(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4795636号
(P4795636)
(45)発行日　平成23年10月19日(2011.10.19)　(24)登録日　平成23年8月5日(2011.8.5)

(51)Int.Cl.　　F I
G06F 9/445 (2006.01)　　G06F 9/06 610Q
G06F 21/22 (2006.01)　　G06F 9/06 660G
H04W 12/00 (2009.01)　　H04B 7/26 109R

請求項の数 6　(全 19 頁)

(21)出願番号　特願2003-500736 (P2003-500736)
(86)(22)出願日　平成14年5月23日 (2002.5.23)
(65)公表番号　特表2005-517220 (P2005-517220A)
(43)公表日　平成17年6月9日 (2005.6.9)
(86)国際出願番号　PCT/US2002/016485
(87)国際公開番号　WO2002/097620
(87)国際公開日　平成14年12月5日 (2002.12.5)
審査請求日　平成17年5月20日 (2005.5.20)
審判番号　不服2009-1998 (P2009-1998/J1)
審判請求日　平成21年1月26日 (2009.1.26)
(31)優先権主張番号　09/872,418
(32)優先日　平成13年5月31日 (2001.5.31)
(33)優先権主張国　米国 (US)

(73)特許権者　595020643
クゥアルコム・インコーポレイテッド
ＱＵＡＬＣＯＭＭ　ＩＮＣＯＲＰＯＲＡＴＥＤ
アメリカ合衆国、カリフォルニア州　９２１２１－１７１４、サン・ディエゴ、モアハウス・ドライブ　５７７５
(74)代理人　100108855
弁理士　蔵田　昌俊
(74)代理人　100091351
弁理士　河野　哲
(74)代理人　100088683
弁理士　中村　誠
(74)代理人　100109830
弁理士　福原　淑弘

最終頁に続く

(54)【発明の名称】サーバによるアプリケーションの処理及び配布のための方法、及びアプリケーションの処理及び配布のためのシステム

(57)【特許請求の範囲】
【請求項１】
ワイヤレスネットワークを介して通信を行うワイヤレス装置上での使用のための、サーバによるアプリケーションの処理及び配布のための方法であって、
前記サーバが、前記アプリケーションと前記アプリケーションに関連する第１の識別情報とを配布元から受信することであって、前記第１の識別情報は前記アプリケーションの配布元の身元を確認するのに使用されることと、
前記サーバが前記アプリケーションを解析することによって、前記アプリケーションが一組の所定の基準における各基準を満足することを認証することであって、各基準は、前記ワイヤレス装置におけるアプリケーション実行環境に合致して決められることと、
前記認証の後に、前記サーバが、前記アプリケーションに対して一組の許可を付与することであって、前記一組の許可は複数の許可を含み、該複数の許可のそれぞれは前記一組の所定の基準における各基準に関連しており、さらに、前記一組の許可は、前記ワイヤレス装置上での前記アプリケーションの実行を許可すべきか否かについて判別するのに用いられる一組の認証フラグを含み、各認証フラグは、前記アプリケーションが前記認証にパスしたか否かに応じてセットされることと、
前記サーバが、前記アプリケーションと、前記一組の許可と、前記サーバの身元を確認するのに使用される第２の識別情報とを前記ワイヤレス装置に送信することと、を具備した前記方法。
【請求項２】

前記ワイヤレス装置への送信にあたって、少なくとも前記アプリケーションに対して、当該アプリケーションが送信される間に変更されたか否かを検出するためのデジタル署名技術が適用される請求項１記載の方法。

【請求項３】

ワイヤレスネットワークを介して通信を行うワイヤレス装置上で使用されるアプリケーションの処理及び配布のためのシステムであって、

キャリアネットワークと、

前記ワイヤレスネットワークを支持するとともに、前記キャリアネットワークに接続され、インターネット及び／又は電話システムで構成されるインフラストラクチャと、

前記キャリアネットワークに結合され、配布元から前記アプリケーションを受信するサーバと、を具備し、

前記サーバは、

前記アプリケーションと前記アプリケーションに関連する第１の識別情報とを受信することであって、前記第１の識別情報は前記アプリケーションの配布元の身元を確認するために使用されることと、

前記サーバが前記アプリケーションを解析することによって、前記アプリケーションが一組の所定の基準における各基準を満足することを認証することであって、各基準は、前記ワイヤレス装置におけるアプリケーション実行環境に合致して決められることと、

前記認証の後に、前記サーバが、前記アプリケーションに対して一組の許可を付与することであって、前記一組の許可は複数の許可を含み、該複数の許可のそれぞれは前記一組の所定の基準における各基準に関連しており、さらに、前記一組の許可は、前記ワイヤレス装置上での前記アプリケーションの実行を許可すべきか否かについて判別するのに用いられる一組の認証フラグを含み、各認証フラグは、前記アプリケーションが前記認証にパスしたか否かに応じてセットされることと、

前記アプリケーションと、前記一組の許可と、前記サーバの身元を確認するのに使用される第２の識別情報とを前記キャリアネットワークと前記インフラストラクチャとを介して前記ワイヤレス装置に送信することと、を行うように構成された前記システム。

【請求項４】

前記アプリケーションと、前記一組の許可と、前記第２の識別情報とを前記ワイヤレス装置に送信するにあたって、前記アプリケーションが前記送信中に変更されたか否かを検出するためのデジタル署名技術が使用される請求項３記載のシステム。

【請求項５】

前記サーバは、

サーバ間ネットワークと、

配布元から前記アプリケーションを受信するように構成された第１のサーバと、

前記アプリケーションを認証するように構成された第２のサーバと、

前記アプリケーションに対して一組の許可を付与するとともに、前記アプリケーションを送信するように構成された第３のサーバであって、前記一組の許可は、前記ワイヤレス装置上での前記アプリケーションの実行を許可すべきか否かについて判別するのに使用される第３のサーバと、を具備し、

前記第１、第２及び第３のサーバはそれぞれ前記サーバ間ネットワークに結合されるとともに、前記第３のサーバは前記キャリアネットワークに結合されている請求項３記載のシステム。

【請求項６】

ワイヤレスネットワークを介して通信を行うワイヤレス装置上での使用のための、アプリケーションの処理及び配布のためのシステムであって、

キャリアネットワーク手段と、

前記ワイヤレスネットワークを支持するとともに、前記キャリアネットワークに接続され、インターネット及び／又は電話システムで構成されるインフラストラクチャ手段と、

前記キャリアネットワークに結合されたサーバ手段であって、

配布元から前記アプリケーションと前記アプリケーションに関連する第１の識別情報とを受信するための受信手段であって、前記第１の識別情報は前記アプリケーションの配布元の身元を確認するために使用される受信手段と、

前記アプリケーションを解析することによって、一組の所定の基準における各基準を満足することを認証する認証手段であって、各基準は、前記ワイヤレス装置におけるアプリケーション実行環境に合致して決められる認証手段と、

前記アプリケーションが前記認証手段によって認証された後に当該アプリケーションに対して一組の許可を付与する付与手段であって、前記一組の許可は複数の許可を含み、該複数の許可のそれぞれは前記一組の所定の基準における各基準に関連しており、さらに、前記一組の許可は、前記ワイヤレス装置上での前記アプリケーションの実行を許可すべきか否かについて判別するのに用いられる一組の認証フラグを含み、各認証フラグは、前記アプリケーションが前記認証にパスしたか否かに応じてセットされる付与手段と、

前記アプリケーションと、前記一組の許可と、前記サーバの身元を確認するのに使用される第２の識別情報とを前記ワイヤレス装置に送信するための送信手段と、を具備した前記システム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明はワイヤレス装置において使用されるアプリケーションの処理に関し、より詳細には、ワイヤレス装置で実行されるアプリケーションの機密保護、安全及び完全性の増大に関するものである。

【背景技術】

【０００２】

ワイヤレス通信は最近、爆発的な成長を遂げた。消費者及びビジネス業界がよりいっそう移動電話やパーソナルデジタルアシスタンツ（ＰＤＡ）などのワイヤレス装置に依存するにつれて、ワイヤレスサービスプロバイダすなわちキャリアはこれらのワイヤレス装置に関して付加的な機能を提供するべく努力をしている。このような付加的な機能は、ワイヤレス装置に対する要求を増大するのみならず、現在のユーザの間での使用を増大している。しかしながら、特に、ワイヤレス装置によってアクセス可能なアプリケーションを増大することによる機能の増加はコスト高及び複雑さを引き起こし、キャリアがこのような機能を提供する意欲を減退させてしまう。

【０００３】

さらに、いったんワイヤレス装置に搭載されたアプリケーションが正常に実行される保証はほとんどない。現在、ワイヤレス装置上で実行するアプリケーションの能力に対する信頼性は開発者、ワイヤレス装置メーカ及び／又はキャリアに依存する。より多くのアプリケーションが開発され、ワイヤレス装置に搭載されるアプリケーションの数が増大するときに、ワイヤレス装置の環境はより動的になる。例えば、ワイヤレス装置は、適当なときに利用可能なアプリケーションの集合体から多数の異なるアプリケーションを検索または実行することを選択することもある。すなわち、任意のアプリケーションがワイヤレス装置に配布されて安全に実行することを保証することは制御が困難になってしまう。

【０００４】

このことは特に、アプリケーションの不正な実行はワイヤレス装置に悪影響を与えるだけでなく、キャリアネットワーク及び他のワイヤレス装置を含む他のネットワーク要素に害を与えてしまう。例えば、１つ（これに限定されない）のアプリケーションはワイヤレス装置のパワー制御部の制御を行うことができ、他のワイヤレス装置との干渉を引き起こし、ワイヤレス装置にサービスを提供しているセルの全容量を低減させてしまう。

【発明の開示】

【発明が解決しようとする課題】

【０００５】

現在のところ、ワイヤレス装置の製造者もキャリアも動的なアプリケーション配布及び

実行環境におけるアプリケーションの試験及び安全配布を支持可能に構成されていない。すなわち、アプリケーションがワイヤレス装置に配布されて実行されて、ワイヤレス装置、キャリアネットワーク、あるいは他のネットワーク要素に対して危害を与える恐れがある。

【０００６】

加えて、より多くのアプリケーションが開発されてアプリケーションがワイヤレス装置に送信される環境がより動的になったときに発生する安全性についての問題が発生する。アプリケーションの数とこれらのアプリケーションを作り上げている開発者の数が増大するとき、任意のアプリケーションのソースすなわち開発者を知りたいという要望は増大する。キャリアまたはハンドセット製造者は、そのアプリケーションが危害を引き起こすならばアプリケーションのソースを決定することができることをある程度の信頼度で知ることを望む。

【０００７】

すなわち、業界で必要とされていることは、ワイヤレス装置上のアプリケーションの配布及び実行に対するより安全な環境を提供するためのシステム及び方法である。

【０００８】

本発明に合致したシステム及び方法は、所定の標準をもつテストアプリケーションが否認防止のために開発者に対する追跡可能性を提供し、アプリケーションに対する意図しない変更があるかどうかを検査し、ワイヤレス装置からのアプリケーションの除去を可能にし、及び／またはアプリケーションが実行される環境を規定する規則及び許可を使用する、アプリケーション配布及び実行のための安全な環境を作り上げることによって、既存のシステムの欠点を克服する。

【０００９】

アプリケーションが所定の標準を満たすことを確実にすることは、実行中に起こるエラーを事前に発見する利点を提供する。このことは、アプリケーションの実行の悪影響を防止することを助ける。

【００１０】

追跡可能性は否認防止の利点を提供する。アプリケーションに何らかの問題があったならば、その問題を解決するためにアプリケーションのソースを追跡することが有益である。加えて、追跡可能性を提供することは、開発者が意図的かどうかとは無関係に、有害な結果を引き起こすアプリケーションを作らないようにする作用をもたらす。

【００１１】

さらに、アプリケーションがワイヤレス装置でそれを受信する前に変更されたかどうかを決定する能力は、受信された当該アプリケーションが送信されたものと同じものであることを確実にすることによって安全性を増大させる利点を提供する。アプリケーションがワイヤレス環境においてより自由に配布されるときに、アプリケーションが変更されたかどうかを決定する能力は、ワイヤレス装置によって受信されたアプリケーションは意図的であるか否かとは無関係に、変更されなかった信頼度を増大する。

【００１２】

アプリケーションがいつ実行されるかを規定する一連の規則及び許可を提供することは、例えば、権限が与えられていないシステムまたは環境などのプラットフォーム上でのアプリケーションの認可されていない実行を防止することによって、アプリケーション配布及び実行システムの安全性を増大する。

【００１３】

ワイヤレス装置からアプリケーションを除去する能力は、アプリケーション配布システムの安全性を増大する。製造者またはアプリケーションダウンロードを介してアプリケーションがハンドセット上にインストールされたときに、予測できない負の結末に備えてアプリケーションを除去する機構を備えることは、有害かつ有害となる不要なコードを除去することによってアプリケーション配布及び実行システムの安全性を増大させる。

【００１４】

本発明に合致するシステム及び方法は、ここに開示された１つまたはそれ以上の技術を用いる。しかしながら、ここに開示及び参照された全ての技術を用いることによって、本発明に合致したシステム及び方法は、高品質及びアプリケーションの安全な配布及び実行を提供する。

【課題を解決するための手段】

【００１５】

本発明の一態様によれば、ワイヤレスネットワークを介して通信を行うワイヤレス装置上での使用のための、サーバによるアプリケーションの処理及び配布のための方法であって、前記サーバが、前記アプリケーションと前記アプリケーションに関連する第１の識別情報とを配布元から受信することであって、前記第１の識別情報は前記アプリケーションの配布元の身元を確認するのに使用されることと、前記サーバが前記アプリケーションを解析することによって、前記アプリケーションが一組の所定の基準における各基準を満足することを認証することであって、各基準は、前記ワイヤレス装置におけるアプリケーション実行環境に合致して決められることと、前記認証の後に、前記サーバが、前記アプリケーションに対して一組の許可を付与することであって、前記一組の許可は複数の許可を含み、該複数の許可のそれぞれは前記一組の所定の基準における各基準に関連しており、さらに、前記一組の許可は、前記ワイヤレス装置上での前記アプリケーションの実行を許可すべきか否かについて判別するのに用いられる一組の認証フラグを含み、各認証フラグは、前記アプリケーションが前記認証にパスしたか否かに応じてセットされることと、前記サーバが、前記アプリケーションと、前記一組の許可と、前記サーバの身元を確認するのに使用される第２の識別情報とを前記ワイヤレス装置に送信することと、を具備し、前記アプリケーションは、前記ワイヤレス装置と前記ワイヤレスネットワーク間で前記アプリケーションを処理するためのメッセージのやり取りを行う無線通信を実行する行為から独立している。

【００１６】

また、本発明の一態様によれば、ワイヤレスネットワークを介して通信を行うワイヤレス装置上で使用されるアプリケーションの処理及び配布のためのシステムであって、キャリアネットワークと、前記ワイヤレスネットワークを支持するとともに、前記キャリアネットワークに接続され、インターネット及び／又は電話システムで構成されるインフラストラクチャと、前記キャリアネットワークに結合され、配布元から前記アプリケーションを受信するサーバと、を具備し、前記サーバは、前記アプリケーションと前記アプリケーションに関連する第１の識別情報とを受信することであって、前記第１の識別情報は前記アプリケーションの配布元の身元を確認するために使用されることと、前記サーバが前記アプリケーションを解析することによって、前記アプリケーションが一組の所定の基準における各基準を満足することを認証することであって、各基準は、前記ワイヤレス装置におけるアプリケーション実行環境に合致して決められることと、前記認証の後に、前記サーバが、前記アプリケーションに対して一組の許可を付与することであって、前記一組の許可は複数の許可を含み、該複数の許可のそれぞれは前記一組の所定の基準における各基準に関連しており、さらに、前記一組の許可は、前記ワイヤレス装置上での前記アプリケーションの実行を許可すべきか否かについて判別するのに用いられる一組の認証フラグを含み、各認証フラグは、前記アプリケーションが前記認証にパスしたか否かに応じてセットされることと、前記アプリケーションと、前記一組の許可と、前記サーバの身元を確認するのに使用される第２の識別情報とを前記キャリアネットワークと前記インフラストラクチャとを介して前記ワイヤレス装置に送信することと、を行うように構成され、前記アプリケーションは、前記ワイヤレス装置と前記ワイヤレスネットワーク間で前記アプリケーションを処理するためのメッセージのやり取りを行う無線通信を実行する行為から独立している。

【００１７】

また、本発明の一態様によれば、ワイヤレスネットワークを介して通信を行うワイヤレス装置上での使用のための、アプリケーションの処理及び配布のためのシステムであって

、
キャリアネットワーク手段と、前記ワイヤレスネットワークを支持するとともに、前記キャリアネットワークに接続され、インターネット及び／又は電話システムで構成されるインフラストラクチャ手段と、前記キャリアネットワークに結合されたサーバ手段であって、配布元から前記アプリケーションと前記アプリケーションに関連する第１の識別情報とを受信するための受信手段であって、前記第１の識別情報は前記アプリケーションの配布元の身元を確認するために使用される受信手段と、前記アプリケーションを解析することによって、一組の所定の基準における各基準を満足することを認証する認証手段であって、各基準は、前記ワイヤレス装置におけるアプリケーション実行環境に合致して決められる認証手段と、前記アプリケーションが前記認証手段によって認証された後に当該アプリケーションに対して一組の許可を付与する付与手段であって、前記一組の許可は複数の許可を含み、該複数の許可のそれぞれは前記一組の所定の基準における各基準に関連しており、さらに、前記一組の許可は、前記ワイヤレス装置上での前記アプリケーションの実行を許可すべきか否かについて判別するのに用いられる一組の認証フラグを含み、各認証フラグは、前記アプリケーションが前記認証にパスしたか否かに応じてセットされる付与手段と、前記アプリケーションと、前記一組の許可と、前記サーバの身元を確認するのに使用される第２の識別情報とを前記ワイヤレス装置に送信するための送信手段と、を具備し、前記アプリケーションは、前記ワイヤレス装置と前記ワイヤレスネットワーク間で前記アプリケーションを処理するためのメッセージのやり取りを行う無線通信を実行する行為から独立している。

【発明の効果】

【００１８】

本発明によれば、高品質及びアプリケーションの安全な配布及び実行を提供することができる。

【発明を実施するための最良の形態】

【００１９】

添付の図面に示されたような本発明の例示的かつ好ましい実施形態を詳細に説明する。ここで、同一の参照符号は図面中において同一あるいは対応する部分を示すものとする。本発明の性質、目的及び利点は、添付の図面を参照した以下の詳細な説明を理解すれば当業者に明らかになるだろう。

【００２０】

本発明は、それが実行される環境に関連した所定の基準を満足することを確実にするためにアプリケーションを試験するシステム及び方法を提供することによって安全で機密保護に優れたアプリケーション配布及び実行を提供する。さらに、規則及び許可リスト、アプリケーション除去、デジタル署名などの変更検出技術を使用することによって、本発明は、アプリケーションが変更されたかどうかを決定し、それが所定のワイヤレス装置環境において実行する許可をもつかを決定し、そうすることが所望される場合には当該アプリケーションを除去することによって、試験されたあるいは未試験のアプリケーションを安全に配布して実行するための機構を提供する。

【００２１】

当業者ならば、前記のことは説明を簡単にするために配布されて実行されるアプリケーションファイルタイプを説明することを認識するであろう。“アプリケーション”は、オブジェクトコード、スクリプト、ＪＡＶＡ（登録商標）ファイル、ブックマークファイル（あるいはＰＱＡファイル）、ＷＭＬスクリプト、バイトコード、そしてパールスクリプトなどの、実行可能なコンテントをもつファイルを含む。加えて、ここで使用される“アプリケーション”は、オープンされるべき文書あるいはアクセスされるべき他のデータファイルなどの通常実行できないファイルを含む。

【００２２】

図１は、本発明の例示的な実施形態に合致した方法でのアプリケーション配布及び実行の高レベル処理を示すフローチャートである。

【００２３】
本発明の実施形態は、開発者識別を当該アプリケーションに関連つけることを可能にし、前記アプリケーションが実行しようとする環境に対してアプリケーションについて試験を行い、どの装置あるいはシステムが前記アプリケーションを実行するかを示すのに使用可能な許可を割り当て、あるアプリケーションが不法あるいは不要な行動を実行するときにアプリケーション除去を提供する。
【００２４】
システム及び方法はアプリケーションの安全な配布及び実行を増大するためにこれら全ての技術を使用することが望ましい。しかしながら、これらの技術の１つまたはそれ以上を使用する場合であってもアプリケーションの安全な配布及び実行を増大することを認識する。
【００２５】
高レベル処理は、開発者識別をアプリケーションに関連付けることにより開始する（ステップＳ１００）。この処理は、それが配布されるときに開発者識別をアプリケーションに結合することにより実行される。他方、関連付けられた開発者識別は、システム内のサーバー上の対応するアプリケーションとともに記憶される。また、開発者識別情報は記憶されて容易に変更できないようにアプリケーション情報と関連付けられることが望ましい。
【００２６】
次に、アプリケーションは不正な動作がないか試験される（ステップＳ１０５）。アプリケーションは不正な動作がアプリケーションが動作している装置に影響を与えるのみならず、当該装置に直接接続されるかあるいは当該装置にネットワーク上で接続されている他の装置にも影響を与える環境に於いて使用される。それが不適切なシステムコールを生成したり動作中に当該装置または接続された他の装置に対して負の影響を与えないように当該アプリケーションを試験することが望ましい。一実施形態において、この試験は、アプリケーションが所定の基準を満たすか否かを決定するために試験される認証処理によって実行される。当該アプリケーションを試験するために、開発者とは独立した認証処理を行うことが望ましい。この認証処理の独立性はより正確で信頼のある試験を促進する。
【００２７】
アプリケーションを実行するに先立って、当該アプリケーションはそれが装置上で実行することが“許可”されるべきかについて検査される（ステップＳ１１０）。この検査は後述される許可及び規則あるいは当業者に知られた他の許可機構を使用することによって実行される。さらに、アプリケーションを実行する毎に検査されることが望ましい。この執拗な検査処理によりアプリケーションを実行するときの安全性が増大する。例えば、他のアプリケーションを介して実行装置上のアプリケーション内に挿入されたトロイの木馬タイプの破壊的なプログラムをもつアプリケーションに対して防護することができる。
【００２８】
次に、不正または不要な動作を実行するアプリケーションは、装置から除去される（ステップＳ１１５）。このことはアプリケーションがさらなる損害を与えることから防止でき、他の使用のために装置内のメモリを解放することになる。一方、アプリケーションは当該アプリケーションから除去される必要はない。アプリケーションを除去することはアプリケーションの不動作を意味し、当該アプリケーションを装置上に残すことになる。
【００２９】
図２は、本発明の例示的な実施形態が実施されるシステムアーキテクチャを示す。開発者２００は、ワイヤレス装置２３０上で使用されるアプリケーションを作り上げる。上記したように、上記の説明はアプリケーションファイルタイプを含むが、他のファイルタイプも使用できることは当業者ならば認識するであろう。さらに、本発明は他のワイヤレスまたは非ワイヤレス装置に適用でき、ワイヤレスネットワーク、非ワイヤレスネットワークあるいはそれらの組み合わせに適用することができる。
【００３０】

概して、開発者２００は、ワイヤレス装置２３０上で実行するためのアプリケーションを開発するための一組の開発仕様を具備する。一実施形態において、ワイヤレス装置は、アプリケーションのワイヤレス装置とのインタフェースを支援するために、QUALCOMM社（カルフォルニア州サンジエゴ）により開発されたＢＲＥＷ（登録商標）ソフトウェアなどのソフトウェアプラットフォームを含む。開発者は、ソフトウェアプラットフォームすなわちＢＲＥＷソフトウェア、仕様標準及び規約を満足するアプリケーションを作り上げる。

【００３１】

一実施形態において、開発者２００は、アプリケーションを電子的に中央サーバー２０５に送信するように、中央サーバー２０５に接続されている。一実施形態において、中央サーバーは、アプリケーションをワイヤレス装置に配布するにあたって使用されるアプリケーションコントロールセンター首脳部（ＡＣＣＨＱ）サーバーである。開発者２００は、アプリケーションが変更されたかを決定するために（以下にさらに説明する）アプリケーションにデジタル的に署名する。中央サーバーに対する物理的接続は不要であることがわかる。例えば、開発者２００は第１種郵便などによりアプリケーションをＣＤ－ＲＯＭ上に記憶された中央サーバー２０５に送信する。

【００３２】

加えて、開発者は、種々の送信元識別情報を中央サーバー２０５に送信する。この送信元識別情報は、会社名、会社のタックスアイデンチフィケーションあるいは他の識別情報などの、開発者を識別するアプリケーションに関連付けられる任意の情報を含む。

【００３３】

中央サーバー２０５は、それ自身あるいは認証サーバー２１０を使用してアプリケーションの解析及び認証に用いられる。一実施形態において、アプリケーションコントロールセンター（ＡＣＣ）は認証サーバーとして使用される。認証サーバー２１０は、アプリケーションが所定の認証基準を満たすかどうかを決定するためにアプリケーションを解析するのに使用される。この基準はアプリケーションがワイヤレス装置あるいはプラットフォーム上での実行のために開発仕様を満足するかどうかを含む。しかしながら、認証基準は、アプリケーションがワイヤレス装置またはプラットフォーム上での実行に先立って満足しなければならない任意の基準である。そのような基準は、（ａ）当該アプリケーションはワイヤレス装置の動作に損害を与えない（例えば電話の機能を停止させない）ように、アプリケーションが開発者により要求された通り機能する、（ｂ）アプリケーションは禁止されているデータまたはメモリにアクセスしない（例えば他のアプリケーション、オペレーティングシステムあるいはプラットフォームソフトウェアにアクセスしない）、（ｃ）ワイヤレス装置の入力と出力を有害に独占化するなど、ワイヤレス装置資源に負の影響を与えない、ことを検証することを含む。

【００３４】

中央サーバー２０５はアプリケーションに関連するリストに一組の許可を割り当てる。この許可リストは、アプリケーションが認証処理をパスしたかどうか、アプリケーションがどのネットワーク２２０上で実行することを許可されたか、ワイヤレス装置がアプリケーションを支持するかどうかについての解析を含む、種々の要因によって決定される。許可リストを決定するのに使用され、本発明を実施するときに当業者に委ねられる多くの要因が存在する。

【００３５】

中央サーバー２０５は、開発者識別情報を受信してそれを開発者２００によって作り上げられたアプリケーションと相関させる。当該アプリケーションに何らかの問題があるならば、中央サーバーはアプリケーションのソースを識別することができる。一実施形態において、開発者情報はワイヤレス装置２３０に渡され、これによって相関がワイヤレス装置または当該ワイヤレス装置に接続された他のシステムによって実行される。

【００３６】

一実施形態において、中央サーバーはさらにアプリケーションダウンロードサーバー（

ＡＤＳ）２１５に接続されている。アプリケーションダウンロードサーバー２１５はアプリケーションをダウンロードするために、ワイヤレスネットワーク２２０を介してワイヤレス装置とのインタフェースを行うのに使用される。中央サーバーは許可リストと当該アプリケーションに関連する開発者識別をＡＤＳに送信し、ワイヤレス装置に送信されるときまで記憶される。アプリケーション、許可リスト、開発者識別は、変更からの安全性を増大するために中央サーバーによってデジタル的に署名されることが望ましい。

【００３７】

当業者ならば、ＡＤＳがアプリケーション、ファイル及び他の情報を種々のワイヤレス装置２３０に配布するべく多数のネットワーク２２０に接続されるのに使用されることを認識するであろう。さらに、ワイヤレス及び非ワイヤレスネットワークはアプリケーションの許可リスト及び開発者識別をワイヤレス装置に送信するのに使用される。

【００３８】

アプリケーションに対する要求に応答して、ＡＤＳ２１５はアプリケーション、許可リスト、開発者識別及びデジタル署名をネットワーク２２０によりワイヤレス装置２３０に送信する。一実施形態において、ワイヤレス装置２３０は、アプリケーション、許可リスト及び／または開発者情報が変更されたか否かを決定するために、デジタル署名を検査するための鍵を含む。

【００３９】

望ましくは、デジタル署名が本発明において使用されるならば、中央サーバーはデジタル署名を生成するために安全鍵を使用し、デジタル署名を評価するためにワイヤレス装置上に鍵をインストールする。安全鍵を使用することにより、ワイヤレス装置は、当該デジタル署名が詐欺師によってではなく中央サーバーによって生成されたという高いレベルの信頼度を有することになる。

【００４０】

アプリケーションがワイヤレス装置上でエラーを引き起こすならば、あるいは他の望ましい理由により、ワイヤレス装置はアプリケーションの除去を開始する。さらに、アプリケーションは、ＡＤＳまたは中央サーバーからの要求に基づいてワイヤレス装置から除去される。サーバーからのこの要求は任意の所望の理由により開始される。例えば、サーバーは、アプリケーションが他の装置上で正当に実行されなかった、新たなバージョンのアプリケーションが配布された、アプリケーションは除去すべきであることを指示するビジネス上の理由により、アプリケーションをワイヤレス装置から除去することを開始する。このアプリケーションの除去処理はさらに、不正な及び／又は破壊的なアプリケーションが反復して実行されることからワイヤレス装置環境を保護する。

【００４１】

図３は、アプリケーション配布システムが本発明の例示的な実施形態において実施されるワイヤレスネットワークアーキテクチャを示す。中央サーバー３０２は、それ自身あるいは認証サーバーと組み合わせて規定組のプログラミング標準または規約と両立するアプリケーションプログラムを認証するエンティティである。上記したように、これらのプログラミング標準は、当該アプリケーションがＢＲＥＷ（商標）プラットフォームなどのソフトウェアプラットフォーム上で実行されるように確立される。

【００４２】

一実施形態において、中央サーバーデータベース３０４は、ネットワーク３００内の各ワイヤレス装置３３０へ随時ダウンロードされる各アプリケーションプログラムに対する識別と、アプリケーションプロトコルをダウンロードした個人のための電子サービス番号（“ＥＳＮ”）、当該アプリケーションプログラムを運ぶワイヤレス装置３３０に対して独自の移動体識別番号（“ＭＩＮ”）の記録からなる。一方、中央サーバーデータベース３０４は、ワイヤレス装置モデルのネットワーク３００内の各ワイヤレス装置３３０、ワイヤレスネットワークキャリア、ワイヤレス装置３３０が使用される領域、さらにどのワイヤレス装置３３０がどのアプリケーションプログラムを有しているかを識別するのに有効な他の任意の情報に対する記録を含む。加えて、中央サーバーデータベースは、アプリ

ケーションに関連するこの開発者識別情報を記憶している。

【００４３】

一実施形態において、中央サーバー３０２は、除去コマンドソース３２２を含む。除去コマンドソース３２２は、１つまたはそれ以上の目標アプリケーションプログラムを除去するための決定を行う人またはエンティティである。除去コマンドソース３２２は、目標のアプリケーションプロトコルを運ぶ識別されたワイヤレス装置３３０に一斉放送する除去コマンド３１６（後述する）を構成するエンティティでもある。一方、除去コマンドソース３２２は制限無しに、開発及び目標アプリケーションプログラムの発行に関わった一人またはそれ以上の人またはエンティティ、ワイヤレス装置３３０の製造に関わった人またはエンティティ、及び／または、ネットワーク３００の一部の機能に関わった人またはエンティティである。

【００４４】

中央サーバー３０２は、好ましくは安全性が確保されたインターネット等のキャリアネットワーク３１０と通信する。キャリアネットワーク３１０はインターネット及びごくありきたりの電話システム（ＰＯＴＳ）（図３において３１１として略称される）によってＭＳＣ３１２と通信する。キャリアネットワーク３１０及びＭＳＣ３１２間のインターネット接続３１１はデータを転送し、ＰＯＴＳ３１１は音声情報を転送する。ＭＳＣ３１２はインターネット３１１（データ転送用）及びＰＯＴＳ３１１（音声情報用）によってＢＴＳに接続されている。ＢＴＳ３１４は、短いメッセージ提供サービス（“ＳＭＳ“）または他のオーバザエア方法によってメッセージをワイヤレスでワイヤレス装置３３０に送信する。

【００４５】

本発明におけるＢＴＳ３１４によって送信されたメッセージの一例は除去コマンド３１６である。以下にさらに説明するように、ワイヤレス装置３３０は除去コマンド３１６を受信することに応答して、ワイヤレス装置３３０上に記憶された目標のアプリケーションプログラムをアンインストールすることによって応答する。一実施形態において、除去プログラムは目標アプリケーションプログラムを付加的にあるいは代替的にデセーブルするべくプログラムされているか異なる方法で実行させるためにそれを再プログラムする。ワイヤレス装置はアプリケーション及び許可リスト等の関連する情報を削除する。

【００４６】

除去コマンド３１６は、（目標のアプリケーションプログラムの除去を開始するための決定を行った同じ人またはエンティティであるかまたはそうではない）除去コマンドソース３２２によって構成される。除去コマンド３１６はワイヤレス装置３３０に一斉放送するためにネットワーク３００を介して除去コマンドソース３２２によって送信される。

【００４７】

上記の実施形態において記述された除去コマンドを使用することによって、アプリケーション配布及び実行の安全性は、不正なあるいは望ましくないアプリケーションをアンインストールするための機構を提供することによって増大される。中央サーバーによって開始される除去コマンドについて説明したが、ワイヤレス装置がアプリケーションの除去あるいはアンインストールを開始する。

【００４８】

同様にして、上記のネットワークは、アプリケーション、許可リストをＭＳＣ及びＢＴＳを介してワイヤレス装置３３０に対するＭＳＣ及びＢＴＳを介して中央サーバーから種々のサーバー３０６に送信するのに使用される。

【００４９】

図４は、ワイヤレス装置と本発明の例示的な実施形態における内部要素を示す。この実施形態は一例としてワイヤレス装置４００に向けられているがこれに制限されることはない。本発明は、パーソナルデジタルアシスタント（“ＰＤＡ”）、ワイヤレスモデム、ＰＣＭＣＩＡカード、アクセス端末コンピュータ、ディスプレイまたはキーパッドの無い装置、あるいはそれらの任意のコンビネーションまたはサブコンビネーションなどの、ワイ

ヤレス及び非ワイヤレス装置を制限無しに含む、ネットワークを介して通信可能な任意の形態の遠隔モジュール上で実行される。遠隔モジュールのこれらの例は、キーパッド、ビジュアルディスプレイあるいはサウンドディスプレイなどの、ユーザインタフェースを備えている。

【００５０】

図４に示されるワイヤレス装置４００は、ワイヤレス装置４００が製造されたときにインストールされた特定用途向け集積回路（“ＡＳＩＣ”）４１５を有する。ＡＳＩＣはＡＳＩＣ内に含まれるソフトウェアにより駆動されるハードウェア要素である。アプリケーションプログラミングインタフェース（“ＡＰＴ”）４１０は製造のときにワイヤレス装置４００内にインストールされる。一実施形態において、ＡＰＩ４１０はＢＲＥＷ ＡＰＩまたはソフトウェアプラットフォームを表す。ＡＰＩ４１０はＡＳＩＣとやり取りを行うように構成されたソフトウェアプログラムである。ＡＰＩ４１０はＡＳＩＣ４１５ハードウェアとワイヤレス装置４００上にインストールされた（以下に説明する）アプリケーションプログラム間のインタフェースとして機能する。一方、ワイヤレス装置４００は、プログラムがワイヤレス装置４００のハードウェア構成と両立する方法で動作することを可能にする任意の他の形態の回路を含む。ワイヤレス装置４００は記憶装置４０５を有する。記憶装置４０５はＲＡＭ及びＲＯＭからなるが、これに限定されず、ＥＰＲＯＭ、ＥＥＰＲＯＭあるいはフラッシュカードインサート等の任意の形態のメモリである。

【００５１】

ワイヤレス装置の記憶エリア４０５は受信されたアプリケーション及び許可リスト４２５を記憶するのに使用される。加えて、記憶エリア４０５は、１つまたはそれ以上の“鍵”４０５を記憶するのに使用される。これらの鍵は、署名された情報が変更されたかどうかを決定するための署名アルゴリズムを使用するデジタル署名に適用可能である。

【００５２】

規則４３５は、ワイヤレス装置４００上にインストールされる。これらの規則は、アプリケーションが実行を許可されたか否かを決定するための許可リストに関連して使用される。例えば、認証フラグが許可リスト内でセットされている（すなわちアプリケーションが認証をパスした）ならばアプリケーションは実行を許可される、と記載した規則が考えられる。許可リストは、それが認証をパスしたか否かによってセットあるいはセットされない状態の認証フラグをもつ。規則を許可リスト内に含まれる情報に適用することによって、アプリケーションを実行するための許可が認可あるいは否定される。

【００５３】

ワイヤレス装置４００の製造者（図示せず）は、ワイヤレス装置４００が製造されたときにアプリケーションプログラムをワイヤレス装置４００の記憶装置４０５にダウンロードする。これらのアプリケーションプログラムは、ゲーム、本あるいは任意のタイプのデータあるいはソフトウェアプログラムなどの、ワイヤレス装置のユーザに役立つあるいはユーザを楽しませる可能性のある任意のプログラムである。アプリケーションプログラムはまた、ワイヤレス装置が製造された後にエアインタフェースを介してワイヤレス装置４００にダウンロードされる。

【００５４】

除去プログラムはワイヤレス装置４００によって実行されるときに、ワイヤレス装置４００上に記憶されたアプリケーションの１つから１つまたはそれ以上の目標アプリケーションプログラムをアンインストールする。目標のアプリケーションプログラムは、以下に述べる種々の理由のためにワイヤレス装置４００からアンインストールされる必要があるアプリケーションプログラムである。

【００５５】

ワイヤレス装置４００は製造者によりインストールされたローカルデータベース４２０を有する。ワイヤレス装置のＡＰＩはローカルデータベース４２０を自動的に更新するようにプログラムされている。アプリケーションプログラムの各々についての情報を識別する記録はワイヤレス装置４００に記憶されている。ローカルデータベース４２０はワイヤ

レス装置４０２に記憶された各アプリケーションプログラムに対して独自の署名識別の記録を含む。さらに、ローカルデータベース４２０は、ワイヤレス装置４００上の記憶装置４２０内のアプリケーションプログラムの位置の記録と、どのアプリケーションプログラムがワイヤレス装置４００にダウンロードされたか、それらはどこに存在するかを追跡するのに使用可能な他の任意の情報を含む。

【００５６】

図５は、デジタル署名を生成するのに用いられ、本発明の例示的な実施形態におけるワイヤレス装置に送信される情報を示す。当業者により知られているように、デジタル署名は、デジタルファイルが変更されたか否かを追跡するのに使用される。上記したように、デジタル署名は、文書、アプリケーション、データベース等を含む任意のデジタルファイルに適用可能である。概して、デジタル署名は署名アルゴリズムを使用して、鍵をファイルに適用することによって生成される。このデジタル署名は、ファイル内に含まれる情報を使用して生成される。概して、デジタル署名はファイルとともに受信者に送信される。当該ファイルとデジタル署名の受信者は受信したファイルとデジタル署名に鍵を適用して当該ファイルが受信への送信の間に変更されたか否かを決定する。

【００５７】

デジタル署名を生成及び評価するのに用いられる鍵は、署名者の身元を決定するために使用される。例えば、エンティティによってデジタル署名を生成するために鍵が生成されて安全に保持される。このエンティティはデジタル署名を評価するのに使用可能な対応する鍵を配布可能である。鍵が安全に保持され改竄されていないならば、デジタル署名を評価する受信者は当該情報が変更されたか否かのみならず署名者の身元をも決定することができる。

【００５８】

一方、第３者のエンティティは安全な方法で特別なエンティティのために鍵を生成することができる。したがって、特別な身元に関連した鍵をもつ受信者は、そのエンティティが署名者であったか否かを決定することができる。

【００５９】

本発明の一実施形態において、デジタル署名５１５は、例えば、中央サーバーの鍵（図２を参照）等の署名者の鍵５２５、アプリケーション５００、許可リスト５０５、デジタル署名アルゴリズム５３０に入力されるときの開発者身元情報５１０を使用することによって生成される。結果的にデジタル署名５１５が生成されるが、これは入力に含まれる情報に依存する。

【００６０】

デジタル署名５１５を生成した後に、アプリケーション５００、許可リスト５０５、開発者身元情報５１０、デジタル署名５１５はワイヤレス装置５２０に送信される。ワイヤレス装置は次に、アプリケーションの一部または関連する情報（すなわち、許可リスト及び開発者身元情報）が変更されたか否かを決定するために、デジタル署名を使用することができる。さらに、安全鍵などの上記した技術の１つを使用して、ワイヤレス装置は、この情報をワイヤレス装置に送信した署名者の身元を信頼するだろう。

【００６１】

図６は、本発明の例示的な実施形態に一致した方法で、アプリケーションを配布するにあたってサーバー（単一あるいは複数）によって使用されるステップを示すフローチャートである。この例示的な実施形態において、処理はアプリケーションとデジタル署名を受信することによって開始される（ステップＳ６００）。デジタル署名は当該アプリケーションに関連する情報であり、それによって当該アプリケーションが受信前に変更された否かを決定可能である。さらに、エンティティ及びアプリケーションに署名する開発者は割り当てられた鍵を受信した開発者であることを有効にするために、当該デジタル署名に署名するのに使用される鍵は第三者によって割り当てられることが望ましい。

【００６２】

アプリケーションとデジタル署名を受信した後に、デジタル署名は、当該アプリケーシ

ョンを送信した開発者がアプリケーションに署名した者と同一であるか否かを決定するために評価される（ステップＳ６０５）。デジタル署名を生成するために第三者が鍵を開発者に割り当てたならば、第三者は、図２に関して記載された中央サーバーなどの受信者へのデジタル署名を評価するために鍵を割り当てる。

【００６３】

開発者の身元、あるいは署名及び／又はアプリケーションを生成したエンティティは記憶されてアプリケーションに関連付けられる（ステップＳ６１０）。記憶媒体はテーブル、データベースあるいは、開発者の身元が決定される必要が生じたときに後で検索できるような他の方法で記憶される。一実施形態において、開発者の識別の記憶は、ワイヤレス装置内に記憶され、サーバーに記憶されない。

【００６４】

受信したアプリケーションは次に、それが特定の基準を満たすかどうかを決定するために認証される（ステップＳ６１５）。一実施形態において、アプリケーションは、ＱＵＡＬＣＯＭＭ社（カルフォルニア州サンジエゴを本拠とする）により開発され、ワイヤレス装置に使用される、ＢＲＥＷプラットフォームなどの、特定のプラットフォーム上で実行するように記述される。特定のプラットフォームあるいは装置はアプリケーションが装置上で実行される前に満たさなければならない特別な要件をもつ。例えば、プラットフォームあるいは装置は、装置の整合性のあるいはメモリに配置された他のアプリケーションが改竄されないように、アプリケーションが装置内の特定のメモリ位置をアクセスしないことを要求される。これらの基準は特定可能であり、アプリケーションはこれらの基準が満たされるか否かを決定するために試験される。好ましくは、これらの基準は予め決定されて開発者に提供され、アプリケーションの開発に組み込まれる。

【００６５】

認証の後、所定の環境のためにアプリケーションに関連する許可は、割り当てられる（ステップＳ６２０）。許可は、本発明が実行される環境によって多くの要因に基づいて割り当てられる。一実施形態において、割り当て許可は例えば、キャリアネットワーク、ワイヤレス装置の要件、認証試験の結果、開発者、キャリアあるいは他の試験環境に依存する。従って、許可リストの一例は、アプリケーションが認証試験をパスして特定キャリアのネットワーク上で実行されることを示している。

【００６６】

次にサーバーはアプリケーション、許可リスト及び開発者識別にデジタル署名する（ステップＳ６２５）。一実施形態において、この署名は、サーバーの身元がこのデジタル署名された情報の受信者によって決定可能なように、安全鍵を使用して実行される。サーバーによって受信された開発者の署名を行ったり、開発者の署名がワイヤレス装置に送信される必要はない。

【００６７】

アプリケーション、許可リスト、開発者識別及びステップＳ６２５において生成された署名は次にワイヤレス装置に送信される（ステップＳ６３０）。

【００６８】

図７は、本発明の例示的な実施形態に合致した方法にてアプリケーションを実行するときにワイヤレス装置によって使用されるステップを示すフローチャートである。この実施形態において、ワイヤレス装置はアプリケーションに関連した許可を評価するために規則を記憶する（ステップＳ７００）。本発明は規則／許可の実例について説明したが、特定の装置またはプラットフォームのためのアプリケーションに対する許可を認定するのに本発明の範囲内で使用される多くの実例が存在する。

【００６９】

次にワイヤレス装置はアプリケーション、許可リスト、開発者識別及びデジタル署名を受信する（ステップＳ７０５）。一実施形態において、ワイヤレス装置は、署名者を決定するために受信したデジタル署名を評価する。また、デジタル署名はアプリケーション、許可リストあるいは開発者識別が署名後に変更されたか否かを決定するために使用される

。
【００７０】
次に，ワイヤレス装置はアプリケーションを実行するための要求を受信する（ステップＳ７１０）。この要求はプログラムを実行することを要望するワイヤレス装置のユーザからくる。一方、要求は、ワイヤレス装置それ自身あるいはネットワークまたはワイヤレス装置への直接的な接続を介して当該ワイヤレス装置に送信されたいくつかの要求から生成される。
【００７１】
当該要求を受信した後、ワイヤレス装置はデジタル署名及びアプリケーションに関連する許可リストをその実行に先立って評価する（ステップＳ７２０）。上記したように、一実施形態において、ワイヤレス装置は、許可リストを評価するための規則を使用する。デジタル署名を評価することによって、アプリケーション、許可リストあるいは開発者識別が変更されていないと決定されたならば、ワイヤレス装置は記憶された規則を使用して許可リストを評価する。変更がなく、許可リストに対する規則の評価が、当該アプリケーションはワイヤレス装置内での実行に対する許可が得られたことを示したならば、処理は装置腕のアプリケーションの実行に移行する（ステップＳ７３０）。
【００７２】
ステップＳ７２０での評価が、署名の後、アプリケーション、許可リストあるいは開発者識別が変更されたこと、あるいはアプリケーションがワイヤレス装置上での実行に対する許可が否定されたことを示したならば、アプリケーションは実行されない（ステップＳ７２５）。処理はワイヤレス装置からアプリケーションを除去するために移行する（ステップＳ７５０）。許可リスト及び開発者識別はワイヤレス装置から除去されることが望ましい。
【００７３】
ステップＳ７３０に続いて、アプリケーションの実行は、それが違法あるいは不正な動作を行ったか否かを決定するために監視される（ステップＳ７３５）。ワイヤレス装置あるいはワイヤレス装置が使用しているプラットフォームはある種の動作を違法あるいは不正であると規定する。これらの動作は、メモリの制限されたエリアあるいは他のプログラム又はファイルにより使用されるメモリ位置をアクセスすることを含む。さらに、これらの動作は、ワイヤレス装置の資源の有害な使用を含む、これにより、それらはワイヤレス装置に影響を与えるだけでなく、ワイヤレス装置が接続されているネットワーク上の他の装置に影響を与える。
【００７４】
そのような違法あるいは不正な動作が企てられた場合にはアプリケーションの実行は停止され（ステップＳ７４５）、好ましくは、開発者識別及び許可リストとともに、ワイヤレス装置から除去される（ステップＳ７５０）。上記したように、除去処理はアプリケーションの動作停止を含み、それによってその実行を防止してワイヤレス装置上のアプリケーションを保持する。
【００７５】
違法、不正な、あるいは望ましくない動作がステップＳ７３５において実行されるならば、アプリケーションは実行の継続を許可される（ステップＳ７４０）。
【００７６】
結論
変更を認証して検出し、ソース身元を決定し、許可を割り当て、本発明に合致してアプリケーション、システム及び方法を除去する能力を組み込む機構を使用することにより、安全かつソースアプリケーション配布及び実行を増大させる。システム及び方法はこれらの機構の一部またはすべてを実現する。機構がより多く実行されるごとに達成される安全の度合いが高くなる。
【００７７】
一実施形態において、開発者はアプリケーションをサーバーに送信する。開発者は認証

されていない変更に対して保護するために当該アプリケーションに署名する。サーバーは開発者の身元を検査し、アプリケーションに関して認証試験を実行する。サーバーはまた、アプリケーションに対する許可を割り当てて、許可リストを生成する。アプリケーション、許可リスト、開発者識別はサーバーによりデジタル的に署名され、デジタル署名とともにワイヤレス装置に送信される。ワイヤレス装置はアプリケーションを実行する前に、記憶された規則に照らし合わせて変更及び許可リストに対するデジタル署名をチェックする。一実施形態において、これらのチェックは、ワイヤレス装置上でアプリケーションを実行するための各企てに先立って実行される。チェックが、アプリケーションは変更されたか実行するための許可を拒否されたことを示すならば、アプリケーションは実行されずワイヤレス装置から除去される。さらに、アプリケーションが実行中に違法あるいは不正な実行を企てるならば、アプリケーションは停止されてワイヤレス装置から除去される。

【００７８】

本発明の実行の上記の説明は、図示及び説明の目的で提示された。それは完全なものではなく本発明を開示された形態に制限するものではない。変更及び変形が上記教義から可能であり、本発明の実施から獲得される。例えば、記述された実施はソフトウェアを含み、本発明の一実施形態は、ハードウェアとソフトウェアの組み合わせとしてまたはハードウェアのみにより実行される。本発明はオブジェクト指向及び非オブジェクト指向のプログラムシステムにより実行される。加えて、本発明の側面はメモリに記憶されるものとして説明したが、当業者ならばこれらの側面は、ハードディスク、フロッピディスク、あるいはＣＤ－ＲＯＭなどの第２記憶装置、インターネットまたは他の伝達媒体からのキャリアウエーブ、あるいは他の形態のＲＡＭまたはＲＯＭなどの，他のタイプのコンピュータ読み取り可能な媒体に記憶可能であることを認識するであろう。本発明の権利範囲は添付の請求の範囲及びそれらの均等物により規定される。

【図面の簡単な説明】

【００７９】

明細書に組み込まれ、その一部を構成する添付図面は、本発明の現時点で好ましい実施形態を示し、上記の一般的な説明と以下に述べる好ましい実施形態の詳細な説明とともに、本発明の原理を説明する役目をもつ。

【図１】本発明の例示的な実施形態における安全なアプリケーション配布と実行の高レベルプロセスを示すフローチャートである。

【図２】本発明の例示的な実施形態が実施されるシステムアーキテクチャを示すブロック図である。

【図３】安全なアプリケーション配布処理システムが本発明の例示的な実施形態において実施されるワイヤレスネットワークアーキテクチャを示すブロック図である。

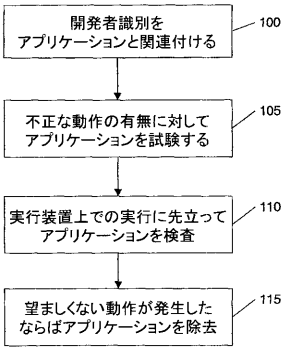
【図４】ワイヤレス装置及び本発明の例示的な実施形態における内部要素を示すブロック図である。

【図５】デジタル署名を生成するのに使用され本発明の例示的な実施形態におけるワイヤレス装置に送信される情報を示すブロック図である。

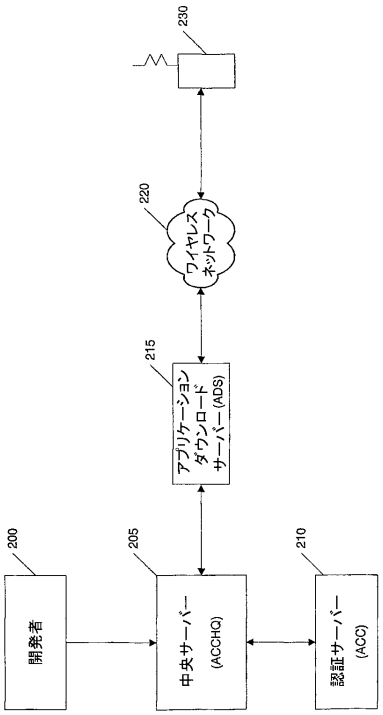
【図６】本発明の例示的な実施形態においてアプリケーションを配布するにあたってサーバーによって使用されるステップを示すフローチャートである。

【図７】本発明の例示的な実施形態においてアプリケーションを実行するときにワイヤレス装置によって使用されるステップを示すフローチャートである。

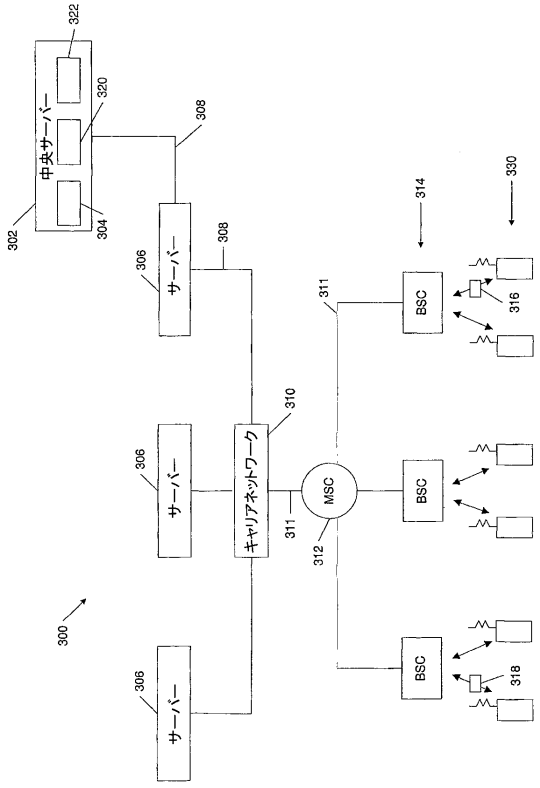
【図１】


開発者識別を
アプリケーションと関連付ける
100
不正な動作の有無に対して
アプリケーションを試験する
105
実行装置上での実行に先立って
アプリケーションを検査
110
望ましくない動作が発生した
ならばアプリケーションを除去
115

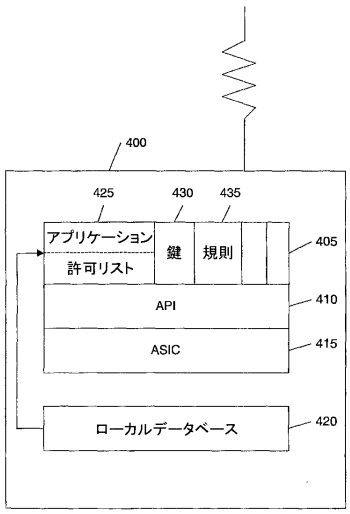
【図２】


230
220
ワイヤレス
ネットワーク
215
アプリケーション
ダウンロード
サーバー (ADS)
200
開発者
205
中央サーバー
(ACCHQ)
210
認証サーバー
(ACC)

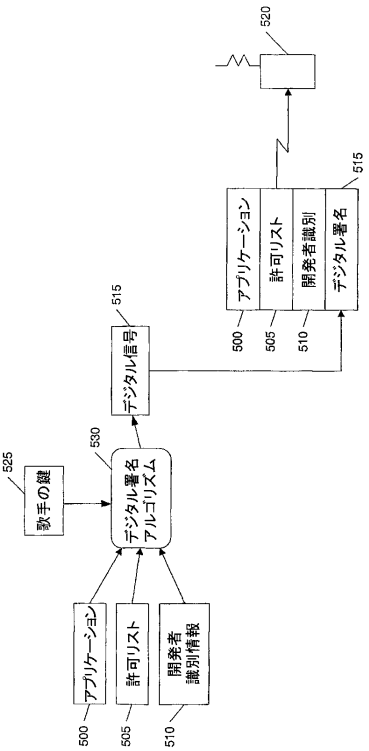
【図３】


322
320
308
中央サーバー
302
304
サーバー
306
308
314
330
311
BSC
316
310
キャリアネットワーク
MSC
311
312
BSC
300
サーバー
306
BSC
318

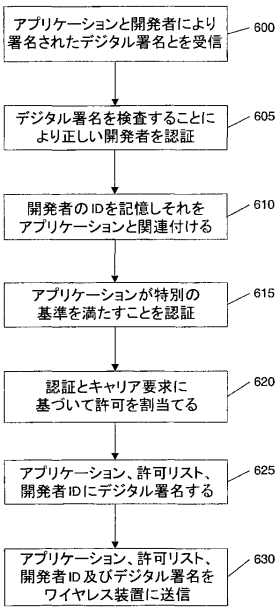
【図４】


400
425
430
435
アプリケーション
許可リスト
鍵
規則
405
API
410
ASIC
415
ローカルデータベース
420

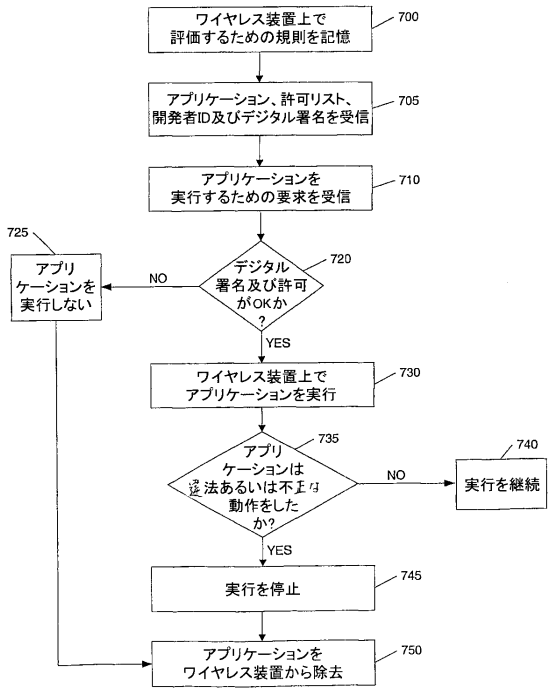
【図５】


520
アプリケーション
許可リスト
開発者識別
デジタル署名
515
500
505
510
デジタル信号
515
525
歌手の鍵
530
デジタル署名アルゴリズム
アプリケーション
許可リスト
開発者識別情報
500
505
510

【図６】


アプリケーションと開発者により署名されたデジタル署名とを受信
600
デジタル署名を検査することにより正しい開発者を認証
605
開発者のIDを記憶しそれをアプリケーションと関連付ける
610
アプリケーションが特別の基準を満たすことを認証
615
認証とキャリア要求に基づいて許可を割当てる
620
アプリケーション、許可リスト、開発者IDにデジタル署名する
625
アプリケーション、許可リスト、開発者ID及びデジタル署名をワイヤレス装置に送信
630

【図７】


ワイヤレス装置上で評価するための規則を記憶
700
アプリケーション、許可リスト、開発者ID及びデジタル署名を受信
705
アプリケーションを実行するための要求を受信
710
725
アプリケーションを実行しない
NO
デジタル署名及び許可がOKか？
720
YES
ワイヤレス装置上でアプリケーションを実行
730
735
アプリケーションは違法あるいは不正な動作をしたか?
NO
740
実行を継続
YES
実行を停止
745
アプリケーションをワイヤレス装置から除去
750

フロントページの続き

(74)代理人 100075672
弁理士 峰 隆司
(74)代理人 100095441
弁理士 白根 俊郎
(74)代理人 100084618
弁理士 村松 貞男
(74)代理人 100103034
弁理士 野河 信久
(74)代理人 100119976
弁理士 幸長 保次郎
(74)代理人 100153051
弁理士 河野 直樹
(74)代理人 100140176
弁理士 砂川 克
(74)代理人 100100952
弁理士 風間 鉄也
(74)代理人 100101812
弁理士 勝村 紘
(74)代理人 100070437
弁理士 河井 将次
(74)代理人 100124394
弁理士 佐藤 立志
(74)代理人 100112807
弁理士 岡田 貴志
(74)代理人 100111073
弁理士 堀内 美保子
(74)代理人 100134290
弁理士 竹内 将訓
(74)代理人 100127144
弁理士 市原 卓三
(74)代理人 100141933
弁理士 山下 元
(72)発明者 ランドブレード、ローレンス
アメリカ合衆国、カリフォルニア州 ９２１１７、サン・ディエゴ、ノーガタック ３０６２
(72)発明者 フィリップス、マーク・エス
アメリカ合衆国、カリフォルニア州 ９２１１７、サン・ディエゴ、グロス・ベンター・アベニュー ４００８
(72)発明者 ミニア、ブライアン
アメリカ合衆国、カリフォルニア州 ９２１２８、サン・ディエゴ、フォンタネレ・プレイス １３７０４
(72)発明者 ジュアン、ヤン
アメリカ合衆国、カリフォルニア州 ９２１２６、サン・ディエゴ、ナンバー１２０、ジェイド・コースト・ロード ８２２３
(72)発明者 クリシュナン、アナンド
アメリカ合衆国、カリフォルニア州 ９２１２８、サン・ディエゴ、ソルボンヌ・コート １３７７５
(72)発明者 スプリッグ、スティーブン・エー
アメリカ合衆国、カリフォルニア州 ９２０６４、ポウェイ、トラバーティン・コート １２１２

４
(72)発明者　クメイテッリ、マゼン
アメリカ合衆国、カリフォルニア州　９２１１０、サン・ディエゴ、ナンバー・ジー、リンウッド・ストリート　１７５３
(72)発明者　オリバー、ミッチェル
アメリカ合衆国、カリフォルニア州　９２１３１、サン・ディエゴ、カミニト・スエルト　９７３７
(72)発明者　ホレル、ジェラルド
カナダ国、ブリティッシュ・コロンビア州　ブイ８エム２エイチ５、ブレントウッド・ベイ、トリン・ロード　６５００
(72)発明者　クロスランド、カレン
アメリカ合衆国、カリフォルニア州　９２１２２、サン・ディエゴ、メイナード・ストリート　５０４４

合議体
審判長　吉岡　浩
審判官　▲吉▼田　美彦
審判官　石井　茂和

(56)参考文献　特開平６－１０３０５８（ＪＰ，Ａ）
関、外３名，”暗号を利用した新しいソフトウェア流通形態の提案　”，情報処理学会研究報告，日本，（社）情報処理学会，１９９３年７月２０日，第９３巻、第６４号（９３－ＩＳ－４５），第１９～２８頁

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F9/06,H04B7/26