

(43) 国際公開日
2006 年 4 月 13 日 (13.04.2006)

PCT

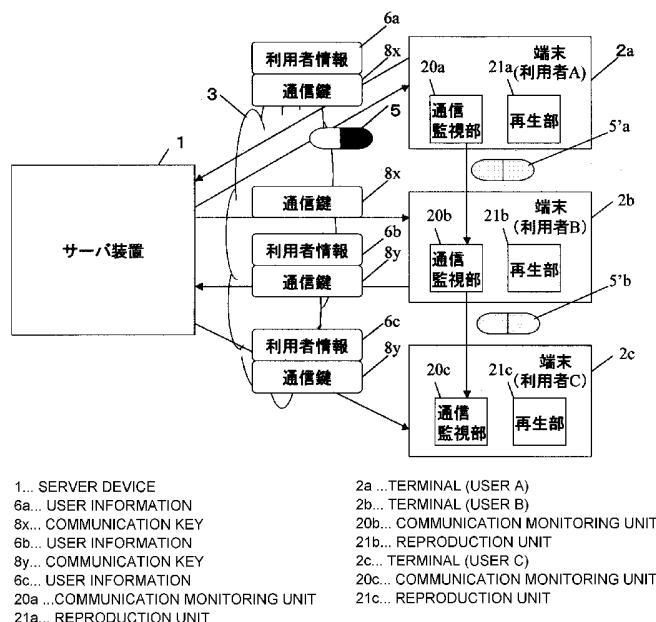
(10) 国際公開番号
WO 2006/038622 A1

- (51) 国際特許分類:
H04L 9/08 (2006.01)
- (21) 国際出願番号: PCT/JP2005/018362
- (22) 国際出願日: 2005 年 10 月 4 日 (04.10.2005)
- (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2004-294249 2004 年 10 月 6 日 (06.10.2004) JP
- (71) 出願人 (米国を除く全ての指定国について): 日本電気株式会社 (NEC CORPORATION) [JP/JP]; 〒1088001 東京都港区芝五丁目 7 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): 仁野 裕一 (NINO, Yuuichi) [JP/JP]; 〒1088001 東京都港区芝五丁目 7 番 1 号 日本電気株式会社内 Tokyo (JP).
- (74) 代理人: 宇高 克己 (UDAKA, Katsuki); 〒1010025 東京都千代田区神田佐久間町 1 - 1 4 第二東ビル 5 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, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.
- (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
— 補正書・説明書

/ 続葉有 /

(54) Title: CONTENT DISTRIBUTION SYSTEM

(54) 発明の名称: コンテンツ配信システム



(57) Abstract: There is provided a content distribution method which limits content distribution means to a particular distribution method and can trace the content distribution route in the distribution method without leak even when there is a user who does not reproduced the content. The content distribution system distributes a content from a server device after performing primary encryption. When distributing the content between terminals, the terminal as the transmission source registers an encryption key for performing communication encryption in the server device and the terminal as the destination acquires the encryption key into the server, so that the server device stores the content distribution route. Furthermore, when each of the terminals reproduces a content, it accesses the server device. When the server device has confirmed the flow to the terminal, it issues a content reproduction key.

/ 続葉有 /



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。

(57) 要約: コンテンツ配信手段を特定の流通方法に限定させ、その流通方法の中でコンテンツの流通経路を、途中でコンテンツを再生しない利用者がいても、漏れがないように追跡するコンテンツ配信方法を提供する。本発明のコンテンツ配信システムは、コンテンツをサーバ装置から配信するときは一次暗号化をして配信する。そして、コンテンツを端末間で流通させる際には、送信元の端末が通信暗号化をするための暗号鍵をサーバ装置に登録し、受信先の端末が暗号鍵をサーバに取得することによって、サーバ装置がコンテンツ流通経路を保存する。さらに、各端末がコンテンツを再生する際にはサーバ装置にアクセスし、サーバ装置がその端末へ流通されたのを確認した場合、コンテンツ再生鍵を発行する。

明 細 書

コンテンツ配信システム

技術分野

- [0001] 本発明はコンテンツ配信システム、方法およびプログラムに関し、特にコンテンツ配信経路を追跡(トレース)できるコンテンツ配信システム、方法およびプログラムに関する。

背景技術

- [0002] 近年、Napster、Gnutella、Winnyなど、コンテンツを個人－個人間で流通するようなピア・ツー・ピア(P2P)型の配信ソフトウェアが普及してきている。それに伴い、ユーザがコンテンツをコンテンツ配信サーバから直接ダウンロードするばかりではなく、ユーザ間で直接受け渡しをする機会も増えてきている。このようなP2P型ソフトを利用して、コンテンツがどのように配信されているかモニタリングすることは、どのようなユーザ層にコンテンツが嗜好されているか、どのようなユーザがそのコンテンツを気にいって周辺に紹介しているか把握することができ、マーケティングに非常に有用である。
- [0003] このようなコンテンツ流通状況を把握する方法として、特許文献1に記載されているコンテンツ配信システムが挙げられる。
- [0004] 図7に示すように、この従来のコンテンツ配信システムは、サーバ装置1と、端末2a、2b、2cとから構成されている。このサーバ装置1は、図8に示すように、利用者情報データベース10と、コンテンツデータベース11と、ウェブサーバ部12と、利用者情報管理部13と、暗号化部14と、コンテンツ流通状況分析部15から構成される。
- [0005] このような構成を有する従来のシステムはつぎのように動作する。
- [0006] すなわち、利用者情報データベース10は、図9に示すような利用者ID、端末ID、利用者情報、コンテンツ名、当該コンテンツを紹介した人、もしくは当該コンテンツを送信した人を示す推薦ID、コンテンツを再生するための再生プログラム名を格納する。また、コンテンツデータベース11は、配信するコンテンツとその再生プログラムを格納している。コンテンツ利用時には、そのコンテンツの利用者(ここでは図7の利用者Aとして説明する)は、自分の端末(端末2a)を用いて、自らの利用者情報6aを、ウェブサ

サーバ部12を通じて登録する。この利用者情報6aには少なくとも利用者ID(ID-A)、端末を特定するための端末ID、氏名・連絡先などの利用者情報、自分の欲しいコンテンツ名が含まれている。

[0007] 利用者情報管理部13は、これらの情報を利用者情報データベース10に保存する。

[0008] つぎに、暗号化部14は利用者Aから要求のあったコンテンツについて、利用者Aの利用者ID(ID-A)を埋め込んだ形(コンテンツ5)で端末2aに送信する。さらに、端末2aは、コンテンツを再生する再生プログラムをサーバ装置1に要求する。

[0009] すると、それを受けて、暗号化部14は利用者Aの利用者情報および少なくともコンテンツ名の情報とコンテンツの符号化列のいずれか一方に基づく暗号鍵によってコンテンツデータベース11内の再生プログラムを暗号化して再生プログラム7aを送信する。端末Aは、再生プログラム7aを利用者Aの利用者情報および少なくともコンテンツ名の情報とコンテンツの符号化列のいずれか一方に基づく復号鍵によって復号し、コンテンツを再生することができる。

[0010] つぎに、利用者Aは、そのコンテンツを利用者Bに紹介する場合は以下のように動作する。

[0011] まず、利用者Aは、ローカルコネクションもしくはP2Pファイル共有ソフトウェアなどを用いて、利用者Bの端末2bにコンテンツ5を送信する。

[0012] 端末2bはそのままではコンテンツ5を再生できないので、再生するための再生プログラムを取得するため、利用者Bに自らの利用者情報の情報をサーバ装置1に登録するように促す。そして、利用者Bは、ウェブサーバ12を通じて、利用者情報6bを登録する。利用者情報6bは、利用者情報6aの情報に加えて、コンテンツ5に埋め込まれている利用者ID(ID-A)をサーバ装置1に送信する。

[0013] サーバ装置1の利用者情報管理部13は、送信された利用者ID(ID-B)、端末ID、利用者情報、コンテンツ名に合わせて、推薦IDとしてID-Aを格納した形で保存する。

[0014] 暗号化部14は利用者Bの利用者情報および少なくともコンテンツ名の情報とコンテンツの符号化列のいずれか一方に基づく暗号鍵によってコンテンツデータベース11内の再生プログラムを暗号化して再生プログラム7bを送信する。

[0015] 端末2bは、再生プログラム7aを利用者Aの利用者情報および少なくともコンテンツ

名の情報とコンテンツの符号化列のいずれか一方に基づく復号鍵によって復号し、コンテンツを再生することができる。

- [0016] つぎに、利用者Bから利用者Cに紹介した場合も利用者Cがコンテンツを視聴する場合は前述した同様の手続きを行う。このとき、利用者情報データベースには、利用者Cの利用者ID(ID-C)の推薦IDがID-Aとなるように保存される。

特許文献1:特開2004-12866号公報

発明の開示

発明が解決しようとする課題

- [0017] 上記に示す従来の方法では、以下に示す問題が生じる。
- [0018] 第1の問題点は、図9に示すように、コンテンツが利用者A→利用者B→利用者Cと流通されているにも関わらず、利用者情報データベース10には利用者A→利用者B、利用者A→利用者Cという形でしか保存されていないため、真の流通経路を把握できないということである。
- [0019] その理由は、コンテンツを最初にダウンロードした利用者のIDをコンテンツに埋め込み、以降の流通ではこのIDをベースに紹介者がサーバに登録されるからである。
- [0020] 第2の問題点は、コンテンツを再生せずに別の利用者にコンテンツを渡した場合は、そのユーザ情報はサーバ装置に登録されないということである。したがって、当該コンテンツがどのようなユーザ層には受け入れられなかったかというマーケティング情報は収集することができない。
- [0021] その理由は、コンテンツを再生しなかった利用者は、再生プログラムを取得するために、サーバ装置1にアクセスにいかないためである。
- [0022] そこで、本発明の目的は上記問題点を鑑みて発明されたものであって、特定の流通方法によって流通したコンテンツの全ての流通経路を追跡できるコンテンツ配信システムを提供することにある。
- [0023] 本発明の他の目的は、コンテンツが再生されなくてもコンテンツ流通経路を追跡できるコンテンツ配信システムを提供することにある。
- [0024] 本発明のさらに他の目的は、コンテンツの流通を特定の流通方法に制限できるコンテンツ配信システムを提供することにある。

課題を解決するための手段

[0025] 上記課題を解決するための第1の発明は、
コンテンツを暗号化した暗号化コンテンツを配信する手段と、
前記暗号化コンテンツを復号するための再生鍵を保管する手段と、
前記暗号化コンテンツを端末間で送受信する際に、通信のための暗号鍵を生成し、この暗号鍵と、前記コンテンツのIDと、送信元端末IDと、送信先端末IDとをサーバに登録する手段と、
前記暗号鍵で暗号化コンテンツを二重に暗号化した二重暗号化コンテンツを前記送信先端末に送信する手段と、
前記二重暗号化コンテンツを受信後、前記コンテンツIDと送信先端末IDと送信元端末IDと共に前記暗号鍵の送信を要求する送信要求を送信する手段と、
前記登録されたコンテンツのID、送信元端末ID及び送信先端末IDと、前記送信要求と共に送信されたコンテンツID、送信先端末ID、及び送信元端末IDとを照合し、一致する場合、登録されている暗号鍵を前記送信先端末に対して送信する手段と、
前記登録されたコンテンツID、送信元端末ID、及び送信先の端末IDを保存する流通管理手段と、
前記コンテンツを再生するために、前記再生鍵の送信を要求する手段と、
前記再生鍵を要求した端末が前記流通管理手段に登録されている端末であれば、前記再生鍵を送信する再生鍵送信手段と
を備えたことを特徴とする。

[0026] 上記課題を解決するための第2の発明は、上記第1の発明において、
前記再生鍵送信手段は、前記流通管理手段に登録されている情報を参照して、再生鍵の送信を要求した端末の使用が過去に多くコンテンツを配信している場合、配信数に応じて値引きして課金する手段を含むことを特徴とする。

[0027] 上記課題を解決するための第3の発明は、
暗号化したコンテンツを配信するステップと、
前記暗号化コンテンツを復号するための再生鍵を保管するステップと、
前記暗号化コンテンツを端末間で送受信する際に、通信のための暗号鍵を生成し

、その暗号鍵と、前記コンテンツのID、送信元端末ID、送信先端末IDをサーバに登録するステップ、

前記送信端末が、前記暗号鍵で前記暗号化コンテンツを二重に暗号化した二重暗号化コンテンツを前記送信先端末に送信するステップと、

前記二重暗号化コンテンツ受信後、コンテンツID、送信先端末ID、送信元端末IDと共に、通信のための暗号鍵の送信要求をサーバに送信するステップと、

前記登録されたコンテンツのID、送信元端末ID及び送信先端末IDと、前記送信要求と共に送信されたコンテンツID、送信先端末ID、及び送信元端末IDとを照合し、一致する場合、登録されている暗号鍵を前記送信先端末に対して送信するステップと、

前記登録されたコンテンツID、送信元端末ID、及び送信先の端末IDを保存する流通管理ステップと、

前記コンテンツを再生するために、前記再生鍵の送信を要求するステップと、

前記再生鍵を要求した端末が前記流通管理手段で登録されている端末であれば、前記再生鍵を送信する再生鍵送信ステップと
を有することを特徴とする。

[0028] 上記課題を解決するための第4の発明は、上記第3の発明において、

前記再生鍵送信ステップは、

前記流通管理ステップで登録された情報を参照するステップと、

前記参照の結果、再生鍵の送信を要求した端末の使用が過去に多くコンテンツを配信している場合、配信数に応じて値引きして課金するステップと
を有することを特徴とする。

[0029] 上記課題を解決するための第5の発明は、

コンテンツを暗号化した暗号化コンテンツを配信する処理と、

前記暗号化コンテンツを復号するための再生鍵を保管する処理と、

前記暗号化コンテンツを端末間で送受信する際に、通信のための暗号鍵を生成し、この暗号鍵と、前記コンテンツのIDと、送信元端末IDと、送信先端末IDとをサーバに登録する処理と、

前記暗号鍵で暗号化コンテンツを二重に暗号化した二重暗号化コンテンツを前記

送信先端末に送信する処理と、

前記二重暗号化コンテンツを受信後、前記コンテンツIDと送信先端末IDと送信元端末IDと共に前記暗号鍵の送信を要求する送信要求を送信する処理と、

前記登録されたコンテンツのID、送信元端末ID及び送信先端末IDと、前記送信要求と共に送信されたコンテンツID、送信先端末ID、及び送信元端末IDとを照合し、一致する場合、登録されている暗号鍵を前記送信先端末に対して送信する処理と、

前記登録されたコンテンツID、送信元端末ID、及び送信先の端末IDを保存する流通管理処理と、

前記コンテンツを再生するために、前記再生鍵の送信を要求する処理と、

前記再生鍵を要求した端末が前記流通管理手段で登録されている端末であれば、前記再生鍵を送信する再生鍵送信処理と

をコンピュータに実行させるためのプログラムであることを特徴とする。

[0030] 上記課題を解決するための第6の発明は、上記第5の発明において、

前記再生鍵送信処理は、前記流通管理処理に登録されている情報を参照して、再生鍵を要求した端末の使用が過去に多くコンテンツを配信している場合、配信数に応じて値引きして課金する処理をコンピュータにさらに実行させることを特徴とする。

[0031] 上記課題を解決するための第7の発明は、

暗号化コンテンツを他の端末に送信する際に、通信鍵を生成し、この通信鍵と暗号化コンテンツのIDと送信元端末IDと送信先端末IDを送信する手段と、

前記通信鍵で、暗号化コンテンツを二重暗号化して二重暗号化コンテンツを生成する手段と、

前記二重暗号化コンテンツを送信する手段と、

前記二重暗号化コンテンツを受信する手段と、

前記通信鍵の送信要求を送信する際に、暗号化コンテンツIDと送信元端末IDと送信先端末IDとを送信する手段と、

前記通信鍵の送信要求に応じて送信された通信鍵を受信し、二重暗号化コンテンツを復号する手段と、

前記復号されたコンテンツを再生するための再生鍵の送信を要求する手段と、
前記再生鍵の送信要求に応じて送信された再生鍵を受信し、コンテンツを再生する手段と
を備えたことを特徴とする。

- [0032] 上記課題を解決するための第8の発明は、
暗号化コンテンツのIDとそれを復号するための再生鍵とを保管する手段と、
通信鍵と前記暗号化コンテンツIDと送信元端末IDと送信先端末IDとを送信元端末から受信する手段と、
通信鍵送信要求と前記暗号化コンテンツIDと送信元端末IDと送信先端末IDを送信先端末から受信する手段と、
前記2つの手段で受信したコンテンツID、送信元端末ID、送信先端末IDを照合し、一致した場合前記通信鍵を送信先端末に送信する手段と、
前記暗号化コンテンツID、送信元端末ID、送信先端末IDをデータベースに登録する手段と、
送信先端末から前記再生鍵の送信要求がきた際に、その端末が上記データベースに登録されているかどうかを確認し、登録されている場合、再生鍵を送信する再生鍵送信手段と
を備えたことを特徴とする。

- [0033] 上記課題を解決するための第9の発明は、上記第8の発明において、
前記再生鍵送信手段が上記データベースに登録されている情報を参照して、再生鍵を要求した端末の使用者が過去に多くコンテンツを配信している場合、配信数に応じて値引きして課金する手段を備えたことを特徴とする。

- [0034] 上記課題を解決するための第10の発明は、
コンテンツ配信システムであって、
コンテンツを送信する際にコンテンツを暗号化し、この暗号化コンテンツを復号するための暗号鍵を生成し、この暗号鍵と前記コンテンツを識別する識別情報と送信元の端末の識別情報と送信先の端末の識別情報とを登録する手段と、
前記暗号化されたコンテンツと前記コンテンツを識別する識別情報と送信元の端末

の識別情報とを送信先端末に送信する手段と、

受信した前記コンテンツの識別情報と、送信元の端末の識別情報及び送信先の端末の識別情報と、前記登録されているコンテンツの識別情報、送信元の端末の識別情報及び送信先の端末の識別情報とを照合し、一致している場合には前記暗号鍵を送信先の端末に送信する手段と

を有し、

前記登録されているコンテンツの識別情報、送信元の端末の識別情報及び送信先の端末の識別情報により流通経路を管理するように構成されていることを特徴とする

。

[0035] 上記課題を解決するための第11の発明は、端末であって、

コンテンツを送信する際にコンテンツを暗号化し、この暗号化コンテンツを復号するための暗号鍵を生成し、この暗号鍵と前記コンテンツを識別する識別情報と送信元の端末の識別情報と送信先の端末の識別情報とを送信する手段と、

前記暗号化されたコンテンツと前記コンテンツを識別する識別情報と送信元の端末の識別情報とを送信先端末に送信する手段と

を有し、

前記送信したコンテンツを識別する識別情報、送信元の端末の識別情報及び送信先の端末の識別情報により流通経路を登録するように構成されていることを特徴とする。

[0036] 上記課題を解決するための第12の発明は、サーバであって、

暗号化されたコンテンツを復号するための暗号鍵と、暗号化されたコンテンツの識別情報と、暗号化されたコンテンツを送信する送信元の端末の識別情報及び送信先の端末の識別情報とを受信する手段と、

前記暗号鍵の送信要求を受信した場合、暗号鍵の送信要求と共に送信されるコンテンツの識別情報、送信元の端末の識別情報及び送信先の端末の識別情報と、前記受信したコンテンツの識別情報、送信元の端末の識別情報及び送信先の端末の識別情報とを照合し、一致している場合には前記暗号鍵を送信する手段と

を有し、

前記受信したコンテンツの識別情報、送信元の端末の識別情報及び送信先の端末の識別情報により流通経路を記録するように構成されていることを特徴とする。

- [0037] 上記課題を解決するための第13の発明は、コンテンツ配信方法であって、
コンテンツを送信する際にコンテンツを暗号化するステップと、
前記暗号化コンテンツを復号するための暗号鍵を生成するステップと、
前記暗号鍵と前記コンテンツを識別する識別情報と送信元の端末の識別情報と送信先の端末の識別情報とを登録するステップと、
前記暗号化されたコンテンツと前記コンテンツを識別する識別情報と前記送信元の端末の識別情報とを送信先端末に送信するステップと、
受信した前記コンテンツの識別情報と、送信元の端末の識別情報及び送信先の端末の識別情報と、前記登録されているコンテンツの識別情報、送信元の端末の識別情報及び送信先の端末の識別情報とを照合し、一致している場合には前記暗号鍵を送信先の端末に送信するステップと
を有することを特徴とする。

- [0038] 上記課題を解決するための第14の発明は、端末のプログラムであって、
前記プログラムは前記端末を、
コンテンツを送信する際にコンテンツを暗号化し、この暗号化コンテンツを復号するための暗号鍵を生成し、この暗号鍵と前記コンテンツを識別する識別情報と送信元の端末の識別情報と送信先の端末の識別情報とを送信する手段と、
前記暗号化されたコンテンツと前記コンテンツを識別する識別情報と送信元の端末の識別情報とを送信先端末に送信する手段と
して機能させることを特徴とする。

- [0039] 上記課題を解決するための第15の発明は、
サーバのプログラムであって、
暗号化されたコンテンツを復号するための暗号鍵と、暗号化されたコンテンツの識別情報と、暗号化されたコンテンツを送信する送信元の端末の識別情報及び送信先の端末の識別情報とを受信する手段と、
前記暗号鍵の送信要求を受信した場合、暗号鍵の送信要求と共に送信されるコン

テンツの識別情報、送信元の端末の識別情報及び送信先の端末の識別情報と、前記受信したコンテンツの識別情報、送信元の端末の識別情報及び送信先の端末の識別情報とを照合し、一致している場合には前記暗号鍵を送信する手段として機能させることを特徴とする。

- [0040] このような構成を採用し、特定の流通方法でコンテンツを流通させるときには必ずサーバ装置にアクセスさせる、特定の流通方法以外で流通したコンテンツには再生鍵を送信しないようにすることにより本発明の目的を達成することができる。

発明の効果

- [0041] 本発明の第1の効果は、特定の流通方法によって流通したコンテンツの全ての流通経路を追跡できることにある。
- [0042] その理由は、特定の流通方法でコンテンツを流通させるときには通信用の暗号鍵を取得するために必ずサーバ装置にアクセスさせるためである。
- [0043] 本発明の第2の効果は、コンテンツが再生されなくてもコンテンツ流通経路を追跡できることにある。
- [0044] その理由は、本手法ではコンテンツ再生時以外にも流通時にサーバ装置にアクセスさせるためである。
- [0045] 本発明の第3の効果は、コンテンツの流通を特定の流通方法に制限できるコンテンツ配信システムを提供することにある。
- [0046] その理由は、コンテンツがメモ리카ード受け渡しなど特定の流通方法以外で流通された場合コンテンツの再生や利用を不可することができるためである。

図面の簡単な説明

- [0047] [図1]本発明の第1の発明を実施するための最良の形態の構成を示すブロック図である。
- [図2]本発明のサーバ装置1の最良の形態の構成を示すブロック図である。
- [図3]本発明の利用者情報データベース10の最良の形態のスキーマを示す図である。
- [図4]本発明の流通管理データベース18の最良の形態のスキーマを示す図である。
- [図5]第1の発明を実施するための最良の形態の動作を示すフローチャートである。

[図6]本発明の第2の発明を実施するための最良の形態の構成を示すブロック図である。

[図7]特許文献1の発明を実施するための最良の形態の構成を示すブロック図である。

[図8]特許文献1の発明のサーバ装置1の最良の形態の構成を示すブロック図である。

[図9]特許文献1の発明の利用者情報データベース10の最良の形態のスキーマを示す図である。

符号の説明

[0048]	1	サーバ装置
	2、2a、2b、2c	端末
	3	ネットワーク
	4	再生鍵
	5、5'a、5'b	暗号化コンテンツ
	6、6a、6b、6c	利用者情報
	7、7a、7b、7c	再生プログラム
	8、8x、8y	通信鍵
	10	利用者情報データベース
	11	コンテンツデータベース
	12	ウェブサーバ部
	13	利用者情報管理部
	14	暗号化部
	15	コンテンツ流通状況分析部
	16	流通管理部
	17	再生管理部
	18	流通管理データベース
	20、20a、20b、20c	通信監視部
	21、21a、21b、21c	再生部

発明を実施するための最良の形態

- [0049] 本発明のコンテンツ配信システムは、コンテンツをサーバ装置から配信するときは一次暗号化をして配信する。そして、このコンテンツを端末間で流通させる際には、送信元の端末が通信暗号化をするための暗号鍵をサーバ装置に登録し、この暗号鍵で次暗号化したコンテンツを送信先の端末に送信する。そして、送信先の端末が暗号鍵をサーバから取得するためにアクセスすることによって、サーバ装置がコンテンツ流通経路を保存する。さらに、各端末がコンテンツを再生する際にはサーバ装置にアクセスし、サーバ装置がその端末へ流通されたのを確認した場合、コンテンツ再生鍵を発行する。
- [0050] 本発明の第1の実施の形態について図面を参照して詳細に説明する。
- [0051] 図1を参照すると、本発明の第1の実施の形態は、プログラム制御により動作するサーバ装置1と端末2(図1では説明の便宜上2a,2b,2cと3つ示したがすべて同じ機能を持つ)から構成されている。
- [0052] サーバ装置1は、図2に示すように、利用者情報データベース10と、コンテンツデータベース11と、ウェブサーバ部12と、利用者情報管理部13と、コンテンツ流通情報分析部15と、流通管理部16と、再生管理部17と、流通管理データベース18とを含む。
- [0053] また、端末2は、通信監視部20(図1では説明の便宜上20a,20b,20cと3つ示したがすべて同じ機能を持つ)と、再生部21(図1では説明の便宜上21a,21b,21cと3つ示したがすべて同じ機能を持つ)とを含む。
- [0054] これらの手段はそれぞれ概略つぎのように動作する。
- [0055] 利用者情報データベース10は、最小限の構成として図3に示すように、端末を特定するためのID(端末ID)と端末を所持する利用者に関する情報(利用者情報)を格納している。この端末IDには、端末を特定するためのシリアル番号、IPアドレス、MACアドレスやそれらのハッシュ値などの符号化列によって各端末にユニークに算出できるものが利用できる。また、各端末の通信監視部や再生部にユニークに割り振られたIDを利用してもよい。利用者情報とは、利用者IDの他に、氏名や、年齢・住所・連絡先・生年月日・職業などのユーザの属性情報、嗜好情報なども含むことができる。

- [0056] コンテンツデータベース11は、最小限の構成として、コンテンツIDをキーにして、暗号化コンテンツ5と、それを復号するための再生鍵4が格納されている。さらに、コンテンツプロバイダからの要求に応じてコンテンツを再生するための利用権利情報も必要に応じて追加することができる。その上、再生鍵4や利用権利情報が付随された再生鍵4を売買する場合にはその価格なども必要に応じて追加することができる。コンテンツIDは、コンテンツを特定するためのコンテンツに対してユニークに割り当てたIDで、サーバ装置1が各コンテンツに対して割り当ててもよいし、暗号化コンテンツ5のデータのハッシュ値などから算出する形態をとってもよい。暗号化コンテンツ5はコンテンツを暗号化したデータに加えて、サーバ装置1にアクセスするためのURL、作者などの著作権情報、またサーバ装置がコンテンツIDを割り当てる場合はコンテンツIDが付加されていてもよい。
- [0057] 流通管理データベース18は、最小限の構成として図4に示すように、コンテンツID、コンテンツを送信した端末ID(送信端末ID)、受信した端末ID(受信端末ID)を格納している。これ以外に、送受信に成功したかどうかのステータス情報や送受信時刻なども含むことができる。
- [0058] 利用者情報管理部13は、利用者情報データベース10のデータの登録・削除などを行う。
- [0059] ウェブサーバ部12は利用者情報の登録・削除情報の通信、コンテンツプロバイダからの暗号化コンテンツと再生鍵および必要に応じて利用条件情報の登録を行う。
- [0060] 流通管理部16は、端末2から暗号化コンテンツの取得要求があった場合、端末2へ送信すると同時に、コンテンツID、送信端末ID、受信端末IDなどの情報を保存する。さらに、端末2の通信監視部20から送信されるOne Timeの通信鍵8(図1では説明の便宜上8x,8yとして示したが、データフォーマットは同じ)を、コンテンツ受信端末の通信監視部20から要求されるまで一時的に保管し、コンテンツ受信端末の通信監視部20に通信鍵8を送信した時点もしくは通信に失敗した時点で、流通管理データベースにコンテンツID、送信端末ID、受信端末IDなどの情報を保存する。尚、One Timeの通信鍵とは、通信鍵の内容が毎回異なる通信鍵であることを示す。
- [0061] 再生管理部17は、端末2の再生部21から再生鍵4の要求があった際に、その端末

が流通管理データベースに登録されている端末かどうか確認し、登録されていれば再生鍵4を送信する。なお、利用条件情報がコンテンツに付加されている場合は、再生鍵4に利用条件情報を添付して端末2の再生部21に送信する。

[0062] 通信監視部20は、端末間でコンテンツを通信する際に、送信側の通信監視部20はOne Timeの通信鍵8を生成して、流通管理部16に登録し、その通信鍵8で暗号化コンテンツ5を二重暗号化して(図1では5'a、5'bとして示した)送信する。受信側の通信監視部20は、通信鍵8を流通管理部16に要求し、通信鍵8が返信されると二重暗号化されたコンテンツを復号する。尚、本実施の形態では、通信監視部20が構成されている場合を用いて説明するが、通信監視部20が構成されていない場合であってもよい。

[0063] 再生部21は、暗号化コンテンツ5を再生する際に、再生管理部17に再生鍵4を要求し、再生鍵4が返信されると暗号化コンテンツ5を復号して再生する。再生鍵4を受信する際にあわせて利用条件情報を取得した場合は、この利用条件の下でコンテンツを再生する。この再生部21は、あらかじめ端末2にインストールされていてもよいし、コンテンツを再生する際に、サーバ装置1からダウンロードするのでもよい。

[0064] コンテンツ流通状況分析部15は、利用者情報データベース10と流通管理データベース18のテーブル情報に基づいて、当該コンテンツを多く配信している利用者、当該コンテンツを受信しても再生しない利用者、P2Pネットワークの中で配信に貢献しているユーザなどを検索するものである。

[0065] 次に、図1、図2、図5を参照して本実施の形態の全体の動作について詳細に説明する。

[0066] まず、コンテンツプロバイダが、暗号化コンテンツ5とその再生鍵4、必要に応じてその利用条件情報やその価格を、ウェブサーバ部12を通じて、コンテンツデータベースに登録する。このとき、コンテンツプロバイダが自分の保有するコンテンツの暗号化ツールを利用して、暗号化してもよいし、サーバ装置1が再生鍵4生成とコンテンツ暗号化用のWebサービスをウェブサーバ部で提供し、コンテンツプロバイダに登録するような形態をとってもよい。また、このコンテンツプロバイダは、一般的な有料コンテンツの事業者もあれば、端末2の利用者であることもありうる。コンテンツプロバイダが端

末2の利用者である場合は、上記の登録内容から暗号化コンテンツ5の代わりに、暗号化コンテンツ5のコンテンツIDを登録しても良い。

[0067] つぎに、利用者は、最初の起動時に、ウェブサーバ部12を通じて端末ID(説明の便宜上、図1の端末2a,2b,2cの各端末IDをID-A,ID-B,ID-Cとする)と利用者情報6(説明の便宜上、図1の端末2a,2b,2cの各利用者情報を6a,6b,6cとする)を入力する。

[0068] 入力された情報は、利用者情報管理部13によって利用者情報データベース10に入力される。(この場合の利用者情報データベースのスキーマ例を図3に示す。)

つぎに、暗号化コンテンツ5をサーバ装置1から端末2a、2b、2cに流通する場合を例に挙げて動作を説明する。

[0069] まず、端末2aから流通管理部16に暗号化コンテンツ5の取得要求を行う。流通管理部16は要求された暗号化コンテンツ5をコンテンツデータベースから検索して送信し、流通管理データベースに送信されたコンテンツID(説明の便宜上、ID-1とする)、送信端末IDとしてサーバ装置1の端末ID(説明の便宜上、ID-Serverとする)、受信端末IDを端末2aの端末ID(ID-A)を記録する。端末2aでコンテンツを再生する場合は、再生部21aがコンテンツIDがID-1である暗号化コンテンツの再生鍵の取得要求とID-Aを再生管理部17に送信する。

[0070] 再生管理部17は流通管理データベース18にアクセスし、ID-Aがサーバからダウンロードされた端末であることを確認し、ID-1に対応する再生鍵4を取得し、再生部21aに返信する。

[0071] 再生部21aはこの再生鍵4を利用して暗号化コンテンツ5を復号し、再生する。

[0072] つぎに、端末2aから端末2bに送信する場合の処理の流れについて、図5を利用して詳細に説明する。

[0073] まず、端末2bの通信管理部20bは暗号化コンテンツ5の取得要求と、自らの端末ID(ID-B)を端末2aへ送信する(図5のステップA1)。

[0074] 次に、端末2aの通信管理部20aはOne Timeの通信鍵を生成し、コンテンツの二重暗号化を行う(ステップA2)。

[0075] さらに、通信管理部20aは、この通信鍵と、暗号化コンテンツのコンテンツID(ID-1)、ID-A、ID-Bを流通管理部16に送信する。(ステップA3)。

- [0076] そして、流通管理部16が受領確認を通信管理部20aに送信すると(ステップA4)、通信管理部20aはステップA2で二重暗号化されたコンテンツ5'aを通信管理部20bに送信する。また、この時点で通信管理部20bは端末2aの端末IDを知らない場合はID-Aも合わせて送信する(ステップA5)。
- [0077] その後、通信管理部20bは、二重暗号化されたコンテンツ5'aを復号するため、通信鍵取得要求と、ID-1、ID-A、ID-Bを流通管理部16に送信する(ステップA6)。
- [0078] 流通管理部16は、ステップA3とステップA6で送信されたコンテンツID、送信端末ID、受信端末IDが同一であるか照合し(ステップA7)、同一であれば通信鍵を送信する。同一でなければエラーを送信する(ステップA8)。
- [0079] 通信管理部20bは通信鍵を受信すると、二重暗号化されたコンテンツを復号し(ステップA9)、復号が成功したかどうかのstatusを流通管理部16に送信する(ステップA10)。
- [0080] 流通管理部16は、statusを受信すると、受領確認を通信管理部20bに送信し(ステップA11)、流通管理データベース18にID-1、ID-A、ID-Bを書き込む。また、必要に応じてstatusも書き込む(ステップA12)。
- [0081] 以下、端末2bでコンテンツを再生する場合も端末2aと同じ処理が行われる。また、端末2bから端末2cへコンテンツが流通する場合も、端末2aから端末2bに送信されるのと同じ処理を行うことによって、流通管理データベース18に、ID-1、ID-A、ID-Bが書き込まれる。(書き込まれた例を図4に示す。)
- ここで、端末2bから端末2cへの暗号化コンテンツ5(ID-1)の送受信がメモリカード渡しなど別な手段で行われた場合について説明する。
- [0082] この場合、流通管理データベース18には、図4に示した4行目の情報が書き込まれていない状態になっている。このとき、端末2cの再生部21cが再生鍵の取得要求を行ったとき、再生管理部17は流通管理データベース18を参照して、ID-1はID-Cの端末に送信された履歴が残っていないので、再生鍵4を送信せず、エラーを送信する。
- [0083] 次に、本実施の形態の効果について説明する。
- [0084] 本実施の形態では、特定の流通方法でコンテンツを流通させるときには通信用の暗号鍵を取得するために必ずサーバ装置にアクセスさせるように構成されているため

、特定の流通方法によって流通したコンテンツの全ての流通経路を追跡できる。

[0085] また、本実施の形態では、さらに、コンテンツ再生時以外にも流通時にサーバ装置にアクセスさせるように構成されているため、コンテンツが再生されなくてもコンテンツ流通経路を追跡できる。

[0086] 最後に、本実施の形態では、コンテンツがメモリカード受け渡しなど特定の流通方法以外で流通された場合コンテンツを利用不可することができるように構成されているため、コンテンツの流通を特定の流通方法に制限できる。

[0087] 次に、本発明の第2の発明を実施するための最良の形態について図面を参照して詳細に説明する。

[0088] 図6を参照すると、本発明の第2の発明を実施するための最良の形態は、第1の発明を実施するための最良の形態に比べて、再生管理部17が、再生鍵4を送信する前に課金できる機能と、コンテンツ流通状況分析部15の分析結果を参照できることが異なる。また、コンテンツデータベース11には、再生鍵4もしくは利用条件情報付きの再生鍵4の価格が必ず格納されている。

[0089] 以下、第1の発明の実施の形態と異なる動作についてのみ説明する。

[0090] 再生管理部17は、端末2の再生部20から暗号化コンテンツ5の再生鍵4の取得要求があった際に、再生鍵4が有料である場合には端末2の利用者に対して課金処理を行う。課金処理を行う際には、コンテンツ流通状況分析部15にアクセスし、その利用者の過去のコンテンツ配信数を取得する。そして、このコンテンツ配信数に応じた値引きを行う。最後に、利用者による支払いが完了したときに、再生鍵4を再生部20に送信する。

[0091] 次に、本実施の形態の効果について説明する。

[0092] 本発明を実施するための最良の形態では、コンテンツを多く配信した利用者には再生鍵配布の際に値引きを行うように構成されているため、端末間でのコンテンツ配信方法がP2Pソフトウェアを利用するような形態である場合、各利用者が配信数を増やすために長時間電源をonにするような効果が期待でき、安定したP2Pネットワークを構成することができる。

[0093] 本発明によれば、コンテンツをP2Pネットワークで配信して、その人気度を収集する

マーケティングといった用途に適用できる。

[0094] また、多くコンテンツを配信するユーザには、キャッシュバックなど何らかのインセンティブを付与することによってP2Pネットワークの安定性を高めるといった用途にも適用可能である。

請求の範囲

- [1] コンテンツを暗号化した暗号化コンテンツを配信する手段と、
前記暗号化コンテンツを復号するための再生鍵を保管する手段と、
前記暗号化コンテンツを端末間で送受信する際に、通信のための暗号鍵を生成し、この暗号鍵と、前記コンテンツのIDと、送信元端末IDと、送信先端末IDとをサーバに登録する手段と、
前記暗号鍵で暗号化コンテンツを二重に暗号化した二重暗号化コンテンツを前記送信先端末に送信する手段と、
前記二重暗号化コンテンツを受信後、前記コンテンツIDと送信先端末IDと送信元端末IDと共に前記暗号鍵の送信を要求する送信要求を送信する手段と、
前記登録されたコンテンツのID、送信元端末ID及び送信先端末IDと、前記送信要求と共に送信されたコンテンツID、送信先端末ID、及び送信元端末IDとを照合し、一致する場合、登録されている暗号鍵を前記送信先端末に対して送信する手段と、
前記登録されたコンテンツID、送信元端末ID、及び送信先の端末IDを保存する流通管理手段と、
前記コンテンツを再生するために、前記再生鍵の送信を要求する手段と、
前記再生鍵を要求した端末が前記流通管理手段で登録されている端末であれば、前記再生鍵を送信する再生鍵送信手段と
を備えたことを特徴とするコンテンツ配信システム。
- [2] 前記再生鍵送信手段は、前記流通管理手段に登録されている情報を参照して、再生鍵の送信を要求した端末の利用者が過去に多くコンテンツを配信している場合、配信数に応じて値引きして課金する手段を含むことを特徴とする請求項1に記載のコンテンツ配信システム。
- [3] 暗号化したコンテンツを配信するステップと、
前記暗号化コンテンツを復号するための再生鍵を保管するステップと、
前記暗号化コンテンツを端末間で送受信する際に、通信のための暗号鍵を生成し、その暗号鍵と、前記コンテンツのID、送信元端末ID、送信先端末IDをサーバに登録するステップ、

前記送信端末が、前記暗号鍵で前記暗号化コンテンツを二重に暗号化した二重暗号化コンテンツを前記送信先端末に送信するステップと、

前記二重暗号化コンテンツ受信後、コンテンツID、送信先端末ID、送信元端末IDと共に、通信のための暗号鍵の送信要求をサーバに送信するステップと、

前記登録されたコンテンツのID、送信元端末ID及び送信先端末IDと、前記送信要求と共に送信されたコンテンツID、送信先端末ID、及び送信元端末IDとを照合し、一致する場合、登録されている暗号鍵を前記送信先端末に対して送信するステップと、

前記登録されたコンテンツID、送信元端末ID、及び送信先の端末IDを保存する流通管理ステップと、

前記コンテンツを再生するために、前記再生鍵の送信を要求するステップと、

前記再生鍵を要求した端末が前記流通管理手段で登録されている端末であれば、前記再生鍵を送信する再生鍵送信ステップと
を有することを特徴とするコンテンツ配信方法。

[4] 前記再生鍵送信ステップは、

前記流通管理ステップで登録された情報を参照するステップと、

前記参照の結果、再生鍵の送信を要求した端末の使用者が過去に多くコンテンツを配信している場合、配信数に応じて値引きして課金するステップと
を有することを特徴とする請求項3に記載のコンテンツ配信方法。

[5] コンテンツを暗号化した暗号化コンテンツを配信する処理と、

前記暗号化コンテンツを復号するための再生鍵を保管する処理と、

前記暗号化コンテンツを端末間で送受信する際に、通信のための暗号鍵を生成し、この暗号鍵と、前記コンテンツのIDと、送信元端末IDと、送信先端末IDとをサーバに登録する処理と、

前記暗号鍵で暗号化コンテンツを二重に暗号化した二重暗号化コンテンツを前記送信先端末に送信する処理と、

前記二重暗号化コンテンツを受信後、前記コンテンツIDと送信先端末IDと送信元端末IDと共に前記暗号鍵の送信を要求する送信要求を送信する処理と、

前記登録されたコンテンツのID、送信元端末ID及び送信先端末IDと、前記送信要

求と共に送信されたコンテンツID、送信先端末ID、及び送信元端末IDとを照合し、一致する場合、登録されている暗号鍵を前記送信先端末に対して送信する処理と、

前記登録されたコンテンツID、送信元端末ID、及び送信先の端末IDを保存する流通管理処理と、

前記コンテンツを再生するために、前記再生鍵の送信を要求する処理と、

前記再生鍵を要求した端末が前記流通管理手段で登録されている端末であれば、前記再生鍵を送信する再生鍵送信処理と

をコンピュータに実行させるためのプログラム。

- [6] 前記再生鍵送信処理は、前記流通管理処理に登録されている情報を参照して、再生鍵を要求した端末の使用者が過去に多くコンテンツを配信している場合、配信数に応じて値引きして課金する処理をコンピュータにさらに実行させることを特徴とする請求項5に記載のプログラム。

- [7] 暗号化コンテンツを他の端末に送信する際に、通信鍵を生成し、この通信鍵と暗号化コンテンツのIDと送信元端末IDと送信先端末IDを送信する手段と、

前記通信鍵で、暗号化コンテンツを二重暗号化して二重暗号化コンテンツを生成する手段と、

前記二重暗号化コンテンツを送信する手段と、

前記二重暗号化コンテンツを受信する手段と、

前記通信鍵の送信要求を送信する際に、暗号化コンテンツIDと送信元端末IDと送信先端末IDとを送信する手段と、

前記通信鍵の送信要求に応じて送信された通信鍵を受信し、二重暗号化コンテンツを復号する手段と、

前記復号されたコンテンツを再生するための再生鍵の送信を要求する手段と、

前記再生鍵の送信要求に応じて送信された再生鍵を受信し、コンテンツを再生する手段と

を備えたことを特徴とする端末。

- [8] 暗号化コンテンツのIDとそれを復号するための再生鍵とを保管する手段と、通信鍵と前記暗号化コンテンツIDと送信元端末IDと送信先端末IDとを送信元端末

から受信する手段と、

通信鍵送信要求と前記暗号化コンテンツIDと送信元端末IDと送信先端末IDを送信先端末から受信する手段と、

前記2つの手段で受信したコンテンツID、送信元端末ID、送信先端末IDを照合し、一致した場合前記通信鍵を送信先端末に送信する手段と、

前記暗号化コンテンツID、送信元端末ID、送信先端末IDをデータベースに登録する手段と、

送信先端末から前記再生鍵の送信要求がきた際に、その端末が上記データベースに登録されているかどうか確認し、登録されている場合、再生鍵を送信する再生鍵送信手段と

を備えたことを特徴とするサーバ。

- [9] 前記再生鍵送信手段が上記データベースに登録されている情報を参照して、再生鍵を要求した端末の使用者が過去に多くコンテンツを配信している場合、配信数に応じて値引きして課金する手段を備えたことを特徴とする請求項8に記載のサーバ。

- [10] コンテンツ配信システムであって、

コンテンツを送信する際にコンテンツを暗号化し、この暗号化コンテンツを復号するための暗号鍵を生成し、この暗号鍵と前記コンテンツを識別する識別情報と送信元の端末の識別情報と送信先の端末の識別情報とを登録する手段と、

前記暗号化されたコンテンツと前記コンテンツを識別する識別情報と送信元の端末の識別情報とを送信先端末に送信する手段と、

受信した前記コンテンツの識別情報と、送信元の端末の識別情報及び送信先の端末の識別情報と、前記登録されているコンテンツの識別情報、送信元の端末の識別情報及び送信先の端末の識別情報とを照合し、一致している場合には前記暗号鍵を送信先の端末に送信する手段と

を有し、

前記登録されているコンテンツの識別情報、送信元の端末の識別情報及び送信先の端末の識別情報により流通経路を管理するように構成されていることを特徴とするコンテンツ配信システム。

- [11] 端末であって、
コンテンツを送信する際にコンテンツを暗号化し、この暗号化コンテンツを復号するための暗号鍵を生成し、この暗号鍵と前記コンテンツを識別する識別情報と送信元の端末の識別情報と送信先の端末の識別情報とを送信する手段と、
前記暗号化されたコンテンツと前記コンテンツを識別する識別情報と送信元の端末の識別情報とを送信先端末に送信する手段と
を有し、
前記送信したコンテンツを識別する識別情報、送信元の端末の識別情報及び送信先の端末の識別情報により流通経路を登録するように構成されていることを特徴とする端末。
- [12] サーバであって、
暗号化されたコンテンツを復号するための暗号鍵と、暗号化されたコンテンツの識別情報と、暗号化されたコンテンツを送信する送信元の端末の識別情報及び送信先の端末の識別情報とを受信する手段と、
前記暗号鍵の送信要求を受信した場合、暗号鍵の送信要求と共に送信されるコンテンツの識別情報、送信元の端末の識別情報及び送信先の端末の識別情報と、前記受信したコンテンツの識別情報、送信元の端末の識別情報及び送信先の端末の識別情報とを照合し、一致している場合には前記暗号鍵を送信する手段と
を有し、
前記受信したコンテンツの識別情報、送信元の端末の識別情報及び送信先の端末の識別情報により流通経路を記録するように構成されていることを特徴とするサーバ。
- [13] コンテンツ配信方法であって、
コンテンツを送信する際にコンテンツを暗号化するステップと、
前記暗号化コンテンツを復号するための暗号鍵を生成するステップと、
前記暗号鍵と前記コンテンツを識別する識別情報と送信元の端末の識別情報と送信先の端末の識別情報とを登録するステップと、
前記暗号化されたコンテンツと前記コンテンツを識別する識別情報と前記送信元の

端末の識別情報とを送信先端末に送信するステップと、

受信した前記コンテンツの識別情報と、送信元の端末の識別情報及び送信先の端末の識別情報と、前記登録されているコンテンツの識別情報、送信元の端末の識別情報及び送信先の端末の識別情報とを照合し、一致している場合には前記暗号鍵を送信先の端末に送信するステップと

を有することを特徴とするコンテンツ配信方法。

[14] 端末のプログラムであって、

前記プログラムは前記端末を、

コンテンツを送信する際にコンテンツを暗号化し、この暗号化コンテンツを復号するための暗号鍵を生成し、この暗号鍵と前記コンテンツを識別する識別情報と送信元の端末の識別情報と送信先の端末の識別情報とを送信する手段と、

前記暗号化されたコンテンツと前記コンテンツを識別する識別情報と送信元の端末の識別情報とを送信先端末に送信する手段と

して機能させることを特徴とするプログラム。

[15] サーバのプログラムであって、

暗号化されたコンテンツを復号するための暗号鍵と、暗号化されたコンテンツの識別情報と、暗号化されたコンテンツを送信する送信元の端末の識別情報及び送信先の端末の識別情報とを受信する手段と、

前記暗号鍵の送信要求を受信した場合、暗号鍵の送信要求と共に送信されるコンテンツの識別情報、送信元の端末の識別情報及び送信先の端末の識別情報と、前記受信したコンテンツの識別情報、送信元の端末の識別情報及び送信先の端末の識別情報とを照合し、一致している場合には前記暗号鍵を送信する手段と

して機能させることを特徴とするプログラム。

補正書の請求の範囲

[2006年2月14日(14.02.06)国際事務局受理：出願当初の請求の範囲
10-15は取り下げられた；他の請求の範囲は変更なし。]

- [1] コンテンツを暗号化した暗号化コンテンツを配信する手段と、
前記暗号化コンテンツを復号するための再生鍵を保管する手段と、
前記暗号化コンテンツを端末間で送受信する際に、通信のための暗号鍵を生成し、
この暗号鍵と、前記コンテンツの ID と、送信元端末 ID と、送信先端末 ID とをサーバに登録する手段と、
前記暗号鍵で暗号化コンテンツを二重に暗号化した二重暗号化コンテンツを前記送信先端末に送信する手段と、
前記二重暗号化コンテンツを受信後、前記コンテンツ ID と送信先端末 ID と送信元端末 ID と共に前記暗号鍵の送信を要求する送信要求を送信する手段と、
前記登録されたコンテンツの ID、送信元端末 ID 及び送信先端末 ID と、前記送信要求と共に送信されたコンテンツ ID、送信先端末 ID、及び送信元端末 ID とを照合し、一致する場合、登録されている暗号鍵を前記送信先端末に対して送信する手段と、
前記登録されたコンテンツ ID、送信元端末 ID、及び送信先の端末 ID を保存する流通管理手段と、
前記コンテンツを再生するために、前記再生鍵の送信を要求する手段と、
前記再生鍵を要求した端末が前記流通管理手段で登録されている端末であれば、前記再生鍵を送信する再生鍵送信手段と
を備えたことを特徴とするコンテンツ配信システム。
- [2] 前記再生鍵送信手段は、前記流通管理手段に登録されている情報を参照して、再生鍵の送信を要求した端末の利用者が過去に多くコンテンツを配信している場合、配信数に応じて値引きして課金する手段を含むことを特徴とする請求項1に記載のコンテンツ配信システム。
- [3] 暗号化したコンテンツを配信するステップと、
前記暗号化コンテンツを復号するための再生鍵を保管するステップと、
前記暗号化コンテンツを端末間で送受信する際に、通信のための暗号鍵を生成し、その暗号鍵と、前記コンテンツの ID、送信元端末 ID、送信先端末 ID をサーバに登録するステップ、

前記送信端末が、前記暗号鍵で前記暗号化コンテンツを二重に暗号化した二重暗号化コンテンツを前記送信先端末に送信するステップと、

前記二重暗号化コンテンツ受信後、コンテンツ ID、送信先端末 ID、送信元端末 ID と共に、通信のための暗号鍵の送信要求をサーバに送信するステップと、

前記登録されたコンテンツの ID、送信元端末 ID 及び送信先端末 ID と、前記送信要求と共に送信されたコンテンツ ID、送信先端末 ID、及び送信元端末 ID とを照合し、一致する場合、登録されている暗号鍵を前記送信先端末に対して送信するステップと、

前記登録されたコンテンツ ID、送信元端末 ID、及び送信先の端末 ID を保存する流通管理ステップと、

前記コンテンツを再生するために、前記再生鍵の送信を要求するステップと、

前記再生鍵を要求した端末が前記流通管理手段で登録されている端末であれば、前記再生鍵を送信する再生鍵送信ステップと
を有することを特徴とするコンテンツ配信方法。

[4] 前記再生鍵送信ステップは、

前記流通管理ステップで登録された情報を参照するステップと、

前記参照の結果、再生鍵の送信を要求した端末の使用が過去に多くコンテンツを配信している場合、配信数に応じて値引きして課金するステップと
を有することを特徴とする請求項 3 に記載のコンテンツ配信方法。

[5] コンテンツを暗号化した暗号化コンテンツを配信する処理と、

前記暗号化コンテンツを復号するための再生鍵を保管する処理と、

前記暗号化コンテンツを端末間で送受信する際に、通信のための暗号鍵を生成し、この暗号鍵と、前記コンテンツの ID と、送信元端末 ID と、送信先端末 ID とをサーバに登録する処理と、

前記暗号鍵で暗号化コンテンツを二重に暗号化した二重暗号化コンテンツを前記送信先端末に送信する処理と、

前記二重暗号化コンテンツを受信後、前記コンテンツ ID と送信先端末 ID と送信元端末 ID と共に前記暗号鍵の送信を要求する送信要求を送信する処理と、

前記登録されたコンテンツの ID、送信元端末 ID 及び送信先端末 ID と、前記送信

要求と共に送信されたコンテンツ ID、送信先端末 ID、及び送信元端末 ID とを照合し、一致する場合、登録されている暗号鍵を前記送信先端末に対して送信する処理と、

前記登録されたコンテンツ ID、送信元端末 ID、及び送信先の端末 ID を保存する流通管理処理と、

前記コンテンツを再生するために、前記再生鍵の送信を要求する処理と、

前記再生鍵を要求した端末が前記流通管理手段で登録されている端末であれば、前記再生鍵を送信する再生鍵送信処理と

をコンピュータに実行させるためのプログラム。

- [6] 前記再生鍵送信処理は、前記流通管理処理に登録されている情報を参照して、再生鍵を要求した端末の使用者が過去に多くコンテンツを配信している場合、配信数に応じて値引きして課金する処理をコンピュータにさらに実行させることを特徴とする請求項5に記載のプログラム。

- [7] 暗号化コンテンツを他の端末に送信する際に、通信鍵を生成し、この通信鍵と暗号化コンテンツの ID と送信元端末 ID と送信先端末 ID を送信する手段と、

前記通信鍵で、暗号化コンテンツを二重暗号化して二重暗号化コンテンツを生成する手段と、

前記二重暗号化コンテンツを送信する手段と、

前記二重暗号化コンテンツを受信する手段と、

前記通信鍵の送信要求を送信する際に、暗号化コンテンツ ID と送信元端末 ID と送信先端末 ID とを送信する手段と、

前記通信鍵の送信要求に応じて送信された通信鍵を受信し、二重暗号化コンテンツを復号する手段と、

前記復号されたコンテンツを再生するための再生鍵の送信を要求する手段と、

前記再生鍵の送信要求に応じて送信された再生鍵を受信し、コンテンツを再生する手段と

を備えたことを特徴とする端末。

- [8] 暗号化コンテンツの ID とそれを復号するための再生鍵とを保管する手段と、

通信鍵と前記暗号化コンテンツ ID と送信元端末 ID と送信先端末 ID とを送信元端

末から受信する手段と、

通信鍵送信要求と前記暗号化コンテンツ ID と送信元端末 ID と送信先端末 ID を送信先端末から受信する手段と、

前記 2 つの手段で受信したコンテンツ ID、送信元端末 ID、送信先端末 ID を照合し、一致した場合前記通信鍵を送信先端末に送信する手段と、

前記暗号化コンテンツ ID、送信元端末 ID、送信先端末 ID をデータベースに登録する手段と、

送信先端末から前記再生鍵の送信要求がきた際に、その端末が上記データベースに登録されているかどうか確認し、登録されている場合、再生鍵を送信する再生鍵送信手段と

を備えたことを特徴とするサーバ。

[9] 前記再生鍵送信手段が上記データベースに登録されている情報を参照して、再生鍵を要求した端末の利用者が過去に多くコンテンツを配信している場合、配信数に応じて値引きして課金する手段を備えたことを特徴とする請求項 8 に記載のサーバ。

[10] (削除)

[11] (削除)

[12] (削除)

[13] (削除)

[14] (削除)

[15] (削除)

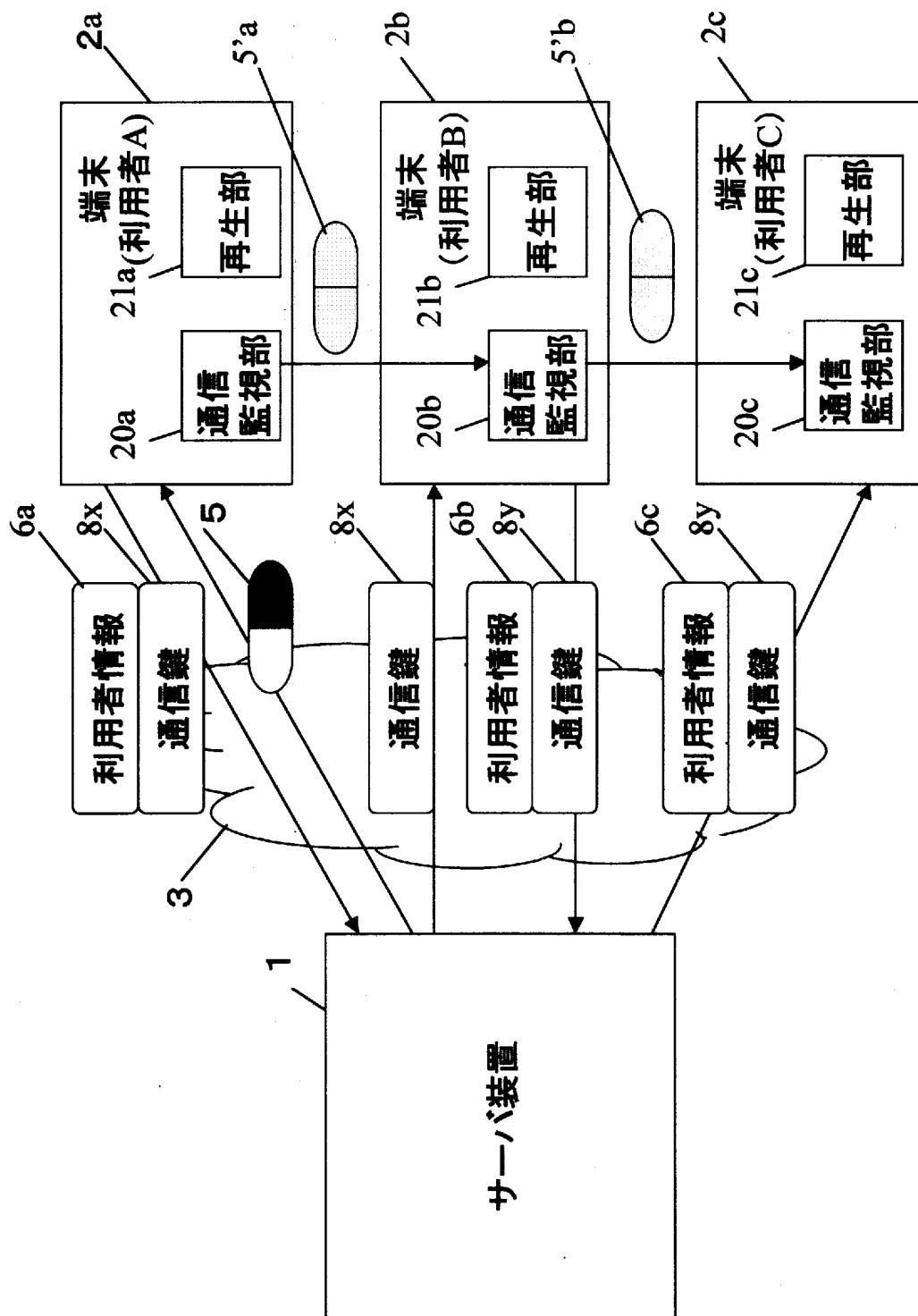
条約第 19 条 (1) に基づく説明書

条約 19 条に基づく説明書

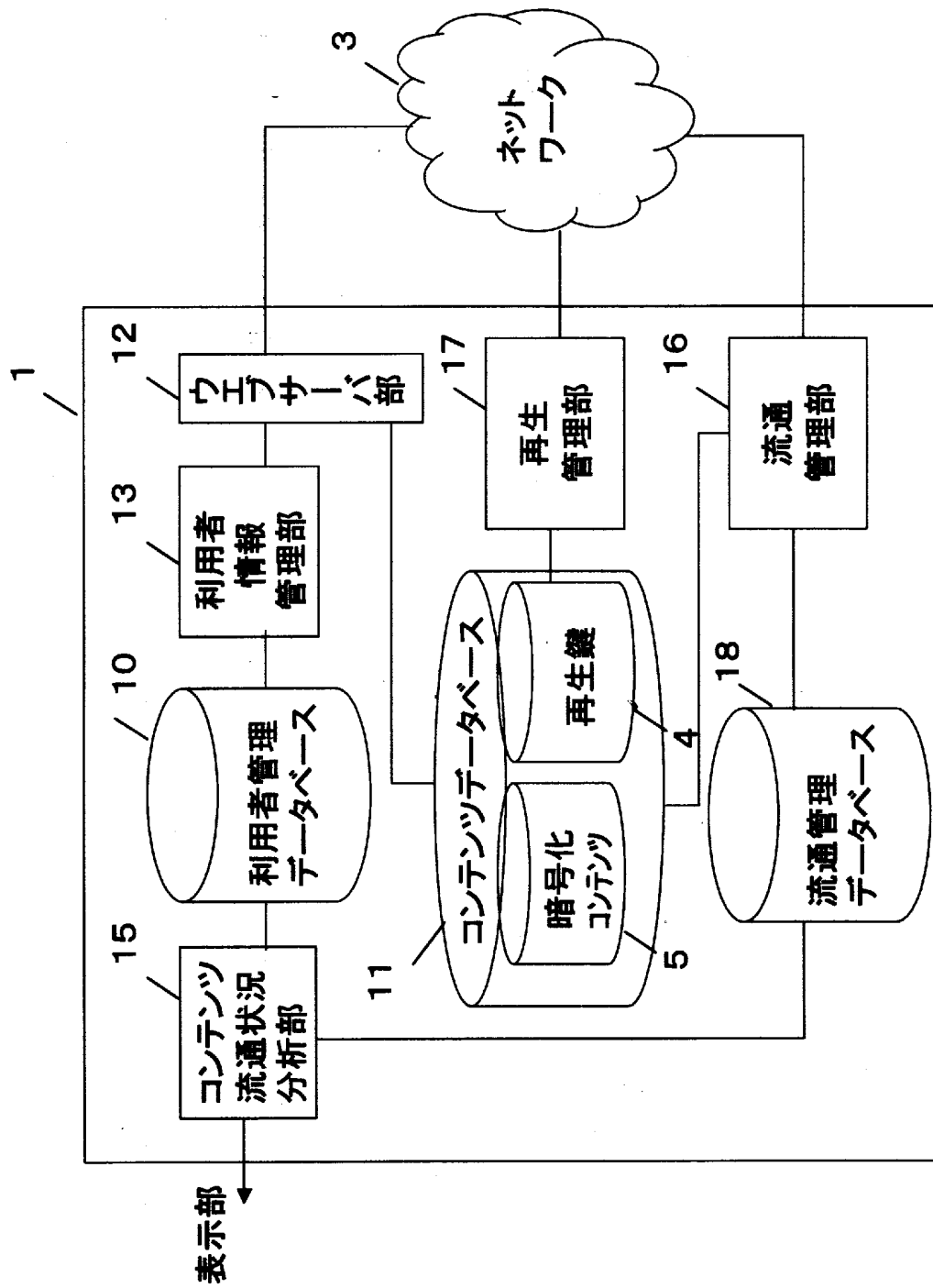
請求の範囲第 1 項、第 2 項、第 3 項、第 4 項、第 5 項、第 6 項、第 7 項、第 8 項、及び第 9 項は、そのまま補正していない。

請求の範囲第 10 項、第 11 項、第 12 項、第 13 項、第 14 項、及び第 15 項は、削除した。

[図1]



[図2]



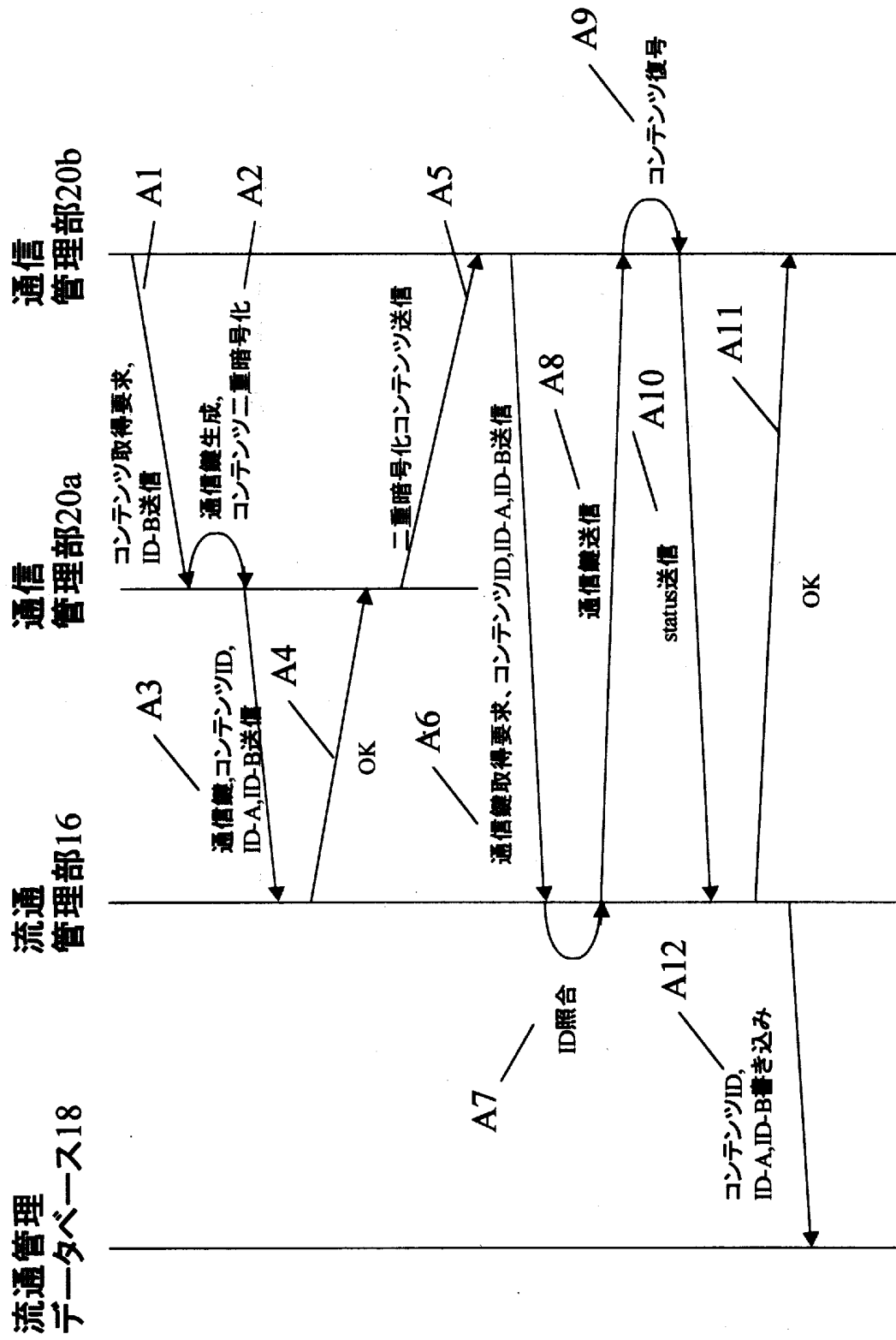
[図3]

端末ID	利用者情報
ID-A	利用者情報6a (ユーザAに関する情報)
ID-B	利用者情報6b (ユーザBに関する情報)
ID-C	利用者情報6c (ユーザCに関する情報)
:	:

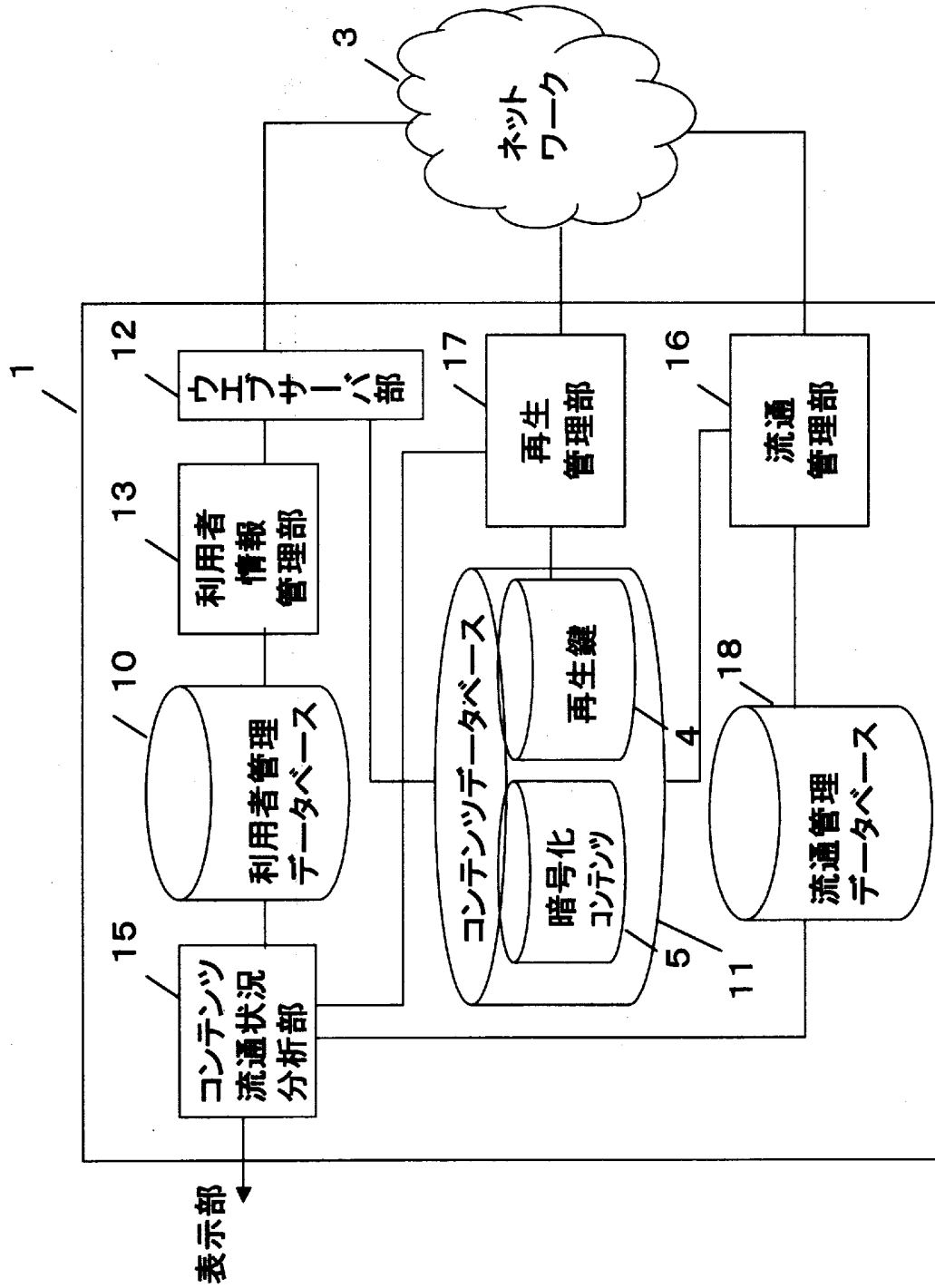
[図4]

コンテンツID	送信端末ID	受信端末ID
ID-1	ID-Server	ID-A
ID-1	ID-A	ID-B
ID-1	ID-B	ID-C

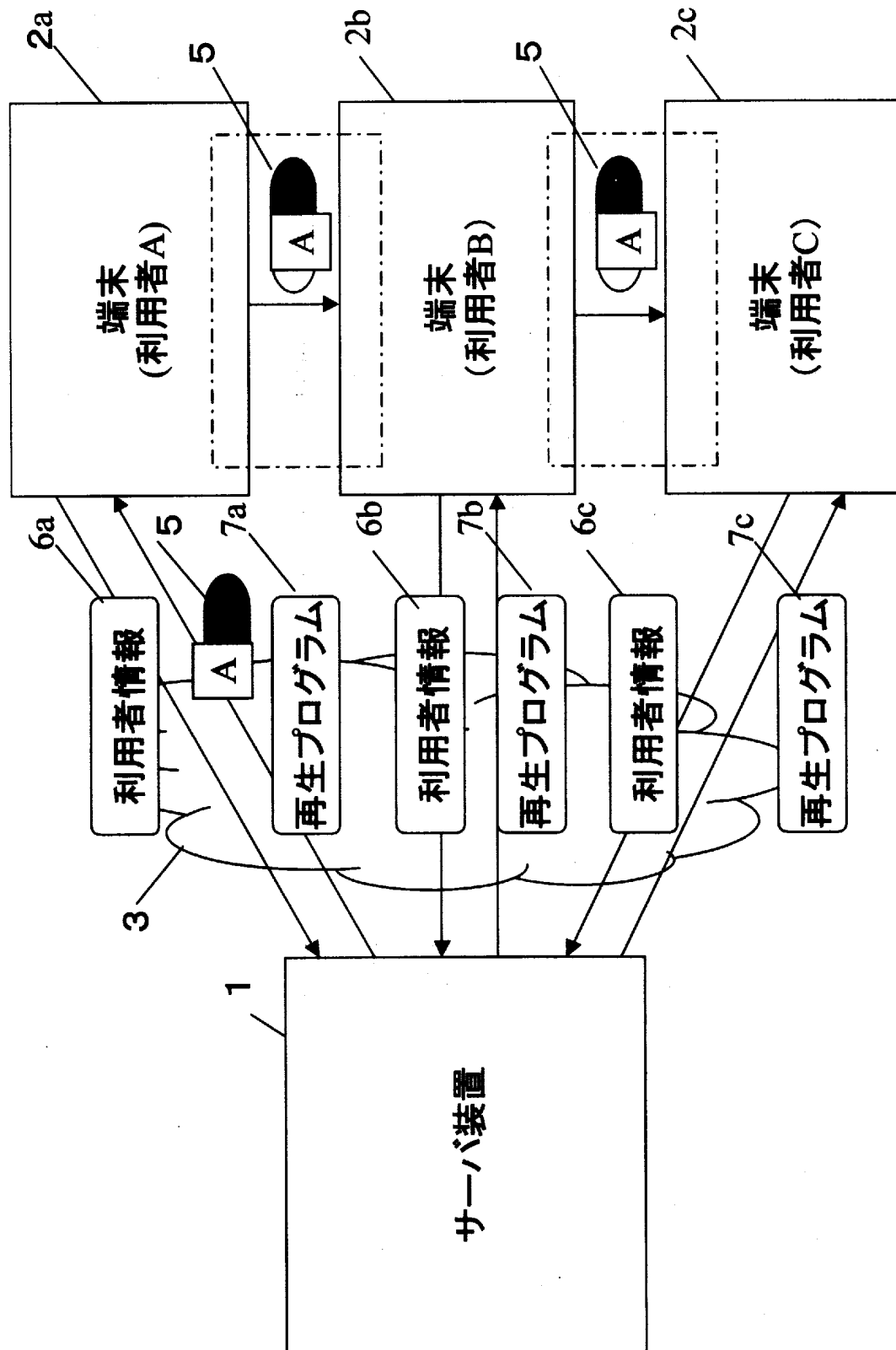
[図5]



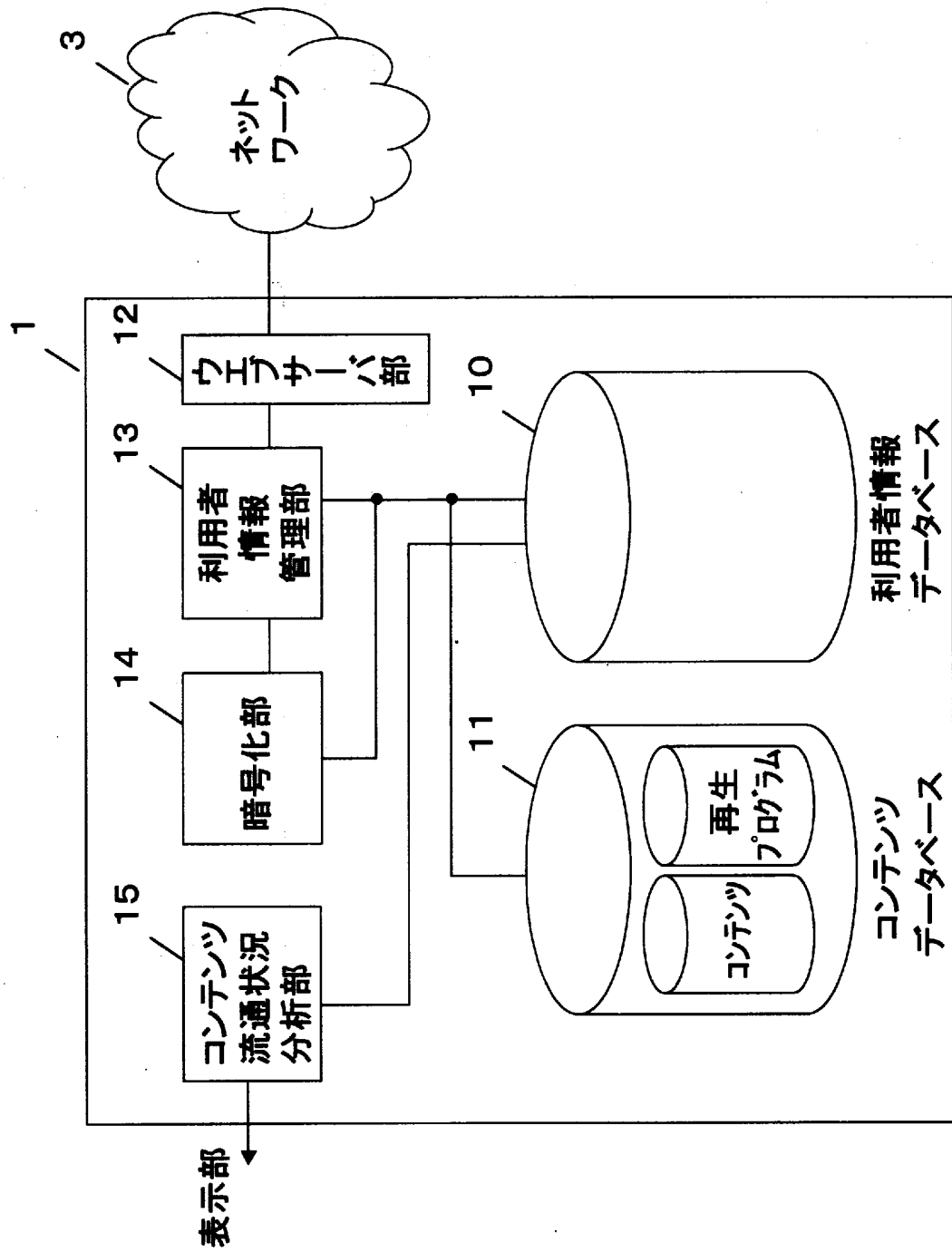
[図6]



[図7]



[図8]



[図9]

利用者ID	端末ID	利用者情報	コンテンツ名	推薦ID	再生プログラム名
ID-A	ID-2				ap
ID-B	ID-3			ID-A	ap
ID-C	ID-4			ID-A	ap
:	:	:	:	:	:

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2005/018362

A. CLASSIFICATION OF SUBJECT MATTER

H04L9/08(2006.01)

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L9/08(2006.01) , **G06Q30/00**(2006.01) , **G06Q50/00**(2006.01)

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

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2005
Kokai Jitsuyo Shinan Koho	1971-2005	Toroku Jitsuyo Shinan Koho	1994-2005

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 A	JP 2000-298689 A (Ryuichi SASAKI), 24 October, 2000 (24.10.00), Fig. 1; Par. Nos. [0037], [0044] (Family: none)	10-15 1-9
X A	JP 2004-38883 A (Toppan Printing Co., Ltd.), 05 February, 2004 (05.02.04), Fig. 3; Par. Nos. [0025] to [0040], [0055] (Family: none)	10-15 1-9
X A	JP 2004-94677 A (Toshiba Corp.), 25 March, 2004 (25.03.04), Fig. 31; Par. Nos. [0089] to [0093] & EP 1536358 A	10-15 1-9

☒ 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
13 December, 2005 (13.12.05)

Date of mailing of the international search report
20 December, 2005 (20.12.05)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2005/018362

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 2003-16287 A (Sanyo Electric Co., Ltd.), 17 January, 2003 (17.01.03), Full text (Family: none)	1-15
A	JP 2003-124921 A (Kabushiki Kaisha Supa Kontentsu Ryutsu), 25 April, 2003 (25.04.03), Full text (Family: none)	1-15
A	JP 2004-12866 A (Nippon Telegraph And Telephone Corp.), 15 January, 2004 (15.01.04), Full text (Family: none)	1-15

A. 発明の属する分野の分類 (国際特許分類 (IPC)) Int.Cl. H04L9/08 (2006.01)			
B. 調査を行った分野 調査を行った最小限資料 (国際特許分類 (IPC)) Int.Cl. H04L9/08 (2006.01), G06Q30/00 (2006.01), G06Q50/00 (2006.01)			
最小限資料以外の資料で調査を行った分野に含まれるもの 日本国実用新案公報 1922-1996年 日本国公開実用新案公報 1971-2005年 日本国実用新案登録公報 1996-2005年 日本国登録実用新案公報 1994-2005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 A	JP 2000-298689 A (佐々木隆一) 2000.10.24, 第1図、【0037】、【0044】段落 (ファミリーなし)	10-15 1-9	
X A	JP 2004-38883 A (凸版印刷株式会社) 2004.02.05, 第3図、【0025】-【0040】、 【0055】段落 (ファミリーなし)	10-15 1-9	
☒ 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 13.12.2005		国際調査報告の発送日 20.12.2005	
国際調査機関の名称及びあて先 日本国特許庁 (ISA/JP) 郵便番号100-8915 東京都千代田区霞が関三丁目4番3号		特許庁審査官 (権限のある職員) 石田 信行 電話番号 03-3581-1101 内線 3546	5S 9469

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
X A	JP 2004-94677 A (株式会社東芝) 2004.03.25, 第31図、【0089】－【0093】段落 & EP 1536358 A	10-15 1-9
A	JP 2003-16287 A (三洋電機株式会社) 2003.01.17, 全文 (ファミリーなし)	1-15
A	JP 2003-124921 A (株式会社スーパーコンテンツ流通) 2003.04.25, 全文 (ファミリーなし)	1-15
A	JP 2004-12866 A (日本電信電話株式会社) 2004.01.15, 全文 (ファミリーなし)	1-15