

(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2006-313975

(P2006-313975A)

(43) 公開日 平成18年11月16日(2006.11.16)

(51) Int. Cl.	F I			テーマコード (参考)
HO4M 11/00 (2006.01)	HO4M	11/00	303	5J104
HO4M 1/00 (2006.01)	HO4M	1/00	J	5K027
HO4M 3/00 (2006.01)	HO4M	3/00	B	5K201
HO4L 9/32 (2006.01)	HO4L	9/00	673A	

審査請求 未請求 請求項の数 4 O L (全 12 頁)

(21) 出願番号	特願2005-135211 (P2005-135211)	(71) 出願人	000002130 住友電気工業株式会社 大阪府大阪市中央区北浜四丁目5番33号
(22) 出願日	平成17年5月6日(2005.5.6)	(71) 出願人	502312498 住友電工ネットワークス株式会社 東京都品川区東五反田三丁目20番14号
		(74) 代理人	100072660 弁理士 大和田 和美
		(72) 発明者	平川 満 大阪府大阪市此花区島屋一丁目1番3号 住友電気工業株式会社大阪製作所内
		(72) 発明者	櫻井 章広 大阪府大阪市此花区島屋一丁目1番3号 住友電気工業株式会社大阪製作所内

最終頁に続く

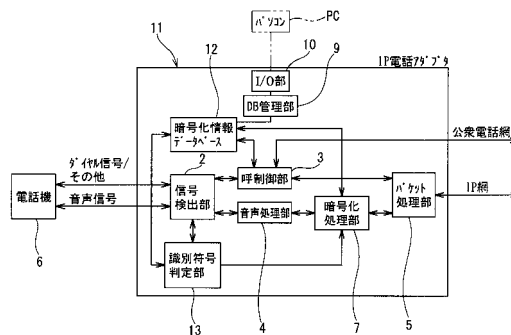
(54) 【発明の名称】 IP電話装置

(57) 【要約】

【課題】 IP電話における暗号化機能の有効/無効等の設定変更を容易化する。

【解決手段】 IP電話による通話の通信暗号化を開始する合図となるダイヤル符号を暗号化識別符号として登録している暗号化情報データベース12と、ユーザ操作されたダイヤル符号が前記暗号化識別符号と一致することを検出した場合に、該検出に続いて始まるIP電話による通話を暗号化させる識別符号判定部13とを備えている。

【選択図】 図1



【特許請求の範囲】**【請求項 1】**

IP 電話による通話の通信暗号化を行う合図となるダイヤル符号を暗号化識別符号として登録している暗号化情報データベースと、

ユーザ操作されたダイヤル符号が前記暗号化識別符号と一致することを検出した場合に該検出に続いて始まる IP 電話による通話を暗号化させる識別符号判定部と、

を備えていることを特徴とする IP 電話装置。

【請求項 2】

IP 電話の暗号化設定として暗号化パラメータ毎に複数の設定値を登録しており、かつ、前記暗号化パラメータの種別を識別するダイヤル符号を暗号化パラメータ識別符号として割り当てていると共に、前記各設定値の種別を識別するダイヤル符号を設定値識別符号として割り当てている暗号化情報データベースと、

ユーザ操作されたダイヤル符号が前記暗号化パラメータ識別符号と前記設定値識別符号とであることを検出した場合に、前記暗号化パラメータ識別符号に対応する暗号化パラメータには前記設定値識別符号に対応する設定値を IP 電話の通話の暗号化に反映させる識別符号判定部と、

を備えていることを特徴とする IP 電話装置。

【請求項 3】

前記識別符号判定部は、前記暗号化パラメータ識別符号と前記設定値識別符号とを 1 組として複数組ダイヤルされたダイヤル符号を判別することで、複数の暗号化パラメータに関して前記設定値識別符号に対応する設定値を IP 電話の通話の暗号化に反映させる構成としている請求項 2 に記載の IP 電話装置。

【請求項 4】

前記暗号化情報データベースに保存された前記暗号化パラメータ識別符号あるいは / および前記設定値識別符号は、外部入力機器からのユーザ操作により変更可能としている請求項 2 または請求項 3 に記載の IP 電話装置。

【発明の詳細な説明】**【技術分野】****【0001】**

本発明は、IP 電話装置に関し、詳しくは、IP 電話による音声通話の通信暗号化を行うものである。

【背景技術】**【0002】**

近年、従来の加入電話に代わる新しい電話形態として、インターネットをはじめとする IP 網を利用して音声を送信する IP 電話が注目されており、既に実用化が開始されている（特開 2005 - 45382 号公報等）。

一般的な IP 電話システムについて図 7 を用いて説明すると、IP 電話アダプタは、電話機からのダイヤル信号や音声信号に対して必要な処理を行い、パケット化して IP 網に送信する。IP 網における発信や着信の制御（呼制御）は呼制御サーバにより行われ、通話中の IP 電話の音声パケットは呼制御サーバを経由せず直接やりとりされる。

【0003】

次に、IP 電話の一般的な接続シーケンスについて図 8 を用いて簡単に説明する。まず初期設定として、ユーザは IP 電話サービス事業者から付与された IP 電話番号を IP 電話アダプタに設定後、IP 電話アダプタを IP 網に接続する。その後 IP 電話アダプタは自動的に IP アドレスを取得し、IP アドレスと IP 電話番号を呼制御サーバへ登録する。

そして、ユーザ A が電話機 A の受話器を上げると、IP 電話アダプタ A は電話機 A に発信音を送出する。その後、相手先電話番号をダイヤルすると、IP 電話アダプタ A は相手先電話番号を呼制御プロトコルの接続要求メッセージにのせて呼制御サーバに送信する。呼制御サーバは図 7 に示すような IP 電話番号と IP アドレスの対応表を管理している。

10

20

30

40

50

呼制御サーバは相手先電話番号に対応するIPアドレスを調べ、そのIPアドレスに対して接続要求メッセージを送信する。

【0004】

接続要求メッセージを受信したIP電話アダプタBは電話機Bに対して着信音を送出して着信を通知すると共に、呼制御サーバ経由でIP電話アダプタAに対して呼出中であることを示すメッセージを送信する。IP電話アダプタAはこれを受けて電話機Aに呼出音を送出する。ユーザBが電話機Bの受話器を上げた時、IP電話アダプタBは呼制御サーバ経由でIP電話アダプタAに対して接続応答メッセージを送信する。接続応答メッセージを受信したIP電話アダプタAは電話機Aに応答を通知し、通話が始まる。

【0005】

次に、一般的なIP電話アダプタ1の構成を図9に示す。信号検出部2は、電話機6からの信号を検出して信号の内容を判定する。呼制御部3は、通話する相手との接続および切断を制御する。また、市販されている殆どのIP電話アダプタ1は、IP電話による通話ができない相手先については公衆電話網を利用する機能を有している。音声処理部4は、アナログ/デジタル信号変換と音声の符号化/復号化を行う。パケット処理部5は、呼制御信号と音声信号のパケット化/脱パケット化を行う。

【0006】

前述したIP電話の主な特長としては、(1)同じプロバイダが提供するIP電話サービスのユーザであれば、時間や距離にかかわらず無料または低料金で通話できる点。(2)050番号を利用することにより、引越しや移転等があっても電話番号を変更しなくてよい点、(3)IP電話と他のアプリケーションを融合した新サービス等の大きな可能性を秘めている点などが挙げられる。

しかしながら、IP電話はインターネット技術を利用しているため盗聴されやすいという問題がある。そこで、インターネット技術の標準化団体であるIETF(Internet Engineering Task Force)では、パケットを暗号化する技術であるSRTP(Secure Real-time Transport Protocol)を標準化(RFC3711)している。SRTPは主に音声や動画などのリアルタイム通信を暗号化する技術であり、IP電話の暗号化方式として期待されている。

【0007】

そこで、暗号化機能を搭載した一般的なIP電話アダプタの構成を図10に示す。暗号化処理部7は、音声信号をユーザ設定値に従って暗号化/復号化する。暗号化情報データベース8は一般的に図11に示す構成となっており、I/O部10で接続されたパソコンからデータベース管理部9により設定可能としている。暗号化パラメータの例としては、暗号化機能の有効/無効、暗号化に使用するアルゴリズム、暗号キーの更新ライフタイム等がある。デフォルト設定値は工場出荷時の設定値を意味し、ユーザ設定値はユーザが独自に設定変更した値を意味する。図11では暗号化パラメータである暗号化有効/無効の設定をユーザが独自に「無効」から「有効」、暗号化アルゴリズムを「DES」(Data Encryption Standard)から「3DES」に変更した例を示している。

【0008】

IP電話の暗号化を行う場合は、相手先と暗号化情報を交渉する。交渉方法の1つとしては、発信側IP電話アダプタが接続要求メッセージに暗号化情報を付加して送信する。このときの暗号化情報は、ユーザ設定値を反映した暗号化パラメータ群である。着信側IP電話アダプタは、その暗号化情報が受け入れられるものであれば接続応答メッセージに暗号化情報を付加して送信し、受け入れられない若しくは暗号化機能を搭載していない場合はエラーメッセージを返して終了する。

【0009】

ところで、前記IP電話アダプタに関する種々の暗号化パラメータの設定は、一般的にはIP電話アダプタにパソコンを接続した後、パソコンからIP電話アダプタにアクセスし、パソコンに表示されるパラメータ設定用のWEBインタフェースを介して設定を行う

10

20

30

40

50

のが通常である。

しかしながら、暗号化機能の有効/無効の設定や他の暗号化パラメータの設定変更を行う場合に、わざわざパソコンを起動して行うとすれば、非常に手間が掛かり煩わしいという問題がある。特に、パソコンは起動するまでに時間が掛かるためユーザにストレスを与えてしまうと共に、パソコン操作に不慣れなユーザは暗号化設定そのものに行えないという不都合が生じる。

【0010】

【特許文献1】特開2005-45382号公報

【非特許文献1】SIP教科書(監修:千村保文、村田利文、IDGジャパン、2003年5月)

【発明の開示】

【発明が解決しようとする課題】

【0011】

本発明は、前記問題に鑑みてなされたもので、IP電話における暗号化機能の有効/無効等の設定変更が容易に行えるようにすることを課題としている。

【課題を解決するための手段】

【0012】

前記課題を解決するため、本発明は第1に、IP電話による通話の通信暗号化を行う合図となるダイヤル符号を暗号化識別符号として登録している暗号化情報データベースと、ユーザ操作されたダイヤル符号が前記暗号化識別符号と一致することを検出した場合に、該検出に続いて始まるIP電話による通話を暗号化させる識別符号判定部と、を備えていることを特徴とするIP電話装置を提供している。

【0013】

前記構成とすると、ユーザはわざわざパソコン等からアクセスして暗号化開始の設定を行う必要が無く、その場の必要に応じてIP電話の通話の暗号化をダイヤル操作により簡単に設定することができ、設定作業の大幅な簡素化が図られる。また、電話機操作だけで暗号化設定が可能であるので、パソコン等に不慣れなユーザでも抵抗なく操作でき、ユーザの操作性や汎用性が飛躍的に向上する。

なお、本発明のIP電話装置は、電話機本体と別体のIP電話アダプタでもよいし、電話機本体と一体型であってもよい。また、前記ダイヤル符号は、例えば0~9の数字や*、#の記号を利用したものであると好適である。また、プッシュ電話、ダイヤル電話のいずれにも適用可能であることは言うまでもない。

【0014】

本発明は、第2に、IP電話の暗号化設定として暗号化パラメータ毎に複数の設定値を登録しており、かつ、前記暗号化パラメータの種別を識別するダイヤル符号を暗号化パラメータ識別符号として割り当てていると共に、前記各設定値の種別を識別するダイヤル符号を設定値識別符号として割り当てている暗号化情報データベースと、

ユーザ操作されたダイヤル符号が前記暗号化パラメータ識別符号と前記設定値識別符号とであることを検出した場合に、前記暗号化パラメータ識別符号に対応する暗号化パラメータには前記設定値識別符号に対応する設定値をIP電話の通話の暗号化に反映させる識別符号判定部と、

を備えていることを特徴とするIP電話装置を提供している。

【0015】

前記構成とすると、ユーザは各種暗号化パラメータの設定値をパソコン等からアクセスして変更する必要がなく、ダイヤル操作だけで行うことができるので、暗号化設定作業の大幅な簡素化が図られてユーザ操作性が飛躍的に向上する。なお、暗号化パラメータの例としては、暗号化機能の有効/無効や、暗号化アルゴリズムの種類や、暗号キーの更新ライフタイムや、暗号化後データの認証アルゴリズムの種類などが挙げられる。また、第1の発明と同様に、前記IP電話装置は、電話機本体と別体のIP電話アダプタでもよいし、電話機本体と一体型であってもよい。また、前記ダイヤル符号は、例えば0~9の数字

や*、#の記号を利用するとよい。また、プッシュ電話、ダイヤル電話のいずれにも適用可能である。

【0016】

前記識別符号判定部は、前記暗号化パラメータ識別符号と前記設定値識別符号とを1組として複数組ダイヤルされたダイヤル符号を判別することで、複数の暗号化パラメータに関して前記設定識別符号に対応する設定値をIP電話の通話の暗号化に反映させる構成としていると好ましい。

前記構成とすると、複数の暗号化パラメータに関して一連のダイヤル操作で一括して設定変更することが可能となりユーザの操作性がさらに向上する。

【0017】

前記暗号化情報データベースに保存された前記暗号化パラメータ識別符号あるいは/および前記設定値識別符号は、外部入力機器からのユーザ操作により変更可能としていると好ましい。

【0018】

即ち、暗号化設定をダイヤル操作で行うための暗号化パラメータ識別符号や設定値識別符号は他人に知られないことが好ましいので、前記構成とすると、IP電話装置にパソコン等の外部入力機器を接続して変更することが可能となり、セキュリティ性が向上する。また、ユーザが覚えやすい符号にカスタマイズ変更できるため、忘れにくくなるという利点もある。

【発明の効果】

【0019】

上述したように、本発明によれば、ユーザはわざわざパソコン等からアクセスして暗号化の設定を行う必要が無く、IP電話の通話の暗号化をダイヤル操作により簡単に設定することができ、設定作業を非常に簡単なものとすることができる。

【発明を実施するための最良の形態】

【0020】

本発明の実施形態を図面を参照して説明する。

図1乃至図3は第1実施形態を示す。

実施形態のIP電話アダプタ11(IP電話装置)は前記図7に示すIP電話システムに適用したもので、システムの全体的な構成は前記図7と同様であるため説明を省略する

【0021】

IP電話アダプタ11は、図1に示すように、信号検出部2と、呼制御部3と、音声処理部4と、パケット処理部5と、暗号化処理部7と、暗号化情報データベース12と、データベース管理部9と、I/O部10と、識別符号判定部13とを備えている。

信号検出部2は、電話機6から送信されるダイヤル信号や音声信号を検出する機能を有する。呼制御部3は、音声以外のダイヤル信号をデジタル化したり、通話開始時に呼制御サーバに送信する相手先電話番号等を含む接続要求メッセージの作成等を行う機能を有する。音声処理部4は、電話機6から送信される音声データをアナログからデジタルに変換する機能を有する。パケット処理部5は、呼制御部3や音声処理部4から送信されるデータのパケット化を行ってIP網に送信したり、IP網から受信したデータの脱パケット化を行う機能を有する。暗号化処理部7は、暗号化情報データベース12に登録された設定内容に基づいて音声データの暗号化/復号化を行う機能を有する。

【0022】

暗号化情報データベース12は、図2に示すように、暗号化パラメータの種別と、各暗号化パラメータの工場出荷時の設定内容であるデフォルト設定値と、各暗号化パラメータのユーザカスタマイズされた設定内容であるユーザ設定値とを登録している。詳しくは、暗号化パラメータとして、暗号化の有効/無効の設定や、暗号キーの更新ライフタイム(乱数により発生する暗号キーの更新までの時間)や、暗号化アルゴリズムや、暗号化識別符号などがある。ここで、暗号化識別符号は、他の暗号化パラメータの設定内容を基にし

10

20

30

40

50

て通話の暗号化を開始する合図となるダイヤル符号を意味している。各パラメータのデフォルト設定値は、暗号化が有効で、暗号キーの更新ライフタイムが1日で、暗号化アルゴリズムがDES (Data Encryption Standard) で、暗号化識別符号が777としている。各パラメータのユーザ設定値は、暗号化が有効で、暗号キーのライフタイムが1日で、暗号化アルゴリズムが3DESで、暗号化識別符号が234としている。なお、ユーザ設定値は、I/O部10に接続されたパソコンPC (外部入力機器) を操作してデータベース管理部9により設定を行っている。

【0023】

識別符号判定部13は、ユーザ操作により電話機6から送信されたダイヤル符号が暗号化情報データベース12に登録された暗号化識別符号と一致することを確認した場合に、IP電話による通話の暗号化開始を信号検出部2に指令する機能を有する。

10

データベース管理部9は、暗号化データベース12の設定内容の変更に関する演算処理を行う機能を有する。I/O部10は、パソコンPCをイーサネット(登録商標)ケーブル等を介してIP電話アダプタ11のデータベース管理部9に接続するインターフェース機能を有する。

【0024】

次に、IP電話アダプタ11の動作について説明する。

図3に示すように、発信側ユーザはIP電話による通話を暗号化して行う場合、電話機6から受話器を上げ(ステップS1)、最初に暗号化識別符号「234」をダイヤルし、その後、相手先電話番号をダイヤルする(ステップS2)。一方、暗号化しない場合は相手先電話番号のみダイヤルする。IP電話アダプタ11は、信号検出部2で検出したダイヤル信号を識別符号判定部13に送る。識別符号判定部13は、暗号化情報データベース12に登録されている暗号化識別符号(234)を参照して、ダイヤルされた符号の最初の符号が暗号化識別符号かどうかを判定し、その結果を信号検出部2に返す(ステップS3)。暗号化識別符号と判定した場合、信号検出部2は呼制御部3に対して、暗号化情報データベース12の各暗号化パラメータの内容を反映させた暗号化情報を付加した接続要求メッセージを作成するよう要求する(ステップS4)。識別符号判定部13で暗号化識別符号が検出されなかった場合は、暗号化されない通常の接続要求メッセージを作成する(ステップS5)。最後に、その接続要求メッセージを呼制御サーバに送信して接続処理を開始する(ステップS6)。

20

30

【0025】

以上の構成とすると、ユーザはパソコンPCからアクセスして暗号化開始の設定を行う必要が無く、その場の必要に応じて、相手先電話番号の先頭に暗号化識別符号である「234」をダイヤルするだけで通話の暗号化開始を簡単に設定することができる。

したがって、設定作業の大幅な簡素化が図られると共にユーザ操作性が飛躍的に向上する。なお、本実施形態では暗号化識別符号を「234」と数字のみにしているが、*や#の記号を使用したものであってもよい。また、IP電話アダプタ11は電話機6と一体型としてもよい。

【0026】

図4乃至図5は第2実施形態を示す。

40

第1実施形態との相違点は、暗号化パラメータの設定値を予め複数用意し、ダイヤル操作によりパラメータ設定を変更可能としている点である。

【0027】

IP電話アダプタ11の構成は図1と同様であり、暗号化情報データベース12および識別符号判定部13の内容が相違している。本実施形態の暗号化情報データベース12には、図4に示すように、各暗号化パラメータに対応して複数の設定値を予め登録している。例えば、暗号化の有効/無効については設定値として有効と無効の2種類を用意し、暗号キーの更新ライフタイムについては設定値として1H(1時間)、5H(5時間)、1日、3日の4種類を用意し、暗号化アルゴリズムについては設定値としてDESと3DESの2種類を用意している。

50

【0028】

また、暗号化情報データベース12では、夫々の暗号化パラメータの種別を識別するためのダイヤル符号を各暗号化パラメータ毎に暗号化パラメータ識別符号として割り当てている。例えば、暗号化パラメータ識別符号は、暗号化の有効/無効については「301」、暗号キーの更新ライフタイムについては「302」、暗号化アルゴリズムについては「303」としている。

【0029】

さらに、暗号化パラメータに対応する各設定値の種別を識別する枝番であるダイヤル符号を各設定値毎に設定値識別符号として割り当てている。例えば、設定値識別符号は、暗号化の有効/無効に関しては有効を「1」、無効を「2」としており、暗号キーの更新ライフタイムに関しては1Hを「1」、5Hを「2」、1日を「3」、3日を「4」としており、暗号化アルゴリズムに関してはDESを「1」、3DESを「2」としている。なお暗号化パラメータ識別符号および設定値識別符号は、必要に応じてパソコンPCからの操作により桁数や符号を変更してもよい。

10

【0030】

識別符号判定部13は、ユーザ操作により電話機6から送信されたダイヤル符号が暗号化情報データベース12に登録された暗号化パラメータ識別符号と設定値識別符号とであることを検出した場合に、その暗号化パラメータに関してその設定値識別符号に対応する設定値を接続要求値に反映させることを信号検出部2に指令する機能を有する。ここで、接続要求設定値は、接続要求メッセージに付加される設定値であり一時的にメモリに保持されるものである。なお、他の構成は第1実施形態と同様であるため説明を省略する。

20

【0031】

次に、第2実施形態のIP電話アダプタの動作について説明する。

図5に示すように、発信側ユーザはIP電話による通話を暗号化して行う場合、電話機6から受話器を上げ(ステップS10)、最初に暗号化識別符号「234」をダイヤルする(ステップS11)。一方、暗号化しない場合は相手先電話番号のみダイヤルする。さらに、特定の暗号化パラメータを変更したい場合、暗号化識別符号の後に変更したい暗号化パラメータ識別符号をダイヤルし、適用する設定値に対応する設定値識別符号をダイヤルする。なお、図5に示すように、複数の暗号化パラメータを変更することも可能である。そして、変更する暗号化パラメータの暗号化パラメータ識別符号および設定値識別符号のダイヤルが終了した後、相手先電話番号をダイヤルする。

30

【0032】

IP電話アダプタの信号検出部2はダイヤル信号を検出後、ダイヤル信号を識別符号判定部13に送る。識別符号判定部13は、暗号化情報データベース12に登録されている暗号化識別符号を参照し、ダイヤルされた符号の最初の符号が暗号化識別符号かどうかを判定する(ステップS12)。該最初の符号が暗号化識別符号と一致しない場合には、その結果を信号検出部2に返し、信号検出部2から呼制御部3に対して指令して、暗号化されない通常の接続要求メッセージを作成し(ステップS13)、該接続要求メッセージを呼制御サーバに送信する(ステップS14)。

【0033】

一方、該最初の符号が暗号化識別符号と一致する場合には、識別番号判定部13は、暗号化識別符号の後に続くダイヤル符号が暗号化情報データベース12に登録されている暗号化パラメータ識別符号かどうかを判定する(ステップS15)。暗号化パラメータ識別符号でない場合には、その結果を信号検出部2に返し、信号検出部2から呼制御部3に対して指令して、暗号化情報データベース12に登録された暗号化パラメータのユーザ設定値を反映させた暗号化情報を付与した接続要求メッセージを作成し(ステップS20)、接続要求メッセージを呼制御サーバに送信する(ステップS14)。

40

【0034】

一方、暗号化識別符号の後に続くダイヤル符号が暗号化パラメータ識別符号と一致する場合には、暗号化パラメータ識別符号の後に続くダイヤル符号が暗号化情報データベース

50

12に登録されている設定値識別符号として有効であると判定した場合は(ステップS16)、暗号化パラメータ識別符号に対応する暗号化パラメータの接続要求設定値を設定値識別符号で指定された設定値に変更してメモリに保持する(ステップS17)。ダイヤルされた符号が設定値識別符号として有効でない場合、例えば、暗号化の有効/無効の暗号化パラメータに対する設定値識別符号が1あるいは2でない場合にはエラー処理として切断する(ステップS19)。

【0035】

さらに、有効に検出された設定値識別符号の後に続くダイヤル符号が、暗号化情報データベース12に登録されている暗号化パラメータ識別符号かどうかを判定する(ステップS18)。暗号化パラメータ識別符号でない場合には、その結果を信号検出部2に返し、信号検出部2から呼制御部3に対して指令して、ステップS17で変更された暗号化パラメータ以外の変更要求のない暗号化パラメータについては、暗号化情報データベース12に登録されたユーザ設定値の複製を接続要求設定値に反映させ、該接続要求設定値の暗号化情報を付与した接続要求メッセージを作成し(ステップS20)、接続要求メッセージを呼制御サーバに送信する(ステップS14)。

10

【0036】

一方、暗号化識別符号の後に続くダイヤル符号が暗号化パラメータ識別符号と一致する場合には、前述同様にステップS16およびステップS17を繰り返した上で、呼制御部3によりメモリ保持された接続要求設定値を利用して接続要求メッセージを作成し(ステップS20)、接続要求メッセージを呼制御サーバに送信する(ステップS14)。

20

【0037】

次に、更に具体的な一例として、相手先電話番号が050-1234-6789、暗号化情報データベース12が図4で表される場合に、暗号化パラメータを変更して暗号化を行う方法について説明する。

例えば、一時的に暗号キーの更新ライフタイムを1日から3日に変更し、暗号化アルゴリズムをDESから3DESに変更して暗号化したいとする。このときユーザは下記のようにダイヤルすればよいことになる。

234-302-4-303-2-050-1234-6789

【0038】

即ち、暗号化識別符号の「234」をダイヤル後、暗号化パラメータの暗号キーの更新ライフタイムを表す暗号化パラメータ識別符号の「302」をダイヤルし、設定値の3日を表す設定値識別符号の「4」をダイヤルする。引き続き暗号化パラメータの暗号化アルゴリズムを表す「303」をダイヤルし、設定値の3DESを表す設定値識別符号の「2」をダイヤルする。その後、相手先電話番号である050-1234-6789をダイヤルする。これにより、暗号化情報データベース12の接続要求設定値は図6のようになり変更された状態でメモリ保持され、この接続要求設定値を利用して接続要求メッセージが作成される。

30

【0039】

以上の構成とすると、ユーザは各種暗号化パラメータの設定値をわざわざパソコンPCからアクセスして変更する必要がなく、電話機6のダイヤル操作だけで行うことができるので、暗号化設定作業の大幅な簡素化を図ることが可能となる。また、複数の暗号化パラメータに関して一連のダイヤル操作で一括して設定変更することが可能となりユーザの操作性が向上する。

40

【図面の簡単な説明】

【0040】

【図1】本発明の第1実施形態のIP電話アダプタを示すブロック図である。

【図2】暗号化情報データベースを示す図面である。

【図3】IP電話アダプタの動作を説明するフローチャートである。

【図4】第2実施形態の暗号化情報データベースを示す図面である。

【図5】IP電話アダプタの動作を説明するフローチャートである。

50

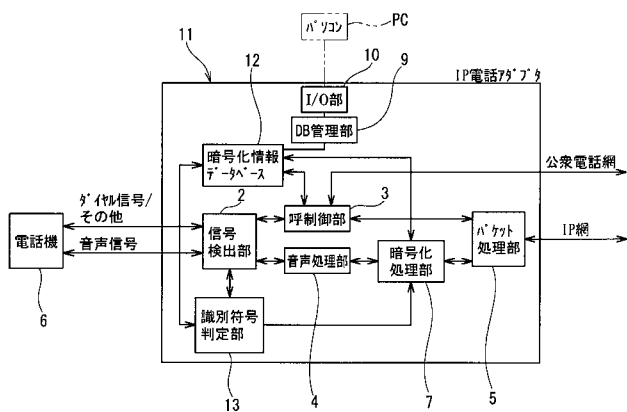
- 【図6】 変更操作後の接続要求設定値を示す図面である。
- 【図7】 IP電話システムの概略図である。
- 【図8】 電話機Aから電話機Bに発信する場合のシーケンスを示す図面である。
- 【図9】 従来例のIP電話アダプタを示すブロック図である。
- 【図10】 別の従来例のIP電話アダプタを示すブロック図である。
- 【図11】 従来の暗号化情報データベースを示す図面である。

【符号の説明】

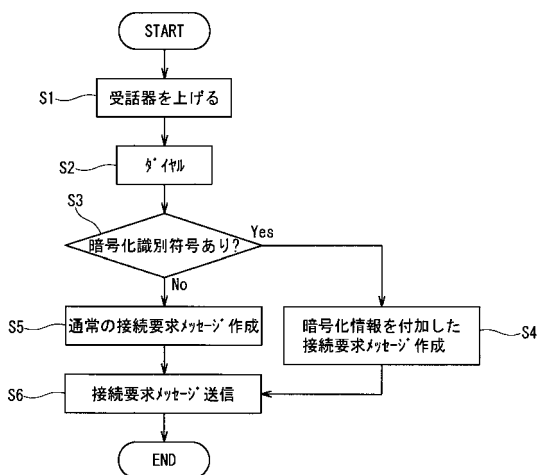
【0041】

- 2 信号検出部
- 3 呼制御部
- 4 音声処理部
- 5 パケット処理部
- 6 電話機
- 7 暗号化処理部
- 11 IP電話アダプタ (IP電話装置)
- 12 暗号化情報データベース
- 13 識別符号判定部

【図1】



【図3】



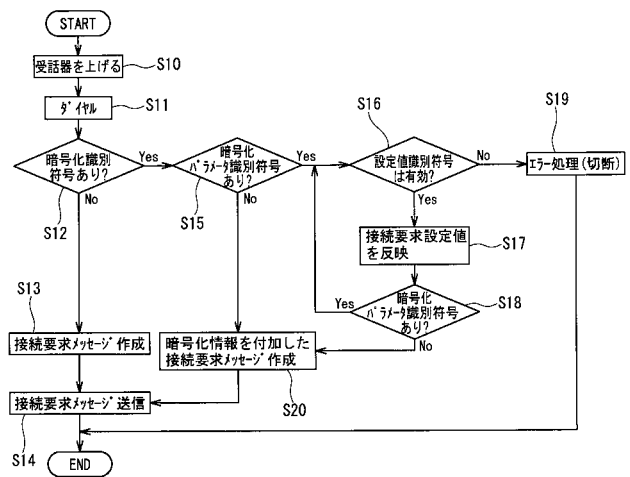
【図2】

暗号化パラメータ	デフォルト設定値	ユーザ設定値
暗号化の有効/無効	有効	有効
暗号キーの更新サイクル	1日	1日
暗号化アルゴリズム	DES	3DES
暗号化識別符号	777	234

【 図 4 】

暗号化パラメータ	暗号化パラメータ識別符号	設定値	設定値識別符号	ユーザ設定値	接続要求設定値
暗号化の有効/無効	301	有効	1	有効	有効
		無効	2		
暗号化の更新サイクル	302	1H	1	1日	1日
		5H	2		
		1日	3		
		3日	4		
暗号化アルゴリズム	303	DES	1	DES	DES
		3DES	2		
暗号化識別符号				234	

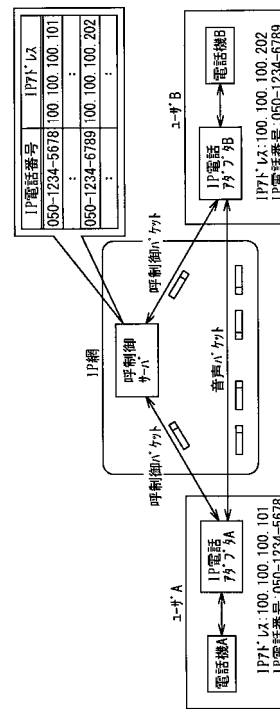
【 図 5 】



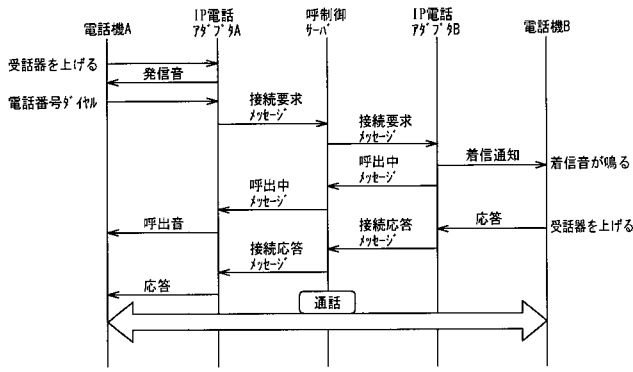
【 図 6 】

暗号化パラメータ	暗号化パラメータ識別符号	設定値	設定値識別符号	ユーザ設定値	接続要求設定値
暗号化の有効/無効	301	有効	1	有効	有効
		無効	2		
暗号化の更新サイクル	302	1H	1	1日	3日
		5H	2		
		1日	3		
		3日	4		
暗号化アルゴリズム	303	DES	1	DES	3DES
		3DES	2		
暗号化識別符号				234	

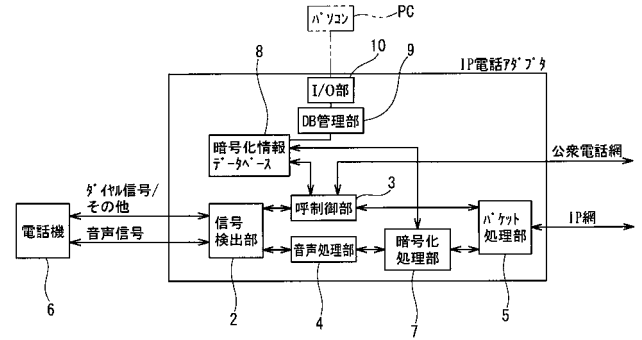
【 図 7 】



【 図 8 】

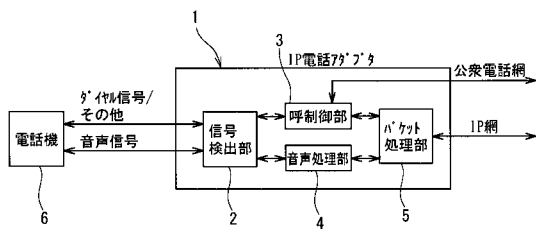


【 図 10 】



【 図 11 】

【 図 9 】



暗号化パラメータ	デフォルト設定値	ユーザ設定値
暗号化の有効/無効	無効	有効
暗号子の更新周期	1日	1日
暗号化アルゴリズム	DES	3DES
⋮	⋮	⋮

フロントページの続き

F ターム(参考) 5J104 AA01 AA32 AA33 JA03 JA13 NA02 NA37 PA07
5K027 AA08 BB04 DD11 DD14 HH26 KK02
5K201 AA05 AA08 CB01 CB02 CB05 CB06 EA05 EA08 EC06 ED02
ED07 EE08