(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2017-539017
(P2017-539017A)
(43)公表日　平成29年12月28日(2017.12.28)

(51)Int.Cl.		F I		テーマコード（参考）
G06F 21/31	(2013.01)	G06F	21/31	
G06F 21/41	(2013.01)	G06F	21/41	

審査請求 未請求　予備審査請求 未請求　（全 26 頁）

(21)出願番号	特願2017-527822 (P2017-527822)
(86)(22)出願日	平成27年11月18日 (2015.11.18)
(85)翻訳文提出日	平成29年7月14日 (2017.7.14)
(86)国際出願番号	PCT/US2015/061438
(87)国際公開番号	WO2016/081665
(87)国際公開日	平成28年5月26日 (2016.5.26)
(31)優先権主張番号	62/081,552
(32)優先日	平成26年11月18日 (2014.11.18)
(33)優先権主張国	米国 (US)
(31)優先権主張番号	14/877,316
(32)優先日	平成27年10月7日 (2015.10.7)
(33)優先権主張国	米国 (US)

(71)出願人　517174913
オースO，インコーポレイテッド
アメリカ合衆国，ワシントン州　９８００４，ベルビュー，ノースイースト　８番ストリート　１０９００，スイート　７００
(74)代理人　100079108
弁理士　稲葉　良幸
(74)代理人　100109346
弁理士　大貫　敏史
(74)代理人　100117189
弁理士　江口　昭彦
(74)代理人　100134120
弁理士　内藤　和彦

最終頁に続く

(54)【発明の名称】サービスとしてのアイデンティティインフラストラクチャ

(57)【要約】
ユーザアイデンティティの認証のために、複数のアプリケーションへのアクセスのシングルポイントを提供するためのアイデンティティサービスの方法およびシステムである。アプリケーションプログラムインタフェース（ＡＰＩ）を介してアプリケーションからの認証要求が受信され、認証要求はログオン情報を含む。認証要求は１または複数のアイデンティティプロバイダに変換される。認証すると、ユーザに関連付けられた１または複数のプログラム拡張スクリプトが連続的に実行される。ユーザに関連付けられたプログラム拡張スクリプトの少なくとも１つに基づいてユーザに権利が付与される。

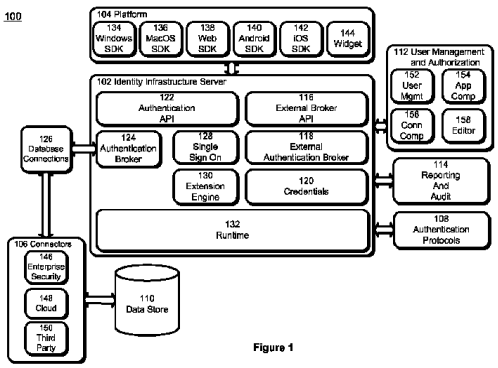


Figure 1

【特許請求の範囲】
【請求項１】
ユーザアイデンティティの認証のために複数のアプリケーションへのアクセスのシングルポイントを提供するように構成されたアイデンティティサービスシステムであって、
外部認証ブローカーにプログラムによるアクセスを提供するように構成されたエンタープライズブローカーアプリケーションプログラミングインタフェース（ＡＰＩ）と、
認証ブローカーと、
前記認証ブローカーに結合された１または複数のデータベース接続と、
前記データベース接続に接続された複数のセキュリティデリゲートと、
前記複数のセキュリティデリゲートに結合され、（ｉ）１または複数のユーザクレデンシャル、（ｉｉ）１または複数の拡張スクリプト、および（ｉｉｉ）メタデータ、の少なくとも１つを格納するように構成されたデータストアと
を備えるシステム。
【請求項２】
前記複数のセキュリティデリゲートは、（ｉ）エンタープライズセキュリティ、（ｉｉ）クラウドサービス、および（ｉｉｉ）第三者認証プロバイダ、の少なくとも１つに委任するように動作可能である、請求項１に記載のシステム。
【請求項３】
前記外部認証ブローカーは、前記エンタープライズブローカーＡＰＩから、（ｉ）認証データフォーマット、（ｉｉ）プロトコル、（ｉｉｉ）およびカスタムクレデンシャルストア、の少なくとも１つへの呼出しを実行する、請求項１に記載のシステム。
【請求項４】
複数の認証技術へのプログラムによるアクセスを提供するように構成された外部認証ＡＰＩを更に備え、前記外部認証ＡＰＩは、（ｉ）前記認証ブローカー、および（ｉｉ）前記複数のセキュリティデリゲートの少なくとも１つを呼び出すように動作可能な前記１または複数のデータベース接続、のうちの少なくとも１つと通信するように構成される、請求項１に記載のシステム。
【請求項５】
前記外部認証ＡＰＩは、ログオンウィジェットを介してシングルサインオン機能を提供するように構成される、請求項４に記載のシステム。
【請求項６】
前記セキュリティデリゲートは、（ｉ）クラウドサービス、（ｉｉ）インターネットホスト型サービス、および（ｉｉｉ）ローカルエリアネットワーク（ＬＡＮ）上でホストされるサービス、の少なくとも１つを含む、請求項１に記載のシステム。
【請求項７】
ユーザの認証時に承認を提供するように動作可能な拡張スクリプトエンジンを更に備える、請求項１に記載のシステム。
【請求項８】
前記１または複数の拡張スクリプトが組み合わさって、アイデンティティサービスのプログラム拡張を構成する、請求項７に記載のシステム。
【請求項９】
追加のセキュリティ分離を提供し、少なくとも前記エンタープライズブローカーＡＰＩ、前記外部認証ブローカー、および前記認証ブローカーの機能を実行するように動作可能なランタイムを更に備える、請求項１に記載のシステム。
【請求項１０】
前記１または複数の拡張スクリプトによって実行され得る変更の範囲を制限するように動作可能なサンドボックスを更に備える、請求項９に記載のシステム。
【請求項１１】
前記エンタープライズブローカーＡＰＩおよび前記外部認証ＡＰＩにアクセスするための（ｉ）ツールおよび（ｉｉ）ライブラリの少なくとも１つを提供するように構成された

、クライアント側のソフトウェア開発キット（ＳＤＫ）を更に備え、前記ＳＤＫの前記ツールは、ＪＡＶＡ（登録商標）スクリプトコードを実行する任意のアプリケーションのログインダイアログのための単体ソースコードを提供するように動作可能なログインウィジェットを含む、請求項１に記載のシステム。

【請求項１２】

ユーザ管理および承認機能を含むダッシュボードを更に備える、請求項１に記載のシステム。

【請求項１３】

前記ダッシュボードは、前記データベース接続の（ｉ）追加、（ｉｉ）削除、（ｉｉｉ）編集、および（ｉｖ）設定の少なくとも１つを行うように動作可能な接続コンポーネントを更に含む、請求項１２に記載のシステム。

【請求項１４】

前記承認機能は、権利が有効または無効にされるアクションをコンテキスト化する１または複数の拡張スクリプトを備えるプログラム拡張の開発をサポートするように動作可能な拡張スクリプトエディタを含む、請求項１２に記載のシステム。

【請求項１５】

ユーザアイデンティティの認証のために複数のアプリケーションへのアクセスのシングルポイントを提供するアイデンティティサービスを提供する方法であって、

アプリケーションプログラムインタフェース（ＡＰＩ）を介して前記複数のアプリケーションのうちのアプリケーションからのユーザの認証要求を受信することであって、前記認証要求はログオン情報を含むことと、

前記認証要求を１または複数のアイデンティティプロバイダに変換することと、

前記１または複数のアイデンティティプロバイダによって認証されると、前記ユーザに関連付けられた１または複数のプログラム拡張スクリプトを連続的に実行することと、

前記ユーザに関連付けられた前記プログラム拡張スクリプトの少なくとも１つに基づいて前記ユーザに権利を付与することと

を備える方法。

【請求項１６】

前記ユーザに対して前記付与された権利を前記アプリケーションに通知することを更に備える、請求項１５に記載の方法。

【請求項１７】

サンドボックス内で前記１または複数のプログラム拡張スクリプトを実行することによって、前記１または複数のプログラム拡張スクリプトによって実行され得る変更の範囲を制限することを更に備える、請求項１５に記載の方法。

【請求項１８】

認証要求ごとに前記ユーザに課金することを更に備える、請求項１５に記載のシステム。

【請求項１９】

前記ユーザがオンプレミスであるかオフプレミスであるかにかかわらず、前記１または複数のアイデンティティプロバイダを介してシングルサインオン（ＳＳＯ）を提供することを更に備える、請求項１５に記載のシステム。

【請求項２０】

ユーザアイデンティティの認証のために複数のアプリケーションへのアクセスのシングルポイントを提供するように構成されたアイデンティティサーバであって、

プロセッサと、

コンテンツおよびプログラミングのためのストレージデバイスと、

前記ストレージデバイスに格納されたプログラムと

を備え、前記プロセッサによる前記プログラムの実行によって、

アプリケーションプログラムインタフェース（ＡＰＩ）を介して前記複数のアプリケーションのうちのアプリケーションからの、ログオン情報を含むユーザの認証要求を受信す

ることと、
前記認証要求を１または複数のアイデンティティプロバイダに変換することと、
前記１または複数のアイデンティティプロバイダによって認証されると、前記ユーザに関連付けられた１または複数のプログラム拡張スクリプトを連続的に実行することと、
前記ユーザに関連付けられた前記プログラム拡張スクリプトの少なくとも１つに基づいて前記ユーザに権利を付与することと
を備える動作を実行するように構成されるアイデンティティサーバ。
【請求項２１】
前記プログラムの実行は更に、サンドボックス内で前記１または複数のプログラム拡張スクリプトを実行することによって前記１または複数のプログラム拡張スクリプトによって実行され得る変更の範囲を制限することを備える動作を実行するように構成される、請求項２０に記載のアイデンティティサーバ。
【請求項２２】
前記プログラムの実行は更に、認証要求ごとに前記ユーザに課金することを備える動作を実行するように構成される、請求項２０に記載のアイデンティティサーバ。
【請求項２３】
前記プログラムの実行は更に、前記ユーザがオンプレミスであるかオフプレミスであるかにかかわらず前記１または複数のアイデンティティプロバイダを介してシングルサインオン（ＳＳＯ）を提供することを備える動作を実行するように構成される、請求項２０に記載のアイデンティティサーバ。
【請求項２４】
前記プログラムの実行は更に、（ｉ）エンタープライズセキュリティ、（ｉｉ）クラウドサービス、および（ｉｉｉ）第三者認証プロバイダ、のうちの少なくとも１つに委任することを備える動作を実行するように構成される、請求項２０に記載のアイデンティティサーバ。
【請求項２５】
前記プログラムの実行は更に、ランタイムを介して、追加のセキュリティ分離と、少なくともエンタープライズブローカーＡＰＩ、外部認証ブローカー、および認証ブローカーの機能の実行とを備える動作を実行するように構成される、請求項２０に記載のアイデンティティサーバ。
【請求項２６】
前記プログラムの実行は更に、サンドボックス内で前記ユーザに関連付けられた前記１または複数のプログラム拡張スクリプトを実行することによって、前記ユーザに関連付けられた前記少なくとも１または複数のプログラム拡張スクリプトによって実行され得る変更の範囲を制限することを備える動作を実行するように構成される、請求項２０に記載のアイデンティティサーバ。
【発明の詳細な説明】
【背景技術】
【０００１】
コンピューティングの能力および普遍性が増加するとともに、人々のコンピューティングへの依存も増し、それはコンピュータハードウェア、コンピュータ実施サービス、またはコンピュータ支援プロセスの形で現れる。コンピューティングへの依存が増加するにつれ、コンピューティングのユーザは、コンピューティングを使用して機密性の高いデータおよび機能を扱うようになった。ユーザは、たとえば個人連絡先情報などの個人情報を日常的に自身のスマートフォンに格納する。ユーザは、注意深く考えることなく、たとえばクレジットカード取引などのコンピュータ化された機能に頼っている。実際、一体化の度合いは、多くのユーザが自身のラップトップ、携帯電話、またはクレジットカードを持っていない時、かつてのユーザが札入れや財布を持っていない時に匹敵する困惑を覚えるほどである。
【０００２】

不都合なことに、このコンピューティング依存によって、悪意を持った第三者が関心を持ちアクセスしようと試みる機密性の高いデータおよび機能が大量に保存されるようになった。一部の悪意を持った第三者は、単純にこれらのデータおよび機能を破損しようとする。他の者は、盗用しようとし得る。したがって、認証されていないユーザが機密データおよび機能にアクセスすることを防ぐためにコンピュータセキュリティシステムが開発されてきた。

【０００３】

コンピュータセキュリティシステムは、特定のコンテキストに特有である。コンテキストは、所与のセキュリティ認証メカニズムが有効である境界を備える。過去、コンテキストはコンピュータアプリケーションのコンテキストであった。たとえば法人ユーザは、人材アプリケーションのための１つのパスワードおよび会計システムのための別のパスワードを有し得る。したがって、第１のパスワードのコンテキストは人材アプリケーションのコンテキストであり、第２のパスワードのコンテキストは会計システムのコンテキストである。あるいは、コンテキストは、たとえばコンピューティングデバイスまたはネットワークなどコンピュータハードウェアプラットフォームのコンテキストであってもよい。たとえば、個人用コンピュータへのログオンは、アプリケーションに特化したセキュリティを有さない、そのコンピュータ上の個人的アプリケーションへのアクセスをもたらし得る。その個人用コンピュータは、ネットワークドライブ、ネットワークプリンタ、および他のネットワークコンピューティングアセットが、その認証されたパーソナルコンピュータに対して使用可能にされ得るように、社内ローカルエリアネットワーク（ＬＡＮ）上でネットワークセキュリティサービスによって認証され得る。

【０００４】

しかし、データまたは機能の機密性が増すにつれ、より多くの層のセキュリティ管理者が追加される。追加のセキュリティは、追加のコンテキストの増加を招き、その結果これらの追加のコンテキストに対応する認証クレデンシャルの増加がもたらされ、その全てをユーザが管理する。たとえば、ネットワークアクセスのためにパスワードが必要であり、同じネットワーク上の社内データベースにアクセスするために別のパスワードが必要であり、社内データベース上の暗号化レコードに関して、同じユーザが同じＬＡＮからそのレコードにアクセスする場合でも暗号鍵が必要であることが珍しくない。

【０００５】

現在、インターネットホスト型サービスの出現により、新たなアプリケーションに関連するコンテキストおよびそれら特有のクレデンシャルも増加してきた。かつてはユーザが自身の個人用ホームネットワーク用のパスワード、自身のワークアカウント、および自身のデビットカード／クレジットカードの個人識別番号（ＰＩＮ）を追跡することしか必要でなかったが、今やそのユーザは、各々が様々なセキュリティコンテキストを表す様々なインターネットサービスのための個々のアカウントを追跡する必要があり得る。たとえばソーシャルネットワーク（たとえばフェイスブック（登録商標））、電子メールサービス（たとえばＧメール（登録商標）やホットメール（登録商標））、および個々のソフトウェアサービス（たとえばＳａｌｅｓｆｏｒｃｅ（登録商標）．ｃｏｍ）は全て独自のセキュリティコンテキストを有し、それによって個々にクレデンシャルを管理する。

【０００６】

同様に、モバイルデバイスの出現により、コンピュータハードウェアプラットフォームに関連する新たなセキュリティコンテキストおよびそれらに付随するセキュリティクレデンシャルが増加してきた。ユーザが、仕事用および個人用コンピュータのパスワード、並びに自身の携帯電話および／またはタブレットデバイスのロックコードを追跡することは珍しくない。ソフトウェアサービスおよびコンピュータハードウェアプラットフォームの増加が相まって、セキュリティコンテキストの紛れもない爆発的増加が生じている。

【０００７】

セキュリティコンテキストの爆発的増加は、今日のアプリケーション開発者に対して課題をもたらした。ユーザは、自身のコンピューティングリソースの実装詳細が取り除かれ

ることを望む。アプリケーションが社内ネットワークに常駐するかインターネットにおけるクラウドベースであるかにかかわらず、ユーザは一貫したユーザ体験を所望し、セキュリティを一切妥協せずに、異なるセキュリティメカニズムが可能な限り統合されることを望む。たとえばユーザは、インターネットアプリケーションにおける認証を自身のフェイスブック（登録商標）ログオンクレデンシャルに委任したいと望み得る。しかし、アプリケーション開発者は、認証メカニズムをプログラミングし、そのメカニズムを異なるコンテキストと統合し、多種多様なコンピューティングハードウェアおよび／またはソフトウェアプラットフォームに実装するというタスクに直面する。

【０００８】

要するに、ソフトウェアサービスおよびハードウェアプラットフォームが増加するにつれ、アプリケーション開発者は、彼らのアプリケーションの魅力的な特徴の開発に投じる時間を犠牲にして、コンピュータセキュリティにますます長い時間をかけることになる。アプリケーション開発者が魅力的な特徴を生み出さなければ、ユーザはアプリケーションを購入しない。しかし、アプリケーションが安全でなければ、ユーザはやはりアプリケーションを購入しない。したがって、従来技術では対処されなかった上記の問題を緩和し、従来技術では考慮されないコンピュータセキュリティオプションを提供するためのアイデンティティサービスへの必要性がある。

【図面の簡単な説明】

【０００９】

詳細な説明は、添付図面を参照して説明される。図面において、異なる図内の同一参照番号の参照用の左端の数字は、類似または同一の要素を示す。

【００１０】

【図１】サービスとしてのアイデンティティインフラストラクチャに関するトップレベルコンテキスト図である。

【図２】サービスとしてのアイデンティティインフラストラクチャに関する典型的なハードウェアおよびソフトウェアプラットフォームを示す。

【図３】サービスとしてのアイデンティティインフラストラクチャに関する典型的な拡張スクリプトエンジンの図である。

【図４】サービスとしてのアイデンティティインフラストラクチャに関する典型的なランタイムの図である。

【図５】サービスとしてのアイデンティティインフラストラクチャにおいて用いられるログインウィジェットの図である。

【図６】サービスとしてのアイデンティティインフラストラクチャにおいて用いられるダッシュボードユーザインタフェースの典型的なルックアンドフィールの図である。

【図７】サービスとしてのアイデンティティインフラストラクチャにおいて用いられる規則ユーザインタフェースの典型的なルックアンドフィールの図である。

【図８】サービスとしてのアイデンティティインフラストラクチャのコンテキストにおけるいくつかの典型的な分析報告を示す。

【発明を実施するための形態】

【００１１】

（予備概念および定義）

現在、個人、企業および他の組織、並びに国家は、それらの活動におけるほぼ全ての分野で、コンピュータハードウェア、コンピュータ実施サービス、またはコンピュータ支援プロセスを含むコンピューティングを用いる。コンピューティングへの依存は、機密データおよび機密性の高い機能、または他者がアクセスした場合ユーザに害を及ぼすことになるデータおよび機能に及ぶまで広がっている。個人ユーザは、電話番号、電子メールアドレス、および他の連絡先情報を追跡するためにスマートフォンのコンピューティング能力を使用し得る。たとえば被雇用者などの企業ユーザは、給料の決定および支払いのためにコンピュータ化された給与システムを使用し得る。国家は、国家防衛および機密性の高い公共インフラストラクチャのためにコンピューティングを使用し得る。その結果、これら

の活動はいずれも機密データおよび機密性の高い機能を含み、そのどちらも、コンピュータおよび／またはコンピュータ支援／実施サービスの任意の潜在的ユーザが保護しようと努めるものである。

【００１２】

コンピュータセキュリティは、機密データを保護するというプライバシーの概念を含む。保護は、機密性が高いものとして指定されたデータへのアクセスを防止するという形でもたらされ得る。たとえば、個人ユーザは、彼／彼女が他人に知られたくないと望む銀行口座残高を有し得る。したがってその個人は、その銀行口座残高情報へのアクセスを、たとえば配偶者、または銀行の従業員などの特定の役割の人物といった特定の個人に限定し得る。また保護は、データの破損を防ぐという形でももたらされ得る。たとえば、個人のユーザは、個人的なスケジュール情報を有する個人用コンピュータを有し得る。悪意を持った者が個人データを読み取ることができないとしても、その代わりに悪事を企て、スケジュール情報を変更、削除、あるいは破壊するためにコンピュータウィルスを仕掛けることがある。

【００１３】

コンピュータセキュリティの概念は、機能の保護も含む。データの保護と同様、機能の保護は、ユーザが、他のユーザが機密性の高いコンピュータ機能にアクセスし、またはそれを実行することを防ぐことと、悪意を持った第三者が機密性の高いコンピュータ機能を破壊することを防ぐこととの両方を含む。前者の例は、個人ユーザが、彼または彼女の銀行口座から他者が預金を電子的に引き出すことを防ごうとすることである。後者の例は、ユーザが、悪意を持った第三者がアプリケーションを破壊しそのコンピュータ機能のサービスへの個人ユーザのアクセスを拒否するようにすることを防ぐためのコンピュータウィルス防止プログラムを追加することである。

【００１４】

上述したように、プライバシーおよび保護機能は、それぞれデータおよび機能を保護することを備える。コンピュータセキュリティメカニズムによって保護され得るデータおよび機能の範囲が、コンピュータセキュリティメカニズムのセキュリティコンテキストである。すなわち、コンピュータセキュリティメカニズムは、そのコンピュータセキュリティメカニズムによる認証および承認が信頼される、データおよび機能のドメインを有する。ドメインの範囲がセキュリティコンテキストであり、セキュリティコンテキストから離れることは、セキュリティコンテキストの信頼境界を越えることであると言える。

【００１５】

したがって、セキュリティコンテキストのための効果的なコンピュータセキュリティは、そのセキュリティコンテキストに関する認証および承認の概念を含む。認証は、正当なユーザを識別し、彼らが保護されたデータおよび／または機能にアクセスできるようにしようとする試みにおけるアイデンティティの証明である。ユーザを認証する一般的な方法としてクレデンシャルがある。クレデンシャルは、様々な形でもたらされ得る。認証は、たとえば保護側のユーザがパスワードを所持することなど、情報の所持によるものであってよい。認証は、たとえばセキュリティユーザが鍵などのアーチファクトを所持することなど、アーチファクトの所持によるものであってよい。所持による認証の個人的形態は、網膜スキャンまたは指紋スキャンによるものである。また認証は、たとえばクレジットカード保有者の過去の購買との一貫性がない購買をクレジットカード会社が停止することなど、挙動によるものであってもよい。要するに、認証は、ユーザが自称する本人であることを証明するためにクレデンシャルを用いることである。

【００１６】

認証は、認証の成功後、所与のコンテキストにおける保護されたデータおよび／またはコンピューティング機能へのアクセスを可能にすることである。上述したように、認証は多くの場合、想定されるクレデンシャルを保持することによってユーザが自称する者であることを証明することに限定される。ただし、認証中、ユーザは人間である必要はなく、機械またはプログラムであってもよい。認証と同様、認証を実行するセキュリティメカニ

ズムは、セキュリティコンテキストによって定められる範囲を有する。したがって、実用的には、認証は多くの場合、ユーザが認証されると、保護されたデータおよび／またはコンピューティング機能へアクセスする権利にユーザをマッピングすることを含む。認証技術は、権利を付与し、アクセス制御リストを作成および保持し、アクセスポリシおよび規則を作成および保持するシステム管理者機能を含む。要するに、認証は、たとえばシステム管理者などの一人のユーザから、他のユーザへの権利の発行である。認証に関するコンテキストは多くの場合、動的である。所与のユーザができることや、彼がアクセスし得るリソースは、たとえば時間、挙動、および場所に基づいて変化してよい。ユーザが一日のうちに異常な回数同じリソースにアクセスした場合、彼は、彼が自称する本人であることの追加の証明を提供するように要求され得る。彼が通常接続しているネットワーク以外のネットワークからアクセスした場合も同様である。

【００１７】

認証に先立って、コンピュータセキュリティは、実際の保護またはデータおよび／もしくはコンピューティング機能を含む。具体的には、保護は、認証されていないアクセスを防ぐために用いられる手段である。現在、データおよび／またはコンピューティング機能の保護には暗号が利用される。暗号は、たとえば長い素数などの数学的鍵を発見する困難を伴わずにアクセスされる場合に、データまたは機能を難解かつ使用不可能な形式に変換することである。現在の暗号技術は一方向関数を利用してよく、一方向関数は、関数の計算（すなわち暗号化）は比較的迅速であるが、逆関数の計算（すなわち復号化）は、数学的鍵がない状態で従来の技術を用いると数年または数百年を要するほど非常に緩慢であるためそのように呼ばれる。

【００１８】

したがって、認証されると、ユーザはコンピュータセキュリティシステムによって鍵を提供され、それによって、ユーザが認証された保護データおよび／または機能へのアクセス権を得る。このように、コンピュータセキュリティは、鍵生成、鍵配布、および鍵管理を含む。鍵生成は、暗号関数に関する１または複数の鍵を作成することである。対称暗号は一般に、秘密に保たれ関係者間で共有される単一の鍵を利用する。非対称暗号は、たとえば楕円曲線および係数指数が鍵ペアを含むような暗号関数を利用し、第１の鍵は、第２のユーザへの通信を暗号化するために第１のユーザに公知され、第２の鍵は、第２のユーザによって秘密に保たれ、第１のユーザによって暗号化された通信を復号化するために使用される。

【００１９】

対称および非対称暗号はどちらも、少なくともいくつかの生成された鍵が秘密に保たれることに頼る。したがって、鍵配布は、鍵を配布するだけではなく、認証されていない者および／または悪意を持った者に鍵が傍受されることを防ぐことにも関係する。鍵配布技術は、認証されたユーザのみが生成された鍵を受け取ることを確実にするためのプロトコルを含む。配布された鍵が漏洩するというリスクが常に伴うので、鍵管理は、鍵をいつどのように作成、配布し、失効させるかに関するポリシを設定および実装することである。

【００２０】

コンピュータデータおよび／またはコンピュータ機能の機密性が十分に高い場合も、最終的にはコンピュータセキュリティは攻撃を受けることもある。監査は、損害予測および応答の開発が十分可能であるようにこれらの攻撃を検出することである。監査は、事前型、リアルタイム、または反応型であってよい。事前監査は、悪意を持った第三者による査察を検出し、コンピュータセキュリティ防衛をテストすることを含んでよい。リアルタイム監査は、現在進行中の攻撃を検出することを含んでよい。反応監査は、攻撃が発生したことを検出することを含んでよく、損害予測を更に含んでもよい。

【００２１】

（サービスとしてのアイデンティティ）

上述したように、認証は、多くの場合、有効であり得る予想通りのクレデンシャルを提示することによって、ユーザ、人間、機械、またはその他が自称するものであることを証

明することである。ユーザと、ユーザ自身のそれぞれのクレデンシャルとが重なることが、そのユーザのアイデンティティである。アイデンティティの概念は、ユーザセキュリティをカプセル化する抽象的概念である。したがって、アイデンティティ管理は、認証、承認、および監査を含むコンピュータセキュリティ機能のサブセットであるが、たとえば暗号インフラストラクチャなど基礎となる保護メカニズムではない。

【００２２】

１つの態様において、本特許出願は、広範囲のセキュリティコンテキストにおけるコンピュータアプリケーションおよびデバイスにためのコンピュータセキュリティ機能をサポートするアイデンティティインフラストラクチャサービスについて説明する。具体的には、アイデンティティインフラストラクチャサービスは、任意のアイデンティティプロバイダ／セキュリティデリゲートまたはアイデンティティプロバイダ／セキュリティデリゲートの任意のセットを用いて、複数のハードウェアおよびソフトウェアプラットフォームにわたって保護されるデータおよび機能の任意のセットに関する任意のセキュリティコンテキストをもたらすことを可能にする。また、アイデンティティインフラストラクチャサービスは、アイデンティティサービスをプログラムで制御する方法を提供し、それによってセキュリティコンテキストの範囲および動作を動的なものにする。したがって、アイデンティティインフラストラクチャサービスは、アプリケーションプログラミングインタフェース（「ＡＰＩ」）を公開する。アイデンティティインフラストラクチャサービスの集中／集合特性により、多くの場合アイデンティティインフラストラクチャサービスは、たとえばプロビジョニング、デプロビジョニング、ユーザ検証、およびユーザプロファイルなどのユーザ管理機能と併用され、または密接に結び付けられ得る。具体的には、ユーザ管理は、セキュリティに関連することも関連しないこともあるユーザ属性を管理することである。

【００２３】

サービスとしてのアイデンティティを開発する利点は、セキュリティコンテキストの信頼境界が、ユーザの観点および管理者の観点の双方から統合されることである。従来技術によるアイデンティティスキームは、様々な認証スキームだけではなく様々な場所で実施される様々なサービスも継ぎ合せていた。たとえばユーザの観点から見ると、社内ＬＡＮへのログオンおよびローカル会計システムへのログオンは、単に独立した２つのログオンを意味するものではない。これは、ユーザが、各ログオンによって少なくとも１つのセキュリティコンテキストの信頼境界を越えなければならないことを意味し、会計システムへのログオンは、ネットワーク上で信頼されていることを意味するものではなく、ＬＡＮへのログオンは、会計システム上で信頼されていることを意味するものではない。管理者は、ユーザが会計システムから印刷およびファイルサービスにアクセスできるように、たとえばＬＡＮ上の会計管理アカウントを作成するといったやり方をする必要があった。管理者の観点から見ると、管理者は、単一のユーザの観点からアカウントのセキュリティステータスを見ることができない。たとえば、ハッカーがユーザをハッキングしようと試みた場合、管理者は、ユーザのＬＡＮアカウントへの攻撃およびユーザの会計システムアカウントへの攻撃を２つの無関係のイベントとして扱わなければならず、その結果、ハッキング攻撃の検出およびそれに対する応答が遅くなる。

【００２４】

１つの態様において、本特許出願は、セキュリティコンテキストに関して、１または複数の拡張スクリプトおよび／もしくは他のプログラムを備えるプログラム拡張を介してプログラムによって、並びに／またはツールおよび他の設定メカニズムを介して管理者によって、コンピュータセキュリティ機能を開発するためのツール、ライブラリ、および他の環境要素を説明する。また、本特許出願は、様々なアイデンティティ管理の使用事例をサポートするための集中型サービスを説明する。

【００２５】

図１は、アイデンティティインフラストラクチャサービスの典型的な実施形態を示すトップレベル図１００である。アイデンティティインフラストラクチャサービスは、アイデ

ンティティおよびユーザ管理サービスへアクセスするためのシングルポイントを提供する。具体的には、図１００は、アイデンティティインフラストラクチャサーバ１０２、様々な開発プラットフォーム１０４との統合、様々なセキュリティデリゲートとの接続１０６、様々な認証プロトコル１０８へのアクセス、様々なクレデンシャルおよび認証のためのストレージ１１０、ユーザ管理および認証機能１１２、並びに監査および分析機能１１４を示す。

【００２６】

（アイデンティティインフラストラクチャサーバ）

アイデンティティインフラストラクチャサーバ１０２は、アプリケーション開発者がアイデンティティおよびユーザ管理サービスへアクセスするためのシングルポイントを提供するソフトウェアサービスのセットである。具体的には、たとえば認証、承認、および監査などの特定の機能がアイデンティティインフラストラクチャサーバ１０２において実行され得る。それによってアイデンティティインフラストラクチャサーバ１０２は、様々なデータおよび機能にわたり、任意のアイデンティティプロバイダを用いて、任意のセキュリティコンテキストの生成をもたらす。

【００２７】

認証は、アイデンティティプロバイダによってネイティブに実行されてよく、または委任されてもよい。アイデンティティプロバイダが委任される場合、これはセキュリティデリゲートとして知られる。インフラストラクチャサーバ１０２は、エンタープライズ外部ブローカーアプリケーションプログラミングインタフェース（「ＡＰＩ」）１１６を認証のために公開する。エンタープライズブローカーＡＰＩ１１６は、たとえばセキュリティアサーションマークアップランゲージ（「ＳＡＭＬ」）、ＷＳ－Ｆｅｄｅｒａｔｉｏｎ、ＷＳ－Ｔｒｕｓｔ、ＯｐｅｎＩＤ接続、ＯＡｕｔｈ１、ＯＡｕｔｈ２、または完全カスタムクレデンシャルストアなどの認証データフォーマットおよび／またはプロトコルへのＡＰＩ呼出しを実行する外部認証ブローカー１１８へのプログラムによるアクセス（Ｐｒｏｇｒａｍｍａｔｉｃ　ａｃｃｅｓｓ）を提供する。このように、ＡＰＩは、一様なプログラミングインタフェースを提供するとともに、過去、現在、および未来の多種多様な認証データフォーマットおよびプロトコルへの参加を可能にする。

【００２８】

いくつかの認証データフォーマットおよび／またはプロトコルは、ユーザクレデンシャル１２０のローカルストレージを想定する。あるいは、ユーザクレデンシャルは非ローカルストレージ１１０に格納されてもよい。

【００２９】

インフラストラクチャサーバ１０２は、様々な認証技術へのプログラムによるアクセスを提供する外部認証ＡＰＩ１２２も公開する。具体的には、外部認証ＡＰＩ１２２は、ソーシャル認証ブローカー１２４にアクセスし、またはデータベース接続１２６とインタフェース接続してよく、それらが様々なセキュリティデリゲートへの様々な接続１０６を呼び出してよい。ただし、セキュリティデリゲートは、クラウドサービスおよび他のインターネットホスト型サービスであってよい。あるいはセキュリティデリゲートは、ＬＡＮ上でホストされるサービスであってもよい。外部認証ＡＰＩ１２２は、外部ブローカー１１６、外部認証ブローカー１１８、および認証ブローカー１２４を含む全てのブローカーおよびデリゲートに対して可視性があるので、シングルサインオン機能１２８を実装し得る。認証時、認証は認証拡張スクリプトエンジン１３０を介して実行される。シングルサインオン１２８および認証拡張スクリプトエンジン１３０の更なる動作詳細は、図３および図４を参照して説明される。

【００３０】

アイデンティティインフラストラクチャサーバ１０２の様々なコンポーネントの実装は、ランタイム１３２において実行されてよい。ランタイムは、更なるセキュリティ分離を提供してよい。ランタイム１３２のセキュリティ特徴は、図４を参照して更に詳しく説明される。

【００３１】
（開発プラットフォーム）
上述したように、アイデンティティインフラストラクチャサーバ１０２は、アイデンティティ管理およびユーザ管理機能、エンタープライズ／ＬＡＮおよび外部データベース／クラウドサービスに関して、また様々なプロトコル、データフォーマットに関して、並びに様々なアイデンティティプロバイダおよびセキュリティデリゲートに対して、一様なＡＰＩを公開する。
【００３２】
同様に、クライアント側で、ソフトウェア開発キット（「ＳＤＫ」）１０４により、ＡＰＩ１１６および１２２へアクセスするためのツールおよびライブラリを提供する。ＳＤＫ１０４は、多種多様なクライアントプラットフォームのサポートにおいて開発者を支援するための一様なプログラムモデルを提供するために役立つ。具体的には、パーソナルコンピュータアプリケーションは、マイクロソフト（登録商標）ウィンドウズ（登録商標）プラットフォームのためのＳＤＫ１３４またはアップル（登録商標）ＭａｃＯＳ（登録商標）のためのＳＤＫ１３６によってサポートされる。ウェブアプリケーションもまた特定のＳＤＫ１３８を有し、アンドロイド（登録商標）ＳＤＫ１４０およびアップルｉＯＳＳＤＫ１４２を介するモバイルデバイスも同様である。
【００３３】
各ＳＤＫ１０４は、その基礎となるオペレーティングシステム／ソフトウェアプラットフォームに特化しているが、様々なオペレーティングシステム／プラットフォームのためのアプリケーション開発を容易にするためにＳＤＫは一貫して実装される。それらが実行している基礎プラットフォームの特異性を考慮して同一の機能を実行する意味的および統語的に同様のライブラリによって、この一貫性の利点が１つの観点から示される。ＪＡＶＡ（登録商標）スクリプトコードを実行することができる任意のアプリケーションのログインダイアログを提供するために単体ソースコードを提供する、ＪＡＶＡスクリプトログインウィジェット１４４によって、この利点が他の観点から示される。ＪＡＶＡスクリプトログインウィジェット１４４の動作は、図５を参照して更に詳しく説明される。
セキュリティ委任のための接続
【００３４】
（セキュリティ委任のための接続）
アイデンティティインフラストラクチャサーバ１０２は通常、セキュリティを実装することはなく、むしろブローカーセキュリティがアイデンティティプロバイダおよびセキュリティデリゲートを形成する。したがって、アイデンティティインフラストラクチャサーバ１０２は、ネイティブアイデンティティプロバイダを介してネイティブセキュリティを公開し、接続１０６を介して多種多様なセキュリティデリゲートとのインタフェース接続を提供する。接続は、エンタープライズセキュリティ１４６、クラウドサービス１４８、または第三者認証プロバイダ１５０に委任し得る。
【００３５】
エンタープライズセキュリティ接続１４６は、一般的にエンタープライズオンプレミスネットワーク（ＬＡＮ）においてセキュリティサーバとのインタフェースを管理する。たとえば、ケルベロスキーサーバは、ＬＡＮドメインに常駐してよい。アイデンティティインフラストラクチャサーバ１０２がケルベロスベースセキュリティサーバへアクセスするために、アイデンティティインフラストラクチャサーバ１０２は、ケルベロスキーサーバの場所を特定しハンドシェイクしなければならない。これは通常、たとえばマイクロソフトアクティブディレクトリなどのドメインディレクトリサービスまたはたとえばＯｐｅｎＬＤＡＰなどのライトウェイトディレクトリアクセスプロトコル（「ＬＤＡＰ」）サービスを介して行われる。セキュリティサーバの特定およびそれとのハンドシェイクが成功すると、ユーザが認証され得る。
【００３６】
クラウドサービス接続１４８は、それらの認証メカニズムへの委任を提供するクラウド

サービスとの接続である。たとえば、フェイスブック（登録商標）およびグーグル（登録商標）Ｇメール（登録商標）はいずれもユーザを認証する。クラウドサービス接続１４８は、ユーザのアイデンティティを証明するために、アプリケーションがそれぞれのＡＰＩを介して第三者クラウドアプリケーションへアクセスすることを可能にする。

【００３７】

第三者認証プロバイダ接続１５０は、クラウドサービス接続とは異なりハイパーテキスト転送プロトコル（「ＨＴＴＰ」）を介して通信するのではない第三者認証プロバイダとの接続である。この例には、ベリサイン（登録商標）および米政府固有の認証プロバイダが含まれる。

【００３８】

（認証サービスおよびプロトコル）

アイデンティティインフラストラクチャサーバ１０２は、多種多様な認証プロトコルをサポートする。したがって、アイデンティティインフラストラクチャサーバ１０２は、特定の認証プロトコルをサポートする外部コンポーネント１０８を利用してよい。たとえばＯＡｕｔｈ２．０は、アイデンティティインフラストラクチャサーバ１０２から遠隔にある信頼される第三者サーバを利用してよい。そのようなシナリオにおいて、アイデンティティインフラストラクチャサーバ１０２は、これらの第三者コンポーネント１０８とインタフェース接続する。

【００３９】

（クレデンシャル永続化）

アイデンティティインフラストラクチャサーバ１０２は、クレデンシャル、認証拡張スクリプト、メタデータ、およびアイデンティティインフラストラクチャサーバ１０２の動作中に使用される他のデータを格納するための外部永続化サーバ１１０を有する。永続化サーバは、限定されないが、リレーショナルデータベース管理サーバ（「ＲＤＭＢＳ」）またはオブジェクト指向データベース、列指向データベース、またはＮｏＳＱＬデータベースであってよい。

【００４０】

永続化サーバ１１０は、たとえばクレデンシャルなどの機密情報を格納し得るので、レコード単位の暗号化を実行してよい。

【００４１】

（ユーザ管理および認証機能）

アイデンティティインフラストラクチャサーバ１０２は、アイデンティティ管理だけではなくユーザ管理および認証機能を提供するダッシュボード１１２を介して操作される。ダッシュボード１１２は、ユーザプロビジョニングが行われるユーザ管理機能１５２を含む。アプリケーションプリファレンスは、アプリケーションコンポーネント１５４を介して設定され得る。接続コンポーネント１５６を介して接続が追加、削除、編集、または設定され得る。拡張スクリプトエディタ１５８は、入力および接続のインタフェースとなるスクリプトを介して、アプリケーション権利に関するユーザの承認のプログラム制御を提供する。ダッシュボード１１２は、図６を参照して更に詳しく説明される。

【００４２】

拡張スクリプトエディタ１５８は、アイデンティティサーバを介してアクセス可能な任意のリソースおよび／またはクライアントにおける任意のリソースに対する非常に高度な論理およびプログラム制御を提供する。具体的には、拡張スクリプトエディタ１５８は、特定の範囲のユーザアクティビティに依存して権利が有効化／無効化される、アクションをコンテキスト化し得る１または複数の拡張スクリプトから成るプログラム拡張の開発をサポートする。コンテキスト化されたアクションは、図３を参照して更に詳しく説明され、拡張スクリプトエディタは図６を参照して更に詳しく説明される。

【００４３】

（監査機能）

ダッシュボード１１２はまた、監査および報告機能１１４もサポートする。管理者は、

たとえばログオン試行、失敗した試行、およびアクセスしたアプリケーションなど、ユーザのアイデンティティに関連する全ての活動をレビューしてよい。報告機能は、多種多様な分析機能および報告を提供することによって、事前の、リアルタイムの、および反応的な監査を支援する。分析機能および報告は、図７を参照して更に詳しく説明される。

【００４４】

（典型的なハードウェアプラットフォーム）

図２は、意味的保証付きアプリケーションの自動ポーティングのためのハードウェア環境２００の考えられる１つの実施形態を示す。

【００４５】

クライアントデバイス２０２は、任意のコンピューティングデバイスである。典型的なコンピューティングデバイスは、限定されないが、パーソナルコンピュータ、タブレットコンピュータ、スマートフォン、スマートテレビ、スマートメディアプレーヤー、およびたとえばキャッシュマシンなどのセキュアキオスクを含む。クライアントデバイス２０２は、プロセッサ２０４およびメモリ２０６を有してよい。クライアントデバイス２０２のメモリ２０６は、アプリケーション２０８および／またはオペレーティングシステム２１０を含むいくつかのプログラムを格納し得る任意のコンピュータ可読媒体である。

【００４６】

コンピュータ可読媒体は少なくとも、２種類のコンピュータ可読媒体、すなわちコンピュータ可読媒体および通信媒体を含む。コンピュータ記憶媒体は、たとえばコンピュータ可読命令、データ構造、プログラムモジュール、または他のデータなどの情報を格納するための任意の方法または技術によって実装される、揮発性および不揮発性、消去可能および消去不可能な媒体を含む。コンピュータ記憶媒体は、ＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭ、フラッシュメモリもしくは他のメモリ技術、ＣＤ－ＲＯＭ、デジタルバーサタイルディスク（ＤＶＤ）もしくは他の光ストレージ、磁気カセット、磁気テープ、磁気ディスクストレージもしくは他の磁気ストレージデバイス、またはコンピューティングデバイスによってアクセスするための情報を格納するために用いられ得る他の任意の非伝送媒体を含むが、これに限定されない。対照的に、通信媒体は、コンピュータ可読媒体、データ構造、プログラムモジュール、または他のデータを、たとえば搬送波や他の伝送メカニズムなどの変調データ信号において具現化し得る。本明細書で定義されるように、コンピュータ記憶媒体は、通信媒体を含まない。

【００４７】

通信環境に参加するために、ユーザ機器デバイス２０２は、ネットワークインタフェース２１２を有してよい。ネットワークインタフェース２１２は、イーサネット（登録商標）、Ｗｉ－Ｆｉ、または任意の数の他の物理およびデータリンク標準インタフェースを含む、１または複数のネットワークインタフェースであってよい。ユーザがスタンドアロン型単独マシンでの動作のみを必要とする場合、ネットワークインタフェース２１２は任意選択である。

【００４８】

クライアント２０２は、サーバ２１４に通信してよい。サーバ２１４は、ネットワークに参加し得る任意のコンピューティングデバイスである。ネットワークは、限定されないが、ローカルエリアネットワーク（「ＬＡＮ」）、仮想プライベートネットワーク（「ＶＰＮ」）、セルラネットワーク、またはインターネットであってよい。クライアントネットワークインタフェース２１２は、サーバネットワークインタフェース２１６を介してサーバ２１４に最終的に接続してよい。サーバネットワークインタフェース２１６は、クライアントネットワークインタフェース２１２に関して説明されたような１または複数のネットワークインタフェースであってよい。

【００４９】

またサーバ２１４は、プロセッサ２１８およびメモリ２２０も有する。クライアントデバイス２０２に関する上記説明のとおり、メモリ２２０は、コンピュータ記憶媒体および通信媒体の両方を含む任意のコンピュータ可読媒体である。

【００５０】
特に、メモリ２２０は、アプリケーション２２２および／またはオペレーティングシステム２２４を含み得るソフトウェアを格納する。メモリ２１６もまた、限定されないが、アプリケーションサーバおよびデータベース管理システムを含み得るアプリケーション２２２を格納し得る。したがって、サーバ２１４はデータストア２２６を含み得る。データストア２２６は、リレーショナルデータベース、オブジェクト指向データベース、ＮｏＳＱＬデータベース、および／または列指向データベース、または拡張可能な永続化をサポートする任意の構成として構成され得る。
【００５１】
サーバ２１４は、オンサイトである、またはクライアントエンタープライズによって操作される必要はない。サーバ２１４は、クラウド設備２２８においてインターネットでホストされてよい。クラウド設備２２８は、仮想ウェブアプリケーションサーバ２３０、２３２の機能、および仮想データベース２３４の機能を提供する複数の個別のサーバを表してよい。クラウド２２８のサービス２３２、２３４は、クラウドインフラストラクチャ２３６を介してアクセス可能にされてよい。クラウドインフラストラクチャ２３６は、クラウドサービス２３０、２３２へのアクセスだけではなく、課金サービスへのアクセスも提供する。クラウドインフラストラクチャ２３６は、たとえばサービスとしてのプラットフォーム（「ＰＡＡＳ」）、サービスとしてのインフラストラクチャ（「ＩＡＡＳ」）、およびサービスとしてのソフトウェア（「ＳＡＡＳ」）など、更なるサービス抽象化を提供し得る。
【００５２】
（サービスとしてのアイデンティティのための支援ツールおよび環境）
（概観）
サービスとしてのアイデンティティは、従来技術によってもたらされない利点を生み出す。アイデンティティおよびセキュリティ機能が集中化されることにより、セキュリティコンテキストの信頼境界が複数回交差せず、その結果、動作と報告との統合が簡単になる。以下、図１を参照して説明されたようなアイデンティティインフラストラクチャを備える選択されたコンポーネントが説明される。
【００５３】
（拡張スクリプトエンジン）
ユーザの認証は、ユーザがシステム全体に関して認証されるか、またはシステムから締め出されるかのいずれかである単純な２項演算から進化を遂げてきた。認証は、システムの一部に対する特定の個別的権利をトリガし得るだけではなく、条件付きであってもよい。システムの特定の部分に特化した権利を許可するための条件のカプセル化は、規則と呼ばれる。たとえば管理者は、３つの特定のマシンのみに対してアクセスが許可され、特定のファイルに対する読取専用の権利が許可される、一時的技術者のロールを構成してよい。
【００５４】
ロールを越えて、サービスとしてのアイデンティティにおいて、プログラム拡張は、１または複数の拡張スクリプトを備える。プログラム拡張は、汎用拡張モデルを提供する。プログラム拡張およびそれらの拡張スクリプトは、任意のプログラム目的に、セキュリティベース、アイデンティティベース、またはその他で適用され得る。たとえば、プログラム拡張は、非セキュリティまたは非アイデンティティベースの情報、および／または非セキュリティまたは非アイデンティティカスタムＡＰＩの集合においてトリガしてよい。
【００５５】
しかし、プログラム拡張は、セキュリティおよび／またはアイデンティティコンテキストにも広範囲に適用されてよい。プログラム拡張は、アプリケーション単位／ユーザ単位でコンテキスト化された認証を可能にする。具体的には、アイデンティティサービスは、たとえば保護されるべきアプリケーションおよび／もしくはそれら各々のＡＰＩ、ネットワークリソース、並びに／または保護されるべきデバイスへのアクセスなど、保護される

任意のデータおよび機能へのアクセスを提供する。ユーザは更に、アプリケーションおよび／またはデバイスをアクセス可能にするためにカスタムＡＰＩを作成してよい。その結果デバイスアクセシビリティに関するサポートは、「モノのインターネット」の要素を保護することを可能にし得る。データおよび機能へのアクセスは、プログラム拡張を構成する１または複数の拡張スクリプトを介して１または複数のアイデンティティプロバイダおよび／またはセキュリティデリゲートによって保護され得る。その結果、拡張スクリプトは、任意のセキュリティコンテキストをプログラムで作成することができる。したがって、１または複数の拡張スクリプトが組み合わさって、アイデンティティサービスのプログラム拡張を構成する。また、プログラム拡張は基本的にプログラムに従うので、作成されたセキュリティコンテキストの範囲および挙動は動的である。プログラム拡張の拡張スクリプトは、アイデンティティサーバおよびクライアントが利用可能な任意の入力へのアクセスを有するので、セキュリティコンテキストの範囲は、これらの入力のいずれかに応答して変化してよい。

【００５６】

プログラム拡張の拡張スクリプトは、任意のアイデンティティ、任意の制約、モジュール内の機能のホワイトリスト、ユニフォームリソース識別子（「ＵＲＩ」）のホワイトリストなどに結び付けてよい。そのようなリソースは全て、セキュリティコンテキストの作成および管理において拡張スクリプトによってプログラムで制御されてよい。一例として、新しい顧客による任意のログオンがスクリプトによって検出され、企業担当者が追跡するために顧客関係管理（「ＣＲＭ」）アプリケーションにおいてレコードが作成された際のプログラム拡張を考える。そのような機能は、全てプログラム拡張による、ＣＲＭ機能を備えたアイデンティティ機能をプログラムによって拡張する例である。

【００５７】

サービスとしてのアイデンティティにおいて、プログラム拡張によって作成されるセキュリティコンテキストは、システムの範囲を超えて適用し、１つのアイデンティティプロバイダおよび／またはメカニズムの範囲を超えて適用し得る。システムおよび様々なアイデンティティプロバイダおよび／またはメカニズムのアイデンティティ／セキュリティサービスの集中化によって、単一の拡張スクリプトにより、任意のサービスおよび／またはメカニズムを制約し得る。図３は、アイデンティティインフラストラクチャにおける、１または複数のプログラム拡張に関する拡張スクリプトの管理およびこれらの拡張スクリプトの実行を示す。

【００５８】

アイデンティティサーバ３０２は、ランタイム３０４、およびサンドボックス３０６を含む。ランタイム３０４およびサンドボックスは、図４を参照して更に詳しく説明される。拡張スクリプト３０８は、アプリケーションＡＰＩ、セキュリティＡＰＩ、アイデンティティプロバイダとのＡＰＩ、およびアイデンティティサーバ３０２が使用可能な他の任意のＡＰＩを呼び出すアイデンティティサービスのプログラム拡張を構成する。最も注目すべきは、単一のプログラム拡張の拡張スクリプトが、様々なアプリケーション、様々なセキュリティメカニズム、様々なアイデンティティプロバイダからＡＰＩを呼び出す可能性があるという点である。したがって、拡張スクリプトは、セキュリティサービスをプログラムによって拡張するためのメカニズムを提供する。プログラム拡張に加えて、管理者は１または複数の拡張スクリプトをプログラムしてよく、この場合拡張スクリプトは、アイデンティティサーバ３０２のためのプログラム拡張に関連付けられた周知のネームスペースを共有する。プログラム拡張の構成要素である拡張スクリプトはその後、通常はアイデンティティサーバのローカルストレージにおいてアイデンティティサーバ３０２へアップロードされるが、ネットワークストレージにアップロードされることもある。反対に、プログラム拡張は、その構成要素である拡張スクリプトをストレージから削除することによって消去され得る。アップロードされた拡張スクリプト３０８は、ユーザ３１０またはユーザロール３１２、すなわち共通の権利のセットを有するユーザグループに関連付けられてよい。アップロードされたプログラム拡張３０８は、アクティブまたは非アクティブ

に設定されてよい。したがって、プログラム拡張３０８を、非アクティブ化のために削除する必要はない。

【００５９】

拡張スクリプトの動作の一例は、プログラム拡張とユーザおよび／またはロールとの関連付けである。この例において、ユーザ３１０は、アプリケーション３１４にログオンしようと試みる。アプリケーション３１４はその後、自身のＡＰＩを介してアイデンティティサーバ３０２を呼び出し、認証要求の形式でログオン情報を送信する。アイデンティティサーバ３０２はその後、認証要求をアイデンティティプロバイダ３１６への要求に変換する。アイデンティティプロバイダ３１６による認証が成功すると、その後アイデンティティサーバ３０２は、ユーザおよび／またはユーザのロールに関連付けられている全ての拡張スクリプトを連続的に実行する。プログラム拡張３０８の少なくとも１つに基づいて、アイデンティティサーバは、それに応じた権利を付与する。アプリケーション３１４はその後、アプリケーションＡＰＩを介して付与された権利を通知される。

【００６０】

（ユーザ、ユーザプロファイル、およびスキーマ）

ユーザがログインする場合、ユーザは、特定のセキュリティコンテキストのための特定のセキュリティメカニズムを介してログインする。その特定のセキュリティメカニズムへの、およびその特定のセキュリティコンテキストへのログインに関するユーザの状態は、複数のフィールドにおいて捕捉されてよい。また、その特定のコンテキストに関するユーザのアイデンティティを備える追加のフィールドがユーザに関連付けられてよい。これらのフィールドのセットは、ユーザスキーマを構成する。

【００６１】

ユーザスキーマは、たとえばユーザネームおよびパスワードなどのデフォルトフィールドを有してよい。一方で、ユーザスキーマは、ダッシュボードに関して以下で説明されるように更にカスタマイズされてよく、またはプログラム拡張を介して動的にカスタマイズされてもよい。

【００６２】

ただし、ユーザは、常に人間であることが想定されるものではない。むしろ、ユーザは、独自のアカウントを有し得る他のメカニズムまたはプログラムであってよい。したがって、スキーマを静的および／または動的にカスタマイズする能力は、全く異なる種類のユーザのプロファイルを管理することを可能にし得る。たとえば人間などいくつかの分類のユーザは、ファーストネームおよびラストネームフィールドを当然有してよい。たとえば機械など他の分類のユーザは、機械識別子フィールドを有してよい。

【００６３】

（ランタイムおよびサンドボックス）

アイデンティティサーバの少なくとも一部は、サンドボックス、すなわち分離されたプログラム実行エリアにおいて実行されてよい。図４は、サンドボックス内で実行中のアイデンティティサーバの典型的なコンテキスト４００を示す。サンドボックスは拡張スクリプトエンジンによって動かされ、その拡張スクリプトがアイデンティティサービスのプログラム拡張を構成する。拡張スクリプトは全てのアイデンティティおよびクライアントリソースへのアクセスを有するので、サンドボックスは、プログラム拡張の構成要素である拡張スクリプトによって実行され得る変更の範囲を制限し得る。

【００６４】

アイデンティティサーバ４０２の設備は、仮想またはその他で、複数のホストサーバ４０４において配置されてよい。各ホストサーバ４０４に、１または複数のランタイム４０６および１または複数の対応するサンドボックス４０８実行エリアが存在してよい。アイデンティティサーバロジックのステートレス部分、たとえばプログラム拡張および接続は、様々なホストにコピーされてよい。したがって、要求４１０が設備に到来すると、それが第１の使用可能サーバに発送され得ることによって拡張性を支援する。アイデンティティサーバロジックのステートフル、または永続化部分は、互いにアクセス可能なデータス

トアまたはデータベースを備えたサーバ４１２に格納されてよい。認証要求はユーザに特有のものであるため、管理者は、データストアを複数のサーバに分割することを選択してよく、ここで、レコードはユーザによって分割される。アイデンティティサーバ４０２は任意選択的に、互いにフェイルオーバーし得る。１つの実施形態において、１つのアイデンティティサーバインスタンスはオンプレミスであってよく、別のアイデンティティサーバインスタンスはオフプレミスであってよい。どのアイデンティティサーバを使用するかに関する条件をプログラムでスクリプトすることによって、プログラム拡張の拡張スクリプトを介してローミングが実行され得る。

【００６５】

（ログインウィジェット）

アプリケーションプログラマに共通の課題は、ログオンダイアログボックスを開発することである。従来、各アプリケーションは、アプリケーションおよびアイデンティティプロバイダの各入れ替え（ｐｅｒｍｕｔａｔｉｏｎ）のための、カスタムビルトのダイアログを必要とした。オープン認証プロトコルの出現がプロセスを簡略化し、唯一の認証プロトコルが使用されるようになった。しかし、サービスとしてのアイデンティティの場合、複数の認証プロトコルおよび複数のアイデンティティプロバイダがアプリケーションによってアクセスされ得る。これによって、ユニバーサルログインウィジェットが可能になる。図５は、ユニバーサルログインウィジェットの図５００である。

【００６６】

ログインウィジェット５０２は、小さなコードスニペットを切り取りアプリケーションに貼り付けることによって実装され得るダイアログボックスである。コードスニペットにおいて、このサブセクションで説明されるようにログインウィジェットがカスタマイズされ得る。ログインウィジェット５０２はアイデンティティサーバ５０４を呼び出し、その設定に基づいて、アイデンティティプロバイダ５０６との１または複数の接続を利用し得る。たとえばログインウィジェット５０２は、たとえばグーグルプラス（登録商標）、フェイスブック（登録商標）、およびツイッター（登録商標）などの第三者認証サービス（不図示）を介した認証へのリンク５０８を含む。アイデンティティサーバ５０４を介したアイデンティティプロバイダ５０６の集中化により、ログインウィジェット５０２は、ログインウィジェットの属性を変更するだけで複数のアイデンティティプロバイダ５０６にアクセスし得る。

【００６７】

ログインウィジェット５０２はまた、ユーザネームテキストボックス５１０、パスワードテキストボックス５１２、およびログオンボタン５１４を備えるユーザ／パスワードログオンも含む。接続と同様、属性により、ログインウィジェット５０２のディスプレイおよびロジックを制御し得る。エンタープライズ接続が設定された場合、ユーザネームテキストボックス５１０は、電子メールアドレスを受け取るように設定される。データベース接続が存在する場合、パスワードテキストボックス５１２が自動的に表示され、任意選択的にサインアップ／パスワード紛失リンク５１４が表示される。リンク５１４をクリックすると、ユーザがサービスにサインアップする、および／またはパスワードを再設定することができるウェブセッションが開く。概して、ログインウィジェット５０２は、属性または接続の種類のいずれかに基づいて、どのフィールドを表示するか、またはどのような挙動を示すかを決定するためのロジックを含む。

【００６８】

ログインウィジェット５０２は、そのユーザのプロファイルに関するスキーマフィールドを作成するためのロジックを含んでよい。またログインウィジェット５０２は、プログラム拡張をトリガしてもよい。たとえば、ログオン時にユーザのプロファイルを作成するプログラム拡張が存在し得る。プロファイル内のフィールドの１つは、外部データによって作成されてよく、ユーザが特定の基準を満たすことを決定し得る。基準が満たされていることが決定されると、プログラム拡張は、自動電子メールメッセージをユーザへ送信し得る。その具体例として、ログインウィジェット５０２を介して新たなユーザが追加され

たことを決定し、その後、新しいユーザが特定のアプリケーション機能を利用するように促す挨拶／追跡電子メールを新しいユーザに送信する顧客関係管理プログラム拡張があってよい。

【００６９】

またログインウィジェット５０２は、単純に属性を設定することによって、カスタムタイトルおよび／またはロゴが表示され得るブランダブルタイトルバー５１８も含む。

【００７０】

（接続）

アイデンティティサーバは、拡張性に富んだモデルを提供する。アイデンティティサーバは、アイデンティティプロバイダの接続の種類にかかわらず、一貫したＡＰＩをアプリケーションに提示する。たとえば、フェイスブック（登録商標）などのソーシャルネットワークプロバイダが呼び出されるか、またはウィンドウズ（登録商標）認証を介したローカルＬＡＮかにかかわらず、アプリケーションは単純にアイデンティティサーバＡＰＩを呼び出すことに依存してよい。この拡張性は、接続のセットによって可能になる。

【００７１】

各接続は、特定のアイデンティティプロバイダおよび／またはアイデンティティプロバイダのプロトコルによって提示されるＡＰＩ単位のアイデンティティサーバＡＰＩの実装を含む。その結果、アイデンティティサーバＡＰＩは、新しいアイデンティティプロバイダおよび／またはセキュリティデリゲートへの新たな接続を迅速に実行するためのメカニズムを提供する。いくつかの場合、接続は、情報および／または機能を提供するためにアイデンティティサーバ以外のサーバまたは他の外部情報に頼る必要があり得る。たとえば、いくつかのＯＡｕｔｈ認証シナリオは、第三者プロバイダを利用し得る。

【００７２】

接続は、アイデンティティサーバに登録され、ＡＰＩを介してプログラムによって列挙され得る。プログラムによって接続を呼び出すために、コードは接続あるいは接続のための探索子（ｓｅａｒｃｈ）を列挙する。接続の機会を得ると、コードは、アイデンティティサーバＡＰＩを介して標準関数を呼び出し得る。

【００７３】

（ダッシュボード）

管理者は、アイデンティティサーバのコア能力を管理するために用いられる集中ダッシュボードへのアクセス権を有する。具体的には、管理者は、アイデンティティプロバイダ、複数のアプリケーション、複数のユーザ、および複数のプログラム拡張への複数の接続を追加し、互いに関連付けてよい。たとえば、Ｇメール（登録商標）へのアイデンティティプロバイダ接続は２つのアプリケーションに関連付けられてよく、それによってこれらのアプリケーションは、自身の認証スキームのためにＧメール（登録商標）認証を用いる。ユーザはロールに関連付けられ得る。ユーザおよび／またはロールは、特定のアプリケーションに対する権利を付与され得る。権利は、上述したように、プログラム拡張に従って制約されてよい。典型的なダッシュボード６００のトップレベルビューが図６に示され、規則エディタユーザインタフェース７００が図７に示される。

【００７４】

ダッシュボードは拡張スクリプトエディタ７０２を有し、これによってアイデンティティサービスへのプログラム拡張がもたらされる。プログラム拡張を構成する拡張スクリプトは最初からプログラムされていてよく、あるいは拡張スクリプトエディタ７０２が、変更されるテンプレート７０４、またはプログラム拡張のための拡張スクリプトを生成する各ステップを通してユーザを動的に助けるウィザードを提供してもよい。拡張スクリプトエディタ７０２によってスクリプトを作成することに加えて、管理者は、プログラムされた拡張スクリプトエディタ７０２内の拡張スクリプトをアップロードの前にテストおよび／またはデバッグしてよい。このように、拡張スクリプトエディタ７０２は、プログラム拡張およびそれらの構成要素である拡張スクリプトのための統合開発環境であると考えられ得る。

【００７５】
配置されると、拡張スクリプトは拡張スクリプトネームスペースに含まれ、たとえばボタン押下などのユーザ入力を受け取ると、拡張スクリプトエディタ７０２から呼び出される。拡張スクリプトエディタは、特定のユーザが認証されたか、および認証されている場合はどの権利が付与されたかを示す。このように、拡張スクリプトは、配置前にテストおよびデバッグされてよい。
【００７６】
またダッシュボード６００はユーザ管理も実行してよい。たとえば、ダッシュボード６００によって、管理者は、ユーザ情報を編集し、特定のセキュリティコンテキストに関するユーザプロファイル内のフィールドを定義するユーザプロファイルスキーマを拡張し、通知を送信し、セキュリティ委任を提供するためにユーザの承認されたなりすましを可能にし、ロール管理、グループ管理、およびアプリケーション管理を提供してよい。また、たとえばログインウィジェットに関してアプリケーションのルックアンドフィールをカスタマイズし、また場合によっては、アプリケーションのためのアイデンティティサービスにアクセスするためのアプリケーションプログラミングインタフェースおよび関連するプログラム通知イベントをカスタマイズするなど、アプリケーションはダッシュボードによってカスタマイズすることができる。
【００７７】
（サービスとしてのアイデンティティに関する典型的な使用事例）
（概観）
以下のサブセクションは、サービスとしてのアイデンティティを備えたアイデンティティおよび／またはセキュリティサービスの集中化によって可能になるいくつかの使用事例を説明する。
【００７８】
（オンプレミス／オフプレミス対称配置）
上述したように、従来技術の結果として、各アイデンティティプロバイダは独自のサイロ内に存在した。アイデンティティプロバイダのコンテキストの外側にあるアプリケーションがアクセスされた場合は常に、独自のクレデンシャルのセットによる個別のログオンが提示された。極端な例は、たとえばエンタープライズ認証などのオンプレミス認証、およびたとえばウェブサービスによるものなどのオフプレミス認証である。開発者の観点から見ると、各アイデンティティプロバイダおよびアプリケーションの入れ替えは、独自のカスタム認証コードベースを受け取るものであった。また、オフプレミスは従来オンプレミスと比べて安全性に欠けると見られていたため、オフプレミスコードはより限定的でヘビーウェイトである傾向があった。
【００７９】
しかし、サービスとしてのアイデンティティによって、セキュリティの実装は、アイデンティティサーバＡＰＩの下で取り除かれた。したがって、アプリケーションに関するコードベースは、オンプレミスからオフプレミスへ移植する際に変更する必要がない。このシナリオは、レガシーエンタープライズアプリケーションがパブリッククラウドへ移植される場合も共通である。
【００８０】
ログインウィジェットコードベースが再利用可能であるのと同様、属性およびコンテナコードのみを変更することによって、アプリケーションは最小限のコード変更で配置し得る。具体的には、アプリケーションの認証部分は、ログインウィジェットコードを使用するだけでよい。あるいはアプリケーションの認証部分は、それが過去にアイデンティティサーバＡＰＩに書き込まれている場合、コードベースの変更なしで単純に属性が変更されるだけでよい。最終的に、認証のための複雑なレガシーコードベースは、アイデンティティサーバおよび任意の指定されたアイデンティティプロバイダに認証を委任するコードに置き換えられ得る。このように、移植は、認証ロジックではなくアプリケーションロジックに重点を置いてよい。

【００８１】
アイデンティティプロバイダが中央アイデンティティサーバから一様にアクセスできるようになった結果は、パブリッククラウド内のアプリケーションはそれでもエンタープライズクレデンシャルによって認証され得ることである。なぜなら、アプリケーションがパブリッククラウド内にある場合でも、アプリケーションは認証のためにアイデンティティサーバを呼び出すからである。アイデンティティサーバが、オンプレミスエンタープライズアイデンティティプロバイダへの接続を有する場合、アプリケーションがパブリッククラウド内にある場合でも、アプリケーションはやはりエンタープライズアイデンティティプロバイダによって認証し得る。
【００８２】
（カスタマイズドサインアップ）
上述したように、ログインウィジェットは属性を提供し、それが設定されるとウェブサービスにサインアップするためまたはパスワードを再設定するためのウェブリンクがもたらされる。サインアップ／パスワード再設定機能は、ログインウィジェットおよびアイデンティティサーバのコンテキスト外で実行されるので、サインアップ／パスワード再設定機能に関する追加のデータ／メタデータを得ることは困難であり得る。
【００８３】
一方、アイデンティティサーバはアイデンティティデータに関する周知の位置を提供するので、サインアップ／パスワード再設定ウェブページは、捕捉されるカスタムフィールドを含むＨＴＭＬフィールドとともに実装され得る。ログインウィジェットは、通常のアプリケーションと同様に、ログインウィジェットをサインアップ／パスワード再設定ＨＴＭＬページに追加し、アイデンティティサーバへ追加のフィールドを送信するためのスクリプトを書き込んでもよい。スクリプトを提出イベントに結び付けることによって、追加のフィールドが作成されると、入力イベント（たとえば提出ボタンの押下）は追加のフィールドの対応する値をアイデンティティサーバへ送信させ得る。その後アイデンティティサーバがデータを解析し、追加のフィールドを認証レコードに関連付ける。たとえば、データはＪＳＯＮレコードの形式で到来してよく、その場合フィールドはユーザの電子メールおよびパスワードを含む。解析後、アイデンティティサーバは、その電子メールとパスワードとの組み合わせに追加のフィールドを関連付けてよい。
【００８４】
（支払い）
認証およびアイデンティティ機能を集中化することにより、ログオン使用ごとおよび認証スキームごとの支払いが可能になる。たとえば、アプリケーションは、Ｇメール（登録商標）を介した一部のユーザログオンおよびフェイスブック（登録商標）を介した他のユーザログオンを有してよい。開発者が、使用回数ごとに、または他の制約に基づいて（たとえば月極加入などのように時間ごとに）課金するアプリケーションを有する場合、ログオン時に今後の請求書作成のための課金レコードを書き込むように規則が実装され得る。あるいは、請求書を準備するためにユーザログオンの課金可能なインスタンスを列挙するために、別の課金アプリケーションがアイデンティティサーバに問い合わせてもよい。
【００８５】
あるいは、アイデンティティプロバイダは、そのアイデンティティプロバイダがアクセスされると常に課金レコードを書き込むようにアイデンティティサーバに規則を実装することによって自身のアクセスを収益化してよい。あるいは別の課金アプリケーションが、そのアイデンティティプロバイダを介したユーザログオンの課金可能なインスタンスを列挙するためにアイデンティティサーバに問い合わせ、それに従って請求書を準備してもよい。
【００８６】
（シングルサインオン）
アイデンティティサーバは、アプリケーションとアイデンティティプロバイダとの間に様々なカーディナリティを提供する。したがって、複数のアイデンティティプロバイダが

単一のアイデンティティプロバイダに委任するシングルサインオン（「ＳＳＯ」）は、アイデンティティサーバに当然備わるシナリオである。ＳＳＯは、複数のアイデンティティプロバイダを有する複数のアプリケーションを、１つのアイデンティティプロバイダに対する複数のアプリケーションに低減することで概念化され得る。

【００８７】

従来技術のＳＳＯに留まらず、アイデンティティサーバを介するＳＳＯは、オンプレミスであるかオフプレミスであるかにかかわらず複数のアイデンティティプロバイダを介してＳＳＯを提供する。具体的には、管理者は、たとえばエンタープライズプロバイダなどの特定のアイデンティティプロバイダをＳＳＯとして指定し、エンタープライズ認証（または指定されたＳＳＯアイデンティティプロバイダ）が認証した場合、他のアイデンティティプロバイダを介した認証を許可させるように規則を設定してよい。

【００８８】

（リンク付けアカウント）

リンク付けアカウントは、単一アプリ内のユーザが、異なる時間に異なるアイデンティティプロバイダを用いて認証し得るものである。したがって、リンク付けアカウントは、複数のアイデンティティプロバイダを有する単一アプリケーションのカーディナリティを有するものとして概念化され得る。具体的には、ユーザは、第１のアイデンティティプロバイダを用いてアプリケーションにログオンする。ユーザはその後アプリケーションから離れ、アプリケーションは時間切れになるとロックする。その後ユーザは、第２のプロバイダを用いて再びアプリケーションにログオンしてよい。同一のアイデンティティサーバによって認証が抽象化されるので、アプリケーションはユーザが離れた場所からアプリケーションセッションを再開し易く、シームレスな移行がもたらされ得る。

【００８９】

（多因子認証）

アイデンティティサーバは複数のアイデンティティプロバイダへのアクセスを有するので、アプリケーションは多因子認証を利用し得る。多因子認証は、ログオンプロセスが２つ以上の因子を利用するものである。この意図は、１セットのクレデンシャルよりも複数のクレデンシャルをハッキングする方が難しいという理由から、複数のクレデンシャルを提示するユーザは単一セットのクレデンシャルを提示するユーザよりも安全性が高いというものであり、なぜなら、１セットのクレデンシャルよりも複数のクレデンシャルをハッキングする方が難しいからである。

【００９０】

多因子認証において、ログオンダイアログが提示される。ユーザは、アイデンティティプロバイダに関する第１のクレデンシャルを入力する。成功すると、ユーザは、クレデンシャルの第２のセットを入力するように促される。ログオンダイアログは、第１の認証試行の成功または失敗を示すように外観を変更してもよいし、第１の認証試行から任意のプロンプトを削除してもよい。ユーザはその後、第２のクレデンシャルを入力してよい。認証が成功すると、任意の適用可能な規則を条件として、ユーザは彼または彼女の権利を受け取る。

【００９１】

たとえばユーザは、フェイスブック（登録商標）接続アイコンおよびＧメール（登録商標）接続アイコンを示すログオンダイアログを提示され得る。ユーザは、自身のフェイスブック（登録商標）クレデンシャルを入力する。成功すると、ユーザは、Ｇメール（登録商標）接続アイコンのみが示されたログオンダイアログを提示される。Ｇメール（登録商標）クレデンシャルの入力が成功すると、ユーザは自身の権利を受け取る。ただしこの例では、どちらのクレデンシャルもオフプレミスクレデンシャルであった。あるいは、オンプレミスアイデンティティプロバイダおよびオフプレミスアイデンティティプロバイダの両方を提供するダイアログが同様に提示されてもよい。

【００９２】

（所有者ユーザ管理機能／監査）

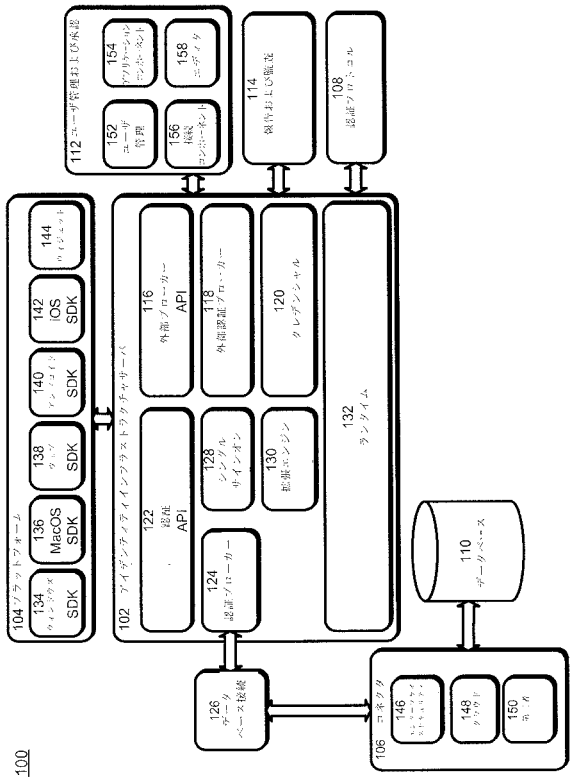
集中アイデンティティサーバは、オンプレミス認証およびオフプレミス認証の両方に関して認証レコードへのアクセスを有する。したがって、管理者は、オンプレミスであるかオフプレミスであるかにかかわらず、複数のアプリケーション、複数のアイデンティティプロバイダにわたり認証アクティビティに関する分析チャートをレビューし得る。図７は、いくつかの典型的な分析報告を提示する。統計報告７０２は、誰によってどのアプリケーションが最も頻繁に使用されているかの報告を示す。したがって、この報告は、利用行動研究のため、場合によっては指向性広告のために用いられ得る。監査報告７０４は、失敗したログオン試行を列挙する。複数のアイデンティティプロバイダについて報告されるので、管理者は、どのアイデンティティプロバイダが最も攻撃を受け、どのアイデンティティプロバイダが潜在的に最も弱いかを検出し得る。報告は、地図形式であってよい。地図位置報告７０６は、ログオン試行の位置の地図を提示する。たとえばオフィスおよび／またはユーザの既知の居住地から遠く離れた場所などの想定外の位置でログオン試行があった場合、管理者は、疑わしいアクティビティを暗示するかを決定し得る。

【００９３】

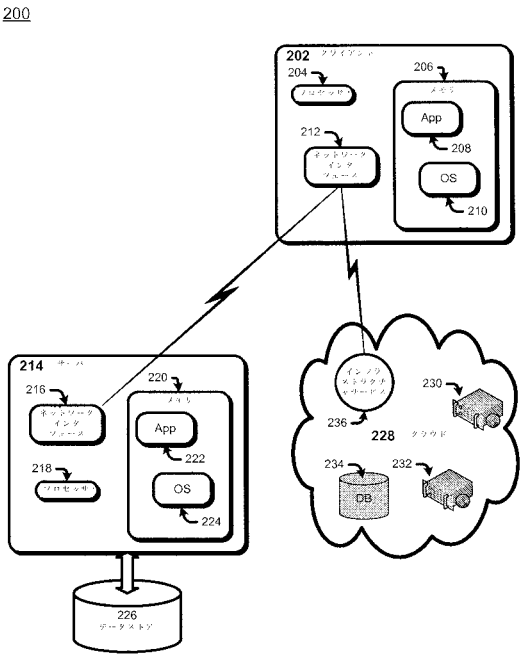
（結論）

主題事項は、構造的特徴および／または方法論的行為に特化した言葉で説明されたが、特許請求の範囲において定義される主題事項は必ずしも上述した特定の特徴または行為に限定されるものではないことを理解すべきである。むしろ、上述した特定の特徴または行為は、特許請求の範囲を実施する例示的な形態として開示されるものである。

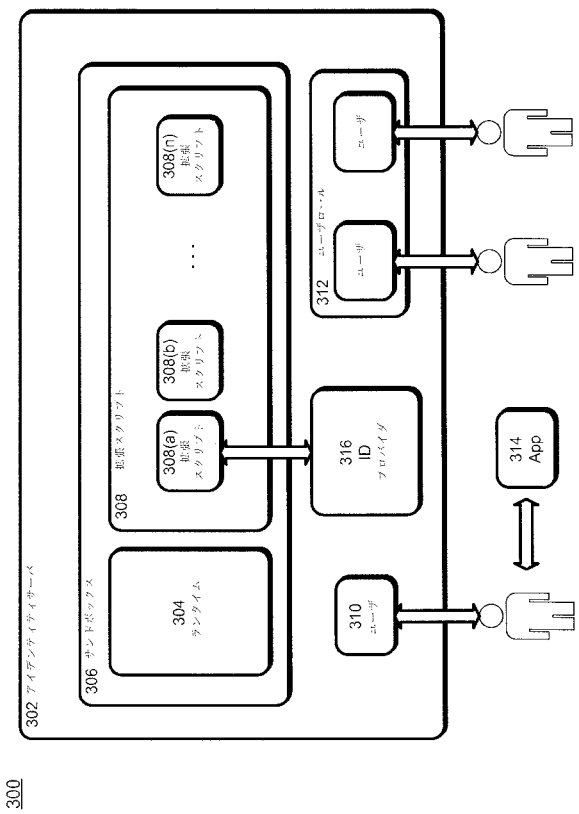
【図１】


100
104 プラットフォーム
134 ウィンドウズ SDK
136 MacOS SDK
138 リナックス SDK
140 アンドロイド SDK
142 iOS SDK
144 ウィジェット
102 アイデンティティインフラストラクチャサーバ
116 外部ブローカー API
118 外部認証ブローカー
120 クレデンシャル
122 認証 API
124 認証ブローカー
128 シングルサインオン
130 監査エンジン
132 ランタイム
110 データベース
112 ユーザ管理および承認
152 ユーザ管理
154 アプリケーション コンポーネント
156 権限コンポーネント
158 ポリシー
114 監査および報告
108 認証プロトコル
106 コネクタ
146 コネクタ
148 コネクタ
150 ポート
126 データベース接続

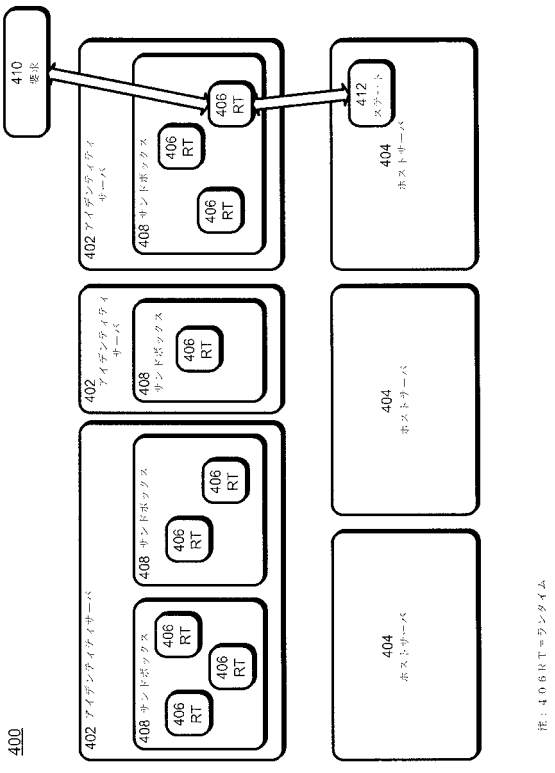
【図２】


200
202 クライアント
204 プロセッサ
206 メモリ
App 208
OS 210
212 ネットワーク インターフェース
214 サーバ
216 ネットワーク インターフェース
218 プロセッサ
220 メモリ
App 222
OS 224
226 データストア
228 クラウド
230
232
234 DB
236 ネットワーク インターフェース

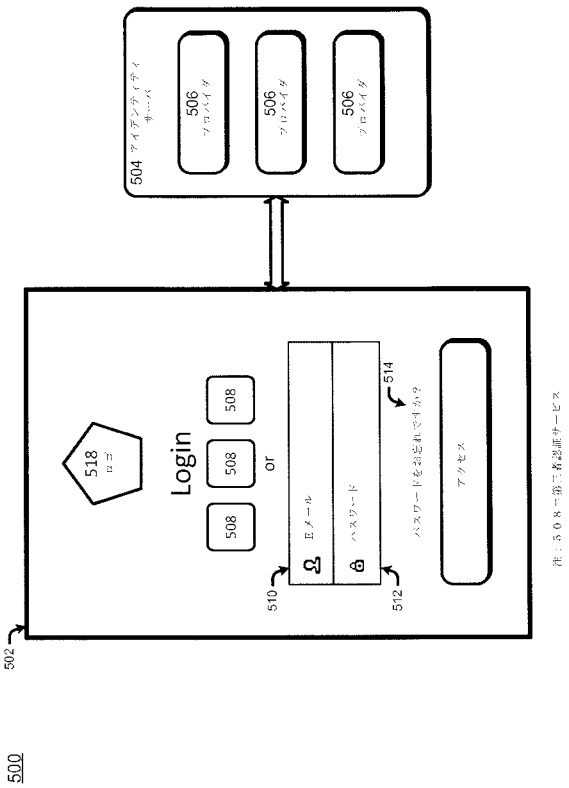
【図３】


300
302 アイデンティティサーバ
306 サンドボックス
304 ランタイム
308 拡張スクリプト
308(a) 拡張スクリプト
308(b) 拡張スクリプト
308(n) 拡張スクリプト
316 ID プロバイダ
310 ユーザ
312 ユーザプロトコル
ユーザ
ユーザ
314 App

【図４】


400
410 要求
402 アイデンティティサーバ
408 サンドボックス
406 RT
412 スクリプト
404 ホストサーバ
注：406RT＝ランタイム

【図５】



【図６】

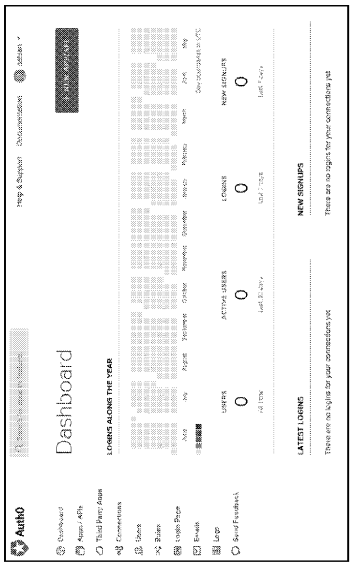


Figure 6

【図７】

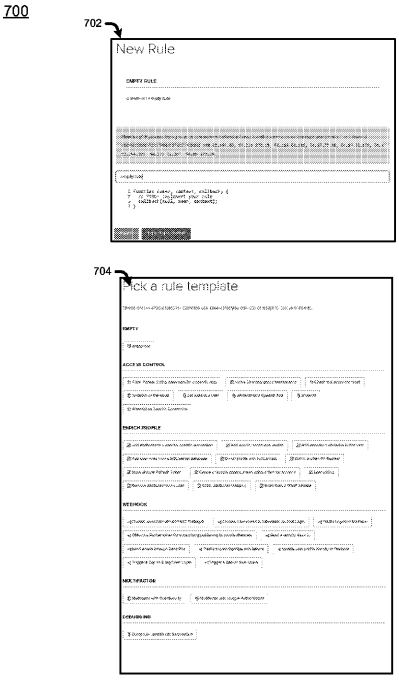
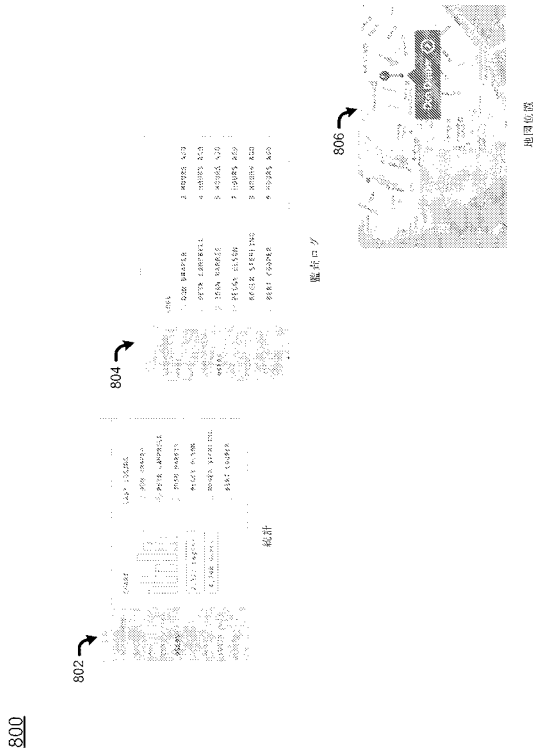


Figure 7

【図８】



【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US15/61438

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - H04L 9/32 (2016.01)
CPC - H04L 9/32
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)
IPC(8) Classification(s): H04L 9/32, 29/06; G06F 21/30, 17/30 (2016.01)
CPC Classification(s): H04L 9/32, 63/20, 63/0815, 63/0884, 63/08; G06F 21/30; H04W 12/06

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)
PatSeer (US, EP, WO, JP, DE, GB, CN, FR, KR, ES, AU, IN, CA, Other Countries (INPADOC), RU, AT, CH, TH, BR, PH); IEEE/IEEEXplore; Google/Google Scholar; IP.com; Keywords: authentication, request, server, proxy, shared, central, external, remote, identification, credentials, provider, interface, script, privileges, permissions, database, metadata, delegate, extension, script, protocol, format, single sign-on

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	US 2007/0277231 A1 (MEDVINSKY, G et al.) 29 November 2007; paragraphs [0019], [0040], [0041], [0059], [0061], [0075], [0090], [0099], [0102], [0106]	1-9, 12 --- 10, 11, 13, 14, 24, 25
X --- Y	US 2006/0288404 Al (KIRSHNAN, M et al.) 21 December 2006; paragraphs [0056], [0058], [0059], [0068], [0069], [0143]	15-17, 19-21, 23, 26 --- 10, 11, 13, 14, 18, 22, 24, 25
Y	US 2009/0293117 A1 (YAN, M et al.) 26 November 2009; paragraph [0033]	11
Y	US 2012/0266229 A1 (SIMONE, J et al.) 18 October 2012; paragraphs [0023], [0054]	11
Y	US 2007/0124490 A1 (KALAVADE, A et al.) 31 May 2007; paragraph [0064]	18, 22
A	US 2003/0145223 A1 (BRICKELL, E et al.) 31 July 2003; entire document	1-26

☐ 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
18 January 2016 (18.01.2016)	02 FEB 2016
Name and mailing address of the ISA/ Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-8300	Authorized officer Shane Thomas PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (January 2015)

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

(72)発明者 ペース，カルロス エウジェニオ
アメリカ合衆国，ワシントン州 ９８００４，ベルビュー，ノースイースト ８番 ストリート １０９００，スイート ７００，オース０ インコーポレイテッド内
(72)発明者 ウロスキー，マティアス
アメリカ合衆国，ワシントン州 ９８００４，ベルビュー，ノースイースト ８番 ストリート １０９００，スイート ７００，オース０ インコーポレイテッド内
(72)発明者 ローマニエロ，ホセ フェルナンド
アメリカ合衆国，ワシントン州 ９８００４，ベルビュー，ノースイースト ８番 ストリート １０９００，スイート ７００，オース０ インコーポレイテッド内