(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第5130734号
(P5130734)

(45)発行日　平成25年1月30日(2013.1.30)　(24)登録日　平成24年11月16日(2012.11.16)

(51)Int.Cl.　F I
H04N 7/173 (2011.01)　H04N 7/173 610Z
H04N 7/167 (2011.01)　H04N 7/167 Z
H04N 7/173 630

請求項の数 11　(全 36 頁)

(21)出願番号　特願2007-34366(P2007-34366)
(22)出願日　平成19年2月15日(2007.2.15)
(65)公開番号　特開2008-199435(P2008-199435A)
(43)公開日　平成20年8月28日(2008.8.28)
審査請求日　平成21年12月21日(2009.12.21)

(73)特許権者　000002185
ソニー株式会社
東京都港区港南１丁目７番１号
(74)代理人　100093241
弁理士　宮田　正昭
(74)代理人　100101801
弁理士　山田　英治
(74)代理人　100086531
弁理士　澤田　俊夫
(74)代理人　100095496
弁理士　佐々木　榮二
(72)発明者　小川　晃通
東京都港区港南１丁目７番１号　ソニー株式会社内

最終頁に続く

(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

(57)【特許請求の範囲】
【請求項１】
放送データを受信し、ネットワーク接続されたクライアントに対して受信データを出力する情報処理装置であり、
放送データを受信する放送受信部と、
前記放送受信部の受信したデータに対する暗号化処理を実行する暗号処理部と、
前記暗号処理部の生成した暗号化データを蓄積するデータ蓄積部と、
前記データ蓄積部に蓄積された暗号化データを格納した通信パケットを生成して出力するデータ送信部と、
前記データ蓄積部における前記暗号化データの滞留状態を監視し、予め定めた許容滞留状態と異なる状態が検出された場合、前記データ蓄積部に蓄積された暗号化データの少なくとも一部を送信データから排除する処理を実行する送信データ制御部と、
前記クライアントに対して提供するユーザインタフェース（ＵＩ）情報を生成するユーザインタフェース生成部を有し、
前記ユーザインタフェース生成部は、
クライアントからの要求に応じて、ユーザインタフェース（ＵＩ）情報を生成し、生成ＵＩ情報を前記暗号処理部に出力する構成であり、
前記データ送信部は、ＵＩ情報を含むＴＣＰパケットを生成してクライアントに対して出力する処理を実行する構成であることを特徴とする情報処理装置。
【請求項２】

前記送信データ制御部は、
前記データ蓄積部における前記暗号化データの滞留状態時間を監視し、予め定めた許容滞留時間を超えた暗号化データを送信データから排除する処理を実行する構成であることを特徴とする請求項１に記載の情報処理装置。
【請求項３】
前記暗号処理部の生成する前記暗号化データは、タイムスタンプを設定したＴＳ（Ｔｒａｎｓｐｏｒｔ　Ｓｔｒｅａｍ）パケットであるＴＴＳパケットを複数個含むＴＴＳパケットサイズの整数倍のサイズを有するＰＣＰ（Ｐｒｏｔｅｃｔｅｄ　Ｃｏｎｔｅｎｔ　Ｐａｃｋｅｔ）であり、
前記送信データ制御部は、
前記データ蓄積部に蓄積される個々のＰＣＰについて、ＰＣＰ単位で滞留時間を監視し、予め定めた許容滞留時間を超えたＰＣＰを送信データから排除する処理を実行する構成であることを特徴とする請求項１または２に記載の情報処理装置。
【請求項４】
前記データ送信部は、
前記データ蓄積部に蓄積されたＰＣＰ中、前記データ蓄積部における滞留時間が、予め定めた許容滞留時間以内のＰＣＰを送信データとしたＴＣＰパケットを生成してネットワーク出力する処理を実行する構成であることを特徴とする請求項３に記載の情報処理装置。
【請求項５】
前記送信データ制御部は、
前記データ蓄積部における前記暗号化データの滞留量を監視し、予め定めた許容滞留量を超えた場合、前記データ蓄積部に蓄積された暗号化データの少なくとも一部を送信データから排除する処理を実行する構成であることを特徴とする請求項１に記載の情報処理装置。
【請求項６】
前記ユーザインタフェース生成部は、
リモコンまたは操作部からの入力に基づいて、ユーザインタフェース（ＵＩ）情報を生成する構成であることを特徴とする請求項１に記載の情報処理装置。
【請求項７】
前記情報処理装置は、さらに、
前記放送受信部を介して入力する放送番組に対応する番組情報を前記放送受信部を介して入力し管理する番組情報管理部と、
前記番組情報管理部の管理する番組情報の更新の有無を監視する番組情報更新監視部を有し、
前記番組情報管理部は、
前記ネットワーク接続されたクライアントからの番組情報に対する閲覧処理の実行有無を示すフラグを保持し、
前記番組情報更新監視部から番組情報更新発生の検出情報を受領した場合、前記フラグの値が閲覧処理有りの値に設定されていることを条件として、番組情報の更新が発生したことを示す情報更新通知をクライアントに対して実行する構成であることを特徴とする請求項１から６いずれかに記載の情報処理装置。
【請求項８】
前記番組情報管理部は、
前記ネットワーク接続されたクライアントからの番組情報に対する閲覧処理の実行有無を示すフラグを、個々の番組情報であるアイテム（ｉｔｅｍ）の上位オブジェクトとしてのコンテナ（Ｃｏｎｔａｉｎｅｒ）単位で保持し、各コンテナ単位で、前記情報更新通知の制御を行う構成であることを特徴とする請求項７に記載の情報処理装置。
【請求項９】
前記番組情報管理部は、

前記ネットワーク接続されたクライアントからの番組情報に対する閲覧処理の実行有無を示すフラグを、個々のクライアント単位で保持し、各クライアント単位で、前記情報更新通知の制御を行う構成であることを特徴とする請求項７に記載の情報処理装置。

【請求項１０】

放送データを受信し、ネットワーク接続されたクライアントに対して受信データを出力する情報処理装置において実行する情報処理方法であり、

放送受信部が、放送データを受信する放送受信ステップと、

暗号処理部が、前記放送受信部の受信したデータに対する暗号化処理を実行する暗号処理ステップと、

データ蓄積部が、前記暗号処理部の生成した暗号化データを蓄積するデータ蓄積ステップと、

データ送信部が、前記データ蓄積部に蓄積された暗号化データを格納した通信パケットを生成して出力するデータ送信ステップと、

送信データ制御部が、前記データ蓄積部における前記暗号化データの滞留状態を監視し、予め定めた許容滞留状態と異なる状態が検出された場合、前記データ蓄積部に蓄積された暗号化データの少なくとも一部を送信データから排除する処理を実行する送信データ制御ステップと、

ユーザインタフェース生成部が、前記クライアントに対して提供するユーザインタフェース（ＵＩ）情報を生成するユーザインタフェース生成ステップを有し、

前記ユーザインタフェース生成ステップは、

クライアントからの要求に応じて、ユーザインタフェース（ＵＩ）情報を生成し、生成ＵＩ情報を前記暗号処理部に出力するステップであり、

前記データ送信ステップは、ＵＩ情報を含むＴＣＰパケットを生成してクライアントに対して出力する処理を実行するステップであることを特徴とする情報処理方法。

【請求項１１】

放送データを受信し、ネットワーク接続されたクライアントに対して受信データを出力する情報処理装置において情報処理を実行させるコンピュータ・プログラムであり、

放送受信部に、放送データを受信させる放送受信ステップと、

暗号処理部に、前記放送受信部の受信したデータに対する暗号化処理を実行させる暗号処理ステップと、

データ蓄積部に、前記暗号処理部の生成した暗号化データを蓄積させるデータ蓄積ステップと、

データ送信部に、前記データ蓄積部に蓄積された暗号化データを格納した通信パケットを生成して出力させるデータ送信ステップと、

送信データ制御部に、前記データ蓄積部における前記暗号化データの滞留状態を監視し、予め定めた許容滞留状態と異なる状態が検出された場合、前記データ蓄積部に蓄積された暗号化データの少なくとも一部を送信データから排除する処理を実行させる送信データ制御ステップと、

ユーザインタフェース生成部に、前記クライアントに対して提供するユーザインタフェース（ＵＩ）情報を生成させるユーザインタフェース生成ステップを実行させ、

前記ユーザインタフェース生成ステップは、

クライアントからの要求に応じて、ユーザインタフェース（ＵＩ）情報を生成し、生成ＵＩ情報を前記暗号処理部に出力するステップであり、

前記データ送信ステップは、ＵＩ情報を含むＴＣＰパケットを生成してクライアントに対して出力する処理を実行するステップであることを特徴とするコンピュータ・プログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

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。さらに、詳細には、チューナによって受信したデータをネッワーク接続されたクライアントに提供する処理を実行する情報処理装置、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】

【０００２】

昨今のデータ通信ネットワークの普及に伴い、家庭内においても家電機器やコンピュータ、その他の周辺機器をネットワーク接続し、各機器間での通信を可能とした、いわゆるホームネットワークが浸透しつつある。ホームネットワークは、ネットワーク接続機器間で通信を行なうことにより各機器のデータ処理機能を共有することを可能とするものである。ネットワーク接続機器間のコンテンツ送受信等、ユーザに利便性・快適性を提供するものであり、今後、ますます普及することが予測される。

【０００３】

チューナにおいて受信した放送データをこのようなホームネットワークを介してネットワーク接続されたＰＣやディスプレイなどの機器に配信し、チューナとは異なる場所の機器において放送コンテンツを再生するといったことも可能となる。

【０００４】

昨今、放送コンテンツを含むＡＶコンテンツの多くがデジタル化されて提供されているが、デジタル化されたコンテンツはコピーや改竄などの不正な操作が比較的容易であることから、個人的又は家庭的なコンテンツの使用を許容しながら不正使用に対する対策が必要となっており、デジタル・コンテンツの著作権保護を目的とした多くの技術が開発されている。例えば、デジタル伝送コンテンツの保護に関する業界標準として、ＤＴＬＡ（Ｄｉｇｉｔａｌ Ｔｒａｎｓｍｉｓｓｉｏｎ Ｌｉｃｅｎｓｉｎｇ Ａｄｍｉｎｉｓｔｒａｔｏｒ）が開発したＤＴＣＰ（Ｄｉｇｉｔａｌ Ｔｒａｎｓｍｉｓｓｉｏｎ Ｃｏｎｔｅｎｔ Ｐｒｏｔｅｃｔｉｏｎ）がある。ＤＴＣＰにおいては著作権が保護された形でコンテンツを伝送させるための仕組みについて規定されている（例えば、非特許文献１を参照のこと）。

【０００５】

ＤＴＣＰでは、コンテンツ伝送時における機器間の認証プロトコルと、暗号化コンテンツの伝送プロトコルについて取り決められている。その規定は、要約すれば、ＤＴＣＰ準拠機器はＭＰＥＧ（Ｍｏｖｉｎｇ Ｐｉｃｔｕｒｅ Ｅｘｐｅｒｔｓ Ｇｒｏｕｐ）など取り扱いが容易な圧縮コンテンツを非暗号の状態で機器外に送出しないことと、暗号化コンテンツを復号するために必要となる鍵交換を所定の相互認証及び鍵交換（Ａｕｔｈｅｎｔｉｃａｔｉｏｎ ａｎｄ Ｋｅｙ Ｅｘｃｈａｎｇｅ：ＡＫＥ）アルゴリズムに従って行なうこと、並びにＡＫＥコマンドにより鍵交換を行なう機器の範囲を制限することなどを取り決めている。

【０００６】

コンテンツ提供元であるサーバ（ＤＴＣＰ Ｓｏｕｒｃｅ）とコンテンツ提供先であるクライアント（ＤＴＣＰ Ｓｉｎｋ）は、ＡＫＥコマンドの送受信により、認証手続きを経て鍵を共有化し、その鍵を用いて伝送路を暗号化してコンテンツの伝送を行なう。したがって、不正なクライアントは、サーバとの認証に成功しないと暗号鍵を取得できないから、コンテンツを享受することはできない。また、ＡＫＥコマンドを送受信する機器の台数や範囲を制限することによって、コンテンツが使用される範囲を著作権法で言うところの個人的又は家庭の範囲内に抑えることができる。

【０００７】

ＤＴＣＰは、原初的には、ＩＥＥＥ１３９４などを伝送路に用いたホームネットワーク上におけるデジタル・コンテンツの伝送について規定したものである。しかしながら、最近では、ＤＬＮＡ（Ｄｉｇｉｔａｌ Ｌｉｖｉｎｇ Ｎｅｔｗｏｒｋ Ａｌｌｉａｎｃｅ）に代表されるように、デジタル化されたＡＶコンテンツをＩＰネットワークを用いて家庭内で流通させようという動きが本格的になっていることから、ＩＰネットワークに対応したＤＴＣＰ技術、すなわちＩＰパケットを利用してＤＴＣＰ規格に従ったコンテンツ流

通を実現させるＤＴＣＰＩＰ（ＤＴＣＰ　ｏｖｅｒ　ＩＰ）規格が提唱されており、この規格に従った機器が、今後のホームネットワーク機器の主流になると予測される。

【０００８】

ホームネットワークの多くはルータなどを経由してインターネットなどの外部のＩＰネットワークに接続されると、コンテンツの不正コピーや改竄の危惧が指摘されるが、ＤＴＣＰ－ＩＰ技術の確立により、デジタル・コンテンツを保護しながらＩＰネットワークを利用した柔軟で効率的なコンテンツの利用が図られることになる。

【０００９】

ＤＴＣＰ－ＩＰは、基本的にはＤＴＣＰ規格に含まれ、ＤＴＣＰ技術をＩＰネットワークに移植した技術であり、伝送路にＩＰネットワークを使用すること、暗号化されたコンテンツの伝送に適用するプロトコルなどについて規定されている。ＩＰネットワーク上にはＰＣを主としたさまざまな機器が接続され、データの盗聴、改竄が簡単に行なわれてしまう危険が高いことから、ＤＴＣＰ－ＩＰは、コンテンツを保護しながらネットワーク伝送する詳細な規定を有している（例えば、非特許文献２を参照のこと）。

【００１０】

ここで、ＤＴＣＰ－ＩＰに準拠したコンテンツ伝送について説明する。ＤＴＣＰ－ＩＰに準拠したソース（Ｓｏｕｒｃｅ）機器およびシンク（Ｓｉｎｋ）機器間でＨＴＴＰプロトコルを利用したコンテンツ伝送を実施する場合について説明する。ソースは例えばコンテンツを提供するサーバ、シンクはサーバからコンテンツを受信するクライアントである。ソース（Ｓｏｕｒｃｅ）機器およびシンク（Ｓｉｎｋ）機器間では、ＴＣＰ（Ｔｒａｎｓｍｉｓｓｉｏｎ　Ｃｏｎｔｒｏｌ　Ｐｒｏｔｏｃｏｌ）ストリームのような長大なバイト・ストリームを伝送の途中でコンテンツ鍵を変更しながら暗号化通信が行なわれ、且つ、暗号化コンテンツの復号処理その他のコンテンツ処理を実施する際にコンテンツ鍵の確認手続きが行なわれる。また、相互認証及び鍵交換（ＡＫＥ）、コンテンツ伝送、並びにコンテンツ鍵確認の手続き毎にＴＣＰコネクションが確立される。

【００１１】

具体的には、ＡＫＥ手続きが成功すると、ソース（ＤＴＣＰ＿Ｓｏｕｒｃｅ）機器とシンク（ＤＴＣＰ＿Ｓｉｎｋ）機器は、認証鍵K_{auth}を共有することができ、それぞれ内部で同様の処理を行なってK_{auth}からコンテンツ鍵の種となる種鍵K_xを生成する。Ｓｏｕｒｃｅ機器は、乱数を用いてノンスN_cを生成して、K_xとN_cを基にコンテンツ鍵K_cを生成する。そして、Ｓｉｎｋ機器から要求されているコンテンツを、コンテンツ鍵K_cを用いて暗号化し、暗号化コンテンツとノンスN_cからなるパケットをＴＣＰストリーム上に乗せてＳｉｎｋ機器に送信する。一方、Ｓｉｎｋ機器側では、ＴＣＰストリームからノンスN_cを取り出すと、これと認証鍵K_{auth}から求めた鍵K_xを用いて同様にコンテンツ鍵K_cを算出し、暗号化コンテンツを復号することができる。

【００１２】

このように、ＤＴＣＰ－ＩＰは、ＤＴＣＰに準拠した機器同士で認証を行ない、ＤＴＣＰ認証が完了した機器同士で鍵を共有し、コンテンツを伝送する際に暗号化および復号をすることにより、伝送路の途中におけるコンテンツの盗聴、改竄を防ぐという、ＩＰネットワーク上においても安全なコンテンツ伝送手法を提供することができる。

【００１３】

例えば、ＨＴＴＰの手続きに従ってコンテンツを要求する場合、ＤＴＣＰ＿ＳｏｕｒｃｅがＨＴＴＰサーバとなり、ＤＴＣＰ＿ＳｉｎｋがＨＴＴＰクライアントとなって、ＨＴＴＰのためのＴＣＰ／ＩＰコネクションがＨＴＴＰクライアントより作成され、コンテンツの伝送を開始する。ＨＴＴＰクライアントは、通常のＨＴＴＰと全く同様の動作手順によりＨＴＴＰサーバ上のコンテンツを要求する。これに対し、ＨＴＴＰサーバは、要求通りのコンテンツをＨＴＴＰレスポンスとして返す。ＤＴＣＰ＿Ｓｏｕｒｃｅは、ＤＴＣＰ＿Ｓｉｎｋから要求されているコンテンツを、コンテンツ鍵K_cを用いて暗号化し、暗号化コンテンツからなるペイロードとノンスN_cを含んだヘッダからなるパケット（ＰＣＰ：Ｐｒｏｔｅｃｔｅｄ　Ｃｏｎｔｅｎｔ　Ｐａｃｋｅｔ（例えば、特許文献１を参照のこ

と））をＴＣＰストリーム上に乗せて送信する。
【００１４】
例えば、放送コンテンツを受信してクライアントに受信コンテンツを提供するネットワークチューナとクライアントの接続されたホームネットワークを想定した場合、放送データを配信するネットワークチューナは、クライアントからのチューナ操作要求に対して少しでも早く応答しなければならない。しかし、通信プロトコルにＴＣＰを採用している場合、データが確実にクライアントに配送されることが保障されている代わりに、大幅な遅延が発生する可能性がある。
【００１５】
すなわちＴＣＰによるデータ送信では通信データの完全性を保証するため、クライアント側が受信できないデータがある場合、クライアントからサーバに対するデータの再送要求が行われ、サーバは再送要求に応じてデータを再送信するといった処理が実行される。
【００１６】
具体的には、例えばネットワークチューナが配信するデータをクライアントが再生しているときに５秒間の通信障害が発生したとする。ＴＣＰに従った処理では、通信復旧後のデータ送信において、障害発生前（５秒前）の映像からの送信が再開され、結果としてクライアントでは５秒前の映像から再生が開始されることになる。以後、この５秒間の遅延は維持されたままデータ送受信が継続される。
【００１７】
このようなデータ送信が行なわれた場合、クライアント側のユーザがチャンネル変更をネットワークチューナに要求しても、５秒の遅延が維持されており最低でも５秒後にチャンネル変更がなされた映像を見ることになってしまう。これは、ユーザからは操作に対する即応性の低下として観察されることになり、ユーザ要求に対する処理遅延という問題を発生させることになる。
【００１８】
【特許文献１】特開２０００－２８７１９２号公報
【非特許文献１】Ｄｉｇｉｔａｌ Ｔｒａｎｓｍｉｓｓｉｏｎ Ｃｏｎｔｅｎｔ Ｐｒｏｔｅｃｔｉｏｎ Ｓｐｅｃｉｆｉｃａｔｉｏｎ Ｖｏｌｕｍｅ １ （Ｉｎｆｏｒｍａｔｉｏｎａｌ Ｖｅｒｓｉｏｎ）, Ｒｅｖｉｓｉｏｎ １．４ （ｈｔｔｐ：／／ｗｗｗ．ｄｔｃｐ．ｃｏｍ）
【非特許文献２】ＤＴＣＰ Ｖｏｌｕｍｅ １ Ｓｕｐｐｌｅｍｅｎｔ Ｅ Ｍａｐｐｉｎｇ ＤＴＣＰ ｔｏ ＩＰ（Ｉｎｆｏｒｍａｔｉｏｎａｌ Ｖｅｒｓｉｏｎ）, Ｒｅｖｉｓｉｏｎ １．１ （ｈｔｔｐ：／／ｗｗｗ．ｄｔｃｐ．ｃｏｍ）
【発明の開示】
【発明が解決しようとする課題】
【００１９】
本発明は、このような状況に鑑みてなされたものであり、ネットワーク接続されたチューナ機能を持つ情報処理装置において、ネットワーク接続されたクライアントに対して大きな遅延を発生させることのないコンテンツ提供処理を実現する情報処理装置、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。
【課題を解決するための手段】
【００２０】
本発明の第１の側面は、
放送データを受信し、ネットワーク接続されたクライアントに対して受信データを出力する情報処理装置であり、
放送データを受信する放送受信部と、
前記放送受信部の受信したデータに対する暗号化処理を実行する暗号処理部と、
前記暗号処理部の生成した暗号化データを蓄積するデータ蓄積部と、
前記データ蓄積部に蓄積された暗号化データを格納した通信パケットを生成して出力するデータ送信部と、

前記データ蓄積部における前記暗号化データの滞留状態を監視し、予め定めた許容滞留状態と異なる状態が検出された場合、前記データ蓄積部に蓄積された暗号化データの少なくとも一部を送信データから排除する処理を実行する送信データ制御部と、
を有することを特徴とする情報処理装置にある。

【００２１】

さらに、本発明の情報処理装置の一実施態様において、前記送信データ制御部は、前記データ蓄積部における前記暗号化データの滞留状態時間を監視し、予め定めた許容滞留時間を超えた暗号化データを送信データから排除する処理を実行する構成であることを特徴とする。

【００２２】

さらに、本発明の情報処理装置の一実施態様において、前記暗号処理部の生成する前記暗号化データは、タイムスタンプを設定したＴＳ（Ｔｒａｎｓｐｏｒｔ　Ｓｔｒｅａｍ）パケットであるＴＴＳパケットを複数個含むＴＴＳパケットサイズの整数倍のサイズを有するＰＣＰ（Ｐｒｏｔｅｃｔｅｄ　Ｃｏｎｔｅｎｔ　Ｐａｃｋｅｔ）であり、前記送信データ制御部は、前記データ蓄積部に蓄積される個々のＰＣＰについて、ＰＣＰ単位で滞留時間を監視し、予め定めた許容滞留時間を超えたＰＣＰを送信データから排除する処理を実行する構成であることを特徴とする。

【００２３】

さらに、本発明の情報処理装置の一実施態様において、前記データ送信部は、前記データ蓄積部に蓄積されたＰＣＰ中、前記データ蓄積部における滞留時間が、予め定めた許容滞留時間以内のＰＣＰを送信データとしたＴＣＰパケットを生成してネットワーク出力する処理を実行する構成であることを特徴とする。

【００２４】

さらに、本発明の情報処理装置の一実施態様において、前記送信データ制御部は、前記データ蓄積部における前記暗号化データの滞留量を監視し、予め定めた許容滞留量を超えた場合、前記データ蓄積部に蓄積された暗号化データの少なくとも一部を送信データから排除する処理を実行する構成であることを特徴とする。

【００２５】

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、前記クライアントに対して提供するユーザインタフェース（ＵＩ）情報を生成するユーザインタフェース生成部を有し、前記ユーザインタフェース生成部は、クライアントからの要求に応じて、ユーザインタフェース（ＵＩ）情報を生成し、生成ＵＩ情報を前記暗号処理部に出力する構成であり、前記データ送信部は、ＵＩ情報を含むＴＣＰパケットを生成してクライアントに対して出力する処理を実行する構成であることを特徴とする。

【００２６】

さらに、本発明の情報処理装置の一実施態様において、前記ユーザインタフェース生成部は、リモコンまたは操作部からの入力に基づいて、ユーザインタフェース（ＵＩ）情報を生成する構成であることを特徴とする。

【００２７】

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、前記放送受信部を介して入力する放送番組に対応する番組情報を前記放送受信部を介して入力し管理する番組情報管理部と、前記番組情報管理部の管理する番組情報の更新の有無を監視する番組情報更新監視部を有し、前記番組情報管理部は、前記ネットワーク接続されたクライアントからの番組情報に対する閲覧処理の実行有無を示すフラグを保持し、前記番組情報更新監視部から番組情報更新発生の検出情報を受領した場合、前記フラグの値が閲覧処理有りの値に設定されていることを条件として、番組情報の更新が発生したことを示す情報更新通知をクライアントに対して実行する構成であることを特徴とする。

【００２８】

さらに、本発明の情報処理装置の一実施態様において、前記番組情報管理部は、前記ネットワーク接続されたクライアントからの番組情報に対する閲覧処理の実行有無を示すフ

ラグを、個々の番組情報であるアイテム（ｉｔｅｍ）の上位オブジェクトとしてのコンテナ（Ｃｏｎｔａｉｎｅｒ）単位で保持し、各コンテナ単位で、前記情報更新通知の制御を行う構成であることを特徴とする。

【００２９】

さらに、本発明の情報処理装置の一実施態様において、前記番組情報管理部は、前記ネットワーク接続されたクライアントからの番組情報に対する閲覧処理の実行有無を示すフラグを、個々のクライアント単位で保持し、各クライアント単位で、前記情報更新通知の制御を行う構成であることを特徴とする。

【００３０】

さらに、本発明の第２の側面は、

放送データを受信し、ネットワーク接続されたクライアントに対して受信データを出力する情報処理装置において実行する情報処理方法であり、

放送受信部が、放送データを受信する放送受信ステップと、

暗号処理部が、前記放送受信部の受信したデータに対する暗号化処理を実行する暗号処理ステップと、

データ蓄積部が、前記暗号処理部の生成した暗号化データを蓄積するデータ蓄積ステップと、

データ送信部が、前記データ蓄積部に蓄積された暗号化データを格納した通信パケットを生成して出力するデータ送信ステップと、

送信データ制御部が、前記データ蓄積部における前記暗号化データの滞留状態を監視し、予め定めた許容滞留状態と異なる状態が検出された場合、前記データ蓄積部に蓄積された暗号化データの少なくとも一部を送信データから排除する処理を実行する送信データ制御ステップと、

を有することを特徴とする情報処理方法にある。

【００４０】

さらに、本発明の第３の側面は、

放送データを受信し、ネットワーク接続されたクライアントに対して受信データを出力する情報処理装置において情報処理を実行させるコンピュータ・プログラムであり、

放送受信部に、放送データを受信させる放送受信ステップと、

暗号処理部に、前記放送受信部の受信したデータに対する暗号化処理を実行させる暗号処理ステップと、

データ蓄積部に、前記暗号処理部の生成した暗号化データを蓄積させるデータ蓄積ステップと、

データ送信部に、前記データ蓄積部に蓄積された暗号化データを格納した通信パケットを生成して出力させるデータ送信ステップと、

送信データ制御部に、前記データ蓄積部における前記暗号化データの滞留状態を監視し、予め定めた許容滞留状態と異なる状態が検出された場合、前記データ蓄積部に蓄積された暗号化データの少なくとも一部を送信データから排除する処理を実行させる送信データ制御ステップと、

を実行させることを特徴とするコンピュータ・プログラムにある。

【００４１】

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などの記録媒体、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。

【００４２】

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。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。

【発明の効果】

【００４３】

本発明の一実施例の構成によれば、ネットワーク接続されたクライアントに対して放送コンテンテを提供する情報処理装置（ネットワークチューナ）において、放送データを含む送信データを蓄積するバッファを監視し、バッファにおけるデータの滞留状態、例えば、データ滞留時間を監視し、予め定めた許容滞留時間を越えたデータを送信データから排除する処理を実行する。本構成により、例えばクライアントからの再送要求などに起因して発生するデータの送信遅延が継続して維持されるという問題や、あるいは遅延が蓄積するなどの問題が解消され、放送コンテンツのリアルタイムでの送信や、クライアントからのチャンネル変更等の処理要求に対する応答性も向上させることが可能となる。

【発明を実施するための最良の形態】

【００４４】

以下、図面を参照しながら本発明の情報処理装置、および情報処理方法、並びにコンピュータ・プログラムの詳細について説明する。なお、説明は、以下の項目に従って行なう。

１．ネットワーク構成例について

２．送信データの破棄によるデータ遅延防止構成

３．クライアントに対するユーザインタフェース（ＵＩ）の提供処理構成

４．クライアントに対する番組情報提供処理構成

【００４５】

［１．ネットワーク構成例について］

まず、本発明の情報処理装置の適用可能なネットワーク環境について図１を参照して説明する。本発明の情報処理装置は、チューナによって受信したデータをネッワーク接続されたクライアントに提供する処理を実行する情報処理装置であり、図１に示すネットワークチューナ２００である。

【００４６】

図１は、様々な情報処理機器が接続されているホームネットワーク構成を示している。ネットワークチューナ２００は、ＴＶチューナを内蔵し、衛星放送、地上波放送を、アンテナ１２１，１２２を介して受信し、受信コンテンツをネットワーク１５０を介してクライアント２５１，２５２に提供する。

【００４７】

図１に示すネットワーク１５０は例えばＩＰ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）ネットワークであり、ネットワーク１５０を介したデジタル・コンテンツの伝送はＤＴＣＰＩＰ（ＤＴＣＰ　ｏｖｅｒ　ＩＰ）規格に従って実行される。ＤＴＣＰ－ＩＰに従ったデジタル・コンテンツの伝送においては、先に説明したように、例えばコンテンツ提供側であるサーバ（ソース）と、コンテンツ受信側であるクライアント（シンク）間での認証処理の後、サーバ側でコンテンツを暗号化して送信し、クライアント側で受信暗号化コンテンツを復号して再生処理が実行される。この一連の処理、すなわち相互認証および鍵交換（ＡＫＥ）、コンテンツ伝送、並びにコンテンツ鍵確認の手続き毎にサーバクライアント間でＴＣＰコネクションが確立されて処理が実行される。

【００４８】

コンテンツは、コンテンツ鍵を用いて暗号化され、暗号化コンテンツからなるペイロード、コンテンツ鍵生成情報（ノンスＮ）を含んだヘッダからなるパケット（ＰＣＰ：Ｐｒｏｔｅｃｔｅｄ　Ｃｏｎｔｅｎｔ　Ｐａｃｋｅｔ）としてＴＣＰ（Ｔｒａｎｓｍｉｓｓｉｏｎ　Ｃｏｎｔｒｏｌ　Ｐｒｏｔｏｃｏｌ）ストリーム上に乗せて送信される。図１に示すネットワークチューナ２００は、アンテナ１２１，１２２を介して放送コンテンツを受信してクライアント２５１，２５２に受信コンテンツを提供する際、受信コンテンツに対する暗号化処理、ＰＣＰの生成を行なって出力する。

【００４９】
［２．送信データの破棄によるデータ遅延防止構成］
前述したように、ＴＣＰ（Ｔｒａｎｓｍｉｓｓｉｏｎ Ｃｏｎｔｒｏｌ Ｐｒｏｔｏｃｏｌ）によるデータ送信では通信データの完全性を保証するため、クライアント側が受信できないデータがある場合、クライアントからサーバに対するデータの再送要求が行われ、サーバは再送要求に応じてデータを再送信するといった処理を実行する。従って、データ配信処理における遅延が発生する可能性が高くなる。
【００５０】
先に説明したようにＴＣＰに従った通信においては、サーバクライアント間の通信復旧後にデータ送信を再開する場合、障害発生前（例えば５秒前）の映像からの送信処理を再開することになり、その後のサーバクライアント間のデータ送受信は、発生した遅延時間（例えば５秒）を維持したまま行なわれることになる。
【００５１】
このように一旦、発生した遅延は、継続したコンテンツ送信期間中、維持され、また再送処理の積み重ねによって遅延が次第に増加するという可能性も高い。このようなデータ送信の結果、例えば、クライアント側のユーザがチャンネル変更をネットワークチューナに要求しても、遅延によって、所定の遅延時間（例えば５秒）後にチャンネル変更がなされることになる。
【００５２】
本発明の情報処理装置、すなわち、図１に示すネットワークチューナ２００は、このような遅延を解消する処理を実行して、よりリアルタイムに近い放送コンテンツの提供を実現し、さらにユーザによる操作、例えばチャンネル変更や、その他のリモコン操作に対する即応性を向上させた構成を持つ。
【００５３】
本発明の情報処理装置、すなわち、図１に示すネットワークチューナ２００は、遅延量が過大になるのを防止するため、鮮度が低下したデータを送信対象データから排除する処理を実行する。すなわち、鮮度が低下したデータの破棄処理を行なう。ただし、データの破棄をただやみくもに行ってしまっては、クライアント２５１，２５２において正しい再生処理ができなくなってしまう可能性がある。特にデジタル放送のネットワーク配信の場合、ネットワーク上はデータを暗号化して送信しなければならず、やみくもに破棄してしまっては、クライアントで復号処理ができなくなってしまう。そこでネットワークチューナ２００は、予め定めたデータの破棄条件を検証しながら、破棄するデータを決定してデータ破棄処理を実行する。
【００５４】
本発明の第１実施例に係る情報処理装置、すなわち、ネットワークチューナ２００の第１実施例の構成例を図２に示す。ネットワークチューナ２００は、図２に示すように放送波受信部２０１、暗号処理部２０２、データ蓄積部（バッファ）２０３、データ送受信部２０４、送信データ制御部２０５を有する。また、送信データ制御部２０５は、データ滞留時間監視部２０６、データ破棄実行部２０７を有する。
【００５５】
放送波受信部２０１は、放送データをアンテナ１２１，１２２を介して受信し、選局されているチャンネル対応の放送コンテンツ（ＭＥＰＧデータ）を取り出して、暗号処理部２０２に出力する。なお、選局情報はデータ送受信部２０４を介するクライアントからの入力、あるいは図示しないリモコンや操作部を介する入力が可能である。
【００５６】
暗号処理部２０２は、放送波受信部２０１で取り出した放送コンテンツ（ＭＰＥＧデータ）をＤＴＣＰ－ＩＰ形式で暗号化して、データ蓄積部（バッファ）２０３に出力する。
【００５７】
暗号処理部２０２においては、コンテンツの暗号用の鍵であるコンテンツ鍵を適用した暗号化処理を実行して、暗号化コンテンツからなるペイロードとコンテンツ鍵の生成情報

を含んだヘッダからなるパケット（ＰＣＰ：Ｐｒｏｔｅｃｔｅｄ　Ｃｏｎｔｅｎｔ　Ｐａｃｋｅｔ）を生成する。コンテンツ鍵は、サーバ（本例ではネットワークチューナ２００）とコンテンツ送信先のクライアント、図１に示すクライアント２５１またはクライアント２５２のいずれかのクライアントとの間で、コンテンツ送信の前処理として実行される相互認証及び鍵交換（ＡＫＥ）に際して決定される鍵である。

【００５８】

本発明の一実施例に係るネットワークチューナ２００の暗号処理部２０２が生成するＰＣＰの構成について図３を参照して説明する。図３（ａ）は、１つが１８８バイトのＴＳパケットに４バイトのタイムスタンプを付加した計１９２バイトのＴＴＳ（Ｔｉｍｅｓｔａｍｐｅｄ　Ｔｒａｎｓｐｏｒｔ　Ｓｔｒｅａｍ）パケットである。図３（ｂ）は、複数のＴＴＳに基づいて生成する送信単位の暗号化パケットであるＰＣＰ（Ｐｒｏｔｅｃｔｅｄ　Ｃｏｎｔｅｎｔ　Ｐａｃｋｅｔ）を示している。

【００５９】

暗号処理部２０２では、放送波受信部２０１において受信する放送コンテンツを入力して、図３（ａ）に示すタイムスタンプを設定したＭＰＥＧ２－ＴＴＳ（１９２ｂｙｔｅ）を構成するとともに、複数のＭＰＥＧ２－ＴＴＳを１つの暗号化単位として設定した図３（ｂ１）に示すＰＣＰを生成して図２に示すデータ蓄積部（バッファ）２０３に出力する。

【００６０】

図３（ｂ１）に示すＰＣＰは、暗号処理部２０２において実行される暗号処理単位であり、また送信データ単位でもある。送信処理は、図３（ｂ２）に示すようにＰＣＰを単位として実行される。ＰＣＰのデータ量（バイト数）は基本的にサーバ側が任意に設定可能であるが、本発明の一実施例に従ったネットワークチューナ２００では、１つのＰＣＰのサイズを、ＴＴＳのバイト数（１９２バイト）の倍数、すなわち１９２×ｎバイトに設定した。

【００６１】

サーバは任意バイト数のＰＣＰを設定して送信を行なうことが可能であり、従来の一般的なＰＣＰの生成処理に際しては、図３（ｃ）に示すように、１つのＴＴＳパケットの途中でデータが区切られたＰＣＰを生成して、ＰＣＰ単位のデータ送信を実行するのが一般的である。このようなＰＣＰの設定、送信処理を行なっても、ＴＣＰに従ったデータ通信を実行して、クライアント側ですべてのデータを受信して、復号処理を実行する設定であればＴＳパケット単位の処理が可能であり復号、再生に問題は発生しない。

【００６２】

しかし、本発明のネットワークチューナ２００では、データ送信における遅延に応じて送信データの破棄処理を実行する構成であり、この破棄処理を考慮して、図３（ｂ１）（ｂ２）に示すように１つのＰＣＰのサイズを、ＴＴＳのバイト数（１９２バイト）の倍数、すなわち１９２×ｎバイトに設定し、送信する構成としている。このようなＰＣＰのサイズ設定とすることで、ＰＣＰ単位での破棄処理を行った場合のクライアント側におけるコンテンツ復号、再生処理に与える影響を低減している。

【００６３】

本発明のネットワークチューナ２００の実行する送信データの破棄処理の１つの具体例について図４以下を参照して説明する。図４に示すように暗号処理部２０２の生成したＰＣＰは、ＰＣＰ単位でデータ蓄積部（バッファ）２０３に蓄積される。

【００６４】

送信データ制御部２０５のデータ滞留時間監視部２０６では、データ蓄積部（バッファ）２０３に格納されるデータのデータ蓄積部（バッファ）２０３における滞留時間を、各ＰＣＰ単位で監視する。送信データ制御部２０５のデータ破棄実行部２０７では、この滞留時間が、予め定めたデータ破棄基準時間：Ｔｄを越えたＰＣＰを抽出しデータの破棄処理を実行する。このようにデータ破棄はＰＣＰを単位として実行される。

【００６５】

送信データ制御部２０５の処理について詳細に説明する。
データ滞留時間監視部２０６は、暗号処理部２０２からデータ蓄積部（バッファ）２０３に入力する各ＰＣＰの入力時刻を入力ＰＣＰに対応付けて記録し、各ＰＣＰのデータ蓄積部（バッファ）２０３における滞留時間を算出する。例えば図５に示すように、各ＰＣＰのデータ蓄積部（バッファ）２０３への格納開始時刻としての入力時刻［Ｔｘ］を入力ＰＣＰのＩＤ［ＰＣＰ－ＩＤ］に対応付けて記録し、各ＰＣＰのデータ蓄積部（バッファ）２０３における滞留時間を、現在時刻［Ｔｎ］との差分、すなわち、
Ｔｎ－Ｔｘ
として算出する。
【００６６】
データ破棄実行部２０７は、各ＰＣＰのデータ蓄積部（バッファ）２０３における滞留時間［Ｔｎ－Ｔｘ］と、予め定めた許容滞留時間としてのデータ破棄基準時間［Ｔｄ］とを比較し、滞留時間［Ｔｎ－Ｔｘ］が、データ破棄基準時間［Ｔｄ］を越えたＰＣＰ、すなわち、
Ｔｎ－Ｔｘ＞Ｔｄ
上記式を満足するＰＣＰが、データ蓄積部（バッファ）２０３に存在することが検出された場合、そのＰＣＰを破棄する処理を実行する。
【００６７】
この結果、データ送受信部２０４へは、データ蓄積部（バッファ）２０３における滞留時間がＴｄ以下のデータのみが選択されて出力される。データ送受信部２０４では、データ蓄積部（バッファ）２０３から入力するデータのみを送信対象のデータとしてＴＣＰに従ったデータ送信処理を実行する。データ送受信部２０４に入力されないデータは、データ送受信部２０４では、送信対象データとして認識されない。
【００６８】
データ送受信部２０４では、いわゆるＩＳＯ参照モデルにおけるＴＣＰレイヤ（トランスポート層）以下の処理を実行する。すなわち、ＩＳＯ参照モデルを上位層から、
アプリケーション層、
トランスポート層（ＴＣＰレイヤ）
インターネット層（ＩＰレイヤ）
物理層
とした場合、データ送受信部２０４では、トランスポート層（ＴＣＰレイヤ）、インターネット層（ＩＰレイヤ）、物理層における処理を実行し、データ蓄積部（バッファ）２０３から入力するＰＣＰに基づいてＴＣＰパケット、ＩＰパケットを生成してネットワークインタフェースを介してデータ送信を実行する。
【００６９】
データ蓄積部（バッファ）２０３における滞留時間がＴｄを超えるデータ（ＰＣＰ）は、ＴＣＰパケットの生成処理前に破棄されており、ＴＣＰに従ったデータ送信の対象として設定されない。送信データ制御部２０５において破棄されたデータは、そもそもＴＣＰパケット生成時には、当初から存在しないデータであり、ＴＣＰパケットはデータ蓄積部（バッファ）２０３における滞留時間がＴｄ以下のデータを対象として生成される。クライアントは、ＴＣＰパケットの解析に基づいて未受信データの再送要求を行うので、クライアントにおけるＴＣＰパケットの解析では、送信データ制御部２０５において破棄されたデータはそもそも存在しないデータとして認識されるので、破棄データについての再送要求は実行されない。結果として、クライアントは、データ蓄積部（バッファ）２０３における滞留時間がＴｄ以下のデータを受信して、復号、再生処理を実行することになる。
【００７０】
先に説明したように、暗号処理部２０２が生成するＰＣＰサイズは、ＭＰＥＧ２－ＴＴＳ（１９２ｂｙｔｅ）の整数倍になるように設定されている。送信データ制御部２０５では、データ破棄をＰＣＰ単位で実行する。このようにＰＣＰサイズをＴＴＳの倍数に設定し、ＰＣＰ単位でのデータ破棄を実行することで、データ滞留時間に基づくＰＣＰデータ

破棄が実行された場合も、データを受け取るクライアントでは、ＭＰＥＧ２－ＴＴＳの単位で区切りの良いデータ受信が可能であり、復号、再生処理を行なった場合のデータ欠落の影響が低減される。

【００７１】

この理由について図６、図７を参照して説明する。図６は、先に図３を参照して説明したように、本発明の一実施例に係る情報処理装置、すなわちネットワークチューナ２００における処理について説明する図である。図６（ａ）は、１つが１８８バイトのＴＳパケットに４バイトのタイムスタンプを付加した計１９２バイトのＭＰＥＧ２－ＴＴＳ（Ｔｉｍｅｓｔａｍｐｅｄ　Ｔｒａｎｓｐｏｒｔ　Ｓｔｒｅａｍ）パケット、図６（ｂ）は、暗号処理部２０２が生成するＰＣＰ（Ｐｒｏｔｅｃｔｅｄ　Ｃｏｎｔｅｎｔ　Ｐａｃｋｅｔ）であり、複数のＭＰＥＧ２－ＴＴＳを１つの暗号化単位として設定したＰＣＰである。

【００７２】

図６（ｃ）に示すように、各ＰＣＰが送信データ単位として設定されＴＣＰパケットに格納されて送信されることになる。例えば、図６（ｄ）に示すＰＣＰ２７１，２７２，２７３中のＰＣＰ２７２がデータ蓄積部（バッファ）２０３における滞留時間がＴｄを超えた場合、ＰＣＰ２７２は、送信データ制御部２０５によって破棄されてしまう。

【００７３】

この場合、クライアントに送信されるＰＣＰは、図６（ｅ）に示すＰＣＰ２７１，２７３となる。しかし、この場合、ＰＣＰ２７１、ＰＣＰ２７３のそれぞれには、完全なＴＴＳ、すなわち１９２バイトの完全なＴＴＳが複数格納されており、不完全なＴＴＳは含まれない。すなわち、クライアントは個々の完全なＴＴＳに基づくデータ再生を行なうことができる。

【００７４】

一方、ＰＣＰサイズをＴＴＳの整数倍としない設定でデータ破棄を実行した場合、クライアント側の再生処理においてより大きな影響が発生する。図７を参照してこの理由について説明する。図７（ａ）は、１つが１８８バイトのＴＳパケットに４バイトのタイムスタンプを付加した計１９２バイトのＭＰＥＧ２－ＴＴＳ（Ｔｉｍｅｓｔａｍｐｅｄ　Ｔｒａｎｓｐｏｒｔ　Ｓｔｒｅａｍ）パケット、図７（ｂ）は、ＴＴＳの整数倍のサイズに相当しないサイズのＰＣＰを示している。

【００７５】

図７（ｃ）に示すように、各ＰＣＰが送信データ単位として設定されＴＣＰパケットに格納されて送信されることになる。例えば、図７（ｄ）に示すＰＣＰ２８１，２８２，２８３中のＰＣＰ２８２がデータ蓄積部（バッファ）２０３における滞留時間がＴｄを超え破棄されるとすると、クライアントに送信されるＰＣＰは、図７（ｅ）に示すＰＣＰ２８１，２８３となる。

【００７６】

ＰＣＰ２８１、ＰＣＰ２８３のそれぞれには、不完全なＴＴＳ、すなわち１９２バイトのデータを持たない不完全なＴＴＳ２９１，２９２が含まれており、クライアントは、これらの不完全なＴＴＳ２９１，２９２に基づく再生データを生成することができない。すなわち、クライアントはＰＣＰ２８１、ＰＣＰ２８３に含まれる１９２バイトの完全なＴＴＳに基づくデータ再生を行なうことになり、不完全なＰＣＰ２９１，２９２については再生に適用できない無駄なデータとして処理せざる得ないこととなる。

【００７７】

上述したように、ＰＣＰサイズを、図６を参照して説明したようにＴＴＳサイズの整数倍に設定してＰＣＰ単位での破棄処理を実行することで、クライアントは、受信データに含まれるＴＴＳの復号、再生を行なうことが可能となる。なお、この場合も破棄されたＰＣＰに含まれるＴＴＳについての再生はできないが、ほとんどのＰＣＰが送信できていれば、再生される映像等の品質を大幅に低下させることはない。

【００７８】

このように、バッファ滞留時間をＰＣＰ単位で計測して、予め定めた許容滞留時間を超

えたＰＣＰを破棄して、クライアントに対する送信データの対象から除去することで、送信データの遅延の発生を防止することが可能となる。すなわち、ＴＣＰに基づくデータ再送要求がクライアントからサーバ（ネットワークチューナ）に対して実行された場合、サーバ（ネットワークチューナ）は、ＴＣＰに基づく再送処理を実行するが、この再送処理の実行などに起因して、バッファ滞留時間が許容滞留時間を超えたＰＣＰについては破棄され、バッファ滞留時間が許容滞留時間以内のデータのみが送信されることになるので、放送コンテンツの送信処理においてほぼリアルタイムでの送信を維持することが可能となる。

【００７９】

結果として、クライアントは放送コンテンツをほぼリアルタイムで再生することが可能となる。すなわち、ＴＣＰパケットの再送要求が発生しても遅延時間は、ＰＣＰの破棄によって解消され遅延時間の維持や蓄積が発生せず、クライアントにおいては放送コンテンツのリアルタイム再生を維持することができる。また、例えばクライアントからのチャンネル変更の要求がサーバ（ネットワークチューナ）に出力された場合でも、サーバ側では遅延のない応答処理が可能となり、ユーザ要求に対する即応性を維持することが可能となる。

【００８０】

なお、上述の実施例では、ＰＣＰをデータ破棄単位として設定した例を説明したが、ＰＣＰを単位とするのではなく、例えばＭＰＥＧデータのＧＯＰ（Group Of Pictures）を破棄単位として設定する構成も可能である。すなわち、データ滞留時間監視部２０６は、データ蓄積部（バッファ）２０３における滞留時間の監視をＧＯＰ単位で実行し、上記条件と同様のＧＯＰ単位で予め定めた許容時間を越えた滞留時間のデータを破棄する構成としてもよい。ただし暗号化データである場合は、復号を行なわないとＧＯＰ単位情報が取得できないため、暗号処理が実行されない送信データの場合にＧＯＰ単位の処理を行なうことが可能である。ただし、暗号化データに対してＭＰＥＧのＧＯＰ情報を付加した設定とする暗号化処理を実行する構成とすれば、この限りではない。

【００８１】

また、上記実施例では、データ破棄の条件を各ＰＣＰのバッファにおける滞留時間のみに基づいて実行する構成として説明したが、例えば、データ蓄積部（バッファ）２０３における滞留量が一定基準を超えたら破棄するといった処理を行なう構成としてもよい。すなわち、送信データ制御部２０５にデータ蓄積部（バッファ）２０３におけるデータ滞留量を監視する監視部を設け、予め定めた許容滞留量以上のデータがデータ蓄積部（バッファ）２０３に滞留していることを検出した場合、データ破棄実行部が、データ蓄積部（バッファ）２０３に格納された時間が早いものから順に規定の単位（例えばＰＣＰ単位）で破棄する。破棄を開始する基準は、例えば放送データのビットレートに応じて変更する設定とする。

【００８２】

さらに、クライアントがデータの破棄要求をサーバ（ネットワークチューナ）に送信する構成とし、破棄要求を受け取ったサーバ（ネットワークチューナ）が規定の単位（例えばＰＣＰ単位）でデータを破棄する構成としてもよい。なお、クライアントが送信する要求は、データの破棄を示す直接的な要求とは限らない。サーバはクライアントからの何らかのリクエストを受け取ったときに、自分の状態を考慮して（前述の滞留時間や滞留量など）、データを破棄する設定としてもよい。例えばチャンネル変更要求などがこれに該当する。クライアントが直接的に破棄要求を送信してくる場合、破棄するデータ量（バイト数や秒数）を要求に含めて送信してくる構成とし、サーバ（ネットワークチューナ）がこの要求に併せてデータ破棄を実行してもよい。

【００８３】

［３．クライアントに対するユーザインタフェース（ＵＩ）の提供処理構成］

次に、サーバ、すなわち、図１に示すネットワークチューナ２００からクライアント２５１，２５２に対してユーザインタフェース（ＵＩ）の提供処理を行なう構成例について

図８以下を参照して説明する。

【００８４】

本実施例に係る情報処理装置、すなわち、図１に示すネットワークチューナ２００の第２実施例の構成を図８に示す。図８に示すネットワークチューナ２００は、図２を参照して説明した第１実施例のネットワークチューナ２００の構成に、ユーザインタフェース（ＵＩ）生成部３０１と、リモコン信号受信部３０２を追加した構成となっている。

【００８５】

ネットワーク出力端子を持つ一般的なテレビなどの表示装置の場合、放送波を受信するチューナ部と、受信コンテンツを出力するディスプレイと、ネットワーク出力端子を備えているが、ディスプレイに出力するデータと、ネットワーク出力するデータとでは必ずしも一致しないものとなっている。すなわち、デジタル・コンテンツの出力は、ＤＴＣＰＩＰに従ってネットワーク出力することが必要であり、放送コンテンツについてはＤＴＣＰＩＰに従ったデータ、すなわち前述したＰＣＰの生成を実行してＴＣＰパケットを、認証処理を行なった特定クライアントに対して出力することになる。

【００８６】

一般的なテレビなどの表示装置の場合、ディスプレイには放送コンテンツの表示を行なうとともに、様々な操作情報、ガイド情報や、メッセージ通知、ブックマーク情報、試聴履歴情報などの放送コンテンツとは異なる各種情報を含むユーザインタフェース（ＵＩ）を表示して、テレビに付属するリモコンなどで操作することが可能であるが、ネットワーク接続されたクライアントには、このようなＵＩ情報は提供されない。

【００８７】

クライアント側で出力映像上にＵＩを描画することにより、ネットワーク経由での操作と物理リモコンでの操作を同様に見せる構成とすることも可能であるが、以下の欠点がある。

１．ネットワーククライアントにおいてＵＩ用のプログラムを作成するのが大変である。

２．ネットワーククライアントにおいて放送されているＢＭＬ（Broadcast Markup language）を解釈しなければならず、開発工数が膨大になる。（なお、ＢＭＬとは、操作ボタンやリンク情報などを設定可能としたユーザインタフェースを構築するＸＭＬベースのページ記述言語である）

３．サーバ側ＵＩがアップデートされた場合、ネットワーククライアントも同期してアップデートを行わなければならない。

４．ＵＩを描画する部分がサーバとクライアントそれぞれに分散していると、物理リモコンと仮想リモコンが同時に利用されたときに同期を取るのが困難になる。

５．ＵＩ操作部がサーバ側にのみ存在するので、放送波からアップデートを送信するだけで修正が可能。ＵＩがサーバとクライアント両方にある場合、クライアント側にはチューナが存在しないので、放送波からソフトウェアアップデートを供給する術がない。

【００８８】

このように、クライアント側で独自のＵＩを生成して利用する構成とすることは様々な問題を引き起こすことになる。図８に示すネットワークチューナ２００は、これらの問題を解決する構成を持つ。すなわち、ネットワークに接続されたクライアントに対して、チューナ受信コンテンツを提供するのみならず、ネットワークチューナ２００のユーザインタフェース（ＵＩ）生成部３０１において生成したユーザインタフェース（ＵＩ）情報をＤＴＣＰＩＰに従って生成されるＴＣＰパケットに格納してクライアントに提供し、クライアント側で受信パケットの処理を放送コンテンツに対する処理と同様の処理を実行させてクライアント側のディスプレイにＵＩを表示する。

【００８９】

クライアント側のディスプレイに表示されるＵＩは、サーバ側で生成したＵＩであり、サーバ側の機能更新などの処理が実行された場合、その更新ＵＩがクライアント側に提供され利用可能となる。また、ＵＩ描画部分は、図８に示すネットワークチューナ２００の

ユーザインタフェース（ＵＩ）生成部３０１に集約されるため物理リモコンと仮想リモコンに対応した処理を画一的に行なうことが可能となる。

【００９０】

なお、物理リモコンは、図８に示すリモコン信号受信部３０２に対してリモコン信号を入力する実際のリモコンであり、仮想リモコンは、サーバ（ネットワークチューナ２００）にネットワーク接続されたクライアント、例えば図１に示すクライアント２５１のディスプレイに表示される仮想リモコンである。図９にクライアント側のディスプレイに出力される表示情報の例を示す。図９に示す表示情報は、仮想リモコン３２１と、サーバ（ネットワークチューナ２００）から受信した放送コンテンツ表示データ３２２から構成される。仮想リモコン３２１は、クライアント側のプログラムによってディステプレイに表示される。

【００９１】

図８を参照して本実施例に係るネットワークチューナ２００の処理について説明する。ネットワークチューナ２００は、図８に示すように放送波受信部２０１、暗号処理部２０２、データ蓄積部（バッファ）２０３、データ送受信部２０４、送信データ制御部２０５を有し、さらに、ユーザインタフェース（ＵＩ）生成部３０１、リモコン信号受信部３０２を有する。

【００９２】

放送波受信部２０１、暗号処理部２０２、データ蓄積部（バッファ）２０３、データ送受信部２０４、送信データ制御部２０５は、先に図２～図７を参照して説明したと同様の構成であり、同様の処理を実行する。ユーザインタフェース（ＵＩ）生成部３０１は、図示しない物理リモコンや、ネットワーク接続されたクライアントのディスプレイに表示される仮想リモコンからの要求に応じた表示情報、ユーザインタフェース情報を生成して出力する。

【００９３】

ユーザインタフェース（ＵＩ）生成部３０１の生成した表示情報は、放送コンテンツと同様のプロセスによってクライアントに提供される。すなわち、暗号処理部２０２における暗号処理によってＤＴＣＰＩＰの規定に従ったＰＣＰが生成されて、データ蓄積部２０３に蓄積された後、データ送受信部２０４においてＴＣＰパケット、ＩＰパケットの生成が成されたクライアントに提供される。クライアント側では、放送コンテンツと同様の処理を実行してユーザインタフェース（ＵＩ）生成部３０１の生成した表示情報をクライアント側のディスプレイに表示する。

【００９４】

なお、ユーザインタフェース（ＵＩ）生成部３０１は、ネットワークチューナの記憶部（図示せず）に格納された表示情報生成プログラムに従って、記憶部に格納された表示コンテンツを利用してクライアントに提供する表示情報（ユーザインタフェース）を生成するか、あるいは、放送受信部２０１が受信した情報、例えばＥＰＧや放送局からのお知らせ情報などを適用して表示情報を生成する。

【００９５】

例えば、図９に示すクライアント側のディスプレイに表示される仮想リモコン３２１に含まれる［ツール］ボタンを操作すると、この操作情報がネットワークを介してネットワークチューナ２００のユーザインタフェース生成部３０１に入力される。この［ツール］ボタンの操作情報がＵＩ要求であるとする。ユーザインタフェース生成部３０１は、このＵＩ要求を受信に応じて、クライアントに対する表示情報（ユーザインタフェース）を生成して出力する。

【００９６】

この処理によって、例えば図１０に示すＵＩ情報３２３がクライアントのディスプレイに表示されることになる。クライアント側では、放送コンテンツと同様のパケット処理、すなわち、復号、再生処理を実行してＵＩ情報３２３を表示することができる。

【００９７】

なお、ユーザインタフェース（ＵＩ）生成部３０１に対するＵＩ生成のリクエストは、クライアント側の仮想リモコンの他、物理リモコンからの要求、ネットワークチューナ２００に付属する操作部からの入力によっても実行可能である。また、クライアント側からの要求態様としても仮想リモコンを利用した処理に限らず、例えばホームネットワーク仕様を規定したＵＰｎＰにおいてネットワーク機器間のメッセージ通信処理の１つとして定義されるＳＯＡＰ（Ｓｉｍｐｌｅ　Ｏｂｊｅｃｔ　Ａｃｃｅｓｓ　Ｐｒｏｔｏｃｏｌ）などを用いたクライアントからのメッセージをユーザインタフェース（ＵＩ）生成部３０１が入力して、この入力に基づいてＵＩを生成してクライアントに提供するといった処理を実行する構成としてもよい。あるいはクライアントに提示されるＷｅｂページを介する要求を受領して応答するという構成としてもよい。

【００９８】

本実施例の構成によれば、例えば以下のような効果を奏する、

１．ＵＩをサーバ（ネットワークチューナ）側とクライアント側の２箇所ではなく、サーバ（ネットワークチューナ）の１箇所で実装すれば良いため、実装工数が削減できる。

２．ＵＩをサーバ側だけで描画するため、物理リモコンと仮想リモコンの同期が容易になる。

３．ＵＩをサーバ側だけで描画するため、仮想リモコンが複数存在した時の同期が容易になる。

４．ＵＩのデザイン変更などを行う時にサーバのみをアップデートすれば良い。

５．ＵＩに不具合があったときにサーバのみをアップデートすれば良い。

【００９９】

［４．クライアントに対する番組情報提供処理構成］

次に、本発明に係る情報処理装置の第３の実施例について説明する。図１１を参照して本発明の第３の実施例に係る情報処理装置、すなわちネットワークチューナ２００の構成、処理について説明する。図１１に示すネットワークチューナ２００は、図２を参照して説明した第１実施例のネットワークチューナ２００の構成に、番組情報管理部５０１と、番組情報更新監視部５０２を追加した構成となっている。

【０１００】

放送波受信部２０１、暗号処理部２０２、データ蓄積部（バッファ）２０３、データ送受信部２０４、送信データ制御部２０５は、図１１では簡略化して示してあるが、先に図２～図７を参照して説明したと同様の構成であり、同様の処理を実行する。以下、番組情報管理部５０１と、番組情報更新監視部５０２の実行する処理の詳細について説明する。

【０１０１】

クライアントに対してコンテンツを提供するサーバであるネットワークチューナ２００は、放送コンテンツのみならず、放送コンテンツに対応する番組情報を、放送受信部２０１を介して受信する。この番組情報は番組情報管理部５０１において管理される。番組情報管理部５０１では、階層構成を有するコンテンツ管理ディレクトリによって番組情報の管理を行なう。番組情報管理部５０１は番組情報の管理処理を、ホームネットワーク仕様を規定したＵＰｎＰにおいて定義されているＣＤＳ（コンテンツディレクトリサービス）を適用して階層構成のディレクトリを用いて実行する。

【０１０２】

ＣＤＳ（コンテンツディレクトリサービス）を適用したデータ管理構成例について、図１２を参照して説明する。階層構成は図１２に示すように分岐ツリー状の図として示すことができる。この階層構成は、コンテンツ提供処理を実行するサーバとしてのネットワークチューナ２００の番組情報管理部５０１のアクセス可能な記憶部に格納された番組情報に対応する論理的な管理構成を示すものである。

【０１０３】

ルート（Ｒｏｏｔ）を頂点ノードとして、カレントチャンネル（ＣＣ）、地上デジタル、ＢＳデジタル、ＣＳデジタル等の下位ノードが設定され、さらに、その下位に各チャンネル対応の番組単位の番組情報のデータが設定されている。個々の番組情報データはアイ

テム（ｉｔｅｍ）と呼ばれる。アイテムの集合として規定されるアイテムの上位オブジェクトをコンテナ（Ｃｏｎｔａｉｎｅｒ）と呼ぶ。カレントチャンネルアイテムは、ネットワークチューナ２００が現在選局しているチャンネルに対応する番組情報である。

【０１０４】

例えばネットワークチューナ２００からネットワークを介して放送コンテンツを受信しているクライアント、例えば図１に示すクライアント２５１側において番組を視聴しているユーザがチャンネルを変更すると、ＣＤＳにおけるカレントチャンネルアイテムは変更され、この変更に応じてカレントチャンネルアイテムを含むコンテナの変更があったことの通知がクライアントに送信される。この処理は、ＵＰｎＰにおいて規定されるＧＥＮＡ（Ｇｅｎｅｒａｌ　Ｅｖｅｎｔ　Ｎｏｔｉｆｉｃａｔｉｏｎ　Ａｒｃｈｉｔｅｃｔｕｒｅ）に従った処理であり、通知情報は、ＧＥＮＡ　Ｎｏｔｉｆｙと呼ばれる。ＧＥＮＡはサーバクライアント間のメッセージ通信に関するアーキテクチャであり、クライアント側の要求の有無に関わらず、サーバ側で情報更新がなされたことをＧＥＮＡ　Ｎｏｔｉｆｙとしてクライアント側に自動的に通知する機能である。

【０１０５】

このようにクライアント側で視聴している番組のチャンネルが変更されると、ネットワークチューナ２００は、カレントチャンネルアイテムを含むコンテナの情報変更があったことをクライアント側にＧＥＮＡ　Ｎｏｔｉｆｙとして通知する処理を実行する。従って、ユーザが頻繁なチャンネル切り替えを行なうと、頻繁にサーバからクライアントに対してＧＥＮＡ　Ｎｏｔｉｆｙが送信されることになる。

【０１０６】

このように頻繁に送信される通知情報は、更新された番組情報に興味がないクライアントにとっては不要な情報に過ぎず、サーバおよびクライアントの負荷を発生させるのみであり、またネットワークにおける無駄な通信を発生させることにもなる。

【０１０７】

図１１に示す本発明の第３実施例に係る情報処理装置、すなわちネットワークチューナ２００は、このような無駄な通知処理をやめ、クライアントが情報を必要としていると判断される場合にのみ通知を行なうことを可能とした構成を持つ。

【０１０８】

クライアントにおいて、番組情報の閲覧（Ｂｒｏｗｓｅ）を行なう場合の処理について図１３を参照して説明する。例えばカレントチャンネルアイテムに対応する番組情報を取得する場合の処理について説明する。クライアント２５１は、ステップＳ１０１において、図に示す番組情報取得要求（ＢｒｏｗｓｅＤｉｒｅｃｔＣｈｉｌｄｒｅｎリクエスト）５２１をネットワークチューナ２００に対して送信する。

【０１０９】

ネットワークチューナ２００は、番組情報取得要求（ＢｒｏｗｓｅＤｉｒｅｃｔＣｈｉｌｄｒｅｎリクエスト）５２１を受信すると、ステップＳ１０２において、図に示すカレントチャンネルアイテムを含むコンテナに対応する番組情報５２２をクライアント２５１に送信し、クライアントは、番組情報５２２を表示部に出力して閲覧することが可能となる。なお、番組情報取得要求５２１、番組情報５２２は例えばＸＭＬデータであり、クライアントでは、ＸＭＬデータからなる番組情報５２２に基づいて表示データを生成してディスプレイに出力する。このように番組情報の提供処理は、クライアントからのブラウズ（Ｂｒｏｗｓｅ）要求に基づいて実行される。

【０１１０】

また、例えば前述したように、クライアント側のユーザが、選局しているチャンネルを変更すると、図１４に示すように、ネットワークチューナ２００では、図１２を参照して説明したカレントチャンネルアイテムの更新が行なわれ、さらに、この更新処理の発生に応じてネットワークチューナ２００は、クライアント２５１に対して情報変更や更新がなされたことの通知処理としてのＧＥＮＡ　Ｎｏｔｉｆｙの送信を実行する。例えば図１４に示すＧＥＮＡ　Ｎｏｔｉｆｙ５２３が送信される。

【０１１１】
本実施例に従ったネットワークチューナ２００は、図１２を参照して説明したＣＤＳによる管理構成である階層構成における各コンテナ（Ｃｏｎｔａｉｎｅｒ）の各々に対応させて、クライアントによるブラウズ（Ｂｒｏｗｓｅ）が実行されたか否かを示すフラグを保持する。すなわち、図１１に示すネットワークチューナ２００の番組情報管理部５０１が、各コンテナ（Ｃｏｎｔａｉｎｅｒ）に対して、クライアントによるブラウズ（Ｂｒｏｗｓｅ）が実行されたか否かを示すフラグを保持する。このフラグをＮｏｔｉｆｙフラグと呼ぶ。例えば、ネットワークチューナ２００の番組情報管理部５０１は、図１５に示すようなフラグ管理テーブルを保持し、以下のような状態変更に応じて、フラグを更新する。

【０１１２】
ネットワークチューナ２００における、Ｎｏｔｉｆｙフラグの更新は以下のように実行される。
（ａ）各コンテナ対応のフラグの初期状態は［０］にセットする。
（ｂ）コンテナに対する閲覧（Ｂｒｏｗｓｅ）要求をクライアントから受信した場合、そのコンテナ対応のフラグを［１］にセットする。
（ｃ１）フラグが［１］の時にそのコンテナに対応する情報（例えばアイテム）に変更が発生したらＧＥＮＡ　Ｎｏｔｉｆｙを送信し、そのコンテナ対応のフラグを［０］にセットする。
（ｃ２）フラグが［０］の時は、そのコンテナに対応する情報（例えばアイテム）に変更が発生してもＧＥＮＡ　Ｎｏｔｉｆｙを送信しない。

【０１１３】
なお、上述の図１３～図１５を参照して説明ではカレントチャンネルアイテムに対応する番組情報を取得する場合の処理例として、図１３に示すクライアント２５１からの番組情報取得要求（ＢｒｏｗｓｅＤｉｒｅｃｔＣｈｉｌｄｒｅｎリクエスト）を利用した処理例について説明したが、コンテナ対応のメタデータ、あるいはコンテナの下位にあるアイテム対応のメタデータに対する閲覧要求（ＢｒｏｗｓｅＭｅｔａｄａｔａ）についても閲覧処理が実行され、これらの閲覧処理が実行された場合に上記フラグのセットを行なう構成としてもよい。

【０１１４】
具体的な処理例について、図１６、図１７を参照して説明する。
まず、Ｎｏｔｉｆｙフラグの設定が［１］の場合の処理について、図１６を参照して説明する。

【０１１５】
図１６（Ａ１）は、Ｎｏｔｉｆｙフラグを［１］に設定する場合の処理である。ネットワークチューナ２００は、ステップＳ２０１において、任意のクライアント２５１からカレントチャンネル対応のコンテナ（Ｃｏｎｔａｉｎｅｒ）に対する閲覧要求であるブラウズ（ＢｒｏｗｓｅＤｉｒｅｃｔＣｈｉｌｄｒｅｎ）要求を受け取ると、ステップＳ２０２において、図１３を参照して説明した番組情報５２２をクライアント２５１に返す。さらに、ステップＳ２０３において、カレントチャンネルのコンテナ（Ｃｏｎｔａｉｎｅｒ）に対応するＮｏｔｉｆｙフラグを［１］にセットする。これらの処理は、図１１に示すネットワークチューナ２００の番組情報管理部５０１が実行する。

【０１１６】
図１６（Ａ２）は、Ｎｏｔｉｆｙフラグが［１］に設定されている場合の番組情報更新通知処理、すなわち、ＧＥＮＡ　Ｎｏｔｉｆｙを通知する際の処理を説明する図である。ネットワークチューナ２００の番組情報更新監視部５０２は、図１２を参照して説明したＣＤＳによる管理構成である階層構成における各コンテナ（Ｃｏｎｔａｉｎｅｒ）単位の情報更新の有無を監視している。ステップＳ２１１において、カレントチャンネルの情報に変更があったことが検知されると、この変更発生情報が、番組情報更新監視部５０２から番組情報管理部５０１に通知される。

【０１１７】
番組情報管理部５０１は、この情報変更の通知を受領するとステップＳ２１２において、変更のあったコンテナに対応するＮｏｔｉｆｙフラグをチェックする。この場合は、カレントチャンネル対応のコンテナに対応するＮｏｔｉｆｙフラグをチェックする。
【０１１８】
ここで示す例は、Ｎｏｔｉｆｙフラグ＝［１］の場合の例である。Ｎｏｔｉｆｙフラグが［１］になっているということは、いずれかのクライアントからカレントチャンネルコンテナに対する閲覧（Ｂｒｏｗｓｅ）要求を受け取ったことがあるということを示している。すなわち、図１６（Ａ１）のステップＳ２０１～Ｓ２０３の処理によって、Ｎｏｔｉｆｙフラグは［１］に設定されている。
【０１１９】
ステップＳ２１２において、ネットワークチューナ２００の番組情報管理部５０１は、カレントチャンネルコンテナに対応するＮｏｔｉｆｙフラグが［１］であることを確認すると、ステップＳ２１３において、情報更新通知であるＧＥＮＡ　Ｎｏｔｉｆｙをクライアント２５１に対して送信する。なお、ＧＥＮＡ　Ｎｏｔｉｆｙを送信する対象となるクライアントは、情報更新があった再にＧＥＮＡ　Ｎｏｔｉｆｙの受領を容認しているクライアント、すなわちＧＥＮＡ　Ｓｕｂｓｃｒｉｂｅをしている全てのクライアントである。すなわち、１つのクライアントからプラウズ（Ｂｒｏｗｓｅ）を受け、Ｎｏｔｉｆｙフラグが［１］に設定されている場合、ネットワークチューナ２００に接続されＧＥＮＡ　Ｓｕｂｓｃｒｉｂｅをしている全てのクライアントに対してＧＥＮＡ　Ｎｏｔｉｆｙが送信される。
【０１２０】
ネットワークチューナ２００の番組情報管理部５０１は、ＧＥＮＡ　Ｎｏｔｉｆｙの送信が完了すると、ステップＳ２１４において、Ｎｏｔｉｆｙフラグを［０］に戻す処理を実行する。
【０１２１】
次に、Ｎｏｔｉｆｙフラグの設定が［０］の場合の処理について、図１７を参照して説明する。図１７（Ｂ１）は、カレントチャンネルコンテナに対応するＮｏｔｉｆｙフラグが［０］に設定された状態を示している。
【０１２２】
図１７（Ｂ２）は、Ｎｏｔｉｆｙフラグが［０］に設定されている場合の番組情報更新通知処理、すなわち、ＧＥＮＡ　Ｎｏｔｉｆｙの通知中止処理を説明する図である。ネットワークチューナ２００の番組情報更新監視部５０２は、図１２を参照して説明したＣＤＳによる管理構成である階層構成における各コンテナ（Ｃｏｎｔａｉｎｅｒ）単位の情報更新の有無を監視している。ステップＳ３１１において、カレントチャンネルの情報に変更があったことが検知されると、この変更発生情報が、番組情報更新監視部５０２から番組情報管理部５０１に通知される。
【０１２３】
番組情報管理部５０１は、この情報変更の通知を受領するとステップＳ３１２において、変更のあったコンテナに対応するＮｏｔｉｆｙフラグをチェックする。この場合は、カレントチャンネル対応のコンテナに対応するＮｏｔｉｆｙフラグをチェックする。
【０１２４】
ここで示す例は、Ｎｏｔｉｆｙフラグ＝［０］の場合の例である。Ｎｏｔｉｆｙフラグが［０］になっているということは、いずれのクライアントからもカレントチャンネルコンテナに対する閲覧（Ｂｒｏｗｓｅ）要求を受け取っていないことを示している。例えば、図１６（Ａ２）において説明したＧＥＮＡ　Ｎｏｔｉｆｙの通知後、クライアントからのブラウズ要求が発生していないことを示している
【０１２５】
ステップＳ３１２において、ネットワークチューナ２００の番組情報管理部５０１は、カレントチャンネルコンテナに対応するＮｏｔｉｆｙフラグが［０］であることを確認す

ると、ステップＳ３１３において、情報更新通知であるＧＥＮＡ　Ｎｏｔｉｆｙのクライアント２５１に対する送信処理を中止する。

【０１２６】

このように、本実施例におけるネットワークチューナ２００は、ＣＤＳの管理する番組情報ディレクトリの各コンテナに対応するクライアントのブラウズの有無を示すＮｏｔｉｆｙフラグを設定して、このＮｏｔｉｆｙフラグの設定値に応じて番組情報の更新通知を実行するか否かを決定する処理を行なう。

【０１２７】

すなわち、クライアントがコンテナに対応する情報変更の発生後に一度も更新された番組情報の閲覧（ブラウズ）を実行していない場合は、それ以後の番組情報の更新通知としてのＧＥＮＡ　Ｎｏｔｉｆｙを送信しない。この処理によって、クライアントに不要なＧＥＮＡ　Ｎｏｔｉｆｙの送信を防止することが可能になる。

【０１２８】

なお、上述した実施例では、ブラウズの有無を示すＮｏｔｉｆｙフラグを各コンテナに対応して設定した例を説明したが、例えば、ネットワーク接続されたクライアントについても識別して、コンテナおよびクライアントごとにＮｏｔｉｆｙフラグを設定する構成としてもよい。すなわち、図１８に示すようなフラグ管理テーブルを保持し、各クライアントからのブラウズ要求の有無に応じて、フラグを更新する。

【０１２９】

上述した実施例では、任意のクライアントが番組情報の閲覧（Ｂｒｏｗｓｅ）要求を実施してきた場合、その後に発生した番組情報の変更通知としてのＧＥＮＡ　Ｎｏｔｉｆｙは所定の条件を満たす全クライアント、すなわちＳＵＢＳＣＲＩＢＥしているクライアントすべてに送信する構成としていた。この場合、ＧＥＮＡ　Ｎｏｔｉｆｙが実際には必要でないクライアントに対しても通知が送信されてしまうという問題がある。

【０１３０】

しかし、図１８に示すようなクライアントの各々に対応するブラウズの有無を示すＮｏｔｉｆｙフラグを設定することで、クライアントごとにＧＥＮＡ　Ｎｏｔｉｆｙの送信の有無を判定して各クライアントに対応する最適な制御が可能となる。

【０１３１】

また、Ｎｏｔｉｆｙフラグは、各コンテナ対応とする設定例の他、図１２に示すＣＤＳツリーに対して１つのフラグを設定する構成としてもよい。すなわちコンテナ毎に区別を行なわない設定である。この場合、ＣＤＳツリーのいずれかのコンテナに対する閲覧（Ｂｒｏｗｓｅ）要求が発生すると、Ｎｏｔｉｆｙフラグは［１］に設定され、ＣＤＳツリーに含まれる情報のいずれかに変更が発生してクライアントに対するＧＥＮＡ　Ｎｏｔｉｆｙが送信された場合は、Ｎｏｔｉｆｙフラグを［０］に戻す処理を実行する構成とする。

【０１３２】

なお、例外的な処理として、特定のクライアントに対しては、Ｎｏｔｉｆｙフラグに関わらずＧＥＮＡ　Ｎｏｔｉｆｙをすべて送信するといった処理も可能である。この場合は、図１８に示すフラグ管理テーブルの特定クライアントに対するフラグの値を［１］に固定することで実行可能である。このような設定を要求しようとするクライアントは、例えば、ＧＥＮＡの設定に際して実行するＧＥＮＡ　ＳＵＢＳＣＲＩＢＥ時にこの例外設定を示す情報を付加（例えばＧＥＮＡ　ＳＵＢＳＣＲＩＢＥのＨＴＴＰヘッダに付加）してネットワークチューナに出力し、ネットワークチューナにおいて例外要求の有無を判別して処理を実行する。

【０１３３】

また、コンテナによっては、Ｎｏｔｉｆｙフラグの値に関わらずすべてＧＥＮＡ　Ｎｏｔｉｆｙを送信するといった設定としてもよい。すなわち、あるコンテナについては、Ｎｏｔｉｆｙフラグの値に関わらず、変更が発生したときに必ずＧＥＮＡ　Ｎｏｔｉｆｙをクライアントに送信する。この処理も例えば、図１５、あるいは図１８に示すフラグ管理テーブルのフラグの設定値を［１］に固定することで実行可能である。なお、このような

例外コンテナは、あらかじめ決定したものとしてもよいし、ＳＵＢＳＣＲＩＢＥ時にクライアントが選択できる設定としても良い。クライアント毎に設定を変更してもよい。この処理は、図１８に示すフラグ管理テーブルのフラグの設定値を［１］に固定するエントリを変更することで実現可能である。

【０１３４】

上述したように本実施例に従ったネットワークチューナは、ＣＤＳの管理する番組情報ディレクトリのコンテナやクライアントに対応してＮｏｔｉｆｙフラグを設定して、Ｎｏｔｉｆｙフラグの設定値に応じて番組情報の更新通知を実行するので、無駄な番組情報の変更通知としてのＧＥＮＡ　Ｎｏｔｉｆｙが送信されなくなるため、

（ア）　クライアントのネットワーク処理負荷が軽減する。

（イ）　サーバのネットワーク処理負荷が軽減する。

（ウ）　ネットワークに無駄なパケットが流れなくなり、ネットワーク帯域の無駄遣いがなくなる。

という効果をもたらす。

【０１３５】

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、特許請求の範囲の欄を参酌すべきである。

【０１３６】

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。

【０１３７】

例えば、プログラムは記録媒体としてのハードディスクやＲＯＭ（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。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エアとして提供することができる。

【０１３８】

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録媒体にインストールすることができる。

【０１３９】

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。また、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。

【産業上の利用可能性】

【０１４０】

以上、説明したように、本発明の一実施例の構成によれば、ネットワーク接続されたクライアントに対して放送コンテンテを提供する情報処理装置（ネットワークチューナ）において、放送データを含む送信データを蓄積するバッファを監視し、バッファにおけるデ

ータの滞留状態、例えば、データ滞留時間を監視し、予め定めた許容滞留時間を越えたデータを送信データから排除する処理を実行する。本構成により、例えばクライアントからの再送要求などに起因して発生するデータの送信遅延が継続して維持されるという問題や、あるいは遅延が蓄積するなどの問題が解消され、放送コンテンツのリアルタイムでの送信や、クライアントからのチャンネル変更等の処理要求に対する応答性も向上させることが可能となる。

【図面の簡単な説明】

【０１４１】

【図１】本発明の情報処理装置の適用可能なネットワーク環境について説明する図である。

【図２】ネットワークチューナの第１実施例の構成例について説明する図である。

【図３】ネットワークチューナの暗号処理部が生成するＰＣＰの構成例について説明する図である。

【図４】ネットワークチューナの実行する送信データの破棄処理の具体例について説明する図である。

【図５】データ滞留時間監視部における各ＰＣＰのデータ蓄積部（バッファ）における滞留時間の算出処理例について説明する図である。

【図６】ＰＣＰのデータサイズとＰＣＰ単位のデータ破棄について説明する図である。

【図７】ＰＣＰのデータサイズとＰＣＰ単位のデータ破棄について説明する図である。

【図８】ユーザインタフェース（ＵＩ）の提供処理を行なうネットワークチューナの構成例について説明する図である。

【図９】クライアント側のディスプレイに出力される表示情報の例を示す図である。

【図１０】クライアント側のディスプレイに出力されるＵＩ情報の例を示す図である。

【図１１】クライアントに対する番組情報提供処理をじっこうするネットワークチューナの構成例について説明する図である。

【図１２】ＣＤＳ（コンテンツディレクトリサービス）を適用したデータ管理構成例について説明する図である。

【図１３】クライアントにおいて、番組情報の閲覧（Ｂｒｏｗｓｅ）を行なう場合の処理について説明する図である。

【図１４】クライアント側のユーザが、選局しているチャンネルを変更した場合の変更情報発生通知（ＧＥＮＡ　Ｎｏｔｉｆｙ）処理について説明する図である。

【図１５】ネットワークチューナの番組情報管理部が保持するフラグ管理テーブルの構成例について説明する図である。

【図１６】Ｎｏｔｉｆｙフラグの設定が［１］の場合のネットワークチューナの実行する処理について説明する図である。

【図１７】Ｎｏｔｉｆｙフラグの設定が［０］の場合のネットワークチューナの実行する処理について説明する図である。

【図１８】ネットワークチューナの番組情報管理部が保持するフラグ管理テーブルの構成例について説明する図である。

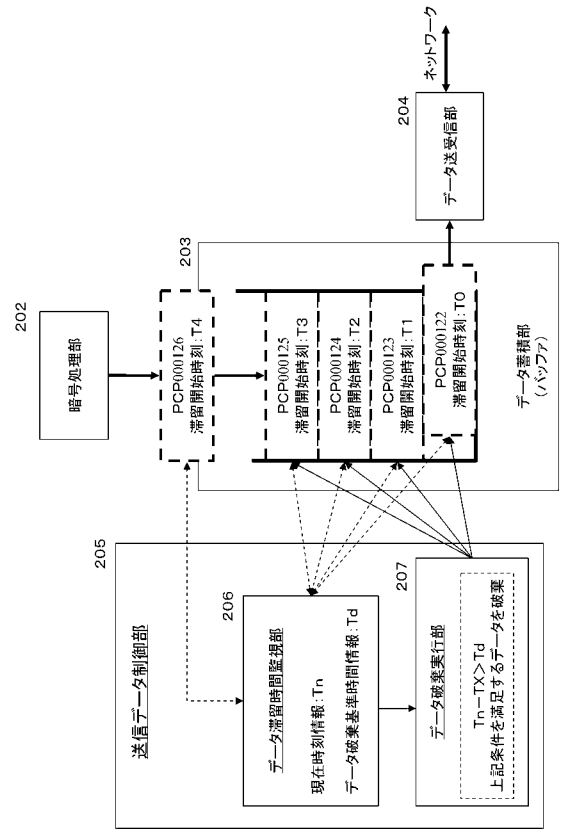
【符号の説明】

【０１４２】

１２１，１２２　アンテナ
１５０　ネットワーク
２００　ネットワークチューナ
２５１，２５２　クライアント
２０１　放送受信部
２０２　暗号処理部
２０３　データ蓄積部（バッファ）
２０４　データ送受信部
２０５　送信データ制御部

２０６　データ滞留時間監視部
２０７　データ破棄実行部
２７１，２７２，２７３　ＰＣＰ（Ｐｒｏｔｅｃｔｅｄ　Ｃｏｎｔｅｎｔ　Ｐａｃｋｅｔ）
２８１，２８２，２８３　ＰＣＰ（Ｐｒｏｔｅｃｔｅｄ　Ｃｏｎｔｅｎｔ　Ｐａｃｋｅｔ）
２９１，２９２　ＴＴＳ（Ｔｉｍｅｓｔａｍｐｅｄ　Ｔｒａｎｓｐｏｒｔ　Ｓｔｒｅａｍ）
３０１　ユーザインタフェース（ＵＩ）生成部
３０２　リモコン信号受信部
３２１　仮想リモコン
３２２　放送コンテンツ表示データ
３２３　ＵＩ情報
５０１　番組情報管理部
５０２　番組情報更新監視部
５２２　番組情報
５２３　ＧＥＮＡ　Ｎｏｔｉｆｙ

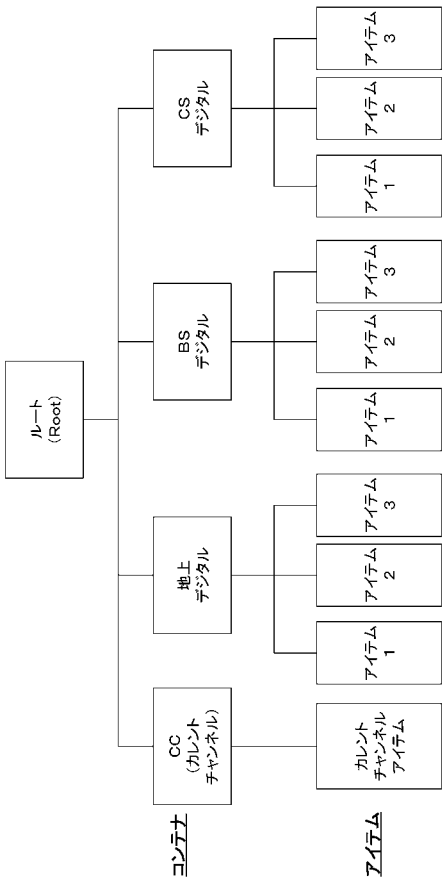
【図４】



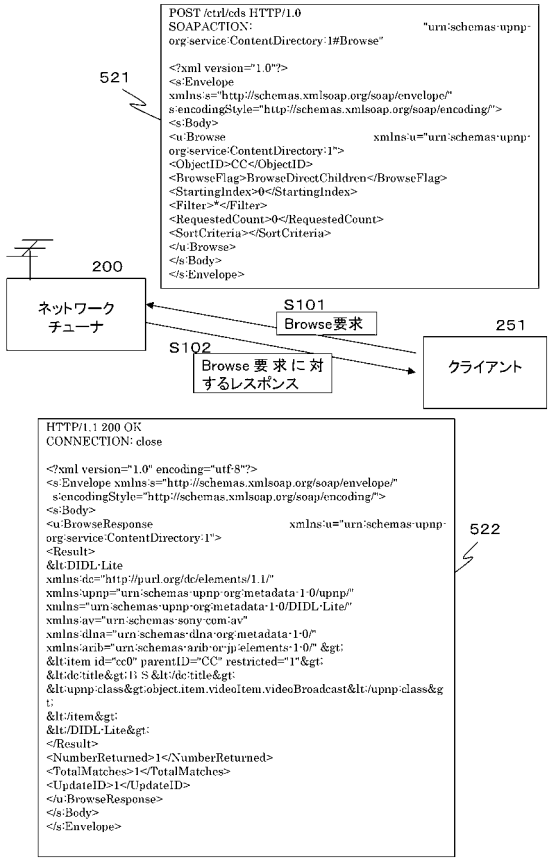
【図５】

PCP−ID	PCP入力時刻 [Tx]	滞留時間 [現在時刻(Tn)−入力時刻(Tx)]
PCP000120	10:10:23.33	0:51
PCP000121	10:10:23.52	0:42
PCP000122	10:10:24.06	0:34
PCP000123	10:10:24.12	0:28
：	：	：

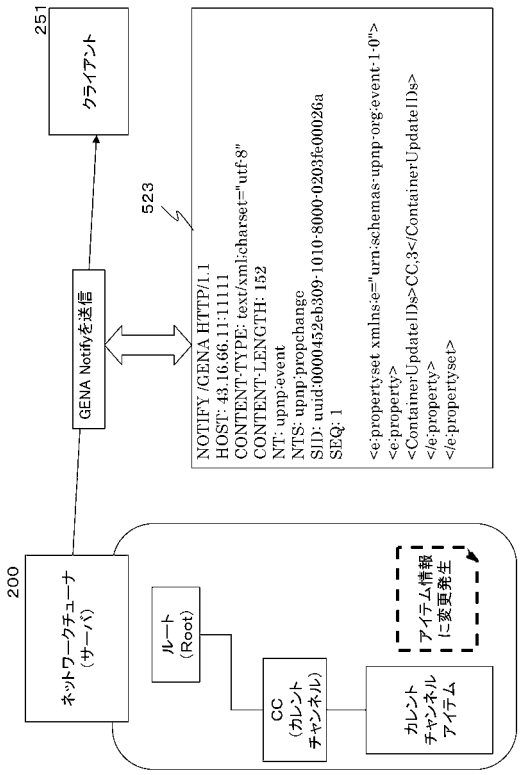
【図１２】



【図１３】



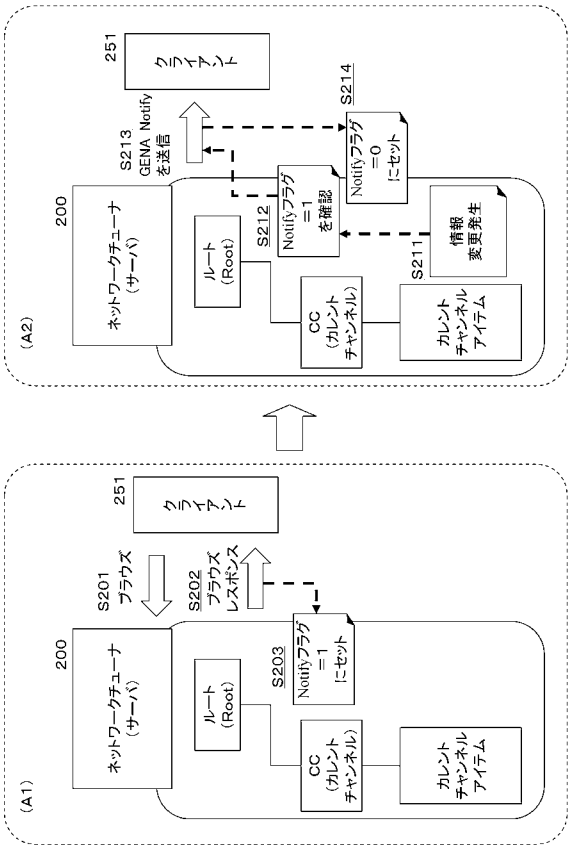
【図１４】



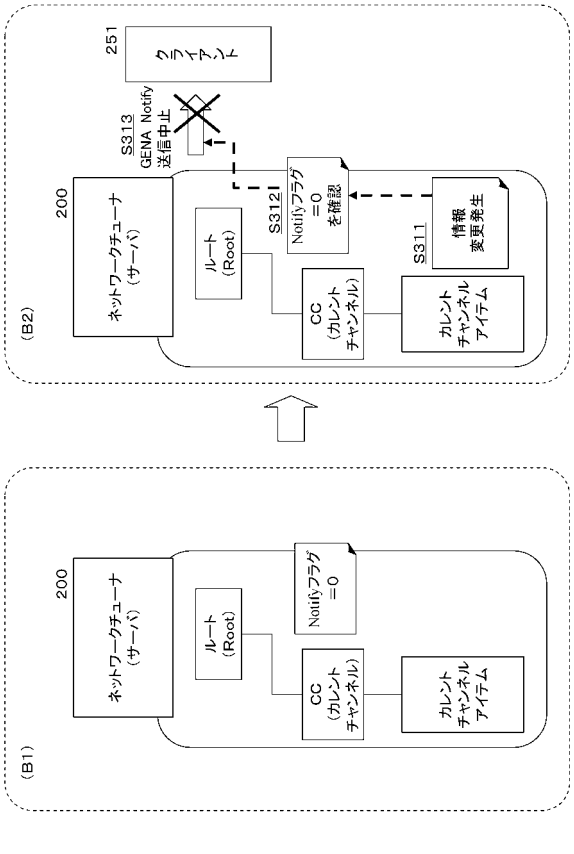
【図１５】

コンテナ	Notifyフラグ
CC (カレント チャンネル)	1
地上 デジタル	0
BS デジタル	0
CS デジタル	1

【図１６】



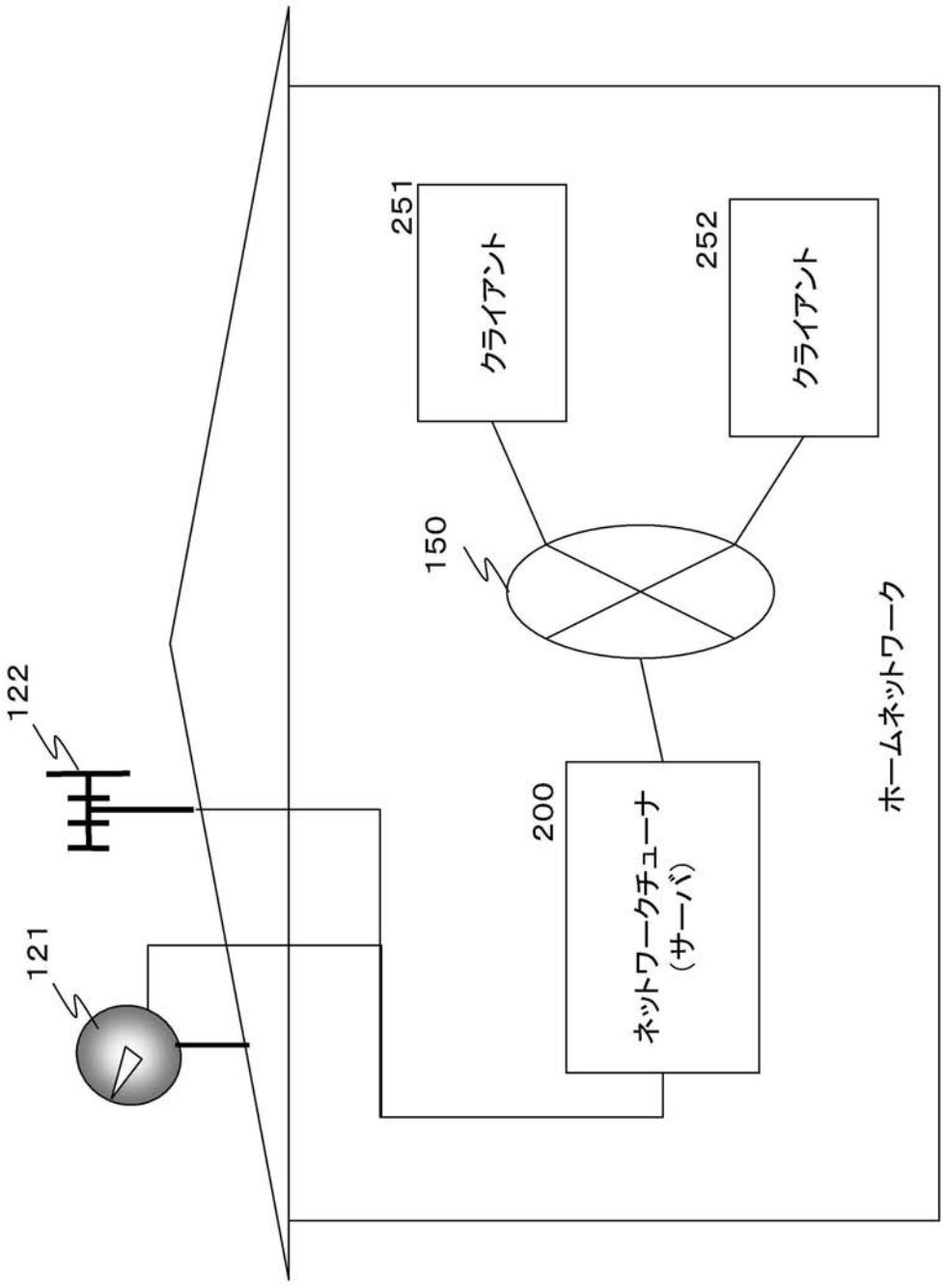
【図１７】



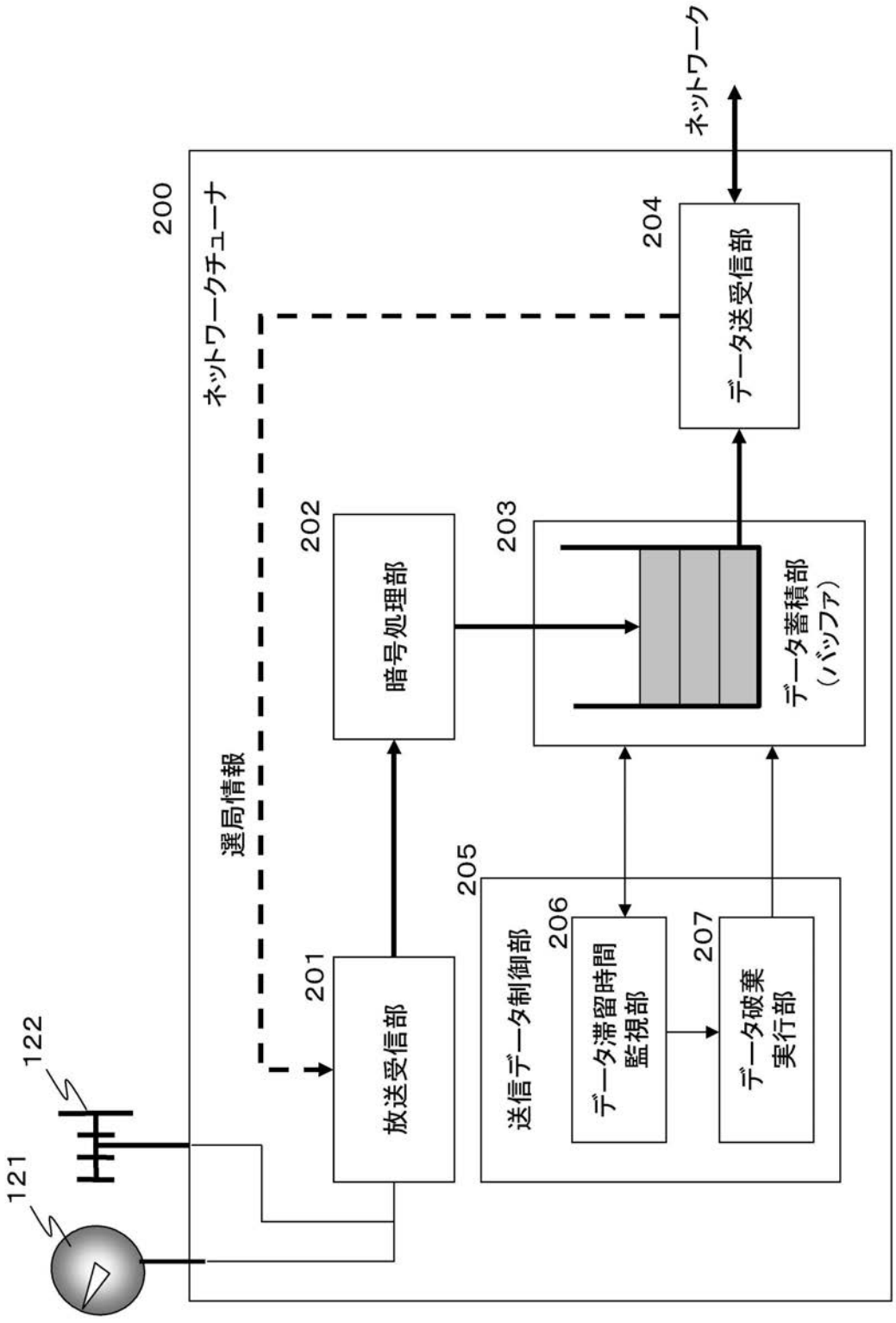
【図１８】

コンテナ	クライアント	Notifyフラグ
CC（カレントチャンネル）	クライアントA	1
	クライアントB	0
	クライアントC	0
BSデジタル	クライアントA	1
	クライアントB	1
	クライアントC	0
地上デジタル	クライアントA	0
	クライアントB	0
	クライアントC	0
：	：	：

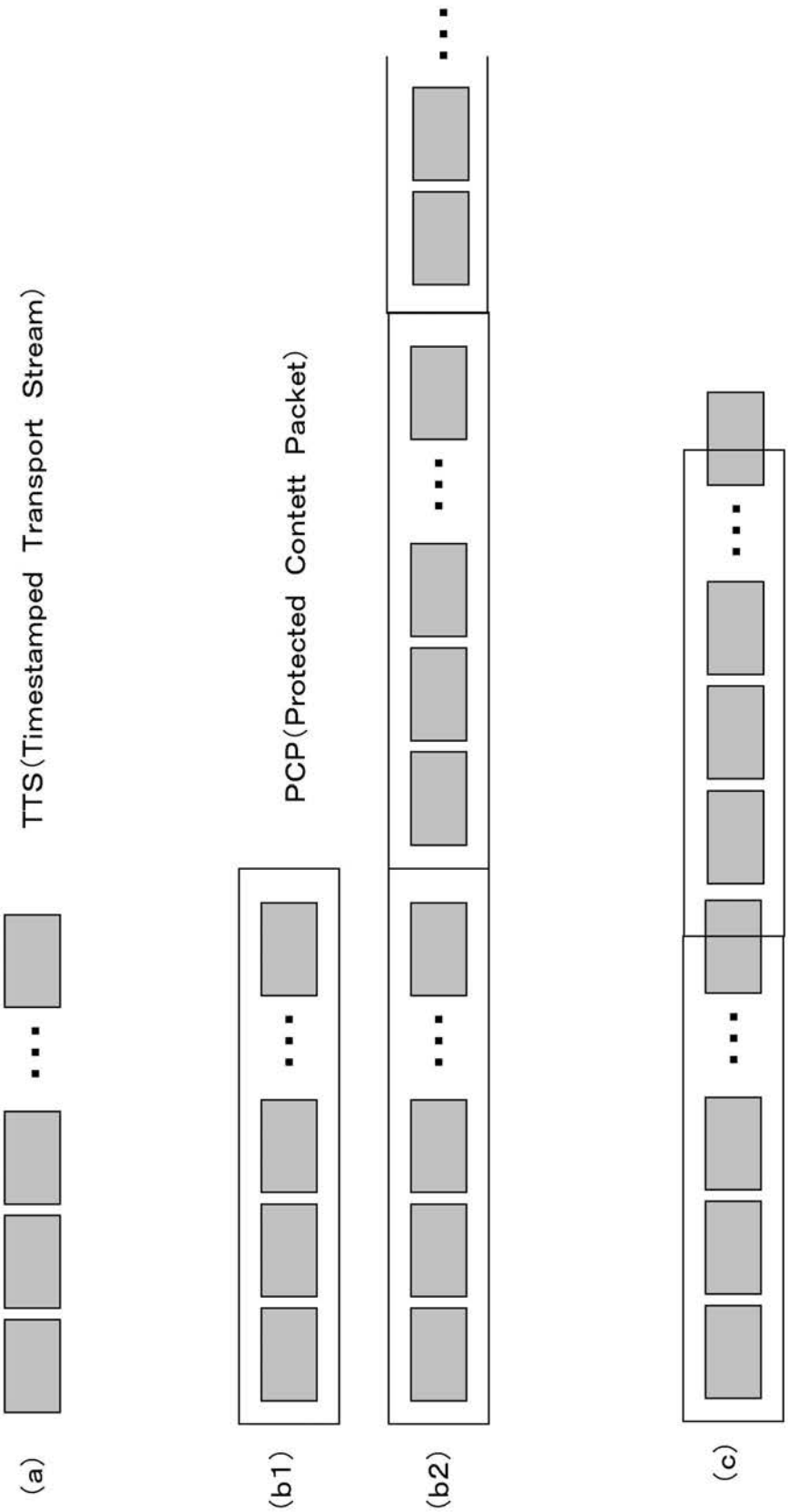
【図１】


121
122
150
200
ネットワークチューナ
(サーバ)
251
クライアント
252
クライアント
ホームネットワーク

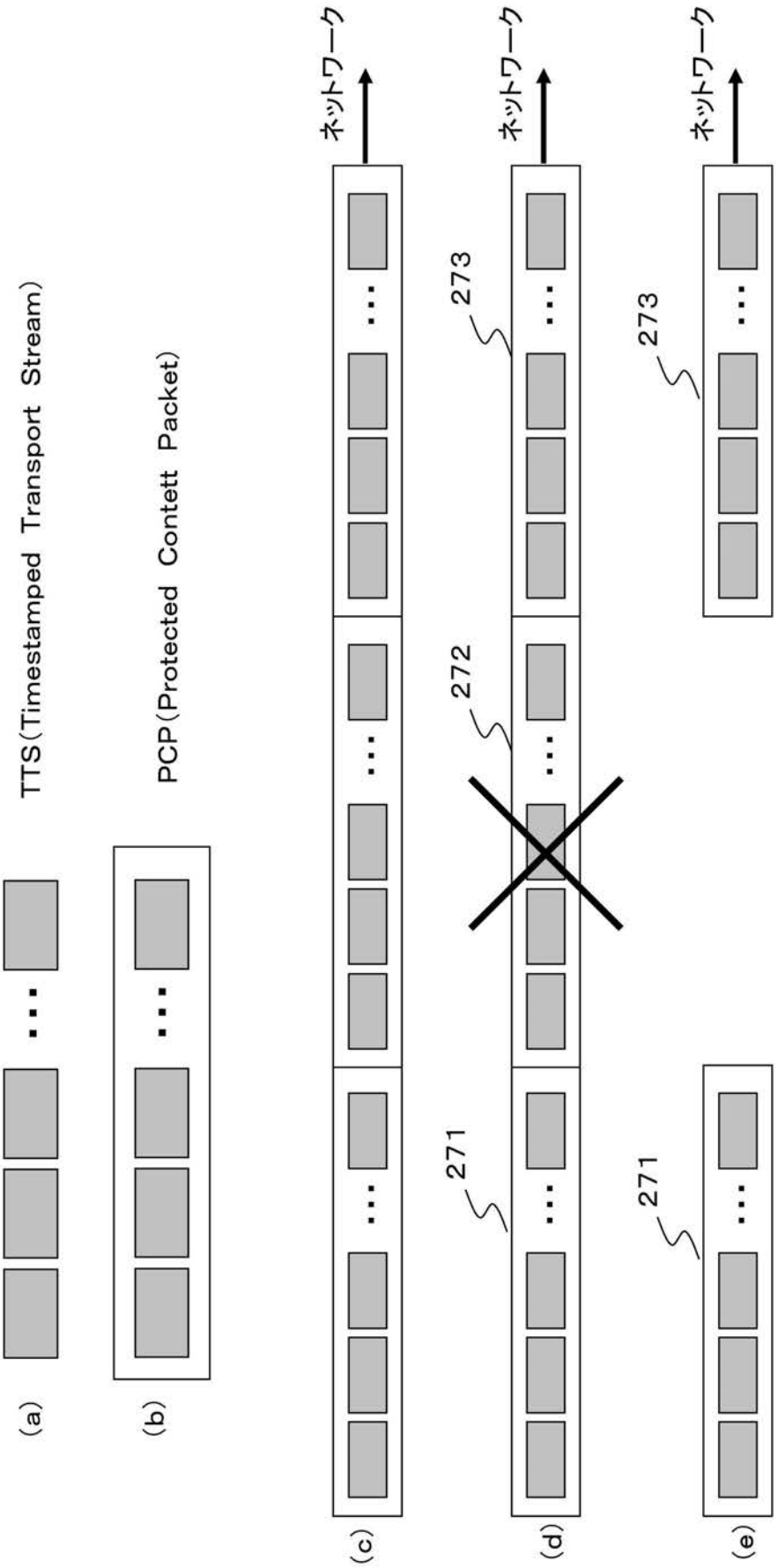
【図２】


ネットワーク
200
ネットワークチューナ
204
データ送受信部
202
暗号処理部
203
データ蓄積部
（バッファ）
選局情報
205
送信データ制御部
206
データ滞留時間
監視部
207
データ破棄
実行部
201
放送受信部
122
121

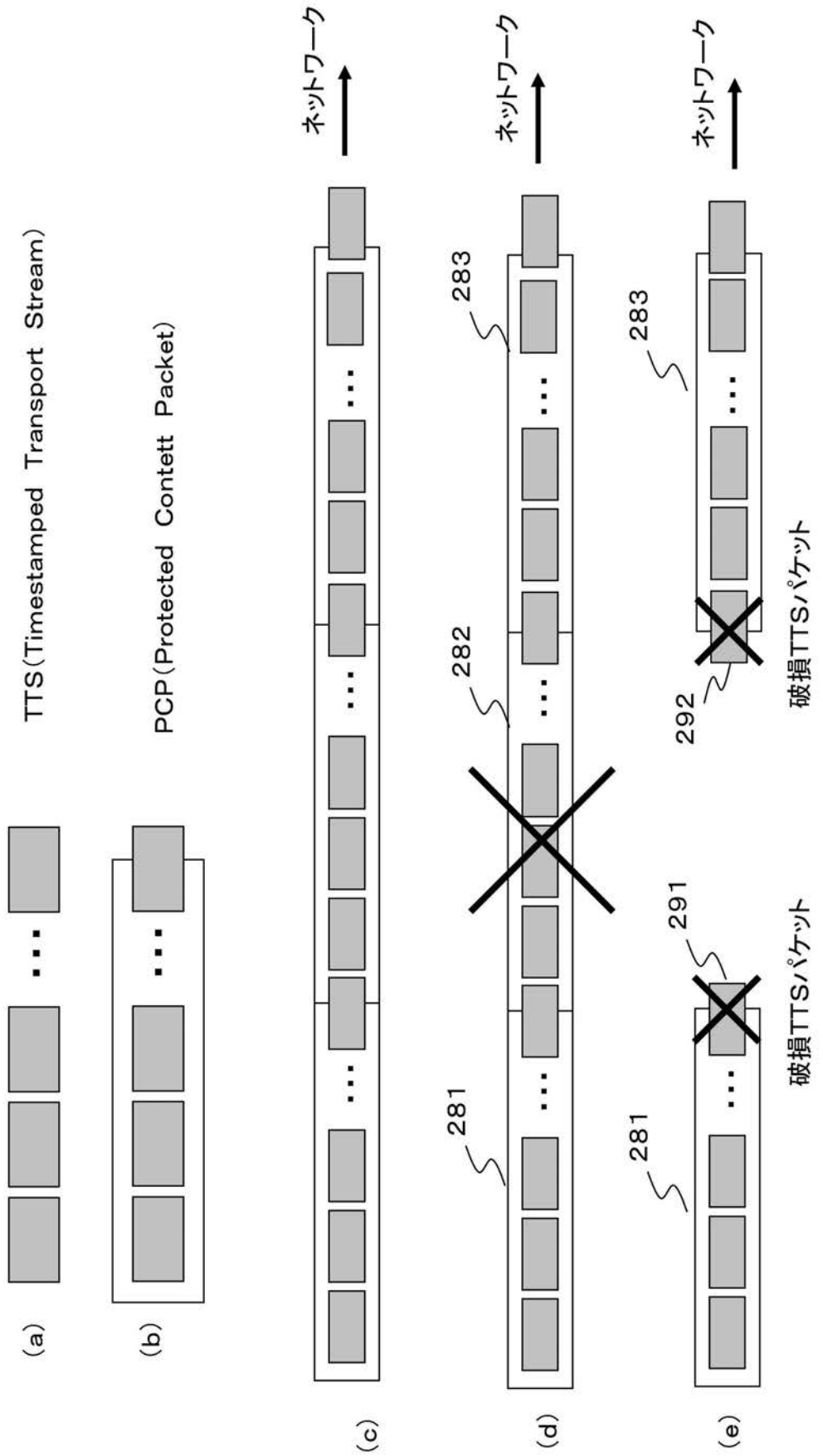
【図３】


TTS(Timestamped Transport Stream)
PCP(Protected Contett Packet)
(a)
(b1)
(b2)
(c)

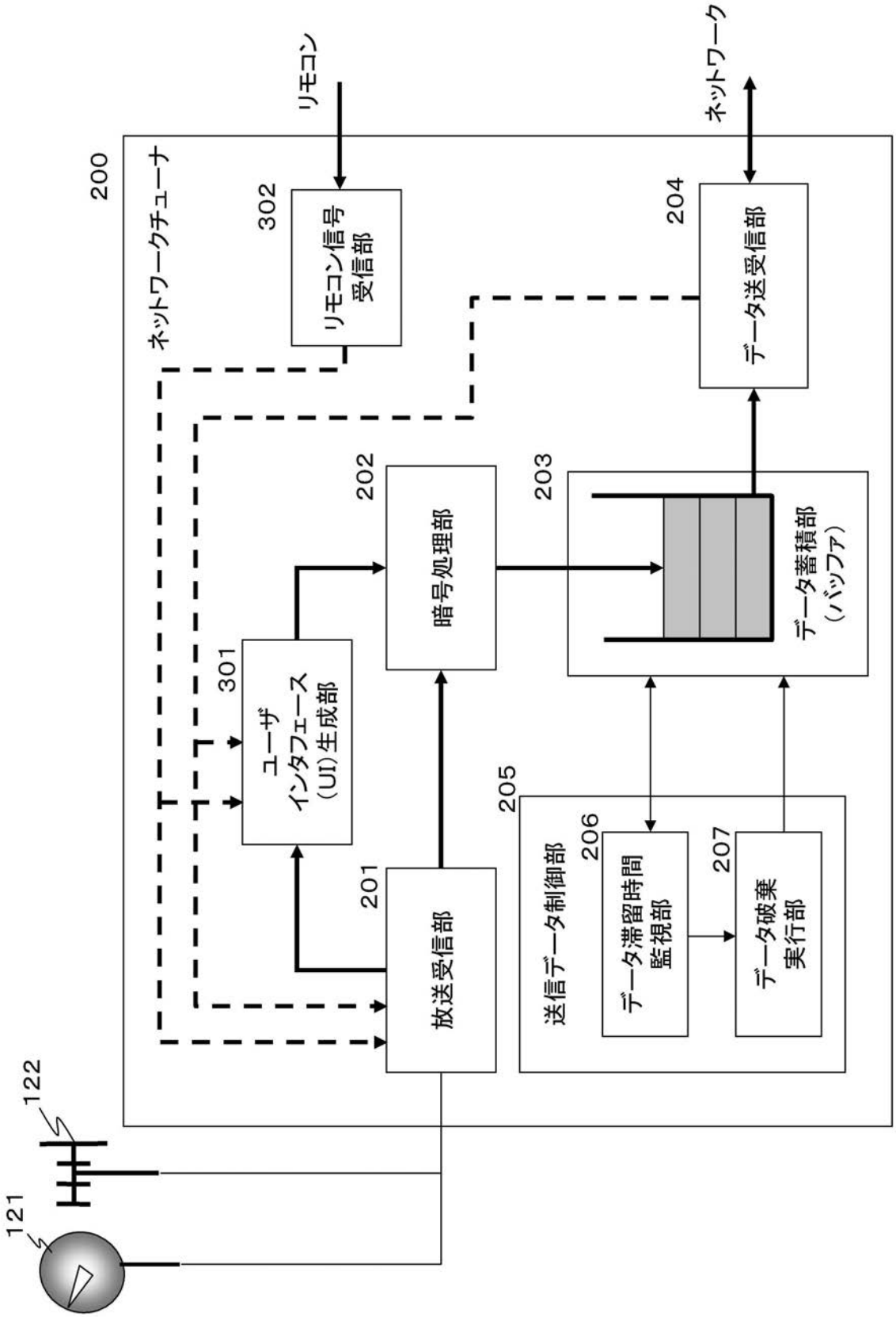
【図６】


TTS(Timestamped Transport Stream)
PCP(Protected Contett Packet)
(a)
(b)
(c)
(d)
(e)
ネットワーク
ネットワーク
ネットワーク
271
272
273
271
273
271

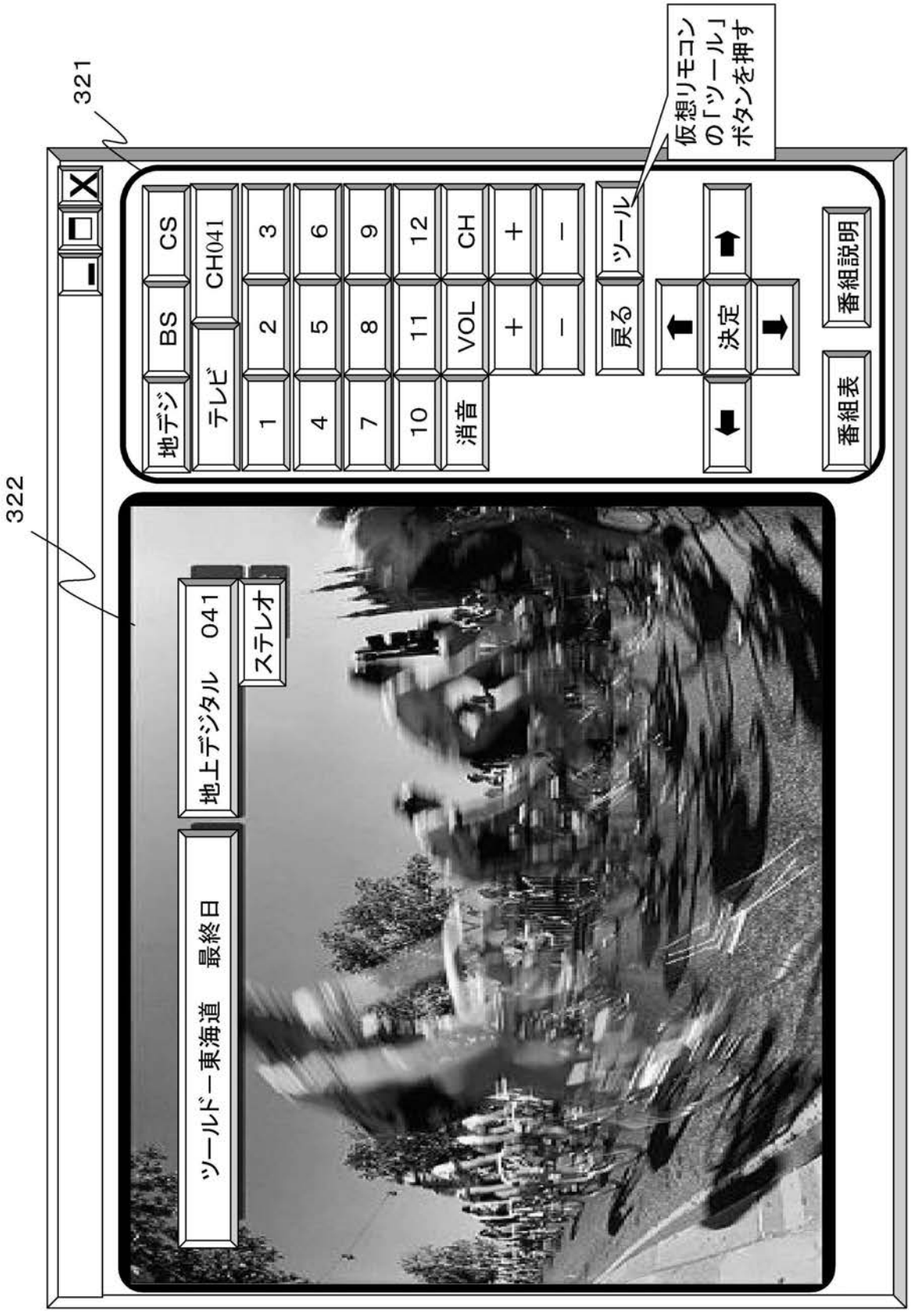
【図７】


TTS(Timestamped Transport Stream)
PCP(Protected Contett Packet)
(a)
(b)
(c)
(d)
(e)
ネットワーク
ネットワーク
ネットワーク
281
282
283
281
283
291
292
破損TTSパケット
破損TTSパケット

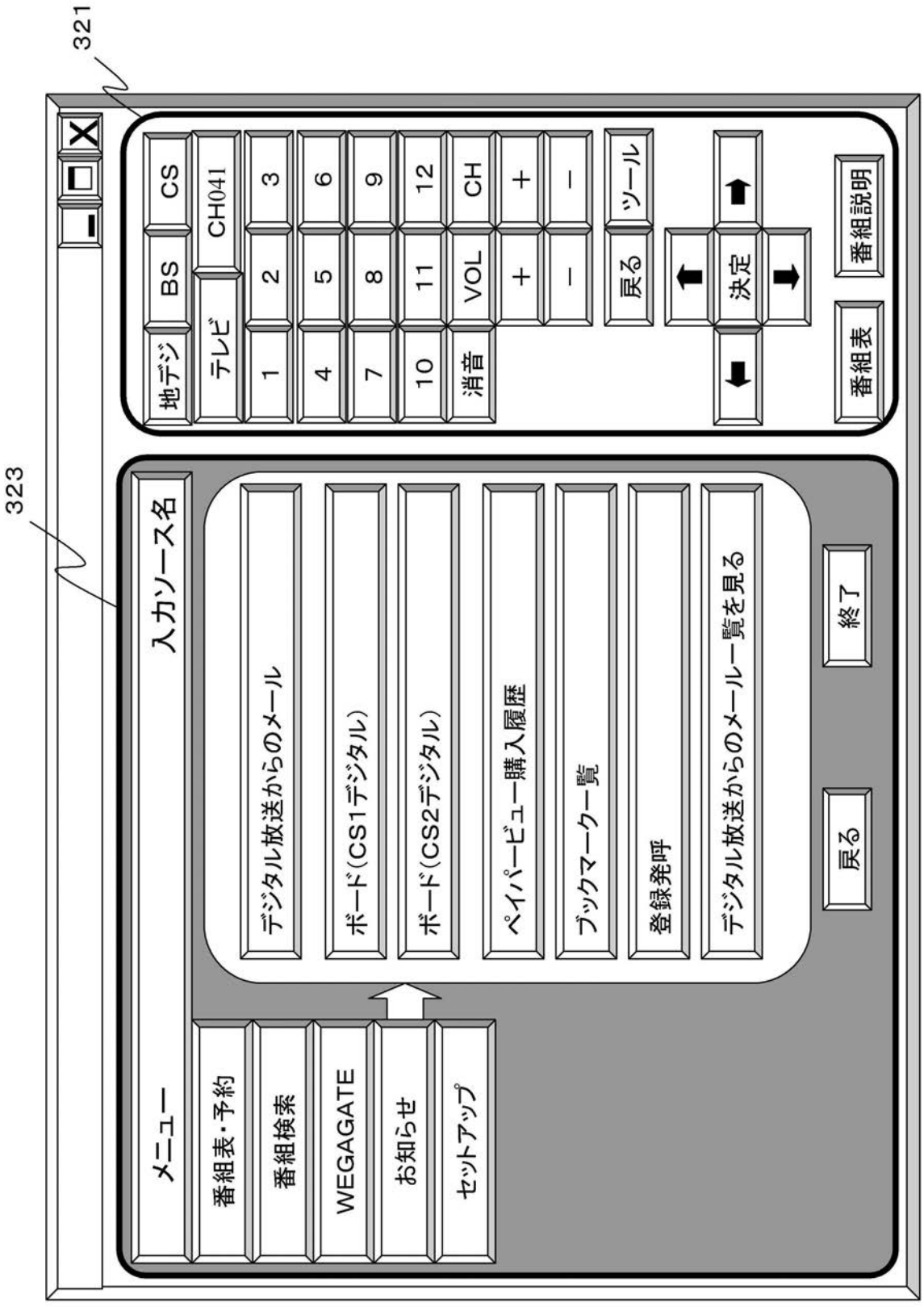
【図８】


200
ネットワークチューナ
リモコン
302
リモコン信号
受信部
ネットワーク
204
データ送受信部
202
暗号処理部
203
データ蓄積部
（バッファ）
301
ユーザ
インタフェース
（UI）生成部
205
送信データ制御部
206
データ滞留時間
監視部
207
データ破棄
実行部
201
放送受信部
122
121

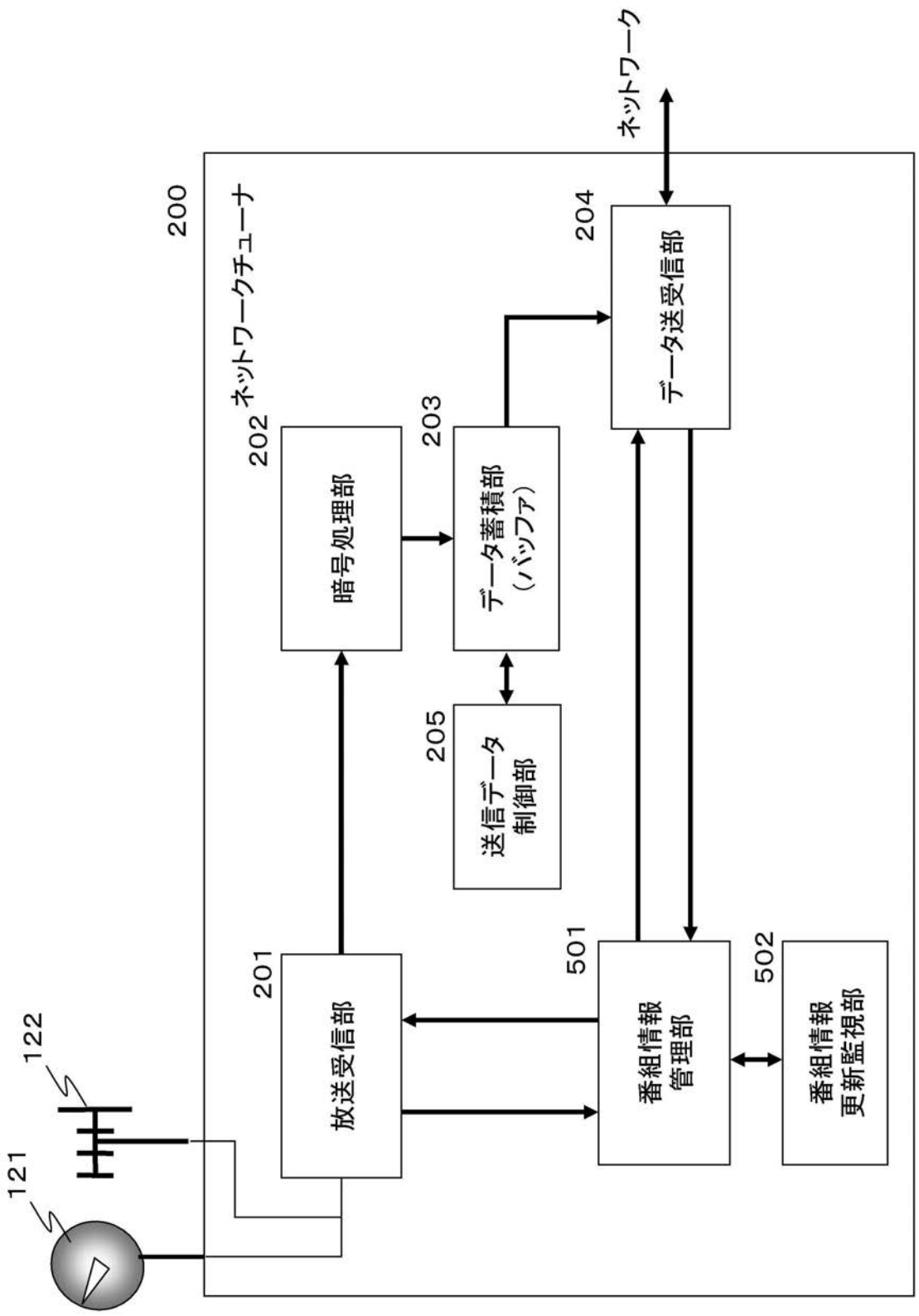
【図９】


321
322
仮想リモコンの「ツール」ボタンを押す
地デジ
BS
CS
テレビ
CH041
1
2
3
4
5
6
7
8
9
10
11
12
消音
VOL
CH
+
−
+
−
ツール
戻る
決定
番組表
番組説明
ツールド一東海道　最終日
地上デジタル　041
ステレオ

【図１０】


321
323
入力ソース名
メニュー
番組表・予約
番組検索
WEGAGATE
お知らせ
セットアップ
デジタル放送からのメール
ボード(CS1デジタル)
ボード(CS2デジタル)
ペイパービュー購入履歴
ブックマーク一覧
登録発呼
デジタル放送からのメール一覧を見る
戻る
終了
地デジ
BS
CS
テレビ
CH041
1
2
3
4
5
6
7
8
9
10
11
12
消音
VOL
CH
+
+
−
−
戻る
ツール
決定
番組表
番組説明

【図１１】


ネットワーク
200
ネットワークチューナ
204
データ送受信部
202
暗号処理部
203
データ蓄積部
（バッファ）
205
送信データ
制御部
201
放送受信部
501
番組情報
管理部
502
番組情報
更新監視部
122
121

フロントページの続き

(72)発明者　見山　成志
東京都港区港南１丁目７番１号　ソニー株式会社内
(72)発明者　尾上　淳
東京都港区港南１丁目７番１号　ソニー株式会社内

審査官　梅岡　信幸

(56)参考文献　特開２００６－０１９９５４（ＪＰ，Ａ）
特開２００５－０５１７０９（ＪＰ，Ａ）
特開２００６－３５２３１２（ＪＰ，Ａ）
特開２００５－１９０３５０（ＪＰ，Ａ）
特開２００６－１８６５８０（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｎ　　７／１４－　７／１７３
Ｈ０４Ｌ　　１２／００－１２／６６