(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2017-517823
(P2017-517823A)
(43)公表日　平成29年6月29日(2017.6.29)

(51)Int.Cl.		F I		テーマコード（参考）
G06F 21/33	(2013.01)	G06F	21/33	
G06F 21/45	(2013.01)	G06F	21/45	

審査請求 未請求　予備審査請求 有　（全 53 頁）

(21)出願番号	特願2017-502760 (P2017-502760)
(86)(22)出願日	平成27年3月23日 (2015.3.23)
(85)翻訳文提出日	平成28年11月25日 (2016.11.25)
(86)国際出願番号	PCT/US2015/021919
(87)国際公開番号	WO2015/148331
(87)国際公開日	平成27年10月1日 (2015.10.1)
(31)優先権主張番号	14/227,419
(32)優先日	平成26年3月27日 (2014.3.27)
(33)優先権主張国	米国 (US)

(71)出願人　314015767
マイクロソフト　テクノロジー　ライセンシング，エルエルシー
アメリカ合衆国　ワシントン州　９８０５２　レッドモンド　ワン　マイクロソフト　ウェイ
(74)代理人　100140109
弁理士　小野　新次郎
(74)代理人　100075270
弁理士　小林　泰
(74)代理人　100101373
弁理士　竹内　茂雄
(74)代理人　100118902
弁理士　山本　修

最終頁に続く

(54)【発明の名称】機械生成認証トークンによってサービスを運用する技法

(57)【要約】
機械生成認証トークンによってサービスを運用する技法であって、クライアントの第１アカウントに関連付けられたクライアント認証情報に少なくとも部分的に基づいて、クライアント・デバイスとの安全な接続を確立し、クライアントの第１アカウントに関連付けられた１つ以上のアカウントのアカウント情報を求める要求を受け、第１アカウントに関連付けられた第２アカウントについてのアカウント情報をクライアントにクライアント・デバイスを通じて提供し、第２アカウントのために認証トークンを生成する要求を受け、クライアントに関連付けられたクライアント認証情報に基づいて認証トークンを生成する要求の有効性を判断する認証トークン管理コンポーネントと、第２アカウントのために認証トークンを生成するトークン生成コンポーネントと含む。他の実施形態についても記載し特許請求する。
【選択図】図１

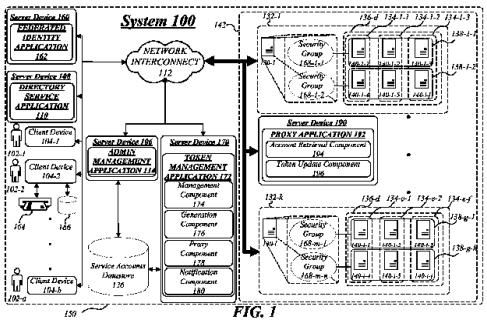

FIG. 1

【特許請求の範囲】
【請求項１】
装置であって、
プロセッサー回路と、
前記プロセッサー回路による実行のためのサーバー・アプリケーションと、
を含み、前記サーバー・アプリケーションが管理コンポーネントを含み、前記管理コンポーネントが、
少なくとも部分的に、前記クライアントの第１アカウントに関連付けられたクライアント認証情報に基づいて、クライアント・デバイスとの安全な接続を確立し、
前記クライアントの第１アカウントに関連付けられた１つ以上のアカウントのアカウント情報を求める要求を受け、
前記第１アカウントに関連付けられた第２アカウントについてのアカウント情報を前記クライアントに、前記クライアント・デバイスを通じて提供し、
前記第２アカウントのために認証トークンを生成する要求を受け、
前記クライアントに関連付けられた前記クライアント認証情報に基づいて、前記認証トークンを生成する要求の有効性を判断する、装置。
【請求項２】
請求項１記載の装置において、前記サーバー・アプリケーションが、更に、
ディレクトリー・サービス・サーバー・デバイスによって管理される前記１つ以上のアカウントのアカウント情報を引き出すように構成されたトークン管理プロキシー・アプリケーションにプロキシー認証情報の一部を提供することによって、前記クライアントの第１アカウントに関連付けられた１つ以上のアカウントのアカウント情報を要求するプロキシー・コンポーネントを含む、装置。
【請求項３】
請求項２記載の装置において、前記プロキシー・コンポーネントが、更に、前記１つ以上のアカウントのアカウント情報を求める前記要求に応答して、前記トークン管理プロキシー・アプリケーションから、前記第１アカウントに関連付けられた第２アカウントについてのアカウント情報を受ける、装置。
【請求項４】
請求項１記載の装置において、前記サーバー・アプリケーションが、更に、
前記第２アカウントのために認証トークンを生成するトークン生成コンポーネントと、
クライアントによる使用のために、前記認証トークンを前記クライアントに、前記安全な接続を介し前記クライアント・デバイスを通じて供給する通知コンポーネントと、
を含む、装置。
【請求項５】
請求項２記載の装置において、前記プロキシー・コンポーネントが、更に、前記第２アカウントに関連付けられたアカウント情報と、前記生成された認証トークンと、前記プロキシー認証情報の一部とを、前記ディレクトリー・サービス・サーバー・デバイスによって管理される前記第２アカウントに関連付けられた前記認証トークンを更新するように構成されたトークン管理プロキシー・アプリケーションに提供する、装置。
【請求項６】
請求項１記載の装置において、前記クライアント・アカウントに関連付けられた前記クライアント認証情報が、ディジタル証明書とアイデンティティ・トークンに関連付けられた個人識別番号（ＰＩＮ）とを含み、前記認証トークンが、少なくとも部分的に長さパラメーターとキャラクター・クラス・パラメーターとに基づいて生成された平文ランダム・パスワードである、装置。
【請求項７】
請求項１記載の装置において、前記認証トークンを生成する要求がトークン要求情報と関連付けられ、前記トークン要求情報が、少なくとも、前記第２アカウントについてのアカウント情報を含む、装置。

【請求項８】
複数の命令を含む少なくとも１つの機械読み取り可能記憶媒体であって、前記命令が、計算デバイス上において実行されることに応答して、請求項１から７までのいずれか１項記載の装置を、前記計算デバイスに実現させる、少なくとも１つの機械読み取り可能記憶媒体。
【請求項９】
コンピューター実装方法であって、
クライアントの第１アカウントに関連付けられたクライアント認証情報に少なくとも部分的に基づいて、クライアント・デバイスとの安全な接続を確立するステップと、
前記クライアントの第１アカウントに関連付けられた１つ以上のアカウントのアカウント情報を求める要求を受けるステップと、
回路によって、前記第１アカウントに関連付けられた第２アカウントについてのアカウント情報を前記クライアントに、前記クライアント・デバイスを通じて、提供するステップと、
前記第２アカウントのために認証トークンを生成する要求を受けるステップと、
前記クライアントに関連付けられた前記クライアント認証情報に基づいて、前記認証トークンを生成する要求の有効性を判断するステップと、
を含む、コンピューター実装方法。
【請求項１０】
請求項９記載のコンピューター実装方法であって、更に、
ディレクトリー・サービス・サーバー・デバイスによって管理される前記１つ以上のアカウントのアカウント情報を引き出すように構成されたトークン管理プロキシー・アプリケーションに少なくともプロキシー認証情報を提供することによって、前記クライアントの第１アカウントに関連付けられた１つ以上のアカウントの前記アカウント情報を要求するステップを含む、コンピューター実装方法。
【請求項１１】
請求項９記載のコンピューター実装方法であって、更に、
前記第２アカウントのために前記認証トークンを生成するステップと、
前記クライアントによる使用のために、少なくとも前記認証トークンを前記クライアントに、前記クライアント・デバイスを通じて前記安全な接続を介して、供給するステップと、
を含む、コンピューター実装方法。
【請求項１２】
請求項９記載のコンピューター実装方法であって、更に、
前記第２アカウントに関連付けられたアカウント情報と、前記生成された認証トークンと、プロキシー認証情報の一部とを、ディレクトリー・サービス・サーバー・デバイスによって管理される前記第２アカウントに関連付けられた前記認証トークンを更新するように構成されたトークン管理プロキシー・アプリケーションに提供するステップを含む、コンピューター実装方法。
【請求項１３】
請求項９から１２までのいずれか１項記載のコンピューター実装方法を実行する手段を含む装置。
【請求項１４】
複数の命令を含む少なくとも１つの機械読み取り可能記憶媒体であって、前記命令が、計算デバイス上において実行されることに応答して、請求項９から１２までのいずれか１項記載の方法を前記計算デバイスに実行させる、少なくとも１つの機械読み取り可能記憶媒体。
【請求項１５】
命令を含む少なくとも１つのコンピューター読み取り可能記憶媒体であって、前記命令が実行されると、システムに、

クライアントの第１アカウントに関連付けられたクライアント認証情報に少なくとも部分的に基づいて、トークン管理アプリケーションとの安全な接続を確立させ、
前記クライアントの第１アカウントに関連付けられた１つ以上のアカウントのアカウント情報を要求させ、
前記要求に応答して、第２アカウントについてのアカウント情報を受けさせ、
前記第２アカウントに関連付けられた認証トークンを生成することを要求させる、
少なくとも１つのコンピューター読み取り可能記憶媒体。
【発明の詳細な説明】
【背景技術】
【０００１】
[0001] 計算システムや通信システムを設計するために今日利用可能な種々の方法が速いペースで開発されていることから、多数のユーザーがシステムの１つ以上のサービスをホストするサーバーにアクセスして、これらのサーバーを検査し、アップグレードし、デバッグし、開発し、展開し、および／または維持する目的を果たす必要があると考えられる。
【発明の概要】
【発明が解決しようとする課題】
【０００２】
しかしながら、ユーザーの増大は、ユーザー・アカウントの増大、アクセス・レベルの増大、および付随するセキュリティ・リスクの増大も招くおそれがある。
【課題を解決するための手段】
【０００３】
[0002] 以下に提示するのは、本明細書において説明する新規な実施形態の基本的な理解を得るための、簡略化された摘要である。この摘要は、広範な全体像ではなく、主要な／肝要なエレメントを識別することを意図するのでもなく、その範囲を明確に定めることを意図するのでもない。その唯一の目的は、後に提示される更に詳細な説明に対する序文として、簡略化した形態で一部の概念を提示することである。
【０００４】
[0003] 種々の実施形態は、一般的に、機械生成認証トークンによってサービスを運用することによって、ネットワーク・セキュリティを強化する技法を対象とする。ある実施形態は、特に、１つ以上のサービス・アカウントに関連付けられた認証トークンを管理する技法を対象とする。
【０００５】
[0004] 一実施形態では、例えば、装置は、プロセッサー回路と、このプロセッサー回路による実行のためのサーバー・アプリケーションとを含むことができる。サーバー・アプリケーションは、管理コンポーネントを含むことができる。管理コンポーネントは、少なくとも部分的にクライアントの第１アカウントに関連付けられたクライアント認証情報に基づいて、クライアント・デバイスとの安全な接続を確立し、クライアントの第１アカウントに関連付けられた１つ以上のアカウントのアカウント情報を求める要求を受け、第１アカウントに関連付けられた第２アカウントについてのアカウント情報をクライアントに、クライアント・デバイスを通じて提供し、第２アカウントのために認証トークンを生成する要求を受け、クライアントに関連付けられたクライアント認証情報に基づいて、認証トークンを生成するためにこの要求の有効性を判断する。サーバー・アプリケーションは、更に、第２アカウントのために認証トークンを生成するトークン生成コンポーネントと、クライアントによる使用のために認証トークンをクライアントに、安全な接続を介してクライアント・デバイスを通じて供給する通知コンポーネントも含むことができる。他の実施形態についても説明し、特許請求する。
【０００６】
[0005] 以上の目的および関連する目的の遂行のために、本明細書では、以下の詳細な説明および添付図面に関連付けて、ある種の例示的態様について説明する。これらの態様

は、本明細書において開示する原理を実施することができる種々の方法を示し、その全ての態様およびその均等物が、特許請求する主題の範囲に該当することを意図している。他の利点および新規な特徴も、以下の詳細な説明を図面と併せて検討することから明白になるであろう。

【図面の簡単な説明】

【０００７】

【図１】図１は、サービス・アカウントのための認証トークン管理システムの例を示す。

【図２】図２は、サービス・アカウントの認証トークンを管理するための認証トークン管理システムのユーザー・インターフェース・ビューの例を示す。

【図３Ａ】図３Ａは、認証トークン管理アプリケーションが、クライアントに関連付けられたサービス・アカウントを求める要求を受けたときの論理フローの例を示す。

【図３Ｂ】図３Ｂは、認証トークン管理アプリケーションが、サービス・アカウントのために認証トークンを生成する要求を受けたときの論理フローの例を示す。

【図３Ｃ】図３Ｃは、トークン管理プロキシー・アプリケーションの論理フローの例を示す。

【図３Ｄ】図３Ｄは、クライアント・デバイスが、関連するサービス・アカウントを要求し、更に関連するサービス・アカウントのための認証トークンの生成を要求するときの論理フローの例を示す。

【図４】図４は、計算アーキテクチャの例を示す。

【発明を実施するための形態】

【０００８】

[0013] 種々の実施形態は、一般的には、１つ以上のアカウントのための認証トークンの管理を行うための認証トークン管理システムを対象とする。この認証トークン管理システムを利用して認証トークン（例えば、パスワード、パスコード、パスフレーズ、個人識別番号（ＰＩＮ）、暗号トークン等）を生成し、電子システムの一部または全部のアカウントのために人が作成した全ての認証トークンと置き換えることによって、電子システムのセキュリティおよびプライバシーを大幅に改善することができる。これらおよびその他の改善を達成するために、認証トークン管理システムは、大まかには、例えば、フェデレーテッド・アイデンティティ・アプリケーション(federated identity application)（例えば、ＭＩＣＲＯＳＯＦＴ（登録商標）Ａｃｔｉｖｅ Ｄｉｒｅｃｔｏｒｙ Ｆｅｄｅｒａｔｉｏｎ Ｓｅｒｖｉｃｅｓ（ＡＤ ＦＳ））、または任意の他のインターネット情報サービス（ＩＩＳ）認証プロバイダーを使用して、多要素認証プロトコル（例えば、スマート・カードおよび関連するＰＩＮを使用する二要素認証）に基づいて、クライアント（例えば、ユーザー、技術者、請負人、顧客、および／またはソフトウェア／ハードウェア・コンポーネント）を認証し、多要素認証プロトコルに基づいてクライアントの認証の有効性を判断するように構成することができる。

【０００９】

[0014] 今日、サービスとしてのソフトウェア（ＳａａＳ）システムを設計するために利用可能な種々の方法が速いペースで開発されるため、多数のユーザー（例えば、検査技師、設計者、請負人、内部顧客、および／または外部顧客）が、これらのサービスを日毎に検査、アップグレード、デバッグ、開発、展開、および／または維持するために、ＳａａＳシステムの１つ以上のサービスをホストするサーバーにアクセスしなければならないと考えられる。サーバーへのアクセスを要求するユーザーが多数いるので、各ユーザーにはこれらのサーバーにアクセスするために１つ以上のユーザー・アカウントが付与される場合がある。しかしながら、ＳａａＳシステムが増えるに連れて、ユーザー・アカウントの数およびそれに伴うセキュリティ・リスクも増大する。これは、追加のユーザー・アカウント毎に、潜在的なエントリー・ポイントを攻撃者に露出するおそれがあり、その結果攻撃者が不正アクセスを取得するための攻撃表面またはベクトルが増大するからである。これら潜在的なエントリー・ポイントは、あるユーザー・アカウントが、彼らの日々のタスクを実行するために、高い特権（例えば、管理者特権）を有することができるときに、

特に問題となる。これらのアカウントが攻撃者によって容易に漏洩されないことを保証するために今日では種々の認証方法が利用可能であるが、人が作成したパスワードの使用は、特に、人が作成したパスワードが短く、単純で、多数のアカウントにわたって再利用されることが多い時には、一貫して弱点であった。これらの素因がＳａａＳシステムにおいて入手可能な多数のアカウントと組み合わせられると、攻撃者が、例えば、ＳａａＳシステムの１つ以上のアカウントに関連付けられた人のパスワードを漏洩することによって、不正アクセスを取得できるという多大なリスクおよび蓋然性(probability)が生ずる。このような攻撃者による不正アクセスは、業務に著しい危害を生ずる原因となり、顧客にとって深刻なセキュリティおよびプライバシーの問題が発生するおそれがある。

【００１０】

[0015] 種々の実施形態では、クライアント（例えば、ユーザー、技術者、請負人、顧客、および／またはソフトウェア／ハードウェア・コンポーネント）が彼らのクライアント・アカウントに関連付けられた１つ以上のサービス・アカウントを引き出すことを可能にするために、認証トークン管理システムは、大まかには、サービス・アカウントの集合体を求める１つ以上のクライアント要求を受け、１つ以上のクライアント要求に応答して、このサービス・アカウントの集合体、およびサービス・アカウントに関連付けられたサービス・アカウント情報（例えば、サービス・アカウント識別子、サービス・アカウント役割（１つまたは複数）、サービス・アカウント範囲、サービス・アカウント存続期間、サービス・アカウント・ステータス等）を供給するように構成することができる。一旦サービス・アカウントの集合体を求める要求を受けたなら、認証トークン管理システムは、更に、１つ以上の受けた要求を認証するように構成することができる。要求の有効性が認められた後、認証トークン管理システムは、データーセンターにおいて公開エンドポイントを露出することができるプロキシー・アプリケーションを介して、少なくとも部分的にプロキシー認証情報（例えば、共有シークレット・ディジタル証明書のディジタル指紋または親指の指紋(thumbprint)）に基づいて１つ以上のサービス・アカウントを引き出しまたは読み出し(fetch)、クライアント・デバイスに、引き出した１つ以上のサービス・アカウントを供給するように構成することができる。

【００１１】

[0016] クライアントが１つ以上のサービス・アカウントのために認証トークンを安全に生成することを可能にするために、認証トークン管理システムは、大まかには、種々のネットワーク相互接続を介して安全な接続（例えば、ハイパーテキスト・トランスファー・プロトコル・セキュア（ＨＴＴＰＳ）を利用した信頼および暗号化接続）を介して１つ以上の要求を受けて、サービス・アカウントのために認証トークンを生成するように構成することができる。一旦１つ以上の認証トークンを生成する要求を受けたなら、認証トークン管理システムは、更に、受けた１つ以上の要求の有効性を判断するように構成することができる。要求の有効性を判断した後、認証トークン管理システムは、少なくとも部分的にクライアント認証情報に基づいて、１つ以上のサービス・アカウントのために認証トークンを生成するように構成することができる。

【００１２】

[0017] 認証トークンを安全に生成するために、認証トークン管理システムは、概略的に、１つ以上の安全なハードウェアおよび／またはソフトウェア・コンポーネント（例えば、信頼プラットフォーム・モジュール（ＴＰＭ）、ＭＩＣＲＯＳＯＦＴ．ＮＥＴ Ｆｒａｍｅｗｏｒｋ ＬｉｂｒａｒｙのＳｙｓｔｅｍ.Ｗｅｂ.Ｓｅｃｕｒｉｔｙ.Ｍｅｍｂｅｒｓｈｉｐ等）を利用して、認証トークン管理システムのサーバー・デバイスによって、認証トークンを生成するように構成することができる。一旦認証トークンがサーバー・デバイスによって生成されると、認証トークン管理システムのサーバー・デバイスは、更に、サービス・アカウントのための認証トークンを更新または設定するように、プロキシー・アプリケーションを介して、少なくとも部分的にプロキシー認証情報（例えば、認証トークン管理アプリケーションとトークン管理プロキシー・アプリケーションとの間における共有シークレット・ディジタル証明書、および共有シークレット・ディジタル証明書のデ

ィジタル指紋または親指の指紋）に基づいて要求するように構成することができる。プロキシー・アプリケーションは、生成された認証トークンによって既存の認証トークンを更新または設定するように、サービス・アカウントを管理するディレクトリー・サービス・サーバー・デバイスに要求する、および／またはディレクトリー・サービス・サーバー・デバイスと通信するように構成することができる。

【００１３】

[0018] １つ以上のサービス・アカウントの安全を更に確保するために、認証トークン管理システムは、大まかには、一旦認証トークンがサービス・アカウントのために生成されたなら、クライアントが認証トークンを変更も更新もできないように（例えば、認証トークンをそれよりも弱い認証トークンに変更または更新する）、生成した認証トークンを不変となるように設定する(configure)ように構成する(arrange)ことができる。その上、認証トークン管理システムは、更に、ＳａａＳシステムにおける２つのサービス・アカウントが同じ認証トークンを有することができないように、一意である認証トークンを生成するように構成することができる。認証トークンがパスワード、パスフレーズ、パスコード、ＰＩＮ等を含む実施形態では、認証トークン管理システムは、英数字キャラクターおよび／または記号のランダムに生成されたシーケンスを含む認証トークンを生成するように構成することができる。生成される英数字キャラクターおよび／または記号のシーケンスは、少なくとも部分的に、長さパラメーター（例えば、２５～３０個の文字(character)および／または記号）および／またはキャラクター・クラス／シンボル・パラメーター（例えば、少なくとも２０個の英数字キャラクターおよび少なくとも５個の記号）に基づいて、複雑さを変化させることができる。

【００１４】

[0019] 一旦認証トークンを生成したなら、認証トークン管理システムは、大まかには、プロキシー・アプリケーションを介して、少なくとも部分的にプロキシー認証情報に基づいて、サービス・アカウントのために生成された認証トークンを設定または更新するように構成することができる。ある実施形態では、更に、クライアントが限定された１組のアクション（例えば、プロキシー認証情報に関連付けられたサービス・アカウントを引き出し、サービス・アカウントのパスワードを更新または設定する）のみを実行し、これら自体のサービス・アカウントに関してこれらの限定された１組のアクションのみを実行することに制限できるように、認証トークン管理システムを制限することができる。加えて、認証トークン管理システムは、更に、プログラム的アクセス（例えば、コピー）、安全な格納、および／または表示のために、種々のネットワーク相互接続および安全な接続を介して、生成した認証トークンをクライアント・デバイスに供給するように構成することができる。

【００１５】

[0020] サービス・アカウントに随意に限定存続期間、限定役割、および／または限定範囲（例えば、ジャスト・イン・タイムでプロビジョニングされるアカウント、即ちＪＩＴアカウント）を関連付けることができる実施形態では、認証トークンはサービス・アカウントの存続期間の間だけ生きる即ち存続することができる（例えば、最大値の９６時間に対して４時間）。更に、サービス・アカウントに対する存続期間の終了時に、認証トークン管理システムは、サービス・アカウントに関連付けられたアクティブなトークン（例えば、アクセス・トークン）はいずれも失効できるように、このサービス・アカウントに関連付けられた認証トークンをリセットするように構成することができる。

【００１６】

[0021] その結果、攻撃者が認証トークンに基づく攻撃を使用して１つ以上のサービス・アカウントを漏洩させる能力は、クライアントが１つ以上のサービス・アカウントに関連付けられた新たな認証トークンを安全に要求し生成することを可能にすることによって、大幅に低減することができる。加えて、生成された認証トークンは、人が作成するパスワードと比較すると、遙かに複雑にすることができるので、従前からの暴力および何らかのソーシャル・エンジニアリングに基づく攻撃であっても、複雑な認証トークンの使用に

よって弱化させることができる。何故なら、これらのトークンは本来の手段および／または媒体（例えば、口頭伝達）によって正確に伝えることが難しいまたは不可能になることもあるからである。更に、人が作成した全てのパスワードを、サービス・アカウント毎にランダムでおよび／または一意である機械生成認証トークンと置き換えることによって、攻撃者が、例えば、共有認証トークンを使用することによって１つ以上のサービス・アカウントを漏洩させる能力は、更に弱化させることができる。１つ以上のサービス・アカウントを更に限定存続期間と関連付けることができる実施形態では、漏洩したサービス・アカウントを使用した攻撃者のアクセスは、更に限定される。何故なら、これらのサービス・アカウントは、これらがディスエーブルされる前には、限定された存続期間しか有することができないからである。このように、ＳａａＳシステムのセキュリティおよびプライバシーを更に改善することができる。

【００１７】

[0022] 本明細書において使用される観念および用語について概略的に参照して、以下に続く詳細の説明では、コンピューターまたはコンピューターのネットワークにおいて実行されるプログラム手順について提示することができよう。これらの手順についての説明および表現は、当業者が彼らの作業の実体(substance)を最も効果的に他の当業者に伝えるために使用される。

【００１８】

[0023] 手順とは、本明細書では、そして一般に、所望の結果に至る動作の自己無撞着な(self-consistent)シーケンスであると考えられる。これらの動作は、物理量の物理的操作を必要とするものである。必ずという訳ではないが、大抵の場合、これらの量は、格納、転送、組み合わせ、比較、およびそれ以外の操作をすることができる電気、磁気、または光信号の形態をなす。これらの信号をビット、値、エレメント、シンボル、キャラクター、用語(terms)、数値等と呼ぶことが、主に共通使用の理由のために、ときには便利であることが分かる。しかしながら、注記すべきは、これらおよび同様の用語は全てしかるべき物理量と関連付けられるはずであり、これらの量に適用される便利な呼称に過ぎないということである。

【００１９】

[0024] 更に、実行される操作は、多くの場合、加算または比較というような用語で引用されるが、一般に、人の操作者によって実行される精神的動作に関連付けられる。１つ以上の実施形態の一部をなす、本明細書において説明される動作においてはいずれも、殆どの場合、このような人の操作者の能力は必要ではなく、望ましくもない。むしろ、これらの動作は機械動作である。種々の実施形態の動作を実行する有用な機械には、汎用ディジタル・コンピューターまたは同様のデバイスが含まれる。

【００２０】

[0025] また、種々の実施形態は、これらの動作を実行する装置またはシステムにも関する。この装置は、必要とされる目的に合わせて特別に組み立てることができ、または汎用コンピューターを含み、このコンピューターに格納されたコンピューター・プログラムによって選択的に作動(activate)または再構成されるのでもよい。本明細書において紹介する手順は、本質的に、特定のコンピューターや他の装置に関係がない。種々の汎用機械を、本明細書における教示にしたがって書かれたプログラムと共に使用することもでき、また、必要とされる方法ステップを実行するように、更に特殊化された装置を組み立てることも便利な場合もある。種々のこれらの機械に必要とされる構造は、以下に示す説明において現れるであろう。

【００２１】

[0026] これより図面を参照するが、図面における同様の参照番号が全体を通じて同様のエレメントを指すために使用される。以下の説明では、説明の目的のために、完全な理解を得るために多数の具体的な詳細について明記する。しかしながら、新規な実施形態はこれらの具体的な詳細がなくても実施可能であることは明白であろう。他方で、周知の構造およびデバイスは、その説明を容易にするために、ブロック図形状で示される。その意

図は、特許請求する主題と一致する全ての変更、均等、および代替を範囲に含めることである。

【００２２】

[0027] 図１は、認証トークン管理システム１００の実施形態を示す。種々の実施形態において、認証トークン管理システム１００は、企業用計算環境１５０（例えば、クラウド・ストレージ・システム、データーセンター等）において、または企業用計算環境１５０と共に実現することもできる。企業用計算環境１５０は、１つ以上のクライアント１０２－ａ（例えば、ユーザー、技術者、請負人、顧客、および／またはソフトウェア／ハードウェア・コンポーネント）を含み、各クライアント（例えば、クライアント１０２－１または１０２－２）は１つ以上のクライアント・アカウントと関連付けることができ、１つ以上のクライアント・アカウントの内各クライアント・アカウントはクライアント・アカウント情報と更に関連付けることができる。クライアント・アカウント情報は、クライアント・アカウント認証情報（例えば、ユーザー主要名称（ＵＰＮ）、アカウント識別子、アカウント・パスワード、あるいはハッシュおよび／またはソルトされたその派生物、アカウント・ドメイン、スマート・カード証明書および関連するＰＩＮ、生物計量等）、クライアント・アカウント許可情報（例えば、クライアント・アカウント役割および範囲情報、アクセス許可、関連グループ等）、および／または１つ以上のクライアント１０２－ａの認証および許可に関連する任意の他の情報を含むことができるが、これらに限定されるのではない。

【００２３】

[0028] １つ以上のクライアント１０２－ａは、例えば、１つ以上の電子システムの１つ以上のサービスを提供するように構成された１つ以上のサーバー・デバイス１４０－ｉ－ｊを含むデーターセンター１４２においてというように、１つ以上のクライアント・アカウントを利用してそれらの関連するサービス・アカウントを要求し、更に１つ以上のリソースおよび／またはアセットを利用することができる。一実施形態では、電子システムはＳａａＳシステムを含むことができ、ＳａａＳシステムは、限定ではなく、ＭＩＣＲＯＳＯＦＴ Ｏｆｆｉｃｅ ３６５、ＭＩＣＲＯＳＯＦＴ Ｅｘｃｈａｎｇｅ Ｏｎｌｉｎｅ，ＭＩＣＲＯＳＯＦＴ ＳｈａｒｅＰｏｉｎｔ Ｏｎｌｉｎｅ、ＭＩＣＲＯＳＯＦＴ Ｄｙｎａｍｉｃｓ ＣＲＭ、およびその他のＳａａＳシステムを含むことができる。実施形態は、必ずしも電子システムの形式には限定されない。

【００２４】

[0029] データーセンター１４２におけるサーバー・デバイス１４０－ｉ－ｊは、更に、互いの間で、ネットワーク相互接続１１２を介して、ＳａａＳシステムによってホストされた種々のサービスを提供するために、相互接続されることも可能である。尚、サーバー・デバイス１４０－ｉ－ｊは、種々の実施形態では、限定ではなく単なる例示のために引用されるに過ぎないことは認めることができよう。したがって、種々の実施形態におけるサーバー・デバイス１４０－ｉ－ｊの内の任意のものまたは全てを、例えば、仮想デバイス、ワークステーション、計算デバイス、移動体デバイス、アプリケーション、サービス、および／または他のソフトウェア／ハードウェア・コンポーネントのような任意の他のリソースおよび／またはアセットと交換してもよい。

【００２５】

[0030] また、「ａ」および「ｂ」および「ｃ」ならびに同様の符号(designator)は、本明細書において使用される場合、任意の正の整数を表す変数であることを意図することも注記するに値する。つまり、例えば、ある実施態様がａ＝２と値を設定した場合、完全な１組のクライアント１０２－ａは、クライアント１０２－１および１０２－２を含むことができる。他の例では、ある実施態様がｉ＝１およびｊ＝６と値を設定した場合、完全な１組のサーバー・デバイス１４０－ｉ－ｊは、サーバー・デバイス１４０－１－１、１４０－１－２、１４０－１－３、１４０－１－４、１４０－１－５、および１４０－１－６を含むことができる。実施形態はこの文脈において限定されることはない。

【００２６】

[0031] 種々の実施形態において、認証トークン管理システム１００は、ネットワーク相互接続１１２を介して１つ以上のＳａａＳシステムのサーバー・デバイス１４０－ｉ－ｊにアクセスまたはサービスするために（例えば、ＳａａＳシステムの１つ以上のリソースおよび／またはアセットを検査、アップグレード、デバッグ、開発、展開、使用および／または維持する）クライアント１０２－ａによって使用される１つ以上のクライアント・デバイス１０４－ｂ（例えば、ラップトップ、コンピューター、電話機、ワークステーション、または任意の他の計算デバイス）を含むことができる。ネットワーク相互接続１１２は、概略的に、企業用計算環境１５０における種々のデバイス、コンポーネント、アプリケーション、サーバー、リソース、および／またはアセット間において、１つ以上のネットワーク（例えば、イントラネットおよび／またはインターネット）を通じて、１つ以上のネットワーク・デバイス（例えば、リピータ、ブリッジ、ハブ、スイッチ、ルーター、ゲートウェイ、ロード・バランサ等）を利用して、ネットワーク接続を設けるように構成することができる。

【００２７】

[0032] 種々の実施形態において、例えば、クライアント・デバイス１０４－２のような、クライアント・デバイス１０４－ｂの少なくとも一部は、クライアントに関連付けられた物理アイデンティティ・トークンに収容されたクライアント認証情報（例えば、ディジタル・スマート・カード証明書）を読み取るため、そして認証するまたは認証において補助するために、物理アイデンティティ・トークン（例えば、スマート・カード）と通信するためにアイデンティティ入力および／または出力（Ｉ／Ｏ）デバイス１６４（例えば、スマート・カード・リーダ）に通信可能に結合することができる。加えてまたは代わりに、例えば、クライアント・デバイス１０４－１のような他のクライアント・デバイス１０４－ｂも、クライアントに関連付けられた仮想アイデンティティ・トークンを読み取り、そして認証するまたは認証において補助するように構成するために、暗号モジュール（例えば、ＴＰＭ（図示せず））に通信可能に結合することができる。

【００２８】

[0033] 加えてまたは代わりに、例えば、クライアント・デバイス１０４－２のような、クライアント・デバイス１０４－ｂの少なくとも一部も、１つ以上の暗号化アルゴリズム（例えば、Ｔｗｏｆｉｓｈ対称鍵ブロック暗号）を利用して、少なくともサービス・アカウント識別子およびそれらの関連認証トークンを暗号化フォーマットで安全に格納するために、認証トークン・データーストア１６６（例えば、パスワード・セーフ）に通信可能に結合することもできる。このように、種々の実施形態において、クライアント・デバイス１０４－２は、クライアント１０２－２に供給された任意の認証トークンを自動的に暗号化して認証トークン・データーストア１６６に格納するように構成することができ、クライアント１０２－２が後にクライアント・デバイス１０４－２を介して、データーセンター１４２における１つ以上のリソースおよび／またはアセットにアクセスするために、以前に格納したサービス・アカウント識別子およびそれらの関連認証トークンを引き出すことを可能にする。

【００２９】

[0034] 種々の実施形態において、認証トークン管理システム１００、具体的には、データーセンター１４２は、１つ以上のディレクトリー・サービス・サーバー・デバイス１３０－ｌを含むまたはこれと統合されてもよい。ディレクトリー・サービス・サーバー・デバイス１３０－ｌは、一般に、１つ以上のサーバー・デバイス１４０－ｉ－ｊを含むデーターセンター１４２を１つ以上の論理グループ、論理サブグループ、および／または論理サブ・サブグループ（例えば、フォーレスト１３２－ｋ、ドメイン１３６－ｄ、および／または組織的ユニット１３４－ｅ－ｆ）の階層に編成するために、アプリケーションの中でもとりわけ、ディレクトリー・サービス・アプリケーション（図示せず）を実行するように構成することができる。 また、ディレクトリー・サービス・サーバー・デバイス１３０－ｌは、ディレクトリー・サービス情報を含む１つ以上のディレクトリー・サービス・データーストア（図示せず）において階層を格納するように構成することもできる。

【００３０】
[0035] １つ以上のディレクトリー・サービス・サーバー・デバイス１３０－ｌが、１つ以上のリソースおよび／またはアセットにアクセスするためのサービス・アカウントを使用して、１つ以上のクライアント１０２－ａからのアクセス要求を認証することができるように、１つ以上のディレクトリー・サービス・サーバー・デバイス１３０－ｌは、１つ以上のサービス・アカウントに関連付けられたサービス・アカウント情報を含むことができる。サービス・アカウント情報は、限定ではなく、サービス・アカウント認証情報（例えば、ユーザー・プリンシパル名（ＵＰＮ）、アカウント識別子、認証トークン、アカウント・ドメイン、スマート・カード証明書、生物計量等）、サービス・アカウント許可情報（例えば、サービス・アカウント役割および範囲情報、サービス・アカウント・アクセス許可、サービス・アカウント関連グループ等）、サービス・アカウント存続期間情報（例えば、サービス・アカウントの存続期間）、ディレクトリー・サービス情報（例えば、サービス・アカウントに関連付けられたディレクトリー・サービス・サーバー・デバイス）、および／または１つ以上のサービス・アカウントの認証、許可、および存続期間に関連する任意の他の情報を含むことができる。
【００３１】
[0036] 種々の実施形態では、各ディレクトリー・サービス・サーバー・デバイス（例えば、ディレクトリー・サービス・サーバー・デバイス１３０－１）は、ディレクトリー・サービス・アプリケーション（図示せず）を含むまたは実装することができる。典型的なディレクトリー・サービス・アプリケーションには、ＭＩＣＲＯＳＯＦＴ Ａｃｔｉｖｅ Ｄｉｒｅｃｔｏｒｙ、ＮＯＶＥＬＬ（登録商標） ｅＤｉｒｅｃｔｏｒｙ、ＡＰＰＬＥ（登録商標） Ｏｐｅｎ Ｄｉｒｅｃｔｏｒｙ、ＯＲＡＣＬＥ（登録商標） Ｉｎｔｅｒｎｅｔ Ｄｉｒｅｃｔｏｒｙ（ＯＩＤ）、ＩＢＭ（登録商標） Ｔｉｖｏｌｉ Ｄｉｒｅｃｔｏｒｙ Ｓｅｒｖｅｒ、あるいはＤｉｒｅｃｔｏｒｙ Ａｃｃｅｓｓ Ｐｒｏｔｏｃｏｌ（ＤＡＰ）、軽量Ｄｉｒｅｃｔｏｒｙ Ａｃｃｅｓｓ Ｐｒｏｔｏｃｏｌ（ＬＤＡＰ）、および／または国際電気通信連合（ＩＴＵ）電気通信標準化セクター（ＩＴＵ－Ｔ）によって公表されたＸ.５００規格を実施する任意の他のアプリケーションを含むことができるが、これらに限定されるのではない。
【００３２】
[0037] 例示として、ディレクトリー・サービス・サーバー・デバイス１３０－１は、ＭＩＣＲＯＳＯＦＴ Ａｃｔｉｖｅ Ｄｉｒｅｃｔｏｒｙの少なくとも一部（例えば、Ａｃｔｉｖｅ Ｄｉｒｅｃｔｏｒｙ Ｄｏｍａｉｎ Ｓｅｒｖｉｃｅ、Ａｃｔｉｖｅ Ｄｉｒｅｃｔｏｒｙ Ｄｏｍａｉｎ Ｃｏｎｔｒｏｌｌｅｒ、Ａｃｔｉｖｅ Ｄｉｒｅｃｔｏｒｙ Ｄａｔａｓｔｏｒｅ等）を含むまたは実装することができる。１つ以上のディレクトリー・サービス・サーバー・デバイス１３０－ｌの各ディレクトリー・サービス・サーバー・デバイス（例えば、ディレクトリー・サービス・サーバー・デバイス１３０－１）は、例えば、フォーレスト１３２－１のような最上位の論理グループを管理するように構成することができる。１つ以上のフォーレスト１３２－ｋは、１つ以上のそれよりも低い論理グループ、例えば、ドメイン１３６－ｄのような、例えば、論理サブグループを含むことができる。１つ以上のドメイン１３６－ｄの各ドメイン（例えば、ドメイン１３６－１）は、それよりも低いレベルの論理グループ、例えば、編成ユニット１３４－ｅ－ｆのような、例えば、論理サブ・サブグループを管理するように構成することができる。随意に、ドメイン１３０－ｄは、更に、例えば、ツリー（図示せず）のような、フォーレスト１３２－ｋとドメイン１３６－ｄとの間において１つ以上の中間論理グループに論理的にグループ化されてもよい。１つ以上の編成ユニット１３４－ｅ－ｆの各編成ユニット（例えば、編成ユニット１３４－１－１）は、例えば、サーバー・デバイス１４０－ｇ－ｈのような、１つ以上のリソースおよび／またはアセットを含むことができる。
【００３３】
[0038] 種々の実施形態において、フォーレスト１３２－ｋ、ドメイン１３６－ｄ、および／または編成ユニット１３４－ｅ－ｆは、限定ではなく例示の目的で引用されるに過

ぎないことは認めることができよう。したがって、種々の実施形態において、フォーレスト１３２－ｋ、ドメイン１３６－ｄ、および／または編成ユニット１３４－ｅ－ｆの内任意のものまたは全てが、所与の実施態様に合わせたそれらの実質的な均等物と置き換えられてもよい。例えば、ディレクトリー・サービス・サーバー・デバイス１３０－ｌがＮＯＶＥＬＬ　ｅＤｉｒｅｃｔｏｒｙの少なくとも一部を含むまたは実装する一実施態様では、フォーレスト１３２－ｋ、ドメイン１３６－ｄ、および編成ユニット１３４－ｅ－ｆは、それぞれ、ＮＯＶＥＬＬ　ｅＤｉｒｅｃｔｏｒｙにおいて実施されるように、ツリー、パーティション、および編成ユニットと置き換えることができる。実施形態はこの文脈において限定されることはない。

【００３４】

[0039] ある実施形態では、データーセンター１４２における各ドメイン（例えば、ドメイン１３６－１）は、１つ以上のサービス・アカウントを漏洩させた可能性がある１人以上の攻撃者の横方向移動を抑える(contain)ために、随意に、１つ以上の違反境界１３８－ｇ－ｈを含むこともできる。例えば、ドメイン１３６－１は、違反境界１３８－１－１および１３８－１－２を含むことができる。加えて、これらの実施形態の内ある実施態様では、違反境界１３８－ｇ－ｈは、１つ以上の編成ユニット１３４－ｅ－ｆとは独立であることもできる。例えば、ドメイン１３６－１において、編成ユニット１３４－１－１、１３４－１－２、１３４－１－３が、違反境界１３８－１－１および１３８－１－２の間に広がることができ、違反境界１３８－１－１のような１つの違反境界が、３つの全ての編成ユニット１３４－１－１、１３４－１－２、１３４－１－３からの、例えば、サーバー・デバイス１４０－１－１、１４０－１－２、１４０－２－３のようなリソースおよび／またはアセットを含むようにすることができる。他のドメインでは、１つの違反境界が１つの編成ユニット１３４－ｅ－ｆからのリソースおよび／またはアセットを含むことができるように、違反境界１３８－ｇ－ｈが１つ以上の編成ユニット１３４－ｅ－ｆと共存することもできる。実施形態は、この文脈において限定されるのではない。

【００３５】

[0040] ある実施形態では、１つ以上の違反境界１３８－ｇ－ｈが、１つ以上のディレクトリー・サービス・サーバー・デバイス１３０－ｌによって管理され、セキュリティ境界（例えば、１つ以上の違反境界１３８－ｇ－ｈの内の１つの違反境界）に関連付けることができる１つ以上のサービス・アカウントに対する１組のアクセス許可を付与しまたは与えて、１つ以上のサービス・アカウントがこのセキュリティ境界内において１つ以上のリソースおよび／またはアセットにアクセスにできるように構成することができる。更に、サービス・アカウントにアクセスできる攻撃者が「パス・ザ・ハッシュ攻撃」（即ち、攻撃者の横方向移動）を利用して１つ以上の違反境界１３８－ｇ－ｈの間で移動できないことを確保するために、随意に、１つ以上の違反境界１３８－ｇ－ｈの各違反境界（例えば、違反境界１３８－１－１および１３８－１－２）は、更に、相互に排他的な、即ち、重複しない１組のリソースおよび／またはアセットを含み、いずれの違反境界１３８－ｇ－ｈの間にも重複がないように構成することができる。

【００３６】

[0041] １つ以上の違反境界１３８－ｇ－ｈの一実施態様例では、１つ以上のディレクトリー・サービス・サーバー・デバイス１３０－ｌのディレクトリー・サービス・アプリケーション（図示せず）が、１つ以上の違反境界セキュリティ・グループ１６８－ｍ－ｎの各違反境界セキュリティ・グループを管理し、および／または１組のアクセス許可を１つ以上のリソースおよび／またはアセットに指定し(assign)、違反境界セキュリティ・グループに追加された任意のメンバー（例えば、１つ以上のサービス・アカウント）が、１組のアクセス許可にしたがってそのセキュリティ・グループによって管理される１つ以上のリソースおよび／またはアセットにアクセスできるように構成することができる。漏洩したサービス・アカウントへのアクセスを取得した攻撃者の横方向移動を抑えるために、１つ以上のディレクトリー・サービス・サーバー・デバイス１３０－ｌは、更に、１つ以上の互いに排他的な、即ち、重複しない違反境界セキュリティ・グループ１６８－ｍ－ｎ

における１つ以上のリソースおよび／またはアセットを管理して、２つの異なる違反境界セキュリティ・グループのメンバーであるサービス・アカウントからは、１つのリソースおよび／またはアセットにはアクセスできない、またはサービスできないように構成することもできる。

【００３７】

[0042] 尚、種々の実施形態では、限定された数の違反境界セキュリティ・グループ（例えば、違反境界セキュリティ・グループ１６８－１－１、１６８－１－２、および１６８－ｍ－１）のみを例示したが、１つ以上のディレクトリー・サービス・サーバー・デバイス１３０－１は、サービス・アカウントに関連付けられた１つ以上の役割に対して複数のグループ（例えば、リモート・アクセス・グループ、デバッガー・グループ等）を管理するように構成することもでき、役割に基づくアクセス制御（ＲＢＡＣ）を達成するために、サービス・アカウントがネスト状で多数のグループのメンバーになることができるように、各グループには、役割に関連付けられた１組のアクセス許可（例えば、１つ以上のリソースおよび／またはアセットへのリモート・アクセス、１つ以上のリソースおよび／またはアセットのデバッグ等）を関連付けできることは認めることができよう。実施形態はこの文脈に限定されるのではない。

【００３８】

[0043] 種々の実施形態において、認証トークン管理システム１００は、更に、サーバー・デバイス１０８も含むことができる。サーバー・デバイス１０８は、大まかには、アプリケーションの中でもとりわけ、ディレクトリー・サービス・アプリケーション１１０を実行するように構成することができる。ディレクトリー・サービス・アプリケーション１１０は、大まかには、クライアント１０２－ａの１つ以上のクライアント・アカウントに関連付けられたクライアント・アカウント情報を格納し提供するように構成することができる。また、ディレクトリー・サービス・アプリケーション１１０は、１つ以上のクライアント１０２－ａがメンバーまたは会員（例えば、会社）となることができる組織の階層構造を含む組織的階層情報を格納するように構成することができる。更に、ディレクトリー・サービス・アプリケーション１１０は、認証トークン管理アプリケーション１７２を介して、１つ以上のサービス・アカウントのために認証トークンを要求する１つ以上のクライアント１０２－ａを認証する、またはその認証において補助するように構成することもできる。典型的なディレクトリー・サービス・アプリケーションまたは実施態様には、ディレクトリー・サービス・サーバー・デバイス１３０－１に関して先に論じたものを含むことができるが、それらに限定されるのではない。

【００３９】

[0044] １つ以上のサービス・アカウントのために認証トークンを要求する１つ以上のクライアント１０２－ａを認証するため、またはその認証を容易にするために、ディレクトリー・サービス・アプリケーション１１０は、１つ以上のアプリケーション・プログラム・インターフェース（ＡＰＩ）を露出するおよび／または実装することもできる。ａｄｍｉｎ管理アプリケーション１１４および／またはトークン管理アプリケーション１７２は、１つ以上のＡＰＩを利用して、サービス・アカウントおよび／またはサービス・アカウントのための認証トークンを要求する１つ以上のクライアント１０２－ａを、１つ以上のクライアント１０２－ａに関連付けられたクライアント・アカウント情報（例えば、クライアント・アカウント識別子またはクライアント・アカウントＵＰＮ、およびクライアント・アカウント・パスワード）に基づいて認証することができる。

【００４０】

[0045] 例示として、ａｄｍｉｎ管理アプリケーション１１４および／または認証トークン管理アプリケーション１７２は、受けたクライアント・アカウント識別子またはクライアント・アカウントＵＰＮと、クライアント・アカウント・パスワードとに基づいて、ネットワーク相互接続１１２を介して、１つ以上のＡＰＩ、および／または１つ以上のローカル手順コール（ＬＰＣ）、および／またはディレクトリー・サービス・アプリケーション１１０のリモート手順コール（ＲＰＣ）メカニズムを利用することによって、１つ以

上のクライアント１０２－ａを認証することができる。尚、典型的なＡＰＩには、ＤＡＰ ＡＰＩ、ＬＤＡＰ ＡＰＩ、ＭＩＣＲＯＳＯＦＴ Ａｃｔｉｖｅ Ｄｉｒｅｃｔｏｒｙ Ｓｅｒｖｉｃｅ Ｉｎｔｅｒｆａｃｅ（ＡＤＳＩ） ＡＰＩ、ＭＩＣＲＯＳＯＦＴ Ｍｅｓｓａｇｉｎｇ ＡＰＩ（ＭＡＰＩ）、ＭＩＣＲＯＳＯＦＴ Ｄｉｒｅｃｔｏｒｙ Ｓｙｓｔｅｍ Ａｇｅｎｔ（ＤＳＡ）ＡＰＩ、および／またはクライアント１０２－ａの認証を可能にする任意の他のＡＰＩを含んでもよいことは認めることができよう。

【００４１】

[0046] 加えてまたは代わりに、認証トークン管理システム１００は、サーバー・デバイス１６０も含むことができる。サーバー・デバイス１６０は、大まかには、アプリケーションの中でもとりわけ、フェデレーテット・アイデンティティ・アプリケーション(federated identity application)１６２を実行するように構成することができる。フェデレーテット・アイデンティティ・アプリケーション１６２は、大まかには、１つ以上の認証プロトコル（例えば、Ｋｅｒｂｅｒｏｓプロトコル）を利用して、多要素認証（例えば、スマート・カード、パスワード／ｐｉｎ、および／または手の指紋を利用する二要素認証）を行うように構成することができる。認証要素は、知識要素、即ち、クライアントが知っている何か（例えば、パスワード、パスコード、パスフレーズ、ＰＩＮ等）、所有要素、即ち、クライアントが有する何か（スマート・カード、仮想スマート・カード、セキュリティ・トークン等）、固有の特性要素、即ち、クライアントであることの何か（例えば、手の指紋、虹彩のパターン、網膜のパターン、生物計量等）、および／またはクライアントの識別および／または認証において補助するために利用することができる任意の他の要素含むことができるが、これらに限定されるのではない。したがって、ある実施形態では、フェデレーテット・アイデンティティ・アプリケーション１６２は、アイデンティティ入力および／または出力（Ｉ／Ｏ）デバイス１６４および／またはディレクトリー・サービス・アプリケーション１１０と合わせて、１つ以上のクライアント１０２－ａの認証を行うように構成することができる。

【００４２】

[0047] 種々の実施形態において、フェデレーテット・アイデンティティ・アプリケーション１６２は、更に、セキュリティ・トークン・サービス（ＳＴＳ）を提供し、１つ以上のセキュリティ・トークン（例えば、セキュリティ・アサーション・マークアップ言語（ＳＡＭＬ： Security Assertion Markup Language）トークン）を１つ以上のクライアント１０２－ａおよび／または要求可能化アプリケーション(claim enabled application)に発行して、１つ以上の要求可能化アプリケーションが、１つ以上のクライアント１０２－ａに関連付けられたクライアント・アカウント情報（例えば、ユーザーの主名称（ＵＰＮ）、アカウント識別子、アカウント・パスワードまたはそのハッシュ派生物、アカウント・ドメイン、スマート・カード証明書等）を直接受けることなく、および／または処理することなく、クライアントを識別できるように、および／またはクライアントとの信頼接続を確立できるように構成することができる。典型的なフェデレーテット・アイデンティティ・アプリケーションは、ＭＩＣＲＯＳＯＦＴ Ａｃｔｉｖｅ Ｄｉｒｅｃｔｏｒｙ Ｆｅｄｅｒａｔｉｏｎ Ｓｅｒｖｉｃｅ（ＡＤ ＦＳ）、ＭＩＣＲＯＳＯＦＴ Ｆｅｄｅｒａｔｉｏｎ Ｇａｔｅｗａｙ、または既に認証されているクライアントのアイデンティティをアサートすることの要求を含むセキュリティ・トークンを発行するように構成された任意の他の連合アイデンティティ・サービス・プロバイダーを含むことができるが、これらに限定されるのではない。

【００４３】

[0048] 種々の実施形態において、クライアント・アカウント識別子またはクライアント・アカウントＵＰＮとクライアント・アカウント・パスワードとに基づいて１つ以上のクライアント１０２－ａを直接認証する代わりに、ａｄｍｉｎ管理アプリケーション１１４および／またはトークン管理アプリケーション１７２は、要求可能化アプリケーションとして構成され(arrange)、したがって、１つ以上のクライアント１０２－ａを認証および／または許可するために、フェデレーテット・アイデンティティ・アプリケーション１

６２によって発行されたセキュリティ・トークンを１つ以上のクライアント・デバイス１０４－ｂから受けるように構成する(configure)ことができる。したがって、ａｄｍｉｎ管理アプリケーション１１４および／またはトークン管理アプリケーション１７２は、受けたセキュリティ・トークンに少なくとも部分的に基づいて、アプリケーションへのアクセスを要求するクライアント１０２－ａを認証および識別することができる。また、受けたセキュリティ・トークンは、１つ以上の要求(claim)も含むことができ、１つ以上の要求(claim)は、１つ以上のクライアント１０２－ａに関連付けられたクライアント・アカウント情報を含むことができる。随意に、受けたセキュリティ・トークンは、更に、１つ以上のクライアント１０２－ａを認証するために使用された認証要素、メカニズム、および／または方法（例えば、スマート・カードおよびＰＩＮ、アカウント識別子およびアカウント・パスワード、アカウント識別子および生物計量指紋等）を示す認証タイプ情報も含むことができる。

【００４４】

[0049] 例示として、クライアント１０２－２は、最初に、アイデンティティ・トークン（即ち、所有要素）を使用してアイデンティティＩ／Ｏデバイス１６４とインターフェースし、クライアント・デバイス１０４－２に通信可能に結合されている標準的な入力デバイス（例えば、キーボード）を介して関連するＰＩＮ（即ち、知識ファクター）を入力することによって、二要素認証を使用してクライアント・デバイス１０４－２を認証することを要求することができる。すると、ディレクトリー・サービス・アプリケーション１１０（例えば、ＭＩＣＲＯＳＯＦＴ Ａｃｔｉｖｅ Ｄｉｒｅｃｔｏｒｙ Ｄｉｒｅｃｔｏｒｙ Ｓｅｒｖｉｃｅｓ（ＡＤ ＤＳ））は、クライアント・デバイス１０４－２からの要求を受けて、少なくとも部分的に、クライアント・デバイス１０４－２によって認証されたおよび／または有効性が認められたアイデンティティ・トークン（例えば、クライアント１０２－２に関連付けられたスマート・カード）に基づいて、クライアント１０２－２のためにチケット付与チケット(Ticket Granting Ticket)（例えば、Ｋｅｒｂｅｒｏｓチケット）をネゴシエートすることができる。一旦クライアント１０２－２が認証されたら、ディレクトリー・サービス・アプリケーション１１０はＴＧＴをクライアント・デバイス１０４－２に供給することができる。随意に、ディレクトリー・サービス・アプリケーション１１０は、付加的に、従前からのクライアント・アカウント識別子またはクライアント・アカウントＵＰＮではなく、アイデンティティ・トークンおよび関連するＰＩＮを使用して、更に関連するクライアント・アカウント・パスワードを使用してクライアント１０２－２が認証されたことを示す、ＴＧＴにおける情報（例えば、スマート・カードおよび関連するＰＩＮによって認証された１つ以上のクライアント１０２－ａを含むセキュリティ・グループを識別するセキュリティ識別子（ＳＩＤ））を含むこともできる。

【００４５】

[0050] 以上の例示を続けると、要求可能化アプリケーション（例えば、ａｄｍｉｎ管理アプリケーション１１４および／またはトークン管理アプリケーション１７２）は、次いで、クライアント１０２－２からのアクセス要求をクライアント・デバイス１０４－２を通じて受けることができる。このアクセス要求に応答して、要求可能化アプリケーションは、クライアント・デバイス１０４－２を要求可能化アプリケーションの信頼ＳＴＳプロバイダー、即ち、フェデレーテット・アイデンティティ・アプリケーション１６２（例えば、ＭＩＣＲＳＯＦＴ ＡＤ ＦＳ）にリダイレクトすることができ、フェデレーテット・アイデンティティ・アプリケーション１６２はディレクトリー・サービス・アプリケーション１１０と通信し、クライアント・デバイス１０４－２とネゴシエートして、クライアント・デバイス１０４－２にセキュリティ・トークン（例えば、ＳＡＭＬトークン）を供給することができる。随意に、フェデレーテット・アイデンティティ・アプリケーション１６２は、付加的に、クライアント１０２－２がクライアントのアイデンティティ・トークンおよび関連するＰＩＮを使用して認証されたことを示すことができる認証タイプ情報を、セキュリティ・トークンにおいて含むこともできる。

【００４６】

[0051] 以上の例示を更に続けると、要求可能化アプリケーションは、次いで、クライアント・デバイス１０４－２からセキュリティ・トークン（例えば、ＳＡＭＬトークン）を受けることができる。これは、フェデレーテット・アイデンティティ・アプリケーション１６２によって供給されたものである。次いで、要求可能化アプリケーションは、このセキュリティ・トークンが、例えば、フェデレーテット・アイデンティティ・アプリケーション１６２のような信頼できるフェデレーテット・アイデンティティ・アプリケーションによって発行されたプロパティであったか否か判定することによって、セキュリティ・トークンを認証する、または有効性を判断することができる。要求可能化アプリケーションとのその後の通信の認証を容易にするために、要求可能化アプリケーションは、その後の通信のために、信頼セッション・クッキー（例えば、ＦｅｄＡｕｔｈクッキー）をクライアント・デバイス１０４－２に供給することもできる。随意に、クライアント１０２－２がアイデンティティ・トークンの使用に基づいて認証されたのか否か、例えば、セキュリティ・トークンが、クライアント１０２－２を含むセキュリティ・グループのＳＩＤを含み、クライアント１０２－２がアイデンティティ・トークンおよび関連するＰＩＮによって認証されたことを示すか否か判定することによって、要求可能化アプリケーションは判定することができる。クライアント１０２－２がクライアントのアイデンティティ・トークンに基づいて認証されたのではないとき、要求可能化アプリケーションはクライアント・デバイス１０４－２の要求可能化アプリケーションへのアクセスを拒否することができる。このように、クライアント・デバイス１０４－２と、少なくとも二要素認証、即ち、アイデンティティ・トークン（即ち、所有要素）および関連するＰＩＮ（即ち、知識要素）に基づいて認証されたクライアント１０２－ａの要求可能化アプリケーションとの間には、少なくとも信頼できる接続を確立することができる。

【００４７】

[0052] 種々の実施形態において、認証トークン管理システム１００は、更に、サービス・デバイス１０６を随意に含むことができる。サービス・デバイス１０６は、任意に、アプリケーションの中でもとりわけ、ａｄｍｉｎ管理アプリケーション１１４を実行するように構成することができる。ａｄｍｉｎ管理アプリケーション１１４は、大まかには、１つ以上のサービス・アカウントを要求する１つ以上のクライアント１０２－ａを認証し、１つ以上のクライアント１０２－ａからの、１つ以上のサーバー・デバイスにアクセスする要求、アクセス許可を昇格させる要求、およびクライアント１０２－ａから受けた１つ以上の要求を認証する要求を受けるように構成することができる。加えて、ａｄｍｉｎ管理アプリケーション１１４は、更に、１つ以上のサービス・アカウントを管理、許可、プロビジョニング、およびイネーブルするように構成することができる。更に、ａｄｍｉｎ管理アプリケーション１１４は、アクセス許可が昇格された、役割が限定された、範囲が限定された、そして存続期間が限定されたサービス・アカウント、言い換えると、ジャスト・イン・タイム（ＪＩＴ）にプロビジョニングされたアカウント（即ち、ＪＩＴアカウント）としても知られているサービス・アカウントを、クライアント１０２－ａによって要求された通りに、プロビジョニングし、更にクライアント１０２－ａに、プロビジョニングされたサービス・アカウント（例えば、プロビジョニングされたＪＩＴアカウント）に関連付けられたサービス・アカウント情報を通知するように構成することができる。

【００４８】

[0053] １つ以上のクライアント１０２－ａを認証可能にするために、ａｄｍｉｎ管理アプリケーション１１４は、クライアント・アカウント情報の少なくとも一部（例えば、アカウントＵＰＮ、アカウント識別子、および／またはアカウント・パスワード）を１つ以上のクライアント１０２－ａに、クライアント・デバイス１０４－ｂを通じて要求する、および／または１つ以上のクライアント１０２－ａから受けるように構成することができ、受けたクライアント・アカウント情報を、１つ以上のクライアント１０２－ａのクライアント・アカウントと関連付けることができる。一旦クライアント・アカウント情報を受けたなら、ａｄｍｉｎ管理アプリケーション１１４は、更に、ネットワーク相互接続１１２およびディレクトリー・サービス・アプリケーション１１０の１つ以上のＡＰＩを介

して通信し、１つ以上のクライアント１０２－ａに関連付けられた、受けたクライアント・アカウント情報（例えば、アカウントＵＰＮ、アカウント識別子、および／またはアカウント・パスワード）を認証するように構成することができる。

【００４９】

[0054] 加えておよび／または代わりに、ａｄｍｉｎ管理アプリケーション１１４は、要求可能化アプリケーション(claims enabled application)を含むことができる。要求可能化アプリケーションは、フェデレーテット・アイデンティティ・アプリケーション１６２によって発行されたセキュリティ・トークン（例えば、ＳＡＭＬトークン）を１つ以上のクライアント・デバイス１０４－ｂから受けるように構成される。更に、ａｄｍｉｎ管理アプリケーション１１４は、受けたセキュリティ・トークンに基づいて、サービス・アカウントを要求した１つ以上のクライアント１０２－ａを認証し識別するように構成することができる。受けたセキュリティ・トークンは、１つ以上のクライアント１０２－ａに関連付けられたクライアント・アカウント情報を含むことができる１つ以上の要求(claim)を含むことができる。クライアント・デバイス１０４－ｂから受けたセキュリティ・トークンを利用することによって、ａｄｍｉｎ管理アプリケーション１１４は１つ以上のクライアント・デバイス１０４－ｂとの信頼接続を少なくとも確立することができる。更に信頼接続が攻撃者によって危殆化されるまたは改竄されるのを防ぐために、ａｄｍｉｎ管理アプリケーション１１４は１つ以上の安全通信プロトコル（例えば、ハイパーテキスト・トランスファー・プロトコル・セキュア（ＨＴＴＰＳ））を利用して、暗号化接続を確立することもできる。このように、安全な接続（例えば、信頼および暗号化接続）をａｄｍｉｎ管理アプリケーション１１４と１つ以上のクライアント・デバイス１０４－ｂとの間に、１つ以上のサービス・アカウントの要求のために確立することができる。

【００５０】

[0055] ある実施形態では、一旦１つ以上のクライアント１０２－ａが認証されたなら、ａｄｍｉｎ管理アプリケーション１１４は、データーセンター１４２における１つ以上のリソースおよび／またはアセットにアクセスするための１つ以上のサービス・アカウントを要求するために、１つ以上の認証されたクライアント１０２－ａがサービス・アカウント要求情報を入力することを可能にするように構成することができる。サービス・アカウント要求情報は、実行される１つ以上のアクションまたはタスク、１つ以上のサーバー・デバイス１４０－ｉ－ｊ、および１つ以上のアクションまたはタスクに関連付けられた要求存続期間情報を含むことができるが、これに限定されるのではない。要求存続期間情報は、サービス・アカウントが失効してディスエーブルされるときの具体的な時刻または経過時間、および／またはサービス・アカウントが削除される具体的な時刻または経過時間を含むことができるが、これに限定されるのではない。任意に、ａｄｍｉｎ管理アプリケーション１１４は、サービス・アカウントに対する要求存続期間情報を、９６時間即ち４日の上限値に限定し、９６時間（例えば、４日）よりも存続期間が長いサービス・アカウントを求める要求をいずれも９６時間即ち４日に限定されるようにすることもできる。実施形態はこの文脈において限定されることはない。

【００５１】

[0056] ある実施形態では、ａｄｍｉｎ管理アプリケーション１１４は、少なくとも部分的に、受けたサービス・アカウント要求情報（例えば、実行される１つ以上のアクションまたはタスク、および１つ以上のサーバー・デバイス１４０－ｉ－ｊ）と、既存のサービス・アカウントについてのサービス・アカウント役割／範囲情報に基づいて決定された要求役割／範囲情報とに基づいて、クライアントに関連付けられた既存のサービス・アカウントを引き出すことによって、サービス・アカウントをプロビジョニングするように構成することができる。加えてまたは代わりに、ａｄｍｉｎ管理アプリケーション１１４は、少なくとも部分的に１つ以上のクライアント１０２－ａからクライアント・デバイス１０４－ｂを介して受けた要求役割／範囲情報と、既存のサービス・アカウントについてのサービス・アカウント役割／範囲情報とに基づいて、クライアントに関連付けられた既存のサービス・アカウントを引き出すことによって、サービス・アカウントをプロビジョニ

ングするように構成することもできる。

【００５２】

[0057] 典型的な(exemplary)要求役割および／またはサービス・アカウント役割には、アドミニストレーター、バックアップ・オペレーター、デバッガー、リモート・ユーザー、テスター等を含むことができるが、これらに限定されるのではない。尚、各役割には、更に、１つ以上のリソースおよび／またはアセット、および／または１つ以上のリソースおよび／またはアセットのコンポーネントに対するアクセスを付与および／または拒否することができる１組のアクセス許可を関連付けることもできることは認めることができよう。典型的な要求範囲および／またはサービス・アカウント範囲には、１つ以上のサーバー・デバイス１４０－１－１、１４０－１－２、１４０－１－３、あるいは他のリソースおよび／またはアセット、および／またはリソースおよび／またはアセットのコンポーネントを含む違反境界１３８－１－１を含むことができるが、これらに限定されるのではない。

【００５３】

[0058] ある実施形態では、ａｄｍｉｎ管理アプリケーション１１４は、同じまたは実質的に同様の要求役割／範囲を有するサービス・アカウントがクライアントのために既に存在するか否か判定するように構成することもできる。次いで、ａｄｍｉｎ管理アプリケーション１１４は、既にそのクライアントのために存在するサービス・アカウントに対するサービス・アカウント役割／範囲が、要求役割／範囲と同じまたは実質的に同様であるとき、サービス・アカウント・データーストア１２６から既存のサービス・アカウントを引き出すように構成することができる。

【００５４】

[0059] あるいは、ａｄｍｉｎ管理アプリケーション１１４が、要求役割／範囲を有するサービス・アカウントがそのクライアントのために存在しないと判定したとき、アカウント・プロビジョニング・コンポーネント１２０は、自動的にそのクライアントのために新たなサービス・アカウントを作成するように構成することができる。これは、言い換えると、サービス・アカウントのレイジー・プロビジョニング(lazy provisioning)としても知られており、ａｄｍｉｎ管理アプリケーション１１４は、役割および範囲が同等または実質的に同様である以前のサービス・アカウントが未だそのクライアントのために存在しないときにのみ、サービス・アカウントを作成するように構成することができる。

【００５５】

[0060] ある実施形態では、ａｄｍｉｎ管理アプリケーション１１４は、更に、少なくとも部分的に、サービス・アカウント要求情報（例えば、要求役割／範囲情報、要求存続期間情報等）とクライアント・アカウント情報とに基づいて、新たなサービス・アカウントおよびその関連するサービス・アカウント情報を作成することができる。例えば、クライアント１０２－２についてのクライアント・アカウント情報がＵＰＮ"EllenAdams@.contoso.com"を含むことができ、要求された役割がリモート・ユーザーおよびデバッガーを含み、要求された範囲が違反境界１３８－１－１を含むと仮定する。ａｄｍｉｎ管理アプリケーション１１４は、クライアント１０２－１が少なくとも部分的にＵＰＮに基づいてサービス・アカウントに対する１つ以上の役割を識別できるように、サービス・アカウントＵＰＮ "EllenAdams_RemoteDebugger_Boundary138-1-1@domain136-1.contoso.com"を含むサービス・アカウント情報によって新たなサービス・アカウントを作成することができる。加えて、ａｄｍｉｎ管理アプリケーション１１４は、更に、新たに作成したサービス・アカウントをサービス・アカウント・データーストア１２６に格納し、この新たに作成したサービス・アカウントをそのクライアントのクライアント・アカウントと関連付けることもできる。

【００５６】

[0061] １つ以上のディレクトリー・サービス・サーバー・デバイス１３０－１によって管理されるリソースおよび／またはアセットが、新たに作成されたサービス・アカウントを使用して１つ以上のクライアント１０２－ａによってアクセス可能および／またはサ

ービス可能であることを確保するために、ａｄｍｉｎ管理アプリケーション１１４は、更に、クライアントがアクセスおよび／またはサービスすることを要求した１つ以上のリソースおよび／またはアセットを含む１つ以上の違反境界１３８－ｇ－ｈを管理する、該当のディレクトリー・サービス・サーバー・デバイスを識別するように構成することができる。一旦該当するディレクトリー・サービス・サーバー・デバイスを識別したなら、ａｄｍｉｎ管理アプリケーション１１４は、更に、サービス・アカウントを作成するために、ネットワーク相互接続１１２および識別したディレクトリー・サービス・サーバー・デバイスの１つ以上のＡＰＩを介して、識別したディレクトリー・サービス・サーバー・デバイスと通信するように構成することができる。加えて、ａｄｍｉｎ管理アプリケーション１１４は、新たに作成したサービス・アカウントおよび関連するサービス・アカウント情報をサービス・アカウント・データーストア１２６に格納し、それを引き出して再利用できるように、この新たに作成したサービス・アカウントおよび関連するサービス・アカウント情報をクライアント・アカウントと関連付けるように構成することができる。

【００５７】

[0062] ある実施形態では、一旦サービス・アカウントが引き出されたならまたは作成されたなら、ａｄｍｉｎ管理アプリケーション１１４は、更に、引き出されたまたは作成されたサービス・アカウントが、クライアントによって要求されたのと同じ役割および範囲を有するように、少なくとも部分的に要求役割／範囲情報に基づいて、サービス・アカウントをイネーブルするように構成することができる。また、これは、作成されたまたは引き出された各サービス・アカウントが、クライアントに要求された通りにリソースおよび／またはアセットにおいてサービスにアクセスするまたはサービスを実行するために必要とされる、１組の最小限の範囲に設定されたアクセス許可を含むことも確保する。サービス・アカウントをイネーブルするために、ａｄｍｉｎ管理アプリケーション１１４は、更に、少なくとも部分的に要求役割／範囲情報に基づいて、１組のアクセス許可をサービス・アカウントに付与する、即ち、与えるように構成することができる。

【００５８】

[0063] 適正な１組のアクセス許可が、プロビジョニングされたサービス・アカウントに付与される即ち与えられることを確保するために、ａｄｍｉｎ管理アプリケーション１１４は、更に、ネットワーク相互接続１１２と１つ以上のディレクトリー・サービス・サーバー・デバイス１３０－１のディレクトリー・サービス・アプリケーション（図示せず）の１つ以上のＡＰＩとを利用することによって、該当する違反境界セキュリティ・グループ１６８－ｍ－ｎを管理するディレクトリー・サービス・サーバー・デバイスを識別し、更に、１つ以上のリソースおよび／またはアセットへのアクセスを付与するように構成された１つ以上の違反境界セキュリティ・グループ１６８－ｍ－ｎを識別するように構成することができる。一旦該当するディレクトリー・サービス・サーバー・デバイスおよび１つ以上の違反境界セキュリティ・グループ１６８－ｍ－ｎが識別されたなら、ａｄｍｉｎ管理アプリケーション１１４は、プロビジョニングしたサービス・アカウントを、識別した違反境界セキュリティ・グループと関連付けるために、識別したディレクトリー・サービス・サーバー・デバイスと通信するように構成することができる。

【００５９】

[0064] ある実施形態では、ａｄｍｉｎ管理アプリケーション１１４は、違反境界セキュリティ・グループに関連付けられた違反境界内の１つ以上のリソースおよび／またはアセットにアクセスするための１組のアクセス許可をサービス・アカウントに付与できるように、サービス・アカウントを１つ以上の違反境界セキュリティ・グループ１６８－ｍ－ｎにメンバーとして追加することによって、サービス・アカウントを違反境界セキュリティ・グループ１６８－ｍ－ｎと関連付けるように構成することができる。攻撃者が漏洩したサービス・アカウントを使用して起こすおそれがある影響の範囲を更に限定するために、ａｄｍｉｎ管理アプリケーション１１４は、更に、サービス・アカウントに関連付けることができる違反境界セキュリティ・グループ１６８－ｍ－ｎの数を限定するように構成することができる（例えば、各サービス・アカウントには１つの違反境界セキュリティ・

グループしか関連付けることができない）。

【００６０】

[0065] ある実施形態では、ａｄｍｉｎ管理アプリケーション１１４は、更に、存続期間が限定された１つ以上のサービス・アカウントをイネーブルするように構成することができる。１つ以上のサービス・アカウントが限定存続期間だけイネーブルされることを確保するために、ａｄｍｉｎ管理アプリケーション１１４は、更に、サービス・アカウント存続期間情報または既定のサービス・アカウント存続期間情報に基づいて、各サービス・アカウントに関連付けられた存続期間を管理するように構成することができる。更に、ａｄｍｉｎ管理アプリケーション１１４は、サービス・アカウント存続期間情報または既定のサービス・アカウント存続期間情報によって指示される通りに、ある時間期間が経過した後、１つ以上のサービス・アカウントをディスエーブルするおよび／または削除するように構成することができる。サービス・アカウント存続期間情報は、サービス・アカウントが失効しディスエーブルされるときの具体的な時刻または経過時間、およびサービス・アカウントが削除されるときの具体的な時刻または経過時間を含むことができるが、これらに限定されるのではないことは認めることができよう。

【００６１】

[0066] ある実施形態では、サービス・アカウント存続期間情報は、所与の実施態様に合わせて、クライアント・デバイス１０４－ｂを介して１つ以上のクライアント１０２－ａから受けたサービス・アカウント要求情報に基づいて判定されるおよび／または導き出されるのでもよい。他の実施形態では、サービス・アカウント存続期間情報は、サービス・アカウント役割／範囲情報によって示される１つ以上の役割に基づいて判定されるおよび／または導き出されてよく、ある役割（例えば、リモート・ユーザーおよびデバッガー）が２時間という関連サービス・アカウント存続期間を有するが、他の役割（例えば、バックアップ・オペレーター）が４時間という存続期間を有する場合もある。実施形態はこの文脈において限定されるのではない。

【００６２】

[0067] 一実施形態例では、サービス・アカウントの存続期間は、サービス・アカウントがプロビジョニングされた時点（例えば、ａｄｍｉｎ管理アプリケーション１１４によってプロビジョニングされた）から開始するのでもよく、サービス・アカウント存続期間情報に基づいて指定された時刻または経過時間において終了する。あるいは、サービス・アカウントの存続期間は、サービス・アカウントが最初に利用された（例えば、サービス・アカウントを使用してクライアントがリソースおよび／またはアセットにアクセスしようとした）時点から開始するのでもよく、サービス・アカウント存続期間情報に基づいて指定された時刻または経過時間において終了する。実施形態例は、この文脈において限定されるのではない。

【００６３】

[0068] 他の実施形態例では、ａｄｍｉｎ管理アプリケーション１１４は、更に、１つ以上のクライアント１０２－ａが、１つ以上のディレクトリー・サービス・サーバー・デバイス１３０－ｌによって管理される１つ以上のリソースおよび／またはアセットにアクセスするとき、ネットワーク相互接続１１２を介して１つ以上のディレクトリー・サービス・サーバー・デバイス１３０－ｌから１つ以上のアクセス承認要求を受けるように構成することができる。更に、ａｄｍｉｎ管理アプリケーション１１４は、サービス・アカウントの存続期間が未だ終わっていないとき、それぞれのディレクトリー・サービス・サーバー・デバイス１３０－ｌによって管理される１つ以上のリソースおよび／またはアセットにアクセスすることを、自動的に１つ以上のクライアント１０２－ａに承認するまたは許可するように構成することができる。

【００６４】

[0069] あるいは、ａｄｍｉｎ管理アプリケーション１１４は、サービス・アカウントの存続期間が既に経過しているとき、それぞれのディレクトリー・サービス・サーバー・デバイス１３０－ｌによって管理される１つ以上リソースおよび／またはアセットに対す

るあらゆる１つ以上のクライアント１０２－ａのアクセスを自動的に否認(deny)するように構成することができる。加えて、一実施形態では、ａｄｍｉｎ管理アプリケーション１１４は、サービス・アカウントをディスエーブルする、および／またはサービス・アカウントを１つ以上の違反境界セキュリティ・グループから離脱させる(disassociate)ように構成することもできる。

【００６５】

[0070] 一実施形態例では、ａｄｍｉｎ管理アプリケーション１１４は、全てのアクセス承認要求を否認することによってサービス・アカウントをディスエーブルし、新たな認証トークンを生成し、この新たに生成した認証トークンをクライアント１０２－ａに供給しないのでもよい。更に、ａｄｍｉｎ管理アプリケーション１１４は、例えば、新たな認証トークンを生成し、認証トークン管理アプリケーション１７２にサービス・アカウントのための認証トークをリセットすることを要請することによって、この新たに生成した認証トークをクライアント１０２－ａに供給しないのでもよい。また、ａｄｍｉｎ管理アプリケーション１１４は、１つ以上の違反境界セキュリティ・グループにおけるメンバーシップからサービス・アカウントを削除することによって、サービス・アカウントを離脱させることもできる。

【００６６】

[0071] 加えてまたは代わりに、ａｄｍｉｎ管理アプリケーション１１４は、更に、任意のイネーブルされたサービス・アカウントを求めてサービス・アカウント・データーストア１２６を周期的にスキャンし、サービス・アカウント存続期間情報に基づいて、存続期間が既に経過したサービス・アカウントをいずれもディスエーブルするように構成することもできる。ある実施形態では、ディスエーブルされたサービス・アカウントは、直ちに、現在使用中のあらゆるサービス・アカウントおよびそれらの関連するアクティブなアクションまたはタスクも終了させる（例えば、強制ログオフ）。１つ以上のリソースおよび／またはアセットを管理する１つ以上のディレクトリー・サーバー・デバイス１３０－１が適正にサービス・アカウント・データーストア１２６と同期されることを確保するために、ａｄｍｉｎ管理アプリケーション１１４は、更に、サービス・アカウントのサービス・アカウント存続期間情報を更新するためおよび／または存続期間が経過したサービス・アカウントをいずれもディスエーブルするために、ネットワーク相互接続１１２とディレクトリー・サービス・サーバー・デバイス１３０－１のディレクトリ・サービス・アプリケーションの１つ以上のＡＰＩとを介して通信するように構成することができる。

【００６７】

[0072] サービス・アカウントがイネーブルされた後、ａｄｍｉｎ管理アプリケーション１１４は、１つ以上の通知メッセージにおいてサービス・アカウント情報を１つ以上のクライアント１０２－ａに、１つ以上のクライアント・デバイス１０４－ｂを通じて通知し供給するように構成することができる。典型的な通知メッセージには、移動体ＳＭＳメッセージング、自動音声コール、電子メール、インタラクティブ・ウェブ・ベースのフォーム、ウェブ警報、インターネットおよび／またはイントラネット・ベースのメッセージング・アプリケーション、あるいは昇格アクセス許可の承認および／または拒否に関して１つ以上のクライアント１０２－ａに通知し、１つ以上のクライアント１０２－ａに要求承認情報、監督承認情報、および／またはサービス・アカウント情報を提供する任意の他の手段を含むことができるが、これらに限定されるのではない。認証トークンを設定または生成するときにクライアントを助けるために、１つ以上のクライアント１０２－ａが認証トークン管理アプリケーション１７２にアクセスして１つ以上のプロビジョニングされたサービス・アカウントのために１つ以上の認証トークンを設定および／または生成することができるように、ａｄｍｉｎ管理アプリケーション１１４は、更に、１つ以上の通知メッセージにおいて、参照（例えば、"https://AuthenticationTokenManagementFrontEnd"または"https://AuthenticationTokenManagementFrontEnd.contoso.com"のようなＵＲＬ）を認証トークン管理アプリケーション１７２に供給するように構成することができる。

【００６８】

[0073] 例示として、「エレン・アダムス」という名前および "EllenAdams@contoso.com"というクライアント・アカウントＵＰＮを有するクライアント１０２－２が、１つ以上のサーバー・デバイス１４０－ｉ－ｊにアクセスするために、サービス・アカウントを、クライアント・デバイス１０４－２とａｄｍｉｎ管理アプリケーション１１４との間における少なくとも暗号化接続を介して要求したと仮定する。この要求に応答して、ａｄｍｉｎ管理アプリケーション１１４は、最初に、クライアント・アカウントＵＰＮ（例えば、"EllenAdams@contoso.com"）と、安全な接続（例えば、信頼および暗号化接続）を確立するためのクライアント・アカウント・パスワードとに基づいて、ａｄｍｉｎ管理アプリケーション１１４にアクセスするためにクライアント１０２－２を認証することができる。あるいは、ａｄｍｉｎ管理アプリケーション１１４は、二要素認証（例えば、スマート・カードおよび関連するＰＩＮ）と、安全な接続を確立するために受けたセキュリティ・トークンとに基づいて、クライアント１０２－２を認証することができる。一旦認証されたなら、クライアント１０２－２は、確立された安全な接続を介して、要求存続期間が４時間のサービス・アカウントを、遠方からサーバー・デバイス１４０－１－１をデバッグするために要求することができる。この要求に応答して、ａｄｍｉｎ管理アプリケーション１１４は、リモート・ユーザーおよびデバッガーという要求役割ならびに違反境界１３８－１－１という要求範囲を含むアクセス許可を有するサービス・アカウントに対して、クライアント１０２－２から受けた要求役割／範囲情報を判定するおよび／または受けることができる。

【００６９】

[0074] 以上の例示を続けると、ａｄｍｉｎ管理アプリケーション１１４は、次いで、クライアント１０２－２のクライアント・アカウントの範囲に該当するまたは適合する１組のアクセス許可を有するサービス・アカウントを求める要求を確保するために、クライアント１０２－２に関連付けられたクライアント・アカウント情報と、サービス・アカウント要求情報（例えば、要求役割／範囲情報）とに基づいて、サービス・アカウントのプロビジョニングを許可するか否か判定することができる。一旦この要求が許可されたなら、ａｄｍｉｎ管理アプリケーション１１４は、要求された役割および範囲と同じまたは実質的に同様の役割および範囲を有する既存のサービス・アカウントがクライアント１０２－２のためにサービス・アカウント・データーストア１２６に既に存在するか否か判定することができる。

【００７０】

[0075] 更に以上の例示を続けて、ａｄｍｉｎ管理アプリケーション１１４が、既存のサービス・アカウントがないと判定したと仮定すると、ａｄｍｉｎ管理アプリケーション１１４は、違反境界セキュリティ・グループ１６８－１－１を利用して違反境界１３８－１－１を実施している１つ以上のディレクトリー・サービス・サーバー・デバイス１３０－ｌの中からディレクトリー・サービス・サーバー・デバイス１３０－ｌを識別することができる。ａｄｍｉｎ管理アプリケーション１１４は、クライアント１０２－２が、ディレクトリー・サービス・サーバー・デバイス１３０－１によって管理されているサーバー・デバイス１４０－１－１、１４０－１－２、１４０－１－３、１４０－１－４、１４０－１－５、１４０－１－６にアクセスできることがあるように、少なくともネットワーク相互接続１１２とディレクトリー・サービス・サーバー・デバイス１３０－１のディレクトリー・サービス・アプリケーション（図示せず）の１つ以上のＡＰＩとを介して通信することによって、サービス・アカウントをプロビジョニングすることができる。

【００７１】

[0076] 更に以上の例示を続けると、ａｄｍｉｎ管理アプリケーション１１４は、違反境界セキュリティ・グループ１６８－１－１を、１組のアクセス許可をサーバー・デバイスサーバー・デバイス１４０－１－１、１４０－１－２、１４０－１－３に付与するように構成された違反境界セキュリティ・グループとして識別することができる。更に、ａｄｍｉｎ管理アプリケーション１１４は、プロビジョニングされたサービス・アカウントに、サーバー・デバイス１４０－１－１、１４０－１－２、１４０－１－３に対する１組の

アクセス許可を付与するために、プロビジョニングされたサービス・アカウントを少なくとも識別された違反境界セキュリティ・グループ１６８－１－１に追加することによって関連付けることもできる。尚、ａｄｍｉｎ管理アプリケーション１１４は、サーバー・デバイス１４０－１－１、１４０－１－２、１４０－１－３においてリモート・デバッグを実行するために、プロビジョニングしたサービス・アカウントがクライアント１０２－１によって使用できるように、リモート・ユーザーおよびデバッガーとしてアクセス許可を付与するために、プロビジョニングしたサービス・アカウントを他のグループ（例えば、リモート・ユーザー・グループ、デバッガー・グループ等）に追加することによって関連付けることもできることは認めることができよう。

【００７２】

[0077] 以上の例示を更に続けると、ａｄｍｉｎ管理アプリケーション１１４は、サービス・アカウント存続期間が４時間であることを示す要求存続期間から導き出され判定されたサービス・アカウント存続期限情報に基づいて、プロビジョニングしたサービス・アカウントをイネーブルすることもできる。サービス・アカウントが午後１２時にクライアント１０２－２にプロビジョニングされたと仮定すると、このプロビジョニングされたサービス・アカウントの存続期間が、サービス・アカウントがプロビジョニングされる時刻である午後１２時から開始し、サービス・アカウントの存続期間が午後４時に終了するときに、ａｄｍｉｎ管理アプリケーション１１４が、このサービス・アカウントに関連付けられたあらゆるアクティブなトークン（例えば、サーバー・デバイス１４０－１－１上における１つ以上のプロセスの実行に使用されるアクセス・トークン）を強制的に終了させるために、認証トークン管理アプリケーション１７２を２回利用して、このサービス・アカウントをディスエーブルし、プロビジョニングされたサービス・アカウントに関連付けられた認証トークンをリセットすることができるようにする。以上の例を更に続けると、一旦サービス・アカウントがイネーブルされたなら、クライアント１０２－２がプロビジョニングされたサービス・アカウントのための認証トークンを設定および／または生成するために認証管理アプリケーション１７２にアクセスできるように、ａｄｍｉｎ管理アプリケーション１１４は、クライアント・デバイス１４０－２を通じて、サービス・アカウント識別子またはサービス・アカウントＵＰＮ（例えば、"EllenAdams_RemoteDebugger@domainl36-l.contoso.com"）と、認証トークン管理アプリケーション１７２への参照（例えば、"https://AuthenticationTokenManagementFrontEnd" または"https://AuthenticationTokenManagementFrontEnd.contoso.com"のようなＵＲＬ）と、をクライアント１０２－２に通知することができる。次いで、クライアント１０２－２は、プロビジョニングされたサービス・アカウントを、生成された認証トークンと共に利用して、午後４時よりも前に、クライアント・デバイス１０４－２およびネットワーク相互接続１１２を介してサーバー・デバイス１４０－１－１を遠方からデバッグする（例えば、リモート・デスクトップ・プロトコル（ＲＤＰ）を利用する）ことができる。

【００７３】

[0078] 種々の実施形態において、認証トークン管理システム１００は、更に、サーバー・デバイス１７０を含むことができる。サーバー・デバイス１７０は、大まかには、アプリケーションの中でもとりわけ、認証トークン管理アプリケーション１７２を実行するように構成することができる。認証トークン管理アプリケーション１７２は、大まかには、認証トークン管理アプリケーション１７２にアクセスするまたはサービス・アカウントのために認証トークンを生成することを要求する１つ以上のクライアント１０２－ａを認証するように構成することができる。認証トークン管理アプリケーション１７２は、ネットワーク相互接続１１２および１つ以上のクライアント・デバイス１０４－２を介して、１つ以上のサービス・アカウントのために１つ以上の認証トークンを生成する要求を、１つ以上のクライアント１０２－ａから受けるように構成することができる。更に、認証トークン管理アプリケーション１７２は、ネットワーク相互接続１１２および１つ以上のクライアント・デバイス１０４－２を介して、サービス・アカウントに関連付けられたサービス・アカウント情報および１つ以上のクライアント１０２－ａのために生成された認証

トークンを、クライアント１０２－ａに供給するように構成することができる。加えて、認証トークン管理アプリケーション１７２は、更に、１つ以上のサービス・アカウントのための１つ以上の認証トークンを管理する、生成する、リセットする、ならびに更新および／または設定することを要求するように構成することができる。

【００７４】

[0079] 種々の実施形態において、認証トークン管理アプリケーション１７２は認証トークン管理コンポーネント１７４を含むことができる。認証トークン管理コンポーネント１７４は、大まかには、認証トークン管理アプリケーション１７２へのアクセス、１つ以上のサービス・アカウントのサービス・アカウント情報の引き出し、および／または１つ以上のディレクトリー・サービス・サーバー・デバイス１３０－ｌおよび／またはａｄｍｉｎ管理アプリケーション１１４の１つ以上のディレクトリー・サービス・アプリケーション（図示せず）によって管理される１つ以上のサービス・アカウントのための認証トークンの生成を要求する１つ以上のクライアント１０２－ａを認証する、またはその有効性を判断するように構成することができる。また、認証トークン管理コンポーネント１７４は、１つ以上のディレクトリー・サービス・サーバー・デバイス１３０－ｌおよび／またはａｄｍｉｎ管理アプリケーション１１４の１つ以上のディレクトリー・サービス・アプリケーション（図示せず）によって管理される１つ以上のサービス・アカウントのサービス・アカウント情報を引き出して提供するように構成することもできる。更に、認証トークン管理コンポーネント１７４は、ａｄｍｉｎ管理アプリケーション１１４からの１つ以上のサービス・アカウントのための認証トークン・リセット要求を受けるように構成することもできる。

【００７５】

[0080] １つ以上のクライアント１０２－ａを認証することを可能にするために、認証トークン管理コンポーネント１７４は、クライアント・アカウント情報の少なくとも一部（例えば、アカウントＵＰＮ、アカウント識別子、および／またはアカウント・パスワード）を１つ以上のクライアント１０２－ａからクライアント・デバイス１０４－ｂを通じて要求するおよび／または受けるように構成することができ、受けたクライアント・アカウント情報を、１つ以上のクライアント１０２－ａのクライアント・アカウントと関連付けることができる。一旦クライアント・アカウント情報を受けたなら、認証トークン管理コンポーネント１７４は、更に、１つ以上のクライアント１０２－ａに関連付けられた、受領(received)クライアント・アカウント情報（例えば、アカウントＵＰＮ、アカウント識別子、および／またはアカウント・パスワード）を認証するためにネットワーク相互接続１１２とディレクトリー・サービス・アプリケーション１１０の１つ以上のＡＰＩとを介して通信するように構成することができる。

【００７６】

[0081] 加えておよび／または代わりに、認証トークン管理コンポーネント１７４は、フェデレーテット・アイデンティティ・アプリケーション１６２によって発行されたセキュリティ・トークン（例えば、ＳＡＭＬトークン）を１つ以上のクライアント１０４－ｂから受けるように構成された要求可能化アプリケーション(claims enabled application)を含むこともできる。更に、認証トークン管理コンポーネント１７４は、受けたセキュリティ・トークンに基づいて、サービス・アカウントを要求した１つ以上のクライアント１０２－ａを認証し識別するように構成することができる。受けたセキュリティ・トークンは、１つ以上のクライアント１０２－ａに関連付けられたクライアント・アカウント情報を含むことができる１つ以上の要求(claim)を含むことができる。クライアント・デバイス１４０－ｂから受けたセキュリティ・トークンを利用することによって、認証トークン管理アプリケーション１７２は少なくとも１つ以上のクライアント・デバイス１０４－ｂとの信頼接続を確立することができる。任意に、認証トークン管理コンポーネント１７４は、更に、認証トークン管理コンポーネント１７４が、認証トークン管理アプリケーション１７２と１つ以上のクライアント１０４－ｂとの間におけるその後のあらゆる通信のために、１つ以上のクライアント１０４－ｂとの信頼接続を確立することができるように、

信頼セッション・クッキー（例えば、ＦｅｄＡｕｔｈクッキー）を１つ以上のクライアント１０４－ｂに供給することもできる。

【００７７】

[0082] 尚、その後の通信のために信頼セッションを維持するための信頼クッキーが１つ以上のクライアント１０４－ｂに供給されなかった場合、認証トークン管理コンポーネント１７４は、１つ以上のクライアント・デバイス１０４－ｂから受けた、サービス・アカウント情報を引き出すまたは認証トークンを生成する各要求の有効性を判断するように構成することもできることは認めることができよう。例えば、認証トークン管理コンポーネント１７４は、受けたセキュリティ・トークンが信頼ＳＴＳプロバイダー、例えば、フェデレーテット・アイデンティティ・アプリケーション１６２によって発行されたこと、そして認証トークンを生成することを要求したクライアントが二要素認証（例えば、スマート・カードおよび関連するＰＩＮ）に基づいて認証されたことを検証することによって、要求の有効性を判断することもできる。

【００７８】

[0083] 信頼接続を更に攻撃者による漏洩または改竄から保護するために、認証トークン管理コンポーネント１７４は、１つ以上のセキュア通信プロトコル（例えば、ハイパーテキスト・トランスファー・プロトコル・セキュア（ＨＴＴＰＳ））を利用して、暗号化接続を確立することもできる。このように、１つ以上のサービス・アカウントの１つ以上の認証トークンを管理するために、認証トークン管理アプリケーション１７２と１つ以上のクライアント・デバイス１０４－ｂとの間に安全な接続（例えば、信頼および暗号化接続）を確立することができる。

【００７９】

[0084] 一旦認証トークン管理アプリケーション１７２と１つ以上のクライアント・デバイス１０４－ｂの各クライアント・デバイスとの間に安全な接続が確立されたなら、認証トークン管理コンポーネント１７４は、クライアントのクライアント・アカウントに関連付けられた１つ以上のサービス・アカウントのサービス・アカウント情報を求める１つ以上の要求を、クライアント１０２－ａからクライアント・デバイス１０４－ｂを通じて、それぞれの安全な接続を介して受けるように構成することができる。認証トークン管理コンポーネント１７４は、少なくとも部分的にクライアント・アカウント情報（例えば、クライアント・アカウント識別子、クライアント・アカウントＵＰＮ等）に基づいて、受けた１つ以上の要求に応答して、１つ以上のサービス・アカウントについてのサービス・アカウント情報を、認証トークン・プロキシー・コンポーネント１７８を介して要求し引き出すように構成することができる。

【００８０】

[0085] 一旦１つ以上のサービス・アカウントについてのサービス・アカウント情報が認証トークン・プロキシー・コンポーネント１７８を介して引き出されたなら、認証トークン管理コンポーネント１７４は、１つ以上のクライアント１０２－ａへの表示のために１つ以上のサービス・アカウントについてのサービス・アカウント情報を１つ以上のクライアント・デバイス１０４－ｂに提供する、および／または１つ以上のクライアント１０２－ｂが１つ以上の認証トークンを生成することを可能にするように構成することができる。加えてまたは代わりに、認証トークン管理コンポーネント１７４は、１つ以上のクライアント・デバイス１０４－ａおよび／またはクライアント１０２－ａに関連付けられたセキュリティ・トークンを受けたことに応答して、少なくとも部分的にクライアント・アカウント情報に基づいて、１つ以上のサービス・アカウントを自動的に引き出して供給するように構成することもできる。

【００８１】

[0086] １つ以上のクライアント・デバイス１０４－ｂに供給された１つ以上のサービス・アカウントについてのサービス・アカウント情報に基づいて、１つ以上のクライアント・デバイス１０４－ｂは、１つ以上のサービス・アカウントのために１つ以上の認証トークンを生成することを要求する１つ以上のクライアント１０２－ａの入力（例えば、キ

ーボード入力、マウス入力、タッチ入力等）を受けるように構成することができる。更に、認証トークン管理コンポーネント１７４は、１つ以上の認証トークンを生成する１つ以上の要求を、１つ以上のクライアント１０２－ａから１つ以上のクライアント・デバイス１０４－ｂを通じて受けるように構成することもできる。尚、認証トークンを生成することの要求は各々、トークン要求情報と関連付けられるとよいことは認められよう。トークン要求情報は、サービス・アカウント識別子、サービス・アカウントＵＰＮ、および／またはサービス・アカウントを識別するための任意の他の情報というような、サービス・アカウント情報を含むことができるが、これらに限定されるのではない。

【００８２】

[0087] 加えて、認証トークンの生成のセキュリティを更に確保するために、認証トークン管理コンポーネント１７４は、更に、クライアントがそれらのクライアント・アカウントに関連付けられたサービス・アカウントのためにのみ認証トークンを生成できることに限定されることが可能となるように、認証トークンを生成することが要求されたサービス・アカウントがクライアント・アカウントと関連付けられているか否か判定することによって、サービス・アカウントのために認証トークンを生成する要求およびトークン要求情報の有効性を判断するように構成することもできる。更に、認証トークン管理コンポーネント１７４は、認証トークン管理コンポーネント１７４が、認証トークンを生成することが要求されたサービス・アカウントがクライアント・アカウントと関連付けられていないと判定したとき、サービス・アカウントのために認証トークンを生成するあらゆる要求を拒否するように構成することができる。

【００８３】

[0088] 更に、サービス・アカウント存続期限情報によって示される少なくとも限定存続期限に随意に関連付けることができるサービス・アカウントに対して、生成された認証トークンは、サービス・アカウントがイネーブルされ続けるまたはアクティブであり続けるのと同じ期間だけ有効である(live)、即ち、存続できることも認めることができよう。つまり、先に論じたように、サービス・アカウントの存続期間の終了時に、即ち、サービス・アカウントの存続期間が終了しサービス・アカウントがディスエーブルされるとき、認証トークン管理コンポーネント１７４は、このaサービス・アカウントに関連付けられたいずれのアクティブなトークン（例えば、アクセス・トークン）も失効できるように、失効したサービス・アカウントの認証トークンをリセットする要求を少なくとも１回（または２回以上）受けるように構成することができる。尚、認証トークンをリセットする各要求が、トークン・リセット情報と関連付けられるとよいことは認めることができよう。トークン・リセット情報は、サービス・アカウント識別子、サービス・アカウントＵＰＮ、および／またはサービス・アカウントのための認証トークンのリセットが望まれる失効サービス・アカウントを識別するための任意の他の情報というようなサービス・アカウント情報を含むことができるが、これらに限定されるのではない。

【００８４】

[0089] 種々の実施形態において、認証トークン管理アプリケーション１７２は、認証トークン生成コンポーネント１７６を含むことができる。認証トークン生成コンポーネント１７６は、大まかには、１つ以上の認証トークンを生成する要求の有効性が認証トークン管理コンポーネント１７４によって判断された後に、様々な複雑さの１つ以上の認証トークンを１つ以上のサービス・アカウントのために生成するように構成することができる。加えてまたは代わりに、認証トークン生成コンポーネント１７６は、更に、１つ以上のサービス・アカウントのための認証トークンをリセットする要求に応答して、サービス・アカウントのための１つ以上の認証トークンを生成するように構成することもできる。更に、認証トークン生成コンポーネント１７６は、認証トークン・プロキシー・コンポーネント１７８を介して、１つ以上のサービス・アカウントのために生成された認証トークンを更新または設定するように構成することができる。

【００８５】

[0090] 安全に認証トークンを生成するために、認証トークン生成コンポーネント１７

６は、１つ以上のセキュア・ハードウェアおよび／またはソフトウェア・コンポーネント（例えば、信頼プラットフォーム・モジュール（ＴＰＭ）、ＭＩＣＲＯＳＯＦＴ．ＮＥＴ Ｆｒａｍｅｗｏｒｋ ＬｉｂｒａｒｙのＳｙｓｔｅｍ.Ｗｅｂ.Ｓｅｃｕｒｉｔｙ.Ｍｅｍｂｅｒｓｈｉｐ等）を利用することによって、認証トークンを生成するように構成することができる。更に、認証トークン生成コンポーネント１７６によって生成された認証トークンは、例えば、１つ以上のセキュア・ハードウェアおよび／またはソフトウェア・コンポーネントによって実現される１つ以上の暗号的に安全な乱数発生器および／またはハッシュ関数を利用する１つ以上のフォーマット（例えば、ユニバーサル・キャラクター・セット（ＵＣＳ）変換フォーマット－８ビット（ＵＴＦ－８）、ＵＴＦ－１６ビット（ＵＴＦ－１６)、基本ストリングまたは二進ストリング（ＢＳＴＲ）、Ｃ－ストリング等）でエンコードされたランダム・データー（例えば、ランダム・バイト等）および／またはランダム・キャラクター・ストリングを含むことができる。加えて、認証トークン生成コンポーネント１７６は、少なくとも長さ／サイズ・パラメーターおよび／またはキャラクター・クラス・パラメーターに基づいて認証トークンを生成することもできる。

【００８６】

[0091] 認証トークンが平文ランダム・パスワード、パスコード、パスフレーズ、ＰＩＮ等を含むことができる実施形態では、長さ／サイズ・パラメーターが、認証トークン生成コンポーネント１７６によって生成される最小長（例えば、２５キャラクター）を指定することができる。あるいは、長さパラメーターは、認証トークン生成コンポーネント１７６が、範囲の下限および上限以内に入る可変長の平文ランダム・パスワードを生成できるように、範囲（例えば、２５から３０キャラクターの間）を指定することもできる。平文ランダム・パスワードのセキュリティを更に確保するために、生成されたランダム・パスワードを１人以上の人間のクライアント１０２－ａが正確に記憶するとき、および／または通常の手段および／または媒体（例えば、手書きのメモ、口頭伝達等）によって伝達するときに著しい困難に直面するとよいように、長さパラメーターは、長さが数百または数千ものキャラクターで平文ランダム・パスワードを生成することを指定するように構成することもできる。

【００８７】

[0092] 認証トークンが平文ランダム・パスワード、パスコード、パスフレーズ、ＰＩＮ等を含むことができる実施形態では、認証トークン生成コンポーネント１７６が１つ以上の特定のキャラクター・クラスの少なくとも１つのキャラクターを含む認証トークンを生成できるように、キャラクター・クラス・パラメーターを使用してキャラクター・クラスの１つ以上の組み合わせを指定することもできる。典型的なキャラクター・クラスには、小文字（例えば、ａからｚまで）、大文字（例えば、ＡからＺまで）、記号（例えば、" ’ ~!@#$% ^ &*()[]{};:'",.?//*-+"）、数値（例えば、数値０から９まで）、または１つ以上のフォーマット（例えば、ＵＴＦ－８、ＵＴＦ－１６等）で定めることができる任意の他のキャラクター・クラスを含むことができるが、これらに限定されるのではない。

【００８８】

[0093] 認証トークンが平文ランダム・パスワード、パスコード、パスフレーズ、ＰＩＮ等を含むことができる実施形態では、認証トークン生成コンポーネント１７６は、更に、１つ以上のサービス・アカウントに関連付けられた言語および／またはロカール情報には関係なく標準的な入力デバイス（例えば、標準的な１０４キーのキーボード）を使用することによって認証トークンの入力を容易にするために、標準的な入力デバイス上に含まれる１つ以上のキャラクター・クラスを含む認証トークンを生成するように構成することもできる。一旦認証トークンが生成されたなら、認証トークン生成コンポーネント１７６は、少なくとも部分的にプロキシー認証情報（例えば、認証トークン・プロキシー・コンポーネント１７８とトークン管理プロキシー・アプリケーション１９２との間における共有シークレット・ディジタル証明書、および共有シークレット・ディジタル証明書のディジタル指紋または親指の指紋）に基づいて、認証トークン・プロキシー・コンポーネント１７８を介して１つ以上のサービス・アカウントのための認証トークンを更新または設定

するように構成することができる。

【００８９】

[0094] 生成された各認証トークンが一意であり、異なるサービス・アカウントのために再利用されないことを確実にするために、認証トークン生成コンポーネント１７６は、更に、１つ以上の以前に生成され使用された認証トークンのダイジェストまたはハッシュを認証トークン衝突データーストア(authentication token collision datastore)（図示せず）に格納するように構成することができる。つまり、例示の一実施態様では、認証トークン生成コンポーネント１７６は、認証トークンを生成し、生成した認証トークンのハッシュまたはダイジェストを決定または計算し、以前に生成された認証トークンが既に使用および／または生成されているか否か判定するために、ハッシュまたはダイジェストを比較することによって、新たに生成した認証トークンを検索するまたは認証トークン衝突データーストアに格納されているものと照合するように構成することができる。一致が発見されない場合、認証トークン生成コンポーネント１７６は新たに生成した認証トークンのハッシュまたはダイジェストを認証トークン衝突データーストアに格納することができ、新たに生成された認証トークンは、サービス・アカウントを更新するために使用することができる。一致が発見された場合、認証トークン生成コンポーネント１７６は、次に、新たな認証トークンを生成すればよく、以上のプロセスは、一意の認証トークンが生成されるまで繰り返される。

【００９０】

[0095] 尚、一旦認証トークンが生成され、その生成された認証トークンがサービス・アカウントのための認証トークンを更新または設定するために利用されたなら、この生成された認証トークンは、一旦失われたなら、１つ以上のクライアント１０２－ａのために復元されてはならないことは認めることができよう。つまり、ある実施形態では、認証トークン生成コンポーネント１７６によって生成された各認証トークンは、復元不可能、不変、および／または一意の認証トークンであってもよい。実施形態はこの文脈において限定されるのではない。

【００９１】

[0096] 更に、認証トークンの生成の安全を確保し監視できるように、認証トークンの生成が集中位置、即ち、認証トークン管理アプリケーション１７０内で実行できるように、認証トークン生成コンポーネント１７６が、認証トークン管理システム１００における唯一の認証トークン生成のためのコンポーネントであるように構成されてもよいことも認めることができよう。

【００９２】

[0097] 種々の実施形態において、認証トークン管理コンポーネント１７２は、認証トークン・プロキシー・コンポーネント１７８を含むことができる。認証トークン・プロキシー・コンポーネント１７８は、大まかには、プロキシー認証情報を格納し、１つ以上のセキュア通信プロトコル（例えば、ＨＴＴＰＳ）およびプロキシー認証情報を利用して、ネットワーク相互接続１１２を介してサーバー・デバイス１９０上で実行するトークン管理プロキシー・アプリケーション１９２との少なくとも暗号化接続を確立するように構成することができる。更に、少なくとも暗号化接続の確立を可能にするために、データーセンター１４２に内蔵されたトークン管理プロキシー・アプリケーション１９２は、認証トークン・プロキシー・コンポ１７８がトークン管理プロキシー・アプリケーションと接続し、少なくとも暗号化接続を確立できるように、公開エンドポイントを露出(expose)または実装することができる。

【００９３】

[0098] 種々の実施形態において、認証トークン・プロキシー・コンポーネント１７８は、更に、確立された暗号化接続を介して、トークン管理プロキシー・アプリケーション１９２を管理しこれと通信するように構成することができる。また、認証トークン・プロキシー・コンポーネント１７８は、ネットワーク相互接続１１２を介してトークン管理プロキシー・アプリケーション１９２と通信することによって、１つ以上のサービス・アカ

ウントのサービス・アカウント情報を引き出すように構成することもできる。また、認証トークン・プロキシー・コンポーネント１７８は、１つ以上のサービス・アカウントのサービス・アカウント情報をトークン管理プロキシー・アプリケーション１９２から、確立された暗号化接続を介して、受けるように構成することもできる。更に、認証トークン・プロキシー・コンポーネント１７８は、確立された暗号化接続を介してトークン管理プロキシー・アプリケーション１９２と通信することによって、１つ以上のサービス・アカウントの生成された認証トークンを更新または設定することを要求するように構成することもできる。

【００９４】

[0099] １つ以上のクライアント１０２－ａに関連付けられた１つ以上のサービス・アカウントを引き出すために、認証トークン・プロキシー・コンポーネント１７８は、少なくともクライアント・アカウント情報（例えば、クライアント・アカウント識別子、クライアント・アカウントＵＰＮ等）と、確立された暗号化接続を介して認証トークン・プロキシー・コンポーネント１７８によって格納されたプロキシー認証情報の一部（例えば、共有シークレット・ディジタル証明書のディジタル指紋または親指の指紋）と、を提供することによって、トークン管理プロキシー・アプリケーション１９２に、１つ以上のサービス・アカウントについてのサービス・アカウント情報を要求することができる。この要求に応答して、認証トークン・プロキシー・コンポーネント１７８は、１つ以上のクライアント１０２－ａに関連付けられた１つ以上のサービス・アカウントの、要求したサービス・アカウント情報を、確立された暗号化接続を介して受けることもできる。

【００９５】

[00100] １つ以上のクライアント１０２－ａに関連付けられた１つ以上のサービス・アカウントのための認証トークンを更新または設定するために、認証トークン・プロキシー・コンポーネント１７８は、少なくともサービス・アカウント情報（例えば、サービス・アカウント識別子、サービス・アカウントＵＰＮ等）、生成した認証トークン、およびプロキシー認証情報の一部（例えば、共有シークレット・ディジタル証明書のディジタル指紋または親指の指紋）を、確立された暗号化接続を介して提供することによって、１つ以上のサービス・アカウントの、生成された認証トークンを更新または設定することを要求するように構成することができる。

【００９６】

[00101] 生成された認証トークンが後の時点において１つ以上のクライアント１０２－ａによってサービス・アカウントを使用して更新されるまたは変更されることができないこと、または復元可能になれないことを確保するために、認証トークン・プロキシー・コンポーネント１７８は、トークン管理プロキシー・アプリケーション１９２によって、確立された暗号化接続を介して、生成された認証トークンを復元不可能および／または不変の認証トークンとして（少なくとも１つ以上のサービス・アカウントに関して）更新または設定することを要求するように構成することができる。

【００９７】

[00102] １つ以上のサービス・アカウントのための１つ以上の認証トークンをリセットするために、認証トークン・プロキシー・コンポーネント１７８は、少なくともサービス・アカウント情報（例えば、サービス・アカウント識別子、サービス・アカウントＵＰＮ等）、生成された認証トークン、およびプロキシー認証情報（例えば、共有シークレット・ディジタル証明書のディジタル指紋または親指の指紋）を、確立された暗号化接続を介して供給することによって、１つ以上のサービス・アカウントの認証トークンを更新または設定することを要求するように構成することができる。

【００９８】

[00103] 種々の実施形態において、認証トークン管理コンポーネント１７２は、更に、認証トークン通知コンポーネント１８０を含むことができる。認証トークン通知コンポーネント１８０は、大まかには、生成された認証トークンを１つ以上のクライアント１０２－ａに、認証トークン管理コンポーネント１７２と１つ以上のクライアント・デバイス

１０４－ｂとの間に以前に確立された安全な接続を介して、供給するように構成することができる。

【００９９】

[00104] 一実施形態では、認証トークン通知コンポーネント１８０は、以前に確立された安全な接続を介して、少なくとも生成された認証トークンを１つ以上のクライアント・デバイス１０４－ｂに、隠れエレメントまたは不可視エレメントとして供給し、１つ以上のクライアント・デバイス１０４－ｂがプログラム的に認証トークンにアクセスする（例えば、プログラム的クリップボード・アクセスおよび／または文書オブジェクト・モデル（ＤＯＭ）アクセス）ことを可能にするように構成することができる。任意に、認証トークン通知コンポーネント１８０は、認証トークンに関連付けられたサービス・アカウント識別子またはサービス・アカウントＵＰＮを、プログラム的アクセスのための隠れエレメントまたは不可視エレメントとして供給するように構成することもできる。

【０１００】

[00105] 加えてまたは代わりに、認証トークン通知コンポーネント１８０は、認証トークンを明示することのクライアント１０２－ａによる要求(demand)に応答して、生成された認証トークンを、クライアント・デバイス１０４－ｂ上で明示できるエレメントとして供給するように構成することもできる。任意に、認証トークン通知コンポーネント１８０は、更に、認証トークンを明示することのクライアント１０２－ａによる要求(demand)に応答して、サービス・アカウント識別子および／またはサービス・アカウントＵＰＮ、ならびに生成された認証トークンを表示することができ、１つ以上のクライアント１０２－ａに同時に見ることができるように、認証トークンに関連付けられたサービス・アカウント識別子またはサービス・アカウントＵＰＮを、クライアント・デバイス１０４－ｂ上において明示できる可視エレメントとして供給するように構成することもできる。

【０１０１】

[00106] 一旦１つ以上のクライアント・デバイス１０４－ｂが認証トークンを受けたなら、クライアント・デバイス１０４－ｂは、自動的そして安全に、サービス・アカウント識別子および／またはサービス・アカウントＵＰＮ、ならびに関連する認証トークンを、認証トークン・データーストア１６６（例えば、パスワード・セーフ）に、１つ以上の暗号アルゴリズム（例えば、Ｔｗｏｆｉｓｈ対称鍵ブロック暗号）を利用した暗号化フォーマットで格納することができる。尚、１つ以上のクライアント・デバイス１０４－ｂが、認証トークン通知コンポーネント１８０によって供給された生成認証トークンを受けた後に、認証トークンが１つ以上のクライアント１０２－ａによって、例えば、認証トークン・データーストア１６６またはその他の場所（例えば、可能であれば、手書き）に格納されなかったなら、生成された認証トークンは、後の時点においてアクセス可能、視認可能、または復元可能にならない場合もあることは認めることができよう。一旦格納されたなら、１つ以上のクライアント１０２－ａは、次いで、１つ以上のリソースおよび／またはアセット（例えば、サービス・デバイス１４０－ｉ－ｊ）にアクセスするために、格納されたサービス・アカウント識別子および／またはサービス・アカウントＵＰＮ、ならびに関連する認証トークンを引き出すことができる。

【０１０２】

[00107] 尚、認証トークンが、１つ以上のサービス・アカウントのための認証トークンをリセットする要求に応答して生成された場合、認証トークン通知コンポーネント１８０が、生成された認証トークンをクライアント１０２－ａにクライアント・デバイス１０４－ｂによってそれぞれの安全な接続を介して供給しないように構成されるとよいことは認めることができよう。

【０１０３】

[00108] 更に、ａｄｍｉｎ管理アプリケーション１１４を利用して、１つ以上のプロビジョニングされたサービス・アカウントのために認証トークンを生成するために認証トークン管理アプリケーション１７２と共に１つ以上のサービス・アカウントを供給することによって、ある実施形態では、データーセンター１４２における１つ以上のＳａａＳシ

ステムにおける各サービス・アカウントは、機械生成認証トークンと置き換えられても、または機械生成認証トークンを利用してもよいことも認めることができよう。

【０１０４】

[00109] 例示として、「エレン・アダムス」という名前および "EllenAdams@contoso.com"というクライアント・アカウントＵＰＮを有するクライアント１０２－２が、４時間の要求存続期間でサーバー・デバイス１４０－１－１を遠方からデバッグするためにサービス・アカウントを要求したと仮定する。このサービス・アカウントを求める要求に応答して、ａｄｍｉｎ管理アプリケーション１１４は、サービス・アカウントＵＰＮ "EllenAdams_RemoteDebugger@domainl36-l.contoso.com"を有するサービス・アカウントをプロビジョニングし、認証トークン管理アプリケーション１７２に対するこのサービス・アカウントＵＰＮおよび https://AuthenticationTokenManagementFrontEnd"または "https://AuthenticationTokenManagementFrontEnd.contoso.com"というＵＲＬを、クライアント・デバイス１０４－２をクライアント１０２－２に通じて通知した。次いで、クライアント１０２－２は、クライアント・デバイス１０４－２上で実行するクライアント・アプリケーション（例えば、ウェブ・ブラウザー）を介して、少なくとも暗号化接続を介して、認証管理アプリケーション１７２にアクセスすることを要求する。

【０１０５】

[00110] 以上の例示を続けると、そして認証管理アプリケーション１７２にアクセスする要求に応答して、認証トークン管理コンポーネント１７４は、最初に、安全な接続（例えば、信頼および暗号化接続）を確立するために、クライアント・アカウントＵＰＮ（例えば、"EllenAdams@contoso.com"）とクライアント・アカウント・パスワードとに基づいて、認証トークン管理コンポーネント１７２にアクセスするクライアント１０２－２を認証することができる。あるいは、認証トークン管理コンポーネント１７４は、二要素認証（例えば、スマート・カードおよび関連するＰＩＮ）と受けたセキュリティ・トークンとに基づいて、安全な接続を確立するために、クライアント１０２－２を認証することができる。一旦認証されたなら、クライアント１０２－２は、確立された安全な接続を介して、クライアント・デバイス１０４－２（例えば、非同期ジャヴァスクリプト（ＡＪＡＸ）ＰＯＳＴ）によって、クライアント・アカウントＵＰＮ "EllenAdams@contoso.com"に関連付けられた１つ以上のサービス・アカウントを要求することができる。

【０１０６】

[00111] 以上の例示を更に続けると、そして１つ以上のサービス・アカウントを求める要求に応答して、または自動的にクライアント１０２－２の認証成功に基づいて、認証トークン管理コンポーネント１７４、次に、認証トークン・プロキシー・コンポーネント１７８を介して、クライアント・アカウントＵＰＮ "EllenAdams@contoso.com"に関連付けられた１つ以上のサービス・アカウントのサービス・アカウント情報を要求することができる。更に、認証トークン・プロキシー・コンポーネント１７８は、次に、データーセンター１４２に収容されているトークン管理プロキシー・アプリケーション１９２によって露出された公開エンドポイントと比較して(against)サービス・アカウント情報を引き出す要求（例えば、リモートパワーシェル(PowerShell)コマンド）を発行することができる。この要求は、クライアント・アカウントＵＰＮ "EllenAdams@contoso.com"と、共有シークレット・ディジタル証明書のディジタル指紋または親指の指紋のような、プロキシー認証情報の一部とを含むことができるが、これらに限定されるのではない。認証トークン管理コンポーネント１７４は、次いで、１つ以上のサービス・アカウントについてのサービス・アカウント情報を受けることができる。サービス・アカウント情報は、"EllenAdams_RemoteDebugger@domainl36-l.contoso.com"というサービス・アカウントＵＰＮを有する、以前にプロビジョニングされたサービス・アカウントについてのサービス・アカウント情報を含むことができるが、これに限定されるのではない。

【０１０７】

[00112] 以上の例示を更に続けると、認証トークン管理コンポーネント１７４は、次いで、クライアント１０２－２に関連付けられた、受領サービス・アカウント情報を、例

えば、ウェブ・ブラウザーにおけるウェブ・ページのような、クライアント・デバイス１０４－２のクライアント・アプリケーションに供給することができる。クライアント・デバイス１０４－２のクライアント・アプリケーションに供給される１つ以上のサービス・アカウントについてのサービス・アカウント情報の実施形態例を図２に示す。サービス・アカウント情報に応答して、クライアント１０２－２は、クライアント・デバイス１０４－２（例えば、ＡＪＡＸ　ＰＯＳＴ）を通じて、サービス・アカウント識別子またはサービス・アカウントＵＰＮによって識別されたサービス・アカウントのために認証トークンを生成することを要求することができる。

【０１０８】

[00113] 以上の例示を更に続けると、そして認証トークンを生成する要求に応答して、認証トークン生成コンポーネント１７６は、典型的な平文ランダム・パスワードが "Xe2&a^%5"を含むように、長さパラメーター（例えば、８文字）およびキャラクター・クラス・パラメーター（例えば、ａ～ｚ、Ａ～Ｚ、０～９、および記号）に基づいて、例えば、一意の平文ランダム・パスワードを生成することができる。尚、実際には、典型的な平文ランダム・パスワードのような、生成される認証トークンは、遙かに多い文字（例えば、長さが２５～３０文字、または１００から１０，０００文字ですら）を含むこともあり、そして遙かに複雑であることもあるので、この典型的な平文ランダム・パスワードは、理解の目的に限って示されたということは認めることができよう。

【０１０９】

[00114] 以上の例を更に続けると、例えば、典型的な平文ランダム・パスワードのような認証トークンが生成された後、認証トークン生成コンポーネント１７６は、認証トークン・プロキシー・コンポーネント１７８を介して、認証トークンを典型的な平文ランダム・パスワード "Xe2&a^%5"に更新または設定する要求を発行することができる。更に、認証トークン・プロキシー・コンポーネント１７８は、次いで、データーセンター１４２内に収容されているトークン管理プロキシー・アプリケーション１９２によって露出された公開エンドポイントと比較して、認証トークンを更新または設定する要求（例えば、リモート・パワーシェル・コマンド）を発行することができる。この要求は、サービス・アカウントＵＰＮ "EllenAdams_RemoteDebugger@domainl36-l.contoso.com"、典型的な平文ランダム・パスワード "Xe2&a^%5"、および共有シークレット・ディジタル証明書のディジタル指紋または親指の指紋のような、プロキシー認証情報の一部を含むことができるが、これらに限定されるのではない。

【０１１０】

[00115] 以上の例示を更に続けると、認証トークンがサービス・アカウントのために更新または設定された後、認証トークン通知コンポーネント１８０は、クライアント１０２－２にクライアント・デバイス１０４－２を通じて、確立された安全な接続（例えば、ＨＴＴＰＳを利用した信頼および暗号化接続）を介して、少なくとも典型的な平文ランダム・パスワード "Xe2&a^%5"（例えば、ジャヴァスクリプト・オブジェクト・ノテーション（ＪＳＯＮ）アレイに格納された）を、クライアント・デバイス１０４－２のウェブ・ブラウザー上のウェブ・ページにおける隠れたｄｉｖ(hidden div)として通知および／または供給することができる。任意に、隠れたｄｉｖは、サービス・アカウントＵＰＮ "EllenAdams_RemoteDebugger@domainl36-l.contoso.com"も含むことができる。

【０１１１】

[00116] 以上の例示を更に続けると、認証トークン通知コンポーネント１８０が、クライアント１０２－２に、典型的な平文ランダム・パスワードおよび／またはサービス・アカウントＵＰＮを通知および／または供給した後、クライアント１０２－２は、次いで、クライアント・デバイス１０４－２のクリップボードを通じて、典型的な平文ランダム・パスワード "Xe2&a^%5"および／またはサービス・アカウントＵＰＮにアクセスし、典型的な平文ランダム・パスワード "Xe2&a^%5"および／またはサービス・アカウントＵＰＮ "EllenAdams_RemoteDebugger@domainl36-l.contoso.com"を、例えば、パスワード・セーフのようなクライアント・デバイス１０４－２に通信可能に結合されている認証トーク

ン・データーストア１６６に格納することができる。加えてまたは代わりに、典型的な平文ランダム・パスワードおよび／またはサービス・アカウントＵＰＮは、典型的な平文ランダム・パスワードを明示するクライアント１０２－２による要求(demand)（即ち、「要求に応じた明示」）に応答して、クライアント・デバイス１０４－２上で明示されることが可能なエレメントとして提示されてもよい。加えてまたは代わりに、クライアント・デバイス１０４－２上でウェブ・ブラウザーと関連付けられたプラグイン・コンポーネントが、ＤＯＭオブジェクトを介して、典型的な平文ランダム・パスワード "Xe2&a^%5"および／またはサービス・アカウントＵＰＮ "EllenAdams_RemoteDebugger@domainl36-l.contoso.com"に自動的にアクセスし、典型的な平文ランダム・パスワードおよび／またはサービス・アカウントＵＰＮを、クライアント１０２－２からの入力が全くなくても、認証トークン・データーストア１６６に自動的に格納するように構成することもできる。

【０１１２】

[00117] 以上の例示を更に続けると、典型的な平文ランダム・パスワードおよび／またはサービス・アカウントＵＰＮがクライアント１０２－２にクライアント・デバイス１０４－２を通じて、確立された安全接続を介して供給された後に、クライアント１０２－２は、次いで、サービス・アカウントＵＰＮ "EllenAdams_RemoteDebugger@domainl36-l.contoso.com"によって識別された、プロビジョニングされたサービス・アカウントを、典型的な平文ランダム・パスワード "Xe2&a^%5"と共に利用して、４時間のサービス・アカウント存続期間内で、データーセンター１４２におけるサーバー・デバイス１４０－１－１にアクセスし遠方からデバッグする（例えば、リモート・デスクトップ・プロトコル（ＲＤＰ）を使用して）ことができる。

【０１１３】

[00118] 種々の実施形態において、認証トークン管理システム１００のデーターセンター１４２は、サーバー・デバイス１９０を含むことができる。サーバー・デバイス１９０は、大まかには、アプリケーションの中でもとりわけ、トークン管理プロキシー・アプリケーション１９２を実行するように構成することができる。トークン管理プロキシー・アプリケーション１９２は、１つ以上のサービス・アカウントのサービス・アカウント情報を引き出し、および／または１つ以上のサービス・アカウントのための１つ以上の認証トークンを更新または設定するために、データーセンター１４２および／またはネットワーク相互接続１１２における１つ以上のネットワークを介して、１つ以上のディレクトリー・サービス・サーバー・デバイス１３０－１に通信可能に結合することができる。

【０１１４】

[00119] トークン管理プロキシー・アプリケーション１９２は、大まかには、認証トークン管理アプリケーション１７２が、認証トークン管理アプリケーション１７２とトークン管理プロキシー・アプリケーション１９２との間に少なくとも暗号化接続（例えば、ＨＴＴＰＳプロトコルを利用する暗号化接続）を接続し確立することを可能にするために、データーセンター１４２における公開エンドポイントを露出(expose)または実装する(implement)ように構成することができる。トークン管理プロキシー・アプリケーション１９２は、少なくとも暗号化接続を確立するために利用することができるプロキシー認証情報を格納するように構成することができる。トークン管理プロキシー・アプリケーション１９２は、更に、サービス・アカウント情報を求める要求を受け、サービス・アカウント情報を引き出し、そして１つ以上のサービス・アカウントのための認証トークンを更新または設定するように構成することができる。

【０１１５】

[00120] 種々の実施形態において、トークン管理プロキシー・アプリケーション１９２はサービス・アカウント引き出しコンポーネント１９４を含むことができる。サービス・アカウント引き出しコンポーネント１９４は、大まかには、認証トークン・プロキシー・コンポーネント１７８からのサービス・アカウント情報を求める要求を、確立された暗号化接続を介して受け、サービス・アカウント情報を１つ以上のディレクトリー・サービス・サーバー・デバイス１３０－１の１つ以上のディレクトリー・サービス・アプリケー

ションから引き出し、引き出したサービス・アカウント情報を認証トークン・プロキシー・コンポーネント１７８に、確立された暗号化接続を介して、提供するように構成することができる。

【０１１６】

[00121] 一実施形態では、サービス・アカウント引き出しコンポーネント１９４は、クライアント・アカウントに関連付けられたサービス・アカウント情報を引き出す要求を受けるように構成することができる。各要求は、少なくともクライアント・アカウント情報（例えば、クライアント・アカウント識別子、クライアント・アカウントＵＰＮ等）と、プロキシー認証情報の一部（例えば、共有シークレット・ディジタル証明書のディジタル指紋または親指の指紋）とを含むことができる。サービス・アカウント情報を求める要求を受けたことに応答して、サービス・アカウント引き出しコンポーネント１９４は、受けたプロキシー認証情報の一部に基づいて、受けた要求を許可するように構成することができる。

【０１１７】

[00122] 一旦要求が許可されたなら、サービス・アカウント引き出しコンポーネント１９４は、更に、クライアント・アカウント識別子またはクライアント・アカウントＵＰＮによって識別されたクライアント・アカウントに関連付けられた１つ以上のサービス・アカウントについてのサービス・アカウント情報を引き出すために、ネットワーク相互接続１１２と、１つ以上のディレクトリー・サービス・サーバー・デバイス１３０－１のディレクトリー・サービス・アプリケーション（図示せず）の１つ以上のＡＰＩと、を介して通信するように構成することができる。一旦サービス・アカウント情報が引き出されたら、サービス・アカウント引き出しコンポーネント１９４は、１つ以上のサービス・アカウントについての引き出したサービス・アカウント情報を、認証プロキシー・コンポーネント１７８に、確立された暗号化接続を介して、提供するように構成することができる。

【０１１８】

[00123] 種々の実施形態において、トークン管理プロキシー・アプリケーション１９２は、更に、認証トークン更新コンポーネント１９６を含むことができる。認証トークン更新コンポーネント１９６は、大まかには、更新要求を受け、サービス・アカウントに関連付けられた１つ以上の認証トークンを更新または設定するように構成することができる。

【０１１９】

[00124] 一実施形態では、認証トークン更新コンポーネント１９６は、更新要求を受け、１つ以上のサービス・アカウントのための認証トークンを更新または設定するように構成することができる。各要求は、少なくともサービス・アカウント情報（例えば、サービス・アカウント識別子、サービス・アカウントＵＰＮ等）、サービス・アカウントのために生成され更新または設定するための認証トークン、およびプロキシー認証情報の一部（例えば、共有シークレット・ディジタル証明書のディジタル指紋または親指の指紋）を含むことができる。サービス・アカウントのための認証トークンを更新する要求を受けたことに応答して、認証トークン更新コンポーネント１９６は、受けたプロキシー認証情報の一部に基づいて、受けた要求を許可するように構成することができる。

【０１２０】

[00125] 一旦要求が許可されたなら、認証トークン更新コンポーネント１９６は、少なくとも部分的に、サービス・アカウントに関連付けられたサービス・アカウント情報に含まれるディレクトリー・サービス情報に基づいて、サービス・アカウントを管理する該当のディレクトリー・サービス・サーバー・デバイス（例えば、サービス・アカウントに関連付けられたディレクトリー・サービス・サーバー・デバイス）を識別するように構成することができる。尚、ディレクトリー・サービス情報を含むサービス・アカウント情報は、要求において認証トークン管理コンポーネント１７４によって提供されてもよいことは認めることができよう。

【０１２１】

[00126] 一旦ディレクトリー・サービス・サーバー・デバイスが識別されたなら、認証トークン更新コンポーネント１９６は、更に、サービス・アカウント識別子またはサービス・アカウントＵＰＮによって識別されたサービス・アカウントのための認証トークンを、生成され受けた認証トークンによって更新または設定するために、ネットワーク相互接続１１２と、識別されたディレクトリー・サービス・サーバー・デバイスのディレクトリー・サービス・アプリケーション（図示せず）の１つ以上のＡＰＩと、を介して通信するように構成することができる。

【０１２２】

[00127] 認証トークンが使用可能な形態で復元不可能であることを確実にするために、ある実施形態では、ディレクトリー・サービス・サーバー・デバイスが漏洩されても、元の認証トークンは攻撃者によって復元可能にはできないように、識別されたディレクトリー・サービス・サーバー・デバイスは、生成されたトークンまたは生成された認証トークンのソルトされたバージョンの暗号一方向ハッシュだけを格納することもできる。

【０１２３】

[00128] 尚、不変の認証トークンが望まれる実施態様では、認証トークン更新コンポーネント１９６は、更に、１つ以上のサービス・アカウントが１つ以上のサービス・アカウントに関連付けられた認証トークを更新するために必要なアクセス許可（１つまたは複数）を有することができないように、サービス・アカウントのために生成され受けた認証トークンを不変の認証トークとして（少なくとも１つ以上のサービス・アカウントに関して）更新または設定するために、ネットワーク相互接続１１２と、識別されたディレクトリー・サービス・サーバー・デバイスのディレクトリー・サービス・アプリケーション（図示せず）の１つ以上のＡＰＩと、を介して通信するように構成することができる。

【０１２４】

[00129] 以上の実施態様の例示の非限定的な実施態様では、トークン管理プロキシー・アプリケーション１９２は、サーバー・デバイス１９０上に格納されたサービス・アカウント引き出しシェル・スクリプト（例えば、MICROSOFT GetAccountsForUser.ps1パワーシェル・スクリプト）および認証トークン更新シェル・スクリプト（例えば、MICROSOFT ResetPassword.ps1パワーシェル・スクリプト）によって実装することもできる。加えて、サービス・デバイス１９０は、サービス・アカウント引き出しシェル・スクリプトおよび認証トークン更新シェル・スクリプトを実行するように構成されたアクセス許可を有するプロキシー・アカウントを含んでもよい。

【０１２５】

[00130] 以上の例示の非限定的な実施態様を続けると、サービス・アカウントを引き出す要求に応答して、トークン管理プロキシー・アプリケーション１９２は、プロキシー認証情報を含む共有ディジタル証明書の受領(received)ディジタル指紋または親指の指紋に基づいて、プロキシー・アカウントを識別するように構成することができる。プロキシー認証情報は、サーバー・デバイス１９０とサーバー・デバイス１７０との間で共有される共有シークレット・ディジタル証明書にマッピングすることができ、更に、共有シークレット・ディジタル証明書はプロキシー・アカウントにマッピングされる。次いで、トークン管理プロキシー・アプリケーション１９２は、アカウント識別子またはサービス・アカウントＵＰＮの入力パラメーターと、共有シークレット・ディジタル証明書および／または識別されたプロキシー・アカウントに基づく実行ポリシーとによって、１つ以上のディレクトリー・サービス・サーバー・デバイス１３０－１から１つ以上のサービス・アカウントを引き出すように構成されたサービス・アカウント引き出しシェル・スクリプトを実行することができる。

【０１２６】

[00131] 以上の例示の非限定的な実施態様を更に続けると、サービス・アカウントのための認証トークンを更新または設定する要求に応答して、トークン管理プロキシー・アプリケーション１９２は、サービス・アカウントを引き出す要求に関して先に論じたのと同様に、プロキシー・アカウントを識別するように構成することができる。次いで、トー

クン管理プロキシー・アプリケーション１９２は、サービス・アカウント識別子の入力パラメーターと、更新または設定するためにサービス・アカウントに生成された認証トークン、ならびに共有シークレット・ディジタル証明書および／または識別されたプロキシー・アカウントに基づく実行ポリシーによって、１つ以上のディレクトリー・サービス・サーバー・デバイス１３０－１に関連付けられたまたはこれによって管理されるサーバー・アカウントの認証トークンを更新するように構成された認証トークン更新シェル・スクリプトを実行することができる。

【０１２７】

[00132] １つ以上のサービス・アカウントに関連付けられた認証トークンのセキュリティを更に確保するために、ある実施形態では、トークン管理プロキシー・アプリケーション１９２は、サービス・アカウント引き出しコンポーネント１９４および認証トークン更新コンポーネント１９６のみを含むように構成することができる。つまり、ある実施形態のある非限定的な実施態様例では、サービス・デバイス１９０のプロキシー・アカウントは、サービス・アカウント引き出しシェル・スクリプトおよび認証トークン更新シェル・スクリプトのみを実行するように構成することもできる。このように、クライアントは、サーバー・デバイス１９０および／またはトークン管理プロキシー・アプリケーション１９２上において２つの異なるアクションだけを実行できるように限定することができる。

【０１２８】

[00133] 例示として、受けたクライアント・アカウント情報が、クライアント１０２－２が「エレン・アダムス」という名前および "EllenAdams@contoso.com"というクライアント・アカウントＵＰＮを有し、４時間の要求存続期間でサーバー・デバイス１４０－１－１を遠方からデバッグするためにサービス・アカウントを以前に要求したことを示すと仮定する。加えて、サービス・アカウントを求める要求に応答して、ａｄｍｉｎ管理アプリケーション１１４は、"EllenAdams_RemoteDebugger@domainl36-l.contoso.com"というサービス・アカウントＵＰＮ、リモート・ユーザーおよびデバッガーというサービス・アカウントの役割、および違反境界１３８－１－１というサービス・アカウントの範囲を有するサービス・アカウントをプロビジョニングした。更に、以上のサービス・アカウントのために認証トークンを生成する要求に応答して、認証トークン管理コンポーネント１７６は、"Xe2&a^%5"という典型的な平文ランダム・パスワードを生成した。

【０１２９】

[00134] 以上の例示を続けると、認証トークン・プロキシー・コンポーネント１７８からのクライアント・アカウントＵＰＮ "EllenAdams@contoso.com"に関連付けられた１つ以上のサービス・アカウントを引き出す要求に応答して、サービス・アカウント引き出しコンポーネント１９４は、クライアント・アカウントＵＰＮ "EllenAdams@contoso.com"に関連付けられた１つ以上のサービス・アカウントを引き出し、サービス・アカウントＵＰＮ "EllenAdams_RemoteDebugger@domainl36-1.contoso.com"によって識別されたサービス・アカウントについてのサービス・アカウント情報を認証トークン・プロキシー・コンポーネント１７８に提供するために、ネットワーク相互接続１１２と、ディレクトリー・サービス・サーバー・デバイス１３０－ｌのディレクトリー・サービス・アプリケーション（図示せず）の１つ以上のＡＰＩとを介して通信することができる。

【０１３０】

[00135] 以上の例示を更に続けると、サービス・アカウントＵＰＮ "EllenAdams_RemoteDebugger@domainl36-1.contoso.com"によって識別されたサービス・アカウントのための認証トークンを、"Xe2&a^%5"という典型的な平文ランダム・パスワードによって更新または設定する要求に応答して、認証トークン更新コンポーネント１９６は、サービス・アカウント情報に含まれるディレクトリー・サービス情報に基づいて、ディレクトリー・サービス・サーバー・デバイス１３０－１を、以上のサービス・アカウントＵＰＮによって識別されたサービス・アカウントに関連付けられたディレクトリー・サービス・サーバー・デバイスとして、またはこのサービス・アカウントを管理するディレクトリー・サービ

ス・サーバー・デバイスとして識別することができる。一旦ディレクトリー・サービス・サーバー・デバイス１３０－ｌが識別されたら、認証トークン更新コンポーネント１９６は、以上のサービス・アカウントＵＰＮによって識別されたサービス・アカウントのための認証トークンを、"Xe2&a^%5"という典型的な平文ランダム・パスワードに更新または設定するために、ネットワーク相互接続１１２と、ディレクトリー・サービス・サーバー・デバイス１３０－ｌのディレクトリー・サービス・アプリケーション（図示せず）の１つ以上のＡＰＩとを介して通信することができる。ここで、クライアント１０２－２は、後に、サービス・アカウントＵＰＮ "EllenAdams_RemoteDebugger@domainl36-l.contoso.com"と、"Xe2&a^%5"という典型的な平文ランダム・パスワードを使用して、違反境界１３８－１－１におけるサーバー・デバイス１４０－１－１、１４０－１－２、１４０－１－３にアクセスすることができる。

【０１３１】

[00136] １つ以上のサービス・アカウントのための機械生成認証トークンの使用によって実現することができる少なくとも１つの技術的利点は、機械生成認証トークンは、人が作成するパスワードと比較すると遙かに複雑であり、従前からの暴力および何らかのソーシャル・エンジニアリングに基づく攻撃であっても、複雑な認証トークンの使用によって弱化させることができる。何故なら、これらのトークンは本来の手段および／または媒体（例えば、口頭伝達）によって正確に伝えることが難しいまたは不可能になると考えられるからである。更に、人が作成した全てのパスワードを、データーセンターにおける一部のまたは全部のサービス・アカウントに対してもランダムおよび／または一意である機械生成認証トークンと置き換えることによって、攻撃者が、例えば、共有認証トークンを使用することによって１つ以上のサービス・アカウントを漏洩させる能力は、更に弱化させることができる。１つ以上のアカウントを更に限定存続期間と関連付けることができる実施形態では、漏洩したサービス・アカウントを使用した攻撃者のアクセスは、更に限定される。何故なら、これらのサービス・アカウントは、これらがディスエーブルされる前には、限定された存続期間しか有することができないからである。このように、データーセンターにおけるＳａａＳシステムのセキュリティおよびプライバシーを大幅に改善することができる。

【０１３２】

[00137] 図１に示す認証トークン管理システム１００はある種のトポロジーではエレメント数が限定されていたが、認証トークン管理システム１００は、代わりのトポロジーでは、所与の実施態様に合わせて望まれる通りに、もっと多いまたは少ないエレメントを含むこともできることは認めることができよう。同様に、種々の実施形態は、１つ以上のクライアント・デバイス１０４－ｂ、サーバー・デバイス１０８、サーバー・デバイス１０６、サーバー・デバイス１６０、サーバー・デバイス１７０、サーバー・デバイス１３０－ｌ、および１つ以上のフォーレスト１３２－ｋを内包する企業用計算環境１５０を示すことができるが、クライアントおよび／またはサーバー・デバイスの内少なくとも一部は、所与の実施態様に合わせて、企業用計算環境１５０の外部にあってもよいことは認めることができよう。更に、種々の実施形態はデーターセンター１４２を、サーバー・デバイス１９０、サーバー・デバイス１３０－ｌ、および１つ以上のフォーレスト１３２－ｋを内包するように例示することができるが、データーセンター１４２は、更に、ある実施態様では、１つ以上のクライアント・デバイス１０４－ｂ、サーバー・デバイス１０６、サーバー・デバイス１０８、サーバー・デバイス１６０、およびサーバー・デバイス１７０も内包するのでもよいことも認めることができよう。

【０１３３】

[00138] 図２は、認証トークン管理システム１００のためのユーザー・インターフェース・ビュー２００の実施形態例を示す。１つ以上のクライアント・デバイス１０４－ｂ上で実行するクライアント・アプリケーション２０２は、１つ以上のクライアント・デバイス１０４－ｂの電子ディスプレイ上での提示に適したユーザー・インターフェース・ビュー２００を生成することができる。また、ユーザー・インターフェース・ビュー２００

は、クライアント１０２－ａ（例えば、クライアント１０２－２）が認証トークン管理システム１００と相互作用することを可能にすることもできる。クライアント・アプリケーション２０２は、ユーザー・インターフェース・ビュー２００において例示するように、クライアント・デバイス１０４－２のような１つ以上の電子デバイス上で実行するウェブ・ブラウザーに実装される単体ウェブ・アプリケーションとして実装することができる。ウェブ・ブラウザーは、限定ではなく、ＩＮＴＥＲＮＥＴ ＥＸＰＬＯＲＥＲ（登録商標）、ＭＯＺＩＬＬＲＡ（登録商標）、ＦＩＲＥＦＯＸ（登録商標）、ＳＡＦＡＲＩ（登録商標）、ＯＰＥＲＡ（登録商標）、ＮＥＴＳＣＡＰＥ ＮＡＶＩＧＡＴＯＲ（登録商標）等を含むことができる。また、ウェブ・ブラウザーは、コンピューター・プログラミング言語、規格、ウェブ・プロトコル、および／またはクライアント・アプリケーション２０２によって必要とされる技術もサポートすることができる。このようなプログラミング言語、規格、ウェブ・プロトコル、および／または技術には、ＨＴＭＬ、ＸＨＴＭＬ、ＸＭＬ、ＦＬＡＳＨ（登録商標）／ＡｃｔｉｏｎＳｃｒｉｐｔ、ＭＩＣＲＯＭＥＤＩＡ（登録商標）ＦＬＡＳＨ（登録商標）、ＪａｖａＳｃｒｉｐｔ（登録商標）、ＥＣＭＡＳｃｒｉｐｔ、ＪＳｃｒｉｐｔ、Ｂａｓｉｃ、ＶＩＳＵＡＬ ＢＡＳＩＣ（登録商標）、ＶＩＳＵＡＬ ＢＡＳＩＣ（登録商標）Ｓｃｒｉｐｔｉｎｇ Ｅｄｉｔｉｏｎ（ＶＢＳｃｒｉｐｔ）、ＣＳＳ、Ａｓｙｎｃｈｒｏｎｏｕｓ ＪａｖａＳｃｒｉｐｔおよびＸＭＬ（ＡＪＡＸ）、ＦＬＥＸ（登録商標）、ＪＡＶＡ（登録商標）、ＰＥＲＬ（登録商標）、Ｃ＃/.ｎｅｔ、および／または他の適したプログラミング、スクリプティング、またはＶＭベースの言語を含むことができるが、これらに限定されるのではない。

【０１３４】

[00139] 種々の実施態様において、ウェブ・ブラウザーは、１つ以上のグラフィカル・ユーザー・インターフェース（ＧＵＩ）コンポーネントを含むユーザー・インターフェース・ビュー２００を、認証トークン管理アプリケーション１７２によってウェブ・ブラウザーに提供された情報および実行可能コンピューター・プログラム命令に基づいて生成することができる。ウェブ・ブラウザーは、ＨＴＭＬ、ＸＨＴＭＬ、ＸＭＬ、ＡＪＡＸ、ＪＡＶＡＳＣＲＩＰＴ（登録商標）、ＦＬＡＳＨ（登録商標）、ＶＢＳｃｒｉｐｔ、および／またはユーザー・インターフェース・ビュー２００を生成するための他のスクリプト型プログラミング言語というようなコンピューター・プログラミング言語で書かれたコンピューター・プログラム命令を解釈し実行するために、スクリプト・インタプリターのような言語インタプリターを含むことができる。

【０１３５】

[00140] クライアント・デバイス１０４－２上で実行するクライアント・アプリケーション２０２のユーザー・インターフェース・ビュー２００は、ウェブ・ページ２０４を含むことができる。ウェブ・ページ２０４は、クライアント・デバイス１０４－２の認証トークン管理アプリケーション１７２へのアクセスの認証が成功したときに、クライアント１０２－２に提示することができる。ウェブ・ページ２０４は、クライアント・アカウントに関連付けられた名前（例えば、「エレン・アダムス」）およびクライアント・アカウントＵＰＮ（例えば、"EllenAdams@contoso.com"）というようなクライアント・アカウント情報、ならびにクライアント１０２－２がクライアント１０２－２に関連付けられた１つ以上のサービス・アカウントの最新のサービス・アカウント情報を要求することを可能にする更新アカウント２０６ボタンを含むことができる。

【０１３６】

[00141] また、ユーザー・インターフェース・ビュー２００は、行２１２－ｐの内１つ以上も含むことができ、各行は、サービス・アカウントを識別するためのサービス・アカウント識別子またはサービス・アカウントＵＰＮ、プロビジョニングされたサービス・アカウントの１つ以上の役割を示すサービス・アカウント役割、プロビジョニングされたサービス・アカウントの範囲を示すサービス・アカウント範囲、年数、週数、日数、時間数、分数、および／またはサービス・アカウントが失効する前に残されている秒数を示すサービス・アカウント存続期間、ならびにサービス・アカウントが未だアクティブか、ま

たは失効したかを示すサービス・アカウント・ステータスを含むことができるが、これらに限定されるのではない。

【０１３７】

[00142] また、ユーザー・インターフェース・ビュー２００は１つ以上のパスワード生成２０８－Ｏボタンも含むことができ、各パスワード生成ボタンをサービス・アカウント識別子またはサービス・アカウントＵＰＮと関連付けることができる。次いで、クライアント１０２－２は、入力デバイス（例えば、タッチ入力デバイス、マウス入力デバイス、キーボード・デバイス等）を介してジェスチャ２１０を使用して、サービス・アカウント識別子またはサービス・アカウントＵＰＮによって識別されたサービス・アカウントのために平文ランダム・パスワードを生成することを要求するために、パスワード生成ボタンを選択することができる。サービス・アカウントおよび／または認証トークンのセキュリティを確保するために、クライアント・アプリケーション２０２は、サービス・アカウント・ステータスが失効となっているサービス・アカウントに対しては、パスワード生成ボタン（例えば、パスワード生成ボタン２０８－２）をディスエーブルするように構成するとよいことは認めることができよう。加えてまたは代わりに、クライアント・アプリケーション２０２は、更に、生成された平文ランダム・パスワードを失ったまたは忘れたかもしれないクライアントが新たな平文ランダム・パスワードを生成することを禁止できるように、平文ランダム・パスワードが、サービス・アカウント・ステータスがアクティブになっているサービス・アカウントのために既に生成された後では、サービス・アカウントのためのパスワード生成ボタンをディスエーブルするように構成することもできる。

【０１３８】

[00143] 本明細書に含まれるのは、開示したアーキテクチャの新規な態様を実行する方法の具体例を表す１組のフロー・チャートである。説明を簡略化する目的のために、ここでは、例えば、フロー・チャートまたは流れ図の形態で示される１つ以上の方法を、一連のアクトとして示し説明するが、これらの方法論は、アクトの順序によって限定されないことは理解されそして認められよう。何故なら、本開示によれば、一部のアクトは、ここで示し説明する順序とは異なる順序で現れること、および／または他のアクトと同時に行われることも可能であるからである。例えば、方法は、代わりに、状態図におけるように、相互に関係付けられた一連の状態またはイベントとして表すことも可能であることは、当業者には理解されそして認められよう。更に、方法に例示される全てのアクトが、新規な実施態様には必要ではない場合もある。

【０１３９】

[00144] 図３Ａは、論理フロー３００の一実施形態を示す。論理フロー３００は、本明細書において説明した１つ以上の実施形態によって実行される動作の一部または全部を表すことができる。

【０１４０】

[00145] 図３Ａに示す例示用の実施形態(illustrated embodiment)では、論理フロー３００はブロック３０２において開始することができ、ブロック３０４において、少なくとも部分的にクライアント認証情報に基づいて、クライアント・デバイスとの安全な接続を確立することができる。例えば、信頼接続を確立するために、ディジタル・スマート・カード証明書および関連するＰＩＮを含むスマート・カードを使用して、クライアント１０２－２がクライアント・デバイス１０４－２に認証した後、認証トークン管理コンポーネント１７４が、信頼できるフェデレーテット・アイデンティティ・アプリケーション１６２によって発行され受けたセキュリティ・トークンに基づいて、クライアント１０２－２を認証することができる。更に、認証トークン管理コンポーネント１７４は、１つ以上のセキュア通信プロトコル（例えば、ＨＴＴＰＳ）を利用して、クライアント・デバイス１０４－２との安全な接続（即ち、信頼および暗号化接続）を確立することもできる。

【０１４１】

[00146] 論理フロー３００は、ブロック３０６において、クライアント・デバイスからのサービス・アカウントのアカウント情報を求める要求を受けることができる。例えば

、認証トークン管理コンポーネント１７４は、クライアント１０２－２からクライアント・デバイス１０４－２を通じて、クライアント１０２－２のクライアント・アカウントに関連付けられた１つ以上のサービス・アカウントを求める要求を受けることができる。

【０１４２】

[00147] 論理フロー３００は、ブロック３０８において、少なくとも部分的にクライアント認証情報に基づいて、サービス・アカウントのアカウント情報を要求することができる。例えば、クライアント・デバイス１０４－２から、クライアント１０２－２のクライアント・アカウントに関連付けられた１つ以上のサービス・アカウントを求める要求を受けたことに応答して、認証トークン管理コンポーネント１７４は、認証トークン・プロキシー・コンポーネント１７８を介して、トークン管理プロキシー・アプリケーション１９２に、クライアント１０２－２のクライアント・アカウントに関連付けられた１つ以上のサービス・アカウントのサービス・アカウント情報を要求することができる。

【０１４３】

[00148] 論理フロー３００は、ブロック３１０において、サービス・アカウントについてのアカウント情報を受けることができる。例えば、認証トークン管理コンポーネント１７４は、１つ以上のアカウントのサービス・アカウント情報を求める要求に応答して、クライアント１０２－２のクライアント・アカウントに関連付けられた１つ以上のサービス・アカウントのサービス・アカウント情報を、認証トークン・プロキシー・コンポーネント１７８を介して受けることができる。

【０１４４】

[00149] 論理フロー３００は、ブロック３１２において、サービス・アカウントについてのアカウント情報をクライアント・デバイスに提供し、ブロック３１４において終了する。例えば、認証トークン管理コンポーネント１７４は、トークン管理プロキシー・アプリケーション１９２からサービス・アカウント情報を受けたことに応答して、クライアント１０２－２のクライアント・アカウントに関連付けられた１つ以上のサービス・アカウントの受けたサービス・アカウント情報を提供することができる。実施形態はこれらの例に限定されるのではない。

【０１４５】

[00150] 図３Ｂは、論理フロー３２０の一実施形態を示す。論理フロー３２０は、本明細書において説明した１つ以上の実施形態によって実行される動作の一部または全部を表すことができる。

【０１４６】

[00151] 図３Ｂに示す例示用の実施形態では、論理フロー３２０はブロック３２２において開始することができ、ブロック３２４において、サービス・アカウントのために認証トークンを生成する要求を、クライアント・デバイスから受けることができる。例えば、認証トークン管理コンポーネント１７４は、クライアント１０２－２のクライアント・アカウントに関連付けられたサービス・アカウントのために認証トークンを生成する要求を、クライアント・デバイス１０４－２から受けることができる。

【０１４７】

[00152] 論理フロー３２０は、ブロック３２６において、サービス・アカウントのために認証トークンを生成するために、クライアント・デバイスから受けた要求の有効性を判断することができる。例えば、認証トークン管理コンポーネント１７４は、受けたセキュリティ・トークンが信頼ＳＴＳプロバイダー、例えば、フェデレーテット・アイデンティティ・アプリケーション１６２によって発行されたこと、そして認証トークンを生成することを要求しているクライアント１０２－２が、二要素認証（例えば、スマート・カードおよび関連するＰＩＮ）に基づいて認証されたことを検証することによって、クライアント・デバイスから受けた、サービス・アカウントのために認証トークンを生成する要求の有効性を判断することができる。

【０１４８】

[00153] 論理フロー３２０は、ブロック３２８において、サービス・アカウントのた

めに認証トークンを生成することができる。例えば、認証トークン生成コンポーネント１７６は、長さパラメーターおよびキャラクター・クラス・パラメーターに基づいて平文ランダム・パスワードを生成することができる。

【０１４９】

[00154] 論理フロー３２０は、ブロック３３０において、サービス・アカウント情報、認証トークン、およびプロキシー認証情報の一部を認証トークン管理プロキシー・アプリケーションに提供することができる。例えば、認証トークン生成コンポーネント１７６は、サービス・アカウント情報によって識別されるサービス・アカウントのために生成された認証トークンを更新または設定するために、認証プロキシー・コンポーネント１７８を介して、サービス・アカウント情報（例えば、サービス・アカウント識別子またはサービス・アカウントＵＰＮ）、生成した認証トークン、および共有シークレット・ディジタル証明書のディジタル指紋または親指の指紋を、トークン管理プロキシー・アプリケーション１９２に供給することができる。

【０１５０】

[00155] 論理フロー３２０は、ブロック３３２において、少なくとも認証トークンをクライアント・デバイスに供給し、ブロック３３４において終了することができる。例えば、認証トークン通知コンポーネント１８０は、認証トークン・データーストア１６６への格納のために、少なくとも生成された認証トークンを隠れたｄｉｖにおいてクライアント１０２－２に、クライアント・デバイス１０４－２を通じて通知または供給することができる。実施形態はこれらの例に限定されるのではない。

【０１５１】

[00156] 図３Ｃは、論理フロー３４０の一実施形態を示す。論理フロー３４０は、本明細書において説明した１つ以上の実施形態によって実行される動作の一部または全部を表すことができる。

【０１５２】

[00157] 図３Ｃに示す例示用の実施形態では、論理フロー３４０はブロック３４２において開始することができ、ブロック３４４において、少なくとも部分的にクライアント・アカウント情報に基づいて、サービス・アカウントのアカウント情報を求める要求を受けることができる。例えば、サービス・アカウント引き出しコンポーネント１９４は、クライアント・アカウント情報に含まれるクライアント・アカウント識別子またはサービス・アカウントＵＰＮによって識別されるクライアント・アカウントに関連付けられた１つ以上のサービス・アカウントのサービス・アカウント情報を求める要求を受けることができる。この要求は、クライアント・アカウント情報と、プロキシー認証情報の一部とを含むことができる。

【０１５３】

[00158] 論理フロー３４０は、ブロック３４６において、少なくとも部分的にクライアント・アカウント情報に基づいて、サービス・アカウントのアカウント情報をディレクトリー・サービス・サーバー・デバイスから引き出すことができる。例えば、サービス・アカウント引き出しコンポーネント１９４は、クライアント・アカウント情報に含まれるクライアント・アカウント識別子またはサービス・アカウントＵＰＮによって識別されるクライアント・アカウントに関連付けられたサービス・アカウント情報を引き出すために、データーセンター１４２における１つ以上のネットワークおよび／またはネットワーク相互接続１１２、ならびに１つ以上のディレクトリー・サービス・サーバー・デバイス１３０－１のディレクトリー・サービス・アプリケーションの１つ以上のＡＰＩを介して通信することができる。

【０１５４】

[00159] 論理フロー３４０は、ブロック３４８において、サービス・アカウントのアカウント情報を認証トークン管理アプリケーションに提供することができる。例えば、サービス・アカウント引き出しコンポーネント１９４は、クライアント・アカウント情報に含まれるクライアント・アカウント識別子またはサービス・アカウントＵＰＮによって識

別されたクライアント１０２－２のクライアント・アカウントに関連付けられた１つ以上のサービス・アカウントの引き出したサービス・アカウント情報を提供することができる。

【０１５５】

[00160] 論理フロー３４０は、ブロック３５０において、サービス・アカウントのための認証トークンを更新または設定する要求を、認証トークン管理アプリケーションから受けることができる。例えば、認証トークン更新コンポーネント１９６は、認証トークン・プロキシー・コンポーネント１７８から、サービス・アカウントのための認証トークンを更新または設定する要求を受けることができる。この要求は、サービス・アカウント情報、認証トークン、およびプロキシー認証情報の一部を含むことができる。

【０１５６】

[00161] 論理フロー３４０は、ブロック３５２において、ディレクトリー・サービス・サーバー・デバイスによって管理されているサービス・アカウントのための認証トークンを更新または設定し、ブロック３５４において終了することができる。例えば、認証トークン更新コンポーネント１９６は、サービス・アカウント情報に含まれるサービス・アカウント識別子またはサービス・アカウントＵＰＮによって識別されたサービス・アカウントのために受けた認証トークンによって、認証トークンを更新または設定することができる。実施形態はこれらの例に限定されるのではない。

【０１５７】

[00162] 図３Ｄは、論理フロー３６０の一実施形態を示す。論理フロー３６０は、本明細書において説明した１つ以上の実施形態によって実行される動作の一部または全部を表すことができる。

【０１５８】

[00163] 図３Ｄに示す例示用の実施形態において、論理フロー３６０はブロック３６２において開始することができ、ブロック３６４において、少なくとも部分的にクライアント認証情報に基づいて、認証トークン管理アプリケーションとの安全な接続を確立することができる。例えば、クライアント・デバイス１０４－２はセキュリティ・トークンを認証トークン管理コンポーネント１７４に供給することができ、クライアント１０２－２が、信頼接続を確立するために、ディジタル・スマート・カード証明書および関連するＰＩＮを含むスマート・カードを使用してクライアント・デバイス１０４－２に認証した後に、認証トークン管理コンポーネント１７４は、信頼フェデレーテット・アイデンティティ・アプリケーション１６２によって発行されたセキュリティ・トークンに基づいて、クライアント１０２－２を認証することができる。また、クライアント・デバイス１０４－２は１つ以上のセキュア通信プロトコル（例えば、ＨＴＴＰＳ）を利用して、認証トークン管理アプリケーション１７２との安全な接続（即ち、信頼および暗号化接続）を確立することもできる。

【０１５９】

[00164] 論理フロー３６０は、ブロック３６６において、サービス・アカウントのアカウント情報を要求することができる。例えば、クライアント・デバイス１０４－２は、クライアント・アカウント情報に含まれるクライアント・アカウント識別子またはクライアント・アカウントＵＰＮによって識別されるクライアント・アカウントを有するクライアント１０２－２に関連付けられた１つ以上のサービス・アカウントについてのサービス・アカウント情報を要求することができる。

【０１６０】

[00165] 論理フロー３６０は、ブロック３６８において、サービス・アカウントのアカウント情報を認証トークン管理アプリケーションから受けることができる。例えば、クライアント１０２－２は、サービス・アカウント情報を求める要求に応答して、クライアント・デバイス１０４－２を通じて、クライアント１０２－２のクライアント・アカウントに関連付けられた１つ以上のサービス・アカウントについてのサービス・アカウント情報を受けることができる。

【０１６１】
[00166] 論理フロー３６０は、ブロック３７０において、サービス・アカウントのために認証トークンを生成することを要求することができる。例えば、クライアント・デバイス１０４－２は、サービス・アカウント情報に含まれるサービス・アカウント識別子またはサービス・アカウントＵＰＮによって識別されるサービス・アカウントのために平文ランダム・パスワードを生成することを要求することができる。
【０１６２】
[00167] 論理フロー３６０は、ブロック３７２において、少なくとも生成された認証トークンを認証トークン管理アプリケーションから受けることができる。例えば、クライアント・デバイス１０４－２は、少なくともサービス・アカウントのために生成された認証トークンを、ウェブ・ページにおける隠されたエレメントとして受けることができる。加えて、クライアント・デバイス１０４－２はサービス・アカウント識別子またはサービス・アカウントＵＰＮを同じウェブ・ページ上で受けることもできる。
【０１６３】
[00168] 論理フロー３６０は、ブロック３７４において、少なくとも認証トークンを認証トークン・データーストアに格納することができる。例えば、クライアント１０２－２は、クライアント・デバイス１０４－２を通じて、サービス・アカウントのために受けた認証トークンを認証トークン・データーストア１６６に格納することができる。典型的な認証トークン・データーストア１６６は、パスワード・セーフを含むことができるが、これに限定されるのではない。加えて、クライアント１０２－２は、クライアント・デバイス１０４－２を通じて、受けた認証トークンに関連付けられたサービス・アカウント識別子またはサービス・アカウントＵＰＮも認証トークン・データーストア１６６に格納することができる。
【０１６４】
[00169] 論理フロー３６０は、ブロック３７６において、少なくとも認証トークンを認証トークン・データーストアから引き出すことができる。例えば、クライアント１０２－２は、クライアント・デバイス１０４－２を通じて、少なくとも格納されている認証トークンを認証トークン・データーストア１６６から引き出すことができる。加えて、クライアント１０２－２は、クライアント・デバイス１０４－２を通じて、受けた認証トークンに関連付けられたサービス・アカウント識別子またはサービス・アカウントＵＰＮも、認証トークン・データーストア１６６から引き出すことができる。
【０１６５】
[00170] 論理フロー３６０は、ブロック３７８において、少なくとも認証トークンを使用してサーバー・デバイスにアクセスし、ブロック３８０において終了することができる。例えば、クライアント１０２－２は、次いで、引き出した認証トークンおよびサービス・アカウントＵＰＮを使用して、クライアント・デバイス１０４－２を通じて、例えば、リモート・デスクトップ・プロトコルを使用してサーバー・デバイス１４０－１－１にアクセスすることができる。実施形態はこれらの例に限定されるのではない。
【０１６６】
[00171] 図４は、既に説明した種々の実施形態を実現するのに適した例示用の計算アーキテクチャ４００の実施形態を示す。一実施形態では、計算アーキテクチャ４００は、クライアント・デバイスおよび／またはサーバー・デバイスの一部を含んでもよく、またはその一部として実装されてもよい。実施形態はこの文脈において限定されることはない。
【０１６７】
[00172] 本願において使用する場合、「システム」および「コンポーネント」という用語は、ハードウェア、ハードウェアおよびソフトウェアの組み合わせ、ソフトウェア、または実行中のソフトウェアのいずれかのコンピューター関連エンティティを指すことを意図しており、その例は具体例としての計算アーキテクチャ４００によって示される。例えば、コンポーネントは、プロセッサー上で実行するプロセス、プロセッサー、ハード・

ディスク・ドライブ、多数の記憶デバイス（光および／または磁気記憶媒体の）、オブジェクト、実行可能ファイル、実行のスレッド、プログラム、および／またはコンピューターであることが可能であるが、これらに限定されるのではない。例示として、サーバー上で実行するアプリケーションおよびサーバーの双方がコンポーネントであることが可能である。１つ以上のコンポーネントがプロセスおよび／または実行のスレッド内に常駐する(reside)ことができ、コンポーネントが１つのコンピューター上に集中配置される(localize)こと、および／または２つ以上のコンピューター間で分散されることが可能である。更に、コンポーネントは、動作を調整するために、種々のタイプの通信媒体によって互いに通信可能に結合することができる。調整には、一方向または双方向の情報交換を必要とする場合もある。例えば、コンポーネントは、通信媒体上で伝達される信号の形態で、情報を伝達することができる。情報は、種々の信号線に割り当てられる信号として実現することができる。このような割り当てでは、各メッセージが信号となる。しかしながら、他の実施形態では、代わりにデーター・メッセージを採用することもできる。このようなデーター・メッセージは、種々の接続を通して送ることができる。接続の具体例には、パラレル・インターフェース、シリアル・インターフェース、およびバス・インターフェースが含まれる。

【０１６８】

[00173] 計算アーキテクチャ４００は、１つ以上のプロセッサー、マルチコア・プロセッサー、コプロセッサー、メモリー・ユニット、チップセット、コントローラー、周辺素子、インターフェース、発振器、タイミング・デバイス、ビデオ・カード、オーディオ・カード、マルチメディア入力／出力（Ｉ／Ｏ）コンポーネント、電源等のような、種々の共通する計算エレメントを含む。しかしながら、実施形態は計算アーキテクチャ４００による実現に限定されるのではない。

【０１６９】

[00174] 図４に示すように、計算アーキテクチャ４００は、処理ユニット４０４、システム・メモリー４０６、およびシステム・バス４０８を含む。処理ユニット４０４は、種々の市販のプロセッサーの内任意のものとすることができ、限定ではなく、ＡＭＤ（登録商標）Ａｔｈｌｏｎ（登録商標）、Ｄｕｒｏｎ（登録商標）およびＯｐｔｅｒｏｎ（登録商標）プロセッサー、ＡＲＭ（登録商標）アプリケーション、埋め込みおよびセキュア・プロセッサー、ＩＢＭ（登録商標）およびＭｏｔｏｒｏｌａ（登録商標）ＤｒａｇｏｎＢａｌｌ（登録商標）、およびＰｏｗｅｒＰＣ（登録商標）プロセッサー、ＩＢＭおよびＳｏｎｙ（登録商標）Ｃｅｌｌプロセッサー、Ｉｎｔｅｌ（登録商標）Ｃｅｌｅｒｏｎ（登録商標）、Ｃｏｒｅ（２）Ｄｕｏ（登録商標）、Ｉｔａｎｉｕｍ（登録商標）、Ｐｅｎｔｉｕｍ（登録商標）、Ｘｅｏｎ（登録商標）、およびＸＳｃａｌｅ（登録商標）プロセッサー、ならびに同様のプロセッサーを含む。デュアル・マイクロプロセッサー、マルチコア・プロセッサー、および他のマルチプロセッサー・アーキテクチャも、処理ユニット４０４として採用することができる。

【０１７０】

[00175] システム・バス４０８は、システム・メモリー４０６から処理ユニット４０４までを含むがこれらに限定されないシステム・コンポーネントのためにインターフェースを設ける。システム・バス４０８は、種々のタイプのバス構造の内任意のものにすることができ、更に、メモリー・バス（メモリー・コントローラー付きまたはメモリー・コントローラーなし）、周辺バス、およびローカル・バスに、種々の市販のバス・アーキテクチャの内任意のものを使用して相互接続することができる。インターフェース・アダプターがシステム・バス４０８に、スロット・アーキテクチャを介して接続することもできる。スロット・アーキテクチャの例には、限定ではなく、加速グラフィクス・ポート（ＡＧＰ）、カード・バス、（拡張）業界標準アーキテクチャ（（Ｅ）ＩＳＡ）、マイクロ・チャネル・アーキテクチャ（ＭＣＡ）、ＮｕＢｕｓ、周辺素子相互接続（拡張）（ＰＣＩ（Ｘ））、ＰＣＩＥｘｐｒｅｓｓ、パーソナル・コンピューター・メモリー・カード国際連合（ＰＣＭＣＩＡ）等を含むことができる。

【０１７１】
[00176] 計算アーキテクチャ４００は、種々の製品(articles of manufacture)を含むまたは実装することができる。製品は、ロジックを格納するためのコンピューター読み取り可能記憶媒体を含むこともできる。コンピューター読み取り可能記憶媒体の例には、電子データーを格納することができるあらゆる有形媒体を含むことができ、揮発性メモリーまたは不揮発性メモリー、リムーバブルまたは非リムーバブル・メモリー、消去可能または消去不可メモリー、書き込み可能または再書き込み可能メモリー等を含むことができる。ロジックの例には、ソース・コード、コンパイル・コード(compiled code)、インタプリター・コード(interpreted code)、実行可能コード、スタティック・コード、ダイナミック・コード、オブジェクト指向コード、ビジュアル・コード等というような、任意の適したタイプのコードを使用して実装される実行可能コンピューター・プログラム命令を含むことができる。また、実施形態は、少なくとも部分的に、一時的ではないコンピューター読み取り可能媒体内またはその上に収容される命令として実現することもでき、本明細書において説明した動作の実行を可能にするために、１つ以上のプロセッサーによって読み取り実行することができる。
【０１７２】
[00177] システム・メモリー４０６は、リード・オンリー・メモリー（ＲＯＭ）、ランダム・アクセス・メモリー（ＲＡＭ）、ダイナミックＲＡＭ（ＤＲＡＭ）、データー倍速ＤＲＡＭ（ＤＤＲＡＭ）、同期ＤＲＡＭ（ＳＤＲＡＭ）、スタティックＲＡＭ（ＳＲＡＭ）、プログラマブルＲＯＭ（ＰＲＯＭ）、消去可能プログラマブルＲＯＭ（ＥＰＲＯＭ）、電気的消去可能プログラマブルＲＯＭ（ＥＥＰＲＯＭ）、フラッシュ・メモリー、強磁性ポリマー・メモリーのようなポリマー・メモリー、オボニック・メモリー、位相変化または強磁性メモリー、シリコン－酸化物－窒化物－酸化物－シリコン（ＳＯＮＯＳ）メモリー、磁気または光カード、独立ディスクの冗長アレイ（ＲＡＩＤ）ドライブのようなデバイスのアレイ、ソリッド・ステート・メモリー・デバイス（例えば、ＵＳＢメモリー、ソリッド・ステート・ドライブ（ＳＳＤ）、およびは情報を格納するのに適した他のあらゆるタイプの記憶媒体というような、１つ以上の高速メモリー・ユニットの形態とした種々のタイプのコンピューター読み取り可能記憶媒体を含むことができる。図４に示す例示の実施形態では、システム・メモリー４０６は不揮発性メモリー４１０および／または揮発性メモリー４１２を含むことができる。基本入力／出力システム（ＢＩＯＳ）は、不揮発性メモリー４１０に格納することができる。
【０１７３】
[00178] コンピューター４０２は、１つ以上の低速メモリー・ユニットの形態とした種々のタイプのコンピューター読み取り可能記憶媒体を含むことができ、内部（または外部）ハード・ディスク・ドライブ（ＨＤＤ）４１４、リムーバブル磁気ディスク４１８に対して読み取りまたは書き込みを行うための磁気フロッピー・ディスク・ドライブ（ＦＤＤ）４１６、ならびにリムーバブル光ディスク４２２（例えば、ＣＤ－ＲＯＭまたはＤＶＤ）に対する読み取りまたは書き込みを行うための光ディスク・ドライブ４２０を含む。ＨＤＤ４１４、ＦＤＤ４１６、および光ディスク・ドライブ４２０は、それぞれ、ＨＤＤインターフェース４２４、ＦＤＤインターフェース４２６、および光ドライブ・インターフェース４２８によって、システム・バス４０８に接続することができる。外部ドライブ実装用のＨＤＤインターフェース４２４は、ユニバーサル・シリアル・バス（ＵＳＢ）およびＩＥＥＥ１３９４インターフェース技術の少なくとも一方または両方を含むことができる。
【０１７４】
[00179] ドライブおよび付随するコンピューター読み取り可能媒体は、データー、データー構造、コンピューター実行可能命令等の揮発性および／または不揮発性ストレージを提供する。例えば、多数のプログラム・モジュールをドライブおよびメモリー・ユニット４１０、４１２に格納することができ、これらのプログラム・モジュールは、オペレーティング・システム４３０、１つ以上のアプリケーション・プログラム４３２、他のプロ

グラム・モジュール４３４、およびプログラム・データー４３６を含む。一実施形態では、１つ以上のアプリケーション・プログラム４３２、他のプログラム・モジュール４３４、およびプログラム・データー４３６は、例えば、システム１００の種々のアプリケーションおよび／またはコンポーネントを含むことができる。

【０１７５】

[00180] ユーザーは、１つ以上の有線／ワイヤレス入力デバイス、例えば、キーボード４３８およびマウス４４０のようなポインティング・デバイスによって、コマンドおよび情報をコンピューター４０２に入力することができる。他の入力デバイスは、マイクロフォン、赤外線（ＩＲ）遠隔制御手段、無線周波数（ＲＦ）遠隔制御手段、ゲーム・パッド、スタイラス・ペン、カード・リーダー、ドングル、指紋読み取り装置、グローブ、グラフィクス・タブレット、ジョイスティック、キーボード、網膜読み取り装置、タッチ・スクリーン（例えば、容量式、抵抗式等）、トラックボール、トラックパッド、センサ、スタイラス等を含むことができる。これらおよびその他の入力デバイスは、多くの場合、入力デバイス・インターフェース４４２を介して処理ユニット４０４に接続され、入力デバイス・インターフェース４４２はシステム・バス４０８に結合されるが、パラレル・ポート、ＩＥＥＥ１３９４シリアル・ポート、ゲーム・ポート、ＵＳＢポート、ＩＲインターフェース等というような、他のインターフェースによって接続することもできる。

【０１７６】

[00181] モニター４４４または他のタイプのディスプレイ・デバイスも、ビデオ・アダプター４４６のようなインターフェースを介して、システム・バス４０８に接続される。モニター４４４は、コンピューター４０２に対して内部でもまたは外部でもよい。モニター４４４に加えて、コンピューターは、通例、スピーカー、プリンター等のような、他の周辺出力デバイスを含む。

【０１７７】

[00182] コンピューター４０２は、論理接続を使用して、ネットワーク接続環境において、リモート・コンピューター４４８のような１つ以上のリモート・コンピューターへの有線通信および／またはワイヤレス通信によって動作することもできる。リモート・コンピューター４４８は、ワークステーション、サーバー・コンピューター、ルーター、パーソナル・コンピューター、携帯用コンピューター、マイクロプロセッサー・ベースの娯楽アプライアンス、ピア・デバイスまたは他の共通ネットワーク・ノードとすることができ、通例、コンピューター４０２に関して説明したエレメントの多くまたは全部を含むが、簡潔さの目的のために、メモリー／記憶デバイス４５０だけが示される。図示する論理接続は、ローカル・エリア・ネットワーク（ＬＡＮ）４５２、および／またはそれよりも大きなネットワーク、例えば、ワイド・エリア・ネットワーク（ＷＡＮ）４５４に対する有線／ワイヤレス接続(connectivity)を含む。このようなＬＡＮおよびＷＡＮネットワーキング環境は、事務所や会社では極一般的であり、イントラネットのような企業規模のコンピューター・ネットワークを容易にする。イントラネットの全ては、グローバル通信ネットワーク、例えば、インターネットに接続することもできる。

【０１７８】

[00183] ＬＡＮネットワーキング環境において使用される場合、コンピューター４０２は有線および／またはワイヤレス通信ネットワーク・インターフェースあるいはアダプター４５６を介して、ＬＡＮ４５２に接続される。アダプター４５６は、ＬＡＮ４５２に対する有線通信および／またはワイヤレス通信を容易にすることができ、アダプター４５６のワイヤレス機能性と通信するために配置されるワイヤレス・アクセス・ポイントも含むことができる。

【０１７９】

[00184] ＷＡＮネットワーキング環境において使用される場合、コンピューター４０２はモデム４５８を含むことができ、あるいはＷＡＮ４５４上の通信サーバーに接続されるか、またはインターネットによってというように、ＷＡＮ４５４上に通信を確立する他の手段を有する。モデム４５８は、内蔵型または外付け型の有線デバイスおよび／または

ワイヤレス・デバイスとすることができ、入力デバイス・インターフェース４４２を介してシステム・バス４０８に接続する。ネットワーク接続環境では、コンピューター４０２に関して図示したプログラム・モジュール、またはその一部をリモート・メモリー／記憶デバイス４５０に格納することができる。尚、図示するネットワーク接続は例示であり、コンピューター間に通信リンクを確立する他の手段を使用することもできることは認められよう。

【０１８０】

[00185] コンピューター４０２は、ワイヤレス通信（例えば、ＩＥＥＥ８０２．１１オーバー・ジ・エア変調技法）において動作的に配置されるワイヤレス・デバイスのような、標準のＩＥＥＥ８０２ファミリーを使用して、有線およびワイヤレス・デバイスまたはエンティティと通信するように動作可能である。これは、少なくとも、Ｗｉ－Ｆｉ（即ち、ワイヤレス・フィデリティ）、ＷｉＭａｘ、およびBluetooth（登録商標）ワイヤレス技術をとりわけ含む。このように、通信は、従来のネットワークのような、予め定められた構造であること、または単に少なくとも２つのデバイス間におけるアド・ホック通信であることができる。Ｗｉ－Ｆｉネットワークは、安全で、信頼性が高く、高速なワイヤレス接続性を提供するために、ＩＥＥＥ８０２．１１ｘ（ａ、ｂ、ｇ、ｎ等）と呼ばれる無線技術を使用する。Ｗｉ－Ｆｉネットワークは、コンピューターを互いに接続するため、インターネットに接続するため、そして有線ネットワーク（ＩＥＥＥ８０２．３関連媒体および機能を使用する）に接続するために使用することができる。

【０１８１】

[00186] 実施形態には、「一実施形態」(one embodiment)または「実施形態」(an embodiment)という表現をその派生語と共に使用して説明するとよいものがある。これらの用語は、当該実施形態と関連付けて説明された特定の特徴、構造、または特性が、少なくとも１つの実施形態に含まれることを意味する。本明細書の種々の場所において「一実施形態では」という句が出てくる場合、必ずしも全てが同じ実施形態を指す訳ではない。更に、実施形態は、「結合される」(coupled)および「接続される」(connected)という表現を、その派生語と共に使用して説明することもできる。これらの用語は、必ずしも互いに対する同義語であることを意図しているのではない。例えば、実施形態の中には、２つ以上のエレメントが直接物理的にまたは電気的に互いに接触していることを示すために、「接続される」および／または「結合される」という用語を使用して説明するとよい場合がある。しかしながら、「結合される」という用語は、２つ以上のエレメントが互いに直接接触していないが、それでも互いに協働するまたは相互作用することを意味することもできる。

【０１８２】

[00187] 尚、開示の要約は、読者が本技術的開示の固有性を素早く確認することを可能にするために設けられることを強調しておく。尚、これは、請求項の範囲または意味を解釈するためや限定するために使用されるのではないことを理解した上で申し述べられることである。加えて、以上の詳細な説明では、開示を簡素化する目的に限って、１つの実施形態において種々の特徴が一緒に纏められていることがわかるであろう。この開示方法は、特許請求する実施形態が各請求項において明示的に記載されるよりも多くの特徴を必要とするという意図を表す(reflect)というように解釈してはならない。逆に、以下の特許請求の範囲が表すように、発明の主題は、１つの開示された実施形態の全ての特徴に存在する訳ではない。つまり、以下の特許請求の範囲は詳細な説明に含まれ、各請求項が別個の実施形態としてそれ自体を成り立たせている(stand on its own)。添付した特許請求の範囲において、「含む」(including)および「において」(in which)という用語は、それぞれ、「含む」(comprising)および「において」(wherein)というそれぞれの用語の平素な英語の同等語(equivalent)として使用されるものとする。更に、「第１」、「第２」、「第３」等の用語は、単に名称として使用されるのであり、それらの目的語に対して数値的な要件を強制することは意図していない。

【０１８３】

[00188] 以上で説明したことは、開示されたアーキテクチャの例を含む。勿論、コンポーネントおよび／または方法の着想可能なあらゆる組み合わせを記載することは不可能であるが、多くの他の組み合わせや置換(permutations)も可能であることは、当業者には認めることができよう。したがって、新規なアーキテクチャは、添付した請求項の主旨および範囲に該当するような全ての改変、変更、および変形を包含することを意図している。

【図１】

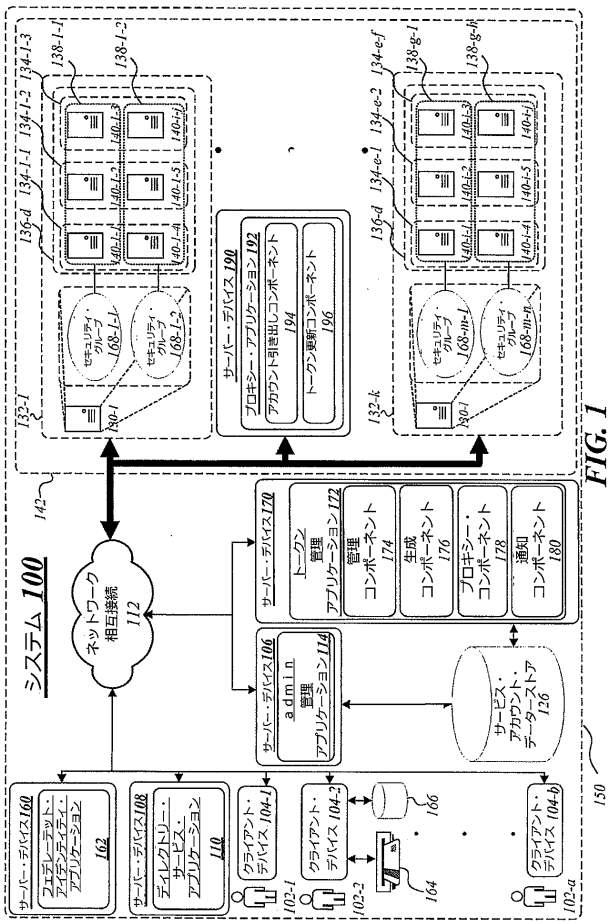

FIG. 1

【図２】

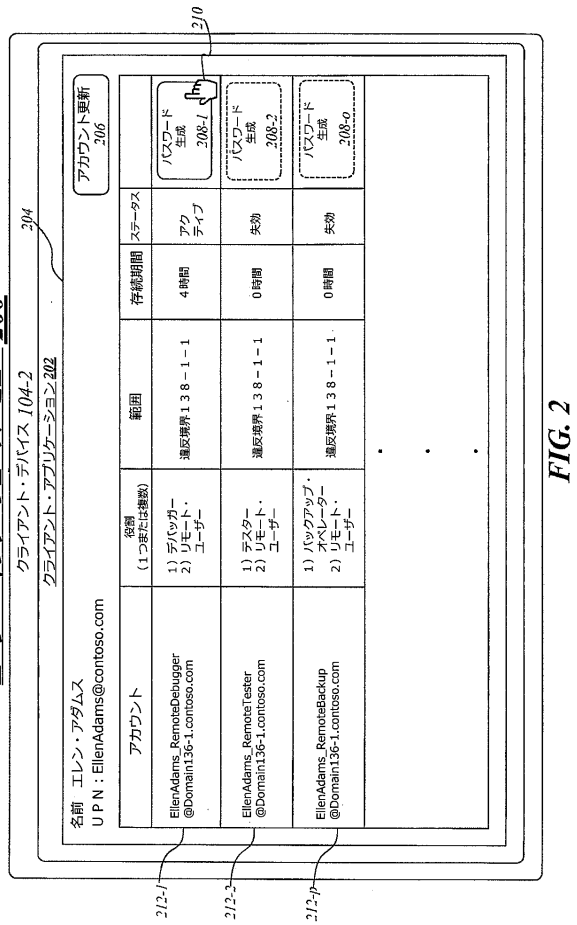

FIG. 2

【図３Ａ】

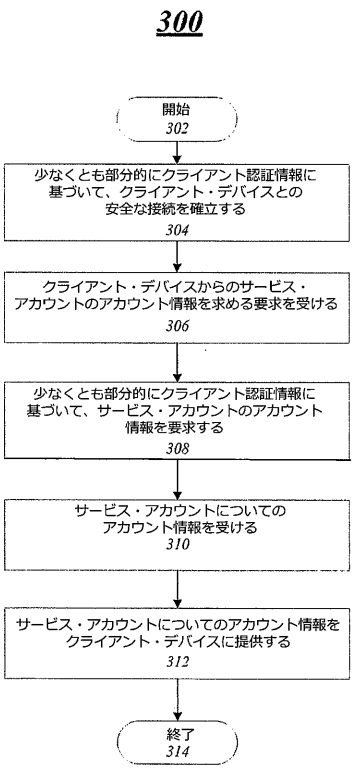

FIG. 3A

【図３Ｂ】

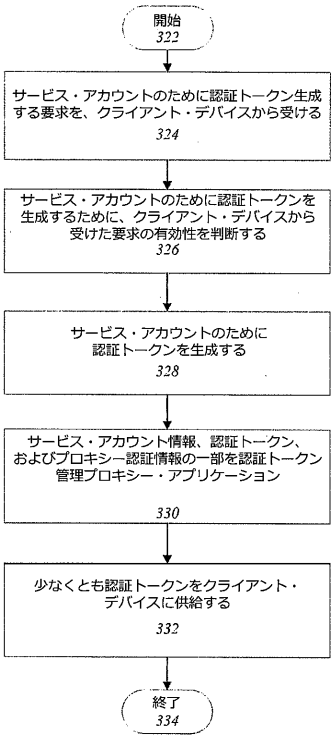

FIG. 3B

【図３Ｃ】

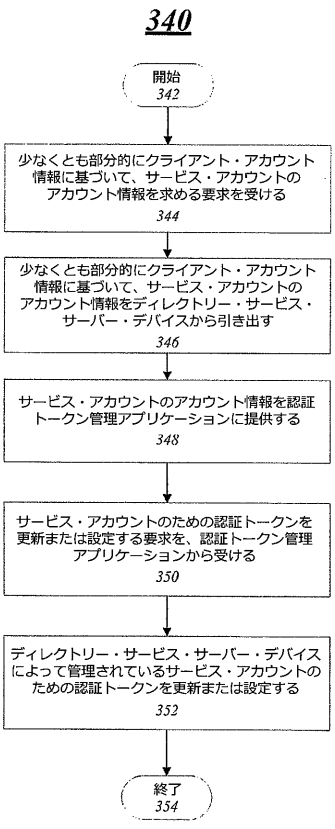

FIG. 3C

【図３Ｄ】

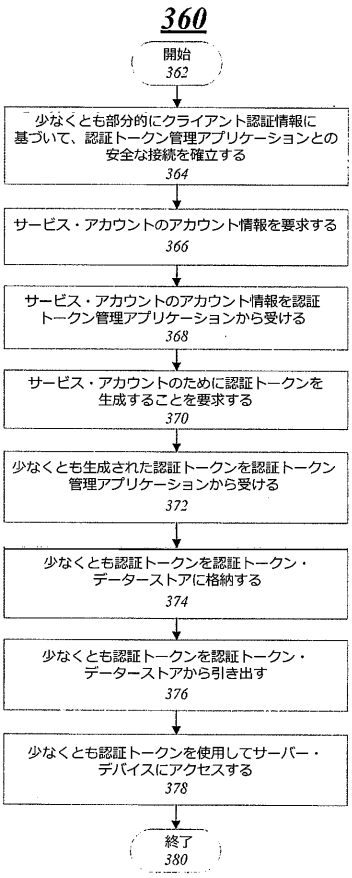

FIG. 3D

【図４】

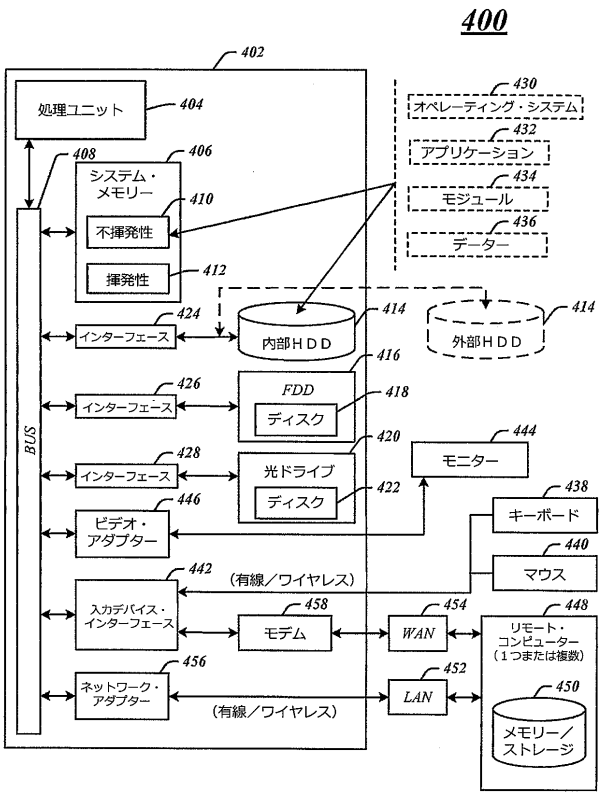
400
402
処理ユニット
404
408
406
システム・
メモリー
410
不揮発性
412
揮発性
BUS
430
オペレーティング・システム
432
アプリケーション
434
モジュール
436
データー
414
内部ＨＤＤ
414
外部ＨＤＤ
424
インターフェース
416
FDD
426
インターフェース
418
ディスク
420
光ドライブ
428
インターフェース
422
ディスク
444
モニター
438
キーボード
446
ビデオ・
アダプター
440
マウス
442
（有線／ワイヤレス）
入力デバイス・
インターフェース
458
モデム
454
WAN
448
リモート・
コンピューター
（１つまたは複数）
456
ネットワーク・
アダプター
452
LAN
450
（有線／ワイヤレス）
メモリー／
ストレージ

FIG. 4

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2015/021919

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06 H04L9/08 H04L9/32 H04W12/04
ADD.

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

B. FIELDS SEARCHED

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

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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2013/318592 A1 (GRIER SR RYAN WESLEY [US] ET AL) 28 November 2013 (2013-11-28) abstract paragraph [0003] - paragraph [0008]; figures 2A,2B paragraphs [0054], [0055], [0060] -----	1-15
A	US 6 144 959 A (ANDERSON BRADY [US] ET AL) 7 November 2000 (2000-11-07) abstract column 4, line 19 - column 5, line 20 -----	1-15
A	US 2013/298215 A1 (KUZNETSOV VSEVOLOD [RU] ET AL) 7 November 2013 (2013-11-07) abstract paragraph [0007] - paragraph [0011] paragraph [0044] -----	1-15

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

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
2 July 2015	09/07/2015

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

1

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

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2015/021919

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2013318592 A1	28-11-2013	NONE	
US 6144959 A	07-11-2000	NONE	
US 2013298215 A1	07-11-2013	US 2013298215 A1	07-11-2013
		WO 2013165274 A2	07-11-2013

Form PCT/ISA/210 (patent family annex) (April 2005)

フロントページの続き

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

(74)代理人 100173565
弁理士 末松 亮太
(72)発明者 ショーエン, ルーク
アメリカ合衆国ワシントン州９８０５２－６３９９, レッドモンド, マイクロソフト コーポレーション, エルシーエイ－インターナショナル・パテンツ（８／１１７２）
(72)発明者 クマール, サントシュ
アメリカ合衆国ワシントン州９８０５２－６３９９, レッドモンド, マイクロソフト コーポレーション, エルシーエイ－インターナショナル・パテンツ（８／１１７２）
(72)発明者 ダニ, ラージャラクシュミ
アメリカ合衆国ワシントン州９８０５２－６３９９, レッドモンド, マイクロソフト コーポレーション, エルシーエイ－インターナショナル・パテンツ（８／１１７２）
(72)発明者 マトゥール, シッダールタ
アメリカ合衆国ワシントン州９８０５２－６３９９, レッドモンド, マイクロソフト コーポレーション, エルシーエイ－インターナショナル・パテンツ（８／１１７２）
(72)発明者 ブレイディ, シェーン
アメリカ合衆国ワシントン州９８０５２－６３９９, レッドモンド, マイクロソフト コーポレーション, エルシーエイ－インターナショナル・パテンツ（８／１１７２）
(72)発明者 アリミリ, ラメシュ
アメリカ合衆国ワシントン州９８０５２－６３９９, レッドモンド, マイクロソフト コーポレーション, エルシーエイ－インターナショナル・パテンツ（８／１１７２）
(72)発明者 ヘザーリントン, デーヴィッド
アメリカ合衆国ワシントン州９８０５２－６３９９, レッドモンド, マイクロソフト コーポレーション, エルシーエイ－インターナショナル・パテンツ（８／１１７２）
(72)発明者 アフージャ, ヴィカス
アメリカ合衆国ワシントン州９８０５２－６３９９, レッドモンド, マイクロソフト コーポレーション, エルシーエイ－インターナショナル・パテンツ（８／１１７２）