

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7470879号
(P7470879)

(45)発行日 令和6年4月18日(2024.4.18)

(24)登録日 令和6年4月10日(2024.4.10)

(51)国際特許分類

F I

G 0 6 F 9/44 (2018.01)

G 0 6 F 9/44

G 0 6 F 21/60 (2013.01)

G 0 6 F 21/60 3 4 0

請求項の数 20 (全24頁)

(21)出願番号	特願2023-563906(P2023-563906)	(73)特許権者	523243306
(86)(22)出願日	令和3年11月17日(2021.11.17)		キーファクター, インコーポレイテッド
(65)公表番号	特表2024-501591(P2024-501591 A)		アメリカ合衆国 オハイオ 4 4 1 3 1 ,
(43)公表日	令和6年1月12日(2024.1.12)		インディペンデンス, オーク ツリー
(86)国際出願番号	PCT/US2021/059618	(74)代理人	ブルバード 6 0 5 0
(87)国際公開番号	WO2022/146571		100078282
(87)国際公開日	令和4年7月7日(2022.7.7)	(74)代理人	弁理士 山本 秀策
審査請求日	令和6年2月26日(2024.2.26)		100113413
(31)優先権主張番号	63/131,085	(74)代理人	弁理士 森下 夏樹
(32)優先日	令和2年12月28日(2020.12.28)		100181674
(33)優先権主張国・地域又は機関	米国(US)	(74)代理人	弁理士 飯田 貴敏
早期審査対象出願			100181641
		(74)代理人	弁理士 石川 大輔
			230113332
			弁護士 山本 健策

最終頁に続く

(54)【発明の名称】 遠隔証明機関管理

(57)【特許請求の範囲】

【請求項1】

コンピュータ実装方法であって、
遠隔証明機関（C A）ゲートウェイコアによって、ユーザデバイス上にインストールされる証明書ライフサイクル管理（C L M）アプリケーションから、要求されるタスクを規定するタスク要求と、タスク実行のための場所を規定する識別子とを受信することと、
遠隔C Aゲートウェイプラグインモジュール上のタスク選別インターフェースによって、前記タスク要求に基づいて、前記要求されるタスクおよび前記要求されるタスクのための前記タスク実行のための前記場所が、オンプレミスC Aデバイスにあることを決定することと、
前記要求されるタスクおよび前記タスク実行の前記場所が前記オンプレミスC Aデバイスにあることを決定することに応答して、前記遠隔C Aゲートウェイプラグインモジュール上のデータ記憶デバイス内に、前記タスク要求を前記タスク実行のための前記場所にリンクさせる要求タスクデータエントリを記憶することと、
前記遠隔C Aゲートウェイプラグインモジュールから、オンプレミスC Aゲートウェイに通知を提供することであって、前記遠隔C Aゲートウェイプラグインモジュールは、永続的なクライアント開始通信プロトコルを介して前記オンプレミスC Aゲートウェイとの一定の通信接続を維持する、ことと、
前記通知に応答して、前記オンプレミスC Aゲートウェイから前記オンプレミスC Aデバイスに、前記タスク実行のために前記要求されるタスクを提供することと

を含む、コンピュータ実装方法。

【請求項 2】

前記オンプレミス C A ゲートウェイは、前記タスク要求を受信することに先立って、前記遠隔 C A ゲートウェイプラグインモジュールとの前記一定の通信接続を開始する、請求項 1 に記載のコンピュータ実装方法。

【請求項 3】

前記永続的なクライアント開始通信プロトコルは、W e b S o c k e t プロトコルに基づく、請求項 1 に記載のコンピュータ実装方法。

【請求項 4】

前記永続的なクライアント開始通信プロトコルは、ロングポーリング通信プロトコルに基づく、請求項 1 に記載のコンピュータ実装方法。

10

【請求項 5】

前記オンプレミス C A ゲートウェイにおいて、前記オンプレミス C A デバイスから、前記オンプレミス C A デバイスによる前記タスク実行に基づくタスク結果を受信することと、
前記遠隔 C A ゲートウェイプラグインモジュールにおいて、前記オンプレミス C A ゲートウェイから前記永続的なクライアント開始通信プロトコルを介して、前記タスク結果を受信することと、

前記遠隔 C A ゲートウェイプラグインモジュール上の前記データ記憶デバイス内に、前記タスク結果を記憶することと、

前記遠隔 C A ゲートウェイプラグインモジュール上のタスク割り当てインターフェースによって、前記タスク結果が前記データ記憶デバイス内に受信されたことを決定することと、

20

前記遠隔 C A ゲートウェイコアによって、前記 C L M アプリケーションを介して前記ユーザデバイスに前記タスク結果を提供することと

をさらに含む、請求項 1 に記載のコンピュータ実装方法。

【請求項 6】

前記オンプレミス C A ゲートウェイは、クライアント接続マネージャを備え、前記遠隔 C A ゲートウェイプラグインモジュールは、クライアント接続受信機を備える、請求項 1 に記載のコンピュータ実装方法。

【請求項 7】

前記オンプレミス C A ゲートウェイは、C A ゲートウェイプラグインモジュールと、前記遠隔 C A ゲートウェイプラグインモジュールとの前記一定の通信接続を管理するように構成される C A 管理ゲートウェイモジュールとを備え、前記 C A ゲートウェイプラグインモジュールは、前記オンプレミス C A デバイスと通信する、請求項 1 に記載のコンピュータ実装方法。

30

【請求項 8】

前記オンプレミス C A ゲートウェイは、1 つまたはそれを上回るクライアントサーバを備える、請求項 1 に記載のコンピュータ実装方法。

【請求項 9】

前記遠隔 C A ゲートウェイプラグインモジュールは、前記データ記憶デバイス内に前記要求タスクデータ エントリ を記憶するように構成されるタスク割り当てインターフェースを備える、請求項 1 に記載のコンピュータ実装方法。

40

【請求項 10】

前記遠隔 C A ゲートウェイプラグインモジュールは、キャッシュ A P I を備え、前記オンプレミス C A ゲートウェイは、前記キャッシュ A P I にアクセスし、前記遠隔 C A ゲートウェイプラグインモジュール上にホストされるインベントリおよび構成データを同期化するように構成される同期化装置を備える、請求項 1 に記載のコンピュータ実装方法。

【請求項 11】

システムであって、

データ処理装置と、

前記データ処理装置とデータ通信している非一過性コンピュータ可読記憶媒体であって

50

、前記非一過性コンピュータ可読記憶媒体は、前記データ処理装置によって実行可能な命令を記憶し、そのような実行に応じて、前記データ処理装置に、

遠隔証明機関（ＣＡ）ゲートウェイコアによって、ユーザデバイス上にインストールされる証明書ライフサイクル管理（ＣＬＭ）アプリケーションから、要求されるタスクを規定するタスク要求と、タスク実行のための場所を規定する識別子とを受信することと、

遠隔ＣＡゲートウェイプラグインモジュール上のタスク選別インターフェースによって、前記タスク要求に基づいて、前記要求されるタスクおよび前記要求されるタスクのための前記タスク実行のための前記場所が、オンプレミスＣＡデバイスにあることを決定することと、

前記要求されるタスクおよび前記タスク実行の前記場所が前記オンプレミスＣＡデバイスにあることを決定することに応じて、前記遠隔ＣＡゲートウェイプラグインモジュール上のデータ記憶デバイス内に、前記タスク要求を前記タスク実行のための前記場所にリンクさせる要求タスクデータエントリを記憶することと、

前記遠隔ＣＡゲートウェイプラグインモジュールから、オンプレミスＣＡゲートウェイに通知を提供することであって、前記遠隔ＣＡゲートウェイプラグインモジュールは、永続的なクライアント開始通信プロトコルを介して前記オンプレミスＣＡゲートウェイとの一定の通信接続を維持する、ことと、

前記通知に応じて、前記オンプレミスＣＡゲートウェイから前記オンプレミスＣＡデバイスに、前記タスク実行のために前記要求されるタスクを提供することと

を含む動作を実施させる、非一過性コンピュータ可読記憶媒体と

を備える、システム。

【請求項１２】

前記オンプレミスＣＡゲートウェイは、前記タスク要求を受信することに先立って、前記遠隔ＣＡゲートウェイプラグインモジュールとの前記一定の通信接続を開始する、請求項１１に記載のシステム。

【請求項１３】

前記永続的なクライアント開始通信プロトコルは、ＷｅｂＳｏｃｋｅｔプロトコルに基づく、請求項１１に記載のシステム。

【請求項１４】

前記永続的なクライアント開始通信プロトコルは、ロングポーリング通信プロトコルに基づく、請求項１１に記載のシステム。

【請求項１５】

前記オンプレミスＣＡゲートウェイは、クライアント接続マネージャを備え、前記遠隔ＣＡゲートウェイプラグインモジュールは、クライアント接続受信機を備える、請求項１１に記載のシステム。

【請求項１６】

前記オンプレミスＣＡゲートウェイは、前記オンプレミスＣＡデバイスから、前記オンプレミスＣＡデバイスによる前記タスク実行に基づくタスク結果を受信するようにさらに構成される、請求項１１に記載のシステム。

【請求項１７】

前記動作は、

前記遠隔ＣＡゲートウェイプラグインモジュールにおいて、前記オンプレミスＣＡゲートウェイから前記永続的なクライアント開始通信プロトコルを介して、前記タスク結果を受信することと、

前記遠隔ＣＡゲートウェイプラグインモジュール上の前記データ記憶デバイス内に、前記タスク結果を記憶することと、

前記遠隔ＣＡゲートウェイプラグインモジュール上のタスク割当インターフェースによって、前記タスク結果が前記データ記憶デバイス内に受信されたことを決定することと、

前記遠隔ＣＡゲートウェイコアによって、前記ＣＬＭアプリケーションを介して前記ユーザデバイスに前記タスク結果を提供することと

10

20

30

40

50

をさらに含む、請求項 11 に記載のシステム。

【請求項 18】

前記オンプレミス C A ゲートウェイは、前記遠隔 C A ゲートウェイプラグインとの前記一定の通信接続を管理するように構成される C A 管理ゲートウェイモジュールと、前記オンプレミス C A デバイスと通信する C A ゲートウェイプラグインモジュールとを備える、請求項 11 に記載のシステム。

【請求項 19】

コンピュータプログラムを用いてエンコードされる非一過性コンピュータ記憶媒体であって、前記コンピュータプログラムは、命令を含み、前記命令は、1 つまたはそれを上回るデータ処理装置によって実行されると、データ処理装置に、

10

遠隔証明機関 (C A) ゲートウェイコアによって、ユーザデバイス上にインストールされる証明書ライフサイクル管理 (C L M) アプリケーションから、要求されるタスクを規定するタスク要求と、タスク実行のための場所を規定する識別子とを受信することと、

遠隔 C A ゲートウェイプラグインモジュール上のタスク選別インターフェースによって、前記タスク要求に基づいて、前記要求されるタスクおよび前記要求されるタスクのための前記タスク実行のための前記場所が、オンプレミス C A デバイスにあることを決定することと、

前記要求されるタスクおよび前記タスク実行の前記場所が前記オンプレミス C A デバイスにあることを決定することに応答して、前記遠隔 C A ゲートウェイプラグインモジュール上のデータ記憶デバイス内に、前記タスク要求を前記タスク実行のための前記場所にリンクさせる要求タスクデータエントリを記憶することと、

20

前記遠隔 C A ゲートウェイプラグインモジュールから、オンプレミス C A ゲートウェイに通知を提供することであって、前記遠隔 C A ゲートウェイプラグインモジュールは、永続的なクライアント開始通信プロトコルを介して前記オンプレミス C A ゲートウェイとの一定の通信接続を維持する、ことと、

前記通知に応答して、前記オンプレミス C A ゲートウェイから前記オンプレミス C A デバイスに、前記タスク実行のために前記要求されるタスクを提供することと

を含む動作を実施させる、非一過性コンピュータ記憶媒体。

【請求項 20】

前記オンプレミス C A ゲートウェイは、前記タスク要求を受信することに先立って、前記遠隔 C A ゲートウェイプラグインモジュールとの前記一定の通信接続を開始する、請求項 19 に記載の非一過性コンピュータ記憶媒体。

30

【発明の詳細な説明】

【技術分野】

【0001】

(関連出願の相互参照)

本願は、参照することによってその全体として本明細書に組み込まれる、2020 年 1 月 28 日に出版された、米国仮出願第 63 / 131,085 号の利益を主張する。

【0002】

本開示は、概して、コンピュータネットワークセキュリティに関し、より具体的には、クラウドによってホストされるサービスを介してセキュアなネットワークにアクセスすることを要求する、コンピューティングデバイスのためのセキュリティポリシーを実装および管理するためのシステムおよび方法に関する。

40

【背景技術】

【0003】

証明機関 (C A) ソフトウェアは、運転免許証またはパスポートに対して暗号で署名されるデジタルパラレルである、デジタル証明書を生成するために使用される。デジタル証明書は、ユーザまたはウェブサイト認証、デジタル署名ソフトウェア、またはシステム間で情報を暗号化することを含む、多種多様なユースケースのために使用される。証明書を

使用するアプリケーションは、非常に普及した状態になりつつあり (例えば、組織内の数

50

百万もの証明書)、したがって、証明書をセキュアに追跡、管理、更新、および発行することは、課題である。

【0004】

標準的な機能性の一部として、証明書ライフサイクル管理(CLM)ソフトウェアが、CAソフトウェアへのネットワーク接続を開始し、新しい証明書を要求する、証明書を延長する、証明書を無効にすること等の機能を実施する、または発行された証明書のインベントリを取得する。これらの接続は、典型的には、CLMソフトウェアによって、CLMソフトウェアのエンドユーザに代わって開始され、CAソフトウェアエンティティから入手可能である、アプリケーションプログラミングインターフェース(API)エンドポイントと通信する。

10

【0005】

多くのエンティティが、CAと、エンティティがそれらのジョブを行うために使用する暗号化キーとの機密性の高い本質に起因して、CAソフトウェアをそれら自体の環境内で実行する。したがって、これらのCAシステムは、多くの場合、利用可能な最高レベルのネットワークおよび物理的セキュリティ制御を用いて保護される。

【0006】

対照的に、多くの組織は、クラウドによってホストされる、またはソフトウェア・アズ・ア・サービス(SaaS)モデルが、提供し得る、多くの恩恵のために、それらのCLMソフトウェアをクラウドベースまたはサードパーティホスト環境内で実行させることを所望する。本コネクティビティの必要性および環境の不均衡が、克服することが困難である、課題を生じさせる。クラウドによってホストされる環境から顧客の内部的にホストされるCAソフトウェアにコンタクトすることは、組織がそれらのネットワーク上に、特に、CA等の機密性の高いシステムの周囲に配置する厳重な制御に起因して、不可能ではないにしても、困難である。本使用法パターンをサポートするために現在利用可能な選択肢は、典型的には、クラウドによってホストされるソフトウェアと組織のネットワークとの間に仮想プライベートネットワーク(VPN)を設定すること、または組織がそれらのCAソフトウェアをリバースネットワークプロキシまたは類似の技術を介してインターネットに公開することであろう。しかしながら、これらの選択肢のいずれも、それらが2つの環境間に公開された「攻撃対象領域」を開放し、サイバー攻撃のリスクを増加させるため、CAユーザにとってあまり魅力的ではない。

20

30

【発明の概要】

【課題を解決するための手段】

【0007】

本明細書は、CAソフトウェアが典型的に置かれている、機密性の高いネットワーク環境を、CLMソフトウェアがホストされるクラウド環境にブリッジさせるための機構を伴う、証明機関(CA)と証明書ライフサイクル管理(CLM)システムとの間のセキュアな通信を促進するためのシステム、方法、デバイス、および技法を説明する。本アプローチは、機密性の高いCAデータセンターからのアウトバウンドネットワーク接続を利用しながら、CLMシステムが、CLMユースケースが、永続的なクライアント開始通信プロトコルを使用して指示する、リアルタイムの動的方式でCAを使用することを可能にする。Web Socketプロトコルまたは「ロングポーリング」アプローチを含み得る、永続的なクライアント開始通信プロトコルが、タスク管理および調整およびゲートウェイフレームワークと併せて活用され、永続的なクライアント通信のための目標を達成する。

40

【0008】

一般に、本明細書において説明される主題の1つの革新的側面は、遠隔証明機関(CA)ゲートウェイコアによって、ユーザデバイス上にインストールされる証明書ライフサイクル管理(CLM)アプリケーションから、要求されるタスクを規定する、タスク要求と、タスク実行のための場所を規定する、識別子とを受信するアクションと、遠隔CAゲートウェイプラグインモジュール上のタスク選別インターフェースによって、タスク要求に基づいて、要求されるタスクおよび要求されるタスクのためのタスク実行のための場所が

50

、オンプレミス C A デバイスにあることを決定するアクションと、要求されるタスクおよびタスクの場所がオンプレミス C A デバイスにあることを決定するアクションにตอบสนองして、遠隔 C A ゲートウェイプラグインモジュール上のデータ記憶デバイス内に、タスク要求をタスク実行のための場所にリンクさせる、要求タスクデータエントリを記憶するアクションと、遠隔 C A ゲートウェイプラグインモジュールから、オンプレミス C A ゲートウェイに通知を提供するアクションであって、遠隔 C A ゲートウェイプラグインモジュールは、永続的なクライアント開始通信プロトコルを介してオンプレミス C A ゲートウェイとの一定の通信接続を維持する、アクションと、通知にตอบสนองして、オンプレミス C A ゲートウェイからオンプレミス C A デバイスに、タスク実行のために要求されるタスクを提供するアクションとを含む、コンピュータ実装方法において具現化されることができる。

10

【 0 0 0 9 】

これらおよび他の実施形態はそれぞれ、随意に、以下の特徴のうちの 1 つまたはそれを上回るものを含むことができる。

【 0 0 1 0 】

いくつかの側面では、オンプレミス C A ゲートウェイは、タスク要求を受信することに先立って、遠隔 C A ゲートウェイプラグインモジュールとの一定の通信接続を開始する。

【 0 0 1 1 】

いくつかの側面では、永続的なクライアント開始通信プロトコルは、Web Socket プロトコルに基づく。いくつかの側面では、永続的なクライアント開始通信プロトコルは、ロングポーリング通信プロトコルに基づく。

20

【 0 0 1 2 】

いくつかの側面では、本方法はさらに、オンプレミス C A ゲートウェイにおいて、オンプレミス C A デバイスから、オンプレミス C A デバイスによるタスク実行に基づく、タスク結果を受信することと、遠隔 C A ゲートウェイプラグインモジュールにおいて、オンプレミス C A ゲートウェイから永続的なクライアント開始通信プロトコルを介して、タスク結果を受信することと、遠隔 C A ゲートウェイプラグインモジュール上のデータ記憶デバイス内に、タスク結果を記憶することと、遠隔 C A ゲートウェイプラグインモジュール上のタスク割当インターフェースによって、タスク結果がデータ記憶デバイス内に受信されたことを決定することと、遠隔 C A ゲートウェイコアによって、C L M アプリケーションを介してユーザデバイスにタスク結果を提供することを含む。

30

【 0 0 1 3 】

いくつかの側面では、オンプレミス C A ゲートウェイは、クライアント接続マネージャを含み、遠隔 C A ゲートウェイプラグインモジュールは、クライアント接続受信機を含む。

【 0 0 1 4 】

いくつかの側面では、オンプレミス C A ゲートウェイは、C A ゲートウェイプラグインモジュールと、遠隔 C A ゲートウェイプラグインモジュールとの一定の通信接続を管理するように構成される、C A 管理ゲートウェイモジュールとを含み、C A ゲートウェイプラグインモジュールは、オンプレミス C A デバイスと通信する。

【 0 0 1 5 】

いくつかの側面では、1 つまたはそれを上回るクライアントサーバは、オンプレミス C A ゲートウェイを含む。いくつかの側面では、遠隔 C A ゲートウェイプラグインモジュールは、データ記憶デバイス内に要求タスクデータを記憶するように構成される、タスク割当インターフェースを含む。

40

【 0 0 1 6 】

いくつかの側面では、遠隔 C A ゲートウェイプラグインモジュールは、キャッシュ A P I を含み、オンプレミス C A ゲートウェイは、キャッシュ A P I にアクセスし、遠隔 C A ゲートウェイプラグインモジュール上にホストされるインベントリおよび構成データを同期化するように構成される、同期化装置を含む。

【 0 0 1 7 】

本明細書に説明される主題の特定の実施形態は、以下の利点のうちの 1 つまたはそれを

50

上回るものを実現するように実装されることができる。例えば、本明細書に議論されるシステムおよび方法は、C A 使用法パターンを達成するための機構を提供しながら、顧客環境内に展開される単一のソフトウェアのみを要求し、これは、C A ゲートウェイ環境に戻るアウトバウンド接続のみを行い、本明細書に議論される「通信開始」要件を本質的に逆転させる。加えて、プライベートエンティティネットワークからクラウドによってホストされるサービスへのアウトバウンド接続は、C A へのインバウンド接続を可能にすることよりも、許容可能であり、セキュアである。

【 0 0 1 8 】

いくつかの実装によると、デバイスは、1つまたはそれを上回るプロセッサと、非一過性メモリと、1つまたはそれを上回るプログラムとを含み、1つまたはそれを上回るプログラムは、非一過性メモリ内に記憶され、1つまたはそれを上回るプロセッサによって実行されるように構成され、1つまたはそれを上回るプログラムは、本明細書に説明される方法のうちのいずれかを実施する、またはその実施を引き起こすための命令を含む。いくつかの実装によると、非一過性コンピュータ可読記憶媒体は、デバイスの1つまたはそれを上回るプロセッサによって実行されると、本デバイスに、本明細書に説明される方法のうちのいずれかを実施させる、またはその実施を引き起こさせる、命令をその中に記憶している。いくつかの実装によると、デバイスは、1つまたはそれを上回るプロセッサと、非一過性メモリと、本明細書に説明される方法のうちのいずれかを実施する、またはその性能を引き起こすための手段とを含む。

【 0 0 1 9 】

前述の主題の種々の特徴および利点が、図に関して下記に説明される。付加的な特徴および利点が、本明細書および請求項に説明される主題から、明白である。

本発明は、例えば、以下を提供する。

(項目 1)

コンピュータ実装方法であって、

遠隔証明機関 (C A) ゲートウェイコアによって、ユーザデバイス上にインストールされる証明書ライフサイクル管理 (C L M) アプリケーションから、要求されるタスクを規定するタスク要求と、タスク実行のための場所を規定する識別子とを受信することと、

遠隔 C A ゲートウェイプラグインモジュール上のタスク選別インターフェースによって、前記タスク要求に基づいて、前記要求されるタスクおよび前記要求されるタスクのためのタスク実行のための前記場所が、オンプレミス C A デバイスにあることを決定することと、

前記要求されるタスクおよび前記タスクの場所が前記オンプレミス C A デバイスにあることを決定することに応答して、前記遠隔 C A ゲートウェイプラグインモジュール上のデータ記憶デバイス内に、前記タスク要求をタスク実行のための前記場所にリンクさせる要求タスクデータエントリを記憶することと、

前記遠隔 C A ゲートウェイプラグインモジュールから、オンプレミス C A ゲートウェイに通知を提供することであって、前記遠隔 C A ゲートウェイプラグインモジュールは、永続的なクライアント開始通信プロトコルを介して前記オンプレミス C A ゲートウェイとの一定の通信接続を維持する、ことと、

前記通知に応答して、前記オンプレミス C A ゲートウェイから前記オンプレミス C A デバイスに、タスク実行のために前記要求されるタスクを提供することと

を含む、コンピュータ実装方法。

(項目 2)

前記オンプレミス C A ゲートウェイは、前記タスク要求を受信することに先立って、前記遠隔 C A ゲートウェイプラグインモジュールとの前記一定の通信接続を開始する、項目 1 に記載のコンピュータ実装方法。

(項目 3)

前記永続的なクライアント開始通信プロトコルは、Web S o c k e t プロトコルに基づく、項目 1 に記載のコンピュータ実装方法。

10

20

30

40

50

(項目 4)

前記永続的なクライアント開始通信プロトコルは、ロングポーリング通信プロトコルに基づく、項目 1 に記載のコンピュータ実装方法。

(項目 5)

前記オンプレミス C A ゲートウェイにおいて、前記オンプレミス C A デバイスから、前記オンプレミス C A デバイスによる前記タスク実行に基づくタスク結果を受信することと、

前記遠隔 C A ゲートウェイプラグインモジュールにおいて、前記オンプレミス C A ゲートウェイから前記永続的なクライアント開始通信プロトコルを介して、前記タスク結果を受信することと、

前記遠隔 C A ゲートウェイプラグインモジュール上の前記データ記憶デバイス内に、前記タスク結果を記憶することと、

前記遠隔 C A ゲートウェイプラグインモジュール上のタスク割当インターフェースによって、前記タスク結果が前記データ記憶デバイス内に受信されたことを決定することと、

前記遠隔 C A ゲートウェイコアによって、前記 C L M アプリケーションを介して前記ユーザデバイスに前記タスク結果を提供することと

をさらに含む、項目 1 に記載のコンピュータ実装方法。

(項目 6)

前記オンプレミス C A ゲートウェイは、クライアント接続マネージャを備え、前記遠隔 C A ゲートウェイプラグインモジュールは、クライアント接続受信機を備える、項目 1 に記載のコンピュータ実装方法。

(項目 7)

前記オンプレミス C A ゲートウェイは、C A ゲートウェイプラグインモジュールと、前記遠隔 C A ゲートウェイプラグインモジュールとの前記一定の通信接続を管理するように構成される C A 管理ゲートウェイモジュールとを備え、前記 C A ゲートウェイプラグインモジュールは、前記オンプレミス C A デバイスと通信する、項目 1 に記載のコンピュータ実装方法。

(項目 8)

前記 1 つまたはそれを上回るクライアントサーバは、前記オンプレミス C A ゲートウェイを備える、項目 1 に記載のコンピュータ実装方法。

(項目 9)

前記遠隔 C A ゲートウェイプラグインモジュールは、前記データ記憶デバイス内に前記要求タスクデータを記憶するように構成されるタスク割当インターフェースを備える、項目 1 に記載のコンピュータ実装方法。

(項目 1 0)

前記遠隔 C A ゲートウェイプラグインモジュールは、キャッシュ A P I を備え、前記オンプレミス C A ゲートウェイは、前記キャッシュ A P I にアクセスし、前記遠隔 C A ゲートウェイプラグインモジュール上にホストされるインベントリおよび構成データを同期化するように構成される同期化装置を備える、項目 1 に記載のコンピュータ実装方法。

(項目 1 1)

システムであって、

データ処理装置と、

前記データ処理装置とデータ通信している非一過性コンピュータ可読記憶媒体であって、前記非一過性コンピュータ可読記憶媒体は、前記データ処理装置によって実行可能な命令を記憶し、そのような実行に応じて、前記データ処理装置に、

遠隔証明機関 (C A) ゲートウェイコアによって、ユーザデバイス上にインストールされる証明書ライフサイクル管理 (C L M) アプリケーションから、要求されるタスクを規定するタスク要求と、タスク実行のための場所を規定する識別子とを受信することと、

遠隔 C A ゲートウェイプラグインモジュール上のタスク選別インターフェースによって、前記タスク要求に基づいて、前記要求されるタスクおよび前記要求されるタスクのためのタスク実行のための前記場所が、オンプレミス C A デバイスにあることを決定すること

10

20

30

40

50

と、

前記要求されるタスクおよび前記タスクの場所が前記オンプレミスＣＡデバイスにあることを決定することに応答して、前記遠隔ＣＡゲートウェイプラグインモジュール上のデータ記憶デバイス内に、前記タスク要求をタスク実行のための前記場所にリンクさせる要求タスクデータエントリを記憶することと、

前記遠隔証明機関ゲートウェイプラグインモジュールから、オンプレミスＣＡゲートウェイに通知を提供することであって、前記遠隔ＣＡゲートウェイプラグインモジュールは、永続的なクライアント開始通信プロトコルを介して前記オンプレミスＣＡゲートウェイとの一定の通信接続を維持する、ことと、

前記通知に応答して、前記オンプレミスＣＡゲートウェイから前記オンプレミスＣＡデバイスに、タスク実行のために前記要求されるタスクを提供することと

を含む動作を実施させる、非一過性コンピュータ可読記憶媒体とを備える、システム。

(項目１２)

前記オンプレミスＣＡゲートウェイは、前記タスク要求を受信することに先立って、前記遠隔ＣＡゲートウェイプラグインモジュールとの前記一定の通信接続を開始する、項目１１に記載のシステム。

(項目１３)

前記永続的なクライアント開始通信プロトコルは、ＷｅｂＳｏｃｋｅｔプロトコルに基づく、項目１１に記載のシステム。

(項目１４)

前記永続的なクライアント開始通信プロトコルは、ロングポーリング通信プロトコルに基づく、項目１１に記載のシステム。

(項目１５)

前記オンプレミスＣＡゲートウェイは、クライアント接続マネージャを備え、前記遠隔ＣＡゲートウェイプラグインモジュールは、クライアント接続受信機を備える、項目１１に記載のシステム。

(項目１６)

前記オンプレミスＣＡゲートウェイはさらに、

前記オンプレミスＣＡデバイスから、前記オンプレミスＣＡデバイスによる前記タスク実行に基づくタスク結果を受信する

ように構成される、項目１１に記載のシステム。

(項目１７)

前記動作はさらに、

前記遠隔ＣＡゲートウェイプラグインモジュールにおいて、前記オンプレミスＣＡゲートウェイから前記永続的なクライアント開始通信プロトコルを介して、前記タスク結果を受信することと、

前記遠隔ＣＡゲートウェイプラグインモジュール上の前記データ記憶デバイス内に、前記タスク結果を記憶することと、

前記遠隔ＣＡゲートウェイプラグインモジュール上のタスク割当インターフェースによって、前記タスク結果が前記データ記憶デバイス内に受信されたことを決定することと、

前記遠隔ＣＡゲートウェイコアによって、前記ＣＬＭアプリケーションを介して前記ユーザデバイスに前記タスク結果を提供することと

を含む、項目１１に記載のシステム。

(項目１８)

前記オンプレミスＣＡゲートウェイは、前記遠隔ＣＡゲートウェイプラグインとの前記一定の通信接続を管理するように構成されるＣＡ管理ゲートウェイモジュールと、前記オンプレミスＣＡデバイスと通信するＣＡゲートウェイプラグインモジュールとを備える、項目１１に記載のシステム。

(項目１９)

10

20

30

40

50

コンピュータプログラムを用いてエンコードされる非一過性コンピュータ記憶媒体であって、前記コンピュータプログラムは、命令を含み、前記命令は、1つまたはそれを上回るデータ処理装置によって実行されると、データ処理装置に、

遠隔証明機関（CA）ゲートウェイコアによって、ユーザデバイス上にインストールされる証明書ライフサイクル管理（CLM）アプリケーションから、要求されるタスクを規定するタスク要求と、タスク実行のための場所を規定する識別子とを受信することと、

遠隔CAゲートウェイプラグインモジュール上のタスク選別インターフェースによって、前記タスク要求に基づいて、前記要求されるタスクおよび前記要求されるタスクのためのタスク実行のための前記場所が、オンプレミスCAデバイスにあることを決定することと、

10

前記要求されるタスクおよび前記タスクの場所が前記オンプレミスCAデバイスにあることを決定することに応答して、前記遠隔CAゲートウェイプラグインモジュール上のデータ記憶デバイス内に、前記タスク要求を前記タスク実行のための場所にリンクさせる要求タスクデータエントリを記憶することと、

前記遠隔CAゲートウェイプラグインモジュールから、オンプレミスCAゲートウェイに通知を提供することであって、前記遠隔CAゲートウェイプラグインモジュールは、永続的なクライアント開始通信プロトコルを介して前記オンプレミスCAゲートウェイとの一定の通信接続を維持する、ことと、

前記通知に応答して、前記オンプレミスCAゲートウェイから前記オンプレミスCAデバイスに、タスク実行のために前記要求されるタスクを提供することと

20

を含む動作を実施させる、非一過性コンピュータ記憶媒体。

（項目20）

前記オンプレミスCAゲートウェイは、前記タスク要求を受信することに先立って、前記遠隔CAゲートウェイプラグインモジュールとの前記一定の通信接続を開始する、項目19に記載の非一過性コンピュータ記憶媒体。

【図面の簡単な説明】

【0020】

【図1】図1は、本開示の実施例による、デバイス上のCLMアプリケーションがクラウドベースのCAゲートウェイおよびオンプレミスに位置するCA管理ゲートウェイプラグインを通してオンプレミスCAに通信する、例示的環境である。

30

【0021】

【図2】図2は、本開示の実施例による、クラウドベースのCAゲートウェイプロトコルを利用してデバイス上のCLMアプリケーションとオンプレミスCAとの間で通信するための方法のタイミング図を図示する。

【0022】

【図3】図3は、クラウドベースのCAゲートウェイおよびオンプレミスに位置するCA管理ゲートウェイプラグインを介してオンプレミスCAにデータを提供するための例示的プロセスのフローチャートである。

【0023】

【図4】図4は、本明細書に説明される実施形態による、本明細書に説明されるソフトウェアコンポーネントを実行することが可能であるコンピュータのための例示的コンピュータアーキテクチャを示す、ブロック図である。

40

【0024】

種々の図面における同様の参照番号および記号は、同様の要素を示す。

【発明を実施するための形態】

【0025】

詳細な説明

本開示は、以下の詳細な説明、実施例、図面、および請求項を参照することによってより容易に理解されることができる。しかしながら、本デバイス、システム、および/または方法が、開示および説明される前に、本開示が、別様に規定されない限り、開示される

50

具体的なデバイス、システム、および／または方法に限定されず、したがって、当然ながら、変動し得ることを理解されたい。また、本明細書に使用される専門用語が、特定の側面を説明する目的のためのものにすぎず、限定することを意図していないことも理解されたい。

【0026】

クラウドによってホストされる環境内の証明機関（CA）と証明書ライフサイクル管理（CLM）システムとの間のセキュアな通信を促進することと関連付けられる問題に対処するために、本開示は、CAソフトウェアが典型的に置かれている、機密性の高いネットワーク環境を、CLMソフトウェアがホストされるクラウド環境にブリッジさせるための機構を提供する。本アプローチは、機密性の高いCAデータセンターからのアウトバウンドネットワーク接続を使用しながら、CLMシステムが、CLMユースケースが指示するリアルタイムの動的な方式においてCAを使用することを可能にする。WebSocketプロトコル、ロングポーリングプロトコル、および同等物等のクライアント開始通信プロトコルが、タスク管理および調整およびゲートウェイフレームワークと併せて活用され、永続的なクライアント開始通信のための目標を達成し得る。

10

【0027】

図1は、CLMシステムがクラウド環境内のCAゲートウェイを通してオンプレミスCAにタスク要求を通信する、例示的環境100である。例示的環境100は、ユーザデバイス110と、1つまたはそれを上回るCAゲートウェイクラウドベースサーバ120と、データ通信ネットワーク102、例えば、ローカルエリアネットワーク（LAN）、広域ネットワーク（WAN）、インターネット、モバイルネットワーク、またはそれらの組み合わせを経由して通信する、1つまたはそれを上回るクライアントサーバ150を含む。加えて、例示的環境100は、1つまたはそれを上回るクライアントサーバ150上に記憶され得る、またはクライアントの地点における別個のデバイスまたはサーバとしての、オンプレミスCAデバイス170を含む。

20

【0028】

ユーザデバイス110は、デスクトップ、ラップトップ、サーバ、またはスマートフォン、タブレット型コンピュータ、ウェアラブルデバイス（例えば、スマートウォッチ）、車内コンピューティングデバイス、および／または他のタイプのモバイルデバイス等のモバイルデバイスを含むことができる。ユーザデバイス110は、1つまたはそれを上回るCAゲートウェイクラウドベースサーバ120における遠隔CAゲートウェイコア122へのタスク要求およびそこからのタスク結果データを管理するための、CLMアプリケーション112等のアプリケーションを含む。ユーザデバイス110は、他のアプリケーションを含むこともできる。

30

【0029】

1つまたはそれを上回るCAゲートウェイクラウドベースサーバ120は、1つまたはそれを上回るユーザデバイスからのCLMアプリケーションから受信される、タスク要求の場所を管理する。1つまたはそれを上回るCAゲートウェイクラウドベースサーバ120のタスク管理プロトコルは、タスクが、1つのクライアントサーバ150によって取り扱われるように、複数のクライアント（例えば、クライアントサーバ150）を管理することによって、冗長な負荷平衡化システムに基づく。例えば、要求されるタスクにサービス提供することが可能である、複数のクライアントが、存在し得、冗長な負荷平衡化システムは、タスクが有能なクライアントのうちの厳密に1つによって実施されることを確実にすることに関わる。

40

【0030】

1つまたはそれを上回るCAゲートウェイクラウドベースサーバ120は、遠隔CAゲートウェイコア122と、遠隔CAゲートウェイプラグイン130とを含む。遠隔CAゲートウェイコア122は、CLMプラットフォームに（例えば、CLMアプリケーション112を介してユーザデバイス110に）、標準化されたインターフェースを提示し、CA固有のプラグインが、所与のCAタイプに対して必要な機能を実施することを可能にす

50

る。クラウド環境内にホストされる遠隔C Aゲートウェイプラグイン130は、タスク要求およびタスク結果を記憶するためのC Aタスクデータベース140と、C Aタスクデータベース140と通信する、タスク割当A P I 132とを含む。遠隔C Aゲートウェイプラグイン130はまた、タスクを実行するために受信された各タスク要求（例えば、タスク実行のための場所データ）の必要な詳細を処理し得る、タスク選別A P I 132も含む。

【0031】

遠隔C Aゲートウェイプラグイン130はさらに、永続的なクライアント開始通信プロトコルに基づくクライアント接続マネージャ166を介して、別のシステム（例えば、オンプレミスC Aゲートウェイ160）との永続的なクライアント開始通信を提供するための、クライアント接続受信機138を含む。いくつかの実装では、Web S o c k e t プロトコルが、永続的なクライアント開始通信のために使用されてもよい。Web S o c k e t プロトコルは、単一のT C P接続を経由して全二重通信チャネルを提供する、コンピュータ通信プロトコルである。加えて、または代替として、ロングポーリング通信プロトコルが、永続的なクライアント開始通信のために使用されてもよい。「ロングポーリング」技法は、サーバが、可能な限り長い時間にわたって、クライアントの接続を開放された状態に保持し、データが入手可能な状態になる、またはタイムアウト閾値が、到達されて初めて応答を送達することを採択するものである。

【0032】

クラウド環境内のクライアント接続受信機138が、要求タスクが実行のためにC Aタスクデータベース140内に出現したことを認めると、クライアント接続受信機138は、永続的なクライアント開始通信接続を使用して、オンプレミスC Aゲートウェイ160におけるオンプレミスC A管理ゲートウェイ162に通知することができる。永続的なクライアント開始通信プロトコル（すなわち、Web S o c k e t、ロングポーリング等）は、クラウドによってホストされるサーバが可能な限り長くクライアント接続を開放した状態に保持し、データ（例えば、C A照合等のタスク結果）が入手可能な状態になる、またはタイムアウト閾値（例えば、1分を上回る長さ）が到達して初めて応答を送達する、技法を提供する。応答を受信した後、クライアントシステムは、即座に次の要求を送信することができる。いくつかの実装では、クライアント側において、単一の要求が、管理される。応答が、受信されると、クライアントは、新しい要求を開始し、本プロセスを必要な回数繰り返すことができる。

【0033】

遠隔C Aゲートウェイプラグイン130はさらに、オンプレミスにホストされたオンプレミスC Aゲートウェイ160についての構成情報および任意の状態情報の通信が、クラウド環境内に記憶されることを可能にする、キャッシュA P I 134を含む。例えば、構成情報、タスク要求/結果データ、および同等物は、クラウド環境内の遠隔C Aゲートウェイプラグインモジュール130において一元的に管理されることができる。C Aゲートウェイプラグイン168は、本情報にアクセスする必要があるときには随時、C A管理ゲートウェイ162におけるインベントリおよび構成同期化装置（例えば、同期化装置164）と通信することができる。C A管理ゲートウェイ162は、必要に応じてホストされるクラウド環境からデータをフェッチするために遠隔C Aゲートウェイプラグイン130におけるキャッシュA P I 134へのアクセスによってバックアップされる、メモリ内キャッシュを含む。

【0034】

1つまたはそれを上回るクライアントサーバは、遠隔C Aゲートウェイプラグイン130を管理し、それと通信する、オンプレミスC Aゲートウェイ160をホストすることができる。本開示の全体を通して使用される、用語「オンプレミス」は、本明細書に議論されるC Aモジュール（例えば、オンプレミスC Aゲートウェイ160）が、1つまたはそれを上回るクライアントサーバ150にインストールされるような、クライアントの地点に物理的に位置する、サーバ、デバイス、システム等を指す。オンプレミスC Aゲートウェイ160は、C A管理ゲートウェイ162と、C Aゲートウェイプラグイン168とを

含む。C A 管理ゲートウェイ 1 6 2 は、クライアント接続受信機 1 3 8 との永続的な通信のための、同期化装置 1 6 4 と、クライアント接続マネージャ 1 6 6 とを含む。同期化装置 1 6 4 は、必要に応じてホストされるクラウド環境からデータをフェッチするために遠隔 C A ゲートウェイプラグイン 1 3 0 におけるキャッシュ A P I 1 3 4 へのアクセスによってバックアップされる、メモリ内キャッシュを含む。C A ゲートウェイプラグイン 1 6 8 は、C A 管理ゲートウェイ 1 6 2 とオンプレミス C A ゲートウェイデバイス 1 7 0 上の C A アプリケーション 1 7 2 との間の通信を管理する。

【 0 0 3 5 】

例示の実装では、C A 管理ゲートウェイサービス（例えば、オンプレミス C A ゲートウェイ 1 6 0 ）が、1 つまたはそれを上回るクライアントサーバ 1 5 0 においてインストールされ、オンにされると、C A 管理ゲートウェイ 1 6 2 は、ネットワーク接続を開始する。例えば、C A 管理ゲートウェイ 1 6 2 は、クライアント接続マネージャ 1 6 6 を介して、ネットワーク 1 0 2 を通してクラウド環境内のクライアント接続受信機 1 3 8 へのネットワーク接続を確立する。本永続的なクライアント開始通信は、クライアント接続受信機 1 3 8 が、C A 管理ゲートウェイ 1 6 2 が構成されたこと、接続されたこと、およびタスクを受信する準備ができたことを、C A タスクデータベース 1 4 0 内に記録することを可能にする。いくつかの実装では、Web S o c k e t プロトコルが、永続的なクライアント開始通信のために使用されてもよい。Web S o c k e t プロトコルは、単一の T C P 接続を経由して全二重通信チャネルを提供する、コンピュータ通信プロトコルである。加えて、または代替として、ロングポーリング通信プロトコルが、永続的なクライアント開始通信のために使用されてもよい。「ロングポーリング」技法は、サーバが、可能な限り長い時間にわたって、クライアントの接続を開放された状態に保持し、データが入手可能な状態になる、またはタイムアウト閾値が、到達されて初めて応答を送達することを採択するものである。

【 0 0 3 6 】

本時点において（例えば、永続的なクライアント開始通信が確立された後）、クライアント接続マネージャ 1 6 6 およびクライアント接続受信機 1 3 8 は、C A 管理ゲートウェイ 1 6 2 が、タスクが実行される準備ができたときに通知され得るように、一定の接続を維持する。C A 管理ゲートウェイ 1 6 2 サービスが、任意の理由（機械再始動等）のために停止されると、本永続的なクライアント開始通信接続は、切断され、クライアント接続受信機 1 3 8 が、C A 管理ゲートウェイ 1 6 2 を、C A タスクデータベース 1 4 0 内でタスクを受信し、実行することが対応不可能であるものとしてマーキングすることを可能にするであろう。

【 0 0 3 7 】

いくつかの実装では、クラウドによってホストされる証明書ライフサイクル管理システム（例えば、C A ゲートウェイクラウドベースサーバ 1 2 0 ）とオンサイト C A システムとの間の通信を管理する例示的実行が、C L M システムがオンサイト C A システム（例えば、オンプレミス C A 1 7 0 ）においてタスクを実行するためのタスク要求を送信すると、開始され得る。例えば、C L M アプリケーション 1 1 2 を使用するユーザデバイス 1 1 0 は、タスク詳細を用いてクラウド環境（例えば、C A ゲートウェイクラウドベースサーバ 1 2 0 ）内の遠隔 C A ゲートウェイコア 1 2 2 にコンタクトする。これは、クラウド環境内の遠隔 C A ゲートウェイプラグイン 1 3 0 に、タスク割当 A P I 1 3 2 を利用させ、C A タスクデータベース 1 4 0 内に未処理のタスクを設置させる。遠隔 C A ゲートウェイプラグイン 1 3 0 におけるクライアント接続受信機 1 3 8 が、タスクが実行のために C A タスクデータベース 1 4 0 内に出現したことを認めると、クライアント接続受信機 1 3 8 は、既存の接続（例えば、永続的なクライアント開始通信プロトコル）を使用して、クライアント接続マネージャ 1 6 6 を介してクライアントサーバ 1 5 0 における C A 管理ゲートウェイ 1 6 2 に通知する。C A 管理ゲートウェイ 1 6 2 は、次いで、遠隔 C A ゲートウェイプラグイン 1 3 0 におけるタスク選別 A P I 1 3 6 と通信し、それを使用し、タスクを実行するための必要な詳細（例えば、タスク実行のための場所データ）を得ることがで

10

20

30

40

50

きる。タスクは、次いで、クライアントサーバ150におけるCAゲートウェイプラグイン168を呼び出すことによって実行され、これは、ひいては、オンプレミスCAデバイス170におけるCAアプリケーション172と通信する。

【0038】

加えて、オンプレミスCAデバイス170からの結果が、本例示的通信経路を逆に辿ることができる。例えば、CAアプリケーション172からのタスク結果が、CAゲートウェイプラグイン168を通してCA管理ゲートウェイ162に通信されることができる。タスク選別API136は、タスク結果データをCAタスクデータベース140内に追加することができる。タスク割当API132は、タスク結果データがCAタスクデータベース140内に記憶されていることを認めた後、次いで、タスク結果をCAゲートウェイコア122を介してタスク要求の発信者に返すことができる。CAゲートウェイコア122は、次いで、タスク結果（例えば、CA照合データ）をCLMシステム（例えば、CLMアプリケーション112を介してユーザデバイス110）に戻るよう通信することができる。本プロセスは、CLMシステムに同期すると考えられ、そのため、双方向使用のために非常に好適である。例えば、エンドユーザは、後続の時間においてCAとの通信に戻る必要なく、永続的なクライアント開始通信プロトコルを介して要求された直後に、要求されるタスクの成功および/または失敗を受信する。

【0039】

いくつかの実装では、例示的環境100のコンポーネント、サーバ、デバイス等の中の1つまたはそれを上回るものが、ハイパーバイザまたはコンテナのいずれかを使用して仮想化される。例えば、ハイパーバイザは、ハイパーバイザが異なる仮想機械を管理するホストオペレーティングシステムの上で実行される、完全オペレーティングシステムを利用してもよく、各仮想機械は、異なるオペレーティングシステムを利用してもよい。コンテナベースの仮想化（オペレーティングシステム仮想化とも称される）は、ゲストオペレーティングシステム全体を実行するように試行する代わりに、ホストオペレーティングシステムを利用して、本プロセスを隔離する。各コンテナは、各仮想環境に対応する。オペレーティングシステムは、仮想環境間のプロセス隔離を提供し、リソース管理を実施し、各プロセス、すなわち、各仮想環境または各コンテナのために、その独自のファイルシステム、メモリ、およびデバイスを指定する。

【0040】

図2は、本開示の実施例による、永続的なクライアント開始通信プロトコルを介した、クラウドによってホストされる証明書ライフサイクル管理システムを介した要求からオンプレミスCAにおいてタスクを実行するための方法のタイミング図200を図示する。タスク要求データメッセージが、デバイス110において発生され、そこからクラウドベースサーバ120に伝送される。しかしながら、クライアントサーバ150がCA管理ゲートウェイを介したクラウドベースサーバ120への永続的な通信プロトコルを開始するまで、クラウドベースサーバ120は、対応不可能通知を返すであろう。例えば、CA管理ゲートウェイ162サービスが、任意の理由（機械再始動等）のために停止されると、本永続的なクライアント開始通信接続は、切断され、クライアント接続受信機138が、CA管理ゲートウェイ162を、CAタスクデータベース140内でタスクを受信し、実行することが対応不可能であるものとしてマーキングすることを可能にするであろう。

【0041】

一定の通信接続が、クライアントサーバ150とクラウドベースサーバ120によって開始された後、次いで、タスク要求が、本システムによって処理されることができる。したがって、図2に図示されるように、タスク要求データメッセージが、デバイス110において発生され、そこからクラウドベースサーバ120に伝送され、その時点で、永続的なクライアント開始通信接続がオンであるため、タスク要求データメッセージは、事実上、クライアントサーバ150およびオンプレミスCAデバイス170に送信される。CAデバイス170は、クライアントサーバ150、クラウドベースサーバ120を通して、デバイス110に戻るよう、実行されたタスク結果メッセージを用いてタスク要求メッ

10

20

30

40

50

セージに応答する。例えば、本明細書において議論されるように、CLMシステムは、オンプレミスCA上でタスクを実行する必要があるとき、タスク詳細を用いてクラウド環境内のCAゲートウェイにコンタクトする。これは、クラウド環境内の遠隔CAゲートウェイプラグインに、タスク割当APIを利用させ、CAタスクデータベース内に未処理のタスクを設置させる。遠隔CAゲートウェイプラグインにおけるクライアント接続受信機が、タスクが実行のためにデータベース内に出現したことを認めると、クライアント接続受信機は、既存の一定のクライアント接続（例えば、Web Socketプロトコル、ロングポーリングプロトコル等の永続的なクライアント開始通信プロトコル）を使用して、クライアントサーバ150におけるCA管理ゲートウェイに通知する。CA管理ゲートウェイは、次いで、遠隔CAゲートウェイプラグインにおけるタスク選別APIと通信し、それを使用し、タスクを実行するための必要な詳細（例えば、タスク実行のための場所データ）を得ることができる。タスクは、次いで、クライアントサーバ150におけるCAゲートウェイプラグインを呼び出すことによって実行され、これは、ひいては、オンプレミスCAと通信する。オンプレミスCAからの結果が、次いで、本経路を逆に辿り、CAゲートウェイプラグインを通してタスク選別APIまで逆に辿る。タスク結果データは、次いで、CAタスクデータベース内に設置され、その場合、タスク割当APIが、次いで、クラウドベースサーバ120内のCAゲートウェイコア内の発信者に結果を返すことができ、これは、ひいては、タスク結果（例えば、CA照合データ）をCLMシステム（例えば、CLMアプリケーション112を介してユーザデバイス110）に戻すように通信する。

10

20

【0042】

図3は、クラウドによってホストされるCLMからオンプレミスCAへの通信のためのシステムを管理するための例示的プロセス300のフローチャートを図示する。プロセス300の動作は、例えば、図1の1つまたはそれを上回るCAゲートウェイクラウドベースサーバ120、および1つまたはそれを上回るクライアントサーバ150上のオンプレミスCAゲートウェイ160等の1つまたはそれを上回るデータ処理装置を含む、システムによって実装されることができる。プロセス300はまた、コンピュータ記憶媒体上に記憶される命令によって実装されることができ、その場合、データ処理装置を含むシステムによる命令の実行が、データ処理装置にプロセス300の動作を実施させる。

【0043】

例示的実装では、1つまたはそれを上回るCAゲートウェイクラウドベースサーバが、1つまたはそれを上回るユーザデバイスからのCLMアプリケーションから受信されるタスク要求の場所を管理する。1つまたはそれを上回るCAゲートウェイクラウドベースサーバのタスク管理プロトコルは、タスクが、クライアントの地点におけるオンプレミスCAゲートウェイによって取り扱われるように、複数のクライアントを管理することによって、冗長な負荷平衡化システムに基づく。例えば、要求されるタスクにサービス提供することが可能である、複数のクライアントが、存在し得、プロセス300の冗長な負荷平衡化システムは、タスクが有能なクライアントのうちの厳密に1つによって実施されることを確実にすることに関わる。

30

【0044】

本システムは、オンプレミスCAゲートウェイから一定の通信接続初期化を受信する（302）。一定の通信接続初期化は、クラウドベースサーバ上の遠隔証明機関ゲートウェイプラグインモジュールにおける、クライアント接続受信機（例えば、クライアント接続受信機138）によって受信されてもよい。一定の通信接続は、クラウドサーバとクライアントの地点におけるオンプレミスCAゲートウェイとの間に永続的なクライアント開始通信を提供する。いくつかの実装では、Web Socketプロトコルは、永続的なクライアント開始通信のために使用されてもよい。Web Socketプロトコルは、単一のTCP接続を経由して全二重通信チャネルを提供する、コンピュータ通信プロトコルである。加えて、または代替として、ロングポーリング通信プロトコルが、永続的なクライアント開始通信のために使用されてもよい。「ロングポーリング」技法は、サーバが、可能

40

50

な限り長い時間にわたって、クライアントの接続を開放された状態に保持し、データが入手可能な状態になる、またはタイムアウト閾値が、到達されて初めて応答を送達することを採択するものである。

【 0 0 4 5 】

本システムは、要求されるタスクを規定する、タスク要求と、タスク実行のための場所を規定する、識別子とを受信する（ 3 0 4 ）。タスク要求は、遠隔 C A ゲートウェイコア（例えば、遠隔 C A ゲートウェイコア 1 2 2 ）によって、ユーザデバイス上にインストールされる、C L M アプリケーション（例えば、ユーザデバイス 1 1 0 上の C L M アプリケーション 1 1 2 ）から受信されてもよい。例えば、C L M システムが、オンプレミス C A 上でタスクを実行する必要があるとき、C L M システムは、タスク詳細を用いてクラウド環境内の C A ゲートウェイにコンタクトする。

10

【 0 0 4 6 】

本システムは、要求されるタスクおよび要求されるタスクのためのタスク実行のための場所がオンプレミス C A デバイスにあることを決定する（ 3 0 6 ）。本システムは、要求されるタスクおよび遠隔 C A ゲートウェイプラグインモジュール（例えば、遠隔 C A ゲートウェイプラグインモジュール 1 3 0 ）上のタスク選別インターフェース（例えば、タスク選別 A P I 1 3 6 ）によって要求されるタスクのためのタスク実行のための場所を決定してもよい。例えば、タスク詳細を用いてクラウド環境内の C A ゲートウェイにコンタクトすることが、タスク割当 A P I と通信するように遠隔 C A ゲートウェイプラグインを開始させる。

20

【 0 0 4 7 】

要求されるタスクおよびタスクの場所がオンプレミス C A デバイスにあることを決定することに応答して、本システムは、タスク要求をタスク実行のための場所にリンクさせる、要求タスクデータエントリを記憶する（ 3 0 8 ）。本システムは、遠隔 C A ゲートウェイプラグインモジュール（例えば、遠隔 C A ゲートウェイプラグインモジュール 1 3 0 ）上のデータ記憶デバイス（例えば、C A タスクデータベース 1 4 0 ）内に要求タスクデータエントリを記憶してもよい。例えば、タスク詳細を用いてクラウド環境内の C A ゲートウェイにコンタクトすることが、タスク割当 A P I を使用し、C A タスクデータベース内に未処理のタスクを設置するように遠隔 C A ゲートウェイプラグインを開始させる。

【 0 0 4 8 】

30

本システムは、永続的なクライアント開始通信プロトコルを介して通知を提供する（ 3 1 0 ）。通知は、遠隔 C A ゲートウェイプラグインモジュール（例えば、遠隔 C A ゲートウェイプラグインモジュール 1 3 0 ）から 1 つまたはそれを上回るクライアントサーバ上のオンプレミス C A ゲートウェイ（例えば、1 つまたはそれを上回るクライアントサーバ 1 5 0 上のオンプレミス C A ゲートウェイ 1 6 0 ）に提供されてもよい。いくつかの実装では、遠隔 C A ゲートウェイプラグインモジュールは、永続的なクライアント開始通信プロトコルを介してオンプレミス C A ゲートウェイとの一定の通信接続を維持する。いくつかの実装では、永続的なクライアント開始通信プロトコルは、Web S o c k e t 通信プロトコルに基づく。代替として、いくつかの実装では、永続的なクライアント開始通信プロトコルは、ロングポーリング通信プロトコルに基づく。例えば、C A ゲートウェイクラウド環境内のクライアント接続受信機（例えば、クライアント接続受信機 1 3 8 ）が、要求タスクが実行のために C A タスクデータベース内に出現したことを認めると、クライアント接続受信機は、既存の永続的なクライアント接続を使用して、C A 管理ゲートウェイ（例えば、オンプレミス C A ゲートウェイ 1 6 0 上のオンプレミス C A 管理ゲートウェイ 1 6 2 ）に通知する。

40

【 0 0 4 9 】

通知の提供に応答して、本システムは、オンプレミス C A デバイスに、タスク実行のために要求されるタスクを提供する（ 3 1 2 ）。要求されるタスクは、1 つまたはそれを上回るクライアントサーバによってオンサイトにホストされるオンプレミス C A ゲートウェイ（例えば、オンプレミス C A ゲートウェイ 1 6 0 ）からオンプレミス C A デバイス（例

50

えば、オンプレミス C A デバイス 1 7 0) に提供されてもよい。

【 0 0 5 0 】

いくつかの実装では、プロセス 3 0 0 はさらに、オンプレミス C A ゲートウェイにおいて、オンプレミス C A デバイスから、オンプレミス C A デバイスによるタスク実行に基づく、タスク結果を受信することと、遠隔 C A ゲートウェイプラグインモジュールにおいて、永続的なクライアント開始通信プロトコルを介して、タスク結果を受信することと、データ記憶デバイス内に、タスク結果を記憶することと、タスク結果がデータ記憶デバイス内に受信されたことを決定することと、ユーザデバイスにタスク結果を提供することとを含む。例えば、C A からのタスク結果が、タスク要求経路を逆に辿り、C A ゲートウェイプラグインを通してタスク選別 A P I まで逆に辿る。結果データは、次いで、C A タスクデータベース内に記憶されてもよく、その場合、タスク割当 A P I は、C A ゲートウェイコア内の発信者への返しを開始してもよい。C A ゲートウェイコアは、ひいては、タスク結果を C L M システムに通信する。したがって、本送信および受信プロセスは、C L M システムに同期すると考えられ、そのため、(例えば、C L M アプリケーション 1 1 2 を利用するユーザデバイス 1 1 0 における)エンドユーザが、後に再びチェックする必要なく、要求された直後に、要求されるタスクの成功 / 失敗を把握する必要があるため、双方向使用のために非常に好適である。

10

【 0 0 5 1 】

例示的実装では、C A データベースは、キャッシュ A P I を利用するクラウド環境内にホストされる。キャッシュ A P I (例えば、キャッシュ A P I 1 3 4) は、オンプレミスにホストされた C A 管理ゲートウェイについての構成情報および任意の状態情報の通信が、クラウド環境内に記憶されることを可能にし、その場合、構成情報、タスク要求 / 結果データ、および同等物は、クラウド環境内の遠隔 C A ゲートウェイプラグインモジュールにおいて一元的に管理されることができる。C A ゲートウェイプラグインは、本情報にアクセスする必要があるときには随時、C A 管理ゲートウェイにおけるインベントリおよび構成同期化装置 (例えば、同期化装置 1 6 4) と通信することができる。C A 管理ゲートウェイ (例えば、C A 管理ゲートウェイ 1 6 2) は、必要に応じてホストされるクラウド環境からデータをフェッチするために遠隔 C A ゲートウェイプラグインにおけるキャッシュ A P I へのアクセスによってバックアップされる、メモリ内キャッシュを含む。

20

【 0 0 5 2 】

図 4 は、C A コンポーネントのためのタスクの送信 / 受信および処理のための、本明細書に説明されるソフトウェアコンポーネントを実行することが可能である、コンピュータ 4 0 2 のための例示的コンピュータアーキテクチャ 4 0 0 を図示する。図 4 に示されるコンピュータアーキテクチャ 4 0 0 (本明細書では「サーバ」とも称される) は、サーバコンピュータ、ワークステーション、デスクトップコンピュータ、ラップトップ、または他のコンピューティングデバイスを例証し、ホストサーバまたは他のコンピューティングプラットフォーム上で実行するものとして説明される、本明細書に提示されるソフトウェアコンポーネントの任意の側面を実行するために利用されてもよい。コンピュータ 4 0 2 は、好ましくは、多数のコンポーネントまたはデバイスがシステムバスまたは他の電気通信経路を介して接続され得るプリント回路基板である、ベース基板、すなわち、「マザーボード」を含む。一例証的实施形態では、1つまたはそれを上回る中央処理ユニット (C P U) 4 0 4 が、チップセット 4 0 6 と連動して動作する。C P U 4 0 4 は、コンピュータ 4 0 2 の動作のために必要な算術および論理動作を実施する、プログラマブルプロセッサであることができる。

30

40

【 0 0 5 3 】

C P U 4 0 4 は、好ましくは、これらの状態を区別し、変化させる、切替要素の操作を通して、1つの離散した物理的状态から次のものに遷移することによって、動作を実施する。切替要素は、概して、フリップフロップ等の2つの二元状態のうち的一方を維持する、電子回路と、論理ゲート等の、1つまたはそれを上回る他の切替要素の状態の論理的組み合わせに基づいて出力状態を提供する、電子回路とを含んでもよい。これらの基本的切

50

替要素は、レジスタ、加算器／減算器、算術論理ユニット、浮動小数点ユニット、または同等物を含む、より複雑な論理回路を生成するために組み合わせられてもよい。

【 0 0 5 4 】

チップセット 4 0 6 は、CPU 4 0 4 とベース基板上のコンポーネントおよびデバイスの残部との間にインターフェースを提供する。チップセット 4 0 6 は、メモリ 4 0 8 にインターフェースを提供してもよい。メモリ 4 0 8 は、コンピュータ 4 0 2 内でメインメモリとして使用される、ランダムアクセスメモリ (RAM) を含んでもよい。メモリ 4 0 8 はさらに、コンピュータ 4 0 2 を起動し、種々のコンポーネントとデバイスとの間で情報を伝達することに役立つ、基本ルーチンを記憶するための、読取専用メモリ (ROM) または不揮発性 RAM (NVRAM) 等のコンピュータ可読記憶媒体を含んでもよい。ROM または NVRAM はまた、本明細書に説明される実施形態による、コンピュータ 4 0 2 の動作のために必要な他のソフトウェアコンポーネントを記憶してもよい。

10

【 0 0 5 5 】

種々の実施形態によると、コンピュータ 4 0 2 は、コンピュータ 4 0 2 を本デバイスおよび他の遠隔コンピュータに接続する、1 つまたはそれを上回るネットワーク 4 1 2、ローカルエリアネットワーク (LAN)、広域ネットワーク (WAN)、インターネット、または当技術分野において公知である任意の他のネットワーキングトポロジを通した、遠隔コンピューティングデバイスへの論理的接続を使用して、ネットワーク化された環境内で動作してもよい。チップセット 4 0 6 は、ギガビットイーサネット (登録商標) アダプタ等の 1 つまたはそれを上回るネットワークインターフェースコントローラ (NIC) 4 1 0 を通してネットワークコネクティビティを提供するための機能性を含む。例えば、NIC 4 1 0 は、コンピュータ 4 0 2 をユーティリティプロバイダのシステム内の他のコンピュータデバイスに接続することが可能であってもよい。コンピュータを本明細書に説明されるもの以外の他のタイプのネットワークおよび遠隔コンピュータシステムに接続する、任意の数の NIC 4 1 0 が、コンピュータ 4 0 2 内に存在し得ることを理解されたい。

20

【 0 0 5 6 】

コンピュータ 4 0 2 は、コンピュータ 4 0 2 のための不揮発性記憶装置を提供する、少なくとも 1 つの大容量記憶デバイス 4 1 8 に接続されてもよい。大容量記憶デバイス 4 1 8 は、本明細書により詳細に説明される、システムプログラム、アプリケーションプログラム、他のプログラムモジュール、およびデータを記憶してもよい。大容量記憶デバイス 4 1 8 は、チップセット 4 0 6 に接続される記憶装置コントローラ 4 1 4 を通して、コンピュータ 4 0 2 に接続されてもよい。大容量記憶デバイス 4 1 8 は、1 つまたはそれを上回る物理的記憶ユニットから成ってもよい。記憶装置コントローラ 4 1 4 は、コンピュータと物理的記憶デバイスとの間を物理的に接続し、その間でデータを伝達するために、シリアル接続 SCSI (SAS) インターフェース、シリアル高度技術アタッチメント (SATA) インターフェース、ファイバチャネル (FC) インターフェース、または他の標準インターフェースを通して、物理的記憶ユニットとインターフェースをとってもよい。

30

【 0 0 5 7 】

コンピュータ 4 0 2 は、記憶されている情報を反映するように物理的記憶ユニットの物理状態を変換することによって、大容量記憶デバイス 4 1 8 上にデータを記憶してもよい。物理状態の具体的な変換は、本説明の異なる実装の種々の要因に依存し得る。そのような要因の実施例は、限定ではないが、物理的記憶ユニットを実装するために使用される技術、大容量記憶デバイス 4 1 8 が、一次または二次記憶装置として特徴付けられているかどうか、または同等物を含み得る。例えば、コンピュータ 4 0 2 は、磁気ディスクドライブユニット内の特定の場所の磁気特性、光学記憶ユニット内の特定の場所の反射または屈折特性、ソリッドステート記憶ユニット内の特定のコンデンサ、トランジスタ、または他の離散コンポーネントの電気特性を改変するための命令を記憶装置コントローラ 4 1 4 を通して発行することによって、情報を大容量記憶デバイス 4 1 8 に記憶してもよい。物理媒体の他の変換も、本説明の範囲および精神から逸脱することなく可能性として考えられ、前述の実施例は、本説明を促進するために提供されるにすぎない。コンピュータ 4 0 2

40

50

はさらに、物理的記憶ユニット内の1つまたはそれを上回る特定場所の物理状態または特性を検出することによって、大容量記憶デバイス418から情報を読み取ってもよい。

【0058】

大容量記憶デバイス418は、コンピュータ402の動作を制御するために利用される、オペレーティングシステム420を記憶してもよい。いくつかの実施形態によると、オペレーティングシステムは、LINUX（登録商標）オペレーティングシステムを含む。別の実施形態によると、オペレーティングシステムは、MICROSOFT Corporation（Redmond, Wash）製のWINDOWS（登録商標）SERVERオペレーティングシステムを含む。さらなる実施形態によると、オペレーティングシステムは、UNIX（登録商標）またはSOLARIS（登録商標）オペレーティングシステムを含んでもよい。他のオペレーティングシステムもまた、利用され得ることを理解されたい。大容量記憶デバイス418は、本明細書に説明されるように、コンピュータ402によって、CAゲートウェイ通信のための通信ネットワーク内の通信を管理するために利用される、CAMジュール422等のコンピュータ402によって利用される、他のシステムまたはアプリケーションプログラムおよびデータを記憶してもよい。

10

【0059】

いくつかの実施形態では、大容量記憶デバイス418は、コンピュータ402の中にロードされると、コンピュータ402を、汎用目的コンピューティングシステムであるものから、本明細書に説明される実施形態を実装することが可能である、特殊目的コンピュータに変換する、コンピュータ実行可能命令を用いてエンコードされてもよい。これらのコンピュータ実行可能命令は、上記に説明されるように、CPU404が状態間で遷移する方法を規定することによって、コンピュータ402を変換する。いくつかの実施形態によると、ホストサーバ106の観点から、大容量記憶デバイス418は、本明細書に説明されるように、コンピュータ402によって実行されると、クラウドによってホストされるCLMからオンプレミスCAへの通信を管理する、プロセス300の一部を実施する、コンピュータ実行可能命令を記憶する。さらなる実施形態では、コンピュータ402は、大容量記憶デバイス418に加えて、またはその代替物として、他のコンピュータ可読記憶媒体へのアクセスを有してもよい。

20

【0060】

コンピュータ402はまた、キーボード、マウス、タッチパッド、タッチスクリーン、電子スタイラス、または他のタイプの入力デバイス等、いくつかの入力デバイスからの入力を受信し、処理するための入/出力コントローラ430を含んでもよい。同様に、入/出力コントローラ430は、コンピュータモニタ、フラットパネルディスプレイ、デジタルプロジェクタ、プリンタ、プロッタ、または他のタイプの出力デバイス等のディスプレイデバイスに出力を提供してもよい。コンピュータ402が、図4に示されるコンポーネントの全てを含まない場合があること、図4に明示的に示されていない他のコンポーネントを含み得ること、または図4に示されるものと完全に異なるアーキテクチャを利用し得ることを理解されたい。

30

【0061】

当業者は、周知のシステム、方法、コンポーネント、デバイス、および回路が、本明細書に説明される例示的実装のより関連のある側面を曖昧にしないように、網羅的詳細において説明されていないことを理解するであろう。また、他の有効な側面および/または異型は、本明細書に説明される具体的な詳細の全てを含むわけではない。したがって、いくつかの詳細は、図面に示されるような例示的側面の徹底的な理解を提供するために説明される。また、図面は、本開示のいくつかの例示的実施形態を示すにすぎず、したがって、限定するものと見なされるべきではない。

40

【0062】

本明細書に説明される主題および動作の実施形態は、デジタル電子回路網において、または本明細書に開示される構造およびそれらの構造均等物を含む、コンピュータソフトウェア、ファームウェア、またはハードウェアにおいて、またはそれらのうちの1つまたは

50

それを上回るものの組み合わせにおいて、実装されることができる。本明細書に説明される主題の実施形態は、1つまたはそれを上回るコンピュータプログラム、すなわち、データ処理装置による実行のために、またはその動作を制御するために、コンピュータ記憶媒体上にエンコードされる、コンピュータプログラム命令の1つまたはそれを上回るモジュールとして、実装されることができる。代替として、または加えて、プログラム命令は、人工的に発生される伝搬信号、例えば、データ処理装置による実行のために好適な受信機装置への伝送のための情報をエンコードするように発生される、機械で発生される電気、光学、または電磁信号上で、エンコードされることができる。コンピュータ記憶媒体は、コンピュータ可読記憶デバイス、コンピュータ可読記憶基板、ランダムまたはシリアルアクセスメモリアレイまたはデバイス、またはそれらのうちの1つまたはそれを上回るものの組み合わせである、またはその中に含まれることができる。また、コンピュータ記憶媒体は、伝搬信号ではないが、コンピュータ記憶媒体は、人工的に発生される伝搬信号でエンコードされる、コンピュータプログラム命令のソースまたは宛先であることができる。コンピュータ記憶媒体はまた、1つまたはそれを上回る別個の物理的コンポーネントまたは媒体（例えば、複数のCD、ディスク、または他の記憶デバイス）である、またはそれに含まれることができる。

10

【0063】

本明細書に説明される動作は、1つまたはそれを上回るコンピュータ可読記憶デバイス上に記憶される、または他のソースから受信されるデータ上でデータ処理装置によって実施される、動作として実装されることができる。

20

【0064】

用語「データ処理装置」は、実施例として、プログラマブルプロセッサ、コンピュータ、システムオンチップ、または前述の複数のものまたは組み合わせを含む、データを処理するためのあらゆる種類の装置、デバイス、および機械を包含する。装置は、特殊用途論理回路網、例えば、FPGA（フィールドプログラマブルゲートアレイ）またはASIC（特定用途向け集積回路）を含むことができる。装置はまた、ハードウェアに加えて、当該コンピュータプログラムのための実行環境を生成するコード、例えば、プロセッサファームウェア、プロトコルスタック、データベース管理システム、オペレーティングシステム、クロスプラットフォームランタイム環境、仮想マシン、またはそれらのうちの1つまたはそれを上回るものの組み合わせを成すコードを含むことができる。装置および実行環境は、ウェブサービス、分散コンピューティング、およびグリッドコンピューティングインフラストラクチャ等の種々の異なるコンピューティングモデルインフラストラクチャを実現することができる。

30

【0065】

コンピュータプログラム（プログラム、ソフトウェア、ソフトウェアアプリケーション、スクリプト、またはコードとしても公知である）は、コンパイラ型またはインタープリタ型言語、宣言型または手続き型言語を含む、任意の形態のプログラミング言語で書き込まれることができ、これは、独立型プログラムとして、またはコンピューティング環境内の使用のために好適なモジュール、コンポーネント、サブルーチン、オブジェクト、または他のユニットとしてを含む、任意の形態で展開されることができる。コンピュータプログラムは、ファイルシステム内のファイルに対応し得るが、その必要はない。プログラムは、他のプログラムまたはデータを保持するファイル（例えば、マークアップ言語文書内に記憶された1つまたはそれを上回るスクリプト）の一部内に、当該プログラム専用の単一のファイル内に、または複数の協調ファイル（例えば、1つまたはそれを上回るモジュール、サブプログラム、またはコードの一部を記憶するファイル）内に記憶されることができる。コンピュータプログラムは、1つのコンピュータ上で、または1つの地点に位置し、または複数の地点を横断して分散され、通信ネットワークによって相互接続される複数のコンピュータ上で、実行されるように展開されることができる。

40

【0066】

本明細書に説明されるプロセスおよび論理フローは、入力データに対して動作し、出力

50

を発生させることによってアクションを実施するように、1つまたはそれを上回るコンピュータプログラムを実行する、1つまたはそれを上回るプログラマブルプロセッサによって、実施されることができる。プロセスおよび論理フローはまた、特殊用途論理回路網、例えば、FPGA（フィールドプログラマブルゲートアレイ）またはASIC（特定用途向け集積回路）によって実施されることができ、装置もまた、それとして実装されることができる。

【0067】

コンピュータプログラムの実行のために好適なプロセッサは、実施例として、汎用および特殊目的マイクロプロセッサの両方、および任意の種類のデジタルコンピュータのいずれか1つまたはそれを上回るプロセッサを含む。概して、プロセッサは、読取専用メモリまたはランダムアクセスメモリまたは両方から、命令およびデータを受信するであろう。コンピュータの不可欠な要素は、命令に従ってアクションを実施するためのプロセッサ、および命令およびデータを記憶するための1つまたはそれを上回るメモリデバイスである。概して、コンピュータはまた、データを記憶するための1つまたはそれを上回る大容量記憶デバイス、例えば、磁気、磁気光学ディスク、または光ディスクを含む、またはそこからデータを受信する、またはそこにデータを転送する、または両方を行うように、動作可能に結合されるであろう。しかしながら、コンピュータは、そのようなデバイスを有する必要はない。また、コンピュータは、別のデバイス、例えば、ほんの数例を挙げると、モバイル電話、携帯情報端末（PDA）、モバイルオーディオまたはビデオプレーヤ、ゲーム機、全地球測位システム（GPS）受信機、またはポータブル記憶デバイス（例えば、ユニバーサルシリアルバス（USB）フラッシュドライブ）に埋設されることができる。コンピュータプログラム命令およびデータを記憶するために好適なデバイスは、実施例として、半導体メモリデバイス、例えば、EPROM、EEPROM、およびフラッシュメモリデバイス、磁気ディスク、例えば、内部ハードディスクまたはリムーバブルディスク、磁気光学ディスク、およびCD-ROMおよびDVD-ROMディスクを含む、あらゆる形態の不揮発性メモリ、媒体、およびメモリデバイスを含む。プロセッサおよびメモリは、特殊目的論理回路網によって補完される、またはそれに組み込まれることができる。

【0068】

ユーザとの相互作用を提供するために、本明細書に説明される主題の実施形態が、情報をユーザに表示するためのディスプレイデバイス、例えば、CRT（陰極線管）またはLCD（液晶ディスプレイ）モニタと、それによってユーザが入力をコンピュータに提供し得る、キーボードおよびポインティングデバイス、例えば、マウスまたはトラックボールとを有する、コンピュータ上で実装されることができる。他の種類のデバイスも、同様にユーザとの相互作用を提供するために使用されることができ、例えば、ユーザに提供されるフィードバックは、任意の形態の感覚フィードバック、例えば、視覚フィードバック、聴覚フィードバック、または触覚フィードバックであり得、ユーザからの入力、音響、発話、または触覚入力を含む、任意の形態で受信されることができる。加えて、コンピュータは、ユーザによって使用されるデバイスに文書を送信し、そこから文書を受信することによって、例えば、ウェブブラウザから受信される要求に回答して、ウェブページをユーザのクライアントデバイス上のウェブブラウザに送信することによって、ユーザと相互作用することができる。

【0069】

本明細書に説明される主題の実施形態は、例えば、データサーバとして、バックエンドコンポーネントを含む、またはミドルウェアコンポーネント、例えば、アプリケーションサーバを含む、またはフロントエンドコンポーネント、例えば、それを通してユーザが本明細書に説明される主題の実装と相互作用し得るグラフィカルユーザインターフェースまたはウェブブラウザを有する、クライアントコンピュータ、または1つまたはそれを上回るそのようなバックエンド、ミドルウェア、またはフロントエンドコンポーネントの任意の組み合わせを含む、コンピューティングシステム内に実装されることができる。システムのコンポーネントは、任意の形態または媒体のデジタルデータ通信、例えば、通信ネッ

10

20

30

40

50

トワークによって、相互接続されることができる。通信ネットワークの実施例は、ローカルエリアネットワーク（「LAN」）および広域ネットワーク（「WAN」）、インターネット（例えば、インターネット）、およびピアツーピアネットワーク（例えば、アドホックピアツーピアネットワーク）を含む。

【0070】

コンピューティングシステムは、クライアントと、サーバとを含むことができる。クライアントおよびサーバは、概して、相互から遠隔にあり、典型的には、通信ネットワークを通して相互作用する。クライアントおよびサーバの関係は、個別のコンピュータ上で起動し、相互にクライアント-サーバ関係を有する、コンピュータプログラムにより、生じる。いくつかの実装では、サーバは、（例えば、クライアントデバイスと相互作用するユーザにデータを表示し、ユーザからユーザ入力を受信する目的のために）データ（例えば、HTMLページ）をクライアントデバイスに伝送する。クライアントデバイスにおいて発生されるデータ（例えば、ユーザ相互作用の結果）が、サーバにおいてクライアントデバイスから受信されることができる。

10

【0071】

本明細書は、多くの具体的実装詳細を含有するが、これらは、任意の発明または請求されるものの範囲への限定としてではなく、むしろ、特定の発明の特定の实装に特有の特徴の説明として解釈されるべきである。別個の実施形態の文脈において本明細書に説明されるある特徴はまた、単一の実施形態において組み合わせられて実装されることもできる。逆に、単一の実施形態の文脈において説明される種々の特徴はまた、複数の実施形態において別個に、または任意の好適な副次的組み合わせにおいて実装されることもできる。また、特徴がある組み合わせにおいて作用するものとして上記に説明され、さらにはそのようなものとして最初に請求され得るが、請求される組み合わせからの1つまたはそれを上回る特徴は、ある場合には、その組み合わせから削除されることができ、請求される組み合わせは、副次的組み合わせまたは副次的組み合わせの変形例を対象とし得る。

20

【0072】

同様に、動作は、特定の順序で図面に描写されるが、これは、望ましい結果を達成するために、そのような動作が示される特定の順序で、または連続順序で実施される、または全ての図示される動作が実施されることを要求するものとして理解されるべきではない。ある状況では、マルチタスクおよび並列処理が、有利であり得る。また、上記に説明される実装における種々のシステムコンポーネントの分離が、全ての実施形態におけるそのような分離を要求するものとして理解されるべきではなく、説明されるプログラムコンポーネントおよびシステムが、概して、単一のソフトウェア製品においてともに統合される、または複数のソフトウェア製品にパッケージ化され得ることを理解されたい。

30

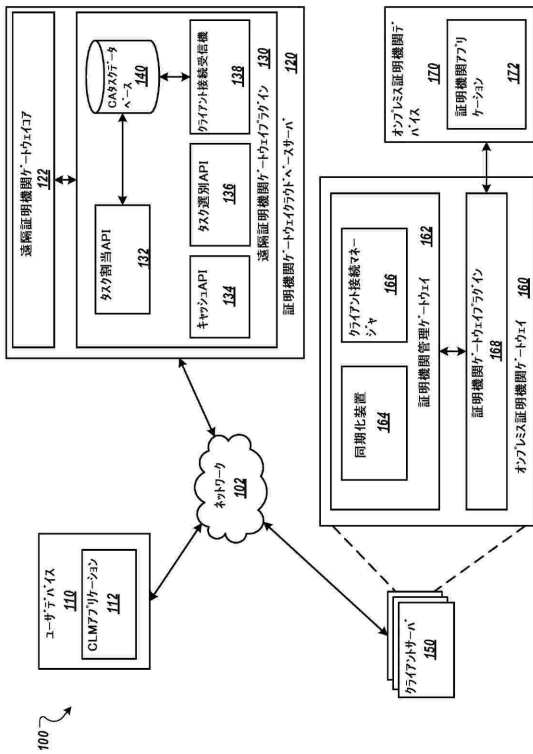
【0073】

したがって、本主題の特定の实施形態が、説明された。他の実装も、以下の請求項の範囲内である。ある場合には、請求項に列挙されるアクションは、異なる順序で実施され、依然として、望ましい結果を達成することができる。加えて、付随の図に描写されるプロセスは、望ましい結果を達成するために、必ずしも示される特定の順序または連続順序を要求するわけではない。ある実装では、マルチタスクおよび並列処理が、有利であり得る。

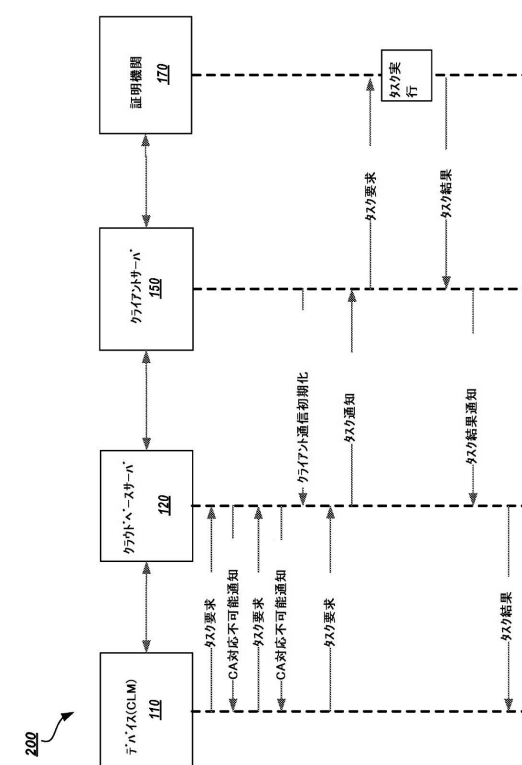
40

【図面】

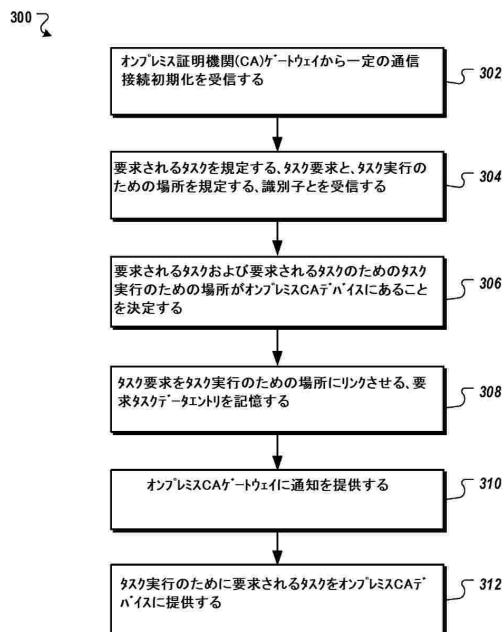
【 図 1 】



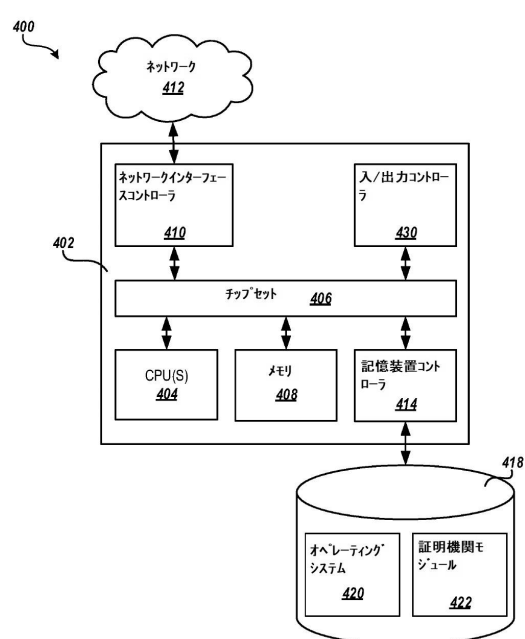
【圖 2】



【圖 3】



【圖 4】



フロントページの続き

- (72)発明者 ブローチ , ジョナサン
 アメリカ合衆国 オハイオ 4 4 1 3 1 , インディペンデンス , イースト プレザント バレー ロ
 ード 6 8 3 5
- (72)発明者 ショーター , エドワード
 アメリカ合衆国 オハイオ 4 4 2 6 2 , マンロー フォールズ , リバー パーク ブールバード 1 4 7
- (72)発明者 ウィーラー , レックス エドワード
 アメリカ合衆国 オレゴン 9 7 2 2 5 , ポートランド , エスダブリュー レーンウッド ストリ
 ート 1 1 4 4 5
- 審査官 武田 広太郎
- (56)参考文献 特表 2 0 2 0 - 5 0 2 6 7 2 (J P , A)
 特開 2 0 1 5 - 2 2 6 3 2 2 (J P , A)
 特表 2 0 1 7 - 5 2 8 9 6 3 (J P , A)
 特開 2 0 1 9 - 1 9 2 9 5 3 (J P , A)
- (58)調査した分野 (Int.Cl. , D B 名)
 G 0 6 F 9 / 4 4
 G 0 6 F 2 1 / 6 0