(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2010-146635
(P2010-146635A)
(43)公開日　平成22年7月1日(2010.7.1)

(51)Int.Cl.		F I			テーマコード（参考）
G11B 20/10	(2006.01)	G11B	20/10	H	5C053
G11B 20/12	(2006.01)	G11B	20/10	301Z	5D044
H04N 5/91	(2006.01)	G11B	20/12		5J104
H04L 9/32	(2006.01)	H04N	5/91	Z	
H04L 9/08	(2006.01)	H04N	5/91	P	

審査請求 未請求　請求項の数 10　ＯＬ　（全 31 頁）　最終頁に続く

(21)出願番号　特願2008-322482 (P2008-322482)
(22)出願日　平成20年12月18日 (2008.12.18)

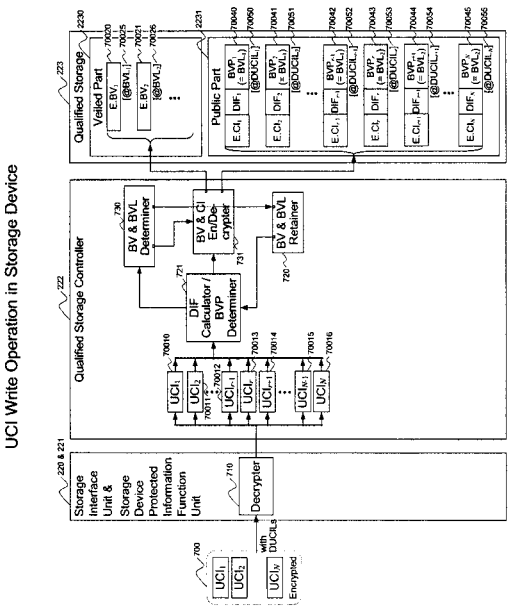
(71)出願人　503116280
ヒタチグローバルストレージテクノロジーズネザーランドビーブイ
オランダ国　アムステルダム　１０７６　エイズィ　パルナスストーレン　ロカテリケード　１
(74)代理人　110000154
特許業務法人はるか国際特許事務所
(72)発明者　平井　達哉
東京都国分寺市東恋ヶ窪一丁目２８０番地　株式会社日立製作所　中央研究所内

Ｆターム(参考)　5C053 FA23 GB06 JA21 LA06 LA14
5D044 AB05 AB07 BC01 CC04 DE03 DE50 GK17

最終頁に続く

(54)【発明の名称】コンテンツ記録再生装置並びにコンテンツの書き込み及び読み出し方法

(57)【要約】
【課題】コンテンツデータと対応付けられる情報を暗号化して媒体上に書き込む、及び暗号化して書き込まれた情報を読み出す処理の負荷を低減する。
【解決手段】本発明のデータ転送システムにおいて、記憶装置120がコンテンツデータと対応付けられる複数の利用制御情報と書き込み先位置情報を受信すると、記憶装置セキュリティ管理部225内の制限アクセス領域制御部222は、利用制御情報の中で値が同一の部分、一つの基準値と基準値からの差分との演算によって得られる部分、利用制御情報毎に完全に異なる部分を掌握する。そして、同一の部分及び基準値を制限アクセス領域223内の秘匿部2230に書き込む一方で、利用制御情報毎に完全に異なる部分や差分を、同一の部分及び基準値を書き込んだ領域を指し示す情報と共に、公開部2231に書き込む。
【選択図】図７



【特許請求の範囲】
【請求項１】
第１の記憶領域を有する記憶媒体と、第２の記憶領域を有する記憶媒体と、制御部と、を備え、
前記制御部は、
コンテンツデータと対応付けられる複数の情報群の何れか同士において一部の情報が所定の関係を有するときに、この所定の関係を有する一部の情報群を暗号化して前記第１の記憶領域に書き込み、
前記所定の関係を有する情報を省略した個別情報群を生成し、暗号化すると共に、前記第１の記憶領域への記録先位置の情報を伴って、前記第２の記憶領域に書き込み、
前記個別情報群と、前記第１の記憶領域への記録先位置の情報を伴って書き込まれた情報群とを読み出し復号化すると共に、前記第１の記憶領域への記録先位置の情報から前記第１の記録先位置上に記録されている情報群を読み出して復号化し、
前記第２の記憶領域から読み出した情報群と、前記第１の記憶領域から読み出した情報群から、前記所定の関係に基づいて前記コンテンツデータと対応付けられる情報群を復元し、この復元した情報郡を外部装置に送信する、
コンテンツ記録再生装置。
【請求項２】
前記複数の情報群のうちの１つの情報に含まれる１つの項目のデータの値が、前記情報群のうちの何れの１つの項目の値とも一致しない場合、この項目の値を前記第１の記憶媒体に暗号化して書き込むと共に、前記項目の値を一時的に自身が保持する、
請求項１に記載のコンテンツ記録再生装置。
【請求項３】
前記所定の関係を有する情報とは、所定の規則で変化する変数を表し、
前記制御部は、前記所定の規則で変化する変数の差分を第２の記憶媒体上の領域に書き込み、
前記省略された情報を、前記外部装置が指定した位置情報で特定される前記第２の記憶媒体上の領域から読み出した前記第１の記憶媒体上の位置を特定する情報に基づいて、前記第１の記憶媒体から情報を読み出し、
前記情報群を、前記第１の記憶媒体から読み出した情報と、前記第２の記憶媒体上の領域から読み出した情報と、前記差分とから、所定の規則に基づいて復元する、
請求項１に記載のコンテンツ記録再生装置。
【請求項４】
前記第１の記憶領域を有する記憶媒体と前記第２の記憶領域を有する記憶媒体とは同一の記憶媒体である、
請求項１に記載のコンテンツ記録再生装置。
【請求項５】
前記第１の記憶領域を有する記憶媒体と前記第２の記憶領域を有する記憶媒体とは、それぞれが異なる特性を持つ独立した記憶媒体である、
請求項１に記載のコンテンツ記録再生装置。
【請求項６】
コンテンツデータを記憶する第１の記憶媒体と、前記コンテンツデータと対応付けられる情報群を記憶する第２の記憶媒体と、これら記憶媒体を制御する制御部と、を備え、
前記制御部は、
第１の情報群と一部の情報が所定の関係を有する第二の情報群を記録する際には、
前記所定の関係を有する情報を省略して生成した個別情報群を、前記第１の情報群中の所定の情報の記録先位置の情報を伴って、前記第２の記憶媒体上の領域に書き込み、
前記第２の情報群を再生する際には、
前記個別情報群と、前記記録先位置の情報を伴って書き込まれた情報群とを読み出し復号化すると共に、前記記録先位置の情報から前記所定の関係を有する前記第１の情報群の

情報を読み出し、この第一の情報群の情報と前記個別情報群とから前記コンテンツデータと対応付けられる情報群を復元し、この復元した情報郡を外部装置に応答する、
コンテンツ記録再生装置。
【請求項７】
前記所定の関係を有する情報とは、所定の規則で変化する変数を表し、
前記制御部は、前記所定の規則で変化する変数の差分を前記個別情報群と共に書き込み、
前記第２の情報群を再生する際には、前記記録先位置の情報に基づいて前記第１の情報群中の所定の関係を有する情報を読み出し、
この読み出した情報と前記差分とから前記省略された情報を復元し、
この復元した省略された情報と、読み出した個別情報群とから、前記第２の情報群を所定の規則に基づいて復元する、
請求項６に記載のコンテンツ記録再生装置。
【請求項８】
前記第１の記憶媒体と前記第２の記憶媒体とは同一の記憶媒体である、
請求項６に記載のコンテンツ記録再生装置。
【請求項９】
コンテンツデータと対応付けられる複数の情報群の何れか同士において一部の情報が所定の関係を有するときに、この所定の関係を有する一部の情報群を暗号化して第１の記憶領域に書き込み、
前記所定の関係を有する情報を省略した個別情報群を生成し、暗号化すると共に、前記第１の記憶領域への記録先位置の情報を伴って、第２の記憶領域に書き込み、
前記個別情報群と、前記第１の記憶領域への記録先位置の情報を伴って書き込まれた情報群とを読み出し復号化すると共に、前記第１の記憶領域への記録先位置の情報から前記第１の記録先位置上に記録されている情報群を読み出して復号化し、
前記第２の記憶領域から読み出した情報群と、前記第１の記憶領域から読み出した情報群から、前記所定の関係に基づいて前記コンテンツデータと対応付けられる情報群を復元してコンテンツを読み出す、
コンテンツの書き込み及び読み出し方法。
【請求項１０】
前記複数の情報群のうちの１つの情報に含まれる１つの項目のデータの値が、前記情報群のうちの何れの１つの項目の値とも一致しない場合、この項目の値を前記第１の記憶媒体に暗号化して書き込むと共に、前記項目の値を一時的に自身が保持する、
請求項９に記載のコンテンツの書き込み及び読み出し方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、コンテンツデータ及びその制御情報を記憶するコンテンツ記録再生装置に関し、コンテンツデータと対応付けられる情報の書き込み及び読み出し処理の効率化に関する。
【背景技術】
【０００２】
動画データや音楽データ等のコンテンツデータを記憶媒体や記憶装置に記録する場合、著作権保護的観点から、コンテンツデータ自体は暗号化する一方で、コンテンツデータのコピー可能回数や視聴可能期間といった利用制御を行うための情報を、コンテンツ暗号化のための鍵データと共に記憶するといった手段が、多くの場合取られる。この場合、鍵データが勝手に読み出されたり、利用制御情報が改竄されたりすることのないように、適切な手段を設ける必要がある。特に、このような情報を光媒体に記録する場合に、暗号化して記録する手段が、下記非特許文献１に記載されている。
【０００３】

また、複数のレコードからなるデータを記憶装置に記録する場合に、ホスト装置が独自データ記憶部と共通データ記憶部を論理的に構成し、含まれるデータの内容に応じて、ホスト装置が媒体上の記録先や読み出し元領域を適切に選択・指定する手段が、下記特許文献１に記載されている。

【非特許文献１】AdvancedAccess Content System (AACS)　Introduction and Common Cryptographic Elements　Revision0.91　February 17, 2006　(http://www.aacsla.com/specifications/specs091/AACS_Spec_Common_0.91.pdf)

【特許文献１】特開２００４－１９９７２２号公報

【発明の開示】

【発明が解決しようとする課題】

【０００４】

非特許文献１に関しては、暗号化して記録すべき情報の数が多くなるに従って、暗／復号化および転送に係る処理の負荷が増大してしまうという点が挙げられる。こういった課題は、暗／復号化を高度かつ厳重にするほど顕著となる。

【０００５】

特許文献１に関しては、記憶装置が着脱型の場合、その内部の構成は技術の進歩等によりに製品毎に異なるため、ホスト装置が記憶装置毎に詳細な内部構成を把握して、本特許に記載されたような方法で記憶領域を管理すること、そのような領域管理方法を設定された記憶装置を他のホスト装置でも利用できるようにすること、即ち相互運用性をの確保、が困難であるという点が挙げられる。

【０００６】

本発明は、上記実情に鑑みて為されたものであり、コンテンツデータと対応付けられる情報の暗／復号化および転送に係る処理の負荷を低減することが可能な、データ転送システム、データ転送方法、データ送信装置およびデータ受信装置を提供する。

【課題を解決するための手段】

【０００７】

本発明にかかるコンテンツ記録再生装置は、第１及び第２の記憶領域を有する記憶媒体と、制御部とを備え、この制御部は、コンテンツデータと対応付けられる複数の情報群の何れか同士において一部の情報が所定の関係を有するときに、この所定の関係を有する一部の情報群（基底値）を暗号化して第１の記憶領域に書き込み、所定の関係を有する情報を省略した個別情報群を生成し、暗号化すると共に、第１の記憶領域への記録先位置の情報を伴って、第２の記憶領域に書き込み、個別情報群と、第１の記憶領域への記録先位置の情報を伴って書き込まれた情報群とを読み出し復号化すると共に、第１の記憶領域への記録先位置の情報から第１の記録先位置上に記録されている情報群を読み出して復号化し、第２の記憶領域から読み出した情報群と、第１の記憶領域から読み出した情報群から、所定の関係に基づいて前記コンテンツデータと対応付けられる情報群を復元し、この復元した情報郡を外部装置に送信する。

【０００８】

或いは、コンテンツデータを記憶する第１の記憶媒体と、前記コンテンツデータと対応付けられる情報群を記憶する第２の記憶媒体と、これら記憶媒体を制御する制御部とを備え、この制御部は、第１の情報群と一部の情報が所定の関係を有する第二の情報群を記録する際には、所定の関係を有する情報を省略して生成した個別情報群を、第１の情報群中の所定の情報の記録先位置の情報を伴って、第２の記憶媒体上の領域に書き込み、第２の情報群を再生する際には、個別情報群と、記録先位置の情報を伴って書き込まれた情報群とを読み出し復号化すると共に、記録先位置の情報から所定の関係を有する第１の情報群の情報を読み出し、この第一の情報群の情報と個別情報群とからコンテンツデータと対応付けられる情報群を復元し、この復元した情報郡を外部装置に応答する。

【発明の効果】

【０００９】

本発明によれば、個別情報群を生成することによって情報量が軽減されるので、暗／復

号化および転送に係る処理の負荷を低減することができる。

【発明を実施するための最良の形態】

【００１０】

本発明の実施形態について、図面を参照しながら説明する。

【実施例１】

【００１１】

図１は、本発明の一実施形態に係るデータ転送システムの構成を表すブロック図である。データ転送システム1は、コンテンツ記録再生装置（Content Recorder / Player: 以下記録再生装置112）と、これに接続された複数の可搬型記憶装置（Detachable Storage Device: 以下 記憶装置120）とを備える。これら記録再生装置112及び記憶装置120は、動画データや音楽データ等のコンテンツデータや、こうしたコンテンツデータに対応付けられる利用制御情報（詳細は後述）を、互いに転送し合う。

【００１２】

ここで、データを送信する側の装置を第１の装置、データを受信する側の装置を第２の装置と定義する。つまり、記録再生装置112がデータを送信し、記憶装置120がこれを受信する場合には、記録再生装置112が第１の装置（データ送信装置）、記憶装置120が第２の装置（データ受信装置）に相当する。これとは逆に、記憶装置120がデータを送信し、記録再生装置112がこれを受信する場合には、記憶装置120が第１の装置（データ送信装置）、記録再生装置112が第２の装置（データ受信装置）に相当する。

【００１３】

記録再生装置112は、主にホスト管理部（Host Manager）110及びホストセキュリティ管理部（Host Security Manager）111を備える。これらは、内部バス109を介して互いに接続されている。

【００１４】

ホスト管理部110は、主に接続されている機器間のデータの転送を制御する機能を有するものである。例えば、ネットワーク（Network）140と接続するネットワークインタフェース部（Network Interface Unit）100、入力装置（Input Device）121を接続する入力装置インタフェース部（Input Device Interface Unit）105、記憶装置120を接続する複数のホストインタフェース部（Host Interface Unit）106、装置内の各構成の動作を統合的に管理するプロセッサ部（Processor Unit: PU）108等を通常含んでいる。

【００１５】

ホストセキュリティ管理部111は、ホスト装置保護情報記録部（Host Device Protected Information Storage）101、記録機能部（Recording Function Unit）102、再生機能部（Playback Function Unit）103、ホスト装置保護情報転送処理部（Host Device Protected Information Transfer function Unit）104を含んでいる。プロセッサ部108によるこれらの詳細な挙動については、後述する。ホストセキュリティ管理部111の一部もしくは全体は、ハードウェア及びソフトウェアの何れで構成されてもよい。

【００１６】

放送波発信元130や配信サーバ150は、コンテンツデータを所定の暗号化方式により暗号化して配信している。そして記録再生装置112は、放送波発信元130や配信サーバ150等から配信されるコンテンツデータを、放送波受信アンテナ131やデジタル信号端子132、ネットワーク140等を介して取得する。コンテンツデータには、暗号化されたコンテンツデータを復号化するための鍵データを含んだ利用制御情報が対応付けられており、この利用制御情報は、コンテンツデータとともに記録再生装置112が取得する。この利用制御情報は、コンテンツデータと同じ配信元から取得してもよいし、異なる配信元から取得してもよい。

【００１７】

こうして取得されるコンテンツデータ及び利用制御情報は、記録機能部102及びホスト装置保護情報転送処理部104の動作により、記録再生装置112に接続された記憶装置120に記憶される。

【００１８】
また、記憶装置120に記憶されたコンテンツデータ及び利用制御情報は、再生機能部103及びホスト装置保護情報転送処理部104の動作により、復号化および再生される。こうして再生されたコンテンツデータは、デジタル信号端子133やディスプレイ134、スピーカー135等に出力される。
【００１９】
ホストセキュリティ管理部111は、耐改竄性を有する形態で実装される。この性質により、ホストセキュリティ管理部111が取り扱う情報、即ち利用制御情報の、一般利用者による不正な取得、複製、改竄などが防止できる。ホストセキュリティ管理部111に含まれる各々の処理部が実行する処理内容の概要は、以下の通りである。ホスト装置保護情報転送処理部104は、記憶装置120との間での認証処理の他、完了した認証処理に基づいて記憶装置との間で利用制御情報の送受信処理を行う。認証処理では、規定された証明書の検証や、失効した証明書情報の検証等の処理が通常行われるが、証明書や証明書の失効情報は、ホスト装置保護情報記録部101に記録されている。また、ホスト装置保護情報記録部101には、認証処理や利用制御情報の転送処理に関する経過ログなどの保護が必要なデータも、処理を実行する過程で適宜記録される。
【００２０】
図２は、記憶装置120の構成例を表すブロック図である。記憶装置120は、記録再生装置112からの要求に応じてデータの読み書きを行う磁気ディスク装置として構成されている。記憶装置は、磁気記録媒体200、データを読み書きするヘッド202、ヘッド202を支持するアーム201、これらを制御する記憶装置制御部（Storage Controller）230及びプロセッサ部（Processor Unit: PU）231、記憶装置インタフェース部（Storage Interface Unit）220等を有している。
【００２１】
磁気記録媒体200には、記録再生装置112が送信した暗号化されたコンテンツデータが記録される。なお、この磁気記録媒体200には、どのような記録再生装置であっても制限なくデータの読み書きを行うことができるものとする。
【００２２】
さらに、記憶装置120は、ホストセキュリティ管理部111に対応する構成として、記憶装置セキュリティ管理部（Storage Security Manager）225を有している。
【００２３】
記憶装置セキュリティ管理部225は、記憶装置保護情報転送機能部（Storage Device Protected Information Transfer Function Unit）221、制限アクセス領域制御部（Qualified Storage Controller: QSC）222、制限アクセス領域（Qualified Storage: QS）223、記憶装置保護情報記録部（Storage Device Protected Information Storage）224を含んでいる。尚、制限アクセス領域223は、秘匿部（Veiled Part: VP）2230と公開部（Public Part: PP）2231とを含む。秘匿部2230と公開部2231の使用法については、図７，図８，図１０，図１１を用いて後で詳述する。記憶装置セキュリティ管理部225は、ホストセキュリティ管理部同様に、耐改竄性を有する形態で実装される。記憶装置セキュリティ管理部225の一部もしくは全体は、ハードウェア及びソフトウェアの何れで構成されてもよい。
【００２４】
これら記憶装置保護情報転送機能部221及び記憶装置保護情報記録部224は、ホスト装置保護情報転送処理部104及びホスト装置保護情報記録部101と同様の処理を行う。また、制限アクセス領域制御部222は、制限アクセス領域223に利用制御情報を記録したり、制限アクセス領域223から利用制御情報を読み出したりする処理を行う。
【００２５】
なお、記憶装置120は磁気ディスク装置として構成されているが、これに限られず、記憶装置セキュリティ管理部225を含んでいれば、半導体メモリデバイス等の他の記憶装置であってもよい。

【００２６】
図１では、ホストセキュリティ管理部111と記憶装置セキュリティ管理部225が近接的に接続された形態が示されているが、両者の接続はこれに限られるものではない。例えば、図３に示される態様であってもよい。その態様は、ホストセキュリティ管理部111を有するコンテンツ記録再生装置3000と、データの送受信機能としてのホスト管理部110のみを有するデータ転送用ホスト装置（Host Device for Data Transfer）3010とがネットワークを介して接続されていて、データ転送用ホスト装置3010に、記憶装置セキュリティ管理部225を有する記憶装置（Storage Device）4020が接続されるというものである。この場合、記憶装置120に対するデータの読み書き処理は、データ転送用ホスト装置3010のホスト管理部110が主体となって行うが、認証や利用制御情報の転送等の保護情報への直接的なアクセスを伴う処理は、コンテンツ記録再生装置112のホストセキュリティ管理部111と、記憶装置4020の記憶装置セキュリティ管理部225とが実行する。尚、図３のコンテンツ記録再生装置3000には、ホスト管理部110やネットワークインタフェース部100が記載されていないが、コンテンツ記録再生装置はネットワークを介して他の装置と通信するため、これらの機能部も当然含んでいる。データ転送用ホスト装置3010も同様である。
【００２７】
次に、記録再生装置112と記憶装置120との間で転送される利用制御情報の例を、図４を用いて説明する。
【００２８】
利用制御情報（Usage Control Information: UCI）は、コンテンツデータの利用を制御する上で必要な複数種類の情報を含む情報群であり、コンテンツデータと対応付けられる。
【００２９】
対応サービスタイプ指示子（Corresponding Service Type Specifier: CSTS）401は、利用制御情報UCIが対応付けられたコンテンツデータが属するサービスを示す。
【００３０】
利用制御情報識別子（Usage Control information Identifier: UCIID）402は、利用制御情報UCIに割り当てられた識別子（ID）である。
【００３１】
記憶装置セキュリティ管理部用利用規則（Usage Rule enforced in Storage Security Manager: UR_S）403は、記憶装置セキュリティ管理部225側において、利用制御情報UCIが対応付けられたコンテンツデータの利用を制限するための規則を示す。UR_Sとしては、例えばコピーや視聴の実行可能回数などが想定される。規則によって許可された条件を超える利用をコンテンツ記録再生装置112から求められた場合、記憶装置セキュリティ管理部225は、利用制御情報UCIを出力しない。尚、下線を伴って記されるx（例えば_S）は、図中では下付きの添え字として表現されている。この表現法は、以降で示される全ての図においても同様に用いられる。
【００３２】
暗号演算関連情報（Cipher Information: CI）404は、利用制御情報UCIに対応付けられている暗号化された状態のコンテンツデータを復号するための鍵データ及び暗号関連演算を実行する上で必要なパラメータを含む情報である。
【００３３】
再生機能部用利用規則（Usage Rule enforced in Playback Function Unit: UR_P）405は、ホストセキュリティ管理部111において、利用制御情報UCIが対応付けられたコンテンツデータの利用を制限するための規則を示す。こうした規則としては、例えば出力可能な接続相手装置を特定する情報や視聴可能期間などが想定される（但し、UR_Sとは重複しない）。この規則によって許可された条件を超える利用を利用者が求めた場合、ホストセキュリティ管理部111は、対応するコンテンツデータを復号しない。
【００３４】
コンテンツデータ識別子（Content Identifier: CID）406は、利用制御情報UCIに対応

付けられたコンテンツデータの識別子（ID）である。

【００３５】

他の情報（Other Information: OIと表す）407は、コンテンツデータの利用制御とは直接関係のない情報である。

【００３６】

以下、記録再生装置112と記憶装置120との間で実現される、本発明の一実施形態に係るデータ転送方法について、図５及び図６を用いて説明する。図６は利用制御情報の転送方法を示すものであり、図５はこの転送に先立って実行する必要がある認証処理を示すものである。

【００３７】

[暗号化について]

本実施形態のデータ転送方法について具体的に説明する前に、まず、本実施形態で用いられる暗号化について説明する。本実施形態では、非対称暗号用の鍵データと対称暗号用の鍵データとが用いられる。このうち、非対称暗号用の２種類の鍵データを公開鍵・秘密鍵と呼び、対称暗号用の鍵データを共通鍵と呼ぶ。

【００３８】

以下の説明では、公開鍵をKpu_Exposition[Device]と表し、秘密鍵をKpr_Exposition[Device]と表す。ここで、[x]のように[]を伴って付けられた添え字xは、秘匿部VP2230上に記録されている基底値（Base Value; BV）を判別するためのものである。例えば、[]の文字「Device」は、それぞれその公開鍵もしくは秘密鍵を保持する装置を表す。角括弧内の文字がHであれば記録再生装置112を表し、Sであれば記憶装置120を表す。また、下付きの文字列「Exposition」は、その公開鍵もしくは秘密鍵の素性を説明するための文字列を表す。例えば、Kpr_CAは、証明書を発行する認証局だけが把握し、また管理している秘密鍵であることを意味する。通常は、発行する証明書に含まれる電子署名を計算する際に用いられる。Kpu_CAは、このKpr_CAに対する公開鍵である。これらは、証明書に含まれる電子署名の検証に用いられる。同様に、Kpu_CRは各証明書に含まれる公開鍵を、Kpr_CRはこのKpu_CRに対する秘密鍵を表す。以上のような観点から、Kpu_CR[Device]を含み、Kpr_CAを用いて計算された電子署名部を含む証明書を、C(Kpr_CA, Kpu_CR[Device])と記述する。

【００３９】

また共通鍵は、K_ch[Device], K_s[Device]Orderと表される。これら２つの共通鍵のうち、K_chをチャレンジ鍵（Challenge Key）、K_sをセッション鍵（Session Key）と呼ぶ。チャレンジ鍵K_chは、証明書を交換する過程で一時的に生成される鍵である。他方K_sは、利用制御情報の転送に際して、この利用制御情報を暗号化する際に用いられる。セッション鍵は、利用制御情報の転送処理を行う度に新しいものを生成して利用するので、その順番を「Order」で表現する。

【００４０】

鍵データXを用いてデータYを暗号化する処理は、E(X, Y)と表される。同様に、鍵データXを用いて暗号化されたデータYを復号する処理は、D(X, Y)と表される。また、データXのハッシュ値を求める処理はH(X)、データXとデータYとを連結する処理はX || Yと表される。

【００４１】

次に、非対称暗号化の演算方法について補足する。本実施形態では、認証処理の過程で公開鍵Kpuを用いた暗号化を何度か実行する。公開鍵Kpuを用いた暗号化、及び公開鍵に対する秘密鍵Kprを用いた復号化は、一般に知られているDiffie-Hellman法（以下DH法）を用いて、1つの鍵データを秘密裏に共有し、この鍵データを用いて対象のメッセージデータを対称暗号化することを想定するが、その方法に限定するものではない。例えば、対象のメッセージデータを、公開鍵Kpuを用いて直接暗号化し、この暗号化されたメッセージデータを受信した側において、秘密鍵を用いて受信したデータを直接復号化するような方法を用いても良い。また、非対称暗号アルゴリズムとしてはどのようなものを用いても構わない。

【００４２】
例として、冪乗演算に基づく原型のDH法による鍵データ共有法と、楕円曲線上の加法演算に基づく鍵データ共有法とを以下に述べる。冪乗演算に基づく原型DH法に基づいて鍵データを２者間で共有するには、まず両者の間で、予めある値Gの共有を行っておく必要がある。説明の都合上、これら２者を装置Ｉ，装置ＩＩと記述する。なお、値Gは公開されていて構わない。続いて、装置Ｉは、所定の長さの自然数aを1つ生成し、秘密裏に保持する。続いて、装置Ｉは、共有化されたGをa乗し、得られた数値G＾a（＾は冪乗を表す）を装置ＩＩへ送信する。装置ＩＩは、装置Ｉと同様に、自然数bを1つ生成し、秘密裏に保持する。そしてG＾aを受信すると、このG＾aを更にb乗し、(G＾a)＾bを得る。一方で、Gをb乗した結果G＾bを装置Ｉに送信する。装置Ｉは、G＾bを受信すると、このG＾bを更にa乗し、(G＾b)＾aを得る。以上の処理によって、装置Ｉと装置ＩＩの間で(G＾b)＾a=(G＾a)＾bが秘密裏に共有されたことになる。

【００４３】
そこで、a，bをそれぞれ装置Ｉ，装置ＩＩの秘密鍵Kpr1，Kpr2とし、G＾a，G＾bをそれぞれ装置Ｉ，装置ＩＩの公開鍵Kpu1，Kpu2とすると、DH法に基づいた、あるメッセージデータMの公開鍵Kpu1による暗号化E(Kpu1，M)は、実際には、(G＾a)＾bを対称暗号用の鍵データとして用いてE((G＾a)＾b，M)を求め、このE((G＾a)＾b，M)にKpu2を連結し、E((G＾a)＾b，M) || Kpu2を生成したものである。なお、演算上は、a，b，G＾a，G＾bは、毎度動的に生成しても、固定的に各装置に記録されていても構わない。

【００４４】
楕円曲線上の加法演算に基づく鍵データ共有法は、冪乗演算に基づく鍵データ共有法とほぼ同じである。但し、以下３点が異なる。

【００４５】
１.一般にGはベースポイントと呼ばれ、２次元の座標(Gx，Gy)であること。

【００４６】
２.冪乗演算G＾aが楕円曲線上のベースポイントのa回加法演算となること（これをa*Gと記す）。

【００４７】
３.b*(a*G)の演算結果が２次元座標値となるため、b*(a*G)に予め決められた演算を行って１次元スカラー値を算出し、この１次元スカラー値を対称暗号化用鍵データとしてメッセージデータMを暗号化すること。

【００４８】
本実施例において、E(Kpu，M)という記述は、上記の通りE((G＾a)＾b，M) || Kpu2もしくはE(ｆ(b*(a*G))，M) || Kpu2を意味するものとする。なお、ｆ(b*(a*G))は、b*(a*G)から１つのスカラー値を求める演算を意味する。一方で、E(*Kpu，M)という記述は、*Kpu=(G＾a)＾bもしくはｆ(b*(a*G))を用いて、メッセージデータMを対称暗号化することを意味する。またM’=E(Kpu，M)の復号はD(Kpr，M’)と記述するが、これは*Kpr=(G＾b)＾aもしくはｆ(a*(b*G))を用いて対称暗号方式の復号演算D((G＾b)＾a，M’)もしくはD(ｆ(a*(b*G))，M’)を行うことを意味する。

【００４９】
図５は、利用制御情報の転送処理に先立って実行される認証処理の例を示す図である。ホストセキュリティ管理部111内のホスト装置保護情報記憶部101には、証明書C(Kpr_CA，Kpu_CR[H])，認証局公開鍵Kpu_CA，ホスト装置公開鍵Kpu_[H]，ホスト装置秘密鍵Kpr_[H]が、予め記録されているものとする(処理5000)。同様に、記憶装置セキュリティ管理部225内の記憶装置保護情報記録部224には、証明書C(Kpr_CA，Kpu_CR[S])，認証局公開鍵Kpu_CA，記憶装置公開鍵Kpu_[S]，記憶装置秘密鍵Kpr_[H]が、予め記録されているものとする（処理5001）。

【００５０】
処理5010において、記憶装置セキュリティ管理部225内の記憶装置保護情報転送機能部221は、記憶装置保護情報記録部224に記録されている証明書C(Kpr_CA，Kpu_CR[S])を、ホ

ストセキュリティ管理部111へ送信する。
【００５１】
処理5011において、ホストセキュリティ管理部111は、以下の処理を実行する。
【００５２】
１.ホスト装置保護情報転送機能部104は、受信した証明書C(Kpr_CA, Kpu_CR[S])の正当性を検証する。
【００５３】
２.受信した証明書の正当性が確認されると、チャレンジ鍵K_ch[H]を生成する。
【００５４】
３.受信した証明書C(Kpr_CA, Kpu_CR[S])に含まれる公開鍵Kpu_CR[S]を用いて、K_ch[H]を暗号化し、暗号化データE(Kpu_CR[S], K_ch[H])を生成する。
【００５５】
４.得られた暗号化データに、自身に記録されている証明書C(Kpr_CA, Kpu_CR[H])を連結する。
【００５６】
処理5020において、ホスト装置保護情報転送機能部104は、得られたデータC(Kpr_CA, Kpu_CR[H])|| E(Kpu_CR[S], K_ch[H])を、記憶装置セキュリティ管理部225に送信する。
【００５７】
処理5021において、記憶装置セキュリティ管理部225は、以下の処理を実行する。
【００５８】
１.記憶装置保護情報転送機能部221は、受信したデータの正当性を検証する。
【００５９】
２.受信したデータの正当性が確認されると、このデータを自身に記録されている公開鍵Kpr_CR[S]を用いて復号し、チャレンジ鍵K_ch[H]を取得する。
【００６０】
３.チャレンジ鍵K_ch[H]の取得を終えると、チャレンジ鍵K_ch[S]を生成し、K_ch[S]と自身に記録されている公開鍵Kpu_[S]とを連結する。
【００６１】
４.処理5021.3において連結されたデータを、受信したホストセキュリティ管理部111の証明書に含まれる公開鍵Kpu_CR[H]で暗号化し、暗号化データE(Kpu_CR[H], K_ch[S] || Kpu_[S])を生成する。更に、得られた暗号化データE(Kpu_CR[H], K_ch[S] || Kpu_[S])を、受信したK_ch[H]で暗号化し、暗号化データ E(K_ch[H], E(Kpu_CR[H], K_ch[S] || Kpu_[S]))を得る。
【００６２】
処理5030において、記憶装置保護情報転送機能部221は、処理5021.4で得られた暗号化データを、ホストセキュリティ管理部111に送信する。
【００６３】
処理5031において、ホストセキュリティ管理部111は、以下の処理を実行する。
【００６４】
１.ホスト装置保護情報転送処理部104は、受信した暗号化データを、自身が保持するK_ch[H], 秘密鍵Kpr_CR[H]で復号する。
【００６５】
２.0次セッション鍵K_s[H]0を生成する。
【００６６】
３.K_s[H]0と自身に記録されている公開鍵Kpu_[H]とを連結する。
【００６７】
４.K_s[H]0||Kpu_[H]をデータの復号結果に含まれるKpu_[S]で暗号化した後、さらにK_ch[S]で暗号化し、暗号化データE(K_ch[S], E(Kpu_[S], K_s[H]0 || Kpu_[H]))を生成する。なお、本演算の結果として、ホスト装置保護情報転送処理部104には、*Kpu_[S]が生成される。

【００６８】
処理5040において、ホスト装置保護情報転送処理部104は、処理5031.4で得られた暗号化データE(K_ch[S], E(Kpu_[S], K_s[H]0 || Kpu_[H]))を、記憶装置セキュリティ管理部225に送信する。
【００６９】
処理5041において、記憶装置セキュリティ管理部225は、以下の処理を実行する。
【００７０】
１.記憶装置保護情報転送機能部221は、受信した暗号化データを、自身が保持するK_ch[S], 秘密鍵Kpr_[S]で復号する。本演算の結果として、記憶装置保護情報転送機能部221には、*Kpr_[S]が生成される。*Kpu_[S]と*Kpr_[S]とは実際には同値である。
【００７１】
２.0次セッション鍵K_s[S]0を生成する。
【００７２】
３.K_s[S]0を、受信した暗号化データの復号結果に含まれるK_s[H]0で暗号化した後、さらにKpu_[H]で暗号化し、暗号化データE(Kpu_[H], E(K_s[H]0, K_s[S]0))を生成する。なお、本演算の結果として、記憶装置セキュリティ管理部には、*Kpu_[H]が生成される。
【００７３】
処理5050において、記憶装置保護情報転送機能部221は、処理5041(3)で得られた暗号化データE(Kpu_[H], E(K_s[H]0, K_s[S]0))を、ホストセキュリティ管理部111に送信する。
【００７４】
処理5051において、ホストセキュリティ管理部111は、以下の処理を実行する。
【００７５】
１.ホスト装置保護情報転送機能部104は、受信した暗号化データを、自身が保持する秘密鍵Kpr_[H], 0次セッション鍵K_s[H]0で復号する。本演算の結果として、ホスト装置保護情報転送機能部104には、*Kpr_[S]が生成される。
【００７６】
なお、上記説明では、受信した暗号化データを復号した際のデータの完全性の確認等の処理については特に述べなかったが、そうした処理は当然に実行するものとする。また、認証処理の過程で、より新しい証明書失効情報を保持している装置から、他方の装置へより新しい証明書失効情報を送信し、古い証明書失効情報を上書きする等の処理を差し挟んでも構わない。
【００７７】
以上に説明した一連の処理手続きは、あくまで装置間で実行される認証処理の一例である。ここで必要なことは、認証処理を完了すると、この認証処理を実行した装置の間で、利用制御情報を暗号化して転送する際に使用する鍵データと、この転送する際に使用する鍵データを共有する鍵データとが共有されているということである。図５に示した例の場合、これらに当たる鍵データは、ホスト装置共有鍵*Kpu_[H](= *Kpr_[H]), 記憶装置共有鍵*Kpu_[S](= *Kpr_[S]), ホスト装置0次セッション鍵(K_s[H]0), 記憶装置0次セッション鍵(K_s[S]0)である。
【００７８】
[記録再生装置から記憶装置への利用制御情報の書き込み処理]
図６は、記録再生装置112から記憶装置120への利用制御情報の転送処理の例を示す図である。なお、転送処理を開始する時点において、ホストセキュリティ管理部111と記憶装置セキュリティ管理部225との間では、*Kpu_[S](=*Kpr_[S]), ホスト装置m次セッション鍵(K_s[H]m), 記憶装置n次セッション鍵(K_s[S]n)が共有されているものとする。これは、転送処理を実行するまでの間に、記録再生装置112から記憶装置120への利用制御情報の転送処理がn回、記憶装置120から記録再生装置112への利用制御情報の転送処理がm回実行されたことを意味する。尚、n, mが0、すなわち認証処理しか実行されていないとしてもよい。
【００７９】

処理6000において、ホスト管理部110は、ホストセキュリティ管理部111内のホスト装置保護情報転送機能部104及び記録機能部102に対して、記憶装置120に送信する予定のN個の利用制御情報UCI_1, …, UCI_Nを準備するように要求する。

【００８０】

処理6001において、記録機能部102は、送信予定のN個の利用制御情報UCI_1, …, UCI_Nを生成する。ホスト装置保護情報転送機能部104は、これら利用制御情報UCI_1, …, UCI_Nを一時的に蓄積する。

【００８１】

処理6010において、ホストセキュリティ管理部111が処理6001を実行している間に、ホスト管理部110は、記憶装置セキュリティ管理部225内の記憶装置保護情報転送機能部221に対してセッション鍵データ生成要求を送信する。

【００８２】

処理6011において、記憶装置セキュリティ管理部225は、以下の処理を実行する。

【００８３】

１.記憶装置保護情報転送機能部221は、セッション鍵K_s[S]n+1を生成する。

【００８４】

２.記憶装置保護情報転送機能部221は、K_s[S]n及びK_s[H]mを用いて、処理6011.1で生成したK_s[S]n+1を暗号化する。K_s[S]n及びK_s[H]mは、本処理を実行する時点で共有されている、記憶装置保護情報転送機能部221及びホスト装置保護情報転送処理部104が過去に生成したセッション鍵のうちで、最新のものである。

【００８５】

処理6020において、記憶装置保護情報転送機能部221は、生成された暗号化データE(K_s[H]m, E(K_s[S]n, K_s[S]n+1))を、ホスト管理部110へ送信する。

【００８６】

処理6021において、ホストセキュリティ管理部111は、以下の処理を実行する。

【００８７】

１.ホスト装置保護情報転送機能部104は、受信した暗号化データE(K_s[H]m, E(K_s[S]n, K_s[S]n+1))を、自身が保持するK_s[H]m及びK_s[S]nを用いて復号する。

【００８８】

２.ホスト装置保護情報転送機能部104は、復号により得たK_s[S]n+1の完全性を確認する。完全性の確認処理とは、例えば、セッション鍵K_s[S]n+1に割り当てられたタグ値に誤りがないか確認したり、セッション鍵K_s[S]n+1に対して付けられた誤り検出符号からデータに誤りがないか確認したり、といった類のものである。

【００８９】

３.ホスト装置保護情報転送機能部104は、処理6001で準備したN個の利用制御情報と、その記録先位置DUCILs（Destination Location for UCIs）とを連結し、復号により得たK_s[S]n+1及び認証処理において共有した*Kpu_[S]で暗号化する。この時、送信用メッセージデータとは別に、ホストインタフェース部106は、書き込み用命令に付随するパラメータとして記録先位置情報を指定しても良い。現在広く使われている磁気ディスク装置等の記憶装置の場合は、受信するデータの大きさを把握する等の目的から、このような手段は有効である。

【００９０】

処理6030において、ホスト装置保護情報転送処理部104は、生成された暗号化データE(*Kpu_[S], E(K_s[S]n+1, UCI_1 || … || UCI_N || DUCILs))を、記憶装置セキュリティ管理部225へ送信する。

【００９１】

処理6031において、記憶装置セキュリティ管理部225は、以下の処理を実行する。

【００９２】

１.記憶装置保護情報転送機能部221は、受信した暗号化データE(*Kpu_[S], E(K_s[S]n+1, UCI_1 || … || UCI_N || DUCILs))を、自身が保持する*Kpr_[S]及びK_s[S]n+1を用い

て復号する。

【００９３】

２.記憶装置保護情報転送機能部221は、復号により得られたUCI_1 || … || UCI_N || DUCILsの完全性を確認する。

【００９４】

３.制限アクセス領域制御部222は、記憶装置セキュリティ管理部用利用規則UR_Sを所定の規則に従って変更した後、DUCILsが指し示す制限アクセス領域223内の位置に、利用制御情報UCI_1, …, UCI_Nを記録する。記録が完了すると、利用制御情報UCI_1, …, UCI_Nは、制限アクセス領域制御部222から消去する。

【００９５】

以上の処理によって、制限アクセス領域223への利用制御情報UCI_1, …, UCI_Nの書き込み処理が完了する。

【００９６】

この時、送信予定のN個の利用制御情報UCI_1, …, UCI_Nが対応付けられたN個のコンテンツデータがまとまって1つの番組を構成しているような場合等には、利用制御情報UCI_1, …, UCI_Nに含まれる情報（図４を参照）のうち、対応サービスタイプ指示子USTS、記憶装置セキュリティ管理部用利用規則UR_S、及び再生機能部用利用規則URPは、多くの場合UCIの番号による違いはない。また、利用制御情報識別子UCIIDおよびコンテンツデータ識別子CIDは、所定の増分（例えば1）で連続する等、所定の規則で変化することが多いと考えられる。

【００９７】

ところで、制限アクセス領域の実現に際して、従来の記憶装置において搭載されていた媒体とは別の改竄及び不正アクセスを防止できるようにするための何らかの物理的手段を伴った新たな媒体を搭載しようとすると、通常その実装には非常に多くの困難を伴う。また、改竄及び不正アクセス防止を実現するには、新規の開発や媒体の搭載が必要になるため、機器単体の開発製造費が高くなるという問題も孕んでいる。このような状態を回避するには、記憶装置インタフェース部220や記憶装置保護情報転送機能部221に、接続されたホスト装置からのアクセスを論理的に制限するような機能を搭載し、媒体としては既に搭載されているものの一部を流用するようにするのが有効である。但し、記憶装置を分解して、装置内の領域に記録されている情報を直接読み取ろうとするような攻撃を無効化するために、保護が必要な情報を制限アクセス領域223へ情報を記録する際には、制限アクセス領域制御部222のみが把握している鍵データを用いて暗号化を施す等の手段を講じるのが有効である。

【００９８】

上記のような方針に従って制限アクセス領域223へデータを記録する場合、書き込み及び読み出し対象のデータが増えると、それに伴う制限アクセス領域制御部222における暗復号化処理が増大し、記憶装置における利用制御情報の転送処理性能低下を招く。

【００９９】

そこで以下では、図７及び図８を用いて、処理6031.3に於いてより効率的に制限アクセス領域223へ利用制御情報を書き込む処理を、詳細に説明する。図７はこの処理の流れを実現するモジュール構成及び受信したN個の利用制御情報を実際に記録する手段を示したものである。

【０１００】

[利用制御情報書き込み処理のための記憶装置セキュリティ管理部内構成要素]

次段に於いて、利用制御情報書き込み処理における記憶装置セキュリティ管理部内の詳細動作を説明する際に、記憶装置セキュリティ管理部の構成要素の役割についての詳細な説明も与えるが、本段でも図７を用いて概要を簡単に記しておく。

【０１０１】

記憶装置セキュリティ管理部内は、基底値（Base Value; BV）及び基底値記録位置（Recorded Location of Base Value; BVL）保持部（BV & BVL Retainer）720, 差分（Differ

ence; DIFと記す）計算／基底値指示子（BV Pointer; BVP）決定部（DIF Calculator / BVP Determiner）721，基底値及び基底値記録位置決定部730（BV & BVL Determiner），基底値及び暗号演算関連情報暗復号化部（BV & CI En/Decrypter）731を、構成要素として持つ。また、制限アクセス領域(QS)223は、秘匿部（Veiled Part; VPと記す）2230と公開部（Public Part; PPと記す）2231から成る。

【０１０２】

基底値及び基底値記録位置保持部（BV & BVL Retainer）720は、基底値及び基底値記録位置（何れも後述）を保持する媒体である。この媒体としては、揮発型のものを用いるのが一般的であるが、不揮発型のものを用いても良い。但し、不揮発型の媒体を用いた場合、動作をし続ける過程で容量を全て消費してしまう可能性がある。その場合は、処理上不要と推測される可能性が高いデータを上書きするのが有効であり、また最も一般的である。例えば、処理実行時から見て最も過去に記録されたデータは、そのような目的に合致する可能性が高い。但し、最も過去に記録されたデータに限る必要はない。差分計算／基底値指示子決定部（DIF Calculator / BVP Determiner）721は、基底値に含まれる利用制御情報識別子(UCIID)及びコンテンツデータ識別子(CID)と、現在処理対象としている利用制御情報UCIの同識別子との差分を計算すること、及び利用制御情報の基となる基底値(BV)を指し示す基底値指示子（Base Value Pointer; BVPと記す）を決定する。基底値及び基底値記録位置決定部（BV & BVL Determiner）730は、受信した利用制御情報(UCI)から基底値(BV)を決定すると共に、制限アクセス領域223内の秘匿部（Veiled Part; VPと記す）2230の空き領域から、基底値の書き込み先位置を決定する。基底値及び暗号演算関連情報暗復号化部（BV & CI En/Decrypter）731は、基底値(BV)及び利用制御情報に含まれる暗号関連演算情報(CI)404を、暗号化及び復号化する。

【０１０３】

公開部(PP)2231は、記憶装置保護情報転送機能部221とホスト装置保護情報転送機能部221の間で規定された認証処理を完了すると、ホストインタフェース部106が位置情報を指定することにより、直接データを書き込んだり、記録されているデータを読み出したりすることができる領域である。一方で秘匿部(VP)2230を記憶装置インタフェース部220の外側から直接アクセスする際に必要な命令や位置情報を特に規定する必要はなく、その意味においてホスト装置からは秘匿されている領域である。但し、規定された一定の処理を記憶装置内で経ることによって、ホスト装置からは秘匿されている領域に対して間接的にデータを記録したり、記録されているデータを読み出したりすることはできる。尚、詳細は後述するが、秘匿部(VP)2230として確保する記憶容量は、処理特性上公開部(PP)2231より小さくて良いので、秘匿部(VP)2230を公開部(PP)2231とは物理的に異なる媒体上に構築しても良い。その場合に、秘匿部(VP)2230を構築した媒体が物理的な耐改竄性を有する態様であった場合は、秘匿されている領域に情報を記録する場合は、平文のまま記録しても良い。

【０１０４】

[利用制御情報書き込み処理における記憶装置セキュリティ管理部内動作]

記憶装置インタフェース部220で受信したN個の暗号化された利用制御情報700を含むデータは、処理6031.1に記述したように、記憶装置保護情報転送機能部221内における復号器(Decrypter)710において、K_s[S]m及び*Kpr_[S]を用いて先ず復号される。この復号処理によって、制限アクセス領域制御部222内には、平文状態でUCI_1からUCI_NのN個の利用制御情報70010，70011，70012，70013，70014，70015，70016が一時的に保持される。以下、動作の説明に先立ち、制限アクセス領域管理部は、次の状態にあることを仮定する。

【０１０５】

(1)N個の利用制御情報のうち、UCI_1，UCI_2，…，UCI_r-1のサービスタイプ指示子(CSTS)401，記憶装置セキュリティ管理部用利用規則(UR_S)403，再生機能部用利用規則(UR_P)405，他の情報(OI)407は、添え字が異なっても同じ値が設定されている。

【０１０６】

(2)UCI_rのサービスタイプ指示子(CSTS)401，記憶装置セキュリティ管理部用利用規則

(UR_S)403，再生機能部用利用規則(UR_P)405，他の情報(OI)407は、UCI_r-1等のそれとは一部もしくは全てが異なるとし、その一方で、UCI_r，UCI_r+1，…，UCI_N-1，UCI_Nのサービスタイプ指示子(CSTS)401，記憶装置セキュリティ管理部用利用規則(UR_S)403，再生機能部用利用規則(UR_P)405，他の情報(OI)407は、添え字が異なっても同じ値が設定されている。

【０１０７】

（3)秘匿部(VP)2230には、L個の基底値（BV[1]，…，BV[L]）が、暗号化された状態で記録されている。尚、1つの基底値(BV)とは、ある1つの利用制御情報(UCI)に実際に含まれていた、暗号関連演算情報CI404を除く全ての項目の値を含む実データである。

【０１０８】

（4)基底値及び基底値記録位置保持部(BV & BVL Retainer)720は、基底値(BV)と、この基底値(BV)が実際に記録されている秘匿部(VP)2230内の記録位置BVLを1つの組として、M個の組（(BV_1，BVL_1)，…，(BV_M，BVL_M)）を一時的に保持している。ここで、Mは0でも良い。ここで下付きの添え字は、制限アクセス領域制御部222に一時的に保持されている基底値BV及び基底値記録位置BVL等を識別するためものである。

【０１０９】

尚、BV[*]という表記は、説明上基底値(BV)の秘匿部(VP)2230内に於ける順番を特に考慮する必要がない（対応するものが、秘匿部(VP)2230内の何れかの領域に適切に記録されている）場合に用いる。

【０１１０】

以下、図８を用いて制限アクセス領域制御部222における処理の流れを説明する。

【０１１１】

[処理800]

復号処理以前（同時並列処理でも良い）に、制限アクセス領域制御部222内の基底値及び暗号演算関連情報暗復号化部（BV & CI En/Decrypter）731は、利用制御情報暗号化鍵K_QSを決定（生成、もしくは既に生成済みのものの中から選択）する。K_QSは、機器製造時等に予め埋め込んでおいた固定データを継続的に使用し続けても、適当な規則に従って新たなものを生成してそれを使用しても良い。何れにしても利用制御情報暗号化鍵K_QSは、制限アクセス領域に利用制御情報を記録する際に、記録するデータを暗復号化する（前段(4)に記載）際に用いる鍵データであるので、制限アクセス領域に記録された利用制御情報を読み出す際に、この利用制御情報の暗号化に用いたK_QSを判別できるようにしておくことは必要である。K_QSは、制限アクセス領域を実現する核となるものであるが、その保持方法の開示は本発明の目的外であるため、本実施の形態では本件に関するこれ以上の説明は与えない。

【０１１２】

[処理801]

差分計算／基底値指示子決定部（DIF Calculator / BVP Determiner）721は、受信したN個の利用制御情報UCIを識別するための添え字変数iに、1を設定する。

【０１１３】

[処理810]

差分計算／基底値指示子決定部（DIF Calculator / BVP Determiner）721は、受信したUCIと比較する基底値BVを識別するための添え字変数jに、1を設定する。

【０１１４】

[処理811]

差分計算／基底値指示子決定部(DIF Calculator / BVP Determiner)721は、基底値及び基底値記録位置保持部(BV & BVL Retainer)720に保持されている基底値BV_j（ここではj=1）及びこの基底値BV[*]_jと組を構成している基底値記録位置BVL[*]_jを読み出す。そして基底値BV[*]_j（j=1）と受信した利用制御情報UCI_i（i=1）の対応サービスタイプ指示子(CSTS)401，記憶装置セキュリティ管理部用利用規則(UR_S)403，再生機能部用利用規則(UR_P)405，他の情報(OI)407とを比較する。

【０１１５】
[処理812]
処理811における比較の結果、比較した全ての項目について基底値BV[*]_j（j=1）と利用制御情報UCI_i（i=1）が一致すれば、処理820を実行する。1つでも一致しない項目があった場合は、処理830を実行する。以下では、先ず処理820から始まる手続きについて説明し、その後830から始まる処理について説明する。
【０１１６】
[処理820]
１.差引値用変数（Variable for Subtracting Value; SVV）に、BV[*]_j（j=1）に含まれる利用制御情報識別子(UCIID)402及びコンテンツデータ識別子(CID)406の値を設定する。差引値用変数は、1つの基底値BVに含まれる利用制御情報識別子(UCIID)402及びコンテンツデータ識別子(CID)406の値を一時的に保持するための、差分計算／基底値指示子決定部(DIF Calculator / BVP Determiner)721が管理する変数である。
【０１１７】
２.基底値指示子BVP_i（利用制御情報UCI_i用，詳細は後述）に、BV_j（j=1）と組になっていた基底値記録位置BVL[*]_j（j=1）を設定する。
【０１１８】
[処理830]
添え字jの値に1を加算する。
【０１１９】
[処理831]
処理830において得られたjの値が、その時点で基底値及び基底値記録位置保持部（BV & BVL Retainer）720が保持している基底値BVの総数Mより大きいか否かを判定する。もしjの値がM以下であった場合は、処理811へ戻る。一方で、jの値がMを超えていた（即ちj=M+1）場合は、処理832を実行する。
【０１２０】
[処理832]
１.差分計算／基底値指示子決定部(DIF Calculator / BVP Determiner)721は、受信した利用制御情報UCI_iを基底値及び基底値記録位置決定部（BV & BVL Determiner）730へ送信する。決定部730は、受信した利用制御情報UCI_iが含むCI以外のデータから、基底値(BV)を生成すると共に、基底値(BV)の記録先位置BVLを決定する。基底値(BV)の記録先位置BVLとしては、秘匿部(VP)2230において使用されていない領域を選択するのが一般的である。そして、基底値BV及び基底値記録位置BVLを、基底値及び暗号演算関連情報暗復号化部(BV & CI En/Decrypter)731及び基底値及び基底値記録位置保持部(BV & BVL Retainer)720へ送信する。尚、基底値(BV)及び基底値記録位置BVLの添え字は、BV[L+1]_j，BVL[L+1]_jであるのは明らかである（ここで、j=M+1である）。拠って、以下ではこのように表記する。
【０１２１】
２.基底値及び暗号演算関連情報暗復号化部(BV & CI En/Decrypter)731は、受信したL+1番目の基底値BV[L+1]を、利用制御情報暗号化鍵K_QSを用いて暗号化し、暗号化されたL+1番目の基底値E.BV[L+1]を得る。
【０１２２】
３.基底値及び暗号演算関連情報暗復号化部(BV & CI En/Decrypter)731は、処理832.2で得られた暗号化されたL+1番目の基底値E.BV[L+1]を、受信した基底値記録位置BVL[L+1]が指し示す秘匿部(VP)2230内の領域に書き込む。
【０１２３】
４.処理832.2及び処理832.3と並行して、基底値及び基底値記録位置保持部(BV & BVL Retainer)720は、受信したL+1番目の基底値BV[L+1]及びこの基底値の記録位置BVL[L+1]を、BV[L+1]_(M+1)，BVL[L+1]_(M+1)）の組で新たに保持する。更に、保持したデータの組を、差分計算／基底値指示子決定部(DIF Calculator / BVP Determiner)721に送信する。

【０１２４】
５.差分計算／基底値指示子決定部(DIF Calculator / BVP Determiner)721は、差引値用変数SVVに、受信したBV[L+1]_(M+1)に含まれる利用制御情報識別子(UCIID)402及びコンテンツデータ識別子(CID)406の値を設定する。
【０１２５】
６.差分計算／基底値指示子決定部(DIF Calculator / BVP Determiner)721は、基底値指示子BVP_iにBV_（M+1）と組になっていた基底値記録位置BVL[L+1]_（M+1）を設定する。
【０１２６】
７.基底値及び暗号演算関連情報暗復号化部(BV & CI En/Decrypter)731が把握している、秘匿部(VP)2230に記録されている基底値BVの数Lに、1を加算する。
【０１２７】
８.基底値及び基底値記録位置保持部(BV & BVL Retainer)720及び差分計算／基底値指示子決定部(DIF Calculator / BVP Determiner)721は、一時的に保持している基底値の総数Mに1を加算する。尚、この加算処理は、基底値及び基底値記録位置保持部(BV & BVL Retainer)720のみが行い、その結果を差分計算／基底値指示子決定部(DIF Calculator / BVP Determiner)721へ送信しても良い。
【０１２８】
[処理840]
１.差分計算／基底値指示子決定部(DIF Calculator / BVP Determiner)721は、現在処理対象となっている利用制御情報UCI_iの利用制御情報識別子(UCIID)402及びコンテンツデータ識別子(CID)406から、処理820.1或いは処理832.5で決定された差引値用変数SVVに含まれる同識別子の値を引き、差分DIF_iを求める。続いて、差分計算／基底値指示子決定部(DIF Calculator / BVP Determiner)721は、求めた差分DIF_i, 利用制御情報UCI_iに含まれる暗号関連演算情報(CI_i)404, 処理820.2或いは処理832.6で決定された基底値指示子BVPを、基底値及び暗号演算関連情報暗復号化部(BV & CI En/Decrypter)731に送信する。
【０１２９】
２.基底値及び暗号演算関連情報暗復号化部(BV & CI En/Decrypter)731は、受信した暗号関連演算情報(CI_i)404を、利用制御情報暗号化鍵K_QSを用いて暗号化し、暗号化された暗号演算関連情報E.CI_iを得る。
【０１３０】
３.基底値及び暗号演算関連情報暗復号化部(BV & CI En/Decrypter)731は、処理840.2で得た暗号化された暗号演算関連情報E.CI_iを、受信した残りの2つのデータと連結し、個別情報群（Individual Information）II_i = E.CI_i || DIF_i || BVP_iを保持する。
【０１３１】
４.N個の利用制御情報UCIを識別するための添え字変数iに1を加算する。
【０１３２】
[処理841]
処理840.4で得られたiの値とNを比較する。
【０１３３】
[処理850]
処理841における比較の結果、iの値がN以下であった場合には、利用制御情報UCI_iに対し処理810以降を実行する。一方で、iの値がNを超えた（即ちN+1）場合には、処理841.3で得られたN個の個別情報群II_iを、記憶装置インタフェース部220が受信したN個のDUCILが指し示す公開部PP（2231）内の領域に書き込む。
【０１３４】
以上の流れに沿って、特定の関係を有しコンテンツデータを各情報群間で共有することができる規定値と、個別情報群とに分け、規定値の部分を共用できるように、個別情報群に規定値を書き込んだ位置を付与して書き込むことにより、共用できる規定値の暗号化処

理が省略可能となる分、全てを暗号化して記録する場合に比べて記憶装置内で利用制御情報暗号化鍵K_QSを用いて利用制御情報を暗号化してから記録する場合の総処理量を、大幅に減らすことができるようになる。

【０１３５】

上記処理は、あくまで一例である。例えば、処理840.4における個別情報群II_iの書き込みは、iの値を1つ決める毎に、個別に行っても良い。制限アクセス領域制御部222内の機能ブロック構成も、あくまで一例である。図８に示した処理が適切に実行できるのであれば、異なった構成でも構わない。

【０１３６】

尚、図７には、幾つかの暗号化された基底値，暗号化された暗号関連演算情報，差分，基底値指示子が、秘匿部(VP)2230及び公開部(PP)2231に記録する態様（記録された結果）の一例を示してある。図７では、利用制御情報の記録先位置DUCIL_1（70050），DUCIL_2（70051），…，DUCIL_(r-1)（70052）に記録されている暗号化された暗号演算関連情報E.CI_1，E.CI_2，…，E.CI_(r-1)及び差分DIF_1，DIF_2，…，DIF_(r-1)は、値がBVL_1(70025)である基底値指示子BVPを伴っている（70040，70041，70042）。この態様により、暗号演算関連情報E.CI_1，E.CI_2，…，E.CI_(r-1)及び差分DIF_1，DIF_2，…，DIF_(r-1)は、秘匿部VP（2230）に記録されているE.BV_1（70020）と一体となることで、元の利用制御情報UCI_1，UCI_2，…，UCI_(r-1)を構成する。一方で、利用制御情報記録先位置DUCIL_r（70053），DUCIL_(r+1)（70054），…，DUCIL_N（70055）に記録されている暗号化された暗号演算関連情報E.CI_r，E.CI_(r+1)，…，E.CI_N及び差分DIF_r，DIF_(r+1)，…，DIF_Nは、値がBVL_2(70026)である基底値指示子BVPを伴っている（70043，70044，70045）。この態様により、暗号演算関連情報E.CI_r，E.CI_(r+1)，…，E.CI_N及び差分DIF_r，DIF_(r+1)，…，DIF_Nは、秘匿部(VP)2230に記録されているE.BV_2（70021）と一体となることで、元の利用制御情報UCI_r，UCI_(r+1)，…，UCI_Nを構成する。

【０１３７】

[記憶装置から記録再生装置への利用制御情報の読み出し処理]

図９は、記憶装置120から記録再生装置112への利用制御情報の転送処理の例を示す図である。なお、図６の場合と同様に、ホストセキュリティ管理部111と記憶装置セキュリティ管理部225との間では、*Kpu_[S](= *Kpr_[S])，ホスト装置m次セッション鍵(K_s[H]m)，記憶装置n次セッション鍵(K_s[S]n)が共有されているものとする。

【０１３８】

処理9000において、ホスト管理部110は、記憶装置保護情報転送機能部221に対して、記録再生装置112に送信予定のN個の利用制御情報UCI_1，…，UCI_Nを、制限アクセス領域223から記憶装置保護情報転送機能部221へ読み出して、転送処理の準備をするように要求する。

【０１３９】

このとき、ホスト管理部110は、送信予定のN個の利用制御情報UCI_1，…，UCI_Nが記憶されている制限アクセス領域223上の位置情報SUCILs（Source Location for UCIs）と、これら利用制御情報UCI_1，…，UCI_Nを特定するための利用制御情報識別子UCIIDとを送信する。なお、利用制御情報識別子UCIIDについては、必ずしも指定しなくてもよい。例えば、記憶装置120がATAインタフェースを伴った磁気ディスク装置であり、読み出し対象の利用制御情報UCI_1，…，UCI_Nが制限アクセス領域223内の連続した領域に記録されている場合は、最初の利用制御情報UCI_1が記録されている位置と、読み出す利用制御情報の数Nとを、読み出し命令に付随して記憶装置120に送信するパラメータの1つとして通知するのが効果的である。

【０１４０】

処理9001において、制限アクセス領域制御部222は、以下の処理を実行する。

【０１４１】

１.制限アクセス領域223から利用制御情報UCI_1，…，UCI_Nを読み出し、一時的に格納する。ここで、制限アクセス領域制御部222は、転送すべき利用制御情報UCI_1，…，UCI_

Nを一時的に格納する一時記憶部としても機能する。

【０１４２】

２.制限アクセス領域制御部222は、処理9001.1において一時的に保持した利用制御情報UCI_1, …, UCI_Nについて、利用制御情報記録状態UCISs（UCIs Status）を決定する。

【０１４３】

処理9030において、ホスト管理部110は、記憶装置セキュリティ管理部225に処理9001を実行させている間に、ホスト装置保護情報転送処理部104に対してセッション鍵データ生成要求を送信する。この時、読み出そうとする利用制御情報のうちの、最初の識別子UCIID_1（UCI_1に含まれるもの）を送信しておくと、後に受信した利用制御情報が意図したものであったかどうか確認する際に、有効である。

【０１４４】

処理9031において、ホスト装置保護情報転送機能部104は、以下の処理を実行する。

【０１４５】

１.セッション鍵K_s[H]m+1を生成する。

【０１４６】

２.生成したK_s[H]m+1を、K_s[H]m及びK_s[S]nで暗号化する。K_s[H]m及びK_s[S]nは、本処理を実行する時点で共有されている、ホスト装置保護情報転送機能部104及び記憶装置保護情報転送機能部221が過去に生成したセッション鍵のうちで最新のものである。

【０１４７】

処理9040において、ホスト装置保護情報転送処理部104は、生成された暗号化データE(K_s[S]n, E(K_s[H]m, K_s[H]m+1))を、記憶装置セキュリティ管理部225へ送信する。

【０１４８】

処理9041において、記憶装置保護情報転送機能部221は、以下の処理を実行する。

【０１４９】

１.受信した暗号化データE(K_s[S]n, E(K_s[H]m, K_s[H]m+1))を、自身が保持するK_s[S]n及びK_s[H]mを用いて復号する。

【０１５０】

２.処理9041.1で得られたK_s[H]m+1の完全性を確認する。

【０１５１】

処理9050において、ホスト管理部110は、利用制御情報UCI_1, …, UCI_Nを読み出す用途を、記憶装置120に通知する。ここでいう用途の例としては、例えば、記録再生装置112の再生機能部103でのコンテンツデータの復号および再生（Play）、他の記憶装置への利用制御情報UCIの複製（Copy）または移動（Move）等が挙げられる。

【０１５２】

処理9051において、記憶装置保護情報転送機能部221は、以下の処理を実行する。

【０１５３】

１.制限アクセス領域制御部222は、9001で準備したN個の利用制御情報UCI_1, …, UCI_Nから、記録再生装置112に実際に転送する転送用の利用制御情報UCI_1.TR, …, UCI_N.TRを生成する。この処理は、利用制御情報UCI_1, …, UCI_Nを制限アクセス領域制御部222内で複製した後、利用制御情報UCI_1.TR, …, UCI_N.TRに含まれる記憶装置セキュリティ管理部用利用規則UR_Sを処理9050で受信した命令に応じて変更することで達成される。

【０１５４】

２.制限アクセス領域制御部222は、処理9051.1で生成した転送用の利用制御情報UCI_1.TR, …, UCI_N.TRを、記憶装置保護情報転送機能部221に送信する。記憶装置保護情報転送機能部221は、受信した転送用の利用制御情報UCI_1.TR, …, UCI_N.TRに、処理9050で受信した命令を特定する動作特定情報（Action Specifier: AS）を連結し、得られたUCI_1.TR || … || UCI_N.TR || ASを、処理9041.2で得たK_s[H]m+1及び認証処理において共有した*Kpu_[H]を用いて暗号化する。

【０１５５】

３.制限アクセス領域制御部222は、自身が保持する利用制御情報UCI_1, …, UCI_Nの記

憶装置セキュリティ管理部用利用規則UR_S 303（UR_S1, …, UR_SN））、を処理9050で受信した命令に従って変更する。

【０１５６】

４.制限アクセス領域制御部222は、処理9051.3において記憶装置セキュリティ管理部用利用規則UR_S 303を変更したN個の利用制御情報UCI_1, …, UCI_Nを、位置情報SUCIL_1, …, SUCIL_Nが指し示す利用制御情報が元来記録されていた制限アクセス領域223内領域へ書き戻す。この時、制限アクセス領域制御部222が保持している利用制御情報UCI_1, …, UCI_Nは、無効化せずに保持し続けても構わない。尚、処理9050で受信した命令が移動（Move）であった場合、制限アクセス領域制御部222は、位置情報SUCIL_1, …, SUCIL_Nが指し示す制限アクセス領域223上の利用制御情報及び制限アクセス領域制御部222が保持している利用制御情報を、記憶装置保護情報転送機能部221から転送用利用制御情報を出力する前に無効化する。

【０１５７】

処理9060において、記憶装置保護情報転送機能部221は、処理9051.2において生成された暗号化データE(*Kpu_[H], E(K_s[H]m+1, UCI_1.TR || … || UCI_1.TR || AS))を、ホストセキュリティ管理部111へ送信する。

【０１５８】

処理9061において、ホスト装置保護情報転送機能部104は、以下の処理を実行する。

【０１５９】

１.受信した暗号化データE(*Kpu_[H], E(K_s[H]m+1, UCI_1.TR || … || UCI_1.TR || AS))を、自身が保持する*Kpr_[H]及びK_s[H]m+1を用いて復号する。

【０１６０】

２.得られたUCI_1.TR || … || UCI_1.TR || ASの完全性を確認する。

【０１６１】

３.再生機能部103は、動作特定情報ASに従った所定の処理を実行する。

【０１６２】

以下では、処理9001において、制限アクセス領域制御部222が制限アクセス領域223に記録されている利用制御情報を読み出す処理を、図１０及び図１１を用いて詳細に説明する。制限アクセス領域制御部222が制限アクセス領域223に記録されている利用制御情報を読み出す処理は、制限アクセス領域制御部222及び制限アクセス領域223にとっては、図７及び図８を用いて説明した利用制御情報の書き込み処理6031.3に対する逆向きの処理である。図１０はこの処理の流れを実現するモジュール構成及び記録されているN個の利用制御情報を、記憶装置保護情報転送機能部221から実際に出力するまでの手段を示したものである。

【０１６３】

[利用制御情報読み出し処理のための記憶装置セキュリティ管理部内構成要素]

利用制御情報読み出し処理における記憶装置セキュリティ管理部内の詳細動作を説明する際に、記憶装置セキュリティ管理部の構成要素の役割についての詳細な説明も与えるが、本段でも図１０を用いて概要を簡単に記しておく。

【０１６４】

利用制御情報の読み出し処理を実行する際に、記憶装置セキュリティ管理部は、書き込み処理時に用いた基底値及び基底値記録位置保持部(BV & BVL Retainer)720, 基底値及び暗号演算関連情報暗復号化部（BV & CI En/Decrypter）731の他に、利用制御構成部（UCI Constructor）1021を構成要素として持つ必要がある。

【０１６５】

[利用制御情報読み出し処理における記憶装置セキュリティ管理部内動作]

利用制御情報の読み出し処理についても、書き込み処理で用いた添え字等の表記法をそのまま踏襲して説明する。以下では、記憶装置セキュリティ管理部内での読み出し処理を詳細に説明する。但し、この読み出し処理を実行する時点に於いて、基底値及び基底値記録位置保持部（BV & BVL Retainer）720は、書き込み処理時と同様に、M個の（基底値,

基底値記録位置）の組（(BV_1, BVL_1), …, (BV_M, BV_M)）を、一時的に保持していることを仮定する。

【０１６６】

以下、図１１を用いて制限アクセス領域制御部222における処理の流れを説明する。

【０１６７】

[処理1100]

復号処理以前（同時並列処理でも良い）に、制限アクセス領域制御部222内の基底値及び暗号演算関連情報暗復号化部731（BV & CI En/Decrypter）は、利用制御情報暗号化鍵K_QSを決定（複数のK_QSを用いている場合は、適切なものを選択）する。

【０１６８】

[処理1101]

記憶装置インタフェース部220が受信したN個の記録元位置情報SUCIL_1, …, SUCIL_Nが指し示す公開部(PP)2231内の領域から、N個の個別情報群D_1, …, D_Nを一括して基底値及び暗号演算関連情報暗復号化部(BV & CI En/Decrypter)731に読み出す。但し、この読み出し処理は、1つずつ或いは数個ずつ行っても良い。尚、既存の多くの記憶装置は、記録媒体上へデータを実際に書き込む或いは記録媒体上からデータを読み出す場合、ある程度の量を一括して目的の処理を実行することを仮定し、説明を続ける。

【０１６９】

[処理1110]

１.利用制御情報構築部（UCI Constructor）1021に於いて、読み出したN個の連結データDを識別するための添え字変数iに、1を設定する。

【０１７０】

[処理1111]

１.基底値及び暗号演算関連情報暗復号化部(BV & CI En/Decrypter)731は、読み出した個別情報群II_iに含まれる暗号関連演算情報E.CI_iを復号化し、暗号演算関連情報CI_iを得る。

【０１７１】

２.利用制御情報構築部(UCI Constructor)1021に於いて、基底値及び基底値記録位置保持部(BV & BVL Retainer)720から読み出す基底値BV及び基底値記録位置BVLを識別するための添え字変数jに、1を設定する。

【０１７２】

[処理1120]

１.利用制御情報構築部(UCI Constructor)1021は、基底値及び基底値記録位置保持部(BV & BVL Retainer)720に保持されている基底値BV[*]_j（ここではj = 1）及びこの基底値BVL_jと組を構成している基底値記録位置BVL[*]_jを読み出す。

【０１７３】

２.処理1101において公開部PP（2231）から読み出した個別情報群II_iに含まれる基底値指示子BVP_iと、処理1120 (1)で得た基底値記録位置BVL[*]_jとを比較する。

【０１７４】

[処理1121]

処理1120.2における比較の結果、双方の値が一致すれば、処理1120を実行する。一致しなかった場合は、処理1140を実行する。以下では、先ず処理1130から始まる手続きについて説明し、その後1140から始まる処理について説明する。

【０１７５】

[処理1130]

基底値用変数（Variable for BV; BVVと記す）に、処理1121において一致した基底値記録位置BVL[*]_jと組を構成している基底値BV[*]_jの値を設定する。

【０１７６】

[処理1140]

添え字jの値に1を加算する。

【０１７７】
[処理1141]
処理1140において得られたjの値が、その時点で基底値及び基底値記録位置保持部(BV & BVL Retainer)720が保持している基底値BVの総数Mより大きいか否かを判定する。もしjの値がM以下であった場合は、処理1120へ戻る。一方で、jの値がMを超えていた（即ちj=M+1）場合は、処理1142を実行する。
【０１７８】
[処理1142]
１.利用制御情報構築部(UCI Constructor)1021は、基底値記録位置BVP_iが指し示す秘匿部(VP)2230内領域から基底値及び暗号演算関連情報暗復号化部(BV & CI En/Decrypter)731に、暗号化された基底値E.BV[*]_jを新たに読み出すよう指示する。
【０１７９】
２.基底値及び暗号演算関連情報暗復号化部(BV & CI En/Decrypter)731は、処理1142.1で読み出した暗号化された基底値E.BV[*]_jを、処理1100に於いて選択した利用制御情報暗号化鍵K_QSを用いて復号し、基底値BV[*]_jを得る。
【０１８０】
３.処理1142.2で得た基底値BV[*]_jを基底値用変数BVVに設定する。
【０１８１】
４.基底値及び基底値記録位置保持部(BV & BVL Retainer)720及び利用制御情報構築部(UCI Constructor)1021は、一時的に保持している基底値の総数Mに1を加算する。尚、この加算処理は、基底値及び基底値記録位置保持部(BV & BVL Retainer)720のみが行い、その結果を利用制御情報構築部(UCI Constructor)1021へ送信しても良い。
【０１８２】
[処理1150]
１.利用制御情報構築部(UCI Constructor)1021は、基底値用変数BVV, 処理1111.1で得た暗号関連演算情報CI_i, 識別子の差分値から、正規の利用制御情報を再構築する。例えば利用制御情報識別子(UCIID)402及びコンテンツデータ識別子(CID)406については、基底値用変数BVVに含まれている利用制御情報識別子UCIID及びコンテンツデータ識別子CIDの値に差分値を加算し、それぞれの正しい値を得る。また2種の利用規則（403, 405）、基底値に含まれている値をそのまま当てはめる。暗号関連演算情報については、処理1111.1で得たものを当てはめる。
【０１８３】
２.添え字iの値に1を加算する。
【０１８４】
[処理1151]
処理1150.2で得られたiの値とNを比較する。
【０１８５】
[処理1150]
処理1151における比較の結果、iの値がN以下であった場合には、処理1111以降を再実行する。一方で、iの値がNを超えた（即ちN+1）場合には、ホスト装置保護情報転送機能部104に対して構築した利用制御情報の送信処理9041を実行する。
【０１８６】
尚、図１０に示した制限アクセス領域223内の態様（暗号化された基底値や暗号関連演算情報、差分、基底値指示子等が記録されている状態）は、図７と同じである。
【０１８７】
ところで、図２等では、同一の記憶媒体内に、秘匿部(VP)2230として用いる領域と公開部(PP)2231として用いる領域領域とを備えた例を示したが、異なる特性を持つ別の種類の記憶媒体上にそれぞれの領域を備えても良い。具体的には、基底値BVを記録するために秘匿部(VP)2230として設けるべき容量は、公開部(PP)2231と比べて、通常遥かに少量である。このため、公開部(PP)2231を磁気ディスク円盤上に論理的に構成する一方で、高価では

あるがアクセス特性が磁気ディスク円盤と異なる半導体等の記憶媒体を記憶装置内に搭載し、その媒体上に秘匿部(VP)2230を設けるようにすると、基底値BVの書き込みや読み出しに際してヘッドのシークや磁気ディスク円盤の回転待ちを行わずに済むようになる。そのため、書き込みや読み出し時間の更なる短縮を図ることができるという効果が得られる。

【実施例２】

【０１８８】

図６に示した利用制御情報書き込み処理6031.3（利用制御情報書き込み処理における記憶装置セキュリティ管理部内動作）及びそれに対応する利用制御情報読み出し処理9001.1（利用制御情報の記憶装置セキュリティ管理部内動作）に関する別の実現手段を適用した実施例を、図１２，図１３，図１４，図１５を用いて説明する。

【０１８９】

[利用制御情報書き込み処理のための記憶装置セキュリティ管理部内構成要素]

本実施例で説明する記憶装置セキュリティ管理部の構成を図１２に示すが、図から明らかなように、多くの点で実施例１において図７に示したものと同一である。異なる点は、制限アクセス領域223が、秘匿部と公開部のような性質がアクセス制限上の特性が異なる複数の部分からなるでのはなく、全てが公開部としての性質を有するものであることである。

【０１９０】

[利用制御情報書き込み処理における記憶装置セキュリティ管理部内動作]

本実施例においても、実施例１に記した4つの仮定をそのまま前提とする。

【０１９１】

この前提に基づく制限アクセス領域への利用制御情報の書き込み処理は、図８に示した流れと多くの点で同じであるが、制限アクセス領域の構成が異なることに起因する、幾つかの相違点がある。以下では、相違点に焦点を絞り、説明する。

【０１９２】

[処理1320]

１.処理820.1と同じである。

【０１９３】

２.処理820.2と同じである。

【０１９４】

３.基底値用変数（Variable for BV; BVV）に、0等の任意の無効な値を設定する。基底値用変数（Variable for BV; BVV）は、差分計算／基底値指示子決定部(DIF Calculator / BVP Determiner)721が管理する変数である。

【０１９５】

[処理1332]

１.処理832.1同様に、受信した利用制御情報UCI_iが含むCI以外のデータから、基底値BVを生成すると共に、基底値BVの記録先位置BVLを決定する。ここで基底値記録先位置BVLとしては、受信した利用制御情報記録先位置DUCIL_iを設定する。

【０１９６】

２.処理832.2と同じである。

【０１９７】

３.基底値用変数BVVに、処理1332.2で得た暗号化された基底値E.BV[L+1]_jを設定する。基底値用変数は、差分計算／基底値指示子決定部(DIF Calculator / BVP Determiner)721が管理する変数である。

【０１９８】

４.処理832.4と同じである。

【０１９９】

５.処理832.5と同じである。

【０２００】

６.処理832.6と同じである。

【０２０１】
７.処理832.7と同じである。
【０２０２】
８.処理832.8と同じである。
【０２０３】
[処理1340]
１.処理840.1と同じである。
【０２０４】
２.処理840.2と同じである。
【０２０５】
３.基底値及び暗号演算関連情報暗復号化部(BV & CI En/Decrypter)731は、処理1320.3もしくは処理1332.3で設定した基底値変数BV、処理1340.2で得た暗号化された暗号演算関連情報E.CI_i、受信した残りの2つのデータと連結し、個別情報群II_i = BVV || E.CI_i || DIF_i || BVP_iを保持する。
【０２０６】
４.処理840.4と同じである。
【０２０７】
以上の流れに沿って利用制御情報の書き込み処理を実行した場合にも、記憶装置内で利用制御情報暗号化鍵K_QSを用いて利用制御情報を暗号化してから記録する場合の総処理量を、大幅に減らすことができるようになる。
【０２０８】
尚、図１２には、幾つかの暗号化された基底値，暗号化された暗号関連演算情報，差分，基底値指示子が、制限アクセス領域223に記録されている態様の一例を示してある。この図では、利用制御情報の記録先位置DUCIL_1（120030），DUCIL_2（120031），…，DUCIL_(r-1)（120032）に記録されている暗号化された暗号演算関連情報E.CI_1，E.CI_2，…，E.CI_(r-1)及び差分DIF_1，DIF_2，…，DIF_(r-1)は、値がDUCIL_1である基底値指示子BVPを伴っている（120040，120041，120042）。図１２に示す態様により、暗号演算関連情報E.CI_1，E.CI_2，…，E.CI_(r-1)及び差分DIF_1，DIF_2，…，DIF_(r-1)は、BV_1（120020）と一体となることで元の利用制御情報UCI_1，UCI_2，…，UCI_(r-1)を構成する態様となっている。一方で、利用制御情報記録先位置DUCIL_r（120033），DUCIL_(r+1)（120034），…，DUCIL_N（120035）に記録されている暗号化された暗号演算関連情報E.CI_r，E.CI_(r+1)，…，E.CI_N及び差分DIF_r，DIF_(r+1)，…，DIF_Nは、値がBVL_2(120023)である基底値指示子BVPを伴っている（120043，120044，120045）。この態様により、暗号演算関連情報E.CI_r，E.CI_(r+1)，…，E.CI_N及び差分DIF_r，DIF_(r+1)，…，DIF_Nは、BV_2（120023）と一体となることで元の利用制御情報UCI_r，UCI_(r+1)，…，UCI_Nを構成する。
【０２０９】
[利用制御情報読み出し処理のための記憶装置セキュリティ管理部内構成要素]
本実施例で説明する記憶装置セキュリティ管理部の構成を図１４に示すが、図１２同様に、制限アクセス領域223が、秘匿部と公開部のような性質がアクセス制限上の特性が異なる複数の部分からなるのではなく、全てが公開部としての性質を有するものであること以外、実施例１において図１０に示したものと同一である。
【０２１０】
[記憶装置から記録再生装置への利用制御情報の読み出し処理]
図１５を用いて、本実施例の記憶装置セキュリティ管理部内での利用制御情報の読み出し処理の流れを説明する。本実施例の制限アクセス領域からの利用制御情報の読み出し処理は、図１１に示した実施例１の流れと多くの点で同じであるが、基底値(BV)を記録する先が制限アクセス領域であることに起因する相違点が1つある。それは、処理1542.1に記述されている部分である。即ち、基底値記録位置BVP_iは、制限アクセス記憶部内の一領域を指し示しているため、暗号化された基底値E.BV[*]_jは制限アクセス記憶部内の領域

から読み出される。

【０２１１】

尚、図１４に示した制限アクセス領域223内の態様（暗号化された基底値や暗号関連演算情報、差分、基底値指示子等が記録されている状態）は、図１２と同じである。

【０２１２】

ところで、以上に説明したように、基底値と個別情報群をホスト装置が指定する位置上に配置すると、異なる媒体に基底値と個別情報群を記録する場合に比べ、書き込み処理に失敗した場合にデータの矛盾を起こさないようにするための復旧処理を簡素化できるという効果が得られる。

【０２１３】

以上２つの実施形態によって、ホスト装置は記憶装置の内部構成によって、利用制御情報の書き込み先や書き込み処理に付随して必要な暗号化等の処理を変えることなく、他の記憶装置同様に書き込み処理を実行することができ、且つ記憶装置における情報書き込み処理時間の短縮化を実現することができる。処理時間の短縮化は、読み出し処理においても同様に図ることができる。

【０２１４】

以上、本発明の２つの実施形態について説明したが、本発明は上記実施形態に限定されるものではなく、種々の変形実施が当業者にとって可能であるのはもちろんである。

【図面の簡単な説明】

【０２１５】

【図１】本発明の一実施形態に係るデータ転送システムの構成を表すブロック図である。

【図２】記憶装置の構成例を表すブロック図である。

【図３】データ転送システムの変形例を表すブロック図である。

【図４】利用制御情報の内容例を示す図である。

【図５】利用制御情報の転送処理に先立って実行される認証処理の例を示す図である。

【図６】書き込みを目的とした、コンテンツ記録再生装置から記憶装置へ利用制御情報の転送処理の例を示す図である。

【図７】第１実施例における利用制御情報の書き込み処理を実現する、記憶装置内の中の記憶装置セキュリティ管理部の構成を示す図である。

【図８】第１実施例における、記憶装置セキュリティ管理部内での利用制御情報の書き込み処理の流れを示す図である。

【図９】読み出しを目的とした、記憶装置からコンテンツ記録再生装置へ利用制御情報の転送処理の例を示す図である。

【図１０】第１実施例における利用制御情報の読み出し処理を実現する、記憶装置内の中の記憶装置セキュリティ管理部の構成を示す図である。

【図１１】第１実施例における、記憶装置セキュリティ管理部内での利用制御情報の読み出し処理の流れを示す図である。

【図１２】第２実施例における利用制御情報の書き込み処理を実現する、記憶装置内の中の記憶装置セキュリティ管理部の構成を示す図である。

【図１３】第２実施例における、記憶装置セキュリティ管理部内での利用制御情報の書き込み処理の流れを示す図である。

【図１４】第２実施例における利用制御情報の読み出し処理を実現する、記憶装置内の中の記憶装置セキュリティ管理部の構成を示す図である。

【図１５】第２実施例における、記憶装置セキュリティ管理部内での利用制御情報の読み出し処理の流れを示す図である。

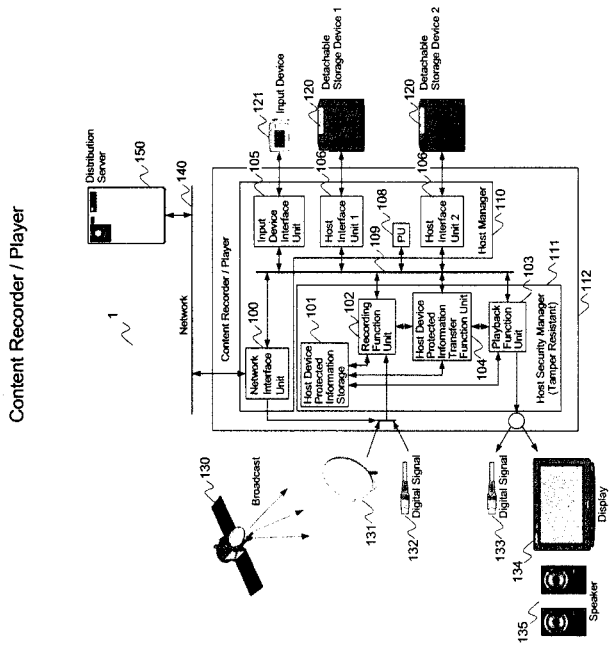
【符号の説明】

【０２１６】

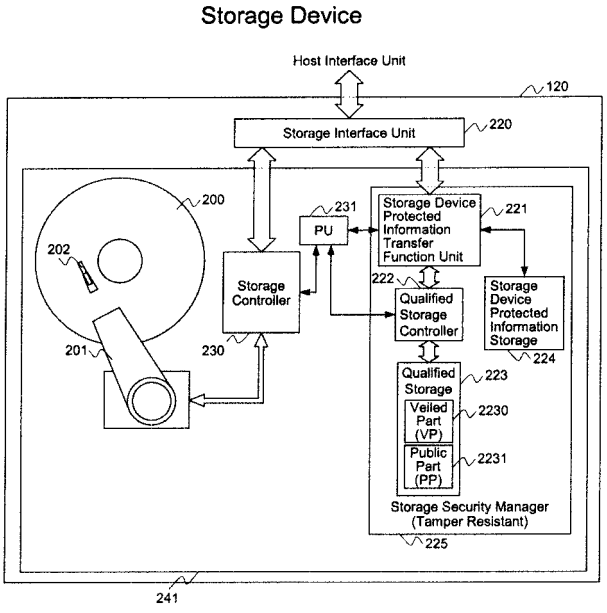
１００…ネットワークインタフェース部（Network Interface Unit）、101…ホスト装置保護情報記録部（Host Device Protected Information Storage）、102…記録機能部（Recording Function Unit）、103…再生機能部（Playback Function Unit）、104…ホスト

装置保護情報転送処理部（Host Device Protected Information Transfer function Unit）、105…入力装置インタフェース部（Input Device Interface Unit）、106…ホストインタフェース部（Host Interface Unit）、108…プロセッサ部（Processor Unit: PU）、110…ホスト管理部（Host Manager）、111　ホストセキュリティ管理部（Host Security Manager）、112…コンテンツ記録再生装置（Content Recorder/Player：記録再生装置）、120…記憶装置（Detachable Storage Device）、121…入力装置（Input Device）、130…放送波配信元、131…放送波受信アンテナ、132…デジタル信号端子、133…デジタル信号端子、134…ディスプレイ、135…スピーカー、140…ネットワーク、150…配信サーバ、200…磁気記録媒体、201…アーム、202…ヘッド、220…記憶装置インタフェース部（Storage Interface Unit）、221…記憶装置保護情報転送機能部（Storage Device Protected Information Transfer Function Unit）、222…制限アクセス領域制御部（Qualified Storage Controller）、223…制限アクセス領域（Qualified Storage）、224…記憶装置保護情報記録部（Storage Device Protected Information Storage）、225…記憶装置セキュリティ管理部（Storage Security Manager）、230…記憶装置制御部（Storage Controller）、231…プロセッサ部（Processor Unit: PU）、240…可搬型記憶装置（Detachable Storage Device：記憶装置）、4000…コンテンツ記録再生装置、4010…データ転送用ホスト装置（Host Device for Data Transfer）、4020…記憶装置（Storage Device）、5000…データ転送用ホスト装置（Host Device for Data Transfer）、5010, 5020…記憶装置（Storage Device）。

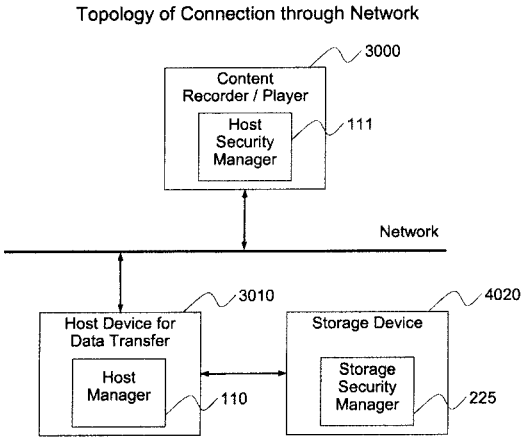
【図１】



【図２】



【図３】

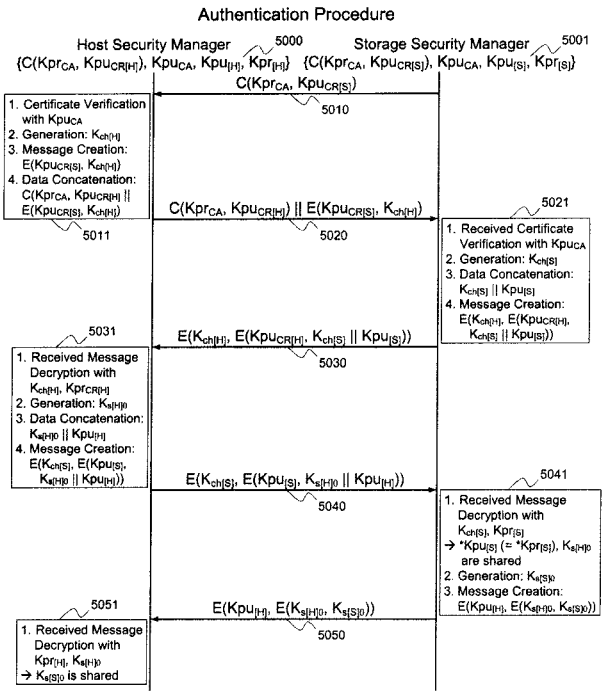


【図４】

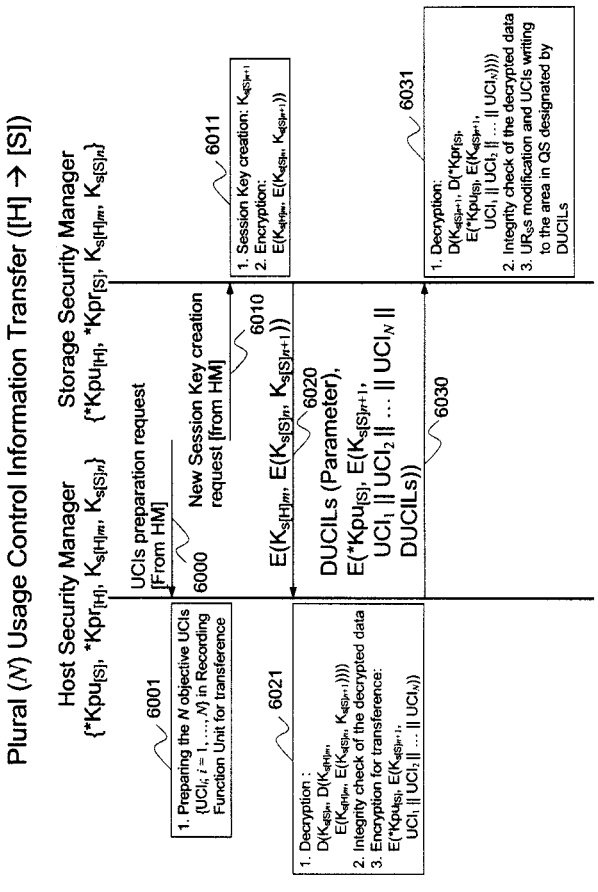
Usage Control Information

Information	Abbreviation	
Corresponding Service Type Specifier	CSTS	401
Usage Control Information Identifier	UCIID	402
Usage Rule enforced in Storage Security Manager (Ex. Allowed Copy Number, Allowed Playback Number)	UR_S	403
Cipher Information (including Content Key)	CI	404
Usage Rule enforced in Playback Function Unit (Ex. Export Control Information)	UR_P	405
Content Identifier	CID	406
Other Information	OI	407

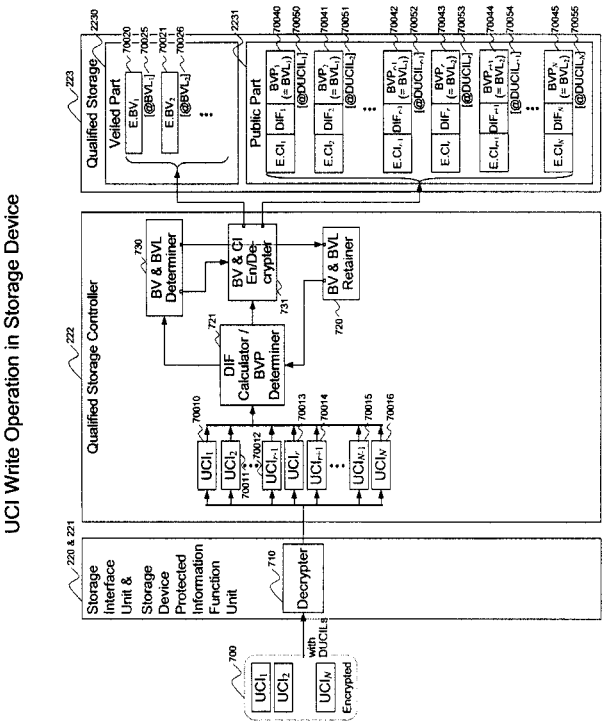
【図５】



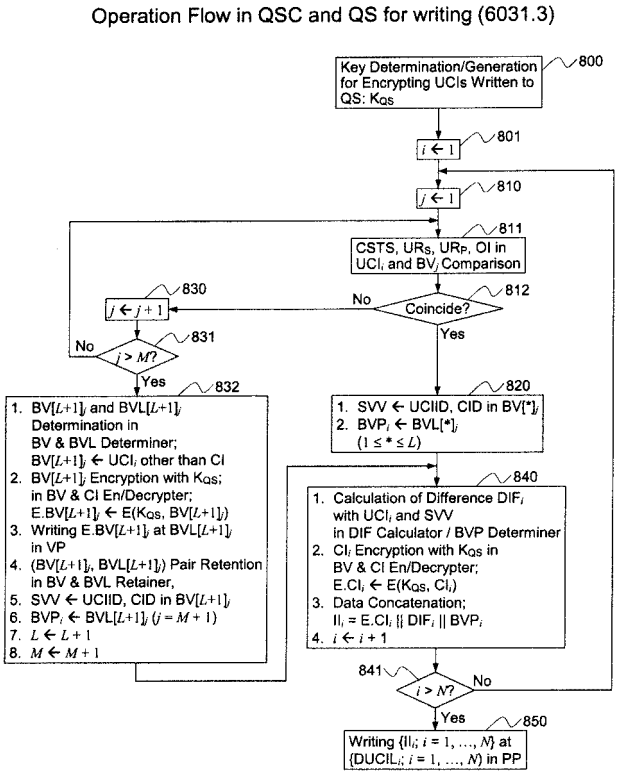
【図６】



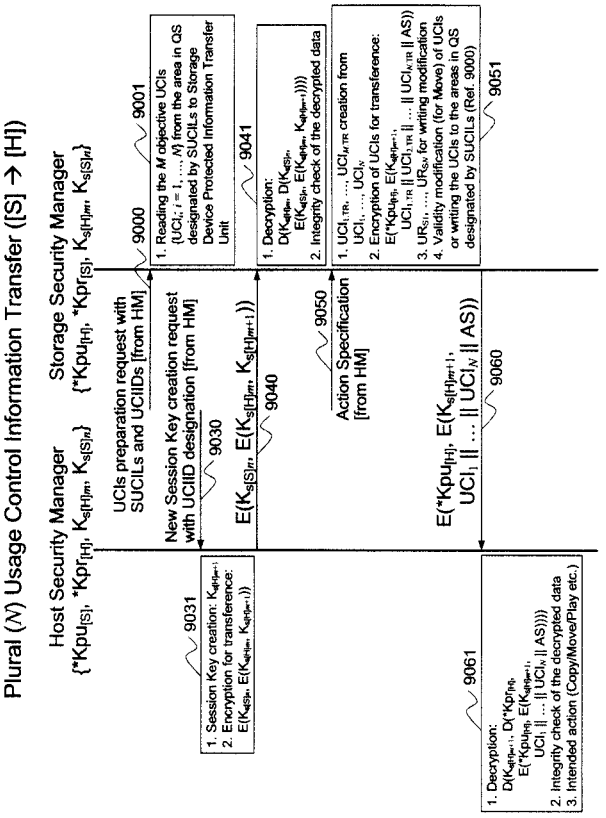
【図７】


UCI Write Operation in Storage Device
Qualified Storage
Veiled Part
Public Part
Qualified Storage Controller
BV & BVL Determiner
BV & CI En/De-crypter
BV & BVL Retainer
DIF Calculator / BVP Determiner
Storage Interface Unit & Storage Device Protected Information Function Unit
Decrypter
Encrypted

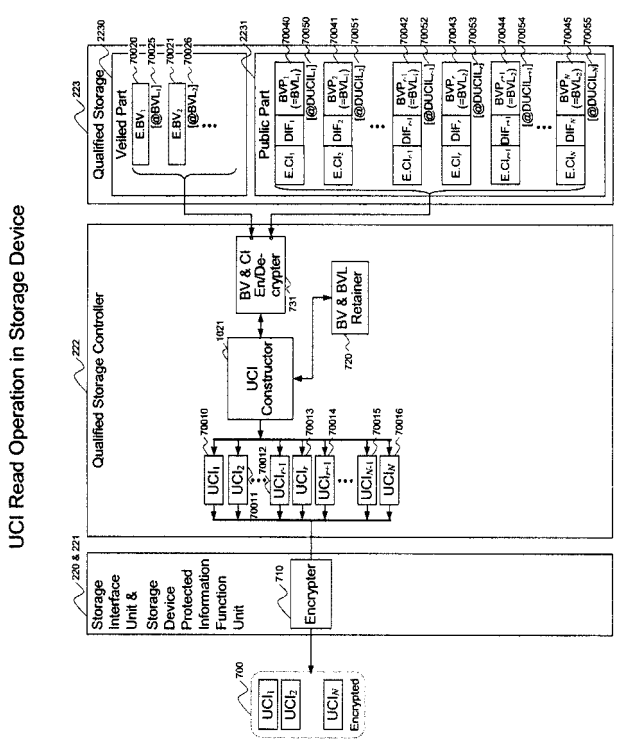
【図８】


Operation Flow in QSC and QS for writing (6031.3)
Key Determination/Generation for Encrypting UCIs Written to QS: KQS
CSTS, URS, URP, OI in UCI, and BV Comparison
Coincide?
No
Yes
SVV ← UCIID, CID in BV[*]1
BVPi ← BVL[*]i
Calculation of Difference DIFi with UCIi and SVV in DIF Calculator / BVP Determiner
CIi Encryption with KQS in BV & CI En/Decrypter; E.CIi ← E(KQS, CIi)
Data Concatenation; IIi = E.CIi || DIFi || BVPi
i ← i + 1
i > N?
Writing {IIi; i = 1, ..., N} at {DUCILi; i = 1, ..., N} in PP

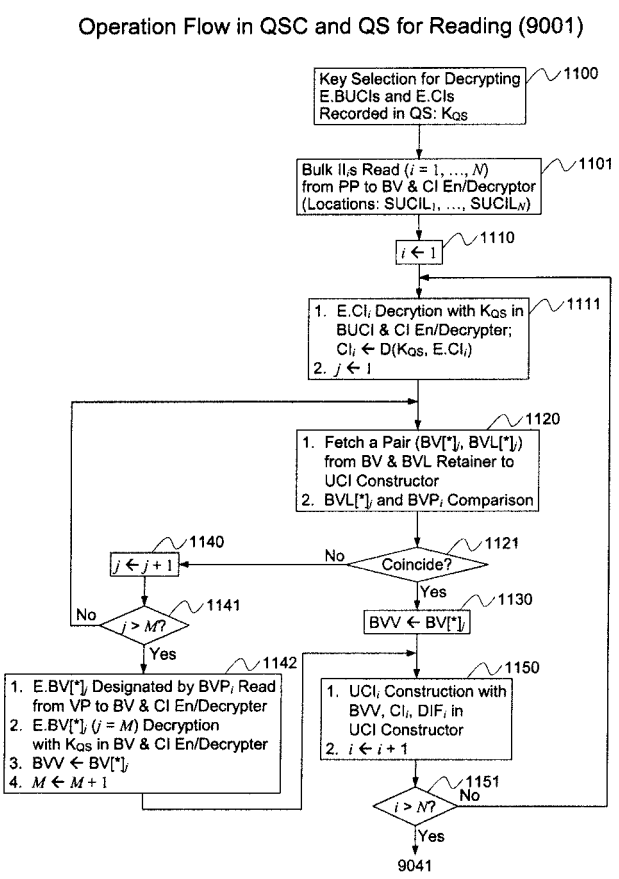
【図９】


Plural (N) Usage Control Information Transfer ([S] → [H])
Host Security Manager
Storage Security Manager
UCIs preparation request with SUCILs and UCIIDs [from HM]
New Session Key creation request with UCIID designation [from HM]
Action Specification [from HM]
Reading the M objective UCIs from the area in QS designated by SUCILs to Storage Device Protected Information Transfer Unit
Session Key creation
Encryption for transference
Decryption
Integrity check of the decrypted data
Intended action (Copy/Move/Play etc.)

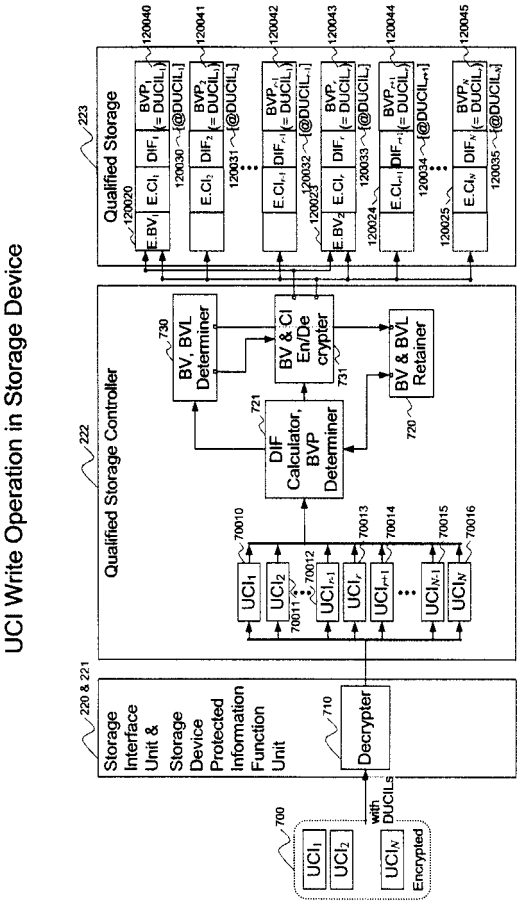
【図１０】


UCI Read Operation in Storage Device
Qualified Storage
Veiled Part
Public Part
Qualified Storage Controller
BV & CI En/De-crypter
UCI Constructor
BV & BVL Retainer
Storage Interface Unit & Storage Device Protected Information Function Unit
Encrypter
Encrypted

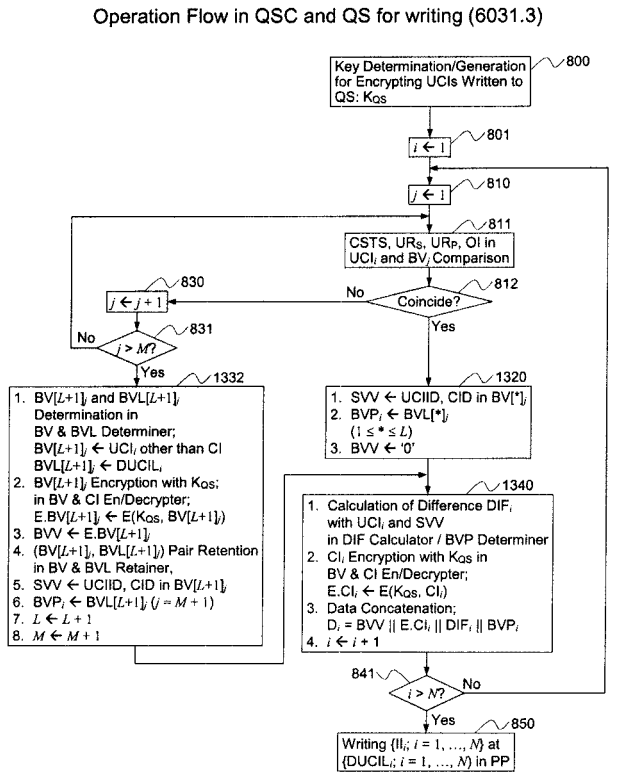
【図１１】



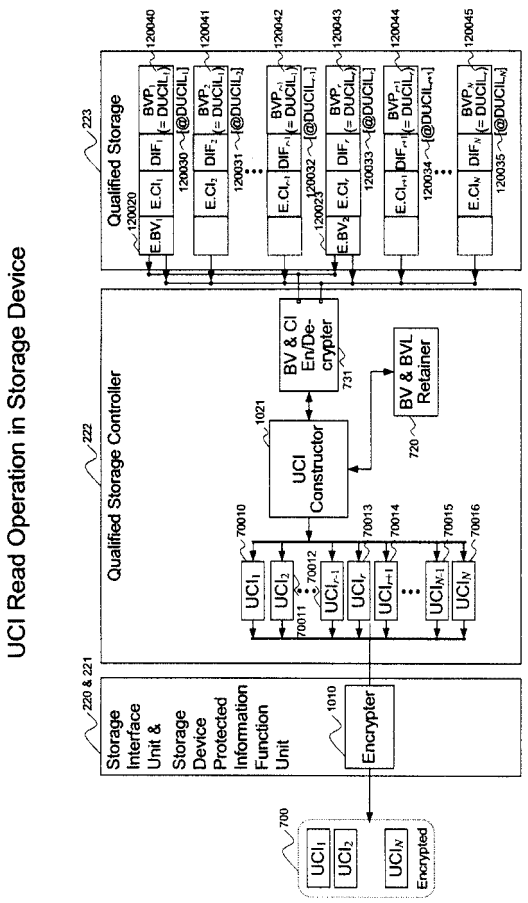
【図１２】



【図１３】

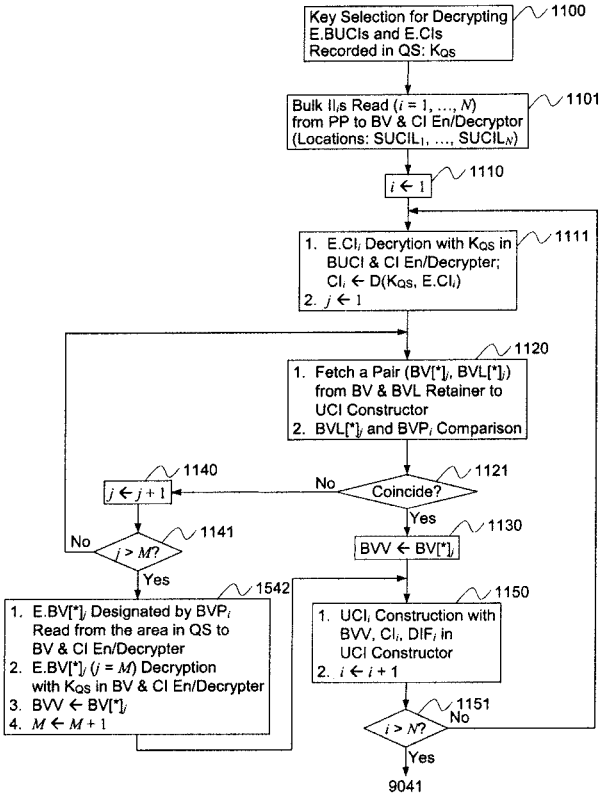


【図１４】



【図１５】

Operation Flow in QSC and QS for Reading (9001)



フロントページの続き

(51)Int.Cl.	F I		テーマコード（参考）
	Ｇ１１Ｂ 20/10	Ｄ	
	Ｈ０４Ｌ 9/00	６７５Ｂ	
	Ｈ０４Ｌ 9/00	６０１Ｂ	

Ｆターム(参考) 5J104 AA08 AA09 AA12 AA16 AA32 EA04 EA08 EA18 EA19 JA03
JA21 LA05 LA06 NA02 NA12 NA27 NA36 NA37 PA07 PA14