

(19) 世界知的所有権機関
国際事務局(43) 国際公開日
2004 年 1 月 29 日 (29.01.2004)

PCT

(10) 国際公開番号
WO 2004/010307 A1

(51) 国際特許分類: G06F 12/14, H04L 9/08, G06F 17/60

(21) 国際出願番号: PCT/JP2003/008267

(22) 国際出願日: 2003 年 6 月 30 日 (30.06.2003)

(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2002-213700 2002 年 7 月 23 日 (23.07.2002) JP

(71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒141-0001 東京都品川区北品川 6 丁目 7 番 3 5 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): 北谷 義道 (KI-TAYA, Yoshimichi) [JP/JP]; 〒141-0001 東京都品川区

北品川 6 丁目 7 番 3 5 号 ソニー株式会社内 Tokyo (JP). 栗屋 志伸 (KURIYA, Shinobu) [JP/JP]; 〒141-0001 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社内 Tokyo (JP).

(74) 代理人: 宮田 正昭, 外 (MIYATA, Masaaki et al.); 〒104-0041 東京都中央区新富一丁目 1 番 7 号 銀座ティーケイビル 澤田・宮田・山田特許事務所 Tokyo (JP).

(81) 指定国 (国内): CN, KR, US.

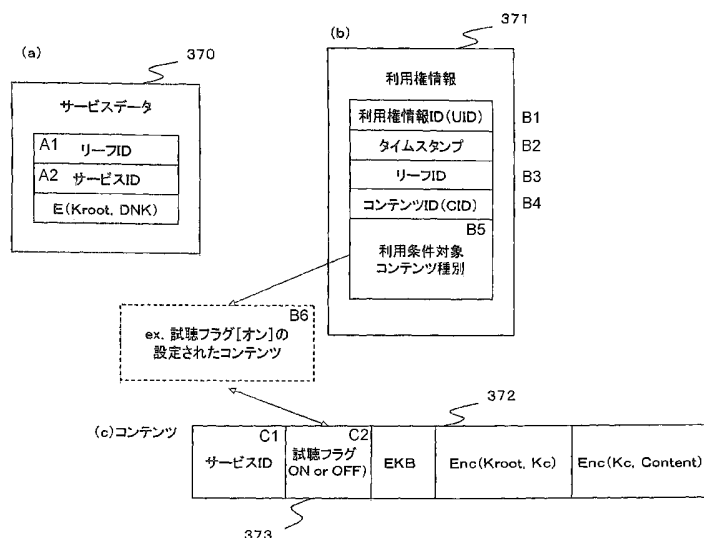
(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR).

添付公開書類:
— 国際調査報告書

[続葉有]

(54) Title: INFORMATION PROCESSING DEVICE, INFORMATION PROCESSING METHOD, AND COMPUTER PROGRAM

(54) 発明の名称: 情報処理装置、および情報処理方法、並びにコンピュータ・プログラム



370...SERVICE DATA
 A1...LEAF ID
 A2...SERVICE ID
 371...USAGE RIGHT INFORMATION
 B1...USAGE RIGHT INFORMATION ID (UID)
 B2...TIME STAMP
 B3...LEAF ID
 B4...CONTENT ID (CID)
 B5...CONTENT TYPE OF USAGE CONDITION
 B6...ex. CONTENT IN WHICH TEST LISTENING FLAG IS SET TO "ON"
 (C)...CONTENT
 C1...SERVICE ID
 C2...TEST LISTENING FLAG ON or OFF

(57) Abstract: A device and a method for realizing an improved processing for content test listening in content use based on content usage right information. Upon registration on a license server, a client acquires a default usage right and upon test listening not requiring content purchase processing, it is judged whether content reproduction is enabled according to the default usage right information. A client allowed to perform test listening is limited to a client who has performed registration on the license server and has default usage right information. Thus, it is possible to prevent flood of test listening data out of order.

(57) 要約: コンテンツの利用権情報に基づくコンテンツ利用構成において、コンテンツ試聴における改良された処理を実現する装置、方法を提供する。クライアントは、ライセンスサーバに対する登録処理の際にデフォルト利用権情報 (Default Usage Right) を取得し、コンテンツの購入処理を伴わない試聴処理の際にデフォルト利用権情報に基づいてコンテンツ再生の可否を判定する。試聴が許可されるクライアントは、ライセンスサーバに対する登録処理を行ない、デフォルト利用権情報を有するクライアントに限定されることになるので、試聴データが無秩序に氾濫してしまうことが防止される。

WO 2004/010307 A1



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

情報処理装置、および情報処理方法、並びにコンピュータ・プログラム

5 技術分野

本発明は、情報処理装置、および情報処理方法、並びにコンピュータ・プログラムに関する。特に、コンテンツの再生等の利用時におけるコンテンツ利用権の確認を実現し、また、コンテンツの試聴、試写処理を可能としてユーザに対するフレキシブルなコンテンツ利用態様を実現した情報処理装置、および情報処理方法、並びにコンピュータ・プログラムに関する。

背景技術

15

昨今、音楽データ、ゲームプログラム、画像データ等、様々なソフトウェアデータ（以下、これらをコンテンツ（Content）と呼ぶ）の、インターネット等のネットワーク、あるいは、メモ리카ード、HD、DVD、CD等の流通可能な記憶媒体を介した流通が盛んになっている。これらの流通コンテンツは、ユーザの所有するPC（Personal Computer）、記録再生器、再生専用器、あるいはゲーム機器内の記憶手段、例えばHD、フラッシュメモリを有するカード型記憶装置、CD、DVD等に格納され、再生処理が実行される。

25

記録再生装置、ゲーム機器、PC等の情報機器には、コンテンツをネットワークから受信するためのインタフェース、あるいはメモ리카ード、HD、DVD、CD等にアクセスするためのインタフェースを有し、コンテンツの再生に必要な制御手段、プログラム、データのメモリ領域として使用されるRAM、ROM等を有する。

音楽データ、画像データ、あるいはプログラム等の様々なコンテンツは、再生機器として利用される記録再生装置、ゲーム機器、P C等の情報機器本体からのユーザ指示、あるいは接続された入力手段を介したユーザの指示により、例えば内蔵、あるいは着脱自在の記憶媒体から呼び出され、情報機器本体、あるいは接続されたディスプレイ、スピーカ等を通じて再生される。

ゲームプログラム、音楽データ、画像データ等、多くのソフトウェア・コンテンツは、一般的にその作成者、販売者に頒布権等が保有されている。従って、これらのコンテンツの配布に際しては、一定の利用制限、すなわち、正規なユーザに対してのみ、ソフトウェアの使用を許諾し、許可のない複製等が行われないようにする、すなわちセキュリティを考慮した構成をとるのが一般的となっている。

また、コンテンツと、コンテンツを利用する利用権とを独立に管理し、ユーザに提供する構成が提案されている。この構成において、ユーザは、例えば暗号化されたコンテンツを取得し、さらに、利用権データを購入することにより、利用権データから取得可能な鍵データ等に基づいて、暗号化コンテンツの復号用の鍵（コンテンツ鍵）を取得して、コンテンツを利用する。

利用権データには、ユーザのコンテンツ利用許可態様の設定情報が格納され、その許可情報において許された範囲でのコンテンツの利用が可能となるといったシステムが提案されている。

25

発明の開示

このように、コンテンツとコンテンツ利用権とを独立に管理し、ユーザに提供するシステムにおいては、コンテンツの利用、例えば音楽デー

タ、画像データの再生、または配信、あるいはダウンロード処理に際して、利用権データのチェックが実行される。

このような構成において、利用権チェックの際、ユーザがコンテンツの利用をする権利がないと判定された場合には、コンテンツの再生、配信、ダウンロードが実行されないことになる。

しかしながら、コンテンツの購入以前に、コンテンツの一部等を試聴、あるいは試写を行なって、コンテンツの内容を確認した上で、コンテンツの購入を行ないたいという要望があるのも事実であり、このような場合に、通常の利用権のチェック処理を行なえば、利用権が無いとの判定によって、コンテンツ再生等の処理が拒否されてしまうことになる。

このような状況に対応するためには、利用権を全く考慮しないフリーのサンプルデータをユーザに対して配布する構成とすることも可能であるが、ほとんどのコンテンツには著作権者の著作権、頒布者の頒布権が存在する。従って、コンテンツの一部であっても、コンテンツが無秩序に流通し、ユーザ間で無断でコピーが行われるといった事態は好ましいことではない。

本発明は、このような状況に鑑みてなされたものであり、ユーザがコンテンツの正規な購入処理を行なって利用権に基づいた正当なコンテンツ利用を可能とするとともに、コンテンツを購入を伴わないコンテンツ試聴、あるいは試写を行なうことを可能とした情報処理装置、および情報処理方法、並びにコンピュータ・プログラムを提供することを目的とするものである。

本発明は、さらに、試聴データ、試写データの無秩序な二次流通の防止を可能とした情報処理装置、および情報処理方法、並びにコンピュータ・プログラムを提供することを目的とするものである。

本発明の第 1 の側面は、

暗号化されたコンテンツの復号及び利用を制御する情報処理装置であって、

- 5 コンテンツ利用の指示に応じて、該コンテンツに対応する利用権情報（u s a g e r i g h t）に基づいて、該コンテンツの利用を制御する制御手段と、

製造時に記録されたあるいはサービス登録時に取得されたデフォルト利用権情報を記録する記録手段とを備え、

- 10 前記制御手段は、前記コンテンツに前記デフォルト利用権情報に対応することを示す情報が含まれている場合に、前記デフォルト利用権情報に記述内容に基づいて前記コンテンツを復号し、利用することを許可する

ことを特徴とする情報処理装置にある。

15

さらに、本発明の情報処理装置の一実施態様において、前記デフォルト利用権情報に基づいて利用が許可される前記コンテンツは、試用の目的で提供されるものであり、前記制御手段は、前記コンテンツに試用コンテンツであることを示すフラグが含まれているかを検証し、検証結果

20 に基づいて前記コンテンツの再生を許可することを特徴とする。

- さらに、本発明の情報処理装置の一実施態様において、前記情報処理装置は、さらに、サービスへの登録要求を送信する送信手段と、登録要求に応じてライセンスサーバから送信されるデフォルト利用権情報を
- 25 受信する受信手段とを備えることを特徴とする。

さらに、本発明の情報処理装置の一実施態様において、前記受信手段は、さらに前記コンテンツの復号に必要な鍵情報を受信することを特徴とする。

さらに、本発明の第2の側面は、

暗号化されたコンテンツの利用条件 (usage rules) が記述された利用権を発行する情報処理装置であって、

5 登録要求を受信する受信手段と、

前記登録要求に応じて、暗号化されたコンテンツの復号に必要な鍵情報と、デフォルト利用権情報を送信する送信手段と、
を備えることを特徴とする情報処理装置にある。

10 さらに、本発明の情報処理装置の一実施態様において、前記デフォルト利用権情報に基づいて利用が許可される前記コンテンツは、試用の目的で提供されるものであり、前記デフォルト利用権情報は、前記コンテンツに試用コンテンツであることを示すフラグが含まれている場合に再生を許可することが記述されていることを特徴とする。

15

さらに、本発明の第3の側面は、

暗号化されたコンテンツの復号及び利用を制御する情報処理方法であって、

コンテンツ利用の指示に応じて、該コンテンツに対応する利用権情報
20 (usage right) に基づくコンテンツ利用を制御する制御ステップを有し、

前記制御ステップは、

前記コンテンツに、製造時に記録されたデフォルト利用権情報、あるいはサービス登録時に取得されたデフォルト利用権情報に対応することを示す情報が含まれているか否かを検証するステップと、

25

デフォルト利用権情報に対応することを示す情報が含まれている場合に、前記デフォルト利用権情報に記述内容に基づいて前記コンテンツを復号し、利用することを許可するステップと、

を含むことを特徴とする情報処理方法にある。

さらに、本発明の情報処理方法の一実施態様において、前記デフォルト利用権情報に基づいて利用が許可される前記コンテンツは、試用の目的で提供されるものであり、前記制御ステップは、さらに、前記コンテンツに試用コンテンツであることを示すフラグが含まれているかを検証し、検証結果に基づいて前記コンテンツの再生を許可するステップを含むことを特徴とする。

さらに、本発明の情報処理方法の一実施態様において、前記情報処理方法は、さらに、サービスへの登録要求を送信する送信ステップと、登録要求に応じてライセンスサーバから送信されるデフォルト利用権情報を受信する受信ステップと、を含むことを特徴とする。

さらに、本発明の情報処理方法の一実施態様において、前記情報処理方法は、さらに、前記コンテンツの復号に必要な鍵情報を受信するステップを含むことを特徴とする。

さらに、本発明の第4の側面は、
暗号化されたコンテンツの利用条件 (usage rules) が記述された利用権を発行する情報処理方法であって、
登録要求を受信する受信ステップと、
前記登録要求に応じて、暗号化されたコンテンツの復号に必要な鍵情報と、デフォルト利用権情報を送信する送信ステップと、
を有することを特徴とする情報処理方法にある。

25

さらに、本発明の情報処理方法の一実施態様において、前記デフォルト利用権情報に基づいて利用が許可される前記コンテンツは、試用の目的で提供されるものであり、前記デフォルト利用権情報は、前記コンテンツに試用コンテンツであることを示すフラグが含まれている場合に

再生を許可することが記述されていることを特徴とする。

さらに、本発明の第5の側面は、

5 暗号化されたコンテンツの復号及び利用を制御する情報処理を実行するコンピュータ・プログラムであって、

コンテンツ利用の指示に応じて、該コンテンツに対応する利用権情報（usage right）に基づくコンテンツ利用を制御する制御ステップを有し、

前記制御ステップは、

10 前記コンテンツに、製造時に記録されたデフォルト利用権情報、あるいはサービス登録時に取得されたデフォルト利用権情報に対応することを示す情報が含まれているか否かを検証するステップと、

デフォルト利用権情報に対応することを示す情報が含まれている場合に、前記デフォルト利用権情報に記述内容に基づいて前記コンテンツを復号し、利用することを許可するステップと、

15 を含むことを特徴とするコンピュータ・プログラムにある。

さらに、本発明のコンピュータ・プログラムの一実施態様において、前記デフォルト利用権情報に基づいて利用が許可される前記コンテンツは、試用の目的で提供されるものであり、前記制御ステップは、さらに、前記コンテンツに試用コンテンツであることを示すフラグが含まれているかを検証し、検証結果に基づいて前記コンテンツの再生を許可するステップを含むことを特徴とする。

25 さらに、本発明のコンピュータ・プログラムの一実施態様において、前記コンピュータ・プログラムは、さらに、サービスへの登録要求を送信する送信ステップと、登録要求に応じてライセンスサーバから送信されるデフォルト利用権情報を受信する受信ステップと、を含むことを特徴とする。

さらに、本発明のコンピュータ・プログラムの一実施態様において、前記コンピュータ・プログラムは、さらに、前記コンテンツの復号に必要なとなる鍵情報を受信するステップを含むことを特徴とする。

5 さらに、本発明の第6の側面は、

暗号化されたコンテンツの利用条件（usage rules）が記述された利用権を発行する情報処理を実行するコンピュータ・プログラムであって、

登録要求を受信する受信ステップと、

10 前記登録要求に応じて、暗号化されたコンテンツの復号に必要なとなる鍵情報と、デフォルト利用権情報を送信する送信ステップと、
を有することを特徴とするコンピュータ・プログラムにある。

さらに、本発明のコンピュータ・プログラムの一実施態様において、
15 前記デフォルト利用権情報に基づいて利用が許可される前記コンテンツは、試用の目的で提供されるものであり、前記デフォルト利用権情報は、前記コンテンツに試用コンテンツであることを示すフラグが含まれている場合に再生を許可することが記述されていることを特徴とする。

20 さらに、本発明の第7の側面は、

暗号化されたコンテンツの復号及び利用を行うコンテンツ利用装置と、暗号化されたコンテンツの利用条件（usage rules）が記述された利用権を発行する利用権発行装置を有するコンテンツ利用管理システムであって、

25 前記コンテンツ利用装置は、

サービスへの登録要求を送信する送信手段と、

登録要求に応じてライセンスサーバから送信されるデフォルト利用権情報を受信する受信手段とを備え、

前記利用権発行装置は、

前記登録要求を受信する受信手段と、
前記登録要求に応じて、暗号化されたコンテンツの復号に必要となる鍵情報と、デフォルト利用権情報を送信する送信手段とを備えた構成、
であることを特徴とするコンテンツ利用管理システムにある。

5

さらに、本発明の第8の側面は、

暗号化されたコンテンツの復号及び利用を行うコンテンツ利用装置
と、暗号化されたコンテンツの利用条件（u s a g e r u l e s）が
記述された利用権を発行する利用権発行装置を有するコンテンツ利用
10 管理システムにおけるコンテンツ利用管理方法であって、

前記コンテンツ利用装置から前記利用権発行装置に対してサービス
への登録要求を送信する登録要求送信ステップと、

前記利用権発行装置において、前記登録要求を受信し、該登録要求に
応じて、暗号化されたコンテンツの復号に必要となる鍵情報と、デフォ
15 ルト利用権情報を送信するデータ送信ステップと、

前記コンテンツ利用装置において、デフォルト利用権情報を受信する
受信ステップと、

を有することを特徴とするコンテンツ利用管理方法にある。

20 本発明の構成によれば、クライアントは、ライセンスサーバに対する
登録処理の際にデフォルト利用権情報（D e f a u l t U s a g e
R i g h t）を取得し、コンテンツの購入処理を伴わない試聴処理の際
にデフォルト利用権情報に基づいてコンテンツ再生が許可され、ユーザ
は、コンテンツの購入を実行することなく、コンテンツの試聴再生が可
25 能となる。また、試聴が許可されるクライアントは、ライセンスサーバ
に対する登録処理を行ない、デフォルト利用権情報を有するクライアン
トに限定されることになるので、試聴データが無秩序に氾濫してしまう
ことが防止される。

さらに、本発明の構成によれば、コンテンツの購入処理を伴わない試聴処理においても、コンテンツ利用機器としてのハードウェアに対応して設定されたカテゴリツリーに対応するEKBとしてのハード対応EKB[EKB(H)]と、コンテンツ利用サービスに対応して設定されたカテゴリツリーに対応するEKBとしてのサービス対応EKB[EKB(S)]に対する正当なDNKを有するユーザのみがコンテンツ再生を実行可能とする構成が適用でき、試聴処理においても再生権限を限定した範囲として設定可能となる。

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

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。

20 なお、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

図面の簡単な説明

25 図1は、本発明を適用したコンテンツ提供システムの概要を示す図である。

図2は、クライアント、および各サーバ、管理システムの構成例を示す図である。

図3は、各種キー、データの暗号化処理、配布処理について説明する

ツリー構成図である。

図 4 は、各種キー、データの配布に使用される有効化キープブロック (E K B) の例を示す図である。

図 5 は、コンテンツキーの有効化キープブロック (E K B) を使用した
5 配布例と復号処理例を示す図である。

図 6 は、有効化キープブロック (E K B) のフォーマット例を示す図である。

図 7 は、有効化キープブロック (E K B) のタグの構成を説明する図である。

10 図 8 は、ツリー構成におけるカテゴリ分割を説明する図である。

図 9 は、ツリー構成におけるカテゴリ分割を説明する図である。

図 10 は、ツリー構成におけるカテゴリ分割の具体例を説明する図である。

図 11 は、コンテンツ購入、または試聴処理における各エンティティ
15 間の実行処理シーケンス (その 1) を示す図である。

図 12 は、管理システムにおいて実行するトランザクション ID 生成、発行処理手順を示すフロー図である。

図 13 は、コンテンツ購入、または試聴処理における各エンティティ間の実行処理シーケンス (その 2) を示す図である。

20 図 14 は、管理システムにおいて実行するダウンロード許可処理手順を示すフロー図である。

図 15 は、起動ファイルのデータ構成例を示す図である。

図 16 は、クライアントにおいて実行する起動ファイルに基づくアプリケーション実行手順を示すフロー図である。

25 図 17 は、サービスデータ、利用権情報のデータ構成例を示す図である。

図 18 は、コンテンツ購入処理における各エンティティ間の実行処理シーケンスを示す図である。

図 19 は、コンテンツ再生処理の概要を説明する図である。

図 20 は、有効化キーブロック (E K B) を適用したコンテンツ復号、利用処理例を説明する図である。

図 21 は、コンテンツ試聴処理における各エンティティ間の実行処理シーケンスを示す図である。

5 図 22 は、試聴コンテンツ再生処理の概要を説明する図である。

図 23 は、ライセンスまたはコンテンツのバックアップ／リストア処理における各エンティティ間の処理シーケンス (その 1) を示す図である。

10 図 24 は、リストア処理要求ファイル [r e s t o r e . d a t] の構成例を示す図である。

図 25 は、M A C 生成処理構成を示す図である。

図 26 は、ライセンスまたはコンテンツのバックアップ／リストア処理における各エンティティ間の処理シーケンス (その 2) を示す図である。

15 図 27 は、ライセンスまたはコンテンツのバックアップ／リストア処理における各エンティティ間の処理シーケンス (その 3) を示す図である。

図 28 は、リコメンドファイルの生成処理フローを示す図である。

図 29 は、リコメンドファイル生成画面を示す図である。

20 図 30 は、リコメンドファイル構成例を示す図である。

図 31 は、リコメンドファイル中に格納されるコンテンツファイルの構成例を示す図である。

図 32 は、リコメンドファイル中に格納されるコンテンツ説明ファイルの表示例を示す図である。

25 図 33 は、リコメンドファイルを受領したクライアントにおけるライセンス情報取得処理フロー (その 1) を示す図である。

図 34 は、リコメンドファイルを受領したクライアントにおけるライセンス情報取得処理フロー (その 2) を示す図である。

発明を実施するための最良の形態

以下、本発明の構成について詳細に説明する。なお、説明は、以下に示す各項目に従って行なう。

- 5 1. コンテンツ提供システム概要
- 2. キー配信構成としてのツリー（木）構造について
- 3. E K Bを使用したキーの配布
- 4. E K Bのフォーマット
- 5. ツリーのカテゴリ分類
- 10 6. コンテンツ購入および試聴処理
- 7. バックアップ／リストア処理
- 8. リコメンドファイルによるコンテンツの二次配信

[1. コンテンツ提供システム概要]

- 15 図 1 は、本発明を適用したコンテンツ提供システムの概要を説明する図である。コンテンツの利用を行なうクライアント 1 0 は、コンテンツを利用、すなわち再生可能な機器としての情報処理装置である。例えば P C、P D A 等、各種の情報処理装置が含まれる。クライアント 1 0 は、ソフトウェアとしてブラウザ 1 1、クライアントアプリケーション 1 2
- 20 を有し、C P U 等の制御手段によりブラウザ 1 1、クライアントアプリケーション 1 2 他のプログラムが実行される。

- 25 クライアントアプリケーション 1 2 は、クライアントにおけるコンテンツの購入および試聴処理、後段において説明するサービスデータ、コンテンツ利用権情報を含むライセンス情報の取得処理、コンテンツおよびライセンス情報のバックアップ／リストア処理、コンテンツ利用権の確認処理、コンテンツ再生管理処理、あるいは、二次配信用のコンテンツファイルとしてのリコメンドファイルの生成処理等を実行するアプリケーションであり、以下、詳細に説明する処理プログラムとして、ク

ライアントの情報処理装置に格納される。なお、本明細書においては、「試聴」は、音声データの試聴のみならず、画像データの試写を包含する意味として用いる。

- 5 クライアント 10 は、例えばインターネット等の通信網を介してショップサーバ 21、ライセンスサーバ 22、およびコンテンツサーバ 23 と接続される。コンテンツサーバ 23 は、クライアント 10 に対してコンテンツを提供する。ライセンスサーバ 22 は、クライアントが利用するコンテンツの利用権情報をクライアント 10 に対して提供する。また、
- 10 ショップサーバ 21 は、クライアント 10 がコンテンツを購入する際の窓口として機能し、購入または試聴可能コンテンツをブラウザを介して提示し、クライアントからの購入あるいは試聴の要求を受け付ける。また、必要に応じて購入コンテンツに関する課金処理を行なう。
- 15 さらに、ショップサーバ 21、およびライセンスサーバ 22 には、管理システム 31 が接続される。管理システム 31 は、ショップサーバ 21 が受け付けたクライアント 10 からのコンテンツ要求に対する許可情報として機能するトランザクション ID (TID) の発行処理、コンテンツダウンロード許可情報の発行処理を行なう。また、管理システム
- 20 31 は、ライセンスサーバ 22 に対して、コンテンツの利用権情報としての利用権データ Usage Right) の発行許可を行なう。これらの処理の詳細は、後段で説明する。

- 25 なお、クライアント 10 は、ライセンスサーバ 22 からの利用権の取得、コンテンツサーバ 23 からのコンテンツ取得を、クライアントアプリケーション 12 の制御の下に実行し、ショップサーバ 21 の提供する情報の閲覧および決済処理は、クライアントアプリケーション 12 の制御の下にブラウザ 11 を起動して実行する。

図1には、クライアントおよび各サーバを1つずつ示してあるが、これらは例えばインターネット等の通信網上に多数接続され、クライアントは、様々なショップサーバに接続し、各ショップサーバで提供するコンテンツを自由に選択し、選択したコンテンツを格納したコンテンツサーバからコンテンツを取得し、取得したコンテンツの利用権を発行する
5 ライセンスサーバを選択して、その選択されたライセンスサーバから利用権を取得する。

コンテンツは、暗号化コンテンツとしてコンテンツサーバ23からクライアント10に提供される。さらに、ライセンスサーバ22からクライアント10に対しては、コンテンツに対応するコンテンツ利用権情報が提供され、クライアント10のクライアントアプリケーション12が、利用権情報を検証し、利用権があると判定された場合に暗号化コンテンツを復号して利用する。
10

15

クライアント10は、コンテンツ利用権に基づくコンテンツ利用を可能とするための鍵情報として、有効化キープブロック (E K B : Enabling Key Block)、デバイス・ノード・キー (D N K : Device Node Key) 等の鍵データを保持する。有効化キープブロック (E K B : Enabling Key Block)、デバイス・ノード・キー (D N K : Device Node Key) は、コンテンツの利用を正当なコンテンツ利用権を有するユーザデバイスにおいてのみ暗号化コンテンツを復号して利用可能とするためのコンテンツ利用に必要な暗号鍵を取得するための鍵データである。E K B, D N Kについては、後段で説明する。
20

25

コンテンツサーバ23は、コンテンツを暗号化して、暗号化コンテンツをクライアント10に提供する。さらに、ライセンスサーバ22は、コンテンツ利用条件に基づいて利用権情報 (U s a g e R i g h t) を生成してユーザデバイス30に提供する。さらに、管理システム31

の提供するデバイスノードキー（DNK：Device Node Key）、有効化キーブロック（EKB：Enabling Key Block）に基づいてサービスデータを生成してクライアント 10 に提供する。サービスデータは、暗号化コンテンツの復号処理の際に必要なサービス・デバイスノードキー（SDNK）を持つ有効化キーブロック（EKB）を含む。

なお、コンテンツの利用条件には、利用期間の限定条件、コピーの回数制限、さらにコンテンツを同時に利用することができるポータブルメディア（PM：Portable Media）の数（いわゆるチェックアウト（Check-out）数に対応）の制限等がある。ポータブルメディア（PM：Portable Media）は例えばフラッシュメモリ、または小型HD、光ディスク、光磁気ディスク、MD（Mini Disk）等、ポータブルデバイスにおいて利用可能な記憶媒体である。

次に、図 2 を参照して、クライアント 10、ショップサーバ 21、ライセンスサーバ 22、コンテンツサーバ 23、管理システム 31 として機能可能な情報処理装置の構成例を示す。これらの各システムは CPU を持つ例えば PC、サーバ等のシステムにそれぞれの処理に応じた処理プログラムを格納することで実現される。

20

まず、図 2 を用いて各システムの構成例について説明する。CPU（Central Processing Unit）101 は、ROM（Read Only Memory）102 に記憶されている各種プログラム、あるいは、記憶部 108 に格納され、RAM（Random Access Memory）103 にロードされたプログラムに従って各種処理を実行する。タイマ 100 は計時処理を行ない、クロック情報を CPU 101 に供給する。

ROM（Read Only Memory）102 は、CPU 101 が使用するプログラムや演算用のパラメータ、固定データ等を格納する。RAM（Random Access Memory）103 は、CPU 101 の実行において使用するプロ

グラムや、その実行において適宜変化するパラメータ等を格納する。これら各素子はCPUバスなどから構成されるバス111により相互に接続されている。

- 5 暗号化復号部104は、コンテンツの暗号化、復号処理、デバイスノードキー（DNK：Device Node Key）、有効化キーブロック（EKB：Enabling Key Block）の適用処理として、例えばDES（Data Encryption Standard）の暗号化アルゴリズムを適用した暗号処理、MAC生成、検証処理等を実行する。さらに、他の接続装置との間で実行されるコンテ
10 ンツあるいはライセンス情報の送受信時の認証およびセッションキー共有処理等、各種暗号処理を実行する。

- コーデック部105は、例えばATRAC（Adaptive Transform Acoustic Coding）3方式、MP3方式、JPEG方式等、各種方式のデー
15 タエンコード処理、デコード処理を実行する。処理対象データは、バス111、入出力インタフェース112、ドライブ110を介してリムーバブル記憶媒体121からまたは通信部109を介して入力する。また処理後のデータは、必要に応じて、リムーバブル記憶媒体121に格納し、または通信部109を介して出力する。

20

- 入出力インタフェース112には、キーボード、マウス等の入力部106、CRT、LCD等のディスプレイ、スピーカ等からなる出力部107、ハードディスク等の記憶部108、モデム、ターミナルアダプタ等によって構成される通信部109が接続され、例えばインターネット
25 等の通信網を介したデータ送受信を行なう。

[2. キー配信構成としてのツリー（木）構造について]

次に、正当なコンテンツ利用権を有するクライアントにおいてのみコンテンツを利用可能とするための、ブロードキャストエンクリプション

(Broadcast Encryption) 方式の一態様であるツリー構成によるデバイスとキーの管理構成について説明する。

図 3 の最下段に示すナンバ 0 ~ 1 5 がコンテンツ利用を行なうクライアントとしてのユーザデバイスである。すなわち図 3 に示す階層ツリー（木）構造の各葉（リーフ：leaf）がそれぞれのデバイスに相当する。

各デバイス 0 ~ 1 5 は、製造時あるいは出荷時、あるいはその後において、図 3 に示す階層ツリー（木）構造における自分のリーフからルートに至るまでのノードに割り当てられた鍵（ノードキー）および各リーフのリーフキーからなるキーセット（デバイスノードキー（DNK：Device Node Key））をメモリに格納する。図 3 の最下段に示す K 0 0 0 0 ~ K 1 1 1 1 が各デバイス 0 ~ 1 5 にそれぞれ割り当てられたリーフキーであり、最上段の K R（ルートキー）から、最下段から 2 番目の節（ノード）に記載されたキー：K R ~ K 1 1 1 をノードキーとする。

図 3 に示すツリー構成において、例えばデバイス 0 はリーフキー K 0 0 0 0 と、ノードキー：K 0 0 0、K 0 0、K 0、K R を所有する。デバイス 5 は K 0 1 0 1、K 0 1 0、K 0 1、K 0、K R を所有する。デバイス 1 5 は、K 1 1 1 1、K 1 1 1、K 1 1、K 1、K R を所有する。なお、図 3 のツリーにはデバイスが 0 ~ 1 5 の 1 6 個のみ記載され、ツリー構造も 4 段構成の均衡のとれた左右対称構成として示しているが、さらに多くのデバイスがツリー中に構成され、また、ツリーの各部において異なる段数構成を持つことが可能である。

25

また、図 3 のツリー構造に含まれる各デバイスには、様々な記録媒体、例えば、デバイス埋め込み型あるいはデバイスに着脱自在に構成された DVD、CD、MD、フラッシュメモリ等を使用する様々なタイプのデバイスが含まれている。さらに、様々なアプリケーションサービスが共

存可能である。このような異なるデバイス、異なるアプリケーションの共存構成の上に図3に示すコンテンツあるいは鍵配布構成である階層ツリー構造が適用される。

5 これらの様々なデバイス、アプリケーションが共存するシステムにおいて、例えば図3の点線で囲んだ部分、すなわちデバイス0, 1, 2, 3を同一の記録媒体を用いる1つのグループとして設定する。例えば、この点線で囲んだグループ内に含まれるデバイスに対しては、まとめて、共通のコンテンツを暗号化してプロバイダから送付したり、各デバイス
10 共通に使用するコンテンツキーを送付したり、あるいは各デバイスからプロバイダあるいは決済機関等にコンテンツ料金の支払データをやはり暗号化して出力するといった処理が実行される。コンテンツサーバ、ライセンスサーバ、あるいはショップサーバ等、各デバイスとのデータ送受信を行なう機関は、図3の点線で囲んだ部分、すなわちデバイス0,
15 1, 2, 3を1つのグループとして一括してデータを送付する処理を実行する。このようなグループは、図3のツリー中に複数存在する。コンテンツサーバ、ライセンスサーバ、あるいはショップサーバ等、各デバイスとのデータ送受信を行なう機関は、メッセージデータ配信手段として機能する。

20

 なお、ノードキー、リーフキーは、ある1つの鍵管理センター機能を持つ管理システムによって統括して管理してもよいし、各グループに対する様々なデータ送受信を行なうプロバイダ、決済機関等のメッセージデータ配信手段によってグループごとに管理する構成としてもよい。これら
25 のノードキー、リーフキーは例えばキーの漏洩等の場合に更新処理が実行され、この更新処理は鍵管理センター機能を持つ管理システム、プロバイダ、決済機関等が実行する。

 このツリー構造において、図3から明らかなように、1つのグループ

- に含まれる3つのデバイス0, 1, 2, 3はデバイスノードキー (DNK : Device Node Key) として共通のキーK00、K0、KRを含むデバイスノードキー (DNK : Device Node Key) を保有する。このノードキー共有構成を利用することにより、例えば共通のキーをデバイス0, 1, 2, 3のみに提供することが可能となる。たとえば、共通に保有するノードキーK00は、デバイス0, 1, 2, 3に共通する保有キーとなる。また、新たなキーKnewをノードキーK00で暗号化した値Enc (K00, Knew) を、ネットワークを介してあるいは記録媒体に格納してデバイス0, 1, 2, 3に配布すれば、デバイス0, 1, 2, 3のみが、それぞれのデバイスにおいて保有する共有ノードキーK00を用いて暗号Enc (K00, Knew) を解いて新たなキーKnewを得ることが可能となる。なお、Enc (Ka, Kb) はKbをKaによって暗号化したデータであることを示す。
- 15 また、ある時点tにおいて、デバイス3の所有する鍵：K0011, K001, K00, K0, KRが攻撃者（ハッカー）により解析されて露呈したことが発覚した場合、それ以降、システム（デバイス0, 1, 2, 3のグループ）で送受信されるデータを守るために、デバイス3をシステムから切り離す必要がある。そのためには、ノードキー：K001, K00, K0, KRをそれぞれ新たな鍵K(t)001, K(t)00, K(t)0, K(t)Rに更新し、デバイス0, 1, 2にその更新キーを伝える必要がある。ここで、K(t)aaaは、鍵Kaaaの世代 (Generation) : tの更新キーであることを示す。
- 25 更新キーの配布処理について説明する。キーの更新は、例えば、図4(A)に示す有効化キーブロック (EKB : Enabling Key Block) と呼ばれるブロックデータによって構成されるテーブルをたとえばネットワーク、あるいは記録媒体に格納してデバイス0, 1, 2に供給することによって実行される。なお、有効化キーブロック (EKB) は、図3に示すよ

うなツリー構造を構成する各リーフに対応するデバイスに新たに更新されたキーを配布するための暗号化キーによって構成される。有効化キーブロック (E K B) は、キー更新ブロック (K R B : Key Renewal Block) と呼ばれることもある。

5

図 4 (A) に示す有効化キーブロック (E K B) には、ノードキーの更新の必要なデバイスのみが更新可能なデータ構成を持つブロックデータとして構成される。図 4 の例は、図 3 に示すツリー構造中のデバイス 0, 1, 2 において、世代 t の更新ノードキーを配布することを目的として形成されたブロックデータである。図 3 から明らかなように、デバイス 0, デバイス 1 は、更新ノードキーとして $K(t) 00$ 、 $K(t) 0$ 、 $K(t) R$ が必要であり、デバイス 2 は、更新ノードキーとして $K(t) 001$ 、 $K(t) 00$ 、 $K(t) 0$ 、 $K(t) R$ が必要である。

図 4 (A) の E K B に示されるように E K B には複数の暗号化キーが含まれる。最下段の暗号化キーは、 $Enc(K0010, K(t) 001)$ である。これはデバイス 2 の持つリーフキー $K0010$ によって暗号化された更新ノードキー $K(t) 001$ であり、デバイス 2 は、自身の持つリーフキーによってこの暗号化キーを復号し、 $K(t) 001$ を得ることができる。また、復号により得た $K(t) 001$ を用いて、図 4 (A) の下から 2 段目の暗号化キー $Enc(K(t) 001, K(t) 00)$ を復号可能となり、更新ノードキー $K(t) 00$ を得ることができる。以下順次、図 4 (A) の上から 2 段目の暗号化キー $Enc(K(t) 00, K(t) 0)$ を復号し、更新ノードキー $K(t) 0$ 、図 4 (A) の上から 1 段目の暗号化キー $Enc(K(t) 0, K(t) R)$ を復号し $K(t) R$ を得る。一方、デバイス $K0000$ 、 $K0001$ は、ノードキー $K000$ は更新する対象に含まれておらず、更新ノードキーとして必要なのは、 $K(t) 00$ 、 $K(t) 0$ 、 $K(t) R$ である。デバイス $K0000$ 、 $K0001$ は、図 4 (A) の上から 3 段目の暗号化キー

25

$E_{nc}(K000, K(t)00)$ を復号し $K(t)00$ を取得し、
 以下、図4(A)の上から2段目の暗号化キー $E_{nc}(K(t)00, K(t)0)$ を復号し、更新ノードキー $K(t)0$ 、図4(A)の上から1段目の暗号化キー $E_{nc}(K(t)0, K(t)R)$ を復号し $K(t)$
 5 R を得る。このようにして、デバイス0, 1, 2は更新した鍵 $K(t)R$ を得ることができる。なお、図4(A)のインデックスは、復号キーとして使用するノードキー、リーフキーの絶対番地を示す。

図3に示すツリー構造の上位段のノードキー： $K(t)0, K(t)$
 10 R の更新が不要であり、ノードキー $K00$ のみの更新処理が必要である場合には、図4(B)の有効化キーブロック(EKB)を用いることで、更新ノードキー $K(t)00$ をデバイス0, 1, 2に配布することができる。

図4(B)に示すEKBは、例えば特定のグループにおいて共有する新たなコンテンツキーを配布する場合に利用可能である。具体例として、図3に点線で示すグループ内のデバイス0, 1, 2, 3がある記録媒体を用いており、新たな共通のコンテンツキー $K(t)_{con}$ が必要であるとすると、このとき、デバイス0, 1, 2, 3の共通のノードキー $K0$
 20 0 を更新した $K(t)00$ を用いて新たな共通の更新コンテンツキー： $K(t)_{con}$ を暗号化したデータ $E_{nc}(K(t), K(t)_{con})$ を図4(B)に示すEKBとともに配布する。この配布により、デバイス4など、その他のグループの機器においては復号されないデータとしての配布が可能となる。

25

すなわち、デバイス0, 1, 2はEKBを処理して得た $K(t)00$ を用いて上記暗号文を復号すれば、 t 時点でのキー、例えばコンテンツの暗号化復号化に適用するコンテンツキー $K(t)_{con}$ を得ることが可能になる。

[3. E K Bを使用したキーの配布]

図 5 に、 t 時点でのキー、例えばコンテンツの暗号化復号化に適用するコンテンツキー $K(t)_{con}$ を得る処理例として、 $K(t)_{00}$ を用いて新たな共通のコンテンツキー $K(t)_{con}$ を暗号化したデータ $Enc(K(t)_{00}, K(t)_{con})$ と図 4 (B) に示す E K B とを記録媒体を介して受領したデバイス 0 の処理例を示す。すなわち E K B による暗号化メッセージデータをコンテンツキー $K(t)_{con}$ とした例である。

図 5 に示すように、デバイス 0 は、記録媒体に格納されている世代： t 時点の E K B と自分があらかじめ格納しているノードキー K_{000} を用いて上述したと同様の E K B 処理により、ノードキー $K(t)_{00}$ を生成する。さらに、復号した更新ノードキー $K(t)_{00}$ を用いて更新コンテンツキー $K(t)_{con}$ を復号して、後にそれを使用するために自分だけが持つリーフキー K_{0000} で暗号化して格納する。

[4. E K B のフォーマット]

図 6 に有効化キープブロック (E K B) のフォーマット例を示す。バージョン 201 は、有効化キープブロック (E K B) のバージョンを示す識別子である。なお、バージョンは最新の E K B を識別する機能とコンテンツとの対応関係を示す機能を持つ。デプスは、有効化キープブロック (E K B) の配布先のデバイスに対する階層ツリーの階層数を示す。データポインタ 203 は、有効化キープブロック (E K B) 中のデータ部の位置を示すポインタであり、タグポインタ 204 はタグ部の位置、署名ポインタ 205 は署名の位置を示すポインタである。

データ部 206 は、例えば更新するノードキーを暗号化したデータを格納する。例えば図 5 に示すような更新されたノードキーに関する各暗

号化キー等を格納する。

タグ部 207 は、データ部に格納された暗号化されたノードキー、リーフキーの位置関係を示すタグである。このタグの付与ルールを図 7 を用いて説明する。図 7 では、データとして先に図 4 (A) で説明した有効化キーブロック (EKB) を送付する例を示している。この時のデータは、図 7 の表 (b) に示すようになる。このときの暗号化キーに含まれるトップノードのアドレスをトップノードアドレスとする。この場合は、ルートキーの更新キー $K(t)R$ が含まれているので、トップノードアドレスは KR となる。このとき、例えば最上段のデータ $Enc(K(t)0, K(t)R)$ は、図 7 の (a) に示す階層ツリーに示す位置にある。ここで、次のデータは、 $Enc(K(t)00, K(t)0)$ であり、ツリー上では前のデータの左下の位置にある。データがある場合は、タグが 0、ない場合は 1 が設定される。タグは {左 (L) タグ, 右 (R) タグ} として設定される。最上段のデータ $Enc(K(t)0, K(t)R)$ の左にはデータがあるので、L タグ = 0、右にはデータがないので、R タグ = 1 となる。以下、すべてのデータにタグが設定され、図 7 (c) に示すデータ列、およびタグ列が構成される。

タグは、データ $Enc(Kxxx, Kyyy)$ がツリー構造のどこに位置しているのかを示すために設定されるものである。データ部に格納されるキーデータ $Enc(Kxxx, Kyyy)...$ は、単純に暗号化されたキーの羅列データに過ぎないので、上述したタグによってデータとして格納された暗号化キーのツリー上の位置を判別可能としたものである。上述したタグを用いずに、先の図 4 で説明した構成のように暗号化データに対応させたノード・インデックスを用いて、例えば、

0 : $Enc(K(t)0, K(t)root)$

00 : $Enc(K(t)00, K(t)0)$

000 : $Enc(K((t)000, K(T)00)$

- ... のようなデータ構成とすることも可能であるが、このようなインデックスを用いた構成とすると冗長なデータとなりデータ量が増大し、ネットワークを介する配信等においては好ましくない。これに対し、上述したタグをキー位置を示す索引データとして用いることにより、少ないデータ量でキー位置の判別が可能となる。

- 図 6 に戻って、E K B フォーマットについてさらに説明する。署名 (Signature) 2 0 8 は、有効化キーブロック (E K B) を発行した例えば鍵管理センター機能を持つ管理システム、コンテンツサーバ、ライセンスサーバ、あるいはショップサーバ等が実行する電子署名である。E K B を受領したデバイスは署名検証によって正当な有効化キーブロック (E K B) 発行者が発行した有効化キーブロック (E K B) であることを確認する。

15 [5 . ツリーのカテゴリ分類]

ノードキー等を定義している階層ツリー構造を各デバイスのカテゴリ毎に分類して効率的なキー更新処理、暗号化キー配信、データ配信を実行する構成について、以下説明する。

- 20 図 8 に階層ツリー構造のカテゴリの分類の一例を示す。図 8 において、階層ツリー構造の最上段には、ルートキー K r o o t 3 0 1 が設定され、以下の中間段にはノードキー 3 0 2 が設定され、最下段には、リーフキー 3 0 3 が設定される。各デバイスは個々のリーフキーと、リーフキーからルートキーに至る一連のノードキー、ルートキーを保有する。

25

ここで、一例として最上段から第 M 段目のあるノードをカテゴリノード 3 0 4 として設定する。すなわち第 M 段目のノードの各々を特定カテゴリのデバイス設定ノードとする。第 M 段の 1 つのノードを頂点として以下、M + 1 段以下のノード、リーフは、そのカテゴリに含まれるデバ

イスに関するノードおよびリーフとする。

例えば図 8 の第 M 段目の 1 つのノード 305 にはカテゴリ [メモリスティック (商標)] が設定され、このノード以下に連なるノード、リーフはメモリスティックを使用した様々なデバイスを含むカテゴリ専用のノードまたはリーフとして設定される。すなわち、ノード 305 以下を、メモリスティックのカテゴリに定義されるデバイスの関連ノード、およびリーフの集合として定義する。

10 さらに、M 段から数段分下位の段をサブカテゴリノード 306 として設定することができる。例えば図に示すようにカテゴリ [メモリスティック] ノード 305 の 2 段下のノードに、メモリスティックを使用したデバイスのカテゴリに含まれるサブカテゴリノードとして、[再生専用器] のノードを設定する。さらに、サブカテゴリノードである再生専用器のノード 306 以下に、再生専用器のカテゴリに含まれる音楽再生機能付き電話のノード 307 が設定され、さらにその下位に、音楽再生機能付き電話のカテゴリに含まれる [PHS] ノード 308 と [携帯電話] ノード 309 を設定することができる。

20 さらに、カテゴリ、サブカテゴリは、デバイスの種類のみならず、例えばあるメーカー、コンテンツプロバイダ、決済機関等が独自に管理するノード、すなわち処理単位、管轄単位、あるいは提供サービス単位等、任意の単位（これらを総称して以下、エンティティと呼ぶ）で設定することが可能である。例えば 1 つのカテゴリノードをゲーム機器メーカーの販売するゲーム機器 XYZ 専用の頂点ノードとして設定すれば、メーカーの販売するゲーム機器 XYZ にその頂点ノード以下の下段のノードキー、リーフキーを格納して販売することが可能となり、その後、暗号化コンテンツの配信、あるいは各種キーの配信、更新処理を、その頂点ノードキー以下のノードキー、リーフキーによって構成される有効化

キーブロック（EKB）を生成して配信し、頂点ノード以下のデバイスに対してのみ利用可能なデータが配信可能となる。

このように、1つのノードを頂点として、以下のノードをその頂点ノードに定義されたカテゴリ、あるいはサブカテゴリの関連ノードとして設定する構成とすることにより、カテゴリ段、あるいはサブカテゴリ段の1つの頂点ノードを管理するメーカー、コンテンツプロバイダ等がそのノードを頂点とする有効化キーブロック（EKB）を独自に生成して、頂点ノード以下に属するデバイスに配信する構成が可能となり、頂点ノードに属さない他のカテゴリのノードに属するデバイスには全く影響を及ぼさずにキー更新を実行することができる。

本発明のシステムにおいては、図9に示されるように、ツリー構成のシステムで、キー管理が行われる。図9の例では、 $8 + 2^4 + 3^2$ 段のノードがツリー構造とされ、ルートノードから下位の8段までの各ノードにカテゴリが対応される。ここにおけるカテゴリとは、例えばメモリスティックなどの半導体メモリを使用する機器のカテゴリ、デジタル放送を受信する機器のカテゴリといったカテゴリを意味する。そして、このカテゴリノードのうちの1つのノードに、ライセンスを管理するシステムとして本システム（Tシステムと称する）が対応する。

すなわち、このTシステムのノードよりさらに下の階層の 2^4 段のノードに対応するキーが、サービスプロバイダ、あるいはサービスプロバイダが提供するサービスに適用される。この例の場合、これにより、 2^4 （約16メガ）のサービスプロバイダあるいはサービスを規定することができる。さらに、最も下側の 3^2 段の階層により、 2^3 （約4ギガ）のユーザ（あるいはユーザデバイス）を規定することができる。最下段の 3^2 段のノードからTシステムのノードまでのパス上の各ノードに対応するキーが、DNK（Device Node Key）を構成し、最下段のリー

フに対応する I D がリーフ I D とされる。

例えば、コンテンツを暗号化したコンテンツキーは更新されたルートキー K R ' によって暗号化され、上位の階層の更新ノードキーは、その
5 直近の下位の階層の更新ノードキーを用いて暗号化され、E K B 内に配置される。E K B における末端から 1 つ上の段の更新ノードキーは E K B の末端のノードキーあるいはリーフキーによって暗号化され、E K B 内に配置される。

10 ユーザデバイスは、サービスデータに記述されている D N K のいずれかのキーを用いて、コンテンツデータとともに配布される E K B 内に記述されている直近の上位の階層の更新ノードキーを復号し、復号して得たキーを用いて、E K B 内に記述されているさらにその上の階層の更新ノードキーを復号する。以上の処理を順次行うことで、ユーザデバイス
15 は、更新ルートキー K R ' を得ることができる。

上述したように、ツリーのカテゴリ分類により、1 つのノードを頂点として、以下のノードをその頂点ノードに定義されたカテゴリ、あるいはサブカテゴリの関連ノードとして設定した構成が可能となり、カテ
20 ゴリ段、あるいはサブカテゴリ段の 1 つの頂点ノードを管理するメーカー、サービスプロバイダ等がそのノードを頂点とする有効化キーブロック (E K B) を独自に生成して、頂点ノード以下に属するデバイスに配信する構成が実現される。

25 さらに、上述のツリー構成のデバイス管理による E K B 配信システムを適用して、複数のカテゴリに基づく E K B 配信構成を採用したコンテンツ配信および利用形態について説明する。

図 1 0 を参照して 2 つのカテゴリについて説明する。図 1 0 に示すよ

うに、ルートノード 3 5 0 の下段に T システムノード 3 5 1 を設定し、その下段に T サービスノード 3 5 2、および T ハードノード 3 5 3 を設定する。T ハードノード 3 5 3 を頂点としたツリーは、ユーザデバイス機器自体をリーフ 3 5 5 として設定し、機器を対象として発行するハード対応 E K B [E K B (H)] を配信するカテゴリツリーである。一方、T サービスノード 3 5 2 を頂点としたツリーは、ユーザデバイス機器に提供するサービスに対応して発行するサービス対応 E K B [E K B (S)] を配信するカテゴリツリーである。

- 10 ハード対応 E K B [E K B (H)]、サービス対応 E K B [E K B (S)] とも、それぞれ正当な権限を持つデバイスに対して与えられる D N K (Device Node Key) すなわち、リーフから T システムのノードまでのパス上の各ノードに対応するキーを有することで、各 E K B の復号が可能となる。

15

[6 . コンテンツ購入および試聴処理]

次に、クライアントがコンテンツを購入または試聴する際の処理の詳細について、図 1 1 以下を参照して説明する。

- 20 図 1 1 は、クライアントアプリケーション、ブラウザを有する P C 等のクライアントと、ショップサーバ、コンテンツサーバ、ライセンスサーバ、および管理システムとの間で実行されるコンテンツ購入処理における通信シーケンスの初期ステップを示している。以下、シーケンス図に示す処理について説明する。

- 25 まず、クライアント側において、コンテンツの購入を行なおうとするユーザは、自己の P C 等の通信可能な情報処理装置に U R L を指定 (ステップ (1)) し、ブラウザが介してショップサーバの提示するコンテンツリスト画面 (ショップページ) を読み出し (ステップ (2)) て、ディスプレイに表示 (ステップ (3)) する。

クライアントは、ショップサーバの提示するコンテンツリストからコンテンツを選択して、さらに、購入または試聴どちらかの指定（ステップ（４））を行なって、ブラウザを介してショップサーバに要求データを送信（ステップ（５））する。要求データには、コンテンツＩＤ（ＣＩＤ）、ショップサーバ識別子（ＳｈｏｐＩＤ）、および購入または試聴どちらかの指定データが含まれる。

ショップサーバは、クライアントからのコンテンツ購入、または試聴要求を受信すると、管理システムに対して、コンテンツの提供の可否判定を要求（ステップ（６））する。この判定要求には、コンテンツＩＤ（ＣＩＤ）、ショップサーバ識別子（ＳｈｏｐＩＤ）が含まれる。

管理システムは、コンテンツの提供の可否判定要求を受信すると、トランザクションＩＤ（ＴＩＤ）の発行処理（ステップ（７））を実行する。トランザクションＩＤ（ＴＩＤ）の発行処理の詳細を図１２のフローを参照して説明する。

管理システムは、まず、ステップＳ１０１において、乱数を発生し、発生乱数に基づいて、トランザクションＩＤ（ＴＩＤ）を生成する。次に、ステップＳ１０２において、生成したトランザクションＩＤ（ＴＩＤ）と、ショップサーバから指定されたコンテンツＩＤ（ＣＩＤ）とを対応付けてトランザクションデータとして記憶部に格納する。次に、生成したトランザクションＩＤ（ＴＩＤ）をショップサーバに対して出力、発行する。

図１１のシーケンス図に戻る。管理システムは、トランザクションＩＤ（ＴＩＤ）の生成後、生成したトランザクションＩＤ（ＴＩＤ）と価格情報をＴＩＤ情報としてショップサーバに送信（ステップ（８））す

る。ただし、価格情報は、コンテンツ購入時においてのみ要求される情報であり、コンテンツ試聴処理に際しては、含まれない。T I D 情報を受信したショップサーバは、クライアントからの要求がコンテンツ購入である場合に、T I D 情報に含まれる価格に基づいて、課金処理（ステップ（9））を実行する。

クライアントからの要求がコンテンツ購入ではなく、コンテンツ試聴要求である場合には、この課金処理（ステップ（9））は省略される。

次に、図 1 3 のシーケンス図を参照して継続する処理について説明する。ショップサーバは、コンテンツ購入処理においては、課金が行われたことを条件として、またコンテンツ試聴処理においては、管理システムからの T I D 情報の受信を条件として、購入または試聴要求対象のコンテンツのダウンロード許可要求を管理システムに対して送信（ステップ（10））する。

管理システムは、ダウンロード許可要求を受信すると、ダウンロード許可要求検証処理（ステップ（11））を実行する。ダウンロード許可要求検証処理の詳細を図 1 4 のフローを参照して説明する。

20

管理システムは、まず、ステップ S 2 0 1 において、受信したダウンロード許可要求に含まれるトランザクション I D（T I D）と、先に生成し、記憶部に格納したトランザクション I D（T I D）とを照合し、さらにステップ S 2 0 2 において、照合の成立したトランザクション I D（T I D）に対応して記録されたコンテンツ I D（C I D）を取得し、ステップ S 2 0 3 において、C I D に対応するコンテンツのダウンロード許可を発行する。

25

図 1 3 のシーケンス図に戻り、説明を続ける。管理システムは、ダウ

ンロード許可要求検証処理（ステップ（11））の後、コンテンツのダウンロード許可をショップサーバに対して発行（ステップ（12））する。ダウンロード許可には、トランザクションID（TID）、コンテンツサーバURL（CURL）、ライセンスサーバURL（LURL）、コンテンツID（CID）、利用権情報ID（UID）、商品（コンテンツ）URL（SURL）、サービスIDが含まれる。

ショップサーバは、管理システムからダウンロード許可を受信すると、クライアントアプリケーションにおけるコンテンツの利用（再生処理等）プログラムを起動させるための起動ファイルを生成してクライアントのブラウザを介してクライアントアプリケーションに対して送付する。

起動ファイルの例を図15を参照して説明する。起動ファイル360は、先に管理システムが生成したトランザクションID（TID）、クライアントが購入あるいは試聴するコンテンツID（CID）、管理システムが生成したダウンロード許可情報に含まれる利用権情報ID（UID）、管理システムが生成したダウンロード許可情報に含まれるサービスID、ライセンスサーバURL、商品（コンテンツ）URL、さらに、処理が購入であるか試聴であるかの識別データが含まれる。

なお、処理が購入であるか試聴であるかの識別データとしては、起動ファイルに設定される拡張子を購入であるか試聴であるかによって区別して設定し、これをクライアントアプリケーションが判別して、それぞれのアプリケーションを起動するようにしてもよい。

クライアントアプリケーションは、起動ファイルに応じて、アプリケーションを起動（ステップ（15））する。

クライアントアプリケーションにおいて実行するアプリケーション
起動処理について、図 1 6 を参照して説明する。ステップ S 3 0 1 に
いて、まず、起動ファイルに設定されたサービス I D 対応のサービスデ
ータをクライアントシステムとしての情報処理装置に格納されている
5 か否かを判定する。

サービスデータは、クライアントが各種のサービス、例えばコンテン
ツ利用サービスを受領したい場合、ライセンスサーバから受領するもの
で、例えば特定のサービスプロバイダの提供サービスの一括したサービ
10 ス利用権を認めるデータである。図 1 7 (a) にサービスデータのデー
タ構成例を示す。

図 1 7 (a) に示すように、サービスデータ 3 7 0 には、E K B 配信
ツリーにおいて設定されるクライアントに固有のリーフ I D、サービス
15 識別子としてのサービス I D、さらにデバイスノードキー (D N K) を
ルートキー (K r o o t) で暗号化したデータ、E (K r o o t , D N
K) が含まれる。サービスデータを受領するためには、クライアントは、
ライセンスサーバに対する登録処理が必要とされる。登録処理は、図 1
3 に示す処理ステップ (1 5)、(1 6) の処理に対応する。

20

図 1 6 に示すステップ S 3 0 1 において、サービス I D 対応のサービ
スデータを保有していないと判定すると、ステップ S 3 0 2 において登
録処理を実行して、サービスデータを受領する。

25 さらに、この登録処理時に、デフォルト利用権情報がライセンスサー
バからクライアントに対して発行される。利用権情報は、通常は、購入
コンテンツの利用条件を格納し、コンテンツの購入に対応して発行され
るものであるが、デフォルト利用権情報は、コンテンツの購入を条件と
して発行するものではなく、クライアントの登録処理、あるいはサービ

スデータの発行処理を条件として発行する。このデフォルト利用権情報は、後段で説明するコンテンツの試聴処理の際の有効なコンテンツ利用権情報として適用される。

- 5 図 1 7 (b) に利用権情報のデータ構成例を示す。図 1 7 (b) に示すように、利用権情報 3 7 1 には、利用権情報識別子としての利用権情報 I D、発行日時情報としてのタイムスタンプ、クライアントに固有のリーフ I D、コンテンツ対応である場合は、コンテンツ I D、さらに、利用条件対象コンテンツ種別情報が格納される。

10

デフォルト利用権情報の場合は、特定の購入コンテンツに対応して発行されるものではないため、コンテンツ I D は省略、あるいは試聴可能なコンテンツに共通な I D が設定される。また、利用条件対象コンテンツ種別情報として、例えば試聴フラグがオン (O N) として設定された
15 コンテンツについての利用が許可される設定とする。コンテンツ 3 7 2 には図 1 7 (c) に示すように、試聴フラグ 3 7 3 が設定され、試聴フラグ 3 7 3 がオン (O N) の設定コンテンツであれば、試聴が許可されたコンテンツであることを示し、試聴フラグがオフ (O F F) の設定コンテンツであれば、試聴が許可されていないコンテンツであることを示
20 す。

クライアントアプリケーションは、試聴コンテンツ再生時には、デフォルト利用権情報を参照して、再生許可の有無を判定するとともに、コンテンツのフラグの検証を実行して、コンテンツの再生を行なうことになる。この処理については、後段で説明する。

25

図 1 6 の処理フローに戻りアプリケーション起動処理の処理手順について説明する。ステップ S 3 0 2 において、登録処理、すなわちライセンスサーバからのサービスデータ、デフォルト利用権情報の取得が終

了すると、ステップ S 3 0 3 において、ショップサーバから受信した起動ファイルが、購入用アプリケーションの起動ファイルであるか、試聴用アプリケーションの起動ファイルであるかを判別する。購入用アプリケーションの起動ファイルである場合は、ステップ S 3 0 4 に進み購入用アプリケーションを実行し、試聴用アプリケーションの起動ファイルである場合は、ステップ S 3 0 5 に進み試聴用アプリケーションを実行する。

次に、購入用アプリケーションの実行シーケンスについて、図 1 8 のシーケンス図を参照して説明する。

購入処理実行の場合、クライアントアプリケーションは、コンテンツダウンロード要求をコンテンツサーバに対して実行（ステップ（2 1））する。これは、先にクライアントが購入要求を行なったコンテンツであり、利用権情報（図 1 7（b）参照）に記録されたコンテンツ ID（C I D）に対応するコンテンツである。クライアントアプリケーションは、コンテンツ ID（C I D）によりコンテンツを指定してコンテンツダウンロード要求をコンテンツサーバに対して実行する。

コンテンツサーバは、コンテンツダウンロード要求を受信すると、C I D に対応するコンテンツ情報をクライアントに送信（ステップ（2 2））する。このコンテンツ情報は、暗号化コンテンツを含み、図 1 7（c）に示すように、コンテンツキー：K c で暗号化されたコンテンツデータ：E n c（K c，C o n t e n t）、コンテンツキー：K c をルートキー：K r o o t で暗号化したデータ：E n c（K r o o t，K c）、さらに：ルートキー：K r o o t を取得するための E K B、さらに試聴フラグデータ、サービス I D 等の情報が付加されたファイルである。

コンテンツ情報を受領したクライアントは、受信コンテンツに対応す

る利用権情報 (U s a g e R i g h t) の取得要求をライセンスサーバに対して送信 (ステップ (23)) する。この要求には、先にショップサーバから受領した起動ファイル (図15参照) 中に含まれる利用権情報ID (U I D)、クライアント識別データとしてのリーフID、および先にショップサーバから受領した起動ファイル (図15参照) 中に含まれるトランザクションID (T I D) が含まれる。

ライセンスサーバは、利用権情報 (U s a g e R i g h t) の取得要求を受信すると、管理システムに対して、注文照会処理 (ステップ (24)) を行なう。この要求には、利用権情報ID (U I D)、トランザクションID (T I D) が含まれる。注文照会を受信した管理サーバは、注文照会応答として、利用権情報ID (U I D) に対応する利用条件を設定した応答情報をライセンスサーバに送信 (ステップ (25)) する。

15 応答情報を受信したライセンスサーバは、コンテンツ利用条件を設定した利用権情報 (U s a g e R i g h t) を生成して、クライアントに対して発行 (ステップ (26)) する。なお、コンテンツ利用条件とは、コンテンツの再生回数、期限、外部機器に対するコピー、チェックアウト処理等の各種処理の許可情報によって構成される。

20

利用権情報 (U s a g e R i g h t) を受信したクライアントは、先にコンテンツサーバから受信したコンテンツについて、利用権情報 (U s a g e R i g h t) に記録された利用条件に基づいてコンテンツの利用が可能となる。ユーザからコンテンツID (C I D)、利用権情報 (U s a g e R i g h t) IDを指定したコンテンツ再生要求 (ステップ (27)) があると、クライアントアプリケーションは、利用条件に従ったコンテンツ再生を実行 (ステップ (28)) する。

基本的なコンテンツ再生処理の手順について、図19を参照して説明

する。前述の説明から理解されるように、コンテンツサーバ382からクライアント383に対してコンテンツが提供されるとともに、ライセンスサーバ381からクライアント383にライセンスとして、サービスデータ、利用権情報 (U s a g e R i g h t) が与えられる。

5

コンテンツは、コンテンツキー: K cにより、暗号化されており (E n c (K c, C o n t e n t)、コンテンツキーK cは、E K Bから取得可能なルートキーK r o o tから得られるキーである。

- 10 クライアント383は、ライセンスサーバから受領したサービスデータからデバイスノードキー (D N K) を取得し、取得したD N Kに基づいてコンテンツファイルのE K Bを復号して、ルートキー: K r o o t を取得し、さらに、取得したルートキー: K r o o tを用いて、E n c (K r o o t, K c) を復号してコンテンツキー: K cを取得し、取得
- 15 したコンテンツキー: K cをにより暗号化コンテンツ: E n c (K c, C o n t e n t) の復号処理を実行してコンテンツを取得し、再生する。

サービスデータ、利用権情報 (U s a g e R i g h t) と対応付けたコンテンツ再生処理の詳細について、図20を参照して説明する。

20

図20は、ハード対応E K B [E K B (H)]、サービス対応E K B [E K B (S)] を適用したコンテンツの復号処理に基づくコンテンツ利用処理シーケンスを説明した図である。

- 25 図20に示すサービスデータ401、および利用権情報403は、ライセンスサーバから受領するデータであり、暗号化コンテンツファイル402はコンテンツサーバから受領するデータである。サービスデータ401は、リーフ識別子としてのリーフI D、適用するE K Bのバージョン、さらに、サービス対応E K B [E K B (S)] の復号に必要なサ

ービス対応デバイスノードキー (SDNK) を、ハード対応カテゴリツリーに対応して設定されるルートキー K_{root} ' によって暗号化したデータ $E(K_{root}', SDNK)$ を格納している。

- 5 暗号化コンテンツファイル 402 は、サービス対応のカテゴリツリーに対応して設定されるルートキー K_{root} を格納したサービス対応 $EKB[EKB(S)]$ 、ルートキー K_{root} でコンテンツ ID (CID) と、コンテンツ暗号処理および復号処理に適用するコンテンツキー (K_c) とを暗号化したデータ $E(K_{root}, CID + K_c)$ 、および、
10 コンテンツ (Content) をコンテンツキー K_c で暗号化したデータ $E(K_c, Content)$ を含むファイルである。

- また、利用権情報 403 は、リーフ ID と、コンテンツの利用条件情報を格納したデータである。コンテンツの利用条件情報には、コンテンツ
15 ツに対応して設定される利用期間、利用回数、コピー制限等の様々な利用条件が含まれる。利用権情報 403 を受領したユーザデバイスは、利用権情報をコンテンツに対応するセキュリティ情報として格納するか、あるいは、コンテンツの索引データとしての AV インデックスファイル内に格納する。

20

- 例えば、PC 等の大容量の記憶手段を有し、プロセッサ等の処理能力が高いユーザデバイスにおいては、利用権情報をコンテンツに対応するセキュリティ情報として格納することが可能であり、すべての利用権情報を格納して、コンテンツ利用の際にすべての利用権情報を参照した処理を行なうことが好ましい。一方、大容量の記憶手段を持たず、またプロセッサ等の処理能力が低いポータブルデバイス (PD) 等のユーザデバイスにおいては、選択された情報からなる利用権情報 403 をコンテンツの索引データとしての AV インデックスファイル内に格納して、コンテンツ利用の際に AV インデックスファイル内の利用条件情報を参
25

照した処理を行なう等の処理が可能である。

ユーザデバイスは、図 20 に示すステップ S 5 0 1 において、ハード
対応のデバイスノードキー (HDNK) 4 1 2 を適用して、ハード対応
5 の EKB (H) 4 1 1 の復号処理を実行し、EKB (H) 4 1 1 から、
ハード対応カテゴリツリーに対応して設定されるルートキー K r o o
t' を取得する。DNK を適用した EKB の処理は、先に図 5 を参照し
て説明した手法に従った処理となる。

10 次に、ステップ S 5 0 2 において、EKB (H) から取り出したルー
トキー K r o o t' を用いて、サービスデータ 4 0 1 内の暗号化データ
E (K r o o t', SDNK) の復号処理を実行し、サービス対応 EKB
B [EKB (S)] の処理 (復号) に適用するデバイスノードキー (S
DNK) を取得する。

15 次に、ステップ S 5 0 3 において、サービスデータから取り出したデ
バイスノードキー (SDNK) を用いて、暗号化コンテンツファイル 4
0 2 内に格納されたサービス対応 EKB [EKB (S)] の処理 (復号)
を実行し、サービス対応 EKB [EKB (S)] 内に格納されたサービ
20 ス対応カテゴリツリーに対応して設定されるルートキー K r o o t を
取得する。

次に、ステップ S 5 0 4 において、サービス対応 EKB [EKB (S)]
から取り出したルートキー K r o o t を用いて、暗号化コンテンツファ
25 イル 4 0 2 内に格納された暗号化データ E (K r o o t, CID + Kc)
の復号処理を実行し、コンテンツ ID (CID) と、コンテンツキー (K
c) を取得する。

次に、ステップ S 5 0 5 において、暗号化コンテンツファイル 4 0 2

から取り出したコンテンツID (CID) と、利用権情報内に格納されたコンテンツIDのマッチング (照合) 処理を実行する。マッチング処理により、コンテンツの利用が可能であることが確認されると、ステップS506において、暗号化コンテンツファイル402から取り出した
5 コンテンツキー (Kc) を適用して、暗号化コンテンツファイル402に格納された暗号化コンテンツE (Kc, Content) を復号してコンテンツの再生を行なう。

上述したように、コンテンツ利用機器としてのハードウェアに対応して
10 て設定されたカテゴリツリーに対応するEKBとしてのハード対応EKB [EKB (H)] と、コンテンツ利用サービスに対応して設定されたカテゴリツリーに対応するEKBとしてのサービス対応EKB [EKB (S)] をそれぞれ個別にユーザに対して提供し、それぞれのEKBに対する正当なDNKを有するユーザのみがサービスの利用を行なう
15 ことが可能となる。

サービス対応EKB [EKB (S)] を復号するためのDNK、すなわちSDNKは、コンテンツに対応したサービスデータ401として提供可能であり、またSDNKを正当なハードウェア対応のDNK、すな
20 わちHDNKを有する機器のみが取得可能なハード対応カテゴリツリーに対応して設定されるルートキーKroot' を適用して暗号化した構成としたので、正当なHDNKを有するユーザデバイスのみが、SDNKを取得でき、サービスが利用となる。

25 また、コンテンツ利用において、暗号化コンテンツファイル402から取得されるコンテンツ識別子 (CID) と、利用権情報から取得されるCIDとのマッチング処理を実行する構成としたので、利用権情報403を取得してCID情報を格納していることがコンテンツ再生プロセスの必須要件とすることが可能となり、利用条件に従ったコンテンツ

利用が実現される。

次に、クライアントアプリケーションの処理が試聴処理の実行アプリケーションである場合の処理について、図 2 1 のシーケンス図を参照して説明する。

試聴処理の場合、コンテンツ購入処理と同様、コンテンツ情報ファイル（図 1 9 参照）を取得してクライアントシステムの記憶部に格納し、その後、購入コンテンツと同様の処理によって再生することも可能であるが、記憶部に格納することなく、ストリーミング再生処理を実行する例について、図 2 1 を参照して説明する。

ストリーミング試聴処理実行の場合、クライアントアプリケーションは、コンテンツダウンロード要求をコンテンツサーバに対して実行（ステップ（3 1））する。これは、先にクライアントが試聴要求を行なったコンテンツである。クライアントアプリケーションは、コンテンツ ID（C I D）によりコンテンツを指定してコンテンツダウンロード要求をコンテンツサーバに対して実行する。

コンテンツサーバは、ストリーミング再生の場合には、コンテンツの部分データ（コンテンツパート）を次々にクライアントに対して送信（ステップ（3 2））する。コンテンツパートを受信したクライアントは、受信コンテンツに対する再生処理を実行（ステップ（3 3））し、後続のコンテンツパートの要求をコンテンツサーバに送信する。この処理を連続して実行することによりストリーミング再生が行なわれる。

試聴再生処理の手順について、図 2 2 のフローを参照して説明する。ステップ S 7 0 1 において、クライアントアプリケーションは、コンテンツサーバから受信した試聴コンテンツファイル中からサービス ID

を取得する。

次にステップ S 7 0 2 において、抽出したサービス ID に対応するデ
フォルト利用権情報 (D e f a u l t U s a g e R i g h t) (図
5 1 7 (b) 参照) の有無を判定する。デフォルト利用権情報は、クライ
アントの登録処理時に、サービスデータ (図 1 7 (a) 参照) とともに、
ライセンスサーバから送信される利用権情報であり、購入コンテンツに
対応して発行される利用権情報と異なり、試聴可能なコンテンツに対し
て利用される利用権情報である。

10

コンテンツ試聴においては、デフォルト利用権情報 (D e f a u l t
U s a g e R i g h t) を保有することが試聴実行許可条件であり、
デフォルト利用権情報を保有していない場合は、ステップ S 7 0 5 に進
み、エラーとしてコンテンツ再生が実行されず処理を終了する。

15

デフォルト利用権情報 (D e f a u l t U s a g e R i g h t)
が格納されている場合は、ステップ S 7 0 3 において、デフォルト利用
権情報を検証し、利用権情報の記録を確認する。デフォルト利用権情報
には、例えば試聴フラグオンのコンテンツの試聴許可、あるいは試聴可
20 能なコンテンツ ID 情報が格納されており、これらの情報を取得する。

次にステップ S 7 0 4 において、デフォルト利用権情報 (D e f a u
l t U s a g e R i g h t) の利用条件に基づいてコンテンツが再
生される。なお、再生処理は、前述の図 1 9、図 2 0 を参照して説明し
25 たように、コンテンツサーバから受信する暗号化コンテンツの復号処理
を伴う再生処理となる。

なお、コンテンツの購入処理を伴わない試聴処理においても、図 2 0
を参照して説明した購入コンテンツの再生と同様、E K B 処理に基づく

キー取得処理によってコンテンツ復号用のキーを取得することが必要となる。例えば、コンテンツ利用機器としてのハードウェアに対応して設定されたカテゴリツリーに対応するEKBとしてのハード対応EKB [EKB (H)] と、コンテンツ利用サービスに対応して設定された

5 カテゴリツリーに対応するEKBとしてのサービス対応EKB [EKB (S)] に対する正当なDNKを有するユーザのみがコンテンツ再生を実行可能とする構成が適用でき、試聴においても再生権限を限定した範囲として設定可能となる。

- 10 上述したように、クライアントは、ライセンスサーバに対する登録処理の際にデフォルト利用権情報 (Default Usage Right) を取得し、コンテンツの購入処理を伴わない、試聴処理の際にデフォルト利用権情報に基づいてコンテンツ再生を可能とした構成であるので、ユーザは、コンテンツの購入を実行することなく、コンテンツ
- 15 の試聴再生が可能となり、また、試聴が許可されるクライアントは、ライセンスサーバに対する登録処理を行ない、デフォルト利用権情報を有するクライアントに限定されることになるので、試聴データが無秩序に氾濫してしまうことが防止される。

- 20 なお、図21のシーケンス図では、ストリーミング再生の例を示したが、試聴データをクライアントの記憶媒体に格納し、再生時に、デフォルト利用権情報 (Default Usage Right) の有無を判定して、デフォルト利用権情報の記録に基づいて再生を行なう構成とすることも可能である。

25

[7. バックアップ／リストア処理]

次にクライアントが購入したコンテンツまたはコンテンツ利用権情報についてのバックアップ処理、リストア処理について説明する。

リストア処理は、クライアントのコンテンツ購入時、あるいは購入後の処理として実行されるコンテンツ対応のライセンス情報、すなわちサービスデータ、利用権情報の再取得、格納処理、あるいはコンテンツの再取得処理として実行される。

5

処理態様としては、サービスデータ、利用権情報、コンテンツのいずれかの再取得、あるいはこれらの全データの再取得が可能である。以下に説明する実施例においては、サービスデータ、利用権情報、コンテンツ全データの再取得、格納処理シーケンス例を説明するが、必ずしもこれら全データを再取得する処理に限らず、いずれかのデータのみを選択的に再取得することも可能である。

10

図 2 3 以下を参照して、バックアップ／リストア処理の詳細について説明する。図 2 3 は、クライアントアプリケーション、ブラウザを有する P C 等のクライアントと、ショップサーバ、コンテンツサーバ、ライセンスサーバ、および管理システムとの間で実行されるバックアップ／リストア処理における通信シーケンスの初期ステップを示している。以下、シーケンス図に示す処理について説明する。

15

クライアントは、前述したコンテンツ購入処理に従って、正規にコンテンツ購入を行なったものとする。図 2 3 に示すシーケンスは、コンテンツ購入に続いて実行されるシーケンスである。

20

コンテンツ購入処理を実行したクライアントは、バックアップ／リストアデータの取得のためのデータファイルとしてのリストア処理要求ファイル [r e s t o r e . d a t] を生成 (ステップ (5 0)) する。リストア処理要求ファイル [r e s t o r e . d a t] の構成を図 2 4 に示す。

25

図 2 4 に示すように、リストア処理要求ファイル [r e s t o r e . d a t] は、E K B 配信ツリーにおけるクライアント識別データとしてのリーフ I D と、ハッシュ (h a s h) 値、例えば M A C (Message Authentication Code) からなる検証データによって構成される。クライアントアプリケーションは、管理システムと共有する秘密の鍵を適用してリーフ I D に基づく検証用データとしてのハッシュ値あるいは M A C を算出し、リーフ I D と検証用データからなるリストア処理要求ファイル [r e s t o r e . d a t] を生成する。

- 10 メッセージ認証符号 (M A C : Message authentication Code) は、データの改竄検証用のデータとして生成されるものである。D E S 暗号処理構成を用いた M A C 値生成例を図 2 5 に示す。図 2 5 の構成に示すように対象となるメッセージを 8 バイト単位に分割し、(以下、分割されたメッセージを M 1、M 2、・・・、M N とする)、まず、初期値 (Initial Value (以下、I V とする)) と M 1 を排他的論理和する (その結果を I 1 とする)。次に、I 1 を D E S 暗号化部に入れ、鍵 (以下、K 1 とする) を用いて暗号化する (出力を E 1 とする)。続けて、E 1 および M 2 を排他的論理和し、その出力 I 2 を D E S 暗号化部へ入れ、鍵 K 1 を用いて暗号化する (出力 E 2)。以下、これを繰り返し、全てのメッセージに対して暗号化処理を施す。最後に出てきた E N がメッセージ認証符号 (M A C (Message Authentication Code)) となる。
- 15
20

- M A C 値は、その生成元データが変更されると、異なる値になり、検証対象のデータ (メッセージ) に基づいて生成した M A C と、記録されている M A C との比較を行い、一致していれば、検証対象のデータ (メッセージ) は変更、改竄がなされていないことが証明される。
- 25

図 2 3 のシーケンスに戻り説明を続ける。クライアントは、ブラウザを介して管理システムの提供するリストアページにアクセス (ステップ

(51)) し、管理システムは、リストアページをクライアントのブラウザに提示 (ステップ (52)) する。管理システムの提示するリストアページは、リストア処理要求ファイル [restore.dat] のアップロード処理を実行する機能を持つページである。

5

クライアントは、管理システムの提示するリストアページにおいて、クライアントアプリケーションの生成したリストア処理要求ファイル [restore.dat] をアップロードする。リストア処理要求ファイル [restore.dat] は、図24を参照して説明したように、EKB配信ツリーにおけるクライアント識別データとしてのリーフIDと、例えばMAC (Message Authentication Code) からなるハッシュ (hash) 値によって構成される。

10

管理システムは、リストア処理要求ファイル [restore.dat] を受信すると、クライアントと共有する秘密鍵を用いて、リーフIDに対するハッシュ値を算出し、算出ハッシュ値と、受信ハッシュ値の照合処理を行ない、受信データの検証 (ステップ (54)) を行なう。算出ハッシュ値と、受信ハッシュ値が適合したことを条件として、バックアップ/リストア用の起動ファイルをクライアントに送信 (ステップ (55)) する。起動ファイルの構成は、先に図15を参照して説明したと同様のファイル構成を持つ。

15

20

起動ファイルは、ブラウザからクライアントアプリケーションに渡され (ステップ (56))、起動ファイルの記述、あるいは拡張子によって判別選択されるバックアップ/リストア実行プログラムを起動し、リストア処理を実行 (ステップ (57)) する。

25

バックアップ/リストア処理の処理対象としては、サービスデータ、コンテンツ、コンテンツ利用権情報がある。サービスデータは前述した

ようにライセンスサーバに対する登録処理によって取得可能であり、コンテンツはコンテンツサーバから取得可能である。また、利用権情報は、ライセンスサーバから取得される。バックアップ／リストア処理においても、これらの各データは、それぞれのサーバから取得することになる。

5

まず、図 26 を参照して、バックアップ／リストア用サービスデータの取得処理について説明する。基本的に、この処理は、先に説明したコンテンツ購入時のクライアント登録処理と同様の手続きに従ったものとなる。

10

まず、クライアントアプリケーションは、登録要求をライセンスサーバに送信（ステップ（61））する。この登録要求には、管理システムが生成した起動ファイル中に含まれるトランザクション ID（TID）が含まれる。

15

登録要求を受信したライセンスサーバは、トランザクション ID（TID）に基づいて、バックアップ／リストア用サービスデータの取得であることを識別し、管理システムに対してサービス事前データ、すなわちサービスデータのバックアップ／リストア用データの割当要求（ステップ（62））を行なう。管理システムは、同じトランザクション ID に基づいて処理を実行したクライアント端末があるか否かを管理データに基づいて検証し、ある場合には、これらに対応付けて記憶（ステップ（63））する。これは、バックアップ／リストア処理の処理回数の上限（例えば 3 回）を設定し、上限を超える処理要求の場合には、処理

20

25

を実行しないという設定を可能とするためである。

管理データの更新処理を実行した管理システムは、サービス事前データ割当応答をライセンスサーバに送信（ステップ（64））する。これは、バックアップ／リストア用サービスデータの発行許可情報として送

信されるものである。

サービス事前データ割当応答を受信したライセンスサーバは、バックアップ／リストア用サービスデータのクライアントに対する発行処理
5 を実行（ステップ（65））する。サービスデータは、先に図17（a）を参照して説明したように、サービスデータ370には、EKB配信ツリーにおいて設定されるクライアントに固有のリーフID、サービス識別子としてのサービスID、さらにデバイスノードキー（DNK）をルートキー（Kroot）で暗号化したデータ、E（Kroot, DNK）
10 が含まれる。

さらに、この処理時に、デフォルト利用権情報（図17（b）参照）もライセンスサーバからクライアントに対して発行される。先に説明したように、利用権情報は、通常は、購入コンテンツの利用条件を格納し、
15 コンテンツの購入に対応して発行されるものであるが、デフォルト利用権情報は、コンテンツの購入を条件として発行するものではなく、クライアントの登録処理、あるいはサービスデータの発行処理を条件として発行する。このデフォルト利用権情報は、前述したようにコンテンツの試聴処理の際の有効な利用権情報として適用される。

20

ライセンスサーバからサービスデータ、デフォルト利用権情報を受領したクライアントは、これらのデータをバックアップ用として、記憶手段に格納（ステップ（66））する。

25 次に、図27を参照して、コンテンツのバックアップ／リストア処理について説明する。コンテンツのバックアップ／リストア処理実行の場合、クライアントアプリケーションは、コンテンツダウンロード要求をコンテンツサーバに対して実行（ステップ（71））する。これは、先にクライアントが購入したコンテンツと同一である。クライアントアプ

リケーションは、コンテンツID (CID) によりコンテンツを指定してコンテンツダウンロード要求をコンテンツサーバに対して実行する。

コンテンツサーバは、コンテンツダウンロード要求を受信すると、CID
5 CIDに対応するコンテンツ情報をクライアントに送信 (ステップ (72)) する。このコンテンツ情報は、暗号化コンテンツを含む情報である。先に図17(c)を参照して説明したように、コンテンツキー: Kcで暗号化されたコンテンツデータ: Enc(Kc, Content)、コンテンツキー: Kcをルートキー: Krootで暗号化したデータ:
10 Enc(Kroot, Kc)、さらに: ルートキー: Krootを取得するためのEKB、さらに試聴フラグデータ、サービスID等の情報が付加されたファイルである。

コンテンツ情報を受領したクライアントは、受信コンテンツに対応する
15 利用権情報 (Usage Right) の取得要求をライセンスサーバに対して送信 (ステップ (73)) する。この要求には、起動ファイル (図15参照) 中に含まれる利用権情報ID (UID)、クライアント識別データとしてのリーフID、トランザクションID (TID) が含まれる。

20

ライセンスサーバは、利用権情報 (Usage Right) の取得要求を受信すると、管理システムに対して、注文照会処理 (ステップ (74)) を行なう。この要求には、利用権情報ID (UID)、トランザクションID (TID) が含まれる。注文照会を受信した管理サーバは、
25 注文照会応答として、利用権情報ID (UID) に対応する利用条件を設定した応答情報をライセンスサーバに送信 (ステップ (75)) する。

応答情報を受信したライセンスサーバは、コンテンツ利用条件を設定した利用権情報 (Usage Right) を生成して、クライアント

に対して再発行（ステップ（76））する。なお、コンテンツ利用条件とは、コンテンツの再生回数、期限、外部機器に対するコピー、チェックアウト処理等の各種処理の許可情報によって構成される。

- 5 利用権情報（U s a g e R i g h t）を受信したクライアントは、先に受信したコンテンツと利用権情報とを記憶手段にバックアップデータとして格納する。

- 10 なお、バックアップ／リストア処理において、ライセンスサーバが発行する利用権情報は、正規なコンテンツ購入処理に際して発行する利用権情報とは異なる利用条件を設定したものとしてもよい。例えば、正規なコンテンツ購入時に発行する利用権情報に含まれる利用条件より厳しい条件、例えば利用期間の制限、コピー禁止、あるいはチェックアウト禁止といった条件を設定してバックアップ／リストア処理用の利用
- 15 権情報を設定発行してもよい。

〔8．リコメンドファイルによるコンテンツの二次配信〕

- 次に、正規にコンテンツを購入したクライアントが、購入コンテンツを他のクライアントに提供するいわゆるコンテンツ二次配信を実行し、
- 20 コンテンツ利用権をライセンスサーバから新たに配布することで、二次配信コンテンツを受領したクライアントにおいても正当なコンテンツ利用権を有することを条件としてコンテンツ利用を可能とし、さらに、コンテンツサーバからのコンテンツ配信負荷の軽減を実現した構成について説明する。

25

前述したように、コンテンツを再生利用するクライアントは、コンテンツを利用するためには、コンテンツサーバから暗号化されたコンテンツを受け取るとともに、ライセンスサーバから、ライセンス情報、すなわちサービスデータと、コンテンツに対応する利用権情報を受領するこ

とが必要となる。

ライセンス情報、すなわちサービスデータおよび利用権情報は、データ容量の小さいデータであるため、インターネット等の通信網を介した送受信が頻繁に行われたとしてもトラフィックの上昇も少なく、多大な配信時間がかかるといった問題は発生しない。しかし、一方、コンテンツは、音楽データ、画像データ、プログラム等様々であり、そのデータ容量も大きなものとなる。このような大容量のコンテンツを特定のコンテンツサーバから多くのクライアントに送信する場合には、送信時間が長くなり、コンテンツサーバの負担、ネットワークトラフィックの上昇等、様々な問題を発生させる。また、通信中の通信エラーによるコンテンツ配信エラーのトラブルも発生しかねない。

以下では、すでに正規なコンテンツを購入したクライアントの保有するコンテンツを他のクライアントに提供、すなわち二次配信を実行し、二次配信によるコンテンツの提供を受けたクライアントが、そのコンテンツのライセンス情報をライセンスサーバから受領することで、コンテンツサーバのクライアントに対するコンテンツ送信の負荷を減少させたシステムについて説明する。

20

図 28 にコンテンツを正規に受領したクライアントが他のクライアントに提供するコンテンツファイルを生成する処理手順を説明したフローを示す。なお、他のクライアントに提供するコンテンツを含むデータファイルをリコメンドファイルと呼ぶ。リコメンドファイルには、暗号化されたコンテンツを含むコンテンツファイル、および必要に応じてそのコンテンツの説明ファイル（例えば HTML ファイル）が含まれる。

25

図 28 の処理フローについて説明する。図 28 の処理を実行するクライアントは、前述したコンテンツ購入処理を実行し、正規にコンテンツ

を購入したクライアント、あるいは、リコメンドファイルを他のクライアントから受領し、その後の手続きにおいて正規なライセンスを取得したクライアントである。図28の処理は、クライアントアプリケーション（図1のクライアントアプリケーション12）の1つの実行プログラムとしてクライアントシステムとしての情報処理装置の制御手段（CPU等）による制御の下に実行される。ステップS801において、クライアントは、自己のクライアント装置のディスプレイにリコメンドファイル作成画面を表示する。

- 10 リコメンドファイル作成画面例を図29に示す。クライアントが正規購入し、再生可能なコンテンツリスト651が中央に表示され、リコメンドファイルを生成する場合は、このコンテンツリスト651からコンテンツを選択（ステップS802）し、右側のリスト654にタイトル等を表示させる。コンテンツリスト651とリスト654間の移動処理
- 15 は、移動スイッチ652、653の操作によって実行される。

- リコメンドファイル生成対象コンテンツが選択されると、ステップS803において、リコメンドファイル作成ボタン655が押下される。リコメンドファイル作成ボタン655が押下されると、ステップS80
- 20 4において、リコメンドファイル内にコンテンツファイルに併せて説明ファイル、例えばHTMLによって記述された説明ファイルを生成格納するか否かを選択する。これはユーザが任意に選択可能である。

- リコメンドファイルには、図30（a）に示すように、暗号化コンテンツを含むコンテンツファイル721とコンテンツ説明ファイル722とを組み合わせたリコメンドファイル720構成と、図30（b）に示すように、暗号化コンテンツを含むコンテンツファイル721のみからなるリコメンドファイル730構成との2つの態様があり、クライアントはその態様を自由に選択可能となる。

ステップ S 8 0 4 において、コンテンツ説明用ファイルの作成をしないと選択した場合は、図 3 0 (b) に示すコンテンツファイル 7 2 1 のみからなるリコmendファイル 7 3 0 が生成される。

5

コンテンツファイルの構成を図 3 1 に示す。コンテンツファイル (M Q T ファイル) 7 2 1 には、暗号化コンテンツと、コンテンツ付加情報としてのメタ情報、さらにコンテンツ購入可能なショップを示すショップサーバ U R L、コンテンツ識別子としてのコンテンツ I D (C I D)

10 が含まれる。

なお、コンテンツファイルに格納される暗号化コンテンツは、コンテンツキー K c により暗号化されたコンテンツであり、コンテンツキー K c は、有効化キーブロック (E K B) 配信ツリー構成を適用して提供される有効化キーブロック (E K B) の復号により取得可能なキーの適用

15 によってのみ取得可能なキーである。

一方、ステップ S 8 0 4 において、コンテンツ説明用ファイル作成を選択した場合は、ステップ S 8 0 6 に進み、コンテンツ説明ファイル (H T M L ファイル) 生成用の説明データ (メタデータ) をコンテンツ管理

20 テーブルから取得する。コンテンツに対応するコンテンツ説明データは、上述したように暗号化コンテンツとともに、コンテンツファイル内にも格納されているが、正規にコンテンツ利用権を取得したクライアントは、コンテンツファイルから取り出したコンテンツ対応のメタデータをコンテンツ管理データとして、別ファイルに格納管理しており、リコmend

25 ファイルにおいて生成される説明ファイル用のメタデータは、このコンテンツ管理データから抽出される。

ステップ S 8 0 7 において、コンテンツ管理データから抽出したメタ

データを、クライアントアプリケーションに設定されたテンプレートHTMLファイルに貼り付ける処理を実行し、コンテンツ対応の説明用HTMLファイルを生成し、ステップS808において、コンテンツファイルと説明用HTMLファイルからなるリコメンドファイルを生成する。

コンテンツ説明用データとしてのHTMLファイルの表示構成例を図32に示す。図32に示す例は、コンテンツが音楽データの場合の例である。説明用ファイルは、図32に示すように、音楽コンテンツの楽曲タイトル、アーティスト、発売元等の情報リスト、さらに、各種の操作、処理に関する説明が記述されている。リコメンドファイルを他のクライアントから受理したクライアントは、まずこの説明ファイルをオープンすることになる。

リコメンドファイルに格納されたコンテンツは暗号化されたコンテンツであり、正規なライセンス情報、すなわちサービスデータとコンテンツ対応の利用権情報を取得していない場合には再生することはできない。従って、リコメンドファイルを受領したクライアントがリコメンドファイルに格納されたコンテンツを利用する場合には、ライセンス情報を取得する手続きを実行することになる。

このライセンス情報取得処理について、図33、図34の処理フローを参照して説明する。リコメンドファイルを受領したクライアントは、図32に示す説明用ファイル（HTMLファイル）をオープンし、試聴、購入コンテンツ配信サイトボタン731をクリック（ステップS811）する。このクリック処理により、クライアントアプリケーションが起動（ステップS812）し、同じリコメンドファイルに格納されたコンテンツファイル（MQTファイル）（図31参照）を読み出して、コンテンツファイルからコンテンツID（CID）とショップURLを抽

出（ステップ S 8 1 3）する。

このように、コンテンツ説明用ファイルの試聴、購入コンテンツ配信
サイトボタン 7 3 1 は、コンテンツファイルからショップサーバ URL
5 を抽出し、抽出 URL をブラウザに出力する処理を実行するクライアン
トアプリケーションプログラムを起動するリンクデータとして構成さ
れている。従って、リコメンドファイルを受領したクライアントが容易
にショップに接続して購入手続きを実行することが可能となる。

- 10 ステップ S 8 1 4 において、コンテンツファイルから抽出したコンテ
ンツ ID（CID）に基づいて、コンテンツファイル名を設定する。こ
れはクライアントアプリケーションにおいて予め設定されたファイル
名設定処理として実行され、例えばコンテンツのタイトル、アーティス
ト名、あるいはその複合データ等が適用される。ステップ S 8 1 5 では、
15 ステップ S 8 1 4 5 で設定したファイル名のコンテンツファイルがクラ
イアントの記憶部に格納される。

- 次に、ステップ S 8 1 6 において、ステップ S 8 1 3 でコンテンツフ
ァイルから抽出したショップ URL がブラウザに渡され、ブラウザは受
20 領 URL に対応するショップページをショップサーバから読み出す。

- 図 3 4 の処理フローのステップ S 8 3 1 において、ショップ画面がク
ライアントのディスプレイに表示される。以下の処理は、基本的には、
前述したコンテンツの購入処理、試聴処理のいずれかの処理と同様であ
25 り、先に図 1 1、図 1 3、図 1 8、図 2 1 に従って説明した処理に従う
ことになる。ただし、コンテンツ自体はすでにコンクライアントが、リ
コメンドファイルから取得済みであるので、コンテンツサーバからのコ
ンテンツ受領処理は、省略される。

一連の処理の概略は、図 3 4 の処理フローのステップ S 8 3 2 以下に示す処理となる。まず、クライアントがショップサーバの提示するショップ画面において購入を指定してショップサーバに購入要求を出力すると、ショップサーバから購入用起動ファイルが送信される。これは、
5 先に、図 1 5 を参照して説明した起動ファイルと同様の構成を持つ。

次に、ステップ S 8 3 3 において、起動ファイルからコンテンツ識別子としてのコンテンツ ID (C I D) を取得する。次に、ステップ S 8 3 3 4 において、コンテンツ ID (C I D) に基づいて、コンテンツファイル名を算出する。クライアント装置にコンテンツを格納する際のコンテンツファイル名は、先の図 3 3 のフローの説明で述べたようにコンテンツ ID (C I D) に基づいて設定されることがクライアントアプリケーションにおいて規定され、C I D とファイル名の対応付けがなされている。
10
15 ステップ S 8 3 5 において、コンテンツ ID (C I D) から算出したファイル名と同一のファイル名のファイルが自己のクライアント装置の記憶部に格納されているか否かを判定する。コンテンツが格納されていない場合は、ステップ S 8 3 7 に進み、コンテンツサーバに接続して、コンテンツダウンロードを行なうことになる。この処理は、先に説明した
20 コンテンツ購入時の処理と同様である。

しかし、リコメンドファイルを受領しているクライアントは、先の図 3 3 のフロー中のステップ S 8 1 4, S 8 1 5 において、所定のファイル名を設定したコンテンツファイルを記憶部に格納しており、コンテンツのダウンロード処理は省略され、ステップ S 8 3 6 のコンテンツ利用
25 権情報の取得処理を実行し処理を終了することが可能となる。

クライアントがコンテンツ再生を実行する際は、前述したように、コンテンツ利用権情報に格納されたコンテンツ識別子 (C I D) と再生対

- 象コンテンツのコンテンツ識別子（C I D）との照合を行ないC I Dの一致を条件としてコンテンツ再生を実行する。また、有効化キーブロック（E K B）配信ツリー構成を適用して提供される有効化キーブロック（E K B）の復号によりコンテンツキーK cを取得し、取得したコンテンツキーK cを適用して暗号化コンテンツの復号処理を実行することにより、コンテンツを再生利用することが可能となる。

- このように、すでにコンテンツを保有しているクライアントが暗号化コンテンツを含むコンテンツファイルと、説明用ファイルからなるリコメンドファイルを他のクライアントに提供することで、他のクライアントがコンテンツ配信サーバへのアクセスなしにコンテンツを受領することが可能となる。他のクライアントは、利用権情報を取得することを条件としてコンテンツの利用が可能となる構成であるので、不正なコンテンツの利用は防止される。

15

- なお、図 3 4 のフローにおいてはサービスデータの取得処理については省略してあるが、サービスデータを保有していないクライアントがリコメンドファイルを受領した場合には、ライセンスサーバに対するアクセスを実行して登録処理を行ない、サービスデータを取得することが必要となる。この登録処理手続きは、先に図 1 3、図 1 6 を参照して説明した処理に対応する処理となる。

20

- 以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

25

なお、明細書中において説明した一連の処理はハードウェア、またはソフトウェア、あるいは両者の複合構成によって実行することが可能である。ソフトウェアによる処理を実行する場合は、処理シーケンスを記録したプログラムを、専用のハードウェアに組み込まれたコンピュータ
5 内のメモリにインストールして実行させるか、あるいは、各種処理が実行可能な汎用コンピュータにプログラムをインストールして実行させることが可能である。

例えば、プログラムは記憶媒体としてのハードディスクやROM
10 (Read Only Memory)に予め記録しておくことができる。あるいは、プログラムはフレキシブルディスク、CD-ROM (Compact Disc Read Only Memory), MO (Magneto optical) ディスク, DVD (Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体に、一時的あるいは永続的に格納(記録)しておくことができる。
15 このようなリムーバブル記録媒体は、いわゆるパッケージソフトウェアとして提供することができる。

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

25 なお、明細書に記載された各種の処理は、記載に従って時系列に実行されるのみならず、処理を実行する装置の処理能力あるいは必要に応じて並列的にあるいは個別に実行されてもよい。

産業上の利用可能性

以上、説明したように、本発明の構成によれば、クライアントは、ライセンスサーバに対する登録処理の際にデフォルト利用権情報（Default Usage Right）を取得し、コンテンツの購入処理を伴わない試聴処理の際にデフォルト利用権情報に基づいてコンテンツ再生が許可され、ユーザは、コンテンツの購入を実行することなく、コンテンツの試聴再生が可能となる。また、試聴が許可されるクライアントは、ライセンスサーバに対する登録処理を行ない、デフォルト利用権情報を有するクライアントに限定されることになるので、試聴データが無秩序に氾濫してしまうことが防止される。

さらに、本発明の構成によれば、コンテンツの購入処理を伴わない試聴処理においても、コンテンツ利用機器としてのハードウェアに対応して設定されたカテゴリツリーに対応するEKBとしてのハード対応EKB [EKB (H)] と、コンテンツ利用サービスに対応して設定されたカテゴリツリーに対応するEKBとしてのサービス対応EKB [EKB (S)] に対する正当なDNKを有するユーザのみがコンテンツ再生を実行可能とする構成が適用でき、試聴処理においても再生権限を限定した範囲として設定可能となる。

請求の範囲

1. 暗号化されたコンテンツの復号及び利用を制御する情報処理装置であって、
5 コンテンツ利用の指示に応じて、該コンテンツに対応する利用権情報（u s a g e r i g h t）に基づいて、該コンテンツの利用を制御する制御手段と、
製造時に記録されたあるいはサービス登録時に取得されたデフォルト利用権情報を記録する記録手段とを備え、
10 前記制御手段は、前記コンテンツに前記デフォルト利用権情報に対応することを示す情報が含まれている場合に、前記デフォルト利用権情報に記述内容に基づいて前記コンテンツを復号し、利用することを許可すること
15 ことを特徴とする情報処理装置。
2. 前記デフォルト利用権情報に基づいて利用が許可される前記コンテンツは、試用の目的で提供されるものであり、
前記制御手段は、前記コンテンツに試用コンテンツであることを示す
20 フラグが含まれているかを検証し、検証結果に基づいて前記コンテンツの再生を許可すること
ことを特徴とする請求項 1 に記載の情報処理装置。
3. 前記情報処理装置は、さらに、
25 サービスへの登録要求を送信する送信手段と、
登録要求に応じてライセンスサーバから送信されるデフォルト利用権情報を受信する受信手段と、
を備えることを特徴とする請求項 1 に記載の情報処理装置。

4. 前記受信手段は、さらに前記コンテンツの復号に必要となる鍵情報を受信することを特徴とする請求項3に記載の情報処理装置。

- 5 5. 暗号化されたコンテンツの利用条件 (u s a g e r u l e s) が記述された利用権を発行する情報処理装置であって、
登録要求を受信する受信手段と、
前記登録要求に応じて、暗号化されたコンテンツの復号に必要となる鍵情報と、デフォルト利用権情報を送信する送信手段と、
10 を備えることを特徴とする情報処理装置。

6. 前記デフォルト利用権情報に基づいて利用が許可される前記コンテンツは、試用の目的で提供されるものであり、
前記デフォルト利用権情報は、前記コンテンツに試用コンテンツであることを示すフラグが含まれている場合に再生を許可することが記述
15 されていることを特徴とする請求項5に記載の情報処理装置。

7. 暗号化されたコンテンツの復号及び利用を制御する情報処理方法であって、
20 コンテンツ利用の指示に応じて、該コンテンツに対応する利用権情報 (u s a g e r i g h t) に基づくコンテンツ利用を制御する制御ステップを有し、
前記制御ステップは、
前記コンテンツに、製造時に記録されたデフォルト利用権情報、あるいはサービス登録時に取得されたデフォルト利用権情報に対応するこ
25 とを示す情報が含まれているか否かを検証するステップと、
デフォルト利用権情報に対応することを示す情報が含まれている場合に、前記デフォルト利用権情報に記述内容に基づいて前記コンテンツを復号し、利用することを許可するステップと、

を含むことを特徴とする情報処理方法。

8. 前記デフォルト利用権情報に基づいて利用が許可される前記コンテンツは、試用の目的で提供されるものであり、

- 5 前記制御ステップは、さらに、前記コンテンツに試用コンテンツであることを示すフラグが含まれているかを検証し、検証結果に基づいて前記コンテンツの再生を許可するステップを含むことを特徴とする請求項7に記載の情報処理方法。

- 10 9. 前記情報処理方法は、さらに、
サービスへの登録要求を送信する送信ステップと、
登録要求に応じてライセンスサーバから送信されるデフォルト利用権情報を受信する受信ステップと、
を含むことを特徴とする請求項7に記載の情報処理方法。

- 15 10. 前記情報処理方法は、さらに、
前記コンテンツの復号に必要な鍵情報を受信するステップを含むことを特徴とする請求項9に記載の情報処理方法。

- 20 11. 暗号化されたコンテンツの利用条件 (usage rules) が記述された利用権を発行する情報処理方法であって、
登録要求を受信する受信ステップと、
前記登録要求に応じて、暗号化されたコンテンツの復号に必要な鍵情報と、デフォルト利用権情報を送信する送信ステップと、
25 を有することを特徴とする情報処理方法。

12. 前記デフォルト利用権情報に基づいて利用が許可される前記コンテンツは、試用の目的で提供されるものであり、

前記デフォルト利用権情報は、前記コンテンツに試用コンテンツであ

ることを示すフラグが含まれている場合に再生を許可することが記述されていることを特徴とする請求項 1 1 に記載の情報処理方法。

1 3. 暗号化されたコンテンツの復号及び利用を制御する情報処理
5 を実行するコンピュータ・プログラムであって、

コンテンツ利用の指示に応じて、該コンテンツに対応する利用権情報
(u s a g e r i g h t) に基づくコンテンツ利用を制御する制御ス
テップを有し、

前記制御ステップは、

10 前記コンテンツに、製造時に記録されたデフォルト利用権情報、ある
いはサービス登録時に取得されたデフォルト利用権情報に対応するこ
とを示す情報が含まれているか否かを検証するステップと、

デフォルト利用権情報に対応することを示す情報が含まれている場
合に、前記デフォルト利用権情報に記述内容に基づいて前記コンテン
15 ツを復号し、利用することを許可するステップと、

を含むことを特徴とするコンピュータ・プログラム。

1 4. 前記デフォルト利用権情報に基づいて利用が許可される前記
コンテンツは、試用の目的で提供されるものであり、

20 前記制御ステップは、さらに、前記コンテンツに試用コンテンツであ
ることを示すフラグが含まれているかを検証し、検証結果に基づいて前
記コンテンツの再生を許可するステップを含むことを特徴とする請求
項 1 3 に記載のコンピュータ・プログラム。

25 1 5. 前記コンピュータ・プログラムは、さらに、

サービスへの登録要求を送信する送信ステップと、

登録要求に応じてライセンスサーバから送信されるデフォルト利用
権情報を受信する受信ステップと、

を含むことを特徴とする請求項 1 3 に記載のコンピュータ・プログラ

ム。

16. 前記コンピュータ・プログラムは、さらに、
前記コンテンツの復号に必要となる鍵情報を受信するステップを含むことを特徴とする請求項15に記載のコンピュータ・プログラム。

17. 暗号化されたコンテンツの利用条件 (usage rules) が記述された利用権を発行する情報処理を実行するコンピュータ・プログラムであって、
10 登録要求を受信する受信ステップと、
前記登録要求に応じて、暗号化されたコンテンツの復号に必要となる鍵情報と、デフォルト利用権情報を送信する送信ステップと、
を有することを特徴とするコンピュータ・プログラム。

18. 前記デフォルト利用権情報に基づいて利用が許可される前記コンテンツは、試用の目的で提供されるものであり、
前記デフォルト利用権情報は、前記コンテンツに試用コンテンツであることを示すフラグが含まれている場合に再生を許可することが記述されていることを特徴とする請求項17に記載のコンピュータ・プログラム。
20

19. 暗号化されたコンテンツの復号及び利用を行うコンテンツ利用装置と、暗号化されたコンテンツの利用条件 (usage rules) が記述された利用権を発行する利用権発行装置を有するコンテンツ
25 利用管理システムであって、
前記コンテンツ利用装置は、
サービスへの登録要求を送信する送信手段と、
登録要求に応じてライセンスサーバから送信されるデフォルト利用権情報を受信する受信手段とを備え、

- 前記利用権発行装置は、
前記登録要求を受信する受信手段と、
前記登録要求に応じて、暗号化されたコンテンツの復号に必要となる鍵情報と、デフォルト利用権情報を送信する送信手段とを備えた構成、
5 であることを特徴とするコンテンツ利用管理システム。

20. 暗号化されたコンテンツの復号及び利用を行うコンテンツ利用装置と、暗号化されたコンテンツの利用条件（usage rules）が記述された利用権を発行する利用権発行装置を有するコンテンツ
10 利用管理システムにおけるコンテンツ利用管理方法であって、
前記コンテンツ利用装置から前記利用権発行装置に対してサービスへの登録要求を送信する登録要求送信ステップと、
前記利用権発行装置において、前記登録要求を受信し、該登録要求に応じて、暗号化されたコンテンツの復号に必要となる鍵情報と、デフォ
15 ルト利用権情報を送信するデータ送信ステップと、
前記コンテンツ利用装置において、デフォルト利用権情報を受信する受信ステップと、
を有することを特徴とするコンテンツ利用管理方法。

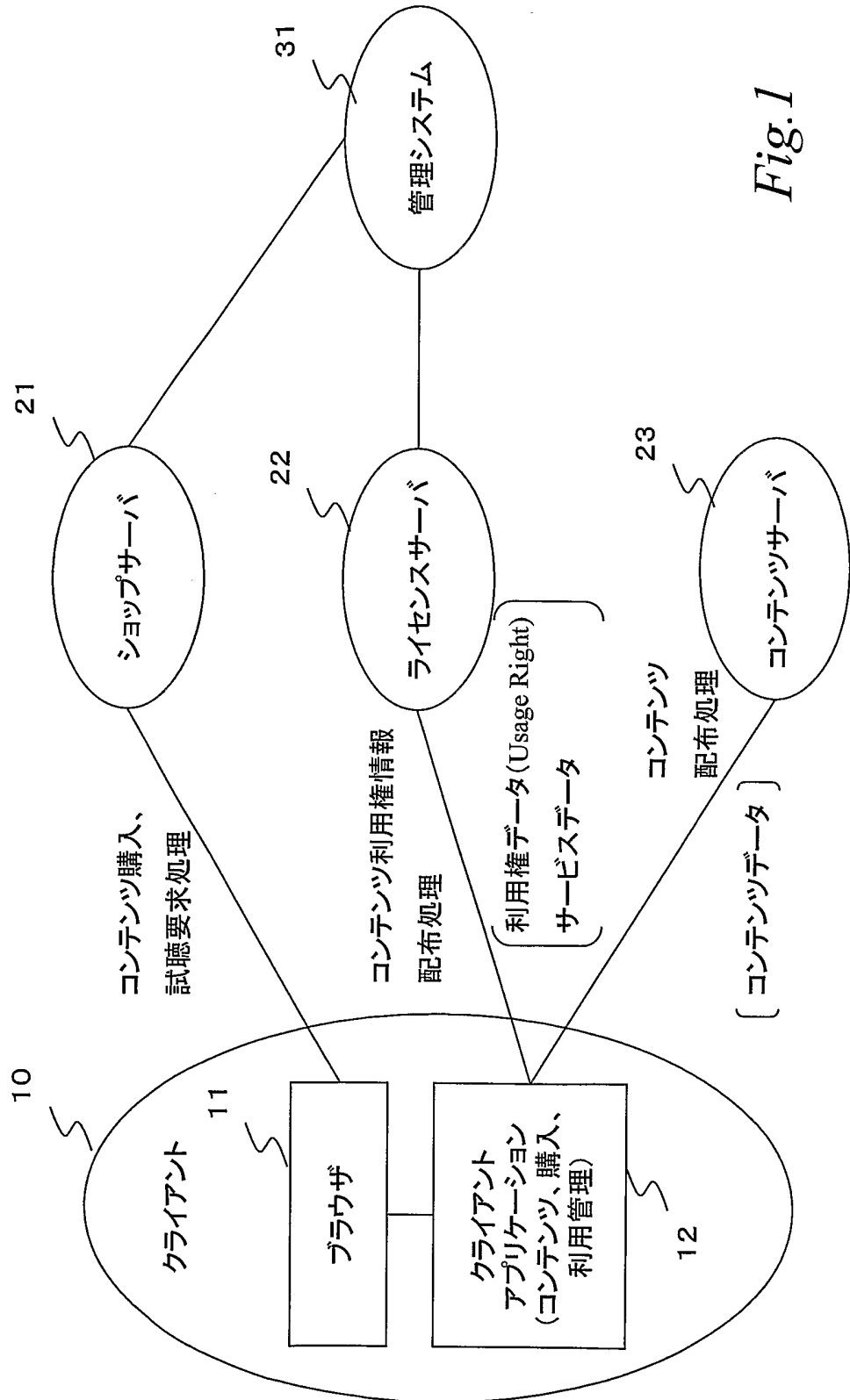


Fig. 1

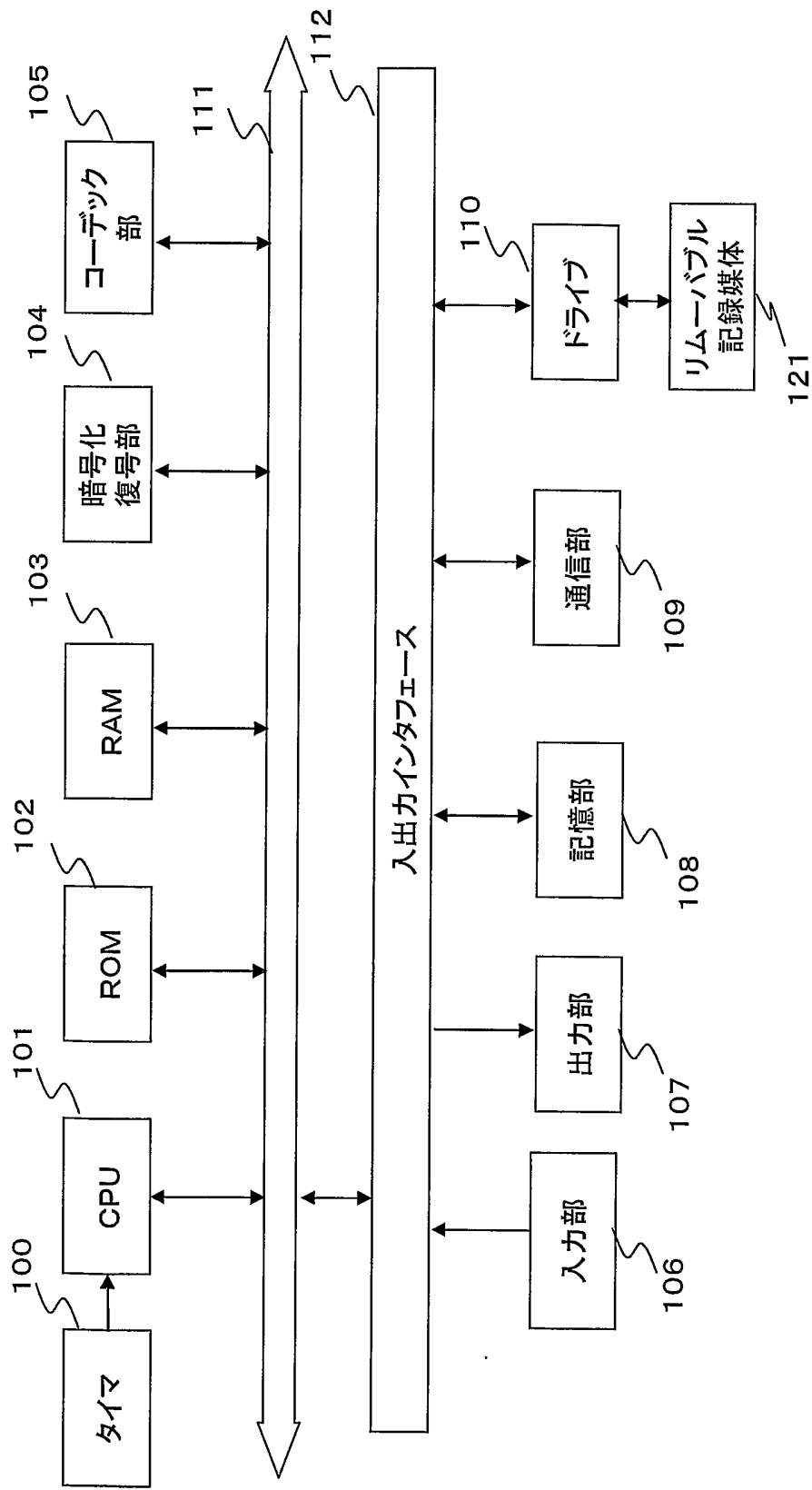
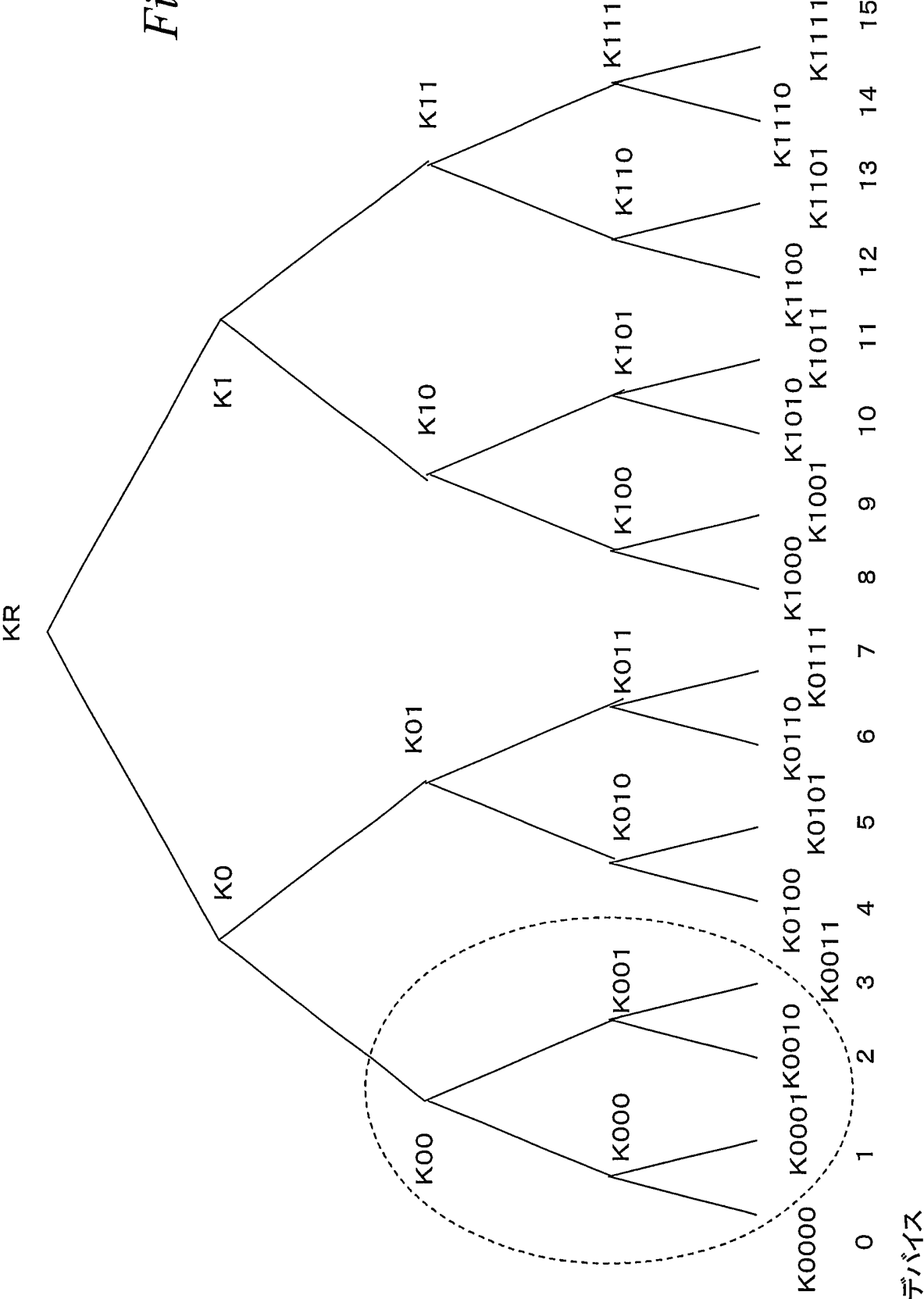


Fig. 2

Fig.3



(A) 有効化キーブロック
(EKB:Enabling Key Block)例1

(B) 有効化キーブロック
(EKB:Enabling Key Block) 例2

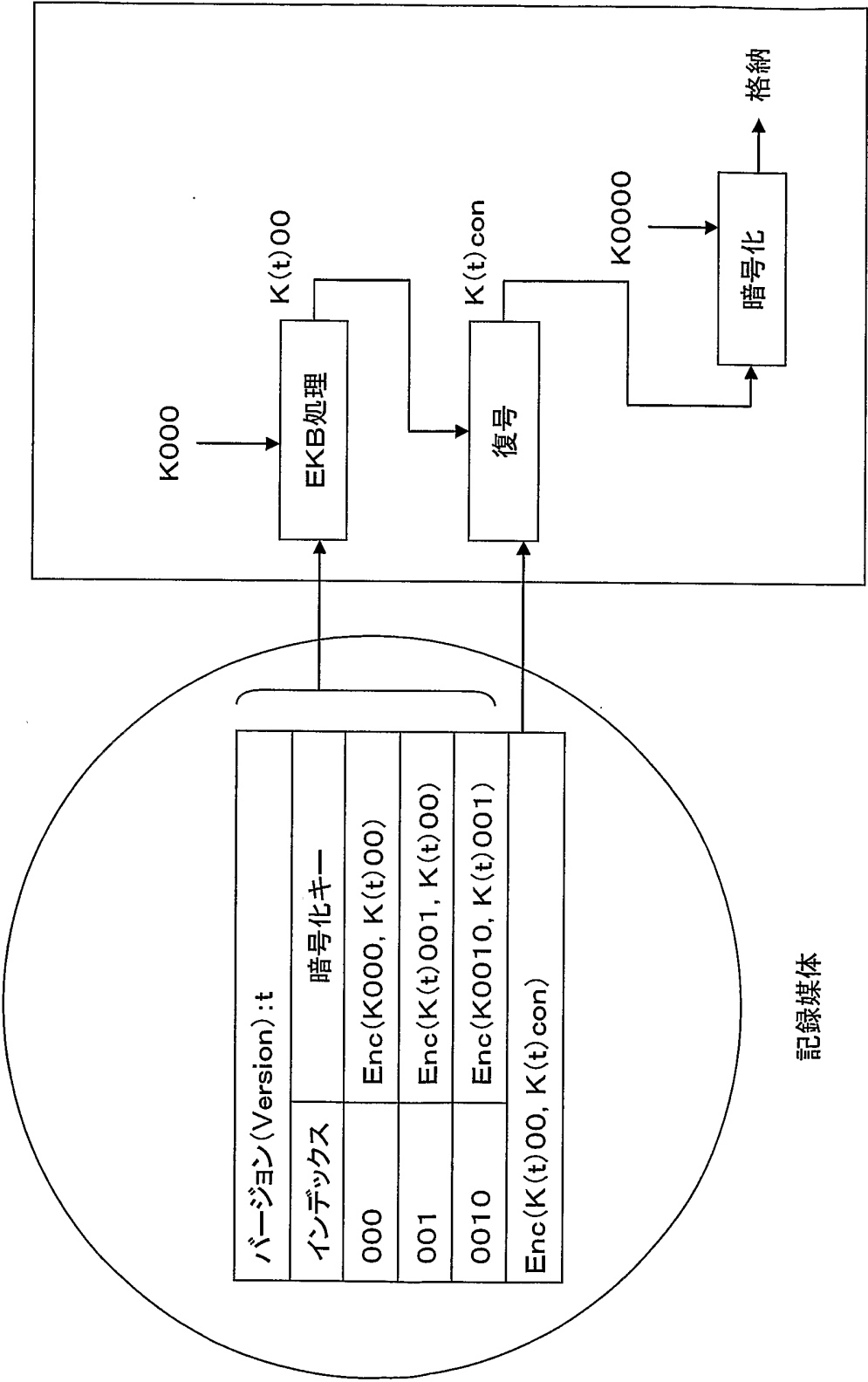
デバイス0, 1, 2にバージョン:tのノードキーを送付

バージョン(Version):t	
インデックス	暗号化キー
0	Enc(K(t)0, K(t)R)
00	Enc(K(t)00, K(t)0)
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

デバイス0, 1, 2にバージョン:tのノードキーを送付

バージョン(Version):t	
インデックス	暗号化キー
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

Fig.4



デバイス0

Fig.5

201	バージョン (version)	202	デプス (depth)
203	データポインタ (Data pointer)	204	タグポインタ (Tag pointer)
205	署名ポインタ (Signature pointer)		リザーブ (reserved)
	データ部(E(k0, Kroot), ...)		
	タグ部({0, 0}, {1, 1}, ...)		
	署名 (Signature)		

Fig.6

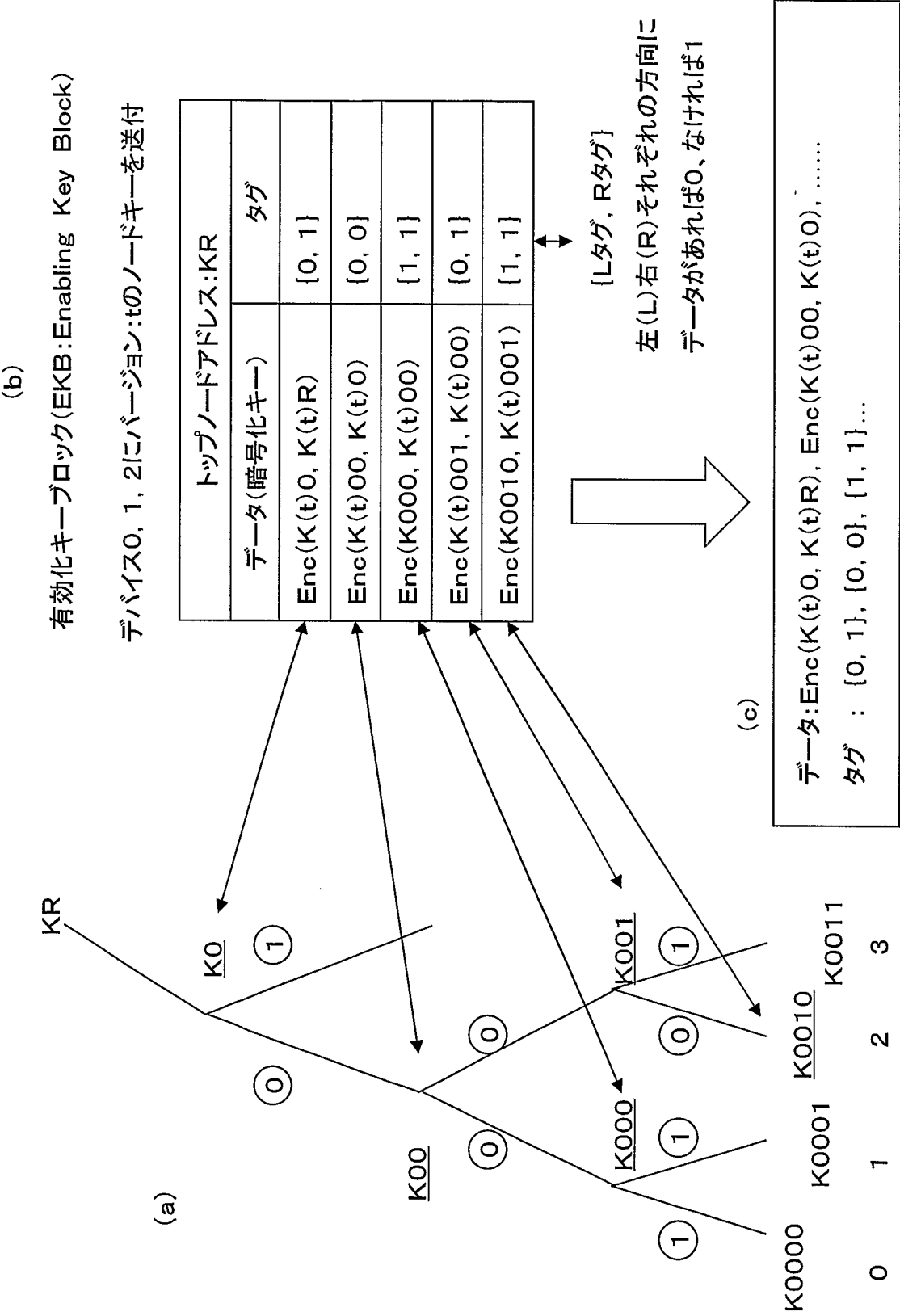


Fig. 7

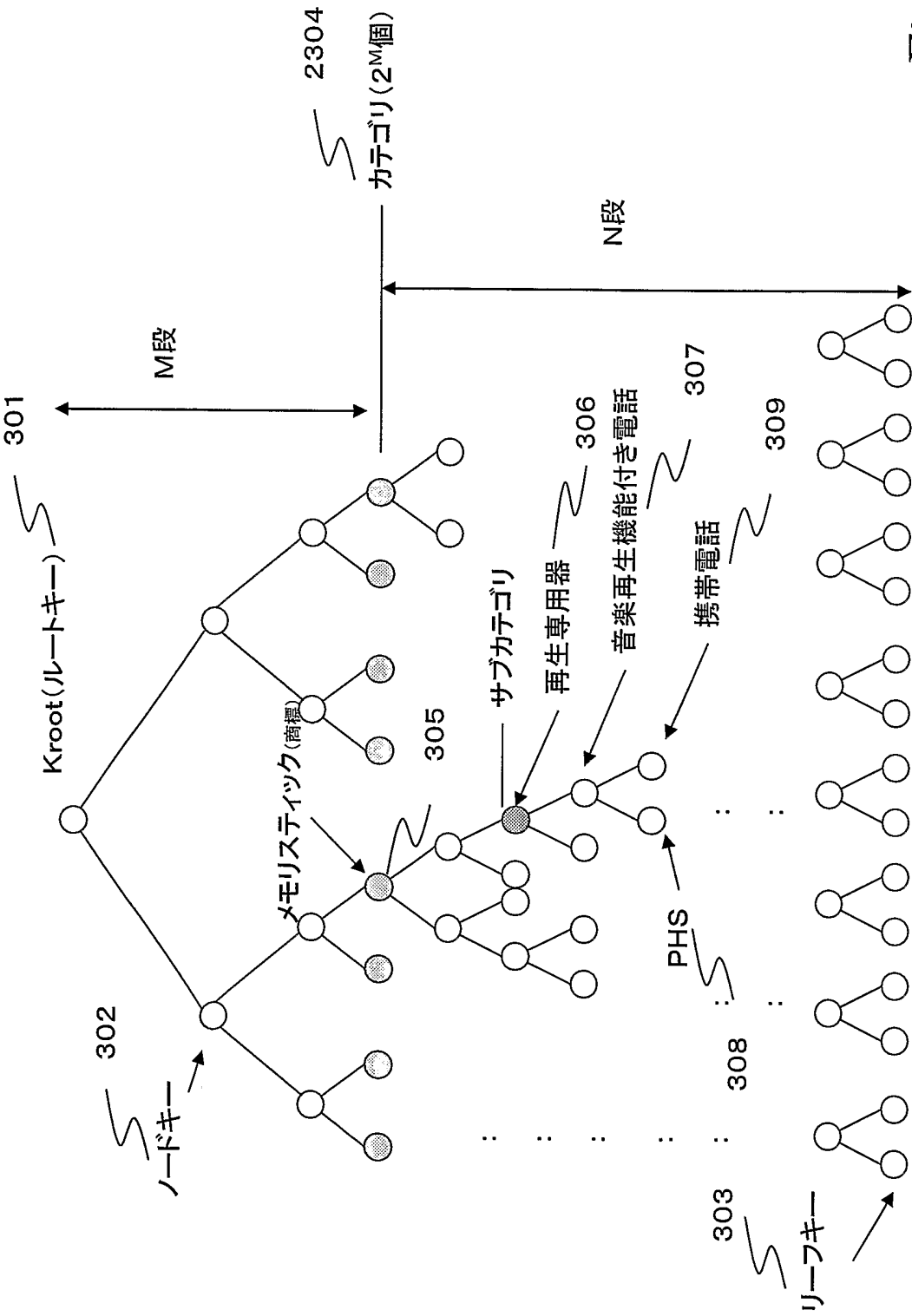


Fig. 8

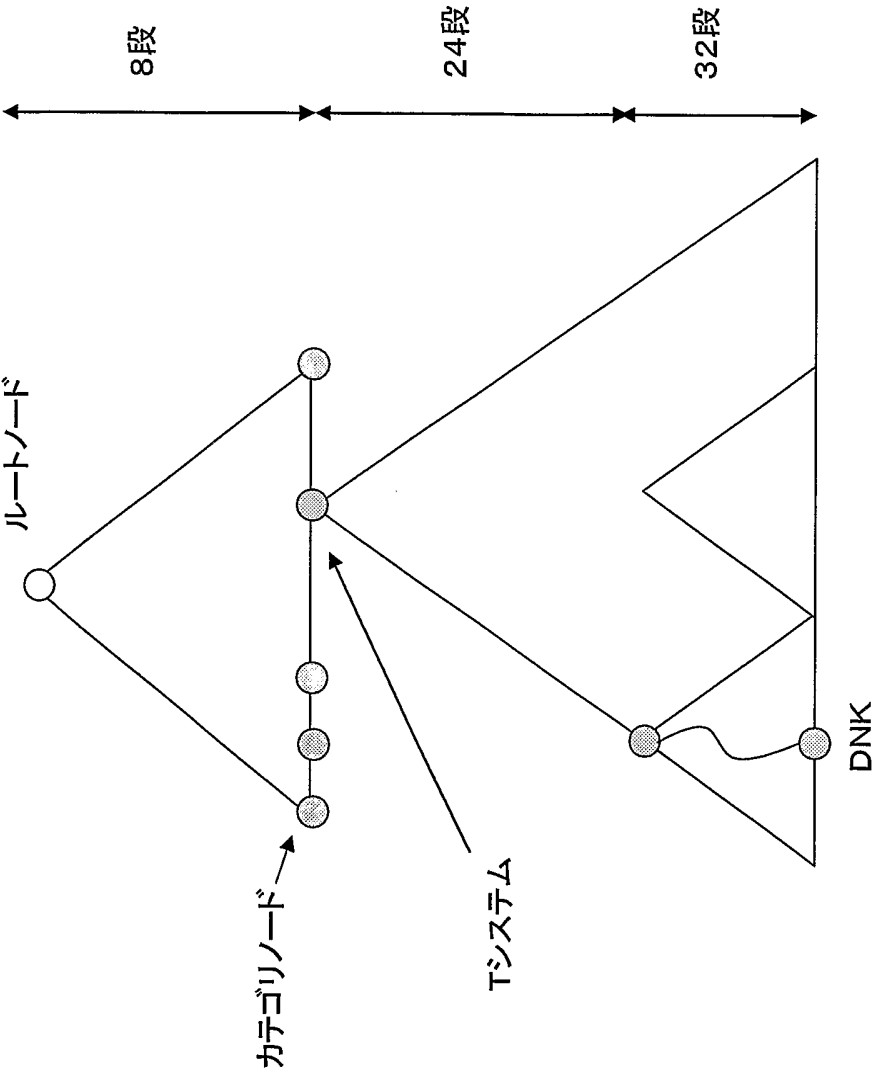
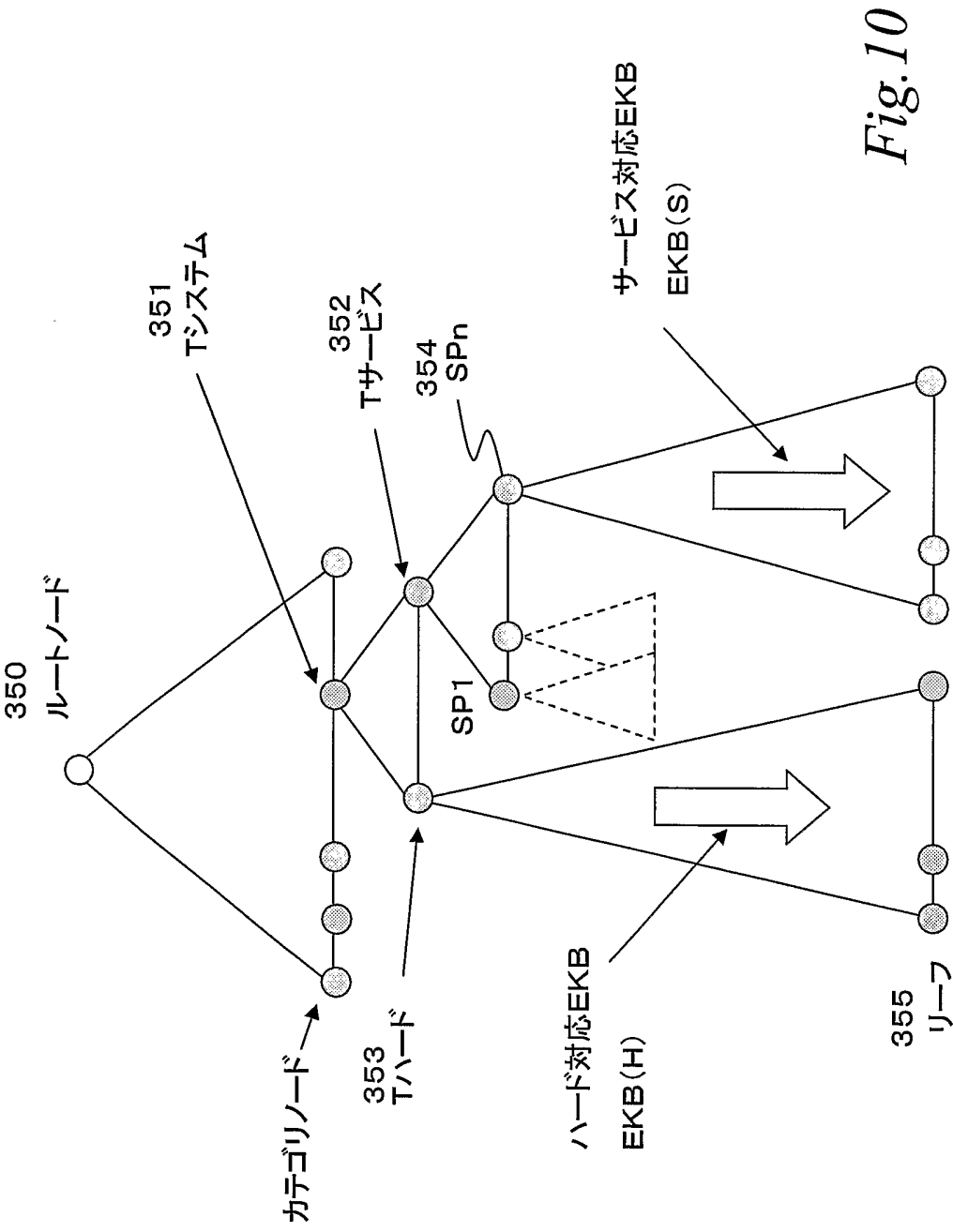


Fig. 9



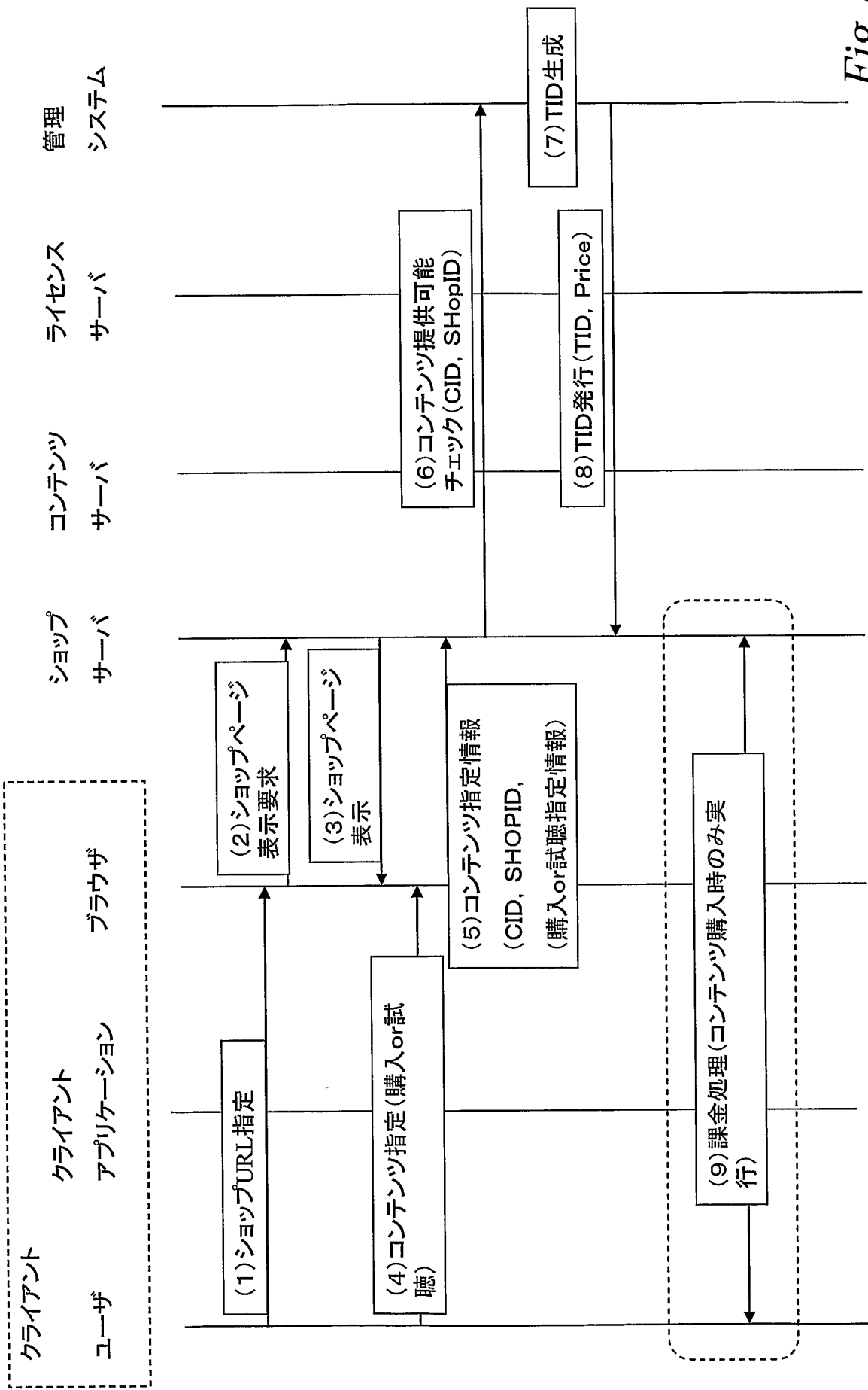


Fig. 11

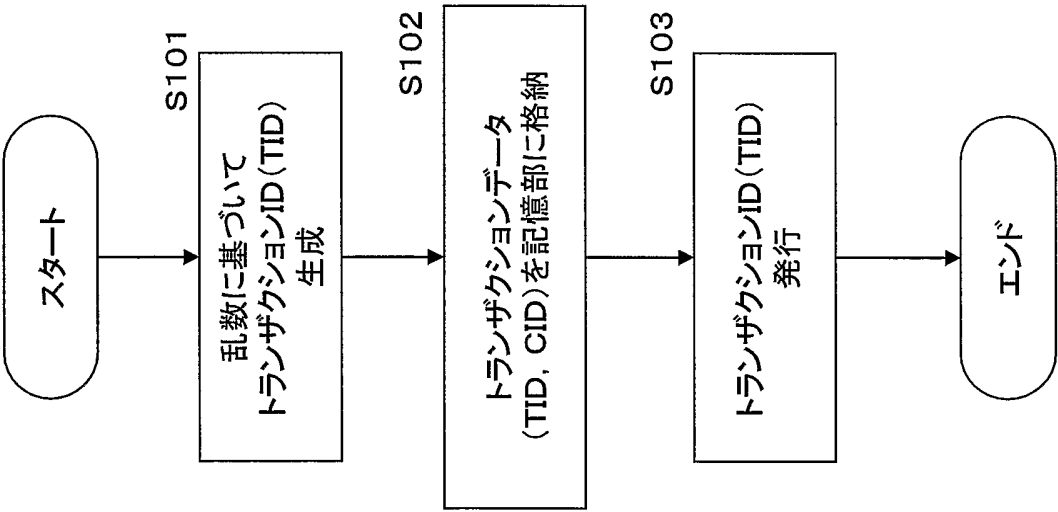


Fig.12

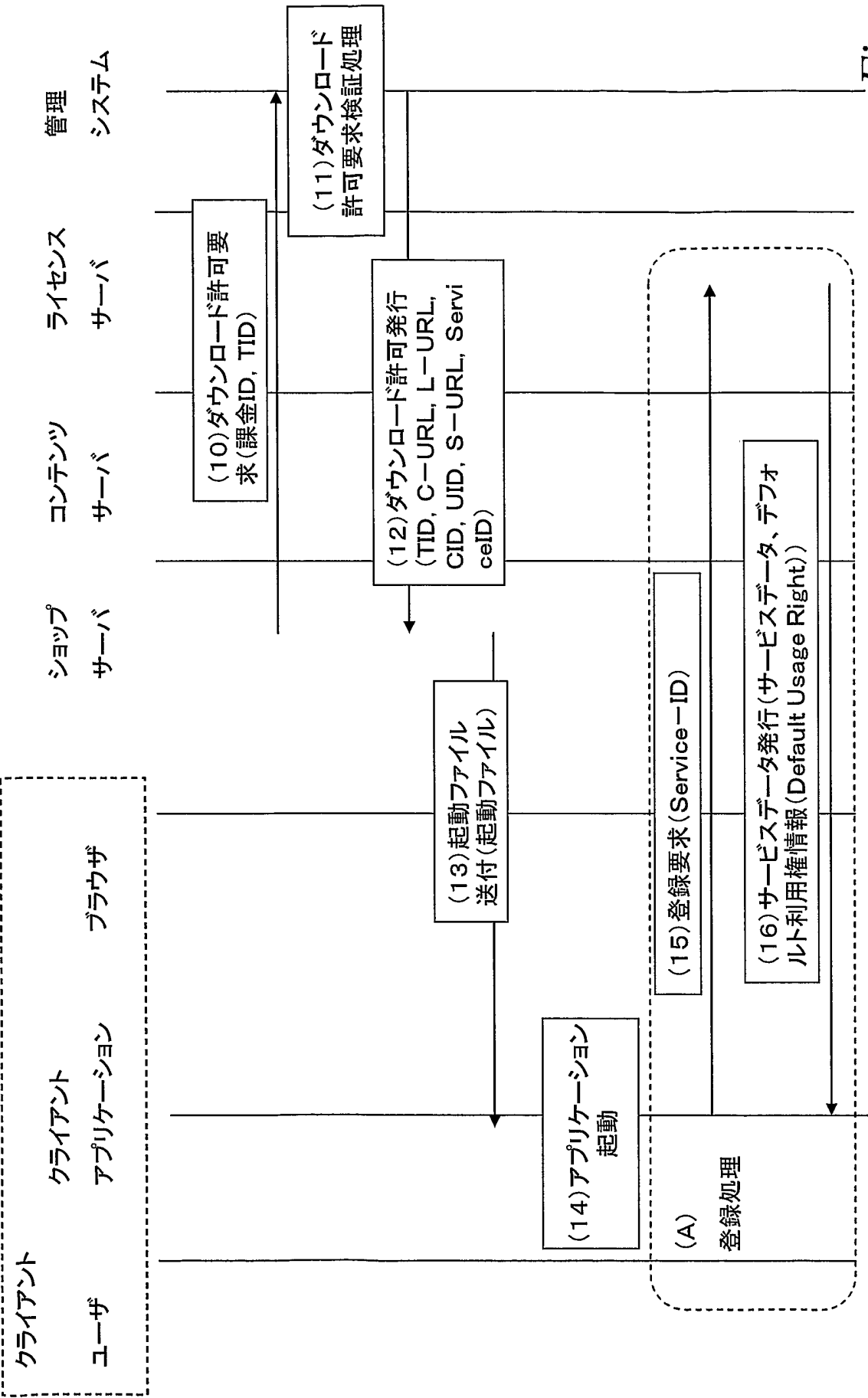


Fig.13

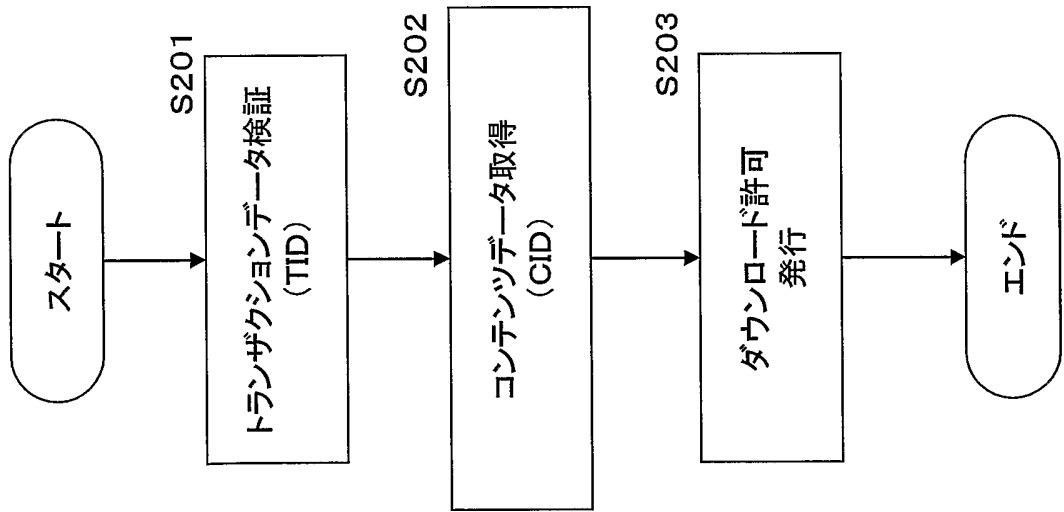


Fig.14

360

起動ファイル	
トランザクションID (TID)	
コンテンツID (CID)	
利用権情報ID (UID)	
サービスID	
コンテンツサーバーURL	
ライセンスサーバーURL	
商品URL	
試聴 or 購入	

Fig.15

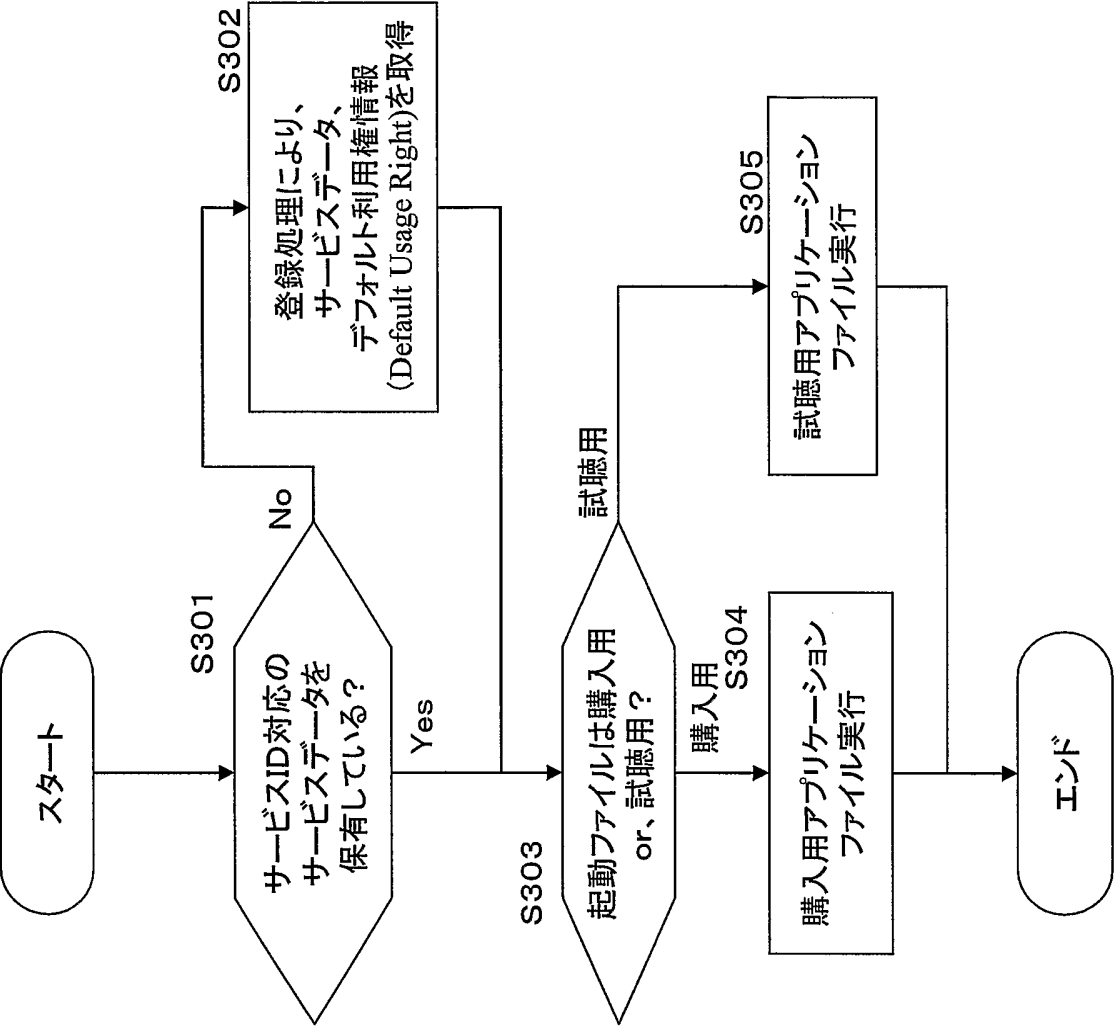


Fig.16

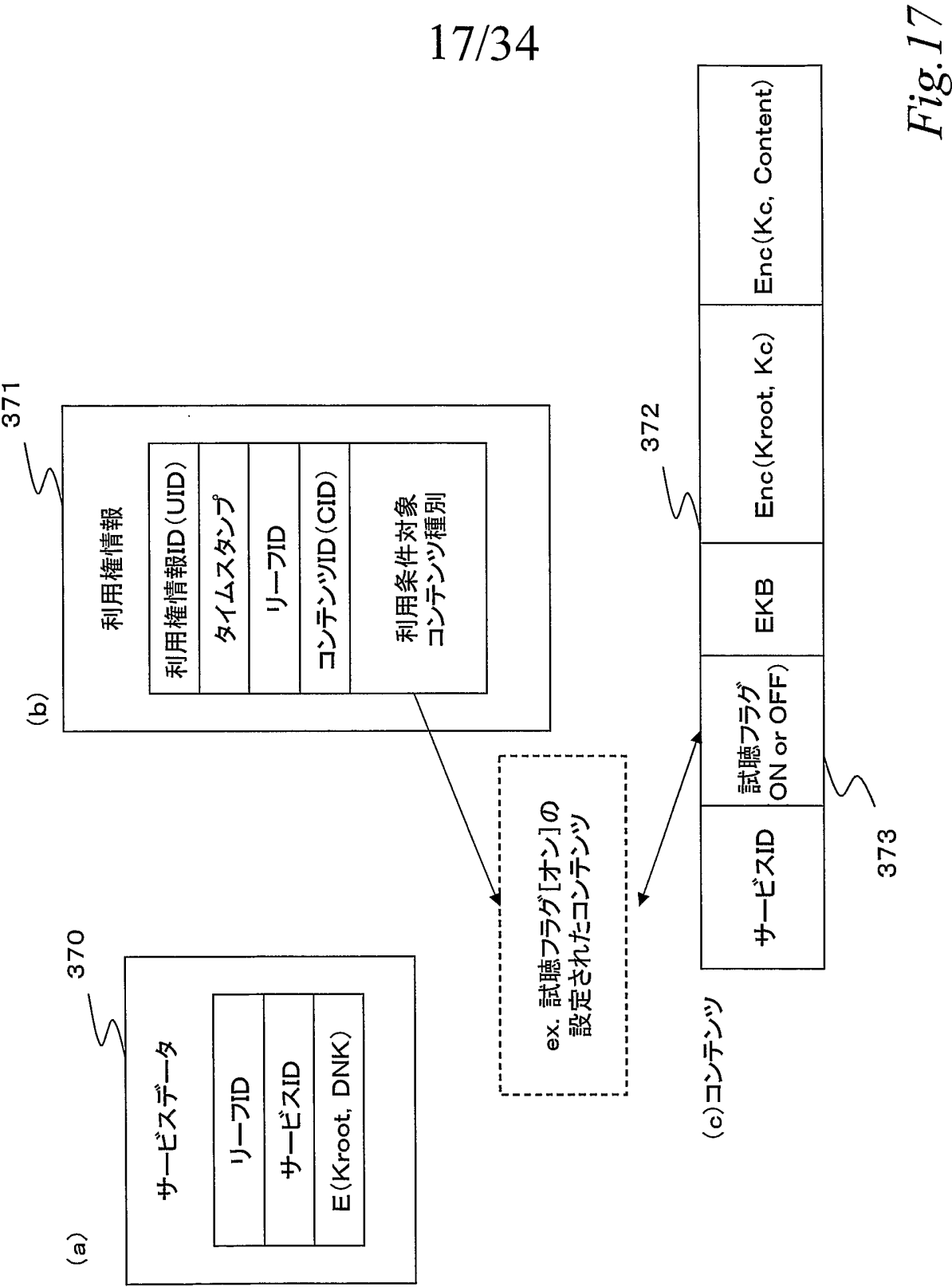


Fig.17

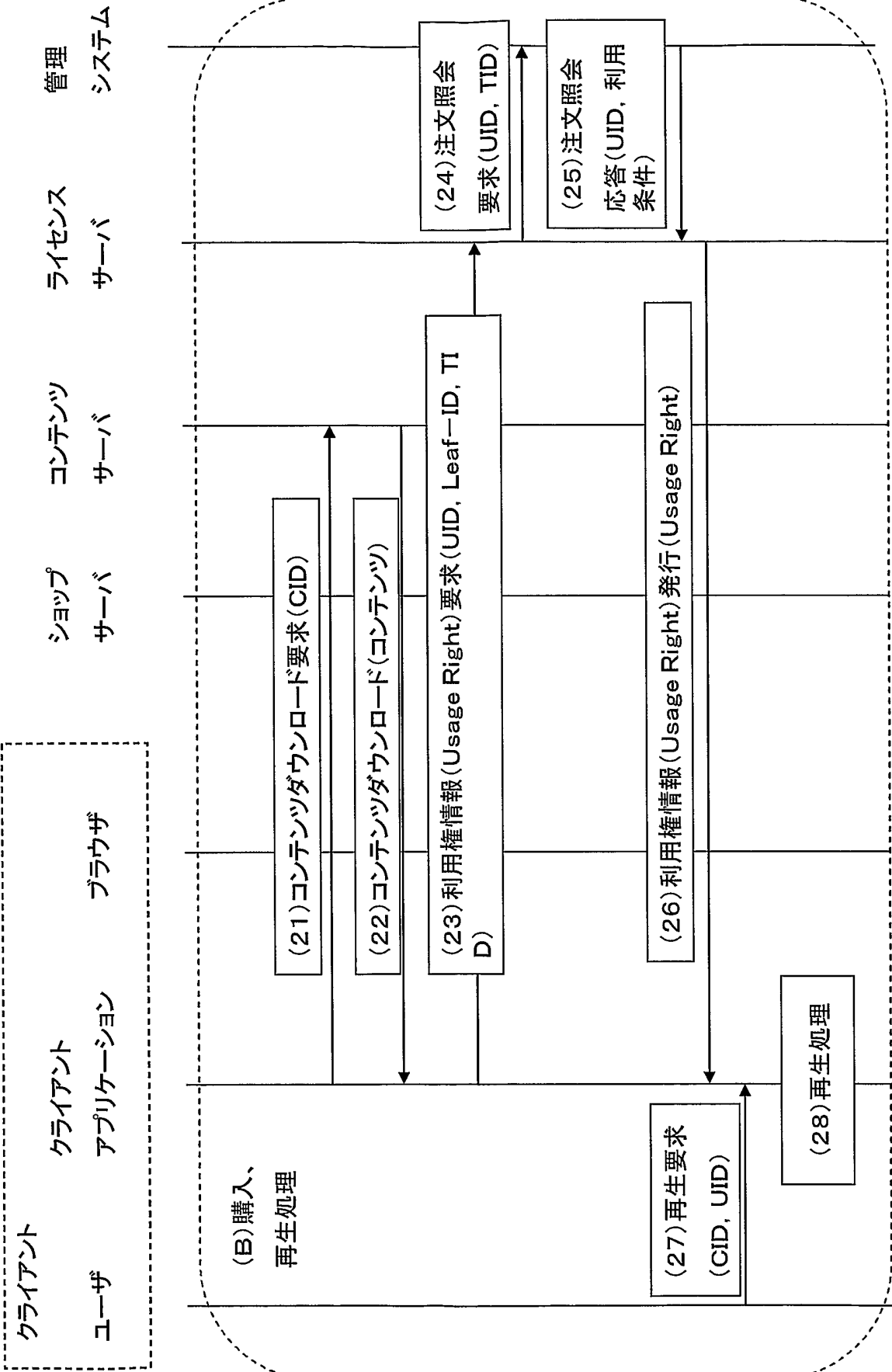


Fig.18

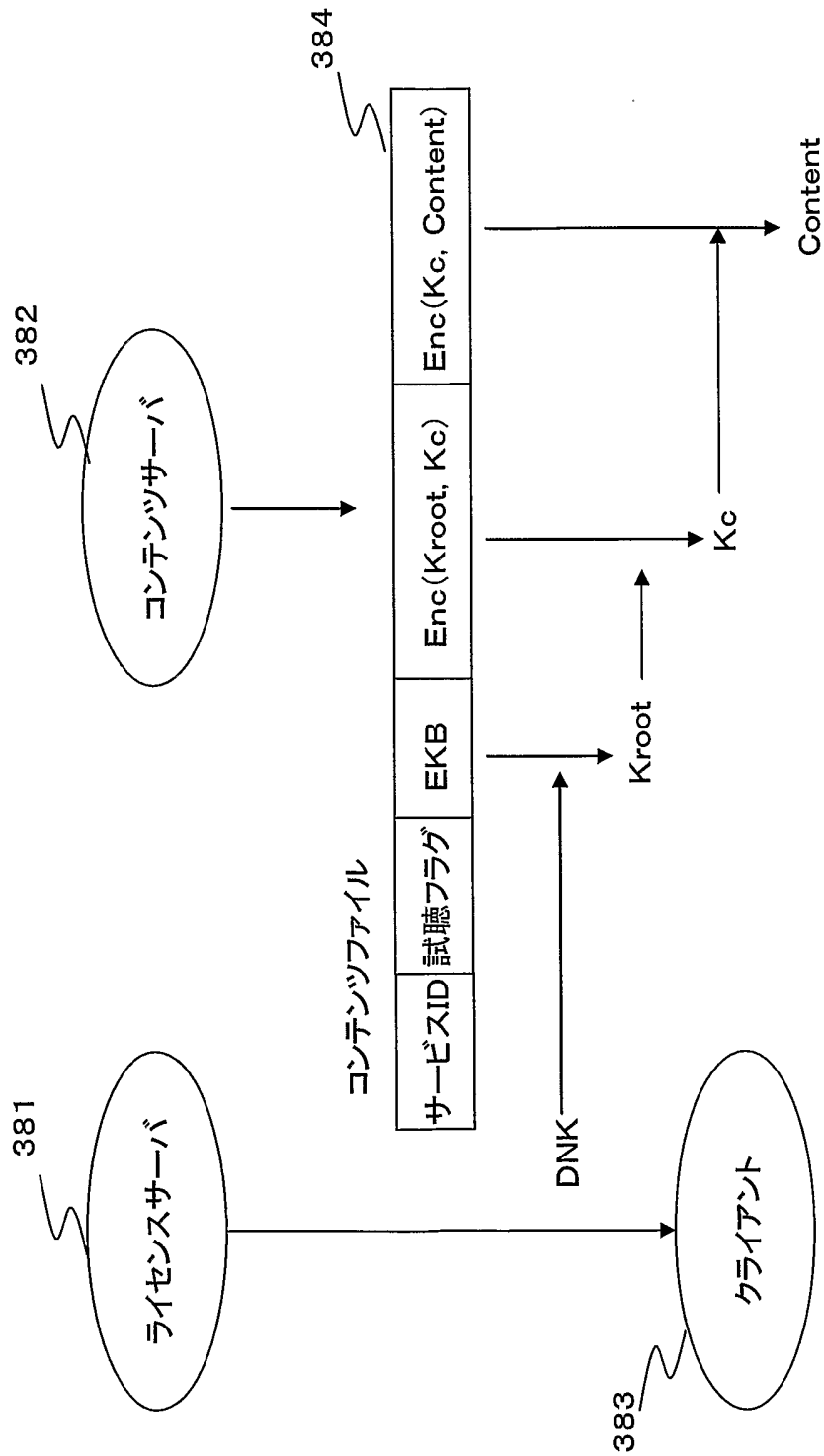
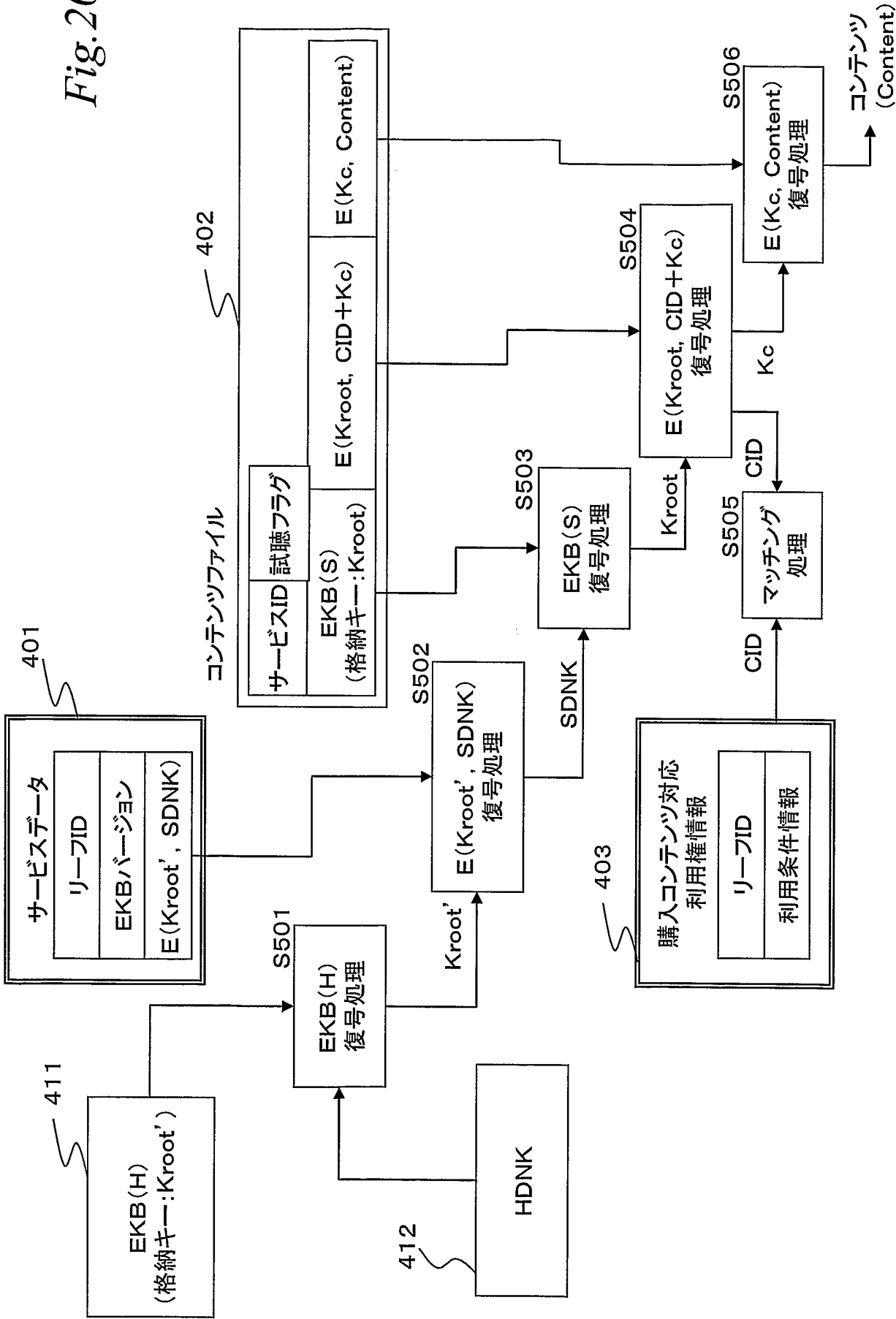


Fig.19

Fig. 20



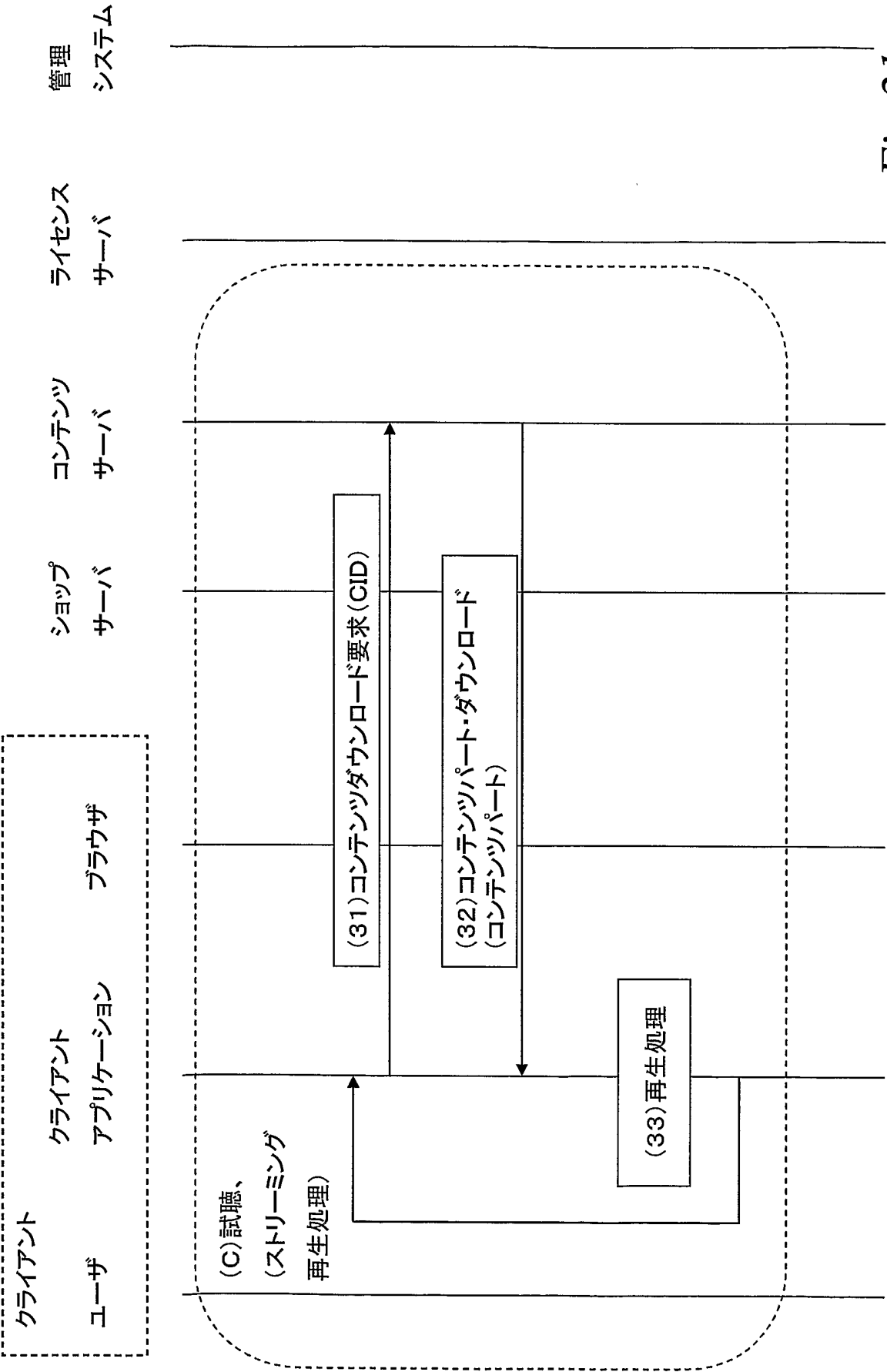
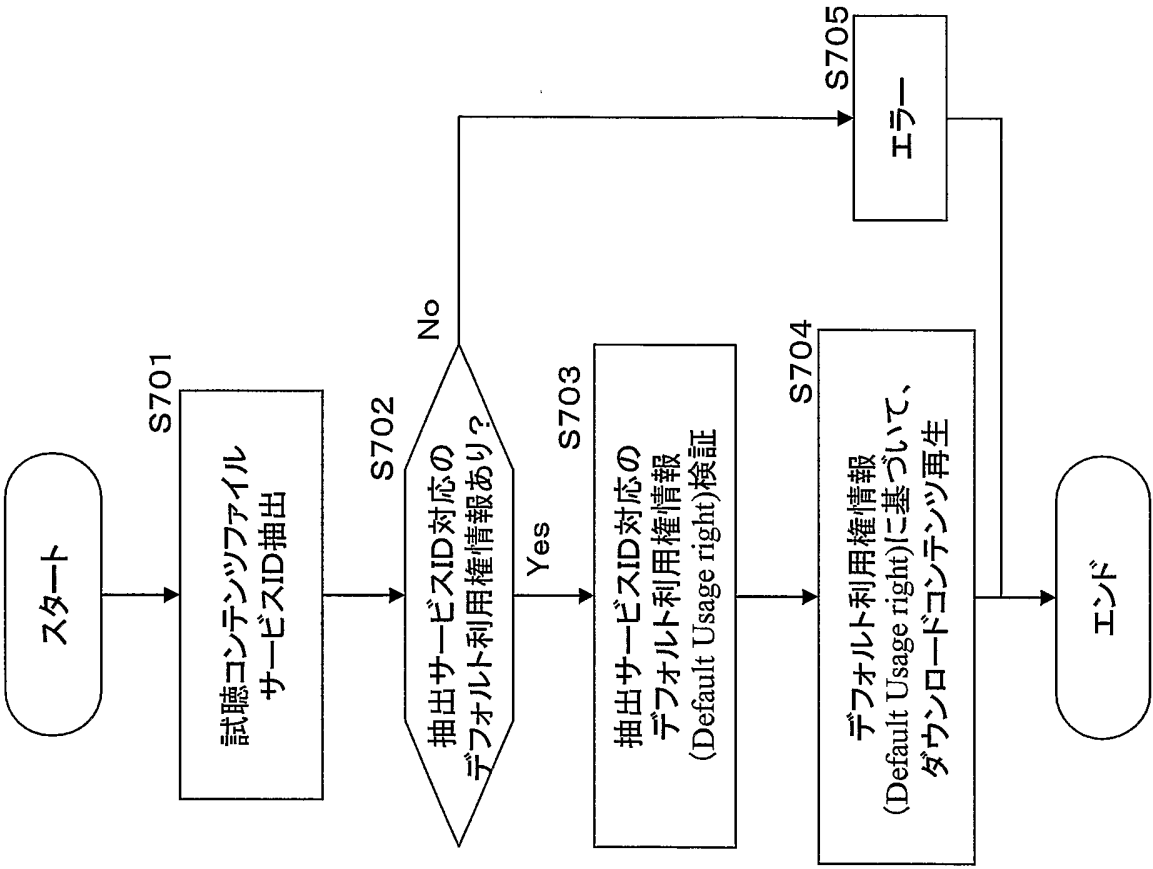


Fig.21

Fig. 22



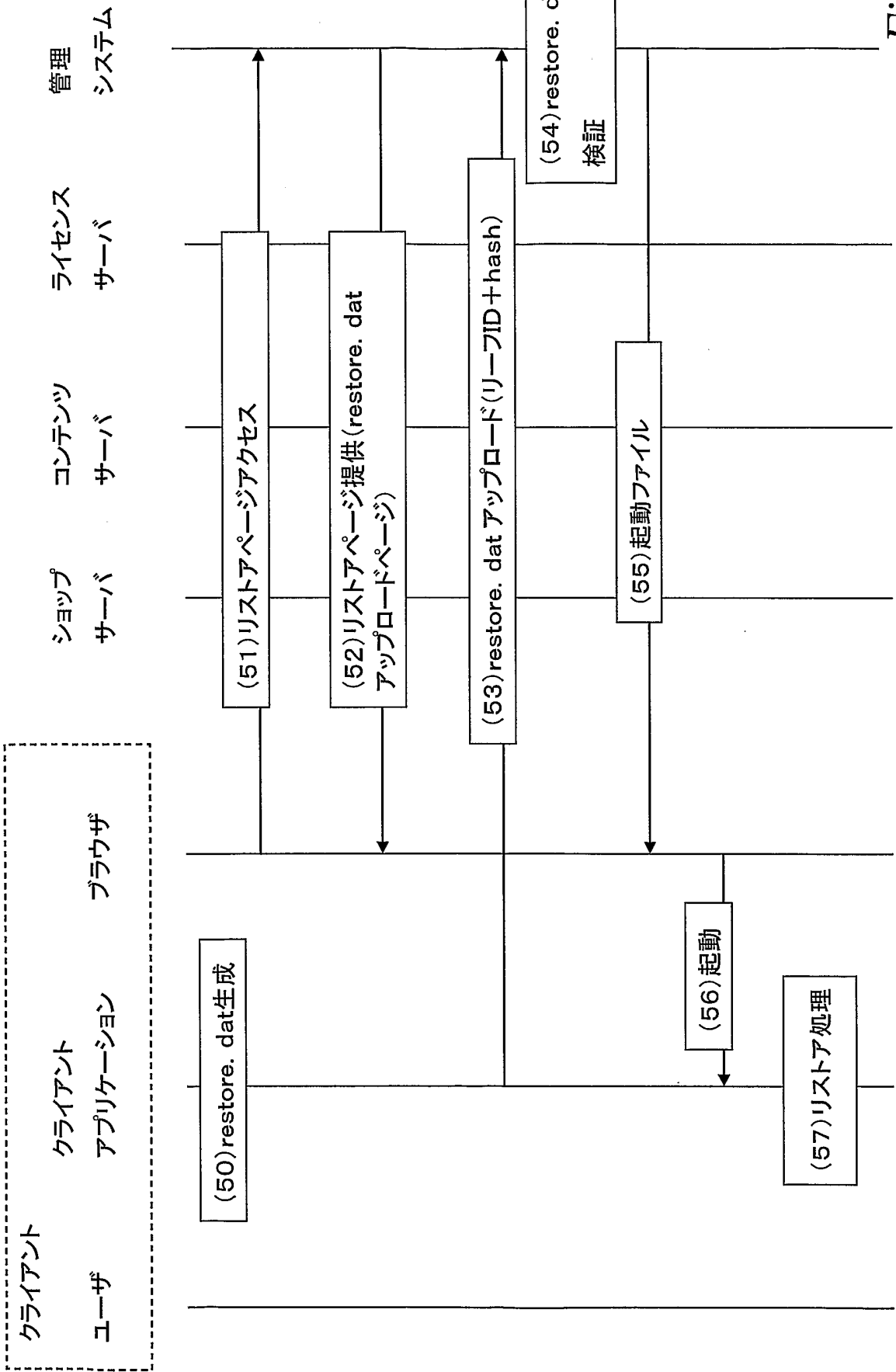


Fig. 23

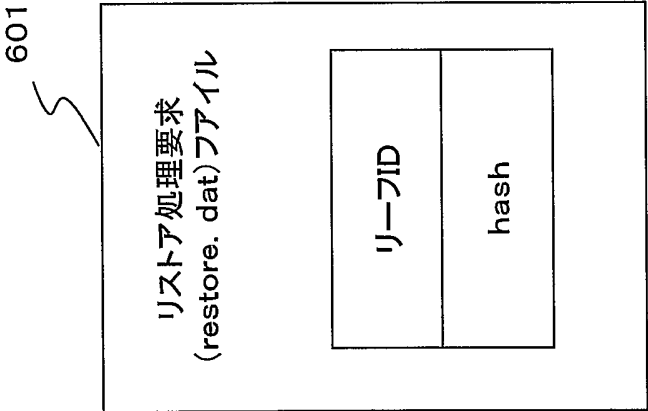
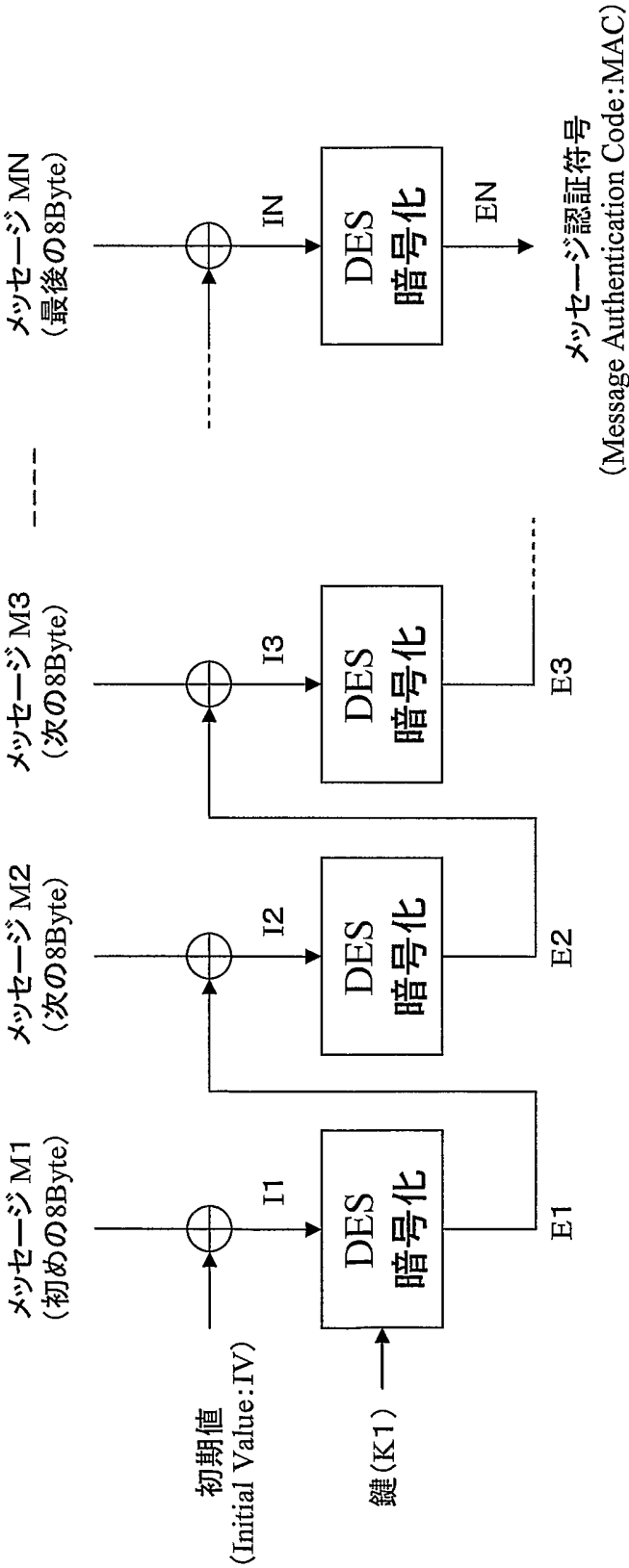


Fig. 24



$\oplus$:排他的論理和処理 (8バイト単位)

Fig.25

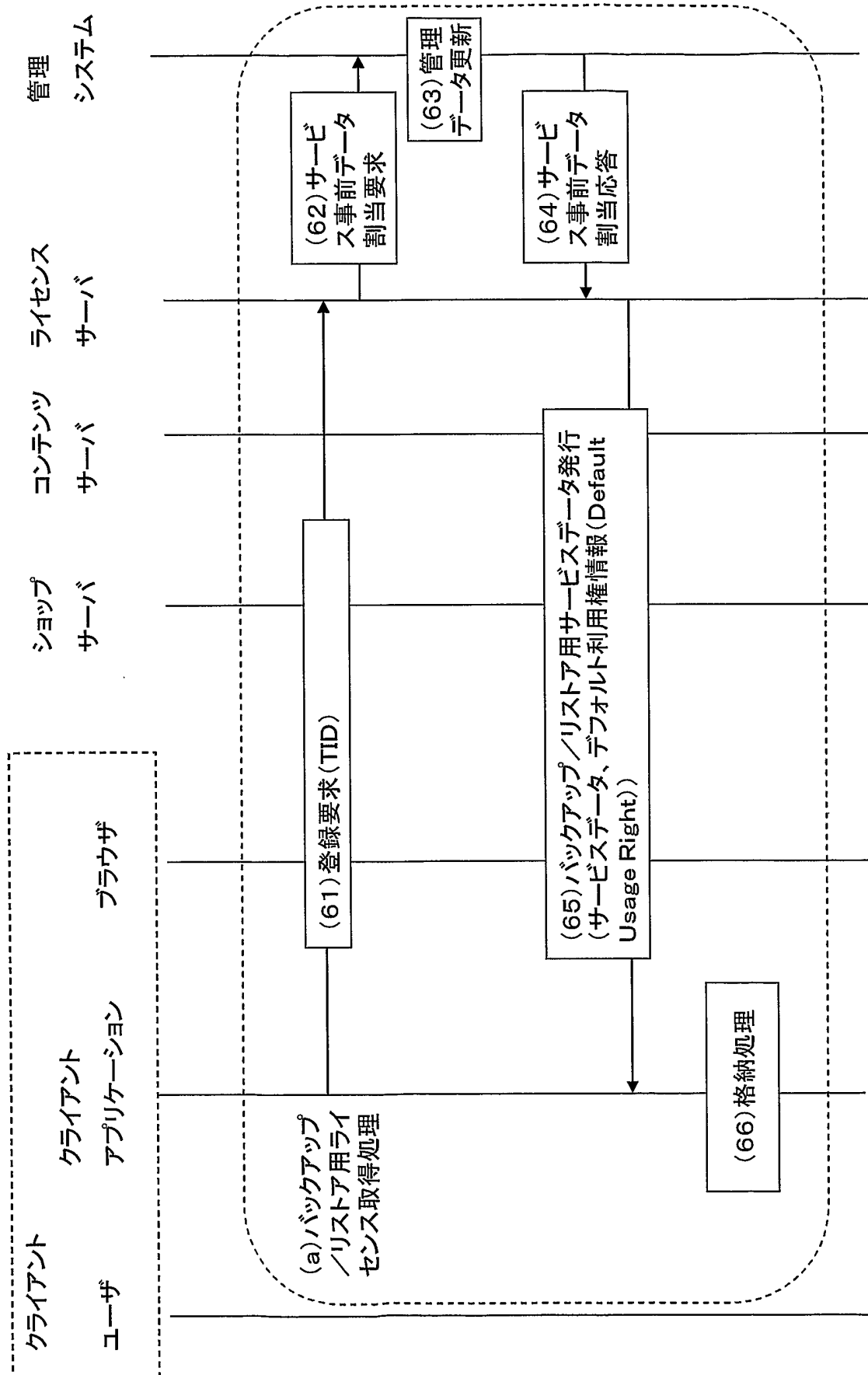


Fig. 26

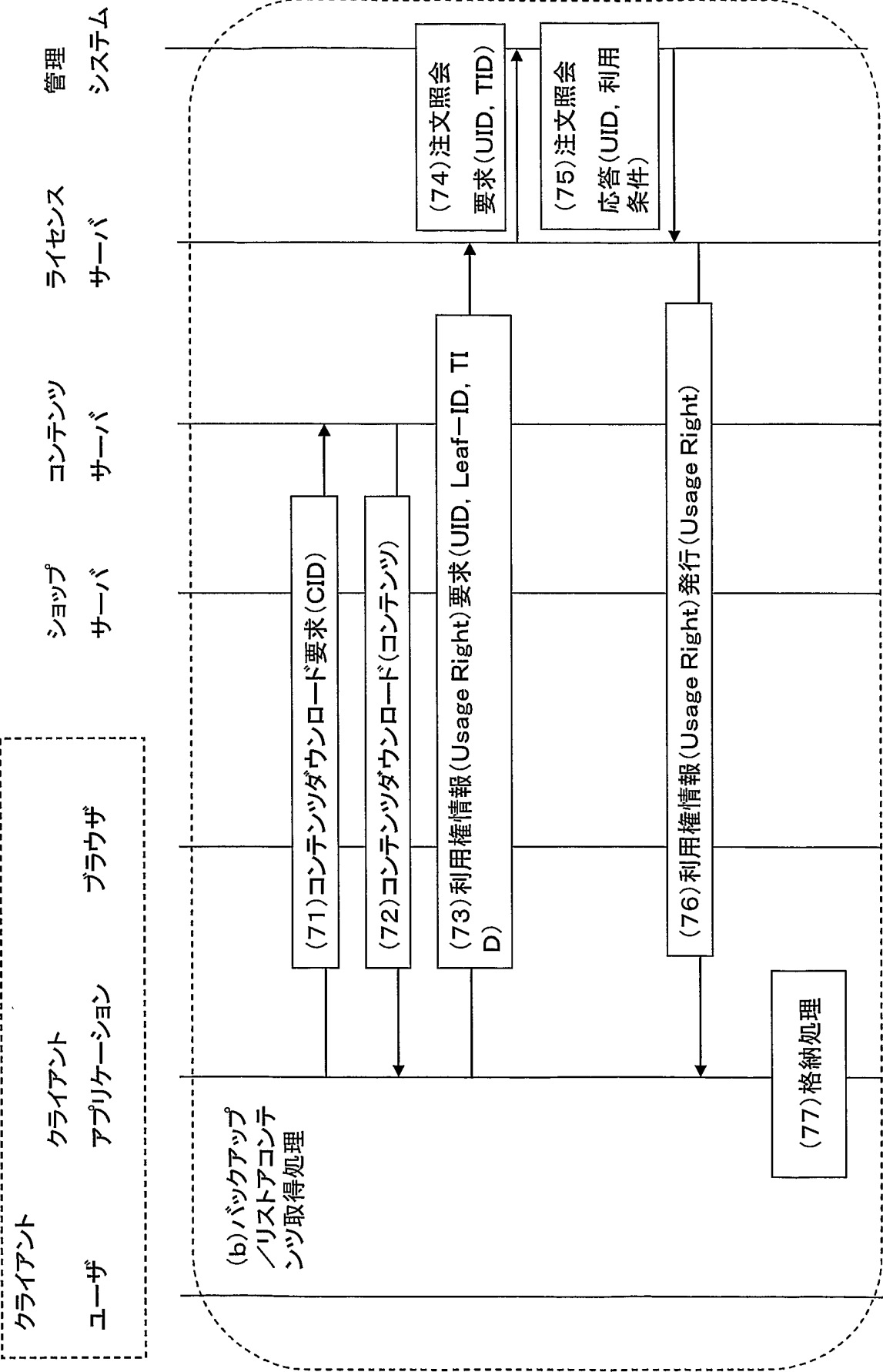
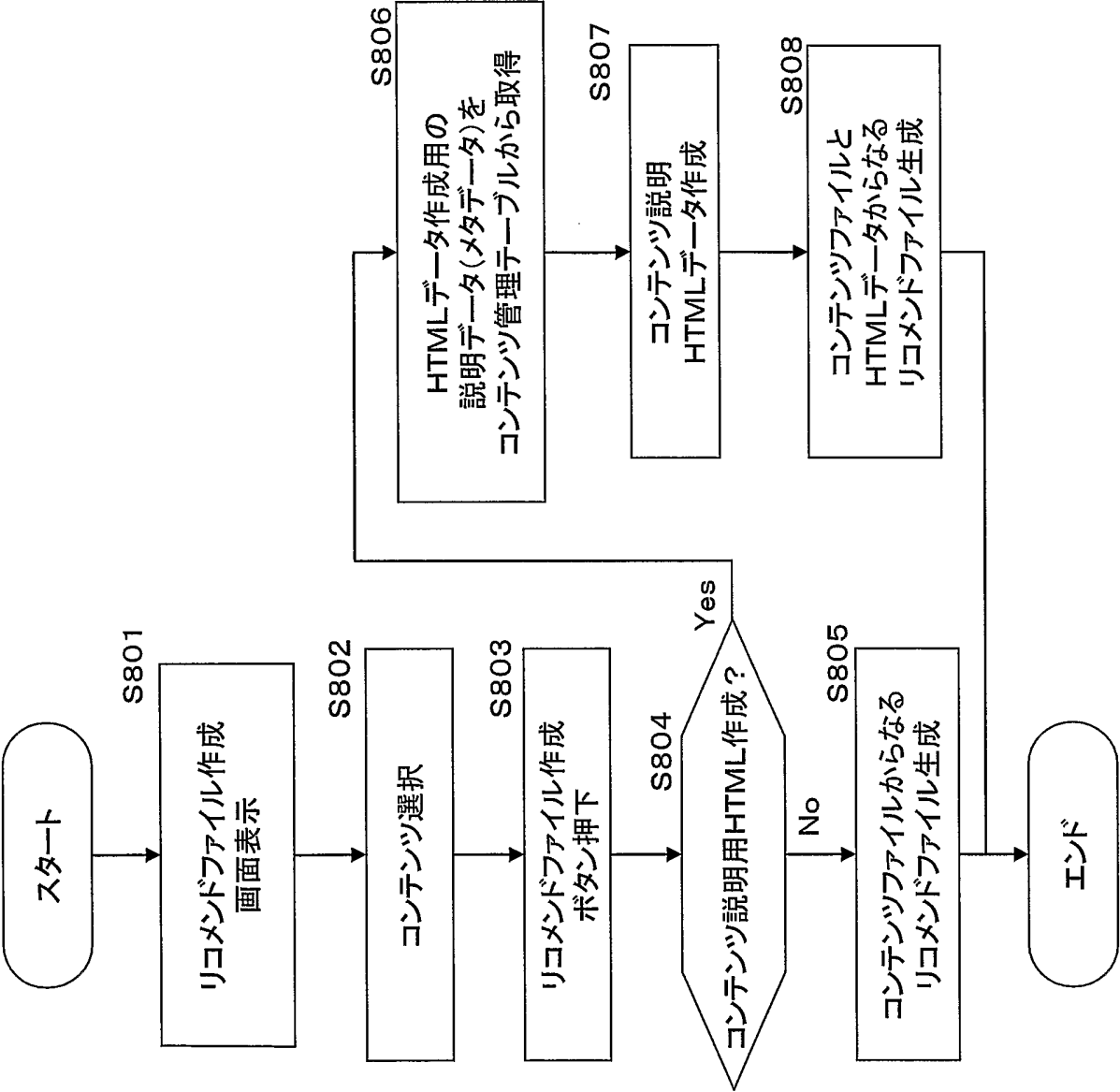


Fig. 27

Fig. 28



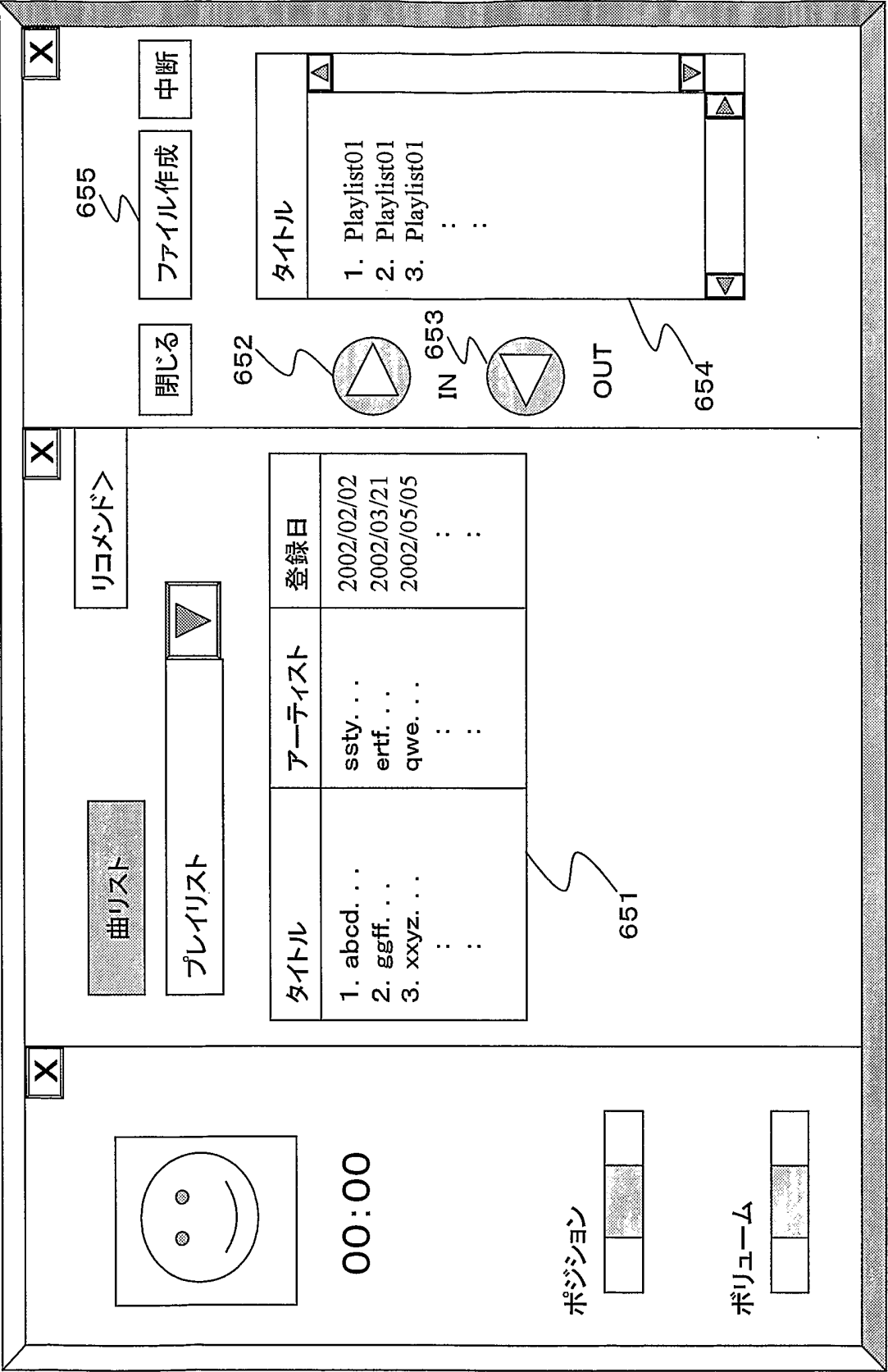


Fig. 29

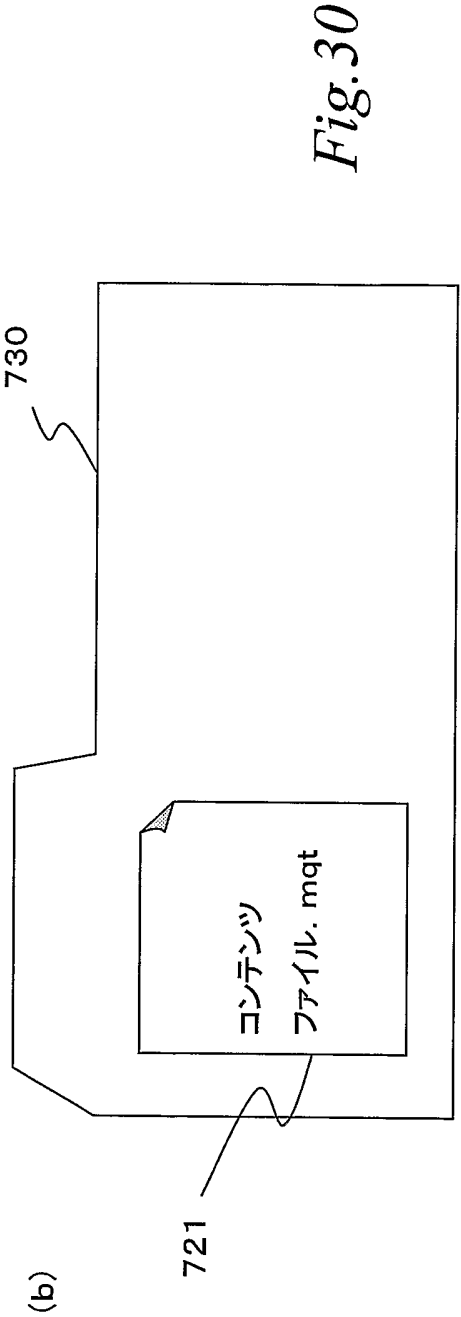
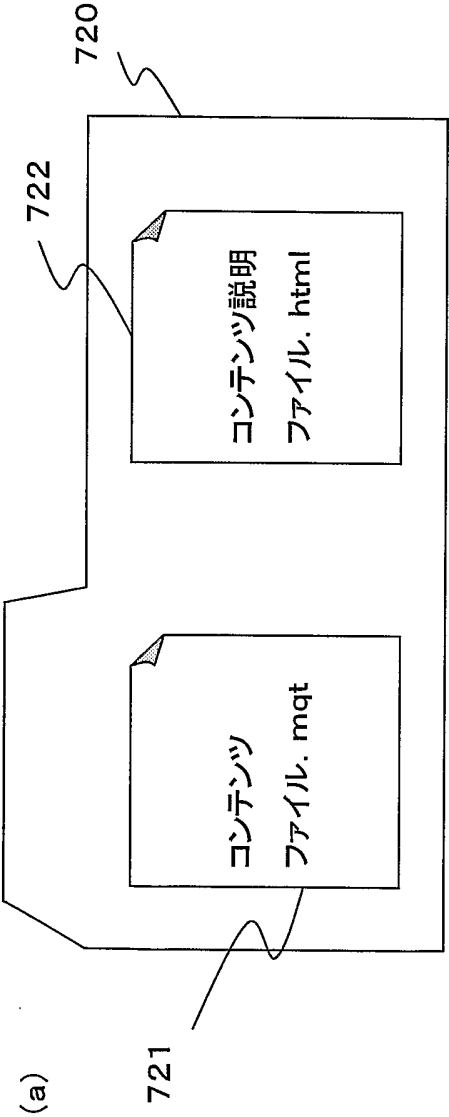


Fig. 30

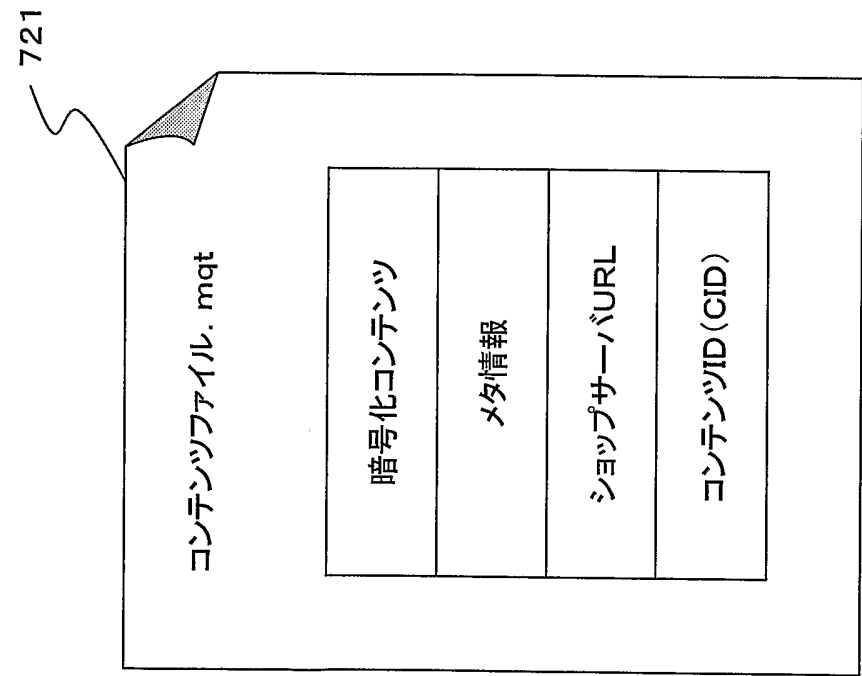


Fig. 31

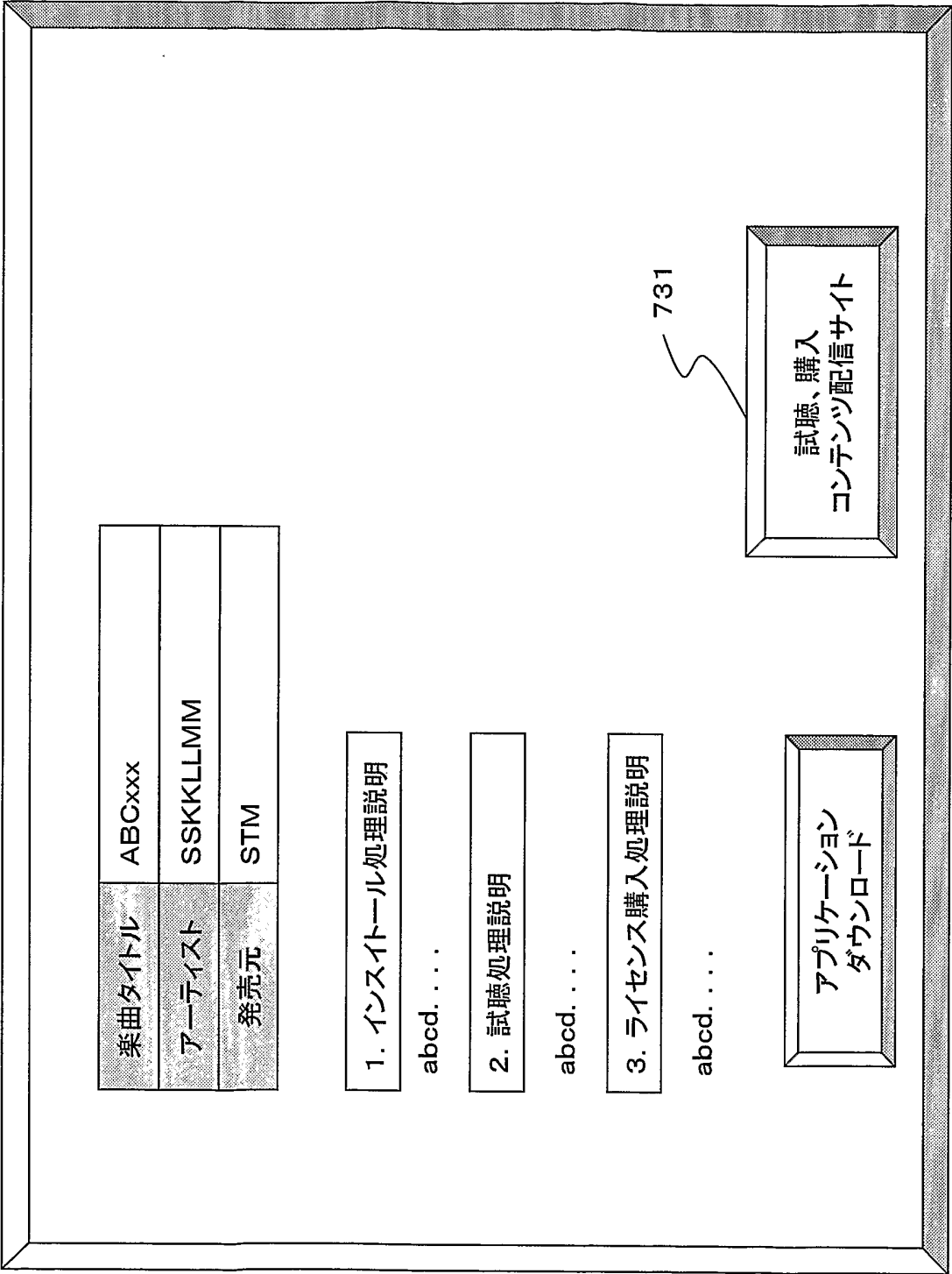


Fig. 32

33/34

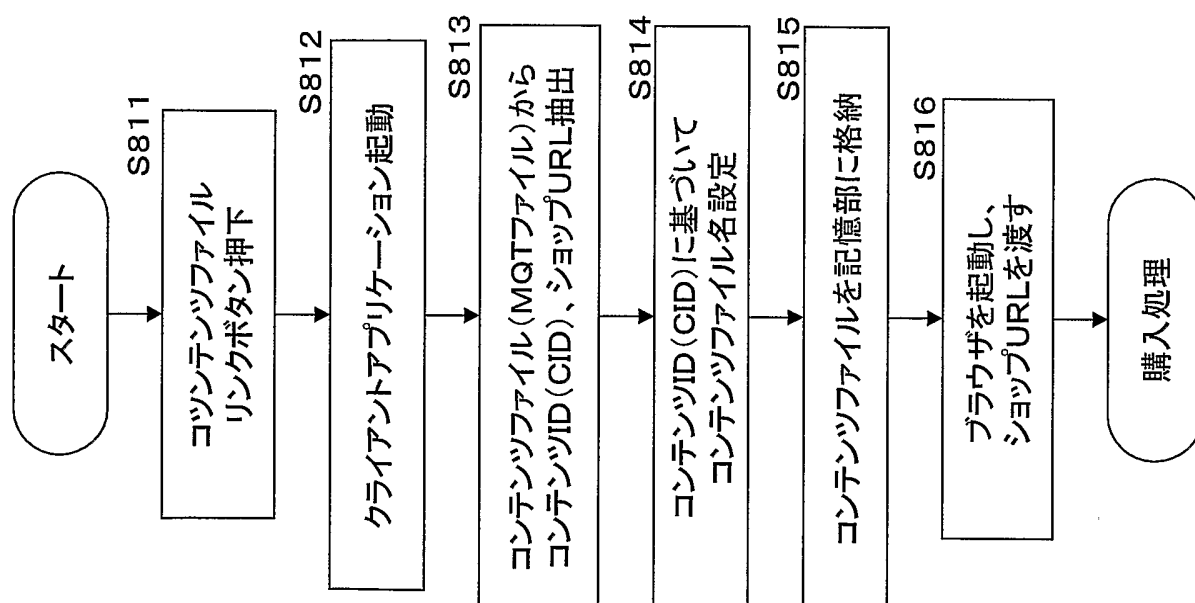


Fig.33

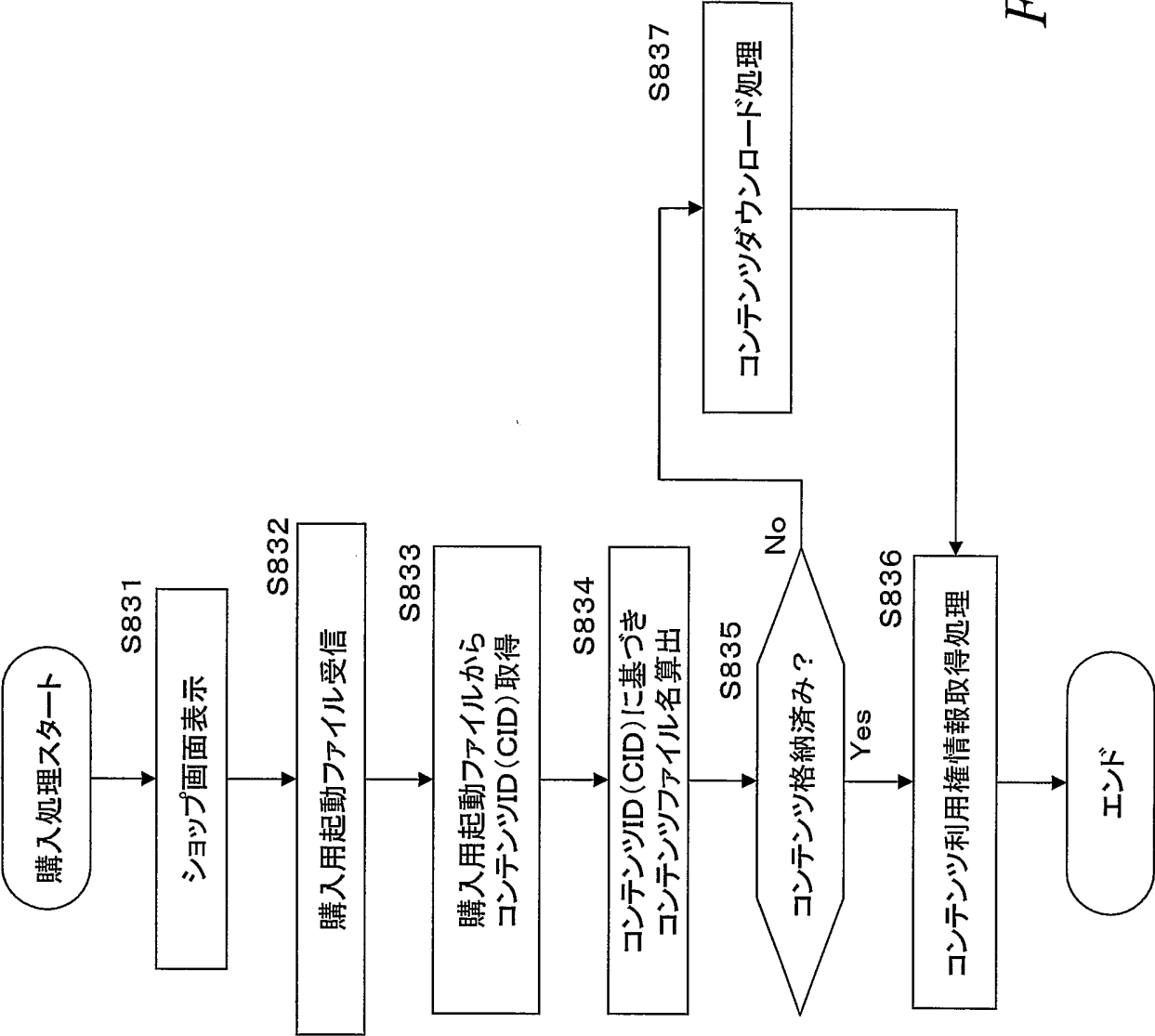


Fig.34

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP03/08267

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl⁷ G06F12/14, H04L9/08, G06F17/60

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)

Int.Cl⁷ G06F12/14, H04L9/08, G06F17/60

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

Jitsuyo Shinan Koho	1926-1996	Toroku Jitsuyo Shinan Koho	1994-2003
Kokai Jitsuyo Shinan Koho	1971-2003	Jitsuyo Shinan Toroku Koho	1996-2003

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	WO 01/44907 A1 (Microsoft Corp.), 21 June, 2001 (21.06.01),	1, 3-5, 11, 17, 19, 20
Y	All pages; all drawings & WO 01/44908 A1 & WO 01/46783 A2	2, 6-10, 12-16, 18
X	"Windows Media Rights Manager FAQ", [online], Microsoft Corporation, 2001, [retrieved on 2003- 09-04], Retrieved from the Internet: <URL: http:// web.archive.org/web/20010813233655/www.microsoft. com/japan/windows/windowsmedia/wm7/DRM/FAQ.asp? LNK=1>	1, 3-5, 11, 17, 19, 20 2, 6-10, 12-16, 18
Y		

☒ 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 document 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
05 September, 2003 (05.09.03)Date of mailing of the international search report
16 September, 2003 (16.09.03)Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP03/08267

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	Itaru HOSOMI, Masayuki NAKAE, Toshiharu ICHIYAMA,	1,3-5,11,
Y	"Digital Joho Ryutsu Architecture MediaShell to sono Riyo-Kakin Seigyo", Information Processing Society of Japan Kenkyu Hokoku 98-EIP-2, Information Processing Society of Japan, 19 September, 1998 (19.09.98), Vol.98, No.85, pages 49 to 56	17,19,20 2,6-10, 12-16,18
X	JP 2000-293439 A (Fujitsu Ltd.),	1,3-5,11,
Y	20 October, 2000 (20.10.00), All pages; all drawings (Family: none)	17,19,20 2,6-10, 12-16,18
Y	JP 8-272746 A (Xerox Corp.),	2,6-10,
	18 October, 1996 (18.10.96), All pages; all drawings & US 5634012 A & EP 715243 A1	12-16,18
Y	JP 7-221751 A (Nippon Telegraph And Telephone Corp.),	2,6-10,
	18 August, 1995 (18.08.95), All pages; all drawings (Family: none)	12-16,18
Y	JP 9-297682 A (NEC Corp.),	2,6-10,
	18 November, 1997 (18.11.97), All pages; all drawings (Family: none)	12-16,18
Y	JP 2002-133147 A (Fujitsu Ltd.),	2,6-10,
	10 May, 2002 (10.05.02), All pages; all drawings (Family: none)	12-16,18

A. 発明の属する分野の分類 (国際特許分類 (IPC))
Int. Cl⁷ G06F12/14, H04L9/08, G06F17/60

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. Cl⁷ G06F12/14, H04L9/08, G06F17/60

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 1926 - 1996
日本国公開実用新案公報 1971 - 2003
日本国登録実用新案公報 1994 - 2003
日本国実用新案登録公報 1996 - 2003

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	WO 01/44907 A1 (マイクロソフト コーポレーション) 2001.06.21, 全頁, 全図 & WO 01/44908 A1 & WO 01/46783 A2	1, 3-5, 11, 17, 19, 20
Y		2, 6-10, 12-16, 18

☒ 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

05.09.03

国際調査報告の発送日

16.09.03

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)

奥村 元宏

電話番号 03-3581-1101 内線 3585

5N 3044

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	"Windows Media Rights Manager FAQ", [online], Microsoft Corporation, 2001, [retrieved on 2003-09-04], Retrieved from the Internet: <URL: http://web.archive.org/web/20010813233655/www.microsoft.com/japan/windows/windowsmedia/wm7/DRM/FAQ.asp?LNK=1 >	1, 3-5, 11, 17, 19, 20
Y		2, 6-10, 12-16, 18
X	細見 格, 中江 政行, 市山 俊治, " デジタル情報流通アーキテクチャMediaShellとその利用・課金制御", 情報処理学会研究報告 98-EIP-2, 社団法人情報処理学会, 1998. 09. 19, Vol. 98, No. 85, pp. 49-56	1, 3-5, 11, 17, 19, 20
Y		2, 6-10, 12-16, 18
X	JP 2000-293439 A (富士通株式会社) 2000. 10. 20, 全頁, 全図 (ファミリーなし)	1, 3-5, 11, 17, 19, 20
Y		2, 6-10, 12-16, 18
Y	JP 8-272746 A (ゼロックス コーポレーション) 1996. 10. 18, 全頁, 全図 & US 5634012 A & EP 715243 A1	2, 6-10, 12-16, 18
Y	JP 7-221751 A (日本電信電話株式会社) 1995. 08. 18, 全頁, 全図 (ファミリーなし)	2, 6-10, 12-16, 18
Y	JP 9-297682 A (日本電気株式会社) 1997. 11. 18, 全頁, 全図 (ファミリーなし)	2, 6-10, 12-16, 18
Y	JP 2002-133147 A (富士通株式会社) 2002. 05. 10, 全頁, 全図 (ファミリーなし)	2, 6-10, 12-16, 18