(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2017-174452
(P2017-174452A)
(43)公開日　平成29年9月28日(2017.9.28)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 9/445	(2006.01)	G06F	9/06	610Q	5B084
G06F 21/12	(2013.01)	G06F	9/06	640A	5B376
G06F 21/33	(2013.01)	G06F	21/12	310	
G06F 21/62	(2013.01)	G06F	21/33		
G06F 13/00	(2006.01)	G06F	21/62	318	

審査請求 有　請求項の数 20　ＯＬ　（全 45 頁）　最終頁に続く

(21)出願番号　特願2017-98391 (P2017-98391)
(22)出願日　平成29年5月17日 (2017.5.17)
(62)分割の表示　特願2016-505456 (P2016-505456)の分割
原出願日　平成25年10月10日 (2013.10.10)
(31)優先権主張番号　61/806,577
(32)優先日　平成25年3月29日 (2013.3.29)
(33)優先権主張国　米国 (US)
(31)優先権主張番号　61/856,930
(32)優先日　平成25年7月22日 (2013.7.22)
(33)優先権主張国　米国 (US)
(31)優先権主張番号　14/015,108
(32)優先日　平成25年8月30日 (2013.8.30)
(33)優先権主張国　米国 (US)

(71)出願人　397074301
サイトリックス　システムズ，インコーポレイテッド
アメリカ合衆国　フロリダ　３３３０９，フォート　ローダーデール，　ウエスト　サイプレス　クリーク　ロード　８５１
(74)代理人　110002310
特許業務法人あい特許事務所
(72)発明者　バットソン，ケヴィン
アメリカ合衆国，フロリダ州　３３３０９，フォート　ローダーデール，ウエスト　サイプレス　クリーク　ロード　８５１，サイトリックス　システムズ，インコーポレイテッド内

最終頁に続く

(54)【発明の名称】企業アプリケーションストアの提供

(57)【要約】　（修正有）
【課題】より効率的な制御が行えるアプリケーションストアを提供する方法、システムおよびコンピュータ読取可能媒体を提供する。
【解決手段】ソフトウェアアプリケーションを求める要求をアプリケーションストアにおいて受信し、シングルサインオンクレデンシャルに基づいて前記ソフトウェアアプリケーションを前記アプリケーションストアにおいて構成し、前記構成済みソフトウェアアプリケーションを前記シングルサインオンクレデンシャルに関連した少なくとも一つの受信者装置に前記アプリケーションストアにより提供する方法であって、前記ソフトウェアアプリケーションを構成するステップは、前記シングルサインオンクレデンシャルに基づいて一つ以上のユーザ固有の設定を確立するステップを含み、前記ソフトウェアアプリケーションは少なくとも一つのリソースにアクセスすべく構成されている。
【選択図】図５

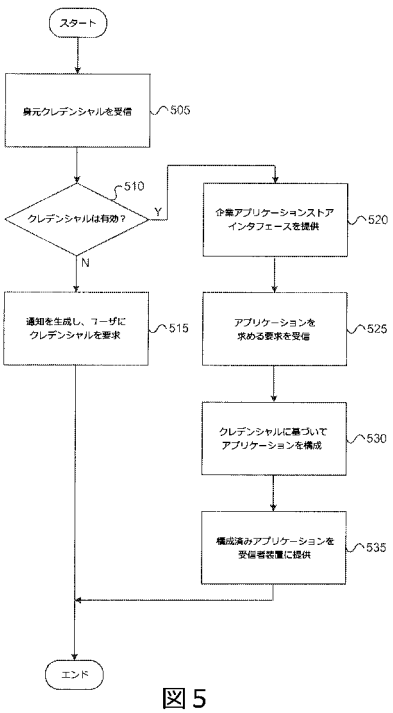

図５

【特許請求の範囲】
【請求項１】
少なくとも一つのアプリケーションに対する更新済みポリシー情報を求めるポリシーエージェントからの要求をアプリケーションストアにおいて受信するステップと、
前記要求を受信したことに応じて、前記アプリケーションストアに用意されているモバイルサービス管理インターフェイスを通した入力に基づいて前記アプリケーションストアにおいて維持され、かつ生成されるポリシー情報に基づいて、前記少なくとも一つのアプリケーションに対する一つまたはそれ以上のポリシーが更新されたか否かを前記アプリケーションストアにおいて判定するステップと、
前記少なくとも一つのアプリケーションに対する前記一つまたはそれ以上のポリシーが更新された旨の判定に基づいて、少なくとも一つのポリシーの更新を前記ポリシーエージェントに提供するステップと、
第１のアプリケーションに対するポリシーの変更を前記アプリケーションストアにおいて受信するステップと、
前記第１のアプリケーションが一または複数のデバイス上に存在している旨を判定するステップと、
前記ポリシーの変更に関連した情報を前記一または複数のデバイスに提供するステップとを含む、方法。
【請求項２】
前記少なくとも一つのアプリケーションに対する前記一つまたはそれ以上のポリシーが更新されていない旨の判定に基づいて、更新データが入手不可能である旨を前記ポリシーエージェントに通知するステップをさらに備える、請求項１に記載の方法。
【請求項３】
更新済みポリシー情報を求める前記要求はラップ済みアプリケーションの実行時に前記ポリシーエージェントから受信される、請求項１に記載の方法。
【請求項４】
前記一または複数のデバイス上において前記第１のアプリケーションに加えて一つまたはそれ以上の他のアプリケーションに対する一つまたはそれ以上のポリシーの更新が入手可能であるか否かを判定するステップと、
前記一つまたはそれ以上の他のアプリケーションに対する一つまたはそれ以上のポリシーの更新が入手可能である旨の判定に基づいて、前記一つまたはそれ以上の他のアプリケーションに対する前記一つまたはそれ以上の入手可能なポリシーの更新を前記一または複数のデバイスに提供するステップとをさらに備える、請求項１に記載の方法。
【請求項５】
前記第１のアプリケーションが前記一または複数のデバイス上に存在している旨の判定は、前記アプリケーションストアに関連した一つまたはそれ以上のユーザ鍵付きのアプリケーションのダウンロード記録に基づく、請求項１に記載の方法。
【請求項６】
前記ポリシーエージェントはモバイルデバイス管理ポリシー強制適用エージェントである、請求項１に記載の方法。
【請求項７】
前記ポリシーエージェントは、前記前記少なくとも一つのアプリケーション上の一または複数のポリシーを適用するように設定されている前記少なくとも一つのアプリケーションに対するアプリケーションラッパである、請求項１に記載の方法。
【請求項８】
前記アプリケーションストアは、前記少なくとも一つのアプリケーションの互いに異なるユーザのために異なったポリシーを維持している、請求項１に記載の方法。
【請求項９】
前記一つまたはそれ以上のポリシーのうちの少なくとも一つのポリシーが、１つまたはそれ以上の所定の条件下で、一または複数の特定の企業リソースへのアクセスをできなく

するように設定されている、請求項８に記載の方法。
【請求項１０】
前記モバイルサービス管理インターフェイスは、少なくとも一人の管理者ユーザがアプリケーションストアで入手可能な一または複数のアプリケーションに適用される一または複数のポリシーを定義することを許容するように構成された一または複数の制御を含み、
前記アプリケーションストアは、前記アプリケーションストアを配置した企業に特有の一または複数の側面を含む企業アプリケーションストアインターフェイスを提供するように構成され、
前記一または複数の側面は、当該企業に属する企業のユーザによって選ばれた一または複数のアプリケーションのリストを含む、請求項１に記載の方法。
【請求項１１】
前記第１のアプリケーションに対するポリシーの変更は、前記少なくとも一人の管理者ユーザから、前記モバイルサービス管理インターフェイスを介して受信される、請求項１０に記載の方法。
【請求項１２】
前記アプリケーションラッパは、保護されたネットワーク資源への認証のためのクライアント証明書の使用をサポートするように設定され、前記アプリケーションラッパは、前記少なくとも一つのアプリケーションのためにネットワークアクセスを統制するように、さらに設定されている、請求項７に記載の方法。
【請求項１３】
少なくとも一つのプロセッサと、
前記少なくとも一つのプロセッサにより実行されると、
少なくとも一つのアプリケーションに対するポリシーエージェントからの更新済みポリシー情報を求める要求をアプリケーションストアにおいて受信し、
前記要求を受信したことに応じて、前記アプリケーションストアに用意されているモバイルサービス管理インターフェイスを介した入力に基づいて前記アプリケーションストアによって維持され、かつ生成されるポリシー情報に基づいて、前記少なくとも一つのアプリケーションに対する一つまたはそれ以上のポリシーが更新されたか否かを前記アプリケーションストアにおいて判定し、
前記少なくとも一つのアプリケーションに対する前記一つまたはそれ以上のポリシーが更新された旨の判定に基づいて、少なくとも一つのポリシーの更新を前記ポリシーエージェントに提供し、
第１のアプリケーションに対するポリシーの変更を前記アプリケーションストアにおいて受信し、
前記第１のアプリケーションが一または複数のデバイス上に存在している旨を判定し、
前記ポリシーの変更に関連した情報を前記一または複数のデバイスに提供する、
各動作を実行させるコンピュータ読取可能命令を記憶するメモリとを備える、装置。
【請求項１４】
前記メモリは、前記少なくとも一つのプロセッサにより実行されると前記装置にさらに、
前記少なくとも一つのアプリケーションに対する前記一つまたはそれ以上のポリシーが更新されていない旨の判定に基づいて、更新データが入手不可能である旨を前記ポリシーエージェントに通知させる、追加のコンピュータ読取可能命令を記憶する、請求項１３に記載の装置。
【請求項１５】
前記ポリシーエージェントからの更新済みポリシー情報を求める前記要求は、ラップ済みアプリケーションの実行時に受信される、請求項１３に記載の装置。
【請求項１６】
前記メモリは、前記少なくとも一つのプロセッサにより実行されると前記装置にさらに、

前記一または複数のデバイス上において前記第１のアプリケーションに加えて一つまたはそれ以上の他のアプリケーションに対して一つまたはそれ以上のポリシーの更新が入手可能であるか否かを判定させ、
前記一つまたはそれ以上のポリシーの更新が入手可能である旨の判定に基づいて、前記一つまたはそれ以上の他のアプリケーションに対する前記一つまたはそれ以上の入手可能なポリシーの更新を前記一または複数のデバイスに提供させる、追加のコンピュータ読取可能命令を記憶する、請求項１３に記載の装置。
【請求項１７】
前記第１のアプリケーションが前記一または複数のデバイス上に存在している旨の判定は、前記アプリケーションストアに関連した一つまたはそれ以上のユーザ鍵付きアプリケーションダウンロードの記録に基づく、請求項１３に記載の装置。
【請求項１８】
前記ポリシーエージェントは、モバイルデバイス管理ポリシーの強制適用エージェントである、請求項１３に記載の装置。
【請求項１９】
前記ポリシーエージェントは、前記少なくとも一つのアプリケーションに対するアプリケーションラッパである、請求項１３に記載の装置。
【請求項２０】
実行されると少なくとも一つの計算装置に、
少なくとも一つのアプリケーションに対する更新済みポリシー情報を求めるポリシーエージェントからの要求をアプリケーションストアにおいて受信し、
前記要求を受信したことに応じて、前記アプリケーションストアに用意されているモバイルサービス管理インターフェイスを通した入力に基づいて前記アプリケーションストアによって維持され、かつ生成されるポリシー情報に基づいて、前記少なくとも一つのアプリケーションに対する一つまたはそれ以上のポリシーが更新されたか否かを前記アプリケーションストアにおいて判定し、
前記少なくとも一つのアプリケーションに対する前記一つまたはそれ以上のポリシーが更新された旨の判定に基づいて、少なくとも一つのポリシーの更新を前記ポリシーエージェントに提供し、
第１のアプリケーションに対するポリシーの変更を前記アプリケーションストアにおいて受信し、
前記第１のアプリケーションが一または複数のデバイス上に存在している旨を判定し、
前記ポリシーの変更に関連した情報を前記一または複数のデバイスに提供する、
各動作を実行させる命令を記憶する一つまたはそれ以上の不揮発性コンピュータ読取可能媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明はコンピュータのハードウェアおよびソフトウェアに関するものである。特に、本発明の一つ以上の態様は、一般的に、企業アプリケーションストアを提供するためのコンピュータのハードウェアおよびソフトウェアに関する。
【背景技術】
【０００２】
企業および組織は、近年ますます、スマートフォン、タブレットコンピュータおよび他のモバイルコンピューティングデバイス等のモバイルデバイスを、自社の従業員および他の関係者に提供し、および／または使用可能にしている。これらのデバイスの人気が高まり続け、増大した数の機能が提供されるにつれて、多くの組織が、これらのデバイスがいかに使用できるか、これらのデバイスがどのようなリソースにアクセスできるか、および、これらのデバイスで実行されるアプリケーションがいかに他のリソースと相互作用できるか、について、一定の管理をしたいと考えるであろう。

【発明の概要】
【発明が解決しようとする課題】
【０００３】
本発明の様々な態様は、モバイルデバイスをどのように使用できるか、モバイルデバイスがどのようなリソースにアクセスできるか、および、これらのデバイスで実行されるアプリケーションおよび他のソフトウェアがどのように他のリソースと相互作用できるか、について制御する、より効率的、効果的、機能的、および便利な方法を提供する。
【課題を解決するための手段】
【０００４】
より詳しく以下に説明される一つ以上の実施形態において、これらおよび特徴を提供することができる企業アプリケーションストアを実装することができる。
【０００５】
本発明のある実施形態によっては、シングルサインオン（ＳＳＯ）機能が企業アプリケーションとともに使用される。例として、ソフトウェアアプリケーションを求める要求が企業アプリケーションストアにおいて受信される。続いて、企業アプリケーションストアにおいて、ＳＳＯクレデンシャルに基づいてソフトウェアアプリケーションが構成される。次に構成済みソフトウェアアプリケーションは企業アプリケーションストアにより、ＳＳＯクレデンシャルに関連した少なくとも一つの受信者デバイスに提供される。
【０００６】
他の実施形態においては、企業アプリケーションストアを介してモバイルデバイス管理機能が提供される。例として、企業アプリケーションストアの管理ユーザの認証クレデンシャル（credential）が企業アプリケーションストアにおいて受信されてもよい。管理ユーザの認証クレデンシャルの有効化に基づいて、モバイルサービス管理インタフェースは企業アプリケーションストアを介して提供されてもよい。その上、モバイルサービス管理インタフェースは、企業アプリケーションストアにおいて入手可能である少なくとも一つのアプリケーションに適用されるべき一つ以上のポリシーを管理ユーザが定義できるように構成された少なくとも一つの制御を含んでいてもよい。
【０００７】
他の実施形態においては、ポリシー更新は企業アプリケーションストアを使用して管理アプリケーションに提供される。例として、少なくとも一つのアプリケーションに対する更新済みポリシー情報を求めるポリシーエージェントからの要求が企業アプリケーションストアにおいて受信されてもよい。要求の受信に基づいて、少なくとも一つのアプリケーションに対する一つ以上のポリシーが更新されたか否かが企業アプリケーションストアにおいて判定されてもよい。少なくとも一つのアプリケーションに対する一つ以上のポリシーが更新された旨の判定に基づいて、少なくとも一つのポリシー更新がポリシーエージェントに提供されてもよい。
【０００８】
これらの特徴は、他の多くの特徴と共に、以下により詳細に検討される。
【０００９】
本発明は、実施形態として示され、添付図面には限定されない図面において、同様の参照符号が類似の要素を示す。
【図面の簡単な説明】
【００１０】
【図１】本発明の１つ以上の実施形態に従って使用されるコンピュータシステムアーキテクチャを示す図である。
【図２】本発明の１つ以上の実施形態に従って使用されるリモートアクセスシステムのアーキテクチャを示す図である。
【図３】本発明の１つ以上の実施形態に従って使用される企業モビリティ管理システムを示す図である。
【図４】本発明の１つ以上の実施形態に従って使用される別の企業モビリティ管理システ

ムを示す図である。
【図５】本発明の一つ以上の実施形態に従って企業アプリケーションストアとともにＳＳＯ機能を使用する方法を説明するためのフローチャートである。
【図６】本発明の一つ以上の実施形態に従って企業アプリケーションストアを介してモバイルサービス管理機能を提供する方法を説明するためのフローチャートである。
【図７】本発明の一つ以上の実施形態に従って企業アプリケーションストアを介してモバイルサービス管理機能を提供する方法を説明するための別のフローチャートである。
【図８】本発明の一つ以上の例示的実施形態に従って企業アプリケーションストアを使用してポリシー更新を管理アプリケーションに提供する方法を説明するためのフローチャートである。
【図９】本発明の一つ以上の実施形態に従って企業アプリケーションストアを使用してポリシー更新を管理アプリケーションに提供する方法を説明するための別のフローチャートである。
【発明を実施するための形態】
【００１１】
様々な実施形態についての以下の記載において、上で特定した添付図面への参照がなされ、それは本願の一部を形成し、そこでは本発明の様々な態様が実践される様々な実施形態が、実施例として示される。
【００１２】
しかし他の実施形態が利用されてもよく、本発明で検討される範囲から逸脱しなければ、構造的および機能的修正がなされてもよい。様々な態様が、他の実施形態の実施を可能とし、実践され、または、様々な異なる方法で実行されることが可能である。
【００１３】
さらに、本発明で使用される語法および用語法は、説明目的であって、限定的とみなされるべきではない。むしろ、本発明で使用される句および用語は、最も広い解釈および意味を与えられるべきである。「含む（including）」、「備える（comprising）」およびその変形の使用は、その後に列挙される項目およびその均等物ならびに追加の項目およびその均等物の包含を意味する。
【００１４】
上述のように、モバイルデバイス管理機能の提供に関する特定の実施形態が、本明細書で検討される。しかしながら、これらの概念のより詳細な検討の前に、本発明の様々な態様の実装および／または別様の提供において使用されてもよいコンピューティングアーキテクチャおよび企業モビリティ管理アーキテクチャのいくつかの実施例が、まず図１～図４を参照して検討される。
【００１５】
〈コンピューティングアーキテクチャ〉
コンピュータソフトウェア、ハードウェアおよびネットワークが、とりわけ、スタンドアローン、ネットワーク接続、リモートアクセス（別名、リモートデスクトップ）、仮想化環境、および／または、クラウドベース環境、を含む様々な異なるシステム環境において利用される。
【００１６】
図１は、スタンドアローンおよび／またはネットワーク接続環境において本明細書で記述される１つ以上の実施形態を実装するために使用される、システムアーキテクチャおよびデータ処理デバイスの一実施例を示す。
【００１７】
様々なネットワークノード１０３，１０５，１０７および１０９が、インターネット等のワイドエリアネットワーク（ＷＡＮ）１０１を介して相互接続されている。プライベートイントラネット、コーポレートネットワーク、ローカルエリアネットワーク（ＬＡＮ）、メトロポリタンエリアネットワーク（ＭＡＮ）、無線ネットワーク、パーソナルネットワーク（ＰＡＮ）等の、他のネットワークが、さらに／あるいは（additionally or alte

rnatively）使用されてもよい。ネットワーク１０１は、例示目的であって、より少ないまたは追加されたコンピュータネットワークで置換されてもよい。ＬＡＮは、１つ以上の任意の公知のＬＡＮトポロジーを有してもよく、イーサネット（登録商標）等の様々な異なる１つ以上のプロトコルを使用してもよい。デバイス１０３，１０５，１０７，１０９および他のデバイス（図示せず）は、ツイステトペア線、同軸ケーブル、光ファイバ、無線波または他の通信媒体を介して１つ以上のネットワークに接続されている。

【００１８】

本明細書で使用され、図面において示される用語「ネットワーク」は、１つ以上の通信パスを介してリモートストレージデバイスが互いに結合されるシステムだけではなく、ストレージ容量を有するようなシステムに随時、結合されるスタンドアローンデバイスをも指す。その結果、用語「ネットワーク」は、「物理ネットワーク」のみならず、全ての物理ネットワークにわたって存在する、単一エンティティに帰するデータからなる「コンテンツネットワーク」をも含む。

【００１９】

コンポーネントは、データサーバ１０３、ウェブサーバ１０５およびクライアントコンピュータ１０７，１０９を含んでいる。データサーバ１０３は、本発明の１つ以上の実施形態を実行するためのデータベースおよび制御ソフトウェアについてのアクセス、制御および管理の全てを提供する。データサーバ１０３は、要求に応じてユーザがデータと相互作用し、データを取得するウェブサーバ１０５へと、接続されている。あるいは、データサーバ１０３は、ウェブサーバ自体として作動してもよく、インターネットに直接接続されてもよい。データサーバ１０３は、直接もしくは間接接続を介して、またはある他のネットワークを介して、ネットワーク１０１（例えばインターネット）を通じてウェブサーバ１０５に接続されていてもよい。

【００２０】

ユーザは、リモートコンピュータ１０７，１０９を使用して、例えばウェブブラウザを使用してデータサーバ１０３と相互作用し、ウェブサーバ１０５によりホストされる外部露出した１つ以上のウェブサイトを介してデータサーバ１０３とやりとりする。クライアントコンピュータ１０７，１０９は、データサーバ１０３と呼応して使用されて、そこに記憶されたデータにアクセスしてもよく、または、他の目的のために使用されてもよい。例えば、この分野で公知のように、インターネットブラウザを使用して、または、コンピュータネットワーク（インターネット等）を介してウェブサーバ１０５および／またはデータサーバ１０３と通信するソフトウェアアプリケーションを実行することにより、ユーザはクライアントデバイス１０７からウェブサーバ１０５にアクセスしてもよい。

サーバおよびアプリケーションは、同一の物理マシン上で組み合わされて、別個の仮想化アドレスまたは論理アドレスを保持してもよく、またそれは別個の物理マシン上に存在してもよい。

【００２１】

図１は、ネットワークアーキテクチャの一実施例を示しているにすぎず、当業者であれば、使用される特定のネットワークアーキテクチャおよびデータ処理デバイスが変更されてもよいこと、さらに本明細書で記述されるように、提供する機能に対して二次的であることを理解するであろう。例えば、ウェブサーバ１０５およびデータサーバ１０３により提供されるサービスは、単一サーバ上で組み合わされてもよい。

【００２２】

各コンポーネント１０３，１０５，１０７，１０９は、公知のコンピュータ、サーバまたはデータ処理デバイスの任意のタイプであってもよい。データサーバ１０３は例えば、データサーバ１０３の全ての動作を制御するプロセッサ１１１を含んでいる。データサーバ１０３は、さらにＲＡＭ１１３、ＲＯＭ１１５、ネットワークインタフェース１１７、入力／出力インタフェース１１９（例えばキーボード、マウス、ディスプレイ、プリンタ等）およびメモリ１２１を含んでいる。

【００２３】

Ｉ／Ｏ１１９は、様々なインタフェースユニット、ならびに、データまたはファイルの読み取り、書き込み、表示および／または印刷を行うドライブを含んでいる。メモリ１２１は、さらにデータ処理デバイス１０３の全ての動作を制御するためのオペレーティングシステムソフトウェア１２３、データサーバ１０３に本発明の態様を実行させるよう命令する制御ロジック１２５、および、本発明の態様とともに使用されても、されなくてもよい、二次的な、サポートおよび／または他の機能を提供する他のアプリケーションソフトウェア１２７をさらに記憶していてもよい。

【００２４】

制御ロジックは、本明細書ではデータサーバソフトウェア１２５と称されることがある。データサーバソフトウェアの機能は、制御ロジックにコード化された規則に基づいて自動的に行われた動作もしくは決定であるか、または、システムへの入力を提供するユーザにより手動でなされた動作または決定であるか、および／またはユーザ入力（例えばクエリ、データ更新等）に基づく自動処理の組み合わせであるかである。

【００２５】

メモリ１２１はまた、第１のデータベース１２９および第２のデータベース１３１を含む、本発明の１つ以上の実施形態の実行において使用されるデータを記憶している。

実施形態によっては、第１のデータベースは、第２のデータベース（例えば、別個のテーブル、レポート等として）を含んでもよい。つまり情報は、システム設計に応じて、単一のデータベースに記憶されることができるし、または、異なる論理、仮想化または物理データベースへと分離されることができる。

【００２６】

デバイス１０５，１０７，１０９は、デバイス１０３に関して記述されたのと同様の、または異なるアーキテクチャを有してもよい。当業者であれば、本明細書で記述されるデータ処理装置１０３（またはデバイス１０５，１０７，１０９）の機能が、複数のデータ処理デバイスに分散されて、例えば複数のコンピュータにわたって処理負荷を分散させ、地理的位置、ユーザアクセスレベル、サービス品質（ＱｏＳ）等に基づいてトランザクションを分離してもよいことを理解するであろう。

【００２７】

１つ以上の態様が、本発明の１つ以上のコンピュータまたは他のデバイスにより実行される、１つ以上のプログラムモジュール等のコンピュータ使用可能または読取可能なデータおよび／またはコンピュータで実行可能な命令において具体化される。

【００２８】

一般的に、プログラムモジュールは、コンピュータまたは他のデバイスにおいてプロセッサにより実行されるときに特定のタスクを実行するか、または、特定の抽出データ型を実装する、ルーチン、プログラム、オブジェクト、コンポーネント、データ構造等を含む。モジュールは、実行のために順次コンパイルされるソースコードプログラミング言語で書かれてもよく、または、（限定されないが）Ｊａｖａ（登録商標）ｓｃｒｉｐｔまたはＡｃｔｉｏｎＳｃｒｉｐｔのようなスクリプト言語で書かれてもよい。

【００２９】

コンピュータで実行可能な命令は、不揮発性ストレージデバイスのようなコンピュータ読取可能媒体上に記憶される。ハードディスク、ＣＤ－ＲＯＭ、光学ストレージデバイス、磁気ストレージデバイス、および／または、これらの任意の組み合わせを含む、任意の適切なコンピュータ読取可能ストレージ媒体が利用されてもよい。さらに、本発明のデータまたはイベントを表す様々な伝送（非ストレージ）媒体が、金属線、光ファイバおよび／または無線伝送媒体（例えば、空中および／または空間）等の信号伝導媒体を介して移動する電磁波形式で、ソースとデスティネーションとの間で伝達されてもよい。

【００３０】

本発明の様々な態様は、方法、データ処理システムまたはコンピュータプログラム製品として具体化される。すなわち、本発明の様々な機能が、ソフトウェア、ファームウェアおよび／またはハードウェア、または、集積回路、フィールドプログラマブルゲートアレ

イ（ＦＰＧＡ）等のハードウェア均等物において、全体として、または、部分的に具体化される。特定のデータ構造が、本発明の１つ以上の態様をより効率的に実装するために使用されてもよく、このようなデータ構造は、本発明のコンピュータ実行可能な命令およびコンピュータ使用可能なデータの範囲内であると考えられる。

【００３１】

さらに図２を参照すると、本発明の１つ以上の態様が、リモートアクセス環境で実装されている。図２は、本発明の１つ以上の実施形態に従って使用されるコンピューティング環境２００においてジェネリックコンピューティングデバイス２０１を含む、実施例としてのシステムアーキテクチャを示す。

【００３２】

ジェネリックコンピューティングデバイス２０１は、クライアントアクセスデバイスに対して仮想化マシンを提供するよう構成された単一サーバまたは複数サーバのデスクトップ仮想化システム（例えば、リモートアクセスまたはクラウドシステム）において、サーバ２０６ａとして使用されている。ジェネリックコンピューティングデバイス２０１は、サーバ、ならびに、ランダムアクセスメモリ（ＲＡＭ）２０５、リードオンリメモリ（ＲＯＭ）２０７、入力／出力（Ｉ／Ｏ）モジュール２０９およびメモリ２１５を含む、その関連コンポーネントの全ての動作を制御するためのプロセッサ２０３を有している。

【００３３】

Ｉ／Ｏモジュール２０９は、ジェネリックコンピューティングデバイス２０１のユーザが入力を提供する、マウス、キーボード、タッチスクリーン、スキャナ、光学リーダおよび／またはスタイラス（または他の入力デバイス）を含んでいてもよく、音声出力を提供するスピーカ、ならびに、テキスト、オーディオビジュアル、および／またはグラフィカル出力を提供するビデオディスプレイデバイスのうちの１つ以上を含んでもよい。

【００３４】

ソフトウェアは、メモリ２１５および／または他のストレージ内に記憶され、ジェネリックコンピューティングデバイス２０１を、本発明の様々な機能を実行するための特別な目的のコンピューティングデバイスへと構成するよう命令をプロセッサ２０３に提供する。例えば、メモリ２１５は、オペレーティングシステム２１７、アプリケーションプログラム２１９および関連するデータベース２２１等の、コンピューティングデバイス２０１により使用されるソフトウェアを記憶している。

【００３５】

コンピューティングデバイス２０１は、ターミナル２４０（クライアントデバイスとも称される）等の１つ以上のリモートコンピュータへの接続をサポートするネットワーク接続環境で動作する。ターミナル２４０は、パーソナルコンピュータ、モバイルデバイス、ラップトップコンピュータ、タブレット、またはジェネリックコンピューティングデバイス１０３または２０１に対して前記の多数または全ての要素を含むサーバであってもよい。

【００３６】

図２に示されたネットワーク接続は、ローカルエリアネットワーク（ＬＡＮ）２２５およびワイドエリアネットワーク（ＷＡＮ）２２９を含むが、他のネットワークも含んでもよい。ＬＡＮネットワーキング環境で使用されるとき、コンピューティングデバイス２０１は、ネットワークインタフェースまたはアダプタ２２３を通じてＬＡＮ２２５に接続される。ＷＡＮネットワーキング環境で使用されるとき、コンピューティングデバイス２０１は、コンピュータネットワーク２３０（例えば、インターネット）等のＷＡＮ２２９を介した通信を確立するためのモデム２２７または他のワイドエリアネットワークインタフェースを含む。示されたネットワーク接続は例示であって、コンピュータ間の通信リンクを確立する他の手段が使用されてもよいことが理解されるであろう。

【００３７】

コンピューティングデバイス２０１および／またはターミナル２４０は、電池、スピーカおよびアンテナ（図示せず）等の様々な他のコンポーネントを含むモバイルターミナル

（例えば、携帯電話、スマートフォン、ＰＤＡ、ノートブック等）であってもよい。
【００３８】
本発明の態様は、幾多の他の汎用目的または特別な目的のコンピューティングシステム環境またはコンフィグレーションで動作する。本発明の態様での使用に適しているであろう、他のコンピューティングシステム、環境および／またはコンフィグレーションの実施例には、限定されないが、パーソナルコンピュータ、サーバコンピュータ、ハンドヘルドまたはラップトップデバイス、マルチプロセッサシステム、マイクロプロセッサベースシステム、セットトップボックス、プログラマブルコンシューマエレクトロニクス、ネットワークＰＣ、ミニコンピュータ、メインフレームコンピュータ、前記のシステムまたはデバイスの任意のものを含む分散コンピューティング環境、等が含まれる。
【００３９】
図２に示すように、１つ以上のクライアントデバイス２４０は、１つ以上のサーバ２０６ａ～２０６ｎ（ここでは一般的にサーバ２０６と称される）と通信する。１つの実施形態において、コンピューティング環境２００は、サーバ２０６とクライアントマシン２４０との間に設置されるネットワークアプライアンスを含んでいる。ネットワークアプライアンスは、クライアント／サーバ接続を管理してもよく、場合によっては、複数のバックエンドサーバ２０６間でクライアント接続をロードバランシング（load balance）できる。
【００４０】
クライアントマシン２４０は、実施形態によっては、単一のクライアントマシン２４０またはクライアントマシン２４０の単一のグループと称されてもよく、サーバ２０６は、単一のサーバ２０６またはサーバ２０６の単一のグループと称されてもよい。１つの実施形態において、単一のクライアントマシン２４０は、２以上のサーバ２０６と通信し、別の実施形態において、単一のサーバ２０６は、２以上のクライアントマシン２４０と通信する。さらに別の実施形態において、単一のクライアントマシン２４０は、単一のサーバ２０６と通信する。
【００４１】
クライアントマシン２４０は、実施形態によっては、以下の非網羅的用語、すなわち、クライアントマシン、クライアント、クライアントコンピュータ、クライアントデバイス、クライアントコンピューティングデバイス、ローカルマシン、リモートマシン、クライアントノード、エンドポイント、またはエンドポイントノード、の任意の１つとして称される。サーバ２０６は、実施形態によっては、以下の非網羅的用語、すなわち、サーバ、ローカルマシン、リモートマシン、サーバファームまたはホストコンピューティングデバイス、の任意の１つとして称される。
【００４２】
１つの実施形態において、クライアントマシン２４０は、仮想化マシンであってもよい。仮想化マシンは任意の仮想化マシンであってもよく、実施形態によっては、仮想化マシンは、タイプ１またはタイプ２ハイパーバイザ、例えば、Ｃｉｔｒｉｘ Ｓｙｓｔｅｍｓ、ＩＢＭ、ＶＭｗａｒｅにより開発されたハイパーバイザまたは任意の他のハイパーバイザにより管理される任意の仮想化マシンであってもよい。ある態様では、仮想化マシンはハイパーバイザにより管理されてよく、また別の態様では、仮想化マシンは、サーバ２０６上で実行するハイパーバイザまたはクライアント２４０上で実行するハイパーバイザにより管理されてもよい。
【００４３】
実施形態によっては、サーバ２０６または他のリモート配置されたマシン上でリモート実行するアプリケーションにより生成されるアプリケーション出力を表示するクライアントデバイス２４０が含まれる。これらの実施形態において、クライアントデバイス２４０は、仮想化マシンクライアントエージェントプログラムまたはアプリケーションを実行して、アプリケーションウィンドウ、ブラウザまたは他の出力ウィンドウにおいて出力を表示する。

【００４４】
一実施例では、アプリケーションは、デスクトップであり、一方、他の実施例では、アプリケーションは、デスクトップを生成または提示するアプリケーションである。デスクトップは、ローカルおよび／またはリモートアプリケーションが統合されることができるオペレーティングシステムのインスタンスのためのユーザインタフェースを提供するグラフィカルシェルを含んでいる。アプリケーションは、ここで使用されるように、オペレーティングシステムのインスタンスが（および任意選択的にデスクトップも）ロードされた後に実行されるプログラムである。
【００４５】
サーバ２０６は、実施形態によっては、リモートプレゼンテーションプロトコルまたは他のプログラムを使用して、データをシンクライアントまたはクライアント上で実行するリモートディスプレイアプリケーションに送信し、サーバ２０６上で実行するアプリケーションにより生成されるディスプレイ出力を提示する。シンクライアントまたはリモートディスプレイプロトコルは、以下のプロトコルの非網羅的リスト、すなわち、フロリダ州フォートローダーデールのＣｉｔｒｉｘ　Ｓｙｓｔｅｍｓ社により開発されたインデペンデントコンピューティングアキテクチャ（ＩＣＡ）プロトコル、または、ワシントン州レドモンドのＭｉｃｒｏｓｏｆｔ社により製造されるリモートデスクトッププロトコル（ＲＤＰ）のうちの任意の１つであることができる。
【００４６】
リモートコンピューティング環境は、２以上のサーバ２０６ａ～２０６ｎを含んでもよく、サーバ２０６ａ～２０６ｎは、例えばクラウドコンピューティング環境において、サーバファーム２０６へと論理的に一緒にグループ化される。サーバファーム２０６は、地理的に分散されるが、論理的に一緒にグループ化されたサーバ２０６、または、互いに近接して配置されるが、論理的に一緒にグループ化されたサーバ２０６を含んでもよい。サーバファーム２０６内の地理的に分散されたサーバ２０６ａ～２０６ｎは、実施形態によっては、ＷＡＮ（ワイド）、ＭＡＮ（メトロポリタン）またはＬＡＮ（ローカル）を使用して通信ができ、異なる地理的領域は、異なる大陸、大陸の異なる領域、異なる国、異なる州、異なる都市、異なるキャンパス、異なる部屋、または前述の地理的位置の任意の組み合わせ、として特徴づけることができる。実施形態によっては、サーバファーム２０６は単一エンティティとして管理されてもよく、一方、他の実施形態において、サーバファーム２０６は複数のサーバファームを含むことができる。
【００４７】
実施形態によっては、サーバファームは、オペレーティングシステムプラットフォーム（例えば、ＷＩＮＤＯＷＳ（登録商標）、ＵＮＩＸ（登録商標）、ＬＩＮＵＸ（登録商標）、ｉＯＳ、ＡＮＤＲＯＩＤ（登録商標）、ＳＹＭＢＩＡＮ等）の実質的に同様のタイプを実行するサーバ２０６を含んでもよい。他の実施形態においては、サーバファーム２０６は、オペレーティングシステムプラットフォームの第１のタイプを実行する１つ以上のサーバの第１のグループ、および、オペレーティングシステムプラットフォームの第２のタイプを実行する１つ以上のサーバの第２のグループを含んでもよい。
【００４８】
サーバ２０６は、必要に応じてサーバの任意のタイプ、例えばファイルサーバ、アプリケーションサーバ、ウェブサーバ、プロキシサーバ、アプライアンス、ネットワークアプライアンス、ゲートウェイ、アプリケーションゲートウェイ、ゲートウェイサーバ、仮想化サーバ、デプロイメントサーバ、ＳＳＬ　ＶＰＮサーバ、ファイアウォール、ウェブサーバ、アプリケーションサーバまたはマスターアプリケーションサーバとして、アクティブディレクトリを実行するサーバ、または、ファイアウォール機能、アプリケーション機能またはロードバランシング機能を提供するアプリケーションアクセラレーションプログラムを実行するサーバ、として構成されることができる。他のサーバタイプが使用されてもよい。
【００４９】

実施形態によっては、クライアントマシン２４０からの要求を受信し、要求を第２のサーバ２０６ｂへ転送し、第２のサーバ２０６ｂからの応答でクライアントマシン２４０により生成された要求に応答する第１のサーバ２０６ａが含まれる。第１のサーバ２０６ａは、クライアントマシン２４０に利用可能なアプリケーションの列挙、および、アプリケーションの列挙によって特定されたアプリケーションをホストするアプリケーションサーバ２０６に関するアドレス情報を取得する。第１のサーバ２０６ａは、ウェブインタフェースを使用してクライアントの要求に対する応答を提示し、直接、クライアント２４０と通信して、特定したアプリケーションへのアクセスをクライアント２４０に提供できる。１つ以上のクライアント２４０および／または１つ以上のサーバ２０６は、ネットワーク２３０、例えばネットワーク１０１を介してデータを送信してもよい。

【００５０】

図２は、例示されたデスクトップ仮想化システムの高レベルアーキテクチャを示す。図示されているように、デスクトップ仮想化システムは、１つ以上のクライアントアクセスデバイス２４０に仮想化デスクトップおよび／または仮想化アプリケーションを提供するよう構成された少なくとも１つの仮想化サーバ２０６を含む、単一サーバまたは複数サーバシステム、またはクラウドシステムであってもよい。

【００５１】

本発明で使用されるように、デスクトップとは、１つ以上のアプリケーションがホストされ、および／または実行されてもよいグラフィカル環境または空間のことを指す。デスクトップは、ローカルおよび／またはリモートアプリケーションが統合されることができるオペレーティングシステムのインスタンスのためのユーザインタフェースを提供するグラフィカルシェルを含んでもよい。

【００５２】

アプリケーションは、オペレーティングシステムのインスタンスが（および任意選択的にデスクトップも）ロードされた後に実行するプログラムを含んでいる。オペレーティングシステムの各インスタンスは、物理的（デバイスにつき１つのオペレーティングシステム）であっても、仮想化（単一デバイス上で実行されるＯＳの複数のインスタンス）であってもよい。各アプリケーションは、ローカルデバイス上で実行されてもよく、または、リモート配置された（例えばリモートされた）デバイス上で実行されてもよい。

【００５３】

〈企業モビリティ管理アーキテクチャ〉

図３は、企業環境、ＢＹＯＤ環境または他のモバイル環境での使用のための企業モビリティアーキテクチャ３００を表す。アーキテクチャは、モバイルデバイス３０２（例えば、クライアント１０７，２１１または別様）のユーザが、企業またはパーソナルリソースにモバイルデバイス３０２からアクセスすること、および、パーソナルユースのためにモバイルデバイス３０２を使用すること、の両方を可能にする。

【００５４】

ユーザは、ユーザにより購入されたモバイルデバイス３０２または企業によりユーザに提供されたモバイルデバイス３０２を使用して、このような企業リソース３０４または企業サービス３０８にアクセスする。ユーザは、ビジネスユースのみのために、または、ビジネスユースおよびパーソナルユースのために、モバイルデバイス３０２を利用してもよい。

【００５５】

モバイルデバイスは、ｉＯＳオペレーティングシステム、Ａｎｄｒｏｉｄ（登録商標）オペレーティングシステムおよび／または同様のものを実行する。企業は、モバイルデバイス３０４を管理するためのポリシーを実装することを選択する。ポリシーは、モバイルデバイスが特定され、安全（secure）にされ、またはセキュリティ検証され、そして、企業リソースへの選択的または完全なアクセスを提供されてもよいように、ファイアウォールまたはゲートウェイを通じて埋め込まれる。ポリシーは、モバイルデバイス管理ポリシー、モバイルアプリケーション管理ポリシー、モバイルデータ管理ポリシー、または、モ

バイルデバイス、アプリケーションおよびデータ管理ポリシーのある組み合わせであってもよい。モバイルデバイス管理ポリシーのアプリケーションを通じて管理されるモバイルデバイス３０４は、エンロールドデバイスと称すことがある。

【００５６】

モバイルデバイスのソフトウェアおよび／またはオペレーティングシステムは管理パーティション５１０と非管理パーティション３１２とに分割されていてもよい。管理パーティション５１０は、自身の上で稼働しているアプリケーションと、自身の内部に記憶されたデータとのセキュリティ保護を行うために適用されるポリシーを有している。管理パーティション上で稼働するアプリケーションはセキュリティ保護アプリケーションであってもよい。セキュリティ保護アプリケーションは電子メールアプリケーション、ウェブ閲覧アプリケーション、サース（ＳａａＳ）アクセスアプリケーション、およびＷｉｎｄｏｗｓ（登録商標）　Ａｐｐｌｉｃａｔｉｏｎ用アクセスアプリケーション等であってもよい。セキュリティ保護アプリケーションは、セキュリティ保護ネイティブアプリケーション３１４、セキュリティ保護アプリケーションランチャ３１８により実行されるセキュリティ保護リモートアプリケーション３２２、およびセキュリティ保護アプリケーションランチャ３１８により実行される仮想化アプリケーション３２６等であってもよい。セキュリティ保護ネイティブアプリケーション３１４はセキュリティ保護アプリケーションラッパ３２０によりラップされてもよい。セキュリティ保護アプリケーションラッパ３２０は、セキュリティ保護ネイティブアプリケーションがモバイルデバイス３０２上で実行されるときにデバイス上で実行される合成ポリシーを含んでいてもよい。セキュリティ保護アプリケーションラッパ３２０は、モバイルデバイス３０２上で稼働するセキュリティ保護ネイティブアプリケーション３１４を、セキュリティ保護ネイティブアプリケーション３１４の実行時に要求されるタスクを完了するのにセキュリティ保護ネイティブアプリケーション３１４が必要としてもよい企業においてホスティングされるリソースに向けるメタデータを含んでいてもよい。

【００５７】

セキュリティ保護アプリケーションランチャ３１８により実行されるセキュリティ保護リモートアプリケーション３２２はセキュリティ保護アプリケーションランチャ３１８の内部で実行されてもよい。セキュリティ保護アプリケーションランチャ３１８により実行される仮想化アプリケーション３２６は、モバイルデバイス３０２上、および企業リソース３０４等においてリソースを利用してもよい。

【００５８】

セキュリティ保護アプリケーションランチャ３１８により実行される仮想化アプリケーション３２６によりモバイルデバイス３０２上で使用されるリソースは、ユーザ対話リソースおよび処理リソース等を含んでいてもよい。ユーザ対話リソースはキーボード入力、マウス入力、カメラ入力、触覚入力、音声入力、視覚入力およびジェスチャ入力等を収集および伝送するのに使用されてもよい。処理リソースは、ユーザインタフェース、および企業リソース３０４から受信した処理データ等を提示するのに使用されてもよい。セキュリティ保護アプリケーションランチャ３１８により実行される仮想化アプリケーション３２６により企業リソース３０４において使用されるリソースは、ユーザインタフェース生成リソースおよび処理リソース等を含んでいてもよい。

【００５９】

ユーザインタフェース生成リソースはユーザインタフェースの組み立て、ユーザインタフェースの修正、およびユーザインタフェースのリフレッシュ等に使用されてもよい。処理リソースは情報の作成、情報の読み込み、情報の更新、および情報の削除等に使用されてもよい。例として、仮想化アプリケーションはＧＵＩに関連したユーザ対話を記録してもよく、サーバアプリケーションがユーザ対話データをサーバ上で作動するアプリケーションへの入力として使用することになるサーバアプリケーションにユーザ対話を伝達してもよい。この構成において、企業はアプリケーションに関連したデータ、ファイル等とともに、サーバ側のアプリケーションを保持することを選択してもよい。

【００６０】
企業はモバイルデバイス上での展開に対していくつかのアプリケーションをセキュリティ保護することによりここでの原理に従ってこれらを「モバイル化」することを選択してもよいし、またこの構成はあるアプリケーションに対して選択されてもよい。たとえば、いくつかのアプリケーションがモバイルデバイス上での使用のためにセキュリティ保護されてもよい一方、他のアプリケーションがモバイルデバイス上での展開のために作成されていない、または展開に適切でなくてもよいため、仮想化技術を通じた未作成アプリケーションへのアクセスをモバイルユーザに提供することを企業は選んでもよい。
【００６１】
別の実施例として、企業は、モバイルデバイスに対してアプリケーションをカスタマイズするのが非常に困難か、または望ましくないような大きく複雑なデータセット（たとえばマテリアルリソースプランニングアプリケーション）を持つ大きく複雑なアプリケーションを有していてもよいため、企業は仮想化技術を通じたアプリケーションへのアクセスを提供することを選んでもよい。また別の実施例として、企業は、セキュリティ保護されたモバイル環境であってもセンシティブであると企業により考えられることがあるセキュリティの高いデータ（たとえば人材データ、顧客データ、技術データ）を保持するアプリケーションを有していてもよいため、企業は仮想化技術を使用してこのようなアプリケーションおよびデータへのモバイルアクセスを許可することを選んでもよい。企業は、モバイルデバイス上の充分にセキュリティ保護されまた充分に機能的なアプリケーションと仮想化アプリケーションとを提供して、サーバ側でより適切に作動すると考えられるアプリケーションへのアクセスを許可することを選んでもよい。ある実施形態において、仮想化アプリケーションはモバイルデバイス上の安全な記憶位置の一つに何らかのデータ、ファイル等を記憶してもよい。例として、企業は、ある情報をデバイス上に記憶することを許可しながら他の情報を許可しないことを選んでもよい。
【００６２】
仮想化アプリケーションに関して、本明細書に記述されるように、モバイルデバイスは、ＧＵＩを提示するよう設計された仮想化アプリケーションを有してもよく、そして、ユーザ相互作用をＧＵＩで記録してもよい。アプリケーションは、ユーザ相互作用をサーバ側に通信し、アプリケーションでのユーザ相互作用としてサーバ側アプリケーションにより使用されてもよい。これに応じて、サーバ側のアプリケーションは、新たなＧＵＩをモバイルデバイスに送信し戻してもよい。例えば、新たなＧＵＩは、静的ページ、動的ページ、アニメーション等である。
【００６３】
管理パーティションで実行中のアプリケーションは、安定化アプリケーションであってもよい。安定化アプリケーションは、デバイスマネージャ３２４によって管理される。デバイスマネージャ３２４は、安定化アプリケーションを監視し、問題を検出および修復する技術を利用してもよく、その問題とは、もし前記問題を検出および修復する技術が利用されなければ、不安定化アプリケーションとなってしまうことを指す。
【００６４】
セキュリティ保護アプリケーションは、モバイルデバイスの管理パーティション５１０において、セキュリティ保護データコンテナ３２８に記憶されたデータにアクセスする。セキュリティ保護データコンテナにおいてセキュリティ保護にされたデータは、セキュリティ保護ラップ化アプリケーション３１４、セキュリティ保護アプリケーションランチャー３２２により実行されるアプリケーション、セキュリティ保護アプリケーションランチャー３２２により実行される仮想化アプリケーション３２６等によりアクセスされる。
【００６５】
セキュリティ保護データコンテナ３２８に記憶されたデータは、ファイルやデータベース等を含んでいる。セキュリティ保護データコンテナ３２８に記憶されたデータは、セキュリティ保護アプリケーション３３２の間で共有され、特定のセキュリティ保護アプリケーション３３０に制限されるデータ等を含んでいる。セキュリティ保護アプリケーション

に制限されるデータは、セキュリティ保護一般データ３３４および高度セキュリティ保護データ３３８を含んでいる。

【００６６】

セキュリティ保護一般データは、ＡＥＳ１２８ビット暗号化等の暗号の強力形態を使用し、一方、高度セキュリティ保護データ３３８は、ＡＥＳ２５４ビット暗号化等の暗号の超強力形態を使用する。セキュリティ保護データコンテナ３２８に記憶されたデータは、デバイスマネージャ３２４からのコマンドの受信時に、デバイスから削除される。セキュリティ保護アプリケーションは、デュアルモードオプション３４０を有している。デュアルモードオプション３４０は、非セキュリティ保護モードでセキュリティ保護アプリケーションを実行するオプションを、ユーザに提示する。

【００６７】

非セキュリティ保護モードでは、セキュリティ保護アプリケーションは、モバイルデバイス３０２の非管理パーティション３１２上の非セキュリティ保護データコンテナ３４２に記憶されたデータにアクセスしてもよい。非セキュリティ保護データコンテナに記憶されたデータは、パーソナルデータ３４４である。非セキュリティ保護データコンテナ３４２に記憶されたデータは、モバイルデバイス３０２の非管理パーティション３１２上で実行中の非セキュリティ保護アプリケーション３４８によりアクセスされる。非セキュリティ保護データコンテナ３４２に記憶されたデータは、セキュリティ保護データコンテナ３２８に記憶されたデータが、モバイルデバイス３０２から削除されるときに、モバイルデバイス３０２に残存してもよい。

【００６８】

企業は、モバイルデバイスから、選択されたまたは全ての、企業により所有、ライセンス化または制御された、データ、ファイルおよび／またはアプリケーション（企業データ）が削除されることを欲してもよく、一方、ユーザにより所有、ライセンス化または制御された、パーソナルデータ、ファイルおよび／またはアプリケーション（パーソナルデータ）を残し、または、別様に保ってもよい。この動作は、選択的ワイプと称すことがある。本開示に記述される態様に従って配置された企業およびパーソナルデータで、企業は、選択的ワイプを実行してもよい。

【００６９】

モバイルデバイスは企業における企業リソース３０４および企業サービス３０８、ならびに公衆インターネット３４８等に接続してもよい。モバイルデバイスは仮想プライベートネットワーク接続（たとえばＩＰＳＥＣ、ＳＳＬ、ＳＯＣＫ５および／またはウェブ転送プロキシ等を利用してもよい）を通じて企業リソース３０４および企業サービス３０８に接続してもよい。仮想プライベートネットワーク接続は特定アプリケーション３５０、特定デバイス、およびモバイルデバイス上の特定セキュリティ保護領域等（たとえば３５２）に固有のものであってもよい。例として、電話機のセキュリティ保護領域における各ラップ済みアプリケーションは、ＶＰＮへのアクセスがアプリケーションに関連した属性に基づいて承諾されるように、場合によってはユーザまたはデバイス属性情報と併せてアプリケーション固有ＶＰＮを通じて企業リソースにアクセスしてもよい。

【００７０】

仮想プライベートネットワーク接続はＭｉｃｒｏｓｏｆｔ Ｅｘｃｈａｎｇｅトラフィック、Ｍｉｃｒｏｓｏｆｔ Ａｃｔｉｖｅ Ｄｉｒｅｃｔｏｒｙマイクロソフトアクティブディレクトリトラフィック、ＨＴＴＰトラフィック、ＨＴＴＰＳトラフィック、およびアプリケーション管理トラフィック等を実行してもよい。仮想プライベートネットワーク接続はＳＳＯ認証処理３５４を支援および有効化してもよい。ＳＳＯ処理は、認証サービス３５８により次に確認されることになる認証クレデンシャルの単一セットをユーザが提供することを許可してもよい。認証サービス３５８は次に、ユーザからのそれぞれの企業リソース３０４への認証クレデンシャルの提供を必要とすることなく複数の企業リソース３０４へのユーザアクセスを承諾してもよい。

【００７１】

仮想化プライベートネットワーク接続は、アクセスゲートウェイ３６０により確立され、管理される。アクセスゲートウェイ３６０は、企業リソース３０４のモバイルデバイス３０２への送達を管理、加速および改善するパフォーマンスを増強させる特徴を含んでいる。アクセスゲートウェイは、モバイルデバイス３０２から公衆インターネット３４８へとトラフィックをリルートしてもよく、モバイルデバイス３０２が、公衆インターネット３４８上で実行される公衆利用可能非セキュリティ保護アプリケーションへアクセスすることを有効化する。

【００７２】

モバイルデバイスは、転送ネットワーク３６２を介してアクセスゲートウェイに接続されてもよい。転送ネットワーク３６２は、有線ネットワーク、無線ネットワーク、クラウドネットワーク、ローカルエリアネットワーク、メトロポリタンエリアネットワーク、ワイドエリアネットワーク、公衆ネットワーク、プライベートネットワーク等である。

【００７３】

企業リソース３０４は電子メールサーバ、ファイル共有サーバ、ＳａａＳアプリケーション、ウェブアプリケーションサーバおよびＷｉｎｄｏｗｓ（登録商標）アプリケーションサーバ等を含んでいる。電子メールサーバはＥｘｃｈａｎｇｅサーバおよびＬｏｔｕｓＮｏｔｅｓサーバ等を含んでいる。ファイル共有サーバはＳｈａｒｅＦｉｌｅサーバ等を含んでいる。ＳａａＳアプリケーションはＳＡＬＥＳＦＯＲＣＥ等を含んでいる。Ｗｉｎｄｏｗｓ（登録商標）アプリケーションサーバは、ローカルＷｉｎｄｏｗｓ（登録商標）オペレーティングシステム等の上で稼働するよう意図されたアプリケーションを提供すべく構築されたいずれのアプリケーションサーバを含んでいる。

【００７４】

企業リソース３０４はプレミスベースのリソース、およびクラウドベースのリソース等である。企業リソース３０４は直接的に、またはアクセスゲートウェイ３６０を通じてモバイルデバイス３０２によりアクセスされる。企業リソース３０４は転送ネットワーク３６２を介してモバイルデバイス３０２によりアクセスされてもよい。転送ネットワーク３６２は有線ネットワーク、無線ネットワーク、クラウドネットワーク、ローカルエリアネットワーク、メトロポリタンエリアネットワーク、ワイドエリアネットワーク、公衆ネットワークおよびプライベートネットワーク等であってもよい。

【００７５】

企業サービス３０８は、認証サービス３５８、脅威検出サービス３６４、デバイスマネージャサービス３２４、ファイル共有サービス３６８、ポリシーマネージャサービス３７０、ソーシャル統合サービス３７２、アプリケーションコントローラサービス３７４等を含んでいる。

【００７６】

認証サービス３５８は、ユーザ認証サービス、デバイス認証サービス、アプリケーション認証サービス、データ認証サービス等を含んでいる。認証サービス３５８は、証明書を使用してもよい。証明書は、企業リソース３０４等によりモバイルデバイス３０２に記憶されてもよい。モバイルデバイス３０２に記憶された証明書は、モバイルデバイス上の暗号化位置に記憶されてもよく、証明書は、認証時の使用等のためにモバイルデバイス３０２上に一時的に記憶されてもよい。

【００７７】

脅威検出サービス３６４は、侵入検出サービス、非許諾アクセス試行検出サービス等を含んでいる。非許諾アクセス試行検出サービスは、デバイス、アプリケーション、データ等へのアクセスの非許諾試行を含んでいる。デバイス管理サービス３２４は、コンフィグレーション、プロビジョニング、セキュリティ、サポート、監視、報告およびデコミッショニングサービスを含んでもよい。ファイル共有サービス３６８は、ファイル管理サービス、ファイルストレージサービス、ファイルコラボレーションサービス等を含んでいる。ポリシーマネージャサービス３７０は、デバイスポリシーマネージャサービス、アプリケーションポリシーマネージャサービス、データポリシーマネージャサービス等を含んでい

る。
【００７８】
ソーシャル統合サービス３７２は、コンタクト統合サービス、コラボレーションサービス、Ｆａｃｅｂｏｏｋ，ＴｗｉｔｔｅｒおよびＬｉｎｋｅｄＩｎ等のソーシャルネットワークとの統合等を含んでいる。アプリケーションコントローラサービス３７４は、管理サービス、プロビジョニングサービス、デプロイメントサービス、アサインメントサービス、リボケーションサービス、ラッピングサービス等を含んでいる。
【００７９】
企業モビリティ技術アーキテクチャ３００はアプリケーションストア３７８を含んでいてもよい。アプリケーションストア３７８は非ラップアプリケーション３８０および事前ラップアプリケーション３８２等を含んでいる。さらに／あるいは、アプリケーションストア３７８はウェブアプリケーション、サース（ＳａａＳ）アプリケーション、仮想化アプリケーションおよび／もしくは他タイプのアプリケーション、ならびに／または他のリソースを含んでいてもよい。アプリケーションはアプリケーション制御部３７４からアプリケーションストア３７８に入力されてもよい。アプリケーションストア３７８はアクセスゲートウェイ３６０または公衆インターネット３４８等を通じてモバイルデバイス３０２によりアクセスされてもよい。アプリケーションストアには直覚的かつ容易に使用できるユーザインタフェースが設けられていてもよい。アプリケーションストア３７８はソフトウェア開発キット３８４へのアクセスを提供してもよい。ソフトウェア開発キット３８４は本明細書に先に述べたようにアプリケーションをラップすることにより、ユーザにより選択されたアプリケーションをセキュリティ保護する能力をユーザに提供する。ソフトウェア開発キット３８４を使用してラップされたアプリケーションは次に、アプリケーション制御部３７４を使用してアプリケーションストア３７８に入力されることによりモバイルデバイス３０２に入手可能にされてもよい。
【００８０】
企業モビリティ技術アーキテクチャ３００は、管理および解析能力を含んでもよい。管理および解析能力は、リソースがどのように使用されるか、リソースがどれくらいの頻度で使用されるか等に関する情報を提供する。リソースは、デバイス、アプリケーション、データ等を含んでもよい。リソースがどのように使用されるかについては、どのデバイスがどのアプリケーションをダウンロードし、どのアプリケーションがどのデータにアクセスするか等を含んでいる。リソースがどれくらいの頻度で使用されるかには、アプリケーションがどれくらいの頻度でダウンロードされたか、データの特定のセットが何回アプリケーションによりアクセスされたか等を含んでいる。
【００８１】
図４に、別の企業モビリティ管理システム４００を示す。図３に関して上述されたモビリティ管理システム３００のコンポーネントのいくつかは、簡明さのために省略されている。図４に示されたシステム４００のアーキテクチャは、図３に関して上述されたシステム３００のアーキテクチャと多くの点で同様であり、上述されない追加の特徴を含んでいる。
【００８２】
この場合、左側には登録されたモバイルデバイス４０２（たとえば一つ以上の管理アプリケーションならびに／またはポリシー管理および強制適用機能を含むモバイルデバイス）が、右側上方に示されるように、ゲートウェイサーバ４０６（アクセスゲートウェイおよびアプリケーション制御部機能を含む）と対話してＥｘｃｈａｎｇｅ、Ｓｈａｒｅｐｏｉｎｔ、リソースＰＫＩ、Ｋｅｒｂｅｒｏｓリソースおよび証明書発行サービス等の様々な企業リソース４０８およびサービス４０９にアクセスするクライアントエージェント４０４とともに提示されている。具体的に示されてはいないが、モバイルデバイス４０２もまたアプリケーションを選択およびダウンロードするために企業アプリケーションストア（たとえばＳｔｏｒｅＦｒｏｎｔ）と対話してもよい。例として、クライアントエージェント４０４は、リモートリソースおよび／または仮想化リソースとの通信を容易にするク

ライアントデバイス上で実行するソフトウェアアプリケーションであってもよい。例として、ゲートウェイサーバ４０６は、企業リソースおよび／またはクラウドリソースへのアクセスを提供するサーバまたは他のリソースであってもよい。

【００８３】

クライアントエージェント４０４は、ＨＤＸ／ＩＣＡ表示リモートプロトコルを使用してアクセスされる、企業データセンターでホストされるＷｉｎｄｏｗｓ（登録商標）アプリ／デスクトップ用ＵＩ（ユーザインタフェース）仲介者として機能する。クライアントエージェント４０４はまた、ネイティブｉＳＯまたはＡｎｄｒｏｉｄ（登録商標）アプリケーション等のモバイルデバイス４０２上におけるネイティブアプリケーションのインストールおよび管理を支援する。例として、上記図面に示す管理アプリケーション４１０（メール、ブラウザ、ラップアプリケーション）はすべてデバイス上で局所的に実行するネイティブアプリケーションである。クライアントエージェント４０４および本アーキテクチャのアプリケーション管理フレームワークは、接続性およびＳＳＯ等の、ポリシーにより駆動される管理能力および特徴を企業リソース／サービス４０８に提供すべく機能する。クライアントエージェント４０４は企業に対する、通常は他のゲートウェイサーバ構成要素に対するＳＳＯを用いてアクセスゲートウェイ（ＡＧ）に対する一次ユーザ認証を処理する。クライアントエージェント４０４はゲートウェイサーバ４０６からポリシーを取得して、モバイルデバイス４０２上における管理アプリケーション４１０の挙動を制御する。

【００８４】

ネイティブアプリケーション４１０およびクライアントエージェント４０４間のセキュリティ保護ＩＰＣリンク４１２は、管理チャネルを表し、これにより、クライアントエージェントが、各アプリケーションを「ラップする」アプリケーション管理フレームワーク４１４により適用されるポリシーを供給することが可能となる。ＩＰＣチャネル４１２はまた、クライアントエージェント４０４が、企業リソース４０８への接続性およびＳＳＯを有効化するクレデンシャルおよび認証情報を供給することを可能とする。最後に、ＩＰＣチャネル４１２は、アプリケーション管理フレームワーク４１４が、オンラインおよびオフライン認証等のクライアントエージェント４０４により実装されるユーザインタフェース機能を起動することを可能とする。

【００８５】

クライアントエージェント４０４およびゲートウェイサーバ４０６間の通信は、本質的に、各ネイティブな管理されたアプリケーション４１０をラップするアプリケーション管理フレームワーク４１４からの管理チャネルの拡張である。アプリケーション管理フレームワーク４１４は、クライアントエージェント４０４からポリシー情報を要求し、一方、クライアントエージェント４０４は、ゲートウェイサーバ４０６からそれを要求する。アプリケーション管理フレームワーク４１４は、認証を要求し、クライアントエージェント４０４は、ゲートウェイサーバ４０６のゲートウェイサービス部分（ＮｅｔＳｃａｌｅｒ Ａｃｃｅｓｓ Ｇａｔｅｗａｙとしても知られる）にログインする。クライアントエージェント４０４は、ゲートウェイサーバ４０６上でサポートサービスも呼び出してもよく、これにより、以下でさらに完全に説明されるように、ローカルデータ貯蔵庫（ｄａｔａ ｖａｕｌｔｓ；以下「データボルト」、「ボルト」と言うことがある）４１６のための暗号化鍵を導出するための入力マテリアルを生成しても、または、ＰＫＩ保護リソースへの直接認証を有効化してもよいクライアント証明書を供給してもよい。

【００８６】

より詳細には、アプリケーション管理フレームワーク４１４は、各管理されたアプリケーション４１０を「ラップする」。これは、明示的な構築ステップを介して、または、構築後処理ステップを介して組み込まれてもよい。アプリケーション管理フレームワーク４１４は、アプリケーション４１０の最初のローンチにおいてクライアントエージェント４０４と「ペアリング」し、セキュリティ保護ＩＰＣチャネルを初期化し、そのアプリケーション用のポリシーを取得する。アプリケーション管理フレームワーク４１４は、クライ

アントエージェントのログイン依存性、および、ローカルＯＳサービスがいかに使用されてよいか、またはそれらがアプリケーション４１０といかに相互作用してよいかについて制限する制約ポリシーのいくつか等、ローカル適用のポリシーの関連部分を適用（enforce）する。

【００８７】

アプリケーション管理フレームワーク４１４は、認証および内部ネットワークアクセスを容易にするために、セキュリティ保護ＩＰＣチャネル４１２を介してクライアントエージェント４０４により提供されるサービスを使用する。プライベートおよび共有データボルト４１６の鍵管理（コンテナ）は、管理されたアプリケーション４１０およびクライアントエージェント４０４間の適切な相互作用により管理される。ボルト４１６は、オンライン認証後にのみ利用可能、または、ポリシーにより許可された場合のオフライン認証後に利用可能にされてもよい。ボルト４１６の最初の使用は、オンライン認証を要求してもよく、オフラインアクセスは、最大でもオンライン認証が再び要求される前のポリシーリフレッシュ期間に制限されてもよい。

【００８８】

内部リソースへのネットワークアクセスは、アクセスゲートウェイ４０６を通じて個別に管理されたアプリケーション４１０から直接、生じる。アプリケーション管理フレームワーク４１４は、各アプリケーション４１０のためのネットワークアクセスのオーケストレーションを担う。クライアントエージェント４０４は、オンライン認証に続いて取得される適切な時間制限二次的クレデンシャルの提供により、これらのネットワーク接続を容易にする。リバースウェブプロキシ接続およびエンドトゥエンドＶＰＮスタイルトンネル４１８等の、ネットワーク接続の複数のモードが使用されてもよい。

【００８９】

メールおよびブラウザ管理アプリケーション４１０はたとえば専用の状態を有していてもよく、一般的には任意のラップアプリケーションに入手可能でないこともある機能を利用してもよい。例として、メールアプリケーションは、フルＡＤログオンを必要とすることなく長時間にわたってＥｘｃｈａｎｇｅにアクセスすることを許可する専用のバックグラウンドネットワークアクセス機構を使用してもよい。ブラウザアプリケーションは複数のプライベートデータボルトを使用して、相異なる種類のデータを分離してもよい。

【００９０】

このアーキテクチャは、様々な他のセキュリティ特徴の組み込みをサポートする。例えば、ゲートウェイサーバ４０６（そのゲートウェイサービスも含む）は、場合によっては、ＡＤパスワードを確認する必要がないであろう。ＡＤパスワードが、状況によってはあるユーザ達に対する認証ファクタとして使用されるか否かについては、企業の裁量に任されたままとすることができる。ユーザがオンラインであるかオフラインであるか（すなわち、ネットワークに接続されているか、接続されていないか）によって、異なる認証方法が使用されてもよい。

【００９１】

ステップアップ認証は、ゲートウェイサーバ４０６が、厳密な認証を要求する高度機密データへのアクセスを有することが許可された、管理されたネイティブアプリケーション４１０を特定し、たとえこれが前回のより弱いレベルのログイン後に再認証がユーザにより要求されることを意味するとしても、これらのアプリケーションへのアクセスが適切な認証の実施後にのみ許可されることを確実にしてもよい特徴である。

【００９２】

このソリューションの別のセキュリティ特徴は、モバイルデバイス４０２上のデータボルト４１６（コンテナ）の暗号化である。ファイル、データベース、およびコンフィグレーションを含む全てのオンデバイスデータが保護されるよう、ボルト４１６を暗号化してもよい。オンラインボルトについては、鍵がサーバ（ゲートウェイサーバ４０６）上に記憶されてもよく、オフラインボルトについては、鍵のローカルコピーがユーザパスワードにより保護されてもよい。データがデバイス４０２上でローカルにセキュリティ保護コン

テナ４１６内に記憶されたときに、ＡＥＳ２５６暗号化アルゴリズムの最小値が利用されることが好ましい。

【００９３】

他のセキュリティ保護コンテナ特徴も実装されてもよい。例えば、ロギング特徴が含まれてもよく、アプリケーション４１０内で発生する全てのセキュリティイベントがログされ、バックエンドに報告される。アプリケーション４１０が改ざんを検出すると関連する暗号化鍵がランダムデータで上書きされ、ユーザデータが破壊されたファイルシステム上になんらヒントを残さない、等のデータ完全削除がサポートされてもよい。スクリーンショット保護は、アプリケーションがスクリーンショットにおいてあらゆるデータの記憶を防止する別の特徴である。例えば、キーウィンドウの隠しプロパティがＹＥＳに設定されてもよい。これにより、いかなるコンテンツが現在スクリーン上に表示されていようとも隠され、通常は任意のコンテンツが存在するはずが、ブランクスクリーンショットとなる。

【００９４】

任意のデータがアプリケーションコンテナ外に（例えばそれをコピーすることまたは外部アプリケーションにそれを送信することにより）ローカルに伝達されるのを防止することによって等、ローカルデータ伝達が防止されてもよい。キーボードキャッシュ特徴は、センシティブテキスト分野用の自動修正機能を無効化するよう動作してもよい。アプリケーションがサーバＳＳＬ証明書を、キーチェーン内にそれを記憶する代わりに、特定的に検証するよう、ＳＳＬ証明書検証は動作可能であってもよい。デバイス上でデータを暗号化するために使用される鍵が、ユーザにより供給されるパスフレーズを使用して生成される（オフラインアクセスが要求される場合）ように、暗号化鍵生成特徴が使用されてもよい。オフラインアクセスが要求されない場合、それは、ランダムに生成されてサーバ側に記憶された別の鍵とＸＯＲされてもよい。鍵導出関数は、その暗号ハッシュを生成するよりもむしろ、ユーザパスワードから生成された鍵がＫＤＦ（鍵導出関数、とりわけＰＢＫＤＦ２）を使用するよう動作してもよい。暗号ハッシュは、総あたりのまたは辞書攻撃を受けやすい鍵を作る。

【００９５】

さらに、１つ以上の初期化ベクトルが、暗号化方法において使用されてもよい。初期化ベクトルにより、同じ暗号化データの複数のコピーが、リプレーアタックおよび暗号解読攻撃の両方を防止しつつ異なる暗号テキスト出力を生成するであろう。これにより、データを暗号化するのに使用される特定の初期化ベクトルが知られていない場合に、盗まれた暗号化鍵であっても、攻撃者が任意のデータを解読することが防止されるであろう。さらに、認証そして解読が使用されてもよく、ユーザがアプリケーション内で認証された後にのみアプリケーションデータは解読される。別の特徴は、メモリ内のセンシティブデータに関連してもよく、これは、必要時にのみメモリ内に（ディスク内ではなく）保存されてもよい。例えば、ログインクレデンシャルは、ログイン後にメモリからワイプされてもよく、暗号化鍵およびオブジェクティブＣのインスタンス変数内の他のデータは、参照されやすいかもしれないので、記憶されない。代わりに、メモリは手動でこれらに割り当てられてもよい。

【００９６】

非活動タイムアウトが実装されてもよく、非活動のポリシー定義期間の後に、ユーザセッションが終了する。

【００９７】

アプリケーション管理フレームワーク４１４からのデータ漏れは、他の方法で防止されてもよい。例えば、アプリケーション４１０がバックグラウンドに置かれるとき、所定（構成可能）期間の後にメモリはクリアされてもよい。バックグラウンド化の際に、フォアグラウンド処理と結びつけるために、アプリケーションの最後に表示されるスクリーンのスナップショットが撮られてもよい。スクリーンショットは、機密データを含むかもしれず、よって、クリアされるべきである。

【００９８】
別のセキュリティ特徴は、１つ以上のアプリケーションへのアクセスのためのＡＤ（アクティブディレクトリ）４２２パスワードの使用を伴わない、ＯＴＰ（ワンタイムパスワード）４２０の使用に関する。場合によっては、あるユーザ達は自身のＡＤパスワードを知らない（または知ることが許されない）ため、これらのユーザは、ＳｅｃｕｒＩＤのようなハードウェアＯＴＰシステムを使用することによって等、ＯＴＰ４２０を使用して認証してもよい（ＯＴＰは、ＥｎｔｒｕｓｔまたはＧｅｍａｌｔｏ等の異なるベンダにより提供されてもよい）。場合によっては、ユーザがユーザＩＤで認証した後に、テキストがＯＴＰ４２０でユーザに送信される。場合によっては、これは、シングルフィールドであるプロンプトで、オンライン使用でのみ実装されてもよい。

【００９９】
オフラインパスワードは、オフライン使用が企業ポリシーを介して許可されるこれらのアプリケーション４１０のためのオフライン認証用に実装されてもよい。例として、企業は企業アプリケーションストアがこの方法でアクセスされることを望んでもよい。この場合、クライアントエージェント４０４はユーザに対してカスタムのオフラインパスワードを設定するよう要求してもよく、ＡＤパスワードは使用されない。ゲートウェイサーバ４０６および／または一つ以上の相異なるサーバは、標準Ｗｉｎｄｏｗｓ（登録商標）　Ｓｅｒｖｅｒパスワード複雑性要件により記載されるようにパスワードの最小長さ、文字クラス構成および使用年数に関してパスワード標準を制御・強制適用すべくポリシーを提供してもよいが、前記要件は修正されてもよい。

【０１００】
別の特徴は、二次クレデンシャル（たとえばアプリケーション管理フレームワークにより提供されてもよいマイクロＶＰＮ特徴を介してＰＫＩ保護ウェブリソースにアクセスする目的のもの）としてのあるアプリケーション４１０用のクライアント側証明書の有効化に関する。例として、@ＷｏｒｋＭａｉｌ等のアプリケーションはこのような証明書を利用してもよい。この場合、ＡｃｔｉｖｅＳｙｎｃプロトコルを使用する証明書ベースの認証が支援されて、クライアントエージェント４０４からの証明書がゲートウェイサーバ４０６により引き出され、キーチェーンにおいて使用されてもよい。各管理アプリケーションは、ゲートウェイサーバ４０６において定義されるラベルにより識別される一つの関連クライアント証明書を有していてもよい。

【０１０１】
ゲートウェイサーバ４０６は、関連する管理されたアプリケーションが内部ＰＫＩ保護リソースへの認証を行なうためのクライアント証明書の発行をサポートするために、企業特別目的ウェブサービスと相互作用してもよい。

【０１０２】
クライアントエージェント４０４およびアプリケーション管理フレームワーク４１４は、内部ＰＫＩ保護ネットワークリソースへの認証のためのクライアント証明書の取得および使用をサポートするために増強されてもよい。セキュリティおよび／または分離要件の様々なレベルに合わせるため等、２つ以上の証明書がサポートされてもよい。証明書は、メールおよびブラウザの管理されたアプリケーションにより、最終的には、任意のラップ化アプリケーションにより、使用されてもよい（それらのアプリケーションが、アプリケーション管理フレームワークがＨＴＴＰＳ要求を媒介することが妥当であるウェブサービススタイル通信パターンを使用するとの条件のもとで）。

【０１０３】
ｉＯＳ上のクライアント証明支援は、各使用期間に対する各管理アプリケーションにおけるｉＯＳキーチェーンへのＰＫＣＳ　１２　ＢＬＯＢ（バイナリラージオブジェクト）のインポートに依存してもよい。クライアント証明支援は、プライベートインメモリ鍵記憶部を用いてＨＴＴＰＳの実装を利用してもよい。クライアント証明書はｉＯＳキーチェーンには決して存在せず、強固に保護された「オンライン限定」データ値内に潜在的以外には存続しないことになる。

【０１０４】
相互ＳＳＬもまた、モバイルデバイス４０２が企業に認証され、そしてその逆の形の認証を要求することにより、さらなるセキュリティを提供するために実装されてもよい。ゲートウェイサーバ４０６への認証のための仮想化スマートカードもまた、実装されてもよい。
【０１０５】
限定および完全Ｋｅｒｂｅｒｏｓサポートの両方が、さらなる特徴であってもよい。完全サポート特徴は、ＡＤパスワードまたは信頼済みクライアント証明書を使用してＡＤ６２２への完全Ｋｅｒｂｅｒｏｓログインを行ない、ＨＴＴＰネゴシエート認証チャレンジに応答するためのＫｅｒｂｅｒｏｓサービスチケットを取得する能力に関する。限定サポート特徴は、ＡＦＥＥにおける制約付き委任に関し、ＡＦＥＥは、Ｋｅｒｂｅｒｏｓプロトコル遷移の誘発をサポートするため、それは、ＨＴＴＰネゴシエート認証チャレンジに応じて、（制約付き委任の対象となる）Ｋｅｒｂｅｒｏｓサービスチケットを取得および使用できる。この機構は、リバースウェブプロキシ（別名ＣＶＰＮ）モードで、ＨＴＴＰ（ＨＴＴＰＳではない）接続がＶＰＮおよびＭｉｃｒｏＶＰＮモードにおいてプロキシされるときに、作動する。
【０１０６】
別の特徴は、アプリケーションコンテナのロックおよびワイプに関し、これは、ジェイルブレイクまたはルーティング検出時に自動で発生し、アドミニストレーションコンソールからのプッシュコマンドとして発生してもよく、たとえアプリケーション４１０が実行中でなくともリモートワイプ機能を含んでもよい。
【０１０７】
企業アプリケーションストアおよびアプリケーションコントローラのマルチサイトアーキテクチャまたはコンフィグレーションがサポートされてもよく、これは、障害時に異なるいくつかの位置の１つからユーザがサービスを受けることを可能にする。
【０１０８】
場合によっては、管理されたアプリケーション４１０は、証明書およびプライベート鍵にＡＰＩ（例としてＯｐｅｎＳＳＬ）を介してアクセスしてもよい。企業の信頼済みの管理されたアプリケーション４１０は、アプリケーションのクライアント証明書おおびプライベート鍵で特定の公開鍵動作を行なってもよい。アプリケーションがブラウザのような挙動をして証明書アクセスが要求されない場合、アプリケーションが「自分が誰か」についての証明書を読み出す場合、アプリケーションが証明書を使用してセキュリティ保護セッショントークンを構築する場合、および、アプリケーションが重要データのデジタルサイニング（例えばトランザクションログ）または一時的データ暗号化のためのプライベート鍵を使用する場合等の、様々な使用状況が特定され、それに応じて処理されてもよい。
【０１０９】
〈企業アプリケーションストアの特徴〉
本発明の様々な態様を提供および／または実装する際に使用される計算アーキテクチャおよび企業移動管理アーキテクチャのいくつかの実施例を説明してきたが、これよりいくつかの実施形態をより詳細に説明する。
【０１１０】
特に、先に紹介したように、本発明のいくつかの態様は一般的に企業アプリケーションストアの提供に関する。以下の記載において、企業アプリケーションストアがどのように提供されるかを一つ以上の実施形態に従って様々な実施例を説明する。その上、以下の説明において、いくつかの実施例はデータを受信および／または処理するとともに他の特徴および機能を提供する企業アプリケーションストアを伴う。実施形態によっては、これらの特徴および機能のいずれかまたは全部は、企業アプリケーションストアを実装および／または提供する際に命令を記憶および／または実行してもよい一つ以上のコンピューティングデバイスにより実施および／または提供されてもよい。
【０１１１】

図５は、ここに説明される一つ以上の例示的態様に従って企業アプリケーションストアを用いてＳＳＯ機能を使用する方法を示すフローチャートである。一つ以上の実施形態において、図５に例示される方法および／またはその一つ以上のステップはコンピューティングデバイス（たとえば汎用コンピューティングデバイス２０１）により実施されてもよい。他の実施形態において、図５に例示される方法および／またはその一つ以上のステップは、不揮発性コンピュータ読取可能メモリ等のコンピュータ読取可能媒体に記憶されたコンピュータ実行可能命令において具体化されてもよい。

【０１１２】

図５にみられるように、前記方法は、身元クレデンシャルが企業アプリケーションストアにおいて受信されるステップ５０５において開始される。たとえば、受信される（たとえばステップ５０５において）身元クレデンシャルは、様々な相異なるウェブサイト、リソース、システムおよび／またはサービスへのアクセスを有効化してもよいＳＳＯクレデンシャルまたはいくつかの他形態の多用途クレデンシャルであってもよい。さらに／あるいは、身元クレデンシャル（たとえばＳＳＯクレデンシャル）は、特定ユーザおよび／または一つ以上の特定デバイスにリンクおよび／または関連付けられていてもよい。

【０１１３】

例として、ステップ５０５において、企業アプリケーションストア（および／または、企業アプリケーションストアを提供する命令を記憶ならびに／もしくは実行してもよい一つ以上のコンピューティングデバイス）は、たとえば企業アプリケーションストアにアクセスしようとしてもよいモバイルデバイス（および／またはこのようなモバイルデバイスのユーザ）からＳＳＯクレデンシャルを受信してもよい。ＳＳＯクレデンシャルは、例として、一つ以上のデータ記憶および管理プラットフォーム、一つ以上のクラウド記憶プラットフォーム、一つ以上の仮想化および／またはリモートアクセスプラットフォーム、および／または一つ以上の他のリソース等、企業アプリケーションストアおよび他の企業リソースを含む複数の相異なる企業リソースにアクセスする際に使用されるべく、および／または使用することが可能であるべく構成された認証クレデンシャルであってもよい。さらに／あるいは、ＳＳＯクレデンシャルはたとえば、一つ以上の非管理データ記憶および管理プラットフォーム、一つ以上のソーシャルネットワーク、および／または一つ以上の他の非企業リソース等の非企業リソースにアクセスする際に使用されるべく、および／または使用することが可能であるべく構成されてもよい。

【０１１４】

ステップ５１０において、ステップ５０５において受信された身元クレデンシャルが有効であるか否かを判定する。例として、ステップ５１０において、企業アプリケーションストアはステップ５０５において受信された身元クレデンシャルを（たとえば有効なクレデンシャルに対するデータベース記録および／または他の情報と受信したクレデンシャルとを比較することにより）評価して、受信した身元クレデンシャルが企業アプリケーションストアにアクセスしたりおよび／または企業アプリケーションストアから情報を取得したりするための一つ以上の権利をクレデンシャルのユーザに提供するか否かを判定してもよい。さらに／あるいは、受信した身元クレデンシャルを評価する際に企業アプリケーションストアはたとえば、検証されるべき一つ以上の外部クレデンシャル評価サービスに受信した身元クレデンシャルを提供してもよく、続いて、受信した身元クレデンシャルが有効であるか否かを示す情報を一つ以上の外部サービスから受信してもよい。

【０１１５】

ステップ５１０において身元クレデンシャルが有効でないと判定された場合、次にステップ５１５において、通知を生成してもよいし、および／または代替クレデンシャルを提供するようユーザに促してもよい。例として、ステップ５１５において、企業アプリケーションストアは、身元クレデンシャルが有効でない旨、および／または企業アプリケーションストアへのアクセスが提供できない旨を示す通知を生成してもよい。その上、企業アプリケーションストアはたとえば、受信した身元クレデンシャルの送信元であるコンピューティングデバイスに生成された通知を送信することにより、生成された通知を表示（た

とえば受信した身元クレデンシャルの送信元であるコンピューティングデバイス上に）させてもよい。さらに／あるいは、企業アプリケーションストアは、代替認証クレデンシャルを提供して企業アプリケーションストアへのアクセスを取得するようユーザに促すべく構成されたプロンプトを生成してもよい。その上、企業アプリケーションストアはたとえば、受信した身元クレデンシャルの送信元であるコンピューティングデバイスに生成されたプロンプトを送信することにより、生成されたプロンプトを表示（たとえば受信した身元クレデンシャルの送信元であるコンピューティングデバイス上に）させてもよい。

【０１１６】

あるいは、ステップ５１０において身元クレデンシャルが有効であると判定された場合、次にステップ５２０において企業アプリケーションストアインタフェースが提供されてもよい。例として、ステップ５２０において企業アプリケーションストアインタフェースを提供する際、企業アプリケーションストアは、一つ以上のユーザインタフェースを生成したり、および／または一つ以上のユーザインタフェースを表示（たとえば受信した身元クレデンシャルの送信元であるコンピューティングデバイス等のモバイルデバイス上で）させたりしてもよい。一つ以上の構成において、企業アプリケーションストアインタフェースは、自身の身元クレデンシャルを使用して企業アプリケーションストアにアクセスしていてもよいモバイルデバイスのユーザ等のユーザが様々なアプリケーションを閲覧および／またはダウンロードできるようにしてもよい。企業アプリケーションストアインタフェースはたとえば、企業アプリケーションストアを展開した、および／または実装している組織または他の企業に固有であってもよい様々な特徴を含むべく一つ以上の管理ユーザにより構成されてもよい。例として、企業アプリケーションストアインタフェースは、組織または企業（および／または組織もしくは企業と連携しているかもしれない他の企業ユーザ）の従業員に入手可能である（および／または従業員に対して選択された、推奨された、および／またはライセンス供与された）一つ以上のアプリケーションのリストを含んでいてもよい。

【０１１７】

その上、特定ユーザに対して（たとえば企業アプリケーションストアインタフェースに含まれたアプリケーションのリストにおいて）提示される一つ以上のアプリケーションは、（ステップ５０５において受信される身元クレデンシャルに基づいて判定されてもよいように）ユーザの身元に基づいて企業アプリケーションストアにより選択されてもよい。たとえば、企業アプリケーションストアにより第１ユーザに提示される（たとえば従業員および／または組織と連携する他のユーザに対して第１組織により提供されてもよい）企業アプリケーションストアインタフェースは第１アプリケーションセットを含んでいてもよい一方、企業アプリケーションストアにより（たとえば身元、職務等の点で第１ユーザとは異なっていてもよい）第２ユーザに提示される企業アプリケーションストアインタフェースは第１アプリケーションセットとは異なる第２アプリケーションセットを含んでいてもよい。たとえば第２アプリケーションセットは、アプリケーションが第２ユーザに対して（たとえば、およびおそらく第１ユーザに対してではなく）推奨され、および／または適当である旨の企業アプリケーソンストアによる判定に基づいて第２ユーザに対して企業アプリケーションストアにより選択された一つ以上のアプリケーションを含んでいてもよい。

【０１１８】

ステップ５２５において、アプリケーションを求める要求が受信される。例として、ステップ５２５において、企業アプリケーションストアはソフトウェアアプリケーションを求める要求を受信してもよい。たとえばステップ５２５において、企業アプリケーションストアは、企業アプリケーションストアにおいてコンピューティングデバイスに入手可能である特定アプリケーションをダウンロードおよび／または提供することを求める要求をコンピューティングデバイスから（たとえば受信した身元クレデンシャルの送信元であるコンピューティングデバイスから）受信してもよい。このような要求はたとえば、ステップ５２０において提供される企業アプリケーションストアインタフェースを使用して企業

アプリケーションストアから特定アプリケーションをダウンロードすることを選択および／または要求するコンピューティングデバイス（たとえばスマートフォン、タブレットコンピュータまたは他のモバイルコンピューティングデバイス等のモバイルデバイスであってもよい）のユーザに基づいて受信されてもよい。

【０１１９】

ステップ５３０において、アプリケーションは身元クレデンシャルに基づいて構成される。例として、ステップ５３０において、企業アプリケーションストアは、ステップ５０５において受信される、および／またはステップ５１０において検証されるＳＳＯクレデンシャルに基づいてソフトウェアアプリケーション（たとえばステップ５２５におけるソフトウェアアプリケーション要求）を構成してもよい。身元クレデンシャルに基づいてアプリケーションを構成する際、以下に説明されるいくつかの実施例において例示されるように、企業アプリケーションストアはたとえば身元クレデンシャルに基づいて一つ以上のユーザ固有の設定を確立したり、身元クレデンシャルに基づいて一つ以上の管理ポリシーをアプリケーションに適用したり、および／または身元クレデンシャルに基づいて（また関連して、身元クレデンシャルの認証ユーザの身元、アクセス権および／または特権に基づいて）提供されるべきアプリケーションの汎用ならびに／もしくはデフォルト設定を修正したりしてもよい。

【０１２０】

たとえば実施形態によっては、身元クレデンシャルに基づいたソフトウェアアプリケーションの構成は、身元クレデンシャルに基づいた一つ以上のユーザ固有の設定の確立を含んでいてもよい。例として、様々なアプリケーション固有の設定は一つ以上のデータソースにおいて（たとえば様々な相異なるアプリケーションに関するあるユーザに対して）定義および／または記憶されてもよく、ユーザ固有の設定を確立する際、企業アプリケーションストアは受信および／または検証された身元クレデンシャルを使用して一つ以上のデータソースからこれらの設定を検索したり、設定にアクセスしたり、および／または設定を取得したりしてもよい。たとえば企業アプリケーションストアは受信および／または検証された身元クレデンシャルを使用して、一つ以上のデータソースを用いて認証し、一つ以上のデータソースにおいて（たとえば身元クレデンシャルから判定されるようにユーザ身元に基づいて）特定ユーザのアプリケーション固有の設定を識別してもよい。

【０１２１】

身元クレデンシャルに基づいて企業アプリケーションストアにより確立されてもよいユーザ固有の設定のいくつかの実施例は、特定アプリケーション（たとえば電子メールクライアント、ウェブブラウザ、文書管理ソフトウェア等）に対して設定されるユーザアカウント設定、特定アプリケーション（たとえば電子メールクライアント、ウェブブラウザ等）に対して設定されるネットワークおよび／または接続設定、特定アプリケーション（たとえばワードプロセッサ、電子メールクライアント等）に対して設定されるカスタム辞書設定、特定アプリケーション（たとえばワードプロセッサ、スプレッドシートツール、電子メールクライアント、文書管理ソフトウェア等）に対して設定されるカスタムビューおよび／または表示設定を含む。

【０１２２】

身元クレデンシャルに基づいて記憶された企業アプリケーションにより確立されてもよいユーザ固有の設定の他の実施例は、ユーザインタフェース設定（たとえば色設定、テーマ設定等）、言語設定、時間帯設定、通貨設定および／または他の設定を含む。これらの実施例は、追加および／または代替実施形態においていくつかの設定が確立されてもよいいくつかの種類のアプリケーションと同様に実施形態によっては確立されてもよいいくつかの種類の設定を例示するが、いずれの他種類のユーザ固有の設定も上記および／または他タイプのアプリケーションのうちいずれに対して確立されてもよい。

【０１２３】

実施形態によっては、身元クレデンシャルに基づいたソフトウェアアプリケーションの構成は、身元クレデンシャルに基づいた一つ以上の管理ポリシーのアプリケーションへの

適用を含んでいてもよい。例として、一つ以上の管理ポリシーは、すべてまたはある状態におけるアプリケーション（たとえば切り取り、コピー、貼り付け等）のある特徴を有効化および／または無効化したり、すべてまたはある状態におけるデバイス（たとえば組み込みカメラの使用）のある特徴を有効化および／または無効化したり、すべてまたはある状態におけるアプリケーションおよび／またはデバイスによるあるリソース（たとえば企業リソース）へのアクセスを有効化および／または無効化したり、および／または特定アプリケーションならびに／あるいはデバイス（たとえば使用時の地理的制限、使用時の時間的制限等）に関して他の機能および／または制限を提供したりするために構成されてもよい。

【０１２４】

一つ以上の構成において、様々なユーザ固有の管理ポリシーは一つ以上のデータリソースにおいて（様々な相異なるアプリケーションに関してあるユーザに対して）定義されおよび／または記憶されてもよい。身元クレデンシャルに基づいてアプリケーションに一つ以上の管理ポリシーを適用する際、企業アプリケーションストアは受信および／または検証された身元クレデンシャルを使用して一つ以上のデータソースからこれらの管理ポリシーを検索したり、管理ポリシーにアクセスしたり、および／または管理ポリシーを取得したりしてもよい。たとえば企業アプリケーションストアは受信および／または検証された身元クレデンシャルを使用して、一つ以上のデータソースを用いて認証し、特定アプリケーションに関する特定ユーザに適用可能であってもよい一つ以上の管理ポリシーを一つ以上のデータソースから取得された情報を使用して識別してもよい。

【０１２５】

たとえばアプリケーションに適用される一つ以上の管理ポリシーは、身元クレデンシャルに関連した少なくとも一つのユーザ職務に基づいて選択されてもよい。例として、受信および／または検証された身元クレデンシャルが第１職務（たとえば組織における情報セキュリティ保護職）を有する第１ユーザに対応する場合、企業アプリケーションストアは第１ユーザにより要求されたアプリケーションに第１管理ポリシーセットを適用してもよいのに対し、受信および／または検証された身元クレデンシャルが第２職務（たとえば組織における営業職）を有する第２ユーザに対応する場合、企業アプリケーションストアは、同じアプリケーションが第２ユーザにより要求されるとき、このアプリケーションに第１管理ポリシーセットとは異なる第２管理ポリシーセットを適用してもよい。

【０１２６】

実施形態によっては、身元クレデンシャルに基づいてソフトウェアアプリケーションを構成する際、アプリケーションストアは受信および／または検証された身元クレデンシャルを使用して一つ以上の企業リソースにアクセスし、身元クレデンシャルに基づいて一つ以上の企業リソースからユーザ固有の情報を取得し、ソフトウェアアプリケーションに対して一つ以上のユーザ固有の設定を確立する際にユーザ固有の情報を使用してもよい。例として、一つ以上の企業リソースは上記実施例（たとえばユーザアカウント設定、ネットワークおよび／または接続設定等）において説明されたような様々なアプリケーションに対するユーザ固有の設定を記憶および／または保持してもよい。企業リソースからユーザ固有の情報を取得する際、企業アプリケーションストアは身元クレデンシャルを使用して企業リソースにログインし、続いて身元クレデンシャルに関連した身元情報に基づいてユーザ固有の設定を検索し引き出してもよい。次にユーザ固有の設定を確立する際にユーザ固有の情報を使用する際、企業アプリケーションストアは、アプリケーションが受信者デバイス（たとえばユーザのコンピューティングデバイス）に提供されるより前に、（たとえば身元クレデンシャルを供給したユーザにより）要求されたアプリケーションにおける一つ以上の未定義および／またはデフォルト設定を設定、定義、上書きおよび／または修正してもよい。

【０１２７】

実施形態によっては、身元クレデンシャルに基づいてソフトウェアアプリケーションを構成する際、アプリケーションストアはアプリケーションを最小限に構成してもよく、続

いて受信者デバイスにアプリケーションを提供する際にアプリケーションストアは最小限に構成されたアプリケーションを受信者（recipient）デバイスに提供してもよい。たとえば、最小限に構成されたアプリケーションは、受信者デバイスに提供される前に企業アプリケーションストアにより完全には構成されていないアプリケーションであってもよい。またたとえば、アプリケーションを最小限に構成する際、アプリケーションストアは例として、このような機能（たとえばブラウザアプリケーションまたは電子メールクライアントアプリケーション用の色テーマ設定および／または他のユーザインタフェース設定）を有効化するのに必須でなくてもよい一つ以上の設定を確立することなくアプリケーション（たとえばブラウザアプリケーションまたは電子メールクライアントアプリケーション用のネットワークおよび／または接続設定）の機能を有効化するのに必須であってもよい一つ以上の設定を確立してもよい。一つ以上の構成において、必須でない設定は代わりに実行時（たとえば、アプリケーションがたとえばモバイルデバイス上で実行されているとき）および／または実行後（たとえば、アプリケーションの特定態様が呼び出される際に必要とされるとき）に受信者デバイス上で確立されてもよい（適用は完全に構成されてもよい）。

【０１２８】

続けて図５を参照し、ステップ５３５において、構成済みアプリケーションは受信者デバイスに提供される。例として、ステップ５３０において身元クレデンシャルに基づいてアプリケーションを構成した後、企業アプリケーションストアはステップ５３５において構成済みソフトウェアアプリケーションを身元クレデンシャルに関連した少なくとも一つの受信者デバイスに提供してもよい。たとえば企業アプリケーションストアは構成済みソフトウェアアプリケーションを、受信（たとえばステップ５２５において）した要求の送信元であるデバイスに提供してもよい。

【０１２９】

実施形態によっては、受信者デバイスに提供（たとえばステップ５３５において）された構成済みソフトウェアアプリケーションは、仮想化アプリケーションに対応するスタブアプリケーションであってもよい。例として、スタブアプリケーションは、一つ以上のリモートサーバおよび／またはデバイス上で実行される仮想化アプリケーション用のコンテナまたはクライアントエージェント（たとえばユーザコンピューティングデバイス上で提供されてもよい）を提供してもよい。このようなスタブアプリケーションを構成する際、企業アプリケーションストアは、特定ユーザ（たとえば、仮想化アプリケーションおよび／または仮想化プラットフォーム用のユーザアカウント設定、および／または仮想化アプリケーションならびに／もしくは仮想化プラットフォーム用のネットワークおよび／または接続設定等）用の仮想化アプリケーションの実行を容易にする一つ以上の設定を確立してもよい。

【０１３０】

その上たとえば、仮想化アプリケーションの実行は身元クレデンシャルにより有効化されてもよい。例として、仮想化アプリケーションの実行は身元クレデンシャルを用いたユーザの認証成功とともに開始されたり、および／または認証成功に依存してもよく、スタブアプリケーションを受信者デバイスに提供（たとえばステップ５３０において）する前に構成する際に企業アプリケーションストアは、企業アプリケーションストアにより受信および検証されたユーザの身元クレデンシャルに基づいてアプリケーションがダウンロードおよび／または構成された旨を示すアプリケーションに関連して一つ以上の設定を確立したり、および／またはデータを記憶してもよい。たとえば仮想化プラットフォームは次に、仮想化プラットフォームがこれらの設定および／または記憶データを使用してユーザを認証し仮想化アプリケーションの実行を開始させることができる場合に、ユーザが身元クレデンシャルを再提出しログオンする必要が無いときにユーザエクスペリエンスを高めるようなスタブアプリケーションの起動時にユーザを認証する際に上記設定および／または記憶データを使用してもよい。

【０１３１】

実施形態によっては、企業アプリケーションストアは身元クレデンシャルの検証に応じてソフトウェアアプリケーションを構成してもよい。例として、（たとえば様々なアプリケーションおよびユーザ用のダウンロード履歴情報に基づいて、様々なアプリケーションおよび／またはユーザ用の更新および／またはバージョン履歴情報に基づいて、様々なデバイスおよび／またはユーザに対してデバイス搭載監視エージェントにより提供される情報に基づいて等）あるデバイスおよび／またはユーザがあるアプリケーションを必要としている旨を企業アプリケーションストアが判定する例において、企業アプリケーションストアは（たとえばこのようなデバイスのユーザが必要な特定アプリケーションのダウンロードを手動で選択することなく）特定デバイスおよび／またはユーザにより提出された身元クレデンシャルの検証に応じて一つ以上の必要なアプリケーションを特定デバイスおよび／またはユーザに自動的に提供してもよい。

【０１３２】

図６は、ここに説明される一つ以上の例示的態様に従って企業アプリケーションストアを介してモバイルサービス管理機能を提供する方法を示すフローチャートである。一つ以上の実施形態において、図６に例示される方法および／またはその一つ以上のステップはコンピューティングデバイス（たとえば汎用コンピューティングデバイス２０１）により実施されてもよい。他の実施形態において、図６に例示される方法および／またはその一つ以上のステップは、不揮発性コンピュータ読取可能メモリ等のコンピュータ読取可能媒体に記憶されたコンピュータ実行可能命令において具体化されてもよい。

【０１３３】

一つ以上の態様に従って、「モバイルサービス管理」（ＭＳＭ）機能は、モバイルデバイス管理（ＭＤＭ）機能および／またはモバイルアプリケーション管理（ＭＡＭ）機能を含んでいてもよい。したがって、たとえばモバイルサービス管理機能の（たとえば企業アプリケーションストアを介した）提供はモバイルデバイス管理機能の独占的な提供を含んでいてもよい。またたとえば、モバイルサービス管理機能の（たとえば企業アプリケーションストアを介した）提供は、モバイルアプリケーション管理機能の独占的な提供を含んでいてもよい。さらにたとえば、モバイルサービス管理機能の（たとえば企業アプリケーションストアを介した）提供は、モバイルデバイス管理機能およびモバイルアプリケーション管理機能両方の提供を含んでいてもよい。

【０１３４】

図６に見られるように、前記方法は、企業アプリケーションストアの管理ユーザの認証クレデンシャルが企業アプリケーションストアにおいて受信されるステップ６０５において開始される。例として、ステップ６０５において、上記実施例に説明された企業アプリケーションストアと同様に、企業アプリケーションストアは管理ユーザの認証クレデンシャルを受信してもよい。管理ユーザはたとえば、アプリケーションストアの他ユーザおよび／または他の企業リソースの他ユーザに対するポリシーを設定および／または修正するためのアプリケーションストアにおけるアクセス権および／または特権を有する企業アプリケーションストアのユーザであってもよい。その上、管理ユーザのクレデンシャルは、管理ユーザに割り当てられた、および／または関連したユーザ名および／またはパスワードを含んでいてもよい。

【０１３５】

ステップ６１０において、管理ユーザの認証クレデンシャルが有効であるか否かを判定する。例として、ステップ６１０において、企業アプリケーションストアはステップ６０５において受信された管理ユーザの認証クレデンシャルを評価して、クレデンシャルが企業アプリケーションストアへのアクセスおよび／または制御を有効化するのに使用できるか否かを判定してもよい。例によっては、管理ユーザの認証クレデンシャルを評価する際、企業アプリケーションストアはたとえば受信したクレデンシャルに含まれたユーザ名およびパスワードを有効なユーザ名およびパスワードのデータテーブルと比較して、提供されたクレデンシャルを検証してもよい。

【０１３６】

ステップ６１０において管理ユーザの認証クレデンシャルが有効でないと判定された場合、次にステップ６１５において、通知を生成してもよいし、および／または代替クレデンシャルを提供するようユーザに促してもよい。例として、ステップ６１５において、企業アプリエーションストアは、受信したクレデンシャルが有効でない旨を示す通知を生成してもよく、さらに、先に説明した（たとえばステップ５１５を参照）実施例において通知が生成および表示される方法と同様に、生成した通知を表示させてもよい。その上、企業アプリケーションストアは代替認証クレデンシャルを提供するようユーザに促すべく構成されたプロンプトを生成してもよく、さらに、（たとえばステップ５１５を参照）先に説明した実施例においてプロンプトが生成および表示される方法と同様に、生成したプロンプトを表示させてもよい。

【０１３７】

あるいは、ステップ６１０において管理ユーザの認証クレデンシャルが有効であると判定された場合、次にステップ６２０においてモバイルサービス管理（ＭＳＭ）インタフェースは企業アプリケーションストアを介して提供される。モバイルサービス管理インタフェースはたとえば、管理ユーザが企業アプリケーションストアにおいて入手可能である一つ以上のアプリケーションに適用されるべき一つ以上のポリシーを定義できるように構成された一つ以上の制御を含んでいてもよい。例として、一つ以上のポリシーは、一つ以上のモバイルデバイス上における一つ以上のアプリケーションの実行中に一つ以上のアプリケーションの機能を制御すべく構成されてもよい。

【０１３８】

さらに／あるいは、一つ以上のポリシーはモバイルデバイス上における特定アプリケーションの実行中にモバイルデバイスの機能を制御すべく構成されてもよい。特に特定ユーザおよび／または特定デバイスに対し、一つ以上のポリシー（たとえばステップ６２０において提供されるモバイルサービス管理インタフェースを使用して管理ユーザにより定義されてもよい）のあるポリシーは、すべてまたはある状態における特定アプリケーションのある特徴を有効化および／または無効化したり、すべてまたはある状態における特定デバイスのある特徴を有効化および／または無効化したり、すべてまたはある状態における特定アプリケーションおよび／または特定デバイスによるあるリソースへのアクセスを有効化および／または無効化したり、および／または特定アプリケーションおよび／または特定デバイスに関する他の機能および／または制限を提供したりする特定アプリケーションに適用されてもよい。

【０１３９】

その上、モバイルサービス管理インタフェースは（たとえば企業アプリケーションストアが管理ユーザに対して表示されたときに）たとえば企業アプリケーションストアの一部分および／または一部として提供されてもよい一方、またたとえばモバイルサービス管理インタフェースは、企業アプリケーションストアおよび／またはその関連リソースにより、および／またはこれと通信して有効化される分離したウェブコンソールとして提供されてもよい。

【０１４０】

実施形態によっては、モバイルサービス管理インタフェース（たとえばステップ６２０において提供されるモバイルサービス管理インタフェース）に含まれた一つ以上の制御はさらに、管理ユーザが一つ以上のアプリケーションの相異なるユーザに対して相異なるポリシーを定義できるように構成されていてもよい。例として、モバイルサービス管理インタフェースに含まれた一つ以上の制御は、管理ユーザが特定アプリケーションに関して第１ユーザまたはユーザグループに対して第１ポリシーを定義できるように構成されていてもよく、さらに、管理ユーザが同一アプリケーションに関して第２ユーザまたはユーザグループに対して第２ポリシーを定義できるように構成されていてもよい。ここで第２ポリシーは第１ポリシーとは異なっており、第２ユーザまたはユーザグループは第１ユーザまたはユーザグループとは異なっている。

【０１４１】

一つ以上の構成において、モバイルサービス管理インタフェース（たとえばステップ６２０において提供されるモバイルサービス管理インタフェース）に含まれた一つ以上の制御はさらに、管理ユーザが相異なるユーザ職務に対して相異なるポリシーを定義できるように構成されていてもよい。例として、このような制御を使用して管理ユーザは企業内の第１職務（たとえば情報セキュリティ保護）を有する第１ユーザまたはユーザグループに対する第１ポリシーと、企業内の第２職務（たとえば営業）を有する第２ユーザまたはユーザグループに対する第２ポリシーとを企業アプリケーションストアにおいて入手可能であってもよい特定アプリケーションに関して定義してもよい。ここで第２ポリシーは（たとえばアプリケーションにおいて有効化および／または無効化される機能に関して、アプリケーションが稼働している間にデバイス上で有効化および／または無効化される機能に関して、アプリケーションによりおよび／またはアプリケーションが稼働している間アクセス可能および／または不可能である企業リソースおよび／または他のリソースに関して等）第１ポリシーとは異なっている。

【０１４２】

実施形態によっては、モバイルサービス管理インタフェース（たとえばステップ６２０において提供されるモバイルサービス管理インタフェース）は企業アプリケーションストアにおける一つ以上のアプリケーションの受信に応じて提供されてもよい。例として、管理ユーザが企業アプリケーションストアに特定アプリケーションをアップロードおよび／または提供した後、企業アプリケーションストアはアプリケーションの受信に応じてモバイルサービス管理インタフェース（たとえば管理ユーザがアップロードされたばかりのアプリケーションに対して一つ以上のポリシーを定義できるように構成されていてもよい）を提供してもよい。これらの特徴を使用して企業アプリケーションストアの管理ユーザはたとえば、企業アプリケーションストアの様々な非管理ユーザに対して企業アプリケーションストアに管理ユーザがアップロードしている、および／または入手可能にしているアプリケーションを構成してもよい。たとえば管理ユーザはモバイルサービス管理インタフェースを使用して、企業アプリケーションストアにアップロードおよび／または追加されたばかりのアプリケーションに対して最初にポリシーを定義することができてもよい。

たとえばモバイルサービス管理インタフェースを提供（たとえばステップ６２０において）した後、アプリケーションに対するポリシー変更はモバイルサービス管理インタフェースを介してステップ６２５において受信されてもよい。例として、たとえばステップ６２５において、企業アプリケーションストアは特定アプリケーションに対するポリシー変更を受信してもよい。このようなポリシー変更はたとえばモバイルサービス管理インタフェースに含まれる一つ以上の制御および／またはステップ６２０において提供されるモバイルサービス管理インタフェースを介して管理ユーザにより提供されるユーザ入力として受信されてもよい。

【０１４３】

このようなポリシー変更の受信（たとえばステップ６２５において）に基づいて、ポリシー変更に関連した情報がステップ６３０においてアプリケーション（すなわちポリシー変更が受信されたアプリケーション）を有する一つ以上のモバイルデバイスに提供されてもよい。

【０１４４】

例として、ステップ６３０において、企業アプリケーションストアはポリシー変更の影響を受けてもよい一つ以上のアプリケーションおよび／またはデバイスに対してポリシー変更を詳細に規定する情報を提供してもよい。たとえば影響を受けるアプリケーションおよび／またはデバイスにこの情報を提供する前に、企業アプリケーションストアは、様々なアプリケーションおよびユーザに対するダウンロード履歴情報、様々なアプリケーションおよびユーザに対する更新および／またはバージョン履歴情報、様々なアプリケーションおよびユーザに対するデバイス搭載監視情報、および様々なアプリケーションおよびユーザに対するポリシー情報（たとえば、いずれのポリシーが現在適切であるか、いずれのポリシーが既に適用されたか等を特定アプリケーションおよび／または特定ユーザに対し

て指定してもよい）に基づいてポリシー変更の影響をいずれのアプリケーションおよび／またはデバイスが受けるのかを識別してもよい。

【０１４５】

実施形態によっては、管理ユーザの承認クレデンシャルを検証（たとえばステップ６１０において）した後、管理ユーザからの新アプリケーションがアプリケーションストアにおいて受信されてもよい。例として、管理ユーザの認証クレデンシャルを検証した後、企業アプリケーションストアは管理ユーザ（および／または管理ユーザにより使用されている一つ以上のコンピューティングデバイス）により企業アプリケーションストアにアップロードされている（および／またはアップロードされたばかりの）新アプリケーションを受信してもよい。

【０１４６】

管理ユーザからこのような新アプリケーションを受信した後（および／または管理ユーザからの新アプリケーションの受信に応じて）アプリケーションストアは、新アプリケーションに適用されるべき一つ以上のポリシーを定義するよう管理ユーザに促してもよい。例として、このようなポリシーを定義するよう管理ユーザに促す際、企業アプリケーションストアは新アプリケーションに対する一つ以上の関連ポリシーを識別してもよい。関連ポリシーはたとえば、新アプリケーションに（たとえばポリシーの性質に基づいて、アプリケーションの性質に基づいて、企業アプリケーションストアを展開および／または提供する企業および／または他の組織により使用される一つ以上のデフォルトポリシーに基づいて、他の管理ユーザにより提供される推薦情報に基づいて等）適用されることができる、および／または適用されるべきであるポリシーを含んでいてもよい。次に新アプリケーションに対する一つ以上の関連ポリシーを識別した後、企業アプリケーションストアはたとえばモバイルサービス管理インタフェース（たとえばステップ６２０において最初に提供されていてもよい）を更新して、管理ユーザが一つ以上の識別されたポリシーを管理できるように構成された少なくとも一つの制御を含ませてもよい。例として、企業アプリケーションストアはモバイルサービス管理インタフェースを更新して、関連性があると識別された一つ以上のポリシーを管理ユーザが有効化および／または無効化できるようにする一つ以上の制御を含ませるとともに、様々なデバイス上でこれらのポリシーを定義および／または強制適用するのに使用されてもよい様々な特徴および／または設定を設定および／または修正してもよい。

【０１４７】

新アプリケーションに（および／またはプロンプトに応じて管理ユーザからの入力および／または他の情報の受信に基づいて）適用されるべき一つ以上のポリシーを定義するよう管理ユーザに促した後、アプリケーションストアは管理ユーザから新アプリケーションに適用されるべき少なくとも一つのポリシーを受信してもよい。

【０１４８】

例として、企業アプリケーションストアは上記実施例において説明された更新済みモバイルサービス管理インタフェースを介して管理ユーザにより提供される一つ以上の選択および／または他の入力を受信してもよい。この方法において、管理ユーザは例として、管理ユーザがアプリケーションに追加した新アプリケーションに適用されるべきである一つ以上のポリシーを定義することが可能であってもよい。その上、管理ユーザにより定義される一つ以上のポリシーは例として、アプリケーションが一つ以上の受信者デバイス（たとえば非管理ユーザにより使用される一つ以上のモバイルデバイス）により提供および／または実行される場合、および／または時に新アプリケーションに適用されてもよい。

図７は、ここに説明される一つ以上の例示的態様に従って企業アプリケーションストアを介してモバイルサービス管理機能を提供する方法を示す別のフローチャートである。一つ以上の実施形態において、図７に例示される方法および／またはその一もしくは複数のステップはコンピューティングデバイス（たとえば汎用コンピューティングデバイス２０１）により実施されてもよい。他の実施形態において、図７に例示される方法および／またはその一もしくは複数のステップは、不揮発性コンピュータ読取可能メモリ等のコンピ

ュータ読取可能媒体に記憶されたコンピュータ実行可能命令において具体化されてもよい。さらに／あるいは、図７に例示される方法はたとえば図６に例示される方法と組み合わせてもよい。例として、図７に例示される方法は、図６に例示される方法を実施する前および／または後に企業アプリケーションストアにより実施されてもよい。

【０１４９】

図７に見られるように前記方法は、非管理ユーザの認証クレデンシャルが企業アプリケーションストアにおいて受信されるステップ７０５において開始される。例として、ステップ７０５において、企業アプリケーションストアは、管理ユーザの認証クレデンシャルが受信されてもよい（たとえばステップ６０５を参照して上述されたように）のと同様に非管理ユーザの認証クレデンシャルを受信してもよい。

【０１５０】

非管理ユーザの認証クレデンシャルは、非管理ユーザに割り当てられた、および／または関連したユーザ名および／またはパスワードを含んでいてもよい。その上、非管理ユーザはたとえば、自身または企業アプリケーションストアの他ユーザに対して、および／または他の企業リソースの他ユーザに対してポリシーを設定および／または修正するアクセス権および／または特権をアプリケーションストアにおいて有していない企業アプリケーションストアのユーザであってもよい。

【０１５１】

非管理ユーザの認証クレデンシャルの受信（たとえばステップ７０５において）に基づいて、非管理ユーザの認証クレデンシャルが有効であるか否かをステップ７１０において判定してもよい。例として、ステップ７１０において、企業アプリケーションストアは、管理ユーザの認証クレデンシャルが検証される方法（たとえばステップ６１０を参照して上述されたように）と同様に、非管理ユーザの認証クレデンシャルを（たとえば提供されたユーザ名およびパスワードを有効なユーザ名およびパスワードのデータテーブル等と比較することにより）評価してもよい。

【０１５２】

ステップ７１０において非管理ユーザの認証クレデンシャルが有効ではないと判定された場合、次にステップ７１５において、通知が生成されてもよいし、および／またはユーザは代替クレデンシャルを提供するよう促されてもよい。例として、ステップ７１５において、企業アプリケーションストアは、通知が先に説明した実施例において（たとえばステップ５１５を参照）生成および表示される方法と同様に、受信したクレデンシャルが有効でない旨を示す通知を生成してもよく、さらに生成された通知を表示させてもよい。その上、企業アプリケーションストアは代替認証クレデンシャルを提供するようユーザに促すべく構成されたプロンプトを生成してもよく、さらに、プロンプトが先に説明した実施例において（たとえばステップ５１５を参照）生成および表示される方法と同様に、生成されたプロンプトを表示させてもよい。

【０１５３】

あるいはステップ７１０において管理ユーザの認証クレデンシャルが有効であると判定された場合、次にステップ７２０において、アプリケーションダウンロードインタフェースが提供されてもよい。たとえばアプリケーション（すなわちステップ６２５においてポリシー変更が受信されたアプリケーション）に対するアプリケーションダウンロードインタフェースは企業アプリケーションストアを介して提供されてもよく、アプリケーションダウンロードインタフェースはアプリケーションに対して（たとえば管理ユーザにより）定義された一つ以上のポリシーに対応する一つ以上のインディケータを含んでいてもよい。

【０１５４】

例として、ステップ７２０において、企業アプリケーションストアは特定アプリケーションに対するアプリケーションダウンロードインタフェースを提供してもよく、アプリケーションダウンロードインタフェースは、ステップ７０５およびステップ７１０において認証された特定非管理ユーザに対してカスタマイズされてもよい。特に、カスタマイズさ

れたアプリケーションダウンロードインタフェースは、企業アプリケーションストアの管理ユーザにより（たとえばモバイルサービス管理インタフェースを使用して）適切にされたポリシーおよび／またはポリシー変更に基づいて、アプリケーションが非管理ユーザによりダウンロードおよび／または使用されたときに特定アプリケーションに適用される（または適用されるべく構成されている）一つ以上のポリシーを識別する情報を含んでいてもよい。したがって、たとえばアプリケーションダウンロードインタフェースは、あるタイプのポリシー（たとえばアプリケーション自身の機能を制限するポリシー、アプリケーションの実行中にデバイスの機能を制限するポリシー等）がアプリケーションダウンロードインタフェースの対象である特定アプリケーションに適用される、または適用されるべく構成された旨を示してもよい、一つ以上のアイコンおよび／または他のイメージ等の簡易情報を含んでいてもよい。

【０１５５】

さらに／あるいは、アプリケーションダウンロードインタフェースはたとえば、アプリケーションダウンロードインタフェースの対象である特定アプリケーションに適用される、または適用されるべく構成されたポリシーに関するより詳細な情報を含んでいてもよい。この詳細な情報はたとえば、ポリシーが何であるか、ポリシーがどのような機能を有効化および／もしくは無効化するか、ならびに／またはポリシーがどのような状態に適用されるか等を説明するコンテンツを送ってもよい。

【０１５６】

図８は、ここに説明される一つ以上の例示的態様に従って企業アプリケーションストアを使用してポリシー更新を管理アプリケーションに提供する方法を示すフローチャートである。一つ以上の実施形態において、図８に例示される方法および／またはその一もしくは複数のステップはコンピューティングデバイス（たとえば汎用コンピューティングデバイス２０１）により実施されてもよい。他の実施形態において、図８に例示される方法および／またはその一もしくは複数のステップは、不揮発性コンピュータ読取可能メモリ等のコンピュータ読取可能媒体に記憶されたコンピュータ実行可能命令において具体化されてもよい。

【０１５７】

図８に見られるように前記方法は、少なくとも一つのアプリケーションに対する更新済みポリシー情報を求めるポリシーエージェントからの要求が企業アプリケーションストアにおいて受信されるステップ８０５において開始される。例として、ステップ８０５において、上記実施例において説明される企業アプリケーションストアと同様、企業アプリケーションストアは更新済みポリシー情報を求める要求を受信してもよい。要求は特定アプリケーションに適用されてもよい（または適用されるべく構成されてもよい）ポリシーに関連していてもよく、たとえば、ユーザコンピューティングデバイス（たとえばスマートフォン、タブレットコンピュータ等のモバイルデバイス）上に常駐している、ユーザコンピューティングデバイス上で実行されている、および／またはユーザコンピューティングデバイスにより提供されるポリシーエージェントから受信されてもよい。

【０１５８】

たとえば更新済みポリシー情報を求める要求は、ラップ済みアプリケーションの実行時に（たとえばステップ８０５において企業アプリケーションストアにより）受信されてもよい。例として、企業アプリケーションストアは、ユーザコンピューティングデバイスがラップ済みアプリケーションを実行し始めた後に更新済みポリシー情報を求める要求を受信してもよい。このようなラップ済みアプリケーションはアプリケーションラッパと同様、たとえば企業アプリケーションおよび／またはラップ済みアプリケーションが実行されているデバイスに関して一つ以上のポリシーを強制適用すべく構成されてもよい企業アプリケーションを含んでいてもよい。その上、このようなアプリケーションラッパはたとえば、先に説明したアプリケーション管理フレームワーク４１４の一つ以上の態様を実現してもよい。

【０１５９】

たとえばポリシーエージェント（たとえばステップ８０５において受信される更新済みポリシー情報を求める要求の送信元）はモバイルデバイス管理（ＭＤＭ）ポリシー強制適用エージェント（たとえばユーザコンピューティングデバイス上の）であってもよい。このようなモバイルデバイス管理ポリシー強制適用エージェントはたとえば、ユーザコンピューティングデバイス上で実行され（または実行されるべく構成されており）さらに様々なアプリケーションおよびデバイス自身に関して様々なポリシーを監視および強制適用すべく構成されている個別のプログラム、処理またはサービスであってもよい。

【０１６０】

たとえばポリシーエージェント（たとえばステップ８０５において受信される更新済みポリシー情報を求める要求の送信元）は特定アプリケーションに対するアプリケーションラッパであってもよい。例として、ポリシーエージェントは、更新済みポリシー情報を求める要求がステップ８０５において受信される特定アプリケーションに対するアプリケーションラッパであってもよい。先に説明したように、このようなアプリケーションラッパはアプリケーションに関して一つ以上のポリシーを強制適用すべく構成されていてもよく、たとえば先に説明したアプリケーション管理フレームワーク４１４の一つ以上の態様を実現してもよい。

【０１６１】

更新済みポリシー情報を求める要求の受信（たとえばステップ８０５において）に基づいて、ステップ８１０において、少なくとも一つのアプリケーションに対する一つ以上のポリシーが更新されたか否かを判定してもよい。例として、ステップ８１０において、企業アプリケーションストアは、一つ以上のアプリケーション（たとえばステップ８０５において受信された要求の対象である一つ以上のアプリケーション）に対する一つ以上のポリシーが更新されたと判定してもよい。特定アプリケーションに対する一つ以上のポリシーはたとえば、アプリケーション自身が更新されていなくても更新されてもよい（たとえばポリシーは、アプリケーションをラップするのに使用されてもよいアプリケーションラッパおよび／またはアプリケーション自身とは無関係に修正することができる）。

【０１６２】

一つ以上の構成において、企業アプリケーションストアは、企業アプリケーションストアにより記憶され、企業アプリケーションストアにより保持され、および／または企業アプリケーションストアにアクセス可能であるポリシー情報に基づいてアプリケーションに対するポリシーが更新されたか否かを判定してもよい。たとえばこのようなポリシー情報は、図６を参照して上記実施例において説明されたように、モバイルサービス管理インタフェースを介して企業アプリケーションストアストアの管理ユーザから受信された情報等、企業アプリケーションの管理ユーザから受信されたユーザ入力および／または他の情報に基づいて企業アプリケーションストアにより作成され、アクセスされ、修正され、および／または記憶されてもよい。

【０１６３】

続けて図８を参照し、ステップ８１０において少なくとも一つのアプリケーションに対する一つ以上のポリシーが更新されなかったと判定された場合、次にステップ８１５において、ポリシーエージェントは更新データが入手不可能である旨を通知される。例として、ステップ８１５において、企業アプリケーションストアは、更新データが入手不可能である旨をポリシーエージェントに通知してもよい。たとえばステップ８１５において、企業アプリケーションストアは一つ以上のメッセージを（たとえばステップ８０５において受信された要求を送信した）ユーザコンピューティングデバイスに送信して、ポリシー更新が入手不可能である旨、および／またはポリシーエージェントが企業アプリケーションストアから既に取得した一つ以上のポリシーをユーザコンピューティングデバイスが使用および／または強制適用し続けるべきである旨をユーザコンピューティングデバイスおよび／またはその上で実行されているポリシーエージェントに通知してもよい。

【０１６４】

あるいは、ステップ８１０において少なくとも一つのアプリケーションに対する一つ以

上のポリシーが更新されたと判定された場合、次にステップ８２０において、少なくとも一つのポリシー更新がポリシーエージェントに提供されてもよい。例として、ステップ８２０において、企業アプリケーションストアは（たとえばステップ８０５において受信された要求を送信した）ユーザコンピューティングデバイスに一つ以上のメッセージを送信して、一つ以上のポリシー更新が入手可能である旨をユーザコンピューティングデバイスおよび／またはその上で実行されているポリシーエージェントに通知してもよい。その上、企業アプリケーションストアによりポリシーエージェントに送信された一つ以上のメッセージはたとえば新たな、および／または修正されたポリシーに関する情報を含んでいてもよく、このような情報は新たな、および／または修正されたポリシーを（たとえばポリシー変更が生じた特定アプリケーションに関して、および／またはデバイス自身に関して）ポリシーエージェントに実装および／または強制適用させるべく構成されている。

先に説明した実施例のように、一つ以上のポリシーは、一つ以上のアプリケーションのある特徴を有効化および／または無効化したり、デバイスのある特徴を有効化および／または無効化したり、あるリソースへのアクセスを有効化および／または無効化したり、他の機能および／または制限を提供したりすべく構成されていてもよく、提供された（たとえばステップ８２０におけるポリシーエージェントに対するポリシー更新として）情報は上記および／または他タイプのポリシーに対してなされたいずれかおよび／またはすべての変更を反映してもよい。

【０１６５】

図９は、ここに説明される一つ以上の例示的態様に従って企業アプリケーションストアを使用して管理アプリケーションにポリシー更新を提供する方法を示す別のフローチャートである。一つ以上の実施形態において、図９に例示される方法および／またはその一もしくは複数のステップはコンピューティングデバイス（たとえば汎用コンピューティングデバイス２０１）により実施されてもよい。他の実施形態において、図９に例示される方法および／またはその一もしくは複数のステップは、不揮発性コンピュータ読取可能メモリ等のコンピュータ読取可能媒体に記憶されたコンピュータ実行可能命令において具体化されてもよい。さらに／あるいは、図９に例示される方法はたとえば図８に例示される方法と組み合わされてもよい。例として、図９に例示される方法は、図８に例示される方法を実施する前および／または後に企業アプリケーションストアにより実施されてもよい。

【０１６６】

図９に見られるように前記方法は、アプリケーションに対するポリシー変更が企業アプリケーションストアにおいて受信されるステップ９０５において開始される。例として、ステップ９０５において、企業アプリケーションストアは、企業アプリケーションストアの管理ユーザから特定アプリケーションに対するポリシー変更を受信してもよい。このようなポリシー変更はたとえば、図６を参照して先に説明したようにモバイルサービス管理インタフェースを介して受信されてもよい。

【０１６７】

続けて図９を参照し、アプリケーションに対するポリシー変更が企業アプリケーションストアにより受信されるが更新済みポリシー情報を求める要求が未だ受信されていない場合、少なくともあるデバイスからの特定アプリケーションに関して、企業アプリケーションストアは影響を受けたデバイスに対してポリシー更新を積極的に提供する旨を判定してもよい。したがって、ポリシー変更の受信（たとえばステップ９０５において）に基づいて、ステップ９１０においてアプリケーション（すなわちステップ９０５においてポリシー変更が受信されたアプリケーション）が一つ以上のデバイス上に存在していると判定してもよい。

【０１６８】

例として、ステップ９１０において、企業アプリケーションストアは、アプリケーションが一つ以上の特定デバイス上にインストールされた、特定デバイスによりダウンロードされた、および／または特定デバイス上に存在していると判定してもよい。たとえばアプリケーションストアは、様々なアプリケーションおよびユーザに対するダウンロード履歴

情報、様々なアプリケーションおよびユーザに対する更新および／もしくはバージョン履歴情報、ならびに／または様々なアプリケーションおよびユーザに対するデバイス搭載監視情報に基づいて、アプリケーションが一つ以上の特定デバイス上にインストールされた、前記デバイスによりダウンロードされた、および／または前記デバイス上に存在していると判定してもよい。一つ以上の構成において、様々なアプリケーションおよびユーザに対するダウンロード履歴情報は、特定ユーザにより企業アプリケーションストアからダウンロードされたいずれかおよび／またはすべてのアプリケーションのバージョンおよび名称を各ユーザに対して示すユーザ鍵付きアプリケーションダウンロード記録と、このようなアプリケーションがダウンロードされた特定デバイスに対する識別情報とを含んでいてもよい。

【０１６９】

アプリケーションが一つ以上のデバイス上に存在している旨の（たとえばステップ９１０における）判定に基づいて、ポリシー変更に関連した情報はステップ９１５において一つ以上のデバイスに提供されてもよい。例として、ステップ９１５において、企業アプリケーションストアは、一つ以上の影響を受けたデバイス（たとえばステップ９１０においてアプリケーションが存在していると判定された一つ以上のデバイス）にポリシー変更に関する情報を提供してもよい。例として、ステップ９１５において、企業アプリケーションストアは、ステップ８２０においてポリシー更新が提供されてもよいのと同様に、ステップ９１０において識別されたデバイスに一つ以上のメッセージを公式化および送信してもよく、ここで一つ以上のメッセージは新たな、および／または修正されたポリシーに関する情報を含む。

【０１７０】

先に例示したように、本発明の様々な態様は企業アプリケーションストアの提供に関する。しかしながら他の実施形態において、ここに説明される概念は、コンシューマアプリケーションストアを含む他のいずれのタイプのアプリケーションにおいても実現することができる。したがって、発明の主題は構造的特徴および／または方法論的作用に固有の専門用語により説明されたが、添付クレームにおいて定義される発明の主題は必ずしも先に説明した固有の特徴および作用に限定されないことを理解されたい。むしろ、先に説明した固有の特徴および作用は以下のクレームのいくつかの実施態様例として記載されたものである。

【０１７１】

本出願は、２０１３年８月３０日に出願された「PROVIDING AN ENTERPRISE APPLICATION STORE」と題する米国特許出願第１４／０１５，１０８号に基づく優先権を主張し、そのすべてを引用により組入れるものである。また、本出願は２０１３年７月２２日に出願された「PROVIDING AN ENTERPRISE APPLICATION STORE」と題する米国仮特許出願第６１／８５６，９３０号に基づく優先権を主張し、そのすべてを引用により組み入れるものである。また、本出願は２０１３年３月２９日に出願された「SYSTEMS AND METHODS FOR ENTERPRISE MOBILITY MANAGEMENT」と題する米国仮特許出願第６１／８０６，５７７号に基づく優先権を主張し、そのすべてを引用により組入れるものである。

【０１７２】

〈サンプル実施形態〉

予備的な請求項１から２０の組Ａを以下に示す。

【０１７３】

本発明のサンプル実施形態は以下を含む。

【０１７４】

１．アプリケーションストアの管理ユーザの認証クレデンシャルを前記アプリケーションストアにおいて受信するステップと、

前記管理ユーザの前記認証クレデンシャルの検証に基づいて前記アプリケーションストアを介してモバイルサービス管理インタフェースを提供するステップと

を含み、

前記モバイルサービス管理インタフェースは、前記管理ユーザが前記アプリケーションストアにおいて入手可能な少なくとも一つのアプリケーションに適用されるべき一つ以上のポリシーを定義できるように少なくとも一つの制御を備えており、
前記一つ以上のポリシーは少なくとも一つのモバイルデバイス上における前記少なくとも一つのアプリケーションの実行中、前記少なくとも一つのアプリケーションの機能を制御すべく構成されていることを特徴とする方法。
【０１７５】
２．前記少なくとも一つの制御はさらに、前記管理ユーザが前記少なくとも一つのアプリケーションの相異なるユーザに対して相異なるポリシーを定義できるように構成されていることを特徴とする、請求項１に記載の方法。
【０１７６】
３．前記相異なるポリシーは相異なるユーザ職務に対して定義されることを特徴とする、請求項２に記載の方法。
【０１７７】
４．前記モバイルサービス管理インタフェースを介して第１アプリケーションに対するポリシー変更を受信するステップと、
前記ポリシー変更に関連した情報を前記第１アプリケーションを有する少なくとも一つのモバイルデバイスに前記アプリケーションストアにより提供するステップとをさらに備えることを特徴とする、請求項１に記載の方法。
【０１７８】
５．前記アプリケーションストアの非管理ユーザの認証クレデンシャルを前記アプリケーションストアにおいて受信するステップと、
前記非管理ユーザの前記認証クレデンシャルの検証に基づいて、前記アプリケーションストアを介して前記少なくとも一つのアプリケーションに対するアプリケーションダウンロードインタフェースを提供するステップと
をさらに備え、
前記アプリケーションダウンロードインタフェースは前記管理ユーザにより定義される一つ以上のポリシーに対応する少なくとも一つのインディケータを備えることを特徴とする、請求項１に記載の方法。
【０１７９】
６．前記モバイルサービス管理インタフェースは前記アプリケーションストアにおける前記少なくとも一つのアプリケーションの受信に応じて提供されることを特徴とする、請求項１に記載の方法。
【０１８０】
７．前記管理ユーザの前記認証クレデンシャルの検証の後、前記アプリケーションストアにおいて前記管理ユーザからの新アプリケーションを受信するステップと、
前記新アプリケーションに適用されるべき一つ以上のポリシーを定義するよう前記管理ユーザに促すステップと、
前記新アプリケーションに適用されるべき前記管理ユーザからの少なくとも一つのポリシーを前記アプリケーションストアにおいて受信するステップとをさらに備えることを特徴とする、請求項１に記載の方法。
【０１８１】
８．前記新アプリケーションに適用されるべき一つ以上のポリシーを定義するよう前記管理ユーザに促すステップは、
前記新アプリケーションに対して一つ以上の関連ポリシーを識別するステップと、
前記モバイルサービス管理インタフェースを更新して、前記管理ユーザが前記一つ以上の検証済みポリシーを管理できるように構成された少なくとも一つの制御を含ませるステップとを含むことを特徴とする、請求項７に記載の方法。
【０１８２】
９．少なくとも一つのプロセッサと、

前記少なくとも一つのプロセッサにより実行されると装置に、
アプリケーションストアの管理ユーザの認証クレデンシャルを前記アプリケーションストアにおいて受信させ、
前記管理ユーザの前記認証クレデンシャルの検証に基づいて前記アプリケーションストアを介してモバイルサービス管理インタフェースを提供させるコンピュータ読取可能命令を記憶するメモリと
を備え、
前記モバイルサービス管理インタフェースは、前記管理ユーザが前記アプリケーションストアにおいて入手可能な少なくとも一つのアプリケーションに適用されるべき一つ以上のポリシーを定義できるように構成された少なくとも一つの制御を備えており、
前記一つ以上のポリシーは少なくとも一つのモバイルデバイス上における前記少なくとも一つのアプリケーションの実行中、前記少なくとも一つのアプリケーションの機能を制御すべく構成されていることを特徴とする装置。

【０１８３】

１０．前記少なくとも一つの制御はさらに、前記管理ユーザが前記少なくとも一つのアプリケーションの相異なるユーザに対して相異なるポリシーを定義できるように構成されていることを特徴とする、請求項９に記載の装置。

【０１８４】

１１．前記相異なるポリシーは相異なるユーザ職務に対して定義されることを特徴とする、請求項１０に記載の装置。

【０１８５】

１２．前記メモリは、前記少なくとも一つのプロセッサにより実行されると前記装置にさらに、
前記モバイルサービス管理インタフェースを介して第１アプリケーションに対するポリシー変更を受信させ、
前記ポリシー変更に関連した情報を前記第１アプリケーションを有する少なくとも一つのモバイルデバイスに前記アプリケーションストアにより提供させる追加コンピュータ読取可能命令を記憶することを特徴とする、請求項９に記載の装置。

【０１８６】

１３．前記メモリは、前記少なくとも一つのプロセッサにより実行されると前記装置にさらに、
前記アプリケーションストアの非管理ユーザの認証クレデンシャルを前記アプリケーションストアにおいて受信させ、
前記非管理ユーザの前記認証クレデンシャルの検証に基づいて、前記アプリケーションストアを介して前記少なくとも一つのアプリケーションに対するアプリケーションダウンロードインタフェースを提供させる追加コンピュータ読取可能命令を記憶し、
前記アプリケーションダウンロードインタフェースは前記管理ユーザにより定義される一つ以上のポリシーに対応する少なくとも一つのインディケータを備えることを特徴とする、請求項９に記載の装置。

【０１８７】

１４．前記モバイルサービス管理インタフェースは前記アプリケーションストアにおける前記少なくとも一つのアプリケーションの受信に応じて提供されることを特徴とする、請求項９に記載の装置。

【０１８８】

１５．前記メモリは、前記少なくとも一つのプロセッサにより実行されると前記装置にさらに、
前記管理ユーザの前記認証クレデンシャルの認証の後、前記アプリケーションストアにおいて前記管理ユーザからの新アプリケーションを受信させ、
前記新アプリケーションに適用されるべき一つ以上のポリシーを定義するよう前記管理ユーザに促させ、

前記新アプリケーションに適用されるべき前記管理ユーザからの少なくとも一つのポリシーを前記アプリケーションストアにおいて受信させる追加コンピュータ読取可能命令を記憶することを特徴とする、請求項９に記載の装置。

【０１８９】

１６．前記新アプリケーションに適用されるべき一つ以上のポリシーを定義するよう前記管理ユーザに促すステップは、

前記新アプリケーションに対して一つ以上の関連ポリシーを識別するステップと、

前記モバイルサービス管理インタフェースを更新して、前記管理ユーザが前記一つ以上の識別済みポリシーを管理できるように構成された少なくとも一つの制御を含ませるステップとを含むことを特徴とする、請求項１５に記載の装置。

【０１９０】

１７．実行されると少なくとも一つの計算装置に、

アプリケーションストアの管理ユーザの認証クレデンシャルを前記アプリケーションストアにおいて受信させ、

前記管理ユーザの前記認証クレデンシャルの検証に基づいて前記アプリケーションを介してモバイルサービス管理インタフェースを提供させる命令を記憶しており、

前記モバイルサービス管理インタフェースは、前記管理ユーザが前記アプリケーションストアにおいて入手可能な少なくとも一つのアプリケーションに適用されるべき一つ以上のポリシーを定義できるように少なくとも一つの制御を備えており、

前記一つ以上のポリシーは少なくとも一つのモバイルデバイス上における前記少なくとも一つのアプリケーションの実行中、前記少なくとも一つのアプリケーションの機能を制御すべく構成されていることを特徴とする一つ以上の不揮発性コンピュータ読取可能媒体。

【０１９１】

１８．実行されると前記少なくとも一つの計算装置にさらに、

前記モバイルサービス管理インタフェースを介して第１アプリケーションに対するポリシー変更を受信させ、

前記ポリシー変更に関連した情報を前記第１アプリケーションを有する少なくとも一つのモバイルデバイスに前記アプリケーションストアにより提供させる追加命令を記憶してあることを特徴とする、請求項１７に記載の一つ以上の不揮発性コンピュータ読取可能媒体。

【０１９２】

さらなる予備的な請求項１から２０の組Ｂを以下に示す。

【０１９３】

本発明の追加サンプル実施形態は以下を含む。

【０１９４】

１．少なくとも一つのアプリケーションに対する更新済みポリシー情報を求めるポリシーエージェントからの要求をアプリケーションストアにおいて受信するステップと、

前記要求の受信に基づいて、前記少なくとも一つのアプリケーションに対する一つ以上のポリシーが更新されたか否かを前記アプリケーションストアにおいて判定するステップと、

前記少なくとも一つのアプリケーションに対する前記一つ以上のポリシーが更新された旨の判定に基づいて、少なくとも一つのポリシー更新を前記ポリシーエージェントに提供するステップと、

第１アプリケーションに対するポリシー変更を前記アプリケーションストアにおいて受信するステップと、

前記第１アプリケーションが一つ以上の装置上に存在している旨を判定するステップと、

前記ポリシー変更に関連した情報を前記一つ以上の装置に提供するステップとを備えることを特徴とする方法。

【０１９５】
２．前記少なくとも一つのアプリケーションに対する前記一つ以上のポリシーが更新されていない旨の判定に基づいて、更新データが入手不可能である旨を前記ポリシーエージェントに通知するステップと
をさらに備えることを特徴とする、請求項１に記載の方法。
【０１９６】
３．前記ポリシーエージェントからの更新済みポリシー情報を求める前記要求はラップ済みアプリケーションの実行時に受信されることを特徴とする、請求項１に記載の方法。
【０１９７】
４．前記一つ以上の装置上において前記第１アプリケーションに加えて一つ以上の他のアプリケーションに対して一つ以上のポリシー更新が入手可能であるか否かを判定するステップと、
前記一つ以上の他のアプリケーションに対して一つ以上のポリシー更新が入手可能である旨の判定に基づいて、前記一つ以上の他のアプリケーションに対する前記一つ以上の入手可能なポリシー更新を前記一つ以上の装置に提供するステップとをさらに備えることを特徴とする、請求項１に記載の方法。
【０１９８】
５．前記第１アプリケーションが前記一つ以上の装置上に存在している旨の判定は、前記アプリケーションストアに関連した一つ以上のユーザ鍵付きアプリケーションダウンロード記録に基づくことを特徴とする、請求項１に記載の方法。
【０１９９】
６．前記ポリシーエージェントはモバイルデバイス管理ポリシー強制適用エージェントであることを特徴とする、請求項１に記載の方法。
【０２００】
７．前記ポリシーエージェントは前記少なくとも一つのアプリケーションに対するアプリケーションラッパであることを特徴とする、請求項１に記載の方法。
【０２０１】
８．少なくとも一つのプロセッサと、
前記少なくとも一つのプロセッサにより実行させると装置に、
少なくとも一つのアプリケーションに対するポリシーエージェントからの更新済みポリシー情報を求める要求をアプリケーションストアにおいて受信させ、
前記要求の受信に基づいて、前記少なくとも一つのアプリケーションに対する一つ以上のポリシーが更新されたか否かを前記アプリケーションストアにおいて判定させ、
前記少なくとも一つのアプリケーションに対する前記一つ以上のポリシーが更新された旨の判定に基づいて、少なくとも一つのポリシー更新を前記ポリシーエージェントに提供させ、
第１アプリケーションに対するポリシー変更を前記アプリケーションストアにおいて受信させ、
前記第１アプリケーションが一つ以上の装置上に存在している旨を判定させ、
前記ポリシー変更に関連した情報を前記一つ以上の装置に提供させる
コンピュータ読取可能命令を記憶するメモリとを備えることを特徴とする装置。
【０２０２】
９．前記メモリは、前記少なくとも一つのプロセッサにより実行されると前記装置にさらに、
前記少なくとも一つのアプリケーションに対する前記一つ以上のポリシーが更新されていない旨の判定に基づいて、更新データが入手不可能である旨を前記ポリシーエージェントに通知させる追加コンピュータ読取可能命令を記憶することを特徴とする、請求項８に記載の装置。
【０２０３】
１０．前記ポリシーエージェントからの更新済みポリシー情報を求める前記要求はラッ

プ済みアプリケーションの実行時に受信されることを特徴とする、請求項８に記載の装置。

【０２０４】

１１．前記メモリは、前記少なくとも一つのプロセッサにより実行されると前記装置にさらに、

前記一つ以上の装置上において前記第１アプリケーションに加えて一つ以上の他のアプリケーションに対して一つ以上のポリシー更新が入手可能であるか否かを判定させ、

前記一つ以上の他のアプリケーションに対して一つ以上のポリシー更新が入手可能である旨の判定に基づいて、前記一つ以上の他のアプリケーションに対する前記一つ以上の入手可能なポリシー更新を前記一つ以上の装置に提供させる追加コンピュータ読取可能命令を記憶することを特徴とする、請求項８に記載の装置。

【０２０５】

１２．前記第１アプリケーションが前記一つ以上の装置上に存在している旨の判定は、前記アプリケーションストアに関連した一つ以上のユーザ鍵付きアプリケーションダウンロード記録に基づくことを特徴とする、請求項８に記載の装置。

【０２０６】

１３．前記ポリシーエージェントはモバイルデバイス管理ポリシー強制適用エージェントであることを特徴とする、請求項８に記載の装置。

【０２０７】

１４．前記ポリシーエージェントは前記少なくとも一つのアプリケーションに対するアプリケーションラッパであることを特徴とする、請求項８に記載の装置。

【０２０８】

１５．実行されると少なくとも一つの計算装置に、

少なくとも一つのアプリケーションに対する更新済みポリシー情報を求めるポリシーエージェントからの要求をアプリケーションストアにおいて受信させ、

前記要求の受信に基づいて、前記少なくとも一つのアプリケーションに対する一つ以上のポリシーが更新されたか否かを前記アプリケーションストアにおいて判定させ、

前記少なくとも一つのアプリケーションに対する前記一つ以上のポリシーが更新された旨の判定に基づいて、少なくとも一つのポリシー更新を前記ポリシーエージェントに提供させ、

第１アプリケーションに対するポリシー変更を前記アプリケーションストアにおいて受信させ、

前記第１アプリケーションが一つ以上の装置上に存在している旨を判定させ、

前記ポリシー変更に関連した情報を前記一つ以上の装置に提供させる命令を記憶する一つ以上の不揮発性コンピュータ読取可能媒体。

【０２０９】

１６．実行されると前記少なくとも一つの計算装置にさらに、

前記少なくとも一つのアプリケーションに対する前記一つ以上のポリシーが更新されていない旨の判定に基づいて、更新データが入手不可能である旨を前記ポリシーエージェントに通知させる追加命令を記憶してある、請求項１５に記載の一つ以上の不揮発性コンピュータ読取可能媒体。

【０２１０】

１７．前記ポリシーエージェントからの更新済みポリシー情報を求める前記要求はラップ済みアプリケーションの実行時に受信されることを特徴とする、請求項１５に記載の一つ以上の不揮発性コンピュータ読取可能媒体。

【０２１１】

１８．実行されると前記少なくとも一つの計算装置にさらに、

前記一つ以上の装置上において前記第１アプリケーションに加えて一つ以上の他のアプリケーションに対して一つ以上のポリシー更新が入手可能であるか否かを判定させ、

前記一つ以上の他のアプリケーションに対して一つ以上のポリシー更新が入手可能であ

る旨の判定に基づいて、前記一つ以上の他のアプリケーションに対する前記一つ以上の入手可能なポリシー更新を前記一つ以上の装置に提供させる追加命令を記憶してある、請求項１５に記載の一つ以上の不揮発性コンピュータ読取可能媒体。

【０２１２】

１９．前記ポリシーエージェントはモバイルデバイス管理ポリシー強制適用エージェントであることを特徴とする、請求項１５に記載の一つ以上の不揮発性コンピュータ読取可能媒体。

【０２１３】

２０．前記ポリシーエージェントは前記少なくとも一つのアプリケーションに対するアプリケーションラッパであることを特徴とする、請求項１５に記載の一つ以上の不揮発性コンピュータ読取可能媒体。

【図１】

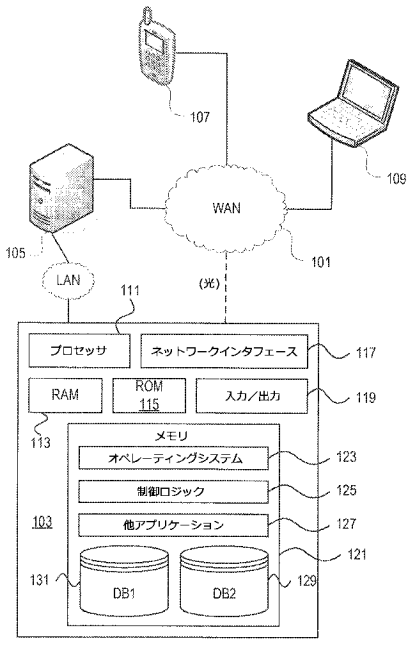

図１

【図２】

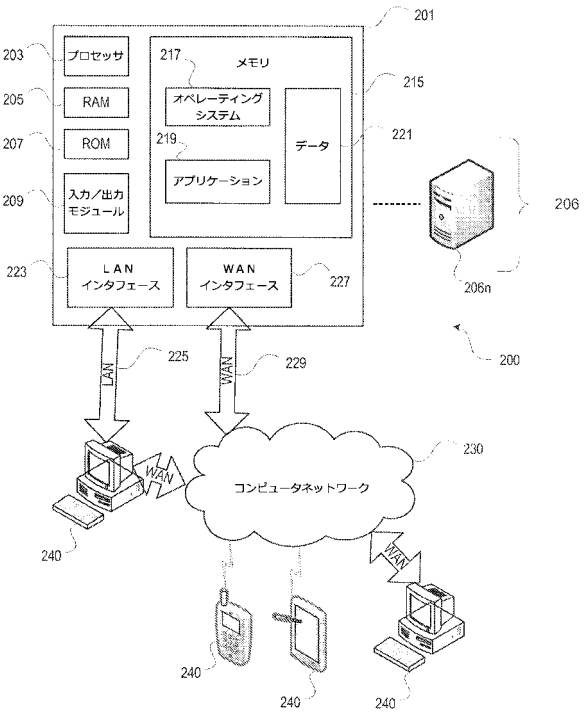

図２

【図３】

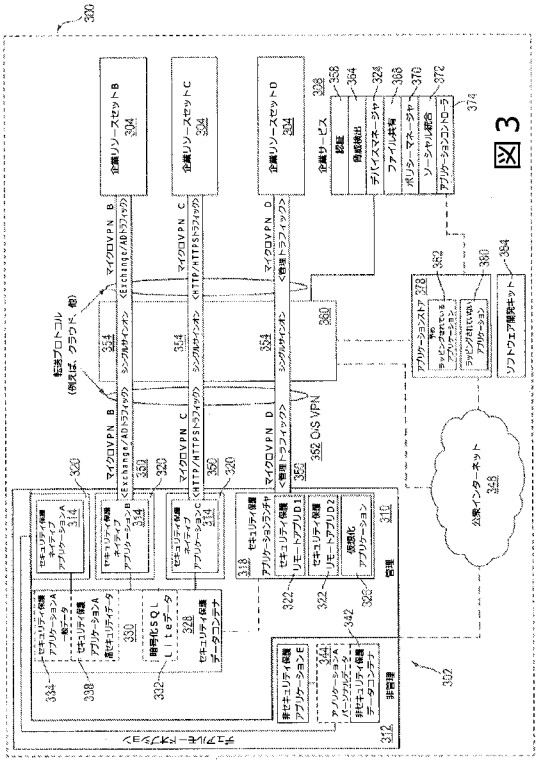

図３

【図４】

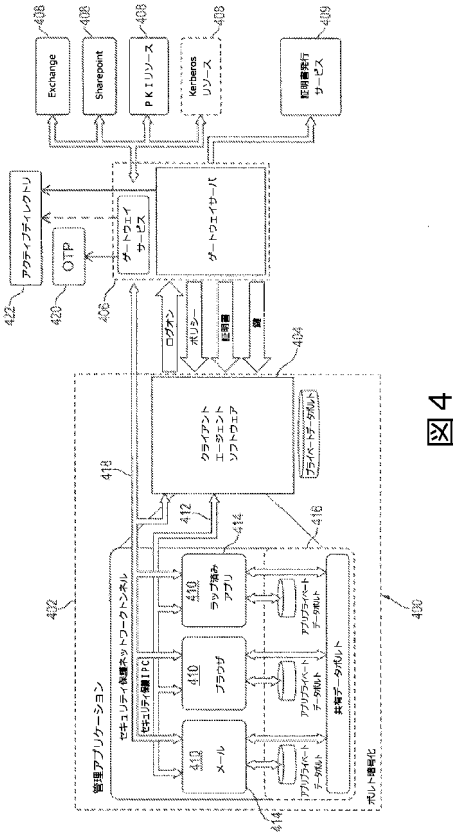

図４

【図５】

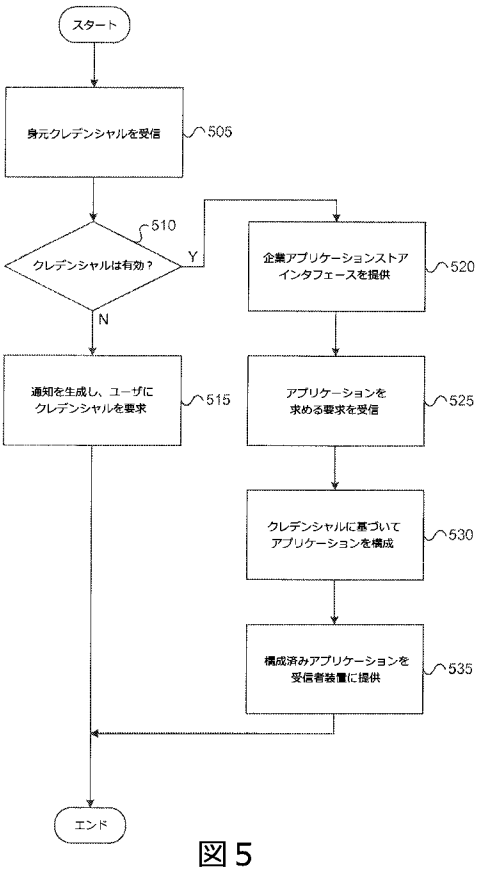

図５

【図６】

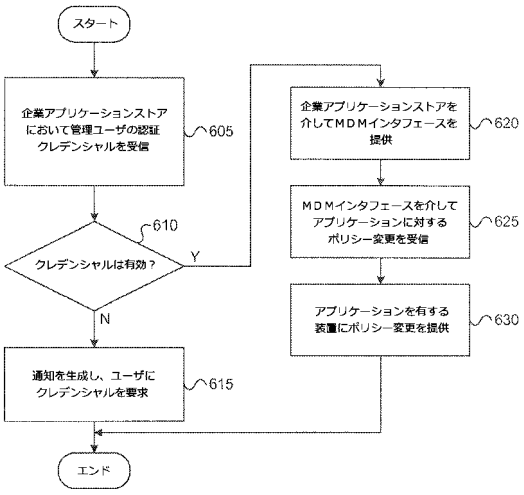

図６

【図７】

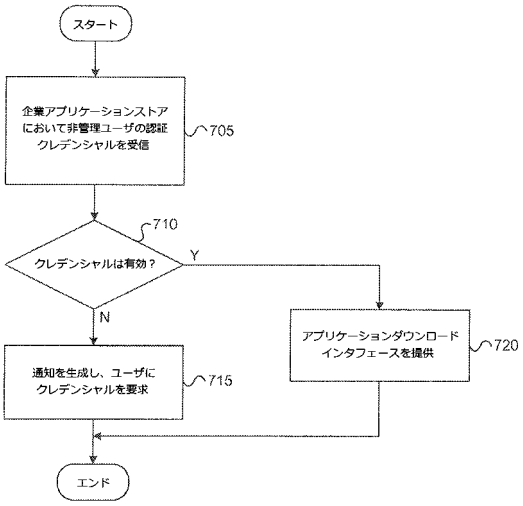

図７

【図８】

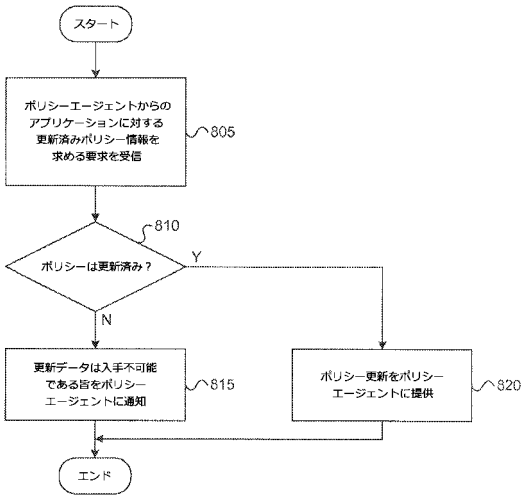

図８

【図９】

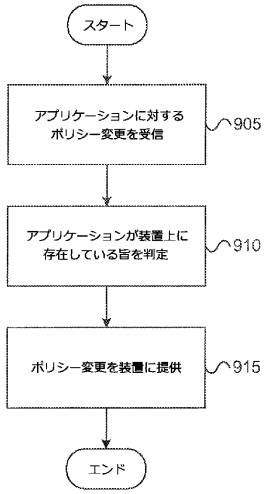

図９

フロントページの続き

(51)Int.Cl.	FI	テーマコード（参考）
	Ｇ０６Ｆ　13/00　　５３０Ａ	

(72)発明者　ヘイトン，リチャード
アメリカ合衆国，フロリダ州　３３３０９，フォート　ローダーデール，ウエスト　サイプレス　クリーク　ロード　８５１，サイトリックス　システムズ，インコーポレイテッド内

Ｆターム(参考) 5B084 AA02 AA12 AA28 AA30 AB16 AB24 AB31 AB36 AB39 BA07
BB16 CC06 CC07 CC14 CD09 CD10 CD22 CD24 CE02 CE12
DA15 DB01 DB08 DC02 DC27 FA24 FA43
5B376 AB06 AB17 FA13