

(19) 世界知的所有権機関
国際事務局(43) 国際公開日
2009 年 1 月 22 日 (22.01.2009)

PCT

(10) 国際公開番号
WO 2009/011049 A1

(51) 国際特許分類:

G11B 20/10 (2006.01) H04L 9/32 (2006.01)
G06F 21/24 (2006.01)

(21) 国際出願番号:

PCT/JP2007/064180

(22) 国際出願日:

2007 年 7 月 18 日 (18.07.2007)

(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): 片多 啓二 (KATATA, Keiji) [JP/JP]; 〒3502288 埼玉県鶴ヶ島市富士見 6 丁目 1 番 2 号 パイオニア株式会社 総合研究所内 Saitama (JP).

(74) 代理人: 江上 達夫, 外 (EGAMI, Tatsuo et al.); 〒1040031 東京都中央区京橋一丁目 16 番 10 号 オークビル京橋 3 階 東京セントラル特許事務所内 Tokyo (JP).

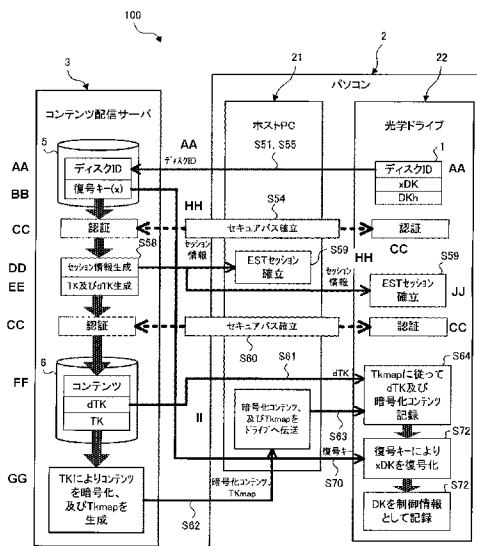
(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK,

[続葉有]

(54) Title: INFORMATION RECORDING MEDIUM, DRIVING DEVICE, SERVER DEVICE FOR MANAGING CHARGE FOR DISTRIBUTION, CONTENT SERVER DEVICE, AND INTERMEDIATION DEVICE

(54) 発明の名称: 情報記録媒体、ドライブ装置、配信課金管理用のサーバ装置、コンテンツサーバ装置、及び仲介装置

[図5]



3 CONTENT DISTRIBUTION SERVER

AA DISK ID

BB DECODING KEY (x)

CC AUTHENTICATION

DD GENERATE SESSION INFORMATION

EE GENERATE TK AND dTK

FF CONTENT

GG ENCODE CONTENT, AND GENERATE Tkmap BY TK

HH SESSION INFORMATION

2 PERSONAL COMPUTER

21 HOST PC

S54 ESTABLISH SECURE BUS

S59 ESTABLISH EST SESSION

S60 ESTABLISH SECURE BUS

II TRANSMIT ENCODED CONTENT AND Tkmap TO DRIVE

S62 ENCODED CONTENT, Tkmap

22 OPTICAL DRIVE

JJ ESTABLISH EST SESSION

S64 RECODE dTK AND ENCODED CONTENT ACCORDING TO Tkmap

S70 DECODING KEY

S72 DECODE xDK BY DECODING KEY

S72 RECORD DK AS CONTROL INFORMATION

(57) Abstract: An information recording medium (1) comprises a content recordable area (34) in which a content at least partially distributed from a server device (3) to a client device (2) through a network (20) can be recorded by the driving device of the client device, a control information recordable area (33) in which control information used for reproducing the content from the content recordable area can be recorded by the driving device, and a characteristic information recorded area (32) in which characteristic information which includes medium identification information for identifying the information recording medium and medium authentication information for authenticating the information recording medium between the driving device and the server device is recorded in advance. This keeps the secrecy of data communicated between the driving device and the server device to prevent unfair recording behaviors.

(57) 要約: 情報記録媒体 (1) は、サーバ装置 (3) 側からネットワーク (20) を介してクライアント装置 (2) 側へ少なくとも部分的に配信されるコンテンツをクライアント装置のドライブ装置で記録可能であるコンテンツ記録可能エリア (34) と、コンテンツ記録可能エリアからコンテンツを再生するのに用いられる制御情報を、ドライブ装置で記録可能である制御情報記録可能エリア (33) と、当該情報記録媒体を識別する媒体識別情報、並びにドライブ装置及びサーバ装置間で当該情報記録媒体についての認証を行うための媒体認証情報を含む固有情報が予め記録されている固有情報記録済みエリア (32) とを備える。これにより、ドライブ装置及びサーバ装置間で通信されるデータの秘密を保持して、不正な記録行為を防止する。



DM, DO, 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, LY, MA, MD, ME, 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.

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, MT, 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,

添付公開書類:

— 国際調査報告書

明 細 書

情報記録媒体、ドライブ装置、配信課金管理用のサーバ装置、コンテンツサーバ装置、及び仲介装置

技術分野

[0001] 本発明は、例えばインターネット等のネットワークを介して、サーバ装置からクライアント装置へ配信され、課金の対象となるコンテンツを記録するための情報記録媒体の技術分野に関する。本発明は更に、該クライアント装置側に設けられ、該情報記録媒体にコンテンツを記録するためのドライブ装置、該コンテンツの配信及び課金を管理するためのサーバ装置、前記コンテンツを配信するコンテンツサーバ装置、並びに該ドライブ装置及び前記サーバ装置間を仲介する仲介装置の技術分野に関する。

背景技術

[0002] この種の情報記録媒体として、例えばDVDに、CSS (Contents Scramble System: コンテンツスクランブルシステム) といった暗号化技術を用いて、情報の書き込みが行われる。具体的には、サーバ装置から配信されるコンテンツが、例えばパソコンや光ディスクレコーダのクライアント装置に内蔵されるHDD (Hard Disc Drive: ハードディスクドライブ) にダウンロードされる。このダウンロードされたコンテンツが、CSSエンコードされ、CSS規格のDVD或いは光ディスクに書き込まれる (特許文献1及び2参照)。

[0003] 特許文献1: 国際公開WO2007/010987号公報

特許文献2: 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

[0004] しかしながら、上述の技術背景によれば、CSSは、一般的なコピープロテクションの規格であって、ライセンス無しで使用可能である。このため、正規に取得したデータを元に、CSS規格のDVD或いは光ディスクが複製可能であって、これが、不正に販売されてしまうといった技術的問題点がある。

[0005] また、クライアント装置及びサーバ装置間のデータ通信において、パソコン等を含

むクライアント装置を不正に操ることで、コンテンツの取得権利を有する正規のユーザに成り済ました第三者によって、サーバ装置からのコンテンツが不正に取得されたり、該DVD或いは光ディスクに予め記録されているコンテンツの情報や、課金情報等のデータが差し替えられたり、記録されている或いは記録しようとするコンテンツが、許諾されていない他のコンテンツに差し替えられてしまうといった技術的問題点がある。

[0006] 本発明は、上述した問題点に鑑みなされたものであり、例えば、クライアント装置及びサーバ装置間で通信されるデータの秘密を保持して、不正な記録行為を防止することを可能ならしめる情報記録媒体、該情報記録媒体にコンテンツを記録するためのドライブ装置、該コンテンツの配信及び課金を管理するためのサーバ装置、前記コンテンツを配信するコンテンツサーバ装置、並びに該ドライブ装置及び前記サーバ装置間を仲介する仲介装置を提供することを課題とする。

課題を解決するための手段

[0007] 本発明に係る情報記録媒体は上記課題を解決するために、ネットワークに收容されるサーバ装置及びクライアント装置を備えるシステムに利用され、該クライアント装置のドライブ装置で記録可能な情報記録媒体であって、前記サーバ装置側から前記ネットワークを介して前記クライアント装置側へ少なくとも部分的に配信されるコンテンツを前記ドライブ装置で記録可能であるコンテンツ記録可能エリアと、前記コンテンツ記録可能エリアから前記コンテンツを再生するのに用いられる制御情報を、前記ドライブ装置で記録可能である制御情報記録可能エリアと、当該情報記録媒体を識別する媒体識別情報、並びに該媒体識別情報と対をなすと共に前記クライアント装置及び前記ドライブ装置間で当該情報記録媒体についての認証を行うための媒体認証情報を含む固有情報が予め記録されている固有情報記録済みエリアとを備える。

[0008] 本発明の情報記録媒体によれば、例えばインターネット等のネットワークには、例えば映画、ドラマ等の配信用のサーバ装置と、例えばハードディスク内蔵型の光ディスクレコーダ、パソコン等のクライアント装置とが、收容されている。クライアント装置は特に、例えば光ディスクドライブなどのドライブ装置を備える。このようなシステムに利用される情報記録媒体として、例えばDVD、BD等の光ディスクや、ポータブルタイプ

の各種メモリなどがある。このような情報記録媒体が、クライアント装置のドライブ装置にセット可能である。

[0009] ここで、コンテンツの販売方法として、コンテンツを取得したいユーザは、例えば店舗販売や通信販売にて、プリペイドされる金額又はこれを若干上乗せ若しくは値引きした金額を、現金やクレジットで支払った上で、コンテンツを記録可能な情報記録媒体を取得する。このように、ユーザによって情報記録媒体が取得された後に、ドライブ装置にセットされると、サーバ装置から、クライアント装置にコンテンツが配信されると共に、この配信されたコンテンツがドライブ装置によってコンテンツ記録可能エリアに記録される。この際、例えばタイトルキー等を用いたCSS方式で暗号化された形で記録されてよい。或いは、暗号化された又はされないコンテンツの一部又は全部が、予め、コンテンツ記録可能エリアに記録されていてもよい。コンテンツの記録状況がどちらであれ、サーバ装置によって、記録の完了がベリファイ或いは確認されることで、次に説明するようにコンテンツを再生するのに用いられる、例えば、DKB(DK、ディスクID、DKBh、DAK)を含んでなる制御情報の取得が、情報記録媒体にて可能となる。

[0010] より具体的には、例えばR-CDZ(即ち、当初は空であると共に書き込み可能なCDZ(コントロールデータゾーン)である制御情報記録可能エリアを、この取得された制御情報で記録済みとすることで、ユーザは自らの所有物として自由に再生することが可能となる。尚、ディスクIDに関連付けられたユーザに対して課金されるのであれば、プリペイドでなくても(即ち、後払いでも)よい。

[0011] このため、情報記録媒体は、サーバ装置側からクライアント装置側へ少なくとも部分的に配信されるコンテンツが記録されるコンテンツ記録可能エリアと、例えばディスクID、ESTsession情報、ディスクキー等の、該コンテンツを再生するのに用いられる制御情報が記録される制御情報記録可能エリアとを備える。制御情報記録可能エリアは、コンテンツが記録される前には、空の状態とされている。即ち、コンテンツ記録可能エリアに、コンテンツが記録されただけでは、制御情報記録可能エリアに制御情報は(少なくとも完全な状態では)存在しないので、コンテンツを再生することは不可能である。

[0012] 本発明では特に、情報記録媒体は、例えばP-DKBZ(プリ・レコーデッドDKBゾーン)である固有情報記録済みエリアを更に備える。固有情報記録済みエリアは、当該情報記録媒体を識別する媒体識別情報、及び当該情報記録媒体についての認証(ECA:Enhanced CSS Authentication)を行うための媒体認証情報を含む、例えばP-DKB(xDK、ディスクID、DKBh、DAK)等を含んでなる固有情報が予め記録されている。ここで「情報記録媒体についての認証」とは、サーバ装置が配信するコンテンツの取得権利を有する、正当な情報記録媒体であることを、確認することを意味する。「媒体認証情報」は、媒体識別情報と対をなす、例えば媒体単位認証キー(DAK)であり、情報記録媒体がセットされるドライブ装置の他に、サーバ装置でも、媒体識別情報に基づいて独自に取得される。サーバ装置では、例えば、販売済みである多数の情報記録媒体に対応付けられた形で各情報記録媒体に固有の媒体認証情報が予め格納されているデータベースから、各媒体識別情報に対応する媒体認証情報が独自に取得される。ここでの「認証」の方法として、例えばチャレンジ／レスポンス認証が採用される。具体的には、ドライブ装置側で読み取られた媒体認証情報が、サーバ装置側で独自に取得された媒体認証情報と一致することが確認される。媒体認証情報の一致が確認されることで、認証が成功すると、例えば情報記録媒体に係る、ディスクIDや、配信されるコンテンツ等の情報を、ドライブ装置及びサーバ装置間で直接に通信するための通信経路が確立される。このような媒体認証情報を含んでなる固有情報は、情報記録媒体について認証するのに用いられる他に、コンテンツの再生を可能ならしめる制御情報を取得するのに用いられる。

[0013] このように構成された情報記録媒体がドライブ装置にセットされると、ドライブ装置では、コンテンツのダウンロードと相前後して又は並行して、固有情報記録済みエリアから固有情報が読み取られて、例えばディスクIDである媒体識別情報が、ネットワークを介してサーバ装置側に送信される。すると、サーバ装置側では、例えば媒体識別情報に対応付けて媒体認証情報を格納する格納手段から、送信された媒体識別情報に対応する媒体認証情報が抽出される。ドライブ装置で固有情報記録済みエリアから読み取られた媒体認識情報が、サーバ装置側で独自に抽出された媒体認識情報と一致することが確認されると、ドライブ装置及びサーバ装置間で通信経路が確立

される。この後、コンテンツ記録可能エリアに対するコンテンツの記録状況が確認される。

[0014] サーバ装置側でコンテンツ記録可能エリアへのコンテンツの記録が完了していることが確認された後に、例えばサーバ装置側からされた取得用情報によって、クライアント装置側で或いはドライブ装置で制御情報が取得される。更に、取得された制御情報が制御情報記録可能エリアに記録される。こうして、当該情報記録媒体は、コンテンツの再生が可能な状態とされる。

[0015] 以上のように本発明の情報記録媒体によれば、媒体識別情報と対をなす媒体認証情報を用いて、ドライブ装置及びサーバ装置間で情報記録媒体についての認証を行い、この認証が成功した場合に、ドライブ装置及びサーバ装置間で通信経路が確立され、確立された通信経路を介して、ドライブ装置及びサーバ装置間でデータが通信される。従って、例えば第三者が、ドライブ装置とは別にクライアント装置を構成するパソコン等を悪用することで(典型的には、ソフトウェア或いはコンピュータプログラムを改竄することで)、正規のユーザに成り済まして、サーバ装置からのコンテンツを不正に取得しようとも、ドライブ装置で媒体認証情報が取得されず、認証が失敗に終わる。或いは、ドライブ装置とは別にクライアント装置を構成するパソコン等を悪用することで、通信経路を介して送信される、例えば制御情報を取得するための情報等を、読み取る或いは差し替えることは困難又は実践上不可能であるので、コンテンツを再生可能な状態にある情報記録媒体は得られない。他方で、正規のユーザに成り済ますためのドライブ装置内のロジック変更等は、一般ユーザや専門家にとって困難であると共にコストが高く付くので、不正を実行しようとする気を削ぐに十二分な効果が発揮される。

[0016] このように、情報記録媒体についての認証により、コンテンツの取得権利におけるセキュリティ性を向上させると共に、クライアント装置が備えるドライブ装置及びサーバ装置間の通信経路により、通信データの秘密を保持することができる。よって、結果として、不正な記録行為を防止して、コンテンツ配布におけるセキュリティ性を向上させることができる。

[0017] 本発明に係る情報記録媒体の一態様では、前記ドライブ装置は、前記コンテンツ

記録可能エリアに、前記認証が行われた後に前記サーバ装置側から前記ネットワークを介して前記ドライブ装置へ配信される、前記コンテンツを構成するタイトルに個別に割り当てられるタイトル単位暗号キーを、記録可能である。

[0018] この態様によれば、当該情報記録媒体についての認証が行われた後に、サーバ装置側からネットワークを介してドライブ装置に、タイトル単位暗号キーが配信される。配信されたタイトル単位暗号キーは、コンテンツ記録可能エリアに記録される。ここで「タイトル単位暗号キー」は、例えばdTKであり、コンテンツを構成するタイトルに個別に割り当てられ、典型的には、暗号化されたコンテンツと共に、コンテンツ記録可能エリアに記録される。「タイトル単位キー」は、例えばTKであり、暗号化されることで、タイトル単位暗号キーとなる。この場合に、情報記録媒体についての認証が成功した後に、サーバ装置側では、媒体識別情報に対応するタイトル単位暗号キーが、通信経路を介して、ドライブ装置に送信される。この送信されたタイトル単位暗号キーと共に、タイトル単位キーで暗号化されたコンテンツが記録される。暗号化されたコンテンツの記録が完了された後は、再生装置(DVDプレーヤー等)で、タイトル単位キーを用いて復号化することで、コンテンツの再生が可能とされる。このように、コンテンツの再生に際して、サーバ装置によってタイトル単位暗号キーが送信される必要があるので、コンテンツの取得権利におけるセキュリティ性を向上させることができる。

[0019] 本発明の情報記録媒体の他の態様では、前記媒体識別情報は、前記制御情報を取得するのに用いられる取得用情報を前記サーバ装置側から配信させるための配信指定情報としても機能する。

[0020] この態様によれば、媒体識別情報は、例えばディスクIDである配信指定情報としても機能し、サーバ装置側に送信される。サーバ装置では、送信された媒体識別情報に対応する取得用情報が取得される。ここで「取得用情報」は、例えば復号キーxであり、制御情報を取得するのに用いられる。取得用情報は、サーバ装置側からクライアント装置側或いはドライブ装置に配信される。このように、コンテンツの再生に際して、サーバ装置によって配信される取得用情報を取得する必要があるので、コンテンツの取得権利におけるセキュリティ性を向上させることができる。

[0021] この態様では、前記取得用情報は、前記配信されるコンテンツが記録されたことが

確認された後に前記サーバ装置側から配信される復号化用情報であり、前記固有情報は、前記制御情報の少なくとも一部が暗号化されてなる暗号化情報であって、前記復号化用情報により復号化が可能である前記暗号化情報を更に含み、前記制御情報記録可能エリアには、前記暗号化情報が復号化されてなる前記制御情報の少なくとも一部が記録可能である。

[0022] この態様によれば、固有情報は、暗号化情報を含んでいる。ここで「暗号化情報」は、例えばxDKであり、制御情報の少なくとも一部(例えばDK)が暗号化されたものであって、復号化用情報により復号化される。「復号化用情報」は、例えば復号キーxであり、サーバ装置側からクライアント装置側或いはドライブ装置に配信され、クライアント装置側或いはドライブ装置で暗号化情報を復号化するのに用いられる。この場合に、配信されたコンテンツの記録が完了した後に、サーバ装置側から、媒体識別情報に対応する復号化用情報がクライアント装置側或いはドライブ装置に配信される。クライアント装置側或いはドライブ装置では、配信された復号化用情報により、固有情報記録済みエリアに記録されている暗号化情報が復号化され、復号化された暗号化情報が制御情報として制御情報記録可能エリアに記録される。このように、制御情報の少なくとも一部が暗号化されており、コンテンツの再生に用いられる制御情報の取得が困難とされるので、悪意あるユーザの犯罪意欲を低下させ、結果として、コンテンツの取得権利におけるセキュリティ性を向上させることができる。

[0023] 本発明に係るドライブ装置は上記課題を解決するために、上述した本発明に係る情報記録媒体(但し、その各種態様を含む)の記録再生用に前記クライアント装置側に設けられる前記ドライブ装置であって、前記コンテンツ記録可能エリア、前記制御情報記録可能エリア及び前記固有情報記録済みエリアに対し読み取り可能であり、前記コンテンツ記録可能エリア及び前記制御情報記録可能エリアに対し書き込み可能である読取書込手段と、前記固有情報記録済みエリアから前記媒体識別情報及び前記媒体認証情報を読み取るように前記読取書込手段を制御し、前記コンテンツ記録可能エリアに対し、前記コンテンツを書き込むように前記読取書込手段を制御する制御手段と、前記読み取られた媒体認証情報に基づくバスキーによって前記サーバ装置及び当該ドライブ装置間に、バスキー通信経路を確立する通信経路確立手

段と、前記読み取られた媒体識別情報を、前記ネットワークを介して前記サーバ装置側へ送信すると共に、前記確立されたバスキー通信経路を介して前記サーバ装置側から配信され、前記制御情報の一部若しくは該一部を取得するための取得用情報又は前記コンテンツ記録可能エリアから前記コンテンツを再生するのに用いられる他の制御情報の少なくとも一部であり、前記クライアント装置側に設けられ、前記ドライブ装置を制御することで前記ドライブ装置及び前記サーバ装置間を仲介する仲介装置に対して秘匿される秘匿情報を、受信するドライブ側通信手段とを備え、前記制御手段は、前記受信される秘匿情報を前記コンテンツ記録可能エリア及び前記制御情報記録可能エリアの少なくとも一方に書き込むように前記書込手段を制御する。

- [0024] 本発明のドライブ装置によれば、特に、制御情報記録可能エリアへの読取書込手段、サーバ装置及びドライブ装置間にバスキー通信経路を確立する通信経路確立手段、及びバスキー通信経路を介して配信される秘匿情報を受信するドライブ側通信手段を備える。ここで「バスキー通信経路」は、媒体認証情報に基づいて、サーバ装置及びドライブ装置間で情報記録媒体についての認証が成功した後に、サーバ装置及びドライブ装置でバスキーを生成し、これを共有することにより、確立される。「バスキー」は、例えばBKであり、サーバ装置及びドライブ装置間で通信されるデータを、暗号化或いは復号化するのに用いられる。この場合に、ドライブ装置で読み取られた媒体識別情報がネットワークを介してサーバ装置側に送信される。サーバ装置側では、送信された媒体識別情報に対応する秘匿情報が、バスキー通信経路を介してドライブ装置に配信される。ここで「秘匿情報」は、制御情報の一部(DK)、若しくは例えば復号キーxである取得用情報、又は例えば暗号化情報(xDK)、媒体識別情報(ディスクID)、ハッシュ値(DKBh)及びエラーディテクションコード(EDC)、並びにタイトル単位暗号キー(dTK)等である、コンテンツを再生するのに用いられる他の制御情報の少なくとも一部である。秘匿情報は、例えばユーザによる悪用が相対的に容易であるパソコン等である、仲介装置に対して秘匿される。バスキー通信経路を介して配信される秘匿情報は、サーバ装置側でバスキーにより暗号化される。暗号化された秘匿情報は、バスキー通信経路を介して送信され、ドライブ側通信手段で受信されると、これと同時に、ドライブ装置側でバスキーにより復号化される。復号化さ

れた秘匿情報が、例えばdTKであれば、コンテンツ記録可能エリアに書き込まれ、例えばxDKであれば、復号キーxにより復号化された後に、制御情報記録可能エリアに書き込まれる。従って、例えば第三者がクライアント装置を構成するパソコン等を悪用することで、正規のユーザに成り済まして、サーバ装置から配信される、取得用情報を含んでなる秘匿情報を取得しようとも、バスキー通信経路を介して送信される取得用情報を読み取ることは困難或いは実践上不可能である。このように、サーバ装置及びドライブ装置間のバスキー通信経路により、通信データの秘密を保持することができる。よって、結果として、不正な記録行為を防止することができる。

[0025] 本発明の情報記録媒体の他の態様では、前記ドライブ側通信手段は、前記確立されたバスキー通信経路を介して、前記読み取られた媒体識別情報を前記サーバ装置側へ送信する。

[0026] この態様によれば、バスキー通信経路が確立された後に、ドライブ装置で読み取られた媒体識別情報は、ネットワークの代わりにバスキー通信経路を介してサーバ装置側に送信される。このように、バスキー通信経路により、媒体識別情報の秘密を保持するので、コンテンツの取得権利におけるセキュリティ性を向上させることができる。

[0027] 本発明の情報記録媒体の一態様では、前記媒体識別情報は、前記制御情報を取得するのに用いられる取得用情報を前記サーバ装置側から配信させるための配信指定情報としても機能し、前記ドライブ側通信手段は、前記送信された媒体識別情報に応じて配信される前記取得用情報を受信し、前記制御手段は、前記受信された取得用情報により前記制御情報を取得して、前記取得された制御情報を前記制御情報記録可能エリアに書き込むように前記書込手段を制御する。

[0028] この態様によれば、媒体識別情報は、例えばディスクIDである配信指定情報としても機能し、サーバ装置側に送信される。サーバ装置では、送信された媒体識別情報に対応する取得用情報が取得される。ここで「取得用情報」は、例えば復号キーxであり、制御情報を取得するのに用いられる。サーバ装置側から配信された取得用情報は、ドライブ装置で受信される。ドライブ装置では、受信された取得用情報により制御情報が取得され、取得された制御情報が制御情報記録可能エリアに書き込まれる。

。このように、コンテンツの再生に際して、サーバ装置によって配信される取得用情報を取得する必要があるので、コンテンツの取得権利におけるセキュリティー性を向上させることができる。

[0029] この態様では、前記コンテンツの書き込みの完了をベリファイするベリファイ手段を更に備え、前記取得用情報は、前記完了がベリファイされた後に前記サーバ装置側から配信される復号化用情報であり、前記制御情報の少なくとも一部が暗号化される暗号化情報を前記受信された復号化用情報により復号化することで前記制御情報を取得し、前記制御手段は、該取得された制御情報を前記制御情報記録可能エリアに書き込むように前記書込手段を制御する。

[0030] この態様によれば、特に、コンテンツ記録可能エリアへのコンテンツの書き込みの完了がベリファイされる。制御情報を取得するための取得用情報は、例えば復号キー x である復号化情報であり、暗号化情報を復号化するのに用いられる。ここで「暗号化情報」は、例えば xDK であり、制御情報の少なくとも一部(例えば DK)が暗号化されたものであって、復号化用情報により復号化される。この場合に、配信されたコンテンツの書き込みの完了がベリファイ或いは確認された後に、サーバ装置側から、媒体識別情報に対応する復号化用情報がドライブ装置に配信される。ドライブ装置では、配信された復号化用情報により、固有情報記録済みエリアに記録されている暗号化情報が復号化され、復号化された暗号化情報が制御情報として制御情報記録可能エリアに記録される。このように、制御情報の少なくとも一部が暗号化されており、コンテンツの再生に用いられる制御情報の取得が困難とされるので、悪意あるユーザの犯罪意欲を低下させ、結果として、コンテンツの取得権利におけるセキュリティー性を向上させることができる。

[0031] 本発明に係るサーバ装置は上記課題を解決するために、上述した本発明に係る情報記録媒体(但し、その各種態様を含む)に対する前記コンテンツの配信及び課金を管理する前記サーバ装置であって、前記媒体認証情報を、前記コンテンツに対する課金の状態を示す課金情報及び前記媒体識別情報に対応付けて、格納する格納手段と、前記固有情報記録済みエリアから読み取られる前記固有情報に含まれる前記媒体識別情報を、前記ドライブ装置から受信するサーバ側通信手段と、該受信さ

れた媒体識別情報に対応する媒体認証情報を、前記格納手段から抽出する抽出手段と、該抽出された媒体認証情報に基づくバスキーによって、前記ドライブ装置及び当該サーバ装置間に、バスキー通信経路を確立する通信経路確立手段と、前記格納手段に格納されていると共に前記受信された媒体識別情報に対応する課金情報に従って、前記課金に係る課金処理を実行する課金処理手段とを備え、前記サーバ側通信手段は、前記確立されたバスキー通信経路を介して、前記制御情報の一部若しくは該一部を取得するための取得用情報又は前記コンテンツ記録可能エリアから前記コンテンツを再生するのに用いられる他の制御情報の少なくとも一部であり、前記クライアント装置側に設けられ、前記ドライブ装置をコンピュータ制御すると共に前記ドライブ装置及び前記サーバ装置間を仲介する仲介装置に対して秘匿される秘匿情報を、配信する。

- [0032] 本発明のサーバ装置によれば、特に、課金情報、媒体識別情報、及び媒体認証情報を格納する、例えばデータベースである格納手段、サーバ装置及びドライブ装置間にバスキー通信経路を確立する通信経路確立手段、媒体識別情報に対応する媒体認証情報を抽出する抽出手段、及びバスキー通信経路を介して秘匿情報を配信するサーバ側通信手段を備える。ここで「課金情報」は、例えば当該サーバ装置から配信される或いは予めコンテンツ記録可能エリアに記録されているコンテンツに対する課金の状態、例えばコンテンツ専用の情報記録媒体を取得した際にプリペイドとして支払われた金額(以下適宜「プリペイド額」という)や、同一情報記録媒体に対して以前にコンテンツ配信が行われた場合における、その分の金額をプリペイド額から差し引いた残金(即ち、余力)や、プリペイド額が完全に使われている(即ち、残金がゼロである)旨を示す。或いは、例えば、今回支払うべき残りの金額等の課金される金額、この金額が引き落とされる対象として、銀行等の口座番号やクレジットカードの会員番号等を示す。「課金処理」では、例えば、プリペイド額から、配信されるコンテンツの代金が引かれる。或いは、単純に残金がないものとされる。或いは、例えば引き落とし対象が銀行の口座番号である場合に、当該サーバ装置が、この銀行が管理するサーバ装置にアクセスして、口座番号及び金額を指定する。この指定により、口座番号が示す銀行口座から、課金される金額が引き落とされる。

[0033] 「バスキー通信経路」は、媒体認証情報に基づいて、サーバ装置及びドライブ装置間で情報記録媒体についての認証が成功した後に、サーバ装置及びドライブ装置で同一のバスキーが共有されることにより、確立される。ここで「情報記録媒体についての認証」とは、サーバ装置が配信するコンテンツの取得権利を有する、正当な情報記録媒体であることを、確認することを意味する。「媒体認証情報」は、課金情報及び媒体識別情報に対応付けされる、例えば媒体単位認証キー(DAK)であり、格納手段から抽出される。「認証」の方法として、例えばチャレンジ／レスポンス認証が採用される。具体的には、抽出された媒体認証情報が、ドライブ装置で読み取られた媒体認証情報と一致することが確認される。「バスキー」は、例えばBKであり、サーバ装置及びドライブ装置間で通信されるデータを、暗号化或いは復号化するのに用いられる。

[0034] この場合に、ドライブ装置で読み取られた媒体識別情報がサーバ装置側に送信される。サーバ装置側では、送信された媒体識別情報に対応する秘匿情報が、バスキー通信経路を介してドライブ装置に配信される。ここで「秘匿情報」は、制御情報の一部(DK)、若しくは例えば復号キーxである取得用情報、又は例えば暗号化情報(x DK)、媒体識別情報(ディスクID)、ハッシュ値(DKBh)及びエラーディテクションコード(EDC)、並びにタイトル単位暗号キー(dTK)等である、コンテンツを再生するのに用いられる他の制御情報の少なくとも一部である。秘匿情報は、仲介装置に対して秘匿される。バスキー通信経路を介して配信される秘匿情報は、サーバ側通信手段でバスキーにより暗号化される。暗号化された秘匿情報は、バスキー通信経路上を送信され、ドライブ装置側で受信されると、これと同時に、バスキーにより復号化される。復号化された秘匿情報が、例えばdTKであれば、コンテンツ記録可能エリアに書き込まれ、例えばxDKであれば、復号キーxにより復号化された後に、制御情報記録可能エリアに書き込まれる。従って、例えば第三者がクライアント装置を構成するパソコン等を悪用することで正規のユーザに成り済まして、サーバ装置から配信される、取得用情報を含んでなる秘匿情報を取得しようとも、バスキー通信経路を介して送信される取得用情報を読み取ることは困難或いは実践上不可能であるので、コンテンツを再生可能な状態にある情報記録媒体は得られない。このように、サーバ装置及び

ドライブ装置間のバスキー通信経路により、通信データの秘密を保持することができる。よって、結果として、不正な記録行為を防止することができる。

[0035] また、例えば復号キーxである取得用情報が、バスキー通信経路を介してドライブ装置に送信されると同時或いはその後に、送信された取得用情報に対応する課金情報に従って、課金処理が実行される。このように、コンテンツの記録を完了した後に、取得用情報をバスキー通信経路を介して送信する段階で課金処理が実行されるので、適切に課金を行うことができる。

[0036] 本発明のサーバ装置の他の態様では、前記格納手段は、前記媒体識別情報に加えて又は代えて、前記制御情報の少なくとも一部が暗号化されてなる暗号化情報(xDK)を更に格納し、前記抽出手段は、前記媒体認証情報に加えて又は代えて、前記受信された媒体識別情報に対応する暗号化情報を、前記格納手段から抽出し、前記サーバ側通信手段は、前記秘匿情報の少なくとも一部として、前記抽出された暗号化情報を送信してもよい。

[0037] この態様によれば、格納手段には、例えばディスクIDである媒体識別情報に代えて又は加えて、例えば復号キーxにより暗号化されたディスクキーxDKである暗号化情報が格納されている。この場合に、当該サーバ装置では、媒体識別情報が受信されると、これに対応する暗号化情報が格納手段から抽出される。抽出された暗号化情報は、秘匿情報の少なくとも一部として、バスキー通信経路を介してクライアント装置側或いはドライブ装置に送信される。クライアント装置側或いはドライブ装置では、コンテンツの記録が完了した後に、送信された暗号化情報が取得用情報(復号キーx)により復号化され、復号化された暗号化情報が制御情報として記録されることで、コンテンツの再生が可能とされる。このように、コンテンツの再生に際して、当該サーバ装置によって暗号化情報が送信される必要があるので、コンテンツの取得権利におけるセキュリティ性、及びコンテンツ配布におけるセキュリティ性を向上させることができる。

[0038] 本発明のサーバ装置の一態様では、前記格納手段は、前記媒体識別情報に加えて又は代えて、前記コンテンツを構成するタイトルに個別に割り当てられるタイトル単位暗号キー(dTK)、及び該タイトル単位暗号キーの元となるタイトル単位キー(TK)

を更に格納し、前記抽出手段は、前記媒体認証情報に加えて又は代えて、前記受信された配信指定情報に対応する前記タイトル単位暗号キー及びタイトル単位キーを、前記格納手段から抽出する。

[0039] この態様によれば、格納手段には、例えばディスクIDである媒体識別情報に代えて又は加えて、例えばタイトル単位暗号キー、又はタイトル単位暗号キーの元となるタイトル単位キーが格納されている。ここで「タイトル単位暗号キー」は、例えばdTKであり、コンテンツを構成するタイトルに個別に割り当てられ、典型的には、暗号化されたコンテンツと共に、コンテンツ記録可能エリアに記録される。「タイトル単位キー」は、例えばTKであり、暗号化されるとタイトル単位暗号キーとなる。この場合に、サーバ装置側では、媒体識別情報が受信されると、これに対応するタイトル単位暗号キー及びタイトル単位キーが格納手段から抽出され、クライアント装置側或いはドライブ装置に送信される。この送信されたタイトル単位キーに従って、暗号化されたコンテンツが、クライアント装置側或いはドライブ装置にて記録される。この暗号化されたコンテンツの記録が完了した後は、クライアント装置側或いはドライブ装置で、タイトル単位キーを用いて復号化することで、コンテンツの再生が可能とされる。このように、コンテンツの再生に際して、当該サーバ装置によってタイトル単位暗号キーが送信される必要があるので、コンテンツの取得権利におけるセキュリティ性、及びコンテンツ配布におけるセキュリティ性を向上させることができる。

[0040] この態様では、前記サーバ側通信手段は、前記秘匿情報の少なくとも一部として、前記抽出されたタイトル単位暗号キーを送信する。

[0041] この態様によれば、格納手段から抽出されたタイトル単位暗号キーdTKが、秘匿情報の少なくとも一部として、バスキー通信経路を介してドライブ装置に送信される。これにより、タイトル単位暗号キーdTKの漏洩及びすり替えを防止するので、コンテンツの取得権利におけるセキュリティ性、及びコンテンツ配布におけるセキュリティ性を向上させることができる。

[0042] 本発明のサーバ装置の一態様では、前記抽出されたタイトル単位キー(TK)により前記コンテンツを暗号化して、前記クライアント装置側へ送信する暗号化手段を更に備える。

- [0043] この態様によれば、コンテンツがタイトル単位キーTKにより暗号化され、暗号化されたコンテンツがクライアント装置側或いはドライブ装置に送信される。これにより、第三者によるコンテンツの不正な読み取りを防止するので、コンテンツの取得権利におけるセキュリティー性を向上させることができる。尚、このセキュリティー性をより向上させるために、タイトル単位キーTKにより暗号化されたコンテンツの少なくとも一部を、バスキー通信経路を介してドライブ装置に送信してもよい。
- [0044] 本発明に係るコンテンツサーバ装置は上記課題を解決するために、上述した本発明に係るサーバ装置(但し、その各種態様を含む)から、前記抽出されたタイトル単位キー(TK)を、前記ネットワークを介して受信するコンテンツ配信側通信手段と、複数のコンテンツを予め格納するコンテンツ格納手段と、前記コンテンツを前記コンテンツ格納手段の中から抽出するコンテンツ抽出手段と、該抽出されたコンテンツを、前記受信されたタイトル単位キーで暗号化するタイトル単位キー暗号化手段とを備え、前記コンテンツ配信側通信手段は、前記暗号化されたコンテンツを、前記ネットワークを介して、前記クライアント装置側に送信する。
- [0045] 本発明のコンテンツサーバ装置によれば、特に、コンテンツを暗号化するタイトル単位キー暗号化手段を備える。この場合に、タイトル単位キーTKがサーバ装置から受信されると、この受信されたタイトル単位キーTKにより、コンテンツ格納手段から抽出されたコンテンツが暗号化される。暗号化されたコンテンツは、ネットワークを介してクライアント装置側に送信される。このように、暗号化されたコンテンツの送信により、第三者によるコンテンツの不正な読み取りを防止するので、コンテンツの取得権利におけるセキュリティー性を向上させることができる。
- [0046] 本発明に係る仲介装置は上記課題を解決するために、上述した本発明に係るドライブ装置(但し、その各種態様を含む)と共に前記クライアント装置側に設けられ、前記ドライブ装置をコンピュータ制御すると共に前記ドライブ装置及び前記サーバ装置間を仲介する仲介装置であって、前記固有情報記録済みエリアから前記ドライブ装置により読み取られる前記固有情報に含まれる前記媒体識別情報を、前記確立されたバスキー通信経路を介して、前記ドライブ装置から受け取ると共に前記サーバ装置側へ送信する第1通信手段と、前記秘匿情報を、前記確立されたバスキー通信経

路を介して、前記サーバ装置から受け取ると共に前記ドライブ装置側へ送信する第2通信手段とを備える。

[0047] 本発明の仲介装置によれば、第1通信手段によって、ドライブ装置で読み取られた、例えばディスクIDである媒体識別情報が、バスキー通信経路を介してサーバ装置側へ送信される。また、第2通信手段によって、サーバ装置側から配信された、例えば復号キーxである秘匿情報が、バスキー通信経路を介してドライブ装置側へ送信される。このような仲介装置を介しての情報の伝達は、好ましくは、仲介装置では情報の中味にアクセスできないバスキー通信回路が、仲介装置内に確立された上で行われる。これにより、ドライブ装置及びサーバ装置の間で当該仲介装置を介して送受される、媒体識別情報及び秘匿情報が、例えばホストコンピュータやパソコンにおけるドライブ装置を除いた部分である、当該仲介装置によって読み取られないので、コンテンツの取得権利におけるセキュリティ性、及びコンテンツ配布におけるセキュリティ性を更に向上させることができる。

[0048] 本発明の作用及び他の利得は次に説明する実施するための最良の形態から明らかにされる。

[0049] 以上詳細に説明したように、本発明の情報記録媒体によれば、固有情報として、当該情報記録媒体についての認証を行うための媒体認証情報が記録されているので、本発明のドライブ装置によれば、サーバ装置との間にバスキー通信経路が確立されるので、本発明のサーバ装置によれば、媒体認証情報が媒体識別情報に対応付けて格納されると共に、ドライブ装置との間にバスキー通信経路が確立されるので、本発明のコンテンツサーバ装置によれば、コンテンツが暗号化されて、クライアント装置側に送信されるので、本発明の仲介装置によれば、バスキー通信経路を介して、ドライブ装置からの媒体識別情報がサーバ装置側に送信されると共に、サーバ装置側からの秘匿情報がドライブ装置に送信されるので、サーバ装置及びドライブ装置間で通信される情報の秘密を保持して、不正な記録行為を防止することが可能となる。

図面の簡単な説明

[0050] [図1]実施形態に係るコンテンツ配信システムの概要を示すブロック図である。

[図2]実施形態に係る情報記録媒体の各種データ記録エリアを示すデータ構成図で

ある。

[図3]実施形態に係るコンテンツの配信及び課金処理を示すフローチャートである。

[図4]実施形態に係る情報記録媒体についての認証処理を示すフローチャートである。

[図5]実施形態における、ホストコンピュータを仲介しての各種データの流れを示す概念図である。

符号の説明

- [0051] 1…光ディスク
2…パソコン
3…コンテンツ配信サーバ
10…再生部
20…インターネット
21…ホストコンピュータ
22…光学ドライブ
100…コンテンツ配信システム

発明を実施するための最良の形態

[0052] 以下、本発明の実施形態について図を参照しつつ説明する。

[0053] 先ず、本実施形態に係るコンテンツ配信システムの構成について図1及び図2を参照して説明する。ここに図1は、本実施形態に係るコンテンツ配信システムのブロック図であり、図2は、本実施形態に係る情報記録媒体のデータ構成図である。

[0054] 図1において、本実施形態に係るコンテンツ配信システム100は、主に、光ディスク1と、パソコン2と、コンテンツ配信サーバ3とを備えている。パソコン2及びコンテンツ配信サーバ3は、インターネット20に収容されており、インターネット20を介して、データの送受信が可能である。

[0055] 光ディスク1は、本実施形態に係る「情報記録媒体」の一例として、例えば追記型のDVD、BD等であって、光学ドライブ22にセットされ、映画、ドラマ等のコンテンツの記録及び再生が可能である。

[0056] 図2に示すように、光ディスク1は、リードインエリアと、プログラムエリアと、リードアウト

トエリアとを有する。リードインエリアは、固有情報記録済みエリア32と、制御情報記録可能エリア33とを含んでいる。プログラムエリアは、コンテンツ記録可能エリア34を含んでいる。光ディスク1は、これらのエリアの他に、セクタ情報記録可能エリア31を有する。

- [0057] セクタ情報記録可能エリア31は、光学ドライブ22によって、ESTセッション情報や、暗号化されたタイトルキーdTK等を記録可能である。ESTセッション情報は、例えばコンテンツ配信サーバ3にログインするためのログインIDであって、パソコン2及びコンテンツ配信サーバ3の間の通信を、所定時間保持するために補完される情報である。このESTセッション情報は、後述のディスクIDがコンテンツ配信サーバ3で受信されるのに応答して生成される。
- [0058] 固有情報記録済みエリア32は、光ディスク1に固有である固有情報を予め記録している。固有情報は、暗号化されたディスクキーxDK、ディスクID、ハッシュ値DKh、及びディスク認証キーDAKを含んでいる。
- [0059] 暗号化されたディスクキーxDKは、光ディスク1に個別に割り当てられたディスクキーDKが暗号化されてなる本実施形態に係る「暗号化情報」の一例である。
- [0060] ディスクIDは、本実施形態に係る「配信指定情報」及び「媒体識別情報」の一例として、光ディスク1を識別する。ディスクIDは、例えば光ディスク1が光学ドライブ22にセットされると同時に、コンテンツ配信サーバ3に送信される。ディスクIDは、コンテンツ配信サーバ3から送信される、暗号化されたディスクキーxDKを復号化するための復号キーxと紐付いている。ディスクIDは、例えばリージョナルコントロール用の情報を含んでいる。このリージョナルコントロールにより、後述のコンテンツ識別番号が識別するコンテンツに、例えば日本語の字幕が付加される。更に、ディスクIDは、例えばR-15の如く年齢制限を示すパレンタルコントロール用の情報を含んでもよい。
- [0061] ハッシュ値DKhは、ディスクキーDKにおけるハッシュ値である。ハッシュ値DKhは、暗号化されたディスクキーxDKが復号キーxにより正当に復号化されたか否か、すなわち正規のディスクキーDKとして復号化されたか否かを判定するのに用いられる。尚、ハッシュ値DKhの代わりに、ディスクキーDKについてのエラーディテクションコードEDCが、この判定のために用いられても構わない。

- [0062] ディスク認証キーDAKは、本実施形態に係る「媒体認証情報」の一例として、光学ドライブ22及びコンテンツ配信サーバ3間で光ディスク1についての認証を行うのに用いられる。ディスク認証キーDAKは、光学ドライブ22で読み取られ、固有情報として取得される他、コンテンツ配信サーバ3で、後述の媒体情報データベース5から読み取られることで独自に取得される。コンテンツ配信サーバ3側では、ディスク認証キーDAKは、ディスクIDに対応付けされており、媒体情報データベース5に格納されている。光ディスク1についての認証は、光学ドライブ22で取得されたディスク認証キーDAKが、コンテンツ配信サーバ3で取得されたディスク認証キーDAKと一致することを確認することである。この認証が行われた後に、後述のセキュアバスが確立される。
- [0063] 制御情報記録可能エリア33は、光学ドライブ22によって制御情報を、追記的に記録可能である。制御情報は、コンテンツ記録可能エリア34に記録されたコンテンツを再生するのに用いられる。制御情報は、ディスクキーDK、並びに、固有情報と同様に、ディスクID、ハッシュ値DKh及びディスク認証キーDAKを含んでいる。但し、コンテンツ記録可能エリア34にコンテンツが記録される以前には、このような制御情報は、制御情報記録可能エリア33に記録されていない。
- [0064] ディスクキーDKは、暗号化されたディスクキーxDKを、復号キーxにより復号化したものである。ディスクキーDKが、制御情報記録可能エリア33に記録されることで、ここに記録されたディスクキーDKを参照してのコンテンツの再生が可能となる。尚、本実施形態では、このディスクキーDKの記録に伴って、ディスクID、ハッシュ値DKh及びディスク認証キーDAKが制御情報記録可能エリア33に記録される。
- [0065] コンテンツ記録可能エリア34は、コンテンツ配信サーバ3から配信される、暗号化されたコンテンツ及び暗号化されたタイトルキーdTKを記録する。暗号化されたコンテンツは、ホストコンピュータ21から送られる。暗号化されたタイトルキーdTKは、光ディスク1についての認証が行われた後に、コンテンツ配信サーバ3から送信される。コンテンツは、コンテンツ配信サーバ3によって、タイトルキーTKを用いたCSS方式により暗号化されている。本実施形態では、コンテンツを再生する際には、制御情報の一部としてのディスクキーDK、タイトルキーTK等が取得されることで、コンテンツが再

生可能な状態となる。

[0066] パソコン2は、本実施形態に係る「クライアント装置」の一例として、ホストコンピュータ21と、光学ドライブ22とを備えている。

[0067] ホストコンピュータ21は、本実施形態に係る「仲介装置」の一例として、主に、CPU8と、HDD9と、再生部10と、インターフェイス13とを備えている。インターフェイス13は、モデム等を備えてなる。

[0068] ホストコンピュータ21は、本実施形態に係る「第1通信手段」の一例として、光学ドライブ22から送られるディスクIDを、コンテンツ配信サーバ3に送信する。ホストコンピュータ21は、この送信に際して、光ディスク1についての認証が行われる前では、インターフェイス13を介して送信を行い、認証が行われた後では、セキュアバスを介して送信を行う。本実施形態では、ホストコンピュータ21は、コンテンツ配信サーバ3へのディスクIDの送信を二度行う。一度目に送信されるディスクIDは、光ディスク1についての認証に用いられる。二度目に送信されるディスクIDは、認証が行われた後に、セキュアバスを介して送信される、信頼性の高い情報であり、ディスクIDの登録を再度確認するのに用いられる。

[0069] ホストコンピュータ21は、本実施形態に係る「第2通信手段」の一例として、光ディスク1についての認証が行われた後に、コンテンツ配信サーバ3から配信される、本実施形態に係る「秘匿情報」の一例である、復号キーx、及び暗号化されたタイトルキーdTKを受信すると共に、セキュアバスを介して、そのまま光学ドライブ22に送る。

[0070] CPU8は、パソコン2の各部と接続されている。CPU8は、再生部10を制御して、HDD9に格納されているコンテンツを再生したり、光学ドライブ22を制御して、セットされる光ディスク1に対して、コンテンツの読み取り及び書き込みを行う。

[0071] CPU8は更に、コンテンツ配信サーバ3から配信される、暗号化されたコンテンツ、及び後述のタイトルキーマップTKmapを受信すると共に、これらをインターフェイス13を介して、光学ドライブ22に送信する。

[0072] 尚、コンテンツの再生に際して、ハッシュ値を用いて、正当な記録が行われたか否かが、即ち正規に購入されたコンテンツであるか否かが、検出されてもよい。CPU8は、制御情報記録可能エリア33に記録された制御情報からハッシュ値を算出する。

この算出されたハッシュ値と、固有情報記録済みエリア32から読み取られた規定のハッシュ値とが同一であるか否かを判定する。CPU8は、これらの算出されたハッシュ値と規定のハッシュ値とが同一である場合に、コンテンツ記録可能エリア34に記録されたコンテンツの読み取りを許可する。これにより、制御情報が読み取られて、コンテンツが再生される。

[0073] 再生部10は、スピーカ12及びモニタ13と接続されており、これらを使用して、HD D9内のコンテンツを再生したり、光学ドライブ22にセットされた光ディスク1に記録されているコンテンツを再生する。再生部10は、制御情報が記録されている光ディスク1内のコンテンツの再生に際して、タイトルキーTKにより、暗号化されたコンテンツを復号化する。この復号化により、コンテンツが再生される。

[0074] 光学ドライブ22は、本実施形態に係る「ドライブ装置」の一例として、コントローラ14と、読み取り／書き込み部15とを備えてなる。コントローラ14は、読み取り／書き込み部15、並びにホストコンピュータ21のCPU8及びインターフェイス13と接続されている。コントローラ14は、本実施形態に係る「制御手段」の一例として、セットされる光ディスク1に対して、本実施形態に係る「読取書込手段」の一例である、読み取り／書き込み部15を作動させる。コントローラ14は、CPU8によって制御される一方、インターフェイス13を介して、コンテンツ配信サーバ3との間で、データの送受信を行う。

[0075] コントローラ14は、本実施形態に係る「通信経路確立手段」の一例として、乱数発生装置14aを備えてなり、コンテンツ配信サーバ3との間に、セキュアバスを確立する。

[0076] セキュアバスは、本実施形態に係る「バスキー通信経路」の一例として、ホストコンピュータ21の内部を素通しする形で確立される。セキュアバスを介する情報は、ホストコンピュータ21によって、意味の或る情報としては読み取り不可能である。コントローラ14は、セキュアバスの確立に際して、先ず、コンテンツ配信サーバ3と相互に、光ディスク1についての認証を行う。乱数発生装置14aは、この認証に必要とされる乱数を発生させる。

[0077] 光ディスク1についての認証では、固有情報に含まれるディスク認証キーDAKが用いられる。コントローラ14は、光ディスク1の固有情報記録済みエリア32から読み取ら

れたディスク認証キーDAKにより、乱数発生装置14aによって発生された乱数を変換し、この変換された乱数の値、即ち変換値を出力する。コンピュータ14は、出力された変換値を、コンテンツ配信サーバ3に送信すると、これと同時に或いは相前後して、コンテンツ配信サーバ3によって同様にして出力された変換値を、コンテンツ配信サーバ3から受信する。コンピュータ14は、コンテンツ配信サーバ3からの変換値に基づいて、固有情報記録済みエリア32内のディスク認証キーDAKが、コンテンツ配信サーバ3で変換値の出力に用いられたディスク認証キーDAKと一致するか確認する。ディスク認証キーDAKの一致が確認され、コンテンツ配信サーバ3に対する、光ディスク1についての認証が成功した後に、コンピュータ14は、コンテンツ配信サーバ3と共に、バスキーBKを生成する。コンピュータ14は、生成されたバスキーBKにより、コンテンツ配信サーバ3に送信すべきディスクIDを、暗号化して送信すると共に、コンテンツ配信サーバ3から配信される、復号キーx、及び暗号化されたタイトルキーdTKを受信すると共に、復号化する。

[0078] こうして、バスキーBKの生成により、光学ドライブ22及びコンテンツ配信サーバ3の間に、セキュアバスが確立されたことになる。従って、例えば悪意のあるユーザ等が、ホストコンピュータ21のソフトウェアを改竄することやホストコンピュータ21内のデータにアクセスすることで、セキュアバス上の情報を読み取ること、更に不正な情報の取得を行うことが著しく困難と成る。

[0079] 読み取り／書き込み部15は、本実施形態に係る「読取書込手段」及び「ベリファイ手段」の一例として、光ディスク1の固有情報記録済みエリア32に記録されている固有情報を読み取ったり、コンテンツ記録可能エリア34に対して、HDD9内に一時的に格納されたコンテンツを書き込む。この書き込みにより、コンテンツの記録が行われる。読み取り／書き込み部15は、コンテンツの記録が完了した後に、記録されたコンテンツに対して、ベリファイを行う。このベリファイにより、コンテンツがエラー無く書き込まれたことが確認される。

[0080] 本実施形態では、読み取り／書き込み部15は、このベリファイの後に、制御情報を取得し、この取得された制御情報を制御情報記録可能エリア33に書き込む。ディスクキーDK等を含む制御情報は、コンテンツの再生に必要とされ、読み取り情報等を

示す。このような制御情報は、復号キーxの配信を受けた光学ドライブ22において、暗号化されたディスクキーxDKを復号キーxにより復号化すること等で取得される。

[0081] 尚、好ましくは、この制御情報の書き込みより前に、読み取り／書き込み部15は、制御情報記録可能エリア33をトレースしてもよい。読み取り／書き込み部15は、このトレースの結果により、制御情報記録可能エリア33が記録可能であるか否かを判定し、制御情報記録可能エリア33が記録可能である場合に、制御情報の書き込みを行う。逆に、制御情報記録可能エリア33が既に記録済みである等の場合には、コンテンツの配信を受けて記録を行うための光ディスク1ではないとして、記録処理を中止する。

[0082] コントローラ14は、本実施形態に係る「ドライブ側通信手段」の一例として、読み取り／書き込み部15によって読み取られた、光ディスク1のディスクIDを、コンテンツ配信サーバ3に送信する。この送信に際して、コントローラ14は、光ディスク1についての認証が行われる前では、インターフェイス13を介して送信を行い、認証が行われた後では、セキュアバスを介して送信を行う。コントローラ14は、読み取り／書き込み部15を制御して、ホストコンピュータ2から送られる、暗号化されたコンテンツをコンテンツ記録可能エリア34に記録し、この記録の完了をベリファイする。コントローラ14は、このベリファイの後に、コンテンツ配信サーバ3から送信される復号キーxを、セキュアバスを介して受信する。コントローラ14は、この受信された復号キーxにより、固有情報記録済みエリア32に記録されている、暗号化されたディスクキーxDKを復号化する。この復号化により、制御情報として、ディスクキーDKを取得する。

[0083] コントローラ14は、読み取り／書き込み部15を制御して、制御情報記録可能エリア33のトレースを行うことで、制御情報記録可能エリア33が記録可能であることを確認した後に、復号化によって取得されたディスクキーDKを、この制御情報記録可能エリア33に記録する。この制御情報の記録により、コンテンツ記録可能エリア34に記録されたコンテンツの再生が可能となる。

[0084] コンテンツ配信サーバ3は、本実施形態に係る「サーバ装置」の一例として、CPU4と、媒体情報データベース5と、コンテンツデータベース6と、インターフェイス7とを備えている。インターフェイス7は、モデム等を備えてなる。

- [0085] 媒体情報データベース5は、ハードディスク等の大規模記憶装置を含んでなり、本実施形態に係る「格納手段」の一例として、複数のディスクID、このディスクIDと夫々紐付いている、ディスク認証キーDAK、復号キーx、コンテンツ識別情報、及び課金情報を格納している。複数のディスクIDは、コンテンツの配信、記録及び再生が許可されている、複数の光ディスクに対して付与されている。典型的には、プリペイドで販売される光ディスク1に対してディスクIDが個別に割り振られている。
- [0086] 媒体情報データベース5に格納されているディスク認証キーDAKは、光ディスク1内に記録されているディスク認証キーDAKと同様に、光学ドライブ22及びコンテンツ配信サーバ3間で光ディスク1についての認証を行うのに用いられる。
- [0087] 媒体情報データベース5に格納されている復号キーxは、本実施形態に係る「復号化用情報」及び「秘匿情報」の一例として、パソコン2側に配信されることで、暗号化されたディスクキーxDKの復号化に用いられる。復号キーxにより復号化されてなるディスクキーDKが、制御情報として、制御情報記録可能エリア33に記録される。
- [0088] コンテンツ識別番号(例えば、タイトル番号)は、送信されたディスクIDに対応する、光ディスク1がセットされるパソコン2側へ配信可能なコンテンツを識別する。コンテンツの各々は、コンテンツ識別番号と紐付いている。
- [0089] 課金情報は、送信されたディスクIDに対応するコンテンツに対する課金の状態、例えばプリペイドされた金額を示す。或いは、ディスクIDに紐付けられたユーザの銀行の口座番号や、コンテンツ取得の代金として、この口座から引き落とされる金額等を示す。この課金情報に従って、CPU4によって、例えばディスクIDに対するプリペイド金額をゼロにするなどの、課金処理が実行される。
- [0090] コンテンツデータベース6は、複数のコンテンツ、並びに、本実施形態に係る「タイトル単位キー」の一例である、タイトルキーTK、及び本実施形態に係る「タイトル単位暗号キー」の一例である、暗号化されたタイトルキーdTK等を、格納している。タイトルキーTK及び暗号化されたタイトルキーdTKは、コンテンツを構成するタイトルに対して作成されている。
- [0091] CPU4は、本実施形態に係る「サーバ側通信手段」、「抽出手段」及び「課金処理手段」として、コンテンツ配信サーバ3の各部と接続されている。CPU4は、インターフ

エイス7を介して、パソコン2の光学ドライブ22から送信されるディスクIDを受信する。この受信されるディスクIDは、光ディスク1についての認証が行われる前では、インターフェイス13を介して送信され、認証が行われた後では、セキュアバスを介して送信される。ディスクIDの受信に応答して、CPU4は、媒体情報データベース5にアクセスして、受信されたディスクIDが、媒体情報データベース5に登録されているか否かを判定する。ディスク販売店等に配布される光ディスク1は、配布前に、そのディスクIDが媒体情報データベース5に登録されている。又は、ディスク販売店等に配布される光ディスク1は、販売店等にてプリペイド手続きがなされる段階で、そのディスクIDがネットワーク20を介して媒体情報データベース5に登録されている。このため、CPU4が判定をする時点では、正規にプリペイドがなされた光ディスク1であれば、媒体情報データベース5に登録されている訳である。本実施形態では、CPU4は、媒体情報データベース5へのディスクIDの登録の確認を二度行う。

[0092] CPU4は、本実施形態に係る「通信経路確立手段」として、乱数発生装置4aを備えてなり、光学ドライブ22との間に、セキュアバスを確立する。CPU4は、セキュアバスの確立に際して、先ず、光学ドライブ22と相互に、光ディスク1についての認証を行う。乱数発生装置4aは、この認証に必要とされる乱数を発生させる。

[0093] 光学ドライブ22のコンピュータ14の場合と同様に、光ディスク1についての認証では、媒体情報データベース5内のディスク認証キーDAKが用いられる。CPU4は、媒体情報データベース5から抽出された、ディスクIDに対応するディスク認証キーDAKにより、乱数発生装置4aによって発生された乱数を変換し、変換値を出力する。CPU4は、出力された変換値を、光学ドライブ22に送信すると、これと同時に或いは相前後して、光学ドライブ22によって同様に出力された変換値を、光学ドライブ22から受信する。CPU4は、光学ドライブ22からの変換値に基づいて、媒体情報データベース5内のディスク認証キーDAKが、光学ドライブ22で変換値の出力に用いられたディスク認証キーDAKと一致するか確認する。ディスク認証キーDAKの一致が確認された後に、CPU4は、光学ドライブ22と共に、バスキーBKを生成する。CPU4は、生成されたバスキーBKにより、光学ドライブ22に送信すべき復号キーx、及び暗号化されたタイトルキーdTKを、暗号化して送信すると共に、光学ドライブ22から

配信される、ディスクIDを受信すると共に、復号化する。こうして、バスキーBKの生成により、光学ドライブ22及びコンテンツ配信サーバ3の間に、双方向のセキュアバスが確立されたことになる。

[0094] 本実施形態では、光学ドライブ22及びコンテンツ配信サーバ3は、上述の光ディスク1についての認証を二度行う。一度目の認証は、一度目のディスクIDの登録確認が行われた後に設定され、二度目の認証は、暗号化されたタイトルキーdTKが、光学ドライブ22に送信される前に設定される。

[0095] CPU4は、本実施形態に係る「暗号化手段」として、コンテンツを暗号化して、ホストコンピュータ21に送信する。CPU4は、ディスクIDに対応するコンテンツ識別番号を、媒体情報データベース5から読み取り、この読み取られたコンテンツ識別番号に対応するコンテンツを、コンテンツデータベース6から抽出する。CPU4は、タイトルキーTKにより、抽出されたコンテンツを暗号化すると共に、プログラムエリアのセクターのアドレスを示すタイトルキーマップTKmapを生成する。タイトルキーマップTKmapは、コンテンツ記録可能エリア34に対する、暗号化されたコンテンツ、及び暗号化されたタイトルキーdTKの記録に用いられる。CPU4は、この暗号化されたコンテンツ、及びタイトルキーマップTKmapを光学ドライブ22に送る。尚、コンテンツの暗号化は、ホストコンピュータ21で行ってもかまわない。

(コンテンツの配信及び課金処理)

次に、以上のように構成されたコンテンツ配信システム100のコンテンツの配信及び課金処理について、図3から図5を参照して説明する。ここに図3は、本実施形態に係る、コンテンツ配信システム100の、光ディスク1についての認証を伴うコンテンツの配信及び課金処理を示すフローチャートであり、図4は、その認証処理を示すフローチャートであり、図5は、ホストコンピュータ21を仲介しての各種データの流れを示す概念図である。

[0096] 図3において先ず、パソコン2の光学ドライブ22に光ディスク1がセットされると、コントローラ14によって、光ディスク1が検出されると共に、読み取り／書き込み部15によって、固有情報記録済みエリア32に記録されているディスクIDが読み取られる。読み取られたディスクIDは、図5に示すように、コンテンツ配信サーバ3に送信される(ス

テップS51)。

- [0097] コンテンツ配信サーバ3では、CPU4によって、光ディスク1において、媒体情報データベース5への登録が確認される(ステップS52)。この確認では、光学ドライブ22から送信されたディスクIDが、媒体情報データベース5に格納されている複数のディスクIDのいずれかと一致するか否かが判定される(ステップS53)。ここで一致しない場合には(ステップS53:NO)、例えば正規にプリペイドされた光ディスクでない等、コンテンツを購入する権利を持たない光ディスク1がセットされているとして、処理を終了する。
- [0098] ステップS53の判定の結果、ディスクIDが一致する場合に(ステップS53:YES)、コンテンツ配信サーバ3及び光学ドライブ22間で光ディスク1についての認証(ECA)が行われる(ステップS54)。
- [0099] 図4に示すようにこのステップS54における認証ではまず、コンテンツ配信サーバ3及び光学ドライブ22の各々にて、ディスク認証キーDAKが読み取られる(ステップS81)。続いて、読み取られたディスク認証キーを用いて乱数の変換値が出力される(ステップS82)。この出力に応答して、コンテンツ配信サーバ3にて出力された変換値が、光学ドライブ22に送信され、光学ドライブ22にて出力された変換値が、コンテンツ配信サーバ3に送信される(ステップS83)。コンテンツ配信サーバ3及び光学ドライブ22の各々にて、送信された変換値に基づいて、コンテンツ配信サーバ3側で読み取られたディスク認証キーDAKと、光学ドライブ22側で読み取られたディスク認証キーDAKとの一致が確認される(ステップS84)。ここで一致しない場合には(ステップS84:NO)、コンテンツを購入する権利を持たない光ディスク1がセットされているとして、処理を終了する。
- [0100] ステップS84の確認の結果、ディスク認証キーDAKが一致する場合には(ステップS84:YES)、コンテンツ配信サーバ3及び光学ドライブ22によって、共通のバスキーが生成される(ステップS85)。これにより、セキュアバスが確立され、一度目の認証が終了する。
- [0101] 再び図3に戻り、以上のようにステップS54における認証処理が完了すると、一度目の認証の後に、読み取り／書き込み部15によって、ディスクIDが再度読み取られ、

図5に示すように、セキュアバスを介して、コンテンツ配信サーバ3に再送信される(ステップS55)。コンテンツ配信サーバ3では、CPU4によって、光ディスク1の登録が再確認され(ステップS56)、光学ドライブ22からのディスクIDが、媒体情報データベース5内の複数のディスクIDのいずれかと一致するか否かが判定される(ステップS57)。この判定の結果、ディスクIDが一致する場合に(ステップS57:YES)、CPU4によって、ディスクIDに対応するESTsession情報、並びに、配信しようとするコンテンツに対するタイトルキーTK、及びこれが暗号化されたタイトルキーdTKが生成される(ステップS58)。生成されたESTsession情報は、図5に示すように、ホストコンピュータ21及び光学ドライブ22の各々に送信される。パソコン2では、CPU8によって、送信されたESTsession情報がセクタ情報記録可能エリア31に記録されることで、コンテンツ配信サーバ3及びパソコン2の間で、ESTsessionが確立される(ステップS59)。

[0102] 続いて、光ディスク1についての認証が再度行われる。コンテンツ配信サーバ3及び光学ドライブ22の各々でディスク認証キーDAKが読み取られ(ステップS81)、読み取られたディスク認証キーDAKを用いて、乱数の変換値が出力される(ステップS82)。この出力された変換値が、コンテンツ配信サーバ3及び光学ドライブ22の相互に送信され(ステップS83)、送信された変換値に基づいて、コンテンツ配信サーバ3側のディスク認証キーDAKと、光学ドライブ22側のディスク認証キーDAKとの一致が確認される(ステップS84)。この確認の結果、ディスク認証キーDAKが一致する場合には(ステップS84:YES)、コンテンツ配信サーバ3及び光学ドライブ22に共通のバスキーが生成され(ステップS85)、セキュアバスが確立される。こうして、二度目の認証が終了する。

[0103] 二度目の認証の後に、暗号化されたタイトルキーdTKは、図5に示すように、確立されたESTsession上で、セキュアバスを介して、光学ドライブ22に送信される(ステップS61)。また、コンテンツ配信サーバ3にて、CPU4によって、コンテンツデータベース6から、ディスクIDに対応するコンテンツ識別番号で示されるコンテンツが読み取られる。読み取られたコンテンツは、生成されたタイトルキーTKを用いて暗号化される。また、この暗号化に併せて、タイトルキーマップTKmapが生成される。この暗号化

されたコンテンツ、及びタイトルキーマップTKmapは、図5に示すように、ホストコンピュータ21に送信される(ステップS62)。続いて、この暗号化されたコンテンツ、及びタイトルキーマップTKmapは、図5に示すように、光学ドライブ22に送信される(ステップS63)。

[0104] これを受けて、光学ドライブ22にて、読み取り／書き込み部15によって、タイトルキーマップTKmapに従って、送信された暗号化されたコンテンツ、及び暗号化されたタイトルキーdTKが、コンテンツ記録可能エリア22に記録される(ステップS64)。この記録が完了すると共に、記録されたコンテンツがベリファイされ(ステップS65)、コンテンツがエラー無しに正しく記録されたか否かが判定される(ステップS66)。

[0105] ベリファイの結果、記録が正しく完了していないことが判明すれば、即ち、ダウンロード中における送信エラーなどにより記録にエラーが含まれる場合には(ステップS66: YES)、例えば暗号化されたコンテンツ及びタイトルキーdTKの記録が再度行われる(ステップS64)。或いは、この場合には、少なくとも課金処理が行われることなく、同一ユーザが所有する別の光ディスクに対して、暗号化されたコンテンツ等の記録が可能とされる。

[0106] ステップS66の判定の結果、記録にエラーが含まれない場合には(ステップS66: NO)、読み取り／書き込み部15によって、セクタ情報記録可能エリア31、リードインエリア及びリードアウトエリア、即ち制御情報記録可能エリア33より他の、コンテンツ記録済みのコンテンツ記録可能エリアを除いたエリアに対する記録が行われる(ステップS67)。この記録の後に、制御情報記録可能エリア33がトレースされ(ステップS68)、制御情報記録可能エリア33が、記録可能か否かが判定される(ステップS69)。ここで制御情報記録可能エリア33が記録できない場合には(ステップS69: NO)、例えば既に制御情報が記録されているとして(即ち、使用済み又は使用不能の光ディスクであるとして)、処理を終了する。

[0107] ステップS69の判定の結果、制御情報記録可能エリア33が記録可能である場合には(ステップS69: YES)、コントローラ14によって、コンテンツの記録がベリファイされた旨の信号が、コンテンツ配信サーバ3に送信される。

[0108] コンテンツ配信サーバ3にて、この旨の信号が受信されるのに応答して、CPU4に

よって、媒体情報データベース5から、ディスクIDに対応する復号キーxが読み取られる。この読み取られた復号キーxは、セキュアバスを介して、光学ドライブ22に送信される(ステップS70)。この送信に伴って、ディスクIDに対応する課金情報に従って、課金処理が実行される(ステップS71)。

[0109] 光学ドライブ22にて、受信された復号キーxにより、固有情報記録済みエリア32に記録されている、暗号化されたディスクキーxDKが復号化される。そして、この復号化されてなるディスクキーDKが制御情報記録可能エリア33に記録される(ステップS72)。この記録が完了されると、一連の、光ディスク1についての認証を伴うコンテンツの配信及び課金処理が終了される。

[0110] このように、本実施形態によれば、光ディスク1に対応付けされるディスク認証キーDAKを用いて、光学ドライブ22及びコンテンツ配信サーバ3間で光ディスク1についての認証を行い、この認証が成功した後に、光学ドライブ22及びコンテンツ配信サーバ3間でセキュアバスが確立され、確立されたセキュアバスを介して、コンテンツの生成に必要とされる、復号キーx及び暗号化されたタイトルキーdTKが光学ドライブ22に送信される。従って、例えばホストコンピュータ21を悪用する第三者が、光ディスク1の正規のユーザに成り済まして、コンテンツ配信サーバ3からのコンテンツを不正に取得しようとも、光学ドライブ22によってディスク認証キーDAKが取得されず、認証が失敗に終わる、或いはセキュアバスを介して送信される、例えば復号キーxや暗号化されたタイトルキーdTKを、読み取る或いは差し替えることは不可能であるので、コンテンツを再生可能な状態にある光ディスクは得られない。このように、光ディスク1についての認証により、コンテンツの取得権利におけるセキュリティー性を向上させると共に、光学ドライブ及びコンテンツ配信サーバで確立されるセキュアバスにより、コンテンツの再生に必要な情報の秘密を保持することができる。よって、結果として、不正な記録行為を防止することができる。

[0111] 尚、上述の実施形態では、コンテンツ配信サーバ3にて、タイトルキーTKを用いてのCSS方式によるコンテンツの暗号化を行っているが、ホストコンピュータ21にて、タイトルキーTKを用いてのCSS方式によるコンテンツの暗号化を行ってもよい。

[0112] 加えて、上述の実施形態によれば、コンテンツ記録可能エリア34において、コンテ

ンツ配信サーバ3から配信されるコンテンツが記録されるが、コンテンツ購入時に、販売者側によってコンテンツの一部又は全部が記録されていてもよい。この場合に、例えば光学ドライブ22にて、コンテンツ記録可能エリア34に対してコンテンツが記録されているか否かが判定される。この判定結果により、コンテンツが記録されている場合に、コンテンツ配信サーバ3から復号キーxが送信される。

[0113] 本発明は、上述した実施形態に限られるものではなく、請求の範囲及び明細書全体から読み取れる発明の要旨或いは思想に反しない範囲で適宜変更可能である。

産業上の利用可能性

[0114] 本発明は、例えばインターネット等のネットワークを介して、サーバ装置からクライアント装置へ配信され、課金の対象となるコンテンツを記録するための情報記録媒体、また、該クライアント装置側に設けられ、該情報記録媒体にコンテンツを記録するためのドライブ装置、該コンテンツの配信及び課金を管理するためのサーバ装置、前記コンテンツを配信するコンテンツサーバ装置、並びに該ドライブ装置及び前記サーバ装置間を仲介する仲介装置に利用することが可能である。

請求の範囲

- [1] ネットワークに收容されるサーバ装置及びクライアント装置を備えるシステムに利用され、該クライアント装置のドライブ装置で記録可能な情報記録媒体であって、
- 前記サーバ装置側から前記ネットワークを介して前記クライアント装置側へ少なくとも部分的に配信されるコンテンツを前記ドライブ装置で記録可能であるコンテンツ記録可能エリアと、
- 前記コンテンツ記録可能エリアから前記コンテンツを再生するのに用いられる制御情報を、前記ドライブ装置で記録可能である制御情報記録可能エリアと、
- 当該情報記録媒体を識別する媒体識別情報、並びに該媒体識別情報と対をなすと共に前記ドライブ装置及び前記サーバ装置間で当該情報記録媒体についての認証を行うための媒体認証情報を含む固有情報が予め記録されている固有情報記録済みエリアと
- を備えることを特徴とする情報記録媒体。
- [2] 前記ドライブ装置は、前記コンテンツ記録可能エリアに、前記認証が行われた後に前記サーバ装置側から前記ネットワークを介して前記ドライブ装置へ配信される、前記コンテンツを構成するタイトルに個別に割り当てられるタイトル単位暗号キーを、記録可能であることを特徴とする請求の範囲第1項に記載の情報記録媒体。
- [3] 前記媒体識別情報は、前記制御情報を取得するのに用いられる取得用情報を前記サーバ装置側から配信させるための配信指定情報としても機能することを特徴とする請求の範囲第1項に記載の情報記録媒体。
- [4] 前記取得用情報は、前記配信されるコンテンツが記録されたことが確認された後に前記サーバ装置側から配信される復号化用情報であり、
- 前記固有情報は、前記制御情報の少なくとも一部が暗号化されてなる暗号化情報であって、前記復号化用情報により復号化が可能である前記暗号化情報を更に含み、
- 前記制御情報記録可能エリアには、前記暗号化情報が復号化されてなる前記制御情報の少なくとも一部が記録可能である
- ことを特徴とする請求の範囲第3項に記載の情報記録媒体。

- [5] 請求の範囲第1項に記載の情報記録媒体の記録再生用に前記クライアント装置側に設けられる前記ドライブ装置であって、

前記コンテンツ記録可能エリア、前記制御情報記録可能エリア及び前記固有情報記録済みエリアに対し読み取り可能であり、前記コンテンツ記録可能エリア及び前記制御情報記録可能エリアに対し書き込み可能である読取書込手段と、

前記固有情報記録済みエリアから前記媒体識別情報及び前記媒体認証情報を読み取るように前記読取書込手段を制御し、前記コンテンツ記録可能エリアに対し、前記コンテンツを書き込むように前記読取書込手段を制御する制御手段と、

前記読み取られた媒体認証情報に基づくバスキーによって前記サーバ装置及び当該ドライブ装置間に、バスキー通信経路を確立する通信経路確立手段と、

前記読み取られた媒体識別情報を、前記ネットワークを介して前記サーバ装置側へ送信すると共に、前記確立されたバスキー通信経路を介して前記サーバ装置側から配信され、前記制御情報の一部若しくは該一部を取得するための取得用情報又は前記コンテンツ記録可能エリアから前記コンテンツを再生するのに用いられる他の制御情報の少なくとも一部であり、前記クライアント装置側に設けられ、前記ドライブ装置を制御することで前記ドライブ装置及び前記サーバ装置間を仲介する仲介装置に対して秘匿される秘匿情報を、受信するドライブ側通信手段と

を備え、

前記制御手段は、前記受信される秘匿情報を前記コンテンツ記録可能エリア及び前記制御情報記録可能エリアの少なくとも一方に書き込むように前記書込手段を制御する

ことを特徴とするドライブ装置。

- [6] 前記ドライブ側通信手段は、前記確立されたバスキー通信経路を介して、前記読み取られた媒体識別情報を前記サーバ装置側へ送信することを特徴とする請求の範囲第5項に記載のドライブ装置。

- [7] 前記媒体識別情報は、前記制御情報を取得するのに用いられる取得用情報を前記サーバ装置側から配信させるための配信指定情報としても機能し、

前記ドライブ側通信手段は、前記送信された媒体識別情報に応じて配信される前

記取得用情報を受信し、

前記制御手段は、前記受信された取得用情報により前記制御情報を取得して、前記取得された制御情報を前記制御情報記録可能エリアに書き込むように前記書込手段を制御する

ことを特徴とする請求の範囲第5項に記載のドライブ装置。

- [8] 前記コンテンツの書き込みの完了をベリファイするベリファイ手段を更に備え、
前記取得用情報は、前記完了がベリファイされた後に前記サーバ装置側から配信される復号化用情報であり、

前記制御情報の少なくとも一部が暗号化されてなる暗号化情報を前記受信された復号化用情報により復号化することで前記制御情報を取得し、

前記制御手段は、該取得された制御情報を前記制御情報記録可能エリアに書き込むように前記書込手段を制御する

ことを特徴とする請求の範囲第7項に記載のドライブ装置。

- [9] 請求の範囲第1項に記載の情報記録媒体に対する前記コンテンツの配信及び課金を管理する前記サーバ装置であって、

前記媒体認証情報を、前記コンテンツに対する課金の状態を示す課金情報及び前記媒体識別情報に対応付けて、格納する格納手段と、

前記固有情報記録済みエリアから読み取られる前記固有情報に含まれる前記媒体識別情報を、前記ドライブ装置から受信するサーバ側通信手段と、

該受信された媒体識別情報に対応する媒体認証情報を、前記格納手段から抽出する抽出手段と、

該抽出された媒体認証情報に基づくバスキーによって、前記ドライブ装置及び当該サーバ装置間に、バスキー通信経路を確立する通信経路確立手段と、

前記格納手段に格納されていると共に前記受信された媒体識別情報に対応する課金情報に従って、前記課金に係る課金処理を実行する課金処理手段と

を備え、

前記サーバ側通信手段は、前記確立されたバスキー通信経路を介して、前記制御情報の一部若しくは該一部を取得するための取得用情報又は前記コンテンツ記録

可能エリアから前記コンテンツを再生するのに用いられる他の制御情報の少なくとも一部であり、前記クライアント装置側に設けられ、前記ドライブ装置をコンピュータ制御すると共に前記ドライブ装置及び前記サーバ装置間を仲介する仲介装置に対して秘匿される秘匿情報を、配信する

ことを特徴とするサーバ装置。

- [10] 前記格納手段は、前記媒体識別情報に加えて又は代えて、前記制御情報の少なくとも一部が暗号化されてなる暗号化情報を更に格納し、

前記抽出手段は、前記媒体認証情報に加えて又は代えて、前記受信された媒体識別情報に対応する暗号化情報を、前記格納手段から抽出し、

前記サーバ側通信手段は、前記秘匿情報の少なくとも一部として、前記抽出された暗号化情報を送信する

ことを特徴とする請求の範囲第9項に記載のサーバ装置。

- [11] 前記格納手段は、前記媒体識別情報に加えて又は代えて、前記コンテンツを構成するタイトルに個別に割り当てられるタイトル単位暗号キー、及び該タイトル単位暗号キーを復号化するタイトル単位キーを更に格納し、

前記抽出手段は、前記媒体認証情報に加えて又は代えて、前記受信された配信指定情報に対応する前記タイトル単位暗号キー及びタイトル単位キーを、前記格納手段から抽出する

ことを特徴とする請求の範囲第9項に記載のサーバ装置。

- [12] 前記サーバ側通信手段は、前記秘匿情報の少なくとも一部として、前記抽出されたタイトル単位暗号キーを送信する

ことを特徴とする請求の範囲第11項に記載のサーバ装置。

- [13] 前記抽出されたタイトル単位キーにより前記コンテンツを暗号化して、前記クライアント装置側へ送信する暗号化手段を更に備える

ことを特徴とする請求の範囲第9項に記載のサーバ装置。

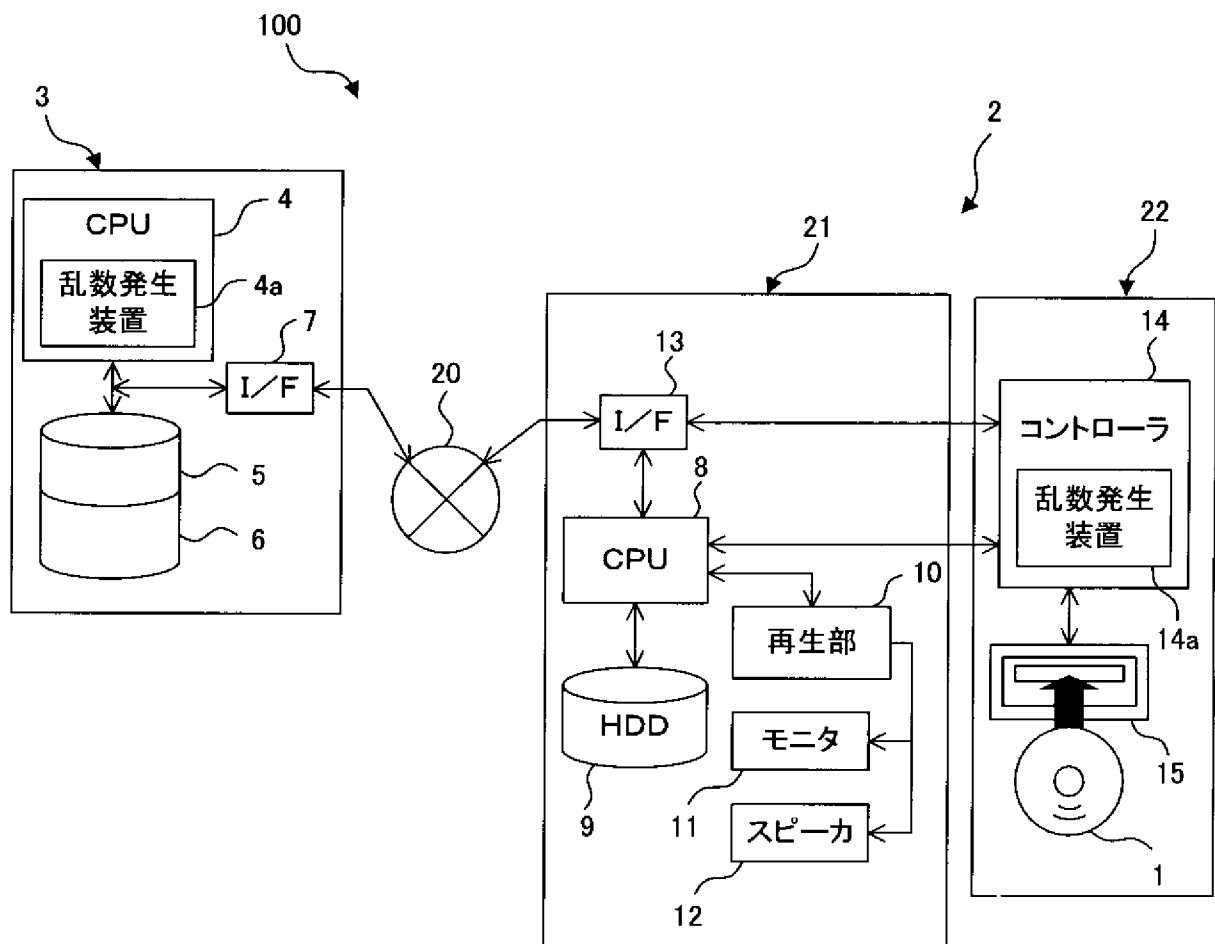
- [14] 請求範囲第11項に記載のサーバ装置から、前記抽出されたタイトル単位キーを、前記ネットワークを介して受信するコンテンツ配信側通信手段と、

複数のコンテンツを予め格納するコンテンツ格納手段と、

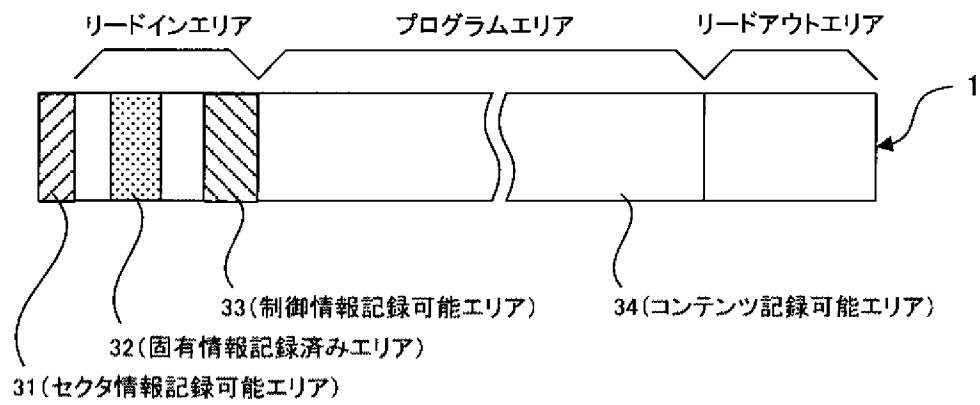
前記コンテンツを前記コンテンツ格納手段の中から抽出するコンテンツ抽出手段と、
該抽出されたコンテンツを、前記受信されたタイトル単位キーで暗号化するタイトル単位キー暗号化手段と
を備え、
前記コンテンツ配信側通信手段は、前記暗号化されたコンテンツを、前記ネットワークを介して、前記クライアント装置側に送信すること
を特徴とするコンテンツサーバ装置。

- [15] 請求の範囲第5項に記載のドライブ装置と共に前記クライアント装置側に設けられ、前記ドライブ装置をコンピュータ制御すると共に前記ドライブ装置及び前記サーバ装置間を仲介する仲介装置であって、
前記固有情報記録済みエリアから前記ドライブ装置により読み取られる前記固有情報に含まれる前記媒体識別情報を、前記確立されたバスキー通信経路を介して、前記ドライブ装置から受け取ると共に前記サーバ装置側へ送信する第1通信手段と、
前記秘匿情報を、前記確立されたバスキー通信経路を介して、前記サーバ装置から受け取ると共に前記ドライブ装置側へ送信する第2通信手段と、
を備えることを特徴とする仲介装置。

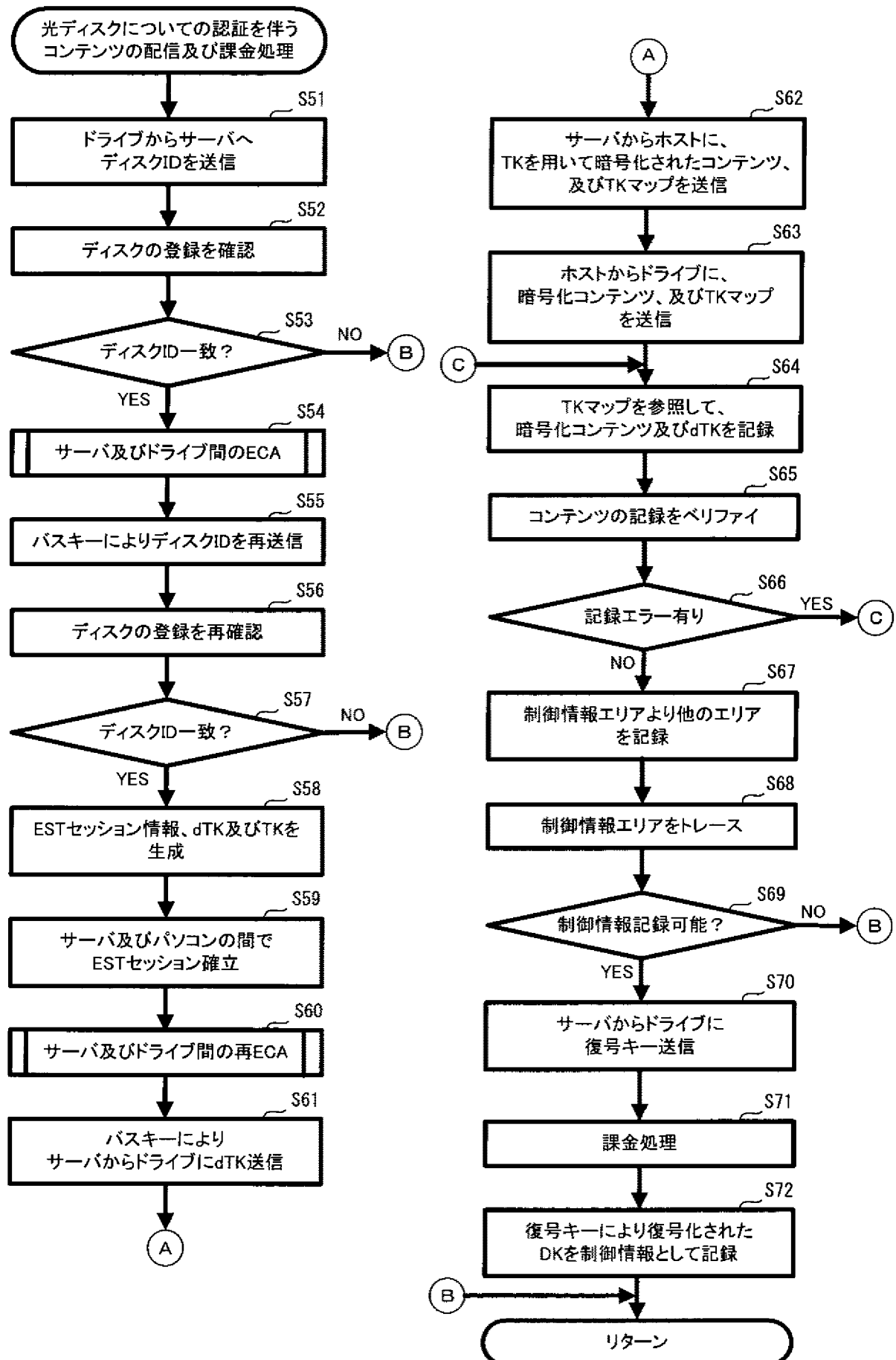
[図1]



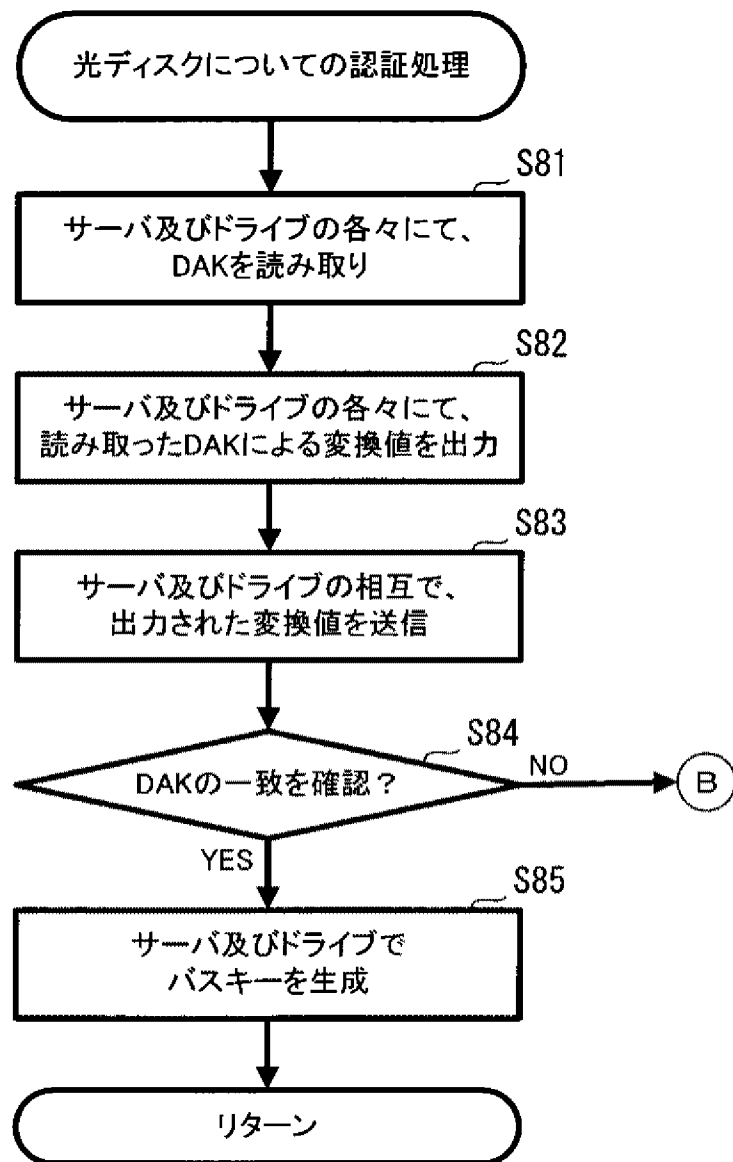
[図2]



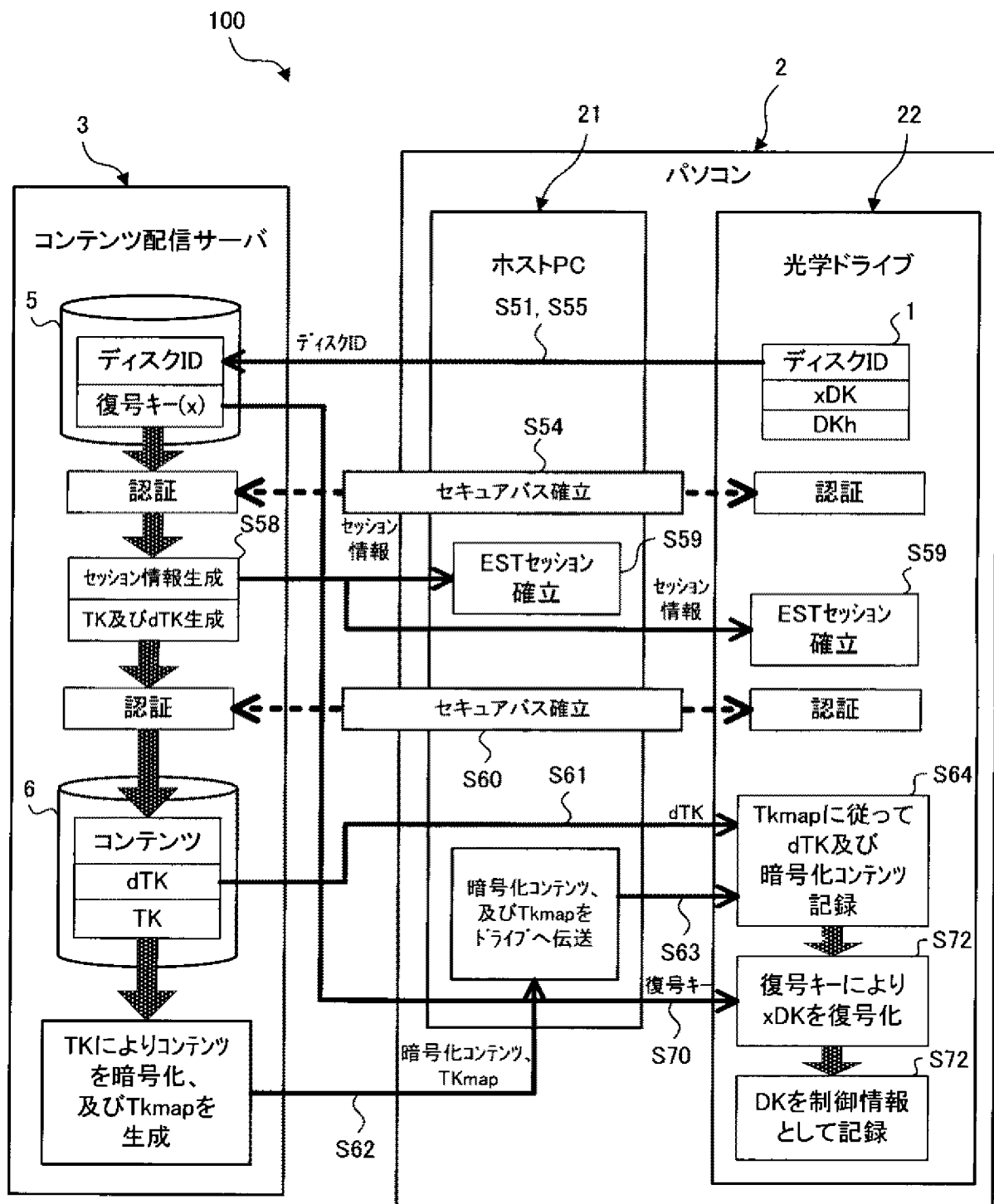
[図3]



[図4]



[図5]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2007/064180

A. CLASSIFICATION OF SUBJECT MATTER

G11B20/10(2006.01)i, G06F21/24(2006.01)i, H04L9/32(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)

G06F12/14, 21/02-21/06, 21/24, G09C1/00-5/00, G11B20/10-20/16, H04K1/00-3/00, H04L9/00-9/38

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	WO 2004/64314 A1 (Sony Corp.), 29 July, 2004 (29.07.04), Full text; all drawings & US 2005/89165 A1	1-7, 15 8-14
X Y	WO 2006/8972 A1 (Sony Corp.), 26 January, 2006 (26.01.06), Full text; all drawings & JP 2006-31818 A	1-7, 15 8-14
Y A	JP 2000-243026 A (Nippon Telegraph And Telephone Corp.), 08 September, 2000 (08.09.00), Full text; all drawings (Family: none)	8 1-7, 9-15

☒ 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
26 September, 2007 (26.09.07)

Date of mailing of the international search report
09 October, 2007 (09.10.07)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2007/064180

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	WO 97/14144 A1 (Matsushita Electric Industrial Co., Ltd.), 17 April, 1997 (17.04.97), Full text; all drawings & EP 802527 B1 & US 6081785 A	9-14 1-8, 15
A	WO 00/72317 A1 (Matsushita Electric Industrial Co., Ltd.), 30 November, 2000 (30.11.00), Full text; all drawings & EP 1098303 B1 & JP 2001-43533 A	1-15
A	EP 1162617 A2 (Pioneer Corp.), 12 December, 2001 (12.12.01), Full text; all drawings & JP 2001-307427 A & US 2001/36268 A1	1-15
A	JP 2007-109316 A (Pioneer Corp.), 26 April, 2007 (26.04.07), Full text; all drawings (Family: none)	1-15
A	WO 2007/10987 A1 (Pioneer Corp.), 25 January, 2007 (25.01.07), Full text; all drawings (Family: none)	1-15
A	WO 2007/46494 A1 (Pioneer Corp.), 26 April, 2007 (26.04.07), Full text; all drawings (Family: none)	1-15
A	WO 2007/49743 A1 (Pioneer Corp.), 03 May, 2007 (03.05.07), Full text; all drawings (Family: none)	1-15

A. 発明の属する分野の分類（国際特許分類（I P C））

Int.Cl. G11B20/10(2006.01)i, G06F21/24(2006.01)i, H04L9/32(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. G06F12/14, 21/02-21/06, 21/24, G09C1/00-5/00, G11B20/10-20/16, H04K1/00-3/00, H04L9/00-9/38

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	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

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	WO 2004/64314 A1（ソニー株式会社）2004.07.29, 全文, 全図 & US 2005/89165 A1	1-7, 15 8-14
X Y	WO 2006/8972 A1（ソニー株式会社）2006.01.26, 全文, 全図 & JP 2006-31818 A	1-7, 15 8-14
Y A	JP 2000-243026 A（日本電信電話株式会社）2000.09.08, 全文, 全 図（ファミリーなし）	8 1-7, 9-15

☒ 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

2 6 . 0 9 . 2 0 0 7

国際調査報告の発送日

0 9 . 1 0 . 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

特許庁審査官（権限のある職員）

松尾 淳一

5 D

8 8 4 2

電話番号 0 3 - 3 5 8 1 - 1 1 0 1 内線 3 5 5 1

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 A	WO 97/14144 A1 (松下電器産業株式会社) 1997. 04. 17, 全文, 全図 & EP 802527 B1 & US 6081785 A	9-14 1-8, 15
A	WO 00/72317 A1 (松下電器産業株式会社) 2000. 11. 30, 全文, 全図 & EP 1098303 B1 & JP 2001-43533 A	1-15
A	EP 1162617 A2 (Pioneer Corporation) 2001. 12. 12, 全文, 全図 & JP 2001-307427 A & US 2001/36268 A1	1-15
A	JP 2007-109316 A (パイオニア株式会社) 2007. 04. 26, 全文, 全図 (ファミリーなし)	1-15
A	WO 2007/10987 A1 (パイオニア株式会社) 2007. 01. 25, 全文, 全図 (ファミリーなし)	1-15
A	WO 2007/46494 A1 (パイオニア株式会社) 2007. 04. 26, 全文, 全図 (ファミリーなし)	1-15
A	WO 2007/49743 A1 (パイオニア株式会社) 2007. 05. 03, 全文, 全図 (ファミリーなし)	1-15