(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2017-524214
(P2017-524214A)
(43)公表日　平成29年8月24日(2017.8.24)

(51)Int.Cl.	F I	テーマコード（参考）
G06F 21/31 (2013.01)	G06F 21/31	

審査請求 有　予備審査請求 未請求　（全 53 頁）

(21)出願番号	特願2017-520865 (P2017-520865)
(86)(22)出願日	平成26年7月25日 (2014.7.25)
(85)翻訳文提出日	平成29年2月14日 (2017.2.14)
(86)国際出願番号	PCT/US2014/048229
(87)国際公開番号	WO2015/199741
(87)国際公開日	平成27年12月30日 (2015.12.30)
(31)優先権主張番号	14/317,795
(32)優先日	平成26年6月27日 (2014.6.27)
(33)優先権主張国	米国 (US)

(71)出願人　397074301
サイトリックス　システムズ，インコーポレイテッド
アメリカ合衆国　フロリダ　３３３０９，フォート　ローダーデール，　ウエスト　サイプレス　クリーク　ロード　８５１
(74)代理人　110002310
特許業務法人あい特許事務所
(72)発明者　イネス，アンドリュー
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】サードパーティの認証サポートを介した企業認証

(57)【要約】
【課題】サードパーティの認証サポートを介した企業認証アプローチを提供する方法およびシステムを提供する。
【解決手段】コンピューティングデバイスから認証デバイスに、フォームログインプロトコルを介してクライアントデバイス・アプリケーションの認証要求を送信する段階と、コンピューティングデバイスによりクライアントデバイス・アプリケーションに、拡張デバイスによって生成され認証デバイスから読み取られた第１の資格情報フォームを送信する段階とを含む。さらに、コンピューティングデバイスによりクライアントデバイス・アプリケーションから、第１の認証資格情報を受信する段階と、コンピューティングデバイスにより拡張デバイスを介して認証サービスに、第１の認証資格情報を送信する段階とを含んでもよい。さらに、コンピューティングデバイスにより、第１の認証資格情報の妥当性検証の成功に応答して、クライアントデバイス・アプリケーションからフォームログインプロトコルを介して行われた認証要求の承認を送信する段階を含んでいてもよい。

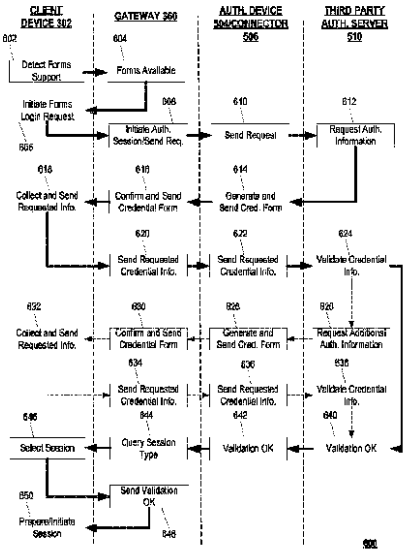


FIG. 6

【特許請求の範囲】
【請求項１】
コンピューティングデバイスから、認証デバイスに、フォームログインプロトコルを介してクライアントデバイス・アプリケーションの認証の要求を送信することと、
前記コンピューティングデバイスが、前記認証デバイスから、第１の認証資格情報を要求する第１の資格情報フォームを取得することであって、前記第１の資格情報フォームは、前記認証デバイスに接続されている拡張デバイスにより、前記クライアントデバイス・アプリケーションに関連する認証サービスから受信した情報に基づいて生成され、前記拡張デバイスは前記クライアントデバイス・アプリケーションに関連する前記認証サービスの１つ以上の認証プロトコルを用いて構成されている、前記取得することと、
前記コンピューティングデバイスから前記クライアントデバイス・アプリケーションに、前記第１の資格情報フォームを送信することと、
前記コンピューティングデバイスが、前記クライアントデバイス・アプリケーションから、前記第１の認証資格情報を受信することと、
前記コンピューティングデバイスから前記拡張デバイスを介して前記認証サービスに、前記第１の認証資格情報を送信することと、
前記コンピューティングデバイスから、前記第１の認証資格情報の妥当性検証の成功に応答して、前記フォームログインプロトコルを介して前記クライアントデバイス・アプリケーションが認証のために行う前記要求の承認を送信することと、
を含む方法。
【請求項２】
前記コンピューティングデバイスから前記クライアントデバイス・アプリケーションに、前記第１の資格情報フォームを送信することは、前記コンピューティングデバイスにより前記クライアントデバイス・アプリケーションに、前記第１の認証資格情報を取得するように構成されているプラグインメカニズムを呼び出す命令を送信することをさらに含み、前記プラグインメカニズムは前記クライアントデバイス・アプリケーションに関連する前記認証サービスと通信するように構成されている、請求項１に記載の方法。
【請求項３】
前記プラグインメカニズムは、ユーザデバイスに、前記クライアントデバイス・アプリケーションに関連する前記認証サービスから取得された情報を使用して、前記第１の認証資格情報を要求するユーザインターフェースを表示するように構成されている、請求項２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が、前記認証デバイスから、第２の認証資格情報を要求する第２の資格情報フォームを取得することと、
前記コンピューティングデバイスから前記クライアントデバイス・アプリケーションに、前記第２の資格情報フォームを送信することと、
前記コンピューティングデバイスが、前記クライアントデバイス・アプリケーションから、前記第２の認証資格情報を受信することと、
前記コンピューティングデバイスから前記認証デバイスに、前記第２の認証資格情報を送信することと、
をさらに含む、請求項１に記載の方法。
【請求項５】
前記コンピューティングデバイスが、第１の認証サービスに関連する前記第１の資格情報フォームを取得することと、
前記コンピューティングデバイスが、第２の認証サービスに関連する前記第２の資格情報フォームを取得することと、
をさらに含む、請求項４に記載の方法。
【請求項６】
前記第１および前記第２の資格情報フォームを送信することは、

前記第１および前記第２の資格情報フォームを第３の資格情報フォームに合体させることと、
前記コンピューティングデバイスから前記クライアントデバイス・アプリケーションに、前記第３のフォームを送信することとを含む、請求項５に記載の方法。
【請求項７】
前記第１の資格情報フォームは第１の認証プロセスに関連し、前記第２の資格情報フォームは第２の認証プロセスに関連し、前記方法は、前記第１の認証プロセスの開始後かつ前記第１の認証プロセスの完了前に、前記第２の認証プロセスの１つ以上のフェーズを実施することをさらに含む、請求項５に記載の方法。
【請求項８】
前記コンピューティングデバイスはゲートウェイデバイスを具備し、前記方法は、前記ゲートウェイデバイスにより前記クライアントデバイス・アプリケーションに、ゲートウェイデバイスの認証セッションに関連する第１セッション識別子と、認証デバイスの認証セッションに関連する第２セッション識別子と、のうちの少なくとも１つを渡すことをさらに含む、請求項１に記載の方法。
【請求項９】
前記コンピューティングデバイスから前記クライアントデバイス・アプリケーションに、前記フォームログインプロトコルを介する認証要求の承認後に、セッション情報を送信することと、
前記コンピューティングデバイスが、前記クライアントデバイス・アプリケーションから、セッションの確認を受信することとをさらに含む、請求項１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が前記クライアントデバイス・アプリケーションから、前記コンピューティングデバイスがフォームログインプロトコルをサポートすることの指示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から前記クライアントデバイス・アプリケーションに、前記コンピューティングデバイスがフォームログインプロトコルをサポートすることを示すメッセージを送信することとをさらに含む、請求項１に記載の方法。
【請求項１１】
前記認証デバイスは前記拡張デバイスを含む、請求項１に記載の方法。
【請求項１２】
前記認証デバイスは、前記クライアントデバイス・アプリケーションに関連する前記認証サービスと、前記拡張デバイスとを含む、請求項１に記載の方法。
【請求項１３】
前記コンピューティングデバイスと前記クライアントデバイス・アプリケーションに関連する前記認証サービスとの間で送信される通信は第１暗号に従い暗号化されたデータを含み、前記認証デバイスと前記コンピューティングデバイスとの間で送信される通信は第２暗号に従い暗号化されたデータを含む、請求項１に記載の方法。
【請求項１４】
少なくとも１つのプロセッサと、
少なくとも１つのメモリとを具備し、前記少なくとも１つのメモリは、前記少なくとも１つのプロセッサで実行したときに、
コンピューティングデバイスから認証デバイスに、フォームログインプロトコルを介してクライアントデバイス・アプリケーションの認証要求を送信することと、
前記コンピューティングデバイスが前記認証デバイスから、第１の認証資格情報を要求する第１の資格情報フォームを読み取ることであって、前記第１の資格情報フォームは、前記認証デバイスに接続されている拡張デバイスにより、前記クライアントデバイス・アプリケーションに関連する認証サービスから受信する情報に基づいて生成され、前記拡張デバイスは前記クライアントデバイス・アプリケーションに関連する前記認証サービスの１つ以上の認証プロトコルを用いて構成されている、前記読み取ることと、

前記コンピューティングデバイスから前記クライアントデバイス・アプリケーションに、前記第１の資格情報フォームを送信することと、
前記コンピューティングデバイスが前記クライアントデバイス・アプリケーションから、前記第１の認証資格情報を受信することと、
前記コンピューティングデバイスから前記拡張デバイスを介して前記認証サービスに、前記第１の認証資格情報を送信することと、
前記コンピューティングデバイスが、前記第１の認証資格情報の妥当性検証の成功に応答して、前記フォームログインプロトコルを介して認証する前記クライアントデバイス・アプリケーションにより行われる前記要求の承認を送信することと、
をシステムに行わせる命令を格納している、システム。

【請求項１５】
前記コンピューティングデバイスが前記クライアントデバイス・アプリケーションに、前記第１の資格情報フォームを送信することは、前記コンピューティングデバイスが前記クライアントデバイス・アプリケーションに、前記第１の認証資格情報を取得するように構成されているプラグインメカニズムを呼び出す命令を送信することをさらに含み、前記プラグインメカニズムは前記クライアントデバイス・アプリケーションに関連する前記認証サービスと通信するように構成されている、請求項１４に記載のシステム。

【請求項１６】
前記命令は、前記システムに、
前記コンピューティングデバイスが前記認証デバイスから、第２の認証資格情報を要求する第２の資格情報フォームを取得することと、
前記コンピューティングデバイスから前記クライアントデバイス・アプリケーションに、前記第２の資格情報フォームを送信することと、
前記コンピューティングデバイスが前記クライアントデバイス・アプリケーションから、前記第２の認証資格情報を受信することと、
前記コンピューティングデバイスが前記認証デバイスに、前記第２の認証資格情報を送信することと、
をさらに行わせる、請求項１４に記載のシステム。

【請求項１７】
前記認証デバイスは前記クライアントデバイス・アプリケーションに関連する前記認証サービスと、前記拡張デバイスとを含む、請求項１４に記載のシステム。

【請求項１８】
１つ以上のプロセッサで実行されたときに、前記１つ以上のプロセッサに、
コンピューティングデバイスから認証デバイスに、フォームログインプロトコルを介してユーザデバイス上のクライアントデバイス・アプリケーションの認証要求を送信することと、
前記コンピューティングデバイスが前記認証デバイスから、第１の認証資格情報を要求する第１の資格情報フォームを取り出すことであって、前記第１の資格情報フォームは、前記認証デバイスに接続されている拡張デバイスにより、前記クライアントデバイス・アプリケーションに関連する認証サービスから受信した情報に基づいて生成され、前記拡張デバイスは前記クライアントデバイス・アプリケーションに関連する前記認証サービスの１つ以上の認証プロトコルを用いて構成されている、取り出すことと、
前記コンピューティングデバイスから前記クライアントデバイス・アプリケーションに、前記第１の資格情報フォームを送信することと、
前記コンピューティングデバイスが前記クライアントデバイス・アプリケーションから、前記第１の認証資格情報を受信することと、
前記コンピューティングデバイスから前記拡張デバイスを介して前記認証サービスに、前記第１の認証資格情報を送信することと、
前記コンピューティングデバイスが、前記第１の認証資格情報の妥当性検証の成功に応答して、前記フォームログインプロトコルを介して認証する前記クライアントデバイス・

アプリケーションが行う前記要求の認証を送信することと、
を行わせる命令を格納している１つ以上の不揮発性コンピュータ読取可能記憶媒体。
【請求項１９】
前記コンピューティングデバイスが前記クライアントデバイス・アプリケーションに、前記第１の資格情報フォームを送信することは、前記コンピューティングデバイスが前記クライアントデバイス・アプリケーションに、前記第１の認証資格情報を取得するように構成されているプラグインメカニズムを呼び出す命令を送信することをさらに含み、前記プラグインメカニズムは前記クライアントデバイス・アプリケーションに関連する前記認証サービスと通信するように構成されている、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記憶媒体。
【請求項２０】
前記命令は、前記１つ以上のプロセッサに、
前記コンピューティングデバイスが前記認証デバイスから、第２の認証資格情報を要求する第２の資格情報フォームを取得することと、
前記コンピューティングデバイスから前記クライアントデバイス・アプリケーションに、前記第２の資格情報フォームを送信することと、
前記コンピューティングデバイスが前記クライアントデバイス・アプリケーションから、前記第２の認証資格情報を受信することと、
前記コンピューティングデバイスから前記認証デバイスに、前記第２の認証資格情報を送信することと、
をさらに行わせる、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記憶媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本明細書に説明する諸側面は一般に、企業（enterprise）システム内のクライアントデバイスの認証に関するものである。より具体的には、本明細書の一定の側面は、サードパーティの認証サポートを介した企業システム上のクライアントデバイスの認証手法を提供する。
【背景技術】
【０００２】
以下に、本明細書に説明するさまざまな側面の簡単な概要を提示する。本概要は広範な全体像ではなく、重要なもしくは欠かせない要素を特定すること、または請求項の範囲を正確に説明することを意図していない。以下の概要は、以下に記載するより詳細な説明の導入として、単にいくつかの概念を簡単な形で提示するにすぎない。
【０００３】
スマートフォン、携帯情報端末、タブレットコンピュータ、他の種類のモバイルおよび非モバイルコンピューティングデバイスなどのモバイルデバイスはますます一般的になってきている。ますます多くの人が個人およびビジネス環境において多様な目的でモバイルデバイスを使用している。
【０００４】
モバイルデバイスを使用する人が増えるにつれて、アプリケーション開発者によってますます多くのモバイルアプリケーションが設計されるようになっている。これらのアプリケーション開発者は、ユーザおよびデバイスの妥当性検証に使用してもよい、彼らのアプリケーションまたは他の開発者のアプリケーションの認証方法を開発することがある。しかし、これらのアプリケーション開発者は、ｉＯＳおよびＡｎｄｒｏｉｄのようなモバイルデバイスのオペレーティングシステム上で稼動している企業管理対象アプリケーションに、彼らの認証プロトコルを実装することができないことがある。
【発明の概要】
【発明が解決しようとする課題】

【０００５】
上記背景に鑑みて、企業の認証プロトコルを維持し、企業認証に適用することのできる認証技術の革新を可能にしながら、サードパーティのアプリケーション開発者がその企業管理対象アプリケーションのために自身の認証プロトコルを実施できるようにする必要がある。たとえば、ユーザは、企業システムが管理しているかもしれないサードパーティのアプリケーションを認証するために、サードパーティの認証技術を利用したいことがある。

【０００６】
そのため、前述した先行技術における制限を克服するとともに、本明細書を読んで理解したときに明らかになる他の制限を克服するために、本明細書に説明する諸側面は企業システム内のクライアントデバイスをゲートウェイデバイスを介して認証および許可するアプローチを提供することに向けられる。

【課題を解決するための手段】
【０００７】
本開示の１つまたは複数の側面によれば、コンピューティングデバイスから認証デバイスに、フォームログインプロトコルを介してクライアントデバイス・アプリケーションの認証要求を送信することと、コンピューティングデバイスによって、認証デバイスから、第１の認証資格情報を要求する第１の資格情報フォームを読み取る（retrieve）こととを含む方法を提供し、前記第１の資格情報フォームは、前記認証デバイスに接続されている拡張デバイスにより、前記クライアントデバイス・アプリケーションに関連する認証サービスから受信した情報に基づいて生成され、前記拡張デバイスは前記クライアントデバイス・アプリケーションに関連する前記認証サービスの１つ以上の認証プロトコルを用いて構成されている。方法はさらに、コンピューティングデバイスによりクライアントデバイス・アプリケーションに、第１の資格情報フォームを送信することと、前記コンピューティングデバイスにより前記クライアントデバイス・アプリケーションから、前記第１の認証資格情報を受信することと、前記コンピューティングデバイスにより前記拡張デバイスを介して前記認証サービスに、前記第１の認証資格情報を送信することとを含んでもよい。方法はさらに、コンピューティングデバイスにより、前記第１の認証資格情報の妥当性検証の成功に応答して、前記フォームログインプロトコルを介して前記クライアントデバイス・アプリケーションにより行われる認証要求の承認を送信することを含んでもよい。

【０００８】
本開示の１つまたは複数の側面は、少なくとも１つのプロセッサと、前記少なくとも１つのプロセッサで実行されたときに、システムに１つ以上のステップを行わせる命令を格納する少なくとも１つのメモリとを含むシステムを提供する。システムが行えるステップは、コンピューティングデバイスにより認証デバイスに、フォームログインプロトコルを介してクライアントデバイス・アプリケーションの認証要求を送信することと、前記コンピューティングデバイスにより前記認証デバイスから、第１の認証資格情報を要求する第１の資格情報フォームを取得（retrieve）することとを含んでもよく、前記第１の資格情報フォームは、前記認証デバイスに接続されている拡張デバイスにより、前記クライアントデバイス・アプリケーションに関連する認証サービスから受信した情報に基づいて生成され、前記拡張デバイスは前記クライアントデバイス・アプリケーションに関連する前記認証サービスの１つ以上の認証プロトコルを用いて構成されている。ステップはさらに、前記コンピューティングデバイスにより前記クライアントデバイス・アプリケーションに、前記第１の資格情報フォームを送信することと、前記コンピューティングデバイスにより前記クライアントデバイス・アプリケーションから、前記第１の認証資格情報を受信することと、前記コンピューティングデバイスにより前記拡張デバイスを介して前記認証サービスに、前記第１の認証資格情報を送信することとを含んでもよい。ステップはさらに、前記コンピューティングデバイスにより、前記第１の認証資格情報の妥当性検証の成功に応答して、前記フォームログインプロトコルを介して前記クライアントデバイス・アプリケーションにより行われる認証要求の承認を送信することを含んでもよい。

【０００９】
本開示の１つまたは複数の側面は、１つ以上のプロセッサにより実行されたときに、前記１つ以上のプロセッサにステップを行わせられる命令を格納している１つ以上の不揮発性コンピュータ読取可能記憶媒体を提供する。１つ以上のプロセッサが行うステップは、コンピューティングデバイスにより認証デバイスに、フォームログインプロトコルを介してクライアントデバイス・アプリケーションの認証要求を送信することと、前記コンピューティングデバイスにより前記認証デバイスから、第１の認証資格情報を要求する第１の資格情報フォームを取り出す（retrieve）こととを含んでもよく、前記第１の資格情報フォームは、前記認証デバイスに接続されている拡張デバイスにより、前記クライアントデバイス・アプリケーションに関連する認証サービスから受信した情報に基づいて生成され、前記拡張デバイスは前記クライアントデバイス・アプリケーションに関連した前記認証サービスの１つ以上の認証プロトコルを用いて構成されている。ステップはさらに、前記コンピューティングデバイスにより前記クライアントデバイス・アプリケーションに、前記第１の資格情報フォームを送信することと、前記コンピューティングデバイスにより前記クライアントデバイス・アプリケーションから、前記第１の認証資格情報を受信することと、前記コンピューティングデバイスにより前記拡張デバイスを介して前記認証サービスに、前記第１の認証資格情報を送信することとを含んでもよい。ステップはさらに、前記コンピューティングデバイスにより、前記第１の認証資格情報の妥当性検証の成功に応答して、前記フォームログインプロトコルを介して前記クライアントデバイス・アプリケーションにより行われる認証要求の承認を送信することを含んでもよい。
【００１０】
以上および追加の側面は、以下のさらに詳細に述べる開示により認識されるであろう。
【００１１】
本明細書で説明する側面およびその利点は、添付の図面を考慮して以下の説明を参照すると、より完全な理解が得られる。図面において、同様の参照番号は同様の特徴を示す。
【図面の簡単な説明】
【００１２】
【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】企業モビリティ管理システムを示す図である。
【図４】別の企業モビリティ管理システムを示す図である。
【図５】本明細書で説明する１つ以上の特徴に従うシステムを示す模式図である。
【図６】本明細書で説明する１つ以上の特徴に従い、サードパーティの認証サポートにより企業システム上のクライアントデバイスの例示的な認証プロセスを示すフローチャートである。
【図７】本明細書で説明する１つ以上の特徴に従う例示的なシステムを示す模式図である。
【図８】本明細書で説明する１つ以上の特徴に従い、サードパーティ認証サービスを介した企業システム上のクライアントデバイスの例示的な認証プロセスを示すフローチャートである。
【図９】本明細書で説明する１つ以上の特徴に従う例示的なユーザインターフェースを示す図である。
【図１０】本明細書で説明する１つ以上の特徴に従う例示的なユーザインターフェースを示す図である。
【図１１】本明細書で説明する１つ以上の特徴に従う例示的なシステムを示す模式図である。
【発明を実施するための形態】
【００１３】

さまざまな実施形態の以下の説明において、上述のとおり特定し、本明細書の一部をなし、例示により本明細書で説明する側面を実施してもよい様々な実施形態を示す添付の図面を参照する。本明細書で説明する範囲を逸脱することなく、他の実施形態を利用し、構造および機能の変型を行えることは理解されるべきである。さまざまな側面は他の実施形態が可能であり、さまざまな異なる方法で実施または実行することが可能である。

【００１４】

以下詳細に説明する主題の概要紹介として、本明細書で説明する側面は、モバイルコンピューティングデバイスの管理対象モバイルアプリケーションを使用して、企業コンピューティングシステムのリソースへのリモートアクセスを制御することに向けられる。

【００１５】

アクセスマネージャは、企業リソースへのアクセスを要求するモバイルアプリケーションが正確に確認され、モバイルコンピューティングデバイスへのインストール後に後で改変されていないかどうかを判定する検証プロセスを行う。このように、アクセスマネージャは企業リソースへのアクセスを要求するモバイルアプリケーションが信頼でき、その企業リソースを保護するために使用されるセキュリティメカニズムを回避しようとしていないことを保証する。その結果、企業に関連する個人は、自分の私用モバイルデバイスで企業リソースを有利に利用することができる。

【００１６】

本明細書で使用される表現および用語は、説明目的であり、制限と見なしてはならないことは理解されるべきである。むしろ、本明細書で使用される表現および用語には、そのもっとも広い解釈および意味が与えられるべきである。「含み」および「備え」ならびにその変形の使用は、これ以降で挙げられるアイテムおよびその等価物ならびに追加アイテムおよびその等価物を包含することが意図されている。「取り付けられている」、「接続されている」、「連結されている」、「位置付けられている」、「係合されている」および同様な用語の使用は、直接および間接的な両方の取り付け、接続、連結、位置付けおよび係合を含むことが意図されている。

【００１７】

〈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。

【００１８】

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。

【００１９】

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、企業ネットワーク、ＬＡＮｓ、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。ローカルエリアネットワーク（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。

【００２０】

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。

【００２１】

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。

【００２２】

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。

【００２３】

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。

【００２４】

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。

【００２５】

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、さらにランダムアクセスメモリ（ＲＡＭ）１１３、リードオンリーメモリ（ＲＯＭ）１１５、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。

【００２６】

入力／出力（Ｉ／Ｏ）１１９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。
【００２７】
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。
【００２８】
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。
【００２９】
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。
【００３０】
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。
【００３１】
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。
【００３２】
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）ハイパーテキストマークアップランゲージ（ＨＴＭＬ）またはエクステンシブルマークアップランゲージ（ＸＭＬ）のようなスクリプト言語で書かれてもよい。
【００３３】
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。
【００３４】
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。

【００３５】
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。
【００３６】
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、ＲＡＭ２０５、ＲＯＭ２０７、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。
【００３７】
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。
【００３８】
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。
【００３９】
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。
【００４０】
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。
【００４１】
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、パーソナルデジタルアシスタント（ＰＤＡｓ）、ノートブック等）であってもよい。
【００４２】
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、ネットワークパーソナルコンピュータ（ＰＣｓ）、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。

【００４３】

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。

【００４４】

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。

【００４５】

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。

【００４６】

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。

【００４７】

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レシーバ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。

【００４８】

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。

【００４９】

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。

【００５０】

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。

【００５１】

実施形態によっては、サーバファームは、オペレーティングシステムプラットフォーム（例えば、ＷＩＮＤＯＷＳ（登録商標）、ＵＮＩＸ（登録商標）、ＬＩＮＵＸ（登録商標）、ｉＯＳ、ＡＮＤＲＯＩＤ（登録商標）、ＳＹＭＢＩＡＮ等）の実質的に同様のタイプを実行するサーバ２０６を含んでもよい。他の実施形態においては、サーバファーム２０６は、オペレーティングシステムプラットフォームの第１のタイプを実行する１つ以上のサーバの第１のグループ、および、オペレーティングシステムプラットフォームの第２のタイプを実行する１つ以上のサーバの第２のグループを含んでもよい。

【００５２】

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、セキュアソケットレイヤー（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。

【００５３】

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。

【００５４】

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。

【００５５】

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。

【００５６】

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。

【００５７】

〈企業モビリティ管理アーキテクチャ〉

図３は、ＢＹＯＤ環境での使用のための企業モビリティ技術アーキテクチャ３００を表す。アーキテクチャは、クライアントデバイス（例えば、モバイルデバイス）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。

【００５８】

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。

【００５９】

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。

【００６０】
いくつかの実施形態では、モバイルデバイスのオペレーティングシステムは、管理対象パーティション３１０と非管理対象パーティション３１２とに分離されていてもよい。管理対象パーティション３１０は管理対象パーティション上で稼動しているアプリケーションおよび管理対象パーティションに格納されているデータをセキュリティ保護するために、ポリシーをそれに適用させてもよい。管理対象パーティション上で稼動しているアプリケーションはセキュリティ保護されたアプリケーションであってもよい。他の実施形態では、すべてのアプリケーションはアプリケーションとは別に受信される１つ以上のポリシーファイルのセットに従って実行してもよく、このポリシーファイルのセットはデバイス上でアプリケーションが実行しているときに、モバイルデバイス管理システムによって強制される１つ以上のセキュリティパラメータ、特徴、リソース制限および／または他のアクセス制御を定義する。それぞれのポリシーファイルに従って操作することにより、各アプリケーションは１つ以上の他のアプリケーションおよび／もしくはリソースとの通信を許可または制限されてもよく、それによって仮想パーティションを作成する。
【００６１】
このように、本明細書で使用するパーティションとは、物理的に分割されたメモリの部分（物理的パーティション）、論理的に分割されたメモリの部分（論理的パーティション）ならびに／または本明細書で説明する複数のアプリにわたり１つ以上のポリシーおよび／もしくはポリシーファイルの強制の結果として作成される仮想パーティション（仮想パーティション）といってもよい。言い換えると、管理対象アプリにポリシーを強制することにより、そのアプリは他の管理対象アプリおよび信頼される企業リソースとのみ通信できるように制限してもよく、それによって非管理対象アプリおよびデバイスが入れない仮想パーティションを作成する。
【００６２】
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。
【００６３】
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。
【００６４】
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。

【００６５】

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、グラフィックユーザーインターフェース（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。

【００６６】

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。

【００６７】

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

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。

【００６８】

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。

【００６９】

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り、それらは遠隔設置されたリソースへのアクセスを提供する。

【００７０】

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。

【００７１】

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。

【００７２】

セキュリティ保護一般データは、アドバンストエンクリプションスタンダード(ＡＥＳ)１２８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、ＡＥＳ２５６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すなわち非管理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。

【００７３】

非セキュリティ保護すなわち非管理モードでは、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。

【００７４】

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。

【００７５】

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、マイクロＶＰＮまたはアプリケーション－スペシフィックＶＰＮとも呼ばれるが、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。

【００７６】

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、ハイパーテキストトランスファープロトコル（ＨＴＴＰ）トラフィック、ハイパーテキストトランスファープロトコルセキュア（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。

【００７７】

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。

【００７８】

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。

【００７９】

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。

【００８０】

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。

【００８１】

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。

【００８２】
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。
【００８３】
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。
【００８４】
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。
【００８５】
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５８０、プリラップ化アプリケーション３８２等を含んでいる。
【００８６】
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。
【００８７】
ソフトウェア開発キット３８４は、本明細書で上述したようにアプリケーションをラッピングすることにより、ユーザが選択したアプリケーションをセキュリティ保護する機能をユーザに提供してもよい。ソフトウェア開発キット３８４を用いてラッピングされたアプリケーションは、さらにアプリケーションコントローラ３７４を用いてアプリケーションストア３７８にそれを移植することにより、モバイルデバイス３０２に利用できるようにしてもよい。
【００８８】
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３８８を含んでもよい。管理および解析能力３８８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。
【００８９】

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。

【００９０】

この場合、左手側は、エンロールドクライアントデバイス４０２（例えば、モバイルデバイス）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、パブリック－キーインフラストラクチャー（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６０９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。

【００９１】

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。

【００９２】

クライアントエージェント４０４は企業データセンターでホストされるＷｉｎｄｏｗｓアプリ／デスクトップのＵＩ（ユーザインターフェース）媒介装置として機能し、企業データセンターはＨｉｇｈ－Ｄｅｆｉｎｉｔｉｏｎ Ｕｓｅｒ Ｅｘｐｅｒｉｅｎｃｅ（ＨＤＸ）／ＩＣＡ表示リモーティングプロトコルを使用してアクセスされる。

【００９３】

クライアントエージェント４０４は、ネイティブｉＯＳやＡｎｄｒｏｉｄアプリケーションなどのモバイルデバイス４０２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。たとえば、上述の図面に図示する管理対象アプリケーション４１０（メール、ブラウザ、ラッピングされたアプリケーション）はすべて、デバイス上でローカルに実行するネイティブアプリケーションである。このアーキテクチャの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は、企業リソース／サービス４０８との接続性やＳＳＯ（シングルサインオン）などのポリシーによる管理の機能および特徴を提供するように機能する。クライアントエージェント４０４は企業への、通常は他のゲートウェイサーバコンポーネントに対するＳＳＯによるアクセス・ゲートウェイ（ＡＧ）への、一次ユーザ認証を行う。クライアントエージェント４０４はゲートウェイサーバ４０６からポリシーを取得して、モバイルデバイス４０２上の管理対象アプリケーション４１０の挙動を制御する。

【００９４】

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

【００９５】

クライアントエージェント４０４およびゲートウェイサーバ４０６間の通信は、本質的に、各ネイティブな管理されたアプリケーション４１０をラップするアプリケーション管理フレームワーク４１４からの管理チャネルの拡張である。アプリケーション管理フレームワーク４１４は、クライアントエージェント４０４からポリシー情報を要求し、一方、

クライアントエージェント４０４は、ゲートウェイサーバ４０６からそれを要求する。アプリケーション管理フレームワーク４１４は、認証を要求し、クライアントエージェント４０４は、ゲートウェイサーバ４０６のゲートウェイサービス部分（ＮｅｔＳｃａｌｅｒ Ａｃｃｅｓｓ Ｇａｔｅｗａｙとしても知られる）にログインする。クライアントエージェント４０４は、ゲートウェイサーバ４０６上でサポートサービスも呼び出してもよく、これにより、以下でさらに完全に説明されるように、ローカルデータ貯蔵庫（ｄａｔａ ｖａｕｌｔｓ；以下「データボルト」、「ボルト」と言うことがある）４１６のための暗号化鍵を導出するための入力マテリアルを生成しても、または、ＰＫＩ保護リソースへの直接認証を有効化してもよいクライアント証明書を供給してもよい。

【００９６】

より詳細には、アプリケーション管理フレームワーク４１４は、各管理されたアプリケーション４１０を「ラップする」。これは、明示的な構築ステップを介して、または、構築後処理ステップを介して組み込まれてもよい。アプリケーション管理フレームワーク４１４は、アプリケーション４１０の最初のローンチにおいてクライアントエージェント４０４と「ペアリング」し、セキュリティ保護ＩＰＣチャネルを初期化し、そのアプリケーション用のポリシーを取得する。アプリケーション管理フレームワーク４１４は、クライアントエージェントのログイン依存性、および、ローカルＯＳサービスがいかに使用されてよいか、またはそれらがアプリケーション４１０といかに相互作用してよいかについて制限する制約ポリシーのいくつか等、ローカル適用のポリシーの関連部分を適用（enforce）する。

【００９７】

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。

【００９８】

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。

【００９９】

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ＡＧ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。

【０１００】

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、アクティブディレクトリ（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。

【０１０１】

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。

【０１０２】

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または生体検証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。

【０１０３】

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。

【０１０４】

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、とりわけパスワードーベースのキー派生関数２（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。

【０１０５】

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。

【０１０６】

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。

【０１０７】

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。

【０１０８】

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。

【０１０９】

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、ストアフロント（ＳｔｏｒｅＦｒｏｎｔ）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。

【０１１０】

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、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。

【０１１１】

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。

【０１１２】

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）。

【０１１３】

ｉＯＳ上のアプリケーション管理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キーチェーンへの公開鍵暗号標準（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。

【０１１４】

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。

【０１１５】

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アクティブディレクトリ（ＡＤ）４２２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、Ｃｉｔｒｉｘ　Ａｃｃｅｓｓ　Ｇａｔｅｗａｙ　Ｅｎｔｅｒｐｒｉｓｅ　Ｅｄｉｔｉｏｎ（ＡＧＥＥ）における制約付き委任に関し、ＡＧＥＥ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しおよび使用できる。この機構は、リバースウェブプロキシ（別名コーポレートヴァーチャルプライベートネットワーク（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。

【０１１６】

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。

【０１１７】

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。

【０１１８】

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。

【０１１９】

〈例示的な実施形態〉

図５、図７および図１１はシステムの例示的な模式図であり、図６および図８は例示的な模式フロー図であり、図９および図１０はユーザインターフェースの例示的な模式図である。これらのすべてがサードパーティの認証サポートを介した企業認証の特徴、方法およびシステムのさまざまな実施例を示す。

【０１２０】

図５～図１１を参照して以下説明する特徴および方法は、図１～図４に図示するさまざまなコンピューティングデバイスおよびシステムなど、コンピューティングデバイスまたはデバイスの組み合わせによって行ってもよく、図３および図４に図示する例示的なシステムなどのさまざまな異なるタイプの企業システム、または他の企業システム（つまり、リソースへのアクセスを与えるときに認証を要するコンピューティングデバイスまたはアプリケーション）内に実装してもよい。図５～図１１を参照して以下説明する特徴、ステップおよび方法は、述べられる順序以外で行ってもよく、１つ以上の特徴、ステップまたは方法を省略および／または追加してもよい。

【０１２１】

図５～図１１はゲートウェイ上、企業システム上（例、認証デバイスを介して）、および／またはサードパーティ認証デバイス上（例、クライアントデバイス上で稼動しているサードパーティのアプリケーションの認証サーバ）のユーザ、クライアントデバイスおよび／またはアプリケーションの認証に関する。

【０１２２】

たとえば、アプリケーションを稼動している端末２４０またはクライアントデバイス３０２もしくは４０２のユーザは、ゲートウェイ３６０または４０６経由で企業システムと通信してもよく、ユーザ、クライアントデバイスまたはアプリケーションのアイデンティティを妥当性検証するために認証資格情報を提供してもよく、さらに企業システムのさまざまなリソースおよびサービスを要求し、アクセスしてもよい。

【０１２３】

図５～１１は、セキュリティアサーションマークアップ言語（ＳＡＭＬ）など、認証および許可情報をやり取りするためのＸＭＬベースの方法であるさまざまなプロトコルを使用している。図６および図８で開示されるステップは、いずれも省略してもよく、述べられる順序以外で行ってもよく、繰り返しおよび／または組み合わせてもよい。

【０１２４】

いくつかの実施形態では、サードパーティのアプリケーション（例、管理対象アプリケーション）の認証方法を開発するサードパーティ（例、ベンダ、アプリケーション開発者等）をサポートしている。これらのサードパーティは、クライアントデバイスまたはユーザを認証する前に、証拠／資格情報を要求してもよい。これらのサードパーティの認証方法はステップアップ認証方法をサポートしてもよい。したがって、開示される実施形態はクライアントデバイスをサードパーティ認証サービス／システム（例、サードパーティのアプリケーションのため）とペアを組ませるとともに、企業認証デバイス／サービスとペアを組ませることができる。

【０１２５】

開示される実施形態では、代理のフォームサービスまたは拡張で認証フォームの生成および処理を可能にする。いくつかの側面によると、これらのフォームはＨＴＴＰまたはＨＴＴＰＳで送信されるＸＭＬフォームとしてもよい。クライアントデバイス、ゲートウェイデバイス、認証デバイス等の間でのフォームおよびレスポンスの流れは、パスワードまたは他の認証情報などのセンシティブな情報を含む会話を構成する。フォーム要求は、代理のフォームクライアントとサーバとの間の相互認証を含んでもよい。要求は、ＳＳＬト

ランスポートセキュリティが使用可能である、および／または使用されている場合でも、フォームレスポンスの暗号化を可能にする鍵素材を交換してもよい。いくつかの側面によると、相互認証および鍵交換を行ったら、セッションコンテキストが確立されてもよく、これを使用してクライアントとサーバとの間のメッセージを暗号化／解読するために使用してもよい。この暗号化は、侵入検知システムなど、ＳＳＬトランスポートレイヤを解読する他のシステムからのユーザまたはクライアントデバイスの資格情報を隠してもよい。

【０１２６】

いくつかの実施形態は、フォーム認証プロトコルをサポートしてもよく、これが、サードパーティに、１組のユーザインターフェース構造を使用して、多くのプラットフォームおよびオペレーティングシステムのために構成されている幅広い認証フォームを表現できるようにさせる。これらのサードパーティは、フォーム言語で定義されるフォームを発行および／または消費してもよいサーバロジックを実施することにより、企業認証方法（例、企業リソースおよびサービスで使用またはサポートされる）を拡張してもよい。このフォーム言語および関連プロトコルは、ネイティブユーザエージェント（例、クライアントデバイス上で稼動しているアプリケーション）および／またはオペレーティングシステムによってサポートされてもよい。

【０１２７】

いくつかの実施形態では、１つ以上のサービスまたはデバイス間におけるメッセージでクライアントデバイスの機能情報が渡されるようにしている。この情報はメッセージに添付されるＨＴＴＰヘッダに提供されてもよい。この機能情報はユーザエージェント、言語機能、資格情報タイプ情報、ラベルタイプ、ストレージ情報、クライアントアドレス、鍵交換情報等を含んでもよい。いくつかの実施形態において、クライアントセッションは、セッション識別情報を含んでもよいメッセージのヘッダを検査することにより識別してもよい。クライアントタイプ要素は、作成するセッションの機能の指示（例、セッションはＶＰＮ、ＣＶＰＮ等が可能であるかどうか）、ゲートウェイ背後のサーバ（例、企業サーバ）にアクセスするためにＵＲＬをどのように書き換えるべきかの指示を提供する情報を含んでもよく、セッションタイプを設定するためにゲートウェイに供給する必要がある可能性のある情報を含んでもよい（これは以下詳しく説明する）。

【０１２８】

いくつかの実施形態では、クライアントデバイスとのログイン会話をサポートするためにセッションクッキーの生成が可能であり、これはさまざまなセッションを混同しないように互いに分けておいてもよい。たとえば、クッキーはゲートウェイから送られて、クライアントデバイスに格納される少しのデータであってもよい。クッキーはＨＴＴＰクッキー、ウェブクッキー、ブラウザクッキー等であってもよい。クッキーはクライアントデバイスの現在のセッション（ログインしたセッションまたはゲートウェイセッションなど）を識別してもよい。セッションクッキーは一般に、現在の呼び出し元（例、クライアントデバイス）が前の呼び出し元と同じであるという一時的な証拠であってもよい。セッションクッキーは一般に一時的であってもよく、たとえば、クライアントデバイスが紛失したり盗まれたりした場合に、攻撃者がゲートウェイ／企業にログインを継続できないようにされている。

【０１２９】

いくつかの実施形態では、ゲートウェイ（または他の開示されるコンポーネント）はセッションクッキーに有効期限を添付し、および／または関連付けてもよい。たとえば、クッキーは５分の制限時間を有して、５分後に、現在のログインセッションを使用不可にして、その後クライアントデバイスはゲートウェイ（または他の開示されるコンポーネント）に再びログインしなければならないようにしてもよい。いくつかの実施形態では、トークンなどの他のセッション情報を使用してもよい。

【０１３０】

図５は、本明細書で説明される１つ以上の特徴を実装している例示的なシステム５００を示す。システム５００はクライアントデバイス３０２（例、図３から）を含んでいても

よく、これはコンピューティングデバイスまたはユーザデバイスであってもよく、端末２４０もしくは登録モバイルデバイス４０２に類似していても、または代わりに端末２４０もしくは登録モバイルデバイス４０２であってもよい。いくつかの例では、クライアントデバイス３０２はクライアントデバイス３０２上で稼動しているソフトウェア（例、クライアントアプリケーション）を含んでもよい。

【０１３１】

いくつかの側面によると、本明細書でクライアントデバイス３０２というときは必ず、該表現はクライアントデバイス３０２上で稼動している（および／もしくはその他関連する）コンピューティングデバイスまたはアプリケーションを含んでいてもよい。クライアントデバイス３０２は企業サービス３０８（例、図３から）と通信してもよい。企業サービス３０８は、アプリケーションコントローラ３７４、アプリケーションストア３７８、企業リソース３０４等のサービスを含んでもよい。クライアントデバイス３０２はゲートウェイ３６０と通信してもよく、これは図３のゲートウェイ３６０と同じものでもよく、および／またはゲートウェイ４０６と類似していてもよい。

【０１３２】

ゲートウェイ３６０はセキュリティ保護されたサーバであってもよく、１つ以上の個別のコンピューティングデバイスとして実装されていてもよい。あるいは、ゲートウェイ３６０はリソースもしくはサービス（例、電子メールサーバ、ウェブアプリケーションサーバ等）を提供するサーバまたは他のコンピューティングデバイス内に実装されていてもよい。ゲートウェイ３６０は、パスワードベース、トークンベース（例、スマートカード、磁気ストライプカード等）、生体情報（例、指紋、声紋、虹彩または網膜スキャン）、リスクベースの認証等、さまざまな追加の認証手法をサポートしてもよい。ステップ５０２で送信される認証情報は１要素または複数要素認証情報であってもよい。たとえば、複数要素認証では、ユーザはパスワードおよびユーザのスマートカードを与えてもよいが、１要素認証ではこのうちの一方だけを与えればよいだろう。認証は複数の認証ステップ（例、チャレンジ質問）および／または相互認証手法も含んでもよい。いくつかの側面によると、ゲートウェイ３６０はクラウド・ゲートウェイ、アクセス・ゲートウェイ等であってもよい。

【０１３３】

クライアントデバイス３０２は認証デバイス５０４と通信してもよい（例、ゲートウェイ３６０を介して）。たとえば、クライアントデバイス３０２は、認証要求および／または資格情報を認証サービスに送信することにより、ゲートウェイ３６０を介して認証デバイス５０４へのログインを試みてもよい。認証要求は、クライアントデバイス３０２が、コンソールアプリケーション、モバイルアプリケーション、ウェブブラウザ、ウェブベースのアプリケーションもしくは他のアプリケーションなど、クライアントデバイス３０２上で稼動しているセキュリティ保護化および／または非保護化アプリケーションを使用して、企業システムへのログインを試みることであってもよい。

【０１３４】

クライアントデバイス３０２のユーザは、クライアントデバイス３０２の入力インターフェース／デバイスを使用して、クライアントデバイス３０２に認証資格情報を入力してもよい。たとえば、ユーザはキーボードまたはタッチスクリーンを使用して、クライアントデバイス３０２にユーザ識別子および／またはパスワードを入力してもよい。クライアントデバイス３０２とのユーザのインタラクションの生体情報面を測定するために使用できるような加速度計、ジャイロスコープおよび他のセンサ／デバイスなど、開示される側面に従い他の種類の入力デバイスも使用してもよい。他の入力デバイスも同様に使用してもよい。認証資格情報は暗号化されて、ならびに／または企業システムのゲートウェイ（例、ゲートウェイ３６０）および／もしくは認証デバイス５０４にセキュアに送信されてもよい。資格情報はさらに認証デバイス５０４に送信されるかまたは渡されてもよい。

【０１３５】

いくつかの側面によると、認証デバイス５０４は認証サービス３５８と同じかまたは類

似していてもよく、それはコンピューティングデバイスおよび／またはサーバであってもよい。ある場合には、認証デバイス５０４は、アプリストア３７８またはアプリコントローラ３７４など、企業リソース（例、企業サービス３０８）の（またはその他の形で関連する）認証サービスであってもよい。くわえて、認証デバイス５０４は、フォームベースのログイン、パスワードログイン、Ｋｅｒｂｅｒｏｓログイン、スマートカードログイン、およびアクセスゲートシングルサインオン（ＡＧ　ＳＳＯ）等、認証／ログイン方法／タイプにさまざまなオプションおよびプロトコルを含んでもよい。

【０１３６】

本明細書で開示される側面に従い、他のログイン／認証方法を実装してもよいことに留意する。いくつかの側面によると、ゲートウェイ３６０は、たとえば、受信した認証資格情報をアクティブディレクトリ（ＡＤ４２２など）に提示することにより、クライアントデバイスを認証し、アクティブディレクトリが認証資格情報の正確さおよび／または妥当性を判断してもよい。該認証は、システム３００および／またはシステム４００などの企業システム上のクライアントデバイス３０２の認証のためであってもよい。

【０１３７】

認証デバイス５０４は、サードパーティ認証サーバ５１０と通信するサードパーティコネクタ５０６を含んでもよい。サーバ５１０はクライアントデバイス３０２により（例、クライアントデバイス３０２上で稼動しているアプリケーションにより）送信される認証資格情報を受信して妥当性検証するように構成されている認証サーバであってもよい。コネクタ５０６はサーバ５１０によって実施される１つ以上の認証プロトコルを用いて構成されていてもよい。該認証プロトコルはリスクベースの証拠、生体情報、テキストベースの情報、話声もしくは音声ベースの情報、ショートメッセージサービス、知識ベース認証、または他の種類の認証情報もしくは証拠を使用することを含んでもよい。コネクタ５０６は認証デバイス５０４の一部であってもよく、または個別のコンポーネント（例、個別のコンピューティングデバイス）であってもよい。コネクタ５０６はソフトウェア開発キット（ＳＤＫ）を用いて構成されている認証拡張に基づいていてもよい。

【０１３８】

サーバ５１０は、クライアントデバイス３０２から要求される要求認証情報などの情報を、コネクタ５０６を介して認証デバイス５０４に提供してもよい。コネクタ５０６はサーバ５１０から受信したこの情報を使って、認証デバイス５０４からゲートウェイ３６０を介してクライアントデバイス３０２に渡してもよいアイテム（例、フォーム、チャレンジ、質問等）を生成してもよい。いくつかの側面により、クライアントデバイス３０２がこの要求認証情報を受信した後、プラグイン５１４またはアプリケーションなど、クライアントデバイス３０２上に（またはクライアントデバイス３０２のリモートに）あるスクリプトまたはプログラムがサードパーティ認証プロトコル（例、生体認証）を呼び出してもよい。プラグイン５１４は、たとえば、クライアントデバイス３０２のユーザから、要求認証情報を要求してもよい。たとえば、ユーザに要求認証情報の入力を要求するクライアントデバイス３０２に、ユーザインターフェースを提示してもよい。

【０１３９】

いくつかの側面によると、このようなユーザインターフェースは、クライアントデバイス３０２に聴覚的にまたは視覚的に提示してもよい。たとえば、認証情報として指紋サンプルが要求される場合、プラグイン５１４は指紋サンプルを要求するユーザインターフェースを表示してもよく、また、指紋を採取するために、対応する指紋リーダまたはスキャナを選択してもよい。プラグイン５１４はサーバ５１０および／またはサーバ５１２からユーザインターフェース情報を取得してもよい（サードパーティゲートウェイデバイス５１６を介して）。

【０１４０】

図６は、本明細書で説明する１つ以上の特徴に従う、サードパーティの認証サポートを介したクライアント認証のフロー模式図を示す例示的なプロセス６００である。

【０１４１】

プロセス６００は、システム５００などのシステム実行される。たとえば、１つ以上の実施形態において、図６に示されるプロセス６００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、図１～図５のいずれかのデバイス）で行ってもよい。他の実施形態では、図６に示されるプロセスおよび／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などのコンピュータ読取可能媒体に格納されるコンピュータ実行可能命令に具現されてもよい。あるいは、または追加で、プロセス６００のステップのうちのいずれかを、クライアントデバイス、ゲートウェイデバイス、企業サーバマシン、および／またはサードパーティサーバもしくはコンピューティングデバイス上で行ってもよい。図５に図示するように、システム６００はクライアントデバイス３０２と、ゲートウェイデバイス３６０と、認証デバイス５０４と、コネクタ５０６と、サードパーティ認証サーバ５１０とを含んでいる。

【０１４２】

プロセス６００はステップ６０２から始まり、クライアントデバイス３０２はゲートウェイ３６０が特定のタイプのログオンプロトコルをサポートするかどうかをたずねる要求を送信する。たとえば、クライアントデバイス３０２上で稼動しているアプリケーションはフォームプロトコルを介して認証したいことがある。クライアントデバイス３０２はこの要求をＰＯＳＴ　ＨＴＴＰメッセージとして送信してもよい。メッセージは、ゲートウェイ３６０の認証要件、コンテンツタイプ（例、フォームプロトコルなど、所望のまたはサポートされる認証プロトコル／タイプ）、ユーザエージェント、ゲートウェイ３６０の場所／アドレス、およびゲートウェイ３６０のホストを判定する要求を含んでもよいフォームスタートＵＲＬに投稿してもよい。

【０１４３】

ステップ６０４で、ゲートウェイ３６０はクライアントデバイス３０２からこの要求を受信する。要求される認証プロトコル（例、フォーム認証）をゲートウェイ３６０がサポートしていない場合、ゲートウェイ３６０は、４０３　Ｆｏｒｂｉｄｄｅｎまたは３０２　Ｆｏｕｎｄ（例、／ｖｐｎ／ｉｎｄｅｘ．ｈｔｍｌなど、別のＵＲＬへのリダイレクト）など、クライアントデバイス３０２にフォールバックオプションを提供してもよい認識可能なＨＴＴＰレスポンスをクライアントデバイス３０２に送信してもよい。要求される認証プロトコルをゲートウェイ３６０がサポートしている場合、ゲートウェイ３６０は、サポートされるコンテンツタイプ（例、フォーム認証）を含んでもよい２００　ＯＫレスポンスなど、要求されるプロトコルをゲートウェイ３６０がサポートすることを示すレスポンスをクライアントデバイス３０２に送信してもよい。

【０１４４】

いくつかの側面によると、ステップ６０２および／または６０４は、クライアントデバイス３０２により出されたリソースアクセス要求の一部として、暗黙のうちに行われてもよい。ある場合には、リソースアクセス要求が、たとえば、ＨＴＴＰヘッダを使って、クライアントデバイス３０２がフォームログインプロトコル（または他の認証プロトコル）を理解することを示すことによって、認証チャレンジをトリガしてもよい。

【０１４５】

ステップ６０６で、要求されるプロトコルのサポートを示すゲートウェイ３６０からレスポンスを受信した後、クライアントデバイス３０２は所望の認証プロトコルを使ってログイン要求を開始する。この実施例では、ログオンプロトコルはフォームベースの認証プロトコルであってもよい。クライアントデバイス３０２は所望の認証プロトコルを理解してもよい。たとえば、クライアントデバイス３０２は認証プロトコルを理解するアプリケーションまたはプログラム（例、企業アプリケーション）を稼動してもよく、また、ゲートウェイ３６０（および／または他のコンポーネント）と通信してもよい。

【０１４６】

別の実施例では、クライアントデバイス３０２は、ＪａｖａＳｃｒｉｐｔ（登録商標）プログラム（例、企業から提供される）を稼動してもよく、認証プロトコルを理解してもよいウェブベースのアプリケーション（例、ウェブページ）を稼動してもよい。この実施

例では、クライアントデバイス３０２はログオンシーケンスを処理するために、ＷｅｂＶｉｅｗコントロールを（例、企業アプリケーションを使って）埋め込んでいる。たとえば、クライアントデバイス３０２上で稼動しているアプリケーションは企業システムへのログオンを望んでいることがあり、クライアントデバイス３０２はゲートウェイ３６０に共通フォームスタート位置（例、ＵＲＬ）へのＧＥＴ　ＨＴＴＰ要求を送信することにより、このフォームログイン要求を開始してもよい。いくつかの側面によると、この要求はゲートウェイ３６０の認証要件、コンテンツタイプ（例、フォームプロトコルなど、所望のまたはサポートされる認証プロトコル／タイプ）、ユーザエージェント、ゲートウェイ３６０の位置／アドレス、およびゲートウェイ３６０のホストなどの情報を含んでもよい。この要求は暗号化鍵（例、鍵交換）情報を含んでもよい。たとえば、クライアントデバイス３０２は、要求に、クライアントデバイス３０２がどのバージョンのフォームプロトコルを理解するかを示してもよい。たとえば、クライアントデバイス３０２は複数の互換性のあるバージョンを特定してもよい。

【０１４７】

いくつかの側面によると、フォームレスポンスはクライアントデバイス３０２からゲートウェイ３６０に（または、ゲートウェイ３６０からクライアントデバイス３０２に）送られる場合、フォーム値は暗号化してもよい。暗号化（ここと本明細書で開示されるあらゆる暗号化）は、ＡＥＳ－１２８暗号など、どのタイプの暗号化を使って実現してもよく、各固有の会話については、クライアントデバイス３０２とゲートウェイ３６０との間（または、開示されるあらゆるデバイス／コンポーネント間）で新たな暗号化鍵が合意される。このように、鍵情報は、パラメータ名と期待値とを含む鍵交換スキームを含んでもよい。いくつかの側面によると、鍵交換スキームを介してクライアントデバイス３０２とゲートウェイ３６０との間でネゴシエーションがあってもよい。これが合意に至ったら、この鍵を使って追加の通信を暗号化してもよい。フォームベースの認証プロトコルが説明されているが、あらゆる他のログオン／認証プロトコルを使用してもよい。

【０１４８】

いくつかの実施形態によると、ゲートウェイ３６０は、前のステップ６０６など、クライアントデバイス３０２の事前認証スキャン（例、エンドポイント分析（ＥＰＡ）スキャン）を行う。このスキャンは、リスクベースの認証について本明細書でさらに説明するのと同様なプロトコルを使用してもよい。このスキャンは、クライアントデバイス３０２がゲートウェイ３６０で認証を開始するのに十分クリーンな環境を備えるかどうかをチェックしてもよい（例、クライアントデバイス３０２が最新のシステムパッチ、稼動しているアンチウイルスソフトウェア等を有しているかどうかを確認するためにチェックする）。このスキャンは、ユーザに通知することなく、またはユーザにユーザインターフェースを表示することなく行ってもよい。

【０１４９】

いくつかの側面によると、ゲートウェイ３６０がクライアントデバイス３０２から追加情報を必要とする場合（例、ゲートウェイ３６０が要求ヘッダを検査することによりスキャンを行うことができない場合）、ゲートウェイ３６０はＥＰＡデータを要求するクライアントデバイス３０２にフォームを送信してもよい。たとえば、フォームはどの証拠を収集および／または供給すべきかを示してもよいＥＰＡ証拠要素を含んでもよく、証拠を提出するためのボタンを含んでもよい。いくつかの実施形態によると、フォームはユーザ提供の資格情報（認証サービス／デバイスが要求するものなど）とＥＰＡ証拠との組み合わせを要求してもよい。さらに、クライアントデバイス３０２はＥＰＡ証拠を収集して、ゲートウェイ３６０に投稿してもよい。さらに、ゲートウェイ３６０は供給された証拠を評価してもよい。たとえば、ゲートウェイ３６０は、クライアントデバイス３０２のＥＰＡ証拠がログオンに適した環境を備えていないとゲートウェイ３６０が判定する場合にログオンを拒否してもよく、また、クライアントデバイス３０２に表示されるエラーメッセージを含むフォームをクライアントデバイス３０２に送ってもよい。さらに、ゲートウェイ３６０はログオンプロセスを終了してもよい。別の実施例では、ゲートウェイ３６０は、

ＥＰＡ証拠がログオンに適した環境を示すとゲートウェイ３６０が判定する場合、ログオンプロセスを継続させてもよい。別の実施例では、ゲートウェイ３６０は、クライアントデバイス３０２が一定のアクションを行うことを条件に、ログオンを許可してもよい。ゲートウェイ３６０は、ゲートウェイ３６０が認証プロセスの続行をさせる前に行う必要がある可能性のあるＥＰＡアクション要素（例、アンチウイルスプログラムのインストール、アンチウイルススキャンの実行等）を示すフォームをクライアントデバイス３０２に送ることにより、クライアントデバイスにこれらのアクションを示してもよい。

【０１５０】

ステップ６０８で、フォームログイン要求の受信後、ゲートウェイ３６０は、事前設定済みのフォーム認証サーバのエンドポイント（例、企業認証デバイス５０４）に要求を送ることにより、フォーム認証セッションを開始してもよい。要求はクライアントデバイス３０２の機能に関する情報、以前の認証イベントからの格納データを含んでもよく、デバイス５０４はこれを認証要求の処理の方法を判定するために使用してもよい。要求はクライアントデバイス３０２のＩＰアドレスおよびクライアント証明書（例、ＳＳＬクライアント認証用）も含んでもよい。ゲートウェイ３６０は、暗号化鍵（前述）、通信チャネルの保護に使用してもよい暗号ノンス等、いくつかの追加のセキュリティ情報も生成してもよい。

【０１５１】

ステップ６１０で、要求を受信した後、デバイス５０４は要求をさらにコネクタ５０６に渡してもよく、さらにサードパーティ認証サーバ５１０に要求を渡してもよい。前述したように、サーバ５１０はクライアントデバイス３０２上で稼動しているアプリケーション（例、管理対象および／または非管理対象アプリケーション）のサードパーティ認証サーバであってもよい。いくつかの側面によると、コネクタ５０６はサードパーティサーバ５１０の認証プロトコルを用いて構成されてもよく、および／またはサードパーティサーバ５１０の認証プロトコルと互換性があってもよい。たとえば、コネクタ５０６は、サードパーティ認証サーバ５１０を認証デバイス５０４と通信できるようにさせてもよい認証デバイス５０４の拡張であってもよい。したがって、コネクタ５０６はサードパーティサーバ５１０が使用するいずれの認証プロトコルの知識を含んでいてもよい。いくつかの側面によると、デバイス５０４、コネクタ５０６および／またはサードパーティサーバ５１０は、事前共有鍵、ノンス、クライアントＩＤ、または鍵交換情報などのセキュリティ情報を使用して、暗号化鍵を生成してもよい。セキュリティ情報はさらにメッセージの暗号化に使用してもよい。

【０１５２】

ステップ６１２で、コネクタ５０６から要求を受信した後、サーバ５１０は、クライアントデバイス３０２の機能、過去の認証イベントから提示されてもよい格納データ、ノンス（nonces）、クライアントデバイス３０２のＩＰアドレス、および認証要求の処理方法の決定に役立つ他の情報（例、セキュリティ情報）を検査する。前述したように、サーバ５１０は、ノンスならびに、事前共有鍵、クライアントＩＤおよび／または鍵交換情報などの他のセキュリティ情報を使用して暗号化鍵を計算してもよく、これを使用してサーバ５１０が送信し、クライアントデバイス３０２またはコネクタ５０６が受信するレスポンスの全部または一部を暗号化してもよい。たとえば、レスポンスは、ユーザが答えることを選んだ知識ベースの質問など、センシティブな情報をそれ自体が含んでもよい認証チャレンジを含んでもよい。

【０１５３】

くわえて、サーバ５１０との認証セッションを表すセッションクッキーを生成／設定してもよい。サーバ５１０はさらに、リスクベースの証拠、生体情報、テキストベースの情報、話声もしくは音声ベースの情報、またはあらゆる他の種類の認証情報もしくは証拠など、１つ以上の認証プロトコルに対して資格情報をクライアントデバイス３０２が提供するよう要求することにより、サーバ５１０上でクライアントデバイス３０２を認証するよう要求してもよい（クライアントデバイス３０２のシェイクまたはスピン、物理的なカー

ド、トークンまたはフォブコードの、ある特定のグリッドリファレンスを探すこと等）。サーバ５１０はさらにクライアントデバイス３０２からの認証情報（例、指紋）を求める要求をコネクタ５０６に送信してもよい。

【０１５４】

ステップ６１４で、コネクタ５０６（および／または認証デバイス５０４）はサーバ５１０から要求された認証情報を含む資格情報フォームを生成する。たとえば、コネクタ５０６は指紋を要求する資格情報フォームを生成してもよい。くわえて、コネクタ５０６（および／またはデバイス５０４）はフォーム内で、認証デバイス５０４上でクライアントデバイス３０２を認証するために必要になる可能性のある追加認証情報を要求してもよい。たとえば、クライアントデバイス３０２は企業サービス３０８（例、アプリストア３７８）を要求したかもしれず、企業サービス３０８へのアクセスを許可する前に、企業認証デバイス５０４にログオンする、および／または企業認証デバイス５０４により認証される必要があるかもしれない。このように、コネクタ５０６（および／またはデバイス５０４）はフォームにこの追加で要求される認証情報（例、テキストベースのパスワード）を含んでもよい。コネクタ５０６（および／またはデバイス５０４）はさらに、この認証情報（例、サーバ５１０およびデバイス５０４の相互認証）のいずれかを含むフォーム（例、１つ以上のフォーム）を生成してもよく、このフォームをゲートウェイ３６０に送ってもよい。ゲートウェイ３６０に送信されるこのレスポンスは、暗号化鍵素材など、フォームへのレスポンスの暗号化を可能にしてもよいセキュリティ情報を含んでもよい。

【０１５５】

いくつかの側面によると、追加暗号化レイヤを使用して、資格情報処理チェーン内の１つ以上のコンポーネント／デバイスから情報（例、資格情報値または生体情報などの他の秘密情報）を隠してもよい。開示されるデバイスおよび／またはコンポーネント間で個別の暗号をネゴシエートして、同じ認証プロセスで使用される暗号化が複数あるようにしてもよい。たとえば、生体サンプルについて、クライアントデバイス３０２はゲートウェイ３６０、認証デバイス５０４、サードパーティコネクタ５０６および／またはサードパーティ認証サーバ５１０に対して暗号化をネゴシエートしてもよい。いくつかの側面によると、ゲートウェイ３６０と認証デバイス５０４との通信は第１暗号化鍵を使用してもよく、認証デバイス５０４（例、サードパーティコネクタ５０６を介して）とサードパーティ認証サーバ５１０との通信は第２鍵を使用してもよい。この状況は、たとえば、個別の認証プロトコル（例、ＳＳＯ）のために、認証デバイス５０４によって開封されて、ゲートウェイ３６０に返される企業パスワードを保護するために使用されてもよい。

【０１５６】

いくつかの側面によると、暗号化レイヤネゴシエーションを使用して、センシティブな情報の受取人（サードパーティコネクタ５０６など）がクライアントデバイス３０２（製造者など）に関連するエンティティによって信頼性を確認されたおよび／または承認された承認済みコードデバイス／モジュールであることを保証して、センシティブな情報を取り扱うときに受取人が確実に適切な配慮をするようにしてもよい。ある場合には、信頼性を確認された受取人には、公開／秘密鍵ペアまたは証明書など、暗号化鍵ネゴシエーション中に使用されるかまたはその他の形で検証されてもよい秘密を提供してもよい。

【０１５７】

ステップ６１６で、ゲートウェイ３６０はフォームを受信し、フォームの妥当性を確認する（例、スキーマチェックを使用して）。いくつかの側面によると、ゲートウェイ３６０はフォームの本体に含まれるホスト相対パス（例、ＰｏｓｔＢａｃｋおよびＣａｎｃｅｌＰｏｓｔＢａｃｋ）を調整してもよい。ゲートウェイ３６０はデバイス５０４および／または５１０によって生成されるクッキーも格納してもよい。ゲートウェイ３６０はクライアントデバイス３０２のゲートウェイ事前認証セッションクッキーを設定／生成してもよい。ゲートウェイ３６０は、クライアントデバイス３１０およびゲートウェイ３６０が以前の通信で合意していてもよい鍵を使用して、フォーム／メッセージを暗号化してもよい。ゲートウェイ３６０はさらにフォーム（クッキーなどの他の情報とともに）をクライ

アントデバイス３０２に送信してもよい。

【０１５８】

ステップ６１８で、クライアントデバイス３０２はゲートウェイ３６０から資格情報フォームを受信する。クライアントデバイス３０２はさらにフォームを処理し、フォームをレンダリングし、フォームを（例、クライアントデバイス３０２のユーザに）、たとえば、サーバ５１０および／またはデバイス５０４によって要求される情報（例、指紋および／またはテキストベースのパスワード）を要求するユーザインターフェースとして表示してもよい。サーバ５１０および／またはデバイス５０４により他の情報が要求された場合、それをクライアントデバイス３０２にレンダリングおよび／または表示してもよいことは留意される。

【０１５９】

いくつかの側面によると、クライアントデバイス３０２上に（またはクライアントデバイス３０２のリモートに）格納されてもよいプラグイン機構５１４をクライアントデバイス３０２で呼び出して、クライアントデバイス３０２に認証資格情報を要求するディスプレイもしくはユーザインターフェースを生成するか、または何か他の方法で認証資格情報を生成もしくは取得してもよい。いくつかの側面によると、ゲートウェイ３６０はクライアントデバイス３０２にプラグイン５１４を呼び出すよう指図してもよい（例、プラグイン５１４でクライアントデバイス３０２と一緒に進行してもよい）。たとえば、フォームがユーザ名および指紋サンプルを要求する場合、プラグイン５１４は正しい／対応するユーザインターフェース（指紋サンプルおよび／またはユーザ名）を表示するように構成してもよく、正しい／対応するリーダ、もしくはスキャナを表示しおよび／または取得して、指紋および／もしくはユーザ名を収集してもよい。くわえて、ユーザインターフェースは特定の入力モジュールを有していてもよい。たとえば、カスタムのキーボードレイアウトをレンダリングしてパスワードをタイプしてもよく、またはユーザ入力に関する情報を反映させないためにカスタムキーボード入力機構を使用してもよい。

【０１６０】

いくつかの側面によると、プラグイン５１４は、サードパーティ認証サーバ５１０などのサードパーティエンティティおよび／またはデバイスと通信してもよい。この場合、サードパーティエンティティはクラウドサービス／エンティティであってもよい。したがって、ある状況において、プラグイン５１４はサードパーティ認証サーバ５１０または別のサードパーティサーバ５１２から正しいフォームを提示するために必要な情報を取得してもよい。ある他の状況において、プラグイン５１４はサードパーティエンティティと通信するためのメカニズムを含んでいないかもしれない。このような場合、サードパーティ認証サーバ５１０が、サードパーティコネクタ５０６によってプラグイン５０４にフォームを利用できるようにするべきであることをクライアントデバイス３０２に認識させるようにフォーマット化されたあるフォーム（例、ｂａｓｅ６４符号化、ＸＭＬ、ＪＳＯＮ等）にフォーマット化される認証情報（認証チャレンジなど）を提供してもよい。

【０１６１】

このような状況において、サードパーティ認証サーバ５１０はプラグイン５１４に任意入力（例、指紋）を提供してもよい。いくつかの実施形態では、プラグイン５１４はクライアントデバイス３０２上で稼動しているアプリケーション（例、個別のアプリケーション）であってもよく（例、クライアントデバイス３０２のオペレーティングシステムがプラグイン機構をサポートしていない場合）、また、前述したのと同様な方法で呼び出してもよい。認証資格情報を収集した後、クライアントデバイス３０２は資格情報をゲートウェイ３６０に投稿してもよい。プラグイン５１４を使用することでクライアントデバイス３０２およびプラグイン５０４（または複数のプラグイン）をフォームの処理時に共同で呼び出させることができる。プラグイン５０４は、フォームがクライアントデバイス３０２によってユーザに表示される前に、フォーム情報を確認して修正してもよい。このように、いくつかの側面によると、プラグイン５０４は隠れて動作し、プラグイン５０４がユーザインターフェースを生成しないようにするが、フォームがクライアントデバイス３０

２によって表示される前にフォームを修正できるようにしてもよい。プラグイン５０４は、最終資格情報がゲートウェイ３６０に投稿される前に、このフォーム（ユーザと供給されるプラグインとの混合とすることができるであろう）で収集された資格情報も確認して処理してもよい。たとえば、（修正または未修正の）フォームから取得したユーザ入力をプラグイン５０４で使用して、本物の認証資格情報を取得または生成するのに役立てることができる。

【０１６２】

図９は、例示的なユーザインターフェース９００を示す。ユーザインターフェース９００はユーザ名テキストフィールド９０２と、パスワードテキストフィールド９０４と、ドメインドロップダウンリスト９０６と、パスワードを保存するチェックボックス９０８と、ログオンボタン９１０と、取消ボタン９１２と、安全な接続指示９１４と、命令９１６とを含んでいる。

【０１６３】

いくつかの側面によると、開示される実施形態はインライン画像も備えて、画像データをフォームに含めるようにしてもよく、これはたとえばサードパーティコネクタ５０６によって動的に生成することができるであろう。ある状況において、フォーム記述は意味論的意味に集中してもよく、開示されるコンポーネントはユーザインターフェースの処理および／またはディスプレイを意味論的意味に基づかせてもよい。いくつかの側面によると、開示される特徴は、開示される側面に従って使用してもよいさまざまなユーザインターフェース・スタイルガイドを有する異なるデバイスタイプとの互換性を可能にしてもよい。

【０１６４】

また、開示される実施形態は、インターフェース処理をプラットフォームスタイルまたは規約に一致させるように調整する、一般に認められているユーザインターフェースパターンを含んでもよい。ある場合には、取消ボタンなどのインターフェースの特徴は、プラットフォームに基づいて異なる種類のナビゲーションコントロールに取り換えてもよい。別の実施例では、ユーザ名フィールドの補助的テキストを生成してもよい。別の実施例では、フォームでユーザ名のドメイン修飾子などの特定の情報を含むようにとの補助的テキスト命令に従わなかった可能性があるユーザ入力を強調表示する。該インターフェース機能は意味論的アクションを含んでもよく、これはプラットフォーム固有のコントロールまたは直接可視化表現を有していないかもしれないジェスチャにより呼び出すこともできる。該インターフェース機能は、たとえばタイムアウトイベント中に、クライアントデバイス３０２によって強制および／または呼び出されてもよい。したがって、意味論的な認証フォームアプローチはクライアントライターで実施してもよく、ローカルなプラットフォーム規約への適応を許容するので、各クライアントデバイス（および／またはプラグイン）はフォームの表示をカスタマイズ可能にアレンジしてもよい。

【０１６５】

いくつかの側面によると、サードパーティ認証サーバ５１０および／または認証デバイス５０６は、たとえば、フォームが動的情報を含まないとき、フォームをキャッシュ可能としてマークしてもよい。クライアントデバイス３０２が鍵ネゴシエーションをまだサポートしていない場合、キャッシュされた初期フォームがユーザに表示されていてもよい間にクライアントデバイス３０２はＧＥＴ要求を送信してもよく（例、無駄な帯域幅を避けるためにＥＴＡＧで）、したがってゲートウェイ３６０に認証サーバ５１０および／または認証デバイス５０６との新鮮な認証会話を開始させることができる。いくつかの側面によると、クライアントデバイス３０２は予め登録された公開鍵に基づいて「一方向」スキームを使用してもよく、ゲートウェイ３６０は、第１の資格情報のＰＯＳＴが生成／送信されるときにオンデマンドでサードパーティ認証サーバ５１０および／または認証デバイス５０６と、自己の暗号化セッションをネゴシエートしてもよい。いくつかの実施形態によると、ゲートウェイ３６０は、ゲートウェイ３６０が認証サービス／デバイスから動的に受信したフォームを修正するときなど、キャッシングを使用不可にしてもよい。

【０１６６】
ステップ６２０で、ゲートウェイ３６０はクライアントデバイス３０２から資格情報を受信してもよい。いくつかの側面によると、暗号化は、クライアントデバイス３０２とゲートウェイ３６０との間で作用することができるであろう。ゲートウェイ３６０はデバイス５０４との認証セッションのために暗号化鍵で、ＰＯＳＴメッセージ本体の一部または全部を暗号化してもよい。ゲートウェイ３６０はさらに認証デバイス５０４にフォームを送信してもよい。
【０１６７】
ステップ６２２で、認証デバイス５０４は資格情報をコネクタ５０６に渡してもよく、さらにこれがサードパーティ認証サーバ５１０により要求される資格情報を渡してもよい。たとえば、コネクタ５０６は指紋のスキャンからの情報をサーバ５１０に渡してもよい。前述したように、暗号化は資格情報処理チェーン内のさまざまなデバイス／コンポーネント間で作用することができるであろう。たとえば、クライアントデバイス３０２からコネクタ５０６またはサードパーティ認証サーバ５１０まで「エンドツーエンド」の暗号化としてもよい。他の側面では、クライアントデバイス３０２からゲートウェイ３６０までの暗号化、ゲートウェイ３６０から認証デバイス５０４までの個別の暗号化（例、再暗号化）等であってもよい。
【０１６８】
ステップ６２４で、サードパーティ認証サーバ５１０はサードパーティサーバ５１２に格納されている資格情報で／に対して、これらの資格情報を妥当性検証／照合しようとしてもよい。いくつかの側面によると、さまざまな資格情報（例、生体情報、テキスト、話声、リスクベース等）は、サードパーティサーバ５１２などのサードパーティによって事前に格納されていてもよく、要求される資格情報と照合確認してもよい。たとえば、指紋資格情報からの情報がサーバ５１０に送信される場合、サーバ５１０はサーバ５１２の指紋資格情報と一致するかどうかを判定してもよい。一致する場合、資格情報はサードパーティ認証サーバ５１０が行う資格情報要求を満たしてもよい。一致しない場合、資格情報はサーバ５１０が行う資格情報要求を満たさないかもしれない。
【０１６９】
いくつかの側面によると、無効であると認定された資格情報をクライアントデバイス３０２が提出する場合、サーバ５１０は、資格情報が無効であると認定された理由をコネクタ５０６に示してもよく、コネクタ５０６は、前の資格情報のエントリ中に間違いがあったかもしれない箇所をクライアントデバイス３０２のユーザに案内する注釈または追加情報を含んでもよい追加の資格情報収集フォームを送信してもよい。
【０１７０】
いくつかの側面によると、ゲートウェイ３６０など、システム５００のいくつかのコンポーネントは記述エラー情報または注釈を取り除いてもよく、より一般的なエラーメッセージを実装してもよく、および／または認証を拒否してもよい。たとえば、ゲートウェイ３６０は自身の一定の認証ポリシー管理を認証プロセスに差し込んでもよい。該状況は、サードパーティ認証サーバ３１０、認証デバイス５０４およびコネクタ５０６をいくつかのクライアントデバイスが直接使用するが、他のクライアントデバイスはこれらのデバイスにゲートウェイ３６０を介してアクセスする場合に有利であるかもしれない。開示される実施形態は、認証意味を記述するためのフォーム記述を許容するこの種の層状コントロールに向けられる。
【０１７１】
いくつかの側面によると、ゲートウェイ３６０（および／または関連コネクタフィルタ）は自身の追加の認証ステップを挿入してもよい。たとえば、ゲートウェイ３６０は、ユーザがシステムにアクセスするために確認しなければならない（例、認証の成功の前に）法的免責事項を挿入してもよい。ゲートウェイ３６０は、これら追加の認証ステップを、確立された認証プロセスのいずれかのステップ（例、プロセス６００もしくは８００等の１つ以上のステップ）の前または後に、たとえば確立された認証プロセスの意味を理解す

る必要の有無に関係なく、挿入してもよい。

【０１７２】

いくつかの側面によると、異なるコンポーネントで制御してもよい複数の認証方法を組み合わせてもよい。たとえば、ゲートウェイ３６０はパスワード資格情報を要求して妥当性検証してもよいのに対し、サードパーティデバイス５１０はハードウェアトークンまたは他のスキーム（例、フォーム認証を介して）に基づいてワンタイムパスワードを要求してもよい。ゲートウェイ３６０はさらにコネクタ５０６が生成するフォーム内の意味論的情報を使用して、必要とする追加の資格情報要求（例、パスワード）を含むようにフォームを書き直してもよく、さらに異なるレスポンスの要素をクライアントデバイス３０２と分離（またはインターリーブ）してもよい。

【０１７３】

いくつかの側面によると、フォーム認証プロセス中、クライアントデバイス３０２は、変更パスワードフォームがいつ処理されるかを認識してもよく、異なるプロトコルの使用に切り替えて（例、フォームプロトコルから切り替えて）、安全な状態でパスワードの変更を行ってから、初期フォーム認証プロセスの後続ステップを続行してもよい。ある状況において、いくつかのクライアントデバイスはパスワードを安全に変更するためにＯＳＡＰＩの使用をサポートしてもよく、またはＫｅｒｂｅｒｏｓ変更パスワードプロトコルを使用してもよい。この特徴は、すでに危険な操作であるかもしれないパスワード変更に高度なセキュリティを可能にしてもよい。

【０１７４】

いくつかの側面によると、サードパーティ認証サーバ５１０は、クライアントデバイス３０２から送られた初期認証情報の妥当性検証後でも、クライアントデバイス３０２から追加の認証情報を要求してもよい。追加の認証情報の要求により追加のセキュリティが与えられてもよい。

【０１７５】

たとえば、リスクベース認証中、サーバ５１０はクライアントデバイス３０２からリスクベース認証（risk-based authentication; ＲＢＡ）の証拠（evidence）を要求してもよい。いくつかの側面によると、このＲＢＡの証拠は、ユーザのインタラクションなく、クライアントデバイス３０２から読み取って、クライアントデバイス３０２から送信してもよい。このように、企業アプリケーションまたはプログラムはクライアントデバイス３０２のデバイス特性を読み取ってもよく、１組のＲＢＡの証拠を構築してもよい。

【０１７６】

このＲＢＡの証拠は、ＲＢＡとともに使用するために特に生成されたＩＤなどのデバイスＩＤ、企業管理ＩＤ、および／またはクライアントデバイスに割り当てられるサードパーティＩＤを含んでもよい。いくつかの側面によると、これらのＩＤのうちの１つ以上は、ＭＡＣアドレス、ＵＤＩＤ等、ハードウェアＩＤに基づかなくてもよく、または基づいていなくてもよいだろう。ＲＢＡの証拠はジオロケーション、脱獄（ジェイルブレイク）ステータス、スクリーンサイズ、ならびに／またはセルラーおよび／もしくはデータプロバイダ／キャリア（例、国別コード、ネットワークコード、キャリア名等）を含んでもよい。ＲＢＡの証拠は、ユーザ選択のデバイス名、現在の時刻、標準時間帯、日時フォーマット（例、１２もしくは２４時間時計、日付表示順序）、表示言語（現在もしくは過去）、使用可能にされたキーボード等、ユーザ設定も含んでもよい。ＲＢＡの証拠は、メディア（例、楽曲、映像、画像、連絡先）情報など、ユーザデータ統計も含んでもよい。リスクベースの評価は既知のアクセスパターンを含んでもよい（例、クライアントデバイス３０２が未知の、またはよく知られていないアクセスパターンを使用している場合、おそらくリスクがあるかもしれない）。

【０１７７】

また、リスクベースの評価は攻撃の知識を使用して（例、リアルタイムの悪意の攻撃の知識）、現在の攻撃または差し迫った攻撃の知識がある場合、より高いリスクを認証要求に関連付けるようにしてもよい。いくつかの側面によると、あるＲＢＡの証拠はゲートウ

ェイ３６０および／または認証デバイス５０４から直接取得してもよい。この情報はクライアントデバイスのＩＰアドレス、ユーザエージェントストリング、ＳＳＬクライアント証明書等を含んでもよい。いくつかの側面によると、このＲＢＡの証拠または情報の少なくともいずれかに基づいて、サーバ５１０がアクセス／認証の状況が危険であるかもしれない（例、高リスクまたは中リスク）と判定する場合、サードパーティ認証サーバ５１０は追加の認証情報を要求してもよく、またはログインを拒否してもよい。

【０１７８】

図１０は、クライアントデバイス３０２に表示されてもよく、追加の認証情報を要求する例示的なユーザインターフェース１０００を示す。ユーザインターフェース１０００は一次命令１００２と、二次命令１００４と、入力を受けるように構成されているフィールド（例、テキストフィールド）１００６と、「次へ」ボタン１００８と、安全な接続の指示１０１０とを含んでもよい。ユーザインターフェース１０００はサーバ５１０が要求する追加の認証情報を要求するために使用してもよい。

【０１７９】

追加の認証情報が要求されない場合、図６のプロセス６００は、初期認証資格情報の妥当性検証の後に、ステップ６４０に進む。追加の認証情報が要求される場合、ステップ６２６で、サーバ５１０はクライアントデバイス３０２から要求される認証情報をコネクタ５０６に示す（例、ステップ６１２と同様）。

【０１８０】

ステップ６２８で、コネクタ５０６（および／または認証デバイス５０４）は資格情報フォームを生成して、これらのフォームをゲートウェイ３６０に送る（例、ステップ６１４と同様）。ステップ６３０で、ゲートウェイはこれらのフォームをクライアントデバイス３０２に送る（例、ステップ６１６と同様）。ステップ６３２で、クライアントデバイス３０２はこれらの資格情報を収集して、それをゲートウェイ３６０に送信する（例、ステップ６１８と同様）。ステップ６３４で、ゲートウェイはこれらの資格情報を収集して、それを認証デバイス５０４に送信する（例、ステップ６２０と同様）。ステップ６３６で、認証デバイス５０４はこれらの資格情報をコネクタ５０６に渡し、これが該資格情報をサードパーティ認証サーバ５１０に渡す（例、ステップ６２２と同様）。ステップ６３８で、サードパーティ認証サーバ５１０はさらに資格情報を妥当性検証しようとする（例、ステップ６２４と同様）。このプロセスは必要な回数繰り返してもよい。

【０１８１】

ステップ６４０で、認証資格情報の妥当性検証の成功後、サーバ５１０は妥当性検証の成功を示すＯＫレスポンス（例、ＨＴＴＰ　２００）を生成する。サーバ５１０はさらに認証デバイス５０４に（例、サードパーティコネクタ５０６を介して）、ユーザＩＤ、グループ情報、セッションパスワード等、クライアントデバイス３０２に関連する情報を送信する。たとえば、認証デバイス５０４はＲＢＡからのリスク評価情報、またはたとえばＳＡＭＬモデルに従ってもよいアイデンティティもしくは属性プロバイダによって主張されてもよいさまざまな種類のクレームを送信してもよい。

【０１８２】

この情報はさまざまな方法またはプロセスで使用してもよい。たとえば、ゲートウェイ３６０および／または認証デバイス５０４はクライアントデバイス３０２上で稼動しているアプリケーション（例、企業関連のアプリケーション）にスマートアクセス条件として情報を渡してもよく、これをさまざまなポリシー評価エンジンへの入力として使用してもよい。

【０１８３】

これらのポリシー管理はさらに、一定のリソースへのアクセスを遮断し、および／またはこれらのリソースを使用するときに、コピーアンドペースト機能の拒否、もしくは企業関連のアプリケーションを介してホストされる企業セッションからの印刷機能の拒否など、一定の機能を使用不可にするために使用してもよい。ある場合において、この情報の一部または全部を前のステップと同じ鍵を使用して暗号化してもよい。ステップ６４２で、

この情報とともにＯＫレスポンスをさらにゲートウェイ３６０に送信する。
【０１８４】
ステップ６４４で、ゲートウェイ３６０はＯＫレスポンスとともに、クライアントデバイス３０２に関連した追加情報（例、ユーザＩＤ、グループ情報、セッションパスワード等）を受信してもよい。ゲートウェイ３６０はこの情報（例、パスワード情報）を処理して妥当性検証してもよく、クライアントデバイス３０２に近似選択を提供してもよい。ゲートウェイ３６０およびクライアントデバイス３０２は、ＳＳＯ認証など、追加認証の目的のためにこのパスワード情報を使用してもよい。
【０１８５】
たとえば、クライアントデバイス３０２は認証デバイス５０４に認証要求をしてもよい（例、企業リソースにアクセスするため）。このような状況において、クライアントデバイス３０２は認証デバイス５０４との会話を開始し、それによりトークン発行者のトークンと要求される企業リソースのトークンとを交換してもよい。たとえば、認証デバイス５０４は認証デバイス５０４にログインするために多数の選択肢を示してもよい（例、シングルサインオン（ＳＳＯ）、パスワード、Ｋｅｒｂｅｒｏｓ、スマートカード、フォームログオン等）。認証の選択肢を選択した後、クライアントデバイス３０２は認証デバイス５０４から、要求される企業リソースのトークン発行者のトークンを要求してもよい。このトークンが、たとえば、認証デバイス５０４から提供された後、クライアントデバイス３０２はトークン発行者から、要求されるリソースにアクセスするためのトークンを要求してもよい。
【０１８６】
いくつかの側面によると、クライアントデバイス３０２と認証デバイス５０４との通信は、ゲートウェイ３６０を介してもよい。このような状況において、このプロセス中、ゲートウェイ３６０は認証プロセス（例、ＳＳＯログインのため）のステップ６４２で送信された情報（例、パスワード情報）を使用してもよい。他の状況においては、クライアントデバイス３０２は認証資格情報を認証デバイス５０４に渡してもよく、これが、これらの資格情報をアクティブディレクトリ４２２に格納されている資格情報と／に対して照合／妥当性検証してもよい。たとえば、ログインメカニズムがＡＤパスワードおよび／またはユーザ名を含む場合（例、ユーザがタイプしたため、もしくはパスワードボールトから復元されるため）、ゲートウェイ３６０はこのパスワードを認証済みのセッションデータの一部としてキャッシングしてもよい。企業リソースがゲートウェイ３６０を介してアクセスされた後、ゲートウェイ３６０はアクセスプロトコル（例、ウェブプロキシモード）を知ってもよい。企業リソースにより要求される認証は、ゲートウェイ３６０に、認証要求に反応して、キャッシュ情報（例、ユーザ名および／またはパスワード）を使ってレスポンスさせてもよく、これはクライアントデバイス３０２がこの知識を持たなくても行われてもよい。
【０１８７】
このように、ある場合において、クライアントデバイス３０２がフォームログインを使用して認証要求するステップは、発生する必要はないかもしれないが、フォームが新しい情報を含んでいる場合には発生してもよい。このキャッシング面は、認証チャレンジをずっとさかのぼってクライアントデバイス３０２まで送らなくてもよいかもしれないので、速度の改善をもたらすことがある。
【０１８８】
ゲートウェイ３６０はさらに、クライアントデバイス３０２に所望のセッションのタイプについての問い合わせを、クライアントデバイス３０２に送信してもよい。セッションタイプ（例、ＶＰＮ、ＣＶＰＮ、ＷＩＣＡ等）はセッションポリシーによって判定してもよく、クライアントデバイス３０２に認証レスポンスを送る前に（例、自動的に）適用してもよい。いくつかの側面によると、ゲートウェイ３６０は所望のセッションを判定する追加フォームを生成してもよく、これらのフォームをクライアントデバイス３０２に送ってもよい。これらのフォームはセッションタイプの選択肢を含んでもよく、ユーザはそこ

からセッションタイプを選択してもよい。ある場合において、セッションタイプはすでに確立されていてもよく、クライアントデバイス３０２がセッションタイプを選ぶ必要がなくてもよい。

【０１８９】

ステップ６４６で、ゲートウェイ３６０はこれらのフォームを受信して表示する。セッションのタイプを選択した後、クライアントデバイス３０２は所望のセッションタイプをゲートウェイ３６０に送信してもよい。

【０１９０】

ステップ６４８で、ゲートウェイ３６０はさらに、セッションのタイプに十分なライセンスがあるかどうか、および／またはセッション転送が必要な可能性があるかどうかを判定する。ある状況において、ゲートウェイ３６０は、企業が十分な数のライセンスを持っていないと判定するかもしれない。このような状況において、ゲートウェイ３６０は、クライアントデバイス３０２に送信および／または表示されてもよいエラーダイアログフォームおよび／またはＨＴＴＰ４８０レスポンスを生成してもよい。クライアント３０２がこのフォームを受理した時点で認証を拒絶してもよい。セッション転送が必要だとゲートウェイ３６０が判定する場合、ゲートウェイ３６０は（例、ユーザの）同意を要求するフォームをクライアントデバイス３０２に送信して、セッションを転送してもよい。転送で使用してもよいセッションが複数ある場合、フォームはこれらのセッションの選択肢を含んでもよい。このように、セッションを判定し、設定した後、ゲートウェイ３６０は選ばれたセッションタイプを起動してもよく、さらにＯＫ認証レスポンスを（例、セッション情報および／または他の情報とともに）クライアントデバイス３０２に送信してもよい。

【０１９１】

ある場合において、ゲートウェイ３６０は認証セッションクッキーをクライアントデバイス３０２に送信してもよく、これがクライアントデバイス３０２について認証されたゲートウェイセッションを確立してもよい。いくつかの側面によると、ゲートウェイ３６０はいずれかの事前認証セッション情報（例、事前認証クッキー、暗号化鍵等）を廃棄してもよく、追加情報（認証セッションクッキーまたは暗号化鍵等）をクライアントデバイス３０２に提供してもよい。

【０１９２】

いくつかの実施形態によると、ゲートウェイ３６０はクライアントデバイス３０２の事後ＥＰＡスキャンを行ってもよく、これは本明細書で説明する事前ＥＰＡスキャンと同様なものであってもよい。この事後ＥＰＡスキャンは、セッションタイプもしくは転送の判定または設定の前に行ってもよく、またクライアントデバイス３０２に認証成功レスポンスを送る前に行ってもよい。

【０１９３】

ステップ６５０で、妥当性検証した認証レスポンスの受信後、クライアントデバイス３１０は選択されたセッション（例、ＷＩＣＡ、ＣＶＰＮ等）を開始してもよい。

【０１９４】

図７は、本明細書で説明する１つ以上の特徴を実装することができる例示的なシステム７００を示す。システム５００はクライアントデバイス３０２（例、図３の）を含んでもよく、これはコンピューティングデバイスであってもよく、端末２４０または登録モバイルデバイス４０２と同様なものであってもよい。クライアントデバイス３０２は企業サービス３０８（例、図３の）と通信してもよい。企業サービス３０８は、アプリケーションコントローラ３７４、アプリケーションストア３７８、企業リソース３０４等のサービスを含んでもよい。クライアントデバイス３０２はゲートウェイ３６０と通信してもよく、これは図３および図５のゲートウェイ３６０と同じであっても、ならびに／またはゲートウェイ４０６と同様なものであってもよい。クライアントデバイス３０２は認証デバイス５０４と（例、ゲートウェイ３６０を介して）通信してもよい。ゲートウェイ３６０はサードパーティ認証サーバの１つ以上の認証ポリシーまたはプロトコルを用いて構成されていてもよい。

【０１９５】
いくつかの側面によると、認証デバイス５０４は認証サービス３５８と同じであっても、または同様なものであってもよい。ある場合において、認証デバイス５０４は、アプリストア３７８またはアプリコントローラ３７４など、企業リソースの（またはその他の形で関連する）認証サービスであってもよい。くわえて、認証デバイス５０４は、フォームベースのログイン、パスワードログイン、Ｋｅｒｂｅｒｏｓログイン、スマートカードログイン、およびアクセスゲートシングルサインオン（ＡＧ　ＳＳＯ）、ならびに同様なものなど、認証／ログインの方法／タイプについてさまざまなオプションおよびプロトコルを含んでもよい。本明細書に開示される側面によると、他のログイン／認証方法を実装してもよいことは留意される。

【０１９６】
いくつかの側面によると、ゲートウェイ３６０は、たとえば、受信した認証資格情報をアクティブディレクトリ（ＡＤ４２２など）に提示することによりクライアントデバイスを認証してもよく、これが認証資格情報の正確さおよび／または妥当性を判断してもよい。該認証は、システム３００および／またはシステム４００などの企業システムのクライアントデバイス３０２の認証のためであってもよい。

【０１９７】
システム７００はサードパーティ認証サーバ７１０を含んでいる。サーバ７１０は、クライアントデバイス３０２によって（例、クライアントデバイス３０２上で稼動しているアプリケーションによって）送信される認証資格情報を受信して妥当性検証するように構成されている認証サーバであってもよい。サードパーティ認証サーバ７１０は、サーバ７１０がゲートウェイ３６０および／またはクライアントデバイス３０２と通信するために使用してもよいサードパーティアダプタ７０６を含んでもよい。いくつかの側面によると、アダプタ７０６は異なるプラットフォームの複数のクライアントに及ぶように構成されていてもよく、また、ゲートウェイ３６０と（例、ＨＴＴＰまたはＨＴＴＰＳを介して）通信してもよい。アダプタ７０６はサーバ７１０の１つ以上の認証プロトコルを用いて構成されていてもよい。該認証プロトコルはリスクベースの証拠、生体情報、テキストベースの情報、話声もしくは音声ベースの情報、ショートメッセージサービス、知識ベース認証、または他の種類の認証情報もしくは証拠の使用を含んでもよい。アダプタ７０６は認証サービス７１０の一部であってもよく、または個別のコンポーネント（例、個別のコンピューティングデバイス）であってもよい。アダプタ７０６はソフトウェア開発キット（ＳＤＫ）を用いて構成されている認証拡張に基づいていてもよい。

【０１９８】
サーバ７１０は、クライアントデバイス３０２から要求される要求認証情報などの情報を、アダプタ７０６に提供する。アダプタ７０６はサーバ７１０から受信したこの情報を使用して、ゲートウェイ３６０を介してクライアントデバイス３０２に渡されるアイテム（例、フォーム、チャレンジ、質問等）を生成する。

【０１９９】
いくつかの側面によると、クライアントデバイス３０２がこの要求された認証情報を受信した後、クライアントデバイス３０２に（またはクライアントデバイス３０２のリモートに）あるプラグイン７１４またはアプリケーションなどのスクリプトまたはプログラムを呼び出してもよく、また、サードパーティ認証プロトコルを呼び出してもよい。プラグイン７１４は、あるフォームにおいて、たとえばクライアントデバイス３０２のユーザから要求される認証情報を要求してもよい。たとえば、クライアントデバイス３０２に、要求される認証情報の入力をユーザに要求するユーザインターフェースを提示してもよい。

【０２００】
いくつかの側面によると、このようなユーザインターフェースはクライアントデバイス３０２に聴覚的にまたは視覚的に提示してもよい。たとえば、認証情報として指紋サンプルが要求される場合、プラグイン７１４は指紋サンプルを要求するユーザインターフェースを表示してもよく、また、指紋を採取するために、対応する指紋リーダまたはスキャナ

を選択してもよい。プラグイン７１４はサーバ７１０および／またはサーバ７１２から（例、サードパーティゲートウェイデバイス７１６を介して）ユーザインターフェース情報を取り出してもよい。

【０２０１】

図８は、本明細書で説明する１つ以上の特徴によるサードパーティの認証サポートを介したクライアント認証のフロー模式図を示す例示的プロセス８００である。

【０２０２】

プロセス８００はシステム６００などのシステムで行ってもよい。たとえば、１つ以上の実施形態において、図８に図示するプロセス８００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、図１～図４および図７のいずれかのデバイス）で行ってもよい。他の実施形態では、図８に図示するプロセスおよび／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などのコンピュータ読取可能媒体に格納されているコンピュータ実行可能命令に具現されてもよい。あるいは、または追加で、プロセス８００のステップのいずれかをクライアントデバイス、ゲートウェイデバイス、企業サーバマシン、またはサードパーティサーバもしくはコンピューティングデバイス上で行ってもよい。図８に図示するように、システム８００はクライアントデバイス３０２と、ゲートウェイデバイス３６０と、認証デバイス５０４と、アダプタ７０６と、サードパーティ認証サーバ７１０とを含んでもよい。

【０２０３】

プロセス８００はステップ８０２から始まり、クライアントデバイス３０２はゲートウェイ３６０が特定のタイプのログオンプロトコルをサポートするかどうかをたずねる要求を送る。このステップは図６に関して上記説明したステップ６０２と同様である。

【０２０４】

ステップ８０４で、ゲートウェイ３６０はクライアントデバイス３０２からこの要求を受信する。要求される認証プロトコル（例、フォーム、シングルサインオン（ＳＳＯ）等）をゲートウェイ３６０がサポートしていない場合、ゲートウェイ３６０はクライアントデバイス３０２に、４０３　Ｆｏｒｂｉｄｄｅｎまたは３０２　Ｆｏｕｎｄ（例、ｖｐｎ／ｉｎｄｅｘ．ｈｔｍｌなどの別のＵＲＬへのリダイレクト）など、認識可能なＨＴＴＰレスポンスを送信してもよく、これがクライアントデバイス３０２にフォールバックオプションを提供してもよい。

【０２０５】

要求される認証プロトコルをゲートウェイ３６０がサポートしている場合、ゲートウェイ３６０はクライアントデバイス３０２に、２００　ＯＫレスポンスなど、サポートされるコンテンツタイプ（例、フォーム、ＳＳＯ等）を含む要求プロトコルをサポートすることを示すレスポンスを送信する。このステップは図６に関して上記説明したステップ６０４と同様である。

【０２０６】

ステップ８０６で、ゲートウェイ３６０から要求プロトコルのサポートを示すレスポンスを受信した後、クライアントデバイス３０２はログオンプロトコルを使ってログイン要求を開始する。この実施例では、ログオンプロトコルはフォームベースのプロトコルである。しかし、あらゆる他のログオン／認証プロトコルを使用してもよい。このステップは図６に関して上記説明したステップ６０６と同様であってもよい。

【０２０７】

いくつかの実施形態によると、ゲートウェイ３６０は、前のステップ８０６など、クライアントデバイス３０２の事前認証スキャン（例、エンドポイント分析（ＥＰＡ）スキャン）を行ってもよい。このスキャンは図６に関して上記でより詳細に述べている。

【０２０８】

ステップ８０８で、フォームログイン要求を受信した後、ゲートウェイ３６０は、サードパーティ認証サーバ・エンドポイント（例、サードパーティ認証サーバ７１０）に関連してもよい事前設定フォームサードパーティアダプタ７０６に要求を送ることにより、フ

ォーム認証セッションを開始する。要求はクライアントデバイス３０２の機能に関する情報と、認証要求の処理方法を決定するために使用してもよい過去の認証イベントからの格納データとを含んでもよい。要求はクライアントデバイス３０２のＩＰアドレスおよびクライアント証明書（例、ＳＳＬクライアント認証用）も含んでもよい。ゲートウェイ３６０は、暗号ノンスなど、通信チャネルを保護するために使用してもよい追加のセキュリティ情報も生成してもよい。

【０２０９】

ステップ８１０で、要求の受信後、アダプタ７０６は要求をサーバ７１０に渡す。前述したように、サーバ７１０はクライアントデバイス３０２上で稼動しているアプリケーション（例、管理対象および／または非管理対象アプリケーション）のサードパーティ認証サーバであってもよい。いくつかの側面によると、アダプタ７０６は、ゲートウェイ３６０および／またはサードパーティサーバ７１０の認証プロトコルを用いて構成されていてもよく、および／または認証プロトコルと互換性があってもよい。たとえば、アダプタ７０６は、サードパーティ認証サーバ７１０をゲートウェイ３６０と通信できるようにさせてもよいサーバ７１０の拡張であってもよい。したがって、アダプタ７０６はサードパーティサーバ７１０および／またはゲートウェイ３６０が使用する認証プロトコルの知識を含んでいてもよい。

【０２１０】

いくつかの側面によると、ゲートウェイ３６０、アダプタ７０６、およびサードパーティサーバ７１０は、事前共有鍵、ノンス、クライアントＩＤなどのセキュリティ情報を使用して、暗号化鍵を生成してもよい。セキュリティ情報はさらに、メッセージの暗号化に使用してもよい。くわえて、サーバ７１０との認証セッションを表すセッションクッキーをサーバ７１０によって生成／設定してもよい。サーバ７１０は、クライアントデバイス３０２の機能、過去の認証イベントから提示されてもよい格納データ、ノンス、クライアントデバイス３０２のＩＰアドレス、および認証要求の処理方法を決定するのに役立つ他の情報（例、セキュリティ情報）など、受信した情報を検査してもよい。

【０２１１】

サーバ７１０はさらに、リスクベースの証拠、生体情報、テキストベースの情報、話声もしくは音声ベースの情報、または他のタイプの認証情報もしくは証拠など、クライアントデバイス３０２が資格情報を１つ以上の認証プロトコルに与えることを要求することにより（クライアントデバイス３０２のシェイクまたはスピン、物理的なカード、トークンまたはフォブコードの、ある特定のグリッドリファレンスを探すこと、および同様なこと）、クライアントデバイス３０２をサーバ７１０上で認証するよう要求してもよい。サーバ７１０はさらにクライアントデバイス３０２からの認証情報（例、指紋）を求める要求をアダプタ７０６に送信してもよい。アダプタ７０６（および／または認証デバイス５０４）はサーバ７１０から要求された認証情報を含む資格情報フォームを生成してもよい。

【０２１２】

ステップ８１２で、ゲートウェイ３６０はこのフォームを受信し、フォームの妥当性を確認する（例、スキーマチェックを使用して）。いくつかの側面によると、ゲートウェイ３６０は、フォームの本体に含まれていてもよいホスト相対パス（例、ＰｏｓｔＢａｃｋおよびＣａｎｃｅｌＰｏｓｔＢａｃｋ）を調整してもよい。ゲートウェイ３６０はまた、デバイス５０４および／またはサーバ７１０によって生成されるクッキーも格納してもよい。ゲートウェイ３６０はクライアントデバイス３０２のゲートウェイ事前認証セッションクッキーを設定／生成してもよい。ゲートウェイ３６０はクライアントデバイス３１０およびゲートウェイ３６０が以前の通信で合意される鍵を使用して、フォーム／メッセージを暗号化してもよい。ゲートウェイ３６０はさらにフォームを（クッキーなどの他の情報とともに）クライアントデバイス３０２に送信してもよい。

【０２１３】

ステップ８１４で、クライアントデバイス３０２はゲートウェイ３６０から資格情報フォームを受信する。クライアントデバイス３０２はさらに、フォームを処理し、フォーム

をレンダリングし、フォームを（例、クライアントデバイス３０２のユーザに）たとえばユーザインターフェースとして表示してもよい。いくつかの側面によると、クライアントデバイス３０２に（またはクライアントデバイス３０２のリモートに）格納されていてもよいプラグインメカニズム７１４をクライアントデバイス３０２で呼び出して、認証資格情報を要求するディスプレイまたはユーザインターフェースをクライアントデバイス３０２に生成してもよい。プラグイン７１４はサードパーティ認証サーバ７１０または別のサードパーティサーバ７１２から正しいフォームを提示するために必要な情報を取得してもよい。いくつかの実施形態では、プラグイン７１４はクライアントデバイス３０２上で稼動しているアプリケーションであってもよい（例、クライアントデバイス３０２のオペレーティングシステムがプラグインメカニズムをサポートしていない場合）。認証資格情報の収集後、クライアントデバイス３０２はデータをゲートウェイ３６０にＰＯＳＴしてもよい。

【０２１４】

ステップ８１６で、ゲートウェイ３６０はクライアントデバイス３０２から資格情報を受信する。ゲートウェイ３６０は、デバイス５０４との認証セッションのために、ＰＯＳＴメッセージ本体の一部または全部を暗号化鍵で暗号化してもよい。ゲートウェイ３６０はさらにフォームをアダプタ７０６に送信してもよい。

【０２１５】

ステップ８１８で、アダプタ７０６は認証サーバ７１０に資格情報を渡す。たとえば、アダプタ７０６は指紋のスキャンからの情報をサーバ７１０に渡してもよい。サードパーティ認証サーバ７１０はさらにこれらの資格情報をサードパーティサーバ７１２に格納されている資格情報で／に対して妥当性検証／照合しようとしてもよい。一致する場合、資格情報はサードパーティ認証サーバ７１０が行う資格情報要求を満たしてもよい。一致しない場合、資格情報はサーバ７１０が行う資格情報要求を満たさないかもしれない。

【０２１６】

いくつかの側面によると、無効であると認定された資格情報をクライアントデバイス３０２が提出する場合、サーバ７１０は、資格情報が無効と認定された理由をアダプタ７０６に示してもよく、アダプタ７０６は、前の資格情報のエントリ中に間違いがあったかもしれない箇所をクライアントデバイス３０２のユーザに案内する注釈または追加情報を含んでもよい追加の資格情報収集フォームをクライアントデバイス３０２に送信してもよい。

【０２１７】

いくつかの側面によると、サードパーティ認証サーバ７１０は、クライアントデバイス３０２によって送られた初期認証情報の妥当性検証後でも、クライアントデバイス３０２から追加の認証情報を要求してもよい。追加の認証情報の要求により追加のセキュリティが与えられてもよい。

【０２１８】

図１０は、クライアントデバイス３０２に表示し、上記説明した追加の認証情報を要求する例示的なユーザインターフェース１０００を示す。ある実施例において、リスクベース認証中、サーバ７１０はクライアントデバイス３０２からリスクベース認証（ＲＢＡ）の証拠を要求してもよい。

【０２１９】

追加の認証情報が要求されない場合、プロセス８００は初期認証資格情報の妥当性検証の後にステップ８３０に進む。追加の認証情報が要求される場合、ステップ８２０で、サーバ７１０はクライアントデバイス３０２から要求される認証情報をアダプタ７０６に示す（例、ステップ８１０と同様）。アダプタ７０６はさらに資格情報フォームを生成して、これらのフォームをゲートウェイ３６０に送ってもよい。

【０２２０】

ステップ８２２で、ゲートウェイはこれらのフォームをクライアントデバイス３０２に送る（例、ステップ８１２と同様）。ステップ８２４で、クライアントデバイス３０２は

これらの資格情報を収集して、それをゲートウェイ３６０に送信する（例、ステップ８１４と同様）。ステップ８２６で、ゲートウェイ３６０はこれらの資格情報を収集して、それをアダプタ７０６に送信する（例、ステップ８１６と同様）。ステップ８２８で、アダプタ７０６は資格情報をサードパーティ認証サーバ７１０に渡す（例、ステップ８１８と同様）。サードパーティ認証サーバ７１０はさらに資格情報を妥当性検証しようとしてもよい。

【０２２１】

ステップ８３０で、認証資格情報の妥当性検証の成功後、サーバ７１０は妥当性検証の成功を示すＯＫレスポンス（例、ＨＴＴＰ　２００）を生成し、これをサードパーティサーバ７１２から取り出されるユーザＩＤ、グループ情報、セッションパスワード等、クライアントデバイス３０２に関連する情報とともに、（例、サードパーティアダプタ７０６を介して）ゲートウェイ３６０に送信する。ある場合において、この情報の一部または全部を前のステップと同じ鍵を使用して暗号化してもよい。

【０２２２】

ステップ８３２で、ゲートウェイ３６０はＯＫレスポンスをクライアントデバイス３０２に関連する追加情報（例、ユーザＩＤ、グループ情報、セッションパスワード等）とともに受信する。ゲートウェイ３６０はこの情報（例、パスワード情報）を処理して妥当性を検証してもよく、クライアントデバイス３０２に近似する選択（approximate choice）を提供してもよい。ゲートウェイ３６０およびクライアントデバイス３０２は、シングルサインオンなど、図６に関して上記説明した追加認証の目的のためにこのパスワード情報を使用してもよい。これらの追加認証プロセス中、ゲートウェイ３６０はステップ８３２の認証プロセスで（例、ＳＳＯログインのため）ゲートウェイ３６０に送信された情報（例、パスワード情報）を使用してもよい。ゲートウェイ３６０はパスワード情報をアクティブディレクトリ４２２に格納されている情報と／に対して照合／妥当性検証してもよい。

【０２２３】

ゲートウェイ３６０はさらに、クライアントデバイス３０２に所望のセッションのタイプについての問い合わせを、クライアントデバイス３０２に送信してもよい。セッションタイプ（例、ＶＰＮ、ＣＶＰＮ、ＷＩＣＡ等）はセッションポリシーによって判定してもよく、クライアントデバイス３０２に認証レスポンスを送る前に適用してもよい。ゲートウェイ３６０は所望のセッションを判定する追加フォームを生成してもよく、これらのフォームをクライアントデバイス３０２に送ってもよい。これらのフォームはセッションタイプの選択肢を含んでもよく、ユーザはそこからセッションタイプを選択してもよい。ある場合において、認証成功の後、セッションタイプはすでに確立されていてもよく、クライアントデバイス３０２がセッションタイプを選ぶ必要がなくてもよい。

【０２２４】

ステップ８３４で、ゲートウェイ３６０はこれらのフォームを受信して表示する。セッションタイプの選択を行った後、クライアントデバイス３０２は所望のセッションタイプをゲートウェイ３６０に送信してもよい。

【０２２５】

ステップ８３６で、ゲートウェイ３６０はさらに、図６に関してステップ６４８で上記説明したセッションのタイプに十分なライセンスがあるかどうか、および／またはセッション転送が必要な可能性があるかどうかを判定する。セッション転送が必要だとゲートウェイ３６０が判定する場合、ゲートウェイ３６０は（例、ユーザの）同意を要求するフォームをクライアントデバイス３０２に送信して、セッションを転送してもよい。転送で使用してもよいセッションが複数ある場合、フォームはこれらのセッションの選択肢を含んでもよい。このように、セッションを判定し、設定した後、ゲートウェイ３６０は選ばれたセッションタイプを起動してもよく、さらにＯＫ認証レスポンスと（例、セッション情報および／または他の情報とともに）クライアントデバイス３０２に送信してもよい。

【０２２６】

ある場合において、ゲートウェイ３６０は認証セッションクッキーをクライアントデバイス３０２に送信し、事前認証セッション情報を廃棄し、追加情報（認証セッションクッキーまたは暗号化鍵など）をクライアントデバイス３０２に提供してもよい。

【０２２７】

いくつかの実施形態によると、ゲートウェイ３６０はクライアントデバイス３０２の事後ＥＰＡスキャンを行ってもよく、これは本明細書で説明する事前ＥＰＡスキャンと同様であってもよい。この事後ＥＰＡスキャンは、セッションタイプもしくは転送の判定または設定の前に行ってもよく、またクライアントデバイス３０２に認証成功レスポンスを送る前に行ってもよい。

【０２２８】

ステップ８３８で、妥当性検証した認証レスポンスの受信後、クライアントデバイス３１０は選択されたセッション（例、ＷＩＣＡ、ＣＶＰＮ等）を開始する。

【０２２９】

図１１は、本明細書で説明する１つ以上の特徴を実装している例示的なシステム１１００を示す。システム１１００はクライアントデバイス３０２と、ゲートウェイ３６０と、企業サービス３０８と、認証サービス１１０４（認証デバイス５０４および／もしくは７０４と同じもの、類似のもの、ならびに／または組み合わせでもよい）と、サードパーティコネクタ５０６と、サードパーティアダプタ７０６と、サードパーティ認証サーバ１１１０（サードパーティ認証サーバ５１０および／もしくは７１０と同じもの、類似のもの、ならびに／または組み合わせでもよい）と、サードパーティサーバ１１１２（サードパーティサーバ５１２および／もしくは７１２と同じもの、類似のもの、ならびに／または組み合わせでもよい）と、アクティブディレクトリ４２２と、プラグイン１１１４（プラグイン５１４および／もしくは７１４と同じもの、類似のもの、ならびに／または組み合わせでもよい）と、サードパーティゲートウェイ１１１６（サードパーティゲートウェイ５１６および／もしくは５１８と同じもの、類似のもの、ならびに／または組み合わせでもよい）とを含んでいる。

【０２３０】

システム１１００はシステム５００および７００の連携環境を示し、図５～図８に関して本明細書で説明するステップのうち任意のステップを行う。たとえば、ゲートウェイ３６０は、ゲートウェイ３６０に格納されているポリシーに応じて、どのコンポーネント（例、認証デバイス１１０４またはアダプタ７０６）と通信させるか、ゲートウェイ３６０の認証構成、クライアントデバイス３０２がどのタイプのログインプロトコルを選択したか等を判定してもよい。くわえて、前述したように、ゲートウェイ３６０は複数のソースからの認証方法を組み合わせて、および／または選択的に選んで、集約または合体した認証プロセスを作成してもよい。このように、ゲートウェイ３６０は独立して作成された２つ以上の認証方法（拡張）を組み合わせて、これらの認証方法を所定の順序またはシーケンスで実施する。

【０２３１】

いくつかの側面によると、ゲートウェイ３６０はクライアントのタイプ（ユーザエージェント）、ＩＰアドレス等、認証要求の属性に基づいて順序を動的に判定してもよい。ポリシーに基づいて、ゲートウェイ３６０は、たとえば、ログインを完了するために認証方法の一部または全部を渡す（例、妥当性検証する）よう要求してもよく、またはゲートウェイ３６０は、第１の認証方法が妥当性検証の成功を報告した後に認証プロセスを停止してもよいかもしれない（例、ＡＮＤとＯＲとの組み合わせ法を使用する）。クライアントデバイス３０２の観点から異なる段階を重複させて、２つ以上の認証サーバ（例、サードパーティ認証サーバ）が要求する資格情報を単一フォームに合体するようにしてもよい。

【０２３２】

いくつかの側面によると、これらの認証サーバは、ローカルアカウントシステムがある場合など、ゲートウェイ３６０の一部であってもよい。いくつかの側面によると、複数の認証サーバが資格情報（例、ユーザ名）を要求し、それが同じであることが予想または要

求されるかもしれない場合、合体フォームが情報（例、ユーザ名）を一回要求してもよい。

【０２３３】

いくつかの実施形態では、合体プロセスを案内するために、認証サーバ（例、サードパーティ認証サーバ）はフォームの資格情報要求フィールドを、提供されてもよい意味内容を超えるようにタグ付けしてもよい。たとえば、数値（例、１００、２００、３００等）を一定の規約に従って各フィールドに記載して、組み合わせたときにフィールドが昇順になるようにしてもよい。組み合わせられる認証ソースは、たとえば、プロセス６００および／または８００を個々に使用して、ゲートウェイ３６０と通信してもよい。いくつかの側面によると、複数の認証方法の成功が情報（例、ユーザ／グループ／資格情報）に矛盾を与える場合、ゲートウェイ３６０はさまざまなポリシーを使用してもよい。いくつかの側面によると、開示される１つ以上のコンポーネント（例、ゲートウェイ３６０、クライアントデバイス３０２等）が複数のフォームを逐次的にまたは同時に送信および／または受信してもよい。

【０２３４】

いくつかの側面によると、各認証デバイス／サーバは、ゲートウェイ３６０だけよりも、クライアントデバイス３０２と暗号化鍵を供給したいかもしれない。このような場合、ゲートウェイ３６０が次の認証デバイス／サーバの通信に切り替えた後、認証プロセス中に暗号化鍵ネゴシエーションステップを繰り返してもよい。

【０２３５】

いくつかの側面によると、ゲートウェイ３６０は、たとえば、ローカルで定義されるアカウントおよび／またはパスワードに基づいて、または認証サーバ／デバイス、ＡＤ４２２または他のタイプのアカウントディレクトリと通信するための他の認証プロトコルを使用して、これらの認証ステップのうちの１つ以上を処理してもよい。たとえば、図７を参照すると、ゲートウェイ３６０は、ＡＤ４２２またはサードパーティ認証サーバ７１０を用いてユーザ名および／またはパスワードを妥当性検証するためにさまざまなプロトコルを使用している。ゲートウェイ３６０はゲートウェイ３６０が生成するフォームを使用してクライアントデバイスにこの資格情報を求める要求を提示してもよく、またはゲートウェイ３６０はこの情報を要求するフィールドと認証サーバ／デバイスが提供するフォームとを合体させてもよい。

【０２３６】

いくつかの側面によると、合体プロセスは、異なる認証サーバ／デバイスに関連する認証プロセスから、個々の認証ステップをインターリーブすることを含んでもよい。ある実施例は、認証サーバがリスク分析を行っているときでもよい。このような場合、認証サーバが分析を行う前に、ゲートウェイ３６０は称されるユーザアイデンティティをあるレベルの信頼度で証明するためには、１つ以上のユーザ資格情報（例、ユーザ名、パスワード等）を妥当性検証する必要があってもよい。しかし、ユーザのパスワードが期限切れで、ログインを完了するために変更しなければならない場合、認証サーバ／デバイスはまずリスク分析を完了して、リスクが高すぎる状況であると判断されたら、パスワード変更を拒否するようにしてもよい。リスク分析の後にはログインを許可する追加の認証ステップ（これはパスワードと独立していてもよい）が行われてもよく、したがって、そのときにパスワードを変更させることができる。

【０２３７】

本発明は構造的特徴および／または方法論的作動に特定的な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作動に制限されないことが理解されよう。むしろ、前記の特定の特徴または作動は、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。

【０２３８】

関連事案のクロスリファレンス：本出願は、２０１４年６月２７日に出願され、「Ｅｎｔｅｒｐｒｉｓｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｖｉａ　Ｔｈｉｒｄ　Ｐａｒｔｙ

Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｓｕｐｐｏｒｔ」と題する米国出願第１４／３１７，７９５号の優先権を主張する。

【図１】

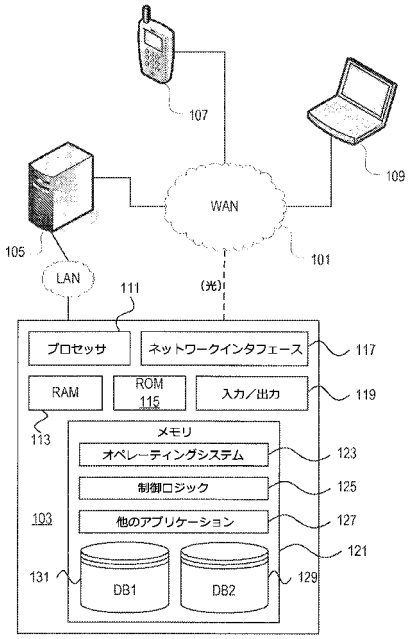


図１

【図２】

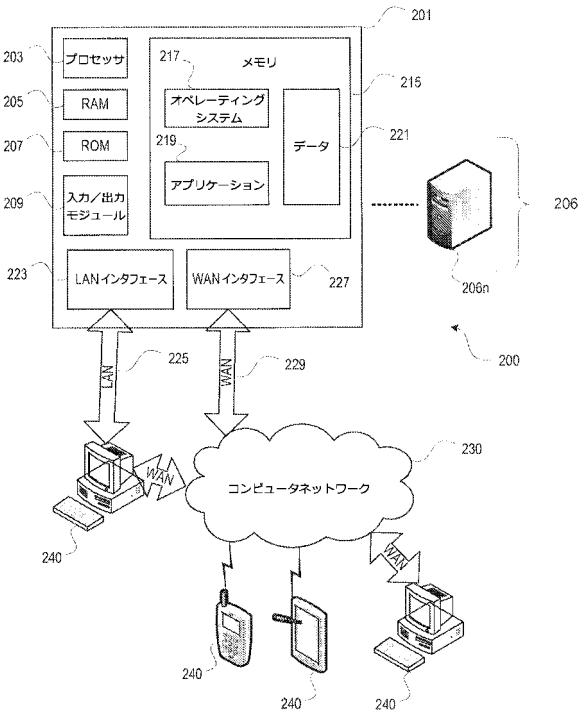
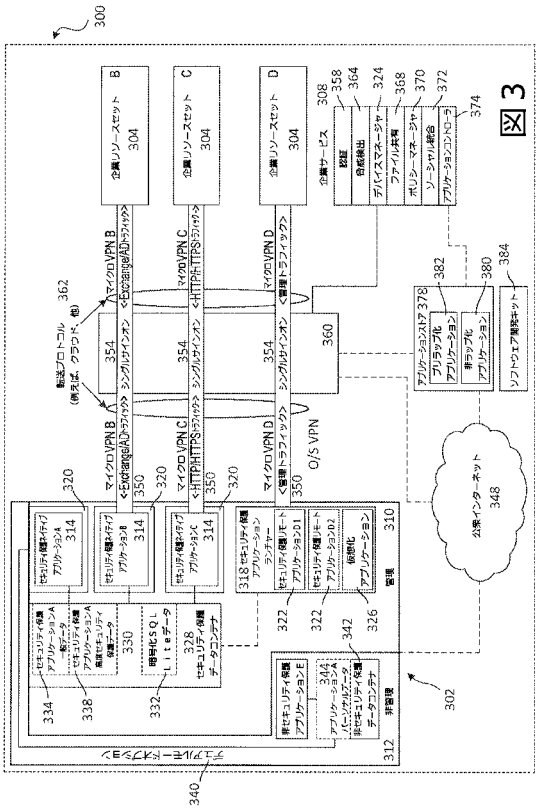
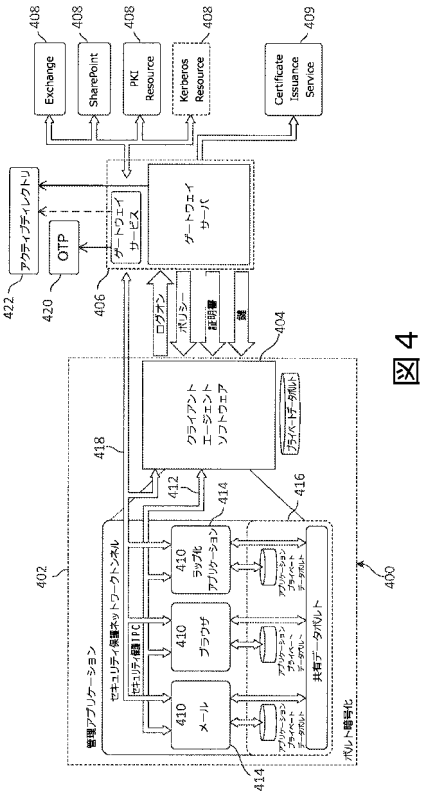


図２

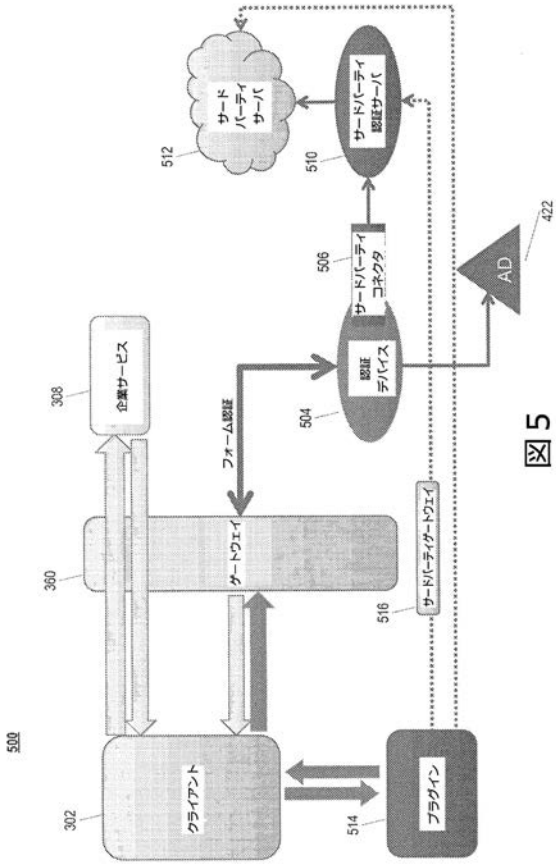
【図３】



【図４】



【図５】



【図６】

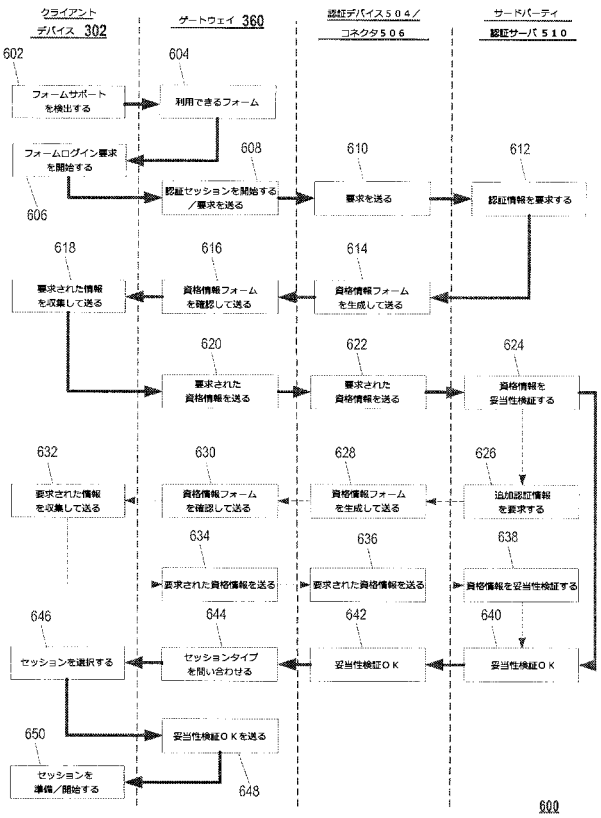

クライアント
デバイス 302
ゲートウェイ 360
認証デバイス504／
コネクタ506
サードパーティ
認証サーバ510
フォームサポート
を検出する
利用できるフォーム
フォームログイン要求
を開始する
認証セッションを開始する
／要求を送る
要求を送る
認証情報を要求する
要求された情報
を収集して送る
資格情報フォーム
を確認して送る
資格情報フォーム
を生成して送る
要求された
資格情報を送る
資格情報を
妥当性検証する
追加認証情報
を要求する
セッションを選択する
セッションタイプ
を問い合わせる
妥当性検証ＯＫ
セッションを
準備／開始する
600

図６

【図７】

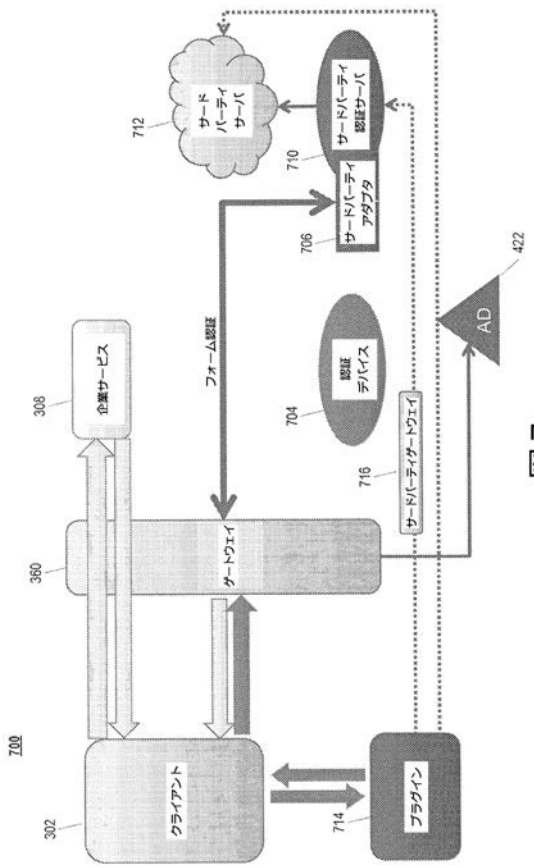


図７

【図８】

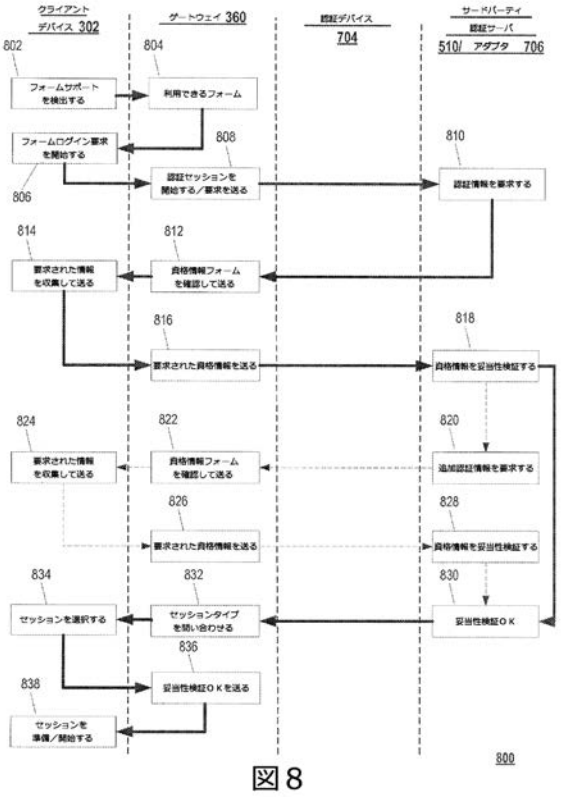


図８

【図９】

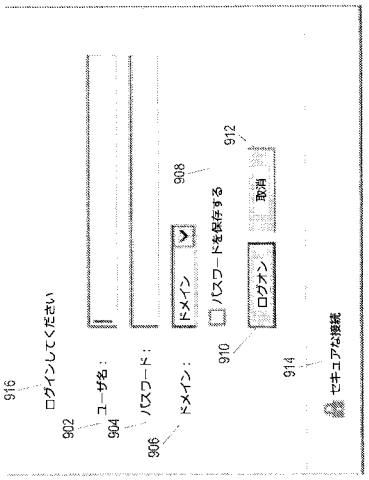


図９

【図１０】

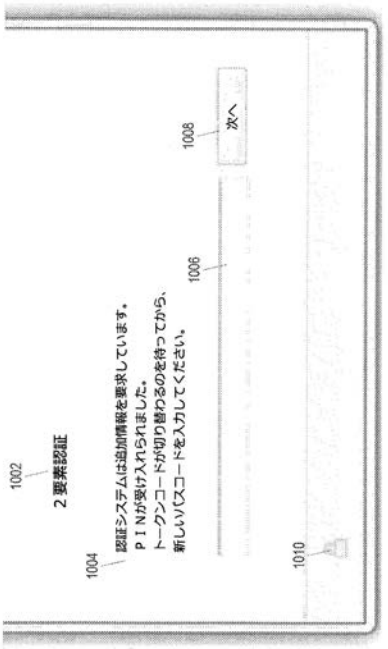


図10

【図１１】

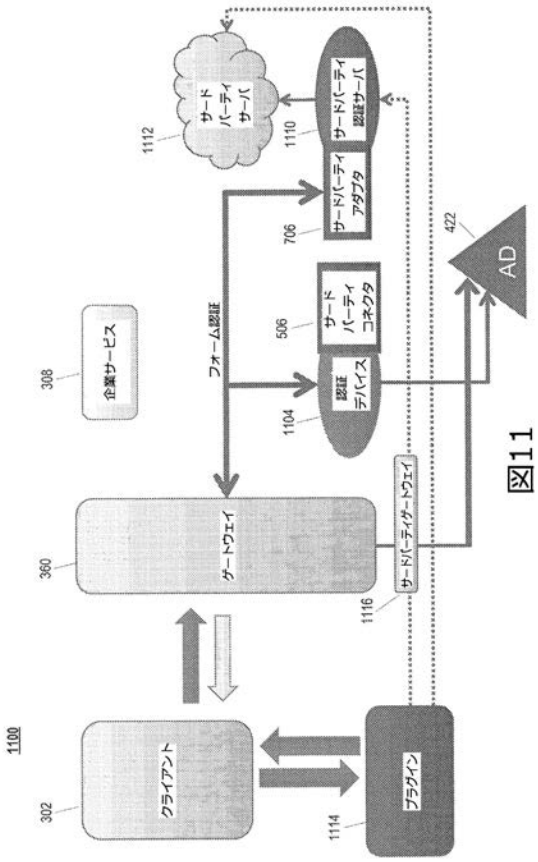

1100
クライアント
302
プラグイン
1114
ゲートウェイ
360
サードパーティゲートウェイ
1116
企業サービス
308
フォーム認証
認証デバイス
1104
サードパーティコネクタ
506
サードパーティアダプタ
706
サードパーティ認証サーバ
1110
サードパーティサーバ
1112
AD
422

図11

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2014/048229

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04W12/06 H04L9/32 H04L29/06
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04W H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2011/023456 A2 (IBM [US]; IBM FRANCE [FR]; GARGARO GIANLUCA [IT]; TRINCHINI PATRIZIO [) 3 March 2011 (2011-03-03) page 6, lines 11-16 page 9, line 11 - page 10, line 14 figures 1,7	1-20
X	US 2014/082715 A1 (GRAJEK GARRET FLORIAN [US] ET AL) 20 March 2014 (2014-03-20) paragraphs [0026], [0042], [0045], [0048], [0054], [0060] figures 1,2	1-20
A	US 2008/134311 A1 (MEDVINSKY GENNADY [US] ET AL) 5 June 2008 (2008-06-05) paragraphs [0018], [0063], [0064] figure 3	1-20

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
25 February 2015	05/03/2015

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Pajatakis, Emmanouil

1

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2014/048229

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2011023456 A2	03-03-2011	US 2012167193 A1	28-06-2012
		US 2013074172 A1	21-03-2013
		US 2014304793 A1	09-10-2014
		US 2014304794 A1	09-10-2014
		WO 2011023456 A2	03-03-2011
US 2014082715 A1	20-03-2014	US 2014082715 A1	20-03-2014
		US 2015007299 A1	01-01-2015
		WO 2014046880 A1	27-03-2014
US 2008134311 A1	05-06-2008	CN 101542965 A	23-09-2009
		EP 2098006 A2	09-09-2009
		JP 5334320 B2	06-11-2013
		JP 5599910 B2	01-10-2014
		JP 2010512069 A	15-04-2010
		JP 2013138474 A	11-07-2013
		KR 20090095630 A	09-09-2009
		TW 200833060 A	01-08-2008
		US 2008134311 A1	05-06-2008
		WO 2008127447 A2	23-10-2008

フロントページの続き

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

(72)発明者 メイヤーズ，クリス
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
(72)発明者 ソニ，アジャイ
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

【要約の続き】
【選択図】図６