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

特許第6350514号
(P6350514)

(45)発行日　平成30年7月4日(2018.7.4)　(24)登録日　平成30年6月15日(2018.6.15)

(51)Int.Cl.		F I		
H04L 9/08	(2006.01)	H04L	9/00	601C
G09C 1/00	(2006.01)	G09C	1/00	660D
G06F 21/10	(2013.01)	H04L	9/00	601E
G06F 21/62	(2013.01)	G06F	21/10	
G06F 21/44	(2013.01)	G06F	21/62	309

請求項の数 6　(全 42 頁)　最終頁に続く

(21)出願番号　特願2015-504195(P2015-504195)
(86)(22)出願日　平成26年1月20日(2014.1.20)
(86)国際出願番号　PCT/JP2014/051014
(87)国際公開番号　WO2014/136480
(87)国際公開日　平成26年9月12日(2014.9.12)
審査請求日　平成28年12月2日(2016.12.2)
(31)優先権主張番号　特願2013-47006(P2013-47006)
(32)優先日　平成25年3月8日(2013.3.8)
(33)優先権主張国　日本国(JP)

前置審査

(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　100095496
弁理士　佐々木　榮二
(74)代理人　100086531
弁理士　澤田　俊夫
(74)代理人　110000763
特許業務法人大同特許事務所

最終頁に続く

(54)【発明の名称】通信装置

(57)【特許請求の範囲】
【請求項１】
端末に提供するコンテンツを取得するコンテンツ取得部と、
ホーム・ネットワーク内で、コンテンツをリモート・アクセスにより提供する端末を、コマンドの往復時遅延時間に関する制限を課した第１の相互認証手続きを経て、第１の所定台数まで登録し、前記登録の日時及び所定の有効期間に基づく有効期限を、前記登録される端末の情報とともに管理する端末登録部と、
前記端末登録部に登録された端末からのリモート・アクセスによるコンテンツの要求に対し、コマンドの往復遅延時間に関する制限を課さない第２の相互認証手続きを通じて前記有効期限の下で第２の所定台数まで配信可能なリモート・アクセス用交換鍵に基づく暗号化コンテンツを提供し、前記有効期限を経過した端末へのコンテンツの提供を制限するコンテンツ提供部と、
を具備する通信装置。
【請求項２】
所定の相互認証及び鍵交換手続きに従って端末を認証するとともに交換鍵を共有する認証部をさらに備え、
前記認証部は、コンテンツをリモート・アクセスにより提供する端末を前記端末登録部に登録する際には前記第１の相互認証手続きを実施し、前記端末登録部に登録された端末がリモート・アクセスによるコンテンツを要求してきたときには前記第２の相互認証手続きを実施して前記アクセス期限制限下で第２の所定台数までリモート・アクセス用交換鍵

を生成し、
前記コンテンツ提供部は、前記認証部が生成した前記リモート・アクセス用交換鍵を用いて暗号化したコンテンツを端末に提供する、
請求項１に記載の通信装置。
【請求項３】
前記認証部は、ＤＴＣＰ－ＩＰが規定する認証及び鍵交換（ＡＫＥ）アルゴリズムに従って、端末と相互認証並びに交換鍵の共有を行ない、
前記端末登録部は、ＤＴＣＰ－ＩＰが規定する手続きに従って端末の登録を行なう、
請求項２に記載の通信装置。
【請求項４】
前記端末登録部は、端末との間で通信遅延時間の測定処理を行ない、通信遅延時間が所定の範囲内であれば、前記認証部で相互認証並びに交換鍵の共有を行なった後、前記端末を登録し、
前記コンテンツ提供部は、前記端末が前記端末登録部に登録されていれば、前記端末との間で通信遅延時間の測定処理を行なうことなく、前記認証部で相互認証並びに交換鍵の共有を行なった後、前記暗号化したコンテンツを端末に提供する、
請求項２又は３のいずれかに記載の通信装置。
【請求項５】
前記コンテンツ提供部は、前記端末登録部に登録される第３の所定台数の端末については、登録日時に基づく制限を免除して、コンテンツを提供する、
請求項１に記載の通信装置。
【請求項６】
前記第２の所定台数は、前記第１の所定台数より少なく設定される、
請求項１に記載の通信装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本明細書で開示する技術は、例えばＤＴＣＰなどの所定の相互認証及び鍵交換（ＡＫＥ）アルゴリズムに従って共有した鍵を用いてコンテンツを暗号化伝送する通信装置及び通信方法、コンピューター・プログラム、並びに通信システムに係り、特に、私的利用の範囲を超えた利用を抑制しながら、家庭内で蓄積したコンテンツを外部ネットワーク経由で伝送する通信装置及び通信方法、コンピューター・プログラム、並びに通信システムに関する。
【背景技術】
【０００２】
ディ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。とりわけ、リモート・アクセスにおいては、個人的又は家庭的なコンテンツの使用を許容しながら、コンテンツ伝送に介在する不正利用の防止、すなわち著作権保護の仕組みが必要である。ディジタル・コンテンツの伝送保護に関する業界標準的な技術として、ＤＴＬＡ（Ｄｉｇｉｔａｌ Ｔｒａｎｓｍｉｓｓｉｏｎ Ｌｉｃｅｎｓｉｎｇ Ａｄｍｉｎｉｓｔｒａｔｏｒ）が開発したＤＴＣＰ（Ｄｉｇｉｔａｌ Ｔｒａｎｓｍｉｓｓｉｏｎ Ｃｏｎｔｅｎｔ Ｐｒｏｔｅｃｔｉｏｎ）が挙げられる。
【０００３】
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である。

【０００４】
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コンテンツ伝送について規定したものである。最近では、ＤＬＮＡ（Ｄｉｇｉｔａｌ　Ｌｉｖｉｎｇ　Ｎｅｔｗｏｒｋ　Ａｌｌｉａｎｃｅ）に代表されるように、家庭内でもディジタル・コンテンツをＩＰネットワーク経由で流通させようという動きが本格的になっている。そこで、ＤＴＣＰ技術をＩＰネットワークに移植した、ＤＴＣＰ－ＩＰ（ＤＴＣＰ　ｍａｐｐｉｎｇ　ｔｏ　ＩＰ）の開発が進められている。
【０００５】
例えば、ホーム・サーバーに蓄積された放送コンテンツや映画などの商用コンテンツを、外出先から遠隔利用する場合、私的利用の範囲を超えて利用されることを適切な制御によって防止することが望まれている。
【０００６】
現在のＤＴＣＰ－ＩＰ（ＤＴＣＰ－ＩＰ　Ｖｏｌｕｍｅ　１　Ｓｐｅｃｉｆｉｃａｔｉｏｎ　Ｒｅｖｉｓｉｏｎ　１．４）では、第三者によるコンテンツの利用を制限することを意図して、家庭内のサーバーへのリモート・アクセスを、そのサーバーに登録した端末だけに限定している。また、端末を家庭内のサーバーに登録する際において、コマンドの往復遅延時間（ＲＴＴ：Ｒｏｕｎｄ　Ｔｒｉｐ　Ｔｉｍｅ）を最大７ミリ秒に制限するとともに、ＩＰルーターのホップ回数の上限が課されている。
【０００７】
例えば、リモート・アクセス時におけるＡＫＥ手続きにおいて、上記のＲＴＴ並びにＴＴＬの制限を解除してリモート・アクセス用の鍵共有を可能にする一方、リモート・アクセスする端末のサーバーへの事前登録、コンテンツのリモート・アクセス利用数制限、鍵供給数制限を課して、不特定多数のユーザーからのリモート・アクセスを制限するようにした通信システムについて、提案がなされている（例えば、特許文献１を参照のこと）。
【０００８】
しかしながら、現在のＤＴＣＰ－ＩＰ規格によると、端末の家庭内のサーバーへの登録は一度だけ行なえば、以後は再び登録を行なわずに、リモート・アクセスによりサーバー内のコンテンツを利用し続けることができる。このため、第三者の端末をサーバーに一度登録すれば、以後はその第三者がサーバー内のコンテンツを利用し続けることができてしまうという問題がある。
【先行技術文献】
【特許文献】
【０００９】
【特許文献１】特開２０１１－８２９５２号公報
【発明の概要】
【発明が解決しようとする課題】
【００１０】
本明細書で開示する技術の目的は、ＤＴＣＰなどの所定の相互認証及び鍵交換アルゴリズムに従って、家庭内で蓄積したコンテンツを外部ネットワーク経由で伝送する際に、私的利用の範囲を超えた利用を好適に抑制することができる、優れた通信装置及び通信方法、コンピューター・プログラム、並びに通信システムを提供することにある。
【課題を解決するための手段】
【００１１】
本願は、上記課題を参酌してなされたものであり、請求項１に記載の技術は、
端末に提供するコンテンツを取得するコンテンツ取得部、又は、端末に提供するコンテンツを記録するコンテンツ記録部と、
コンテンツを提供する端末を登録する端末登録部と、
端末の登録日時に基づいて端末へのコンテンツの提供を制御するコンテンツ提供部と、
を具備する通信装置である。
【００１２】

本願の請求項２に記載の技術によれば、請求項１に記載の通信装置は、所定の相互認証及び鍵交換手続きに従って端末を認証するとともに交換鍵を共有する認証及び鍵共有部をさらに備えている。そして、前記コンテンツ提供部は、前記交換鍵を用いて暗号化したコンテンツを端末に提供するように構成されている。

【００１３】

本願の請求項３に記載の技術によれば、請求項２に記載の通信装置の前記認証及び鍵共有部は、ＤＴＣＰ－ＩＰが規定する認証及び鍵交換（ＡＫＥ）アルゴリズムに従って、端末と相互認証並びに交換鍵の共有を行ない、前記端末登録部は、ＤＴＣＰ－ＩＰが規定する手続きに従って端末の登録を行なうように構成されている。

【００１４】

本願の請求項４に記載の技術によれば、請求項１に記載の通信装置の前記端末登録部は、ホーム・ネットワーク内で端末を登録し、前記コンテンツ提供部は、外部ネットワークからアクセスした登録後の端末にコンテンツを提供するように構成されている。

【００１５】

本願の請求項５に記載の技術によれば、請求項１に記載の通信装置の前記端末登録部は、端末の登録日時に第１の所定期間を加算した有効期限を端末の情報とともに管理し、前記コンテンツ提供部は、有効期限を経過した端末へのコンテンツの提供を制限するように構成されている。

【００１６】

本願の請求項６に記載の技術によれば、請求項１に記載の通信装置の前記端末登録部は、端末の登録日時に第１の所定期間を加算した有効期限を端末の情報とともに管理し、前記コンテンツ提供部は、有効期限を経過した端末へのコンテンツの提供を制限するように構成されている。

【００１７】

本願の請求項７に記載の技術によれば、請求項１に記載の通信装置の前記コンテンツ提供部は、前記端末登録部に登録される所定台数の端末については、登録日時に基づく制限を免除して、コンテンツを提供するように構成されている。

【００１８】

本願の請求項８に記載の技術によれば、請求項１に記載の通信装置は、コンテンツ毎又はコンテンツ・グループ毎に、登録日時に基づく制限を免除する端末を設定し、前記コンテンツ提供部は、提供するコンテンツ又はコンテンツが含まれるコンテンツ・グループについて登録日時に基づく制限が免除された端末に対して、登録日時に拘わらずコンテンツを提供するように構成されている。

【００１９】

本願の請求項９に記載の技術によれば、請求項８に記載の通信装置の前記コンテンツ記録部は、コンテンツ又はコンテンツが含まれるコンテンツ・グループについて登録日時に基づく制限を免除する端末を該当するコンテンツ又はコンテンツ・グループのメタデータに記録するように構成されている。

【００２０】

本願の請求項１０に記載の技術によれば、請求項５に記載の通信装置は、コンテンツ毎又はコンテンツ・グループ毎に、有効期限に基づく制限を免除する端末を設定している。そして、前記コンテンツ提供部は、提供するコンテンツを含むコンテンツ・グループ又は提供するコンテンツについて前記免除が設定された端末に対しては、有効期限に拘わらずコンテンツを提供するように構成されている。

【００２１】

本願の請求項１１に記載の技術によれば、請求項６に記載の通信装置は、コンテンツ毎又はコンテンツ・グループ毎に、限界日時に基づく制限を免除する端末を設定している。そして、前記コンテンツ提供部は、提供するコンテンツを含むコンテンツ・グループ又は提供するコンテンツについて前記免除が設定された端末に対しては、限界日時に拘わらずコンテンツを提供するように構成されている。

【００２２】
　また、本願の請求項１２に記載の技術は、
　端末に提供するコンテンツを取得するコンテンツ取得ステップ、又は、端末に提供するコンテンツをコンテンツ記録部に記録するコンテンツ記録ステップと、
　コンテンツを提供する端末を登録する端末登録ステップと、
　端末の登録日時に基づく制限をかけながら、前記コンテンツ取得ステップで取得したコンテンツ又は前記コンテンツ記録ステップで記録したコンテンツを端末に提供するコンテンツ提供ステップと、
を有する通信方法である。
【００２３】
　また、本願の請求項１３に記載の技術は、
　端末に提供するコンテンツを取得するコンテンツ取得部、又は、端末に提供するコンテンツを記録するコンテンツ記録部、
　コンテンツを提供する端末を登録する端末登録部、
　端末の登録日時に基づいて端末へのコンテンツの提供を制御するコンテンツ提供部、
としてコンピューターを機能させるようにコンピューター可読形式で記述されたコンピューター・プログラムである。
【００２４】
　本願の請求項１３に係るコンピューター・プログラムは、コンピューター上で所定の処理を実現するようにコンピューター可読形式で記述されたコンピューター・プログラムを定義したものである。換言すれば、本願の請求項１３に係るコンピューター・プログラムをコンピューターにインストールすることによって、コンピューター上では協働的作用が発揮され、本願の請求項１に係る通信装置と同様の作用効果を得ることができる。
【００２５】
　また、本願の請求項１４に記載の技術は、
　ユーザーによる操作情報が入力される入力部と、
　登録日時を管理するサーバーに対して登録要求を行なう登録要求部と、
　前記入力部に入力される操作情報に応じて、前記サーバーに対してコンテンツの要求を行なうコンテンツ要求部と、
　前記のコンテンツの要求に応じて、前記登録日時に基づく制限下で、前記サーバーから前記コンテンツの再生が許可されるコンテンツ再生部と、
を具備する通信装置である。
【００２６】
　本願の請求項１５に記載の技術によれば、請求項１４に記載の通信装置の前記コンテンツ再生部は、前記サーバーへの登録日時に第１の所定期間を加算した有効期限以降は、前記サーバーからのコンテンツの再生が制限される。
【００２７】
　本願の請求項１６に記載の技術によれば、請求項１４に記載の通信装置の前記コンテンツ再生部は、サーバーへの登録日時に第２の所定期間を加算した日時以降にサーバーが取得し又は記録したコンテンツの再生が制限される。
【００２８】
　本願の請求項１７に記載の技術によれば、請求項１４に記載の通信装置は、所定台数以内でサーバーに登録したときには、前記コンテンツ再生部は、サーバーへの登録日時に基づく制限を受けずに、サーバーからコンテンツを再生することができる。
【００２９】
　また、本願の請求項１８に記載の技術は、
　ユーザーによる操作情報が入力される入力ステップと、
　登録日時を管理するサーバーに対して登録要求を行なう登録要求ステップと、
　前記入力部に入力される操作情報に応じて、前記サーバーに対してコンテンツの要求を行なうコンテンツ要求ステップと、

前記のコンテンツの要求に応じて、前記登録日時に基づく制限下で、前記サーバーから前記コンテンツの再生が許可されるコンテンツ再生ステップと、
を有する通信方法である。
【００３０】
また、本願の請求項１９に記載の技術は、
ユーザーによる操作情報が入力される入力部、
登録日時を管理するサーバーに対して登録要求を行なう登録要求部、
前記入力部に入力される操作情報に応じて、前記サーバーに対してコンテンツの要求を行なうコンテンツ要求部、
前記のコンテンツの要求に応じて、前記登録日時に基づく制限下で、前記サーバーから前記コンテンツの再生が許可されるコンテンツ再生部、
としてコンピューターを機能させるようにコンピューター可読形式で記述されたコンピューター・プログラムである。
【００３１】
本願の請求項１９に係るコンピューター・プログラムは、コンピューター上で所定の処理を実現するようにコンピューター可読形式で記述されたコンピューター・プログラムを定義したものである。換言すれば、本願の請求項１９に係るコンピューター・プログラムをコンピューターにインストールすることによって、コンピューター上では協働的作用が発揮され、本願の請求項１４に係る通信装置と同様の作用効果を得ることができる。
【００３２】
また、本願の請求項２０に記載の技術は、
コンテンツを要求する端末と、
コンテンツを提供する端末を登録するとともに、その登録日時に基づいて前記端末へのコンテンツの提供を制御するサーバーと、
を具備する通信システムである。
【００３３】
但し、ここで言う「システム」とは、複数の装置（又は特定の機能を実現する機能モジュール）が論理的に集合した物のことを言い、各装置や機能モジュールが単一の筐体内にあるか否かは特に問わない。
【発明の効果】
【００３４】
本明細書で開示する技術によれば、ＤＴＣＰなどの所定の相互認証及び鍵交換アルゴリズムに従って、家庭内で蓄積したコンテンツを外部ネットワーク経由で伝送する際に、私的利用の範囲を超えた利用を好適に抑制することができる、優れた通信装置及び通信方法、コンピューター・プログラム、並びに通信システムを提供することができる。
【００３５】
本明細書で開示する技術によれば、端末から家庭内のサーバーへのリモート・アクセスを、端末のサーバーへの登録日時に基づいて制限することにより、一旦登録した第三者が利用し続けることを防止し、私的利用の範囲を超えたコンテンツの利用を好適に抑制することができる。
【００３６】
また、本明細書で開示する技術によれば、端末のサーバーへの登録日時から第１の所定の期間のみ、端末からサーバー内のコンテンツへのリモート・アクセスを可能にする、すなわち、登録日時から第１の所定の期間を経過した以降はリモート・アクセスを禁止することにより、第三者による私的利用の範囲を超えたコンテンツの利用を抑制することができる。
【００３７】
また、本明細書で開示する技術によれば、端末がリモート・アクセスにより利用可能なコンテンツを、端末のサーバーへの登録日時から第２の所定の期間以前に記録されたものだけに制限することにより、第三者による私的利用の範囲を超えたコンテンツの利用を好

適に抑制することができる。
【００３８】
また、本明細書で開示する技術によれば、所定台数の端末までは、サーバーへの登録日時に基づくリモート・アクセスの制限を免除することにより、私的利用の範囲内でのコンテンツの利用の利便性を確保することができる。
【００３９】
また、本明細書で開示する技術によれば、コンテンツ毎に、又は、コンテンツのグループ毎に、サーバーへの登録日時に基づくリモート・アクセスの制限を免除する端末を設定することにより、例えば家族のメンバー毎の複数の端末による私的利用の範囲内でのコンテンツの利用の利便性を確保することができる。
【００４０】
本明細書で開示する技術のさらに他の目的、特徴や利点は、後述する実施形態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。
【図面の簡単な説明】
【００４１】
【図１】図１は、本明細書で開示する技術を適用した通信システム１００の構成例を模式的に示した図である。
【図２】図２は、本明細書で開示する技術を適用した通信システム２００の他の構成例を模式的に示した図である。
【図３】図３は、図１並びに図２において、サーバー１０１、２０１として動作する通信装置３００の機能的構成を模式的に示した図である。
【図４】図４は、図１並びに図２において、端末１０２、２０２として動作する通信装置４００の機能的構成を模式的に示した図である。
【図５】図５は、ＤＴＣＰ仕様書に記載されている、リモート・アクセスを行なうＳｉｎｋをＳｏｕｒｃｅに登録する手順を示した図である。
【図６】図６は、リモート・アクセスを行なうＳｉｎｋデバイスを、有効期限とともにＳｏｕｒｃｅデバイスに登録する手順を示した図である。
【図７】図７は、Ｓｉｎｋ－ＩＤと有効期限をペアにしたｒｅｍｏｔｅ　ｓｉｎｋ　ｒｅｇｉｓｔｒｙの登録内容を例示した図である。
【図８】図８は、ＳｏｕｒｃｅデバイスとＳｉｎｋデバイス間でリモート・アクセスによるコンテンツ伝送を行なう手順を模式的に示した図である。
【図９】図９は、コンテンツ・リスト閲覧フェーズ（ＳＥＱ８０１）の中身を模式的に示した図である。
【図１０】図１０は、ＤＴＣＰの仕様書のＶ１ＳＥ．１０．７．２節に記載されている、ＲＡ－ＡＫＥ手続きフェーズの中身を示した図である。
【図１１】図１１は、有効期限が切れたＳｉｎｋ－ＩＤをｒｅｍｏｔｅ　ｓｉｎｋ　ｒｅｓｉｓｔｒｙから抹消する処理を含んだ、ＲＡ－ＡＫＥ手続きフェーズの中身を示した図である。
【図１２】図１２は、ｒｅｍｏｔｅ　ｓｉｎｋ　ｒｅｇｉｓｔｒｙのメンテナンス処理の手順を示したフローチャートである。
【図１３】図１３は、リモート・アクセスを行なうＳｉｎｋデバイスを、限界日時とともにＳｏｕｒｃｅデバイスに登録する手順を示した図である。
【図１４】図１４は、Ｓｉｎｋ－ＩＤと限界日時をペアにしたｒｅｍｏｔｅ　ｓｉｎｋ　ｒｅｇｉｓｔｒｙの登録内容を例示した図である。
【図１５】図１５は、リモート・アクセス用交換鍵K_R及びその交換鍵ラベルK_{R_label}をＳｉｎｋ－ＩＤと対応付けてＲＡＣ　ｒｅｃｏｒｄとして記憶する様子を示した図である。
【図１６】図１６は、リモート・アクセス用交換鍵K_Rを用いて暗号化伝送するコンテンツ伝送フェーズ（ＳＥＱ８０３）の中身を模式的に示した図である。
【図１７】図１７は、ＳＥＱ１６０２において実施するコンテンツ出力管理処理の手順を

示したフローチャートである。
【図１８】図１８は、有効期限に基づくコンテンツの出力管理を含んだコンテンツ伝送フェーズ（ＳＥＱ８０３）の中身を模式的に示した図である。
【図１９】図１９は、ＳＥＱ１８０２において実施するコンテンツ出力管理の処理手順を示したフローチャートである。
【図２０】図２０は、有効期限に基づくリモート・アクセスの制限の適用を免除する端末が登録されている場合の、コンテンツ出力管理の処理手順を示したフローチャートである。
【図２１】図２１は、限界日時に基づくリモート・アクセスの制限の適用を免除する端末が登録されている場合の、コンテンツ出力管理の処理手順を示したフローチャートである。
【図２２】図２２は、リモート・アクセスするＳｉｎｋデバイスの有効期限に基づいてＣＤＳ情報の提供を制限するための処理手順を示したフローチャートである。
【図２３】図２３は、コンテンツ・リスト閲覧フェーズにおいてＳｉｎｋデバイスの有効期限に基づくＣＤＳ情報の提供制限を免除するための処理手順を示したフローチャートである。
【図２４】図２４は、リモート・アクセスするＳｉｎｋデバイスの限界日時に基づいてＣＤＳ情報の提供を制限するための処理手順を示したフローチャートである。
【図２５】図２５は、コンテンツ・リスト閲覧フェーズにおいてＳｉｎｋデバイスの限界日時に基づくＣＤＳ情報の提供制限を免除するための処理手順を示したフローチャートである。
【図２６】図２６は、コンピューター・プログラム配信システム２６００の構成を示した図である。
【発明を実施するための形態】
【００４２】
以下、図面を参照しながら本明細書で開示する技術の実施形態について詳細に説明する。
【００４３】
Ａ．システム構成
図１には、本明細書で開示する技術を適用した通信システム１００の構成例を模式的に示している。図示の通信システム１００は、家庭内に敷設されたホーム・ネットワーク１１０上に接続されたサーバー１０１と端末１０２で構成される。同図では、簡素化のため、サーバーと端末をそれぞれ１台ずつしか描いていないが、２台以上のサーバー並びに端末がホーム・ネットワーク１１０上に設置されることも想定される。
【００４４】
サーバー１０１は、端末１０２に提供するコンテンツを蓄積している。サーバー１０１は、例えば、地上ディジタル放送で受信した放送コンテンツや、ブルーレイ・ディスクなどの記録媒体（図示しない）から読み込んだ映画などの商用コンテンツ、さらにはインターネット上のコンテンツ・サーバー（図示しない）からダウンロードしたコンテンツを蓄積している。
【００４５】
ホーム・ネットワーク１１０を介したサーバー１０１と端末１０２間のコンテンツ伝送には、ＤＴＣＰ技術が適用されている。したがって、コンテンツを利用したい端末１０２は、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、サーバー１０１と相互認証するとともに鍵を共有した後に、サーバー１０１内に蓄積されたコンテンツを要求することができる。サーバー１０１は、要求されたコンテンツを、共有した鍵を用いて暗号化伝送する。コンテンツを提供するサーバー１０１はＳｏｕｒｃｅデバイスに相当し、コンテンツを利用する端末１０２はＳｉｎｋデバイスに相当する。
【００４６】

なお、端末１０２で外出先などホーム・ネットワーク１１０の外からサーバー１０１にアクセスしたいときには、ホーム・ネットワーク１１０上で端末１０２をサーバー１０１に事前登録しておく必要がある。

【００４７】

また、図２には、本明細書で開示する技術を適用した通信システム２００の他の構成例を模式的に示している。図示の通信システム２００は、家庭内に敷設されたホーム・ネットワーク２１０上に接続されたサーバー２０１と、インターネットなどの外部ネットワーク２２０上に接続された端末２０２で構成される。ホーム・ネットワーク２１０と外部ネットワーク２２０は、ＩＰ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）プロトコルに従い、ルーター２３０経由で相互接続されている。同図では、簡素化のため、サーバーと端末をそれぞれ１台ずつしか描いていないが、ホーム・ネットワーク２１０上に２台以上のサーバーが設置されることや、ホーム・ネットワーク２１０上にも端末が接続され、さらに外部ネットワーク２２０上に２台以上の端末が接続されることも想定される。

【００４８】

サーバー２０１は、放送コンテンツや商用コンテンツなど、端末２０２に提供するコンテンツを蓄積している。また、ホーム・ネットワーク２１０及び外部ネットワーク２２０を介したサーバー２０１と端末２０２間のコンテンツ伝送には、ＤＴＣＰ－ＩＰ技術が適用されている。したがって、コンテンツを利用したい端末２０２は、ホーム・ネットワーク２１０上でサーバー２０１に事前に登録しておく必要がある（前述）。そして、端末２０２は、ホーム・ネットワーク２１０及び外部ネットワーク２２０からなるＩＰネットワーク越しに、サーバー２０１と相互認証するとともに交換鍵を共有した後に、サーバー２０１内に蓄積されたコンテンツを要求することができる。サーバー２０１は、要求されたコンテンツを、共有した交換鍵を用いて暗号化伝送する。コンテンツを提供するサーバー２０１はＳｏｕｒｃｅデバイスに相当し、コンテンツを利用する端末２０２はＳｉｎｋデバイスに相当する。

【００４９】

図３には、図１並びに図２において、サーバー１０１、２０１（すなわち、Ｓｏｕｒｃｅデバイス）として動作する通信装置３００の機能的構成を模式的に示している。

【００５０】

通信・制御部３０１は、ホーム・ネットワーク並びに外部ネットワークを介した通信動作を制御するとともに、当該通信装置３００全体の動作を統括的に制御する。また、通信・制御部３０１は、ＨＤＭＩ（登録商標）（Ｈｉｇｈ　Ｄｅｆｉｎｉｔｉｏｎ　Ｍｕｌｔｉｍｅｄｉａ　Ｉｎｔｅｒｆａｃｅ）やＵＳＢ（Ｕｎｉｖｅｒｓａｌ　Ｓｅｒｉａｌ　Ｂｕｓ）などの外部機器接続用（若しくは、コンテンツのディジタル出力用）のインターフェースを備えており、ハード・ディスク装置やブルーレイ・ディスク装置などの録画再生機器を接続することができる。

【００５１】

コンテンツ記録部３０２は、ホーム・ネットワーク並びに外部ネットワーク越しで端末に提供するコンテンツを記録する。コンテンツ記録部３０２に記録された各コンテンツは、一般的なファイル・システムの管理下で、記録日時やアクセス日時が保持される。

【００５２】

本実施形態では、コンテンツ記録部３０２に記録されたコンテンツ毎にリモート・アクセスの制限を設定したり、複数のコンテンツをグループ化してコンテンツのグループ毎にリモート・アクセスの制限を設定したりすることができるが、その詳細については後述に譲る。また、コンテンツ記録部３０２は、各コンテンツ、又はコンテンツ・グループのメタデータも記録する。

【００５３】

コンテンツ取得部３０３は、端末に提供するコンテンツを取得する。コンテンツ取得部３０３は、例えば地上ディジタル放送用チューナーなどからなり、放送コンテンツを取得する。この場合のコンテンツ取得部３０３は、例えばＡＲＩＢ（Ａｓｓｏｃｉａｔｉｏｎ

ｏｆ Ｒａｄｉｏ Ｉｎｄｕｓｔｒｉｅｓ ａｎｄＢｕｓｉｎｅｓｓｅｓ：電波産業会）で規定される仕様に基づく。コンテンツ取得部３０３は、例えば、放送チャンネルの全セグメント又は一部のセグメントの受信機能、ＥＰＧ（Ｅｌｅｃｔｒｏｎｉｃ Ｐｒｏｇｒａｍ Ｇｕｉｄｅ）の機能（番組検索、番組情報の表示、番組予約）、ＨＤＣＰ（Ｈｉｇｈ－ｂａｎｄｗｉｄｔｈ Ｄｉｇｉｔａｌ Ｃｏｎｔｅｎｔ Ｐｒｏｔｅｃｔｉｏｎ）仕様などに基づくコピー制御機能、放送コンテンツを限定受信したり受信した放送コンテンツを外部出力する際に暗号化したりするコンテンツ保護機能、などを備えている。

【００５４】

また、コンテンツ取得部３０３は、ブルーレイ・ディスクなどのメディア再生装置からなり、映画などの商用コンテンツをメディアから読み取る。また、コンテンツ取得部３０３は、ブラウザーなどからなり、インターネット上のコンテンツ・サーバー（図示しない）から有償又は無償のコンテンツをダウンロードする。コンテンツ取得部３０３は、取得したコンテンツは、必要に応じて上記のコンテンツ記録部３０２内に記録してもよい。また、コンテンツ取得部３０３は、端末に提供するコンテンツをコンテンツ記録部３０２から取得することもある。

【００５５】

放送コンテンツや商用コンテンツなどの取得日時は、コンテンツ取得部３０３が放送コンテンツを受信し又は商用コンテンツを読み出す現在日時である。また、コンテンツ記録部３０２内のコンテンツの取得日時は、コンテンツを記録した記録日時であり、ファイル・システムなどが管理している。本実施形態では、リモート・アクセスする端末に対してコンテンツの取得日時又は記録日時に基づいてコンテンツの提供を制限する点に１つの特徴があるが、その詳細については後述に譲る。

【００５６】

コンテンツ提供部３０４は、端末からの要求に応答して、コンテンツ取得部３０３が取得したコンテンツを端末に提供する。コンテンツ提供部３０４は、例えばＨＴＴＰ（Ｈｙｐｅｔ Ｔｅｘｔ Ｔｒａｎｓｆｅｒ Ｐｒｏｔｏｃｏｌ）プロトコルが利用して、端末へコンテンツを伝送する。また、コンテンツ提供部３０４は、伝送するコンテンツを、認証・鍵共有部３０６により端末と共有した交換鍵を用いて暗号化する。端末が外部ネットワーク上からのリモート・アクセスによりコンテンツを要求する場合、その端末は端末管理部３０７に事前に登録されたものでなければならない。本実施形態では、コンテンツ提供部３０４は、リモート・アクセスする端末に対して登録日時やコンテンツの取得日時に基づいてコンテンツの提供を制限する点に１つの特徴があるが、その詳細については後述に譲る。

【００５７】

コンテンツ・リスト提供部３０５は、例えば端末からの要求に応答して、端末に提供可能なコンテンツのリストと詳細情報を、端末に提供する。上述からも分かるように、サーバー１０１、２０１が端末に提供可能なコンテンツは、コンテンツ取得部３０３が受信する放送コンテンツやメディアから読み出す商用コンテンツ、コンテンツ記録部３０２に既に記録されているコンテンツが挙げられる。コンテンツ・リストの提供には、例えば、ＤＬＮＡのベースとなるＵＰｎＰ（Ｕｎｉｖｅｒｓａｌ Ｐｌｕｇ ａｎｄＰｌａｙ）で策定されている、コンテンツのリストとコンテンツの詳細情報を階層化して配信するＣＤＳ（Ｃｏｎｔｅｎｔ Ｄｉｒｅｃｔｏｒｙ Ｓｅｒｖｉｃｅ）機能が適用される。本実施形態では、リモート・アクセスする端末に対して登録日時やコンテンツの取得日時に基づいてコンテンツの提供を制限する点に１つの特徴があるが、その詳細については後述に譲る。

【００５８】

認証・鍵共有部３０６は、コンテンツの要求元となる端末との間で、ＤＴＣＰ－ＩＰが規定する認証及び鍵交換（ＡＫＥ）アルゴリズムに従って、相互認証並びにコンテンツ暗号化のための交換鍵の共有を行なう。認証・鍵共有部３０６は、外部ネットワークからリモート・アクセスによりコンテンツを要求してくる端末に対しては、リモート・アクセス

用交換鍵K_Rを共有する（後述）。

【００５９】

端末管理部３０７は、コンテンツを要求する端末の情報を管理する。端末管理部３０７は、外部ネットワークからリモート・アクセスによりコンテンツを利用する端末に対して事前登録の処理を行なうとともに、その端末の情報を「ｒｅｍｏｔｅ　ｓｉｎｋ　ｒｅｇｉｓｔｒｙ」や「ＲＡＣ（Ｒｅｍｏｔｅ　Ａｃｃｅｓｓ　Ｃｏｎｎｅｃｔｉｏｎ）　ｒｅｇｉｓｔｒｙ」として管理するが、その詳細については後述に譲る。コンテンツの利用は私的利用の範囲内に制限すべきである。本実施形態では、リモート・アクセスする端末に対して登録日時やコンテンツの取得日時に基づいてコンテンツの提供を制限することにより、コンテンツの利用を私的利用の範囲に制限するようにする点に１つの特徴があるが、その点の詳細については後述に譲る。

【００６０】

なお、上記の機能ブロック３０３～３０７は、通信・制御部３０１において、オペレーティング・システムやＴＣＰ／ＩＰプロトコルの上位で実行するアプリケーション・プログラムとして実現することもできる。また、この種のアプリケーション・プログラムは、インターネットなどの広域ネットワーク上で所定のダウンロード・サイトで配信することができ、ディジタル放送チューナーやＴＶ受像機などのＣＥ（Ｃｏｎｓｕｍｅｒ　Ｅｌｅｃｔｒｏｎｉｃｓ）機器、スマートフォンなどの多機能端末にダウンロードして利用に供される。

【００６１】

このようなダウンロード・サイトは、例えば、コンピューター・プログラムを記憶する記憶装置２６１１と、コンピューター・プログラムのダウンロード要求を受信したことに応じてそのダウンロードを認める通信装置２６１２とを備えたサーバー２６１０からなり（図２６を参照のこと）、ダウンロードしたコンピューター・プログラムをインストールするクライアント装置（ＤＴＣＰ＿Ｓｏｕｒｃｅ又はＤＴＣＰ＿Ｓｉｎｋ）と併せてコンピューター・プログラム配信システム２６００を構成する。この種のサーバーは、クライアントからのコンピューター・プログラムのダウンロード要求に対して、コンピューター・プログラムの名称を示す情報を通知する情報通知装置２６１３をさらに備えている。情報通知装置２６１３は、コンピューター・プログラムの名称とともに、例えば、家庭内に記録した商用コンテンツを遠隔地の端末に提供するアプリケーションであることを示す情報を通知する。

【００６２】

図４には、図１並びに図２において、端末１０２、２０２（すなわち、Ｓｉｎｋ）として動作する通信装置４００の機能的構成を模式的に示している。

【００６３】

通信・制御部４０１は、ホーム・ネットワーク並びに外部ネットワークを介した通信動作を制御するとともに、当該通信装置４００全体の動作を統括的に制御する。

【００６４】

コンテンツ・リスト閲覧部４０２は、Ｓｏｕｒｃｅとなるサーバー１０１、２０１に対して、コンテンツ・リストの取得要求を行ない、取得したコンテンツ・リストの閲覧画面を表示する。例えば、サーバー１０１、２０１が提供可能なコンテンツのリストをＣＤＳ情報（前述）として取得したときには、コンテンツ一覧画面が表示される。ユーザーはこの一覧画面を通して、再生出力したいコンテンツを選択することができる。本実施形態では、サーバー２０１にリモート・アクセスする端末２０２の場合、提供可能なコンテンツのリストは、サーバー２０１への登録日時やコンテンツの取得日時に基づいて制限される点に１つの特徴があるが、その詳細については後述に譲る。

【００６５】

コンテンツ取得部４０３は、コンテンツの取得要求をサーバー１０１、２０１に送信して、サーバー内のコンテンツを取得する。コンテンツ取得部４０３は、例えば、コンテンツ・リスト閲覧部４０２が表示するコンテンツ一覧画面の中でユーザーが選択したコンテ

ンツの取得を要求する。サーバー１０１、２０１に対するコンテンツの取得要求並びにコンテンツの取得には、例えばＨＴＴＰプロトコルが利用される（後述）。本実施形態では、サーバー２０１にリモート・アクセスする端末２０２の場合、取得可能なコンテンツは、サーバー２０１への登録日時やコンテンツの取得日時に基づいて制限される点に１つの特徴があるが、その詳細については後述に譲る。

【００６６】

サーバー１０１、２０１から取得したコンテンツは、認証・鍵共有部４０６によりサーバー１０１、２０１との間で共有した交換鍵を用いて暗号化されている。コンテンツ復号部４０４は、サーバー１０１、２０１から取得した暗号化コンテンツこの暗号鍵を用いて復号化する。そして、コンテンツ再生出力部４０５は、復号したコンテンツを再生出力する。

【００６７】

認証・鍵共有部４０６は、コンテンツの要求先となるサーバー１０１、２０１との間で、ＤＴＣＰ－ＩＰが規定する認証及び鍵交換（ＡＫＥ）アルゴリズムに従って、相互認証並びにコンテンツ暗号化のための暗号鍵の共有を行なう。認証・鍵共有部４０６は、外部ネットワークからリモート・アクセスによりコンテンツを要求するサーバー２０１との間では、リモート・アクセス用交換鍵K_Rを共有する。また、認証・鍵共有部４０６は、ホーム・ネットワーク２１０接続時において、サーバー１０１に対してリモート・アクセスのための事前登録を行なう。

【００６８】

上記の機能ブロック４０２～４０６は、通信・制御部４０１において、オペレーティング・システムやＴＣＰ／ＩＰプロトコルの上位で実行するアプリケーション・プログラムとして実現することもできる。この種のアプリケーション・プログラムは、インターネットなどの広域ネットワーク上で所定のダウンロード・サイトで配信することができ、スマートフォンなど、ホーム・サーバー内のコンテンツを再生する多機能端末にダウンロードして利用に供される。

【００６９】

このようなダウンロード・サイトは、例えば、コンピューター・プログラムを記憶する記憶装置２６１１と、コンピューター・プログラムのダウンロード要求を受信したことに応じてそのダウンロードを認める通信装置２６１２とを備えたサーバー２６１０からなり（図２６を参照のこと）、ダウンロードしたコンピューター・プログラムをインストールするクライアント装置（ＤＴＣＰ＿Ｓｏｕｒｃｅ又はＤＴＣＰ＿Ｓｉｎｋ）と併せてコンピューター・プログラム配信システム２６００を構成する。この種のサーバーは、クライアントからのコンピューター・プログラムのダウンロード要求に対して、コンピューター・プログラムの名称を示す情報を通知する情報通知装置２６１３をさらに備えている。情報通知装置２６１３は、コンピューター・プログラムの名称とともに、例えば、家庭内に記録した商用コンテンツを遠隔地で閲覧することが認められるアプリケーションであることを示す情報を通知する。

【００７０】

本実施形態では、図２に示したような端末２０２からサーバー２０１へのリモート・アクセスはサーバー２０１への登録日時に基づいて制御され、登録日時から所定の期間が経過するとリモート・アクセスが制限されるようになっている（後述）。リモート・アクセスする端末２０２は、例えば認証・鍵共有部４０６がサーバー２０１への登録日時を管理し、所定の期間が経過する前に再登録の手続きを自動実行して、リモート・アクセスが制限されないように、登録日時をリフレッシュするようにしてもよい。

【００７１】

Ｂ．登録手続き

図５には、ＤＴＣＰの仕様書、ＤＴＣＰ Ｖｏｌｕｍｅ １ Ｓｕｐｐｌｅｍｅｎｔ Ｅ Ｍａｐｐｉｎｇ ＤＴＣＰ ｔｏ ＩＰ, Ｒｅｖｉｓｉｏｎ １．４ｅｄ１（Ｉｎｆｏｒｍａｔｉｏｎａｌ Ｖｅｒｓｉｏｎ）のＶ１ＳＥ．１０．７．１節に記載されている

、リモート・アクセスを行なうＳｉｎｋデバイスをＳｏｕｒｃｅデバイスに登録する手順を図解している。同図中、Ｓｉｎｋデバイスは端末２０２に相当し、Ｓｏｕｒｃｅデバイスはサーバー２０１に相当するものと理解されたい。

【００７２】

まず、ＳｏｕｒｃｅデバイスとＳｉｎｋデバイス間で、ＲＴＴ（Ｒｏｕｎｄ Ｔｒｉｐ Ｔｉｍｅ）の制限下で、ＡＫＥ手続きが実施される（ＳＥＱ５０１）。例えば、ＳｏｕｒｃｅデバイスとＳｉｎｋデバイスがホーム・ネットワーク２１０内にあれば、ＲＴＴの制限をクリアして、ＡＫＥ手続きが成功裏に終了する。ＲＴＴ－ＡＫＥ手続き自体は、本明細書で開示する技術の要旨に直接関連しないので、ここでは詳細な説明を省略する。

【００７３】

次いで、Ｓｉｎｋデバイスは、コマンドＲＡ＿ＲＥＧＩＳＴＥＲ．ＣＭＤを用いて、自分のＳｉｎｋ－ＩＤをＳｏｕｒｃｅデバイスに送信する（ＳＥＱ５０２）。

【００７４】

ここで、Ｓｉｎｋデバイスは、Ｓｉｎｋ－ＩＤとして、自分に固有のＤｅｖｉｃｅ ＩＤ、又は、ＩＤｕを送信する（ＳｉｎｋデバイスがＣｏｍｍｏｎ Ｄｅｖｉｃｅ ＫｅｙとＣｏｍｍｏｎ Ｄｅｖｉｃｅ Ｃｅｒｔｉｆｉｃａｔｅを実装することで、Ｄｅｖｉｃｅ ＩＤがＳｉｎｋの特定情報とならない場合には、ＩＤｕがＳｉｎｋ－ＩＤとして用いられる）。

【００７５】

Ｓｏｕｒｃｅデバイスは、ＲＡ＿ＲＥＧＩＳＴＥＲ．ＣＭＤで受け取ったＳｉｎｋ－ＩＤが、直前に完了したＲＴＴ－ＡＫＥ手続で受信したＤｅｖｉｃｅ ＩＤ又はＩＤｕと一致するかどうかをチェックする。

【００７６】

また、Ｓｏｕｒｃｅデバイスは、受け取ったＳｉｎｋ－ＩＤが、（端末管理部３０７で管理している）ｒｅｍｏｔｅ ｓｉｎｋ ｒｅｇｉｓｔｒｙに既に記憶されているかどうかをチェックする。受け取ったＳｉｎｋ－ＩＤが既に記憶されている場合は、そのまま本手続きを終了する。

【００７７】

他方、受け取ったＳｉｎｋ－ＩＤがまだｒｅｍｏｔｅ ｓｉｎｋ ｒｅｇｉｓｔｒｙに記憶されていないときには、Ｓｏｕｒｃｅデバイスは、ｒｅｍｏｔｅ ｓｉｎｋ ｒｅｇｉｓｔｒｙが満杯でないことを確認する。そして、受け取ったＳｉｎｋ－ＩＤが、直前に完了したＲＴＴ－ＡＫＥ手続で受信したＤｅｖｉｃｅ ＩＤ又はＩＤｕと一致し、且つ、ｒｅｍｏｔｅ ｓｉｎｋ ｒｅｇｉｓｔｒｙが満杯でなければ、Ｓｏｕｒｃｅデバイスは Ｓｉｎｋ－ＩＤをｒｅｍｏｔｅ ｓｉｎｋ ｒｅｇｉｓｔｒｙに追加記憶する（ＳＥＱ５０４）。

【００７８】

また、Ｓｏｕｒｃｅデバイスは、登録した結果を、コマンドＲＡ＿ＲＥＧＩＳＴＥＲ．ＲＳＰでＳｉｎｋデバイスに返す（ＳＥＱ５０３）。

【００７９】

図２に示した通信システム２００に当てはめて考察すると、Ｓｏｕｒｃｅデバイスとしてのサーバー２０１は、ＲＴＴ－ＡＫＥ手続きに成功した端末２０１（但し、ホーム・ネットワーク２１０に接続しているとき）のＳｉｎｋ－ＩＤを、端末管理部３０７で管理しているｒｅｍｏｔｅ ｓｉｎｋ ｒｅｇｉｓｔｒｙに追加記憶する。

【００８０】

ここで、サーバー２０１がｒｅｍｏｔｅ ｓｉｎｋ ｒｅｇｉｓｔｒｙに一度登録したＳｉｎｋ－ＩＤを保持し続けると、第三者の端末をサーバーに一度登録すれば、以後はその第三者がサーバー内のコンテンツを利用し続けることができてしまうという問題がある。

【００８１】

そこで、本実施形態では、サーバー２０１は、端末２０２からのリモート・アクセスを

、端末２０２のサーバー２０１への登録日時に基づいて制限することにより、一旦登録した第三者が利用し続けることを防止し、私的利用の範囲を超えたコンテンツの利用を好適に抑制するようにしている。

【００８２】

Ｃ．登録日時に基づくリモート・アクセスの制限（１）

サーバー２０１が、登録日時に基づいて端末２０２からのリモート・アクセスを制限する方法の１つとして、登録日時から第１の所定の期間（例えば、３０日間）を端末のリモート・アクセスを許可する有効期限として設定する方法が挙げられる。サーバー２０１は、コンテンツへのリモート・アクセスを要求した端末２０２が有効期限内であれば、コンテンツの利用を許可するが、有効期限を過ぎた端末２０２からのリモート・アクセスを許可しない。

【００８３】

サーバー２０１は、例えば、端末２０２をｒｅｍｏｔｅ　ｓｉｎｋ　ｒｅｇｉｓｔｒｙに登録する際に、現在日時に第１の所定期間を加算してその端末２０２の有効期限を算出して、Ｓｉｎｋ－ＩＤとともに有効期限をペアにして、端末管理部３０７内に記憶するようにすればよい。

【００８４】

図６には、リモート・アクセスを行なうＳｉｎｋデバイスを、有効期限とともにＳｏｕｒｃｅデバイスに登録する手順を図解している。但し、Ｓｏｕｒｃｅデバイスは、ホーム・ネットワーク２１０に設置され、コンテンツを送信するサーバー２０１に相当し、Ｓｉｎｋデバイスは、サーバー２０１にコンテンツを要求する端末２０２に相当する（以下同様）。Ｓｉｎｋデバイスは、ホーム・ネットワーク２１０上で図６に示す登録手続きを一旦行なった後は、インターネットなどの外部ネットワーク２２０からサーバー２０１にリモート・アクセスする。

【００８５】

まず、ＳｏｕｒｃｅデバイスとＳｉｎｋデバイス間で、ＲＴＴ（Ｒｏｕｎｄ　Ｔｒｉｐ　Ｔｉｍｅ）の制限下で、ＡＫＥ手続きが実施される（ＳＥＱ６０１）。

【００８６】

そして、ＲＴＴ－ＡＫＥ手続きに成功裏に終了すると、Ｓｉｎｋデバイスは、コマンドＲＡ＿ＲＥＧＩＳＴＥＲ．ＣＭＤを用いて、自分のＳｉｎｋ－ＩＤをＳｏｕｒｃｅデバイスに送信する（ＳＥＱ６０２）。

【００８７】

これに対し、Ｓｏｕｒｃｅデバイスは、ＲＡ＿ＲＥＧＩＳＴＥＲ．ＣＭＤで受け取ったＳｉｎｋ－ＩＤが、直前に完了したＲＴＴ－ＡＫＥ手続で受信したＤｅｖｉｃｅ　ＩＤ又はＩＤｕと一致し、ｒｅｍｏｔｅ　ｓｉｎｋ　ｒｅｇｉｓｔｒｙにまだ記憶しておらず、且つ、ｒｅｍｏｔｅ　ｓｉｎｋ　ｒｅｇｉｓｔｒｙが満杯でないかどうかをチェックする。そして、これらの条件をクリアし、Ｓｉｎｋ－ＩＤをｒｅｍｏｔｅ　ｓｉｎｋ　ｒｅｇｉｓｔｒｙに追加記憶するときには、Ｓｏｕｒｃｅデバイスは、コマンドＲＡ＿ＲＥＧＩＳＴＥＲ．ＲＳＰでＳｉｎｋデバイスに返す（ＳＥＱ６０３）。

【００８８】

また、Ｓｏｕｒｃｅデバイスは、Ｓｉｎｋデバイスの登録日時として現在日時を取得すると（ＳＥＱ６０４）、Ｓｉｎｋデバイスの登録の有効期間としての第１の所定の期間（例えば、３０日間）を現在日時に加算して有効期限を算出すると（ＳＥＱ６０５）、Ｓｉｎｋ－ＩＤと有効期限のペアを、ｒｅｍｏｔｅ　ｓｉｎｋ　ｒｅｇｉｓｔｒｙに記憶する（ＳＥＱ６０６）。

【００８９】

図７には、Ｓｉｎｋ－ＩＤと有効期限をペアにして格納したｒｅｍｏｔｅ　ｓｉｎｋ　ｒｅｇｉｓｔｒｙの登録内容を例示している。但し、図７に示したような端末の登録日時や有効期限の情報の管理を、ホーム・ネットワーク２１０上のサーバー２０１内で個別に行なうのではなく、クラウド上などに置かれた管理用サーバーで一元的に行なうようにし

てもよい。

【００９０】

Ｓｏｕｒｃｅデバイス（サーバー２０１）は、登録日時としての現在日時を、例えば、サーバー内蔵の時計機能（図３では図示を省略）、放送波に含まれる時刻信号（例えば、コンテンツ取得部３０３がチューナー機能を装備して放送波を受信する場合）、ネットワーク上のサーバー（図示しない）から得た時刻情報などから取得することができる。

【００９１】

なお、端末２０２は、ユーザーが知らない間に、サーバー２０１へのリモート・アクセスが登録日時に基づいて制限されてしまわないように、認証・鍵共有部４０６などでサーバー２０１への登録日時を管理し、所定の期間が経過する前に再登録の手続き（すなわち、図６に示した処理シーケンスの再起動）を自動実行して、リモート・アクセスが制限されないように、登録日時をリフレッシュするようにしてもよい。勿論、端末２０２のユーザーがマニュアル操作で登録日時のリフレッシュを行なうようにしてもよい。

【００９２】

図８には、上記の事前登録を行なった後のＳｏｕｒｃｅデバイスとＳｉｎｋデバイス間でリモート・アクセスによるコンテンツ伝送を行なう手順を模式的に示している。図示のコンテンツ伝送は、Ｓｉｎｋデバイスが伝送を要求するコンテンツを指定するコンテンツ・リスト閲覧フェーズ（ＳＥＱ８０１）と、ＳｏｕｒｃｅデバイスとＳｉｎｋデバイス間で相互認証及び鍵交換手順を実施してリモート・アクセス用交換鍵K_Rを共有するＲＡ－ＡＫＥ手続きフェーズ（ＳＥＱ８０２）と、コンテンツ・リスト閲覧フェーズで指定されたコンテンツを、リモート・アクセス用交換鍵K_Rを用いて暗号化伝送するコンテンツ伝送フェーズ（ＳＥＱ８０３）からなる。

【００９３】

図９には、コンテンツ・リスト閲覧フェーズ（ＳＥＱ８０１）の中身を模式的に示している。

【００９４】

Ｓｉｎｋデバイスからは、コンテンツ・リスト閲覧部４０２から、コンテンツ・リストの閲覧要求が発行される（ＳＥＱ９０１）。

【００９５】

本実施形態では、コンテンツ・リストの閲覧には、ＤＬＮＡのベースとなるＵＰｎＰで策定されている、コンテンツのリストとコンテンツの詳細情報を階層化して配信するＣＤＳ（Ｃｏｎｔｅｎｔ　Ｄｉｒｅｃｔｏｒｙ　Ｓｅｒｖｉｃｅ）機能が適用される。したがって、ＳＥＱ９０１では、ＳｉｎｋデバイスからＣＤＳ：Ｂｒｏｗｓｅアクションが発行される。

【００９６】

コンテンツ・リストの閲覧要求には、Ｓｉｎｋデバイスを特定するＳｉｎｋ－ＩＤが含められる。ＣＤＳ：ＢｒｏｗｓｅリクエストでＳｉｎｋ－ＩＤを送る手段としては、新たにヘッダー・フィールド（例えば、ＳｉｎｋＩＤ．ｄｔｃｐ．ｃｏｍ）を設け、そのパラメーターとしてＨＴＴＰのヘッダー部分で送ることが考えられる。

【００９７】

Ｓｏｕｒｃｅデバイス側では、コンテンツ提供部３０４で提供可能なコンテンツ（例えば、コンテンツ取得部３０３で取得可能な放送コンテンツや商用コンテンツ、あるいは、自身のストレージであるコンテンツ記録部３０２に既に記録されているコンテンツなど）に対してＣＤＳ：Ｂｒｏｗｓｅアクションが発行されたので、コンテンツ・リスト提供部３０５は、該当するコンテンツに関する取得可能なすべてのコンテンツ情報を取得して（ＳＥＱ９０２）、十分な情報量のＣＤＳ情報を生成する（ＳＥＱ９０３）。Ｓｏｕｒｃｅデバイスは、リモート・アクセスするＳｉｎｋデバイスに対しては、Ｓｉｎｋデバイスの有効期限に基づいてＣＤＳ情報の提供を制限するようにしてもよい（後述）。そして、Ｓｏｕｒｃｅデバイスは、Ｓｉｎｋデバイスに対してＣＤＳ　Ｒｅｓｕｌｔとして返す（ＳＥＱ９０４）。

【００９８】
Ｓｉｎｋデバイス側では、コンテンツ・リスト閲覧部４０２が、受信したＣＤＳ　Ｒｅｓｕｌｔを解析して、コンテンツのタイトル並びにより詳細情報を含むコンテンツ情報を表示する（ＳＥＱ９０５）。
【００９９】
図２２には、コンテンツ・リスト閲覧フェーズ（ＳＥＱ８０１）において、Ｓｏｕｒｃｅデバイスが、リモート・アクセスするＳｉｎｋデバイスに対して、Ｓｉｎｋデバイスの有効期限に基づいてＣＤＳ情報の提供を制限するための処理手順をフローチャートの形式で示している。
【０１００】
まず、Ｓｏｕｒｃｅデバイスは、提供可能なコンテンツ情報をクリアする（ステップＳ２２０１）。
【０１０１】
次いで、Ｓｏｕｒｃｅデバイスは、要求元のＳｉｎｋデバイスのＳｉｎｋ－ＩＤに対応する有効期限を、ｒｅｍｏｔｅ　ｓｉｎｋ　ｒｅｇｉｓｔｒｙから取得するとともに（ステップＳ２２０２）、現在日時を取得する（ステップＳ２２０３）。
【０１０２】
そして、Ｓｏｕｒｃｅデバイスは、現在日時が要求元のＳｉｎｋデバイスの有効期限を過ぎていないかどうかをチェックする（ステップＳ２２０４）。現在日時が有効期限を過ぎている場合には（ステップＳ２２０４のＮｏ）、後続のコンテンツ情報の追加処理をスキップし、空のままコンテンツ情報を送信する（ステップＳ２２０８）。
【０１０３】
一方、現在日時が要求元のＳｉｎｋデバイスの有効期限を過ぎていないときには（ステップＳ２２０４のＹｅｓ）、通常通り、コンテンツ情報の作成を行なう。すなわち、すべてのコンテンツ情報を処理するまで（ステップＳ２２０５のＮｏ）、未処理のコンテンツのコンテンツ情報の参照と（ステップＳ２２０６）、このコンテンツ情報を提供可能なコンテンツ情報に追加する処理を（ステップＳ２２０７）、繰り返し実行する。そして、Ｓｏｕｒｃｅデバイスは、完成したコンテンツ情報を、要求元のＳｉｎｋデバイスに送信する（ステップＳ２２０８）。
【０１０４】
図２２に示した処理手順は、例えば、図９に示したシーケンス図中のＳＥＱ９０３において実施される。但し、Ｓｏｕｒｃｅデバイスは、この処理手順を必ず実施する必要はなく、Ｓｉｎｋデバイスの有効期限に拘わらず、自ら提供可能なすべてのコンテンツについてコンテンツ情報を提供するようにしてもよい。
【０１０５】
Ｓｉｎｋデバイスのユーザーは、表示されているコンテンツ・リストの中から、再生したいコンテンツを選択することができる。そして、コンテンツが選択されると、Ｓｏｕｒｃｅデバイスからデバイスへのコンテンツの伝送が開始されるが、コンテンツ伝送に先駆けて、ＳｉｎｋデバイスとＳｏｕｒｃｅデバイス間で、リモート・アクセス用の相互認証及び鍵交換すなわちＲＡ－ＡＫＥ処理が実施される。
【０１０６】
図１０には、ＤＴＣＰの仕様書（前述）のＶ１ＳＥ．１０．７．２節に記載されている、ＲＡ－ＡＫＥ手続きフェーズ（ＳＥＱ８０２）の中身の詳細を示している。
【０１０７】
Ｓｉｎｋデバイスは、リモート・アクセス用交換K_R（Ｒｅｍｏｔｅ　Ｅｘｃｈａｎｇｅ　Ｋｅｙ）用のビットが設定された交換鍵フィールドを含んだＣＨＡＬＬＥＮＧＥコマンドを送信して、Ｓｏｕｒｃｅデバイスに対してＡＫＥ処理を要求する（ＳＥＱ１００１）。そして、ＳｏｕｒｃｅデバイスとＳｉｎｋデバイス間で、認証手続きのうちチャレンジ・レスポンス部分が実行される（ＳＥＱ１００２～１００４）。
【０１０８】

但し、ＣＨＡＬＬＥＮＧＥコマンドのK_R用のビットが設定されていないときには、Ｓｏｕｒｃｅデバイスは－ＡＫＥ手続きを中止し、ＲＡ－ＡＫＥ以外のＡＫＥ手続きを引き続き行なうことができる。

【０１０９】

Ｓｏｕｒｃｅデバイスは、チャレンジ・レスポンス手続きでＳｉｎｋデバイスから、Ｄｅｖｉｃｅ　ＩＤ又はＩＤｕをＳｉｎｋ－ＩＤとして受け取ると（ＳＥＱ１００５）、そのＳｉｎｋ－ＩＤが自身の端末管理部３０７内で管理しているｒｅｍｏｔｅ　ｓｉｎｋ　ｒｅｇｉｓｔｒｙに登録されているかどうかをチェックする（ＳＥＱ１００６）。

【０１１０】

Ｓｉｎｋ－ＩＤがｒｅｍｏｔｅ　ｓｉｎｋ　ｒｅｇｉｓｔｒｙにリストされていない場合には（ＳＥＱ１００６のＮｏ）、Ｓｏｕｒｃｅデバイスは、ＳｉｎｋデバイスにＡＫＥ＿ＣＡＮＣＥＬコマンドを送信して（ＳＥＱ１０１４）、ＲＡ－ＡＫＥ手続きを中止する（ＳＥＱ１０１５）。

【０１１１】

一方、Ｓｉｎｋ－ＩＤがｒｅｍｏｔｅ　ｓｉｎｋ　ｒｅｇｉｓｔｒｙに既に登録されている場合には（ＳＥＱ１００６のＹｅｓ）、Ｓｏｕｒｃｅデバイスは、このＳｉｎｋ－ＩＤに該当するＲＡＣ　ｒｅｃｏｒｄが既に存在するかどうかを判別するために、ＲＡＣ　ｒｅｇｉｓｔｒｙ（後述）内をチェックする（ＳＥＱ１００７）。

【０１１２】

Ｓｉｎｋ－ＩＤに該当するＲＡＣ　ｒｅｃｏｒｄが存在する場合には（ＳＥＱ１００７のＹｅｓ）、Ｓｏｕｒｃｅデバイスは、そのＲＡＣ　ｒｅｃｏｒｄに格納されているリモート・アクセス用交換鍵K_R及びその交換鍵ラベルK_R＿ｌａｂｅｌを使うことに決定する。あるいは、Ｓｏｕｒｃｅデバイスは、リモート・アクセス用交換鍵K_Rを用いてコンテンツの伝送を行なっていないのであれば、ＲＡＣ　ｒｅｃｏｒｄ内を参照し、格納されているK_R及びK_R＿ｌａｂｅｌの値を更新するようにしてもよい（ＳＥＱ１０１３）。

【０１１３】

Ｓｉｎｋ－ＩＤはｒｅｍｏｔｅ　ｓｉｎｋ　ｒｅｇｉｓｔｒｙに登録済みであるが、該当するＲＡＣ　ｒｅｃｏｒｄが存在しない場合には（ＳＥＱ１００７のＮｏ）、Ｓｏｕｒｃｅデバイスは、ＲＡＣ　ｒｅｃｏｒｄをカウントするカウント値ＲＡＣＣが$RACC_{max}$未満であるかどうかをチェックする（ＳＥＱ１００８）。ここで、$RACC_{max}$は、リモート・アクセス・コネクションをカウントするカウンターであり、リモート・アクセス・コネクションが存在しないときにゼロに初期化される。

【０１１４】

ＲＡＣＣがその$RACC_{max}$未満でないときには（ＳＥＱ１００８のＮｏ）、Ｓｏｕｒｃｅデバイスは、ＳｉｎｋデバイスにＡＫＥ＿ＣＡＮＣＥＬコマンドを送信して（ＳＥＱ１０１４）、ＲＡ－ＡＫＥ手続きを中止する（ＳＥＱ１０１５）。

【０１１５】

ＲＡＣＣが$RACC_{max}$未満であれば（ＳＥＱ１００８のＹｅｓ）、Ｓｏｕｒｃｅデバイスは、ＲＡＣＣの値を１だけインクリメントした後（ＳＥＱ１００９）、所定の演算規則に従って、リモート・アクセス用交換鍵K_R及びその交換鍵ラベルK_R＿ｌａｂｅｌを生成して（ＳＥＱ１０１０）、これらをＳｉｎｋデバイスのＳｉｎｋ－ＩＤと対応付けて、ＲＡＣ　ｒｅｇｉｓｔｒｙ内のＲＡＣ　ｒｅｃｏｒｄに格納する（ＳＥＱ１０１１）。サーバー２０１は、例えば端末管理部３０７内でＲＡＣ　ｒｅｃｏｒｄを管理する。図１５には、Ｓｉｎｋデバイスに対して生成したリモート・アクセス用交換鍵K_R及びその交換鍵ラベルK_R＿ｌａｂｅｌをＳｉｎｋ－ＩＤと対応付けてＲＡＣ　ｒｅｃｏｒｄとして記憶する様子を示している。

【０１１６】

そして、Ｓｏｕｒｃｅデバイスは、既存のＲＡＣ　ｒｅｃｏｒｄから取り出したリモート・アクセス用交換鍵K_R及びその交換鍵ラベルK_R＿ｌａｂｅｌ（更新した場合を含む）、又は、新たに生成したリモート・アクセス用交換鍵K_R及びその交換鍵ラベルK_R＿ｌａ

ｂｅｌを、Ｓｉｎｋデバイスに送信する（ＳＥＱ１０１６）。
【０１１７】
Ｓｏｕｒｃｅデバイスが$RA_MANAGEMENT$機能をサポートしている場合には、リモート・アクセス用交換K_Rを維持するためのK_R用生存タイマーを開始させ、少なくとも１分間K_Rを保持する（ＳＥＱ１０１２）。
【０１１８】
図１０に示したＤＴＣＰの仕様書のＶ１ＳＥ．１０．７．２節に記載されているＲＡ－ＡＫＥ手続きでは、Ｓｏｕｒｃｅデバイスは、最初の条件判断ＳＥＱ１００６で、ＳｉｎｋデバイスのＳｉｎｋ－ＩＤがｒｅｍｏｔｅ　ｓｉｎｋ　ｒｅｇｉｓｔｒｙに登録されていることを確認した上でリモート・アクセス用交換鍵K_Rを共有する。
【０１１９】
上述したように、Ｓｏｕｒｃｅデバイスがｒｅｍｏｔｅ　ｓｉｎｋ　ｒｅｇｉｓｔｒｙに一度登録したＳｉｎｋ－ＩＤを保持し続けると、第三者の端末をサーバーに一度登録すれば、以後はその第三者がサーバー内のコンテンツを利用し続けることができてしまうという問題がある。
【０１２０】
そこで、本実施形態では、Ｓｏｕｒｃｅデバイスは、ｒｅｍｏｔｅ　ｓｉｎｋ　ｒｅｓｉｓｔｒｙに登録したＳｉｎｋ－ＩＤに登録日時からの有効期限を設定し（図６、図７を参照のこと）、有効期限が切れたＳｉｎｋ－ＩＤをｒｅｍｏｔｅ　ｓｉｎｋ　ｒｅｓｉｓｔｒｙから抹消することで、一旦登録した第三者が利用し続けることを防止し、私的利用の範囲を超えたコンテンツの利用を好適に抑制するようにしている。有効期限が切れたＳｉｎｋ－ＩＤの抹消処理は、例えばＳｏｕｒｃｅデバイス内で行なうことができる。
【０１２１】
図１１には、有効期限が切れたＳｉｎｋ－ＩＤをｒｅｍｏｔｅ　ｓｉｎｋ　ｒｅｓｉｓｔｒｙから抹消する処理を含んだ、ＲＡ－ＡＫＥ手続きフェーズ（ＳＥＱ８０２）の中身の詳細を示している。
【０１２２】
Ｓｉｎｋデバイスがリモート・アクセス用交換K_R用のビットが設定された交換鍵フィールドを含んだＣＨＡＬＬＥＮＧＥコマンドを送信して、Ｓｏｕｒｃｅデバイスに対してＡＫＥ処理を要求すると（ＳＥＱ１１０１）、ＳｏｕｒｃｅデバイスとＳｉｎｋデバイス間で、認証手続きのうちチャレンジ・レスポンス部分が実行される（ＳＥＱ１１０２～１１０４）。そして、Ｓｏｕｒｃｅデバイスは、チャレンジ・レスポンス手続きでＳｉｎｋデバイスから、Ｄｅｖｉｃｅ　ＩＤ又はＩＤｕをＳｉｎｋ－ＩＤとして受け取ることができる（ＳＥＱ１１０５）。
【０１２３】
ここで、Ｓｏｕｒｃｅデバイスは、ｒｅｍｏｔｅ　ｓｉｎｋ　ｒｅｓｉｓｔｒｙのメンテナンス、すなわち、有効期限が切れたＳｉｎｋ－ＩＤをｒｅｍｏｔｅ　ｓｉｎｋ　ｒｅｓｉｓｔｒｙから抹消する処理を実施する（ＳＥＱ１１０６）。登録日時を基準にして設定された有効期限が切れたＳｉｎｋ－ＩＤをｒｅｍｏｔｅ　ｓｉｎｋ　ｒｅｓｉｓｔｒｙから抹消することで、一旦登録した第三者が利用し続けることを防止する。ｒｅｍｏｔｅ　ｓｉｎｋ　ｒｅｓｉｓｔｒｙのメンテナンス処理が実施された後は、有効期限内のエントリーのみが残っているものとする。ｒｅｍｏｔｅ　ｓｉｎｋ　ｒｅｓｉｓｔｒｙのメンテナンス処理の詳細については、後述に譲る。
【０１２４】
次いで、Ｓｏｕｒｃｅデバイスは、受け取ったＳｉｎｋ－ＩＤが自身の端末管理部３０７内で管理しているｒｅｍｏｔｅ　ｓｉｎｋ　ｒｅｇｉｓｔｒｙにリストされているかどうかをチェックする（ＳＥＱ１１０７）。
【０１２５】
Ｓｉｎｋ－ＩＤがｒｅｍｏｔｅ　ｓｉｎｋ　ｒｅｇｉｓｔｒｙにリストされていない場合には（ＳＥＱ１１０７のＮｏ）、Ｓｏｕｒｃｅデバイスは、ＳｉｎｋデバイスにＡＫＥ

＿ＣＡＮＣＥＬコマンドを送信して（ＳＥＱ１１１６）、ＲＡ－ＡＫＥ手続きを中止する（ＳＥＱ１１１７）。

【０１２６】

一方、Ｓｉｎｋ－ＩＤがｒｅｍｏｔｅ　ｓｉｎｋ　ｒｅｇｉｓｔｒｙにリストされている場合には（ＳＥＱ１１０７のＹｅｓ）、Ｓｏｕｒｃｅデバイスは、このＳｉｎｋ－ＩＤに該当するＲＡＣ　ｒｅｃｏｒｄが既に存在するかどうかを判別するために、ＲＡＣ　ｒｅｇｉｓｔｒｙ（後述）内をチェックする（ＳＥＱ１１０８）。

【０１２７】

Ｓｉｎｋ－ＩＤに該当するＲＡＣ　ｒｅｃｏｒｄが存在する場合には（ＳＥＱ１１０８のＹｅｓ）、Ｓｏｕｒｃｅデバイスは、そのＲＡＣ　ｒｅｃｏｒｄに格納されているリモート・アクセス用交換鍵K_R及びその交換鍵ラベルK_R＿ｌａｂｅｌを使うことに決定する。あるいは、Ｓｏｕｒｃｅデバイスは、リモート・アクセス用交換鍵K_Rを用いてコンテンツの伝送を行なっていないのであれば、ＲＡＣ　ｒｅｃｏｒｄ内を参照し、格納されているK_R及びK_R＿ｌａｂｅｌの値を更新するようにしてもよい（ＳＥＱ１１１４）。

【０１２８】

Ｓｉｎｋ－ＩＤはｒｅｍｏｔｅ　ｓｉｎｋ　ｒｅｇｉｓｔｒｙにリストされているが、該当するＲＡＣ　ｒｅｃｏｒｄが存在しない場合には（ＳＥＱ１１０８のＮｏ）、Ｓｏｕｒｃｅデバイスは、ＲＡＣ　ｒｅｃｏｒｄをカウントするカウント値ＲＡＣＣが$RACC_{max}$未満であるかどうかをチェックする（ＳＥＱ１１０９）。

【０１２９】

ＲＡＣＣがその$RACC_{max}$未満でないときには（ＳＥＱ１１０９のＮｏ）、Ｓｏｕｒｃｅデバイスは、ＳｉｎｋデバイスにＡＫＥ＿ＣＡＮＣＥＬコマンドを送信して（ＳＥＱ１１１５）、ＲＡ－ＡＫＥ手続きを中止する（ＳＥＱ１１１６）。

【０１３０】

ＲＡＣＣが$RACC_{max}$未満であれば（ＳＥＱ１１０９のＹｅｓ）、Ｓｏｕｒｃｅデバイスは、ＲＡＣＣの値を１だけインクリメントした後（ＳＥＱ１１１０）、所定の演算規則に従って、リモート・アクセス用交換鍵K_R及びその交換鍵ラベルK_R＿ｌａｂｅｌを生成して（ＳＥＱ１１１１）、これらをＳｉｎｋデバイスのＳｉｎｋ－ＩＤと対応付けて、ＲＡＣ　ｒｅｇｉｓｔｒｙ内のＲＡＣ　ｒｅｃｏｒｄに格納する（ＳＥＱ１１１２）。サーバー２０１は、例えば端末管理部３０７内でＲＡＣ　ｒｅｃｏｒｄを管理する。図１５には、Ｓｉｎｋデバイスに対して生成したリモート・アクセス用交換鍵K_R及びその交換鍵ラベルK_R＿ｌａｂｅｌをＳｉｎｋ－ＩＤと対応付けてＲＡＣ　ｒｅｃｏｒｄとして記憶する様子を示している。

【０１３１】

そして、Ｓｏｕｒｃｅデバイスは、既存のＲＡＣ　ｒｅｃｏｒｄから取り出したリモート・アクセス用交換鍵K_R及びその交換鍵ラベルK_R＿ｌａｂｅｌ（更新した場合を含む）、又は、新たに生成したリモート・アクセス用交換鍵K_R及びその交換鍵ラベルK_R＿ｌａｂｅｌを、Ｓｉｎｋデバイスに送信する（ＳＥＱ１１１７）。また、ＳｏｕｒｃｅデバイスがＲＡ＿ＭＡＮＡＧＥＭＥＮＴ機能をサポートしている場合には、リモート・アクセス用交換K_Rを維持するためのK_R用生存タイマーを開始させ、少なくとも１分間K_Rを保持する（ＳＥＱ１１１３）。

【０１３２】

ＳＥＱ１１０６で実施されるｒｅｍｏｔｅ　ｓｉｎｋ　ｒｅｇｉｓｔｒｙのメンテナンス処理では、Ｓｉｎｋ－ＩＤと有効期限をペアにして格納したｒｅｍｏｔｅ　ｓｉｎｋ　ｒｅｇｉｓｔｒｙの登録内容（図７を参照のこと）を参照して、登録日時を基準にして設定された有効期限が切れたＳｉｎｋ－ＩＤのエントリーをｒｅｍｏｔｅ　ｓｉｎｋ　ｒｅｓｉｓｔｒｙから抹消する。このメンテナンス処理は、Ｓｏｕｒｃｅデバイスとしてのサーバー２０１内で行なうことができるが、クラウド上などに置かれた管理用サーバーで一元的に端末の登録日時や有効期限の情報の管理とともに行なうようにしてもよい。

【０１３３】

図１２には、ｒｅｍｏｔｅ　ｓｉｎｋ　ｒｅｇｉｓｔｒｙのメンテナンス処理の手順をフローチャートの形式で示している。以下では、便宜上、Ｓｏｕｒｃｅデバイスとしてのサーバー２０１内でメンテナンス処理を行なうものとして説明する。このメンテナンス処理は、例えばサーバー２０１内の認証・鍵共有部３０６が、ＲＡ－ＡＫＥ手続きフェーズの中で実施する。

【０１３４】

サーバー２０１は、端末管理部３０７内で管理しているｒｅｍｏｔｅ　ｓｉｎｋ　ｒｅｇｉｓｔｒｙ中で、有効期限を未確認のＳｉｎｋデバイスに関して（ステップＳ１２０１のＮｏ）、そのＳｉｎｋ－ＩＤとペアにして記憶されている有効期限を参照し（ステップＳ１２０２）、現在日時が有効期限を過ぎていないかどうかをチェックする（ステップＳ１２０３）。そして、現在日時が有効期限を過ぎているＳｉｎｋ－ＩＤのエントリーを（ステップＳ１２０３のＹｅｓ）、ｒｅｍｏｔｅ　ｓｉｎｋ　ｒｅｇｉｓｔｒｙから削除する（ステップＳ１２０４）。

【０１３５】

そして、サーバー２０１は、ｒｅｍｏｔｅ　ｓｉｎｋ　ｒｅｇｉｓｔｒｙ内に登録されているすべてのＳｉｎｋのエントリーについてステップＳ１２０２～Ｓ１２０４の処理を終了するまで（ステップＳ１２０１のＹｅｓ）、繰り返し実行する。

【０１３６】

図１２に示したｒｅｍｏｔｅ　ｓｉｎｋ　ｒｅｇｉｓｔｒｙのメンテナンス処理は、各サーバー２０１が個別に実施する（言い換えれば、サーバー２０１が設置されたホーム・ネットワーク２１０単位で実施する）のではなく、クラウド上の管理サーバーなどで各家庭のサーバー２０１のｒｅｍｏｔｅ　ｓｉｎｋ　ｒｅｇｉｓｔｒｙを一元的に集中管理するようにしてもよい。

【０１３７】

また、図１２に示したようなｒｅｍｏｔｅ　ｓｉｎｋ　ｒｅｇｉｓｔｒｙのメンテナンス処理を、ＲＡ－ＡＫＥ手続き時に逐次行なうのではなく、サーバー２０１又はクラウド上の管理サーバーなどが、（ＲＡ－ＡＫＥ手続きを実施するか否かに拘わらず）定期的に行なうようにしてもよい。

【０１３８】

また、図１１及び図１２では、１回のメンテナンス処理でｒｅｍｏｔｅ　ｓｉｎｋ　ｒｅｇｉｓｔｒｙ内のすべてのエントリーについて有効期限の確認処理を実行するようになっているが、ＲＡ－ＡＫＥ手続きの対象となっているＳｉｎｋ－ＩＤに対応するエントリーについてのみ有効期限の確認処理（有効期限を過ぎたエントリーの抹消処理）を行なうだけでもよい。

【０１３９】

また、ＲＡ－ＡＫＥ手続きフェーズで有効期限が過ぎた端末のレコードの抹消処理を行なう代わりに、後段のコンテンツ伝送フェーズで有効期限を過ぎた端末へのコンテンツの送信を制限する「コンテンツ出力管理」を含めるようにしてもよい。この場合、図１１ではなく、抹消処理を含まない図１０に示した手順に従ってＲＡ－ＡＫＥ手続きを実施して、有効期限に拘わらず、すべてのＳｉｎｋデバイスにリモート・アクセス用交換鍵K_R及びその交換鍵ラベル$K_{R_}$ｌａｂｅｌを配布しておく。そして、ＳＥＱ８０３のコンテンツ伝送フェーズにおいて、要求元Ｓｉｎｋデバイスの有効期限のチェックを行なうようにする。

【０１４０】

図１８には、有効期限に基づくコンテンツの出力管理を含んだコンテンツ伝送フェーズ（ＳＥＱ８０３）の中身を模式的に示している。

【０１４１】

Ｓｉｎｋデバイスは、ＲＡ－ＡＫＥ手続により取得したリモート・アクセス用交換鍵K_R及びその交換鍵ラベル$K_{R_}$ｌａｂｅｌを取得した後に、例えば、ＨＴＴＰ　ＧＥＴメソッドを用いたＨＴＴＰリクエスト（ＨＴＴＰ　ＧＥＴ　ｒｅｑｕｅｓｔ）により、Ｓｏｕ

ｒｃｅデバイスに対して、コンテンツの伝送を要求する（ＳＥＱ１８０１）。この要求の際には、コンテンツのＵＲＬ（Ｕｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒ）とともに、リモート・アクセス用交換鍵K_RのＩＤであるラベルK_R＿ｌａｂｅｌを送る。ここで、ＳｉｎｋデバイスからＳｏｕｒｃｅデバイスに交換鍵のＩＤ（K_R＿ｌａｂｅｌ）を送るためのヘッダー・フィールドを定義する。

【０１４２】

ここで、Ｓｏｕｒｃｅデバイスは、Ｓｉｎｋデバイスからコンテンツの伝送要求を受けると、有効期限に基づくコンテンツ出力管理の処理を実行する（ＳＥＱ１８０２）。

【０１４３】

Ｓｏｕｒｃｅデバイスは、ＲＡ－ＡＫＥ手続きにおいて、リモート・アクセス用交換鍵K_R及びその交換鍵ラベルK_R＿ｌａｂｅｌをＳｉｎｋデバイスに送る際に、これらをＳｉｎｋ－ＩＤと対応付けてＲＡＣ　ｒｅｃｏｒｄとして記憶している（前述並びに図１５を参照のこと）。したがって、Ｓｏｕｒｃｅデバイスは、コンテンツ要求に含まれる交換鍵ラベルK_R＿ｌａｂｅｌに該当するＲＡＣ　Ｒｅｃｏｒｄから、要求元ＳｉｎｋデバイスのＳｉｎｋ－ＩＤを調べることができる。

【０１４４】

また、Ｓｏｕｒｃｅデバイスは、Ｓｉｎｋデバイスの登録時、すなわち、Ｓｉｎｋ－ＩＤをｒｅｍｏｔｅ　ｓｉｎｋ　ｒｅｇｉｓｔｒｙに登録する際に、有効期限を算出して、Ｓｉｎｋ－ＩＤとペアにして記憶している（前述並びに図７を参照のこと）。したがって、ＲＡＣ　Ｒｅｃｏｒｄから得たＳｉｎｋ－ＩＤに基づいて、そのＳｉｎｋデバイスの有効期限を調べることができる。

【０１４５】

そして、Ｓｏｕｒｃｅデバイスは、現在日時が要求元Ｓｉｎｋデバイスの有効期限を過ぎていなければコンテンツ要求を許可するが、現在日時が有効期限を過ぎているときにはコンテンツ要求を許可しない。また、Ｓｏｕｒｃｅデバイスは、有効期限を過ぎたＳｉｎｋデバイスのエントリーをｒｅｍｏｔｅ　ｓｉｎｋ　ｒｅｇｉｓｔｒｙから削除するようにしてもよい。

【０１４６】

Ｓｏｕｒｃｅデバイスは、Ｓｉｎｋデバイスからのコンテンツ要求を許可する場合には、交換鍵ラベルK_R＿ｌａｂｅｌで指定されたリモート・アクセス用交換鍵K_RをＲＡＣ　ｒｅｃｏｒｄから取り出すと、これ用いてコンテンツを暗号化して、ＨＴＴＰレスポンス（ＨＴＴＰ　ＧＥＴ　ｒｅｓｐｏｎｓｅ）としてＳｉｎｋデバイスに伝送する（ＳＥＱ１８０３）。

【０１４７】

図１９には、ＳＥＱ１８０２において実施するコンテンツ出力管理の処理手順をフローチャートの形式で示している。以下では、便宜上、Ｓｏｕｒｃｅデバイスとしてのサーバー２０１内で、例えばコンテンツ提供部３０４がコンテンツ出力管理処理を行なうものとして説明する。

【０１４８】

サーバー２０１は、コンテンツ要求（ＨＴＴＰ　ＧＥＴ　ｒｅｑｕｅｓｔ）に含まれる交換鍵ラベルK_R＿ｌａｂｅｌを参照し（ステップＳ１９０１）、同じ交換鍵ラベルK_R＿ｌａｂｅｌのＲＡＣ　ｒｅｃｏｒｄが端末管理部３０７内に存在するかどうかをチェックする（ステップＳ１９０２）。

【０１４９】

ここで、同じ交換鍵ラベルK_R＿ｌａｂｅｌのＲＡＣ　ｒｅｃｏｒｄが存在しない場合には（ステップＳ１９０２のＮｏ）、要求元のＳｉｎｋデバイスがＲＡ－ＡＫＥ手続きを行なっていないなどの原因により、不正なコンテンツ要求である。そこで、サーバー２０１は、後続の処理をすべてスキップして、本処理ルーチンを終了する。

【０１５０】

一方、同じ交換鍵ラベルK_R＿ｌａｂｅｌのＲＡＣ　ｒｅｃｏｒｄが存在する場合には

（ステップＳ１９０２のＹｅｓ）、サーバー２０１は、そのＲＡ　ｒｅｃｏｒｄから、交換鍵ラベルK_{R}＿ｌａｂｅｌに対応するＳｉｎｋ－ＩＤを取得する（ステップＳ１９０３）。

【０１５１】

次いで、サーバー２０１は、端末管理部３０７内のｒｅｍｏｔｅ　ｓｉｎｋ　ｒｅｇｉｓｔｒｙから、Ｓｉｎｋ－ＩＤとペアにして記憶されている有効期限を取得する（ステップＳ１９０４）。但し、各Ｓｉｎｋ－ＩＤの有効期限を例えばクラウド上の管理サーバーに委ねている場合には、サーバー２０１は、通信・制御部３０１を介して管理サーバーにアクセスして、該当する有効期限の情報を取得する。

【０１５２】

そして、サーバー２０１は、現在日時を取得し（ステップＳ１９０５）、現在日時が要求元のＳｉｎｋデバイスの有効期限を過ぎていないかどうかをチェックする（ステップＳ１９０６）。現在日時が有効期限を過ぎている場合には（ステップＳ１９０６のＹｅｓ）、該当するＳｉｎｋ－ＩＤのエントリーを、ｒｅｍｏｔｅ　ｓｉｎｋ　ｒｅｇｉｓｔｒｙから削除して（ステップＳ１９０７）、本処理ルーチンを終了する。

【０１５３】

一方、現在日時が要求元のＳｉｎｋデバイスの有効期限を過ぎていないときには（ステップＳ１９０６のＮｏ）、サーバー２０１は、Ｓｉｎｋデバイスからのコンテンツ要求を許可し、要求されたコンテンツの送信を例えばＨＴＴＰ　ＧＥＴ　ｒｅｓｐｏｎｓｅで行なう（ステップＳ１９０８）。

【０１５４】

このように、端末のサーバーへの登録日時に第１の所定の期間を加算した有効期限を設定し、有効期限内の端末に対してのみサーバー内のコンテンツへのリモート・アクセスを許可し、有効期限を経過した以降はリモート・アクセスを禁止することにより、第三者による私的利用の範囲を超えたコンテンツの利用を抑制することができる。

【０１５５】

Ｄ．登録日時に基づくリモート・アクセスの制限（２）

サーバー２０１が、登録日時に基づいて端末２０２からのリモート・アクセスを制限する他の方法として、登録日時から第２の所定期間α（例えば、３日間）を端末２０２がリモート・アクセス可能なコンテンツの限界日時として設定する方法が挙げられる。例えば、端末２０２が持つ限界日時より以前にコンテンツ記録部３０２に記録されたコンテンツのリモート・アクセスは許可されるが、限界日時以降に記録されたコンテンツのリモート・アクセスは許可されない。また、限界日時より以前にコンテンツ取得部３０３が取得するコンテンツのリモート・アクセスは許可されるが、限界日時以降にコンテンツ取得部３０３が取得するコンテンツのリモート・アクセスは許可されない。

【０１５６】

サーバー２０１は、例えば、端末２０２をｒｅｍｏｔｅ　ｓｉｎｋ　ｒｅｇｉｓｔｒｙに登録する際に、現在日時に第２の所定期間αを加算してその端末２０２の限界日時を算出して、Ｓｉｎｋ－ＩＤとともに限界日時をペアにして記憶するようにすればよい。

【０１５７】

図１３には、リモート・アクセスを行なうＳｉｎｋデバイスを、限界日時とともにＳｏｕｒｃｅデバイスに登録する手順を図解している。

【０１５８】

まず、ＳｏｕｒｃｅデバイスとＳｉｎｋデバイス間で、ＲＴＴ（Ｒｏｕｎｄ　Ｔｒｉｐ　Ｔｉｍｅ）の制限下で、ＡＫＥ手続きが実施される（ＳＥＱ１３０１）。そして、ＲＴＴ－ＡＫＥ手続きに成功裏に終了すると、Ｓｉｎｋデバイスは、コマンドＲＡ＿ＲＥＧＩＳＴＥＲ．ＣＭＤを用いて、自分のＳｉｎｋ－ＩＤをＳｏｕｒｃｅデバイスに送信する（ＳＥＱ１３０２）。

【０１５９】

Ｓｏｕｒｃｅデバイスは、ＲＡ＿ＲＥＧＩＳＴＥＲ．ＣＭＤで受け取ったＳｉｎｋ－Ｉ

Dが、直前に完了したＲＴＴ－ＡＫＥ手続で受信したＤｅｖｉｃｅ　ＩＤ又はＩＤｕと一致し、ｒｅｍｏｔｅ　ｓｉｎｋ　ｒｅｇｉｓｔｒｙにまだ記憶しておらず、且つ、ｒｅｍｏｔｅ　ｓｉｎｋ　ｒｅｇｉｓｔｒｙが満杯でないかどうかをチェックする。そして、これらの条件をクリアし、Ｓｉｎｋ－ＩＤをｒｅｍｏｔｅ　ｓｉｎｋ　ｒｅｇｉｓｔｒｙに追加記憶するときには、Ｓｏｕｒｃｅデバイスは、コマンドＲＡ＿ＲＥＧＩＳＴＥＲ．ＲＳＰでＳｉｎｋデバイスに返す（ＳＥＱ１３０３）。

【０１６０】

また、Ｓｏｕｒｃｅデバイスは、Ｓｉｎｋデバイスの登録日時として現在日時を取得すると（ＳＥＱ１３０４）、Ｓｉｎｋデバイスの登録の限界日時としての第２の所定の期間α（例えば、３日間）を現在日時に加算して限界日時を算出して（ＳＥＱ１３０５）、Ｓｉｎｋ－ＩＤと限界のペアを、ｒｅｍｏｔｅ　ｓｉｎｋ　ｒｅｇｉｓｔｒｙに記憶する（ＳＥＱ１３０６）。

【０１６１】

図１４には、Ｓｉｎｋ－ＩＤと限界日時をペアにして格納したｒｅｍｏｔｅ　ｓｉｎｋ　ｒｅｇｉｓｔｒｙの登録内容を例示している。但し、図１４に示したような端末の登録日時や限界日時の情報の管理を、ホーム・ネットワーク２１０上のサーバー２０１内で個別に行なうのではなく、クラウド上などに置かれた管理用サーバーで一元的に行なうようにしてもよい。

【０１６２】

なお、Ｓｏｕｒｃｅデバイス（サーバー２０１）は、登録日時としての現在日時を、例えば、サーバー内蔵の時計機能（図３では図示を省略）、放送波に含まれる時刻信号（例えば、コンテンツ取得部３０３がチューナー機能を装備して放送波を受信する場合）、ネットワーク上のサーバー（図示しない）から得た時刻情報などから取得することができる。

【０１６３】

コンテンツ伝送に先駆けて、ＳｉｎｋデバイスとＳｏｕｒｃｅデバイス間で、リモート・アクセス用の相互認証及び鍵交換すなわちＲＡ－ＡＫＥ処理が実施された後に、コンテンツ伝送が開始される。

【０１６４】

図１６には、リモート・アクセス用交換鍵K_Rを用いて暗号化伝送するコンテンツ伝送フェーズ（ＳＥＱ８０３）の中身を模式的に示している。図示のシーケンスには、限界日時に基づくコンテンツ出力管理の処理が含まれている。

【０１６５】

Ｓｉｎｋデバイスは、ＲＡ－ＡＫＥ手続により取得したリモート・アクセス用交換鍵K_R及びその交換鍵ラベルK_R＿ｌａｂｅｌを取得した後に、例えば、ＨＴＴＰ　ＧＥＴメソッドを用いたＨＴＴＰリクエスト（ＨＴＴＰ　ＧＥＴ　ｒｅｑｕｅｓｔ）により、Ｓｏｕｒｃｅデバイスに対して、コンテンツの伝送を要求する（ＳＥＱ１６０１）。この要求の際には、コンテンツのＵＲＬ（Ｕｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒ）とともに、リモート・アクセス用交換鍵K_RのＩＤであるラベルK_R＿ｌａｂｅｌを送る。ここで、ＳｉｎｋデバイスからＳｏｕｒｃｅデバイスに交換鍵のＩＤ（K_R＿ｌａｂｅｌ）を送るためのヘッダー・フィールドを定義する。

【０１６６】

ここで、Ｓｏｕｒｃｅデバイスは、Ｓｉｎｋデバイスからコンテンツの伝送要求を受けると、限界日時に基づくコンテンツ出力管理の処理を実行する（ＳＥＱ１６０２）。

【０１６７】

Ｓｏｕｒｃｅデバイスは、ＲＡ－ＡＫＥ手続きにおいて、リモート・アクセス用交換鍵K_R及びその交換鍵ラベルK_R＿ｌａｂｅｌをＳｉｎｋデバイスに送る際に、これらをＳｉｎｋ－ＩＤと対応付けてＲＡＣ　ｒｅｃｏｒｄとして記憶している（前述並びに図１５を参照のこと）。したがって、Ｓｏｕｒｃｅデバイスは、コンテンツ要求に含まれる交換鍵ラベルK_R＿ｌａｂｅｌに該当するＲＡＣ　Ｒｅｃｏｒｄから、要求元Ｓｉｎｋデバイス

のＳｉｎｋ－ＩＤを調べることができる。

【０１６８】

また、Ｓｏｕｒｃｅデバイスは、Ｓｉｎｋデバイスの登録時、すなわち、Ｓｉｎｋ－ＩＤをｒｅｍｏｔｅ　ｓｉｎｋ　ｒｅｇｉｓｔｒｙに登録する際に、限界日時を算出して、Ｓｉｎｋ－ＩＤとペアにして記憶している（前述並びに図１４を参照のこと）。したがって、ＲＡＣ　Ｒｅｃｏｒｄから得たＳｉｎｋ－ＩＤに基づいて、そのＳｉｎｋデバイスの限界日時を調べることができる。

【０１６９】

そして、Ｓｏｕｒｃｅデバイスは、要求元Ｓｉｎｋデバイスが持つ限界日時より以前にＳｏｕｒｃｅデバイスに記録されたコンテンツであれば、Ｓｉｎｋデバイスからのコンテンツ要求を許可するが、限界日時を経過した以降にＳｏｕｒｃｅデバイスに記録されたコンテンツについては、Ｓｉｎｋデバイスからのコンテンツ要求を許可しない。

【０１７０】

Ｓｏｕｒｃｅデバイスは、Ｓｉｎｋデバイスからのコンテンツ要求を許可する場合には、交換鍵ラベルK_R＿ｌａｂｅｌで指定されたリモート・アクセス用交換鍵K_RをＲＡＣ　ｒｅｃｏｒｄから取り出すと、これ用いてコンテンツを暗号化して、ＨＴＴＰレスポンス（ＨＴＴＰ　ＧＥＴ　ｒｅｓｐｏｎｓｅ）としてＳｉｎｋデバイスに伝送する（ＳＥＱ１６０３）。

【０１７１】

図１７には、ＳＥＱ１６０２において実施するコンテンツ出力管理処理の手順をフローチャートの形式で示している。以下では、便宜上、Ｓｏｕｒｃｅデバイスとしてのサーバー２０１内で、例えばコンテンツ提供部３０４がコンテンツ出力管理処理を行なうものとして説明する。

【０１７２】

サーバー２０１は、コンテンツ要求（ＨＴＴＰ　ＧＥＴ　ｒｅｑｕｅｓｔ）に含まれる交換鍵ラベルK_R＿ｌａｂｅｌを参照し（ステップＳ１７０１）、同じ交換鍵ラベルK_R＿ｌａｂｅｌのＲＡＣ　ｒｅｃｏｒｄが端末管理部３０７内に存在するかどうかをチェックする（ステップＳ１７０２）。

【０１７３】

ここで、同じ交換鍵ラベルK_R＿ｌａｂｅｌのＲＡＣ　ｒｅｃｏｒｄが存在しない場合には（ステップＳ１７０２のＮｏ）、要求元のＳｉｎｋデバイスがＲＡ－ＡＫＥ手続きを行なっていないなどの原因により、不正なコンテンツ要求である。そこで、サーバー２０１は、後続の処理をすべてスキップして、本処理ルーチンを終了する。

【０１７４】

一方、同じ交換鍵ラベルK_R＿ｌａｂｅｌのＲＡＣ　ｒｅｃｏｒｄが存在する場合には（ステップＳ１７０２のＹｅｓ）、サーバー２０１は、そのＲＡ　ｒｅｃｏｒｄから、交換鍵ラベルK_R＿ｌａｂｅｌに対応するＳｉｎｋ－ＩＤを取得する（ステップＳ１７０３）。

【０１７５】

次いで、サーバー２０１は、端末管理部３０７内のｒｅｍｏｔｅ　ｓｉｎｋ　ｒｅｇｉｓｔｒｙから、Ｓｉｎｋ－ＩＤとペアにして記憶されている限界日時を取得する（ステップＳ１７０４）。但し、各Ｓｉｎｋ－ＩＤの限界日時を例えばクラウド上の管理サーバーに委ねている場合には、サーバー２０１は、通信・制御部３０１を介して管理サーバーにアクセスして、該当する限界日時の情報を取得する。

【０１７６】

また、サーバー２０１は、コンテンツ要求（ＨＴＴＰ　ＧＥＴ　ｒｅｑｕｅｓｔ）で要求されているコンテンツがコンテンツ記録部３０２に記録された記録日時を、ファイル・システムから取得する（ステップＳ１７０５）。但し、要求されているコンテンツが、放送コンテンツなどコンテンツ取得部３０４で取得するコンテンツの場合には、その取得日時として現在日時（受信日時）を取得する。

【０１７７】
そして、サーバー２０１は、コンテンツ要求されているコンテンツの記録日時又は取得日時が、Ｓｉｎｋデバイスに設定されている限界日時を超えていないかどうかをチェックする（ステップＳ１７０６）。
【０１７８】
コンテンツの記録日時又は取得日時がＳｉｎｋデバイスの限界日時を超えていないときには（ステップＳ１７０６のＹｅｓ）、サーバー２０１は、Ｓｉｎｋデバイスからのコンテンツ要求を許可し、次ステップＳ１７０７で、要求されたコンテンツの送信を例えばＨＴＴＰ　ＧＥＴ　ｒｅｓｐｏｎｓｅで行なう。
【０１７９】
また、コンテンツの記録日時又は取得日時がＳｉｎｋデバイスの限界日時を超えているときには（ステップＳ１７０６のＮｏ）、サーバー２０１は、Ｓｉｎｋデバイスからのコンテンツ要求を許可せず、後続の処理をスキップして、本処理ルーチンを終了する。
【０１８０】
このように、端末のサーバーへの登録日時に第２の所定の期間を加算した限界日時を設定して、端末がリモート・アクセスにより利用可能なコンテンツを、限界日時以前に記録されたコンテンツ又は限界日時以前に取得されたコンテンツだけに制限することにより、第三者による私的利用の範囲を超えたコンテンツの利用を好適に抑制することができる。
【０１８１】
なお、限界日時に基づくリモート・アクセスの制限を、コンテンツ・リスト閲覧フェーズ（ＳＥＱ８０１）で行なうこともできる。
【０１８２】
図２４には、コンテンツ・リスト閲覧フェーズ（ＳＥＱ８０１）において、Ｓｏｕｒｃｅデバイスが、リモート・アクセスするＳｉｎｋデバイスに対して、Ｓｉｎｋデバイスの限界日時に基づいてＣＤＳ情報の提供を制限するための処理手順をフローチャートの形式で示している。
【０１８３】
まず、Ｓｏｕｒｃｅデバイスは、提供可能なコンテンツ情報をクリアする（ステップＳ２４０１）。次いで、Ｓｏｕｒｃｅデバイスは、要求元のＳｉｎｋデバイスのＳｉｎｋ－ＩＤに対応する限界日時を、ｒｅｍｏｔｅ　ｓｉｎｋ　ｒｅｇｉｓｔｒｙから取得する（ステップＳ２４０２）。
【０１８４】
そして、Ｓｏｕｒｃｅデバイスは、すべてのコンテンツ情報を処理するまで（ステップＳ２４０３のＮｏ）、コンテンツ情報の作成を行なう。すなわち、Ｓｏｕｒｃｅデバイスは、未処理のコンテンツのコンテンツ情報を参照すると（ステップＳ２４０４）、そのコンテンツがコンテンツ記録部３０２に記録された記録日時を、ファイル・システムから取得する（ステップＳ２４０５）。但し、要求されているコンテンツが、放送コンテンツなどコンテンツ取得部３０４で取得するコンテンツの場合には、その取得日時として現在日時（受信日時）を取得する。
【０１８５】
そして、Ｓｏｕｒｃｅデバイスは、そのコンテンツの記録日時又は取得日時が、Ｓｉｎｋデバイスに設定されている限界日時を超えていないかどうかをチェックする（ステップＳ２４０６）。
【０１８６】
そのコンテンツの記録日時又は取得日時がＳｉｎｋデバイスの限界日時を超えていないときには（ステップＳ２４０６のＹｅｓ）、Ｓｏｕｒｃｅデバイスは、このコンテンツ情報を提供可能なコンテンツ情報に追加する（ステップＳ２４０７）。そして、ステップＳ２４０３に戻り、すべてのコンテンツ情報を処理したかどうかをチェックする。
【０１８７】
一方、そのコンテンツの記録日時又は取得日時がＳｉｎｋデバイスの限界日時を超えて

いるときには（ステップＳ２４０６のＮｏ）、Ｓｏｕｒｃｅデバイスは、このコンテンツ情報を提供可能なコンテンツ情報に追加することなく、ステップＳ２４０３に戻り、すべてのコンテンツ情報を処理したかどうかをチェックする。

【０１８８】

そして、すべてのコンテンツ情報の処理が終了したときには（ステップＳ２４０３のＹｅｓ）、Ｓｏｕｒｃｅデバイスは、完成したコンテンツ情報を、要求元のＳｉｎｋデバイスに送信する（ステップＳ２４０８）。

【０１８９】

このように、限界日時以前に記録されたコンテンツ又は限界日時以前に取得されたコンテンツだけに制限して、Ｓｉｎｋデバイスにコンテンツ情報を提供することによっても、第三者による私的利用の範囲を超えたコンテンツの利用を好適に抑制することができる。

【０１９０】

Ｅ．登録日時に基づくリモート・アクセスの制限の緩和

上記のＣ項並びにＤ項では、端末２０２をサーバー２０１に登録した登録日時に基づいて設定した有効期限又は限界日時を用いて端末２０２からのリモート・アクセスを制限することによって、一旦登録した第三者が利用し続けることを防止し、私的利用の範囲を超えたコンテンツの利用を抑制するようにしている。

【０１９１】

ところが、サーバー２０１に登録するすべての端末に対して、登録日時に基づくリモート・アクセスの制限を課すと、第三者による利用を抑制できる反面、正規のユーザーによる正当な（すなわち、私的利用の範囲内での）コンテンツの利用まで不必要に制限され、ユーザーに不便を感じさせてしまうおそれがある。ユーザーに不便を与えると、せっかくの通信システム２００の利用が普及しなくなってしまう。

【０１９２】

そこで、サーバー２０１に登録する所定の台数の端末については、登録日時に基づくリモート・アクセスの制限の適用を免除するようにしてもよい。

【０１９３】

この場合、図１１ではなく図１０に示した手順に従ってＲＡ－ＡＫＥ手続きを実施して、有効期限による登録抹消処理を行なうことなしに、すべてのＳｉｎｋデバイスにリモート・アクセス用交換鍵K_R及びその交換鍵ラベルK_{R_label}を配布しておく。そして、ＳｉｎｋデバイスをＳｏｕｒｃｅデバイスに登録する手続きにおいて（図６、図１３を参照のこと）、所定の台数の端末については、有効期限や限界日時として大きな値、又は、有効期限や限界日時が免除されていることを示す特定の値を設定する。このようにすれば、コンテンツ伝送フェーズ（図１８、図１６を参照のこと）におけるコンテンツ出力管理処理では（図１９、図１７を参照のこと）、ステップＳ１９０５、ステップＳ１７０６において、有効期限や限界日時による制限が適用されないようにすることができる。

【０１９４】

所定台数の端末までは、サーバーへの登録日時に基づくリモート・アクセスの制限を免除することにより、私的利用の範囲内でのコンテンツの利用の利便性を確保することができる。

【０１９５】

また、図２２並びに図２４には、コンテンツ・リスト閲覧フェーズ（ＳＥＱ８０１）において、リモート・アクセスするＳｉｎｋデバイスに対して、有効期限や限界日時に基づいてＣＤＳ情報の提供を制限するための処理手順を示した。この場合も同様に、所定台数の端末まではサーバーへの登録日時に基づく制限なしにＣＤＳ情報の提供を行なうことにより、私的利用の範囲内でのコンテンツの利用の利便性を確保することができる。

【０１９６】

また、登録日時に基づくリモート・アクセスの制限の適用を免除する端末を、サーバー２０１内に記録しているコンテンツ毎、あるいはコンテンツのグループ毎に設定するようにしてもよい。

【０１９７】
例えば、ユーザーがサーバー２０１に対しコンテンツの記録予約や記録要求を行なう際に、端末管理部３０７内（すなわち、ｒｅｍｏｔｅ　ｓｉｎｋ　ｒｅｇｉｓｔｒｙ）に登録されている利用可能な端末の中から、制限の適用を免除する端末を選択する方法や、ユーザー毎に制限の適用を免除する端末のＳｉｎｋ－ＩＤを登録しておくことで、コンテンツの記録予約や記録要求の操作を行なったユーザーの端末を自動的に適用免除に割り当てる方法が考えられる。なお、その際のユーザーを認識する手段として、例えばサーバー２０１へのログインＩＤ、ユーザーによる指示、カメラ又はセンサーによるユーザー認識などが挙げられる。

【０１９８】
制限の適用を免除する端末をコンテンツ毎に登録する場合、各コンテンツに関するメタデータとして端末のＳｉｎｋ－ＩＤを保持する。また、制限の適用を免除する端末をコンテンツのグループ毎に登録する場合には、各コンテンツ・グループに関するメタデータとして端末のＳｉｎｋ－ＩＤを保持することとする。

【０１９９】
リモート・アクセスの制限の適用を免除する端末を、コンテンツ毎、あるいはコンテンツのグループ毎に設定する場合、図１１ではなく、図１０に示した手順に従ってＲＡ－ＡＫＥ手続きを実施して、有効期限による登録抹消処理を行なうことなしに、すべてのＳｉｎｋデバイスにリモート・アクセス用交換鍵K_R及びその交換鍵ラベル$K_{R_}$ｌａｂｅｌを配布しておく。そして、コンテンツ伝送フェーズ（図１８、図１６を参照のこと）におけるコンテンツ出力管理処理において、コンテンツ毎又はコンテンツのグループ毎に設定されたリモート・アクセスの制限適用免除に従って、端末へのコンテンツ送信を制御する。

【０２００】
図２０には、有効期限に基づくリモート・アクセスの制限の適用を免除する端末が登録されている場合の、コンテンツ出力管理処理の手順をフローチャートの形式で示している。以下では、便宜上、Ｓｏｕｒｃｅデバイスとしてのサーバー２０１内で、例えばコンテンツ提供部３０４がコンテンツ出力管理処理を行なうものとして説明する。

【０２０１】
サーバー２０１は、コンテンツ要求（ＨＴＴＰ　ＧＥＴ　ｒｅｑｕｅｓｔ）に含まれる交換鍵ラベル$K_{R_}$ｌａｂｅｌを参照し（ステップＳ２００１）、同じ交換鍵ラベル$K_{R_}$ｌａｂｅｌのＲＡＣ　ｒｅｃｏｒｄが端末管理部３０７内に存在するかどうかをチェックする（ステップＳ２００２）。

【０２０２】
ここで、同じ交換鍵ラベル$K_{R_}$ｌａｂｅｌのＲＡＣ　ｒｅｃｏｒｄが存在しない場合には（ステップＳ２００２のＮｏ）、要求元のＳｉｎｋデバイスがＲＡ－ＡＫＥ手続きを行なっていないなどの原因により、不正なコンテンツ要求である。そこで、サーバー２０１は、後続の処理をすべてスキップして、本処理ルーチンを終了する。

【０２０３】
一方、同じ交換鍵ラベル$K_{R_}$ｌａｂｅｌのＲＡＣ　ｒｅｃｏｒｄが存在する場合には（ステップＳ２００２のＹｅｓ）、サーバー２０１は、そのＲＡ　ｒｅｃｏｒｄから、交換鍵ラベル$K_{R_}$ｌａｂｅｌに対応するＳｉｎｋ－ＩＤを取得する（ステップＳ２００３）。

【０２０４】
次いで、サーバー２０１は、要求されているコンテンツを含むコンテンツ・グループのメタデータに、このＳｉｎｋ－ＩＤが存在するかどうか、すなわち、当該コンテンツ・グループに対する有効期限によるリモート・アクセスの制限の適用が免除されているＳｉｎｋ－ＩＤであるかどうかをチェックする（ステップＳ２００４）。そして、当該コンテンツ・グループのメタデータにＳｉｎｋ－ＩＤが存在する場合には（ステップＳ２００４のＹｅｓ）、サーバー２０１は、Ｓｉｎｋデバイスからのコンテンツ要求を許可し、要求されたコンテンツの送信を例えばＨＴＴＰ　ＧＥＴ　ｒｅｓｐｏｎｓｅで行なう（ステップ

Ｓ２００９）。
【０２０５】
また、サーバー２０１は、当該コンテンツ・グループのメタデータにＳｉｎｋ－ＩＤが存在しない場合には（ステップＳ２００４のＮｏ）、要求されているコンテンツのメタデータに、このＳｉｎｋ－ＩＤが存在するかどうか、すなわち、当該コンテンツに対する有効期限によるリモート・アクセスの制限の適用が免除されているＳｉｎｋ－ＩＤであるかどうかをチェックする（ステップＳ２００５）。そして、当該コンテンツのメタデータにＳｉｎｋ－ＩＤが存在する場合には（ステップＳ２００５のＹｅｓ）、サーバー２０１は、Ｓｉｎｋデバイスからのコンテンツ要求を許可し、要求されたコンテンツの送信を例えばＨＴＴＰ　ＧＥＴ　ｒｅｓｐｏｎｓｅで行なう（ステップＳ２００９）。
【０２０６】
他方、Ｓｉｎｋ－ＩＤがコンテンツ・グループ並びにコンテンツのいずれのメタデータにも存在しない場合、すなわち、有効期限によるリモート・アクセスの制限の適用が免除されていない場合には（ステップＳ２００４、Ｓ２００５のＮｏ）、端末管理部３０７内のｒｅｍｏｔｅ　ｓｉｎｋ　ｒｅｇｉｓｔｒｙから、Ｓｉｎｋ－ＩＤとペアにして記憶されている有効期限を取得する（ステップＳ２００６）。
【０２０７】
そして、サーバー２０１は、現在日時を取得し（ステップＳ２００７）、現在日時が要求元のＳｉｎｋデバイスの有効期限を過ぎていないかどうかをチェックする（ステップＳ２００８）。現在日時が有効期限を過ぎている場合には（ステップＳ２００８のＮｏ）、コンテンツを送信することなく、本処理ルーチンを終了する。
【０２０８】
一方、現在日時が要求元のＳｉｎｋデバイスの有効期限を過ぎていないときには（ステップＳ２００８のＹｅｓ）、サーバー２０１は、Ｓｉｎｋデバイスからのコンテンツ要求を許可し、要求されたコンテンツの送信を例えばＨＴＴＰ　ＧＥＴ　ｒｅｓｐｏｎｓｅで行なう（ステップＳ２００９）。
【０２０９】
なお、有効期限に基づくリモート・アクセスの制限の適用免除を、コンテンツ・リスト閲覧フェーズ（ＳＥＱ８０１）で行なうこともできる。
【０２１０】
図２３には、コンテンツ・リスト閲覧フェーズ（ＳＥＱ８０１）において、Ｓｏｕｒｃｅデバイスが、リモート・アクセスするＳｉｎｋデバイスに対して、Ｓｉｎｋデバイスの有効期限に基づくＣＤＳ情報の提供制限を免除するための処理手順をフローチャートの形式で示している。
【０２１１】
まず、Ｓｏｕｒｃｅデバイスは、提供可能なコンテンツ情報をクリアする（ステップＳ２３０１）。
【０２１２】
次いで、Ｓｏｕｒｃｅデバイスは、要求元のＳｉｎｋデバイスのＳｉｎｋ－ＩＤに対応する有効期限を、ｒｅｍｏｔｅ　ｓｉｎｋ　ｒｅｇｉｓｔｒｙから取得するとともに（ステップＳ２３０２）、現在日時を取得する（ステップＳ２３０３）。
【０２１３】
そして、Ｓｏｕｒｃｅデバイスは、すべてのコンテンツ情報を処理するまで（ステップＳ２３０４のＮｏ）、コンテンツ情報の作成を行なう。
【０２１４】
Ｓｏｕｒｃｅデバイスは、未処理のコンテンツのコンテンツ情報を参照すると（ステップＳ２３０５）、そのコンテンツを含むコンテンツ・グループのメタデータに、要求元のＳｉｎｋ－ＩＤが存在するかどうか、すなわち、当該コンテンツ・グループに対する有効期限によるリモート・アクセスの制限の適用が免除されているＳｉｎｋ－ＩＤであるかどうかをチェックする（ステップＳ２３０６）。そして、当該コンテンツ・グループのメタ

データにＳｉｎｋ－ＩＤが存在する場合には（ステップＳ２３０６のＹｅｓ）、Ｓｏｕｒｃｅデバイスは、ステップＳ２３０５で参照したコンテンツ情報を提供可能なコンテンツ情報に追加してから（ステップＳ２３０９）、ステップＳ２３０４に戻る。

【０２１５】

また、Ｓｏｕｒｃｅデバイスは、当該コンテンツ・グループのメタデータにＳｉｎｋ－ＩＤが存在しない場合には（ステップＳ２３０６のＮｏ）、そのコンテンツのメタデータに、要求元のＳｉｎｋ－ＩＤが存在するかどうか、すなわち、当該コンテンツに対する有効期限によるリモート・アクセスの制限の適用が免除されているＳｉｎｋ－ＩＤであるかどうかをチェックする（ステップＳ２３０７）。そして、当該コンテンツのメタデータにＳｉｎｋ－ＩＤが存在する場合には（ステップＳ２３０７のＹｅｓ）、Ｓｏｕｒｃｅデバイスは、ステップＳ２３０５で参照したコンテンツ情報を提供可能なコンテンツ情報に追加してから（ステップＳ２３０９）、ステップＳ２３０４に戻る。

【０２１６】

他方、Ｓｉｎｋ－ＩＤがコンテンツ・グループ並びにコンテンツのいずれのメタデータにも存在しない場合、すなわち、有効期限によるリモート・アクセスの制限の適用が免除されていない場合には（ステップＳ２３０６、Ｓ２３０７のＮｏ）、Ｓｏｕｒｃｅデバイスは、ステップＳ２３０３で取得した現在日時が要求元のＳｉｎｋデバイスの有効期限を過ぎていないかどうかをチェックする（ステップＳ２３０８）。

【０２１７】

ここで、現在日時がまだ有効期限を過ぎていなければ（ステップＳ２３０８のＹｅｓ）、Ｓｏｕｒｃｅデバイスは、ステップＳ２３０５で参照したコンテンツ情報を提供可能なコンテンツ情報に追加してから（ステップＳ２３０９）、ステップＳ２３０４に戻る。

【０２１８】

一方、現在日時が有効期限を過ぎている場合には（ステップＳ２３０８のＮｏ）、ステップＳ２３０５で参照したコンテンツ情報を提供可能なコンテンツ情報に追加することなく、ステップＳ２３０４に戻る。

【０２１９】

そして、すべてのコンテンツ情報を処理し終えると（ステップＳ２３０４のＹｅｓ）、Ｓｏｕｒｃｅデバイスは、完成したコンテンツ情報を、要求元のＳｉｎｋデバイスに送信する（ステップＳ２３１０）。

【０２２０】

また、図２１には、限界日時に基づくリモート・アクセスの制限の適用を免除する端末が登録されている場合の、コンテンツ出力管理処理の手順をフローチャートの形式で示している。以下では、便宜上、Ｓｏｕｒｃｅデバイスとしてのサーバー２０１内で、例えばコンテンツ提供部３０４がコンテンツ出力管理処理を行なうものとして説明する。

【０２２１】

サーバー２０１は、コンテンツ要求（ＨＴＴＰ　ＧＥＴ　ｒｅｑｕｅｓｔ）に含まれる交換鍵ラベルK_{R}＿ｌａｂｅｌを参照し（ステップＳ２１０１）、同じ交換鍵ラベルK_{R}＿ｌａｂｅｌのＲＡＣ　ｒｅｃｏｒｄが端末管理部３０７内に存在するかどうかをチェックする（ステップＳ２１０２）。

【０２２２】

同じ交換鍵ラベルK_{R}＿ｌａｂｅｌのＲＡＣ　ｒｅｃｏｒｄが存在しない場合には（ステップＳ２１０２のＮｏ）、サーバー２０１は、後続の処理をすべてスキップして、本処理ルーチンを終了する。

【０２２３】

一方、同じ交換鍵ラベルK_{R}＿ｌａｂｅｌのＲＡＣ　ｒｅｃｏｒｄが存在する場合には（ステップＳ２１０２のＹｅｓ）、サーバー２０１は、そのＲＡ　ｒｅｃｏｒｄから、交換鍵ラベルK_{R}＿ｌａｂｅｌに対応するＳｉｎｋ－ＩＤを取得する（ステップＳ２１０３）。

【０２２４】

次いで、サーバー２０１は、要求されているコンテンツを含むコンテンツ・グループのメタデータに、このＳｉｎｋ－ＩＤが存在するかどうか、すなわち、当該コンテンツ・グループに対する限界日時によるリモート・アクセスの制限の適用が免除されているＳｉｎｋ－ＩＤであるかどうかをチェックする（ステップＳ２１０４）。そして、当該コンテンツ・グループのメタデータにＳｉｎｋ－ＩＤが存在する場合には（ステップＳ２１０４のＹｅｓ）、サーバー２０１は、Ｓｉｎｋデバイスからのコンテンツ要求を許可し、要求されたコンテンツの送信を例えばＨＴＴＰ　ＧＥＴ　ｒｅｓｐｏｎｓｅで行なう（ステップＳ２１０９）。

【０２２５】

また、サーバー２０１は、当該コンテンツ・グループのメタデータにＳｉｎｋ－ＩＤが存在しない場合には（ステップＳ２１０４のＮｏ）、要求されているコンテンツのメタデータに、このＳｉｎｋ－ＩＤが存在するかどうか、すなわち、当該コンテンツに対する限界日時によるリモート・アクセスの制限の適用が免除されているＳｉｎｋ－ＩＤであるかどうかをチェックする（ステップＳ２１０５）。そして、当該コンテンツのメタデータにＳｉｎｋ－ＩＤが存在する場合には（ステップＳ２１０５のＹｅｓ）、サーバー２０１は、Ｓｉｎｋデバイスからのコンテンツ要求を許可し、要求されたコンテンツの送信を例えばＨＴＴＰ　ＧＥＴ　ｒｅｓｐｏｎｓｅで行なう（ステップＳ２１０９）。

【０２２６】

他方、Ｓｉｎｋ－ＩＤがコンテンツ・グループ並びにコンテンツのいずれのメタデータにも存在しない場合、すなわち、限界日時によるリモート・アクセスの制限の適用が免除されていない場合には（ステップＳ２１０４、Ｓ２１０５のＮｏ）、端末管理部３０７内のｒｅｍｏｔｅ　ｓｉｎｋ　ｒｅｇｉｓｔｒｙから、Ｓｉｎｋ－ＩＤとペアにして記憶されている限界日時を取得する（ステップＳ２１０６）。

【０２２７】

また、サーバー２０１は、要求されているコンテンツがコンテンツ記録部３０２に記録された記録日時を、ファイル・システムから取得する（ステップＳ２１０７）。但し、要求されているコンテンツが、放送コンテンツなどコンテンツ取得部３０４で取得するコンテンツの場合には、その取得日時として現在日時（受信日時）を取得する。

【０２２８】

そして、サーバー２０１は、コンテンツ要求されているコンテンツの記録日時又は取得日時が、Ｓｉｎｋデバイスに設定されている限界日時を超えていないかどうかをチェックする（ステップＳ２１０８）。

【０２２９】

コンテンツの記録日時又は取得日時がＳｉｎｋデバイスの限界日時を超えていないときには（ステップＳ２１０８のＹｅｓ）、サーバー２０１は、Ｓｉｎｋデバイスからのコンテンツ要求を許可し、次ステップＳ２１０９で、要求されたコンテンツの送信を例えばＨＴＴＰ　ＧＥＴ　ｒｅｓｐｏｎｓｅで行なう。

【０２３０】

また、コンテンツの記録日時又は取得日時がＳｉｎｋデバイスの限界日時を超えているときには（ステップＳ２１０８のＮｏ）、サーバー２０１は、Ｓｉｎｋデバイスからのコンテンツ要求を許可せず、後続の処理をスキップして、本処理ルーチンを終了する。

【０２３１】

なお、限界日時に基づくリモート・アクセスの制限の適用免除を、コンテンツ・リスト閲覧フェーズ（ＳＥＱ８０１）で行なうこともできる。

【０２３２】

図２５には、コンテンツ・リスト閲覧フェーズ（ＳＥＱ８０１）において、Ｓｏｕｒｃｅデバイスが、リモート・アクセスするＳｉｎｋデバイスに対して、Ｓｉｎｋデバイスの限界日時に基づくＣＤＳ情報の提供制限を免除するための処理手順をフローチャートの形式で示している。

【０２３３】

まず、Ｓｏｕｒｃｅデバイスは、提供可能なコンテンツ情報をクリアする（ステップＳ２５０１）。次いで、Ｓｏｕｒｃｅデバイスは、要求元のＳｉｎｋデバイスのＳｉｎｋ－ＩＤに対応する限界日時を、ｒｅｍｏｔｅ　ｓｉｎｋ　ｒｅｇｉｓｔｒｙから取得するとともに（ステップＳ２５０２）。

【０２３４】

そして、Ｓｏｕｒｃｅデバイスは、すべてのコンテンツ情報を処理するまで（ステップＳ２５０３のＮｏ）、コンテンツ情報の作成を行なう。

【０２３５】

Ｓｏｕｒｃｅデバイスは、未処理のコンテンツのコンテンツ情報を参照すると（ステップＳ２５０４）、そのコンテンツを含むコンテンツ・グループのメタデータに、要求元のＳｉｎｋ－ＩＤが存在するかどうか、すなわち、当該コンテンツ・グループに対する限界日時によるリモート・アクセスの制限の適用が免除されているＳｉｎｋ－ＩＤであるかどうかをチェックする（ステップＳ２５０５）。そして、当該コンテンツ・グループのメタデータにＳｉｎｋ－ＩＤが存在する場合には（ステップＳ２５０５のＹｅｓ）、Ｓｏｕｒｃｅデバイスは、ステップＳ２５０４で参照したコンテンツ情報を提供可能なコンテンツ情報に追加してから（ステップＳ２５０９）、ステップＳ２５０３に戻る。

【０２３６】

また、Ｓｏｕｒｃｅデバイスは、当該コンテンツ・グループのメタデータにＳｉｎｋ－ＩＤが存在しない場合には（ステップＳ２５０５のＮｏ）、そのコンテンツのメタデータに、要求元のＳｉｎｋ－ＩＤが存在するかどうか、すなわち、当該コンテンツに対する限界日時によるリモート・アクセスの制限の適用が免除されているＳｉｎｋ－ＩＤであるかどうかをチェックする（ステップＳ２５０６）。そして、当該コンテンツのメタデータにＳｉｎｋ－ＩＤが存在する場合には（ステップＳ２５０６のＹｅｓ）、Ｓｏｕｒｃｅデバイスは、ステップＳ２５０４で参照したコンテンツ情報を提供可能なコンテンツ情報に追加してから（ステップＳ２５０９）、ステップＳ２５０３に戻る。

【０２３７】

他方、Ｓｉｎｋ－ＩＤがコンテンツ・グループ並びにコンテンツのいずれのメタデータにも存在しない場合、すなわち、限界日時によるリモート・アクセスの制限の適用が免除されていない場合には（ステップＳ２５０５、Ｓ２５０６のＮｏ）、Ｓｏｕｒｃｅデバイスは、ステップＳ２５０４で参照したコンテンツ情報が限界日時を超えていないかどうかをチェックする。

【０２３８】

限界日時のチェックのために、Ｓｏｕｒｃｅデバイスは、そのコンテンツがコンテンツ記録部３０２に記録された記録日時を、ファイル・システムから取得する（ステップＳ２５０７）。但し、要求されているコンテンツが、放送コンテンツなどコンテンツ取得部３０４で取得するコンテンツの場合には、その取得日時として現在日時（受信日時）を取得する。そして、Ｓｏｕｒｃｅデバイスは、そのコンテンツの記録日時又は取得日時が、Ｓｉｎｋデバイスに設定されている限界日時を超えていないかどうかをチェックする（ステップＳ２５０８）。

【０２３９】

そのコンテンツの記録日時又は取得日時がＳｉｎｋデバイスの限界日時を超えていないときには（ステップＳ２５０８のＹｅｓ）、Ｓｏｕｒｃｅデバイスは、このコンテンツ情報を提供可能なコンテンツ情報に追加してから（ステップＳ２５０９）、ステップＳ２５０３に戻る。

【０２４０】

一方、そのコンテンツの記録日時又は取得日時がＳｉｎｋデバイスの限界日時を超えているときには（ステップＳ２５０８のＮｏ）、Ｓｏｕｒｃｅデバイスは、このコンテンツ情報を提供可能なコンテンツ情報に追加することなく、ステップＳ２５０３に戻る。

【０２４１】

そして、すべてのコンテンツ情報を処理し終えると（ステップＳ２５０３のＹｅｓ）、

Ｓｏｕｒｃｅデバイスは、完成したコンテンツ情報を、要求元のＳｉｎｋデバイスに送信する（ステップＳ２５１０）。

【０２４２】

図２０、図２１、並びに、図２３、図２５に示したように、特定の端末に特定してリモート・アクセスの制限を免除するのではなく、コンテンツ毎に、又は、コンテンツのグループ毎に、サーバーへの登録日時に基づくリモート・アクセスの制限を免除する端末を設定することにより、例えば家族のメンバー毎の複数の端末による私的利用の範囲内でのコンテンツの利用の利便性を確保することができる。

【産業上の利用可能性】

【０２４３】

以上、特定の実施形態を参照しながら、本明細書で開示する技術について詳細に説明してきた。しかしながら、本明細書で開示する技術の要旨を逸脱しない範囲で当業者が該実施形態の修正や代用を成し得ることは自明である。

【０２４４】

本明細書では、本明細書で開示する技術をＩＰネットワーク並びにＤＴＣＰ仕様のネットワークに適用した実施形態を中心に説明してきたが、本明細書で開示する技術の要旨はこれに限定されるものではない。ＤＴＣＰ－ＩＰ以外の、ホーム・ネットワーク内のコンテンツへのリモート・アクセスに制限が課されるさまざまな通信システムにも、同様に本明細書で開示する技術で開示する技術を適用することができる。

【０２４５】

また、本明細書で開示する技術の適用範囲は、ホーム・ネットワークへのリモート・アクセスに限定されない。ホーム・ネットワーク内でのローカル・アクセス時においても、ホーム・サーバーへの端末の登録日時に基づいてアクセスを制限したい場合に、同様に本明細書で開示する技術を適用することができる。

【０２４６】

要するに、例示という形態により本明細書で開示する技術について説明してきたのであり、本明細書の記載内容を限定的に解釈するべきではない。本明細書で開示する技術の要旨を判断するためには、特許請求の範囲を参酌すべきである。

【０２４７】

なお、本明細書の開示の技術は、以下のような構成をとることも可能である。

（１）端末に提供するコンテンツを取得するコンテンツ取得部、又は、端末に提供するコンテンツを記録するコンテンツ記録部と、

コンテンツを提供する端末を登録する端末登録部と、

端末の登録日時に基づいて端末へのコンテンツの提供を制御するコンテンツ提供部と、

を具備する通信装置。

（２）所定の相互認証及び鍵交換手続きに従って端末を認証するとともに交換鍵を共有する認証及び鍵共有部をさらに備え、

前記コンテンツ提供部は、前記交換鍵を用いて暗号化したコンテンツを端末に提供する、

上記（１）に記載の通信装置。

（３）前記認証及び鍵共有部は、ＤＴＣＰ－ＩＰが規定する認証及び鍵交換（ＡＫＥ）アルゴリズムに従って、端末と相互認証並びに交換鍵の共有を行ない、

前記端末登録部は、ＤＴＣＰ－ＩＰが規定する手続きに従って端末の登録を行なう、

上記（２）に記載の通信装置。

（４）前記端末登録部は、ホーム・ネットワーク内で端末を登録し、

前記コンテンツ提供部は、外部ネットワークからアクセスした登録後の端末にコンテンツを提供する、

上記（１）に記載の通信装置。

（５）前記端末登録部は、端末の登録日時に第１の所定期間を加算した有効期限を端末の情報とともに管理し、

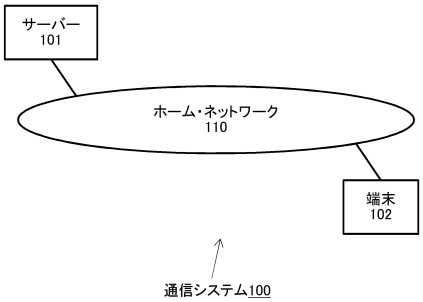
前記コンテンツ提供部は、有効期限を経過した端末へのコンテンツの提供を制限する、
上記（１）に記載の通信装置。
（６）前記端末登録部は、端末の登録日時に第２の所定期間を加算した限界日時を端末の情報とともに管理し、
前記コンテンツ提供部は、前記コンテンツ取得部の取得日時又は前記コンテンツ記録部への記録日時が限界日時以降となるコンテンツの端末への提供を制限する、
上記（１）に記載の通信装置。
（７）前記コンテンツ提供部は、前記端末登録部に登録される所定台数の端末については、登録日時に基づく制限を免除して、コンテンツを提供する、
上記（１）に記載の通信装置。
（８）コンテンツ毎又はコンテンツ・グループ毎に、登録日時に基づく制限を免除する端末を設定し、
前記コンテンツ提供部は、提供するコンテンツ又はコンテンツが含まれるコンテンツ・グループについて登録日時に基づく制限が免除された端末に対して、登録日時に拘わらずコンテンツを提供する、
上記（１）に記載の通信装置。
（９）前記コンテンツ記録部は、コンテンツ又はコンテンツが含まれるコンテンツ・グループについて登録日時に基づく制限を免除する端末を該当するコンテンツ又はコンテンツ・グループのメタデータに記録する、
上記（８）に記載の通信装置。
（１０）コンテンツ毎又はコンテンツ・グループ毎に、有効期限に基づく制限を免除する端末を設定し、
前記コンテンツ提供部は、提供するコンテンツを含むコンテンツ・グループ又は提供するコンテンツについて前記免除が設定された端末に対しては、有効期限に拘わらずコンテンツを提供する、
上記（５）に記載の通信装置。
（１１）コンテンツ毎又はコンテンツ・グループ毎に、限界日時に基づく制限を免除する端末を設定し、
前記コンテンツ提供部は、提供するコンテンツを含むコンテンツ・グループ又は提供するコンテンツについて前記免除が設定された端末に対しては、限界日時に拘わらずコンテンツを提供する、
上記（６）に記載の通信装置。
（１２）端末に提供可能なコンテンツに関する情報を端末に提供するコンテンツ情報提供部をさらに備え、
前記コンテンツ提供部は、端末側で閲覧しているコンテンツ情報を介して選択されたコンテンツを提供する、
上記（１）に記載の通信装置。
（１３）前記コンテンツ情報提供部は、端末の登録日時に基づいて端末へのコンテンツ情報の提供を制限する、
上記（１２）に記載の通信装置。
（１４）前記端末登録部は、端末の登録日時に第１の所定期間を加算した有効期限を端末の情報とともに管理し、
前記コンテンツ情報提供部は、有効期限を経過した端末へのコンテンツ情報の提供を制限する、
上記（１３）に記載の通信装置。
（１５）前記端末登録部は、端末の登録日時に第２の所定期間を加算した限界日時を端末の情報とともに管理し、
前記コンテンツ情報提供部は、前記コンテンツ取得部の取得日時又は前記コンテンツ記録部への記録日時が限界日時以降となるコンテンツについては端末へのコンテンツ情報の提供を制限する、

上記（１３）に記載の通信装置。
（１６）前記コンテンツ情報提供部は、前記端末登録部に登録される所定台数の端末については、登録日時に基づく制限を免除して、コンテンツ情報を提供する、
上記（１３）に記載の通信装置。
（１７）コンテンツ毎又はコンテンツ・グループ毎に、有効期限に基づく制限を免除する端末を設定し、
前記コンテンツ情報提供部は、有効期限が経過した端末であっても、当該端末に対して前記免除が設定されたコンテンツ・グループに含まれるコンテンツ、又は、前記免除が設定されたコンテンツのコンテンツ情報を提供する、
上記（１４）に記載の通信装置。
（１８）コンテンツ毎又はコンテンツ・グループ毎に、限界日時に基づく制限を免除する端末を設定し、
前記コンテンツ情報提供部は、提供先の端末に対して前記免除が設定されたコンテンツ又はコンテンツ・グループについては、取得日時又は記録日時が限界日時以降であってもコンテンツ情報を提供する、
上記（１５）に記載の通信装置。
（１９）端末に提供するコンテンツを取得するコンテンツ取得ステップ、又は、端末に提供するコンテンツをコンテンツ記録部に記録するコンテンツ記録ステップと、
コンテンツを提供する端末を登録する端末登録ステップと、
端末の登録日時に基づく制限をかけながら、前記コンテンツ取得ステップで取得したコンテンツ又は前記コンテンツ記録ステップで記録したコンテンツを端末に提供するコンテンツ提供ステップと、
を有する通信方法。
（２０）端末に提供するコンテンツを取得するコンテンツ取得部、又は、端末に提供するコンテンツを記録するコンテンツ記録部、
コンテンツを提供する端末を登録する端末登録部、
端末の登録日時に基づいて端末へのコンテンツの提供を制御するコンテンツ提供部、
としてコンピューターを機能させるようにコンピューター可読形式で記述されたコンピューター・プログラム。
（２１）ユーザーによる操作情報が入力される入力部と、
登録日時を管理するサーバーに対して登録要求を行なう登録要求部と、
前記入力部に入力される操作情報に応じて、前記サーバーに対してコンテンツの要求を行なうコンテンツ要求部と、
前記のコンテンツの要求に応じて、前記登録日時に基づく制限下で、前記サーバーから前記コンテンツの再生が許可されるコンテンツ再生部と、
を具備する通信装置。
（２２）ＤＴＣＰ－ＩＰが規定する手続きに従ってサーバーへの登録を行なうとともに、ＤＴＣＰ－ＩＰが規定する認証及び鍵交換（ＡＫＥ）アルゴリズムに従って前記サーバーと相互認証及び交換鍵の共有を行なう認証部をさらに備え、
前記コンテンツ再生部は、前記交換鍵で暗号化されたコンテンツを前記サーバーから取得し、前記交換鍵で復号して再生する、
上記（２１）に記載の通信装置。
（２３）前記登録要求部は、ホーム・ネットワーク内で前記サーバーに対して登録を行ない、
前記コンテンツ再生部は、外部ネットワーク経由で前記サーバーからコンテンツを取得する、
上記（２１）に記載の通信装置。
（２４）前記登録要求部は、前記登録日時から所定の期間が経過する前に、前記サーバーに対する登録要求の処理を再度行なう、
上記（２１）に記載の通信装置。

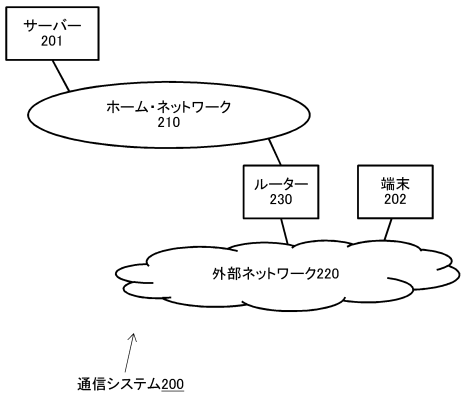
（２５）前記コンテンツ再生部は、前記サーバーが受信した放送コンテンツ又は記録メディアから読み出した商用コンテンツ、又は、前記サーバーが記録するコンテンツを再生する、
上記（２１）に記載の通信装置。
（２６）前記コンテンツ再生部は、前記サーバーへの登録日時に第１の所定期間を加算した有効期限以降は、前記サーバーからのコンテンツの再生が制限される、
上記（２１）に記載の通信装置。
（２７）前記コンテンツ再生部は、サーバーへの登録日時に第２の所定期間を加算した日時以降にサーバーが取得し又は記録したコンテンツの再生が制限される、
上記（２１）に記載の通信装置。
（２８）所定台数以内でサーバーに登録したときには、前記コンテンツ再生部は、サーバーへの登録日時に基づく制限を受けずに、サーバーからコンテンツを再生することができる、
上記（２１）に記載の通信装置。
（２９）前記コンテンツ再生部は、前記通信装置に対して登録日時に基づく制限が免除されたコンテンツ又はコンテンツ・グループに含まれるコンテンツを、登録日時に拘わらず再生することができる、
上記（２１）に記載の通信装置。
（３０）前記コンテンツ再生部は、前記通信装置に対して有効期限に基づく制限が免除されたコンテンツ又はコンテンツ・グループに含まれるコンテンツを、設定された有効期限に拘わらず再生することができる、
上記（２６）に記載の通信装置。
（３１）前記コンテンツ再生部は、前記通信装置に対して限界日時に基づく制限が免除されたコンテンツ又はコンテンツ・グループに含まれるコンテンツを、サーバーによる取得又は記録日時が限界日時より前か否かに拘わらず再生することができる、
上記（２７）に記載の通信装置。
（３２）前記サーバーで提供可能なコンテンツに関する情報を閲覧するコンテンツ情報閲覧部をさらに備え、
　前記コンテンツ要求部は、前記コンテンツ情報閲覧部で閲覧している情報を介して選択されたコンテンツを前記サーバーに要求する、
上記（２１）に記載の通信装置。
（３３）前記コンテンツ情報閲覧部は、サーバーへの登録日時に基づく制限下で、サーバーで提供可能なコンテンツに関する情報を閲覧する、
上記（３２）に記載の通信装置。
（３４）前記コンテンツ情報閲覧部は、サーバーへの登録日時に第１の所定期間を加算した有効期限以降は、コンテンツ情報の閲覧が制限される、
上記（３２）に記載の通信装置。
（３５）前記コンテンツ情報閲覧部は、サーバーへの登録日時に第２の所定期間を加算した日時以降にサーバーが取得し又は記録したコンテンツ情報の閲覧が制限される、
上記（３２）に記載の通信装置。
（３６）所定台数以内でサーバーに登録したときには、前記コンテンツ情報閲覧部は、サーバーへの登録日時に基づく制限を受けずに、コンテンツ情報を閲覧することができる、
上記（３３）に記載の通信装置。
（３７）前記コンテンツ情報閲覧部は、前記通信装置に対して有効期限に基づく制限が免除されたコンテンツ又はコンテンツ・グループに含まれるコンテンツ情報を、設定された有効期限に拘わらず閲覧することができる、
上記（３４）に記載の通信装置。
（３８）前記コンテンツ情報閲覧部は、前記通信装置に対して限界日時に基づく制限が免除されたコンテンツ又はコンテンツ・グループに含まれるコンテンツ情報を、サーバーによる取得又は記録日時が限界日時より前か否かに拘わらず閲覧することができる、

上記（３５）に記載の通信装置。
（３９）ユーザーによる操作情報が入力される入力ステップと、
登録日時を管理するサーバーに対して登録要求を行なう登録要求ステップと、
前記入力部に入力される操作情報に応じて、前記サーバーに対してコンテンツの要求を行なうコンテンツ要求ステップと、
前記のコンテンツの要求に応じて、前記登録日時に基づく制限下で、前記サーバーから前記コンテンツの再生が許可されるコンテンツ再生ステップと、
を有する通信方法。
（４０）ユーザーによる操作情報が入力される入力部、
登録日時を管理するサーバーに対して登録要求を行なう登録要求部、
前記入力部に入力される操作情報に応じて、前記サーバーに対してコンテンツの要求を行なうコンテンツ要求部、
前記のコンテンツの要求に応じて、前記登録日時に基づく制限下で、前記サーバーから前記コンテンツの再生が許可されるコンテンツ再生部、
としてコンピューターを機能させるようにコンピューター可読形式で記述されたコンピューター・プログラム。
（４１）コンテンツを要求する端末と、
コンテンツを提供する端末を登録するとともに、その登録日時に基づいて前記端末へのコンテンツの提供を制御するサーバーと、
を具備する通信システム。
【符号の説明】
【０２４８】
１００…通信システム
１０１…サーバー、１０２…端末、１１０…ホーム・ネットワーク
２０１…サーバー、２０２…端末
２００…通信システム
２０１…サーバー、２０２…端末
２１０…ホーム・ネットワーク、２２０…外部ネットワーク
２３０…ルーター
３００…通信装置（Ｓｏｕｒｃｅデバイス）
３０１…通信・制御部、３０２…コンテンツ記録部
３０３…コンテンツ取得部、３０４…コンテンツ提供部
３０５…コンテンツ・リスト提供部、３０６…認証・鍵共有部
３０７…端末管理部
４００…通信装置
４０１…通信・制御部
４０２…コンテンツ・リスト閲覧部、４０３…コンテンツ取得部
４０４…コンテンツ復号部、４０５…コンテンツ再生出力部
４０６…認証・鍵共有部、４０７…入力部

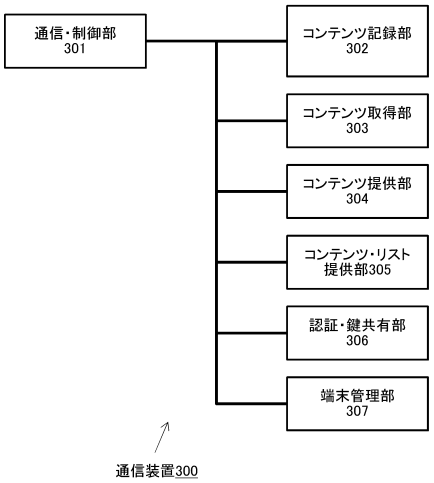
【図１】



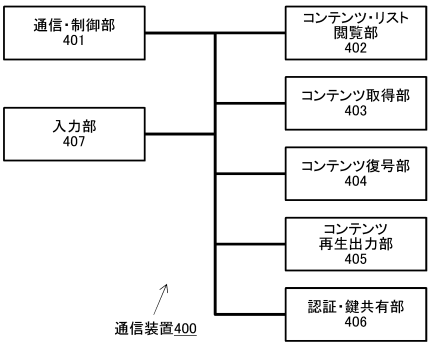
【図２】



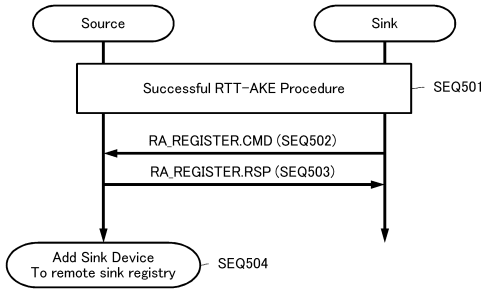
【図３】



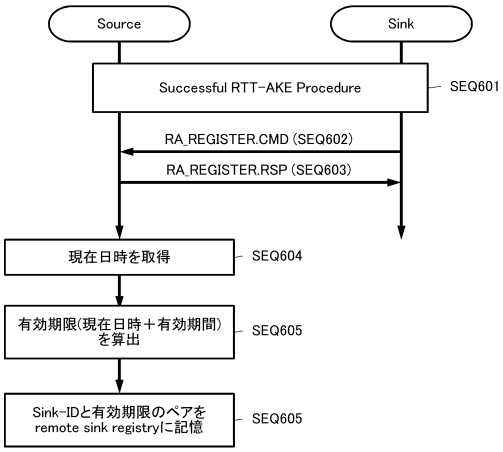
【図４】



【図５】



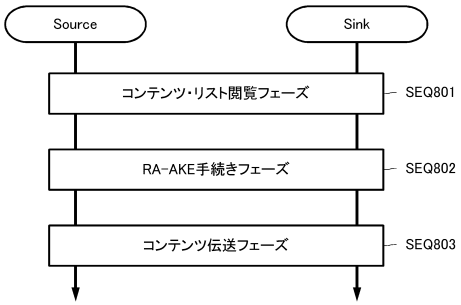
【図６】



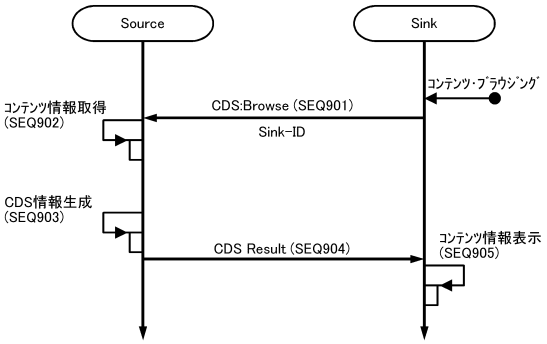
【図７】

Sink-ID	有効期限
0x800000e924	November 16, 2013
0x80000100af	January 25, 2014

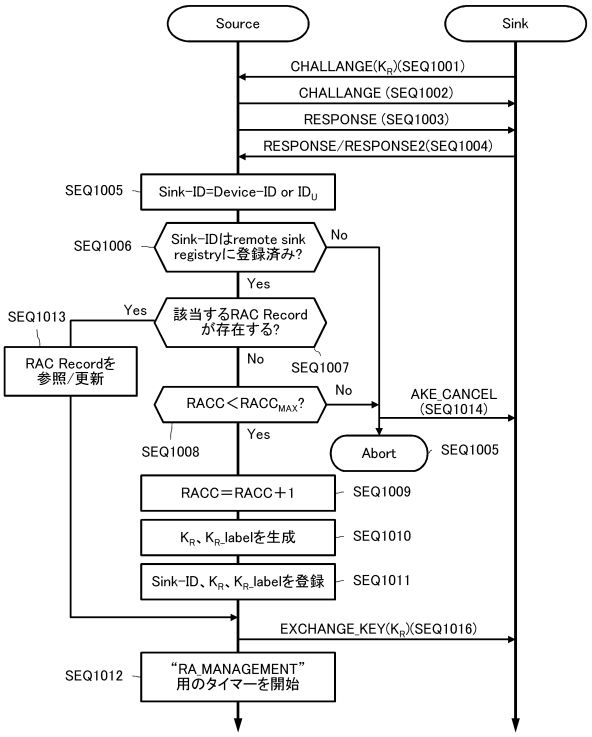
【図８】



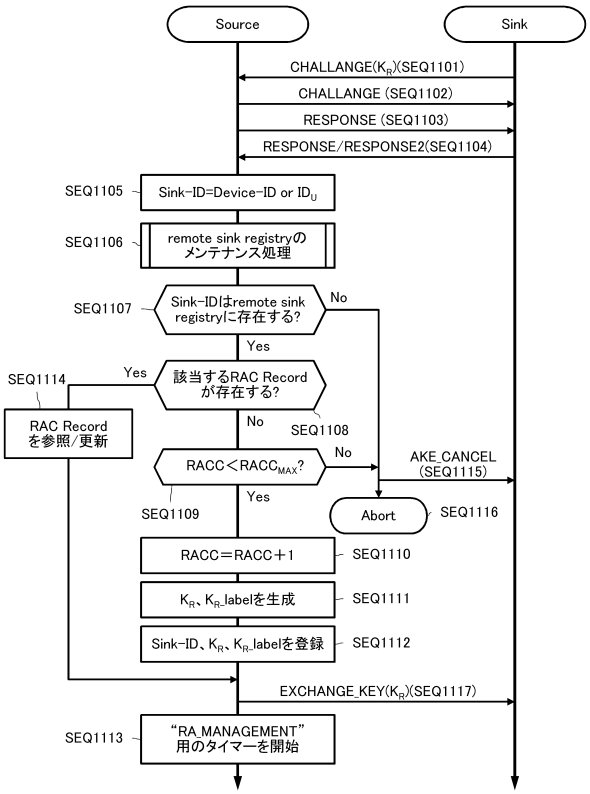
【図９】



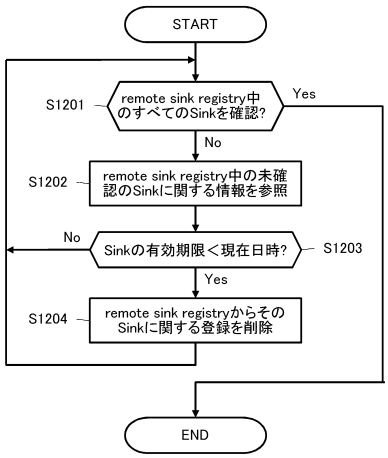
【図１０】



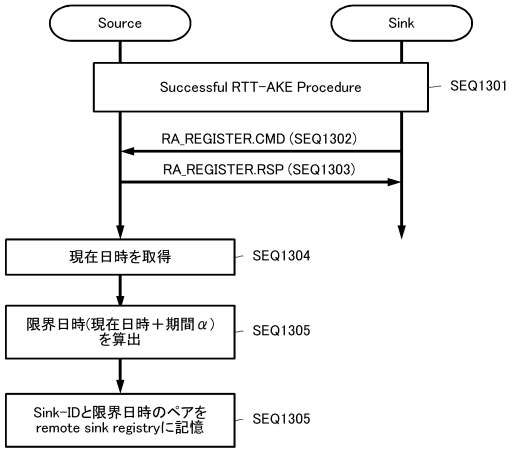
【図１１】



【図１２】



【図１３】



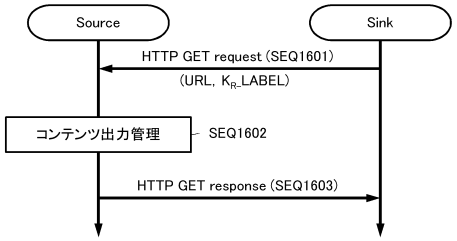
【図１４】

Sink-ID	限界日時
0x800000e924	November 16, 2013
0x80000100af	January 25, 2014

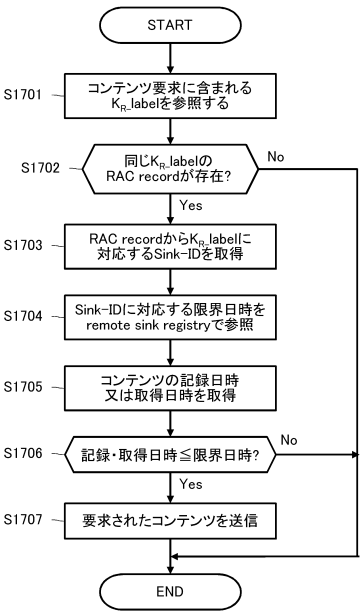
【図１５】

Sink-ID	K_R	K_R_label
0x800000e924	0x7f4130de0a6 100e257cf68db	0xe9

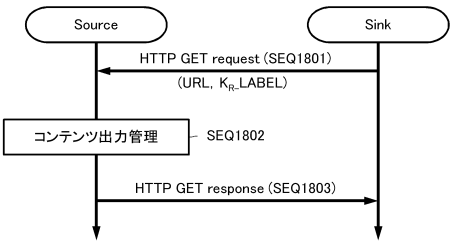
【図１６】



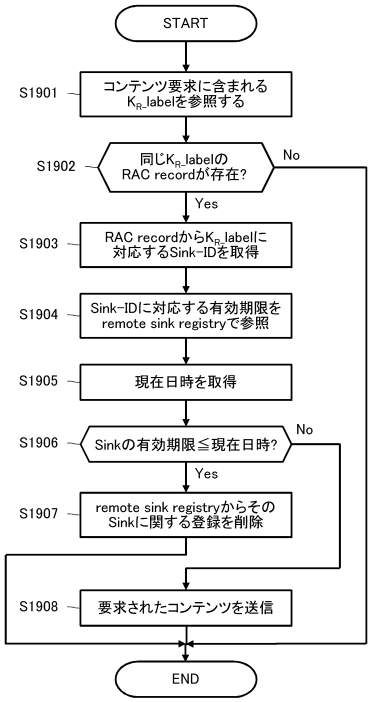
【図１７】



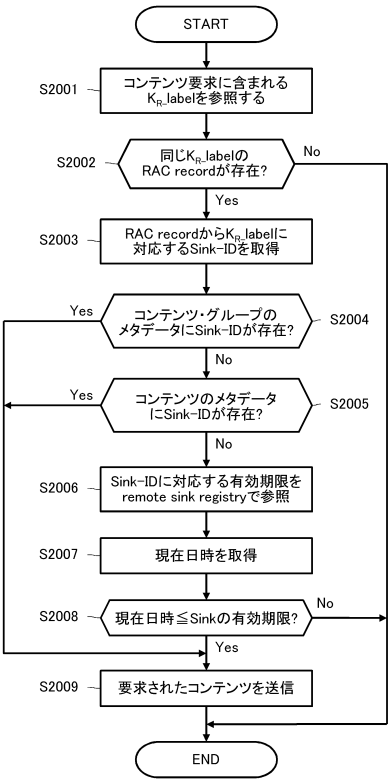
【図１８】



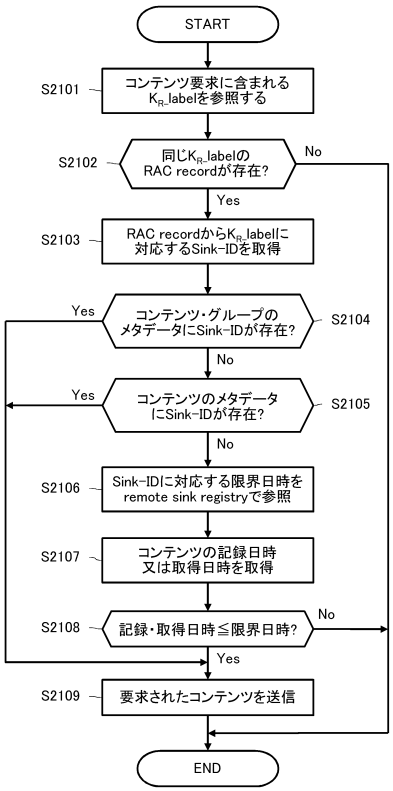
【図１９】



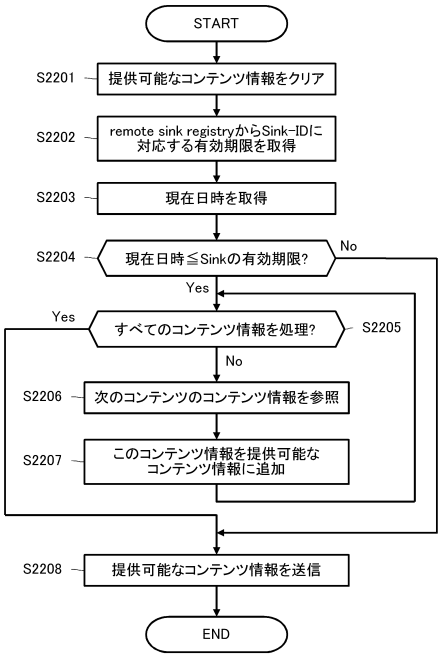
【図２０】



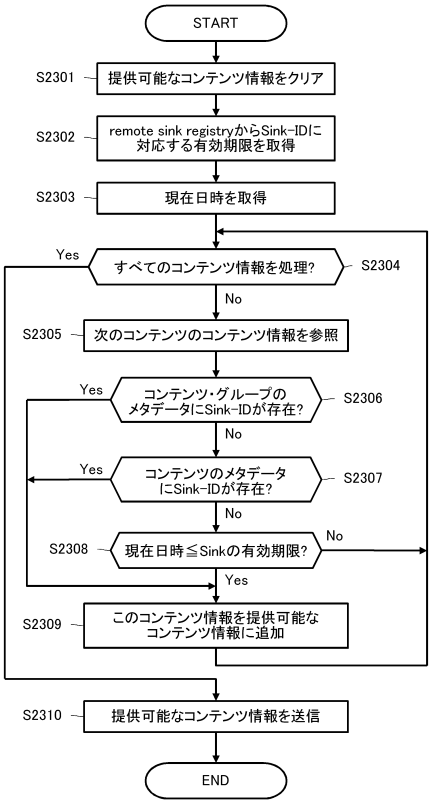
【図２１】



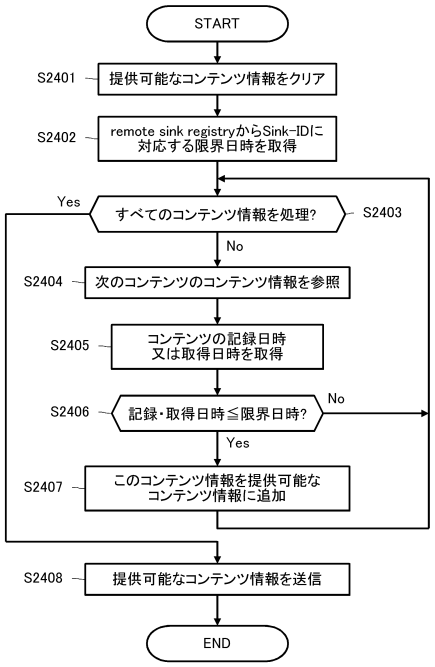
【図２２】



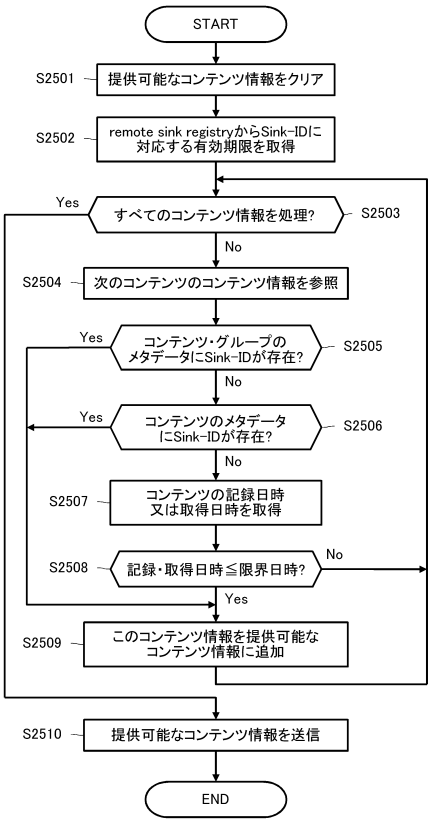
【図２３】



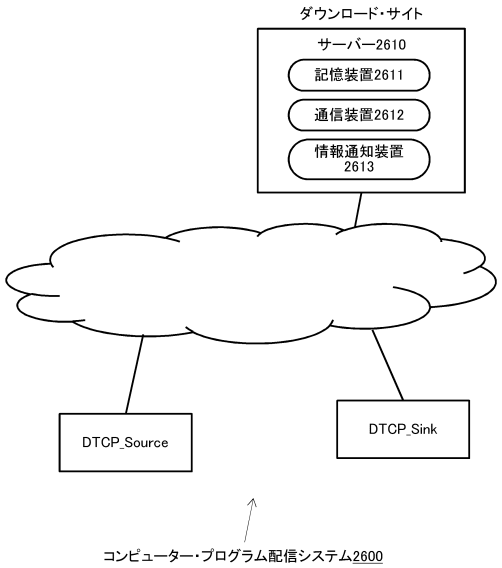
【図２４】



【図２５】



【図２６】



フロントページの続き

(51)Int.Cl.　　FI
　　G06F　21/44　　350

(72)発明者　中野　雄彦
　　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　青木　重徳

(56)参考文献　特開２０１３－０１５９３７（ＪＰ，Ａ）
　　特開２０１１－０８２９５２（ＪＰ，Ａ）
　　特開２０１１－２４４１６５（ＪＰ，Ａ）
　　特開２００４－２３４６４８（ＪＰ，Ａ）
　　特開２００４－１８００２０（ＪＰ，Ａ）
　　国際公開第２０１１／０３０６０５（WO，Ａ１）
　　特開２００５－２０４０９４（ＪＰ，Ａ）
　　特開２００７－１６４２９９（ＪＰ，Ａ）
　　特開２００３－１８６７７８（ＪＰ，Ａ）
　　特開２０１１－１９７９１７（ＪＰ，Ａ）
　　国際公開第２００６／００６６７８（WO，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
　　Ｈ０４Ｌ　　９／０８
　　Ｇ０６Ｆ　２１／１０
　　Ｇ０６Ｆ　２１／４４
　　Ｇ０６Ｆ　２１／６２
　　Ｇ０９Ｃ　　１／００