

(19) 世界知的所有権機関
国際事務局(43) 国際公開日
2008年8月28日 (28.08.2008)

PCT

(10) 国際公開番号
WO 2008/102425 A1

(51) 国際特許分類:

H04L 9/08 (2006.01) G11B 20/10 (2006.01)
G06F 13/00 (2006.01) H04L 9/10 (2006.01)
G09C 1/00 (2006.01)

(21) 国際出願番号: PCT/JP2007/052968

(22) 国際出願日: 2007年2月19日 (19.02.2007)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(71) 出願人 (米国を除く全ての指定国について): パイオニア株式会社 (PIONEER CORPORATION) [JP/JP];
〒1538654 東京都目黒区目黒1丁目4番1号 Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 並木 剛 (NAMIKI,

Tsuyoshi) [JP/JP]; 〒3598522 埼玉県所沢市花園4丁目2610番地 パイオニア株式会社 所沢事業所内 Saitama (JP). 長谷部 剛 (HASEBE, Tsuyoshi) [JP/JP]; 〒3598522 埼玉県所沢市花園4丁目2610番地 パイオニア株式会社 所沢事業所内 Saitama (JP).

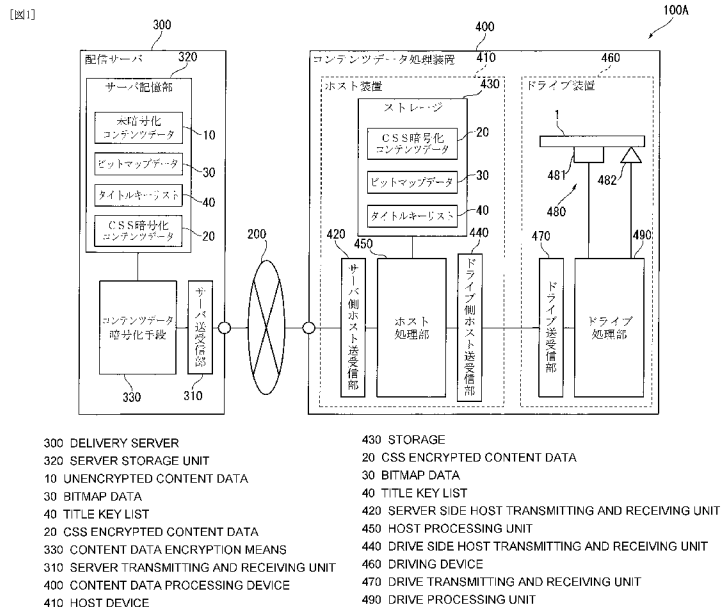
(74) 代理人: 木下 實三, 外 (KINOSHITA, Jitsuzo et al.);
〒1670051 東京都杉並区荻窪5丁目26番13号 荻窪TMビル3階 Tokyo (JP).

(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, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

[続葉有]

(54) Title: DATA TRANSMISSION DEVICE, DATA RECORDING DEVICE, DATA PROCESSING SYSTEM, DATA TRANSMISSION METHOD, AND DATA RECORDING METHOD

(54) 発明の名称: データ送信装置、データ記録装置、データ処理システム、データ送信方法、および、データ記録方法



(57) Abstract: A delivery server (300) in a data processing system (100A) transmits CSS encrypted content data (20), which is obtained by partially encrypting unencrypted content data (10) with a title key, to a host device (410) together with bitmap data (30) and a title key list (40). The host device (410) encrypts the title key list (40) so as to be decryptable with a bus key in a driving device (460) and transfers the encrypted title key list (40) to the driving device (460) together with the bitmap data (30) and main data. According to the title key list (40) decrypted with the bus key and bitmap data (30), the driving device (460) records, on a DVD-R (1), sector data including sector encryption information, in which information indicating not being encrypted is recorded, and unencrypted main data and sector data including sector encryption information, in which the title key is recorded, and encrypted main data.

[続葉有]



(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, 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).

添付公開書類:
— 国際調査報告書

(57) 要約: データ処理システム 100A の配信サーバ 300 は、未暗号化コンテンツデータ 10 をタイトルキーにより部分的に暗号化した CSS 暗号化コンテンツデータ 20 を、ビットマップデータ 30 およびタイトルキーリスト 40 とともにホスト装置 410 へ送信する。ホスト装置 410 は、タイトルキーリスト 40 をバスキーによりドライブ装置 460 で復号化可能に暗号化して、ビットマップデータ 30 およびメインデータとともにドライブ装置 460 へ転送する。ドライブ装置 460 は、バスキーで復号化したタイトルキーリスト 40 およびビットマップデータ 30 に基づいて、暗号化されていない旨の情報が記録されたセクタ暗号化情報および未暗号化メインデータを有するセクタデータや、タイトルキーが記録されたセクタ暗号化情報および暗号化メインデータを有するセクタデータを DVD-R1 に記録する。

明 細 書

データ送信装置、データ記録装置、データ処理システム、データ送信方法、および、データ記録方法

技術分野

[0001] 本発明は、暗号化された部分データおよび暗号化されていない部分データからなる部分暗号化データの記録媒体への記録に関する処理をするデータ送信装置、データ記録装置、データ処理システム、データ送信方法、および、データ記録方法に関する。

背景技術

[0002] 従来、情報送信装置で暗号化されたコンテンツデータを、ネットワークを介して情報記録再生装置に送信して、この情報記録再生装置により、暗号化されたコンテンツデータを記録媒体に記録する構成が知られている(例えば、特許文献1参照)。

[0003] この特許文献1に記載のものは、情報送信装置にて、DVD-RW(Digital Versatile Disc - Re - Recordable)に記録されるものと同一の暗号化キーを利用して、DVD-RWに記録されるべき音楽などの情報である記録情報を暗号化する。そして、この暗号化した記録情報を、ネットワークを介して、情報記録再生装置へ出力する。また、情報記録再生装置は、情報送信装置から暗号化された記録情報を取得する。そして、この記録情報を、その暗号化に利用された暗号化キーがあらかじめ記録されたDVD-RWに記録する構成が採られている。

[0004] 一方、著作権保護技術として、CSS(Content Scrambling System)が知られている。このCSSは、従来、DVD-Video(Digital Versatile Disc - Video)のみに利用可能であったが、今後、特許文献1に記載のような送信されたコンテンツデータを例えばDVD-R(Digital Versatile Disc - Recordable)のような記録媒体に記録する構成においても適用が許可されることが考えられる。

[0005] 特許文献1:特開2001-307427号公報

発明の開示

発明が解決しようとする課題

[0006] ところで、CSSでは、記録媒体に記録するセクタの50%を越えるセクタを暗号化することが認められていない。

このため、送信されるコンテンツデータを記録媒体に記録する構成にCSSを用いる場合、暗号化されたセクタ単位のデータ(以下、暗号化部分データと称す)と、暗号化されていないセクタ単位のデータ(以下、未暗号化部分データと称す)と、を混在させて送信するとともに、例えば暗号化部分データを復号化するためのタイトルキーとその後の書き込みデータが暗号化されていることを示すデータをバスキーで暗号化して送信した後に、暗号化部分データを送信する。その後のデータが暗号化されていないことを示すデータを送信した後に、未暗号化部分データを送信する。そして、暗号化されているかいないかのデータに基づいて、暗号化部分データか否かを判断し、適切な形で暗号化部分データと未暗号化部分データを記録したりすることが考えられる。

しかしながら、このような構成では、タイトルキーを送信の途中経路で解読されることがなく安全に送信できるが、送信データが暗号化されているか否かが頻繁に変化する場合、その変化するごとにタイトルキーを送信することとなり、記録速度の高速化を図ることができないおそれがある。

一方、記録速度の高速化を図るために、暗号化部分データおよびタイトルキーを1つのデータ構造にするとともに暗号化して、または、暗号化せずに送信することが考えられる。

しかしながら、暗号化部分データおよびタイトルキーを1つのデータ構造にして暗号化して送信する構成では、タイトルキーを安全に送信できるが、復号化するデータ量が多くなり記録速度の高速化を図ることができないおそれがある。また、暗号化部分データおよびタイトルキーを1つのデータ構造にして暗号化せずに送信する構成では、復号化するデータ量の増大が抑制され記録速度の高速化を図ることができるが、この暗号化されていないタイトルキーが送信の途中経路で容易に解読されてしまうおそれがある。

これらのことから、タイトルキーを安全に送信しつつ、暗号化部分データおよび未暗号化部分データを有する部分暗号化データの記録速度の高速化を図れる構成が望

まれている。

- [0007] 本発明の目的は、暗号鍵で暗号化された部分データおよび暗号化されていない部分データからなる部分暗号化データの記録速度の高速化を容易に図れるとともに暗号鍵の安全な送信を可能にするデータ送信装置、データ記録装置、データ処理システム、データ送信方法、および、データ記録方法を提供することである。

課題を解決するための手段

- [0008] 本発明のデータ送信装置は、暗号化された部分データおよび暗号化されていない部分データからなる部分暗号化データをデータ記録装置へ送信して、記録媒体に記録させるデータ送信装置であって、前記暗号化の対象となる前記部分データを特定する暗号化対象特定情報を前記データ記録装置へ送信する暗号化対象特定情報送信手段と、前記部分暗号化データを前記データ記録装置へ送信する部分暗号化データ送信手段と、を具備したことを特徴とする。
- [0009] 本発明のデータ記録装置は、暗号化された部分データおよび暗号化されていない部分データからなる部分暗号化データをデータ送信装置から受信して、記録媒体に記録するデータ記録装置であって、前記暗号化の対象となる前記部分データを特定する暗号化対象特定情報を取得する暗号化対象特定情報取得手段と、前記部分暗号化データを取得する部分暗号化データ取得手段と、前記暗号化対象特定情報に基づいて、前記部分暗号化データを、前記部分データが暗号化されているか否かに関する情報とともに前記記録媒体に記録する記録処理手段と、を具備したことを特徴とする。
- [0010] 本発明のデータ処理システムは、暗号化された部分データおよび暗号化されていない部分データからなる部分暗号化データをデータ送信装置からデータ記録装置へ送信して、記録媒体に記録するデータ処理システムであって、前記データ送信装置は、前記暗号化の対象となる前記部分データを特定する暗号化対象特定情報を前記データ記録装置へ送信する暗号化対象特定情報送信手段と、前記部分暗号化データを前記データ記録装置へ送信する部分暗号化データ送信手段と、を備え、前記データ記録装置は、前記暗号化対象特定情報を前記データ送信装置から取得する暗号化対象特定情報取得手段と、前記部分暗号化データを取得する部分暗号化

データ取得手段と、前記暗号化対象特定情報に基づいて、前記部分暗号化データを、前記部分データが暗号化されているか否かに関する情報とともに記録処理手段と、を備えたことを特徴とする。

[0011] 本発明のデータ送信方法は、演算手段により、暗号化された部分データおよび暗号化されていない部分データからなる部分暗号化データをデータ記録装置へ送信して、記録媒体に記録させるデータ送信方法であって、前記演算手段は、前記暗号化の対象となる前記部分データを特定する暗号化対象特定情報を前記データ記録装置へ送信し、前記部分暗号化データを前記データ記録装置へ送信することを特徴とする。

[0012] 本発明のデータ記録方法は、演算手段により、暗号化された部分データおよび暗号化されていない部分データからなる部分暗号化データをデータ送信装置から受信して、記録媒体に記録するデータ記録方法であって、前記演算手段は、前記暗号化の対象となる前記部分データを特定する暗号化対象特定情報を取得し、前記部分暗号化データを取得し、前記暗号化対象特定情報に基づいて、前記部分暗号化データを、前記部分データが暗号化されているか否かに関する情報とともに前記記録媒体に記録することを特徴とする。

図面の簡単な説明

[0013] [図1]本発明の第1実施形態に係るデータ処理システムの概略構成を示すブロック図である。

[図2]前記第1実施形態における未暗号化コンテンツデータおよびCSS暗号化コンテンツデータの概略構成を示す模式図である。

[図3]前記第1実施形態におけるビットマップデータの概略構成を示す模式図である。

[図4]前記第1実施形態および本発明の第2実施形態に係るタイトルキーリストの概略構成を示す模式図である。

[図5]前記第1実施形態におけるホスト処理部の概略構成を示すブロック図である。

[図6]前記第1, 第2実施形態におけるライトコマンドの概略構成を示す模式図である。

[図7]前記第1実施形態におけるドライブ処理部の概略構成を示すブロック図である。

[図8]前記第1実施形態におけるCSS暗号化コンテンツデータの記録処理時におけるホスト装置の動作を示すフローチャートである。

[図9]前記第1実施形態におけるCSS暗号化コンテンツデータの記録処理時におけるドライブ装置の動作を示すフローチャートである。

[図10]前記第2実施形態におけるデータ処理システムの概略構成を示すブロック図である。

[図11]前記第2実施形態における未暗号化コンテンツデータおよびCSS暗号化コンテンツデータの概略構成を示す模式図である。

[図12]前記第2実施形態におけるホスト処理部の概略構成を示すブロック図である。

[図13]前記第2実施形態におけるドライブ処理部の概略構成を示すブロック図である。

[図14]前記第2実施形態におけるCSS暗号化コンテンツデータの記録処理時におけるホスト装置の動作を示すフローチャートである。

[図15]前記第2実施形態におけるCSS暗号化コンテンツデータの記録処理時におけるドライブ装置の動作を示すフローチャートである。

符号の説明

- [0014] 1…記録媒体としてのDVD-R
 10…未暗号化データとしての未暗号化コンテンツデータ
 11…タイトルデータ
 12…部分データとしてのメインデータ
 12A…未暗号化メインデータ
 12B…暗号化メインデータ
 20…暗号化データとしてのCSS暗号化コンテンツデータ
 30…暗号化対象特定情報としてのビットマップデータ
 31…暗号化対象情報としての暗号化フラグ情報
 40…暗号鍵リストとしてのタイトルキーリスト
 41…暗号鍵としてのタイトルキー

42…タイトルデータ特定情報としてのタイトル先頭アドレス情報
70…暗号化対象特定情報としての暗号化ルール情報
100A, 100B…データ処理システム
200…ネットワーク200
300, 600…データ送信装置を構成するサーバ装置としての配信サーバ
310…サーバ送信手段としても機能するサーバ送受信部
330, 630…部分暗号化データ生成手段としてのコンテンツデータ暗号化手段
410, 710…データ送信装置を構成するクライアント装置としてのホスト装置
450, 750…演算手段としてのホスト処理部
454…暗号化対象特定情報送信手段としてのビットマップデータ転送手段
455…暗号鍵送信手段および暗号鍵暗号化手段としてのタイトルキーリスト暗号化手段
457…部分暗号化データ送信手段としてのデータ転送制御手段
460, 760…データ記録装置としてのドライブ装置
480…記録処理手段を構成する記録部
490, 790…演算手段としてのドライブ処理部
493…暗号化対象特定情報取得手段としてのビットマップデータ取得手段
494…暗号鍵取得手段および暗号鍵復号化手段としてのタイトルキーリスト復号化手段
495, 795…部分暗号化データ取得手段としても機能する記録処理手段を構成する記録制御手段
754…暗号化対象特定情報送信手段としての暗号化ルール情報転送手段
755…暗号鍵送信手段および暗号鍵暗号化手段としてのタイトルキー暗号化手段
793…暗号化対象特定情報取得手段としての暗号化ルール情報取得手段
794…暗号鍵取得手段および暗号鍵復号化手段としてのタイトルキー復号化手段
発明を実施するための最良の形態

[0015] [第1実施形態]

以下、本発明の第1実施形態に係るデータ処理システムについて説明する。

この第1実施形態および後述する第2実施形態では、CSS(Content Scrambling System)に準拠してタイトルキーで暗号化されたメインデータおよび暗号化されていないメインデータを有するCSS暗号化コンテンツデータと、タイトルキーと、をDVD-R(Digital Versatile Disc - Recordable)に記録するデータ処理システムを例示して説明する。なお、ここでは、コンテンツを再生するためのCSS暗号化コンテンツデータを記録する構成について例示するが、アプリケーションソフトやゲームのデータを記録する構成としてもよい。また、CSSに準拠して暗号化された構成について例示するが、CSSに準拠しなくても、暗号化されたメインデータおよび暗号化されていないメインデータが混在する状態で暗号化されたいかなる構成としてもよい。

なお、以下において、暗号化されたメインデータを暗号化メインデータと、暗号化されていないメインデータを未暗号化メインデータと、暗号化メインデータおよび未暗号化メインデータをまとめて表現する際にはメインデータと、それぞれ称して説明する。

図1は、データ処理システムの概略構成を示すブロック図である。図2は、未暗号化コンテンツデータおよびCSS暗号化コンテンツデータの概略構成を示す模式図である。図3は、ビットマップデータの概略構成を示す模式図である。図4は、タイトルキーリストの概略構成を示す模式図である。図5は、ホスト処理部の概略構成を示すブロック図である。図6は、ライトコマンドの概略構成を示す模式図である。図7は、ドライブ処理部の概略構成を示すブロック図である。

[0016] 〔データ処理システムの構成〕

図1において、100Aはデータ処理システムである。

このデータ処理システム100Aは、ネットワーク200と、データ送信装置を構成するサーバ装置としての配信サーバ300と、コンテンツデータ処理装置400と、を備えている。

[0017] ネットワーク200には、配信サーバ300、および、コンテンツデータ処理装置400が接続されている。このネットワーク200としては、インターネット、イントラネット、LAN(Local Area Network)、無線媒体により情報が送受信可能な複数の基地局がネットワークを構成する通信回線網や放送網などのネットワーク、さらには、配信サーバ300、

および、コンテンツデータ処理装置400間で情報を直接送受信するための媒体となる有線媒体自体や無線媒体自体などが例示できる。

[0018] 配信サーバ300は、サーバ送信手段としても機能するサーバ送受信部310と、サーバ記憶部320と、部分暗号化データ生成手段としてのコンテンツデータ暗号化手段330と、などを備えている。

[0019] サーバ送受信部310は、ネットワーク200に接続され、コンテンツデータ処理装置400との各種情報の送受信を実施する。具体的には、サーバ送受信部310は、コンテンツデータ処理装置400から送信される各種情報を受信してコンテンツデータ暗号化手段330へ適宜出力し、コンテンツデータ暗号化手段330から取得した各種情報をコンテンツデータ処理装置400へ適宜送信する。

[0020] サーバ記憶部320は、未暗号化データとしての未暗号化コンテンツデータ10と、暗号化対象特定情報としてのビットマップデータ30と、暗号鍵リストとしてのタイトルキーリスト40と、を適宜読み出し可能に記憶している。また、コンテンツデータ暗号化手段330で生成された部分暗号化データとしてのCSS暗号化コンテンツデータ20を適宜読み出し可能に記憶する。

[0021] 未暗号化コンテンツデータ10は、映画やドラマなどのコンテンツを再生するためのデータであり、図2に示すように、一連のデータ列構造を有し、複数のタイトルデータ11を備えている。また、このタイトルデータ11は、暗号化されていない部分データとしてのメインデータ12、つまり未暗号化メインデータ12Aを備えている。この未暗号化メインデータ12A、つまりメインデータ12は、例えば2048byteのデータ長を有している。すなわち、未暗号化メインデータ12Aは、記録媒体としてのDVD-R1(図1参照)における1つのセクタに記録可能なデータ長を有している。

なお、図2において、メインデータ12を意味する四角形の図形の中に「×」が描かれているものは、未暗号化メインデータ12Aを表し、「○」が描かれているものは、暗号化メインデータ12Bを表す。

[0022] ビットマップデータ30には、全てのメインデータ12のそれぞれが暗号化の対象か否かに関する情報が記録されている。このビットマップデータ30は、図3に示すように、それぞれのメインデータ12が暗号化の対象か否かを表す暗号化対象情報としての

暗号化フラグ情報31と、を備えている。

この暗号化フラグ情報31は、例えば1セクタ、1ECC (1ECC=16セクタ)などの所定のデータ単位に対応しており、少なくとも1つのメインデータ12に関連付けられ、メインデータ12のアドレスを特定可能な構成を有している。

例えば、図3に示すように、右端の暗号化フラグ情報31に関連付けられたメインデータ12が暗号化の対象でない場合、この暗号化フラグ情報31に、暗号化の対象でない旨を表す「0」が記録されている。また、その右隣の暗号化フラグ情報31に関連付けられたメインデータ12が暗号化の対象の場合、この暗号化フラグ情報31に、暗号化されている旨を表す「1」が記録されている。

なお、このビットマップデータ30は、CSSに準拠した暗号化処理を実施可能な構成を有している。すなわち、図2に示すようなCSS暗号化コンテンツデータ20において、全メインデータ12に対する暗号化メインデータ12Bの割合が50%未満となるように設定された暗号化フラグ情報31を有している。

[0023] タイトルキーリスト40は、図4に示すように、各タイトルデータ11の暗号化に利用される暗号鍵としてのタイトルキー41と、このタイトルキー41で暗号化されるタイトルデータ11の先頭アドレスに関するタイトルデータ特定情報としてのタイトル先頭アドレス情報42と、を備えている。

例えば、図2に示すように、「Title1」のタイトルデータ11の先頭アドレスが「Adr1」の場合、「Adr1」が記録されたタイトル先頭アドレス情報42に、「TitleKey1」のタイトルキー41が関連付けられている。また、「Title2」のタイトルデータ11の先頭アドレスが「Adr2」の場合、「Adr2」が記録されたタイトル先頭アドレス情報42に、「TitleKey1」とは異なる「TitleKey2」のタイトルキー41が関連付けられている。

[0024] コンテンツデータ暗号化手段330は、各種プログラムにより構成され、図2に示すような未暗号化コンテンツデータ10を部分的に暗号化したCSS暗号化コンテンツデータ20を生成する。

具体的には、コンテンツデータ暗号化手段330は、未暗号化コンテンツデータ10と、ビットマップデータ30と、タイトルキーリスト40と、をサーバ記憶部320から取得する。また、ビットマップデータ30に基づいて、暗号化対象のメインデータ12のアドレスを

特定する。さらに、この特定したアドレスと、タイトルキーリスト40のタイトル先頭アドレス情報42と、に基づいて、暗号化に利用するタイトルキー41を認識する。そして、この認識したタイトルキー41でメインデータ12を暗号化して、暗号化メインデータ12Bを生成する。さらに、暗号化していないメインデータ12である未暗号化メインデータ12Aと、暗号化メインデータ12Bと、で構成されるCSS暗号化コンテンツデータ20を生成して、例えばサーバ記憶部320に記憶させる。つまり、上述したように、CSSに準拠したCSS暗号化コンテンツデータ20を生成する。

例えば、「Title1」のタイトルデータ11の未暗号化メインデータ12Aを、「TitleKey1」のタイトルキー41で暗号化して、暗号化メインデータ12Bを生成する。

[0025] また、コンテンツデータ暗号化手段330は、例えばコンテンツデータ処理装置400からのCSS暗号化コンテンツデータ20を購入する旨の要求を認識すると、サーバ送受信部310を制御して、ネットワーク200を介して、CSS暗号化コンテンツデータ20と、ビットマップデータ30と、タイトルキーリスト40と、をコンテンツデータ処理装置400へ出力する。

なお、CSS暗号化コンテンツデータ20をサーバ記憶部320に記憶させずに、購入要求を認識するごとにCSS暗号化コンテンツデータ20を生成して送信する構成としてもよい。

[0026] コンテンツデータ処理装置400は、図1に示すように、データ送信装置を構成するクライアント装置としてのホスト装置410と、データ記録装置としてのドライブ装置460と、を備えている。

[0027] ホスト装置410は、サーバ側ホスト送受信部420と、ストレージ430と、ドライブ側ホスト送受信部440と、演算手段としてのホスト処理部450と、などを備えている。

[0028] サーバ側ホスト送受信部420は、ネットワーク200に接続され、配信サーバ300との各種情報の送受信を実施する。具体的には、サーバ側ホスト送受信部420は、配信サーバ300から送信される各種情報を受信してホスト処理部450へ適宜出力し、ホスト処理部450から取得した各種情報を配信サーバ300へ適宜送信する。

[0029] ストレージ430は、ホスト処理部450の制御により、配信サーバ300からネットワーク200を介して送信されたCSS暗号化コンテンツデータ20、ビットマップデータ30、お

よび、タイトルキーリスト40を適宜読み出し可能に記憶する。

- [0030] ドライブ側ホスト送受信部440は、バスを介してドライブ装置460に接続され、ドライブ装置460との各種情報の送受信を実施する。具体的には、ドライブ側ホスト送受信部440は、ドライブ装置460から送信される各種情報を受信してホスト処理部450へ適宜出力し、ホスト処理部450から取得した各種情報をドライブ装置460へ適宜送信する。
- [0031] ホスト処理部450は、各種プログラムにより構成され、図5に示すように、記憶制御手段451と、ホスト相互認証手段452と、ホストバスキー生成手段453と、暗号化対象特定情報送信手段としてのビットマップデータ転送手段454と、暗号鍵送信手段および暗号鍵暗号化手段としてのタイトルキーリスト暗号化手段455と、ライトコマンド生成手段456と、部分暗号化データ送信手段としてのデータ転送制御手段457と、などを備えている。
- [0032] 記憶制御手段451は、例えば利用者による設定入力に基づいて、所定のCSS暗号化コンテンツデータ20を購入する旨の要求を配信サーバ300へ送信する。そして、ネットワーク200およびドライブ側ホスト送受信部440を介して、配信サーバ300からCSS暗号化コンテンツデータ20と、ビットマップデータ30と、タイトルキーリスト40と、を取得して、ストレージ430に記憶させる。
- [0033] ホスト相互認証手段452は、例えば利用者によるCSS暗号化コンテンツデータ20をDVD-R1に記録する旨の設定入力を認識すると、ドライブ側ホスト送受信部440を制御して、ドライブ装置460との相互認証処理を実施する。そして、相互認証が正常に完了したことを認識すると、その旨の相互認証完了信号をホストバスキー生成手段453へ出力する。
- [0034] ホストバスキー生成手段453は、ホスト相互認証手段452から相互認証完了信号を取得すると、タイトルキーリスト40の暗号化に利用されるバスキーを生成する。そして、このバスキーを、タイトルキーリスト暗号化手段455へ出力する。なお、このバスキーは、ドライブ装置460においても同一のものが生成される。
- [0035] ビットマップデータ転送手段454は、ホスト相互認証手段452による相互認証が正常に完了したことを認識すると、ストレージ430からビットマップデータ30を取得する。

そして、ドライブ側ホスト送受信部440を制御して、このビットマップデータ30をドライブ装置460へ転送する。

- [0036] タイトルキーリスト暗号化手段455は、ストレージ430からタイトルキーリスト40を取得する。さらに、ホストバスキー生成手段453からバスキーを取得する。そして、このバスキーを利用してタイトルキーリスト40を暗号化する。

ここで、上述したように、ドライブ装置460において、このタイトルキーリスト40の暗号化に利用されたバスキーと同一のバスキーが生成される。つまり、タイトルキーリスト暗号化手段455は、ドライブ装置460でバスキーを利用して復号化可能にタイトルキーリスト40を暗号化する。

そして、ドライブ側ホスト送受信部440を制御して、バスキーで暗号化したタイトルキーリスト40をドライブ装置460へ転送する。

- [0037] ライトコマンド生成手段456は、図6に示すようなライトコマンド50を生成する。

具体的には、ライトコマンド生成手段456は、例えばCSS暗号化コンテンツデータ20をDVD-R1に記録する旨の設定入力を認識すると、CSS暗号化コンテンツデータ20を記録する旨を要求するコードが記録されたオペレーションコード情報51を生成する。

また、DVD-R1での記録位置のアドレスが記録されたロジカルブロックアドレス情報52を生成する。

さらに、1個のライトコマンド50に対応してドライブ装置460へ転送するメインデータ12のサイズとして、あらかじめ設定されている数ECCである旨が記録されたトランスファレンス情報53を生成する。つまり、1個のライトコマンド50に対応して、異なるタイトルデータ11に属するメインデータ12が送信されうるトランスファレンス情報53を生成する。なお、あらかじめ設定された転送するメインデータ12のサイズとしては、ECCブロックの整数倍に限らず、任意のデータ長としてもよい。

そして、これらオペレーションコード情報51、ロジカルブロックアドレス情報52、および、トランスファレンス情報53を備えたライトコマンド50を生成する。さらに、ライトコマンド生成手段456は、CSS暗号化コンテンツデータ20の全てのメインデータ12を転送するためのライトコマンド50を生成する。つまり、ロジカルブロックアドレス情報52

の内容のみが互いに異なる複数のライトコマンド50を生成する。

[0038] データ転送制御手段457は、ライトコマンド50に基づいて、ドライブ側ホスト送受信部440を制御して、CSS暗号化コンテンツデータ20をドライブ装置460へ転送する。

具体的には、データ転送制御手段457は、ライトコマンド50を取得して、ロジカルブロックアドレス情報52およびトランスファレンス情報53に対応する数ECCのメインデータ12をストレージ430から取得する。そして、この取得したメインデータ12をライトコマンド50とともに、ドライブ装置460へ転送する。さらに、順次、互いに異なるライトコマンド50に対応する数ECCのメインデータ12を取得して、ライトコマンド50とともに、ドライブ装置460へ転送する。

[0039] ドライブ装置460は、図1に示すように、ドライブ送受信部470と、記録処理手段を構成する記録部480と、演算手段としてのドライブ処理部490と、などを備えている。

[0040] ドライブ送受信部470は、バスを介してホスト装置410に接続され、ホスト装置410との各種情報の送受信を実施する。具体的には、ドライブ送受信部470は、ホスト装置410から送信される各種情報を受信してドライブ処理部490へ適宜出力し、ドライブ処理部490から取得した各種情報をホスト装置410へ適宜送信する。

[0041] 記録部480は、DVD-R1の搬入出の際にDVD-R1が載置される図示しないトレイと、DVD-R1を回転可能に保持するターンテーブル481と、DVD-R1の記録面にCSS暗号化コンテンツデータ20を記録するピックアップ482と、などを備えている。これらトレイ、ターンテーブル481、および、ピックアップ482などは、ドライブ処理部490の制御により、所定の処理を実施する。

[0042] ドライブ処理部490は、各種プログラムにより構成され、図7に示すように、ドライブ相互認証手段491と、ドライブバスキー生成手段492と、暗号化対象特定情報取得手段としてのビットマップデータ取得手段493と、暗号鍵取得手段および暗号鍵復号化手段としてのタイトルキーリスト復号化手段494と、部分暗号化データ取得手段としても機能する記録処理手段を構成する記録制御手段495と、などを備えている。

[0043] ドライブ相互認証手段491は、ドライブ送受信部470を制御して、ホスト装置410との相互認証処理を実施する。そして、相互認証が正常に完了したことを認識すると、その旨の相互認証完了信号をドライブバスキー生成手段492へ出力する。

[0044] ドライブバスキー生成手段492は、ドライブ相互認証手段491から相互認証完了信号を取得すると、タイトルキーリスト40の暗号化に利用され、ホストバスキー生成手段453で生成されたバスキーと同一のバスキーを生成する。そして、このバスキーを、タイトルキーリスト復号化手段494へ出力する。

[0045] ビットマップデータ取得手段493は、ホスト装置410から送信されるビットマップデータ30を取得する。そして、このビットマップデータ30を記録制御手段495へ出力する。

[0046] タイトルキーリスト復号化手段494は、ホスト装置410にてバスキーで暗号化されたタイトルキーリスト40を取得する。さらに、ドライブバスキー生成手段492からバスキーを取得する。そして、タイトルキーリスト40を復号化して、記録制御手段495へ出力する。

[0047] 記録制御手段495は、記録部480を制御して、ホスト装置410から送信されるCSS暗号化コンテンツデータ20に基づいて、ここでは図示しないが複数のセクタデータを生成する。そして、このセクタデータをDVD-R1に記録する。

具体的には、記録制御手段495は、ビットマップデータ30と、復号化されたタイトルキーリスト40と、を取得する。また、ホスト装置410から送信されるライトコマンド50と、このライトコマンド50に対応する数ECCのメインデータ12と、を取得する。そして、このメインデータ12に関連付けられた暗号化フラグ情報31をビットマップデータ30から検索する。さらに、この検索した暗号化フラグ情報31が、暗号化されている旨を表しているか否かを判断する。

そして、暗号化されていない旨を表している場合、つまり、未暗号化メインデータ12Aの場合、固有のID (Identity) が記録されたID情報、エラー訂正フラグ、および、暗号化されていない旨の情報が記録されたセクタ暗号化情報を有するセクタヘッダと、1個の未暗号化メインデータ12Aと、などを備えたセクタデータを生成して、DVD-R1に記録する。

また、暗号化フラグ情報31が暗号化されている旨を表している場合、つまり、暗号化メインデータ12Bの場合、この暗号化メインデータ12Bのアドレスおよびタイトルキーリスト40のタイトル先頭アドレス情報42に基づいて、暗号化メインデータ12Bの暗

号化に利用されたタイトルキー41を取得する。さらに、ID情報、エラー訂正フラグ、および、取得したタイトルキー41が記録されたセクタ暗号化情報を有するセクタヘッダと、1個の暗号化メインデータ12Bと、などを備えたセクタデータを生成して、DVD-R1に記録する。ここで、タイトルキー41は、暗号化されている旨を表す情報としてセクタ暗号化情報に記録される。

[0048] 〔データ処理システムの動作〕

次に、データ処理システム100Aの動作として、CSS暗号化コンテンツデータ20をDVD-R1に記録する際におけるホスト装置410、および、ドライブ装置460の動作について説明する。

[0049] （ホスト装置の動作）

まず、ホスト装置410の動作について説明する。

図8は、CSS暗号化コンテンツデータの記録処理時におけるホスト装置の動作を示すフローチャートである。

[0050] コンテンツデータ処理装置400のホスト装置410は、CSS暗号化コンテンツデータ20をDVD-R1に記録する際の要求を認識すると、図8に示すように、ドライブ装置460との相互認証処理を実施する（ステップS101）。そして、相互認証が正常に完了したことを認識すると、バスキーを生成して（ステップS102）、ドライブ装置460へビットマップデータ30を転送する（ステップS103）。さらに、タイトルキーリスト40をバスキーで暗号化して、すなわちドライブ装置460で復号化可能に暗号化して、ドライブ装置460へ転送する（ステップS104）。そして、ホスト装置410は、CSS暗号化コンテンツデータ20を構成する数ECCのメインデータ12を、ライトコマンド50とともにドライブ装置460へ転送する（ステップS105）。

[0051] この後、CSS暗号化コンテンツデータ20を構成する全てのメインデータ12の転送が完了したか否かを判断する（ステップS106）。

このステップS106において、転送が完了してないと判断した場合、ステップS105に戻り、次に送信すべきメインデータ12をライトコマンド50とともに転送する。一方、ステップS106において、転送が完了したと判断した場合、DVD-R1のイジェクト動作を実施する旨の要求をドライブ装置460にする（ステップS107）。

[0052] (ドライブ装置の動作)

次に、ドライブ装置460の動作について説明する。

図9は、CSS暗号化コンテンツデータの記録処理時におけるドライブ装置の動作を示すフローチャートである。

[0053] コンテンツデータ処理装置400のドライブ装置460は、CSS暗号化コンテンツデータ20をDVD-R1に記録する際の要求がされると、図9に示すように、ホスト装置410との相互認証処理を実施する(ステップS201)。そして、相互認証が正常に完了したことを認識すると、ホスト装置410で生成されたバスキーと同一のバスキーを生成する(ステップS202)。

この後、ホスト装置410からビットマップデータ30を受信する(ステップS203)。さらに、ホスト装置410で暗号化されたタイトルキーリスト40を受信して、このタイトルキーリスト40をバスキーで復号化する(ステップS204)。そして、ホスト装置410からライトコマンド50およびメインデータ12を受信して、ビットマップデータ30およびタイトルキーリスト40などに基づいて、メインデータ12の暗号化の状態に対応した適切なセクタヘッダを有するセクタデータを生成して、DVD-R1に記録する(ステップS205)。

[0054] この後、CSS暗号化コンテンツデータ20を構成する全てのメインデータ12の記録が終了したか否かを判断する(ステップS206)。

このステップS206において、記録が完了してないと判断した場合、ステップS205に戻り、次に送信されたライトコマンド50およびメインデータ12を受信して、DVD-R1に記録する。一方、ステップS206において、記録が完了したと判断した場合、ホスト装置410の要求に基づいて、トレイをオープンする(ステップS207)。

[0055] [第1実施形態の作用効果]

上述したように、上記第1実施形態では、データ処理システム100Aの配信サーバ300は、未暗号化メインデータ12Aおよび暗号化メインデータ12Bを有するCSS暗号化コンテンツデータ20と、ビットマップデータ30と、タイトルキーリスト40と、をコンテンツデータ処理装置400のホスト装置410へ送信する。

ホスト装置410は、配信サーバ300からCSS暗号化コンテンツデータ20、ビットマップデータ30、タイトルキーリスト40を取得すると、ビットマップデータ30をドライブ装置

460へ転送するとともに、タイトルキーリスト40をバスキーによりドライブ装置460で復号化可能に暗号化してドライブ装置460へ転送する。そして、ホスト装置410は、メインデータ12をドライブ装置460へ転送する。

ドライブ装置460は、ホスト装置410からCSS暗号化コンテンツデータ20、ビットマップデータ30、復号化可能に暗号化されたタイトルキーリスト40を取得すると、タイトルキーリスト40をバスキーで復号化する。この後、ビットマップデータ30に基づいて、所定のメインデータ12が暗号化されているか否かを判断するとともに、必要に応じて、タイトルキーリスト40に基づいて、暗号化されたメインデータ12のタイトルキー41を認識する。そして、未暗号化メインデータ12Aまたは暗号化メインデータ12Bと、暗号化されているか否かの情報が記録されたセクタ暗号化情報と、などを有するセクタデータをDVD-R1に記録する。

このため、ホスト装置410にて、タイトルキーリスト40をドライブ装置460で復号化可能に暗号化して転送するので、タイトルキーリスト40が転送の経路途中で容易に解読されることを防止できる。また、ドライブ装置460にて、ビットマップデータ30に基づいてメインデータ12が暗号化されているか否かを判断できるので、メインデータ12が暗号化されているか否かが頻繁に変化する場合であっても、その変化するごとにタイトルキー41を取得する必要がなくなり、記録速度の高速化を図ることができる。

さらに、メインデータ12を暗号化せずに、タイトルキーリスト40のみを暗号化して転送するので、タイトルキー41を安全に転送しつつ、ドライブ装置460での復号化するデータ量を最小限に抑えることができる。

よって、データ処理システム100Aは、未暗号化メインデータ12Aおよび暗号化メインデータ12Bを有するCSS暗号化コンテンツデータ20の記録速度の高速化を容易に図ることができるとともに、タイトルキー41を安全に送信できる。

[0056] また、配信サーバ300は、ビットマップデータ30およびタイトルキーリスト40に基づいて、未暗号化コンテンツデータ10をタイトルキー41により部分的に暗号化して、CSS暗号化コンテンツデータ20を生成する。そして、CSS暗号化コンテンツデータ20と、ビットマップデータ30と、タイトルキーリスト40と、をコンテンツデータ処理装置400のホスト装置410へ送信する。

このため、配信サーバ300にCSS暗号化コンテンツデータ20を生成する機能を設けているので、データ処理システム100Aは、未暗号化コンテンツデータ10を取得するだけでよい。したがって、データ処理システム100Aの汎用性を向上できる。

[0057] また、配信サーバ300は、ビットマップデータ30の暗号化フラグ情報31に基づいて、暗号化対象のメインデータ12を暗号化して暗号化メインデータ12Bを生成する。また、ドライブ装置460は、メインデータ12に関連付けられた暗号化フラグ情報31をビットマップデータ30から検索し、この検索した暗号化フラグ情報31に基づいて、メインデータ12が暗号化されているか否かを判断する。

このため、複数のメインデータ12のそれぞれについて暗号化されているか否かを表すビットマップデータ30を利用するので、暗号化されているか否かの判断処理の効率化を図ることができる。よって、記録速度をより高速化できる。

[0058] そして、配信サーバ300は、タイトルキー41およびタイトル先頭アドレス情報42を有するタイトルキーリスト40を取得する。この後、暗号化対象のメインデータ12のアドレスと、タイトルキーリスト40のタイトル先頭アドレス情報42と、に基づいて、暗号化に利用するタイトルキー41を特定して、暗号化メインデータ12Bを生成する。また、ドライブ装置460は、メインデータ12のアドレスと、タイトルキーリスト40のタイトル先頭アドレス情報42と、に基づいて、暗号化に利用されたタイトルキー41を特定して、このタイトルキー41をセクタ暗号化情報に記録したセクタデータを生成する。

このため、複数のタイトルデータ11の暗号化に利用される複数のタイトルキー41を1度にドライブ装置460へ転送することができ、複数のタイトルキー41を安全に転送しつつ、複数のタイトルデータ11のDVD-R1への記録速度をさらに高速化できる。

[0059] さらに、タイトルキーリスト40に、タイトルキー41で暗号化されるタイトルデータ11の先頭アドレスを表すタイトル先頭アドレス情報42を組み込んでいる。

このため、タイトル先頭アドレス情報42として、先頭アドレスおよび最終アドレスによりタイトルデータ11の範囲を表す構成を適用する場合と比べて、タイトル先頭アドレス情報42のデータ量を最小限に抑えることができる。

[0060] また、本発明のデータ処理システム、データ送信装置、および、データ記録装置を、CSSに準拠して暗号化されたCSS暗号化コンテンツデータ20をDVD-R1に記

録する構成に適用している。

このため、従来、DVD－Videoのみに記録可能であったCSS暗号化コンテンツデータ20を、DVD－R1にも記録させることができるので、CSS暗号化コンテンツデータ20の販売促進を容易に図ることができる。

[0061] そして、コンテンツデータ処理装置400にて、配信サーバ300で暗号化されたCSS暗号化コンテンツデータ20を、ネットワーク200を介して取得して、DVD－R1に記録する構成としている。

このため、一般的にデータ処理システム100Aの利用者が保有するコンテンツデータ処理装置400に暗号化する機能を設けていないので、コンテンツデータ処理装置400の構成の簡略化を図れ、低価格化を容易に図れる。したがって、コンテンツデータ処理装置400の販売促進を容易に図れ、データ処理システム100Aの利用拡大をさらに容易に図ることができる。

[0062] [第2実施形態]

次に、本発明の第2実施形態に係るデータ処理システムについて説明する。

なお、第1実施形態と同一の構成については、同一名称および同一符号を付し、説明を適宜省略あるいは簡略化する。また、第1実施形態と略等しい構成については、同一名称を付し、説明を適宜簡略化する。

図10は、データ処理システムの概略構成を示すブロック図である。図11は、未暗号化コンテンツデータおよびCSS暗号化コンテンツデータの概略構成を示す模式図である。図12は、ホスト処理部の概略構成を示すブロック図である。図13は、ドライブ処理部の概略構成を示すブロック図である。

[0063] [データ処理システムの構成]

図10において、100Bはデータ処理システムである。

このデータ処理システム100Bは、ネットワーク200と、データ送信装置を構成するサーバ装置としての配信サーバ600と、コンテンツデータ処理装置700と、を備えている。

[0064] 配信サーバ600は、サーバ送受信部310と、サーバ記憶部620と、部分暗号化データ生成手段としてのコンテンツデータ暗号化手段630と、などを備えている。

[0065] サーバ記憶部620は、未暗号化コンテンツデータ10と、暗号化対象特定情報としての暗号化ルール情報70と、図4に示すようなタイトルキーリスト40と、を適宜読み出し可能に記憶している。また、コンテンツデータ暗号化手段630で生成されたCSS暗号化コンテンツデータ20を適宜読み出し可能に記憶する。

なお、ここでは、サーバ記憶部620にタイトルキーリスト40を記憶させる構成について例示するが、タイトルキー41と、このタイトルキー41に対応するタイトルデータ11と、を関連付ける、いかなる構成のデータを記憶させてもよい。

[0066] 未暗号化コンテンツデータ10は、図11に示すように、一連のデータ列構造を有し、未暗号化メインデータ12Aのみを有する複数のタイトルデータ11を備えている。この未暗号化メインデータ12A、つまりメインデータ12は、例えば2048byteのデータ長を有している。

[0067] 暗号化ルール情報70には、未暗号化コンテンツデータ10のメインデータ12を暗号化する際のルールに関する情報が記録されている。具体的には、暗号化ルール情報70には、メインデータ12の配列方向に所定周期で存在するメインデータ12が暗号化対象である旨の情報が記録されている。

なお、この暗号化ルール情報70は、CSSに準拠した暗号化処理を実施可能な構成を有している。すなわち、図11に示すようなCSS暗号化コンテンツデータ20において、全メインデータ12に対する暗号化メインデータ12Bの割合が50%未満となるように設定されたルールが記録されている。

[0068] コンテンツデータ暗号化手段630は、各種プログラムにより構成され、図11に示すような未暗号化コンテンツデータ10を部分的に暗号化したCSS暗号化コンテンツデータ20を生成する。

具体的には、コンテンツデータ暗号化手段630は、未暗号化コンテンツデータ10と、暗号化ルール情報70と、タイトルキーリスト40と、をサーバ記憶部620から取得する。さらに、暗号化ルール情報70に基づいて、暗号化するメインデータ12の配列方向の周期を認識する。

また、この認識した周期ごとに存在する暗号化対象のメインデータ12を特定する。さらに、この特定した暗号化対象のメインデータ12のアドレスと、タイトルキーリスト40

のタイトル先頭アドレス情報42と、に基づいて、暗号化に利用するタイトルキー41を認識する。そして、この認識したタイトルキー41でメインデータ12を暗号化して、メインデータ12の配列方向に所定周期で暗号化メインデータ12Bが存在するCSS暗号化コンテンツデータ20を生成する。つまり、上述したように、CSSに準拠したCSS暗号化コンテンツデータ20を生成して、サーバ記憶部620に記憶させる。

例えば、暗号化ルール情報70に、配列方向に4個ごとに存在するメインデータ12が暗号化対象である旨が記録されている場合、図11に示すように、それぞれ対応するタイトルキー41で暗号化された暗号化メインデータ12Bが、配列方向に4個ごとに存在するようなCSS暗号化コンテンツデータ20を生成する。

[0069] また、コンテンツデータ暗号化手段630は、例えばコンテンツデータ処理装置700からのCSS暗号化コンテンツデータ20を購入する旨の要求を認識すると、ネットワーク200を介して、CSS暗号化コンテンツデータ20と、暗号化ルール情報70と、タイトルキーリスト40と、をコンテンツデータ処理装置700へ出力する。

なお、CSS暗号化コンテンツデータ20をサーバ記憶部620に記憶させずに、購入要求を認識するごとにCSS暗号化コンテンツデータ20を生成して送信する構成としてもよい。

[0070] コンテンツデータ処理装置700は、図10に示すように、データ送信装置を構成するクライアント装置としてのホスト装置710と、データ記録装置としてのドライブ装置760と、を備えている。

[0071] ホスト装置710は、サーバ側ホスト送受信部420と、ストレージ730と、ドライブ側ホスト送受信部440と、演算手段としてのホスト処理部750と、などを備えている。

[0072] ストレージ730は、ホスト処理部750の制御により、配信サーバ600からネットワーク200を介して送信されたCSS暗号化コンテンツデータ20、暗号化ルール情報70、および、タイトルキーリスト40を適宜読み出し可能に記憶する。

[0073] ホスト処理部750は、各種プログラムにより構成され、図12に示すように、記憶制御手段751と、ホスト相互認証手段452と、ホストバスキー生成手段453と、暗号化対象特定情報送信手段としての暗号化ルール情報転送手段754と、暗号鍵送信手段および暗号鍵暗号化手段としてのタイトルキー暗号化手段755と、ライトコマンド生成手

段756と、データ転送制御手段457と、などを備えている。

[0074] 記憶制御手段751は、所定のCSS暗号化コンテンツデータ20を購入する旨の要求を配信サーバ600へ送信する。そして、配信サーバ600からCSS暗号化コンテンツデータ20と、暗号化ルール情報70と、タイトルキーリスト40と、を取得して、ストレージ730に記憶させる。

[0075] 暗号化ルール情報転送手段754は、ホスト相互認証手段452による相互認証が正常に完了したことを認識すると、ストレージ730から暗号化ルール情報70を取得して、ドライブ装置760へ転送する。

[0076] タイトルキー暗号化手段755は、ストレージ730からタイトルキーリスト40を取得するとともに、ホストバスキー生成手段453からバスキーを取得する。さらに、タイトルキーリスト40のタイトル先頭アドレス情報42に基づいて、ライトコマンド50に基づき送信が開始されるメインデータ12に対応するタイトルキー41を認識する。そして、バスキーを利用して、このタイトルキー41を暗号化して、ドライブ装置760へ転送する。

さらに、所定のタイトルデータ11のメインデータ12の送信が完了して、他のタイトルデータ11のメインデータ12が送信されることを認識すると、このメインデータ12に対応するタイトルキー41をバスキーで暗号化して、ドライブ装置760へ転送する。

[0077] ライトコマンド生成手段756は、図6に示すような、オペレーションコード情報51と、ロジカルブロックアドレス情報52と、トランスファレングス情報53と、を備えたライトコマンド50を生成する。

なお、この第2実施形態におけるライトコマンド生成手段756は、1個のライトコマンド50に対応して、異なるタイトルデータ11に属するメインデータ12が送信されないようなロジカルブロックアドレス情報52、および、トランスファレングス情報53を生成する。つまり、1個のライトコマンド50に対応してドライブ装置460へ転送するメインデータ12のサイズとして、適宜異なる値が記録されたトランスファレングス情報53を生成する。

[0078] データ転送制御手段457は、ライトコマンド50に基づいて、CSS暗号化コンテンツデータ20をドライブ装置760へ転送する。

[0079] ドライブ装置760は、図10に示すように、ドライブ送受信部470と、記録部480と、

演算手段としてのドライブ処理部790と、などを備えている。

- [0080] ドライブ送受信部470は、バスを介してホスト装置710に接続され、ホスト装置710との各種情報の送受信を実施する。具体的には、ドライブ送受信部470は、ホスト装置710から送信される各種情報を受信してドライブ処理部790へ適宜出力し、ドライブ処理部790から取得した各種情報をホスト装置710へ適宜送信する。
- [0081] 記録部480は、DVD-R1の搬入出の際にDVD-R1が載置される図示しないトレイと、DVD-R1を回転可能に保持するターンテーブル481と、DVD-R1の記録面にCSS暗号化コンテンツデータ20を記録するピックアップ482と、などを備えている。これらトレイ、ターンテーブル481、および、ピックアップ482などは、ドライブ処理部790の制御により、所定の処理を実施する。
- [0082] ドライブ処理部790は、各種プログラムにより構成され、図13に示すように、ドライブ相互認証手段491と、ドライブバスキー生成手段492と、暗号化対象特定情報取得手段としての暗号化ルール情報取得手段793と、暗号鍵取得手段および暗号鍵復号化手段としてのタイトルキー復号化手段794と、部分暗号化データ取得手段としても機能する記録処理手段を構成する記録制御手段795と、などを備えている。
- [0083] 暗号化ルール情報取得手段793は、ホスト装置710から送信される暗号化ルール情報70を取得して、記録制御手段795へ出力する。
- [0084] タイトルキー復号化手段794は、ホスト装置710にてバスキーで暗号化されたタイトルキー41を取得する。さらに、ドライブバスキー生成手段492からバスキーを取得する。そして、タイトルキー41を復号化して、記録制御手段795へ出力する。また、新たなタイトルキー41を取得すると、復号化して記録制御手段795へ出力する。
- [0085] 記録制御手段795は、ホスト装置710から送信されるCSS暗号化コンテンツデータ20に基づいて、複数のセクタデータをDVD-R1に記録する。
- 具体的には、記録制御手段795は、暗号化ルール情報70と、復号化されたタイトルキー41と、ライトコマンド50と、メインデータ12と、を取得して、メインデータ12に関連付けるセクタヘッダを生成する。
- このセクタヘッダの生成の際、記録制御手段795は、暗号化ルール情報70に基づいて、暗号化メインデータ12Bが存在する周期を認識する。そして、4個ごとに存在

するセクタデータのセクタ暗号化情報にタイトルキー41を記録するとともに、残りのセクタデータのセクタ暗号化情報に暗号化されていない旨を表す情報を記録して、DVD-R1に記録する。

また、タイトルキー復号化手段794から新たなタイトルキー41を取得すると、この新たなタイトルキー41を適宜セクタ暗号化情報に記録したセクタデータを、DVD-R1に記録する。

[0086] 〔データ処理システムの動作〕

次に、データ処理システム100Bの動作として、CSS暗号化コンテンツデータ20をDVD-R1に記録する際におけるホスト装置710、および、ドライブ装置760の動作について説明する。

なお、第1実施形態と同様の処理については、同一符号を付して説明を簡略にする。

[0087] （ホスト装置の動作）

まず、ホスト装置710の動作について説明する。

図14は、CSS暗号化コンテンツデータの記録処理時におけるホスト装置の動作を示すフローチャートである。

[0088] コンテンツデータ処理装置700のホスト装置710は、図14に示すように、ドライブ装置760との相互認証処理(ステップS101)、バスキーの生成処理(ステップS102)を実施して、ドライブ装置760へ暗号化ルール情報70を転送する(ステップS301)。さらに、タイトルキー41をバスキーで暗号化して、すなわちドライブ装置760で復号化可能に暗号化して、ドライブ装置760へ転送する(ステップS302)。そして、ホスト装置710は、CSS暗号化コンテンツデータ20を構成する数ECCのメインデータ12を、ライトコマンド50とともにドライブ装置760へ転送する(ステップS303)。

[0089] この後、CSS暗号化コンテンツデータ20に含まれる所定のタイトルデータ11の転送が完了したか否かを判断する(ステップS304)。

このステップS304において、所定のタイトルデータ11の転送が完了していないと判断した場合、ステップS303に戻り、従前に送信したメインデータ12と同じタイトルデータ11に属するメインデータ12をライトコマンド50とともに転送する。一方、ステップS

304において、所定のタイトルデータ11の転送が完了したと判断した場合、CSS暗号化コンテンツデータ20に含まれる全てのタイトルデータ11の転送が完了したか否かを判断する(ステップS305)。

そして、このステップS305において、全てのタイトルデータ11の転送が完了していないと判断した場合、ステップS302に戻り、次に送信すべきタイトルデータ11に対応するタイトルキー41をバスキーで暗号化して転送する。一方、ステップS305において、全てのタイトルデータ11の転送が完了したと判断した場合、イジェクト動作をドライブ装置760に要求する(ステップS107)。

[0090] (ドライブ装置の動作)

次に、ドライブ装置760の動作について説明する。

図15は、CSS暗号化コンテンツデータの記録処理時におけるドライブ装置の動作を示すフローチャートである。

[0091] コンテンツデータ処理装置700のドライブ装置760は、図15に示すように、ホスト装置710との相互認証処理(ステップS201)、ホスト装置710で生成されたバスキーと同一のバスキーの生成処理(ステップS202)を実施して、ホスト装置710から暗号化ルール情報70を受信する(ステップS401)。さらに、ホスト装置710で暗号化されたタイトルキー41を受信して、このタイトルキー41をバスキーで復号化する(ステップS402)。そして、ホスト装置710からライトコマンド50およびメインデータ12を受信して、暗号化ルール情報70およびタイトルキー41などに基づいて、メインデータ12の暗号化の状態に対応した適切なセクタヘッダを有するセクタデータを生成して、DVD-R1に記録する(ステップS403)。

[0092] この後、CSS暗号化コンテンツデータ20に含まれる全てのタイトルデータ11の記録が完了したか否かを判断する(ステップS404)。

このステップS404において、全てのタイトルデータ11の記録が完了したと判断した場合、ホスト装置710の要求に基づいて、トレイをオープンする(ステップS207)。一方、ステップS404において、全てのタイトルデータ11の記録が完了していないと判断した場合、新たなタイトルキー41を受信したか否かを判断する(ステップS405)。

そして、このステップS405において、受信したと判断した場合、この受信したタイト

ルキー41をバスキーで復号化して、セクタデータに記録するタイトルキー41を変更する(ステップS406)。そして、ステップS403に戻り、この変更したタイトルキー41を新たに受信したメインデータ12に適宜関連付けたセクタデータを、DVD-R1に記録する。一方、ステップS405において、新たなタイトルキー41を受信していないと判断した場合、ステップS403に戻り、従前に受信しているタイトルキー41を新たに受信したメインデータ12に適宜関連付けたセクタデータを、DVD-R1に記録する。

[0093] [第2実施形態の作用効果]

上述したように、上記第2実施形態では、第1実施形態と同様の作用効果に加え、以下のような作用効果を奏することができる。

[0094] すなわち、ドライブ装置760は、ホスト装置710から復号化可能に暗号化されたタイトルキー41と、暗号化ルール情報70と、を取得する。そして、この暗号化ルール情報70に基づいて、暗号化メインデータ12Bが存在する周期を認識し、この認識した周期ごとにタイトルキー41をセクタ暗号化情報に記録したセクタデータを生成する。

このため、ホスト装置710にて、タイトルキー41をドライブ装置760で復号化可能に暗号化して転送するので、タイトルキー41が転送の経路途中で容易に解読されることを防止できる。また、ドライブ装置760にて、暗号化ルール情報70に基づいてメインデータ12が暗号化されているか否かを判断できるので、メインデータ12が暗号化されているか否かが頻繁に変化する場合であっても、その変化するごとにタイトルキー41を取得する必要がなくなり、記録速度の高速化を図ることができる。

さらに、メインデータ12を暗号化せずに、タイトルキー41のみを暗号化して転送するので、タイトルキー41を安全に転送しつつ、ドライブ装置760での復号化するデータ量を最小限に抑えることができる。

そして、配列方向に所定周期で存在するメインデータ12が暗号化対象か否かを表す暗号化ルール情報70を利用するので、暗号化されているか否かの判断処理の効率化を図ることができ、記録速度をより高速化できる。

[0095] [実施形態の変形]

なお、本発明は、上述した第1、第2実施形態に限定されるものではなく、本発明の目的を達成できる範囲で以下に示される変形をも含むものである。

[0096] すなわち、第1, 第2実施形態において、配信サーバ300, 600に、未暗号化コンテンツデータ10に応じて、適宜異なるビットマップデータ30や暗号化ルール情報70を生成する機能を設ける構成としてもよい。

[0097] また、第1, 第2実施形態において、配信サーバ300, 600に、コンテンツデータ暗号化手段330, 630を設けずに、サーバ記憶部320, 620に他の暗号化装置で暗号化されたCSS暗号化コンテンツデータ20を記憶させ、このCSS暗号化コンテンツデータ20をホスト装置410, 710に送信する構成としてもよい。

[0098] また、第1, 第2実施形態において、タイトル先頭アドレス情報42として、先頭アドレスおよび最終アドレスによりタイトルデータ11の範囲を表す構成を適用してもよい。

[0099] そして、第1, 第2実施形態において、コンテンツデータ暗号化手段330, 630を、配信サーバ300, 600に設けずに、ホスト装置410, 710に設ける構成としてもよい。

このような構成の場合、ホスト装置410, 710にて、ストレージ430, 730に記憶された、あるいは、ネットワーク200を介して配信サーバ300, 600から送信される未暗号化コンテンツデータ10を取得する。そして、この取得した未暗号化コンテンツデータ10に基づいて、CSS暗号化コンテンツデータ20を生成して、ドライブ装置460, 760でDVD-R1に記録させる。

このような構成にしても、上記第1, 第2実施形態と同様に、CSS暗号化コンテンツデータ20の記録速度の高速化を容易に図ることができる。

[0100] また、第1, 第2実施形態において、全メインデータ12に対する暗号化メインデータ12Bの割合が50%以上かつ100%未満となるように未暗号化コンテンツデータ10を暗号化する構成に、本発明を適用してもよい。

さらに、アプリケーションソフトやゲームなどのコンテンツ以外のデータを記録する構成に、本発明を適用してもよい。

[0101] そして、1個のタイトルデータ11のみを有する未暗号化コンテンツデータ10を暗号化する構成に、本発明を適用してもよい。

さらに、DVD-R1に限らず、DVD+R、DVD+RW、DVD-RW、Blu-ray Disc、HD DVD (High Definition DVD) に記録する構成に、本発明を適用してもよい。

[0102] また、上述した各機能をプログラムとして構築したが、例えば回路基板などのハードウェアあるいは1つのIC (Integrated Circuit) などの素子にて構成するなどしてもよく、いずれの形態としても利用できる。なお、プログラムや別途記録媒体から読み取らせる構成とすることにより、上述したように取扱が容易で、利用の拡大が容易に図れる。

[0103] その他、本発明の実施の際の具体的な構造および手順は、本発明の目的を達成できる範囲で他の構造などに適宜変更できる。

[0104] [実施形態の効果]

上述したように、上記実施形態では、データ処理システム100Aの配信サーバ300は、未暗号化メインデータ12Aおよび暗号化メインデータ12Bを有するCSS暗号化コンテンツデータ20と、ビットマップデータ30と、タイトルキーリスト40と、をコンテンツデータ処理装置400のホスト装置410へ送信する。

ホスト装置410は、ビットマップデータ30およびメインデータ12をドライブ装置460へ転送するとともに、タイトルキーリスト40をバスキーによりドライブ装置460で復号化可能に暗号化してドライブ装置460へ転送する。

ドライブ装置460は、タイトルキーリスト40をバスキーで復号化するとともに、ビットマップデータ30に基づいて、所定のメインデータ12が暗号化されているか否かを判断し、必要に応じて、タイトルキーリスト40に基づいて、暗号化されたメインデータ12のタイトルキー41を認識する。そして、暗号化されていない旨の情報が記録されたセクタ暗号化情報と、未暗号化メインデータ12Aと、などを有するセクタデータや、タイトルキー41が記録されたセクタ暗号化情報と、暗号化メインデータ12Bと、などを有するセクタデータをDVD-R1に記録する。

このため、ホスト装置410にて、タイトルキーリスト40をドライブ装置460で復号化可能に暗号化して転送するので、タイトルキーリスト40が転送の経路途中で容易に解読されることを防止できる。また、ドライブ装置460にて、ビットマップデータ30に基づいてメインデータ12が暗号化されているか否かを判断できるので、メインデータ12が暗号化されているか否かが頻繁に変化する場合であっても、その変化するごとにタイトルキー41を取得する必要がなくなり、記録速度の高速化を図ることができる。

さらに、メインデータ12を暗号化せずに、タイトルキーリスト40のみを暗号化して転

送するので、タイトルキー41を安全に転送しつつ、ドライブ装置460での復号化するデータ量を最小限に抑えることができる。

よって、未暗号化メインデータ12Aおよび暗号化メインデータ12Bを有するCSS暗号化コンテンツデータ20の記録速度の高速化を容易に図ることができるとともに、タイトルキー41を安全に送信できるデータ処理システム100Aを提供できる。

すなわち、配信サーバ300およびホスト装置410は、ドライブ装置460にCSS暗号化コンテンツデータ20のDVD-R1への記録処理を高速に実施させることができるとともに、ドライブ装置460へタイトルキー41を安全に送信できる。

また、ドライブ装置460は、CSS暗号化コンテンツデータ20をDVD-R1へ高速に記録できるとともに、安全に送信されたタイトルキー41を取得できる。

産業上の利用可能性

- [0105] 本発明は、暗号鍵を利用して暗号化された部分データおよび暗号化されていない部分データからなる部分暗号化データの記録媒体への記録に関する処理をするデータ送信装置、データ記録装置、データ処理システム、データ送信方法、および、データ記録方法として利用できる。

請求の範囲

- [1] 暗号化された部分データおよび暗号化されていない部分データからなる部分暗号化データをデータ記録装置へ送信して、記録媒体に記録させるデータ送信装置であって、
- 前記暗号化の対象となる前記部分データを特定する暗号化対象特定情報を前記データ記録装置へ送信する暗号化対象特定情報送信手段と、
- 前記部分暗号化データを前記データ記録装置へ送信する部分暗号化データ送信手段と、
- を具備したことを特徴としたデータ送信装置。
- [2] 請求項1に記載のデータ送信装置であって、
- 前記部分暗号化データは、少なくとも1つの前記部分データを有する複数のタイトルデータを備え、
- 前記部分暗号化データにおける前記タイトルデータの位置を特定するタイトルデータ特定情報と、前記タイトルデータ特定情報で特定される前記タイトルデータの暗号化に利用された暗号鍵と、を有する暗号鍵リストを前記データ記録装置へ送信する暗号鍵送信手段を具備した
- ことを特徴としたデータ送信装置。
- [3] 請求項2に記載のデータ送信装置であって、
- 前記タイトルデータ特定情報は、前記部分暗号化データにおける前記タイトルデータのそれぞれの開始位置を特定する情報を有する
- ことを特徴としたデータ送信装置。
- [4] 請求項1ないし請求項3のいずれかに記載のデータ送信装置であって、
- 前記暗号化対象特定情報は、前記複数の前記部分データの各々が暗号化の対象か否かを表す暗号化対象情報を備えた
- ことを特徴としたデータ送信装置。
- [5] 請求項1ないし請求項3のいずれかに記載のデータ送信装置であって、
- 前記暗号化対象特定情報は、前記部分暗号化データに含まれる前記部分データのうち暗号化対象となる前記部分データが存在する周期を表す

- ことを特徴としたデータ送信装置。
- [6] 請求項1ないし請求項5のいずれかに記載のデータ送信装置であって、
前記部分暗号化データは、CSS (Content Scrambling System) に準拠する状態で暗号化された
ことを特徴としたデータ送信装置。
- [7] 請求項1ないし請求項6のいずれかに記載のデータ送信装置であって、
前記暗号化対象特定情報に基づいて、前記暗号化されていない複数の前記部分データのみに有する未暗号化データにおける前記暗号化の対象の前記部分データを暗号化して、前記部分暗号化データを生成する部分暗号化データ生成手段を具備し、
前記部分暗号化データ送信手段は、前記部分暗号化データ生成手段で生成された前記部分暗号化データを送信する
ことを特徴としたデータ送信装置。
- [8] 請求項1に記載のデータ送信装置であって、
前記部分データの暗号化に利用される暗号鍵を前記データ記録装置で復号化可能に暗号化する暗号鍵暗号化手段と、
前記復号化可能に暗号化された前記暗号鍵を前記データ記録装置へ送信する暗号鍵送信手段と、
を具備したことを特徴としたデータ送信装置。
- [9] 請求項2または請求項3に記載のデータ送信装置であって、
前記暗号鍵リストを前記データ記録装置で復号化可能に暗号化する暗号鍵暗号化手段を具備し、
前記暗号鍵送信手段は、前記復号化可能に暗号化された前記暗号鍵リストを前記データ記録装置へ送信する
ことを特徴としたデータ送信装置。
- [10] 暗号化された部分データおよび暗号化されていない部分データからなる部分暗号化データをデータ送信装置から受信して、記録媒体に記録するデータ記録装置であって、

前記暗号化の対象となる前記部分データを特定する暗号化対象特定情報を取得する暗号化対象特定情報取得手段と、

前記部分暗号化データを取得する部分暗号化データ取得手段と、

前記暗号化対象特定情報に基づいて、前記部分暗号化データを、前記部分データが暗号化されているか否かに関する情報とともに前記記録媒体に記録する記録処理手段と、

を具備したことを特徴としたデータ記録装置。

[11] 請求項10に記載のデータ記録装置であって、

前記部分暗号化データは、少なくとも1つの前記部分データを有する複数のタイトルデータを備え、

前記部分暗号化データにおける前記タイトルデータの位置を特定するタイトルデータ特定情報と、前記タイトルデータ特定情報で特定される前記タイトルデータの暗号化に利用された暗号鍵と、を有する暗号鍵リストを前記データ送信装置から取得する暗号鍵取得手段を具備し、

前記記録処理手段は、前記暗号化対象特定情報に基づいて前記暗号化の対象となっている部分データを特定し、この部分データが属する前記タイトルデータの暗号化に利用される前記暗号鍵を前記部分データに関連付けて記録する

ことを特徴としたデータ記録装置。

[12] 請求項10または請求項11に記載のデータ記録装置であって、

前記暗号化対象特定情報は、前記複数の前記部分データの各々が暗号化の対象か否かを表す暗号化対象情報を備え、

前記記録処理手段は、前記暗号化対象情報に基づいて、前記部分データが暗号化されているか否かに関する情報を記録する

ことを特徴としたデータ記録装置。

[13] 請求項10または請求項11に記載のデータ記録装置であって、

前記暗号化対象特定情報は、前記部分暗号化データに含まれる前記部分データのうち暗号化対象となる前記部分データが存在する周期を表し、

前記記録処理手段は、前記暗号化対象特定情報に基づいて、前記部分データが

暗号化されているか否かに関する情報を記録すること
ことを特徴としたデータ記録装置。

- [14] 請求項10ないし請求項13のいずれかに記載のデータ記録装置であって、
前記部分暗号化データは、CSS (Content Scrambling System) に準拠する状態で
暗号化された
ことを特徴としたデータ記録装置。
- [15] 請求項10に記載のデータ記録装置であって、
復号化可能に暗号化され前記部分データの暗号化に利用される暗号鍵を前記データ送信装置から取得する暗号鍵取得手段と、
前記暗号鍵を復号化する暗号鍵復号化手段と、
を具備し、
前記記録処理手段は、前記部分データが暗号化されているか否かに関する情報として、前記暗号化対象特定情報に基づき特定される前記暗号化の対象の部分データに関連付けて前記暗号鍵を前記記録媒体に記録すること
ことを特徴としたデータ記録装置。
- [16] 請求項11に記載のデータ記録装置であって、
前記暗号鍵取得手段は、復号化可能に暗号化された前記暗号鍵リストを取得し、
前記暗号鍵リストを復号化する暗号鍵復号化手段を具備した
ことを特徴としたデータ記録装置。
- [17] 暗号化された部分データおよび暗号化されていない部分データからなる部分暗号化データをデータ送信装置からデータ記録装置へ送信して、記録媒体に記録するデータ処理システムであって、
前記データ送信装置は、
前記暗号化の対象となる前記部分データを特定する暗号化対象特定情報を前記データ記録装置へ送信する暗号化対象特定情報送信手段と、
前記部分暗号化データを前記データ記録装置へ送信する部分暗号化データ送信手段と、
を備え、

- 前記データ記録装置は、
前記暗号化対象特定情報を前記データ送信装置から取得する暗号化対象特定情報取得手段と、
前記部分暗号化データを取得する部分暗号化データ取得手段と、
前記暗号化対象特定情報に基づいて、前記部分暗号化データを、前記部分データが暗号化されているか否かに関する情報とともに記録処理手段と、
を備えたことを特徴としたデータ処理システム。
- [18] 請求項17に記載のデータ処理システムであって、
前記データ送信装置は、サーバ装置と、このサーバ装置にネットワークを介して各種情報を送受信可能に接続されたクライアント装置と、を備え、
前記サーバ装置は、
前記暗号化対象特定情報および前記部分暗号化データを、前記ネットワークを介して前記クライアント装置へ送信するサーバ送信手段を備え、
前記クライアント装置は、
前記サーバ装置から前記暗号化対象特定情報を取得して、前記データ記録装置へ転送する前記暗号化対象特定情報送信手段と、
前記サーバ装置から前記部分暗号化データを取得して、前記データ記録装置へ送信する前記部分暗号化データ送信手段と、
を備えたことを特徴としたデータ処理システム。
- [19] 演算手段により、暗号化された部分データおよび暗号化されていない部分データからなる部分暗号化データをデータ記録装置へ送信して、記録媒体に記録させるデータ送信方法であって、
前記演算手段は、
前記暗号化の対象となる前記部分データを特定する暗号化対象特定情報を前記データ記録装置へ送信し、
前記部分暗号化データを前記データ記録装置へ送信することを特徴とするデータ送信方法。
- [20] 演算手段により、暗号化された部分データおよび暗号化されていない部分データ

からなる部分暗号化データをデータ送信装置から受信して、記録媒体に記録するデータ記録方法であって、

前記演算手段は、

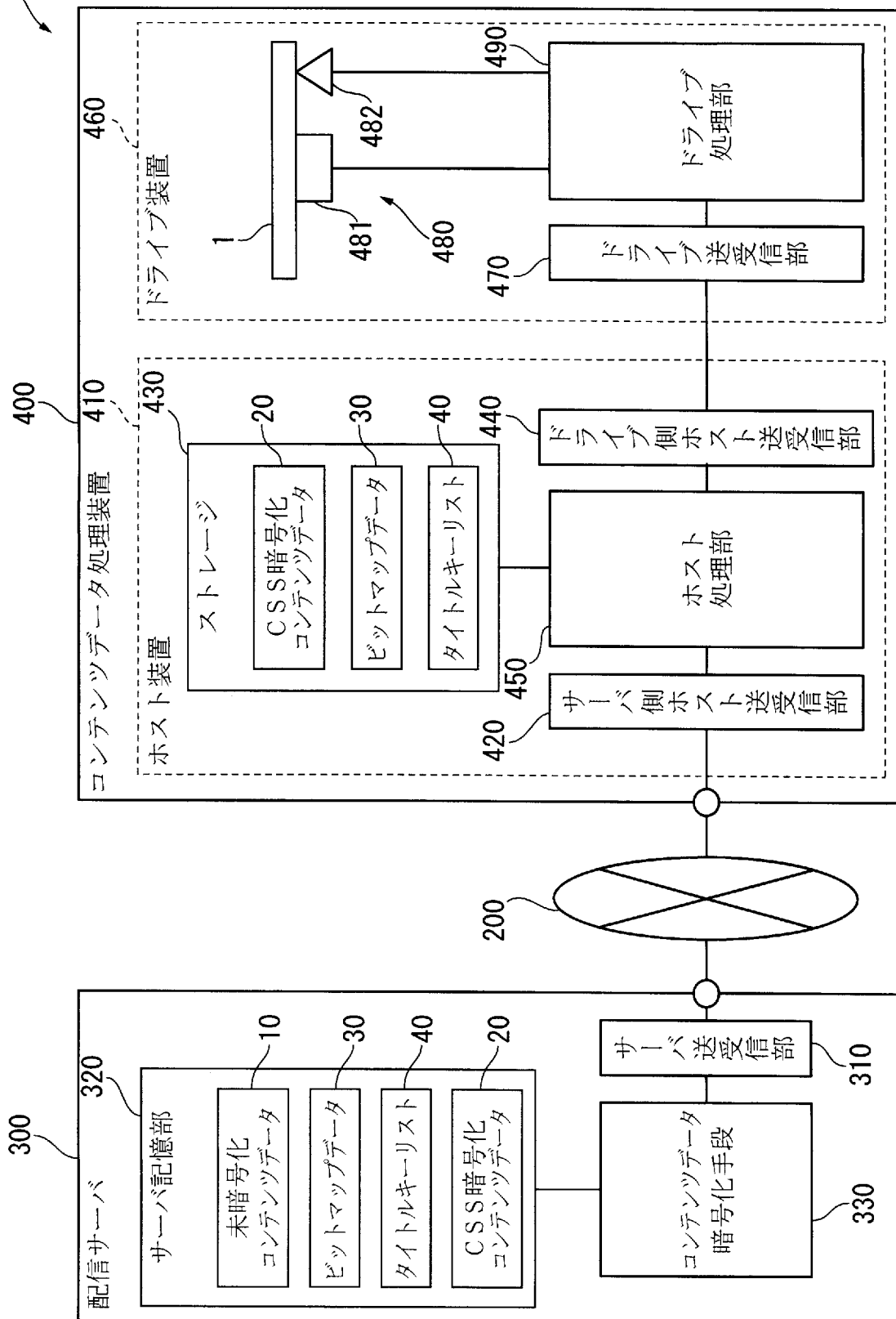
前記暗号化の対象となる前記部分データを特定する暗号化対象特定情報を取得し、

前記部分暗号化データを取得し、

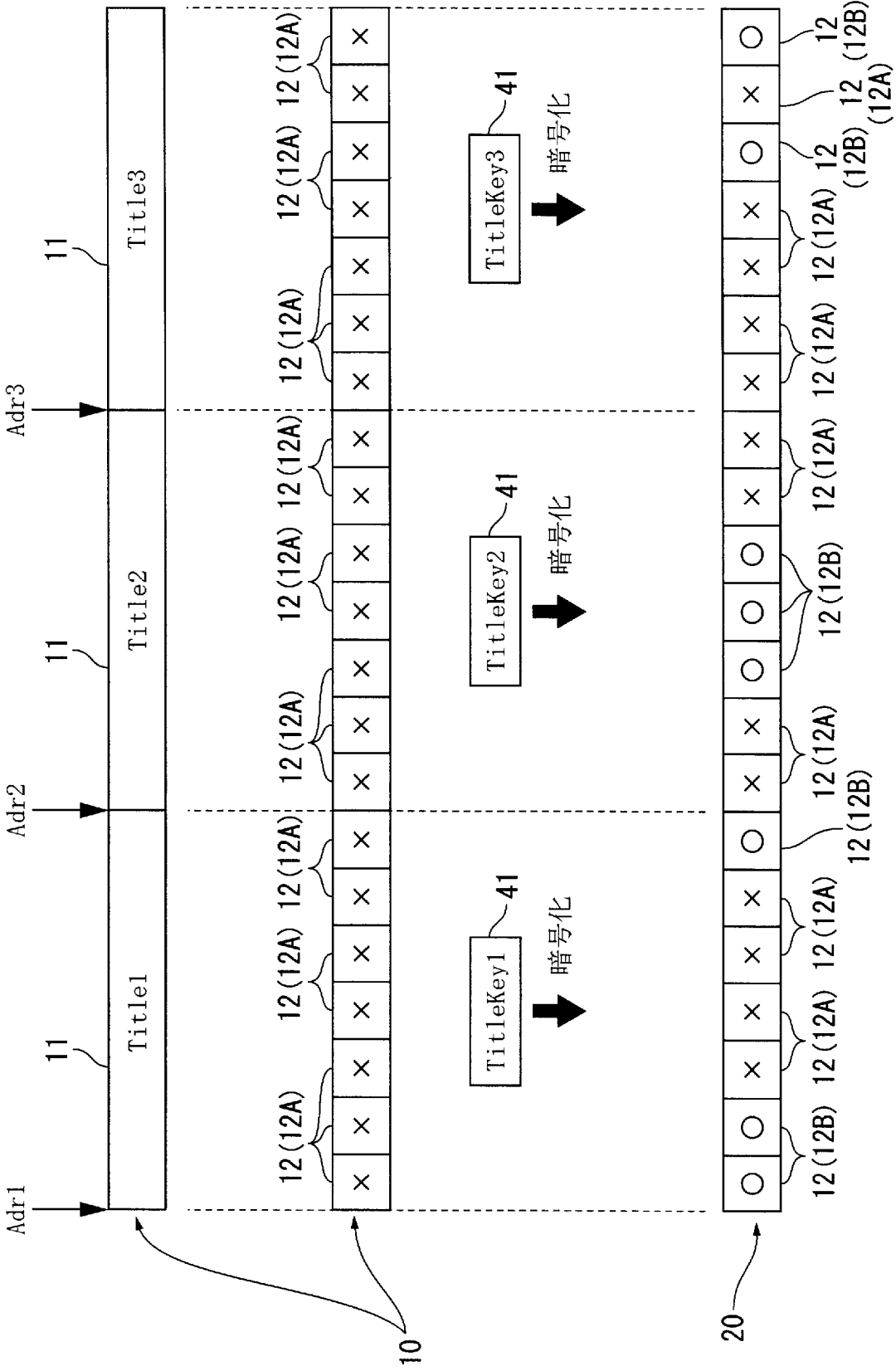
前記暗号化対象特定情報に基づいて、前記部分暗号化データを、前記部分データが暗号化されているか否かに関する情報とともに前記記録媒体に記録することを特徴とするデータ記録方法。

[図1]

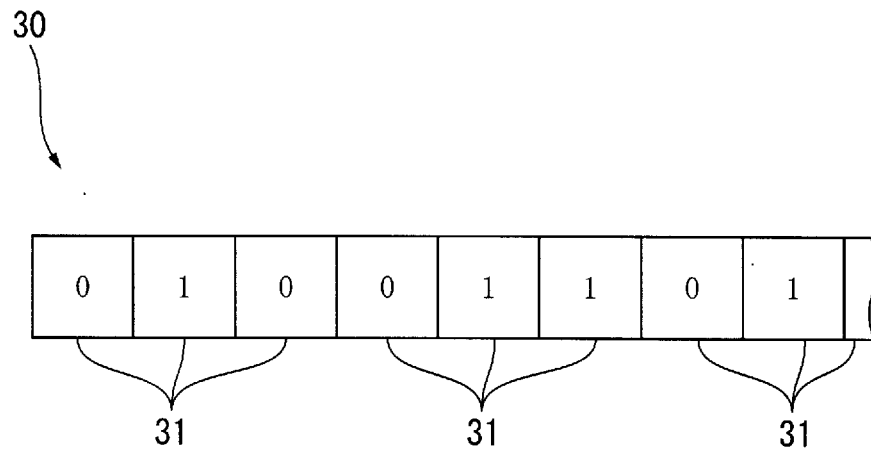
100A



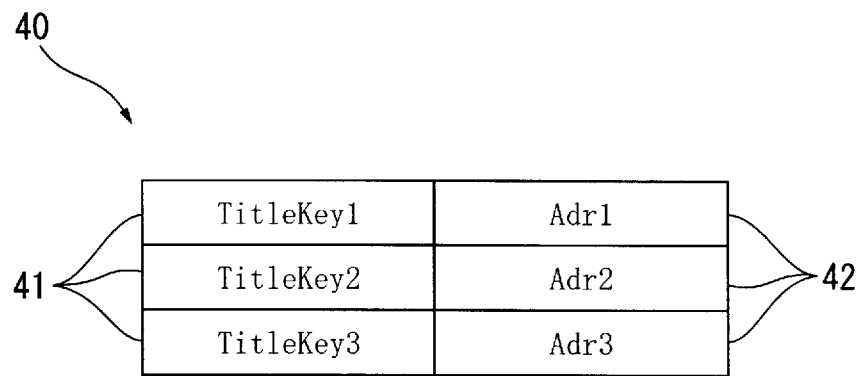
[図2]



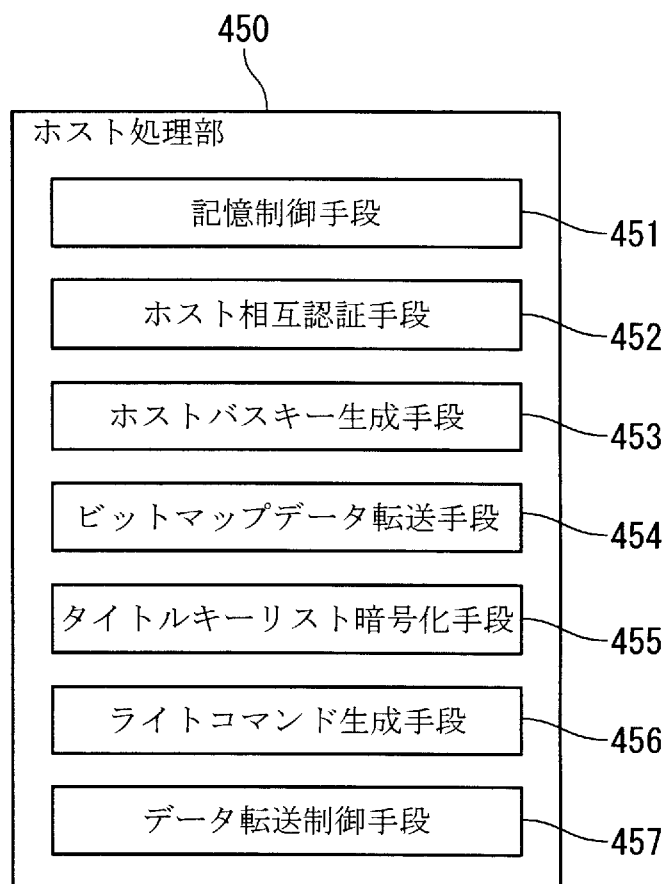
[図3]



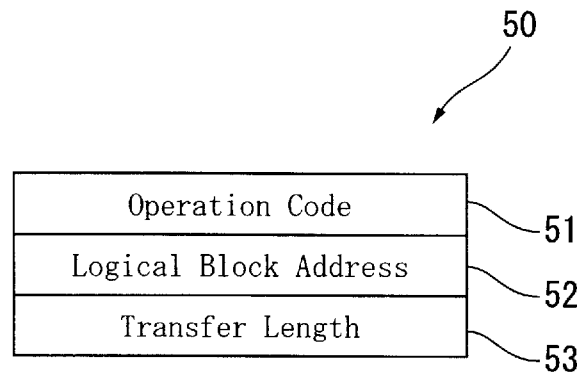
[図4]



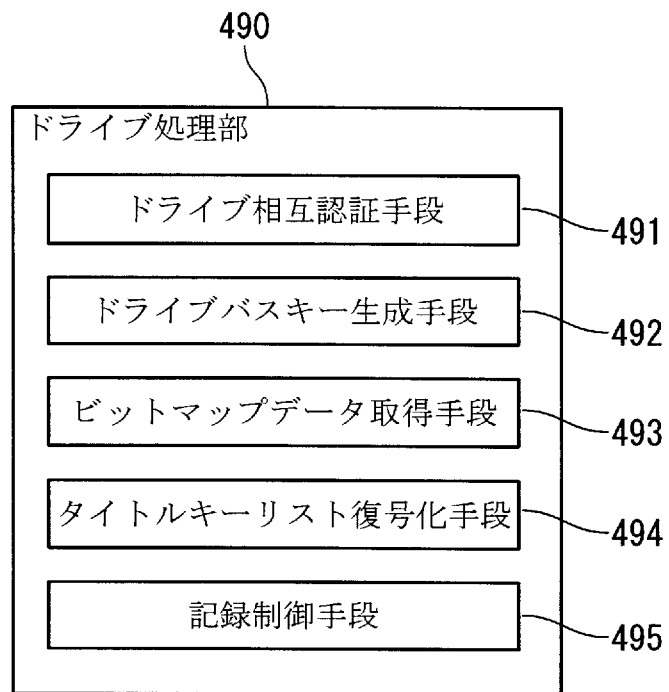
[図5]



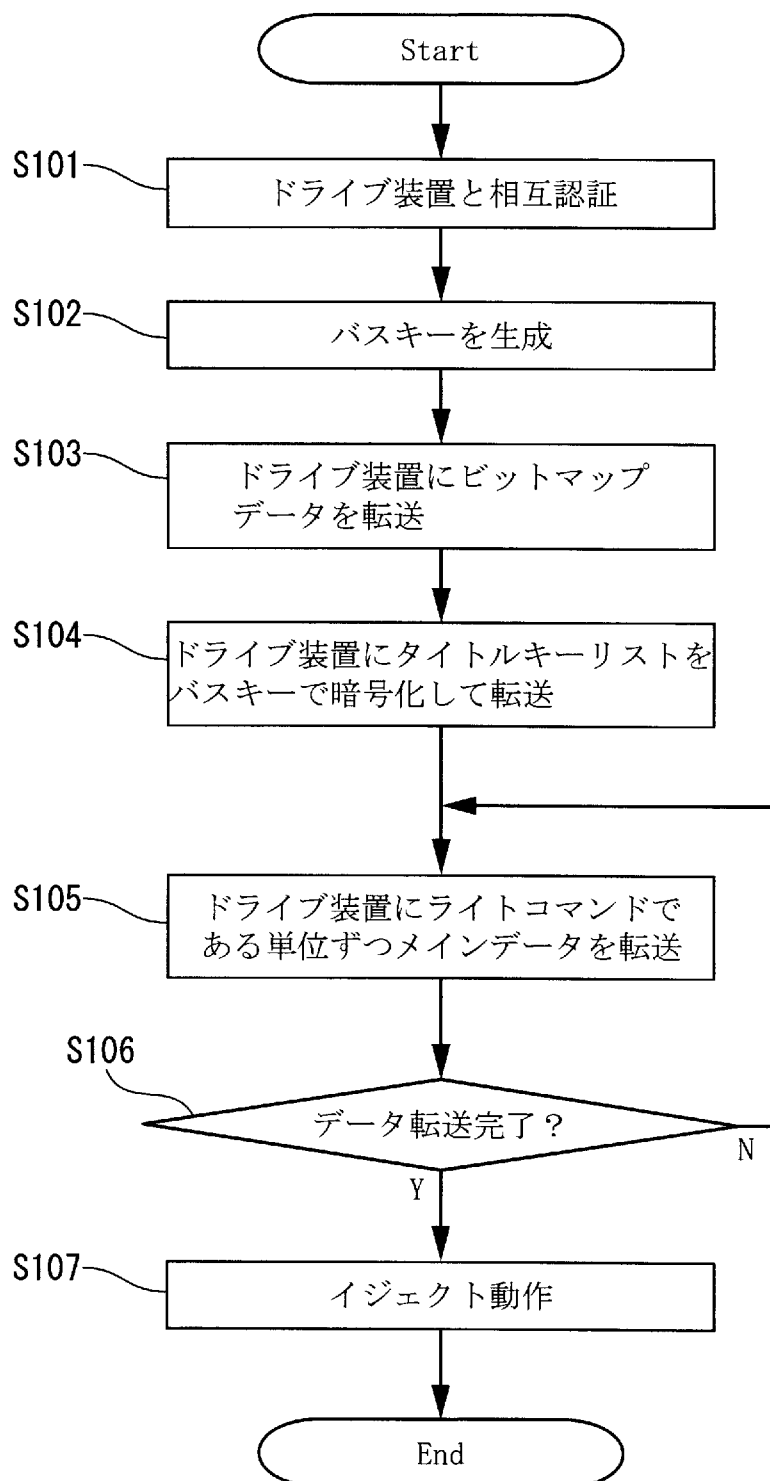
[図6]



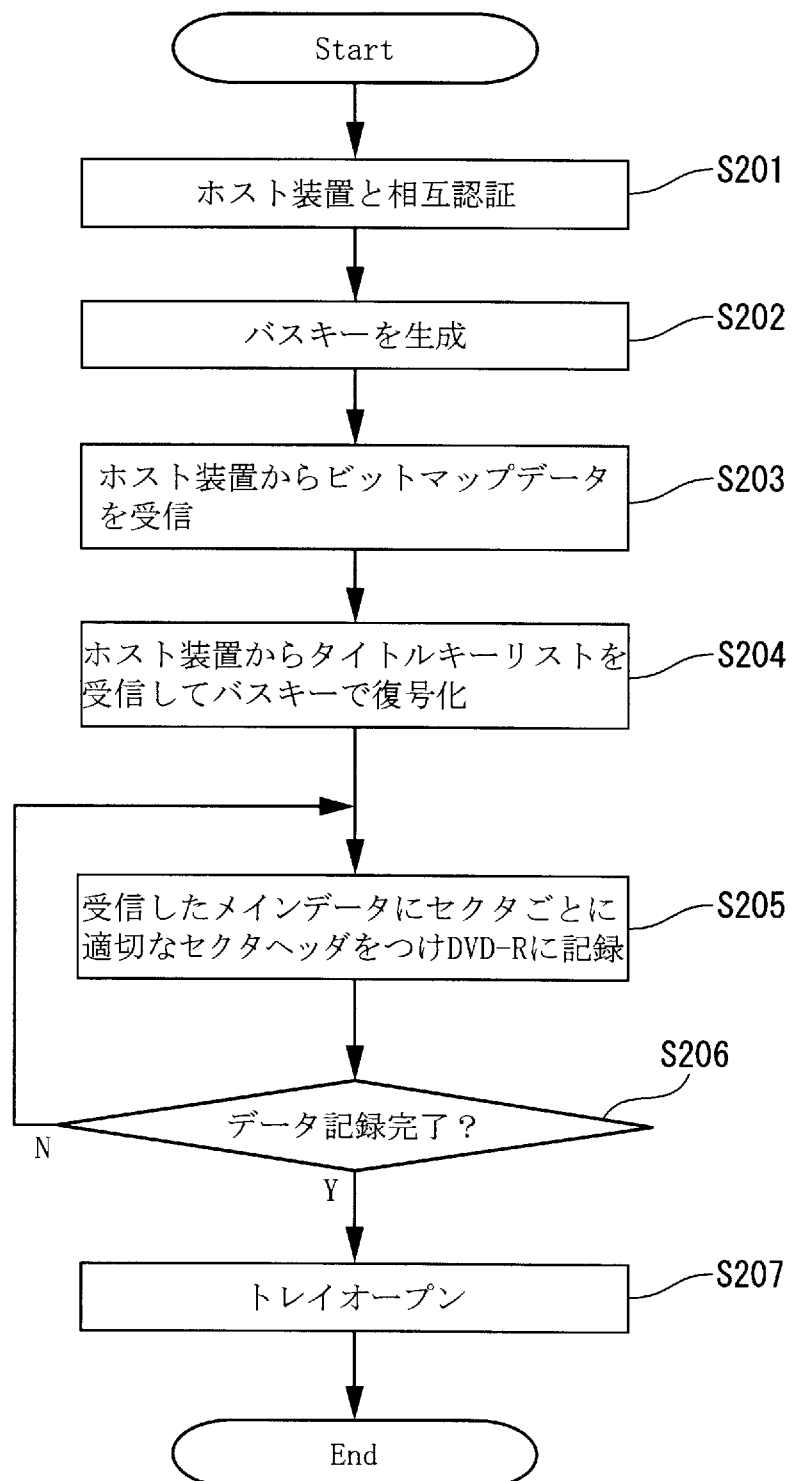
[図7]



[図8]

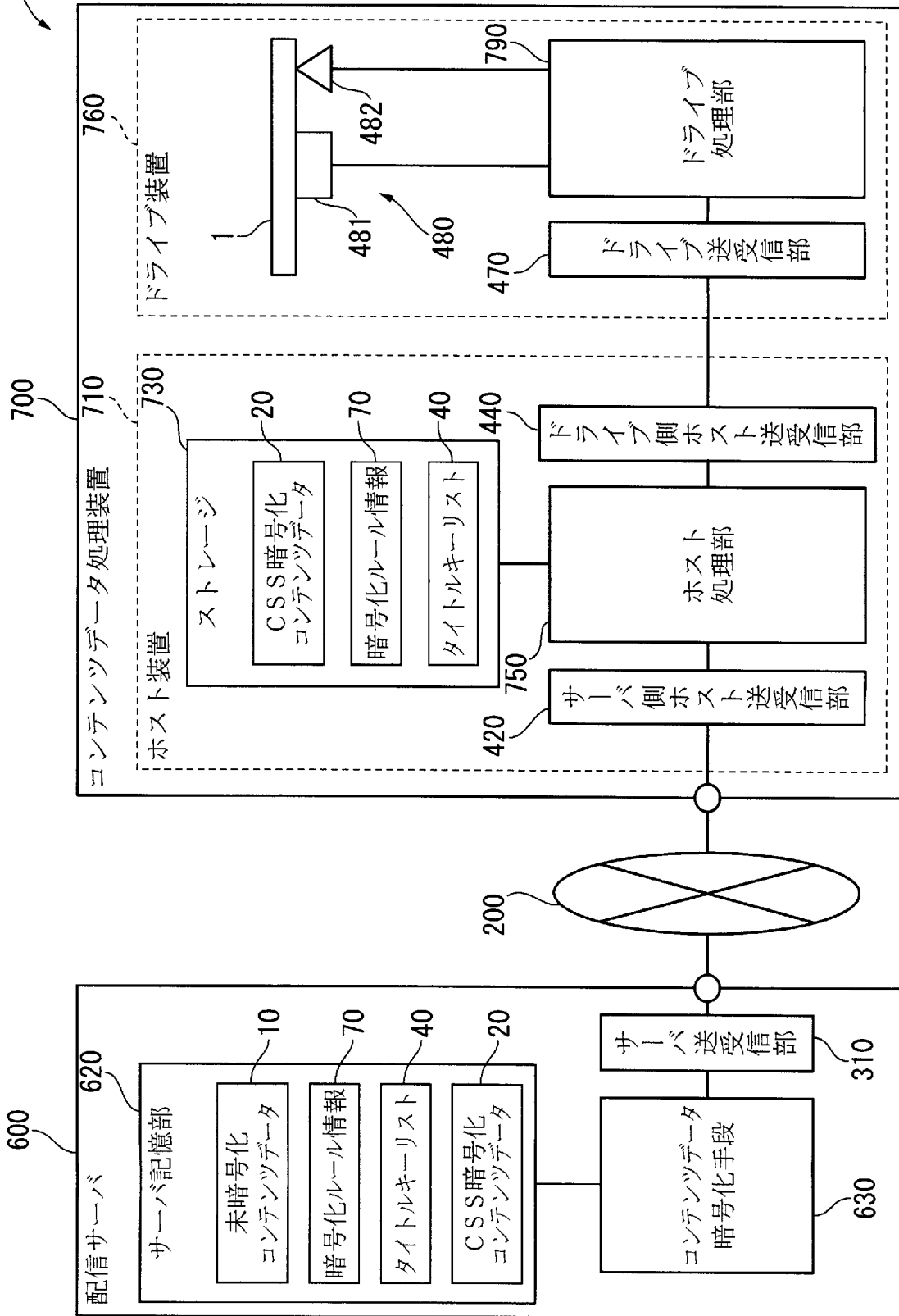


[図9]

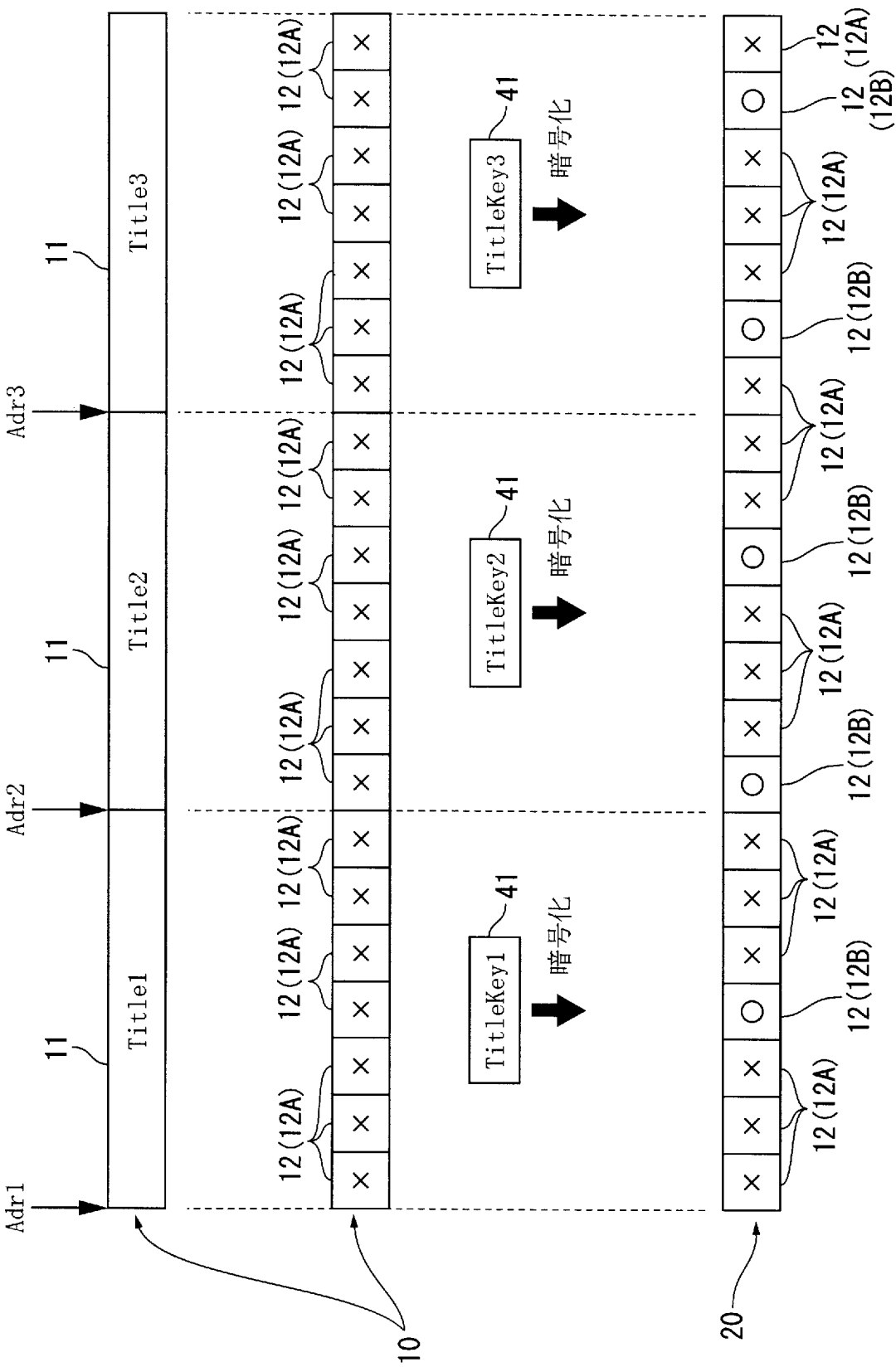


[図10]

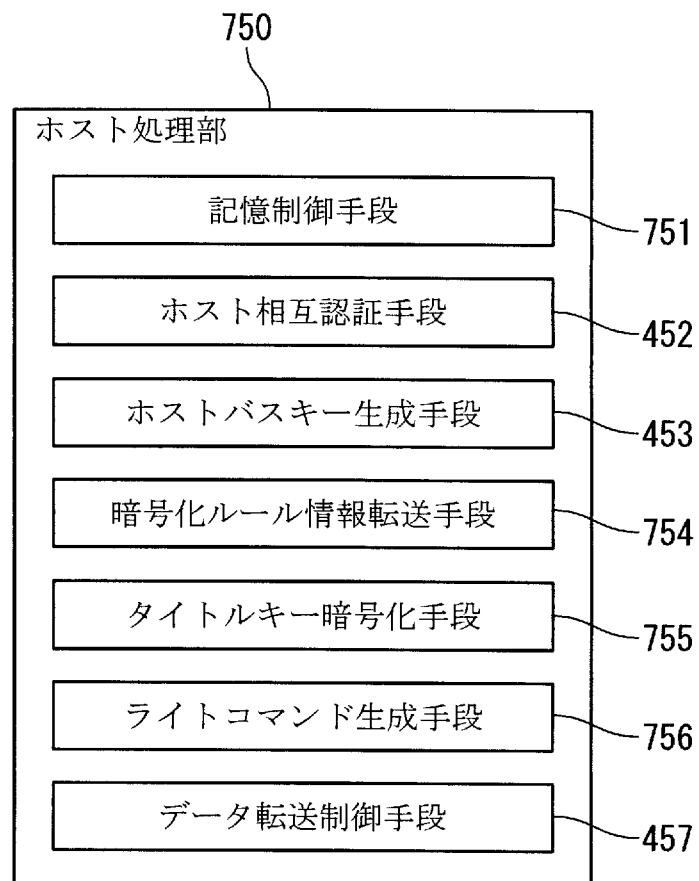
100B



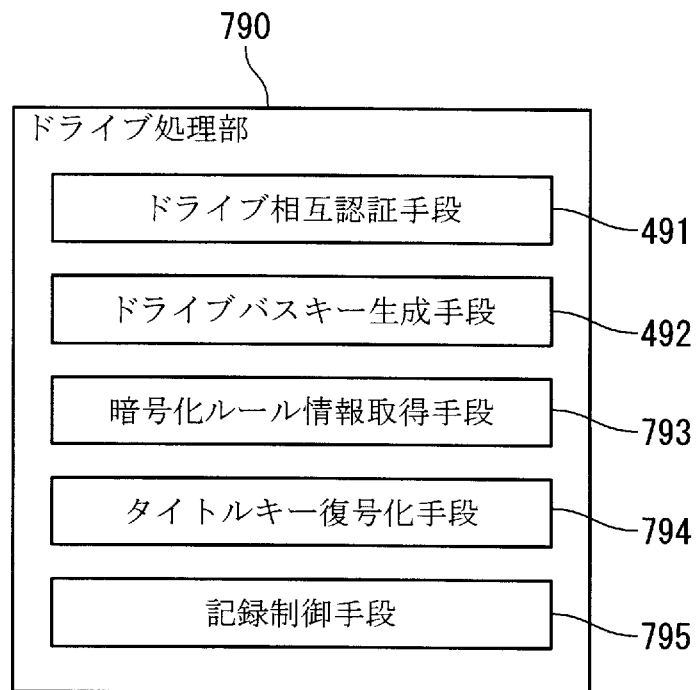
[図11]



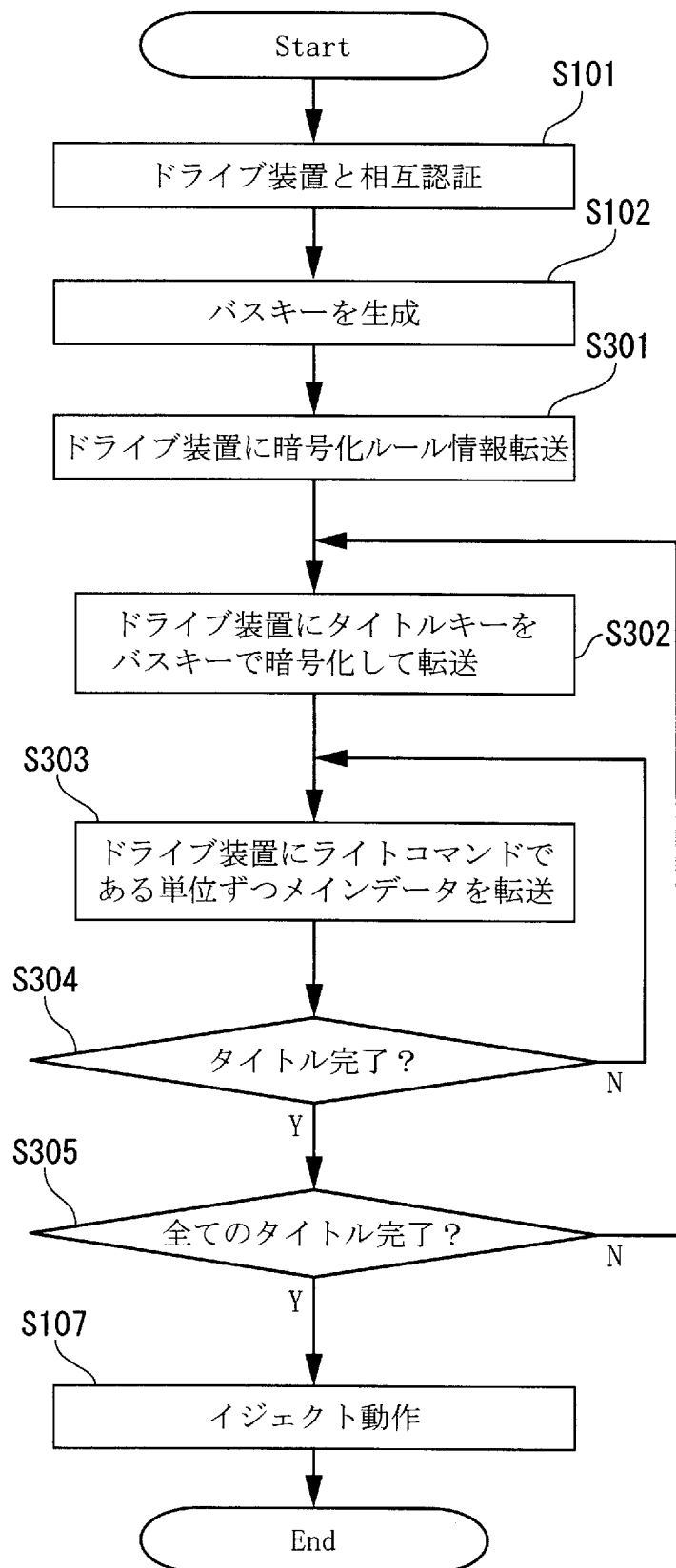
[図12]



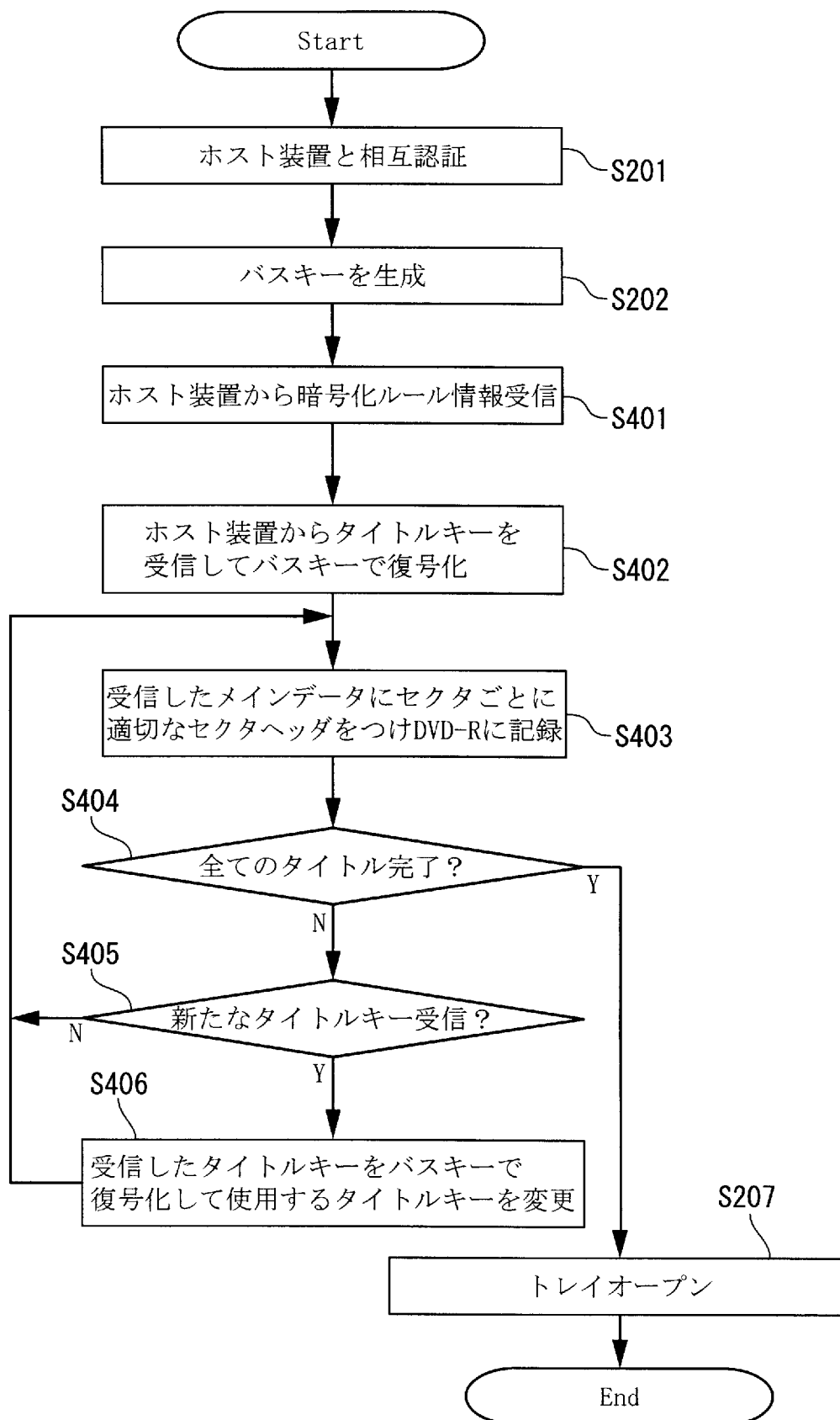
[図13]



[図14]



[図15]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2007/052968

A. CLASSIFICATION OF SUBJECT MATTER

H04L9/08(2006.01)i, G06F13/00(2006.01)i, G09C1/00(2006.01)i, G11B20/10(2006.01)i, H04L9/10(2006.01)i

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)

H04L9/08, G06F13/00, G09C1/00, G11B20/10, H04L9/10

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	1996-2007
Kokai Jitsuyo Shinan Koho	1971-2007	Toroku Jitsuyo Shinan Koho	1994-2007

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.
X Y	JP 2002-9757 A (Casio Computer Co., Ltd.), 11 January, 2002 (11.01.02), Figs. 2 to 21; Par. Nos. [0016], [0034], [0023], [0039] & US 2001/0053221 A1	1-4, 7, 19 5, 6, 8-18, 20
X Y	JP 2001-156771 A (Victor Company Of Japan, Ltd.), 08 June, 2001 (08.06.01), Fig. 1; Par. No. [0021] (Family: none)	1, 4, 7, 19 5, 6, 8-18, 20
Y	JP 2002-158654 A (Hitachi, Ltd.), 31 May, 2002 (31.05.02), Fig. 11; Par. Nos. [0141] to [0149] & US 2003/0097575 A1	5-6, 8, 9, 13, 15, 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
11 April, 2007 (11.04.07)

Date of mailing of the international search report
24 April, 2007 (24.04.07)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2007/052968

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2004-70049 A (Denso Corp.), 04 March, 2004 (04.03.04), Fig. 2 & US 2005/0249348 A1	5-6, 8, 9, 13, 15, 16
Y	JP 2005-109840 A (Sony Corp.), 21 April, 2005 (21.04.05), Figs. 10 to 27; Par. No. [0047] & WO 2005/034422 A1	6, 8-18, 20
A	JP 11-88859 A (International Business Machines Corp.), 30 March, 1999 (30.03.99), Full text & EP 887723 A2	1-20

A. 発明の属する分野の分類（国際特許分類（I P C）） Int.Cl. H04L9/08(2006.01)i, G06F13/00(2006.01)i, G09C1/00(2006.01)i, G11B20/10(2006.01)i, H04L9/10(2006.01)i												
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（I P C）） Int.Cl. H04L9/08, G06F13/00, G09C1/00, G11B20/10, H04L9/10												
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 <table border="0"> <tr> <td>日本国実用新案公報</td> <td>1 9 2 2－1 9 9 6年</td> </tr> <tr> <td>日本国公開実用新案公報</td> <td>1 9 7 1－2 0 0 7年</td> </tr> <tr> <td>日本国実用新案登録公報</td> <td>1 9 9 6－2 0 0 7年</td> </tr> <tr> <td>日本国登録実用新案公報</td> <td>1 9 9 4－2 0 0 7年</td> </tr> </table>				日本国実用新案公報	1 9 2 2－1 9 9 6年	日本国公開実用新案公報	1 9 7 1－2 0 0 7年	日本国実用新案登録公報	1 9 9 6－2 0 0 7年	日本国登録実用新案公報	1 9 9 4－2 0 0 7年	
日本国実用新案公報	1 9 2 2－1 9 9 6年											
日本国公開実用新案公報	1 9 7 1－2 0 0 7年											
日本国実用新案登録公報	1 9 9 6－2 0 0 7年											
日本国登録実用新案公報	1 9 9 4－2 0 0 7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 <table border="1"> <thead> <tr> <th>引用文献の カテゴリー*</th> <th>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</th> <th>関連する 請求の範囲の番号</th> </tr> </thead> <tbody> <tr> <td>X Y</td> <td>J P 2 0 0 2－9 7 5 7 A（カシオ計算機株式会社） 2 0 0 2.0 1.1 1, 第2－2 1図、【0 0 1 6】、【0 0 3 4】、 【0 0 2 3】、【0 0 3 9】段落 & U S 2 0 0 1 / 0 0 5 3 2 2 1 A 1</td> <td>1-4, 7, 19 5, 6, 8-18, 20</td> </tr> <tr> <td>X Y</td> <td>J P 2 0 0 1－1 5 6 7 7 1 A（日本ビクター株式会社） 2 0 0 1.0 6.0 8, 第1図、【0 0 2 1】段落 （ファミリーなし）</td> <td>1, 4, 7, 19 5, 6, 8-18, 20</td> </tr> </tbody> </table>				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	X Y	J P 2 0 0 2－9 7 5 7 A（カシオ計算機株式会社） 2 0 0 2.0 1.1 1, 第2－2 1図、【0 0 1 6】、【0 0 3 4】、 【0 0 2 3】、【0 0 3 9】段落 & U S 2 0 0 1 / 0 0 5 3 2 2 1 A 1	1-4, 7, 19 5, 6, 8-18, 20	X Y	J P 2 0 0 1－1 5 6 7 7 1 A（日本ビクター株式会社） 2 0 0 1.0 6.0 8, 第1図、【0 0 2 1】段落 （ファミリーなし）	1, 4, 7, 19 5, 6, 8-18, 20
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										
X Y	J P 2 0 0 2－9 7 5 7 A（カシオ計算機株式会社） 2 0 0 2.0 1.1 1, 第2－2 1図、【0 0 1 6】、【0 0 3 4】、 【0 0 2 3】、【0 0 3 9】段落 & U S 2 0 0 1 / 0 0 5 3 2 2 1 A 1	1-4, 7, 19 5, 6, 8-18, 20										
X Y	J P 2 0 0 1－1 5 6 7 7 1 A（日本ビクター株式会社） 2 0 0 1.0 6.0 8, 第1図、【0 0 2 1】段落 （ファミリーなし）	1, 4, 7, 19 5, 6, 8-18, 20										
☒ 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、国際出願日以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		の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 1 1 . 0 4 . 2 0 0 7		国際調査報告の発送日 2 4 . 0 4 . 2 0 0 7										
国際調査機関の名称及びあて先 日本国特許庁（I S A / J P） 郵便番号1 0 0－8 9 1 5 東京都千代田区霞が関三丁目4番3号		<table border="1"> <tr> <td>特許庁審査官（権限のある職員）</td> <td>5 S</td> <td>9 4 6 9</td> </tr> <tr> <td>石田 信行</td> <td colspan="2"></td> </tr> <tr> <td>電話番号 0 3－3 5 8 1－1 1 0 1</td> <td>内線</td> <td>3 5 4 6</td> </tr> </table>		特許庁審査官（権限のある職員）	5 S	9 4 6 9	石田 信行			電話番号 0 3－3 5 8 1－1 1 0 1	内線	3 5 4 6
特許庁審査官（権限のある職員）	5 S	9 4 6 9										
石田 信行												
電話番号 0 3－3 5 8 1－1 1 0 1	内線	3 5 4 6										

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
Y	J P 2 0 0 2 - 1 5 8 6 5 4 A (株式会社日立製作所) 2 0 0 2 . 0 5 . 3 1 , 第 1 1 図、【 0 1 4 1 】 - 【 0 1 4 9 】 段落 & U S 2 0 0 3 / 0 0 9 7 5 7 5 A 1	5-6, 8, 9, 13, 15, 16
Y	J P 2 0 0 4 - 7 0 0 4 9 A (株式会社デンソー) 2 0 0 4 . 0 3 . 0 4 , 第 2 図 & U S 2 0 0 5 / 0 2 4 9 3 4 8 A 1	5-6, 8, 9, 13, 15, 16
Y	J P 2 0 0 5 - 1 0 9 8 4 0 A (ソニー株式会社) 2 0 0 5 . 0 4 . 2 1 , 第 1 0 - 2 7 図、【 0 0 4 7 】 段落 & W O 2 0 0 5 / 0 3 4 4 2 2 A 1	6, 8-18, 20
A	J P 1 1 - 8 8 8 5 9 A (インターナショナル・ビジネス・マシーンズ・コーポレーション) 1 9 9 9 . 0 3 . 3 0 , 全文 & E P 8 8 7 7 2 3 A 2	1-20