

(19) 日本国特許庁(JP)

(12) 公表特許公報(A)

(11) 特許出願公表番号

特表2017-528811

(P2017-528811A)

(43) 公表日 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 610A	5B376
G06F 21/31 (2013.01)	G06F 21/31	
	G06F 9/06 610Q	

審査請求 未請求 予備審査請求 有 (全 15 頁)

(21) 出願番号 特願2017-507818 (P2017-507818)
 (86) (22) 出願日 平成27年9月17日 (2015. 9. 17)
 (85) 翻訳文提出日 平成29年3月31日 (2017. 3. 31)
 (86) 国際出願番号 PCT/US2015/050543
 (87) 国際公開番号 W02016/044502
 (87) 国際公開日 平成28年3月24日 (2016. 3. 24)
 (31) 優先権主張番号 14/491, 006
 (32) 優先日 平成26年9月19日 (2014. 9. 19)
 (33) 優先権主張国 米国 (US)

(71) 出願人 314015767
 マイクロソフト テクノロジー ライセン
 シング, エルエルシー
 アメリカ合衆国 ワシントン州 9805
 2 レッドモンド ワン マイクロソフト
 ウェイ
 (74) 代理人 100079108
 弁理士 稲葉 良幸
 (74) 代理人 100109346
 弁理士 大貫 敏史
 (74) 代理人 100117189
 弁理士 江口 昭彦
 (74) 代理人 100134120
 弁理士 内藤 和彦

最終頁に続く

(54) 【発明の名称】 多数のアイデンティティのアプリケーションに対するポリシーの適用

(57) 【要約】

管理アカウントと関連するアプリケーションの挙動の制御。デバイスは1つ以上のアプリケーションを含む。アプリケーションのうち少なくとも1つは、0以上の管理ユーザアカウントを含む複数のユーザアカウントと共に使用されるように構成される。デバイスはクライアントコンポーネントを含むか、又は通信する。クライアントコンポーネントは、アプリケーションに対し有効なユーザアカウントを識別するように構成される。クライアントコンポーネントはさらに、管理システムからポリシーを受信するように構成され、ポリシーはユーザアカウントを基準としてアプリケーション制御を指定する。クライアントコンポーネントは、さらに、管理システムや有効なユーザアカウントのポリシーに基づいたアプリケーション構成を実施するように構成されている。

【選択図】 図1

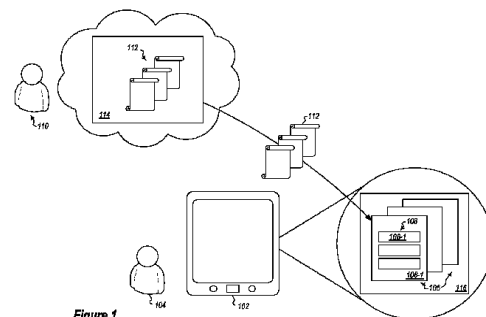


Figure 1

【特許請求の範囲】**【請求項 1】**

管理アカウントに関連するアプリケーションの挙動を制御するコンピュータに実装される方法であって、

前記コンピュータに実装される方法は、前記方法のためにコンピュータで実行可能な命令を実行する1つ以上のプロセッサによって行われ、

前記コンピュータに実装される方法は、

前記アプリケーションに有効な0以上の管理ユーザアカウントを含む1つ以上のユーザアカウントのセットを識別することを含む、アプリケーションの状態を識別することと、

前記アプリケーションの状態に関するポリシーを調べることであって、前記ポリシーは、管理ユーザアカウント用に定義された1つ以上の異なるポリシーを備え、それぞれの異なるポリシーは、1つ以上の管理ユーザアカウントに対してアプリケーション構成の制御を定義することと、

前記ポリシー及び前記アプリケーションの状態に基づいて、前記ポリシーに対して有効なユーザアカウントを含む、前記ポリシーに対するアプリケーション構成を制御することと、

前記アプリケーションに有効な1つ以上のユーザアカウントの前記セットの変更を含む、変更されたアプリケーションの状態を識別することと、

ポリシー及び前記変更されたアプリケーションの状態に基づいて、前記アプリケーション構成の制御を変更することと、

を含む、方法。

【請求項 2】

アプリケーション状態は、グローバルアプリケーションの状態である、請求項1に記載のコンピュータに実装される方法。

【請求項 3】

アプリケーション状態は、スレッド状態である、請求項1に記載のコンピュータに実装される方法。

【請求項 4】

アプリケーション状態は、プロセス状態である、請求項1に記載のコンピュータに実装される方法。

【請求項 5】

1つ以上のユーザアカウントのセットの識別が前記アプリケーションによって行われ、管理システムのクライアントコンポーネントに伝達される、請求項1に記載のコンピュータに実装される方法。

【請求項 6】

1つ以上のユーザアカウントのセットの識別がクライアント管理エンティティによって行われる、請求項1に記載のコンピュータに実装される方法。

【請求項 7】

前記アプリケーション構成の制御が、データ使用、データ共有、暗号化、アカウントの起動時間のチェック又は動作環境のうち1つ以上を制御することを含む、請求項1に記載のコンピュータに実装される方法。

【請求項 8】

前記アプリケーション構成の制御は、管理権限によって定義されたグラフィカルユーザインタフェースの性能を含む、請求項1に記載のコンピュータに実装される方法。

【請求項 9】

1つ以上のアカウントのセットの識別がデータセットの特徴を取得することによって行われる、請求項1に記載のコンピュータに実装される方法。

【請求項 10】

1つ以上のプロセッサと、

前記1つ以上のプロセッサによって実行されると、前記1つ以上のプロセッサに、管理

10

20

30

40

50

アカウントに関連するアプリケーションの挙動を制御するコンピュータに実装される方法を行わせるコンピュータで実行可能な命令を含む1つ以上のコンピュータ可読媒体と、を備え、

前記コンピュータに実装される方法は、

前記アプリケーションに有効な0以上の管理ユーザアカウントを含む1つ以上のユーザアカウントのセットを識別することを含む、アプリケーションの状態を識別することと、

前記アプリケーションの状態に関するポリシーを調べることであって、前記ポリシーは、管理ユーザアカウント用に定義された1つ以上の異なるポリシーを備え、それぞれの異なるポリシーは、1つ以上の管理ユーザアカウントに対してアプリケーション構成の制御を定義することと、

前記ポリシー及び前記アプリケーションの状態に基づいて、前記ポリシーに対して有効なユーザアカウントを含む、前記ポリシーに対するアプリケーション構成を制御することと、

前記アプリケーションに有効な1つ以上のユーザアカウントの前記セットの変更を含む、変更されたアプリケーションの状態を識別することと、

ポリシー及び前記変更されたアプリケーションの状態に基づいて、前記アプリケーション構成の制御を変更することと、を含む、コンピューティングシステム。

10

【発明の詳細な説明】

20

【技術分野】

【0001】

【0001】 IT管理者は、長期間にわたりデバイスに管理ポリシーを対象とすることが可能であった。モバイル機器の出現により、産業上の解決策を通じて特定のアプリケーションを含むことを目的としたポリシーが拡大されてきた。例えば、様々なプロバイダによって利用可能な様々なモバイル用のアプリケーション管理策である。加えて、ユーザはますます同一デバイスを仕事、個人的な使用又は多数の会社用に使用している。例えば、コンサルタントや請負業者は、同じデバイスを使用して、異なる企業のリソースにアクセスすることができる。これは、多数のアカウント又はアイデンティティによる使用をサポートするアプリケーションによってもたらされる。例えば、メールアプリケーションは、1つ以上の異なる企業の受信箱と同様に個人の受信箱を含み得る。代替的实施例では、クラウドストレージのアプリケーションは、多数の異なる企業サービスに接続することが可能であり得る。

30

【0002】

【0002】 しかしながら、問題の1つは、IT管理ポリシーは、デバイス又はアプリケーションに包括的にしか適用されることができない。これは、多数のアイデンティティに使用されるアプリケーションは同一のポリシーにより制約されるという望ましくない副次的な影響がある。この制限により、IT管理者が特定の企業のアイデンティティを管理しようとするためだけであったとしても、すべてのアイデンティティに対し、アプリケーションから機能を削除又は除去できる。現在、IT管理者は、アプリケーション内ですべてのアイデンティティに対し同一のポリシーを有するか、同一のアプリケーションに多数のコピーを配布するか、又は特定のアプリケーションから（個人又はその他のアクセスを不可能にする一方で）企業のアクセスのみを可能にするかを余儀なくさせられ、どのバージョンが使用されるべきかユーザに混乱を生じる結果になる。

40

【発明の概要】

【0003】

【0003】 本明細書において特許請求される主題は、いかなる不利な点をも解決し、又は前述したもののような環境においてのみ動作する実施形態に限定されるものではない。むしろ、この背景技術は、本明細書に記載されるいくつかの実施形態が実行され得る、1つの例示的な技術領域を例示するためにのみ提供されている。

50

【0004】

[0004] 本明細書に示される一実施形態では、コンピューティング環境で実行することができる方法を含む。本方法は、管理アカウントと関連するアプリケーションの挙動を制御するための動作を含む。この方法は、アプリケーションの状態を識別することを含む。これはアプリケーションに対し有効な0以上の管理ユーザアカウントを含む、1つ以上のユーザアカウントのセットを識別することを含む。本方法はさらに、アプリケーションの状態に関するポリシーを調べることを含む。ポリシーは、管理ユーザアカウント用に定義された1つ以上の異なるポリシーを備える。それぞれの異なるポリシーは、1つ以上の管理ユーザアカウントに対してアプリケーション構成の制御を定義する。ポリシー及びアプリケーションの状態に基づいて、本方法は、ポリシーに対するアプリケーション構成を制御することを含み、これはポリシーに対して有効なユーザアカウントを含む。この方法は、アプリケーションで有効な1つ以上のユーザアカウントのセットを変更することを含む、変更されたアプリケーションの状態を識別することを含む。本方法はさらに、ポリシー及び変更されたアプリケーションの状態に基づいて、アプリケーション構成の制御を変更することを含む。

10

【0005】

[0005] 別の実施形態は、管理アカウントに関連するアプリケーションの挙動を制御するように構成されたコンピューティングデバイスを含む。デバイスは1つ以上のアプリケーションを含む。アプリケーションのうち少なくとも1つは、0以上の管理ユーザアカウントを含む複数のユーザアカウントと共に使用されるように構成される。デバイスはクライアントコンポーネントを含む。クライアントコンポーネントは、アプリケーションに対し有効なユーザアカウントを識別するように構成される。クライアントコンポーネントはさらに、管理システムからポリシーを受信するように構成され、ポリシーはユーザアカウントに基づいてアプリケーションの制御を特定する。クライアントコンポーネントは、さらに、管理システムや有効なユーザアカウントのポリシーに基づいたアプリケーション構成を行うように構成されている。

20

【0006】

[0006] 本概要は、発明を実施するための形態において以下にさらに記載された、簡略化した形態における概念の選択を導入するために提供される。本概要は、請求する主題の鍵となる特徴又は本質的な特徴を識別することを意図するものではなく、請求する主題の範囲を決定する上での手助けとして、単独で使用されることを意図していない。

30

【0007】

[0007] 追加の特徴及び利点は、以下の説明に記載され、記載から一部は明らかになり、又は本明細書の教示を実行することによって知り得る。本発明の特徴と利点は添付請求項に具体的に記載されている要素及び組み合わせによって実現され、得られ得る。本発明の特徴は、以下の説明及び添付の請求項によりさらに明らかになるか、又は本明細書において以下に記述する発明を実行することにより取得され得る。

【0008】

[0008] 前述の、及びその他の利点並びに特徴が得られることが可能な手法を記載するために、上記で簡潔に述べた主題のより具体的な記載が、添付の図面に示された特定の実施形態への参照によって示されるであろう。これらの図面は典型的な実施形態のみを示し、したがって範囲を制限すると考えられないという理解のもと、実施形態は、添付図面の使用を通してさらに具体的かつ詳細に記載され説明されるであろう。

40

【図面の簡単な説明】

【0009】

【図1】[0009]アプリケーション構成が有効なユーザアカウントに基づいて制御される環境を示す。

【図2】[0010]管理アカウントに関連するアプリケーションの挙動を制御する方法を示す。

【発明を実施するための形態】

50

【 0 0 1 0 】

[0011] 本明細書の実施形態は、IT管理者が、ポリシーと、クライアント及び/又は対象のアプリケーションにおける管理アイデンティティのためだけにポリシーを有効にし、行うアプリケーションコンポーネントとを有する特定のアイデンティティを対象にするのを可能にする。このように、ポリシーは管理アイデンティティに適用され、一方、非管理アイデンティティにはポリシーを適用されない。さらに、異なるポリシーは異なる管理アイデンティティに適用されることができ、このように、機能を制限するポリシーは、その他のアイデンティティへの管理性能も保持しつつ、いくつかのアイデンティティに対する機能を保持するために、異なるアイデンティティに必要とされないときには適用されない。したがって、例えば、同一のアプリケーション内では、ユーザは、管理企業のアイデンティティを（雇用されている組織で使用する目的で）使用する場合には、データの切り取り及び貼り付けを制限される可能性があるが、個人用のアイデンティティを（自分の個人的使用のために）使用する場合には制限されないであろう。

10

【 0 0 1 1 】

[0012] ここで図1を参照すると、一実施例が示されている。図1は、デバイス102を示す。デバイス102は、携帯電話、タブレット又はその他の適切なコンピューティングデバイスであり得る。デバイス102は、通常、ユーザ104が所有する。

【 0 0 1 2 】

[0013] デバイス102は、複数のアプリケーション106を有し得る。各アプリケーションは複数のアカウント108を提供し得る。したがって、例えば、アプリケーション106-1は、個人用アカウントを有する電子メールのアプリケーション及び1つ以上の管理企業（又はその他の組織）のアカウントであり得る。デバイス102が企業アカウントにアクセスするために使用されると、これらのアカウントに関連する企業（又はその他の組織）は、これらのアカウントが使用されている間、デバイス102のアプリケーションに特定の制限をかけることを望み得る。例えば、企業は、企業データが閲覧されるときに、アプリケーション106-1において切り取り/コピー/貼り付け機能ができることを望まない場合がある。しかしながら、ユーザが個人アカウント108-1を使用する場合、切り取り/コピー/貼り付け機能が有効であるか企業は気にかけないか、又は制御するための基準を有さない可能性がある。しかしながら、ユーザ104は、このような機能が有効であることを望み得る。実施形態は異なるポリシーを異なるデバイスの同一ユーザにサポートし得る。例えば、株式トレーダのモバイル機器では、いくつかのアプリケーション機能がロックされ得るが、しかし、取引フロアの株式トレーダのラップトップあるいはタブレット上では、機能はロックされない。

20

30

【 0 0 1 3 】

[0014] IT管理者110は、1つ以上のアプリケーション用に、管理システム114で管理ポリシー112を作成する。IT管理者110は、アプリケーションの特定のユーザを対象とするポリシーを作成して、ポリシーをユーザのデバイスに配布させることができる。あるいは又はさらにIT管理者は、ユーザの代わりに特定のドメインを対象とするポリシーを作成することができる。例えば、特定のサイトアドレスのすべてのユーザには、同一のポリシーが適用されるであろう。

40

【 0 0 1 4 】

[0015] 図1に示すように、管理システム114は、ポリシー112を適切なアプリケーション106-1に配布する。デバイス102のクライアントコンポーネント116はポリシー112を解釈し処理する。

【 0 0 1 5 】

[0016] ユーザ104がアプリケーション106-1を起動すると、ユーザは、明示的に（例えば、資格情報を入力し、アカウントを選択することによって等）、又は暗示的に（例えば、閲覧するコンテンツ、アクセスするファイル、対象とするアカウント等に基づいて）、ユーザ自身を識別する必要がある。アプリケーション106-1は、クライアントコンポーネント116に有効なアイデンティティを通知し、クライアントコンポーネント

50

116 はポリシーを実施する。

【0016】

[0017] アプリケーションのユーザインタフェースが、ポリシーを適切に実施するために変更が必要な場合は、クライアントコンポーネント116はアプリケーション106-1に通知する。例えば、アプリケーションが任意の場所にコンテンツを保存するのをサポートする場合には、クライアントコンポーネントはアプリケーションに、ポリシー112がそのように特定するときには、特定のリストに保存先を限定するか、又は特定の場所をブロックする必要があることを通知する。一つの例示的な実施形態においては、2つの態様が考えられる。第1に、新しいポリシーに基づいてユーザインタフェースを変更する（一例として保存を制限する）ことである。第2に、ソフトウェア開発キット（SDK：Software Development Kit）から呼び出されたアプリケーション内でのコールバックである。実施形態はアプリケーションに、有効なユーザが有効なアカウントを変更するために、アプリケーションに迅速な変更が必要であると通知するであろう。アプリケーションが同時に1つの有効なアカウントのみをサポートし、画面上に正しい情報（電子メール、共有ファイル等）を表示するために使用する場合の例を考える。異なるユーザに対応する入力データがある場合には、アプリケーションは又、アプリケーションビューを変更して新しいアカウントに対応する適切な情報を表示する。

10

【0017】

[0018] 上述したように、ポリシー管理システムは、ポリシーを、デバイス上の1つ以上のアプリケーション用に特定のユーザのアイデンティティ又はアカウントを対象として配布できる。

20

【0018】

[0019] ポリシー管理システムは、デバイス上の1つ以上のアプリケーションで特定のユーザのアイデンティティ又はアカウントに対し動作を呼び出す（例えば、データを消去する）機能を含み得る。

【0019】

[0020] いくつかの実施形態では、ポリシー管理システムのクライアントコンポーネント116は、デバイス用にSDKを使用して実装され得る。クライアントコンポーネント116は、ポリシーを受信し実施するための様々な特徴を含み得る。例えば、クライアントコンポーネント116は、ポリシー管理システム114と通信をするための機能を含み、アプリケーション内で1つ以上のアイデンティティ又はアカウントを対象とするポリシーを受信し得る。クライアントコンポーネント116は、さらに、アプリケーション（アプリケーション106-1のような）と通信するための機能を含み、アプリケーション内で1つ以上のアイデンティティ又はアカウントを対象とするポリシーを実施する。クライアントコンポーネント116は、アプリケーション内で1つ以上のアイデンティティ又はアカウントのポリシーの状態を管理システム114のリモートコンポーネントに報告する機能を含み得る。

30

【0020】

[0021] クライアントコンポーネント116は、クライアントコンポーネント116が適切なポリシーを実施できるように、アプリケーション106-1がクライアントコンポーネント116にアプリケーション内の現在の有効なアイデンティティを通知することが可能な機能を含み得る。クライアントコンポーネント116は、クライアントコンポーネント116が適切なポリシーを実施できるように、アプリケーション106-1がクライアントコンポーネント116にデータ（例えばファイル又はデータバッファ）に対応するアイデンティティを通知する機能を含み得る。クライアントコンポーネント116は、クライアントコンポーネント116がアプリケーション106-1に、アプリケーション106-1の特定のユーザインタフェース要素（例えば、「名前をつけて保存」は切り取り/コピー/貼り付け機能等を対象とする）は、ポリシーに基づいて制限されねばならないと通知することを可能にする機能を含み得る。クライアントコンポーネント116は、クライアントコンポーネント116がアプリケーション106-1に、現在の有効なアカウン

40

50

ト及び表示された任意の関連するデータは新しいアカウントに変更されなければならないと通知することを可能にする機能を含み得る。これは、例えば、定義されたスキーマ、プログラムの方法又はその他の適切な手段を使用して通信され得る。

【0021】

[0022] したがって、一例示的な実施形態は、以下の4つのコンポーネントを含み得る。

【0022】

[0023] (1) 管理アプリケーション(アプリケーション106-1等) - 図示された実施例では、これは、ポリシー管理システム(ポリシー管理システム114等)によって管理され、1つ以上のアイデンティティのためにポリシー(ポリシー112等)を受信するアプリケーションである。

10

【0023】

[0024] (2) ポリシー管理システムのクライアント/アプリケーションコンポーネント(クライアントコンポーネント116等) - 図示された実施例では、これはサービスとアプリケーションとの間の通信を促進して自動的にポリシーを実施するSDKである。一般的に、このSDKは、アプリケーションによって直接実装され得る。いくつかの実施形態では、このSDKは、ワシントン州レッドモントのマイクロソフト社から入手可能なIntune又はConfiguration Managerの特徴を使用して提供され得る。別の実施例においては、サービスはSDKの概念に取って代わる。つまり、アプリケーションは定義されたプロトコルを介してサービスと通信することを意味する。

【0024】

20

[0025] (3) ポリシー管理システム(ポリシー管理サービス114等) - 図示された実施例では、このポリシー管理システムはITの専門家がポリシーを作り、対象とし、管理アプリケーション内にアイデンティティ又はアカウントを配布するインタフェースである。いくつかの実施形態では、このポリシー管理システムは、ワシントン州レッドモントのマイクロソフト社から入手可能なIntune又はConfiguration Managerを使用して実装され得る。

【0025】

[0026] (4) 通信スキーマ - 図示された実施例では、この通信スキーマは、アプリケーションがポリシーと有効なアイデンティティに基づいて実施しなければならないユーザインタフェースの制限を記載した、バージョン化したXMLスキーマ(又はその他のスキーマ)である。

30

【0026】

[0027] ここで以下の議論は、行われ得るいくつかの方法及び行われ得る方法の動作を示す。方法の動作は、特定の順序で起こるように、ある順序で記載され、又はフローチャートに示され得るが、特に記載しない限り特定の順序は必要とされず、又は動作が行われる前に完了された別の動作に依存するため必要とされない。

【0027】

[0028] ここで図2を参照すると、方法200が示されている。方法200は、コンピューティング環境において実行され得る。本方法200は、管理アカウントに関連するアプリケーションの挙動を制御するための動作を含む。アプリケーションの挙動は、例えば、データ使用に対して制御され得る。特に、あるアカウントでは、あるデータ利用の挙動が、下記により詳細に示されるように、制限され得る。

40

【0028】

[0029] この方法200は、アプリケーションの状態を識別することを含み、アプリケーションに対し有効な0以上の管理ユーザアカウントを含む、1つ以上のユーザアカウントのセットを識別することを含む(動作202)。例えば、図1に示されているように、アプリケーション106-1は、複数のユーザアカウント108と関連している。これは組織のリソースにアクセスするのに使用されるアカウントのような、いくつかの管理アカウントを含み得る。例えば、アプリケーション106-1は電子メールのアプリケーションであり得る。アカウントのうち1つは、ユーザが契約者である場合、雇用者又はユーザの

50

顧客（又はユーザの雇用者）に企業の電子メールにアクセスするユーザ用のユーザアカウントであり得る。このアカウントは、企業はどのように企業データがアプリケーション 106 - 1 によって使用されるかを制御することを望み、又は企業がデバイス 102 もしくはアプリケーション 106 - 1 が特定の予防（パスワード、データ暗号化又はその他の予防）を実装していることを確実にすることを望み得るという点において管理アカウントであり得る。アカウント 108 のその他のアカウントは、個人アカウント又は管理されないその他のアカウントであり得る。したがって、実施形態はどのアカウントが有効かを識別することを欲し得る。一実施例では、どのアカウントが有効かの判断は、対象とするアカウントを決定することによって行われ得る。例えば、ユーザは、フォルダ、ビュー又は特定のユーザアカウントのデータに焦点を当てるその他のインタフェース要素を選択することが可能であり得る。これは、例えば、データを閲覧、編集可能にし、又はその他の何らかの方法でその他のアカウント用のアプリケーションが使用するか、又は使用可能なその他のデータと本データを区別することを含み得る。あるいは、ユーザは手動でアカウントをアカウント選択ダイアログボックスから選択可能であり得る。アカウントを識別するその他の方法は、追加的に又は代替的に使用され得る。

【0029】

[0030] 本方法 200 はさらに、アプリケーションの状態に関するポリシーを調べることを含む（動作 204）。ポリシーは、管理ユーザアカウント用に定義された 1 つ以上の異なるポリシーを含む。それぞれの異なるポリシーは、1 つ以上の管理ユーザアカウントに対してアプリケーション構成の制御を定義する。したがって、例えば、図 1 では、ポリシー 112 を示している。これらのポリシーは、データがどのように使用されることができるか及び/又は様々なユーザアカウントに対してデータ使用にどのような制限が加えられるべきかを定義し得る。したがって、例えば、アプリケーション構成の制御は、データ使用に対する制御を含み得る。例えば、ポリシーは、切り取り/コピー/貼り付け機能が特定のユーザアカウントに対して無効となるべきであると指定し得る。追加的に又は代替的に、ポリシーはデータがバックアップされることができないように指定し得る。アプリケーション構成の制御は、追加的に又は代替的に、データ共有に関する制御を含み得る。例えば、アプリケーションは、アプリケーションの外部データをその他のアプリケーションと共有可能にすべきではないとポリシーにより指定し得る。アプリケーション構成の制御は、追加的に又は代替的に、暗号化に関する制御を含み得る。例えば、ポリシーは、特定のユーザアカウントのデータは暗号化されるべきであると指定し得る。アプリケーション構成の制御は、追加的に又は代替的にアカウントの起動時間のチェックに関する制御を含み得る（アカウントがアプリケーションの起動又はアカウントの変更のためアプリケーション内で有効になるときを意味する）。例えば、ポリシーは、特定のユーザアカウントに対してピン又はパスワードを入力する必要があるか、又はデバイスが特定のポリシー又はヒース制約を遵守する必要があることを示し得る。アプリケーション構成の制御は、追加的に又は代替的に、動作環境に関する制御を含み得る。例えば、ポリシーは、あるアプリケーションが特定のユーザアカウントを有する 1 つ以上のアプリケーションを使用する際には、デバイス上で動作すべきではないように指定し得る。すなわち、あるアプリケーションは同時に動作すべきではない。データアクセスの別の変形においては、特定の URL へのアクセスは、管理されたブラウザ上の特有のアカウントのホワイトリスト/ブラックリストに基づいて許可されるか、ブロックされる可能性がある。

【0030】

[0031] アプリケーション構成の制御は、管理権限によって定義されたグラフィカルユーザインタフェースの性能に関する制御を含み得る。例えば、制御は、ユーザアカウントがアプリケーションに使用されているときに、特定のブランド化性能が有効になるように指定し得る。ある色のパレット、テキスト、画像、ロゴ又はその他のグラフィカルユーザインタフェースの性能が指定され得る。

【0031】

[0032] 方法 200 はさらに、ポリシー及びアプリケーションの状態に基づいて、ポリシ

10

20

30

40

50

ーに対して有効なユーザアカウントを含む、ポリシーに対するデータのアプリケーションの使用を制御することを含む（動作206）。例えば、クライアントコンポーネントは、データ使用、データの共有、暗号化、起動時間のチェック、動作環境等の特定された制御を実施し得る。いくつかの実施形態では、データのアプリケーションの使用を制御することは、アプリケーションのユーザインタフェースを変更することを含み得る。例えば、アプリケーションは、あるユーザアカウントがアプリケーションで有効である場合に、ユーザインタフェースを変更するように指示され、「名前をつけて保存」又は切り取り/コピー/貼り付け機能を無効にし得る。

【0032】

[0033] 方法200は、データのアプリケーションの使用を制御することは、データの消去、データの更新、有効なアカウントの変更等を含み得る場合に実行され得る。

10

【0033】

[0034] 方法200はさらに、アプリケーションに有効な1つ以上のユーザアカウントのセットを変更することを含む、変更されたアプリケーションの状態を識別することを含む（動作208）。例えば、異なるユーザアカウントのデータは、アプリケーションを対象としており、又は異なるアカウントがユーザによって選択され得る。

【0034】

[0035] 方法200はさらに、ポリシー及び変更されたアプリケーションの状態に基づいて、アプリケーション構成の制御を変更することを含む（動作210）。例えば、対象になる個人のユーザアカウント（又は制約が少ない組織アカウント）のため、データのアプリケーションの使用を制御すると、アプリケーションがデータの追加機能を行うのを可能にするように緩和され得る。

20

【0035】

[0036] 方法200は、アプリケーションの状態がグローバルなアプリケーションの状態である場合に実行され得る。これは又、キャッシュの状態をも含み得る。あるいは、方法200は、アプリケーションの状態がスレッドの状態である場合に行われ得る。あるいは、方法200は、アプリケーションの状態がプロセス状態である場合に行われ得る。3つの状態は、コードがアプリケーション内で実行できる異なるコンテキストと関連している。これらはアプリケーションが0の、1つの又は多くのプロセスを有し、プロセスが1つ又は多くのスレッドを有することができるように階層になっている。

30

1. グローバルアプリケーションの状態は、アプリケーション全体に適用される状態である。これは、ユーザがアプリケーションを使用し、特定のスレッド又はプロセス状態がない場合には、実施形態は、アプリケーション内の有効なアカウントにグローバル状態を使用することを意味する。例えば、例示的なアプリケーションが動作していなく、単にコンピュータにインストールされている場合には、関連するいくつかの状態がある（この状態は「有効ユーザなし」又は「権限なし」であり得る）。

2. プロセス状態は、アプリケーションの動作中インスタンス内の適用可能な状態である。これは、ユーザがアプリケーションを使用し、特定のスレッド状態がない場合には、実施形態は、有効なアカウントのプロセス状態を使用することを意味する。以前の実施例を続けるために、インストールされたアプリケーションを起動した場合、ここで、ユーザアカウントで動作し、これはいくつかの状態（例えば、その他の誰もできない編集が可能ないくつかの文書があり得る）が付随する。

40

3. スレッド状態は、アプリケーションにおいて動作中のプロセス内で適用可能な状態である。これは、ユーザがアプリケーションを使用している場合、一般に、プロセス状態を使用するが、異なる状態でスレッドを動作する結果になり得ることを意味する。例えば、同僚がインストールされたアプリケーションを実行し、非常に大きな文書のアップロードを開始し、文書を閉じ、次に、アプリケーションの動作を継続すると、依然としてバックグラウンドで同僚の大きな文書のアップロードを行うスレッドが存在し得る。一方、アプリケーションでユーザの直接的な使用をサポートする別のスレッドがあり得る。

【0036】

50

[0037] 方法200は、1つ以上のユーザアカウントのセットの識別がアプリケーションによって行われ、管理システムのクライアントコンポーネントに伝達される場合に実行され得る。あるいは、方法200は、1つ以上のユーザアカウントのセットの識別がクライアント管理エンティティによって行われる場合に実行され得る。例えば、これはSDK、管理エージェント、プラットフォーム等によって行われ得る。

【0037】

[0038] 方法200は、1つ以上のアカウントのセットの識別がデータセットの特徴を取得することによって行われる場合に実行され得る。例えば、実施形態は、アプリケーションにアクセスしている間、どのユーザアカウントが使用されるかを識別するためにアプリケーションによって操作されるファイル又はファイルのセグメント、メモリセグメント等を調査し得る。これはアカウント関係を識別するアプリケーションによって行われ得る。あるいは、これは、データセットに対応するアカウントを決定するクライアント管理エンティティ(クライアントコンポーネント116等)によって行われ得る。

10

【0038】

[0039] 方法200の実施形態はさらに、アプリケーション及びポリシーのアイデンティティ遵守を報告することを含み得る。例えば、このような遵守は管理システム114に報告され得る。これは、データをデバイス102から消去させる管理システム114を促進することができ、監査のためにIT管理者又はデバイス102上で行われるその他の管理機能に通知する。

【0039】

20

[0040] さらに、本方法は、1つ以上のプロセッサ及びコンピュータメモリのようなコンピュータ可読媒体を含むコンピュータシステムによって実行され得る。特に、コンピュータメモリは、1つ以上のプロセッサによって実行されると、実施形態に引用される動作のような、様々な機能が行われるコンピュータで実行可能な命令を記憶し得る。

【0040】

[0041] 本発明の実施形態は、下記により詳細に記載されるようなコンピュータハードウェアを含む専用又は汎用コンピュータを備えるか利用し得る。本発明の範囲内の実施形態は又、コンピュータで実行可能な命令及び/又はデータ構造を保持又は記憶するための物理的及びその他のコンピュータ可読媒体を含む。このようなコンピュータ可読媒体は、汎用もしくは専用コンピュータシステムによってアクセス可能な任意の入手可能な媒体であり得る。コンピュータで実行可能な命令を記憶するコンピュータ可読媒体は、物理的記憶媒体である。コンピュータで実行可能な命令を保持するコンピュータ可読媒体は、伝送媒体である。したがって、実施例として、限定するものではないが、本発明の実施形態は、物理的コンピュータ可読記憶媒体と、伝送コンピュータ可読媒体の、少なくとも2つの明らかに異なる種類のコンピュータ可読媒体を含むことができる。

30

【0041】

[0042] 物理的コンピュータ可読記憶媒体は、RAM、ROM、EEPROM、CD-ROM又はその他の光ディスクストレージ(CD、DVD等)、磁気ディスクストレージ又はその他の磁気ストレージデバイス、ソリッドステートストレージデバイス等を含み、コンピュータで実行可能な命令又はデータ構造の形態で所望のプログラムコード手段を記憶するために使用されることができ、汎用又は専用コンピュータによってアクセスされることができ。

40

【0042】

[0043] 「ネットワーク」は、コンピュータシステム及び/又はモジュール及び/又はその他の電子デバイス間の電子データの移送を可能にする、1つ以上のデータリンクとして定義されている。情報が、ネットワーク上もしくは別の通信接続(ハードワイヤード、ワイヤレス又はハードワイヤードとワイヤレスの組み合わせの何れか)でコンピュータに転送又は提供されると、コンピュータは伝送媒体として、接続を適切に閲覧する。伝送媒体はネットワーク及び/又はデータリンクを含むことができる。コンピュータで実行可能な命令又はデータ構造の形態で所望のプログラムコード手段を保持するために使用されるこ

50

とができ、汎用又は専用コンピュータによってアクセスされることができる。上記の組み合わせも、コンピュータ可読媒体の範囲内に含まれる。

【0043】

[0044] さらに、様々なコンピュータシステムのコンポーネントに到達すると、コンピュータで実行可能な命令又はデータ構造の形態のプログラムコード手段は、伝送コンピュータ可読媒体から物理的コンピュータ可読ストレージ媒体（又は逆も同様）に自動的に転送されることができる。例えば、ネットワーク又はデータリンクを介して受信されたコンピュータで実行可能な命令又はデータ構造は、ネットワークインターフェイスモジュール（例えば、「NIC」）内のRAMにバッファされることができ、そして最終的に、コンピュータシステムRAM及び/又はコンピュータシステムで揮発性の低いコンピュータ可読の物理的ストレージ媒体に転送される。したがって、コンピュータ可読の物理的ストレージ媒体は、伝送媒体も（又は主に）利用するコンピュータシステムコンポーネントに含まれることができる。

10

【0044】

[0045] コンピュータで実行可能な命令には、例えば、汎用コンピュータ、専用コンピュータ又は専用の処理デバイスに一定の機能又は一連の機能を行わせる命令及びデータが含まれる。コンピュータで実行可能な命令は、例えば、アセンブリ言語又はさらにはソースコードのようなバイナリ形式の命令、中間形式の命令であり得る。主題は構造上の特徴及び/又は方法論的動作に特有の言語で記載されているが、添付の請求項に定義された主題は、必ずしも記載された特徴又は前述の動作に限定されないことを理解されたい。むしろ、記載された特徴及び動作は、請求項を実装する例示的な形態として開示されている。

20

【0045】

[0046] 当業者は、本発明は、パーソナルコンピュータ、デスクトップコンピュータ、ラップトップコンピュータ、メッセージプロセッサ、携帯用デバイス、マルチプロセッサシステム、マイクロプロセッサベース又はプログラム可能な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、携帯電話、PDA、ポケットベル、ルータ、スイッチ等を含む、多くの種類のコンピュータシステム構成を備えるネットワークコンピューティング環境において実行され得ることを理解するであろう。本発明は又、ネットワークを介して（ハードワイヤードデータリンク、ワイヤレスデータリンク又はハードワイヤードとワイヤレスデータリンクとの組み合わせの何れかによって）リンクされたローカル及びリモートコンピュータシステムの両方がタスクを行う分散システム環境において実行され得る。分散システム環境においては、プログラムモジュールはローカル及びリモートの両方のメモリストレージデバイスに配置され得る。

30

【0046】

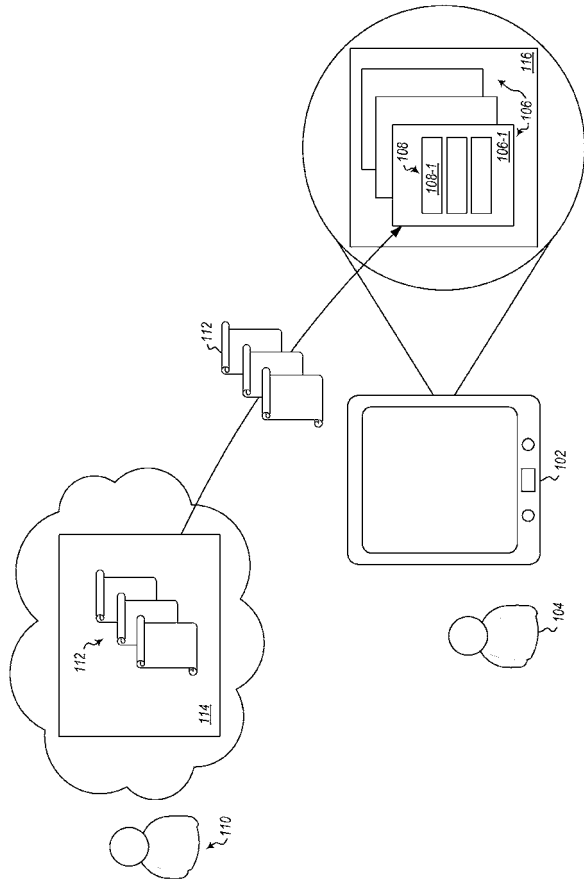
[0047] あるいは又はさらに、本明細書に記載された機能は、少なくとも部分的に1つ以上のハードウェアロジックコンポーネントによって行うことができる。例えば、これらに限定されないが、使用可能なハードウェアロジックコンポーネントの例示的な種類は、フィールドプログラマブルゲートアレイ（FPGA）、特定用途向け集積回路（ASIC）、プログラム特定標準製品（ASSP）、システムオンチップ型システム（SOC）、コンプレックスプログラマブルロジックデバイス（CPLD）等を含む。

40

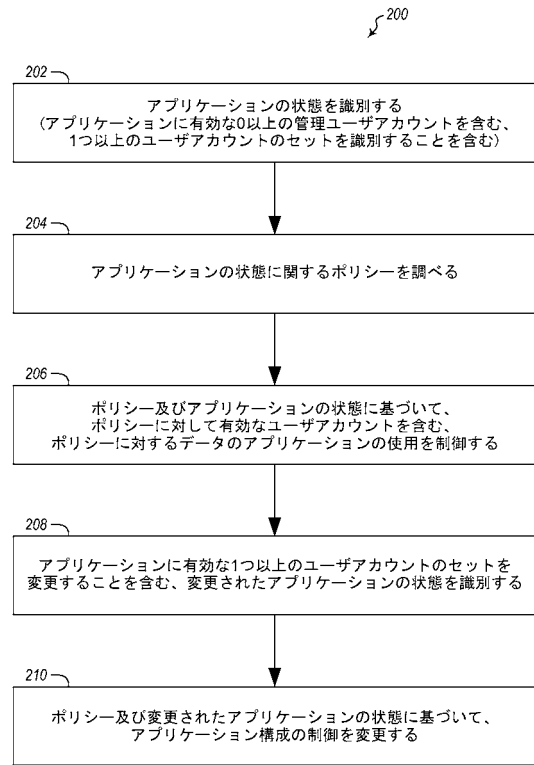
【0047】

[0048] 本発明は、その精神又は特徴から逸脱することなくその他の特定の形態で具現化され得る。記載された実施形態は、あらゆる点において、単に例示的であり、限定されないものと認定される。したがって、本発明の範囲は、上述の説明よりもむしろ、添付の特許請求の範囲によって示されている。特許請求の範囲の意味及び特許請求の範囲に相当するすべての変更は、その範囲内であると理解されたい。

【 図 1 】



【 図 2 】



【 国際調査報告 】

INTERNATIONAL SEARCH REPORT

International application No PCT/US2015/050543

A. CLASSIFICATION OF SUBJECT MATTER INV. G06Q10/10 ADD.		
According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) G06Q		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) EPO-Internal, INSPEC, WPI Data		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2013/298185 A1 (KONERU RAJ KUMAR [US] ET AL) 7 November 2013 (2013-11-07) abstract paragraph [0006] - paragraph [0020] paragraph [0026] - paragraph [0071] -----	1-10
X	US 2013/290709 A1 (MUPPIDI SRIDHAR R [US] ET AL) 31 October 2013 (2013-10-31) abstract paragraph [0008] - paragraph [0012] paragraph [0041] - paragraph [0059] -----	1-10
<input type="checkbox"/> Further documents are listed in the continuation of Box C. <input checked="" type="checkbox"/> See patent family annex.		
* Special categories of cited documents : "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier application or patent but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family		
Date of the actual completion of the international search		Date of mailing of the international search report
4 November 2015		12/11/2015
Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016		Authorized officer Lozza, Mario

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2015/050543

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2013298185	A1	07-11-2013	NONE

US 2013290709	A1	31-10-2013	US 2013290709 A1
			US 2013291055 A1
			WO 2013161212 A1

フロントページの続き

(81)指定国 AP(BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), EA(AM, AZ, BY, KG, KZ, RU, TJ, TM), EP(AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OA(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG), AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US

(74)代理人 100108213
弁理士 阿部 豊隆

(74)代理人 100140648
弁理士 佐藤 宏樹

(72)発明者 エマソン, ダニエル フロイド
アメリカ合衆国, ワシントン州 98052-6399, レッドモンド, ワン マイクロソフト
ウェイ, マイクロソフト テクノロジー ライセンシング, エルエルシー, エーティーティーエヌ
: パテント グループ ドケティング (ビルディング 8/1000)

(72)発明者 ドーフマン, ジェレミー クリストファー
アメリカ合衆国, ワシントン州 98052-6399, レッドモンド, ワン マイクロソフト
ウェイ, マイクロソフト テクノロジー ライセンシング, エルエルシー, エーティーティーエヌ
: パテント グループ ドケティング (ビルディング 8/1000)

(72)発明者 ジェーコブソン, ネイル アダム
アメリカ合衆国, ワシントン州 98052-6399, レッドモンド, ワン マイクロソフト
ウェイ, マイクロソフト テクノロジー ライセンシング, エルエルシー, エーティーティーエヌ
: パテント グループ ドケティング (ビルディング 8/1000)

Fターム(参考) 5B376 AA10 AA25 AA35 AA38