情報の中の更新時間をチェックし、前回の更新から所定の時間が経過している場合は、その鍵の復元可否を不可に変更する。
ステップＳ７２において、鍵情報復元部２６から、何らかのアクセスがあるか否か、チェックする。ここで、アクセスとは、復元可否の問合せ，更新依頼などである。アクセスがなければ、ステップＳ７１へ戻り、復元状況情報のチェックを続ける。
ステップＳ７３において、アクセスが復元可否の問合せの場合、ステップＳ７４へ進む。ステップＳ７５においてアクセスが更新依頼の場合、ステップＳ７６へ進む。その他のアクセスの場合はステップＳ７１へ戻る。

【００８７】

ステップＳ７４において、復元状況情報を参照し、問合せに対する返答を、鍵情報復元部２６へ送る。すなわち問合せのあった鍵Ｋ２についての復元可否の判断結果を、鍵情報復元部２６へ返す。
ただし、１回目の鍵復元要求の際に行われる問合せに対しては、復元状況情報はまだ作成されていないので、復元可という返答を返す。
この後、ステップＳ７１へ戻る。

【００８８】

ステップＳ７６において、更新依頼のあった鍵に対する更新時間を現在の時刻に変更する。あるいは、最初の更新要求の場合は、新たに更新時間を追加する。
また、更新依頼に、鍵の使用終了という意味の情報が含まれている場合は、その鍵の使用を開放するために、その鍵に対する復元状況情報を削除する。これにより、アプリケーションプログラムによるその鍵の使用が終了したことになるので、この後、他のアプリケーションプログラムによって、同じ鍵の復元要求は受理できるようになる。

【００８９】

ステップＳ７７において、復元可否の判断基準として鍵の使用個数の上限が設定されている場合、現在の使用個数をチェックし、この設定値を越える数の鍵が使用されることになっている場合は、その鍵の使用（復元可否）を不可に設定する。
逆に使用個数のチェックの結果、上限値を下回る数の鍵しか使用されていない状況になっている場合は、不可とされていた鍵の使用（復元可否）を、可に設定変更する。
なお、１つのコンテンツについて、以前いくつかの鍵が使用中であったが、現在使用されている鍵が１つもなくなった場合には、そのコンテンツの再生が終了したと考えて、そのコンテンツの復元状況情報をすべて削除してもよい。
また、図１２のような復元状況情報の作成は、復元要求や更新依頼のあるごとに行ってもよいが、最初の復元要求があったときに、そのコンテンツに対するすべての鍵に対する情報を先に作成しておいてもよい。

【００９０】
図１４に、鍵情報復元時におけるタイムチャートの一実施例を示す。
ここでは、鍵情報の復元要求や更新依頼がアプリケーションから連続的に出され、鍵の復元が許可される場合と、そうでない場合の一つの実施例を示している。
まず、Ｓ１０１において、アプリケーションプログラムから、セキュア制御部に対して、あるコンテンツについての鍵情報および鍵の復元要求があったとする。
Ｓ２０１において、セキュア制御部は、受理した鍵情報から、対応する鍵を復元してよいか判断し、鍵情報復元管理部２７で管理している復元状況情報を作成する。ここで、最初の復元要求であったとすると、復元要求されたコンテンツと鍵についての復元状況情報（図１２のＣ１～Ｃ５）が作成される。
【００９１】
そして、最初の復元要求の場合は、受信した鍵情報ＫＪをもとに、鍵Ｋ２－１を復元し、鍵Ｋ２－１をアプリケーションプログラムへ出力する。鍵Ｋ２－１を受理したアプリケーションプログラムは、その鍵Ｋ２－１を用いて、対応するブロックコンテンツを復号する。
次に、Ｓ１０２において、次のブロックコンテンツを異なる鍵で復号するために、鍵情報をセキュア制御部へ与える。
Ｓ２０２において、セキュア制御部は、この鍵情報に対応する鍵Ｋ２－２の復元が可能か否かチェックし、復元状況情報に復元しようとする鍵Ｋ２－２の情報がなければ追加作成する。このとき、復元可否は可とする。
そして、復元可であるとすると、鍵Ｋ２－２を復元し、アプリケーションプログラムに出力する。ここで、１つのコンテンツに対して使用中の鍵は２つとなる。
この新たな鍵Ｋ２－２を受理したアプリケーションは、対応するブロックコンテンツを復元する。
【００９２】
次に、Ｓ１０３において、この鍵Ｋ２－１を継続して使用するために、鍵Ｋ２－１の更新依頼を、セキュア制御部へ送る。この更新要求を受理したセキュア制御部は、更新依頼が正当な時間内に受理したものと判断すれば、その鍵Ｋ２－１についての更新時間を更新する（Ｓ２０３）。
次に、Ｓ１０４において、アプリケーションプログラムから、新たな鍵Ｋ２－３を取得するため、次の鍵情報をセキュア制御部へ送信したとする。セキュア制御部では、この鍵情報に対する鍵Ｋ２－３の復元を許可してもよいか判断し、してよい場合は、復元状況情報に、鍵Ｋ２－３の情報を新たに追加作成し、復元した鍵Ｋ２－３を、アプリケーションプログラムへ送る（Ｓ２０４）。
また、このコンテンツについての同時使用を許可する鍵の数の上限が３であったとすると、復元状況情報の中の「復元可否」を「不可」に設定変更する。
【００９３】
次に、Ｓ１０５において、アプリケーションプログラムから、次の鍵Ｋ２－４を取得するために、鍵情報をセキュア制御部へ送ったとする。このとき、Ｓ２０５において、セキュア制御部が復元可否のチェックをすると、復元管理情報の「復元可否」が「不可」となっているので、鍵Ｋ２－４の復元は許可されない。このとき、鍵Ｋ２－４の復元が不可である旨を、アプリケーションプログラムに返信してもよい。
【００９４】
鍵Ｋ２－４の取得に失敗したことを通知されたアプリケーションプログラムは、新たな鍵Ｋ２－４を取得できるようにするために、鍵Ｋ２－１の使用を終了する旨の更新依頼をセキュア制御部へ送ったとする（Ｓ１０６）。
この鍵Ｋ２－１の使用終了を受理したセキュア制御部は、鍵Ｋ２－１に対応した復元状況情報の部分を削除し、現在使用中の鍵の数が３から２になったことから、「復元可否」を可に設定変更する（Ｓ２０６）。
この直後に、次の鍵Ｋ２－４の取得のための更新要求があれば、鍵Ｋ２－４を復元して

、アプリケーションプログラムへ出力する。

【００９５】

しかし、図１４に示すようにＳ２０６の後、所定の設定時間が経過しても、アプリケーションプログラムから更新依頼がなかったとすると、セキュア制御部の鍵情報復元管理部２７は、「復元可否」を不可に設定変更する。

次に、この設定時間経過後に、アプリケーションプログラムから次の鍵Ｋ２－４の取得要求のための鍵情報を、送ったとする（Ｓ１０７）。このとき、「復元可否」は、不可となっているので、鍵Ｋ２－４は復元されず、失敗となる（Ｓ２０７）。

以上が連続した鍵Ｋ２の復元要求があった場合のタイムチャートの実施例であるが、このように、鍵の復元の可否を判断しつつ鍵の復元を行うので、再生時におけるコンテンツの不正利用を、より効果的に防止することができ、安全なセキュリティ状態を維持したまま複数のコンテンツの同時使用も可能となる。

また、鍵の使用状況を管理して鍵の復元の可否を判断するので、不正な鍵の取得を防止することができる。

【００９６】

なお、図１１および図１３に、鍵の復元可否の判断の一実施例を示したが、これに限るものではない。

たとえば、セキュア制御部と、アプリケーションプログラムとの間でのみ利用する共有メモリを設け、この共有メモリに対して互いに特定のデータの書込みと読出しを、定期的に行うことにより、鍵の更新チェックと復元の可否の判断を行ってもよい。

たとえば、セキュア制御部が、共有メモリに更新依頼を意味する特定のデータＡを書込んだ後、一定時間内に、アプリケーションプログラムが特定のデータＡを確認して共有メモリに特定のデータＢを書き込むか否かをチェックする。セキュア制御部が特定のデータＢが書込まれたことを確認したことをもって正当なアプリケーションプログラムが鍵の更新を要求したと判断する。

共有メモリに書込まれる特定のデータ（Ａ，Ｂ）を、正当なアプリケーションプログラムの設計時に予め決めておくことにより、不正なアプリケーションの介在による鍵Ｋ２の不正流出を防止することができる。

【００９７】

次に、前記各実施形態に関し、次の付記を示す。

（付記１）

コンテンツを複数のブロックに分割して入力する入力部と、

１つのブロックまたは複数のブロックを暗号化するための鍵を順次生成する鍵生成部と、

前記生成鍵を用いて前記１つのブロックまたは複数のブロックを暗号化するコンテンツ暗号部と、

前記暗号化に用いた生成鍵を復元するための鍵情報をその生成鍵から生成する鍵情報生成部と、

前記コンテンツ暗号部によって暗号化された各ブロックのコンテンツと、前記鍵情報生成部で生成された鍵情報とを外部記憶装置へ出力する記憶制御部とを備え、

前記鍵生成部が順次生成する鍵は、所定の条件を満たしたときに新たに生成され、１つのブロックまたは複数のブロックごとに異なることを特徴とする鍵管理機能を持つセキュア素子。

（付記２）

前記外部記憶装置に記憶されていた鍵情報を受信する復元制御部と、

受信した鍵情報から前記暗号化に用いた生成鍵を復元する鍵情報復元部と、

前記外部記憶装置に記憶された各ブロックのコンテンツを復号する情報処理機構に、前記復元された生成鍵を出力する出力部とをさらに備えたことを特徴とする付記１のセキュア素子。

（付記３）

前記鍵情報復元部によって復元された生成鍵の復元状況を管理し、すでに復元された生成鍵の復元状況に基づいて、すでに復元された生成鍵の更新の可否および新たに復元すべき生成鍵の復元の可否を判断する鍵情報復元管理部をさらに備え、

復元を許可しないと判断した場合には、前記鍵情報復元部はその許可されなかった生成鍵を復元しないことを特徴とする付記２のセキュア素子。

（付記４）

前記鍵情報には、セキュア素子固有のマスタ鍵によって暗号化された生成鍵を含むことを特徴とする付記１のセキュア素子。

（付記５）

前記鍵情報には、前記生成鍵と、暗号化のためにその生成鍵を適用したコンテンツのブロックを特定する範囲情報とが含まれることを特徴とする付記１のセキュア素子。

（付記６）

前記鍵生成部が生成した生成鍵を記憶する鍵情報記憶部をさらに備え、前記鍵情報には、鍵情報記憶部に記憶された生成鍵を特定する鍵インデックスを含むことを特徴とする付記１のセキュア素子。

（付記７）

前記鍵情報に、前記鍵インデックスによって特定される生成鍵を適用したコンテンツのブロックを特定する範囲情報をさらに含むことを特徴とする付記６のセキュア素子。

（付記８）

前記鍵生成部は、鍵初期値を生成しその鍵初期値から所定の規則に基づいてその後の鍵を生成し、前記鍵情報には、鍵初期値を含むことを特徴とする付記１のセキュア素子。

（付記９）

コンテンツを暗号化するための生成鍵の生成および復元と、コンテンツを前記生成鍵を用いて暗号化する機能を有するセキュア制御部と、

前記暗号化されたコンテンツと、前記コンテンツの暗号化に用いた生成鍵を復元することが可能なデータからなる鍵情報とを記憶したコンテンツ記憶部と、

コンテンツ記憶部に記憶されたコンテンツを再生する情報処理部とを備えた鍵管理機能を持つ情報処理装置であって、

前記セキュア制御部が、コンテンツを複数のブロックに分割して入力する入力部と、

所定の条件を満たしたときに、１つのブロックまたは複数のブロックを暗号化するための生成鍵を順次生成する鍵生成部と、前記生成鍵を用いて前記１つのブロックまたは複数のブロックを暗号化するコンテンツ暗号部と、前記暗号化に用いた生成鍵を復元するための鍵情報を、その生成鍵から生成する鍵情報生成部と、前記コンテンツ暗号部によって暗号化された各ブロックのコンテンツと、前記鍵情報生成部で生成された鍵情報とを、前記コンテンツ記憶部へ出力する記憶制御部と、前記情報処理部から、前記暗号化に用いた生成鍵を復元するための鍵情報を受信する復元制御部と、受信した鍵情報から前記暗号化に用いた生成鍵を復元する鍵情報復元部と、前記復元した生成鍵を前記情報処理部へ出力する出力部とを備え、

前記情報処理部が、前記コンテンツ記憶部から、再生すべきブロックのコンテンツおよび鍵情報を取得する情報取得部と、取得された鍵情報を前記セキュア制御部に与えることにより、その鍵情報に対応する生成鍵をセキュア制御部から取得する鍵取得部と、前記セキュア制御部から取得した生成鍵を用いて、前記コンテンツ記憶部から取得したブロックのコンテンツを順次復元してコンテンツを再生するコンテンツ復元部とを備えたことを特徴とする鍵管理機能を持つ情報処理装置。

（付記１０）

付記９に記載の情報処理装置の鍵管理機能を、コンピュータに実現させるためのプログラム。

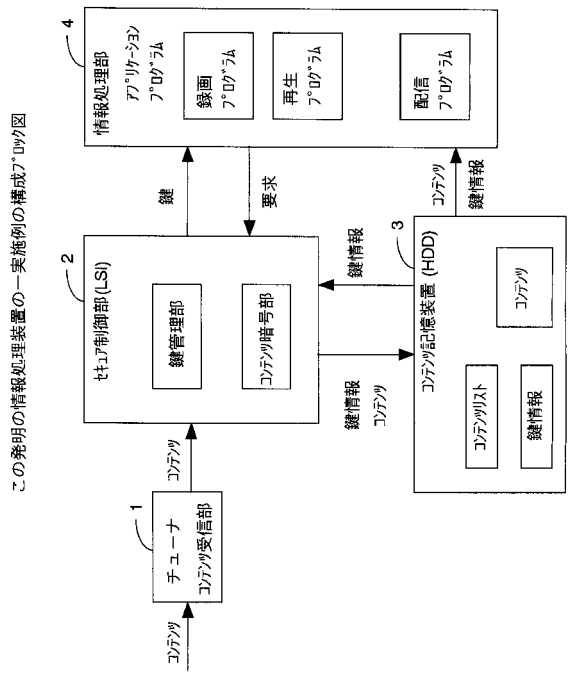
【図面の簡単な説明】

【００９８】

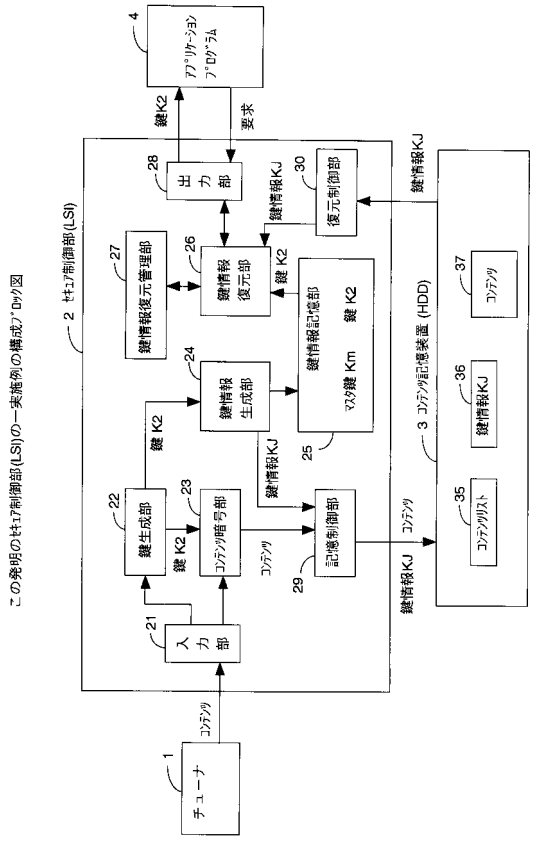
【図１】この発明の情報処理装置の一実施例の構成ブロック図である。

【図２】この発明のセキュア制御部（ＬＳＩ）の一実施例の構成ブロック図である。
【図３】この発明のコンテンツと鍵の暗号化等の一実施例の説明図である。
【図４】従来のコンテンツと鍵の暗号化等の一実施例の説明図である。
【図５】この発明のコンテンツ記憶装置の一実施例の説明図である。
【図６】この発明のコンテンツ及び鍵情報の関係の一実施例の説明図である。
【図７】この発明の鍵情報の一実施例の説明図である。
【図８】この発明のアプリケーションプログラムの暗号化処理のフローチャートである。
【図９】この発明のセキュア制御部の暗号化処理のフローチャートである。
【図１０】この発明のアプリケーションプログラムの復号処理のフローチャートである。
【図１１】この発明のセキュア制御部の復号処理のフローチャートである。
【図１２】この発明の鍵情報復元管理部が管理する復元状況情報の一実施例の説明図である。
【図１３】この発明の鍵情報復元管理部の復元可否の判断処理のフローチャートである。
【図１４】この発明の鍵情報復元処理のタイムチャートの一実施例である。
【符号の説明】
【００９９】
１　コンテンツ受信部（チューナ）
２　セキュア制御部（ＬＳＩ）
３　コンテンツ記憶装置（ＨＤＤ）
４　情報処理部（アプリケーションプログラム）
２１　入力部
２２　鍵生成部
２３　コンテンツ暗号部
２４　鍵情報生成部
２５　鍵情報記憶部
２６　鍵情報復元部
２７　鍵情報復元管理部
２８　出力部
２９　記憶制御部
３０　復元制御部
３５　コンテンツリスト
３６　鍵情報ＫＪ
３７　コンテンツ

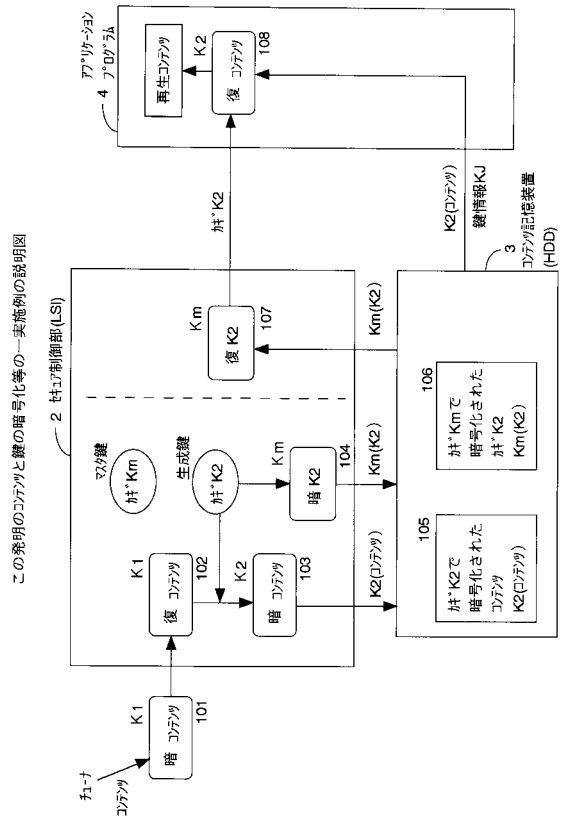
【図１】


この発明の情報処理装置の一実施例の構成ﾌﾞﾛｯｸ図
4
情報処理部
ｱﾌﾟﾘｹｰｼｮﾝ ﾌﾟﾛｸﾞﾗﾑ
録画 ﾌﾟﾛｸﾞﾗﾑ
再生 ﾌﾟﾛｸﾞﾗﾑ
配信 ﾌﾟﾛｸﾞﾗﾑ
鍵
要求
2
ｾｷｭｱ制御部(LSI)
鍵管理部
ｺﾝﾃﾝﾂ暗号部
鍵情報
ｺﾝﾃﾝﾂ
3
ｺﾝﾃﾝﾂ記憶装置 (HDD)
ｺﾝﾃﾝﾂ
ｺﾝﾃﾝﾂﾘｽﾄ
鍵情報
1
ﾁｭｰﾅ
ｺﾝﾃﾝﾂ受信部
ｺﾝﾃﾝﾂ
ｺﾝﾃﾝﾂ

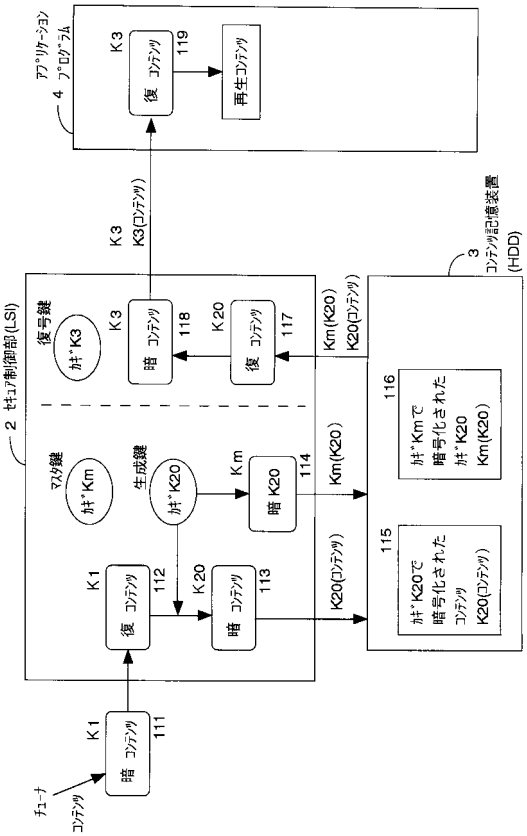
【図２】


この発明のｾｷｭｱ制御部(LSI)の一実施例の構成ﾌﾞﾛｯｸ図
4
ｱﾌﾟﾘｹｰｼｮﾝ ﾌﾟﾛｸﾞﾗﾑ
鍵K2
要求
2
ｾｷｭｱ制御部(LSI)
28
出力部
鍵情報KJ
30
復元制御部
27
鍵情報復元管理部
26
鍵情報復元部
鍵K2
24
鍵情報生成部
鍵情報記憶部
ﾏｽﾀ鍵 Km 鍵 K2
25
鍵情報KJ
22
鍵生成部
鍵 K2
23
ｺﾝﾃﾝﾂ暗号部
鍵 K2
ｺﾝﾃﾝﾂ
29
記憶制御部
ｺﾝﾃﾝﾂ
鍵情報KJ
21
入力部
ｺﾝﾃﾝﾂ
3
ｺﾝﾃﾝﾂ記憶装置 (HDD)
35
ｺﾝﾃﾝﾂﾘｽﾄ
36
鍵情報KJ
37
ｺﾝﾃﾝﾂ
1
ﾁｭｰﾅ

【図３】

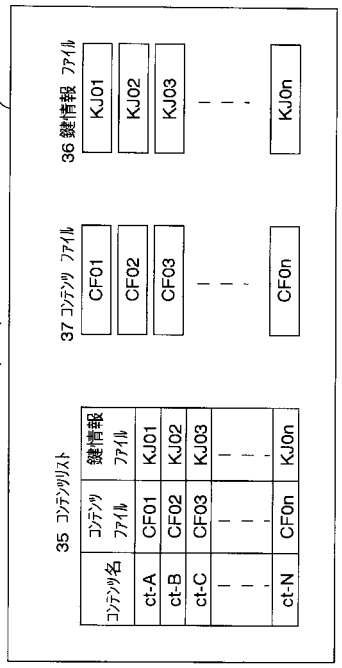

この発明のｺﾝﾃﾝﾂと鍵の暗号化等の一実施例の説明図
ｱﾌﾟﾘｹｰｼｮﾝ
4 ﾌﾟﾛｸﾞﾗﾑ
再生ｺﾝﾃﾝﾂ
K2
復 ｺﾝﾃﾝﾂ
108
ｶﾞK2
2 ｾｷｭｱ制御部(LSI)
Km
復 K2
107
Km(K2)
K2(ｺﾝﾃﾝﾂ)
鍵情報KJ
3
ｺﾝﾃﾝﾂ記憶装置
(HDD)
ﾏｽﾀ鍵
ｶﾞKm
生成鍵
ｶﾞK2
Km
暗 K2
104
Km(K2)
106
ｶﾞKmで
暗号化された
ｶﾞK2
Km(K2)
K1
復 ｺﾝﾃﾝﾂ
102
K2
暗 ｺﾝﾃﾝﾂ
103
K2(ｺﾝﾃﾝﾂ)
105
ｶﾞK2で
暗号化された
ｺﾝﾃﾝﾂ
K2(ｺﾝﾃﾝﾂ)
K1
暗 ｺﾝﾃﾝﾂ
101
ﾁｭｰﾅ
ｺﾝﾃﾝﾂ

【図４】


従来のｺﾝﾃﾝﾂと鍵の暗号化等の一実施例の説明図
ｱﾌﾟﾘｹｰｼｮﾝ
4 ﾌﾟﾛｸﾞﾗﾑ
K3
復 ｺﾝﾃﾝﾂ
119
再生ｺﾝﾃﾝﾂ
K3
K3(ｺﾝﾃﾝﾂ)
2 ｾｷｭｱ制御部(LSI)
復号鍵
ｶﾞK3
暗 ｺﾝﾃﾝﾂ
118
K20
復 ｺﾝﾃﾝﾂ
117
Km(K20)
K20(ｺﾝﾃﾝﾂ)
3
ｺﾝﾃﾝﾂ記憶装置
(HDD)
ﾏｽﾀ鍵
ｶﾞKm
生成鍵
ｶﾞK20
Km
暗 K20
114
Km(K20)
116
ｶﾞKmで
暗号化された
ｶﾞK20
Km(K20)
K1
復 ｺﾝﾃﾝﾂ
112
K20
暗 ｺﾝﾃﾝﾂ
113
K20(ｺﾝﾃﾝﾂ)
115
ｶﾞK20で
暗号化された
ｺﾝﾃﾝﾂ
K20(ｺﾝﾃﾝﾂ)
K1
暗 ｺﾝﾃﾝﾂ
111
ﾁｭｰﾅ
ｺﾝﾃﾝﾂ

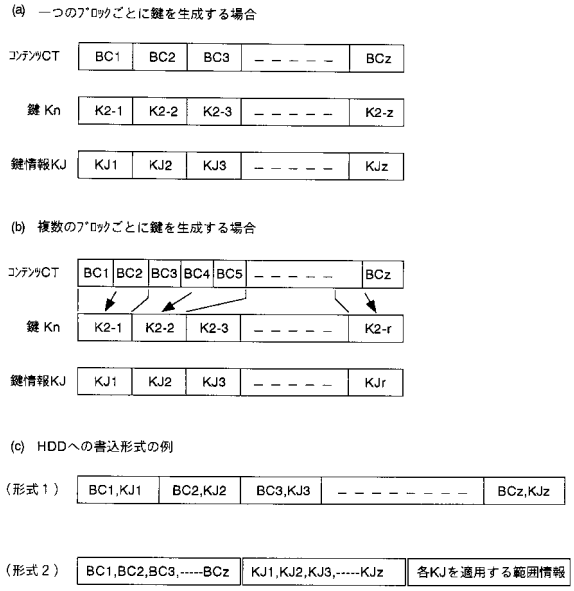
【図５】

この発明のｺﾝﾃﾝﾂ記憶装置（HDD)の一実施例の説明図



【図６】

この発明のｺﾝﾃﾝﾂ及び鍵情報の関係の一実施例の説明図

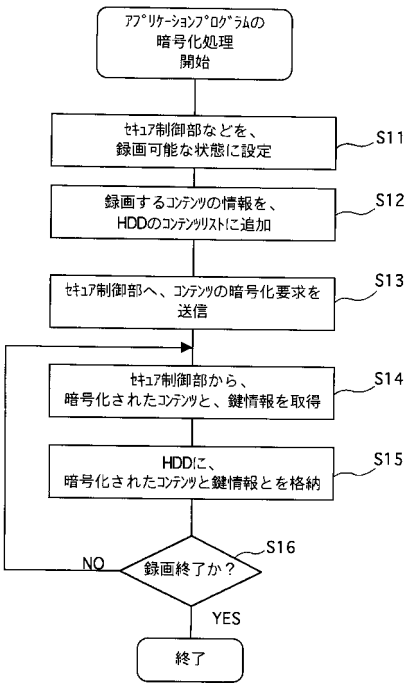


【図７】

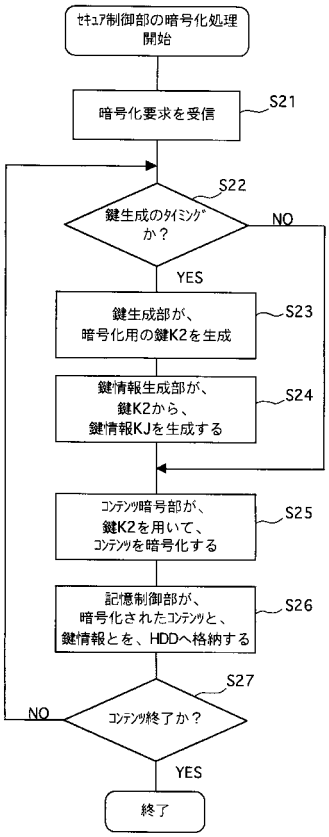
この発明の鍵情報の一実施例の説明図

	HDDに記憶される 鍵情報KJ	ｾｷｭｱ制御部の 鍵情報記憶部
1	暗号化された鍵 Km(K2)	——
2	暗号化された鍵 Km(K2) ｺﾝﾃﾝﾂ範囲情報	——
3	鍵ｲﾝﾃﾞｯｸｽn	生成鍵 K2-n
4	鍵ｲﾝﾃﾞｯｸｽn ｺﾝﾃﾝﾂ範囲情報	生成鍵 K2-n
5	ｺﾝﾃﾝﾂID 鍵ｲﾝﾃﾞｯｸｽn	生成鍵 K2-n
6	ｺﾝﾃﾝﾂID 鍵ｲﾝﾃﾞｯｸｽn ｺﾝﾃﾝﾂ範囲情報	生成鍵 K2-n
7	鍵初期値	——
8	鍵初期値 鍵計算式	——
9	ｲﾝﾃﾞｯｸｽ	鍵初期値 鍵計算式
10	鍵初期値 ｲﾝﾃﾞｯｸｽ	鍵計算式

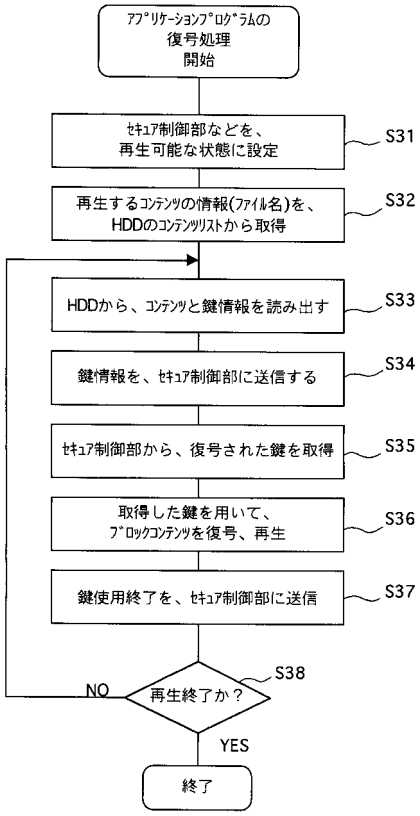
【図８】



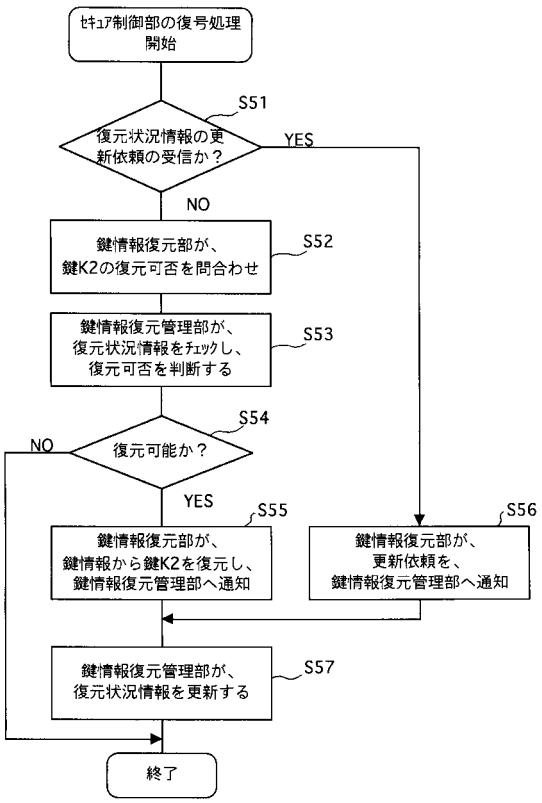
【図９】



【図１０】



【図１１】

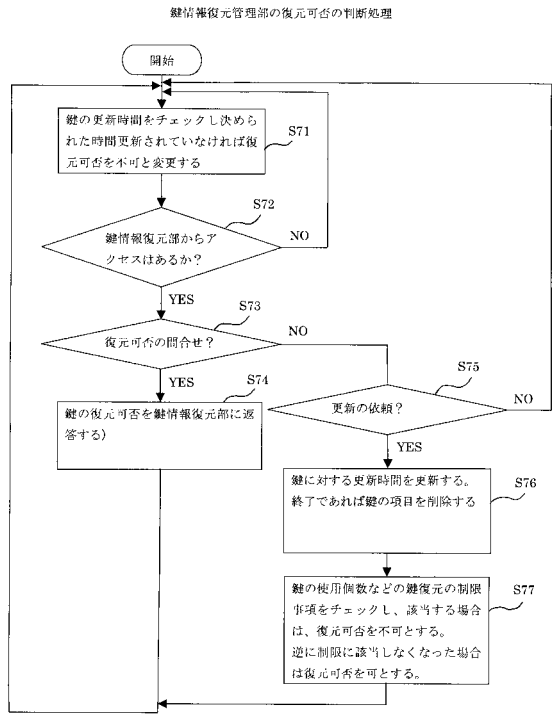


【図１２】

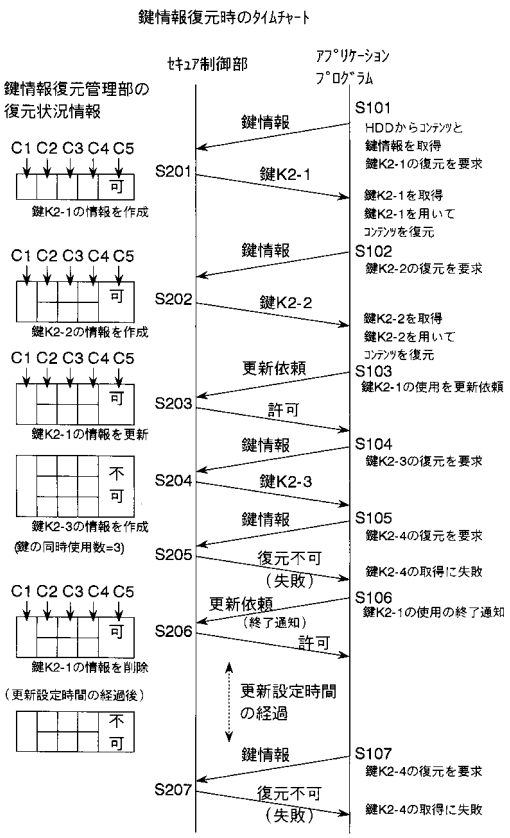
この発明の復元状況情報の一実施例の説明図

C1	C2	C3	C4	C5
ｺﾝﾃﾝﾂID	鍵ID	取得時間	更新時間	復元可否
25	1	2006/06/01,12:34:20	2006/06/01,12:34:23	復元 可
	3	2006/06/01,12:34:21	2006/06/01,12:34:24	
5432	5	2006/06/01,00:00:00	2006/06/01,00:00:00	復元 不可

【図１３】


鍵情報復元管理部の復元可否の判断処理
開始
鍵の更新時間をチェックし決められた時間更新されていなければ復元可否を不可と変更する
S71
S72
鍵情報復元部からアクセスはあるか？
NO
YES
S73
復元可否の問合せ？
NO
YES
S74
鍵の復元可否を鍵情報復元部に返答する)
S75
更新の依頼？
NO
YES
鍵に対する更新時間を更新する。終了であれば鍵の項目を削除する
S76
鍵の使用個数などの鍵復元の制限事項をチェックし、該当する場合は、復元可否を不可とする。逆に制限に該当しなくなった場合は復元可否を可とする。
S77

【図１４】


鍵情報復元時のタイムチャート
セキュア制御部
アプリケーション プログラム
鍵情報復元管理部の復元状況情報
C1 C2 C3 C4 C5
可
鍵K2-1の情報を作成
S201
鍵情報
鍵K2-1
S101
HDDからコンテンツと鍵情報を取得
鍵K2-1の復元を要求
鍵K2-1を取得
鍵K2-1を用いてコンテンツを復元
鍵K2-2の情報を作成
S202
鍵K2-2
S102
鍵K2-2の復元を要求
鍵K2-2を取得
鍵K2-2を用いてコンテンツを復元
鍵K2-1の情報を更新
S203
更新依頼
許可
S103
鍵K2-1の使用を更新依頼
不可
鍵K2-3の情報を作成
(鍵の同時使用数=3)
S204
鍵K2-3
S104
鍵K2-3の復元を要求
S205
復元不可（失敗）
S105
鍵K2-4の復元を要求
鍵K2-4の取得に失敗
鍵K2-1の情報を削除
S206
更新依頼（終了通知）
許可
S106
鍵K2-1の使用の終了通知
（更新設定時間の経過後）
更新設定時間の経過
S207
鍵情報
復元不可（失敗）
S107
鍵K2-4の復元を要求
鍵K2-4の取得に失敗

フロントページの続き

(56)参考文献 国際公開第２００６／０８０５１０（WO，Ａ１）
特開２００４－３４２２４６（ＪＰ，Ａ）
特開２００４－０９６６６６（ＪＰ，Ａ）
国際公開第０１／０３００１９（WO，Ａ１）
特開２００２－２０４２２８（ＪＰ，Ａ）
特開２００２－３５３９５７（ＪＰ，Ａ）
特開２００３－１９８５２７（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／１４