

(43) 国際公開日
2007 年 10 月 4 日 (04.10.2007)

PCT

(10) 国際公開番号
WO 2007/111196 A1

- (51) 国際特許分類:
G06F 21/24 (2006.01) H04N 7/167 (2006.01)
G11B 20/10 (2006.01)
- (21) 国際出願番号: PCT/JP2007/055655
- (22) 国際出願日: 2007 年 3 月 20 日 (20.03.2007)
- (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2006-084097 2006 年 3 月 24 日 (24.03.2006) JP
- (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): 黒田 和男 (KURODA, Kazuo) [JP/JP]; 〒3598522 埼玉県所沢市

花園 4 丁目 2 6 1 0 番地 パイオニア株式会社 所沢工場内 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 1 6 番 1 0 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).

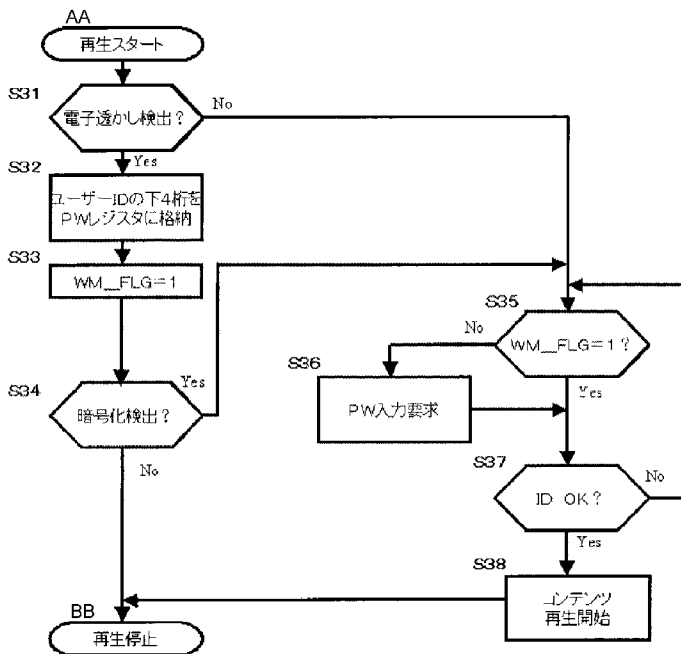
- (81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, MG, MK, MN, MW, MX, 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.

- (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,

[続葉有]

(54) Title: INFORMATION DELIVERY APPARATUS, INFORMATION RECORDING MEDIUM, AND INFORMATION REPRODUCING APPARATUS

(54) 発明の名称: 情報配信装置、情報記録媒体、および情報再生装置



AA... START REPRODUCTION
S31... DIGITAL WATERMARKS DETECTED?
S32... STORE LAST 4 DIGITS OF USER ID IN PW REGISTER
S34... ENCRYPTION DETECTED?
BB... STOP REPRODUCTION
S36... REQUEST PW INPUT
S38... START CONTENT REPRODUCTION

(57) Abstract: A user ID and a content ID are embedded in content data as digital watermarks. Reproduction control data including a PGC having a routine requesting an input of a password composed of the last four digits of the user ID is generated. Information content including the content data and reproduction control data is recorded on a recording medium. An information reproducing apparatus detects the digital watermarks to automatically generate a password from the user ID. This eliminates the need for the user to input the password and promotes the protection of the copyright holder and the like of the information content by using the digital watermarks.

(57) 要約: コンテンツデータに対し、ユーザーIDおよびコンテンツIDを電子透かしとして埋め込む。また、ユーザーIDの下4桁からなるパスワードの入力を求めるルーチンを有するPGCを含む再生制御データを生成する。これらコンテンツデータと再生制御データからなる情報コンテンツを記録媒体に記録しておく。情報再生装置は、電子透かしを検出し、ユーザーIDからパスワードを自動生成する。これによれば、ユーザーによるパスワード入力の手間が省け、かつ電子透かしを利用することにより情報コンテンツに対する著作権者等の保護を図ることができる。



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).

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

情報配信装置、情報記録媒体、および情報再生装置

技術分野

[0001] 本発明は、映画などの情報コンテンツを配信するコンテンツ配信装置、情報コンテンツが記録された情報記録媒体、かかる情報記録媒体を再生する情報再生装置などに関する。

背景技術

[0002] 現在、DVD-R (DVD Recordable)、DVD-RW (DVD ReWritable) などの追記型・書換可能型の情報記録媒体が普及している。これらの追記型・書換可能型情報記録媒体を用いることにより、ユーザーは、コンテンツ配信業者よりネットワークを介して配信される映画等の情報コンテンツを自ら所有する情報記録媒体に記録することができる。たとえば、インターネットを介してコンテンツ配信業者が開設するホームページを閲覧し、当該ホームページ内でリスト化されたコンテンツ群の中から自分の所望する情報コンテンツをデジタルデータとして自己のPC等にダウンロードして記録する。

[0003] ここで配信される情報コンテンツはデジタルデータゆえ、違法な複製が問題となる。映画等の情報コンテンツがネットワークを介して容易にデジタル情報として記録することが可能になると、このような違法な複製を防止して著作権者の保護を図ることが重要になる。

[0004] この問題に対処する方法としてまず、コンテンツデータ自体を暗号化するCSS暗号化方式(以下、適宜「CSS」と称す)がある。このCSSにより暗号化されたコンテンツデータはよりセキュアにネットワーク上を流通したのだが、このCSSの暗号を解読するいわゆるDeCSSと呼ばれるソフトウェアがネットワーク上で配布されるという事態が発生したため、コンテンツデータにかけた暗号が違法に解除されてしまうという問題が新たに起きた。

[0005] そこで従来は、このような違法な暗号解除行為を防止するため、電子透かし技術を利用して複製を制御する手法が開発されており、たとえば特許文献1等に記載されて

いるように、CSSと電子透かしとを組み合わせ、コンテンツ製作者等が有する著作権の保護を図っている。

[0006] 一方、上記電子透かしとは別に、DVDに記録された情報コンテンツを再生する際に、パスワードの入力を求める手法が存在する。例えば特許文献2には、DVD－Video規格に準拠した再生制御情報にパスワード入力を要求するプログラムを組み込み、これにより視聴制限を行っている。

[0007] 特許文献1:特開2003－317378号公報

特許文献2:特開2003－132624号公報

発明の開示

発明が解決しようとする課題

[0008] しかしながら電子透かしを単純に組み込む従来の手法では、装置の製造側に負荷を与えるわりには最終的な使用者であるエンドユーザーに対してメリットが少なく、電子透かしに関連する機能を搭載する装置を開発するインセンティブに欠ける。

[0009] 他方で、パスワード入力をユーザーに求める手法では、再生装置としては負荷無く製造ができるが、ユーザーにとっては情報コンテンツの再生の度にいちいちパスワードを入力する必要があり、そもそも著作権保護の観点からも違法な複製に対して保護が不十分となってしまう。

[0010] 本発明は上記に示したような課題を一例として鑑みてなされたものであり、本発明の目的は、装置の製造側、エンドユーザー及びコンテンツ提供側のいずれもがメリットを享受できる機器やシステムを提供しつつ、あわせて著作権の保護を図っていくことにある。

課題を解決するための手段

[0011] 上記課題を解決するために本発明の情報生成装置は、識別情報を電子透かしによりコンテンツデータに埋め込む電子透かし埋め込み部と、前記識別情報から生成可能なパスワードの入力を求めるルーチンを有するとともに前記コンテンツデータの再生制御を行う再生制御データを生成する再生制御情報生成部と、前記識別情報が埋め込まれたコンテンツデータの少なくとも一部を暗号化する暗号化部と、前記暗号化されたコンテンツデータと前記再生制御データとからなる情報コンテンツを生成

する手段と、を有することを特徴とする。

[0012] なお前記識別情報は、前記情報コンテンツの配信を要求するユーザーを識別するためのユーザーID、前記情報コンテンツを特定するためのコンテンツID、または前記情報コンテンツを記録媒体に記録する記録装置を識別するための記録装置IDの少なくとも一つを含むことが好ましい。

[0013] また、前記識別情報は前記ユーザーIDであり、前記パスワードは前記ユーザーIDの少なくとも一部からなることが好ましい。

[0014] さらに、上記課題を解決するために、本発明の情報配信装置は、上記のいずれかに記載の情報生成装置と、前記情報コンテンツを配信する配信部と、を具備することを特徴とする。

また、上記課題を解決するため、本発明のデータ構造は、ネットワークを介してダウンロード可能なデータ構造であって、電子透かしにより識別情報が埋め込まれたコンテンツデータと、前記識別情報から生成可能なパスワードの入力を求めるルーチンを有するとともに前記コンテンツデータの再生制御を行う再生制御データと、からなることを特徴とする。

[0015] また、上記課題を解決するために、本発明の情報記録媒体は、上記記載のデータ構造からなる情報コンテンツが記録されている。

[0016] また、上記課題を解決するために、本発明の情報再生装置は、上記に記載の情報記録媒体を再生する情報再生装置であり、前記コンテンツデータに前記電子透かしが埋め込まれているか否か検出する電子透かし検出部と、前記コンテンツデータの少なくとも一部が暗号化されているか否かを検出する暗号化検出部と、前記電子透かしが検出されたにも拘わらず、前記コンテンツデータが暗号化されていない場合、前記情報コンテンツの再生を禁止する再生制御部と、を備えることを特徴とする。

[0017] なお上記情報再生装置は、前記電子透かしが検出されたにも拘わらず、前記コンテンツデータが暗号化されていない場合、前記識別情報を外部機器に送信する送信部を備えることが好ましい。また、前記再生制御部は、前記電子透かしにより埋め込まれた前記識別情報が、前記送信された前記識別情報に基づき前記外部機器により生成された再生禁止リストに含まれる場合、前記情報コンテンツの再生を禁止す

ることが好ましい。

- [0018] また、上記課題を解決するために、本発明の情報再生プログラムは、上記に記載の情報記録媒体を再生するための情報再生プログラムであり、前記コンテンツデータに前記電子透かしが埋め込まれているか否かを検出し、前記コンテンツデータの少なくとも一部が暗号化されているか否かを検出し、前記電子透かしが検出されたにも拘わらず、前記コンテンツデータが暗号化されていない場合、前記情報コンテンツの再生を禁止するようコンピュータを制御することを特徴とする。
- [0019] また、上記課題を解決するために、本発明の情報記録装置は、情報コンテンツを記録媒体に記録する情報記録装置であり、前記情報コンテンツは、コンテンツデータと、パスワードの入力を求めるルーチンを有するとともに前記コンテンツデータの再生制御を行う再生制御データと、からなり前記コンテンツデータの少なくとも一部が暗号化されており、前記情報記録装置は、前記パスワードを生成可能な識別情報を電子透かしとして生成する電子透かし生成部と、前記生成された前記電子透かしを前記コンテンツデータに埋め込む電子透かし埋め込み部と、を備えることを特徴とする。
- [0020] また、上記課題を解決するために、本発明の情報記録プログラムは、情報コンテンツを記録媒体に記録するための情報記録プログラムであり、前記情報コンテンツは、コンテンツデータと、パスワードの入力を求めるルーチンを有するとともに前記コンテンツデータの再生制御を行う再生制御データと、からなり前記コンテンツデータの少なくとも一部が暗号化されており、前記情報記録プログラムは、前記パスワードを生成可能な識別情報を電子透かしとして生成し、前記生成された前記電子透かしを前記コンテンツデータに埋め込むようコンピュータを制御することを特徴とする。
- [0021] 上記課題を解決するために、コンピュータ読取可能な媒体内の第1コンピュータプログラム製品は、上述した本発明の情報再生装置(但し、その各種態様を含む)に備えられたコンピュータにより実行可能なプログラム命令を明白に具現化し、該コンピュータを、前記電子透かし検出部、前記暗号化検出部及び前記再生制御部のうち少なくとも一部として機能させる。
- [0022] 上記課題を解決するために、コンピュータ読取可能な媒体内の第2コンピュータプログラム製品は、上述した本発明の情報記録装置(但し、その各種態様を含む)に備

えられたコンピュータにより実行可能なプログラム命令を明白に具現化し、該コンピュータを、前記電子透かし生成部及び前記電子透かし埋め込み部のうち少なくとも一部として機能させる。

[0023] 本発明の第1又は第2コンピュータプログラム製品によれば、当該コンピュータプログラム製品を格納するROM、CD-ROM、DVD-ROM、ハードディスク等の記録媒体から、当該コンピュータプログラム製品をコンピュータに読み込めば、或いは、例えば伝送波である当該コンピュータプログラム製品を、通信手段を介してコンピュータにダウンロードすれば、上述した本発明の情報再生装置又は情報記録装置を比較的容易に実施可能となる。更に具体的には、当該コンピュータプログラム製品は、上述した本発明の情報再生装置又は情報記録装置として機能させるコンピュータ読取可能なコード(或いはコンピュータ読取可能な命令)から構成されてよい。

[0024] 本発明のこのような作用及び他の利得は次に説明する実施例から明らかにされる。

図面の簡単な説明

[0025] [図1]本発明の実施例に係るコンテンツ配信システムの構成を示す概念図である。

[図2]本発明の実施例に係るコンテンツ配信装置のブロック図である。

[図3]本発明の実施例に係る電子透かしにより埋め込まれる情報を示す図である。

[図4]DVDフォーマットに準拠した記録構造を示す図である。

[図5]本発明の実施例に係るユーザーPCのブロック図である。

[図6] (a)はコンテンツ配信装置における処理のフローを示す図であり、(b)はユーザーPCにおける処理のフローを示す図である。

[図7]電子透かし検出機能を備えていない従来の情報再生装置における再生処理のフローチャートである。

[図8]電子透かし検出機能を備えたDVD再生プログラムがインストールされたPCにおける再生処理のフローチャートである。

[図9]電子透かし検出機能とリボケーション機能を備えたDVD再生プログラムがインストールされたPCにおける再生処理のフローチャートである。

符号の説明

[0026] 1 コンテンツ配信装置

- 1a 電子透かし埋込み部
- 1b 電子透かし生成部
- 1c DVDフォーマッタ
- 1d 再生制御情報生成部
- 1e 暗号化部
- 1f インターフェース
- 1g 制御回路
- 2 インターネット
- 3 ユーザーPC
- 3a 光ディスクドライブ
- 3b メモリ
- 3c CPU
- 3d インターフェース
- 3e ATAPインターフェース
- 3f 電子透かし検出部
- 3g グラフィックボード
- 3h HDD
- 3i モニタ

発明を実施するための最良の形態

[0027] 以下、本発明を実施するための最良の形態について実施例毎に順に図面に基づいて説明する。

[0028] 図1に、本発明のコンテンツ配信システムのブロック図を示す。図1において、映画等の情報コンテンツは、コンテンツホルダーが所有するコンテンツ配信装置1からネットワークであるインターネット2を介して配信され、ユーザー端末であるPC3にてダウンロードされる。この場合、例えばユーザーは、インターネット上のホームページを閲覧するなどして自己の所望する情報コンテンツを特定する。そして特定した情報コンテンツを自己のPC3にインターネット2を介してダウンロードする。

[0029] 図2は、情報配信装置としてのコンテンツ配信装置1をより具体的に表したものであ

る。コンテンツ配信装置1は、情報生成装置と配信部とから構成される。情報生成装置は、電子透かし埋込み部1a、電子透かし生成部1b、DVDフォーマッタ1c、再生制御情報生成部1d、CSS暗号化部1e、制御回路1gからなり、配信部はインターフェース1fと制御回路1gからなる。なお、本明細書においては、「電子透かし」を適宜「ウォーターマーク」あるいは「WM」と記載する。

[0030] 電子透かし埋込み部1aは、特定されたコンテンツデータの映像データ、音声データやそれらに付随するデータに対して電子透かしにより識別情報を埋め込むものである。なお、識別情報としては、情報コンテンツの配信を要求するユーザーを識別するためのユーザーIDと情報コンテンツを特定するためのコンテンツIDとを含む。電子透かし生成部1bは、制御回路1gの制御に基づき、コンテンツIDとユーザーIDからなる識別情報を電子透かしとして生成し、生成された電子透かしを電子透かし埋込み部1aに供給する。

[0031] なお、識別情報としては、コンテンツIDとユーザーID以外に、例えばユーザー名やクレジット番号、情報コンテンツを記録媒体に記録する記録装置を識別するための記録装置IDなどを用いても良い。なお、記録装置IDとしては、例えば光ディスクドライブ3aのシリアル番号や、光ディスクドライブ3aにインストールされているファームウェアのシリアル番号などが挙げられる。

[0032] 図3に、電子透かし生成部1bにて生成される電子透かし情報の一例を示す。この例では電子透かし情報は16バイトの情報量を持って構成され、コンテンツIDおよびユーザーIDはそれぞれ2バイト割り当てられている。なお、本実施例ではコンテンツIDとユーザーIDの双方を電子透かしとしてコンテンツデータに埋め込む例を示すが、これに限定されるものではなく、どちらか一方のみを電子透かしとしてコンテンツデータに埋め込んでもよい。

[0033] なお、本実施例の電子透かしは、著作権情報も3バイトの情報量をもって挿入されており、著作権情報の例としては、著作者情報やCCI(Copy Control Information)などがある。

[0034] 再生制御情報生成部1dは、制御回路1gの制御に基づき、情報コンテンツの再生時に所定のパスワード入力を求めるルーチンを有する再生制御情報(PGC)を生成

し、生成した再生制御データをDVDフォーマッタ1cに送出する。DVDフォーマッタ1cは、再生制御情報生成部1dから再生制御データを受け取るとともに、電子透かしが埋め込まれたコンテンツデータをDVD-Video規格のフォーマットに従って変換し、出力する。

[0035] また、CSS暗号化部1eは、フォーマット化されたコンテンツデータの少なくとも一部に対してCSS方式による暗号化を施し、暗号化されたコンテンツデータと再生制御データとからなる情報コンテンツを生成し、インターフェース1fへ送出する。

[0036] そして制御回路1gは、情報コンテンツをインターフェース1fを介してネットワーク上に送出するまで各部の統括制御を行う。

[0037] 図4にDVDフォーマットのDVD-Video規格に準拠した記録構造を示す。上述のパスワード入力を求める制御情報は、図4におけるVTSの下位層に位置するPGC内のプリコマンドにより設定される。

[0038] 以上が図1におけるコンテンツ配信側の構成であるが、続いてコンテンツ受信側であるユーザー端末のPC3の具体的な構成を図5に示す。

[0039] 図5において、PC3は情報記録プログラムと情報再生プログラムがインストールされることにより情報記録再生装置を構成するものであり、光ディスクドライブ3a、メモリ3b、暗号化検出部および再生制御部として機能するCPU3c、インターフェース3d、ATA/PATAインターフェース3e、電子透かし検出部3f、グラフィックボード3g、HDD3h、モニタ3iを備えてなる。

[0040] なお、コンテンツ配信装置1により、コンテンツデータに電子透かしを埋め込むようにしたが、その代わりに、PC3側に電子透かし生成部と電子透かし埋込み部を設け、コンテンツデータに電子透かしを埋め込むようにしてもよい。例えば電子透かし生成部は、CPU3cからの指示により、情報コンテンツの再生に用いられるパスワードを生成可能な識別情報に基づき電子透かしを生成し、生成した電子透かしをコンテンツデータに埋め込む処理を行う。なお、電子透かし生成部と電子透かし埋込み部は、ハードウェアにより構成しても、情報記録プログラムからなるソフトウェアによって構成しても良い。

[0041] 一方、図5に示されるインターフェース3dは、CPU3cの制御のもと、インターネット

を介してダウンロードした情報コンテンツを受信し、バスを通じてATAPインターフェース3eへ受信した情報コンテンツを送出する。

[0042] 光ディスクドライブ3aは、ATAPインターフェース3eを介して情報コンテンツを受信し、受信した情報コンテンツを当該光ディスクドライブ3aに挿入されているDVD-Rなどの光ディスク(図示しない)に記録する。なお、ダウンロードした情報コンテンツを光ディスクドライブ3aではなく、HDD3hにいったん記録し、HDD3hから光ディスクに記録するようにしてもよい。

[0043] 次に、コンテンツ配信側およびコンテンツ受信側での具体的な処理の流れを、図5～図8に基づいて説明する。

[0044] 図6のうち、(a)は、コンテンツ配信側であるコンテンツ配信装置1における処理のフローを示す図であり、(b)はユーザー端末であるPC3における処理のフローを示す図である。

[0045] まず図6(a)に従いコンテンツ配信装置1の処理フローを説明する。コンテンツ配信装置1では、ユーザー端末であるPC3からのコンテンツ配信要求の有無を確認する(ステップS1)。コンテンツ配信要求が無い場合、すなわちステップS1で「No」の場合には、続けてPC3からのコンテンツIDの受信の有無を確認する(ステップS2)。なお、詳細は後述するが、違法な複製が行われた情報コンテンツが再生された時、コンテンツデータに電子透かしとして埋め込まれていたコンテンツIDおよびユーザーIDがユーザー端末からコンテンツ配信装置1に向けて送信される。

[0046] コンテンツIDの受信が無い場合、すなわちステップS2で「No」の場合には、再びステップS1に戻る。また、ステップS2でコンテンツIDを受信した場合(ステップS2で「Yes」)、コンテンツ配信装置1は受信したコンテンツIDを再生禁止IDリストに追加する処理を行う(ステップS7)。この再生禁止IDリストは、例えばコンテンツ配信装置1側の図示しないHostサーバーに記録保持される。

[0047] 続いて、ステップS1でPC3からのコンテンツ配信要求があった場合(ステップS1で「Yes」)、コンテンツ配信装置1はユーザー端末であるユーザーPC3と課金・決済の手続きを行う(ステップS3)。この課金・決済手続きの際に、コンテンツ配信装置1はユーザーIDを認識し、配信する情報コンテンツに対応したコンテンツIDを生成する。

- [0048] そしてステップS4においては、課金手続きの際に認識したユーザーIDと生成したコンテンツIDとを識別情報として電子透かし生成部に送信する。なお、電子透かし生成部では、上述のとおりこの識別情報に基づいてコンテンツデータに埋め込むべき電子透かし情報を生成し、生成した電子透かし情報を電子透かし埋込み部1aにより配信するコンテンツデータに埋め込む。
- [0049] 続いてステップS5においては、課金手続きの際に認識したユーザーIDのうち、例えばその下4桁をパスワードとする再生制御情報(プログラムチェーンPGC)を生成する。なお、パスワード設定に関するPGCの生成手法に関しては、特開2003-132624号公報等の開示がなされている。
- [0050] 電子透かしが埋め込まれたコンテンツデータと生成された再生制御データは、DVDフォーマット1cに入力され、そこでDVDフォーマットに従って変換出力される。そして、出力されたコンテンツデータは、CSS暗号化部1eによりCSS方式による暗号化処理がなされた後、最終的に情報コンテンツとしてPC3に向けてインターネットを介して配信される(ステップS6)。
- [0051] 続いて、図6(b)に従いユーザーPC3の処理フローを説明する。ユーザーが所望する情報コンテンツが特定されると、ユーザーPC3は、特定された情報コンテンツをダウンロードすべくコンテンツ配信装置1(配信サーバー)に対して配信要求を行う(ステップS11)。この際、配信要求とともにユーザーIDをコンテンツ配信装置1に対して送信する。通常、ユーザーはコンテンツホルダーとの間でコンテンツダウンロードに関する入会手続き等の契約処理を事前に行い、この入会手続きの際にユーザーIDが割り振られる。
- [0052] 続いてステップS12では、特定された情報コンテンツのダウンロードに関する課金手続きがコンテンツ配信装置1との間で行われる。例えばインターネット上のコンテンツホルダーのホームページ内にて、所定の方式により電子決済が行われる。決済の方法としては、電子マネーやクレジット番号の入力などを利用してもよい。
- [0053] そして課金手続きを終えると、コンテンツ配信装置1から所望する情報コンテンツのダウンロードが行われ、光ディスクへの記録が開始される(ステップS13)。そして、情報コンテンツのダウンロードが完了すると(ステップS14「Yes」)、記録が停止される(

ステップS15)。

- [0054] 次にPC3において、配信された情報コンテンツを再生する際のフローについて図5および図7～9に基づいて説明する。なお、図7は電子透かし検出機能を備えていない一般的な情報再生装置における再生処理のフローを示す図、図8はいわゆるスタンドアローン型の電子透かし検出機能を備えた特別な情報再生装置における再生処理のフローを示す図、図9は電子透かし検出機能を備えかつネットワークへの接続機能を有する特別な情報再生装置における再生処理のフローを示す図である。
- [0055] また、本実施例にて説明に用いられる情報コンテンツはコンテンツデータと再生制御データとからなるデータ構造をもつ。そしてコンテンツデータには、ユーザーIDとコンテンツIDが電子透かしとして埋め込まれており、かつ再生制御データには再生時にパスワード入力を求めるPGCが含まれるものとする。また、入力されるパスワードとしては、ユーザーIDの下4桁が設定されているものとする。
- [0056] まず図7に基づいて、電子透かし検出機能を備えていない従来のPC(図示しない)にて光ディスクに記録された情報コンテンツの再生処理を行う例を説明する。
- [0057] ユーザーが情報コンテンツを再生しようとする場合、ユーザーによる再生指示が行われることにより処理がスタートする。なお、当該情報コンテンツがDVD等に記録されている場合には、DVDを情報再生装置に挿入時に自動的に再生指示が行われる場合もある。
- [0058] そして再生指示に基づいて情報コンテンツの再生処理がスタートすると、再生制御データに含まれるPGCに基づき、パスワードの入力を要求する(ステップS21)。このとき、ユーザーはPCに接続されたキーボードなどの入力手段を用いて、パスワードを入力する。この場合、パスワードは上述のとおりユーザーIDの下4桁であり、ユーザーはメモなどを参照しながらユーザーIDの下4桁を入力することになる。
- [0059] 次に、入力されたパスワードが正しいものであるかチェックが行われる(ステップS22)。ここで正しいパスワードが入力されない場合(ステップS22で「No」)、再度ステップS21に戻りパスワードの入力を求める。このとき、ステップS21に戻る回数を制限してもよい。例えば3回、正しいパスワードが入力されなければ処理を中止するように制御してもよい。

- [0060] ステップS22で正しいパスワードが入力された場合、情報コンテンツの再生を開始する(ステップS23)。
- [0061] 次に図8に基づいて、電子透かし検出機能を備えたDVD再生プログラムがインストールされたPC3(情報再生装置)における再生処理について説明する。
- [0062] まずユーザーが自己のPC上にて再生指示を入力することにより、情報コンテンツの再生処理がスタートする。
- [0063] 再生処理がスタートすると、まずCPU3cは、電子透かし検出部3fを制御して、再生するコンテンツデータに電子透かしがあるのか否かを確認する(ステップS31)。
- [0064] 電子透かしが検出されない場合、すなわちステップS31において「No」の場合には、続けて電子透かしが検出されたか否かのフラグを確認し(ステップS35)、当該フラグは「1」とはなっていないのでパスワード入力を要求し(ステップS36)、入力されたパスワードが正しいかをチェックし(ステップS37)、正しいパスワード(この場合であればユーザーIDの下4桁)が入力されていればそのまま情報コンテンツの再生を開始する(ステップS38)。なお、ユーザーによるパスワード入力の方法としては、図示しないキーボード等を用い、ユーザーIDの下4桁を入力することが考えられる。
- [0065] 一方、ステップS31において「Yes」の場合、すなわち電子透かしを検出した場合には、検出された電子透かしの内容であるユーザーIDの下4桁をメモリ3bに設けられたパスワードレジスタ部に格納する(ステップS32)。そして続けて電子透かしを検出したこと示すフラグWM_FLGを立てる(ステップS33)。
- [0066] 続いてステップS34においては、再生するコンテンツデータに対する暗号化の有無をチェックする。すなわち、再生しようとするコンテンツデータがCSS方式による暗号化がなされているかを確認し、暗号化が検出されればステップS35へ移行する。
- [0067] 一方、このステップS34において暗号化が検出されなければ、すなわち当該コンテンツデータに暗号化処理がなされていなければ、当該情報コンテンツの再生を中止する。なぜなら、このような情報コンテンツはDeCSSなどにより違法に暗号化が解除され、情報記録媒体に複製された可能性が高いものであるからである。
- [0068] 次に、ステップS34にて暗号化を検出した後は、ステップS35に移行し、CPU3cはメモリ3bを参照して電子透かしを検出したか否かのフラグを確認する。上述のとおり、

電子透かしが検出されているので当該フラグは「WM_FLG=1」である。したがって、CPU3cは、パスワードレジスタ部に格納されたパスワード(ユーザーIDの下4桁)を参照し、自動的に入力されたパスワードとして当該レジスタに保持されたパスワードを用いてパスワード入力処理を完了させる。

- [0069] パスワード入力処理が自動的に行われた後は、入力されたパスワードが正しいパスワードであるかチェックを行う(ステップS37)。なお、この場合のパスワード入力処理は、電子透かしにより検出されたユーザーIDの下4桁が機械的に処理されているので間違い可能性は低い。
- [0070] そしてパスワードのチェックを終えた後に、引き続いて情報コンテンツの再生を開始する(ステップS38)。これにより、ユーザーは、キーボードを用いてパスワードをいちいち入力する必要がなくなり、コンテンツ再生に関する利便性が向上する。
- [0071] 次に図9に基づいて、電子透かし検出機能とリボケーション機能を備えたDVD再生プログラムがインストールされたPC3(情報再生装置)における再生処理について説明する。
- [0072] まずユーザーが自己のPC上にて再生指示を入力することにより、情報コンテンツの再生処理がスタートする。
- [0073] 再生処理がスタートすると、まずCPU3cは、電子透かし検出部3fを制御して、再生されたコンテンツデータに電子透かしがあるのか否かを確認する(ステップS41)。
- [0074] 電子透かしが検出されない場合、すなわちステップS41において「No」の場合には、続けて電子透かしが検出されたか否かのフラグを確認し(ステップS46)、当該フラグは「1」とはなっていないのでパスワード入力を要求し(ステップS47)、入力されたパスワードが正しいかをチェックし(ステップS48)、正しいパスワード(この場合であればユーザーIDの下4桁)が入力されていればそのまま情報コンテンツの再生を開始する(ステップS49)。なお、ユーザーによるパスワード入力の方法としては、図示しないキーボード等を用い、ユーザーIDの下4桁を入力することが考えられる。
- [0075] 一方、ステップS41において「Yes」の場合、すなわち電子透かしを検出した場合には、検出された電子透かしの内容であるユーザーIDの下4桁をメモリ3bのパスワードレジスタ部に格納する(ステップS42)。そして続けて電子透かしを検出したこと示す

フラグを立てる(ステップS43)。

[0076] 次にステップS44においては、電子透かしにより埋め込まれていた情報が、コンテンツ配信装置1などの管理センターにより管理される再生禁止リスト(Revocation List)に入っているか否かをネットワーク経由で確認する。なお、この「再生禁止リスト(Revocation List)」は、ブラックリスト的な情報で、このリストには違法コピーされたコンテンツデータに埋め込まれたコンテンツIDとかかる情報コンテンツをダウンロードしたユーザーIDが記載されている。なお、違法コピーされた情報コンテンツが再生されるとかかるコンテンツIDとユーザーIDは管理センターに送信され、これを受けて再生禁止リストが逐次更新される。

[0077] そしてステップS44において、再生しようとするコンテンツデータに電子透かしとして埋め込まれた識別情報が再生禁止リストに登録されていた場合、この埋め込まれていた識別情報をコンテンツ配信装置1に送信する(ステップS50)。これにより、違法コピーされた情報コンテンツが何度再生されたのか把握することができる。なお、管理センターはコンテンツ配信業者が運営するコンテンツ配信装置1の他、多数のコンテンツ配信業者により設立された第三者機関であっても良い。さらにP2Pの技術が搭載された情報再生装置であれば、上述の管理センターへの識別情報の送信に加え、他の情報再生装置にこの識別情報を送信し、情報再生装置間で再生禁止リストを共有し、再生装置内に保存された再生禁止リストを用いてステップS44を確認するようにしてもよい。

[0078] 一方、電子透かしとして埋め込まれた識別情報が再生禁止リストに登録されていない場合、再生しようとするコンテンツデータに対する暗号化の有無をチェックする(ステップS45)。すなわち、再生しようとするコンテンツデータがCSS方式による暗号化がなされているかを確認し、暗号化が検出されればステップS46へ移行する。

[0079] 一方、このステップS45において暗号化が検出されなければ、ステップS44、Yesの場合と同様に電子透かしとして検出された識別情報を管理センターへ送信する(ステップS50)。なぜなら、このような情報コンテンツは違法に暗号化が解除され、情報記録媒体に複製された可能性が高いものであるので、今後の再生禁止を行うべく当該情報コンテンツに関する識別情報を外部へ通知することが好ましいからである。

- [0080] なお本実施例においては、コンテンツIDとユーザーIDの両方を用いて再生禁止リストを作成しているが、いずれか一方だけを用いて再生禁止リストを作成しても良い。
- [0081] 次に、ステップS45にて暗号化を検出した後、CPU3cは図示しないメモリを参照して電子透かしを検出したか否かのフラグを確認する(ステップS46)。上述のとおり、電子透かしは検出されているので当該フラグは「WM_FLG=1」である。
- [0082] そして当該フラグが「WM_FLG=1」の場合、CPU3cは、パスワードレジスタに格納されたパスワード(ユーザーIDの下4桁)を参照し、自動的にパスワードとして当該レジスタに保持されたパスワードを用いてパスワード入力処理を完了させる。
- [0083] パスワード入力処理が自動的に行われた後は、入力されたパスワードが正しいパスワードであるかチェックを行う(ステップS48)。なお、この場合のパスワード入力処理は、電子透かしにより検出されたユーザーIDの下4桁が機械的に処理されているので間違い可能性は低い。
- [0084] そしてパスワードのチェックを終えた後に、引き続いて情報コンテンツの再生を開始する(ステップS49)。これにより、ユーザーは、キーボードを用いてパスワードをいちいち入力する必要がなくなり、情報コンテンツの再生に関する利便性が向上する。
- [0085] なお、PC3のHDD3hにインストールされる情報再生プログラムや情報記録プログラム、また光ディスクドライブ3aにインストールされるファームウェアは、管理センターなどから逐次最新版のものをダウンロードして更新できるようにしても良い。この更新時、管理センターはダウンロードしようとするユーザーのユーザーIDが上述再生禁止リストに登録されていないか確認し、登録されている場合には、記録再生プログラムやファームウェアのダウンロードを禁止するようにしても良い。
- [0086] また、本実施例によれば、PC3により情報記録再生装置を構成したが、スタンドアローン型の家庭用DVDプレーヤーやレコーダであっても良い。
- [0087] また、本実施例においては、情報コンテンツは情報配信装置からネットワークを介して送信される例を示したが、本発明はこの電子配信の形態に限定されない。例えば情報コンテンツの配信側にて、識別情報が電子透かしとして埋め込まれた情報コンテンツを記録原盤に記録し、スタンプ等を用いて再生専用の情報記録媒体を大量生産し、それをエンドユーザーに有償又は無償で配布しても良い。

[0088] なお、情報再生装置がネットワークに接続されている場合、上記の実施例と同様にWMをチェックし、ネットワークを介して既に入手済みのリボケーションリストのデータをチェックし、WMで埋め込まれた識別情報が当該リボケーションリストにあれば、違法コピーコンテンツとして再生を許可しないようにしてもよい。また違法コピーコンテンツを検出した場合は、ネットワークに接続されている管理センターや、他の情報再生装置に識別情報を送付し、違法コピーコンテンツの蔓延を防止する。この際Peer to Peerの技術が導入されていれば、サーバーに送るだけでなく、接続されている機器間で直接違法コピーリストを送受信することができる。

[0089] また、PCを用いたネットワークプレーヤーは、常駐部と非常駐部からなり、常駐部で、再生機能が動作しないときにでも、違法コピーの監視を行い、発見したときは、ネットワークにつながっているときは、即座に、つながっていないときは、次につながったときに所定の場所あるいはネットワークにつながっているネットワークプレーヤーに情報を提供することが望ましい。

[0090] このように本実施例においては、電子透かし検出器を備える情報再生装置と、備えない情報再生装置とで再生制御フローが異なっている。電子透かし検出器を備えていない従来の情報再生装置であると、情報コンテンツの再生時にはパスワードをユーザーが入力する必要がある。一方、本実施例のように電子透かし検出機能を有する情報再生装置では、情報コンテンツの再生に際してパスワードをユーザーが入力する必要はない。よって、ユーザーはパスワード入力作業が軽減されることになる。また、加えて違法な複製が行われた情報記録媒体の再生を制限することができ、著作権者の保護が図れることになる。

なお、以上に示した実施例は、本発明を実施する最良の形態であるが、この形態に限定されるものではなく本発明の技術思想または趣旨を逸脱しない範囲で適宜変更可能であることは言うまでもない。

産業上の利用可能性

[0091] 本発明に係る情報配信装置、情報記録媒体、および情報再生装置は、例えば映画などの情報コンテンツを配信するコンテンツ配信装置、情報コンテンツが記録された情報記録媒体、かかる情報記録媒体を再生する情報再生装置に利用可能である

。また、例えば民生用或いは業務用の各種コンピュータ機器に搭載される又は各種コンピュータ機器に接続可能な情報配信装置及び情報再生装置等にも利用可能である。

請求の範囲

- [1] 識別情報を電子透かしによりコンテンツデータに埋め込む電子透かし埋め込み部と、
- 前記識別情報から生成可能なパスワードの入力を求めるルーチンを有するとともに前記コンテンツデータの再生制御を行う再生制御データを生成する再生制御情報生成部と、
- 前記識別情報が埋め込まれたコンテンツデータの少なくとも一部を暗号化する暗号化部と、
- 前記暗号化されたコンテンツデータと前記再生制御データとからなる情報コンテンツを生成する手段と、を有することを特徴とする情報生成装置。
- [2] 前記識別情報は、前記情報コンテンツの配信を要求するユーザーを識別するためのユーザーID、前記情報コンテンツを特定するためのコンテンツID、または前記情報コンテンツを記録媒体に記録する記録装置を識別するための記録装置IDの少なくとも一つを含むことを特徴とする請求の範囲第1項に記載の情報生成装置。
- [3] 前記識別情報は前記ユーザーIDであり、前記パスワードは前記ユーザーIDの少なくとも一部からなることを特徴とする請求の範囲第2項に記載の情報生成装置。
- [4] 請求の範囲第1項に記載の情報生成装置と、
- 前記情報コンテンツを配信する配信部と、を具備することを特徴とする情報配信装置。
- [5] 電子透かしにより識別情報が埋め込まれたコンテンツデータと、
- 前記識別情報から生成可能なパスワードの入力を求めるルーチンを有するとともに前記コンテンツデータの再生制御を行う再生制御データと、からなることを特徴とするデータ構造。
- [6] 請求の範囲第5項に記載のデータ構造からなる情報コンテンツが記録された情報記録媒体。
- [7] 請求の範囲第6項に記載の情報記録媒体を再生する情報再生装置であり、
- 前記コンテンツデータに前記電子透かしが埋め込まれているか否か検出する電子透かし検出部と、

前記コンテンツデータの少なくとも一部が暗号化されているか否かを検出する暗号化検出部と、

前記電子透かしが検出されたにも拘わらず、前記コンテンツデータが暗号化されていない場合、前記情報コンテンツの再生を禁止する再生制御部と、
を備えることを特徴とする情報再生装置。

[8] 前記電子透かしが検出されたにも拘わらず、前記コンテンツデータが暗号化されていない場合、前記識別情報を外部機器に送信する送信部を備えることを特徴とする請求の範囲第7項に記載の情報再生装置。

[9] 前記再生制御部は、前記電子透かしにより埋め込まれた前記識別情報が、前記送信された前記識別情報に基づき前記外部機器により生成された再生禁止リストに含まれる場合、前記情報コンテンツの再生を禁止することを特徴とする請求の範囲第7項に記載の情報再生装置。

[10] 請求の範囲第6項に記載の情報記録媒体を再生するための情報再生プログラムであり、

前記コンテンツデータに前記電子透かしが埋め込まれているか否か検出し、
前記コンテンツデータの少なくとも一部が暗号化されているか否かを検出し、
前記電子透かしが検出されたにも拘わらず、前記コンテンツデータが暗号化されていない場合、前記情報コンテンツの再生を禁止するようコンピュータを制御することを特徴とする情報再生プログラム。

[11] 情報コンテンツを記録媒体に記録する情報記録装置であり、

前記情報コンテンツは、コンテンツデータと、パスワードの入力を求めるルーチンを有するとともに前記コンテンツデータの再生制御を行う再生制御データと、からなり前記コンテンツデータの少なくとも一部が暗号化されており、

前記情報記録装置は、
前記パスワードを生成可能な識別情報を電子透かしとして生成する電子透かし生成部と、前記生成された前記電子透かしを前記コンテンツデータに埋め込む電子透かし埋め込み部と、を備えることを特徴とする情報記録装置。

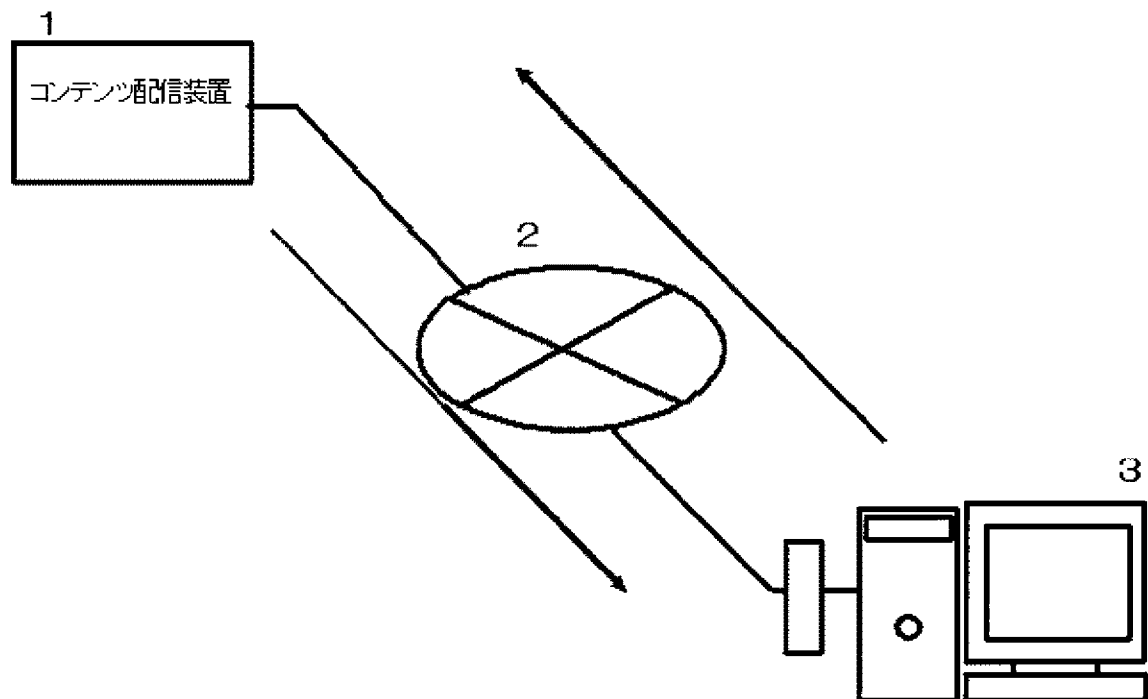
[12] 情報コンテンツを記録媒体に記録するための情報記録プログラムであり、

前記情報コンテンツは、コンテンツデータと、パスワードの入力を求めるルーチンを有するとともに前記コンテンツデータの再生制御を行う再生制御データと、からなり前記コンテンツデータの少なくとも一部が暗号化されており、

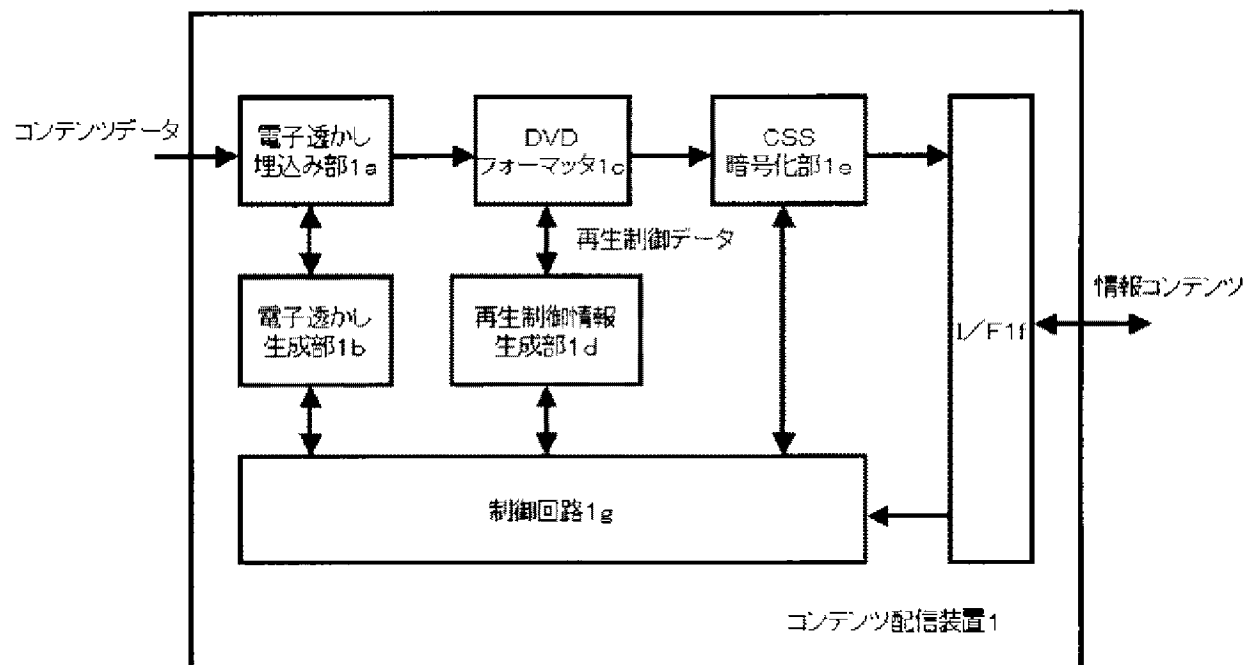
前記情報記録プログラムは、

前記パスワードを生成可能な識別情報を電子透かしとして生成し、
前記生成された前記電子透かしを前記コンテンツデータに埋め込むようコンピュータを制御することを特徴とする情報記録プログラム。

[図1]



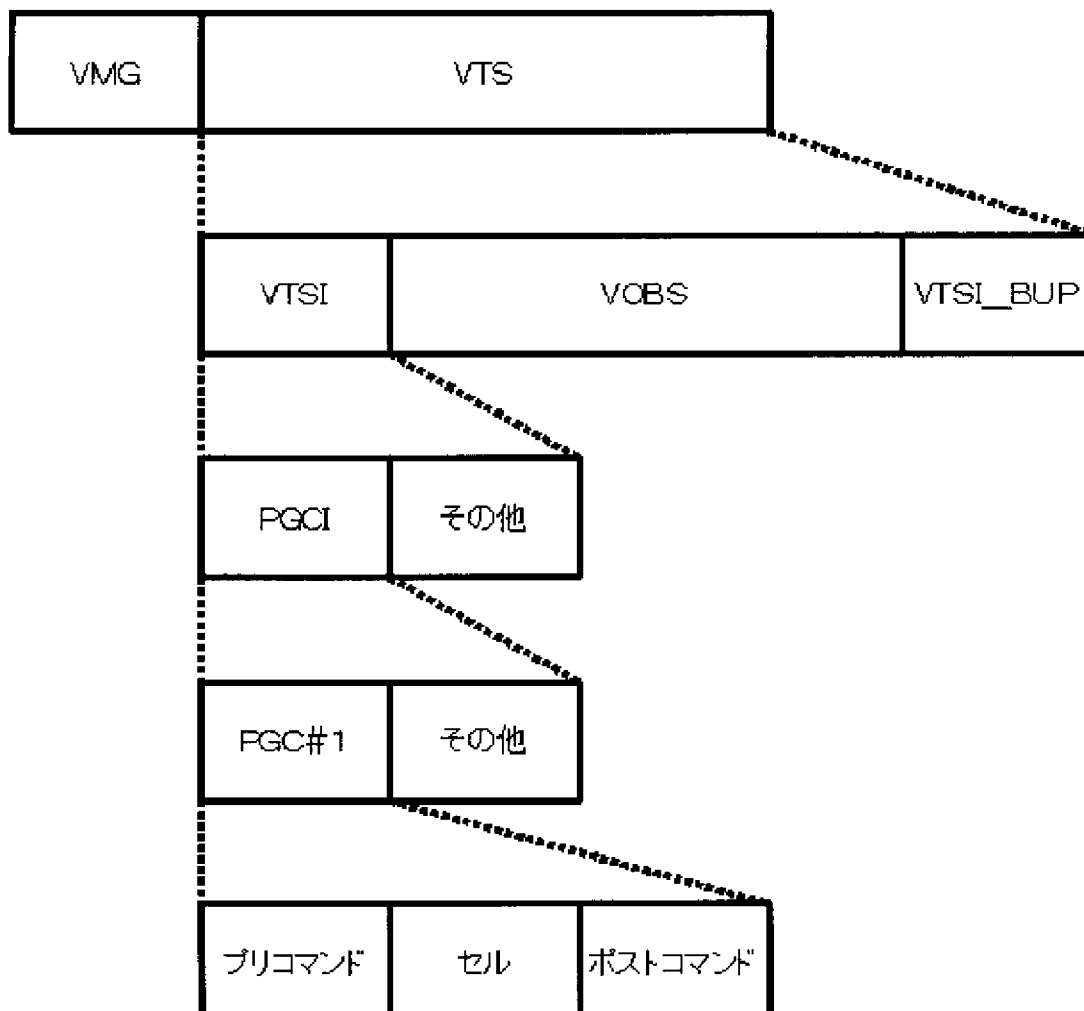
[図2]



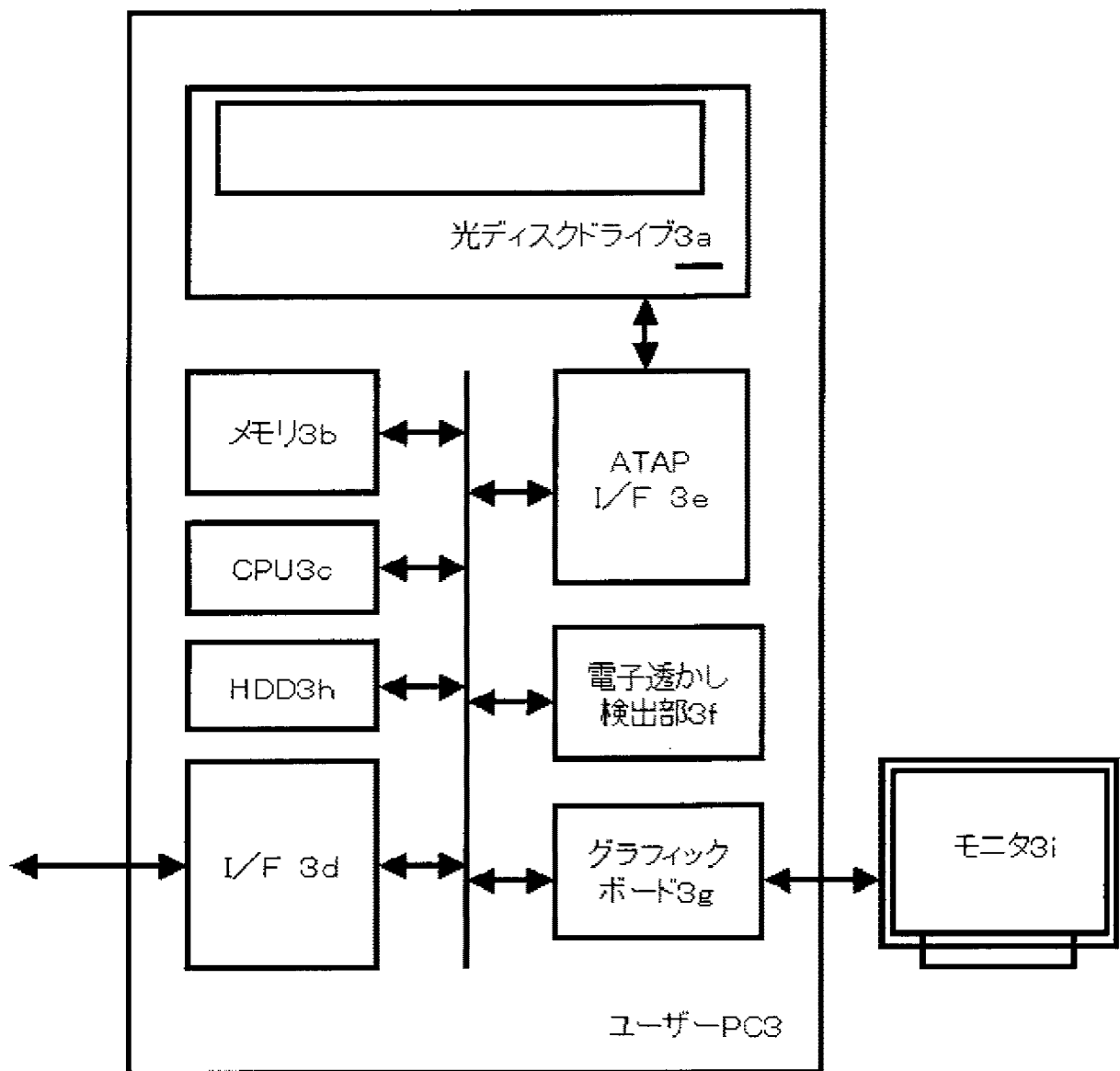
[図3]

バイト位置	内容
0	ヘッダ／制御情報
1-2	コンテンツID
3-4	ユーザーID
5	コピー制御情報
6-8	著作権情報
9-15	その他

[図4]

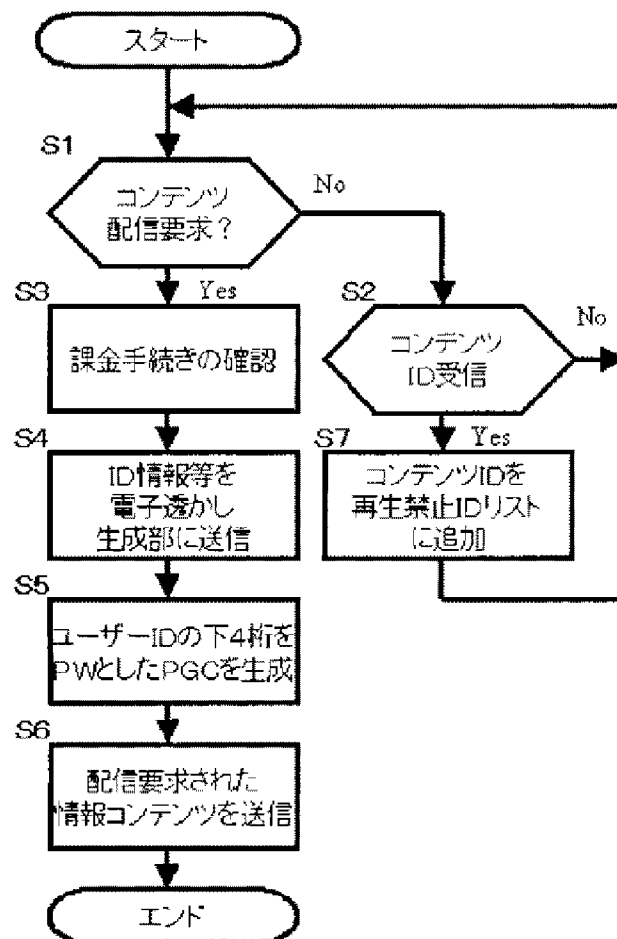


[図5]

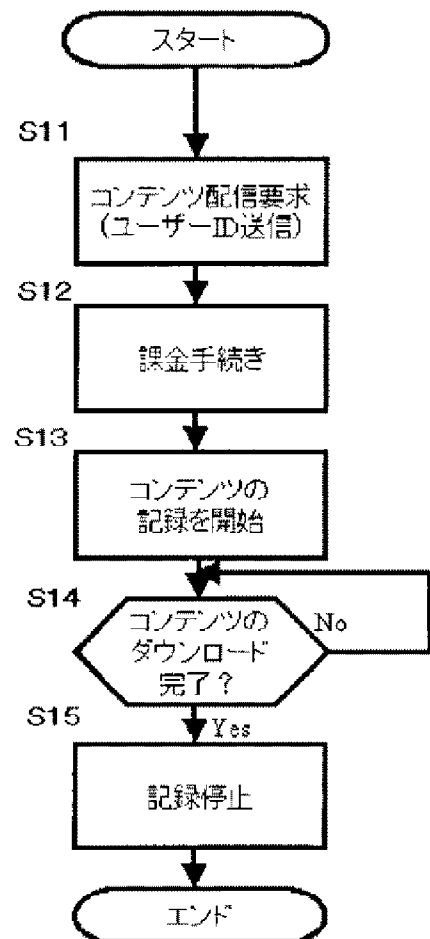


[図6]

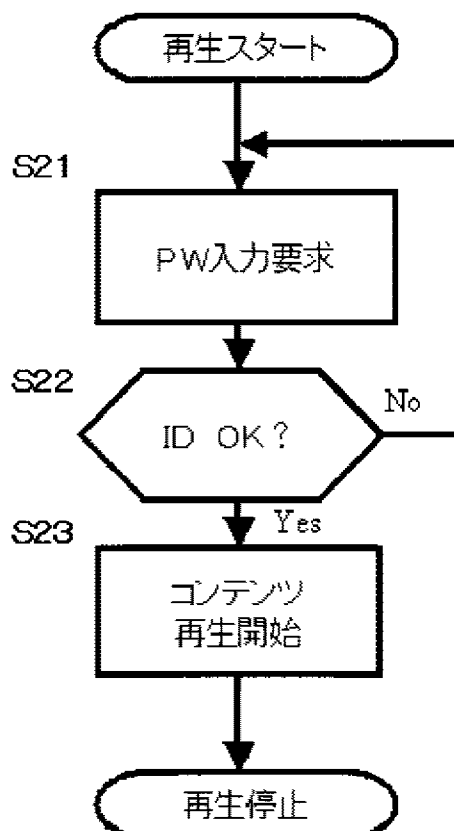
(a)



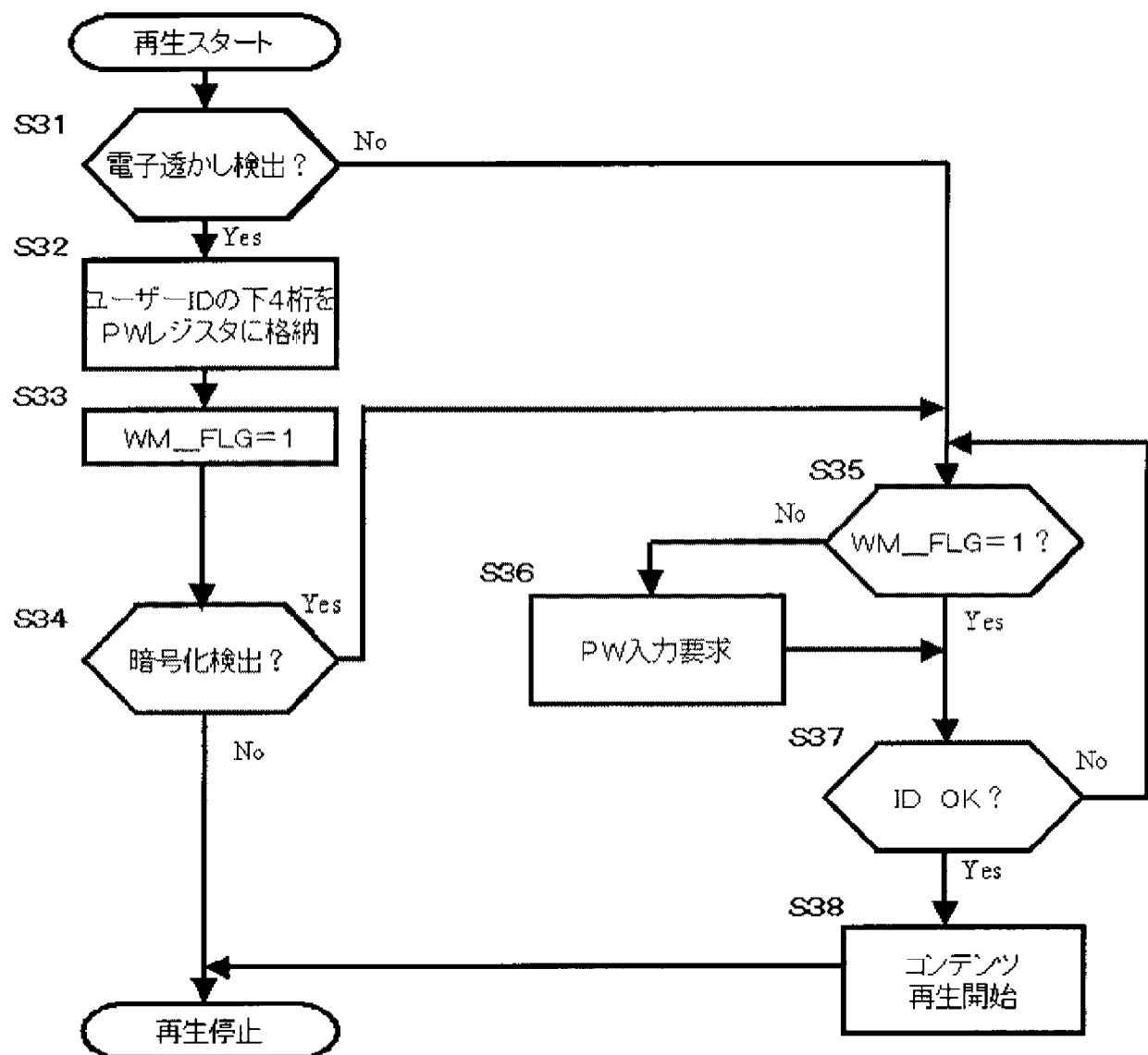
(b)



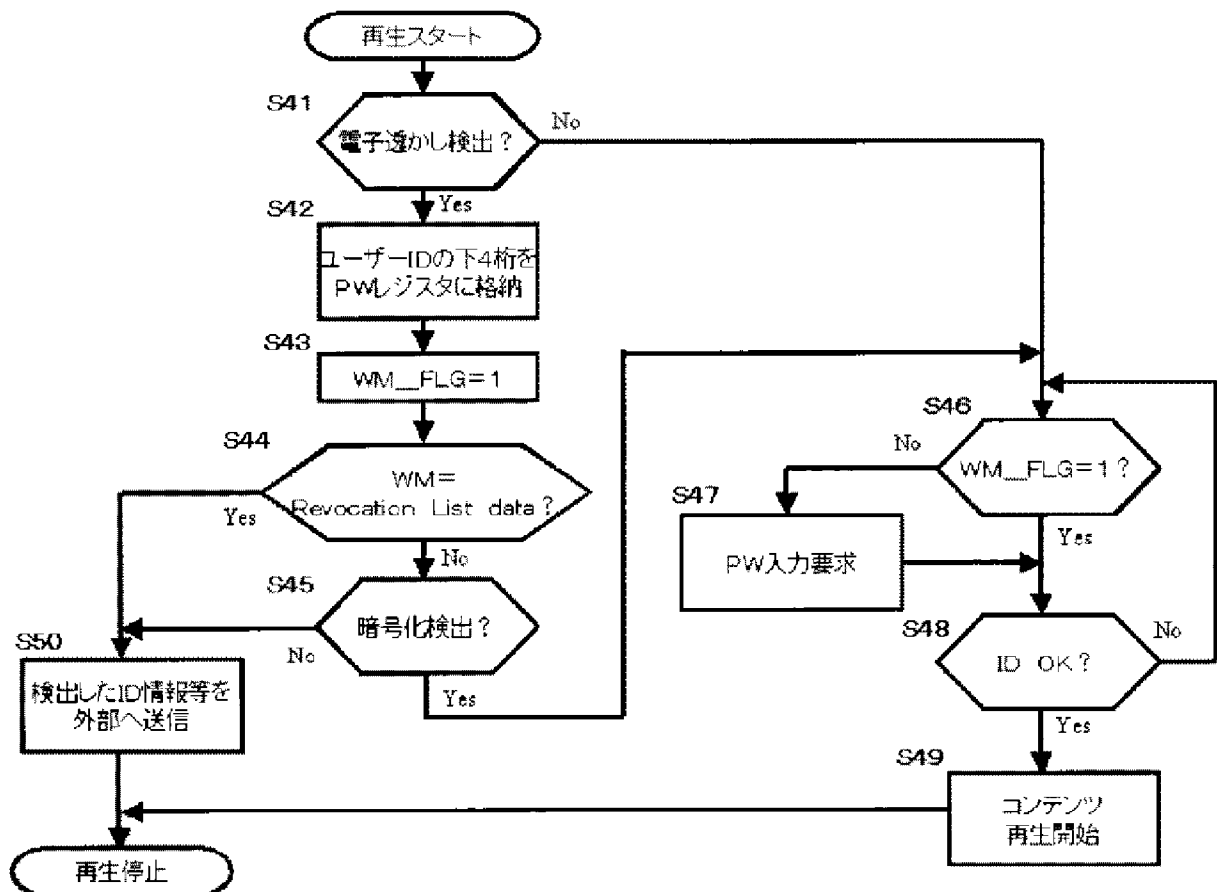
[図7]



[図8]



[図9]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2007/055655

A. CLASSIFICATION OF SUBJECT MATTER

G06F21/24(2006.01) i, G11B20/10(2006.01) i, H04N7/167(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)

G06F21/24, G11B20/10, H04N7/167

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 2001-184789 A (Taiyo Yuden Co., Ltd.), 06 July, 2001 (06.07.01), Par. Nos. [0061] to [0076], [0087] to [0101] (Family: none)	1-6, 11-12 7-10
Y	JP 2003-317378 A (Sony Corp.), 07 November, 2003 (07.11.03), Abstract & EP 1355308 A1 & US 2003/0231869 A1	7-10
A	JP 2001-325181 A (Nippon Telegraph And Telephone Corp.), 22 November, 2001 (22.11.01), Par. Nos. [0014] to [0019] (Family: none)	1-12



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
10 April, 2007 (10.04.07)

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/JP2007/055655

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2003-242042 A (Canon Inc.) , 29 August, 2003 (29.08.03) , Full text; all drawings (Family: none)	1-12

A. 発明の属する分野の分類（国際特許分類（I P C）） Int.Cl. G06F21/24(2006.01)i, G11B20/10(2006.01)i, H04N7/167(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. G06F21/24, G11B20/10, H04N7/167			
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	JP 2001-184789 A(太陽誘電株式会社) 2001.07.06, [0061]-[0076], [0087]-[0101] (ファミリーなし)	1-6, 11-12 7-10	
Y	JP 2003-317378 A (ソニー株式会社) 2003.11.07, [要約] & EP 1355308 A1 & US 2003/0231869 A1	7-10	
☒ 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 0 . 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		特許庁審査官（権限のある職員） 平井 誠 電話番号 0 3 - 3 5 8 1 - 1 1 0 1 内線 3 5 4 6	5 S 9 0 7 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
A	JP 2001-325181 A (日本電信電話株式会社) 2001. 11. 22, [0014]-[0019] (ファミリーなし)	1-12
A	JP 2003-242042 A (キヤノン株式会社) 2003. 08. 29, 全文, 全図 (フ ァミリーなし)	1-12