(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2007-221806
(P2007-221806A)
(43)公開日　平成19年8月30日(2007.8.30)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/08	(2006.01)	H04L	9/00	601F	5B285
G06F 13/00	(2006.01)	G06F	13/00	610S	5J104
G06F 21/20	(2006.01)	G06F	15/00	330A	

審査請求 有　請求項の数 1　OL　（全 36 頁）

(21)出願番号　特願2007-61073 (P2007-61073)
(22)出願日　平成19年3月9日 (2007.3.9)
(62)分割の表示　特願2003-504272 (P2003-504272)の分割
原出願日　平成14年6月12日 (2002.6.12)
(31)優先権主張番号　60/297,681
(32)優先日　平成13年6月12日 (2001.6.12)
(33)優先権主張国　米国 (US)
(31)優先権主張番号　60/365,533
(32)優先日　平成14年3月20日 (2002.3.20)
(33)優先権主張国　米国 (US)

（特許庁注：以下のものは登録商標）
1．Ｂｌｕｅｔｏｏｔｈ

(71)出願人　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　100078282
弁理士　山本　秀策
(74)代理人　100062409
弁理士　安村　高明

最終頁に続く

(54)【発明の名称】証明書の管理および送信のシステムおよび方法

(57)【要約】
【課題】メッセージングを行うクライアントには、Ｃｅｒｔ管理およびローディングを
単純化するＣｅｒｔの管理および送信メカニズムを提供すること。
【解決手段】メッセージングクライアント間で証明書を管理および転送する方法およびシステムが開示される。第１のメッセージングクライアントと第２のメッセージングクライアントとの間に通信が確立された場合、第１のメッセージングクライアントに格納された１つ以上の証明書が選択されて、第２のメッセージングクライアントに転送され得る。メッセージングクライアントは、これにより、証明書を共有する。証明書削除、証明書更新、および証明書状態チェック等の証明書の管理機能も提供され得る。
【選択図】図４

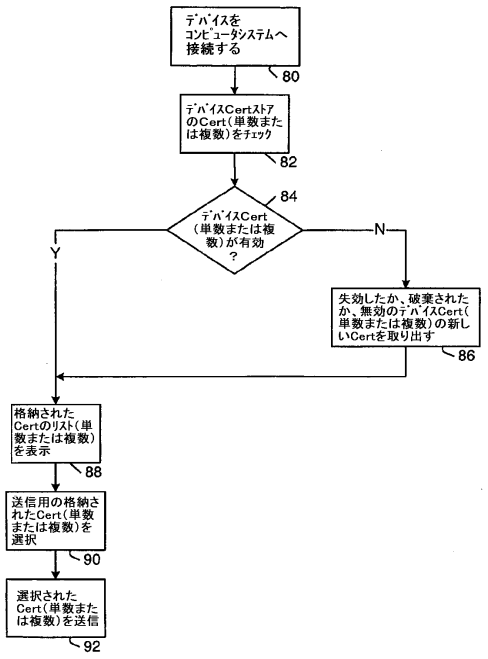

FIG. 4

【特許請求の範囲】
【請求項１】
コンピュータシステムとワイヤレス通信デバイスとの間で証明書（Ｃｅｒｔ）を管理および転送する方法であって、該コンピュータシステムは、第１のデータ転送インターフェースを有し、該ワイヤレス通信デバイスは、ワイヤレス通信ネットワークでの通信が可能であり、かつ、該第１のデータ転送インターフェースと互換性のある第２のデータ転送インターフェースを有し、
該方法は、
該第１のデータ転送インターフェースと該第２のデータ転送インターフェースとを介して、該コンピュータシステムと該ワイヤレス通信デバイスとの間に通信を確立するステップと、
該コンピュータシステムおよび該ワイヤレス通信デバイスの他方に転送するために、該コンピュータシステムおよび該ワイヤレス通信デバイスの一方に格納された１つ以上のＣｅｒｔを選択するためのユーザ入力を受信するステップと、
該選択されたＣｅｒｔを該コンピュータシステムおよび該ワイヤレス通信デバイスの一方から該コンピュータシステムおよび該ワイヤレス通信デバイスの他方に転送するステップと、
該通信を確立するステップの後に、該コンピュータシステムにおいて、該ワイヤレス通信デバイスに格納された各Ｃｅｒｔの状態をチェックすることにより、データストアにおける期限切れの、取消された、または、無効のＣｅｒｔを検出し、各検出された期限切れの、取消された、または、無効のＣｅｒｔに対して新しいＣｅｒｔを取り出し、各新しいＣｅｒｔを該コンピュータシステムから該ワイヤレス通信デバイスに転送するステップと
を包含し、
転送された新しいＣｅｒｔは、該ワイヤレス通信デバイスが該ワイヤレス通信ネットワークで可能な該通信を介して受信された、または、送信されるべきデータまたはメッセージを処理するために用いられる、方法。
【発明の詳細な説明】
【背景技術】
【０００１】
（関連出願の相互参照）
本願は、２００１年６月１２日に出願された米国仮出願第Ｓ／Ｎ　６０／２９７，６８１号、および２００２年３月２０日に出願された米国仮出願第Ｓ／Ｎ　６０／３６５，５３３号の優先権を主張する。これらの仮出願のそれぞれの図面を含む完全な開示は、本明細書中で参照として援用される。
【０００２】
（発明の背景）
（発明の分野）
本発明は、一般的にセキュアな電子メッセージングの分野に関し、特にセキュアなメッセージングを行うクライアント間の証明書管理および送信に関する。
【０００３】
（従来技術の状況の説明）
デスクトップコンピュータシステム上で動作する電子メールソフトウェアアプリケーションを含む、公知のセキュアなメッセージングを行うクライアントのほとんどは、証明書（「Ｃｅｒｔ」）のような情報のセキュアなメッセージングを行うために、データストア、または少なくとも専用データ格納領域を維持する。Ｃｅｒｔは、通常、エンティティの公開鍵、および１つ以上のデジタル署名を有する公開鍵に拘束された識別情報を含む。Ｓ／ＭＩＭＥ（Ｓｅｃｕｒｅ　Ｍｕｌｔｉｐｕｒｐｏｓｅ　Ｉｎｔｅｒｎｅｔ　Ｍａｉｌ　Ｅｘｔｅｎｓｉｏｎ）では、例えば、公開鍵を利用して、受信したセキュアなメッセージのデジタル署名を認証し、送信されるメッセージを暗号化するために利用されたセッション鍵を暗号化する。他のセキュアなメッセージングの技術では、公開鍵は、データまたは

メッセージを暗号化するために利用され得る。公開鍵が、暗号化またはデジタル署名認証のために必要とされる時に、メッセージングを行うクライアントにおいて利用可能でない場合は、Ｃｅｒｔは、これらの動作が実行され得る前にメッセージングを行うクライアントにロードされなければならない。通常、各メッセージングを行うクライアントは、Ｃｅｒｔソースとの通信を確立させて、任意の必要とされるＣｅｒｔを取得し、かつ他のメッセージングを行うクライアントとは独立してその自分の専用のＣｅｒｔおよび秘密鍵を管理する。しかし、１人のユーザが、デスクトップまたはラップトップパーソナルコンピュータ（ＰＣ）およびワイヤレスモバイル通信デバイス上で動作する１つより多いメッセージングを行うクライアントを有する場合、例えば、Ｃｅｒｔは、通常、Ｃｅｒｔソースからそれぞれのメッセージンを行うクライアントにロードされなければならない。

【発明の開示】

【発明が解決しようとする課題】

【０００４】

従って、メッセージングを行うクライアントには、Ｃｅｒｔ管理およびローディングを単純化するＣｅｒｔの管理および送信メカニズムが必要である。

【０００５】

関連して、Ｃｅｒｔの管理およびローディングのシステムおよび方法の必要がある。

【課題を解決するための手段】

【０００６】

（要旨）

第１のメッセージングを行うクライアントと第２のメッセージングを行うクライアントとの間のＣｅｒｔ管理および送信方法が提供される。この方法は、第１のメッセージング行うクライアントと第２のメッセージングを行うクライアントとの間の通信を確立させるステップと、第２のメッセージングを行うクライアントへの送信のために、第１のメッセージングを行うクライアントに格納される１つ以上のＣｅｒｔを選択するステップと、第１のメッセージングを行うクライアントから第２のメッセージングを行うクライアントへ選択されたＣｅｒｔを送信するステップを包含する。

【０００７】

さらに、第１のメッセージングを行うクライアントと第２のメッセージングを行うクライアントとの間のＣｅｒｔ管理および送信のためのシステムが提供される。このシステムは、第１のメッセージングを行うクライアントにおいて、Ｃｅｒｔを格納するように構成される第１のＣｅｒｔストアを備える第１のメモリと、第１のＣｅｒｔストアにアクセスするように構成される第１のＣｅｒｔ同期（ｓｙｎｃ）システムと、第１の通信インターフェイスを備える。第２のメッセージングを行うクライアントにおいて、このシステムは、Ｃｅｒｔを格納するように構成される第２のＣｅｒｔストアを備える第２のメモリと、第２のＣｅｒｔストアにアクセスするように構成さえる第２のＣｅｒｔ同期システムと、第１の通信インターフェイスと互換性のある第２の通信インターフェイスとを備え得る。さらに、第１のＣｅｒｔ同期システムは、第１の通信インターフェイスおよび第２の通信インターフェイスを介して通信リンクが第１のメッセージングを行うクライアントと第２のメッセージングを行うクライアントとの間で確立される時は、第１のＣｅｒｔストアに格納されたＣｅｒｔを第１のメッセージングを行うクライアントから第２のメッセージングを行うクライアントへ送信するように構成され得る。

【０００８】

また、コンピュータシステムとワイヤレスモバイル通信デバイスとの間でＣｅｒｔを送信する、さらなるシステムが提供される。このシステムは、コンピュータシステムに関連するシリアルポートと、インターフェイスを有する、シリアルポートに接続されたモバイルデバイスクレードルと、ワイヤレスモバイル通信デバイスに関連し、かつモバイルデバイスクレードルのインターフェイスと互換性のあるモバイルデバイスインターフェイスとを備える。コンピュータシステムに格納されたＣｅｒｔは、ワイヤレスモバイル通信デバイスをモバイルデバイスクレードルに配置することによって、通信リンクがコンピュータ

システムとワイヤレスモバイル通信デバイスとの間に確立される時、ワイヤレスモバイル通信デバイスに送信され得る。

【０００９】

また、ワイヤレスモバイル通信デバイスが提供され、ワイヤレストランシーバと、ワイヤレストランシーバに接続されたメッセージングシステムと、通信インターフェイスと、Ｃｅｒｔを格納するように構成されたＣｅｒｔストアと、Ｃｅｒｔストアおよび通信インターフェイスに接続されるＣｅｒｔ同期システムを備える。さらに、このメッセージングシステムは、ワイヤレストランシーバを介してＣｅｒｔストアに受信されたＣｅｒｔを格納するように構成され得る。Ｃｅｒｔ同期システムは、通信インターフェイスを介してＣｅｒｔストアに受信されたＣｅｒｔを格納するように構成される。

【発明を実施するための最良の形態】

【００１０】

（詳細な説明）

セキュアなメッセージとは、データ機密性、データ整合性、およびユーザ認証の１つ以上を保証するために、メッセージ送信側、または可能であればメッセージ送信側とメッセージ受信側との間の中間システムによって処理されたメッセージである。セキュアなメッセージングの従来技術は、デジタル署名によるメッセージの署名、および／またはメッセージの暗号化を含む。例えば、セキュアなメッセージは、Ｓ／ＭＩＭＥ（Ｓｅｃｕｒｅ Ｍｕｌｔｉｐｕｒｐｏｓｅ Ｉｎｔｅｒｎｅｔ Ｍａｉｌ Ｅｘｔｅｎｓｉｏｎｓ）の改良型に従って、メッセージ送信側により署名され、暗号化され、暗号化の後に署名され、または署名の後に暗号化されたメッセージであり得る。

【００１１】

メッセージングを行うクライアントは、自身が動作するシステムがメッセージを受信および可能であれば送信することを許可する。メッセージングを行うクライアントは、通信能力を有するコンピュータシステム、ハンドヘルドデバイス、または任意の他のシステムもしくはデバイス上で動作し得る。また、多くのメッセージングを行うクライアントは、さらなる非メッセージング機能を有する。

【００１２】

図１は、例示的なメッセージングシステムのブロック図である。このシステム１０は、コンピュータシステム１４に接続された広域エリアネットワーク（ＷＡＮ）１２、ワイヤレスネットワークゲートウェイ１６、および企業ローカルエリアネットワーク（ＬＡＮ）１８を備える。ワイヤレスネットワークゲートウェイ１６は、さらにワイヤレス通信ネットワーク２０に接続され、ワイヤレス通信ネットワーク２０では、ワイヤレスモバイル通信デバイス２２（「モバイルデバイス」）が動作するように構成される。

【００１３】

コンピュータシステム１４は、デスクトップまたはラップトップＰＣであり得、それらは、例えばインターネット等のＷＡＮ１２と通信するように構成される。コンピュータステム１４のようなＰＣは、通常、インターネットサービスプロバイダ（ＩＳＰ）、アプリケーションサービスプロバイダ（ＡＳＰ）等を介してインターネットにアクセスする。

【００１４】

企業ＬＡＮ１８は、ネットワークに基づくメッセージングを行うクライアントの例である。企業ＬＡＮ１８は、通常は、セキュリティファイアウォール２４の後ろに位置付けられる。企業ＬＡＮ３０内には、ファイアウォール２４の後ろのコンピュータ上で動作する、メッセージサーバ２６が、ＷＡＮ１２を介して、ＬＡＮ１８内と他の外部のメッセージングを行うクライアントとの両方のメッセージを交換するように、主要なインターフェイスとして動作する。２つの公知のメッセージサーバ２６は、例えば、Ｍｉｃｒｏｓｏｆｔ（Ｒ） Ｅｘｃｈａｎｇｅ ＳｅｒｖｅｒおよびＬｏｔｕｓ Ｄｏｍｉｎｏ（Ｒ）を含む。これらのサーバは、多くの場合、通常は、ＵＮＩＸ（登録商標）ベースのＳｅｎｄｍａｉｌプロトコルを利用してメールをルーティングおよび送達する、インターネットメールルータ

を連動して利用される。さらに、メッセージサーバ２６は、カレンダー、トゥドゥリスト、タスクリスト、電子メールおよびドキュメンテーションのためのダイナミックデータベース格納装置のような付加的な機能を提供し得る。

【００１５】

メッセージサーバ２６は、ＬＡＮ１８に接続されるネットワーク接続されたコンピュータシステム２８へのメッセージング能力を提供する。通常のＬＡＮ１８は、複数のコンピュータシステム２８を含み、複数のコンピュータシステム２８のそれぞれは、Ｍｉｃｒｏｓｏｆｔ　Ｏｕｔｌｏｏｋ（Ｒ）、Ｌｏｔｕｓ　Ｎｏｔｅ（Ｒ）等のようなメッセージングを行うクライアントを実装する。ＬＡＮ１８内では、メッセージは、メッセージサーバ２６によって受信され、受信されたメッセージにアドレスされるユーザアカウントに対する適切なメールボックスに分配され、その後、コンピュータシステム２８上で動作するメッセージを行うクライアントを介してユーザによってアクセスされる。

【００１６】

ワイヤレスゲートウェイ１６は、インターフェイスをワイヤレスネットワーク２０に提供し、ワイヤレスネットワーク２０を介してメッセージは、モバイルデバイス２２と交換され得る。モバイルデバイス２２は、例えばデータ通信デバイス、音声通信デバイス、データおよび音声通信機能の両方を有するごく最近のセルラー電話のようなデュアルモード通信デバイス、ワイヤレス通信を可能にするパーソナルデジタルアシスタント（ＰＤＡ）、あるいはワイヤレスモデムを有したラプトップまたはデスクトップコンピュータシステムであり得る。

【００１７】

モバイルデバイス２２のアドレシング、ワイヤレス送信のためのメッセージの暗号化またはそうでなければ変換、ならびに任意の他の要求されるインターフェイス機能のような機能が、ワイヤレスゲートウェイ１６によって実行され得る。ワイヤレスゲートウェイ１６は、１つより多いワイヤレスネットワーク２０と共に動作するように構成され得、この場合、ワイヤレスゲートウェイ１６はまた、所定のモバイルデバイスユーザを位置付けるための最も可能性の高いネットワークを決定し得、かつ複数の国またはネットワーク間を徘徊しながらどうにかしてユーザをトラッキングする。

【００１８】

ＷＡＮ１２とアクセスする任意のコンピュータシステムは、ワイヤレスネットワークゲートウェイ１６を介してモバイルデバイス２２とメッセージを交換し得る。もしくは、ワイヤレス仮想プライベートネットワーク（ＶＰＮ）のようなプライベートワイヤレスネットワークゲートウェイは、さらにワイヤレスネットワークにプライベートインターフェイスを提供するように実装され得る。例えば、ＬＡＮ１８内で実装されるワイヤレスＶＰＮは、ＬＡＮ１８から１つ以上のワイヤレスモバイル通信デバイス２２へワイヤレスネットワーク２０を介してプライベートネットワークを提供し得る。そのようなワイヤレスネットワークゲートウェイ１６および／またはワイヤレスネットワーク２０を介したワイヤレスモバイル通信デバイス２２へのプライベートインターフェイスは、さらに、メッセージ転送、またはメッセージサーバ２６と共に動作するあて先変更（ｒｅｄｉｒｅｃｔｉｏｎ）システムを提供することによって、ＬＡＮ１８の外のエンティティへ効果的に拡張され得る。そのようなメッセージあて先変更システムは、本明細書中で参照として援用する、米国特許第６，２１９，６９４号に記載される。このタイプのシステムでは、メッセージサーバ２６により受信され、モバイルデバイス２２のユーザにアドレスされる入来メッセージは、ワイヤレスネットワークインターフェイス、例えばワイヤレスＶＰＮルータ、ワイヤレスゲートウェイ１６、または他のインターフェイスのいずれかを介してワイヤレスネットワーク２０およびユーザのモバイルデバイス２２へ送信される。メッセージサーバ２６におけるユーザのメールボックスに対する別の代替のインターフェイスは、ワイヤレスアプリケーションプロトコル（ＷＡＰ）ゲートウェイであってもよい。ＷＡＰゲートウェイを介して、メッセージサーバ２６上のユーザのメールボックスにおけるメッセージのリスト、および可能であれば各メッセージまたは各メッセージの一部は、モバイルデバイ

ス２２に送信され得る。いくつかの通信システムの例が、以下にさらに詳細に説明される。

【００１９】

ワイヤレスネットワーク２０は、通常、モバイルデバイス２２から基地局とモバイルデバイス２２との間のＲＦ送信を介して、モバイルデバイス２２へ、およびモバイルデバイス２２からメッセージを送達する。ワイヤレスネットワーク２０は、例えば、（１）データ中心ワイヤレスネットワーク、（２）音声中心ワイヤレスネットワーク、または（３）同一のインフラストラクチャを介して音声およびデータ通信の両方をサポートし得るデュアルモードネットワークであり得る。近年開発されたネットワークは、（１）コード分割多重アクセス（ＣＤＭＡ）ネットワーク、（２）ＧＳＭ（Ｇｒｏｕｐｅ Ｓｐｅｃｉａｌ Ｍｏｂｉｌｅ）またはＧＳＭ（Ｇｌｏｂａｌ Ｓｙｓｔｅｍ ｆｏｒ Ｍｏｂｉｌｅ Ｃｍｍｕｎｉｃａｔｉｏｎｓ）およびＧＰＲＳ（Ｇｅｎｅｒａｌ Ｐａｃｋｅｔ Ｒａｄｉｏ Ｓｅｒｖｉｃｅ）（共に、ＣＥＰＴの規格委員会によって開発された）、および（３）ＥＤＧＥ（Ｅｎｈａｎｃｅｄ Ｄａｔａ ｒａｔｅ ｆｏｒ Ｇｌｏｂａｌ Ｅｖｏｌｕｔｉｏｎ）およびＵＭＴＳ（Ｕｎｉｖｅｒｓａｌ Ｍｏｂｉｌｅ Ｔｅｌｅｃｏｍｍｕｎｉｃａｔｉｏｎｓ Ｓｙｓｔｅｍｓ）第３世代（３Ｇ）ネットワーク（現在開発中）を含む。

【００２０】

ＧＰＲＳは、既存のＧＳＭワイヤレスネットワークのトップのデータオーバーレイであり、これは、ヨーロッパの実質的に全ての国で利用され稼動している。いくつかの旧式のデータ中心ネットワークの例は、（１）Ｍｏｂｉｔｅｘ（Ｒ） Ｒａｄｉｏ Ｎｅｔｗｏｒｋ（「Ｍｏｂｉｔｅｘ」）および（２）Ｄａｔａ ＴＡＣ（Ｒ） Ｒａｄｉｏ Ｎｅｔｗｏｒｋ（「ＤａｔａＴＡＣ」）を含むが、これらに制限されない。公知の音声中心データネットワークの例は、北アメリカおよび世界的に数年間利用されていたＣＤＭＡ、ＧＳＭ、および時分割多重アクセス（ＴＤＭＡ）システムのような、パーソナルコミュニケーションシステム（ＰＣＳ）ネットワークを含む。

【００２１】

モバイルデバイス２２は、音声、データ、および他のタイプの通信が可能な、データ通信デバイス、音声通信デバイス、または多重モードデバイスであり得る。モバイルデバイス２２の例は、以下にさらなる詳細が説明される。

【００２２】

おそらく、現在利用されている最も普通のタイプのメッセージングは、ｅメールである。標準的なｅメールシステムでは、ｅメールメッセージは、可能であればメッセージサーバおよび／またはサービスプロバイダシステムを介してｅメール発信者によって送信され、通常は、１つ以上のメッセージ受信者にインターネットを介してルーティングされる。ｅメールメッセージは、通常、安全に（ｉｎ ｔｈｅ ｃｌｅａｒ）送信され、かつ従来のＳＭＴＰ（Ｓｉｍｐｌｅ Ｍａｉｌ Ｔｒａｎｓｆｅｒ Ｐｒｏｔｏｃｏｌ）、ＲＦＣ８２２ヘッダ、およびＭＩＭＥボディ部分を利用してｅメールメッセージのフォーマットを規定する。

【００２３】

近年、ｅメールメッセージのようなメッセージのコンテンツおよびインテグリティの両方を保護する、セキュアなメッセージング技術が進歩した。Ｓ／ＭＩＭＥおよびＰｒｅｔｔｙ Ｇｏｏｄ Ｐｒｉｖａｃｙ（Ｒ）（ＰＧＰ（Ｒ））は、データコンテンツを保護する暗号化および署名の両方を提供する、２つの公開鍵セキュアｅメールメッセージングプロトコルである。この暗号化および署名の両者は、メッセージのインテグリティを保護し、かつメッセージ受信者により発信者の認証を提供する。セキュアなメッセージングは、さらにエンコードされ、圧縮され、またはそうでなければ暗号化および／または署名に加えて処理され得る。

【００２４】

図２は、メッセージングシステムにおけるセキュアなｅメールメッセージ交換を示すブ

ロック図である。このシステムは、ＷＡＮ３２およびワイヤレスゲートウェイ３４に接続されるｅメール発信者３０を含み、ワイヤレスゲートウェイ３４は、ＷＡＮ３２とワイヤレスネットワーク３６との間のインターフェイスを提供する。モバイルデバイス３８は、ワイヤレスネットワーク３６内部で動作するように適応される。さらに、図２に示されるのは、さらなる詳細が示される、モバイルデバイス３８またはモバイルデバイス３８のユーザに関連するコンピュータシステム３１である。コンピュータシステム３１は、インターフェイスまたはコネクタ３５への通信リンク３３を有し、破線３９で示されるように、インターフェイスまたはコネクタ３５を介して、モバイルデバイス３８と情報が交換され得る。

【００２５】

ｅメール発信者３０は、図１のシステム１４のようなＰＣであってもよいし、またはコンピュータシステム２８のようなネットワークに接続されたコンピュータであってもよい。ｅメール発信者３０は、ｅメールメッセージが作成され、かつ送信され得るモバイルデバイスであってもよい。ＷＡＮ３２、ワイヤレスゲートウェイ３４、ワイヤレスネットワーク３６、およびモバイルデバイス３８は、図１の同様のラベルがつけられたコンポーネントと実質的に同じである。

【００２６】

Ｓ／ＭＩＭＥおよびＰＧＰのようなセキュアなメッセージングスキーマによると、メッセージは、ｅメール発信者３０によって選択されたワンタイムセッション鍵を用いて暗号化される。セッション鍵を利用して、メッセージボディを暗号化し、かつその後セ、セッション鍵自体が、メッセージが送信されるべきアドレスされた各メッセージ受信者の公開鍵を用いて、暗合化される。４０に示されるように、この方法で暗号化されたメッセージは、暗号化メッセージボディ４４と暗号化セッション鍵４６を含む。このタイプのメッセージ暗号化スキーマでは、ｅメール発信者３０のようなメッセージ発信者は、暗号化メッセージが送信されるべき各エンティティの公開鍵へのアクセスを有しなければならない。

【００２７】

セキュアなｅメールメッセージ発信者３０は、通常、メッセージのダイジェストを取得し、かつ発信者の秘密鍵を利用してダイジェストに署名することによってメッセージに署名する。ダイジェストは、例えば、チェックサム、ＣＲＣ（Ｃｙｃｌｉｃ　Ｒｅｄｕｎｄａｎｃｙ　Ｃｈｅｃｋ）、またはメッセージに対するハッシュのような好ましいいくつかの他の非可逆演算を実行することによって生成され得る。このダイジェストは、その後、発信者の秘密鍵を利用して発信者によって署名される。秘密鍵を利用し、ダイジェストに対して暗号化、または他の変換演算を実行して、ダイジェスト署名を生成し得る。ダイジェストおよびダイジェスト署名を含むデジタル署名は、その後、出て行くメッセージに添付される。さらに、発信者のＣｅｒｔは、発信者の公開鍵および発信者識別情報を含み、発信者識別情報は、１つ以上のデジタル署名により公開鍵に拘束される。発信者のＣｅｒｔおよび任意のチェーン化されたＣｅｒｔに関連した発信者のＣｅｒｔおよび可能であれば任意のチェーン化されたＣｅｒｔおよびＣＲＬ（Ｃｅｒｔｉｆｉｃａｔｅ　Ｒｅｖｏｃａｔｉｏｎ　Ｌｉｓｔ）は、さらにセキュアなメッセージに添付され得る。

【００２８】

ｅメール発信者３０によって送信されたセキュアなｅメールメッセージ４０は、デジタル署名４２、ならびに暗号化メッセージボディ４４および暗号化セッション鍵４６を含み得、暗号化メッセージボディ４４および暗号化セッション鍵４６は、署名される。発信者のＣｅｒｔ、任意のチェーン化Ｃｅｒｔ、および１つ以上のＣＲＬはまた、メッセージ４０に含まれ得る。Ｓ／ＭＩＭＥセキュアメッセージング技術では、Ｃｅｒｔ、ＣＲＬ、およびデジタル署名は、通常、メッセージのはじめに配置され、かつメッセージボディは、ファイル添付物に含まれる。他のセキュアなメッセージングスキーマによって生成されたメッセージは、メッセージコンポーネントを示されたものと異なるオーダーの配置するか、または付加的および／または異なるコンポーネントを含み得る。例えば、セキュアなメッセージ４０は、「Ｔｏ：」および「Ｆｒｏｍ：」ｅメールアドレス、ならびに他のヘッ

ダ情報のような、アドレシング情報を含み得る。

【００２９】

セキュアなｅメールメッセージ４０がｅメール発信者３０から送信された場合、それは、ＷＡＮ３２を介してコンピュータシステム３１までルーティングされる。コンピュータシステム３１は、ほとんどの場合、ユーザＡのｅメールアドレスに関連したＰＣか、またはメッセージングサーバ上のメールボックスにアクセスするネットワークに接続されたコンピュータワークステーションのどちらかである。コンピュータシステム３１は、セキュアなメッセージ４０を電子エンベロープへと再パッケージ化し、かつ再パッケージ化されたメッセージをワイヤレスゲートウェイ３４に転送する。再パッケージ化されたメッセージは、その後、ワイヤレスネットワーク３６を介してモバイルデバイス３８に送信される。モバイルデバイス３８では、電子エンベロープは、その後再パッケージ化されたメッセージから除去されて、オリジナルのセキュアなメッセージ４０を復元する。オリジナルのセキュアなメッセージ４０は、その後、モバイルデバイス３８において処理され得る。このメッセージ再パッケージ化は、圧縮、暗号化、符号化のような演算を含み得、通常は、コンピュータシステム３１で動作するソフトウェアモジュールまたはアプリケーションによって実行される。しかし、コンピュータシステム３１が、メッセージングサーバにおける受信したｅメールにアクセスする場合、再パッケージ化演算は、メッセージングサーバまたは可能であればメッセージングサーバと連動して動作する別のシステムにおいて実行され得る。モバイルデバイス３８では、逆演算が、システムまたはソフトウェアモジュールを逆パッケージ化することよって、同様に実行される。

【００３０】

コンピュータシステム３１は、セキュアなメッセージ４０を受信し、メッセージを再パッケージ化し、さらに図２のシステム例のモバイルデバイス３８へ再パッケージ化されたメッセージを送信するように示されたが、他の実装もまた可能である。例えば、モバイルデバイス３８は、直接的にアドレス可能であってもよく、この場合、メッセージ４０は、コンピュータシステム３１ではなくワイヤレスゲートウェイ３４にルーティングされる。ワイヤレスゲートウェイ３４は、その後、任意の必要とされるアドレス変換、符号化、または同様の機能、ならびに必要であれば、ワイヤレスネットワーク３６を介してモバイルデバイス３８へメッセージを送信する。

【００３１】

さらに、メッセージは、モバイルデバイス３８へワイヤレスゲートウェイ以外の送信メカニズムを用いてルーティングまたは転送され得る。例えば、ワイヤレスネットワーク３６へのルーティングは、ｅメール発信者３０と関連するか、またはコンピュータシステム３１において受信された後モバイルデバイス３８へ転送されるメッセージの場合は、コンピュータシステム３１と関連するワイヤレスＶＰＮルータを用いて達成され得る。

【００３２】

署名入りのメッセージの各受信者（図２のコンピュータシステム３１およびモバイルデバイス３８）は、メッセージボディ４４および暗号化セッション鍵４６のダイジェストを生成し、デジタル署名４２からダイジェストを抽出し、生成されたダイジェストをデジタル署名４２から抽出されたダイジェストと比較し、かつデジタル署名４２のダイジェスト署名と検証することによって、デジタル署名４２を検証する。セキュアなメッセージ受信者によって用いられるダイジェストアルゴリズムは、メッセージ発信者によって用いられるアルゴリズムと同一であり、かつ例えばメッセージヘッダまたは可能であればデジタル署名４２において特定され得る。通常用いられる１つのダイジェストアルゴリズムは、いわゆるＳＨＡ１（Ｓｅｃｕｒｅ　Ｈａｓｈｉｎｇ　Ａｌｇｏｒｉｔｈｍ１）であるが、ＭＤ５（Ｍｅｓｓａｇｅ－Ｄｉｇｅｓｔ　Ａｌｇｏｒｉｔｈｍ５）のような他のダイジェストアルゴリズムもまた、利用され得る。

【００３３】

ダイジェスト署名４２を検証するために、メッセージ受信者は、ダイジェスト署名に対して逆変換を実行することによって発信者の公開鍵を取り出し、かつデジタル署名４２の

ダイジェストにおける署名を検証しなければならない。例えば、メッセージ発信者が、公開鍵を利用してダイジェストを暗号化することによってダイジェスト署名を生成下場合、受信者は、発信者の公開鍵を利用してダイジェスト署名を復号化してオリジナルダイジェストを復元する。セキュアなメッセージが発信者のＣｅｒｔを含む場合、発信者の公開鍵は、Ｃｅｒｔから抽出され得る。もしくは、発信者の公開鍵は、例えば公開鍵が、発信者からの以前のメッセージから抽出され、かつ受信者のローカルストアの鍵ストアに格納されていた場合、ローカルストアから取り出され得る。あるいは、公開鍵は、ローカルストアに格納されている場合は発信者のＣｅｒｔから、または公開鍵サーバ（ＰＫＳ）から取り出され得る。ＰＫＳは、通常ＣＡ（Ｃｅｒｔｉｆｉｃａｔｅ Ａｕｔｈｏｒｉｔｙ）と関連したサーバであり得、ＣＡから、エンティティの公開鍵を含むエンティティのＣｅｒｔが入手され得る。ＰＫＳは、１８（図１）のような企業ＬＡＮ内、あるいはＷＡＮ３２、インターネット、またはメッセージ受信者がＰＫＳとの通信を確立し得る他のネットワークもしくはシステム内に常駐していてもよい。発信者Ｃｅｒｔは、以下に詳細が示されるように、モバイルデバイス３８上で関連するコンピュータシステム３１からローディングされ得る。

【００３４】

ダイジェストアルゴリズムは、好ましくは、一意のインプット毎に一意の出力を生成する非可逆関数であり得る。従って、オリジナルメッセージが変更されるか、または改悪された場合、受信者により生成されたダイジェストは、デジタル署名から抽出されたダイジェストとは異なり、従って、署名の検証は失敗する。しかし、ダイジェストアルゴリズムは公に知られているので、あるエンティティがセキュアなメッセージを変更し、変更されたメッセージの新しいダイジェストを生成し、かつ任意のアドレスされたメッセージ受信者に対して変更されたメッセージを転送することが可能である。この場合、変更されたメッセージを基に受信者において生成されたダイジェストは、メッセージを変更したエンティティによって付け加えられた新しいダイジェストと整合する。ダイジェスト署名のチェックは、そのような状況におけるデジタル署名の検証を妨げることが意図される。たとえ生成された新しいダイジェストが整合したにせよ、発信者が専用の秘密鍵を用いてオリジナルダイジェストに署名しているので、メッセージを変更したエンティティは、発信者の秘密鍵によって検証され得る新しいダイジェスト署名を生成できない。従って、変更されたメッセージのダイジェストが整合しようとも、ダイジェスト署名は、ダイジェスト署名検証が失敗するために検証されない。

【００３５】

これらの数学的演算は、誰かがセキュアなメッセージのコンテンツを見ることを防止しないが、発信者によって署名されているため、メッセージが改竄されていないことと、メッセージがメッセージの「Ｆｒｏｍ」フィールドに示される人物によって署名されたこととを保証する。

【００３６】

デジタル署名４２が検証された際に、またはデジタル署名検証が失敗した場合でさえも、暗号化されたメッセージボディ４４は、その後、図２におけるメッセージングを行うクライアント、コンピュータシステム３１、およびモバイルデバイス３８を受信することによって、表示され、またはさらに処理される前に、暗号化されなくてはならない。メッセージ受信者は、秘密鍵を利用して、暗号化セッション鍵４６を復号化し、その後、復号化セッション鍵を利用して、暗号化メッセージボディ４４を復号化し、それによりオリジナルメッセージを復元する。

【００３７】

１つ以上の受信者にアドレスされる暗号化メッセージは、受信者の公開鍵を用いて暗号化された各受信者のセッション鍵の暗号化バージョンを含む。各受信者は、同一のデジタル署名検証動作を実行するが、専用の秘密鍵を用いて暗号化セッション鍵と異なる鍵を復号化する。

【００３８】

従って、セキュアなメッセージングシステムでは、メッセージングを行うクライアントの送信は、暗号化メッセージが送信されるべき任意の受信者の公開鍵へのアクセスを有しなければならない。メッセージングを行うクライアントの受信は、署名されたメッセージのデジタル署名を検証するために、様々なメカニズムを介してメッセージングを行うクライアントに入手可能であり得る、発信者の公開鍵を取り出すことができなければならない。モバイルデバイス３８はセキュアなメッセージ４０の受信者であるが、モバイルデバイス３８は、２方向通信が可能であってもよく、従って、メッセージ送信およびメッセージ受信動作の両方のための公開鍵を必要とし得る。

【００３９】

公開鍵は、通常、Ｃｅｒｔにて提供される。上述のように、任意の特定のエンティティに対するＣｅｒｔは、通常、エンティティの公開鍵および識別情報を含み、識別情報は、デジタル署名により公開鍵に拘束される。いくつかのタイプのＣｅｒｔは、現在、例えば、Ｘ．５０９Ｃｅｒｔを含む広範な用途がある。Ｘ．５０９Ｃｅｒｔは、通常、Ｓ／ＭＩＭＥにおいて利用される。ＰＧＰは、Ｃｅｒｔを異なるフォーマットで利用する。本発明のある局面によるシステムおよび方法は、任意のこれらのタイプのＣｅｒｔ、および他のタイプのＣｅｒｔ、ならびに現在知られているタイプおよび開発され得る他のタイプの両者と共に利用される。Ｃｅｒｔのデジタル署名は、Ｃｅｒｔの発行者によって生成され、かつ上述のように実質的にメッセージ受信者によってチェックされ得る。Ｃｅｒｔは、時には、満了時間または有効期間を含み得、そこから、メッセージングを行うクライアントは、Ｃｅｒｔが失効したかどかを判定し得る。Ｃｅｒｔの妥当性の検証は、さらにＣｅｒｔチェーンを介した証明書の経路のトレースを含む。Ｃｅｒｔチェーンは、ユーザのＣｅｒｔおよび、可能であればユーザのＣｅｒｔが認証されていることを検証する他のＣｅｒｔを含む。Ｃｅｒｔはまた、Ｃｅｒｔが取り消されていないことを保証するために、ＣＲＬに対してチェックされ得る。

【００４０】

特定のエンティティのＣｅｒｔにおけるデジタル署名が有効であれば、Ｃｅｒｔは、満了も、失効もしておらず、かつＣｅｒｔまたはチェーン化されたＣｅｒｔのどちらかの発行者は信用され、Ｃｅｒｔの公開鍵は、Ｃｅｒｔが発行された対象のエンティティの公開鍵であると仮定され、さらにＣｅｒｔの対象者として参照される。

【００４１】

Ｃｅｒｔは、いくつかのソースからのメッセージングを行うクライアントに対して利用可能である。Ｃｅｒｔが受信しメッセージに添付されている場合、Ｃｅｒｔは、メッセージから抽出され、かつメッセージングを行うクライアントによって格納される。そうでなければ、Ｃｅｒｔは、リクエストされ、かつＬＡＮ、インターネット、またはリクエストした者が通信を確立し得る他のネットワーク上のＰＫＳからダウンロードされ得る。もしくは、本発明のある局面によると、メッセージングを行うクライアントは、ＰＫＳ以外のソースからＣｅｒｔをロードし得る。多くの現在のモバイルデバイスは、ＰＣと接続するように構成されている。そのようなデバイスをＰＣと接続して、シリアルポートまたはＵＳＢポートのような物理的接続を介してＣｅｒｔをダウンロードすることによって、Ｃｅｒｔの空中を介した（ｏｖｅｒ－ｔｈｅ－ａｉｒ）送信が低減され得る。そのような物理的接続を利用して、ユーザが暗号化メッセージを送信することを期待するエンティティのＣｅｒｔをロードする場合、これらのＣｅｒｔは、暗号化メッセージが任意のこれらのエンティティに送信されるべき際にダウンロードされる必要がない。ユーザは、同様に、署名入りのメッセージが受信されることが期待される任意のエンティティのＣｅｒｔをロードすることにより、これらのエンティティの１つが署名されたメッセージにそのＣｅｒｔを添付していない場合でさえも、デジタル署名は、検証され得る。

【００４２】

公知のシステムでは、任意のＣｅｒｔは、Ｃｅｒｔソースからリクエストされて、各メッセージングを行うクライアントに格納されなくてはならない。Ｃｅｒｔは、通常、メッセージングを行うクライアントが同一のユーザと関連しているときでさえ、メッセージン

グを行うクライアント間で共用されていない。図２のシステムでは、例えば、ユーザＡは、コンピュータシステム３１およびモバイルデバイス３８の両方において、別のエンティティ、ユーザＢのＣｅｒｔを必要とする。そして、ユーザＢのＣｅｒｔは、２度（コンピュータシステム３１に対して１回、モバイルデバイスに対して１回）リクエストされ、かつロードされなくてはならない。しかし、Ｃｅｒｔの管理および送信システムを利用すると、ユーザＢのＣｅｒｔは、コンピュータシステム３１およびモバイルデバイス３８の１つのみにおいて、リクエストされ、かつロードされる必要がある。

【００４３】

図３は、モバイルデバイス、およびＣｅｒｔの管理および送信システムを実装する、関連するコンピュータシステムのブロック図である。図３では、Ｃｅｒｔの管理および送信動作に直接含まれるコンポーネントのみが、示される。当業者に対して明らかにされるべきは、モバイルデバイスおよびコンピュータシステムは、通常、さらなるコンポーネントを含む。コンピュータシステム３１およびモバイルデバイス３８は、第１のメッセージングを行うクライアントおよび第２のメッセージングを行うクライアントとの概略的な例であり、第１のメッセージングを行うクライアントと第２のメッセージングを行うクライアントとの間で、Ｃｅｒｔは、送信され得る。また、第１および第２のメッセージングを行うクライアントは、可能であれば２つのモバイルデバイスまたは２つのコンピュータシステムであり得る。

【００４４】

図３に示されるように、Ｃｅｒｔの管理および送信システムを組み込む、モバイルデバイス３８は、メモリ５２、メッセージングシステム６０、Ｃｅｒｔ同期（ｓｙｎｃ）システム６２、ユーザインターフェイス（ＵＩ）６４、ワイヤレストランシーバ６６、およびコネクタ６８のインターフェイスを備える。メモリ５２は、好ましくは、Ｃｅｒｔストア、および可能であればアドレスブック５６のような他のデータストアのための５４の格納領域と、アプリケーションデータ格納領域５８とを含む。アドレスブック５６には、メッセージンングコンタクト情報が格納される。アプリケーションデータ格納領域５８は、モバイルデバイス３８上のソフトウェアアプリケーションと関連するデータを格納する。データストア５６および５８は、メモリ５２およびモバイルデバイス３８において実装され得るストアの概略的な例である。メモリ５２はまた、図３に示されるシステムに加えて、他のデバイスシステムによって利用されて、他のタイプのデータを格納し得る。

【００４５】

メモリ５２は、他のデバイスコンポーネントがデータを書き込み得るＲＡＭのような書き込み可能ストアである。Ｃｅｒｔストア５４は、モバイルデバイス３８のＣｅｒｔ格納専用の格納領域である。Ｃｅｒｔは、Ｃｅｒｔストア５４に、それらが受信されるフォーマットで格納されるか、あるいは、ストア５４に書き込まれる前に、解析されるか、そうでなければ格納フォーマットに変換され得る。

【００４６】

メッセージングシステム６０は、ワイヤレストランシーバ６６に接続され、それにより、ワイヤレスネットワークを介して通信が可能になる。Ｃｅｒｔ同期システム６２は、インターフェイス／コネクタ６８に接続されて、インターフェイス／コネクタ３５とコネクション３９および３３との共同を通じて、コンピュータシステム３１との通信を可能にする。

【００４７】

ＵＩ６４は、キーボードまたはキーパッド、ディスプレイ、あるいはモバイルデバイス３８からの入力をアクセプトし得、またはモバイルデバイス３８のユーザに出力を提供し得る、他のコンポーネントのようなＵＩコンポーネントを含み得る。図３に単一のブロックとして示されるように、モバイルデバイス３８は、通常、１つより多いＵＩを含み、したがってＵＩ６４は１つ以上のユーザインターフェイスを示すことが意図されることが、理解されるべきである。

【００４８】

コンピュータシステム３１は、Ｃｅｒｔがインターフェイスまたはコネクタ３５を介してモバイルデバイス３８に送信され得る物理的接続３３を含む。図３に外部のコンポーネントとして示されるが、あるいは、インターフェイス／コネクタ３５は、コンピュータシステム３１に対して内部に存在し得る。モバイルデバイス３８のように、コンピュータシステム３１は、Ｃｅｒｔ同期システム７０を含み、Ｃｅｒｔ同期システム７０は、多くの実装において、ソフトウェアアプリケーションであり得る。Ｃｅｒｔ同期システム７０は、ＵＩ７１とインターフェイスし、ＵＩ７１は、１つ以上の入力および出力コンポーネント、ならびに接続３３およびＣｅｒｔストア７２を含み得る。Ｃｅｒｔストア７２は、可能であれば、例えばローカルハードディスクドライブまたは他のメモリユニットを含む、任意のコンピュータ格納媒体であり得る。Ｃｅｒｔは、パブリックな情報であるが、例えばネットワーク内部のコンピュータシステム間で共用され得、その結果、ストア７２は、外部にあるが、例えばネットワークファイルサーバ上のコンピュータシステム３１にアクセス可能である。メッセージングシステム７０は、Ｃｅｒｔストア７２および通信サブシステム７６の両方に接続される。

【００４９】

Ｃｅｒｔの管理および送信システムを実装するメッセージングを行うクライアントは、さらに好ましくは、従来の態様のＣｅｒｔを取り出し得る。これは、メッセージングシステム６０、７４、Ｃｅｒｔストア５４、７２、通信システム、すなわちワイヤレストランシーバ６６または通信サブシステム７６のどちらかの間の接続によって、図３に表現される。したがって、モバイルデバイス３８上のメッセージングシステム６０は、受信されたメッセージの発信者の公開鍵または送信されるべきメッセージのアドレスを必要とする場合、Ｃｅｒｔは、例えばワイヤレストランシーバ６６を介してＰＫＳから、リクエストされ、かつ受信され得る。Ｃｅｒｔが受信されたメッセージに添付されている場合は、メッセージングシステム６０は、メッセージからＣｅｒｔを抽出し、かつＣｅｒｔをＣｅｒｔストア５４に格納し得る。コンピュータシステム３１は、同様の演算を実行して、任意の必要とされるＣｅｒｔを取得し得る。

【００５０】

図３に示されるＣｅｒｔの格納および送信システムのユーザもまた、好ましくは、Ｃｅｒｔを選択し、かつインターフェイスまたはコネクタ６８と３５との間に確立される通信リンクを介して、コンピュータシステム３１からモバイルデバイス３８へ、またはモバイルデバイス３８からコンピュータシステム３１へ送信し得る。インターフェイスまたはコネクタ６８および３５は、任意の複数の互換性のあるデータ送信コンポーネントであり得る。このコンポーネントは、例えば、Ｉｎｆｒａｒｅｄ Ｄａｔａ Ａｓｓｏｃｉａｔｉｏｎ（ＩｒＤＡ）ポートのような光学データ送信インターフェイス、他の短い範囲のワイヤレス通信インターフェイス、あるいはシリアルまたはユニバーサルシリアルバス（ＵＳＢ）のような有線インターフェイスおよび接続を含み得る。公知の短い範囲のワイヤレス通信インターフェイスは、例えば、それぞれＢｌｕｅｔｏｏｔｈまたは８０２．１１規格に従った「Ｂｌｕｅｔｏｏｔｈ」モジュールおよび８０２．１１モジュールを含む。Ｂｌｕｅｔｏｏｔｈおよび８０２．１１は、ワイヤレスＬＡＮおよびワイヤレスパーソナルエリアネットワークにそれぞれ関連する、ＩＥＥＥ（Ｉｎｓｔｉｔｕｔｅ ｏｆ Ｅｌｅｃｔｒｉｃａｌ ａｎｄ Ｅｌｅｃｔｒｏｎｉｃｓ Ｅｎｇｉｎｅｅｒｓ）から利用可能な規格のセットを意味することが、当業者には理解されるべきである。

【００５１】

コンピュータシステム３１とモバイルデバイス３８との間の通信は、必ずしも物理的接続を介しする必要はないので、関連するコンピュータにモバイルデバイスを接続することへの参照は、物理的接続またはワイヤレス送信スキーマのどちらかによって、コンピュータシステムとモバイルデバイスとの間の通信を確立することを含む。したがって、モバイルデバイス３８は、コンピュータシステム３１におけるシリアルポートに接続されたモバイルデバイスクレードルにモバイルデバイス３８を配置することによってか、モバイルデバイス３８をその光学ポートがコンピュータシステム３１の同様のポートの視野方向（ｌ

ｉｎｅ　ｏｆ　ｓｉｇｈｔ）にあるように位置付けることによってか、あるいはデータが交換され得るようにいくつかのほかの方法でモバイルデバイス３８およびコンピュータシステム３１を物理的に接続するか、または配置することによって、コンピュータシステム３１に接続され得る。モバイルデバイスとコンピュータシステムとの間の通信を確立する際に含まれうる特定の動作は、インターフェイスおよび／またはコネクタのタイプに依存する。

【００５２】

図３に再び戻って、モバイルデバイス３８がコンピュータシステム３１に接続される場合、Ｃｅｒｔ同期システム７０は、好ましくは自動的に開始される。好ましくはコンピュータシステム３１、モバイルデバイス３８、または両方において確立されたユーザにより指定された設定に従って、モバイルデバイス３８がコンピュータシステム３１に接続される場合、他の動作もまた自動的に実行され得る。

【００５３】

Ｃｅｒｔ同期システム７０は、Ｃｅｒｔストア７２にアクセスして、どのＣｅｒｔが内部に格納されているかを判定し得る。Ｃｅｒｔ同期システム７０は、その後、好ましくは、コンピュータシステム３１におけるＵＩ７１、好ましくはディスプレイスクリーン上に格納されたＣｅｒｔのリストを生成する。Ｃｅｒｔは、例えばＣｅｒｔストア７２に格納された順序、利用頻度順、Ｃｅｒｔが発行されたエンティティの名前のアルファベット順（すなわち、対象者名）、あるいは任意のほかのディフォルトまたはユーザに設定された順序で、リストにされ得る。このリストでは、Ｃｅｒｔは、好ましくは、対象者名によって識別され、あるいはＣｅｒｔの対象者のコンタクト情報がコンピュータシステム３１のアドレスブックまたは同様のコンタクト情報ストアに格納されている場合、Ｃｅｒｔは、例えばなじみのある名前のようなコンタクト情報の一部分を利用して識別され得る。

【００５４】

ユーザは、マウス、キーボード、またはコンピュータシステム３１に関連するＵＩ７１として実装され得る他の入力デバイスを用いて、コンピュータシステム３１上に格納されたどのＣｅｒｔが、モバイルデバイス３８に送信されるべきかを選択し得る。選択されたＣｅｒｔは、コネクションおよびインターフェイス３３、３５、３９、６８を介してモバイルデバイス３８に送信される。Ｃｅｒｔ送信動作は、例えば、選択されたＣｅｒｔを、モバイルデバイス３８のＣｅｒｔストア５４に加える付加動作であってもよい。あるいは、Ｃｅｒｔ送信動作は、例えば、モバイルデバイス３８のＣｅｒｔストア５４の失効したＣｅｒｔを、選択されたＣｅｒｔに置換するか、またはより低頻度で利用されるＣｅｒｔを、より利用頻度が高いか、または高くなると予測されるＣｅｒｔと置換する、更新動作であってもよい。あるいは、Ｃｅｒｔ送信動作は、モバイルデバイス３８のＣｅｒｔストア５４の全てのＣｅｒｔが消去され、かつ選択されたＣｅｒｔが、Ｃｅｒｔストア５４に対して格納される、全ての置換動作であってもよい。他のタイプのＣｅｒｔ送信も可能であり、Ｃｅｒｔ同期システム７０、Ｃｅｒｔ同期システム６２、またはその両方を用いて選択可能、または設定可能であってもよい。

【００５５】

モバイルデバイス３８において、Ｃｅｒｔは、Ｃｅｒｔ同期システム６２によって受信され、ユーザによって選択された送信動作のタイプに応じて処理されて、Ｃｅｒｔストア５４に対して送信されたＣｅｒｔを格納する。送信されたＣｅｒｔは、Ｃｅｒｔストア５４に既に格納されているＣｅｒｔに加えて（付加動作）またはその代わりに（更新動作）、あるいはＣｅｒｔストア５４のＣｅｒｔが消去されたの後（全ての置換動作）に、ストアに付加されてもよい。Ｃｅｒｔがこの方法でモバイルデバイス３８に送信された場合、メッセージ発信者または中間システム（これを介して、メッセージがモバイルデバイス３８まで送信される）は、モバイルデバイス３８にセキュアなメッセージについてＣｅｒｔを送信する必要がない。中間システムはまた、Ｃｅｒｔが既にモバイルデバイス３８に送信されていた場合は、モバイルデバイス３８に送信される前に、受信したセキュアなメッセージから、存在するならば、Ｃｅｒｔ、および可能であれば他の比較的多量の情報を、

剥ぎ取り得る。

【００５６】

モバイルデバイス３８におけるメモリ５２は、制限される傾向があるので、Ｃｅｒｔストア５４のようなデータストアは、Ｃｅｒｔの特定の数のみを格納するために十分なスペースを有し得る。Ｃｅｒｔストア５４が満杯の場合、新しいＣｅｒｔは、Ｃｅｒｔストア５４の１つ以上の既存のＣｅｒｔが上書きされるか、または消去されない限り、コンピュータシステム３１からＣｅｒｔストア５４に送信されない。Ｃｅｒｔストア５４のオーバーフローは、モバイルデバイスＣｅｒｔ同期システム６２、コンピュータＣｅｒｔ同期システム７０のどちらか、または両方によって操作され得る。例えば、モバイルデバイス３８のＣｅｒｔ同期システム６２は、Ｃｅｒｔストア５４の最近最も使われていない（ＬＲＵ）置換ポリシーを実装するように構成され得る。ここで、最近最も使われていないＣｅｒｔは、Ｃｅｒｔストア５４が満杯である時に、新しいＣｅｒｔがモバイルデバイス３８にローディングされる場合、自動的に上書きされる。もしくは、モバイルデバイス３８およびコンピュータシステム３１が接続されている一方で、Ｃｅｒｔストア５４が満杯であるか、または満杯になる場合に、Ｃｅｒｔ同期システム６２は、Ｃｅｒｔ同期システム７０を警告するように構成され得る。さらに、またはもしくは、警告は、ユーザがＣｅｒｔを満杯のＣｅｒｔストア５４に加えようと試みる時に、Ｃｅｒｔ同期システム７０まで戻る。この場合、ユーザは、ＵＩ７１を介して、Ｃｅｒｔストア５４のＣｅｒｔが加えられるべきＣｅｒｔと置換されるべきかどうかを選択するように促され得、もし置換すべきであれば、可能であれば置換されるべきＣｅｒｔを選択するように促され得る。そのようなスキーマは、Ｃｅｒｔストア５４が満杯である場合に、ユーザに付加動作を中断させることができる。

【００５７】

コンピュータシステム３１におけるＣｅｒｔ同期システム７０は、さらにＣｅｒｔストア７２の各Ｃｅｒｔをチェックして、有効なＣｅｒｔのみがモバイルデバイス３８へ送信されることを保証し得る。これは、１つ以上のＣＲＬ、満了時期または有効期限のチェックを含み、かつ、可能であれば、各Ｃｅｒｔに対する外部システム（示されない）へのステータス問い合わせを提示する。失効したか、もはや有効ではない任意のＣｅｒｔは、Ｃｅｒｔストア７２から消去され得、好ましくは、Ｃｅｒｔ同期システム７０によって生成されたＣｅｒｔリストに含まれない。Ｃｅｒｔストア７２の失効もしくは無効のＣｅｒｔの消去はまた、対象者の名前または失効もしくは無効のＣｅｒｔの同様のフィールドで識別されるエンティティに対する新しいＣｅｒｔのリクエストをトリガーするか、あるいは、新しいＣｅｒｔをリクエストするか、または新しいＣｅｒｔをリクエストすることなく失効もしくは無効のＣｅｒｔを単に消去するなどのさらなるアクションを選択するようにユーザプロンプトをトリガーし得るかのどちらかである。

【００５８】

メッセージングシステム７４またはコンピュータシステム３１のコンポーネントが、全ての格納されたＣｅｒｔのステータスを定期的にチェックする場合、Ｃｅｒｔ同期システム７０によるステータスチェックは、必ずしもモバイルデバイスがコンピュータシステム３１に接続されるたびでなくともよい。どちらの場合でも、ユーザは、コンピュータシステム３１からモバイルデバイス３８に送信されたＣｅｒｔが送信された時点では有効であったことを保証され得る。しかし、本質的に、ＣＲＬのサイズ、Ｃｅｒｔステータスチェックに関連するロードの処理、およびＣｅｒｔステータス情報が外部ソースからリクエストされなければならない場合のネットワークのレイテンシのために、モバイルデバイス３８に対するＣｅｒｔステータスチェックは、問題を含みがちであり、したがって、通常実行されない。送信時に有効であろうとも、送信後に失効したか、破棄されたか、または無効化されたＣｅｒｔストア５４のＣｅｒｔは、常にモバイルデバイス３８上で検知されなくてもよい。

【００５９】

Ｃｅｒｔの管理システムおよび方法は、モバイルデバイス３８のＣｅｒｔストア５４に

おける失効されたか、破棄されたか、または無効のＣｅｒｔのこの問題を軽減し得る。Ｃｅｒｔ同期システム６２および７０は、モバイルデバイス３８とコンピュータシステム３１との間でＣｅｒｔ情報を交換し得る。Ｃｅｒｔ同期システム６２は、上述されたＣｅｒｔ同期システム７０と同様、好ましくは、モバイルデバイス３８がコンピュータシステム３１に接続されている時に、Ｃｅｒｔストア５４にアクセスするように構成され、少なくともＣｅｒｔストア５４に格納されたＣｅｒｔのリストを生成する。Ｃｅｒｔのステータスをチェックするように Ｃｅｒｔ同期システム７０によってリクエストされた情報によって、Ｃｅｒｔのリストだけではなく、Ｃｅｒｔストア５４のＣｅｒｔのコピーが、Ｃｅｒｔ同期システム７０まで送られ得る。リストまたは完全なＣｅｒｔは、自動的か、またはＣｅｒｔ同期システム７０からＣｅｒｔ同期システム６２までのリクエストに応答してかのどちらかで、Ｃｅｒｔ同期システム７０に送られ得る。リストまたはＣｅｒｔ、および任意のＣＲＬ、満了時期または有効期限の情報、ならびにリクエストされた場合は外部ソースからの任意の情報を用いて、Ｃｅｒｔ同期システム７０は、各Ｃｅｒｔのステータスをチェックする。

【００６０】

モバイルデバイス３８のＣｅｒｔが失効しているか、破棄されたか、または無効化された場合、Ｃｅｒｔ同期システム７０は、好ましくは、専用のＣｅｒｔストア７２か、もしくは外部のＣｅｒｔソースのどちらかから、失効したＣｅｒｔを置換する新しいＣｅｒｔを取り出す。もしくは、ユーザは、（ＵＩ７１または６４を介して）ＣｅｒｔがＣｅｒｔストア５４から消去されるべきかどうか、または新しいＣｅｒｔが取り出されるべきかを選択するように促され得る。Ｃｅｒｔ同期システム６２は、消去されるか、あるいは、失効したか、破棄されたか、または無効化されたＣｅｒｔを、コンピュータシステム３１からの新しいＣｅｒｔで置換するかのどちらかである。

【００６１】

モバイルデバイス３８またはコンピュータシステム３１は、好ましくは、モバイルデバイス上にＣｅｒｔの少なくとも最新のＣｅｒｔチェックのレコードを維持することにより、モバイルデバイス３８に格納されたＣｅｒｔに対するＣｅｒｔチェックの頻度が、制御され得る。モバイルデバイス３８がコンピュータシステム３１に接続されている場合、このＣｅｒｔチェックレコードは、Ｃｅｒｔストア５４に格納されたＣｅｒｔがチェックされるべきかどうかを判定するためにアクセスされる。

【００６２】

Ｃｅｒｔ同期システム６２および７０の調整された動作がまた、さらなるＣｅｒｔ管理機能を提供する。Ｃｅｒｔ同期システム７０が専用のＣｅｒｔストア７２と、Ｃｅｒｔ同期システム６２を介して、モバイルデバイスＣｅｒｔストア５４との両方へのアクセスを有するので、コンピュータシステム３１およびモバイルデバイス３８に格納されたＣｅｒｔの別々のリストが生成され、ユーザに表示され得る。ユーザは、その後、どのＣｅｒｔがすでにモバイルデバイス３８上にローディングされたかを容易に判定し得る。もしくは、モバイルデバイスＣｅｒｔストア５４に格納されたＣｅｒｔは、Ｃｅｒｔストア７２に格納されたＣｅｒｔのリストから除去され得、その結果、モバイルデバイスＣｅｒｔストア５４に格納されていないＣｅｒｔストア７２で利用可能なこれらのＣｅｒｔのみが、選択およびモバイルデバイス３８への送信のために表示される。

【００６３】

モバイルデバイスＣｅｒｔストア５４に格納されたＣｅｒｔのリストが、コンピュータシステム３１のユーザに表示される場合、ユーザは、よりよくモバイルデバイスストア５４のＣｅｒｔを管理することができる。例えば、ユーザは、デバイスリストから消去のためのＣｅｒｔを選択し得、さらに、モバイルデバイス３８に格納されたＣｅｒｔの数、および可能であれば、Ｃｅｒｔストア５４に保存されるスペースの大きさを判定し得る。

【００６４】

Ｃｅｒｔはまた、モバイルデバイス３８からコンピュータシステム３１へ送信され得る。上述されたように、コンピュータシステム３１およびモバイルデバイス３８の両方が、

様々なソースからＣｅｒｔを取り出し得る。例えば、コンピュータシステム３１およびモバイルデバイス３８が別々にアドレス可能である場合、それらは、異なる発信者からセキュアなメッセージを受信し得、それにより異なるＣｅｒｔがメッセージを処理する必要がある。異なるＣｅｒｔはまた、セキュアなメッセージを異なる受領者に送信することが要求され得る。要求されたＣｅｒｔが、コンピュータシステム３１からＣｅｒｔストア５４に送信されなかった場合は、モバイルデバイス３８は、例えばワイヤレスネットワークを介して別のソースからＣｅｒｔを取り出し得る。この場合、モバイルデバイスＣｅｒｔストア５４は、コンピュータシステム３１のＣｅｒｔストア７２において利用可能でなくともよいＣｅｒｔを含む。そのようなＣｅｒｔは、上述されたように実質的にモバイルデバイス３８からコンピュータシステム３１へ送信され得る。

【００６５】

同様に、モバイルデバイスＵＩ６４がディスプレイスクリーンおよびキーボード、親指ホイールなどの１つ以上の入力デバイスを含む場合、Ｃｅｒｔ管理および送信動作は、Ｃｅｒｔ同期システム６２によって制御され得る。

【００６６】

Ｃｅｒｔ管理動作が完全な場合は、モバイルデバイス３８およびコンピュータシステム３１の両方が、好ましくは通常の動作モードに戻る。Ｃｅｒｔ同期システム６２および７０が、ソフトウェアアプリケーションとして実現される場合、そのアプリケーションは、選択されたＣｅｒｔが送信された後に自動的に、閉じられるか、または代わりに終了し得る。Ｃｅｒｔ同期システム６２、７０はまた、モバイルデバイス３８がコンピュータシステム３１に接続された場合に自動的にではなく、同期システムの１つまたは各々がユーザによって呼び出された場合にのみ、開始するように構成され得る。

【００６７】

図４は、メッセージングを行うクライアント間のＣｅｒｔ管理および送信の方法を示すフローチャートである。図４では、モバイルデバイスおよびコンピュータシステムは、Ｃｅｒｔの管理および送信方法を実装する第１のメッセージングクライアントおよび第２のメッセージングクライアントの例として示されるが、図３に関連して上述されたように、Ｃｅｒｔはまた、モバイルデバイス間または複数のコンピュータシステム間で交換され得る。

【００６８】

この方法は、モバイルデバイスがコンピュータシステムに接続された時に、ステップ８０で開始する。ステップ８０は、例えば、シリアルまたはＵＳＢ接続のような物理的リンク、あるいは光学的、Ｂｌｕｅｔｏｏｔｈ、８０２．１１、または短い範囲の通信リンクのようなワイヤレスリンクを介して、モバイルデバイスとコンピュータシステムとの間の通信を確立させるステップを包含する。ステップ８２では、コンピュータシステムは、上述のように、モバイルデバイスのＣｅｒｔストアに格納された任意のＣｅｒｔのステータスをチェックし得、可能であれば、モバイルデバイスＣｅｒｔストアにおける各失効したか、破棄されたか、または無効のＣｅｒｔに対する新しいＣｅｒｔを取り出す。ステップ８６は、自動的であってもよいし、あるいはモバイルデバイスに格納されたＣｅｒｔの１つ以上が、失効しているか、破棄されたか、または無効であるとわかった時に生成されるプロンプトまたは警告へのユーザの応答に依存していてもよい。

【００６９】

新しいＣｅｒｔが任意のこのようなＣｅｒｔに対して取り出されたか、または取り出されない時に、モバイルデバイスにおけるＣｅｒｔのいずれも失効されておらず、破棄されておらず、かつ無効化されていない場合、あるいは、ステータスチェックが、モバイルデバイス上に格納されたＣｅｒｔに対して実行されない場合、ステップ８８において、コンピュータシステムのＣｅｒｔストアに格納されたＣｅｒｔのリストが生成され、ユーザに対して表示される。上述のように、各メッセージングクライアントに格納されたＣｅｒｔのリストが、ユーザに対して表示され得る。ユーザは、その後、ステップ９０においてどちらかのリストから１つ以上の格納されたＣｅｒｔを選択し得、かつ選択されたＣｅｒｔ

は、ステップ９２において、あるメッセージングクライアントから他のメッセージングクライアントへ送信される。ステップ９０および９２は、各選択されたＣｅｒｔに対して繰り返され得る。もしくは、ユーザは、ステップ９０において複数のＣｅｒｔを選択し得、ユーザの一部にさらなるアクションを要求することなく、ステップ９２において各Ｃｅｒｔを送信し得る。ステップ９２のＣｅｒｔ送信は、コンピュータシステムからモバイルデバイスへか、またはモバイルデバイスからコンピュータシステムへかのどちらかであり得る。Ｃｅｒｔの選択および送信ステップ９０および９２は、所望のＣｅｒｔ送信動作を実行するために必要な程度に頻繁に繰り返され得る。Ｃｅｒｔストアのオーバーフロー操作は、例えばＬＲＵ置換ポリシーによって、あるいは、格納されたＣｅｒｔを置換するか、またはＣｅｒｔ送信動作を停止するユーザのさらなる選択に応答して、設定可能であり得る。

【００７０】

コンピュータシステムは、通常、モバイルデバイスと比較してより高速かつ強力な処理リソースを有し、かつＰＫＳまたは他のＣｅｒｔソースへのずっと高速の通信リンクにアクセスするので、リモートソースからコンピュータシステムへのＣｅｒｔローディングは、比較的高速であり、かつ単純なプロセスである。したがって、ステップ９２におけるほとんどのＣｅｒｔ送信は、コンピュータシステムからモバイルデへの送信である可能性が高い。しかし、Ｃｅｒｔがコンピュータシステム間で管理および／または共用されるべきときは、コンピュータシステム間のＣｅｒｔ送信もまた可能である。例えば企業ＬＡＮ内のコンピュータシステム間のＣｅｒｔの共有は、任意のＣｅｒｔに対する外部ＰＫＳまたは他のＣｅｒｔソースとの通信を最小化する。任意のＣｅｒｔは、ＬＡＮ内のコンピュータシステムによって外部のソースから取り出されたものである。

【００７１】

ステップ９２のＣｅｒｔ送信は、上述のように、選択されたＣｅｒｔをメッセージングクライアントのＣｅｒｔストアに加え得るか、あるいはメッセージングクライアント上のＣｅｒｔストアの任意または全てのＣｅｒｔを置換し得る。図４には明確に示されないが、Ｃｅｒｔ送信以外のＣｅｒｔ管理動作もまた、格納されたＣｅｒｔのリストがステップ８８において生成され、かつ表示された後に、実行され得る。例えば、Ｃｅｒｔはまた、消去、あるいは別のメッセージングクライアントへの送信以外の動作のために選択され得る。

【００７２】

図５は、本発明が実装され得るメッセージクライアントの例としての、ワイヤレスモバイル通信デバイスのブロック図である。モバイル通信デバイス５００は、好適には、少なくともボイスおよび／またはデータ通信能力を有する２方向通信デバイスである。モバイルデバイスは、好適には、インターネット上の他のコンピュータシステムと通信する能力を有する。モバイルデバイスによって提供される機能性に依存して、モバイルデバイスは、データメッセージングデバイス、２方向ページャ、メッセージング能力を有するセルラー電話、ワイヤレスインターネットアプライアンス、またはデータ通信デバイス（テレフォニ能力を有するか、または有しない）と呼ばれ得る。上述のように、このようなデバイスは、本明細書中にて、概して、単に、モバイルデバイスと呼ばれる。

【００７３】

モバイルデバイス５００は、トランシーバ５１１、マイクロプロセッサ５３８、ディスプレイ５２２、フラッシュメモリ５２４、ＲＡＭ５２６、補助入力／出力（Ｉ／Ｏ）デバイス５２８、シリアルポート５３０、キーボード５３２、スピーカ５３４、マイクロホン５３６、短距離ワイヤレス通信サブシステム５４０を含み、さらに、他のデバイスサブシステム５４２を含み得る。トランシーバ５１１は、好適には、送信アンテナ５１６および受信アンテナ５１８、受信器（Ｒｘ）５１２、送信器（Ｔｘ）５１４、１つ以上のローカルオシレータ（ＬＯ）５１３、およびデジタル信号プロセッサ（ＤＳＰ）５２０を含む。フラッシュメモリ５２４の中で、モバイルデバイス５００は、好適には、マイクロプロセッサ５３８（および／またはＤＳＰ５２０）によって実行され得る複数のソフトウェアモ

ジュール５２４Ａ～５２４Ｎを含み、これらは、複数の他の機能を実行するためのボイス通信モジュール５２４Ａ、データ通信モジュール５２４Ｂおよび複数の他の動作モジュール５２４Ｎを含む。

【００７４】

モバイル通信デバイス５００は、好適には、ボイスおよびデータ通信能力を有する２方向通信デバイスである。従って、例えば、モバイルデバイス５００は、アナログまたはデジタルセルラーネットワークのいずれか等のボイスネットワークを介して通信し得、さらに、データネットワークを介して通信し得る。ボイスおよびデータネットワークは、通信タワー５１９で図５に示される。これらのボイスおよびデータネットワークは、基地局、ネットワークコントローラ等の別個のインフラストラクチャを用いる別個の通信ネットワークであり得るか、または、これらは、単一のワイヤレスネットワークに統合され得る。従って、ネットワーク５１９に関しては、単一のボイス、およびデータネットワークまたは別個のネットワークの両方を含むと解釈されるべきである。

【００７５】

通信サブシステム５１１は、ネットワーク５１９と通信するために用いられる。ＤＳＰ５２０は、送信器５１４への、および受信器５１２からの通信信号を送受信するために用いられ、さらに、送信器５１４および受信器５１２とコントロール情報を交換し得る。ボイスおよびデータ通信が、単一周波数、または密接に間隔が詰まったセットの周波数で生じる場合、単一のＬＯ５１３は、送信器５１４および受信器５１２と共に用いられ得る。あるいは、ボイス通信対データ通信に対して異なった周波数が利用される場合、ネットワーク５１９に対応する複数の周波数を生成するために複数のＬＯ５１３が用いられ得る。２つのアンテナ５１６、５１８が図５にて示されるが、モバイルデバイス５００は、単一のアンテナ構造で用いられ得る。ボイスおよびデータ情報の両方を含む情報は、ＤＳＰ５２０とマイクロプロセッサ５３８との間のリンクを介して、通信モジュール５１１に、および通信モジュール５１１から伝達される。

【００７６】

周波数帯域、コンポーネントの選択肢、電力レベル等の通信サブシステム５１１の詳細な設計は、展開することが意図されるデバイス通信ネットワーク５１９に依存する。例えば、北米市場において展開するように意図されたモバイルデバイス５００は、ＭｏｂｉｔｅｘまたはＤａｔａＴＡＣモバイルデータ通信ネットワークで動作するように設計され、および、ＡＭＰＳ、ＴＤＭＡ、ＣＤＭＡ、ＰＣＳ等の種々のボイス通信ネットワークのいずれかで動作するように設計された通信サブシステム５１１を含み得、これに対して、欧州で用いることが意図されたデバイス５００は、ＧＰＲＳデータ通信ネットワークおよびＧＳＭボイス通信ネットワークで動作するように構成され得る。他のタイプのデータおよびボイスネットワークは、別個のもの、および統合されたものの両方があり、モバイルデバイス５００によっても利用され得る。

【００７７】

ネットワーク５１９のタイプに依存して、モバイルデバイス５００へのアクセス要件も変化し得る。例えば、ＭｏｂｉｔｅｘおよびＤａｔａＴＡＣデータネットワークにおいて、モバイルデバイスは、各デバイスと関連付けられた一意的識別番号を用いてネットワーク上に登録される。しかしながら、ＧＰＲＳにおいては、ネットワークアクセスは、モバイルデバイス５００の加入者またはユーザと関連付けられ得る。ＧＰＲＳデバイスは、通常、加入者アイデンティティモジュール（「ＳＩＭ」）を必要とし、これは、ＧＰＲＳネットワーク上でモバイルデバイス５００を動作させるために必要とされる。ローカル、または非ネットワーク通信機能（存在する場合）が、ＳＩＭを用いなくても動作可能であり得るが、モバイルデバイス５００は、「９１１」緊急呼出し等の、任意の法定動作以外は、ネットワークを介しての通信を含む任意の機能を実行することができない。

【００７８】

任意の必要とされるネットワークレジストレーションまたは起動手順が完了した後、モバイルデバイス５００は、好適には、ネットワーク５１９を介してボイスおよびデータ信

号の両方を含む通信信号を送受信し得る。アンテナ５１６によって受信された通信ネットワーク５１９からの信号は、受信器５１２にルーティングされ、これは、信号増幅、周波数ダウンコンバージョン、フィルタリング、チャネル選択等を提供し、さらに、アナログデジタル変換を提供し得る。受信信号のアナログデジタル変換は、デジタル復調およびデコードがＤＳＰ５２０を用いて実行されることを可能にする。同様に、ネットワーク５１９に送信されるべき信号は、例えば、ＤＳＰ５２０による変調およびエンコードを含む処理がなされ、その後、デジタルアナログ変換、周波数アップコンバージョン、フィルタリング、増幅、およびアンテナ５１８を介して通信ネットワーク５１９への送信のための送信器５１４に提供される。単一のトランシーバ５１１が、ボイスおよびデータ通信の両方に関して図５に示されるが、モバイルデバイス５００は、２つの異なるトランシーバ、ボイス信号を送受信するための第１のトランシーバ、およびデータ信号を送受信するための第２のトランシーバを含み得ることが可能である。

【００７９】

通信信号を処理することに加えて、ＤＳＰ５２０は、さらに、受信器および送信器のコントロールを提供し得る。例えば、受信器５１２および送信器５１４における通信信号に付与されるゲインレベルは、ＤＳＰ５２０において実現される自動ゲインコントロールアルゴリズムを通じて、調整可能に制御され得る。他のトランシーバコントロールアルゴリズムは、より洗練されたトランシーバ５１１のコントロールを提供するために、ＤＳＰ５２０において実現され得る。

【００８０】

マイクロプロセッサ５３８は、好適には、モバイルデバイス５００の動作全体を管理および制御する。複数のタイプのマイクロプロセッサまたはマイクロコントローラがここで用いられ得るか、あるいは、マイクロプロセッサ５３８の機能を実行するために、単一のＤＳＰ５２０が用いられ得る。少なくともデータおよびボイス通信を含む低レベルの通信機能がトランシーバ５１１においてＤＳＰ５２０を通じて実行される。他の、ボイス通信アプリケーション５２４Ａおよびデータ通信アプリケーション５２４Ｂといった高レベル通信アプリケーションは、マイクロプロセッサ５３８によって実行するためのフラッシュメモリ５２４において格納され得る。例えば、ボイス通信モジュール５２４Ａは、モバイルデバイス５００と複数の他のボイスデバイスとの間でネットワーク５１９を介してボイスコールを送受信するように動作し得る高レベルユーザインターフェースを提供し得る。同様に、データ通信モジュール５２４Ｂは、ネットワーク５１９を介して、ｅメールメッセージ、ファイル、オーガナイザ情報、ショートテキストメッセージ等のデータを送受信するように動作し得る高レベルユーザインターフェースをモバイルデバイス５００と複数の他のデータデバイスとの間に提供し得る。モバイルデバイス５００上で、セキュアなメッセージングソフトウェアアプリケーションは、例えば図３におけるメッセージングシステム６０およびＣｅｒｔ同期システム６２と対応するソフトウェアモジュールを組み込み、上述の技術を実現するために、データ通信モジュール５２４Ｂと共に動作し得る。

【００８１】

マイクロプロセッサ５３８もまた、ディスプレイ５２２、フラッシュメモリ５２４、ランダムアクセスメモリ（ＲＡＭ）５２６、補助入力／出力（Ｉ／Ｏ）サブシステム５２８、シリアルポート５３０、キーボード５３２、スピーカ５３４、マイクロホン５３６、短距離通信サブシステム５４０、および、通常、５４２として設計される任意の他のデバイスサブシステム等の他のデバイスサブシステムと双方向通信する。例えば、モジュール５２４Ａ～Ｎは、マイクロプロセッサ５３８によって実行され、モバイルデバイスのユーザトモバイルデバイスとの間に高レベルインターフェースを提供し得る。このインターフェースは、通常、ディスプレイ５２２を通じて提供されるグラフィカルコンポーネント、および、補助Ｉ／Ｏ５２８、キーボード５３２、スピーカ５３４、またはマイクロホン５３６を通じて提供される入力／出力コンポーネントを含む。そのようなインターフェイスは、図３のＵＩ６４のように一般的に設計される。

【００８２】

図５に示されるサブシステムのいくつかは、通信関連機能を実行し、これに対して、他のサブシステムは、「常駐」またはオンデバイス機能を提供し得る。明らかに、キーボード５３２およびディスプレイ５２２等のいくつかのサブシステムは、データ通信ネットワークを介して送信するためのテキストメッセージを入力する通信関連機能、および計算器またはタスクリストまたは他のＰＤＡタイプの機能といったデバイス常駐機能の両方のために用いられ得る。

【００８３】

マイクロプロセッサ５３８によって用いられるオペレーティングシステムソフトウェアは、好適には、フラッシュメモリ５２４等の永久ストアに格納される。オペレーティングシステムおよび通信モジュール５２４Ａ～Ｎに加えて、フラッシュメモリ５２４はまた、さらに、データを格納するためのファイルシステムを含み得る。格納領域は、図３のデータストア５４、５６、および５８に示されるように、好ましくは、フラッシュメモリ５２４に提供され、Ｃｅｒｔ、アドレスブック全体、および可能であれば他のメッセージングに必要とされる情報を格納する。オペレーティングシステム、特定のデバイスアプリケーションまたはモジュール、あるいは、それらの部分が、より高速に動作するためのＲＡＭ５２６等の揮発性ストアに一時的にロードされ得る。さらに、受信された通信信号も、永久ストア５２４に配置されたファイルシステムにこれらを永久書き込みする前に、一時的にＲＡＭ５２６に格納され得る。

【００８４】

モバイルデバイス５００上にロードされ得る例示的アプリケーションモジュール５２４Ｎは、カレンダイベント、アポイントメント、およびタスクアイテム等のＰＤＡ機能性を提供するパーソナルインフォーメーションマネージャ（ＰＩＭ）である。このモジュール５２４Ｎは、さらに、通話、ボイスメール等を管理するためのボイス通信モジュール５２４Ａと双方向通信し得、ｅメール通信および他のデータ送信を管理するためのデータ通信モジュール５２４Ｂとも双方向通信し得る。あるいは、ボイス通信モジュール５２４Ａおよびデータ通信モジュール５２４Ｂの機能性のすべては、ＰＩＭモジュールに統合され得る。

【００８５】

フラッシュメモリ５２４は、好適には、デバイス上へのＰＩＭデータアイテムの格納を容易にするためにファイルシステムを提供する。ＰＩＭアプリケーションは、好適には、単独で、またはボイスおよびデータ通信モジュール５２４Ａ、５２４Ｂと共に、ワイヤレスネットワーク５１９を介してデータアイテムを送受信する能力を含む。ＰＩＭデータアイテムは、好適には、ホストコンピュータシステムによって格納されたか、または、これと関連したデータアイテムの対応するセットを用いて、ワイヤレスネットワーク５１９を介してシームレスに統合され、同期化、かつ、更新され、これにより、特定のユーザと関連付けられたデータアイテムのためのミラーリングされたシステムを生成する。

【００８６】

モバイルデバイス５００は、さらに、モバイルデバイス５００のシリアルポート５３０をホストシステムのシリアルポートに結合するインターフェースクレードルにモバイルデバイス５００を配置することによってホストシステムと手動で同期化され得る。シリアルポート５３０は、さらに、上述のように、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を通じて選好を設定すること、インストールのために他のアプリケーションモジュール１７２４Ｎをダウンロードすること、および、デバイス上のＣｅｒｔを管理することを可能にするために用いられ得る。この有線ダウンロード経路は、さらに、デバイス上の暗号化鍵をロードするために利用され得、これは、ワイヤレスネットワーク５１９を介して暗号化情報を交換するよりもセキュアな方法である。

【００８７】

さらなるアプリケーションモジュール５２４Ｎが、ネットワーク５１９を介して、補助Ｉ／Ｏサブシステム５２８を介して、シリアルポート５３０を介して、短い範囲の通信サブシステム５４０を介して、または任意の他の適切なサブシステム５４２を介して、モバ

イルデバイス５００上にロードされ得、かつフラッシュメモリ５２４またはＲＡＭ５２６においてユーザによってインストールされ得る。アプリケーションインストールのこのような柔軟性は、モバイルデバイス５００の機能性を増大させ、かつ、例えば拡張されたオンデバイス（ｏｎ－ｄｅｖｉｃｅ）機能、通信関連機能、またはその両方を提供し得る。例えば、セキュアな通信アプリケーションはまた、電子コマース機能、およびモバイルデバイス５００を用いて実行されるべき他のこのような金融取引を可能にし得る。

【００８８】

モバイルデバイス５００が、データ通信モードで動作している場合、テキストメッセージ、またはウェブページダウンロードのような受信信号が、トランシーバ５１１によって処理され、かつマイクロプロセッサ５３８によって提供される。マクロプロセッサ５３８は、好ましくは、ディスプレイ５２２、あるいは補助Ｉ／Ｏデバイス５２８への出力のために、さらに受信信号を処理する。例えば、ＰＫＳへのリクエストに応答して、トランシーバ５１１によって受信されたか、またはセキュアなメッセージに添付されたＣｅｒｔは、上述のように処理されて、Ｃｅｒｔが既に格納されていない場合はＣｅｒｔをフラッシュメモリ５２４のＣｅｒｔストアへ加え、かつ必要であればフラッシュメモリ５２４の新しいアドレスブックエントリのコンタクト情報を抽出および格納する。モバイルデバイスのユーザはまた、キーボード５３２を用いて、ｅメールメッセージのようなデータアイテムを作成し得る。キーボード５３２は、好ましくは、ＱＷＥＲＴＹスタイルで設計された完全な英数字キーボードであるが、他のタイプの公知のＤＶＯＲＡＫスタイルのような完全英数字キーボードもまた、利用され得る。モバイルデバイス５００へのユーザ入力は、さらに複数の補助Ｉ／Ｏデバイス５２８によって強化され、補助Ｉ／Ｏデバイス５２８は、親指ホイール入力デバイス、タッチパッド、様々なスイッチ、ロッカー入力スイッチ等を含み得る。ユーザによって作成されたデータアイテム入力は、トランシーバ５１１を介して通信ネットワーク５１９を通って送信され得る。

【００８９】

モバイルデバイス５００が、音声通信モードで動作している場合、モバイルデバイス５００の全体の動作は、受信信号が好ましくはスピーカ５３４へ出力され、かつ送信用の音声信号がマイクロフォン５３６によって生成される以外は、実質的にデータモードと同様である。さらに、上述のセキュアなメッセージング技術は、必ずしも音声通信に適用されなくてもよい。音声メッセージ記録サブシステムのような、代わりの音声またはオーディオＩ／Ｏサブシステムがまた、モバイルデバイス５００において実装され得る。音声またはオーディオ信号出力は、好ましくは、スピーカ５３４を介して最初に実現されるが、さらにディスプレイ５２２を利用して、発呼者のアイデンティティ、音声コールの継続時間、または他の音声コール関連情報のインディケーションを提供し得る。例えば、マイクロプロセッサ５３８は、音声通信モジュール５２４Ａおよびオペレーティングシステムソフトウェアと連動して、入来音声コールの発呼者識別情報を検知し、かつそれをディスプレイ５２２に表示し得る。

【００９０】

短い範囲の通信サブシステム５４０はまた、モバイルデバイス５００に含まれ得る。例えば、サブシステム５４０は、インフラレッドデバイスおよび関連した回路およびコンポーネント、あるいはＢｌｕｅｔｏｏｔｈもしくは８０２．１１短い範囲のワイヤレス通信モジュールを含み、同様のことが可能であるシステムおよびデバイスとの通信を提供し得る。したがって、上述のＣｅｒｔの管理および送信動作は、シリアルポート５３０または他の短い範囲の通信サブシステム５４０を介して、モバイルデバイス５００において有効にされ得る。１より多いこのようなインターフェイスは、モバイルデバイスＣｅｒｔの管理および／または送信動作が実行され得るメッセージングクライアントのタイプに依存して、利用され得る。モバイルデバイスからコンピュータシステムへの動作に対して、シリアルポート５３０がまた利用され得る一方で、モバイルデバイスからモバイルデバイスへの動作に対して、別の短い範囲の通信サブシステム５４０が利用され得る。

【００９１】

図２に示される通信システムを意図して、セキュアなメッセージ送信の例が上述されたが、Ｃｅｒｔの管理および送信は、他のタイプの通信システムにおいて有用であり得る。

【００９２】

図６は、通信システムの例を示すブロック図である。図６では、コンピュータシステム６０２、ＷＡＮ６０４、セキュリティファイアウォール６０８の背後の企業ＬＡＮ６０６、ワイヤレスインフラストラクチャ６１０、ワイヤレスネットワーク６１２および６１４、ならびにモバイルデバイス６１６および６１８が示される。企業ＬＡＮ６０６は、メッセージサーバ６２０、ワイヤレスコネクタシステム６２８、少なくとも複数のメールボックス６１９を含むデータストア６１７、物理的接続６２４を介してインターフェイスまたはコネクタ６２６へのようなモバイルデバイスへの直接の通信リンクを有するデスクトップコンピュータシステム６２２、ならびにワイヤレスＶＰＮルータ６３２を含む。図６のシステムの動作は、メッセージ３３、３４、および３６を参照して、以下に説明される。

【００９３】

コンピュータシステム６０２は、図１のコンピュータシステム１４のように、例えば、ＷＡＮ６０４と接続するように構成されたラップトップ、デスクトップ、またはパルムトップコンピュータシステムであり得る。このようなコンピュータシステムは、ＩＳＰまたはＡＳＰを介してＷＡＮ６０４に接続し得る。あるいは、通信システム６０２は、ＬＡＮまたは他のネットワークを通じてＷＡＮ６０４にアクセスするネットワーク接続されたコンピュータシステムであり得る。複数の最近のモバイルデバイスは、種々のインフラストラクチャおよびゲートウェイ構成を通じてＷＡＮへの接続のために使用可能にされ、従って、コンピュータシステム６０２もまたモバイルデバイスであり得る。

【００９４】

企業ＬＡＮ６０６は、ワイヤレス通信システムのために使用可能にされた中央、サーバベースのメッセージングシステムの図式的例である。企業ＬＡＮ６０６は、「ホストシステム」と呼ばれ得、ここで、企業ＬＡＮは、メッセージ用のメールボックス６１９を有するデータストア６１７、および、場合によっては、さらに、モバイルデバイス６１６および６１８に送信されるか、または、これらから受信され得る他のデータアイテム用のデータストア（図示せず）の両方、ならびに、ワイヤレスコネクタシステム６２８、ワイヤレスＶＰＮルータ６３２、または、場合によっては、企業ＬＡＮ６０６と、一つ以上のモバイルデバイス６１６および６１８との間の通信を可能にする他のコンポーネントをホストし得る。より一般的な意味では、ホストシステムは、一つ以上のコンピュータであり得、ここで、これと共に、またはこれと関連してワイヤレスコネクタシステムが動作する。企業ＬＡＮ６０６は、ホストシステムの１つの好適な実施形態であり、この実施形態にて、ホストシステムは、少なくとも１つのセキュリティ通信ファイアウォール６０８の背後で、およびこれによって保護されて動作する企業ネットワーク環境サーバコンピュータ内で走行するサーバコンピュータである。他の可能な中央ホストシステムは、ＩＡＰ、ＡＳＰおよび他のサーバプロバイダまたはメールシステムを含む。デスクトップコンピュータシステム６０４およびインターフェース／コネクタ６２６は、このようなホストシステムの外側に配置され得るが、ワイヤレス通信動作は、後述されるものと類似であり得る。

【００９５】

企業ＬＡＮ６０６は、ワイヤレスコネクタシステム６２８を、通常、ソフトウェアプログラム、ソフトウェアアプリケーション、または、少なくとも１つ以上のメッセージサーバで動作するように確立されたソフトウェアコンポーネントであるコンポーネントを使用可能にする関連したワイヤレス通信として実現する。ワイヤレスコネクタシステム６２８は、ユーザ選択情報を、１つ以上のワイヤレスネットワーク６１２および６１４を介して、１つ以上のモバイルデバイス６１６および６１８に送信するため、および、１つ以上のモバイルデバイス６１６および６１８から情報を受信するために用いられる。ワイヤレスコネクタシステム６２８は、図６に示されるようなメッセージング師ステムの別個のコンポーネントであり得るか、または、その代わりに、部分的、または全体が他の通信システムコンポーネントに組み込まれ得る。例えば、メッセージサーバ６２０は、ソフトウェア

プログラム、アプリケーション、または、ワイヤレスコネクタシステム６２８を実現するコンポーネント、その部分、または、その機能性のいくつか、または、すべてを搭載し得る。

【００９６】

ファイアウォール６０８の後のコンピュータ上で走行するメッセージサーバ６２０は、例えば、ｅメール、カレンダリングデータ、ボイスメール、電子ドキュメント、および、他のパーソナルインフォーメーションマネージメント（ＰＩＭ）データを含むメッセージを、通常、インターネットであるＷＡＮ６０４と交換するための企業用のメインインターフェースとして機能する。メッセージサーバは、多くの場合、インターネットメールルータと連動して利用され、メッセージをルーティングおよび送達する。特定の中間動作およびコンピュータは、特定のタイプのメッセージ送達メカニズム、およびメッセージが交換されるネットワークに依存し、従って、図６に示されていない。メッセージサーバ６２０の機能性は、上述のように、メッセージ送信および受信の他に、カレンダ、トゥドゥリスト、タスクリスト、ｅメールおよびドキュメンテーションのようなデータのためのダイナミックデータベースストレージといった機能を提供する。

【００９７】

６２０等のメッセージサーバは、通常、サーバ上にアカウントを有するユーザごとに６１７等の１つ以上のデータストアにおいて、複数のメールボックス６１９を維持する。データストア６１７は、複数の（「ｎ」個の）ユーザアカウントのメールボックス６１９を含む。ユーザ、ユーザアカウント、メールボックス、または、場合によっては、メッセージ受信側としてのユーザ、アカウントまたはメールボックス６１９と関連した別のアドレスを識別するメッセージサーバ６２０によって受信されるメッセージは、通常、対応するメールボックス６１９に格納される。メッセージが複数の受信側または配信リストにアドレス指定される場合、同じメッセージのコピーが１つ以上のメールボックス６１９に格納され得る。あるいは、メッセージサーバ６２０は、このようなメッセージの単一のコピーを、メッセージサーバ上にアカウントを有するユーザのすべてにアクセス可能なデータストアに格納し、かつ、ポインタまたは他の識別子を各受信側のメールボックス６１９に格納し得る。通常のメッセージングシステムにおいて、各ユーザは、メールボックス６１９、および、そのコンテンツを、通常、ＬＡＮ６０６に接続されたデスクトップコンピュータシステム６２２等のＰＣ上で動作するＭｉｃｒｏｓｏｆｔ　Ｏｕｔｌｏｏｋまたは Ｌｏｔｕｓ　Ｎｏｔｅｓ等のメッセージングクライアントを用いてアクセスし得る。ただ１つのデスクトップコンピュータシステム６２２が図６に示されるが、当業者は、ＬＡＮが、通常、複数のデスクトップ、ノートブック、およびラップトップコンピュータシステムを含むことを理解する。各メッセージングクライアントは、通常、メールサーバ６２０を通じてメールボックス６１９にアクセスするが、いくつかのシステムにおいて、メッセージングクライアントは、デスクトップコンピュータシステム６２２によって、その上に格納されたデータストア６１７およびメールボックス６１９にダイレクトアクセスすることを可能にし得る。メッセージは、さらに、データストア６１７から、デスクトップコンピュータシステム６２２上のローカルデータストア（図示せず）にダウンロードされ得る。

【００９８】

企業ＬＡＮ６０６内で、ワイヤレスコネクタシステム６２８は、メッセージサーバ６２０と共に動作する。ワイヤレスコネクタシステム６２８は、メッセージサーバ６２０と同じコンピュータシステム上に常駐し得か、または、異なったコンピュータシステム上で実現され得る。ワイヤレスコネクタシステム６２８を実現するソフトウェアは、さらに、部分的または全体がメッセージサーバ６２０と統合され得る。ワイヤレスコネクタシステム６２８およびメッセージサーバ６２０は、好適には、情報をモバイルデバイス６１６、６１８にプッシュすることを可能にするように連係および双方向通信するように設計される。このようなインスタレーションにおいて、ワイヤレスコネクタシステム６２８は、好適には、企業ＬＡＮ６０６と関連した１つ以上のデータストアに格納される情報を、企業ファイアウォール６０８を通じて、ならびに、ＷＡＮ６０４、およびワイヤレスネットワー

ク６１２、６１４の１つを介して、１つ以上のモバイルデバイス６１６、６１８に送信されるように構成される。例えば、データストア６１７にアカウントおよび関連したメールボックス６１９を有するユーザは、さらに、６１６のようなモバイルデバイスを有し得る。上述のように、ユーザ、アカウントまたはメールボックス６１９を識別するメッセージサーバ６２０によって受信されたメッセージは、メッセージサーバ６２０によって対応するメールボックス６１９に格納される。ユーザが６１６等のモバイルデバイスを有する場合、メッセージサーバ６２０により受信され、かつ、ユーザのメールボックス６１９に格納されるメッセージは、好適には、ワイヤレスコネクタシステム６２８によって検出され、かつ、ユーザのモバイルデバイス６１６に送信される。このタイプの機能性は、「プッシュ」メッセージ送信技術を表す。ワイヤレスコネクタシステム６２８は、その代わりに、「プッシュ」技術を採用し得、この技術で、メールボックス６１９に格納されたアイテムは、モバイルデバイス、または、両方の技術の特定の組み合わせを用いて行われるリクエストまたはアクセス動作に応答するモバイルデバイス６１６、６１８に送信される。

【００９９】

これにより、ワイヤレスコネクタ６２８の使用は、メッセージサーバ６２０を含むメッセージングシステムが拡張されることを可能にし、これにより、各ユーザのモバイルデバイス６１６、６１８は、メッセージサーバ６２０の格納されたメッセージにアクセスする。本明細書中で説明されるシステムおよび方法は、プッシュベースの技術にのみ制限されないが、プッシュベースメッセージングのより詳細な説明は、上述の米国特許第６，２１９，６９４号において、および以下の同時継続中でありかつ一般的に所有される米国特許出願において理解され、それらの特許の全てが、’６９４号特許に関連している。米国特許出願シリアルナンバー第０９／４０１，８６８号、第０９／５４５，９６３号、第０９／５２８，４９５号、第０９／５４５，９６２号、および第０９／６４９，７５５号。図面および請求項を含む’６９４号特許の完全な開示およびこれらの出願のそれぞれは、本明細書中で参照として援用される。このプッシュ技術は、ワイヤレスフレンドリー符号化、圧縮、および暗号化技術を用いて、全ての情報をモバイルデバイスに送達し、それにより企業ファイアウォール８を効果的に拡張して、モバイルデバイス６１６、６１８を含む。

【０１００】

図６に示されるように、企業ＬＡＮ６０６からモバイルデバイス６１６、６１８と情報を交換するためには、いくつかの経路が存在する。１つの可能な情報送信経路は、インターフェイスまたはコネクタ６２６を用いて、シリアルポートのような物理的接続６２４を介するものである。この経路は、例えば、上述のようなＣｅｒｔおよびＣＲＬのような多量の情報に対して、あるいは、多くの場合モバイルデバイス６１６、６１８のインストール時に実行されるか、またはモバイルデバイス６１６、６１８のユーザがコンピュータシステム６２２のようなＬＡＮ６０６内のコンピュータシステムにおいて動作している時に周期的に実行される更新に対して有用であり得る。また、物理的接続６２４を利用して、デスクトップコンピュータシステム６２２と関連する秘密暗号化鍵または署名鍵のような秘密鍵を含む、他の情報をデスクトップコンピュータシステム６２２から、モバイルデバイス６１６、６１８へ送信し得る。

【０１０１】

物理的接続６２４およびコネクタまたはインターフェイス６２６を用いる秘密鍵交換は、ユーザのデスクトップコンピュータシステム６２２およびモバイルデバイス６１６または６１８に、全ての暗号化されたおよび／または署名されたメールにアクセスするための少なくとも１つのアイデンティティを共有させることができる。それによりユーザのデスクトップコンピュータシステム６２２およびモバイルデバイス６１６または６１８をさらに利用して、秘密鍵を管理および送信し得、その結果、ホストシステム６２２あるいはモバイルデバイス６１６または６１８のどちらかは、メッセージサーバ６２０のユーザのメールボックスまたはアカウントにアドレスされたセキュアなメッセージを処理し得る。

【０１０２】

公知の「同期化」タイプのワイヤレスメッセージングシステムにおいて、メッセージをメッセージサーバ６２０と関連したメールボックス６１９からモバイルデバイス６１６および６１８に転送するために物理的経路が用いられる。

【０１０３】

データをモバイルデバイス６１６、６１８と交換するための別の方法は、空中を介して、ワイヤレスコネクタシステム６２８を通じて、かつ、ワイヤレスネットワーク６１２、６１４を用いる。図６に示されるように、あるいは、これは、ネットワーク６０６において利用可能であれば、ワイヤレスＶＰＮルータ６３２を含み得、または、１つ以上のワイヤレスネットワーク６１２、６１４にインターフェイスを提供するワイヤレスインフラストラクチャ６１０への従来のＷＡＮ接続を含み得る。ワイヤレスＶＰＮルータ６３２は、特定のワイヤレスネットワーク６１２を直接介するワイヤレスデバイス６１６へのＶＰＮ接続の生成を提供する。そのようなワイヤレスＶＰＮルータ６３２は、スタティックアドレシングスキーマと関連して利用され得る。例えば、ワイヤレスネットワーク６１２がインターネットプロトコル（ＩＰ）ベースワイヤレスネットワークである場合、新しいＩＰバージョン６（ＩＰＶ６）は、ネットワーク６１２内で動作するように構成された全てのモバイルデバイス６１６に対してＩＰアドレスを専有化させるのに十分なＩＰアドレスを提供して、それにより任意の時間に情報をモバイルデバイス６１６にプッシュすることを可能にするべきである。ワイヤレスＶＰＮルータ６３２の主な有利な点は、ワイヤレスインフラストラクチャ６１０を必要としない既成のＶＰＮコンポーネントであり得ることである。ＶＰＮ接続は、メッセージをモバイルデバイス６１６に、および、ここから直接送達するために、ＩＰを介するＴＣＰ／ＩＰ（Ｔｒａｎｓｍｉｓｓｉｏｎ Ｃｏｎｔｒｏｌ Ｐｒｏｔｏｃｏｌ）またはＩＰ（ＵＤＰ／ＩＰ）接続を介するＵｓｅｒ Ｄａｔａｇｒａｍ Ｐｒｏｔｏｃｏｌを用い得る。

【０１０４】

ワイヤレスＶＰＮルータ６３２が利用可能でない場合、ＷＡＮ６０４（通常、インターネット）へのリンクは、ワイヤレスコネクタシステム６２８によって用いられ得る一般的に用いられる接続メカニズムである。モバイルデバイス６１６および任意の他の必要とされるインターフェース機能のアドレシングを処理するために、ワイヤレスインフラストラクチャ６１０が、好適には、用いられる。ワイヤレスインフラストラクチャ６１０のある例は、図１のゲートウェイ１６である。ワイヤレスインフラストラクチャ６１０はまた、所与のユーザの位置を特定する最も可能性の高いワイヤレスネットワークを判定し得、複数の国またはネットワークの間をうろうろする際のユーザをトラッキングする。６１２および６１４のようなワイヤレスネットワークにおいて、メッセージは、通常、基地局（示されない）とモバイルデバイス６１６、６１８との間のＲＦ送信を介して、モバイルデバイス６１６、６１８へ、およびそこから送達される。

【０１０５】

ワイヤレスネットワーク６１２および６１４への複数の接続が提供され得る。これらの接続は、例えば、インターネット中で利用されるＴＣＰ／ＩＰプロトコルを用いる、統合サービスデジタルネットワーク（ＩＳＤＮ）、Ｆｒａｍｅ Ｒｅｌａｙ、またはＴ１接続を含む。ワイヤレスネットワーク６１２および６１４は、明確で、一意で、かつ関連していないネットワークを表現し得、または、それらは、異なる国の同一のネットワークを表現し得、ならびに図１のワイヤレスネットワーク２０と関連して上述された任意の異なるタイプのネットワークであり得る。

【０１０６】

いくつかのインプリメンテーションにおいて、複数の空中を介する情報交換メカニズムは、企業ＬＡＮ６０６において提供され得る。図６の例示的通信システムにおいて、例えば、メッセージサーバ６２０上のユーザアカウントと関連するメールボックス６１９を有するユーザと関連したモバイルデバイス６１６、６１８は、異なったワイヤレスネットワーク６１２および６１４上で動作するように構成される。ワイヤレスネットワーク６１２が、Ｉｐｖ６アドレシングを支援した場合、ワイヤレスＶＰＮルータ６３２は、ワイヤレ

スネットワーク６１２内で動作する任意のモバイルデバイス６１６とデータを交換するためにワイヤレスコネクタシステム６２８によって用いられ得る。しかしながら、ワイヤレスネットワーク６１４は、Ｍｏｂｉｔｅｘネットワーク等の異なったタイプのワイヤレスネットワークであり得、この場合、情報は、代替的に、ＷＡＮ６０４およびワイヤレスインフラストラクチャ６１０を介して、ワイヤレスコネクタシステム６２８によってワイヤレスネットワーク６１４内で動作するモバイルデバイス６１８と交換され得る。

【０１０７】

ここで、図６のシステムの動作が、ｅメールメッセージ６３３の例を利用して示される。ｅメールメッセージ６３３は、コンピュータシステム６０２から送信され、かつ、アカウントおよびメールボックス６１９、またはメッセージサーバ６２０と関連したデータストア、およびモビアルデバイス６１６または６１８の両方を有する少なくとも１つの受信側にアドレス指定される。企業ＬＡＮ６０６間での他のタイプの情報の交換は、好適には、さらに、ワイヤレスコネクタシステム６２８によっても可能にされる。

【０１０８】

ＷＡＮ６０４を介してコンピュータシステム６０２から送信されたｅメールメッセージ６３３は、用いられる特定のメッセージングスキーマに依存して、全く安全であり得るか、または、デジタル署名で署名および／または暗号化され得る。例えば、コンピュータシステム６０２がＳ／ＭＩＭＥを用いてセキュアなメッセージングを可能になる場合、ｅメールメッセージ６３３は、署名、暗号化、またはこれらの両方がなされ、かつ上述のように処理され得る。

【０１０９】

６３３のようなｅメールメッセージは、通常、Ｓｉｍｐｌｅ Ｍａｉｌ Ｔｒａｎｓｆｅｒ Ｐｒｏｔｏｃｏｌ（ＳＭＴＰ）、ＲＦＣ８２２ヘッダ、およびＭｕｌｔｉｐｕｒｐｏｓｅ Ｉｎｔｅｒｎｅｔ Ｍａｉｌ Ｅｘｔｅｎｓｉｏｎｓ（ＭＩＭＥ）ボディ部分を用いて、ｅメールメッセージのフォーマットを定義する。これらの技術は全て、当業者には周知である。ｅメールメッセージ６３３は、メッセージサーバ６２０に到達し、メッセージサーバ６２０は、どのメールボックス６１９にｅメールメッセージ６３３が格納されるべきかを判定する。上述のように、ｅメールメッセージ６３３のようなメッセージは、ユーザ名、ユーザアカウント、メールボックス識別子、あるいは特定のアカウントにマッピングされ、またはメッセージサーバ６２０によってメールボックス６１９に関連付けられ得る他のタイプの識別子を含み得る。ｅメールメッセージ６３３に対して、受領者は、通常、ユーザアカウント、従ってメールボックス６１９に対応するｅメールアドレスを用いて識別される。

【０１１０】

ワイヤレスコネクタシステム６２８は、好適には、１つ以上のトリガーイベントが起こったことを検出すると、ワイヤレスネットワーク６１２または６１４を介して、企業ＬＡＮ６０６からユーザのモバイルデバイス６１６または６１８に特定のユーザ選択データアイテム、またはデータアイテムの部分を送信またはミラーリングする。トリガーイベントは、ユーザのネットワーク接続されたコンピュータシステム６２２におけるスクリーンセーバの起動、ユーザのモバイルデバイス６１６または６１８の、インターフェース６２６からの切断、またはモバイルデバイス６１６または６１８からホストシステムに送信された、ホストシステムに格納された１つ以上のメッセージの送信を開始するというコマンドの受信を含むが、これらに限定されない。従って、ワイヤレスコネクタシステム６２８は、コマンドの受信等のメッセージサーバ６２０と関連した、または、１つ以上のネットワーク接続されたコンピュータシステム６２２と関連した、スクリーンセーバ、および上述のイベントの切断を含む、トリガーイベントを検出し得る。モバイルデバイス６１６または６１８の企業データへのワイヤレスアクセスがＬＡＮ６０６で活性化された場合、例えば、ワイヤレスコネクタシステム６２８がモバイルデバイスユーザのトリガーイベントの出現を検出した場合、ユーザによって選択されたデータアイテムは、好適には、ユーザのモバイルデバイスに送信される。ｅメールメッセージ６３３の例において、トリガーイベ

ントが検出されたと想定すると、メッセージサーバ６２０におけるメッセージ６３３の到着は、ワイヤレスコネクタシステム６２８によって検出される。これは、例えば、メッセージサーバ６２０と関連したメールボックス６１９をモニタリングまたは照会することによって達成され得るか、または、メッセージサーバ６２０がＭｉｃｒｏｓｏｆｔ Ｅｘｃｈａｎｇｅサーバである場合、ワイヤレスコネクタシステム６２８は、新しいメッセージがメールボックス６１９にいつ格納されたかという通知を受信するために、ＭＡＰＩ（Ｍｉｃｒｏｓｏｆｔ Ｍｅｓｓａｇｉｎｇ Ａｐｐｌｉｃａｔｉｏｎ Ｐｒｏｇｒａｍｍｉｎｇ Ｉｎｔｅｒｆａｃｅ）によって提供されたアドバイスｓｙｎｃｓについて登録し得る。

【０１１１】

ｅメールメッセージ６３３等のデータアイテムがモバイルデバイス６１６または６１８に送信されるべき場合、ワイヤレスコネクタシステム６２８は、好適には、モバイルデバイスに対してトランスペアレントである態様で、データアイテムを再パッケージ化する。その結果、モバイルデバイスに送信され、かつモバイルデバイスによって受信された情報は、図６のホストシステム、ＬＡＮ６０６に格納され、かつアクセス可能なである情報と同様であるように見える。ある好ましい再パッケージ化方法は、電子エンベロープのワイヤレスネットワーク６１２、６１４を介して送信されるべき受信されたメッセージをラッピングするステップを包含する。電子エンベロープは、メッセージが送信されるべきモバイルデバイス６１６、６１８のワイヤレスネットワークアドレスに対応する。あるいは、特別用途のＴＣＰ／ＩＰラッピング技術のような、他の再パッケージ化方法を利用し得る。このような再パッケージ化はまた、結果として、ｅメールメッセージがモバイルデバイスから作成され、かつ送信されようとも、モバイルデバイス６１６または６１８から送信されるｅメールメッセージは、対応するホストシステムアカウントまたはメールボックス６１９に由来するように見える。従って、モバイルデバイス６１６または６１８のユーザは、ホストシステムアカウントまたはメールボックス６１９とモバイルデバイスとの間で単一のｅメールアドレスを効果的に共有する。

【０１１２】

ｅメールメッセージ６３３の再パッケージ化は、６３４および６３６で指示される。再パッケージ化技術は、任意の利用可能な送信経路と同様であり得るか、または特定の送信経路に依存し得、ワイヤレスインフラストラクチャ６１０またはワイヤレスＶＰＮルータ６３２のいずれかである。例えば、ｅメールメッセージ６３３は、好ましくは、６３４で再パッケージ化される前または後のどちらかに、圧縮され、かつ暗号化されて、それにより、モバイルデバイス６１８へのセキュアな送信を効果的に提供する。圧縮は、メッセージを送信するために必要とされる帯域幅を低減する一方で、暗号化は、モバイルデバイス６１６および６１８に送信される任意のメッセージまたは他の情報の機密性を保証する。対照的に、ＶＰＮルータ６３２を介して送信されたメッセージは、ＶＰＮルータ６３２によって確立されたＶＰＮ接続が本質的にセキュアであるために、圧縮のみがなされ、暗号化はされなくてもよい。メッセージは、従って、ワイヤレスコネクタシステム６２８の暗号化か、ＶＰＮルータ６３２のどちらかを介して、モバイルデバイス６１６および６１８にセキュアに送信される。ワイヤレスコネクタシステム６２８は、非標準的なＶＰＮトンネルまたは例えばＶＰＮのような接続を考慮されなくてもよい。従って、モバイルデバイス６１６または６１８を用いたメッセージへのアクセスは、デスクトップコンピュータシステム６２２を用いたＬＡＮ６０６のメールボックスへのアクセスと比較して、セキュアではない。

【０１１３】

再パッケージ化されたメッセージ６３４または６３６が、ワイヤレスインフラストラクチャ６１０、またはワイヤレスＶＰＮルータ６３２を介してモバイルデバイス６１６または６１８に到着した場合、モバイルデバイス６１６または６１８は、再パッケージ化されたメッセージ６３４または６２６から外部電子エンベロープを除去し、任意の必要とされる解凍および復号化動作を実行する。オリジナルメッセージ６３３が、セキュアなメッセ

ージである場合、さらなる処理がまた、モバイルデバイス６１６、６１８によって実行され得る。モバイルデバイス６１６または６１８から送信され、かつ、１つ以上の受信側にアドレス指定されたメッセージは、好適には、同様に再パッケージ化され、場合によっては、圧縮および暗号化されて、ＬＡＮ６０６等のホストシステムに送信される。ホストシステムは、その後、再パッケージ化されたメッセージから電子エンベロープを除去し、所望である場合、メッセージを復号化および解凍して、アドレス指定された受信側にメッセージをルーティングし得る。

【０１１４】

外側のエンベロープを用いる別の目的は、オリジナルｅメールメッセージ６３３にアドレス指定情報の少なくともいくつかを維持することである。情報をモバイルデバイス６１６、６１８にルーティングするために利用される外部エンベロープは、１つ以上のモバイルデバイスのネットワークアドレスを用いてアドレス指定されるが、外部のエンベロープは、好ましくは、可能であれば圧縮されおよび／または暗号化された形式で、少なくとも１つのアドレスフィールドを含む、オリジナルのｅメールメッセージ６３３全体をカプセル化する。これは、ｅメールメッセージ６３３のオリジナル「Ｔｏ」、「Ｆｒｏｍ」および「ＣＣ」アドレスを、外部エンベロープが除去され、かつメッセージがモバイルデバイス６１６または６１８上で表示された場合に表示させることができる。この再パッケージ化はまた、ホストシステムのモバイルデバイスユーザのアカウントまたはメールボックスのアドレスを反映する「Ｆｒｏｍ」フィールドによって、モバイルデバイスから送信され再パッケージ化され出て行くメッセージの外部エンベロープが、ワイヤレスコネクタシステム６２８によって除去された場合に、返答メッセージがアドレス指定された受領側に送信されることを可能にする。モバイルデバイス６１６または６１８からのユーザのアカウントまたはメールボックスアドレスを用いることは、モバイルデバイスから送信されたメッセージが、モバイルデバイスではなくホストシステムのユーザのメールボックス６１９またはアカウントから由来したメッセージであるように見えるようにすることができる。

【０１１５】

図７は、代替的な例示的通信システムのブロック図であり、ここで、ワイヤレス通信システムは、ワイヤレスネットワークのオペレータと関連付けられたコンポーネントによって使用可能にされる。図７に示されるように、システムは、コンピュータシステム７０２、ＷＡＮ７０４、セキュリティファイアウォール７０８の後に配置された企業ＬＡＮ７０７、ネットワークオペレータインフラストラクチャ７４０、ワイヤレスネットワーク７１１、およびモバイルデバイス７１３および７１５を含む。コンピュータシステム７０２、ＷＡＮ７０４、セキュリティファイアウォール７０８、メッセージサーバ７２０、データストア７１７、メールボックス７１９、およびＶＰＮルータ７３５は、実質的に、図６に同様に符号付けされたコンポーネントと同じである。しかしながら、ＶＰＮルータ７３５は、ネットワークオペレータインフラストラクチャ７４０と通信するので、これは、必ずしも図７のシステムにおけるワイヤレスＶＰＮルータである必要はない。ネットワークオペレータインフラストラクチャ７４０は、それぞれ、コンピュータシステム７４２および７５２と関連付けられ、かつ、ワイヤレスネットワーク７１１内で動作するように構成されるＬＡＮ７０７とモバイルデバイス７１３、７１５との間のワイヤレス情報交換を可能にする。ＬＡＮ７０７において、複数のデスクトップコンピュータシステム７４２、７５２はが示され、これらの各々は、インターフェースまたはコネクタ７４８、７５８への物理的接続７４６、７５６を有する。ワイヤレスコネクタシステム７４４、７５４は、各コンピュータシステム７４２、７５２上でまたはこれと共に動作する。

【０１１６】

ワイヤレスコネクタシステム７４４、７５４は、ｅメールメッセージ、およびメールボックス７１９に格納される他のアイテム、ならびに、場合によっては、ローカルまたはネットワークダータストアに格納されたデータアイテム等のデータアイテムが、ＬＡＮ７０７から１つ以上のモバイルデバイス７１３、７１５に送信されることを可能にするという点で、上述のワイヤレスコネクタシステム７２８と同様である。しかしながら、図７にお

いて、ネットワークオペレータインフラストラクチャ７４０は、モバイルデバイス７１３、７１５とＬＡＮ７０７との間にインターフェースを提供する。上述のように、図７に示されるシステムの動作は、モバイルデバイス７１３、７１５に送信され得るデータアイテムの図式的例としてｅメールメッセージの文脈で後述される。

【０１１７】

メッセージサーバ７２０上にアカウントを有する１つ以上の受信側にアドレス指定されたｅメールメッセージ７３３がメッセージサーバ７２０によって受信された場合、中央メールボックスまたはデータストアに格納されたメッセージ、またはメッセージの単一のコピーへのポインタがこのような各受信側のメールボックス７１９に格納される。一旦ｅメールメッセージ７３３またはポインタがメールボックス７１９に格納されると、これは、好適には、モバイルデバイス７１３または７１５を用いてアクセスされ得る。図７に示された例において、ｅメールメッセージ７３３は、デスクトップコンピュータシステム７４２および７５２の両方、従って、モバイルデバイス７１３および７１５の両方と関連したメールボックス７１９にアドレス指定されている。

【０１１８】

当業者が理解するように、一般的に、ＬＡＮ７０７および／またはＷＡＮ７０４等のワイヤドネットワークにおいて用いられる通信ネットワークプロトコルは、７１１等のワイヤレスネットワーク内で用いられるワイヤレスネットワーク通信プロトコルと適切でなく、かつ互換性がない。例えば、主に、ワイヤレスネットワーク通信と関係する通信帯域幅、プロトコルオーバーヘッドおよびネットワーク待ち時間は、通常、ワイヤレスネットワークよりもはるかに高いキャパシティおよび高速を有するワイヤドネットワークにおいてはあまり重要でない。従って、モバイルデバイス７１３および７１５は、通常、データストア７１７に直接アクセスし得ない。ネットワークオペレータインフラストラクチャ７４０は、ワイヤレスネットワーク７１１とＬＡＮ７０７との間に中継を提供する。

【０１１９】

ネットワークオペレータインフラストラクチャ７４０は、モバイルデバイス７１３、７１５が、ＷＡＮ７０４を通じてＬＡＮ７０７への接続を確立することを可能にし、かつ、例えば、ワイヤレスネットワーク７１１のオペレータ、またはモバイルデバイス７１３および７１５にワイヤレス通信サービスを提供するサービスプロバイダによって操作され得る。プルベースのシステムにおいて、モバイルデバイス７１３、７１５は、情報が機密の状態であるべき場合、ワイヤレスネットワーク互換通信スキーマ、好適には、ＷＴＬＳ（Ｗｉｒｅｌｅｓｓ　Ｔｒａｎｓｐｏｒｔ　Ｌａｙｅｒ　Ｓｅｃｕｒｉｔｙ）等のセキュアスキーマ、および、ＷＡＰ（Ｗｉｒｅｌｅｓｓ　Ａｐｐｌｉｖａｔｉｏｎ　Ｐｒｏｔｏｃｏｌ）ブラウザ等のワイヤレスウェブブラウザを用いて、ネットワークオペレータインフラストラクチャ７４０との通信セッションを確立し得る。ユーザは、その後、（モバイルデバイスに常駐するソフトウェアにおける手動の選択または事前選択されたデフォルトを通じて）、例えば、ＬＡＮ７０７におけるデータストア７１７におけるメールボックス７１９に格納された任意の、またはすべての情報、または新しい情報のみをリクエストし得る。セッションがまだ確立されていない場合、ネットワークオペレータインフラストラクチャ７４０は、例えば、ＨＴＰＳ（Ｓｅｃｕｒｅ　Ｈｙｐｅｒｔｅｘｔ　Ｔｒａｎｓｆｅｒ　Ｐｒｏｔｏｃｏｌ）を用いて、ワイヤレスコネクタシステム７４４、７５４との接続またはセッションを確立する。上述のように、ネットワークオペレータインフラストラクチャ７４０とワイヤレスコネクタシステム７４４、７５４との間のセッションは、利用可能である場合、典型的なＷＡＮ接続を介してか、または、ＶＰＮルータ７３５を通じて成され得る。モバイルデバイス７１３、７１５からのリクエストの受信と、リクエストされた情報のデバイスへの返却との間の時間遅延が最小化されるべきであり、ネットワークオペレータインフラストラクチャ７４０およびワイヤレスコネクタシステム７４４、７５４は、一旦通信接続が確立されるとオープンの状態であるように構成され得る。

【０１２０】

図７のシステムにおいて、モバイルデバイスＡ７１３およびＢ７１５から発信されたリ

クエストは、ワイヤレスコネクタシステム７４４および７５４それぞれに送信される。ネットワークオペレータインフラストラクチャ７４０からの情報のリクエストを受信すると、ワイヤレスコネクタシステム７４４、７５４は、リクエストされた情報をデータストアから取り出す。ｅメールメッセージ７３３について、ワイヤレスコネクタシステム７４４、７５４は、通常、メッセージサーバ７２０を介してか、または、直接的に、メールボックス７１９にアクセスし得るコンピュータシステム７４２、７５２と共に動作するメッセージングクライアントを通じて、適切なメールボックス７１９からｅメールメッセージ７３３を取り出す。あるいは、ワイヤレスコネクタシステム７４４、７５４は、メールボックス７１９それ自体に直接か、またはメッセージサーバ７２０を通じてアクセスするように構成され得る。さらに、他のデータストア、データストア７１７と類似のネットワークデータストア、および各コンピュータシウテム７４２、７５２と関連付けられたローカルデータストアの両方が、ワイヤレスコネクタシステム７４４、７５４、従って、モバイルデバイス７１３、７１５にアクセス可能であり得る。

【０１２１】

ｅメールメッセージ７３３が、コンピュータシステム７４２および７５２ならびにデバイス７１３および７１５の両方と関連付けられたメッセージサーバアカウントまたはメールボックス７１９にアドレス指定された場合、ｅメールメッセージ７３３は、７６０および７６２に示されるように、ネットワークオペレータインフラストラクチャ７４０に送信され得、これは、その後、７６４および７６６に示されるように、ｅメールメッセージのコピーを各モバイルデバイス７１３よび７１５に送信する。情報は、ＷＡＮ７４４またはＶＰＮルータ７３５への通接続を介して、ワイヤレスコネクタシステム７４４、７５４と、ネットワークオペレータインフラストラクチャ７４０との間で送信され得る。ネットワークオペレータインフラストラクチャ７４０が、異なったプロトコルを介してワイヤレスコネクタシステム７４４、７５４およびモバイルデバイス７１３、７１５と通信する場合、ネットワークオペレータインフラストラクチャ７４０によって翻訳動作が実行され得る。再パッケージ化技術は、さらに、ワイヤレスコネクタシステム７４４、７５４と、ネットワークオペレータインフラストラクチャ７４０との間、および、各モバイルデバイス７１３、７１５と、ネットワークオペレータインフラストラクチャ７４０との間で用いられ得る。

【０１２２】

モバイルデバイス７１３、７１５から送信されるべきメッセージまたは他の情報が同様に処理され得、このような情報は、最初に、モバイルデバイス７１３、７１５からネットワークオペレータインフラストラクチャ７４０に送信される。ネットワークオペレータインフラストラクチャ７４０は、その後、例えば、メッセージサーバ７２０によって、メールボックス７１９に格納、および、任意のアドレス指定された受信側に送達するために、ワイヤレスコネクタシステム７３３、７５４に情報を送信し得るか、または、代替的に、アドレス指定された受信側に情報を送達し得る。

【０１２３】

図７におけるシステムについてのこれまでの説明は、プルベース動作に関する。ワイヤレスコネクタシステム７４４、７５４およびネットワークオペレータインフラストラクチャは、その代わりに、データアイテムをモバイルデバイス７１３および７１５にプッシュするように構成され得る。組み合わされたプッシュ／プルシステムもまた可能である。例えば、現在、ＬＡＮ７０７におけるデータストアに格納される新しいメッセージの通知またはデータアイテムのリストは、モバイルデバイス７１３、７１５にプッシュされ得、これは、その後、ネットワークオペレータインフラストラクチャ７４０を介してＬＡＮ７０７からメッセージまたはデータアイテムをリクエストするために用いられ得る。

【０１２４】

ＬＡＮ７０７上のユーザアカウントと関連付けられたモバイルデバイスが、異なったワイヤレスネットワーク内で動作するように構成された場合、各ワイヤレスネットワークは、２０４０と類似の関連したワイヤレスネットワークインフラストラクチャコンポーネン

トを有し得る。

【０１２５】

図７のシステムにおけるコンピュータシステム７４２、７５２ごとに、別個の専用ワイヤレスコネクタシステム７４４、７５４が示されるが、１つ以上のワイヤレスコネクタシステム７４４、７５４は、好適には、複数のコンユータシステム７４２、７５２と共に動作するようにか、または、複数のコンピュータシステムと関連付けられたデータストアまたはメールボックス７１９にアクセスするように構成され得る。例えば、ワイヤレスコネクタシステム７４４は、コンピュータシステム７４２およびコンピュータシステム７５２の両方と関連付けられたメールボックス７１９へのアクセスが認められ得る。モバイルデバイスＡ７１３またはＢ７１５からのデータアイテムのリクエストは、その後、ワイヤレスコネクタシステム７４４によって処理され得る。この構成は、デスクトップコンピュータシステム７４２、７５２がモバイルデバイスユーザごとに走行することを必要とすることなく、ＬＡＮ７０７とモバイルデバイス７１３および７１５との間のワイヤレス通信を可能にするために有用であり得る。ワイヤレスコンピュータシステムは、その代わりに、ワイヤレス通信を可能にするためにメッセージサーバ７２０と共に実現され得る。

【０１２６】

図８は、別の代替的通信システムのブロック図である。システムは、コンピュータシステム８０２、ＷＡＮ８０４、セキュリティファイアウォール８０８の後に配置された企業ＬＡＮ８０９、アクセスゲートウェイ８８０、データストア８８２、ワイヤレスネットワーク８８４および８８６、ならびにモバイルデバイス８８８および８９０を含む。ＬＡＮ８０９において、コンピューアシステム８０２、ＷＡＮ８０４、セキュリティファイアウォール８０８、メッセージサーバ８２０、データストア８１７、メールボックス８１９、デスクトップコンピュータシステム８２２、物理的接続８２４、インターフェースまたはコネクタ８２６、ならびにＶＰＮルータ８３５は、実質的に、上述の対応するコンポーネントと同じである。アクセスゲートウェイ８８０およびデータストア８８２は、モバイルデバイス８８８および８９０にＬＡＮ８０９に格納されたデータアイテムへのアクセスを提供する。図８において、ワイヤレスコネクタシステム８７８は、メッセージサーバ８２０上またはこれと共に動作するが、ワイヤレスコネクタシステムは、むしろ、ＬＡＮ８０９における１つ以上のデスクトップコンピュータシステム上またはこれと共に動作し得る。

【０１２７】

ワイヤレスコネクタシステム８７８は、１つ以上のモバイルデバイス８８８、８９０へのＬＡＮ８０９に格納されたデータアイテムの転送を提供する。これらのデータアイテムは、好適には、データストア８１７におけるメールボックス８１９に格納されたｅメールメッセージ、および、場合によっては、データストア８１７または別のネットワークデータストア、または８２２等のコンピュータシステムのローカルデータストアに格納された他のアイテムを含む。

【０１２８】

上述のように、メッセージサーバ８１７上にアカウントを有する１つ以上の受信側にアドレス指定され、かつ、メッセージサーバ８２０によって受信されたｅメールメッセージ８３３は、そのような各受信側のメールボックス８１９に格納され得る。図８のシステムにおいて、外部データストア８８２は、好適には、データストア８１７と類似の構造を有し、かつ、このデータストアと同期化された状態である。データストア８８２に格納されたＰＩＭ情報またはデータは、好適には、独立して、ホストシステムに格納されたＰＩＭ情報またはデータに変更可能である。この特定の構成において、外部データストア８８２における独立して変更可能な情報は、ユーザと関連付けられた複数のデータストアの同期化を維持し得る（すなわち、モバイルデバイス上のデータ、自宅のパーソナルコンピュータ上のデータ、企業ＬＡＮにおけるデータ等）。この同期化は、例えば、１日の特定の時間、または、ＬＡＮ８０９で起動された場合に、データストア８８２にてメッセージサーバ８２０またはコンピュータシステム８２２によってか、場合によっては、アクセスゲー

トウェイ８８０を通じてモバイルデバイス８８８、８９０によって、データストア８１７に入力が追加または変更されるたびに、ワイヤレスコネクタシステム８７８によって、特定の時間間隔でデータストア８８２に送信される更新を通じて達成され得る。

【０１２９】

例えば、ｅメールメッセージ８３３の場合、ｅメールメッセージ８３３が受信された後のいつか、データストア８８２に送信された更新は、メッセージ８３３がストア８１７における特定のメールボックス８１９に格納されたことを示し得、ｅメールメッセージのコピーは、データストア８８２における対応する格納領域に格納される。ｅメールメッセージ８３３が、例えば、モバイルデバイス２０８８および２０９０に対応するメールボックス２０１９に格納された場合、図８において８９２および８９４で示されるｅメールメッセージの１つ以上のコピーが、データストア８８２における対応する格納領域またはメールボックスに送信され、ここに格納される。示されるように、データストア８１７において格納された情報の更新またはコピーは、ＷＡＮ８０４またはＶＰＮルータ８３５への接続を介してデータストア８８２に送信され得る。例えば、ワイヤレスコネクタシステム８７８は、更新、または格納された情報を、ＨＴＴＰポストリクエストを介してデータストア８８２におけるリソースにポストし得る。あるいは、ＨＴＴＰＳまたはＳＳＬ（Ｓｅｃｕｒｅ　ｓｏｃｋｅｔｓ　Ｌａｙｅｒ）等のセキュアプロトコルが用いられ得る。当業者は、ＬＡＮ８０９のデータストアにおける複数のロケーションロケーションに格納されたデータアイテムの単一のコピーが、むしろ、データストア８８２に送信され得ることを理解する。データアイテムのこのコピーは、その後、データストア８８２における複数の対応するロケーションに格納され得るか、または、単一のコピーは、データストア８８２における各対応するロケーションに格納されている格納されたデータアイテムのポインタまたは他の識別子を共にデータストア８８２に格納され得る。

【０１３０】

アクセスゲートウェイ８８０は、データストア８８２へのアクセスを有するモバイルデバイス８８８および８９０を提供するという点で有効なアクセスプラットフォームである。データストア８８２は、ＷＡＮ８０４上にアクセス可能なリソースとして構成され得、アクセスゲートウェイ８８０は、モバイルデバイス８８８および８９０がＷＡＮ８０に接続し得るＩＳＰシステムまたはＷＡＰゲートウェイであり得る。ＷＡＰブラウザ、またはワイヤレスネットワーク８８４および８８６と互換性のある他のブラウザが、データストア８１７と同期化されたデータストア８８２にアクセスし、かつ、格納されたデータアイテムを、自動的に、またはモバイルデバイス８８８、８９０からのリクエストに応答してダウンロードする。８９６および８９８に示されるように、データストア８１７に格納されたｅメールメッセージ８３３のコピーが、モバイルデバイス８８８および８９０に送信され得る。各モバイルデバイス８８８、８９０上のデータストア（図示せず）は、これにより、メールボックス８１９等の、企業ＬＡＮ８０９上のデータストア８１７の一部分と同期化され得る。モバイルデバイスデータストアへの変更は、データストア８８２および８１７に、同様に反映され得る。

【０１３１】

上述の記載は、好適な例示的実施形態に関することが理解される。本発明の複数の変形が、当該分野の当業者に明らかであり、このような明らかな変形は、明示的に記載されたか否かに関わらず、記載および主張された本発明の範囲内である。

【０１３２】

例えば、ワイヤレスモバイル通信デバイスは、メッセージングクライナントの１つとして図３～図５に示され、かつ記載されるが、本発明は、デスクトップおよびラップトップコンピュータシステム、ネットワークコンピュータワークステーション、ならびに、例えば、Ｃｅｒｔを管理および転送して、Ｃｅｒｔを共有することを可能にすることが所望される他のタイプのメッセージングクライアント上で動作するものを含む、他のメッセージングクライアントにも適用可能である。

【０１３３】

他のＣｅｒｔ関連情報が、上述のように、実質的にメッセージングクライアント間で管理および転送され得ることもまた考えられる。ＣＲＬ、公開鍵および秘密鍵は、同様に、管理および／または転送され得る。

【図面の簡単な説明】

【０１３４】

【図１】図１は、例示的なメッセージングシステムのブロック図である。

【図２】図２は、メッセージングシステムのセキュアな電子メールメッセージ交換を示すブロック図である。

【図３】図３は、ワイヤレスモバイル通信デバイス、ならびに関連するＣｅｒｔの管理および送信システムを実装するコンピュータシステムのブロック図である。

【図４】図４は、メッセージングを行うクライアント間のＣｅｒｔの管理および送信方法を示すフローチャートである。

【図５】図５は、本発明の局面に従ったシステムおよび方法が実装され得るメッセージングを行うクライアントの例となる、ワイヤレスモバイル通信デバイスのブロック図である。

【図６】図６は、通信システムの例を示すブロック図である。

【図７】図７は、別の通信システムの例のブロック図である。

【図８】図８は、さらに別の通信システムのブロック図である。

【図１】

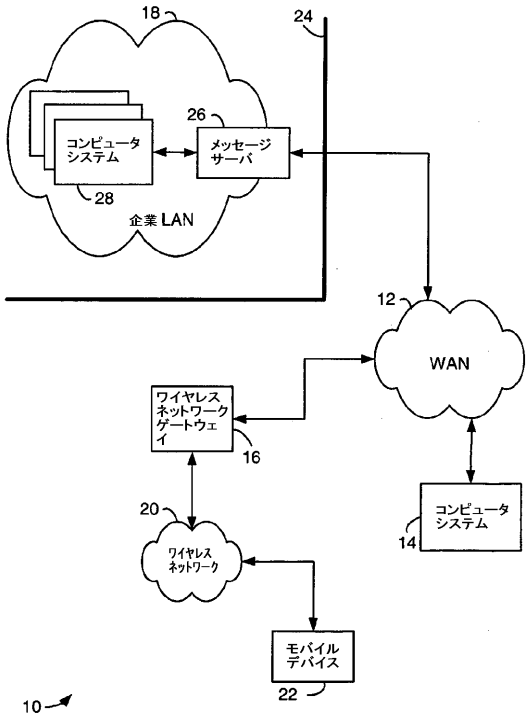

FIG. 1

【図２】

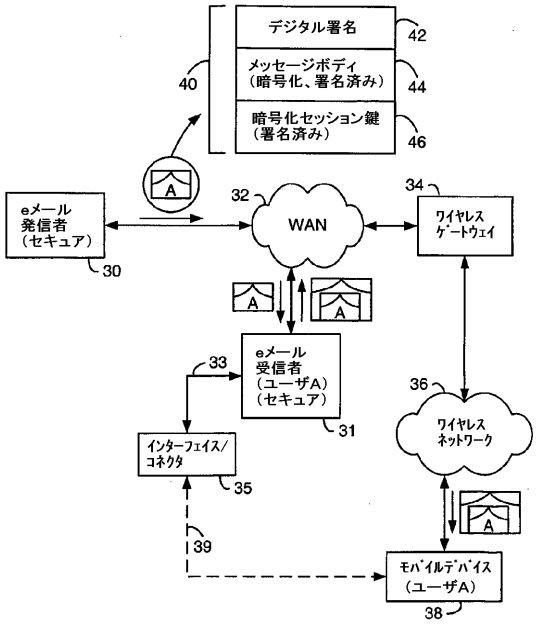

FIG. 2

【図３】

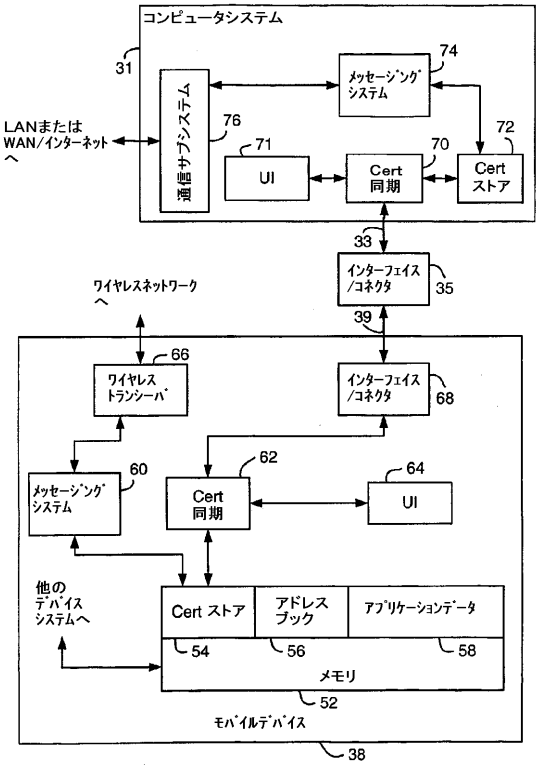

FIG. 3

【図４】

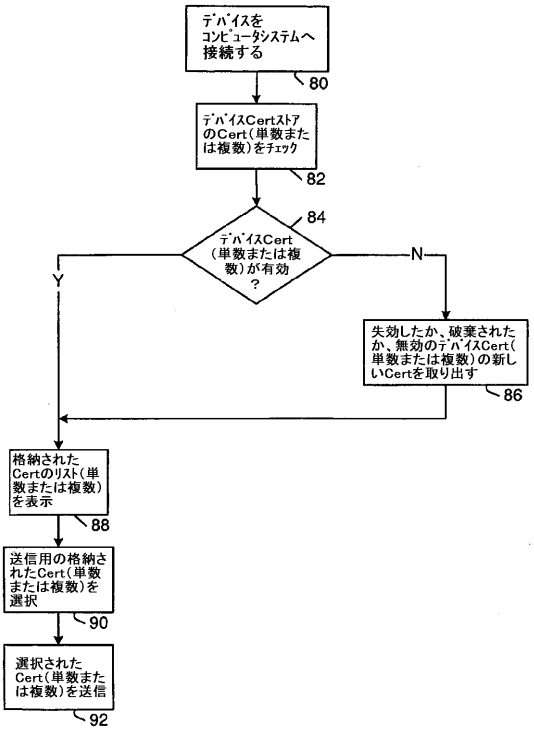

FIG. 4

【図５】

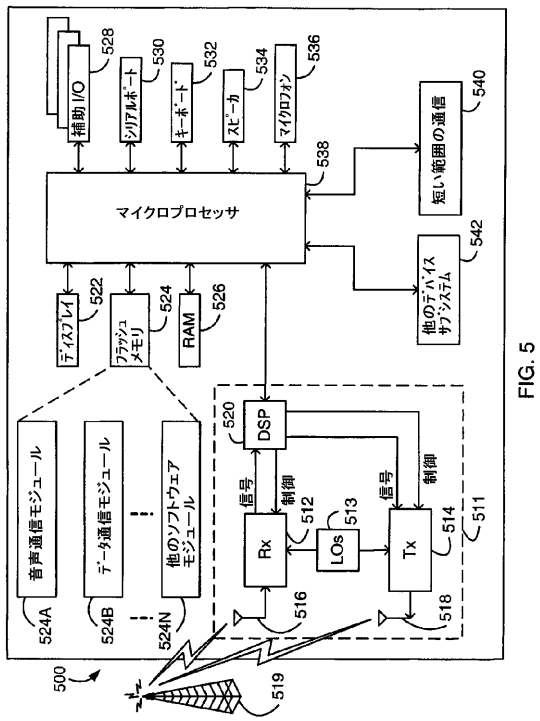

FIG. 5

【図６】

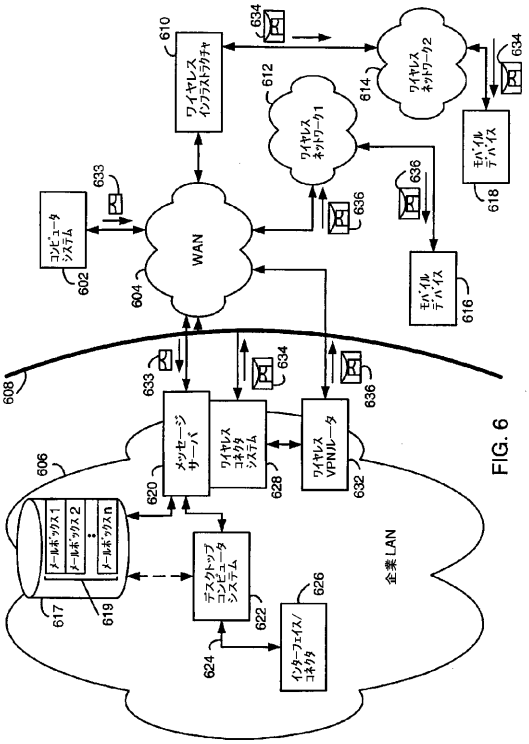

FIG. 6

【図７】

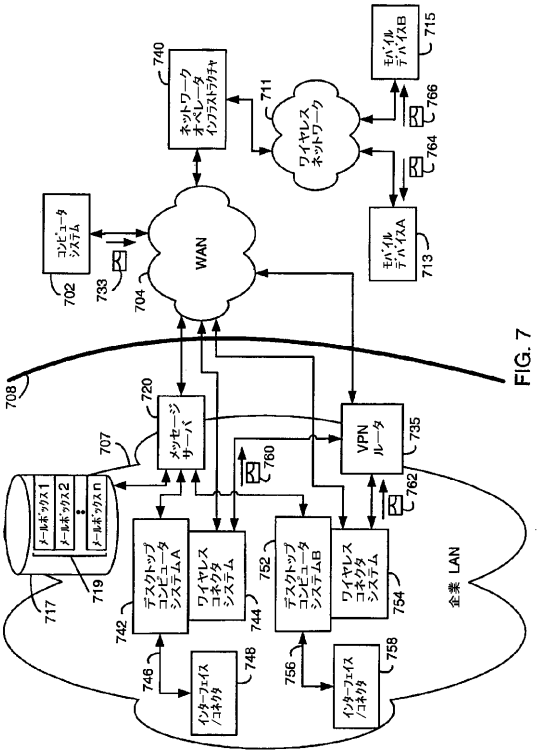

FIG. 7

【図８】

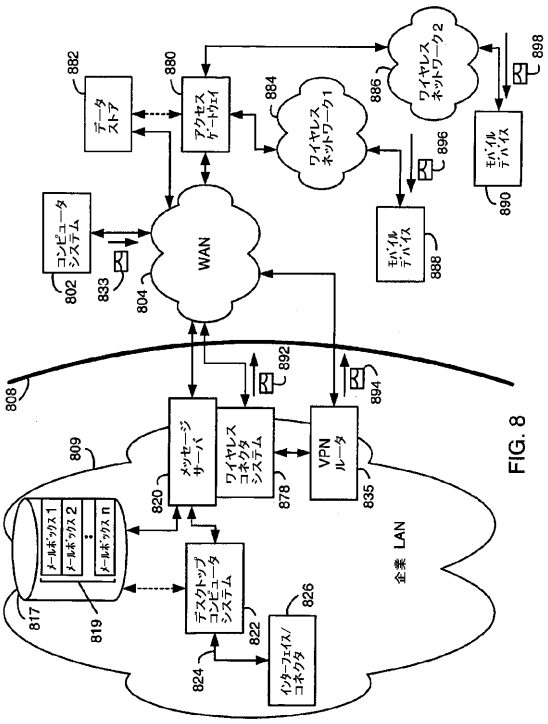

FIG. 8

フロントページの続き

(74)代理人 100113413
弁理士 森下 夏樹
(72)発明者 ハーバート エイ. リトル
カナダ国 オンタリオ エヌ２ティー ２ブイ８, ウォータールー, オールド オーク プレイス ５０４
(72)発明者 ネイル ピー. アダムス
カナダ国 オンタリオ エヌ２ジェイ ３エックス２, ウォータールー, マックグレゴー クレス １５１, アパートメント ５
(72)発明者 デイビット ピー. タプスカ
カナダ国 オンタリオ エヌ２エル １ダブリュー５, ウォータールー, アーブ ストリート ウェスト ５１２－２８５
(72)発明者 マイケル エス. ブラウン
カナダ国 オンタリオ エヌ２ケイ ４ビー１, ウォータールー, ユニバーシティ ダウンズ クレ. ３５０
(72)発明者 マイケル ジー. カークアップ
カナダ国 オンタリオ ケイ７エム ２エイ９, キングストン, クイーン メアリー アールディ ２０４, アパートメント ５１０
(72)発明者 ジェイムズ エイ. ゴッドフレイ
カナダ国 オンタリオ エヌ２ジェイ ３ビー８, ウォータールー, レジーナ ストリート エヌ. ３００, ナンバー１５０６エイ
Ｆターム(参考) 5B285 AA04 CA02 CA44 DA05
5J104 AA16 EA05 KA02 KA05 PA07