(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2004 年11 月18 日 (18.11.2004)

PCT

(10) 国際公開番号
WO 2004/100457 A1

(51) 国際特許分類[7]: H04L 12/46, 12/66, G06F 15/00

(21) 国際出願番号: PCT/JP2004/003336

(22) 国際出願日: 2004 年3 月12 日 (12.03.2004)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2003-132903 2003 年5 月12 日 (12.05.2003) JP

(71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒1410001 東京都品川区北品川６丁目７番３５号 Tokyo (JP).

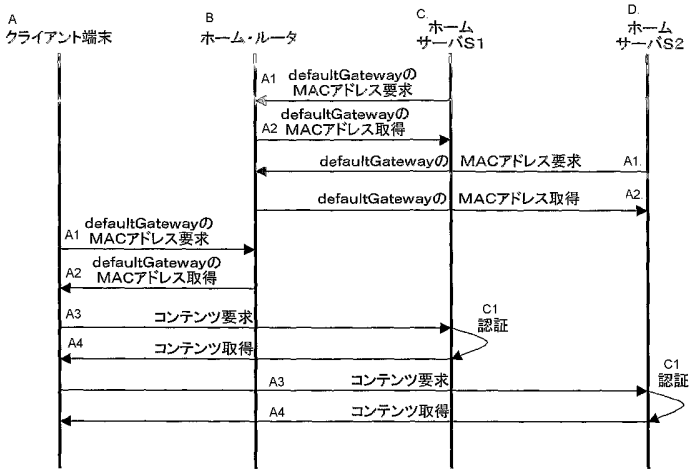
(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 高林 和彦 (TAKABAYASHI, Kazuhiko) [JP/JP]; 〒1410001 東京都品川区北品川６丁目７番３５号ソニー株式会社内 Tokyo (JP). 中野 雄彦 (NAKANO, Takehiko) [JP/JP]; 〒1410001 東京都品川区北品川６丁目７番３５号ソニー株式会社内 Tokyo (JP). 本田 康晃 (HONDA, Yasuaki) [JP/JP]; 〒1410001 東京都品川区北品川６丁目７番３５号ソニー株式会社内 Tokyo (JP). 五十嵐 卓也 (IGARASHI, Tatsuya) [JP/JP]; 〒1410001 東京都品川区北品川６丁目７番３５号ソニー株式会社内 Tokyo (JP).

(74) 代理人: 山田 英治 , 外 (YAMADA, Eiji et al.); 〒1040041 東京都中央区新富一丁目１番７号 銀座ティーケイビル 澤田・宮田・山田特許事務所 Tokyo (JP).

[続葉有]

(54) Title: INTER-DEVICE AUTHENTICATION SYSTEM, INTER-DEVICE AUTHENTICATION METHOD, COMMUNICATION DEVICE, AND COMPUTER PROGRAM

(54) 発明の名称: 機器間認証システム及び機器間認証方法、通信装置、並びにコンピュータ・プログラム



A...CLIENT TERMINAL
A1...DEFAULT GATEWAY MAC ADDRESS REQUEST
A2...DEFAULT GATEWAY MAC ADDRESS ACQUISITION
A3...CONTENT REQUEST
A4...CONTENT ACQUISITION

B...HOME ROUTER
C...HOME SERVER S1
C1...AUTHENTICATION
D...HOME SERVER S2

(57) Abstract: Considering that a home network is connected to an external network via a home router, an access from the same network has a transmission source MAC address but an access from outside via the router has a transmission source rewritten into the router MAC address. Accordingly, by comparing the MAC address of the communication partner to the MAC address of the home router, it is possible to automatically check whether the access is an access from the home network. It is possible to manage the use of the content acquired validly on the home server, within the private use range admitted by the copyright law, by the client terminal.

(57) 要約: ホーム・ネットワークがホーム・ルータ経由で外部ネットワークに接続されていることを鑑み、同じネットワークからのアクセスであれば送信元のＭＡＣアドレスが付されているが、外部からのルータ越しのアクセスの場合は

[続葉有]

WO 2004/100457 A1

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書
— 補正書・説明書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

送信元がルータのＭＡＣアドレスに書き換えられることを利用し、通信相手のＭＡＣアドレスをホーム・ルータのＭＡＣアドレスと比較することによりホーム・ネットワーク内からのアクセスであるかどうかを自動識別する。ホーム・サーバ上で正当に取得されているコンテンツを著作権法で認められる私的使用の範囲内でクライアント端末が利用するように管理することができる。

明 細 書

機器間認証システム及び機器間認証方法、通信装置、並びにコンピュータ・プログラム

技術分野

本発明は、ネットワークなどによって配信される音楽データや画像データ、電子出版物などのデジタル・データや動画像などコンテンツの機器間での利用を管理する機器間認証システム及び機器間認証方法、通信装置、並びにコンピュータ・プログラムに係り、特に、著作権法で認められる私的使用の範囲内でコンテンツの利用を管理する機器間認証システム及び機器間認証方法、通信装置、並びにコンピュータ・プログラムに関する。

さらに詳しくは、本発明は、ルータ経由で外部ネットワークに接続されているホーム・ネットワーク上で、著作権法で認められる私的使用の範囲内でコンテンツの利用を管理する機器間認証システム及び機器間認証方法、通信装置、並びにコンピュータ・プログラムに係り、特に、ホーム・ネットワーク上の各クライアント端末がホーム・サーバ上で正当に取得されているコンテンツを著作権法で認められる私的使用の範囲内で利用するように管理する機器間認証システム及び機器間認証方法、通信装置、並びにコンピュータ・プログラムに関する。

背景技術

近年のインターネットの普及により、コンピュータ・ファイルを始めとした各種のデジタル･コンテンツをネットワーク配信することが盛んに行なわれている。また、広帯域通信網（ｘＤＳＬ（ｘ Ｄｉｇｉｔａｌ Ｓｕｂｓｃｒｉｂｅｒ Ｌｉｎｅ）、ＣＡＴＶ（Ｃａｂｌｅ ＴＶ）、無線ネットワークなど）の普及により、音楽データや画像データ、電子出版物などのデジタル・データや、さらには動画像などリッチ・コンテンツの配信もユーザにストレスなく伝送できるような仕組

みが整いつつある。

一方、配信されるコンテンツはデジタル・データであり、コピーや改竄などの不正な操作を比較的容易に行なうことができる。また、現在これらのコンテンツのコピーや改竄などの不正行為は頻繁に行なわれており、これがデジタル・コンテンツ・ベンダの利益を阻害する主要な要因となっている。この結果、コンテンツの値段も高くしなければならなくなり、普及の障壁となるという悪循環が起こっている。

例えば、最近では一般家庭内にもコンピュータやネットワークなどの技術が深く浸透してきている。家庭内のパーソナル・コンピュータやＰＤＡ（Ｐｅｒｓｏｎａｌ　Ｄｉｇｉｔａｌ　Ａｓｓｉｓｔａｎｔｓ）などの情報機器、さらにはテレビ受像機やビデオ再生装置などの各種の情報家電がホーム・ネットワーク経由で相互接続されている。また、このようなホーム・ネットワークは、多くの場合、ルータ経由でインターネットを始めとする外部の広域ネットワークに相互接続されている。そして、インターネット上のサーバから正当に取得されたコンテンツは、ホーム・ネットワーク上のサーバ（以下、「ホーム・サーバ」とも呼ぶ）に蓄積された後、家庭内の他の端末（クライアント）へホーム・ネットワーク経由で配信される。

著作権法の下、著作物としてのコンテンツは無断の複製や改竄などの不正使用から保護を受ける。一方、著作物の正当な利用者においては、私的な使用、すなわち個人的に又は家庭内その他これに準ずる限られた範囲内において使用することを目的としてコンテンツを複製することが許されている（著作権法第３０条を参照のこと）。

この私的使用の範囲を上述したホーム・ネットワークにおいて適用した場合、ホーム・ネットワークに接続されているクライアント端末は、個人的又は家庭の範囲内での使用であると推定される。したがって、ホーム・サーバにおいて正当に取得されているコンテンツは、ホーム・ネットワーク上のクライアント端末は自由に使用することが相当であると思料される（勿論、コンテンツを享受できる端末の台数に一定の制限を設ける必要がある）。

しかしながら、ホーム・ネットワーク上にログインしたクライアント端末が私

的使用の範囲にあるかどうかを識別することは、現状の技術では困難である。

例えば、ホーム・ネットワークはルータを介して外部のネットワークとＩＰプロトコル・ベースで相互接続されていることから、ホーム・サーバにとってはアクセスしてきたクライアントが実際にどこにいるのかは不明である。外部（遠隔）からのアクセスに対しホーム・サーバがコンテンツを提供してしまうと、コンテンツの利用はほぼ無制限となってしまい、コンテンツに関する著作権は保護されないに等しい。この結果、コンテンツ製作者は創作意欲を失いかねない。

また、ホーム・サーバがホーム・ネットワーク内のクライアント端末に対して一様にコンテンツの利用を許可した場合、同じクライアント端末が時間差をおいて複数のホーム・ネットワークに跨ってログインすることにより、ほぼ無尽蔵にコンテンツを利用することが可能となってしまう。

他方、クライアント端末に対して厳しい制限を課してしまうと、ユーザは、本来著作権法上で認められている私的使用を確保することができなくなってしまう。この結果、ユーザがコンテンツを十分に享受することができず、ホーム・サーバやコンテンツ配信サービスの利用が進まないために、コンテンツ事業の発展自体を阻害しかねない。

例えば、著作物を正規に購入した利用者に自由利用が認められているということに鑑み、利用者がネットワーク上での情報を複製して利用するにあたって、コンテンツの権利保持者の理解が得られ易い方法に関する提案がなされている（例えば、特開２００２－７３８６１号公報を参照のこと）。しかしながら、これは利用者を情報の利用権保持者との関係レベルによって分類し、関係レベル毎に異なる配信方法で情報を配信するというもので、ネットワーク上のどこまでが私的使用の範囲に該当するのかを識別するものではない。

ところで、ホーム・ネットワークを構成するプロトコルとして、例えばＵＰｎＰ（登録商標）が知られている。ＵＰｎＰによれば、複雑な操作を伴うことなく容易にネットワークを構築することが可能であり、ネットワーク接続された機器間では困難な操作や設定を伴うことなくコンテンツ提供サービスを行なうことが可能となる。また、ＵＰｎＰは、オペレーティング・システム（ＯＳ）に非依存であり、容易に機器の追加ができるという利点を持つ。

ＵＰｎＰでは、ネットワーク接続された機器間で、ＸＭＬ（ｅＸｔｅｎｄｅｄ Ｍａｒｋｕｐ Ｌａｎｇｕａｇｅ）形式で記述された定義ファイルを交換して相互認証を行なう。ＵＰｎＰの処理の概要は以下の通りである。

（１）アドレッシング処理：ＩＰアドレスなどの自己のデバイスＩＤを取得する

（２）ディスカバリ処理：ネットワーク上の各デバイスの検索を行ない、各デバイスから受信した応答に含まれるデバイス種別や機能などの情報を取得する

（３）サービス要求処理：ディスカバリ処理で取得された情報に基づいて各デバイスにサービスを要求する

このような処理手順を行なうことで、ネットワーク接続された機器を適用したサービスの提供並びに受領が可能となる。新たにネットワークに接続される機器は、アドレッシング処理によりデバイスＩＤを取得し、ディスカバリ処理によりネットワーク接続されている他のデバイスの情報を取得し、サービス要求が可能となる。

ホーム・サーバに格納されたコンテンツは、ホーム・ネットワーク上の他の機器からアクセス可能となる。例えば、上述したＵＰｎＰ接続を実行した機器によってコンテンツを取得することが可能である。コンテンツが映像データや音声データの場合、ネットワーク接続機器として、ＴＶやプレーヤなどを接続すれば、映画や音楽を視聴することができる。

しかし、ホーム・ネットワーク内の機器、例えばホーム・サーバには私的なコンテンツや有料コンテンツなど著作権管理を要求されるコンテンツが格納されていることから、不正アクセスの対策を考慮する必要がある。

コンテンツの利用権（ライセンス）を有するユーザの機器によるアクセスは許容されて当然である。しかしながら、ホーム・ルータ経由で外部ネットワークに相互接続されているホーム・ネットワーク環境では、ライセンスを持たないユーザがホーム・ネットワークに入り込むことも可能である。

不正アクセスを排除するため、例えば、ホーム・サーバにアクセスを許容するクライアントのリストを保持させ、クライアントからホーム・サーバへのアクセス要求が行なわれる度に、リストとの照合処理を実行して、不正アクセスを排除することができる。

例えば、各通信機器に固有の物理アドレスであるＭＡＣ（Ｍｅｄｉａ　Ａｃｃｅｓｓ　Ｃｏｎｔｒｏｌ）アドレスを用いてアクセス許容機器リストとして設定するＭＡＣアドレス・フィルタリングが知られている。すなわち、ホーム・ネットワークのような内部ネットワークと外部ネットワークとを隔離するルータ又はゲートウェイにアクセスを許容する各機器のＭＡＣアドレスを登録しておき、受信したパケットに付されているＭＡＣアドレスと登録されたＭＡＣアドレスとを照合し、未登録のＭＡＣアドレスを持つ機器からのアクセスを拒否する（例えば、特開平１０－２７１１５４号公報を参照のこと）。

しかしながら、アクセス許容機器リストを構築するためには、内部ネットワークに接続されるすべての機器のＭＡＣアドレスを調べる必要があり、また、取得したすべてのＭＡＣアドレスを入力してリストを作成する手間が必要である。また、ホーム・ネットワークにおいては、接続される機器が比較的頻繁に変更され、かかる変更の度にアクセス許容機器リストを修正しなければならない。

発明の開示

本発明の目的は、ルータ経由で外部ネットワークに接続されているホーム・ネットワーク上において機器間でのコンテンツの利用を好適に管理することができる、優れた機器間認証システム及び機器間認証方法、通信装置、並びにコンピュータ・プログラムを提供することにある。

本発明のさらなる目的は、ホーム・ネットワーク上の各クライアント端末がホーム・サーバ上で正当に取得されているコンテンツを著作権法で認められる私的使用の範囲内で利用するように好適に管理することができる、優れた機器間認証システム及び機器間認証方法、通信装置、並びにコンピュータ・プログラムを提供することにある。

本発明は、上記課題を参酌してなされたものであり、その第１の側面は、ルータ経由で外部ネットワークに接続可能なホーム・ネットワーク上の機器を認証する機器間認証システムであって、前記ホーム・ネットワーク上の機器に対してア

クセスする他の機器が前記ホーム・ネットワーク上に存在するかどうかを確認するローカル環境管理手段を備えることを特徴とする機器間認証システムである。

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。

ここで、一方の機器は、ホーム・サーバであり、前記ルータ経由で外部ネットワークから、あるいはパッケージ・メディアや放送受信などを介して、コンテンツを正当に取得する。また、他方の機器はホーム・サーバに対してコンテンツを要求し利用するクライアントである。そして、双方の機器が同じホーム・ネットワーク上に存在することが確認されたことに応じて、前記ホーム・サーバは前記クライアントに対しコンテンツの提供及び／又はコンテンツに関するライセンスの発行を行なう。

著作権法の下、著作物としてのコンテンツは無断の複製や改竄などの不正使用から保護を受ける。一方、著作物の正当な利用者においては、私的な使用、すなわち個人的に又は家庭内その他これに準ずる限られた範囲内において使用することを目的としてコンテンツを複製することが許されている。

そこで、本発明では、ホーム・ネットワーク内のクライアント端末は、私的な使用の範囲内にあるという前提に立ち、ローカル環境下のクライアントに限り、ホーム・サーバ上に蓄積されているコンテンツを利用することができるようにした。

前記ホーム・ネットワーク上には２台以上のホーム・サーバを設置可能である。このような場合、各ホーム・サーバは、同じホーム・ネットワーク上のクライアント端末はローカル環境下にあることから、それぞれ独自にこれらをメンバー登録してグループを形成し、コンテンツ配信並びにコンテンツ使用のライセンスを発行する。さらに、クライアント端末は、同じホーム・ネットワーク上の２台以上のホーム・サーバに対し同時にメンバー登録し複数のグループに所属し、各々のホーム・サーバからコンテンツのライセンスを取得することができる。

この場合も、クライアント端末は、それぞれのホーム・サーバにとってローカル環境下に存在し、個人的又は家庭の範囲内での使用であると推定されるから、

ローカル環境内の各ホーム・サーバのコンテンツを自由に使用することが相当である。

一方、クライアント端末が複数のホーム・サーバに同時にメンバー登録できるからといって、時間差をおいて、複数のホーム・ネットワークに跨って複数のホーム・サーバのグループに所属することまでは認めるべきでない。別のホーム・ネットワークに接続した時点で、元の接続先のホーム・ネットワークから見ればクライアント端末がリモート環境に移動したことに相当し、あるいは、あるホーム・ネットワークに接続した時点で他のホーム・ネットワークにとってクライアント端末はリモート環境に存在することに等しいからである。

したがって、クライアントは、同じホーム・ネットワーク上の複数のホーム・サーバから取得したコンテンツを利用可能であるが、別のホーム・ネットワーク上のホーム・サーバに接続した時点で、それ以外のホーム・ネットワーク上のホーム・サーバから取得したコンテンツを利用不能とする。

前記ローカル環境管理手段は、例えば、アクセス要求元の機器のＭＡＣアドレスがデフォルト・ゲートウェイ（ｄｅｆａｕｌｔ　ｇａｔｅｗａｙ）に設定されているルータのＭＡＣアドレスに一致しないかどうかによって同じホーム・ネットワーク上に存在するかどうかを確認することができる。

ホーム・ネットワークはホーム・ルータ経由で外部ネットワークに接続されている。そして、同じネットワークからのアクセスであれば送信元のＭＡＣアドレスが付されているが、外部からのルータ越しのアクセスの場合は送信元がルータのＭＡＣアドレスに書き換えられる。このような既存のＩＰプロトコルの仕組みを利用し、通信相手のＭＡＣアドレスをホーム・ルータのＭＡＣアドレスと比較することによりホーム・ネットワーク内からのアクセスであるかどうかを自動識別することができるという訳である。

あるいは、前記ローカル環境管理手段は、各機器がホーム・ネットワークに関する同じ識別情報を共有するかどうかによって同じホーム・ネットワーク上に存在するかどうかを確認することができる。

例えば、各機器はデフォルト・ゲートウェイに設定されているルータのＭＡＣアドレスをホーム・ネットワークに関する識別情報として取得し、機器同士が同

じデフォルト・ゲートウェイのＭＡＣアドレスを保持しているかどうかによって同じホーム・ネットワーク上に存在するかどうかを確認する。

または、ホーム・ネットワーク上にネットワーク識別情報を供給するローカル環境管理装置を設置しておき、各機器は前記ローカル環境管理装置のＭＡＣアドレスをホーム・ネットワークに関する識別情報として取得し、機器同士が同じローカル環境管理装置のＭＡＣアドレスを保持しているかどうかによって同じホーム・ネットワーク上に存在するかどうかを確認することができる。

また、本発明の第２の側面は、ルータ経由で外部ネットワークに接続され、外部ネットワークからコンテンツを正当に取得するホーム・サーバとコンテンツを要求し利用するクライアントが存在するホーム・ネットワーク上において機器を認証するための処理をコンピュータ・システム上で実行するようにコンピュータ可読形式で記述されたコンピュータ・プログラムであって、

前記ホーム・サーバと前記クライアントが前記ホーム・ネットワーク上に存在するかどうかを確認するローカル環境管理ステップと、

双方の機器が同じホーム・ネットワーク上に存在することが前記ローカル環境管理ステップにより確認されたことに応じて、前記ホーム・サーバは前記クライアントに対しコンテンツの提供及び／又はコンテンツに関するライセンスの発行を行なうコンテンツ提供ステップと、

を具備することを特徴とするコンピュータ・プログラムである。

本発明の第２の側面に係るコンピュータ・プログラムは、コンピュータ・システム上で所定の処理を実現するようにコンピュータ可読形式で記述されたコンピュータ・プログラムを定義したものである。換言すれば、本発明の第２の側面に係るコンピュータ・プログラムをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され、本発明の第１の側面に係る機器間認証システムと同様の作用効果を得ることができる。

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施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

図１は、ホーム・ネットワークの基本構成を模式的に示した図である。

図２は、２台のホーム・サーバが存在するホーム・ネットワークの構成例を示した図である。

図３は、クライアント端末が複数のホーム・ネットワークに跨って接続する様子を示した図である。

図４は、本発明の一実施形態に係るホーム・ネットワークの構成を模式的に示した図である。

図５は、本発明の他の実施形態に係るホーム・ネットワークの構成を模式的に示した図である。

図６は、サーバやクライアントなどとしてホーム・ネットワークに接続されるホスト装置のハードウェア構成を模式的に示した図である。

図７は、本発明に係るホーム・ネットワーク上での動作シーケンスを示した図である。

図８は、ローカル環境管理テーブルの構成を示した図である。

図９は、クライアント端末上でコンテンツを利用するときの処理手順を示したフローチャートである。

図１０は、図４に示したホーム・ネットワークの変形例を示した図である。

図１１は、本発明に係るホーム・ネットワーク上での動作シーケンスを示した図である。

図１２は、図１０の変形例を示した図である。

発明を実施するための最良の形態

以下、図面を参照しながら本発明の実施形態について詳解する。

著作権法の下、著作物としてのコンテンツは無断の複製や改竄などの不正使用

から保護を受ける。一方、著作物の正当な利用者においては、私的な使用、すなわち個人的に又は家庭内その他これに準ずる限られた範囲内において使用することを目的としてコンテンツを複製することが許されている（著作権法第３０条を参照のこと）。

本発明者らは、ホーム・ネットワーク内（以下、「ローカル環境」とも呼ぶ）のクライアント端末は、私的な使用の範囲内にあるという前提に立ち、ローカル環境下のクライアントに限り、ホーム・サーバ上に蓄積されているコンテンツを利用することができるというシステムを提案する。

ここで、ローカル環境の定義について説明しておく。

図１には、ホーム・ネットワークの基本構成を模式的に示している。同図に示すように、家庭内に敷設されるホーム・ネットワークは、ホーム・ルータ経由でインターネットなどの外部ネットワークに接続されている。

ホーム・ネットワーク上には、ホーム・サーバと、１以上のクライアント端末が存在する。ホーム・サーバは、ホーム・ルータ経由で外部ネットワーク上のコンテンツ・サーバから正当にコンテンツを取得し、蓄積し、家庭内でコンテンツを配信する。勿論、ホーム・サーバは、パッケージ・メディアや放送受信など、ネットワーク以外の手段により、コンテンツを取得することができる。また、各クライアント端末は、ホーム・サーバに所望のコンテンツを要求し、これを取得して利用する。

ホーム・ネットワークに接続されているクライアント端末は、ローカル環境下に存在し、個人的又は家庭の範囲内での使用であると推定される。したがって、ホーム・サーバにおいて正当に取得されているコンテンツは、ホーム・ネットワーク上のクライアント端末は自由に使用することが相当であると思料される。そこで、ホーム・サーバは、ローカル環境下のこれらクライアント端末をメンバー登録し、コンテンツ配信並びにコンテンツ使用のライセンスを発行する。勿論、クライアントの接続を無限に認めることはできないので、コンテンツを享受できる端末の台数に一定の制限を設ける必要がある。

ローカル環境下では、クライアント端末は、ホーム・サーバからコンテンツを取得し、コピーやストリーミングなどコンテンツを利用し、さらにローカル環境

外（リモート環境）にコンテンツを持ち出して利用することができる。

一方、ホーム・ネットワーク上に存在しない、すなわちリモート環境のクライアント端末は、個人的又は家庭の範囲内での使用であるとは考えられない。リモート環境のクライアント端末にコンテンツの利用を認めると、コンテンツの利用はほぼ無制限となってしまい、コンテンツに関する著作権は保護されないに等しくなるからである。そこで、ホーム・サーバは、リモート環境のクライアントをメンバーとして登録せず、また、コンテンツのライセンスを発行しない。

図１に示した例では、ホーム・ネットワーク上には１つのホーム・サーバしか存在しないが、勿論、２以上のホーム・サーバを同じホーム・サーバ上に設置して、各ホーム・サーバがホーム・ネットワーク内でそれぞれ独自にコンテンツの配信サービスを行なうようにしてもよい。

図２には、２台のホーム・サーバが存在するホーム・ネットワークの構成例を示している。

この場合、各ホーム・サーバは、同じホーム・ネットワーク上のクライアント端末はローカル環境下にあることから、それぞれ独自にこれらをメンバー登録してグループを形成し、コンテンツ配信並びコンテンツ使用のライセンスを発行する。クライアント端末は、ホーム・サーバからコンテンツを取得し、コピーやストリーミングなどコンテンツを利用し、さらにローカル環境外（リモート環境）にコンテンツを持ち出して利用することができる。

さらに、クライアント端末は、同じホーム・ネットワーク上の２台以上のホーム・サーバに対し同時にメンバー登録し複数のグループに所属し、各々のホーム・サーバからコンテンツのライセンスを取得することができる。この場合も、クライアント端末は、それぞれのホーム・サーバにとってローカル環境下に存在し、個人的又は家庭の範囲内での使用であると推定されるから、ローカル環境内の各ホーム・サーバのコンテンツを自由に使用することが相当であると思料される。

一方、クライアント端末が複数のホーム・サーバに同時にメンバー登録できるからといって、時間差をおいて、複数のホーム・ネットワークに跨って複数のホーム・サーバのグループに所属することまでは認めるべきでない（図３を参照のこと）。

別のホーム・ネットワークに接続した時点で、元の接続先のホーム・ネットワークから見ればクライアント端末がリモート環境に移動したことに相当し、あるいは、あるホーム・ネットワークに接続した時点で他のホーム・ネットワークにとってクライアント端末はリモート環境に存在することに等しいからである。ローカル環境が個人的又は家庭の範囲内であるのに対し、リモート環境は個人的又は家庭の範囲を逸脱する。

クライアント端末が時間差をかけて複数のホーム・ネットワークに跨って接続することは技術的には可能であるが、これに併せてコンテンツの利用を逐次許可していくと、コンテンツの利用はほぼ無制限となってしまい、コンテンツに関する著作権は保護されないに等しくなる。

以上を総括すると、ホーム・ネットワーク上において、個人的又は家庭の範囲内での使用であると推定されるローカル環境を実現するためには、以下の事柄が必要条件であることが導出される。

（1）ホーム・サーバは、ホーム・ネットワーク外からのメンバー登録を認めない。

（2）同じホーム・ネットワーク内に２台以上のホーム・サーバがあるときには、ホーム・サーバ毎にメンバー登録、グループ管理を行なう。ホーム・ネットワーク上の各クライアントは２以上のホーム・サーバに登録することができる。但し、同時登録されるホーム・サーバは同じホーム・ネットワークに存在しなければならない。

このようなローカル環境を実現するためには、ホーム・サーバとクライアント端末間で、お互い同じホーム・ネットワーク上に存在するかどうかを識別する仕組みが必要となる。

現状のネットワーク・プロトコルでは、ホーム・ネットワークなどネットワークをセグメント単位で識別する仕組みは提供されていない。そこで、本発明者らは、ホーム・ネットワークがホーム・ルータ経由で外部ネットワークに接続されていることを鑑み、同じネットワークからのアクセスであれば送信元のＭＡＣアドレスが付されているが、外部からのルータ越しのアクセスの場合は送信元がルータのＭＡＣアドレスに書き換えられるという既存のＩＰプロトコルの仕組みを

利用し、通信相手のＭＡＣアドレスをホーム・ルータのＭＡＣアドレスと比較することによりホーム・ネットワーク内からのアクセスであるかどうかを自動識別する方法を提案する。

以下、図面を参照しながら本発明の実施形態について詳解する。

図４には、本発明の一実施形態に係るホーム・ネットワークの構成を模式的に示している。

家庭内に敷設されるホーム・ネットワークは、ホーム・ルータ経由でインターネットなどＷＡＮ、あるいは他のＬＡＮに接続されている。ホーム・ネットワークのデフォルト・ゲートウェイはホーム・ルータに設定されている。

ホーム・ネットワークは、例えばハブ（集結装置）にホーム・サーバやクライアント端末などのホスト装置のＬＡＮケーブルを接続することにより構成される。

ホーム・サーバやクライアント端末、ホーム・ルータなどのホーム・ネットワーク上のホスト装置、並びに外部ネットワーク上のホスト装置は、機器固有のＭＡＣアドレスを有している。ホスト装置は、受信先ＭＡＣアドレス及び送信元ＭＡＣアドレスを含んだヘッダ情報を持つパケット、例えばイーサネット（登録商標）フレームを、ネットワーク経由で送受信する。

ホーム・サーバやクライアント端末などのホーム・ネットワーク上のホスト装置は、例えばＵＰｎＰ対応機器として構成される。この場合、ネットワークに対する接続機器の追加や削除が容易である。ホーム・ネットワークに新たに接続する機器は、以下の手順に従って、コンテンツ利用などホーム・ネットワーク上のサービスを享受することができるようになる。

（１）アドレッシング処理：ＩＰアドレスなどの自己のデバイスＩＤを取得する

（２）ディスカバリ処理：ネットワーク上の各デバイスの検索を行ない、各デバイスから受信した応答に含まれるデバイス種別や機能などの情報を取得する

（３）サービス要求処理：ディスカバリ処理で取得された情報に基づいて各デバイスにサービスを要求する

ホーム・ネットワーク上では、個人的又は家庭の範囲内での使用であると推定されるローカル環境が形成されている。したがって、ホーム・サーバは、ホーム・ルータ経由で外部ネットワーク上のコンテンツ・サーバから正当にコンテンツを

取得し、蓄積し、家庭内でコンテンツを配信する。また、各クライアント端末は、ホーム・サーバに所望のコンテンツを要求し、これを取得して利用することが許容される。

ローカル環境下では、クライアント端末は、ホーム・サーバからコンテンツを取得し、コピーやストリーミングなどコンテンツを利用し、さらにローカル環境外（リモート環境）にコンテンツを持ち出して利用することができる。

また、図５には、本発明の他の実施形態に係るホーム・ネットワークの構成を模式的に示している。

ホーム・ネットワークは、ホーム・ルータ経由でインターネットなどＷＡＮ、あるいは他のＬＡＮに接続されている。この場合も、ホーム・ネットワークのデフォルト・ゲートウェイ（ｄｅｆａｕｌｔ　ｇａｔｅｗａｙ）はホーム・ルータに設定されている。

図４との相違は、ホーム・ネットワーク上に２台のホーム・サーバが存在する点である。各ホーム・サーバは、ホーム・ネットワーク上に同時に存在してもよいし、あるいは時間差を以って接続されてもよい。

この場合、各ホーム・サーバは、同じホーム・ネットワーク上のクライアント端末はローカル環境下にあることから、これらをメンバー登録してグループを形成し、コンテンツ配信並びコンテンツ使用のライセンスを発行する。クライアント端末は、ホーム・サーバからコンテンツを取得し、コピーやストリーミングなどコンテンツを利用し、さらにローカル環境外（リモート環境）にコンテンツを持ち出して利用することができる。また、クライアント端末は、同じホーム・ネットワーク上の２台以上のホーム・サーバに対し同時にメンバー登録し複数のグループに所属し、各々のホーム・サーバからコンテンツのライセンスを取得することができる。

図６には、サーバやクライアントなどとしてホーム・ネットワークに接続されるホスト装置のハードウェア構成を模式的に示している。

このシステムは、プロセッサ１０を中心に構成されている。プロセッサ１０は、メモリに記憶されたプログラムに基づいて各種の処理を実行する。また、プロセッサは、バス３０を介して接続されている各種の周辺機器を制御している。バス

３０に接続された周辺機器は次のようなものである。

メモリ２０は、例えばＤＲＡＭ（Ｄｙｎａｍｉｃ ＲＡＭ）などの半導体メモリで構成され、プロセッサ１０において実行されるプログラム・コードをロードしたり、実行プログラムの作業データを一時格納したりするために使用される。

ディスプレイ・コントローラ２１は、プロセッサ１０から送られてくる描画命令に従って表示画像を生成し、表示装置２２に送る。ディスプレイ・コントローラに接続された表示装置２２は、ディスプレイ・コントローラ２１から送られた表示画像情報に従い、その画像を画面に表示出力する。

入出力インターフェース２３は、キーボード２４やマウス２５が接続されており、キーボード２４やマウス２５からの入力信号をプロセッサ１０へ転送する。

ネットワーク・インターフェース２６は、ＬＡＮやインターネットなどの外部ネットワークに接続されており、インターネットを介したデータ通信を制御する。すなわち、プロセッサ１０から送られたデータをインターネット上の他の装置へ転送するとともに、インターネットを介して送られてきたデータを受け取りプロセッサ１０に渡す。

ハード・ディスク装置（ＨＤＤ：Ｈａｒｄ Ｄｉｓｋ Ｄｒｉｖｅ）コントローラ２７には、ＨＤＤなどの大容量外部記憶装置２８が接続されており、ＨＤＤ コントローラ２７が接続されたＨＤＤ２８へのデータの入出力を制御する。ＨＤＤ２８には、プロセッサが実行すべきオペレーティング・システム（ＯＳ）のプログラム、アプリケーション・プログラム、ドライバ・プログラムなどが格納されている。アプリケーション・プログラムは、例えば、ホーム・サーバとしてホーム・ネットワーク上の各クライアント端末の認証処理を行なったり、コンテンツの提供やライセンスの発行を行なったりするサーバ・アプリケーションや、サーバから提供されたコンテンツの再生などコンテンツの利用を行なうクライアント・アプリケーションなどである。

なお、ホスト装置を構成するためには、図６に示した以外にも多くの電気回路などが必要である。但し、これらは当業者には周知であり、また、本発明の要旨を構成するものではないので、本明細書中では省略している。また、図面の錯綜を回避するため、図中の各ハードウェア・ブロック間の接続も一部しか図示して

いない点を了承されたい。

図７には、本実施形態に係るホーム・ネットワーク上での動作を示している。但し、ネットワーク上にはクライアント端末と、２台のホーム・サーバと、ホーム・ルータが少なくとも存在し、ホーム・ルータがデフォルト・ゲートウェイに設定されているものとする。

クライアント端末は、ホーム・サーバからコンテンツを取得し、コピーやストリーミングなどコンテンツを利用するが、各ホーム・サーバはコンテンツ配信サービスの開始に先立ち、ホーム・ルータからデフォルト・ゲートウェイのＭＡＣアドレスを取得しておく。

クライアント端末は、サーバにアクセスする際、まずホーム・ルータからデフォルト・ゲートウェイのＭＡＣアドレスを取得し、取得したＭＡＣアドレスを付してサーバにアクセス要求を送信する。

アクセス要求されたサーバ側では、要求パケットから送信元のＭＡＣアドレスを取り出して、これを自身があらかじめ取得しておいたデフォルト・ゲートウェイのＭＡＣアドレスと比較する。同じネットワークからのアクセスであれば送信元のＭＡＣアドレスが付されているが、外部からのルータ越しのアクセスの場合は送信元がルータのＭＡＣアドレスに書き換えられる。したがって、送信元のＭＡＣアドレスがデフォルト・ゲートウェイのＭＡＣアドレスと一致するかどうかによって、要求元のクライアントが同じホーム・ネットワークすなわちローカル環境に置かれているかどうかを簡易に判別することができる。そして、ローカル環境に置かれている場合には要求されたコンテンツを配信するとともにそのライセンスを発行するが、ローカル環境に置かれていない場合は要求を拒否する。このようにして形成されたローカル環境内においてのみ、機器間でコンテンツの利用を認めることにより、コンテンツの不正流通を効果的に抑制することができる。

クライアント端末は、要求先サーバから返送パケットを受け取ると、サーバのＭＡＣアドレスとサーバ名を取り出し、これをアクセス要求に先立って取得したデフォルト・ゲートウェイのＭＡＣアドレスと組にしてローカル環境管理テーブルに格納しておく。

図８には、ローカル環境管理テーブルの構成を模式的に示している。図示のロ

ーカル環境管理テーブルは、新たなサーバに対してコンテンツ要求が行なわれる度にレコードがエントリされる。各レコードはＬＡＳＴフラグと、ネットワーク識別ＩＤと、サーバのＭＡＣアドレスと、サーバ名が格納される。ネットワーク識別ＩＤには、サーバ・アクセス時に先立って取得されたデフォルト・ゲートウェイのＭＡＣアドレスが記載される。また、ＬＡＳＴフラグは、最後にアクセスされたサーバのレコードにフラグが設定されるようになっている。

図８に示す例では、クライアント端末は、ホーム・ルータＡに接続されているホーム・ネットワーク上のサーバＳ１、ホーム・ルータＡに接続されているホーム・ネットワーク上のサーバＳ２、並びにホーム・ルータＢに接続されているホーム・ネットワーク上のサーバＳ３にアクセスした履歴が示されている。また、クライアント端末が最後にアクセスしたのはホーム・ルータＡに接続されているホーム・ネットワーク上のサーバＳ２である。

クライアント端末は、同じホーム・ネットワーク上の２台以上のホーム・サーバに対し同時にメンバー登録し複数のグループに所属し、各々のホーム・サーバからコンテンツのライセンスを取得することができる。この場合、クライアント端末は、それぞれのホーム・サーバにとってローカル環境下に存在し、個人的又は家庭の範囲内での使用であると推定されるからである。

他方、クライアント端末が時間差をかけて別のホーム・ネットワークに接続した場合、その時点で、元の接続先のホーム・ネットワークから見ればクライアント端末がリモート環境に移動したことに相当する。クライアント端末がサーバにアクセスする際に所得するデフォルト・ゲートウェイのＭＡＣアドレスをローカル環境管理テーブル上で照合し、ホーム・ネットワーク間で移動したかどうかを判別することができる。

クライアント端末は、ホーム・サーバからコンテンツを取得し、コピーやストリーミングなどコンテンツを利用し、さらにローカル環境外（リモート環境）にコンテンツを持ち出して利用することができる。但し、時間差をかけて複数のホーム・ネットワークに接続して、逐次取得されるコンテンツを無制限に利用することは認められない。そこで、本実施形態では、クライアント端末上でのコンテンツの利用は、現在接続しているホーム・ネットワークから取得されたものに制

限するようにしている。

図８に示したローカル環境管理テーブル中のＬＡＳＴフラグは、最後にアクセスされたホーム・サーバを指示する。本実施形態では、最後にアクセスしたホーム・サーバが存在するホーム・ネットワークがクライアント端末の現在のローカル環境であると規定する。したがって、ＬＡＳＴフラグが付されたホーム・サーバと同じデフォルト・ゲートウェイのＭＡＣアドレスを持つホーム・サーバはローカル環境に存在すると推定される。

図９には、クライアント端末上でコンテンツを利用するときの処理手順をフローチャートの形式で示している。クライアント端末上でコンテンツを利用（再生）しようとするとき、ローカル環境管理テーブルを参照し、ＬＡＳＴフラグが設定されているレコードと同じデフォルト・ゲートウェイのＭＡＣアドレスを持つサーバが他にあるかどうかを判別し（ステップＳ１）、同じＭＡＣアドレスを持つサーバから取得したコンテンツを利用可能にし（ステップＳ２）、それ以外のサーバから取得したコンテンツを利用不能にする（ステップＳ３）。

上述した実施形態では、同じネットワークからのアクセスであれば送信元のＭＡＣアドレスが付されているが、外部からのルータ越しのアクセスの場合は送信元がルータのＭＡＣアドレスに書き換えられるという既存のＩＰプロトコルの仕組みを利用し、通信相手のＭＡＣアドレスをホーム・ルータのＭＡＣアドレスと比較することによりホーム・ネットワーク内からのアクセスであるかどうかを自動識別するというものであった。但し、ホスト装置が同じホーム・ネットワーク上にあることを識別する方法はこれに限定されない。

図１０には、図４に示したホーム・ネットワークの変形例を示している。

図示の例では、ホーム・ネットワークは、ホーム・ルータ経由でインターネットなどＷＡＮ、あるいは他のＬＡＮに接続されている。ホーム・ネットワークのデフォルト・ゲートウェイはホーム・ルータに設定されるが、これは任意である。

ホーム・ネットワークは、ハブにホーム・サーバやクライアント端末などのホスト装置のＬＡＮケーブルを接続することにより構成される。本実施形態では、ホーム・ネットワークに対して識別機能を付与するローカル識別装置がホーム・ネットワークに接続されている点が図４とは相違する。

ホーム・ネットワーク上では個人的又は家庭の範囲内での使用であると推定されるローカル環境が形成されている。したがって、ホーム・サーバは、ホーム・ルータ経由で外部ネットワーク上のコンテンツ・サーバから正当にコンテンツを取得し、蓄積し、家庭内でコンテンツを配信する。また、各クライアント端末は、ホーム・サーバに所望のコンテンツを要求し、これを取得して利用することが許容される（同上）。

図１１には、図１０に示したホーム・ネットワーク上での動作を示している。

クライアント端末は、ホーム・サーバからコンテンツを取得し、コピーやストリーミングなどコンテンツを利用するが、各ホーム・サーバはコンテンツ配信サービスの開始に先立ち、ローカル識別装置のＭＡＣアドレスを取得しておく。

クライアント端末は、サーバにアクセスする際、まずローカル識別装置のＭＡＣアドレスを取得し、取得したＭＡＣアドレスを付してホーム・サーバにアクセス要求を送信する。

アクセス要求されたサーバ側では、要求パケットからローカル識別装置のＭＡＣアドレスを取り出して、これを自身があらかじめ取得しておいたローカル識別装置のＭＡＣアドレスと比較する。そして、両者のＭＡＣアドレスと一致するかどうかによって、要求元のクライアントが同じホーム・ネットワークすなわちローカル環境に置かれているかどうかを簡易に判別する。ローカル環境に置かれている場合には要求されたコンテンツを配信するとともにそのライセンスを発行するが、ローカル環境に置かれていない場合は要求を拒否する。このようにして形成されたローカル環境内においてのみ、機器間でコンテンツの利用を認めることにより、コンテンツの不正流通を効果的に抑制することができる。

クライアント端末は、要求先サーバから返送パケットを受け取ると、サーバのＭＡＣアドレスとサーバ名を取り出し、これをアクセス要求に先立って取得したローカル識別装置のＭＡＣアドレスと組にして、ローカル環境管理テーブルに格納しておく。この場合のローカル環境管理テーブルの各レコードには、ネットワーク識別ＩＤには、デフォルト・ゲートウェイのＭＡＣアドレスに代えて、ローカル識別装置のＭＡＣアドレスが記載される。

図１２には、図１０に示したホーム・ネットワークの変形例を示している。図

示の通り、ローカル識別装置は、専用機としてホーム・ネットワークに接続される以外に、ホーム・ルータあるいはホーム・ネットワーク上の他のホスト装置に組み込んで構成することができる。

ローカル識別装置の必要条件として、クライアント端末からの要求に常時応答できることを挙げることができる。このため、ローカル識別装置は常に電源が投入された状態であり、且つ、家庭内に最低１台あることが好ましい。ホーム・サーバは、例えばＴＶ受像機やビデオ録画再生装置などであり、これらの機器は常時起動しているとは限らないので（電源が投入されていないためにローカル環境を確認できなくなる)、ローカル識別装置の要件として不十分である。一方、冷蔵庫は、一家に一台あり、常に電源が投入されていることから、ローカル識別装置としての要件を満たしている。加えて、冷蔵庫は重量物で、固定的・移動不能であることから、外部に持ち出して不正を働くことが困難であるという副次的な効果もある。

なお、ローカル識別装置は、１つのホーム・ネットワーク上に２台以上存在していてもよい。この場合、クライアント端末がローカル識別装置を指定して認証を要求し、あるいは逆にサーバがローカル識別装置を指定して認証を要求する。または､クライアント端末がローカル識別装置にサーバを指定して認証を要求し、ローカル識別装置がサーバと認証を行なう。

本明細書で説明した実施形態では、機器間の認証に機器のＭＡＣアドレスの照合を用いているが、ホーム・ルータやローカル識別装置はＭＡＣアドレスを暗号的な手段を用いて偽装困難な形で保持していることを前提とする。

追補

以上、特定の実施形態を参照しながら、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形態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、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。

産業上の利用可能性

本発明によれば、ルータ経由で外部ネットワークに接続されているホーム・ネットワーク上で機器間でのコンテンツの利用を好適に管理することができる、優れた機器間認証システム及び機器間認証方法、通信装置、並びにコンピュータ・プログラムを提供することができる。

また、本発明によれば、ホーム・ネットワーク上の各クライアント端末がホーム・サーバ上で正当に取得されているコンテンツを著作権法で認められる私的使用の範囲内で利用するように好適に管理することができる、優れた機器間認証システム及び機器間認証方法、通信装置、並びにコンピュータ・プログラムを提供することができる。

本発明によれば、ローカル環境内においてのみ、機器間でコンテンツの利用を認めることにより、コンテンツの不正流通を効果的に抑制することができる。

請求の範囲

1．ルータ経由で外部ネットワークに接続可能なホーム・ネットワーク上の機器を認証する機器間認証システムであって、

前記ホーム・ネットワーク上の機器に対してアクセスする他の機器が前記ホーム・ネットワーク上に存在するかどうかを確認するローカル環境管理手段を備える、

ことを特徴とする機器間認証システム。

2．一方の機器はコンテンツを正当に取得するホーム・サーバであり、他方の機器はホーム・サーバに対してコンテンツを要求し利用するクライアントであり、

双方の機器が同じホーム・ネットワーク上に存在することが確認されたことに応じて、前記ホーム・サーバは前記クライアントに対しコンテンツの提供及び／又はコンテンツに関するライセンスの発行を行なう、

ことを特徴とする請求項１に記載の機器間認証システム。

3．前記ホーム・ネットワーク上には２台以上のホーム・サーバを設置可能であり、

ホーム・サーバ毎に、同じホーム・ネットワーク上に存在することが確認されたクライアントに対しコンテンツの提供及び／又はコンテンツに関するライセンスの発行を行なう、

ことを特徴とする請求項１に記載の機器間認証システム。

4．クライアントは、同じホーム・ネットワーク上の２台以上のホーム・サーバからコンテンツの提供及び／又はコンテンツに関するライセンスの発行を受けることができる、

ことを特徴とする請求項３に記載の機器間認証システム。

5．クライアントは、同じホーム・ネットワーク上の複数のホーム・サーバから

取得したコンテンツを利用可能であるが、別のホーム・ネットワーク上のホーム・サーバに接続した時点で、それ以外のホーム・ネットワーク上のホーム・サーバから取得したコンテンツを利用不能となる、

ことを特徴とする請求項３に記載の機器間認証システム。

６．前記ローカル環境管理手段は、アクセス要求元の機器のＭＡＣアドレスがデフォルト・ゲートウェイに設定されているルータのＭＡＣアドレスに一致しないかどうかによって同じホーム・ネットワーク上に存在するかどうかを確認する、

ことを特徴とする請求項１に記載の機器間認証システム。

７．前記ローカル環境管理手段は、各機器がホーム・ネットワークに関する同じ識別情報を共有するかどうかによって同じホーム・ネットワーク上に存在するかどうかを確認する、

ことを特徴とする請求項１に記載の機器間認証システム。

８．各機器はデフォルト・ゲートウェイに設定されているルータのＭＡＣアドレスをホーム・ネットワークに関する識別情報として取得し、機器同士が同じデフォルト・ゲートウェイのＭＡＣアドレスを保持しているかどうかによって同じホーム・ネットワーク上に存在するかどうかを確認する、

ことを特徴とする請求項７に記載の機器間認証システム。

９．ホーム・ネットワーク上にネットワーク識別情報を供給するローカル環境管理装置を設置し、

各機器は前記ローカル環境管理装置のＭＡＣアドレスをホーム・ネットワークに関する識別情報として取得し、機器同士が同じローカル環境管理装置のＭＡＣアドレスを保持しているかどうかによって同じホーム・ネットワーク上に存在するかどうかを確認する、

ことを特徴とする請求項７に記載の機器間認証システム。

１０．ルータ経由で外部ネットワークに接続可能なホーム・ネットワーク上の機器を認証する機器間認証方法であって、

前記ホーム・ネットワーク上の機器に対してアクセスする他の機器が前記ホーム・ネットワーク上に存在するかどうかを確認するローカル環境管理ステップを備える、

ことを特徴とする機器間認証方法。

１１．一方の機器はコンテンツを正当に取得するホーム・サーバであり、他方の機器はホーム･サーバに対してコンテンツを要求し利用するクライアントであり、

双方の機器が同じホーム・ネットワーク上に存在することが前記ローカル環境管理ステップにより確認されたことに応じて、前記ホーム・サーバは前記クライアントに対しコンテンツの提供及び／又はコンテンツに関するライセンスの発行を行なう、

ことを特徴とする請求項１０に記載の機器間認証方法。

１２．前記ホーム・ネットワーク上には２台以上のホーム・サーバを設置可能であり、

ホーム・サーバ毎に、同じホーム・ネットワーク上に存在することが確認されたクライアントに対しコンテンツの提供及び／又はコンテンツに関するライセンスの発行を行なう、

ことを特徴とする請求項１０に記載の機器間認証方法。

１３．クライアントは、同じホーム・ネットワーク上の２台以上のホーム・サーバからコンテンツの提供及び／又はコンテンツに関するライセンスの発行を受けることができる、

ことを特徴とする請求項１２に記載の機器間認証方法。

１４．クライアントは、同じホーム・ネットワーク上の複数のホーム・サーバから取得したコンテンツを利用可能であるが、別のホーム・ネットワーク上のホー

ム・サーバに接続した時点で、それ以外のホーム・ネットワーク上のホーム・サーバから取得したコンテンツを利用不能となる、
ことを特徴とする請求項１２に記載の機器間認証方法。

１５．前記ローカル環境管理ステップでは、アクセス要求元の機器のＭＡＣアドレスがデフォルト・ゲートウェイに設定されているルータのＭＡＣアドレスに一致しないかどうかによって同じホーム・ネットワーク上に存在するかどうかを確認する、
ことを特徴とする請求項１０に記載の機器間認証方法。

１６．前記ローカル環境管理ステップでは、各機器がホーム・ネットワークに関する同じ識別情報を共有するかどうかによって同じホーム・ネットワーク上に存在するかどうかを確認する、
ことを特徴とする請求項１０に記載の機器間認証方法。

１７．前記ローカル環境管理ステップにおいて、各機器はデフォルト・ゲートウェイに設定されているルータのＭＡＣアドレスをホーム・ネットワークに関する識別情報として取得し、機器同士が同じデフォルト・ゲートウェイのＭＡＣアドレスを保持しているかどうかによって同じホーム・ネットワーク上に存在するかどうかを確認する、
ことを特徴とする請求項１６に記載の機器間認証方法。

１８．ホーム・ネットワーク上にネットワーク識別情報を供給するローカル環境管理装置が設置されており、
前記ローカル環境管理ステップにおいて、各機器は前記ローカル環境管理装置のＭＡＣアドレスをホーム・ネットワークに関する識別情報として取得し、機器同士が同じローカル環境管理装置のＭＡＣアドレスを保持しているかどうかによって同じホーム・ネットワーク上に存在するかどうかを確認する、
ことを特徴とする請求項１６に記載の機器間認証方法。

１９．ルータ経由で外部ネットワークに接続可能なホーム・ネットワーク上で動作する通信機器であって、

自己が接続されているホーム・ネットワーク経由でアクセスする他の機器が同じホーム・ネットワーク上に存在するかどうかを確認するローカル環境管理手段を備える、

ことを特徴とする通信機器。

２０．ホーム・ネットワーク上でコンテンツを提供するホーム・サーバとして動作し、

前記ローカル環境管理手段により同じホーム・ネットワーク上に存在することが確認された機器に対してのみコンテンツの提供及び／又はコンテンツに関するライセンスの発行を行なうコンテンツ提供手段をさらに備える、

ことを特徴とする請求項１９に記載の通信機器。

２１．ホーム・ネットワーク上でホーム・サーバに対してコンテンツを要求するクライアントとして動作し、

前記ローカル環境管理手段により同じホーム・ネットワーク上に存在することが確認されたホーム・サーバからのみコンテンツの提供及び／又はコンテンツに関するライセンスの発行を受けるコンテンツ利用手段をさらに備える、

ことを特徴とする請求項１９に記載の通信機器。

２２．前記ホーム・ネットワーク上には２台以上のホーム・サーバを設置可能であり、

前記コンテンツ利用手段は、前記ローカル環境管理手段により同じホーム・ネットワーク上に存在することが確認された２台以上のホーム・サーバからコンテンツの提供及び／又はコンテンツに関するライセンスの発行を受けることができる、

ことを特徴とする請求項２１に記載の通信機器。

２３．前記コンテンツ利用手段は、同じホーム・ネットワーク上の複数のホーム・サーバから取得したコンテンツを利用可能であるが、別のホーム・ネットワーク上のホーム・サーバに接続した時点で、それ以外のホーム・ネットワーク上のホーム・サーバから取得したコンテンツを利用不能となる、
ことを特徴とする請求項２１に記載の通信機器。

２４．前記ローカル環境管理手段は、アクセス要求元の機器のＭＡＣアドレスがデフォルト・ゲートウェイに設定されているルータのＭＡＣアドレスに一致しないかどうかによって同じホーム・ネットワーク上に存在するかどうかを確認する、
ことを特徴とする請求項１９に記載の通信機器。

２５．前記ローカル環境管理手段は、各機器がホーム・ネットワークに関する同じ識別情報を共有するかどうかによって同じホーム・ネットワーク上に存在するかどうかを確認する、
ことを特徴とする請求項１９に記載の通信機器。

２６．前記ローカル環境管理手段は、デフォルト・ゲートウェイに設定されているルータのＭＡＣアドレスをホーム・ネットワークに関する識別情報として取得するとともに、通信相手が同じデフォルト・ゲートウェイのＭＡＣアドレスを保持しているかどうかによって同じホーム・ネットワーク上に存在するかどうかを確認する、
ことを特徴とする請求項２５に記載の通信機器。

２７．ホーム・ネットワーク上にネットワーク識別情報を供給するローカル環境管理装置が設置されており、
前記ローカル環境管理手段は、前記ローカル環境管理装置のＭＡＣアドレスをホーム・ネットワークに関する識別情報として取得するとともに、通信相手が同じローカル環境管理装置のＭＡＣアドレスを保持しているかどうかによって同じホーム・ネットワーク上に存在するかどうかを確認する、

ことを特徴とする請求項２５に記載の通信機器。

２８．ルータ経由で外部ネットワークに接続可能で、コンテンツを正当に取得するホーム・サーバとコンテンツを要求し利用するクライアントが存在するホーム・ネットワーク上において、機器を認証するための処理をコンピュータ・システム上で実行するようにコンピュータ可読形式で記述されたコンピュータ・プログラムであって、

前記ホーム・サーバと前記クライアントが前記ホーム・ネットワーク上に存在するかどうかを確認するローカル環境管理ステップと、

双方の機器が同じホーム・ネットワーク上に存在することが前記ローカル環境管理ステップにより確認されたことに応じて、前記ホーム・サーバは前記クライアントに対しコンテンツの提供及び／又はコンテンツに関するライセンスの発行を行なうコンテンツ提供ステップと、

を具備することを特徴とするコンピュータ・プログラム。

補正書の請求の範囲

［２００４年8月１６日（１６．０８．０４）国際事務局受理 ： 出願当初の請求の範囲１、７、１０、１６、１９、２５、２８は補正された；出願当初の請求の範囲６、１５及び２４は取り下げられた。他の請求の範囲は変更なし。（１１頁）］

１．（補正後）ルータ経由で外部ネットワークに接続可能なホーム・ネットワーク上の機器を認証する機器間認証システムであって、

デフォルト・ゲートウェイに設定されている前記ルータのＭＡＣアドレスを保持する手段と、

前記ホーム・ネットワーク上の機器に対してアクセスする他の機器が前記ホーム・ネットワーク上に存在するかどうかを、該アクセス要求元の機器のＭＡＣアドレスがデフォルト・ゲートウェイに設定されているルータのＭＡＣアドレスに一致しないかどうかによって確認するローカル環境管理手段と、

を具備することを特徴とする機器間認証システム。

２．一方の機器はコンテンツを正当に取得するホーム・サーバであり、他方の機器はホーム・サーバに対してコンテンツを要求し利用するクライアントであり、

双方の機器が同じホーム・ネットワーク上に存在することが確認されたことに応じて、前記ホーム・サーバは前記クライアントに対しコンテンツの提供及び／又はコンテンツに関するライセンスの発行を行なう、

ことを特徴とする請求項１に記載の機器間認証システム。

３．前記ホーム・ネットワーク上には２台以上のホーム・サーバを設置可能であり、

ホーム・サーバ毎に、同じホーム・ネットワーク上に存在することが確認されたクライアントに対しコンテンツの提供及び／又はコンテンツに関するライセンスの発行を行なう、

ことを特徴とする請求項１に記載の機器間認証システム。

４．クライアントは、同じホーム・ネットワーク上の２台以上のホーム・サーバからコンテンツの提供及び／又はコンテンツに関するライセンスの発行を受けることができる、

ことを特徴とする請求項３に記載の機器間認証システム。

5．クライアントは、同じホーム・ネットワーク上の複数のホーム・サーバから取得したコンテンツを利用可能であるが、別のホーム・ネットワーク上のホーム・サーバに接続した時点で、それ以外のホーム・ネットワーク上のホーム・サーバから取得したコンテンツを利用不能となる、
ことを特徴とする請求項３に記載の機器間認証システム。

6．（削除）

7．（補正後）ルータ経由で外部ネットワークに接続可能なホーム・ネットワーク上の機器を認証する機器間認証システムであって、
同じホーム・ネットワーク上の機器同士でホーム・ネットワークに関する同じ識別情報を共有する手段と、
各機器がホーム・ネットワークに関する同じ識別情報を共有するかどうかによって同じホーム・ネットワーク上に存在するかどうかを確認するローカル環境管理手段と、
を具備することを特徴とする機器間認証システム。

8．各機器はデフォルト・ゲートウェイに設定されているルータのＭＡＣアドレスをホーム・ネットワークに関する識別情報として取得し、機器同士が同じデフォルト・ゲートウェイのＭＡＣアドレスを保持しているかどうかによって同じホーム・ネットワーク上に存在するかどうかを確認する、
ことを特徴とする請求項７に記載の機器間認証システム。

9．ホーム・ネットワーク上にネットワーク識別情報を供給するローカル環境管理装置を設置し、
各機器は前記ローカル環境管理装置のＭＡＣアドレスをホーム・ネットワークに関する識別情報として取得し、機器同士が同じローカル環境管理装置のＭＡＣアドレスを保持しているかどうかによって同じホーム・ネットワーク上に存在するかどうかを確認する、

ことを特徴とする請求項７に記載の機器間認証システム。

１０．（補正後）ルータ経由で外部ネットワークに接続可能なホーム・ネットワーク上の機器を認証する機器間認証方法であって、

デフォルト・ゲートウェイに設定されている前記ルータのＭＡＣアドレスを保持するステップと、

前記ホーム・ネットワーク上の機器に対してアクセスする他の機器が前記ホーム・ネットワーク上に存在するかどうかを、該アクセス要求元の機器のＭＡＣアドレスがデフォルト・ゲートウェイに設定されているルータのＭＡＣアドレスに一致しないかどうかによって確認するローカル環境管理ステップと、

を具備することを特徴とする機器間認証方法。

１１．一方の機器はコンテンツを正当に取得するホーム・サーバであり、他方の機器はホーム･サーバに対してコンテンツを要求し利用するクライアントであり、

双方の機器が同じホーム・ネットワーク上に存在することが前記ローカル環境管理ステップにより確認されたことに応じて、前記ホーム・サーバは前記クライアントに対しコンテンツの提供及び／又はコンテンツに関するライセンスの発行を行なう、

ことを特徴とする請求項１０に記載の機器間認証方法。

１２．前記ホーム・ネットワーク上には２台以上のホーム・サーバを設置可能であり、

ホーム・サーバ毎に、同じホーム・ネットワーク上に存在することが確認されたクライアントに対しコンテンツの提供及び／又はコンテンツに関するライセンスの発行を行なう、

ことを特徴とする請求項１０に記載の機器間認証方法。

１３．クライアントは、同じホーム・ネットワーク上の２台以上のホーム・サーバからコンテンツの提供及び／又はコンテンツに関するライセンスの発行を受けることができる、

ことを特徴とする請求項１２に記載の機器間認証方法。

１４．クライアントは、同じホーム・ネットワーク上の複数のホーム・サーバから取得したコンテンツを利用可能であるが、別のホーム・ネットワーク上のホーム・サーバに接続した時点で、それ以外のホーム・ネットワーク上のホーム・サーバから取得したコンテンツを利用不能となる、
ことを特徴とする請求項１２に記載の機器間認証方法。

１５．(削除)

１６．(補正後) ルータ経由で外部ネットワークに接続可能なホーム・ネットワーク上の機器を認証する機器間認証方法であって、
同じホーム・ネットワーク上の機器同士でホーム・ネットワークに関する同じ識別情報を共有するステップと、
各機器がホーム・ネットワークに関する同じ識別情報を共有するかどうかによって同じホーム・ネットワーク上に存在するかどうかを確認するローカル環境管理ステップと、
を具備することを特徴とする機器間認証方法。

１７．前記ローカル環境管理ステップにおいて、各機器はデフォルト・ゲートウェイに設定されているルータのＭＡＣアドレスをホーム・ネットワークに関する識別情報として取得し、機器同士が同じデフォルト・ゲートウェイのＭＡＣアドレスを保持しているかどうかによって同じホーム・ネットワーク上に存在するかどうかを確認する、
ことを特徴とする請求項１６に記載の機器間認証方法。

１８．ホーム・ネットワーク上にネットワーク識別情報を供給するローカル環境管理装置が設置されており、
前記ローカル環境管理ステップにおいて、各機器は前記ローカル環境管理装置のＭＡＣアドレスをホーム・ネットワークに関する識別情報として取得し、機器同士が同じローカル環境管理装置のＭＡＣアドレスを保持しているかどうかによ

って同じホーム・ネットワーク上に存在するかどうかを確認する、
ことを特徴とする請求項１６に記載の機器間認証方法。

１９．（補正後）ルータ経由で外部ネットワークに接続可能なホーム・ネットワーク上で、ホーム・サーバに対してコンテンツを要求するクライアントとして動作する通信機器であって、

デフォルト・ゲートウェイに設定されている前記ルータのＭＡＣアドレスを保持する手段と、

アクセス要求元の機器のＭＡＣアドレスがデフォルト・ゲートウェイに設定されているルータのＭＡＣアドレスに一致しないかどうかによって同じホーム・ネットワーク上に存在するかどうかを確認するローカル環境管理手段と、

ことを特徴とする通信機器。

２０．ホーム・ネットワーク上でコンテンツを提供するホーム・サーバとして動作し、

前記ローカル環境管理手段により同じホーム・ネットワーク上に存在することが確認された機器に対してのみコンテンツの提供及び／又はコンテンツに関するライセンスの発行を行なうコンテンツ提供手段をさらに備える、

ことを特徴とする請求項１９に記載の通信機器。

２１．ホーム・ネットワーク上でホーム・サーバに対してコンテンツを要求するクライアントとして動作し、

前記ローカル環境管理手段により同じホーム・ネットワーク上に存在することが確認されたホーム・サーバからのみコンテンツの提供及び／又はコンテンツに関するライセンスの発行を受けるコンテンツ利用手段をさらに備える、

ことを特徴とする請求項１９に記載の通信機器。

２２．前記ホーム・ネットワーク上には２台以上のホーム・サーバを設置可能であり、

前記コンテンツ利用手段は、前記ローカル環境管理手段により同じホーム・ネットワーク上に存在することが確認された２台以上のホーム・サーバからコンテンツの提供及び／又はコンテンツに関するライセンスの発行を受けることができ

る、

ことを特徴とする請求項２１に記載の通信機器。

２３．前記コンテンツ利用手段は、同じホーム・ネットワーク上の複数のホーム・サーバから取得したコンテンツを利用可能であるが、別のホーム・ネットワーク上のホーム・サーバに接続した時点で、それ以外のホーム・ネットワーク上のホーム・サーバから取得したコンテンツを利用不能となる、
ことを特徴とする請求項２１に記載の通信機器。

２４．（削除）

２５．（補正後）ルータ経由で外部ネットワークに接続可能なホーム・ネットワーク上で、ホーム・サーバに対してコンテンツを要求するクライアントとして動作する通信機器であって、
同じホーム・ネットワーク上の機器との間でホーム・ネットワークに関する同じ識別情報を共有する手段と、
各機器がホーム・ネットワークに関する同じ識別情報を共有するかどうかによって同じホーム・ネットワーク上に存在するかどうかを確認するローカル環境管理手段と、
を具備することを特徴とする通信機器。

２６．前記ローカル環境管理手段は、デフォルト・ゲートウェイに設定されているルータのＭＡＣアドレスをホーム・ネットワークに関する識別情報として取得するとともに、通信相手が同じデフォルト・ゲートウェイのＭＡＣアドレスを保持しているかどうかによって同じホーム・ネットワーク上に存在するかどうかを確認する、
ことを特徴とする請求項２５に記載の通信機器。

２７．ホーム・ネットワーク上にネットワーク識別情報を供給するローカル環境管理装置が設置されており、
前記ローカル環境管理手段は、前記ローカル環境管理装置のＭＡＣアドレスをホーム・ネットワークに関する識別情報として取得するとともに、通信相手が同

じローカル環境管理装置のＭＡＣアドレスを保持しているかどうかによって同じホーム・ネットワーク上に存在するかどうかを確認する、
ことを特徴とする請求項２５に記載の通信機器。

２８．（補正後）ルータ経由で外部ネットワークに接続可能で、コンテンツを正当に取得するホーム・サーバとコンテンツを要求し利用するクライアントが存在するホーム・ネットワーク上において、機器を認証するための処理をコンピュータ・システム上で実行するようにコンピュータ可読形式で記述されたコンピュータ・プログラムであって、

アクセス要求元のクライアントのＭＡＣアドレスがデフォルト・ゲートウェイに設定されているルータのＭＡＣアドレスに一致しないかどうかによって、前記ホーム・サーバと前記クライアントが前記ホーム・ネットワーク上に存在するかどうかを確認するローカル環境管理ステップと、

双方の機器が同じホーム・ネットワーク上に存在することが前記ローカル環境管理ステップにより確認されたことに応じて、前記ホーム・サーバは前記クライアントに対しコンテンツの提供及び／又はコンテンツに関するライセンスの発行を行なうコンテンツ提供ステップと、
を具備することを特徴とするコンピュータ・プログラム。

条約第１９条（１）に基づく説明書

請求の範囲第１項では、機器間認証システムがデフォルト・ゲートウェイに設定されている前記ルータのＭＡＣアドレスを保持する手段を備える点、並びにローカル環境管理手段が「アクセス要求元の機器のＭＡＣアドレスがデフォルト・ゲートウェイに設定されているルータのＭＡＣアドレスに一致しないかどうかによって」前記ホーム・ネットワーク上の機器に対してアクセスする他の機器が前記ホーム・ネットワーク上に存在するかどうかを確認するという点を明確にした。また、これに伴い、請求の範囲第６項を削除した。

また、請求の範囲第７項では、機器間認証システムが同じホーム・ネットワーク上の機器同士でホーム・ネットワークに関する同じ識別情報を共有する手段を備える点を明確にし、独立項とした。

また、請求の範囲第１０項では、機器間認証方法がデフォルト・ゲートウェイに設定されている前記ルータのＭＡＣアドレスを保持するステップを備える点、並びに、ローカル環境管理ステップでは、「アクセス要求元の機器のＭＡＣアドレスがデフォルト・ゲートウェイに設定されているルータのＭＡＣアドレスに一致しないかどうかによって」前記ホーム・ネットワーク上の機器に対してアクセスする他の機器が前記ホーム・ネットワーク上に存在するかどうかを確認するという点を明確にした。また、これに伴い、請求の範囲第１５項を削除した。

また、請求の範囲第１６項では、機器間認証方法が、同じホーム・ネットワーク上の機器同士でホーム・ネットワークに関する同じ識別情報を共有するステップを備えている点を明確にした。

また、請求の範囲第１９項では、通信機器がデフォルト・ゲートウェイに設定されている前記ルータのＭＡＣアドレスを保持する手段を備えている点、並びに、ローカル環境管理手段が、「アクセス要求元の機器のＭＡＣアドレスがデフォルト・ゲートウェイに設定されているルータのＭＡＣアドレスに一致しないかどうかによって」同じホーム・ネットワーク上に存在するかどうかを確認するという点を明確にした。また、これに伴い、請求の範囲第２４項を削除した。

また、請求の範囲第２５項では、通信機器が同じホーム・ネットワーク上の機

器同士でホーム・ネットワークに関する同じ識別情報を共有する手段を備える点を明確にし、独立項とした。

また、請求の範囲第２８項では、ローカル環境管理ステップでは、「アクセス要求元の機器のＭＡＣアドレスがデフォルト・ゲートウェイに設定されているルータのＭＡＣアドレスに一致しないかどうかによって」前記ホーム・ネットワーク上の機器に対してアクセスする他の機器が前記ホーム・ネットワーク上に存在するかどうかを確認するという点を明確にした。

なお、本願明細書の第１３頁第１行乃至同頁第３行には、「通信相手のＭＡＣアドレスをホーム・ルータのＭＡＣアドレスと比較することによりホーム・ネットワーク内からのアクセスであるかどうかを自動識別する」という点が明記されている。

また、本願明細書の第１９頁第１４行乃至同頁第１６行には、「アクセス要求されたサーバ側では、要求パケットからローカル識別装置のＭＡＣアドレスを取り出して、これを自身があらかじめ取得しておいたローカル識別装置のＭＡＣアドレスと比較する。そして、両者のＭＡＣアドレスと一致するかどうかによって、要求元のクライアントが同じホーム・ネットワークすなわちローカル環境に置かれているかどうかを簡易に判別する」という点が明記されている。

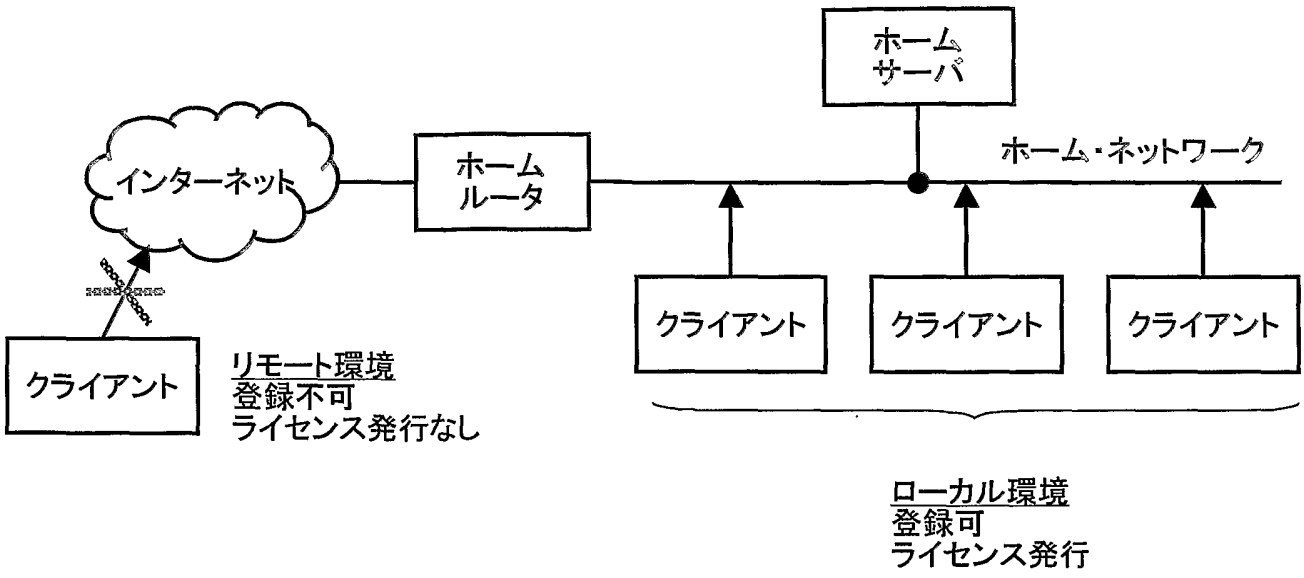

ホーム
サーバ
ホーム・ネットワーク
インターネット
ホーム
ルータ
クライアント
クライアント
クライアント
クライアント
リモート環境
登録不可
ライセンス発行なし
ローカル環境
登録可
ライセンス発行

図1

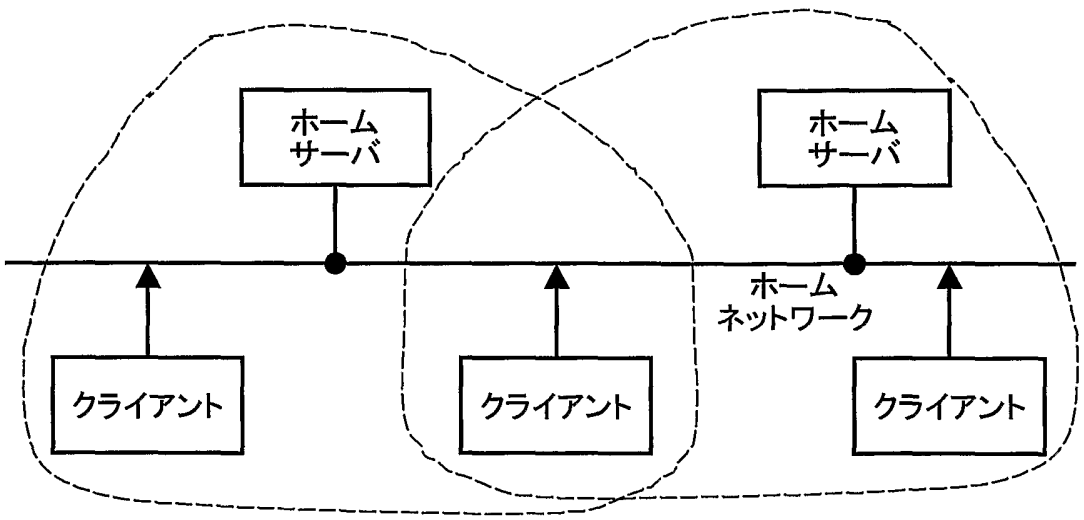

ホーム
サーバ
ホーム
サーバ
ホーム
ネットワーク
クライアント
クライアント
クライアント
2台のホーム・サーバ
に同時に登録可

図2

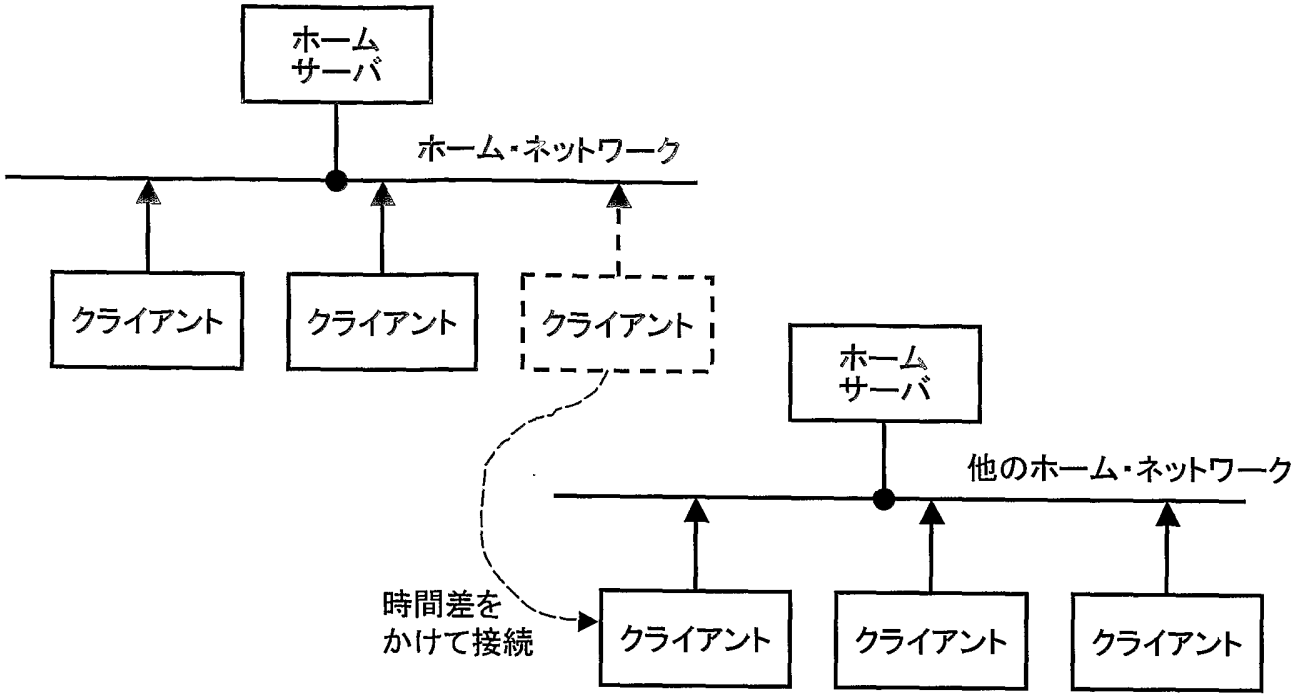

ホーム
サーバ
ホーム・ネットワーク
クライアント
クライアント
クライアント
ホーム
サーバ
他のホーム・ネットワーク
時間差を
かけて接続
クライアント
クライアント
クライアント

図3

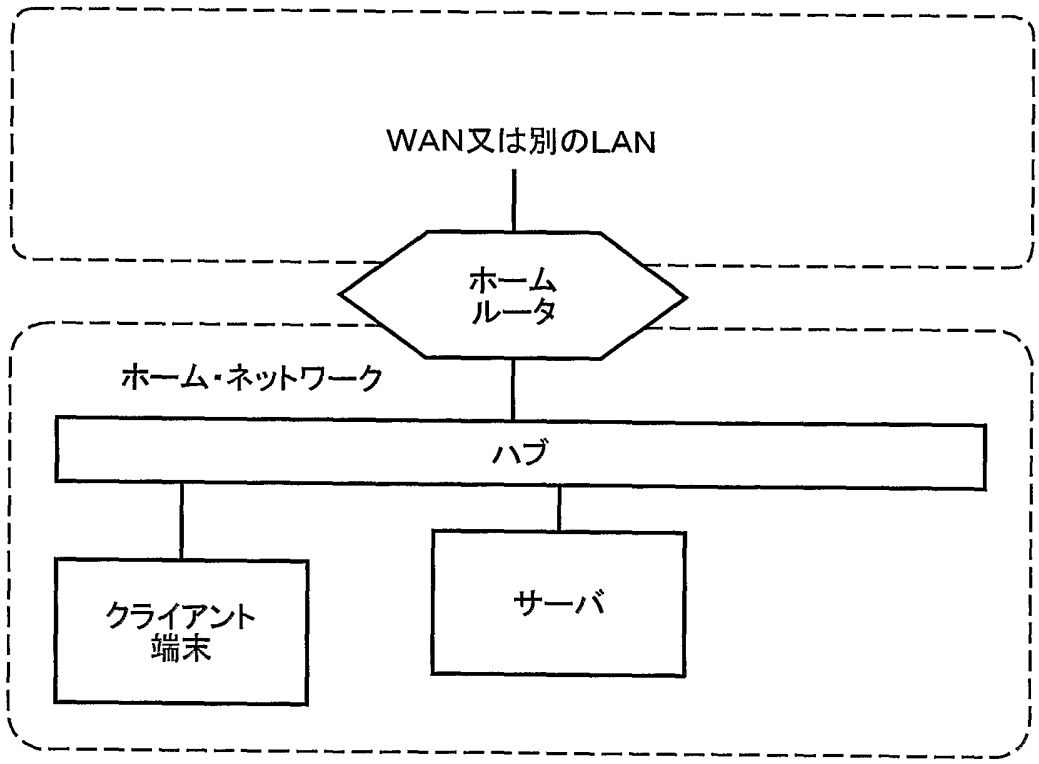

WAN又は別のLAN
ホーム
ルータ
ホーム・ネットワーク
ハブ
クライアント
端末
サーバ

図4

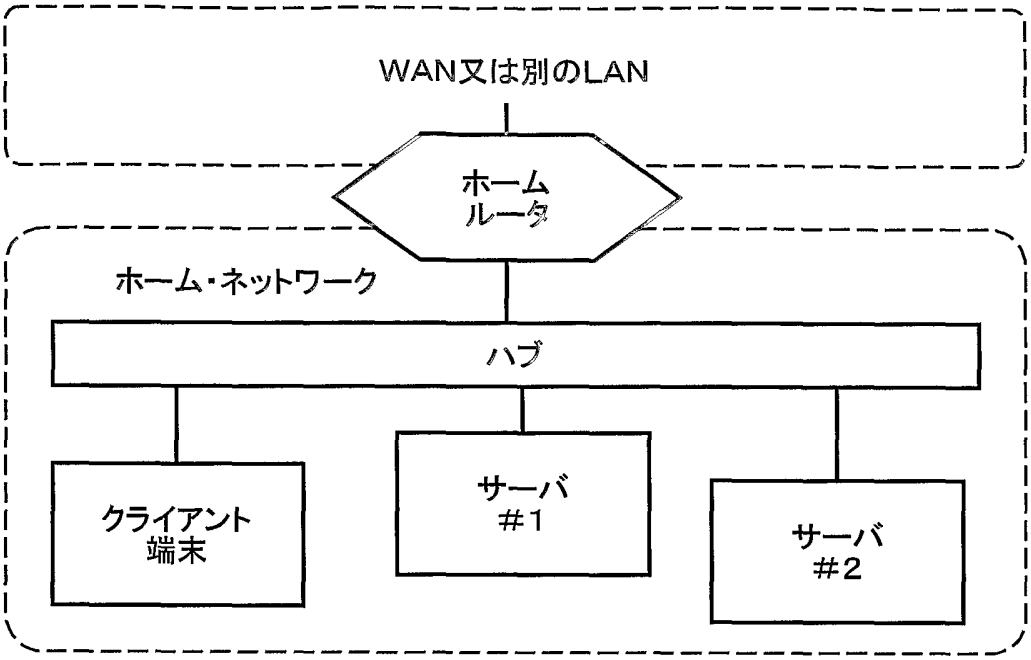

WAN又は別のLAN
ホーム
ルータ
ホーム・ネットワーク
ハブ
クライアント
端末
サーバ
#1
サーバ
#2

図5

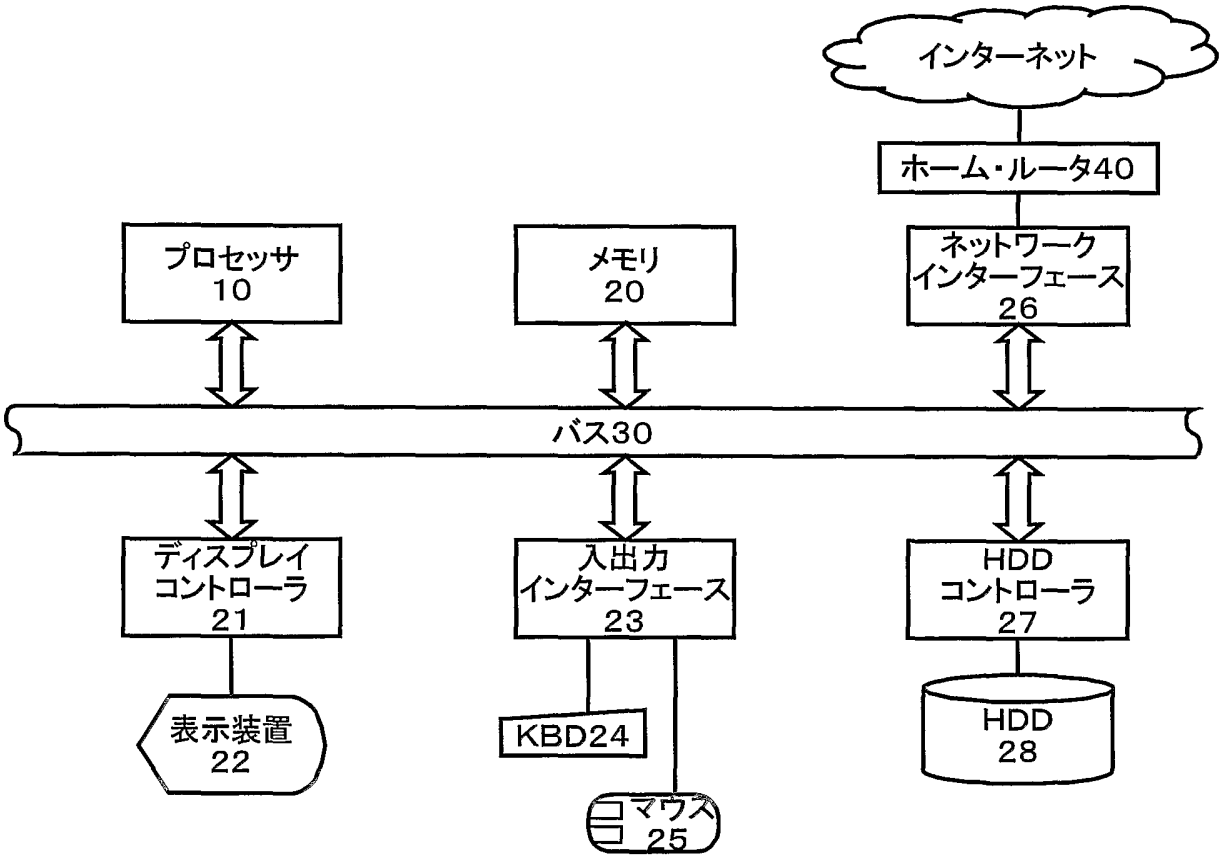

インターネット
ホーム・ルータ40
プロセッサ
10
メモリ
20
ネットワーク
インターフェース
26
バス30
ディスプレイ
コントローラ
21
入出力
インターフェース
23
HDD
コントローラ
27
表示装置
22
KBD24
マウス
25
HDD
28

図6

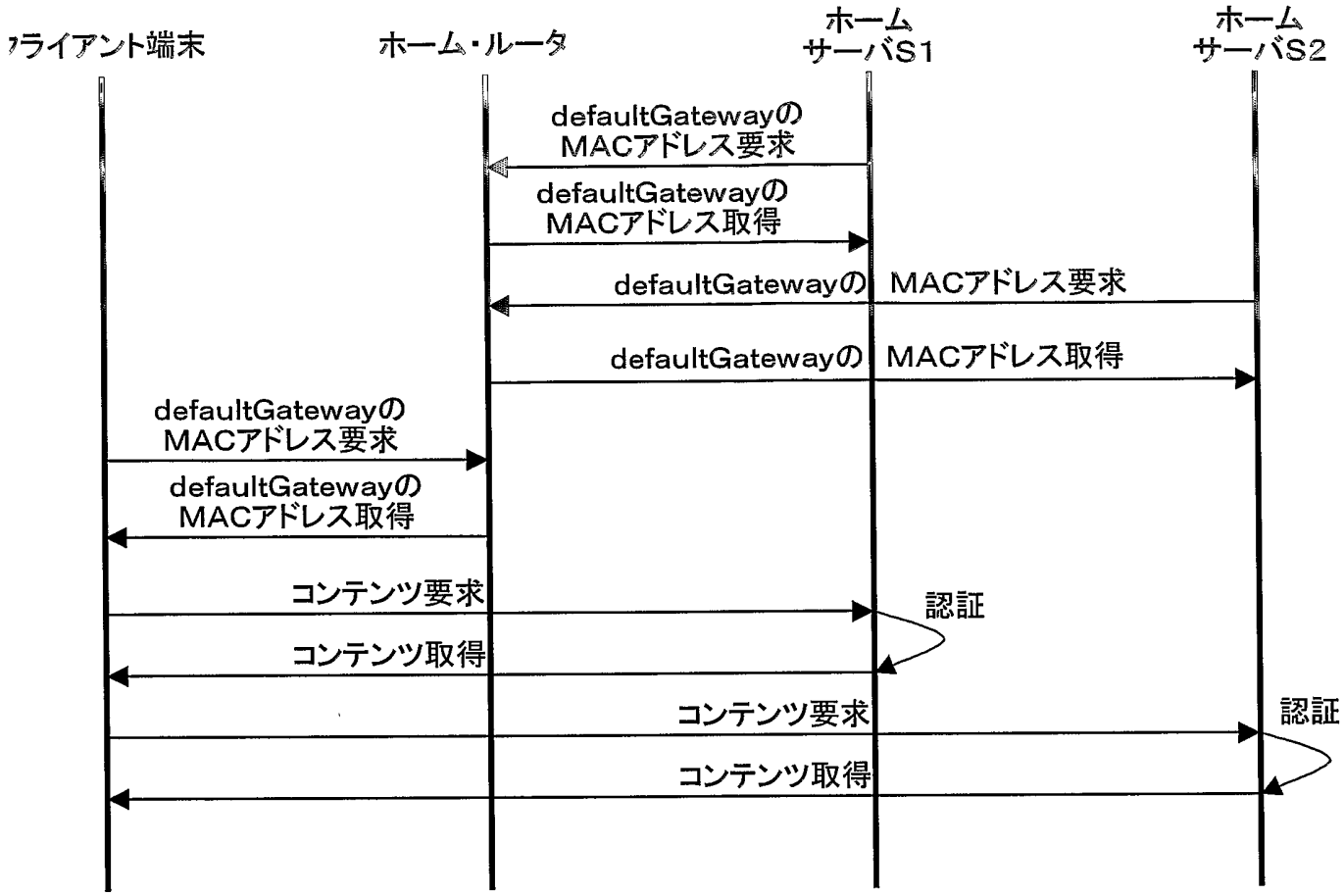


図7

LAST フラグ	ネットワーク識別ID	サーバのMACアドレス	サーバ名
	ホーム・ルータAの defaultGateway	サーバS1のMACアドレス	サーバS1
✓	ホーム・ルータAの defaultGateway	サーバS2のMACアドレス	サーバS2
	ホーム・ルータBの defaultGateway	サーバS3のMACアドレス	サーバS3

図8

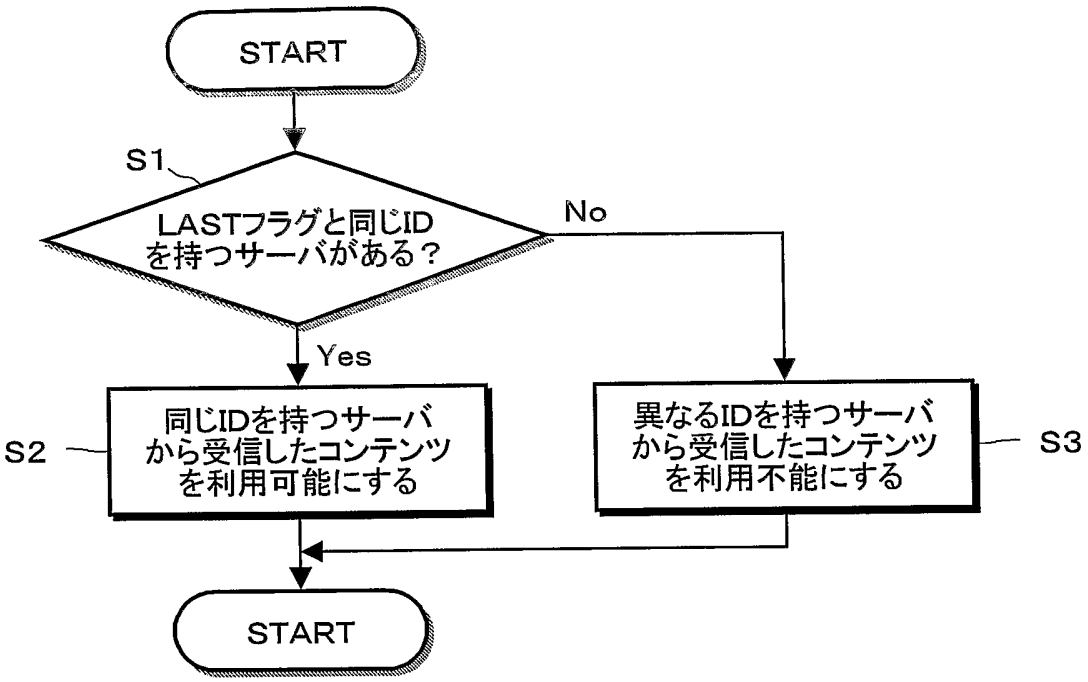

START
S1
LASTフラグと同じID
を持つサーバがある？
No
Yes
S2
同じIDを持つサーバ
から受信したコンテンツ
を利用可能にする
異なるIDを持つサーバ
から受信したコンテンツ
を利用不能にする
S3
START

図9

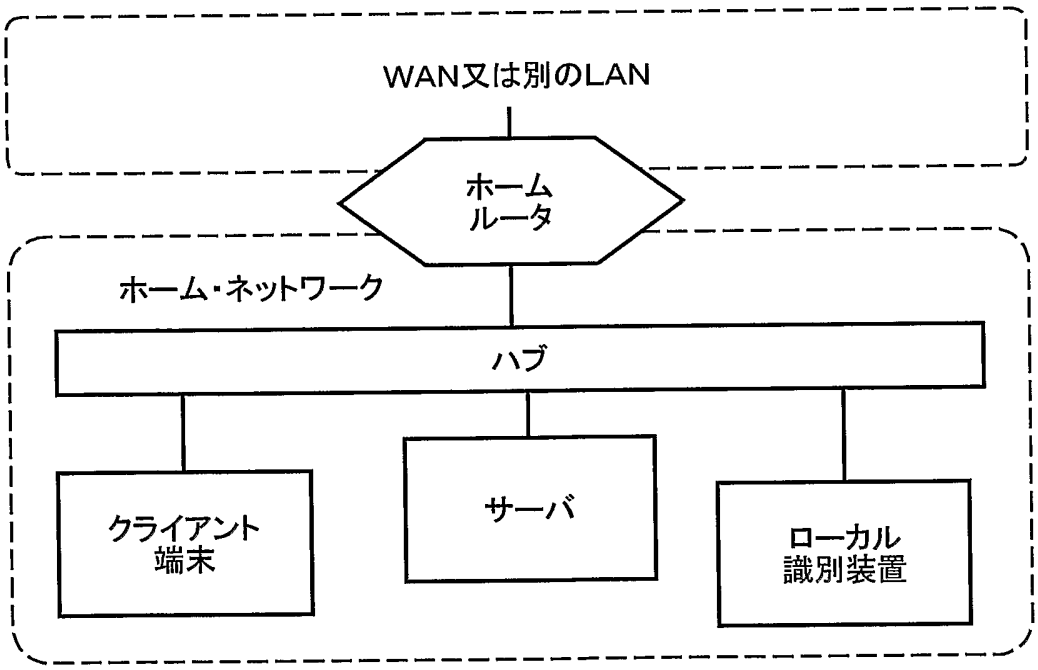

WAN又は別のLAN
ホーム
ルータ
ホーム・ネットワーク
ハブ
クライアント
端末
サーバ
ローカル
識別装置

図10

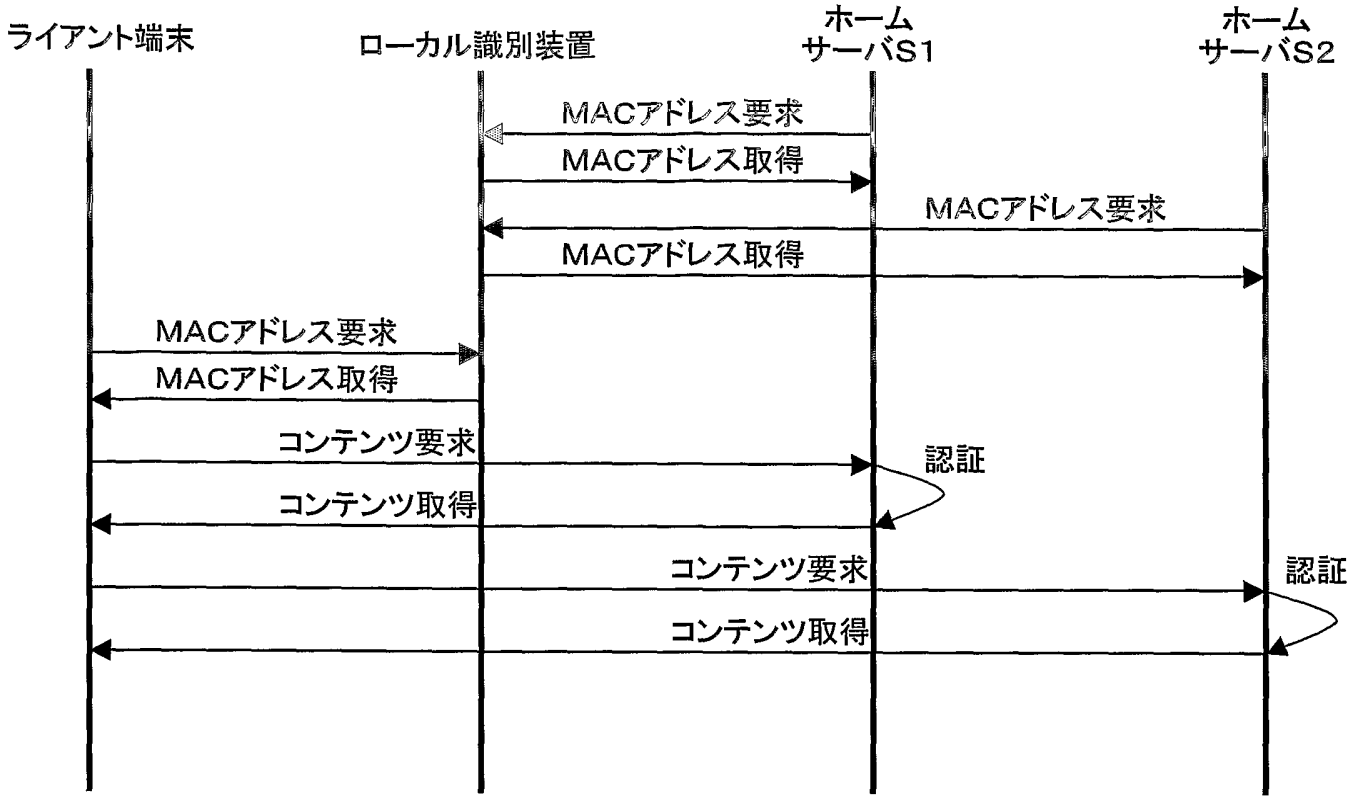

ライアント端末
ローカル識別装置
ホーム
サーバS1
ホーム
サーバS2
MACアドレス要求
MACアドレス取得
MACアドレス要求
MACアドレス取得
MACアドレス要求
MACアドレス取得
コンテンツ要求
認証
コンテンツ取得
コンテンツ要求
認証
コンテンツ取得

図11

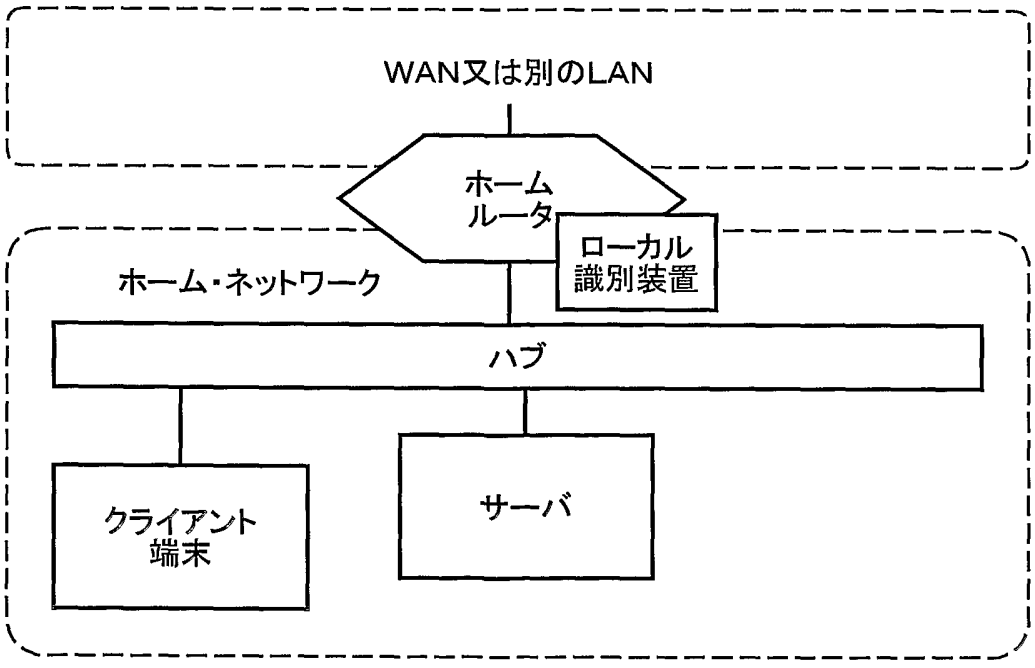

WAN又は別のLAN
ホーム
ルータ
ローカル
識別装置
ホーム・ネットワーク
ハブ
クライアント
端末
サーバ

図12

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/003336

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04L12/46, H04L12/66, G06F15/00

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] H04L12/46, H04L12/66, G06F15/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2004
Kokai Jitsuyo Shinan Koho 1971-2004 Jitsuyo Shinan Toroku Koho 1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y A	JP 11-203249 A (Fuji Xerox Co., Ltd.), 30 July, 1999 (30.07.99), Par. Nos. [0049] to [0056]; Fig. 7 (Family: none)	1-4,10-13, 19-20,28 5,14 6-9,15-18, 21-27
Y	JP 2003-076805 A (International Business Machines Corp.), 14 March, 2003 (14.03.03), Par. No. [0027] (Family: none)	5,14
A	JP 2001-285283 A (Toshiba Corp.), 12 October, 2001 (12.10.01), Fig. 3 (Family: none)	1-28

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
17 May, 2004 (17.05.04)	22 June, 2004 (22.06.04)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (January 2004)

国際調査報告

国際出願番号　PCT／JP2004／003336

A.　発明の属する分野の分類（国際特許分類（IPC））
Int. Cl⁷　　H04L12／46, H04L12／66, G06F15／00

B.　調査を行った分野
調査を行った最小限資料（国際特許分類（IPC））
Int. Cl⁷　　H04L12／46, H04L12／66, G06F15／00

最小限資料以外の資料で調査を行った分野に含まれるもの
日本国実用新案公報　　1922－1996年
日本国公開実用新案公報　　1971－2004年
日本国登録実用新案公報　　1994－2004年
日本国実用新案登録公報　　1996－2004年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X	JP　11－203249　A（富士ゼロックス株式会社） 1999．07．30，【0049】－【0056】，図7 （ファミリーなし）	1-4, 10-13, 19-20, 28
Y		5, 14
A		6-9, 15-18, 21-27

☒ C欄の続きにも文献が列挙されている。　　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
17．05．2004	22.6.2004

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）	
日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	中木　努	5X　9299
	電話番号　03－3581－1101　内線　3596	

C（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	JP　2003－076805　A（インターナショナル・ビジネス・マシーンズ・コーポレーション）2003．03．14，【0027】（ファミリーなし）	5,14
A	JP　2001－285283　A（株式会社東芝）2001．10．12，図3（ファミリーなし）	1-28