

(19) 世界知的所有権機関
国際事務局(43) 国際公開日
2006年9月21日 (21.09.2006)

PCT

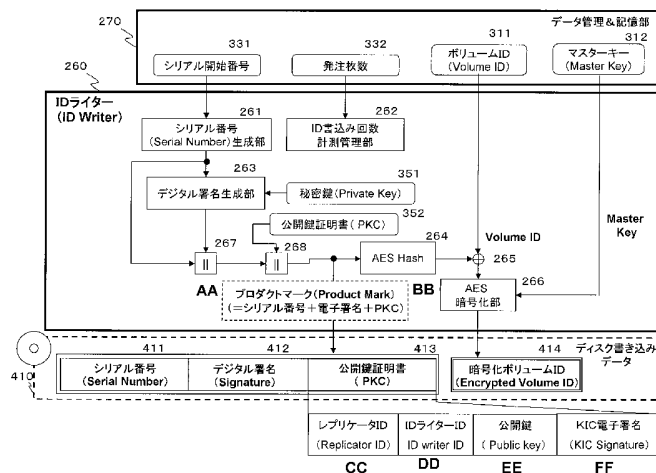
(10) 国際公開番号
WO 2006/098151 A1

- (51) 国際特許分類:
G11B 7/007 (2006.01) **G06F 21/24** (2006.01)
G11B 7/0045 (2006.01) **G09C 1/00** (2006.01)
G11B 20/10 (2006.01) **H04L 9/32** (2006.01)
G11B 20/12 (2006.01)
- (21) 国際出願番号: PCT/JP2006/303843
- (22) 国際出願日: 2006年3月1日 (01.03.2006)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
 特願2005-072351 2005年3月15日 (15.03.2005) JP
- (71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒1410001 東京都品川区北品川6丁目7番35号 Tokyo (JP).
- (72) 発明者; および
- (75) 発明者/出願人 (米国についてののみ): 木谷 聡 (KITANI, Satoshi) [JP/JP]; 〒1410001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo (JP). 小林 誠司 (KOBAYASHI, Seiji) [JP/JP]; 〒1410001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo (JP).
- (74) 代理人: 宮田 正昭, 外 (MIYATA, Masaaki et al.); 〒1040041 東京都中央区新富一丁目1番7号 銀座ティークイビル 澤田・宮田・山田特許事務所 Tokyo (JP).
- (81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR,

/ 続葉有 /

(54) Title: DISC MANUFACTURING METHOD, DATA RECORDING DEVICE, INFORMATION RECORDING MEDIUM, INFORMATION PROCESSING DEVICE AND METHOD, AND COMPUTER PROGRAM

(54) 発明の名称: ディスク製造方法、データ記録装置、情報記録媒体、情報処理装置および方法、並びにコンピュータ・プログラム



- | | |
|---|----------------------------|
| 331 SERIAL START NUMBER | BB AES ENCRYPTION UNIT |
| 332 NUMBER OF DISCS ORDERED | 411 SERIAL NUMBER |
| 311 VOLUME ID | 412 DIGITAL SIGNATURE |
| 312 MASTER KEY | 413 PUBLIC KEY CERTIFICATE |
| 260 ID WRITER | 414 ENCRYPTED VOLUME ID |
| 261 SERIAL NUMBER GENERATION UNIT | 410 DATA WRITTEN ONTO DISC |
| 262 ID WRITE NUMBER MEASUREMENT/MANAGEMENT UNIT | CC REPLICATOR ID |
| 263 DIGITAL SIGNATURE GENERATION UNIT | DD ID WRITER ID |
| 351 PRIVATE KEY | EE PUBLIC KEY |
| 352 PUBLIC KEY CERTIFICATE | FF KIC DIGITAL SIGNATURE |
| AA PRODUCT MARK (= SERIAL NUMBER + DIGITAL SIGNATURE + PKC) | |

(57) Abstract: A disc manufacturing method generates an encryption volume ID calculated according to a product mark containing a public key certificate issued to a disc manufacturing entity or a disc manufacturing device, a product mark corresponding value such as a Hash value generated according to the product mark, and a volume ID as an identifier set for a certain set of the manufactured discs and records the product mark and the encryption volume ID as information for generating a decoding key for the encrypted content on the disc by the reflection film removal recording method. With this configuration, it is impossible to read a product mark or an encryption volume ID as key generation information from a pirated disc onto which a pit shape is physically copied according to an authorized disc on market, thereby preventing unauthorized reproduction or use of a content.

(57) 要約: ディスク製造エンティティ、またはディスク製造機器に対して発行された公開鍵証明書を含むプロダクトマークと、プロダクトマークに基づいて生成されるハッシュ値などのプロダクトマーク

に対応値と、製造ディスクの一定の集合に対して設定される識別子としてのボリュームIDとに基づく演算によって算出される暗号化ボリュームIDを生成し、これらのプロダクトマークおよび暗号化ボリュームIDを暗号化コンテンツの復号用鍵の生成情報とし、反射膜除去記録方式によってディスクに記録する。本構成により、市販の正当なディスクに基づいて、ピット形状を物理的にコピーした海賊版ディスクからは、鍵生成情報としてのプロダクトマークまたは暗号化ボリュームIDを読み取ることができず、コンテンツの不正な再生や利用を防止することができる。



LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX,
MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU,
SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT,
TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR),
OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML,
MR, NE, SN, TD, TG).

- (84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE,

添付公開書類:

— 国際調査報告書

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

明 細 書

ディスク製造方法、データ記録装置、情報記録媒体、情報処理装置および方法、並びにコンピュータ・プログラム

技術分野

[0001] 本発明は、ディスク製造方法、データ記録装置、情報記録媒体、情報処理装置および方法、並びにコンピュータ・プログラムに関する。さらに、詳細には、海賊版ディスクによるコンテンツの不正利用の防止や海賊版ディスクの製造元追跡を可能とするディスク製造方法、データ記録装置、情報記録媒体、情報処理装置および方法、並びにコンピュータ・プログラムに関する。

背景技術

[0002] 近年、DVD(Digital Versatile Disc)や、BD[青色レーザーディスク:Blu-ray Disc(商標)]など、大容量データを格納可能な情報記録媒体が普及してきている。これらの大容量ディスクには、例えば高精細度画像データなどのデジタルデータが記録される。

[0003] デジタルデータは、画像や音声を劣化させることなく記録、再生を繰り返すことが可能であり、不正コピーされたコンテンツのインターネットを介した配信や、CD-R、DVD等の記録媒体にコンテンツをコピーした海賊版ディスクの流通は大きな問題となってきた。

[0004] 特に、昨今、DVD製造設備を整え、市販の正当なDVDディスクに基づいてスタンパを作成して、そのスタンパに基づいて海賊版ディスクを大量に生産して流通させるという問題が発生している。また、正規にライセンスを受けたディスク工場においても、ライセンスによって承認された発注枚数以上の生産を不正に行い、余剰分を勝手に販売するといった不正ディスク製造、販売も発生している。このような不正ディスクの流通は、コンテンツの著作権を侵害するものであり、何らかの防止策が必要である。

[0005] DVDやBDなどのディスクの製造工程について、図1を参照して説明する。図1は、正当なコンテンツ利用権に基づく利用が許容されるコンテンツを格納した情報記録媒体、例えばDVDやBDディスクなどからなるROMディスクの製造処理工程につい

て説明する図である。図1に示すように、コンテンツは、コンテンツの所有者であるコンテンツオーナー11からコンテンツの編集処理を行なうコンテンツ編集エンティティ12に渡されて編集処理(オーサリング)が行なわれてディスク記録用の編集コンテンツが生成され、その後、ディスク製造工場20において市場に流通されるディスク50が製造される。

[0006] コンテンツオーナー11は、コンテンツ編集エンティティ12に対して、コンテンツとともにコンテンツの利用権を定めたコンテンツ利用制御情報(Usage Rule)が渡される。利用制御情報(Usage Rule)は例えばコンテンツに対応して設定され、コンテンツのコピー処理の可否などの情報が含まれる。最終的にユーザに渡されるディスク30にもコンテンツに併せて利用制御情報が格納され、再生装置などのユーザデバイスにおけるコンテンツの利用に際しては、ユーザデバイスで実行されるコンテンツ利用アプリケーションが利用制御情報を参照して利用制御情報に従ったコンテンツの利用を実行することになる。

[0007] ディスク製造工場20は、コンテンツ編集エンティティ12から編集済みのコンテンツと、利用制御情報(Usage Rule)を受領し、さらに、コンテンツの利用管理を行なうライセンスエンティティ13からコンテンツの暗号化、復号処理に適用する鍵情報を受領する。ライセンスエンティティ13は、コンテンツの利用管理を行ない、MKB(Media Key Block)、メディアキー(Km)等、各種の鍵データを生成してディスク製造工場20に提供する。

[0008] MKB(Media Key Block)は、ブロードキャストエンクリプション方式の一態様として知られる木構造の鍵配信方式に基づいて生成される暗号鍵ブロックである。MKBは有効なライセンスを持つユーザの情報処理装置に格納されたデバイスキー(Kd)に基づく処理(復号)によってのみ、コンテンツの復号に必要なキーであるメディアキー(Km)の取得を可能とした鍵情報ブロックである。これはいわゆる階層型木構造に従った情報配信方式を適用したものであり、ユーザデバイス(情報処理装置)が有効なライセンスを持つ場合にのみ、メディアキー(Km)の取得を可能とし、無効化(リボーク処理)されたユーザデバイスにおいては、メディアキー(Km)の取得が不可能となる。

- [0009] ライセンスエンティティ13はMKBに格納する鍵情報の暗号化に用いるデバイスキーの変更により、特定のユーザデバイスに格納されたデバイスキーでは復号できない、すなわちコンテンツ復号に必要なメディアキーを取得できない構成を持つMKBを生成することができる。従って、任意タイミングで不正デバイスを排除(リボーク)して、有効なライセンスを持つデバイスに対してのみ復号可能な暗号化コンテンツを提供することが可能となる。
- [0010] ディスク製造工場20では、コンテンツ暗号化、各データのフォーマット処理などをフォーマッタ31において実行し、さらに、フォーマットデータに基づく原盤、スタンパの生成をカッティングマシン32で実行した後、レプリケータ33において、生成されたスタンパを適用してディスク50を製造する。ディスク製造工場20では、ライセンスエンティティ13から許容された枚数のディスク50を製造する。
- [0011] フォーマッタ31において実行するコンテンツ暗号化、およびディスク格納データの生成処理について、図2を参照して説明する。図2には、ディスク製造工場20の処理と、情報記録媒体(ディスク)50の格納データ、および情報記録媒体(ディスク)50の格納コンテンツの利用を行なうユーザデバイスとしての情報処理装置(再生装置)60の処理を示している。
- [0012] なお、図2では、図1に示すカッティングマシン32、レプリケータ33の処理は省略してある。基本的には、フォーマッタ31において生成されたデータが情報記録媒体(ディスク)50に格納される。図2のディスク製造工場20の処理について説明する。
- [0013] MKB21は、前述したように、ライセンスエンティティ13から受領した暗号鍵ブロックであり、正当なライセンスを持つユーザデバイス、すなわち、図2に示す情報処理装置(再生装置)60のメモリに格納されたデバイスキー(Kd)61を適用した処理によって、メディアキー(Km)を取り出すことが可能な暗号鍵ブロックである。
- [0014] MKB21は、情報記録媒体(ディスク)50に格納される。図に示すMKB51である。ボリュームID22は、所定の枚数のディスク単位に設定される識別子(ID)であり、ディスク工場20において乱数生成処理などによって生成される。ボリュームID22は、情報記録媒体(ディスク)50に対して記録される。図に示すボリュームID52である。ボリュームID52は、通常のユーザデバイスとしての記録装置で実現可能とされるデータ

記録形式と異なる形式で記録される。すなわち専用の信号処理を適用したデータ書き込みが行われる。データ読み取りに際しても専用の信号処理が必要となる。たとえばROM-Mark方式(side-channel方式)などが適用される。

- [0015] さらに、ディスク製造工場20は、ステップS11において、ライセンスエンティティ13から受領したメディアキー(Km)23とボリュームID22とを連結し、ステップS12においてハッシュ値を算出して、ボリュームユニークキー(Kvu)を生成する。さらに、ステップS13において、ディスク格納コンテンツに対応する利用制御情報(Usage Rule)25のハッシュ値を算出し、ステップS14において、ディスク工場20において乱数生成などによって生成したコンテンツに対応して設定されるタイトルキー(Title Key)24と利用制御情報ハッシュ値との排他論理和を算出する。ステップS15において、この排他論理和演算結果を、ボリュームID22とメディアキー(Km)に基づいて生成したボリュームユニークキー(Kvu)で暗号化して情報記録媒体50に格納する。図に示す暗号化キー(Encrypted Key)53である。暗号化キー(Encrypted Key)53は、タイトルキー24と利用制御情報25のハッシュ値データに基づく暗号化データである。
- [0016] さらに、利用制御情報25も情報記録媒体50に格納する。図に示す利用制御情報54である。コンテンツ26は、図1を参照して説明したコンテンツ編集エンティティ12によって生成された編集済みのコンテンツである。コンテンツ26は、ステップS16においてタイトルキー24によって暗号化処理が実行され、暗号化コンテンツ55として情報記録媒体50に格納される。
- [0017] この結果、情報記録媒体(ディスク)50には、図に示すように、メディアキー(Km)を格納した暗号鍵ブロックとしてのMKB51、専用の信号処理によって書き込まれたボリュームID52、暗号化キー53、利用制御情報(Usage Rule)54、暗号化コンテンツ55が格納される。
- [0018] この情報記録媒体50は、ユーザデバイスとしての情報処理装置(再生装置)60にセットされ、所定のデータ再生アプリケーションを実行することで、予め設定された処理シーケンスが実行されてコンテンツの再生が行なわれることになる。
- [0019] 情報処理装置(再生装置)60は、まず、ステップS21において、情報処理装置(再

生装置)60のメモリに格納されたデバイスキー(Kd)を適用して情報記録媒体50から読み出したMKB51の処理を実行してメディアキー(Km)を取得する。なお、MKB51からメディアキー(Km)を取得するためには、有効なライセンスを持つ情報処理装置に格納されたデバイスキー(Kd)を適用することが必要である。無効化(リボーク処理)されたユーザデバイスにおいては、メディアキー(Km)の取得が不可能となる。

[0020] 次に、ステップS22において、MKBから取得したメディアキー(Km)と情報記録媒体50から読み出したボリュームIDを連結し、ステップS23においてハッシュ値を算出し、ボリュームユニークキー(Kvu)を生成する。

[0021] 次に、ステップS24において、生成したボリュームユニークキー(Kvu)を適用して、情報記録媒体50から読み出した暗号化キー(Encrypted Key)53の復号処理を実行し、さらに、ステップS25において、情報記録媒体50から読み出した利用制御情報54のハッシュ値を算出し、ステップS26においてこのハッシュ値と、ステップS24の復号結果との排他論理和演算を実行する。

[0022] このステップS24～S26の処理は、ディスク製造工場20において実行されたステップS13～S16の逆のプロセスに相当し、ステップS24～S26の処理によって、タイトルキーが算出されることになる。ステップS27では、生成したタイトルキーを適用して、情報記録媒体50から読み出した暗号化コンテンツ55の復号処理を実行してコンテンツ62を出力する。

[0023] このように、情報記録媒体50には、正当なライセンスを有するユーザデバイスにおいてのみコンテンツの利用を可能とするため、様々なデータが格納される。ディスク製造工場20では、必要なデータをライセンスエンティティ13、コンテンツ編集エンティティ12から受領して、予め決められたプロセスに従った処理を実行して情報記録媒体50を製造する。一方、ユーザデバイスとしての情報処理装置60においても予め決められたシーケンスに従った処理を行なうことでコンテンツの復号、再生が可能となる。

[0024] しかし、前述したように、様々な処理によって、海賊版ディスクが製造され、流通している。図3～図6を参照して、複数の海賊版ディスクの製造態様について説明する。

海賊版ディスクの製造態様には、例えば以下の態様がある。

- (1) ライセンスされた許容枚数以上の生産による海賊版ディスク生産
 - (2) 横流しスタンプによる海賊版ディスク生産
 - (3) 正当市販ディスクからの読み取り信号(RF信号)のコピーに基づく海賊版ディスク生産
 - (4) 正当市販ディスクからのピット形状の物理的コピーによる海賊版ディスク生産
- 以下、これらの各処理について説明する。

[0025] 図3は、(1)ライセンスされた許容枚数以上の生産による海賊版ディスク生産処理を説明する図である。ディスク製造工場20は、正当なライセンスを保有し、正当なライセンスに基づくディスク50の生産が許容された工場である。しかし、ライセンスされた許容枚数以上の生産によって海賊版ディスク70を生産して、不正なルートで販売する処理である。

[0026] 図4は、(2)横流しスタンプによる海賊版ディスク生産処理を説明する図である。ディスク製造工場20は、正当なライセンスを保有し、正当なライセンスに基づくディスク50の生産が許容された工場である。しかし、カッティングマシン32において製造したスタンプ、すなわちフォーマット済みのデータが記録されたスタンプを横流して、海賊版ディスク製造工場80に提供し、この海賊版ディスク製造工場80に設置されたレプリケータ81を利用して海賊版ディスク70を生産する処理である。

[0027] 図5は、(3)正当市販ディスクからの読み取り信号(RF信号)のコピーに基づく海賊版ディスク生産処理を説明する図である。この処理は、(1)、(2)と異なり、市販の正当なディスク50を利用して海賊版ディスク70を生産する。

[0028] 海賊版ディスク製造工場90は、市販の正当なディスク50をリーダー91にセットして、正当なディスク50からRF信号の読み取りを行なう。RF信号は、再生信号に変換する前のディスク50からの読み取り光信号から変換される信号である。このRF信号を原盤やスタンプを作成するカッティングマシン92に入力して、スタンプを製造して、レプリケータ93を利用して大量の海賊版ディスク70を生産する。

[0029] 図6は、(4)正当市販ディスクからのピット形状の物理的コピーによる海賊版ディスク生産処理を説明する図である。この処理も、(3)と同様、市販の正当なディスク50を利用して海賊版ディスク70を生産する。

[0030] この処理では、海賊版ディスク製造工場95は、市販の正当なディスク50をディスク分離装置96にセットして、ディスク50の表面の保護膜、反射膜を分離する。この処理によって、ディスクのピット形状がむき出しの状態になる。次に、転写装置97において、ピット形状を物理的にコピーしてスタンプを作成する。その後、このスタンプを適用し、レプリケータ98を利用して大量の海賊版ディスク70を生産する。

[0031] このように、海賊版ディスクの製造方法には、様々な手法があり、これらを防止する効果的な対応策が求められている。

発明の開示

発明が解決しようとする課題

[0032] 本発明は、上述の問題点に鑑みてなされたものであり、海賊版ディスクによるコンテンツ不正利用の防止や、海賊版ディスクの製造に関係した機器の特定を可能とするディスク製造方法、データ記録装置、情報記録媒体、情報処理装置および方法、並びにコンピュータ・プログラムを提供することを目的とする。

課題を解決するための手段

[0033] 本発明の第1の側面は、

暗号化コンテンツを格納したディスクのディスク製造方法であり、
ディスク製造エンティティ、またはディスク製造機器に対応する公開鍵証明書であり、
ディスク製造エンティティ、またはディスク製造機器の識別情報を含む公開鍵証明書を構成データとするプロダクトマークを、前記暗号化コンテンツの復号に適用する鍵の生成情報として生成するプロダクトマーク生成ステップと、

前記プロダクトマークに基づいて生成されるプロダクトマーク対応値と、製造ディスクの一定の集合に対して設定される識別子としてのボリュームIDとに基づく演算結果に対する暗号化データとしての暗号化ボリュームIDを、前記暗号化コンテンツの復号に適用する鍵の生成情報として生成する暗号化ボリュームID生成ステップと、

前記プロダクトマークと前記暗号化ボリュームIDを各ディスク個別に記録するステップであり、プロダクトマークと暗号化ボリュームIDの少なくともいずれかのデータを反射膜除去記録方式によって記録する個別データ記録ステップと、

を有することを特徴とするディスク製造方法にある。

- [0034] さらに、本発明のディスク製造方法の一実施態様において、前記プロダクトマーク生成ステップは、前記公開鍵証明書に加え、製造ディスク毎に設定されるシリアル番号、および該シリアル番号に対応して設定されるデジタル署名データを構成データとするプロダクトマークを生成するステップであり、前記暗号化ボリュームID生成ステップは、前記公開鍵証明書と、シリアル番号、および該シリアル番号に対応して設定されるデジタル署名データとを含むプロダクトマークに基づいて生成されるプロダクトマーク対応値と、前記ボリュームIDに基づいて暗号化ボリュームIDを生成するステップであることを特徴とする。
- [0035] さらに、本発明のディスク製造方法の一実施態様において、前記プロダクトマーク生成ステップは、前記公開鍵証明書に加え、製造ディスクの製造日時情報、および該製造日時情報に対応して設定されるデジタル署名データを構成データとするプロダクトマークを生成するステップであり、前記暗号化ボリュームID生成ステップは、前記公開鍵証明書と、製造日時情報、および該製造日時情報に対応して設定されるデジタル署名データとを含むプロダクトマークに基づいて生成されるプロダクトマーク対応値と、前記ボリュームIDに基づいて暗号化ボリュームIDを生成するステップであることを特徴とする。
- [0036] さらに、本発明のディスク製造方法の一実施態様において、前記暗号化ボリュームID生成ステップは、前記プロダクトマークに基づくハッシュ値として生成されるプロダクトマーク対応値と、前記ボリュームIDとに基づいて暗号化ボリュームIDを生成するステップであることを特徴とする。
- [0037] さらに、本発明のディスク製造方法の一実施態様において、暗号化ボリュームID生成ステップは、前記プロダクトマーク対応値と、ボリュームIDとに基づく演算による算出値を、製造ディスクの一定の集合に対して設定されるマスターキー、または該マスターキーのハッシュ値を適用した暗号化処理によって暗号化ボリュームIDを生成するステップであることを特徴とする。
- [0038] さらに、本発明のディスク製造方法の一実施態様において、前記ディスク製造方法は、さらに、前記マスターキーを、ディスクに記録する暗号化コンテンツの記録態様と異なる変調処理を施して記録するステップを有することを特徴とする。

[0039] さらに、本発明のディスク製造方法の一実施態様において、前記ディスク製造方法において、前記プロダクトマーク、および前記暗号化ボリュームIDは、ディスク製造に適用する原盤またはスタンプに対する記録情報とすることなく、前記個別データ記録ステップにおいて、各製造ディスク個別に生成し記録することを特徴とする。

[0040] さらに、本発明の第2の側面は、

情報記録媒体に対するデータ記録処理を実行するデータ記録装置であり、

情報記録媒体製造エンティティ、または情報記録媒体製造機器に対応する公開鍵証明書であり、情報記録媒体製造エンティティ、または情報記録媒体製造機器の識別情報を含む公開鍵証明書を構成データとするプロダクトマークを、前記情報記録媒体に記録する暗号化コンテンツの復号に適用する鍵の生成情報として生成するプロダクトマーク生成部と、

前記プロダクトマークに基づいて生成されるプロダクトマーク対応値と、製造する情報記録媒体の一定の集合に対して設定される識別子としてのボリュームIDとに基づく演算結果に対する暗号化データとしての暗号化ボリュームIDを、前記情報記録媒体に記録する暗号化コンテンツの復号に適用する鍵の生成情報として生成する暗号化ボリュームID生成部と、

前記プロダクトマークと前記暗号化ボリュームIDを各情報記録媒体個別に記録するデータ記録部であり、プロダクトマークと暗号化ボリュームIDの少なくともいずれかのデータを反射膜除去記録方式によって記録するデータ記録部と、

を有することを特徴とするデータ記録装置にある。

[0041] さらに、本発明のデータ記録装置の一実施態様において、前記プロダクトマーク生成部は、前記公開鍵証明書に加え、製造する情報記録媒体毎に設定されるシリアル番号、および該シリアル番号に対応して設定されるデジタル署名データを構成データとするプロダクトマークを生成する構成であり、前記暗号化ボリュームID生成部は、前記公開鍵証明書と、シリアル番号、および該シリアル番号に対応して設定されるデジタル署名データとを含むプロダクトマークに基づいて生成されるプロダクトマーク対応値と、前記ボリュームIDに基づいて暗号化ボリュームIDを生成する構成であることを特徴とする。

[0042] さらに、本発明のデータ記録装置の一実施態様において、前記プロダクトマーク生成部は、前記公開鍵証明書に加え、製造する情報記録媒体の製造日時情報、および該製造日時情報に対応して設定されるデジタル署名データを構成データとするプロダクトマークを生成する構成であり、前記暗号化ボリュームID生成部は、前記公開鍵証明書と、製造日時情報、および該製造日時情報に対応して設定されるデジタル署名データとを含むプロダクトマークに基づいて生成されるプロダクトマーク対応値と、前記ボリュームIDに基づいて暗号化ボリュームIDを生成する構成であることを特徴とする。

[0043] さらに、本発明の第3の側面は、
暗号化コンテンツを記録した情報記録媒体であり、
情報記録媒体製造エンティティ、または情報記録媒体製造機器に対応する公開鍵証明書であり、情報記録媒体製造エンティティ、または情報記録媒体製造機器の識別情報を含む公開鍵証明書を構成データとするデータであり、前記暗号化コンテンツの復号に適用する鍵の生成情報となるプロダクトマークと、
前記情報記録媒体に記録する暗号化コンテンツの復号に適用する鍵の生成情報であり、前記プロダクトマークに基づいて生成されるプロダクトマーク対応値と、製造される情報記録媒体の一定の集合に対して設定される識別子としてのボリュームIDとに基づく演算結果に対する暗号化データであり、前記暗号化コンテンツの復号に適用する鍵の生成情報となる暗号化ボリュームIDを格納し、
前記プロダクトマークまたは前記暗号化ボリュームIDの少なくともいずれかが反射膜除去記録方式によって記録された構成を有することを特徴とする情報記録媒体にある。

[0044] さらに、本発明の情報記録媒体の一実施態様において、前記プロダクトマークは、前記公開鍵証明書に加え、製造される情報記録媒体毎に設定されるシリアル番号、および該シリアル番号に対応して設定されるデジタル署名データを構成データとすることを特徴とする。

[0045] さらに、本発明の情報記録媒体の一実施態様において、前記プロダクトマークは、前記公開鍵証明書に加え、製造される情報記録媒体毎に設定される製造日時情報

、および該製造日時情報に対応して設定されるデジタル署名データを構成データとすることを特徴とする。

[0046] さらに、本発明の第4の側面は、

暗号化コンテンツを記録した情報記録媒体からのデータ読み取りおよびコンテンツ再生処理を実行する情報処理装置であり、

情報記録媒体からのデータ読み取りを実行するデータ取得部と、

前記データ取得部の取得したデータに基づくデータ処理を実行してコンテンツ復号用の鍵を生成する鍵生成部と、

前記鍵生成部の生成した鍵に基づいて暗号化コンテンツの復号処理を実行する復号処理部とを有し、

前記鍵生成部は、

情報記録媒体製造エンティティ、または情報記録媒体製造機器に対応する公開鍵証明書であり、情報記録媒体製造エンティティ、または情報記録媒体製造機器の識別情報を含む公開鍵証明書を構成データとするプロダクトマークと、

前記プロダクトマークに基づいて生成されるプロダクトマーク対応値と、情報記録媒体の一定の集合に対して設定される識別子としてのボリュームIDとに基づく演算結果に対する暗号化データである暗号化ボリュームIDと、

を含む鍵生成情報を前記データ取得部から入力し、該鍵生成情報を適用したデータ処理を実行してコンテンツ復号用の鍵を生成する構成であることを特徴とする情報処理装置にある。

[0047] さらに、本発明の第5の側面は、

暗号化コンテンツを記録したディスクからのデータ読み取りおよびコンテンツ再生処理を実行する情報処理方法であり、

情報記録媒体からのデータ読み取りを実行するデータ取得ステップと、

前記データ取得部の取得したデータに基づくデータ処理を実行してコンテンツ復号用の鍵を生成する鍵生成ステップと、

前記鍵生成部の生成した鍵に基づいて暗号化コンテンツの復号処理を実行する復号処理ステップとを有し、

前記鍵生成ステップは、

情報記録媒体製造エンティティ、または情報記録媒体製造機器に対応する公開鍵証明書であり、情報記録媒体製造エンティティ、または情報記録媒体製造機器の識別情報を含む公開鍵証明書を構成データとするプロダクトマークと、

前記プロダクトマークに基づいて生成されるプロダクトマーク対応値と、情報記録媒体の一定の集合に対して設定される識別子としてのボリュームIDとに基づく演算結果に対する暗号化データである暗号化ボリュームIDと、

を含む鍵生成情報を入力し、該鍵生成情報を適用したデータ処理を実行してコンテンツ復号用の鍵を生成するステップであることを特徴とする情報処理方法にある。

[0048] さらに、本発明の第6の側面は、

情報記録媒体に対するデータ記録処理をコンピュータ上において実行させるコンピュータ・プログラムであり、

情報記録媒体製造エンティティ、または情報記録媒体製造機器に対応する公開鍵証明書であり、情報記録媒体製造エンティティ、または情報記録媒体製造機器の識別情報を含む公開鍵証明書を構成データとするプロダクトマークを、前記情報記録媒体に記録される暗号化コンテンツの復号に適用する鍵の生成情報として生成するプロダクトマーク生成ステップと、

前記プロダクトマークに基づいて生成されるプロダクトマーク対応値と、製造情報記録媒体の一定の集合に対して設定される識別子としてのボリュームIDとに基づく演算結果に対する暗号化データとして暗号化ボリュームIDを、前記情報記録媒体に記録される暗号化コンテンツの復号に適用する鍵の生成情報として生成する暗号化ボリュームID生成ステップと、

前記プロダクトマークと前記暗号化ボリュームIDを各情報記録媒体個別に記録するデータ記録部であり、プロダクトマークと暗号化ボリュームIDの少なくともいずれかのデータを反射膜除去記録方式によって記録するデータ記録ステップと、

を有することを特徴とするコンピュータ・プログラムにある。

[0049] さらに、本発明の第7の側面は、

暗号化コンテンツを記録したディスクからのデータ読み取りおよびコンテンツ再生処

理をコンピュータ上において実行させるコンピュータ・プログラムであり、
情報記録媒体からのデータ読み取りを実行するデータ取得ステップと、
前記データ取得部の取得したデータに基づくデータ処理を実行してコンテンツ復号用の鍵を生成する鍵生成ステップと、
前記鍵生成部の生成した鍵に基づいて暗号化コンテンツの復号処理を実行する復号処理ステップとを有し、
前記鍵生成ステップは、
情報記録媒体製造エンティティ、または情報記録媒体製造機器に対応する公開鍵証明書であり、情報記録媒体製造エンティティ、または情報記録媒体製造機器の識別情報を含む公開鍵証明書を構成データとするプロダクトマークと、
前記プロダクトマークに基づいて生成されるプロダクトマーク対応値と、情報記録媒体の一定の集合に対して設定される識別子としてのボリュームIDとに基づく演算結果に対する暗号化データである暗号化ボリュームIDと、
を含む鍵生成情報を入力し、該鍵生成情報を適用したデータ処理を実行してコンテンツ復号用の鍵を生成するステップであることを特徴とするコンピュータ・プログラムにある。

[0050] なお、本発明のコンピュータ・プログラムは、例えば、様々なプログラム・コードを実行可能なコンピュータ・システムに対して、コンピュータ可読な形式で提供する記録媒体、通信媒体、例えば、CDやFD、MOなどの記録媒体、あるいは、ネットワークなどの通信媒体によって提供可能なコンピュータ・プログラムである。このようなプログラムをコンピュータ可読な形式で提供することにより、コンピュータ・システム上でプログラムに応じた処理が実現される。

[0051] 本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。なお、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

発明の効果

[0052] 本発明の構成によれば、ディスク製造エンティティ、またはディスク製造機器に対し

て発行された公開鍵証明書を含むプロダクトマークと、プロダクトマークに基づいて生成されるハッシュ値などのプロダクトマーク対応値と、製造ディスクの一定の集合に対して設定される識別子としてのボリュームIDとに基づく演算によって算出される暗号化ボリュームIDを生成し、これらのプロダクトマークおよび暗号化ボリュームIDをディスクに格納する暗号化コンテンツの復号用鍵の生成情報としてディスク各々に記録するとともに、これらのプロダクトマークと暗号化ボリュームIDの少なくともいずれかのデータを反射膜除去記録方式によって記録する構成としたので、市販の正当なディスクに基づいて、ピット形状を物理的にコピーした海賊版ディスクからは、鍵生成情報としてのプロダクトマークまたは暗号化ボリュームIDを読み取ることができず、コンテンツの不正な再生や利用を防止することができる。

- [0053] さらに、本発明の構成によれば、プロダクトマークに、情報記録媒体製造エンティティ、または情報記録媒体製造機器の識別情報を含む公開鍵証明書を含める構成としたので、ピット形状の物理的コピー以外の例えばRF信号読み取りデータに基づいて生成した海賊版ディスクについては、ディスクから公開鍵証明書を取得することで、海賊版ディスクの製造に関係した情報記録媒体製造エンティティや情報記録媒体製造機器を追跡し特定することが可能となる。

図面の簡単な説明

- [0054] [図1]従来のディスク製造処理の概要を説明する図である。
- [図2]従来の暗号化コンテンツ記録ディスクに対するデータ記録および再生シーケンスを説明する図である。
- [図3]従来のディスク製造処理における海賊版ディスクの製造例について説明する図である。
- [図4]従来のディスク製造処理における海賊版ディスクの製造例について説明する図である。
- [図5]従来のディスク製造処理における海賊版ディスクの製造例について説明する図である。
- [図6]従来のディスク製造処理における海賊版ディスクの製造例について説明する図である。

[図7]本発明の一実施例に係るディスクの製造処理構成について説明する図である。

[図8]本発明の一実施例に係るディスクの製造処理構成について説明する図である。

[図9]本発明の一実施例に係るディスク製造に適用するフォーマットの処理例について説明する図である。

[図10]本発明の一実施例に係るディスク製造に適用するフォーマットの処理例について説明する図である。

[図11]本発明の一実施例に係るディスク製造に適用するIDライターの処理例について説明する図である。

[図12]本発明の一実施例に係るディスク製造に適用するIDライターの処理例について説明する図である。

[図13]反射膜除去方式によるデータ記録処理について説明する図である。

[図14]反射膜除去方式によるデータ記録処理について説明する図である。

[図15]本発明の一実施例に係るディスク製造に適用するIDライターの処理例について説明する図である。

[図16]本発明の一実施例に係るディスク製造に適用するIDライターの処理例について説明する図である。

[図17]ボリュームIDの一例について説明する図である。

[図18]本発明の一実施例に係るディスクに対するデータ記録および再生処理について説明する図である。

[図19]本発明の一実施例に係るディスクに対するデータ記録および再生処理について説明する図である。

[図20]再生処理を実行する情報処理装置の構成例について説明する図である。

[図21]ディスクの解析処理例について説明する図である。

[図22]ディスクの解析処理例について説明する図である。

[図23]ディスクに対するデータ記録処理を実行するデータ記録装置および再生処理を実行する情報処理装置の構成例について説明する図である。

発明を実施するための最良の形態

[0055] 以下、図面を参照しながら本発明ディスク製造方法、データ記録装置、情報記録媒

体、情報処理装置および方法、並びにコンピュータ・プログラムの詳細について説明する。なお、説明は、以下の項目に従って行なう。

1. ディスク製造プロセス概要
2. ディスク製造プロセスの詳細
 - (2. 1)フォーマッタにおける処理例1
 - (2. 2)フォーマッタにおける処理例2
 - (2. 3)IDライターにおける処理例1
 - (2. 4)IDライターにおける処理例2
 - (2. 5)IDライターにおける処理例3
3. ディスク記録データの生成および再生処理の詳細
4. ディスク検証処理
5. 情報処理装置の構成

[0056] [1. ディスク製造プロセス概要]

まず、図7を参照して、本発明の一実施形態に係る情報記録媒体(ディスク)製造工程について説明する。図7は、先に図1を参照して説明したと同様、正当なコンテンツ利用権に基づく利用が許容されるコンテンツを格納した情報記録媒体、例えばDVDやBDディスクなどからなるROMディスクの製造処理工程について説明する図である。図7に示すように、コンテンツは、コンテンツの所有者であるコンテンツオーナー101からコンテンツの編集処理を行なうコンテンツ編集エンティティ102に渡されて編集処理(オーサリング)が行なわれてディスク記録用の編集コンテンツが生成され、その後、ディスク製造工場200において市場に流通されるディスク360が製造される。

[0057] コンテンツオーナー101は、コンテンツ編集エンティティ102に対して、コンテンツとともにコンテンツの利用権を定めたコンテンツ利用制御情報(Usage Rule)が渡される。利用制御情報(Usage Rule)は例えばコンテンツに対応して設定され、コンテンツのコピー処理の可否などの情報が含まれる。最終的にユーザに渡されるディスク360にもコンテンツに併せて利用制御情報が格納され、再生装置などのユーザデバイスにおけるコンテンツの利用に際しては、ユーザデバイスで実行されるコンテンツ利用アプリケーションが利用制御情報を参照して利用制御情報に従ったコンテンツの

利用を実行することになる。

- [0058] ディスク製造工場200は、コンテンツ編集エンティティ102から編集済みのコンテンツと、利用制御情報(Usage Rule)を受領し、さらに、コンテンツの利用管理を行なうライセンス管理エンティティ103からコンテンツの暗号化、復号処理に適用する鍵情報を受領する。ライセンス管理エンティティ103は、コンテンツの利用管理を行ない、MKB(Media Key Block)、メディアキー(Km)等、各種の鍵データを生成してディスク製造工場200に提供する。
- [0059] MKB(Media Key Block)は、先に説明したように、ブロードキャストエンクリプション方式の一態様として知られる木構造の鍵配信方式に基づいて生成される暗号鍵ブロックである。MKBは有効なライセンスを持つユーザの情報処理装置に格納されたデバイスキー(Kd)に基づく処理(復号)によってのみ、コンテンツの復号に必要なキーであるメディアキー(Km)の取得を可能とした鍵情報ブロックである。これはいわゆる階層型木構造に従った情報配信方式を適用したものであり、ユーザデバイス(情報処理装置)が有効なライセンスを持つ場合にのみ、メディアキー(Km)の取得を可能とし、無効化(リボーク処理)されたユーザデバイスにおいては、メディアキー(Km)の取得が不可能となる。
- [0060] ライセンス管理エンティティ103はMKBに格納する鍵情報の暗号化に用いるデバイスキーの変更により、特定のユーザデバイスに格納されたデバイスキーでは復号できない、すなわちコンテンツ復号に必要なメディアキーを取得できない構成を持つMKBを生成することができる。従って、任意タイミングで不正デバイスを排除(リボーク)して、有効なライセンスを持つデバイスに対してのみ復号可能な暗号化コンテンツを提供することが可能となる。
- [0061] ディスク製造工場200は、さらに、情報記録媒体(ディスク)製造管理エンティティ(KIC)104から、ディスク製造工場200、またはディスク製造工場200の製造機械に対応する公開鍵を格納した公開鍵証明書(PKC)および公開鍵に対応する秘密鍵を受領する。具体的には、例えば後段で説明するレプリケータ250あるいはIDライター260に対応する公開鍵を格納した公開鍵証明書(PKC)および公開鍵に対応する秘密鍵を受領する。なお、図には、レプリケータ250とIDライター260を別々に示してあ

るが、これらは1つの装置として構成することも可能であり、IDライター260がレプリケータ250の中に組み込まれた構成も可能である。この場合には、レプリケータ250に対応する公開鍵を格納した公開鍵証明書(PKC)および公開鍵に対応する秘密鍵を情報記録媒体(ディスク)製造管理エンティティ(KIC)104から受領する。

[0062] ディスク製造工場200では、コンテンツ暗号化、各データのフォーマット処理などをフォーマッタ230において実行し、さらに、フォーマットデータに基づく原盤、スタンパの生成をカッティングマシン240で実行する。その後、レプリケータ250において、スタンパを適用してレプリカとしての多数のディスクを製造し、さらに、製造したディスクに対して、IDライター260を適用して、各ディスクに固有の識別子としてのIDを記録して、コンテンツを格納したディスク360を完成させる。なお、IDライター260を適用して、各ディスクに記録されるデータは、プロダクトマークおよび暗号化ボリュームIDであり、少なくともこれらのデータのいずれかは、反射膜除去方式によって記録されることになる。記録データの構成および記録方式については後段で詳細に説明する。

[0063] また、ディスク製造工場200は、データ管理およびデータ記憶を実行するデータ管理&記憶部270を有する。データ管理&記憶部270は、コンテンツオーナー101から許可されたディスクの製造枚数である発注枚数を記憶し、さらに、必要に応じてコンテンツオーナー101から付与されたディスクに対して設定すべきシリアル番号の開始番号を保持する。さらに、ディスク製造工場200のフォーマッタ230において生成するデータ、例えばマスターキー、ボリュームIDを記憶する。これらのデータは、IDライター260に入力される。これらのデータの保持、転送はディスク製造工場200におけるLAN、専用線、スマートカードなどを適用し漏洩・改ざん等のないセキュアなデータ管理の下に実行される。

[0064] IDライター260は、データ管理&記憶部270から入力するデータと、情報記録媒体(ディスク)製造管理エンティティ104から受領した公開鍵証明書(PKC)、秘密鍵を適用して、ディスク1枚ごとに異なる記録情報を生成して各ディスクに記録する処理を実行して、コンテンツを格納したディスク360を完成させる。なお、IDライター260を適用して、各ディスクに記録されるデータは、プロダクトマークおよび暗号化ボリューム

ムIDであり、少なくともこれらのデータのいずれかは、反射膜除去方式によって記録されることになる。記録データの構成および記録方式については後段で詳細に説明する。

[0065] 図8を参照して、ディスク製造工場200において実行する一連のプロセスについて説明する。図8上段の(A)マスタリングプロセスは、図7に示すフォーマッタ230とカッティングマシン240において実行するプロセスを示し、下段の(B)レプリケーションプロセスは、図7に示すレプリケータ250とIDライター260において実行するプロセスを示している。

[0066] ステップS101は、図7に示すフォーマッタ230における処理であり、ライセンス管理エンティティからコンテンツの暗号化、復号処理に適用する鍵情報としてのMKB(Media Key Block)301と、メディアキー(Km)302を入力し、コンテンツ編集エンティティから編集済みのコンテンツ303と、利用制御情報(Usage Rule)304を受領し、ディスクに記録するデータの生成、すなわちコンソーン等の記録データの暗号化処理、およびフォーマット処理を実行する。この処理過程で、フォーマッタ230は、ボリュームID、マスターキー、タイトルキー等を、例えば乱数生成処理によって生成する。これらの処理の詳細については、図9他を参照して後段で説明する。

[0067] ボリュームID、マスターキー、タイトルキーは、図7に示すフォーマッタ230において、例えば1つの編集コンテンツに対応して設定されるデータであり、所定の生産枚数のディスクに共通の値として設定される。ボリュームID、マスターキーは、図7を参照して説明したように、データ管理&記憶部270に格納された後、IDライター260に入力されて、IDライターにおける書き込みデータの生成に適用される。タイトルキーは、コンテンツの暗号化キーとして適用される。これらの各処理については後段で説明する。

[0068] ステップS101のフォーマッタ230におけるコンテンツ暗号化、フォーマッティング処理が終了すると、ステップS102、S103のカッティング処理、ケミカルプロセスが実行され、メタルマスタ341、スタンパ342が生成される。これらの処理は、図7に示すカッティングマシン240において実行される。この処理は、フォーマッタ230の生成した暗号化コンテンツを含むフォーマットデータに対応する記録信号としてのピット形状を持

つ原盤、スタンプを生成する工程であり、従来から行なわれている処理と同様の処理である。

[0069] 次に、図8(B)のレプリケーションプロセスに移行する。ステップS121～S123は、図7に示すレプリケータ250の処理である。ステップS121のモールド処理により、スタンプのピット形状をコピーしたデータ記録ディスクとしてのベアディスク(Bare Disc) 343を製造し、ステップS122のスパッタリング処理によって、反射膜を生成し、さらに、ステップS123において、コーティング処理によって保護膜を生成する。

[0070] ステップS124の処理は、図7に示すIDライター260の処理である。この処理において、IDライター260は、データ記録済みのディスクの1枚毎に、異なるデータの書き込み処理を行なう。IDライター260を適用して、各ディスクに記録されるデータは、前述したようにプロダクトマークおよび暗号化ボリュームIDなどであり、少なくともこれらのデータのいずれかは、反射膜除去方式によって記録される。これらの処理によって、ディスク360が完成する。

[0071] 本発明の処理においては、図7に示すフォーマッタ230の処理と、IDライター260の処理が、従来の処理と大きく異なる処理を行なうことになる。フォーマッタ230の処理と、IDライター260の処理の詳細については、後段で説明する。

[0072] [2. ディスク製造プロセスの詳細]

本発明の処理においては、主に図7に示すフォーマッタ230の処理と、IDライター260の処理が、従来の処理と大きく異なる処理を行なうことになる。図9以下を参照して、フォーマッタ230の処理と、IDライター260の処理の詳細について説明する。まず、フォーマッタの処理例として2つの処理例を図9、および図10を参照して説明する。

[0073] (2. 1)フォーマッタにおける処理例1

図9を参照して、第1のフォーマッタ処理例について説明する。図9に示すフォーマッタ230は、ライセンス管理エンティティからコンテンツの暗号化、復号処理に適用する鍵情報としてのMKB(Media Key Block) 301と、メディアキー(Km) 302を入力し、コンテンツ編集エンティティから編集済みのコンテンツ303と、図示しない利用制御情報(Usage Rule)を受領し、ディスクに記録するデータの生成、すなわちコン

ツン等の記録データの暗号化処理、およびフォーマット処理を実行する。

- [0074] 図9に示すフォーマッタ230は、乱数生成部231において乱数に基づくボリュームIDを生成する。ボリュームIDは、例えば編集コンテンツ303単位、スタンパ単位など、複数のディスクに対応して共通に適用されるIDである。ボリュームIDは、暗号化処理部232に入力され、メディアキー302他のデータを適用した一連の暗号化処理シーケンスが実行されて、コンテンツ暗号化処理、その他の記録データの生成、暗号化処理が実行される。なお、具体的な暗号化処理シーケンスについては、図17、図18を参照して後段で説明する。
- [0075] データ連結部233では、暗号化処理部232において生成された暗号化コンテンツを含む記録データと、MKB301を連結し、変調処理部A234において変調処理が実行され、カッティングマシン240に出力される。変調処理部A234において実行する変調処理は、例えば17p-p変調方式が用いられる。17p-p変調方式は、EFMやEFM+変調方式等の固定ビット長(8ビット)の変調方式とは異なり、変調単位が2ビットの変調方式である。
- [0076] さらに、フォーマッタ230の乱数生成部235は、乱数に基づくマスターキーを生成する。マスターキーも、例えば編集コンテンツ303単位、スタンパ単位など、複数のディスクに対応して共通に適用される鍵データである。生成されたマスターキーは、変調処理部B236において、変調処理部A234において実行される変調処理とは異なる変調処理、例えばサイドチャネル(side-channel)変調処理が実行されて、カッティングマシン240に出力される。
- [0077] 変調処理部A234において実行される変調処理結果としてディスクに記録されるデータは、ユーザデバイスにおける一般的なコンテンツ再生方式において読み取ることが可能なデータであるが、変調処理部B234は、その変調処理結果としての記録データを再生する場合には、特殊な再生方式を適用することが必要となる。
- [0078] すなわち、マスターキーの読み取りには、例えばサイドチャネル(side-channel)変調処理、ROM-Markデコードなどの特殊な再生方式を適用したデータ読み取りを必要とする。コンテンツ再生処理を実行するユーザデバイスの再生アプリケーションは、これらの特殊なデータ読み取りを実行してマスターキーの読み取りを行なうこと

になる。再生処理の詳細については、図17他を参照して後段で説明する。

[0079] 乱数生成部231において生成したボリュームID、および乱数生成部235において生成したマスターキーは、データ管理&記憶部270に格納される。図に示すボリュームID311、およびマスターキー312である。これらのデータは、セキュアな管理の下、IDライター260に入力され、IDライターでのディスクに対する書き込みデータの生成に適用される。この処理については、後段で説明する。なお、ボリュームIDやマスターキーは、ディスクに記録される暗号化コンテンツの復号処理に使用するデータである。復号処理の詳細については、図17他を参照して後段で説明する。

[0080] 図9を参照して説明したフォーマッタ230の処理によれば、暗号化コンテンツとマスターキーは、カッティングマシン240に入力されて原盤、スタンプに記録されるが、ディスクに記録される暗号化コンテンツの復号処理に使用するデータであるボリュームIDは、カッティングマシン240に入力されず、メタルマスタ(原盤)、スタンプに記録されることがない。従って、メタルマスタ(原盤)やスタンプにはボリュームIDが記録されないため、メタルマスタ(原盤)やスタンプが流出してもそれだけでは複製ディスクを生産することができないことになる。

[0081] (2. 2)フォーマッタにおける処理例2

図10を参照して、第2のフォーマッタ処理例について説明する。図10に示すフォーマッタ230と、図9のフォーマッタ230との差異は、乱数生成部235において生成したマスターキーに対して、ハッシュ処理部237において、メディアキー(Km)302を適用したハッシュ処理を実行してデータ管理&記憶部270に格納する点のみである。その他の構成については、図9の構成、処理と同様である。

[0082] 図10に示す構成では、乱数生成部231において生成したボリュームID、および乱数生成部235において生成したマスターキーのハッシュ値が、データ管理&記憶部270に格納される。図に示すボリュームID311、およびマスターキーハッシュ値321である。これらのデータは、セキュアな管理の下、IDライター260に入力され、IDライターでのディスクに対する書き込みデータの生成に適用される。この処理については、後段で説明する。なお、ボリュームIDやマスターキーハッシュ値は、ディスクに記録される暗号化コンテンツの復号処理に使用するデータである。復号処理の詳細につ

いては、図17他を参照して後段で説明する。

[0083] (2. 3) IDライターにおける処理例1

次に、図7に示すIDライター260の処理例について説明する。IDライターは、図7に示すレプリケータ250において生成されたコンテンツ記録ディスク1枚毎に異なる記録データを生成して記録する処理を実行する。

[0084] IDライター260は、図11に示すように、データ管理&記憶部270(図7参照)から入力するデータと、情報記録媒体(ディスク)製造管理エンティティ104から受領した公開鍵証明書(PKC)、秘密鍵を適用して、ディスク1枚ごとに異なる記録情報を生成して各ディスクに記録する処理を実行する。各ディスクに記録されるデータは、プロダクトマークおよび暗号化ボリュームIDであり、少なくともこれらのデータのいずれかは、反射膜除去方式によって記録されることになる。

[0085] IDライター260は、図11に示すように、ディスク製造エンティティ、またはディスク製造適用機器に対して発行された公開鍵証明書を含むプロダクトマークを生成するプロダクトマーク生成部260Aと、プロダクトマークに基づいて生成されるハッシュ地等のプロダクトマーク対応値と、製造するディスクの一定の集合に対して設定される識別子としてのボリュームIDとに基づく演算結果に対する暗号化データとして暗号化ボリュームIDを生成する暗号化ボリュームID生成部260Bと、プロダクトマークと暗号化ボリュームIDを各ディスク個別に記録するデータ記録部260Cを有する。データ記録部260Cは、プロダクトマークと暗号化ボリュームIDの少なくともいずれかのデータを反射膜除去記録方式によって記録する。

[0086] まず、IDライターにおける処理例1について、図12を参照して説明する。図12の上段には、データ管理&記憶部270に格納されているデータを示し、中段にIDライター260の処理、下段にディスク書き込みデータ400を示している。

[0087] データ管理&記憶部270には、先に図7を参照して説明したコンテンツオーナー101から受領したシリアル開始番号331、発注枚数332、およびフォーマット230の生成したボリュームID311、マスターキー312が格納されている。なお、本例では、マスターキー312を適用した処理例を説明するが、図10を参照して説明したマスターキーハッシュ値を適用してもよい。

- [0088] なお、IDライター260は、先に図7を参照して説明したように、情報記録媒体(ディスク)製造管理エンティティ(KIC)104からディスク工場、あるいは製造機器(IDライターを含む機器)に対応する公開鍵を格納した公開鍵証明書(PKC)352と、公開鍵に対応する秘密鍵351を保有している。
- [0089] IDライター260は、これらのデータに基づいて、各ディスク毎に異なる記録データ、すなわちプロダクトマークと暗号化ボリュームIDを生成する。図12に示す処理例は、プロダクトマークを情報記録媒体(ディスク)製造管理エンティティ(KIC)104から受領した公開鍵証明書(PKC)とした処理例である。
- [0090] IDライター260の処理について図12を参照して説明する。なお、図12に示す処理は、各ディスク毎に実行する処理である。まず、シリアル番号生成部261において、コンテンツオーナー101から受領したシリアル開始番号331に基づいて、ディスクに設定するシリアル番号を生成する。例えば、コンテンツオーナー101から受領したシリアル開始番号が10001で、発注枚数が、1000枚である場合、IDライターは、各ディスクに対して、10001～11000のシリアル番号を付与することになる。ID書き込み回数計測部262は、IDライター260によるID書き込み処理の実行されたディスク枚数の管理を行い、発注枚数までの処理のみを許容する。
- [0091] デジタル署名生成部263は、シリアル番号生成部261において生成したシリアル番号に対して、情報記録媒体(ディスク)製造管理エンティティ(KIC)104の管理する秘密鍵351を適用してデジタル署名を生成し、シリアル番号とデジタル署名をディスク書き込みデータ400の構成データとして記録する。図に示すディスク書き込みデータ400中のシリアル番号401、デジタル署名402である。この処理例1では、シリアル番号401、デジタル署名402は、プロダクトマークの構成要素ではなく、これらは、通常のデータ再生によって再生可能なデータとして記録してもよいし、BCA方式(バーストカッティング)、コード記録方式などの特殊なデータ記録、再生を必要とする方式を適用して記録してもよい。
- [0092] この処理例1では、情報記録媒体(ディスク)製造管理エンティティ(KIC)104から受領した公開鍵証明書(PKC)352をプロダクトマークとしてディスクに書き込む。図に示すディスク書き込みデータ400中の公開鍵証明書(PKC)403である。公開鍵証

明書には、レプリケータの識別子としてのレプリケータID、IDライターの識別子としてのIDライターID、さらに、公開鍵、これらのデータに対する情報記録媒体(ディスク)製造管理エンティティ(KIC)の電子署名が含まれる。

[0093] さらに、IDライター260のAESハッシュ部264は、情報記録媒体(ディスク)製造管理エンティティ(KIC)104から受領した公開鍵証明書(PKC)352のハッシュ値を算出し、フォーマッタ230が生成し、データ管理&記憶部270に格納されたボリュームID311との演算処理を演算部265で実行する。演算部265で実行する演算は、例えば排他論理和演算(XOR)である。さらに、その演算結果をAES暗号化部266に入力して、フォーマッタ230が生成し、データ管理&記憶部270に格納されたマスターキー312を適用したAES暗号処理を実行して暗号化ボリュームIDを生成する。

[0094] AES暗号化部266の生成した暗号化ボリュームIDは、ディスクに書き込まれる。図に示すディスク書き込みデータ400中の暗号化ボリュームID404である。

[0095] ディスク書き込みデータ400中の、プロダクトマークとしての公開鍵証明書403と、暗号化ボリュームID404との少なくともいずれか一方は、反射膜除去方式によって各ディスクに書き込む。

[0096] 反射膜除去方式について、図13を参照して説明する。ディスク405のデータ記録トラックには、予め、所定の凹凸形状としてのピット、ランドが形成され、反射膜406が設定されている。反射膜除去方式は、このトラック中の所定の位置のランドに対して、高出力レーザを照射することにより、そのランドをピット化して記録を行うという、レーザ照射処理による方法である。つまり、ランドをピット化することができる領域を、記録領域上の複数の所定の部分に設けておき、記録データとしてのプロダクトマークやボリュームIDのビット情報に応じて、各部分をピット化するかランドの状態のままとするかを判断して、各部分にレーザ光を照射していく。

[0097] 具体的には、図13(B)に示すように、ある所定の位置のランドに対して高出力レーザを照射する。高出力レーザは、再生パワーより充分高いパワーでありランドの反射膜が溶融する程度のパワーである。このようにランドに高出力レーザを照射すると、図13(C)に示すように、ランドに塗布されていた反射膜406が溶融して無くなる。このように反射膜406が無くなった部分に光を照射すると、反射光が戻ってこない。即ち、

その部分がピットと同等の反射特性となる。このように一旦、スタンパでピット/ランドのパターンを転写した後に、ランドをピット化することにより、スタンパで生成したオリジナルノビットパターンと異なるビットパターンを記録することが可能となる。

- [0098] すなわち、反射膜除去前は、図14(A)に示すように、ピット=0、ランド=1とした場合、ビットパターンは、000100であるが、反射膜除去後は、図14(C)に示すように、ビットパターンは000000となる。このように、反射膜除去によって、所定のビットパターンを生成して、公開鍵証明書403を含むプロダクトマークと、ボリュームID404との少なくともいずれか一方については反射膜除去方式を適用して書き込む。両者を反射膜除去方式によって書き込む構成としてもよい。一方のデータを反射膜除去方式を適用しないで書き込む場合は、そのデータについては一般的なデータ記録方式、サイドチャネル方式、ROMマーク方式などの方式によって書き込む。
- [0099] この反射膜除去方式によって記録されたデータを持つディスクに基づいて、先に図6を参照して説明した海賊版ディスク製造方法、すなわち、正当市販ディスクからのピット形状の物理的コピーによる海賊版ディスク生産を実行すると、生産された海賊版ディスクは、ピットパターンを物理的にコピーして、反射膜を全面に塗布して生成することになるので、正当なディスクの反射膜除去部分にも反射膜が形成されることになる。その結果、正当ディスクにおいて、反射膜除去部分から読み取られるデータと、海賊版ディスクから読み取られるデータは異なるデータとなる。
- [0100] 処理例1では、プロダクトマークとしての公開鍵証明書403と、暗号化ボリュームID404との少なくともいずれか一方がこの反射膜除去方式で記録されることになる。これらのデータは、コンテンツの復号に適用する鍵の生成情報として設定される。具体的なコンテンツ暗号化、復号シーケンスについては図17以下を参照して説明する。
- [0101] 海賊版ディスクにおいては、プロダクトマーク、または暗号化ボリュームIDの少なくともいずれかが正確に読み取ることができなくなるので、コンテンツの復号が不可能になる。このように、暗号鍵生成情報としてのプロダクトマーク、またはボリュームIDの少なくともいずれかを反射膜除去方式で記録することで、コンテンツの不正利用を防止することが可能となる。

- [0102] (2. 4) IDライターにおける処理例2

次に、IDライター260の処理例2について図15を参照して説明する。図15の上段には、データ管理&記憶部270に格納されているデータを示し、中段にIDライター260の処理、下段にディスク書き込みデータ410を示している。なお、本例でも、マスターキー312を適用した処理例を説明するが、図10を参照して説明したマスターキーハッシュ値を適用してもよい。

- [0103] 処理例1では、プロダクトマークを情報記録媒体(ディスク)製造管理エンティティ(KIC)104から受領した公開鍵証明書(PKC)352のみとして設定した例であったが、処理例2では、この公開鍵証明書(PKC)に、シリアル番号生成部261において生成したシリアル番号と、シリアル番号に対して秘密鍵351を適用して生成したデジタル署名とを加えたデータ、すなわち、図15のディスク書き込みデータ410中のシリアル番号411、デジタル署名412、公開鍵証明書(PKC)413のすべてをプロダクトマークとして設定した例である。なお、シリアル番号411のみ、デジタル署名412のみ、シリアル番号411とデジタル署名412の連結データ、のいずれをプロダクトマークとして設定しても期待される発明の効果は同じである。
- [0104] 図15に示すIDライター260の連結部267において、シリアル番号とデジタル署名を連結し、更に連結部268で公開鍵証明書(PKC)を連結し、これらの連結データをプロダクトマークとしてディスク書き込みデータ410とする。
- [0105] なお、AESハッシュ部264は、シリアル番号とデジタル署名と公開鍵証明書(PKC)との連結データのハッシュ値を算出し、この算出ハッシュ値と、ボリュームID311との演算処理、例えば排他論理和演算(XOR)を演算部265で実行し、その演算結果をAES暗号化部266に入力して、データ管理&記憶部270に格納されたマスターキー312を適用したAES暗号処理を実行して暗号化ボリュームIDを生成する。
- [0106] AES暗号化部266の生成した暗号化ボリュームIDは、ディスクに書き込まれる。図に示すディスク書き込みデータ410中の暗号化ボリュームID414である。ディスク書き込みデータ410中の、プロダクトマーク、すなわち、シリアル番号411とデジタル署名412と公開鍵証明書(PKC)413との連結データと、暗号化ボリュームID414との少なくともいずれか一方は、前述した反射膜除去方式によって各ディスクに書き込む。

[0107] 反射膜除去方式によって記録されたデータを持つディスクに基づいて、正当市販ディスクからのピット形状の物理的コピーによる海賊版ディスク生産を実行しても、前述したように、正当ディスクの反射膜除去部分から読み取られるデータと、海賊版ディスクから読み取られるデータは異なるデータとなり、プロダクトマークと、暗号化ボリュームIDを、コンテンツの復号に適用する鍵の生成情報として設定することで、海賊版ディスクにおいては、コンテンツの復号が不可能になる。

[0108] (2. 5) IDライターにおける処理例3

次に、IDライター260の処理例3について図16を参照して説明する。図16の上段には、データ管理&記憶部270に格納されているデータを示し、中段にIDライター260の処理、下段にディスク書き込みデータ420を示している。なお、本例でも、マスターキー312を適用した処理例を説明するが、図10を参照して説明したマスターキーハッシュ値を適用してもよい。

[0109] 処理例3では、シリアル番号ではなく、セキュアタイムをプロダクトマークの構成要素として設定した例である。セキュアタイム生成部269において、セキュアな時間情報を提供する機関から受領した時間情報(製造日時情報)を取得、あるいは厳密な管理のなされた時間情報生成手段において生成した時間情報を取得する。デジタル署名生成部263は、セキュアタイム生成部269において生成した製造日時情報に対して、情報記録媒体(ディスク)製造管理エンティティ(KIC)104の管理する秘密鍵351を適用してデジタル署名を生成する。その後の処理は、図15を参照して説明した処理例2と同様である。なお、製造日時421のみ、デジタル署名422のみ、製造日時421とデジタル署名422の連結データ、のいずれをプロダクトマークとして設定しても期待される発明の効果は同じである。

[0110] 図16に示すIDライター260の連結部267において、セキュアタイム(製造日時)とデジタル署名を連結し、更に連結部268で公開鍵証明書(PKC)を連結し、これらの連結データをプロダクトマークとしてディスク書き込みデータ420とする。

[0111] なお、AESハッシュ部264は、セキュアタイム(製造日時)とデジタル署名と公開鍵証明書(PKC)との連結データのハッシュ値を算出し、この算出ハッシュ値と、ボリュームID311との演算処理、例えば排他論理和演算(XOR)を演算部265で実行し、

その演算結果をAES暗号化部266に入力して、データ管理&記憶部270に格納されたマスターキー312を適用したAES暗号処理を実行して暗号化ボリュームIDを生成する。

- [0112] AES暗号化部266の生成した暗号化ボリュームIDは、ディスクに書き込まれる。図に示すディスク書き込みデータ420中の暗号化ボリュームID424である。ディスク書き込みデータ420中の、プロダクトマーク、すなわち、セキュアタイム(製造日時)421とデジタル署名422と公開鍵証明書(PKC)423との連結データと、暗号化ボリュームID424との少なくともいずれか一方は、前述した反射膜除去方式によって各ディスクに書き込む。
- [0113] 反射膜除去方式によって記録されたデータを持つディスクに基づいて、正当市販ディスクからのピット形状の物理的コピーによる海賊版ディスク生産を実行しても、前述したように、正当ディスクの反射膜除去部分から読み取られるデータと、海賊版ディスクから読み取られるデータは異なるデータとなり、プロダクトマークと、暗号化ボリュームIDを、コンテンツの復号に適用する鍵の生成情報として設定することで、海賊版ディスクにおいては、コンテンツの復号が不可能になる。
- [0114] 上述の例では、暗号化ボリュームIDと、少なくとも公開鍵証明書(PKC)を含むプロダクトマークを個別データとして説明したが、これらのデータは1まとめのデータとしてディスクに反射膜除去方式を適用して書き込む構成としてもよい。
- [0115] 図17に、プロダクトマークを含む暗号化ボリュームIDのデータフォーマット例を示す。(A)は、プロダクトマークを含む暗号化ボリュームIDのデータフォーマットであり、(B)は、暗号化ボリュームIDに含まれる公開鍵証明書(PKC)のデータフォーマット例である。
- [0116] 図17(A)に示すように、暗号化ボリュームIDは、ヘッダ、レングス、マーキングデータ、署名、公開鍵証明書(PKC)、暗号化ボリュームIDの各データを含む。また、公開鍵証明書(PKC)は、タイプ、バージョン、証明書ID、機器(IDライター)ID、公開鍵、KICの署名の各データを含む構成である。
- [0117] 図17(A)に示す暗号化ボリュームID中のマーキングデータは、シリアル番号または製造日時情報のいずれかのデータの格納領域であり、ヘッダ=0x00のときは

、シリアル番号が格納され、ヘッダ＝0x01のときは、製造日時情報が格納される。

[0118] [3. ディスク記録データの生成および再生処理の詳細]

次に、図18、図19を参照して、ディスク記録データの生成および再生処理の詳細について説明する。図18は、暗号化ボリュームIDの暗号鍵としてマスターキーを適用した例であり、図19は、暗号化ボリュームIDの暗号鍵としてマスターキーハッシュ値を適用した例である。すなわち、先に説明したフォーマット230についての図9の処理構成に対応する例が図18であり、図10の処理構成に対応する例が図19である。

[0119] まず、暗号化ボリュームIDの暗号鍵としてマスターキーを適用した図18の処理例について説明する。図18には、ディスク製造工場500の処理と、情報記録媒体(ディスク)600の格納データ、および情報記録媒体(ディスク)600の格納コンテンツの利用を行なうユーザデバイスとしての情報処理装置(再生装置)700の処理を示している。

[0120] なお、図18のディスク製造工場500の処理において、プロダクトマークの生成と記録処理、およびボリュームIDの暗号化処理、記録処理が図7に示すIDライター260の実行する処理であり、マスターキーの生成、ボリュームIDの生成、タイトルキーの生成、コンテンツの暗号化処理、およびこれらの記録データの生成は、フォーマット230の実行する処理である。

[0121] ディスク製造工場において使用するデータ、MKB501～コンテンツ508の各々について、順に説明する。

[0122] MKB501は、前述したように、図7に示すライセンス管理エンティティ103から受領した暗号鍵ブロックであり、正当なライセンスを持つユーザデバイス、すなわち、図18に示す情報処理装置(再生装置)700のメモリに格納されたデバイスキー(Kd)701を適用した処理によって、メディアキー(Km)を取り出すことが可能な暗号鍵ブロックである。MKB501は、情報記録媒体(ディスク)600に格納される。図に示すMKB601である。

[0123] プロダクトマーク502は、先に、図12～図17を参照して説明したように、

(a)公開鍵証明書

(b)シリアル番号+デジタル署名+公開鍵証明書

(c) 製造日時＋デジタル署名＋公開鍵証明書

のいずれかによって構成されるデータであり、図7に示すIDライター260の生成するデータである。プロダクトマーク502は、情報記録媒体(ディスク)600に格納される。図に示すプロダクトマーク602である。なお、図示されないが、(b)において、シリアル番号のみ、デジタル署名のみ、またはシリアル番号＋デジタル署名をプロダクトマークの対象とした場合も発明の効果は等しく得られ、また、(c)において、製造日時のみ、デジタル署名のみ、製造日時＋デジタル署名をプロダクトマークの対象とした場合も同様に発明の効果は等しく得られる。

- [0124] 情報記録媒体(ディスク)600に記録されるデータ中、プロダクトマーク602または暗号化ボリュームID604の少なくとも一方のデータは、前述した反射膜除去方式に従って記録される。
- [0125] マスターキー503は、図9、図10を参照して説明したように、図7に示すフォーマッタ230において生成されるデータである。マスターキー503は、情報記録媒体(ディスク)600に格納される。図に示すマスターキー603である。マスターキー603は、例えばサイドチャネル方式、ROM-Mark方式など、特殊なデータ再生方式によってのみ読み取り可能なデータとして記録される。
- [0126] ボリュームID504は、図9、図10を参照して説明したように、図7に示すフォーマッタ230において生成されるデータである。ボリュームID504は、ステップS301において生成されたプロダクトマークのハッシュ値と、ステップS302において例えば排他論理和演算がなされ、演算結果に対して、ステップS303において、マスターキー503を適用した暗号化処理が実行されて、暗号化ボリュームID604として情報記録媒体(ディスク)600に格納される。この処理は、先に、図12～図17を参照して説明したIDライター260の処理である。
- [0127] 前述したように、プロダクトマーク602または暗号化ボリュームID604の少なくとも一方のデータは、前述した反射膜除去方式に従って記録される。
- [0128] メディアキー505は、図7に示すライセンス管理エンティティ103から受領する鍵データであり、ステップS304において、ボリュームID504との連結がなされ、ステップS305において連結データのハッシュ値が算出されて、ボリュームユニークキー(Kvu)

を生成するために適用される。メディアキー505は、情報記録媒体(ディスク)600には格納されない。ただし、メディアキー505は、MKB501に格納された鍵であり、正当なライセンスを持つユーザデバイス、すなわち、図18に示す情報処理装置(再生装置)700のメモリに格納されたデバイスキー(Kd)701を適用した処理によって、メディアキー(Km)を取り出すことが可能である。

[0129] タイトルキー506は、図7に示すフォーマット230において生成されるコンテンツ508の暗号化(S309)に適用する鍵データである。

利用制御情報(Usage Rule)507は、図7に示すコンテンツ編集エンティティ102から編集コンテンツとともに受領するデータである。

[0130] ステップS306において、利用制御情報(Usage Rule)507のハッシュ値が算出され、ステップS307において、タイトルキー506とハッシュ値との排他論理和(XOR)が算出され、その演算結果が、ステップS308において、ボリュームID504、メディアキー(Km)505にもとづいて生成されたボリュームユニークキー(Kvu)を適用して暗号化がなされて、暗号化キー605として情報記録媒体(ディスク)600に格納される。

[0131] コンテンツは、図7に示すコンテンツ編集エンティティ102から受領する編集コンテンツであり、ステップS309において、タイトルキー506を適用した暗号化処理がなされて、暗号化コンテンツ607として情報記録媒体(ディスク)600に格納される。

[0132] この結果、情報記録媒体(ディスク)600には、図に示すように、メディアキー(Km)を格納した暗号鍵ブロックとしてのMKB601、

(a)公開鍵証明書

(b)シリアル番号+デジタル署名+公開鍵証明書

(c)製造日時+デジタル署名+公開鍵証明書

のいずれかによって構成されるプロダクトマーク602、

マスターキー603、

暗号化ボリュームID604、

暗号化キー605、

利用制御情報606、

暗号化コンテンツ607

の各データが格納される。

- [0133] これらのデータ中、マスターキー603は、サイドチャネル方式、ROMマーク記録方式などの、コンテンツの読み取りなど通常のデータ読み取りとは異なるデータ読み取り方式によってのみ読み取り可能なデータ方式で書き込まれる。また、プロダクトマーク602、暗号化ボリュームID604の少なくとも一方は、前述した反射膜除去方式によって書き込まれる。また、暗号化ボリュームID604はIDライター260毎に異なるデータであり、プロダクトマーク602も、シリアル番号＋デジタル署名＋公開鍵証明書、製造日時＋デジタル署名＋公開鍵証明書とした場合は、ディスク1枚毎に異なるデータとされる。
- [0134] これらのデータを記録した情報記録媒体600は、ユーザデバイスとしての情報処理装置(再生装置)700にセットされ、所定のデータ再生アプリケーションを実行することで、予め設定された処理シーケンスが実行されてコンテンツの再生が行なわれることになる。情報記録媒体(ディスク)600に格納されたデータの読み取り、コンテンツ再生を実行する情報処理装置(再生装置)700の処理について説明する。
- [0135] 情報処理装置(再生装置)700は、まず、ステップS351において、情報処理装置(再生装置)700のメモリに格納されたデバイスキー(Kd)701を適用して情報記録媒体600から読み出したMKB601の処理を実行してメディアキー(Km)を取得する。なお、MKB601からメディアキー(Km)を取得するためには、有効なライセンスを持つ情報処理装置に格納されたデバイスキー(Kd)を適用することが必要である。無効化(リボーク処理)されたユーザデバイスにおいては、メディアキー(Km)の取得が不可能となる。
- [0136] 次に、ステップS352において、情報記録媒体600から読み出した暗号化ボリュームID604を、情報記録媒体600から読み出したマスターキー603を適用して復号しボリュームIDを算出する。次に、ステップS353において、情報記録媒体600から読み出したプロダクトマーク602のハッシュ値を算出し、ステップS354において、ボリュームIDとの演算(排他論理和)を実行し、さらに、ステップS355において、MKB処理によって取得したメディアキー(Km)と連結した後、ステップS356で連結データのハッシュ値を算出する。

- [0137] この結果、ボリュームユニークキー (Kvu) が生成される。ステップS352～S356の処理は、ディスク製造工場におけるステップS301～S305の処理と同様の処理であり、ボリュームユニークキー (Kvu) が生成される。
- [0138] 次に、ステップS357において、情報記録媒体600から読み出した暗号化キー605をボリュームユニークキー (Kvu) で復号し、ステップS358において、情報記録媒体600から読み出した利用制御情報606のハッシュ値を算出して、ステップS359において、ステップS357の復号結果と演算 (排他論理和) を実行して、タイトルキーを算出する。
- [0139] ステップS357～S359の処理は、ディスク製造工場におけるステップS306～S308の処理に対応する処理であり、タイトルキーが生成される。
- [0140] 次に、ステップS360において、生成したタイトルキーを適用して、情報記録媒体600から読み出した暗号化コンテンツ607の復号処理を実行してコンテンツ750を生成、出力する。
- [0141] このように、情報記録媒体600に格納された暗号化コンテンツの復号には、MKBからメディアキー (Km) を取得することの他に、情報記録媒体600に格納されたプロダクトマーク602、マスターキー603、暗号化ボリュームID604など、特殊なデータ記録方式によって記録されたデータを正確に読み取ることが必要となる。反射膜除去方式によって記録されたプロダクトマーク602、または暗号化ボリュームID604は、ピット形状の物理的コピーを実行して生成した海賊版ディスクからは正確なデータ読み取りが実行されず、コンテンツの復号は不可能になる。
- [0142] 次に、図19を参照して、暗号化ボリュームIDの暗号鍵としてマスターキーハッシュ値を適用した構成例について説明する。図19において図18との差異部分を中心として説明する。
- [0143] マスターキー503は、図7に示すフォーマッタ230において生成されるマスターキー503であり、ステップS401において、メディアキー505を適用してハッシュ値が算出され、ステップS404において、マスターキーハッシュ値を適用して、ボリュームID504とプロダクトマーク502のハッシュ値との連結データに対する暗号化が実行されて暗号化ボリュームID624として記録される。

[0144] ディスク製造工場500におけるその他の処理は、図18を参照して説明したと同様の処理であり、説明を省略する。

[0145] 図19に示す処理例においても、情報記録媒体(ディスク)600には、図に示すように、メディアキー(Km)を格納した暗号鍵ブロックとしてのMKB621、

(a)公開鍵証明書

(b)シリアル番号+デジタル署名+公開鍵証明書

(c)製造日時+デジタル署名+公開鍵証明書

のいずれかによって構成されるプロダクトマーク622、

マスターキー623、

暗号化ボリュームID624、

暗号化キー625、

利用制御情報626、

暗号化コンテンツ627

の各データが格納される。

[0146] これらのデータ中、マスターキー623は、サイドチャネル方式、ROMマーク記録方式などの、コンテンツの読み取りなど通常のデータ読み取りとは異なるデータ読み取り方式によってのみ読み取り可能なデータ方式で書き込まれる。また、プロダクトマーク622、暗号化ボリュームID624の少なくとも一方は、前述した反射膜除去方式によって書き込まれる。また、暗号化ボリュームID624はディスク一枚毎に異なるデータであり、プロダクトマーク622も、シリアル番号+デジタル署名+公開鍵証明書、製造日時+デジタル署名+公開鍵証明書とした場合は、1枚毎に異なるデータとされる。

[0147] これらのデータを記録した情報記録媒体600は、ユーザデバイスとしての情報処理装置(再生装置)700にセットされ、所定のデータ再生アプリケーションを実行することで、予め設定された処理シーケンスが実行されてコンテンツの再生が行なわれることになる。情報記録媒体(ディスク)600に格納されたデータの読み取り、コンテンツ再生を実行する情報処理装置(再生装置)700の処理について、図18に示す処理との差異部分を中心として説明する。

[0148] 情報処理装置(再生装置)700の処理において、図18に示す処理との差異は、ス

テップS452において、情報記録媒体600から読み出したマスターキー623に対して、MKB621から取得したメディアキー(Km)を適用してハッシュ値を算出して、ステップS453において、マスターキーハッシュ値を適用して、情報記録媒体600から読み出した暗号化ボリュームID624の復号を実行してボリュームIDを算出する点である。その他の処理は、図18を参照して説明したと同様の処理であり、説明を省略する。

- [0149] この処理例でも、情報記録媒体600に格納された暗号化コンテンツの復号には、MKBからメディアキー(Km)を取得することの他に、情報記録媒体600に格納されたプロダクトマーク622、マスターキー623、暗号化ボリュームID624など、特殊なデータ記録方式によって記録されたデータを正確に読み取ることが必要となる。反射膜除去方式によって記録されたプロダクトマーク622、または暗号化ボリュームID624は、ピット形状の物理的コピーを実行して生成した海賊版ディスクからは正確なデータ読み取りが実行されず、コンテンツの復号は不可能になる。
- [0150] 図20を参照して、ユーザデバイスとしての情報処理装置(再生装置)700の構成について説明する。情報処理装置(再生装置)700は、暗号化コンテンツを記録した情報記録媒体からのデータ読み取りおよびコンテンツ再生処理を実行する。
- [0151] 情報処理装置(再生装置)700は、情報記録媒体からのデータ読み取りを実行するデータ取得部771と、データ取得部771の取得したデータに基づくデータ処理を実行してコンテンツ復号用の鍵を生成する鍵生成部772と、鍵生成部772の生成した鍵に基づいて暗号化コンテンツの復号処理を実行する復号処理部773とを有する。鍵生成部771は、図18、図19を参照して説明したように、ディスク製造エンティティ、またはディスク製造適用機器に対して発行された公開鍵証明書を含むプロダクトマークと、プロダクトマークに基づいて生成されるハッシュ値などのプロダクトマーク対応値と、ディスクの一定の集合に対して設定される識別子としてのボリュームIDとに基づく演算結果に対する暗号化データである暗号化ボリュームIDとを含む鍵生成情報をデータ取得部771から入力し、これらの鍵生成情報を適用したデータ処理を実行してコンテンツ復号用の鍵、すなわちタイトルキーを生成する。
- [0152] [4. ディスク検証処理]
- 次に、市場に流通するディスクの検証によって、海賊版ディスクを特定し、その出所

を追跡する処理について、図21、図22を参照して説明する。図21は、シリアル番号を各ディスクに書き込んだ場合の検証、追跡例であり、図22は、製造日時情報を各ディスクに書き込んだ場合の検証、追跡例である。

[0153] まず、図21を参照してシリアル番号を各ディスクに書き込んだ場合の検証、追跡例について説明する。

[0154] 図21の最上段にはディスク書き込みデータ800として、シリアル番号801、デジタル署名802、公開鍵証明書(PKC)803、暗号化ボリュームID804を示している。シリアル番号801、デジタル署名802、公開鍵証明書(PKC)803はプロダクトマークの構成データであり、プロダクトマーク、暗号化ボリュームID804は反射膜除去方式によって記録されているものとする。

[0155] 公開鍵証明書(PKC)803には、レプリケータID811、IDライターID812、公開鍵813、KIC電子署名814が記録されている。

[0156] まず、市場のディスクを検証する場合、ステップS501において、プロダクトマークの構成要素である公開鍵証明書(PKC)803から公開鍵813を取得して、プロダクトマークの構成要素であるデジタル署名802を読み出して、署名検証処理を行なう。この署名検証処理によって、シリアル番号801の改竄検証が可能となる。

[0157] シリアル番号801の改竄が明らかになった場合、それは不正に運用されたIDライターの利用による海賊盤ディスクの市場の流通を意味する。すなわち、シリアル番号801の改ざん検証により、海賊盤ディスクの流通を検知することが可能となる。

[0158] 同様に、公開鍵証明書(PKC)803に格納されたKIC電子署名814の署名検証をKIC公開鍵821を適用して実行し、公開鍵証明書(PKC)803の改竄の有無を検証し、改竄があると判定された場合は、不正に運用されたIDライターによる海賊盤ディスクが市場に流通していると判定することができる。

[0159] また、公開鍵証明書(PKC)803に格納されたKIC電子署名814の署名検証をKIC公開鍵821を適用して実行し、公開鍵証明書(PKC)803の改竄がないと判定された場合、ステップS503において、不正機器の登録情報であるリボケーションリスト(CRL)822を適用して、リボケーション状況判定を行い、ディスクの製造機器としてのレプリケータや、IDライターがリボークされた機器であるか否かを判定することができる。

。

- [0160] また、ステップS521では、ディスク製造工場への発注データベースを参照して発注数量を確認することで、工場の水増し生産を検証することが可能となる。水増し生産が明らかになった場合、公開鍵証明書(PKC)803に記録されたレプリケータID811、IDライターID812が特定されるので、これらのIDに対応する機器が水増し生産に関係したと判定することができる。また、ステップS522では、シリアル番号と個人情報をバインドしたユーザ登録データベースを参照し、シリアル番号の重複を調べることで複製ディスクの流通を検証することが可能となる。
- [0161] 図22は、製造日時情報を各ディスクに書き込んだ場合の検証、追跡例である。図22の最上段にはディスク書き込みデータ850として、製造日時851、デジタル署名802、公開鍵証明書(PKC)803、暗号化ボリュームID804を示している。製造日時851、デジタル署名802、公開鍵証明書(PKC)803はプロダクトマークの構成データであり、プロダクトマーク、暗号化ボリュームID804は反射膜除去方式によって記録されているものとする。
- [0162] ステップS531の処理は、プロダクトマークの構成要素である公開鍵証明書(PKC)803から公開鍵813を取得して、プロダクトマークの構成要素であるデジタル署名802を読み出して、署名検証処理を行なう。この署名検証処理によって、製造日時851の改竄検証が可能となる。
- [0163] 製造日時851の改竄が明らかになった場合、それは不正に運用されたIDライターの利用による海賊盤ディスクの市場の流通を意味する。すなわち、シリアル番号801の改ざん検証により、海賊盤ディスクの流通を検知することが可能となる。ステップS502, S503の処理は、図21を参照して説明した処理と同様であるので説明を省略する。
- [0164] ステップS532の処理は、ディスク製造工場への発注データベースを参照して納品後などの発注契約上ありえない製造年月日を確認することで、工場の水増し生産を検証する処理である。水増し生産が明らかになった場合、公開鍵証明書(PKC)803に記録されたレプリケータID811、IDライターID812が特定されるので、これらのIDに対応する機器が水増し生産に関係したと判定することができる。

[0165] このように、本発明の構成では、

(a)公開鍵証明書

(b)シリアル番号＋デジタル署名＋公開鍵証明書

(c)製造日時＋デジタル署名＋公開鍵証明書

のいずれかによって構成されるプロダクトマークと、

上記のプロダクトマークに基づく例えばハッシュ値と、ボリュームIDとを含む連結データをマスターキーまたはマスターキーハッシュ値によつての暗号化して生成した暗号化ボリュームIDを情報記録媒体に記録する構成とし、少なくともプロダクトマーク、暗号化ボリュームIDの一方は、反射膜除去方式によつて記録する構成としたので、海賊版の生成が困難となり、海賊盤ディスクの市場での流通が検知可能となり、また、万が一、海賊版ディスクが流通した場合においても、関係した製造機器を特定することが可能となる。なお、図示されないが、(b)において、シリアル番号のみ、デジタル署名のみ、またはシリアル番号＋デジタル署名をプロダクトマークの対象とした場合も発明の効果は等しく得られ、また、(c)において、製造日時のみ、デジタル署名のみ、製造日時＋デジタル署名をプロダクトマークの対象とした場合も同様に発明の効果は等しく得られる。

[0166] [5. 情報処理装置の構成]

次に、図23を参照して、情報記録媒体(ディスク)に対する記録データの生成を実行するIDライターに相当するデータ記録装置としての情報処理装置、および情報記録媒体(ディスク)からのデータ再生を実行する再生装置としての情報処理装置のハードウェア構成例について説明する。

[0167] 情報処理装置900は、データ記録またはコンテンツ再生処理を実行するプログラム、暗号鍵生成処理プログラムなどの各種プログラムに従ったデータ処理を実行するCPU901、プログラム、パラメータ等の記憶領域としてのROM902、メモリ903、信号を入出力する入出力I/F904、暗号鍵生成、コンテンツの暗号化、復号処理など各種の暗号処理を実行する暗号処理手段905を有し、バス910に各ブロックが接続されている。

[0168] データ記録部906は、IDライターとしてのデータ記録装置の構成要素であり、反射

膜除去方式によるデータ記録が可能な構成を持つ。記録媒体I/F907は、データ再生処理を実行する情報処理装置の構成要素であり、暗号化コンテンツ、その他のデータを格納したディスクからのデータ読み取りを実行する。

- [0169] IDライターとしてのデータ記録装置は、マスターキー、ボリュームID、シリアル開始番号、発注枚数などの秘密情報を、入出力I/F904を介して入力する。ROM902またはメモリ903には、これらのデータの他、公開鍵証明書、秘密鍵が格納される。また、再生処理を実行する情報処理装置であれば、ROM902またはメモリ903には、デバイスキーなどが格納される。暗号化処理、復号処理、鍵生成処理は、暗号化処理手段907によって、例えば、AESアルゴリズムなどを適用して実行される。
- [0170] なお、図23に示す構成は、本発明に従った処理を行うために必要な構成を示すものであり、本発明に係る処理以外の構成要素については省略して示してある。例えば、コンテンツ再生を実行する情報処理装置の場合は、図23に示す構成の他、例えば、アナログ信号を入出力するインタフェース、A/D、D/Aコンバータ、MPEGデータのエンコード、デコード処理を実行するMPEGコーデック、TS (Transport Stream)・PS (Program Stream)処理を実行するTS・PS処理手段などの構成を持つ。
- [0171] 以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、特許請求の範囲の欄を参酌すべきである。
- [0172] なお、明細書中において説明した一連の処理はハードウェア、またはソフトウェア、あるいは両者の複合構成によって実行することが可能である。ソフトウェアによる処理を実行する場合は、処理シーケンスを記録したプログラムを、専用のハードウェアに組み込まれたコンピュータ内のメモリにインストールして実行させるか、あるいは、各種処理が実行可能な汎用コンピュータにプログラムをインストールして実行させることが可能である。
- [0173] 例えば、プログラムは記録媒体としてのハードディスクやROM (Read Only Memory)に予め記録しておくことができる。あるいは、プログラムはフレキシブルディスク、CD

—ROM(Compact Disc Read Only Memory), MO(Magneto optical)ディスク, DVD(Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体に、一時的あるいは永続的に格納(記録)しておくことができる。このようなリムーバブル記録媒体は、いわゆるパッケージソフトウェアとして提供することができる。

[0174] なお、プログラムは、上述したようなリムーバブル記録媒体からコンピュータにインストールする他、ダウンロードサイトから、コンピュータに無線転送したり、LAN(Local Area Network)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを受信し、内蔵するハードディスク等の記録媒体にインストールすることができる。

[0175] なお、明細書に記載された各種の処理は、記載に従って時系列に実行されるのみならず、処理を実行する装置の処理能力あるいは必要に応じて並列的にあるいは個別に実行されてもよい。また、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

産業上の利用可能性

[0176] 以上、説明したように、本発明の構成によれば、ディスク製造エンティティ、またはディスク製造機器に対して発行された公開鍵証明書を含むプロダクトマークと、プロダクトマークに基づいて生成されるハッシュ値などのプロダクトマーク対応値と、製造ディスクの一定の集合に対して設定される識別子としてのボリュームIDとに基づく演算によって算出される暗号化ボリュームIDを生成し、これらのプロダクトマークおよび暗号化ボリュームIDをディスクに格納する暗号化コンテンツの復号用鍵の生成情報としてディスク各々に記録するとともに、これらのプロダクトマークと暗号化ボリュームIDの少なくともいずれかのデータを反射膜除去記録方式によって記録する構成としたので、市販の正当なディスクに基づいて、ピット形状を物理的にコピーした海賊版ディスクからは、鍵生成情報としてのプロダクトマークまたは暗号化ボリュームIDを読み取ることができず、コンテンツの不正な再生や利用を防止することができる。

[0177] さらに、本発明の構成によれば、プロダクトマークに、情報記録媒体製造エンティティ、または情報記録媒体製造機器の識別情報を含む公開鍵証明書を含める構成としたので、ピット形状の物理的コピー以外の例えばRF信号読み取りデータに基づい

て生成した海賊版ディスクについては、ディスクから公開鍵証明書を取得することで、海賊版ディスクの製造に関係した情報記録媒体製造エンティティや情報記録媒体製造機器を追跡し特定することが可能となる。

請求の範囲

- [1] 暗号化コンテンツを格納したディスクのディスク製造方法であり、
ディスク製造エンティティ、またはディスク製造機器に対応する公開鍵証明書であり、
ディスク製造エンティティ、またはディスク製造機器の識別情報を含む公開鍵証明書を構成データとするプロダクトマークを、前記暗号化コンテンツの復号に適用する鍵の生成情報として生成するプロダクトマーク生成ステップと、
前記プロダクトマークに基づいて生成されるプロダクトマーク対応値と、製造ディスクの一定の集合に対して設定される識別子としてのボリュームIDとに基づく演算結果に対する暗号化データとしての暗号化ボリュームIDを、前記暗号化コンテンツの復号に適用する鍵の生成情報として生成する暗号化ボリュームID生成ステップと、
前記プロダクトマークと前記暗号化ボリュームIDを、各ディスク個別に記録するステップであり、プロダクトマークと暗号化ボリュームIDの少なくともいずれかのデータを反射膜除去記録方式によって記録する個別データ記録ステップと、
を有することを特徴とするディスク製造方法。
- [2] 前記プロダクトマーク生成ステップは、
前記公開鍵証明書に加え、製造ディスク毎に設定されるシリアル番号、および該シリアル番号に対応して設定されるデジタル署名データを構成データとするプロダクトマークを生成するステップであり、
前記暗号化ボリュームID生成ステップは、
前記公開鍵証明書と、シリアル番号、および該シリアル番号に対応して設定されるデジタル署名データとを含むプロダクトマークに基づいて生成されるプロダクトマーク対応値と、前記ボリュームIDに基づいて暗号化ボリュームIDを生成するステップであることを特徴とする請求項1に記載のディスク製造方法。
- [3] 前記プロダクトマーク生成ステップは、
前記公開鍵証明書に加え、製造ディスクの製造日時情報、および該製造日時情報に対応して設定されるデジタル署名データを構成データとするプロダクトマークを生成するステップであり、
前記暗号化ボリュームID生成ステップは、

前記公開鍵証明書と、製造日時情報、および該製造日時情報に対応して設定されるデジタル署名データとを含むプロダクトマークに基づいて生成されるプロダクトマーク対応値と、前記ボリュームIDに基づいて暗号化ボリュームIDを生成するステップであることを特徴とする請求項1に記載のディスク製造方法。

- [4] 前記暗号化ボリュームID生成ステップは、
前記プロダクトマークに基づくハッシュ値として生成されるプロダクトマーク対応値と、前記ボリュームIDとに基づいて暗号化ボリュームIDを生成するステップであることを特徴とする請求項1に記載のディスク製造方法。
- [5] 暗号化ボリュームID生成ステップは、
前記プロダクトマーク対応値と、ボリュームIDとに基づく演算による算出値を、製造ディスクの一定の集合に対して設定されるマスターキー、または該マスターキーのハッシュ値を適用した暗号化処理によって暗号化ボリュームIDを生成するステップであることを特徴とする請求項1に記載のディスク製造方法。
- [6] 前記ディスク製造方法は、さらに、
前記マスターキーを、ディスクに記録する暗号化コンテンツの記録態様と異なる変調処理を施して記録するステップを有することを特徴とする請求項5に記載のディスク製造方法。
- [7] 前記ディスク製造方法において、
前記プロダクトマーク、および前記暗号化ボリュームIDは、ディスク製造に適用する原盤またはスタンプに対する記録情報とすることなく、前記個別データ記録ステップにおいて、各製造ディスク個別に生成し記録することを特徴とする請求項1に記載のディスク製造方法。
- [8] 情報記録媒体に対するデータ記録処理を実行するデータ記録装置であり、
情報記録媒体製造エンティティ、または情報記録媒体製造機器に対応する公開鍵証明書であり、情報記録媒体製造エンティティ、または情報記録媒体製造機器の識別情報を含む公開鍵証明書を構成データとするプロダクトマークを、前記情報記録媒体に記録する暗号化コンテンツの復号に適用する鍵の生成情報として生成するプロダクトマーク生成部と、

前記プロダクトマークに基づいて生成されるプロダクトマーク対応値と、製造する情報記録媒体の一定の集合に対して設定される識別子としてのボリュームIDとに基づく演算結果に対する暗号化データとしての暗号化ボリュームIDを、前記情報記録媒体に記録する暗号化コンテンツの復号に適用する鍵の生成情報として生成する暗号化ボリュームID生成部と、

前記プロダクトマークと前記暗号化ボリュームIDを各情報記録媒体個別に記録するデータ記録部であり、プロダクトマークと暗号化ボリュームIDの少なくともいずれかのデータを反射膜除去記録方式によって記録するデータ記録部と、

を有することを特徴とするデータ記録装置。

[9] 前記プロダクトマーク生成部は、

前記公開鍵証明書に加え、製造する情報記録媒体毎に設定されるシリアル番号、および該シリアル番号に対応して設定されるデジタル署名データを構成データとするプロダクトマークを生成する構成であり、

前記暗号化ボリュームID生成部は、

前記公開鍵証明書と、シリアル番号、および該シリアル番号に対応して設定されるデジタル署名データとを含むプロダクトマークに基づいて生成されるプロダクトマーク対応値と、前記ボリュームIDに基づいて暗号化ボリュームIDを生成する構成であることを特徴とする請求項8に記載のデータ記録装置。

[10] 前記プロダクトマーク生成部は、

前記公開鍵証明書に加え、製造する情報記録媒体の製造日時情報、および該製造日時情報に対応して設定されるデジタル署名データを構成データとするプロダクトマークを生成する構成であり、

前記暗号化ボリュームID生成部は、

前記公開鍵証明書と、製造日時情報、および該製造日時情報に対応して設定されるデジタル署名データとを含むプロダクトマークに基づいて生成されるプロダクトマーク対応値と、前記ボリュームIDに基づいて暗号化ボリュームIDを生成する構成であることを特徴とする請求項8に記載のデータ記録装置。

[11] 暗号化コンテンツを記録した情報記録媒体であり、

情報記録媒体製造エンティティ、または情報記録媒体製造機器に対応する公開鍵証明書であり、情報記録媒体製造エンティティ、または情報記録媒体製造機器の識別情報を含む公開鍵証明書を構成データとするデータであり、前記暗号化コンテンツの復号に適用する鍵の生成情報となるプロダクトマークと、

前記情報記録媒体に記録する暗号化コンテンツの復号に適用する鍵の生成情報であり、前記プロダクトマークに基づいて生成されるプロダクトマーク対応値と、製造される情報記録媒体の一定の集合に対して設定される識別子としてのボリュームIDとに基づく演算結果に対する暗号化データであり、前記暗号化コンテンツの復号に適用する鍵の生成情報となる暗号化ボリュームIDを格納し、

前記プロダクトマークまたは前記暗号化ボリュームIDの少なくともいずれかが反射膜除去記録方式によって記録された構成を有することを特徴とする情報記録媒体。

[12] 前記プロダクトマークは、

前記公開鍵証明書に加え、製造される情報記録媒体毎に設定されるシリアル番号、および該シリアル番号に対応して設定されるデジタル署名データを構成データとすることを特徴とする請求項11に記載の情報記録媒体。

[13] 前記プロダクトマークは、

前記公開鍵証明書に加え、製造される情報記録媒体毎に設定される製造日時情報、および該製造日時情報に対応して設定されるデジタル署名データを構成データとすることを特徴とする請求項11に記載の情報記録媒体。

[14] 暗号化コンテンツを記録した情報記録媒体からのデータ読み取りおよびコンテンツ再生処理を実行する情報処理装置であり、

情報記録媒体からのデータ読み取りを実行するデータ取得部と、

前記データ取得部の取得したデータに基づくデータ処理を実行してコンテンツ復号用の鍵を生成する鍵生成部と、

前記鍵生成部の生成した鍵に基づいて暗号化コンテンツの復号処理を実行する復号処理部とを有し、

前記鍵生成部は、

情報記録媒体製造エンティティ、または情報記録媒体製造機器に対応する公開鍵

証明書であり、情報記録媒体製造エンティティ、または情報記録媒体製造機器の識別情報を含む公開鍵証明書を構成データとするプロダクトマークと、

前記プロダクトマークに基づいて生成されるプロダクトマーク対応値と、情報記録媒体の一定の集合に対して設定される識別子としてのボリュームIDとに基づく演算結果に対する暗号化データである暗号化ボリュームIDと、

を含む鍵生成情報を前記データ取得部から入力し、該鍵生成情報を適用したデータ処理を実行してコンテンツ復号用の鍵を生成する構成であることを特徴とする情報処理装置。

- [15] 暗号化コンテンツを記録したディスクからのデータ読み取りおよびコンテンツ再生処理を実行する情報処理方法であり、

情報記録媒体からのデータ読み取りを実行するデータ取得ステップと、

前記データ取得部の取得したデータに基づくデータ処理を実行してコンテンツ復号用の鍵を生成する鍵生成ステップと、

前記鍵生成部の生成した鍵に基づいて暗号化コンテンツの復号処理を実行する復号処理ステップとを有し、

前記鍵生成ステップは、

情報記録媒体製造エンティティ、または情報記録媒体製造機器に対応する公開鍵証明書であり、情報記録媒体製造エンティティ、または情報記録媒体製造機器の識別情報を含む公開鍵証明書を構成データとするプロダクトマークと、

前記プロダクトマークに基づいて生成されるプロダクトマーク対応値と、情報記録媒体の一定の集合に対して設定される識別子としてのボリュームIDとに基づく演算結果に対する暗号化データである暗号化ボリュームIDと、

を含む鍵生成情報を入力し、該鍵生成情報を適用したデータ処理を実行してコンテンツ復号用の鍵を生成するステップであることを特徴とする情報処理方法。

- [16] 情報記録媒体に対するデータ記録処理をコンピュータ上において実行させるコンピュータ・プログラムであり、

情報記録媒体製造エンティティ、または情報記録媒体製造機器に対応する公開鍵証明書であり、情報記録媒体製造エンティティ、または情報記録媒体製造機器の識

別情報を含む公開鍵証明書を構成データとするプロダクトマークを、前記情報記録媒体に記録される暗号化コンテンツの復号に適用する鍵の生成情報として生成するプロダクトマーク生成ステップと、

前記プロダクトマークに基づいて生成されるプロダクトマーク対応値と、製造情報記録媒体の一定の集合に対して設定される識別子としてのボリュームIDとに基づく演算結果に対する暗号化データとして暗号化ボリュームIDを、前記情報記録媒体に記録される暗号化コンテンツの復号に適用する鍵の生成情報として生成する暗号化ボリュームID生成ステップと、

前記プロダクトマークと前記暗号化ボリュームIDを各情報記録媒体個別に記録するデータ記録部であり、プロダクトマークと暗号化ボリュームIDの少なくともいずれかのデータを反射膜除去記録方式によって記録するデータ記録ステップと、

を有することを特徴とするコンピュータ・プログラム。

[17] 暗号化コンテンツを記録したディスクからのデータ読み取りおよびコンテンツ再生処理をコンピュータ上において実行させるコンピュータ・プログラムであり、

情報記録媒体からのデータ読み取りを実行するデータ取得ステップと、

前記データ取得部の取得したデータに基づくデータ処理を実行してコンテンツ復号用の鍵を生成する鍵生成ステップと、

前記鍵生成部の生成した鍵に基づいて暗号化コンテンツの復号処理を実行する復号処理ステップとを有し、

前記鍵生成ステップは、

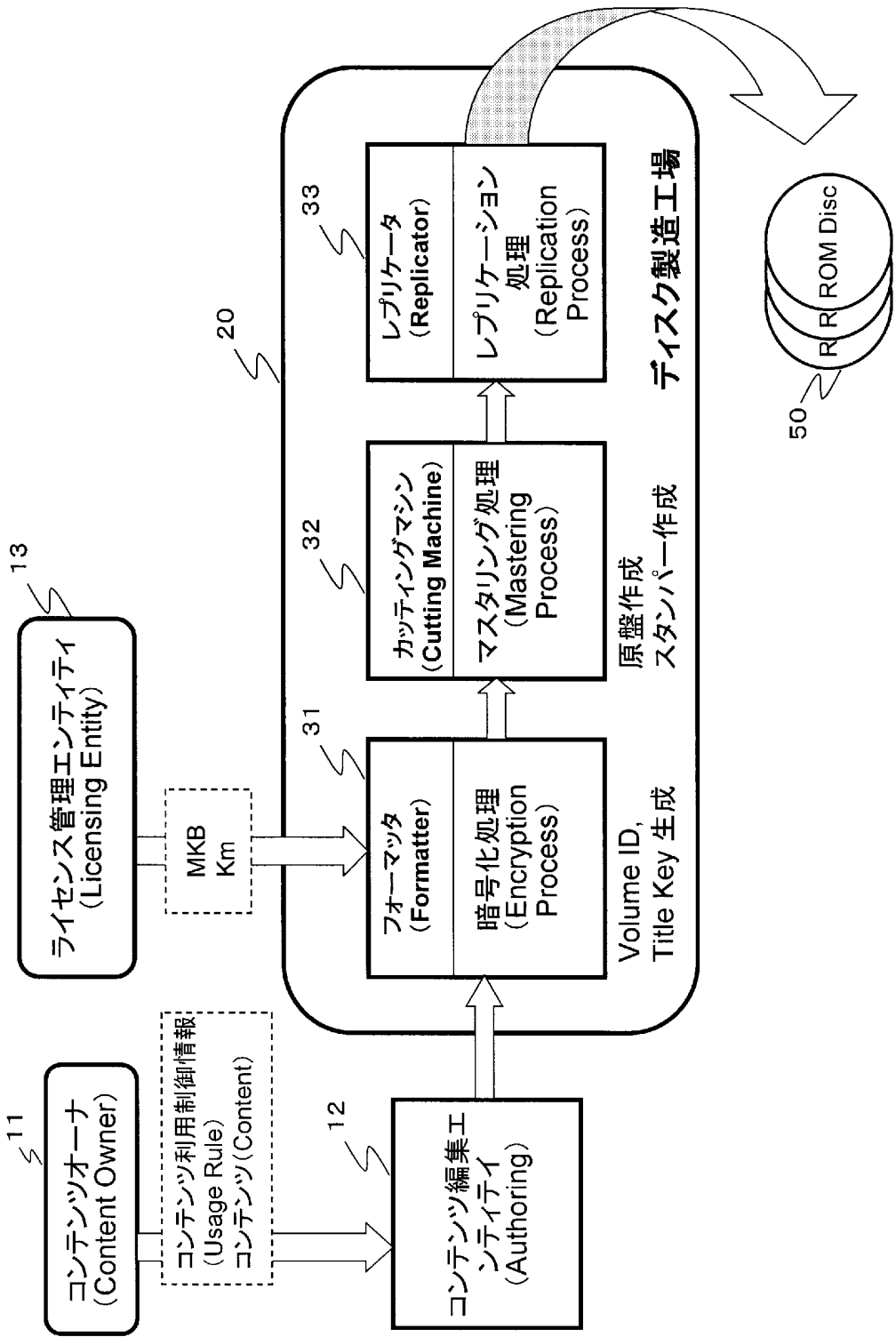
情報記録媒体製造エンティティ、または情報記録媒体製造機器に対応する公開鍵証明書であり、情報記録媒体製造エンティティ、または情報記録媒体製造機器の識別情報を含む公開鍵証明書を構成データとするプロダクトマークと、

前記プロダクトマークに基づいて生成されるプロダクトマーク対応値と、情報記録媒体の一定の集合に対して設定される識別子としてのボリュームIDとに基づく演算結果に対する暗号化データである暗号化ボリュームIDと、

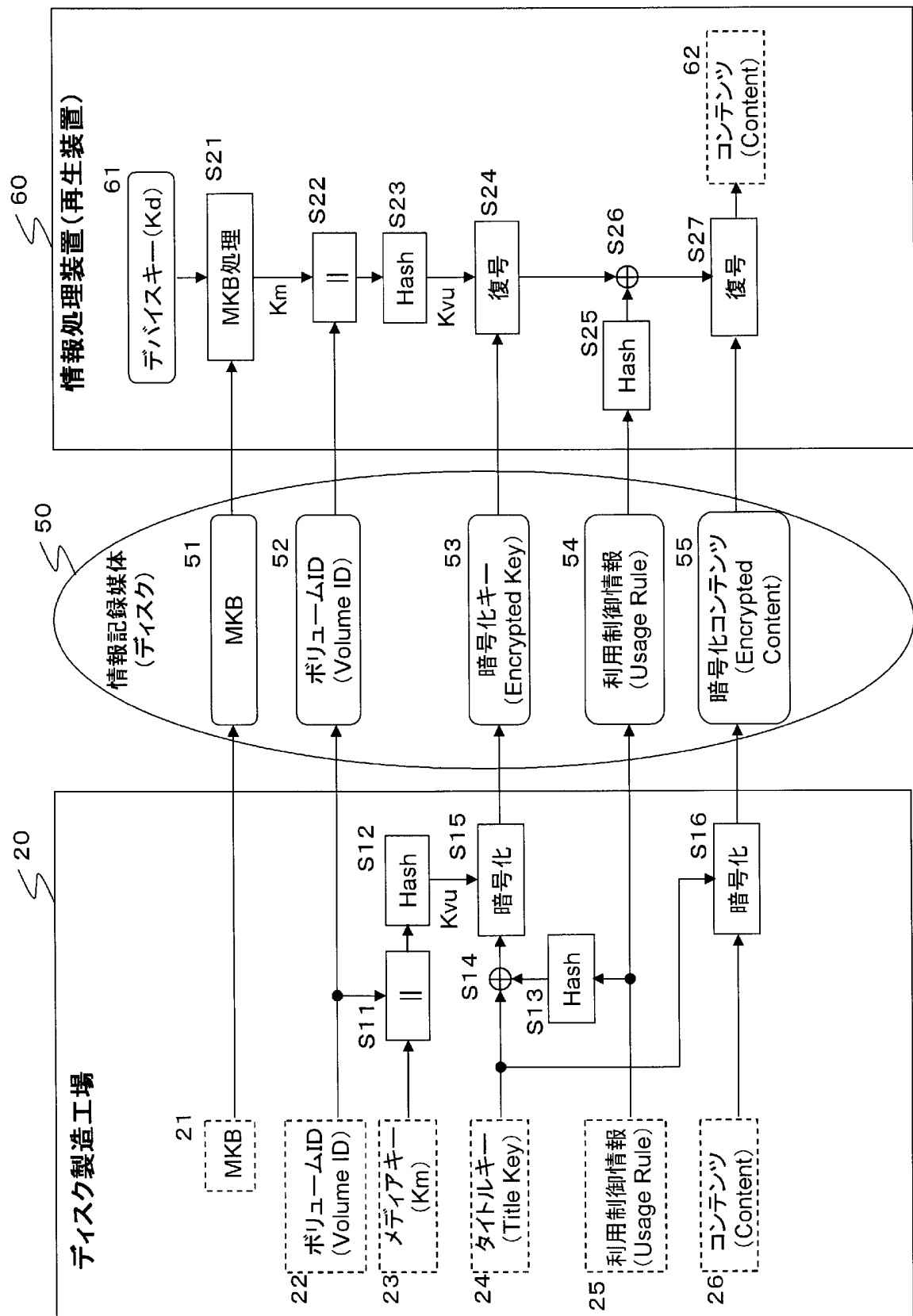
を含む鍵生成情報を入力し、該鍵生成情報を適用したデータ処理を実行してコンテンツ復号用の鍵を生成するステップであることを特徴とするコンピュータ・プログラム

o

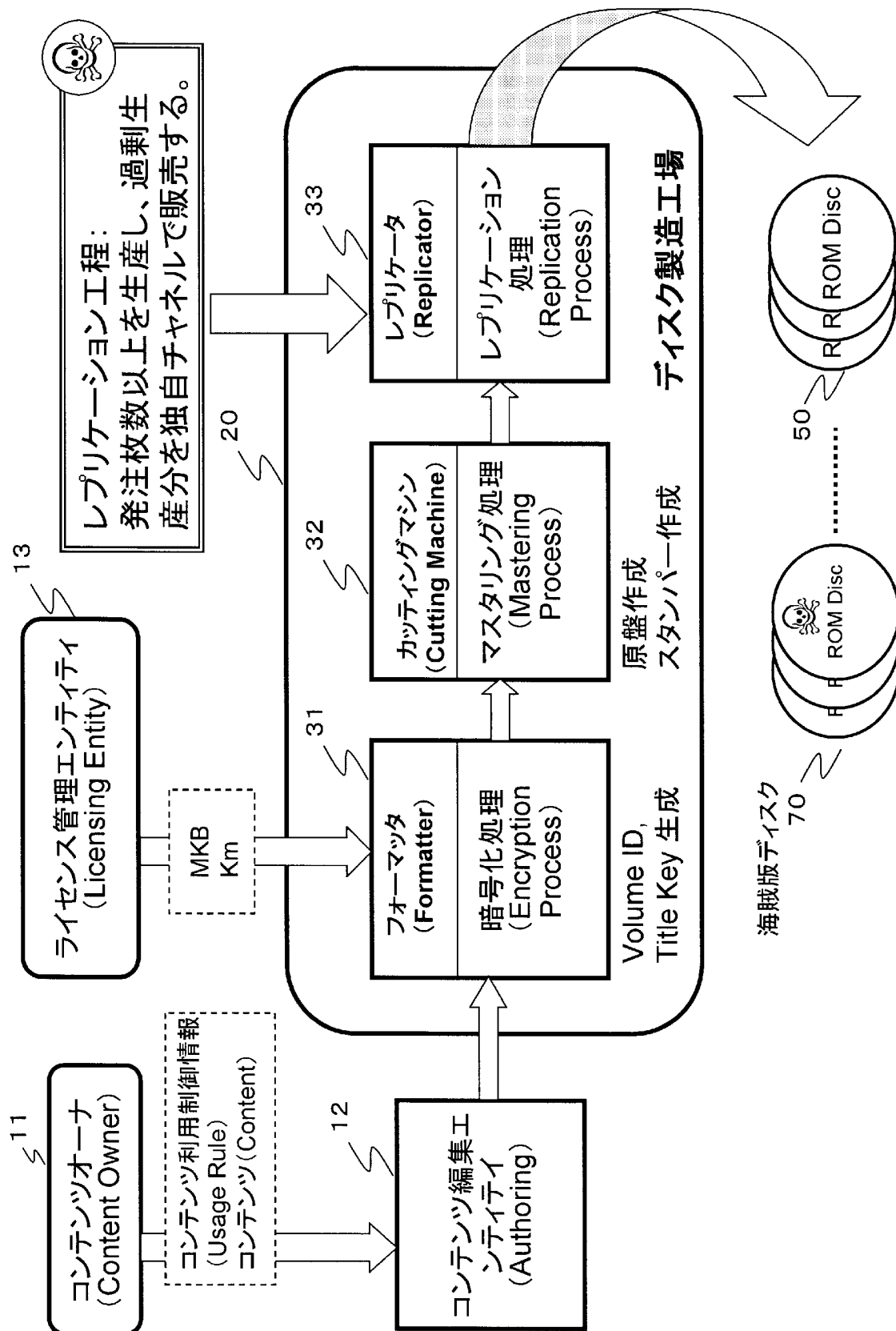
[図1]



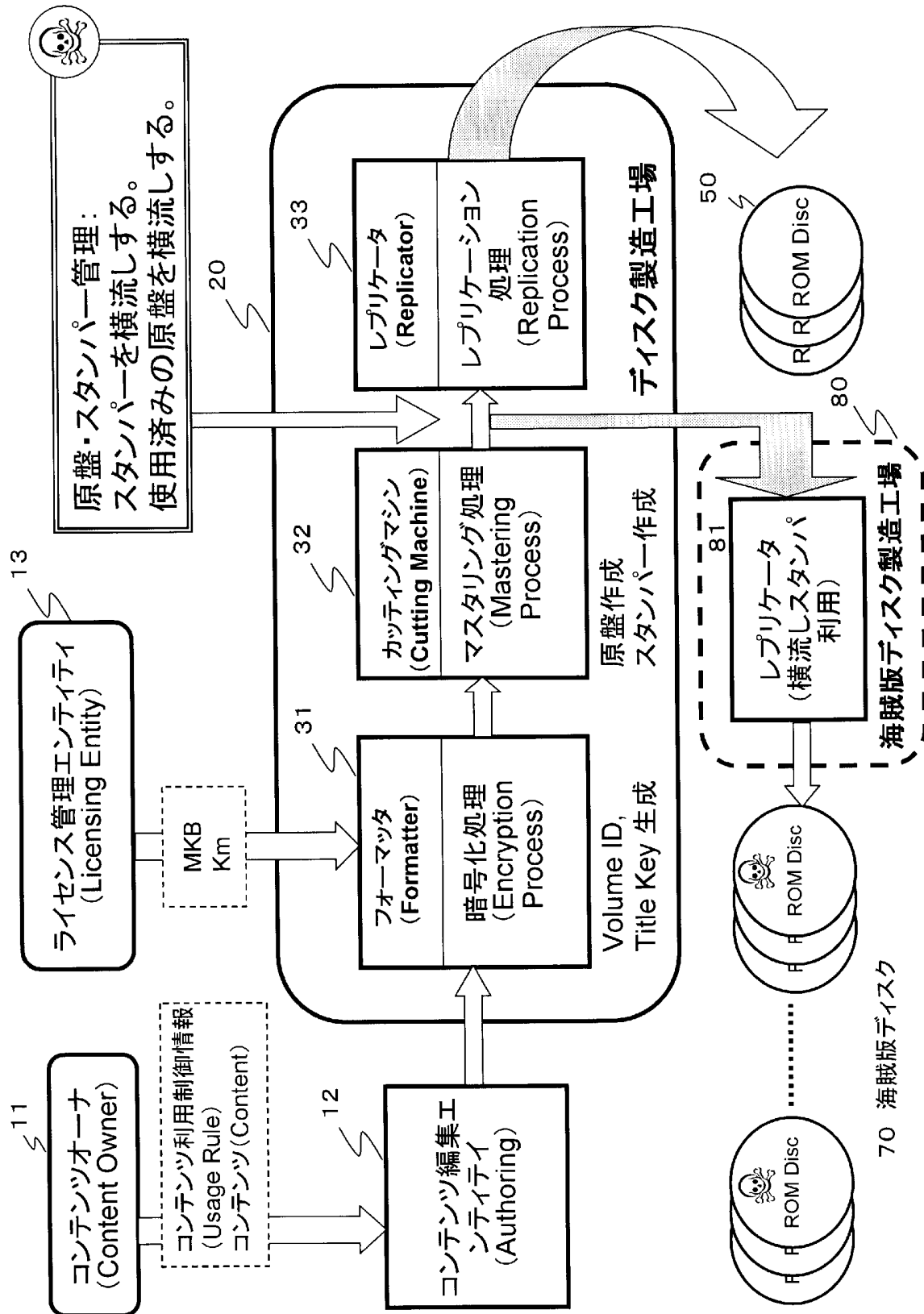
[図2]



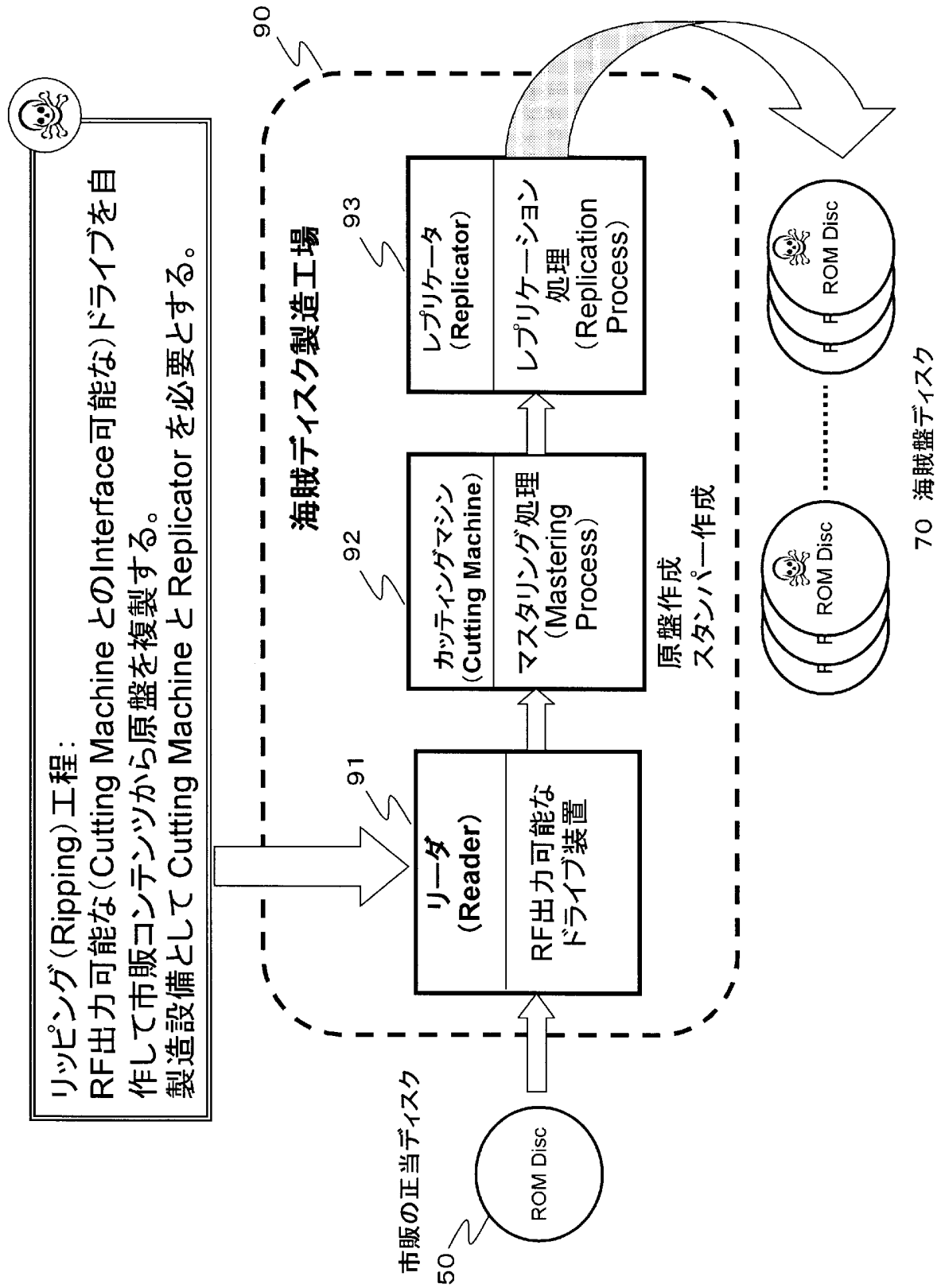
[図3]



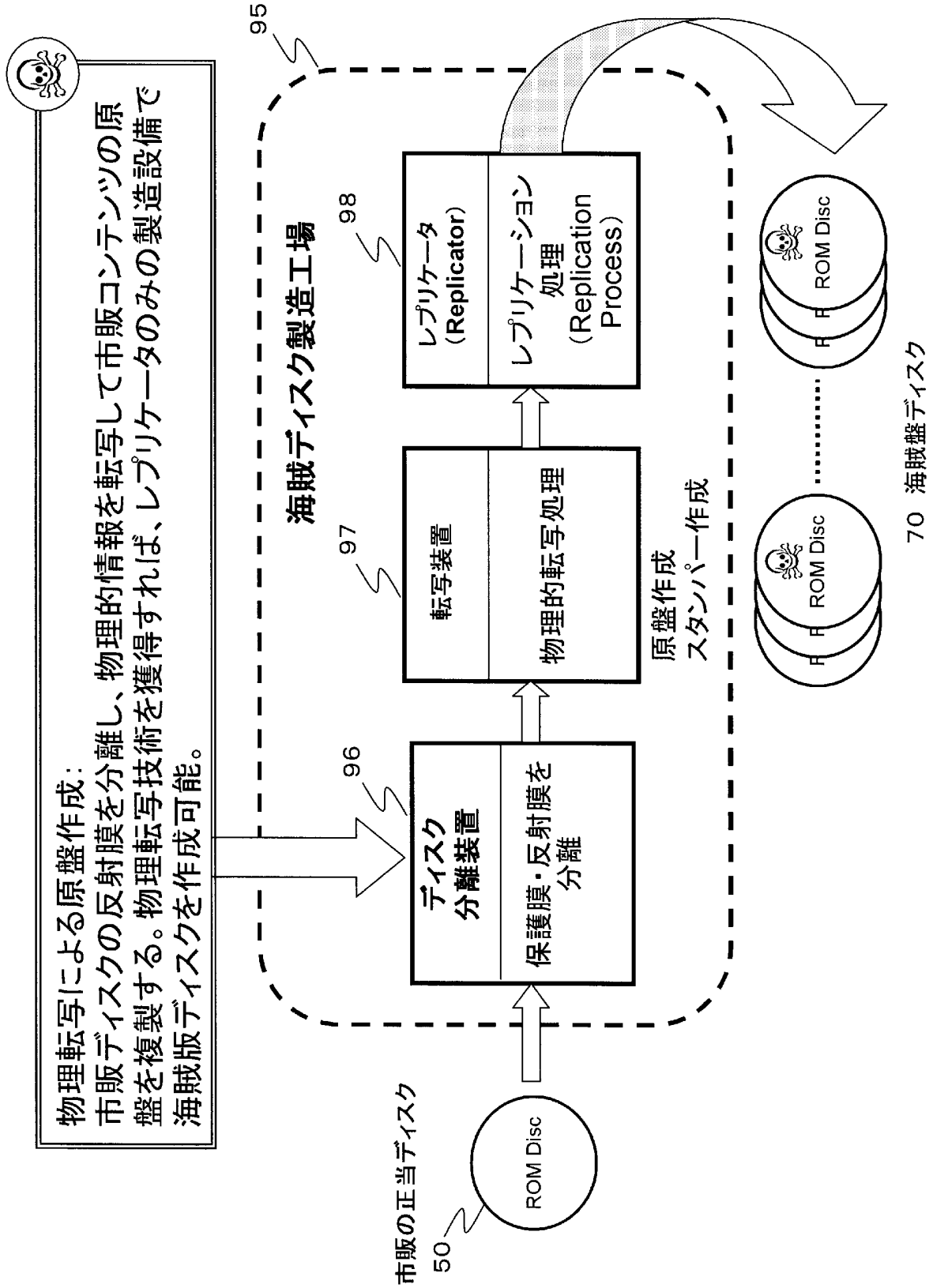
[図4]



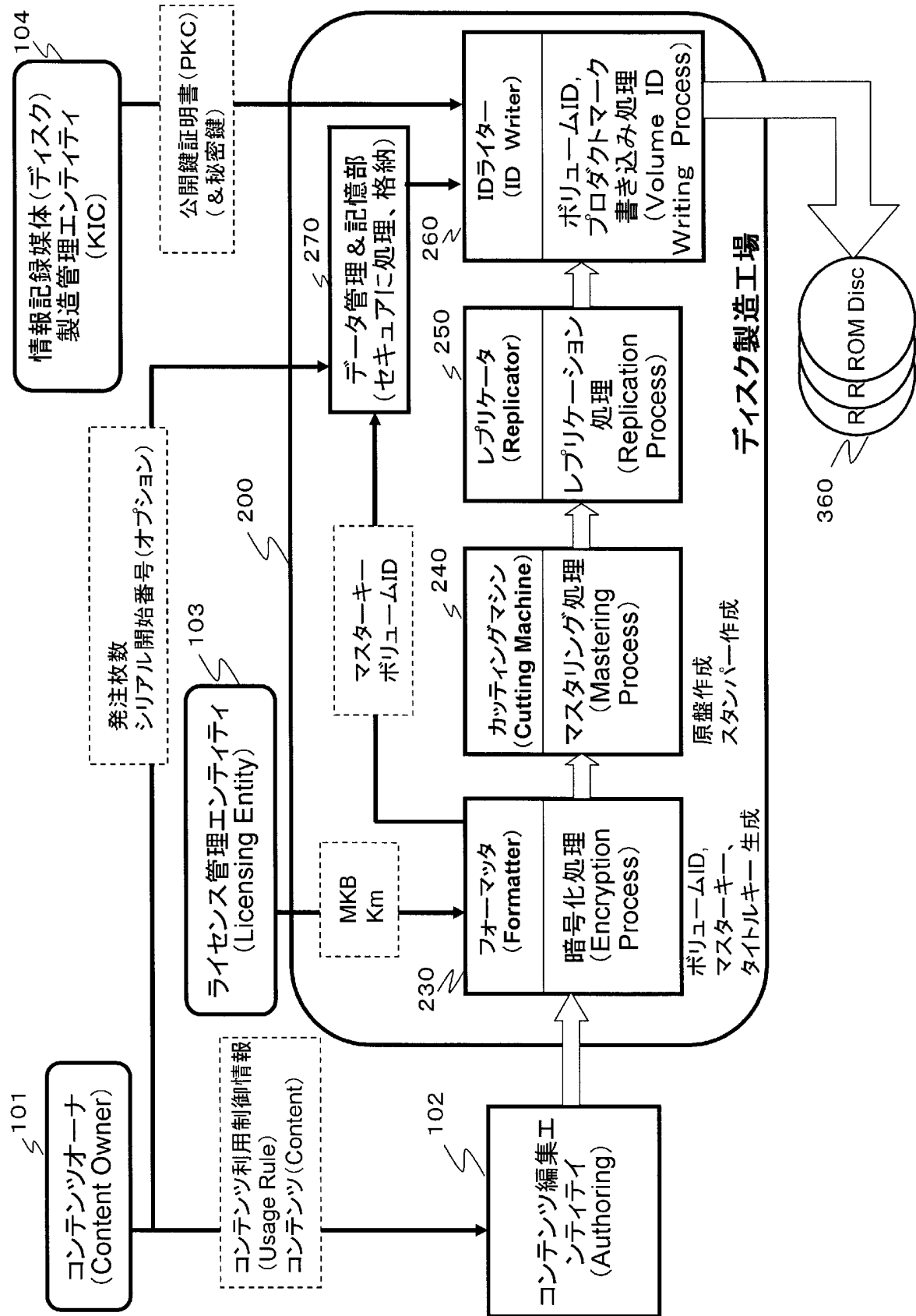
[図5]



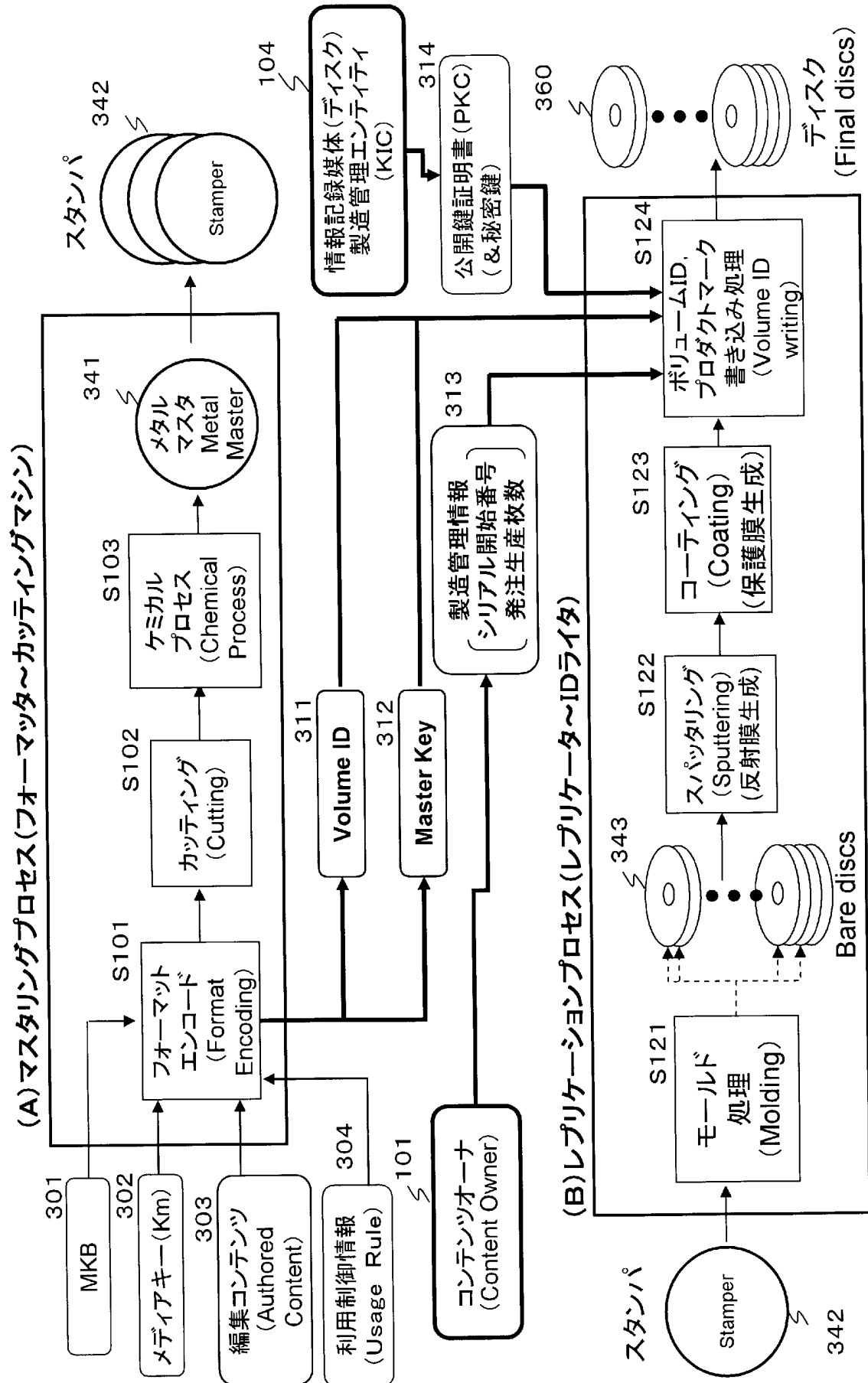
[図6]



[図7]



[図8]



[図9]

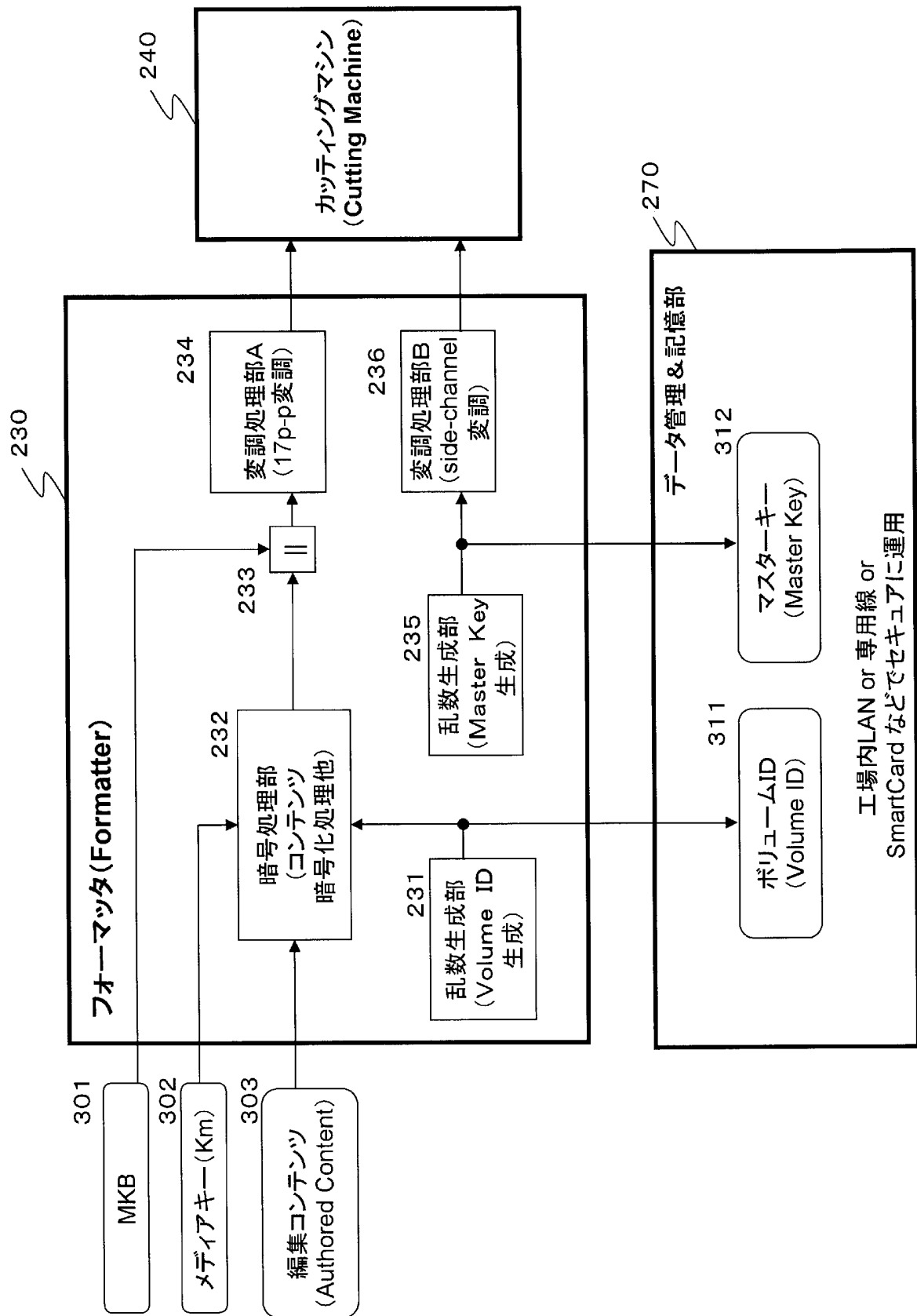


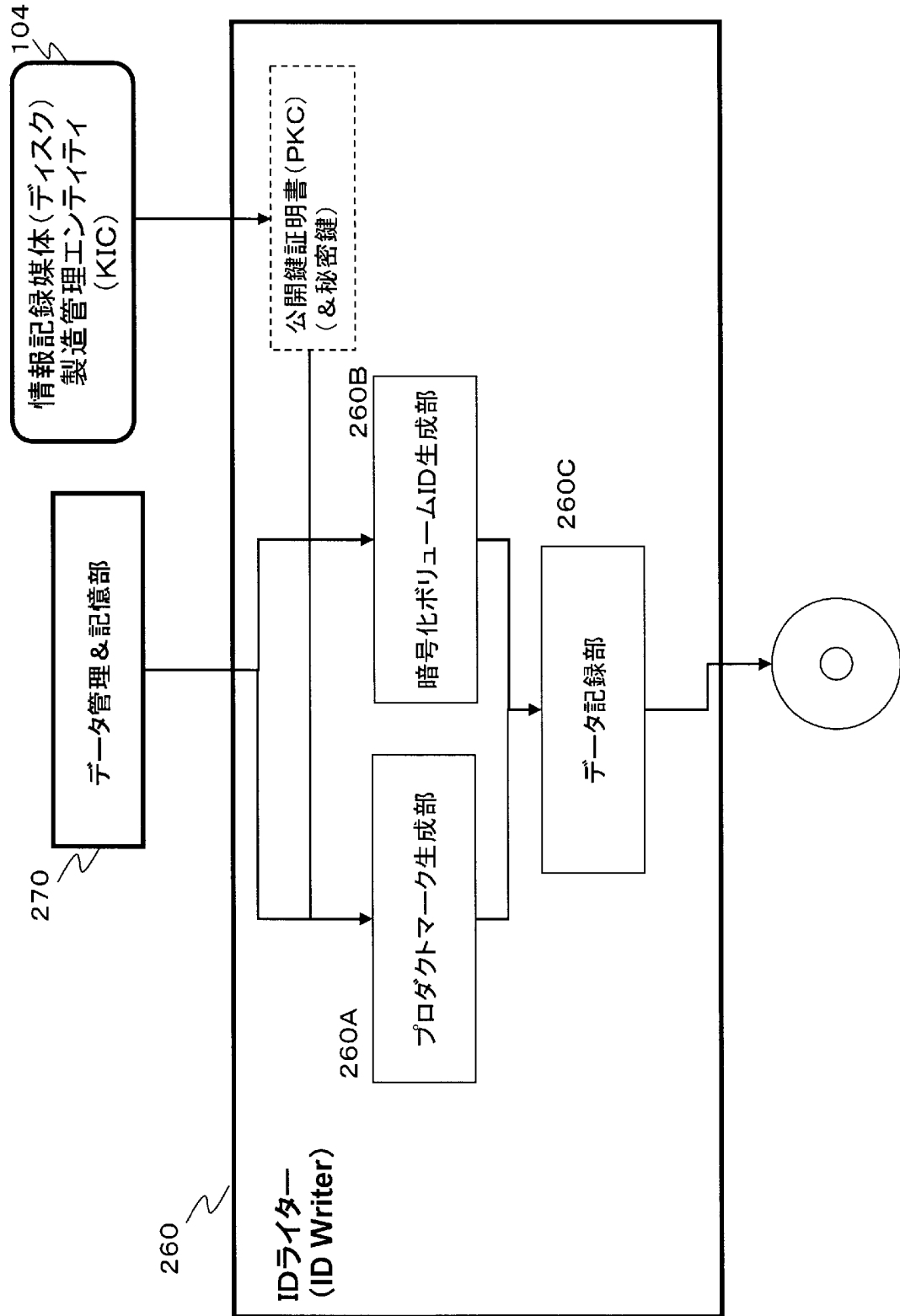
Figure 1 is a block diagram illustrating the system architecture. The system is divided into two main sections: the **フォーマッタ (Formatter)** (230) and the **データ管理 & 記憶部** (Data Management & Storage Unit) (270).

The **フォーマッタ (Formatter)** (230) receives three inputs: **MKB** (301), **メディアキー (Km)** (302), and **編集コンテンツ (Authorized Content)** (303). These inputs are processed by the **暗号処理部 (コンテンツ 暗号化処理他)** (232). The output of the encryption unit is fed into the **変調処理部A (17p-p変調)** (234) and the **変調処理部B (side-channel変調)** (236). The output of the 17p-p modulation unit (234) is sent to the **カッティングマシン (Cutting Machine)** (240). The output of the side-channel modulation unit (236) is also sent to the **カッティングマシン (Cutting Machine)** (240).

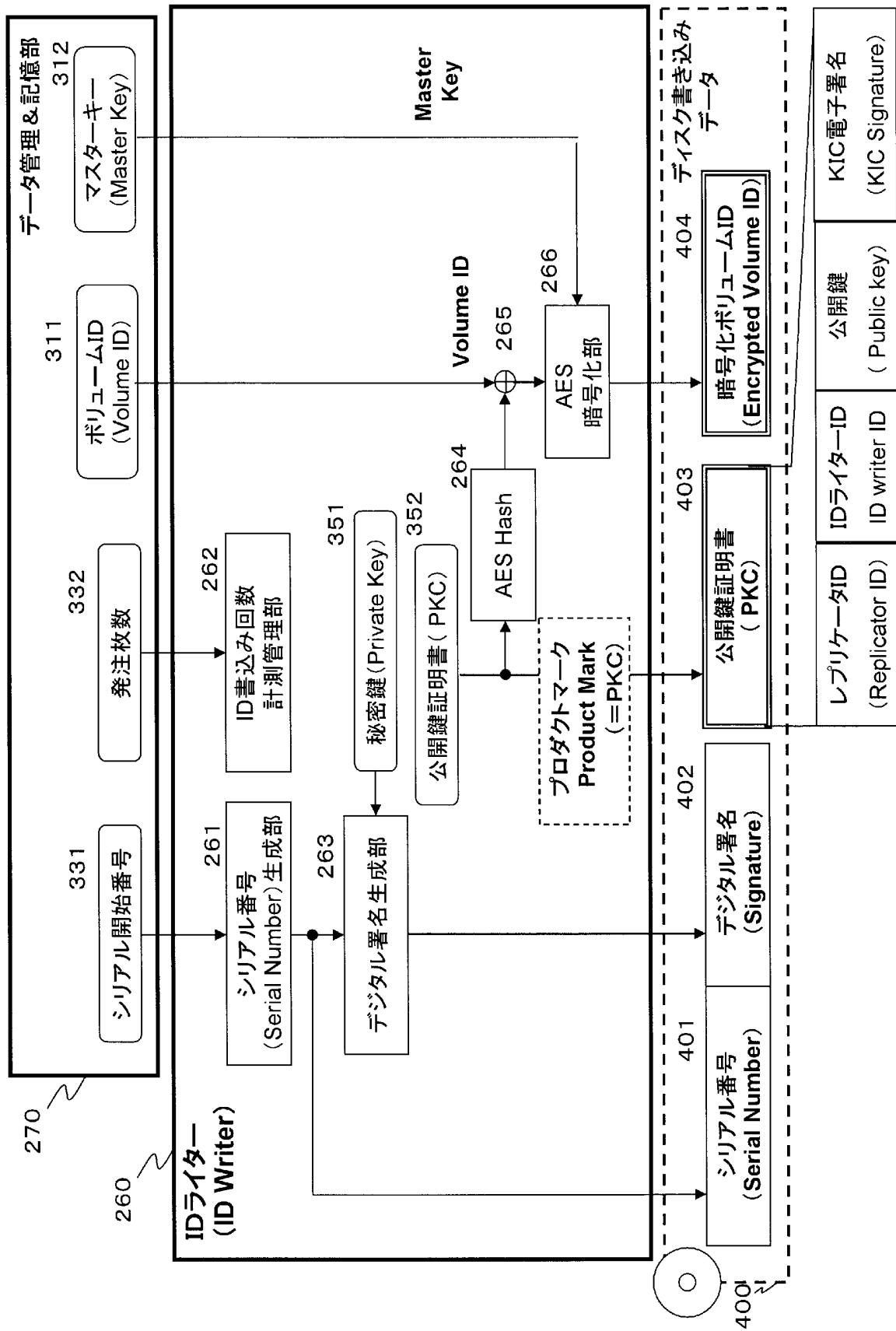
The **フォーマッタ (Formatter)** (230) also includes a **乱数生成部 (Volume ID生成)** (231) which outputs the **ボリュームID (Volume ID)** (311) to the **データ管理 & 記憶部** (270). Additionally, the **フォーマッタ (Formatter)** (230) includes a **乱数生成部 (Master Key生成)** (235) which outputs the **マスターキー** (237) to the **Hash** (237) and the **変調処理部B (side-channel変調)** (236). The **マスターキー** (237) is also used to generate the **マスターキーハッシュ値 (Hashed Master Key)** (321) in the **データ管理 & 記憶部** (270).

The **データ管理 & 記憶部** (270) stores the **ボリュームID (Volume ID)** (311) and the **マスターキーハッシュ値 (Hashed Master Key)** (321). These are used for security operations, such as **工場内LAN or 専用線 or SmartCard などセキュリティに運用** (Operation for security in factory LAN or dedicated line or SmartCard, etc.).

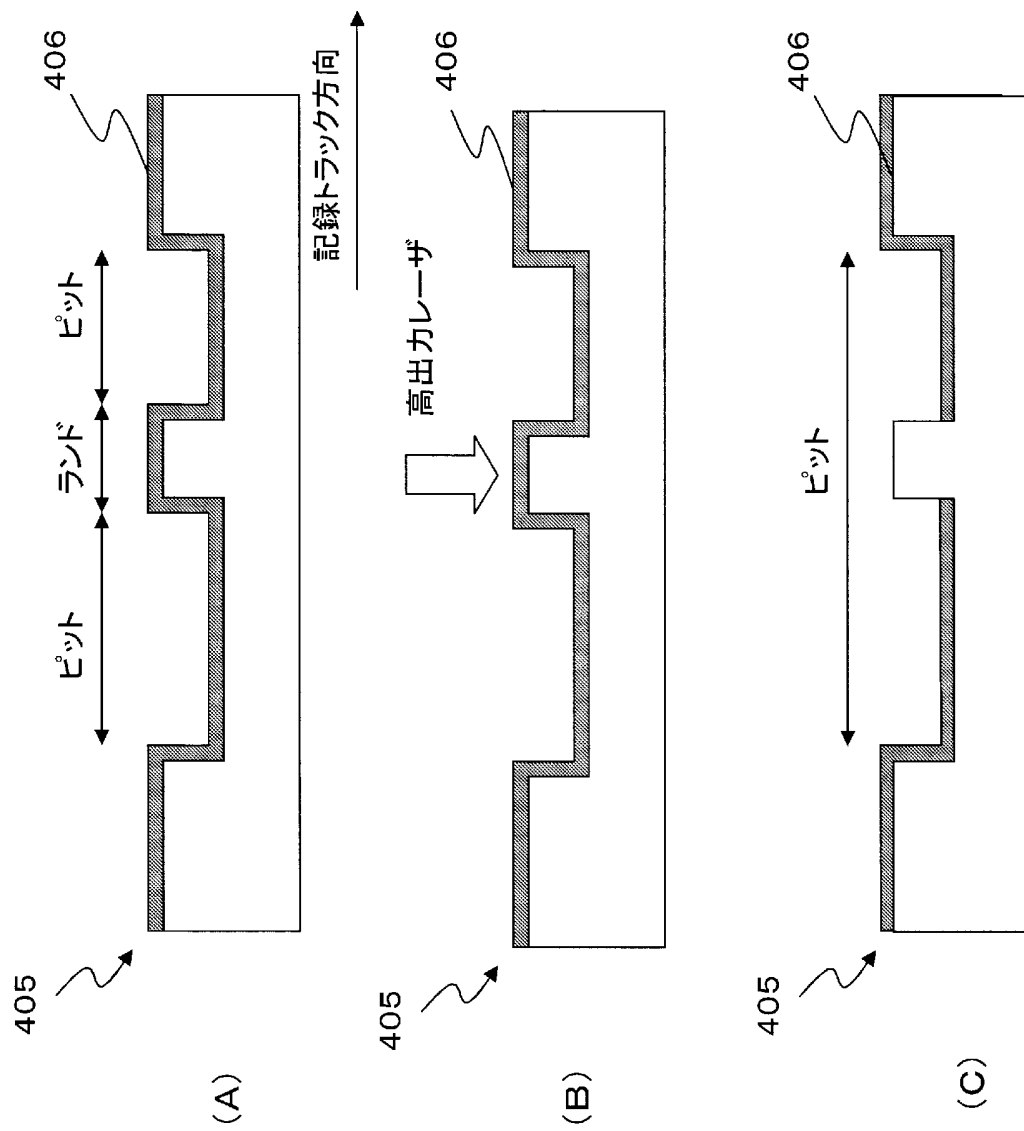
[図11]



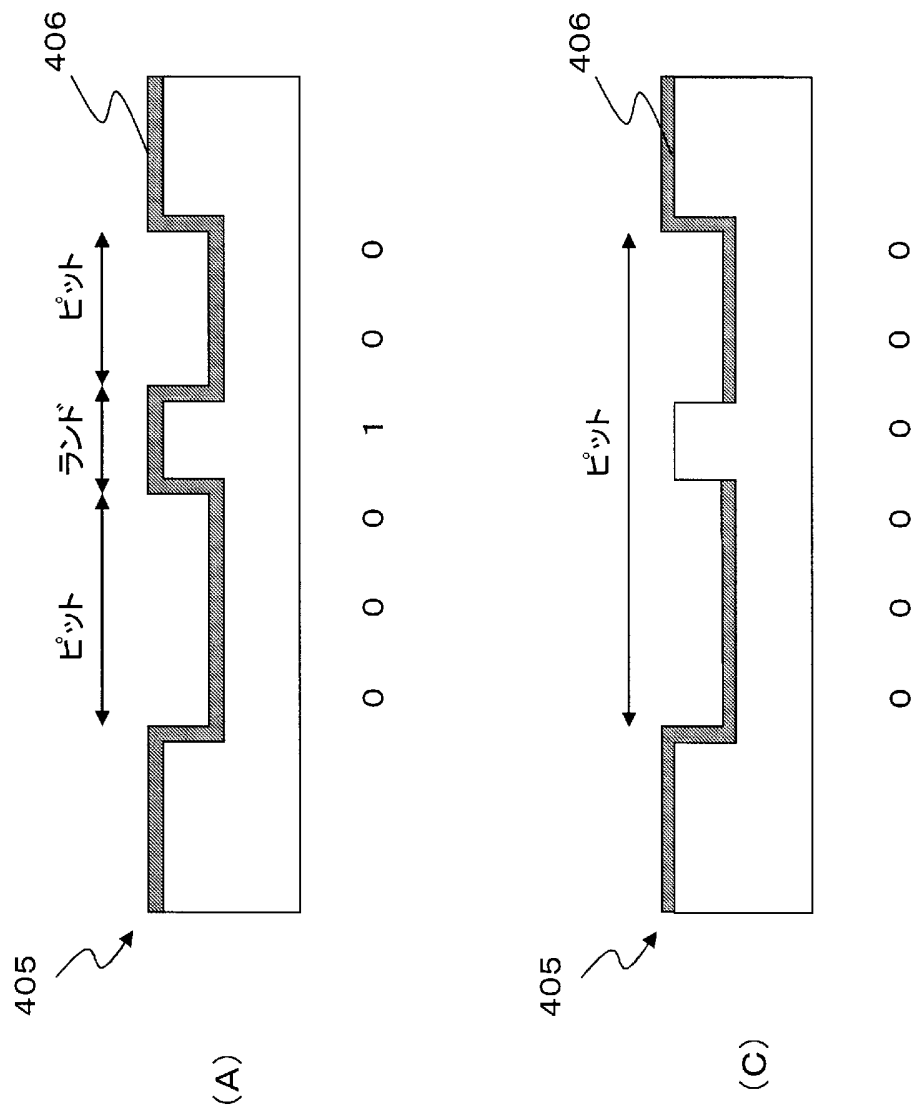
[図12]



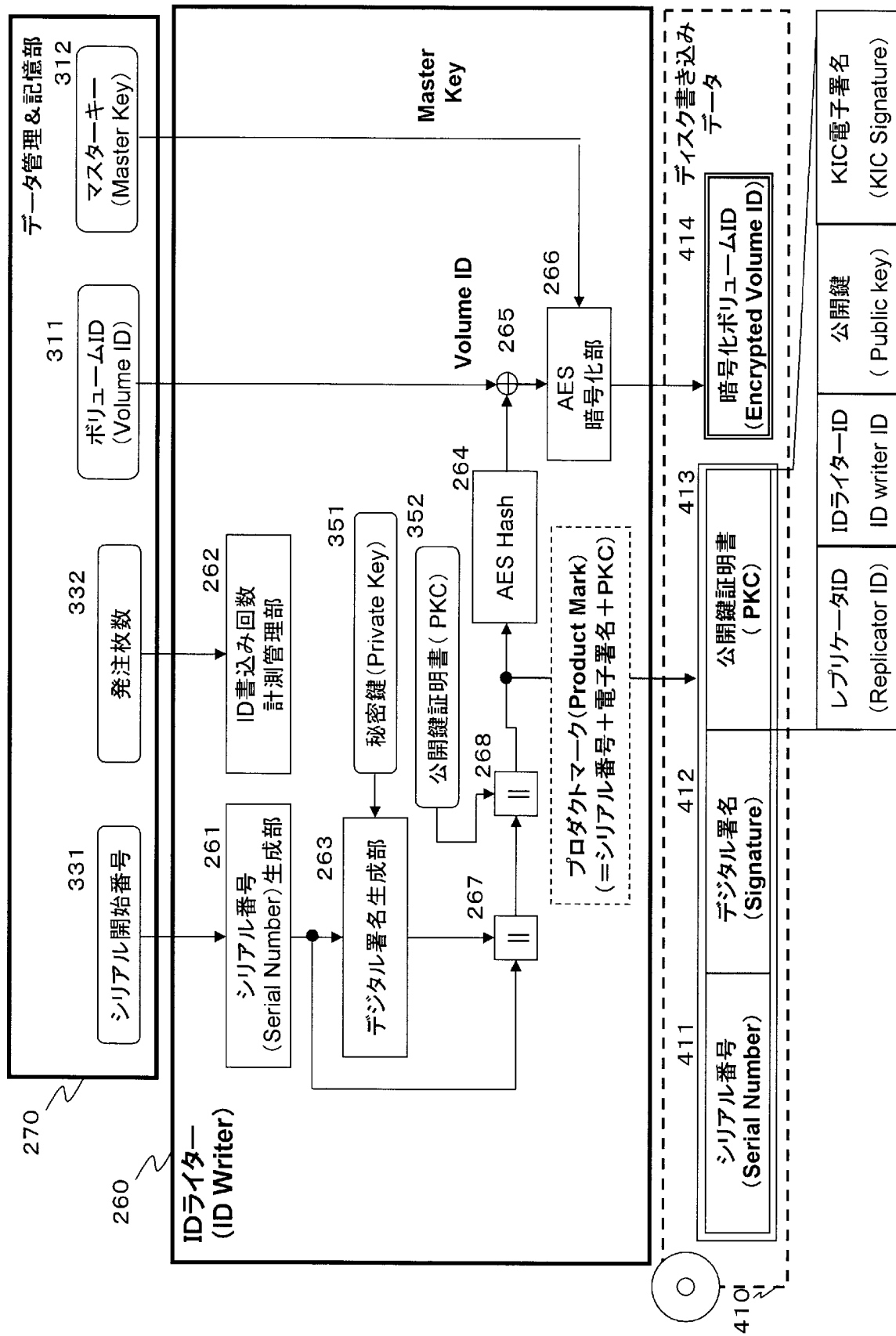
[図13]



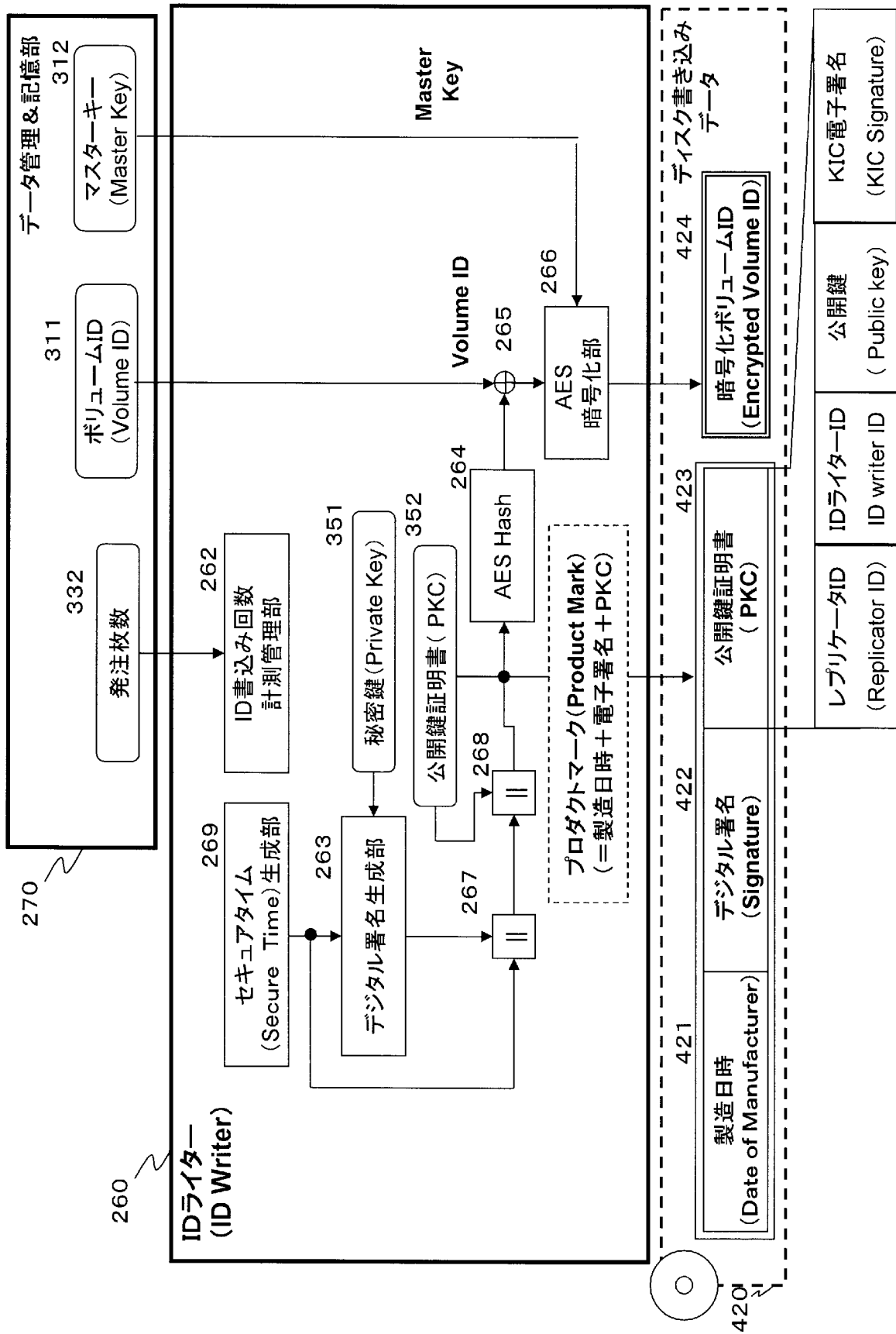
[図14]



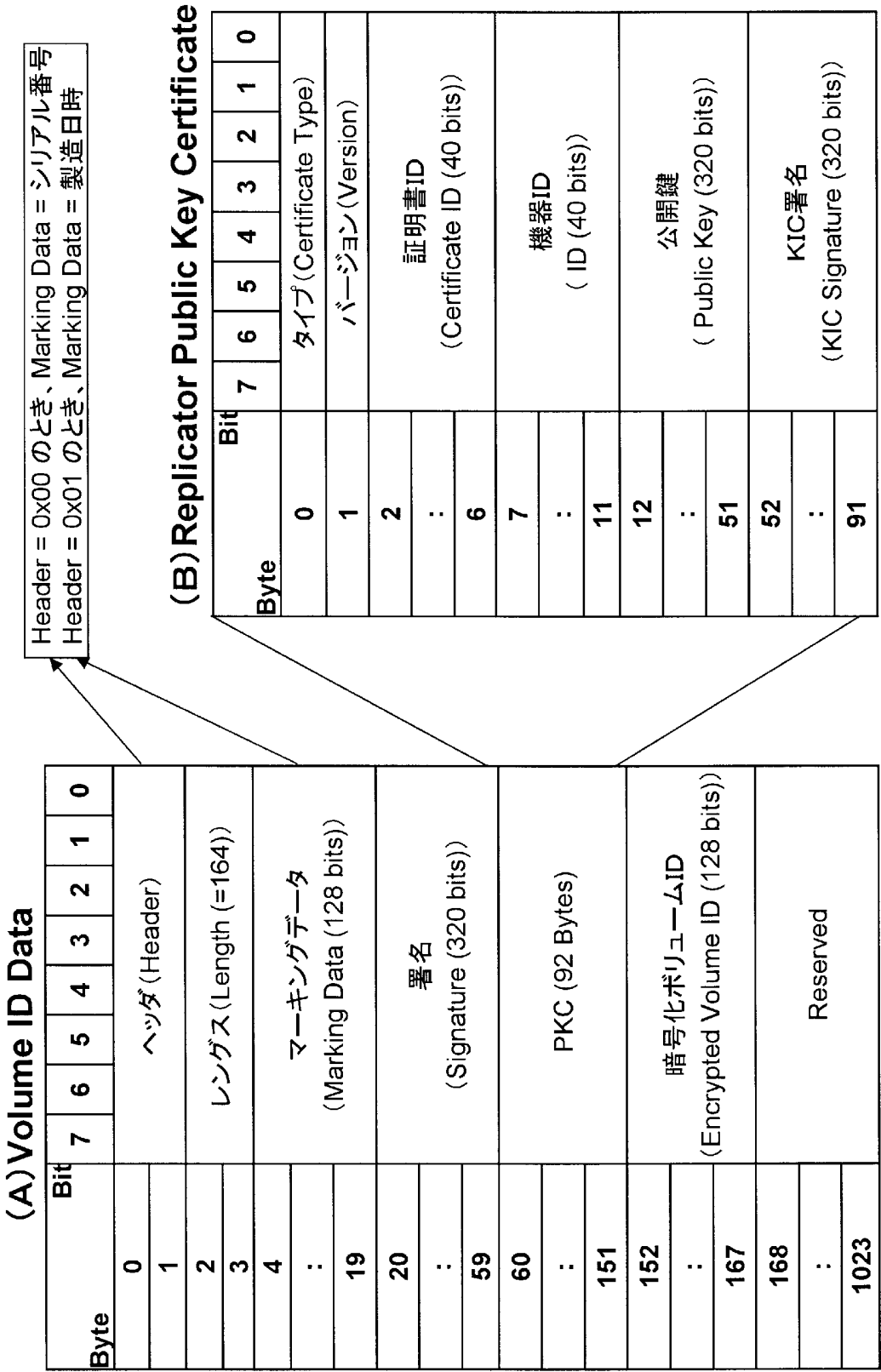
[図15]



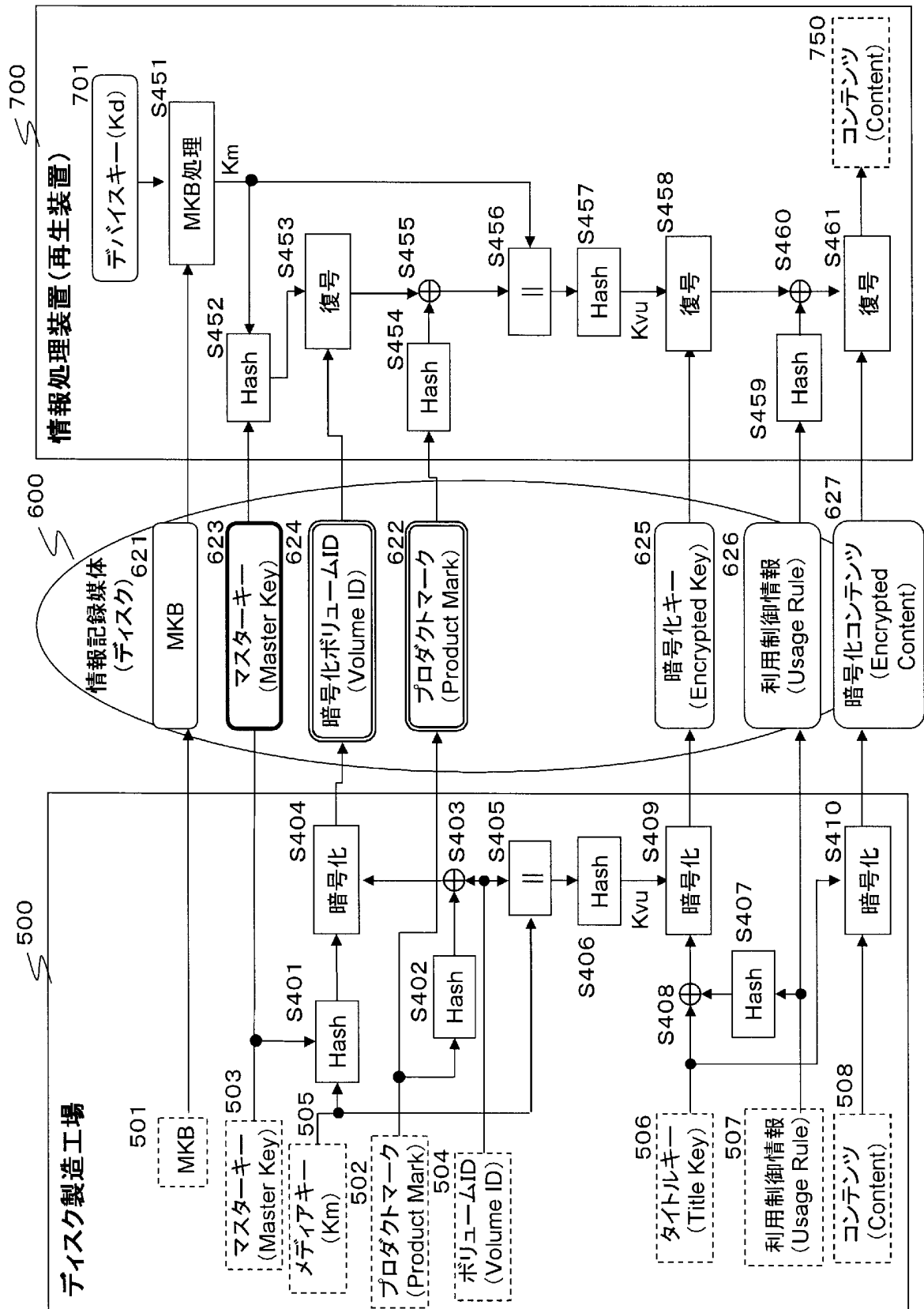
[図16]



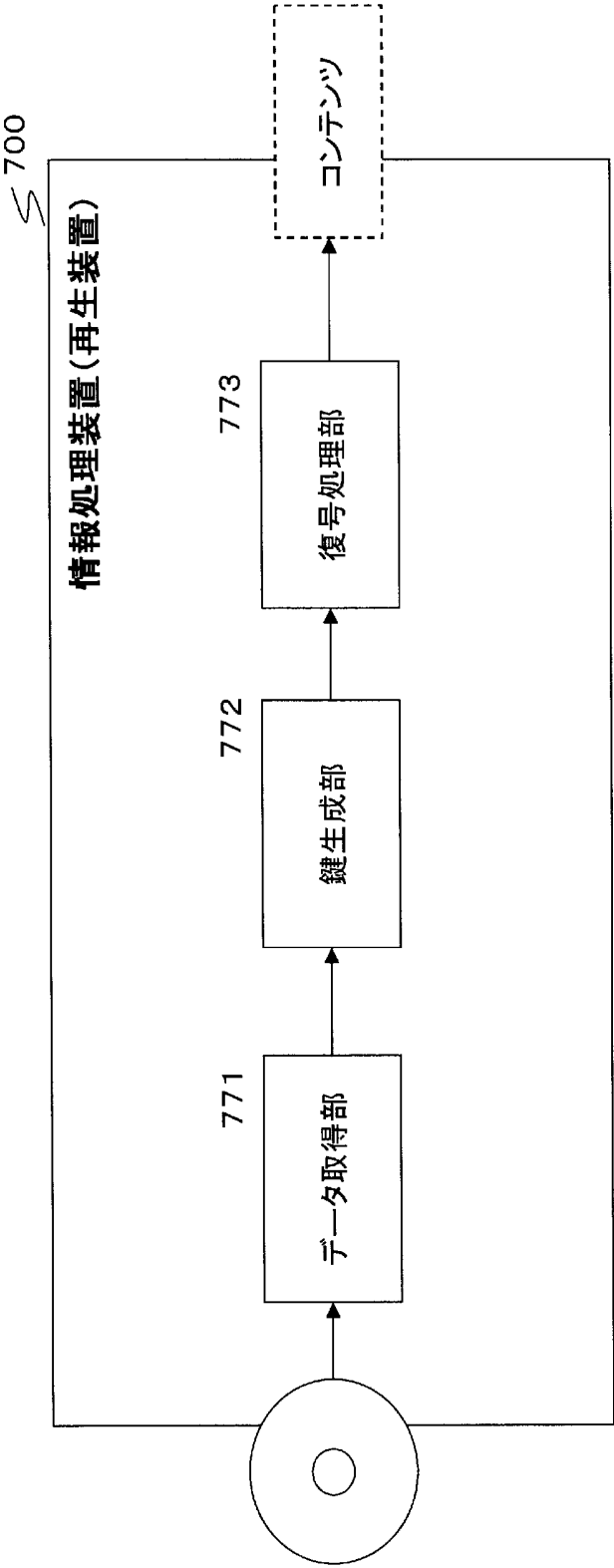
[図17]



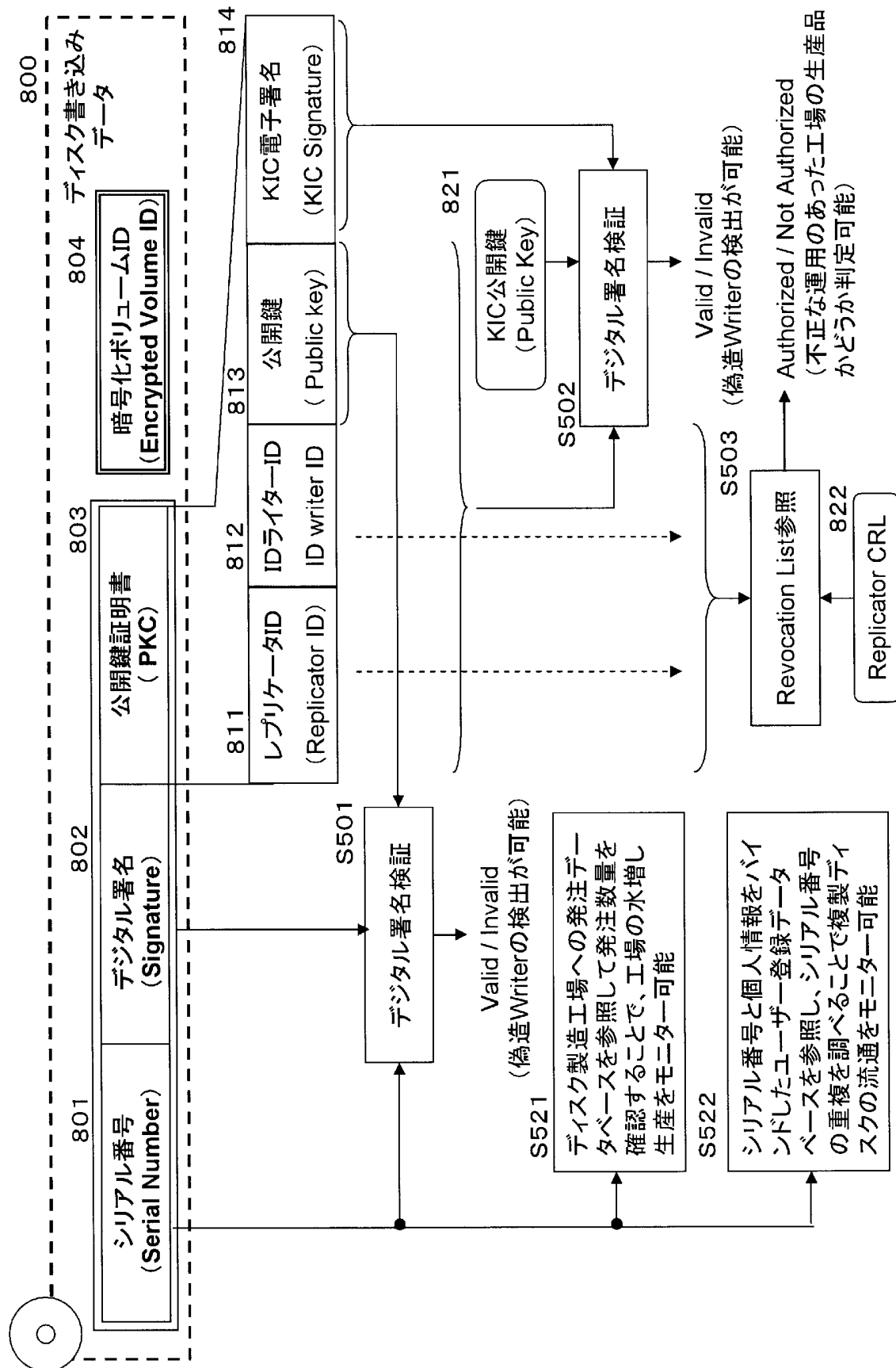
[図19]



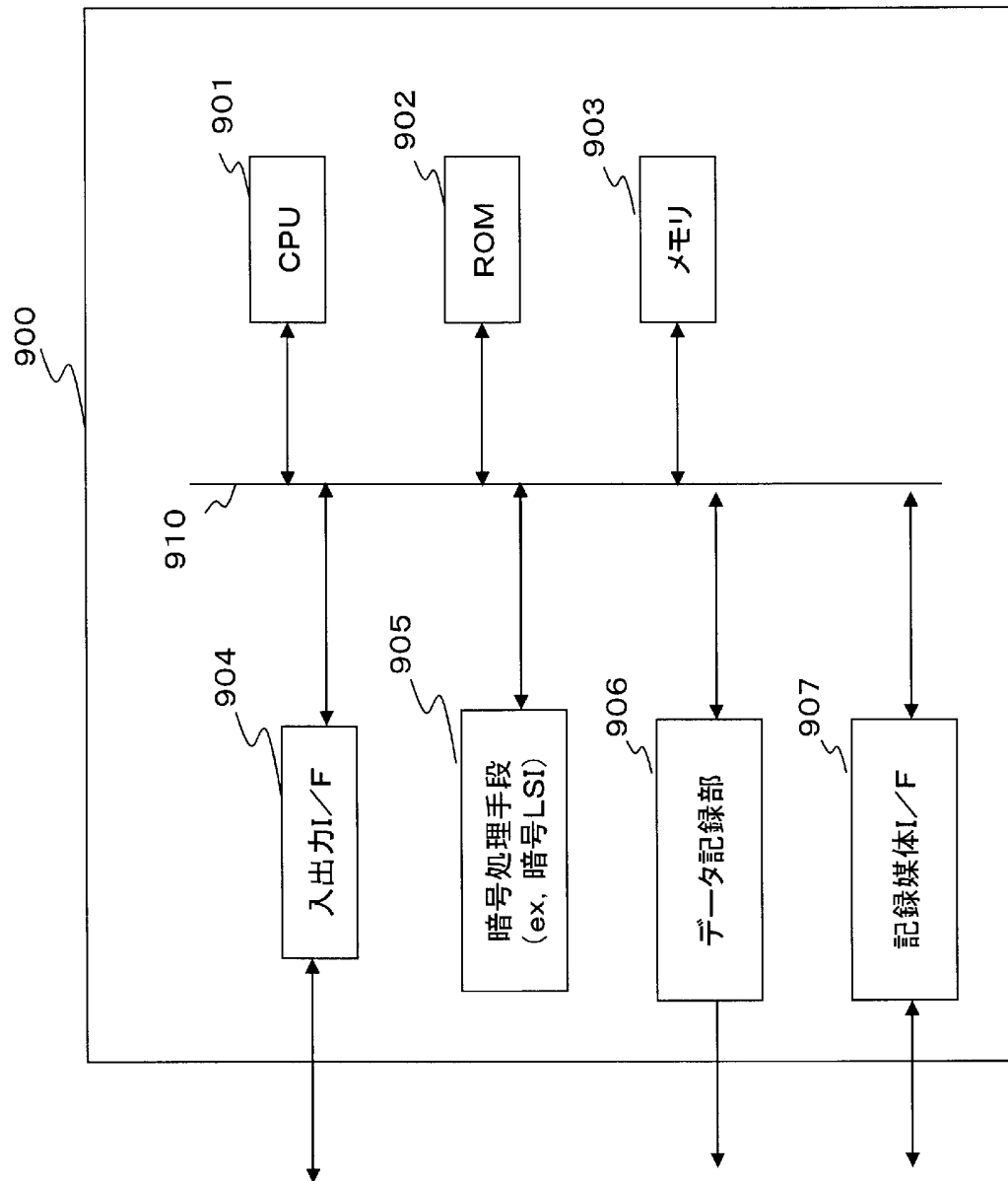
[図20]



[図21]



[図23]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2006/303843

A. CLASSIFICATION OF SUBJECT MATTER

G11B7/007(2006.01), **G11B7/0045**(2006.01), **G11B20/10**(2006.01), **G11B20/12**(2006.01), **G06F21/24**(2006.01), **G09C1/00**(2006.01), **H04L9/32**(2006.01)

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G11B7/007(2006.01), **G11B7/0045**(2006.01), **G11B20/10**(2006.01), **G11B20/12**(2006.01), **G06F21/24**(2006.01), **G09C1/00**(2006.01), **H04L9/32**(2006.01)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2006
Kokai Jitsuyo Shinan Koho	1971-2006	Toroku Jitsuyo Shinan Koho	1994-2006

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 96/16401 A1 (Matsushita Electric Industrial Co., Ltd.), 30 May, 1996 (30.05.96), Full text; Figs. 1 to 42 & JP 8-273164 A & US 5761301 A1 & EP 0741382 A1 & DE 69523139 T & CN 1138915 A & SG 0083122 A	1-13, 16
A	JP 2003-196836 A (Sony Corp.), 11 July, 2003 (11.07.03), Full text; Figs. 1 to 12 (Family: none)	1-13, 16
E, A	JP 2006-85813 A (Memory-Tech Corp.), 30 March, 2006 (30.03.06), Full text; Fig. 1 (Family: none)	1-13, 16

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance
 "E" earlier application or patent but published on or after the international filing date
 "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
 "O" document referring to an oral disclosure, use, exhibition or other means
 "P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
31 May, 2006 (31.05.06)

Date of mailing of the international search report
06 June, 2006 (06.06.06)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2006/303843

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
E, A	JP 2006-134385 A (Sony Corp.) , 25 May, 2006 (25.05.06) , Full text; Figs. 1 to 33 (Family: none)	1-13, 16

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2006/303843

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:
2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:
3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

The inventions of claims 1-13, 16 relate to recording at least one of the product mark and the encrypted volume ID by the reflection film removal recording method.

The inventions of claims 14-15, 17 relate to generation of a key for decoding a content by executing the data processing to which key generation information containing the product mark and the encrypted volume ID is applied.

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.: 1-13, 16

Remark on Protest
the

- ☐ The additional search fees were accompanied by the applicant's protest and, where applicable, payment of a protest fee..
- ☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.
- ☐ No protest accompanied the payment of additional search fees.

A. 発明の属する分野の分類 (国際特許分類 (IPC))			
Int.Cl. G11B7/007(2006.01), G11B7/0045(2006.01), G11B20/10(2006.01), G11B20/12(2006.01), G06F21/24(2006.01), G09C1/00(2006.01), H04L9/32(2006.01)			
B. 調査を行った分野			
調査を行った最小限資料 (国際特許分類 (IPC))			
Int.Cl. G11B7/007(2006.01), G11B7/0045(2006.01), G11B20/10(2006.01), G11B20/12(2006.01), G06F21/24(2006.01), G09C1/00(2006.01), H04L9/32(2006.01)			
最小限資料以外の資料で調査を行った分野に含まれるもの			
日本国実用新案公報 1922-1996年 日本国公開実用新案公報 1971-2006年 日本国実用新案登録公報 1996-2006年 日本国登録実用新案公報 1994-2006年			
国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)			
C. 関連すると認められる文献			
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号	
A	WO 96/16401 A1 (松下電器産業株式会社) 1996.05.30 全文, 第1-42図 & JP 8-273164 A & US 5761301 A1 & EP 0741382 A1 & DE 69523139 T & CN 1138915 A & SG 0083122 A	1-13, 16	
☒ C欄の続きにも文献が列挙されている。 ☐ パテントファミリーに関する別紙を参照。			
* 引用文献のカテゴリー 「A」 特に関連のある文献ではなく、一般的技術水準を示すもの 「E」 国際出願日前の出願または特許であるが、国際出願日後に公表されたもの 「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す) 「O」 口頭による開示、使用、展示等に言及する文献 「P」 国際出願日前で、かつ優先権の主張の基礎となる出願日の後に公表された文献 「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの 「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの 「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの 「&」 同一パテントファミリー文献			
国際調査を完了した日 31.05.2006		国際調査報告の発送日 06.06.2006	
国際調査機関の名称及びあて先 日本国特許庁 (ISA/J P) 郵便番号100-8915 東京都千代田区霞が関三丁目4番3号		特許庁審査官 (権限のある職員) 五貫 昭一 電話番号 03-3581-1101 内線 3551	

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	J P 2003-196836 A (ソニー株式会社) 2003.07.11 全文, 図1-12 (ファミリーなし)	1-13, 16
E, A	J P 2006-85813 A (メモリーテック株式会社) 2006.03.30 全文, 図1 (ファミリーなし)	1-13, 16
E, A	J P 2006-134385 A (ソニー株式会社) 2006.05.25 全文, 図1-33 (ファミリーなし)	1-13, 16

第Ⅱ欄 請求の範囲の一部の調査ができないときの意見（第1ページの2の続き）

法第8条第3項（P C T 17条(2) (a)）の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1. ☐ 請求の範囲 _____ は、この国際調査機関が調査をすることを要しない対象に係るものである。つまり、
2. ☐ 請求の範囲 _____ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、
3. ☐ 請求の範囲 _____ は、従属請求の範囲であってP C T 規則6.4(a)の第2文及び第3文の規定に従って記載されていない。

第Ⅲ欄 発明の単一性が欠如しているときの意見（第1ページの3の続き）

次に述べるようにこの国際出願に二以上の発明があるところの国際調査機関は認めた。

請求の範囲1-13、16は、プロダクトマークと暗号化ボリュームIDの少なくともいずれかのデータを反射膜除去記録方式によって記録するものに関する。

請求の範囲14-15、17は、プロダクトマークと暗号化ボリュームIDとを含む鍵生成情報を適用したデータ処理を実行してコンテンツ復号用の鍵を生成するものに関する。

1. ☐ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。
2. ☐ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。
3. ☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったため、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。
4. ☒ 出願人が必要な追加調査手数料を期間内に納付しなかったため、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

1-13、16

追加調査手数料の異議の申立てに関する注意

- ☐ 追加調査手数料及び、該当する場合には、異議申立手数料の納付と共に、出願人から異議申立てがあった。
- ☐ 追加調査手数料の納付と共に出願人から異議申立てがあったが、異議申立手数料が納付命令書に示した期間内に支払われなかった。
- ☐ 追加調査手数料の納付を伴う異議申立てがなかった。