(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2005-354136
(P2005-354136A)
(43)公開日　平成17年12月22日(2005.12.22)

(51)Int.Cl.[7]	F I		テーマコード（参考）
H04L 12/28	H04L 12/28	303	5K027
H04M 1/725	H04M 1/725		5K033
H04M 11/00	H04M 11/00	301	5K067
H04Q 7/38	H04B 7/26	109S	5K101

審査請求 未請求　請求項の数 6　OL　（全 12 頁）

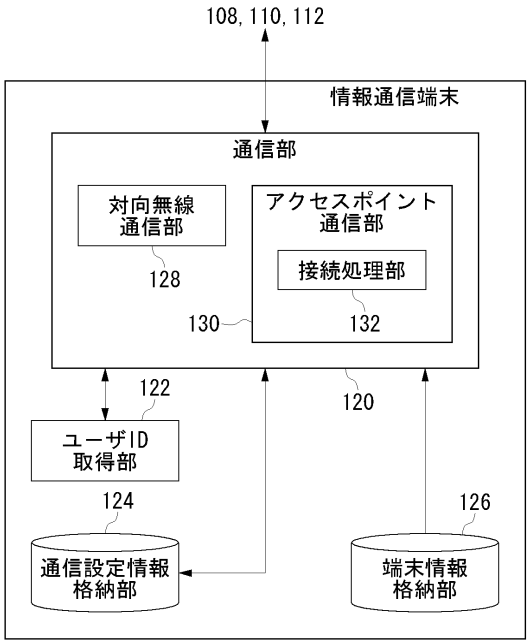
(21)出願番号　特願2004-169438 (P2004-169438)
(22)出願日　平成16年6月8日 (2004.6.8)

(71)出願人　000001889
三洋電機株式会社
大阪府守口市京阪本通２丁目５番５号
(74)代理人　100105924
弁理士　森下　賢樹
(72)発明者　橋爪　淳
大阪府守口市京阪本通２丁目５番５号　三洋電機株式会社内

Fターム(参考)　5K027 AA11 BB02 CC08 HH23 MM03
5K033 AA03 BA01 DA01 DA06 DA17
5K067 AA30 AA34 BB04 BB21 DD17
EE02 EE10 EE16 FF02 HH22
HH23 KK15
5K101 LL12 NN25 PP03 QQ09 RR05
RR27 SS07

(54)【発明の名称】通信端末装置、接続管理サーバおよび通信システム

(57)【要約】
【課題】　情報通信端末を所定の通信ネットワークに接続させるために必要とされる設定入力の煩雑さは、通信システムの利便性を低下させる。
【解決手段】　端末情報格納部１２６は、所定の構内通信網において情報通信端末１００を識別するために必要とされる情報である端末ＩＤを記憶する。対向無線通信部１２８は、非接触ＩＣメモリリーダライタ１１０に対し、近距離無線通信によって端末ＩＤを送信する。対向無線通信部１２８は、非接触ＩＣメモリリーダライタ１１０を介して端末ＩＤを受信した接続管理サーバから、当該情報通信端末１００が構内通信網と接続するために必要とする通信設定情報を非接触ＩＣメモリリーダライタ１１０を介した近距離無線通信により受信する。接続処理部１３２は、通信設定情報に基づいて、構内通信網と接続する。【選択図】　図２



【特許請求の範囲】
【請求項１】
通信機能を有する通信端末装置であって、
所定の構内通信網において当該端末装置を識別するために必要とされる情報である端末ＩＤを記憶する端末ＩＤ記憶部と、
当該端末装置と前記構内通信網の接続を支援する接続支援装置に対し、近距離無線通信によって前記端末ＩＤを送信する端末ＩＤ送信部と、
前記接続支援装置を介して前記端末ＩＤを受信した接続管理サーバから、当該端末装置が前記構内通信網と接続するために必要とする通信設定情報を前記接続支援装置を介した近距離無線通信により受信する通信設定情報受信部と、
前記通信設定情報に基づいて、前記構内通信網と接続する接続処理部と、
を備えることを特徴とする通信端末装置。
【請求項２】
ユーザを前記構内通信網において識別するために必要とされる情報であるユーザＩＤの入力を受け付けるユーザＩＤ入力部と、
近距離無線通信によって前記ユーザＩＤを前記接続支援装置に対して送信するユーザＩＤ送信部と、を更に備えることを特徴とする請求項１に記載の通信端末装置。
【請求項３】
所定の構内通信網において通信端末装置を識別するために必要とされる情報である端末ＩＤを、前記通信端末装置と前記構内通信網の接続を支援する接続支援装置を介して前記通信端末装置から受信する端末ＩＤ受信部と、
前記通信端末装置が前記構内通信網に接続するために必要とする通信設定情報を生成する通信設定情報生成部と、
前記生成された通信設定情報を、前記接続支援装置を介して前記通信端末装置に送信する通信設定情報送信部と、
を備えることを特徴とする接続管理サーバ。
【請求項４】
請求項１に記載の通信端末装置と、
請求項３に記載の接続管理サーバと、
近距離無線通信により前記通信端末装置とデータを送受信することにより、前記通信端末装置と前記構内通信網との接続を支援する接続支援装置と、
を備えることを特徴とする通信システム。
【請求項５】
通信端末装置を制御するためのコンピュータプログラムであって、
所定の構内通信網において前記通信端末装置を識別するために必要とされる情報である端末ＩＤを記憶する機能と、
前記通信端末装置と前記構内通信網の接続を支援する接続支援装置に対し、近距離無線通信によって前記端末ＩＤを送信する機能と、
前記接続支援装置を介して前記端末ＩＤを受信した接続管理サーバから、前記通信端末装置が前記構内通信網と接続するために必要とする通信設定情報を前記接続支援装置を介した近距離無線通信により受信する機能と、
前記通信設定情報に基づいて、前記構内通信網と接続する機能と、
をコンピュータに発揮させることを特徴とする通信プログラム。
【請求項６】
所定の構内通信網において通信端末装置を識別するために必要とされる情報である端末ＩＤを、前記通信端末装置と前記構内通信網の接続を支援する接続支援装置を介して前記通信端末装置から受信する機能と、
前記通信端末装置が前記構内通信網に接続するために必要とする通信設定情報を生成する機能と、
前記生成された通信設定情報を、前記接続支援装置を介して前記通信端末装置に送信す

る機能と、
　をコンピュータに発揮させることを特徴とする接続管理プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
　本発明は、移動通信技術に関し、とくに、移動通信端末が所定の通信ネットワークと接続するための設定処理に関する。
【背景技術】
【０００２】
　ブロードバンドネットワークの整備に伴い、いわゆるユビキタス社会への移行が進みつつある。現代の情報機器の多くは、ネットワークを介して、情報交換することを前提として設計されている。パーソナルコンピュータはもとより、ＰＤＡ（Personal Digital Assistance）などの携帯端末機器のアプリケーションソフトウェアにおいても、これらの機器が有する通信機能を利用するものは多い。
【特許文献１】特開２００３－３２４４４６号公報
【発明の開示】
【発明が解決しようとする課題】
【０００３】
　これらの通信機能を有する情報機器（以下、「情報通信端末」とよぶ）が、ＩＥＥＥ８０２．１１などにより規格策定される無線ＬＡＮ（Local Area Network）に接続するためには、さまざまな通信設定が必要である。たとえば、無線ＬＡＮとの接続においては、ＥＳＳＩＤ（Extended Service Set Identifier）やＷＥＰ（Wired Equivalent Privacy）キー、ＩＥＥＥ　８０２．１１ｉ／ＷＰＡ（Wi-Fi Protected Access）やＩＥＥＥ　８０２．１ｘにおいて認証に利用される電子証明書もしくはＰＳＫ（Pre shared key）など、無線ＬＡＮのセキュリティに関する各種情報を情報通信端末に設定する必要がある。また、無線ＬＡＮに接続するための通信設定情報は恒常的なものではなく、システムの運用変更に応じて、その設定を適宜変更する必要がある。
【０００４】
　このように、情報通信端末を所定の通信ネットワークに接続させるために必要とされる設定入力の煩雑さは、通信システムの利便性を低下させる。また、家電製品がネットワーク接続機能を有する場合には、その設定のための入力インタフェースを設けること自体が困難となる場合もある。
【０００５】
　本発明は、このような課題に鑑みてなされたものであり、その主たる目的は、簡便なインタフェースにより、情報通信端末が通信ネットワークと接続するために必要な設定を行うための技術を提供することである。
【課題を解決するための手段】
【０００６】
　上記課題を解決するために、本発明のある態様の通信端末装置は、所定の構内通信網において当該端末装置を識別するために必要とされる情報である端末ＩＤを記憶し、当該端末装置と構内通信網の接続を支援する接続支援装置に対し、近距離無線通信によって端末ＩＤを送信する。この装置は、接続支援装置を介して端末ＩＤを受信した接続管理サーバから、当該端末装置が構内通信網と接続するために必要とする通信設定情報を接続支援装置を介した近距離無線通信により受信し、その通信設定情報に基づいて構内通信網と接続する。
【０００７】
　この態様によると、通信端末装置は接続支援装置との近距離無線通信を介して、接続管理サーバとデータを送受信する。近距離無線通信とは、たとえば、ＲＦＩＤ（Radio Frequency-Identification）カード、ブルートゥース（bluetooth：登録商標）やＩｒＤＡ（Infrared Data Association）など、所定範囲内における電磁波や光を搬送波とする通信で

あってよい。なお、通信端末装置は、ピアツーピアの有線接続により、接続支援装置と接続してもよいし、直接接続管理サーバと接続してもよい。通信端末装置は、このような簡易な通信インタフェースにより、接続先として本来目的とする構内通信網に対する通信設定情報を取得できる。そのため、通信端末装置に通信設定情報を設定する上での大幅な省力化が可能となる。

【０００８】

本発明の別の態様は、接続管理サーバである。この接続管理サーバは、所定の構内通信網において通信端末装置を識別するために必要とされる情報である端末ＩＤを、通信端末装置と構内通信網の接続を支援する接続支援装置を介して通信端末装置から受信し、通信端末装置が構内通信網に接続するために必要とする通信設定情報を生成して接続支援装置を介して通信端末装置に送信する。

【０００９】

この態様によると、接続管理サーバは通信端末装置が通信ネットワークに接続するために必要な通信設定情報を生成する。また、その通信設定情報は、接続支援装置を介した近距離無線通信によって通信端末装置に送信される。そのため、通信端末装置のユーザにとっては、通信設定情報を自ら設定する手間が省かれるため、通信システムの利便性が向上する。

【発明の効果】

【００１０】

本発明によれば、情報通信端末が通信ネットワークと接続するための設定を簡便化する上で効果がある。

【発明を実施するための最良の形態】

【００１１】

図１は、本実施例における通信システム３００のハードウェア構成図である。ＬＡＮ１０６は、一般家庭などの屋内に設置される。ＬＡＮ１０６はゲートウェイ１０４を介して、インターネット１０２と接続される。同図において実線は有線接続を表す。また、破線は無線接続を表す。

【００１２】

ＬＡＮ１０６には、アクセスポイント１１２ａ、アクセスポイント１１２ｂ（以下、まとめていうときには、単に「アクセスポイント１１２」とよぶ）が接続される。各アクセスポイント１１２は、それぞれ所定のエリアを管理する。たとえば、アクセスポイント１１２ａが管理するエリア１４０ａは、リビングルームをカバーする。また、アクセスポイント１１２ｂが管理するエリア１４０ｂは、書斎をカバーする。エリア１４０ａ内のテレビ１１４やハードディスクレコーダ１１６は、アクセスポイント１１２ａを介してＬＡＮ１０６と接続する。同様に、エリア１４０ｂ内のパーソナルコンピュータ１１８は、アクセスポイント１１２ｂを介してＬＡＮ１０６と接続する。また、ＬＡＮ１０６は、ゲートウェイ１０４を介してインターネット１０２と接続される。アクセスポイント１１２にはルータ機能があってもよいし、アクセスポイント１１２とＬＡＮ１０６の間にルータを設置してもよい。

【００１３】

ＬＡＮ１０６には、非接触ＩＣメモリリーダライタ１１０が接続される。非接触ＩＣメモリリーダライタ１１０は、情報通信端末１００やＲＦＩＤカード１０８とＲＦＩＤプロトコルにより無線通信する。ＬＡＮ１０６に接続される接続管理サーバ２００は、情報通信端末１００がＬＡＮ１０６と接続するための制御を行う。接続管理サーバ２００と非接触ＩＣメモリリーダライタ１１０は、ＬＡＮ１０６を介さずにＵＳＢ（Universal Serial Bus）などのケーブルによって接続されてもよいし、アドホックモードにて無線通信してもよい。

【００１４】

情報通信端末１００は、デジタルカメラや携帯電話などのネットワーク接続機能を有する装置全般であってよい。すなわち、テレビ１１４やハードディスクレコーダ１１６、パ

ーソナルコンピュータ１１８も情報通信端末１００の一種である。ＲＦＩＤカード１０８は、ユーザをユニークに識別するための情報であるユーザＩＤを記憶する。ユーザＩＤは、通信システム３００について専用に設定されてもよい。あるいは、ユーザＩＤは、免許証番号などの汎用的に使用される情報であってもよい。すなわち、ＲＦＩＤカード１０８は、通信システム３００に対応した専用カードであってもよいが、非接触ＩＣチップを内蔵する運転免許証や住民カードなどの汎用のカードであってもよい。

【００１５】

ユーザがＲＦＩＤカード１０８と情報通信端末１００を非接触ＩＣメモリリーダライタ１１０にかざすと、非接触ＩＣメモリリーダライタ１１０はそれぞれからユーザＩＤと端末情報を読み取る。ここでいう端末情報とは、情報通信端末１００のＭＡＣ（Media Access Control）アドレス、情報通信端末１００の種別、非接触ＩＣメモリ固有のシリアル番号などの情報をいう。非接触ＩＣメモリリーダライタ１１０が読み取ったユーザＩＤと端末情報は、接続管理サーバ２００に送信される。なお、端末情報のうち、ＭＡＣアドレスのように、情報通信端末１００をユニークに識別する情報のことを、以下、「端末ＩＤ」とよぶ。端末ＩＤは、通信システム３００について専用に設定されてもよい。

【００１６】

接続管理サーバ２００は、登録ユーザとして複数のユーザのユーザＩＤを記憶している。接続管理サーバ２００は、非接触ＩＣメモリリーダライタ１１０により受信されたユーザＩＤが、登録ユーザのユーザＩＤとして登録されているか判定する。登録ユーザでなければ、接続を許可しない。このような方法により、ＬＡＮ１０６への不正ユーザによるアクセスを防ぐ。たとえば、情報通信端末１００が盗難されても、登録ユーザのユーザＩＤが記録されたＲＦＩＤカード１０８がなければ、情報通信端末１００はＬＡＮ１０６への接続を接続管理サーバ２００により拒否される。

【００１７】

情報通信端末１００とＬＡＮ１０６との接続を許可する場合には、接続管理サーバ２００は情報通信端末１００がＬＡＮ１０６に接続するために必要な情報である通信設定情報を非接触ＩＣメモリリーダライタ１１０を介して情報通信端末１００に送信する。ここでいう通信設定情報とは、ＥＳＳＩＤやＷＥＰＫＥＹ、ＩＥＥＥ　８０２．１１ｉ／ＷＰＡ（Wi-Fi Protected Access）やＩＥＥＥ　８０２．１ｘにおいて認証に利用される電子証明書もしくはＰＳＫ（Pre shared key）、アクセスポイント１１２のＭＡＣアドレスや通信チャネルなどをいう。情報通信端末１００は、非接触ＩＣメモリリーダライタ１１０から送信された通信設定情報を内蔵メモリに記録する。情報通信端末１００は、エリア１４０ａやエリア１４０ｂなどの各エリアに入ると、記録した通信設定情報に基づいて、各アクセスポイント１１２と接続する。以下、ユーザが情報通信端末１００とＲＦＩＤカード１０８を非接触ＩＣメモリリーダライタ１１０にかざして、情報通信端末１００をＬＡＮ１０６と接続させるための操作のことを、「登録依頼操作」とよぶ。

【００１８】

この態様によれば、情報通信端末１００のユーザは、情報通信端末１００とＲＦＩＤカード１０８を非接触ＩＣメモリリーダライタ１１０にかざすだけで、ＬＡＮ１０６と接続するために必要な通信設定がなされる。なお、情報通信端末１００は、ユーザＩＤを記録した記録媒体からユーザＩＤを読み取り、端末情報と併せて非接触ＩＣメモリリーダライタ１１０に送信してもよい。この場合には、この記録媒体が非接触ＩＣチップを内蔵することは必須条件ではない。

【００１９】

情報通信端末１００が、たとえば、大型テレビのように可搬性を有しない、または、可搬性に乏しい装置である場合には、情報通信端末１００自体を非接触ＩＣメモリリーダライタ１１０にかざすことは現実的ではない。この場合には、大型テレビのうちＬＡＮ１０６と接続するために必要な機能を端末用ＲＦＩＤカードとして別個に設けてもよい。この場合、ユーザはこの端末用ＲＦＩＤカードとユーザＩＤ用のＲＦＩＤカード１０８を非接触ＩＣメモリリーダライタ１１０にかざすことにより、通信設定情報を端末用ＲＦＩＤカ

ードに記憶させる。この装置は端末用ＲＦＩＤカードからその通信設定情報を装置に内蔵または外付けされる非接触ＩＣリーダライタに読み込ませる。これにより、装置はアクセスポイント１１２と接続する。あるいは、非接触ＩＣメモリリーダライタ１１０そのものを携帯可能に構成してもよい。その場合、ユーザは非接触ＩＣメモリリーダライタ１１０を大型テレビとＲＦＩＤカード１０８にかざすことにより、通信設定情報を取得する。

【００２０】

図２は、情報通信端末１００の機能ブロック図である。ここに示す各ブロックは、ハードウェア的には、コンピュータのＣＰＵをはじめとする素子や機械装置で実現でき、ソフトウェア的にはコンピュータプログラム等によって実現されるが、ここでは、それらの連携によって実現される機能ブロックを描いている。したがって、これらの機能ブロックはハードウェア、ソフトウェアの組合せによっていろいろなかたちで実現できることは、当業者には理解されるところである。

【００２１】

情報通信端末１００は、通信部１２０、ユーザＩＤ取得部１２２、通信設定情報格納部１２４および端末情報格納部１２６を含む。通信部１２０は、外部との通信処理を行う。通信設定情報格納部１２４は、通信設定情報を格納する。端末情報格納部１２６は、端末情報を格納する。端末情報格納部１２６は、たとえば、ＲＯＭ（Read Only Memory）であってもよい。ユーザＩＤ取得部１２２は、必要に応じてＲＦＩＤカード１０８からユーザＩＤを取得する。

【００２２】

通信部１２０は、対向無線通信部１２８とアクセスポイント通信部１３０を含む。対向無線通信部１２８は、非接触ＩＣメモリリーダライタ１１０と無線通信によりデータを送受信する。情報通信端末１００を非接触ＩＣメモリリーダライタ１１０にかざすと、対向無線通信部１２８は端末情報格納部１２６が格納する端末情報を非接触ＩＣメモリリーダライタ１１０に送信する。図１に関連して説明したようにユーザＩＤは、ＲＦＩＤカード１０８から非接触ＩＣメモリリーダライタ１１０に送信される。あるいは、ユーザＩＤ取得部１２２がユーザＩＤを取得して、対向無線通信部１２８が端末情報と併せてユーザＩＤを送信してもよい。

【００２３】

対向無線通信部１２８は、接続管理サーバ２００から非接触ＩＣメモリリーダライタ１１０を介して通信設定情報を受信し通信設定情報格納部１２４に格納する。アクセスポイント通信部１３０は、アクセスポイント１１２と無線通信によりデータを送受信する。アクセスポイント通信部１３０は、更に接続処理部１３２を含む。接続処理部１３２は、通信設定情報格納部１２４に格納される通信設定情報に基づいて、各アクセスポイント１１２との接続処理を実行する。

【００２４】

図３は、接続管理サーバ２００の機能ブロック図である。ここに示す各ブロックも、ハードウェア的には、コンピュータのＣＰＵをはじめとする素子や機械装置で実現でき、ソフトウェア的にはコンピュータプログラム等によって実現されるが、ここでは、それらの連携によって実現される機能ブロックを描いている。したがって、これらの機能ブロックはハードウェア、ソフトウェアの組合せによっていろいろなかたちで実現できることは、当業者には理解されるところである。

【００２５】

接続管理サーバ２００は、リーダライタインタフェース処理部２０２、接続管理部２０４、設定入力部２０６、登録ユーザ格納部２０８および接続設定情報格納部２１０を含む。リーダライタインタフェース処理部２０２は、非接触ＩＣメモリリーダライタ１１０とのインタフェース処理を担当する。接続管理部２０４は、情報通信端末１００のＬＡＮ１０６との接続を統括的に管理する。登録ユーザ格納部２０８は、登録ユーザのユーザＩＤを格納する。接続設定情報格納部２１０は、接続設定情報を格納する。接続設定情報格納部２１０のデータ構造については、図４に関連して後述する。設定入力部２０６は、接続

設定情報について権限のあるユーザからの設定入力を受け付ける。この入力は、接続管理サーバ２００のキーボードやマウスなどの入力デバイスを介してなされてもよいし、ＬＡＮ１０６を介して外部からなされてもよい。入力データはそれぞれ、登録ユーザ格納部２０８や接続設定情報格納部２１０に格納される。また、ユーザからの入力ではなく接続管理サーバ２００が乱数を利用して自動生成してもよい。

【００２６】

リーダライタインタフェース処理部２０２は、端末情報取得部２２０、ユーザＩＤ取得部２２２および通信設定情報送信部２２４を含む。端末情報取得部２２０は、情報通信端末１００から端末情報を取得する。ユーザＩＤ取得部２２２は、ＲＦＩＤカード１０８からユーザＩＤを取得する。通信設定情報送信部２２４は、通信設定情報生成部２１６が生成する通信設定情報を情報通信端末１００に送信する。

【００２７】

接続管理部２０４は、接続可否判定部２１２、メール送受信部２１４、通信設定情報生成部２１６および端末登録部２１８を含む。接続可否判定部２１２は、接続依頼操作に対する接続可否を判定する。登録ユーザでないユーザによる接続依頼操作の場合、接続可否判定部２１２は、情報通信端末１００とＬＡＮ１０６との接続を許可しない。

【００２８】

メール送受信部２１４は、ユーザが各情報通信端末１００を操作してデータを送受信するときの制限解除のために、管理者と電子メールを送受信する。本実施例においては、登録ユーザであっても、アクセスポイント１１２が管理するすべてのエリアにある機器（テレビ１１４、ハードディスクレコーダ１１６、パソコン１１８）をネットワーク経由にて操作できるわけではなく、所定の制限を受ける場合がある。以下、情報通信端末１００を利用して、ＬＡＮ１０６を介したアクセスポイント１１２が管理するすべてのエリアにある機器（テレビ１１４、ハードディスクレコーダ１１６、パソコン１１８）の操作をいうときには、「ネットワーク経由操作」とよぶ。たとえば、リビングルームのテレビ１１４やハードディスクレコーダ１１６は、登録ユーザであればだれでもネットワーク経由操作できるが、書斎のパソコン１１８は、一部の登録ユーザしかネットワーク経由操作できないとしてもよい。書斎のパソコン１１８をネットワーク経由操作する権限を有しないユーザが、ネットワーク経由操作を行おうとするとき、メール送受信部２１４は管理者として指定されたユーザに対して、許可を求める旨のメールを自動送信する。管理者から許可する旨のメールが受信されると、当該ユーザは当該情報通信端末１００をネットワークに接続できるようになり、書斎のパソコン１１８をネットワーク経由操作できるようになる。更に詳しくは、次の図４以降に関連して後述する。通信設定情報生成部２１６は、接続依頼操作に対して接続を許可する場合に送信すべき通信設定情報を生成する。端末登録部２１８は、アクセスポイント１１２やゲートウェイ１０４、アクセスポイント１１２が管理する任意の機器(ハードディスクレコーダ１１６、パソコン１１８等)の中で、必要な機器に対して、各情報通信端末１００の端末情報を登録する。

【００２９】

図４は、接続設定情報格納部２１０のデータ構造図である。アクセスポイントＩＤ欄２３０は、各アクセスポイント１１２を識別するアクセスポイントＩＤを示す。端末ＩＤ欄２３２は、端末ＩＤを示す。管理者ＩＤ欄２３４は、各アクセスポイント１１２が担当するエリア１４０の管理者として設定されるユーザのユーザＩＤを示す。

【００３０】

管理者は、各情報通信端末１００を操作する上で制限を受けない。管理者は、接続設定情報を設定変更する権限を有する。ファミリー権限欄２３６は、ファミリーユーザとして設定されるユーザの各情報通信端末１００に対するネットワーク経由操作の権限を示す。ファミリーユーザは登録ユーザのうち、管理者以外のユーザである。ファミリーユーザは、各情報通信端末１００をネットワーク経由操作する上で一定の制限を受ける。ゲスト権限欄２３８はゲストユーザとして設定されるユーザの各情報通信端末１００におけるネットワーク経由操作の権限を示す。ゲストユーザは、ゲストカードとよばれるゲスト専用の

ユーザＩＤ（以下、「ゲストＩＤ」とよぶ）が記録されたＲＦＩＤカード１０８によって、各情報通信端末１００をネットワーク経由操作する。すなわち、ゲストユーザは特殊な登録ユーザとして扱われる。ゲストユーザは、特別な登録ユーザとして情報通信端末１００を操作可能である。ゲストユーザによるネットワーク経由操作も一定の制限を受ける。アドレス欄２４０は、管理者の電子メールアドレスを示す。

【００３１】

ユーザは、ＬＡＮ１０６に接続された情報通信端末１００を利用して、ネットワーク経由操作するときには、当該情報通信端末１００と自己のＲＦＩＤカード１０８を、非接触ＩＣメモリリーダライタ１１０にかざす。情報通信端末１００は、受信した通信設定情報を利用してネットワークに接続する。更に、ユーザＩＤ取得部１２２により取得したユーザＩＤを利用して、任意の機器（ハードディスクレコーダ１１６、パソコン１１８等）に接続する。端末登録部２１８は、接続設定情報に基づいて、各機器に設定制御の為の情報を登録している。すなわち、情報通信端末１００は、ネットワークに接続しても、ユーザＩＤに依存して、操作可能な機器が制限される。

【００３２】

同図において、アクセスポイントＩＤ「０１」のアクセスポイント１１２には、端末ＩＤが「０４」、「０６」および「０８」の３つの情報通信端末１００が接続許可されている。たとえば、端末ＩＤ「０４」の情報通信端末１００を利用して、ユーザＩＤ「０２」の管理者であるユーザがネットワーク経由操作をするとき、情報通信端末１００は、端末ＩＤ「０４」をアクセスポイントＩＤ「０１」のアクセスポイント１１２に送信する。接続設定情報に従い、当該アクセスポイント１１２は、端末「０４」に基づくデータの送受信を制限しない。続いて、ユーザＩＤ「０２」に基づいて、任意の機器に接続する。そのため、この管理者であるユーザは、当該情報通信端末１００を当該アクセスポイント１１２に接続させた上で、外部機器とデータを送受信可能となる。すなわち、当該ユーザは、当該情報通信端末１００を制限無くネットワーク経由操作することができる。

【００３３】

一方、この情報通信端末１００をユーザＩＤ「０１」のファミリーユーザがネットワーク経由操作をする場合にも、情報通信端末１００は端末ＩＤ「０４」をアクセスポイント１１２に送信し、ユーザＩＤ「０１」に基づいて、任意の機器に接続する。同図において、端末ＩＤ「０４」の情報通信端末１００のファミリーユーザによるネットワーク経由操作は、受信のみが許可されている。すなわち、ゲートウェイ１０４に受信のみ登録されており、外部機器からＬＡＮ１０６を経由してデータを受信することは可能であるが、データを外部に送信することはできない。この場合、当該情報通信端末１００の接続対象となる任意の機器もしくはゲートウェイ１０４は、当該装置へのデータ転送は制限しないが、当該装置からのデータ転送を制限する。

【００３４】

アクセスポイント１１２がデータ転送を制限するとき、アクセスポイント１１２は、対象となっている端末ＩＤ「０４」を接続管理サーバ２００に送信する。メール送受信部２１４は、端末ＩＤ「０４」について、管理者として設定されているユーザの電子メールアドレスをアドレス欄２４０を参照して検出する。同図においては、「ａｘａ@ｘｘｘ．ｃｏｍ」である。この電子メールアドレスは、たとえば、管理者の携帯電話やノートパソコンなどのアドレスであってよい。

【００３５】

メール送受信部２１４は、この電子メールアドレスを送信先として、データ転送許可を依頼する旨の電子メールを自動送信する。メール送受信部２１４は、管理者により接続を許可する旨の回答を受信すると、当該アクセスポイント１１２にこれを通知する。これにより、アクセスポイント１１２の設定は一時的に変更され、ファミリーユーザであっても端末ＩＤ「０４」を介して外部へデータ送信できるようになる。同図において、ゲストユーザは端末ＩＤ「０４」の情報通信端末１００をアクセスポイント１１２に接続させることはできないが、この場合にも、管理者からの許可があれば一時的に接続を許可される。

【００３６】
より具体的な一例として、たとえば、ユーザがネットワーク接続機能を有するデジタルカメラによりパーソナルコンピュータに保存されている画像を参照したり、撮影した画像を保存する場合を示す。このときユーザはＲＦＩＤカード１０８とデジタルカメラを、非接触ＩＣメモリリーダライタ１１０にかざして、デジタルカメラはＲＦＩＤカード１０８のユーザＩＤの権限で接続設定情報と通信設定情報を読み取り、端末情報(端末ＩＤ)を報告する。ここで接続管理サーバ２００は、管理者に対して、ネットワーク接続報告する為、電子メールを送信し、管理者から接続許可する旨の回答を受信する。接続管理サーバ２００は、接続許可のメールを受信すると、該当するアクセスポイント１１２に、端末情報を登録する。デジタルカメラは、読み取った通信設定情報を利用してネットワークに接続し、更に、読み取ったユーザＩＤを利用して、パーソナルコンピュータにログインする。こうしてデジタルカメラは、保存されている画像を参照したり、撮影した画像を保存する。

【００３７】
図１に基づいて説明すれば、このとき該当するアクセスポイント１１２が、デジタルカメラがネットワークに接続させるか否かを判定する。管理者から接続許可メールを受信している場合、ネットワーク接続可能となり、当該ユーザＩＤがパーソナルコンピュータ１１８に対するログイン権限を有していれば、パーソナルコンピュータ１１８内の画像データ等を、送受信することが可能となる。一方、管理者から接続許可メールを受信していない場合は、たとえ当該ユーザＩＤが、パーソナルコンピュータ１１８に対するログイン権限を有している場合でも、ネットワーク接続できない為、パーソナルコンピュータ１１８内の画像データ等を、利用することができない。

【００３８】
このように、端末情報(端末ＩＤ)によって、アクセスポイント１１２に対する接続可否を簡単に管理する為、不正なアクセスを防止しやすい。また、電子メールを利用した管理者に対する確認により、予め設定された接続設定情報に関わらず、柔軟に通信システム３００を運用することができる。

【００３９】
図５は、情報通信端末１００をＬＡＮ１０６に接続させるときの情報通信端末１００を中心とした処理過程を示すフローチャートである。ユーザが情報通信端末１００とＲＦＩＤカード１０８を非接触ＩＣメモリリーダライタ１１０にかざすとき、ＲＦＩＤカード１０８からユーザＩＤが非接触ＩＣメモリリーダライタ１１０に送信される（Ｓ１０）。ユーザＩＤ取得部１２２がＲＦＩＤカード１０８からユーザＩＤを取得し、対向無線通信部１２８がこれを送信してもよい。通信部１２０は、端末情報格納部１２６から端末情報を読み出す（Ｓ１２）。対向無線通信部１２８は、読み出された端末情報を非接触ＩＣメモリリーダライタ１１０に送信する（Ｓ１４）。

【００４０】
対向無線通信部１２８は、非接触ＩＣメモリリーダライタ１１０を介して接続管理サーバ２００から通信設定情報を受信する。所定時間内に受信できなければ（Ｓ１６のＮ）、接続失敗として処理は終了する。接続管理サーバ２００の接続可否判定部２１２は、非接触ＩＣメモリリーダライタ１１０を介して受信したユーザＩＤが、登録ユーザのユーザＩＤでない場合には、通信設定情報送信を拒否する。対向無線通信部１２８が、接続管理サーバ２００から通信設定情報の受信に成功すると（Ｓ１６のＹ）、対向無線通信部１２８は通信設定情報を通信設定情報格納部１２４に保存する（Ｓ１８）。情報通信端末１００は、各エリア１４０内においてそのエリアを担当するアクセスポイント１１２に接続処理を実行する。ただし、図４に関連して説明したように、接続が許可されていない場合には、アクセスポイント１１２により接続拒否される。

【００４１】
図６は、情報通信端末１００をＬＡＮ１０６に接続させるときの接続管理サーバ２００の処理過程を示すフローチャートである。ユーザが、ＲＦＩＤカード１０８と情報通信端

末１００を非接触ＩＣメモリリーダライタ１１０にかざすと、ユーザＩＤ取得部２２２は、非接触ＩＣメモリリーダライタ１１０を介してユーザＩＤを受信する（Ｓ３０）。端末情報取得部２２０は、同様に非接触ＩＣメモリリーダライタ１１０を介して端末ＩＤを受信する（Ｓ３２）。接続可否判定部２１２は、ユーザＩＤが登録ユーザのユーザＩＤであるか判定して、当該ユーザによる情報通信端末１００の接続可否を判定する（Ｓ３４）。接続が許可されると（Ｓ３６のＹ）、端末登録部２１８は各アクセスポイント１１２に対して当該情報通信端末１００に関する端末ＩＤ等の接続設定情報を接続設定情報格納部２１０から読み出して登録する（Ｓ４４）。次に、通信設定情報生成部２１６は情報通信端末１００がＬＡＮ１０６と接続するための設定である通信設定情報を生成する（Ｓ４６）。通信設定情報送信部２２４は、非接触ＩＣメモリリーダライタ１１０からその通信設定情報を送信する（Ｓ４８）。

【００４２】

一方、Ｓ３６において、接続が許可されていなければ（Ｓ３６のＮ）、端末登録部２１８は各アクセスポイント１１２に当該情報通信端末１００の端末ＩＤを接続が許可されない情報通信端末１００として登録する（Ｓ４２）。これにより当該情報通信端末１００はＬＡＮ１０６のいずれのアクセスポイント１１２とも接続不能となり、不正に情報通信端末１００がＬＡＮ１０６と接続されないように処置される。

【００４３】

以上、実施例にもとづいて、本発明を説明した。本実施例によれば、ＲＦＩＤなどのユーザに負担のかからないユーザインタフェースにより、ネットワークに接続するための設定を簡単に行うことができる。また、ユーザＩＤによって、情報通信端末１００の使用者を認識することにより、ユーザに応じた情報通信端末１００の制御が可能となる。

【００４４】

以上、実施の形態をもとに本発明を説明した。なお本発明はこの実施の形態に限定されることなく、そのさまざまな変形例もまた、本発明の態様として有効である。

【００４５】

本実施例においては、接続管理サーバ２００の接続可否判定部は、非接触ＩＣメモリリーダライタ１１０にアクセスしてきたユーザが登録ユーザやゲストユーザでなければ、情報通信端末１００の接続を許可しないとして説明した。

これとは別に、アクセスしてきたユーザが登録ユーザやゲストユーザであるか否かにかかわらず、情報通信端末１００は無線ＬＡＮ１０６と接続可能としてもよい。端末情報は各アクセスポイント１１２に一旦登録され、情報通信端末１００には、非接触ＩＣメモリリーダライタ１１０を介して通信設定情報が送信される。

【００４６】

情報通信端末１００が非接触ＩＣメモリリーダライタ１１０に端末情報を送信すると、接続管理サーバ２００は、予め管理者として登録しているユーザに対し、接続がなされた旨を電子メールにて通知する。このメールには、接続してきたユーザ名や端末名などについて記載される。管理者は、電子メールを確認し、接続を許可してもよい場合には、その旨を返信する。あるいは、所定時間返信しないことを以て許可としてもよい。接続させたくないときには、管理者は所定のフォームにて不許可の旨を示す電子メールを接続管理サーバ２００に送信する。接続管理サーバ２００は、管理者から接続不許可の旨の電子メールを受信すると、各アクセスポイント１１２のＭＡＣアドレスフィルタを制御して、当該情報通信端末１００の接続を拒否するように設定変更してもよい。このような方法により、管理者が認めないユーザによる無線ＬＡＮ１０６へのアクセスを制限することができる。

【００４７】

本実施例においては、各情報通信端末１００についてのネットワーク経由操作を対象として説明したが、各情報通信端末１００の各機能に対してユーザごとの権限がさだめられてもよい。たとえば、ハードディスクレコーダに記録されるデータの一部しか読み出せないユーザと、すべてを読み出せるユーザが設定されてもよい。これにより、各情報通信端

末１００の有するデータをきめ細かく制御することができる。

【図面の簡単な説明】

【００４８】

【図１】本実施例における通信システムのハードウェア構成図である。

【図２】情報通信端末の機能ブロック図である。

【図３】接続管理サーバの機能ブロック図である。

【図４】接続設定情報格納部のデータ構造図である。

【図５】情報通信端末を無線ＬＡＮに接続させるときの情報通信端末を中心とした処理過程を示すフローチャートである。

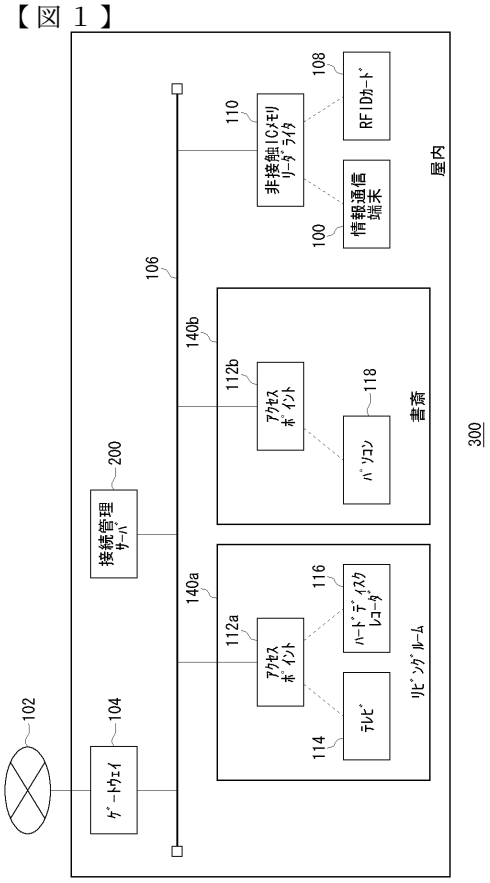
【図６】情報通信端末を無線ＬＡＮに接続させるときの接続管理サーバの処理過程を示すフローチャートである。

【符号の説明】

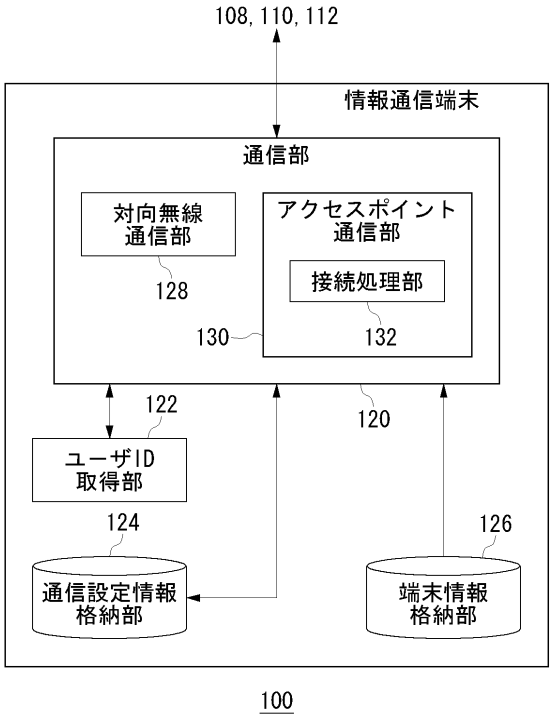
【００４９】

１００　情報通信端末、１０６　ＬＡＮ、１０８　ＲＦＩＤカード、１１０　非接触ＩＣメモリリーダライタ、１１２　アクセスポイント、１２０　通信部、１２２　ユーザＩＤ取得部、１２４　通信設定情報格納部、１２６　端末情報格納部、１２８　対向無線通信部、１３０　アクセスポイント通信部、１３２　接続処理部、２００　接続管理サーバ、２０２　リーダライタインタフェース処理部、２０４　接続管理部、２０６　設定入力部、２０８　登録ユーザ格納部、２１０　接続設定情報格納部、２１２　接続可否判定部、２１４　メール送受信部、２１６　通信設定情報生成部、２１８　端末登録部、２２０　端末情報取得部、２２２　ユーザＩＤ取得部、２２４　通信設定情報送信部、３００　通信システム。

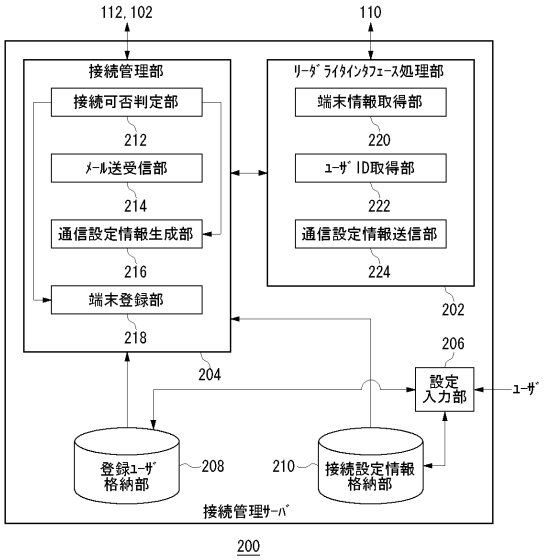
【図１】



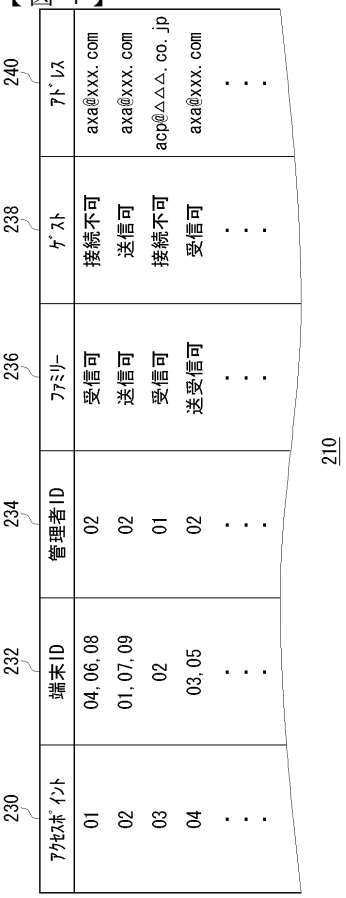
【図２】



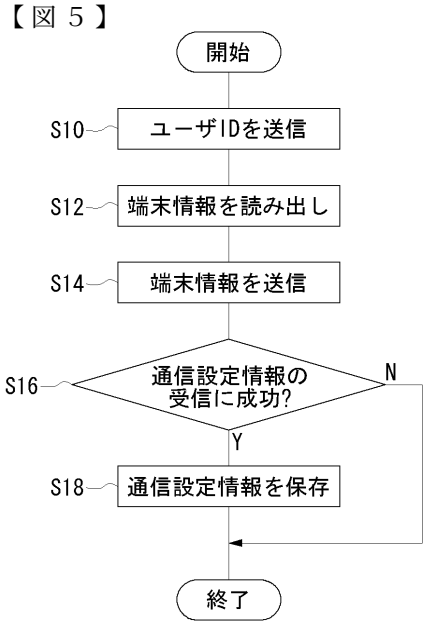
【図３】


112,102
110
接続管理部
接続可否判定部
212
ﾒｰﾙ送受信部
214
通信設定情報生成部
216
端末登録部
218
204
ﾘｰﾀﾞｰﾗｲﾀｲﾝﾀﾌｪｰｽ処理部
端末情報取得部
220
ﾕｰｻﾞIID取得部
222
通信設定情報送信部
224
202
206
設定入力部
ﾕｰｻﾞ
登録ﾕｰｻﾞ格納部
208
210
接続設定情報格納部
接続管理ｻｰﾊﾞ
200

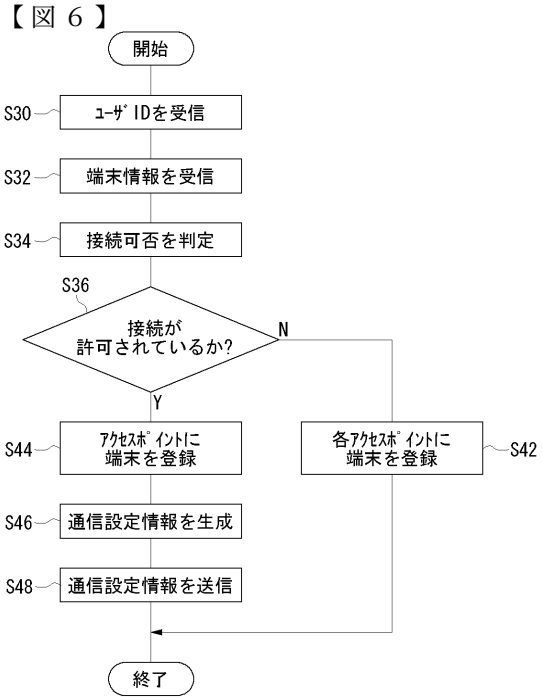
【図４】


240
ｱﾄﾞﾚｽ
axa@xxx.com
axa@xxx.com
acp@△△△.co.jp
axa@xxx.com
238
ｹﾞｽﾄ
接続不可
送信可
接続不可
受信可
236
ﾌｧﾐﾘｰ
受信可
送信可
受信可
送受信可
234
管理者ID
02
02
01
02
232
端末ID
04,06,08
01,07,09
02
03,05
230
ｱｸｾｽﾎﾟｲﾝﾄ
01
02
03
04
210

【図５】


開始
S10
ユーザIDを送信
S12
端末情報を読み出し
S14
端末情報を送信
S16
通信設定情報の受信に成功?
N
Y
S18
通信設定情報を保存
終了

【図６】


開始
S30
ﾕｰｻﾞIDを受信
S32
端末情報を受信
S34
接続可否を判定
S36
接続が許可されているか?
N
Y
S44
ｱｸｾｽﾎﾟｲﾝﾄに端末を登録
S42
各ｱｸｾｽﾎﾟｲﾝﾄに端末を登録
S46
通信設定情報を生成
S48
通信設定情報を送信
終了