

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第6957764号
(P6957764)

(45) 発行日 令和3年11月2日 (2021.11.2)

(24) 登録日 令和3年10月8日 (2021.10.8)

(51) Int. Cl. F I
G O 6 F 21/34 (2013.01) G O 6 F 21/34
G O 6 F 21/60 (2013.01) G O 6 F 21/60 3 2 0

請求項の数 20 (全 67 頁)

(21) 出願番号	特願2020-542836 (P2020-542836)	(73) 特許権者	397074301
(86) (22) 出願日	平成31年1月24日 (2019.1.24)		サイトリックス システムズ, インコーポ レイテッド
(65) 公表番号	特表2021-513164 (P2021-513164A)		アメリカ合衆国 フロリダ 33309, フォート ローダーデール, ウェスト サイプレス クリーク ロード 851
(43) 公表日	令和3年5月20日 (2021.5.20)		
(86) 国際出願番号	PCT/US2019/014954	(74) 代理人	110002310
(87) 国際公開番号	W02019/156822		特許業務法人あい特許事務所
(87) 国際公開日	令和1年8月15日 (2019.8.15)	(72) 発明者	ディヴー, ユベール
審査請求日	令和2年10月2日 (2020.10.2)		アメリカ合衆国, フロリダ州 33309 , フォート ローダーデール, ウェスト 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
(31) 優先権主張番号	62/627,790		
(32) 優先日	平成30年2月8日 (2018.2.8)		
(33) 優先権主張国・地域又は機関	米国 (US)		
(31) 優先権主張番号	16/111,328		
(32) 優先日	平成30年8月24日 (2018.8.24)		
(33) 優先権主張国・地域又は機関	米国 (US)		

最終頁に続く

(54) 【発明の名称】 高速スマートカードログオン

(57) 【特許請求の範囲】

【請求項 1】

サーバとクライアントデバイスとの間にリモートチャネルを確立することと、
 前記サーバによって、前記クライアントデバイスから、パーソナルコンピュータ／スマ
 ートカード（PC／SC）プロトコルを介して、前記クライアントデバイスに関連付けら
 れたスマートカードの識別子を含むメッセージを受信することと、

前記サーバによって、前記識別子を前記スマートカードの代替識別子に置き換えること
 と、

前記代替識別子に基づいて、前記サーバによって、前記スマートカードに関連する 1 つ
 または複数の暗号動作に使用する暗号サービスプロバイダを決定することと、

前記決定された暗号サービスプロバイダを介して、前記リモートチャネルを介し
 て、前記クライアントデバイスに、前記スマートカードを必要とする暗号動作の 1 つまた
 は複数の要求を送信することと、

を含む、方法。

【請求項 2】

前記識別子はリセット応答（ATR）データを含み、前記代替識別子は代替 ATR デー
 タを含む、請求項 1 に記載の方法。

【請求項 3】

前記暗号サービスプロバイダを決定することは、前記代替識別子と、前記スマートカー
 ドを用いた 1 つまたは複数の暗号動作に使用する前記暗号サービスプロバイダとの間の関

10

20

連付けについてデータベースに照会することを含む、請求項 1 に記載の方法。

【請求項 4】

前記データベースはレジストリを含む、請求項 3 に記載の方法。

【請求項 5】

前記代替識別子を生成することと、

前記スマートカードを用いた 1 つまたは複数の暗号動作に使用する前記暗号サービスプロバイダに関連付けて前記代替識別子を前記データベースに記憶することと、
をさらに含む、請求項 3 に記載の方法。

【請求項 6】

前記スマートカードを用いた 1 つまたは複数の暗号動作に使用する前記暗号サービスプロバイダに関連付けて前記代替識別子を記憶することは、前記スマートカードを用いた 1 つまたは複数の暗号動作に使用する前記暗号サービスプロバイダを識別する情報と同じファイルに前記代替識別子を記憶することを含む、請求項 5 に記載の方法。

10

【請求項 7】

前記スマートカードの前記識別子は、前記スマートカードのスマートカードタイプを識別する、請求項 1 に記載の方法。

【請求項 8】

プロセッサと、

コンピュータ実行可能命令を記憶するメモリと、

を備える装置であって、前記コンピュータ実行可能命令は、前記プロセッサによって実行された場合に、前記装置に、

20

前記装置とクライアントデバイスとの間にリモートリングチャネルを確立することと、

前記クライアントデバイスから、パーソナルコンピュータ／スマートカード（P C／S C）プロトコルを介して、前記クライアントデバイスに関連付けられたスマートカードの識別子を含むメッセージを受信することと、

前記識別子を前記スマートカードの代替識別子に置き換えることと、

前記代替識別子に基づいて、前記スマートカードに関連する 1 つまたは複数の暗号動作に使用する暗号サービスプロバイダを決定することと、

前記決定された暗号サービスプロバイダを介して、前記リモートリングチャネルを介して、前記クライアントデバイスに、前記スマートカードを必要とする暗号動作の 1 つまたは複数の要求を送信することと、
を行わせる、前記装置。

30

【請求項 9】

前記識別子はリセット応答（A T R）データを含み、前記代替識別子は代替 A T R データを含む、請求項 8 に記載の装置。

【請求項 10】

前記暗号サービスプロバイダを決定することは、前記代替識別子と、前記スマートカードを用いた 1 つまたは複数の暗号動作に使用する前記暗号サービスプロバイダとの間の関連付けについてデータベースに照会することを含む、請求項 8 に記載の装置。

【請求項 11】

40

前記データベースはレジストリを含む、請求項 10 に記載の装置。

【請求項 12】

前記メモリは、コンピュータ実行可能命令を記憶し、前記コンピュータ実行可能命令は、前記プロセッサによって実行された場合に、前記装置に、

前記代替識別子を生成することと、

前記スマートカードを用いた 1 つまたは複数の暗号動作に使用する前記暗号サービスプロバイダに関連付けて前記代替識別子を前記データベースに記憶することと、
を行わせる、請求項 10 に記載の装置。

【請求項 13】

前記スマートカードを用いた 1 つまたは複数の暗号動作に使用する前記暗号サービスプロ

50

ロバイダに関連付けて前記代替識別子を記憶することは、前記スマートカードを用いた1つまたは複数の暗号動作に使用する前記暗号サービスプロバイダを識別する情報と同じファイルに前記代替識別子を記憶することを含む、請求項12に記載の装置。

【請求項14】

前記スマートカードの前記識別子は、前記スマートカードのスマートカードタイプを識別する、請求項8に記載の装置。

【請求項15】

コンピュータ可読命令を記憶する1つまたは複数の非一時的コンピュータ可読媒体であって、前記コンピュータ可読命令は、コンピューティングデバイスによって読み取られた場合に、前記コンピューティングデバイスに、

10

前記コンピューティングデバイスとクライアントデバイスとの間にリモートリングチャネルを確立することと、

前記クライアントデバイスから、パーソナルコンピュータ／スマートカード（PC／SC）プロトコルを介して、前記クライアントデバイスに関連付けられたスマートカードの識別子を含むメッセージを受信することと、

前記識別子を前記スマートカードの代替識別子に置き換えることと、

前記代替識別子に基づいて、前記スマートカードに関連する1つまたは複数の暗号動作に使用する暗号サービスプロバイダを決定することと、

前記決定された暗号サービスプロバイダを介して、前記リモートリングチャネルを介して、前記クライアントデバイスに、前記スマートカードを必要とする暗号動作の1つまたは複数の要求を送信することと、

20

を行わせる、前記1つまたは複数の非一時的コンピュータ可読媒体。

【請求項16】

前記識別子はリセット応答（ATR）データを含み、前記代替識別子は代替ATRデータを含む、請求項15に記載の1つまたは複数の非一時的コンピュータ可読媒体。

【請求項17】

前記暗号サービスプロバイダを決定することは、前記代替識別子と、前記スマートカードを用いた1つまたは複数の暗号動作に使用する前記暗号サービスプロバイダとの間の関連付けについてデータベースに照会することを含む、請求項15に記載の1つまたは複数の非一時的コンピュータ可読媒体。

30

【請求項18】

前記データベースはレジストリを含む、請求項17に記載の1つまたは複数の非一時的コンピュータ可読媒体。

【請求項19】

コンピュータ可読命令を記憶し、前記コンピュータ可読命令は、前記コンピューティングデバイスによって読み取られた場合に、前記コンピューティングデバイスに、

前記代替識別子を生成することと、

前記スマートカードを用いた1つまたは複数の暗号動作に使用する前記暗号サービスプロバイダに関連付けて前記代替識別子を前記データベースに記憶することと、

を行わせる、請求項17に記載の1つまたは複数の非一時的コンピュータ可読媒体。

40

【請求項20】

前記スマートカードを用いた1つまたは複数の暗号動作に使用する前記暗号サービスプロバイダに関連付けて前記代替識別子を記憶することは、前記スマートカードを用いた1つまたは複数の暗号動作に使用する前記暗号サービスプロバイダを識別する情報と同じファイルに前記代替識別子を記憶することを含む、請求項19に記載の1つまたは複数の非一時的コンピュータ可読媒体。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は概して、スマートカードを使用してリモートコンピューティング環境にクライ

50

アントをログオンさせることに関する。

【背景技術】

【0002】

従来、スマートカード認証は、サーバ（認証）デバイスとクライアントデバイスとの間の多数のインタラク션을必要とする。リモートコンピューティング環境では、その多数のインタラク션は、サーバとクライアントとの間の接続におけるレイテンシの増加によって、大幅に遅くなる。

【発明の概要】

【0003】

以下に、本明細書に記載の様々な態様の簡略化した概要を提示する。本概要は広範な概観ではなく、主要なもしくは重要な要素を特定することも、特許請求の範囲を線引きすることも意図していない。以下の概要は、以下に提供するより詳細な説明への導入的な前置きとして、一部の概念を簡略化した形で提示するものにすぎない。

【0004】

上述した従来技術の限界を克服し、本明細書を読解すると明らかになる他の限界を克服するために、本明細書に記載の態様は、たとえばスマートカードを用いた、より高速かつより効率的なログオンのための方法及びシステムを対象とする。

【0005】

高速スマートカードログオンを使用して、レイテンシを短縮し、セキュリティを向上させ得る。たとえば、システムは、認証に使用されるサーバデバイスとクライアントデバイスとの間の動作（たとえば、インタラク션）の回数を削減し得る。これらの動作は、スマートカードからユーザ証明書をフェッチすること、またはデータに署名することを含んでもよい。高速スマートカードログオンはまた、任意選択でネットワークを介したPIN（または他の資格情報）の伝送を回避し、PINキャッシングに頼ることのない、実際のリモートコンピューティング環境へのログオンにスマートカードを使用した、認証イベント（たとえば、セキュアソケットレイヤ（SSL）またはトランスポートレイヤセキュリティ（TLS）認証）からのシングルサインオンを可能にすることにより、セキュリティを向上させ得る。

【0006】

高速スマートカードログオンを実装するために使用されるコンポーネントはまた、フェデレーテッドフルドメインログオンを実装するために使用されてもよい。外部認証イベントの受諾に基づいて、仮想スマートカード資格情報が発行されてもよく、これは一時的なものでもよい。例示的な外部認証イベントには、セキュリティアサーションマークアップ言語（SAML）アイデンティティプロバイダにおけるログオンと、TLSまたはSSLを介したスマートカード認証と、ADパスワードを使用しないバイオメトリクスまたはワンタイムパスワード（OTP）などの代替的な認証資格情報と、が含まれる。また、高速スマートカードログオンからの証明書動作インターセプトコンポーネントを使用して、PC/SCのAPIレベルでスマートカードを完全にエミュレートすることなく、仮想スマートカードとのインタラク션을可能にし得る。仮想スマートカードは、リモートコンピューティング環境上でローカルに、または高度に保護され得る別のサーバ上で作成されてもよい。

【0007】

本明細書に記載の態様は、より高速なスマートカードログオンのためのシステム、装置、コンピュータ可読媒体、メモリ、及び方法を対象とする。方法は、サーバとクライアントデバイスとの間にリモーティングチャネルを確立することを含んでもよい。サーバは、クライアントデバイスから、及び／またはパーソナルコンピュータ／スマートカード（PC/SC）プロトコルを介して、クライアントデバイスに関連付けられたスマートカードの識別子を含むメッセージを受信してもよい。サーバは、識別子をスマートカードの代替識別子に置き換えてもよい。代替識別子に基づいて、サーバは、スマートカードに関連する1つまたは複数の暗号動作に使用する暗号サービスプロバイダを決定してもよい。この

10

20

30

40

50

方法は、決定された暗号サービスプロバイダを介して、リモートチャネルを介して、及び／またはクライアントデバイスに、スマートカードを必要とする暗号動作の1つまたは複数の要求を送信することを含んでもよい。

【0008】

一部の例では、識別子はリセット応答（ATR）データを含んでもよく、代替識別子は代替ATRデータを含んでもよい。追加的または代替的には、スマートカードの識別子は、スマートカードのスマートカードタイプを識別してもよい。

【0009】

一部の例では、暗号サービスプロバイダを決定することは、代替識別子と、スマートカードを用いた1つまたは複数の暗号動作に使用する暗号サービスプロバイダとの間の関連付けについてデータベースに照会することを含んでもよい。一部のシナリオでは、データベースはレジストリを含んでもよい。この方法は、代替識別子を生成すること、及び／または、スマートカードを用いた1つまたは複数の暗号動作に使用する暗号サービスプロバイダに関連付けて代替識別子をデータベースに記憶すること、を含んでもよい。一部の例では、スマートカードを用いた1つまたは複数の暗号動作に使用する暗号サービスプロバイダに関連付けて代替識別子を記憶することは、スマートカードを用いた1つまたは複数の暗号動作に使用する暗号サービスプロバイダを識別する情報と同じファイルに代替識別子を記憶することを含んでもよい。

【0010】

これら及び追加の態様は、以下でさらに詳細に説明する本開示の恩恵を受けて理解されよう。

【0011】

添付図面を考慮して以下の説明を参照することによって、本明細書に記載の態様及びそれらの利点のより完全な理解が得られ、添付図面では、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】本明細書に記載の1つまたは複数の態様に従って使用され得る例示的なコンピュータシステムのアーキテクチャを示す図である。

【図2】本明細書に記載の1つまたは複数の態様に従って使用され得る例示的なリモートアクセスシステムのアーキテクチャを示す図である。

【図3】本明細書に記載の1つまたは複数の態様に従って使用され得る例示的な仮想化（ハイパーバイザ）システムのアーキテクチャを示す図である。

【図4】本明細書に記載の1つまたは複数の態様に従って使用され得る例示的なクラウドベースのシステムのアーキテクチャを示す図である。

【図5】例示的な企業モビリティ管理システムを示す図である。

【図6】他の例示的な企業モビリティ管理システムを示す図である。

【図7】本明細書に記載の1つまたは複数の態様によるスマートカードログオンのための例示的なシステムを示す図である。

【図8】本明細書に記載の1つまたは複数の態様による高速スマートカードログオンのための例示的なシステムを示す図である。

【図9】本明細書に記載の1つまたは複数の態様による高速スマートカードログオンのための他の例示的なシステムを示す図である。

【図10】本明細書に記載の1つまたは複数の態様による高速スマートカードログオンのためのさらに他の例示的なシステムを示す図である。

【図11】本明細書に記載の1つまたは複数の態様によるフェデレーテッドログオンのための例示的なシステムを示す図である。

【図12A】本明細書に記載の1つまたは複数の態様によるフェデレーテッドログオンのための他の例示的なシステムを示す図である。

【図12B】本明細書に記載の1つまたは複数の態様によるフェデレーテッドログオンの

10

20

30

40

50

ためのさらに他の例示的なシステムを示す図である。

【図 1 2 C】本明細書に記載の 1 つまたは複数の態様によるフェデレーテッドログオンのための他の例示的なシステムを示す図である。

【図 1 3】本明細書に記載の 1 つまたは複数の態様によるアプリケーションストア、資格情報マッパー、及び仮想化エージェントの間の例示的なインタラクションを示す図である。

【図 1 4】本明細書に記載の 1 つまたは複数の態様によるフェデレーテッドログオンのためのさらに他の例示的なシステムを示す図である。

【図 1 5】本明細書に記載の 1 つまたは複数の態様による資格情報マッピングサービスを提供するための例示的なシステムを示す図である。

10

【図 1 6 A】本明細書に記載の 1 つまたは複数の態様による例示的なスマートカードのデータベースを示す図である。

【図 1 6 B】本明細書に記載の 1 つまたは複数の態様による例示的なスマートカードのデータベースを示す図である。

【図 1 7】本明細書に記載の 1 つまたは複数の態様による例示的なユーザインターフェースを示す図である。

【発明を実施するための形態】

【0 0 1 3】

様々な実施形態の以下の説明では、上記で明らかにした、本明細書の一部を形成する添付図面を参照し、添付図面では、本明細書に記載の態様が実施され得る様々な実施形態を例として示している。本明細書に記載の範囲から逸脱することなく、他の実施形態が利用されてもよく、構造的及び機能的な変更が加えられてもよいことは理解されたい。様々な態様は他の実施形態が可能であり、様々な異なる方法で実施または実行することが可能である。

20

【0 0 1 4】

以下でより詳細に説明する主題の概略的な紹介として、本明細書に記載の態様は、より高速なスマートカードログオンのためのシステム、装置、コンピュータ可読媒体、メモリ、及び方法を対象とする。サーバとクライアントデバイスとの間にリモートチャネルが確立されてもよい。サーバは、クライアントデバイスから、及び／またはパーソナルコンピュータ／スマートカード（PC／SC）プロトコルを介して、クライアントデバイスに関連付けられたスマートカードの識別子を含むメッセージを受信してもよい。サーバは、スマートカードの識別子を代替識別子に置き換えてもよい。代替識別子に基づいて、サーバは、スマートカードに関連する 1 つまたは複数の暗号動作に使用する暗号サービスプロバイダを決定してもよい。一部の態様では、たとえば、決定された暗号サービスプロバイダを介して、及び／またはリモートチャネルを介して、クライアントデバイスに、スマートカードを必要とする暗号動作の 1 つまたは複数の要求が送信されてもよい。

30

【0 0 1 5】

本明細書で使用する表現及び用語は、説明を目的としたものであり、限定するものと見なされるべきでないことは理解されたい。むしろ、本明細書で使用する表現及び用語には、それらの最も広い解釈及び意味が与えられるべきである。「含む（including）」及び「備える（comprising）」ならびにそれらの変形の使用は、それらの後に列挙した項目及びそれらの均等物、ならびに追加の項目及びそれらの均等物を包含するものとする。「取り付けられた」、「接続された」、「結合される」、「位置付けられた」、「係合された」という用語及び同様の用語の使用は、直接及び間接両方の取り付け、接続、結合、位置付け、及び係合を含むものとする。

40

【0 0 1 6】

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、ハードウェア及びネットワークは、とりわけ、スタンドアロン環境、ネットワーク化環境、リモートアクセス（リモートデスクトップとしても知られている）環境、仮想化環境、及び／またはクラウドベースの環境を含む、多様な異なる

50

システム環境で利用され得る。図1に、スタンドアロン環境及び／またはネットワーク化環境において本明細書に記載の1つまたは複数の例示的な態様を実装するために使用され得るシステムアーキテクチャ及びデータ処理デバイスの一例を示す。様々なネットワークノード103、105、107、及び109が、インターネットなど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もよい。プライベートイントラネット、企業ネットワーク、ローカルエリアネットワーク(LAN)、メトロポリタンエリアネットワーク(MAN)、無線ネットワーク、パーソナルネットワーク(PAN)などを含む他のネットワークが追加的にまたは代替的に使用されてもよい。ネットワーク101は例示を目的としたものであり、より少数のまたは追加のコンピュータネットワークに置き換えられてもよい。ローカルエリアネットワーク133はあらゆる知られているLANトポロジのうちの1つまたは複数を有してもよく、Ethernetなどの多様な異なるプロトコルのうちの1つまたは複数を使用してもよい。デバイス103、105、107、及び109ならびに他のデバイス(図示せず)は、ツイストペア線、同軸ケーブル、光ファイバ、電波、または他の通信媒体を介してネットワークのうちの1つまたは複数に接続されてもよい。

10

【0017】

本明細書で使用し、図面に示す「ネットワーク」という用語は、リモートストレージデバイスが1つまたは複数の通信経路を介して相互に結合されるシステムを指すだけでなく、記憶機能を有するそのようなシステムに、その時々に関与するスタンドアロンデバイスも指す。結果的に、「ネットワーク」という用語は、「物理ネットワーク」だけでなく、全ての物理ネットワークにわたって存在する、単一のエンティティに帰属する、データから構成される「コンテンツネットワーク」も含む。

20

【0018】

コンポーネントは、データサーバ103、ウェブサーバ105、及びクライアントコンピュータ107、109を含んでもよい。データサーバ103は、本明細書に記載の1つまたは複数の例示的な態様を実施するためのデータベース及び制御ソフトウェアの全体的なアクセス、制御、及び管理を提供する。データサーバ103はウェブサーバ105に接続されてもよく、それを介してユーザはインタラクトし、要求通りにデータを取得する。代替的には、データサーバ103は、ウェブサーバ自体として機能し、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、ローカルエリアネットワーク133、ワイドエリアネットワーク101(たとえば、インターネット)経由で、直接もしくは間接的な接続を介して、または他の何らかのネットワークを介して、ウェブサーバ105に接続されてもよい。ユーザはリモートコンピュータ107、109を使用して、たとえばウェブブラウザを使用して、ウェブサーバ105によってホストされる1つまたは複数の外部に公開されたウェブサイトを介してデータサーバ103に接続することによって、データサーバ103とインタラクトしてもよい。クライアントコンピュータ107、109をデータサーバ103と協働させて使用して、そこに記憶されたデータにアクセスしてもよく、または他の目的で使用してもよい。たとえば、クライアントデバイス107から、ユーザは当技術分野で知られている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(インターネットなど)を介してウェブサーバ105及び／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、ウェブサーバ105にアクセスしてもよい。

30

40

【0019】

サーバ及びアプリケーションは、同じ物理マシン上で組み合わせられ、別々の仮想アドレスもしくは論理アドレスを保持してもよく、または別々の物理マシンに存在してもよい。図1は、使用され得るネットワークアーキテクチャのほんの一例を示しており、当業者は、使用される特定のネットワークアーキテクチャ及びデータ処理デバイスが変更されてもよく、本明細書でさらに説明するように、それらが提供する機能に対して二次的なものであることを理解するであろう。たとえば、ウェブサーバ105及びデータサーバ103によって提供されるサービスは単一のサーバ上で組み合わせられてもよい。

50

【0020】

各コンポーネント103、105、107、109は、任意のタイプの知られているコンピュータ、サーバ、またはデータ処理デバイスであってもよい。データサーバ103は、たとえば、データサーバ103の動作全体を制御するプロセッサ111を含んでもよい。データサーバ103は、ランダムアクセスメモリ(RAM)113、読み取り専用メモリ(ROM)115、ネットワークインターフェース117、入力/出力インターフェース119(たとえば、キーボード、マウス、ディスプレイ、プリンタなど)、及びメモリ121をさらに含んでもよい。入力/出力(I/O)119は、データまたはファイルの読み込み、書き込み、表示、及び/または印刷のための多様なインターフェースユニット及びドライブを含んでもよい。メモリ121は、データ処理デバイス103の動作全体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と、本明細書に記載の態様を実施するようにデータサーバ103に指示するための制御ロジック125と、本明細書に記載の態様と共に使用してもよく、使用しない場合もある二次的な機能、サポート機能、及び/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と、をさらに記憶してもよい。制御ロジック125は、本明細書ではデータサーバソフトウェア125と呼ぶこともある。データサーバソフトウェア125の機能は、制御ロジック125内にコード化されたルールに基づいて自動的に行われる動作もしくは判定、ユーザがシステムに入力を提供することによって手動で行われる動作もしくは判定、及び/またはユーザ入力に基づく自動処理(たとえば、クエリ、データ更新など)の組み合わせを指す場合がある。

10

20

【0021】

メモリ121は、第1のデータベース129及び第2のデータベース131を含む、本明細書に記載の1つまたは複数の態様を実施する際に使用されるデータも記憶してもよい。一部の実施形態では、第1のデータベース129は、第2のデータベース131を(たとえば、別個のテーブル、レポートなどとして)含んでもよい。すなわち、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するか、または異なる論理データベース、仮想データベース、もしくは物理データベースに分けることができる。デバイス105、107、及び109は、デバイス103に関して説明し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。本明細書に記載のデータ処理デバイス103(またはデバイス105、107、もしくは109)の機能を複数のデータ処理デバイスに拡散させて、たとえば、複数のコンピュータに処理負荷を分散させて、地理的な場所、ユーザアクセスレベル、サービス品質(QoS)などに基づいてトランザクションを分別してもよいことを当業者は理解するであろう。

30

【0022】

1つまたは複数の態様は、本明細書に記載の1つまたは複数のコンピュータまたは他のデバイスによって実行される1つまたは複数のプログラムモジュールなどの中の、コンピュータ使用可能もしくは読取可能データ及び/またはコンピュータ実行可能命令で具現化されてもよい。一般に、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内のプロセッサによって実行された場合に、特定のタスクを実施するかまたは特定の抽象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、データ構造などを含む。モジュールは、実行のために後でコンパイルされるソースコードプログラミング言語で記述されてもよく、またはハイパーテキストマークアップ言語(HTML)もしくは拡張可能マークアップ言語(XML)などの(ただし、これらに限定されない)スクリプト言語で記述されてもよい。コンピュータ実行可能命令は、不揮発性ストレージデバイスなどのコンピュータ可読媒体に記憶されてもよい。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、及び/またはそ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可読記憶媒体が利用されてもよい。加えて、本明細書に記載のデータまたはイベントを表す様々な伝送(非記憶)媒体は、金属線、光ファイバ、及び/または無線伝送媒体(たとえば、空気及び/または空間)などの信号伝導媒体の中を進む電磁波の形で、ソースと宛先との間で転送されてもよい。本明細書に記載の様

40

50

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現化されてもよい。そのため、様々な機能は、ソフトウェア、ファームウェア、及び／またはハードウェアもしくはハードウェア均等物、たとえば、集積回路、フィールドプログラマブルゲートアレイ（FPGA）などで、全体的にまたは部分的に具現化されてもよい。本明細書に記載の1つまたは複数の態様をより効果的に実装するために特定のデータ構造が使用されてもよく、そのようなデータ構造は、本明細書に記載のコンピュータ実行可能命令及びコンピュータ使用可能データの範囲内で企図される。

【0023】

図2をさらに参照すると、本明細書に記載の1つまたは複数の態様はリモートアクセス環境に実装されてもよい。図2に、本明細書に記載の1つまたは複数の例示的な態様に従って使用され得る例示的なコンピューティング環境200におけるコンピューティングデバイス201を含む例示的なシステムアーキテクチャを示す。コンピューティングデバイス201は、単一サーバまたはマルチサーバのデスクトップ仮想化システム（たとえば、リモートアクセスまたはクラウドシステム）内のサーバ206aとして使用されてもよく、クライアントアクセスデバイスに仮想マシンを提供するように構成することができる。コンピューティングデバイス201は、デバイス201の動作全体を制御するプロセッサ203と、それに関連するコンポーネント、たとえば、RAM205、ROM207、入力／出力（I/O）モジュール209、及びメモリ215と、を有してもよい。

【0024】

I/Oモジュール209は、コンピューティングデバイス201のユーザがそれを介して入力を提供し得るマウス、キーパッド、タッチスクリーン、スキャナ、光学リーダ、及び／またはスタイラス（もしくは他の入力デバイス（複数可））を含んでもよく、また、音声出力を提供するためのスピーカのうち1つまたは複数と、テキスト、オーディオビジュアル、及び／またはグラフィカル出力を提供するためのビデオディスプレイデバイスのうちの1つまたは複数と、を含んでもよい。ソフトウェアは、本明細書に記載の様々な機能を実施するために、コンピューティングデバイス201を専用コンピューティングデバイスに構成するための命令をプロセッサ203に提供するように、メモリ215及び／または他のストレージ内に記憶されてもよい。たとえば、メモリ215は、コンピューティングデバイス201によって使用されるソフトウェア、たとえば、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、及び関連するデータベース221を記憶してもよい。

【0025】

コンピューティングデバイス201は、端末240（クライアントデバイスとも呼ばれる）などの1つまたは複数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化環境で動作してもよい。端末240は、コンピューティングデバイス103または201に関して上述した要素の多くまたは全てを含む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、またはサーバであってもよい。図2に示すネットワーク接続は、ローカルエリアネットワーク（LAN）225及びワイドエリアネットワーク（WAN）229を含むが、他のネットワークをさらに含んでもよい。LANネットワーク環境で使用される場合、コンピューティングデバイス201は、ネットワークインターフェースまたはアダプタ223を介してLAN225に接続されてもよい。WANネットワーク環境で使用される場合、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（たとえば、インターネット）などのWAN229を介して通信を確立するためのモデムまたは他のワイドエリアネットワークインターフェース227を含んでもよい。図示したネットワーク接続は例示的なものであり、コンピュータ間に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は理解されよう。コンピューティングデバイス201及び／または端末240はまた、バッテリー、スピーカ、及びアンテナ（図示せず）などの他の様々なコンポーネントを含むモバイル端末（たとえば、携帯電話、スマートフォン、携帯情報端末（PDA）、ノートブックなど）であってもよい。

10

20

30

40

50

【0026】

本明細書に記載の態様は、他の多くの汎用または専用コンピューティングシステム環境または構成でも動作可能であってもよい。本明細書に記載の態様での使用に適し得る他のコンピューティングシステム、環境、及び／または構成の例には、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のシステム、セットトップボックス、プログラム可能な家電製品、ネットワークパーソナルコンピュータ（PC）、ミニコンピュータ、メインフレームコンピュータ、上記のシステムまたはデバイスのいずれかを含む分散コンピューティング環境などが含まれるが、これらに限定されない。

【0027】

10

図2に示すように、1つまたは複数のクライアントデバイス240は、1つまたは複数のサーバ206a～206n（本明細書では総称して「サーバ（複数可）206」と呼ぶ）と通信可能であってもよい。一実施形態では、コンピューティング環境200は、サーバ（複数可）206とクライアントマシン（複数可）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もよい。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、一部のケースでは、複数のバックエンドサーバ206間でクライアント接続の負荷分散を行うことができる。

【0028】

クライアントマシン（複数可）240は、一部の実施形態では、単一クライアントマシン240または単一グループのクライアントマシン240と呼ぶ場合があり、サーバ（複数可）206は、単一サーバ206または単一グループのサーバ206と呼ぶ場合がある。一実施形態では、単一クライアントマシン240は2つ以上のサーバ206と通信し、他の実施形態では、単一サーバ206は2つ以上のクライアントマシン240と通信する。さらに他の実施形態では、単一クライアントマシン240は単一サーバ206と通信する。

20

【0029】

クライアントマシン240は、一部の実施形態では、次の非網羅的な用語、すなわち、クライアントマシン（複数可）、クライアント（複数可）、クライアントコンピュータ（複数可）、クライアントデバイス（複数可）、クライアントコンピューティングデバイス（複数可）、ローカルマシン、リモートマシン、クライアントノード（複数可）、エンドポイント（複数可）、またはエンドポイントノード（複数可）、のうちのいずれか1つによって言及する場合がある。サーバ206は、一部の実施形態では、次の非網羅的な用語、すなわち、サーバ（複数可）、ローカルマシン、リモートマシン、サーバファーム（複数可）、またはホストコンピューティングデバイス（複数可）、のうちのいずれか1つによって言及する場合がある。

30

【0030】

一実施形態では、クライアントマシン240は仮想マシンであってもよい。仮想マシンは任意の仮想マシンであってもよく、一部の実施形態では、仮想マシンは、タイプ1またはタイプ2ハイパーバイザ、たとえば、Citrix Systems、IBM、VMwareによって開発されたハイパーバイザ、または他の任意のハイパーバイザによって管理される任意の仮想マシンであってもよい。一部の態様では、仮想マシンはハイパーバイザによって管理されてもよく、他の態様では、仮想マシンは、サーバ206上で実行されるハイパーバイザ、またはクライアント240上で実行されるハイパーバイザによって管理されてもよい。

40

【0031】

一部の実施形態は、サーバ206またはリモート配置された他のマシン上で、リモートで実行されるアプリケーションによって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を含む。これらの実施形態では、クライアントデバイス240は、仮想マシンの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出力を表示してもよい。一例では

50

、そのアプリケーションはデスクトップであり、他の例では、その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、ローカル及び／またはリモートアプリケーションを統合す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に対するユーザインター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。アプリケーションとは、本明細書で使用する場合、オペレーティングシステムのインスタンスが（及び任意選択でデスクトップも）ロードされた後に実行されるプログラムである。

【0032】

サーバ206は、一部の実施形態では、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トコルを使用して、シンククライアントまたはクライアント上で実行されるリモートディスプレイアプリケーションにデータを送信し、サーバ206上で実行されるアプリケーションによって生成されたディスプレイ出力を提示する。シンク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、次の非網羅的なプロトコルのリスト、すなわち、Citrix Systems, Inc., Ft. Lauderdale, Floridaによって開発されたインディペンデントコンピューティングアーキテクチャ（ICA）プロトコル、またはMicrosoft Corporation, Redmond, Washingtonによって作られたリモートデスクトッププロトコル（RDP）、のうちのいずれか1つとすることができる。

【0033】

リモートコンピューティング環境は、2つ以上のサーバ206a～206nを含むことによって、サーバ206a～206nが、たとえばクラウドコンピューティング環境におけるサーバファーム206に論理的にグループ化されるようにしてもよい。サーバファーム206は、論理的にグループ化されつつも地理的に分散しているサーバ206、または論理的にグループ化されつつも互いに近接して配置されたサーバ206を含んでもよい。サーバファーム206内の地理的に分散したサーバ206a～206nは、一部の実施形態では、WAN（ワイド）、MAN（メトロポリタン）、またはLAN（ローカル）を使用して通信することができ、異なる地理的地域は、異なる大陸、ある大陸の異なる地域、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な場所の任意の組み合わせとみなすことができる。一部の実施形態では、サーバファーム206は単一のエンティティとして管理されてもよく、他の実施形態では、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。

【0034】

一部の実施形態では、サーバファームは、実質的に同様のタイプのオペレーティングシステムプラットフォーム（たとえば、WINDOWS（登録商標）、UNIX（登録商標）、LINUX、iOS、ANDROID（登録商標）、SYMBIANなど）を実行するサーバ206を含んでもよい。他の実施形態では、サーバファーム206は、第1のタイプのオペレーティングシステムプラットフォームを実行する第1のグループの1つまたは複数のサーバと、第2のタイプのオペレーティングシステムプラットフォームを実行する第2のグループの1つまたは複数のサーバとを含んでもよい。

【0035】

サーバ206は、必要に応じて、任意のタイプのサーバとして、たとえば、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（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、もしくはマスターアプリケーションサーバ、アクティブディレクトリ（Active Directory）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、もしくは負荷分散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てもよい。他のサーバタイプも使用されてもよい。

【0036】

一部の実施形態は、第1のサーバ206aを含み、第1のサーバ206aは、クライアントマシン240から要求を受信し、要求を第2のサーバ206b（図示せず）に転送し、第2のサーバ206b（図示せず）からの応答を用いて、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はクライアントマシン240が利用可能なアプリケーションの一覧表に加え、アプリケーションの一覧表内で識別される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に関連するアドレス情報を取得してもよい。第1のサーバ206aは次いで、ウェブインター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、クライアント240と直接通信して、識別されたアプリケーションへのアクセスをクライアント240に提供することができる。1つまたは複数のクライアント240及び／または1つまたは複数のサーバ206は、ネットワーク230、たとえばネットワーク101上でデータを伝送してもよい。

10

【0037】

図3に、例示的な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。図示のように、デスクトップ仮想化システムは、1つまたは複数のクライアントアクセスデバイス240に仮想デスクトップ及び／または仮想アプリケーションを提供するように構成される少なくとも1つの仮想化サーバ301を含む、単一サーバもしくはマルチサーバシステム、またはクラウドシステムであってもよい。本明細書で使用する場合、デスクトップとは、1つまたは複数のアプリケーションがホスト及び／または実行されてもよいグラフィカル環境または空間を指す。デスクトップは、ローカル及び／またはリモートアプリケーションを統合す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に対するユーザインター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。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（及び任意選択でデスクトップも）がロードされた後に実行されるプログラムを含んでもよい。オペレーティングシステムの各インスタンスは、物理的なもの（たとえば、1デバイスにつき1つのオペレーティングシステム）であってもよく、仮想的なもの（たとえば、単一デバイス上で稼動するOSの多数のインスタンス）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、リモート配置されたデバイス上で実行（たとえば、リモートティング）されてもよい。

20

【0038】

コンピュータデバイス301は、仮想化環境における仮想化サーバとして、たとえば、単一サーバ、マルチサーバ、またはクラウドコンピューティング環境として構成されてもよい。図3に示す仮想化サーバ301は、図2に示すサーバ206の1つまたは複数の実施形態、あるいは他の知られているコンピューティングデバイスとしてデプロイすることができる。及び／またはそれらによって実装することができる。1つまたは複数の物理ディスク304、1つまたは複数の物理デバイス306、1つまたは複数の物理プロセッサ308、及び1つまたは複数の物理メモリ316を含むことができるハードウェアレイヤが、仮想化サーバ301に含まれる。一部の実施形態では、ファームウェア312を物理メモリ316のメモリ素子内に記憶することができ、物理プロセッサ308のうちの1つまたは複数によって実行することができる。仮想化サーバ301は物理メモリ316のメモリ素子内に記憶され、物理プロセッサ308のうちの1つまたは複数によって実行され得るオペレーティングシステム314をさらに含んでもよい。またさらに、ハイパーバイザ302を物理メモリ316のメモリ素子内に記憶してもよく、物理プロセッサ308のうちの1つまたは複数によって実行することができる。

30

40

【0039】

物理プロセッサ308のうちの1つまたは複数で実行されるのは、1つまたは複数の仮想マシン332A～C（総称して332）であってもよい。各仮想マシン332は仮想ディスク326A～C及び仮想プロセッサ328A～Cを有してもよい。一部の実施形態では、第1の仮想マシン332Aは、仮想プロセッサ328Aを使用して、ツールスタック324を含む制御プログラム320を実行してもよい。制御プログラム320は、制御仮想マシン、Dom0、ドメイン0、またはシステム管理及び／または制御に使用される他

50

の仮想マシンと呼ばれる場合がある。一部の実施形態では、1つまたは複数の仮想マシン332B～Cは、仮想プロセッサ328B～Cを使用して、ゲストオペレーティングシステム330A～Bを実行することができる。

【0040】

仮想化サーバ301は、仮想化サーバ301と通信する1つまたは複数のハードウェアを有するハードウェアレイヤ310を含んでもよい。一部の実施形態では、ハードウェアレイヤ310は、1つまたは複数の物理ディスク304、1つまたは複数の物理デバイス306、1つまたは複数の物理プロセッサ308、及び1つまたは複数の物理メモリ316を含むことができる。物理コンポーネント304、306、308、及び316は、たとえば、上述したコンポーネントのいずれを含んでもよい。物理デバイス306は、たとえば、ネットワークインターフェースカード、ビデオカード、キーボード、マウス、入力デバイス、モニタ、ディスプレイデバイス、スピーカー、光学ドライブ、ストレージデバイス、ユニバーサルシリアルバス接続、プリンタ、スキャナ、ネットワーク要素（たとえば、ルータ、ファイアウォール、ネットワークアドレス変換器、ロードバランサ、仮想プライベートネットワーク（VPN）ゲートウェイ、動的ホスト構成プロトコル（DHCP）ルータなど）、または仮想化サーバ301に接続されるかもしくはこれと通信する任意のデバイスを含んでもよい。ハードウェアレイヤ310内の物理メモリ316は、任意のタイプのメモリを含んでもよい。物理メモリ316はデータを記憶してもよく、一部の実施形態では、1つまたは複数のプログラム、あるいは実行可能命令のセットを記憶してもよい。図3に、仮想化サーバ301の物理メモリ316内にファームウェア312が記憶される一実施形態を示す。物理メモリ316に記憶されたプログラムまたは実行可能命令は、仮想化サーバ301の1つまたは複数のプロセッサ308によって実行することができる。

【0041】

仮想化サーバ301はまた、ハイパーバイザ302を含んでもよい。一部の実施形態では、ハイパーバイザ302は、仮想化サーバ301上でプロセッサ308によって実行されて、任意の数の仮想マシン332を作成して管理するプログラムであってもよい。ハイパーバイザ302は、仮想マシンモニタ、またはプラットフォーム仮想化ソフトウェアと呼ばれる場合がある。一部の実施形態では、ハイパーバイザ302は、実行可能命令と、コンピューティングマシン上で実行される仮想マシンを監視するハードウェアとの任意の組み合わせとすることができる。ハイパーバイザ302はタイプ2ハイパーバイザであってもよく、そのハイパーバイザは、仮想化サーバ301上で実行されるオペレーティングシステム314内で実行される。仮想マシンは次いで、ハイパーバイザ302より上のレベルで実行されてもよい。一部の実施形態では、タイプ2ハイパーバイザをユーザのオペレーティングシステムのコンテキスト内で実行させて、タイプ2ハイパーバイザがユーザのオペレーティングシステムとインタラクトするようにしてもよい。他の実施形態では、仮想化環境における1つまたは複数の仮想化サーバ301は、代わりにタイプ1ハイパーバイザ（図示せず）を含んでもよい。タイプ1ハイパーバイザは、ハードウェアレイヤ310内のハードウェア及びリソースに直接アクセスすることによって、仮想化サーバ301上で実行され得る。すなわち、タイプ2ハイパーバイザ302は、図示のようにホストオペレーティングシステム314経由でシステムリソースにアクセスするのに対し、タイプ1ハイパーバイザは、ホストオペレーティングシステム314なしで全てのシステムリソースに直接アクセスし得る。タイプ1ハイパーバイザは仮想化サーバ301の1つまたは複数の物理プロセッサ308上で直接実行され得、物理メモリ316に記憶されたプログラムデータを含み得る。

【0042】

ハイパーバイザ302は、一部の実施形態では、システムリソースに直接アクセスできるオペレーティングシステム330または制御プログラム320をシミュレートする任意の方法で、仮想マシン332上で実行されるオペレーティングシステム330または制御プログラム320に仮想リソースを提供することができる。システムリソースは、物理デ

10

20

30

40

50

バイス306、物理ディスク304、物理プロセッサ308、物理メモリ316、及び仮想化サーバ301のハードウェアレイヤ310に含まれる他の任意のコンポーネントを含むことができるが、これらに限定されない。ハイパーバイザ302は、仮想ハードウェアのエミュレート、物理ハードウェアの分割、物理ハードウェアの仮想化、及び／またはコンピューティング環境へのアクセスを提供する仮想マシンの実行を行うために使用されてもよい。さらに他の実施形態では、ハイパーバイザ302は、仮想化サーバ301上で実行される仮想マシン332に対してプロセッサのスケジューリング及びメモリの分割を制御してもよい。ハイパーバイザ302は、VMWare, Inc., Palo Alto, Californiaによって製造されたもの、オープンソースのXenProject.orgコミュニティによって開発が監督されるオープンソース製品であるXENPROJECTハイパーバイザ、Microsoftによって提供されるHyperV、VirtualServer、もしくはvirtual PCハイパーバイザ、またはその他を含んでもよい。一部の実施形態では、仮想化サーバ301は、ゲストオペレーティングシステムがその上で実行され得る仮想マシンプラットフォームを作成するハイパーバイザ302を実行してもよい。これらの実施形態では、仮想化サーバ301はホストサーバと呼ぶ場合がある。そのような仮想化サーバの一例は、Citrix Systems, Inc., Fort Lauderdale, FLによって提供されるXENSERVRである。

【0043】

ハイパーバイザ302は、ゲストオペレーティングシステム330がその中で実行される1つまたは複数の仮想マシン332B～C（総称して332）を作成してもよい。一部の実施形態では、ハイパーバイザ302は仮想マシンイメージをロードして仮想マシン332を作成してもよい。他の実施形態では、ハイパーバイザ302は仮想マシン332内でゲストオペレーティングシステム330を実行してもよい。さらに他の実施形態では、仮想マシン332はゲストオペレーティングシステム330を実行してもよい。

【0044】

仮想マシン332を作成することに加えて、ハイパーバイザ302は少なくとも1つの仮想マシン332の実行を制御してもよい。他の実施形態では、ハイパーバイザ302は、仮想化サーバ301によって提供される少なくとも1つのハードウェアリソース（たとえば、ハードウェアレイヤ310内で利用可能な任意のハードウェアリソース）の抽象化を、少なくとも1つの仮想マシン332に与えてもよい。他の実施形態では、ハイパーバイザ302は、仮想マシン332が仮想化サーバ301内で利用可能な物理プロセッサ308にアクセスする方法を制御してもよい。物理プロセッサ308へのアクセスを制御することは、仮想マシン332がプロセッサ308にアクセスすべきか否かを判定し、物理プロセッサの能力がどのように仮想マシン332に与えられるかを決定することを含んでもよい。

【0045】

図3に示すように、仮想化サーバ301は1つまたは複数の仮想マシン332をホストまたは実行してもよい。仮想マシン332は、プロセッサ308によって実行された場合に、仮想マシン332が物理コンピューティングデバイスによく似たようにプログラム及びプロセスを実行することができるよう、物理コンピュータの動作を模倣し得る実行可能命令のセットである。図3には仮想化サーバ301が3つの仮想マシン332をホストする一実施形態を示しているが、他の実施形態では、仮想化サーバ301は任意の数の仮想マシン332をホストすることができる。ハイパーバイザ302は、一部の実施形態では、各仮想マシン332に、その仮想マシン332が利用可能な物理ハードウェア、メモリ、プロセッサ、及び他のシステムリソースの固有の仮想ビューを提供してもよい。一部の実施形態では、固有の仮想ビューは、仮想マシンのパーミッション、1つまたは複数の仮想マシン識別子へのポリシーエンジンの適用、仮想マシンにアクセスするユーザ、仮想マシン上で実行されるアプリケーション、仮想マシンによってアクセスされるネットワーク、または他の任意の所望の基準に基づくことができる。たとえば、ハイパーバイザ302

は1つまたは複数の非セキュア仮想マシン332と、1つまたは複数のセキュア仮想マシン332とを作成してもよい。非セキュア仮想マシン332は、セキュア仮想マシン332にはアクセスが許可され得るリソース、ハードウェア、メモリ位置、及びプログラムへのアクセスが禁止され得る。他の実施形態では、ハイパーバイザ302は各仮想マシン332に、その仮想マシン332が利用可能な物理ハードウェア、メモリ、プロセッサ、及び他のシステムリソースの実質的に同様の仮想ビューを提供してもよい。

【0046】

各仮想マシン332は仮想ディスク326A～C（総称して326）と、仮想プロセッサ328A～C（総称して328）とを含んでもよい。仮想ディスク326は、一部の実施形態では、仮想化サーバ301の1つまたは複数の物理ディスク304、あるいは仮想化サーバ301の1つまたは複数の物理ディスク304の一部の仮想化ビューである。物理ディスク304の仮想化ビューは、ハイパーバイザ302によって生成、提供、及び管理することができる。一部の実施形態では、ハイパーバイザ302は各仮想マシン332に物理ディスク304の固有のビューを提供する。このように、これらの実施形態では、各仮想マシン332に含まれる特定の仮想ディスク326は、他の仮想ディスク326と比較した場合に、固有であり得る。

【0047】

仮想プロセッサ328は、仮想化サーバ301の1つまたは複数の物理プロセッサ308の仮想化ビューとすることができる。一部の実施形態では、物理プロセッサ308の仮想化ビューは、ハイパーバイザ302によって生成、提供及び管理することができる。一部の実施形態では、仮想プロセッサ328は、少なくとも1つの物理プロセッサ308と同じ特徴の実質的に全てを有する。他の実施形態では、仮想プロセッサ308は、仮想プロセッサ328の特徴の少なくとも一部が、対応する物理プロセッサ308の特徴と異なるような、物理プロセッサ308の修正ビューを提供する。

【0048】

図4をさらに参照すると、本明細書に記載の一部の態様は、クラウドベースの環境に実装されてもよい。図4に、クラウドコンピューティング環境（またはクラウドシステム）400の一例を示す。図4に見られるように、クライアントコンピュータ411～414はクラウド管理サーバ410と通信して、クラウドシステムのコンピューティングリソース（たとえば、ホストサーバ403a～403b（本明細書では総称して「ホストサーバ403」と呼ぶ）、ストレージリソース404a～404b（本明細書では総称して「ストレージリソース404」と呼ぶ）、及びネットワークリソース405a～405b（本明細書では総称して「ネットワークリソース405」と呼ぶ））にアクセスしてもよい。

【0049】

管理サーバ410は1つまたは複数の物理サーバ上に実装されてもよい。管理サーバ410は、たとえば、とりわけ、Citrix Systems, Inc., Ft. Lauderdale, FLのCLOUDPLATFORM、またはOPENSTACKを稼働させてもよい。管理サーバ410は、たとえば、ホストコンピュータ403、データストレージデバイス404、及びネットワークングデバイス405などのクラウドハードウェア及びソフトウェアリソースを含む様々なコンピューティングリソースを管理してもよい。クラウドハードウェア及びソフトウェアリソースは、プライベート及び／またはパブリックコンポーネントを含んでもよい。たとえば、クラウドは1つまたは複数の特定の顧客もしくはクライアントコンピュータ411～414によって、及び／またはプライベートネットワークを介して使用されるプライベートクラウドとして構成されてもよい。他の実施形態では、パブリッククラウドまたはハイブリッドのパブリックプライベートクラウドが、他の顧客によって、オープンネットワークまたはハイブリッドネットワークを介して使用されてもよい。

【0050】

管理サーバ410は、クラウドオペレータ及びクラウド顧客がクラウドシステム400とインタラクトし得るユーザインターフェースを提供するように構成されてもよい。たと

10

20

30

40

50

えば、管理サーバ410は、クラウドオペレータがクラウドリソースを管理し、仮想化レイヤを構成し、顧客アカウントを管理し、他のクラウド管理タスクを行うことを可能にするユーザインターフェースを有する、アプリケーションプログラミングインタフェース（API）のセット、及び／または1つまたは複数のクラウドオペレータコンソールアプリケーション（たとえば、ウェブベースもしくはスタンドアロンのアプリケーション）を提供してもよい。管理サーバ410はまた、クライアントコンピュータ411～414を介したエンドユーザからのクラウドコンピューティング要求、たとえば、クラウド内で仮想マシンを作成、修正、または破棄する要求を受信するように構成されるユーザインターフェースを有する、APIのセット及び／または1つまたは複数の顧客コンソールアプリケーションを含んでもよい。クライアントコンピュータ411～414はインターネットまたは他の何らかの通信ネットワークを介して管理サーバ410に接続してもよく、管理サーバ410によって管理されるコンピューティングリソースのうちの1つまたは複数へのアクセスを要求してもよい。クライアントの要求にตอบสนองして、管理サーバ410は、クライアント要求に基づいて、クラウドシステムのハードウェアレイヤ内の物理リソースを選択してプロビジョニングするように構成されるリソースマネージャを含んでもよい。たとえば、管理サーバ410及びクラウドシステムの追加のコンポーネントは、クライアントコンピュータ411～414の顧客に対して、ネットワーク（たとえば、インターネット）を介して、仮想マシン及びそれらの動作環境（たとえば、ハイパーバイザ、ストレージリソース、ネットワーク要素によって提供されるサービスなど）をプロビジョニングし、作成し、管理し、顧客に計算リソース、データストレージサービス、ネットワーク能力、ならびにコンピュータプラットフォーム及びアプリケーションサポートを提供するように構成されてもよい。クラウドシステムはまた、セキュリティシステム、開発環境、ユーザインターフェースなどを含む様々な特定のサービスを提供するように構成されてもよい。

10

20

【0051】

特定のクライアント411～414は、同じエンドユーザ、または同じ会社もしくは組織に属する異なるユーザのために、仮想マシンを作成する異なるクライアントコンピュータなどに関連付けられてもよい。他の例では、特定のクライアント411～414は、異なる会社または組織に属するユーザなど、無関係であってもよい。無関係のクライアントの場合、任意の1人のユーザの仮想マシンまたはストレージに関する情報は、他のユーザから隠されてもよい。

30

【0052】

ここでクラウドコンピューティング環境の物理ハードウェアレイヤを参照すると、可用性ゾーン401～402（またはゾーン）は、一緒に配置された物理コンピューティングリソースのセットを指す場合がある。コンピューティングリソースのクラウド全体において、ゾーンは他のゾーンとは地理的に離れ得る。たとえば、ゾーン401はカリフォルニア州にある第1のクラウドデータセンターであってもよく、ゾーン402はフロリダ州にある第2のクラウドデータセンターであってもよい。管理サーバ410は可用性ゾーンのうちの1つ、または別の場所に配置されてもよい。各ゾーンは、管理サーバ410などのゾーン外のデバイスとゲートウェイ経由でインターフェースする内部ネットワークを含んでもよい。クラウドのエンドユーザ（たとえば、クライアント411～414）は、ゾーン間の区別を認識してもよく、しなくてもよい。たとえば、エンドユーザは、指定量のメモリ、処理能力、及びネットワーク能力を有する仮想マシンの作成を要求してもよい。管理サーバ410はユーザの要求にตอบสนองしてもよく、ゾーン401またはゾーン402のいずれのリソースを使用して仮想マシンが作成されたかどうかをユーザが知ることなく、仮想マシンを作成するためのリソースを割り当ててもよい。他の例では、クラウドシステムは、特定のゾーン内で、またはあるゾーン内の特定のリソース403～405上で仮想マシン（または他のクラウドリソース）が割り当てられるように、エンドユーザが要求することを可能にし得る。

40

【0053】

50

この例では、各ゾーン401～402は様々な物理ハードウェアコンポーネント（またはコンピューティングリソース）403～405、たとえば、物理ホスティングリソース（またはプロセッシングリソース）、物理ネットワークリソース、物理ストレージリソース、スイッチ、及びクラウドコンピューティングサービスを顧客に提供するために使用され得る追加のハードウェアリソースの配置を含んでもよい。クラウドゾーン401～402内の物理ホスティングリソースは、上述した仮想化サーバ301など、仮想マシンのインスタンスを作成してホストするように構成され得る1つまたは複数のコンピュータサーバ403を含んでもよい。クラウドゾーン401または402内の物理ネットワークリソースは、ファイアウォール、ネットワークアドレス変換器、ロードバランサ、仮想プライベートネットワーク（VPN）ゲートウェイ、動的ホスト構成プロトコル（DHCP）ルータなど、クラウド顧客にネットワークサービスを提供するように構成されるハードウェア及び／またはソフトウェアを含む1つまたは複数のネットワーク要素405（たとえば、ネットワークサービスプロバイダ）を含んでもよい。クラウドゾーン401～402内のストレージリソースは、ストレージディスク（たとえば、ソリッドステートドライブ（SSD）、磁気ハードディスクなど）、及び他のストレージデバイスを含んでもよい。

【0054】

図4に示す例示的なクラウドコンピューティング環境はまた、クラウドの物理リソースを使用して仮想マシンを作成して管理し、他のサービスを顧客に提供するように構成される追加のハードウェア及び／またはソフトウェアリソースを有する仮想化レイヤ（たとえば、図1～図3に図示）を含んでもよい。仮想化レイヤは、図3で上述したハイパーバイザを、ネットワーク仮想化、ストレージ仮想化などを提供する他のコンポーネントと共に含んでもよい。仮想化レイヤは、物理リソースレイヤとは別のレイヤとしてもよく、または物理リソースレイヤと同じハードウェア及び／またはソフトウェアリソースの一部または全部を共有してもよい。たとえば、仮想化レイヤは、仮想化サーバ403のそれぞれにインストールされたハイパーバイザを、物理コンピューティングリソースと共に含んでもよい。あるいは、たとえば、WINDOWS（登録商標）AZURE（Microsoft Corporation, Redmond Washington）、AMAZON EC2（Amazon.com Inc., Seattle, Washington）、IBM BLUE CLOUD（IBM Corporation, Armonk, New York）、またはその他など、知られているクラウドシステムが使用されてもよい。

【0055】

企業モビリティ管理アーキテクチャ

図5に、「Bring Your Own Device」（BYOD）環境で使用するための企業モビリティ技術アーキテクチャ500を示す。このアーキテクチャは、モバイルデバイス502のユーザがモバイルデバイス502から企業リソースまたは個人リソースにアクセスすることと、モバイルデバイス502を個人用途に使用することと、の両方を可能にする。ユーザは、ユーザが購入したモバイルデバイス502、または企業がユーザに支給したモバイルデバイス502を使用して、そのような企業リソース504または企業サービス508にアクセスしてもよい。ユーザはモバイルデバイス502を仕事専用にしてもよく、仕事及び個人兼用にしてもよい。モバイルデバイス502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などを稼働させてもよい。企業はモバイルデバイス502を管理するためのポリシーを実装することを選んでよい。ポリシーは、モバイルデバイス502が識別、セキュア化、もしくはセキュリティ検証がなされ、企業リソース（たとえば、504及び508）への選択的アクセスもしくはフルアクセスが提供され得るように、ファイアウォールまたはゲートウェイ経由で実装されてもよい。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、及びデータ管理ポリシーのなんらかの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適用を通じて管理されるモバイルデバイス502を、登録

済みデバイスと呼ぶ場合がある。

【0056】

一部の実施形態では、モバイルデバイス502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510と非管理対象パーティション512とに分離されてもよい。管理対象パーティション510は、管理対象パーティション510上で稼動するアプリケーション及びそこに記憶されたデータをセキュア化するためのポリシーが適用されてもよい。管理対象パーティション510上で稼動するアプリケーションは、セキュアアプリケーションであってもよい。他の実施形態では、全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する1つまたは複数のポリシーファイルのセットに従って実行されてもよく、これらは、1つまたは複数のセキュリティパラメータ、機能、リソース制約、及び／または、そのアプリケーションがモバイルデバイス502上で実行されている場合にモバイルデバイス管理システムによって施行される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（複数可）に従って動作することにより、各アプリケーションは、1つまたは複数の他のアプリケーション及び／またはリソースとの通信が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が作成される。このように、本明細書で使用する場合、パーティションとは、メモリの物理的に分割された部分（物理パーティション）、メモリの論理的に分割された部分（論理パーティション）、及び／または、本明細書に記載のように複数のアプリケーションにわたって1つまたは複数のポリシー及び／またはポリシーファイルを施行した結果として作成される仮想的なパーティション（仮想パーティション）を指す場合がある。別の言い方をすれば、管理対象アプリケーションにポリシーを施行することにより、それらのアプリケーションを、他の管理対象アプリケーション及び信頼済みの企業リソースとしか通信できないように制限することによって、非管理対象アプリケーション及びデバイスにはアクセスできない仮想パーティションを作成してもよい。

【0057】

セキュアアプリケーションは、電子メールアプリケーション、ウェブブラウジングアプリケーション、ソフトウェアアズアサービス（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などであってもよい。セキュアアプリケーションは、セキュアネイティブアプリケーション514、セキュアアプリケーションランチャ518によって実行されるセキュアリモートアプリケーション522、セキュアアプリケーションランチャ518によって実行される仮想化アプリケーション526などであってもよい。セキュアネイティブアプリケーション514は、セキュアアプリケーションラッパー520によってラッピングされてもよい。セキュアアプリケーションラッパー520は、セキュアネイティブアプリケーション514がモバイルデバイス502上で実行される場合に、モバイルデバイス502上で実行される統合されたポリシーを含んでもよい。セキュアアプリケーションラッパー520は、モバイルデバイス502上で稼動するセキュアネイティブアプリケーション514を、セキュアネイティブアプリケーション514の実行時に要求されるタスクを完了するためにセキュアネイティブアプリケーション514が必要とし得る、企業でホストされるリソース（たとえば、504及び508）に差し向けるメタデータを含んでもよい。セキュアアプリケーションランチャ518によって実行されるセキュアリモートアプリケーション522は、セキュアアプリケーションランチャ518内で実行されてもよい。セキュアアプリケーションランチャ518によって実行される仮想化アプリケーション526は、モバイルデバイス502上のリソース、企業リソース504におけるリソースなどを利用してよい。セキュアアプリケーションランチャ518によって実行される仮想化アプリケーション526によってモバイルデバイス502上で使用されるリソースは、ユーザインタラクションリソース、プロセッシングリソースなどを含んでもよい。ユーザインタラクションリソースは、キーボード入力、マウス入力、カメラ入力、触覚入力、オーディオ入力、ビジュアル入力、ジェスチャ入力などを収集して伝送するために使用されてもよい。プロセッシングリソースは、ユーザインターフェースを提示し、企業リソース504から受信し

10

20

30

40

50

たデータを処理するなどのために使用されてもよい。セキュアアプリケーションランチャ 518 によって実行される仮想化アプリケーション 526 によって企業リソース 504 において使用されるリソースは、ユーザインターフェース生成リソース、プロセッシングリソースなどを含んでもよい。ユーザインターフェース生成リソースは、ユーザインターフェースをアSEMBルし、ユーザインターフェースを修正し、ユーザインターフェースをリフレッシュするなどのために使用されてもよい。プロセッシングリソースは、情報を作成し、情報を読み込み、情報を更新し、情報を削除するなどのために使用されてもよい。たとえば、仮想化アプリケーション 526 は、グラフィカルユーザインターフェース（GUI）に関連するユーザインタラクションを記録し、それらをサーバアプリケーションに伝達してもよく、サーバアプリケーションは、ユーザインタラクションデータをサーバ上で動作するアプリケーションへの入力として使用することになる。そのような構成では、企業は、アプリケーションに関連するデータ、ファイルなどと同様に、アプリケーションをサーバ側で維持することを選択してもよい。企業は、一部のアプリケーションをセキュア化してモバイルデバイス 502 にデプロイすることにより、それらを本明細書の原理に従って「モバイル化」することを選択してもよいが、この構成は特定のアプリケーションのためにも選択されてもよい。たとえば、一部のアプリケーションはモバイルデバイス 502 で使用するためにセキュア化されてもよいが、その他は、モバイルデバイス 502 にデプロイする準備ができていないかまたはそれに適さない場合があるので、企業は仮想化技術を通じて、準備ができていないアプリケーションへのアクセスをモバイルユーザに提供することを選択してもよい。他の例として、企業は、大規模かつ複雑なデータセットを有する大規模かつ複雑なアプリケーション（たとえば、材料資源計画アプリケーション）を有する場合があります、モバイルデバイス 502 用にアプリケーションをカスタマイズするのは非常に難しく、あるいは望ましくないと思われるので、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。さらに他の例として、企業は、セキュア化されたモバイル環境にとっても機密性が高すぎると企業に見なされ得る高セキュア化データ（たとえば、人事データ、顧客データ、技術データ）を維持するアプリケーションを有する場合があります、そのため企業は、そのようなアプリケーション及びデータへのモバイルアクセスを許可するために仮想化技術を使用することを選択してもよい。企業は、完全にセキュア化されかつ完全に機能するアプリケーションをモバイルデバイス 502 上に提供すると共に、仮想化アプリケーション 526 が、サーバ側でより適切に動作すると見なされるアプリケーションへのアクセスを許可することを選択してもよい。一実施形態では、仮想化アプリケーション 526 は、モバイルデバイス 502 の一部のデータ、ファイルなどをセキュアな記憶場所のうちの 1 つに記憶してもよい。企業は、たとえば、特定の情報をモバイルデバイス 502 に記憶することを許可するが、他の情報は許可しないことを選択してもよい。

【0058】

本明細書に記載の仮想化アプリケーション 526 に関連して、モバイルデバイス 502 は、GUI を提示して GUI とのユーザインタラクションを記録するように設計された仮想化アプリケーション 526 を有してもよい。仮想化アプリケーション 526 は、ユーザインタラクションをサーバ側に伝達し、これはサーバ側アプリケーションによって、アプリケーションとのユーザインタラクションとして使用されてもよい。それに応答して、サーバ側のアプリケーションは、モバイルデバイス 502 に新たな GUI を返してもよい。たとえば、新たな GUI は、静的なページ、動的なページ、アニメーションなどであってもよく、それによってリモート配置されたリソースへのアクセスを提供する。

【0059】

セキュアアプリケーション 514 は、モバイルデバイス 502 の管理対象パーティション 510 内のセキュアデータコンテナ 528 に記憶されたデータにアクセスしてもよい。セキュアデータコンテナ内でセキュア化されたデータは、セキュアネイティブアプリケーション 514、セキュアアプリケーションランチャ 518 によって実行されるセキュアリモートアプリケーション 522、セキュアアプリケーションランチャ 518 によって実行

10

20

30

40

50

される仮想化アプリケーション526などによってアクセスされてもよい。セキュアデータコンテナ528に記憶されたデータは、ファイル、データベースなどを含んでもよい。セキュアデータコンテナ528に記憶されたデータは、特定のセキュアアプリケーション530に制限されるデータ、セキュアアプリケーション532の間で共有されるデータなどを含んでもよい。あるセキュアアプリケーションに制限されるデータは、セキュア一般データ534と、高セキュアデータ538とを含んでもよい。セキュア一般データは、高度暗号化標準(AES)128ビット暗号化などの強力な暗号化形式を使用してもよく、高セキュアデータ538は、AES256ビット暗号化などの非常に強力な暗号化形式を使用してもよい。セキュアデータコンテナ528に記憶されたデータは、デバイスマネージャ524からのコマンドを受信すると、モバイルデバイス502から削除されてもよい。セキュアアプリケーション(たとえば、514、522、及び526)は、デュアルモードオプション540を有してもよい。デュアルモードオプション540は、セキュア化アプリケーションを非セキュア化または非管理モードで動作させるオプションをユーザに提示し得る。非セキュア化または非管理モードでは、セキュアアプリケーションは、モバイルデバイス502の非管理対象パーティション512の非セキュア化データコンテナ542に記憶されたデータにアクセスし得る。非セキュア化データコンテナに記憶されたデータは、個人データ544であってもよい。非セキュア化データコンテナ542に記憶されたデータはまた、モバイルデバイス502の非管理対象パーティション512で稼動する非セキュア化アプリケーション546によってアクセスされてもよい。セキュアデータコンテナ528に記憶されたデータがモバイルデバイス502から削除される場合に、非セキュア化データコンテナ542に記憶されたデータはモバイルデバイス502上に残してもよい。企業は、企業によって所有、ライセンス、または管理される選択されたもしくは全てのデータ、ファイル、及び／またはアプリケーション(企業データ)をモバイルデバイス502から削除しつつ、ユーザによって所有、ライセンス、または管理される個人データ、ファイル、及び／またはアプリケーション(個人データ)を残すかまたは別の方法で保存したい場合がある。この動作は選択的ワイプと呼ばれる場合がある。本明細書に記載の態様に従って配置される企業データ及び個人データを用いて、企業は選択的ワイプを行ってもよい。

【0060】

モバイルデバイス502は企業の企業リソース504及び企業サービス508、公衆インターネット548などに接続してもよい。モバイルデバイス502は仮想プライベートネットワーク接続を介して企業リソース504及び企業サービス508に接続してもよい。仮想プライベートネットワーク接続は、マイクロVPNまたはアプリケーション別VPNとも呼ばれるが、特定のアプリケーション(マイクロVPN550として示す)、特定のデバイス、モバイルデバイス上の特定のセキュア化エリア(O/S VPN552として示す)などに専用のものであってもよい。たとえば、モバイルデバイス502のセキュア化エリア内のラッピングされたアプリケーションのそれぞれは、VPNへのアクセスが、場合によりユーザまたはデバイスの属性情報と共に、アプリケーションに関連する属性に基づいて付与されるように、アプリケーション別VPN経由で企業リソースにアクセスしてもよい。仮想プライベートネットワーク接続はMicrosoft Exchangeトラフィック、Microsoft Active Directoryトラフィック、ハイパーテキスト転送プロトコル(HTTP)トラフィック、ハイパーテキスト転送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などを搬送してもよい。仮想プライベートネットワーク接続は、シングルサインオン認証プロセス554をサポートし、有効化してもよい。シングルサインオンプロセスは、ユーザが単一セットの認証資格情報を提供できるようにしてもよく、これは後で認証サービス558によって検証される。認証サービス558は次いで、各個々の企業リソース504に認証資格情報を提供するようにユーザに求めることなく、複数の企業リソース504へのアクセスをユーザに付与し得る。

【0061】

仮想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560によって確立され、管理されてもよい。アクセスゲートウェイ560は、モバイルデバイス502への企業リソース504の配信を管理し、高速化し、改善するパフォーマンス向上機能を含んでもよい。アクセスゲートウェイ560はまた、モバイルデバイス502からのトラフィックを公衆インターネット548に経路切替して、モバイルデバイス502が公衆インターネット548上で稼動する公的に利用可能な非セキュア化アプリケーションにアクセスすることを可能にし得る。モバイルデバイス502は、転送ネットワーク562を介してアクセスゲートウェイに接続してもよい。転送ネットワーク562は1つまたは複数の転送プロトコルを使用してもよく、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、パブリックネットワーク、プライベートネットワークなどであってもよい。

10

【0062】

企業リソース504は、電子メールサーバ、ファイル共有サーバ、SaaSアプリケーション、ウェブアプリケーションサーバ、Windows（登録商標）アプリケーションサーバなどを含んでもよい。電子メールサーバは、Exchangeサーバ、Lotus Notesサーバなどを含んでもよい。ファイル共有サーバは、ShareFileサーバなどを含んでもよい。SaaSアプリケーションは、Salesforceなどを含んでもよい。Windows（登録商標）アプリケーションサーバは、ローカルなWindows（登録商標）オペレーティングシステムで稼動するように意図されたアプリケーションなどを提供するように構築される任意のアプリケーションサーバを含んでもよい。企業リソース504はプレミスペースのリソース、クラウドベースのリソースなどであってもよい。企業リソース504はモバイルデバイス502によって直接、またはアクセスゲートウェイ560経由でアクセスされてもよい。企業リソース504はモバイルデバイス502によって転送ネットワーク562を介してアクセスされてもよい。

20

【0063】

企業サービス508は、認証サービス558、脅威検出サービス564、デバイスマネージャサービス524、ファイル共有サービス568、ポリシーマネージャサービス570、ソーシャル統合サービス572、アプリケーションコントローラサービス574などを含んでもよい。認証サービス558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などを含んでもよい。認証サービス558は証明書を使用してもよい。証明書は、企業リソース504などによって、モバイルデバイス502上に記憶してもよい。モバイルデバイス502上に記憶された証明書は、モバイルデバイス502上の暗号化された場所に記憶されてもよく、証明書は認証時に使用するなどのためにモバイルデバイス502に一時的に記憶されてもよい。脅威検出サービス564は、侵入検出サービス、不正アクセス試行検出サービスなどを含んでもよい。不正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、データなどへの不正なアクセスの試行を含んでもよい。デバイス管理サービス524は、構成サービス、プロビジョニングサービス、セキュリティサービス、サポートサービス、監視サービス、報告サービス、及び廃止サービスを含んでもよい。ファイル共有サービス568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などを含んでもよい。ポリシーマネージャサービス570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などを含んでもよい。ソーシャル統合サービス572は、連絡先統合サービス、コラボレーションサービス、Facebook、Twitter、及びLinkedInなどのソーシャルネットワークとの統合などを含んでもよい。アプリケーションコントローラサービス574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、割り当てサービス、失効サービス、ラッピングサービスなどを含んでもよい。

30

40

【0064】

企業モビリティ技術アーキテクチャ500は、アプリケーションストア578を含んでもよい。アプリケーションストア578は、ラッピングされていないアプリケーション5

50

80、事前にラッピングされたアプリケーション582などを含んでもよい。アプリケーションは、アプリケーションコントローラ574からアプリケーションストア578に配置されてもよい。アプリケーションストア578は、モバイルデバイス502によって、アクセスゲートウェイ560、公衆インターネット548などを経由してアクセスされてもよい。アプリケーションストア578には、直観的かつ使いやすいユーザインターフェースが設けられてもよい。

【0065】

ソフトウェア開発キット584は、本明細書で前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、ユーザにより選択されたアプリケーションをセキュア化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584を使用してラッピングされたアプリケーションは次いで、アプリケーションコントローラ574を使用してアプリケーションストア578内に配置することにより、モバイルデバイス502に利用可能にされてもよい。

【0066】

企業モビリティ技術アーキテクチャ500は、管理・解析機能588を含んでもよい。管理・解析機能588は、リソースの使用方法、リソースの使用頻度などに関連する情報を提供してもよい。リソースは、デバイス、アプリケーション、データなどを含んでもよい。リソースの使用方法は、どのデバイスがどのアプリケーションをダウンロードするか、どのアプリケーションがどのデータにアクセスするか、などを含んでもよい。リソースの使用頻度は、アプリケーションがダウンロードされた頻度、特定のデータセットがアプリケーションによってアクセスされた回数などを含んでもよい。

【0067】

図6は、他の例示的な企業モビリティ管理システム600である。図5を参照して上述したモビリティ管理システム500のコンポーネントのうちの一部は、簡単にするために省略している。図6に示すシステム600のアーキテクチャは、図5を参照して上述したシステム500のアーキテクチャと多くの点で類似しており、上述していない追加機能を含み得る。

【0068】

この場合、左手側は、クライアントエージェント604を有する登録済みモバイルデバイス602を表しており、クライアントエージェント604は、ゲートウェイサーバ606（これはアクセスゲートウェイ及びアプリケーションコントローラ機能を含む）とインタラクトして、右手側上方に示す様々な企業リソース608及びサービス609、たとえば、Exchange、Sharepoint、公開鍵基盤（PKI）リソース、ケルベロス（Kerberos）リソース、証明書発行サービスにアクセスする。具体的には示していないが、モバイルデバイス602はまた、アプリケーションの選択及びダウンロードのために企業アプリケーションストア（StoreFront）とインタラクトしてもよい。

【0069】

クライアントエージェント604は、高品位ユーザエクスペリエンス（HDX）／ICAディスプレイリモートプロトコルを使用してアクセスされる、企業データセンターでホストされるWindows（登録商標）アプリ／デスクトップへの媒介となるUI（ユーザインターフェース）として機能する。クライアントエージェント604は、ネイティブiOSまたはAndroid（登録商標）アプリケーションなど、モバイルデバイス602へのネイティブアプリケーションのインストール及び管理もサポートする。たとえば、上記の図に示す管理対象アプリケーション610（メール、ブラウザ、ラッピングされたアプリケーション）は全て、モバイルデバイス602上でローカルに実行されるネイティブアプリケーションである。クライアントエージェント604及びこのアーキテクチャのアプリケーション管理フレームワークは、企業リソース／サービス608との接続性及びSSO（シングルサインオン）などのポリシー主導の管理機能及び機能を提供するように機能する。クライアントエージェント604は、企業への、通常はアクセスゲート

ウェイ（AG）606への一次ユーザ認証を、他のゲートウェイサーバコンポーネントへのSSOと共に担当する。クライアントエージェント604はゲートウェイサーバ606からポリシーを取得して、モバイルデバイス602上の管理対象アプリケーション610の挙動を制御する。

【0070】

ネイティブアプリケーション610とクライアントエージェント604との間のセキュアプロセス間通信（IPC）リンク612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は、ポリシーを供給することが可能になり得、ポリシーは、アプリケーション管理フレームワーク614が各アプリケーションを「ラッピング」することによって施行される。IPCチャネル612はまた、クライアントエージェント604が、企業リソース608との接続性及びSSOを可能にする資格情報及び認証情報を供給することを可能にし得る。最後に、IPCチャネル612は、アプリケーション管理フレームワーク614が、クライアントエージェント604によって実装されるユーザインターフェース機能、たとえばオンライン及びオフライン認証を呼び出すことを可能にし得る。

10

【0071】

クライアントエージェント604とゲートウェイサーバ606との間の通信は、基本的には、各ネイティブ管理対象アプリケーション610をラッピングするアプリケーション管理フレームワーク614から管理チャネルを拡張したものである。アプリケーション管理フレームワーク614はクライアントエージェント604にポリシー情報を要求してもよく、今度はクライアントエージェント604がゲートウェイサーバ606にポリシー情報を要求してもよい。アプリケーション管理フレームワーク614は認証を要求してもよく、クライアントエージェント604は、（NETSCALER ACCESS GATEWAYとしても知られている）ゲートウェイサーバ606のゲートウェイサービス部分にログインしてもよい。クライアントエージェント604はまた、ゲートウェイサーバ606上のサポートサービスを呼び出してもよく、これは、以下で十分に説明するように、ローカルデータボルト616用の暗号化鍵を導出するための入力素材を生成してもよく、またはPKI保護リソースへの直接認証を可能にし得るクライアント証明書を提供してもよい。

20

【0072】

より詳細には、アプリケーション管理フレームワーク614は各管理対象アプリケーション610を「ラッピング」する。これは明確な構築ステップ、または構築後の処理ステップによっ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614は、アプリケーション610の初回起動時にクライアントエージェント604と「ペア」を組んで、セキュアIPCチャネル612を初期化し、そのアプリケーションのポリシーを取得してもよい。アプリケーション管理フレームワーク614は、ローカルに適用されるポリシーの関連部分、たとえば、クライアントエージェントのログイン依存関係、及びローカルOSサービスが使用され得る方法、またはそれらが管理対象アプリケーション610とインタラクトし得る方法を制限する閉じ込め（containment）ポリシーの一部を施行してもよい。

30

【0073】

アプリケーション管理フレームワーク614は、セキュアIPCチャネル612を介してクライアントエージェント604によって提供されるサービスを使用して、認証及び内部ネットワークアクセスを容易にしてもよい。プライベート及び共有データボルト616（コンテナ）の鍵管理もまた、管理対象アプリケーション610とクライアントエージェント604との間の適切なインタラクションによって管理されてもよい。ボルト616はオンライン認証後にのみ利用可能になってもよく、またはポリシーによって許可される場合にはオフライン認証後に利用可能になされてもよい。ボルト616の最初の使用はオンライン認証を求めてもよく、オフラインアクセスは、最大でも、オンライン認証が再び求めら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。

40

【0074】

50

内部リソースへのネットワークアクセスは、個々の管理対象アプリケーション610からアクセスゲートウェイ606を介して直接行われてもよい。アプリケーション管理フレームワーク614は、各管理対象アプリケーション610の代わりにネットワークアクセスの指揮を担ってもよい。クライアントエージェント604は、オンライン認証後に取得される適切な時間制限付きの二次資格情報を提供することにより、これらのネットワーク接続を容易にしてもよい。リバースウェブプロキシ接続及びエンドツーエンドVPN型トンネル618など、複数のネットワーク接続のモードが使用されてもよい。

【0075】

メール及びブラウザ管理対象アプリケーション610は特別なステータスを有し、任意のラッピングされたアプリケーションには一般に利用可能でない場合がある設備を利用してもよい。たとえば、メールアプリケーション610は、フルAGログオンを必要とせず、長時間にわたってExchangeサーバ608にアクセスすることを許可する特別なバックグラウンドネットワークアクセスメカニズムを使用してもよい。ブラウザアプリケーション610は複数のプライベートデータボルト616を使用して、異なる種類のデータを分別してもよい。

10

【0076】

このアーキテクチャは、他の様々なセキュリティ機能の組み込みをサポートしてもよい。たとえば、ゲートウェイサーバ606（そのゲートウェイサービスを含む）は、一部のケースでは、Active Directory（AD）パスワードの有効性検証をする必要がなくてもよい。ADパスワードが一部の状況において一部のユーザ用の認証要素として使用されてもよいか否かは、企業の裁量に任せることができる。ユーザがオンラインの場合とオフラインの場合とで（すなわち、ネットワークに接続されている場合と接続されていない場合とで）、異なる認証方法が使用されてもよい。

20

【0077】

ステップアップ認証とは、ゲートウェイサーバ606が、強力な認証を必要とする極秘データへのアクセスが許可される管理対象ネイティブアプリケーション610を識別し、以前の弱いレベルのログイン後にユーザによる再認証が必要になることになって、これらのアプリケーションへのアクセスが適切な認証を行った後にのみ許可されるようにし得る機能である。

【0078】

このソリューションの他のセキュリティ機能は、モバイルデバイス602上でのデータボルト616（コンテナ）の暗号化である。ボルト616は、ファイル、データベース、及び構成を含むデバイス上の全データが保護されるように暗号化されてもよい。オンラインボルトの場合、鍵はサーバ（ゲートウェイサーバ606）上に記憶されてもよく、オフラインボルトの場合、鍵のローカルコピーがユーザパスワードまたはバイオメトリック認証によって保護されてもよい。データがローカルにモバイルデバイス602のセキュアコンテナ616に記憶される場合または時に、最低でもAES256暗号化アルゴリズムが利用されるのが好ましい場合がある。

30

【0079】

他のセキュアコンテナ機能も実装されてもよい。たとえば、管理対象アプリケーション610内で起こるセキュリティイベントがログ記録されてバックエンドに報告され得るロギング機能が含まれてもよい。データワイプがサポートされてもよく、管理対象アプリケーション610が改ざんを検出した場合または時などに、関連する暗号化鍵をランダムデータで上書きして、ユーザデータが破棄されたことの手がかりをファイルシステムに残さないようにしてもよい。スクリーンショットの保護が他の機能であってもよく、アプリケーションはいかなるデータもスクリーンショットに記憶されないようにしてもよい。たとえば、鍵ウイ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、現在スクリーンに表示されているあらゆるコンテンツが隠され得るので、通常は任意のコンテンツが存在するはずのスクリーンショットがブランクになる。

40

【0080】

50

たとえば、データを外部のアプリケーションにコピーするかまたは送るなど、データがアプリケーションコンテナ外にローカルに転送されることを防止することによって、ローカルなデータ転送が防止されてもよい。キーボードキャッシュ機能は、機密性が高いテキストフィールドのオートコレクト機能を無効化するように動作してもよい。SSL証明書の有効性検証は、アプリケーションがサーバSSL証明書を特別に有効性検証し、チェーンには記憶しないように動作可能であってもよい。モバイルデバイス602上でデータを暗号化するために使用される鍵が、（オフラインアクセスが必要な場合に）ユーザによって供給されるパスフレーズまたはバイオメトリックデータを使用して生成されるような、暗号化鍵生成機能を使用されてもよい。オフラインアクセスが必要でない場合、サーバ側でランダムに生成されて記憶される他の鍵とのXORがとられてもよい。鍵導出関数は、ユーザパスワードから生成される鍵が、その暗号学的ハッシュを作成するのではなく、KDF（鍵導出関数、特にパスワードベースの鍵導出関数2（PBKDF2））を使用するように動作してもよい。後者では、鍵が総当たり攻撃または辞書攻撃を受けやすくなる。

10

【0081】

さらに、暗号化方法において1つまたは複数の初期化ベクトルが使用されてもよい。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は異なる暗号文出力を生成することになり、リプレイアタック及び暗号解読攻撃の両方が防止される。これにより攻撃者は、盗んだ暗号鍵を用いても、いかなるデータも復号できなくなる。さらに、ユーザがアプリケーション内で認証した後でのみ、アプリケーションデータが復号される、認証後復号が使用されてもよい。他の機能はメモリ内の機密性が高いデータに関するものでもよく、それは必要な場合にのみ、メモリに（ディスクにではなく）保管されてもよい。たとえば、ログイン資格情報はログイン後にメモリからワイプされてもよく、オブジェクトブCインスタンス変数内の暗号化鍵及び他のデータは、簡単に参照され得るので記憶されない。その代わりに、これらにメモリが手動で割り当てられてもよい。

20

【0082】

ポリシーで定義された無活動期間の後に、ユーザセッションが終了される無活動タイムアウトが実装されてもよい。

【0083】

アプリケーション管理フレームワーク614からのデータ漏洩は、他の方法で防止されてもよい。たとえば、管理対象アプリケーション610がバックグラウンドになった場合または時に、所定の（設定可能な）期間の後にメモリがクリアされてもよい。バックグラウンド化される場合、アプリケーションの最後に表示された画面のスナップショットをとって、フォアグラウンドのプロセスを固定してもよい。スクリーンショットは機密データを含む場合があるので、クリアされるべきである。

30

【0084】

他のセキュリティ機能は、1つまたは複数のアプリケーションにアクセスするために、AD（Active Directory）622のパスワードを使用せずに、OTP（ワンタイムパスワード）620を使用することに関するものでもよい。一部のケースでは、一部のユーザは自身のADパスワードを知らず（または知ることを許可されておらず）、そのためこれらユーザはOTP620を使用して、たとえばSecurIDのようなハードウェアOTPシステムを使用して、認証してもよい（OTPは、EntrustやGemaltoなど、異なるベンダによって提供されてもよい）。一部のケースでは、ユーザがユーザIDで認証した後、OTP620を有するテキストがユーザに送られてもよい。一部のケースでは、これは、プロンプトが単一フィールドである、オンライン利用の場合にのみ実施されてもよい。

40

【0085】

企業ポリシーによってオフライン使用が許可される管理対象アプリケーション610については、オフライン認証のためにオフラインパスワードが実装されてもよい。たとえば、企業は、StoreFrontがこの方法でアクセスされることを望む場合がある。こ

50

の場合、クライアントエージェント604は、ユーザにカスタムオフラインパスワードを設定するように求めてもよく、ADパスワードは使用されない。ゲートウェイサーバ606は、パスワードの最小長、文字種の組み合わせ、及び有効期限に関するパスワード標準を管理及び施行するポリシーを提供してもよく、たとえば、標準的なWindows（登録商標）Serverのパスワードの複雑さの要件によって記述されるものなどであるが、これらの要件は修正されてもよい。

【0086】

他の機能は、特定のアプリケーション610用のクライアント側証明書を二次資格情報として有効化すること（アプリケーション管理フレームワークのマイクロVPN機能を介してPKI保護ウェブリソースにアクセスするため）に関するものでもよい。たとえば、管理対象アプリケーション610はそのような証明書を利用し得る。この場合、ActiveSyncプロトコルを使用した証明書に基づく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604からの証明書はゲートウェイサーバ606によって取得され、キーチェーンで使用されてもよい。各管理対象アプリケーション610は、ゲートウェイサーバ606で定義されるラベルによって識別される1つの関連付けられたクライアント証明書を有してもよい。

【0087】

ゲートウェイサーバ606は、企業専用ウェブサービスとインタラクトして、クライアント証明書の発行をサポートし、関連する管理対象アプリケーションが内部PKI保護リソースへ認証することを可能にし得る。

【0088】

クライアントエージェント604及びアプリケーション管理フレームワーク614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及び使用をサポートするように増強されてもよい。様々なレベルのセキュリティ及び／または分離要件に応じるなどのために、2つ以上の証明書がサポートされてもよい。証明書は、メール及びブラウザ管理対象アプリケーション610によって、及び究極的には任意のラッピングされたアプリケーション610によって使用されてもよい（ただし、アプリケーション管理フレームワークがHTTPS要求を仲介するのが合理的な、ウェブサービス型の通信パターンをこれらのアプリケーションが使用する場合である）。

【0089】

iOSで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、公開鍵暗号標準（PKCS）12BLOB（バイナリラージオブジェクト）を各管理対象アプリケーション610のiOSキーチェーンに、各使用期間中にインポートすることに依存してもよい。アプリケーション管理フレームワークのクライアント証明書サポートは、プライベートのメモリ内キーストレージを用いたHTTPS実装を使用してもよい。クライアント証明書はiOSキーチェーンに存在しなくてもよく、強力に保護された「オンライン限定の」データ値に存在する場合を除いて、存続させなくてもよい。

【0090】

相互SSLまたはTLSも実装して、モバイルデバイス602が企業へ認証すること及びその逆を必要とすることにより、追加のセキュリティを提供してもよい。ゲートウェイサーバ606への認証用の仮想スマートカードも実装されてもよい。

【0091】

限定及びフル両方のKerberosサポートが追加機能であってもよい。フルサポート機能は、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、Active Directory（AD）622へのフルKerberosログインを行い、HTTPネゴシエート認証チャレンジに応答するためにKerberosサービスチケットを取得できることに係るものである。限定サポート機能は、Citrixアクセスゲートウェイエンタープライズエディション（AGEE）での制約付き委任に関するものであり、AGEEはKerberosプロトコル移行の呼び出しをサポートするので、HTTPネゴシエート認証チャレンジに応答してKerberosサービスチケット（制約付き委任

を条件とする)を取得して使用することができる。このメカニズムは、リバースウェブプロキシ(別名、企業仮想プライベートネットワーク(CVPN))モードで、HTTP(ただし、HTTPSではない)接続がVPN及びマイクロVPNモードでプロキシされる場合に、機能する。

【0092】

他の機能はアプリケーションコンテナのロック及びワイプに関するものでもよく、これはジェイルブレイクまたはルート化の検出時に自動的に行われ、管理コンソールからプッシュされるコマンドとして行われてもよく、管理対象アプリケーション610が稼動していない場合でも、リモートワイプ機能を含んでもよい。

【0093】

障害時にいくつかの異なる場所のうちの1つからユーザがサービスを受けられるようになる企業アプリケーションストア及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構成がサポートされてもよい。

【0094】

一部のケースでは、管理対象アプリケーション610は、API(たとえば、OpenSSL)を介した証明書及び秘密鍵へのアクセスが許可されてもよい。企業の信頼済み管理対象アプリケーション610は、アプリケーションのクライアント証明書及び秘密鍵を用いて特定の公開鍵動作を行うことが許可されてもよい。たとえば、アプリケーションがブラウザのように挙動し、証明書アクセスが必要ない場合または時、アプリケーションが「who am I」に関する証明書を読み込んだ場合または時、アプリケーションが証明書を使用してセキュアセッショントークンを構築する場合または時、及びアプリケーションが重要なデータ(たとえば、トランザクションログ)のデジタル署名のため、または一時的なデータ暗号化のために秘密鍵を使用する場合または時など、様々なユースケースが特定され、適宜対処され得る。

【0095】

スマートカードログインの例示的な実施形態

高速スマートカードログオンは、レイテンシを短縮し、セキュリティを向上させながら、スマートカードを使用してインタラクティブサーバ(たとえば、MICROSOFT仮想デスクトップインフラストラクチャ(VDI)/リモートデスクトップサービス(RDS)サーバ)などのサーバに対してユーザまたはクライアントデバイスを認証を行うために使用されてもよい。たとえば、システムは、認証に使用されるサーバデバイスとクライアントデバイスとの間の動作(たとえば、インタラクション)の回数を削減し得る。これらの動作は、スマートカードからユーザ証明書をフェッチすること、またはデータに署名することを含んでもよい。その結果、PC/SCログオンを遅くするスマートカードネットワークチャター(chatting)が低減され得る。高速スマートカードログオンはまた、任意選択でネットワークを介したPIN(または他の資格情報)の伝送を回避し、スマートカードを使用した認証イベント(たとえば、セキュアソケットレイヤ(SSL)またはトランスポートレイヤセキュリティ(TLS)認証)から、PINキャッシングに頼ることなく、実際のインタラクティブサーバへのログオンへのシングルサインオンを可能にすることにより、セキュリティを向上させ得る。

【0096】

図7に、本明細書に記載の1つまたは複数の例示的な態様によるスマートカードログオンのための例示的なシステムを示す。前述のように、図7に示すクライアントデバイス701は、同じく図7に示すサーバ721とインタラクトして、認証を行い、サーバ721がリモートアプリケーションサービスを提供するようにしてもよい。たとえば、クライアントデバイス701は、サーバ721または他のサーバ上で、リモートで実行されるアプリケーションによって生成されるアプリケーション出力を表示するために使用される仮想マシンプログラムまたはアプリケーションなどのクライアントエージェント703を含んでもよい。

【0097】

クライアントデバイス701は、アプリケーションがデータを暗号化するかまたはこれに署名するのを可能にする暗号アプリケーションプログラミングインターフェース709（C A P I）と、暗号サービスプロバイダ711（C S P）と、ミニドライバ713と、を含んでもよい。一部の実施形態では、C A P I 709、C S P 711、及びミニドライバ713は、スマートカードログオン中にクライアントデバイス701によって使用されなくてもよい。

【0098】

サーバ721は、仮想化エージェント（または仮想エージェント）723を含んでもよい。サーバ721はまた、資格情報プロバイダ725、K e r b e r o sモジュール727、C A P I 729、C S P 731、及びミニドライバ737を含んでもよい。サーバ721はこれらのコンポーネントを使用して、クライアントデバイス701を認証してもよく、及び／またはクライアントデバイス701がデータに署名するようにしてもよい。クライアントデバイス701及びサーバ721のそれぞれはまた、スマートカードの統合に使用される低レベルのパーソナルコンピュータ／スマートカード（P C／S C）レイヤ715または739を含んでもよい。スマートカード717は、図7に示すように、クライアントデバイス701に物理的に接続されてもよい。クライアントデバイス701は、追加的または代替的に、以下にさらに詳細に説明するように、仮想スマートカードを使用してもよい。

【0099】

一部の態様では、ユーザは、認証のために個人識別番号（P I N）または他の資格情報の入力をも促されてもよい。クライアントエージェント703は、P I Nをキャプチャし、任意選択でP I Nを記憶し、サーバ721の仮想エージェント723にネットワーク接続を介してP I Nを送ってもよい。サーバ721のC A P I 729は、サードパーティA P IまたはパブリックA P Iを含んでもよい。また、スマートカード認証用のドライバはサーバ側にあってもよく、これによりオペレーティングシステム間の互換性を可能にし得る。サーバ側の暗号サービスプロバイダ731は、クライアントデバイス701から受信したP I Nを記憶（たとえば、キャッシュ）してもよい。認証プロセス中に、サーバ721は、P C／S Cレイヤ739を介してクライアントデバイス701にP I Nを送り返して、クライアントデバイス701のスマートカード717から1つまたは複数の証明書などの資格情報を取得するようにしてもよい。P C／S Cレイヤ715及び739でのスマートカードインタラクションの間に、クライアントデバイス701及びサーバ721は、数百回、たとえば、約500回の往復の要求でインタラクトし得る。高速スマートカードログインのための第2の方法は、以下に説明するように、たとえば、1回、2回、または3回のインタラクションなど、スマートカード認証中にクライアントデバイス701及びサーバ721がインタラクトする回数を低減し得る。

【0100】

図8に、本明細書に記載の1つまたは複数の例示的な態様による高速スマートカードログオンのための例示的なシステムを示す。高速スマートカードログオンは、P C／S Cレベル815及び839ではなく、より高い通信レベルでのクライアントデバイス801及びサーバ821間のインタラクション（たとえば、クライアント証明書によるドメインログオン）を含んでもよい。これにより、クライアントデバイス801及びサーバ821間のインタラクションの回数、及び／またはクライアントデバイス801及びサーバ821間で交換されるデータの量（たとえば、ボリューム）が減少し得る。

【0101】

図7に関して前述したように、クライアントデバイスは、クライアントエージェント803、C A P I 809、C S P 811（たとえば、図8に示すC S P 2）、ミニドライバ813、及びP C／S C 815を含んでもよい。しかしながら、クライアントデバイスは、サーバのC A P I 829、C S P 831、及びミニドライバ837に頼るのではなく、自身のC A P I 809、C S P 2 811、及びミニドライバ813をスマートカード認証に使用してもよい。スマートカード817もまた、これはバイオメトリックスマートカ

ード（または他の任意のスマートカード）であってもよいが、クライアントデバイス 8 0 1 に物理的に接続されてもよい。スマートカード 8 1 7 は、証明書などの資格情報を記憶してもよい。

【0102】

クライアントエージェント 8 0 3 は、仮想エージェント 8 2 3 へのディスプレイリモータリング接続を介して、サーバ 8 2 1 の仮想エージェント 8 2 3 とのネゴシエーションセッションを確立する。ネゴシエーションセッション中に、サーバ 8 2 1（たとえば、サーバ 8 2 1 の仮想エージェント 8 2 3）は、従来のスマートカードログオンまたは高速スマートカードログオンのいずれを実行するかを決定してもよい。上記のように、高速スマートカードログオンは、サーバ 8 2 1 とクライアントデバイス 8 0 1 との間のより少数のインタラク션을必要とし得る。クライアントデバイス 8 0 1 及びサーバ 8 2 1 は、ネゴシエーションセッション中に互いに自身の機能を知らせてもよい。

10

【0103】

仮想エージェント 8 2 3 はまた、クライアントエージェント 8 0 3 が仮想エージェント 8 2 3 に自動ログオン資格情報を提供したか否かを判定してもよい。ブローカリングステップ中に、クライアントデバイス 8 0 1 は、他の（たとえば、認証）サーバと認証している場合があり、ユーザはパスワード、PIN、バイオメトリクス、または他の資格情報を提供している場合がある。スマートカード 8 1 7 は、ブローカリングステップ中に使用されている場合があり、最初のサーバとの認証が成功した場合、スマートカード 8 1 7 がロック解除されている場合がある。ブローカリングステップ及びスマートカードロック解除ステップは、クライアントエージェント 8 0 3 と仮想エージェント 8 2 3 との間のネゴシエーションセッションの前に行われてもよく、またはクライアントエージェント 8 0 3 と仮想エージェント 8 2 3 との間のネゴシエーションセッション中に行われてもよい。したがって、仮想エージェント 8 2 3 は、自動ログオン資格情報がクライアントエージェント 8 0 3 によって提供されたと、ネゴシエーションセッション中に判定し得る。一部の態様では、自動ログオン資格情報が提供された場合など、クライアントにおける将来の PIN（または他の資格情報）プロンプトが有益にブロックされ得る場合、仮想エージェント 8 2 3 は、高速スマートカードログオンを使用することを決定してもよい。それ以外の場合、仮想エージェント 8 2 3 は、従来のスマートカードログオン（たとえば、PC/SC レイヤを介したスマートカード認証）を使用することを決定してもよい。

20

30

【0104】

サーバ 8 2 1 は、どのログオン方式を使用するかを決定するために 1 つまたは複数の他の要因を考慮してもよい。たとえば、サーバ 8 2 1 は、クライアントデバイス 8 0 1 が高速スマートカードログオン（たとえば、スマートカード認証）を使用することを好むことを（たとえば、ネゴシエーションセッション中に）クライアントデバイス 8 0 1 が指示している場合、高速スマートカードログオンを使用することを決定してもよい。サーバ 8 2 1 はまた、それが高速スマートカードログオンを行うことが可能であるか否かを判定してもよい。一部の態様では、サーバ 8 2 1 は、PIN のユーザプロンプトの回数に基づいて、高速スマートカードログオンを実行するか否かを決定してもよい。たとえば、サーバ 8 2 1 は、1 回またはより少ない回数のユーザ PIN プロンプトが発生する場合（たとえば、ブローカリングステップ中に 1 回、またはブローカリングステップ及びネゴシエーションステップ中に 1 回）、高速スマートカードログオンを使用することを決定してもよい。PIN プロンプトの他の任意の閾値回数が使用されてもよい。それ以外の場合、サーバ 8 2 1 は、高速スマートカードログオン方式を使用しないことを決定してもよい。

40

【0105】

ユーザが PIN または他の資格情報（たとえば、バイオメトリック）を提供した後、クライアントデバイス 8 0 1 の CSP 8 1 1 は、PIN、バイオメトリック、または他の資格情報を記憶（たとえば、キャッシュ）するか、または別の方法でスマートカードをロック解除されたままにして、クライアントデバイス 8 0 1 がさらに使用できるようにしてもよい。CSP 2 8 1 1 に PIN またはバイオメトリックを記憶することにより、図 7 に

50

示すように、サーバ821のCSP831がスマートカード817と通信して証明書を取得するのではなく、クライアントデバイス801がスマートカード817と直接通信して、セキュリティ証明書を取得し得る。したがって、PINまたはバイオメトリックは、セキュア化されているかまたはされていない場合があるネットワークを介してクライアントデバイス801とサーバ821との間で（時には複数回）伝送されるのではなく、クライアントデバイス801上に残り得る。代替的な実施形態では、クライアントエージェント803は、PINまたはバイオメトリックをサーバ821に送ってもよい。サーバ821は、以下にさらに詳細に説明するように、CSP833などにPINまたはバイオメトリックを記憶してもよい。バイオメトリクス（たとえば、指紋）の例では、指紋または他のバイオメトリクスに使用されるデータが多いので、スマートカード認証は（他のスマートカード認証方式と比べて）大幅に高速化され得る。

10

【0106】

クライアントデバイス801はまた、スマートカード817を用いるなどして証明書動作を処理するように構成される秘密鍵動作（PK動作）SDKモジュール807を含んでもよい。PK動作SDK807の機能は、同時係属中の米国非仮特許出願第13／886,845号に記載されており、その全体が引用により本明細書に組み込まれている。具体的には、クライアントデバイス801のPK動作SDKモジュール807は、鍵ストアへのアクセスを容易にし得て、この鍵ストアは、認証用の署名に使用され得る対応する秘密鍵と共に、1つまたは複数のクライアント証明書を記憶する。たとえば、クライアントデバイス801は、クライアントデバイス801のユーザを表すクライアント証明書へのアクセスを許可してもよく、またはそれを所持してもよい。一部の態様では、証明書は、企業が発行した証明書であってもよい。証明書は、暗号モジュールを有する物理スマートカードにバインドされてもよい。換言すれば、暗号秘密は、スマートカードにとどめられてもよい。ユーザはクライアントデバイス801がスマートカードで保護された証明書にアクセスすることを許可してもよい。

20

【0107】

代替的には、証明書は派生資格情報（たとえば、仮想スマートカード）にバインドされてもよく、これはハードウェア及び／またはソフトウェアモジュールを使用して鍵を保護してもよい。派生資格情報内の証明書は、クライアントデバイス801に記憶されてもよく、物理スマートカード817上の証明書と同様にアクセスされてもよい。派生資格情報からの証明書は、クライアントデバイス801における信頼済みの環境に記憶されてもよい。

30

【0108】

クライアントデバイス801及び／またはクライアントデバイスの取り外し可能なハードウェアモジュールは、証明書及び秘密鍵を記憶することを、プロビジョニングプロセスによって許可されてもよい。クライアント証明書の秘密鍵を必要とする動作を許可するために、ユーザは、クライアントデバイス801を使用してPINまたは他の資格情報（たとえば、バイオメトリック）を入力するように要求され得る。クライアントデバイス801（たとえば、スマートフォン）とは別の他の外部デバイスが証明書を管理してもよく、クライアントデバイス801は、カスタムリーダーインターフェースを利用して、外部デバイスによって管理される証明書にアクセスしてもよい。

40

【0109】

ここでサーバ821に着目すると、サーバ821は、図7に関して上記に前述したように、仮想エージェント823及びCAPI829を含んでもよい。サーバ821はCSP831を含んでもよいが、CSP831をスマートカード認証に利用しなくてもよい。むしろ、クライアント側CSP811が代わりに利用されてもよい。サーバ821はまた、スマートカードログオンを開始するように構成される資格情報プロバイダ825（または資格情報プロバイダフィルタ）を含む1つまたは複数の資格情報プロバイダを含んでもよい。仮想エージェント823は、高速スマートカードログオンに使用する資格情報プロバイダ、たとえば、資格情報プロバイダ825を選択してもよい。Kerberos認証が

50

利用される場合、資格情報プロバイダ 825 は、以下の例でさらに詳細に説明するように、信頼済みのサードパーティデバイス 827（たとえば、Kerberos モジュール）と通信してもよい。

【0110】

サーバ 821 は、暗号サービスプロバイダ CSP 831、及び／または（任意選択で）図示していないキーストレージプロバイダ（KSP）を含んでもよい。換言すれば、CSP 831 は、KSP に置き換えられてもよい。KSP は、CSP 831 によってサポートされていない場合がある代替的なスマートカードのアルゴリズムをサポートするために使用されてもよい。同様に、クライアントデバイス 801 の CSP 811 は、KSP に置き換えられてもよい。CSP（及び／または KSP）は、証明書動作をインターセプトするように構成されてもよい。資格情報プロバイダ 825 は、高速スマートカードログオンに使用する CSP、たとえば CSP 831 を選択してもよい。サーバ 821 の CSP 831（及び／または KSP）は、リモートチャネル 836 を介してクライアントデバイス 801 の PK 動作 SDK 807 と通信してもよい。たとえば、クライアントデバイス 801 とサーバ 821 との間の仮想チャネル 836 は、クライアントデバイス 801 の仮想チャネルドライバ 805 と、サーバ 821 の仮想チャネルドライバ 835 とによって確立されてもよい。

10

【0111】

クライアントデバイス 801 を使用する動作、たとえば、スマートカード 817 からの証明書の要求、またはデータ署名の要求などは、サーバ 821 の CSP 831（及び／または KSP）からクライアントデバイス 801 の PK 動作 SDK 807 に（たとえば、仮想チャネル 836 を介して）送られてもよい。より高いレベルで（たとえば、PC/SC トンネル 838 ではなく仮想チャネル 836 を介して）通信することにより、図 8 に示すサーバ及びクライアントデバイスのペアは、図 7 に示すサーバ及びクライアントデバイスのペアよりも少ない回数で、及び／または少ない情報を相互に通信し、それによって潜在的なレイテンシが短縮され得る。

20

【0112】

サーバ 821 はまた、クライアントデバイス 801（またはスマートカード 817）との通信を必要としないサーバ側の認証動作のための、サードパーティ CSP などの CSP 833 を含んでもよい。前述のように、サーバ 821 はまた、ミニドライバ 837 及び PC/SC フック 839 を含んでもよい。一部の態様では、ミニドライバ 837 及び PC/SC 839 は、クライアントデバイスの認証に使用されなくてもよい。他の態様では、PC/SC 839 は、他の仮想チャネル 838 を介してクライアントデバイス 801 の PC/SC 815 と通信してもよい。

30

【0113】

ここで、Kerberos によるスマートカード 817 を使用した認証のための一般的な動作についてさらに詳細に説明する。サーバの資格情報プロバイダ 825 は、KERB__CERTIFICATE__LOGON 構造体を使用して、スマートカードクラスユーザ証明書を用了 Active Directory ログオンなどのログオンをトリガしてもよい。サーバの資格情報プロバイダ 825 は KERB__CERTIFICATE__LOGON 構造体を使用して、KERB__CERTIFICATE__LOGON 構造体は、次のように構成されてもよい。

40

【0114】

【数 1】

```
typedef struct _KERB_CERTIFICATE_LOGON {
    KERB_LOGON_SUBMIT_TYPE MessageType;
    UNICODE_STRING      DomainName;
    UNICODE_STRING      UserName;
    UNICODE_STRING      Pin;
    ULONG               Flags;
    ULONG               CspDataLength;
    PCHAR               CspData;
} KERB_CERTIFICATE_LOGON, *PKERB_CERTIFICATE_LOGON;
```

【0115】

さらに、KERB_CERTIFICATE_LOGON構造体に記述されているように、「CspData」は、KERB_SMARTCARD_CSP_INFO構造体へのポインタをコンプロマイズし得る。KERB_SMARTCARD_CSP_INFO構造体は、次のように構成されてもよい。

【0116】

【数 2】

```
typedef struct _KERB_SMARTCARD_CSP_INFO {
    DWORD dwCspInfoLen;
    DWORD MessageType;
    union { PVOID ContextInformation; ULONG64 SpaceHolderForWow64; };
    DWORD flags;
    DWORD KeySpec;
    ULONG nCardNameOffset;
    ULONG nReaderNameOffset;
    ULONG nContainerNameOffset;
    ULONG nCSPNameOffset;
    TCHAR bBuffer;
} KERB_SMARTCARD_CSP_INFO, *PKERB_SMARTCARD_CSP_INFO;
```

(一部/全部?の) PKINIT暗号
動作に使用するCSPの名前

【0117】

この構造体は、サーバの資格情報プロバイダ825によって生成されてもよい。特に、この構造体は、CSP831及び／またはKSPの名前などを識別してもよい。

【0118】

引用により本明細書に組み込まれている米国特許出願第13／886, 845号にさらに詳細に説明されているように、Kerberosリソース認証は、KerberosのKDC（たとえば、Active Directoryドメインコントローラ）からサービスチケットを取得することを必要としてもよい。たとえば、サーバ821におけるKerberos認証パッケージは、Active Directoryログオンを実行するために、コメント要求（RFC）4556に記載されたようなKerberosにおける初期認証用公開鍵暗号（PKINIT）プロトコルを使用してもよい。

【0119】

サーバの資格情報プロバイダ825、Kerberosモジュール827、またはスマートカードを使用する他のアプリケーションによる情報の処理中に、サーバ821側のCSP831及び／またはKSPは、資格情報プロバイダ825及びKerberosモジュール827によって行われる関連する証明書動作をインターセプトし、それらの動作をクライアントデバイス801（たとえば、クライアントデバイス801のPK動作SDK807）にリモーティングしてもよい。たとえば、CSP831及び／またはKSPが証明書要求またはデータ署名動作を検出した場合、CSP831及び／またはKSPは、認証データをパッケージ化し、証明書及び／または署名の要求をクライアントデバイス801に送ってもよい。それ以外の場合、クライアント情報を使用しない動作は一般に、クライアントデバイス801に関与せずに、（たとえば、サードパーティCSP833を介して）サーバ821で行われてもよく、それによって、クライアントデバイス801及びサーバ821の間で交換されるデータの量と、クライアントデバイス801及びサーバ82

10

20

30

40

50

1がインタラクトする回数とを減少し得る。クライアントデバイス801にリモーティングされる例示的な動作には、スマートカード817上の証明書をリスト化（たとえば、列挙）する要求、証明書の要求、スマートカード817の秘密鍵を使用した署名動作、及びスマートカード817の秘密鍵を使用した復号動作が含まれるが、これらに限定されない。クライアントデバイス801に送られなくてもよい（たとえば、リモーティングされなくてもよい）例示的な動作（たとえば、サードパーティCSP833によって、あるいはサーバ821で行われてもよい）には、コンテキスト及びハンドル管理、パラメータ収集及びハンドリング、乱数生成、対称鍵生成及び導出、バルク暗号化及び復号、メッセージダイジェストを生成するためのデータのハッシング、セッション鍵のラッピング、署名検証、及び他の特定の動作が含まれるが、これらに限定されない。

10

【0120】

CSP831及び／またはKSPはまた、クライアント801がデータに署名するかもしれない又はこれを復号するために、またはクライアント801に關与する他の任意の動作のために、証明書の要求と共にクライアントデバイス801にPKINITコンテキスト情報などのコンテキスト情報を供給してもよい。コンテキスト情報の供給については、米国特許出願第13／886,845号にさらに詳細に説明されており、その全体が引用により本明細書に組み込まれている。コンテキスト情報を供給することにより、（仮想チャネルドライバ805及び835を介して確立された）サーバ821とクライアントデバイス801との間のリモーティングチャネル836の誤用から保護され得る。

20

【0121】

ここで、例示的な署名動作について説明する。Kerberosモジュール827は、ログオン中にCSP831の呼び出しを行って、たとえば、クライアントデバイスの署名が望まれていることを示してもよい。たとえば、米国特許出願第13／886,845号にさらに詳細に説明されているように、Kerberosモジュール827は、PKINIT中に署名すべきAuthPackに署名する呼び出しを行ってもよい。

【0122】

【数3】

CryptCreateHash	}	署名の生成の一部としての
CryptHashData		PKINIT AuthPack 構造の
CryptGetHashParam		ハッシュの計算
CryptSignHash	}	秘密鍵を用いた AuthPack の実際の署名

30

【0123】

スマートカード817の秘密鍵は、クライアントデバイス801によってAuthPack構造に署名するために使用されてもよい。署名は、RFC5652に記載されている暗号メッセージ構文（CMS）を使用して行われてもよい。特に、RFC5652に記載されているように、AuthPackはSignedDataエンベロープ内に配置されてもよい。したがって、署名動作はCSPレベルで認識可能であり得、その理由は、ハッシュ関数呼び出しに渡される生データが、整形された（well-formed）ASN.1構造を有し得るためであり、これはRFC4556及び5652で定義されており、また、米国特許出願第13／886,845号でさらに詳細に議論されており、その議論は引用により本明細書に組み込まれている。一部の態様では、クライアントデバイス801にリモーティングされる動作（たとえば、署名及び復号）は、プロトコルコンテキスト（たとえば、ASN.1または他の認識可能な構造）を示さなくてもよい。したがって、これらの動作は、これらの動作を生じさせるプロトコルコンテキストの証明を提供することなく、提供され得る。

40

【0124】

上記で説明したように、クライアントデバイス801は、認証プロセス中にサーバ821から1つまたは複数の要求を受信してもよい。クライアントデバイス801上のプロセ

50

スは、1つまたは複数のプロセス間通信（IPC）メカニズムを介して通信してもよい。また、各プロセスは他のどのプロセスが最初のプロセスを呼び出しているかを特定してもよく、これを使用して、認証中の余分なPINプロンプト（または他の資格情報プロンプト）を防ぐか否かを決定してもよい。あるプロセスが既にスマートカード817をロック解除している場合、1つまたは複数のその後のPINプロンプトをブロックして、ユーザが再度PINを提供する必要がないようにしてもよい。しかしながら、どのプロセスもスマートカード817を使用していない場合、ユーザはPINの入力を促されてもよい。クライアントエージェント803は、論理的には（ユーザの観点から）1つのアプリケーションで構成されていても良いが、複数のプロセスで構成されてもよい。それらのプロセスの1つは、ブローカリング中の以前の認証のために、スマートカードの使用を許可される場合があり（また、その他は許可されない場合があり）、そのため、クライアントデバイス801は、これらの追加のスマートカード動作を、クライアントエージェントのログオンステップから最初のプロセスに戻るように経路指定して、これ以上のPINプロンプトを回避してもよい。

10

【0125】

一方、さらなるPINプロンプトが一部の状況で発生する場合がある。クライアントデバイス801が再びユーザにユーザのPIN（または他の資格情報）の入力を促すか否かは、どのプロセスがスマートカードのPINを呼び出しているかに依存してもよい。一部の態様では、ユーザが、スマートカードを使用したい各アプリケーションを許可してもよい。これは、ロック解除されたスマートカードが、PINプロンプトを発生させてユーザ許可を取得した最初のプロセスとは目的が異なり得る他のプロセスには必ずしも使用可能ではなくなるように、オペレーティングシステム及びCSPによって実装されてもよい。一部のケースでは、スマートカード自体が、PINプロンプトを強制する内部ポリシーを有してもよい。

20

【0126】

一部の態様では、前述の認証方法は、CSP（たとえば、CSP831）及び／またはKSP上で実装されてもよい。CSPまたはKSPが使用される場合、ハッシュ関数を使用されなくてもよい。一般に、CSP関数の多くは、CpSignHash及びCpDecryptなどのクライアントデバイス801を使用する動作以外は、標準的なCSP（たとえば、サードパーティCSP833）に委任され得る。一部の実施形態では、Kerberosモジュール827がユーザ証明書もフェッチしてAS-REQパケットに入れる場合、Kerberosモジュール827は、CryptGetKeyParamを呼び出してユーザ証明書を読み込んでもよい。それに応じて、CryptGetKeyParamは、クライアントデバイス801にユーザ証明書を要求するようにCSP831をトリガしてもよい。

30

【0127】

クライアントデバイス801にリモートイングされる動作（たとえば、1つ、2つ、3つ、または4つの動作）を行った後、Kerberosシステム827は、ドメインコントローラへのその認証を完了させて、基本的なオペレーティングシステムのログオンを完了してもよい。

40

【0128】

サーバ821は、スマートカードの取り外しポリシーをサポートしてもよい。一部の態様では、クライアント側のPC/SC815とサーバ側のPC/SC839との間に他の仮想チャネル838が存在してもよい。サーバ821は、この仮想チャネル838を使用してスマートカードレイヤを見ることができるので、スマートカード817が取り外されたときを特定することができる。この例では、資格情報プロバイダ825は、正しいスマートカードリーダー名がKERB_SMARTCARD_CSP_INFOなどのデータフィールドにリストされていることを確認して、それがPC/SC仮想チャネル838によって公開されている情報と一致するようにしてもよい。他の態様では、PC/SC仮想チャネル838は、使用されなくてもよい。その代わりに、サーバ821が、サーバ側のC

50

S P 8 3 1とクライアント側のP K動作8 0 7との間の仮想チャネル8 3 6を使用して、スマートカード8 1 7のステータスを特定してもよい。たとえば、クライアントデバイス8 0 1がスマートカード8 1 7のステータスを特定してもよく、ステータスはP K動作8 0 7によって仮想チャネル8 3 6を介してC S P 8 3 1に送られてもよい。サーバ8 2 1は、スマートカード8 1 7のステータスをエミュレートする仮想スマートカードリーダー（図示せず）を生成して記憶してもよい。サーバ8 2 1は、サーバ8 2 1における仮想スマートカードリーダーのステータスを特定することによって、スマートカード8 1 7のステータスを特定してもよい。サーバ8 2 1は、スマートカードが取り外されたと判定した後に、様々なアクションを実行してもよい。たとえば、サーバ8 2 1は、ユーザが自身のアクセス端末から離れた場合に、セッションをロックして、それをセキュアなままにしてもよい。これにより、ユーザは自身のカードを携行する以外に何もする必要がなくなり得る。

10

【0 1 2 9】

図9に、本明細書に記載の1つまたは複数の例示的な態様による高速スマートカードログオンのための他の例示的なシステムを示す。図9に示すシステムは、図8に示すシステムの拡張を含み、補助的なサードパーティ（たとえば、ベンダー）C S P関数をサポートしてもよい。図8に示すコンポーネントに加えて、図9の例におけるサーバ8 2 1は、サードパーティC S PであるC S P 9 3 2を含んでもよい。一部の態様では、C S P 9 3 2は図7に示すC S P 7 3 1であってもよい。両方のC S PはユーザのP I Nまたはバイオメトリックを記憶してもよい。この例では、クライアントデバイス8 0 1は、P I N（または他の資格情報）をサーバ8 2 1に送ってもよい。P I N（または他の資格情報）は、たとえば、D i f f i e - H e l m a nなどの、クライアントデバイス8 0 1とサーバ8 2 1との間の鍵ネゴシエーションにより、伝送中に保護されてもよい。鍵ネゴシエーションは、T L Sなどの任意の下位レベルの転送セキュリティメカニズムに加えて、P K動作の仮想チャネル内で行われてもよい。P I N（または他の資格情報）を受信すると、C S P 9 3 2はP I Nを記憶（たとえば、キャッシュ）してもよい。P I Nを記憶することにより、C S P 9 3 2は、ログオン後のアプリケーション使用（たとえば、インタラクティブサーバセッションで稼働中のアプリケーション及び／または他の同様の機能のためのもの）のために、スマートカード8 1 7をロック解除してもよい。仮想セッション内の例示的なアプリケーションには、ウェブブラウザ、生産性ソフトウェア、電子メールクライアントなどが含まれてもよい。また、C S P 9 3 2はログオン中に直接使用されていない場合があるので、C S P 9 3 2へのP I Nの記憶は、ログオンパフォーマンス（たとえば、速度、レイテンシ、セキュリティなど）にほとんどまたは全く影響を与えない場合がある。C S P 9 3 2へのP I Nの記憶は、インタラクティブサーバセッションで稼働するアプリケーションへのシングルサインオンに使用されてもよい。たとえば、アプリケーションは、C S P 9 3 2からP I Nに直接アクセスして、ユーザをサインオンさせてもよい。

20

30

【0 1 3 0】

一部の実施形態では、インタラクティブサーバセッションで稼働するアプリケーション、たとえば、ウェブブラウザ、文書への署名を利用するアプリケーション、または他のアプリケーションは、ログオンのためにスマートカード資格情報にアクセスしてもよい。本明細書に記載の動作は、スマートカード資格情報にアクセスするアプリケーションのために使用されてもよい。これらの例では、サーバ側のK e r b e r o sコンポーネント8 2 7は、スマートカードへのアクセスを要求するアプリケーションに置き換えられてもよく、スマートカード資格情報にアクセスするための動作は上記のように行われてもよい。また、仮想チャネル8 3 6を使用して得られたユーザ証明書は、ユーザセッション用の証明書ストア、たとえば、W I N D O W S（登録商標）または他のO Sの証明書ストアに伝達されてもよい。O Sはこの動作を通常のスマートカードログオンのために、P C / S CのA P Iを使用するバックグラウンドプロセスとして実行してもよい。それに応じて、証明書は、カード用の通常のC S P（たとえば、図9に示すC S P 9 3 2）ではなく、C S P 8 3 1にリンクされてもよい。

40

【0 1 3 1】

50

サーバ側のK e r b e r o sコンポーネント827が、スマートカードへのアクセスを要求するアプリケーションに置き換えられる場合、C S P 8 3 1（及びP K動作S D K、ならびに他のコンポーネント）は、アプリケーションごとのユーザ許可が所望されるならば、サーバ側の異なるアプリケーション間を区別し得る。異なるサーバ側アプリケーションがカードの使用を試みる場合があるので、P I Nプロンプトが自動的に行われないうちがあり、秘密鍵動作は、既に許可されているクライアント側のプロセスに戻り得る。そのため、C S P 8 3 1は、サーバ821によって使用されるP I Nプロンプトポリシーを示してもよく、それにより秘密鍵動作はクライアント801によって実行され得る。一部のケースでは、これは、サーバ側のC A P I 829によりサポートされるスマートカード動作の概念を公開して、クライアント801上のC A P I 809に動作をミラーリングできるようにすることによって行われ得る。

10

【0132】

一部の実施形態では、スマートカードはまだロック解除されていない場合があり、インタラクティブなP I Nプロンプトが使用されてもよい。これらの実施形態では、P I Nプロンプトは、クライアント801ではなく、サーバ821によって処理されてもよい。サーバ821上でのP I Nの収集は、クライアント801上でのP I Nの収集よりも安全でない場合がある。しかしながら、この場合にはサーバでの実装がより容易であり得、その理由は、コアセキュリティシステム（たとえば、W I N D O W S（登録商標）上のL S A）が、ユーザの入力を待つ際に、本来ブロックされ得るときに、ブロックされない場合があるためである。上述のような（P C / S Cではなく）P K動作のリモートリングの速度上の利益は、これらの実施形態において存在し得る。簡単な例として、このモードは、スマートカードの取り外しによってロックがかかったが、セッションは切断されなかった場合に、リモートセッションをロック解除するために使用されてもよい。ユーザがスマートカードを再挿入した場合、スマートカードの挿入が（たとえば、P C / S CまたはP K動作の仮想チャネルを介して）信号伝達されてもよく、ユーザはP I Nを入力してカードをロック解除するように促されてもよい。

20

【0133】

図10に、本明細書に記載の1つまたは複数の例示的な態様による高速スマートカードログオンのためのさらに他の例示的なシステムを示す。クライアントデバイス1001は、前述のように、クライアントエージェント1003を含んでもよい。クライアントデバイス1001は、1つまたは複数の仮想チャネル1005を介してサーバ1021と通信してもよい。クライアントデバイス1001はまた、認証マネージャ1008を含んでもよく、これは、図8を参照して前述したクライアントデバイスのC A P I、C S P 2、及び／またはミニドライバモジュールのうちの1つまたは複数を含んでもよい。認証マネージャ1008は、図7及び図8に示す（そして前述した）P K動作S D Kを実装するクライアントエージェント1003内のモジュールであってもよい。クライアントデバイスのオペレーティングシステムに応じて、認証マネージャ1008は、オペレーティングシステム提供のC A P Iを使用してもよく、独自のC A P Iを含んでもよい。認証マネージャ1008は、スマートカード1017及び／またはシングルサインオンデバイス1019、たとえば、セキュアなP I Nキャッシングサービス及び／またはデバイスと通信してもよい。認証マネージャ1008は、認証中にユーザによって提供されたP I Nまたは他の資格情報を記憶してもよい。高速スマートカードログオンは、クライアントデバイス1001が認証マネージャと通信して新たな認証向けのスマートカード証明書サービスにアクセスするための新たなI P Cチャネルに依存してもよい。

30

40

【0134】

サーバ1021はブローカーエージェントサービス1035を含んでもよく、これはクライアントデバイス1001とサーバ1021との間の仮想チャネル1005とインターフェースしてもよい。たとえば、ブローカーエージェントサービス1035は、図8に示す仮想チャネルドライバ835を含んでもよい。ブローカーエージェントサービス1035は、認証を容易にし得る。サーバ1021は、図8を参照して前述したように、暗号サ

50

ービスプロバイダCSP1031及び資格情報プロバイダ1025（たとえば、証明書資格情報プロバイダ）を含んでもよい。サーバ1021はまた、資格情報プロバイダマネージャ1024を含んでもよく、これは前述の仮想エージェント823を含んでもよい。資格情報プロバイダマネージャ1024は、認証のためにスマートカードログイン（たとえば、図7に示す実施形態）または高速スマートカードログイン（たとえば、図8に示す実施形態）のいずれを使用するかを決定するために使用されてもよい。

【0135】

ここで、図10に示すコンポーネントによって実施され得る認証ステップについて説明する。まず、クライアントデバイス1001とサーバ1021との間の仮想チャンネル1005が確立されてもよい。クライアントデバイス1001は、たとえばクライアントエー 10
ジェント1003を介して、サーバ1021と、たとえば資格情報プロバイダマネージャ1024を介してネゴシエートして、使用する資格情報プロバイダ1025を決定してもよい。一部の例では、サーバ1021は、複数の資格情報プロバイダ1025を有してもよく、及び／または、そうでなければ、複数の資格情報プロバイダとインタラクトしてもよい。また、クライアントエージェント1003は、資格情報プロバイダマネージャ1024とネゴシエートして、スマートカードログインまたは高速スマートカードログインのいずれを使用するかを決定してもよい。クライアントエージェント1003は、クライアントデバイス1001がスマートカードまたは他の資格情報を使用した認証を希望していることをサーバ1021に通知してもよい。

【0136】

高速スマートカードログインを使用（たとえば、有効化）すべきことをサーバ1021の資格情報プロバイダマネージャ1024が検出した場合、資格情報プロバイダ1025がトリガされてもよい。換言すれば、資格情報プロバイダマネージャ1024は、特定の資格情報プロバイダ1025にスマートカードログイン手順を実行するように通知してもよい。このトリガは、CSP1031で見つかった証明書を使用して認証するようにドメインログインプロセス（たとえば、WinLogon.exe）に通知してもよい。CSP1031は、証明書の取得及び署名動作などのクライアントデバイス1001に關与する動作をクライアント1001に指示しつつ、サーバ1021上でローカルに他の暗号関数を実行してもよい。図8を参照して前述したように、資格情報プロバイダ1025は、 30
認証のためにKerberosモジュールと通信してもよい。資格情報プロバイダ1025とKerberosモジュールとの間での動作中に、CSP1031は、証明書動作及び／または署名動作（またはクライアントデバイス1001に記憶された情報を使用する他の動作）を実行するために呼び出されてもよい。CSP1031は、所望のクライアントまたはユーザ情報を取得するために、サーバ側のブローカーエージェントサービス1035及びクライアント側の仮想チャンネル1005を介して、クライアントデバイス1001の認証マネージャ1008と通信してもよい。

【0137】

クライアントデバイス1001が情報の要求を受信した後、証明書の選択及びPINの要求を含むユーザインターフェースのインタラクションは、クライアントデバイス1001上の認証マネージャサービス1008によって処理されてもよい。スマートカードログインが有効化されている場合、既存のスマートカードの仮想チャンネル（たとえば、PC/SC）ではなく、（前述のような）仮想チャンネルが使用されてもよい。一部の態様では、クライアントデバイス1001は、サーバ1021によって要求された動作を実行するために、（たとえば、証明書の選択、PINまたはバイオメトリックの入力などのために）インタラクティブにユーザに入力を促してもよい。たとえば、ユーザインタラクションステップは、資格情報プロバイダがトリガされる前に、クライアントエージェント接続中の初期に行われてもよい。

【0138】

以下の動作またはコマンドは、スマートカードログインまたは高速スマートカードログインの間で選択するために使用されてもよい。

10

20

30

40

50

【0139】

【表1】

ポリシー識別子	説明
POLICY_VIRTUAL_CHANNEL_DISABLED	管理者は高速スマートカード認証仮想チャネル（クライアントまたはサーバ端）を明示的に無効化している
ICAFILE_DISABLE_CTRL_ALT_DEL	これを真に設定することで、個別のクライアントエージェントファイルは、スマートカードログオンが接続に使用されるべきであることを示す
POLICY_SMARTCARD_DISABLED	古いスマートカード仮想チャネルを無効化することは、高速スマートカード仮想チャネルを無効化することには「ならない」
POLICY_USE_LOCAL_USER_AND_PASSWORD	PINパススルーを無効化すると、VDAへの認証時に（すなわち、認証マネージャを使用して以前にロック解除している場合に）スマートカードPINの入力をユーザに強制しなくなる

10

20

【0140】

ログオンシーケンスにおけるステップは、クライアントデバイス1001上の認証マネージャサービス1008によって制御されてもよく、これは、グラフィカルユーザインターフェース（GUI）を介して情報を入力するようにユーザに促すか否かを決定してもよい。起動時に、クライアントエージェント1003は仮想チャネルをロードしてもよく、これは高速スマートカード仮想チャネルを有効化するか否かの決定に進み得る。POLICY_VIRTUAL_CHANNEL_DISABLEDが偽であり、ICAFILE_DISABLE_CTRL_ALT_DELが真であり、認証マネージャサービスのIsCertificateLogonEnabled（）が真である場合に、高速スマートカード仮想チャネルが有効化されてもよい。POLICY_VIRTUAL_CHANNEL_DISABLEDが偽であり、スマートカードデバイスが検出された場合に、IsCertificateLogonEnabled（）は真になり得る。

30

【0141】

サーバ1021の資格情報プロバイダマネージャ1024はまた、アクティブ化ステップを実行してもよい。たとえば、ICAFILE_DISABLE_CTRL_ALT_DELが真である場合、資格情報プロバイダマネージャ1024は、スマートカードログオンを試みてもよい。この時点で、資格情報プロバイダマネージャ1024は、POLICY_VIRTUAL_CHANNEL_DISABLEDが偽であり、仮想チャネルがクライアントデバイス1001によって有効化されており、資格情報プロバイダマネージャ1024が仮想チャネルのGetCertificate（）の呼び出しを介して（たとえば、クライアントデバイス1001が証明書を取得するため）ログオン証明書を取得することができる場合に、高速スマートカード認証仮想チャネルの使用を試みてもよい。それ以外の場合、（高速スマートカードログオンではなく、スマートカードログオンを有効化するために）既存のスマートカード仮想チャネルがアクティブ化されてもよい。

40

【0142】

クライアントデバイスコンポーネントは、GetCertificate（）の呼び出しに応答してもよい。仮想チャネルが有効化されていたと仮定すると、GetCertificate（）要求は、サーバ1021からクライアントデバイスの認証マネージャサービス1008に直接渡されてもよい。認証マネージャサービス1008は、POLICY_VIRTUAL_CHANNEL_DISABLEDが偽であり、スマートカードデ

50

バイスが存在し、証明書が適切なフォーマットを有する（たとえば、証明書のタイプについてのポリシーを満たす）ことを検証した後、サーバ1021に証明書を返してもよい。必要であれば、スマートカードが検出されなかった場合、及び／または適切なフォーマットの複数の利用可能な証明書が存在する場合、認証マネージャサービス1008は、ユーザにスマートカード1017を挿入するか、または証明書を選択するように促してもよい。

【0143】

サーバ1021の資格情報プロバイダ1025及びCSP1031は、様々なステップを実行してもよい。資格情報プロバイダマネージャ1024は、証明書を受信した場合、資格情報プロバイダ1025を起動し、暗号学的にランダムなCSPアクセスチケットを資格情報プロバイダ1025に送ってもよい。CSP1031は、ブローカーエージェントサービス1035のローカル認証サービスによって提供される証明書機能を使用してインタラクティブログオンを行ってもよい。たとえば、ローカル認証サービス1035は、SignHash（）または他の動作を実行するために仮想チャネルを使用する前に、CSPの呼び出し元がアクセスチケットを知っていたことを検証してもよい。

【0144】

クライアントデバイスコンポーネントは、SignHash（）動作に応答してもよい。仮想チャネルが有効化されていたと仮定すると、SignHash（）要求が、クライアントデバイス1001の認証マネージャサービス1008に直接渡されてもよい。POLICY__VIRTUAL__CHANNEL__DISABLEDが偽であり、証明書がユーザによって選択されたものであり、PINがシングルサインオンサービスから入手可能であるか、もしくは（たとえば、ユーザが他のサービスに認証したときの以前のステップからの）以前のスマートカードセッションが存在する場合、またはスマートカード1017のロック解除に使用される正しいPINまたは他の資格情報、たとえば、指紋や他のバイオメトリックなどをユーザが供給した場合、認証マネージャサービス1008は、ハッシュに署名してもよい。

【0145】

高速スマートカードは、1つまたは複数のオペレーティングシステムと統合（たとえば、完全に統合）されてもよく、期待されるエンドユーザエクスペリエンスを提供し得る。高速スマートカードログオンをオペレーティングシステムと統合することにより、スマートカードがローカルに（たとえば、リモートセッションプロトコルなしで）使用されたシナリオと同じまたは同様のエンドユーザエクスペリエンスがもたらされ得る。たとえば、1つまたは複数のリソースにアクセスするために、クライアントデバイス上の実行可能プログラムまたは他のプログラム（たとえば、WINDOWS（登録商標）のLogonUI）を使用して、スマートカードPINまたは他のスマートカード資格情報を入力するようにユーザに促してもよい。本明細書に記載の態様は、ユーザが、たとえばログオンユーザインターフェースプログラム（LogonUIなど）を介して、スマートカードPINまたは他の資格情報をオペレーティングシステムに提供することにより、インタラクティブにリモートセッションにログオンすることを可能にし得る。本明細書に記載の態様は、ユーザが、たとえばログオンユーザインターフェースプログラムを介して、ユーザのスマートカード資格情報をオペレーティングシステムに提供することにより、リモートセッションをロック解除することを可能にし得る。したがって、ユーザは、リモートセッションをロック時に切断し、次いでシングルサインオンを使用して再接続する必要がなくなり得る。本明細書に記載の態様は、様々なPC/SC関数、たとえば、PC/SCのSCardListCards関数、PC/SCのSCardGetCardTypeProviderName関数、または他の関数の呼び出しなどを介して、スマートカードに関連付けられたCSPを発見するためにリソースマネージャへの標準クエリを使用し得るセッション内アプリケーションを使用することを可能にし得る。

【0146】

一部の態様では、1つ（または複数）の代用スマートカードを使用して、高速スマート

10

20

30

40

50

カードを1つまたは複数のオペレーティングシステム、たとえば、W I N D O W S（登録商標）、L I N U Xなどと統合してもよい。代用スマートカードは現実のスマートカード（たとえば、現実の物理スマートカード）でなくてもよい。その代わりに、代用スマートカードは、サーバの1つまたは複数のサーバ側コンポーネント、たとえば、図8及び図9に示すサーバ821、図10に示すサーバ1021、または本明細書に記載の他の任意のサーバの1つまたは複数のコンポーネントなどによって生成されてもよく、及び／またはそれらに知られていてもよい。前述のように、クライアントデバイス801は、リモートセッションプロトコルを介してサーバ821に接続されてもよい。

【0147】

1つまたは複数の代用スマートカードは、代用スマートカードタイプ識別子によって識別されてもよい。代用スマートカードタイプ識別子は、たとえば、代用スマートカードのスマートカードタイプを示してもよい。代用スマートカードの代用スマートカードタイプ識別子は、たとえば、リセット応答（A T R）メッセージまたはファイルに含まれてもよい。代用スマートカードのA T Rは、現実のスマートカードと同様に、スマートカードのタイプを一意に識別するデータのシーケンス（たとえば、バイトのシーケンス）を含んでもよく、これはI S O 7 8 1 6仕様に従って定義されてもよい。サーバは、I S O 7 8 1 6フォーマットに従って1つ（または複数）の代用スマートカードA T Rを作成してもよい。一部の態様では、サーバは、仮想マシンのインストールなどのインストール時に、代用スマートカードと、それに関連付けられる代用スマートカード識別子とを作成する。

【0148】

生成された代用スマートカード識別子（たとえば、A T R）は、C S P（たとえば、高速スマートカードC S P）に関連付けられてもよく、C S Pは一部のシナリオでは暗号動作に使用されてもよい。代用スマートカード識別子とC S Pとの間の関連付けは、サーバ側コンピュータ（たとえば、サーバ821）に記憶されてもよい。たとえば、サーバはデータベースを含んでもよく、識別子（たとえば、A T R）とC S Pとの間の関連付けは、サーバのデータベースに追加されてもよい。W I N D O W S（登録商標）オペレーティングシステムの場合、代用スマートカード識別子と、対応するC S P（たとえば、高速スマートカードC S P）との間の関連付けは、P C / S Cリソースマネージャデータベースに追加されてもよい。たとえば、関連付けはW I N D O W S（登録商標）レジストリに追加されてもよい。

【0149】

図16Aに、本明細書に記載の1つまたは複数の例示的な態様による例示的なスマートカードのデータベースを示す。データベース（たとえば、スマートカードリソースマネージャデータベース）は、レジストリであってもよく、複数のスマートカード1605に関する情報を含んでもよい。たとえば、スマートカードの1つは、リモートスマートカード1610を含んでもよく、これはサーバ側で生成及び記憶される代用スマートカードであってもよい。リモートスマートカード1610の対応するファイル1612は、リモートスマートカード1610に関する情報、たとえば、スマートカード識別子1615（たとえば、A T R）、及びC S P 1620を識別する情報を含んでもよい。スマートカード識別子1615及びC S P 1620を識別する情報は、同じファイル（たとえば、リモートスマートカードファイル）に記憶されてもよい。図示のように、リモートスマートカード1610は、16進値（たとえば、3 b 1 f d 9 4 3 6 9 7 4 7 2 6 9 7 8 5 3 6 d 6 1 7 2 7 4 4 3 6 1 7 2 6 4 9 6）を持つA T Rを有してもよい。2進値またはA S C I I値などの他のタイプの値を使用して、A T Rを表現してもよい。C S P 1620を識別する情報は、C I T R I Xスマートカード暗号プロバイダなどのC S Pの名前（またはC S Pへの他のポインタ）を含んでもよい。この名前は、C S P（たとえば、ダイナミックリンクライブラリ（D L L）データ）のパスを示す、データベース内の場所を指してもよい。

【0150】

図16Bに、本明細書に記載の1つまたは複数の例示的な態様による例示的なスマート

10

20

30

40

50

カードのデータベースを示す。前述のように、C S P 1 6 2 0を識別する情報は、C I T R I Xスマートカード暗号プロバイダなどのC S Pの名前を含んでもよい。C S Pの名前は、データベース内の場所1 6 2 5を指してもよい。場所1 6 2 5は、C S Pの場所を指すデータ1 6 3 0などのデータを含んでもよい。たとえば、C S Pファイル（たとえば、D L L）をロードする（たとえば、動的にロードする）ためのパスは、C : ¥ P r o g r a m F i l e s ¥ C i t r i x ¥ S y s t e m 3 2 ¥ C t x S m a r t C A r d C S P 6 4 . d l lであってもよい。これらの例では、データベースは、スマートカード識別子（たとえば、A T R）を適切なC S Pに関連付けてもよい。

【0151】

図1 6 Aを参照すると、他のスマートカード1 6 0 5または他のタイプのスマートカードは、スマートカード1 6 1 0と同じまたは類似の情報を含んでもよい。たとえば、異なるタイプのスマートカードはそれぞれ、異なるスマートカード識別子を有してもよい。同じタイプのスマートカードは、同じスマートカード識別子（たとえば、A T R）を使用してもよい。結果的に、同じタイプのスマートカードは同じC S Pを使用してもよい。たとえば、同じタイプの一部のスマートカードは、同じ識別子（たとえば、A T R）と、同じC S P識別子（たとえば、C S P名またはC S Pの他のポインタ）とを記憶する対応するファイルを有してもよい。

【0152】

一部の態様では、複数の代用A T Rまたは他の識別子が使用されてもよい。たとえば、クライアントデバイスが複数のスマートカードを同時に（または異なる時間に）使用してもよく、それらのスマートカードは異なるタイプのスマートカードを含んでもよい。異なるタイプのスマートカードが、単一の代替A T R（または他の識別子）に関連付けられてもよく、したがって、同じC S P（たとえば、図8に示すC S P 8 3 1）を使用してもよい。しかしながら、クライアント側で異なるC S Pが使用されてもよい。たとえば、クライアントデバイス8 0 1は、あるタイプのスマートカードに対処するためのC S P 8 1 1と、他のタイプのスマートカードに対処するための他のC S P（図8には図示せず）とを含んでもよい。クライアントデバイス8 0 1は、どのC S Pを使用するかを知っていてもよい。サーバ8 2 1からクライアントデバイス8 0 1への暗号動作要求があるたびに、要求内のフィールドは、クライアント側で使用するC S P（たとえば、C S P 8 1 1または他のC S P）の名前を含んでもよい。

【0153】

追加的または代替的には、異なるタイプのスマートカードはそれぞれ、異なる代替A T R（または他の識別子）に関連付けられてもよく、したがって、サーバ側で異なるC S Pを使用してもよい。たとえば、図8に示すC S P 8 3 1は、あるタイプのスマートカードに使用されてもよく、サーバ側の他のC S P（図8には図示せず）は、他のタイプのスマートカードに使用されてもよい。異なるタイプのスマートカード用の異なるC S Pは、ダブルアップシナリオで、たとえば、関与するクライアント8 0 1からサーバ8 2 1へ、そしてサーバ8 2 1から他のサーバ（図8には図示せず）への認証などで使用されてもよい。他のサーバは、高速スマートカード機能を使用しない場合があり、A T Rを現実のスマートカード8 1 7に代替し戻すために、現実のスマートカード8 1 7のスマートカードタイプを知る必要がある場合がある。

【0154】

本明細書に記載の1つまたは複数の例は、暗号動作の高速スマートカードリダイレクトと、一部の（たとえば、初期）P C / S C関数のP C / S Cリダイレクトとを使用する。図8を参照すると、サーバ8 2 1は、ログオンユーザインターフェースアプリケーションを含んでもよい。たとえば、そのアプリケーションはW I N D O W S（登録商標）オペレーティングシステムのL o g o n U Iであってもよい。サーバ8 2 1は、そのアプリケーションを介して、クライアントデバイス8 0 1が1つまたは複数のスマートカードリーダーを含むかあるいはそれに接続されているか否かを判定してもよい。そのアプリケーションは、P C / S C要求を介して、たとえば、サーバ8 2 1のP C / S Cフック8 3 9を介し

10

20

30

40

50

て、スマートカードリーダー（複数可）を発見してもよい。発見要求は、サーバ821の暗号API829をバイパスしてもよい。PC/SCフック839は仮想チャネルドライバ835及び／または仮想チャネルドライバ805を介してクライアント801のPC/SC815に要求を伝達してもよく、要求はPC/SCレベルで送られてもよい。クライアント側のPC/SC815は、PC/SCレイヤを介して、クライアントデバイス801が1つまたは複数のスマートカードリーダーを有することの指示を返してもよい。

【0155】

サーバ821は、WINDOWS（登録商標）のLogonUIなどのアプリケーションを介して、たとえば、スマートカードが存在するか否か（たとえば、カードが挿入されているか否か）を確認するために、リーダー（複数可）のステータスの要求をスマートカードリーダー（複数可）に送ってもよい。ステータス要求は、PC/SCフック839の直接呼び出しなど、PC/SCレベルで送信されてもよい。ステータス要求は暗号API829をバイパスしてもよい。PC/SCフック839は、仮想チャネルドライバ835及び／または仮想チャネルドライバ805を介してPC/SC815に要求を伝達してもよく、要求はPC/SCレベルで送られてもよい。クライアント側のPC/SC815は、PC/SCレイヤを介して、スマートカードがリーダーに挿入されているか否かの指示を返してもよい。

【0156】

スマートカード（たとえば、スマートカード817）が識別された場合、クライアントデバイス801は、PC/SC815を介して、スマートカード817に関連する情報、たとえば、スマートカード817の一意の識別子、またはスマートカードのタイプを（たとえば、ATRファイルとして）取得してもよい。スマートカードのATR（または他の識別子）は、たとえば、SCardGetStatusChangeのPC/SC関数によってスマートカード817から取得されてもよい。クライアントデバイス801は、仮想チャネルドライバ805及び／または仮想チャネルドライバ835を介してサーバ821に応答を送信してもよい。応答はPC/SCレベルで送信されてもよい。応答は、スマートカードのATR（または他の識別子）を含んでもよい。

【0157】

サーバ821は、仮想チャネルドライバ835を介して、スマートカードの一意の識別子（たとえば、ATR）を含む応答を受信してもよい。前述のように、サーバ821は、たとえばプロトコルネゴシエーションを介して、高速スマートカードリダイレクトが有効化されているか否かを知ってもよい。高速スマートカードが有効化されている場合、サーバ821のPC/SCリダイレクトレイヤ（たとえば、スマートカードサービス）は、スマートカード817のATRを代用スマートカードのATRに代替してもよい。現実のスマートカードのATRの代用スマートカードのATRへの代替は、PC/SCリダイレクトレイヤによって、クライアントからサーバへの方向、及び／またはサーバからクライアントへの方向に、オンザフライで実行されてもよい。代替されたATRを含むスマートカード817に関連する情報は、PC/SCフック839に送られてもよい。サーバ821のログオンユーザインターフェースは、PC/SCフック839を介して代替されたATRを含む情報を取得してもよい。

【0158】

代替されたATRに基づいて、サーバ821のログオンユーザインターフェースは、暗号動作に使用するCSPを決定してもよい。たとえば、ログオンユーザインターフェースは、リソースデータベースに照会して、データベース内の任意のエントリがATRまたはその一部を含むか否か、及び／または任意のエントリがATRを特定のCSPに関連付けているか否かを判定してもよい。例示的なデータベースを図16A及び図16Bに示す。

【0159】

図16Aを参照して、たとえば、代替されたATRが3b 1f d9 43 69 74 72 69 78 53 6d 61 72 74 43 61 72 64 96の16進数値を含むと仮定する。サーバ821は、ログオンユーザインターフェースを

介して、対応する（たとえば、一致する）A T R（たとえば、3 b 1 f d 9 4 3 6 9 7 4 7 2 6 9 7 8 5 3 6 d 6 1 7 2 7 4 4 3 6 1 7 2 6 4 9 6 の 1 6 進数値を有するもの）をデータベースで検索してもよい。サーバ 8 2 1 は A T R 1 6 1 5 を見つけ、それが代替された A T R に対応すると判定してもよい。

【0160】

サーバ 8 2 1 が A T R 1 6 1 5 を識別した後、サーバ 8 2 1 はその A T R に対応するスマートカードの名前を取得することを試みてもよい。たとえば、スマートカード名を取得するために S C A r d L i s t C A r d s の P C / S C 関数が呼び出されてもよい。この例では、取得されるスマートカード名は、リモートスマートカード 1 6 1 0 であってもよい。

10

【0161】

サーバ 8 2 1 がスマートカード名（たとえば、リモートスマートカード 1 6 1 0）を取得した後、サーバ 8 2 1 は、データベース（たとえば、レジストリ）に照会するなどして、スマートカードに関連付けられた C S P を特定してもよい。たとえば、S C A r d G e t C A r d T y p e P r o v i d e r N a m e の P C / S C 関数を呼び出して、C S P を特定してもよい。この例では、取得される C S P 名は、スマートカード暗号プロバイダ 1 6 2 0 であってもよく、スマートカード暗号プロバイダ 1 6 2 0 は、たとえば、図 8 及び図 9 に示す C S P 8 3 1 を識別してもよい。それに応じて、サーバ 8 2 1 は、ログオンユーザインターフェースアプリケーションを介して、C S P 1 6 2 0 と A T R 1 6 1 5 との間の関連付けを発見してもよい。サーバ 8 2 1 は C S P をロードし、クライアントにおけるスマートカード（たとえば、スマートカード 8 1 7）を必要とする暗号動作に C S P を使用してもよい。C S P 8 3 1 などの高速スマートカード C S P を使用する様々な例は、前述している。また、暗号 A P I 8 2 9 を使用して、C S P 8 3 1 にアクセスしてもよい。C S P 名を指定する C r y p t A c q u i r e C o n t e x t 関数を使用して、高速スマートカードメカニズムと連携する暗号動作を実行してもよい。

20

【0162】

前述のように、スマートカード 8 1 7 を必要とする 1 つまたは複数の動作は、P C / S C レイヤよりも上位のレイヤで仮想チャネル 8 3 6 を介してクライアントデバイス 8 0 1 にリダイレクトされてもよい。一部の態様では、システムは、P C / S C レイヤではなく、より上位のレイヤにできるだけ多くの動作をリダイレクトすることを試みてもよい。前述のように、（たとえば、リモートセッションプロトコルを介して）クライアントデバイス 8 0 1 にリモーティングされ得る例示的な暗号動作には、スマートカード 8 1 7 上の証明書を一覧化する要求、証明書の要求、スマートカード 8 1 7 の秘密鍵を使用した署名動作、及びスマートカード 8 1 7 の秘密鍵を使用した復号動作が含まれるが、これらに限定されない。高速スマートカードログオンを使用することにより、たとえば長いレイテンシが存在する場合に、より高速なパフォーマンスが提供され得る。

30

【0163】

C S P 8 3 1 は、高速スマートカードログオン暗号動作に使用されてもよく、C S P 8 3 1 は、仮想チャネルドライバ 8 3 5（及び／またはクライアントデバイス 8 0 1 の対応する仮想チャネルドライバ 8 0 5）を介してクライアントデバイス 8 0 1 と通信してもよい。クライアントデバイスの暗号 A P I 8 0 9 は、C S P 8 1 1 と通信して、スマートカード 8 1 7 を使用した暗号動作を完了してもよい。

40

【0164】

P C / S C レイヤよりも上位のレイヤで通信することにより、いくつかの技術的な利益がもたらされ得る。たとえば、P C / S C はチャッティ（c h a t t y）なプロトコルであり得、スマートカードから証明書（複数可）を取得すると、（たとえば、S C A r d T r a n s m i t の P C / S C 関数を介して）何百もの同期 P C / S C 要求／応答に変換され得る。ネットワークのレイテンシが長い（たとえば、1 5 0 ミリ秒以上である）場合、リモートスマートカードの使用は、エンドユーザにとって遅すぎて、パフォーマンスが低下し得る。たとえば、場合によっては 1 回の動作で何百もの要求／応答のレイテンシが合

50

計されるので、暗号動作は実行に長い時間がかかり得る。スマートカードの動作をより上位のレイヤにリダイレクトすることにより、スマートカードを使用した認証または他の動作の速度が向上し得る。

【0165】

暗号動作中に、資格情報を受信するためのユーザインターフェースが、クライアントデバイス801に関連付けられたディスプレイに表示されてもよい。図17に、本明細書に記載の1つまたは複数の例示的な態様による例示的なユーザインターフェース1700を示す。ユーザインターフェース1700は、たとえば、ユーザ名及び／またはサインインオプション、たとえば、パスワードを使用するか、スマートカードを使用するかなどを表示してもよい。ユーザは、スマートカードを使用して認証するオプション1710を選択してもよく、PINなどのスマートカードに関連付けられた資格情報を入力してもよい。ユーザがPINまたは他の資格情報を提供すると、資格情報は暗号化され、ユーザの認証に使用され得る。前述のように、PIN（または他の資格情報）は記憶されてもよく、記憶されたPIN（または他の資格情報）を使用して、ログオン後にアプリケーションで使用するためにスマートカード817をロック解除してもよい。クライアントデバイス801は、スマートカード817を使用してドメインコントローラへ認証されてもよい。

10

【0166】

図8を参照すると、（たとえば、LogonUIアプリケーションを介して）PIN（または他の資格情報）がUIから取得され、サーバ側のCSP（たとえば、図8に示すCSP831及び／またはCSP833）に提供されてもよい。前述のように、PINはクライアント側のエージェントに送られてもよく、PINは仮想チャネル836を介して搬送されてもよい。公開／秘密鍵ペアまたは他の任意の非対称暗号を使用して、PINを保護してもよい。クライアントエージェント803は、たとえば起動時に、公開／秘密鍵ペアをオンザフライで生成してもよい。鍵ペアはメモリに記憶されてもよく、高速スマートカードが有効化されている場合に実行されてもよい。スマートカード仮想チャネルがネゴシエーションを終えた後（たとえば、高速スマートカードが有効化されている場合）、生成された公開鍵はサーバ側に送られてもよい。CSP831は次いで、受信した公開鍵を取得してもよい。スマートカードのPIN（または他の資格情報）をクライアント側に送る場合、CSP831はPINを公開鍵で暗号化してもよい。PINは、暗号化された状態で仮想チャネル836を介して、及び／または仮想チャネルドライバ805に送り返されてもよい。仮想チャネルドライバ805及び／またはクライアントエージェント803は、メモリに記憶された秘密鍵でPINを復号してもよい。仮想チャネルドライバ805及び／またはクライアントエージェント803は次いで、CSP811を介して、PINを使用する1つまたは複数の暗号動作を実行してもよい。これにより、CSP831から仮想チャネルドライバ805及び／またはクライアントエージェント803までのPINの保護が可能になり得、これは、PIN（または他のスマートカード資格情報）を使用するCSP811を用いて1つまたは複数の暗号動作を実行してもよい。

20

30

【0167】

フェデレーテッドログオンの例示的な実施形態

前述の高速スマートカードログオンを実装するために使用されるコンポーネントはまた、フェデレーテッドフルドメイン（たとえば、Active Directory（AD））ログオンを実装するために使用されてもよい。フルドメインログオン後、セッションはフルネットワーク資格情報（たとえば、Kerberosチケット付与チケット（TGT）及びチャレンジ／応答パスワードハッシュ（たとえば、NTLMパスワードハッシュ））を有し得る。たとえば、ユーザは、SAML許可トークンを提供することにより、Active Directoryユーザアカウントとして、仮想デスクトップセッション、物理PC、またはリモートデスクトップサーバセッションへ認証してもよい。以下の例でさらに詳細に説明するように、ユーザは、適切な任意のタイプの資格情報及び／または認証プロトコルを使用して、外部コンポーネント／サービス／デバイス、たとえば、アイデンティティプロバイダ（IdP）へ認証してもよい。この認証は、外部認証イベントと

40

50

呼ばれる場合がある。例示的な外部認証イベントには、セキュリティアサーションマークアップ言語（SAML）アイデンティティプロバイダにおけるログオン、TLSまたはSSLを介したスマートカード認証、及びADパスワードを使用しないバイオメトリクスまたはワンタイムパスワード（OTP）などの代替的な認証資格情報が含まれる。

【0168】

IdPとの認証後、IdPは確認トークン（たとえば、SAMLトークン）を指名されたリライティングパーティ（RP）またはサービスプロバイダに発行してもよく、これを使用してユーザからのサービスアクセス要求を処理し得る。RPは、認証の詳細全てを知るとも、資格情報と直接インタラクトすることも必要とせずに、IdPからのフレッシュなSAMLトークンを使用して、要求元ユーザのアイデンティティを信用し得る。IdPがユーザのアイデンティティを確認したことが（後述の）資格情報マッピングサービスに保証され得る限り、SAMLトークンの代わりに、他のトークンフォーマットまたはアイデンティティ確認メカニズムが使用されてもよい。外部認証イベント（たとえば、IdPによる認証）の受諾に基づいて、仮想スマートカードの資格情報（短期間ログオン証明書とも呼ばれる）が発行されてもよい。

10

【0169】

上記の高速スマートカードログオンからの証明書動作インターセプトコンポーネントを使用して、PC/SCのAPIレベルでスマートカードを完全にエミュレートすることなく、仮想スマートカードとのインタラクションを可能にし得る。仮想スマートカードは、IdPにおいて、リモートコンピューティング環境（たとえば、認証サーバ）においてローカルに、及び／または高度に保護され得る別個のサーバ、たとえば、資格情報マッピングサービスをホストするサーバなどにおいて、作成されてもよい。

20

【0170】

様々なフェデレーションシナリオが存在する。たとえば、外部ユーザの従来のフェデレーションは、ビジネスツービジネス（たとえば、サプライチェーン、共同開発などのパートナー）であり得る。コンシューマツービジネスは、たとえば、市民、退職者、退役軍人などを含み得る。クラウドサービスは、企業リソースにアクセスするためにクラウドデスクトップが使用されるソフトウェアアズアサービス（SaaS）製品及び／またはデータアズアサービス（Daas）にアクセスするための企業管理型のユーザ認証を含み得る。次世代の企業セキュリティモデルは、アイデンティティプロバイダ（IdP）を、デバイスからのSaaS及びオンプレムリソース用のユーザ認証のための中心点として含んでもよい。IdP自体が、アイデンティティアズアサービス（IDaaS）などの、オンプレムまたはクラウドサービスであってもよい。

30

【0171】

図11に、本明細書に記載の1つまたは複数の例示的な態様によるフェデレーテッドログオンのための例示的なシステムを示す。図11に示すシステムは、図12A～図12Cに示す例示的なシステムで使用されるように、資格情報マッパーを使用しなくてもよい。

【0172】

図12Aに、本明細書に記載の1つまたは複数の例示的な態様によるフェデレーテッドログオンのための他の例示的なシステムを示す。一部の態様では、スマートカードは、このフェデレーテッドログオンの場合に使用されなくてもよい。その代わりに、証明書が認証に使用されてもよく、リソースシステム1221（たとえば、顧客の構内）は、証明書がスマートカード証明書であると考えてもよい。システム1221はセットアップフェーズを開始してもよい。アプリケーションストア1225は、信頼済みのデバイスを含んでもよく、ユーザのドメイン（たとえば、ADまたはディレクトリサービス1241）ログオン資格情報を資格情報マッパー1229に要求するために使用されてもよい。資格情報は、短い有効期間のスマートカードクラス証明書（たとえば、仮想スマートカード証明書）を含んでもよい。資格情報マッパー1229は、ADユーザ用の短い有効期間のスマートカードクラス証明書を要求するために、サードパーティ証明書サービス（たとえば、MICROSOFT証明書サービス）などの、証明書サービス1231によって信頼されて

40

50

もよい。資格情報マッパー 1 2 2 9 は、ユーザ用の仮想スマートカードを作成するために使用されてもよい。資格情報マッパー 1 2 2 9 は、証明書サービス 1 2 3 1 に証明書を要求してもよく、証明書サービス 1 2 3 1 は、ユーザ用のスマートカードクラス証明書を資格情報マッパー 1 2 2 9 に返してもよい。仮想スマートカードは、資格情報マッパー 1 2 2 9 に記憶（たとえば、キャッシュ）されてもよい。

【0173】

カスタムテンプレートが、制御を提供するために使用されてもよい。発行インフラストラクチャへの制御を提供する（たとえば、スマートカードクラス証明書を要求するのに信頼されるサーバを制限または識別する）だけでなく、カスタムテンプレートはまた、特別なマーカを発行される証明書に含ませることができ、これにより特別なグループメンバーシップがログオントークン及び Kerberos チケットに挿入されることになる。一部の態様では、複数のマーカが証明書内に配置されてもよく、各マーカが各自のグループメンバーシップを選択する。これにより、認証及びサービスプロバイダアクセス要求の完全な状況を構成する異なる属性を個別のグループにマッピングするための柔軟性が提供され得、所望のリソースアクセス制御ポリシーを表現し易くなる。これらのマーカによって、たとえば、WINDOWS（登録商標）ベースのインフラストラクチャ及びサービスは、現実のスマートカードまたはパスワードを使用するのではなく、この特定のメカニズムによってユーザが AD へ認証したことを認識することが可能になり得る。

【0174】

異なるテンプレートが、資格情報マッピングサービス 1 2 2 9 によって、SAML トークンの属性、または真の認証保証レベルの他の指示に基づいて使用されてもよい。追加または代替の認証状況が、認証保証レベル以外の関心対象であってもよい。たとえば、ユーザの地理的位置、またはサービスプロバイダにアクセスするために使用される接続経路（たとえば、境界線の内か外か）が、関心対象であってもよい。証明書テンプレートは、これらの利用可能な属性及び状況指標の一部または全部からのマッピングに基づいて選択されてもよい。追加的または代替的には、資格情報マッピングサービス 1 2 2 9 によって、たとえば、資格情報マッパーサービス 1 2 2 9 により認証局に送られる証明書署名要求を介して、カスタムステートメントまたは属性が証明書に追加されてもよい。これらはセキュリティグループにマッピングされなくてもよく、クライアント証明書認証を直接使用するウェブアプリケーションなどのアプリケーションによって検査することができる。

【0175】

ディレクトリサービス 1 2 4 1 は、ユーザログオン用のスマートカードクラス証明書を発行する証明書サービス 1 2 3 1 を信頼してもよい。この信頼ステップは、仮想スマートカード証明書を Active Directory ログオンなどに使用することを可能にし得る。信頼ファブリックが、サービスツースーサービスのアイデンティティ及びセキュアな通信を確立する適所にあってもよい。任意選択で、資格情報マッパー 1 2 2 9 は、アイデンティティプロバイダ (IdP) 1 2 1 3 によって発行された SAML トークンをクロスチェックしてもよい。

【0176】

システムは実行フェーズを開始してもよい。クライアントエージェント 1 2 0 1 内のウェブビュー 1 2 0 3 は、IdP ログオンに対処するために使用されてもよい。クライアントエージェント 1 2 0 1 は、ログオンのために資格情報を IdP 1 2 1 3 に送ってもよい。ウェブビュー 1 2 0 3 はまた、ゲートウェイサーバ 1 2 2 3 またはアプリケーションスタック 1 2 2 5 への SAML ログオンのための標準的なセキュリティアサーションマークアップ言語 (SAML) プロトコルをサポートしてもよい。ゲートウェイサーバ 1 2 2 3 は、企業リソース及び／またはクラウドリソースへのアクセスを提供するサーバまたは他のリソースであってもよい。ログオンプロセス中に、IdP 1 2 1 3 は、アイデンティティ確認トークン（たとえば、SAML トークン）をクライアントエージェント 1 2 0 1 に返してもよい。SAML トークンはクライアントエージェント 1 2 0 1 によって、アイデンティティシステム 1 2 1 1 と認証したことの証明として使用されてもよく、これはリソー

システム 1 2 2 1 の外部パートナーを含んでもよい。

【0 1 7 7】

ウェブフォームを含む HTML ページを含み得るログオンページ 1 2 1 5 を使用して、ユーザから、または場合によってはブラウザもしくはクライアントエージェント自体から認証資格情報を収集してもよい。これらの資格情報は、ユーザ名及びパスワードフォームから、高度なリスクベースの認証システムにまで及ぶことができる。I d P 1 2 1 3 はこれらのログオンページ 1 2 1 5 を使用して、1 つまたは複数の任意の適切な認証方法で正規ユーザを認証してもよい。

【0 1 7 8】

ディレクトリ 1 2 1 7 は、アイデンティティストアもしくはアカウントデータベース、または I d P 1 2 1 5 をサポートする他のディレクトリを含んでもよい。たとえば、ディレクトリ 1 2 1 7 は、他の会社のネットワーク内の A c t i v e D i r e c t o r y のインスタンスであってもよく、または他のベンダーの L D A P ディレクトリ製品を使用してもよい。

【0 1 7 9】

D i r S y n c 1 2 1 9 は、（仮想化サーバ 1 2 3 7 を介して公開され得る）リソースシステム 1 2 2 1 でホストされるアプリケーション及びデスクトップへのアクセスを許可されるべきであるディレクトリ 1 2 1 7 内の正当で許可されたユーザごとにディレクトリサービス 1 2 4 1 においてシャドウアカウントが存在するようにするメカニズムまたはメカニズムのセットを含んでもよい。D i r S y n c 1 2 1 9 メカニズムの例には、許可されたユーザ名及び他の関連するアイデンティティまたは許可情報のリストを有するスプレッドシートを電子メール送信またはアップロードするなどの手動手順が含まれる。他の例には、（場合によってはディレクトリの区別された部分における）一部または全部のアカウントについてディレクトリ 1 2 1 7 を照会してディレクトリサーバ 1 2 4 1 に送信する、定期的にスケジュールされたまたは恒久的に繰り返すバッチジョブが含まれる。他の例には、ディレクトリ 1 2 1 7 の変更を監視し、それらの変更を発生時に、またはスケジュールに従って送信することが含まれる。他のメカニズムは暗黙的なものであり、すなわち、ディレクトリ 1 2 1 7 における新たな許可ユーザの存在が、そのユーザアイデンティティを引用するフェデレーショントークンがリソースシステム 1 2 2 1 に提示された場合に、暗示され得る。

【0 1 8 0】

一部の態様では、証明鍵バインディングが使用されてもよい。S A M L トークン証明鍵は、フルドメインログオンを許可するために作成される仮想スマートカードにリンクされてもよい。この証明鍵（または関連する証明鍵）は次いで、リモートコンピューティング環境によって、仮想スマートカードを実際に使用するために使用されてもよい。クライアントエージェント 1 2 0 1 は、I d P 1 2 1 3 により発行された S A M L トークンにバインドされる証明鍵をネゴシエートしてもよい。

【0 1 8 1】

一部の態様では、S A M L トークンまたは他の信頼済みのログオン資格情報が、対応する A D ユーザパスワードにマッピングされてもよく、これはそのパスワードが、（以下でさらに詳細に説明する）ゲートウェイサーバ 1 2 2 3 またはアプリケーションストア 1 2 2 5 のログオンプロセス中に直接利用できない場合でも行われ得る。たとえば、パスワードは、I d P 1 2 1 3 によってそのログオン中にキャプチャされ、信頼済みのバックチャネルを介してゲートウェイサーバ 1 2 2 3 またはアプリケーションストア 1 2 2 5 に中継されてもよい。他の態様では、パスワードボルトまたはパスワード管理サービスが、パスワードをゲートウェイサーバ 1 2 2 3 またはアプリケーションストア 1 2 2 5 に返してもよい。他の例では、資格情報マッパー 1 2 2 9 は、それ自体が特定のユーザアカウントのパスワードを管理してもよい。これらのパスワードは、ユーザが選択したパスワードでなくてもよく、したがって、マスター鍵からユーザごとのソルトを使用して導出することができる。この例では、データベースまたはパスワードボルトは使用されなくてもよい。

【0182】

フルドメインログオンが要求される場合、クライアントエージェント1201は、ゲートウェイサーバ1223及び／またはアプリケーションストア1225にSAMLトークンを送ってもよい。ゲートウェイサーバ1223及び／またはアプリケーションストア1225は、（たとえば、バックチャネルを介して）SAMLトークンを送るなどしてIdP1213と通信することにより、クライアント1201がアイデンティティシステム1211と認証されたことを検証してもよい。SAMLトークンが有効期間などの時間を含む場合、IdP1213は現在時刻が有効期間内であることを検証してもよい。追加的または代替的には、リライディングパーティ（コンポーネント）は、IdPの署名証明書のローカルに記憶された（たとえば、信頼済みの）コピーを使用して、SAMLトークンが含むデジタル署名をチェックすることにより、SAMLトークンをローカルに有効性検証してもよい。

10

【0183】

アプリケーションストア1225、デリバリーコントローラ1235、及び／または仮想化デバイス1237は、アプリケーションストア1225によって提供されたカスタムログオンデータを、仮想化デバイス1237上でのログオンプロセスを駆動するために使用され得る資格情報プラグイン1239にセキュアに搬送してもよい。アプリケーションストアは、ログオンデータプロバイダなどの認証拡張1227を含んでもよく、これは本明細書に記載のように、仮想スマートカード参照と、仮想化デバイス1237が仮想スマートカードにアクセスするための一致する資格情報プラグインと、仮想スマートカードを実装するためのサポート用サービスインフラストラクチャ（たとえば、資格情報マッパー1229）と、を取得するために使用されてもよい。

20

【0184】

クライアント1201が認証されたことが検証されると、ゲートウェイ1223、アプリケーションストア1225、及び／またはデリバリーコントローラ1235（たとえば、デスクトップデリバリーコントローラ）は、資格情報マッパー1229が、指定された仮想化マシン上でのADログオン用の時間制限付きの（たとえば、一時的な）スマートカードクラス証明書を取得することを許可してもよい。換言すれば、一時的な証明書は、スマートカード（たとえば、スマートカード内の1つまたは複数の証明書）をエミュレートするために作成されてもよい。時間制限付き証明書は、数分、数時間、数日、またはさらに短いもしくはさらに長い期間の間に有効であってもよい。許可ステップをサポートするために、ストア1225／コントローラ1235は、IdP1213からのオリジナルのSAMLトークンを提示して、その有効性が資格情報マッピングサービス1229によって再び検証されるようにしてもよい。たとえば、資格情報マッパー1229は、IdP1213と通信してSAMLトークンを検証してもよい。このステップはまた、SAMLトークンから仮想スマートカードへバインドする証明鍵の転送、または新たな証明鍵のネゴシエーションを容易にすることができる。

30

【0185】

ログオンチケットが発行され、リモートディスプレイプロトコル（たとえば、クライアントエージェント）ファイルに入ってもよい。ログオンチケットの手法では、クライアントエージェント1201に送られたログオンチケットはまた、資格情報マッピングサービス1229によって保持される仮想スマートカードの秘密鍵を最初に暗号化するために使用されてもよい。追加的または代替的には、クライアントエージェント1201によって保持される証明鍵が、短い有効期間の証明書にリンク（たとえば、バインド）されてもよい。任意選択で、資格情報マッパー1229に、クライアント1201による有効なログオンの証拠として、オリジナルのIdP認証トークンが提示されてもよい。ログオンチケットは、追加的または代替的には、資格情報マッパー1229によって提供される仮想スマートカードへのセキュアな参照を暗号化するために使用されてもよい。この例では、仮想スマートカードは、デリバリーコントローラ1235によって仮想スマートカードを使用することが許可された仮想化エージェント1237のみによって復元されてもよい。暗

40

50

号化された仮想スマートカード参照は、アプリケーションストア1225からデリバリーコントローラ1235へ、そして仮想化エージェント1237へ送られてもよく、一方、ログオンチケットはクライアントエージェント1201に送られる。これにより、仮想化エージェント1237が知られる前に仮想スマートカードが作成されること、または複数の仮想化エージェントに別々にログオンするために使用されることが可能になり得る。

【0186】

仮想化エージェント1237は、ログオンチケット（またはログオンチケットを使用して復号されるセキュアな仮想スマートカード参照）を資格情報マッピングサービス1229に提示し、スマートカードクラス証明書を使用して、クライアントデバイス1201をMICROSOFT ADなどのディレクトリサービス1241にログオンさせてもよい。資格情報プラグイン1239（たとえば、ログオンフック）は、前述の高速スマートカードログオンの手法に非常に類似しているかまたは同一であってもよい。資格情報プラグイン1239は、図8を参照して説明したサーバ側の仮想エージェント823、資格情報プロバイダ825、及び／またはCSP831を含んでもよい。

10

【0187】

資格情報マッパー1229は証明書サービス1231とインタラクトしてもよく、これは、スマートカードクラスユーザ認証証明書に対応する秘密鍵と共に取得するための認証局、たとえば、WINDOWS（登録商標）証明書サービスを含んでもよい。すなわち、資格情報マッパー1229は、ユーザ用の登録局（たとえば、MICROSOFT登録エージェント）として使用されてもよい。資格情報マッパー1229は、証明書サービス1231に要求を送るときに認証証明書として使用する登録局証明書を有してもよい。資格情報を初めて取得するためのブートストラッププロセスが存在してもよく、その後、手動ステップを最小限にするために必要に応じて更新が自動的に行われてもよい。

20

【0188】

スマートカードクラス証明書は、ディレクトリサービス1241（たとえば、ADドメイン）によって、関連するユーザアカウント用のインタラクティブログオン資格情報として信頼されてもよい。換言すれば、証明書は仮想スマートカードとして、たとえば、スマートカードクラスユーザ証明書として扱われてもよい。証明書は、資格情報マッパーサーバ1229上の鍵ストアに保持された対応する秘密鍵を用いた、Kerberosなどを介したADログオンのための適切な鍵使用が可能であってもよい。ハードウェアベースの鍵の保護が、たとえば、信頼済みプラットフォーム（たとえば、WINDOWS（登録商標）トラステッドプラットフォームモジュール（TPM））及び／またはハードウェアセキュリティモジュール（HSM）を介して、秘密鍵に対して使用されてもよい。ハードウェアベースの鍵の保護はまた、ログオンレイテンシを有益に短縮するために使用されてもよい。

30

【0189】

アプリケーションストア1225の認証拡張1227は、アプリケーションストア1225の起動シーケンス中に（及び任意選択でアプリケーションストア1225のログオンシーケンス中に）資格情報マッパー1229とインタラクトして、ユーザ用の仮想スマートカードを準備するようにしてもよい。ユーザ用の仮想スマートカードはオンデマンドで、たとえば、起動もしくは再接続イベントのたびに作成されてもよく、または様々なセキュリティポリシー及びパフォーマンスニーズに応じて一定の期間の間、再使用されてもよい。仮想スマートカードは、事前に作成されてもよく、特に上述のように秘密鍵へのハードウェア保護が存在する場合には、物理スマートカードに使用されるものに近い有効期間を有してもよい。

40

【0190】

仮想化サーバ1237の資格情報プラグイン1239は、ログオン中に仮想スマートカードを使用する関連するオペレーティングシステムコールをインターセプトして、資格情報マッパーサーバ1229に特定の動作をリダイレクトしてもよく、そこでそれらが暗号API及びプロバイダを使用して実行されることになる。

50

【0191】

図12Bに、本明細書に記載の1つまたは複数の例示的な態様によるフェデレーテッドログオンのためのさらに他の例示的なシステムを示す。図12Bに示す認証システムは、図12Aを参照して説明した認証システムと類似し得る。しかしながら、アイデンティティ確認（たとえば、SAMLトークン）を使用する代わりに、クライアントエージェント1201は、ワンタイムパスワード（OTP）または実際のスマートカード資格情報を、リソースシステム1221内のコンポーネントのうちの1つまたは複数、たとえばゲートウェイサーバ1223に送ってもよい。ゲートウェイサーバ1223は、以下でさらに詳細に説明するように、ベンダー認証サービス1251を用いてクライアントまたはユーザーを認証してもよい。また、ゲートウェイサーバ1223は、同じく以下で説明するように、RADIUSまたはRESTプロトコルを使用して認証サービス1251と通信してもよい。

10

【0192】

図12Cに、本明細書に記載の1つまたは複数の例示的な態様によるフェデレーテッドログインのための他の例示的なシステムを示す。図12Cに関して説明するコンポーネントを使用して、仮想スマートカードを作成して使用することによって、ユーザセッション（たとえば、仮想デスクトップセッション）を開始してもよい。ユーザアカウントを保持するADドメインは、証明書サービス1231などの認証局（CA）によって発行されたスマートカードクラスユーザ証明書をフルADドメインログオンに使用することを可能にするために、正しいフォームの事前に築かれた信頼を有してもよい。最初に、いくつかのデプロイメントステップが実行されてもよい（図示せず）。たとえば、システムは、資格情報マッパー1229をデプロイし、図12Cに示すコンポーネント間に信頼を築くためのステップ（これは手動ステップでもよい）を実行してもよい。

20

【0193】

資格情報マッパー1229は、CAへの登録局（たとえば、登録エージェント）を含んでもよい。資格情報マッパー1229は、組織のCA管理者（たとえば、セキュリティ責任者）による手動承認を使用し得るブートストラップ証明書テンプレートを使用してCAによって発行されたクライアント証明書などの自身の資格情報を要求してもよい。最初の証明書が発行されると、第2の証明書テンプレートは、RA証明書のロールオーバーが自動的に処理されることを可能にし得る。ロールオーバーは、現在の証明書の有効期限が近づくと、新たな証明書を発行することを含んでもよい。

30

【0194】

また、第2の証明書テンプレートによって、資格情報マッパー1229の1つのインスタンスは、他のサーバがグループに参加し、資格情報マッパー1229の他のインスタンスをホストすることを許可することが可能になり得る。これは、セットアップ及び継続的な保守の運用負担を最小限に抑えながら、スケールアウト及び冗長性のために使用されてもよい。これは、この機能のユーザが、高可用性を維持しながら、そのような証明書ベースのデプロイメントを運用及び保守する専門家ではない場合に有益であり得る。

【0195】

ここで、図12Cを参照して例示的な流れを説明する。クライアントエージェント1201（またはブラウザ）は、ゲートウェイサーバ1223にログオンしてもよい。一部の態様では、ワンタイムパスワード（OTP）がADパスワードの代わりに使用されてもよい。ユーザにOTPが発行されてもよい。代替的には、他の認証資格情報、たとえば、SAMLトークン、スマートカード資格情報、チャレンジ/応答資格情報、Kerberos資格情報、バイオメトリクス、PINなどが、OTPの代わりに使用されてもよい。ステップ1270において、クライアントエージェント1201（またはクライアントデバイス上のブラウザ）は、ゲートウェイサーバ1223にOTPを送ってもよい。ADパスワードが使用されないため、ゲートウェイサーバ1223は、アプリケーションストア1225に（たとえば、シングルサインオンで）サインオンするためにパスワードを使用できない場合がある。その代わりに、ステップ1272において、ゲートウェイサーバ12

40

50

23は、ベンダー認証サービス1251を介してユーザを認証してもよい。たとえば、ゲートウェイサーバ1223は、リモート認証ダイヤルインユーザサービス(RADIUS)ネットワークプロトコル、軽量ディレクトリアクセスプロトコル(LDAP)、表現可能状態転送(REST)ネットワークプロトコル、またはOTPに基づいてユーザを認証するための他の任意のタイプのネットワークプロトコルを使用してもよい。ゲートウェイサーバ1223は、たとえば、平文のユーザ資格情報が、RADIUS、LDAP、またはRESTなどの転送プロトコルの一部として暗号化されたものを送ってもよい。認証サービス1251は、平文の資格情報を復元し、それらを有効性検証してもよい。認証サービス1251は、資格情報が有効であるか否かを折り返し報告し、場合によっては追加のアイデンティティ情報、たとえば、正規のユーザ名及びグループIDを供給してもよい。

10

【0196】

ステップ1274において、ゲートウェイサーバ1223は、シングルサインオンプロトコルを介して、ユーザのアイデンティティ(たとえば、ADアイデンティティ)をアプリケーションストア1225に送ってもよい。ゲートウェイサーバ1223はまた、セキュリティコンテキスト情報をアプリケーションストア1225に送ってもよい。ステップ1274で送られる例示的な情報には、認証方法、クライアントデバイス上で実行されたスキャンを識別する情報、及び／またはクライアントデバイスの位置が含まれる。ゲートウェイサーバ1223によって開始されるSSOセッション中に、いくつかのステップが行われてもよい。

【0197】

20

ステップ1276において、アプリケーションストア1225は、資格情報マッパー1229(たとえば、ユーザ資格情報サービス)に連絡して、Windows(登録商標)のADログオンを有効化するために、一致するユーザ証明書及び秘密鍵が利用可能であることを確認してもよい。ゲートウェイサーバ1223によってアプリケーションストア1225に渡されたセキュリティコンテキスト情報の一部または全部が、ユーザ証明書に組み込むために資格情報マッパー1229に送られてもよい。コンテキスト情報は、要約、補足、またはマッピングされた形で送られてもよい。アプリケーションストア1225は、どのようなセキュリティコンテキスト情報が資格情報マッパー1229に渡されるかを制御してもよい。渡され得る他の情報は、セキュリティグループ(たとえば、WINDOWS(登録商標)セキュリティグループ)に関連付けられた役割ラベルを含んでもよい。役割ラベルは、生のセキュリティコンテキスト情報に基づいて選択されてもよく、顧客のセキュリティポリシーの決定事項であってもよい。ユーザがセキュリティグループに追加されてもよい。

30

【0198】

アプリケーションストア1225はまた、Kerberosまたはデバイス証明書を使用するなどして、資格情報マッパー1229へ認証してもよい。マシンレベル認証を使用する場合、資格情報マッパー1229は、資格情報ハンドルを要求するのに信頼済みのマシンのホワイトリストを実装してもよく、これは後で(たとえば、異なる信頼済みマシンのセットにより)ログオンのために使用することができる(たとえば、ユーザの偽装)。代替的には、アプリケーションストア1225は、Kerberos制約付き委任(KCD)及びプロトコル遷移を使用して、直ちにユーザに偽装し、資格情報マッパー1229へのKerberosユーザ認証を実行してもよい。これにより、標準的なAD制御をKCDに使用してホワイトリストを管理することが可能になり得る。これはまた、ユーザの偽装から除外することができる、管理者などの特定の機密性が高いユーザアカウントをブラックリストに載せるメカニズムを提供し得る。

40

【0199】

ステップ1278において、資格情報マッパー1229は、資格情報マッパー1229が特定のユーザ用の証明書を要求することを可能にする事前に確立された許可に基づいて、証明書サービス1231(CA)への登録局(たとえば、登録エージェント)として機能してもよい。アプリケーションストア1225によって提供された役割ラベルを使用し

50

て、資格情報マッパー 1 2 2 9 は、特定のセッション用の証明書を取得するために使用する C A と証明書テンプレートとの組み合わせを決定してもよい。顧客は、A D の認証メカニズム保証機能及びエンタープライズ証明書サービス（たとえば、W I N D O W S（登録商標） S E R V E R 2 0 0 8）を使用して、これらの証明書に基づくユーザセッションを W I N D O W S（登録商標）セキュリティグループなどの特定のセキュリティグループに所属させることができる。これにより、標準的な W I N D O W S（登録商標）アクセス制御リスト（A C L）を使用して、仮想化セッション 1 2 3 7 に、ネットワークリソースへのアクセスを許可または拒否することが可能になり得る。A C L は、被信頼者（t r u s t e e）を識別し、被信頼者に対するアクセス権を指定するために使用されるアクセス制御エントリ（A C E）をリスト化してもよい。

10

【0 2 0 0】

資格情報マッパー 1 2 2 9 は、デプロイメント中にプロビジョニングされたその R A 証明書を使用して、そのサービスアイデンティティを証明書サービス 1 2 3 1 に対して証明してもよい。これは、証明書サービス 1 2 1 3 によって、要求された証明書テンプレートへのアクセスを許可または拒否し、ひいては証明書発行要求 1 2 7 8 を許可または拒否するために使用されてもよい。W I N D O W S（登録商標）エンタープライズ証明書サービスは、どのエンティティが証明書を発行することができるか、また、どの対象に対してかについて制限することを可能にする証明書テンプレート及び登録エージェントの A C L を許可してもよい。

20

【0 2 0 1】

ステップ 1 2 8 0 において、資格情報マッパー 1 2 2 9 がセッションに適切なユーザ証明書を作成または配置すると、資格情報マッパー 1 2 2 9 は、アプリケーションストア 1 2 2 5 にセキュアなハンドルを返してもよく、これは仮想化マシンが後で証明書資格情報にアクセスするために使用することができる。返されたハンドルは、O A u t h トークンと類似していてもよい。たとえば、ハンドルは、サーバのアイデンティティタグなどの他の情報と組み合わせられたセキュアな乱数を含んでもよく、これは後で他のマシンからのネットワークアクセスを可能にする。ハンドルは、純粋にベアラ所持トークンとして使用可能でなくてもよい。むしろ、トークンは、（たとえば、K e r b e r o s またはマシン証明書を使用して）自身のアイデンティティを独立して証明することができ、許可済みマシンのホワイトリスト上にあるマシンによって提示された場合に、使用されてもよい。

30

【0 2 0 2】

ステップ 1 2 8 2 において、アプリケーションストア 1 2 2 5 がユーザのパスワードをキャッシュし得る方法と同様に、アプリケーションストア 1 2 2 5 は資格情報ハンドルをキャッシュしてもよい。そのサイズ及び他の考慮事項に応じて、ハンドルは、アプリケーションストア 1 2 2 5 の認証サービスにより発行された S A M L 認証トークン内にそのままの形で配置されて、クライアントエージェント 1 2 0 1 または他のコンポーネントによってキャッシュされてもよい。代替的には、ハンドルは、アプリケーションストアサーバ 1 2 2 5 上に維持される資格情報ホルダまたはボルト内に配置して、処理が後でハンドルを要求した場合にアクセスできるようにしてもよい。アプリケーションストア 1 2 2 5 のログオンプロセスは、この段階で完了してもよい。

40

【0 2 0 3】

ステップ 1 2 8 4 において、ゲートウェイサーバ 1 2 2 3 及び／またはアプリケーションストア 1 2 2 5 によるログオンの後に、リソース起動要求が行われてもよい。資格情報ハンドルが、アプリケーションストア 1 2 2 5 の S A M L 認証トークンから直接的または間接的に復元されてもよい。起動処理の一部として、後に行われ得るディスプレイリモート接続に備えて、ユーザのセッション（たとえば、W I N D O W S（登録商標）セッションなどの仮想化セッション 1 2 3 7）をホストするマシンに、デスクトップコントローラコンポーネント 1 2 6 1 を介して、ハンドルが転送されてもよい。たとえば、ハンドルは、リモートアプリケーションまたはデスクトップコントローラ 1 2 6 1 を使用して、仮想化セッション 1 2 3 7 に渡されてもよい。セッションは仮想デスクトップまたは仮

50

想アプリケーションセッションを含んでもよく、ホスト1237は一度に1つのユーザセッション専用であってもよく、または（たとえば、リモートデスクトップサービスを使用して）複数の独立したユーザセッションを可能にし得る。ユーザセッションは、これが再接続イベントである場合には既に存在し得、またはこれが初回の起動イベントである場合には、まもなく作成され得る。セッションホスト1239は、ハンドルを受信してもよく、ディスプレイリモート接続を待つ間、一時的にハンドルをキャッシュしてもよい。ハンドルはまた、ハンドルを開示するリスクを最小化するために、送信及びキャッシングステップの前に暗号化されてもよい。ハンドルを復号するための鍵は、通常のクライアントエージェント起動ファイルの一部として、ログオンチケットの形でクライアントエージェント1201に送られてもよい。

10

【0204】

ステップ1286において、クライアントエージェントのエンジンは、アプリケーションストア1225から受信したクライアントエージェント起動ファイルを使用して始動されてもよい。クライアントエージェント1201は、クライアントエージェントセッションネゴシエーションの一部として、セッションホスト1237にログオンチケットを提示してもよい。図示していないが、クライアントエージェントの接続は、別の許可チケットを必要とするゲートウェイサーバ1223を介してプロキシされてもよい。

【0205】

ステップ1288において、ログオンチケットを使用して復号鍵を導出することによって、資格情報ハンドルを復元し、これを使用して、資格情報動作が資格情報マップパー1229によって実行されることを要求してもよい。要求された動作は、ユーザ証明書自体を取得する動作など、スマートカードログオンをリモートで実行するため、1つまたは複数の署名動作を実行するため、及び／または1つまたは複数の復号動作を実行してKerberosセッション鍵をラッピング解除するために使用されてもよい。代替の形態のインタラクションは、仮想化エージェント1237上で直接（たとえば、ジャストインタイムで）一時的な仮想スマートカードを作成することであってもよい。この例では、CSPは、鍵のペアを作成し、次いで、通常の証明書取得要求の代わりに、公開鍵の証明書署名要求を資格情報マップパー1229に送ってもよい。この要求は、証明書ハンドルを使用し、マシン認証を使用して行われてもよい。

20

【0206】

資格情報マップパー1229は、前述のように、役割及び他のセキュリティコンテキスト情報に基づいてユーザ用の証明書を要求する。証明書は仮想化エージェント1237に返されてもよいが、鍵がローカルに存在するときに、残りの仮想スマートカード動作がローカルで実行されてもよい。

30

【0207】

資格情報マップパー1229は、鍵のペアを作成しないように修正されてもよい。その代わりに、資格情報マップパー1229は、ユーザ証明書（たとえば、ユーザアイデンティティ、役割、または他のセキュリティコンテキスト情報）を取得するための関連情報を覚えてもよい。資格情報ハンドルは、その情報を使用して既に準備された仮想スマートカードではなく、この情報への参照であってもよい。

40

【0208】

高速スマートカードログインの場合と同様に、CSPは多くまたはほとんどの動作を仮想化エージェント1237上の他のCSP（たとえば、標準CSP）に委任してもよい。フルフェデレーテッドログオンの場合、標準CSPは、TPMまたは他のHSMを活用して強力な鍵の保護または高速化機能を提供することができるCSPで構成されてもよい。鍵は、セッション中の使用できるように維持されてもよい。鍵はまた、ログオンに使用するのに十分に長くメモリに保持され、その後破棄されてもよい。前述の例では、暗号動作を仮想化エージェント1237にわたって分散させて、資格情報マップパー1229への負荷を軽減してもよい。

【0209】

50

セッションホストマシン（たとえば、仮想化セッション1237）は、たとえばKerberosまたはデバイス証明書を使用して、資格情報マップパー1229へ認証してもよい。資格情報マップパー1229は、ユーザログオン（たとえば、ユーザの偽装）を実現するためにこのように資格情報ハンドルを使用するのに信頼済みのマシンのホワイトリストを実装してもよい。

【0210】

図13に、本明細書に記載の1つまたは複数の例示的な態様によるアプリケーションストア1225、資格情報マップパー1229、及び仮想化エージェント1237の間の例示的なインタラクションを示す。この例では、前述の高速スマートカードログオン用のコンポーネントが、フェデレーテッドフルドメインログオンを実装するために再使用され得る。たとえば、資格情報マップパー1229は、ネットワーク仮想スマートカードのように機能してもよいが、前述のように、スマートカード1290が一時的なものであって、SAMLトークンまたは他の信頼済みアイデンティティ確認に基づいて発行されてもよいことを除く。また、ワンショットログオンチケット（または前述の証明鍵）が、ブローカーまたは資格情報マップパー1229によって、リモートセッション起動要求をリモートディスプレイプロトコル接続にリンクさせるために生成されてもよい。

【0211】

証明鍵が使用され得る複数の方法が存在し、そのいくつかは上述している。他の方法は、クライアントエージェントが、IDPへの認証中にSAML認証トークンにリンクされる証明鍵を有してもよいというものである。この証明鍵はまた、仮想スマートカード証明書にリンクされてもよく、この証明鍵を必要とするクライアントエージェントと仮想化エージェントとの間のインタラクションは、仮想スマートカードが使用可能になる前に行われてもよい。仮想化エージェントは、クライアントエージェントが（たとえば、仮想スマートカードを使用するための前提条件として）証明鍵を所持しているか否かを確認してもよい。代替的には、仮想化エージェントは、クライアントエージェントと資格情報マップパーとの間の間接的なインタラクションを仲介してもよい。仲介を使用して、仮想スマートカード動作を許可する前に証明鍵の所持を証明してもよく、または場合によっては、仲介を使用して、仮想スマートカードの秘密鍵を復号することができる。

【0212】

アプリケーションストア1225は、認証サービス1227（たとえば、ログオンデータプロバイダ拡張）を呼び出して、1つまたは複数の起動要求についてのカスタムログオンデータを取得してもよい。ステップ1305において、認証サービス1227は、資格情報マップパー1229からログオンデータを取得してもよい。資格情報マップパー1229との最初のインタラクションはまた、起動中の遅延の最小化を支援するためにアプリケーションストア1225のログオン中に行われてもよい。資格情報マップパー1229からのログオンデータは、資格情報マップパー1229によって管理される仮想スマートカード1290への参照を含んでもよい。アプリケーションストア1225は、資格情報マップパー1229からログオンデータを受信してもよい。

【0213】

ステップ1310において、アプリケーションストア1225は、ログオンデータを暗号化し、暗号化したデータをデリバリーコントローラ1235に送ってもよい。ステップ1310は、たとえば、クライアントのログオンステップ中に実行されてもよい。一部の態様では、デリバリーコントローラ1235に送られる暗号化されたログオンデータは、無署名であってもよい。ステップ1315において、デリバリーコントローラ1235は、暗号化されたログオンデータを仮想化エージェント1237に送ってもよい。ステップ1315は、暗号化されたユーザ名及びパスワードが標準的な起動要求中に渡されるのによく似たように、セッション準備中などに実行されてもよい。アプリケーションストア1225は、暗号化鍵またはそれを導出できるランダム値をクライアントエージェントファイル内にログオンチケットとして入れてもよい。

【0214】

仮想化エージェント 1237 は、資格情報プラグイン 1239（図 12A～図 12C などに図示）を含んでもよく、資格情報プラグイン 1239 は、仮想化エージェント 1237 に事前に登録されてもよい。資格情報プラグイン 1239 は、特定の資格情報タイプに関連付けられてもよく、その資格情報タイプは、アプリケーションストア 1225 によって、仮想化エージェント 1237 に送られたログオンデータを用いて宣言されてもよい。

【0215】

前述のように、KCD がログオンに使用されてもよい。KCD の実装では、アプリケーションストア 1225 からのカスタムログオンデータは、アプリケーションストア 1225 が発行したトークンまたはチケットを提示してアプリケーションストア 1225 に（または資格情報マッパー 1229 に）認証されたコンタクトを返すように、異なる仮想化エ
10
ージェント 1237 の資格情報プラグインに指示してもよい。アプリケーションストア 1225 は次いで KCD を使用して、ユーザアイデンティティを仮想化エージェント 1237 にジャストインタイトムで委任してもよい。この実装は、デリバリーコントローラ 1235 に対する XML インターフェースと、仮想化エージェント 1237 に対するブローリングプロトコルインターフェースとを介して、フル Kerberos 委任チェーンを構築することを回避してもよい。仮想化エージェントの資格情報プラグインは次いで認証パッケージを呼び出して、KCD からのネットワークログオントークンをフルインタラクティブログオントークンに変換してもよい。

【0216】

クライアントとの接続が行われ、ログオンチケットが提示された場合、仮想化エージェント 1237 は自動ログオン処理を実行してもよい。たとえば、仮想化エージェント 1237 は、資格情報プロバイダ 1292 に信号を送ってもよく、これはワークステーションセッションなどのために登録されてもよい。資格情報プロバイダの代わりに、資格情報プロバイダフィルタが、リモートデスクトップセッションの場合などに、使用されてもよい。
20
。ステップ 1315 で受信した暗号化ログオンデータを復号し、検査して、資格情報タイプを特定してもよい。資格情報タイプはカスタム資格情報タイプであってもよいので、復号されたデータが、登録された資格情報プラグインに渡されてもよい。資格情報プラグインは、WINDOWS（登録商標）のログオンシステム（または他の任意の OS のログオンシステム）によって使用される、適切なシリアル化された資格情報構造を生成してもよい。シリアル化された資格情報は、処理のために資格情報プロバイダ 1292（またはフ
30
ィルタ）から返されてもよい。

【0217】

資格情報プラグイン 1239 は、前述のように、KERB__CERTIFICATE__LOGON 構造体を生成してもよい。KERB__CERTIFICATE__LOGON 構造体は、スマートカードメインログオンが実行されることをオペレーティングシステムに示してもよい。前述のように、データ構造は、スマートカードとのインタラクションに使用されるドライバ（たとえば、CSP 1294 などの CSP または KSP）への参照を含んでもよい。ステップ 1320 において、CSP 1294 は次いで、仮想スマートカードが存在する資格情報マッパー 1229 に関連する動作をリダイレクトしてもよい。

【0218】

仮想化エージェント 1237 が特定の仮想スマートカードを使用するための許可は、二重にされてもよい。第 1 に、仮想化エージェント 1237 が、資格情報マッパー 1229 によって信頼済みのホストのホワイトリストにあることが確認されてもよい。第 2 に、仮想化エージェント 1237 がセッションの準備中にデリバリーコントローラ 1235 から参照を受信したことが確認されてもよい。アプリケーションストア 1225 とデリバリー
40
コントローラ 1235 との間のリソース起動インタラクションの性質のため、アプリケーションストア 1225（ひいては資格情報マッパー 1229）は、仮想スマートカード参照を取得する際にデリバリーコントローラ 1235 によって選択される仮想化ホスト 1237 のアイデンティティを知らない場合がある。したがって、仮想スマートカード参照は、任意の信頼済みの仮想化ホストによって使用可能になるように選択され得る。任意の信
50

頼済みの仮想化エージェントホストは、資格情報参照を使用して、仮想スマートカードをローカルに作成することができる。

【0219】

図14に、本明細書に記載の1つまたは複数の例示的な態様によるフェデレーテッドログオンのためのさらに他の例示的なシステムを示す。仮想化デプロイメントの観点から、図14（ならびに前述の図12A～図12C）に示したコンポーネントによって実行されるステップは、SAMLを介した参照チケットなどの従来のチケットログオンモデルに類似したモデルであってもよい。

【0220】

前述のように、クライアントデバイス1401は、アイデンティティプロバイダからSAML認証トークンを受信してもよい。フルドメインアクセスを有するために、クライアントデバイス1401は、認証のためにアプリケーションストア1411にSAMLトークンを送ってもよい。アプリケーションストア1411は、ブローカーエージェントサービス1423及び／またはサーバ1421のデリバリーコントローラにSAMLトークン（たとえば、ユーザの平文のパスワードではない）を送ってもよく、これを使用して参照チケットを要求してもよい。SAMLトークンは、クライアント1401によって送られたSAMLトークンと同じであってもよく、またはサードパーティIDPによって修正されてもよい。（たとえば、デリバリーコントローラが資格情報マッピングサービス1425を用いてSAMLトークンを検証することによって）SAMLトークンが受諾可能であるとサーバ1421が判定した場合、サーバ1421は、ユーザのチケット（これは一時的なものでもよい）を作成し、また、作成したチケットを参照または識別する参照チケットを返してもよい。たとえば、資格情報マッピングサービス1425は、PKCS10要求を生成して認証局（CA）1431に送り、この段階でCA1431から証明書を取得してもよい。チケットはサーバ1421に、たとえば資格情報マッピングサービス1425に記憶されてもよい。サーバ1421はアプリケーションストア1411に参照チケットを送ってもよく、アプリケーションストア1411は、セルフサービスプラグイン1403を介してクライアント1401に参照チケットを送ってもよい。一方、SAMLアサーションが資格情報マッピングサービス1425によって却下された場合に、「アクセス拒否」エラーコードが代わりにアプリケーションストア1411に返されてもよい。

【0221】

クライアントデバイス1401は、参照チケットをフルドメインログオンと引き換えてもよい。たとえば、クライアントエージェント1405は、セルフサービスプラグインから参照チケットを受信し、任意選択で参照チケットを記憶し、転送（たとえば、リモートイング）プロトコルを使用して参照チケットを仮想化マシン1441に送ってもよい。仮想化マシン1441は、参照チケットをサーバ1421に、たとえば、サーバ1421のデリバリーコントローラ（たとえば、DDC）（図示せず）に送ってもよい。チケットはCITRIX接続ブローカリングプロトコル（CBP）などのブローカープロトコルによって送られてもよい。仮想化マシン1441は、参照チケットがSAMLアサーションログインを表すか否かを、ブローカーに送るまで知らない場合がある。ブローカーからの応答は、平文パスワード、または公開鍵PKCS7認証証明書チェーンを含む新たな応答構造のいずれかであってもよい。

【0222】

参照チケットを受信した後、デリバリーコントローラは、（参照チケットに含まれる情報に基づいて）チケットが平文パスワード認証プロセスではなく資格情報マッピングサービス1425の認証プロセスに使用されたと判定してもよい。したがって、仮想化マシン1441に平文のパスワードを返すのではなく、デリバリーコントローラは、資格情報マッピングサービス1425によって以前に生成及び／または記憶されたログオン証明書を返してもよい。

【0223】

図12A～図12Cを参照して前述したように、サーバ1421のコンポーネントは、

10

20

30

40

50

参照チケットが正しくかつタイムリーである（たとえば、特定の期間内に引き換えられる）ことを検証してもよい。ブローカーは、SAMLアサーションを表す有効な参照チケットを受信した場合、仮想化マシン1441と資格情報マッピングサービス1425との間のプロキシとして機能してもよい。

【0224】

証明書が提供されると、クライアント1401には、ブローカープロトコルを介した秘密鍵署名動作へのアクセスが与えられてもよい。仮想化マシン1441は、ADスマートカード認証を使用して、ユーザをログインさせてもよい。最初の通信パッケージは、公開PKCS7証明書チェーンの要求であってもよい。仮想化マシンからの後続の要求は、秘密鍵署名動作に関するものであってもよい。

10

【0225】

様々なセキュリティポリシーが使用され得る。資格情報マッピングサービス1425には、認証局1431（たとえば、MICROSOFT認証局）への特権的アクセスが付与されてもよい。認証局1431はユーザ用の証明書を発行してもよい。認証局1431によって資格情報マッピングサービス1425に課せられるあらゆる制限に加えて、セキュリティポリシーのクラスが、資格情報マッピングサービスの管理者によって構成されてもよい。第1に、どのユーザがログインできるかが制御されてもよい。アクセス制御リスト（ACL）は、資格情報マッピングサービス1425を使用して、誰の認証を許可できるか及びできないかを指定してもよい。たとえば、ドメイン管理者グループのどのメンバーもこのようにアクセスすることを許可されないことが決定されてもよい。第2に、どの仮想化マシンがチケットを引き換えてよいかが制限されてもよい。ブローカーの要求時に、チケットは、指名された仮想化マシン（たとえば、Kerberosドメインアカウントまたは信頼エリアRID）によって引き換え可能であってもよい。資格情報マッピングサービス1425は、仮想化マシンのリストを制限することが可能であってもよい。たとえば、1つの仮想化マシンカタログが、本明細書に記載のメカニズムを使用して認証を許可されるべきであると決定されてもよい。

20

【0226】

第3に、証明書の有効期間が使用されてもよい。証明書は、数分などの短い期間に使用可能であってもよい。これは認証局1431を介して制御可能であってもよい。より長い有効期間の証明書が望ましい場合、失効システムが、たとえばユーザのログオフによってトリガまたは実行されてもよい。代替的には、より長い有効期間のネットワーク仮想スマートカードが利用されてもよい。ネットワーク仮想スマートカードは、たとえば、ハードウェアセキュリティモジュールまたはトラステッドプラットフォームモジュール（TPM）を使用して仮想スマートカード秘密鍵を暗号化することによって、より高いセキュリティレベルまで保護されてもよい。代替的には、各秘密鍵が、特定のクライアントエージェントによって保持される永続的な証明鍵にリンクされてもよい。仮想スマートカードは、ログオフ時に失効されなくてもよく、資格情報マッピングサービス1425によって永続的に記憶することができる。したがって、資格情報マッピングサービス1425に記憶された仮想スマートカードは、長期間にわたって（たとえば、セッションの期間中に、ドメインログオンのためだけではなく）再使用されてもよく、その理由は、（特定の仮想化ホストではなく）仮想スマートカードのより強力な保護及び他のパフォーマンス上の利益を提供し得る資格情報マッピングサービス1425に記憶されているためである。

30

40

【0227】

第4に、証明書のキャッシング及び有効性の再検証が制御されてもよい。証明書は、最初の認証と、その後のデスクトップのロック解除動作との両方に使用されてもよい。デフォルトでは、証明書はある期間だけキャッシュされてもよいが、新たなSAMLトークンを提出することによって新たな証明書が生成されるポリシーを構成することを管理者は望む場合がある。第5に、SAMLアサーションの検証が実装されてもよい。SAMLトークンの検証に対する標準的な制御が提供されてもよい。Windows（登録商標）のUPNを主張するSAMLトークンが最初に許可されてもよく、これにはサードパーティI

50

d P の特別な構成が必要な場合がある。

【0228】

他の様々なセキュリティ制御が、本明細書に記載のコンポーネントのために構成されてもよい。たとえば、ディレクトリサービス（たとえば、AD）の管理者などの管理者が、ユーザドメインごとに、関連するCAの信頼を手動で構成してもよい。たとえば、管理者は、ルートまたは下位ルート証明書などの証明書を保護されたデータストアに、たとえば、AD内のMICROSOFTのNTAuth証明書ストアにインポートしてもよい。これらの証明書をインポートすることにより、関連するCAがスマートカードまたはドメインコントローラのタイプの証明書を発行するのに信頼されていることが示され得る。WINDOWS（登録商標）証明書サービスが企業CAとしてデプロイされている場合、証明書のインポートは自動的に実行されてもよい。

10

【0229】

CA管理者はまた、たとえば、3つの証明書テンプレートをインポートまたは作成してもよい。第1のテンプレートは、データセンターサーバ内の初期信頼をブートストラップするために使用されてもよく、これにより仮想化コンポーネント及びサービスが提供され得る。第2のテンプレートは、データセンターサーバの資格情報の自動化された証明書の更新と、クラスタに参加する新たなデータセンターサーバの資格情報の発行と、を可能にするために使用されてもよい。第3のテンプレートは、ユーザ用のスマートカードログオン証明書を発行するために使用されてもよい。CAは、どのデータセンターサーバがテンプレートを使用できるかを決定するアクセス制御を有してもよい。

20

【0230】

他のセキュリティ制御は、データセンターサーバからの証明書要求への信頼をブートストラップするための、CA管理者による手動の承認を含んでもよい。さらに他のセキュリティ制御は、データセンターサーバ自体が、セキュリティ制御のセットを実装して、仮想スマートカードの作成を要求することが許可されたアプリケーションストアサーバと、ログオンに仮想スマートカードを使用することが許可された仮想化マシンと、を識別することを含んでもよい。それはまた、このように偽装することができるユーザのセットを識別または制限するための制御を有してもよい。

【0231】

資格情報マッピングサービスの例示的な実施形態

30

前述の資格情報マッピングサービスの実施形態は、様々な方法で実装されてもよい。1つの目標は、ユーザが証明書を使用してActive Directoryユーザアカウントに簡単かつ迅速にログオンできるシステムである。

【0232】

一態様では、本明細書に記載のリモートサービスは、クライアントデバイス上のクライアントエージェントに配置されてもよい。これらの態様では、クライアントエージェントはユーザのスマートカードを直接使用して、認証ステップを実行してもよい。これは、前述のように、新たな仮想チャネルを使用してもよい。

【0233】

他の態様では、リモートサービスは、前述のように、資格情報マッピングサービスを含んでもよい。このサービスは、企業向けMICROSOFT認証局などの認証局を使用して、オンザフライでスマートカード証明書を発行及び記憶するために使用されてもよい。代替的には、証明書は事前に作成されてもよい。認証局と組み合わせた資格情報マッピングサービスを使用して、認証ポリシーの様々な態様を施行してもよい。

40

【0234】

図15に、本明細書に記載の1つまたは複数の例示的な態様による資格情報マッピングサービスを提供するための例示的なシステムを示す。サードパーティIdP1551は、アイデンティティ確認トークン（たとえば、SAMLトークン）をフェデレーションサーバ1553に送ってもよい。フェデレーションサーバ1553はトークンをアプリケーションストア1511に送ってもよく、アプリケーションストア1511はトークンをデリ

50

10

20

30

40

50

50

50

50

50

50

50

50

高速スマートカードログオン機能について、WINDOWS（登録商標）のPKI NI

Tログオンシステムとの統合があってもよい。資格情報プロバイダパッケージが、この認証システムと相互運用することになるサーバマシンにインストールされてもよい。これは、一部のシステムに既に含まれる資格情報プロバイダの拡張を含んでもよい。このパッケージの新機能は、C S Pを使用してP K I N I Tを用いてログインするようにW I N D O W S（登録商標）に指示することであってもよい。C S Pは究極的には、実際のログオン証明書を提供し、関連する秘密鍵動作を行うリモートプロセスと通信してもよい。仮想チャネルは、C S Pと、クライアント上で稼動する既存の認証マネージャプログラムとの間のコンジットとして機能してもよい。3つのトランザクション（または動作）は、「スマートカードユーザ証明書の取得」、「秘密鍵署名の実行」、及び「秘密鍵による復号」を含む。認証マネージャは、ローカルスマートカードを直接使用してP K動作要求を満たしてもよく、これによりユーザを仮想化マシンにログインさせてもよい。認証マネージャは、スマートカードを既にロック解除して、アプリケーションストアにログインし得るので、これはS S O機能も提供し得る。

10

【0241】

一部の追加の態様では、仮想チャネルを介してクライアントにP K動作要求を渡すのではなく、要求が資格情報マッピングサービス（C M S）に向けられてもよい。C M Sサーバはログオンを許可し、P K動作を実行してもよい。別個のサーバにインストールされた信頼済みのサービスが、C S PからのP K動作要求にサービスして、許可チェックを実行した後に適切なユーザをログインさせてもよい。デリバリーコントローラとの別個のセキュアな通信経路を有するので、C M Sは期待しているログオン要求を許可してもよい。C S Pによって提示される「シングルユースチケット」は、これを実現するための1つのメカニズムであってもよい。C M Sはスマートカード証明書を自動的に登録してもよい。ユーザログオンを実行するために、C M Sは内部で自動的にスマートカード証明書要求を生成し、それらをM I C R O S O F T認証局またはサードパーティC Aによって発行させてもよい。C S PからのP K動作要求は、これらの証明書に基づいてサービスされてもよい。C M Sは追加的に、シングルユースチケットから得られる鍵ラッピング鍵による暗号化を使用して、あるいはハードウェアセキュリティモジュールもしくはトラステッドプラットフォームモジュールまたは他の同様の手段を使用して、証明書用の秘密鍵を保護してもよい。

20

【0242】

一般的なセキュリティ要件が存在してもよい。秘密鍵は保護され、P K I N I T要求への署名に使用されてもよい。P K動作の秘密鍵署名要求にサービスするたびに、サーバは、署名するデータが適切なK e r b e r o sプロトコルデータに対応するA S N - 1構造であることを検査することにより、K e r b e r o sログオンを実際に実行していることを確認してもよい。他のデータ構造に秘密鍵動作を実行しようとする試みは、却下されてもよい。復号動作について、復号されたデータは、サーバに返す前に検査して、K e r b e r o sプロトコル動作に対応する期待されるA S N - 1構造を有することを確認してもよい。秘密鍵は仮想化マシン上で生成または記憶されなくてもよい。P K動作プロトコルは、ユーザがログインしているマシン上に秘密鍵が存在しなくてもよいようにしてもよい。秘密鍵は、クライアントマシン上のスマートカード内、または分離し得るC M Sサーバ内に存在してもよい。

30

40

【0243】

一部の実施形態では、ユーザはリモートセッション（たとえば、リモートアプリケーションまたはデスクトップセッション）に再接続してもよい。再接続は、異なる認証方法及び／または異なるセキュリティコンテキストを最初の起動として使用してもよい。再接続時には、クレームを、新たな認証方法、保証レベル、及び／または他のセキュリティコンテキスト情報、たとえば、位置及びデバイスなどを反映するように更新することができる。この更新は、（セキュリティグループのメンバーシップが追跡される場合は）K e r b e r o sチケットに、また、セッション証明書自体に情報を反映することに加えて行われてもよく、これを上述のようにT L Sクライアント認証に使用し、次いで他のサーバによ

50

って検査することができる。一部の態様では、証明書の事前作成を使用したり、上述のモデルをキャッシュしたりするのではなく、起動または再接続のたびに新たな証明書が生成されてもよい。

【0244】

起動と同様に、通常の（たとえば、WINDOWS（登録商標）または他のOSの）認証プロセスが、前述のように再接続のために行われてもよい。OSレベルで、この認証（たとえば、現在のログオン中のセッションユーザの再認証）を使用して、正しいユーザが存在しているためにセッションがロック解除され得ることを確認してもよい。ユーザが正しいユーザであることを確認した後、既存のセッションをアクセス可能にして、ユーザがユーザのアプリケーションを見て使用できるようにしてもよい。しかしながら、（再接続動作中にこの活動を指揮し得る）仮想化エージェントは、（セッションを起動するための最初の認証に基づく）セッション用のKerberosチケット情報が廃棄され、再認証中に得られた新たなKerberosチケットに置き換えられるように構成してもよい。OS内の既存のAPIを使用して、このようにKerberosチケットを破棄して置き換えてもよい。たとえば、WINDOWS（登録商標）コマンドklist.exeが使用されてもよい。更新された情報はまた、特別な方法で動作するOSの特定の部分、たとえば、ファイル共有アクセスを管理するサービスなどに伝播されてもよい。

10

【0245】

代替的には、最初のセッション証明書が新たな証明書に置き換えられてもよい。セッション証明書は、前述のログオン証明書であるが、セッション中に使用するのに十分に長い有効期間を有するものを含み、OSの証明書ストアに伝播して、アプリケーションにアクセスできるようにしてもよい。以前の証明書に基づくあらゆるアプリケーションレベルTLS接続状態をクリーンアップするために、ブラウザを再起動などして、新たな証明書を正しくピックアップするようにしてもよい。代替的には、属性権限モデルが使用されてもよい。たとえば、セッション証明書は、実際のセキュリティコンテキスト情報を含まなくてもよく、むしろその情報を知っているサービス、たとえば、前述の資格情報マッパーサービスなどへのポインタ（たとえば、適切なセッション参照を有するもの）を含んでもよい。TLSクライアント認証を使用するウェブサイトは、真の情報を知るために、この属性サービスを照会してもよい。

20

【0246】

関連出願の相互参照

本出願は、2018年8月24日に出願され、「FAST SMART CARD LOGON」と題された米国仮特許出願第16/111,328号の優先権を主張する。本出願はまた、2018年2月8日に出願され、「FAST SMART CARD LOGON」と題された米国仮特許出願第62/627,790号の優先権を主張する。本出願は、2015年9月30日に出願され、「FAST SMART CARD LOGON」と題された米国特許出願第14/870,435号と、2014年9月30日に出願され、「FAST SMART CARD LOGON AND FEDERATED FULL DOMAIN LOGON」と題された米国仮特許出願第62/057,344号とに関連する。各先行出願は、その全体が引用により本明細書に組み込まれる。

30

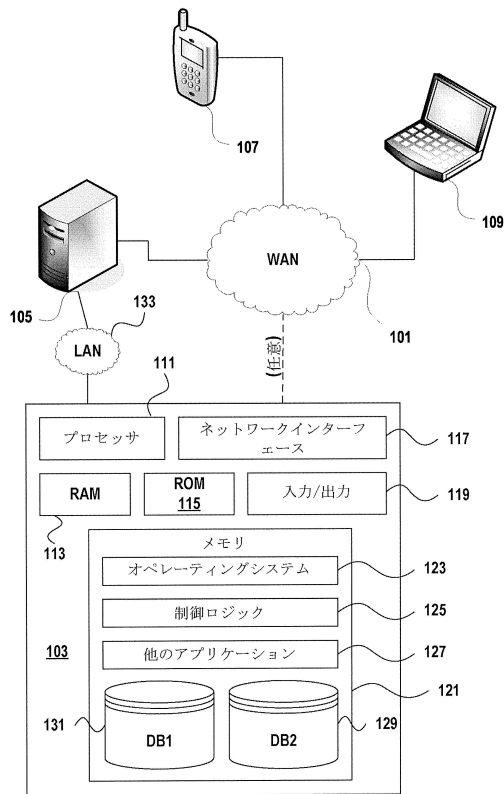
40

【0247】

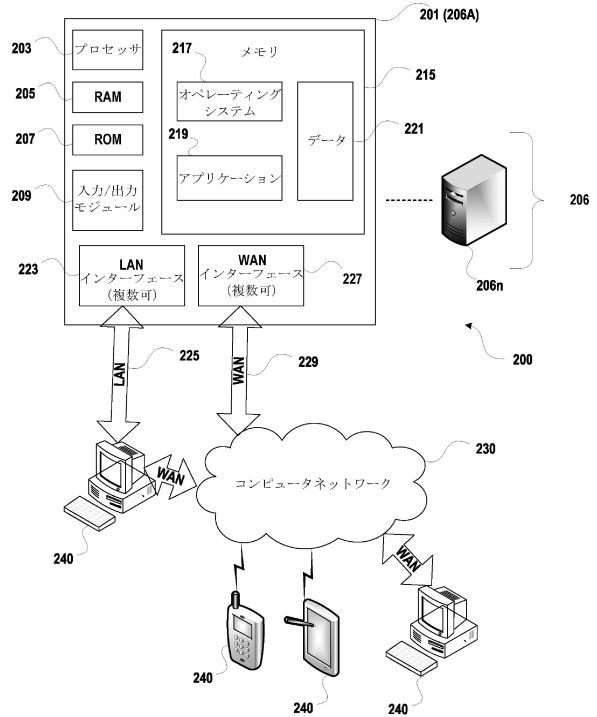
本主題は構造的特徴及び／または方法論的行為に特有の文言で説明してきたが、添付の特許請求の範囲で定義する本主題が必ずしも上述の特定の特徴または行為に限定されないことを理解されたい。むしろ、上述の特定の特徴及び行為は、添付の特許請求の範囲の例示的な実施態様として説明している。

【図 1】

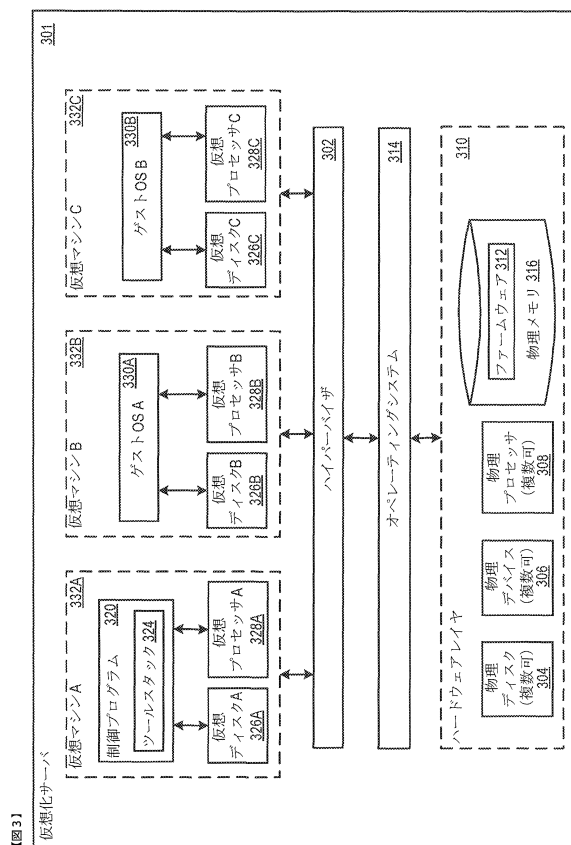
【図 1】



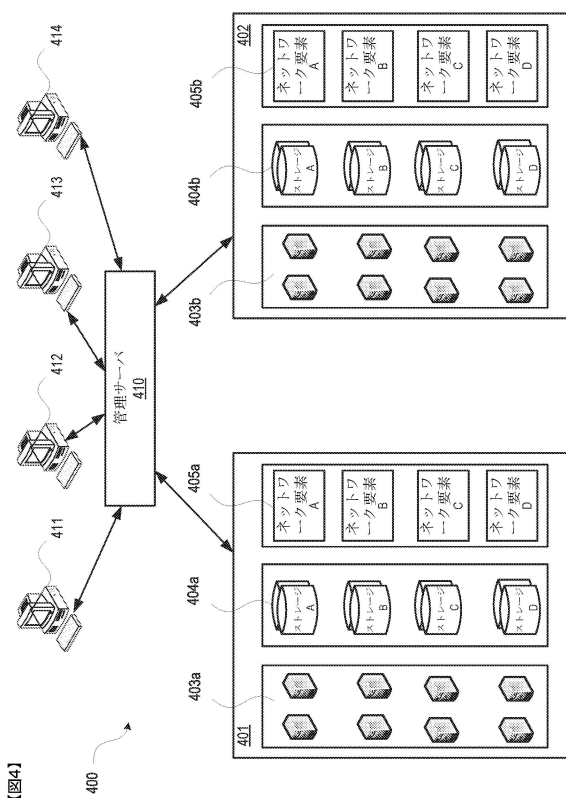
【図 2】



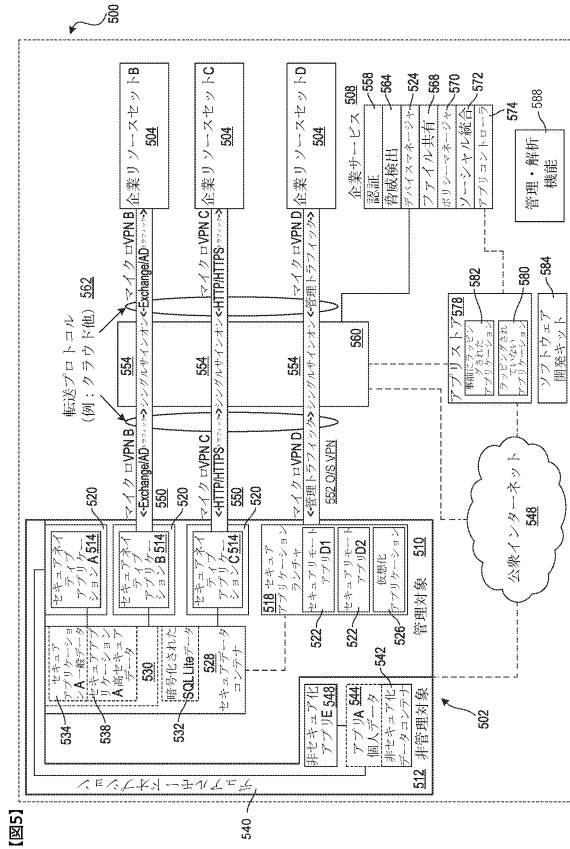
【図 3】



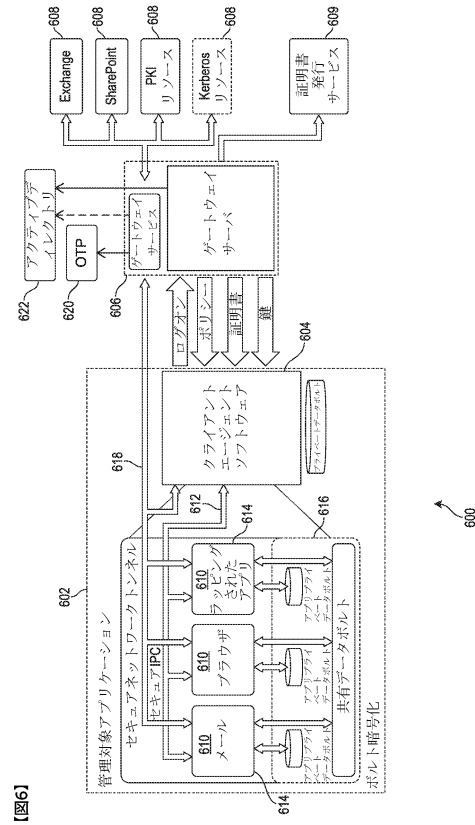
【図 4】



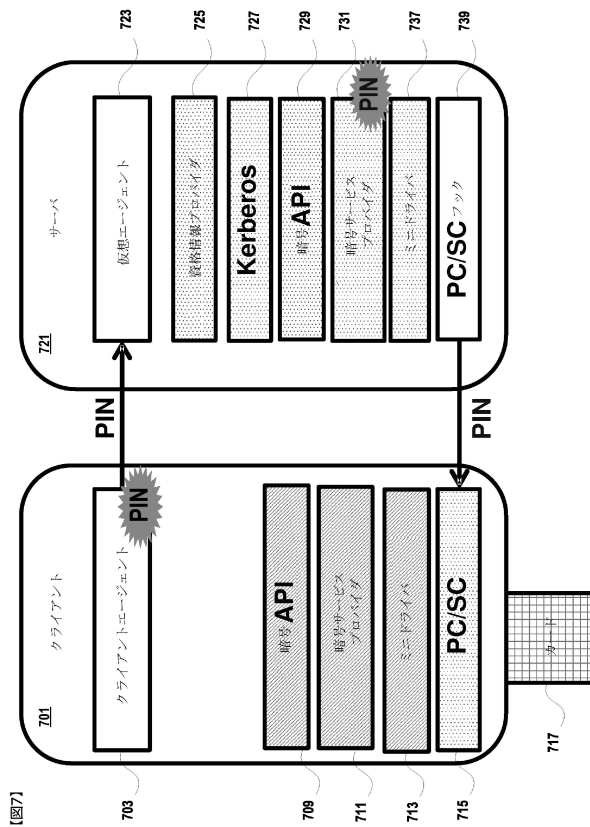
【図5】



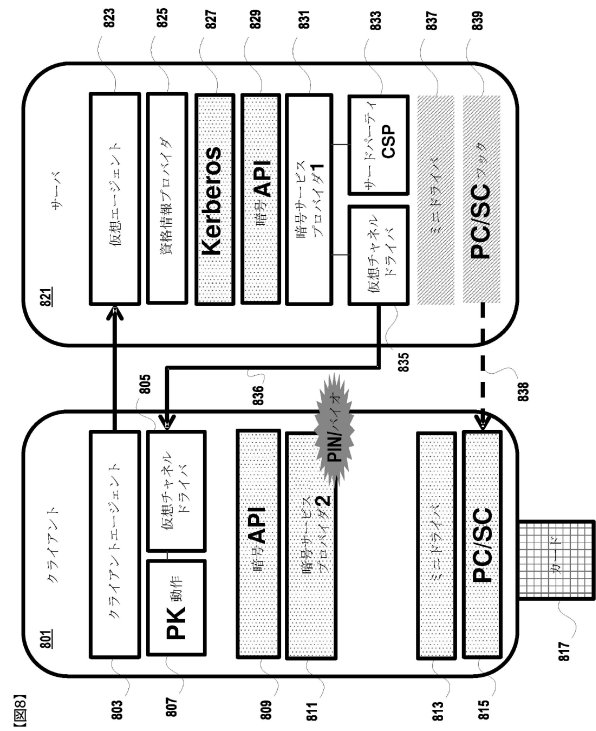
【図6】



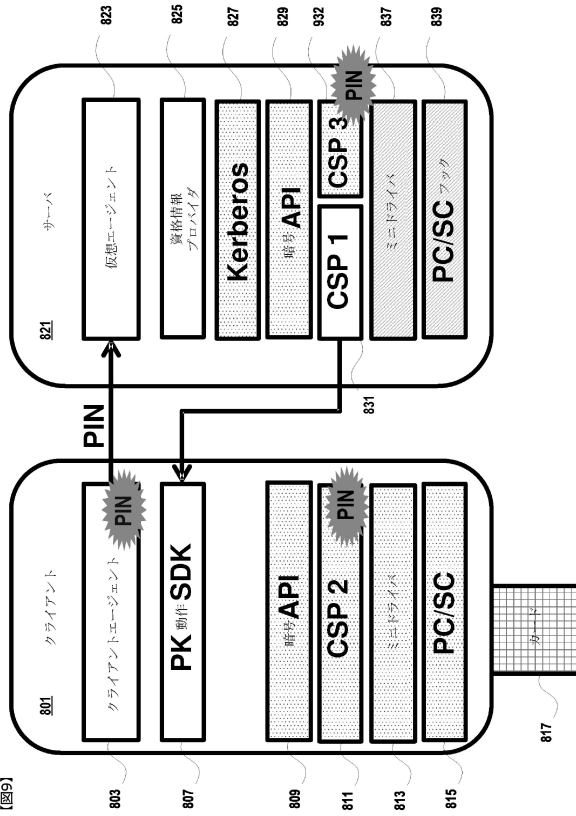
【図7】



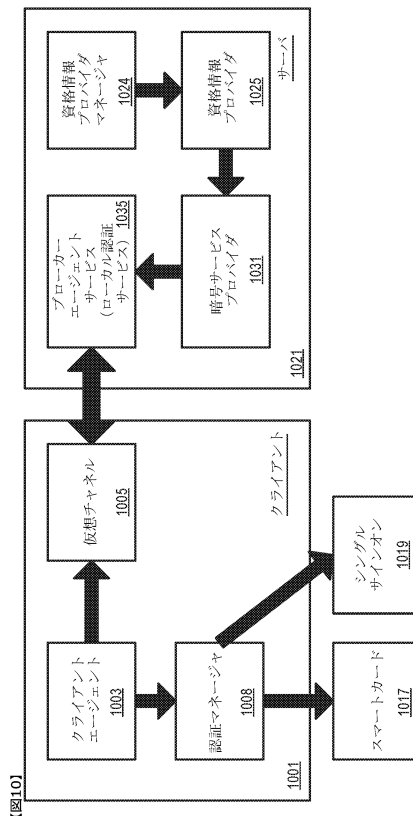
【図8】



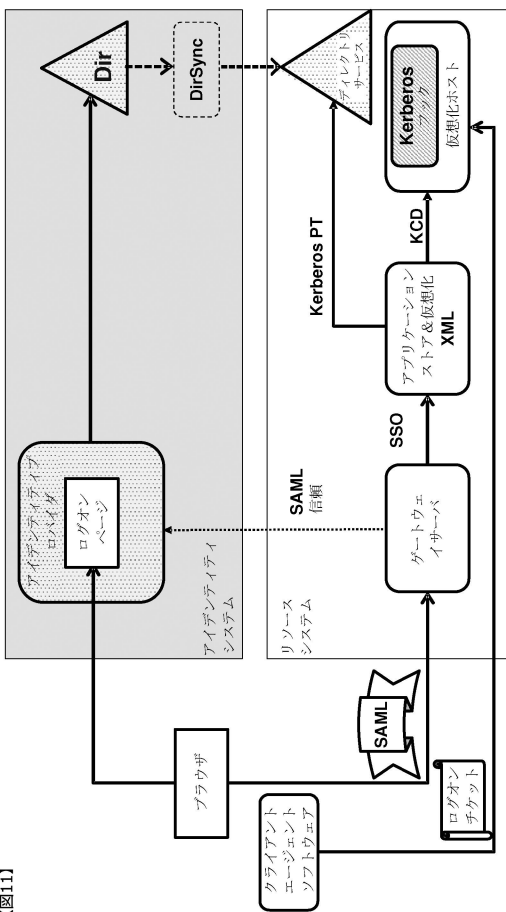
【図9】



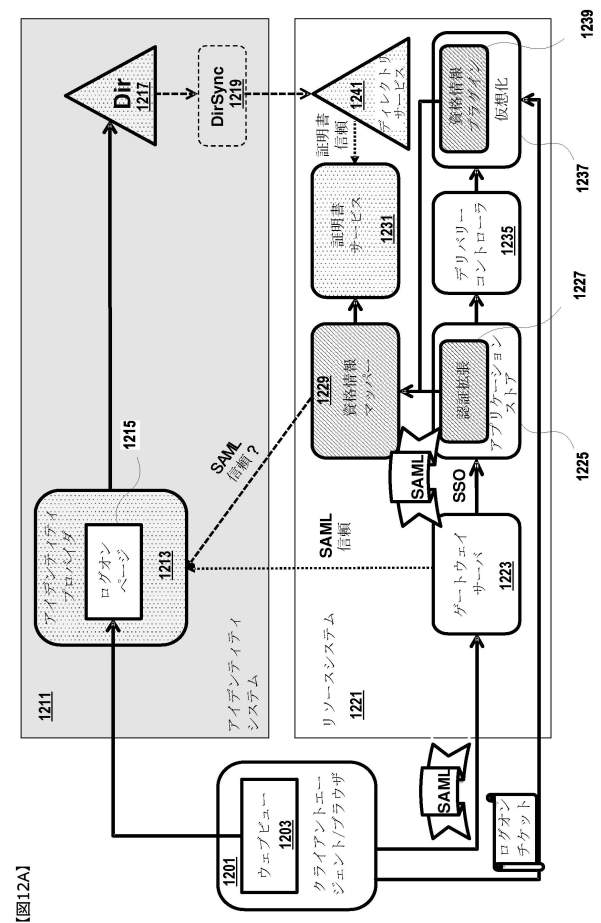
【図10】



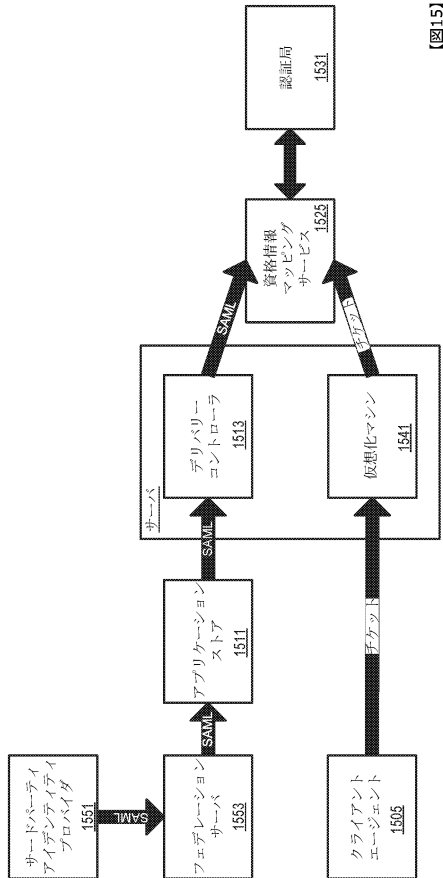
【図11】



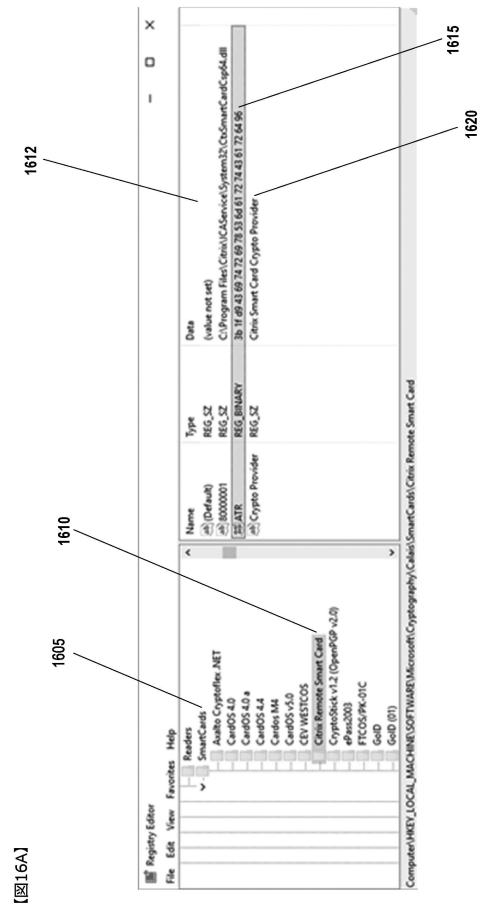
【図12A】



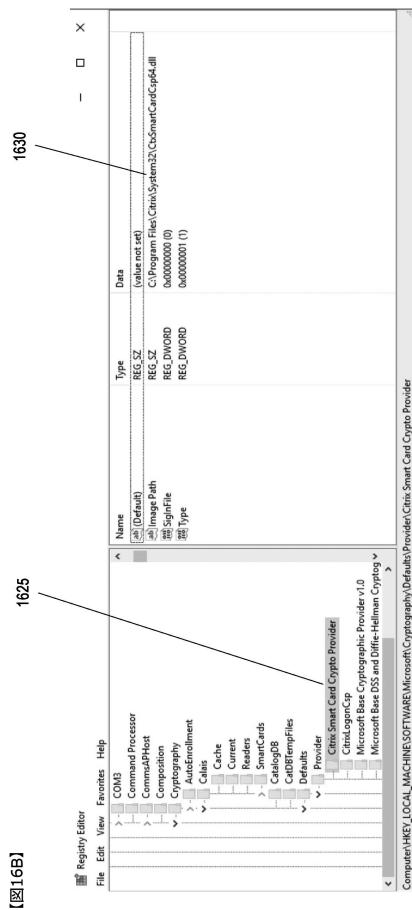
【図 15】



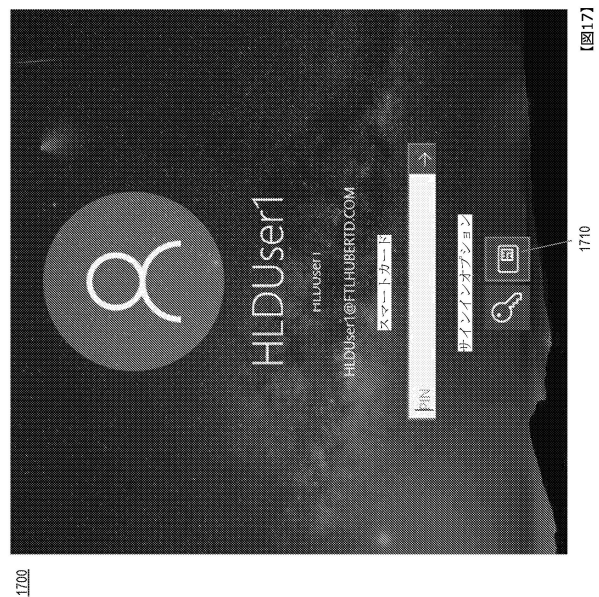
【図 1 6 A】



【図 1 6 B】



【図 17】



フロントページの続き

(72)発明者 ウィリアムズ, デイビッド
アメリカ合衆国, フロリダ州 33309, フォート ローダーデール, ウェスト 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

審査官 小林 秀和

(56)参考文献 特表2010-537340 (JP, A)
特開2013-191117 (JP, A)
特表2015-511470 (JP, A)

(58)調査した分野(Int.Cl., DB名)
G06F 21/34
G06F 21/60