(19)日本国特許庁(JP)　(12)公 開 特 許 公 報(A)　(11)特許出願公開番号

特開2016-201150

(P2016-201150A)

(43)公開日　平成28年12月1日(2016.12.1)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/33	(2013.01)	G06F	21/33		5B376
G06F 9/445	(2006.01)	G06F	9/06	650C	
G06F 21/62	(2013.01)	G06F	21/62		

審査請求 有　請求項の数 12　ＯＬ　外国語出願　（全 24 頁）

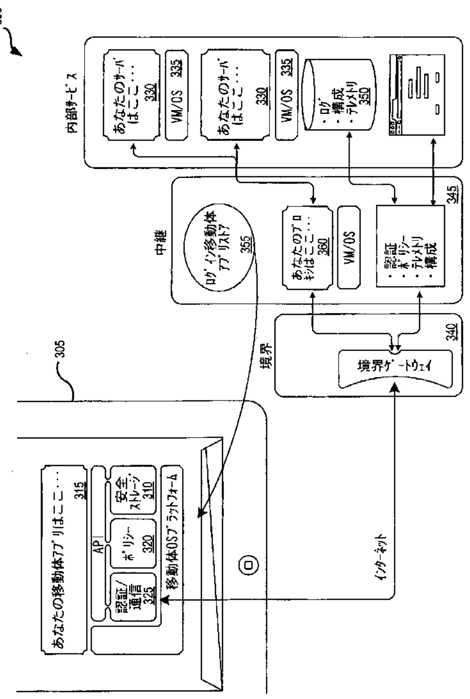
(21)出願番号　特願2016-167496(P2016-167496)
(22)出願日　平成28年8月30日(2016.8.30)
(62)分割の表示　特願2015-503684(P2015-503684)の分割
原出願日　平成25年4月1日(2013.4.1)
(31)優先権主張番号　61/618,511
(32)優先日　平成24年3月30日(2012.3.30)
(33)優先権主張国　米国(US)
(31)優先権主張番号　61/806,763
(32)優先日　平成25年3月29日(2013.3.29)
(33)優先権主張国　米国(US)

(71)出願人　516245070
シンクロノス　テクノロジーズ　インコーポレイテッド
アメリカ合衆国　ニュージャージー州　０８８０７　ブリッジウォーター　クロッシング　ブールバード　２００
(74)代理人　100086771
弁理士　西島　孝喜
(74)代理人　100088694
弁理士　弟子丸　健
(74)代理人　100094569
弁理士　田中　伸一郎
(74)代理人　100067013
弁理士　大塚　文昭

最終頁に続く

(54)【発明の名称】安全移動体フレームワーク

(57)【要約】
【課題】移動体デバイス上で走るアプリケーションを企業内サービスへ安全に接続する安全移動体フレームワークのためのシステム及び方法を提供する。
【解決手段】様々な実施形態は、移動体デバイスとゲートウェイからアクセスされるエンドポイントサービスの間でのデータ及び通信を保障する、信頼できる許可、認証、異常検知、不正検知、及びポリシー管理の機構を提供している。幾つかの実施形態は、サーバ側及びクライアント側の機密保護機構、ユーザー／アプリケーション／デバイスのエンドポイントサービスへの束縛、並びに複数の暗号化機構、の一体化を提供している。例えば安全移動体フレームワークは、移動体デバイス上の安全コンテナ、安全ファイル、仮想ファイルシステムパーティション、多レベル認証手法（例えば、移動体デバイス上の安全コンテナにアクセスする場合と企業サービスにアクセスする場合）、及びサーバ側の不正検知システムを提供する。
【選択図】図３



【特許請求の範囲】

【請求項１】

企業と関連付けられるゲートウェイにて、遠隔デバイスからの、前記企業によって提供されているサービスにアクセスするための認証要求を、受信する段階であって、当該要求は前記遠隔デバイス上で走る企業管理型アプリケーションから生じている、認証要求を受信する段階と、

前記遠隔デバイスがアクセスすることを要求してきている、前記企業によって提供されている前記サービスに基づいて、フレームワーク認証トークン及び機密保護ポリシーを生成する段階と、

前記フレームワーク認証トークン及び前記機密保護ポリシーを前記遠隔デバイスへ送信する段階であって、前記遠隔デバイスは前記サービスへ接続するための接続要求を生成する前に前記機密保護ポリシーの順守を保証することになる、段階と、

前記遠隔デバイスから、前記フレームワーク認証トークン及び前記機密保護ポリシーに基づく前記接続要求を受信する段階であって、サービス認証部が前記遠隔デバイスは前記サービスにアクセスすることを許可されているかどうかを判定することになる、段階と、を備えている方法。

【請求項２】

ユーザー識別子及びアプリケーション識別子に基づいてユーザー束縛トークンを生成する段階を更に備えている、請求項１に記載の方法。

【請求項３】

前記フレームワーク認証トークンを生成する段階は、前記企業認証トークン、前記ユーザー束縛トークン、及びフレームワーク認証トークン有効期限、を束縛する段階を含んでいる、請求項２に記載の方法。

【請求項４】

前記フレームワーク認証トークンにデジタル署名する段階を更に備えている、請求項３に記載の方法。

【請求項５】

オペレーティングシステム完全性チェックを遂行して、期待されるオペレーティングシステム完全性が存在しているかどうかを判定する段階と、

前記期待されるオペレーティングシステム完全性が存在していない場合に前記遠隔デバイスの前記ゲートウェイへのアクセスを拒否する段階と、を更に備えている、請求項１に記載の方法。

【請求項６】

前記遠隔デバイスは、前記サービスに関係のあるデータを記憶するための安全コンテナを含んでおり、前記機密保護ポリシーは、前記アプリケーション及び前記安全コンテナのためのアクセス制御を指し示す要件のセットを提供している、請求項１に記載の方法。

【請求項７】

前記フレームワーク認証トークンは、前記安全コンテナに記憶される、請求項６に記載の方法。

【請求項８】

前記安全コンテナへのアクセスは、ユーザー信用証明書の妥当性確認成功及びオペレーティングシステム完全性チェック成功に依存している、請求項６に記載の方法。

【請求項９】

前記機密保護ポリシーは、前記サービスに基づくパスワード構造及びパスワード存続期間を識別している、請求項１に記載の方法。

【請求項１０】

前記企業管理型アプリケーションと前記サービスの間の対話を監視する段階と、

１つ又はそれ以上の不正ポリシーの違反に際し、高位の認証要求又は前記ゲートウェイ及び前記サービスへのアクセスの中止を生成する段階と、を更に備えている、請求項１に記載の方法。

【請求項１１】
前記サービスは、ｅメールサービス、取引サービス、支払処理サービス、顧客関係管理サービス、在庫システムサービス、ビジネスインテリジェンスサービス、保健サービス、学生情報サービス、又は予約サービス、を含んでいる、請求項１に記載の方法。
【請求項１２】
前記サービスは、安全サービス又は機密情報を内包するサービスを含んでいる、請求項１に記載の方法。
【請求項１３】
企業によって管理されている１つ又はそれ以上のアプリケーションを記憶させている遠隔デバイスの当該企業のサービスへのアクセスを提供するように構成されているゲートウェイと、
ゲートウェイがアクセスできる認証部であって、ユーザーが前記企業にアクセスするのを許可されているかどうかを判定するように、及び前記１つ又はそれ以上のアプリケーションの管理に関してポリシーを構築するように、構成されている認証部と、
ゲートウェイがアクセスできるトークン生成部であって、前記企業によって管理されている前記１つ又はそれ以上のアプリケーションと前記サービスの間に安全接続を作成するための１つ又はそれ以上のトークンを生成するように構成されているトークン生成部と、
前記ポリシーを前記遠隔デバイスへ通信するように構成されている通信モジュールと、を備えているシステム。
【請求項１４】
前記企業の前記サービスのうちのどれを前記１つ又はそれ以上のアプリケーションと接続するべきかを確定するように構成されている発見サービスを更に備えている、請求項１３に記載のシステム。
【請求項１５】
前記発見サービスが前記１つ又はそれ以上のアプリケーションと接続するのに前記企業の前記サービスのうちのどれを選択するかは、前記ユーザー及び関連付けられる特権のセットに基づいている、請求項１４に記載のシステム。
【請求項１６】
前記トークン生成部は、企業認証トークン、ユーザー束縛トークン、及びフレームワーク認証トークンを生成する、請求項１３に記載のシステム。
【請求項１７】
フレームワーク認証トークンは、前記企業認証トークン、前記ユーザー束縛トークン、及びフレームワーク認証トークン有効期限、を含んでいる、請求項１６に記載のシステム。
【請求項１８】
前記ユーザー束縛トークンは、ユーザー識別子、デバイス識別子、デバイス型式識別子、及びアプリケーション群識別子、に基づいて生成されている、請求項１６に記載のシステム。
【請求項１９】
前記システムは、前記遠隔デバイスと前記サービスの間の活動を監視し、異常表示を生成するように構成されている異常検知部を更に備えており、前記異常検知部は、更に、異常表示への反応を判定する、前記請求項１３に記載のシステム。
【請求項２０】
前記ゲートウェイは、それぞれ単独の認証プロトコル及び活動ロギングを提供している複数のレベルを含んでいる、請求項１３に記載のシステム。
【請求項２１】
ゲートウェイにて、開始デバイスからの、前記開始デバイス上で走る企業管理型アプリケーションと企業サービスの間のサービス接続を確立するための要求を、受信する段階であって、当該要求はエンドユーザーと関連付けられる認証信用証明書を含んでいる、要求を受信する段階と、

フレームワーク認証トークンを生成する段階と、
前記フレームワーク認証トークンを前記開始デバイスへ送信する段階であって、前記開始デバイスは、受信し次第、前記認証トークンに基づいてサービス接続要求を開始することになる、段階と、
前記サービス接続要求の妥当性確認が成功し次第、前記企業サービスと前記開始デバイスの間に安全接続を作成する段階と、を備えている方法。
【請求項２２】
前記開始デバイスへ送信される何れかのデータは、前記企業管理型アプリケーションしかアクセスできない安全コンテナ内に記憶される、請求項２１に記載の方法。
【請求項２３】
前記開始デバイス及び前記企業管理型アプリケーションについての情報を収集する段階を更に備えている、請求項２１に記載の方法。
【請求項２４】
前記企業管理型アプリケーションを管理するに当たり前記開始デバイスが制定するべきポリシーを確定する段階を更に備えている、請求項２１に記載の方法。
【請求項２５】
前記企業が前記開始デバイスは前記ポリシーを制定しようとしていると確認できなければ、前記安全接続は作成されなくなってしまう、請求項２４に記載の方法。
【発明の詳細な説明】
【技術分野】
【０００１】
（関連出願の相互参照）
本願は、２０１２年3月３０日出願の米国仮特許出願第６１／６１８，５１１号及び２０１３年3月２９日出願の米国仮特許出願第６１／８０６，７６３号に対する優先権を主張し、両出願の内容全体をここに参考文献としてあらゆる目的に援用する。
【０００２】
本発明の様々な実施形態は、概括的には、移動体デバイスに関する。より厳密には、本発明の幾つかの実施形態は、移動体デバイス上で走るアプリケーションを企業内サービスへ安全に接続するための安全移動体フレームワークに関する。
【背景技術】
【０００３】
多くの会社又は企業は、移動体デバイス（スマートフォン、タブレット、など）を従業員へ供与しているか又は従業員が自分の移動体デバイスを持ち込むことを容認している。しかしながら、従業員が会社内のサービスに移動体デバイスを通じてアクセスできるようにしていることで、会社が潜在的な機密保護侵害に曝されることが増加してきている。例えば、従業員が自分の移動体デバイスを紛失すれば、許可されていない当事者が電話機上で安全確保されていないデータを読み出し、そして恐らくは会社内のサービスにアクセスしてしまうかもしれない。別の例として、従業員が会社を去り、移動体デバイスを返還しないなら、元従業員がデバイス上に又は会社内に記憶されている機密データにアクセスしてしまう可能性も依然としてある。
【０００４】
この種の許可されていないアクセスを抑制するために、多くの会社は、移動体デバイスの制御を拘束する移動体デバイス管理（ＭＤＭ）ポリシーを使用しており、それにより、企業内サービスへ接続する可能性のある移動体デバイスについての潜在的機密保護リスクの低減を図っている。企業によって設定されるＭＤＭポリシーは、移動体デバイスの構成設定の管理を通じてデータを制御及び保護する。構成設定を管理するために、オーバー・ディ・エア・プログラミング（ＯＴＡ）ケイパビリティが使用されることが多い。ＯＴＡケイパビリティの使用は、企業が、単一の移動体デバイス又は一団の移動体デバイス全体を遠隔的に構成すること、ソフトウェア及びＯＳ更新を送信すること、及びデバイスが紛失又は盗難された場合などにデバイス上に記憶されているデータを保護するためにデバイ

スを遠隔的にロック及びワイプすること、を行えるようにしている。

【０００５】

しかしながら、ＭＤＭポリシーによって課される拘束は、個人的立場でもデバイスを使用しているユーザーにとっては煩わしいこともある。例えば、ＭＤＭポリシーは、移動体デバイスに、自動ロックし、そして移動体デバイスがロック解除される前にユーザーに特定の特徴のセットを有するパスワードを提供するよう入力を促すこと、を求めている場合がある。ユーザーは、これらの拘束がうっとうしいと感じているかもしれない。この様に、従来の移動体デバイス管理には多数の課題及び非効率が生じている。

【先行技術文献】

【特許文献】

【０００６】

【特許文献１】米国仮特許出願第６１／６１８，５１１号

【特許文献２】米国仮特許出願第６１／８０６，７６３号

【発明の概要】

【０００７】

移動体デバイス上で走るアプリケーションを企業内サービス（例えば、ｅメールサービス、取引サービス、又は予約サービス）へ安全に接続することのできる安全移動体フレームワークのためのシステム及び方法が記載されている。幾つかの実施形態では、遠隔デバイスからの、企業によって提供されるサービスにアクセスするための認証要求は、企業と関連付けられるゲートウェイにて受信されるようになっている。要求は、遠隔デバイス上で走る企業管理型アプリケーション(enterprise managed application)から生じるようになっている。フレームワーク認証トークン及び機密保護ポリシー（例えば、パスワード構造、パスワード存続期間、アプリケーション及び／又は安全データコンテナについてのアクセス制御、など）が生成されるようになっている。

【０００８】

機密保護ポリシーは、企業によって提供されているサービスであって遠隔デバイスがアクセスすることを要求してきているサービスに基づくものとされている。次いでフレームワーク認証トークン及び機密保護ポリシーが遠隔デバイスへ送信され、企業内サービスへ接続するための接続要求を生成する前に機密保護ポリシーの順守が保証されるようにする。接続要求は、フレームワーク認証トークン及び機密保護ポリシーに基づくものとされている。サービス認証部(service authenticator)は、遠隔デバイス上で走るアプリケーションがサービスにアクセスすることを許可されているかどうかを判定する。幾つかの実施形態は、企業管理型アプリケーションとサービスの間の対話を監視する。移動体デバイス及び／又はゲートウェイにて１つ又はそれ以上の不正ポリシーの違反が検知されるや、高位の認証要求が生成されるようになっている。

【０００９】

幾つかの実施形態では、開始デバイス上で走る企業管理型アプリケーションと企業サービスの間のサービス接続を確立するための要求が、開始デバイスから受信されるようになっている。要求は、エンドユーザーと関連付けられる認証信用証明書を含んでいる。フレームワーク認証トークンが生成され、開始デバイスへ送信されると、開始デバイスは、それを受信し次第、認証トークンに基づいてサービス接続要求を開始する。サービス接続要求の妥当性確認（例えば、許可及び認証）が成功し次第、企業サービスと開始デバイスの間に安全接続が作成されることになる。記憶された接続を使用して開始デバイスへ送信される何れかのデータは、企業管理型アプリケーションしかアクセスできない安全コンテナ内に記憶させることができる。

【００１０】

本発明の実施形態は、更に、１つ又はそれ以上のプロセッサにここに記載の方法、方法の変型、及び他の動作を遂行させる命令のセットを格納するコンピュータ可読記憶媒体を含んでいる。

【００１１】

様々な実施形態では、システムは、ゲートウェイ、認証部、トークン生成部、通信モジュール、発見サービス、及び／又は不正検知モジュール、を含むことができる。ゲートウェイは、企業のサービスへの遠隔デバイスアクセスを提供するように構成されていてもよい。幾つかの実施形態では、ゲートウェイは、それぞれ単独の認証プロトコル及び活動ロギングを提供している複数のレベルを含んでいてもよい。遠隔デバイスは、デバイス上に企業によって管理されている１つ又はそれ以上のアプリケーションを記憶させておくことができる。認証部は、ユーザーが企業にアクセスすることを許可されているかどうかを判定するように、及び１つ又はそれ以上のアプリケーションの管理に関してポリシーを構築するように、構成されていてもよい。

【００１２】

トークン生成部は、企業によって管理されている１つ又はそれ以上のアプリケーションとサーバの間に安全接続を作成するための１つ又はそれ以上のトークン（例えば、認証トークン、ユーザー束縛トークン、及び／又はフレームワーク認証トークン）を生成するように構成されていてもよい。トークンは様々な識別子に基づくものとすることができ、例えば、限定するわけではないが次のもの、即ち、ユーザー識別子、デバイス識別子、デバイス型式識別子、アプリケーション群識別子、など、であってもよい。トークンには、他のトークンの束縛を含んでいるものもあろう。例えば、１つの実施形態では、フレームワーク認証トークンは、企業認証トークン、ユーザー束縛トークン、及び／又はフレームワーク認証トークン有効期限、に基づくものであってもよい。幾つかの実施形態では、トークンの１つ又はそれ以上は、当該トークンが改ざん又は改変された場合にシステムが検知できるように、暗号学的に安全確保（例えば、デジタル署名）されるようになっている。

【００１３】

通信モジュールは、ポリシーを遠隔デバイスへ通信するように構成されていてもよい。発見サービスは、企業のサービスのうちのどれを１つ又はそれ以上のアプリケーションと接続するべきかを確定するように構成されていてもよい。異常検知部は、遠隔デバイスとサーバの間の活動を監視し活動での異常の表示を生成するように構成されていてもよい。例えば、異常検知部は、ユーザーのＩＰ速度、ログイン試行の失敗、など、を監視するようになっていてもよい。

【００１４】

複数の実施形態が開示されているが、本発明の例示的な実施形態を示し説明している次の詳細な説明から当業者には本発明の更に他の実施形態が自明となるであろう。認識されてゆく様に、本発明は、各種態様に修正の余地があり、修正はどれも本発明の範囲から逸脱せずになされるものである。従って、図面及び詳細な説明は、本質的に説明目的と見なされるべきであって限定を課すものと見なされるべきではない。

【００１５】

本発明の実施形態を、添付図面の使用を通じて説明及び解説してゆく。

【図面の簡単な説明】

【００１６】

【図１】本発明の幾つかの実施形態を利用することのできるネットワークベース環境の一例を示している。

【図２】本発明の１つ又はそれ以上の実施形態による、企業管理型アプリケーションと企業サービスの間に束縛を作成するための例示としての動作のセットに係る流れ図である。

【図３】本発明の様々な実施形態により使用することのできる安全フレームワークのための全体としてのアーキテクチャを示している。

【図４】本発明の幾つかの実施形態による、企業管理型アプリケーションを許可するための例示としての動作のセットを示す流れ図である。

【図５】本発明の１つ又はそれ以上の実施形態による、企業サービスと遠隔デバイス上で走る企業管理型アプリケーションの間に安全チャネルを作成するための例示としての動作のセットを示す流れ図である。

【図６】本発明の様々な実施形態と共に使用することのできる安全移動体フレームワーク

上に築かれたアプリケーションの一例である。
【図７】本発明の幾つかの実施形態による、企業内サービスにアクセスする遠隔デバイスを示している。
【図８】本発明の１つ又はそれ以上の実施形態による、デバイスアプリケーションと企業の間の初期認証フローを示すシーケンス線図である。
【図９】本発明の様々な実施形態による、デバイスアプリケーションと企業の間の連続的な認証フローを示すシーケンス線図である。
【図１０】本発明の幾つかの実施形態を利用することのできるコンピュータシステムの一例を示している。
【００１７】
図面は必ずしも縮尺を合わせて描かれているわけではない。例えば、図中の要素のうちの幾つかの寸法は、本発明の実施形態の理解を高めるうえで助けとなるように拡大又は縮小されていることもある。同様に、幾つかの構成要素及び／又は幾つかの動作は、本発明の実施形態のうちの幾つかを論じることを目的に、異なったブロックへ別けられていることもあれば単一ブロックへ組み合わされていることもある。また、本発明は、様々な修正及び代替形態を受ける余地があるが、図面には特定の実施形態が一例として示されており、以下に詳細に説明されている。但し、本発明は、当該発明を説明されている特定の実施形態に限定するつもりはない。そうではなく、本発明は、付随の特許請求の範囲によって定義される本発明の範囲内に入るあらゆる修正物、等価物、及び代替物を網羅することを意図している。
【発明を実施するための形態】
【００１８】
本発明の様々な実施形態は、概括的には、移動体デバイス上で走るアプリケーションを企業内サービスへ安全に接続することのできる安全移動体フレームワークに関する。企業によって提供されているサービスの幾つかの例には、限定するわけではないが、ｅメールサービス、取引サービス、支払処理サービス、顧客関係管理サービス、在庫システムサービス、ビジネスインテリジェンスサービス、保健サービス、学生情報サービス、予約サービス、安全サービス、及び／又は機密情報を内包する他のサービス、が含まれる。幾つかの実施形態によれば、安全移動体フレームワークは、ソフトウェア開発者に、非企業移動体デバイス上に安全アプリケーションを築く能力を提供するソフトウェアライブラリ及びサービス構成要素の集まりを提供している。安全移動体フレームワークは、ファイアウォール制御されているコンテンツ、サービス、及び公共ネットワークからのＤＭＺ型式アーキテクチャ手段を介したネットワーク、を有する企業によって連係して使用されることが可能である。結果として、企業の既存の認証及び許可システムの多くが利用できるようになる。クライアントライブラリ及びサーバライブラリを利用又は拡張して、クライアントアプリケーションとサーバアプリケーションの両方で安全な記憶及び通信が提供されるようにすることができる。
【００１９】
内部ポリシー又は内部規定を通じて、確実に企業のコンテンツ及び通信が保護され、管理され、監視されるようにすることを必要としている企業は、多数存在する。通常は、企業によって管理されるデバイスについては、前述の制御要件はデバイス及びオペレーティングシステム（ＯＳ）管理を通じて直接実施されている。また一方で、企業によって管理されていないデバイス及び企業ネットワークへ直接接続することがあってはならないデバイスについては、確実に同じ制御がこれらの非管理デバイス上で走る企業アプリケーションに適用されるようにする必要性がある。
【００２０】
様々な実施形態によれば、安全移動体フレームワークは、企業内サービスを接続し利用するために以下の特徴のうちの１つ又はそれ以上を提供することができ、即ち、１）企業コンテンツをデバイス上に保護された方式で記憶する機構であって、それにより、企業コンテンツには、場合によってはオフラインの、許可されたユーザーしかアクセスできなく

なり、企業コンテンツは企業ポリシーを通じてしか管理できなくなる、ようにする機構、２）ゲートウェイに対する認証（即ち、フレームワーク認証）及び企業サービスに対する認証（即ち、企業認証）の複数の認証を提供し、許可されている場合にはそれらの企業サービスへの安全接続を提供し、サービス毎にアクセスを企業ポリシーを通じて管理する機構、３）接続されたアプリケーション及びそれらの従属サービスを管理及びサポートする機構、４）好ましくない若しくは安全でないオペレーティングシステム環境を動的に検知し、多段処理（例えば、ポリシーを評価すること、プログラムの問合せ、ＯＳの問合せ、及び／又はクライアント環境及び／又はサーバ環境での他のチェックを遂行すること）を通じて管理する機構、のうちの１つ又はそれ以上を提供することができる。

【００２１】

ゲートウェイは、認証のために使用できる１つ又はそれ以上のトークンを生成することができる。例えば、幾つかの実施形態では、単要素又は多要素信用証明書を表現する企業認証トークン（ＥＡＴ）が生成されるようになっており、トークンは所与の会社に関して認証するに当たりあたかも当該単要素又は多要素信用証明書が提示されているかの如く或る有限期間に亘って使用できる。１つ又はそれ以上の実施形態ではユーザー束縛トークン（ＵＢＴ）も使用されている。ＵＢＴは、ユーザー（ｉｄ）、デバイス（ｉｄ）、デバイスの型式、及びアプリ群、を合体させた固有表現であるとしてもよい。加えて、フレームワーク認証トークン（ＦＡＴ）が様々な実施形態で使用されている。ＦＡＴは、フレームワークに関して認証するのに使用されるＥＡＴ、ＵＢＴ、及び有効期限を束縛することによって作成されていてもよい。ＦＡＴをこの様に構築することの１つの利点は、詳細事項が許可されていない当事者によって改ざんされ得ないことである。

【００２２】

幾つかの実施形態では、安全移動体フレームワークのクライアント構成要素及びサーバ構成要素が、クライアントアプリケーションのための動作環境の完全性を検知するのに使用されている。クライアントアプリケーションが管理されていないオペレーティングシステム環境内で実行されようとしていることを考えれば、当該環境が安全でないと見なされるかどうかを、あらんかぎりの能力を尽くして確かめる必要があろう。

【００２３】

次に続く説明では、本発明の実施形態を十二分に理解してもらうために、解説を目的として数多くの特定の詳細事項が述べられている。とはいえ、本発明の実施形態はこれらの特定の詳細事項の幾つか無しに実践することもできることが当業者には自明であろう。

【００２４】

便宜上、本発明の実施形態は、専用の企業ベースのセットアップに関連付けて説明されているが、本発明の実施形態は、クラウドベースのモデルの様な他の様々な運用モデルにも等しく適用できる。また、ここに紹介されている技法は、特殊用途ハードウェア（例えば、回路構成）として、ソフトウェア及び／又はファームウェアに関して適切にプログラムされるプログラム可能回路構成として、又は特殊用途回路構成とプログラム可能回路構成の組合せとして、具現化させることができる。よって、実施形態は、処理を遂行するようコンピュータ（又は他の電子デバイス）をプログラムするのに使用することのできる命令を記憶させた機械可読媒体を含み得る。機械可読媒体には、限定するわけではないが、フロッピーディスケット、光ディスク、コンパクトディスク読み出し専用メモリ（ＣＤ－ＲＯＭ）、光磁気ディスク、ＲＯＭ、ランダムアクセスメモリ（ＲＡＭ）、消去可能プログラム可能読み出し専用メモリ（ＥＰＲＯＭ）、電気的消去可能プログラム可能読み出し専用メモリ（ＥＥＰＲＯＭ）、特定用途向け集積回路（ＡＳＩＣ）、磁気式又は光学式カード、フラッシュメモリ、又は電子的命令を記憶するのに適する他の型式の媒体／機械可読媒体が含まれよう。

用語法

【００２５】

本願全体を通して使用される用語、略語、及び語句の簡単な定義を以下に示す。

【００２６】

「接続されている」又は「連結されている」という用語及び関連語は、動作上の意味で使用されており、必ずしも直接の物理的接続又は連結に限定されるわけではない。よって、例えば、２つのデバイスは、直接に連結されていることもあれば、１つ又はそれ以上の中継の媒体又はデバイスを介して連結されていることもある。別の例として、デバイス（例えば、移動体デバイス、サーバ機械、など）は、何らの物理的接続も互いと共有していないにもかかわらず互いとの間で情報を受け渡すことのできるやり方で連結されていることがある。ここに提供されている開示に基づき、当業者には、上記定義に則った接続又は連結の様々な存在様式が認知されるであろう。

【００２７】

「幾つかの実施形態では」、「幾つかの実施形態によれば」、「示されている実施形態では」、「他の実施形態では」、など、の語句は、概して、当該語句の次にくる特定の特徴、構造、又は特性が、本発明の少なくとも１つの実施形に含まれている、及び１つより多くの実施形に含まれていることもあり得る、ということを意味する。加えて、その様な語句は、必ずしも同じ実施形態を又は異なった実施形態を指しているとは限らない。

【００２８】

本明細書が、或る構成要素又は特徴が、「含まれていることもある」、「含まれていてもよい」、「含まれ得る」、「含まれよう」、又は或る特性を「有していることもある」、「有していてもよい」、「有し得る」、「有していよう」と叙述している場合、当該特定の構成要素又は特徴は、含まれていること又は当該特性を有していることが必須とされているわけではない。

【００２９】

「モジュール」という用語は、広義に、ソフトウェア、ハードウェア、ファームウェア、又はサービス（又はそれらからなる何らかの組合せ）構成要素を指す。モジュールは、典型的には、有用なデータ又は他の出力を指定された（単数又は複数の）入力を使用して生成することのできる機能的構成要素である。モジュールは、内蔵型であってもよいし、内蔵型でなくてもよい。アプリケーションプログラム（「アプリケーション」とも呼ばれる）が１つ又はそれ以上のモジュールを含んでいることもあれば、モジュールが１つ又はそれ以上のアプリケーションプログラムを含んでいることもある。

全体としての説明

【００３０】

図１は、本発明の幾つかの実施形態を利用することのできるネットワークベースの環境１００の一例を示している。図１に示されている様に、様々な企業管理型アプリケーション１１０Ａ－１１０Ｎがユーザーデバイス１２０Ａ－１２０Ｎ上で走っていよう。本発明の様々な実施形態によれば、ユーザーデバイス１２０Ａ－１２０Ｎは、企業によって管理されていてもよいし、管理されていなくてもよい。ユーザーデバイス１２０Ａ－１２０Ｎは、企業内サービス及びデータにアクセスするのに使用することのできる企業管理型アプリケーション１１０Ａ－１１０Ｎを含んでいよう。ユーザーデバイス１２０Ａ－１２０Ｎは、ネットワーク１４０を使用して企業内サービスからの情報を申し込み、読み出すことがある。ユーザーデバイス１２０Ａ－１２０Ｎは、ＩＯＳ（登録商標）又はＡＮＤＲＯＩＤ（登録商標）の様な、デバイスのネイティブオペレーティングシステム上で走っているアプリケーションプログラミングインターフェース（ＡＰＩ）を通じて、様々な企業サービスと対話することができる。

【００３１】

ゲートウェイ１３０は、企業管理型アプリケーション１１０Ａ－１１０Ｎ及びユーザーデバイス１２０Ａ－１２０Ｎのアクセスを管理する。ゲートウェイ１３０は、企業管理型アプリケーション１１０Ａ－１１０Ｎと企業によって提供されているビジネス特定サービスの間の信頼関係を確認し確立するのに使用することができる。例えば、幾つかの実施形態では、企業管理型アプリケーション１１０Ａ－１１０Ｎによって最初に提出されるデータ及び要求は、デバイスとゲートウェイ１３０の間をネットワーク１４０を介して転送される。ゲートウェイ１３０がデバイスの機密保護に納得したら、ゲートウェイ１３０は、

アプリケーション管理プラットフォーム１５０内の何れかのビジネス特定サービス及び企業サービス１６０へのチャネルを開く。ゲートウェイ１３０及びアプリケーション管理プラットフォーム１５０内のサービスは、機密保護及びチェックの複数の独立した層を有していてもよい。

【００３２】

ユーザーデバイス１２０Ａ－１２０Ｎは、ユーザー入力を受信することができると共にネットワーク１４０を介してデータを送信及び／又は受信することのできる何れかのコンピューティングデバイスとすることができる。１つの実施形態では、ユーザーデバイス１２０Ａ－１２０Ｎは、パーソナルデジタルアシスタント（ＰＤＡ）、移動体電話、スマートフォン、タブレット、着用型式の移動体コンピュータ、身体装着型コンピュータ、又は類似のデバイスの様な、コンピュータ機能性を有する何れかのデバイスとすることができる。ユーザーデバイス１２０Ａ－１２０Ｎは、有線式及び／又は無線式の通信システムを使用するネットワーク１４０であってローカルエリアネットワーク及び／又はワイドエリアネットワークからなる何れかの組合せを備えていてもよいとされるネットワーク１４０を介して通信するように構成されていてもよい。１つの実施形態では、ネットワーク１４０は、標準通信技術及び／又はプロトコルを使用している。而して、ネットワーク１４０は、イーサネット（登録商標）、８０２．１１、ワールドワイド・インターオペラビリティ・フォー・マイクロウェーブ・アクセス（ＷｉＭＡＸ）、３Ｇ、４Ｇ、ＣＤＭＡ、デジタル加入者回線（ＤＳＬ）、など、の様な技術を使用するリンクを含んでいよう。

【００３３】

同様に、ネットワーク１４０の様々な層内で使用されているネットワーキングプロトコルには、マルチプロトコルラベルスイッチング（ＭＰＬＳ）、伝送制御プロトコル／インターネットプロトコル（ＴＣＰ／ＩＰ）、ユーザーデータグラムプロトコル（ＵＤＰ）、ハイパーテキスト輸送プロトコル（ＨＴＴＰ）、ハイパーテキスト輸送プロトコルセキュア（ＨＴＴＰｓ）、簡易メール転送プロトコル（ＳＭＴＰ）、ファイル転送プロトコル（ＦＴＰ）、安全ファイル転送プロトコル（ＳＦＴＰ）、及び／又は他のネットワーキングプロトコルが含まれよう。ネットワーク１４０上でやり取りされるデータは、ハイパーテキストマークアップ言語（ＨＴＭＬ）又は拡張可能マークアップ言語（ＸＭＬ）を含む技術又はフォーマットを使用して表現されていてもよい。加えて、全てのリンク又は幾つかのリンクは、安全ソケット層（ＳＳＬ）、輸送層機密保護（ＴＬＳ）、及びインターネットプロトコル機密保護（ＩＰｓｅｃ）の様な、従来の暗号化技術を使用して暗号化することができる。

【００３４】

図２は、本発明の１つ又はそれ以上の実施形態による、企業管理型アプリケーションと企業サービスの間に束縛を作成するための例示としての動作のセット２００に係る流れ図である。図２に示されている様に、インストール動作２１０が、企業制御アプリケーションを遠隔デバイスへインストールする。アプリケーションは、デバイスのエンドユーザー、企業からの個人、又は他のソース、によってインストールされよう。例えば、幾つかの実施形態では、アプリケーションは、アプリケーションストアから遠隔的にインストール又はダウンロードされるようになっている。アプリケーションがインストールされたら、認証動作２２０が、遠隔デバイスのユーザーに、フレームワークに対して認証させることのできる信用証明書のセットを提供するよう入力を促す。様々な機密保護プロトコル及び標準（例えば、パスワード、パスコード、時間ベースのトークン、暗号化されたデータ、自動ロック、など）が、遠隔デバイス及びアプリケーションの機密保護及び認証処理の一部として使用されよう。

【００３５】

認証動作２３０中、企業では、様々な認証チェック及び機密保護チェックが遂行される。幾つかの実施形態では、例えば、ユーザーから信用証明書のセットが受信されたら、認証要求が遠隔デバイス（即ち、クライアント）からゲートウェイサーバへ送られることになる。ゲートウェイサーバは、遠隔デバイスにて適用されるべき現在のポリシーを確定し

、ポリシー情報をゲートウェイサーバから遠隔デバイスへ送る。次いで、デバイス特性がチェックされ、必要なら新しいコンテナ信用証明書が取得されることになる。ゲートウェイが、アプリケーションは企業内の１つ又はそれ以上のサーバへアクセスして当然であると判定した場合には、作成動作２４０が使用されて、アプリケーションと企業サービスの間に束縛が作成されることになる。

【００３６】

図３は、本発明の様々な実施形態による安全移動体フレームワークのための全体としてのアーキテクチャ３００を示している。安全移動体フレームワークの構成要素は、移動体デバイス３０５上に記憶されている企業コンテンツを管理及び保護するのに使用することができる。幾つかの実施形態では、移動体デバイス３０５は、安全ストレージ３１０、ポリシー３２０、及び／又は移動体アプリケーション３１５のための認証ストア３２５、を含んでいてもよい。移動体アプリケーション３１５は、アプリケーションの下に置かれている仮想ファイルシステムを有していてもよい。幾つかの実施形態では、移動体アプリケーション３１５は１つ又はそれ以上の暫定キーを使用又は生成するようになっており、それらキーは複数の構成要素を有していることもある。暫定キーは、ファイル１つ１つをそれ独自のキーで暗号化するために仮想ファイルシステムの各パーティションに割り当てられるようになっていてもよい。

【００３７】

安全ストレージ３１０は、企業データを局所的に移動体デバイス３０５上に安全に記憶させることができる。安全ストレージ３１０は、ポリシー３２０を通じて単一ユニットとして管理されている保護ファイルのグループを含んでいよう。幾つかの実施形態では、企業コンテンツは、暗号化ファイルに記憶され、ランダムアクセス方式によりアクセスされるようになっていてもよい。加えて、様々な機構を使用して、暗号ブロックサイズをファイル単位で設定し、また同時にクライアントとサービスの間の同期コンテンツを支援するのに使用されるサイドカー索引ファイルを維持するようにしてもよい。保護ファイルは、ファイル毎の暗号化キー及びアプリケーションファイル名の間の翻訳を保持したりファイル名を難読化したりするのに単一のマスターファイルを使用している安全パーティションに保持される。この安全ファイルパーティション機構は、アプリケーションコンテンツを直接的に保障（securiteze）するのに使用されるのみならず、デバイス上でホストされるデータベースサーバ、ロギング、及び顧客サポートのためのテレメトリデータ、のための仮想ファイルシステムとして使用することもできる。

【００３８】

ポリシー３２０は、アプリケーション３１５が順守すべきとされる、企業によって設定されているアプリケーション特定（又はアプリケーション群）機密保護ポリシーとしてもよい。アプリケーション群とは、概して、共通ポリシーによって統制されるアプリケーションであって所与のユーザーについて所与のデバイス上での許可及び認証情報へのアクセスを共有するアプリケーションのグループ化を指す。ポリシー３１０は、デバイス上で許可、認証、及びデータ保障に使用される機密保護変数の値を含んでいてもよい。例えば、ポリシー３２０は、パスワード構造、どれほど長くデバイスをゲートウェイから切断されたままにしておくことができるか、何回までならユーザーは正しいパスワードの入力に失敗してもよいか、及び他の機密保護変数、を含んでいよう。

【００３９】

安全ファイルパーティションの更なる事例は認証ストア３２５であって、認証ストア３２５は、認証信用証明書(例えば、トークン及びアサーション)、ポリシー詳細事項、及び全ての他の安全ファイルパーティションマスターファイルを暗号化するのに使用されるマスター暗号化キー、を格納することができる。認証ストアマスターファイルストアは、ユーザーパスワード又はフレーズに基づいて生成される暫定キーで暗号化することができる。また、認証ストア３２５は、デバイス上の複数のアプリケーションの間で共有され、企業アクセス及び暗号化コンテンツ共有のための共通ストアが形成されるようにしていてもよい。

【００４０】

アプリケーション３１５及び対応する構成要素が移動体デバイス３０５上にインストールされたら、アプリケーション３１５は、１つ又はそれ以上のデバイス機密保護チェックに合格した後、サーバ３３０又は仮想機械３３５上で走る企業内の１つ又はそれ以上の内部サービスへのアクセスを要求することができる。アプリケーション３１５からの要求はまず境界ゲートウェイ３４０に受信され、そこで中継層３４５へのアプリケーションアクセスを許容する段階の前に認証の第１ラウンドが確立される。中継層３４５は、ユーザーを認証し、アプリケーション３１５によって施行されようとしているポリシーが最新であることを保証する。加えて、移動体デバイステレメトリ及び構成の諸設定が、収集され、処理され、分析され、評価され、及び／又はデータベース３５０内に記録されるようになっていてもよい。この情報は、不正又は異常検知の様々な表示を（例えば、リアルタイム又はほぼリアルタイムで）作成する場合に有用となろう。中継層３４５は、更に、アプリケーション３１５が移動体アプリケーションストア３５０の中へログインできるようにする。加えて、アプリケーション３１５とサーバ３３０の間の介在物としてプロキシ３５５が使用されていてもよい。

【００４１】

図４は、本発明の幾つかの実施形態による、企業管理型アプリケーションを許可するための例示としての動作のセット４００を示す流れ図である。受信動作４１０中に、企業管理型アプリケーションからの要求が受信される。要求は、アプリケーションが接続したがっている名指しされた企業内サービスを識別している。開始動作４２０が境界ゲートウェイとの安全接続を開始する。次いで、境界ゲートウェイは、ポリシー確認動作４３０を使用して、デバイス上で機能するポリシーが最新であることを保証し、そしてユーザー確認動作４４０で、ユーザーが企業サービスにアクセスすることをまだ許可されていることを保証する。

【００４２】

ポリシーとユーザーの妥当性確認が成功した場合、次いで妥当性確認動作４５０がゲートウェイでユーザーの認証信用証明書を妥当性確認する。次いで提出動作４６０中に企業信用証明書が宛先サービスへ受け渡されると、そこでは確認動作４７０中に認証及び許可が行われる。認証が成功し次第、束縛動作４８０がアプリケーションと名指しされたサービスの間に束縛を作成する。

【００４３】

図５は、本発明の１つ又はそれ以上の実施形態による、企業サービスと遠隔デバイス上で走る企業管理型アプリケーションの間に安全チャネルを作成するための例示としての動作のセット５００を示す流れ図である。図５に示されている様に、ユーザーは、立ち上げ動作５１０中に、クライアントデバイス上で走る企業管理型アプリケーションを立ち上げる。アプリケーションは、ユーザーに、コンテナ信用証明書のセットについて入力を促す。クライアントデバイスは、ユーザーから信用証明書を受け取ったら、暗号化動作５２０を使用して企業のサーバゲートウェイ相手のデータ及び通信を暗号化する。

【００４４】

企業管理型アプリケーションは、ゲートウェイ相手に認証するのにフレームワーク認証トークン（ＦＡＴ）を、またサービス相手に認証するのに企業認証トークン（ＥＡＴ）を使用することができる。妥当性確認動作５３０が、ＦＡＴの妥当性を（例えば、フレームワーク認証システムを使用して）判定する。すると、サーバ許可部が、企業サービスへの安全接続を作成するための１つ又はそれ以上のトークンを構築することができる。例えば、幾つかの実施形態では、サーバ許可部は、ユーザーｉｄ、アプリケーションｉｄ、及びデバイスｉｄから成るユーザー束縛トークン（ＵＢＴ）を作成することができる。加えて、ＦＡＴは、ＵＢＴ、ＥＡＴ、及び有効期限を束縛することによって作成されていてもよい。加えて、サーバ許可部は、ユーザーが企業にアクセスすることを許可されているかどうかを判定するようになっていてもよい。安全移動体フレームワークサーバは、ユーザーが対話することのできる企業サービスに基づいてポリシーを構築することができる。ポリ

シー内の情報には、ＦＡＴの有効期限、ＦＡＴが失効したときにユーザーが遂行しなくてはならない企業認証の型式、及び移動体デバイス上のデータを安全確保するのに使用される他のポリシー情報、を含めることができる。こうして、安全移動体フレームワークサーバゲートウェイは、移動体デバイスにＦＡＴ及びポリシーを応返する。

【００４５】

呼び出し側のクライアント（例えば、移動体デバイス）は、認証ストアを使用してＦＡＴ及びポリシーコンテンツを保存することができる。次いで、アプリケーションは、ポリシー施行が確認され次第、生成動作５４０を使用して接続要求を生成することができる。次いで、作成動作５５０が、企業管理型アプリケーションと企業サービスの間に安全チャネルを作成する。例えば、アプリケーションは、クライアント安全移動体フレームワークに、特定の企業サービスへ接続するように何らかの正準名(canonical name)を使用して依頼することができる。するとフレームワークは、サービス名をＵＢＴ共々、同じ接続上で安全移動体フレームワークサーバサービス認証部へ送る。サービス認証部は、ＵＢＴが当該宛先へ接続するのを許容されているかどうかを判定する。

【００４６】

安全移動体フレームワークサーバサービスルータが、次いで、正準名をサービスの実アドレスへマップし、接続を確立する。移動体アプリケーションは、企業認証が成功裏に完了したら、これより安全確保されたチャネル上で自由に通信することができる。以降の接続要求に際し、アプリケーションは安全移動体フレームワークに特定のサービスへ接続するように何らかの正準名を使用して依頼する。すると安全移動体フレームワークは、サービス名をＵＢＴ及びＥＡＴ共々、安全移動体フレームワークゲートウェイへ送る。幾つかの実施形態では、次にアプリケーションがサービスと接続しようと試みたときに、ユーザーが入力した企業信用証明書ではなしにこの情報が、少なくともＦＡＴが失効するまでは、使用されることになる。

【００４７】

図６は、本発明の様々な実施形態と共に使用することのできる安全移動体フレームワーク上に築かれたアプリケーションの一例である。図６に示されている様に、ウェブブラウザ６０５は、カスタムプロトコルにラップされていてもよいとされる標準ＨＴＴＰ／Ｓ要求を生成することのできるウェブブラウザの実施形を表現している。ウェブブラウザ６０５は、通信ＡＰＩ６１０を使用してゲートウェイへの接続を確立することができる。幾つかの実施形態では、通信ＡＰＩ６１０は、ユーザーを認証するにあたり安全ファクトリＡＰＩ６１５にアクセスするように安全ソケット層（ＳＳＬ）の上に築かれていてもよい。典型的なウェブベースのアプリケーションは、サーバ及び履歴ＵＲＬと共有されるクッキーの様なデータのストレージを必要とする。図６に示されているウェブブラウザの実施形は、ストレージＡＰＩ６２０及び安全ファイルパーティションマネジャを使用して、オペレーティングシステムの下層のファイルシステム６２５を利用する前にデータを暗号化する。

【００４８】

通信ＡＰＩ６１０は、安全キーストア６３０を使用して企業ゲートウェイとの接続を確立するために、ユーザーの生の信用証明書又は記憶されているトークンを入手する。例えば、ユーザーの信用証明書を受信し次第、安全キーが安全キーストア６３０から読み出されるようになっていてもよい。このキーを使用してキーチェーンにアクセスすることができ、アクセスした後にフレームワークのサブコンポーネントが初期化されることになる。システム管理６３５は、デバイス／アプリケーションから、アプリケーションと関連付けられる現在のポリシーの識別を受信することができる。ポリシー管理６４０を使用すれば、アプリケーションと関連付けられる現在のポリシーが最新であるか又は更新される必要があるかに関して判定を下すことができる。システム管理６３５は、確実に、適正なロギング、仮想ファイルシステム管理、及びページキャッシングが起こるようにすることができる。

【００４９】

許可及び認証が成功し次第、ゲートウェイは、通信ＡＰＩ６１０からのポリシー及びデバイス情報を要求する。妥当性確認が成功し次第、ゲートウェイは、企業内でＨＴＴＰ／Ｓ呼び出しを行うことのできるウェブブラウザプロキシサービスへの接続を束縛することができる。するとウェブブラウザ６０５がラップされているＨＴＴＰ／Ｓ要求をこのチャネルを通して送信する。

【００５０】

図７は、本発明の幾つかの実施形態による、企業内のサーバ７１０にアクセスする遠隔デバイス７０５を示している。図７に示されている様に、本発明の様々な実施形態は、遠隔デバイス７０５がマルチレベルの認証処理を経て企業にアクセスできるようにしている。例えば、企業内のサーバ７１０上で走るエンドポイントサービスへ接続するために、幾つかの実施形態では、コンテナ認証、フレームワーク認証、及び企業認証が、全て成功裏に完了されなくてはならない。多くの従来の認証システムであれば、移動体デバイス上のアプリケーションを使用するためには、ユーザーが典型的にパスワードを入力してデバイスをロック解除し、次いで遠隔デバイスに対して認証するためにユーザー名とパスワードを供給する、ということが求められるところである。対照的に、本発明の様々な実施形態は、複数の機密保護層を使用した末に始めてデバイス上のデータへのアクセス又は遠隔サービスへの接続が許容される。

【００５１】

アプリケーション７１５が立ち上がり次第、要求が遠方移動体コンテンツゲートウェイ７２０へ送られる。遠方移動体コンテンツゲートウェイ７２０の主積層７２５内で、ユーザーとデバイスの妥当性確認及び認証が承認される。例えば、幾つかの実施形態では、企業認証システム７３０（例えば、ＲＳＡ（登録商標）又はＫｅｒｂｅｒｏｓ（商標））を使用することができる。幾つかの実施形態では、認証処理は、ユーザー名、ホワイトリストチェック、ポリシーチェック、及び／又は宛先チェックを含むことができる。加えて、デバイスのテレメトリ及び構成が監視され第２の中継認証層へ送信されるようになっていてもよい。これらは、ユーザー、デバイス、及びアプリケーションを認証させることができる。

【００５２】

ユーザー、デバイス、及びアプリケーションが認証されたら、サーバ７１０相手に接続が確立されることになる。多くの実施形態は、ユーザー、デバイス、及びアプリケーションの認証中に作成された様々なトークンを、サーバ７１０との接続を確立するために使用する。遠方移動体コンテンツゲートウェイ７２０は、企業内のサーバへのアクセスについての追加の認証サービスのために移動体ゲートウェイサービス７３５と接続することができる。例えば、幾つかの実施形態では、ユーザーがパスワード又は他の認証信用証明書をアプリケーション７１５内に入力すれば、それを使用してデバイス上に局所的に記憶されているデータが復号されるようにしている。そうすれば、ユーザーは、遠隔環境上で走るゲートウェイ処理へＦATを提示すればよい。ゲートウェイ処理は、ＦATを使用して、ユーザー及びデバイスを許可及び認証する。今度は、何れかの特定のサービスにアクセスするため、ユーザーはＥAＴを遠隔サービスへ提示しようとするはずである。幾つかの実施形態では、ＦAT及びＥAＴは、１つ又はそれ以上のプラガブル形式の認証（例えば、タイムコード＋ピン、生体認証、パスワード、など）を事前に形成した後にデバイス上に局所的に記憶されるようになっている。

【００５３】

幾つかの実施形態では、認証の形式は、所定のスケジュールで（例えば、周期的に）又は１つ又はそれ以上の事象が検知された時点でローテーションさせることができる。例えば、ゲートウェイは、現在の認証形式を移動体デバイスへ安全に送信して、それを安全ストアに記憶させることができる。図７は、ＨＴＴＰＳ及びＴＬＳの様な、使用できる安全接続の例を示しているが、本発明の他の実施形態は、システム構成要素間のメッセージング及びデータ転送のために接続を作成するのに異なったプロトコルを使用することもできる。

【００５４】
　図８は、本発明の１つ又はそれ以上の実施形態による、デバイスアプリケーションと企業の間の初期認証フローを示すシーケンス線図である。図８に示されている様に、ユーザーがデバイスアプリケーションを立ち上げる。完全性検知処理を使用して、期待されるＯＳ完全性が存在しているかどうかが判定される。例えば、完全性検知処理は、デバイスが高位の許可されていない特権（例えば、ルート化又はジェイルブレイク）モードで動作していないかどうかを判定することができる。デバイスアプリケーションは、ノード識別子（例えば、Ｋｅｒｂｅｒｏｓ（商標）ＩＤ）及び認証パスワードを要求する。その時点でデバイス識別子がデバイスから入手される。次いで、初期認証要求が遠方コンテンツゲートウェイへ（例えば、安全接続を使用して）提出されることになる。初期認証要求は、認証パスワード、デバイス識別子、アプリケーション群、デバイス形式、及び／又は他の情報、を含んでいよう。すると、遠方コンテンツゲートウェイは、認証要求を認証サービスへ送ることになる。認証サービスがユーザーを認証したら、ＵＢＴが移動体認証サービスによって登録される。
【００５５】
　移動体認証サービスは、アクセスを許可し、ＵＢＴを生成し、そしてデバイス識別子、ユーザー名、アプリケーション群、及びＵＢＴを記憶する。移動体認証サービスは、ＵＢＴ及び認証トークンに署名したうえで、ポリシー、ＵＢＴ、及びデジタル署名を遠方コンテンツゲートウェイへ戻す。すると、遠方コンテンツゲートウェイは、ＦＡＴを生成し、それが、ポリシー、ＵＢＴ、及びデジタル署名と共にデバイスアプリケーションへ戻される。場合によっては、ポリシーは、デバイスアプリケーションに安全コンテナのための新しいパスワードを要求するように求めることもある。そうすれば、ＦＡＴ、ＵＢＴ、及びデジタル署名は、パスワードでロックすることのできる安全コンテナに記憶させることができる。
【００５６】
　図９は、本発明の様々な実施形態による、デバイスアプリケーションと企業の間の連続的な認証フローを示すシーケンス線図である。図９に示されている実施形態では、ユーザーがデバイスアプリケーションを立ち上げる。すると、オペレーティングシステム完全性チェック（例えば、ジェイルブレイク検知処理）を使用して、オペレーティングシステムの完全性が危うくなっていないかどうかが判定される。オペレーティングシステム完全性チェックがオペレーティングシステムは期待通りでないと判定した場合、アプリケーションはゲートウェイと接続できなくなってしまう。オペレーティングシステムの完全性が期待通りである場合、デバイスアプリケーションは、ユーザーから安全コンテナパスワードを読み出し、安全コンテナをロック解除して現在のポリシーを読み出す。デバイスアプリケーションは、ポリシーの施行をチェックし、遠方コンテンツゲートウェイへ接続する。遠方コンテンツゲートウェイは、ＵＢＴ及び認証トークンのデジタル署名をチェックする。遠方コンテンツゲートウェイは、更に、ディレクトリをチェックしてユーザー名の状態及びＵＢＴがホワイトリストに載っているかどうかをチェックすることになる。
【００５７】
　デバイスアプリケーションは、デバイスアプリケーションが接続したいと思っている企業サービスの正準名を提出する。遠方コンテンツゲートウェイは、宛先サービスモジュールを使用して、ＵＢＴが当該サービスへ接続するのを許容されているかどうかを判定する。ＵＢＴが接続を許容されている場合には、遠方コンテンツゲートウェイは、企業サービス又は当該サービスへのプロキシへの接続を束縛する。成功コードが遠方コンテンツゲートウェイからデバイスアプリケーションへ最新のポリシーバージョンと共に戻される。デバイスアプリケーションは、戻されたばかりのポリシーバージョンが安全コンテナから読み出されたポリシーを上回るかどうかをチェックして見極める。当該ポリシーバージョンが上回っている場合、新しいポリシーが適用される。次いで、ＦＡＴが安全コンテナから読み出され、遠方コンテンツゲートウェイとの会話を開始できるようになる。
　例示としてのコンピュータシステムの概観

【００５８】
本発明の実施形態は、以上に説明されてきた様々な段階及び動作を含んでいる。様々なこれらの段階及び動作は、本発明の実施形態の中で使用されている移動体デバイス、サーバ、又は他のコンピュータシステムの一部であるハードウェア構成要素によって遂行されていてもよい。幾つかの実施形態では、これらの段階及び動作は、機械実行可能命令に具現化され、当該命令をプログラムされた一般用途又は特定用途のプロセッサにそれら段階を遂行させるのに使用されるようになっていてもよい。代わりに、それら段階は、ハードウェア、ソフトウェア、及び／又はファームウェアの組合せによって遂行されるようになっていてもよい。而して、図１０は、本発明の幾つかの実施形態を利用することのできるコンピュータシステム１０００の一部として使用される幾つかの構成要素を示している。図１０に示されている様に、コンピュータシステムは、バス１０１０、少なくとも１つのプロセッサ１０２０、少なくとも１つの通信ポート１０３０、主メモリ１０４０、取り外し可能な記憶媒体１０５０、読み出し専用メモリ１０６０、及び大容量ストレージ１０７０、を含んでいてもよい。場合によっては、コンピュータシステム１０００は、取り外し可能な記憶媒体１０５０、大容量ストレージ１０７０、及び同種物、の様なローカルストレージを一切含んでいないこともあろう。

【００５９】
（単数又は複数の）プロセッサ１０２０は、限定するわけではないが、Ｉｎｔｅｌ（登録商標）Ｉｔａｎｉｕｍ（登録商標）又はＩｔａｎｉｕｍ　２（登録商標）プロセッサ、ＡＭＤ（登録商標）Ｏｐｔｅｒｏｎ（登録商標）又はＡｔｈｌｏｎ　ＭＰ（登録商標）プロセッサ、ＡＲＭベースのプロセッサ、又はＭｏｔｏｒｏｌａ（登録商標）系統のプロセッサの様な、何れかの既知のプロセッサとすることができる。（単数又は複数の）通信ポート１０３０は、モデムベースのダイアルアップ式接続に係る使用のためのＲＳ－２３２ポート、１０／１００イーサネット（登録商標）ポート、又は銅線又はファイバを使用するギガビットポート、のうちの何れかとすることができる。（単数又は複数の）通信ポート１０３０は、ローカルエリアネットワーク（ＬＡＮ）、ワイドエリアワークネットワーク（ＷＡＮ）、又はコンピュータシステム１０００が接続している何れかのネットワークの様な、ネットワークに依存して選定されていてもよい。

【００６０】
主メモリ１０４０は、ランダムアクセスメモリ（ＲＡＭ）又は当技術で一般的に知られている何れかの他の（単数又は複数の）動的ストレージデバイスとすることができる。読み出し専用メモリ１０６０は、プロセッサのための命令の様な静的情報を記憶するためのプログラマム可能読み出し専用メモリ（ＰＲＯＭ）チップの様な、何れかの（単数又は複数の）静的ストレージデバイスとすることができる。

【００６１】
大容量ストレージ１０７０は、情報及び命令を記憶するのに使用することができる。例えば、Ａｄａｐｔｅｃ（登録商標）系のＳＣＳＩドライブの様なハードディスク、光ディスク、ＲＡＩＤの様なディスクのアレイであって例えばＡｄａｐｔｅｃ系のＲＡＩＤドライブ、又は何れかの他の大容量ストレージデバイス、が使用されてもよい。

【００６２】
バス１０１０は、（単数又は複数の）プロセッサ１０２０を、他のメモリ、ストレージデバイス、及び通信のブロックと、通信可能に連結する。バス１０１０は、使用されるストレージデバイスに依存して、ＰＣＩ／ＰＣＩ－Ｘベース又はＳＣＳＩベースのシステムバスとすることができる。

【００６３】
取り外し可能な記憶媒体１０５０は、外部ハードドライブ、フロッピードライブ、ＩＯＭＥＧＡ(登録商標)Ｚｉｐドライブ、コンパクトディスク－読み出し専用メモリ（ＣＤ－ＲＯＭ）、コンパクトディスク－書き込み可能（ＣＤ－ＲＷ）、及び／又はデジタルビデオディスク－読み出し専用メモリ（ＤＶＤ－ＲＯＭ）の何れかの種類であってもよい。

【００６４】

上述の構成要素は、候補の数型式を典型的に示そうとしたものである。上記の例は、単に例示としての実施形態であることから、発明の範囲を一切限定するものではない。また、本発明の実施形態によって企図されているコンピュータシステムの幾つか（例えば、サーバ、クライアント、移動体デバイス、など）は、これらの構成要素全てを含んでいるとは限らない。加えて、コンピュータシステムの幾つかは、図１０に示されているものとは異なった構成及び／又は追加の構成要素を含んでいてもよい。例えば、幾つかのコンピュータシステム（例えば、移動体デバイス）は、ＧＰＳユニット及び様々な型式のＩ／Ｏデバイス（例えば、タッチスクリーン、視線追跡モジュール、自然言語プロセッサ、ＬＣＤ、キーボード、など）を含んでいる場合もあろう。

【００６５】

総括すると、本発明は、企業管理型アプリケーションにとっての安全移動体フレームワークのための新規性のあるシステム、方法、及び配列を提供している。本発明の１つ又はそれ以上の実施形態の詳細な説明が以上に与えられているが、本発明の精神から外れることなく、様々な代替物、修正物、及び等価物が当業者には自明であろう。例えば、以上に説明されている実施形態は特定の特徴に言及しているが、本発明の範囲は、特徴の異なった組合せを有する実施形態及び記載されている特徴全てを含んでいるとは限らない実施形態も包含している。

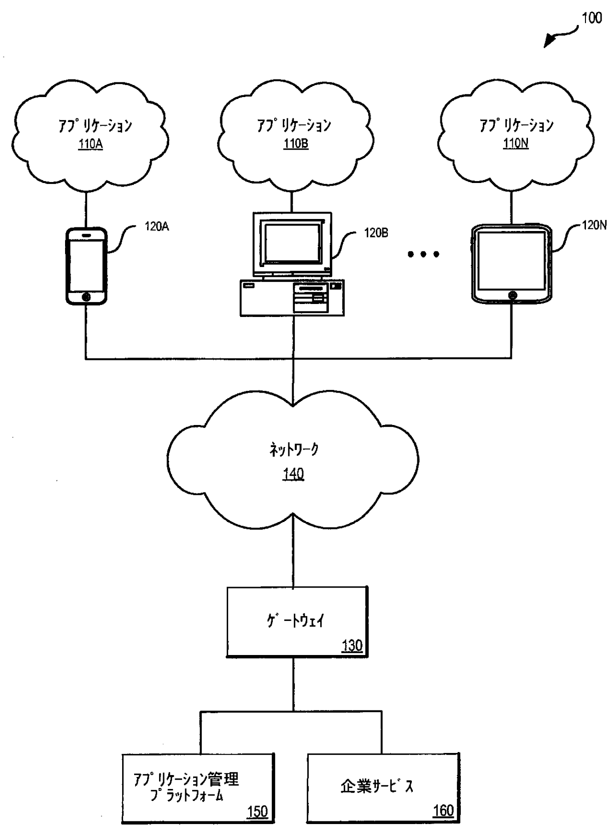
【符号の説明】

【００６６】

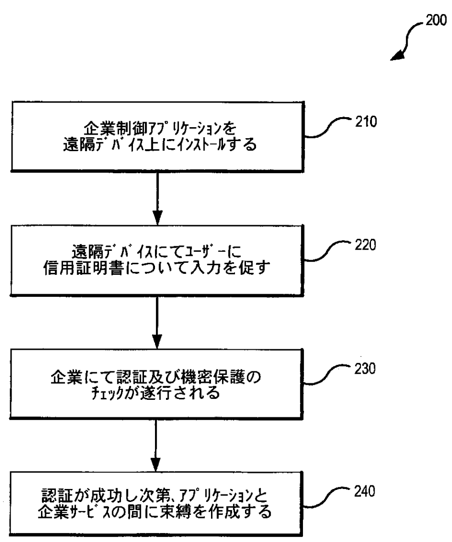
１００　ネットワークベースの環境
１１０Ａ、１１０Ｂ、１１０Ｎ　企業管理型アプリケーション
１２０Ａ、１２０Ｂ、１２０Ｎ　ユーザーデバイス
１３０　ゲートウェイ
１４０　ネットワーク
１５０　アプリケーション管理プラットフォーム
１６０　企業サービス
３００　安全移動体フレームワークの全体的なアーキテクチャ
３０５　移動体デバイス
３１０　安全ストレージ
３１５　移動体アプリケーション
３２０　ポリシー
３２５　認証ストア
３３０　サーバ
３３５　仮想機械
３４０　境界ゲートウェイ
３４５　中継層
３５０　データベース、移動体アプリケーションストア
３５５　プロキシ
６０５　ウェブブラウザ
６１０　通信ＡＰＩ
６１５　安全ファクトリＡＰＩ
６２０　ストレージＡＰＩ
６２５　ファイルシステム
６３０　安全キーストア
６３５　システム管理
６４０　ポリシー管理
７０５　遠隔デバイス
７１０　サーバ
７１５　アプリケーション
７２０　遠方移動体コンテンツゲートウェイ

７２５　主積層
７３０　企業認証システム
７３５　移動体ゲートウェイサービス
１０００　コンピュータシステム
１０１０　バス
１０２０　プロセッサ
１０３０　通信ポート
１０４０　主メモリ
１０５０　取り外し可能な記憶媒体
１０６０　読み出し専用メモリ
１０７０　大容量ストレージ

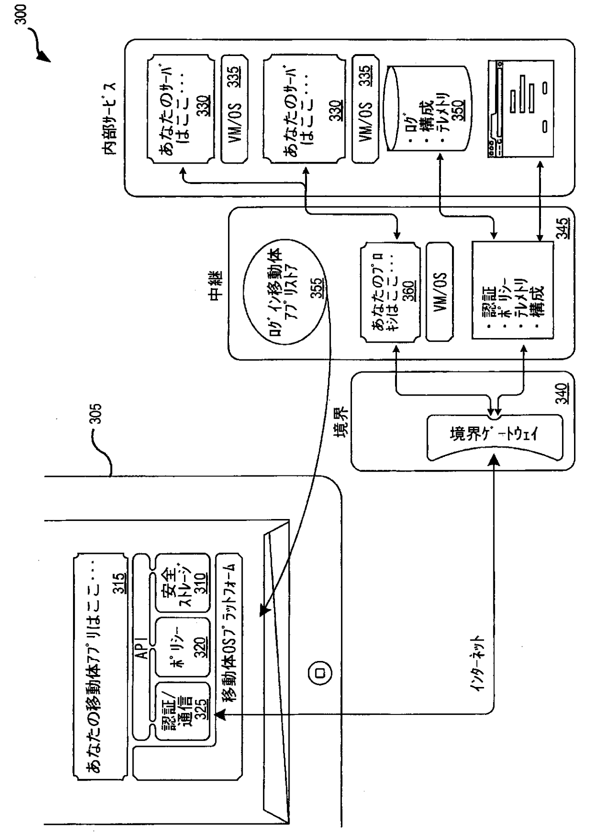
【図１】



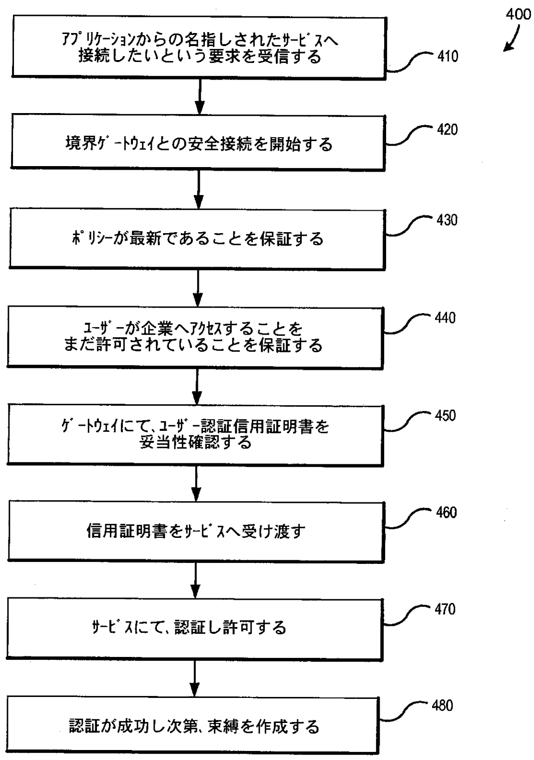
【図２】



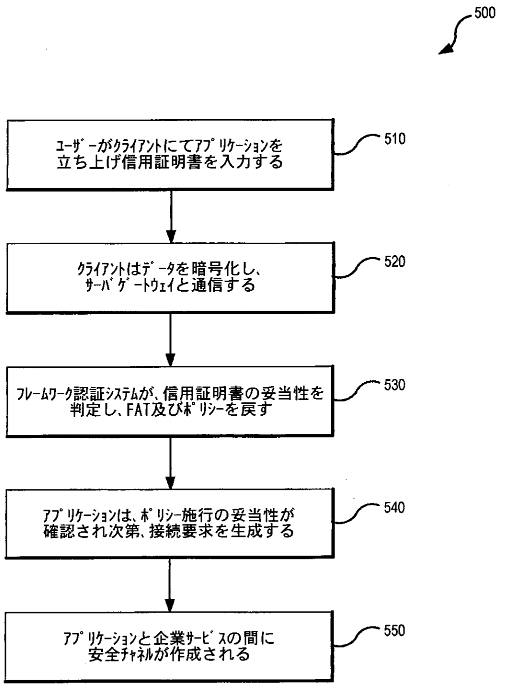
【図３】


300
内部サービス
あなたのサーバはここ…
330
VM/OS
335
・ログ
・構成
・テレメトリ
350
中継
ログイン移動体アプリストア
355
あなたのプロキシはここ…
360
VM/OS
・認証
・ポリシー
・テレメトリ
・構成
345
境界
境界ゲートウェイ
340
305
あなたの移動体アプリはここ…
315
API
認証/通信
325
ポリシー
320
安全ストレージ
310
移動体OSプラットフォーム
インターネット

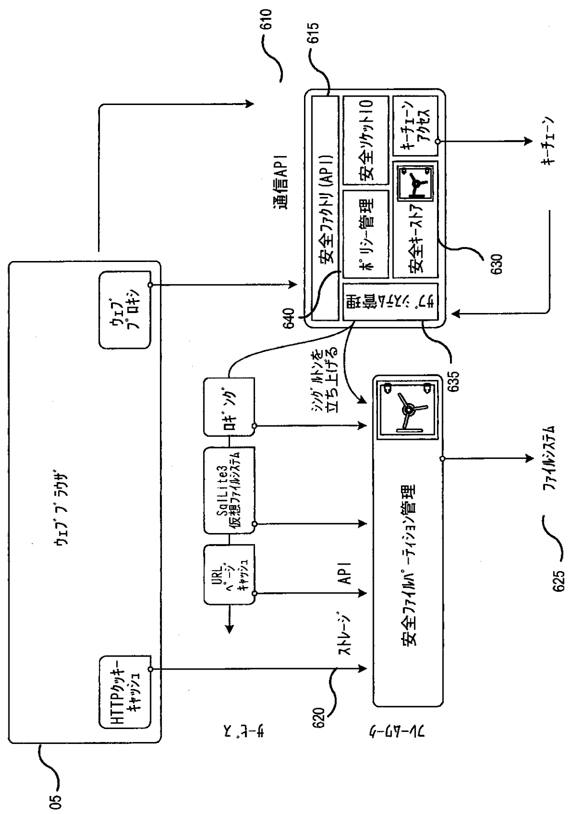
【図４】


400
アプリケーションからの名指しされたサービスへ接続したいという要求を受信する
410
境界ゲートウェイとの安全接続を開始する
420
ポリシーが最新であることを保証する
430
ユーザーが企業へアクセスすることをまだ許可されていることを保証する
440
ゲートウェイにて、ユーザー認証信用証明書を妥当性確認する
450
信用証明書をサービスへ受け渡す
460
サービスにて、認証し許可する
470
認証が成功し次第、束縛を作成する
480

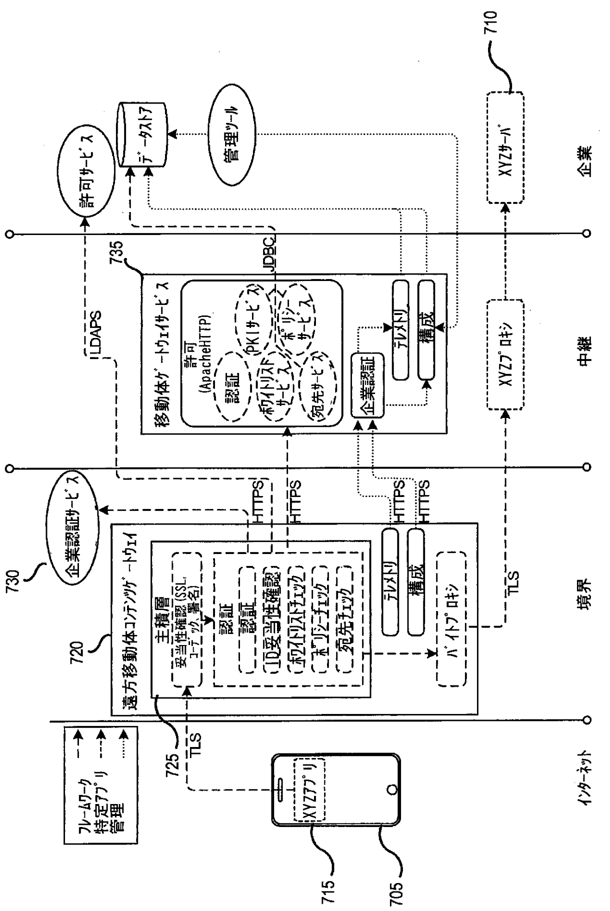
【図５】


500
ユーザーがクライアントにてアプリケーションを立ち上げ信用証明書を入力する
510
クライアントはデータを暗号化し、サーバゲートウェイと通信する
520
フレームワーク認証システムが、信用証明書の妥当性を判定し、FAT及びポリシーを戻す
530
アプリケーションは、ポリシー施行の妥当性が確認され次第、接続要求を生成する
540
アプリケーションと企業サービスの間に安全チャネルが作成される
550

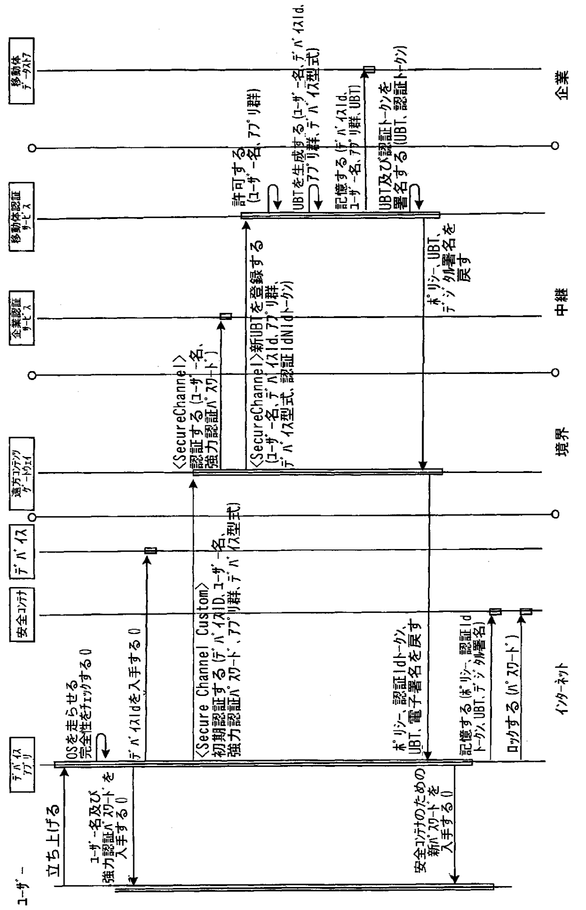
【図６】


610
615
通信API
安全ファクトリ（API）
安全ソケットIO
キーチェーンアクセス
キーチェーン
ポリシー管理
安全キーストア
630
640
ウェブプロキシ
シングルトンを立ち上げる
635
ロギング
SqlLite3仮想ファイルシステム
URLページキャッシュ
API
ストレージ
安全ファイルパーティション管理
ファイルシステム
625
ウェブブラウザ
HTTPクッキーキャッシュ
620
05

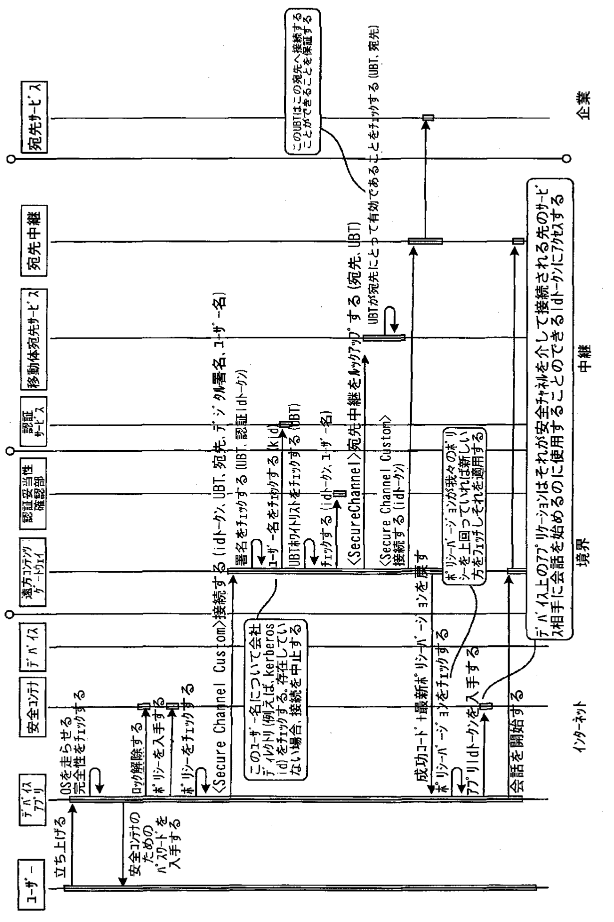
【図７】


705
710
715
720
725
730
735
XYZアプリ
遠方移動体コンテンツゲートウェイ
移動体ゲートウェイサービス
企業認証サービス
許可サービス
データストア
管理ツール
XYZサーバ
XYZプロキシ
LDAPS
JDBC
HTTPS
TLS
インターネット
境界
中継
企業

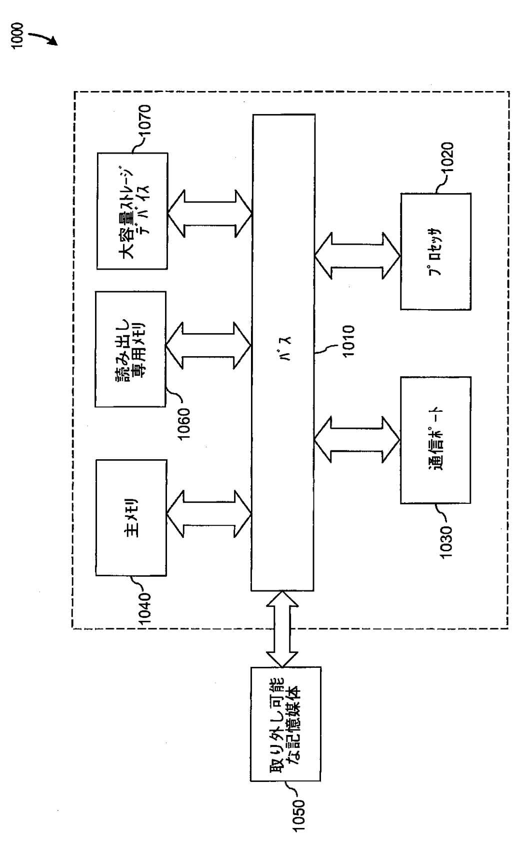
【図８】


ユーザー
デバイスアプリ
安全コンテナ
デバイス
遠方コンテンツゲートウェイ
企業認証サービス
移動体認証サービス
移動体データストア
立ち上げる
インターネット
境界
中継
企業

【図９】


ユーザー
デバイスアプリ
安全コンテナ
デバイス
遠方コンテンツゲートウェイ
認証妥当性確認部
認証サービス
移動体宛先サービス
宛先中継
宛先サービス
立ち上げる
インターネット
境界
中継
企業

【図１０】


1000
1010
1020
1030
1040
1050
1060
1070
大容量ストレージデバイス
読み出し専用メモリ
主メモリ
バス
プロセッサ
通信ポート
取り外し可能な記憶媒体

【手続補正書】
【提出日】平成28年9月2日(2016.9.2)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
遠隔デバイスに企業のサービスへのアクセスを提供するゲートウェイサーバであって、各遠隔デバイスは前記企業により管理されている１又は複数のアプリケーションをメモリに記憶している、ゲートウェイサーバと、
前記ゲートウェイサーバがアクセスできる認証部であって、
前記遠隔デバイスのうちの１つのユーザが前記企業にアクセスするのを許可されているかどうかを判定するように、及び前記１又は複数のアプリケーションの管理に関して、前記遠隔デバイスのうちの１つの前記ユーザが前記遠隔デバイスのうちの１つにアクセスするのを許可される前記サービスに基づいているポリシーを構築するように、構成されるプロセッサを含む認証部と、
前記ゲートウェイサーバがアクセスできる、及び前記企業により管理されている前記１又は複数のアプリケーションと前記サービスの間に安全接続を作成するための１又は複数のトークンを生成するように構成されるプロセッサを含む、トークン生成部であって、
前記１又は複数のトークンは、前記ユーザのユーザ識別子、前記ユーザの前記遠隔デバイスのデバイス識別子、前記１又は複数のアプリケーションと関連付けられるアプリケーション群、及び前記デバイス識別子と関連付けられるデバイスの型式を合体させた固有の表現を含むユーザ束縛トークンを含む、トークン生成部と、
前記ポリシーを前記遠隔デバイスへ通信するように構成されるプロセッサを含む通信モジュールと、を備えるシステム。
【請求項２】
前記企業の前記サービスのうちのどれを前記１又は複数のアプリケーションと接続するべきかを確定する発見サービスを更に備える、請求項１に記載のシステム。
【請求項３】
前記発見サービスが前記１又は複数のアプリケーションと接続するのに前記サービスのうちのどれを選択するかは、前記ユーザ及び関連付けられる特権のセットに基づいている、請求項２に記載のシステム。
【請求項４】
前記トークン生成部は、企業認証トークン及びフレームワーク認証トークンを生成する、請求項１に記載のシステム。
【請求項５】
前記フレームワーク認証トークンは、前記企業認証トークン、前記ユーザ束縛トークン、及びフレームワーク認証トークン有効期限、を含む、請求項４に記載のシステム。
【請求項６】
前記ユーザ束縛トークンは、ユーザ識別子、デバイス識別子、デバイス型式識別子、及びアプリケーション群識別子、に基づいて生成される、請求項４に記載のシステム。
【請求項７】
前記システムは、前記遠隔デバイスと前記サービスの間の活動を監視し、異常表示を生成する異常検知部を更に備え、前記異常検知部は、更に、異常表示への反応を判定する、請求項１に記載のシステム。
【請求項８】
前記ゲートウェイサーバは、それぞれ単独の認証プロトコル及び活動ロギングを提供する複数のレベルを含む、請求項１に記載のシステム。

【請求項９】
　前記複数のレベルは、境界ゲートウェイ及び中継ゲートウェイを含む、請求項８に記載のシステム。
【請求項１０】
　前記中継ゲートウェイは、移動体デバイステレメトリ及び構成の設定を使用して不正又は異常検知の表示を生成する、請求項９に記載のシステム。
【請求項１１】
　前記１又は複数のアプリケーションの管理に関して構築される前記ポリシーは、前記１又は複数のアプリケーションごとに固有のポリシーを含む、請求項１に記載のシステム。
【請求項１２】
　前記１又は複数のアプリケーションの管理に関して構築される前記ポリシーは、許可及び認証情報へのアクセスを共有する前記１又は複数のアプリケーションのサブセットごとに共通のポリシーを含む、請求項１に記載のシステム。

フロントページの続き

(74)代理人　100109070
弁理士　須田　洋之
(74)代理人　100109335
弁理士　上杉　浩
(74)代理人　100120525
弁理士　近藤　直樹
(74)代理人　100196612
弁理士　鎌田　慎也
(72)発明者　ファルティン　ダニエル
アメリカ合衆国　ニューヨーク州　１０２８２　ニューヨーク　ウェスト　ストリート　２００
(72)発明者　スミス　アンドリュー　ジェイ　アール
アメリカ合衆国　ニューヨーク州　１０２８２　ニューヨーク　ウェスト　ストリート　２００

Ｆターム(参考) 5B376 AC13

【外国語明細書】
2016201150000001.pdf