(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2004 年4 月22 日 (22.04.2004)

PCT

(10) 国際公開番号
WO 2004/034636 A1

(51) 国際特許分類[7]: H04L 9/32, 9/06

(21) 国際出願番号: PCT/JP2003/012847

(22) 国際出願日: 2003 年10 月7 日 (07.10.2003)

(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2002-296782 2002 年10 月9 日 (09.10.2002) 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３５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): 松井 康範 (MATSUI,Yasunori) [JP/JP]; 〒141-0001 東京都 品川区 北品川６丁目７番３５号 ソニー株式会社内 Tokyo (JP).

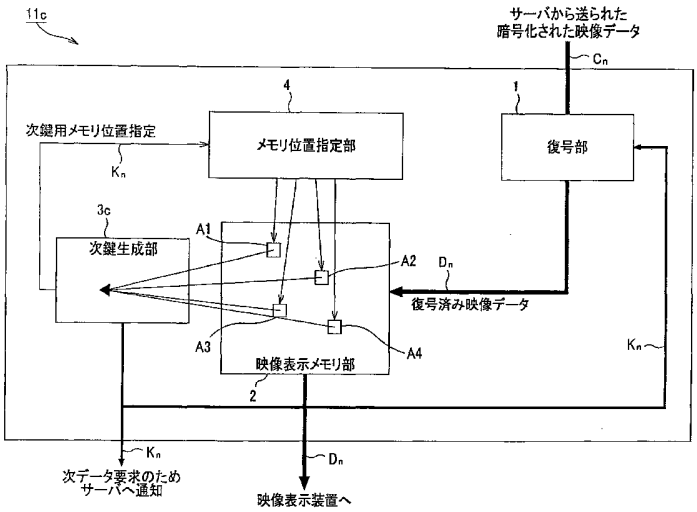
(74) 代理人: 小池 晃, 外(KOIKE,Akira et al.); 〒100-0011 東京都 千代田区 内幸町一丁目１番７号 大和生命ビル１１階 Tokyo (JP).

(81) 指定国 (国内): CN, KR, US.

添付公開書類:
— 国際調査報告書

(54) Title: DATA MANAGEMENT SYSTEM AND ATA DECODING DEVICE

(54) 発明の名称: データ管理システム及び データ復号装置



Cn...ENCRYPTED VIDEO DATA TRANSMITTED FROM SERVER
Kn...MEMORY POSITION SPECIFICATION FOR THE NEXT KEY
4...MEMORY POSITION SPECIFICATION SECTION
1...DECRYPTION SECTION
3c...NEXT KEY GENERATION SECTION
Dn...DECRYPTED VIDEO DATA
2...VIDEO DISPLAY MEMORY SECTION
Kn...NOTIFICATION TO SERVER FOR THE NEXT DATA REQUEST
Dn...TO VIDEO DISPLAY DEVICE

(57) **Abstract:** A data management system (300) includes a server device (20c) for transmitting a partial content C_n obtained by dividing an encrypted content C by a predetermined time unit and a client terminal (10c) for viewing/hearing the content. The client terminal decrypts the content C_n by using an encryption key K_{n-1} acquired as a decryption key from the partial content C_{n-1}, writes the decrypted data into a memory section (2) so as to cause a display device to display it, and generates a decryption key K_n from the decrypted data written into the memory section (2). This encryption key K_n is used as a decryption key of the next content C_{n+1}

[続葉有]

WO 2004/034636 A1

and sent to a key management server device (24), where it is used for authentication of the client terminal. The server device next transmits a content only to the client terminal authenticated.

(57) 要約:

本発明は、暗号化されたコンテンツＣが所定時間単位毎に分割された部分コンテンツC_nをネットワークを介して送信するサーバ装置（２０ｃ）と、コンテンツを視聴するクライアント端末（１０ｃ）とを備えるデータ管理システム（３００）であり、クライアント端末は、部分コンテンツC_{n-1}から取得した暗号鍵K_{n-1}を復号鍵としてコンテンツC_nを復号し、この復号データを表示装置に表示させるためのメモリ部２に書き込み、メモリ部２に書き込まれた復号データから暗号鍵K_nを生成する。この暗号鍵K_nは、次のコンテンツC_{n+1}の復号鍵として使用されるとともに、鍵管理サーバ装置（２４）に送られ、クライアント端末の認証として使用され、サーバ装置は、認証したクライアント端末に対してのみ次にコンテンツを送信する。

データ管理システム及びデータ復号装置

明細書

データ管理システム、データ管理方法、クライアント端末、サーバ装置、データ復号装置、データ復号方法、及び記録媒体

技術分野

本発明は、サーバ装置からネットワークを介して接続されたクライアント端末に送信されるデータを管理するデータ管理システム、及びデータ管理方法、並びにこのデータ管理システムを構成するクライアント端末、及びサーバ装置、並びにサーバ装置からネットワークを介して送られるようなデータを管理するのに好適な暗号化データが記録された記録媒体、及びこれを復号するデータ復号装置及びデータ復号方法に関する。

本出願は、日本国において２００２年１０月９日に出願された日本特許出願番号２００２－２９６７８２を基礎として優先権を主張するものであり、この出願は参照することにより、本出願に援用される。

背景技術

映像や音声をデジタルデータとして配信して、表示し出力するシステムにおいては、映像や音声に関するコンテンツの著作権を保護する処理を施すことが必要となる。即ち、デジタルデータは複製によってデータの劣化が発生しないため、複製データがそのまま視聴できるようになっていると大量のコピーが生成され、コンテンツの商業的価値を減じてしまうことになるためである。

そのため、デジタル映像・音声データに対しては、著作権管理システムによって暗号化等による保護策をとるようにし、データのコピーはできても、暗号化されたデータを復号する鍵がない限り再生をできないようにすることが一般的である。鍵の管理によってコンテンツの視聴を制御するようになっている。

例えば、ブロック単位で暗号化したデータを、前のブロックデータと連鎖させ

ていくことで、暗号強度を上げるＣＢＣ（Ciphering Block Chaining）方式により著作権保護を図った技術が特開２００２－２０２７１９号公報に記載されている。

この特許文献に記載の技術においては、コンテンツデータをブロック化し、鎖状に連鎖して暗号化することにより、暗号強度を上げるとともに、暗号化を行う際の最初のブロックに必要な初期値を、例えばＭＰＥＧストリームの場合には、ヘッダのユニークな情報等、そのセクタのコンテンツデータから生成することにより、データ領域のロスを低減するものである。

近時、コンテンツ提供者が提供する著作権が保護されず、コンテンツ提供者に多大な被害を与える場合がある。上述の鍵管理は数学理論に基づいた高度な暗号システムに基づくものであるものの、近年の暗号技術開発・研究の急速な進展、及び計算機の高速化に伴い、暗号鍵を破られるケースが多発している。暗号鍵は、一度破られてしまうと、その手法及び復号されたコンテンツがインターネット等を通じて急速に広まるため、コンテンツ提供者側に対して深刻な被害をもたらす。暗号化されているとはいえ、１つのコンテンツの全データが利用者側に置かれている場合、暗号が破られると、１つのコンテンツがまるまるコピーされてしまうことになる。したがって、コンテンツは、複数の部分データに分けて管理することが望ましいが、コンテンツの一部分を実際に視聴しなくても、次の部分を要求することができてしまえば、悪意のあるユーザによってコンテンツ全体のデータの取得が可能である。

また、コンテンツ提供者にとってのもう１つの問題として、デジタル映像及び音声データの場合、任意の時間から視聴を開始したり、番組途中に挿入されているＣＭ（コマーシャルフィルム）を視聴せずに飛ばして視聴したりすることが容易である。例えば、上述の特許文献に記載された技術においても、一旦データを復号すれば、そのデータを任意の時間から視聴したり、飛ばして視聴したりすることが可能となる。これは、視聴者側の利便性を向上させるものの、コンテンツ提供者にとっては広告効果を減じることになり、好ましいものでない。

発明の開示

本発明の目的は、上述したような従来の技術が有する問題点を解消することができる新規なデータ管理システム、データ管理方法、クライアント端末、サーバ装置、データ復号装置、データ復号方法、及び記録媒体を提供することにある。

本発明の他の目的は、コンテンツデータの提供者側の被害を低減し、且つコンテンツデータを安全に管理することができるデータ管理システム、及びデータ管理方法、並びにクライアント端末及びサーバ装置を提供することにある。

本発明の更に他の目的は、暗号化データを提供者側の被害を低減し、且つ安全に管理することができる暗号化データが記録された記録媒体、及びこれを復号するデータ復号装置及びデータ復号方法を提供することにある。

本発明に係るデータ管理システムは、ネットワークに接続され、ブロック化されたブロックデータを順次送信するサーバ装置と、ネットワークに接続されサーバ装置からのブロックデータを受信して再生するクライアント端末とを有するデータ管理システムであって、クライアント端末は、ブロックデータを記憶するデータ記憶手段と、データ記憶手段に記憶されたデータに基づき認証鍵を生成する鍵生成手段と、鍵生成手段により生成された認証鍵をサーバ装置に送信する送信手段とを備え、サーバ装置は、クライアント端末から送信された認証鍵を認証する認証手段と、この認証手段により該認証鍵を認証したときのみ次のブロックデータを送信する送信手段とを備える。

本発明においては、サーバ装置は、ブロックデータを送信した後、クライアント端末からの認証鍵を受信し、認証しなければ、次のブロックデータを送信しないため、サーバ装置が認証していない第三者にブロックデータが送信されることを防止して、サーバ装置が送信するデータを安全に管理することができる。

また、ブロックデータは、所定の時間単位に分割され、暗号化された暗号化データであって、クライアント端末は、暗号化データを復号する復号手段を有することができ、暗号化データを送信するようにすれば、更にサーバ装置から送信されるデータの安全性が高まる。

更に、鍵生成手段は、データ記憶手段に記憶されたデータに基づき復号鍵を生成し、復号手段は、復号鍵を使用して暗号化データを復号するか、認証鍵に基づ

き復号鍵を生成し、復号手段は、復号鍵を使用して暗号化データを復号するか、鍵生成手段により生成された認証鍵を復号鍵として使用して暗号化データを復号することにより、サーバ装置に認証されたクライアント端末でしか、暗号化データを復号する復号鍵を取得することができない。

更にまた、データ記憶手段は、ＶＲＡＭ（ビデオメモリ）であり、クライアント端末は、ＶＲＡＭに書き込まれたデータを表示する表示装置であり、鍵生成手段は、ＶＲＡＭにデータが書き込まれて表示装置に表示されると復号鍵を生成することができ、これにより、クライアント端末である表示装置に表示するためのＶＲＡＭにデータを展開しなければ、復号鍵を生成することができず、次のデータを得るために前のデータを必ず再生し若しくは表示する必要があるため、クライアント端末の使用者は、データを途中から再生したり、飛ばして再生することがなく、データ提供者側の被害を低減する。

本発明に係るデータ管理方法は、ネットワークに接続され、ブロック化されたブロックデータを順次送信するサーバ装置と、ネットワークに接続されサーバ装置からのブロックデータを受信して再生するクライアント端末とを有するデータ管理システムのデータ管理方法であって、サーバ装置がブロックデータをクライアント端末に送信する送信工程と、クライアント端末がサーバ装置から送信されたブロックデータを受信してデータ記憶手段に記憶するデータ記憶工程と、データ記憶手段に記憶されたデータに基づき認証鍵を生成する鍵生成工程と、鍵生成工程にて生成された認証鍵をサーバ装置に送信する送信工程と、サーバ装置がクライアント端末から送信された認証鍵を認証する認証工程とを有し、サーバ装置のブロックデータをクライアント端末に送信する送信工程では、認証工程にて認証鍵を認証した場合のみ、次のブロックデータが送信される。

本発明においては、サーバ装置の送信工程では、クライアント端末から送信された認証鍵を認証したときのみ次のブロックデータが送信されるため、サーバ装置に認証されていないクライアント端末にはブロックデータが送られることがなく、サーバ装置から送信するデータを安全に管理することができる。

本発明に係るクライアント端末は、ブロック化されたブロックデータを順次送信するサーバ装置にネットワークを介して接続され、サーバ装置からのブロック

データを受信して再生するクライアント端末であって、サーバ装置から送信されるブロックデータを受信する受信手段と、ブロックデータを記憶するデータ記憶手段と、データ記憶手段に記憶されたデータに基づき認証鍵を生成する鍵生成手段と、鍵生成手段により生成された認証鍵をサーバ装置に送信する送信手段とを備え、受信手段は、サーバ装置が上記送信手段により送信された認証鍵を認証したときのみ、次のブロックデータを受信する。

本発明に係るサーバ装置は、ブロック化されたブロックデータを、ネットワークを介してクライアント端末に順次送信するサーバ装置であって、ブロックデータを送信する送信手段と、クライアント端末がブロックデータに基づき生成した認証鍵を受信する受信手段と受信手段により受信された記認証鍵を認証する認証手段とを有し、送信手段は、認証手段により認証鍵が認証されたときのみ、ブロックデータを送信する。

本発明に係るデータ管理システムは、ネットワークに接続され、暗号化された複数の暗号化データを送信するサーバ装置と、ネットワークに接続されサーバ装置から送信される暗号化データを受信するクライアント端末とを有するデータ管理システムであって、サーバ装置は、暗号化データを送信する送信手段を少なくとも備え、クライアント端末は、暗号化データを復号する復号手段と、復号手段により復号された復号データを記憶するデータ記憶手段と、データ記憶手段に記憶された復号データに基づき暗号鍵を生成する暗号鍵生成手段とを備え、クライアント端末の復号手段は、暗号鍵生成手段により、第１の暗号化データが復号された第１の復号データから生成された暗号鍵が供給され、暗号鍵を使用して第１の暗号化データの次の第２の暗号化データを復号する。

本発明においては、サーバ装置から送られてくる複数の暗号化データは、前の暗号化データが復号された復号データから生成された暗号鍵を復号鍵としなければ、次の暗号化データを復号できないため、最初の暗号化データを復号できないクライアント端末では、暗号化データを復号することができず、サーバ装置が送信するデータを安全に管理することができる。

また、クライアント端末は、暗号鍵をサーバ装置に送信する送信手段を有し、サーバ装置は、クライアント端末からの暗号鍵を受信する受信手段を有し、サー

バ装置の送信手段は、受信手段が第１の暗号化データに基づく第１の暗号鍵を受信すると、第２の暗号化データを送信してもよく、前の暗号化データから生成した暗号鍵を次の暗号化データの復号鍵として使用するとともに、クライアント端末の認証として使用することができ、更にサーバ装置が送信するデータを更に安全に管理することができる。

更に、データ記憶手段は、ＶＲＡＭであり、クライアント端末はＶＲＡＭに書き込まれたデータを表示する表示装置であり、鍵生成手段は、ＶＲＡＭに第１の復号データが書き込まれて表示装置に表示されると第２の暗号化データを復号する暗号鍵を生成することができ、クライアント端末は、データを一旦ＶＲＡＭに書き込んで再生し若しくは表示しなければ、次の暗号化データを復号する暗号鍵を生成することができないため、クライアント端末の使用者がデータを任意の位置から再生したり、飛ばして再生したりすることがない。

本発明に係るデータ管理方法は、ネットワークに接続され、複数の暗号化データを送信するサーバ装置と、該ネットワークに接続されサーバ装置から送信される暗号化データを受信するクライアント端末とを有するデータ管理システムのデータ管理方法であって、サーバ装置がクライアント端末に暗号化データを送信する送信工程と、クライアント端末がサーバ装置から送信された暗号化データを受信して復号する復号工程と、クライアント端末が復号工程にて復号された復号データをデータ記憶手段に記憶するデータ記憶工程と、クライアント端末がデータ記憶工程にて記憶された復号データに基づき暗号鍵を生成する暗号鍵生成工程とを有し、復号工程では、第１の暗号化データが復号された第１の復号データから暗号鍵生成工程にて生成された第１の暗号鍵を使用して、第１の暗号化データの次に受信された第２の暗号化データが復号される。

本発明においては、サーバ装置からクライアント端末に送信される時間的に連続する第１及び第２の暗号化データにおいて、第１の暗号化データから生成された第１の暗号鍵により、第２の暗号化データが復号されるため、第１の暗号化データを取得していないクライアント端末では第２の暗号化データを復号することができず、サーバ装置が送信するデータを安全に管理することができる。

本発明に係るクライアント端末は、複数の暗号化データを送信するサーバ装置

にネットワークを介して接続され、サーバ装置から送信される暗号化データを受信するクライアント端末であって、暗号化データを受信する受信手段と、暗号化データを復号する復号手段と、復号手段により復号された復号データを記憶するデータ記憶手段と、データ記憶手段に記憶された復号データに基づき暗号鍵を生成する暗号鍵生成手段とを備え、復号手段は、暗号鍵生成手段により、第１の暗号化データが復号された第１の復号データから生成された第１の暗号鍵が供給され、第１の暗号鍵を使用して第１の暗号化データの次に受信された第２の暗号化データを復号する。

本発明に係るデータ復号装置は、所定の時間単位に分割され、暗号化された複数の暗号化データを復号するデータ復号装置において、暗号化データを復号する復号手段と、復号手段により復号された復号データを記憶するデータ記憶手段と、データ記憶手段に記憶された復号データに基づき暗号鍵を生成する暗号鍵生成手段とを備え、復号手段は、暗号鍵生成手段により、第１の暗号化データが復号された第１の復号データから生成された第１の暗号鍵が供給され、第１の暗号鍵を使用して第１の暗号化データの次の第２の暗号化データを復号する。

本発明に係る記録媒体は、所定の時間単位に分割され、暗号化された複数の暗号化データが記録された記録媒体であって、第２の暗号化データを復号する第１の復号鍵が、第２の暗号化データの時間的に前の第１の暗号化データが復号された復号データに含まれるものであって、第１の復号鍵は、第１の暗号化データを復号して再生すると得られるものである。

本発明の更に他の目的、本発明によって得られる具体的な利点は、以下において図面を参照して説明される実施の形態の説明から一層明らかにされるであろう。

図面の簡単な説明

図１Ａは、本発明の第１の実施の形態におけるデータ管理システムを模式的に示すブロック図であり、図１Ｂは、サーバ装置から視聴端末であるクライアント端末に配信されるコンテンツを示す模式図である。

図２は、本発明の第１の実施の形態におけるクライアント端末のデータ視聴管

理部を示すブロック図である。

図３は、本発明の第２の実施の形態におけるデータ管理システムを模式的に示すブロック図である。

図４は、本発明の第２の実施の形態におけるクライアント端末のデータ視聴管理部を示すブロック図である。

図５は、本発明の第３の実施の形態におけるデータ管理システムを模式的に示すブロック図である。

図６は、本発明の第３の実施の形態におけるデータ管理システムにおけるデータの流れを示す図である。

図７は、本発明の第３の実施の形態におけるクライアント端末１０ｂのデータ視聴管理部を示すブロック図である。

図８Ａ及び図８Ｂは、本発明の第３の実施の形態におけるデータ管理システム全体の動作を示す図であって、夫々サーバ装置側の動作、及び端末側の動作を示すフローチャートである。

図９は、本発明の第３の実施の形態においけるクライアント端末の暗号鍵生成方法を示すフローチャートである。

発明を実施するための最良の形態

以下、本発明を適用した具体的な実施の形態について、図面を参照しながら詳細に説明する。

上述したように、ユーザが実際にコンテンツの一部を視聴したことを確認した後、その次の部分のコンテンツを提供できるようなシステムが望まれているが、ユーザに対して、例えば、ＣＭをみたらボタンを押す等の明示的な入力フィードバックをいちいち要求するのは非現実的である。

ところで、通常のデジタル機器であれば、デジタルデータの表示用メモリであるＶＲＡＭ（ＶｉｄｅｏＲＡＭ）にデータが書き込まれることによって、そのデータが示す映像がディスプレイに表示される。そこで、本実施の形態においては、ＶＲＡＭにデータを書き込むことをデータの表示とみなし、映像データがＶＲＡ

Mに展開されなければ、即ち、映像データがディスプレイに表示されなければ、次のコンテンツが取得できないようなしくみを提供するものである。なお、以下では、映像データを再生するシステムについて説明するが、音声データに関しても、同様に構築することができることは言うまでもない。

以下、本発明の第１の実施の形態について説明する。

図１Ａは、本第１の実施の形態におけるデータ管理システムを模式的に示すブロック図、図１Ｂは、サーバ装置から視聴端末であるクライアント端末に配信されるコンテンツを示す模式図である。図１Ａに示すように、データ管理システム１００は、コンテンツ配信事業者により管理されるサーバ装置２０ａと、配信されるコンテンツを視聴するクライアント端末１０ａとから構成され、両者はネットワークを介して接続されている。サーバ装置２０ａは、コンテンツを実際に配信するコンテンツ配信サーバ装置２１ａと、クライアント端末１０ａの認証鍵を管理する認証管理サーバ装置２２とから構成される。クライアント端末１０ａは、データ視聴管理部１１ａを有する。

コンテンツ配信サーバ装置２１ａは、図１Ｂに示すように、１つの映像を示す映像データであるコンテンツＣを複数のブロックデータに分割した部分コンテンツC_n（C_1～C_n）を順次クライアント端末１０ａに送信する。このブロックデータのブロック長（時間長さ）は、一定長でも可変でもよい。クライアント端末１０ａは、データ視聴管理部１１ａにより、コンテンツ配信サーバ装置２１ａから送信される部分コンテンツC_nを順次再生（表示）する。

コンテンツ配信サーバ装置２１ａは、図１Ｂに示すように、１つの映像を示す映像データであるコンテンツＣを複数のブロックデータに分割した部分コンテンツC_n（C_1～C_n）を順次クライアント端末１０ａに送信する。このブロックデータのブロック長（時間長さ）は、一定長でも可変でもよい。クライアント端末１０ａは、データ視聴管理部１１ａにより、コンテンツ配信サーバ装置２１ａから送信される部分コンテンツC_nを順次再生（表示）する。

クライアント端末１０ａは、サーバ装置２０の認証管理サーバ装置２２に対し、コンテンツ視聴許可の要求R_0をし、この要求R_0がサーバ装置２０にて承諾されるとコンテンツ配信サーバ装置２１ａからは、最初のコンテンツC_1が送信される。

要求R_0としては、クライアント端末１０ｂを識別可能な認証番号等を合わせて送信するようにしてもよい。

クライアント端末１０ａは、最初のコンテンツC_1から、後述する方法により次の部分コンテンツC_2の要求R_1を行うための鍵K_1を生成する。この鍵K_1の一部又は全部をクライアント端末１０ａの認証として認証管理サーバ装置２２に送信する。本実施の形態においては、鍵K_1をクライアント端末１０ａの認証とするとともに、コンテンツＣ２の要求R_1とするものとする。この鍵K_1は、鍵K_0を持たないクライアント端末では生成不可能なため、クライアント端末１０ａの認証として使用することができる。

認証管理サーバ装置２２は、追加データである次コンテンツC_2の要求R_1があると、クライアント端末１０ａから送信された鍵K_1を確認し、確認すると、コンテンツ配信サーバ装置２１ａに対して、次コンテンツC_2をクライアント端末１０ａへ送信するよう指示する。コンテンツ配信サーバ装置２１ａは、この指示に従い次コンテンツC_2をクライアント端末１０ａに送信する。クライアント端末１０ａでは、次コンテンツC_2から再び鍵K_2を生成する。この鍵K_2は、コンテンツC_2の次のコンテンツC_3の要求R_2及びクライアント端末１０ａの認証に使用される。

次に、上述の鍵の生成について説明する。図２は、クライアント端末１０ａのデータ視聴管理部１１ａを示すブロック図である。データ視聴管理部１１ａは、コンテンツ配信サーバ装置２１ａから送信される映像データからなる部分コンテンツC_nを受信する受信部（図示せず）と、この部分コンテンツC_nを記憶する映像表示メモリ部２と、映像表示メモリ部２に書き込まれた映像データに基づき鍵K_nを生成する次鍵生成部３ａと、鍵K_nを生成するために、映像表示メモリ部２のデータのアドレスを指定するメモリ位置指定部４とを備える。

映像表示メモリ部２は、所謂ＶｉｄｅｏＲＡＭ、又はフレームバッファと呼ばれる映像表示用のメモリである。この映像表示メモリ部２には、部分コンテンツC_nが供給されて展開されると、図示しない映像表示装置に映像が表示される。この映像表示メモリ部２は、部分コンテンツC_nが供給されると、メモリ位置指定部４によって映像表示メモリ部２内のアドレスが指定される。

次鍵生成部３ａは、映像表示メモリ部２において、メモリ位置指定部４によっ

て指定されたアドレスのデータを使用して、鍵K_nを生成する。例えは、映像データにおける４つのアドレスＡ１～Ａ４を指定し、これらのアドレスＡ１～Ａ４のデータを繋ぎ合わせた鍵K_nを生成する。ここで生成された鍵K_nには、次の部分コンテンツC_{n+1}から鍵K_{n+1}を生成するための、映像表示メモリ部２におけるアドレスを指定する情報が含まれており、この鍵K_nは、メモリ位置指定部４に供給される。また、この鍵K_nは、図示しない送信部から、図１Ａに示す認証管理サーバ装置２２へ送られ、上述した如く、次の部分コンテンツC_{n+1}の要求R_nとして使用されるとともに、クライアント端末１０ａを認証する認証鍵としても利用される。

メモリ位置指定部４は、鍵K_nから、次の鍵K_{n+1}を生成するためのアドレスを取得する。次の部分コンテンツC_{n+1}が、映像表示メモリ部２に書き込まれると、メモリ位置指定部４は、鍵K_nから取得したアドレスにより、映像表示メモリ部２のアドレスを指定することができる。これにより、次鍵生成部３ａでは、鍵K_{n+1}を生成することができる。

部分コンテンツC_nは、映像データの場合は、複数フレーム分のデータである。次鍵生成部３ａは、全てのフレームにおいて鍵を生成してもよいが、コンテンツ配信サーバ装置２１ａからリアルタイムにコンテンツが送信される場合、１フレームずつ鍵K_nを生成し、これを認証として認証管理サーバ装置２２に送信し、次のフレームデータを要求することは現実的ではないため、例えば、複数フレームからなるコンテンツC_nに含まれる、例えば最初のフレームから鍵を生成する。以下、鍵を生成するフレームをキーフレームという。メモリ位置指定部４は、キーフレームにおけるアドレスを指定するが、キーフレームを部分コンテンツC_nに含まれる最初のフレームとせず、鍵K_nが、キーフレームのアドレスを指定するための情報とともに、何番目のフレームをキーフレームとするかの情報を含むものとしてもよい。こうして全フレームからではなく、所定時間単位で送られてくる部分コンテンツ内の映像フレームのうち、１フレーム又は主要フレームにおける指定アドレスのデータを鍵生成に利用することができる。

ここで、本実施の形態においては、部分コンテンツC_nは、ＶＲＡＭである映像表示メモリ部２に書き込まれ映像が表示されなければ、次鍵K_nを生成することが

できず、次の部分コンテンツC_{n+1}を得ることができないようなデータとする。このようにＶＲＡＭに展開しなければ鍵K_nを生成することができないようなデータとしては、例えば、展開時にデータを補間するようなもの等がある。また、例えば、メモリ位置指定部４により指定されたアドレス位置のデータを計算により求めて鍵K_nを得ることが可能である場合であっても、そのように計算により鍵K_nを得るには処理に時間がかかり、クライアント端末１０ａの処理負担が大きく、リアルタイムに部分コンテンツC_nを再生することができなくなってしまう。したがって、映像表示メモリ分２に展開されたデータを使用して鍵K_nを得るものとする。

また、部分コンテンツC_nが音声データである場合、例えは、部分コンテンツ内の時間を指定し、その時間におけるデータから鍵を生成すればよい。

本実施の形態においては、クライアント端末１０ａは、分割されて送られてくる部分コンテンツC_nから鍵K_nを生成し、これを次の部分コンテンツC_{n+1}の要求R_nに使用するとともに、クライアント端末１０ａの認証として使用する。これにより、クライアント端末１０ａでは、コンテンツC_nを視聴（再生）しないと、認証となる鍵を生成することができないため、コンテンツの途中に挿入されているＣＭ等の一部のコンテンツを視聴せずに飛ばして視聴することを防止することができる。

また、この第１の実施の形態におけるコンテンツの暗号化は任意であり、暗号化を施しても施さなくてもよく、暗号化した場合に使用する復号鍵としては、上述の認証鍵の一部又は全部を用いてもよく、又は復号鍵を別途用意してもよい。

次に、本発明の第２の実施の形態について説明する。上述の第１の実施の形態においては、部分コンテンツを表示しなければ、クライアント端末を認証するための鍵が生成できず、次のコンテンツが送信されないようなシステムであったのに対し、本第２の実施の形態では、サーバ装置は、暗号化されたコンテンツを送信するものとし、１つの部分コンテンツを復号しなければ、次の部分コンテンツを復号するための暗号鍵を取得できず、次のコンテンツが復号できないようなしくみを提供するものである。なお、以下の実施の形態において、図１及び図２に示す第１の実施の形態と同一の構成要素には同一の符号を付してその詳細な説明

は省略する。

図３は、本第２の実施の形態におけるデータ管理システムを模式的に示すブロック図である。図３に示すように、本データ管理システム２００におけるサーバ装置２０ｂは、図１に示す認証管理サーバ装置２２の代わりに暗号化されたコンテンツの鍵管理を行う鍵管理サーバ装置２３を備える。クライアント端末１０ｂは、データ視聴管理部１１ｂを有する。

本実施の形態におけるコンテンツ配信サーバ装置２１ｂがクライアント端末１０ｂに送信する部分コンテンツC_nは、暗号化されたものである。クライアント端末１０ｂは、データ視聴管理部１１ｂにより、コンテンツ配信サーバ装置２１ｂから送信される部分コンテンツC_nを順次復号して表示する。

本システム２００においては、クライアント端末１０ｂは、サーバ装置２０の鍵管理サーバ装置２２に対し、コンテンツ視聴許可の要求R_0をし、この要求R_0がサーバ装置２０にて承諾されると、鍵管理サーバ装置２２から、クライアント端末１０ｂに初期鍵K_0が通知される。この初期鍵K_0は、コンテンツ配信サーバ装置２１ｂから送信されてくる最初のコンテンツC_1を復号するための復号鍵である。ここで、初期鍵K_0は、クライアント端末１０ｂだけに固有の鍵として、予めクライアント端末１０ｂが所有していてもよい。要求R_0としては、クライアント端末１０ｂを識別可能な認証番号等を合わせて送信する。その後、コンテンツ配信サーバ装置２１ｂからは、コンテンツC_nが順次送信される。

クライアント端末１０ｂは、最初のコンテンツC_1を初期鍵K_0により復号する。そして、クライアント端末１０ｂは、コンテンツC_1を復号すると同時に、後述する方法により次の部分コンテンツC_2を復号するために必要な暗号鍵K_1を生成する。

コンテンツ配信サーバ装置２１ｂは、部分コンテンツC_nを順次配信する。本実施の形態においては、部分コンテンツC_nは、暗号化されており、初期鍵を持たないクライアント端末では復号できないため、部分コンテンツ毎に認証する必要がない。

次に、上述の暗号鍵の生成について説明する。図４は、クライアント端末１０ｂのデータ視聴管理部１１ｂを示すブロック図である。データ視聴管理部１１ｂ

は、コンテンツ配信サーバ装置２１ｂから送信される暗号化された映像データからなる部分コンテンツC_nを受信する受信部（図示せず）と、この受信部から部分コンテンツC_nが供給され、これを復号する復号部１と、復号された映像データを記憶する映像表示メモリ部２と、映像表示メモリ部２に書き込まれた映像データに基づき暗号鍵K_nを生成する次鍵生成部３ｂと、暗号鍵K_nを生成するために、映像表示メモリ部２のデータのアドレスを指定するメモリ位置指定部４とを備える。

復号部１には、暗号鍵生成部３ｂにより生成された暗号鍵K_{n-1}が供給され、復号部１は、この暗号鍵K_{n-1}を復号鍵として使用し、コンテンツ配信サーバ装置２１ｂから送られる暗号化された映像データであるコンテンツC_nを復号し、復号済み映像データD_nを映像表示メモリ部２に送る。

次鍵生成部３ｂは、映像表示メモリ部２において、メモリ位置指定部４によって指定されたアドレスの映像データを使用して、暗号鍵K_nを生成する。この暗号鍵K_nには、次の部分コンテンツC_{n+1}から暗号鍵K_{n+1}を生成するための、映像表示メモリ部２におけるアドレスを指定する情報が含まれており、この暗号鍵K_nは、メモリ位置指定部４に供給される。また、本実施の形態においては、暗号鍵K_nを、次の部分コンテンツC_{n+1}のデータを復号する復号鍵として使用するため、暗号鍵K_nは復号部１へ供給される。

復号部１には、次の部分コンテンツC_{n+1}が供給され、暗号鍵K_nを復号鍵として、次の部分コンテンツC_{n+1}を復号し、この復号した映像データD_{n+1}が、映像表示メモリ部２に書き込まれると、メモリ位置指定部４は、暗号鍵K_nから取得したアドレスにより、映像表示メモリ部２のアドレスを指定する。これにより、次鍵生成部３ｂでは、暗号鍵K_{n+1}を生成することができる。

本実施の形態においては、暗号化された部分コンテンツC_nを表示して、復号しなければ、次の部分コンテンツC_{n+1}が復号できないため、最初に認証され、初期鍵を受け取ったクライアント端末のみが、部分コンテンツを最後まで復号することができ、途中の部分コンテンツを取得しても、復号することができないため、コンテンツ提供者側の著作権が保護される。また、第１の実施の形態と同様に、コンテンツは一旦表示しなければ、次のコンテンツを復号する復号鍵を生成でき

ないため、視聴者が部分的にコンテンツを飛ばして視聴することを防止する。

次に、本発明の第３の実施の形態について説明する。本実施の形態は、第１の実施の形態と第２の実施の形態を組み合わせたものであって、サーバ装置は、暗号化された部分コンテンツを順次配信するものとし、クライアント端末は、部分コンテンツから生成した鍵を認証として使用するとともに、復号鍵としても使用するものである。

図５は、本第３の実施の形態におけるデータ管理システムを模式的に示すブロック図である。図５に示すように、本データ管理システム３００におけるサーバ装置２０ｃは、図１に示す認証管理サーバ装置２２の代わりに暗号化されたコンテンツの鍵管理を行うとともに、クライアント端末の認証を行う鍵管理サーバ装置２４を備える。クライアント端末１０ｃは、データ視聴管理部１１ｃを有する。

コンテンツ配信サーバ装置２１ｃは、図１Ｂに示すように、暗号化した１つの映像を示す映像データであるコンテンツＣを、所定時間単位毎（所定ブロック毎）に分割した部分コンテンツC_n（C_1～C_n）を順次クライアント端末１０ｃに送信する。クライアント端末１０ｃは、データ視聴管理部１１ｃにより、コンテンツ配信サーバ装置２１ｃから送信される部分コンテンツC_nを順次復号して表示する。

図６は、本実施の形態におけるデータ管理システムにおけるデータの流れを示す図である。先ず、クライアント端末１０ｃは、サーバ装置２０ｃの鍵管理サーバ装置２２に対し、コンテンツ視聴許可の要求R_0をし、この要求R_0がサーバ装置２０ｃにて承諾されると、鍵管理サーバ装置２４から、クライアント端末１０ｃに初期鍵K_0が通知され、コンテンツ配信サーバ装置２１ｃからは、最初のコンテンツC_1が送信される。

クライアント端末１０ｃは、最初のコンテンツC_1を初期鍵K_0により復号する。そして、クライアント端末１０ｃは、コンテンツC_1を復号すると同時に、第２の実施の形態と同様の方法により次の部分コンテンツC_2を復号するために必要な暗号鍵K_1を生成する。次に、クライアント端末１０ｃは、サーバ装置２０ｃに対して、次コンテンツC_2の要求R_1を行うとともに、この暗号鍵K_1の一部又は全部を端末１０ｃの認証として鍵管理サーバ装置２４に送信する。本実施の形態におい

ては、暗号鍵K_1をクライアント端末１０ｃの認証とするとともに、コンテンツC_2の要求R_1とするものとする。この暗号鍵K_1は、初期鍵K_0を持たないクライアント端末では生成不可能なため、クライアント端末１０ｃの認証として使用することができる。

鍵管理サーバ装置２４は、追加データである次コンテンツC_2の要求R_1があると、クライアント端末１０ｃから送信された暗号鍵K_1を確認し、確認すると、コンテンツ配信サーバ装置２１ｃに次コンテンツC_2をクライアント端末１０ｃに送信するよう指示する。コンテンツ配信サーバ装置２１ｃは、この指示に従い次コンテンツC_2をクライアント端末１０ｃに送信する。クライアント端末１０ｃでは、最初のコンテンツC_1から得た暗号鍵K_1を、次コンテンツC_2を復号する復号鍵として使用して復号し、同時に暗号鍵K_2を生成する。この暗号鍵K_2は、コンテンツC_2の次のコンテンツC_3の要求R_2に使用されるとともに、コンテンツC_3の復号に使用される。このように、クライアント端末１０ｃは、分割されて送られてくる部分コンテンツC_nを順次復号して出力するとともに、暗号鍵K_nを生成し、これを使用して次の部分コンテンツC_{n+1}の要求R_nに使用するとともに、次の部分コンテンツC_{n+1}の復号鍵として使用する。そして、サーバ装置２０ｃは、部分コンテンツC_nをクライアント端末１０ｃからの要求に従い順次送信する。

次に、上述の暗号鍵の生成について説明する。図７は、クライアント端末１０ｃのデータ視聴管理部１１ｃを示すブロック図である。本実施の形態のデータ視聴管理部１１ｃは、次鍵生成部３ｃにより生成された暗号鍵K_nが、図示しない送信部から、図５に示す鍵管理サーバ装置２４へ送られる点が図４に示すデータ視聴管理部１１ｂと異なる。その他の点は、第２の実施の形態におけるデータ視聴管理部１１ｂと同様の構成である。

以下、本実施の形態のデータ管理システムの動作について説明する。図８Ａ及び図８Ｂは、データ管理システム全体の動作を示す図であって、夫々サーバ装置側の動作、及び端末側の動作を示すフローチャートである。先ず、上述した如く、図８Ａに示すクライアント端末１０ｃは鍵管理サーバ装置２４に対して、先ず、コンテンツ視聴要求R_0を出し、初期鍵K_0を取得し、これにより、クライアント端末１０ｃは、順次コンテンツC_nを要求するとともに暗号鍵K_nを生成する。そ

して、クライアント端末１０ｃによって、コンテンツ配信サーバ装置２１ｃには、コンテンツC_nの配信要求が出され、これに従ってコンテンツ配信サーバ装置２１ｃはコンテンツC_nをクライアント端末１０ｃに順次配信する。

即ち、図８Ａに示すように、コンテンツ配信サーバ装置２１ｃは、暗号化された映像データである部分コンテンツC_nをクライアント端末１０ｃに配信し（ステップＳ１）、部分コンテンツC_nを送信し終わった後は、クライアント端末１０ｃから次コンテンツ要求R_nを受信するまで待機する。実際は、連続した視聴が可能となるよう、次コンテンツ要求R_nは、前の部分コンテンツC_nの送信が終了する前に受信される（ステップＳ２）。

本実施の形態においては、上述したように、現在の部分コンテンツC_nを復号して得られた暗号鍵K_nを、次の部分コンテンツC_{n+1}の要求R_nとするとともに、認証鍵としても使用する。したがって、鍵管理サーバ装置２４は、クライアント端末から送られた次コンテンツ要求である暗号鍵K_n（認証鍵）が、正しい認証鍵であるか否かを判定し（ステップＳ３）、正しくなければこの時点でコンテンツの配信を停止するようコンテンツ配信サーバ装置２１ｃに指示する。一方、認証鍵が正しいと認証されれば、ステップＳ１に戻り、コンテンツ配信サーバ装置２１ｃは、次のコンテンツC_{n+1}を送付する。

また、クライアント端末１０ｃは、図８Ｂに示すように、暗号化された映像データであるコンテンツC_nを受信し（ステップＳ１１）、最初のコンテンツC_1のときは、図７に示す復号部１にて、鍵管理サーバ装置２４から送信されている初期鍵K_0により復号し、映像表示メモリ部２に書き込み、映像を表示する。最初以外の部分コンテンツC_nの場合は、鍵生成部３ｃにより生成された暗号鍵K_{n-1}を使用して、コンテンツC_nを復号し、これを映像表示メモリ部２に書き込み、映像を表示する（ステップＳ１２）。

映像表示メモリ部２に、復号された映像が書き込まれると、暗号鍵生成部３ｃにて、次データを取得するための次コンテンツC_{n+1}の暗号鍵K_nが生成される（ステップＳ１３）。そして、この暗号鍵K_nを鍵管理サーバ装置２４に送付すると、鍵管理サーバ装置２４がクライアント端末１０ｃを認証して、コンテンツ配信サーバ装置２１ｃから次コンテンツC_{n+1}が送信される。

次に、暗号鍵生成方法について更に詳細に説明する。図９は、クライアント端末１０ｃの暗号鍵生成方法を示すフローチャートである。図９に示すように、図７に示す復号部１は、暗号化されたデータを受信する（ステップＳ２１）と、その前の部分コンテンツC_{n-1}から取得した暗号鍵K_{n-1}を復号鍵として復号し、その復号済み映像データD_nを映像表示メモリ部２に送る（ステップＳ２２）。

メモリ位置指定部４は、映像表示メモリ部２に送られた復号済み映像データのフレームがキーフレームであるか否を判断し（ステップＳ２３）、キーフレームであった場合は、映像表示メモリ部２に書き込まれた映像データのうち、メモリ位置指定部４によって指定されたアドレス（番地）のデータを次鍵生成部３ｃに送る（ステップＳ２４）。

次鍵生成部３ｃでは、この値を利用して、次の暗号鍵K_nを生成する（ステップＳ２５）。この暗号鍵K_nは、次のコンテンツC_{n+1}の復号鍵として使用するため、復号部１に送られるとともに、暗号鍵K_nから、次の暗号鍵K_{n+1}を生成するために必要なアドレスを指定するアドレス値を取得し、メモリ位置指定部４へ供給する（ステップＳ２６）。また、暗号鍵K_nは鍵管理サーバ装置２４に送られ、次の部分コンテンツC_{n+1}の要求R_nとして使用されるとともに、クライアント端末１０ｃの認証として使用される（ステップＳ２７）。以降、最後のコンテンツが復号されるまで、ステップＳ２１～ステップＳ２７の処理を繰り返す。

ここで、暗号鍵K_nを生成するためのアドレスは、最も単純な場合は、常に同じアドレスを指定することも可能であるし、キーフレームの位置毎に異なるアドレスを指定することも可能である。

また、生成された暗号鍵K_nを、鍵管理サーバ装置２４へ通知することによって、次の映像データブロックである部分コンテンツC_{n+1}の要求をし、鍵管理サーバ装置２４側ではその受信した暗号鍵K_nが正しいことを確認することによって、次の映像データブロックである部分コンテンツC_{n+1}を送信することにより、クライアント端末１０ｃにて、部分コンテンツC_nが実際に表示された場合にのみ、次のコンテンツC_{n+1}を取得できるようにすることができる。この認証は、暗号鍵K_nとしてもよいが、暗号鍵K_nの一部分又は暗号鍵K_nから生成されたデータを認証として送ってもよい。例えば、クライアント端末１０ｃに固有の固有鍵を用意し、

生成される暗号鍵K_nを暗号化されたものとし、この固有鍵で暗号鍵K_nを復号したものを認証として使用してもよい。同様に、暗号鍵K_nを復号鍵として使用しているが、暗号鍵K_nの一部又は暗号鍵K_nから所定の方法で生成したデータを復号鍵としてもよい。

更に、映像表示機としてのクライアント端末１０ｃのハードウェアを識別するＩＤを付与することにより、クライアント端末１０ｃに対応した固有の鍵を持つ映像データのみ表示できるように制御することができる。

こうして、映像の一部分を示す部分映像を実際に表示しなければ、次のコンテンツが取得できないようなしくみをつくることにより、配信事業者が望むような、視聴者が視聴したことを保証しつつ映像を配信するようなサービスを提供することができる。

なお、本発明は上述した実施の形態のみに限定されるものではなく、本発明の要旨を逸脱しない範囲において種々の変更が可能であることは勿論である。例えば、コンテンツは、サーバ装置からネットワークを介してクライアント端末に送信するものとしたが、暗号化データを復号する復号鍵が当該暗号化データの時間的に前の暗号化データが復号された復号データに含まれるものであって、その復号鍵が上記前の暗号化データを復号して再生すると得られるような暗号化データを記録媒体等に記憶したものを事業者がクライアントに提供し、クライアントが図７に示すような端末を復号装置として使用し、暗号化データを復号するようにすることもできる。このような暗号化データは、実際に表示しなければ復号できないため、暗号データを提供する側である事業者の利益を保護することができる。なお、この場合は、図７で説明した受信手段は不要である。

また、上述の実施の形態では、ハードウェアの構成として説明したが、これに限定されるものではなく、任意の処理を、ＣＰＵ（Central Processing Unit）にコンピュータプログラムを実行させることにより実現することも可能である。この場合、コンピュータプログラムは、記録媒体に記録して提供することも可能であり、また、インターネットその他の伝送媒体を介して伝送することにより提供することも可能である。

また、上述した如く、音声データも同様の方法で管理することができる。即ち、

例えば、サーバ装置からは暗号化した音声データを所定時間単位毎（ブロック毎）に送信し、暗号鍵によって復号化した後、音声再生用メモリ領域に音声データを書き込むことによって音声再生を行う。そして、音声用メモリ領域の指定のアドレスにあるデータを次鍵生成のために利用し、生成された鍵をサーバ装置へ通知することによって次の音声データブロックを要求し、サーバ装置側ではその受信した暗号鍵が正しいことを確認することによって次の音声データブロックを送信するようにすることで、音声データを映像データと同様に取り扱うことができる。

なお、本発明は、図面を参照して説明した上述の実施例に限定されるものではなく、添付の請求の範囲及びその主旨を逸脱することなく、様々な変更、置換又はその同等のものを行うことができることは当業者にとって明らかである。

産業上の利用可能性

本発明は、配信事業者から配信されるコマーシャルなどのデータの視聴者による視聴を保証しつつ、映像や音楽を配信するようなサービスを提供することができるとともに、実際にコマーシャルを視聴しないと、次の映像及び音楽の配信を受けられないので、コピーのみを目的としたユーザを排除し、映像及び音楽の著作権の保護を達成するたことができる。

請求の範囲

1．ネットワークに接続され、ブロック化されたブロックデータを順次送信するサーバ装置と、上記ネットワークに接続され上記サーバ装置からのブロックデータを受信して再生するクライアント端末とを有するデータ管理システムであって、

上記クライアント端末は、上記ブロックデータを記憶するデータ記憶手段と、上記データ記憶手段に記憶されたデータに基づき認証鍵を生成する鍵生成手段と、上記鍵生成手段により生成された認証鍵を上記サーバ装置に送信する送信手段とを備え、

上記サーバ装置は、上記クライアント端末から送信された上記認証鍵を認証する認証手段と、該認証手段により該認証鍵を認証したときのみ次のブロックデータを送信する送信手段とを備えることを特徴とするデータ管理システム。

2．上記ブロックデータは、所定の時間単位に分割され、暗号化された暗号化データであって、

上記クライアント端末は、上記暗号化データを復号する復号手段を有することを特徴とする請求の範囲第1項記載のデータ管理システム。

3．上記データ記憶手段は、ＶＲＡＭ（ビデオメモリ）であることを特徴とする請求の範囲第1項記載のデータ管理システム。

4．上記クライアント端末は、上記データ記憶手段に書き込まれたデータを表示する表示装置であることを特徴とする請求の範囲第1項記載のデータ管理システム。

5．上記鍵生成手段は、上記データ記憶手段に記憶されたデータに基づき復号鍵を生成し、

上記復号手段は、上記復号鍵を使用して上記暗号化データを復号することを特徴とする請求の範囲第2項記載のデータ管理システム。

6．上記データ記憶手段は、ＶＲＡＭであり、

上記クライアント端末は、上記ＶＲＡＭに書き込まれたデータを表示する表示装置であり、

上記鍵生成手段は、上記ＶＲＡＭに上記データが書き込まれて上記表示装置に

表示されると上記復号鍵を生成することを特徴とする請求の範囲第５項記載のデータ管理システム。

７．上記鍵生成手段は、上記認証鍵に基づき復号鍵を生成し、

上記復号手段は、上記復号鍵を使用して上記暗号化データを復号することを特徴とする請求の範囲第２項記載のデータ管理システム。

８．上記クライアント端末の復号手段は、上記鍵生成手段により生成された認証鍵を復号鍵として使用して上記暗号化データを復号することを特徴とする請求の範囲第２項記載のデータ管理システム。

９．上記クライアント端末の上記鍵生成手段は、上記データ記憶手段に記憶されたデータのアドレスを指定する位置指定手段を有し、該位置指定手段により指定されたアドレスのデータを使用して認証鍵を生成することを特徴とする請求の範囲第１項記載のデータ管理システム。

１０．ネットワークに接続され、ブロック化されたブロックデータを順次送信するサーバ装置と、上記ネットワークに接続され上記サーバ装置からのブロックデータを受信して再生するクライアント端末とを有するデータ管理システムのデータ管理方法であって、

上記サーバ装置が上記ブロックデータを上記クライアント端末に送信する送信工程と、

上記クライアント端末が上記サーバ装置から送信されたブロックデータを受信してデータ記憶手段に記憶するデータ記憶工程と、

上記データ記憶手段に記憶されたデータに基づき認証鍵を生成する鍵生成工程と、

上記鍵生成工程にて生成された認証鍵を上記サーバ装置に送信する送信工程と、

上記サーバ装置が上記クライアント端末から送信された上記認証鍵を認証する認証工程とを有し、

上記サーバ装置の上記ブロックデータを上記クライアント端末に送信する送信工程では、上記認証工程にて上記認証鍵を認証した場合のみ、次のブロックデータが送信されることを特徴とするデータ管理方法。

１１．上記ブロックデータは、所定の時間単位に分割され、暗号化された暗号化

データであって、

上記クライアント端末が上記サーバ装置から送信された上記暗号化データを復号する復号工程を有し、

上記データ記憶工程では、上記復号されたデータが記憶されることを特徴とする請求の範囲第１０項記載のデータ管理方法。

１２．ブロック化されたブロックデータを順次送信するサーバ装置にネットワークを介して接続され、該サーバ装置からのブロックデータを受信して再生するクライアント端末であって、

上記サーバ装置から送信される上記ブロックデータを受信する受信手段と、

上記ブロックデータを記憶するデータ記憶手段と、

上記データ記憶手段に記憶されたデータに基づき認証鍵を生成する鍵生成手段と、

上記鍵生成手段により生成された認証鍵を上記サーバ装置に送信する送信手段とを備え、

上記受信手段は、上記サーバ装置が上記送信手段により送信された上記認証鍵を認証したときのみ、次のブロックデータを受信することを特徴とするクライアント端末。

１３．上記ブロックデータは、所定の時間単位に分割され、暗号化された暗号化データであって、

上記暗号化データを復号する復号手段を有することを特徴とする請求の範囲第１２項記載のクライアント端末。

１４．ブロック化されたブロックデータを、ネットワークを介してクライアント端末に順次送信するサーバ装置であって、

上記ブロックデータを送信する送信手段と、

上記クライアント端末が上記ブロックデータに基づき生成した認証鍵を受信する受信手段と

上記受信手段により受信された上記認証鍵を認証する認証手段とを有し、

上記送信手段は、上記認証手段により上記認証鍵が認証されたときのみ、ブロックデータを送信することを特徴とするサーバ装置。

１５．上記ブロックデータは、所定の時間単位に分割され、暗号化された暗号化データであり、上記クライアント端末は表示装置であって、

上記暗号化データは、上記クライアント端末にて復号され表示されると生成可能な上記認証鍵を含むことを特徴とする請求の範囲第１４項記載のサーバ装置。

１６．ネットワークに接続され、暗号化された複数の暗号化データを送信するサーバ装置と、該ネットワークに接続され上記サーバ装置から送信される上記暗号化データを受信するクライアント端末とを有するデータ管理システムであって、

上記サーバ装置は、上記暗号化データを送信する送信手段を少なくとも備え、

上記クライアント端末は、上記暗号化データを復号する復号手段と、上記復号手段により復号された復号データを記憶するデータ記憶手段と、上記データ記憶手段に記憶された復号データに基づき暗号鍵を生成する暗号鍵生成手段とを備え、

上記クライアント端末の復号手段は、上記暗号鍵生成手段により、第１の暗号化データが復号された第１の復号データから生成された第１の暗号鍵が供給され、該第１の暗号鍵を使用して上記第１の暗号化データの次の第２の暗号化データを復号することを特徴とするデータ管理システム。

１７．上記クライアント端末の上記暗号鍵生成手段は、上記第１の復号データから得られた上記第１の暗号鍵とこの第１の暗号鍵を使用して上記第２の暗号化データが復号された第２の復号データとから、第２の暗号化データの次の第３の暗号化データを復号する第２の暗号鍵を生成することを特徴とする請求の範囲第１６項記載のデータ管理システム。

１８．上記クライアント端末の上記暗号鍵生成手段は、上記復号データのアドレスを指定する位置指定手段を有し、該位置指定手段により指定されたアドレスの復号データを使用して暗号鍵を生成することを特徴とする請求の範囲第１６項記載のデータ管理システム。

１９．上記データ記憶手段は、ＶＲＡＭであることを特徴とする請求の範囲第１６項記載のデータ管理システム。

２０．上記クライアント端末は、上記データ記憶手段に書き込まれたデータを表示する表示装置であることを特徴とする請求の範囲第１６項記載のデータ管理システム。

２１．上記データ記憶手段は、ＶＲＡＭであり、

上記クライアント端末は、上記ＶＲＡＭに書き込まれたデータを表示する表示装置であり、

上記暗号鍵生成手段は、上記ＶＲＡＭに上記第１の復号データが書き込まれて上記表示装置に表示されると上記第２の暗号化データを復号する上記第１の暗号鍵を生成することを特徴とする請求の範囲第１６項記載のデータ管理システム。

２２．上記暗号化データは、複数のフレームデータが暗号化されたものであり、

上記クライアント端末の上記位置指定手段は、複数のフレームデータのうち、予め決められた所定のフレームデータにおけるアドレスを指定することを特徴とする請求の範囲第１８項記載のデータ管理システム。

２３．上記暗号化データは、複数のフレームデータが暗号化されたものであり、

上記クライアント端末の上記位置指定手段は、複数フレームデータのいずれかであるキーフレームを指定するとともに該キーフレームにおけるアドレスを指定することを特徴とする請求の範囲第１８項記載のデータ管理システム。

２４．上記クライアント端末は、上記暗号鍵を上記サーバ装置に送信する送信手段を有し、

上記サーバ装置は、上記クライアント端末からの上記暗号鍵を受信する受信手段を有し、

上記サーバ装置の送信手段は、上記受信手段が上記第１の暗号化データに基づく第１の暗号鍵を受信すると、上記第２の暗号化データを送信することを特徴とする請求の範囲第１６項記載のデータ管理システム。

２５．上記クライアント端末は、上記暗号鍵に基づく認証データを送信する送信手段を有し、

上記サーバ装置は、該クライアント端末からの上記認証データを認証する認証手段を有し、該認証手段が上記第１の暗号鍵に基づく第１の認証データを認証すると、上記第２の暗号化データを送信することを特徴とする請求の範囲第１６項記載のデータ管理システム。

２６．ネットワークに接続され、複数の暗号化データを送信するサーバ装置と、該ネットワークに接続され上記サーバ装置から送信される上記暗号化データを受

信するクライアント端末とを有するデータ管理システムのデータ管理方法であって、

上記サーバ装置が上記クライアント端末に暗号化データを送信する送信工程と、

上記クライアント端末が上記サーバ装置から送信された暗号化データを受信して復号する復号工程と、

上記クライアント端末が上記復号工程にて復号された復号データをデータ記憶手段に記憶するデータ記憶工程と、

上記クライアント端末が上記データ記憶工程にて記憶された復号データに基づき暗号鍵を生成する暗号鍵生成工程とを有し、

上記復号工程では、第１の暗号化データが復号された第１の復号データから生成された第１の暗号鍵を使用して、上記第１の暗号化データの次に受信された第２の暗号化データが復号されることを特徴とするデータ管理方法。

２７．上記暗号鍵生成工程では、上記第１の復号データから得られた第１の暗号鍵とこの第１の暗号鍵を使用して上記第２の暗号化データが復号された第２の復号データとから、上記第２の暗号化データの次に受信された第３の暗号化データを復号する第２の暗号鍵が生成されることを特徴とする請求の範囲第２６項記載のデータ管理方法。

２８．上記クライアント端末が上記暗号鍵を上記サーバ装置に送信する送信工程と、

上記サーバ装置が上記暗号鍵を受信する受信工程とを有し

上記サーバ装置が上記クライアント端末に暗号化データを送信する送信工程では、上記受信工程にて上記クライアント端末からの上記第１の暗号化データに基づく第１の暗号鍵を受信すると、上記第２の暗号化データが送信されることを特徴とする請求項２６記載のデータ管理方法。

２９．上記クライアント端末が上記暗号鍵に基づく認証データを上記サーバ装置に送信する送信工程と、

上記サーバ装置が上記クライアント端末からの認証データを認証する認証工程とを有し、

上記サーバ装置が上記クライアント端末に暗号化データを送信する送信工程で

は、上記認証工程にて上記第１の暗号鍵に基づく第１の認証データが認証されると、上記第２の暗号化データが送信されることを特徴とする請求の範囲第２６項記載のデータ管理方法。

３０．複数の暗号化データを送信するサーバ装置にネットワークを介して接続され、該サーバ装置から送信される該暗号化データを受信するクライアント端末であって、

上記暗号化データを受信する受信手段と、

上記暗号化データを復号する復号手段と、

上記復号手段により復号された復号データを記憶するデータ記憶手段と、

上記データ記憶手段に記憶された復号データに基づき暗号鍵を生成する暗号鍵生成手段とを備え、

上記復号手段は、上記暗号鍵生成手段により、第１の暗号化データが復号された第１の復号データから生成された第１の暗号鍵が供給され、該第１の暗号鍵を使用して上記第１の暗号化データの次に受信された第２の暗号化データを復号することを特徴とするクライアント端末。

３１．上記暗号鍵生成手段は、上記第１の復号データから得られた第１の暗号鍵とこの第１の暗号鍵を使用して上記第２の暗号化データが復号された第２の復号データとから、上記第２の暗号化データの次に受信された第３の暗号化データを復号する第２の暗号鍵を生成することを特徴とする請求の範囲第３０項記載のクライアント端末。

３２．所定の時間単位に分割され、暗号化された複数の暗号化データを復号するデータ復号装置において、

上記暗号化データを復号する復号手段と、

上記復号手段により復号された復号データを記憶するデータ記憶手段と、

上記データ記憶手段に記憶された復号データに基づき暗号鍵を生成する暗号鍵生成手段とを備え、

上記復号手段は、上記暗号鍵生成手段により、第１の暗号化データが復号された第１の復号データから生成された第１の暗号鍵が供給され、該第１の暗号鍵を使用して上記第１の暗号化データの次の第２の暗号化データを復号することを特

徴とするデータ復号装置。

３３．所定の時間単位に分割され、暗号化された複数の暗号化データを復号するデータ復号方法において、

上記暗号化データを復号する復号工程と、

上記復号工程にて復号された復号データをデータ記憶手段に記憶する記憶工程と、

上記データ記憶手段に記憶された復号データに基づき暗号鍵を生成する暗号鍵生成工程と有し、

上記復号工程では、上記暗号鍵生成工程にて、第１の暗号化データが復号された第１の復号データから生成された第１の暗号鍵が供給され、該第１の暗号鍵を使用して上記第１の暗号化データの次の第２の暗号化データが復号されることを特徴とするデータ復号方法。

３４．所定の時間単位に分割され、暗号化された複数の暗号化データが記録された記録媒体であって、

第２の暗号化データを復号する第１の復号鍵が、該第２の暗号化データの時間的に前の第１の暗号化データが復号された復号データに含まれるものであって、該第１の復号鍵は、上記第１の暗号化データを復号して再生すると得られるものであることを特徴とする暗号化データが記録された記録媒体。

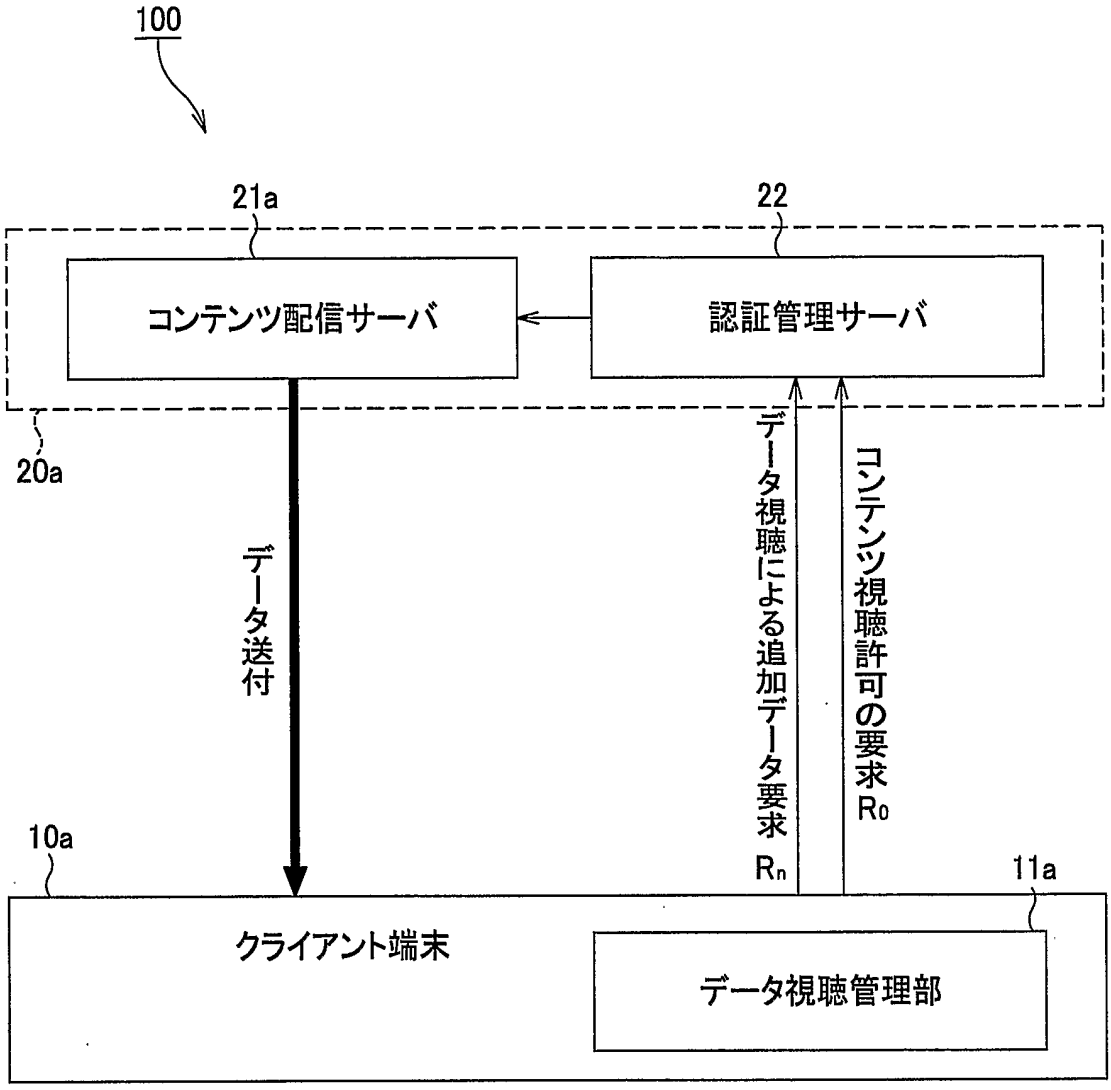

100
21a
22
コンテンツ配信サーバ
認証管理サーバ
20a
データ送付
データ視聴による追加データ要求 Rn
コンテンツ視聴許可の要求 R0
10a
11a
クライアント端末
データ視聴管理部

FIG.1A

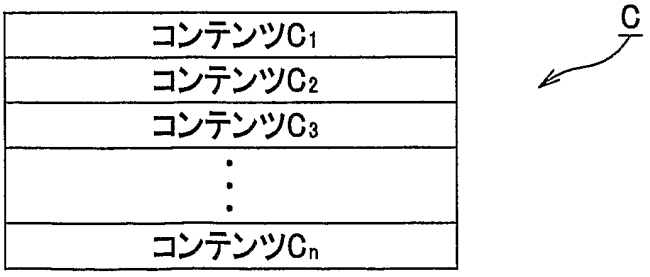

コンテンツC1
コンテンツC2
コンテンツC3
コンテンツCn
C

FIG.1B

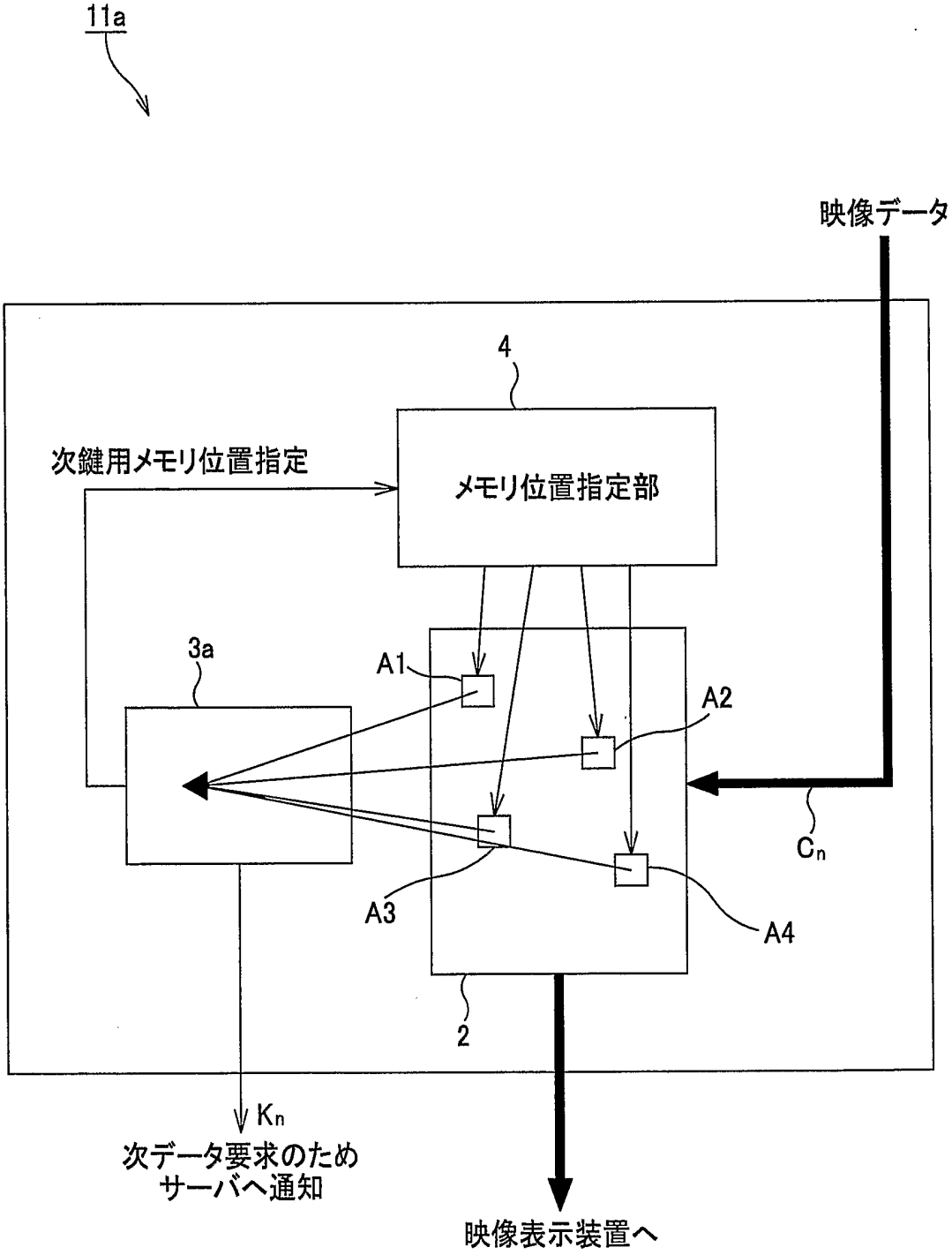

11a
映像データ
4
次鍵用メモリ位置指定
メモリ位置指定部
3a
A1
A2
A3
A4
Cn
2
Kn
次データ要求のため
サーバへ通知
映像表示装置へ

FIG.2

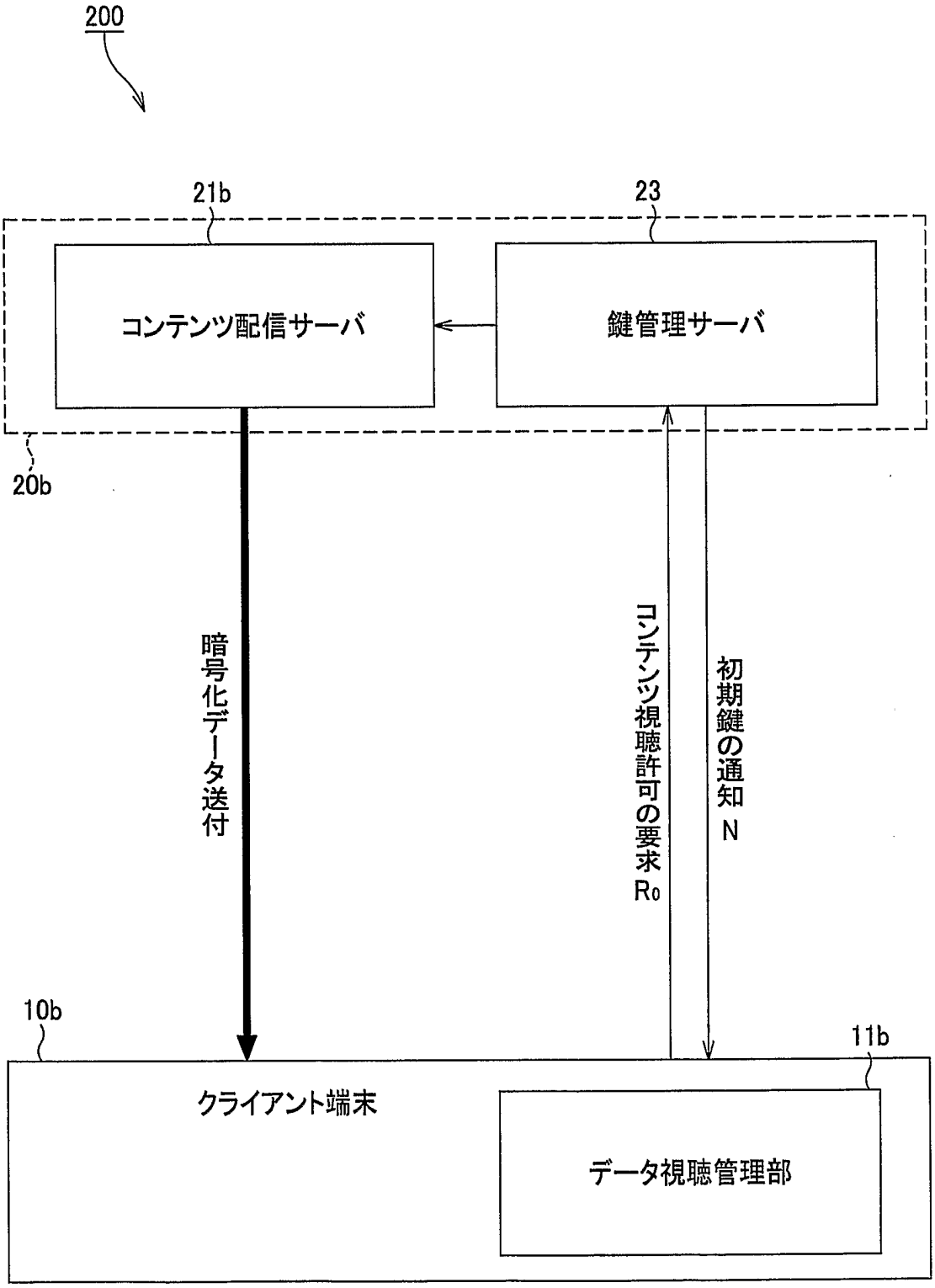

200
21b
23
コンテンツ配信サーバ
鍵管理サーバ
20b
暗号化データ送付
コンテンツ視聴許可の要求 R0
初期鍵の通知 N
10b
11b
クライアント端末
データ視聴管理部

FIG.3

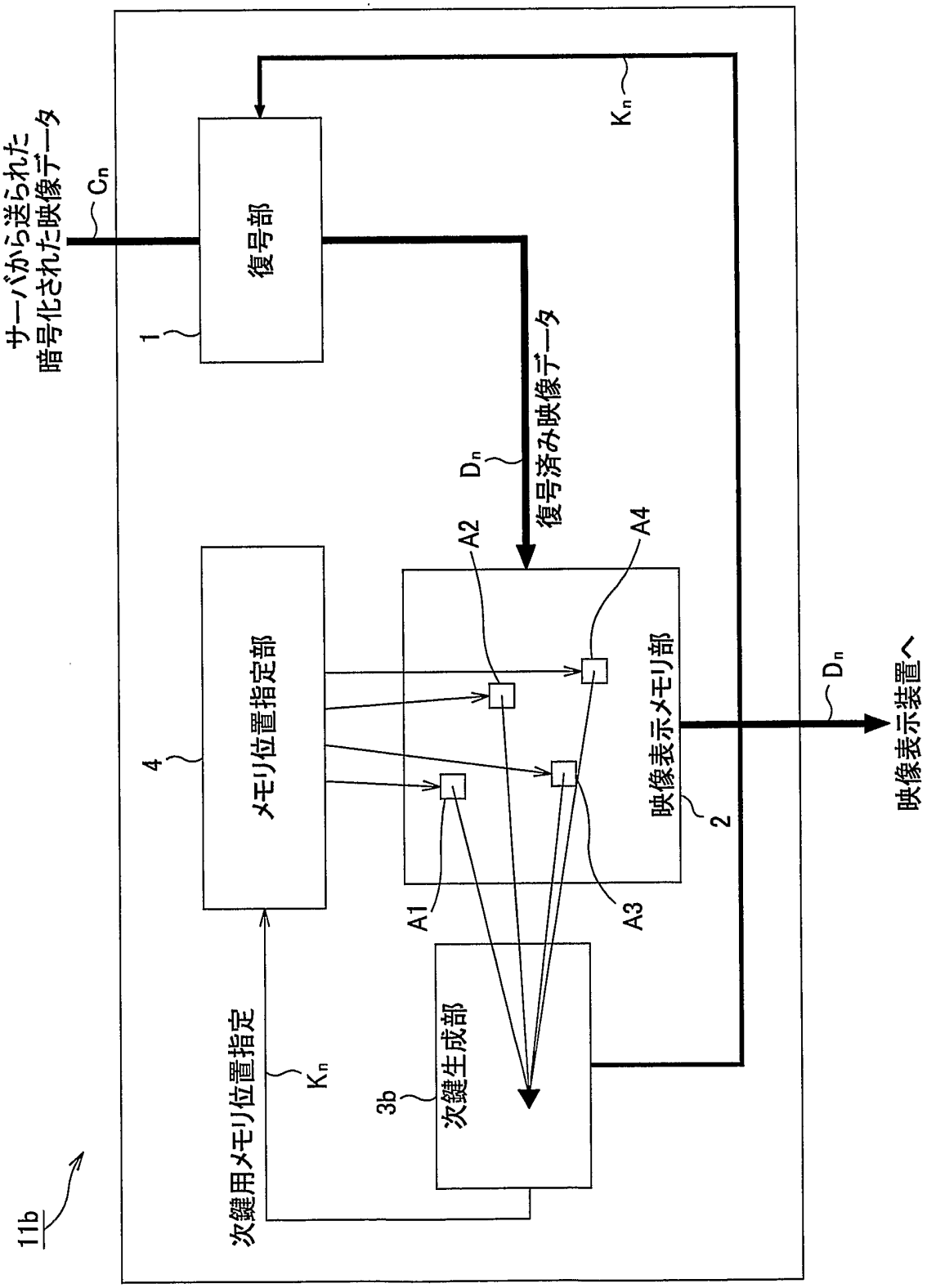

サーバから送られた
暗号化された映像データ
Cn
復号部
1
Kn
Dn
復号済み映像データ
A2
A4
メモリ位置指定部
4
映像表示メモリ部
2
Dn
映像表示装置へ
A1
A3
次鍵生成部
3b
次鍵用メモリ位置指定
Kn
11b

FIG.4

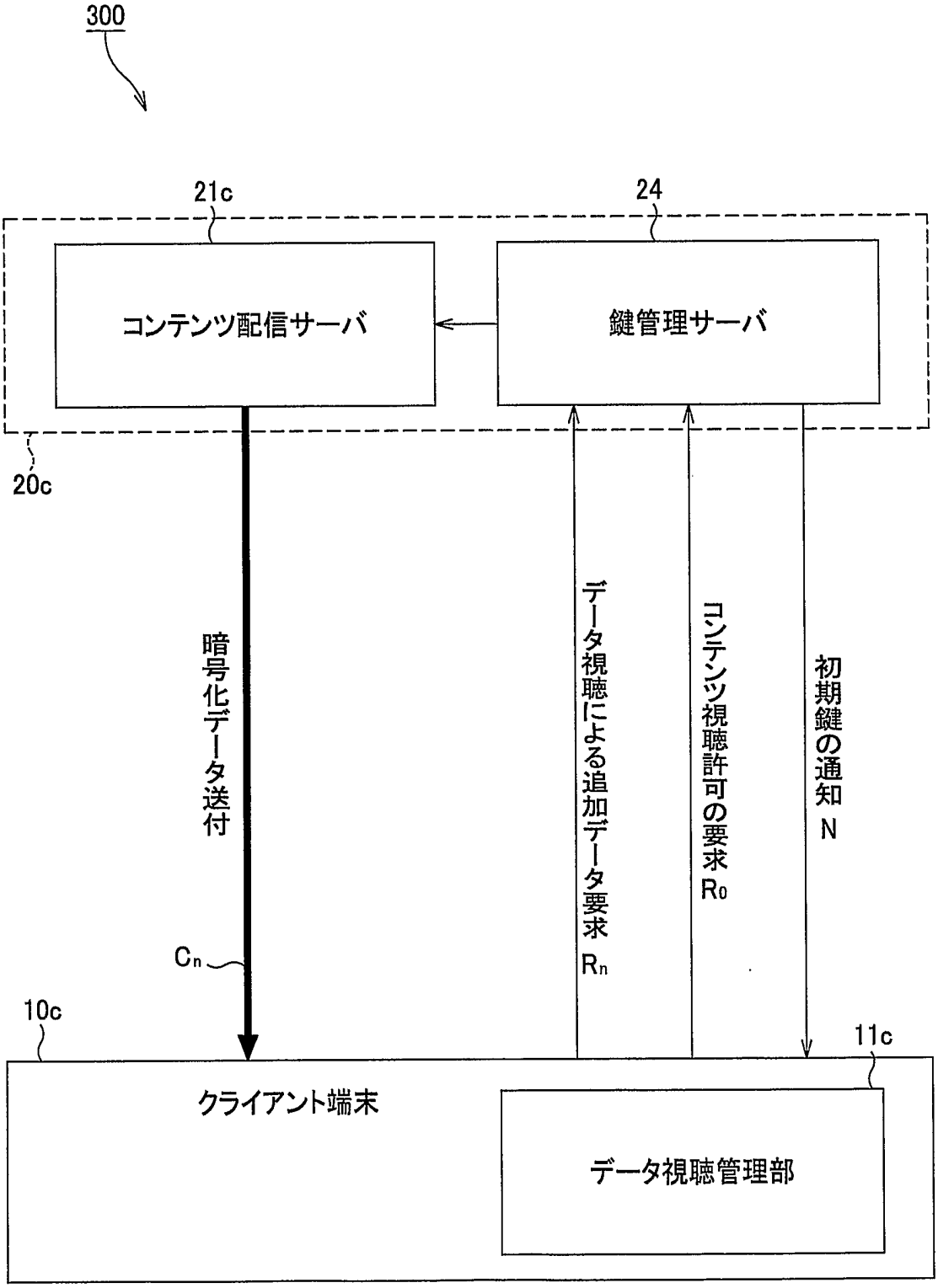

300
21c
24
コンテンツ配信サーバ
鍵管理サーバ
20c
暗号化データ送付
データ視聴による追加データ要求
Rn
コンテンツ視聴許可の要求
R0
初期鍵の通知
N
Cn
10c
11c
クライアント端末
データ視聴管理部

FIG.5

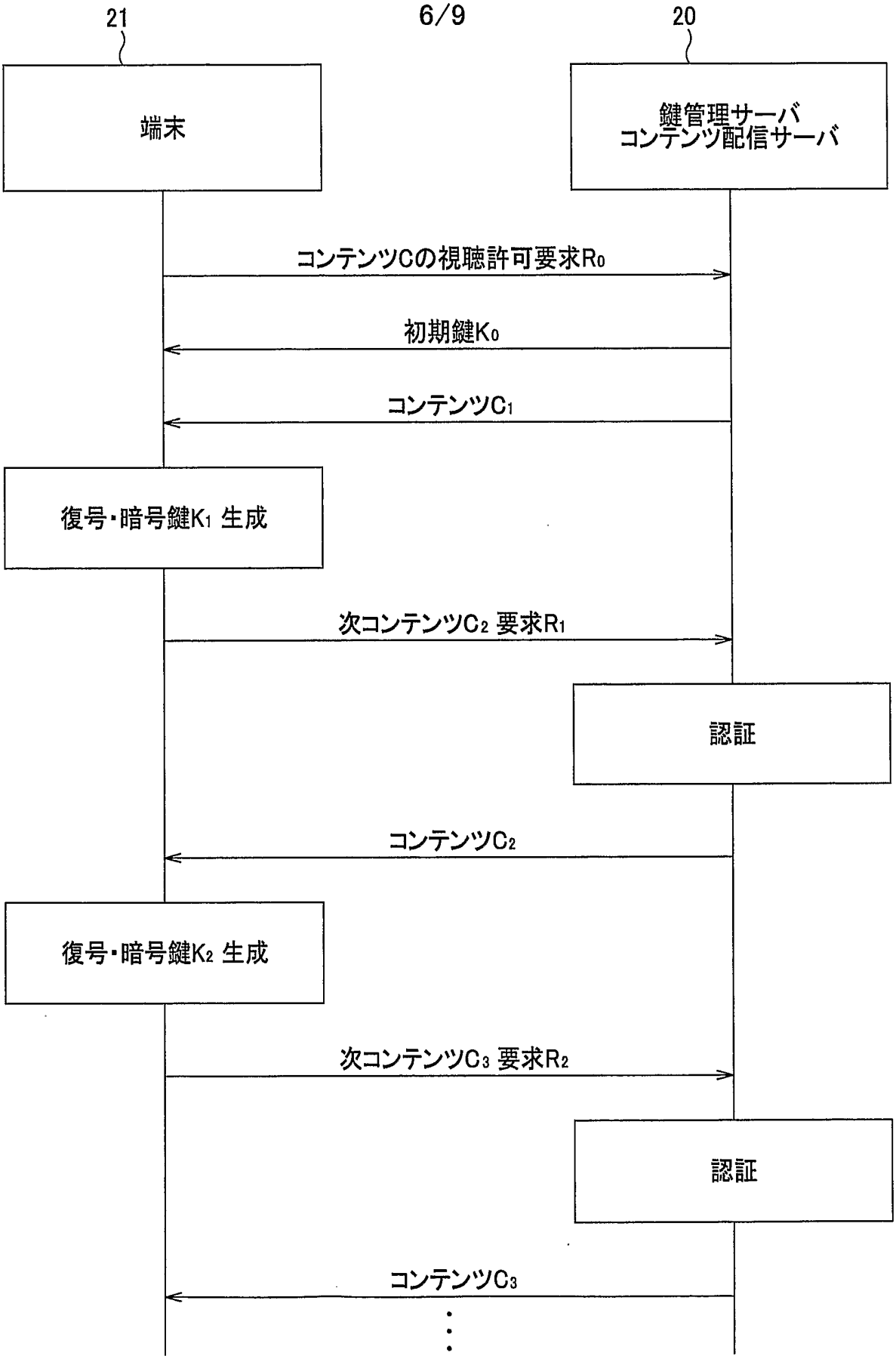

21
20
端末
鍵管理サーバ
コンテンツ配信サーバ
コンテンツCの視聴許可要求R0
初期鍵K0
コンテンツC1
復号・暗号鍵K1 生成
次コンテンツC2 要求R1
認証
コンテンツC2
復号・暗号鍵K2 生成
次コンテンツC3 要求R2
認証
コンテンツC3

FIG.6

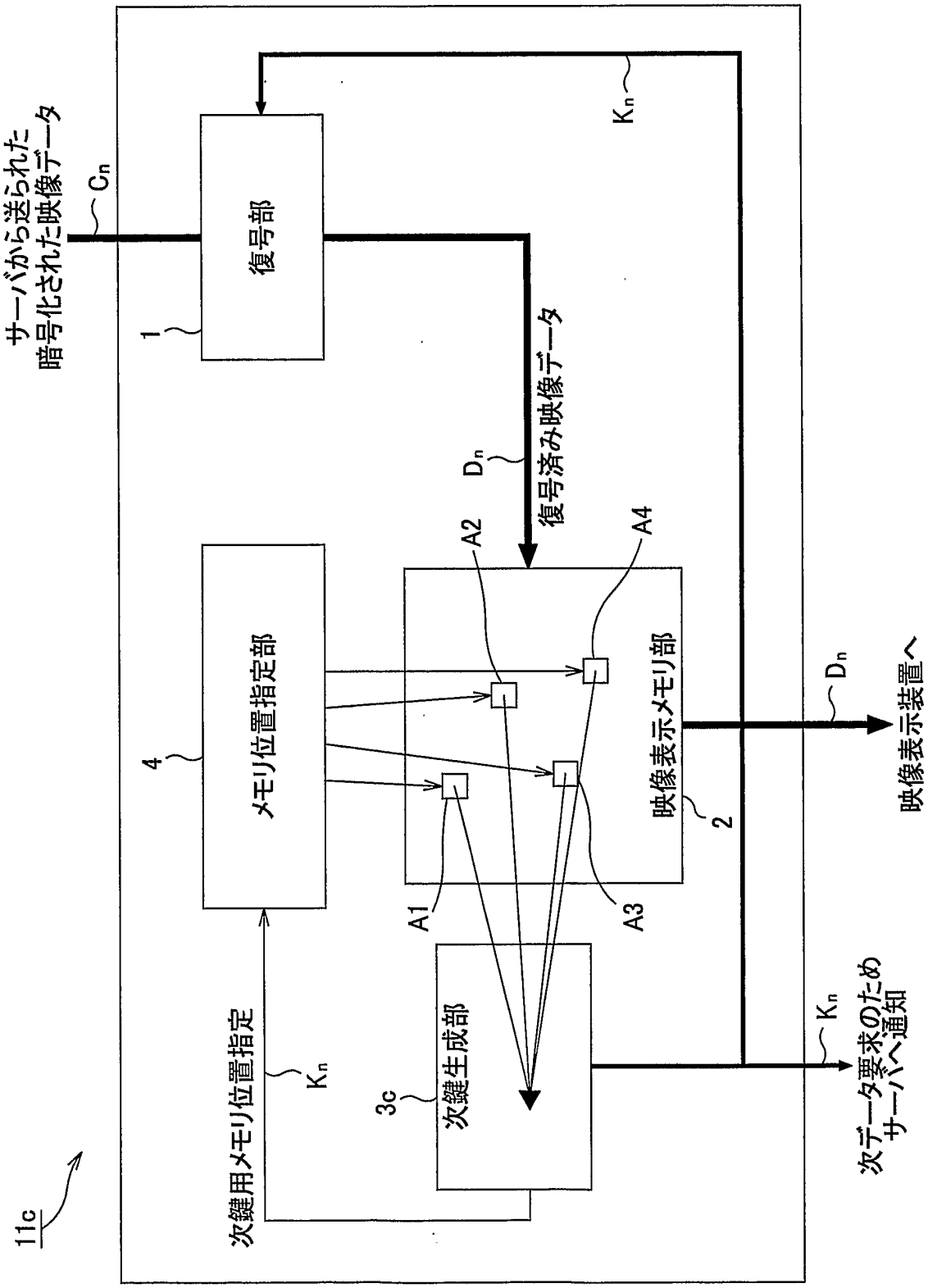

サーバから送られた
暗号化された映像データ
Cn
復号部
1
Kn
Dn
復号済み映像データ
A2
A4
メモリ位置指定部
4
映像表示メモリ部
2
Dn
映像表示装置へ
A1
A3
次鍵用メモリ位置指定
Kn
3c
次鍵生成部
Kn
次データ要求のため
サーバへ通知
11c

FIG.7

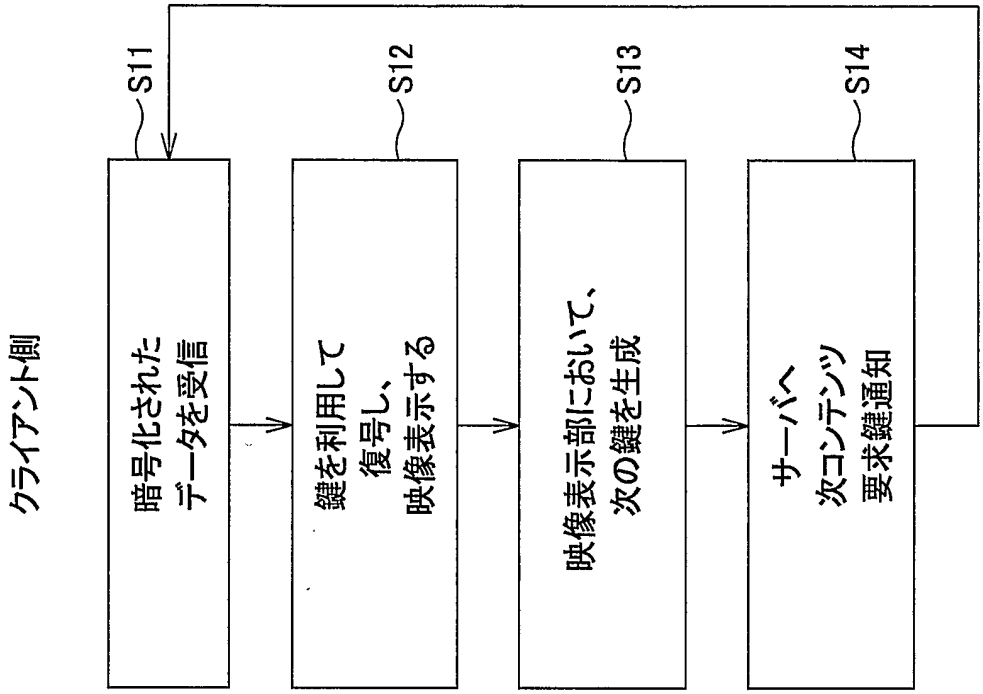

クライアント側
S11
暗号化された
データを受信
S12
鍵を利用して
復号し、
映像表示する
S13
映像表示部において、
次の鍵を生成
S14
サーバへ
次コンテンツ
要求鍵通知

FIG.8B

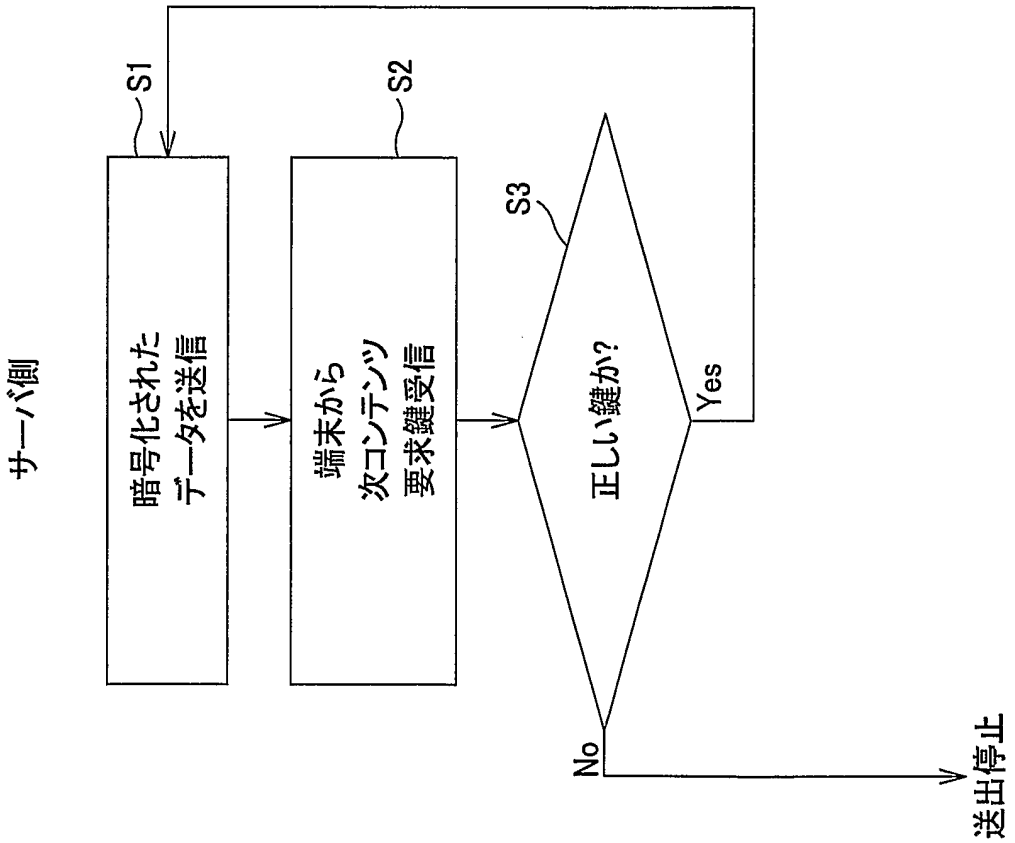

サーバ側
S1
暗号化された
データを送信
S2
端末から
次コンテンツ
要求鍵受信
S3
正しい鍵か?
Yes
No
送出停止

FIG.8A

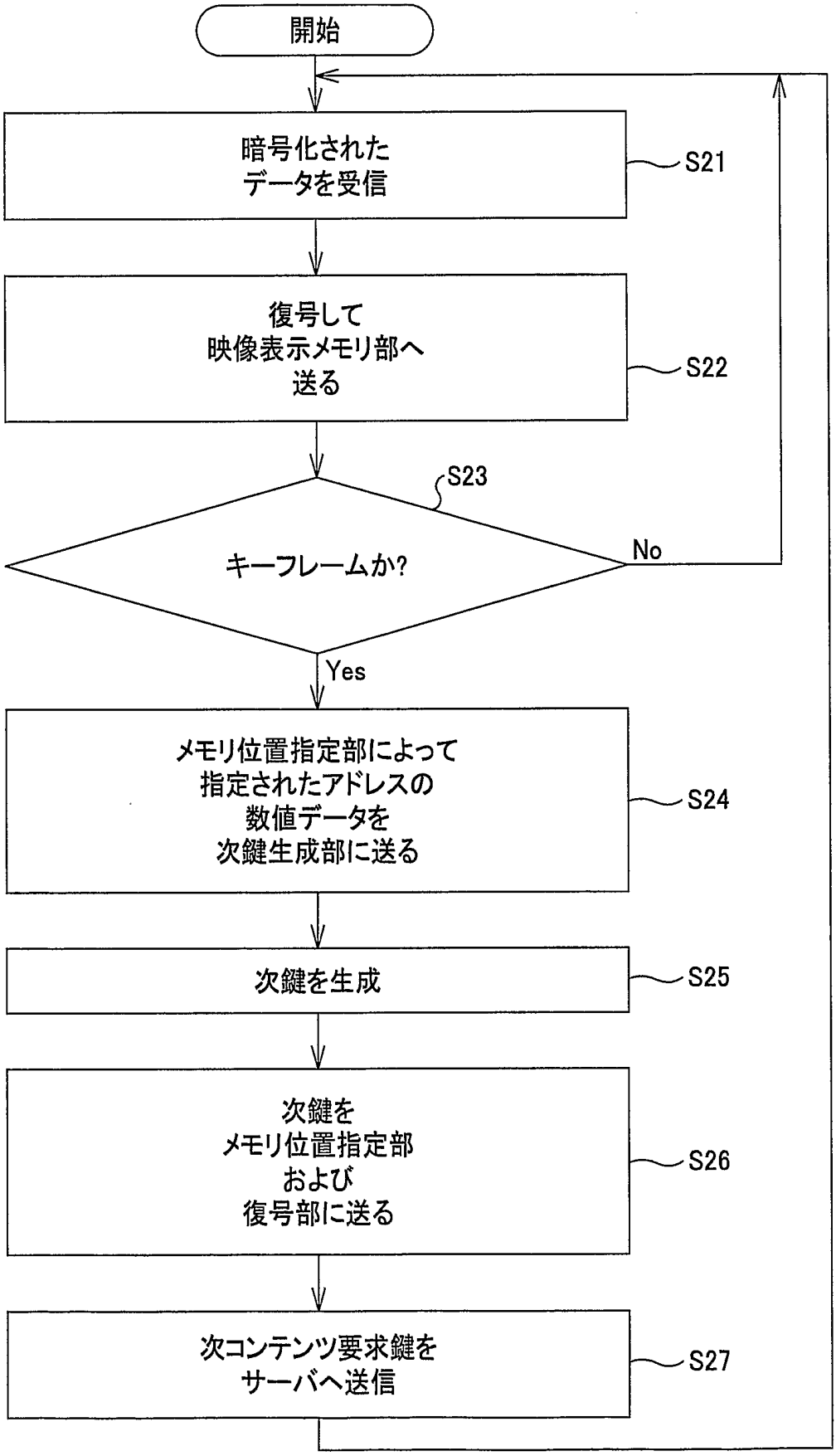

開始
暗号化された
データを受信
S21
復号して
映像表示メモリ部へ
送る
S22
S23
キーフレームか?
No
Yes
メモリ位置指定部によって
指定されたアドレスの
数値データを
次鍵生成部に送る
S24
次鍵を生成
S25
次鍵を
メモリ位置指定部
および
復号部に送る
S26
次コンテンツ要求鍵を
サーバへ送信
S27

FIG.9

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP03/12847

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04L9/32, H04L9/06

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.Cl[7] H04L9/32, H04L9/06, H04N7/16-173

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

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2004
Kokai Jitsuyo Shinan Koho	1971-2004	Jitsuyo Shinan Toroku Koho	1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
JICST FILE(JOIS), WPI, content, advertisement, ad.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 9-65321 A (Hitachi, Ltd.), 07 March, 1997 (07.03.97), Par. Nos. [0026], [0027] (Family: none)	1-15,24,25, 28,29
Y	US 4697209 A (A.C. Nielsen Co.), 29 September, 1987 (29.09.87), Column 4, line 25 to column 5, line 45; column 11, line 36 to column 12, line 34 & EP 161512 A1 & EP 283570 A2 & JP 60-236331 A & BR 8501964 A & BR 8501965 A & CA 1279124 A & CA 1290052 A	1-15,24,25, 28,29

[X] 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	Date of mailing of the international search report
07 January, 2004 (07.01.04)	20 January, 2004 (20.01.04)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP03/12847

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	JP 2002-156905 A (Nippon Telegraph And Telephone Corp.), 31 May, 2002 (31.05.02), Par. Nos. [0017] to [0043] (Family: none)	16-23,26,27, 30-34 2,5,7,8,11, 15,24,25,28, 29

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP03/12847

Box I Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

The inventions of the claims of the present application are divided into the following two groups:

1. claims 1-15
2. claims 16-34

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☒ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

国際調査報告	国際出願番号　ＰＣＴ／ＪＰ０３／１２８４７

A.　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Ｉｎｔ．Ｃｌ⁷　　Ｈ０４Ｌ９／３２，Ｈ０４Ｌ９／０６

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　　Ｈ０４Ｌ９／３２，Ｈ０４Ｌ９／０６，Ｈ０４Ｎ７／１６－１７３

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	１９７１－２００４年
日本国登録実用新案公報	１９９４－２００４年
日本国実用新案登録公報	１９９６－２００４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）

ＪＩＣＳＴファイル（ＪＯＩＳ），ＷＰＩ
content, advertisement, ad.

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
Y	JP 9-65321 A (株式会社日立製作所) 1997.03.07, 第26,27段落　(ファミリなし)	1-15,24,25,28,29
Y	US 4697209 A (A.C. Nielsen Company) 1987.09.29, 第4欄第25行-第5欄第45行, 第11欄第36行-第12欄第34行 & EP 161512 A1 & EP 283570 A2 & JP 60-236331 A & BR 8501964 A & BR 8501965 A & CA 1279124 A & CA 1290052 A	1-15,24,25,28,29

☒ 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	国際調査報告の発送日
０７．０１．０４	20.1.2004

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）	
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	中里　裕正	5M　9364
	電話番号　０３－３５８１－１１０１　内線　３５９７	

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	JP 2002-156905 A（日本電信電話株式会社） 2002.05.31，第17-43段落　（ファミリなし）	16-23, 26, 27, 30-34
Y		2, 5, 7, 8, 11, 15, 24, 25, 28, 29

国際調査報告	国際出願番号　ＰＣＴ／ＪＰ０３／１２８４７

第Ⅰ欄　請求の範囲の一部の調査ができないときの意見（第１ページの２の続き）

法第８条第３項（ＰＣＴ１７条(2)(a)）の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1．☐ 請求の範囲 _____ は、この国際調査機関が調査をすることを要しない対象に係るものである。
つまり、

2．☐ 請求の範囲 _____ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、

3．☐ 請求の範囲 _____ は、従属請求の範囲であってＰＣＴ規則6.4(a)の第２文及び第３文の規定に従って記載されていない。

第Ⅱ欄　発明の単一性が欠如しているときの意見（第１ページの３の続き）

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。

本願の請求の範囲に係る発明は、以下の２群に分けられるものと認める。

1．請求の範囲 1-15
2．請求の範囲 16-34

1．☐ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。

2．☒ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。

3．☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったので、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。

4．☐ 出願人が必要な追加調査手数料を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数料の異議の申立てに関する注意

☐ 追加調査手数料の納付と共に出願人から異議申立てがあった。

☐ 追加調査手数料の納付と共に出願人から異議申立てがなかった。