

(19) 日本国特許庁(JP)

(12) 特許公報(B2)

(11) 特許番号

特許第4085386号
(P4085386)

(45) 発行日 平成20年5月14日(2008.5.14)

(24) 登録日 平成20年2月29日(2008.2.29)

(51) Int.Cl.

H04Q 7/38 (2006.01)

F 1

H04B 7/26 109M

請求項の数 2 (全 14 頁)

(21) 出願番号 特願2003-316861 (P2003-316861)
 (22) 出願日 平成15年9月9日 (2003.9.9)
 (65) 公開番号 特開2005-86510 (P2005-86510A)
 (43) 公開日 平成17年3月31日 (2005.3.31)
 審査請求日 平成17年10月26日 (2005.10.26)

(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 100082131
 弁理士 稲本 義雄
 (72) 発明者 中野 雄彦
 東京都品川区北品川6丁目7番35号 ソニーブルーバード内

審査官 望月 章俊

(58) 調査した分野 (Int.Cl., DB名)
 H04B 7/24-7/26
 H04Q 7/00-7/38

(54) 【発明の名称】通信装置および方法

(57) 【特許請求の範囲】

【請求項 1】

ローカルネットワークを介して、通信範囲が限定されているコンテンツを他の通信装置に送信する通信装置において、

前記コンテンツを管理する管理手段と、

前記他の通信装置に対して認証データ生成の基となるデータを前記他の通信装置に送信し、その後、前記データを基に生成される認証データを応答メッセージとして返送することを要求する応答要求コマンドを前記他の通信装置に送信するとともに、前記応答要求コマンドを送信してから前記応答要求コマンドに対応する前記応答メッセージを受信するまでの応答時間と、前記応答メッセージに組み込まれた認証データに基づいて、前記他の通信装置が通信可能な装置であるか否かの判定を行い、その判定結果を表す判定結果情報を保存する通信可否判定手段と、

前記通信可否判定手段により記憶された前記判定結果情報に基づき、前記コンテンツ管理手段により管理されている前記コンテンツを前記他の通信装置に送信する送信制御手段と、

前記通信装置のAC電源プラグの抜き差しの状態を検知する電源状態検知手段とを備え、

前記送信制御手段は、前記コンテンツを前記他の通信装置に送信する際、前記判定結果情報が、前記他の通信装置が通信可能な装置でないことを示している場合、前記通信可否判定手段に前記判定を行わせ、その判定結果に基づいて前記コンテンツを前記他の通信装

置に送信するとともに、前記判定結果情報が前記他の通信装置が通信可能な装置であることを示している場合、前記他の通信装置が管理する、前記通信装置が前記他の通信装置に対して通信可能な装置であるかまたは通信可能な装置でないことを示す判定結果情報を取得し、その判定結果情報に基づいて、前記コンテンツを前記他の通信装置に送信し、

前記電源状態検知手段により電源状態の変化が検知された場合、前記判定結果情報を、前記他の通信装置が通信可能な装置でないことを示すように書き換える

通信装置。

【請求項 2】

ローカルネットワークを介して、通信範囲が限定されているコンテンツを他の通信装置に送信する通信装置の通信方法において、

10

前記コンテンツを管理する管理ステップと、

前記他の通信装置に対して認証データ生成の基となるデータを前記他の通信装置に送信し、その後、前記データを基に生成される認証データを応答メッセージとして返送することを要求する応答要求コマンドとを前記他の通信装置に送信するとともに、前記応答要求コマンドを送信してから前記応答要求コマンドに対応する前記応答メッセージを受信するまでの応答時間と、前記応答メッセージに組み込まれた認証データに基づいて、前記他の通信装置が通信可能な装置であるか否かの判定を行い、その判定結果を表す判定結果情報を保存する通信可否判定ステップと、

前記通信可否判定ステップの処理で記憶された前記判定結果情報に基づき、前記コンテンツ管理ステップの処理で管理されている前記コンテンツを前記他の通信装置に送信する送信制御ステップと、

20

前記通信装置のAC電源プラグの抜き差しの状態を検知する電源状態検知ステップとを含み、

前記送信制御ステップは、前記コンテンツを前記他の通信装置に送信する際、前記判定結果情報が、前記他の通信装置が通信可能な装置でないことを示している場合、前記通信可否判定ステップでの前記判定を行わせ、その判定結果に基づいて前記コンテンツを前記他の通信装置に送信するとともに、前記判定結果情報が前記他の通信装置が通信可能な装置であることを示している場合、前記他の通信装置が管理する、前記通信装置が前記他の通信装置に対して通信可能な装置であるかまたは通信可能な装置でないことを示す判定結果情報を取得し、その判定結果情報に基づいて、前記コンテンツを前記他の通信装置に送信し、

30

前記電源状態検知ステップの処理で電源状態の変化が検知された場合、前記判定結果情報を、前記他の通信装置が通信可能な装置でないことを示すように書き換える

通信方法。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、通信装置および方法に関し、特に、通信可能範囲が制限されているコンテンツを、適切に送信することができるようとした通信装置および方法に関する。

【背景技術】

【0002】

近年、インターネットに代表される公共性のある広域に亘るネットワーク（以下、WAN(Wide Area Network)と記述する）や一般家屋等に設けられる局所的なネットワーク（以下、LAN(Local Area Network)と記述する）の普及に伴い、それらのネットワークを介した各種データ通信が盛んに行われている。

40

【0003】

その通信形態の1つのとして、通信可能範囲を制限してコンテンツを提供することが考えられる。例えば、同一のLANに接続されている端末（通信距離が短い端末）間においてのみコンテンツの授受が可能となるように通信を制御するようなものである。

【発明の開示】

50

【発明が解決しようとする課題】**【0004】**

ところで、このように通信可能範囲が制限されている場合、通信相手が通信可能な範囲に存在するか否かを判別し（例えば、同一のLANに接続されているか否かを判定し）、その判定結果に基づいて、コンテンツの送信を行う必要があるが、従来においては、このようなコンテンツ送信を適切にかつ効率よく行う方法が存在しなかった。

【0005】

本発明はこのような状況に鑑みてなされたものであり、通信可能範囲が制限されているコンテンツを適切にかつ効率よく送信することができるようとするものである。

【課題を解決するための手段】

10

【0006】

本発明の一側面の通信装置は、ローカルネットワークを介して、通信範囲が限定されているコンテンツを他の通信装置に送信する通信装置において、前記コンテンツを管理する管理手段と、前記他の通信装置に対して認証データ生成の基となるデータを前記他の通信装置に送信し、その後、前記データを基に生成される認証データを応答メッセージとして返送することを要求する応答要求コマンドとを前記他の通信装置に送信するとともに、前記応答要求コマンドを送信してから前記応答要求コマンドに対応する前記応答メッセージを受信するまでの応答時間と、前記応答メッセージに組み込まれた認証データに基づいて、前記他の通信装置が通信可能な装置であるか否かの判定を行い、その判定結果を表す判定結果情報を保存する通信可否判定手段と、前記通信可否判定手段により記憶された前記判定結果情報に基づき、前記コンテンツ管理手段により管理されている前記コンテンツを前記他の通信装置に送信する送信制御手段と、前記通信装置のAC電源プラグの抜き差しの状態を検知する電源状態検知手段とを備え、前記送信制御手段は、前記コンテンツを前記他の通信装置に送信する際、前記判定結果情報が、前記他の通信装置が通信可能な装置でないことを示している場合、前記通信可否判定手段に前記判定を行わせ、その判定結果に基づいて前記コンテンツを前記他の通信装置に送信するとともに、前記判定結果情報が前記他の通信装置が通信可能な装置であることを示している場合、前記他の通信装置が管理する、前記通信装置が前記他の通信装置に対して通信可能な装置であるかまたは通信可能な装置でないことを示す判定結果情報を取得し、その判定結果情報に基づいて、前記コンテンツを前記他の通信装置に送信し、前記電源状態検知手段により電源状態の変化が検知された場合、前記判定結果情報を、前記他の通信装置が通信可能な装置でないことを示すように書き換える。

20

【0007】

本発明の一側面の通信方法は、ローカルネットワークを介して、通信範囲が限定されているコンテンツを他の通信装置に送信する通信装置の通信方法において、前記コンテンツを管理する管理ステップと、前記他の通信装置に対して認証データ生成の基となるデータを前記他の通信装置に送信し、その後、前記データを基に生成される認証データを応答メッセージとして返送することを要求する応答要求コマンドとを前記他の通信装置に送信するとともに、前記応答要求コマンドを送信してから前記応答要求コマンドに対応する前記応答メッセージを受信するまでの応答時間と、前記応答メッセージに組み込まれた認証データに基づいて、前記他の通信装置が通信可能な装置であるか否かの判定を行い、その判定結果を表す判定結果情報を保存する通信可否判定ステップと、前記通信可否判定ステップの処理で記憶された前記判定結果情報に基づき、前記コンテンツ管理ステップの処理で管理されている前記コンテンツを前記他の通信装置に送信する送信制御ステップと、前記通信装置のAC電源プラグの抜き差しの状態を検知する電源状態検知ステップとを含み、前記送信制御ステップは、前記コンテンツを前記他の通信装置に送信する際、前記判定結果情報が、前記他の通信装置が通信可能な装置でないことを示している場合、前記通信可否判定ステップでの前記判定を行わせ、その判定結果に基づいて前記コンテンツを前記他の通信装置に送信するとともに、前記判定結果情報が前記他の通信装置が通信可能な装置であることを示している場合、前記他の通信装置が管理する、前記通信装置が前記他の通信

30

40

50

装置に対して通信可能な装置であるかまたは通信可能な装置でないことを示す判定結果情報を取得し、その判定結果情報に基づいて、前記コンテンツを前記他の通信装置に送信し、前記電源状態検知ステップの処理で電源状態の変化が検知された場合、前記判定結果情報を、前記他の通信装置が通信可能な装置でないことを示すように書き換える。

【0008】

本発明の一側面の通信装置および通信方法においては、コンテンツが管理され、前記他の通信装置に対して認証データ生成の基となるデータが前記他の通信装置に送信され、その後、前記データを基に生成される認証データを応答メッセージとして返送することを要求する応答要求コマンドとが前記他の通信装置に送信されるとともに、前記応答要求コマンドを送信してから前記応答要求コマンドに対応する前記応答メッセージを受信するまでの応答時間と、前記応答メッセージに組み込まれた認証データに基づいて、前記他の通信装置が通信可能な装置であるか否かの判定が行われ、その判定結果を表す判定結果情報が保存され、記憶された前記判定結果情報に基づき、管理されている前記コンテンツが前記他の通信装置に送信され、前記通信装置のAC電源プラグの抜き差しの状態が検知される。前記コンテンツが前記他の通信装置に送信される際、前記判定結果情報が、前記他の通信装置が通信可能な装置でないことを示している場合、前記判定が行われ、その判定結果に基づいて前記コンテンツが前記他の通信装置に送信されるとともに、前記判定結果情報が前記他の通信装置が通信可能な装置であることを示している場合、前記他の通信装置が管理する、前記通信装置が前記他の通信装置に対して通信可能な装置であるかまたは通信可能な装置でないことを示す判定結果情報が取得され、その判定結果情報に基づいて、前記コンテンツが前記他の通信装置に送信され、電源状態の変化が検知された場合、前記判定結果情報が、前記他の通信装置が通信可能な装置でないことを示すように書き換えられる。

10

20

【発明の効果】

【0015】

本発明によれば、通信可能範囲が制限されているコンテンツを適切にかつ効率よく送信することができる。

【発明を実施するための最良の形態】

【0016】

図1は、本発明を適用した端末11からなる情報通信システムの構成例を示している。

30

【0017】

LAN1-1, 1-2(以下、個々に区別する必要がない場合、単位、LAN1と称する。他の場合についても同様である)がインターネットに代表されるWAN2を介して相互に接続されている。

【0018】

LAN1-1は、家屋A内に設けられ、例えば、その家族(特定の個人)が使用する程度の規模のものであり、それには、スイッチングハブ(図示せず)を介して、パソコンコンピュータやAV機器等の端末11-1および端末11-2が接続されている。LAN1-1と端末11-1および11-2との接続は、例えば、Ethernet(R)(100BASE-TX)等の高速インタフェースによる。端末11-1および11-2は、LAN1-1およびWN2を介して、LAN1-2に接続することができる。

40

【0019】

LAN1-2は、家屋B内に設けられ、LAN1-1と同様に、例えば、その家族(特定の個人)が使用する程度の規模のものであり、それには、端末11-3が接続されている。

【0020】

端末11は、通信可能範囲が制限されている所定のコンテンツを授受することができる。例えば、通信可能範囲が同一LAN1内に制限されている場合、端末11は、受信側の端末11が、自分と同じLAN1に接続されているか否かを判定し、その判定結果に基づいて、コンテンツの送信を行う。また所定の地域においてのみ配信可能なコンテンツに対

50

しては、端末 11 は、受信側の端末 11 がその領域に存在するか否かを判定し、その判定結果に基づいて、コンテンツの送信を行う。

【0021】

なおこのような通信制御は、映画などのコンテンツを一定の地域に対して先行配給し、他の地域には後日配給するなどのコンテンツ配給ビジネスに適用することができる。

【0022】

図2は、端末 11-1 の、本発明にかかる部分の構成例を示している。

【0023】

通信可否判定部 22 は、例えば、端末 11-2 または 11-3 に、通信可能範囲が制限されているコンテンツを送信する場合、通信部 26 を介して、受信側の端末 11 と後述するように通信することで、受信側の端末 11 が、通信可能な範囲に存在するか否かを判定し、その判定結果を利用して、受信側の端末 11 がそのコンテンツについて通信可能な端末 11 であるか否かを判定する。

【0024】

通信可否判定部 22 はまた、例えば、端末 11-2 または 11-3 において、通信可能範囲が制限されているコンテンツが受信されたとき、送信側の端末 11 がそのコンテンツについて通信可能な端末 11 であると判定する。

【0025】

移動検知部 23 は、端末 11-1 の移動を検知する。

【0026】

具体的には、外部の AC 電源 51 に接続されていたプラグ 25A が、AC 電源 51 から抜かれた場合、端末 11-1 は、別の場所に移動される可能性があるので、移動検知部 23 は、端末 11-1 と AC 電源 51 との接続状態を、各部に必要な電源を供給する電源部 25 を介して確認し、その接続が切断されたことをもって、端末 11-1 の移動を検知する。

【0027】

また移動検知部 23 は、電源部 25 を監視する代わりに、通信可否判定部 22 により通信可能とされた端末 11 との通信上の接続状態を、通信部 26 を介して確認し、その接続が切れたことをもって、端末 11-1 の移動を検知することもできる。なお通信上の接続状態の確認は、所定のバイアス電圧を利用する通信の場合、その電圧の変化を、定期的に所定の信号が授受される通信の場合、その信号の有無等を検出することによって行われる。また定期的に通信可能であるか否かを確認するようにして行うこともできる。

【0028】

コンテンツ管理部 24 は、受信側の端末 11 に送信されるコンテンツを格納したり、送信側の端末 11 から送信されてきたコンテンツを格納する。

【0029】

なお、コンテンツ管理部 24 を、他の端末 11 に送信されるコンテンツとしての放送を受信する放送チューナ、また他の端末 11 に送信されるコンテンツが記録されている記録メディアを再生する再生装置で構成することもできる。

【0030】

通信部 26 は、LAN 1-1 に接続されており、同一の LAN 1-1 内の端末 11-2 、または WAN 2 を介して異なる LAN 1-2 に接続されている端末 11-3 との通信を行う。

【0031】

制御部 21 は、例えば、端末 11-2 , 11-3 に対応する通信可否判定フラグ 31 を有している。フラグ 31A は、端末 11-2 に対応し、フラグ 31B は、端末 11-3 に対応する通信可否判定フラグ 31 である。なお、通信可否判定フラグ 31 は、揮発性メモリで構成されている。

【0032】

制御部 21 は、通信可否判定部 22 により、受信側の端末 11 または送信側の端末 11

10

20

30

40

50

が、通信可能な端末 1 1 であると判定された場合、その端末 1 1 に対応する通信可否判定フラグ 3 1 に 1 を設定する。すなわち 1 が設定された通信可否判定フラグ 3 1 は、それに對応する端末 1 1 が、端末 1 1 - 1 と通信可能な端末 1 1 であることを意味する。

【 0 0 3 3 】

制御部 2 1 はまた、移動検知部 2 3 により、端末 1 1 - 1 の移動が検知されたとき、通信可否判定フラグ 3 1 をリセットする。これは、通信可否判定部 2 2 による、受信側としての端末 1 1 または送信側としての端末 1 1 が通信可能な端末 1 1 であるか否かの判定は、端末 1 1 - 1 とそれらの端末 1 1 との通信距離、すなわち現状の位置関係に基づいてなされているので、端末 1 1 - 1 が移動された場合、先になされた通信可否判定部 2 2 による判定は意味をなさなくなるからである。

10

【 0 0 3 4 】

端末 1 1 - 2 と端末 1 1 - 3 は、端末 1 1 - 1 と同様に、図 2 に示した構成と同じ構成を有しているので、その図示および説明は省略する。

【 0 0 3 5 】

次に、図 3 のフローチャートを参照して、通信可能範囲が制限されているコンテンツを送信する場合の端末 1 1 の動作を説明する。

【 0 0 3 6 】

ステップ S 1 において、送信側の端末 1 1 の制御部 2 1 は、コンテンツ送信の指令が、例えば、図示せぬ操作部から入力されると、ステップ S 2 に進む。

20

【 0 0 3 7 】

ステップ S 2 において、送信側の端末 1 1 の制御部 2 1 は、受信側の端末 1 1 に対応する通信可否判定フラグ 3 1 に 1 が設定されているか否かを判定し、1 が設定されていないと判定した場合、ステップ S 3 に進む。

【 0 0 3 8 】

ステップ S 3 において、送信側の端末 1 1 の制御部 2 1 は、後述するようにして受信側の端末 1 1 が通信可能な端末 1 1 であるか否かの判定処理を行い、ステップ S 4 において、その処理結果に基づいて、受信側の端末 1 1 が通信可能な端末 1 1 であるか否かを判定する。

【 0 0 3 9 】

ステップ S 4 で、受信側の端末 1 1 が通信可能な端末 1 1 であると判定された場合、ステップ S 5 に進み、送信側の端末 1 1 の制御部 2 1 は、受信側の端末 1 1 に対応する通信可否判定フラグ 3 1 に 1 を設定する。

30

【 0 0 4 0 】

次に、ステップ S 6 において、送信側の端末 1 1 の制御部 2 1 は、通信部 2 6 を制御して、コンテンツ管理部 2 4 に格納されている所定のコンテンツを、受信側の端末 1 1 に送信させる。ステップ S 4 で、受信側の端末 1 1 が通信可能な端末 1 1 ではないと判定されたとき、ステップ S 5 , S 6 の処理はスキップされ、すなわち、コンテンツが送信されることなく、処理は終了する。

【 0 0 4 1 】

ステップ S 2 で、受信側の端末 1 1 に対応する通信可否判定フラグ 3 1 に 1 が設定されていると判定された場合、ステップ S 7 に進み、送信側の端末 1 1 の制御部 2 1 は、通信部 2 6 を制御して、受信側の端末 1 1 の、送信側の端末 1 1 に対応する通信可否判定フラグ 3 1 の内容の送信を要求するコマンドを、受信側の端末 1 1 を送信させる。

40

【 0 0 4 2 】

ステップ S 8 において、送信側の端末 1 1 の制御部 2 1 は、通信部 2 6 を介して、受信側の端末 1 1 から送信されてきた、受信側の端末 1 1 の、送信側の端末 1 1 に対応する通信可否判定フラグ 3 1 の内容を受信し、ステップ S 9 において、それが 1 であるか否かを判定する。

【 0 0 4 3 】

ステップ S 9 で、受信側の端末 1 1 の、送信側の端末 1 1 に対応する通信可否判定フラ

50

グ31が1であると判定されたとき、ステップS6に進み、送信側の端末11の制御部21は、通信部26を制御して、コンテンツ管理部24に格納されている所定のコンテンツを、受信側の端末11に送信させる。

【0044】

送信側の端末11の、受信側の端末11に対応する通信可否判定フラグ31に1が設定されていることは(ステップS2)、通信可否判定処理がすでになされ(ステップS3)、受信側の端末11は、通信可能な端末11であると判定されていることを意味し、そして受信側の端末11の、送信側の端末11に対応する通信可否判定フラグ31が1であることは(ステップS9)、受信側の端末11が、通信可否判定後移動されておらず、受信側の端末11が通信可能な端末11であることの判定は有効であることを意味しているので、この場合、通信可否判定は行われず(ステップS3乃至ステップS5がスキップされて)、コンテンツの送信が行われる(ステップS6)。

【0045】

一方、ステップS9で、受信側の端末11の、送信側の端末11に対する通信可否判定フラグ31が1ではないと判定されたとき、ステップS3に進み、送信側の端末11の制御部21は、受信側の端末11に対する通信可否判定を行う。

【0046】

受信側の端末11の、送信側の端末11に対応する通信可否判定フラグ31が1ではないとき(ステップS9)、受信側の端末11の移動があったことを意味しているので(正確には、移動された可能性があることを意味しているので)、この場合、ステップS3で、再度、受信側の端末11に対する通信可否判定がされる。

【0047】

以上のようにして端末11の移動を検知し、その移動がない場合、一度行った通信可否判定の結果が有効であるとして、コンテンツの送信を行うようにしたので、通信毎に通信可否判定を行わなくても、適切にコンテンツの送信を行うことができる。

【0048】

次に、コンテンツを受信する場合の端末11の動作を、図3のフローチャートを参照して説明する。

【0049】

ステップS21において、受信側の端末11の制御部21は、送信側の端末11から送信されてきた、受信側の端末11の、送信側の端末11に対応する通信可否判定フラグ31の送信を要求するコマンド(ステップS7)を受信すると、ステップS22において、通信部26を介して、そのフラグ31の内容を送信側の端末11に送信する。

【0050】

なお通信可否判定フラグ31を送信する場合、その改竄を防止するために、送信側の端末11と受信側の端末11で共通する秘密鍵で、通信可否判定フラグ31の内容を暗号化したり、通信可否判定フラグ31の内容とともに内容の鍵付きハッシュ値を伝送するようにもできる。この場合以外にも、送信側の端末11と受信側の端末11の送信については、適宜、このような改竄防止の対策を施すことができる。

【0051】

次に、ステップS23において、受信側の端末11の制御部21は、送信側の端末11において通信可否判定処理(ステップS3)が開始されたか否かを判定し、開始されたと判定した場合、ステップS24に進み、送信側の端末11の処理に対応して、後述するように通信可否判定処理を行う。

【0052】

ステップS23で、送信側の端末11において通信可否判定処理が開始されなかったと判定されたとき、またはステップS24で通信可否判定処理が行われたとき、ステップS25に進み、受信側の端末11の制御部21は、送信側の端末11からのコンテンツが受信されたか否かを判定し、受信されたと判定した場合、ステップS26に進む。

【0053】

10

20

30

40

50

ステップS26において、送信側の端末11からコンテンツが送信されたことは、送信側の端末11との通信が可能であることを意味しているので、受信側の端末11の制御部21は、受信側の端末11の、送信側の端末11に対応する通信可否判定フラグ31に1を設定する。その後、処理を終了する。

【0054】

次に、図3のステップS3の処理を行う場合の送信側の端末11の動作を、図4のフローチャートを参照して説明する。なおここでは、送信側の端末11は、所定のコマンドに対する受信側の応答時間に基づいて、受信側の端末11との位置関係を判定し、その判定結果に基づいて、受信側の端末11が、通信可能な端末であるか否かを判定する。

【0055】

ステップS31において、送信側の端末11の通信可否判定部22は、ランダムチャレンジを生成し、ステップS32において、通信部26を介して受信側の端末11に送信する。

【0056】

次に、ステップS33において、通信可否判定部22はまた、生成したランダムチャレンジに対して鍵付きハッシュ処理を施して、受信側の端末11で生成される認証データの期待値を生成する。

【0057】

なおこの例の場合、通信可否判定部22は、データ送信の可否を判定するのに、最大N(=1, 2, ...)回応答要求コマンドを送信するので、ここでは、送信され得るN個の応答要求コマンドに応じた認証データのN個の期待値が生成される。

【0058】

N個の期待値は、例えば、ランダムチャレンジに対して鍵付きハッシュ処理を施した結果得られたデータを複数個に分割し、その分割して得られたデータから生成することができる。

【0059】

ステップS34において、通信可否判定部22は、後述するように受信側の端末11から送信されてきた、ステップS32で送信されたランダムチャレンジを受信した旨を示すRC受信メッセージを(ステップS53)、通信部26を介して受信する。

【0060】

ステップS35において、通信可否判定部22は、応答要求コマンドが何番目に送信されるものか(送信の順番)を示すカウンタ*i*に1を初期設定する。

【0061】

次に、ステップS36において、通信可否判定部22は、通信部26を介して、応答要求コマンドを受信側の端末11に送信し、ステップS37において、応答時間の計測を開始する。なお通信可否判定部22は、この場合、図示せぬタイマーを内蔵しており、そのタイマーを起動させて、応答時間の計測を開始する。

【0062】

ステップS38において、通信可否判定部22は、後述するように受信側の端末11から送信されてきた、ステップS36で送信された応答要求コマンドに対する応答しての応答メッセージを、通信部26を介して受信し、ステップS39において、応答時間の計測を終了する。すなわちステップS37で開始しステップS39で終了する時間計測で得られた時間が受信側の端末11の応答時間となる。

【0063】

ステップS40において、通信可否判定部22は、応答メッセージに組み込まれている認証データと、ステップS33で生成した、その認証データの期待値(具体的には、カウンタ*i*が示す順番に送信された応答要求コマンド(以下、第*i*番目に送信された応答要求コマンドと称する)に対応する期待値)とが一致するか否かを判定し、一致すると判定した場合、受信側の端末11を、情報通信システムにおける正規の端末であると認証し、ステップS41に進む。

10

20

30

40

50

【0064】

ステップS41において、通信可否判定部22は、計測された、第*i*番目に送信された応答要求コマンドに対する受信側の端末11の応答時間が所定の時間Xを越えているか否かを判定する。時間Xは、例えば、同一LAN1に接続された端末11間で要する通信時間である。すなわち応答時間が時間Xを越える場合、受信側の端末11は、送信側の端末11と異なるLAN1に接続され、また、時間Xを越えない場合（応答時間 = 時間Xを含む）、同一のLAN1に接続されていると判定することができる（位置関係を判別することができる）。

【0065】

ステップS41で、時間Xを越えると判定された場合、ステップS42に進み、通信可否判定部22は、カウンタ*i*を1だけインクリメントする。 10

【0066】

ステップS43において、通信可否判定部22は、カウンタ*i* = N + 1であるか否かを判定し、カウンタ*i* = N + 1でないと判定した場合には、例えば所定時間経過後、ステップS36に戻る。

【0067】

ステップS40で、受信側の端末11が本情報通信システムにおける正規の機器ではないと判定されたとき、ステップS41で、第*i*番目に送信された応答要求コマンドに対する応答時間が、時間Xを越えないと判定された場合（受信側の端末11が、本情報通信システムにおける正規の機器であり、かつ、例えば送信側の端末11と同じLAN1に接続されている端末11であると判定されたとき）、またはステップS43で、カウンタ*i* = N + 1であると判定されたとき（応答要求コマンドの送信がN回行われたとき）、ステップS44に進み、通信可否判定部22は、それらの処理結果に基づいて、受信側の端末11が通信可能な端末11であるか否かを判定する。 20

【0068】

その後、ステップS45において、通信可否判定部22は、通信部26を介して、送信可否判定が終了した旨を表すメッセージ（以下、判定終了メッセージと称する）を受信側の端末11に送信する。その後、送信側の端末11の送信可否判定処理は、処理を終了する。

【0069】

次に、図3のステップS24の処理を行う場合の受信側の端末11の動作を、図4のフローチャートを参照して説明する。 30

【0070】

ステップS51において、受信側の端末11の通信可否判定部22は、送信先の端末11から送信されてきたランダムチャレンジを（ステップS32）、通信部26を介して受信する。ステップS52において、通信可否判定部22は、受信されたランダムチャレンジに対して、送信側の端末11における鍵付きハッシュ処理（ステップS33）と同様の鍵付きハッシュ処理を施し、認証データを生成する。

【0071】

なおこの例では、最大N個の応答要求コマンドを受信し得るので、その応答要求コマンドに対応する期待値と対比される（ステップS40）N個の認証データが生成される。 40

【0072】

このように認証データが生成されると、ステップS53において、通信可否判定部22は、通信部26を介して、RC受信メッセージを送信側の端末11に送信する。

【0073】

ステップS54において、通信可否判定部22は、これから受信する応答要求コマンドが何番目に受信されるものかを示すカウンタ*j*に1を初期設定し、ステップS55において、カウンタ*j*が示す順番に受信される応答要求コマンド（以下、第*j*番目に受信される応答要求コマンドと称する）に対応する認証データを組み込んだ応答メッセージを生成する。 50

【 0 0 7 4 】

次に、ステップ S 5 6において、通信可否判定部 2 2は、送信先の端末 1 1から送信されてきた応答要求コマンドを(ステップ S 3 6)、通信部 2 6を介して受信すると、ステップ S 5 7において、ステップ S 5 5で生成された第 j 番目に受信される応答要求コマンドに応じた認証データが組み込まれた応答メッセージを、通信部 2 6を介して、送信側の端末 1 1に送信する。これにより上述したように送信側の端末 1 1で(ステップ S 4 0で)、第 j 番目に受信された(第 i 番目に送信された)応答要求コマンドに対応する認証データと、第 i 番目に送信された(第 j 番目に受信された)応答要求コマンドの期待値とが比較される。

【 0 0 7 5 】

10

ステップ S 5 8において、受信側の端末 1 1の通信可否判定部 2 2は、送信側の端末 1 1から送信される判定終了メッセージ(ステップ S 4 5)が受信されたか否かを判定し、所定の時間内に受信されていないと判定した場合、ステップ S 5 9に進む。ステップ S 5 9において、通信可否判定部 2 2は、カウンタ j を 1だけインクリメントし、ステップ S 6 0で、カウンタ j = N + 1であるか否かを判定する。

【 0 0 7 6 】

ステップ S 6 0で、カウンタ j = j + 1ではないと判定されたとき(すなわち、応答要求コマンドが N 回受信されていないとき)、ステップ S 5 5に戻り、通信可否判定部 2 2は、次に受信される応答要求コマンドに対して、それ以降の処理を実行する。

【 0 0 7 7 】

20

ステップ S 5 8で、判定終了メッセージが受信されたとき、またはステップ S 6 0で、カウンタ j = N + 1であると判定されたとき(すなわち、応答要求コマンドが N 回受信されたとき)、受信側の端末 1 1の通信可否判定部 2 2は、通信可否判定処理を終了する。

【 0 0 7 8 】

次に、通信可能範囲が制限されているコンテンツを送信する場合の端末 1 1の他の動作を、図 5 のフローチャートを参照して説明する。この例の場合、送信側の端末 1 1は、ある場所に固定されており移動できないものとする。すなわちこの場合、図 3 のステップ S 2 の処理のように、自分の移動があったか否かの判定はなされない。

【 0 0 7 9 】

30

ステップ S 7 1において、送信側の端末 1 1の制御部 2 1は、コンテンツ送信の指令が、例えば、図示せず操作部から入力されると、ステップ S 7 2において、通信部 2 6を制御して、受信側の端末 1 1の、送信側の端末 1 1に対応する通信可否判定フラグ 3 1の内容の送信を要求するコマンドを、受信側の端末 1 1を送信させる。

【 0 0 8 0 】

ステップ S 7 3において、送信側の端末 1 1の制御部 2 1は、通信部 2 6を介して、受信側の端末 1 1から送信されてきた、受信側の端末 1 1の、送信側の端末 1 1に対応する通信可否判定フラグ 3 1の内容を受信し、ステップ S 7 4において、それが 1 であるか否かを判定する。

【 0 0 8 1 】

40

ステップ S 7 4で、受信側の端末 1 1の、送信側の端末 1 1に対応する通信可否判定フラグ 3 1が 1 ではないと判定されたとき、ステップ S 7 5に進み、制御部 2 1は、後述するようにして受信側の端末 1 1が通信可能な端末であるか否かを判定する。

【 0 0 8 2 】

次に、ステップ S 7 6において、送信側の端末 1 1の制御部 2 1は、ステップ S 7 5の判定処理の結果に基づいて、受信側の端末 1 1が通信可能な端末 1 1であるか否かを判定し、通信可能な端末 1 1であると判定した場合、ステップ S 7 7に進む。

【 0 0 8 3 】

ステップ S 7 7において、送信側の端末 1 1の制御部 2 1は、受信側の端末 1 1に対応する通信可否判定フラグ 3 1に 1 を設定する。

【 0 0 8 4 】

50

次に、ステップS78において、送信側の端末11の制御部21は、通信部26を制御して、コンテンツ管理部24に格納されている所定のコンテンツを、受信側の端末11に送信させる。

【0085】

ステップS76で、受信側の端末11が通信可能な端末11ではないと判定された場合、ステップS77、S78の処理はスキップされて、処理は終了する。

【0086】

ステップS74で、受信側の端末11の、送信側の端末11に対応する通信可否判定フラグ31が1であると判定された場合、ステップS75乃至ステップS77の処理はスキップされ、ステップS78に進み、所定のコンテンツが受信側の端末に送信される。 10

【0087】

受信側の端末11の、送信側の端末11に対応する通信可否判定フラグ31に1が設定されていることは、通信可否判定処理がすでになされ、受信側の端末11は、通信可能な端末11であると判定されていることを意味し、かつ、受信側の端末11が、通信可否判定後移動されておらず、受信側の端末11が通信可能な端末11であるとの判定は有効であることを意味しているので、この場合、通信可否判定は行われず（ステップS75乃至ステップ77がスキップされて）、コンテンツの送信が行われる（ステップS78）。

【0088】

なお、上述した送信側の端末11の動作に対応する受信側の端末11の動作は、後述するステップS94の処理を除き、図3における場合と同様であるので、その説明は省略する。 20

【0089】

次に、図6のフローチャートを参照して、図5のステップS75の処理を行う場合の送信側の端末11の動作を説明する。ここでは、送信側の端末11が、受信側の端末11がその地域に存在するならば受信することができる放送局を指定し、受信側の端末11がその放送を受信できたか否かによって、受信側の端末11が通信可能な端末11であるか否かが判定される。

【0090】

ステップS101において、送信側の端末11の制御部21は、受信側の端末11がその地域に存在すれば受信することができる放送局を指定したコマンドを生成し、ステップS102において、それを、通信部26を介して受信側の端末11に送信する。 30

【0091】

ステップS103において、送信側の端末11の制御部21は、受信側の端末11から送信されてきた、ステップS102の処理で送信されたコマンドで指定された放送局の放送の受信結果を受信する。

【0092】

ステップS104において、送信側の端末11の制御部21は、ステップS103で受信した放送の受信結果に基づいて、受信側の端末11が、通信可能な端末11であるか否かを判定する。すなわち受信側の端末11が指定した放送局からの放送を適切に受信することができた場合、受信側の端末11が受信可能な領域に存在するので、受信側の端末11は、通信可能な端末11であると判定される。一方受信側の端末11が指定した放送局からの放送を受信することができない場合、受信側の端末11は受信可能な領域に存在しないので、受信側の端末11は、通信可能な端末11ではないと判定される。 40

【0093】

なお放送を適切に受信することができたか否かは、例えば、受信信号が、放送上定められているフォーマットに準拠しているか否かによって判定される。またスクランブルがかけられている放送である場合、そのスクランブルを解除できたか否かによても判定することができる。

【0094】

次に、図5のステップS94の処理を行う場合の受信側の端末11の動作を、図6のフ 50

ローチャートを参照して説明する。この場合、受信側の端末 1 1 は、図 7 に示すように、放送の受信を行う放送受信部 6 1 が設けられている。

【 0 0 9 5 】

ステップ S 1 1 1 において、受信側の端末 1 1 の制御部 2 1 は、通信部 2 6 を介して、送信側の端末 1 1 から送信されてきた、所定の放送局が指定されたコマンドを受信し、ステップ S 1 1 2 において、そのコマンドに指定されている放送局の放送の受信を試みる。

【 0 0 9 6 】

ステップ S 1 1 3 において、受信側の端末 1 1 の制御部 2 1 は、ステップ S 1 1 2 での受信結果を、通信部 2 6 を介して、送信側の端末 1 1 に送信する。

【 0 0 9 7 】

なお、以上においては、所定の放送局の放送の受信を受信側の端末 1 1 が試みる場合を例として説明したが、放送に限らず何らかの通信を利用することもできる。

【 図面の簡単な説明 】

【 0 0 9 8 】

【 図 1 】本発明を適用した端末 1 1 を利用した情報通信システムの構成例を示す図である。

【 図 2 】図 1 の端末 1 1 の構成例を示すブロック図である。

【 図 3 】図 1 の端末 1 1 の動作を説明するフローチャートである。

【 図 4 】図 3 のステップ S 3 およびステップ S 2 4 の処理を説明するフローチャートである。

【 図 5 】図 1 の端末 1 1 の他の動作を説明するフローチャートである。

【 図 6 】図 5 のステップ S 7 5 およびステップ S 9 4 の処理を説明するフローチャートである。

【 図 7 】図 1 の端末 1 1 の他の構成例を示すブロック図である。

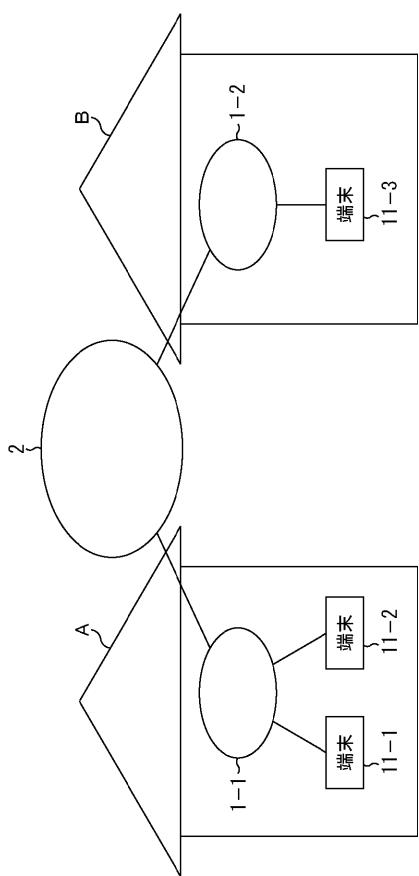
【 符号の説明 】

【 0 0 9 9 】

1 1 端末 , 2 1 制御部 , 2 2 通信可否判定部 , 2 3 移動検知部 , 2 4
コンテンツ管理部 , 2 5 電源部 , 2 5 A プラグ , 5 1 A C 電源 , 6 1
放送受信部

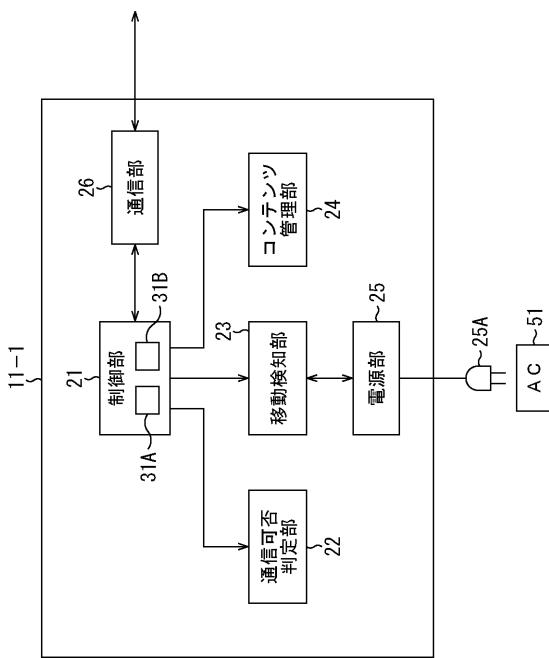
【図1】

図1



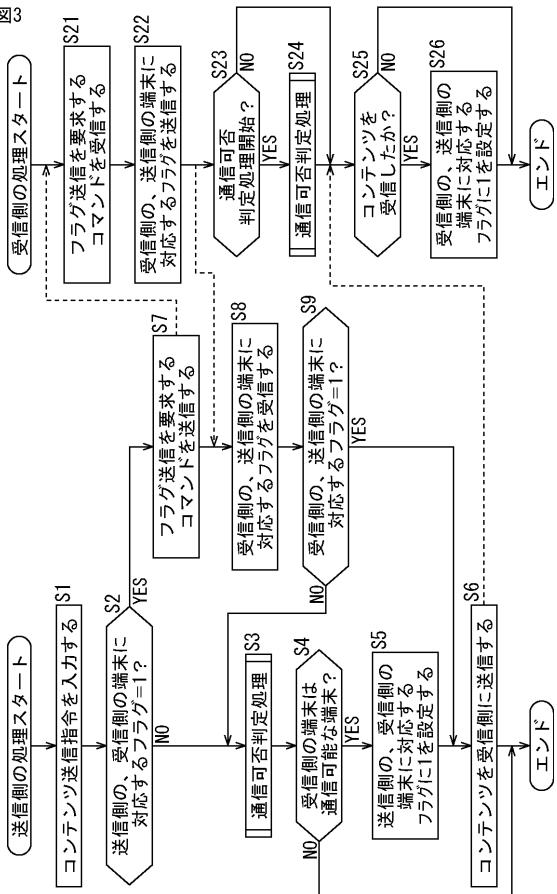
【図2】

図2



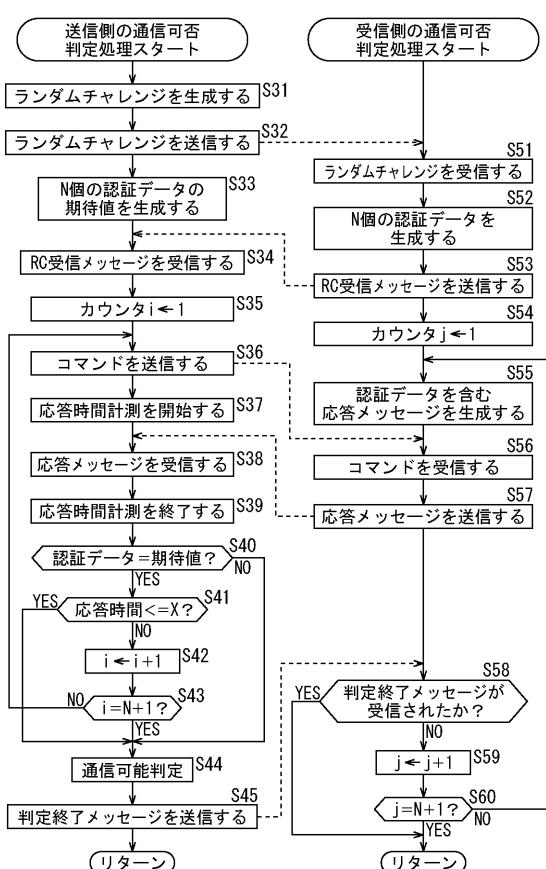
【図3】

図3



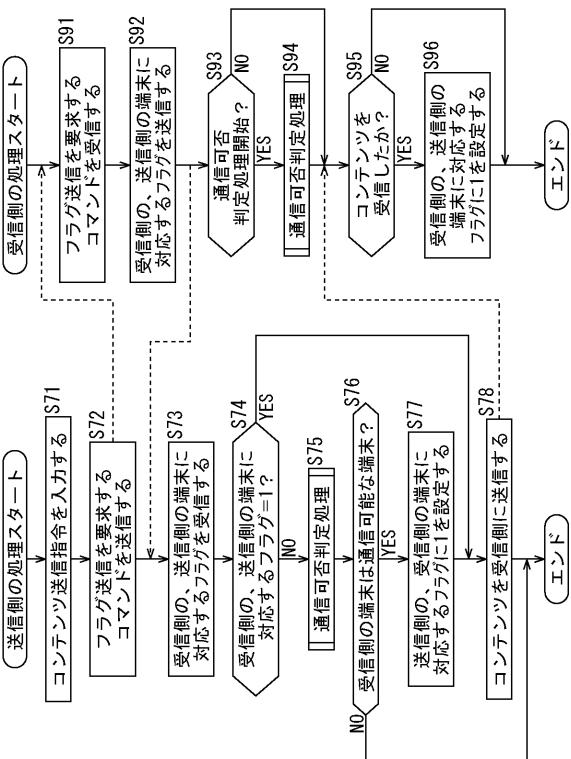
【図4】

図4



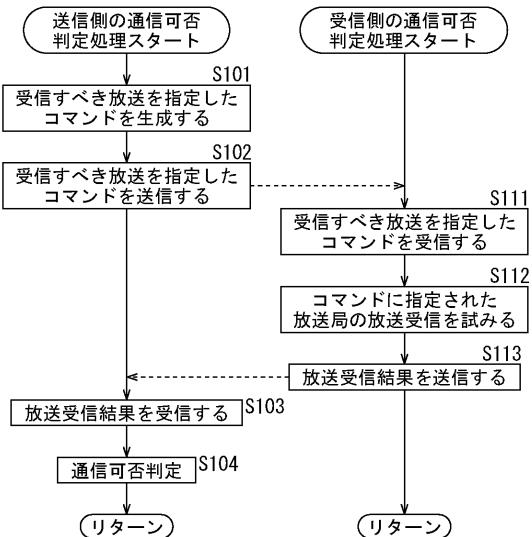
【図5】

図5



【図6】

図6



【図7】

図7

