(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4029629号
(P4029629)
(45)発行日　平成20年1月9日(2008.1.9)　(24)登録日　平成19年10月26日(2007.10.26)

(51)Int.Cl.		F I		
H04L 12/28	(2006.01)	H04L	12/28	300Z
H04L 29/06	(2006.01)	H04L	13/00	305C
H04Q 7/38	(2006.01)	H04B	7/26	109M

請求項の数 6　(全 50 頁)

(21)出願番号　特願2002-45145(P2002-45145)
(22)出願日　平成14年2月21日(2002.2.21)
(65)公開番号　特開2002-359623(P2002-359623A)
(43)公開日　平成14年12月13日(2002.12.13)
審査請求日　平成17年2月1日(2005.2.1)
(31)優先権主張番号　特願2001-91423(P2001-91423)
(32)優先日　平成13年3月27日(2001.3.27)
(33)優先権主張国　日本国(JP)

(73)特許権者　000002369
セイコーエプソン株式会社
東京都新宿区西新宿２丁目４番１号
(74)代理人　100098084
弁理士　川▲崎▼　研二
(72)発明者　宮腰　大輔
長野県諏訪市大和３丁目３番５号　セイコーエプソン株式会社内
(72)発明者　無藤　和彦
長野県諏訪市大和３丁目３番５号　セイコーエプソン株式会社内
(72)発明者　山門　均
長野県諏訪市大和３丁目３番５号　セイコーエプソン株式会社内

最終頁に続く

(54)【発明の名称】通信機器、通信方法およびプログラム

(57)【特許請求の範囲】
【請求項１】
無線通信が可能な第１通信部と、
前記第１通信部とは異なる第２通信部と、
通信網に接続している１以上の通信機器の各々に関し、当該通信機器が実行可能な通信形態に関する案内情報を記憶する記憶部と、
制御部と
を備え、
前記制御部は、
新たに前記通信網に接続しようとする他の通信機器から、前記他の通信機器が実行可能な通信形態に関する案内情報を、前記第２通信部を用いて受信し、
前記第１通信部を利用して前記１以上の通信機器の各々と前記他の通信機器とが通信を行うための通信パラメータを前記記憶部に記憶されている案内情報および前記受信した案内情報に基づき決定し、
前記決定した通信パラメータの少なくとも一部を前記第２通信部を利用して前記他の通信機器に送信する
ことを特徴とする通信機器。
【請求項２】
前記第２通信部は前記他の通信機器と直接接触することにより有線通信接続を確立することを特徴とする請求項１に記載の通信機器。

【請求項３】
前記第２通信部は、前記他の通信機器との間で、前記第１通信部と前記他の通信機器との間で確立される無線通信接続と比べて近距離の無線通信接続を確立する
ことを特徴とする請求項１または２に記載の通信機器。
【請求項４】
前記制御部は、前記第２通信部を用いて前記他の通信機器から前記他の通信機器の識別子を受信し、前記識別子に基づき前記第１通信部を用いた前記他の通信機器との間の通信を行うか否かを決定する
ことを特徴とする請求項１乃至３のいずれかに記載の通信機器。
【請求項５】
無線通信が可能な第１通信部と前記第１通信部とは異なる第２通信部と記憶部とを有する一の通信機器が、通信網に接続している１以上の通信機器の各々に関し、当該通信機器が実行可能な通信形態に関する案内情報を前記記憶部に記憶する段階と、
前記一の通信機器が、新たに前記通信網に接続しようとする他の通信機器から、前記他の通信機器が実行可能な通信形態に関する案内情報を、前記第２通信部を用いて受信する段階と、
前記一の通信機器が、前記第１通信部を利用して前記１以上の通信機器の各々と前記他の通信機器とが通信を行うための通信パラメータを前記記憶部に記憶されている案内情報および前記受信した案内情報に基づき決定する段階と、
前記一の通信機器が、前記決定した通信パラメータの少なくとも一部を前記第２通信部を利用して前記他の通信機器に送信する段階と
を備えることを特徴とする通信方法。
【請求項６】
無線通信が可能な第１通信部と前記第１通信部とは異なる第２通信部と記憶部とを有する通信機器に、
通信網に接続している１以上の通信機器の各々に関し、当該通信機器が実行可能な通信形態に関する案内情報を前記記憶部に記憶させる処理と、
新たに前記通信網に接続しようとする他の通信機器から、前記他の通信機器が実行可能な通信形態に関する案内情報を、前記第２通信部を用いて受信させる処理と、
前記第１通信部を利用して前記１以上の通信機器の各々と前記他の通信機器とが通信を行うための通信パラメータを前記記憶部に記憶されている案内情報および前記受信した案内情報に基づき決定させる処理と、
前記決定した通信パラメータの少なくとも一部を前記第２通信部を利用して前記他の通信機器に送信させる処理と
を実行させるプログラム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、特定区域内情報通信網（ＬＡＮ）のためのパラメータ設定方法、通信端末、アクセスポイント、記録媒体およびプログラムに係り、特に、無線ＬＡＮのための各種設定を行うための技術に関する。
【０００２】
【従来の技術】
通信網に新たに通信端末を接続するには、一般的に次のような手順を踏む。まず通信端末のユーザが、自分の通信端末が利用可能な通信プロトコルに関する情報を通信網の管理者に伝える。次に管理者が通信網において利用可能な通信プロトコルの情報と、通信端末のユーザから得た通信端末が利用可能な通信プロトコルの情報とを考慮して、通信網と通信端末の両方が利用可能な通信プロトコルを１つもしくは複数選択する。続いて、管理者は選択した通信プロトコルのパラメータから変更を加える必要があるものを決定し、その決定したパラメータを通信端末のユーザに伝える。ユーザはこのパラメータを通信端末に設

定する。
上記のパラメータは通常、管理者以外は知らない情報を含んでいる。このため、例えば管理者が不在の場合には設定作業を行うことができない。また、たとえ必要なパラメータが得られたとしても、そのパラメータを用いて通信端末の設定を正しく迅速に行うことは、通常のユーザにとって容易ではない。更に、専門的な技術知識を持つ管理者であっても、利用可能な通信プロトコルが複数存在する場合、それぞれの通信プロトコルの通信速度等を考慮して、それらの通信プロトコルから適する通信プロトコルを選択することは容易ではない。

【０００３】
以上の事情から、必要なパラメータの設定を自動化することに対するニーズは高い。そのニーズに対し、まず、有線通信と無線通信に共通する中位および高位のレイヤのプロトコルに関するパラメータ設定を自動化する技術的努力がなされている。その例として、DHCP (Dynamic Host Configuration Protocol) サーバの利用がある。インターネットの普及に伴い多くの人がTCP/IP (Transmission Control Protocol / Internet Protocol) を利用しているが、TCP/IPにおいてはIPアドレスを通信網上の全ての通信機器に重複することなく割り当てる必要がある。以前は管理者がこの作業を手動で行い、ユーザは管理者から割り当てられたIPアドレスを自分の通信端末に手動で設定する必要があった。現在、DHCPサーバ・プログラムのインストールされた通信機器が通信網内の通信機器にIPアドレスを自動的に割り当て、DHCPクライアント・プログラムのインストールされた通信機器が、その通信機器に割り当てられたIPアドレスを自動的に受信し、設定することが広く行われている。

【０００４】
更に、利用する通信網が無線通信網である場合に、無線通信用の低位レイヤのプロトコルに関するパラメータ設定に関しては、有線通信と無線通信に共通する中位および高位のレイヤのプロトコルに関するパラメータ設定以上に、その自動化に対するニーズが高い。その主たる理由は、通信プロトコルの数が多いことによる。低位レイヤのプロトコルに関して、有線通信網においては現在IEEE802.3 (Ethernet、Fast Ethernet) がほぼ標準として定着しているのに対し、無線通信網においてはIEEE802.11bやBluetoothのように定着しつつある通信プロトコルが複数存在する。さらに、IEEE802.11a、IEEE802.15、IEEE802.16等の新たな通信プロトコルも登場しつつある。加えて、これらの無線通信網用の通信プロトコルの一部は同じ周波数帯を利用することから、場合によってはある通信プロトコルを用いるために他の通信プロトコルの使用を制限する必要がある。従って、無線通信網における通信プロトコルの選択は有線通信網におけるものより複雑である。
これに対し、無線通信用の低位レイヤのプロトコルに関するパラメータ設定自動化の技術として、周波数チャンネルの自動ネゴシエーションがある。これは、無線通信機器が一定の条件を満たす電波圏に入ると、無線通信機器がその電波の発信元の通信機器と相互に利用可能な周波数チャンネルを探し出し、その周波数チャンネルが無線通信機器に自動的に設定される、という技術である。

【０００５】
【発明が解決しようとする課題】
しかしながら、無線通信網に接続する際の設定は依然として手入力による部分が多い。その背景には、無線通信網においては有線通信網における場合と比較し、部外者が見えないところで接続を行い、通信情報の盗聴を行う可能性が高い、という事情がある。無線通信網においては、それらの通信情報の盗聴を防ぐため、有線通信網の場合と異なり、通常、低位レイヤのプロトコルにおいて接続認証およびデータの暗号化が行われる。これらの認証および暗号化のためのパラメータ設定は、セキュリティ上の理由から手入力によらざるを得ず、煩雑さが解消されていない。
更に、上述の従来技術によっても、無線通信網において利用可能な通信プロトコルが複数存在する場合にそれら複数の通信プロトコルから最適なものを選択する際の困難さは解消されていない。

【０００６】
本発明は上述した事情に鑑みてなされたものであり、無線通信網において新たな通信端末を接続する際、誰もが簡易に望ましい通信プロトコルを選択し、その選択された通信プロトコルを利用するにあたり必要となるパラメータ設定を行うことを可能とする無線通信設定方法、通信端末、アクセスポイント、記録媒体およびプログラムを提供することを目的としている。
【００１０】
また、本発明は、無線通信が可能な第１通信部と、前記第１通信部とは異なる第２通信部と、通信網に接続している１以上の通信機器の各々に関し、当該通信機器が実行可能な通信形態に関する案内情報を記憶する記憶部と、制御部とを備え、前記制御部は、新たに前記通信網に接続しようとする他の通信機器から、前記他の通信機器が実行可能な通信形態に関する案内情報を、前記第２通信部を用いて受信し、前記第１通信部を利用して前記１以上の通信機器の各々と前記他の通信機器とが通信を行うための通信パラメータを前記記憶部に記憶されている案内情報および前記受信した案内情報に基づき決定し、前記決定した通信パラメータの少なくとも一部を前記第２通信部を利用して前記他の通信機器に送信することを特徴とする通信機器を提供する。
【００１１】
好ましい態様において、前記第２通信部は前記他の通信機器と直接接触することにより有線通信接続を確立するように構成されていてもよい。
【００１２】
また、他の好ましい態様において、前記第２通信部は、前記他の通信機器との間で、前記第１通信部と前記他の通信機器との間で確立される無線通信接続と比べて近距離の無線通信接続を確立するように構成されていてもよい。
【００１３】
また、他の好ましい態様において、前記制御部は、前記第２通信部を用いて前記他の通信機器から前記他の通信機器の識別子を受信し、前記識別子に基づき前記第１通信部を用いた前記他の通信機器との間の通信を行うか否かを決定するように構成されていてもよい。
【００１５】
また、本発明は、無線通信が可能な第１通信部と前記第１通信部とは異なる第２通信部と記憶部とを有する一の通信機器が、通信網に接続している１以上の通信機器の各々に関し、当該通信機器が実行可能な通信形態に関する案内情報を前記記憶部に記憶する段階と、前記一の通信機器が、新たに前記通信網に接続しようとする他の通信機器から、前記他の通信機器が実行可能な通信形態に関する案内情報を、前記第２通信部を用いて受信する段階と、前記一の通信機器が、前記第１通信部を利用して前記１以上の通信機器の各々と前記他の通信機器とが通信を行うための通信パラメータを前記記憶部に記憶されている案内情報および前記受信した案内情報に基づき決定する段階と、前記一の通信機器が、前記決定した通信パラメータの少なくとも一部を前記第２通信部を利用して前記他の通信機器に送信する段階とを備えることを特徴とする通信方法を提供する。
【００１７】
また、本発明は、無線通信が可能な第１通信部と前記第１通信部とは異なる第２通信部と記憶部とを有する通信機器に、通信網に接続している１以上の通信機器の各々に関し、当該通信機器が実行可能な通信形態に関する案内情報を前記記憶部に記憶させる処理と、新たに前記通信網に接続しようとする他の通信機器から、前記他の通信機器が実行可能な通信形態に関する案内情報を、前記第２通信部を用いて受信させる処理と、前記第１通信部を利用して前記１以上の通信機器の各々と前記他の通信機器とが通信を行うための通信パラメータを前記記憶部に記憶されている案内情報および前記受信した案内情報に基づき決定させる処理と、前記決定した通信パラメータの少なくとも一部を前記第２通信部を利用して前記他の通信機器に送信させる処理とを実行させるプログラムを提供する。
【００２９】

【発明の実施の形態】
次に本発明の望ましい実施形態について説明する。これらの実施形態は本発明の一態様を示すものであってこの発明を限定するものではなく、本発明はその技術的思想の範囲内で任意に変更が可能である。
【００３０】
［１］第１実施形態
［１．１］第１実施形態の構成
［１．１．１］無線通信システムの構成
本発明の第１実施形態においては、本発明の通信パラメータ設定方法により、互いに未接続の２台の携帯型情報端末が１対１の無線通信を行うことが可能となる。図１に、本発明の第１実施形態における通信パラメータ設定段階の無線通信システムの状態と、通信パラメータ設定後の無線通信システムの状態を示す。なお、本発明の第１実施形態における通信パラメータ設定後に実現される無線通信システムを以下、「無線通信システム１」と呼ぶ。無線通信システム１は携帯型情報端末Ａ１および携帯型情報端末Ｂ２により構成される。
【００３１】
［１．１．２］携帯型情報端末の構成
図２に、本発明の第１実施形態における携帯型情報端末Ａ１の構成を示す。なお、携帯型情報端末Ｂ２の構成は、携帯型情報端末Ａ１と同様であるので、説明を省略する。
【００３２】
携帯型情報端末Ａ１は、接触型有線通信部１４、無線通信部１５、操作部１６、表示部１７および記憶部１８と、これらに接続された制御部１９とを有している。
【００３３】
接触型有線通信部１４は、他の同種の接触型有線通信部と直接接触することにより電気的導通状態を作り、制御部１９の制御の下で、パラメータ情報などを含む電気信号を送受信する。接触型有線通信部１４と同種の接触型有線通信部を持つ全ての携帯型情報端末は同じ有線用通信プロトコルを１つ持っており、携帯型情報端末Ａ１はその有線用通信プロトコルを用いて接触型有線通信部１４を介した情報の送受信を行う。
【００３４】
無線通信部１５はアンテナ（図示略）を有しており、このアンテナの受信信号から文字、画像、その他の通信情報を含むベースバンド信号を復調し、このベースバンド信号を制御部１９に送信する。また、無線通信部１５は、制御部１９からベースバンド信号を受信し、このベースバンド信号によってキャリアを変調し、変調した信号をアンテナ（図示略）を介して外部に送信する。無線通信部１５は不揮発性メモリ（図示略）を有し、この不揮発性メモリに通信パラメータを記憶し、前記の無線通信を行う際、記憶されている通信パラメータに基づいて通信に用いるチャンネルID、PIN Codeなどを選択する。無線通信部１５は複数の無線通信プロトコルに対応しており、それぞれの無線通信プロトコルを使用するための複数の異なるMACアドレスが無線通信部１５に割り当てられている。無線通信部１５は制御部１９の制御の下、これら複数の無線通信プロトコルを使い分ける。
【００３５】
操作部１６はキーパッド（図示略）を有し、ユーザがこのキーパッドのキーを操作すると、操作されたキーに対応した信号を制御部１９に送信する。
【００３６】
表示部１７は、液晶パネル（図示略）、駆動回路（図示略）およびビデオRAM (Random Access Memory)（図示略）を有している。制御部１９は表示したい文字や図形をビットマップ情報に変換し、このビットマップ情報をビデオRAMに書き込む。駆動回路は一定の時間間隔でビデオRAM内の一画面分のビットマップ情報を読み出し、その情報に基づいて液晶パネルの表示を更新する。
【００３７】
記憶部１８は大容量不揮発性メモリである。記憶部１８のデータは、制御部１９によって

書き込みおよび読み出しが行われる。制御部１９は記憶部１８の中に一連の情報の集合体としてのファイルを複数作成し、それを管理する。
記憶部１８は、プロトコル情報ファイル１８１、暗号鍵情報ファイル１８２および端末情報ファイル１８３を記憶している。
【００３８】
図３はプロトコル情報ファイル１８１の構成を例示したものである。プロトコル情報ファイル１８１は、携帯型情報端末Ａ１が利用可能な無線通信プロトコルの数と等しい数のレコードを持っている。各レコードは、携帯型情報端末Ａ１が利用可能な１つの無線通信プロトコルに関する情報の集まりであり、「プロトコル」フィールド、「MACアドレス」フィールド、「パラメータセット」フィールド、および「優先順位」フィールドを持つ。
「プロトコル」フィールドは、対象のプロトコルのプロトコル名情報を含む。プロトコル名情報としては、例えば、IEEE802.11b、Bluetooth、IrDA（Infrared Data Association）などがある。
「MACアドレス」フィールドは、対象のプロトコルに従って通信を行うときの携帯型情報端末Ａ１のMAC (Media Access Control) アドレスを含む。
「パラメータセット」フィールドは複数の子フィールド「パラメータ１」、「パラメータ２」・・・を持ち、各子フィールドは対象のプロトコルのパラメータ情報を１つずつ持つ。パラメータ情報としては、例えばIEEE802.11bのチャネルIDやBluetoothのPIN Codeなどがある。
「優先順位」フィールドは、携帯型情報端末Ａ１において利用可能な全ての無線通信プロトコルにおける対象のプロトコルの優先順位を示す正の整数を持つ。この正数値が小さいほど、対象のプロトコルが優先的に利用される。
【００３９】
図４は暗号鍵情報ファイル１８２の構成を例示したものである。暗号鍵情報ファイル１８２は「識別子」アイテムと「暗号鍵」アイテムを持つ。「識別子」アイテムは、携帯型情報端末Ａ１を他の携帯型情報端末から識別するために携帯型情報端末Ａ１に与えられた識別子を含む。この識別子は数字および記号の列であり、他の携帯型情報端末の識別子と同じ値をとることはない。「暗号鍵」アイテムは、無線通信システム１において携帯型情報端末Ａ１が情報を送信する際に、その情報を暗号化するために用いる暗号鍵情報を含む。
【００４０】
図５は端末情報ファイル１８３の構成を例示したものである。端末情報ファイル１８３は、携帯型情報端末Ａ１が今までに本発明の第１実施形態による１対１の無線通信を行った携帯型情報端末に関する情報のファイルである。端末情報ファイル１８３は、携帯型情報端末Ａ１が今までに無線通信を行った相手の携帯型情報端末の数と等しい数のレコードを持つ。各レコードは「識別子」フィールド、「アクセス権限」フィールド、「暗号鍵」フィールド、「プロトコル」フィールド、および「MACアドレス」フィールドを持つ。
「識別子」フィールドは、１対１通信の相手の携帯型情報端末の識別子を含む。
「アクセス権限」フィールドは、相手の携帯型情報端末が携帯型情報端末Ａ１のネットワーク資源を利用する場合に、相手の携帯型情報端末に与えられるアクセス権限を表す情報を含む。アクセス権限の例としては、読み取り専用およびフルアクセスがある。あるレコードの「アクセス権限」フィールドが読み取り専用を表している場合、そのレコードの対象である携帯型情報端末が携帯型情報端末Ａ１の持つ共有フォルダ等のネットワーク資源を利用するときには、そのネットワーク資源の参照のみが許可される。一方、あるレコードの「アクセス権限」フィールドがフルアクセスを表している場合、そのレコードの対象である携帯型情報端末が携帯型情報端末Ａ１のネットワーク資源を利用するときには、そのネットワーク資源の参照、変更および削除が許可される。
「暗号鍵」フィールドは、携帯型情報端末Ａ１が相手の携帯型情報端末から暗号化された情報を受信する際、その情報を復号化するために用いる暗号鍵情報を含む。
「プロトコル」フィールドは、携帯型情報端末Ａ１が相手の携帯型情報端末と無線通信を行う場合に用いるプロトコル名情報を含む。

「MACアドレス」フィールドは、携帯型情報端末Ａ１が相手の携帯型情報端末と無線通信を行う場合に用いる、相手の携帯型情報端末のMACアドレスを含む。

【００４１】

制御部１９は不揮発性メモリ（図示略）を有し、この不揮発性メモリに携帯型情報端末Ａ１の制御を指示するプログラムを記憶し、他の構成要素各部から受信する情報に基づいて、このプログラムに従った処理および構成要素各部の制御を行う。

【００４２】

［１．２］第１実施形態の動作

［１．２．１］通信パラメータ設定段階

次に、図６を用いて第１実施形態において無線通信パラメータ設定が行われる際の動作例を説明する。

この動作例は、携帯型情報端末Ａ１が、携帯型情報端末Ｂ２に対し接続要求を行う場合の動作である。なお、携帯型情報端末Ａ１と携帯型情報端末Ｂ２の同種の構成要素を区別するために、各構成要素を特定する符号に“Ａ”および“Ｂ”を付加する。

以下の動作において、携帯型情報端末Ａ１と携帯型情報端末Ｂ２との間の情報の送受信は全て接触型有線通信部１４Ａおよび接触型有線通信部１４Ｂを介して行われる。

【００４３】

まず、携帯型情報端末Ａ１または携帯型情報端末Ｂ２のユーザは、携帯型情報端末Ａ１の接触型有線通信部１４Ａと携帯型情報端末Ｂ２の接触型有線通信部１４Ｂとを直接接触させる（ステップＳ１０１）。

【００４４】

次に、ユーザは携帯型情報端末Ａ１の操作部１６Ａによって送信指示を入力する。操作部１６Ａは送信指示信号を制御部１９Ａに送信する（ステップＳ１０２）。制御部１９Ａはこの信号を受信すると、携帯型情報端末Ｂ２に接続要求信号を送信する（ステップＳ１０３）。

【００４５】

携帯型情報端末Ｂ２の制御部１９Ｂは接続要求信号を受信し、携帯型情報端末Ｂ２が携帯型情報端末Ａ１の接続要求に応じることが可能であることを示す接続許可信号を携帯型情報端末Ａ１に送信する（ステップＳ１０４）。

携帯型情報端末Ａ１の制御部１９Ａは接続許可信号を受信すると、プロトコル情報ファイル１８１Ａおよび暗号鍵情報ファイル１８２Ａを読み出し、通信パラメータ決定のための案内情報として以下の情報を準備する。

－　プロトコル情報ファイル１８１Ａの全レコードの「プロトコル」フィールドおよび「MACアドレス」フィールドの値（以下、「プロトコル・テーブルA」と呼ぶ）

－　暗号鍵情報ファイル１８２Ａの「識別子」アイテムの値（以下、「ID-A」と呼ぶ）

－　暗号鍵情報ファイル１８２Ａの「暗号鍵」アイテムの値（以下、「Key-A」と呼ぶ）

上記の情報を準備した後、制御部１９Ａはこの情報を携帯型情報端末Ｂ２に送信する（ステップＳ１０５）。

【００４６】

携帯型情報端末Ｂ２の制御部１９Ｂは案内情報として、プロトコル・テーブルA、ID-AおよびKey-Aを受信する。続いて制御部１９Ｂは端末情報ファイル１８３Ｂを読み出し、いずれかのレコードの「識別子」フィールドにID-Aと一致する値があるか否かを判定する（ステップＳ１０６）。端末情報ファイル１８３Ｂのいずれのレコードの「識別子」フィールドにもID-Aと一致する値がない場合、制御部１９Ｂはステップ Ｓ１０６の判定で「Ｎｏ」を得る。これは携帯型情報端末Ｂ２に携帯型情報端末Ａ１が未登録であることを意味する。一方、端末情報ファイル１８３Ｂのいずれかのレコードの「識別子」フィールドの値がID-Aと一致する場合、制御部１９Ｂはステップ Ｓ１０６の判定で「Ｙｅｓ」を得る。これは携帯型情報端末Ｂ２に携帯型情報端末Ａ１が登録済みであることを意味する。

【００４７】

ステップＳ１０６の判定において「Ｎｏ」を得た場合、制御部１９Ｂは端末情報ファイル

１８３Ｂに新しいレコードを追加し、この新たなレコードの「識別子」フィールドの値をID-Aとし、「アクセス権限」フィールドの値を“読み取り専用”とし、「暗号鍵」フィールドの値をKey-Aとする（ステップＳ１０７）。

【００４８】

一方、ステップＳ１０６の判定において「Ｙｅｓ」を得た場合、制御部１９Ｂは、端末情報ファイル１８３Ｂの「識別子」フィールドの値がID-Aと一致するレコードを検索し、検索されたレコードの「暗号鍵」の値をKey-Aで更新する（ステップＳ１０８）。

【００４９】

ステップＳ１０７もしくはステップＳ１０８を終えた後、制御部１９Ｂはプロトコル情報ファイル１８１Ｂを読み出し、その全レコードの中から、「プロトコル」フィールドに含まれる値が、ステップＳ１０６において携帯型情報端末Ａ１から受信したプロトコル・テーブルAのいずれかのレコードの「プロトコル」フィールドの値と一致するレコードを抽出する。プロトコル情報ファイル１８１Ｂから複数のレコードが抽出された場合、制御部１９Ｂは抽出されたレコードの「優先順位」フィールドの値を比較し、「優先順位」フィールドの値が最も小さいレコードを選択する。一つのレコードのみが抽出された場合、制御部１９Ｂはそのレコードを選択する。続いて制御部１９Ｂは、選択されたレコードの「プロトコル」フィールドの値（以下、「決定プロトコル１」と呼ぶ）と「MACアドレス」フィールドの値（以下、「MAC-B」と呼ぶ）を取り出す。

次に制御部１９Ｂはプロトコル・テーブルAの全レコードのうち「プロトコル」フィールドの値が決定プロトコル１と一致するレコードを検索し、検索されたレコードの「MACアドレス」フィールドの値（以下、「MAC-A」と呼ぶ）を取り出す。

次に制御部１９Ｂは端末情報ファイル１８３Ｂを読み出し、全レコードから「識別子」フィールドの値がID-Aと一致するレコードを検索し、検索されたレコードの「プロトコル」フィールドの値を決定プロトコル１で、「MACアドレス」フィールドの値をMAC-Aで更新する（ステップＳ１０９）。

【００５０】

続いて、制御部１９Ｂは、プロトコル情報ファイル１８１Ｂを読み出し、その全レコードから「プロトコル」フィールドの値が決定プロトコル１と一致するレコードを検索し、検索されたレコードの「パラメータセット」フィールドの値に基づき、携帯型情報端末Ａ１用のプロトコル・パラメータを決定する（ステップＳ１１０）。例えば、決定プロトコル１が“IEEE802.11b"であり、それに対応する「パラメータセット」フィールドが“チャネルID＝１”をその値として含んでいれば、制御部１９Ｂは携帯型情報端末Ａ１用のIEEE802.11bのパラメータとして“チャネルID＝１”を決定する。以下、ステップＳ１１０において決定されたプロトコル・パラメータを「決定パラメータセット１」と呼ぶ。

【００５１】

次に、制御部１９Ｂは暗号鍵情報ファイル１８２Ｂを読み出し、「識別子」アイテムの値（以下、「ID-B」と呼ぶ）および「暗号鍵」アイテムの値（以下、「Key-B」と呼ぶ）を取り出す。

続いて、制御部１９Ｂは通信パラメータとして、ID-B、Key-B、決定プロトコル１、MAC-B、および決定パラメータセット１を携帯型情報端末Ａ１に送信する（ステップＳ１１１）。

【００５２】

携帯型情報端末Ａ１の制御部１９Ａは、ID-B、Key-１B決定プロトコル１、MAC-Bおよび決定パラメータセット１を通信パラメータとして受信する。続いて、制御部１９Ａは端末情報ファイル１８３Ａを読み出し、その全レコードから「識別子」フィールドの値がID-Bと一致するレコードを検索し、検索されたレコードの「暗号鍵」フィールドの値をKey-Bで、「プロトコル」フィールドの値を決定プロトコル１で、「MACアドレス」フィールドの値をMAC-Bで更新する。端末情報ファイル１８３Ａのいずれのレコードの「識別子」フィールドの値もID-Bと一致しない場合は、制御部１９Ａは端末情報ファイル１８３Ａに新たなレコードを追加し、そのレコードの「識別子」フィールドの値をID-Bとし、「アクセス

権限」フィールドの値を“読み取り専用”とし、「暗号鍵」フィールドの値をKey-Bとし、「プロトコル」フィールドの値を決定プロトコル１とし、「MACアドレス」フィールドの値をMAC-Bとする。続いて、制御部１９Ａは無線通信部１５Ａに決定プロトコル１および決定パラメータセット１を送信し、無線通信部１５Ａは不揮発性メモリに記憶している決定プロトコル１に関するプロトコル・パラメータを決定パラメータセット１によって更新する。その後、制御部１９Ａは無線通信パラメータの設定完了のメッセージを表示部１７Ａに表示する（ステップＳ１１２）。

【００５３】

［１．２．２］暗号鍵を用いた通信方法

ステップＳ１１２までの設定作業を終えた後、携帯型情報端末Ａ１が携帯型情報端末Ｂ２に情報を送信する場合、まず制御部１９Ａは暗号鍵情報ファイル１８２Ａを読み出し、携帯型情報端末Ｂ２に送信する情報を「暗号鍵」アイテムの値、すなわちKey-Aで暗号化する。続いて制御部１９Ａは端末情報ファイル１８３Ａを読み出し、「MACアドレス」フィールドの値が情報の送信先のMACアドレス、すなわちMAC-Bと一致するレコードを検索し、検索されたレコードの「プロトコル」フィールドの値が示す通信プロトコルに従って暗号化した情報をフォーマットする。続いて制御部１９Ａはフォーマットした情報に送信先を示すMAC-Bおよび送信元を示すMAC-Aを付加し、無線通信部１５Ａを介してその情報を携帯型情報端末Ｂ２に送信する。

【００５４】

また、ステップＳ１１２までの設定作業を終えた後、携帯型情報端末Ａ１が携帯型情報端末Ｂ２から暗号化された情報を受信する場合、まず制御部１９Ａは受信した情報から送信元のMACアドレス、すなわちMAC-Bを取り出す。続いて制御部１９Ａは端末情報ファイル１８３Ａを読み出し、「MACアドレス」フィールドの値がMAC-Bと一致するレコードを検索し、検索されたレコードの「暗号鍵」フィールドの値、すなわちKey-Bを用いて携帯型情報端末Ａ１受信した情報を復号化する。こうして復号化された情報が、携帯型情報端末Ｂ２が携帯型情報端末Ａ１のネットワーク資源を利用することを要求していることを示す情報を含む場合、制御部１９Ａは先に読み出したレコードの「アクセス権限」フィールドの値に従い、その要求を許可もしくは拒絶する。

【００５５】

［１．３］第１実施形態の効果

第１実施形態においては、２つの携帯型情報端末が無線通信を行う場合に、ユーザがただそれらの携帯型情報端末の接触型有線通信部を直接接触させることにより、通信に必要となる識別子等の端末情報、無線通信プロトコルに関するパラメータ、暗号鍵等が携帯型情報端末に設定される。従って、携帯型情報端末のユーザがネットワーク技術に関する専門的な知識を持たない場合であっても、簡易に無線通信を開始することができる。

【００５６】

第１実施形態においては、携帯型情報端末が無線通信システム１にて用いられる無線通信プロトコルが、利用可能な無線通信プロトコルの全てに予め設定されている優先順位に基づき選択される。従って、携帯型情報端末のユーザが無線通信プロトコルに関する技術知識を持たない場合であっても、最適な無線通信プロトコルを用いることできる。

【００５７】

第１実施形態により実現される無線通信システム１においては、携帯型情報端末間で通信される情報が暗号化されるため、部外者がその情報を受信した場合でもその情報を解読することができず、情報の漏洩が防止される。

【００５８】

［１．４］第１実施形態の変形例

第１実施形態においては無線通信に必要な通信パラメータを決定する側の通信機器が、通信パラメータを決定しない側の通信機器と同じ携帯型情報端末であるが、通信パラメータを決定する側の通信機器の通信機器は携帯型情報端末に限られない。例えば、通信パラメータを決定する側の通信機器は複数の無線通信機器の通信を中継するアクセスポイントで

あってもよい。その場合、新たに無線通信を行う携帯型情報端末は本発明の通信パラメータ設定方法により無線通信のための設定を完了した後、アクセスポイントを経由してアクセスポイントに接続している複数の通信機器と通信を行うことができる。

【００５９】

第１実施形態においては、携帯型情報端末のユーザは携帯型情報端末の接触型有線通信部を他の同種の接触型有線通信部と直接接触させることにより接続を確立し、携帯型情報端末はこの接続において無線通信システム１における無線通信のための情報の送受信を行っているが、接続の方法はこれに限らない。例えば、携帯型情報端末の有線通信部を相互に通信ケーブルで接続してもよい。

また、無線通信システム１における無線通信のための情報を送受信するにあたり、第１実施形態において用いられている接触型有線通信部の代わりに無線通信部が用いられてもよい。この場合には、無線通信システム１において無線通信を行おうとする携帯型情報端末の両方に予め同じ通信パラメータ設定用として無線通信プロトコルを１つ準備しておき、その設定用の無線通信プロトコルを用いて、無線通信システム１において用いる無線通信プロトコルのための通信パラメータ設定を行う。これにより、直接接続やケーブル接続をする手間が省かれ、より簡易に無線通信に関する通信パラメータ設定を行うことが可能となる。

【００６０】

第１実施形態においては、ユーザが送信指示の操作を行うことにより接続要求信号が送信されているが、接続要求信号が送信される方法はこれに限られない。例えば、接触型有線通信部が接続された後、タイマにより設定された時間が経過した後に携帯型情報端末の制御部が接続要求信号を送信してもよい。

【００６１】

第１実施形態においては、無線通信システム１用の独自の識別子が携帯型情報端末に割り当てられているが、識別子は独自のものでなくともよい。例えば、MACアドレスを識別子として用いてもよい。MACアドレスは、通信機器ごとに必ず付加されているため、本発明を用いるにあたり、新たに管理者等が携帯型情報端末ごとに識別子を割り振る必要がなくなる。

【００６２】

第１実施形態においては、無線通信の通信パラメータ設定完了のメッセージが表示部に表示されるが、通信パラメータ設定完了の通知方法はこれに限らない。例えば、携帯型情報端末が音声出力部を有し、無線通信の設定が完了した場合、携帯型情報端末の制御部が音声出力部を用いて音声により通信パラメータ設定の完了を通知してもよい。

【００６３】

携帯型情報端末は、第１実施形態における携帯型情報端末の各種制御を制御部に実行させるためのプログラムを、必ずしも予め内部に記憶していなくともよい。例えば、携帯型情報端末がデータ読込部を有し、制御部がこのデータ読込部を用いて前記のプログラムが記録された記録媒体からプログラムを読み取った後に、そのプログラムを実行してもよい。また、携帯型情報端末が電気通信回線により外部の記憶装置のデータにアクセスできる通信部を有し、制御部がこの通信部を用いて前記のプログラムをダウンロードした後に、そのプログラムを実行してもよい。

【００６４】

第１実施形態において実現される無線通信システム１においては、暗号鍵として共通暗号鍵が用いられているが、本発明において用いられる暗号化の方法は共通鍵方式に限らない。例えば、公開鍵方式により情報を暗号化してもよい。

【００６５】

［２］第２実施形態

［２．１］第２実施形態の構成

［２．１．１］無線通信システムの構成

本発明の第２実施形態においては、本発明の通信パラメータ設定方法により、第１実施形

態と同様に互いに未接続の２台の通信端末が１対１の無線通信を行うことが可能となる。図７に本発明の第２実施形態における通信パラメータ設定段階の状態と通信パラメータ設定後の無線通信システムの状態を示す。なお、本発明の第２実施形態により実現される通信パラメータ設定後の無線通信システムを以下、「無線通信システム２」と呼ぶ。無線通信システム２は通信端末C3および通信端末D4により構成される。　第１実施形態においては無線通信のための通信パラメータの決定を要求する通信端末と通信パラメータの決定を行う通信端末を決定するために、いずれかの通信端末のユーザが操作部を用いて通信端末に通信パラメータ設定動作の開始の指示を与える必要があったが、第２実施形態においてはその必要はない。通信パラメータ設定段階において、ユーザの介入なしに２台の通信端末のいずれか１つが通信パラメータの決定を要求する役割を選択し、他の１つが通信パラメータの決定を行う役割を選択する。以下、通信パラメータの決定を行う通信端末を「マスタ」、通信パラメータの決定を行わない通信端末を「スレーブ」と呼ぶ。すなわち、マスタは２台の通信端末が無線通信システム２における無線通信を行うために必要な通信パラメータを決定し、その決定された通信パラメータに基づいて自分の通信パラメータの変更を行うと共に、決定された通信パラメータをスレーブに送信する。スレーブはマスタから通信パラメータを受信し、これに従って自分の通信パラメータを変更する。
また、第１実施形態においてはIEEE802.11b等の下位レイヤに関する無線通信プロトコルのパラメータ設定のみが扱われていたが、第２実施形態においてはTCP/IP等の中位レイヤに関する通信プロトコルのパラメータ設定も併せて扱う。

【００６６】

［２．１．２］通信端末の構成

図８に、通信端末Ｃ３の構成を示す。なお、通信端末Ｄ４の構成は通信端末Ｃ３の構成と同じであるので、その説明を省略する。

【００６７】

通信端末Ｃ３は有線通信部２０、無線通信部２１、操作部２２、表示部２３、制御部２４および記憶部２５を有している。これらの構成要素はバス２６を介して電気的に接続されている。

【００６８】

有線通信部２０、無線通信部２１、操作部２２、表示部２３、制御部２４は第１実施形態における携帯型情報端末Ａ１の接触型有線通信部１４、無線通信部１５、操作部１６、表示部１７、制御部１９とそれぞれ同様であるので、説明を省略する。また、記憶部２５の機能も第１実施形態における携帯型情報端末Ａ１の記憶部１８と同様であるので、説明を省略する。

【００６９】

記憶部２５は、設定管理情報ファイル２５１、端末情報ファイル２５２、自機プロトコル情報ファイル２５３、他機プロトコル情報ファイル２５４、決定プロトコル情報ファイル２５５を記憶し、作業領域２５６を有している。

【００７０】

図９は設定管理情報ファイル２５１の構成を例示したものである。設定管理情報ファイル２５１は「マスタ・スレーブ」アイテム、「自機識別子」アイテム、「他機識別子」アイテム、「パスワード」アイテム、「共通鍵」アイテム、「設定完了通知フラグ」アイテムを持つ。「マスタ・スレーブ」アイテムは、通信端末Ｃ３が無線通信システム２のための無線通信パラメータ設定の際、マスタとして機能するか、スレーブとして機能するかが決定される際に用いられ、“０”、“１”、“２”のいずれかの値をとる。“０”は未設定、“１”はマスタ、“２”はスレーブを意味する。「自機識別子」アイテムは通信端末Ｃ３を他の通信端末から識別するための識別子を含み、この識別子は変更されることはない。なお、識別子は数字および文字の列である。「他機識別子」アイテムは通信端末Ｃ３が無線通信システム２において無線通信を行う相手の通信端末の識別子を含む。「パスワード」アイテムは通信端末Ｃ３のユーザ以外が通信端末Ｃ３を無断で無線通信接続することを防ぐためのパスワードの値を含み、このパスワードの値はユーザが予め任意に設定する

。「共通鍵」アイテムは無線通信システム２において通信端末Ｃ３が他の通信端末と通信を行う際に通信情報を暗号化および復号化するための暗号鍵情報を含む。「設定完了通知フラグ」アイテムは通信端末Ｃ３が無線通信システム２において無線通信を行う相手の通信端末が、無線通信パラメータ設定を完了したことを確認する為に用いられ、“ OFF ”、“ ON ”のいずれかの値をとる。“ OFF ”は未完了、“ ON ”は完了を意味する。

【００７１】

図１０は端末情報ファイル２５２の構成を例示したものである。端末情報ファイル２５２は、今までに通信端末Ｃ３に対する接続を許可された通信端末の数と等しい数のレコードを持ち、各レコードは対象の通信端末の識別子を含む「識別子」フィールドを持つ。

【００７２】

図１１は自機プロトコル情報ファイル２５３の構成を例示したものである。自機プロトコル情報ファイル２５３は通信端末Ｃ３が利用可能な通信プロトコルの情報からなるファイルである。なお、以下、「プロトコルセット」という言葉を用いる場合、これは下位レイヤのプロトコルと中位レイヤのプロトコルの組み合わせを意味する。プロトコルセットの例としては、“ IEEE802.11b - TCP/IP ”、“ Bluetooth - NetBEUI ”などがある。自機プロトコル情報ファイル２５３は通信端末Ｃ３が利用可能な通信プロトコルセットの数と等しい数のレコードを持ち、各レコードは１つの通信プロトコルセットの情報の集まりであり、「優先順位」フィールド、「MACアドレス」フィールド、「パラメータセット」フィールドを持つ。「優先順位」フィールドは正の整数をとり、この正の整数が小さいほど、対象の通信プロトコルセットの優先順位が高いことを示す。この正の整数は予めユーザもしくは管理者により設定されている。「MACアドレス」フィールドは対象の通信プロトコルセットに割り当てられているMACアドレスを含む。「プロトコルセット」フィールドは対象の通信プロトコルセットの名称を示す情報を含む。「パラメータセット」フィールドは複数の子フィールド「パラメータ１」、「パラメータ２」、・・・を持ち、各子フィールドは対象の通信プロトコルセットのパラメータ情報を１つずつ含む。なお、通信プロトコルセットによりパラメータの数が異なるため、「パラメータセット」フィールドの子フィールドの数はあらゆる通信プロトコルセットが必要とするパラメータを含むことができるよう、十分に大きな数が確保されている。

【００７３】

図１２は他機プロトコル情報ファイル２５４の構成を例示したものである。他機プロトコル情報ファイル２５４は無線通信システム２において通信端末Ｃ３に接続を行う相手の通信端末が利用可能な通信プロトコルセットの情報を含む。他機プロトコル情報ファイル２５４は相手の通信端末が利用可能な通信プロトコルセットの数と等しい数のレコードを持ち、各レコードは１つの通信プロトコルセットに関する情報の集まりであり、「MACアドレス」フィールドおよび「プロトコルセット」フィールドを持つ。「MACアドレス」は対象の通信プロトコルセットに割り当てられたMACアドレスを含む。「プロトコルセット」フィールドは対象の通信プロトコルセットの名称を示す情報を含む。

【００７４】

図１３は決定プロトコル情報ファイル２５５の構成を例示したものである。決定プロトコル情報ファイル２５５は無線通信システム２において使用される通信プロトコルセットに関する情報を含む。決定プロトコル情報ファイル２５５は１つのレコードからなり、このレコードは「自機MACアドレス」フィールド、「他機MACアドレス」フィールド、「プロトコルセット」フィールド、「パラメータセット」フィールドを持つ。「自機MACアドレス」フィールドは通信端末Ｃ３が対象の通信プロトコルセットを用いて相手の通信端末と通信を行う際の、通信端末Ｃ３のMACアドレスを含む。「他機MACアドレス」フィールドは相手の通信端末が対象の通信プロトコルセットを用いて通信端末Ｃ３と通信を行う際の、相手の通信端末のMACアドレスを含む。「プロトコルセット」フィールドは対象の通信プロトコルセットの名称を示す情報を含む。「パラメータセット」フィールドは子フィールド「パラメータ１」、「パラメータ２」・・・を持ち、各子フィールドは対象の通信プロトコルセットに関するパラメータを１つずつ含む。

【００７５】
作業領域２５６は制御部２４が制御処理を行う際にプログラムやデータを一時的に記憶するための領域である。
【００７６】
［２．２］第２実施形態の動作
第２実施形態において、無線通信システム２を実現するための通信パラメータ設定動作および通信パラメータ設定後の通信動作について説明する。通信パラメータ設定は接続認証段階、マスタ・スレーブ決定段階およびパラメータ設定段階から成る。以下の動作例は、通信端末Ｃ３と通信端末Ｄ４が互いに１対１の無線通信を行うことを可能とする際の動作例である。なお、通信端末Ｃ３と通信端末Ｄ４の同種の構成要素を区別するために、各構成要素を特定する符号に“Ｃ”および“Ｄ”を付加する。
以下の接続認証段階、マスタ・スレーブ決定段階、およびパラメータ設定段階において、通信端末Ｃ３と通信端末Ｄ４の間で行われる情報の送受信は全て有線通信部２０Ｃおよび有線通信部２０Ｄを介して行われる。
【００７７】
［２．２．１］接続認証段階
通信端末Ｃ３および通信端末Ｄ４はまず、相手の通信端末の認証を行う。図１４を用いてその動作説明を行う。
以下の動作は通信端末Ｃ３と通信端末Ｄ４のそれぞれにおいて並行して行われ、通信端末Ｃ３と通信端末Ｄ４の動作は同じである。従って、ここでは通信端末Ｃ３の動作のみを説明する。通信端末Ｄ４の動作については、以下の説明における符号“Ｃ”と“Ｄ”とを入れ替えることにより、その説明が得られる。
【００７８】
はじめに、通信端末Ｃ３または通信端末Ｄ４のユーザは、通信端末Ｃ３の有線通信部２０Ｃと通信端末Ｄ４の有線通信部２０Ｄとを直接接続させる（ステップＳ２０１）。
【００７９】
制御部２４Ｃは、有線通信部２０Ｃを介して他の通信端末との有線接続を検知すると、設定管理情報ファイル２５１Ｃを読み出し、「マスタ・スレーブ」アイテムの値を“０”、「設定完了通知フラグ」アイテムの値を“OFF”とする（ステップＳ２０２）。
【００８０】
次に、制御部２４Ｃは設定管理情報ファイル２５１Ｃの「自機識別子」アイテムの値（以下、「ID-C」と呼ぶ）を通信端末Ｄ４に送信する（ステップＳ２０３）。
一方、通信端末Ｄ４も同様に設定管理情報ファイル２５１Ｄの「自機識別子」アイテムの値（以下、「ID-D」と呼ぶ）を通信端末Ｃ３に送信する。制御部２４ＣはID-Dを受信し、設定管理情報ファイル２５１Ｃの「他機識別子」アイテムの値をID-Dで更新する（ステップＳ２０４）。
【００８１】
続いて、制御部２４Ｃは端末情報ファイル２５２Ｃを読み出し、いずれかのレコードの「識別子」フィールドの値がID-Dと一致するか否かを判定する（ステップＳ２０５）。通信端末Ｃ３が過去に通信端末Ｄ４の接続を認証したことがない場合、いずれのレコードの「識別子」フィールドの値もID-Dと一致せず、制御部２４ＣはステップＳ２０５の判定で「Ｎｏ」を得る。通信端末Ｃ３が過去に通信端末Ｄ４の接続を認証したことがある場合、いずれかのレコードの「識別子」フィールドの値がID-Dと一致し、制御部２４ＣはステップＳ２０５の判定で「Ｙｅｓ」を得る。
【００８２】
ステップＳ２０５において「Ｙｅｓ」を得た場合、制御部２４Ｃは制御を後述するステップＳ２１０に移す。
【００８３】
ステップＳ２０５において「Ｎｏ」を得た場合、制御部２４Ｃはパスワード入力要求のメッセージを表示部２３Ｃに表示する（ステップＳ２０６）。このパスワード入力は、通信

端末Ｃ３が通信端末Ｄ４の通信端末Ｃ３に対する接続を新たに認証することの確認作業である。
通信端末Ｃ３のユーザが操作部２２Ｃによってパスワード（以下、このパスワードの値を「入力パスワードC」と呼ぶ）を入力し、制御部２４Ｃが入力パスワードCを受信すると（ステップＳ２０７）、制御部２４Ｃは設定管理情報ファイル２５１Ｃを読み出し、入力パスワードCが設定管理情報ファイル２５１Ｃの「パスワード」アイテムの値（以下、「登録パスワードC」と呼ぶ）と一致するか否かを判定する（ステップＳ２０８）。入力パスワードCが登録パスワードCと異なる場合、制御部２４Ｃはステップ２０８の判定で「Ｎｏ」を得る。入力パスワードCが登録パスワードCと同じ場合、制御部２４Ｃはステップ２０８の判定で「Ｙｅｓ」を得る。
ステップＳ２０８において「Ｎｏ」を得た場合、制御部２４Ｃは制御をステップＳ２０６に移す。その後、これら２つのパスワードが一致するまで、ステップＳ２０６からステップＳ２０８までが繰り返される。なお、上記ステップＳ２０６からステップＳ２０８までの動作を以下、「パスワード照合作業」と呼ぶ。
【００８４】
ステップＳ２０８において「Ｙｅｓ」を得た場合、制御部２４Ｃは端末情報ファイル２５２Ｃを読み出し、新しいレコードを追加し、そのレコードの「識別子」フィールドの値をID-Dとする（ステップＳ２０９）。この作業により、通信端末Ｄ４は通信端末Ｃ３に新規登録される。制御部２４Ｃはステップ２０９を終えると、制御をステップＳ２１０に移す。なお、上記ステップＳ２０５からステップＳ２０９までの動作を以下、「識別子登録作業」と呼ぶ。
【００８５】
［２．２．２］マスタ・スレーブ決定段階
上述の接続認証段階を終えた後、通信端末Ｃ３および通信端末Ｄ４はどちらの通信端末がマスタとなり、どちらの通信端末がスレーブとなるかを決定する。図１５を用いてその動作説明を行う。
以下の動作は通信端末Ｃ３と通信端末Ｄ４のそれぞれにおいて並行して行われ、通信端末Ｃ３と通信端末Ｄ４とは同じ動作をする。従って、ここでは通信端末Ｃ３の動作のみを説明する。通信端末Ｄ４の動作については、以下の説明における符号ＣとＤとを入れ替えることにより、その説明が得られる。
【００８６】
制御部２４Ｃは通信端末Ｄ４の接続認証を終えると、設定管理情報ファイル２５１Ｃを読み出し、「自機識別子」アイテムの値、すなわちID-Cと、「他機識別子」アイテムの値、すなわちID-Dを用いた演算により、通信端末Ｃ３がマスタとして機能すべきか否かを判定する（ステップＳ２１０）。この判定ための演算の例として、ID-CとID-Dの２進数表現による値の和をとり、その和が偶数の場合は識別子が大きい方の通信端末をマスタとし、その和が奇数の場合は識別子が小さい方の通信端末をマスタとする方法がある。ただし、この方法に限らず、通信端末Ｃ３と通信端末Ｄ４のいずれがマスタとして機能すべきかを一意に決定可能な方法であれば何であってもよい。通信端末Ｃ３がマスタとして機能すべき場合、制御部２４Ｃはステップ２１０の判定で「Ｙｅｓ」を得る。通信端末Ｄ４がマスタとして機能すべき場合、制御部２４Ｃはステップ２１０の判定で「Ｎｏ」を得る。
【００８７】
ここで、以下のステップにおいて通信端末Ｄ４が通信端末Ｃ３に対して行う割り込み処理要求について説明する。
通信端末Ｃ３はステップ２１０の判定に基づき、下記のステップＳ２１３もしくはステップＳ２１４において、通信端末Ｄ４に対しマスタ設定要求もしくはスレーブ設定要求を割り込み要求として送信する。同様に、通信端末Ｄ４は通信端末Ｃ３に対しマスタ設定要求もしくはスレーブ設定要求を割り込み要求として送信する。通信端末Ｃ３の制御部２４Ｃはマスタ設定要求を受信すると、それまでの処理を一時停止し、設定管理情報ファイル２５１Ｃを読み出し、「マスタ・スレーブ」アイテムの値を“１”で更新した後、一時停

止した前記処理を再開する。同様に、制御部２４Ｃはスレーブ設定要求を受信すると、それまでの処理を一時停止し、設定管理情報ファイル２５１Ｃを読み出し、「マスタ・スレーブ」アイテムの値を“２”で更新した後、一時停止した前記処理を再開する。
これらの割り込み処理要求の送信はマスタ・スレーブ決定段階においてのみ行われるが、受信はマスタ・スレーブ決定段階のみでなく、接続認証段階においても行われる可能性がある。以上が割り込み処理要求の説明である。

【００８８】
ステップＳ２１０において「Ｙｅｓ」を得た場合、制御部２４Ｃは設定管理情報ファイル２５１Ｃを読み出し、「マスタ・スレーブ」アイテムの値を取り出す（ステップＳ２１１）。この時点で、通信端末Ｃ３が既に通信端末Ｄ４からマスタ設定要求を受信している場合、制御部２４Ｃはステップ Ｓ２１１で「１」を得る。この時点で、通信端末Ｃ３がまだ通信端末Ｄ４からマスタ設定要求を受信していない場合、制御部２４Ｃはステップ Ｓ２１１で「０」を得る。通信端末Ｃ３と通信端末Ｄ４は同じ演算を行うので、この場合、通信端末Ｄ４が通信端末Ｃ３に対しスレーブ設定要求を送信することはなく、従って制御部２４Ｃはステップ Ｓ２１１で「２」を得ることはない。

【００８９】
ステップＳ２１１において「０」を得た場合、制御部２４Ｃは予め定められた短時間、例えば１秒間だけ待機した後、ステップＳ２１１に制御を戻す（ステップＳ２１２）。この動作はステップＳ２１１において、「マスタ・スレーブ」の値が“０”である限り繰り返される。この間、通信端末Ｃ３は通信端末Ｄ４から送信されてくるべきマスタ設定要求の待ち状態にある。

【００９０】
ステップＳ２１１において「１」を得た場合、制御部２４Ｃは通信端末Ｄ４に対し、スレーブ設定要求を送信する（ステップＳ２１３）。これは通信端末Ｃ３が通信端末Ｄ４の行った演算処理と同じ結果を得たことの確認通知の意味を持つ。制御部２４Ｃはステップ Ｓ２１３を終えると、後述するステップＳ２１９に制御を移す。

【００９１】
ステップＳ２１０において「Ｎｏ」を得た場合、制御部２４Ｃは通信端末Ｄ４に対し、マスタ設定要求を送信する（ステップＳ２１４）。これは通信端末Ｃ３が自分の行った演算処理の結果を通信端末Ｄ４に通知し、通信端末Ｄ４にその結果の確認を要求する意味を持つ。

【００９２】
ステップＳ２１４において通信端末Ｄ４にマスタ設定要求を送信した後、制御部２４Ｃは設定管理情報ファイル２５１Ｃを読み出し、「マスタ・スレーブ」アイテムの値を取り出す（ステップＳ２１５）。この時点で、通信端末Ｃ３が既に通信端末Ｄ４からスレーブ設定通知を受信している場合、制御部２４Ｃはステップ Ｓ２１５で「２」を得る。この時点で、通信端末Ｃ３がまだ通信端末Ｄ４からスレーブ設定要求を受信していない場合、制御部２４Ｃはステップ Ｓ２１５で「０」を得る。通信端末Ｃ３と通信端末Ｄ４は同じ演算を行うので、この場合、通信端末Ｄ４が通信端末Ｃ３に対しマスタ設定要求を送信することはなく、従って制御部２４Ｃはステップ Ｓ２１５で「１」を得ることはない。

【００９３】
ステップＳ２１５において「０」を得た場合、制御部２４Ｃは予め定められた短時間、例えば１秒間だけ待機した後、ステップＳ２１５に制御を戻す（ステップＳ２１６）。この動作はステップＳ２１５において、「マスタ・スレーブ」の値が“０”である限り繰り返される。この間、通信端末Ｃ３は通信端末Ｄ４から送信されてくるべきスレーブ設定要求の待ち状態にある。

【００９４】
ステップＳ２１５において「２」を得た場合、制御部２４Ｃは後述するステップＳ２１７に制御を移す。

【００９５】

［２．２．３］パラメータ設定段階
上述のマスタ・スレーブ決定段階を終えた後、通信端末Ｃ３および通信端末Ｄ４は無線通信のためのパラメータ設定を行う。図１６および図１７を用いてその動作説明を行う。
【００９６】
なお、以下においてはマスタとして機能する通信端末Ｍとスレーブとして機能する通信端末Ｓの動作について説明を行う。従って、通信端末Ｃ３がマスタの場合には符号ＭをＣと入れ替えることにより、また通信端末Ｃ３がスレーブの場合には符号ＳをＣと入れ替えることにより、その説明が得られる。通信端末Ｄについても同様である。
なお、通信端末Ｍと通信端末Ｓの同種の構成要素を区別するために、各構成要素を特定する符号に“Ｍ”および“Ｓ”を付加する。
【００９７】
まず、通信端末Ｓの制御部２４Ｓは、任意の暗号鍵を生成し、設定管理情報ファイル２５１Ｓを読み出し、「共通鍵」アイテムの値を生成した暗号鍵（以下、「Key-2」と呼ぶ）で更新する（ステップＳ２１７）。この暗号鍵は文字、数字および記号の列であり、乱数関数により生成される。乱数関数については既に多くの既知のものがあるため、ここでの説明は省略する。
【００９８】
次に制御部２４Ｓは自機プロトコル情報ファイル２５３Ｓを読み出し、全レコードの「MACアドレス」フィールドおよび「プロトコルセット」フィールドの値（以下、「プロトコルセット・テーブルS」と呼ぶ）を各レコードにおける対応関係を維持したままで取り出す。プロトコルセット・テーブルSは通信端末Ｓが無線通信部２１Ｓを用いた通信を行う際に利用可能なプロトコルセットに関する案内情報である。続いて制御部２４Ｓはプロトコルセット・テーブルSと、ステップＳ２１７で生成したKey-2を通信端末Ｍに送信する（ステップＳ２１８）。通信端末Ｍの制御部２４ＭはプロトコルセットテーブルSおよびKey-2を受信すると、他機プロトコル情報ファイル２５４Ｍを読み出し、他機プロトコル情報ファイル２５４Ｍの各レコードの「MACアドレス」フィールドおよび「プロトコルセット」フィールドの値を、プロトコルセット・テーブルSの各レコードの「MACアドレス」フィールドおよび「プロトコルセット」フィールドの値で更新する。更に、設定管理情報ファイル２５１Ｍを読み出し、「共通鍵」アイテムの値をKey-2で更新する（ステップＳ２１９）。
【００９９】
次に制御部２４Ｍは自機プロトコル情報ファイル２５３Ｍおよび他機プロトコル情報ファイル２５４Ｍを読み出し、それぞれの「プロトコルセット」フィールドに共通する値が存在するか否かの判定をする（ステップＳ２２０）。自機プロトコル情報ファイル２５３Ｍの「プロトコルセット」フィールドと他機プロトコル情報ファイル２５４Ｍの「プロトコルセット」フィールドの両方に同じプロトコルセットの名称を示す値が存在する場合には、制御部２４Ｍはステップ２２０で「Ｙｅｓ」を得る。同じプロトコルセットが存在しない場合には、制御部２４Ｍはステップ２２０で「Ｎｏ」を得る。
【０１００】
ステップＳ２２０で「Ｎｏ」を得ると、制御部２４Ｍは通信不成立通知を通信端末Ｓに送信する。また制御部２４Ｍは、無線通信の設定が不可能であることを通知するメッセージを表示部２３Ｍに表示する（ステップＳ２２１）。このステップを経た場合、制御部２４Ｍの動作は終了する。
通信端末Ｓの制御部２４Ｓは、通信端末Ｍより通信不成立通知を受信すると、無線通信の設定が不可能であることを通知するメッセージを表示部２３Ｓに表示する（ステップＳ２２２）。このステップを経た場合、制御部２４Ｓの動作は終了する。なお、ステップＳ２２０からステップＳ２２２までの動作を以下、「通信可能確認作業」と呼ぶ。
【０１０１】
ステップＳ２２０で「Ｙｅｓ」を得た場合、制御部２４Ｍは、自機プロトコル情報ファイル２５３Ｍの全てのレコードの中から、「プロトコルセット」フィールドに含まれる値が

他機プロトコル情報ファイル２５４Ｍのいずれかのレコードの「プロトコルセット」フィールドの値と一致するレコードを抽出する。自機プロトコル情報ファイル２５３Ｍから複数のレコードが抽出された場合、制御部２４Ｍは抽出されたレコードの「優先順位」フィールドの値を比較し、「優先順位」フィールドの値が最も小さいレコードを選択する。一つのレコードのみが抽出された場合、制御部２４Ｍはそのレコードを選択する。次に、制御部２４Ｍは決定プロトコル情報ファイル２５５Ｍを読み出し、その唯一のレコードの「自機MACアドレス」フィールドの値を選択されたレコードの「MACアドレス」フィールドの値（以下、「MAC-M」と呼ぶ）で、「プロトコルセット」フィールドの値を選択されたレコードの「プロトコルセット」フィールドの値（以下、「決定プロトコルセット２」と呼ぶ）で更新する。続いて、制御部２４Ｍは他機プロトコル情報ファイル２５４Ｍの全てのレコードの中から、「プロトコルセット」フィールドの値が決定プロトコルセット２と一致するレコードを検索し、決定プロトコル情報ファイル２５５Ｍの「他機MACアドレス」フィールドの値を検索されたレコードの「MACアドレス」フィールドの値（以下、「MAC-S」と呼ぶ）で更新する（ステップＳ２２３）。

【０１０２】

次に、制御部２４Ｍはステップ２２３において選択された自機プロトコル情報ファイル２５３Ｍのレコードの「パラメータセット」フィールドの値に基づいて、通信端末Ｓが通信端末Ｍと決定プロトコルセット２の示すプロトコルセットを用いて無線通信を行うために変更の必要な通信パラメータの値を決定する（ステップＳ２２４）。以下、通信端末Ｍ用のパラメータセットを「パラメータセットＭ」、通信端末Ｓ用のパラメータセットを「パラメータセットＳ」と呼ぶ。

【０１０３】

ステップＳ２２４におけるパラメータセットの決定動作について、例を挙げて説明する。例えば、今、決定プロトコルセット２が“IEEE802.11b - TCP/IP”を示し、自機プロトコル情報ファイル２５３Ｍの「プロトコルセット」の値が“IEEE802.11b - TCP/IP”を示すレコードの「パラメータセット」フィールドの値が、

パラメータ１　“IEEE802.11b: モード＝Infrastructure”
パラメータ２　“IEEE802.11b: チャンネルID＝３”
パラメータ３　“IPアドレス / サブネットマスク＝192.168.0.220 / 255.255.255.0”

であったとする。この場合、制御部２４Ｍはパラメータセットとして、Ｍ

パラメータ１　“IEEE802.11b: モード＝Ad Hoc”
パラメータ２　“IEEE802.11b: チャンネルID＝５”

を決定する。また、パラメータセットＳとして、

パラメータ１　“IEEE802.11b: モード＝Ad Hoc”
パラメータ２　“IEEE802.11b: チャンネルID＝５”
パラメータ３　“IPアドレス / サブネットマスク＝192.168.0.221 / 255.255.255.0”

を決定する。ここで、InfrastructureモードはIEEE802.11bにおいて規定されているアクセスポイントを中継する通信形態を、またAd HocモードはIEEE802.11bにおいて規定されているピア・トゥ・ピアの通信形態を指す。

【０１０４】

通信端末Ｍは、元の設定ではIEEE802.11において、Infrastructureモードを用いている。無線通信システム２においては１対１の無線通信が行われることから、制御部２４ＭはIEEE802.11bの通信モードとしてAd Hocモードを選定している。また、通信端末Ｍは元の設定ではIEEE802.11bのチャンネルIDとして３を用いている。チャンネルID３は通信端末Ｍが元の設定で属していた無線通信網における周波数であり、無線通信システム２においてこれを用いると周波数の衝突が生ずるので、制御部２４Ｍは３以外の未使用なチャンネルIDとして５を選定している。

また、TCP/IPのパラメータに関しては、通信端末Ｍは元の設定ではIPアドレスとして192.168.0.220、サブネットマスクとして255.255.255.0を用いている。ここで通信端末ＭのIPアドレスおよびサブネットマスクを変更する必要はないので、通信端末Ｍ用のパラメータ

セットにはIPアドレス / サブネットマスクに関するパラメータが含まれていない。一方、通信端末ＳのIPアドレスおよびサブネットマスクは通信端末Ｍと同じネットワークに属し、異なるアドレスを示すものである必要があるので、制御部２４Ｍは通信端末Ｓ用のパラメータとして、IPアドレスとして192.168.0.221、またサブネットマスクとして 255.255.255.0を選定している。

【０１０５】

ステップＳ２２４においてパラメータセットＭおよびパラメータセットＳを決定した後、まず制御部２４Ｍは決定プロトコル情報ファイル２５５Ｍを読み出し、その唯一のレコードの「パラメータセット」フィールドの値をパラメータセットＭで更新する。続いて、制御部２４Ｍはそのレコードの「自機MACアドレス」フィールドの値、すなわちMAC-M、および「プロトコルセット」フィールドの値、すなわち決定プロトコルセット２を取り出し、MAC-M、決定プロトコルセット２およびパラメータセットＳを通信端末Ｓに送信する（ステップＳ２２５）。これらの情報は通信端末Ｓが無線通信部２１Ｓを用いて通信端末Ｍと通信を行うための通信パラメータである。

【０１０６】

制御部２４ＳはMAC-M、決定プロトコルセット２およびパラメータセットＳを通信端末Ｍから受信すると、決定プロトコル情報ファイル２５５Ｓを読み出し、唯一のレコードの「他機MACアドレス」フィールドの値をMAC-M、「プロトコルセット」フィールドの値を決定プロトコルセット２、「パラメータセット」フィールドの値をパラメータセットＳで更新する。続いて、制御部２４Ｓは自機プロトコル情報ファイル２５３Ｓを読み出し、その全レコードから「プロトコルセット」フィールドの値が決定プロトコルセット２と一致するレコードを検索し、検索されたレコードの「MACアドレス」フィールドの値、すなわちMAC-Sを取りだし、決定プロトコル情報ファイル２５５Ｓの唯一のレコードの「自機MACアドレス」フィールドの値をMAC-Sで更新する（ステップＳ２２６）。

【０１０７】

以下の動作は通信端末Ｍと通信端末Ｓのそれぞれにおいて並行して行われ、通信端末Ｍと通信端末Ｓとは同じ動作をする。従って、ここでは通信端末Ｍの動作のみを説明する。通信端末Ｓの動作については、以下の説明における符号ＭとＳとを入れ替えることにより、その説明が得られる。

【０１０８】

制御部２４Ｍは決定プロトコル情報ファイル２５５Ｍを読み出し、その唯一のレコードの「プロトコルセット」フィールドの値、すなわち決定プロトコルセット２および「パラメータセット」フィールドの値、すなわちパラメータセットＭを無線通信部２１Ｍに送信する。無線通信部２１Ｍは決定プロトコルセット２およびパラメータセットＭを受信すると、不揮発性メモリに記憶されている、決定プロトコルセット２が示す通信プロトコルセットに関する通信パラメータを、パラメータセットＭに基づいて変更する。なお、この変更を終えた無線通信部２１Ｍは、設定終了を制御部２４Ｍに通知する（ステップＳ２２７）。

【０１０９】

設定終了の通知を無線通信部２１Ｍより受信すると、制御部２４Ｍは設定完了通知を通信端末Ｓに送信する（ステップＳ２２８）。

【０１１０】

ここで、以下の動作で通信端末Ｓが通信端末Ｍに対して行う割り込み処理要求について説明する。上述のとおり、通信端末Ｍはステップ２２８において、通信端末Ｓに対し設定完了通知を送信するが、同様に通信端末Ｓは通信端末Ｍに対し設定完了通知を送信する。この設定完了通知を受信すると、制御部２４Ｍは、それまでの処理を一時停止し、設定管理情報ファイル２５１Ｍを読み出し、「設定完了通知フラグ」アイテムの値を“ON”で更新した後、一時停止した前記処理を再開する。

【０１１１】

ステップＳ２２８において設定完了通知を送信した後、制御部２４Ｍは設定管理情報ファ

イル２５１Ｍを読み出し、「設定完了通知フラグ」アイテムの値が“ON”であるか否かを判定する（ステップＳ２２９）。この時点で、通信端末Ｍが通信端末Ｓより既に設定完了通知を受信している場合、制御部２４Ｍはステップ２２９の判定結果として「Ｙｅｓ」を得る。通信端末Ｍが通信端末Ｓより設定完了通知を受信していない場合、制御部２４Ｍはステップ２２９の判定結果として「Ｎｏ」を得る。
ステップＳ２２９において、「Ｎｏ」を得た場合、制御部２４Ｍは予め定められた短時間、例えば１秒間だけ待機した後、ステップＳ２２９に制御を戻す（ステップＳ２３０）。この動作はステップＳ２２９において、「設定完了通知フラグ」の値が“OFF”である限り繰り返される。この間、通信端末Ｍは通信端末Ｓから送信されてくるべき設定完了通知の待ち状態にある。

【０１１２】
ステップＳ２２９において、「Ｙｅｓ」を得た場合、制御部２４Ｍは、無線通信の設定が完了したことを通知するメッセージを表示部２３Ｍに表示する（ステップＳ２３１）。

【０１１３】
ステップＳ２３１において表示されたメッセージにより、無線通信のパラメータ設定が完了したことを確認した通信端末Ｍおよび通信端末Ｓのユーザは、有線通信部２０Ｍと有線通信部２０Ｓとの接続を解除できる。
以上の動作により、通信端末Ｍおよび通信端末Ｓは決定プロトコルセット２を用いて、無線通信部２１Ｍおよび無線通信部２１Ｓを用いた１対１の無線通信を行うことができるようになる。

【０１１４】
［２．２．４］共通鍵を用いた通信方法
上記の通信パラメータ設定段階を終えた後、通信端末Ｃ３および通信端末Ｄ４は無線通信システム２における１対１の無線通信を行う際、その通信情報を共通鍵を用いて暗号化および復号化する。以下、その通信動作を説明する。なお、以下は通信端末Ｃ３が通信端末Ｄ４に情報を送信する場合について説明するが、通信端末Ｃ３および通信端末Ｄ４の立場が逆となってもよい。

【０１１５】
通信端末Ｃ３が通信端末Ｄ４に情報を送信する必要が生じると、まず制御部２４Ｃは決定プロトコル情報ファイル２５５Ｃを読み出し、送信先である通信端末Ｄ４のMACアドレス（以下、「MAC-D」と呼ぶ）を、決定プロトコル情報ファイル２５５Ｃの唯一のレコードの「他機MACアドレス」フィールドの値と比較する。この比較は情報の送信先が無線通信システム２において確立されている１対１の無線通信の相手の通信端末であることの確認作業である。この比較において２つの値が一致すると、制御部２４Ｃは設定管理情報ファイル２５１Ｃを読み出し、「共通鍵」アイテムの値、すなわちKey-2で通信端末Ｄ４に送信する情報を暗号化する。次に制御部２４Ｃは決定プロトコル情報ファイル２５５Ｃの唯一のレコードの「プロトコルセット」フィールドの値が示す通信プロトコルセットに従って、暗号化した情報をフォーマットする。続いて制御部２４Ｃは決定プロトコル情報ファイル２５５Ｃの唯一のレコードの「自機MACアドレス」フィールドの値（以下、「MAC-C」と呼ぶ）を取り出し、フォーマットした情報に送信先を示すMAC-Dおよび送信元を示すMAC-Cを付加し、無線通信部２１Ｃを介してその情報を通信端末Ｄ４に送信する。

【０１１６】
通信端末Ｄ４の制御部２４Ｄは無線通信部２１Ｄを介して、通信端末Ｃ３から暗号化された情報を受信すると、まず制御部２４Ｄは受信した情報から送信元のMACアドレス、すなわちMAC-Cを取り出す。続いて制御部２４Ｄは決定プロトコル情報ファイル２５５Ｄを読み出し、MAC-Cを、その唯一のレコードの「他機MACアドレス」フィールドの値と比較する。この比較は情報の送信元が無線通信システム２において確立されている１対１の無線通信の相手の通信機器であることの確認作業である。この比較において２つの値が一致すると、制御部２４Ｄは設定管理情報ファイル２５１Ｄを読み出し、「共通鍵」アイテムの値、すなわちKey-2で受信した情報を復号化する。

【０１１７】
［２．３］第２実施形態の効果
第２実施形態においては、各通信端末のユーザは通信端末の有線通信部を直接接触させる、という直感的に理解可能な方法によって無線通信のパラメータ設定を行うことができ、その他、アプリケーションソフトを起動する等の手間を要しない。これはユーザにとっての通信パラメータ設定準備作業を大幅に軽減する。
【０１１８】
第２実施形態において、通信パラメータ設定時に無線通信のユーザが行うべきことは、ユーザが自分で任意に登録したパスワードの入力のみである。これはユーザにとっての通信パラメータ設定作業を大幅に軽減する。なお、この通信パラメータ設定においては、いずれかの通信端末において優先度が高く設定されている通信プロトコルが自動的に選択されるため、設定が自動化されたために不適当な通信プロトコルが選択されて通信効率が落ちる、といったことはない。
【０１１９】
第２実施形態において実現される無線通信システム２においては、通信端末間の情報は全て暗号化されるため、部外者の無線機器がその情報を受信した場合においても、その情報の内容の漏洩を防ぐことができる。暗号化は既によく知られた技術であるが、共通鍵を用いる方法は公開鍵を用いる方法と比べてスピードの速い情報の暗号化および復号化が可能である一方で、共通鍵の盗用の危険性がある。しかしながら、無線通信システム２においては通信端末が直接接続されることによりこの共通鍵が受け渡されるため、効率的な共通鍵による暗号技術を安全に用いることができる。
【０１２０】
［３］第３実施形態
［３．１］第３実施形態の構成
［３．１．１］無線通信システムの構成
本発明の第３実施形態においては、本発明の通信パラメータ設定方法により、複数の通信機器を含む既に稼働している無線通信網に対し新たに通信機器が無線接続し、この新たに参加する通信機器がこの無線通信網に含まれる複数の通信機器と通信を行うことが可能となる。図１８に本発明の第３実施形態における通信パラメータ設定段階の状態と通信パラメータ設定後の状態を示す。本発明の第３実施形態により実現される通信パラメータ設定後の無線通信システムを以下、「無線通信システム３」と呼ぶ。
第３実施形態においては、通信端末Ｆ６、通信端末Ｇ７および通信端末Ｈ８が既に無線通信で互いに接続されており、通信端末Ｅ５が通信端末Ｆ６とケーブルにより接続されることにより、新たに通信端末Ｅ５が通信端末Ｆ６、通信端末Ｇ７および通信端末Ｈ８と無線通信を行うことができるようになる。
第３実施形態においては、通信端末Ｅ５のユーザが通信端末Ｅ５の操作部を用いて通信パラメータ設定の開始指示を行うことにより、通信端末Ｅ５が無線通信システム３における通信のための通信パラメータの決定を要求する側の通信機器、通信端末Ｆ６が通信パラメータの決定を行う側の通信機器となる。これにより、通信端末Ｆ６は通信端末Ｅ５が無線通信システム３における無線通信を行うための通信パラメータを決定し、その決定された通信パラメータを通信端末Ｅ５に送信する。通信端末Ｅ５は通信端末Ｆ６から通信パラメータを受信し、受信した通信パラメータに基づいて自分の通信パラメータを変更する。なお、第３実施形態においては第２実施形態と同様に、TCP/IP等の中位レイヤに関する通信プロトコルのパラメータ設定も併せて行う。
【０１２１】
［３．１．２］通信端末の構成
［３．１．２．１］有線通信部を有する通信端末の構成
第３実施形態において、通信端末Ｅ５は通信端末Ｆ６とケーブルで接続されることにより、他の通信端末と無線通信が可能となる。図１９を用いて通信端末Ｅ５の構成を説明する。なお、通信端末Ｆ６の構成は通信端末Ｅ５のものと同じであるので、通信端末Ｆ６の説

明は省略する。

【０１２２】

通信端末Ｅ５は有線通信部２７、無線通信部２８、操作部２９、表示部３０、制御部３１および記憶部３２を備えている。これらの構成要素はバス３３を介して電気的に接続されている。

【０１２３】

無線通信部２８、操作部２９、表示部３０、制御部３１の機能および構成は第２実施形態における通信端末Ｃ３の無線通信部２１、操作部２２、表示部２３、制御部２４のものとそれぞれ同様であるので、説明を省略する。また、記憶部３２の機能も第２実施形態における通信端末Ｃ３の記憶部２５のものと同様であるので、説明を省略する。

【０１２４】

有線通信部２７の機能は第２実施形態における通信端末Ｃ３の有線通信部２０と同様であるが、その形状は直接接続ではなく、ケーブル接続が可能な形状をしている。

【０１２５】

記憶部３２は、設定管理情報ファイル３２１、端末情報ファイル３２２、自機プロトコル情報ファイル３２３、他機プロトコル情報ファイル３２４、決定プロトコル情報ファイル３２５、識別子情報ファイル３２６および公開鍵情報ファイル３２７を記憶し、また作業領域３２８を有している。

【０１２６】

端末情報ファイル３２２、他機プロトコル情報ファイル３２４および作業領域３２８の構成に関しては第２実施形態における通信端末Ｃ３の端末情報ファイル２５２、他機プロトコル情報ファイル２５４および作業領域２５６のものと同様であるので、説明を省略する。

【０１２７】

図２０は設定管理情報ファイル３２１の構成を例示したものである。設定管理情報ファイル３２１は「自機識別子」アイテム、「パスワード」アイテム、「秘密鍵」アイテム、「公開鍵」アイテムを持つ。「自機識別子」アイテムおよび「パスワード」アイテムの機能は第２実施形態における通信端末Ｃ３の設定管理情報ファイル２５１のものと同様である。「秘密鍵」アイテムは、無線通信システム３において通信端末Ｅ５が通信端末Ｅ５以外の通信端末から暗号化された通信情報を受信する際、その通信情報を復号化するための暗号鍵情報を含む。「公開鍵」アイテムは、無線通信システム３において通信端末Ｅ５以外の通信端末が通信端末Ｅ５に対し情報を送信する際、その通信情報を暗号化するための暗号鍵情報を含む。「秘密鍵」アイテムの値と「公開鍵」アイテムの値は１対をなし、「公開鍵」アイテムの値によって暗号化された情報は「秘密鍵」アイテムの値によってのみ、復号化される。

【０１２８】

図２１は自機プロトコル情報ファイル３２３の構成を例示したものである。自機プロトコル情報ファイル３２３の構成は第２実施形態における通信端末Ｃ３の自機プロトコル情報ファイル２５３とほぼ同様であるが、「優先順位」フィールドは不要なため、持っていない。

【０１２９】

図２２は決定プロトコル情報ファイル３２５の構成を例示したものである。決定プロトコル情報ファイル３２５の構成は第２実施形態における通信端末Ｃ３の決定プロトコル情報ファイル２５５とほぼ同様であるが、通信端末Ｅ５と通信端末Ｆ６とが共通して利用可能な通信プロトコルセットの数と等しい数のレコードを持ち、それぞれのレコードは１つの通信プロトコルセットに対応した情報の集まりである。

【０１３０】

図２３は識別子情報ファイル３２６の構成を例示したものである。識別子情報ファイル３２６は今までに通信端末Ｅ５が無線通信システム３における通信を行ったことがある相手の通信端末のMACアドレスおよび識別子を記憶する。識別子情報ファイル３２６は今まで

に通信端末Ｅ５が無線通信システム３における通信を行ったことがある通信端末のMACアドレスの数と等しい数のレコードを持ち、各レコードは「MACアドレス」フィールドと「識別子」フィールドを持つ。「MACアドレス」フィールドは対象の通信端末のMACアドレスを含み、「識別子」フィールドは対象の通信端末の識別子を含む。１つの通信端末が複数のMACアドレスを持つ場合、それら複数のMACアドレスに対応するレコードにおける「識別子」フィールドの値は等しい。

【０１３１】

図２４は公開鍵情報ファイル３２７の構成を例示したものである。公開鍵情報ファイル３２７は今までに通信端末Ｅ５が無線通信システム３における通信を行ったことがある相手の通信端末の公開鍵情報を記憶する。公開鍵情報ファイル３２７は今までに通信端末Ｅ５が無線通信システム３における通信を行ったことがある通信端末の数と等しい数のレコードを持ち、各レコードは「識別子」フィールドと「公開鍵」フィールドを持つ。「識別子」フィールドは対象の通信端末の識別子を含み、「公開鍵」フィールドは対象の通信端末の公開鍵情報を含む。

【０１３２】

［３．１．２．２］有線通信部を有さない通信端末の構成

第３実施形態において、通信端末Ｇ７および通信端末Ｈ８は通信端末Ｅ５とケーブルで接続されることはなく、それらの構成は通信端末Ｅ５および通信端末Ｆ６の構成と異なる。図２５を用いて通信端末Ｇ７の構成を説明する。通信端末Ｈ８の構成は通信端末Ｇ７のものと同じであるので、通信端末Ｈ８の説明は省略する。

【０１３３】

通信端末Ｇ７は無線通信部３４、操作部３５、表示部３６、制御部３７および記憶部３８を備えている。これらの構成要素はバス３９を介して電気的に接続されている。

【０１３４】

無線通信部３４、操作部３５、表示部３６、制御部３７の機能および構成は第２実施形態における通信端末Ｃ３の無線通信部２１、操作部２２、表示部２３、制御部２４のものと同様であるので、説明を省略する。また、記憶部３８の機能も第２実施形態における通信端末Ｃ３の記憶部２５のものと同様であるので、説明を省略する。

【０１３５】

記憶部３８は、設定管理情報ファイル３８１、識別子情報ファイル３８２および公開鍵情報ファイル３８３を記憶し、また作業領域３８４を有している。

【０１３６】

識別子情報ファイル３８２および公開鍵情報ファイル３８３の構成に関しては通信端末Ｅ５の識別子情報ファイル３２６および公開鍵情報ファイル３２７のものと同様であるので、説明を省略する。また、作業領域３２８の構成に関しては、第２実施形態における通信端末Ｃ３の作業領域２５６のものと同様であるので、説明を省略する。

【０１３７】

図２６は設定管理情報ファイル３８１の構成を例示したものである。設定管理情報ファイル３８１は「自機識別子」アイテム、「秘密鍵」アイテムおよび「公開鍵」アイテムを持つ。「自機識別子」アイテムの機能は第２実施形態における通信端末Ｃ３の設定管理情報ファイル２５１のものと同様である。「秘密鍵」アイテムおよび「公開鍵」アイテムの機能は通信端末Ｅ５の設定管理情報ファイル３２１のものと同様である。

【０１３８】

［３．２］第３実施形態の動作

第３実施形態において、無線通信システム３を実現するための通信パラメータ設定動作および通信パラメータ設定後の通信動作を説明する。通信パラメータ設定は接続認証段階およびパラメータ設定段階から成る。以下の説明において、通信端末Ｅ５、通信端末Ｆ６、通信端末Ｇ７の同種の構成要素を区別するために、各構成要素を特定する符号に“Ｅ”、“Ｆ”、“Ｇ”を付加する。

なお、以下の接続認証段階およびパラメータ設定段階において、通信端末Ｅ５と通信端末

Ｆ６の間で行われる情報の送受信は全て有線通信部２７Ｅおよび有線通信部２７Ｆを介して行われる。

【０１３９】

［３．２．１］接続認証段階

まず、通信端末Ｆ６は通信端末Ｅ５の接続要求に応じて、通信端末Ｅ５が自分の通信端末に接続することの認証作業を行う。以下、図２７を用いてその動作説明を行う。

【０１４０】

はじめに、通信端末Ｅ５および通信端末Ｆ６のユーザは接続ケーブルの一端をそれぞれ有線通信部２７Ｅおよび有線通信部２７Ｆに接続する。有線通信部２７Ｅと有線通信部２７Ｆが接続ケーブルによって電気的に導通すると、制御部３１Ｅおよび制御部３１Ｆは有線通信部２７Ｅおよび有線通信部２７Ｅを介してこの接続を検知する（ステップＳ３０１）。

【０１４１】

制御部３１Ｅは次にパスワード照合作業を行う。パスワード照合作業は第２実施形態におけるステップＳ２０６からステップＳ２０８とほぼ同様であるので、詳細な説明を省略する（ステップＳ３０２からステップＳ３０４）。ただし、ステップＳ３０２において表示部３０Ｅに表示されるメッセージは、新たに無線通信網に参加する通信端末側のユーザのみ、パスワード入力を行うように指示する。このパスワード入力は、正しいユーザが通信端末Ｅ５の無線通信網への接続を試みていることを確認すると同時に、通信端末Ｅ５の相手の通信端末が以下の動作において通信パラメータの決定を行うことを通信端末Ｅ５に指示するための動作である。

通信端末Ｆ６の制御部３１Ｆは、ステップＳ３０１に続き制御部３１Eと同様のパスワード入力要求のメッセージ表示（ステップＳ３０２）を行うが、通信端末Ｆ６は新たに無線通信網に参加する通信端末ではないので、通信端末Ｆ６のユーザはパスワードを入力せず、従って制御部３１Ｆはパスワード照合作業のステップＳ３０３およびステップＳ３０４を行わない。

【０１４２】

ステップＳ３０４において、２つのパスワードが一致した場合、制御部３１Ｅは設定管理情報ファイル３２１Ｅおよび自機プロトコル情報ファイル３２３Ｅを読み出し、まず設定管理情報ファイル３２１Ｅの「自機識別子」アイテムの値（以下、「ID-E」と呼ぶ）を取り出す。次に制御部３１Ｅは自機プロトコル情報ファイル３２３Ｅの全レコードの「MACアドレス」フィールドおよび「プロトコルセット」フィールドの値（以下、「プロトコルセット・テーブルE」と呼ぶ）を各レコードにおける対応関係を維持したままで取り出す。プロトコルセット・リストＥは通信端末Ｅ５が無線通信部２８Ｅを用いた通信を行う際に利用可能なプロトコルに関する案内情報である。次に、制御部３１ＥはID-Eおよびプロトコルセット・テーブルEを通信端末Ｆ６に送信する（ステップＳ３０５）。ステップＳ３０５を終えた制御部３１Ｅは制御を後述のステップＳ３１４に移す。

【０１４３】

通信端末Ｆ６の制御部３１ＦはID-Eおよびプロトコルセット・テーブルＥを受信すると、まず設定管理情報ファイル３２１Ｆを読み出し、「他機識別子」アイテムの値をID-Eで更新する。続いて、制御部３１Ｆは他機プロトコル情報ファイル３２４Ｆを読み出し、その各レコードの「MACアドレス」フィールドおよび「プロトコルセット」フィールドの値をプロトコルセット・テーブルEの各レコードの「MACアドレス」フィールドおよび「プロトコルセット」フィールドの値でそれぞれ更新する（ステップＳ３０６）。

【０１４４】

通信端末Ｆ６は次に識別子登録作業を行う。識別子登録作業は第２実施形態におけるステップＳ２０５からステップＳ２０９と同様であるので、説明を省略する（ステップＳ３０７からステップＳ３１１）。ステップＳ３１１を終えた制御部３１Ｆは制御を後述のステップＳ３１２に移す。

【０１４５】

［３．２．２］パラメータ設定段階
上記の接続認証段階を終えた後、通信端末Ｆ６は通信端末Ｅ５が無線通信のために必要とする通信パラメータの決定を行い、通信端末Ｅ５は通信端末Ｆ６により決定されたパラメータに従い、パラメータの設定を行う。以下、図２８を用いてその動作説明を行う。
【０１４６】
まず、通信端末Ｅ５および通信端末Ｆ６は通信可能確認作業を行う。通信可能確認作業は第２実施形態におけるステップＳ２２０からステップＳ２２２と同様であるので、説明を省略する（ステップＳ３１２からステップＳ３１４）。ただし、この通信可能確認作業において、通信端末Ｅ５および通信端末Ｆ６はそれぞれ第２実施形態における通信端末Ｓおよび通信端末Ｍにあたる。
【０１４７】
ステップＳ３１２において、自機プロトコル情報ファイル３２３Ｆの「プロトコルセット」フィールドと他機プロトコル情報ファイル３２４Ｆの「プロトコルセット」フィールドの両方に同じプロトコルセットの名称を示す情報が存在し、判定結果として「Ｙｅｓ」を得た場合、制御部３１Ｆは自機プロトコル情報ファイル３２３Ｆの全てのレコードの中から、「プロトコルセット」フィールドの値が他機プロトコル情報ファイル３２４Ｆの「プロトコルセット」フィールドの値のいずれかと一致するものを抽出する。この場合、複数のレコードが抽出されてもよい。続いて、制御部３１Ｆは決定プロトコル情報ファイル３２５Ｆを読み出し、その各レコードの「自機MACアドレス」フィールドの値および「プロトコルセット」フィールドの値を、抽出された各レコードの「MACアドレス」フィールドの値（以下、「MAC-List-F」と呼ぶ）および「プロトコルセット」フィールドの値（以下、「決定プロトコルセット・リスト３」と呼ぶ）でそれぞれ更新する。続いて制御部３１Ｆは決定プロトコル情報ファイル３２５Ｆの「他機MACアドレス」フィールドの値を更新するために、決定プロトコル情報ファイル３２５Ｆの各レコードに関して以下の動作を行う。まず制御部３１Ｆは他機プロトコル情報ファイル３２４Ｆの全レコードの中から、その「プロトコルセット」フィールドの値が対象のレコードの「プロトコルセット」フィールドの値と一致するレコードを検索する。次に、制御部３１Ｆは決定プロトコル情報ファイル３２５Ｆの対象のレコードの「他機MACアドレス」フィールドの値を、検索されたレコードの「MACアドレス」フィールドの値で更新する（ステップＳ３１５）。
【０１４８】
次に、制御部３１Ｆは決定プロトコル情報ファイル３２５Ｆを読み出し、全レコードに関し次の動作を行う。制御部３１Ｆは自機プロトコル情報ファイル３２３Ｆを読み出し、その全レコードの中から、その「プロトコルセット」フィールドの値が、決定プロトコル情報ファイル３２５Ｆの対象のレコードの「プロトコルセット」フィールドの値と一致するレコードを検索する。次に、制御部３１Ｆは検索されたレコードの「パラメータセット」フィールドの値に基づいて、通信端末Ｅ５が他の通信端末と対象のレコードの「プロトコルセット」フィールドの値が示すプロトコルセットを用いて無線通信を行うために変更の必要な通信パラメータを決定する。次に、制御部３１Ｆは決定プロトコル情報ファイル３２５Ｆの対象のレコードの「パラメータセット」フィールドの値を、決定した通信パラメータで更新する（ステップＳ３１６）。以下、ステップＳ３１６において決定された通信端末Ｅ５用の複数の通信パラメータセットを「パラメータセット・リストE」と呼ぶ。
【０１４９】
ステップＳ３１６におけるパラメータセットの決定動作について、例を挙げて説明する。今、決定プロトコルセット・リスト３が「IEEE802.11b - TCP/IP」と「Bluetooth - NetBEUI」の２つの値を持ち、自機プロトコル情報ファイル３２３Ｆの「プロトコルセット」フィールドの値が「IEEE802.11b - TCP/IP」および「Bluetooth - NetBEUI」であるレコードの「パラメータセット」フィールドの値がそれぞれ以下の通りであったとする。
「IEEE802.11b - TCP/IP」
パラメータ１　「IEEE802.11b: モード＝Ad Hoc」
パラメータ２　「IEEE802.11b: チャンネルID＝３」

パラメータ３　「IPアドレス / サブネットマスク＝192.168.0.220 / 255.255.255.0」
「Bluetooth - NetBEUI」
パラメータ１　「Bluetooth: PIN Code＝4E63」
この場合、制御部３１Ｆはパラメータセット・リストEとして、
「IEEE802.11b - TCP/IP」
パラメータ１　「IEEE802.11b: モード＝Ad Hoc」
パラメータ２　「IEEE802.11b: チャンネルID＝３」
パラメータ３　「IPアドレス / サブネットマスク＝192.168.0.222 / 255.255.255.0」
「Bluetooth - NetBEUI」
パラメータ１　「Bluetooth: PIN Code＝4E63」
を決定する。ここで、PIN CodeはBluetoothにおいて規定されている接続認証用のPersonal Identification Number Codeのことである。

【０１５０】

まず、通信端末Ｆ６の属する無線通信網においては、IEEE802.11bがTCP/IPとの組み合わせで用いられている。この無線通信網においては、まずIEEE802.11bに関して、通信モードとしてAd Hocモード、チャンネルIDとして３が用いられている。これらのパラメータはこの無線通信網に参加する通信機器において同じである必要があるので、制御部３１Ｆはパラメータセット・リストEにこれらのコピーを追加している。またTCP/IPに関して、この無線通信網においては、IPアドレスとして192.168.0.xxx（xxxは255以下の正の整数）、サブネットマスクとして255.255.255.0が用いられている。制御部３１Ｆは通信端末Ｆ６のIPアドレスに隣接するIPアドレスが既に使用されていないかを無線通信網にブロードキャストすることにより確認し、通信端末Ｅ５用の未使用のIPアドレス／サブネットマスクとして192.168.0.222 / 255.255.255.0をパラメータセット・リストEに追加している。また、この無線通信網においては、BluetoothがNetBEUIとの組み合わせで用いられている。Bluetoothにおいては同じ通信網内の全ての通信機器が同じPIN Codeを用いる必要があるので、制御部３１Ｆはこれをパラメータセット・リストEに追加している。NetBEUIに関しては、この例においては設定変更を必要としていないので、制御部３１Ｆはプロトコルセット・リストＥに何も追加していない。

【０１５１】

ステップＳ３１６においてパラメータセット・リストEを決定した後、制御部３１Ｆは決定プロトコル情報ファイル３２５Ｆを読み出し、全レコードの「自機MACアドレス」フィールドの値、すなわちMAC-List-F、「プロトコルセット」フィールドの値、すなわち決定プロトコルセット・リスト３、「パラメータセット」フィールドの値、すなわちパラメータセット・リストEを通信端末Ｅ５に送信する（ステップＳ３１７）。これらの情報は通信端末Ｅ５が無線通信部２８Ｅを用いて他の通信端末と通信を行うための通信パラメータである。

【０１５２】

制御部３１ＥはMAC-List-F、決定プロトコルセット・リスト３およびパラメータセット・リストEを通信端末Ｆ６から受信すると、決定プロトコル情報ファイル３２５Ｅを読み出し、「他機MACアドレス」フィールドの値、「プロトコルセット」フィールドの値および「パラメータセット」フィールドの値をそれぞれMAC-List-F、決定プロトコルセット・リスト３およびパラメータセット・リストEで更新する（ステップＳ３１８）。

【０１５３】

続いて、制御部３１Ｅは決定プロトコル情報ファイル３２５Ｅの全レコードの「プロトコルセット」フィールドの値および「パラメータセット」フィールドの値を無線通信部２８Ｅに送信する。無線通信部２８Ｅはこれらの情報を受信すると、不揮発性メモリに記憶されている、「プロトコルセット」フィールドの値が示す通信プロトコルセットに関する通信パラメータを、「パラメータセット」フィールドの値が示す情報に基づいて変更する。なお、この変更を終えた無線通信部２８Ｅは、設定終了を制御部３１Ｅに通知する（ステップＳ３１９）。

【０１５４】
設定終了の通知を無線通信部２８Ｅより受信すると、制御部３１Ｅは設定完了通知を通信端末Ｆ６に送信し（ステップＳ３２０）、通信端末Ｆ６の制御部３１Ｆは設定完了通知を通信端末Ｅ５から受信する（ステップＳ３２１）。
ステップＳ３２０を終えた後、制御部３１Ｅは無線通信の設定が完了したことを通知するメッセージを表示部３０Ｅに表示する（ステップＳ３２２）。同様に、ステップＳ３２１を終えた後、制御部３１Ｆは無線通信の設定が完了したことを通知するメッセージを表示部３０Ｆに表示する（ステップＳ３２３）。
【０１５５】
ステップＳ３２２およびステップＳ３２３において表示されたメッセージにより、パラメータ設定が完了したことを確認した通信端末Ｅ５および通信端末Ｆ６のユーザは、有線通信部２７Ｅと有線通信部２７Ｆに接続していたケーブルを取り外すことができる。その後、通信端末Ｅ５は決定プロトコルセット・リスト３に含まれるプロトコルセットによって他の通信端末と無線通信が可能となる。
例えば、通信端末Ｆ６が通信端末Ｇ７とはIEEE802.11b - TCP/IPにて、通信端末Ｈ８とはBluetooth - NetBEUIにて無線通信を行っているとする。この場合、通信端末Ｅ５は通信端末Ｆ６とはは IEEE802.11b - TCP/IPおよびBluetooth - NetBEUIにて、通信端末Ｇ７とはIEEE802.11b - TCP/IPにて、通信端末Ｈ８とはBluetooth - NetBEUIにて無線通信が可能となる。
【０１５６】
［３．２．３］公開鍵を用いた通信方法
上記の通信パラメータ設定を終了した後、通信端末Ｅ５は無線通信システム３において他の通信端末と無線通信を行う際、公開鍵および秘密鍵を用いて交換される情報を暗号化および復号化する。以下、図２９および図３０を用いてその通信動作を説明する。なお、以下の動作は無線通信システム３において、通信端末Ｅ５と他の通信端末のいずれかとの間において行われる動作であり、その動作はどの通信端末を相手とする場合であっても同じである。従って、ここでは例として通信端末Ｇ７相手の場合を説明する。なお、通信端末Ｅ５と通信端末Ｇ７の立場が逆転しても構わない。
また、以下の通信動作においては、通信端末Ｅ５と通信端末Ｇ７の間で行われる情報の送受信は全て無線通信部２８Ｅおよび無線通信部３４Ｇを介して行われる。
今、通信端末Ｅ５が通信端末Ｇ７にある処理を要求する場合を考える。まず、通信端末Ｅ５の制御部３１Ｅは識別子情報ファイル３２６Ｅを読み出し、通信先である通信端末Ｇ７のMACアドレス（以下、「MAC-G」と呼ぶ）が、識別子情報ファイル３２６Ｅのいずれかのレコードの「MACアドレス」フィールドの値と一致するか否かを判定する（ステップＳ３２４）。MAC-Gが識別子情報ファイル３２６Ｅのいずれかのレコードの「MACアドレス」フィールドの値と一致する場合、制御部３１ＥはステップＳ３２４の判定結果として「Ｙｅｓ」を得る。MAC-Gが識別子情報ファイル３２６Ｅのいずれのレコードの「MACアドレス」フィールドの値とも一致しない場合、制御部３１ＥはステップＳ３２４の判定結果として「Ｎｏ」を得る。
【０１５７】
ステップＳ３２４で「Ｙｅｓ」を得た場合、制御部３１Ｅは制御を後述するステップＳ３２９に移す。
【０１５８】
ステップＳ３２４で「Ｎｏ」を得た場合、制御部３１Ｅは通信端末Ｇ７に対し識別子要求を送信し（ステップＳ３２５）、制御部３７Ｇは通信端末Ｅ５から識別子要求を受信する（ステップＳ３２６）。
【０１５９】
制御部３７Ｇは設定管理情報ファイル３８１Ｇを読み出し、「自機識別子」アイテムの値（以下、「ID-G」と呼ぶ）を通信端末Ｅ５に送信する（ステップＳ３２７）。制御部３１ＥはID-Gを受信すると、識別子情報ファイル３２６Ｅを読み出し、新た

なレコードを追加し、その追加されたレコードの「MACアドレス」フィールドの値および「識別子」フィールドの値を、それぞれMAC-GおよびID-Gとする（ステップＳ３２８）。

【０１６０】

続いて、制御部３１Ｅは公開鍵情報ファイル３２７Ｅを読み出し、ID-Gがいずれかのレコードの「識別子」フィールドの値と一致するか否かを判定する（ステップＳ３２９）。ID-Gが公開鍵情報ファイル３２７Ｅのいずれかのレコードの「識別子」フィールドの値と一致する場合、制御部３１Ｅはステップ Ｓ３２９の判定結果として「Ｙｅｓ」を得る。ID-Gが公開鍵情報ファイル３２７Ｅのいずれのレコードの「識別子」フィールドの値とも一致しない場合、制御部３１Ｅはステップ Ｓ３２９の判定結果として「Ｎｏ」を得る。

【０１６１】

ステップＳ３２９で「Ｙｅｓ」を得た場合、制御部３１Ｅは制御を後述するステップＳ３３４に移す。

【０１６２】

ステップＳ３２９で「Ｎｏ」を得た場合、制御部３１Ｅは通信端末Ｇ７に対し公開鍵要求を送信し（ステップＳ３３０）、制御部３７Ｇは通信端末Ｅ５から公開鍵要求を受信する（ステップＳ３３１）。

【０１６３】

制御部３７Ｇは設定管理情報ファイル３８１Ｇを読み出し、「公開鍵」アイテムの値（以下、「Key-G」と呼ぶ）を通信端末Ｅ５に送信する（ステップＳ３３２）。制御部３１Ｅは通信端末Ｇ７からKey-Gを受信すると、公開鍵情報ファイル３２７Ｅを読み出し、新たなレコードを追加し、追加されたレコードの「識別子」フィールドの値および「公開鍵」フィールドの値をそれぞれID-GおよびKey-Gとする（ステップＳ３３３）。ステップＳ３３３を終えた制御部３１Ｅは制御をステップＳ３３４に移す。なお、上記ステップＳ３２４からステップＳ３３３までの動作を以下、「公開鍵取得作業１」と呼ぶ。

【０１６４】

公開鍵更新作業１を終えた後、制御部３１Ｅは通信端末Ｇ７に対する処理要求情報を準備する。この処理要求情報は通信端末Ｇ７に対する処理の要求に加え、処理に必要なデータを含んでいる（ステップＳ３３４）。次に、制御部３１Ｅは準備した処理要求情報をKey-Gを用いて暗号化し、暗号化した処理要求情報を通信端末Ｇ７に送信する（ステップＳ３３５）。

【０１６５】

通信端末Ｇ７の制御部３７Ｇは暗号化された処理要求情報を受信すると、設定管理情報ファイル３２１Ｆを読み出し、「秘密鍵」アイテムの値を用いて暗号化された処理要求情報を復号化する（ステップＳ３３６）。

【０１６６】

制御部３７Ｇは復号化された処理要求情報に従って処理を行い、その処理結果情報を作業領域３８４Ｇに保存する（ステップＳ３３７）。

【０１６７】

ステップＳ３３７を終えた後、通信端末Ｅ５および通信端末Ｇ７は上述した公開鍵取得作業１（ステップＳ３２４からステップＳ３３３まで）の動作と同様の動作として、公開鍵取得作業２を行う（ステップＳ３３８からステップＳ３４７）。この公開鍵取得作業２は通信端末Ｅ５と通信端末Ｇ７の立場を入れ替えただけのものであるので、説明は省略する。

【０１６８】

公開鍵更新作業２を終えた後、制御部３７Ｇは作業領域３８４Ｇからステップ Ｓ３３７において保存した処理結果情報を読み出す。また、制御部３７Ｇは公開鍵情報ファイル３８３Ｇを読み出し、「識別子」フィールドの値が通信端末Ｅ５の識別子（以下、「MAC-E」と呼ぶ）と一致するレコードを検索し、検索されたレコードの「公開鍵」フィールドの値（以下、「Key-E」と呼ぶ）を取り出す。制御部３７Ｇは処理結果情報をKey-Eを用いて暗号化した後、通信端末Ｅ５に送信する（ステップＳ３４８）。

【０１６９】
通信端末Ｅ５の制御部３１Ｅは、暗号化された処理結果情報を受信すると、設定管理情報ファイル３２１Ｅを読み出し、「秘密鍵」アイテムの値を用いて暗号化された処理結果情報を復号化する（ステップＳ３４９）。こうして、制御部３１Ｅは通信端末Ｇ７に要求した処理結果を受信する。
【０１７０】
［３．３］第３実施形態の効果
第３実施形態においては、新たに無線通信網に加わる通信端末のユーザが自分の通信端末を既に無線通信網に接続している通信端末とケーブルにて接続する、という直感的に理解可能な方法によって無線通信のパラメータ設定を行うことができ、その他、アプリケーションソフトを起動する等の手間を要しない。これはユーザにとっての通信パラメータ設定準備作業を大幅に軽減する。
【０１７１】
第３実施形態において、通信パラメータ設定時に新たに無線通信網に加わる通信端末のユーザが行うべきことは、ユーザが自分で任意に登録したパスワードの入力のみである。これはユーザにとっての通信パラメータ設定作業を大幅に軽減する。なお、この通信パラメータ設定においては、利用可能な通信プロトコルが複数選ばれるため、アクセスポイントによる無線通信の中継を介さずとも、無線通信網の多くの通信端末との通信が可能となる。
【０１７２】
第３実施形態において実現される無線通信システム３においては、通信端末間の情報は全て暗号化されるため、部外者の通信機器がその情報を受信した場合においても、その情報の内容の漏洩を防ぐことができる。多くの無線通信プロトコルは暗号化の方法を有しているが、必ずしも暗号化は義務づけられていない。新たに無線通信網に接続する通信端末のユーザはその無線通信網において暗号化が用いられているか否かを知ることは困難であり、また暗号化がなされていないと分かっても、既に稼働している無線通信網の設定を変更することは容易ではない。これに対し本発明の第３実施形態における通信パラメータ設定によれば、既存の無線通信網に変更を加えることなく、暗号化の使用を確実に行うことができる。
【０１７３】
［４］第４実施形態
［４．１］第４実施形態の構成
［４．１．１］無線通信システムの構成
本発明の第４実施形態においては、本発明の通信パラメータ設定方法により、無線通信を中継するアクセスポイントを介して既に複数の無線通信機器が通信を行っている無線通信網に対し新たに通信機器が無線接続し、この新たに参加する通信機器が前記アクセスポイントに接続している全ての通信機器と無線を介した通信を行うことが可能となる。図３１に本発明の第４実施形態における通信パラメータ設定段階の状態と通信パラメータ設定後の状態を示す。本発明の第４実施形態により実現される通信パラメータ設定後の無線通信システムを以下、「無線通信システム４」と呼ぶ。
【０１７４】
第４実施形態においては、まず無線通信を中継するアクセスポイント１０があり、このアクセスポイント１０は無線通信により通信端末Ｊ１１と接続されている。また、アクセスポイント１０は有線通信により通信端末Ｋ１２およびネットワークサーバ１３と接続されている。また、アクセスポイント１０は有線通信により接続されているインターネットを介して、遠距離にある本社データベースに接続が可能である。なお、有線通信および無線通信によって、アクセスポイント１０はプリンター（図示略）やスキャナー（図示略）等の周辺機器とも接続されている。
【０１７５】
この既に機能している通信網において、まだ未接続の通信端末Ｉ９をアクセスポイント１

０に赤外線で接続することにより、通信端末Ｉ９に対して本発明による通信パラメータ設定が行われる。その結果、通信端末Ｉ９はアクセスポイント１０を介して通信端末Ｊ１１、通信端末Ｋ１２、インターネット、プリンターやスキャナー等の周辺機器との通信を行うことが可能となる。

【０１７６】

第４実施形態においては、通信端末Ｉ９が無線通信システム４における通信を行うための通信パラメータの決定を要求する側の通信機器、アクセスポイント１０が通信パラメータの決定を行う側の通信機器となる。アクセスポイント１０は通信端末Ｉ９が無線通信システム４における無線通信を行うための通信パラメータを決定し、その決定された通信パラメータを通信端末Ｉ９に送信する。通信端末Ｉ９はアクセスポイント１０から通信パラメータを受信し、自分の通信機器に対しその情報に従ったパラメータの変更を行う。この際、第４実施形態においては第２実施形態および第３実施形態と同様に、TCP/IP等の中位レイヤに関する通信プロトコルのパラメータ設定も併せて行う。

【０１７７】

ここでは説明例として、この第４実施形態における通信網はＡ社Ｂ支部Ｃセクションのものとする。Ａ社の本社データベースは、Ａ社の全ての通信機器の識別子をその属するセクション名とともに記憶しており、これらの情報は常に新しいものに更新されている。

【０１７８】

Ａ社の本部および全ての支部の通信網においては、共有フォルダ、共有プリンター等のネットワーク資源のそれぞれは、それぞれのアカウント・グループに対し一定のアクセス権限を設定しており、ネットワークサーバ１３がこれらのアクセス権限を管理している。アカウント・グループには、「同支部同セクション」「同支部他セクション」「他支部」がある。アクセス権限には、読み取り、変更、削除を許可する「フルアクセス」、読み取りのみを許可する「読み取り専用」、利用を禁止する「アクセス拒否」がある。例えばある共有フォルダは同支部同セクションに属するユーザ・アカウントに対してはフルアクセス、同支部他セクションに属するユーザ・アカウントに対しては読み取り専用、他支部に属するユーザ・アカウントに対してはアクセス拒否のようにアクセス権限を設定している。

【０１７９】

アクセスポイント１０は有線通信によりネットワークサーバ１３と接続しているが、アクセスポイント１０は第４実施形態における通信網に対し、３つの異なるユーザ・アカウントによって同時にログインしている。１つは同支部同セクションに属するユーザ・アカウント（以下このユーザ・アカウントを「アカウントP1」と呼ぶ）、１つは同支部他セクションに属するユーザ・アカウント（以下このユーザ・アカウントを「アカウントP2」と呼ぶ）、他の１つは他支部に属するユーザ・アカウント（以下このユーザ・アカウントを「アカウントP3」と呼ぶ）である。

【０１８０】

［４．１．２］通信機器の構成

［４．１．２．１］新規参入する通信端末の構成

図３２に、第４実施形態において新たにアクセスポイントを介して通信網へ接続を行う通信端末Ｉ９の構成を示す。

【０１８１】

通信端末Ｉ９は赤外線通信部４０、無線通信部４１、操作部４２、表示部４３、制御部４４および記憶部４５を備えている。これらの構成要素はバス４６を介して電気的に接続されている。

【０１８２】

無線通信部４１、操作部４２、表示部４３、制御部４４の機能および構成は第２実施形態における通信端末Ｃ３の無線通信部２１、操作部２２、表示部２３、制御部２４のものと同様であるので、説明を省略する。また、記憶部４５の機能も第２実施形態における通信端末Ｃ３の記憶部２５のものと同様であるので、説明を省略する。

【０１８３】

赤外線通信部４０は他の通信機器の赤外線通信部と赤外線により接続され、通信端末Ｉ９が他の通信機器と無線通信を行う為に必要な通信パラメータ等の情報を送受信する。赤外線通信部４０はアンテナ（図示略）を有し、このアンテナを介して変調された信号を受信すると、この受信した信号をベースバンド信号に復調し、ベースバンド信号を制御部４４に送信する。また、赤外線通信部４０は制御部４４よりベースバンド信号を受け取ると、これを用いてキャリアを変調し、変調した信号を前記アンテナを介して外部に送信する。赤外線通信部４０と同種の通信部を持つ全ての通信機器は共通した赤外線用通信プロトコルを１つ共有しており、通信端末Ｉ９はその赤外線用通信プロトコルを用いて、これらの赤外線通信部を介した情報の送受信を行う。

【０１８４】

記憶部４５は、設定管理情報ファイル４５１、自機プロトコル情報ファイル４５２、他機プロトコル情報ファイル４５３および決定プロトコル情報ファイル４５４を記憶し、また作業領域４５５を有している。

【０１８５】

自機プロトコル情報ファイル４５２、他機プロトコル情報ファイル４５３、決定プロトコル情報ファイル４５４および作業領域４５５の構成に関しては第２実施形態における通信端末Ｃ３の自機プロトコル情報ファイル２５３、他機プロトコル情報ファイル２５４、決定プロトコル情報ファイル２５５および作業領域２５６のものと同様であるので、説明を省略する。

【０１８６】

図３３は設定管理情報ファイル４５１の構成を例示したものである。設定管理情報ファイル４５１は、「自機識別子」アイテム、「パスワード」アイテム、「秘密鍵」アイテム、「公開鍵」アイテム、「共通鍵」アイテムを持つ。「自機識別子」アイテムおよび「パスワード」アイテムの機能は第２実施形態における通信端末Ｃ３の設定管理情報ファイル２５１のものと同様である。「秘密鍵」アイテムは、無線通信パラメータの設定段階において通信端末Ｉ９がアクセスポイント１０から暗号化された通信情報を受信する際、その通信情報を復号化するための暗号鍵情報を含む。「公開鍵」アイテムは、無線通信パラメータの設定段階においてアクセスポイント１０が通信端末Ｉ９に対し情報を送信する際、その通信情報を暗号化するための暗号鍵情報を含む。「秘密鍵」アイテムの値と「公開鍵」アイテムの値は１対をなし、「公開鍵」アイテムの値によって暗号化された情報は「秘密鍵」アイテムの値によってのみ、復号化される。「共通鍵」アイテムは無線通信システム４において通信端末Ｉ９がアクセスポイント１０を介して他の通信機器と通信を行う際、送受信される情報を暗号化および復号化する為の暗号鍵情報を含む。

【０１８７】

［４．１．２．２］アクセスポイントの構成

図３４を用いて、第４実施形態において無線通信を中継するアクセスポイント１０の構成を説明する。

【０１８８】

アクセスポイント１０は赤外線通信部４７、無線通信部４８、有線通信部４９、制御部５０および記憶部５１を備えている。これらの構成要素はバス５２を介して電気的に接続されている。

【０１８９】

赤外線通信部４７の機能および構成は通信端末Ｉ９の赤外線通信部４０のものと同様であるので、説明を省略する。また無線通信部４８の機能および構成は第２実施形態における通信端末Ｃ３の無線通信部２１のものと同様であるので、説明を省略する。また、記憶部５１の機能も第２実施形態における通信端末Ｃ３の記憶部２５のものと同様であるので、説明を省略する。

【０１９０】

有線通信部４９は他の通信機器の有線通信部とＬＡＮケーブルや光ケーブル等にて接続され、アクセスポイント１０が他の通信機器と有線通信を行う際の情報の送受信を行う。有

線通信部４９は外部より電気信号もしくは光信号を受け取ると、これを制御部５０が判読可能な電気信号に変換した後に転送する。また制御部５０より電気信号を受け取ると、これを外部の通信機器が判読可能な電気信号もしくは光信号に変換した後に転送する。

【０１９１】

制御部５０の構成は第２実施形態の通信端末Ｃ３における制御部２４と同様であるが、無線通信部４８を経由して送受信される情報量の履歴を作業領域５１８に記録し、その履歴を用いて定期的に各通信プロトコルセットの処理速度を推定し、推定された処理速度が速いものから優先順位を振り直す機能を有する。この優先順位が変わると、制御部５０は記憶部から後述する自機プロトコル情報ファイル５１３を読み出し、「優先順位」フィールドの値を変化後の優先順位を示す正の整数値で更新する。

【０１９２】

記憶部５１は、設定管理情報ファイル５１１、アクセス権限情報ファイル５１２、自機プロトコル情報ファイル５１３、他機プロトコル情報ファイル５１４、決定プロトコル情報ファイル５１５、識別子情報ファイル５１６および共通鍵情報ファイル５１７を記憶し、また作業領域５１８を有している。

【０１９３】

自機プロトコル情報ファイル５１３、他機プロトコル情報ファイル５１４、決定プロトコル情報ファイル５１５および作業領域５１８の構成に関しては第２実施形態における通信端末Ｃ３の自機プロトコル情報ファイル２５３、他機プロトコル情報ファイル２５４、決定プロトコル情報ファイル２５５および作業領域２５６のものと同様であるので、説明を省略する。識別子情報ファイル５１６の構成に関しては、第３実施形態における通信端末Ｅ５の識別子情報ファイル３２６のものと同様であるので、説明を省略する。

【０１９４】

図３５は設定管理情報ファイル５１１の構成を例示したものである。設定管理情報ファイル５１１は「他機識別子」アイテムおよび「他機公開鍵」アイテムを持つ。「他機識別子」アイテムは新規にアクセスポイント１０を介して通信網に接続を行う通信端末の識別子を含む。「他機公開鍵」アイテムは、アクセスポイント１０が新規にこのアクセスポイントを介して通信網に接続を行う通信端末に対し、通信パラメータ設定段階における情報を送信する際に、その情報を暗号化する為の暗号鍵情報を含む。

【０１９５】

図３６はアクセス権限情報ファイル５１２の構成を例示したものである。アクセス権限情報ファイル５１２はＡ社の本社データベースに登録されている通信機器の数と等しい数のレコードを持ち、各レコードは１つの通信機器に関する情報の集まりである。各レコードには「識別子」フィールドと「アカウント・グループ」フィールドがあり、「識別子」フィールドは通信機器の識別子を、「アカウント・グループ」フィールドはアクセスポイント１０が属するＡ社Ｂ支部Ｃセクションにおいて、対象の通信機器が属するアカウント・グループの情報を含む。アクセスポイント１０は定期的にインターネットを介して本社データベースから登録されている通信機器の識別子および所属のセクション名をダウンロードする。その際、アクセスポイント１０は所属のセクション名を１つづつ読み出し、その値がＡ社Ｂ支部Ｃセクションを示すものであれば「同支部同セクション」、Ａ社Ｂ支部であるがＣセクション以外のセクションを示すものであれば「同支部他セクション」、Ａ社の他支部を示すものであれば、「他支部」に変換する。そして、「識別子」フィールドの値をダウンロードした識別子で、また「アカウント・グループ」フィールドの値を変換した後の、各通信機器のアカウント・グループを示す情報で更新する。

【０１９６】

図３７は共通鍵情報ファイル５１７の構成を例示したものである。共通鍵情報ファイル５１７は今までにアクセスポイント１０に接続した通信機器の数と等しい数のレコードを持つ。各レコードは「識別子」フィールドと「共通鍵」フィールドを持つ。「識別子」フィールドは対象の通信機器の識別子を含み、「共通鍵」フィールドはアクセスポイント１０が対象の通信機器と無線通信部４８もしくは有線通信部４９を介した通信を行う際、通信

する情報を暗号化および復号化する為の暗号鍵情報を含む。
【０１９７】
アクセスポイント１０は操作部および表示部を持たないが、管理者は赤外線通信部４７、無線通信部４８もしくは有線通信部４９を介し、他の通信機器より操作を行うことができる。
【０１９８】
［４．１．２．３］新規参入する通信端末以外の通信端末の構成
第４実施形態において、新たに通信網に接続する通信端末以外の通信端末は同じ構成であるので、図３８を用いて通信端末Ｊ１１の構成を説明し、通信端末Ｋ１２の説明は省略する。
【０１９９】
通信端末Ｊ１１は通信部５３、操作部５４、表示部５５、制御部５６および記憶部５７を備えている。これらの構成要素はバス５８を介して電気的に接続されている。
【０２００】
操作部５４、表示部５５および制御部５６の機能および構成は第２実施形態における通信端末Ｃ３の操作部２２、表示部２３および制御部２４のものと同様であるので、説明を省略する。また、記憶部５７の機能も第２実施形態の通信端末Ｃ３における記憶部２５のものと同様であるので、説明を省略する。
【０２０１】
通信部５３は他の通信機器の通信部と有線もしくは無線により接続され、通信端末Ｊ１１が他の通信機器と通信を行う際の情報の送受信を行う。通信部５３は外部より電気信号、光信号、もしくは電波信号を受け取ると、これを制御部５６が判読できる電気信号に変換後、これを制御部５６に転送する。また、制御部５６より電気信号を受け取ると、これを他の通信機器が判読可能な電気信号もしくは電磁波信号に変換した後に転送する。
【０２０２】
記憶部５７は、設定管理情報ファイル５７１を記憶し、また作業領域５７２を有している。
【０２０３】
作業領域５７２の機能に関しては第２実施形態における通信端末Ｃ３の作業領域２５６のものと同様であるので、説明を省略する。
【０２０４】
図３９は設定管理情報ファイル５７１の構成を例示したものである。設定管理情報ファイル５７１は「自機識別子」アイテムおよび「共通鍵」アイテムを持つ。「自機識別子」アイテムの機能は第２実施形態における通信端末Ｃ３の設定管理情報ファイル２５１のものと同様である。また、「共通鍵」アイテムは通信端末Ｊ１１がアクセスポイント１０と通信部５３を介して通信する際、情報を暗号化および復号化する為の暗号鍵情報を含む。
【０２０５】
［４．２］第４実施形態の動作
第４実施形態において、無線通信システム４を実現するための通信パラメータ設定および通信パラメータ設定後の通信方法の動作例を説明する。以下の説明において、通信端末Ｉ９とアクセスポイント１０の同種の構成要素を区別するために、各構成要素を特定する符号に“Ｉ”および“Ｐ”を付加する。
【０２０６】
［４．２．１］接続認証及びパラメータ設定段階
はじめに、アクセスポイント１０は通信端末Ｉ９がアクセスポイント１０に接続することの認証作業を行う。続いてアクセスポイント１０は通信端末Ｉ９が無線通信のために必要とする通信パラメータの決定を行い、通信端末Ｉ９はアクセスポイント１０により決定された通信パラメータに従い、通信パラメータの変更を行う。以下、図４０および図４１を用いてその動作説明を行う。
なお、以下の接続認証およびパラメータ設定段階においては、通信端末Ｉ９とアクセスポ

イント１０の間で行われる情報の送受信は全て赤外線通信部４０Ｉおよび赤外線通信部４７Ｐを介して行われる。

【０２０７】

まず、通信端末Ｉ９のユーザはアクセスポイント１０の赤外線通信部４７Ｐを見通せる位置に通信端末Ｉ９を置く。赤外線通信部４０Ｉおよび赤外線通信部４７Ｐは相手から送信される赤外線信号を検知し、赤外線接続を確立する（ステップＳ４０１）。

【０２０８】

制御部４４Ｉは次にパスワード照合作業を行う。このパスワード照合作業は第２実施形態におけるステップＳ２０６からS０８と同様であるので、説明を省略する（ステップＳ４０２からステップＳ４０４）。なお、このパスワード入力作業は、正しいユーザが通信端末Ｉ９の無線通信網に対する接続を試みていることを確認するための動作である。

【０２０９】

ステップＳ４０４において２つのパスワードが一致した場合、制御部４４Ｉは秘密鍵と公開鍵のセットを新たに生成し、設定管理情報ファイル４５１Ｉを読み出し、「秘密鍵」アイテムの値および「公開鍵」アイテムの値をそれぞれ生成した秘密鍵および公開鍵の情報で更新する。ここで、秘密鍵と公開鍵の生成の方法については既に知られる方法によるので、説明を省略する（ステップＳ４０５）。

【０２１０】

次に、制御部４４Ｉは設定管理情報ファイル４５１Ｉおよび自機プロトコル情報ファイル４５２Ｉを読み出し、まず設定管理情報ファイル４５１Ｉの「自機識別子」アイテムの値（以下、「ID-I」と呼ぶ）および「公開鍵」アイテムの値（以下、「Key-I」と呼ぶ）を取り出す。続いて、制御部４４Ｉは自機プロトコル情報ファイル４５２Ｉの全レコードの「MACアドレス」フィールドおよび「プロトコルセット」フィールドの値（以下、「プロトコルセット・テーブルI」と呼ぶ）を各レコードにおける対応関係を維持したままで取り出す。プロトコルセット・テーブルIは通信端末Ｉ９が無線通信部４１Ｉを用いた通信を行う際に利用可能なプロトコルに関する案内情報である。次に、制御部４４ＩはID-I、Key-I、およびプロトコルセット・テーブルＩをアクセスポイント１０に送信する（ステップＳ４０６）。

アクセスポイント１０の制御部５０PはID-I、Key-Iおよびプロトコルセット・テーブルIを受信すると、まず設定管理情報ファイル５１１Ｐを読み出し、その「他機識別子」アイテムの値をID-Iで、「他機公開鍵」アイテムの値をKey-Iで更新する。続いて、制御部５０Ｐは他機プロトコル情報ファイル５１４Ｐを読み出し、その「MACアドレス」フィールドおよび「プロトコルセット」フィールドの値をプロトコルセット・テーブルIの「MACアドレス」フィールドおよび「プロトコルセット」フィールドの値でそれぞれ更新する（ステップＳ４０７）。

【０２１１】

続いて、制御部５０Ｐはアクセス権限情報ファイル５１２Ｐを読み出し、ID-Iがいずれかのレコードの「識別子」フィールドの値と一致するか否かを判定する（ステップＳ４０８）。ID-Iがアクセス権限情報ファイル５１２Ｐのいずれかのレコードの「識別子」フィールドの値と一致する場合、制御部５０Ｐはステップ Ｓ４０８の判定結果として「Ｙｅｓ」を得る。ID-Iがアクセス権限情報ファイル５１２Ｐのいずれのレコードの「識別子」フィールドの値とも一致しない場合、制御部５０Ｐはステップ Ｓ４０８の判定結果として「Ｎｏ」を得る。

【０２１２】

ステップＳ４０８で「Ｙｅｓ」を得ると、制御部５０Ｐは制御を後述するステップＳ４１１に移す。

【０２１３】

ステップＳ４０８で「Ｎｏ」を得ると、制御部５０Ｐは接続拒絶通知を通信端末Ｉ９に送信する（ステップＳ４０９）。これは、通信端末Ｉ９が登録されておらず、この無線通信網への接続が拒否されたことを意味する。

通信端末Ｉ９の制御部４４Ｉはアクセスポイント１０より接続拒絶通知を受信すると、接続が拒絶されたことを通知するメッセージを表示部４３Ｉに表示する（ステップＳ４１０）。このステップを経た場合、制御部４４Ｉは動作を終了する。

【０２１４】

ステップＳ４０８において制御部５０Ｐが「Ｙｅｓ」の判定を得た場合、通信端末Ｉ９およびアクセスポイント１０は通信可能確認作業を行う。通信可能確認作業は第２実施形態におけるステップＳ２２０からS２２とほぼ同様であるので、詳細な説明を省略する（ステップＳ４１１からステップＳ４１３）。この通信可能確認作業において、通信端末Ｉ９およびアクセスポイント１０はそれぞれ第２実施形態における通信端末Ｓおよび通信端末Ｍにあたる。ただし、ステップＳ４１２において、制御部５０Ｐは無線通信の設定が不可能であることを通知するメッセージの表示を行わない。

【０２１５】

ステップＳ４１１の判定結果として「Ｙｅｓ」を得た場合、制御部５０Ｐは自機プロトコル情報ファイル５１３Ｐを読み出し、その全てのレコードの中から、「プロトコルセット」フィールドの値が他機プロトコル情報ファイル５１４Ｐのいずれかのレコードの「プロトコルセット」フィールドの値と一致するレコードを全て抽出する。自機プロトコル情報ファイル５１３Ｐから複数のレコードが抽出された場合、制御部５０Ｐは抽出されたレコードの「優先順位」フィールドの値を比較し、「優先順位」フィールドの値が最も小さいものを選択する。一つのレコードのみが抽出された場合、制御部５０Ｐはそのレコードを選択する。次に、制御部５０Ｐは決定プロトコル情報ファイル５１５Ｐを読み出し、その唯一のレコードの「自機MACアドレス」フィールドの値を選択されたレコードの「MACアドレス」フィールドの値（以下、「MAC-P」と呼ぶ）で、「プロトコルセット」フィールドの値を選択されたレコードの「プロトコルセット」フィールドの値（以下、「決定プロトコルセット４」と呼ぶ）で更新する。続いて、制御部５０Ｐは他機プロトコル情報ファイル５１４Ｐの全てのレコードの中から、「プロトコルセット」フィールドの値が決定プロトコルセット４と一致するレコードを検索し、決定プロトコル情報ファイル５１５Ｐの「他機MACアドレス」フィールドの値を検索されたレコードの「MACアドレス」フィールドの値（以下、「MAC-I」と呼ぶ）で更新する（ステップＳ４１４）。

【０２１６】

次に、制御部５０ＰはステップＳ４１４において選択された自機プロトコル情報ファイル５１３Ｐのレコードの「パラメータセット」フィールドの値に基づいて、通信端末Ｉ９がアクセスポイント１０と決定プロトコルセット４の示すプロトコルセットを用いて無線通信を行うために変更の必要なパラメータセットの値を決定する。以下、通信端末Ｉ９用のパラメータセットを「パラメータセットI」と呼ぶ。次に制御部５０Ｐは決定プロトコル情報ファイル５１５Ｐを読み出し、その唯一のレコードの「パラメータセット」フィールドの値をパラメータセットIで更新する（ステップＳ４１５）。なお、パラメータセットの決定方法は第２実施形態および第３実施形態におけるパラメータセットの決定方法と同様であるので、説明を省略する。

【０２１７】

次に、制御部５０Ｐは通信端末Ｉ９がアクセスポイント１０と無線通信部４１Ｉと無線通信部４８Ｐを用いて通信を行う際に通信情報を暗号化および復号化する任意の暗号鍵（以下、「Key'-I」と呼ぶ）を作成する。暗号鍵は文字、数字および記号の列であり、乱数関数により生成される。乱数関数については既に多くの既知のものがあるため、ここでは説明を省略する。続いて、制御部５０Ｐは設定管理情報ファイル５１１Ｐを読み出し、「他機識別子」アイテムの値、すなわちID-Iを取り出す。次に共通鍵情報ファイル５１７Ｐを読み出し、「識別子」フィールドの値がID-Iと一致するレコードを検索し、検索されたレコードの「共通鍵」フィールドの値をKey'-Iで更新する。共通鍵情報ファイル５１７Ｐのいずれのレコードの「識別子」フィールドの値もID-Iと一致しない場合には、制御部５０Ｐは共通鍵情報ファイル５１７Ｐに新たなレコードを追加し、追加されたレコードの「識別子」フィールドの値をID-Iとし、「共通鍵」フィールドの値をKey'-Iとする（ステップ

Ｓ４１６）。
【０２１８】
続いて、制御部５０Ｐは設定管理情報ファイル５１１Ｐを読み出し、「他機識別子」アイテムの値、すなわちID-Iと、「他機公開鍵」アイテムの値、すなわちKey-Iを取り出す。次に制御部５０Ｐは共通鍵情報ファイル５１７Ｐを読み出し、「識別子」フィールドの値がID-Iと一致するレコードを検索し、検索されたレコードの「共通鍵」フィールドの値、すなわちKey'-Iを取り出す。次に、制御部５０Ｐは決定プロトコル情報ファイル５１５Ｐを読み出し、唯一のレコードの「自機MACアドレス」フィールドの値、すなわちMAC-P、「プロトコルセット」フィールドの値、すなわち決定プロトコルセット４、「パラメータセット」フィールドの値、すなわちパラメータセットI、を取り出す。これらの情報は通信端末Ｉ９が無線通信部４１Ｉを用いてアクセスポイント１０と通信を行うための通信パラメータである。続いて、制御部５０ＰはMAC-P、決定プロトコルセット４、パラメータセットIおよびKey'-IをKey-Iを用いて暗号化した後、それらを通信端末Ｉ９に送信する（ステップＳ４１７）。
【０２１９】
通信端末Ｉ９の制御部４４ＩはMAC-P、決定プロトコルセット４、パラメータセットIおよびKey'-Iを含む暗号化された情報を受信すると、設定管理情報ファイル４５１Ｉを読み出し、受信した情報を「秘密鍵」アイテムの値で復号化する。続いて、制御部４４Ｉは決定プロトコル情報ファイル４５４Ｉを読み出し、唯一のレコードの「他機MACアドレス」フィールドの値、「プロトコルセット」フィールドの値、「パラメータセット」フィールドの値をそれぞれMAC-P、決定プロトコルセット４、パラメータセットIで更新する。次に、制御部４４Ｉは自機プロトコル情報ファイル４５２Ｉを読み出し、「プロトコルセット」フィールドの値が決定プロトコルセット４と一致するレコードを検索する。続いて、制御部４４Ｉは決定プロトコル情報ファイル４５４Ｉの唯一のレコードの「自機MACアドレス」フィールドの値を、検索されたレコードの「MACアドレス」フィールドの値、すなわちMAC-Iで更新する。次に、制御部４４Ｉは設定管理情報ファイル４５１Ｉを読み出し、「共通鍵」アイテムの値をKey'-Iで更新する（ステップＳ４１８）。
【０２２０】
制御部４４Ｉは決定プロトコル情報ファイル４５４Ｉを読み出し、唯一のレコードの「プロトコルセット」フィールドの値および「パラメータセット」の値を無線通信部４１Ｉに送信する。無線通信部４１Ｉはこれらの情報を受信すると、不揮発性メモリに記憶されている、「プロトコルセット」フィールドの値が示す通信プロトコルセットに関する通信パラメータを、「パラメータセット」フィールドの値が示す情報に基づいて変更する。なお、この変更を終えた無線通信部４１Ｉは、設定終了を制御部４４Ｉに通知する（ステップＳ４１９）。
【０２２１】
設定終了の通知を無線通信部４１Ｉより受信すると、制御部４４Ｉは無線通信の設定が完了したことを通知するメッセージを表示部４３Ｉに表示する（ステップＳ４２０）。
【０２２２】
ステップＳ４２０において表示されたメッセージにより、パラメータ設定が完了したことを確認した通信端末Ｉ９のユーザは、赤外線通信部４０Ｉを介したアクセスポイント１０との通信接続を切断することができる。その後、通信端末Ｉ９のユーザは決定プロトコルセット４の示すプロトコルセットによって、アクセスポイント１０を介して他の通信端末との無線通信が可能となる。
【０２２３】
［４．２．２］共通鍵を用いた通信方法
上記の通信パラメータ設定を終了した後、通信端末Ｉ９が無線通信システム４において他の通信機器と通信を行う際、通信情報は共通鍵を用いて暗号化される。また、アクセスポイント１０は通信端末Ｉ９が無線通信網の共有資源を利用する場合、通信端末Ｉ９の代行としてそれらにアクセスすることにより、ネットワークサーバ１３が通信端末Ｉ９のアク

セス権限管理を行うことを可能にする。図４２および図４３を用いてその動作説明を行う。なお、以下の動作は通信端末Ｉ９がアクセスポイント１０を介して通信端末Ｊ１１にある処理を要求する場合の例である。また、説明の為、本例においては通信端末Ｉ９はＡ社Ｄ支部Ｅセクションに属するものであるとする。以下、通信端末Ｉ９、アクセスポイント１０および通信端末Ｊ１１の同種の構成要素を区別するために、各構成要素を特定する符号にそれぞれ“Ｉ”、“Ｐ”および“Ｊ”を付加する。
また、以下の動作においては、通信端末Ｉ９とアクセスポイント１０の間で行われる情報の送受信は全て無線通信部４１Ｉおよび無線通信部４８Ｐを介して、アクセスポイント１０と通信端末Ｊ１１の間で行われる情報の送受信は全て無線通信部４８Ｐもしくは有線通信部４９Ｐおよび通信部５３Ｊを介して行われる。

【０２２４】
まず、制御部４４Ｉは通信端末Ｊ１１に対する処理要求情報を準備する（ステップＳ４２１）。この処理要求情報は通信端末Ｊ１１のMACアドレス（以下、「MAC-J」と呼ぶ）、通信端末Ｊ１１に対する処理の要求に加え、処理に必要なデータを含んでいる。
次に、制御部４４Ｉは設定管理情報ファイル４５１Ｉを読み出し、「共通鍵」アイテムの値、すなわちKey'-Iを取り出し、処理要求情報をKey'-Iを用いて暗号化する。次に、制御部４４Ｉは決定プロトコル情報ファイル４５４Ｉを読み出し、唯一のフィールドの「自機MACアドレス」フィールドの値、すなわちMAC-Iを取り出し、暗号化された処理要求情報にMAC-Iを付加して、これをアクセスポイント１０に送信する（ステップＳ４２２）。

【０２２５】
アクセスポイント１０の制御部５０PはMAC-Iが付加された、暗号化された処理要求情報を受信すると、識別子情報ファイル５１６Ｐを読み出し、その全レコードから「MACアドレス」フィールドの値がMAC-Iと一致するレコードを検索し、検索されたレコードの「識別子」フィールドの値、すなわちID-Iを取り出す。次に、制御部５０Ｐは共通鍵情報ファイル５１７Ｐを読み出し、その全レコードから「識別子」フィールドの値がID-Iと一致するレコードを検索し、検索されたレコードの「共通鍵」フィールドの値、すなわちKey'-Iを取り出す。制御部５０Ｐは暗号化された処理要求情報をKey-'Iを用いて復号化する。制御部５０Ｐはこの処理要求情報をKey'-Iと共に作業領域５１８Ｐに保存する（ステップＳ４２３）。

【０２２６】
次に、制御部５０Ｐはアクセス権限情報ファイル５１２Ｐを読み出し、その全レコードから「識別子」フィールドの値がステップＳ４２３で取り出したID-Iと一致するレコードを検索し、検索されたレコードの「アカウント・グループ」フィールドの値を取り出す（ステップＳ４２４）。ここで、第４実施形態における通信網はＡ社Ｂ支部Ｃセクションに所属し、通信端末Ｉ９はＡ社Ｄ支部Ｅセクションに所属することから、ここで検索されたレコードの「アカウント・グループ」フィールドの値は「他支部」となっている。

【０２２７】
続いて、制御部５０Ｐは作業領域５１８Ｐから処理要求情報を読み出し、処理要求情報からこの処理要求の宛先であるMAC-Jを取り出す。次に、制御部５０Ｐは識別子情報ファイル５１６Ｐを読み出し、その全レコードから「MACアドレス」フィールドの値がMAC-Jと一致するレコードを検索し、検索されたレコードの「識別子」フィールドの値（以下、「ID-J」と呼ぶ）を取り出す。次に、制御部５０Ｐは共通鍵情報ファイル５１７Ｐを読み出し、その全レコードから「識別子」フィールドの値がID-Jと一致するレコードを検索し、検索されたレコードの「共通鍵」フィールドの値（以下、「Key'-J」と呼ぶ）を取り出す。制御部５０Ｐは処理要求情報をKey'-Jを用いて暗号化する。次に、制御部５０Ｐは暗号化された処理要求情報に対し、送信元ユーザ・アカウント情報として「アカウントP3」を付加し、通信端末Ｊ１１に送信する（ステップＳ４２５）。アカウントP3は既述のとおり、アクセスポイント１０が「他支部」に属するユーザとしてログインしているユーザ・アカウントであり、通信端末Ｉ９に対応するアカウント・グループが他支部であることから、制御部５０Ｐはここでアカウント P3を選択している。

【０２２８】
通信端末Ｊ１１の制御部５６Ｊは暗号化された処理要求情報を受信すると、設定管理情報ファイル５７１Ｊを読み出し、「共通鍵」アイテムの値、すなわちKey'-Jを用いて暗号化された処理要求情報を復号化する（ステップＳ４２６）。
【０２２９】
制御部５６Ｊは受信した処理要求情報に基づき処理を行うが、その処理を行うに当たり通信網の共有ネットワーク資源を利用する必要が生じると、制御部５６Ｊはネットワークサーバ１３に対し、アカウントP3に与えられている、そのネットワーク資源に関するアクセス権限情報を要求する。ネットワークサーバ１３はこの要求に応じて、アカウントP3が対象のネットワーク資源に対し有しているアクセス権限情報を通信端末Ｊ１１に送信する。
制御部５６Ｊは受信した情報に基づき、要求されている処理がアカウントＰ３に与えられているアクセス権限によって可能か否かを判定する（ステップＳ４２７）。処理に必要な動作がアカウントP3のアクセス権限では実行できない場合、制御部５６Ｊはステップ４２７の判定結果として「Ｎｏ」を得、処理を中断する。要求された処理を行うための全ての動作がアカウントP3のアクセス権限で実行できる場合、制御部５６Ｊはステップ４２７の判定結果として「Ｙｅｓ」を得る。
【０２３０】
ステップＳ４２７において「Ｎｏ」を得ると、制御部５６Ｊは処理拒絶通知をアクセスポイント１０に送信する（ステップＳ４２８）。
アクセスポイント１０の制御部５０Ｐは通信端末Ｊ１１より処理拒絶通知を受信すると、その通知を通信端末Ｉ９に転送する（ステップＳ４２９）。
通信端末Ｉ９の制御部４４Ｉはアクセスポイント１０より処理拒絶通知を受信すると、表示部４３Ｉに処理が拒絶されたことを通知するメッセージを表示する（ステップＳ４３０）。ステップＳ４３０を終えると、制御部４４Ｉの動作は終了する。
【０２３１】
ステップＳ４２７において「Ｙｅｓ」を得ると、制御部５６Ｊは要求された処理を完了する（ステップＳ４３１）。
要求された処理が終了すると、制御部５６Ｊは設定管理情報ファイル５７１Ｊを読み出し、を取り出し、処理結果情報を「共通鍵」アイテムの値、すなわちKey'-Jを用いて暗号化する。次に、制御部５６Ｊは暗号化された処理結果情報に送信元のMACアドレスとしてMAC-Jを付加した後、これをアクセスポイント１０に送信する（ステップＳ４３２）。
【０２３２】
アクセスポイント１０の制御部５０ＰはMAC-Jの付加された暗号化された処理結果情報を受信すると、識別子情報ファイル５１６Ｐを読み出し、その全レコードから「MACアドレス」フィールドの値が処理結果情報に付加されているMAC-Jと一致するレコードを検索し、検索されたレコードの「識別子」フィールドの値、すなわちID-Jを取り出す。次に、制御部５０Ｐは共通鍵情報ファイル５１７Ｐを読み出し、その全レコードから「識別子」フィールドの値がID-Jと一致するレコードを検索し、検索されたレコードの「共通鍵」フィールドの値、すなわちKey'-Jを取り出す。制御部５０Ｐは処理結果情報をKey'-Jを用いて復号化する（ステップＳ４３３）。
【０２３３】
次に、制御部５０Ｐは作業領域５１８ＰからステップＳ４２３において保存した処理要求情報およびKey'-Iを読み出す。そして、制御部５０Ｐは復号化された処理結果情報がこの処理要求情報に対するものであることを確認し、処理結果情報をKey'-Iを用いて暗号化する。制御部５０Ｐは暗号化された処理結果情報を通信端末Ｉ９に送信する（ステップＳ４３４）。
【０２３４】
通信端末Ｉ９の制御部４４Ｉは暗号化された処理結果情報を受信すると、設定管理情報ファイル４５１Ｉを読み出し、「共通鍵」フィールドの値、すなわちKey'-Iを用いて暗号化された処理結果情報を復号化する（ステップＳ４３５）。上記の動作により、制御部４４

Ｉは通信端末Ｊ１１に対し要求した処理の結果を受信することができる。

【０２３５】

［４．３］第４実施形態の効果

第４実施形態においては、無線通信網に新たに参入を望む通信端末のユーザは、この無線通信網における通信の中継を行っているアクセスポイントの近くに通信端末を置き、ユーザが自分で任意に登録したパスワードの入力を行うだけでよい。それにより、自動的に無線通信のパラメータ設定が行われる。これはユーザにとっての通信パラメータ設定作業を大幅に軽減する。また、通信パラメータ設定時に用いられる赤外線接続は通信機器が互いに見通しがきく範囲内における近距離無線接続であるので、アクセスポイントが手の届きにくい場所に設置されていても通信パラメータ設定が可能であると同時に、見えないところで部外者が通信機器の接続を試みることを防ぐことができる。これにより、高い利便性とセキュリティを両立できる。

【０２３６】

第４実施形態においては、通信パラメータ設定作業において利用可能な通信プロトコルのうち、処理速度が最も速いと推定される通信プロトコルが選択されるため、効率の高い通信網が実現される。

【０２３７】

第４実施形態におけるアクセスポイントは新たな通信端末の接続を、通信端末の所属情報により認証する。これにより、部外者の通信端末が通信網に接続することを防ぐことが出来る。

【０２３８】

無線通信システム４においては、新たに参入した通信端末と他の通信機器間の情報は全て暗号化されるため、部外者の通信端末がその情報を受信した場合においても、その情報の内容の漏洩を防ぐことができる。暗号化には共通鍵が用いられ、高い通信速度を実現できる。また、それぞれの通信機器に対応した共通鍵をアクセスポイントが集中管理することにより、管理者の負担が軽減される。

【０２３９】

無線通信システム４においては、新たに参入した通信端末の所属情報に基づき、その通信端末が通信網において行うネットワーク資源へのアクセスが管理される。その際、既存の通信網の設定には何ら変更が加えられない。これは通信網のアクセス権限管理に要する作業を大幅に軽減する。

【０２４０】

【発明の効果】

上述したように、本発明によれば、無線通信網において新たな通信端末を接続する際、誰もが簡易に必要となるパラメータ設定を行うことが可能となる。その際、ユーザや管理者の介入なく、適当な通信プロトコルが選択される。さらに、本発明によれば、新たな通信端末が無線通信網に接続した後、その新たな通信端末の送受信する通信情報は暗号化により漏洩から保護され、その新たな通信端末のネットワーク資源の利用に関しては不正な利用が防止される。

【図面の簡単な説明】

【図１】　本発明の第１実施形態における無線通信システムの概要構成を示す図である。

【図２】　本発明の第１実施形態における携帯型情報端末の概要構成を示す図である。

【図３】　本発明の第１実施形態における携帯型情報端末のプロトコル情報ファイルの構成を示す図である。

【図４】　本発明の第１実施形態における携帯型情報端末の暗号鍵情報ファイルの構成を示す図である。

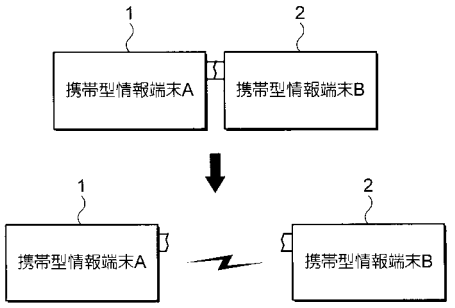
【図５】　本発明の第１実施形態における携帯型情報端末の端末情報ファイルの構成を示す図である。

【図６】　本発明の第１実施形態における無線通信に関する設定の動作例を示すフロー図である。

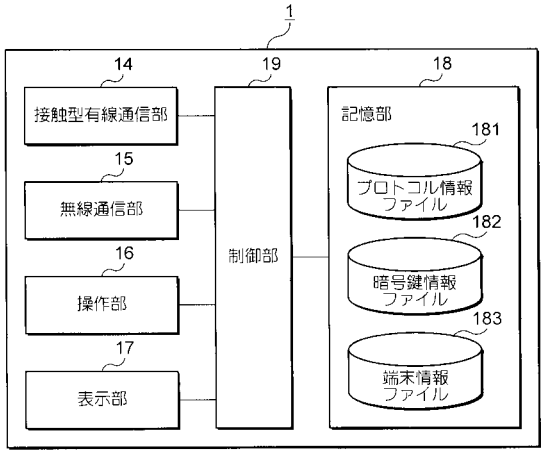
【図７】　本発明の第２実施形態における無線通信システムの概要構成を示す図である。
【図８】　本発明の第２実施形態における通信端末の概要構成を示す図である。
【図９】　本発明の第２実施形態における通信端末の設定管理情報ファイルの構成を示す図である。
【図１０】　本発明の第２実施形態における通信端末、および第３実施形態における有線通信部を有する通信端末の端末情報ファイルの構成を示す図である。
【図１１】　本発明の第２実施形態における通信端末、第４実施形態における新規参入する通信端末、および第４実施形態におけるアクセスポイントの自機プロトコル情報ファイルの構成を示す図である。
【図１２】　本発明の第２実施形態における通信端末、第３実施形態における有線通信部を有する通信端末、第４実施形態における新規参入する通信端末、および第４実施形態におけるアクセスポイントの他機プロトコル情報ファイルの構成を示す図である。
【図１３】　本発明の第２実施形態における通信端末、および第４実施形態における新規参入する通信端末およびアクセスポイントの決定プロトコル情報ファイルの構成を示す図である。
【図１４】　本発明の第２実施形態における無線通信に関する設定の接続認証段階の動作例を示すフロー図である。
【図１５】　本発明の第２実施形態における無線通信に関する設定のマスタ・スレーブ決定段階の動作例を示すフロー図である。
【図１６】　本発明の第２実施形態における無線通信に関する設定のパラメータ設定段階の動作例を示すフロー図である。
【図１７】　本発明の第２実施形態における無線通信に関する設定のパラメータ設定段階の動作例を示すフロー図である。
【図１８】　本発明の第３実施形態における無線通信システムの概要構成を示す図である。
【図１９】　本発明の第３実施形態における有線通信部を有する通信端末の概要構成を示す図である。
【図２０】　本発明の第３実施形態における有線通信部を有する通信端末の設定管理情報ファイルの構成を示す図である。
【図２１】　本発明の第３実施形態における有線通信部を有する通信端末の自機プロトコル情報ファイルの構成を示す図である。
【図２２】　本発明の第３実施形態における有線通信部を有する通信端末の決定プロトコル情報ファイルの構成を示す図である。
【図２３】　本発明の第３実施形態における有線通信部を有する通信端末および有線通信部を有さない通信端末、第４実施形態におけるアクセスポイントの識別子情報ファイルの構成を示す図である。
【図２４】　本発明の第３実施形態における有線通信部を有する通信端末および有線通信部を有さない通信端末の公開鍵情報ファイルの構成を示す図である。
【図２５】　本発明の第３実施形態における有線通信部を有さない通信端末の概要構成を示す図である。
【図２６】　本発明の第３実施形態における有線通信部を有さない通信端末の設定管理情報ファイルの構成を示す図である。
【図２７】　本発明の第３実施形態における無線通信に関する設定の接続認証段階の動作例を示すフロー図である。
【図２８】　本発明の第３実施形態における無線通信に関する設定のパラメータ設定段階の動作例を示すフロー図である。
【図２９】　本発明の第３実施形態における無線通信に関する設定完了後の通信の動作例を示すフロー図である。
【図３０】　本発明の第３実施形態における無線通信に関する設定完了後の通信の動作例を示すフロー図である。

【図３１】　本発明の第４実施形態における無線通信システムの概要構成を示す図である。
【図３２】　本発明の第４実施形態における新規参入する通信端末の概要構成を示す図である。
【図３３】　本発明の第４実施形態における新規参入する通信端末の設定管理情報ファイルの構成を示す図である。
【図３４】　本発明の第４実施形態におけるアクセスポイントの概要構成を示す図である。
【図３５】　本発明の第４実施形態におけるアクセスポイントの設定管理情報ファイルの構成を示す図である。
【図３６】　本発明の第４実施形態におけるアクセスポイントのアクセス権限情報ファイルの構成を示す図である。
【図３７】　本発明の第４実施形態におけるアクセスポイントの共通鍵情報ファイルの構成を示す図である。
【図３８】　本発明の第４実施形態における新規参入する通信端末以外の通信端末の概要構成を示す図である。
【図３９】　本発明の第４実施形態における新規参入する通信端末以外の設定管理情報ファイルの構成を示す図である。
【図４０】　本発明の第４実施形態における無線通信に関する設定の接続認証およびパラメータ設定段階の動作例を示すフロー図である。
【図４１】　本発明の第４実施形態における無線通信に関する設定の接続認証およびパラメータ設定段階の動作例を示すフロー図である。
【図４２】　本発明の第４実施形態における無線通信に関する設定完了後の通信の動作例を示すフロー図である。
【図４３】　本発明の第４実施形態における無線通信に関する設定完了後の通信の動作例を示すフロー図である。
【符号の説明】
１，２　携帯型通信端末
３，４，５，６，７，８，９，１１，１２　通信端末
１０　アクセスポイント
１３　ネットワークサーバ
１４　接触型有線通信部
１５，２１，２８，３４，４１，４８　無線通信部
１６，２２，２９，３５，４２，５４　操作部
１７，２３，３０，３６，４３，５５　表示部
１８，２５，３２，３８，４５，５１，５７　記憶部
１９，２４，３１，３７，４４，５０，５６　制御部
２０，２７，４９　有線通信部
２６，３３，３９，４６，５２，５８　バス
４０，４７　赤外線通信部
５３　通信部

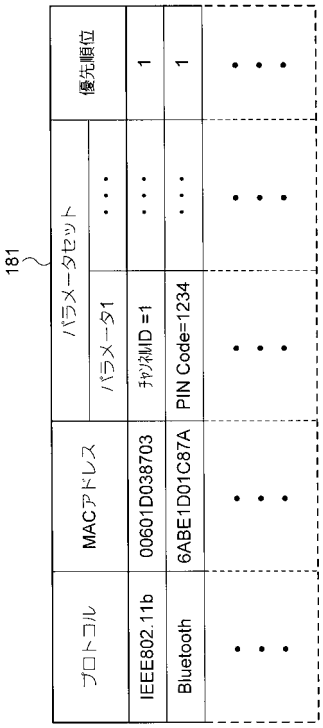
【図１】



【図２】



【図３】



【図４】

182

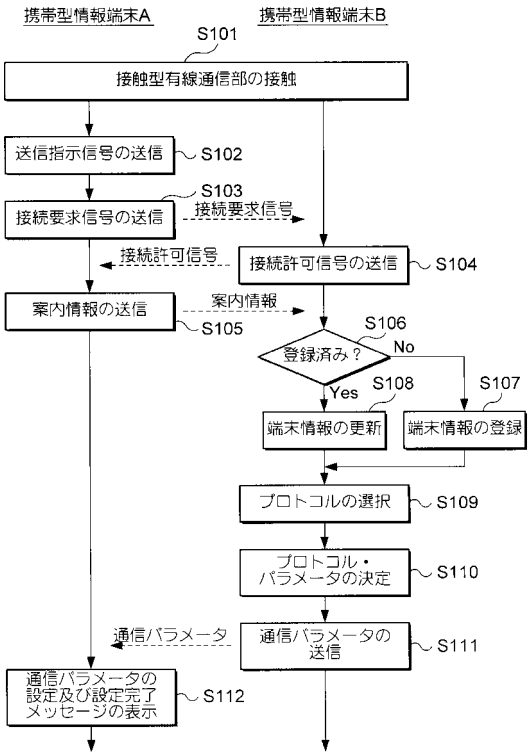
識別子	暗号鍵
EP00002	3d068c4a50

【図５】

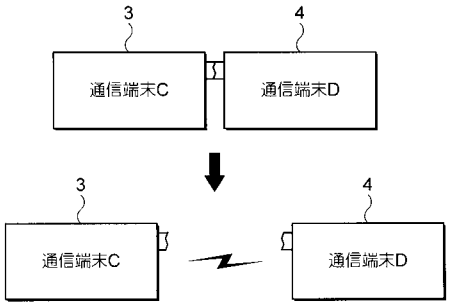
183

識別子	アクセス権限	暗号鍵	プロトコル	MACアドレス
EP00001	読み取り専用	07003a8b4a	Bluetooth	00601D038702
EP00003	フルアクセス	top5ofb2wg	IEEE802.11b	00601D038705
・	・	・	・	・
・	・	・	・	・
・	・	・	・	・

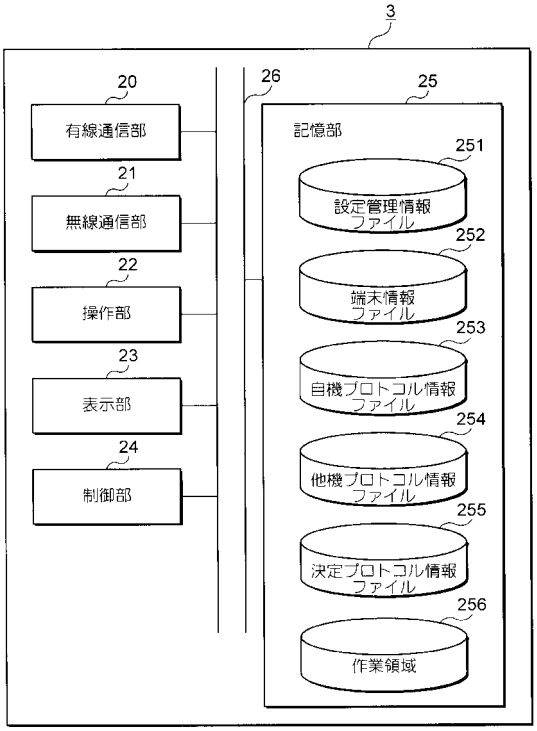
【図６】



【図７】



【図８】



【図９】

251

マスタ・スレーブ	1
自機識別子	0585CA2C
他機識別子	BC5E7DC0
パスワード	AZ23\#c7
共通鍵	v1h4e5jqxhp3em6feak#vcun
設定完了通知フラグ	OFF

【図１０】

252

識別子
57242C0D
BBA60A16
・ ・ ・

【図１１】

253

優先順位	MACアドレス	プロトコルセット	パラメータセット		
			パラメータ1	パラメータ2	パラメータ3
1	E8B0324FC8E5	IEEE802.11b - NetBEUI	IEEE802.11b モード＝AdHoc	IEEE802.11b チャンネルID＝7	—
2	5B98007E03E2	IEEE802.11b - TCP/IP	IEEE802.11b モード＝Infrastructure	IEEE802.11b チャンネルID＝3	IPアドレス/サブネットマスク 192.168.0.220/255.255.255.0
3	F0A6998BF3CB	Bluetooth - NetBEUI	Bluetooth PIN Code＝2851	—	—
・ ・ ・	・ ・ ・	・ ・ ・	・ ・ ・	・ ・ ・	・ ・ ・

【図１２】

254

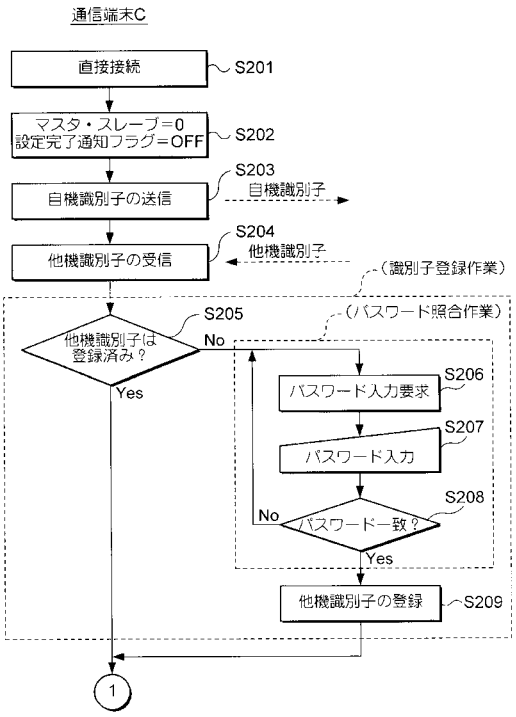
MACアドレス	プロトコルセット
58DF46499F0C	IEEE802.11b - TCP/IP
58DF46499F0C	IEEE802.11b - IPX/SPX
C59166816E84	HomeRF - NetBEUI
・	・
・	・
・	・

【図１３】

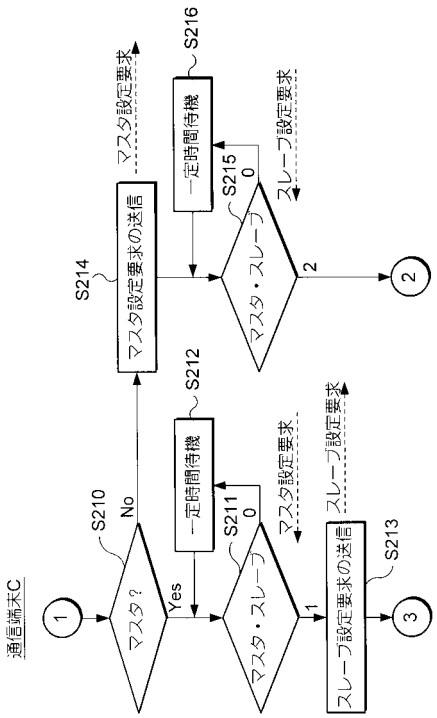
255

自機MACアドレス	他機MACアドレス	プロトコルセット	パラメータセット			
			パラメータ1	パラメータ2	パラメータ3	・・・
5B98007E03E2	58DF46499F0C	IEEE802.11b - TCP/IP	IEEE802.11b ﾓｰﾄﾞ=AdHoc	IEEE802.11b ﾁｬﾝﾈﾙID=5	IPｱﾄﾞﾚｽ/ｻﾌﾞﾈｯﾄﾏｽｸ 192.168.0.221/ 255.255.255.0	・・・

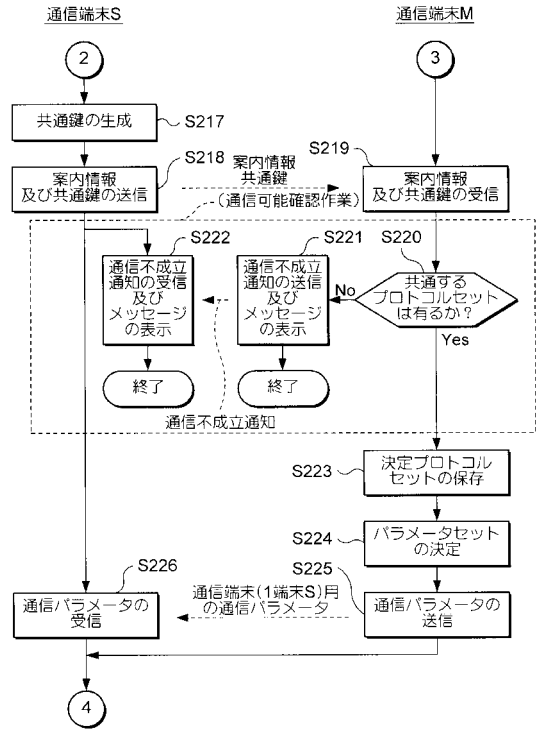
【図１４】



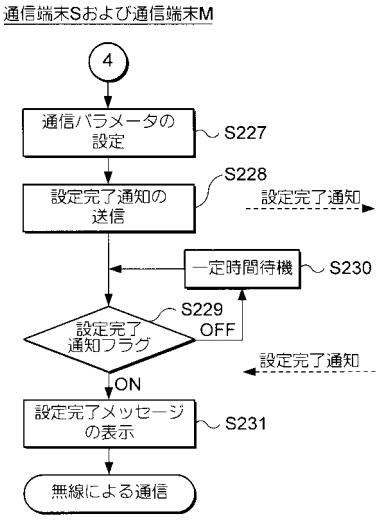
【図１５】



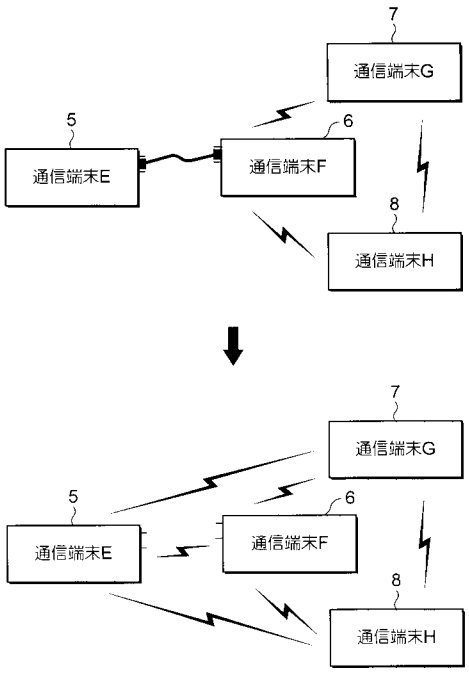
【図１６】



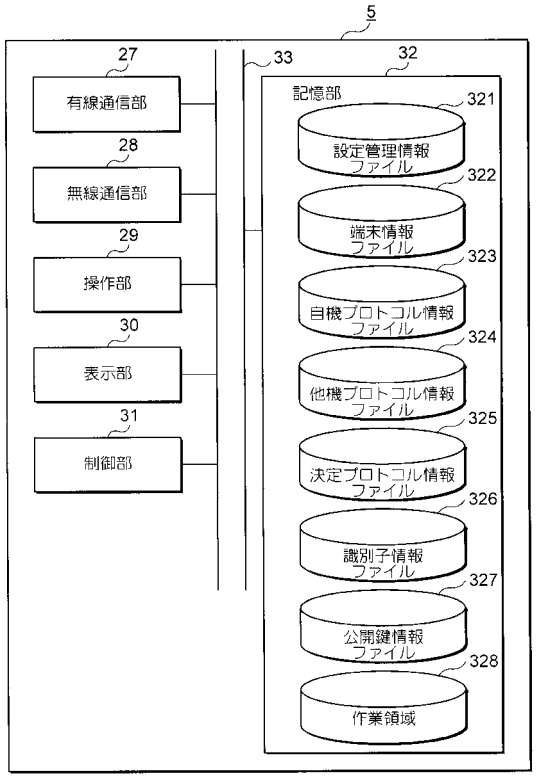
【図１７】



【図１８】



【図１９】



【図２０】

321

自機識別子	19ABB17A
パスワード	7bAIk8b#
秘密鍵	law#q&s26f9ry3q%soo%tleu
公開鍵	gc3rxwzjrf946s29p25c2$mp

【図２１】

323

MACアドレス	プロトコルセット	パラメータセット			
		パラメータ1	パラメータ2	パラメータ3	・・・
A05CBE6ADEE5	IEEE802.11b - NetBEUI	IEEE802.11b モード＝AdHoc	IEEE802.11b チャンネルID＝5	—	・・・
A05CBE6ADEE5	IEEE802.11b - TCP/IP	IEEE802.11b モード＝AdHoc	IEEE802.11b チャンネルID＝5	IPアドレス/サブネットマスク 192.168.0.60/ 255.255.255.0	・・・
BB2214AA3C1A	Bluetooth - NetBEUI	Bluetooth PIN Code＝ 7218	—	—	・・・
・・・	・・・	・・・	・・・	・・・	・・・

【図２２】

325

自機MACアドレス	他機MACアドレス	プロトコルセット	パラメータセット			
			パラメータ1	パラメータ2	パラメータ3	・・・
A05CBE6ADEE5	5FFD147EFFFF	IEEE802.11b - TCP/IP	IEEE802.11b モード＝AdHoc	IEEE802.11b チャンネルID＝3	IPアドレス/サブネットマスク 192.168.0.222/ 255.255.255.0	・・・
BB2214AA3C1A	ABF82A04D002	Bluetooth - NetBEUI	Bluetooth PIN=4E63	—	—	・・・
・・・	・・・	・・・	・・・	・・・	・・・	・・・

【図２３】

326

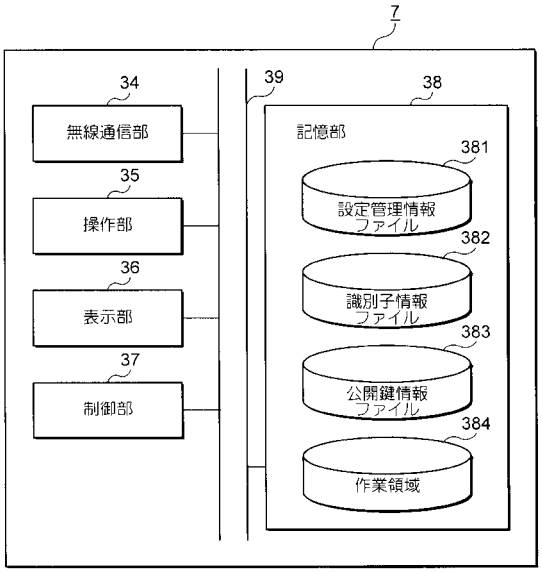
MACアドレス	識別子
B7614A795845	34FA9FF7
5FFD147EFFFF	32CCA022
ABF82A04D002	32CCA022
48D6A6626071	942D7BE6
・	・
・	・
・	・

【図２４】

327

識別子	公開鍵
0243B88E	tjfsjwrz#e5eyega$27db#%8
32CCA022	u#y#09v$3jqea%ivvz5ya0m5
3869B1F4	oc#&m6lbs%z7v#hip3ztha&1
・	・
・	・
・	・

【図２５】

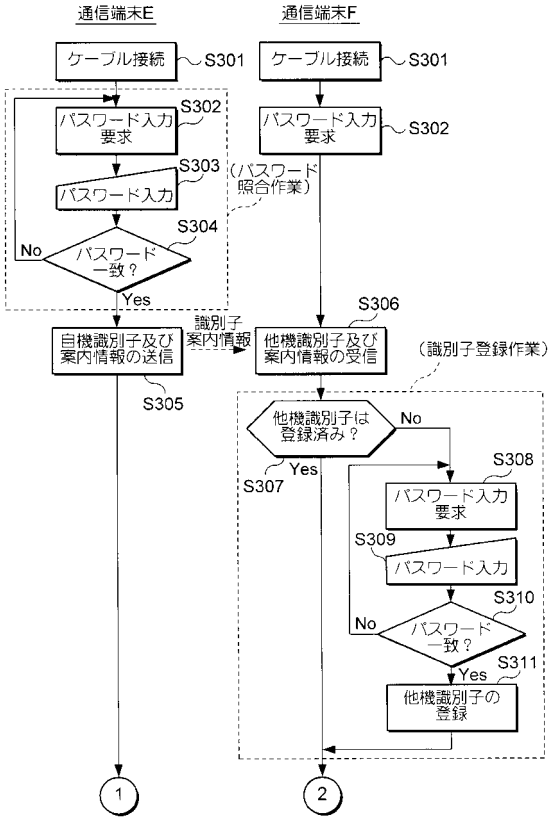


【図２６】

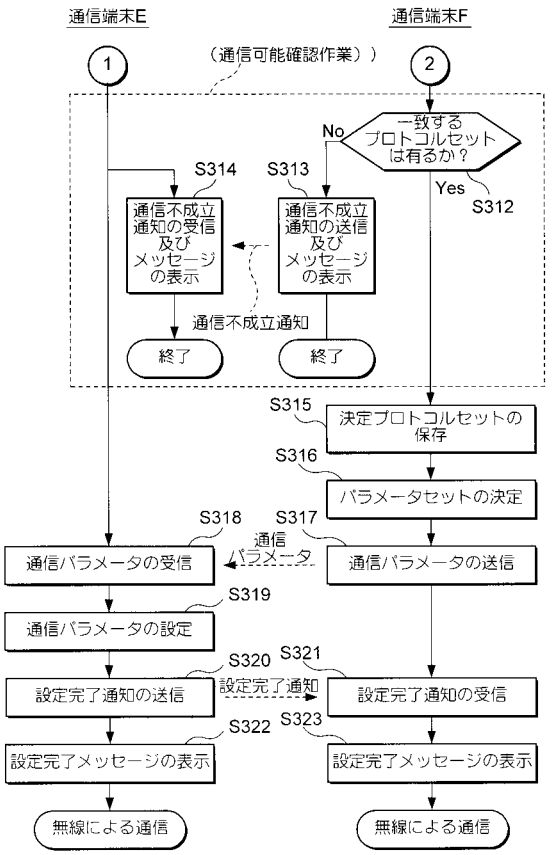
381

自機識別子	3869B1F4
秘密鍵	zw1y3u3g&uk5onlnls1mnlk$
公開鍵	oc#&m6lbs%z7v#hip3ztha&1

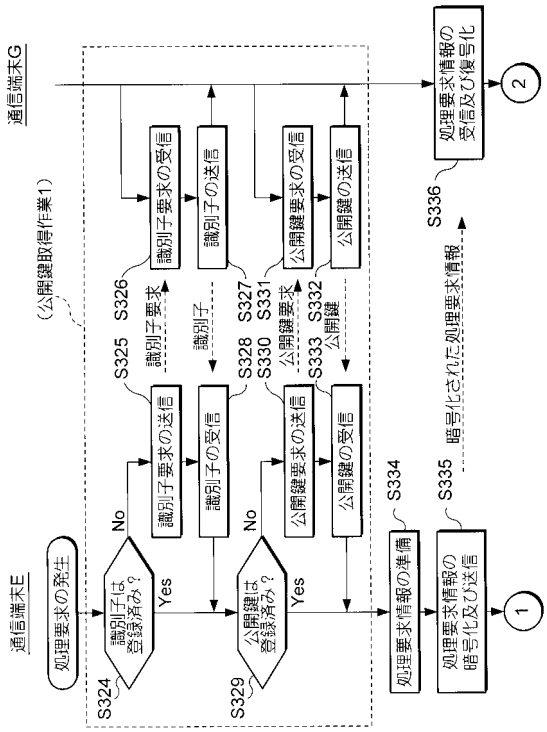
【図２７】



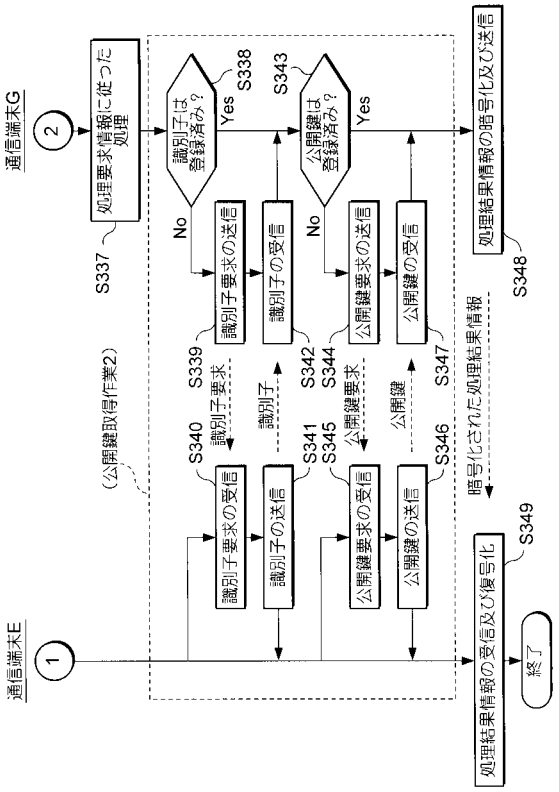
【図２８】



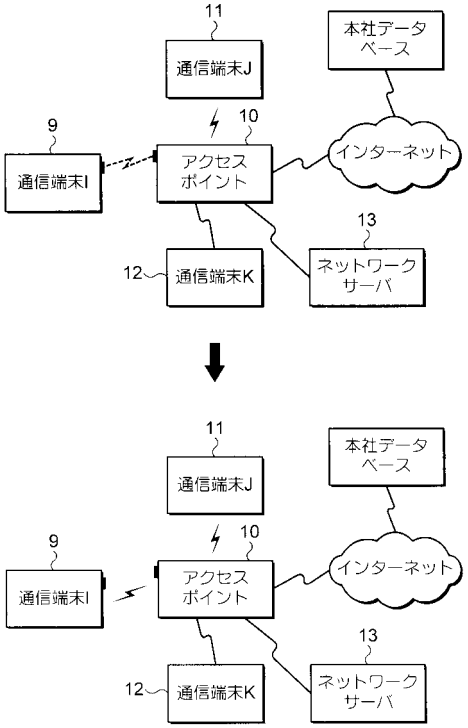
【図２９】



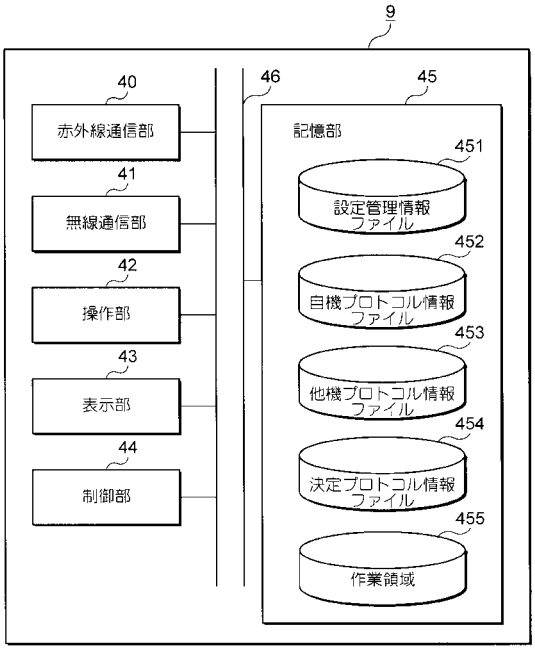
【図３０】



【図３１】



【図３２】

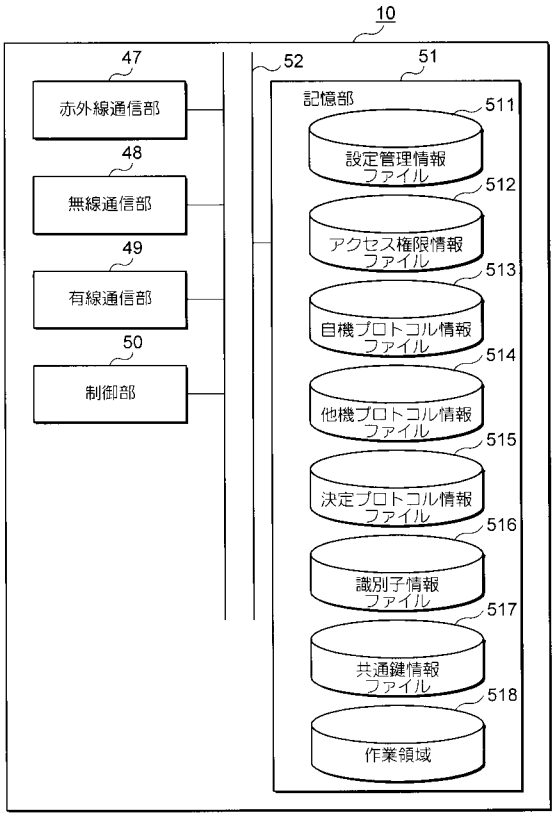


【図３３】

451

自機識別子	D24F7B85
パスワード	&rTqk$Q1
秘密鍵	$8j#fsbnf#y0tm8o3qml$36s
公開鍵	10tiz9#0vj5mciqgqb1j3z9b
共通鍵	#08dvq763&qkyda52xhua022

【図３４】



【図３５】

511

他機識別子	D24F7B85
他機公開鍵	10tiz9#0vj5mciqgqb1j3z9b

【図３６】

512

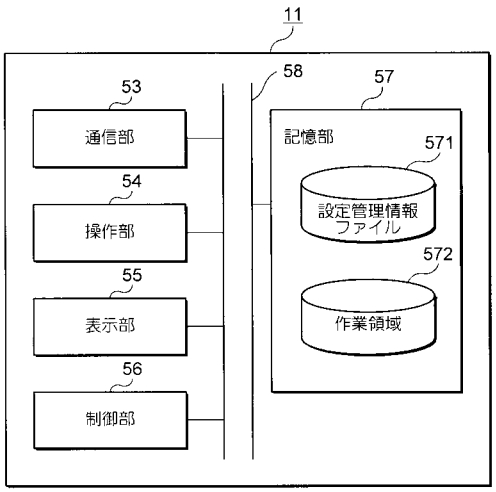
識別子	アカウント・グループ
8B78BF6A	同支部同セクション
D24F7B85	他支部
0C485394	同支部他セクション
・	・
・	・
・	・

【図３７】

517

識別子	共通鍵
46EB8684	2%76o7kimv8l3cw9#ume5qo6
CEAF30D5	$471t69xrkud69exhl%m5ntb
D24F7B85	#08dvq763&qkyda52xhua022
・	・
・	・
・	・

【図３８】

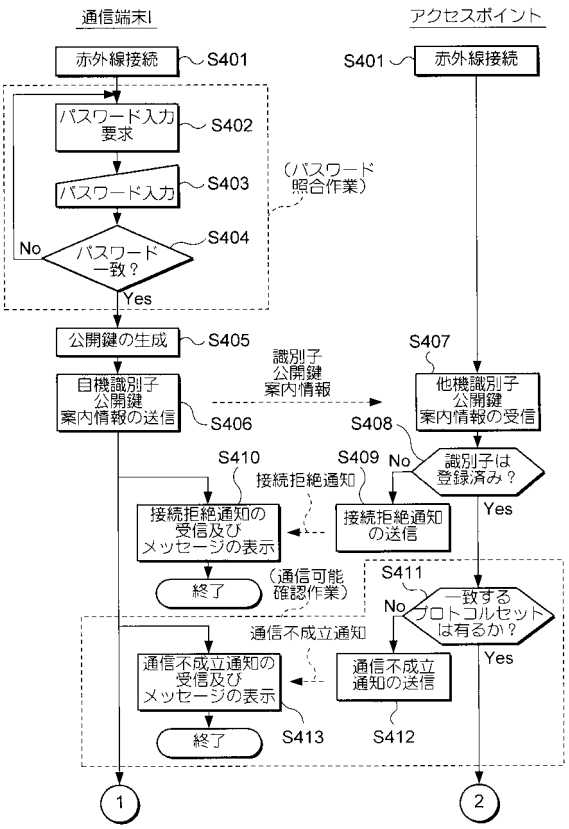


【図３９】

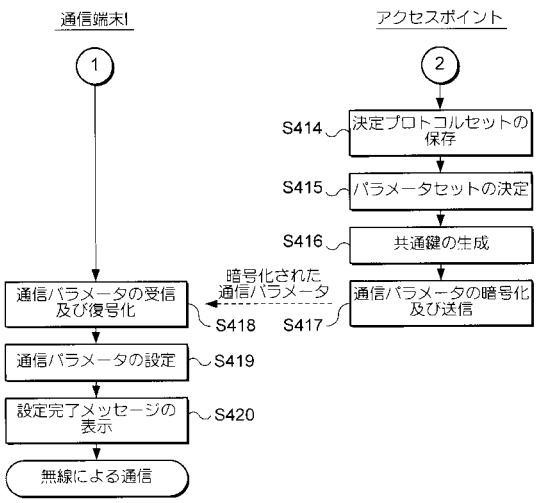
571

自機識別子	46EB8684
共通鍵	2%76o7kimv8l3cw9#ume5qo6

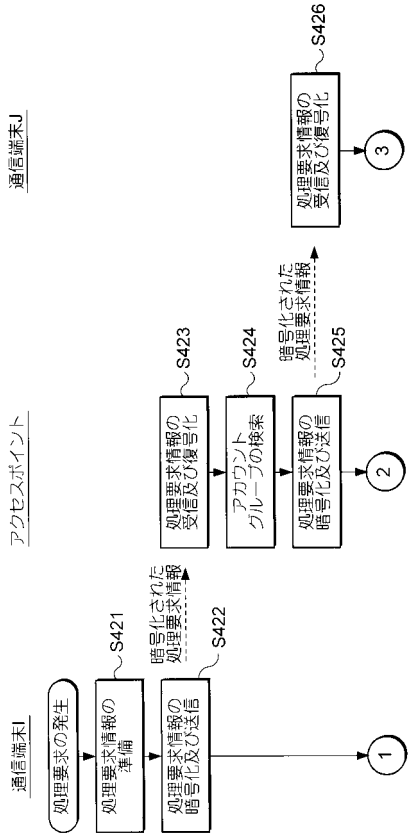
【図４０】



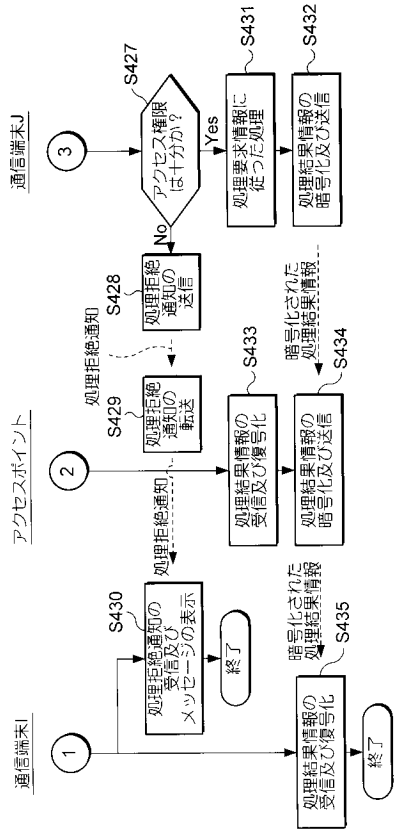
【図４１】


通信端末I
アクセスポイント
1
2
S414
決定プロトコルセットの保存
S415
パラメータセットの決定
S416
共通鍵の生成
暗号化された通信パラメータ
通信パラメータの受信及び復号化
S418
S417
通信パラメータの暗号化及び送信
通信パラメータの設定
S419
設定完了メッセージの表示
S420
無線による通信

【図４２】


通信端末J
アクセスポイント
通信端末J
処理要求の発生
処理要求情報の準備
S421
暗号化された処理要求情報
処理要求情報の暗号化及び送信
S422
処理要求情報の受信及び復号化
S423
アカウントグループの検索
S424
暗号化された処理要求情報
処理要求情報の暗号化及び送信
S425
処理要求情報の受信及び復号化
S426
1
2
3

【図４３】


通信端末J
アクセスポイント
通信端末I
3
2
1
アクセス権限は十分か？
S427
No
Yes
処理要求情報に従った処理
S431
処理結果情報の暗号化及び送信
S432
処理拒絶通知の送信
S428
処理拒絶通知
処理拒絶通知の転送
S429
処理結果情報の受信及び復号化
S433
暗号化された処理結果情報
処理結果情報の暗号化及び送信
S434
処理拒絶通知
処理拒絶通知の受信及びメッセージの表示
S430
終了
暗号化された処理結果情報
処理結果情報の受信及び復号化
S435
終了

フロントページの続き

(72)発明者　宮本　徹
長野県諏訪市大和３丁目３番５号　セイコーエプソン株式会社内

審査官　羽岡　さやか

(56)参考文献　特開平１１－３１３３７１（ＪＰ，Ａ）
特開平１０－２８５６５５（ＪＰ，Ａ）
特開平１１－１５０５４７（ＪＰ，Ａ）
特開平０９－２１８８３７（ＪＰ，Ａ）
特開２０００－２６１４６１（ＪＰ，Ａ）
特開２００１－０２８７８１（ＪＰ，Ａ）
特開平１０－２９０２４７（ＪＰ，Ａ）
ＰＨＳを使ったデータ伝送システムＰＩＡＦＳのテクニック，エレクトロニクス　ELECTRONICS MAGAZINE，日本，株式会社オーム社，１９９６年１０月　１日，第41巻

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L 12/28-46