(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4064990号
(P4064990)

(45)発行日　平成20年3月19日(2008.3.19)　(24)登録日　平成20年1月11日(2008.1.11)

(51)Int.Cl.		F I		
H04L 12/56	(2006.01)	H04L	12/56	100Z
H04L 9/32	(2006.01)	H04L	9/00	673C
H04M 3/42	(2006.01)	H04M	3/42	T
H04M 11/00	(2006.01)	H04M	3/42	E
H04M 3/00	(2006.01)	H04M	11/00	302

請求項の数 20　(全 21 頁)　最終頁に続く

(21)出願番号　特願2005-313650 (P2005-313650)
(22)出願日　平成17年10月28日 (2005.10.28)
(65)公開番号　特開2006-141004 (P2006-141004A)
(43)公開日　平成18年6月1日 (2006.6.1)
審査請求日　平成17年10月28日 (2005.10.28)
(31)優先権主張番号　04105426.3
(32)優先日　平成16年10月29日 (2004.10.29)
(33)優先権主張国　欧州特許庁 (EP)

(73)特許権者　500043574
リサーチ　イン　モーション　リミテッド
Ｒｅｓｅａｒｃｈ　Ｉｎ　Ｍｏｔｉｏｎ　Ｌｉｍｉｔｅｄ
カナダ国　エヌ２エル　３ダブリュー８　オンタリオ，　ウォータールー，　フィリップ　ストリート　２９５
２９５　Ｐｈｉｌｌｉｐ　Ｓｔｒｅｅｔ，　Ｗａｔｅｒｌｏｏ，　Ｏｎｔａｒｉｏ　Ｎ２Ｌ　３Ｗ８　Ｃａｎａｄａ
(74)代理人　100064447
弁理士　岡部　正夫
(74)代理人　100085176
弁理士　加藤　伸晃

最終頁に続く

(54)【発明の名称】安全なピアツーピア・メッセージング送信勧誘アーキテクチャ

(57)【特許請求の範囲】

【請求項１】

無線ネットワーク（１５）および前記無線ネットワーク（１５）に結合されたルーティング・サーバ（２０）を備え、各移動デバイス（１０）が１つまたは複数の通信アプリケーション（１６２）を有し、各移動デバイス（１０）がさらにメッセージング・アプリケーション（１６０）を有し、第１の移動デバイス（１０Ａ）が第１の個人識別番号を有し、第２の移動デバイス（１０Ｂ）が第２の個人識別番号を有するシステムで第１の移動デバイス（１０Ａ）と第２の移動デバイス（１０Ｂ）との間で個人識別番号を安全に交換する方法であって、

前記第１の個人識別番号を暗号化する工程（３２６）と、

前記暗号化された第１の個人識別番号を前記第１の移動デバイス（１０Ａ）から前記第２の移動デバイス（１０Ｂ）に前記通信アプリケーション（１６２）の１つを使用して送信する工程（３３０）と、

前記暗号化された第１の個人識別番号を復号化し、前記第１の個人識別番号を前記第２の移動デバイス（１０Ｂ）のメモリに格納する工程（３３４）と、

前記第２の個人識別番号を暗号化する工程（３１８）と、

前記暗号化された第２の個人識別番号を前記第２の移動デバイス（１０Ｂ）から前記第１の移動デバイス（１０Ａ）に前記通信アプリケーション（１６２）の１つを使用して送信する工程（３２２）と、

前記暗号化された第２の個人識別番号を復号化し、前記第２の個人識別番号を前記第１

の移動デバイス（１０Ａ）のメモリに格納する工程（３３２）とを含み、
ピアツーピア・メッセージが前記第１の移動デバイス（１０Ａ）と前記第２の移動デバイス（１０Ｂ）との間で前記メッセージング・アプリケーション（１６０）を使用して交換され、各ピアツーピア・メッセージが前記個人識別番号の１つを含み、各ピアツーピア・メッセージが前記個人識別番号の前記１つに基づいて前記ルーティング・サーバ（２０）によってルーティングされることを特徴とする方法。
【請求項２】
送信勧誘を前記第１の移動デバイスから前記第２の移動デバイスに前記通信アプリケーション（１６２）の前記１つを使用して送信し、前記送信勧誘が第１の公開鍵を含む工程（３０８）をさらに含むことを特徴とする、請求項１に記載の方法。
【請求項３】
前記第２の個人識別番号を暗号化する前記工程（３１８）が、前記第１の公開鍵を使用して前記第２の個人識別番号を暗号化することを含み、前記暗号化された第２の個人識別番号を送信する前記工程（３２２）が、受諾を送信することを含み、前記受諾が、前記暗号化された第２の個人識別番号を含み、第２の公開鍵を含むことを特徴とする、請求項１または２に記載の方法。
【請求項４】
前記第１の個人識別番号を暗号化する前記工程（３２６）が、前記第２の公開鍵を使用して前記第１の個人識別番号を暗号化することを含み、前記暗号化された第１の個人識別番号を送信する前記工程（３３０）が、肯定応答を送信することを含み、前記肯定応答が、前記暗号化された第１の個人識別番号を含むことを特徴とする、請求項１乃至３のいずれか１項に記載の方法。
【請求項５】
暗号化および復号化する前記工程が、共有セッション鍵を使用して実行され、前記方法が、鍵値を交換し、前記共有セッション鍵を前記交換された鍵値から導出する工程をさらに含むことを特徴とする、請求項１乃至４のいずれか１項に記載の方法。
【請求項６】
前記第１の移動デバイス（１０Ａ）が第１のユーザと関連付けられ、前記方法が、前記第１のユーザから送信勧誘命令を受信してから前記方法の工程を実行する工程をさらに含むことを特徴とする、請求項１乃至５のいずれか１項に記載の方法。
【請求項７】
前記第２の移動デバイス（１０Ｂ）が第２のユーザと関連付けられ、前記方法が、前記第２のユーザからの受諾命令を受信してから前記暗号化された第２の個人識別番号を送信する前記工程を実行する工程（３１４）をさらに含むことを特徴とする、請求項６に記載の方法。
【請求項８】
前記メッセージング・アプリケーション（１６０）が暗号化、復号化、および送信する前記工程を前記送信勧誘命令および前記受諾命令の受信に応答して自動的に実行することを特徴とする、請求項７に記載の方法。
【請求項９】
前記通信アプリケーション（１６２）の前記１つが電子メール・アプリケーションを含むことを特徴とする、請求項１乃至８のいずれか１項に記載の方法。
【請求項１０】
複数の移動デバイス（１０）、無線ネットワーク（１５）、および前記無線ネットワーク（１５）に結合されたルーティング・サーバ（２０）を含むピアツーピア・メッセージング・システムであって、各移動デバイス（１０）が１つまたは複数の通信アプリケーション（１６２）を有し、各移動デバイス（１０）が
第１の個人識別番号を格納するメモリ（１２４、１２６、１５６）、および
メッセージング・アプリケーション（１６０）を含んでおり、前記メッセージング・アプリケーション（１６０）が、

前記第１の個人識別番号を暗号化し、前記暗号化された第１の個人識別番号を通信に組み込んで、前記通信アプリケーション（１６２）の１つを使用して他の移動デバイスに伝送するための暗号化構成要素と、

前記他の移動デバイスから前記通信アプリケーション（１６２）の前記１つを介して到来する通信を受信し、前記到来通信は暗号化された第２の個人識別番号を含んでおり、前記暗号化された第２の個人識別番号を抽出し復号化するための復号化構成要素と、

前記通信アプリケーション（１６２）の前記１つを使用して前記他の移動デバイスとの送信勧誘および受諾の交換を自動的に管理するための連絡先管理構成要素と、

ピアツーピア・メッセージを送受信するためのメッセージング構成要素とを含み、前記ピアツーピア・メッセージはそれぞれ、前記個人識別番号の１つを含み、前記ピアツーピア・メッセージは前記個人識別番号の前記１つに基づいて前記ルーティング・サーバ（２０）によってルーティングされることを特徴とする、ピアツーピア・メッセージング・システム。

【請求項１１】

前記暗号化構成要素が第１の公開／秘密鍵ペアを生成するための鍵生成構成要素を含み、前記連絡先管理構成要素が第１の公開鍵を前記他の移動デバイスに前記通信アプリケーション（１６２）の前記１つを使用して送信することを特徴とする、請求項１０に記載のシステム。

【請求項１２】

前記連絡先管理構成要素が送信勧誘を作成し、前記送信勧誘を前記他の移動デバイスに前記通信アプリケーション（１６２）の前記１つを使用して伝送するための送信勧誘構成要素を含み、前記送信勧誘が前記第１の公開鍵を含むことを特徴とする、請求項１１に記載のシステム。

【請求項１３】

前記連絡先管理構成要素が受諾を作成し、前記受諾を前記他の移動デバイスに前記通信アプリケーション（１６２）の前記１つを使用して伝送するための受諾構成要素を含み、前記受諾が前記第１の公開鍵および前記暗号化された第１の個人識別番号を含むことを特徴とする、請求項１１または１２に記載のシステム。

【請求項１４】

前記暗号化構成要素が前記第１の個人識別番号を第２の公開鍵を使用して暗号化し、前記第２の公開鍵が前記他の移動デバイスから前記通信アプリケーション（１６２）の前記１つを使用して受信され、前記送信勧誘構成要素が受諾通信の受信に応答して肯定応答通信をさらに作成し、前記肯定応答通信が前記暗号化された第１の個人識別番号を含むことを特徴とする、請求項１１乃至１３のいずれか１項に記載のシステム。

【請求項１５】

前記暗号化構成要素および前記復号化構成要素が共有セッション鍵を使用し、前記連絡先管理構成要素が公開値および秘密値を生成し、前記公開値を前記他の移動デバイスと交換し、前記連絡先管理構成要素が前記共有セッション鍵を前記公開値、前記秘密値、および前記他の移動デバイスから受信された他の公開値から導出することを特徴とする、請求項１０に記載のシステム。

【請求項１６】

前記移動デバイスが、表示画面（１２２）およびユーザ入力デバイス（１３２）をさらに備え、前記連絡先管理構成要素が送信勧誘命令を前記ユーザ入力デバイス（１３２）から受信し、それに応答して前記連絡先管理構成要素が送信勧誘を自動的に生成し前記他の移動デバイスに送信することを特徴とする、請求項１０乃至１５のいずれか１項に記載のシステム。

【請求項１７】

前記移動デバイスが、表示画面（１２２）およびユーザ入力デバイス（１３２）をさらに備え、前記連絡先管理構成要素が送信勧誘通信を前記他の移動デバイスから受信すると前記表示画面（１２２）上に標識を提供し、前記連絡先管理構成要素が受諾命令を前記ユ

ーザ入力デバイス（１３２）から受信し、それに応答して前記連絡先管理構成要素が受諾を自動的に生成し前記他の移動デバイスに送信することを特徴とする、請求項１０乃至１５のいずれか１項に記載のシステム。

【請求項１８】

前記通信アプリケーション（１６２）の前記１つが電子メール・アプリケーションを含むことを特徴とする、請求項１０乃至１７のいずれか１項に記載のシステム。

【請求項１９】

無線ネットワーク（１５）を介して他の移動デバイスとピアツーピア・メッセージングを行うための移動デバイス（１０）であって、前記無線ネットワーク（１５）はルーティング・サーバ（２０）を含み、前記移動デバイス（１０）は、

無線ネットワーク（１５）との無線通信を行うための通信サブシステム（１１１）と、

第１の個人識別番号を格納するメモリ（１２４、１２６、１５６）と、

前記メモリおよび前記通信サブシステム（１１１）に接続されて前記通信サブシステム（１１１）の動作を制御するプロセッサ（１３８）と、

通信を作成し前記他の移動デバイスに送信するための通信アプリケーション（１６２）とを含んでおり、

前記移動デバイスが、

メッセージング・アプリケーション（１６０）を含んでおり、前記メッセージング・アプリケーション（１６０）が、

前記第１の個人識別番号を暗号化し、前記暗号化された第１の個人識別番号を通信に組み込んで、前記通信アプリケーション（１６２）を使用して他の移動デバイスに伝送するための暗号化構成要素と、

前記他の移動デバイスから前記通信アプリケーション（１６２）を介して到来するメッセージを受信し、前記到来メッセージは暗号化された第２の個人識別番号を含んでおり、前記暗号化された第２の個人識別番号を抽出し復号化するための復号化構成要素と、

前記通信アプリケーション（１６２）を使用する前記他の移動デバイスとの送信勧誘および受諾の交換を自動的に管理するための連絡先管理構成要素と、

ピアツーピア・メッセージを送受信するためのメッセージング構成要素とを含み、前記ピアツーピア・メッセージはそれぞれ、前記個人識別番号の１つを含み、前記ピアツーピア・メッセージは前記個人識別番号の前記１つに基づいて前記ルーティング・サーバ（２０）によってルーティングされることを特徴とする、移動デバイス（１０）。

【請求項２０】

前記暗号化構成要素が第１の公開／秘密鍵ペアを生成するための鍵生成構成要素を含み、前記連絡先管理構成要素が前記第１の公開鍵を前記他の移動デバイスに前記通信アプリケーション（１６２）を使用して送信することを特徴とする、請求項１９に記載の移動デバイス。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、一般に、セル・フォン、スマート・フォン、携帯情報端末（ＰＤＡ）、ページャ、ハンドヘルド・コンピュータ、電話可能なラップトップ・コンピュータ、および他の移動電子デバイスなど、移動デバイスのための安全なメッセージング送信勧誘アーキテクチャに関し、より詳細には、移動デバイスのためのピアツーピア即時メッセージング・ソリューションに関する。

【背景技術】

【０００２】

インスタント・メッセージング（ＩＭ）は、友達または同僚など他の個人がオンライン状態になった場合にユーザに知らせて、電子メール・ソリューションに固有の蓄積交換の遅延を発生させずに、ユーザがメッセージを互いに実時間で送信することができるようにするサービスである。インスタント・メッセージングでは、各ユーザは、自分が通信を望

む他のユーザの（通常「メンバー・リスト」と呼ばれる）リストを作成する。インスタント・メッセージング・サーバは、それを利用する各ユーザの（存在情報と呼ばれる）オンライン状況を把握し、ユーザのメンバー・リストの誰かがオンライン状態になった場合に、サービスがユーザに知らせ、他のユーザと即座に接触することができるようにする。

【０００３】

ＩＭソリューションは高速で乗算できるため、地上通信線環境だけでなく、セル・フォン、スマート・フォン、携帯情報端末（ＰＤＡ）、ページャ、電話可能なラップトップ・コンピュータ、および他の移動電子デバイスなど移動デバイスによって使用される無線環境でも使用される。無線環境では、ユーザが移動デバイスを持ち歩く時間に基づく、強化ＩＭソリューションが見込まれる。ＩＭソリューションを実行することができる使用可能な携帯デバイスの数は何億にもなる。

【０００４】

ＩＭ顧客を移動デバイスにポートして、多くの使用可能なＩＭサービスの１つへのアクセス権を得ることは、当技術分野で周知である。こうしたサービスには、ＡＯＬのＩｎｓｔａｎｔ Ｍｅｓｓｅｎｇｅｒ（ＡＩＭ）、ＩＣＱ、Ｙａｈｏｏ！、およびＭｉｃｒｏｓｏｆｔのＭＳＮ Ｍｅｓｓｅｎｇｅｒ製品が含まれる。こうした製品には、各ＩＭサーバによってサポートされる何億ものユーザがあることが知られており、これらのコミュニティは相互接続されてさらに大きいコミュニティが作成されることが多い。しかし、地上通信線およびデスクトップ・ベースのＩＭソリューションは、移動している場合が多いユーザが、自分の移動デバイスを携帯している場合に常に要求し必要とするもの、すなわち良好なＩＭ機能性が不十分である。さらに、移動デバイスの小さい画面およびメモリは、路上でＩＭを使用しようと試みる人をいらだたせることが多い。こうした人々は、古いデスクトップＩＭソリューションを操作しており他に選択すべきオプションを持たない地上通信線のユーザとの接触を望み、またはそうする必要があるため、乏しい性能を受け入れ、既存のＩＭソリューションを使用せざるを得ない。したがって、移動デバイスの「常時オン状態」特性の利点を得ることができる無線移動電子デバイス用に設計された（ＩＭのような即時メッセージングが可能な）より良好でより完全なメッセージング・ソリューションが求められている。

【０００５】

既存のＩＭアプリケーションに関する他の問題は、セキュリティが不十分なことである。既存のＩＭアプリケーションでは、ユーザのＩＤを共有することが簡単である。すなわち、１人のＩＤが許可なく広範に配布されるため、未知の、または望まないソースからメッセージを受信することがある。これは、ジャンク・メッセージ、スパム、ウィルス、または他のセキュリティの懸念の激増につながる。また、送信勧誘のソースを確認または認証してメッセージングを開始することも難しく、成り済ましや関連するセキュリティ問題が発生することもある。

【０００６】

別の通常の無線メッセージング標準は、北米中、および特にヨーロピアン・チャイナとインドで使用される短メッセージ・サービス（ＳＭＳ）である。このサービスにも多くの欠点がある。第１に、各ＳＭＳユーザのアドレス指定をＳＭＳユーザのＭＳ－ＩＳＤＮまたは電話番号を介して行われなければならない。この電話番号は、非常に簡単に回されるため、送信側の認証を確認することが不可能である。第２に、暗黙的存在または実際の転送情報がないため、情報の交換にはそれに関連する危険が多く伴う。ＳＭＳは、永続する会話の概念もなく、実際、第３者とのＳＭＳ会話に関する長期の状況情報を保持するＳＭＳデバイスも存在しない。

【発明の開示】

【発明が解決しようとする課題】

【０００７】

本出願は、移動デバイス間の即時ピアツーピア・メッセージングを提供するシステムおよび方法を記載する。

【課題を解決するための手段】
【０００８】
このシステムおよび方法は、システム内の移動デバイスの各ユーザの対象アドレスＩＤの秘密性を維持することによってセキュリティの向上をもたらすものである。ユーザが自分の個人識別番号（ＰＩＮ）に直接アクセスし、またはそれを提供する必要を回避して、ＰＩＮの交換を可能にする送信勧誘アーキテクチャを開示する。メッセージング・アプリケーションは、その関連するＰＩＮを暗号化してから、それを他の移動デバイスのメッセージング・アプリケーションに既存の通信アプリケーションを介して提供する。送信勧誘アーキテクチャは、暗号化、必要な鍵交換全て、送信勧誘と受諾メッセージの作成、およびＰＩＮの復号化と格納を自動的に管理する。
【０００９】
一態様では、本出願は、第１の移動デバイスと第２の移動デバイスとの間の個人識別番号の安全な交換方法を提供する。この移動デバイスは、無線ネットワークおよび無線ネットワークに結合されたルーティング・サーバを備えたシステムで使用される。各移動デバイスは、１つまたは複数の通信アプリケーションを有し、各移動デバイスはさらにメッセージング・アプリケーションを有する。第１の移動デバイスは、第１の個人識別番号を有し、第２の移動デバイスは第２の個人識別番号を有する。この方法は、第１の個人識別番号を暗号化する工程、暗号化された第１の個人識別番号を第１の移動デバイスから第２の移動デバイスに通信アプリケーションの１つを使用して送信する工程、および暗号化された第１の個人識別番号を復号化し、第１の個人識別番号を第２の移動デバイスのメモリに格納する工程を含む。この方法は、第２の個人識別番号を暗号化する工程、暗号化された第２の個人識別番号を第２の移動デバイスから第１の移動デバイスに通信アプリケーションの１つを使用して送信する工程、および暗号化された第２の個人識別番号を復号化し、第２の個人識別番号を第１の移動デバイスのメモリに格納する工程も含む。このＰＩＮの交換後、ピアツーピア・メッセージが第１の移動デバイスと第２の移動デバイスとの間でメッセージング・アプリケーションを使用して交換される。各ピアツーピア・メッセージは、個人識別番号の１つを含み、各ピアツーピア・メッセージは個人識別番号に基づいてルーティング・サーバによってルーティングされる。
【００１０】
他の態様では、本出願は、ピアツーピア・メッセージング・システムを提供する。このシステムは、複数の無線デバイス、無線ネットワーク、および無線ネットワークに結合されたルーティング・サーバを備える。各移動デバイスは、１つまたは複数の通信アプリケーションを有し、各移動デバイスは第１の個人識別番号を格納するメモリを備える。各移動デバイスは、メッセージング・アプリケーションも含み、メッセージング・アプリケーションは、暗号化構成要素、復号化構成要素、連絡先管理構成要素、およびメッセージング構成要素を含む。暗号化構成要素は、第１の個人識別番号を暗号化し、暗号化された第１の個人識別番号を通信に組み込んで、他の移動デバイスに通信アプリケーションの１つを使用して伝送するためのものである。復号化構成要素は、他の移動デバイスから通信アプリケーションの１つを介して到来する通信を受信し、到来通信には、暗号化された第２の個人識別番号が含まれており、暗号化された第２の個人識別番号を抽出し復号化するためのものである。連絡先管理構成要素は、通信アプリケーションの１つを使用する他の移動デバイスとの送信勧誘および受諾の交換を自動的に管理するためのものである。メッセージング構成要素は、ピアツーピア・メッセージを送受信するためのものであり、ピアツーピア・メッセージはそれぞれ、個人識別番号の１つを含み、ピアツーピア・メッセージは個人識別番号に基づいてルーティング・サーバによってルーティングされる。
【００１１】
他の態様では、本出願は、他の移動デバイスと無線ネットワークを介してピアツーピア・メッセージングを行う移動デバイスを提供する。無線ネットワークは、ルーティング・サーバを備える。移動デバイスは、無線通信で無線ネットワークと接続するための通信サブシステム、第１の個人識別番号を格納するメモリ、およびメモリと通信サブシステムに

接続されて通信サブシステムの動作を制御するためのプロセッサを備える。移動デバイスは、通信を作成し他の移動デバイスに送信するための通信アプリケーションおよびメッセージング・アプリケーションも含む。メッセージング・アプリケーションは、暗号化構成要素、復号化構成要素、連絡先管理構成要素、およびメッセージング構成要素を含む。暗号化構成要素は、第１の個人識別番号を暗号化し、暗号化された第１の個人識別番号を通信に組み込んで、通信アプリケーションの１つを使用して他の移動デバイスに伝送するためのものである。復号化構成要素は、他の移動デバイスから通信アプリケーションの１つを介して到来する通信を受信し、到来通信には、暗号化された第２の個人識別番号が含まれており、暗号化された第２の個人識別番号を抽出し復号化するためのものである。連絡先管理構成要素は、通信アプリケーションの１つを使用する他の移動デバイスとの送信勧誘および受諾の交換を自動的に管理するためのものである。メッセージング構成要素は、ピアツーピア・メッセージを送受信するためのものであり、ピアツーピア・メッセージはそれぞれ、個人識別番号の１つを含み、ピアツーピア・メッセージは個人識別番号に基づいてルーティング・サーバによってルーティングされる。

【００１２】

本出願の他の態様および特徴は、以下の詳細な説明、および１つまたは複数の実装形態を示す図面を参照すれば、当業者には明らかであろう。

次に、実装形態を添付の図を参照して単なる一例として説明する。図にわたって使用されている同様の参照番号は同様の要素および特徴を示すものである。

【発明を実施するための最良の形態】

【００１３】

次に図面を参照すると、図１は、即時ピアツーピア・メッセージングを可能にするシステム５を示すブロック図である。システム５は、図１で示したように、移動デバイス１０Ａおよび１０Ｂなど複数の移動局１０を備える。移動局１０は、２～３例を挙げると、セル・フォン、スマート・フォン、携帯情報端末（ＰＤＡ）、ページャ、ハンドヘルド・コンピュータ、または電話可能なラップトップ・コンピュータなど任意のタイプの無線移動電子通信デバイスでもよい。周知のように、各移動デバイス１０には、無線電話アプリケーション、電子メール・アプリケーション、短メッセージ・サービス（ＳＭＳ）アプリケーション、マルチメディア・メッセージング・サービス（ＭＭＳ）アプリケーション、エンハンスド・メッセージ・サービス（ＥＭＳ）アプリケーション、および他のインターネット可能なメッセージング・アプリケーション（これら全てを本明細書で「既存の通信アプリケーション」と呼ぶことができる）など、他の移動デバイス１０との通信を可能にする１つまたは複数の現在存在するアプリケーションが含まれるがそれだけに限定されない、様々なアプリケーションが提供されている。さらに、各移動デバイス１０には、本明細書に記載されたピアツーピア・メッセージング・ソリューションを実装する（本明細書で「メッセージング・アプリケーション」と呼ばれる）アプリケーションが提供されている。本明細書で使用されるように、用語「アプリケーション」は、１つまたは複数のプログラム、ルーチン、サブルーチン、関数呼出し、または他のタイプのソフトウェアあるいはファームウェアなどを、単独または組み合わせて含むものとする。システム５は無線ネットワーク１５も備える。無線ネットワーク１５は、Ｍｏｂｉｌｔｅｘ（商標）、ＤａｔａＴＡＣ（商標）、ＡＭＰＳ、ＴＤＭＡ、ＣＤＭＡ、ＧＳＭ／ＧＰＲＳ、ＰＣＳ、ＥＤＧＥ、ＵＭＴＳ、またはＣＤＰＤが含まれるがそれだけに限定されない、任意の無線通信ネットワークまたは相互接続されたネットワークの組合せでもよい。周知のように、無線ネットワーク１５は、無線周波数（ＲＦ）プロトコルを実装して移動デバイス１０Ａおよび１０Ｂとのデータおよび音声交換をサポートする複数の基地局を備える。ルーティング・サーバ２０は、無線ネットワーク１５に結合される。ルーティング・サーバ２０は、ＳａｎＪｏｓｅ、ＣａｌｉｆｏｒｎｉａのＣｉｓｃｏ Ｓｙｓｔｅｍｓ、Ｉｎｃ．によって販売されているＴＣＰ／ＩＰルータ、またはネットワーク・アドレス変換（ＮＡＴ）サーバなどが含まれるがそれだけに限定されないデータ・パケットをルーティングすることができる任意のタイプのルーティング機器でもよい。

【００１４】
システム５の各移動デバイス１０には固有の個人識別番号（ＰＩＮ）が割り当てられ、それを格納する。各移動デバイス１０用のＰＩＮは、移動デバイス１０が製造されたときに、またはその加入者ＩＤモジュール（ＳＩＭ）によって割り当てられ、移動デバイス１０に格納される。各ＰＩＮは、データを移動デバイス１０にルーティングすることができるようにする無線ネットワーク１５上の対応する移動デバイス１０用にネットワーク・アドレスにマップされる。ルーティング・サーバ２０は、このマッピングに基づいて移動デバイス１０によって送信されるメッセージをルーティングするための１つまたは複数のルーティング・テーブルを含む。例示の一実装形態では、ＰＩＮは実際のネットワーク・アドレス自体でもよく、他の例示の実装形態では、ＰＩＮは、移動デバイス１０の電話番号または移動デバイス１０用の移動加入者ＩＳＤＮ（ＭＳＩＳＤＮ）など固有ＩＤでもよく、ネットワーク・アドレスはＩＰアドレスなどでもよい。理解されるように、本明細書で使用する用語「個人識別番号」または「ＰＩＮ」は、数字の識別子だけに限定されるものではなく、広範に理解されるべきであり、英数字識別子、２値識別子、またはピアツーピア・メッセージングを可能にするために使用することができる他の識別子を含むことができるものとする。

【００１５】
２つの移動デバイス１０の間のピアツーピア・メッセージング・セッションの確立および維持の説明の便宜上、図１で示した移動デバイス１０Ａおよび１０Ｂを参照されたい。しかし理解されるように、任意の２つの移動デバイス１０の間のピアツーピア・メッセージング・セッションに同じ説明が適用される。移動デバイス１０Ａのユーザが、移動デバイス１０Ｂなど他の移動デバイス１０とのピアツーピア・メッセージング・セッションを確立することを望む場合、移動デバイス１０Ａは送信勧誘を生成し、移動デバイス１０Ａと移動デバイス１０Ｂの両方に共通の１つまたは複数の既存の通信アプリケーションを使用して、移動デバイス１０Ｂに送信する。これは、移動デバイス１０Ａの表示装置上でユーザに表示される適切なメニューおよび／またはダイアログ・ボックスを使用して、ピアツーピア・メッセージング・アプリケーションによって容易に行われることが好ましい。たとえば、一実装形態では、ユーザが、メッセージング・アプリケーションに関連したダイアログ・ボックスまたはメニューの送信勧誘オプションを選択して、送信勧誘を開始する。ユーザには、既存の通信アプリケーションを使用して送信勧誘をルーティングするためのアドレス情報を提供するようにプロンプトが出される。たとえば、ユーザは、移動デバイス１０Ｂに関連した電子メール・アドレスを提供することができる。次いで、メッセージング・アプリケーションは、電子メールを作成し、電子メール・アプリケーションを使用して移動デバイス１０Ｂに送信するようにさせる。

【００１６】
送信勧誘は、いずれの場合も、電子メール、ＳＭＳ、ＥＭＳ、あるいはＭＭＳメッセージ、または無線電話呼出しなど、特定の既存の通信アプリケーションに適したメッセージで構成され、そのメッセージは、移動デバイス１０Ｂのユーザが送信勧誘を受諾し、移動デバイス１０Ａとのピアツーピア・メッセージング・セッションを、移動デバイス１０Ｂおよびそのメッセージがピアツーピア・メッセージングを行うための送信勧誘であることを確認する１つまたは複数の標識を使用して確立することを望むかどうかについてのある形の要求を含む。１つまたは複数の標識は、添付物、組込みテキスト、または移動デバイス１０Ｂのメッセージング・アプリケーションがメッセージを送信勧誘として認識することができるようにする他のデータ要素を含むことができる。メッセージング・アプリケーションは、「受信箱」を監視し、または１つあるいは複数の既存の通信アプリケーションと関連したメッセージの受信を監視するように構成される。具体的には、メッセージング・アプリケーションは、到来するメッセージを監視して、そのメッセージがピアツーピア・メッセージング送信勧誘であることを示す１つまたは複数の標識を含むかどうかを判断する。

【００１７】

移動デバイス１０Ｂのメッセージング・アプリケーションは、こうした送信勧誘を受信すると、受諾プロセスまたはルーチンを呼び出す。具体的には、メッセージング・アプリケーションは、移動デバイス１０Ｂのユーザに送信勧誘が受信されたことを知らせ、その送信勧誘を受諾すべきかどうかに関するユーザからの入力を求める。この通知は、電子メール・アドレス、または送信勧誘から得られる他のこうした情報など、移動デバイス１０Ａのユーザを識別する情報を含むことができる。一実装形態では、この通知を移動デバイス１０Ｂのユーザにダイアログ・ボックス、メニュー、ポップアップ・ウィンドウ、または他のグラフィカル・ユーザ・インターフェース（ＧＵＩ）の形のメッセージング・アプリケーションによって表示することができる。通知ウィンドウまたはインターフェースは、一実装形態では、選択可能なボタンまたは他のグラフィカル入力機能を含んで、移動デバイス１０Ｂのユーザがその送信勧誘が受諾されたかどうかを示すことができるようにする。

【００１８】

移動デバイス１０Ｂのユーザが、送信勧誘を受諾し、したがってピアツーピア・メッセージング・セッションの確立を望むことを、たとえばＧＵＩの「受諾」ボタンを選択することによって示した場合、移動デバイス１０Ｂのメッセージング・アプリケーションは、受諾通信を発信移動デバイス１０Ａに適した既存の通信アプリケーションで伝送させる。たとえば一実装形態では、メッセージング・アプリケーションは、受諾電子メールを作成し、電子メール・アプリケーションを使用して送信させる。移動デバイス１０Ａのメッセージング・アプリケーションは、受諾電子メールなど受諾メッセージの受信を認識するように構成される。

【００１９】

既存の通信アプリケーションを使用した送信勧誘および受諾の交換に追加して、またはそれと併せて、移動デバイス１０Ａおよび１０ＢはＰＩＮを交換する。一実装形態では、移動デバイス１０Ｂ用のＰＩＮは受諾メッセージと共に送信される。一実装形態では、移動デバイス１０Ａ用のＰＩＮを、送信勧誘メッセージと共に、または受諾メッセージの受信に後続する肯定応答メッセージと共に送信することができる。

【００２０】

本出願によれば、移動デバイス間でＰＩＮを交換する必要があっても、ＰＩＮの秘密性および機密性が維持される。ユーザのＰＩＮを安全でないチャネルで送信することによって他のユーザに全般的に使用可能になった場合、他のユーザがそのＰＩＮを広範なユーザと共有しやすくなり、または許可されていない受信者がメッセージを傍受してＰＩＮを取得しやすくなる。大抵の既存の通信アプリケーションは、電子メールのように、安全でないチャネルを使用している。その結果、移動デバイスが、その移動デバイスのＰＩＮを取得した望まないソースからメッセージを受信することがある。したがって、本出願で開示した実装形態では、ＰＩＮは暗号化された形で交換される。

【００２１】

暗号化されたＰＩＮを、既存の通信アプリケーションを使用して送信されるメッセージに直接組み込むことができ、またはメッセージに添付することができる。たとえば、電子メール・アプリケーションでは、暗号化されたＰＩＮをバイナリ・ファイルとして添付することができる。理解されるように、バイナリ・ファイルが添付された電子メールは、ファイアウォールおよびスパム・フィルタを通過する際に問題を起こすことがある。したがって、他の実装形態では、暗号化されたＰＩＮが電子メールの本文に直接組み込まれる。この実装形態では、電子メールの読取装置は暗号化ＰＩＮを一連の不可解なテキスト記号として見るであろうが、メッセージング・アプリケーションはその暗号化ＰＩＮを抽出し復号化するように構成される。暗号化ＰＩＮおよび関連する鍵管理および鍵交換操作に関するさらなる詳細を以下に提供する。

【００２２】

理解されるように、上記の工程が完了した後、移動デバイス１０Ａは移動デバイス１０Ｂ用のＰＩＮを有し、移動デバイス１０Ｂは移動デバイス１０Ａ用のＰＩＮを有する。次

に、移動デバイス１０Ａまたは１０Ｂのどちらかが他方にピアツーピア・メッセージを送信することを望む場合、移動デバイスはピアツーピア・メッセージング・アプリケーションを使用してピアツーピア・メッセージを準備する。ピアツーピア・メッセージには、送信すべきメッセージ情報と共に、メッセージ・ヘッダに受信側移動デバイス１０（場合によって１０Ａまたは１０Ｂ）のＰＩＮが含まれることが好ましい。次いでピアツーピア・メッセージは、移動デバイス１０によって無線ネットワーク１５を介してルーティング・サーバ２０に送信される。ルーティング・サーバ２０は、ピアツーピア・メッセージからＰＩＮを獲得し、それを使用して、受信側移動デバイス１０（場合によって１０Ａまたは１０Ｂ）のネットワーク・アドレスをルーティング・サーバ２０に格納された１つまたは複数のルーティング・テーブルを使用して決定し、メッセージを受信側移動デバイス１０（場合によって１０Ａまたは１０Ｂ）に無線ネットワーク１５を介し決定されたネットワーク・アドレスを使用して送信する。受信後、ピアツーピア・メッセージ、具体的にはその中に含まれたメッセージ情報を受信側移動デバイス１０（場合によって１０Ａまたは１０Ｂ）のユーザに表示することができる。

【００２３】

次に、図５を参照されたい。図５は、移動デバイス１０の例示の実装形態を示すブロック図である。この例示の実装形態では、移動デバイス１０はデータを有し、場合によっては音声通信能力も有することができる両方向移動通信デバイス１０である。例示の一実装形態では、デバイス１０は、インターネットで他のコンピュータ・システムと通信する能力を有する。移動デバイス１０によって提供される機能性によって、様々な実装形態で、このデバイスは、データ通信デバイス、データと音声の両方の通信用に構成された多重モード通信デバイス、移動電話、ＰＤＡ可能な無線通信、または、とりわけ無線モデムを備えたコンピュータ・システムでもよい。

【００２４】

デバイス１０は、通信サブシステム１１１を含み、この通信サブシステム１１１は、受信器１１２、送信機１１４、および１つまたは複数の好ましくは組込み型または内部のアンテナ要素１１６および１１８など関連する構成要素、並びにディジタル信号プロセッサ（ＤＳＰ）１２０など処理モジュールを備える。一部の実装形態では、通信サブシステムは１つまたは複数のローカル発振器（ＬＯ）１１３を備え、また一部の実装形態では、通信サブシステム１１１とマイクロプロセッサ１３８が１つの発振器を共有する。通信分野の当業者には理解されるように、通信サブシステム１１１の具体的な設計は、デバイス１０が動作することが意図された通信ネットワークに依存するものである。

【００２５】

無線ネットワーク１５を介してアンテナ１１６によって受信される信号は、受信器１１２に入力され、受信器１１２は、信号増幅、周波数下方変換、フィルタリング、チャネル選択など通常の受信器機能を実装し、一部の実装形態ではアナログ・デジタル変換器の機能を実装することができる。同様の方法で、伝送すべき信号が、たとえばＤＳＰ１２０による変調および暗号化を含む処理を受け、送信機１１４に入力されて、ディジタル・アナログ変換、周波数上方変換、フィルタリング、増幅、およびアンテナ１１８を介した無線ネットワーク１５上での伝送が行われる。

【００２６】

デバイス１０は、デバイスの動作全体を制御するマイクロプロセッサ１３８を備える。このマイクロプロセッサ１３８は、通信サブシステム１１１と対話し、さらにグラフィックス・サブシステム１４４、フラッシュ・メモリ１２４、ランダム・アクセス・メモリ（ＲＡＭ）１２６、加入者識別モジュール（ＳＩＭ）１５６、補助入出力（Ｉ／Ｏ）サブシステム１２８、シリアル・ポート１３０、キーボードまたはキーパッド１３２、スピーカ１３４、マイクロフォン１３６、近距離通信サブシステム１４０、および全般的に１４２で示した任意の他のデバイス・サブシステムなどデバイス・サブシステムとも対話する。グラフィックス・サブシステム１４４は、ディスプレイ１２２と対話し、グラフィックスまたはテキストをディスプレイ１２２上に表示する。

【００２７】
マイクロプロセッサ１３８によって使用されるオペレーティング・システム・ソフトウェア１５４および多様なソフトウェア・アプリケーション１５８は、例示の一実装形態では、フラッシュ・メモリ１２４など永続記憶装置または同様の記憶要素に格納される。当業者には理解されるように、オペレーティング・システム１５４、ソフトウェア・アプリケーション１５８、またはその一部をＲＡＭ１２６など揮発性記憶装置に一時的にロードすることができる。受信通信信号をＲＡＭ１２６に格納することもできることが企図されている。

【００２８】
マイクロプロセッサ１３８は、そのオペレーティング・システム機能の他に、デバイスのソフトウェア・アプリケーション１５８の実装が可能であることが好ましい。所定のセットの通信アプリケーション１６２を製造中にデバイス１０に導入することができる。通信アプリケーション１６２は、データ通信アプリケーションおよび／または音声通信アプリケーションを含むことができる。通常のデータ通信アプリケーションは、電子メッセージング・モジュールを含んで、ユーザがテキストベースのメッセージを受信し、読み取り、作成し、送信することができるようにする。たとえば、電子メッセージング・モジュールは、電子メール・アプリケーション、ＳＭＳアプリケーション、ＭＭＳアプリケーション、および／またはＥＭＳアプリケーションを含むことができる。さらにソフトウェア・アプリケーション１５８および／または通信アプリケーション１６２をデバイス１０に、無線ネットワーク１５、補助Ｉ／Ｏサブシステム１２８、シリアル・ポート１３０、近距離通信サブシステム１４０、または任意の他の適したサブシステム１４２を介してロードすることができ、またはユーザがＲＡＭ１２６または不揮発性記憶装置に格納してマイクロプロセッサ１３８によって実装することもできる。アプリケーション導入のこうした柔軟性によって、デバイス１０の機能性が向上し、拡張されたデバイスの機能、通信関連機能、またはその両方を提供することができる。

【００２９】
データ通信モードでは、ダウンロードされたテキスト・メッセージまたはウェブ・ページのダウンロードなどの受信信号が通信サブシステム１１１によって処理され、マイクロプロセッサ１３８に入力され、それによって受信信号がさらに処理されて、ディスプレイ１２２にグラフィックス・サブシステム１４４あるいは補助Ｉ／Ｏサブシステム１２８を介して出力される。デバイス１０のユーザは、キーパッド１３２をディスプレイ１２２および場合によっては補助Ｉ／Ｏサブシステム１２８と併せて使用して、ソフトウェア・アプリケーション１５８、またはたとえば電子メール・メッセージなど通信アプリケーション１６２でデータ・アイテムを作成することもできる。次いで、この作成されたアイテムを通信ネットワークを介して通信サブシステム１１１によって伝送することができる。

【００３０】
図５で示したシリアル・ポート１３０は、通常、ユーザのデスクトップ・コンピュータ（図示せず）との同期化が望ましい携帯情報端末（ＰＤＡ）タイプの通信デバイスで実装されるが、これは任意選択のデバイス構成要素である。こうしたポート１３０によって、ユーザが外部デバイスまたはソフトウェア・アプリケーションによって選好を設定することができるようなり、情報またはソフトウェアのデバイス１０へのダウンロードを無線通信ネットワークを介さずに可能にすることによって、デバイスの能力が拡大される。

【００３１】
近距離通信サブシステム１４０は、デバイス１０と様々なシステムまたはデバイスとの間の通信を提供することができるさらなる構成要素であるが、必ずしも同様のデバイスである必要はない。たとえば、サブシステム１４０は、赤外線デバイスおよび関連する回路と構成要素、またはＢｌｕｅｔｏｏｔｈ（商標）通信モジュールを含んで、同様に可能なシステムおよびデバイスとの通信を提供することができる。デバイス１０は、ハンドヘルド・デバイスでもよい。

【００３２】

デバイス１０は、さらにメッセージング・アプリケーション１６０を含む。メッセージング・アプリケーション１６０は、モニタ構成要素、送信勧誘構成要素、および受諾構成要素を含むことができ、それらを集合的に連絡先管理構成要素と呼ぶことができる。連絡先管理構成要素の役割は、連絡先または「メンバー」関係を確立すること、すなわち、新しい連絡先の送信勧誘および受諾の送信または受信に基づいて連絡先情報を更新し維持することである。メッセージング・アプリケーション１６０は、さらに、連絡先情報を使用してピアツーピア・メッセージングを行うためのメッセージング構成要素を含む。

【００３３】

移動デバイス１０に関連するＰＩＮはメモリに格納される。ＰＩＮは、たとえばＳＩＭ１５６、ＲＡＭ１２６、ファームウェアに、または別の方法で格納することができる。デバイス１０のメモリには、メッセージング・アプリケーション１６０に関連して使用される連絡先情報も格納される。連絡先情報は、連絡先名および関連するＰＩＮを含む。

【００３４】

メッセージング・アプリケーション１６０の送信勧誘構成要素は、送信勧誘を作成して予定の連絡先に送信する。デバイス１０のユーザは、メッセージング・アプリケーション１６０が送信勧誘を他のデバイスに送信するように命令する。ユーザは、電子メール・アドレスなど、他のデバイスに到達するためのアドレスを提供することができる。送信勧誘構成要素は、送信勧誘メッセージを生成して、電子メール・アプリケーションなど通信アプリケーション１６２の１つを介して送信する。

【００３５】

メッセージング・アプリケーション１６０のモニタ構成要素は、他の移動デバイス１０からの送信勧誘メッセージの受信を監視する。たとえば、モニタ構成要素は、電子メール・アプリケーションの受信箱を監視して、受信メッセージがメッセージング送信勧誘かどうかを判断する。メッセージング送信勧誘は、所定のテキスト、コード、または他のデータ要素を含んで、それがメッセージング送信勧誘であることを示すことができる。モニタ構成要素が送信勧誘であることを確認した場合、モニタ構成要素はユーザに知らせ、ユーザがその送信勧誘を受諾または拒否するようにプロンプトを出す。たとえば、モニタ構成要素は、送信勧誘の送信者に関する情報を示し、ユーザに「受諾」および「拒否」ボタンなどの選択を提供するダイアログ・ボックスまたはポップアップ・ウィンドウを表示することができる。ユーザが送信勧誘の受諾を示した場合、受諾構成要素が起動される。

【００３６】

受諾構成要素は、受諾メッセージを自動的に生成し、それを電子メール・アプリケーションなど通信アプリケーション１６２の１つを介して送信する。

メッセージング・アプリケーション１６０は、ＰＩＮを交換するための、暗号化、復号化、および関連鍵管理機能を実装する構成要素を含む。こうした構成要素を送信勧誘および受諾構成要素の一部として、またはそれと対話する別々の構成要素として提供することができる。こうした構成要素は、常駐ＰＩＮの暗号化、任意の必要とされる鍵値またはセッション鍵の生成および計算、暗号化されたＰＩＮをメッセージに添付または組み込んで既存の通信アプリケーション１６２の１つを介して送信すること、および他の移動デバイス１０から通信アプリケーション１６２の１つを介して受信された暗号化ＰＩＮの復号化を管理する。送信勧誘アーキテクチャのコンテキストでの暗号化、復号化、および鍵交換に関してさらに詳細に以下に記載する。

【００３７】

再び図１を参照されたい。一実装形態では、上述の送信勧誘を複数の通信経路で複数の既存の通信アプリケーションを使用して送信することによって、セキュリティをピアツーピア・メッセージングで向上させることができる。理解されるように、各通信経路は、送信勧誘の送信者の様々なアドレスＩＤ確認することによって、送信勧誘の確実性を確認する助けをする。たとえば、移動デバイス１０Ａのユーザは、電子メール・アプリケーションとＳＭＳアプリケーションの両方を使用して、上述のように送信勧誘を送信することによって、移動デバイス１０Ｂのユーザとのピアツーピア・メッセージング・セッションを

確立することを望むことができる。この場合、送信勧誘メッセージが移動デバイス１０Ｂによって受信されたときに、移動デバイス１０Ｂの「受信箱」または同様のものが移動デバイス１０Ａからの２つのメッセージ、すなわち電子メール送信勧誘およびＳＭＳ送信勧誘を示す。メッセージが到達したときに、移動デバイス１０Ｂのユーザが、カレンダ・アプリケーション、アドレス帳アプリケーション、またはブラウザ・アプリケーションあるいは電話アプリケーションなど、移動デバイス１０Ｂの任意のアプリケーションを作動している可能性があり、またはその時点で移動デバイス１０Ｂを（電源が入っていても）全く使用していない可能性もある。ユーザには、移動デバイス１０Ｂによって受信される任意の他のメッセージと同じ方法で（たとえば、呼び出し音および／または振動によって）送信勧誘メッセージの到来が知らされる。移動デバイス１０Ｂのユーザがこの２つのメッセージのどちらかを開封した場合、ピアツーピア・メッセージング・アプリケーションが呼び出されてそのメッセージを処理する。ピアツーピア・メッセージング・アプリケーションの自動呼出しは、各送信勧誘の形に関係なく特別の標識を提供して、それがピアツーピア・メッセージング・セッションのための送信勧誘であることを示し、ピアツーピア・アプリケーションが到来するメッセージ全てをこうした標識について監視するようにプログラミングすることによって行うことができる。さらに、各送信勧誘メッセージは、ピアツーピア・メッセージング・アプリケーションで生成された場合に、（様々な経路で）送信された送信勧誘メッセージの数の標識を含む。この例のように複数の経路が使用された場合、ピアツーピア・メッセージング・アプリケーションは次に他の１つまたは複数の送信勧誘メッセージについて「受信箱」または同様のものを走査する。たとえば、電子メール送信勧誘メッセージが最初に開封された場合、ピアツーピア・メッセージング・アプリケーションはＳＭＳ送信勧誘メッセージについて「受信箱」または同様のものを走査する。上記のように、メッセージに提供された特別の標識によって送信勧誘メッセージを識別することができる。この実装形態では、ピアツーピア・メッセージング・アプリケーションは、移動デバイス１０Ｂのユーザに他の１つまたは複数の送信勧誘メッセージが見つかるまで送信勧誘を受諾する能力を提供しない。１つまたは複数の他の送信勧誘メッセージが発見された後、移動デバイス１０のユーザはその送信勧誘を上記のように受諾、拒否、または受諾あるいは拒否の決定を延期することができる。

【００３８】

次に、図４を参照されたい。図４は、ユーザにメッセージング送信勧誘の受信を知らせるためのグラフィカル・ユーザ・インターフェース２００の例示の一実装形態を示す図である。グラフィックス・ユーザ・インターフェース２００は、受信箱表示画面２０２の上にオーバレイまたはカスケードされたポップアップ・ダイアログ・ボックス２０４を含む。図４で示されたポップアップ・ダイアログ・ボックス２０４は、送信者の名前、時刻、日付を示し、この送信勧誘の送信に複数の経路が使用されたことを確認し、それによってソースに関してある認証を提供する。ポップアップ・ダイアログ・ボックス２０４は、その送信勧誘の受諾、送信勧誘の拒否、および送信勧誘を受諾するか拒否するかどうかの決定を遅らせるオプションに対応する３つの選択可能なボタンもユーザに提示する。

【００３９】

再び図１および５を参照されたい。上記のように、本出願に記載した送信勧誘アーキテクチャでは、それぞれ移動デバイス１０のＰＩＮは既存の通信アプリケーションの１つを使用して隠密に交換される。送信側移動デバイスはそのＰＩＮを暗号化してから、通信アプリケーションを使用してそれを伝送する。受信側移動デバイスで、受信された暗号化ＰＩＮが復号化される。適切な鍵管理によって、非暗号化ＰＩＮへのアクセスがそれぞれ２つの移動デバイスのメッセージング・アプリケーションに限定される。

【００４０】

本出願の範囲で様々な実装形態に使用することができる幾つかの暗号化および鍵管理技法がある。さらに、鍵値と共に使用してＰＩＮを暗号化ＰＩＮに変換することができる特定の変換または関数には、広範な暗号変換または関数が含まれる。当業者には理解されるように、広範なこうした関数が知られており、特定のアプリケーションまたはシステムに

関連する処理電力および常時の制約を考慮して選択することができる。

【００４１】

一実装形態では、メッセージング・アプリケーション１６０は対称暗号化を使用する。対称暗号化は、鍵ペアの１つの鍵を他の鍵から確定するのが計算的に容易な場合の暗号化技法である。大抵の対称暗号方式では、鍵は同一である。対称暗号化は、鍵の機密性に依存する。したがって、鍵ペアは通常、安全に分配され、非セキュア・チャネルでは分配されない。一実装形態では、移動デバイス１０Ａのユーザは、音声チャネルなど比較的安全なチャネルを使用して、移動デバイス１０Ｂのユーザに鍵値または鍵を導出することができるシード値を提供する。たとえば、第１のユーザは第２のユーザにコードワードまたはパスワードを提供し、第２のユーザにプロンプトが出された場合に第２のユーザがそれを移動デバイス１０Ｂに入力する。コードワードまたはパスワードをシード値としてアルゴリズムと共に使用して、通信の暗号化および復号化に使用する秘密鍵を計算することができる。

【００４２】

他の実装形態では、メッセージング・アプリケーション１６０は公開鍵暗号化を使用する。公開鍵暗号化は、暗号化変換および復号化変換を有する暗号化技法であり、暗号化変換からの復号化変換の確定が計算的に実行不可能である。換言すれば、暗号化関数は、出力暗号文を提供するトラップドア一方向関数である。暗号文および暗号化鍵を知っていても、復号化鍵を決定することができないため、非暗号化コンテンツを得ることができない。

【００４３】

公開鍵暗号化は、各移動デバイス１０に公開／秘密鍵ペアを生成させることによって機能する。各デバイスは、その公開鍵を共有するが、秘密鍵の機密性を保護する。他のデバイスは、第１のデバイスへのメッセージを第１のデバイスの公開鍵を使用して暗号化することができるが、第１のデバイスだけが対応する秘密鍵を有しているため、第１のデバイスだけがそのメッセージを復号化することができる。

【００４４】

本明細書に記載したメッセージング・システムのコンテキストでは、メッセージング・アプリケーション１６０は鍵ペア生成および鍵交換を管理する構成要素を含む。鍵ペアは、たとえば時刻および日付など無作為のシード値、または他の擬似無作為のシードから生成される。各移動デバイス１０用の公開鍵は、通信アプリケーション１６２の１つを使用して他の移動デバイス１０に通信される。たとえば公開鍵値を、１つの移動デバイス１０Ａから他の移動デバイス１０Ｂに送信される電子メールに組込み、または添付することができる。一部の実装形態では、開始移動デバイス１０Ａのメッセージング・アプリケーション１６０は、その公開鍵K_aを受信側移動デバイス１０Ｂに送信される送信勧誘メッセージに組込みまたは添付する。受信側移動デバイス１０は、その公開鍵K_bを開始移動デバイス１０Ａに送信される受諾メッセージに組込みまたは添付する。一実装形態では、メッセージング・アプリケーション１６０によって送信勧誘および受諾手順を実行するために使用される通信アプリケーション１６２は、電子メール・アプリケーションである。こうした実装形態では、公開鍵をバイナリ・ファイルとして電子メールに添付することができる。あるいは、電子メール・テキスト本文に組み込むことができる。当業者は、公開鍵データの既存の通信アプリケーション・メッセージへの添付または組込みの可能な範囲に精通しているであろう。

【００４５】

次に、図６を参照されたい。図６は、移動メッセージング・システムでのＰＩＮの安全な交換方法３００を示す流れ図である。図６で示した方法３００は、公開鍵暗号方式を使用する一実装形態に関連する。

【００４６】

この方法３００は工程３０２で開始され、第１の公開／秘密鍵ペアE_A、D_Aが第１のデバイス１０Ａ（図１）のメッセージング・アプリケーション１６０（図５）によって生

成される。鍵ペアは、デバイス１０Ａによって送信される送信勧誘ごとに生成され、またはデバイス１０Ａによって１回だけ、あるいは単に定期的に生成され、２つ以上の送信勧誘メッセージング・プロセスに使用される。

【００４７】

工程３１０で、第２のデバイス１０Ｂは第２の公開／秘密鍵ペアE_B、D_Bを生成する。工程３０２に関して、工程３１０を受信された送信勧誘ごとに新規に実装することができ、または１回（あるいは定期的に）計算し、２つ以上の送信勧誘メッセージング・プロセスで使用することができる。理解されるように、デバイス１０によって生成された公開／秘密鍵ペアＥ、Ｄを、開始デバイスとしての送信勧誘の送信と、受信デバイスとしての送信勧誘への応答の両方に使用することができる。一部の実装形態では、鍵ペアはオフラインで生成され、製造または配備時にデバイス１０に格納される。

【００４８】

デバイス１０Ａのユーザは、送信勧誘コマンドをメッセージング・アプリケーション１６０に提供することによって送信勧誘プロセスを起動させる。送信勧誘コマンドは、ユーザがメニューから選択してもよい。ユーザは、送信勧誘の意図される受信者にアドレスまたは他の連絡先情報を提供するように要求される。この送信勧誘コマンドによって、メッセージング・アプリケーション１６０の送信勧誘構成要素が呼び出され、それによって、工程３０４で送信勧誘メッセージが作成される。このメッセージは、電子メール・アプリケーションなど通信アプリケーション１６２の１つを使用して作成される。メッセージング・アプリケーション１６０によって、作成されたメッセージが、受信側移動デバイス１０Ｂのメッセージング・アプリケーション１６０にそのメッセージが送信勧誘であることを知らせるための標識を含むことが保証される。

【００４９】

工程３０６で、メッセージング・アプリケーション１６０は、第１の公開鍵E_Aを作成された送信勧誘メッセージに添付し、または組み込む。一実装形態では、メッセージは電子メール・メッセージであり、第１の公開鍵E_Aが電子メール・メッセージのテキスト本文に挿入されてそのメッセージがファイアウォールおよびスパム・フィルタを通過することができるようになされる。

【００５０】

工程３０８で、通信アプリケーションは、送信勧誘メッセージを受信側移動デバイス１０Ｂに送信する。このメッセージは、受信側移動デバイス１０Ｂで通信アプリケーション用の「受信箱」内に現れる。送信勧誘メッセージの受信時またはユーザがその送信勧誘メッセージを開封した後に、メッセージング・アプリケーション１６０のモニタ構成要素はそれが送信勧誘であることを認識する。したがって工程３１２で、メッセージング・アプリケーション１６０が起動される。

【００５１】

メッセージング・アプリケーション１６０は、工程３１４で、ユーザにユーザがその送信勧誘を受諾または拒否するかどうかを決定することを問い合わせる。ユーザが送信勧誘を拒否した場合、方法３００が終了する。ユーザが送信勧誘を受諾した場合、メッセージング・アプリケーション１６０は工程３１６で、第１の公開鍵E_Aを送信勧誘メッセージから抽出する。工程３１８で、抽出した第１の公開鍵E_Aを使用して、所定の暗号変換または関数に従ってＰＩＮを第２の移動デバイス１０Ｂ用（すなわちPIN_B）に暗号化する。次いで工程３２０で、メッセージング・アプリケーション１６０は、受諾メッセージを作成して、電子メール・アプリケーションなど通信アプリケーション１６２の１つを介して送信する。この受諾メッセージは、暗号化PIN_Bおよび第２の公開鍵E_Bを含む。暗号化PIN_Bおよび第２の公開鍵E_Bを受諾メッセージに組込み、または添付することができる。次いで工程３２２で、この受諾メッセージは、第１の移動デバイス１０Ａに送信される。

【００５２】

第１の移動デバイス１０Ａのメッセージング・アプリケーション１６０は、受信時また

はユーザがメッセージを開封した後に受諾メッセージを認識し、工程３２４で受諾メッセージから第２の公開鍵E_Bを抽出する。工程３２６で、メッセージング・アプリケーション１６０は、所定の暗号化変換または関数に従って開始移動デバイス１０Ａ用（すなわちPIN_A）のＰＩＮを暗号化する。次いでメッセージング・アプリケーション１６０は、工程３２８で、肯定応答メッセージを作成して、電子メール・アプリケーションなど通信アプリケーション１６２の１つを介して送信する。この肯定応答メッセージは、肯定応答メッセージに組込み、または添付することができる暗号化PIN_Aを含む。次いで工程３３０で、この肯定応答メッセージは、第２の移動デバイス１０Ｂに送信される。

【００５３】

各移動デバイス１０は、工程３３２および３３４で示したように、受信した暗号化ＰＩＮをそれぞれその秘密鍵D_A、D_Bを使用して復号化する。次いで、デバイス１０は、他のデバイス１０のユーザのための連絡先情報と関連して復号化ＰＩＮを格納する。したがって、他のデバイス１０のユーザは、いまやメッセージング・アプリケーション１６０によって使用される「メンバー・リスト」または連絡先リストの一部である。次にメッセージは、１つのユーザから他のユーザにメッセージング・アプリケーションを使用して直接送信されて、ルーティングのための他のユーザのＰＩＮを組み込んだメッセージが作成される。

【００５４】

他の実装形態では、メッセージング・アプリケーション１６０は、Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ鍵共有プロトコルを使用して、２つの移動デバイス１０間で共有される秘密鍵を確立する。このプロトコルは、２つのパラメータｐおよびｇを必要とする。ただし、ｐは素数であり、ｇはｐより小さい数であり、プロパティは、１とｐ－１との間のそれを含む全ての数ｎごとにｇの電力ｋがありｎ＝g^k ｍｏｄ ｐである。本出願のピアツーピア・メッセージング・システムのメッセージング・アプリケーション１６０のコンテキストでは、第１のメッセージング・アプリケーションが、秘密値ａおよび公開値g^a ｍｏｄ ｐを生成する。ただし、ａは１からｐ－２までから選択された整数である。第２のメッセージング・アプリケーションは、それ自体の秘密値ｂおよび公開値g^b ｍｏｄ ｐを生成する。ただしｂは１からｐ－２までの整数である。メッセージング・アプリケーションは、図５と併せて上記に記載したように、公開値を交換し、次いで共有セッション鍵ｋをｋ＝g^{ba}＝$(g^a)^b$ ｍｏｄ ｐの関係から計算する。

【００５５】

他の実装形態では、本出願の送信勧誘アーキテクチャは、パスコード・ベースの認証手順を含む。第１の移動デバイスから第２の移動デバイスに送信される送信勧誘は質問を含む。第２の移動デバイスのユーザに提示されるＧＵＩダイアログ・ボックスは、質問の表示を含み、ユーザに応答の選択または送信の機会を提供する。応答は、第２のデバイスから第１のデバイスに伝送される受諾メッセージと共に伝送される。第１のデバイスは、受諾メッセージに含まれた応答と第１の移動デバイスに格納された正しい応答を比較して第２の移動デバイスのユーザのＩＤを認証する。第１の移動デバイスのユーザは、第２の移動デバイスのユーザに正しい応答を音声呼など代替通信アプリケーションを介して提供することができる。パスコード・ベースの認証手順によって、メッセージング関係が正しい当事者間で確立されることを保証するセキュリティの強化がもたらされる。

【００５６】

次に、図１を再び参照されたい。本出願の他の態様によれば、各移動デバイス１０のピアツーピア・メッセージング・アプリケーションには、名前および／または他の識別情報、および移動デバイス１０のユーザがピアツーピア・メッセージング・アプリケーションを使用して通信した、または通信を望む、他の移動デバイス１０のユーザごとの対応するＰＩＮを格納する連絡先データベースが含まれる。したがって、この連絡先データベースは、ＩＭアプリケーションの一部である「メンバー・リスト」と同様のものである。ユーザおよびＰＩＮ情報を、ユーザが他のユーザとのピアツーピア・メッセージング・セッションを確立する度に連絡先データベース部に追加または格納することができる。入力を連

絡先データベースから選択的にユーザによって削除することもできる。図２は、ピアツーピア・メッセージング・アプリケーションの一部であり、連絡先データベースに格納された連絡先のリスト３０を表示する例示の連絡先データベース画面２５を示す移動デバイス１０の表示の一部を示す図である。図２で分かるように、連絡先データベース画面２５はリスト３０にリストされた連絡先ごとに、「暗黙的可用性」と呼ばれるピアツーピア・メッセージング・セッションに関与するための特定の連絡先の可用性に関連する状況情報３５も提供する。この可用性情報を以下でより詳細に論じる。

【００５７】

本出願のさらなる態様によれば、（分かりやすくするために「第１の移動デバイス１０」と呼ばれる）各移動デバイス１０は、データ・トラフィックを最低限に抑えるために１０分ごとなど定期的に、それに付随する可用性情報を第１の移動デバイス１０の連絡先データベースにリストされた各ユーザの（分かりやすくするために「他の移動デバイス１０」と呼ばれる）移動デバイス１０に、無線ネットワーク１５またはルーティング・サーバ２０を介してこうした各ユーザの格納されたＰＩＮを使用して伝送する。特定の一実装形態では、他の移動デバイス１０の任意のものが範囲外に存在する場合、ルーティング・サーバ２０は、こうした他の移動デバイス１０を対象とする幾つかの可用性情報メッセージをキューに入れ、他の移動デバイス１０がターン・オンされ、または範囲内に戻った後にそれらを転送する。可用性情報は、時間が経過するにつれて変化し、第１の移動デバイス１０の現在の動作状態から導出される。可用性情報は、第１の移動デバイス１０でのユーザのアクティビティを表示して、連絡先データベースにある他の移動デバイス１０の各ユーザに、第１の移動デバイス１０のユーザが第１の移動デバイス１０のユーザに送信されたピアツーピア・メッセージを呼んで返答する可能性の高さを推定して提供するものである。したがって、システム５の移動デバイス１０全てが（以下に記載するように使用不可でない場合に）、その可用性情報を連絡先全てに伝送するため、理解されるように、システム５の各移動デバイス１０はその連絡先データベースにあるそれぞれ他のユーザについての可用性情報を有する。その結果、移動デバイス１０全てのユーザが移動デバイス１０の連絡先データベースにリストされた連絡先全ての可用性情報を考慮して、特定の連絡先がピアツーピア・メッセージを受信し応答する可能性が高いかどうかに関するアイデアを得ることができる。この情報はピアツーピア・メッセージを送信するかどうかに関する決定に影響を与える。

【００５８】

可用性情報は、たとえば、移動デバイス１０の電源が入っており無線ネットワーク１５の範囲内に存在し、電話アプリケーションを使用して通話中であるなどピアツーピア・メッセージが受信されるのを妨げるアプリケーションをアクティブにして使用していないことを示す「使用可能」、または、たとえば移動デバイス１０の電源が入っていない、あるいは無線ネットワーク１５の範囲外に存在することなどを示す「使用不可能」などの通常の状況標識で構成することができる。さらに、可用性情報は、到来する電話呼を無視する、ユーザが移動デバイス１０の電源をオフにする、第１の移動デバイス１０が現在通話中である、第１の移動デバイス１０のユーザが移動デバイス１０に提供されたカレンダ・アプリケーションへの入力で示されたように会議中である、または移動デバイス１０のユーザが現在ピアツーピア・メッセージング・アプリケーションを使用している、など移動デバイス１０に発生する特定の状態またはイベントに関連付けることができる。理解されるように、可用性情報を移動デバイス１０の動作全ておよび／または移動デバイス１０で使用可能な情報一部に結合することができ、かつそれから導出することができ、上記にリストした特定の例は単に例示であって限定するものではない。また、通常の状況標識は、移動デバイス１０に発生する特定の状態および／またはイベントに関連する情報に基づく可用性の幾つかのレベルまたは程度を含むことができる。この場合、可用性情報を、「可用性レベル１」、「可用性レベル２」など可用性の様々なレベルまたは程度を示すスケールで報告することができる。さらに、移動デバイス１０の所与のユーザがその可用性をあまり詳細に追跡されることを望まない場合、ユーザは自分の移動デバイス１０が可用性情報

を伝送するのを選択的に阻止することができる。

【００５９】

図３は、ピアツーピア・メッセージング・アプリケーションの一部を形成する例示の状況画面４０を示す移動デバイス１０のディスプレイの一部を示す図である。状況画面４０は、ピアツーピア・メッセージング・アプリケーションの主画面であり、移動デバイス１０のユーザにピアツーピア・メッセージング・アプリケーションに関連する状況情報全体を提供する。具体的には、状況画面４０は、現在の会話グループ４５、ブロックされた通信者グループ５０、および保留の会話グループ５５を含む様々なグループに関連する情報を提供する。現在の会話グループ４５は、移動デバイス１０が現在通話している、会話とも呼ばれるピアツーピア・メッセージング・セッション全てに関連する情報をリストし提供する。現在の会話とは、移動デバイス１０が上記のように送信勧誘を他の移動デバイス１０に送信し、その応答として上記のように受諾メッセージを受信したこと、または他の移動デバイス１０が移動デバイス１０に上記のように送信勧誘を送信し、移動デバイス１０が上記のように受諾メッセージで応答したことを指す。ブロックされた通信者グループ５０は、この移動デバイス１０のユーザがもはやピアツーピア・メッセージの受信を望まない他の移動デバイス１０のユーザのリストを提供する。すなわちそのメッセージはブロックされ、ユーザに表示されない。好ましくは、「使用不可能な」可用性情報が移動デバイス１０によってそれぞれブロックされた通信者に伝送される。あるいは、この移動デバイス１０のユーザがもはやピアツーピア・メッセージの受信を望まない他の移動デバイス１０のユーザからのピアツーピア・メッセージを、こうした他のユーザを連絡先データベースから除去することによって、ブロックしユーザに表示されないようにすることができる。この場合、ピアツーピア・メッセージング・アプリケーションは、連絡先データベースにリストされていないユーザ全てからのメッセージをブロックするように構成されるのである。保留会話グループ５５は、移動デバイス１０の現在の保留中の会話全てに関連する情報を提供する。保留の会話とは、移動デバイス１０が上記のように送信勧誘を他の移動デバイス１０に送信したが、応答をまだ受信していないこと、または他の移動デバイス１０が移動デバイス１０に上記のように送信勧誘を送信したが、移動デバイス１０がまだ応答していないことを指す。

【００６０】

現在の会話グループ４５、ブロックされた通信者グループ５０、および保留の会話グループ５５を選択的に拡張して追加の情報を表示し、または縮小して追加の情報が表示されないようにすることができる。それぞれ現在の会話グループ４５、ブロックされた通信者グループ５０、および保留の会話グループ５５が図３で拡張されて示されている。ユーザは、移動デバイス１０の一部として含まれた、複数のキーおよび／または回転サムホイールなど入力装置で移動デバイス１０に入力することによって、拡張状態と縮小状態をトグルスイッチで選択することができる。拡張状態では、現在の会話グループ４５は、現在の会話ごとに、（１）他の移動デバイス１０に関連付けられているユーザ、（２）他の移動デバイス１０に関連する可用性情報、（３）送信または受信された最近のメッセージの日付および／または時刻をリストする。ピアツーピア・メッセージング・セッションは、たとえば数週間または数ヶ月など長期にわたってオープンかつアクティブのままにすることができるため、項目（３）はどの会話が最もアクティブで現行のものであるかに関する即時参照を提供する。拡張状態では、保留の会話グループ５５は、保留の会話ごとに、（１）他の移動デバイス１０と関連付けられているユーザ、および（２）他の移動デバイス１０と関連する可用性情報をリストする。図３で分かるように、可用性情報を示すアイコン６０が、現在の会話グループ４５および保留会話グループ５５への各入力の次に提供されて、ユーザにとって参照しやすくすることが好ましい。

【００６１】

上記の説明は、ＰＩＮ、鍵、または他のデータ要素を通信アプリケーションの１つによって送信されるメッセージに組込み、または添付する可能性を指すものであるが、理解されるように、本明細書で使用される用語「組み込む」または「組込み」は、添付、組込み

、または別の方法によるメッセージを有するこうしたデータ要素などの伝送または送信を含むものとして広範に解釈されるものである。

【図面の簡単な説明】

【００６２】

【図１】移動デバイス間の即時ピアツーピア・メッセージングを提供するシステムを示すブロック図である。

【図２】ピアツーピア・メッセージング・アプリケーションの一部である例示の連絡先データベース画面を示す移動デバイスのディスプレイの一部を示す図である。

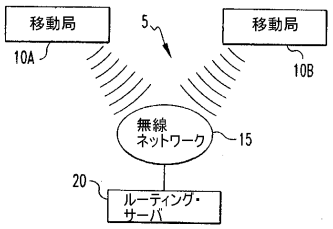
【図３】ピアツーピア・メッセージング・アプリケーションの一部を形成する例示の状況画面を示す移動デバイスのディスプレイの一部を示す図である。

【図４】ユーザにメッセージング送信勧誘の受信を知らせるためのグラフィカル・ユーザ・インターフェースの例示の一実装形態を示す図である。

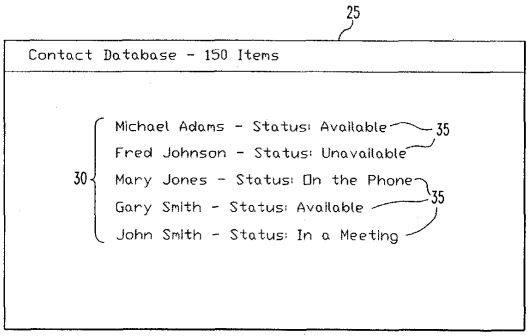
【図５】ピアツーピア・メッセージングを提供するように構成された移動デバイスを示すブロック図である。

【図６】移動メッセージング・システムでの個人識別番号の安全な交換方法を示す流れ図である。

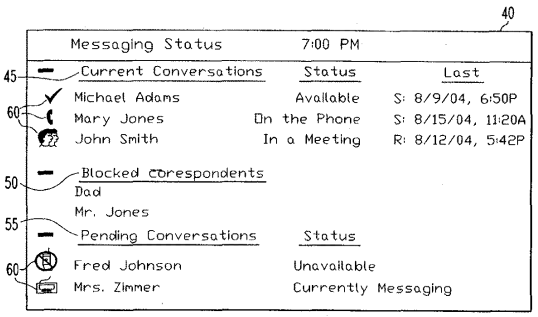
【図１】



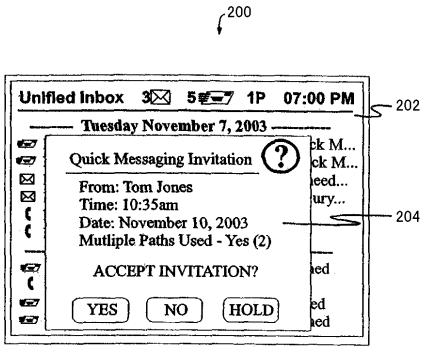
【図２】



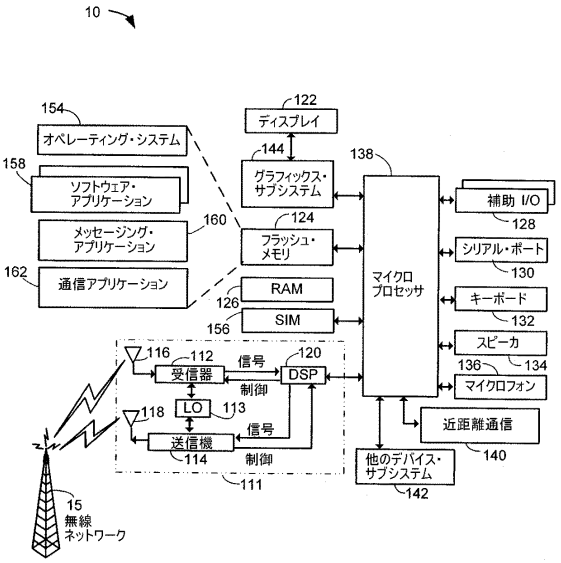
【図３】



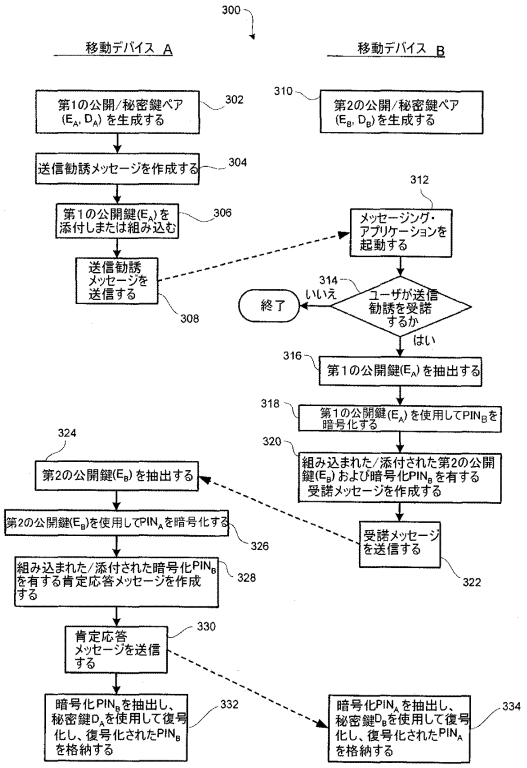
【図４】



【図５】


10
154
オペレーティング・システム
158
ソフトウェア・アプリケーション
160
メッセージング・アプリケーション
162
通信アプリケーション
122
ディスプレイ
144
グラフィックス・サブシステム
124
フラッシュ・メモリ
126
RAM
156
SIM
138
マイクロプロセッサ
128
補助 I/O
130
シリアル・ポート
132
キーボード
134
スピーカ
136
マイクロフォン
140
近距離通信
142
他のデバイス・サブシステム
116
112
受信器
信号
120
DSP
制御
118
LO
113
送信機
114
信号
制御
111
15
無線ネットワーク

【図６】


300
移動デバイス A
移動デバイス B
第1の公開/秘密鍵ペア (E_A, D_A) を生成する
302
第2の公開/秘密鍵ペア (E_B, D_B) を生成する
310
送信勧誘メッセージを作成する
304
第1の公開鍵(E_A)を添付しまたは組み込む
306
メッセージング・アプリケーションを起動する
312
送信勧誘メッセージを送信する
308
終了
いいえ
314
ユーザが送信勧誘を受諾するか
はい
第1の公開鍵(E_A)を抽出する
316
第1の公開鍵(E_A)を使用してPIN$_B$を暗号化する
318
組み込まれた/添付された第2の公開鍵(E_B)および暗号化PIN$_B$を有する受諾メッセージを作成する
320
受諾メッセージを送信する
322
第2の公開鍵(E_B)を抽出する
324
第2の公開鍵(E_B)を使用してPIN$_A$を暗号化する
326
組み込まれた/添付された暗号化PIN$_B$を有する肯定応答メッセージを作成する
328
肯定応答メッセージを送信する
330
暗号化PIN$_B$を抽出し、秘密鍵D_Aを使用して復号化し、復号化されたPIN$_B$を格納する
332
暗号化PIN$_A$を抽出し、秘密鍵D_Bを使用して復号化し、復号化されたPIN$_A$を格納する
334

フロントページの続き

(51)Int.Cl. FI
H04M 3/00 C

(74)代理人 100094112
弁理士 岡部 譲
(74)代理人 100096943
弁理士 臼井 伸一
(74)代理人 100101498
弁理士 越智 隆夫
(74)代理人 100096688
弁理士 本宮 照久
(74)代理人 100104352
弁理士 朝日 伸光
(74)代理人 100128657
弁理士 三山 勝巳
(72)発明者 ゲールハルト ディートリッヒ クラッセン
カナダ エヌ2ティー 1エッチ7 オンタリオ, ウォータールー, ヘザーヒル プレイス 510
(72)発明者 サメル ファーミー
カナダ エヌ2エル 3ピー8 オンタリオ, ウォータールー, ハゼル ストリート 406, アパートメント 9
(72)発明者 デーヴィッド ヤック
カナダ エヌ2ケイ 2エヌ1 オンタリオ, ウォータールー, キャッスルフィールド アヴェニュー 254

審査官 清水 稔

(56)参考文献 特表2007－520117（JP, A）
山崎洋一, インスタント・メッセージ製品／サービス、在席確認やメッセージの即時交換が可能 ステータス機能やログ管理などに差, 日経Internet Solutions, 日経BP社, 2003年 1月22日, 第67号, p.86～93

(58)調査した分野(Int.Cl., DB名)
H04L 12／56
H04L 9／32
H04M 3／00
H04M 3／42
H04M 11／00