

(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
2010年11月25日(25.11.2010)

PCT

(10) 国際公開番号
WO 2010/134182 A1

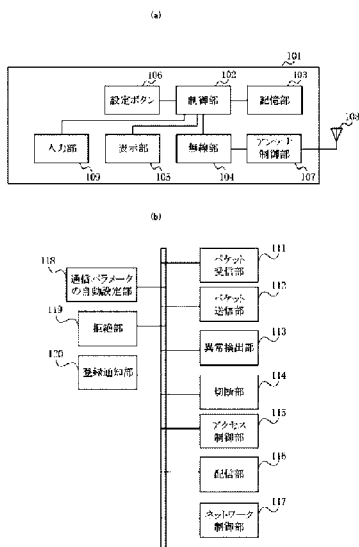
- (51) 国際特許分類:
H04W 12/06 (2009.01) H04W 84/18 (2009.01)
H04W 80/02 (2009.01)
- (21) 国際出願番号: PCT/JP2009/059349
- (22) 国際出願日: 2009年5月21日(21.05.2009)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (71) 出願人(米国を除く全ての指定国について): キヤノン株式会社(CANON KABUSHIKI KAISHA) [JP/JP]; 〒1468501 東京都大田区下丸子3丁目30番2号 Tokyo (JP).
- (72) 発明者: および
- (75) 発明者/出願人(米国についてのみ): 後藤 史英(GOTO Fumihide) [JP/JP]; 〒1468501 東京都大田区下丸子3丁目30番2号キヤノン株式会社内 Tokyo (JP).
- (74) 代理人: 阿部 琢磨, 外(ABE Takuma et al.); 〒1468501 東京都大田区下丸子3丁目30番2号キヤノン株式会社内 Tokyo (JP).
- (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, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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, NA, 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, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF,

[続葉有]

(54) Title: COMMUNICATION DEVICE, COMMUNICATION DEVICE CONTROL METHOD AND PROGRAM

(54) 発明の名称: 通信装置、通信装置の制御方法、プログラム

[図1]



106 SETTING BUTTON
102 CONTROL PART
103 STORING PART
108 ENTERING PART
105 DISPLAY PART
104 RADIO PART
107 ANTENNA CONTROL PART
118 AUTOMATIC COMMUNICATION PARAMETER SETTING PART
119 REJECTING PART
120 REGISTRATION NOTIFYING PART
111 PACKET RECEIVING PART
112 PACKET TRANSMITTING PART
113 ABNORMAL CONDITION DETECTING PART
114 DISCONNECTING PART
115 ACCESS CONTROL PART
116 DISTRIBUTING PART
117 NETWORK CONTROL PART

(57) Abstract: Networks are allowed to share information of devices the communication of which should be rejected. A communication device, which exists in a first network, registers information for identifying a device the communication of which should be rejected, and then notifies the registered information to the other devices existing in the first network. Further, the communication device and the other devices constitute a second network that is different from the first network where the device the communication of which should be rejected exists.

(57) 要約: 【課題】 通信を拒否する対象の装置をネットワークで共有できるようにする。【解決手段】 通信装置は、第1のネットワークに存在し、通信を拒否する対象である拒否対象装置の識別情報を登録し、登録した拒否対象装置の識別情報を第1のネットワークに存在する他の装置に通知する。また、拒否対象装置が存在する第1のネットワークと異なる第2のネットワークを他の装置と構成する。

WO 2010/134182 A1

WO 2010/134182 A1



CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, 添付公開書類:
TG).

— 国際調査報告 (条約第 21 条(3))

明 細 書

発明の名称： 通信装置、通信装置の制御方法、プログラム

技術分野

[0001] 本発明は、通信装置、通信装置の制御方法、プログラムに関する。

背景技術

[0002] 近年、家電製品のネットワーク対応が進んでおり、無線LANを搭載した通信機器同士が無線基地局を経由せずに、お互いが通信を行うという使い方が増加している。

[0003] IEEE 802.11シリーズ規格に準拠した無線LANデバイスにおいて、デバイス同士を直接接続するためにIBSS (Independent Basic Service Set) というアドホックネットワーク仕様がある。アドホックネットワークにおいては、すべての通信機器が対等な関係にあり、一般的に通信パラメータが正しく設定されていれば該当する通信機器同士を容易に接続することが可能である。

[0004] 通信機器同士の通信を制限する方法として、MACアドレス等の相手のアドレスを指定して受信パケットをフィルタリングする方法がある。なお、無線基地局と無線子局との間でのインフラストラクチャネットワークにおいては、基地局において接続を拒否したいMACアドレスを指定して子局の接続を制限する仕組みがある（特許文献1、2参照）。

[0005] また、無線基地局と無線子局との間で通信パラメータを簡単に設定する機能（WPS）が、業界標準団体であるWi-Fi Allianceから提案されている（非特許文献1参照）。

特許文献1：特開2003-204338号公報

特許文献2：特開2004-072682号公報

非特許文献1：Wi-Fi CERTIFIED (TM) for Wi-Fi Protected Setup: Easing the User Experience for Home and Small Office

ce Wi-Fi (R) Networks, <http://www.wi-fi.org/wp/wifi-protected-setup>

発明の開示

発明が解決しようとする課題

- [0006] 無線LANを搭載した通信機器同士が無線基地局を経由しないで直接接続する場合は、アドホックネットワークを使用することが多い。アドホックネットワークは、通信パラメータが通信機器同士で一致していれば、通信をすることが可能であり利便性が高い。また、通信パラメータの設定については前述のWPSを適用することで容易に設定が可能である。
- [0007] ある特定の通信機器をネットワークに参加させたくない場合は、インフラストラクチャネットワークでは、基地局を介して通信するので基地局にMACアドレスによるフィルタリング設定等の接続拒否の設定をすればよい。しかしながら、アドホックネットワークの通信は、基地局のような特定の機器を介して行われるわけではない。したがって、すべての通信機器にMACアドレスによるフィルタリング設定等の接続拒否の設定をしなければならず、操作が煩雑になる。
- [0008] また、基地局に接続拒否の設定をしても、WPSのような通信パラメータの簡単設定技術を利用して通信機器同士で通信パラメータを設定してしまうと、通信したくない機器との通信が簡単に行えてしまう可能性もある。
- [0009] 本発明は、通信を拒否する対象の装置をネットワークで共有できるようにする目的とする。
- [0010] また、本発明の他の目的は、以下の明細書及び図面より明らかになるであろう。

課題を解決するための手段

- [0011] 本発明は、通信装置であって、第1のネットワークに存在し、通信を拒否する対象である拒否対象装置の識別情報を登録する登録手段と、前記登録手段により登録した拒否対象装置の識別情報を第1のネットワークに存在する他の装置に通知する通知手段と、前記拒否対象装置が存在する前記第1のネ

ットワークと異なる第２のネットワークを前記他の装置と構成する構成手段と、を有することを特徴とする。

発明の効果

- [0012] 本発明によれば、通信を拒否する対象の装置をネットワークで共有でき、拒否対象装置との通信を防止できる。

図面の簡単な説明

- [0013] [図1]実施例における装置構成図
[図2]実施例１および実施例３におけるネットワーク構成図
[図3]実施例１における動作シーケンス図
[図4]実施例１における装置Ａの動作フローチャート
[図5]実施例１における装置Ｂまたは装置Ｃの動作フローチャート
[図6]実施例１における動作シーケンス図
[図7]実施例１における装置Ａの動作フローチャート
[図8]実施例２におけるネットワーク構成図
[図9]実施例２における動作シーケンス図
[図10]実施例２における装置Ａの動作フローチャート
[図11]実施例２における動作シーケンス図
[図12]実施例３における動作シーケンス図
[図13]実施例３における通信装置の動作フローチャート

符号の説明

- [0014] １０１ 装置全体
１０２ 制御部
１０３ 記憶部
１０４ 無線部
１０５ 表示部
１０６ 設定ボタン
１０７ アンテナ制御部
１０８ アンテナ

- １０９ 入力部
- １１１ パケット受信部
- １１２ パケット送信部
- １１３ 異常検出部
- １１４ 切断部
- １１５ アクセス制御部
- １１６ 配信部
- １１７ ネットワーク制御部
- １１８ 自動設定部
- １１９ 拒絶部
- １２０ 登録通知部

発明を実施するための形態

[0015]

実施例 １

[0016] 以下、本実施形態に係る通信装置について、図面を参照しながら詳細に説明する。以下では、ＩＥＥＥ８０２．１１シリーズに準拠した無線ＬＡＮシステムを用いた例について説明するが、通信形態は必ずしもＩＥＥＥ８０２．１１準拠の無線ＬＡＮには限らない。

[0017] 図１は本発明を適用できる実施形態に係る、後述の各装置の構成の一例を表すブロック図である。図１（ａ）は、ハードウェア構成の一例であり、図（ｂ）は、ソフトウェア機能ブロックの構成の一例である。図１（ａ）の１０１は装置全体を示す。１０２は、記憶部１０３に記憶される制御用のコンピュータプログラムを実行することにより装置全体を制御する制御部である。制御部１０２は、他の装置との間で通信パラメータの設定制御も行う。１０３は制御部１０２が実行する制御プログラムと、通信パラメータ等の各種情報を記憶する記憶部である。後述する各種動作は、記憶部１０３に記憶された制御プログラムを制御部１０２が実行することにより行われる。１０４はＩＥＥＥ８０２．１１シリーズに準拠した無線ＬＡＮ通信を行うための無

線部である。１０５は各種表示を行う表示部でありＬＣＤやＬＥＤのように視覚で認知可能な情報の出力、あるいはスピーカなどの音出力が可能な機能を有する。表示部１０５は視覚情報および音情報の少なくともどちらか一方を出力する機能を備えるものである。

[0018] １０６は通信パラメータ設定処理を開始するトリガを与える設定ボタンである。設定ボタン１０６が操作されると、通信パラメータの自動設定処理が開始される。制御部１０２は、ユーザによる設定ボタン１０６の操作を検出すると、後述する処理を実施する。１０７はアンテナ制御部、そして１０８はアンテナである。１０９は、ユーザが各種入力を行うための入力部である。

[0019] 図１（ｂ）の１１１は各種通信にかかわるパケットを受信するパケット受信部である。１１２は各種通信にかかわるパケットを送信するパケット送信部である。１１３は、異常検出部であり、通信相手装置の異常の検出を行う。異常検出部１１３は、通信相手のセキュリティ上の問題が発生した場合に該問題を検出する。例えば、通信相手がＤｏＳ攻撃の送信元であることを検出、又はコンピュータウィルスへの感染を検出する。また、異常検出部１１３は、通信相手の通信が他の装置の通信を妨害し、その装置が存在することにより通信帯域を圧迫していることも異常として検出する。また、通信相手の故障も異常として検出する。さらに、通信相手がネットワークポリシーに反する動作を実施した場合、ユーザの意思（操作）による接続拒否設定を実施する場合も、異常として検出する。

[0020] １１４は、通信相手との接続を切断する切断部である。切断部１１４は、通信相手を切断する場合は、切断通知を相手に送信し、該相手を切断する。また、通信相手から切断通知を受けた場合は、切断通知を送信してきた装置との接続を切断する。１１５は、アクセス制御部であり、後述するＭＡＣアドレスフィルタリングなどの無線通信の許可・不許可を制御する機能は、本アクセス制御部２１３にて実施される。フィルタリングする通信拒否対象の通信装置の識別情報であるＭＡＣアドレス情報は、記憶部１０３の拒否ＭＡ

Cアドレスリストに保持される。116は、配信部であり、記憶部103に記憶している拒否MACアドレスリストを他の装置に配信する。また、配信部116は、他の装置から配信された拒否MACアドレスリストを受信する。配信部116が受信した拒否MACアドレスリストに基づき、アクセス制御部115は既に記憶している拒否MACアドレスリストを更新する。

[0021] 117は、無線LANネットワークの構築、ネットワークへの接続処理等のネットワークの各種制御を行うネットワーク制御である。118は、ネットワーク情報である通信パラメータの自動設定部である。本実施形態では、ネットワーク識別子としてのSSID、暗号方式、暗号鍵、認証方式、認証鍵等の無線LAN通信を行うために必要な通信パラメータの自動設定を行う。なお、通信パラメータの自動設定を、以下、自動設定と簡略化する。自動設定部118は、ネットワークの管理装置を決定するための処理、通信パラメータを他の装置に提供する処理、又は提供される通信パラメータを受信するための処理を行う。通信パラメータの共有処理（提供処理、受信処理）は、予め決められている通信プロトコルを装置間で実施することにより行われる。また、自動設定部118は、設定ボタン106のユーザによる操作を検出すると、各種処理を開始する。

[0022] これら機能ブロックはソフトウェアもしくはハードウェア的に相互関係を有するものである。また、上記機能ブロックは一例であり、複数の機能ブロックが1つの機能ブロックを構成するようにしてもよいし、何れかの機能ブロックが更に複数の機能を行うブロックに分かれてもよい。

[0023] 図2は、通信装置A22（以下、装置A）、通信装置B23（以下、装置B）、通信装置C24（以下、装置C）、ネットワークA21（以下、ネットワークA）を示した図である。これらの通信装置は、図1の構成を有している。装置AがネットワークAの管理装置となっており、装置Aのネットワーク制御部117がネットワークを構築し、装置Aに装置Bおよび装置Cが接続している。

[0024] 図3は、装置A、装置Bおよび装置Cにおいて設定ボタン106が押下さ

れ、各装置間で通信パラメータの自動設定処理を実施して接続した後に装置Cに問題が発生し、装置Aが装置Cを切り離す例を示すシーケンス図である。

[0025] ユーザは、装置Aと装置Bにおいてそれぞれ設定ボタン106を押下する。これにより、装置Aと装置Bとの間で無線LANのセットアップ処理が実施される(F301)。無線LANのセットアップ処理において、装置AはネットワークAの管理装置として動作することが決定される。そして、自動設定部118の処理により装置Aから装置Bに通信パラメータが提供され、装置Aと装置Bとで通信パラメータが共有化される。セットアップ完了後、装置Bが装置Aに接続する。

[0026] 装置Aと装置Cの設定ボタン106の押下が検出されると、装置Aと装置Cとの間でも無線LANのセットアップ処理が実施される(F302)。装置Aと装置Bとの場合と同様に、セットアップ完了後、装置Cが装置Aに接続する。なお、装置Aと装置Cがセットアップを実施している間も、装置Bは装置Aと継続して通信可能である。

[0027] 装置A、装置Bおよび装置Cにより第1のネットワークであるネットワークAが構成された後、装置Aの異常検出部113が、装置Cの異常を検出したとする(F303)。異常検出部113は、セキュリティ上の問題を検出、装置Cの通信が他の装置の通信を妨害し、装置Cが存在することにより通信帯域を圧迫していることを検出、デバイスの故障などを検出する。セキュリティ上の問題を検出とは、装置CがDos攻撃の送信元であることを検出、又はコンピュータウィルスへの感染を検出である。また、装置CがネットワークAのネットワークポリシーに反する動作を実施した場合なども、異常として検出する。また、ユーザの意思(操作)による接続拒否設定を実施する場合も、異常として検出する。

[0028] 異常を検知した装置Aは装置CをネットワークAから切り離すために、切断部114により装置Cに切断通知を送信し、装置Cを切断する(F304)。装置Cをネットワークから切り離した装置Aのアクセス制御部115は

、装置CのMACアドレスを記憶部103の拒否MACアドレスリストに登録する(F305)。拒否MACアドレスリストとは、装置Aが無線通信を不許可とするMACアドレスフィルタリングの対象となった装置のMACアドレスを管理しているリストである。

[0029] 拒否MACアドレスリストを更新した装置Aは、配信部116により配下の通信装置（本実施例では、装置B）へ拒否MACアドレスリストを配信する(F306)。配信する拒否MACアドレスリストには、装置Aが接続拒否を実施している全てのMACアドレスが記載されていても良いし、追加・変更・削除のあったMACアドレスのみが記載されていても良い。

[0030] 装置Aからの拒否MACアドレスリストを受信した装置Bのアクセス制御部115は、装置CのMACアドレスを記憶部103の拒否MACアドレスリストに登録する(F307)。また、拒否MACアドレスリストを正常に受信したことを通知するために、リスト受領通知を装置Aに送信する(F308)。

[0031] リスト受領通知を受信した装置Aは、ネットワーク制御部117により第2のネットワークであるネットワークAを再構成する(F309)。このときは、装置Cを除外した新しいネットワークを構築する。なお、ネットワークを再構成せずに、単に拒否MACアドレスリストだけを更新することでもよい。すなわちネットワークの再構成の実施は任意である。しかしながら、MACアドレスは改竄される可能性があるため、ネットワークは再構成することが望ましい。

[0032] 図4は装置Aにおける処理を説明するフローチャートであり、図5は装置Bおよび装置Cの処理を説明するフローチャートである。これらの処理は、制御部102が記憶部103に記憶されている制御プログラムを読み出して実行することにより実施される。図4においては、無線LANセットアップは省略してある。すなわち、図3におけるF303以降の動作フロー図となっている。

[0033] 通信装置（装置A）は、異常検出部113により、通信相手装置の異常を

検知するかを判定する（S 4 0 1）。異常検出部 1 1 3 が異常を検知した場合は、切断部 1 1 4 が異常を検知した通信装置（本実施例では装置 C）へ向けて切断通知を送信して接続を切断する切断処理を行う（S 4 0 2）。その後、異常と判定した通信装置（本実施例では装置 C）の MAC アドレスをアクセス制御部 1 1 5 が記憶部 1 0 3 の拒否 MAC アドレスリストに登録し、MAC アドレスフィルタリングを設定（更新）する（S 4 0 3）。この設定により、異常と判定した通信装置（本実施例では装置 C）との通信が拒否される。

[0034] 拒否 MAC アドレスリストを更新した後、配信部 1 1 6 が該リストを配下の通信装置（本実施例では装置 B）へ配信する（S 4 0 4）。リスト配信後、配信部 1 1 6 は配信先の全ての通信装置から受領通知を受信したかを判定する（S 4 0 5）。本実施例では配信対象の通信装置は装置 B 一つのみであるが、ネットワークの規模が大きな場合は、複数の配信対象の通信装置が存在し、配信部 1 1 6 はリストをこれら複数の装置に配下する。所定時間が経過しても全ての配信先から受領通知を受信していない場合は、S 4 0 4 に戻り、再度、拒否 MAC アドレスリストを配信する。ここでの再送処理については、受領通知を受信していない通信装置のみに対してでもよいし、全ての通信装置に再送してもよい。

[0035] リストを配信した全ての通信装置から受領通知を受信した場合は、ネットワーク制御部 1 1 7 は、ネットワークの再構成処理を開始するための開始通知をネットワークに送信する（S 4 0 6）。その後、ネットワーク制御部 1 1 7 は、ネットワークを再構成する（S 4 0 7）。ネットワークの再構成は、ネットワークの再構成開始の通知を送信した後に改めて無線 LAN セットアップを実施することで実現できる。もしくは、初回の無線 LAN セットアップ（F 3 0 1）において、複数の通信パラメータを配布しておき、S 4 0 6 においてネットワークの再構成を通知する際に、使用する通信パラメータを指定し、指定した通信パラメータに切り替えるという手法をとっても良い。

- [0036] 図5に基づいて装置Bおよび装置Cの動作を説明する。図5は図4と同様に、無線LANセットアップ処理は省略してあり、すでにネットワークが構築されているものとする。
- [0037] 通信装置（装置B、C）は、配信部116により拒否MACアドレスリストを受信したか否かを判定する（S501）。リストを受信しない場合は、切断部114により切断通知を受信したかを判定する（S506）。切断通知を受信しなければ、ステップS501に戻る。本実施例の場合は、装置Bは、拒否MACアドレスリストを受信し、装置Cは切断通知を受信する。
- [0038] S501において拒否MACアドレスリストを受信した装置Bのアクセス制御部115は、リストに掲載されている通信を拒否すべき装置のMACアドレスを、自身のMACアドレスフィルタリング機能に追加設定する（S502）。MACアドレスフィルタリングに設定ができたのち、アクセス制御部115は、受領通知を拒否MACアドレスリストの送信元へと送信する（S503）。受領通知を送信したのち、装置Aからは、ネットワークの再構成開始通知が送信される。装置Bのネットワーク制御部117は、ネットワークの再構成の開始を通知する開始通知が受信されたか否かを判定する（S504）。
- [0039] 再構成の開始通知を受信した場合は、ネットワークを再構成実施する（S505）。ネットワークの再構成は、ネットワークの再構成開始の通知を送信した後に改めて無線LANセットアップを実施することにより実現できる。もしくは、初回の無線LANセットアップ（F301）において、複数の通信パラメータが配布され、S506においてネットワークの再構成を通知された際に、利用する通信パラメータが指定され、指定された通信パラメータに切り替えるという手法をとっても良い。S502において切断通知を受信した装置Cの切断部114は、装置Aとの接続を切断する切断処理を行う（S507）。
- [0040] 次に、拒否MACアドレスリストに登録し、該通信機器を切断した後の処理について説明する。

- [0041] 図6は、装置A、装置Bおよび装置Cにおいて、装置Cに問題が発生し、装置Aが装置Cを切り離れた後に、再度それぞれの装置において設定ボタン106を操作した場合の例を示すシーケンス図である。
- [0042] 装置A、装置Bおよび装置CからネットワークAが構築されている場合に、装置Cになんらかの異常が発生し、装置Aの切断部114が装置Cに向けて切断通知を送信する(F601)。装置Cを切り離れた装置Aのアクセス制御部115は、装置CのMACアドレスを記憶部103の拒否MACアドレスリストに登録する(F602)。装置Aの配信部116は配下の通信装置(本実施例では装置B)に向けて拒否MACアドレスリストの情報を配信する(F603)。拒否MACアドレスリスト情報の配信を受けた通信装置(装置B)のアクセス制御部115は、受信したリストに基づいて、装置CのMACアドレスを記憶部103の拒否MACアドレスリストに登録する(F604)。そして、リスト受領通知を送信する(F605)。異常が発生した通信装置以外の通信装置(本実施例では、装置Aと装置B)とで新たなネットワークを構築する(F606)。
- [0043] ここで、ネットワークを再構成した後、装置Aと装置Cにおいて、再度、設定ボタン106がユーザにより操作され、該操作が検出されたとする(F607、F608)。装置Aにおいては、F602において登録した拒否MACアドレスリストが有効であるため、装置Aの拒絶部119が装置Cに向けて参加拒絶通知を送信し、装置Cの新規参加を拒絶する。(F609)。設定ボタン106の操作が検出されると、自動設定部118は、相手装置を探索するための処理、ネットワーク管理装置の決定のための処理、通信パラメータを提供又は受信するための処理のために、装置間で信号を送受信する。この信号には、信号の送信元の装置のMACアドレスが付加されている。自動設定部118が探索処理、管理装置決定処理又は通信パラメータの自動設定処理を行う際に、アクセス制御部115は、受信した信号に付加されているMACアドレスが、拒否MACアドレスリストに登録されているかどうかを確認する。拒否MACアドレスリストに登録されている装置から、管理

装置決定のための処理が要求された場合と、通信パラメータの提供が要求された場合は、拒絶部 119 が要求元に参加拒絶通知を送信する。装置 A は、参加を拒絶した装置とは、管理装置決定の処理及び通信パラメータの提供処理は実施しない。

[0044] 次に、装置 B と装置 C との間で設定ボタン 106 が操作された場合（F 610、F 611）を考える。

[0045] この場合、装置 B には装置 A が保持しているものと同内容の拒否 MAC アドレスリストが設定されているため、装置 A と装置 C の場合と同様に、装置 B の拒絶部 119 は装置 C の新規参加を拒絶する。よって、装置 B から装置 C に向けて参加拒絶通知を送信する（F 612）。

[0046] 以上のように、拒否 MAC アドレスリストに登録された通信装置は、再度セットアップを実施しようとしても接続を拒否され、ネットワーク A に参加する装置との通信ができなくなる。

[0047] 図 7 に基づいて、装置 A 及び装置 B の処理を説明する。この処理も制御部 102 が記憶部 103 に記憶されている制御プログラムを読み出して実行するとにより実施される。通信装置において設定ボタン 106 が操作されたことを検出する（S 701）。設定ボタン 106 の操作が検出されると、自動設定部 118 が通信パラメータの自動設定処理を開始する。自動設定処理を相手装置と行うために、設定処理のパケットが受信される。アクセス制御部 115 は相手の装置の MAC アドレスが拒否 MAC アドレスリストに含まれているかどうかを判定する（S 702）。相手装置が拒否 MAC アドレスリストに含まれない場合は、自動設定部 118 は管理装置の決定処理、及び通信パラメータの提供又は受信処理を行うネットワーク設定処理（セットアップ処理）を実施する（S 703）。

[0048] 相手装置（本実施例では装置 C）が拒否 MAC アドレスリストに含まれる場合は、拒絶部 119 が相手（装置 C）に対して参加拒絶通知を送信し（S 704）、該相手との通信パラメータの自動設定処理が実行しないようにする。そして、拒絶部 119 は、表示部 105 に自動設定の実行を拒否するこ

とをユーザに通知するために、設定拒否（エラー）を表示する（S705）。

[0049] なお、参加拒絶状態を解除するためには、F303で検出した異常が回復したことを検出した時点で自動的に解除する方法がある。または、ユーザ操作により明示的に解除処理を実施してもよい。

[0050] 以上のように、ある装置が特定の装置をネットワークから切り離す設定を行うと、他の装置にその設定を反映させることができる。その結果、ネットワークから切り離した装置が別の経路（別装置経由）でネットワークに参加することを防ぐことができる。また、特定の装置をネットワークから切り離した後に、他の装置とネットワークを再構成することにより、切り離した装置が再接続することを防止できる。また、ネットワークから切り離した装置において通信パラメータの自動設定の操作が行われても、その装置とは自動設定処理が実行されないようにし、再接続を防止できる。また、自動設定処理が実行されなかった場合は、相手が接続拒否対象の装置のために設定が拒否されたことをユーザに通知するため、操作性（使い勝手）を向上できる。

[0051] また、通信相手の通信装置の異常を検出した場合に、該装置をネットワークから切り離すことが可能となる。同時に、ネットワークの他の装置に異常が検出された装置の情報を配信し、再設定・再接続を禁止することができる。これらの効果は、基地局を経由せずに通信装置同士が直接通信するシステムにおいて特に有効である。

実施例 2

[0052] 図8は、通信装置である装置A82（装置A）、装置B83（装置B）、装置C84（装置C）、ネットワークA81（ネットワークA）、アクセスポイント85（AP）、ITインフラサーバ86（インフラサーバ）を示した図である。装置A、装置Bおよび装置Cは、実施例1で説明した図1の構成を有している。

[0053] インフラサーバは、ネットワークの接続ポリシーを管理しており、ネットワークへ接続しようとする通信機器の機器認証やユーザ認証を行うサーバで

ある。装置AがAPと無線LAN又は有線LAN等によって接続する場合は、装置Aに接続する装置はインフラサーバによる認証処理が実施される。

[0054] 装置Aは、ネットワークAの管理装置となっており、装置Aに装置Bおよび装置Cが接続している。装置Aはさらに、APへ接続し、装置AおよびAPはインフラサーバによって管理されている。すなわち、装置Aを中心とするネットワークAはインフラサーバの管轄下にある。装置Bおよび装置Cは、装置Aとの間で無線LANセットアップを実施している。装置AがネットワークAの管理装置となり、装置Bおよび装置Cを含むネットワークAを構築している。

[0055] 図9は、装置AがAPに接続している状態で、各装置間の中で自動設定処理を実施し接続を試みた場合に、装置Cに問題があり、装置Aが装置Cを切り離す例を示すシーケンス図である。

[0056] 装置Aと装置Bにおいてそれぞれ設定ボタン106が押下されたことを検出する。これにより、装置Aと装置Bとの間で無線LANのセットアップ処理が実施される(F901)。無線LANのセットアップ処理において、装置AはネットワークAの管理装置として動作することが決定される。

[0057] セットアップ処理中又はセットアップ処理が完了すると、装置Aの登録通知部120はインフラサーバにネットワークAに新規参加する通信装置が存在することを通知する(F902)。この通知は、装置Aの登録通知部120がインフラサーバへ向けて、装置Bの情報を登録通知信号に付加して送信する。装置Bの情報としては、装置BのMACアドレス、デバイスタイプ(種類)、機能などである。または、セットアップ処理時又はセットアップ処理終了後に、装置Aが装置Bからパスワード等の認証情報を受信し、この認証情報をインフラサーバに通知してもよい。

[0058] 登録通知(F902)を受信したインフラサーバは、自身の保有するネットワークポリシーに基づいて、装置Bをネットワークに参加させることの可否を判定する。装置Bについてはネットワークへの参加を認めるものとする場合は、インフラサーバは装置Aへ向けて登録OKの通知を送信する(F9

03)。

[0059] 登録OK通知を受信した装置Aは、ネットワークAの管理装置として動作することと決定されているため、装置Bから接続が要求されると、装置Bとの接続を許可する。ここでいうネットワークポリシーは、例えば、装置Bがインフラサーバに事前登録済か否か、あるいは装置Bがもつセキュリティ機能がインフラサーバのセキュリティポリシーと合致するか否かなどが考えられる。また、パスワード等の認証情報による認証の成否でもよい。

[0060] 次に、装置Aと装置Cとの間で無線LANのセットアップ処理を実施する(F904)。なお、装置Aと装置Cがセットアップを実施している間も、装置Bは装置Aと通信はできる。無線LANのセットアップ処理において、装置AはネットワークAの管理装置として動作することが決定される。

[0061] セットアップ処理中又はセットアップ処理が完了すると、装置Aの登録通知部120はインフラサーバにネットワークAに新規参加する通信装置が存在することを通知する(F905)。この通知は、装置Aの登録通知部120がインフラサーバへ向けて、装置Cの情報を登録通知信号に付加して送信する。装置Cの情報としては、装置CのMACアドレス、デバイスタイプ(種類)、機能などである。または、セットアップ処理時又はセットアップ処理終了後に、装置Aが装置Cからパスワード等の認証情報を受信し、この認証情報をインフラサーバに通知してもよい。

[0062] 登録通知(F905)を受信したインフラサーバは自身の保有するネットワークポリシーに基づいて、装置Cをネットワークに参加させることの可否を判定する。装置Cについてはネットワークへの参加を認めないものとする場合は、インフラサーバは装置Aへ向けて登録拒絶の通知を送信する(F906)。

[0063] 登録拒絶の通知を受信した装置Aの切断部114は、装置Cへ向けて切断通知(又は拒絶部119が参加拒否の通知)を送信する(F907)。その後は、実施例1において装置Cの異常を検出した場合の装置Aからの装置Cの切り離し処理と同様のシーケンスとなる。すなわち、装置Cをネットワー

クから切り離れた装置Aのアクセス制御部115は、装置CのMACアドレスを拒否MACアドレスリストに登録する(F908)。拒否MACアドレスリストを更新した装置Aは、配信部116により配下の通信装置(本実施例では、装置B)へ拒否MACアドレスリストを配信する(F909)。

[0064] 装置Aからの拒否MACアドレスリストを受信した装置Bのアクセス制御部115は、拒否MACアドレスリストを更新し、接続拒否対象の装置のMACアドレスを拒否MACアドレスリストに登録する(F910)。また、リストを正常に受信した旨の、リスト受領通知を送信する(F911)。

[0065] リスト受領通知を受信した装置Aのネットワーク制御部117は、ネットワークAを再構成する(F912)。このネットワーク再構成では、装置Cを除外した新しいネットワークを構築する。なお、ネットワークは再構築せずに、単に拒否MACアドレスリストだけを更新することでもよい。この後、装置Cにより設定ボタン106が操作されても、ネットワークAの装置とは自動設定は行われない。

[0066] ここで、インフラサーバへの登録通知(F902、F905)及び、認証結果の通知(F903、F906)は、セットアップ処理中又はセットアップ処理完了後でもよいとした。セットアップ処理中にこれらの処理を実施する場合は、管理装置である装置Aから装置Bに通知パラメータが提供される前に、登録通知と認証結果の受信を実施する。そして、インフラサーバから登録OKが送られてきた場合には、自動設定部118の処理により通信パラメータの自動設定処理(装置Aから装置Bに提供)を行い、装置Aと装置Bとで通信パラメータを共有化する。また、登録が拒絶された場合は、セットアップ処理を中断し、通信パラメータを拒絶対象の装置(装置C)に提供しないようにする。このとき装置Cには、通信パラメータをまだ提供していないので、ネットワークへの参加を拒絶するために、拒絶部119が参加拒絶を通知する(F907)。

[0067] このように、インフラサーバによりネットワークAへの参加が許可された装置に対しては通信パラメータを提供し、参加が拒否された装置には提供しな

いようにする。このようにすることにより、参加が拒否される装置へ通信パラメータが提供されることを防止し、ネットワークのセキュリティを強化できる。

[0068] また、セットアップ処理完了後に登録通知と認証結果の受信を実施する場合は、装置Aから装置B又は装置Cに通知パラメータが提供された後にインフラサーバに登録通知が行われる。このとき装置Cには、通信パラメータを提供済みなので、ネットワークからの切断を指示するために、切断部114が切断通知を送信する（F907）。このようにすることにより、通信パラメータの自動設定処理とネットワークへの参加のための認証処理を別々に行うことができ、自動設定処理時の負荷が大きくなることを防止できる。

[0069] 本実施例における装置Aにおける処理を図10を用いて説明する。この処理も制御部102が記憶部103に記憶されている制御プログラムを実行することにより実施される。

[0070] 装置Aの自動設定部118は、設定ボタン106が押下されたかどうかを判定する（S1001）。設定ボタン106の押下を検出した場合、セットアップ処理を実施する通信相手を検索する。装置Aのアクセス制御部115は、検索の結果検出された通信相手のMACアドレスが、自装置の保有する拒否MACアドレスリストに登録されているかどうかを判定する（S1002）。通信相手のMACアドレスが拒否MACアドレスリストに含まれない場合は、自動設定部118は管理装置の決定処理、及び通信パラメータの提供又は受信処理を行うネットワーク設定処理（セットアップ処理）を開始する（S1003）。そして、装置Aの登録通知部120はインフラサーバに登録通知を送信する（S1004）。なお、ステップS1004は、ネットワーク設定処理中（セットアップ処理中）に実施する方法と、終了後に実施する方法とがある。

[0071] 登録通知送信後、装置Aは、インフラサーバからの返信を待つ（S1005）。返信の結果が、登録OKであれば、処理を終了する。なお、ネットワーク設定処理中（セットアップ処理中）にステップS1004を実施した場

合は、登録OKを受信した後に、自動設定処理により通信パラメータの提供、受信が行われる。一方、返信の結果が、登録拒絶であった場合は、切断部114（又は拒絶部119）が切断通知（又は参加拒絶通知）を通信相手へ送信する（S1008）。なお、ネットワーク設定処理中（セットアップ処理中）にステップS1004を実施した場合は、拒絶部119が参加拒絶を通知し、ネットワーク設定処理後（セットアップ処理後）にステップS1004を実施した場合は、切断部114が切断を通知する。そして、その通信相手のMACアドレスを拒否MACアドレスリストに登録する（S1109）。

[0072] 拒否MACアドレスリストに登録後、配信部116がリストを配下の通信装置へ配信する（S1010）。拒否MACアドレスリストを配信した後、配信した全ての通信装置からの受領通知を待つ（S1011）。すべての通信装置から受領通知を受信したら、ネットワークの再構成を実施（S1012）し処理を終了する。すべての通信装置から受領通知を受信しない場合は、再度拒否MACアドレスリストを配信する。

[0073] また、ステップS1002において、通信相手のMACアドレスが拒否MACアドレスリストに含まれている場合は、拒絶部119が相手装置にネットワークへの参加を拒絶する参加拒絶通知を送信する（S1006）。参加拒絶通知を送信して、該相手との通信パラメータの自動設定処理が実行しないようにする。そして、拒絶部119は、表示部105に自動設定の実行する拒否することをユーザに通知するために、設定拒否（エラー）を表示する（S1007）。

[0074] ここまでの説明では、セットアップ処理中又はセットアップ処理完了後に登録通知を装置Aがインフラサーバに通知する構成について説明してきた。この他にも、装置Aが配下の通信装置情報を定期的にインフラサーバに通知するようにしてもよい。このような構成をとると、一時的にネットワークから離脱した通信装置が存在する場合や、ネットワークへの接続が完了した後にネットワークの接続ポリシーが変化した場合などに対応が可能となる。

- [0075] この構成の場合のシーケンスが図 11 である。装置 A と装置 B においてそれぞれ設定ボタン 106 を押下する。これにより、装置 A と装置 B との間で無線 LAN のセットアップ処理が実施される (F 1101)。セットアップ処理中又は完了後に、装置 A はインフラサーバにネットワーク A に新規参加の通信装置が存在することを通知するために、登録通知を送信する (F 1102)。登録通知 (F 1102) を受信したインフラサーバは自身の保有するネットワークポリシーに基づいて、装置 B をネットワークに参加させることの可否を判定する。ここで、装置 B についてはネットワークへの参加を認めるものとする場合は、インフラサーバは装置 A へ向けて登録 OK 通知を送信する (F 1103)。ネットワーク A の管理装置として、装置 A は動作することとあらかじめ決定されているため、セットアップ完了後、装置 B が装置 A に接続することとなる。装置 A は定期的に配下の通信装置の状況をインフラサーバに報告するために、配下端末報告を送信する (F 1104 ~ F 1105)。
- [0076] ここでセットアップをしておらず、偶然通信パラメータが同一であった装置 C がネットワーク A に接続してくる場合を考える。装置 C はインフラサーバのネットワーク管理ポリシーに反している装置であるとする。
- [0077] 装置 C が装置 A に接続を行う (F 1106)。装置 A は装置 C が接続してきたため、次回の IT インフラサーバへの定期報告にて装置 C の存在も合わせて報告する (F 1107)。F 1107 の配下端末報告を受けたインフラサーバは、装置 C がネットワークポリシーに反するため、排除勧告を装置 A に送信する (F 1108)。排除勧告 F 1108 を受信した装置 A の切断部 114 は、装置 C へ向けて切断通知を送信する (F 1109)。その後は、実施例 1 において装置 C の異常を検出した場合の装置 A からの装置 C の切り離し処理と同様のシーケンスとなる。すなわち、装置 C をネットワークから切り離した装置 A は、装置 C の MAC アドレスを拒否 MAC アドレスリストに登録する (F 1110)。拒否 MAC アドレスリストを更新した装置 A は配下の通信装置 (本実施例では、装置 B) へ拒否 MAC アドレスリストを配

信する（F 1 1 1 1）。

[0078] 装置Aからの拒否MACアドレスリストを受信した装置Bは、拒否MACアドレスリストを更新し（F 1 1 1 2）、リストを正常に受信した旨の、リスト受領通知を送信する（F 1 1 1 3）。

[0079] リスト受領通知を受信した装置Aは、ネットワークAを再構成する。（F 1 1 1 4）このとき装置Aと装置Bは、装置Cを除外した新しいネットワークを構築する。ただし、場合によってはネットワークを再構成しないまま、拒否MACアドレスリストを更新することでもよい。

[0080] 図12では、装置Cは偶然ネットワークAと同一の通信パラメータを保持していたと述べた。それ以外にも、装置Aと装置Cであらかじめセットアップ処理が実施済みであり、一時的にネットワークAから離脱しており、その離脱期間中にインフラサーバの保持するネットワークポリシーが変化した場合についても同様のシーケンスで説明することが可能である。

[0081] さらに、セットアップ時はすべての通信装置の接続が認められていながら、接続完了後に、インフラサーバのネットワークポリシーが変更された場合は、ネットワークポリシーに反してしまう通信装置が出てくることがある。このような場合についても、図11で説明したような動作シーケンスによって処理を説明することができる。

[0082] 以上のように本実施形態では、ネットワークAに参加できる通信装置をインフラサーバが保持するネットワークポリシーに基づいて制御することができる。

実施例 3

[0083] 実施例1では、ネットワーク管理装置（実施例1では装置A）がネットワーク接続装置（実施例1では装置C）の異常を検知してネットワークから排除する場合について説明した。実施例3では、ネットワーク接続装置（ここでは装置C）がネットワーク管理装置（ここでは装置A）の異常を検知した場合の挙動について説明する。

[0084] 通信装置は、実施例1および実施例2と同様に図1の構成を有している。

また、ネットワーク構成は実施例 1 と同様に図 2 の構成であるとする。

[0085] 図 1 2 は、装置 A、装置 B および装置 C において設定ボタン 1 0 6 が押下され、各装置間の中で自動設定処理を実施し接続したのちに、装置 A に問題が発生した場合に、装置 A が装置 C を切り離す一例を示すシーケンス図である。

[0086] 装置 A と装置 B においてそれぞれ設定ボタン 1 0 6 を押下されると、装置 A と装置 B との間で無線 LAN のセットアップ処理が実施される（F 1 2 0 1）。セットアップ処理において、装置 A はネットワーク A の管理装置として動作することが決定される。よって、セットアップ完了後、装置 B が装置 A に接続する。

[0087] 装置 A と装置 C との間で無線 LAN のセットアップ処理が実施される（F 1 2 0 2）。装置 A と装置 B との場合と同様に、セットアップ完了後、装置 C が装置 A に接続する。なお、装置 A と装置 C がセットアップを実施している間も、装置 B は装置 A と通信はできる。

[0088] 装置 A、装置 B および装置 C からネットワーク A が構成された後、装置 B および装置 C は、装置 A の異常を検知するとする（F 1 2 0 3、F 1 2 0 5）。ここでの異常の定義は、実施例 1 の説明で述べたものと同等とする。異常を検知した装置 B は装置 A との接続を取りやめるために、切断通知を送信する（F 1 2 0 4）。同様に、装置 C も装置 A へ向けて切断通知を送信する（F 1 2 0 6）。装置 A をネットワークから切り離した装置 B および装置 C は、装置 A の MAC アドレスを拒否 MAC アドレスリストに登録する（F 1 2 0 7、F 1 2 0 8）。

[0089] 以上の動作により、ネットワーク A から装置 B および装置 C は離脱することとなる。ここで、装置 A と装置 C の設定ボタン 1 0 6 を押下（F 1 2 0 9、F 1 2 1 0）した場合は、装置 C から装置 A へ参加拒絶通知が送信され、セットアップは実施しない（F 1 2 1 1）。同様に、装置 A と装置 B との設定ボタン 1 0 6 を押下（F 1 2 1 2、F 1 2 1 3）しても、装置 B から装置 A へ参加拒絶通知が送信される（F 1 2 1 4）。

- [0090] 一方、装置Bと装置Cの設定ボタン106を操作した場合は、装置Bと装置Cとの間でセットアップ処理が実施（F1217）され、新たなネットワークが構築される。
- [0091] 装置Aの処理を図13を用いて説明する。図13の処理も装置Aの制御部102が記憶部103に記憶されている制御プログラムを実行することにより実施される。図13は図5のステップS403とステップS404との間に新たな判定処理S1301を追加したものである。
- [0092] 図13に基づいて通信装置の処理を説明する。本フロー図においては、無線LANセットアップは省略してある。すなわち、図12のF1203以降の動作フロー図となっている。
- [0093] 通信装置において、通信相手の異常を検知するかを判定する（S401）。S401において異常を検知した場合は、その通信装置へ向けて切断通知を送信する（S402）。その後、切断した通信装置のMACアドレスを拒否MACアドレスリストに登録し、MACアドレスフィルタリングを実施する（S403）。
- [0094] ここで、通信相手の通信装置の役割がネットワーク接続装置（クライアント）なのかネットワーク管理装置なのかを判定する（S1301）。
- [0095] 判定の結果、クライアントであった場合は、図5のステップS404以降と同じ処理を実施する。また、ステップS1301の判定処理において、通信相手の通信装置の役割が管理装置であった場合は、この時点で処理を終了する。
- [0096] 以上のように、通信装置の役割（管理装置なのかクライアントなのか）によらず、ネットワークポリシーや挙動に基づいてネットワークへの参加を制御することができる。
- [0097] 上記説明における管理装置は、アクセスポイントであってもよい。この場合、装置間で管理装置を決定し、管理装置と決まった装置がアクセスポイントとして動作し、ネットワークを構築する。そして、上記各実施例で説明した管理装置としての動作を実施する。

また、上記説明はIEEE 802.11準拠の無線LANを例に説明した。しかしながら、本発明は、ワイヤレスUSB、MBOA、Bluetooth（登録商標）、UWB、ZigBee等の他の無線媒体において実施してもよい。また、有線LAN等の有線通信媒体において実施してもよい。

[0098] ここで、MBOAは、Multi Band OFDM Allianceの略である。また、UWBは、ワイヤレスUSB、ワイヤレス1394、WINE Tなどが含まれる。

[0099] また、通信パラメータとしてネットワーク識別子、暗号方式、暗号鍵、認証方式、認証鍵を例にしたが、他の情報であってもよいし、他の情報も通信パラメータには含まれるようにしてもよいことは言うまでも無い。

請求の範囲

- [請求項1] 通信装置であって、
- 第1のネットワークに存在し、通信を拒否する対象である拒否対象装置の識別情報を登録する登録手段と、
- 前記登録手段により登録した拒否対象装置の識別情報を第1のネットワークに存在する他の装置に通知する通知手段と、
- 前記拒否対象装置が存在する前記第1のネットワークと異なる第2のネットワークを前記他の装置と構成する構成手段と、
- を有することを特徴とする通信装置。
- [請求項2] ネットワークを構成するための通信パラメータを装置間で共有化するための共有処理を行う共有手段を有し、
- 前記構成手段は、前記他の装置と前記共有手段により前記共有処理を実行し、前記第2のネットワークを構成することを特徴とする請求項1に記載の通信装置。
- [請求項3] 前記共有手段は、前記通信パラメータを提供又は受信するための処理を実行することを請求項2に記載の通信装置。
- [請求項4] 前記構成手段は、前記第1のネットワークを構成する際に共有された複数のネットワーク情報のいずれかのネットワーク情報を使用して前記第2のネットワークを構成することを特徴とする請求項1に記載の通信装置。
- [請求項5] 前記複数のネットワーク情報のいずれかを指定する指定手段を有し、
- 前記構成手段は、前記指定手段により指定したネットワーク情報を使用して前記第2のネットワークを構成することを特徴とする請求項4に記載の通信装置。
- [請求項6] ネットワークを構成するための通信パラメータを装置間で共有化するための共有処理を行う共有手段を有し、
- 前記共有手段は、前記共有処理を行う通信相手が前記登録手段に通

信拒否対象として登録されている装置か否かに応じて、前記共有処理を実行することを特徴とする請求項 1 に記載の通信装置。

[請求項7] 前記登録手段により拒否対象装置として登録する装置との接続を切断する切断手段を有することを特徴とする請求項 1 に記載の通信装置。

[請求項8] 前記登録手段は、前記通信装置が異常を検出した装置を拒否対象装置として登録することを特徴とする請求項 1 に記載の通信装置。

[請求項9] 前記登録手段は、認証装置による認証結果に応じて、拒否対象装置を特定し、該装置を拒否対象装置として登録することを特徴とする請求項 1 に記載の通信装置。

[請求項10] 通信装置であって、
通信を拒否する対象である拒否対象装置の識別情報を登録する登録手段と、

前記登録手段により登録した拒否対象装置の識別情報を他の装置に通知する通知手段と、

ネットワークを構成するための通信パラメータを装置間で共有化するための共有処理を行う共有手段と、

前記共有処理を行う通信相手が前記登録手段に通信拒否対象として登録されている装置か否かに応じて、前記共有処理を実行するか否かを判定する判定手段と、を有し、

前記共有手段は、前記判定手段による判定に応じて、前記共有処理を実行することを特徴とする通信装置。

[請求項11] 通信装置の制御方法であって、

第 1 のネットワークに存在し、通信を拒否する対象である拒否対象装置の識別情報を登録する登録工程と、

前記登録工程において登録した拒否対象装置の識別情報を第 1 のネットワークに存在する他の装置に通知する通知工程と、

前記拒否対象装置が存在する前記第 1 のネットワークと異なる第 2

のネットワークを前記他の装置と構成する構成工程と、
を有することを特徴とする通信装置の制御方法。

[請求項12]

通信装置の制御方法であって、

通信を拒否する対象である拒否対象装置の識別情報を登録する登録工程と、

前記登録工程において登録した拒否対象装置の識別情報を他の装置に通知する通知工程と、

ネットワークを構成するための通信パラメータを装置間で共有化するための共有処理を行う共有工程と、

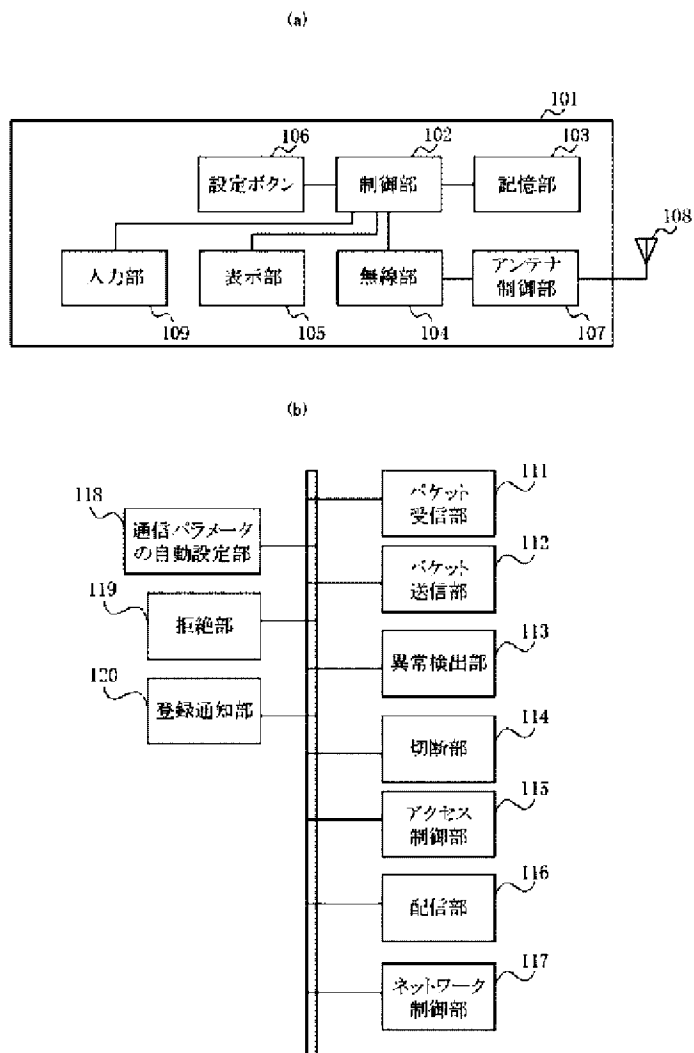
前記共有処理を行う通信相手が前記登録手段に通信拒否対象として登録されている装置か否かに応じて、前記共有処理を実行するか否かを判定する判定工程と、を有し、

前記共有工程は、前記判定工程における判定に応じて、前記共有処理を実行することを特徴とする通信装置の制御方法。

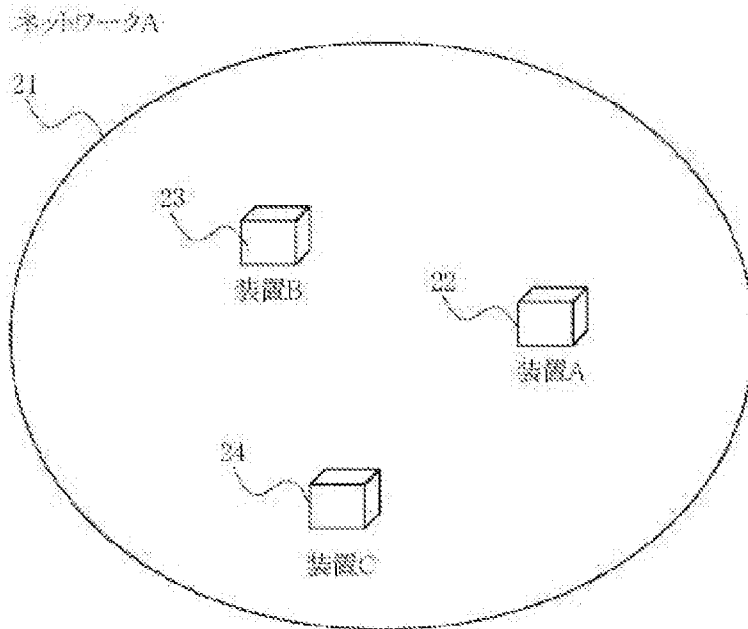
[請求項13]

請求項 1 1 又は請求項 1 2 に記載の制御方法の各工程をコンピュータに実行させるためのプログラム。

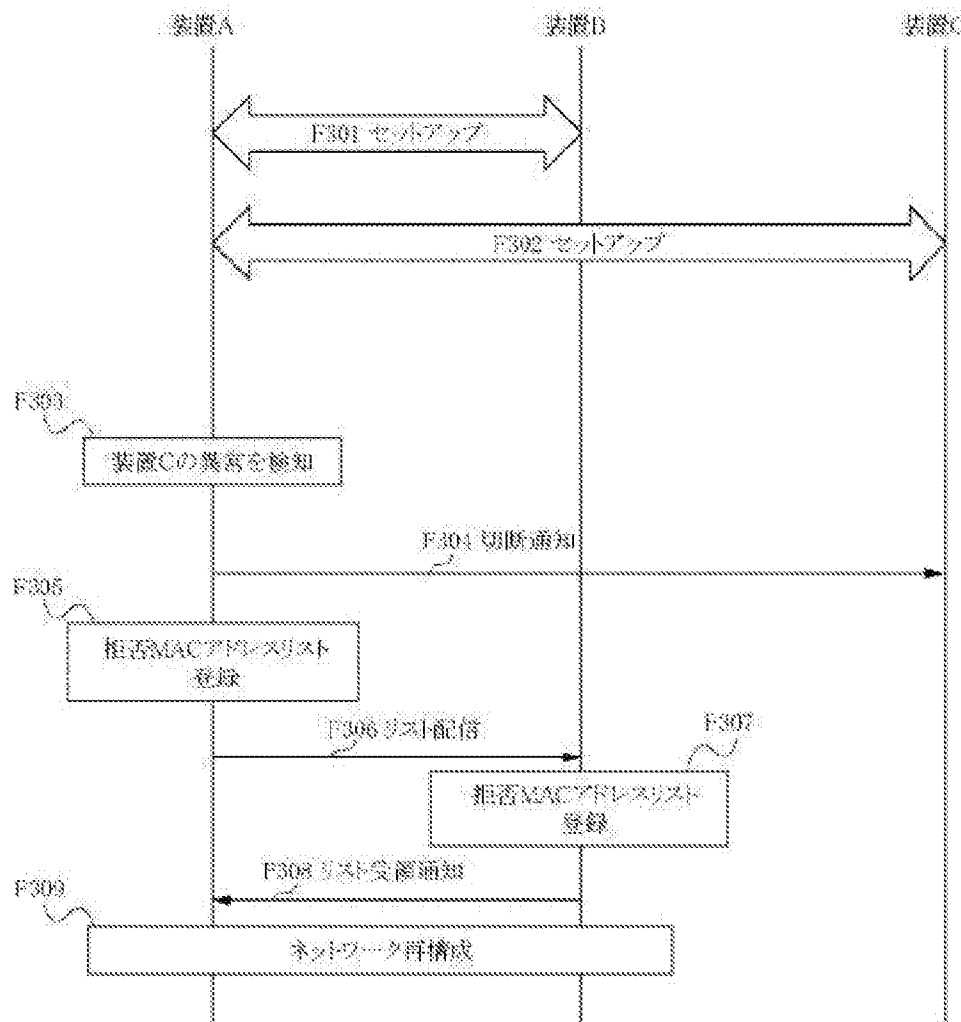
[図1]



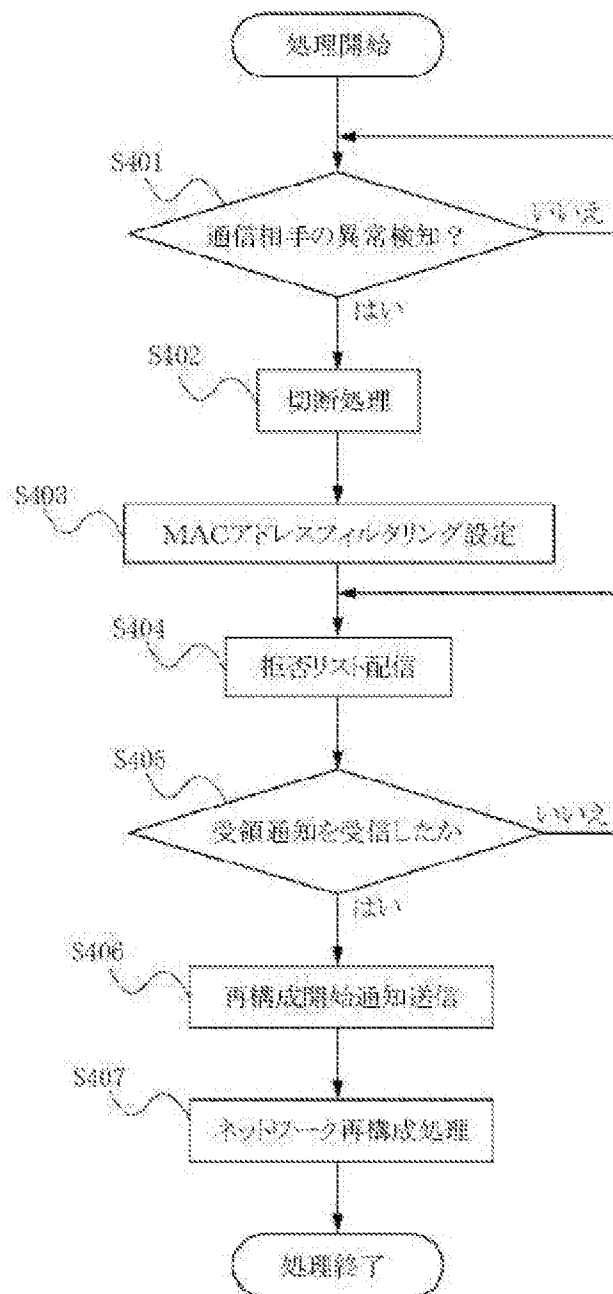
[図2]



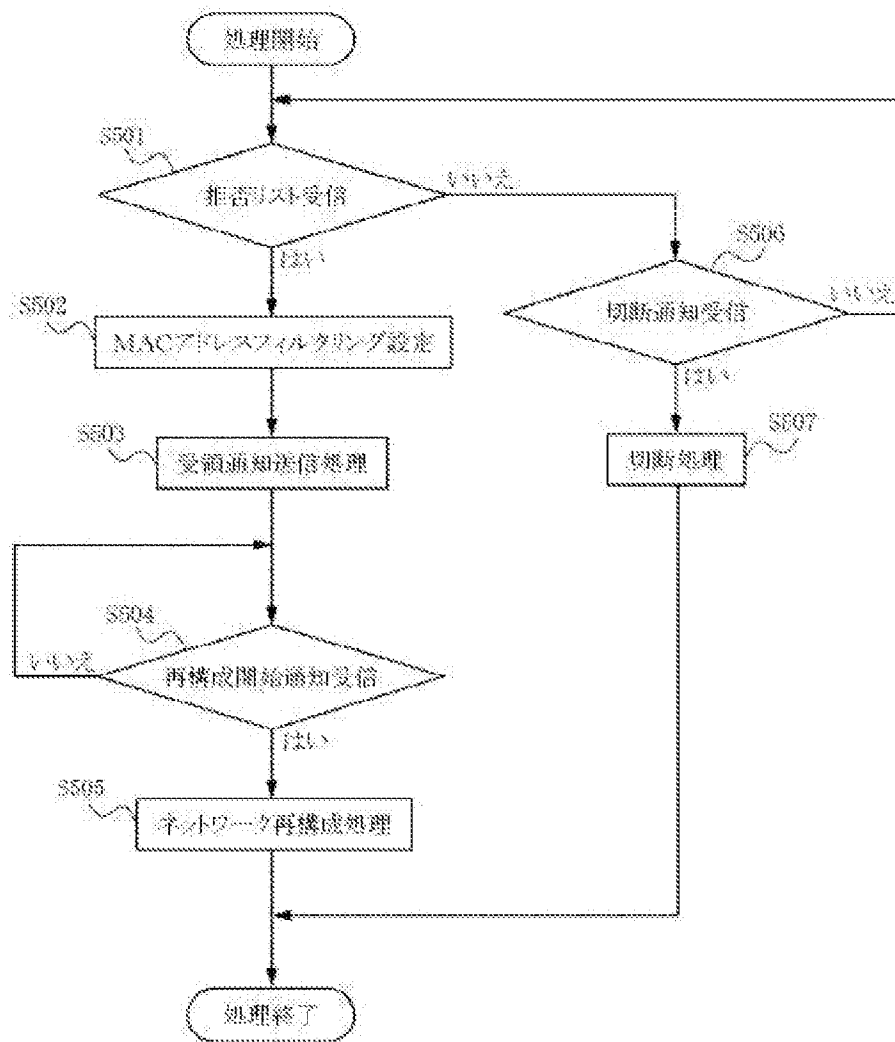
[図3]



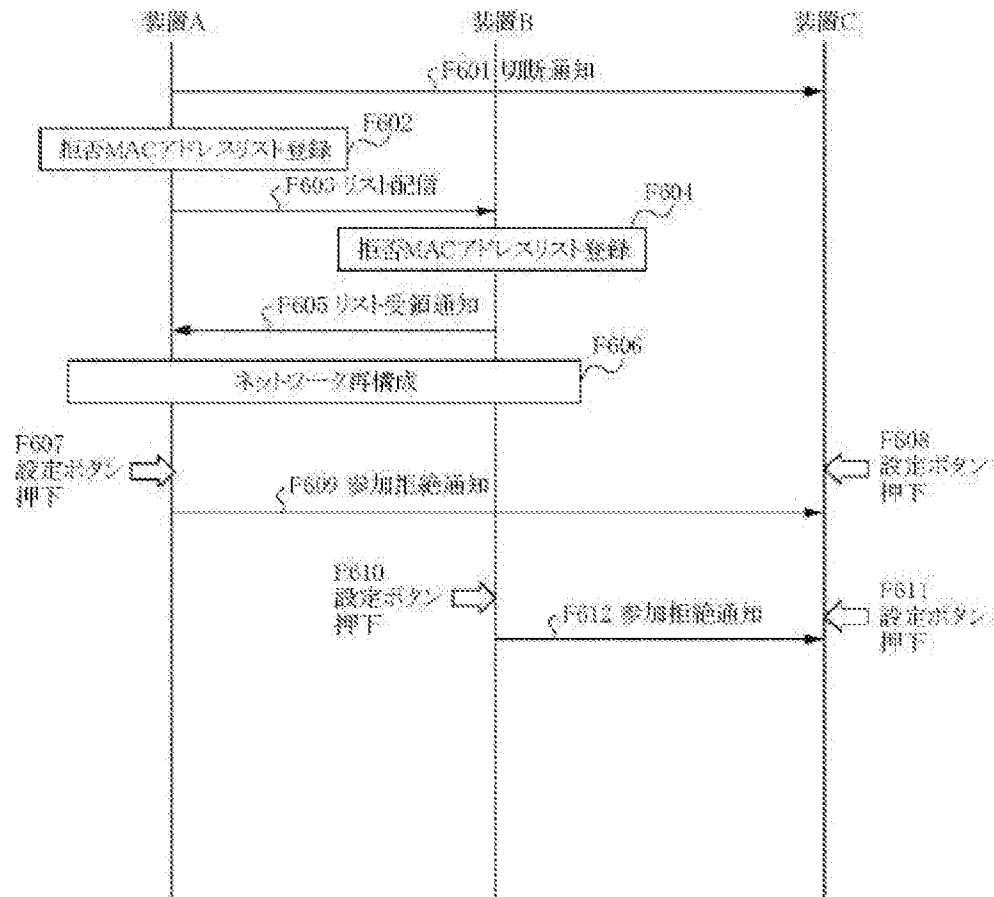
[図4]



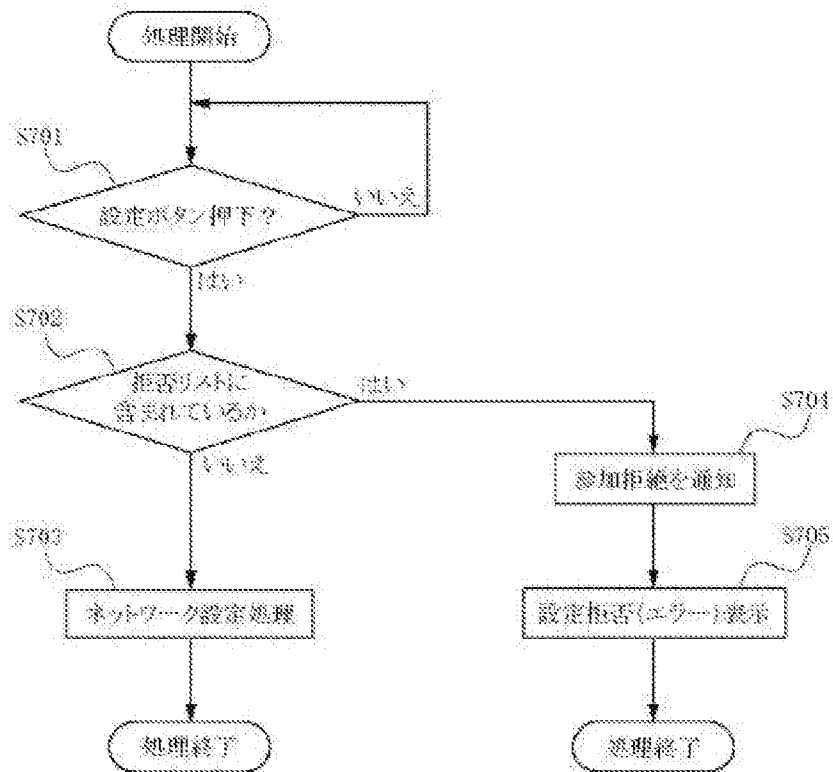
[図5]



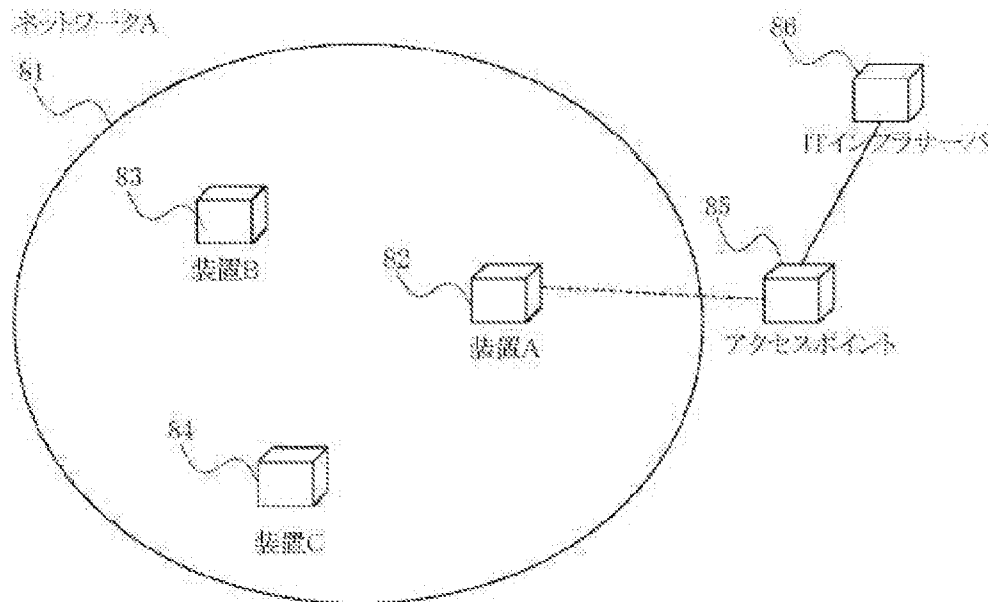
[図6]



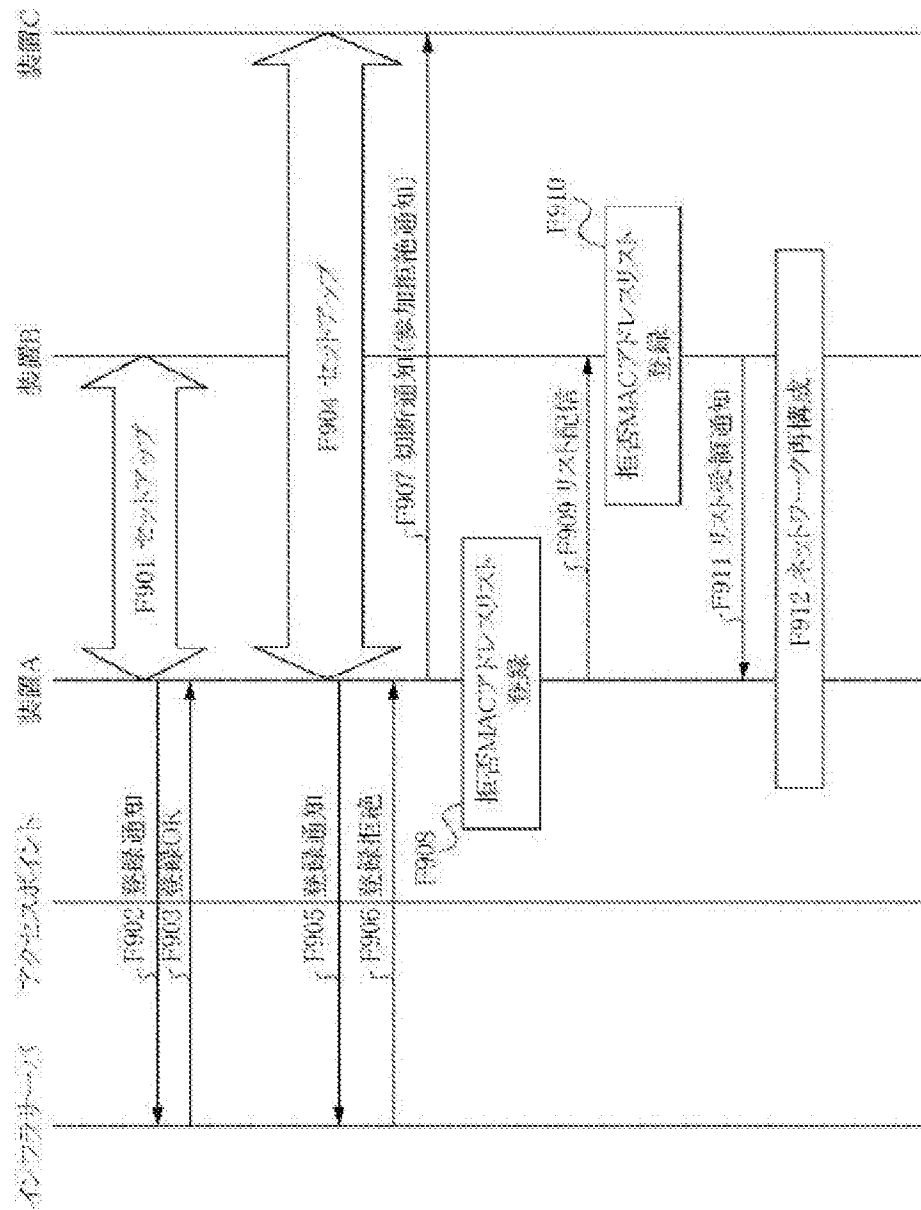
[図7]



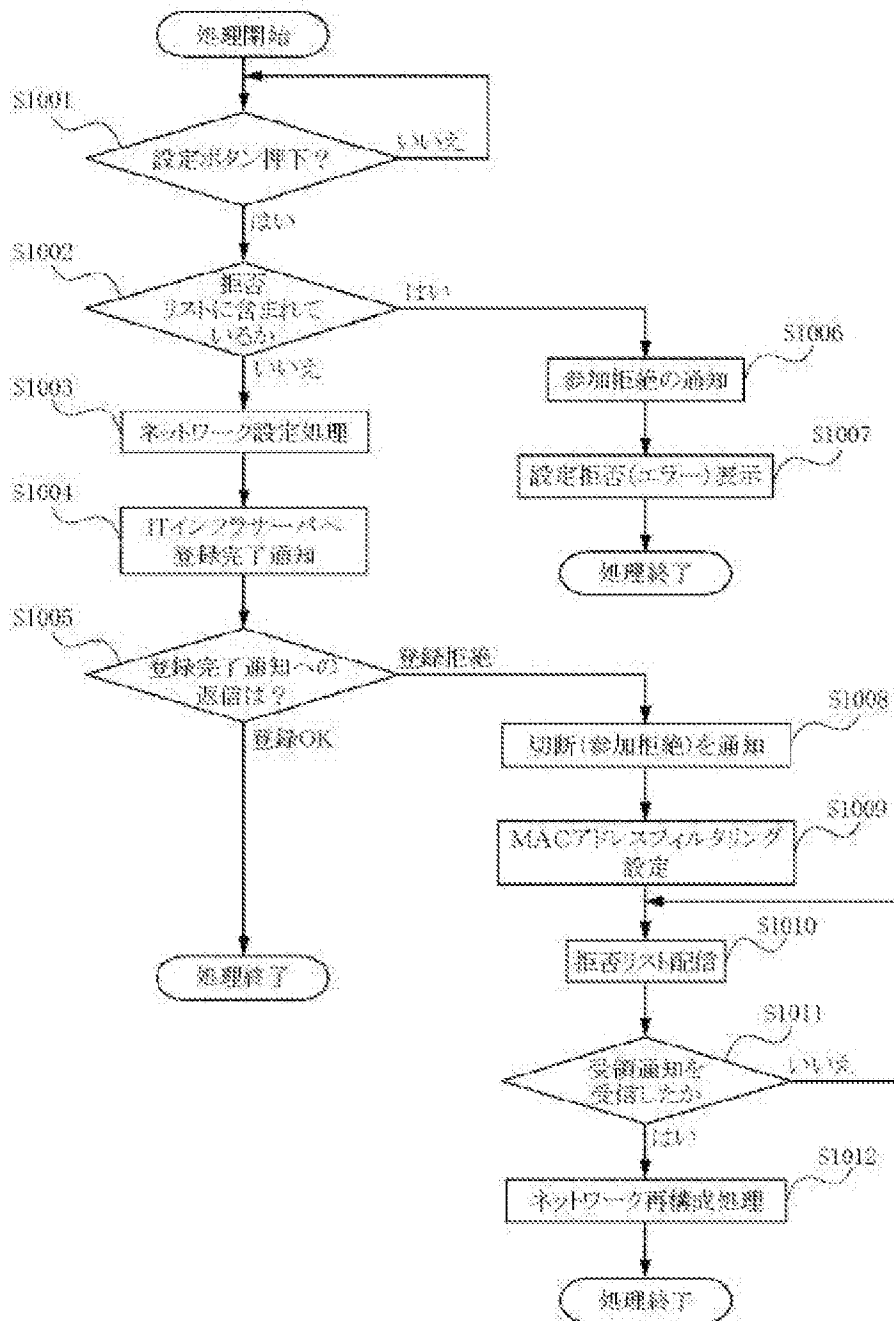
[図8]



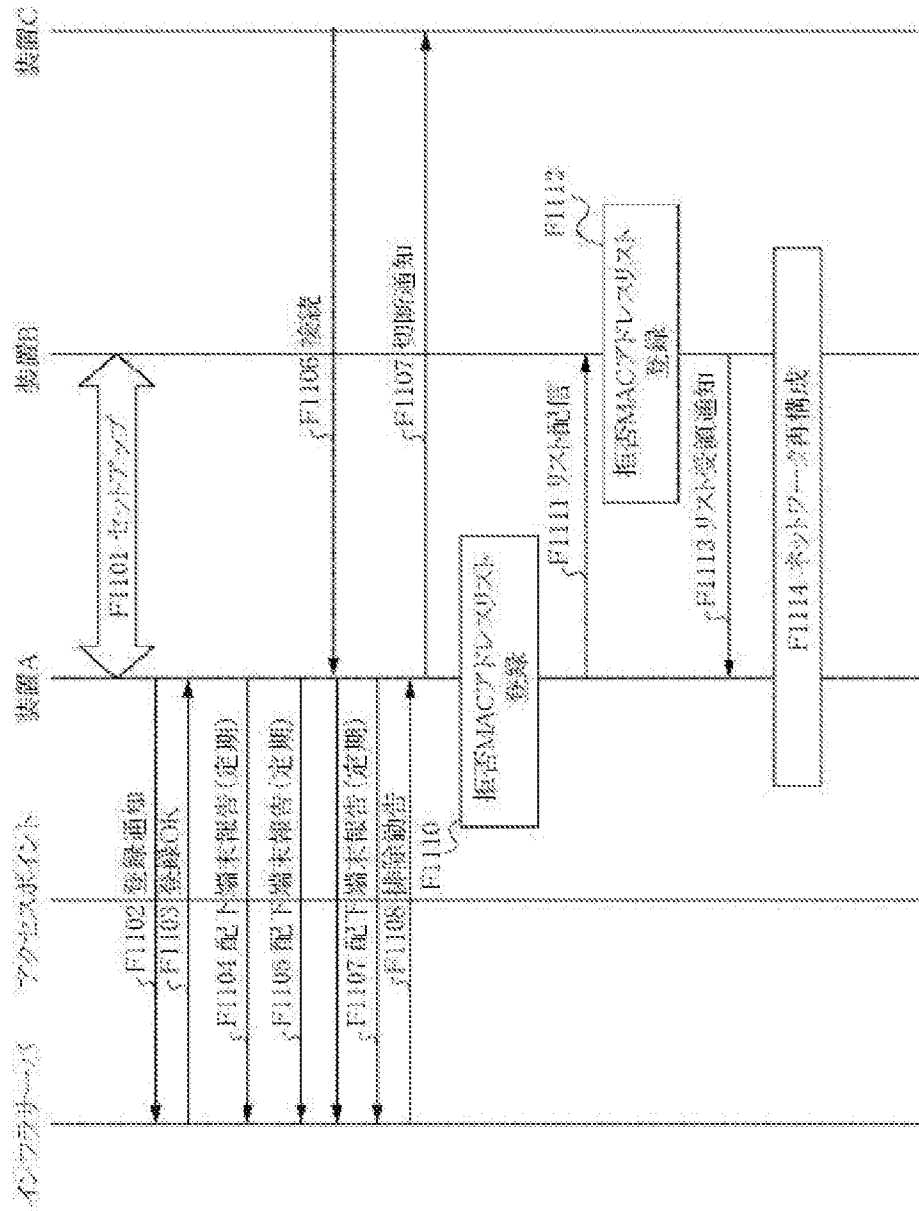
[図9]



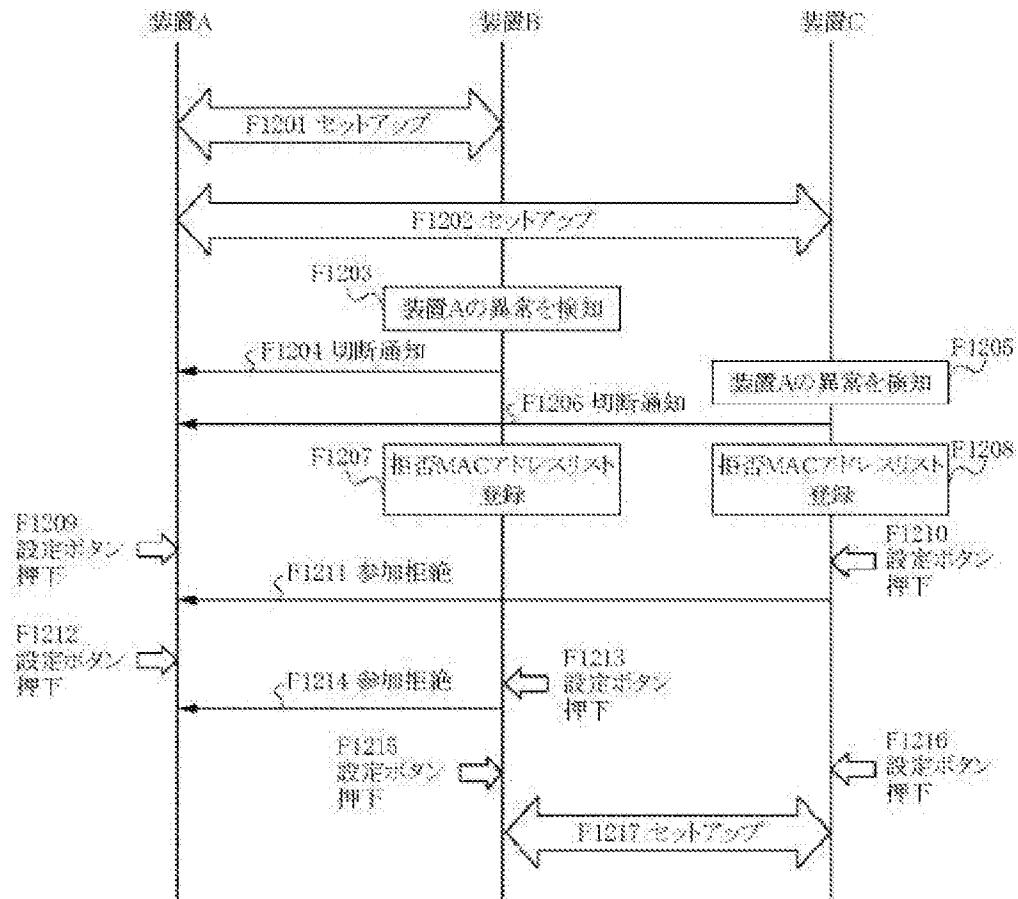
[図10]



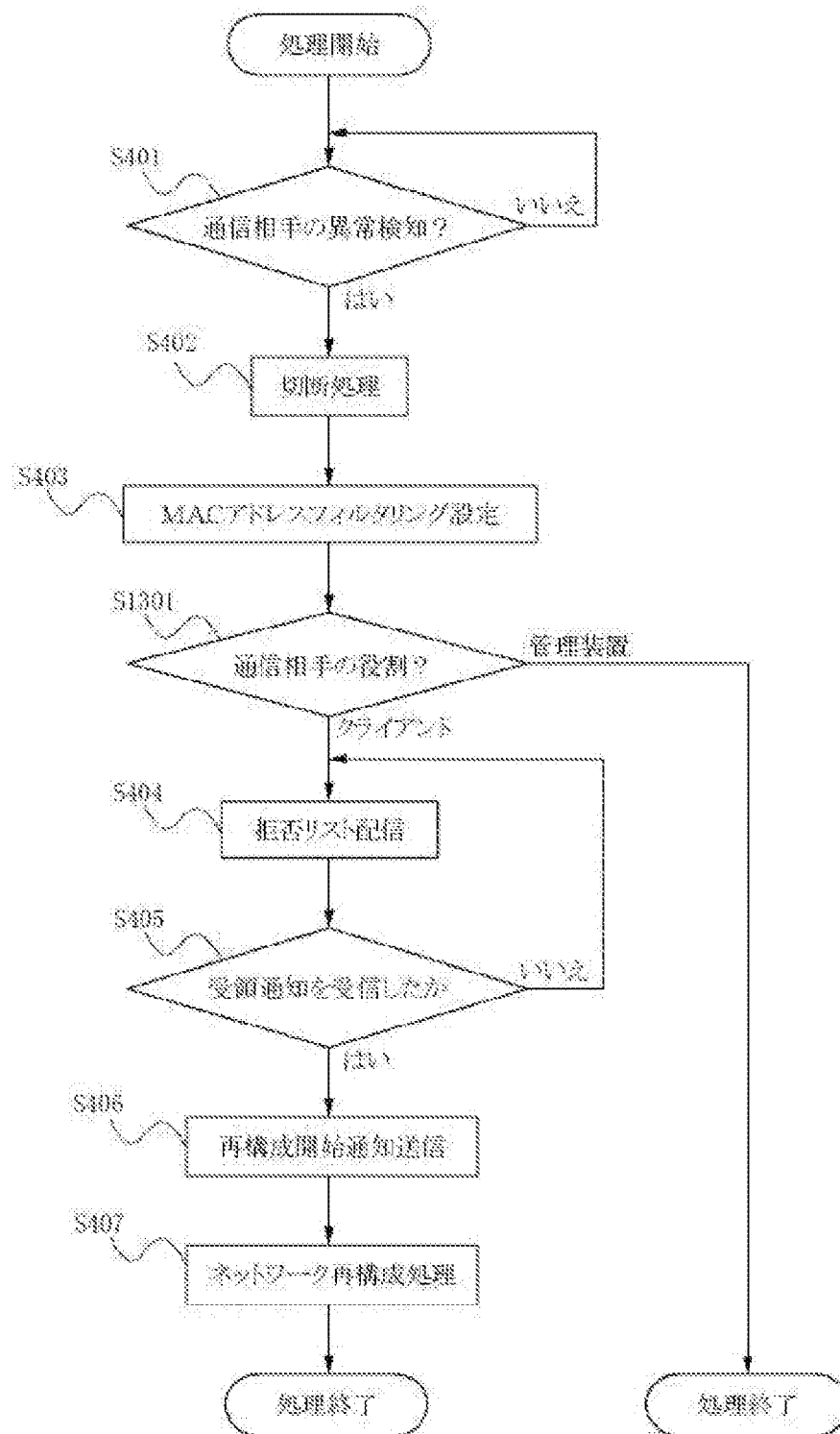
[図11]



[図12]



[図13]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2009/059349

A. CLASSIFICATION OF SUBJECT MATTER

H04W12/06(2009.01) i, H04W80/02(2009.01) i, H04W84/18(2009.01) i

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)

H04B7/24-7/26, H04W4/00-99/00

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

Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2009

Kokai Jitsuyo Shinan Koho 1971-2009 Toroku Jitsuyo Shinan Koho 1994-2009

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	JP 2007-074393 A (NTT Docomo Inc.), 22 March, 2007 (22.03.07), Par. Nos. [0058] to [0062] (Family: none)	1-7, 10-13 8, 9
X Y	JP 2007-074392 A (NTT Docomo Inc.), 22 March, 2007 (22.03.07), Par. Nos. [0054] to [0059] (Family: none)	1-7, 10-13 8, 9
Y	JP 2008-099214 A (Oki Electric Industry Co., Ltd.), 24 April, 2008 (24.04.08), Par. Nos. [0077] to [0084] & US 2008/0092218 A1	8, 9

☐ 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
07 July, 2009 (07.07.09)Date of mailing of the international search report
21 July, 2009 (21.07.09)Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

A. 発明の属する分野の分類（国際特許分類（I P C））

Int.Cl. H04W12/06(2009.01)i, H04W80/02(2009.01)i, H04W84/18(2009.01)i

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（I P C））

Int.Cl. H04B7/24-7/26, H04W4/00-99/00

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	1 9 2 2 - 1 9 9 6 年
日本国公開実用新案公報	1 9 7 1 - 2 0 0 9 年
日本国実用新案登録公報	1 9 9 6 - 2 0 0 9 年
日本国登録実用新案公報	1 9 9 4 - 2 0 0 9 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 請求項の番号
X Y	JP 2007-074393 A (株式会社エヌ・ティ・ティ・ドコモ) 2007.03.22, 第 58-62 段落 (ファミリーなし)	1-7, 10-13 8, 9
X Y	JP 2007-074392 A (株式会社エヌ・ティ・ティ・ドコモ) 2007.03.22, 第 54-59 段落 (ファミリーなし)	1-7, 10-13 8, 9
Y	JP 2008-099214 A (沖電気工業株式会社) 2008.04.24, 第 77-84 段落 & US 2008/0092218 A1	8, 9

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

0 7 . 0 7 . 2 0 0 9

国際調査報告の発送日

2 1 . 0 7 . 2 0 0 9

国際調査機関の名称及びあて先

日本国特許庁（I S A / J P）

郵便番号 1 0 0 - 8 9 1 5

東京都千代田区霞が関三丁目 4 番 3 号

特許庁審査官（権限のある職員）

松野 吉宏

電話番号 0 3 - 3 5 8 1 - 1 1 0 1 内線 3 5 3 5

5 J

3 5 7 1