(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4491402号
(P4491402)
(45)発行日　平成22年6月30日(2010.6.30)　(24)登録日　平成22年4月9日(2010.4.9)

(51)Int.Cl.　F I
H04L 9/32 (2006.01)　H04L 9/00 675B
H04L 9/00 675Z

請求項の数 11　(全 28 頁)

(21)出願番号　特願2005-313157(P2005-313157)
(22)出願日　平成17年10月27日(2005.10.27)
(65)公開番号　特開2006-129490(P2006-129490A)
(43)公開日　平成18年5月18日(2006.5.18)
審査請求日　平成17年10月27日(2005.10.27)
(31)優先権主張番号　04105424.8
(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　100107489
弁理士　大塩　竹志

最終頁に続く

(54)【発明の名称】証明書におけるデジタル署名を確証するためのシステムおよび方法

(57)【特許請求の範囲】
【請求項１】
コンピューティング装置上で証明書上のディジタル署名を検証する方法であって、該コンピューティング装置は、入力手段とプロセッサと記憶装置とを含み、
該方法は、
該入力手段が、該証明書と、該デジタル署名と、該証明書の発行者に関連付けられている公開鍵とを受信するステップと、
該プロセッサが、該受信された公開鍵と同一である公開鍵が該記憶装置に格納されているかどうかを決定するステップと、
該プロセッサが、該受信された公開鍵と同一である該公開鍵が該記憶装置に格納されていないと決定した場合には、
該プロセッサが、
該受信された公開鍵を用いて、該ディジタル署名に対して署名検証処理を実行することと、
該署名検証処理において該ディジタル署名の検証が成功したかどうかを決定することと、
該署名検証処理において該ディジタル署名の検証が成功したと決定された場合には、該公開鍵を該記憶装置に格納し、該ディジタル署名の検証が成功したことを示すことを行うステップと、
該プロセッサが、該受信された公開鍵と同一である該公開鍵が該記憶装置に格納されて

いると決定した場合には、該プロセッサが、該ディジタル署名の検証が成功したことを示すステップと
を含む、方法。
【請求項２】
コンピューティング装置上で証明書上のディジタル署名を検証する方法であって、該コンピューティング装置は、入力手段とプロセッサと記憶装置とを含み、
該方法は、
該入力手段が、該証明書と、該デジタル署名と、該証明書の発行者に関連付けられている公開鍵とを受信するステップと、
該プロセッサが、該受信された公開鍵と同一である公開鍵が該記憶装置に格納されているかどうかを決定するステップと、
該プロセッサが、該受信された公開鍵と同一である該公開鍵が該記憶装置に格納されていないと決定した場合には、
該プロセッサが、
該受信された公開鍵を用いて、該ディジタル署名に対して署名検証処理を実行することと、
該署名検証処理において該ディジタル署名の検証が成功したかどうかを決定することと、
該公開鍵を該記憶装置に格納することと、
該公開鍵に対応する結果を該記憶装置に格納することであって、該結果は、該署名検証処理において該ディジタル署名の検証が成功したかどうかを示す、ことと
を行うステップと、
該プロセッサが、該受信された公開鍵と同一である該公開鍵が該記憶装置に格納されていると決定した場合には、該プロセッサが、該格納された公開鍵に対応する結果を該記憶装置から検索し、該検索された結果が該署名検証処理において該ディジタル署名の検証が成功したことを示しているかどうかを決定するステップと、
該プロセッサが、該検索された結果が該署名検証処理において該ディジタル署名の検証が成功したことを示していると決定した場合には、該プロセッサが、該ディジタル署名の検証が成功したことを示すステップと
を含む、方法。
【請求項３】
前記プロセッサが、前記署名検証処理において前記ディジタル署名の検証が成功しなかったと決定した場合、該プロセッサが、該ディジタル署名の検証が失敗したことを示すステップをさらに含む、請求項１に記載の方法。
【請求項４】
前記プロセッサが、前記署名検証処理において前記ディジタル署名の検証が成功しなかったと決定し、かつ、該プロセッサが、前記検索された結果が該署名検証処理において該ディジタル署名の検証が成功しなかったことを示していると決定した場合には、該プロセッサが、該ディジタル署名の検証が失敗したことを示すステップをさらに含む、請求項２に記載の方法。
【請求項５】
前記コンピューティング装置は、モバイル装置である、請求項１から４のいずれか１項に記載の方法。
【請求項６】
コンピューティング装置上で実行されるプログラムコード手段を含むコンピュータ読み取り可能な媒体であって、該プログラムコード手段が実行されることにより、請求項１から５のいずれか一項に記載の方法のステップを実行することを該コンピューティング装置に行わせる、コンピュータ読み取り可能な媒体。
【請求項７】
証明書上のディジタル署名を検証するシステムであって、該システムは、少なくとも１

つのコンピューティング装置を含み、該少なくとも１つのコンピューティング装置のそれぞれは、プログラムコード手段を実行することにより、請求項１から５のいずれか一項に記載の方法のステップを実行することを各コンピューティング装置に行わせるように構成されている、システム。

【請求項８】

証明書上のディジタル署名を検証するモバイル装置であって、

該モバイル装置は、

該証明書と、該デジタル署名と、該証明書の発行者に関連付けられている公開鍵とを受信する入力手段と、

少なくとも１つの公開鍵を格納する記憶装置と、

該受信された公開鍵と同一である公開鍵が該記憶装置における該少なくとも１つの公開鍵のうちの１つとして格納されているかどうか決定するプロセッサと

を含み、

該受信された公開鍵と同一である公開鍵が、該記憶装置における該少なくとも１つの公開鍵のうちの１つとして格納されていないと決定された場合には、

該プロセッサが、

該受信された公開鍵を用いて、該ディジタル署名に対して署名検証処理を実行することと、

該署名検証処理において該ディジタル署名の検証が成功したかどうかを決定することと、

該署名検証処理において該ディジタル署名の検証が成功したと決定された場合には、該公開鍵を該記憶装置に格納し、該ディジタル署名の検証が成功したことを示すことと

を行うようにさらに構成されており、

該プロセッサが、該受信された公開鍵と同一である該公開鍵が該記憶装置における該少なくとも１つの公開鍵のうちの１つとして格納されていると決定した場合には、該プロセッサが、該ディジタル署名の検証が成功したことを示すようにさらに構成されている、モバイル装置。

【請求項９】

証明書上のディジタル署名を検証するモバイル装置であって、

該モバイル装置は、

該証明書と、該デジタル署名と、該証明書の発行者に関連付けられている公開鍵とを受信する入力手段と、

少なくとも１つの公開鍵と少なくとも１つの結果とを格納する記憶装置であって、該少なくとも１つの結果のそれぞれは、該少なくとも１つの公開鍵のうちの１つに対応している、記憶装置と、

該受信された公開鍵と同一である公開鍵が該記憶装置における該少なくとも１つの公開鍵のうちの１つとして格納されているかどうか決定するプロセッサと

を含み、

該受信された公開鍵と同一である公開鍵が、該記憶装置における該少なくとも１つの公開鍵のうちの１つとして格納されていないと決定された場合には、

該プロセッサは、

該受信された公開鍵を用いて、該ディジタル署名に対して署名検証処理を実行することと、

該署名検証処理において該ディジタル署名の検証が成功したかどうかを決定することと、

該受信された公開鍵を該少なくとも１つの公開鍵のうちの１つとして該記憶装置に格納することと、

該受信された公開鍵に対応する結果を該少なくとも１つの結果のうちの１つとして該機構装置に格納することであって、該結果は、該署名検証処理において該ディジタル署名の検証が成功したかどうかを示す、ことと

を行うようにさらに構成されており、
該受信された公開鍵と同一である該公開鍵が、該記憶装置における該少なくとも１つの公開鍵のうちの１つとして格納されていると決定された場合には、
該プロセッサは、
該受信された公開鍵と同一である該公開鍵に対応する該結果を該記憶装置から検索することと、
該検索された結果が、該署名検証処理において該ディジタル署名の検証が成功したことを示すかどうかを決定することと、
該検索された結果が、該署名検証処理において該ディジタル署名の検証が成功したことを示すと決定された場合には、該ディジタル署名の検証が成功したことを示すことと
を行うようにさらに構成されている、モバイル装置。
【請求項１０】
前記署名検証処理において前記ディジタル署名の検証が成功しなかったと決定された場合には、前記プロセッサは、該ディジタル署名の検証が失敗したことを示すようにさらに構成されている、請求項９に記載のモバイル装置。
【請求項１１】
前記署名検証処理において前記ディジタル署名の検証が成功しなかったと決定され、かつ、前記検索された結果が、前記署名検証処理において前記ディジタル署名の検証が成功しなかったことを示していると決定された場合には、前記プロセッサは、該ディジタル署名の検証が失敗したことを示すようにさらに構成されている、請求項１０に記載のモバイル装置。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、一般的にｅメールメッセージのようなメッセージを処理すること、より詳細にはエンコードされたメッセージを処理することにおいて使用される証明書を確証するためのシステムおよび方法に関する。
【背景技術】
【０００２】
電子メール（「ｅメール」）メッセージは、多くの既知のプロトコルの一つを利用してエンコードされ得る。Ｓｅｃｕｒｅ Ｍｕｌｔｉｐｌｅ Ｉｎｔｅｒｎｅｔ Ｍａｉｌ Ｅｘｔｅｎｓｉｏｎｓ（「Ｓ／ＭＩＭＥ」）のように、これらのプロトコルの一部は、守秘性確保と防護とを提供するために、プライベート暗号化鍵に、および、認証と認可とを提供する情報を通信するための公開鍵基盤（ＰＫＩ）に、依存している。秘密鍵／公開鍵の対のうちの秘密鍵を利用して暗号化されたデータは、その対になって対応する公開鍵を利用することだけによって解読され得、その逆もまた然りであり得る。メッセージをエンコードすることにおいて利用される公開鍵の真正性は、証明書を使うことで確証される。特に、コンピュータ装置の利用者は、メッセージが特定の人に送られる前に、そのメッセージを暗号化したい場合、その利用者は、その人の証明書を要求する。その証明書は、通常、他の身分証明に関する情報だけでなく、その人の公開鍵をも含む。
【０００３】
証明書は、通常、認証局によって発行されるデジタル文書である。特定の公開鍵を信用するためには、通常公開鍵は、信用されている認証局、または、信用される認証局に関連した存在によって発行される必要がある。信用された認証局と発行された公開鍵との間の関係は、証明書チェーンとも呼ばれる、一連の関連された証明書によって示され得る。証明書チェーンは、証明書の妥当性を決定するために、追跡され得る。
【０００４】
通常、認証局はそれぞれの証明書において示されるように、特定の公開鍵が、目的とされる所有者に属することを確証するために、発行するそれぞれの証明書にデジタルで署名

する。証明書チェーンを作り上げることにおいて、そのチェーンの証明書におけるデジタル署名が確証される必要がある。証明書のデジタル署名の確証は、証明書を発行する認証局の公開鍵を要求するプロセスである。

【発明の開示】

【課題を解決するための手段】

【０００５】

確証のプロセスは、特に、たとえばモバイル装置等、小型のデバイス上で確証が実行される場合には、時間を要し、コストのかかるものとなる可能性がある（コンピューティングリソースの使用の点において）。複数の証明書がユーザのコンピューティング装置上で処理される場合、同一の署名が１回以上確証され得る。本発明の実施形態は、概して署名確証処理に用いられたある種の情報を、再使用のために格納することによって、署名の確証をより効率的にするシステムおよび方法に向けられている。

【０００６】

本発明の広い視野において、コンピューティング装置上において証明書上のディジタル署名を確証する方法であって、第１の証明書の発行者に関連する第１の公開鍵を用いて、ディジタル署名に対し、第１の署名確証処理を実行するステップと、第１の署名確証処理においてディジタル署名が首尾よく確証されたかどうかを決定するステップと、第１の公開鍵を記憶装置内に格納するステップと、証明書の発行者に関連する第２の公開鍵を用いて、ディジタル署名に対し、第２の署名確証処理を実行するための要求を受けるステップと、第２の公開鍵を、記憶装置内に格納された第１の公開鍵と比較し、第１および第２の公開鍵が一致するかを決定するステップと、第１の署名確証処理においてディジタル署名が首尾よく確証された場合、および比較のステップにおいて一致が決定された場合、要求への応答の際に、ディジタル署名の確証の成功を指示するステップであって、そのため署名確証処理が実行される必要のない、ステップとを包含する、署名確証方法。

【０００７】

本発明は、さらに以下の手段を提供する。

【０００８】

（項目１）

コンピューティング装置上において証明書上のディジタル署名を確証する方法であって、

該証明書の発行者に関連する第１の公開鍵を用いて、該ディジタル署名に対し、第１の署名確証処理を実行するステップと、

該第１の署名確証処理において該ディジタル署名が首尾よく確証されたかどうかを決定するステップと、

該第１の公開鍵を記憶装置内に格納するステップと、

該証明書の発行者に関連する第２の公開鍵を用いて、該ディジタル署名に対し、第２の署名確証処理を実行するための要求を受けとるステップと、

該第２の公開鍵を、該記憶装置内に格納された該第１の公開鍵と比較し、該第１および第２の公開鍵が一致するかを決定するステップと、

該第１の署名確証処理において該ディジタル署名が首尾よく確証された場合、および該比較のステップにおいて一致が決定された場合、該要求への応答の際に、該ディジタル署名の確証の成功を指示するステップであって、そのため該第２の署名確証処理が実行される必要のない、ステップと

を包含する、方法。

【０００９】

（項目２）

上記第１の署名確証処理において上記ディジタル署名が首尾よく確証された場合にのみ、上記格するステップにおいて上記記憶装置内に上記第１の公開鍵が格納される、項目１に記載の方法。

【００１０】

（項目３）
上記格納するステップが、さらに、上記第１の署名確証処理において上記ディジタル署名が首尾よく確証されたか否かを示す結果の格納することを包含し、該結果が、上記指示のステップにおいて、該第１の署名確証処理において該ディジタル署名が首尾よく確証されたか否かを決定するために用いられる、項目２に記載の方法。
【００１１】
（項目４）
上記要求への応答の際、上記指示するステップにおいて、上記第１の署名確証処理において上記ディジタル署名が首尾よく確証されなかったことが示された場合、および、上記比較のステップにおいて一致が決定された場合に、該ディジタル署名の確証の失敗を指示するステップをさらに包含する、項目３に記載の方法。
【００１２】
（項目５）
上記コンピューティング装置がモバイル装置である、項目１から４に記載の方法。
【００１３】
（項目６）
コンピューティング装置上で実行するためのソフトウェアアプリケーションであって、コンピュータ可読媒体上に格納され、項目１から５のいずれかに一項に記載された方法のステップを実行するための複数の命令を備える、ソフトウェアアプリケーション。
【００１４】
（項目７）
証明書上のディジタル署名を確証するためのシステムであって、少なくとも１つのコンピューティング装置を備え、証明書確証アプリケーションが、該少なくとも１つのコンピューティング装置のコンピューティング装置上で実行し、かつ常駐し、該証明書確証アプリケーションが、項目１から５のいずれかに一項に記載の方法のステップを実行するようにプログラムされた、システム。
【００１５】
本発明の実施形態をより良く理解するために、また、本発明がどのように実行され得るのか示すために、例示の方法によって、添付の図面を参照する。
【発明を実施するための最良の形態】
【００１６】
本発明における一部の実施形態は移動局を利用する。移動局は、他のコンピュータ装置と通信する能力を持つ高度なデータ通信能力を有する２ウェイの通信装置である。モバイル装置はまた、音声通信のための能力も含み得る。モバイル装置によって提供された機能に依存して、それはデータメッセージング装置、送受信両用小型通信機、データメッセージング能力を有する携帯電話、ワイヤレスインターネット機器、または、データ通信装置（電話機能があってもなくても）などと呼ばれ得る。モバイル装置は、受信局のネットワークを介して他の装置と通信する。
【００１７】
モバイル装置の構造および、他の装置と通信する方法を理解することにおいて、読者を助けるために、図１から図３を参照し得る。
【００１８】
最初に図１を参照し、例示的な一実施におけるモバイル装置のブロック図が１００に示される。モバイル装置１００は、多くの構成要素を含み、制御の構成要素はマイクロプロセッサ１０２である。マイクロプロセッサ１０２は、モバイル装置１００の全体にわたる動作を制御する。データおよび音声通信を含む通信機能は、通信サブシステム１０４を介して実行される。通信サブシステム１０４は、ワイヤレスネットワーク２００からメッセージを受信および送信する。この例のモバイル装置の実施において、通信サブシステム１０４は、Ｇｌｏｂａｌ Ｓｙｓｔｅｍ ｆｏｒ Ｍｏｂｉｌｅ Ｃｏｍｍｕｎｉｃａｔｉｏｎ（ＧＳＭ）およびＧｅｎｅｒａｌ Ｐａｃｋｅｔ Ｒａｄｉｏ Ｓｅｒｖｉｃｅｓ（

ＧＰＲＳ）標準にしたがって構成されている。ＧＳＭ／ＧＰＲＳワイヤレスネットワークは、世界中で利用されており、これらの標準は、Ｅｎｈａｎｃｅｄ Ｄａｔａ ＧＳＭ Ｅｎｖｉｒｏｎｍｅｎｔ（ＥＤＧＥ）およびＵｎｉｖｅｒｓａｌ Ｍｏｂｉｌｅ Ｔｅｌｅｃｏｍｍｕｎｉｃａｔｉｏｎｓ Ｓｅｒｖｉｃｅ（ＵＭＴＳ）によって、最終的には取って代わられることが期待されている。新しい標準はまだ制限されているが、それらはここで説明されるネットワークの性質と類似性を有すると信じられており、本発明は未来において発展される、他の任意のふさわしい標準にも利用することを意図されていることが、当業者によってもまた理解されている。通信サブシステム１０４とネットワーク２００とを接続するワイヤレスリンクは、一つ以上の異なるラジオ周波数（ＲＦ）チャンネルを示しており、ＧＳＭ／ＧＰＲＳ通信のために特定化された限定のプロトコルにしたがって動作する。より新しいネットワークプロトコルを有し、これらのチャンネルは、回路変換音声通信およびパケット交換データ通信の両方をサポートすることができる。

【００１９】

モバイル装置１００に関連するワイヤレスネットワークは、一実施例におけるモバイル装置１００の実行におけるＧＳＭ／ＧＰＲＳワイヤレスネットワークであるけれども、他のワイヤレスネットワークはまた、異なる実行におけるモバイル装置１００に関連させられ得る。使用され得るワイヤレスネットワークの異なるタイプは、例えば、データ中心ワイヤレスネットワーク、音声中心ワイヤレスネットワーク、および同じ物理的基地局を媒体にして音声およびデータ通信の両方をサポートすることができるデュアルモードネットワークを含む。組み合わされたデュアルモードネットワークは、符号分割多重アクセス（ＣＤＭＡ）、ＣＤＭＡ２０００ネットワーク、ＧＳＭ／ＧＰＲＳネットワーク（上述したように）、またはＥＤＧＥやＵＭＴＳのような未来の第三世代（３Ｇ）ネットワークを含み得るが、限定されるものではない。データ中心ネットワークの一部のより古い実施例は、Ｍｏｂｉｔｅｘ（登録商標）ラジオネットワークおよびＤａｔａＴＡＣ（登録商標）ラジオネットワークを含む。音声中心データネットワークのより古い実施例は、ＧＳＭのようなＰｅｒｓｏｎａｌ Ｃｏｍｍｕｎｉｃａｔｉｏｎ Ｓｙｓｔｅｍｓ（ＰＣＳ）ネットワークおよびＴｉｍｅ Ｄｉｖｉｓｉｏｎ Ｍｕｌｔｉｐｌｅ Ａｃｃｅｓｓ（ＴＤＭＡ）システムを含む。

【００２０】

マイクロプロセッサ１０２はまた、ランダムアクセスメモリ１０６、フラッシュメモリ１０８、ディスプレイ１１０、補助入力／出力（Ｉ／Ｏ）サブシステム１１２、シリアルポート１１４、キーボード１１６、スピーカ１１８、マイクロフォン１２０、近距離通信１２２、および他の装置１２４のような追加のサブシステムと相互作用する。

【００２１】

モバイル装置１００のサブシステムの一部は、通信関連機能を実行するが、他のサブシステムは、「常駐」またはデバイス上の機能を提供し得る。実施例によって、ディスプレイ１１０およびキーボード１１６は、ネットワーク２００を媒体として送信のためのテキストメッセージを入力するような通信関連機能、および計算機またはタスクリストのようなデバイス－常駐機能の両方のために利用され得る。マイクロプロセッサ１０２によって利用されるシステムソフトウェアを動作することは、通常、フラッシュメモリ１０８のような永続性記憶装置において記憶され、それは、代替的には、読み出し専用記憶装置または類似した記憶装置要素（図には示されてない）であり得る。当業者は、オペレーティングシステム、特定の装置アプリケーションまたはその一部が、ＲＡＭ１０６のような揮発性記憶装置に一時的にロードされ得る。

【００２２】

モバイル装置１００は、要求されたネットワーク登録または始動手続きが完了した後に、ネットワーク２００を媒体として通信信号を送受信し得る。ネットワークアクセスは、モバイル装置１００の加入者または利用者に関連している。加入者の身元を確証するために、モバイル装置１００は、ネットワークと通信するための加入者確証モジュールまたはＳＩＭインターフェース１２８が挿入された「ＳＩＭ」カード１２６を要求する。ＳＩＭ

１２６は、モバイル装置１００の加入者の身元を確証するため、およびモバイル装置１００をパーソナライズするために利用される従来の「スマートカード」の中の一タイプである。ＳＩＭ１２６なしでは、モバイル装置１００は、ネットワーク２００との通信において、十分に動作しない。ＳＩＭ１２６をＳＩＭインターフェース１２８に挿入することによって、加入者は、加入者用の全てのサービスにアクセスできる。サービスは、ウェッブ閲覧、ｅメール、ボイスメール、ショートメッセージサービス（ＳＭＳ）、およびマルチメディアメッセージングサービス（ＭＭＳ）などのメッセージングを含むことができる。さらに高度なサービスは、販売時点情報管理（ｐｏｉｎｔ　ｏｆ　ｓａｌｅ）、フィールドサービス（ｆｉｅｌｄ　ｓｅｒｖｉｃｅ）、および営業支援システム（ｓａｌｅｓ　ｆｏｒｃｅ　ａｕｔｏｍａｔｉｏｎ）を含む。ＳＩＭ１２６は、情報を記憶するためにプロセッサとメモリを含む。一度ＳＩＭ１２６がＳＩＭインターフェース１２８に挿入されると、それはマイクロプロセッサ１０２に結合される。加入者の身元を確証するために、ＳＩＭ１２６は、Ｉｎｔｅｒｎａｔｉｏｎａｌ　Ｍｏｂｉｌｅ　Ｓｕｂｓｃｒｉｂｅｒ　Ｉｄｅｎｔｉｔｙ（ＩＭＳＩ）のような一部の利用者パラメータを含む。ＳＩＭ１２６を利用することの利点は、加入者が任意の単一の物理的モバイル装置によっても必然的に拘束されないことである。ＳＩＭ１２６は、メモ帳（またはカレンダー）情報および最近の通話情報を含み、モバイル装置のための追加的な加入者情報もまた記憶し得る。

【００２３】

モバイル装置１００は、バッテリー電力供給装置であり、一つ以上の再充電可能なバッテリー１３０を収容するためのバッテリーインターフェース１３２を含む。バッテリーインターフェース１３２は、調整装置（図には示されていない）に結合され、それは電力Ｖ＋をモバイル装置１００に供給することでバッテリー１３０を補助する。現在の技術はバッテリーを利用するが、マイクロ燃料電池のような未来の技術は、モバイル装置１００に電力を供給し得る。

【００２４】

そのオペレーティングシステム機能に付け加えて、マイクロプロセッサ１０２は、モバイル装置１００のソフトウェアアプリケーションの実行を可能にする。データおよび音声通信アプリケーションを含み、基本装置動作を制御する一式のアプリケーションは、通常その製造過程の間に、モバイル装置１００にインストールされている。モバイル装置１００にロードされ得る他のアプリケーションは、パーソナルインフォメーションマネージャー（ＰＩＭ）である。ＰＩＭは、ｅメール、カレンダーイベント、ボイスメール、予約、タスクアイテムなど（限定されないが）のような、当該のデータアイテムを、加入者へ、組織および管理する機能を持つ。ＰＩＭアプリケーションは、ワイヤレスネットワーク２００を介して、データアイテムを送受信する能力を持つ。ＰＩＭデータアイテムは、ホストコンピュータシステムに記憶および／または関連されたモバイル装置加入者の対応するデータアイテムを有するワイヤレスネットワーク２００を介して、継ぎ目なく統合され、同期化され、またアップデートされ得る。この機能は、そのようなアイテムに関して、モバイル装置１００のミラーホストコンピュータを創る。これは、ホストコンピュータシステムがモバイル装置加入者のオフィスコンピュータシステムである場合、特に有益であり得る。

【００２５】

追加的なアプリケーションはまた、ネットワーク２００、補助Ｉ／Ｏサブシステム１１２、シリアルポート１１４、近距離通信サブシステム１２２、または任意の他の適切なサブシステム１２４を介して、モバイル装置１００にロードされ得る。アプリケーションのインストールにおけるこの柔軟性は、モバイル装置１００の機能を増加させ、強化型のデバイス上の機能、通信関連機能、または両方を提供し得る。例えば、安全な通信アプリケーションは、電子商業機能および他の経済的取引に、モバイル装置１００の使用を実行させることを可能にし得る。

【００２６】

シリアルポート１１４は、外部装置またはソフトウェアアプリケーションを介して加入

者に好みを設定させることが可能であり、ワイヤレス通信ネットワークを介するのとは異なったモバイル装置１００へ、情報またはソフトウェアのダウンロードを提供することによって、モバイル装置１００の性能を拡張する。代替的なダウンロード経路は、例えば、安全な装置通信を提供するために、直接の、信頼および信用された接続を介して、モバイル装置１００へ暗号化鍵をロードするために利用され得る。

【００２７】

近距離通信サブシステム１２２は、ネットワーク２００の利用なしで、モバイル装置１００と異なるシステムまたは装置との間に通信を提供する。例えば、サブシステム１２２は、赤外線装置、関連される回路および近距離通信の構成要素を含み得る。近距離通信の実施例は、Ｉｎｆｒａｒｅｄ　Ｄａｔａ　Ａｓｓｏｃｉａｔｉｏｎ（ＩｒＤＡ）、Ｂｌｕｅｔｏｏｔｈ（登録商標）、および、ＩＥＥＥによって開発された８０２．１１標準ファミリーを含む。

【００２８】

使用において、テキストメッセージ、ｅメールメッセージ、またはウェッブページのダウンロードなどのような受信された信号は、通信サブシステム１０４によって処理され、マイクロプロセッサ１０２へ入力される。マイクロプロセッサ１０２は、ディスプレイ１１０または代替的に、補助Ｉ／Ｏサブシステム１１２へ出力するために、受信された信号を処理する。加入者はまた、例えばディスプレイ１１０および可能ならば、補助Ｉ／Ｏサブシステム１１２に接続しているキーボード１１６を使って、ｅメールメッセージなどのデータアイテムを作成し得る。補助サブシステム１１２は、タッチスクリーン、マウス、トラックボール、赤外線指紋検出器、またはダイナミックボタンプレス能力を有するローラーウィールなどの装置を有し得る。キーボード１１６は、英数字キーボードおよび／または電話型キーパッドである。作成されたアイテムは、通信サブシステム１０４を介して、ネットワーク２００を媒体にして送信され得る。

【００２９】

音声通信にとって、モバイル装置１００の全ての動作は、受信された信号がスピーカ１１８に出力され、送信のための信号がマイクロフォン１２０によって生成されることを除いて、実質的に類似している。音声メッセージ記録サブシステムのような代替の音声または音声Ｉ／Ｏサブシステムはまた、モバイル装置１００に提供され得る。音声または音声信号出力は、第１にスピーカ１１８を介して完了されるが、ディスプレイ１１０はまた、通話者の身元確証、音声通話の継続時間、または音声通話に関連した情報などの追加的情報を提供するために利用され得る。

【００３０】

図２を参照すると、図１の通信サブシステム構成要素１０４のブロック図が示されている。通信サブシステム１０４は、受信機１５０、送信機１５２、一つ以上のはめ込みの、または内部のアンテナ要素１５４、１５６、ローカル発振器（ＬＯｓ）１５８、およびデジタル信号プロセッサ（ＤＳＰ）１６０のような処理モジュールを含む。

【００３１】

通信サブシステム１０４の特定のデザインは、モバイル装置１００が動作することを意図されているネットワーク２００に依存しており、図２で示されたデザインがほんの一実施例であることは理解されるべきである。ネットワーク２００を介してアンテナ１５４によって受信された信号は、受信機１５０に入力され、それは、信号アンプ、周波数低減変換、フィルタリング、チャンネル選択、およびアナログからデジタルへの変換（Ａ／Ｄ）などとしての通常の受信機機能を実行し得る。受信された信号のＡ／Ｄ変換は、復調およびデコーディングなどのより複雑な通信機能をＤＳＰ１６０において実行させることを許可する。類似した方法において、変調およびエンコーディングを含み、送信される信号はＤＳＰ１６０によって処理される。これらのＤＳＰ処理信号は、デジタルからアナログ（Ｄ／Ａ）変換、周波数増加変換、フィルタリング、アンプ、およびアンテナ１５６を介してネットワーク２００を媒体にした送信などのために、送信機１５２へ入力される。ＤＳＰ１６０は、通信信号を処理するだけでなく、受信機および送信機の制御も提供する。例

えば、受信機１５０および送信機１５２における通信信号に適用されたゲインは、ＤＳＰ１６０に提供された自動ゲイン制御アルゴリズムを介して適応できるように制御され得る。

【００３２】

モバイル装置１００とネットワーク２００との間のワイヤレスリンクは、一つ以上の異なるチャンネル、通常異なるＲＦチャンネル、および、モバイル装置１００とネットワーク２００との間で利用される関連されたプロトコルを含み得る。ＲＦチャンネルは、通常、全ての帯域幅における制限およびモバイル装置１００のバッテリー電力制限のために、節約されなければならない限定された資源である。

【００３３】

モバイル装置１００が十分に動作する場合、送信機１５２は、ネットワーク２００に送信している場合にのみ、通常、入力され、またはオンにされる。そうでない場合は、資源を節約するためにオフにされる。同様に、受信機１５０は、指定された時間の間に、信号または情報（仮にあるならば）を受信するために必要とされるまで、電力を節約するために定期的にオフにされる。

【００３４】

図３を参照すると、ワイヤレスネットワークのノードのブロック図が２０２として示されている。実際には、ネットワーク２００は、一つ以上のノード２０２を含む。モバイル装置１００は、ワイヤレスネットワーク２００の中で、ノード２０２と通信する。図３の実施例の実行において、ノード２０２は、Ｇｅｎｅｒａｌ Ｐａｃｋｅｔ Ｒａｄｉｏ Ｓｅｒｖｉｃｅ（ＧＰＲＳ）および、Ｇｌｏｂａｌ Ｓｙｓｔｅｍｓ ｆｏｒ Ｍｏｂｉｌｅ ｔｅｃｈｎｏｌｏｇｉｅｓ（ＧＳＭ）にしたがって構成される。ノード２０２は、関連した塔型基地局２０６を有する基地局制御装置（ＢＳＣ）２０４、ＧＳＭにおけるＧＰＲＳのサポートを追加されたパケット制御ユニット（ＰＣＵ）２０８、移動通信交換局（ＭＳＣ）２１０、Ｈｏｍｅ Ｌｏｃａｔｉｏｎ Ｒｅｇｉｓｔｅｒ（ＨＬＲ）２１２、Ｖｉｓｉｔｏｒ Ｌｏｃａｔｉｏｎ Ｒｅｇｉｓｔｒｙ（ＶＬＲ）２１４、Ｓｅｒｖｉｎｇ ＧＰＲＳ Ｓｕｐｐｏｒｔ Ｎｏｄｅ（ＳＧＳＮ）２１６、Ｇａｔｅｗａｙ ＧＰＲＳ Ｓｕｐｐｏｒｔ Ｎｏｄｅ（ＧＧＮＳ）２１８および、Ｄｙｎａｍｉｃ Ｈｏｓｔ Ｃｏｎｆｉｇｕｒａｔｉｏｎ Ｐｒｏｔｏｃｏｌ（ＤＨＣＰ）２２０を含む。構成要素のこのリストは、ＧＳＭ／ＧＰＲＳの中の全てのノード２０２の包括的なリストであることを意味しているのではなく、むしろ、ネットワーク２００を介して通信に、通常利用される構成要素のリストである。

【００３５】

ＧＳＭネットワークにおいて、ＭＳＣ２１０は、ＢＳＣ２０４および、回路交換要求を満たすための、Ｐｕｂｌｉｃ Ｓｗｉｔｃｈｅｄ Ｔｅｌｅｐｈｏｎｅ Ｎｅｔｗｏｒｋ（ＰＳＴＮ）２２２のような地上通信線ネットワークに結合される。公共またはプライベートネットワーク（インターネット）２２４（一般的に、共有されたネットワークインフラストラクチャとも呼ばれる）への、ＰＣＵ２０８、ＳＧＳＮ２１６およびＧＧＳＮ２１８を介した接続は、ＧＰＲＳの可能なモバイル装置のためのデータ経路を表している。ＧＰＲＳの能力を拡張したＧＳＭネットワークにおいて、ＢＳＣ２０４はまた、分割や無線チャンネル割り当てを制御するため、およびパケット交換要求を満たすために、ＳＧＳＮ２１６へ接続するパケット制御ユニット（ＰＣＵ）２０８を含む。モバイル装置の位置ならびに、回路交換およびパケット交換要求両方の利用を追跡するために、ＨＬＲ２１２は、ＭＳＣ２１０とＳＧＳＮ２１６との間でシェアされる。ＶＬＲ２１４へのアクセスは、ＭＳＣ２１０によって制御される。

【００３６】

基地局２０６は固定されたトランシーバー基地局である。基地局２０６およびＢＳＣ２０４はともに、固定されたトランシーバー装置を形成する。固定されたトランシーバー装置は、通常「セル」と呼ばれる特定の範囲エリアのためにワイヤレスネットワーク範囲を提供する。固定されたトランシーバー装置は、基地局２０６を介してそのセル内のモバイ

ル装置へ通信信号を送信および受信する。固定されたトランシーバー装置は通常、制御装置の制御のもとで、特定の、通常は前もって決定された通信プロトコルおよびパラメータにしたがったモバイル装置へ送信されるための信号の変調および、可能な場合、エンコードおよび／または暗号化としての機能を実行する。固定された受トランシーバー装置は同様に、必要であれば、そのセル内のモバイル装置１００から受信された任意の通信信号を復調および、可能な場合、デコードおよび／または暗号解読する。通信プロトコルおよびパラメータは、異なるノードの間で変化し得る。例えば、一つのノードは、異なる変調スキームを利用し得、他のノードとは異なる周波数にて動作し得る。

【００３７】

特定のネットワークに記録された全てのモバイル装置１００にとって、利用者のプロフィールのような恒常的な構成データは、ＨＬＲ２１２に記憶される。ＨＬＲ２１２はまた、それぞれの記録されたモバイル装置の位置情報を含み、モバイル装置の現在の位置を決定するために照会され得る。ＭＳＣ２１０は、位置エリアの集まりを監督下に置き、ＶＬＲ２１４における監督エリアにおいて、目下、モバイル装置のデータを記憶する。さらに、ＶＬＲ２１４はまた、他のネットワークを訪れているモバイル装置の情報を含む。ＶＬＲ２１４における情報は、より速いアクセスのために、ＨＬＲ２１２からＶＬＲ２１４へ送信された恒常のモバイル装置データの一部を含む。遠隔ＨＬＲ２１２ノードからＶＬＲ２１４への追加的情報を動かすことによって、これらのノード間のデータ流通量は、音声およびデータサービスがより速い応答時間、と同時により少ないコンピュータリソースの使用を要求することを提供され得るために、減少され得る。

【００３８】

ＳＧＳＮ２１６およびＧＧＳＮ２１８は、ＧＳＭ内のＧＰＲＳサポート、主にｐａｃｋｅｔ ｓｗｉｔｃｈｅｄ ｄａｔａ ｓｕｐｐｏｒｔのために追加された要素である。ＳＧＳＮ２１６およびＭＳＣ２１０は、それぞれのモバイル装置１００の位置の追跡をすることによって、ワイヤレスネットワーク２００内で、類似した責任を有する。ＳＧＳＮ２１６はまた、ネットワーク２００でのデータ流通のためのセキュリティ機能およびアクセス制御を実行する。ＧＧＳＮ２１８は、外部パケット交換ネットワークとインターネット接続し、ネットワーク２００内で操作されるインターネットプロトコル（ＩＰ）バックボーンネットワークを介して、一つ以上のＳＧＳＮ２１６に接続する。通常動作の間、所定のモバイル装置１００は、ＩＰアドレスを獲得するため、およびデータサービスにアクセスするために、「ＧＰＲＳアタッチ」を実行しなければならない。Ｉｎｔｅｇｒａｔｅｄ Ｓｅｒｖｉｃｅｓ Ｄｉｇｉｔａｌ Ｎｅｔｗｏｒｋ（ＩＳＤＮ）アドレスが、掛かってきた通話および掛けた通話をルートするために利用される場合、この要求は、回路交換音声チャンネルには存在しない。現在、全てのＧＰＲＳの可能なネットワークは、ダイナミックに、プライベートの割り当てられたＩＰアドレスを利用し、ＧＧＳＮ２１８へ接続されたＤＨＣＰサーバ２２０を要求する。Ｒｅｍｏｔｅ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｄｉａｌ－Ｉｎ Ｕｓｅｒ Ｓｅｒｖｉｃｅ（ＲＡＤＩＵＳ）サーバおよびＤＨＣＰサーバの組み合わせを利用することを含み、ダイナミックＩＰアドレス割り当てのための多くのメカニズムがある。一度、ＧＰＲＳアタッチが完了されると、論理接続は、モバイル装置１００から、ＰＣＵ２０８およびＳＧＳＮ２１６を介して、ＧＧＳＮ２１８内のアクセスポイントノード（ＡＰＮ）へ確立される。ＡＰＮは、ダイレクトインターネット互換サービスまたはプライベートネットワーク接続のどちらかにアクセスできるＩＰトンネルの論理的エンド（ｅｎｄ）を示している。ＡＰＮはまた、それぞれのモバイル装置１００が一つ以上のＡＰＮに割り当てられなければならず、および、モバイル装置１００が、利用の認可されたＡＰＮへＧＰＲＳアタッチを第１に実行せずに、データを交換しえなくなる限りにおいて、ネットワーク２００のためのセキュリティメカニズムを示している。ＡＰＮは、「ｍｙｃｏｎｎｅｃｔｉｏｎ．ｗｉｒｅｌｅｓｓ．ｃｏｍ」のような、インターネットドメイン名と類似していると考えられ得る。

【００３９】

一度ＧＰＲＳアタッチが完了すると、トンネルは創られ、ＩＰパケットにおいてサポー

トされ得る任意のプロトコルを使用した全てのデータ流通は標準ＩＰパケット内で交換される。これはバーチャルプライベートネットワーク（ＶＰＮ）を用いて利用される一部のＩＰセキュリティ（ＩＰｓｅｃ）接続においてはよくあることだが、ＩＰ　ｏｖｅｒ　ＩＰのようなトンネル方法を含む。これらのトンネルはまた、パケットデータプロトコル（ＰＤＰ）状況と呼ばれ、ネットワーク２００においては、限定された利用可能数がある。ＰＤＰ状況を最大利用するために、ネットワーク２００は、活動に欠如があるかどうかを決定するために、それぞれのＰＤＰ状況に持ち時間を与える。モバイル装置１００がそのＰＤＰ状況を利用しない場合、ＰＤＰ状況は、割り当てを取り消され得、ＩＰアドレスは、ＤＨＣＰサーバ２２０によって管理されるＩＰアドレスプールへ戻る。

【００４０】

図４を参照して、一実施例の構成におけるホストシステムの構成要素が図示されているブロック図が示されている。ホストシステム２５０は、通常、企業オフィスまたは他のローカルエリアネットワーク（ＬＡＮ）であるが、例えば、異なる実行においては、ホームオフィスコンピュータまたは一部の他のプライベートシステムでもあり得る。図４において示された実施例において、ホストシステム２５０は、モバイル装置１００のユーザが属する組織のＬＡＮとして図示されている。

【００４１】

ＬＡＮ２５０は、ＬＡＮ接続２６０によってお互いに接続された多くのネットワーク構成要素を含む。例えば、ユーザのモバイル装置１００のための付随クレイドル２６４を有するユーザのデスクトップコンピュータ２６２ａはＬＡＮ２５０に置かれる。モバイル装置１００のためのクレイドル２６４は、例えば、シリアル接続またはＵｎｉｖｅｒｓａｌ　Ｓｅｒｉａｌ　Ｂｕｓ（ＵＳＢ）接続によって、コンピュータ２６２ａに結合され得る。他のユーザコンピュータ２６２ｂはまた、ＬＡＮ２５０に置かれ、それぞれは、モバイル装置のための付随クレイドル２６４を備え得、または備え得ない。クレイドル２６４は、ユーザコンピュータ２６２ａからモバイル装置１００への情報（例えば、ＰＩＭデータ、モバイル装置１００とＬＡＮ２５０との間の安全な通信を容易にするための暗号化対称秘密鍵（ｐｒｉｖａｔｅ　ｓｙｍｍｅｔｒｉｃ　ｅｎｃｒｙｐｔｉｏｎ　ｋｅｙｓ））のロードを容易にし、モバイル装置１００の使用を初期設定することにおいて実行される、大量の情報アップデートにとって、特に有益であり得る。モバイル装置１００へダウンロードされた情報は、メッセージ交換において利用される証明書を含み得る。ユーザコンピュータ２６２ａ、２６２ｂはまた、図４にて明示的に示されてはいないが、他の周辺装置に接続されることが、当業者によって理解される。

【００４２】

さらに、ＬＡＮ２５０のネットワーク構成要素のサブセットのみが、説明のために図４において示され、ＬＡＮ２５０が、図４において明示的に示されてはいないが、この実施例の構成のために、追加の構成要素を含むことが当業者によって理解される。さらに一般的には、ＬＡＮ２５０は、この組織の、より大きなネットワーク（図示されていない）のより小さな一部を示し得、異なる構成要素を含み得、および／または、図４の実施例において示されたのとは異なるトポロジーにおいて配置され得る。

【００４３】

本実施例において、モバイル装置１００は、ワイヤレスネットワーク２００のノード２０２および、サービスプロバイダーネットワークまたはパブリックインターネットのような、共有されたネットワークインフラストラクチャ２２４を介してＬＡＮ２５０と通信する。ＬＡＮ２５０へのアクセスは、一つ以上の経路（図には示されていない）を介して提供され得、ＬＡＮ２５０のコンピュータ装置は、ファイアウォールの後ろから、またはプロキシサーバ２６６から、動作し得る。

【００４４】

異なる実行において、ＬＡＮ２５０は、ＬＡＮ２５０とモバイル装置１００との間のデータ交換を容易にするために、ワイヤレスＶＰＮルータ（図には示されていない）を含む。ワイヤレスＶＰＮルータのコンセプトは、ワイヤレス産業においては新しく、ＶＰＮ接

続は、特定のワイヤレスネットワークを介してモバイル装置１００へ、直接に確立され得ることを意味する。ワイヤレスＶＰＮルータの使用の見込みは、最近になりようやく利用可能となり、新しいインターネットプロトコル（ＩＰ）バージョン６（ＩＰＶ６）がＩＰベースのワイヤレスネットワークに届く場合に、利用され得ている。この新しいプロトコルは、ＩＰアドレスを全てのモバイル装置に与えるために、十分なＩＰアドレスを提供し、いつでもモバイル装置へ情報を送ることを可能にさせる。ワイヤレスＶＰＮルータを使用することの利点は、規格品のＶＰＮ構成要素であり得、使用される分離ワイヤレスゲートウェイおよび分離ワイヤレスインフラストラクチャを要求しない。ＶＰＮ接続は、この異なる実行において、モバイル装置１００へ直接にメッセージを運ぶために、好ましくはトランスミッションコントロールプロトコル（ＴＣＰ）／ＩＰ、またはユーザデータグラムプロトコル（ＵＤＰ）／ＩＰ接続である。

【００４５】

モバイル装置１００のユーザのために意図されたメッセージは、ＬＡＮ２５０のメッセージサーバ２６８によって最初に受信される。そのようなメッセージは、多数のソースの中の任意のソースから始まり得る。例えば、メッセージは、供給されたネットワークインフラストラクチャ２２４を介して、ワイヤレスネットワーク２００または異なるワイヤレスネットワークに接続された異なるモバイル装置から（図には示されていない）、あるいは、異なるコンピュータ装置またはメッセージ送信可能な他の装置から、および可能な場合、例えば、アプリケーションサービスプロバイダ（ＡＳＰ）またはインターネットサービスプロバイダ（ＩＳＰ）を介して、ＬＡＮ２５０内のコンピュータ２６２ｂから送信者によって送信され得る。

【００４６】

メッセージサーバ２６８は通常、組織内および共有されたネットワークインフラストラクチャ２２４へ、メッセージ交換、特にｅメールメッセージ交換のために、第１インターフェースとしてアクトする。メッセージを送受信するためにセットアップされている組織におけるそれぞれのユーザは、通常、メッセージサーバ２６８によって管理されるユーザアカウントに関連される。メッセージサーバ２６８の一実施例は、Ｍｉｃｒｏｓｏｆｔ Ｅｘｃｈａｎｇｅ（登録商標）サーバである。一部の実行において、ＬＡＮは、マルチプルメッセージサーバ２６８を含み得る。メッセージサーバ２６８はまた、例えばカレンダーやタスクリストと関連させられたデータの管理を含み、メッセージ管理の範囲を超えて、追加的機能を提供するために適合され得る。

【００４７】

メッセージがメッセージサーバ２６８によって受信された場合、それらは通常、メッセージ記憶装置に記憶され得、メッセージはその後、引き出され得、利用者に運ばれ得る。例えば、ユーザのコンピュータ２６２ａにあるｅメールクライアントアプリケーションオペレーティングは、メッセージサーバ２６８に記憶されたそのユーザアカウントに関連されたｅメールメッセージを要求し得る。これらのメッセージは、通常、メッセージサーバ２６８から引き出され、コンピュータ２６２ａに局地的に記憶される。

【００４８】

モバイル装置１００を動作する場合、ユーザは、ｅメールメッセージを持ち運びのために、ハンドヘルドから引き出されることを望み得る。モバイル装置１００上で動作するｅメールクライアントアプリケーションはまた、メッセージサーバ２６８からのユーザアカウントに関連されたメッセージを要求し得る。ｅメールクライアントは、（ユーザによって、または管理者によって、可能な場合、組織の情報技術（ＩＴ）ポリシーにしたがい）ユーザの指令で、一部の所定の定義された時間間隔で、または一部の所定の定義され得たイベントの発生にて、この要求をするために設定され得る。一部の実行において、モバイル装置１００は、それ自身のｅメールアドレスを割り当てられ、特にモバイル装置１００へアドレスされたメッセージは、メッセージサーバ２６８によってそれらが受信されるように、自動的にモバイル装置１００にリダイレクトさせる。

【００４９】

モバイル装置１００とＬＡＮ２５０との間のメッセージのワイヤレス通信およびメッセージに関連されたデータを容易にするために、多くのワイヤレス通信のサポート構成要素２７０は提供され得る。本実施例の実行において、ワイヤレス通信をサポートする構成要素２７０は、例えば、メッセージ管理サーバ２７２を含む。メッセージ管理サーバ２７２は、特に、モバイル装置によって扱われるｅメールメッセージのようなメッセージの管理のためのサポートを提供するために利用される。一般には、メッセージはメッセージサーバ２６８に記憶される一方で、メッセージ管理サーバ２７２は、メッセージがモバイル装置１００へ、いつ、どのように、および、送られるべきかどうかを制御するために利用され得る。メッセージ管理サーバ２７２はまた、モバイル装置１００で作成されたメッセージの扱いを容易にし、次の送達のためにメッセージサーバ２６８へ送られる。

【００５０】

例えば、メッセージサーバ２７２は、新しいｅメールメッセージのために、ユーザの「メールボックス」（例えば、メッセージサーバ２６８のユーザアカウントに関連されたメッセージ記憶装置など）を監視し得、メッセージがユーザのモバイル装置１００へ、どのように、および、中継されるかどうかを決定するために、ユーザが定義可能なフィルタを新しいメッセージに適用し得、新しいメッセージを圧縮および暗号化（例えば、データ暗号か標準（ＤＥＳ）またはトリプルＤＥＳ）し得、共有されたネットワークインフラストラクチャ２２４およびワイヤレスネットワーク２００を介して、モバイル装置１００へそれらをプッシュし得、モバイル装置１００で作成されたメッセージ（例えば、トリプルＤＥＳを使って暗号化された）を受信し得、作成されたメッセージが解読および解凍され得、それらのメッセージがユーザコンピュータ２６２ａから来ているように所望される場合に、作成されたメッセージを再フォーマットし得、送達のためにメッセージサーバ２６８へ作成されたメッセージを再ルートし得る。

【００５１】

モバイル装置１００から送信、および／または、受信されるメッセージに関連された属性または規制は、メッセージ管理サーバ２７２によって定義および強化（ＩＴポリシーにしたがった管理者によって）され得る。これらは、モバイル装置１００が、最小の暗号化鍵サイズで暗号化された、および／または署名されたメッセージ、を受信し得るかどうか、送信メッセージが暗号化、および／または署名されなければならないかどうか、および、モバイル装置１００から送られた全ての安全なメッセージのコピーが例えば、所定のコピーアドレスへ送られたかどうかを含み得る。

【００５２】

メッセージ管理サーバ２７２はまた、メッセージ情報、またはメッセージサーバ２６８に記憶されたメッセージの所定の一部（例えば、ブロックなど）をモバイル装置１００にプッシュするなどように、他の制御機能を提供するために適用され得る。例えば、メッセージが、メッセージサーバ２６８からモバイル装置１００によって最初に引き出される場合、メッセージ管理サーバ２７２は、所定のサイズ（例えば２ＫＢ）の一部を有し、メッセージの最初の一部だけをモバイル装置１００へプッシュするために適用される。モバイル装置１００へ、メッセージ管理サーバ２７２によって同様なサイズのブロックにて送られるため、ユーザはそれゆえ、可能な場合、最大の所定のメッセージサイズまで、メッセージの多くを要求することができる。

【００５３】

したがって、メッセージ管理サーバ２７２は、モバイル装置１００に通信されるデータのタイプおよびデータ量に対してより良い制御を容易にし、帯域幅の潜在的な無駄または他のリソースを最小限にすることを助けることができる。

【００５４】

メッセージ管理サーバ２７２は、ＬＡＮ２５０または他のネットワークにおける分離した物理サーバにおいて実行される必要がないことは、当業者によって理解される。例えば、メッセージ管理サーバ２７２に関連された機能の一部または全ては、メッセージサーバ２６８またはＬＡＮ２５０における一部の他のサーバに統合され得る。そのうえ、ＬＡＮ

２５０は、特に多数のモバイル装置がサポートされる必要がある場合の異なった実行において、多数のメッセージ管理サーバ２７２を含み得る。

【００５５】

本発明の実施形態は一般に、暗号化され、および／または署名される例えばｅメールメッセージのように、エンコードされたメッセージの処理において使用される証明書に関する。ＳＭＴＰ（Ｓｉｍｐｌｅ Ｍａｉｌ Ｔｒａｎｓｆｅｒ Ｐｒｏｔｏｃｏｌ）、ＲＦＣ８８２ヘッダ、およびＭＩＭＥ（Ｍｕｌｔｉｐｕｒｐｏｓｅ Ｉｎｔｅｒｎｅｔ Ｍａｉｌ Ｅｘｔｅｎｓｉｏｎｓ）の本体部分は、エンコードを必要としない一般的なｅメールのフォーマットを定義するために利用され得る一方で、ＭＩＭＥプロトコルの一バージョンであるＳ／ＭＩＭＥ（Ｓｅｃｕｒｅ／ＭＩＭＥ）は、（例えば、安全なメッセージングアプリケーションにおいて）、エンコードされたメッセージの通信において利用され得る。Ｓ／ＭＩＭＥは終端間（ｅｎｄ－ｔｏ－ｅｎｄ）の認証および守秘性確保を可能とし、メッセージの受信者によってデコードされ読まれるまで、メッセージの作成者がメッセージを送信する時点からデータの防護およびプライバシーを保護する。他の既知の標準およびプロトコルは、Ｐｒｅｔｔｙ Ｇｏｏｄ Ｐｒｉｖａｃｙ（登録商標）（ＰＧＰ）、ＯｐｅｎＰＧＰ、および技術的に既知の他のものなどのように、安全なメッセージ通信を容易にするために利用され得る。

【００５６】

Ｓ／ＭＩＭＥのような安全なメッセージングプロトコルは、守秘性確保および防護を提供するために、および、公開鍵インフラストラクチャ（ＰＫＩ）上で、認証および認可を提供する情報を通信するために、公開鍵および秘密暗号鍵に依存している。公開鍵／秘密鍵のペアのうちの秘密鍵を使用して暗号化されたデータは、そのペアのうちの対応する公開鍵を使用することでのみ解読され得、その逆もまた然りである。秘密鍵情報は、決して公開されないが、公開鍵情報は共有される。

【００５７】

例えば、送信者がメッセージを暗号化された形式において受信者に送りたい場合、受信者の公開鍵は、メッセージを暗号化するために利用され、次いで、受信者の秘密鍵を使用することによってのみ解読され得る。代替的に、一部のエンコード技術において、一度限りのセッション鍵は、通常、対称暗号化技術を用いて（例えば、Ｔｒｉｐｌｅ ＤＥＳ）、メッセージの本体を暗号化するために作られ、利用される。セッション鍵は、次いで、受信者の公開鍵を使用することで暗号化され（例えば、ＲＳＡのような公開鍵暗号化アルゴリズムを用いて）、次いで、受信者の秘密鍵を使用することによってのみ、解読され得る。解読されたセッション鍵は、メッセージの本体を解読するために使用され得る。メッセージのヘッダは、メッセージを解読するために使用されなければならない特定の解読スキームを特定するために利用され得る。公開鍵暗号化に基づいた他の暗号化技術は、異なる実行において利用され得る。しかしながら、これらの各場合において、受信者の秘密鍵のみが、そのメッセージの解読を容易にするために利用され得、この方法において、メッセージの守秘性確保が維持され得る。

【００５８】

さらなる実施例として、送信者が、デジタル署名を利用するメッセージに署名し得る。デジタル署名は、送信者の秘密鍵を使用することで暗号化されるメッセージのダイジェスト（例えば、メッセージのハッシュなど）であり、送信されるメッセージへ添付され得る。受信された場合にメッセージのデジタル署名を確証するために、受信者は、受信されたメッセージのダイジェストを得るための（例えば、同じ標準ハッシュアルゴリズムを使って）、送信者と同じ技術を使用する。受信者もまた、受信されたメッセージのためのダイジェストと一致するものを得るために、デジタル署名を解読するための送信者の公開鍵を使用する。受信されたメッセージのダイジェストが一致しない場合、メッセージのコンテンツが運ばれる間に変化されたか、および／または、メッセージが、公開鍵が確証のために使用された送信者から来たものではなかったかのどちらかであることを示す。デジタル署名アルゴリズムは、送信者の秘密鍵の知識を有する者のみが、受信者が送信者の公開鍵

を使用することで正しくデコードする署名をエンコードすることが可能となるべきであるようにデザインされている。それゆえ、この方法において、デジタル署名を確証することによって、送信者の認証およびメッセージ防護が維持され得る。

【００５９】

エンコードされたメッセージは、暗号化され、署名され、または、暗号化および署名の両方をされ得る。これらの動作において使用される公開鍵の真正性は、証明書を使用することで、確証される。証明書は、認証局（ＣＡ）によって発行されたデジタル文書である。証明書は、ユーザおよびユーザの公開鍵との間の関連を認証するために利用され、主として、ユーザの公開鍵の真正性における信用の水準を提供する。証明書は、通常、容認された標準（例えば、Ｘ．５０９）にしたがってフォーマットされた証明書のコンテンツを有し、証明書所持者についての情報を含む。

【００６０】

図５において、証明書チェーン３００の実施例が示される。「Ｊｏｈｎ　Ｓｍｉｔｈ」へ発行された証明書３１０は、個々人に発行された証明書の実施例であり、エンドエンティティ証明書と呼ばれ得る。エンドエンティティ証明書３１０は、通常、証明書保持者３１２（例えば、本実施例におけるＪｏｈｎ　Ｓｍｉｔｈ）および証明書３１４の発行者を識別し、発行者３１６および証明書保持者の公開鍵３１８のデジタル署名を含む。証明書３１０はまた、通常、他の情報および、証明書所持者を識別する属性（例えば、ｅメールメッセージ、組織名、組織単位名、位置など）を含む。個人が受信者に送られるメッセージを作成する場合、メッセージとともにその個人の証明書３１０を含むことは習慣的である。

【００６１】

信用される公開鍵にとって、それを発行する組織が信用されなければならない。信用されたＣＡとユーザの公開鍵との間の関係は、証明書チェーンとも呼ばれる一連の関連された証明書によって示されることができる。

【００６２】

例えば、図５に示された本実施例の証明書チェーン３００において、Ｊｏｈｎ　Ｓｍｉｔｈによって送信を意図されたメッセージの受信者は、受信されるメッセージに添付された証明書３１０の信用状態を確証することを望み得る。例えば、受信者のコンピュータ装置（例えば、図４のコンピュータ２６２ａ）上の証明書３１０の信用状態を確証するためには、発行者ＡＢＣの証明書３２０が得られ、証明書３１０が発行者ＡＢＣによって署名されたことを確証するために使用され得る。証明書３２０は既に、コンピュータ装置上の証明書記憶装置において記憶され得、または、証明書ソース（例えば、図４のＬＤＡＰサーバ２８４、または、一部の他の公開または秘密ＬＤＡＰサーバなど）から引き出される必要があり得る。証明書３２０が既に受信者のコンピュータ装置に記憶され、証明書が受信者によって信用されたと指示があった場合、証明書３１０は、それが記憶され、信用された証明書へチェーンされるゆえに、信用されたと考えられる。

【００６３】

しかしながら、図５における本実施例において、証明書３３０はまた、証明書３１０の信用状態を確証することが要求される。証明書３３０は、自署名であり、および、ルート証明書と呼ばれる。したがって、証明書３２０は、証明書チェーン３００における「中間証明書」と呼ばれ得る。ルート証明書へのチェーンが特定およびエンティティ証明書のために決定され得ることを想定し、ルート証明書への任意の所定の証明書チェーンは、ゼロ、一つ、または複数の中間証明書を含み得る。証明書３３０は、信用されたソース（例えば、ＶｅｒｉｓｉｇｎまたはＥｎｔｒｕｓｔのようなより大きな認証局から）によって発行されたルート証明書であり、証明書３１０は、それが信用された証明書へチェーンするゆえに、信用されると考えられる。その意味は、メッセージの送信者および受信者の両方が、ルート証明書３３０のソースを信用するということである。証明書が信用された証明書へチェーンされ得ない場合、その証明書は、「信用されない」と考えられ得る。

【００６４】

証明書サーバは、証明書および、無効にされた証明書を識別するリストについての情報を記憶する。これらの証明書サーバは、証明書を得るために、ならびに、証明書の真正性および無効状態を確証するために、アクセスされ得る。例えば、Ｌｉｇｈｔｗｅｉｇｈｔ Ｄｉｒｅｃｔｏｒｙ Ａｃｃｅｓｓ Ｐｒｏｔｏｃｏｌ（ＬＤＡＰ）サーバは、証明書を得るために使用され得るし、Ｏｎｌｉｎｅ Ｃｅｒｔｉｆｉｃａｔｅ Ｓｔａｔｕｓ Ｐｒｏｔｏｃｏｌ（ＯＣＳＰ）サーバは、証明書の無効状態を確証するために使用され得る。

【００６５】

標準のｅメールセキュリティプロトコルは、通常、モバイル型ではないコンピュータ装置（例えば、図４のコンピュータ２６２ａ、２６２ｂ、遠隔のデスクトップ装置など）との間の安全なメッセージ伝送を容易にする。図４を再び参照し、送信者から受信された署名されたメッセージがモバイル装置１００から読まれ得、暗号化されたメッセージがそれらの送信者に送信され得るために、モバイル装置１００は、証明書および他の個人の関連された公開鍵を記憶するために適応される。ユーザのコンピュータ２６２ａ上に記憶された証明書は、例えば、通常、コンピュータ２６２ａからモバイル装置１００へ、クレイドル２６４を介して、ダウンロードされる。

【００６６】

コンピュータ２６２ａ上に記憶され、および、モバイル装置１００へダウンロードされた証明書は、個人に関連された証明書に限定されないが、例えば、ＣＡで発行された証明書もまた含み得る。コンピュータ２６２ａおよび／またはモバイル装置１００において記憶された証明書はまた、ユーザによって、「信用された」と明示的に示され得る。したがって、証明書が、ユーザまたはモバイル装置１００によって受信された場合、証明書と、モバイル装置１００上に記憶され、信用されたと示されるもの、または、そうでなければ、信用された証明書へチェーンされることが決定されたものとを一致させることによって、モバイル装置１００上で確証され得る。

【００６７】

モバイル装置１００はまた、モバイル装置１００のユーザが、モバイル装置１００にて作成された送信されるメッセージに署名し、および、ユーザの公開鍵を用いて暗号化され、ユーザに送信されたメッセージを解読するように、ユーザに関連された公開鍵／秘密鍵のペアのうちの秘密鍵を記憶するために適応され得る。秘密鍵は、例えば、ユーザのコンピュータ２６２ａから、クレイドル２６４を介して、モバイル装置１００へダウンロードされ得る。秘密鍵は、ユーザがメッセージにアクセスするための一つの識別および一つの方法を共有し得るように、コンピュータ２６２ａとモバイル装置１００との間において、好ましく交換される。

【００６８】

ユーザコンピュータ２６２ａ、２６２ｂは、２６２ａ、２６２ｂおよび／またはモバイル装置（例えば、モバイル装置１００）上でのストレージのために、多くのソースから証明書を得ることが出来る。これらの証明書ソースは、秘密（例えば、組織内で使用のために専念される）または公開であり得、局地的または遠隔的に存在し得、例えば、組織のプライベートネットワーク内から、またはインターネットを介して、アクセスすることが可能であり得る。図４において示された本実施例において、組織に関連された複数のＰＫＩサーバ２８０は、ＬＡＮ２５０に存在する。ＰＫＩサーバ２８０は、発行する証明書のためのＣＡサーバ２８２、証明書を検索し、ダウンロードするために使用されるＬＤＡＰサーバ２８４、証明書の無効状態を確証するために使用されるＯＣＳＰサーバ２８６を含む。

【００６９】

証明書は、例えば、クレイドル２６４を介してモバイル装置１００へダウンロードされるために、ユーザのコンピュータ２６２ａによってＬＤＡＰサーバ２８４から引き出され得る。しかしながら、異なる実施形態において、ＬＤＡＰサーバ２８４は、モバイル装置１００によって直接に（例えば、この文脈においては、「放送で（ｏｖｅｒ ａｉｒ）」

）アクセスされ得、モバイル装置１００は、モバイルデータサーバ２８８を介して、個々の証明書を検索し得、および引き出し得る。同様に、モバイルデータサーバ２８８は、ＯＣＳＰサーバ２８６を直接クエリすることをモバイル装置１００に許可するために、適応され得、証明書の無効状態を確証し得る。

【００７０】

異なる実施形態において、選択されたＰＫＩサーバ２８０のみが、モバイル装置にアクセス可能（例えば、証明書の無効状態をモバイル装置１００から照合されることを許可する一方で、証明書に、ユーザのコンピュータ２６２ａ、２６２ｂからのみダウンロードさせることを許可する）とされ得る。

【００７１】

異なる実施形態において、ＰＫＩサーバ２８０は、特定のユーザ（ＩＴ管理者によって特定されるように、可能な場合、例えば、ＩＴポリシーにしたがって）に登録されたモバイル装置のみにアクセス可能にされ得る。

【００７２】

証明書の他のソース（図には示されていない）は、例えば、Ｗｉｎｄｏｗｓ（登録商標）、ＬＡＮ２５０上または外の他の安全な証明書、および、スマートカード（ｓｍａｒｔ　ｃａｒｄ）などを含み得る。

【００７３】

ここで図６を参照すると、メッセージサーバ（たとえば図４のメッセージサーバ２６８）によって受信され得る、暗号化されたメッセージの一例の構成要素を図示するブロック図が、全体で３５０として示されている。暗号化されたメッセージ３５０は一般的に、以下のうち１つ以上を含む。ヘッダ部分３５２、暗号化された本文部分３５４、随意的に１つ以上の暗号化された添付物、１つ以上の暗号化されたセッション鍵３５８、そして署名および署名に関連する情報３６０である。たとえば、ヘッダ部分３５２は一般的に、”Ｔｏ”、”Ｆｒｏｍ”、および”ＣＣ”等のアドレス情報を含み、また、たとえばメッセージ長指示子および送信者の暗号、署名スキーム識別子などを含んでもよい。実際のメッセージの内容は、通常メッセージ本文またはデータ部分３５４と、場合によっては１つ以上の添付物３５６とを含み、これは送信者の使用するセッション鍵によって暗号化され得る。セッション鍵が用いられた場合、一般的には、セッション鍵は意図された受取人に対して、各自のための公開鍵を用いて暗号化されており、メッセージ中の３５８に含まれる。メッセージが署名されたものであれば、署名および署名に関連する情報も含まれる。これには、たとえば送信者の証明書が含まれる。

【００７４】

図６中に示したような、暗号化されたメッセージのフォーマットは、例示のみによって与えられるものとする。また、他のフォーマットにおいても暗号化されたメッセージが存在し得ることは、当業者であれば理解できよう。たとえば、用いられた特定のメッセージスキームに従って、暗号化されたメッセージの構成要素は図６に示されるものとは異なる順序で現れることもあり、暗号化されたメッセージは、構成要素がより少ないか、さらなる構成要素を含むか、または異なる構成要素を含むことが可能であり、これは暗号化されたメッセージが暗号化されているか、署名されているか、またはその両方かどうかによる。

【００７５】

本発明の実施形態は、概して、署名の認証作業に利用したある種の情報を再使用のために格納することによって、証明書上のディジタル署名をさらに効率的に認証できるようにするシステムおよび方法に向けられたものである。証明書のチェーン（図５の例において論じる）を構築する際、証明書上のディジタル署名が認証されていることが必要であることが多い。多数の証明書がユーザのコンピューティング装置上で処理される場合、同一のディジタル署名は２つ以上の認証を受けなければならない。このことは、特に、クロス証明書を含む証明書チェーンが形成されている場合に有効となり得る。クロス証明書については、図７Ｂを参照して以下でさらに詳細に論じる。

【００７６】
まず図７Ａを参照すると、２例の証明書チェーンのブロック図が示されている。２例の証明書チェーンは、全体で４００ａおよび４００ｂとして図示されている。証明書チェーン４００ａおよび４００ｂが例として挙げられているということは、当業者であれば理解できよう。詳細には、証明書チェーンは図示した例の中に描かれているものよりも少数あるいは多数の証明書を含み得る。
【００７７】
多数の組織が、独自の組織内の個人に対して厳密に証明書を発行するＣＡを設けている。個々の組織内の個人に対して発行されるエンドエンティティ証明書は、その組織と提携している１つのＣＡによって発行される必要はない。エンドエンティティ証明書は、ルートＣＡを筆頭とする、組織用のＣＡ階層内の、従属する、または中間の複数のＣＡのうちの１つによって発行されることが多い。このルートＣＡは自署されたルート証明書を発行することができ、これは「トラストアンカー」、つまり組織内で発行された証明書を確証するための開始点として用いられる。
【００７８】
証明書チェーン４００ａは、組織「ＡＢＣ」内の１個人「ユーザ１」に対して発行された証明書４０２ａを確証するために形成された１例の証明書チェーンを説明する。証明書４０２ａは、組織のルートＣＡによって中間ＣＡへ発行された中間証明書４０６ａを介し、自署ルート証明書４０４ａと連結する。自署ルート証明書４０４ａは組織のルートＣＡによって発行され、なおかつユーザ１によって信用されている。組織ＡＢＣ内で発行された証明書は、たとえば、組織が管理するＬＤＡＰサーバ（たとえば図４のＬＤＡＰサーバ２８４）から検索したり引き出したりすることができる。
【００７９】
同様に、証明書チェーン４００ｂは、別の組織「ＸＹＺ」内の１個人「ユーザ２」に対して発行された証明書４０２ｂを確証するために形成された１例の証明書のチェーンを説明する。証明書４０２ｂは、中間証明書４０６ｂを介し、自署ルート証明書４０４ｂと連結する。自署ルート証明書４０４ｂは組織ＸＹＺのルートＣＡによって発行され、なおかつユーザ２によって信用されている。組織ＸＹＺ内で発行された証明書は、たとえば、組織ＸＹＺが管理するＬＤＡＰサーバから検索したり引き出したりすることができる。
【００８０】
組織ＡＢＣのユーザ１が組織ＸＹＺのユーザ２から暗号化されたメッセージを受け取った場合という状況例を考慮されたい。ユーザ２が自分の証明書４０２ｂをメッセージに添付していても、ユーザ１にはその証明書のみを用いてユーザ２の証明書４０２ｂの信用状態を確証することは不可能であろう。（まだ、ユーザ１はユーザ２の証明書４０２ｂを格納し信用されるものとしてマークしていないものと仮定する。）ユーザ１が組織ＸＹＺからの証明書を信用しない場合、この証明書は信用されている証明書と連結しないため、ユーザ２の証明書４０２ｂは確証され得ない。
【００８１】
異なる組織のユーザ間での安全なコミュニケーションを可能にするためには、証明書が組織間で使用でき、信用できることが望ましい。クロス証明書として知られる認証方法は、一方の組織のＣＡが他方の組織のＣＡを証明いしている場合に、２つの組織間で実行できる。
【００８２】
クロス証明書という用語は、広く２つの処理について言うときに使用され得る。第１の処理は、一般には実行頻度が比較的低く、クロス証明書と呼ばれる証明書の中に一方のＣＡが他方のＣＡの公開鍵を署名することを通じて２つのＣＡ間（たとえば組織間または同一組織内）に信頼関係を確立することに関連する。第２の処理は、一般には実行頻度が比較的高く、このようなクロス証明書を少なくとも１つ含む証明書チェーンを構築することを通じてユーザ証明書を確証することを含む。
【００８３】

ここで図７Ｂを参照すると、２例の証明書チェーンを連結するクロス証明書を図示したブロック図が示されている。組織ＸＹＺのルートＣＡが組織ＡＢＣのルートＣＡに対して発行したクロス証明書４１０を本例において示す。同様に、組織ＡＢＣのルートＣＡが組織ＸＹＺのルートＣＡに対して発行したクロス証明書４１２を示す。

【００８４】

図７Ｂの例は、２つのＣＡ間における相互のクロス証明を説明する。ただし、様々な実行において他のクロス証明の方法が可能である。たとえば、クロス証明書は１つの組織内の従属するＣＡによって別の組織のルートＣＡに対して発行されてもよい。さらなる例として、第１の組織に対して第２の組織によってクロス証明書を発行し返さなくても、第１の組織のＣＡが第２の組織のＣＡに対してクロス証明書を発行してよい。

【００８５】

さらに、たとえば組織のＩＴ方針規定によって、組織間の証明書の使用が制限されることがある。たとえば、他の組織からの証明書は暗号化されたｅメールメッセージを処理する目的でのみ信用される、というふうにある組織のＩＴ方針が規定していることがある。また、一方の発行ＣＡがクロス証明書を取消し、他の組織との信頼関係を終結させることもできる。このことによって、異なる組織の個人間における安全なｅメールコミュニケーションをさらに効率的に管理することが可能になる。

【００８６】

クロス証明書によって信頼関係を確立した組織の個人間における安全なコミュニケーションが可能である。組織ＡＢＣのユーザ１が、暗号化されたメッセージを組織ＸＹＺのユーザ２から受け取った場合の状況を再度考慮されたい。ユーザ１は、ユーザ２の証明書４０２ｂのチェーン内にある証明書を引出し、ユーザ１の組織のルートＣＡによって発行され、なおかつユーザ１の信用する証明書４０４ａを探し出すことによって、ユーザ２の証明書４０２ｂの信用状態を確証することができるであろう。厳密に言えば、図７Ｂの例に示すように、チェーンにはＡＢＣのルート証明書４０４ａと、クロス証明書４１２と、ＸＹＺのルート証明書４０４ｂと、中間証明書４０６ｂと、ユーザ２の証明書４０２ｂとが含まれる。

【００８７】

ユーザ１がユーザ２の証明書４０２ｂの信用状態を確証するには、ユーザ１は証明書４０２ｂを入手しなければならない。この証明書は、ユーザ２からユーザ１へのメッセージに関連するのが慣習である。ただし、証明書４０２ｂが与えられておらず、また、ユーザ１のコンピューティングディバイスにも特に格納されていない場合には、たとえば組織ＸＹＺの管理するＬＤＡＰまたは他の証明書サーバからそれを引出さなければならない。さらに、証明書４０２ｂの信用状態を確証するために、チェーン内に残っている各証明書も引出さなければならない。チェーン内にあるそれ以外の証明書、本例においてはルート証明書およびクロス証明書を含むが、それらをＡＢＣのＬＤＡＰサーバ、ＸＹＺのＬＤＡＰサーバ、またはユーザ１にアクセス可能なその他のＬＤＡＰサーバから引出す必要があろう。

【００８８】

図５、図７Ａ、および図７Ｂを参照して論じたように、証明書チェーンを構築する際には、証明書上に発行ＣＡのディジタル署名が必要であることが多い。証明書を確証する際には、たとえば証明書の日付が有効であることの確証、または、組織がＩＴ方針に従って設け得るその他の基準が有効であることの確証等、他のタスクが実行されることもある。

【００８９】

証明書上のディジタル署名の確証は、発行ＣＡの公開鍵を必要とするプロセスである。ＣＡが証明書にディジタル署名をする場合、たとえば証明書の所持者の氏名や公開鍵を含む証明書情報、またはハッシュアルゴリズムの実行を介して得たこのような情報のハッシュは、一般的にそのＣＡの秘密鍵を用いて暗号化される。発行ＣＡが証明書に署名するために用いるアルゴリズムは、一般的に証明書中で識別される。したがって、公開鍵を用いて暗号化された情報またはハッシュを復号し、結果を予測される証明書情報またはそのハ

ッシュとそれぞれ比較することによって、ユーザが署名した、メッセージのディジタル署名を確証する際に用いたのと類似の方法で証明書上のＣＡのディジタル署名を確証することができる。それらの一致に成功すれば、証明書の所持者の公開鍵を証明書の所持者と正当に結びつけてよいということをＣＡが証明したということであり、ＣＡが信用されていれば証明書の所持者の公開鍵は信用できるという意味である。

【００９０】

証明書の署名の確証は、特に、モバイル装置等の小型のデバイス上で実行される場合には、時間を要し、コストもかかるプロセスとなる可能性がある（コンピューティングリソースの使用の点において）。本発明の実施形態は、概して、署名の確証処理に用いられたある種の情報を再使用のために格納することによって、証明書上のディジタル署名をより効率的に確証することができるようなシステムおよび方法に向けられている。

【００９１】

少なくとも１つの実施形態において、独自の証明書を発行したＣＡの公開鍵が１つ以上、証明書と結び付けられ、キャッシュまたは格納される。上記したように、ＣＡによって署名された証明書上のディジタル署名を確証しようと試みる際には、そのＣＡの公開鍵が必要である。ただし、同一のＣＡに属すると思われる複数の証明書（それぞれ、添付の公開鍵をもつ）が存在し得る。この状況は、たとえば、何通かの証明書が同一または類似のサブジェクトデータ（すなわち、証明書の所持者を識別する証明書データである）を有する場合、またはＣＡが複数の公開鍵（そのうちのいくつかはもはや有効でない）を発行している場合に起こり得る。したがって、個々の公開鍵のいずれが個々の証明書を確証するのに有効に使用されたか、追跡することは有益となり得る。

【００９２】

図８を参照すると、本発明の一実施形態中の、証明書上のディジタル署名を確証する方法におけるステップを図示するフローチャートが示されている。

【００９３】

本発明の１つの実施形態において、方法のステップのうち少なくともいくつかは、モバイル装置上で実行し常駐する証明書確証アプリケーションによって実行される。様々な実施形態において、証明書確証アプリケーションはモバイル装置以外のコンピューティング装置上で実行し常駐することができる。さらに、証明書確証アプリケーションは、独立型のアプリケーションである必要はなく、証明書確証アプリケーションの機能性は、モバイルまたは他のコンピューティング装置上で実行し常駐する１つ以上のアプリケーション内でも実行される。

【００９４】

一般的に、方法４２０において、与えられた公開鍵が証明書上のディジタル署名の確証に有効に使用される場合、その公開鍵の複製がキャッシュに格納されるか、そうでなければ記憶装置内に格納される。たとえば公開鍵は、証明書に関連する証明書データと共に、または、有効な証明書確証に使用された公開鍵を格納するのに適した独立型の記憶装置（たとえばｌｏｏｋｕｐ　ｔａｂｌｅ）に格納できる。次に同一の証明書上のディジタル署名を確証する試行が為された場合には、少なくとも公開鍵を用いていくつかのデータを復号する必要のある高価な署名確証処理を即座に実行するよりも、代わりに再度ディジタル署名を確証するのに使用されるであろう公開鍵を、格納されている公開鍵と初めに比較するのがよい。これらの公開鍵が一致した場合、用いられる公開鍵が署名確証処理において以前に有効に使用された鍵と一致するため、確証は成功だと考えられる。
同一のディジタル署名に対しては、実際の署名確証処理を再度実行する必要はないと考えられる。したがって、その後の署名確証処理の少なくともいくつかを、より効率的な同等の処理に置き換えることができる（たとえばバイトアレイ）。以下に、方法４２０のステップをさらに詳細に説明する。

【００９５】

ステップ４３０において、証明書上のディジタル署名の確証が開始される（たとえば証明書確証アプリケーションによって）。たとえばユーザが受け取った特定の証明書を確証

するために証明書チェーンを構築する際に、証明書上のディジタル署名の確証を実行することができる（図５を参照して論じたように、たとえば受信したメッセージに添付された証明書の信用状態を確証するため）。本実施形態において、確証される証明書上のディジタル署名は、それぞれの証明書を発行した認証局のものである。前述したように、署名確証処理において、証明書を発行した認証局の公開鍵が必要である。モバイルまたは他のコンピューティング装置上の証明書格納領域に、認証局の証明書および公開鍵が既に格納されていなければ、このステップにおいてそれらを引出すことが必要となり得る。

【００９６】

与えられた公開鍵に対しては、ステップ４４０において、この公開鍵を用いて署名確証処理を実行するのに先行して、承認されるべき証明書上のディジタル署名が以前にこの公開鍵を用いて首尾よく確証されたことがあるかどうかに関する決定がなされる。上述したように、これは、以前に用いられ、承認されるべき証明書上の署名を有効に確証し、格納されている証明書発行者の公開鍵（ステップ４７０においてキャッシュまたは他の記憶装置内に格納された公開鍵として、１つの鍵が存在する場合）を、ディジタル署名を確証するのに用いようとしている公開鍵と比較することによって実行することができ、一致があるかどうかを決定する。本実施形態においては、成功した確証の試行に用いられた公開鍵のみがキャッシュまたは他の記憶装置内に格納されるため、一致が決定された場合、承認されるべき証明書上のディジタル署名は以前に首尾よく確証されたことのある鍵だということになるであろう。

【００９７】

承認されるべき証明書上のディジタル署名が、与えられた公開鍵を用いて首尾よく確証されたことが以前にない場合、ステップ４５０において、ディジタル署名は、この公開鍵を用いて既知の方法で確証される。ステップ４６０において決定されるように、この公開鍵を用いて首尾よく署名が確証された場合、この成功した確証において用いられた公開鍵は、本実施形態に従って、将来ステップ４７０で使用されるためにキャッシュまたは他の記憶装置内に格納される。たとえば、ステップ４７０において格納された公開鍵は、承認されるべき証明書に関連したデータと共に格納されるか、公開鍵用の中枢記憶装置内（たとえばｌｏｏｋｕｐ　ｔａｂｌｅ内）に証明書によって索引をつけて（たとえば公開鍵と共に、発行者の名前および証明書のシリアルナンバーを格納することによって）格納されてもよい。

【００９８】

他方で、ステップ４４０において決定されるように、承認されるべき証明書上のディジタル署名が与えられた公開鍵を用いて以前に首尾よく確証されたことがあれば、ステップ４８０において、確証は成功するという指示が与えられる。これは、少なくともいくつかのデータを公開鍵を用いて復号する必要のある現在の署名確証処理を実行する代わりに行われ、それによって署名確証のプロセスをより効率的にする。これは、バッテリの電力を節約し、また、たとえば特にモバイル装置等の小型のデバイスに対するユーザの能力を高めるのに役立つ。

【００９９】

方法４２０のステップは、追加の公開鍵に対して繰り返されてもよい。

【０１００】

図８Ｂを参照すると、本発明の別の実施形態における、ディジタル署名の確証方法のステップを図示するフローチャートが、全体で４２０ｂとして示されている。

【０１０１】

成功した署名確証に用いられた公開鍵のみがキャッシュまたは他の記憶装置に格納される方法４２０とは対照的に、方法４２０ｂにおいては、いかなる署名確証の試行（成功したものも成功しなかったものも）に用いられた公開鍵も、確証の試行の結果と共にキャッシュまたは他の記憶装置内に格納されるが、そのことを除いて方法４２０ｂは方法４２０と類似している。

【０１０２】

概して、方法４２０ｂにおいては、与えられた公開鍵が証明書上のディジタル署名の確証に用いられる際、処理結果と共に、その公開鍵の複製がキャッシュに格納されるか、そうでなければ記憶装置内に格納される。たとえば、公開鍵およびそれに伴う結果は、証明書に関連する証明書情報と共に格納されるか、独立型の記憶装置（たとえばｌｏｏｋｕｐ　ｔａｂｌｅ）内に格納されることができる。与えられた鍵を用いて、次に同一の証明書上のディジタル署名を確証する試行が為される場合、少なくともいくつかのデータをその鍵を用いて復号する必要のある高価な署名確証処理を実行するよりも、代わりに、ディジタル署名を再度確証するために使用されるであろう公開鍵を格納された公開鍵と初めに比較するのがよい。与えられた公開鍵が格納されている公開鍵と一致した場合、格納されている公開鍵と関連して格納されている結果に従って、この確証の試行は成功しているまたは成功していないと考えられる。格納されている結果が、その公開鍵を用いた以前の確証の試行は成功したことを示す場合、この確証の試行は成功すると考えられるであろう。格納されている結果が、その公開鍵を用いた以前の確証の試行は成功しなかったことを示す場合、この確証の試行は失敗すると考えられるであろう。したがって、そうでなければ公開鍵を用いていくつかのデータを復号する必要があるであろう次の署名確証処理を、より効率的な同等の処理に置き換えることができる（たとえばバイトアレイ）。

【０１０３】

方法４２０を参照して説明したように、ステップ４３０において、証明書上のディジタル署名の確証が開始される（たとえば証明書確証アプリケーションによって）。

【０１０４】

与えられた公開鍵に対しては、ステップ４４０ｂにおいて、この公開鍵を用いて署名確証処理を実行するのに先行して、承認されるべき証明書上のディジタル署名が以前にこの公開鍵を用いて首尾よく確証されたことがあるかどうかに関する決定がなされる。上述したように、これは、以前に用いられ、承認されるべき証明書上の署名を有効に確証し、格納されている証明書発行者の公開鍵（ステップ４７０においてキャッシュまたは他の記憶装置内に格納された公開鍵として、１つの鍵が存在する場合）を、ディジタル署名を確証するのに用いようとしている公開鍵と比較することによって実行することができ、一致があるかどうかを決定する。一致が決定された場合、承認されるべき証明書上のディジタル署名の確証は以前に行われたことがあるということになるであろう。

【０１０５】

承認されるべき証明書上のディジタル署名を確証する試行が以前になされていない場合、方法４２０を参照して同様に説明したとおり、署名確証処理はステップ４５０において既知の方法で実行される。確証に用いられた公開鍵および確証の試行結果（すなわち、ディジタル署名が確証に成功しているか、そうでないかを示すもの）は、本実施形態に従って、キャッシュまたは他の記憶装置内に格納される。たとえば、ステップ４７０ｂにおいて格納された公開鍵および結果は、承認されるべき証明書に関連する情報と共に格納されるか、証明書によって索引をつけて（たとえば公開鍵と共に証明書のシリアルナンバーを格納することによって）公開鍵用の中枢記憶装置内（たとえばｌｏｏｋｕｐ　ｔａｂｌｅ内）に格納されてもよい。

【０１０６】

ステップ４４０ｂにおいて決定されるように、承認されるべき証明書上のディジタル署名が与えられた公開鍵を用いて以前に首尾よく確証されたことがあれば、ステップ４７２において、以前の確証の試行結果がこの鍵と共にキャッシュまたは他の記憶装置から引出される。そして、格納されている結果が、この鍵を用いた以前の確証の試行は成功したことを示すか、そうでないかについての決定がなされる。成功したことを示した場合、ステップ４８０において、この確証は成功するという指示が与えられる。また、そうでなければ、ステップ４９０において、この確証は成功しないという指示が与えられる。

【０１０７】

方法４２０ｂのステップは、追加の公開鍵に対して繰り返されてもよい。

【０１０８】

この公開鍵を用いた確証が失敗するかどうかを決定するために、少なくとも公開鍵を用いていくつかのデータを復号する必要のある署名確証処理を実行する代わりに以前の確証の試行結果が用いられ、それによって署名確証処理をより効率的なものにする。特に、ユーザが、同一の無効な公開鍵を用いて証明書上のディジタル署名の確証処理を何度も要求した場合、少なくとも公開鍵を用いていくつかのデータを復号する必要があり高価な現在の署名確証処理は、一度だけ実行する必要があるが、次の試行は、比較的効率的な同等の処理（たとえばバイトアレイ）を実行した後、即座に失敗するであろう。このことは、バッテリの電力を節約し、また、たとえば特にモバイル装置等の小型のデバイスに対するユーザの能力を高めるのにさらに役立ち得る。

【０１０９】

所望であれば、様々な実施形態において、上記した公開鍵および確証の試行結果に加え他の情報もキャッシュまたは他の記憶装置内に格納され得ることは当業者であれば理解できよう。

【０１１０】

様々な実施形態において、キャッシュまたは他の記憶装置に格納されている、公開鍵および他の情報（たとえば確証の試行結果）は、限られた有効期間の、公開鍵を比較する際の使用のためにのみ認められている。その後には、それらは古いと考えられ、キャッシュまたは他の記憶装置から削除しなければならない。これはセキュリティの目的で行われるので、少なくとも公開鍵を用いていくつかのデータを復号する必要のある現在の署名確証処理は、何度も再行されなければならない。この有効期間は、たとえばＩＴ方針に従って設定される。同様に、本発明の別の実施形態において、キャッシュまたは他の記憶装置に格納された、いくつかの、または全ての公開鍵および他の情報は、たとえばユーザまたはアドミニストレータによって手動で命令されることもあるが、古いとみなされるか削除され得るため、署名確証処理が再実行されなければならない。さらに高度なセキュリティのために、たとえば、格納した後に公開鍵（たとえば以前に首尾よく証明書の署名を確証した公開鍵）が無効になっていないことを確証するための確証処理も実行してもよい。

【０１１１】

本発明の実施形態における、証明書上のディジタル署名を確証する方法のステップは、伝送型媒体を含めたコンピュータ可読媒体に格納された、実行可能なソフトウェア命令として提供されてもよい。

【０１１２】

本発明を多数の実施形態に関して説明したが、ここに付属する請求項において定義される本発明の範囲から逸脱することなく、他の変更および修正が行われてもよいことは、当業者であれば理解できよう。

【図面の簡単な説明】

【０１１３】

【図１】１つの例の実行におけるモバイル装置のブロック図である。

【図２】図１のモバイル装置の、コミュニケーションサブシステムの構成要素のブロック図である。

【図３】無線ネットワークのノードのブロック図である。

【図４】１つの例の構成における、ホストシステムの構成要素を図示するブロック図である。

【図５】証明書チェーンの例を示すブロック図である。

【図６】暗号化されたメッセージの例の構成要素を示すブロック図である。

【図７Ａ】証明書チェーンの２つの例を示すブロック図である。

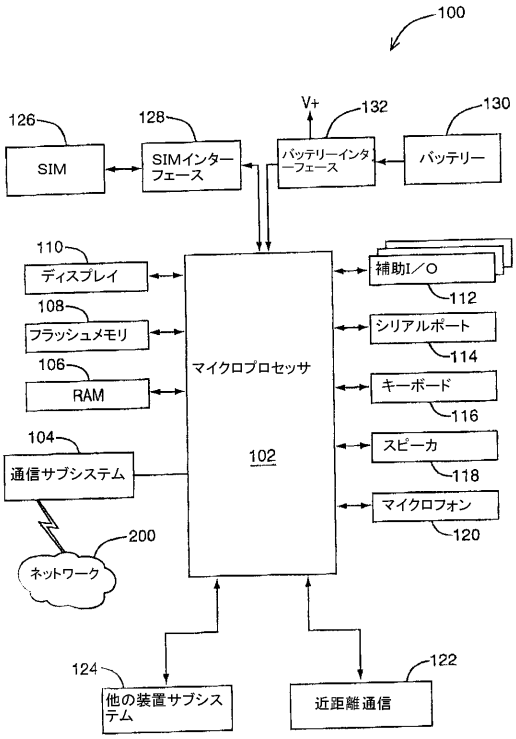
【図７Ｂ】図７Ａの証明書チェーンと連結するクロス証明書を示すブロック図である。

【図８Ａ】本発明の一実施形態における、証明書上のディジタル署名の確証方法のステップを図示するフローチャートである。

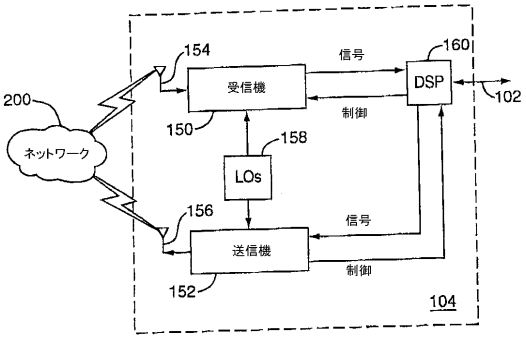
【図８Ｂ】本発明の別の実施形態における、証明書上のディジタル署名の確証方法のステップを図示するフローチャートである。

【符号の説明】
【０１１４】
１００　モバイル装置
１０２　マイクロプロセッサ
１０６　ＲＡＭ
１０８　フラッシュメモリ
１０４　通信サブシステム
１５０　送信機
１５１　受信機
１６０　デジタル信号プロセッサ

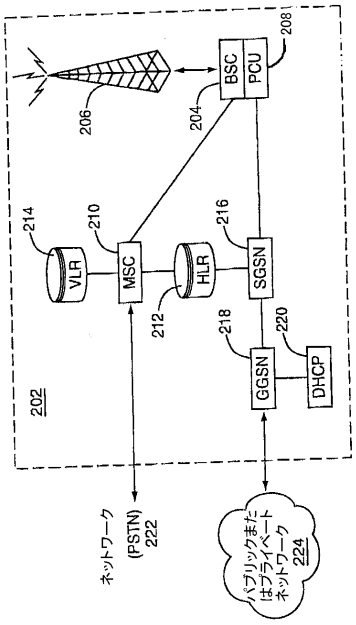
【図１】



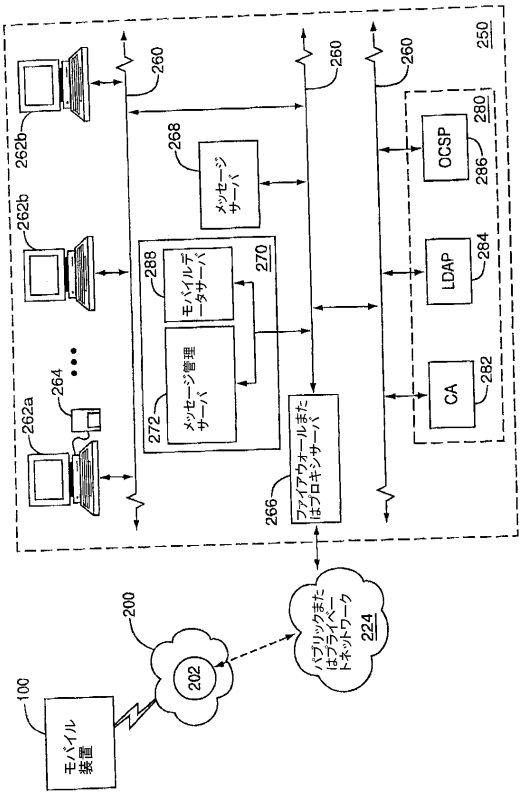
【図２】



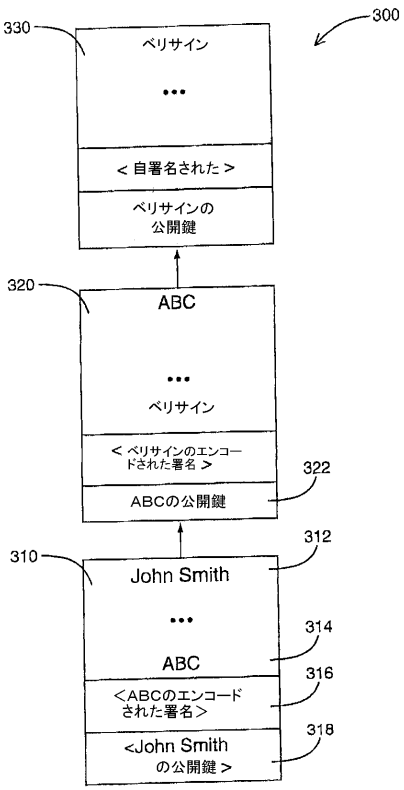
【図３】


BSC
PCU
208
206
204
214
210
216
VLR
MSC
HLR
SGSN
212
218
220
GGSN
DHCP
202
ネットワーク
(PSTN)
222
パブリックまたは
プライベート
ネットワーク
224

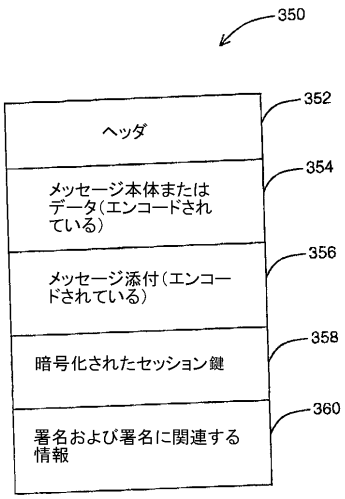
【図４】


250
260
262b
268
メッセージ
サーバ
OCSP
280
286
288
モバイルデータサーバ
270
LDAP
284
メッセージ管理
サーバ
272
CA
282
264
262a
ファイアウォールまたは
プロキシサーバ
266
200
202
パブリックまたは
プライベート
ネットワーク
224
100
モバイル
装置

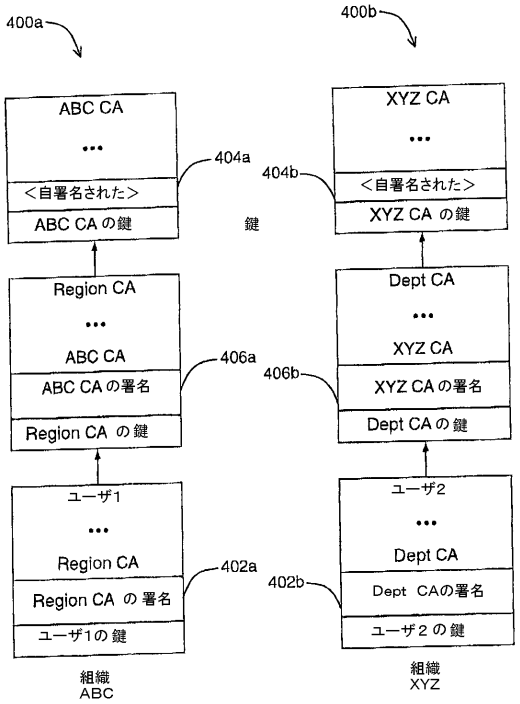
【図５】


300
330
ベリサイン
< 自署名された >
ベリサインの
公開鍵
320
ABC
ベリサイン
< ベリサインのエンコードされた署名 >
322
ABCの公開鍵
310
312
John Smith
314
ABC
316
<ABCのエンコードされた署名>
318
<John Smith
の公開鍵 >

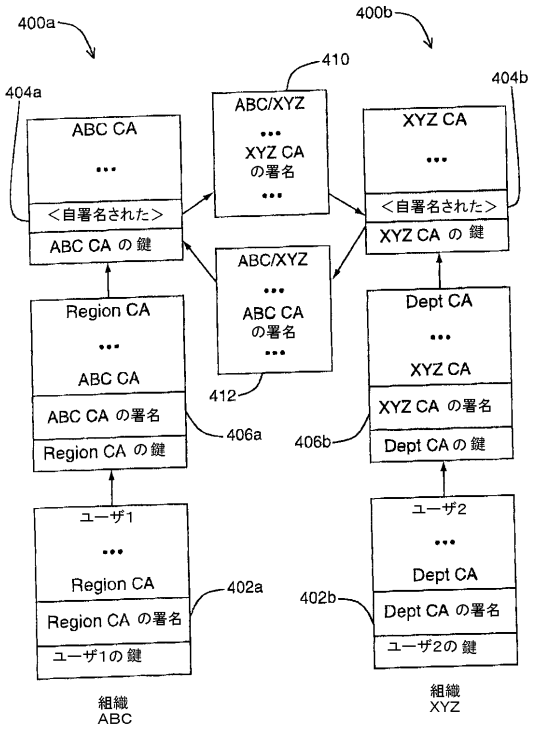
【図６】


350
352
ヘッダ
354
メッセージ本体または
データ(エンコードされ
ている)
356
メッセージ添付(エンコー
ドされている)
358
暗号化されたセッション鍵
360
署名および署名に関連する
情報

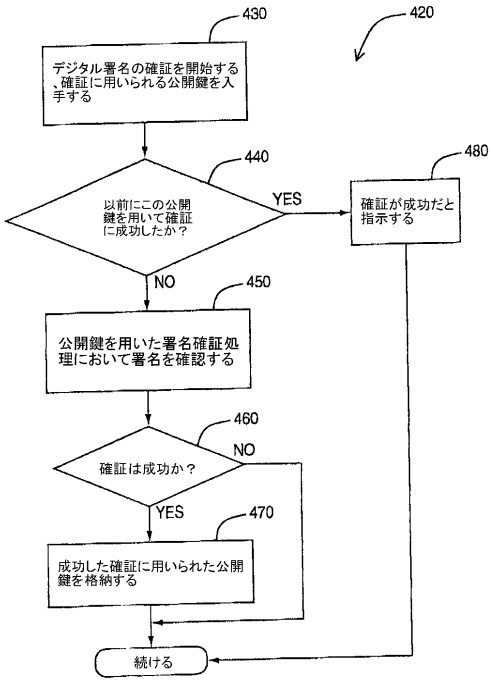
【図７Ａ】



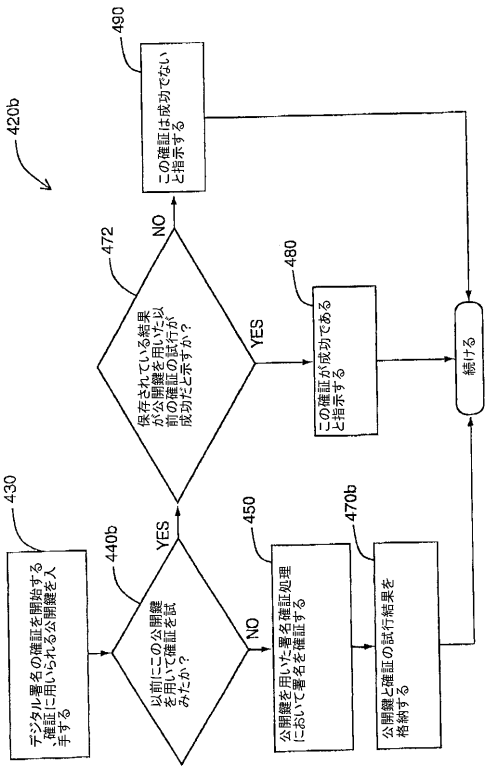
【図７Ｂ】



【図８Ａ】



【図８Ｂ】



フロントページの続き

(72)発明者 ブラウン, マイケル ケー.
カナダ国 エヌ２エム ２ゼット２ オンタリオ, キッチナー, ファーンウッド プレイス ８
(72)発明者 ブラウン, マイケル エス.
カナダ国 エヌ２ケー ４ビー１ オンタリオ, ウォータールー, ユニバーシティー ダウンズ クレセント ３５０

審査官 松平 英

(56)参考文献 特開平０９－２０５４２４（ＪＰ，Ａ）
特開平１０－０７９０２５（ＪＰ，Ａ）
特開２０００－０１０４７７（ＪＰ，Ａ）
特開２０００－３１２２０４（ＪＰ，Ａ）
特開２００２－１８９９７６（ＪＰ，Ａ）
特開２００３－１６２５０８（ＪＰ，Ａ）
特開２００４－０１５２５７（ＪＰ，Ａ）
特開２００４－２４７７９９（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ ９／００
Ｇ０９Ｃ １／００
Ｇ０６Ｆ ９／０６
Ｇ０６Ｆ １２／１４
Ｇ０６Ｆ １５／００
Ｈ０４Ｋ １／００