(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6397957号
(P6397957)
(45)発行日　平成30年9月26日(2018.9.26)　(24)登録日　平成30年9月7日(2018.9.7)

(51)Int.Cl.　F I
G06F 21/62 (2013.01)　G06F 21/62 318
G06F 21/12 (2013.01)　G06F 21/12 380

請求項の数 23　(全 83 頁)

(21)出願番号　特願2017-81342(P2017-81342)
(22)出願日　平成29年4月17日(2017.4.17)
(62)分割の表示　特願2016-505457(P2016-505457)の分割
原出願日　平成25年10月10日(2013.10.10)
(65)公開番号　特開2017-168111(P2017-168111A)
(43)公開日　平成29年9月21日(2017.9.21)
審査請求日　平成29年5月16日(2017.5.16)
(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　61/866,229
(32)優先日　平成25年8月15日(2013.8.15)
(33)優先権主張国　米国(US)

(73)特許権者　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　クレーシー，ワヒード
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

最終頁に続く

(54)【発明の名称】管理されたブラウザの提供

(57)【特許請求の範囲】
【請求項１】
コンピューティングデバイスにより、管理されたブラウザをロードするステップであって、前記管理されたブラウザは、前記管理されたブラウザに１つまたはそれ以上のポリシーが適用される少なくとも１つの管理モードを提供するように設定され、前記１つまたはそれ以上のポリシーは、前記管理されたブラウザの少なくとも１つの機能を制限するよう設定されている、前記ステップと、
前記コンピューティングデバイスにより、前記管理されたブラウザを介して１つまたはそれ以上の企業リソースのアクセスへの要求を受信するステップと、
前記コンピューティングデバイスにより、前記要求に基づいて前記１つまたはそれ以上の企業リソースから企業データを取得するステップと、
前記コンピューティングデバイスにより、前記取得された企業データをセキュリティ保護されたドキュメントコンテナ内に記憶するステップとを含み、
前記管理されたブラウザは、前記管理されたブラウザが少なくとも１つのデバイス管理者によって管理されることがなく、前記管理されたブラウザにいかなるポリシーも適用されない、非管理モードを提供するようにさらに設定されている、方法。
【請求項２】
前記管理されたブラウザが前記非管理モードで動作しているときに、前記取得された企業データへのアクセスを選択的にブロック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】
前記管理されたブラウザが前記少なくとも１つの管理モードで動作しているときにのみ、前記コンピューティングデバイスにより、前記管理されたブラウザを介して前記セキュリティ保護されたドキュメントコンテナへのアクセスを提供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４】
前記コンピューティングデバイスにより、前記セキュリティ保護されたドキュメントコンテナからデータを選択的にワイプ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５】
前記セキュリティ保護されたドキュメントコンテナからデータを選択的にワイプするステップは、前記要求に基づいて前記１つまたはそれ以上の企業リソースから取得された前記企業データを削除することを含む、請求項４に記載の方法。
【請求項６】
前記データは、前記管理されたブラウザが閉じられたときに前記セキュリティ保護されたドキュメントコンテナから選択的にワイプされる、請求項４に記載の方法。
【請求項７】
前記データは、前記１つまたはそれ以上のポリシーに基づいて前記セキュリティ保護されたドキュメントコンテナから選択的にワイプされ、前記セキュリティ保護されたドキュメントコンテナから前記データをワイプするステップは、前記セキュリティ保護されたドキュメントコンテナから所定の期間に記憶されたデータを消去し、他のデータを残すことを含む、請求項４に記載の方法。
【請求項８】
前記１つまたはそれ以上のポリシーのうち少なくとも１つのポリシーは、前記コンピューティングデバイスに関連したデバイス状態情報に基づいて、前記管理されたブラウザを前記少なくとも１つの管理モードから前記非管理モードに切り換えるように設定されている１または複数のルールを含む、請求項１から請求項７のいずれかに記載の方法。
【請求項９】
前記管理されたブラウザは、更新されたデバイス状態情報に基づいて、前記非管理モードから前記少なくとも１つの管理モードに遷移して戻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】
前記コンピューティングデバイスに関連したデバイス状態情報は、（１）前記コンピューティングデバイス上に存在する１つ以上アプリケーションを特定する情報、（２）前記コンピューティングデバイスの現在位置を特定する情報、（３）前記コンピューティングデバイスが接続される少なくとも１つのネットワーク接続を特定する情報、のうち少なくとも１つを含む、請求項８または請求項９に記載の方法。
【請求項１１】
コンピューティングデバイスであって、
少なくとも１つのプロセッサと、
前記少なくとも１つのプロセッサにより実行されたときに、前記コンピューティングデバイスに、
管理されたブラウザをロードするステップであって、前記管理されたブラウザは、前記管理されたブラウザに１つまたはそれ以上のポリシーが適用される少なくとも１つの管理モードを提供するよう設定され、前記１つまたはそれ以上のポリシーは、前記管理されたブラウザの少なくとも１つの機能を制限するよう設定されている、前記ステップと、
前記管理されたブラウザを介して１つまたはそれ以上の企業リソースのアクセスへの要求を受信するステップと、
前記要求に基づいて前記１つまたはそれ以上の企業リソースから企業データを取得するステップと、

前記取得された企業データをセキュリティ保護されたドキュメントコンテナ内に記憶するステップとを行なわせる、
コンピュータ読取可能命令を記憶するメモリとを備え、前記管理されたブラウザは、前記管理されたブラウザが少なくとも１つのデバイス管理者によって管理されることがなく、前記管理されたブラウザにいかなるポリシーも適用されない非管理モードを提供するようにさらに設定されている、コンピューティングデバイス。
【請求項１２】
前記管理されたブラウザは、少なくとも１つの企業リソースから取得されたデータのセキュリティ保護されたブラウジングおよびキャッシングを提供するよう設定され、前記セキュリティ保護されたブラウジングおよびキャッシングを提供するステップは、１つまたはそれ以上の符号化されたローカルなキャッシュに、前記少なくとも１つの企業リソースから得られるデータをキャッシングすることを含む、請求項１１に記載のコンピューティングデバイス。
【請求項１３】
前記メモリは、前記少なくとも１つのプロセッサにより実行されたときに、前記コンピューティングデバイスにさらに、
前記管理されたブラウザが前記少なくとも１つの管理モードで動作しているときにのみ、前記セキュリティ保護されたドキュメントコンテナに記憶され、前記管理されたブラウザを介して取得された企業データへのアクセスを提供することを行なわせるさらなるコンピュータ読取可能命令を記憶し、
前記取得された企業データへのアクセスを提供するステップは、前記１つまたはそれ以上のポリシーのうち少なくとも１つのポリシーをシングルサインオン（ＳＳＯ）認証に基づいて適用するステップを含み、前記少なくとも１つのポリシーは、前記取得された企業データへのアクセスを制限するように設定されている、請求項１１に記載のコンピューティングデバイス。
【請求項１４】
前記メモリは、前記少なくとも１つのプロセッサにより実行されたときに、前記コンピューティングデバイスにさらに、
前記セキュリティ保護されたドキュメントコンテナからデータを選択的にワイプするステップを行なわせる、さらなるコンピュータ読取可能命令を記憶する請求項１１に記載のコンピューティングデバイス。
【請求項１５】
前記セキュリティ保護されたドキュメントコンテナからデータを選択的にワイプするステップは、前記要求に基づいて前記１つまたはそれ以上の企業リソースから取得された前記企業データを削除することを含む、請求項１４に記載のコンピューティングデバイス。
【請求項１６】
前記データは、前記管理されたブラウザが閉じられたときに前記セキュリティ保護されたドキュメントコンテナから選択的にワイプされる、請求項１４に記載のコンピューティングデバイス。
【請求項１７】
前記データは、前記１つまたはそれ以上のポリシーに基づいて前記セキュリティ保護されたドキュメントコンテナから選択的にワイプされ、前記セキュリティ保護されたドキュメントコンテナから前記データを選択的にワイプするステップは、前記セキュリティ保護されたドキュメントコンテナから所定のセッションに記憶されたデータを消去し、他のデータを残すことを含む、請求項１４に記載のコンピューティングデバイス。
【請求項１８】
実行されたときに、コンピューティングデバイスに、
管理されたブラウザをロードするステップであって、前記管理されたブラウザは、前記管理されたブラウザに１つまたはそれ以上のポリシーが適用される少なくとも１つの管理モードを提供するよう設定され、前記１つまたはそれ以上のポリシーは、前記管理された

ブラウザの少なくとも１つの機能を制限するよう設定されている、前記ステップと、
前記管理されたブラウザを介して１つまたはそれ以上の企業リソースのアクセスへの要求を受信するステップと、
前記要求に基づいて前記１つまたはそれ以上の企業リソースから企業データを取得するステップと、
前記取得された企業データをセキュリティ保護されたドキュメントコンテナ内に記憶するステップとを行なわせる、コンピュータ読取可能命令を記憶し、
前記管理されたブラウザは、前記管理されたブラウザが少なくとも１つのデバイス管理者によって管理されることがなく、前記管理されたブラウザにいかなるポリシーも適用されない、非管理モードを提供するようにさらに設定されている、１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。

【請求項１９】
前記管理されたブラウザは、少なくとも１つの企業リソースから取得されたデータのセキュリティ保護ブラウジングおよびキャッシングを提供するよう設定され、前記セキュリティ保護されたブラウジングおよびキャッシングを提供するステップは、１つまたはそれ以上の符号化されたローカルなキャッシュに、前記少なくとも１つの企業リソースから得られるデータをキャッシングすることを含む、請求項１８に記載の１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。

【請求項２０】
実行されたときに、前記コンピューティングデバイスにさらに、
前記管理されたブラウザが前記少なくとも１つの管理モードで動作しているときにのみ、前記管理されたブラウザを介して前記セキュリティ保護されたドキュメントコンテナへのアクセスを提供するステップを行なわせる、記憶されたさらなる命令を有する、請求項１８に記載の１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。

【請求項２１】
実行されたときに、前記コンピューティングデバイスにさらに、
前記セキュリティ保護されたドキュメントコンテナからデータを選択的にワイプすることを行なわせる、記憶されたさらなる命令を有する、請求項１８に記載の１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。

【請求項２２】
前記データは、前記管理されたブラウザが前記管理モードで動作しているときに前記管理されたブラウザに適用される少なくとも１つのポリシーに基づいて、前記セキュリティ保護されたドキュメントコンテナから選択的にワイプされる、請求項２１に記載の１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。

【請求項２３】
前記データは、前記管理されたブラウザが閉じられたときに前記セキュリティ保護されたドキュメントコンテナから選択的にワイプされる、請求項２１に記載の１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１つ以上の態様は、一般に、管理されたブラウザ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】

下記に詳述される本発明の１つ以上の実施形態において、１つ以上の前述した、および／または他の利点を提供するために、複数の異なる方法で、モバイルデバイス管理機能が展開され、実装され、および／または、使用される。

【０００５】

本発明のある実施形態においては、コンピューティングデバイスが、管理されたブラウザをロードする。引き続いて、コンピューティングデバイスが、管理されたブラウザを介して１つ以上の企業リソースへのアクセスの要求を受信する。そして、コンピューティングデバイスは、ブラウザから１つ以上の企業リソースへの管理された少なくとも１つのアプリケーショントンネルを生成する。コンピューティングデバイスはそして、少なくとも１つのアプリケーショントンネルを介して１つ以上の企業リソースから企業データを取得する。

【０００６】

ある実施形態においては、コンピューティングデバイスが、管理されたブラウザをロードしてもよい。引き続いて、コンピューティングデバイスは、デバイスクラウドを開始するために少なくとも１つの他のコンピューティングデバイスへの接続を確立してもよい。そして、コンピューティングデバイスは、管理されたブラウザのセッションをデバイスクラウドにわたって拡張してもよい。

【０００７】

ある実施形態においては、コンピューティングデバイスが、管理されたブラウザをロードしてもよい。引き続いて、コンピューティングデバイスは、デバイス状態情報（state information）を取得してもよい。そして、コンピューティングデバイスは、デバイス状態情報に基づいて、管理されたブラウザの１つ以上の動作モードを選択的な無効化するべきかどうかを判定してもよい。管理されたブラウザの少なくとも１つの動作モードの選択的無効化の判定に応じて、コンピューティングデバイスは、少なくとも１つの動作モードを無効化してもよい。

【０００８】

ある実施形態においては、コンピューティングデバイスが、管理されたブラウザをロードしてもよい。引き続いて、コンピューティングデバイスは、１つ以上のポリシーを受信してもよい。そして、コンピューティングデバイスは、管理されたブラウザに１つ以上のポリシーを適用してもよい。

【０００９】

ある実施形態においては、コンピューティングデバイスが、管理されたブラウザをロードしてもよい。引き続いて、コンピューティングデバイスは、管理されたブラウザを介して１つ以上の企業リソースのアクセスへの要求を受信してもよい。そして、コンピューティングデバイスは、要求に基づいて１つ以上の企業リソースから企業データを取得してもよい。コンピューティングデバイスはそして、取得された企業データをセキュリティ保護ドキュメントコンテナ内に記憶してもよい。

【００１０】

ある実施形態においては、コンピューティングデバイスが、管理されたブラウザをロードしてもよい。引き続いて、コンピューティングデバイスは、少なくとも１つのユーザアカウントに関するシングルサインオン（ＳＳＯ）クレデンシャル（credential）を受信してもよい。そして、コンピューティングデバイスは、ＳＳＯクレデンシャルに基づいて１つ以上の企業リソースから企業データを取得してもよい。コンピューティングデバイスはそして、取得された企業データへのアクセスを管理されたブラウザを介して提供してもよい。

【００１１】

ある実施形態においては、コンピューティングデバイスが、管理されたブラウザをロードしてもよい。引き続いて、コンピューティングデバイスは、管理されたブラウザを介してアプリケーションストアへのアクセスの要求を受信してよい。そして、コンピューティングデバイスは、要求に基づいてアプリケーションストアから企業データを取得してもよい。

【００１２】

他の実施形態においては、コンピューティングデバイスが、管理されたブラウザをロードしてもよい。引き続いて、コンピューティングデバイスは、管理されたブラウザを介して１つ以上の企業リソースのアクセスへの要求を受信してもよい。そして、コンピューティングデバイスは、要求に基づいて１つ以上の企業リソースから企業データを取得してもよい。コンピューティングデバイスはそして、１つ以上のポリシーに基づいて取得された企業データを制御してもよい。

【００１３】

ある実施形態においては、モバイルコンピューティングデバイスが、アプリケーションストアから少なくとも１つのモバイルデバイス管理ポリシーを受信してもよい。引き続いて、モバイルコンピューティングデバイスに関する状態情報が、モバイルデバイス管理エージェントを介して監視されてもよい。そして、少なくとも１つのモバイルデバイス管理ポリシーが、監視された状態情報に基づいて強制されてもよい。

【００１４】

ある実施形態においては、モバイルコンピューティングデバイスが、少なくとも１つのユーザアカウントに関するシングルサインオン（ＳＳＯ）クレデンシャル（credential）を受信してもよい。引き続いて、モバイルコンピューティングデバイスに関する状態情報が、モバイルデバイス管理エージェントを介して監視されてもよい。そして、少なくとも１つのモバイルデバイス管理ポリシーが、監視された状態情報およびＳＳＯクレデンシャルに基づいて適用されてもよい。

【００１５】

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。

【００１６】

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】

【００１７】

【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１つ以上の実施形態に従って、管理されたブラウザから１つ以上の企業リソースへのアプリケーショントンネルを生成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１つ以上の実施形態に従って、管理されたブラウザのセッションをデバイスクラウドにわたって拡張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１つ以上の実施形態に従って、管理されたブラウザの動作モードを選択的に無効化する方法を説明するためのフローチャートである。
【図８】本発明の１つ以上の実施形態に従って、管理されたブラウザに１つ以上のモバイルデバイス管理ポリシーを適用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１つ以上の実施形態に従って、管理されたブラウザを介してセキュリティ保護ドキュメントコンテナへのアクセス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１０】本発明の１つ以上の実施形態に従って、ＳＳＯクレデンシャルに基づいて企業データを取得し、管理されたブラウザを介してデータへのアクセス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１１】本発明の１つ以上の実施形態に従って、管理されたブラウザを介してアプリケーションストアへのアクセス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１２】本発明の１つ以上の実施形態に従って、管理されたブラウザで企業データを取得および制御する方法を説明するためのフローチャートである。
【図１３】本発明の１つ以上の実施形態に従って、管理されたブラウザ用の１つ以上のポリシーをアドミニストレーションする方法を説明するためのフローチャートである。
【図１４】本発明の１つ以上の実施形態に従って、管理されたブラウザを介してアプリケーションストアへのアクセスを提供する別の方法を説明するためのフローチャートである。
【図１５】本発明の１つ以上の実施形態に従って、管理されたブラウザ内で管理された実行環境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。
【発明を実施するための形態】
【００１８】
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。
【００１９】
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。
【００２０】
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。
【００２１】
上述のように、管理されたブラウザ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。
【００２２】
〈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）、ヴァーチャル環境、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。

【００２３】

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。

【００２４】

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 alternatively）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。

【００２５】

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。

【００２６】

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。

【００２７】

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。

【００２８】

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、別個のヴァーチャル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。

【００２９】

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。

【００３０】

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。

【００３１】

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。

【００３２】

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。

【００３３】

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。

【００３４】

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、ヴァーチャルまたは物理データベースへと分離されることができる。

【００３５】

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。

【００３６】

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。

【００３７】

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。

【００３８】

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。

【００３９】

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。

【００４０】

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。

【００４１】

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ヴァーチャル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。

【００４２】

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。

【００４３】

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。

【００４４】

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

。
【００４５】
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。
【００４６】
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。
【００４７】
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。
【００４８】
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。
。
【００４９】
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。
【００５０】
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。
【００５１】
１つの実施形態において、クライアントマシン２４０は、ヴァーチャルマシンであって

もよい。ヴァーチャルマシンは任意のヴァーチャルマシンであってもよく、実施形態によっては、ヴァーチャルマシンは、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ヴァーチャルマシンであってもよい。ある態様では、バーチャル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、ヴァーチャルマシンは、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。

【００５２】

実施形態によっては、サーバ２０６または他の遠隔配置されたマシン上で遠隔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、ヴァーチャル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。

【００５３】

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。

【００５４】

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。

【００５５】

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。

【００５６】

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２０

６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。

【００５７】

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。

【００５８】

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。

【００５９】

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にヴァーチャルデスクトップおよび／またはヴァーチャル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。

【００６０】

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。

【００６１】

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、ヴァーチャル（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、遠隔配置された（例えばリモートされた）デバイス上で実行されてもよい。

【００６２】

〈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。

【００６３】
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。

【００６４】
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。

【００６５】
モバイルデバイスのオペレーティングシステムは、管理パーティション３１０および非管理パーティション３１２に分離されてもよい。管理パーティション３１０は、実行中のアプリケーションおよび管理パーティションに記憶されたデータをセキュリティ保護するために、それ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実行中の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、Ｗｉｎｄｏｗｓ（登録商標）Ａｐｐｌｉｃａｔｉｏｎ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ー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、セキュリティ保護アプリケーションランチャー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ー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ー３２０は、セキュリティ保護ネイティブアプリケーションがデバイス上で実行されるときにモバイルデバイス３０２上で実行される、統合されたポリシーを含んでもよい。

【００６６】
セキュリティ保護アプリケーションラッパー３２０は、モバイルデバイス３０２上で実行され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ためにセキュリティ保護ネイティブアプリケーション３１４が要求する、企業でホストされるリソースへとポイントするメタデータを含んでもよい。セキュリティ保護アプリケーションランチャー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ーアプリケーション３１８内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ー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上で、また企業リソース３０４等で、リソースを利用してもよい。セキュリティ保護アプリケーションランチャー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、ユーザ相互作用リソース、処理リソース等を含んでいる。

【００６７】
ユーザ相互作用リソースは、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、映像入力、ジェスチャ入力等を収集して送信するために使用される。処理リソー

スは、ユーザインタフェースを提示する、企業リソース３０４から受信されたデータを処理する、等のために使用される。

【００６８】

セキュリティ保護アプリケーションランチャー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で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、処理リソース等を含んでいる。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をアセンブルする、ユーザインタフェースを修正する、ユーザインタフェースをリフレッシュする、等のために使用される。処理リソースは、情報を生成する、情報を読み出す、情報を更新する、情報を削除する、等のために使用される。例えば、仮想化アプリケーションは、ＧＵＩに関するユーザ相互作用を記録し、それらをサーバアプリケーションに通信してもよく、サーバアプリケーションは、サーバ上で動作するアプリケーションへの入力としてユーザ相互作用データを使用するであろう。この構成において、企業はサーバ側のアプリケーションを、アプリケーションに関するデータ、ファイル等とともに維持することを選択してもよい。

【００６９】

企業は、モバイルデバイスでの展開のためにそれらをセキュリティ保護することにより、本開示の原理に応じていくつかのアプリケーションを「モビライズ」することを選択してもよい一方で、この構成は、特定のアプリケーションのために選択される。例えば、いくつかのアプリケーションがモバイルデバイスでの使用のためにセキュリティ保護されるかもしれず、他のアプリケーションがモバイルデバイスでの展開のためには用意されないまたは適切ではないかもしれないため、企業は、仮想化技術を通じて、用意されないアプリケーションへのモバイルユーザアクセスを提供することを選択する。

【００７０】

別の実施例として、企業は、大規模で複雑なデータセットを伴う大規模で複雑なアプリケーション（例えば、マテリアルリソースプランニングアプリケーション）を有し、モバイルデバイス用にアプリケーションをカスタマイズすることは、非常に困難で、または別様に望ましくないため、企業は、仮想化技術を通じて、アプリケーションへのアクセスを提供することを選択してもよい。

【００７１】

さらに別の実施例として、企業は、たとえセキュリティ保護されたモバイル環境であっても企業があまりにもセンシティブであるとみなすかもしれない高度にセキュリティ保護されたデータ（例えば、人的資源データ、顧客データ、エンジニアリングデータ）を維持するアプリケーションを有し、企業は、仮想化技術を使用して、そ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択する。企業は、サーバ側でより適切に動作するとみなされるアプリケーションへのアクセスを許可するために、モバイルデバイス上で完全にセキュリティ保護および完全に機能的なアプリケーションならびに仮想化アプリケーションの両方を提供することを選択してもよい。

【００７２】

本発明の実施形態において、仮想化アプリケーションは、セキュリティ保護されたストレージ位置の１つで、いくつかのデータ、ファイル等を携帯電話上に記憶する。企業は、例えば電話上に記憶された特定の情報を許可し、一方、他の情報を許可しないように選択する。

【００７３】

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。

【００７４】
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。
【００７５】
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３１０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３１８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３１８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。
【００７６】
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。
【００７７】
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。
【００７８】
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。
【００７９】
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。
【００８０】
モバイルデバイスは、企業において企業リソース３０４、企業サービス３０８に、および公衆インターネット３４８等に接続される。モバイルデバイスは、ヴァーチャルプライベートネットワーク接続を通じて企業リソース３０４および企業サービス３０８に接続す

る。ヴァーチャルプライベートネットワーク接続は、特定のアプリケーション３５０、特定のデバイス、モバイルデバイス上の特定のセキュリティ保護エリア等（例えば、３５２）に特有である。例えば、電話のセキュリティ保護エリアにおける各ラップ済みアプリケーションは、アプリケーション特有のＶＰＮを通じて企業リソースにアクセスしてもよく、これにより、ＶＰＮへのアクセスが、アプリケーションに関する属性に基づいて、おそらくはユーザまたはデバイス属性情報に関連付けられて、許可されるであろう。

【００８１】

ヴァーチャル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トラフィック、ＨＴＴＰトラフィック、ＨＴＴＰＳトラフィック、アプリケーション管理トラフィック等を伝送してもよい。ヴァーチャルプライベートネットワーク接続は、ＳＳＯ認証処理３５４をサポートおよび有効化してもよい。ＳＳＯ処理は、ユーザが認証クレデンシャルの単一セットを提供することを許可してもよく、認証クレデンシャルは、認証サービス３５８により検証される。認証サービス３５８はそして、各個別企業リソース３０４への認証クレデンシャルの提供をユーザに要求することなく、ユーザに複数の企業リソース３０４へのアクセスを許可してもよい。

【００８２】

ヴァーチャル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。

【００８３】

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。

【００８４】

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、Ｗｅｂアプリケーションサーバ、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、Ｌｏｔｕｓ Ｎｏｔｅｓサーバ等を含んでいる。ファイル共有サーバは、ＳＨＡＲＥＦＩＬＥサーバ、他のファイル共有サービス等を含んでいる。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上での実行が意図されるアプリケーションの提供のために構築された任意のアプリケーションサーバ等を含んでいる。

【００８５】

企業リソース３０４は、プレミスベースリソース、クラウドベースリソース等である。企業リソース３０４は、モバイルデバイス３０２によって直接、または、アクセスゲートウェイ３６０を通じてアクセスされる。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によって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、プライベートネットワーク等であってもよい。

【００８６】

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。
【００８７】
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。
【００８８】
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。
【００８９】
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。
【００９０】
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を含んでもよい。アプリケーションストア３７８は、非ラップ化アプリケーション３８０、プリラップ化アプリケーション３８２等を含んでいる。
【００９１】
アプリケーションは、アプリケーションコントローラ３７４からアプリケーションストア３７８に集約されてもよい。アプリケーションストア３７８は、アクセスゲートウェイ３６０を通じて、または公衆インターネット３４８を通じて等、モバイルデバイス３０２によりアクセスされる。アプリケーションストアには、直覚的および使用しやすいユーザインタフェースが提供されてもよい。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、本明細書に以前に記述したようにアプリケーションをラップすることによって、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そして、アプリケーションコントローラ３７４を使用してそれをアプリケーションストア３７８に集約することにより、モバイルデバイス３０２に利用可能にされる。
【００９２】
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。
【００９３】

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。

【００９４】

この場合、左手側は、エンロールドモバイルデバイス４０２（クライアント１０７，２１２，３０２等）をクライアントエージェント４０４とともに表し、これは、右手側上方に示された、Ｅｘｃｈａｎｇｅ、Ｓｈａｒｅｐｏｉｎｔ、ＰＫＩ　Ｒｅｓｏｕｒｃｅ、Ｋｅｒｂｅｒｏｓ　ＲｅｓｏｕｒｃｅおよびＣｅｒｔｉｆｉｃａｔｅ　Ｉｓｓｕａｎｃｅ　Ｓｅｒｖｉｃｅ等の様々な企業リソース４０８およびサービス４０９へのアクセスのために、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コントローラ機能を含む）と相互作用する。

【００９５】

特に示してはいないが、モバイルデバイス４０２は、アプリケーションの選択およびダウンロードのための企業アプリケーションストア（例えば、ＳｔｏｒｅＦｒｏｎｔ）と相互作用してもよい。クライアントエージェント４０４は、例えば、リモートリソースおよび／または仮想化リソースで通信を容易にする、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る。ゲートウェイサーバ４０６は、例えば、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る。

【００９６】

クライアントエージェント４０４は、ＥｎｔｅｒｐｒｉｓｅデータセンタでホストされるＷｉｎｄｏｗｓ（登録商標）アプリ／デスクトップ媒介用のＵＩ（ユーザインタフェース）として作動し、Ｗｉｎｄｏｗｓ（登録商標）アプリ／デスクトップは、ＨＤＸ／ＩＣＡディスプレイリモーティングプロトコルまたは他のリモーティングプロトコルを使用してアクセスされる。クライアントエージェント４０４は、ネイティブｉＯＳ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上の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もサポートする。

【００９７】

例えば、上述の図に示された、管理されたアプリケーション４１０（メール、ブラウザ、ラップ化アプリケーション）は全て、デバイス上でローカルに実行され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およびフロリダ州フォートローダーデールのＣｉｔｒｉｘ　Ｓｙｓｔｅｍｓ社によるＭＤＸ（モバイルエクスペリエンステクノロジ）等のアプリケーション管理フレームワーク（他のアプリケーション管理フレームワークも用いられてもよい）は、企業リソース／サービス４０８への接続性およびＳＳＯ等のポリシー駆動管理能力および特徴を提供するために作動する。

【００９８】

クライアントエージェント４０４は、企業への、通常他のゲートウェイサーバコンポーネントへのＳＳＯを伴うアクセスゲートウェイ（ＡＧ）への、一次的ユーザ認証を取り扱う。クライアントエージェント４０４は、モバイルデバイス４０２上での管理されたアプリケーション４１０の挙動を制御するために、ゲートウェイサーバ４０６からポリシーを取得する。本発明で使用されるように、管理されたアプリケーションは、独立に定義されて通信されたポリシーファイルに基づいて制御され、それに従って動作することが可能なアプリケーションである。

【００９９】

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。

【０１００】

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（ｄａｔａｖａｕｌｔｓ；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。

【０１０１】

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６１４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。

【０１０２】

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。

【０１０３】

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。

【０１０４】

メールおよびブラウザの管理されたアプリケーション４１０は、特別な状態を有してお

り、また任意のラップ化アプリケーションに一般的に利用可能ではないかもしれない能力を使用する。例えば、メールアプリケーションは、完全なＡＤログオンを要求することなく延長された期間、Ｅｘｃｈａｎｇｅへのアクセスを可能とする、特別な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、異なる種類のデータを分離するために複数のプライベートなデータボルトを使用してもよい。

【０１０５】

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。

【０１０６】

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。

【０１０７】

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。

【０１０８】

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。

【０１０９】

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。

【０１１０】

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。

【０１１１】

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。

【０１１２】

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。

【０１１３】

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。

【０１１４】

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それらのアプリケーション４１０用のオフライン認証のために実装されてもよい。例えば、企業は、企業アプリケーションストアが、このようにアクセスされることを欲するかもしれない。この場合、クライアントエージェント４０４は、ユーザにカスタムオフラインパスワードを設定することを要求してもよく、ＡＤパスワードは使用されない。ゲートウェイサーバ４０６は、標準Ｗｉｎｄｏｗｓ（登録商標）　Ｓｅｒｖｅｒパスワード複雑化（complexity）要件による記述等の、最小長、文字クラス構成およびパスワードの期限に関するパスワード基準を制御および適用するためのポリシーを提供してもよいが、これらの要件は修正されてもよい。

【０１１５】

別の特徴は、二次的クレデンシャルとしての特定のアプリケーション４１０用のクライアント側証明書の有効化に関する（アプリケーション管理フレームワークマイクロＶＰＮ特徴を介したＰＫＩ保護ウェブリソースへのアクセス目的で）。例えば、企業電子メール

アプリケーション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認証がサポートされてもよく、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により取得され、キーチェーンで使用されてもよい。各管理されたアプリケーションは、ゲートウェイサーバ４０６内で定義されるラベルにより特定される、１つの関連クライアント証明書を有してもよい。

【０１１６】

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。

【０１１７】

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）。

【０１１８】

ｉＯＳ上のアプリケーション管理フレームワーククライアント証明書サポートは、各使用期間における各管理されたアプリケーション内の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）のインポートに依拠してもよい。アプリケーション管理フレームワーククライアント証明書サポートは、プライベートインメモリキーストレージを伴うＨＴＴＰＳ実装を使用してもよい。クライアント証明書は、ｉＯＳキーチェーン内に決して存在せず、強力に保護された「オンラインのみ」のデータ値内に潜在的に存することを除いて、持続されないであろう。

【０１１９】

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への認証のためのヴァーチャルスマートカードもまた、実装されてもよい。

【０１２０】

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ＡＤ４２２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。

【０１２１】

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。

【０１２２】

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。

【０１２３】

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。

【０１２４】

〈管理されたブラウザの特徴〉

本発明の様々な態様の提供および／または実装において使用される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について、以下、多数の実施形態がより詳細に検討される。特に、前記で紹介されたように、開示のいくつかの態様が一般的に管理されたブラウザの提供に関する。下記においては、いかに管理されたブラウザが１つ以上の実施形態に従って提供されてもよいかを例示する様々な例が検討される。

【０１２５】

図５は、本発明の１つ以上の例示的態様に従って、管理されたブラウザから１つ以上の企業リソースへのアプリケーショントンネルを生成する方法を示すフローチャートである。１つ以上の実施形態では、図５に例示された方法および／または１つ以上のそのステップは、コンピューティングデバイス（例えば、ジェネリックコンピューティングデバイス２０１）によって実行される。他の実施形態においては、図５に例示された方法および／または１つ以上のそのステップは、不揮発性コンピュータで読取可能な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で具体化される。

【０１２６】

図５に示されるように、この方法は、管理されたブラウザがロードされるステップ５０５で始まる。例えば、ステップ５０５において、コンピューティングデバイス（例えば、ラップトップコンピュータ、タブレットコンピュータ、スマートフォンまたは他のタイプのモバイルデバイス等のモバイルコンピューティングデバイス）は、管理されたブラウザをロードする（例えば、管理されたブラウザを開くおよび／または別様にその実行を開始することによって）。

【０１２７】

１つ以上の実施形態において、管理されたブラウザは、１つ以上の企業セキュリティ特徴を提供するよう構成されたウェブブラウザであってもよい（例えば、モバイルデバイス管理特徴、モバイルアプリケーション管理特徴、ポリシー取得および強制特徴等）。さらに／あるいは、管理されたブラウザは、ブラウザ内で実行されるよう構成されるモバイルデバイスアプリケーションでの使用のために様々な企業セキュリティ特徴を拡張してもよい。例えば、企業は、一部または全部のその従業員および／または他のユーザに、企業セキュリティリスク低減のため自身のデバイスの持込（ｂｒｉｎｇ－ｙｏｕｒ－ｏｗｎ－ｄｅｖｉｃｅ：ＢＹＯＤ）スキームにおいて自身の各モバイルデバイス上に管理されたブラウザをインストールして使用することを要求してもよい。さらに、管理されたブラウザは、例えば、モバイルデバイスユーザが企業イントラネットおよび／または他の企業リソースにヴァーチャルプライベートネットワーク（ＶＰＮ）への接続なしでアクセスすることを可能とするために使用されることができる。例えば、管理されたブラウザは、企業イントラネットおよび／または他の企業リソースへのこのようなアクセスを可能とする下記に詳述されるようなもの等の、アプリケーショントンネリング機能を実装しおよび／または提供してもよい。

【０１２８】
１つ以上の実施形態において、管理されたブラウザは、さらに／あるいは、少なくとも１つの企業リソースから取得されたデータのセキュリティ保護ブラウジングおよびキャッシングを提供するよう構成されてもよい。例えば、企業リソースからデータを取得するよう構成されることに加えて（例えば、企業ネットワークに接続された、および／または別様にその一部であるサーバまたはデータベース）、管理されたブラウザは、取得されたデータを安全（secure）にキャッシュするようさらに構成されてもよい（例えば、１つ以上のローカルキャッシュにおいて、１つ以上の暗号化プロトコルを用いて暗号化されてもよい）。さらに／あるいは、管理されたブラウザは、取得されたデータのセキュリティ保護ブラウジングを提供するようさらに構成されてもよい（例えば、１つ以上の認証クレデンシャルの検証に基づいて、１つ以上のモバイルデバイス管理ならびに／あるいはモバイルアプリケーション管理ポリシーの遵守および／または強制に基づいて等、取得されたデータへのアクセスを制御および提供することによって）。

【０１２９】
１つ以上の実施形態において、管理されたブラウザは、管理されたブラウザに１つ以上のポリシーが適用される少なくとも１つの管理モードを提供するよう構成されてもよい。１つ以上のポリシーは、例えば、管理されたブラウザの１つ以上の機能を制限するよう構成されてもよい。例えば、１つ以上のポリシーは、管理されたブラウザを使用してアクセスされることができる情報のタイプ、管理されたブラウザを使用してアクセスされることができるリソース（例えば、企業リソース、ネットワークリソース等）、管理されたブラウザを使用して情報にアクセスすることができるユーザ、情報の特定のタイプにアクセスするために管理されたブラウザが使用されることができる時間、情報の特定のタイプにアクセスするために管理されたブラウザが使用されることができる位置、を選択的に制限してもよく、および／または、他のものが、他の制限を課してもよい。配置によっては、１つ以上のポリシーのうちの少なくとも１つのポリシーは、下記において検討されるように、管理されたブラウザのアプリケーショントンネリング機能を限定および／または別様に制限してもよい。さらに／あるいは、管理されたブラウザは、管理されたブラウザが、１つ以上のポリシーによって課されるかもしれない制限なしで動作してもよいよう、１つ以上のポリシー（これは例えば、管理モードにおいてブラウザに適用されてもよい）が管理されたブラウザに適用されないかもしれない少なくとも１つの非管理モードを提供するよう構成されてもよい。

【０１３０】
ステップ５１０において、管理されたブラウザを介して１つ以上の企業リソースのアクセスへの要求が受信される。例えば、ステップ５１０において、コンピューティングデバイスは、管理されたブラウザを介して１つ以上の企業リソースのアクセスへの要求を受信してもよい。このような要求は、例えば、管理されたブラウザを介してコンピューティングデバイスにより受信されたユーザ入力に基づいておよび／または対応してもよい（例えば、管理されたブラウザを使用したネットワークリソースへのリンクのユーザ選択および／または別様のアクセス要求に基づいて）。

【０１３１】
ステップ５１５において、少なくとも１つのアプリケーショントンネルが、管理されたブラウザから１つ以上の企業リソースへと生成される。例えば、ステップ５１５において、コンピューティングデバイスは、例えば、管理されたブラウザが企業サーバおよび／または他の企業リソースから企業データにセキュリティ保護された状態でアクセスしてそれを取得できるようにしてもよい、企業サーバおよび／または他の企業リソースへの１つ以上のＶＰＮスタイルトンネルを生成および／または別様に確立してもよい。１つ以上の配置において、アプリケーショントンネリングは、１つのネットワークプロトコル（例えば、送達プロトコル）が異なるネットワークプロトコルを包含する技術を含んでもよい。アプリケーショントンネリングの使用によって、非信頼ネットワークを通じてセキュリティ保護パスが提供されてもよい。

【０１３２】
実施形態によっては、少なくとも１つのアプリケーショントンネルを生成することは、管理されたブラウザから第１の企業リソースへの第１のアプリケーショントンネルを生成することと、管理されたブラウザから第１の企業リソースとは異なる第２の企業リソースへの第２のアプリケーショントンネルを生成することとを含んでもよい。例えば、１つ以上のアプリケーショントンネルの生成において（例えば、ステップ５１５において）、コンピューティングデバイスは、管理されたブラウザによりアクセスされてもよい各企業リソースについての異なる個別のアプリケーショントンネルを生成してもよい。例によっては、第１の企業リソースは、第１のセキュリティレベルを有してもよく、第２の企業リソースは、第１のセキュリティレベルとは異なる第２のセキュリティレベルを有してもよい。例えば、第２の企業リソースは、第１の企業リソースよりも高度のセキュリティレベルを有してもよく、さらなる認証クレデンシャルおよび／またはよりセキュリティ保護されたアクセスプロトコルおよび／または暗号化方法が、第２の企業リソースのアクセスに必要とされてもよい（例えば、第１の企業リソースのアクセスと比較して）。
【０１３３】
実施形態によっては、少なくとも１つのアプリケーショントンネルが、管理されたブラウザに適用されてもよい１つ以上のポリシーに基づいて生成されてもよい（例えば、ステップ５１５において）。例えば、少なくとも１つのアプリケーショントンネルの生成において、管理されたブラウザおよび／または管理されたブラウザを実行中のコンピューティングデバイスは、管理されたブラウザに適用されてもよい、および／または、アプリケーショントンネルを生成ならびに／あるいは使用する管理されたブラウザの能力を選択的に限定および／または別様に制限してもよい、１つ以上のポリシーに従って、少なくとも１つのアプリケーショントンネルを生成してもよい。例えば、１つ以上のポリシーのうちの少なくとも１つのポリシーは、アプリケーショントンネルを使用してアクセスされることができる情報のタイプ、アプリケーショントンネルを使用してアクセスされることができるリソース、アプリケーショントンネルを使用して情報にアクセスすることができるユーザ、管理されたブラウザがアプリケーショントンネルを生成することができる時間、管理されたブラウザがアプリケーショントンネルを生成することができる位置、を選択的に制限してもよく、および／または、他のものが、他の制限を課してもよい。
【０１３４】
ステップ５２０において、１つ以上の企業リソースからの企業データは、少なくとも１つのアプリケーショントンネルを介して取得されてもよい。例えば、ステップ５２０において、コンピューティングデバイスは、１つ以上の企業リソースから企業データを、ステップ５１５において生成されたアプリケーショントンネルを介して取得してもよい。企業データの取得に加えて、コンピューティングデバイスは、管理されたブラウザを介して取得された企業データへのアクセスも提供してもよい（例えば、取得された企業データのいくつかまたは全てを管理されたブラウザに表示されるようにすることによって）。
【０１３５】
実施形態によっては、１つ以上のポリシーが、管理されたブラウザに適用されてもよい。さらに、１つ以上のポリシーは、管理されたブラウザの少なくとも１つの機能を制限するよう構成されてもよい。例えば、１つ以上のポリシーは、管理されたブラウザの特定の機能が選択的に無効化されるべき特定の状況を定義してもよく、コンピューティングデバイスが、（例えば、下記において検討されるように、デバイス状態情報に基づいて）これらの状況を検出および／または別様に特定し、引き続いて１つ以上のポリシーに従って機能を無効化してもよい。例によってはポリシーにより限定されてもよい管理されたブラウザの機能のいくつかの実施例には、カットアンドペースト機能、インスタントメッセージング機能、およびビデオチャット機能が含まれる。これらの機能は、例によっては限定されてもよい機能の実施例としてここに列挙されるが、他の機能が同様に他の例において限定されてもよい。
【０１３６】

実施形態によっては、１つ以上のポリシーが、管理されたブラウザに適用されてもよく、１つ以上のポリシーのうちの少なくとも１つのポリシーが、取得された企業データの使用を制限するよう構成されてもよい。例えば、１つ以上のポリシーが、企業データ（例えば、ステップ５２０においてコンピューティングデバイスおよび／または管理されたブラウザによりアプリケーショントンネルを介して取得された企業データ）が特定の方法でのみ使用されることができる特定の状況を定義してもよく、コンピューティングデバイスが、（例えば、下記において検討されるように、デバイス状態情報に基づいて）これらの状況を検出および／または別様に特定し、引き続いて１つ以上のポリシーに従ってデータが使用されることができる方法を制限および／または別様に制御してもよい。例えば、１つ以上のポリシーのうちの少なくとも１つのポリシーが、取得された企業データが（例えば管理されたブラウザから別のアプリケーションへと）コピーアンドペーストされることができる状況を制限するよう構成されてもよい。別の例として、１つ以上のポリシーのうちの少なくとも１つのポリシーが、取得された企業データが（例えば、管理されたブラウザによりおよび／またはコンピューティングデバイスにより）セーブまたはプリントされることができる状況を制限するよう構成されてもよい。

【０１３７】

実施形態によっては、１つ以上のポリシーのうちの少なくとも１つのポリシーは、デバイス状態情報に依存してもよい。例えば、（例えば、１つ以上のポリシーにより課されるような）管理されたブラウザの機能の制限および／または（さらに／あるいは、１つ以上のポリシーにより課されるような）企業データが管理されたブラウザにより使用されてもよい方法の制限は、コンピューティングデバイスの現在状態を示す状態情報に依存してもよい。このような状態情報は、例えば、コンピューティングデバイス上で（例えば、バックグラウンドアプリケーション、サービスまたは処理として）実行されるよう構成され、例えば（前記において検討された）クライアントエージェント４０４の１つ以上の態様を組み込んでもよいモバイルリソース管理（ＭＲＭ）エージェントにより収集および／または監視されてもよい。

【０１３８】

ＭＲＭエージェントは、例えば、モバイルデバイス管理（ＭＤＭ）機能、モバイルアプリケーション管理（ＭＡＭ）機能および／または他の機能を提供してもおよび／または提供するよう構成されてもよい。例えば、ＭＲＭエージェントは、デバイスに記憶されたおよび／またはデバイスで実行中のオペレーティングシステムおよび／またはアプリケーションを示す状態情報、デバイスに利用可能なおよび／またはデバイスで使用中のネットワーク接続を示す状態情報、および／または、デバイスが位置するおよび／または使用されている現在位置を示す状態情報（例えば、地理座標について、「家庭」または「仕事」等のセマンティックラベルについて）等の、デバイスレベル状態情報を収集および／または監視するよう構成されてもよい。

【０１３９】

これらのタイプの状態情報は、例によっては（例えば、ＭＲＭエージェントにより、コンピューティングデバイス上の１つ以上の他のアプリケーションまたはサービスまたは処理により等）収集および／または監視されてもよい状態情報のタイプの実施例としてここで列挙されるが、さらなるおよび／または代替的な状態情報のタイプが同様に他の例において収集および／または監視されてもよい。さらに、この状態情報のいずれかおよび／または全てが、管理されたブラウザ上への、前記において検討されたポリシー等のポリシーの適用および／または強制において使用されてもよい（例えば、コンピューティングデバイスによりおよび／または管理されたブラウザにより）。

【０１４０】

図６は、本発明で検討される１つ以上の例示的態様に従って、管理されたブラウザのセッションをデバイスクラウドにわたって拡張する方法を示すフローチャートである。１つ以上の実施形態において、図６に示す方法および／またはその１つ以上のステップは、コンピューティングデバイス（例えば、ジェネリックコンピューティングデバイス２０１）

により実行される。他の実施形態において、図６に示す方法および／またはその１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具体化されてもよい。

【０１４１】

図６に見られるように、方法は、管理されたブラウザがロードされるステップ６０５で開始される。例えば、ステップ６０５において、コンピューティングデバイス（例えば、ラップトップコンピュータ、タブレットコンピュータ、スマートフォンまたは他のタイプのモバイルデバイス等のモバイルコンピューティングデバイス）は、ステップ５０５（前記において検討された）においてこのような管理されたブラウザがロードされる方法と同様に、管理されたブラウザをロードしてもよい。

【０１４２】

管理されたブラウザは、例えば、管理されたブラウザに１つ以上のポリシーが適用される少なくとも１つの管理モードを提供するよう構成されてもよく、１つ以上のポリシーは、例えば、前記において検討されたように、管理されたブラウザの１つ以上の機能を制限するよう構成されてもよい。さらに、管理されたブラウザは、実施形態によっては、少なくとも１つの企業リソースから取得されたデータのセキュリティ保護ブラウジングおよびキャッシングを提供するよう構成されてもよい。

【０１４３】

ステップ６１０において、デバイスクラウドを開始するために、少なくとも１つの他のコンピューティングデバイスへの接続が確立されてもよい。例えば、ステップ６１０において、コンピューティングデバイスは、デバイスクラウドを開始するために、１つ以上の他のコンピューティングデバイスへのネットワーク接続を確立してもよい。１つ以上の配置において、デバイスクラウドは、例えば、単一機能またはタスクを実行するために２つ以上のコンピューティングデバイスを互いに組み合わせて使用されることを可能としてもよい。典型的な例において、デバイスは同じユーザに使用されてもよく、および／または、両方が互いの近く（例えば、互いの所定距離内）および／またはユーザの近く（例えば、ユーザの所定距離内）に位置していてもよい。

【０１４４】

例によっては、デバイスクラウドは、ユーザのデバイスの１つによりサポートされてはいないが、ユーザのデバイスの別の１つによりサポートされている機能を提供してもよい。例えば、ラップトップコンピュータのユーザが、別の人とのビデオカンファレンスを行ないたいと考えるが、ラップトップコンピュータがカメラを含んでいない場合がある。しかしながら、ユーザがカメラを含むスマートフォン（または他のコンピューティングデバイス）をも有する場合、デバイスクラウドは２つのデバイスにより提供される機能を動的にリンクするために使用されてもよく、それによって、それらはビデオカンファレンスを提供するために使用されてもよい。特に、この実施例において、デバイスクラウドは、ユーザのスマートフォンがビデオカンファレンス用のビデオ入力装置として使用され（これは例えば、管理されたブラウザ内で実行されてもよいビデオカンファレンシングプラグイン、アプレット、ウェブアプリケーション等により容易化されてもよい）、一方、ユーザのラップトップコンピュータがビデオカンファレンスを行なうのに必要とされる他の機能（例えば、他の人のデバイスへの接続の確立、テキストベースチャット機能の提供等）を実行するために使用されることができるよう、確立される。この実施例は、実施形態によってはデバイスクラウドが１つ以上のデバイスの機能を拡張するために使用されてもよいいくつかの方法を例示するが、このようなデバイスクラウドは、他の実施形態において様々なデバイスの追加のおよび／または代替的な機能を拡張するために他の方法で使用されてもよい。

【０１４５】

ステップ６１５において、管理されたブラウザのセッションが、デバイスクラウドにわたって拡張される。例えば、ステップ６１５において、コンピューティングデバイスは、管理されたブラウザのセッション（例えば、コンピューティングデバイスのユーザが相互

作用中の管理されたブラウザの現在のセッション）をデバイスクラウド（例えば、ステップ６１０において生成されたデバイスクラウド）にわたって拡張してもよい。１つ以上の配置において、デバイスクラウドにわたる管理されたブラウザのセッションの拡張は、少なくとも１つの他の管理されたブラウザが少なくとも１つの他のコンピューティングデバイス上にロードされるようにすることと、少なくとも１つの他の管理されたブラウザでセッションデータを共有することとを含んでもよい。例えば、デバイスクラウドにわたる管理されたブラウザのセッションの拡張において、コンピューティングデバイスは最初に、管理されたブラウザのインスタンスがデバイスクラウドに参加中の他のデバイス上にロードされるようにしてもよい。引き続いて、コンピューティングデバイスは、デバイスクラウドに参加中の他のデバイス上で実行中の管理されたブラウザのインスタンスとセッションデータを共有してもよい。

【０１４６】

このようなセッションデータの共有において、コンピューティングデバイスは、例えば、企業データおよび／または非企業データを含んでもよい、コンピューティングデバイス上の管理されたブラウザにより現在使用中のおよび／または表示中の情報のいくつかまたは全てを送信してもよい。さらに／あるいは、デバイスクラウドに参加中の他のデバイス上で実行中の管理されたブラウザのインスタンスとのセッションデータの共有において、コンピューティングデバイスは、引き続いてコンピューティングデバイス上の管理されたブラウザにより表示および／または別様に使用されてもよい情報を受信してもよい。

【０１４７】

実施形態によっては、１つ以上のポリシーが、管理されたブラウザに適用されてもよく、１つ以上のポリシーが、管理されたブラウザの少なくとも１つの機能を制限するよう構成されてもよい。例えば、コンピューティングデバイスおよび／またはコンピューティングデバイス上で実行中の（ＭＲＭエージェント等の）ソフトウェアは、管理されたブラウザの機能を制限するよう構成された１つ以上のポリシーを管理されたブラウザに適用してもよい。

【０１４８】

実施形態によっては、１つ以上のポリシーが、管理されたブラウザに適用されてもよく、１つ以上のポリシーが、デバイスクラウドを制限するよう構成されてもよい。例えば、コンピューティングデバイスおよび／またはコンピューティングデバイス上で実行中の（ＭＲＭエージェント等の）ソフトウェアは、例によっては、デバイスクラウド（例えば、ステップ６１０において生成されたデバイスクラウド）の様々な態様を制限するよう構成された１つ以上のポリシーを管理されたブラウザに適用してもよい。

【０１４９】

１つ以上のポリシーがデバイスクラウドを制限するよう構成される例によっては、１つ以上のポリシーのうちの少なくとも１つのポリシーは、少なくとも１つの他のコンピューティングデバイスに少なくとも１つの役割を割り当てるよう構成されてもよい。例えば、１つ以上のポリシーがデバイスクラウドを制限するよう構成される例において、コンピューティングデバイスおよび／またはコンピューティングデバイス上で実行中のソフトウェアは、デバイスクラウドに参加中の他のコンピューティングデバイスにデバイスクラウド内の特定の役割を割り当てるよう構成された少なくとも１つのポリシーを定義、適用および／または強制してもよい。例えば、ビデオカンファレンスを必要とする前記の実施例では、モバイルデバイス管理ポリシーは、ビデオキャプチャの役割をデバイスクラウドに必要とされるスマートフォンに割り当ててもよく、モバイルデバイス管理ポリシーは、接続維持の役割をデバイスクラウドに必要とされるラップトップコンピュータに割り当ててもよい。

【０１５０】

実施形態によっては、少なくとも１つの他のコンピューティングデバイスへの接続は、管理されたブラウザに適用されてもよい１つ以上のポリシーのうちの少なくとも１つのポリシーに基づいて確立されてもよい。例えば、少なくとも１つの他のコンピューティング

デバイスへの接続の確立において、管理されたブラウザおよび／または管理されたブラウザを実行中のコンピューティングデバイスは、管理されたブラウザに適用されてもよい１つ以上のポリシーに従って、少なくとも１つの他のコンピューティングデバイスに接続および／または少なくとも１つの他のコンピューティングデバイスとデータ交換してもよい。例えば、１つ以上のポリシーは、デバイスクラウドを開始する管理されたブラウザの能力が選択的に有効化、選択的に無効化および／または別様に制限されてもよい特定の状況を定義してもよい。例えば、１つ以上のポリシーのうちの少なくとも１つのポリシーは、他のコンピューティングデバイスと交換されることができる情報のタイプ、他のコンピューティングデバイスと交換される情報にアクセスすることができるユーザ、管理されたブラウザが他のコンピューティングデバイスと情報を交換することができる時間、管理されたブラウザが他のコンピューティングデバイスと情報を交換することができる位置、を選択的に制限してもよく、および／または、他のものが、他の制限を課してもよい。これらの制限のいずれかおよび／または全てが、コンピューティングデバイスが少なくとも１つの他のコンピューティングデバイスへの接続を確立することができる状況を制限してもよく、および／または、デバイスクラウドが開始されることができる状況を別様に制限してもよい。

【０１５１】

実施形態によっては、少なくとも１つの他のコンピューティングデバイスへの接続の確立は、少なくとも１つの他のコンピューティングデバイスに関する状態情報を評価し、評価された状態情報に基づいて少なくとも１つのコンピューティングデバイスがデバイスクラウドに参加することを許可するかを判断することを含んでもよい。例えば、少なくとも１つの他のコンピューティングデバイスへの接続の確立において（例えば、ステップ６１０において）、コンピューティングデバイスは、少なくとも１つの他のコンピューティングデバイスに関する状態情報を取得および／または評価してもよい。

【０１５２】

このような状態情報は、例えば、少なくとも１つの他のコンピューティングデバイス上でインストールおよび／または実行されているアプリケーション、少なくとも１つの他のコンピューティングデバイスが接続されているネットワーク、少なくとも１つの他のコンピューティングデバイスの位置および／または他の考慮事項等の、少なくとも１つの他のコンピューティングデバイスの現在のデバイス状態の様々な態様を記述してもよい。

【０１５３】

引き続いて、コンピューティングデバイスは、この状態情報の評価に基づいて、少なくとも１つの他のコンピューティングデバイスのデバイスクラウドへの参加を許可するかどうかを判定してもよい。このような判定は、例えば、１つ以上のポリシーに基づいてもよい。例えば、１つ以上のポリシーは、少なくとも１つの他のコンピューティングデバイスに関する状態情報が、デバイスが特定の位置に位置しているかいないか、デバイス上でインストールされたおよび／または実行中の特定のアプリケーションを有しているかいないか、１つ以上の特定のネットワークに接続されているかいないか、および／または同様のものを示す場合に、少なくとも１つの他のコンピューティングデバイスがデバイスクラウドに参加することをコンピューティングデバイスが許可してもよいことを指示してもよい。

【０１５４】

図７は、本発明で検討される１つ以上の例示的態様に従って、管理されたブラウザの動作モードを選択的に無効化する方法を示すフローチャートである。１つ以上の実施形態において、図７に示す方法および／またはその１つ以上のステップは、コンピューティングデバイス（例えば、ジェネリックコンピューティングデバイス２０１）により実行される。他の実施形態において、図７に示す方法および／またはその１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具体化されてもよい。

【０１５５】

図７に見られるように、この方法は、管理されたブラウザがロードされるステップ７０５で開始する。例えば、ステップ７０５において、コンピューティングデバイス（例えば、ラップトップコンピュータ、タブレットコンピュータ、スマートフォンまたは他のタイプのモバイルデバイス等のモバイルコンピューティングデバイス）は、ステップ５０５（前記において検討された）においてこのような管理されたブラウザがロードされる方法と同様に、管理されたブラウザをロードしてもよい。管理されたブラウザは、例えば、管理されたブラウザに１つ以上のポリシーが適用される少なくとも１つの管理モードを提供するよう構成されてもよく、１つ以上のポリシーは、例えば、前記において検討されたように、管理されたブラウザの１つ以上の機能を制限するよう構成されてもよい。さらに、管理されたブラウザは、実施形態によっては、少なくとも１つの企業リソースから取得されたデータのセキュリティ保護ブラウジングおよびキャッシングを提供するよう構成されてもよい。

【０１５６】

１つ以上の配置において、管理されたブラウザは、管理モードおよび非管理モードを有するデュアルモードアプリケーションであってもよい。さらに、管理されたブラウザの管理モードは、企業データへのアクセスを提供するよう構成されてもよく、管理されたブラウザの非管理モードは、企業データへのアクセスを制限するよう構成されてもよい。例えば、管理モードにおいて、管理されたブラウザは、特定のコンテンツフィルタを適用、特定のダウンロードを制限、および／または、特定のプラグインをブロックしてもよく、一方、非管理モードにおいて、管理されたブラウザは、このようなフィルタを適用せず、このようなダウンロードを制限せず、および／または、このようなプラグインをブロックせずともよい。例によっては、コンピューティングデバイスおよび／またはコンピューティングデバイス上で実行中の他のソフトウェア（例えば、ＭＲＭエージェント）は、下記において検討されるように、（例えば、管理されたブラウザの管理モードが、コンピューティングデバイスによりおよび／またはコンピューティングデバイス上で実行中の他の適切なソフトウェアにより再有効化されるまで）管理されたブラウザが非管理モードにおいてのみ実行および／または実行継続されることができるよう、管理されたブラウザの管理モードを選択的に無効化してもよい。

【０１５７】

ステップ７１０において、デバイス状態情報が取得される。例えば、ステップ７１０において、コンピューティングデバイスは、コンピューティングデバイスの現在状態を示す状態情報を取得してもよい。例によっては、このような状態情報は、前記の例において検討されたＭＲＭエージェント等の、コンピューティングデバイス上で実行中のＭＲＭエージェントにより取得されてもよい。

【０１５８】

実施形態によっては、デバイス状態情報は、コンピューティングデバイス上に存在する１つ以上のアプリケーションを特定する情報を含んでもよい。例えば、デバイス状態情報の取得において（例えば、ステップ７１０において）、コンピューティングデバイスおよび／またはコンピューティングデバイス上で実行中のＭＲＭエージェントは、どのようなアプリケーションがコンピューティングデバイス上に記憶され、インストールされ、コンピューティングデバイス上で以前に実行され、および／または、コンピューティングデバイス上で現在実行されているかを判定するために、１つ以上のストレージデバイス（これは例えば、コンピューティングデバイスに接続および／または別様にアクセス可能にされてもよい）および／またはインストールログ（これは例えば、コンピューティングデバイスにより維持されてもよい）を検査してもよい。

【０１５９】

実施形態によっては、デバイス状態情報は、コンピューティングデバイスにより使用される１つ以上のネットワーク接続を特定する情報を含んでもよい。例えば、デバイス状態情報の取得において（例えば、ステップ７１０において）、コンピューティングデバイスおよび／またはコンピューティングデバイス上で実行中のＭＲＭエージェントは、どのよ

うなネットワークがコンピューティングデバイスにアクセス可能および／またはその範囲内か、どのようなネットワークにコンピューティングデバイスが以前に接続されていたか、および／または、どのようなネットワークにコンピューティングデバイスが現在接続されているかを判定するために、１つ以上のネットワークインタフェースおよび／または他のネットワークデバイス（これは例えば、コンピューティングデバイスに接続および／または別様に使用可能にされてもよい）および／または１つ以上の接続ログ（これは例えば、コンピューティングデバイスにより維持されてもよい）を検査してもよい。

【０１６０】

実施形態によっては、デバイス状態情報は、コンピューティングデバイスの現在位置を特定する情報を含んでもよい。例えば、デバイス状態情報の取得において（例えば、ステップ７１０において）、コンピューティングデバイスおよび／またはコンピューティングデバイス上で実行中のＭＲＭエージェントは、コンピューティングデバイスの現在位置を、判定および／または１つ以上の他のコンポーネント（例えば、ＧＰＳ受信機、他の処理コンポーネント等）および／またはデバイスに判定させてもよい。例によっては、位置情報は、コンピューティングデバイスの現在位置を示す地理座標を含んでもよい。例によっては、位置情報は、１つ以上のユーザ特有のランドマークに関するコンピューティングデバイスの現在位置を示すセマンティックラベル（例えば、「家庭」または「仕事」）を含んでもよい。この位置のいずれかおよび／または全ては、例えば、１つ以上の位置ベースモバイルデバイス管理ポリシーの適用および／または強制において、コンピューティングデバイスおよび／またはコンピューティングデバイス上で実行中のＭＲＭエージェントにより使用されてもよい。

【０１６１】

ステップ７１５において、デバイス状態情報に基づいて、管理されたブラウザの１つ以上の動作モードを選択的に無効化するべきかどうかを判定する。例えば、ステップ７１５において、コンピューティングデバイスは、ステップ７１０において取得されたデバイス状態情報に基づいて、管理されたブラウザの１つ以上の動作モードを選択的に無効化するべきかどうかを判定してもよい。前記において検討されたように、管理されたブラウザは、例によっては、管理モードおよび非管理モードを有するデュアルモードアプリケーションであってもよい。

【０１６２】

このように、例によっては、コンピューティングデバイスは、ステップ７１５において、ステップ７１０において取得されたデバイス状態情報に基づいて管理されたブラウザの管理モードを選択的に無効化するべきかどうかを判定してもよい。例えば、コンピューティングデバイスは、コンピューティングデバイス上に存在する１つ以上のアプリケーションを特定する情報、コンピューティングデバイスにより使用される１つ以上のネットワーク接続を特定する情報および／またはコンピューティングデバイスの現在位置を特定する情報に基づいて、管理されたブラウザの管理モードを選択的に無効化するべきかどうかを判定してもよい。例によっては、コンピューティングデバイスは、さらに／あるいは、管理されたブラウザのモード（例えば、管理されたブラウザの管理モード）を選択的に無効化するべきかどうかの判定において、デバイス状態情報と組み合わせて１つ以上のポリシーを評価してもよい。

【０１６３】

ステップ７１５において、管理されたブラウザの１つ以上の動作モードが無効化されないと判定されると、方法は終了する。さらに／あるいは、（例えば、更新されたデバイス状態情報を取得および／または再評価して、管理されたブラウザの１つ以上の動作モードを選択的に無効化するべきかどうかを判定するために）ステップ７１０および７１５が周期的に繰り返されるように、方法はループ内で継続してもよい。

【０１６４】

一方、ステップ７１５において、管理されたブラウザの少なくとも１つの動作モードが選択的に無効化されるべきであると判定されると、ステップ７２０において、管理された

ブラウザの少なくとも１つの動作モードが無効化される。例えば、ステップ７２０において、コンピューティングデバイスは、管理されたブラウザの少なくとも１つの動作モード（例えば、ステップ７１５で無効化されるべきであると判定されたモード）を無効化してもよく、および／または、管理されたブラウザの少なくとも１つの動作モードが無効化されるようにしてもよい。管理されたブラウザが管理モードおよび非管理モードを有するデュアルモードアプリケーションである例においては、管理されたブラウザは、例えば、ステップ７２０においてコンピューティングデバイスにより無効化されてもよい（および／またはコンピューティングデバイスにより無効化されるようにされてもよい）。

【０１６５】

実施形態によっては、少なくとも１つの管理モードが無効化されるようにすることは、管理されたブラウザに少なくとも１つの管理モードとは異なる第２のモードに入らせることを含んでもよい。例えば、管理されたブラウザの管理モードの管理モードを無効化することおよび／または別様に管理されたブラウザの管理モードが無効化されるようにすることにおいて（例えば、ステップ７２０において）、コンピューティングデバイスは、管理されたブラウザが以前動作していた管理モードとは異なる第２のモードに、管理されたブラウザを入らせてもよい。例によっては、第２のモードは、管理されたブラウザが以前動作していた管理モードとは単に異なる別の管理モードであってもよい（例えば、異なるポリシーが管理されたブラウザに適用されたので）。すなわち、第２のモードは、例によっては、１つ以上のポリシーのうちの第２のセットが管理されたブラウザに適用され、１つ以上のポリシーのうちの第２のセットは、少なくとも１つの管理モードにおいて管理されたブラウザに適用される１つ以上のポリシーとは異なる少なくとも１つのポリシーを含む、管理モードであってもよい。

【０１６６】

他の例においては、第２のモード（これには例えば、少なくとも１つの管理モードが無効化された後に、管理されたブラウザが入ってもよい）は、管理されたブラウザがもはや少なくとも１つのデバイスマネージャにより管理されない非管理モードであってもよい。例えば、管理されたブラウザの管理モードを無効化することおよび／または別様に無効化されるようにすることにおいて（例えば、ステップ７２０において）、コンピューティングデバイスは、管理されたブラウザが少なくとも１つのデバイスマネージャにより管理されない前記において検討された非管理モード等の、非管理モードに管理されたブラウザを入らせてもよい。このようなデバイスマネージャは、例えば、デバイス上で実行中であり、１つ以上のポリシーを管理されたブラウザおよび／またはデバイスの他のアプリケーション、サービスおよび／または機能に適用および／または強制するよう構成されたモバイルリソース管理エージェントであってもよい。

【０１６７】

実施形態によっては、１つ以上のリソースへのアクセスは、非管理モードにおいてブロックされてもよい。例えば、非管理モードに入った後、管理されたブラウザおよび／またはコンピューティングデバイスは、特定の企業リソース等の特定のリソースへのアクセスをブロックしてもよい。このようなブロックは、例えば、管理されたブラウザを使用して別様にアクセスされるかもしれない企業情報のセキュリティを確保するために、ポリシー強制、監視および／または他のセキュリティ特徴が適用されないおよび／または利用可能ではない非管理モードで管理されたブラウザが動作する間、管理されたブラウザのユーザが企業リソースおよび／または他の特定のリソースにアクセスするのを防止してもよい。

【０１６８】

リモート企業リソースに遠隔記憶された情報へのアクセスのブロックに加えて、管理されたブラウザおよび／またはコンピューティングデバイスはまた、非管理モードにおいて、デバイスにローカルにキャッシュされてもよい特定の情報へのアクセスをブロックしてもよい。例えば、非管理モードの間、このようなブロッキングは、管理されたブラウザが、ローカルにキャッシュされた企業アプリケーションストア情報および／または他のローカルにキャッシュされた企業情報等の、本来的には企業リソースから取得された、ローカ

ルにキャッシュされたデータにアクセスすることを防止してもよい。

【０１６９】

実施形態によっては、管理されたブラウザは、更新されたデバイス状態情報に基づいて非管理モードから少なくとも１つの管理モードに遷移して戻るよう構成されてもよい。例えば、非管理モードに入った後、管理されたブラウザおよび／またはコンピューティングデバイスは、管理されたブラウザが管理モード（そこでは例えば、１つ以上のポリシーが管理されたブラウザに適用され、管理されたブラウザはデバイスマネージャ等に管理されてもよい）に再び入ることができるかどうかを判定するために、現在のデバイス状態情報を監視および周期的に再評価するように構成されてもよい。

【０１７０】

例えば、管理されたブラウザおよび／またはコンピューティングデバイスが、例えば状態情報に基づいて、特定の状況が満たされたと判定した場合、コンピューティングデバイスは、管理されたブラウザに管理モードへと切り替わって戻させてもよい。例によっては、管理されたブラウザが管理モードに再び入ることができるかどうかの判定において、コンピューティングデバイスおよび／または管理されたブラウザは、例えばまず、管理されたブラウザを非管理モードに切り替えるべきかの判定において評価された１つ以上のポリシーを含んでもよい、１つ以上のポリシーに鑑みて現在のデバイス状態情報を評価してもよい。

【０１７１】

図８は、本発明の１つ以上の態様に従って、１つ以上のモバイルデバイス管理ポリシーを管理されたブラウザに適用する方法を示すフローチャートである。１つ以上の実施形態において、図８に例示する方法および／またはその１つ以上のステップは、コンピューティングデバイス（例えば、ジェネリックコンピューティングデバイス２０１）により実行されてもよい。他の実施形態において、図８に示す方法および／またはその１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具体化されてもよい。

【０１７２】

図８に見られるように、この方法は、管理されたブラウザがロードされるステップ８０５で開始する。例えば、ステップ８０５において、コンピューティングデバイス（例えば、ラップトップコンピュータ、タブレットコンピュータ、スマートフォンまたは他のタイプのモバイルデバイス等のモバイルコンピューティングデバイス）は、ステップ５０５（前記において検討された）においてこのような管理されたブラウザがロードされる方法と同様に、管理されたブラウザをロードしてもよい。管理されたブラウザは、例えば、管理されたブラウザに１つ以上のポリシーが適用される少なくとも１つの管理モードを提供するよう構成されてもよく、１つ以上のポリシーは、例えば、前記において検討されたように、管理されたブラウザの１つ以上の機能を制限するよう構成されてもよい。さらに、管理されたブラウザは、実施形態によっては、少なくとも１つの企業リソースから取得されたデータのセキュリティ保護ブラウジングおよびキャッシングを提供するよう構成されてもよい。

【０１７３】

ステップ８１０において、１つ以上のポリシーが受信されてもよい。例えば、ステップ８１０において、コンピューティングデバイスは１つ以上のポリシーを受信してもよい。１つ以上のポリシーは、例えば、デバイス状態情報（state information）（例えば、コンピューティングデバイスおよび／またはコンピューティングデバイス上で実行中のＭＲＭエージェントにより取得および／または監視されたデバイス状態情報）を使用して評価されてもよい状況の異なるセットに基づいて、許可された、禁止されたおよび／または制限された機能を定義するモバイルデバイス管理ポリシーであってもよい。このように、ポリシーは、管理されたブラウザの様々な機能を含む様々な機能へのデバイス状態ベースの挙動制限の強制において使用されてもよい。

【０１７４】

実施形態によっては、１つ以上のポリシーは、ポリシーサーバから受信されてもよい。例えば、ポリシーの受信において、コンピューティングデバイスは、ステップ８１０において、ポリシーサーバに接続されおよび／またはポリシーサーバからいくつかのポリシーを受信してもよい。ポリシーサーバは、例えば、企業ネットワークインフラストラクチャの一部であってもよく、（例えば、ステップ８１０においてコンピューティングデバイスにより）受信されたポリシーに従って管理されたブラウザによりアクセスされてもよい１つ以上の企業リソースに接続されおよび／または含まれてもよい。

【０１７５】

ステップ８１５において、１つ以上のポリシーは、管理されたブラウザに適用される。例えば、ステップ８１５において、コンピューティングデバイスは、（例えば、コンピューティングデバイスおよび／またはコンピューティングデバイス上で実行中のＭＲＭエージェントにより取得および／または監視されたデバイス状態情報に基づいて）管理されたブラウザの特定の機能が選択的に有効化および／または無効化されてもよいよう、（例えば、ステップ８１０において受信されたような）１つ以上のポリシーを管理されたブラウザに適用してもよい。

【０１７６】

実施形態によっては、１つ以上のポリシーは、コンピューティングデバイスのユーザに関するアイデンティティ情報に基づいて管理されたブラウザに適用されてもよい。例えば、管理されたブラウザへの１つ以上のポリシーの適用において（例えば、ステップ８１５において）、コンピューティングデバイスは、コンピューティングデバイスの現在のユーザに関するアイデンティティ情報を要求および／または取得してもよい。このようなアイデンティティ情報は、例えば、ユーザに自身のログイン情報および／または他の認証クレデンシャルの提供を促すよう構成された１つ以上の認証プロンプトを介して取得されてもよい。アイデンティティ情報に基づいた管理されたブラウザへのポリシー適用により、管理されたブラウザおよび／またはコンピューティングデバイスの現在のユーザについて（例えば、管理されたブラウザに適用中の１つ以上のポリシーにより）選択的に有効化、無効化および／または制限された特定の機能は、ユーザのアイデンティティに鑑みて、特定の現在のユーザに対してより調整されてもよい。

【０１７７】

実施形態によっては、１つ以上のポリシーは、コンピューティングデバイスのユーザに関する役割情報（role information）に基づいて管理されたブラウザに適用されてもよい。例えば、管理されたブラウザへの１つ以上のポリシーの適用において（例えば、ステップ８１５において）、コンピューティングデバイスは、コンピューティングデバイスの現在のユーザに関するアイデンティティ情報および／または役割情報を要求および／または取得してもよい。役割情報は、例えば、（例えば、販売、技術、法務、会計、役員等の）企業内の現在のユーザの役割を特定してもよい。例によっては、コンピューティングデバイスは、例えば、コンピューティングデバイスの現在のユーザについてのアイデンティティ情報に基づいてコンピューティングデバイスの現在のユーザについての役割情報を判定してもよい（例えば、アイデンティティ情報を使用して１つ以上のデータベース、ディレクトリおよび／または企業リソース内のユーザについての役割情報にアクセスおよび／またはルックアップすることによって）。役割情報に基づいた管理されたブラウザへのポリシー適用により、管理されたブラウザおよび／またはコンピューティングデバイスの現在のユーザについて（例えば、管理されたブラウザに適用中の１つ以上のポリシーにより）選択的に有効化、無効化および／または制限された特定の機能は、企業内のユーザの役割に鑑みて、特定の現在のユーザの必要性および／またはアクセスレベルに対してより調整されてもよい。

【０１７８】

例えば、病院等のヘルスケア企業のコンテキストにおける役割情報に基づいた管理されたブラウザへの１つ以上のポリシーの適用において、コンピューティングデバイスは、（例えば、コンピューティングデバイスの現在のユーザについてのアイデンティティ情報を

取得および／または解析することにより）コンピューティングデバイスの現在のユーザが医者または看護師であるかどうかを判定する。コンピューティングデバイスがコンピューティングデバイスの現在のユーザが医者であると判定した場合、コンピューティングデバイスは、管理されたブラウザにポリシーの第１のセットを適用してもよく、またコンピューティングデバイスがコンピューティングデバイスの現在のユーザが看護師であると判定した場合には、コンピューティングデバイスは、管理されたブラウザにポリシーの第１のセットとは異なるポリシーの第２のセットを適用してもよい。特に、ポリシーの第２のセットは、例えば、ヘルスケア企業内の看護師の役割と医者の役割との違いに基づいて、ポリシーの第１のセットとは異なって、管理されたブラウザの追加のおよび／または代替的な機能を、選択的に有効化、無効化および／または制限してもよい。例えば、管理されたブラウザに適用されるポリシーの結果として、医者は例えば、コンピューティングデバイス上の管理されたブラウザを使用して、看護師がアクセスすることができないかもしれない特定のリソースにアクセスすることができるようにしてもよい。

【０１７９】

別の実施例として、法律事務所等のリーガル企業のコンテキストにおける役割情報に基づいた管理されたブラウザへの１つ以上のポリシーの適用において、コンピューティングデバイスは、コンピューティングデバイスの現在のユーザが、法律事務所が取り扱う特定の事件および／または他の事項からスクリーニングされたプロフェッショナルグループ内の弁護士または他のプロフェッショナルであるかどうかを判定してもよい。コンピューティングデバイスがコンピューティングデバイスの現在のユーザがスクリーニングされたプロフェッショナルグループ内のものであると判定した場合、コンピューティングデバイスは、管理されたブラウザにポリシーの第１のセットを適用してもよい。コンピューティングデバイスがコンピューティングデバイスの現在のユーザがスクリーニングされたプロフェッショナルグループ内のものではないと判定した場合、コンピューティングデバイスは、管理されたブラウザにポリシーの第１のセットとは異なるポリシーの第２のセットを適用してもよい。

【０１８０】

特に、ポリシーの第２のセットは、例えば、リーガル企業内の特定のプロフェッショナルの役割の違いに基づいて、ポリシーの第１のセットとは異なって、管理されたブラウザの追加のおよび／または代替的な機能を、選択的に有効化、無効化および／または制限してもよい。例えば、管理されたブラウザに適用されるポリシーの結果として、特定の弁護士は、コンピューティングデバイス上の管理されたブラウザを使用して、法律事務所内の他の弁護士がアクセスすることができないかもしれない特定のリソースにアクセスすることができるようにしてもよい。

【０１８１】

実施形態によっては、管理されたブラウザへの１つ以上のポリシーの適用は、管理されたブラウザを介してアクセス可能な１つ以上の企業リソースへのアクセスを制御することを含んでもよい。例えば、管理されたブラウザへの１つ以上のポリシーの適用において（例えば、ステップ８１５において）、コンピューティングデバイスは、管理されたブラウザを使用してアクセス可能な企業リソースへのアクセスを制御してもよい。特に、１つ以上のポリシーのうちの少なくとも１つのポリシーは、例えば、特定のデータベース、サーバおよび／または他の企業リソース（これは例えば、企業インフラストラクチャの全部および／またはその一部に接続されてもよい）等の、特定の企業リソースへのアクセスを選択的に有効化、無効化および／または制限してもよい。さらに／あるいは、このようなポリシーは、例えば、コンピューティングデバイスの現在の状態に基づいて特定の企業リソースへのアクセスが制御されてもよいよう、デバイス状態情報（これは例えば、コンピューティングデバイス上に存在する１つ以上のアプリケーションを特定する情報、コンピューティングデバイスにより使用される１つ以上のネットワーク接続を特定する情報および／またはコンピューティングデバイスの現在位置を特定する情報を含んでもよい）に依存してもよい。

【０１８２】
実施形態によっては、管理されたブラウザへの１つ以上のポリシーの適用は、管理されたブラウザを介して１つ以上の企業リソースから取得された情報の使用を制御することを含んでもよい。例えば、管理されたブラウザへの１つ以上のポリシーの適用において（例えば、ステップ８１５において）、コンピューティングデバイスは、管理されたブラウザを使用して企業リソースから取得された情報等の、企業リソースから取得された情報がいかに使用されることができるか（例えば、管理されたブラウザによっておよび／またはコンピューティングデバイス上の他のアプリケーション、サービスならびに／あるいは処理によって）を制御してもよい。
【０１８３】
特に、１つ以上のポリシーのうちの少なくとも１つのポリシーは、例えば、企業リソースから取得された情報をセーブする能力、企業リソースから取得された情報をプリントする能力、企業リソースから取得された情報をカット、コピーならびに／あるいはペーストする能力、企業リソースから取得された情報をエディットする能力および／または企業リソースから取得された情報に相互作用および／またはそれを使用する他の能力を、選択的に許可、禁止および／または別様に制限してもよい。さらに／あるいは、このようなポリシーは、例えば、コンピューティングデバイスの現在の状態に基づいて企業リソースから取得された特定の情報の使用が制御されてもよいよう、デバイス状態情報（これは例えば、コンピューティングデバイス上に存在する１つ以上のアプリケーションを特定する情報、コンピューティングデバイスにより使用される１つ以上のネットワーク接続を特定する情報および／またはコンピューティングデバイスの現在位置を特定する情報を含んでもよい）に依存してもよい。
【０１８４】
図９は、本発明で検討される１つ以上の例示的態様に従って、管理されたブラウザを介してセキュリティ保護ドキュメントコンテナへのアクセスを提供する方法を示すフローチャートである。１つ以上の実施形態において、図９に示す方法および／またはその１つ以上のステップは、コンピューティングデバイス（例えば、ジェネリックコンピューティングデバイス２０１）により実行されてもよい。他の実施形態において、図９に示す方法および／またはその１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具体化されてもよい。
【０１８５】
図９に見られるように、方法は、管理されたブラウザがロードされるステップ９０５で開始される。例えば、ステップ９０５において、コンピューティングデバイス（例えば、ラップトップコンピュータ、タブレットコンピュータ、スマートフォンまたは他のタイプのモバイルデバイス等のモバイルコンピューティングデバイス）は、ステップ５０５（前記において検討された）においてこのような管理されたブラウザがロードされる方法と同様に、管理されたブラウザをロードしてもよい。管理されたブラウザは、例えば、管理されたブラウザに１つ以上のポリシーが適用される少なくとも１つの管理モードを提供するよう構成されてもよく、１つ以上のポリシーは、例えば、前記において検討されたように、管理されたブラウザの１つ以上の機能を制限するよう構成されてもよい。さらに、管理されたブラウザは、実施形態によっては、少なくとも１つの企業リソースから取得されたデータのセキュリティ保護ブラウジングおよびキャッシングを提供するよう構成されてもよい。
【０１８６】
ステップ９１０において、管理されたブラウザを介した１つ以上の企業リソースのアクセスへの要求が受信されてもよい。例えば、ステップ９１０において、コンピューティングデバイスは、管理されたブラウザを介した１つ以上の企業リソースのアクセスへの要求を受信してもよい。このような要求は、例えば、管理されたブラウザを介してコンピューティングデバイスにより受信されたユーザ入力に基づいておよび／または対応してもよい（例えば、管理されたブラウザを使用したネットワークリソースへのユーザのリンク選択

および／または別様のアクセス要求に基づいて）。

【０１８７】

ステップ９１５において、１つ以上の企業リソースからの企業データは、要求に基づいて取得される。例えば、ステップ９１５において、コンピューティングデバイスは、ステップ９１０において受信された要求に基づいて１つ以上の企業リソースに接続し、１つ以上の企業リソースから情報を要求し、引き続いて、情報を受信および／または別様に取得してもよい。

【０１８８】

ステップ９２０において、取得された企業データは、セキュリティ保護ドキュメントコンテナに記憶される。例えば、ステップ９２０において、コンピューティングデバイスは、ステップ９１５において取得された企業データをセキュリティ保護ドキュメントコンテナに記憶してもよい。１つ以上の配置において、セキュリティ保護ドキュメントコンテナは、１つ以上の企業リソースからコンピューティングデバイスにより受信される企業データをセキュリティ保護された状態で記憶するよう構成されるコンピューティングデバイス上のデータリポジトリであってもよい。さらに／あるいは、１つ以上のモバイルデバイス管理ポリシーは、セキュリティ保護ドキュメントコンテナへのアクセスが制限、修正および／または別様に制御されるべき特定の状況を定義してもよく、コンピューティングデバイスおよび／またはコンピューティングデバイス上で実行中のＭＲＭエージェントは、デバイス状態情報に基づいてこれらの状況を検出してもよく、引き続いてポリシーに従ってセキュリティ保護ドキュメントコンテナへのアクセスを制限、修正および／または別様に制御してもよい。他の例において、セキュリティ保護ドキュメントコンテナの他の態様（例えば、セキュリティ保護ドキュメントコンテナへのアクセス以外）は、１つ以上のモバイルデバイス管理ポリシーにより同様に制御されてもよい。

【０１８９】

ステップ９２５において、セキュリティ保護ドキュメントコンテナへのアクセスは、管理されたブラウザを介して提供される。例えば、ステップ９２５において、コンピューティングデバイスは、セキュリティ保護ドキュメントコンテナへのアクセスを管理されたブラウザを介して提供してもよい。セキュリティ保護ドキュメントコンテナへのアクセスの管理されたブラウザを介した提供において、コンピューティングデバイスは、例えば、セキュリティ保護ドキュメントコンテナに記憶された企業データおよび／または他の情報が閲覧され、エディットされおよび／または別様にアクセスされることを許可するよう構成された１つ以上のユーザインタフェースを、管理されたブラウザに表示および／または別様に提示させてもよい。例えば、ステップ９２５において、コンピューティングデバイスは、コンピューティングデバイスのユーザが、セキュリティ保護ドキュメントコンテナに記憶された情報をブラウズ、セキュリティ保護ドキュメントコンテナに記憶された特定のファイルおよび／または他の情報を閲覧、セキュリティ保護ドキュメントコンテナに記憶された情報をエディット、セキュリティ保護ドキュメントコンテナに記憶された情報を削除、および／または、セキュリティ保護ドキュメントコンテナに記憶された情報に別様に相互作用ならびに／あるいはアクセスすることを許可する１つ以上のユーザインタフェースを、管理されたブラウザに表示および／または別様に提示させてもよい。

【０１９０】

ステップ９３０において、データは、セキュリティ保護ドキュメントコンテナから選択的にワイプ（wipe）される。例えば、ステップ９３０において、コンピューティングデバイスは、セキュリティ保護ドキュメントコンテナから情報を選択的にワイプおよび／または別様に削除してもよい。１つ以上の配置において、コンピューティングデバイスは、デバイス状態情報、１つ以上のポリシー、および／または他のファクターおよび／またはコンピューティングデバイスならびに／あるいはコンピューティングデバイス上で実行中のＭＲＭエージェントにより評価および／または検出されてもよい状況に基づいてセキュリティ保護ドキュメントコンテナからデータを選択的にワイプしてもよい。

【０１９１】

例によっては、コンピューティングデバイスは、セキュリティ保護ドキュメントコンテナに記憶されてもよい他の企業データを含む他のデータ等の他のデータを残しつつ、ステップ９１５において取得された企業データ等のいくつかのデータをセキュリティ保護ドキュメントコンテナからワイプしてもよい。他の例において、コンピューティングデバイスは、他のデータ（例えば、異なる期間に受信および／または記憶されたデータ）を残しつつ、特定の期間（例えば、直近４時間以内）に受信および／または記憶されたデータをセキュリティ保護ドキュメントコンテナからワイプしてもよい。さらに他の例において、コンピューティングデバイスは、他のデータ（例えば、管理されたブラウザの他のアプリケーションおよび／または他のセッションに関するデータ）を残しつつ、管理されたブラウザおよび／または管理されたブラウザの特定のセッションに関連して受信および／または記憶されたデータをセキュリティ保護ドキュメントコンテナからワイプしてもよい。

【０１９２】

実施形態によっては、セキュリティ保護ドキュメントコンテナからのデータの選択的ワイプは、要求に基づいて１つ以上の企業リソースから取得された企業データを削除することを含んでもよい。例えば、セキュリティ保護ドキュメントコンテナからのデータの選択的ワイプにおいて（例えば、ステップ９３０において）、コンピューティングデバイスは、ステップ９１５において企業リソースから取得された企業データを削除してもよい。この企業データの削除において、コンピューティングデバイスは、例えば、セキュリティ保護ドキュメントコンテナに記憶されてもよい他のデータ（これは例えば、他のブラウジングセッションの間に取得されてもよく、他のアプリケーション等に関連してもよい）を残しつつおよび／または別様に保存しつつ、企業データが取得された特定のブラウジングセッションの間に取得された企業データ、ならびに、このブラウジングセッションの間に取得された任意の他の情報を削除してもよい。

【０１９３】

実施形態によっては、管理されたブラウザが閉じられたときに、データがセキュリティ保護ドキュメントコンテナから選択的にワイプされてもよい。例えば、コンピューティングデバイスは、例によっては、管理されたブラウザが閉じられたこと（例えば、コンピューティングデバイスのユーザが管理されたブラウザを閉じたとき、コンピューティングデバイスのユーザが管理されたブラウザのタブを閉じたおよび／または管理されたブラウザの特定のセッションを別様に閉じたとき、コンピューティングデバイス上で実行中のＭＲＭエージェント等のコンピューティングデバイス上の別のアプリケーション、サービスまたは処理により管理されたブラウザが閉じられたおよび／または閉じるようにされたとき等）に応じておよび／または別様に基づいてデータをセキュリティ保護ドキュメントコンテナから選択的にワイプしてもよい。

【０１９４】

実施形態によっては、データは、１つ以上のポリシーに基づいてセキュリティ保護ドキュメントコンテナから選択的にワイプされてもよい。例えば、コンピューティングデバイスは、例によっては、１つ以上のモバイルデバイス管理ポリシーに基づいてデータをセキュリティ保護ドキュメントコンテナから選択的にワイプしてもよい。例えば、１つ以上のモバイルデバイス管理ポリシーは、特定のタイプのデータがセキュリティ保護ドキュメントコンテナから選択的にワイプされるべき特定の状況を定義してもよく、コンピューティングデバイスおよび／またはコンピューティングデバイス上で実行中のＭＲＭエージェントは、デバイス状態情報に基づいてこれらの状況を検出し、引き続いてポリシーに従ってセキュリティ保護ドキュメントコンテナからデータをワイプしてもよい。

【０１９５】

例えば、デバイス状態情報（これは例えば、コンピューティングデバイス上に存在する１つ以上のアプリケーションを特定する情報、コンピューティングデバイスにより使用される１つ以上のネットワーク接続を特定する情報および／またはコンピューティングデバイスの現在位置を特定する情報を含んでもよい）に基づいて、コンピューティングデバイスおよび／またはコンピューティングデバイス上で実行中のＭＲＭエージェントは、（例

えば、ステップ９１５において）管理されたブラウザを使用して１つ以上の企業リソースから取得され、引き続いて（例えば、ステップ９２０において）セキュリティ保護ドキュメントコンテナに記憶された企業データをセキュリティ保護ドキュメントコンテナから選択的にワイプしてもよい。

【０１９６】

実施形態によっては、データは、管理されたブラウザが管理モードで開かれるときに管理されたブラウザに適用される１つ以上のポリシーに基づいてセキュリティ保護ドキュメントコンテナから選択的にワイプされてもよい。例えば、コンピューティングデバイスは、例によっては、管理モードにおいて管理されたブラウザに適用される１つ以上のポリシーに基づいてセキュリティ保護ドキュメントコンテナからデータを選択的にワイプしてもよく、少なくとも１つのこのようなポリシーは、特定のデータ（これは例えば、管理されたブラウザを使用して取得されていてもよい）がセキュリティ保護ドキュメントコンテナから選択的に削除されるべき特定の状況を定義してもよい。さらに、これらの特定の状況は、コンピューティングデバイスおよび／またはコンピューティングデバイス上で実行中のＭＲＭエージェントにより、前記において検討された例でのようにデバイス状態情報に基づいて検出されてもよい。

【０１９７】

図１０は、本発明で検討される１つ以上の例示的態様に従って、ＳＳＯクレデンシャルに基づいて企業データを取得し、管理されたブラウザを介してデータへのアクセスを提供する方法を示すフローチャートである。１つ以上の実施形態において、図１０に示す方法および／またはその１つ以上のステップは、コンピューティングデバイス（例えば、ジェネリックコンピューティングデバイス２０１）により実行されてもよい。他の実施形態において、図１０に示す方法および／またはその１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具体化されてもよい。

【０１９８】

図１０に見られるように、この方法は、管理されたブラウザがロードされるステップ１００５で開始する。例えば、ステップ１００５において、コンピューティングデバイス（例えば、ラップトップコンピュータ、タブレットコンピュータ、スマートフォンまたは他のタイプのモバイルデバイス等のモバイルコンピューティングデバイス）は、ステップ５０５（前記において検討された）においてこのような管理されたブラウザがロードされる方法と同様に、管理されたブラウザをロードしてもよい。管理されたブラウザは、例えば、管理されたブラウザに１つ以上のポリシーが適用される少なくとも１つの管理モードを提供するよう構成されてもよく、１つ以上のポリシーは、例えば、前記において検討されたように、管理されたブラウザの１つ以上の機能を制限するよう構成されてもよい。さらに、管理されたブラウザは、実施形態によっては、少なくとも１つの企業リソースから取得されたデータのセキュリティ保護ブラウジングおよびキャッシングを提供するよう構成されてもよい。

【０１９９】

ステップ１０１０において、少なくとも１つのユーザアカウントに関するＳＳＯクレデンシャルが受信される。例えば、ステップ１０１０において、コンピューティングデバイスは、ＳＳＯクレデンシャルを受信してもよく、ＳＳＯクレデンシャルは、コンピューティングデバイスの特定のユーザおよび／または特定のユーザアカウント（これは例えば、コンピューティングデバイスおよび／または企業リソースならびに／あるいは他のネットワークリソース等の他のリソースに対するアクセスおよび／または使用において利用されてもよい）にリンクおよび／または別様に関連づけられてもよい。１つ以上の配置において、ＳＳＯクレデンシャルは、少なくとも２つの異なる企業リソース（様々な企業ウェブサイト、データベース、サーバ、他のリソース等）でのアクセスにおいて使用されるよう構成される認証クレデンシャルであってもよい。

【０２００】

さらに／あるいは、ＳＳＯクレデンシャルは、ユーザが、コンピューティングデバイス上のユーザアカウントにログインする、コンピューティングデバイス上のアプリケーションにログインする、コンピューティングデバイスを介してアクセス中のウェブサイトにログインする、コンピューティングデバイス上に存在する認証プロンプトと相互作用する、および／または、他の方法のときに、受信されてもよい。例によっては、ＳＳＯクレデンシャルは、例えば、１つ以上の企業リソースおよび／または他のリソースのアクセスへの要求または試行、または管理されたブラウザを使用する情報と関連して、管理されたブラウザを介して受信されてもよい。

【０２０１】

ステップ１０１５において、１つ以上の企業リソースからの企業データは、ＳＳＯクレデンシャルに基づいて取得される。例えば、ステップ１０１５において、コンピューティングデバイスは、ステップ１０１０において受信されたＳＳＯクレデンシャルを使用して、１つ以上の企業リソースへの接続、要求および引き続いて１つ以上の企業リソースから情報を受信および／または別様に取得してもよい。例によっては、ＳＳＯクレデンシャルは、例えば、企業リソースでの認証、企業リソースからの権利制御情報の要求および／または企業リソースからの企業データの別様の受信において使用されてもよい。例えば、１つ以上の企業リソースからの企業データの取得において、コンピューティングデバイスは、特定の企業リソースへの接続を開始してもよく、これは管理されたブラウザに認証情報を提供するようチャレンジしてもよい。チャレンジに応じて、管理されたブラウザは、企業リソースで認証するおよび／または企業リソースから情報を取得するためにＳＳＯクレデンシャル（例えば、ステップ１０１０において受信されたような）を企業リソースに提供してもよい。

【０２０２】

ステップ１０２０において、取得された企業データへのアクセスは、管理されたブラウザを介して提供されてもよい。例えば、ステップ１０２０において、コンピューティングデバイスは、管理されたブラウザを介してステップ１０１５において取得された企業データへのアクセスを提供してもよい。管理されたブラウザを介して取得された企業データへのアクセスの提供において、コンピューティングデバイスは、例えば、企業データが閲覧され、エディットされおよび／または別様にアクセスされることを許可するよう構成された１つ以上のユーザインタフェースを、管理されたブラウザに表示および／または別様に提示させてもよい。例えば、ステップ９２０において、コンピューティングデバイスは、コンピューティングデバイスのユーザが、取得された企業データをブラウズ、エディット、削除、および／または、取得された企業データに別様に相互作用および／またはアクセスすることを許可する１つ以上のユーザインタフェースを、管理されたブラウザに表示および／または別様に提示させてもよい。

【０２０３】

実施形態によっては、ＳＳＯクレデンシャルに基づいた１つ以上の企業リソースからの企業データの取得において、コンピューティングデバイスおよび／またはコンピューティングデバイス上で実行中の管理されたブラウザは、１つ以上のポリシーおよび／またはデバイス状態情報に依存して、ユーザを巻き込むことなくＳＳＯクレデンシャルを使用して、１つ以上の認証チャレンジ（これは例えば、１つ以上の企業リソースにより提示されてもよい）に応答してもよい。例えば、このような認証チャレンジは、１つ以上のポリシーおよび／またはデバイス状態情報に基づいてＳＳＯクレデンシャルを使用して、管理されたブラウザおよび／またはコンピューティングデバイスにより自動的にアドレスされてもよい。さらに、このように自動的にアドレスされてもよい特定の認証チャレンジおよび／または認証チャレンジのタイプは、１つ以上のポリシーおよび／またはデバイスの現在のコンテキスト（これは例えば、前記において検討された実施例でのように、デバイス状態情報により示されてもよい）に依存して変更してもよい。

【０２０４】

このように、１つ以上の実施形態において、ＳＳＯクレデンシャルに基づいた１つ以上

の企業リソースからの企業データの取得（例えば、ステップ１０１５において）は、１つ以上の企業リソースのうちの少なくとも１つの企業リソースから認証チャレンジを受信することと、１つ以上のポリシーのうちの少なくとも１つのポリシーに基づいて、認証チャレンジに応じて少なくとも１つの企業リソースへとＳＳＯクレデンシャルを提供すべきかどうかを判定することと、認証チャレンジに応じた少なくとも１つの企業リソースへのＳＳＯクレデンシャルの提供の判定に基づいて、ＳＳＯクレデンシャルを少なくとも１つの企業リソースへと提供することとを含んでもよい。例えば、ＳＳＯクレデンシャルを使用した１つ以上の企業リソースからの企業データの取得（例えば、ステップ１０１５において）において、コンピューティングデバイスおよび／またはコンピューティングデバイス上で実行中の管理されたブラウザは、（例えば、管理されたブラウザがアクセスを試行している）企業リソースから認証チャレンジを受信してもよい。このような認証チャレンジは通常、例えば、対応するリソースにアクセスするために１つ以上の認証クレデンシャルを提供することをユーザに要求する。

【０２０５】

認証チャレンジの受信後、コンピューティングデバイスおよび／またはコンピューティングデバイス上で実行中の管理されたブラウザは、１つ以上のポリシーに基づいて、認証チャレンジに応答するために企業リソースへのＳＳＯクレデンシャルの提供を行なうべきかどうかを判定してもよい。例えば、コンピューティングデバイスおよび／または管理されたブラウザは、ＳＳＯクレデンシャルを使用して管理されたブラウザがこのような認証チャレンジに自動的に応答することができる特定の状況を定義する１つ以上のポリシー上で、このような決定を行なってもよい。さらに、コンピューティングデバイスおよび／または管理されたブラウザは、このようなデバイス状態情報が前記において検討された例で評価されてもよい方法と同様に、デバイス状態情報に基づいてこれらの状況を評価してもよい。

【０２０６】

コンピューティングデバイスおよび／または管理されたブラウザが、１つ以上のポリシーおよび／またはデバイス状態情報に鑑みて、認証チャレンジに応答するために企業リソースにＳＳＯクレデンシャルが提供されることができると判定すると、コンピューティングデバイスおよび／または管理されたブラウザは、ＳＳＯクレデンシャルを企業リソースに提供してもよい。例えば、コンピューティングデバイスおよび／または管理されたブラウザは、認証チャレンジに自動的に応答するためにＳＳＯクレデンシャル（これは例えば、ステップ１０１０において受信されていてもよい）を企業リソースに送信してもよく、一方、コンピューティングデバイスおよび／または管理されたブラウザが、企業リソースからのおよび／または企業リソースにより記憶された情報にアクセスできるようにしてもよい。

【０２０７】

さらに、コンピューティングデバイスおよび／または管理されたブラウザは、ユーザを巻き込むことなくこのようにＳＳＯクレデンシャルを送信してもよい。例えば、コンピューティングデバイスおよび／または管理されたブラウザは、ユーザに任意の認証クレデンシャルの提供を促すことなく、ならびに／もしくは、ユーザにＳＳＯクレデンシャルが企業リソースに提供中であることを通知することさえなく、ＳＳＯクレデンシャルを送信してもよい。あるいは、コンピューティングデバイスおよび／または管理されたブラウザが、１つ以上のポリシーおよび／またはデバイス状態情報に鑑みて、認証チャレンジに応答するために企業リソースにＳＳＯクレデンシャルが提供されることができないと判定すると、コンピューティングデバイスおよび／または管理されたブラウザはそして、ユーザに１つ以上の認証クレデンシャル（これは例えば、そして認証チャレンジに応じてコンピューティングデバイスおよび／または管理されたブラウザにより使用されてもよい）の提供を促してもよい。このように、１つ以上の実施形態において、認証チャレンジへの応答で少なくとも１つの企業リソースへとＳＳＯクレデンシャルが提供されないとの判定に基づいて、コンピューティングデバイスおよび／またはコンピューティングデバイス上で実行

中の管理されたブラウザは、コンピューティングデバイスのユーザから少なくとも１つの認証クレデンシャルを受信するよう構成された認証プロンプトを生成してもよい。

【０２０８】

実施形態によっては、管理されたブラウザを介して取得された企業データへのアクセスの提供は、ＳＳＯクレデンシャルに基づいて１つ以上のポリシーを強制することを含んでもよい。例えば、ＳＳＯクレデンシャルに基づいて取得された企業データへのアクセスの提供および／またはポリシーの強制において、コンピューティングデバイスは、（例えば、ＳＳＯクレデンシャルに基づいてポリシーサーバおよび／または他の企業リソースから１つ以上のポリシーをダウンロード、受信、および／または別様に取得することにより）ＳＳＯクレデンシャルに基づいて１つ以上のポリシーを取得し、（例えば、ＳＳＯクレデンシャルに関してもよいアイデンティティ情報に鑑みてコンピューティングデバイスの現在のユーザに適用可能および／または適切なポリシーを選択的にアクティブ化、非アクティブ化および／または強制することにより）ＳＳＯクレデンシャルに基づいて適用可能なポリシーを選択し、および／または、（例えば、ＳＳＯクレデンシャル、１つ以上のポリシーおよび／またはデバイス状態情報に鑑みてユーザのアイデンティティおよび／または役割に適用可能ならびに／もしくは適切な管理されたブラウザ上の挙動制限を強制することにより）ポリシーに従って管理されたブラウザ上に１つ以上の挙動制限を課してもよい。

【０２０９】

ＳＳＯクレデンシャルに基づいて１つ以上のポリシーが強制される実施形態によっては、１つ以上のポリシーは、管理されたブラウザの１つ以上の機能を制限するよう構成されてもよい。例えば、１つ以上のポリシーは、管理されたブラウザの特定の機能が特定のユーザについて選択的に無効化されるべき特定の状況を定義してもよく、コンピューティングデバイスは、（例えば、デバイス状態情報に基づいて）これらの状況を検出および／または別様に特定してもよく、引き続いて１つ以上のポリシーに従っておよびステップ１０１０にて受信されたＳＳＯクレデンシャルに基づいて機能を無効化してもよい。前記において検討されたように、例えばポリシーにより制限されてもよい管理されたブラウザの機能の実施例によっては、カットアンドペースト機能、インスタントメッセージング機能、およびビデオチャット機能が含まれる。さらに、これらの機能は、例によっては限定されてもよい機能の実施例としてここに列挙されるが、他の機能が同様に他の例において限定されてもよい。

【０２１０】

ＳＳＯクレデンシャルに基づいて１つ以上のポリシーが強制される実施形態によっては、１つ以上のポリシーが、取得された企業データへのアクセスを制限するよう構成されてもよい。例えば、１つ以上のポリシーは、企業データ（例えば、ステップ１０１５において取得された企業データ）が特定の方法でのみアクセスおよび／または使用されることができる特定の状況を定義してもよく、コンピューティングデバイスは、（例えば、デバイス状態情報に基づいて）これらの状況を検出および／または別様に特定してもよく、引き続いてデータが１つ以上のポリシーに従っておよびステップ１０１０にて受信されたＳＳＯクレデンシャルに基づいてアクセスおよび／または使用されることができる方法を制限および／または別様に制御してもよい。例えば、１つ以上のポリシーのうちの少なくとも１つのポリシーが、（例えば、管理されたブラウザから別のアプリケーションへと）取得された企業データがコピーアンドペーストされることができる状況を制限するよう構成されてもよい。別の実施例として、１つ以上のポリシーのうちの少なくとも１つのポリシーが、（例えば、管理されたブラウザによりおよび／またはコンピューティングデバイスにより）取得された企業データがセーブまたはプリントされることができる状況を制限するよう構成されてもよい。

【０２１１】

ＳＳＯクレデンシャルに基づいて１つ以上のポリシーが強制される実施形態によっては、１つ以上のポリシーのうちの少なくとも１つのポリシーの強制は、デバイス状態情報に

依存してもよい。例えば、（例えば、１つ以上のポリシーにより課されるような）管理されたブラウザの機能上の制限および／または（例えば、さらに／あるいは１つ以上のポリシーにより課されるような）企業データが管理されたブラウザによりアクセスおよび／または使用されてもよい方法上の制限は、コンピューティングデバイスの現在の状態を示す状態情報に依存してもよい。このような状態情報は、例えば、前記において検討された実施例のように、コンピューティングデバイス上で実行するよう構成されたＭＲＭエージェント（例えば、バックグラウンドアプリケーション、サービスまたは処理として）により収集および／または監視されてもよい。例えば、ＭＲＭエージェントは、デバイス上で記憶および／または実行中のオペレーティングシステムおよび／またはアプリケーションを示す状態情報、デバイスにより利用可能および／または使用中のネットワーク接続を示す状態情報、および／または、デバイスが位置するおよび／または使用中の現在位置を示す状態情報等のデバイスレベル状態情報を収集および／または監視するよう構成されてもよい。さらに、この状態情報のいずれかおよび／または全てが、ＳＳＯクレデンシャル（これは例えば、前記において検討されたように、ステップ１０１０において受信されてもよい）と組み合わせて、前記において検討されたポリシー等の、ポリシーの管理されたブラウザ上への適用および／または強制において（例えば、コンピューティングデバイスによりおよび／または管理されたブラウザにより）使用されてもよい。

【０２１２】

図１１は、本発明で検討される１つ以上の例示的態様に従って、管理されたブラウザを介してアプリケーションストアへのアクセスを提供する方法を示すフローチャートである。１つ以上の実施形態において、図１１に示す方法および／またはその１つ以上のステップは、コンピューティングデバイス（例えば、ジェネリックコンピューティングデバイス２０１）により実行されてもよい。他の実施形態において、図１１に示す方法および／またはその１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具体化されてもよい。

【０２１３】

図１１に見られるように、この方法は、管理されたブラウザがロードされるステップ１１０５で開始する。例えば、ステップ１１０５において、コンピューティングデバイス（例えば、ラップトップコンピュータ、タブレットコンピュータ、スマートフォンまたは他のタイプのモバイルデバイス等のモバイルコンピューティングデバイス）は、ステップ５０５（前記において検討された）においてこのような管理されたブラウザがロードされる方法と同様に、管理されたブラウザをロードしてもよい。管理されたブラウザは、例えば、管理されたブラウザに１つ以上のポリシーが適用される少なくとも１つの管理モードを提供するよう構成されてもよく、１つ以上のポリシーは、例えば、前記において検討されたように、管理されたブラウザの１つ以上の機能を制限するよう構成されてもよい。さらに、管理されたブラウザは、実施形態によっては、少なくとも１つの企業リソースから取得されたデータのセキュリティ保護ブラウジングおよびキャッシングを提供するよう構成されてもよい。

【０２１４】

ステップ１１１０において、管理されたブラウザを介したアプリケーションストアのアクセスへの要求が受信される。例えば、ステップ１１１０において、コンピューティングデバイスは、管理されたブラウザを介してアプリケーションストアにアクセスするための要求を受信してもよい。このような要求は、例えば、管理されたブラウザを介してコンピューティングデバイスにより受信されるユーザ入力に基づいてもおよび／または対応してもよい（例えば、管理されたブラウザを使用したアプリケーションストアへのリンクのユーザ選択および／または別様のアクセス要求に基づいて）。例えば、管理されたブラウザは、アイコンまたはツールバーの選択時に管理されたブラウザ内にアプリケーションストアが表示されるよう構成されてもよいアイコンまたはツールバーを含んでもよい。さらに／あるいは、管理されたブラウザに適用される特定のポリシーは、コンテキスト（例えば、ブラウザの状態および／またはデバイス上で実行中であってもよい様々な他のプログラ

ム）、ユーザアカウント情報および／またはユーザ役割情報等の１つ以上のファクターに基づいて動的にブラウザを正しいアプリケーションストアにダイレクトしてもよい。

【０２１５】

１つ以上の配置において、アプリケーションストア（例えば、ステップ１１１０においてアクセスが要求される）は、企業アプリケーションを１つ以上のモバイルコンピューティングデバイスに提供するよう構成される企業アプリケーションストアであってもよい。企業アプリケーションを様々なデバイスに提供するよう構成されることに加えて、企業アプリケーションストアはまた、１つ以上のモバイルデバイス管理ポリシーおよび／またはポリシー更新を様々なデバイスに提供するよう構成されてもよい。例えば、アプリケーションストアは、１つ以上のモバイルコンピューティングデバイスおよび／または他のユーザデバイスによりダウンロードされることができ、引き続いてこのようなユーザデバイス上でネイティブに実行されることができる１つ以上のアプリケーションを提供するよう構成されてもよい。

【０２１６】

アプリケーションストアはまた、１つ以上のウェブアプリケーションおよび／または１つ以上のヴァーチャル化アプリケーションへのアクセスに使用されることができる情報を提供してもよい。例えば、アプリケーションストアは、このようなウェブアプリケーションまたはヴァーチャル化アプリケーションを実行中および／または提供するよう別様に構成されたサーバの位置決定および／またはそれへの接続を行なうために、管理されたブラウザによって使用されることができるポインタおよび／または位置情報を提供してもよい。例によっては、ポインタおよび／または位置情報はまた、ウェブアプリケーションまたはヴァーチャル化アプリケーションを実行するためにコンピューティングデバイス上の異なるアプリケーションへと管理されたブラウザにより渡されてもよい。

【０２１７】

ステップ１１１５において、アプリケーションストアからの企業データは、要求に基づいて取得される。例えば、ステップ１１１５において、コンピューティングデバイスは、ステップ１１１０において受信された要求に基づいて、アプリケーションストアに接続、要求、引き続いてアプリケーションストアから情報を受信および／または別様に取得してもよい。

【０２１８】

ステップ１１２０において、取得された企業データの少なくとも一部は、管理されたブラウザを介して提示される。例えば、ステップ１１２０において、コンピューティングデバイスは、管理されたブラウザを介して、ステップ１１１５においてアプリケーションストアから取得された企業データの少なくとも一部を提示してもよい。管理されたブラウザを介した企業データの提示において、コンピューティングデバイスは、例えば、アプリケーションストアから取得された企業データが閲覧され、相互作用されおよび／または別様にアクセスされることを許可するよう構成された１つ以上のユーザインタフェースを、管理されたブラウザに表示および／または別様に提示させてもよい。例えば、ステップ１１２０において、コンピューティングデバイスは、ユーザが、アプリケーションストアにおいて利用可能なアプリケーションおよび／または他のコンテンツを閲覧し、このようなアプリケーションおよび／または他のコンテンツを選択および／またはダウンロードし、および／または別様にアプリケーションストアデータと相互作用することを許可する１つ以上のユーザインタフェースを、管理されたブラウザに表示および／または別様に提示させてもよい。

【０２１９】

実施形態によっては、取得された企業データの少なくとも一部の提示は、管理されたブラウザを介し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るようにすることを含んでもよい。例えば、アプリケーションストアから取得された企業データの少なくとも一部の提示において、コンピューティングデバイスは、管理されたブラウザを表示してもよく、および／または管理されたブラウザにアプリケーションダウンロードインタフ

ェースを表示ならびに／あるいは別様に提示させてもよい。アプリケーションダウンロードインタフェースは、例えば、アプリケーションストアを介したダウンロードに利用可能であってもよい、および／または、利用可能なアプリケーションをダウンロードするために選択可能な１つ以上のリンクならびに／もしくは他の制御を含んでもよい、１つ以上のアプリケーションについての情報を含んでもよい。

【０２２０】

実施形態によっては、取得された企業データの少なくとも一部の提示は、アプリケーションストアから少なくとも１つのアプリケーションへのアクセスを提供することを含んでもよく、少なくとも１つのアプリケーションは管理されたブラウザを介してのみアクセス可能である。例えば、アプリケーションストアから取得された企業データの少なくとも一部の提示において、コンピューティングデバイスは、アプリケーションストアが管理されたブラウザで（例えば、従来のおよび／または管理されていないブラウザではなく）アクセスされるときのみ、（アクセス、ダウンロード等に）利用可能であるアプリケーションストア内のアプリケーションへのアクセスを提供してもよい。例によっては、特定のアプリケーション（これは例えば、アプリケーションストアにて利用可能および／またはアプリケーションストアから取得されていてもよい）に関する特定のタイプの情報は、ユーザデバイスが管理されたブラウザを介してアプリケーションストアにアクセス中であるときのみユーザデバイスに提供されるかもしれない。例えば、企業テンプレート、特定のデータセット、共同者レビュー、アプリケーションが使用されている特定のプロジェクトについての情報、アプリケーションをダウンロードしている他のユーザおよび／または従業員の列挙、および／または、特定のアプリケーションに関する他のタイプの情報へのアクセスが、管理されたブラウザを介してのみ提供されてもよい。この情報は、例えば、企業に特有であると考えられ、従って、情報へのアクセスは、管理されたブラウザの使用を通じて制限されてもよい。

【０２２１】

実施形態によっては、取得された企業データの少なくとも一部の提示は、少なくとも１つのアプリケーションのヴァーチャル化セッションが、管理されたブラウザを介して提供されるようにすることを含んでもよい。例えば、アプリケーションストアから取得された企業データの少なくとも一部の提示において、コンピューティングデバイスは、アプリケーションのヴァーチャル化セッションが管理されたブラウザを介して提供されるようにしてもよい。例えば、コンピューティングデバイスは、管理されたブラウザがアプリケーションの１つ以上のヴァーチャル化ユーザインタフェースを表示および／または別様に提供するようにしてもよく、これはアプリケーションストアならびに／もしくは１つ以上の企業リソースから取得および／またはアプリケーションストアならびに／もしくは１つ以上の企業リソースにより遠隔実行されてもよい。

【０２２２】

実施形態によっては、管理されたブラウザは、デバイス状態情報を監視およびデバイス状態情報に基づいて１つ以上のポリシーを強制するようにさらに構成されてもよい。例えば、アプリケーションストアから取得された企業データを提示するよう構成されることに加えて、管理されたブラウザは、デバイス状態情報を監視し、１つ以上のポリシーを強制するようさらに構成されてもよい（例えば、管理されたブラウザ自身上でおよび／またはデバイス上で実行中であってもよい１つ以上の他のアプリケーション上で）。例えば、管理されたブラウザは、管理されたブラウザがコンピューティングデバイス上で、企業リソースにセキュリティ保護された状態でアクセスできるブラウザとしてだけでなく、デバイス状態情報を監視し、状態情報に基づいてデバイスの様々なアプリケーションおよび／または他の機能にポリシーを強制することができるモバイルリソース管理エージェントとしても動作してもよいよう、前記において検討されたＭＲＭエージェントのように動作するおよび／またはそれと同様の機能を提供するよう構成されてもよい。

【０２２３】

図１２は、本発明で検討される１つ以上の例示的態様に従って、管理されたブラウザで

企業データを取得および制御する方法を示すフローチャートである。１つ以上の実施形態において、図１２に示す方法および／またはその１つ以上のステップは、コンピューティングデバイス（例えば、ジェネリックコンピューティングデバイス２０１）により実行される。他の実施形態において、図１２に示す方法および／またはその１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具体化されてもよい。

【０２２４】

図１２に見られるように、この方法は、管理されたブラウザがロードされるステップ１２０５で開始される。例えば、ステップ１２０５において、コンピューティングデバイス（例えば、ラップトップコンピュータ、タブレットコンピュータ、スマートフォンまたは他のタイプのモバイルデバイス等のモバイルコンピューティングデバイス）は、ステップ５０５（前記において検討された）においてこのような管理されたブラウザがロードされる方法と同様に、管理されたブラウザをロードしてもよい。管理されたブラウザは、例えば、管理されたブラウザに１つ以上のポリシーが適用される少なくとも１つの管理モードを提供するよう構成されてもよく、１つ以上のポリシーは、例えば、前記において検討されたように、管理されたブラウザの１つ以上の機能を制限するよう構成されてもよい。さらに、管理されたブラウザは、実施形態によっては、少なくとも１つの企業リソースから取得されたデータのセキュリティ保護ブラウジングおよびキャッシングを提供するよう構成されてもよい。

【０２２５】

ステップ１２１０において、管理されたブラウザを介した１つ以上の企業リソースのアクセスへの要求が受信されてもよい。例えば、ステップ１２１０において、コンピューティングデバイスは、管理されたブラウザを介した１つ以上の企業リソースのアクセスへの要求を受信してもよい。このような要求は、例えば、管理されたブラウザを介してコンピューティングデバイスにより受信されたユーザ入力に基づいておよび／または対応してもよい（例えば、管理されたブラウザを使用したネットワークリソースへのリンクのユーザ選択および／または別様のアクセス要求に基づいて）。

【０２２６】

ステップ１２１５において、１つ以上の企業リソースからの企業データは、要求に基づいて取得されてもよい。例えば、ステップ１２１５において、コンピューティングデバイスは、ステップ１２１０において受信された要求に基づいて、１つ以上の企業リソースに接続、要求、および引き続いて、１つ以上の企業リソースから情報を受信および／または別様に取得してもよい。

【０２２７】

ステップ１２２０において、取得された企業データは、１つ以上のポリシーに基づいて制御されてもよい。例えば、ステップ１２２０において、コンピューティングデバイスは、１つ以上のモバイルデバイス管理ポリシーを使用して、ステップ１２１５において取得された企業データを制御してもよい。１つ以上のモバイルデバイス管理ポリシーは、例えば、特定の機能（例えば、管理されたブラウザの特定の機能、取得された企業データを必要とする特定の機能等）が、許可、禁止および／または別様に制限されてもよい特定の状況を定義してもよい。さらに／あるいは、コンピューティングデバイスは、デバイス状態情報に基づいてこれらの状況を評価し、引き続いて１つ以上のポリシーに従って企業データを制御するよう構成されてもよい。例によっては、取得された企業データは、管理モードにおいて管理されたブラウザに適用されてもよいポリシーの同じセット（例えば、ポリシーの第１のセット）を使用して制御されてもよい。他の例において、取得された企業データは、管理モードにおいて管理されたブラウザに適用されるのとは異なるポリシーのセット（例えば、ポリシーの第１のセットとは異なるポリシーの第２のセット）を使用して制御されてもよい。

【０２２８】

実施形態によっては、（例えば、ステップ１２２０において）企業データの制御におい

て使用されるポリシーは、ヘルスケア、金融、法務、技術等の１つ以上の特定の産業に特有であってもおよび／またはグループ化されてもよい。このようにポリシーをグループ化および／または別様に実装することにより、産業特有のポリシーの団結したグループが、産業特有のブラウザを生成するために管理されたブラウザに適用されてもよい。例えば、ヘルスケア関連ポリシーの団結したグループが、例えば、規制および／またはプライバシー事項を満たすためにポリシーが特定の機能をブロックするよう動作してもよい「ヘルスケアブラウザ」を生成するために管理されたブラウザに適用されてもよい。

【０２２９】

実施形態によっては、企業データの制御において（例えばステップ１２２０において）使用されるポリシーは、ロギング機能および／または他の監視機能が選択的に適用および／または実行されるのを許可するおよび／または生じさせる１つ以上のポリシーを含んでもよい。このようなロギング機能および／または他の監視機能は、管理されたブラウザにおよび／またはコンピューティングデバイス上で実行中の１つ以上の他のアプリケーションおよび／またはサービスに適用されてもよい。例えば、１つ以上のポリシーは、特定の期間、特定の位置で、および／またはデバイスの現在のコンテキストに基づいて、ネットワークトラフィックを監視および／または選択的にフィルタリングしてもよい。さらに／あるいは、１つ以上のポリシーは、ユーザの役割情報、パフォーマンス情報（これは例えば、デバイスパフォーマンスおよび／またはネットワークパフォーマンスを含んでもよい）および／または１つ以上の他のファクターに基づいて、ネットワークトラフィックを監視および／または選択的にフィルタリングしてもよい。

【０２３０】

実施形態によっては、取得された企業データの制御は、少なくとも１つのポリシーをコンピューティングデバイス上の少なくとも１つの他のアプリケーションに適用するよう構成されたモバイルリソース管理（ＭＲＭ）エージェント等の、モバイルリソース管理（ＭＲＭ）エージェントで管理されたブラウザを制御することを含んでもよい。例えば、（例えば、管理されたブラウザ上にポリシーを適用および／または強制することにより）管理されたブラウザを制御するよう構成されることに加えて、コンピューティングデバイス上で実行中であってもよいＭＲＭエージェントは、様々なモバイルデバイス管理ポリシーをコンピューティングデバイス上で記憶されたおよび／または実行中の他のアプリケーションへと適用するようさらに構成されてもよい。このようなＭＲＭエージェントは、例えば、クライアントエージェント４０４（前記において検討された）の１つ以上の態様を組み込んでもよい。

【０２３１】

実施形態によっては、１つ以上のポリシーのうちの少なくとも１つのポリシーは、デバイス状態情報に基づいて管理されたブラウザの１つ以上の機能を選択的に無効化するよう構成されてもよい。例によってはこのようなポリシーにより選択的に無効化されてもよい管理されたブラウザの機能のいくつかの実施例は、カットアンドペースト機能、インスタントメッセージング機能およびビデオチャット機能を含む。これらの機能は、例によっては選択的に無効化されてもよい機能の実施例としてここで列挙されるが、他の機能も同様に他の例において無効化されてもよい。さらに、１つ以上のポリシーの評価において使用されてもよいデバイス状態情報は、前記において検討された例でのように、コンピューティングデバイス上に存在する１つ以上のアプリケーションを特定する情報、コンピューティングデバイスにより使用される１つ以上のネットワーク接続を特定する情報および／またはコンピューティングデバイスの現在位置を特定する情報を含んでもよい。

【０２３２】

実施形態によっては、１つ以上のポリシーに基づいた取得された企業データの制御は、取得された企業データへのアクセスを制御することを含んでもよい。さらに、取得された企業データへのアクセスの制御は、例によっては、取得された企業データの使用を制御することを含んでもよい。

【０２３３】

例えば、１つ以上のポリシーが、企業データ（例えば、ステップ１２１５において管理されたブラウザを使用して取得された企業データ）が特定の方法でのみアクセスおよび／または使用されることができる特定の状況を定義してもよく、コンピューティングデバイスが、（例えば、デバイス状態情報に基づいて）これらの状況を検出および／または別様に特定し、引き続いて１つ以上のポリシーに従ってデータがアクセスおよび／または使用されることができる方法を制限および／または別様に制御してもよい。例えば、１つ以上のポリシーのうちの少なくとも１つのポリシーが、取得された企業データが（例えば、管理されたブラウザから別のアプリケーションへと）コピーアンドペーストされることができる状況を制限するよう構成されてもよい。別の例として、１つ以上のポリシーのうちの少なくとも１つのポリシーが、取得された企業データが（例えば、管理されたブラウザによりおよび／またはコンピューティングデバイスにより）セーブまたはプリントされることができる状況を制限するよう構成されてもよい。

【０２３４】

実施形態によっては、管理されたブラウザは、ポリシー管理サーバからＭＲＭエージェントについての１つ以上のポリシー更新を受信するよう構成されてもよい。例えば、管理されたブラウザは、例によっては、１つ以上のポリシー更新（これは例えば、管理されたブラウザ、他のアプリケーションおよび／またはコンピューティングデバイスの他の態様に適用されるべき新たなおよび／または更新されたポリシーを含んでもよい）を受信してもよい。このようなポリシー更新は、例えば、ポリシー管理サーバから受信されてもよく、このようなポリシー更新の受信後に、管理されたブラウザは、ポリシー更新およびその関連情報をＭＲＭエージェント（これは例えば、適宜新たなおよび／または更新されたポリシーを受信および適用してもよい）に提供してもよい。

【０２３５】

実施形態によっては、取得された企業データの制御は、管理されたブラウザが非管理モードで動作中のときに取得された企業データへのアクセスを選択的にブロックすることを含んでもよい。例えば、１つ以上の企業リソースからの企業データの取得後に（例えば、ステップ１２１５において）、管理されたブラウザおよび／または管理されたブラウザを実行中のコンピューティングデバイスは、管理されたブラウザが（例えば、前記の実施例において検討したように、１つ以上のポリシーがブラウザに適用されないかもしれない）非管理モードで動作中のときに取得された企業データへのアクセスを選択的にブロックしてもよい。すなわち、管理されたブラウザおよび／または管理されたブラウザを実行中のコンピューティングデバイスは、コンピューティングデバイスのユーザが、管理されたブラウザが管理モードで実行中の間のみ、管理されたブラウザで取得された企業データにアクセスすることが可能であって、管理されたブラウザが管理モードで実行されていない間（例えば、管理されたブラウザが非管理モードで実行中のとき）は、管理されたブラウザを介して取得された企業データにアクセスすることが防止されてもよいよう構成されてもよい。

【０２３６】

図１３は、本発明で検討される１つ以上の例示的態様に従って、管理されたブラウザについて１つ以上のポリシーをアドミニストレーションする方法を示すフローチャートである。

【０２３７】

１つ以上の実施形態において、図１３に示す方法および／またはその１つ以上のステップは、コンピューティングデバイス（例えば、ジェネリックコンピューティングデバイス２０１）により実行されてもよい。他の実施形態において、図１３に示す方法および／またはその１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具体化されてもよい。

【０２３８】

図１３に見られるように、この方法は、１つ以上のユーザコンピューティングデバイス上の管理されたブラウザに適用されるべき少なくとも１つのポリシーが受信されるステッ

プ１３０５で開始する。例えば、このようなポリシーは、サーバコンピューティングデバイス（これは例えば、ジェネリックコンピューティングデバイス２０１の１つ以上の態様を組み込んでもよく、および／または、企業組織および／またはその様々なユーザについてのポリシー管理機能を提供するよう構成されてもよい）により受信されてもよい。さらに、ポリシーは、様々なユーザコンピューティングデバイス上の管理されたブラウザに適用されるべき１つ以上の新たなおよび／または更新されたポリシーを定義していてもよいアドミニストラティブユーザからおよび／またはこのようなユーザにより操作されているコンピューティングデバイスからサーバコンピューティングデバイスにより受信されてもよい。前記において検討された実施例でのように、管理されたブラウザは、例えば、管理されたブラウザに１つ以上のポリシーが適用される少なくとも１つの管理モードを提供するよう構成されてもよく、１つ以上のポリシーは、管理されたブラウザの１つ以上の機能を制限するよう構成されてもよい。さらに、管理されたブラウザは、実施形態によっては、少なくとも１つの企業リソースから取得されたデータのセキュリティ保護ブラウジングおよびキャッシングを提供するよう構成されてもよい。

【０２３９】

ステップ１３１０において、少なくとも１つのポリシー更新は、少なくとも１つのポリシーに基づいて１つ以上のユーザコンピューティングデバイスのうちの少なくとも１つのユーザコンピューティングデバイスに提供される。例えば、ステップ１３１５において、サーバコンピューティングデバイスは、ステップ１３０５において受信されたポリシーに基づいてポリシー更新をユーザコンピューティングデバイスに提供してもよい。ユーザコンピューティングデバイスへのポリシー更新の提供において、サーバコンピューティングデバイスは、例えば、ユーザコンピューティングデバイスに接続し、ステップ１３０５においてサーバコンピューティングデバイスにより受信されていてもよい新たなおよび／または更新されたポリシーについての情報を、ユーザコンピューティングデバイスにプッシュおよび／または別様に送信してもよい。

【０２４０】

１つ以上の配置において、少なくとも１つのポリシー更新は、少なくとも１つのユーザコンピューティングデバイスに、少なくとも１つの受信されたポリシーを少なくとも１つのユーザコンピューティングデバイス上の管理されたブラウザに適用させるよう構成されてもよい。例えば、ポリシー更新（これは例えば、ステップ１３１０においてサーバコンピューティングデバイスによりユーザコンピューティングデバイスに提供されてもよい）は、ユーザコンピューティングデバイスに、ユーザコンピューティングデバイス上の管理されたブラウザにポリシー（これは例えば、ステップ１３０５においてサーバコンピューティングデバイスにより受信されてもよい）を適用させるよう構成されてもよい。このような管理されたブラウザは、例えば、サーバコンピューティングデバイスから（例えば、ステップ１３１０において）ポリシー更新を受信するユーザコンピューティングデバイス上において、実行され、記憶されおよび／または別様に存在してもよい。

【０２４１】

配置によっては、ポリシー（これは例えば、サーバコンピューティングデバイスによりステップ１３０５において受信され、引き続いてステップ１３１０においてポリシー更新を介してユーザコンピューティングデバイスに提供および受信されてもよい）は、管理されたブラウザ上におよび／または管理されたブラウザを実行中のユーザコンピューティングデバイス上に強制されてもよい１つ以上の特定の規則を定義してもよい。このような規則は、例えば、デバイス状態情報（これは例えば、どのような他のアプリケーションが実行中か、ユーザコンピューティングデバイス上にインストールされているか、および／または別様に存在するか、ユーザコンピューティングデバイスがどこに位置するか、ユーザコンピューティングデバイスがどのようなネットワークに接続されているか等についての情報を含んでもよい）に関して定義および／またはデバイス状態情報に基づいて評価されてもよい特定の状況において強制されてもよい。

【０２４２】

実施形態によっては、少なくとも１つの受信されたポリシーは、１つ以上のコンテンツフィルタリング規則を含んでもよい。例えば、例によっては、サーバコンピューティングデバイスによりステップ１３０５において受信されたポリシーは、１つ以上のコンテンツフィルタリング規則を含んでもよい。このようなコンテンツフィルタリング規則は、例えば、特定の企業リソースを含んでもよい特定のネットワークリソースにアクセスする管理されたブラウザの能力を制御してもよい。例えば、コンテンツフィルタリング規則は、デバイス状態情報（これは例えば、前記において検討されたように、どのような他のアプリケーションが実行中か、ユーザコンピューティングデバイス上にインストールされているか、および／または別様に存在するか、ユーザコンピューティングデバイスがどこに位置するか、ユーザコンピューティングデバイスがどのようなネットワークに接続されているか等についての情報を含んでもよい）および／または他の特定の基準に基づいて管理されたブラウザによるコンテンツの特定のタイプへのアクセスを選択的にブロックおよび／または選択的に許可してもよい。

【０２４３】

実施形態によっては、少なくとも１つの受信されたポリシーは、１つ以上のキャッシング規則を含んでもよい。例えば、例によっては、サーバコンピューティングデバイスによりステップ１３０５において受信されたポリシーは、１つ以上のコンテンツキャッシング規則を含んでもよい。このようなコンテンツキャッシング規則は、例えば、１つ以上の企業リソースから受信された特定のタイプのコンテンツ、他のネットワークリソースから受信された特定のタイプのコンテンツ（例えば、ウェブコンテンツ、クッキー等）および／または他のタイプの情報を含んでもよい特定のタイプのコンテンツをキャッシュする管理されたブラウザの能力を制御してもよい。例えば、コンテンツキャッシング規則は、デバイス状態情報（これは例えば、前記において検討されたように、どのような他のアプリケーションが実行中か、ユーザコンピューティングデバイス上にインストールされているか、および／または別様に存在するか、ユーザコンピューティングデバイスがどこに位置するか、ユーザコンピューティングデバイスがどのようなネットワークに接続されているか等についての情報を含んでもよい）および／または他の特定の基準に基づいて、管理されたブラウザにより特定のタイプのコンテンツのキャッシングを選択的にブロックおよび／または選択的に許可してもよい。

【０２４４】

実施形態によっては、少なくとも１つの受信されたポリシーは、１つ以上のプラグイン規則を含んでもよい。例えば、例によっては、サーバコンピューティングデバイスによりステップ１３０５において受信されたポリシーは、１つ以上のプラグイン管理規則を含んでもよい。このようなプラグイン管理規則は、例えば、特定のプラグイン（これは例えば、様々なタイプのアプリケーション、エクステンション、アプレット、スクリプトおよび／または他のタイプのプラグインを含んでもよい）のアクセス、実行および／または別様の使用を行なう管理されたブラウザの能力を制御してもよい。例えば、プラグイン管理規則は、デバイス状態情報（これは例えば、前記において検討されたように、どのような他のアプリケーションが実行中か、ユーザコンピューティングデバイス上にインストールされているか、および／または別様に存在するか、ユーザコンピューティングデバイスがどこに位置するか、ユーザコンピューティングデバイスがどのようなネットワークに接続されているか等についての情報を含んでもよい）および／または他の特定の基準に基づいて、管理されたブラウザによる１つ以上の特定のプラグインのアクセス、実行ならびに／あるいは別様の使用を選択的に防止および／または選択的に有効化してもよい。

【０２４５】

実施形態によっては、少なくとも１つの受信されたポリシーは、１つ以上のクレデンシャル管理規則を含んでもよい。例えば、サーバコンピューティングデバイスによりステップ１３０５において受信されたポリシーは、１つ以上のクレデンシャル管理規則を含んでもよい。このようなクレデンシャル管理規則は、例えば、特定のクレデンシャルを使用する管理されたブラウザの能力を制御してもよく、特定のクレデンシャルは、例えば、１つ

以上のリソースへのアクセス時の１つ以上のＳＳＯクレデンシャルを含んでもよい。例えば、クレデンシャル管理規則は、デバイス状態情報（これは例えば、前記において検討されたように、どのような他のアプリケーションが実行中か、ユーザコンピューティングデバイス上にインストールされているか、および／または、別様に存在するか、ユーザコンピューティングデバイスがどこに位置するか、ユーザコンピューティングデバイスがどのようなネットワークに接続されているか等についての情報を含んでもよい）および／または他の特定の基準に基づいて、管理されたブラウザによる１つ以上の特定のクレデンシャルのアクセスおよび／または使用を選択的に防止および／または有効化してもよい。

【０２４６】

実施形態によっては、少なくとも１つの受信されたポリシーは、デバイス状態情報に基づいて少なくとも１つのユーザコンピューティングデバイスにより強制されるよう構成されてもよい。例えば、例によっては、サーバコンピューティングデバイスによりステップ１３０５において受信されたポリシーは、ユーザコンピューティングデバイスに関するデバイス状態情報に基づいてユーザコンピューティングデバイスにより強制されるよう構成されてもよい。このようなポリシーは、例えば、ユーザコンピューティングデバイスに関する状態情報に基づいて、１つ以上の特定の機能が実行され、および／または、１つ以上の他の特定の機能が実行されるのを防止されるようにしてもよい。

【０２４７】

前記において検討したように、このようなデバイス状態情報は、例えば、どのような他のアプリケーション（例えば、管理されたブラウザ以外で）が実行中か、ユーザコンピューティングデバイス上にインストールされているか、および／または別様に存在するかについての情報、ユーザコンピューティングデバイスがどこに位置するかについての情報、ユーザコンピューティングデバイスがどのようなネットワークに接続されているかについての情報および／または他の情報を含んでもよい。

【０２４８】

実施形態によっては、少なくとも１つの受信されたポリシーは、１つ以上の基準に基づいて管理されたブラウザに非管理モードに切り替わらせるよう構成される１つ以上の規則を含んでもよい。例えば、例によっては、サーバコンピューティングデバイスによりステップ１３０５において受信されたポリシーは、１つ以上の基準に基づいてユーザコンピューティングデバイス上の管理されたブラウザに管理モードから非管理モードに切り替わらせるよう構成される１つ以上の規則を含んでもよい。１つ以上の基準は、例えば、ユーザコンピューティングデバイスに関するデバイス状態情報に基づいておよび／またはこれを含んでもよい。前記において検討されたように、このような状態情報は、例えば、どのような他のアプリケーション（例えば、管理されたブラウザ以外で）が実行中か、ユーザコンピューティングデバイス上にインストールされているか、および／または別様に存在するかについての情報、ユーザコンピューティングデバイスがどこに位置するかについての情報、ユーザコンピューティングデバイスがどのようなネットワークに接続されているかについての情報および／または他の情報を含んでもよい。

【０２４９】

図１４は、本発明で検討される１つ以上の例示的態様に従って、管理されたブラウザを介してアプリケーションストアへのアクセスを提供する別の方法を示すフローチャートである。１つ以上の実施形態において、図１４に示す方法および／またはその１つ以上のステップは、コンピューティングデバイス（例えば、ジェネリックコンピューティングデバイス２０１）により実行されてもよい。他の実施形態において、図１４に示す方法および／またはその１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具体化されてもよい。

【０２５０】

図１４に見られるように、この方法は、アプリケーションストアの第１の部分にアクセスするために、アプリケーションストアにおいて、ユーザコンピューティングデバイス上の管理されたブラウザからの要求が受信されるステップ１４０５で開始する。例えば、ス

テップ１４０５において、コンピューティングデバイスは、アプリケーションストアを提供し、および／または、企業アプリケーションストアを提供するよう構成されたサーバコンピューティングデバイス等のように、アプリケーションストアとして構成されてもよく、特定のアプリケーションおよび／または特定のタイプのアプリケーションに関するアプリケーションストアの部分等の、アプリケーションストアの特定の部分にアクセスするために、ユーザコンピューティングデバイス上の管理されたブラウザからの要求を受信してもよい。

【０２５１】

ステップ１４１０において、アプリケーションストアにより、管理されたブラウザが、管理されたブラウザに１つ以上のポリシーが適用される管理モードで動作中かどうかが判定され、１つ以上のポリシーは、管理されたブラウザの少なくとも１つの機能を制限するよう構成されている。例えば、ステップ１４１０において、コンピューティングデバイスは、ユーザコンピューティングデバイス上で実行中の管理されたブラウザが管理モードで実行中かどうかを判定してもよい。例えば、ユーザコンピューティングデバイス上の管理されたブラウザは、例えば、１つ以上のポリシーが管理されたブラウザに適用される、前記の例において検討された、管理されたブラウザの管理モードと同様の、管理モードを提供および／または有してもよい。さらに、アプリケーションストアは、管理されたブラウザでその現在の動作モードを判定するために情報（これは例えば、ユーザコンピューティングデバイスに関するデバイス状態情報を含んでもよい）をインタロゲートおよび／または別様に交換することにより、管理されたブラウザが管理モードで動作中かどうかを判定してもよい。

【０２５２】

ステップ１４１０において、管理されたブラウザが管理モードで動作中であると判定されると、ステップ１４１５において、アプリケーションストアは、管理されたブラウザがアプリケーションストアの第１の部分にアクセスするのを許可する。例えば、ステップ１４１５において、コンピューティングデバイスは、管理されたブラウザにアプリケーションストアの第１の部分へのアクセスを提供してもよい（これは例えば、管理されたブラウザに、特定のアプリケーションおよび／または特定のタイプのアプリケーションに関する情報等の、アプリケーションの第１の部分に関する情報を提供することを含んでもよい）。このように、ユーザコンピューティングデバイス上の管理されたブラウザは、管理モードで実行中の間、この実施例におけるアプリケーションストアの第１の部分等のアプリケーションストアの特定の部分にアクセスすることができ、下記に示されるように、管理モードで実行中でない場合（例えば、ブラウザが非管理モードで実行中のとき）は、管理されたブラウザは、アプリケーションストアの特定の部分にアクセスすることができないかもしれない。

【０２５３】

このように、ステップ１４１０において、管理されたブラウザが管理モードで動作中ではないと判定されると、ステップ１４２０において、アプリケーションストアは、管理されたブラウザがアプリケーションストアの第１の部分にアクセスするのを防止する。例えば、ステップ１４２０において、コンピューティングデバイスは、管理されたブラウザ（および／または管理されたブラウザを実行中のユーザコンピューティングデバイス）がアプリケーションストアの第１の部分にアクセスするおよび／または別様にそこから情報を取得することを防止および／またはブロックしてもよい。

【０２５４】

さらに／あるいは、ステップ１４２５において、アプリケーションストアは、管理されたブラウザにアプリケーションストアの第１の部分とは異なるアプリケーションストアの第２の部分へのアクセスを提供してもよい。例えば、（例えば、ステップ１４１０において）管理されたブラウザが管理モードで動作中ではないとの判定後に、アプリケーションストアは、ステップ１４２５において、管理されたブラウザに（例えば、管理されたブラウザおよび／または管理されたブラウザのユーザにより本来、要求されていた部分とは）

異なるアプリケーションストアの部分へのアクセスを提供してもよい。

【０２５５】

さらに／あるいは、ステップ１４３０において、アプリケーションストアは管理されたブラウザにコマンドを送信してもよく、コマンドは、管理されたブラウザに管理モードに入らせるよう構成されてもよい。例えば、（例えば、ステップ１４１０において）管理されたブラウザが管理モードで動作中ではないとの判定後に、アプリケーションストアは、ステップ１４３０において、このようなコマンドを管理されたブラウザに送信してもよい。このようなコマンドの送信において、アプリケーションストアを提供するコンピューティングデバイスは、例えば、データを送信および／またはデータを管理されたブラウザを実行中のユーザコンピューティングデバイスと交換してもよい。さらに、アプリケーションストアがこのようなコマンドを送信したかもしれないが、例えば、１つ以上のポリシーおよび／またはユーザコンピューティングデバイスについての現在のデバイス状態情報が、管理されたブラウザが管理モードに入ることを防止している場合には、ユーザコンピューティングデバイス上の管理されたブラウザは、管理モードに入らないかもしれない。

【０２５６】

このように、ステップ１４３５において、アプリケーションストアは、管理されたブラウザへのコマンドの送信後に管理されたブラウザが管理モードで動作中かどうかを再評価する。例えば、ステップ１４３５において、アプリケーションストアは、再びユーザコンピューティングデバイスおよび／またはユーザコンピューティングデバイス上で実行中の管理されたブラウザにインタロゲートおよび／またはそれらと別様に情報交換してもよく、これは、ユーザコンピューティングデバイスからデバイス状態情報を取得および／または分析することを含んでもよい。

【０２５７】

ステップ１４３５における再評価後に、管理されたブラウザが管理モードで動作中であると判定された場合、ステップ１４４０において、アプリケーションストアは、管理されたブラウザがアプリケーションストアの第１の部分にアクセスするのを許可する。例えば、ステップ１４４０において、コンピューティングデバイスは、ステップ１４１５においてアプリケーションストアがこのようなアクセスを提供してもよい方法と同様に、管理されたブラウザにアプリケーションストアの第１の部分へのアクセスを提供してもよい。あるいは、ステップ１４３５における再評価後に、管理されたブラウザがまだ管理モードで動作中ではないと判定された場合、ステップ１４４５において、アプリケーションストアは、管理されたブラウザに通知を生成および／または送信してもよく、このような通知は、管理されたブラウザが管理モードで動作中ではない間、アプリケーションストアの第１の部分へのアクセスが提供されることができないことを示してもよい。例えば、ステップ１４４５において、アプリケーションストアは、管理されたブラウザのユーザが手動で管理されたブラウザを管理モードに切り替える、および／または、管理されたブラウザが管理モードに入るのを許可するためにデバイス状態情報および／または１つ以上のポリシーの遵守を変更する他の行動を取ることを期待して、管理されたブラウザにこのような通知を送信してもよい。このような行動は、例えば、管理されたブラウザ以外でユーザコンピューティングデバイス上に存在してもよい特定のアプリケーションを閉じるおよび／または削除すること、ユーザコンピューティングデバイスをデバイスが現在位置している位置とは異なる別の位置に移動させること、および／または、ユーザコンピューティングデバイスをデバイスが現在接続している現在のネットワーク以外の１つ以上の他のネットワークに接続することを含んでもよい。

【０２５８】

図１５は、本発明で検討される１つ以上の例示的態様に従って、管理されたブラウザ内に管理された実行環境を提供する方法を示すフローチャートである。１つ以上の実施形態において、図１４に示す方法および／またはその１つ以上のステップは、コンピューティングデバイス（例えば、ジェネリックコンピューティングデバイス２０１）により実行されてもよい。他の実施形態において、図１４に示す方法および／またはその１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具体化されてもよい。

【０２５９】

図１５に見られるように、この方法は、管理されたブラウザがロードされるステップ１５０５で開始する。例えば、ステップ１５０５において、コンピューティングデバイス（例えば、ラップトップコンピュータ、タブレットコンピュータ、スマートフォンまたは他のタイプのモバイルデバイス等のモバイルコンピューティングデバイス）は、ステップ５０５（前記において検討された）においてこのような管理されたブラウザがロードされる方法と同様に、管理されたブラウザをロードしてもよい。管理されたブラウザは、例えば、管理されたブラウザに１つ以上のポリシーが適用される少なくとも１つの管理モードを提供するよう構成されてもよく、１つ以上のポリシーは、前記において検討されたように、管理されたブラウザの１つ以上の機能を制限するよう構成されてもよい。さらに、管理されたブラウザは、実施形態によっては、少なくとも１つの企業リソースから取得されたデータのセキュリティ保護ブラウジングおよびキャッシングを提供するよう構成されてもよい。

【０２６０】

ステップ１５１０において、管理された実行環境は、管理されたブラウザ内に提供される。管理された実行環境は、１つ以上のウェブアプリケーションの実行を容易にするよう構成されてもよく、管理された実行環境は、１つ以上のウェブアプリケーションへ１つ以上のポリシーのうちの少なくとも１つのポリシーを適用するようさらに構成されてもよい。例えば、ステップ１５１０において、コンピューティングデバイスは、管理された実行環境を、管理されたブラウザ内で提供してもよい。管理された実行環境は、例えば、１つ以上のウェブアプリケーションが実行されてもよいシェルとして動作してもよい。

【０２６１】

管理された実行環境内で実行されてもよいウェブアプリケーションは、例えば、様々な異なるプログラミング言語（これは例えば、管理された実行環境内でのランタイム時にコンピューティングデバイスにより実行された場合に、インタープリットされてもよい）で書かれてもおよび／または別様にそれらを利用してもよい。さらに／あるいは、１つ以上のポリシーが、管理された実行環境内で実行されるウェブアプリケーションに適用されてもよく、１つ以上のポリシーは、コンピューティングデバイス、コンピューティングデバイス上で実行中のＭＲＭエージェント、管理されたブラウザおよび／または管理された実行環境自身により定義されおよび／または課されてもよい。管理された実行環境内でウェブアプリケーションに適用されるポリシーは、前記の実施例において検討されたポリシーと同様であってもよく、例えば、デバイス状態情報（これは例えば、管理された実行環境を提供するコンピューティングデバイスについてのデバイス状態情報を含んでもよい）に基づいて強制されおよび／またはそれに別様に依存してもよい。

【０２６２】

実施形態によっては、管理された実行環境は、少なくとも１つのＨＴＭＬ５（ＨｙｐｅｒＴｅｘｔ　Ｍａｒｋｕｐ　Ｌａｎｇｕａｇｅ　５）アプリケーションの実行を容易にするよう構成されてもよい。例えば、例によっては、管理された実行環境内で実行されることができる１つ以上のウェブアプリケーションのうちの少なくとも１つのウェブアプリケーションは、例えばＨＴＭＬ５マークアップ言語でコード化されたＨＴＭＬ５アプリケーションであってもよい。

【０２６３】

実施形態によっては、１つ以上のポリシーのうちの少なくとも１つのポリシーは、ポリシー管理サーバから受信されてもよい。例えば、例によっては、管理された実行環境においてウェブアプリケーションに適用されてもよい１つ以上のポリシーは、ポリシー管理サーバから受信されてもよい。このようなポリシー管理サーバは、例えば、管理されたブラウザ内の管理された実行環境において実行されてもよい様々なウェブアプリケーションに適用されるべき新たなおよび／または更新されたポリシーを提供するために、コンピュー

ティングデバイス上の管理された実行環境と、および／または、管理されたブラウザおよび／またはコンピューティングデバイス上で実行中のＭＲＭエージェントと、直接通信してもよい。

【０２６４】

実施形態によっては、少なくとも１つのポリシー（これは例えば、管理された実行環境において１つ以上のウェブアプリケーションに適用されてもよい）は、１つ以上のウェブアプリケーションの少なくとも１つのローカルストレージリソースへのアクセスを防止するよう構成されてもよい。例えば、管理された実行環境により適用されてもよい１つ以上のポリシーに基づいておよび／またはデバイス状態情報（これは例えば、前記において検討された例でのように、いかに特定のポリシーが強制されるかに影響を及ぼすかもしれない）に基づいて、管理された実行環境および／または管理されたブラウザ内で管理された実行環境を提供しているコンピューティングデバイスが、管理された実行環境内の１つ以上のウェブアプリケーションがコンピューティングデバイス上の１つ以上のローカルリソースにデータを記憶することを防止してもよい。さらに／あるいは、管理された実行環境により適用されてもよい１つ以上のポリシーに基づいておよび／またはデバイス状態情報に基づいて、管理された実行環境および／または管理されたブラウザ内で管理された実行環境を提供しているコンピューティングデバイスが、管理された実行環境内の１つ以上のウェブアプリケーションがローカルに記憶されたデータ（これは例えば、コンピューティングデバイス上の１つ以上のローカルリソースに記憶されてもよい）にアクセスすることを防止してもよい。

【０２６５】

実施形態によっては、少なくとも１つのポリシー（これは例えば、管理された実行環境において１つ以上のウェブアプリケーションに適用されてもよい）は、１つ以上のウェブアプリケーションの少なくとも１つのローカルストレージへのアクセスを選択的に有効化するよう構成されてもよい。例えば、管理された実行環境により適用されてもよい１つ以上のポリシーに基づいておよび／またはデバイス状態情報（これは例えば、前記において検討された実施例でのように、いかに特定のポリシーが強制されるかに影響を及ぼすかもしれない）に基づいて、管理された実行環境および／または管理されたブラウザ内で管理された実行環境を提供しているコンピューティングデバイスが、管理された実行環境内の１つ以上の特定のウェブアプリケーションがコンピューティングデバイス上の１つ以上のローカルリソース内のデータにアクセスすることを許可してもよい。

【０２６６】

さらに／あるいは、管理された実行環境により適用されてもよい１つ以上のポリシーに基づいておよび／またはデバイス状態情報に基づいて、管理された実行環境および／または管理されたブラウザ内で管理された実行環境を提供しているコンピューティングデバイスが、管理された実行環境内の１つ以上の特定のウェブアプリケーションがコンピューティングデバイス上の１つ以上のローカルリソース内のデータを記憶および／または修正することを許可してもよい。例によっては、このようなポリシーはさらに／あるいは、１つ以上のウェブアプリケーションがローカルストレージリソースと相互作用しているインスタンス内の１つ以上の暗号化機能（例えば、ローカルリソースからアクセスされているおよび／またはローカルリソースに記憶されているデータを暗号化するための）を利用するために１つ以上のウェブアプリケーションを要求してもよい。

【０２６７】

実施形態によっては、管理された実行環境は、コンピューティングデバイス上のポリシー管理エージェントを１つ以上のウェブアプリケーションにエクスポーズするよう構成されてもよい。例えば、管理された実行環境および／または管理されたブラウザ内で管理された実行環境を提供しているコンピューティングデバイスは、例によっては、コンピューティングデバイス上で実行中のポリシー管理エージェント（これは例えば、前記の実施例において検討されたように、ＭＲＭエージェントであってもよい）を管理された実行環境内で実行されてもよい１つ以上のウェブアプリケーションにエクスポーズしてもよい。こ

のようにポリシー管理エージェントをウェブアプリケーションにエクスポーズすることにより、管理された実行環境は、ポリシー管理機能、セキュリティ保護鍵管理機能および／または他の機能を、管理された実行環境および／または管理された実行環境内のウェブアプリケーションに拡張することができるかもしれない。

【０２６８】

実施形態によっては、管理された実行環境は、アプリケーションプログラミングインタフェースを介して１つ以上のウェブアプリケーションに１つ以上の機能をエクスポーズするよう構成されてもよい。例えば、管理された実行環境および／または管理されたブラウザ内で管理された実行環境を提供しているコンピューティングデバイスは、例によっては、このようなウェブアプリケーションが他のウェブアプリケーションにより提供されるよりもより高いレベルの機能を提供するのを許可してもよい１つ以上のインタフェースを介して、１つ以上の機能を１つ以上のウェブアプリケーションにエクスポーズしてもよい。例えば、エクスポーズされた機能は、管理された実行環境内のウェブアプリケーションが、暗号化機能、セキュリティ保護トンネリング機能、セキュリティ保護データストレージ機能、ポリシー管理機能および／または例えばコンピューティングデバイス上で実行中のＭＲＭエージェント等のコンピューティングデバイス上で実行中の他のアプリケーションならびに／あるいはサービスにより提供されてもよい他の機能を利用することを許可してもよい。

【０２６９】

実施形態によっては、管理された実行環境は、１つ以上のウェブアプリケーションのために認証サービスを提供するよう構成されてもよい。例えば、管理された実行環境および／または管理されたブラウザ内で管理された実行環境を提供しているコンピューティングデバイスは、例によっては、管理された実行環境内の１つ以上のウェブアプリケーションのための認証サービスを提供してもよい。このような認証サービスの提供において、管理された実行環境および／または管理された実行環境を提供しているコンピューティングデバイスは、例えば、クレデンシャルの取得、鍵の維持および／または特定の状況において様々なハンドシェイクを容易にするためのクレデンシャルならびに／あるいは鍵の提供を含んでもよいウェブアプリケーションのためのマルチファクター認証処理を取り扱ってもよい。例によっては、このようなマルチファクター認証処理を取り扱うことにより、管理された実行環境および／または管理された実行環境を提供しているコンピューティングデバイスは、例えば、特定のウェブアプリケーション内の１つ以上の特定の機能の実行を可能としてもよく、および／または、ウェブアプリケーション自身の実行を可能としてもよい。

【０２７０】

実施形態によっては、管理された実行環境は、１つ以上のウェブアプリケーションにポリシーのデフォルトセットを適用するよう構成されてもよい。例えば、管理された実行環境および／または管理された実行環境を提供しているコンピューティングデバイスは、例によっては、管理された実行環境内の１つ以上の特定のウェブアプリケーションにポリシーのデフォルトセットすなわち「ポリシーバンドル」を適用するよう構成されてもよい。ポリシーのデフォルトセットは、例えば、ポリシー管理サーバから受信されてもよく、および／または、周期的にポリシー管理サーバにより更新されてもよい。さらに、ポリシーのデフォルトセットは、異なるおよび／またはカスタマイズされたポリシーのセットがウェブアプリケーションのために定義されていない限り、管理された実行環境内の特定のウェブアプリケーションに適用されてもよい。

【０２７１】

実施形態によっては、管理された実行環境は、１つ以上のウェブアプリケーションに適用されるポリシーのセットを動的に更新するよう構成されてもよい。例えば、管理された実行環境および／または管理された実行環境を提供しているコンピューティングデバイスは、例によっては、デバイスの現在の使用コンテキストに基づいて管理された実行環境の挙動をリアルタイムに変更するためにデバイス状態情報および／またはユーザ情報（これ

は例えば、ユーザ役割情報を含んでもよい）に基づいて、管理された実行環境内の特定のウェブアプリケーションに適用されるポリシーを動的に更新および／またはオンザフライで別様に修正してもよい。

【０２７２】

例えば、デバイス状態情報（これは例えば、どのような他のアプリケーションが実行中か、ユーザコンピューティングデバイス上にインストールされているか、および／または別様に存在するか、ユーザコンピューティングデバイスがどこに位置するか、ユーザコンピューティングデバイスがどのようなネットワークに接続されているか等についての情報を含んでもよい）に基づいて、管理された実行環境および／または管理された実行環境を提供しているコンピューティングデバイスは、管理された実行環境内の１つ以上のウェブアプリケーションに適用されてもよい１つ以上のポリシーを選択的に有効化および／または選択的に無効化してもよい。別の実施例として、ユーザ情報の変化（これは例えば、ユーザのアカウント切り替えの結果としておよび／またはデバイスへの異なるユーザのログインの結果として生じてもよい）に基づいて、管理された実行環境および／または管理された実行環境を提供しているコンピューティングデバイスは、管理された実行環境内の１つ以上のウェブアプリケーションに適用されてもよい１つ以上のポリシーを選択的に有効化および／または選択的に無効化してもよい。このように、管理された実行環境は、管理された実行環境内に存在するおよび／または実行されるウェブアプリケーションに課されるべき制御の異なるレベルを要求するかもしれない、変化する状況に動的に適応してもよい。

【０２７３】

本発明の様々な態様が、モバイルコンピューティングデバイス上の管理されたブラウザの提供に関して説明された。他の実施形態において、しかしながら、本明細書で検討された概念は、コンピューティングデバイスの任意の他のタイプ（例えば、デスクトップコンピュータ、サーバ、コンソール、セットトップボックス等）でも実装されることができる。本発明は構造的特徴および／または方法論的行動に特有の言語において記述されてきたが、添付の特許請求の範囲に定義される本発明は、必ずしも前記の特定の特徴または行動に制限されないことが理解されよう。むしろ、前記の特定の特徴および行動は、続く特許請求の範囲のいくつかの実施態様例として記述される。

【０２７４】

本願は、２０１３年9月３０日出願の「ＰＲＯＶＩＤＩＮＧ　ＭＡＮＡＧＥＤ　ＢＲＯＷＳＥＲ」と題された米国特許出願第１４／０４０，８３１号の優先権を主張し、当該出願は、その全体において参照により本願に組み込まれる。本願はまた、２０１３年８月１５日出願の「ＰＲＯＶＩＤＩＮＧ　ＳＥＣＵＲＥ　ＢＲＯＷＳＥＲ」と題された米国仮特許出願第６１／８６６，２２９号の利益を主張し、当該出願は、その全体において参照により本願に組み込まれる。本願はさらに、２０１３年3月２９日出願の「ＳＹＳＴＥＭＳ　ＡＮＤ　ＭＥＴＨＯＤＳ　ＦＯＲ　ＥＮＴＥＲＰＲＩＳＥ　ＭＯＢＩＬＩＴＹ　ＭＡＮＡＧＥＭＥＮＴ」と題された米国仮特許出願第６１／８０６，５７７号の利益を主張し、当該出願は、その全体において参照により本願に組み込まれる。

〈予備的な請求項〉

予備的な請求項１から２０の組Ａを以下に示す。

【０２７５】

１．　コンピューティングデバイスにより、管理されたブラウザをロードすることであって、前記管理されたブラウザは、前記管理されたブラウザに１つ以上のポリシーが適用される少なくとも１つの管理モードを提供するよう構成され、前記１つ以上のポリシーは、前記管理されたブラウザの少なくとも１つの機能を制限するよう構成された、前記管理されたブラウザをロードすることと、

前記コンピューティングデバイスにより、デバイスクラウドを開始するために少なくとも１つの他のコンピューティングデバイスへの接続を確立することと、

前記コンピューティングデバイスにより、前記管理されたブラウザのセッションを前記

デバイスクラウドにわたって拡張することであって、
少なくとも１つの他の管理されたブラウザが前記少なくとも１つの他のコンピューティングデバイス上にロードされるようにすることと、
前記少なくとも１つの他の管理されたブラウザでセッションデータを共有することとを含む、前記管理されたブラウザのセッションを拡張することと
を備える方法。
【０２７６】
２．　前記管理されたブラウザは、少なくとも１つの企業リソースから取得されたデータのセキュリティ保護ブラウジングおよびキャッシングを提供するよう構成される、請求項１に記載の方法。
【０２７７】
３．　前記デバイスクラウドは、２つ以上のコンピューティングデバイスが単一機能を実行するために互いに組み合わせて使用されることを可能とする、請求項１に記載の方法。
【０２７８】
４．　前記１つ以上のポリシーのうちの少なくとも１つのポリシーは、前記デバイスクラウドを制限するよう構成される、請求項１に記載の方法。
【０２７９】
５．　前記１つ以上のポリシーのうちの少なくとも１つのポリシーは、前記少なくとも１つの他のコンピューティングデバイスに少なくとも１つの役割を割り当てるよう構成される、請求項４に記載の方法。
【０２８０】
６．　前記少なくとも１つの他のコンピューティングデバイスへの接続は、前記１つ以上のポリシーのうちの少なくとも１つのポリシーに基づいて確立される、請求項１に記載の方法。
【０２８１】
７．　前記少なくとも１つのポリシーは、前記デバイスクラウドを開始するために前記管理されたブラウザの能力を制限する、請求項６に記載の方法。
【０２８２】
８．　前記少なくとも１つの他のコンピューティングデバイスへの接続を確立することは、
前記少なくとも１つの他のコンピューティングデバイスに関する状態情報を評価することと、
前記評価された状態情報に基づいて、前記少なくとも１つの他のコンピューティングデバイスの前記デバイスクラウドへの参加を許可するよう判定することとを含む、請求項１に記載の方法。
【０２８３】
９．　コンピューティングデバイスであって、
少なくとも１つのプロセッサと、
前記少なくとも１つのプロセッサにより実行されたときに、前記コンピューティングデバイスに、
管理されたブラウザをロードすることであって、前記管理されたブラウザは、前記管理されたブラウザに１つ以上のポリシーが適用される少なくとも１つの管理モードを提供するよう構成され、前記１つ以上のポリシーは、前記管理されたブラウザの少なくとも１つの機能を制限するよう構成された、前記管理されたブラウザをロードすることと、
デバイスクラウドを開始するために少なくとも１つの他のコンピューティングデバイスへの接続を確立することと、
前記管理されたブラウザのセッションを前記デバイスクラウドにわたって拡張することであって、
少なくとも１つの他の管理されたブラウザが前記少なくとも１つの他のコンピューティ

ングデバイス上にロードされるようにすることと、
前記少なくとも１つの他の管理されたブラウザでセッションデータを共有することとを含む、前記管理されたブラウザのセッションを拡張することとを行なわせる、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、コンピューティングデバイス。
【０２８４】
１０．　前記管理されたブラウザは、少なくとも１つの企業リソースから取得されたデータのセキュリティ保護ブラウジングおよびキャッシングを提供するよう構成される、請求項９に記載のコンピューティングデバイス。
【０２８５】
１１．　前記デバイスクラウドは、２つ以上のコンピューティングデバイスが単一機能を実行するために互いに組み合わせて使用されることを可能とする、請求項９に記載のコンピューティングデバイス。
【０２８６】
１２．　前記１つ以上のポリシーのうちの少なくとも１つのポリシーは、前記デバイスクラウドを制限するよう構成される、請求項９に記載のコンピューティングデバイス。
【０２８７】
１３．　前記１つ以上のポリシーのうちの少なくとも１つのポリシーは、前記少なくとも１つの他のコンピューティングデバイスに少なくとも１つの役割を割り当てるよう構成される、請求項１２に記載のコンピューティングデバイス。
【０２８８】
１４．　前記少なくとも１つの他のコンピューティングデバイスへの接続は、前記１つ以上のポリシーのうちの少なくとも１つのポリシーに基づいて確立される、請求項９に記載のコンピューティングデバイス。
【０２８９】
１５．　前記少なくとも１つのポリシーは、前記デバイスクラウドを開始するために前記管理されたブラウザの能力を制限する、請求項１４に記載のコンピューティングデバイス。
【０２９０】
１６．　実行されたときに、コンピューティングデバイスに、
管理されたブラウザをロードすることであって、前記管理されたブラウザは、前記管理されたブラウザに１つ以上のポリシーが適用される少なくとも１つの管理モードを提供するよう構成され、前記１つ以上のポリシーは、前記管理されたブラウザの少なくとも１つの機能を制限するよう構成された、前記管理されたブラウザをロードすることと、
デバイスクラウドを開始するために少なくとも１つの他のコンピューティングデバイスへの接続を確立することと、
前記管理されたブラウザのセッションを前記デバイスクラウドにわたって拡張することであって、
少なくとも１つの他の管理されたブラウザが前記少なくとも１つの他のコンピューティングデバイス上にロードされるようにすることと、
前記少なくとも１つの他の管理されたブラウザでセッションデータを共有することとを含む、前記管理されたブラウザのセッションを拡張することと
を行なわせる、記憶された命令を有する１つ以上の不揮発性コンピュータ読取可能媒体。
【０２９１】
１７．　前記管理されたブラウザは、少なくとも１つの企業リソースから取得されたデータのセキュリティ保護ブラウジングおよびキャッシングを提供するよう構成される、請求項１６に記載の１つ以上の不揮発性コンピュータ読取可能媒体。
【０２９２】
１８．　前記デバイスクラウドは、２つ以上のコンピューティングデバイスが単一機能

を実行するために互いに組み合わせて使用されることを可能とする、請求項１６に記載の１つ以上の不揮発性コンピュータ読取可能媒体。

【０２９３】

１９．　前記１つ以上のポリシーのうちの少なくとも１つのポリシーは、前記デバイスクラウドを制限するよう構成される、請求項１６に記載の１つ以上の不揮発性コンピュータ読取可能媒体。

【０２９４】

２０．　前記１つ以上のポリシーのうちの少なくとも１つのポリシーは、前記少なくとも１つの他のコンピューティングデバイスに少なくとも１つの役割を割り当てるよう構成される、請求項１９に記載の１つ以上の不揮発性コンピュータ読取可能媒体。

【０２９５】

さらなる予備的な請求項１から２０の組Ｂを以下に示す。

【０２９６】

１．　コンピューティングデバイスにより、管理されたブラウザをロードすることであって、前記管理されたブラウザは、前記管理されたブラウザに１つ以上のポリシーが適用される少なくとも１つの管理モードを提供するよう構成され、前記１つ以上のポリシーは、前記管理されたブラウザの少なくとも１つの機能を制限するよう構成された、前記管理されたブラウザをロードすることと、

前記コンピューティングデバイスにより、前記管理されたブラウザを介して１つ以上の企業リソースのアクセスへの要求を受信することと、

前記コンピューティングデバイスにより、前記１つ以上のポリシーのうちの少なくとも１つのポリシーに基づいて、前記１つ以上の企業リソースへの前記管理されたブラウザからの少なくとも１つのアプリケーショントンネルを生成することと、

前記コンピューティングデバイスにより、前記少なくとも１つのアプリケーショントンネルを介して前記１つ以上の企業リソースから企業データを取得することとを備える方法。

【０２９７】

２．　前記管理されたブラウザは、少なくとも１つの企業リソースから取得されたデータのセキュリティ保護ブラウジングおよびキャッシングを提供するよう構成される、請求項１に記載の方法。

【０２９８】

３．　前記少なくとも１つのアプリケーショントンネルを生成することは、

前記管理されたブラウザから第１の企業リソースへの第１のアプリケーショントンネルを生成することと、

前記管理されたブラウザから前記第１の企業リソースとは異なる第２の企業リソースへの第２のアプリケーショントンネルを生成することとを含む、請求項１に記載の方法。

【０２９９】

４．　前記第１の企業リソースは第１のセキュリティレベルを有し、前記第２の企業リソースは前記第１のセキュリティレベルとは異なる第２のセキュリティレベルを有する、請求項３に記載の方法。

【０３００】

５．　前記１つ以上のポリシーのうちの少なくとも１つのポリシーは、アプリケーショントンネルを生成する前記管理されたブラウザの能力を選択的に制限するよう構成される、請求項１に記載の方法。

【０３０１】

６．　前記１つ以上のポリシーのうちの少なくとも１つのポリシーは、前記取得された企業データの使用を制限するよう構成される、請求項１に記載の方法。

【０３０２】

７．　前記１つ以上のポリシーのうちの少なくとも１つのポリシーはデバイス状態情報に依存する、請求項６に記載の方法。

【０３０３】
８．　コンピューティングデバイスであって、
少なくとも１つのプロセッサと、
前記少なくとも１つのプロセッサにより実行されたときに、前記コンピューティングデバイスに、
管理されたブラウザをロードすることであって、前記管理されたブラウザは、前記管理されたブラウザに１つ以上のポリシーが適用される少なくとも１つの管理モードを提供するよう構成され、前記１つ以上のポリシーは、前記管理されたブラウザの少なくとも１つの機能を制限するよう構成された、前記管理されたブラウザをロードすることと、
前記管理されたブラウザを介して１つ以上の企業リソースのアクセスへの要求を受信することと、
前記１つ以上のポリシーのうちの少なくとも１つのポリシーに基づいて、前記１つ以上の企業リソースへの前記管理されたブラウザからの少なくとも１つのアプリケーショントンネルを生成することと、
前記少なくとも１つのアプリケーショントンネルを介して前記１つ以上の企業リソースから企業データを取得することとを行なわせる、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、コンピューティングデバイス。
【０３０４】
９．　前記管理されたブラウザは、少なくとも１つの企業リソースから取得されたデータのセキュリティ保護ブラウジングおよびキャッシングを提供するよう構成される、請求項８に記載のコンピューティングデバイス。
【０３０５】
１０．　前記少なくとも１つのアプリケーショントンネルを生成することは、
前記管理されたブラウザから第１の企業リソースへの第１のアプリケーショントンネルを生成することと、
前記管理されたブラウザから前記第１の企業リソースとは異なる第２の企業リソースへの第２のアプリケーショントンネルを生成することとを含む、請求項８に記載のコンピューティングデバイス。
【０３０６】
１１．　前記第１の企業リソースは第１のセキュリティレベルを有し、前記第２の企業リソースは前記第１のセキュリティレベルとは異なる第２のセキュリティレベルを有する、請求項１０に記載のコンピューティングデバイス。
【０３０７】
１２．　前記１つ以上のポリシーのうちの少なくとも１つのポリシーは、アプリケーショントンネルを生成する前記管理されたブラウザの能力を選択的に制限するよう構成される、請求項８に記載のコンピューティングデバイス。
【０３０８】
１３．　前記１つ以上のポリシーのうちの少なくとも１つのポリシーは、前記取得された企業データの使用を制限するよう構成される、請求項８に記載のコンピューティングデバイス。
【０３０９】
１４．　前記１つ以上のポリシーのうちの少なくとも１つのポリシーはデバイス状態情報に依存する、請求項１３に記載のコンピューティングデバイス。
【０３１０】
１５．　実行されたときに、コンピューティングデバイスに、
管理されたブラウザをロードすることであって、前記管理されたブラウザは、前記管理されたブラウザに１つ以上のポリシーが適用される少なくとも１つの管理モードを提供するよう構成され、前記１つ以上のポリシーは、前記管理されたブラウザの少なくとも１つの機能を制限するよう構成された、前記管理されたブラウザをロードすることと、

前記管理されたブラウザを介して１つ以上の企業リソースのアクセスへの要求を受信することと、
前記１つ以上のポリシーのうちの少なくとも１つのポリシーに基づいて、前記１つ以上の企業リソースへの前記管理されたブラウザからの少なくとも１つのアプリケーショントンネルを生成することと、
前記少なくとも１つのアプリケーショントンネルを介して前記１つ以上の企業リソースから企業データを取得することとを行なわせる、記憶された命令を有する１つ以上の不揮発性コンピュータ読取可能媒体。
【０３１１】
１６．　前記管理されたブラウザは、少なくとも１つの企業リソースから取得されたデータのセキュリティ保護ブラウジングおよびキャッシングを提供するよう構成される、請求項１５に記載の１つ以上の不揮発性コンピュータ読取可能媒体。
【０３１２】
１７．　前記少なくとも１つのアプリケーショントンネルを生成することは、
前記管理されたブラウザから第１の企業リソースへの第１のアプリケーショントンネルを生成することと、
前記管理されたブラウザから前記第１の企業リソースとは異なる第２の企業リソースへの第２のアプリケーショントンネルを生成することと
を含む、請求項１５に記載の１つ以上の不揮発性コンピュータ読取可能媒体。
【０３１３】
１８．　前記第１の企業リソースは第１のセキュリティレベルを有し、前記第２の企業リソースは前記第１のセキュリティレベルとは異なる第２のセキュリティレベルを有する、請求項１７に記載の１つ以上の不揮発性コンピュータ読取可能媒体。
【０３１４】
１９．　前記１つ以上のポリシーのうちの少なくとも１つのポリシーは、アプリケーショントンネルを生成する前記管理されたブラウザの能力を選択的に制限するよう構成される、請求項１５に記載の１つ以上の不揮発性コンピュータ読取可能媒体。
【０３１５】
２０．　前記１つ以上のポリシーのうちの少なくとも１つのポリシーは、前記取得された企業データの使用を制限するよう構成される、請求項１５に記載の１つ以上の不揮発性コンピュータ読取可能媒体。
【０３１６】
さらなる予備的な請求項１から２０の組Ｃを以下に示す。
【０３１７】
１．　少なくとも１つのサーバコンピューティングデバイスにより、１つ以上のユーザコンピューティングデバイス上の管理されたブラウザに適用されるべき少なくとも１つのポリシーを受信することであって、前記管理されたブラウザは、前記管理されたブラウザに１つ以上のポリシーが適用される少なくとも１つの管理モードを提供するよう構成される、前記少なくとも１つのポリシーを受信することと、
前記少なくとも１つのサーバコンピューティングデバイスにより、前記少なくとも１つの受信されたポリシーに基づいて、前記１つ以上のユーザコンピューティングデバイスのうちの少なくとも１つのユーザコンピューティングデバイスに少なくとも１つのポリシー更新を提供することとを備える、方法。
【０３１８】
２．　前記少なくとも１つのポリシー更新は、前記少なくとも１つのユーザコンピューティングデバイスに、前記少なくとも１つのユーザコンピューティングデバイス上の管理されたブラウザに前記少なくとも１つの受信されたポリシーを適用させるよう構成される、請求項１に記載の方法。
【０３１９】
３．　前記少なくとも１つの受信されたポリシーは、１つ以上のコンテンツフィルタリ

ング規則を含む、請求項１に記載の方法。
【０３２０】
４．　前記少なくとも１つの受信されたポリシーは、１つ以上のキャッシング規則を含む、請求項１に記載の方法。
【０３２１】
５．　前記少なくとも１つの受信されたポリシーは、１つ以上のプラグイン規則を含む、請求項１に記載の方法。
【０３２２】
６．　前記少なくとも１つの受信されたポリシーは、１つ以上のクレデンシャル管理規則を含む、請求項１に記載の方法。
【０３２３】
７．　前記少なくとも１つの受信されたポリシーは、デバイス状態情報に基づいて前記少なくとも１つのユーザコンピューティングデバイスにより強制されるよう構成される、請求項１に記載の方法。
【０３２４】
８．　前記少なくとも１つの受信されたポリシーは、１つ以上の基準に基づいて前記管理されたブラウザを非管理モードへと切り替えさせるよう構成された１つ以上の規則を含む、請求項１に記載の方法。
【０３２５】
９．　コンピューティングデバイスであって、
少なくとも１つのプロセッサと、
前記少なくとも１つのプロセッサにより実行されたときに、前記コンピューティングデバイスに、
１つ以上のユーザコンピューティングデバイス上の管理されたブラウザに適用されるべき少なくとも１つのポリシーを受信することであって、前記管理されたブラウザは、前記管理されたブラウザに１つ以上のポリシーが適用される少なくとも１つの管理モードを提供するよう構成される、前記少なくとも１つのポリシーを受信することと、
前記少なくとも１つの受信されたポリシーに基づいて、前記１つ以上のユーザコンピューティングデバイスのうちの少なくとも１つのユーザコンピューティングデバイスに少なくとも１つのポリシー更新を提供することとを行なわせる、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、コンピューティングデバイス。
【０３２６】
１０．　前記少なくとも１つのポリシー更新は、前記少なくとも１つのユーザコンピューティングデバイスに、前記少なくとも１つのユーザコンピューティングデバイス上の管理されたブラウザに前記少なくとも１つの受信されたポリシーを適用させるよう構成される、請求項９に記載のコンピューティングデバイス。
【０３２７】
１１．　前記少なくとも１つの受信されたポリシーは、１つ以上のコンテンツフィルタリング規則を含む、請求項９に記載のコンピューティングデバイス。
【０３２８】
１２．　前記少なくとも１つの受信されたポリシーは、１つ以上のキャッシング規則を含む、請求項９に記載のコンピューティングデバイス。
【０３２９】
１３．　前記少なくとも１つの受信されたポリシーは、１つ以上のプラグイン規則を含む、請求項９に記載のコンピューティングデバイス。
【０３３０】
１４．　前記少なくとも１つの受信されたポリシーは、１つ以上のクレデンシャル管理規則を含む、請求項９に記載のコンピューティングデバイス。
【０３３１】
１５．　前記少なくとも１つの受信されたポリシーは、デバイス状態情報に基づいて前

記少なくとも１つのユーザコンピューティングデバイスにより強制されるよう構成される、請求項９に記載のコンピューティングデバイス。

【０３３２】

１６．　前記少なくとも１つの受信されたポリシーは、１つ以上の基準に基づいて前記管理されたブラウザを非管理モードへと切り替えさせるよう構成された１つ以上の規則を含む、請求項９に記載のコンピューティングデバイス。

【０３３３】

１７．　実行されたときに、コンピューティングデバイスに、

１つ以上のユーザコンピューティングデバイス上の管理されたブラウザに適用されるべき少なくとも１つのポリシーを受信することであって、前記管理されたブラウザは、前記管理されたブラウザに１つ以上のポリシーが適用される少なくとも１つの管理モードを提供するよう構成される、前記少なくとも１つのポリシーを受信することと、

前記少なくとも１つの受信されたポリシーに基づいて、前記１つ以上のユーザコンピューティングデバイスのうちの少なくとも１つのユーザコンピューティングデバイスに少なくとも１つのポリシー更新を提供することとを行なわせる、記憶された命令を有する１つ以上の不揮発性コンピュータ読取可能媒体。

【０３３４】

１８．　前記少なくとも１つのポリシー更新は、前記少なくとも１つのユーザコンピューティングデバイスに、前記少なくとも１つのユーザコンピューティングデバイス上の管理されたブラウザに前記少なくとも１つの受信されたポリシーを適用させるよう構成される、請求項１７に記載の１つ以上の不揮発性コンピュータ読取可能媒体。

【０３３５】

１９．　前記少なくとも１つの受信されたポリシーは、デバイス状態情報に基づいて前記少なくとも１つのユーザコンピューティングデバイスにより強制されるよう構成される、請求項１７に記載の１つ以上の不揮発性コンピュータ読取可能媒体。

【０３３６】

２０．　前記少なくとも１つの受信されたポリシーは、１つ以上の基準に基づいて前記管理されたブラウザを非管理モードへと切り替えさせるよう構成された１つ以上の規則を含む、請求項１７に記載の１つ以上の不揮発性コンピュータ読取可能媒体。

【０３３７】

さらなる予備的な請求項１から２０の組Ｄを以下に示す。

【０３３８】

１．　コンピューティングデバイスにより、管理されたブラウザをロードすることであって、前記管理されたブラウザは、前記管理されたブラウザに１つ以上のポリシーが適用される少なくとも１つの管理モードを提供するよう構成され、前記１つ以上のポリシーは、前記管理されたブラウザの少なくとも１つの機能を制限するよう構成された、前記管理されたブラウザをロードすることと、

前記コンピューティングデバイスにより、前記管理されたブラウザを介して１つ以上の企業リソースのアクセスへの要求を受信することと、

前記コンピューティングデバイスにより、前記要求に基づいて前記１つ以上の企業リソースから企業データを取得することと、

前記コンピューティングデバイスにより、前記取得された企業データをセキュリティ保護ドキュメントコンテナ内に記憶することとを備える方法。

【０３３９】

２．　前記管理されたブラウザは、少なくとも１つの企業リソースから取得されたデータのセキュリティ保護ブラウジングおよびキャッシングを提供するよう構成される、請求項１に記載の方法。

【０３４０】

３．　前記コンピューティングデバイスにより、前記管理されたブラウザを介して前記セキュリティ保護ドキュメントコンテナへのアクセスを提供することをさらに備える、請

求項１に記載の方法。
【０３４１】
４．　前記コンピューティングデバイスにより、前記セキュリティ保護ドキュメントコンテナからデータを選択的にワイプすることをさらに備える、請求項１に記載の方法。
【０３４２】
５．　前記セキュリティ保護ドキュメントコンテナからデータを選択的にワイプすることは、前記要求に基づいて前記１つ以上の企業リソースから取得された前記企業データを削除することを含む、請求項４に記載の方法。
【０３４３】
６．　前記データは、前記管理されたブラウザが閉じられたときに前記セキュリティ保護ドキュメントコンテナから選択的にワイプされる、請求項４に記載の方法。
【０３４４】
７．　前記データは、前記１つ以上のポリシーに基づいて前記セキュリティ保護ドキュメントコンテナから選択的にワイプされる、請求項４に記載の方法。
【０３４５】
８．　コンピューティングデバイスであって、
少なくとも１つのプロセッサと、
前記少なくとも１つのプロセッサにより実行されたときに、前記コンピューティングデバイスに、
管理されたブラウザをロードすることであって、前記管理されたブラウザは、前記管理されたブラウザに１つ以上のポリシーが適用される少なくとも１つの管理モードを提供するよう構成され、前記１つ以上のポリシーは、前記管理されたブラウザの少なくとも１つの機能を制限するよう構成された、前記管理されたブラウザをロードすることと、
前記管理されたブラウザを介して１つ以上の企業リソースのアクセスへの要求を受信することと、
前記要求に基づいて前記１つ以上の企業リソースから企業データを取得することと、
前記取得された企業データをセキュリティ保護ドキュメントコンテナ内に記憶することとを行なわせる、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、コンピューティングデバイス。
【０３４６】
９．　前記管理されたブラウザは、少なくとも１つの企業リソースから取得されたデータのセキュリティ保護ブラウジングおよびキャッシングを提供するよう構成される、請求項８に記載のコンピューティングデバイス。
【０３４７】
１０．　前記メモリは、前記少なくとも１つのプロセッサにより実行されたときに、前記コンピューティングデバイスにさらに、
前記管理されたブラウザを介して前記セキュリティ保護ドキュメントコンテナへのアクセスを提供することを行なわせるさらなるコンピュータ読取可能命令を記憶する請求項８に記載のコンピューティングデバイス。
【０３４８】
１１．　前記メモリは、前記少なくとも１つのプロセッサにより実行されたときに、前記コンピューティングデバイスにさらに、
前記セキュリティ保護ドキュメントコンテナからデータを選択的にワイプすることを行なわせる、さらなるコンピュータ読取可能命令を記憶する請求項８に記載のコンピューティングデバイス。
【０３４９】
１２．　前記セキュリティ保護ドキュメントコンテナからデータを選択的にワイプすることは、前記要求に基づいて前記１つ以上の企業リソースから取得された前記企業データを削除することを含む、請求項１１に記載のコンピューティングデバイス。
【０３５０】

１３．　前記データは、前記管理されたブラウザが閉じられたときに前記セキュリティ保護ドキュメントコンテナから選択的にワイプされる、請求項１１に記載のコンピューティングデバイス。

【０３５１】

１４．　前記データは、前記１つ以上のポリシーに基づいて前記セキュリティ保護ドキュメントコンテナから選択的にワイプされる、請求項１１に記載のコンピューティングデバイス。

【０３５２】

１５．　実行されたときに、コンピューティングデバイスに、

管理されたブラウザをロードすることであって、前記管理されたブラウザは、前記管理されたブラウザに１つ以上のポリシーが適用される少なくとも１つの管理モードを提供するよう構成され、前記１つ以上のポリシーは、前記管理されたブラウザの少なくとも１つの機能を制限するよう構成された、前記管理されたブラウザをロードすることと、

前記管理されたブラウザを介して１つ以上の企業リソースのアクセスへの要求を受信することと、

前記要求に基づいて前記１つ以上の企業リソースから企業データを取得することと、

前記取得された企業データをセキュリティ保護ドキュメントコンテナ内に記憶することとを行なわせる、記憶された命令を有する１つ以上の不揮発性コンピュータ読取可能媒体。

【０３５３】

１６．　前記管理されたブラウザは、少なくとも１つの企業リソースから取得されたデータのセキュリティ保護ブラウジングおよびキャッシングを提供するよう構成される、請求項１５に記載の１つ以上の不揮発性コンピュータ読取可能媒体。

【０３５４】

１７．　実行されたときに、前記コンピューティングデバイスにさらに、

前記管理されたブラウザを介して前記セキュリティ保護ドキュメントコンテナへのアクセスを提供することを行なわせる、記憶されたさらなる命令を有する、請求項１５に記載の１つ以上の不揮発性コンピュータ読取可能媒体。

【０３５５】

１８．　実行されたときに、前記コンピューティングデバイスにさらに、

前記セキュリティ保護ドキュメントコンテナからデータを選択的にワイプすることを行なわせる、記憶されたさらなる命令を有する、請求項１５に記載の１つ以上の不揮発性コンピュータ読取可能媒体。

【０３５６】

１９．　前記セキュリティ保護ドキュメントコンテナからデータを選択的にワイプすることは、前記要求に基づいて前記１つ以上の企業リソースから取得された前記企業データを削除することを含む、請求項１８に記載の１つ以上の不揮発性コンピュータ読取可能媒体。

【０３５７】

２０．　前記データは、前記管理されたブラウザが閉じられたときに前記セキュリティ保護ドキュメントコンテナから選択的にワイプされる、請求項１８に記載の１つ以上の不揮発性コンピュータ読取可能媒体。

【０３５８】

さらなる予備的な請求項１から２０の組Ｅを以下に示す。

【０３５９】

１．　コンピューティングデバイスにより、管理されたブラウザをロードすることであって、前記管理されたブラウザは、前記管理されたブラウザに１つ以上のポリシーが適用される少なくとも１つの管理モードを提供するよう構成され、前記１つ以上のポリシーは、前記管理されたブラウザの少なくとも１つの機能を制限するよう構成された、前記管理されたブラウザをロードすることと、

前記コンピューティングデバイスにより、少なくとも１つのユーザアカウントに関するＳＳＯクレデンシャルを受信することと、
前記コンピューティングデバイスにより、前記ＳＳＯクレデンシャルに基づいて１つ以上の企業リソースから企業データを取得することと、
前記コンピューティングデバイスにより、前記取得された企業データへのアクセスを前記管理されたブラウザを介して提供することとを備え、
前記ＳＳＯクレデンシャルに基づいて前記１つ以上の企業リソースから前記企業データを取得することは、
前記１つ以上の企業リソースのうちの少なくとも１つの企業リソースから認証チャレンジを受信することと、
前記１つ以上のポリシーのうちの少なくとも１つのポリシーに基づいて、前記認証チャレンジに応じて前記少なくとも１つの企業リソースへと前記ＳＳＯクレデンシャルを提供すべきかどうかを判定することと、
前記認証チャレンジに応じた前記ＳＳＯクレデンシャルの前記少なくとも１つの企業リソースへの提供の判定に基づいて、前記ＳＳＯクレデンシャルを前記少なくとも１つの企業リソースへと提供することとを含む、方法。

【０３６０】

２．　前記管理されたブラウザは、少なくとも１つの企業リソースから取得されたデータのセキュリティ保護ブラウジングおよびキャッシングを提供するよう構成される、請求項１に記載の方法。

【０３６１】

３．　前記ＳＳＯクレデンシャルは、少なくとも２つの異なる企業リソースへのアクセスに使用されるよう構成された認証クレデンシャルである、請求項１に記載の方法。

【０３６２】

４．　前記管理されたブラウザを介して前記取得された企業データへのアクセスを提供することは、前記ＳＳＯクレデンシャルに基づいて前記１つ以上のポリシーのうちの少なくとも１つのポリシーを強制することを含む、請求項１に記載の方法。

【０３６３】

５．　前記認証チャレンジに応じて前記少なくとも１つの企業リソースへと前記ＳＳＯクレデンシャルを提供しないとの判定に基づいて、前記コンピューティングデバイスにより、前記コンピューティングデバイスのユーザから少なくとも１つの認証クレデンシャルを受信するよう構成された認証プロンプトを生成することをさらに備える、請求項１に記載の方法。

【０３６４】

６．　前記１つ以上のポリシーのうちの少なくとも１つのポリシーは、前記取得された企業データへのアクセスを制限するよう構成される、請求項４に記載の方法。

【０３６５】

７．　前記１つ以上のポリシーのうちの少なくとも１つのポリシーの強制は、デバイス状態情報に依存する、請求項４に記載の方法。

【０３６６】

８．　コンピューティングデバイスであって、
少なくとも１つのプロセッサと、
前記少なくとも１つのプロセッサにより実行されたときに、前記コンピューティングデバイスに、
管理されたブラウザをロードすることであって、前記管理されたブラウザは、前記管理されたブラウザに１つ以上のポリシーが適用される少なくとも１つの管理モードを提供するよう構成され、前記１つ以上のポリシーは、前記管理されたブラウザの少なくとも１つの機能を制限するよう構成された、前記管理されたブラウザをロードすることと、
少なくとも１つのユーザアカウントに関するＳＳＯクレデンシャルを受信することと、
前記ＳＳＯクレデンシャルに基づいて１つ以上の企業リソースから企業データを取得す

ることと、
前記取得された企業データへのアクセスを前記管理されたブラウザを介して提供することとを行なわせる、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ＳＳＯクレデンシャルに基づいて前記１つ以上の企業リソースから前記企業データを取得することは、
前記１つ以上の企業リソースのうちの少なくとも１つの企業リソースから認証チャレンジを受信することと、
前記１つ以上のポリシーのうちの少なくとも１つのポリシーに基づいて、前記認証チャレンジに応じて前記少なくとも１つの企業リソースへと前記ＳＳＯクレデンシャルを提供すべきかどうかを判定することと、
前記認証チャレンジに応じた前記ＳＳＯクレデンシャルの前記少なくとも１つの企業リソースへの提供の判定に基づいて、前記ＳＳＯクレデンシャルを前記少なくとも１つの企業リソースへと提供することとを含む、コンピューティングデバイス。
【０３６７】
９．　前記管理されたブラウザは、少なくとも１つの企業リソースから取得されたデータのセキュリティ保護ブラウジングおよびキャッシングを提供するよう構成される、請求項８に記載のコンピューティングデバイス。
【０３６８】
１０．　前記ＳＳＯクレデンシャルは、少なくとも２つの異なる企業リソースへのアクセスに使用されるよう構成された認証クレデンシャルである、請求項８に記載のコンピューティングデバイス。
【０３６９】
１１．　前記管理されたブラウザを介して前記取得された企業データへのアクセスを提供することは、前記ＳＳＯクレデンシャルに基づいて前記１つ以上のポリシーのうちの少なくとも１つのポリシーを強制することを含む、請求項８に記載のコンピューティングデバイス。
【０３７０】
１２．　前記メモリは、前記少なくとも１つのプロセッサにより実行されたときに、前記コンピューティングデバイスにさらに、
前記認証チャレンジに応じて前記少なくとも１つの企業リソースへと前記ＳＳＯクレデンシャルを提供しないとの判定に基づいて、前記コンピューティングデバイスにより、前記コンピューティングデバイスのユーザから少なくとも１つの認証クレデンシャルを受信するよう構成された認証プロンプトを生成することを行なわせる、さらなるコンピュータ読取可能命令を記憶する、請求項８に記載のコンピューティングデバイス。
【０３７１】
１３．　前記１つ以上のポリシーのうちの少なくとも１つのポリシーは、前記取得された企業データへのアクセスを制限するよう構成される、請求項１１に記載のコンピューティングデバイス。
【０３７２】
１４．　前記１つ以上のポリシーのうちの少なくとも１つのポリシーの強制は、デバイス状態情報に依存する、請求項１１に記載のコンピューティングデバイス。
【０３７３】
１５．　実行されたときに、コンピューティングデバイスに、
管理されたブラウザをロードすることであって、前記管理されたブラウザは、前記管理されたブラウザに１つ以上のポリシーが適用される少なくとも１つの管理モードを提供するよう構成され、前記１つ以上のポリシーは、前記管理されたブラウザの少なくとも１つの機能を制限するよう構成された、前記管理されたブラウザをロードすることと、
少なくとも１つのユーザアカウントに関するＳＳＯクレデンシャルを受信することと、
前記ＳＳＯクレデンシャルに基づいて１つ以上の企業リソースから企業データを取得す

ることと、
前記取得された企業データへのアクセスを前記管理されたブラウザを介して提供することとを行なわせる、記憶された命令を有する１つ以上の不揮発性コンピュータ読取可能媒体であって、
前記ＳＳＯクレデンシャルに基づいて前記１つ以上の企業リソースから前記企業データを取得することは、
前記１つ以上の企業リソースのうちの少なくとも１つの企業リソースから認証チャレンジを受信することと、
前記１つ以上のポリシーのうちの少なくとも１つのポリシーに基づいて、前記認証チャレンジに応じて前記少なくとも１つの企業リソースへと前記ＳＳＯクレデンシャルを提供すべきかどうかを判定することと、
前記認証チャレンジに応じた前記ＳＳＯクレデンシャルの前記少なくとも１つの企業リソースへの提供の判定に基づいて、前記ＳＳＯクレデンシャルを前記少なくとも１つの企業リソースへと提供することとを含む、１つ以上の不揮発性コンピュータ読取可能媒体。
【０３７４】
１６．　前記管理されたブラウザは、少なくとも１つの企業リソースから取得されたデータのセキュリティ保護ブラウジングおよびキャッシングを提供するよう構成される、請求項１５に記載の１つ以上の不揮発性コンピュータ読取可能媒体。
【０３７５】
１７．　前記ＳＳＯクレデンシャルは、少なくとも２つの異なる企業リソースへのアクセスに使用されるよう構成された認証クレデンシャルである、請求項１５に記載の１つ以上の不揮発性コンピュータ読取可能媒体。
【０３７６】
１８．　前記管理されたブラウザを介して前記取得された企業データへのアクセスを提供することは、前記ＳＳＯクレデンシャルに基づいて前記１つ以上のポリシーのうちの少なくとも１つのポリシーを強制することを含む、請求項１５に記載の１つ以上の不揮発性コンピュータ読取可能媒体。
【０３７７】
１９．　実行されたときに、前記コンピューティングデバイスにさらに、
前記認証チャレンジに応じて前記少なくとも１つの企業リソースへと前記ＳＳＯクレデンシャルを提供しないとの判定に基づいて、前記コンピューティングデバイスにより、前記コンピューティングデバイスのユーザから少なくとも１つの認証クレデンシャルを受信するよう構成された認証プロンプトを生成することを行なわせる、記憶されたさらなる命令を有する、請求項１８に記載の１つ以上の不揮発性コンピュータ読取可能媒体。
【０３７８】
２０．　前記１つ以上のポリシーのうちの少なくとも１つのポリシーは、前記取得された企業データへのアクセスを制限するよう構成される、請求項１８に記載の１つ以上の不揮発性コンピュータ読取可能媒体。
【０３７９】
さらなる予備的な請求項１から２０の組Ｆを以下に示す。
【０３８０】
１．　アプリケーションストアにおいて、ユーザコンピューティングデバイス上の管理されたブラウザから前記アプリケーションストアの第１の部分のアクセスへの要求を受信することと、
前記アプリケーションストアにより、前記管理されたブラウザが１つ以上のポリシーが前記管理されたブラウザに適用される管理モードで動作中かどうかを判定することであって、前記１つ以上のポリシーが前記管理されたブラウザの少なくとも１つの機能を制限するよう構成される、判定することと、
前記管理されたブラウザが前記管理モードで動作中であるとの判定に基づいて、前記アプリケーションストアにより、前記管理されたブラウザが前記アプリケーションストアの

前記第１の部分にアクセスするのを許可することとを備える、方法。
【０３８１】
２．　前記管理されたブラウザが前記管理モードで動作中ではないとの判定に基づいて、前記アプリケーションストアにより、前記管理されたブラウザが前記アプリケーションストアの前記第１の部分にアクセスするのを防止することをさらに備える、請求項１に記載の方法。
【０３８２】
３．　前記アプリケーションストアにより、前記管理されたブラウザに前記第１の部分とは異なる前記アプリケーションストアの第２の部分へのアクセスを提供することをさらに備える、請求項２に記載の方法。
【０３８３】
４．　前記管理されたブラウザが前記管理モードで動作中ではないとの判定に基づいて、前記アプリケーションストアにより、前記管理されたブラウザに前記管理モードに入らせるよう構成されたコマンドを前記管理されたブラウザに送信することをさらに備える、請求項１に記載の方法。
【０３８４】
５．　前記アプリケーションストアにより、前記管理されたブラウザへの前記コマンドの送信後に前記管理されたブラウザが前記管理モードで動作中かどうかを再評価することをさらに備える、請求項４に記載の方法。
【０３８５】
６．　前記再評価後に、前記管理されたブラウザが前記管理モードで動作中であるとの判定に基づいて、前記アプリケーションストアにより、前記管理されたブラウザが前記アプリケーションストアの前記第１の部分にアクセスするのを許可することをさらに備える、請求項５に記載の方法。
【０３８６】
７．　前記再評価後に、前記管理されたブラウザが前記管理モードで動作中ではないとの判定に基づいて、前記アプリケーションストアにより、前記管理されたブラウザへの通知を送信することをさらに備える、請求項５に記載の方法。
【０３８７】
８．　コンピューティングデバイスであって、
少なくとも１つのプロセッサと、
前記少なくとも１つのプロセッサにより実行されたときに、前記コンピューティングデバイスに、
前記コンピューティングデバイスにより提供されたアプリケーションストアにおいて、ユーザコンピューティングデバイス上の管理されたブラウザから前記アプリケーションストアの第１の部分のアクセスへの要求を受信することと、
前記アプリケーションストアにより、前記管理されたブラウザが１つ以上のポリシーが前記管理されたブラウザに適用される管理モードで動作中かどうかを判定することであって、前記１つ以上のポリシーが前記管理されたブラウザの少なくとも１つの機能を制限するよう構成される、判定することと、
前記管理されたブラウザが前記管理モードで動作中であるとの判定に基づいて、前記アプリケーションストアにより、前記管理されたブラウザが前記アプリケーションストアの前記第１の部分にアクセスするのを許可することとを行なわせる、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、コンピューティングデバイス。
【０３８８】
９．　前記メモリは、前記少なくとも１つのプロセッサにより実行されたときに、前記コンピューティングデバイスにさらに、
前記管理されたブラウザが前記管理モードで動作中ではないとの判定に基づいて、前記アプリケーションストアにより、前記管理されたブラウザが前記アプリケーションストア

の前記第１の部分にアクセスするのを防止することを行なわせる、さらなるコンピュータ読取可能命令を記憶する請求項８に記載のコンピューティングデバイス。

【０３８９】

１０．　前記メモリは、前記少なくとも１つのプロセッサにより実行されたときに、前記コンピューティングデバイスにさらに、

前記アプリケーションストアにより、前記管理されたブラウザに前記第１の部分とは異なる前記アプリケーションストアの第２の部分へのアクセスを提供することを行なわせる、さらなるコンピュータ読取可能命令を記憶する、請求項９に記載のコンピューティングデバイス。

【０３９０】

１１．　前記メモリは、前記少なくとも１つのプロセッサにより実行されたときに、前記コンピューティングデバイスにさらに、

前記管理されたブラウザが前記管理モードで動作中ではないとの判定に基づいて、前記アプリケーションストアにより、前記管理されたブラウザに前記管理モードに入らせるよう構成されたコマンドを前記管理されたブラウザに送信することを行なわせる、さらなるコンピュータ読取可能命令を記憶する、請求項８に記載のコンピューティングデバイス。

【０３９１】

１２．　前記メモリは、前記少なくとも１つのプロセッサにより実行されたときに、前記コンピューティングデバイスにさらに、

前記アプリケーションストアにより、前記管理されたブラウザへの前記コマンドの送信後に前記管理されたブラウザが前記管理モードで動作中かどうかを再評価することを行なわせる、さらなるコンピュータ読取可能命令を記憶する、請求項１１に記載のコンピューティングデバイス。

【０３９２】

１３．　前記メモリは、前記少なくとも１つのプロセッサにより実行されたときに、前記コンピューティングデバイスにさらに、

前記再評価後に、前記管理されたブラウザが前記管理モードで動作中であるとの判定に基づいて、前記アプリケーションストアにより、前記管理されたブラウザが前記アプリケーションストアの前記第１の部分にアクセスするのを許可することを行なわせる、さらなるコンピュータ読取可能命令を記憶する、請求項１２に記載のコンピューティングデバイス。

【０３９３】

１４．　前記メモリは、前記少なくとも１つのプロセッサにより実行されたときに、前記コンピューティングデバイスにさらに、

前記再評価後に、前記管理されたブラウザが前記管理モードで動作中ではないとの判定に基づいて、前記アプリケーションストアにより、前記管理されたブラウザへの通知を送信することを行なわせる、さらなるコンピュータ読取可能命令を記憶する、請求項１２に記載のコンピューティングデバイス。

【０３９４】

１５．　実行されたときに、コンピューティングデバイスに、

前記コンピューティングデバイスにより提供されたアプリケーションストアにおいて、ユーザコンピューティングデバイス上の管理されたブラウザから前記アプリケーションストアの第１の部分のアクセスへの要求を受信することと、

前記アプリケーションストアにより、前記管理されたブラウザが１つ以上のポリシーが前記管理されたブラウザに適用される管理モードで動作中かどうかを判定することであって、前記１つ以上のポリシーが前記管理されたブラウザの少なくとも１つの機能を制限するよう構成される、判定することと、

前記管理されたブラウザが前記管理モードで動作中であるとの判定に基づいて、前記アプリケーションストアにより、前記管理されたブラウザが前記アプリケーションストアの前記第１の部分にアクセスするのを許可することとを行なわせる、記憶された命令を有す

る１つ以上の不揮発性コンピュータ読取可能媒体。
【０３９５】
１６．　実行されたときに、前記コンピューティングデバイスにさらに、
前記管理されたブラウザが前記管理モードで動作中ではないとの判定に基づいて、前記アプリケーションストアにより、前記管理されたブラウザが前記アプリケーションストアの前記第１の部分にアクセスするのを防止することを行なわせる、記憶されたさらなる命令を有する請求項１５に記載の１つ以上の不揮発性コンピュータ読取可能媒体。
【０３９６】
１７．　実行されたときに、前記コンピューティングデバイスにさらに、
前記アプリケーションストアにより、前記管理されたブラウザに前記第１の部分とは異なる前記アプリケーションストアの第２の部分へのアクセスを提供することを行なわせる、記憶されたさらなる命令を有する、請求項１６に記載の１つ以上の不揮発性コンピュータ読取可能媒体。
【０３９７】
１８．　実行されたときに、前記コンピューティングデバイスにさらに、
前記管理されたブラウザが前記管理モードで動作中ではないとの判定に基づいて、前記アプリケーションストアにより、前記管理されたブラウザに前記管理モードに入らせるよう構成されたコマンドを前記管理されたブラウザに送信することを行なわせる、記憶されたさらなる命令を有する、請求項１５に記載の１つ以上の不揮発性コンピュータ読取可能媒体。
【０３９８】
１９．　実行されたときに、前記コンピューティングデバイスにさらに、
前記アプリケーションストアにより、前記管理されたブラウザへの前記コマンドの送信後に前記管理されたブラウザが前記管理モードで動作中かどうかを再評価することを行なわせる、記憶されたさらなる命令を有する、請求項１８に記載の１つ以上の不揮発性コンピュータ読取可能媒体。
【０３９９】
２０．　実行されたときに、前記コンピューティングデバイスにさらに、
前記再評価後に、前記管理されたブラウザが前記管理モードで動作中であるとの判定に基づいて、前記アプリケーションストアにより、前記管理されたブラウザが前記アプリケーションストアの前記第１の部分にアクセスするのを許可することを行なわせる、記憶されたさらなる命令を有する、請求項１９に記載の１つ以上の不揮発性コンピュータ読取可能媒体。
【０４００】
さらなる予備的な請求項１から２０の組Ｇを以下に示す。
【０４０１】
１．　コンピューティングデバイスにより、管理されたブラウザをロードすることであって、前記管理されたブラウザは、前記管理されたブラウザに１つ以上のポリシーが適用される少なくとも１つの管理モードを提供するよう構成され、前記１つ以上のポリシーは、前記管理されたブラウザの少なくとも１つの機能を制限するよう構成された、前記管理されたブラウザをロードすることと、
前記コンピューティングデバイスにより、前記管理されたブラウザを介して１つ以上の企業リソースのアクセスへの要求を受信することと、
前記コンピューティングデバイスにより、前記要求に基づいて１つ以上の企業リソースから企業データを取得することと、
前記コンピューティングデバイスにより、１つ以上のポリシーに基づいて前記取得された企業データを制御することとを備え、
前記取得された企業データを制御することは、前記コンピューティングデバイス上の少なくとも１つの他のアプリケーションに少なくとも１つのポリシーを適用するよう構成されたモバイルリソース管理（ＭＲＭ）エージェントで管理されたブラウザを制御すること

を含む、方法。
【０４０２】
２．　前記管理されたブラウザは、少なくとも１つの企業リソースから取得されたデータのセキュリティ保護ブラウジングおよびキャッシングを提供するよう構成される、請求項１に記載の方法。
【０４０３】
３．　前記管理されたブラウザは、ポリシー管理サーバから前記ＭＲＭエージェントのために１つ以上のポリシー更新を受信するよう構成される、請求項１に記載の方法。
【０４０４】
４．　前記取得された企業データを制御することは、前記管理されたブラウザが非管理モードで動作中のときに前記取得された企業データへのアクセスを選択的にブロックすることを含む、請求項１に記載の方法。
【０４０５】
５．　前記デバイス状態情報は、前記コンピューティングデバイス上に存在する１つ以上のアプリケーションを特定する情報、前記コンピューティングデバイスにより使用される１つ以上のネットワーク接続を特定する情報、および、前記コンピューティングデバイスの現在位置を特定する情報、のうちの少なくとも１つを含む、請求項１に記載の方法。
【０４０６】
６．　前記取得された企業データを制御することは、前記取得された企業データへのアクセスを制御することを含む、請求項１に記載の方法。
【０４０７】
７．　前記取得された企業データへのアクセスを制御することは、前記取得された企業データの使用を制御することを含む、請求項６に記載の方法。
【０４０８】
８．　コンピューティングデバイスであって、
少なくとも１つのプロセッサと、
前記少なくとも１つのプロセッサにより実行されたときに、前記コンピューティングデバイスに、
管理されたブラウザをロードすることであって、前記管理されたブラウザは、前記管理されたブラウザに１つ以上のポリシーが適用される少なくとも１つの管理モードを提供するよう構成され、前記１つ以上のポリシーは、前記管理されたブラウザの少なくとも１つの機能を制限するよう構成された、前記管理されたブラウザをロードすることと、
前記管理されたブラウザを介して１つ以上の企業リソースのアクセスへの要求を受信することと、
前記要求に基づいて１つ以上の企業リソースから企業データを取得することと、
１つ以上のポリシーに基づいて前記取得された企業データを制御することとを行なわせる、コンピュータ読取可能命令を記憶するメモリとを備え、
前記取得された企業データを制御することは、前記コンピューティングデバイス上の少なくとも１つの他のアプリケーションに少なくとも１つのポリシーを適用するよう構成されたモバイルリソース管理（ＭＲＭ）エージェントで管理されたブラウザを制御することを含む、コンピューティングデバイス。
【０４０９】
９．　前記管理されたブラウザは、少なくとも１つの企業リソースから取得されたデータのセキュリティ保護ブラウジングおよびキャッシングを提供するよう構成される、請求項８に記載のコンピューティングデバイス。
【０４１０】
１０．　前記管理されたブラウザは、ポリシー管理サーバから前記ＭＲＭエージェントのために１つ以上のポリシー更新を受信するよう構成される、請求項８に記載のコンピューティングデバイス。
【０４１１】

１１．　前記取得された企業データを制御することは、前記管理されたブラウザが非管理モードで動作中のときに前記取得された企業データへのアクセスを選択的にブロックすることを含む、請求項８に記載のコンピューティングデバイス。

【０４１２】

１２．　前記デバイス状態情報は、前記コンピューティングデバイス上に存在する１つ以上のアプリケーションを特定する情報、前記コンピューティングデバイスにより使用される１つ以上のネットワーク接続を特定する情報、および、前記コンピューティングデバイスの現在位置を特定する情報、のうちの少なくとも１つを含む、請求項８に記載のコンピューティングデバイス。

【０４１３】

１３．　前記取得された企業データを制御することは、前記取得された企業データへのアクセスを制御することを含む、請求項８に記載のコンピューティングデバイス。

【０４１４】

１４．　前記取得された企業データへのアクセスを制御することは、前記取得された企業データの使用を制御することを含む、請求項１３に記載のコンピューティングデバイス。

【０４１５】

１５．　実行されたときに、コンピューティングデバイスに、

管理されたブラウザをロードすることであって、前記管理されたブラウザは、前記管理されたブラウザに１つ以上のポリシーが適用される少なくとも１つの管理モードを提供するよう構成され、前記１つ以上のポリシーは、前記管理されたブラウザの少なくとも１つの機能を制限するよう構成された、前記管理されたブラウザをロードすることと、

前記管理されたブラウザを介して１つ以上の企業リソースのアクセスへの要求を受信することと、

前記要求に基づいて１つ以上の企業リソースから企業データを取得することと、

１つ以上のポリシーに基づいて前記取得された企業データを制御することとを行なわせる、記憶された命令を有する１つ以上の不揮発性コンピュータ読取可能媒体であって、

前記取得された企業データを制御することは、前記コンピューティングデバイス上の少なくとも１つの他のアプリケーションに少なくとも１つのポリシーを適用するよう構成されたモバイルリソース管理（ＭＲＭ）エージェントで管理されたブラウザを制御することを含む、１つ以上の不揮発性コンピュータ読取可能媒体。

【０４１６】

１６．　前記管理されたブラウザは、少なくとも１つの企業リソースから取得されたデータのセキュリティ保護ブラウジングおよびキャッシングを提供するよう構成される、請求項１５に記載の１つ以上の不揮発性コンピュータ読取可能媒体。

【０４１７】

１７．　前記管理されたブラウザは、ポリシー管理サーバから前記ＭＲＭエージェントのために１つ以上のポリシー更新を受信するよう構成される、請求項１５に記載の１つ以上の不揮発性コンピュータ読取可能媒体。

【０４１８】

１８．　前記取得された企業データを制御することは、前記管理されたブラウザが非管理モードで動作中のときに前記取得された企業データへのアクセスを選択的にブロックすることを含む、請求項１５に記載の１つ以上の不揮発性コンピュータ読取可能媒体。

【０４１９】

１９．　前記デバイス状態情報は、前記コンピューティングデバイス上に存在する１つ以上のアプリケーションを特定する情報、前記コンピューティングデバイスにより使用される１つ以上のネットワーク接続を特定する情報、および、前記コンピューティングデバイスの現在位置を特定する情報、のうちの少なくとも１つを含む、請求項１５に記載の１つ以上の不揮発性コンピュータ読取可能媒体。

【０４２０】

２０．　前記取得された企業データを制御することは、前記取得された企業データへのアクセスを制御することを含む、請求項１５に記載の１つ以上の不揮発性コンピュータ読取可能媒体。

【０４２１】

さらなる予備的な請求項１から２０の組Ｈを以下に示す。

【０４２２】

１．　コンピューティングデバイスにより、管理されたブラウザをロードすることであって、前記管理されたブラウザは、前記管理されたブラウザに１つ以上のポリシーが適用される少なくとも１つの管理モードを提供するよう構成され、前記１つ以上のポリシーは、前記管理されたブラウザの少なくとも１つの機能を制限するよう構成された、前記管理されたブラウザをロードすることと、

前記コンピューティングデバイスにより、前記管理されたブラウザ内に管理された実行環境を提供することとを備え、

前記管理された実行環境は、１つ以上のウェブアプリケーションの実行を容易にするよう構成され、

前記管理された実行環境は、前記１つ以上のウェブアプリケーションへ前記１つ以上のポリシーのうちの少なくとも１つのポリシーを適用するよう構成される、方法。

【０４２３】

２．　前記管理された実行環境は、少なくとも１つのＨＴＭＬ５アプリケーションの実行を容易にするよう構成される、請求項１に記載の方法。

【０４２４】

３．　前記１つ以上のポリシーのうちの少なくとも１つのポリシーは、ポリシー管理サーバから受信される、請求項１に記載の方法。

【０４２５】

４．　前記少なくとも１つのポリシーは、前記１つ以上のウェブアプリケーションの少なくとも１つのローカルストレージリソースへのアクセスを防止するよう構成される、請求項１に記載の方法。

【０４２６】

５．　前記少なくとも１つのポリシーは、前記１つ以上のウェブアプリケーションの少なくとも１つのローカルストレージへのアクセスを選択的に有効化するよう構成される、請求項１に記載の方法。

【０４２７】

６．　前記管理された実行環境は、前記コンピューティングデバイス上のポリシー管理エージェントを前記１つ以上のウェブアプリケーションにエクスポーズするよう構成される、請求項１に記載の方法。

【０４２８】

７．　前記管理された実行環境は、アプリケーションプログラミングインタフェースを介して前記１つ以上のウェブアプリケーションに１つ以上の機能をエクスポーズするよう構成される、請求項１に記載の方法。

【０４２９】

８．　前記管理された実行環境は、前記１つ以上のウェブアプリケーションのために認証サービスを提供するよう構成される、請求項１に記載の方法。

【０４３０】

９．　前記管理された実行環境は、前記１つ以上のウェブアプリケーションにポリシーのデフォルトセットを適用するよう構成される、請求項１に記載の方法。

【０４３１】

１０．　前記管理された実行環境は、前記１つ以上のウェブアプリケーションに適用されるポリシーのセットを動的に更新するよう構成される、請求項１に記載の方法。

【０４３２】

１１．　コンピューティングデバイスであって、

少なくとも１つのプロセッサと、
前記少なくとも１つのプロセッサにより実行されたときに、前記コンピューティングデバイスに、
管理されたブラウザをロードすることであって、前記管理されたブラウザは、前記管理されたブラウザに１つ以上のポリシーが適用される少なくとも１つの管理モードを提供するよう構成され、前記１つ以上のポリシーは、前記管理されたブラウザの少なくとも１つの機能を制限するよう構成された、前記管理されたブラウザをロードすることと、
前記管理されたブラウザ内に管理された実行環境を提供することとを行なわせる、コンピュータ読取可能命令を記憶するメモリとを備え、
前記管理された実行環境は、１つ以上のウェブアプリケーションの実行を容易にするよう構成され、
前記管理された実行環境は、前記１つ以上のウェブアプリケーションへ前記１つ以上のポリシーのうちの少なくとも１つのポリシーを適用するよう構成される、コンピューティングデバイス。

【０４３３】
１２．　前記管理された実行環境は、少なくとも１つのＨＴＭＬ５アプリケーションの実行を容易にするよう構成される、請求項１１に記載のコンピューティングデバイス。

【０４３４】
１３．　前記１つ以上のポリシーのうちの少なくとも１つのポリシーは、ポリシー管理サーバから受信される、請求項１１に記載のコンピューティングデバイス。

【０４３５】
１４．　前記少なくとも１つのポリシーは、前記１つ以上のウェブアプリケーションの少なくとも１つのローカルストレージリソースへのアクセスを防止するよう構成される、請求項１１に記載のコンピューティングデバイス。

【０４３６】
１５．　前記少なくとも１つのポリシーは、前記１つ以上のウェブアプリケーションの少なくとも１つのローカルストレージへのアクセスを選択的に有効化するよう構成される、請求項１１に記載のコンピューティングデバイス。

【０４３７】
１６．　前記管理された実行環境は、前記コンピューティングデバイス上のポリシー管理エージェントを前記１つ以上のウェブアプリケーションにエクスポーズするよう構成される、請求項１１に記載のコンピューティングデバイス。

【０４３８】
１７．　前記管理された実行環境は、アプリケーションプログラミングインタフェースを介して前記１つ以上のウェブアプリケーションに１つ以上の機能をエクスポーズするよう構成される、請求項１１に記載のコンピューティングデバイス。

【０４３９】
１８．　前記管理された実行環境は、前記１つ以上のウェブアプリケーションのために認証サービスを提供するよう構成される、請求項１１に記載のコンピューティングデバイス。

【０４４０】
１９．　前記管理された実行環境は、前記１つ以上のウェブアプリケーションにポリシーのデフォルトセットを適用するよう構成される、請求項１１に記載のコンピューティングデバイス。

【０４４１】
２０．　実行されたときに、コンピューティングデバイスに、
管理されたブラウザをロードすることであって、前記管理されたブラウザは、前記管理されたブラウザに１つ以上のポリシーが適用される少なくとも１つの管理モードを提供するよう構成され、前記１つ以上のポリシーは、前記管理されたブラウザの少なくとも１つの機能を制限するよう構成された、前記管理されたブラウザをロードすることと、

前記管理されたブラウザ内に管理された実行環境を提供することと
を行なわせる、記憶された命令を有する１つ以上の不揮発性コンピュータ読取可能媒体であって、
前記管理された実行環境は、１つ以上のウェブアプリケーションの実行を容易にするよう構成され、
前記管理された実行環境は、前記１つ以上のウェブアプリケーションへ前記１つ以上のポリシーのうちの少なくとも１つのポリシーを適用するよう構成される、１つ以上の不揮発性コンピュータ読取可能媒体。

【図１】

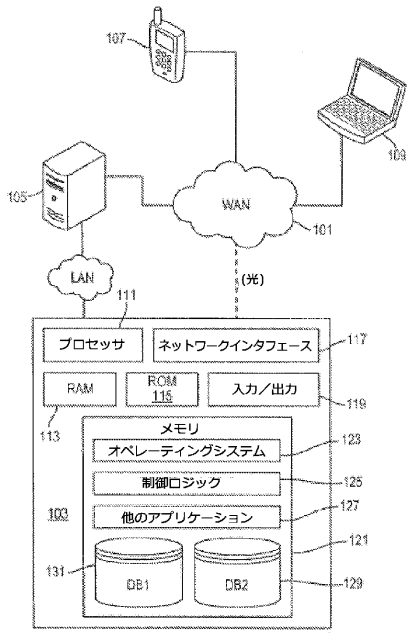

図１

【図２】

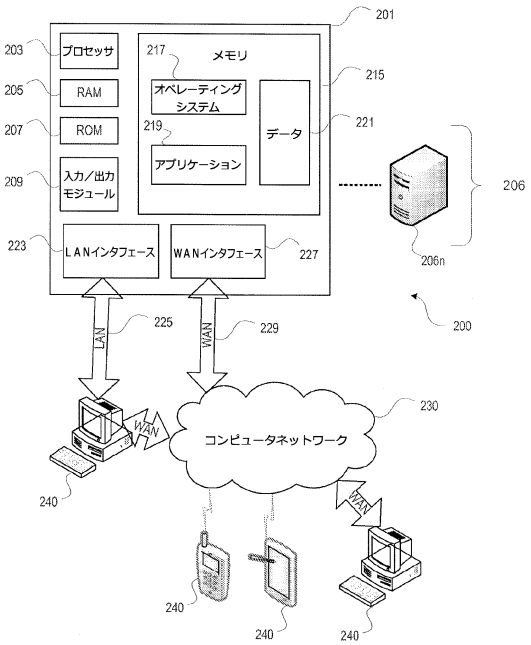

図２

【図３】

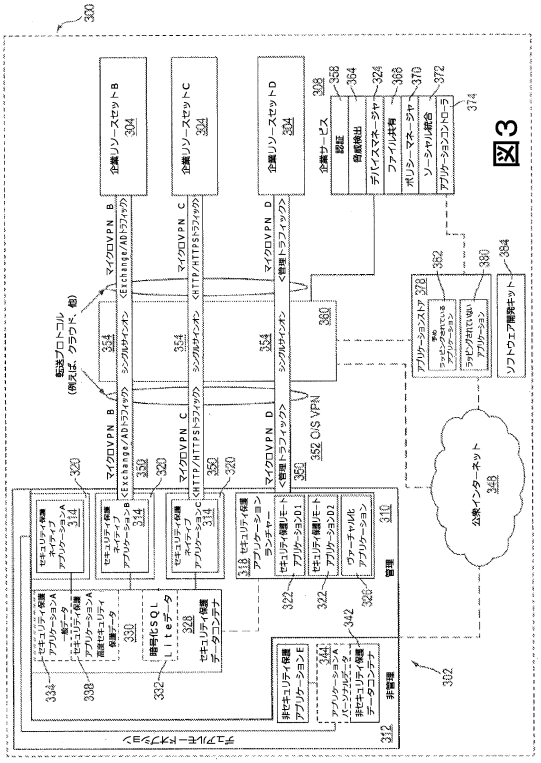

図3

【図４】

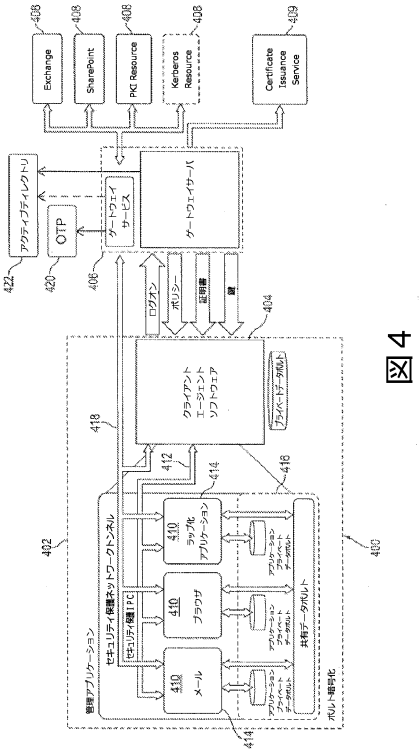

図4

【図５】

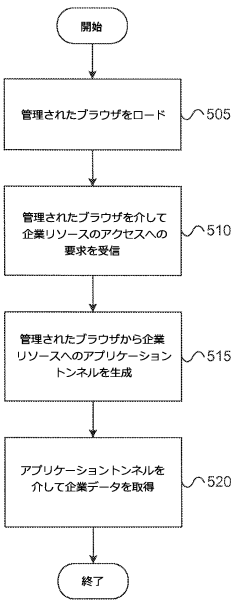

図5

【図６】

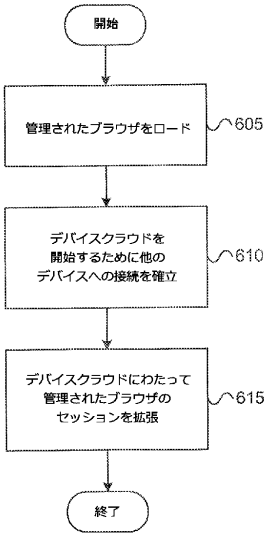

図6

【図７】

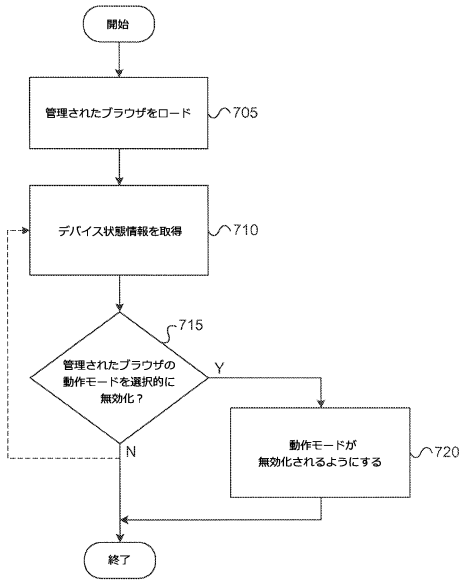

図７

【図８】

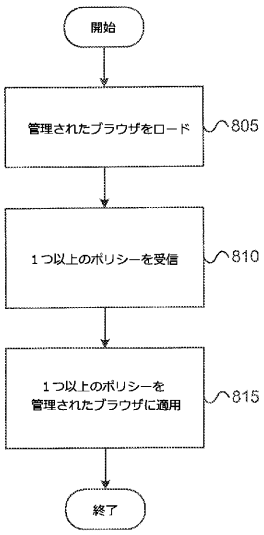

図８

【図９】

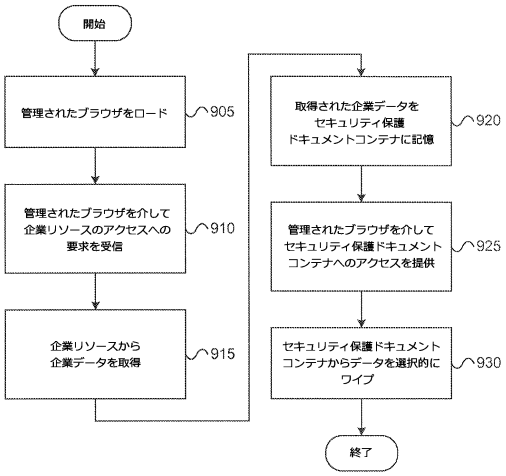

図９

【図１０】

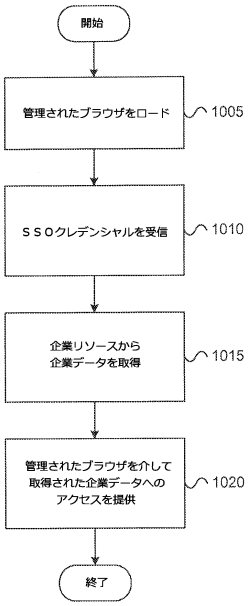

図１０

【図１１】

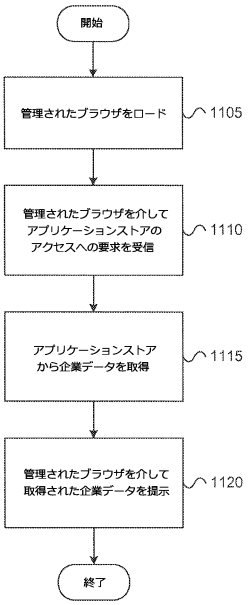

図11

【図１２】

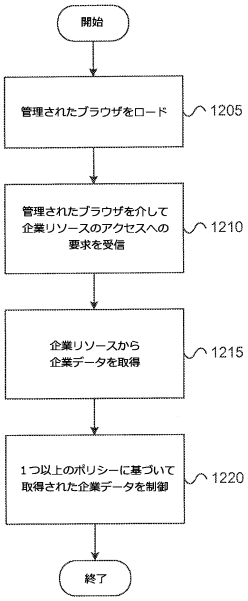

図12

【図１３】

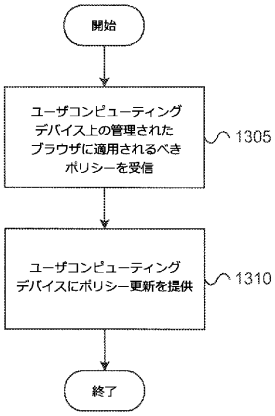

図13

【図１４】

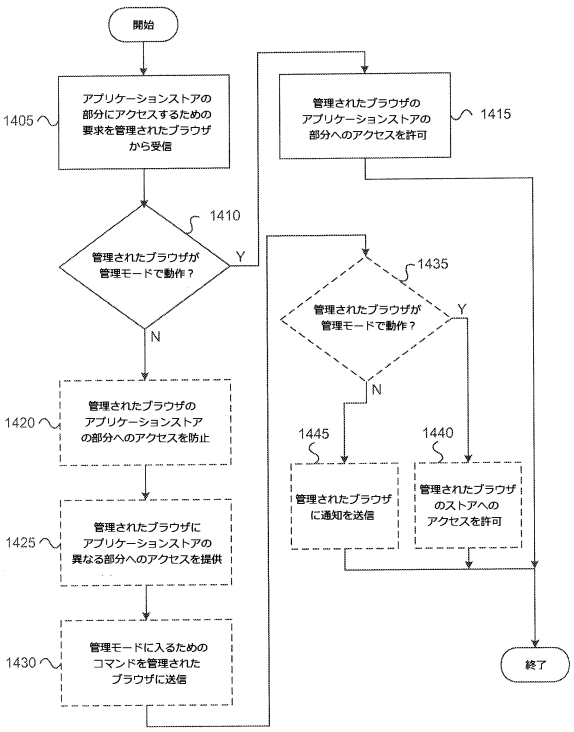

図１４

【図１５】

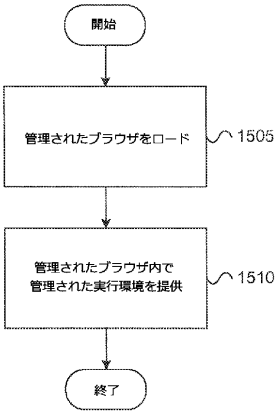

図15

フロントページの続き

(31)優先権主張番号　14/040,831
(32)優先日　平成25年9月30日(2013.9.30)
(33)優先権主張国　米国(US)

審査官　金木　陽一

(56)参考文献　特開平１１－２０５３８０（ＪＰ，Ａ）
特開２００６－１５５５２２（ＪＰ，Ａ）
特開２００９－８０８１４（ＪＰ，Ａ）
特開２０１３－５８２２３（ＪＰ，Ａ）
特開２０１３－２１４２１９（ＪＰ，Ａ）
国際公開第２００９／１５７４９３（WO，Ａ１）
米国特許第８３４７３４９（ＵＳ，Ｂ１）
米国特許出願公開第２００４／０１９８４５６（ＵＳ，Ａ１）
米国特許出願公開第２００６／０１３６５７６（ＵＳ，Ａ１）
米国特許出願公開第２０１２／０３１１６９５（ＵＳ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／６２
Ｇ０６Ｆ　２１／１２