(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7459928号
(P7459928)

(45)発行日　令和6年4月2日(2024.4.2)

(24)登録日　令和6年3月25日(2024.3.25)

(51)国際特許分類

Ｇ０６Ｆ　21/41　(2013.01)		Ｇ０６Ｆ	21/41
Ｇ０６Ｆ　21/33　(2013.01)		Ｇ０６Ｆ	21/33

ＦＩ

請求項の数　21　（全29頁）

(21)出願番号　特願2022-508510(P2022-508510)
(86)(22)出願日　令和2年8月31日(2020.8.31)
(65)公表番号　特表2022-547402(P2022-547402A)
(43)公表日　令和4年11月14日(2022.11.14)
(86)国際出願番号　PCT/JP2020/032878
(87)国際公開番号　WO2021/049355
(87)国際公開日　令和3年3月18日(2021.3.18)
審査請求日　令和5年7月6日(2023.7.6)
(31)優先権主張番号　16/570,973
(32)優先日　令和1年9月13日(2019.9.13)
(33)優先権主張国・地域又は機関
米国(US)

(73)特許権者　000002185
ソニーグループ株式会社
東京都港区港南１丁目７番１号
(74)代理人　100121131
弁理士　西川 孝
(74)代理人　100082131
弁理士　稲本 義雄
(74)代理人　100168686
弁理士　三浦 勇介
(72)発明者　村尾 貞佳
インド カルナータカ州、５６０ １０３、バンガロール市 ヴァルツルホブリ、デヴァラベサネハリ、アウターリンクロード エンバシー テク ヴィレッジ、ハイビスカス タワー２ ２階 ソニーイン
最終頁に続く

(54)【発明の名称】　複数の認証オプションによるシングルサインオン（ＳＳＯ）認証

(57)【特許請求の範囲】
【請求項１】
ハイブリッド認証システムであって、
ウェブアプリケーションサーバおよびスマートコントラクトを記憶する公開台帳に通信可能に結合されている制御回路を備え、
前記制御回路は、
リソースサーバ上のセキュアコンテンツにアクセスすることを求める要求を前記ウェブアプリケーションサーバから受信することと、
前記受信される要求に基づいてユーザデバイスのユーザインターフェース上のユーザ選択可能オプションのセットの表示を制御することであって、
前記ユーザ選択可能オプションのセットは、ウェブベースの認証方式およびウォレットベースの認証方式に相当し、
前記ウォレットベースの認証方式は、前記公開台帳上の前記記憶されているスマートコントラクトに基づく、制御することと、
規定のセキュリティ基準または前記ユーザ選択可能オプションの表示されているセットのうちの１つを介したユーザ入力に基づいて、前記ウェブベースの認証方式および前記ウォレットベースの認証方式のうちの１つを認証方式として選択することと、
前記選択された認証方式に基づいて、前記受信される要求の認証を制御することと
を行うように構成されている、ハイブリッド認証システム。
【請求項２】

前記ウェブアプリケーションサーバは、少なくとも１つのウェブアプリケーションをホストし、
前記ウェブアプリケーションサーバは、前記少なくとも１つのウェブアプリケーションへのシングルサインオン（ＳＳＯ）アクセスを求めるユーザ開始要求の受信に基づいて前記要求を提供する、請求項１に記載のハイブリッド認証システム。
【請求項３】
前記スマートコントラクトは、ウォレットアドレス、前記リソースサーバのアクセストークン、ユーザ識別子、およびステータス識別子を記憶する自己実行可能プログラムであり、
前記ウォレットアドレスは、前記公開台帳上のユーザのウォレットアカウントのためのものであり、
前記ステータス識別子は、前記ユーザのウォレットアカウントの前記ウォレットアドレスまたはウォレットアイデンティティ（ＩＤ）のうちの一方が、アイデンティティプロバイダのウェブＩＤにリンクされているか、またはリンクされていないことを示す、請求項１に記載のハイブリッド認証システム。
【請求項４】
前記リソースサーバは、アイデンティティプロバイダによって管理されるアプリケーションプログラミングインターフェース（ＡＰＩ）サーバであり、
前記リソースサーバは、前記セキュアコンテンツとしてユーザ固有の情報を記憶する、請求項１に記載のハイブリッド認証システム。
【請求項５】
前記ウェブアプリケーションサーバは、前記ユーザデバイスのウェブクライアントからのユーザのアクセス要求に基づいて、前記ハイブリッド認証システムにアクセス要求およびユーザ登録詳細を送信する、請求項１に記載のハイブリッド認証システム。
【請求項６】
前記制御回路は、
前記ウェブアプリケーションサーバによって送信される前記アクセス要求および前記ユーザ登録詳細を受信することと、
前記受信されるアクセス要求の認証のために、前記受信されるアクセス要求をアイデンティティプロバイダにリダイレクトすることと、
前記受信されるアクセス要求の認証に基づいて前記アイデンティティプロバイダからアクセストークンを受信することと
を行うようにさらに構成されている、請求項５に記載のハイブリッド認証システム。
【請求項７】
前記制御回路は、
前記受信されるアクセストークンおよび前記受信されるユーザ登録詳細を、前記スマートコントラクトを介して前記公開台帳に安全に記憶することと、
前記スマートコントラクト内のステータス識別子をリンクされていないものとして更新することであって、前記更新されているステータス識別子は、ユーザのウォレットアカウントのウォレットアドレスまたはウォレットアイデンティティ（ＩＤ）のうちの一方が前記アイデンティティプロバイダのウェブＩＤにリンクされていないことを示す、更新することと
を行うようにさらに構成されている、請求項６に記載のハイブリッド認証システム。
【請求項８】
前記制御回路は、
イベントリスナを前記公開台帳に展開することと、
前記展開されたイベントリスナによって、前記公開台帳上の前記記憶されたスマートコントラクトに関連付けられた１つまたは複数のイベントを検出することと
を行うようにさらに構成されている、請求項７に記載のハイブリッド認証システム。
【請求項９】

前記制御回路は、
前記公開台帳上の前記検出された１つまたは複数のイベントに基づいて、前記アイデンティティプロバイダによる前記受信されるアクセストークンの有効性検証要求を開始することと、
前記開始された検証要求に対する前記アイデンティティプロバイダの応答を受信することと、
前記受信された応答に基づいて前記受信されたアクセストークンの有効性を検証するように構成されている、請求項８に記載のハイブリッド認証システム。
【請求項１０】
前記制御回路は、
前記受信されるアクセストークンの前記有効性検証に基づいて、アイデンティティプロバイダのウェブＩＤを、前記公開台帳上の前記ユーザのウォレットアカウントのウォレットアドレスまたはウォレットＩＤとリンクさせることと、
前記リンクに基づいて前記スマートコントラクト内の前記ステータス識別子をリンクされているものとして更新することと
を行うようにさらに構成されている、請求項９に記載のハイブリッド認証システム。
【請求項１１】
前記制御回路は、
相当する複数のアイデンティティプロバイダの複数のウェブＩＤを、前記公開台帳上の前記ユーザのウォレットアカウントのウォレットアドレスまたはウォレットＩＤとリンクさせることと、
前記リンクに基づいて前記スマートコントラクト内の前記ステータス識別子をリンクされているものとして更新することと
を行うようにさらに構成されている、請求項９に記載のハイブリッド認証システム。
【請求項１２】
前記制御回路は、
前記ウェブベースの認証方式の選択のために前記表示されたユーザ選択可能オプションのセットの第１のユーザ選択可能オプションを介して前記ユーザ入力を受信することと、
前記受信されるユーザ入力に基づいて前記ウェブベースの認証方式として前記認証方式を選択することと、
前記ウェブベースの認証方式に従って前記受信される要求の前記認証を制御することと
を行うようにさらに構成されており、
前記ウェブベースの認証方式は、Ｏａｕｔｈプロトコルに基づく、請求項１に記載のハイブリッド認証システム。
【請求項１３】
前記制御回路は、
前記ウォレットベースの認証方式の選択のために前記表示されたユーザ選択可能オプションのセットの第２のユーザ選択可能オプションを介して前記ユーザ入力を受信することと、
前記受信されるユーザ入力に基づいて前記ユーザデバイスのウェブクライアント上でプロンプトをトリガすることであって、
前記プロンプトは、ユーザのウォレットアカウントのウォレットアドレスおよび前記ウォレットアドレスに関連付けられた秘密鍵を使用して、前記ユーザのウォレットアカウントへのユーザログインを可能にするようにトリガされる、トリガすることと、
前記ユーザデバイス上の前記ウェブクライアントを介して、前記ユーザのウォレットアカウントへの前記ユーザログインを検出することと、
前記ウォレットアドレスに関連付けられた公開鍵、前記ユーザログインの前記検出、および前記記憶されているスマートコントラクトに基づいて、前記受信される要求の前記認証を制御することと
を行うようにさらに構成されており、

前記公開鍵は、前記ハイブリッド認証システムに記憶される、請求項１に記載のハイブリッド認証システム。
【請求項１４】
前記制御回路は、前記受信される要求の前記認証に基づいてアクセス認証情報を前記ウェブアプリケーションサーバと共有するようにさらに構成されている、請求項１に記載のハイブリッド認証システム。
【請求項１５】
前記ウェブアプリケーションサーバは、
前記共有認証情報を使用して前記リソースサーバ上の前記セキュアコンテンツにアクセスすることと、
前記アクセスされたセキュアコンテンツに基づいて前記ユーザデバイスのウェブクライアント上の前記ウェブアプリケーションのセッションを初期化することと、
前記初期化されたセッションにセッションＩＤを割り当てることであって、前記割り当てられるセッションＩＤはウェブベースのログインに基づくサインオンのセッションＩＤと同一である、割り当てることと
を行う、請求項１４に記載のハイブリッド認証システム。
【請求項１６】
前記制御回路は、前記受信される要求の前記認証に基づいてユーザプロファイルイメージを構築するようにさらに構成されており、前記ユーザプロファイルイメージは、前記ウェブアプリケーションサーバ上でホストされている少なくとも１つのウェブアプリケーションのアプリケーション統一資源位置指定子（ＵＲＬ）、認証タイプ、アイデンティティプロバイダ名、アクセストークンに事前に割り当てられている有効期間、および再認証ステータスを含む、請求項１に記載のハイブリッド認証システム。
【請求項１７】
前記規定のセキュリティ基準は、前記ウェブアプリケーションサーバ上でホストされている少なくとも１つのウェブアプリケーションのうちの特定のウェブアプリケーションについての規定のセキュリティレベル、前記特定のウェブアプリケーションについてのユーザが選好する認証方式、または前記ウェブベースの認証方式もしくは前記ウォレットベースの認証方式のうちの１つに基づいて以前に試みられた前記認証の失敗ステータスを含む、請求項１に記載のハイブリッド認証システム。
【請求項１８】
方法であって、
ウェブアプリケーションサーバおよびスマートコントラクトを記憶する公開台帳に通信可能に結合されているハイブリッド認証システムにおいて、
リソースサーバ上のセキュアコンテンツにアクセスすることを求める要求を前記ウェブアプリケーションサーバから受信することと、
前記受信される要求に基づいてユーザデバイスのユーザインターフェース上のユーザ選択可能オプションのセットの表示を制御することであって、
前記ユーザ選択可能オプションのセットは、ウェブベースの認証方式およびウォレットベースの認証方式に相当し、
前記ウォレットベースの認証方式は、前記公開台帳上の前記記憶されているスマートコントラクトに基づく、制御することと、
規定のセキュリティ基準または前記ユーザ選択可能オプションの表示されているセットのうちの１つを介したユーザ入力に基づいて、前記ウェブベースの認証方式および前記ウォレットベースの認証方式のうちの１つを認証方式として選択することと、
前記選択された認証方式に基づいて、前記受信される要求の認証を制御することと
を含む、方法。
【請求項１９】
前記ウェブベースの認証方式の選択のために前記表示されたユーザ選択可能オプションのセットの第１のユーザ選択可能オプションを介して前記ユーザ入力を受信することと、

前記受信されるユーザ入力に基づいて前記ウォレットベースの認証方式として前記認証方式を選択することと、
前記ウェブベースの認証方式に従って前記受信される要求の前記認証を制御することと
をさらに含み、
前記ウェブベースの認証方式は、Ｏａｕｔｈプロトコルに基づく、請求項１８に記載の方法。
【請求項２０】
前記ウォレットベースの認証方式の選択のために前記表示されたユーザ選択可能オプションのセットの第２のユーザ選択可能オプションを介して前記ユーザ入力を受信することと、
前記受信されるユーザ入力に基づいて前記ユーザデバイスのウェブクライアント上でプロンプトをトリガすることであって、
前記プロンプトは、ユーザのウォレットアカウントのウォレットアドレスおよび前記ウォレットアドレスに関連付けられた秘密鍵を使用して、前記ユーザのウォレットアカウントへのユーザログインを可能にするようにトリガされる、トリガすることと、
前記ユーザデバイス上の前記ウェブクライアントを介して、前記ユーザのウォレットアカウントへの前記ユーザログインを検出することと、
前記ウォレットアドレスに関連付けられた公開鍵、前記ユーザログインの前記検出、および前記記憶されているスマートコントラクトに基づいて、前記受信される要求の前記認証を制御することと
をさらに含み、
前記公開鍵は、前記ハイブリッド認証システムに記憶される、請求項１８に記載の方法。
【請求項２１】
ハイブリッド認証システムによって実行されると、前記ハイブリッド認証システムに動作を実行させるコンピュータ実行可能命令を記憶されている非一時的コンピュータ可読媒体であって、前記動作は、
リソースサーバ上のセキュアコンテンツにアクセスすることを求める要求をウェブアプリケーションサーバから受信することと、
前記受信される要求に基づいてユーザデバイスのユーザインターフェース上のユーザ選択可能オプションのセットの表示を制御することであって、
前記ユーザ選択可能オプションのセットは、ウェブベースの認証方式およびウォレットベースの認証方式に相当し、
前記ウォレットベースの認証方式は、公開台帳上のスマートコントラクトに基づく、制御することと、
規定のセキュリティ基準または前記ユーザ選択可能オプションの表示されているセットのうちの１つを介したユーザ入力に基づいて、前記ウェブベースの認証方式および前記ウォレットベースの認証方式のうちの１つを認証方式として選択することと、
前記選択された認証方式に基づいて、前記受信される要求の認証を制御することと
を含む、非一時的コンピュータ可読媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本開示の様々な実施形態は、認証技術に関する。より具体的には、本開示の様々な実施形態は、複数の認証オプションによるシングルサインオン（ＳＳＯ）認証のためのシステムおよび方法に関する。
【０００２】
＜関連出願の相互参照／参照による組み込み＞
なし。
【背景技術】
【０００３】

認証技術の進歩により、ユーザに様々な認証オプションが提供されている。従来、場合によっては、ユーザはシングルサインオン（ＳＳＯ）機能を使用することを選択することができ、それによってユーザは単一のユーザアカウント（例えば、電子メールまたはソーシャルメディアアカウント）に基づいて異なるアプリケーションにサインオンする柔軟性を有する。いくつかの他の例では、安全性の低い環境での認証のための抽象化およびセキュリティの追加の層を追加するために、複数の認証オプションも組み込まれる。例えば、ＳＳＯ認証オプションおよびワンタイムパスワード（ＯＴＰ）ベースの認証オプションによる２要素認証である。従来の認証オプションのほとんどは、多くの場合、重要なもしくは重要でないユーザ情報の損失の可能性を残す安全性の低い方法でユーザを認証するか、またはユーザにとって望ましくないもしくは許容できない煩わしさを生じさせる。

【０００４】

本出願の残りの部分に、および、図面を参照して説明される本開示のいくつかの態様との記載されたシステムの比較を通して、慣習的な手法および従来の手法のさらなる制限および欠点が当業者に明らかになるであろう。

【発明の概要】

【０００５】

複数の認証オプションによるシングルサインオン（ＳＳＯ）認証のためのシステムおよび方法が、特許請求の範囲により完全に記載されているように、図面の少なくとも１つに実質的に示され、かつ／またはそれに関連して説明されているように、提供される。

【０００６】

本開示のこれらのおよび他の特徴および利点は、本開示の以下の詳細な説明を、添付の図面とともに検討することによって理解され得る。図面において、同様の参照符号は全体にわたって同様の部分を指す。

【図面の簡単な説明】

【０００７】

【図１】本開示の一実施形態による、複数の認証オプションによるＳＳＯ認証のための例示的なネットワーク環境を示す図である。

【図２】本開示の一実施形態による、複数の認証オプションによるＳＳＯ認証のための例示的なハイブリッド認証システムを示すブロック図である。

【図３Ａ】図３Ｂとまとめて、本開示の一実施形態による、アイデンティティプロバイダのウェブＩＤをユーザのウォレットアカウントにリンクさせるためのシーケンス図である。

【図３Ｂ】図３Ａとまとめて、本開示の一実施形態による、アイデンティティプロバイダのウェブＩＤをユーザのウォレットアカウントにリンクさせるためのシーケンス図である。

【図４Ａ】図４Ｂとまとめて、本開示の一実施形態による、複数の認証オプションによるＳＳＯ認証のためのシーケンス図である。

【図４Ｂ】図４Ａとまとめて、本開示の一実施形態による、複数の認証オプションによるＳＳＯ認証のためのシーケンス図である。

【図５】本開示の一実施形態による、ユーザ識別子と、複数のユーザアカウントと、複数のウェブアカウントまたは複数のウェブＩＤとの間の関連付けを示す例示的な図である。

【図６】本開示の一実施形態による、複数の認証オプションによるＳＳＯ認証のための例示的な方法を示す流れ図である。

【発明を実施するための形態】

【０００８】

以下に説明される実施態様は、複数の認証オプションによるシングルサインオン（ＳＳＯ）認証のための開示されたシステムおよび方法に見出すことができる。本開示の例示的な態様は、ＳＳＯ認証のためのハイブリッド認証システムを提供する。ハイブリッド認証システムは、ウェブアプリケーションの複数の認証オプションをユーザに提供するシングルサインインシステムであり得る。例として、ハイブリッド認証システムは、２つの認証オプション、すなわちウェブベースの認証およびウォレットベースの認証を提供する。ウェブベースの認証は、Ｏａｕｔｈプロトコルに基づくことができ、それによって、Ｏａｕ

ｔｈサーバ等のアイデンティティプロバイダは、リソースサーバ（ＡＰＩサーバとも呼ばれる）上のユーザ固有の情報にアクセスすることを求める要求の認証を担当することができる。一方、ウォレットベースの認証は、公開台帳に記憶されたスマートコントラクトと、公開台帳上のユーザのウォレットアカウントに関連付けられた秘密鍵とに基づくことができる。スマートコントラクトは、アイデンティティプロバイダによって事前共有されたアクセストークンと、ユーザのウォレットアカウントのウォレットアドレスと、ユーザのウォレットアカウントがアイデンティティプロバイダのウェブＩＤ（またはウェブアカウント）にリンクされているか否かを示すステータス識別子とを記憶することができる。

【０００９】

ハイブリッド認証システムは、２要素認証または２要素認証のうちの一方、すなわちウェブベースの認証とウォレットベースの認証のうちの一方または両方を選択する柔軟性をユーザに提供する。例えば、ユーザは通常のログイン認証情報（例えば、電子メールＩＤ／電話番号およびパスワード）を使用してウェブアプリケーションに対してＳＳＯを行う柔軟性を有するか、または、ユーザはユーザのウォレットアカウントのウォレットＩＤおよび秘密鍵を使用して公開台帳上のユーザのウォレットアカウントにログインすることでウェブアプリケーションに対してＳＳＯを行うことができる。付加的または代替的に、セキュリティ基準は、２要素認証を選択するかまたは２要素認証のうちの一方を選択するかに基づいて定義されてもよい。例として、セキュリティ基準は、ウェブアプリケーションサーバ上でホストされている特定のウェブアプリケーションについての規定のセキュリティレベル（例えば、ユーザ定義のセキュリティレベル）、特定のウェブアプリケーションについてのユーザが選好する認証、またはウェブベースの認証もしくはウォレットベースの認証のうちの１つに基づいて以前に試みられた認証の失敗ステータスを含むことができる。ウォレットベースの認証に基づくＳＳＯアクセスの場合、ユーザデバイスのウェブクライアント上の初期化されたセッションが、ウェブベースのログインに基づいて初期化されたセッションのセッションＩＤとして発行され得る。したがって、ウェブアプリケーションへのサインオン後、認証オプションのいずれかの選択にかかわらず、クライアント側インターフェースの状態はユーザにとって同一のままであり得る。

【００１０】

図１は、本開示の一実施形態による、複数の認証オプションによるＳＳＯ認証のための例示的なネットワーク環境を示す図である。図１を参照すると、ネットワーク環境１００が示されている。ネットワーク環境１００は、ハイブリッド認証システム１０２と、ウェブアプリケーションサーバ１０４と、ウェブアプリケーションサーバ１０４上でホストされるウェブアプリケーション１０６とを含む。ネットワーク環境１００は、リソースサーバ１０８と、アイデンティティプロバイダ１１０と、公開台帳１１２と、例えば、ウェブブラウザ等のウェブクライアント１１４ａをホストするユーザデバイス１１４とをさらに含む。ＳＳＯクライアント１０６ａおよびＳＳＯクライアント１０８ｂが、それぞれウェブアプリケーション１０６およびリソースサーバ１０８上に存在することができる。ネットワーク環境１００は、通信ネットワーク１１６をさらに含む。通信ネットワーク１１６は、ネットワーク環境１００の複数のコンピューティングデバイス間で確立することができる。例として、通信ネットワーク１１６は、ハイブリッド認証システム１０２、ウェブアプリケーションサーバ１０４、アイデンティティプロバイダ１１０、リソースサーバ１０８、公開台帳１１２、およびユーザデバイス１１４の間にあってもよい。ユーザデバイス１１４に関連付けられたユーザ１１８がさらに示されている。

【００１１】

ハイブリッド認証システム１０２は、リソースサーバ１０８上のセキュアコンテンツ１０８ａへのアクセスを要求するユーザおよび／またはウェブアプリケーションのためのアイデンティティ（ＩＤ）管理に関連する動作を実行するように構成することができる適切なロジック、回路、およびインターフェースを備えることができる。ハイブリッド認証システム１０２は、リソースサーバ１０８上のセキュアコンテンツ１０８ａにアクセスすることを求める要求の認証および／または認証レベル（例えば、単一要素または２要素認証

）を制御するように構成することができる。一例として、要求は、ウェブアプリケーションサーバ１０４上でホストされている少なくとも１つのウェブアプリケーション（ウェブアプリケーション１０６等）へのＳＳＯアクセスを求める、ユーザ開始要求の受信に基づいてウェブアプリケーションサーバ１０４によって提供されてよい。さらに、ハイブリッド認証システム１０２は、要求の認証状態の維持ならびにユーザおよび／またはウェブアプリケーションのアクセスプロファイル管理に関連する動作を処理することができる。ハイブリッド認証システム１０２の例は、サーバ、サーバの分散ネットワーク、コンピューティングデバイス、メインフレームマシン、コンピュータワークステーション、および／または家電（ＣＥ）デバイスを含むことができるが、これらに限定されない。

【００１２】

ウェブアプリケーションサーバ１０４は、少なくとも１つのウェブアプリケーションをホストするように構成することができる適切なロジック、回路、およびインターフェースを備えることができる。例として、ウェブアプリケーションサーバ１０４は、ウェブアプリケーション１０６のサーバ側ロジック、サーバ側プログラム、およびアプリケーションデータをホストすることができる。ユーザ１１８がウェブクライアント１１４ａを介してウェブアプリケーション１０６の機能にアクセスするようにウェブアプリケーションサーバ１０４に要求するときはいつでも、ウェブアプリケーションサーバ１０４は、要求を満たすようにウェブアプリケーションのサーバ側プログラムおよびサーバ側ロジックを実行する。ウェブアプリケーションサーバ１０４の例は、サーバ、リモートサーバ、コンピューティングデバイス、メインフレームマシン、コンピュータワークステーション、および／または家電（ＣＥ）デバイスを含むことができるが、これらに限定されない。

【００１３】

ウェブアプリケーション１０６は、クライアント－サーバコンピュータ実装プログラムであってもよく、例えば、クライアント側インターフェース、クライアント側ロジック、サーバ側プログラム、およびサーバ側ロジックを含んでもよい。ウェブアプリケーション１０６は、ウェブアプリケーションサーバ１０４上でホストされる１つまたは複数のウェブアプリケーションのうちの１つであってもよい。例として、クライアント側インターフェースは、ウェブブラウザにロードされているウェブページであってもよい。クライアント側ロジックは、ＡＳＰ、ＪＳＰ／Ｊａｖａ、Ｎｏｄｅ．ｊｓ、ＰＨＰ、またはＰｙｔｈｏｎ等のウェブ技術を使用して、ウェブページから要求を受信し、サーバ側プログラムのクエリ、更新、またはアクションとして要求を処理するプログラムであってもよい。ウェブアプリケーション１０６の例は、ウェブブラウザにロードアップするウェブページベースのアプリケーション、モバイルアプリケーション、ネイティブウェブアプリケーション、デスクトップベースのウェブアプリケーションを含むことができるが、これらに限定されない。

【００１４】

ＳＳＯクライアント１０６ａはウェブアプリケーションサーバ１０４上でホストされるウェブアプリケーション１０６上に存在するアプリケーションであってよい。ＳＳＯクライアント１０６ａは、ウェブアプリケーション１０６および／またはユーザデバイス１１４のウェブクライアント１１４ａとのアクセス、対話、および／または情報交換のためにハイブリッド認証システム１０２へのインターフェースを提供することができる。例として、ＳＳＯクライアント１０６ａはウェブブラウザ（すなわち、ウェブクライアント１１４ａ）を介してユーザにＳＳＯアクセスに関連する一連のサービスを提供することができる。ハイブリッド認証システム１０２上のＳＳＯエージェント（図１には図示せず）はＳＳＯクライアント１０６ａと通信することができる。一例として、ＳＳＯクライアント１０６ａは、ハイブリッド認証システム１０２がユーザデバイス１１４のウェブクライアント１１４ａからユーザ認証情報を取り出すこと、またはウェブアプリケーション１０６へのＳＳＯアクセスのためのユーザ認証情報を提供するようユーザをトリガするユーザインターフェースをプッシュすることを可能にできる。

【００１５】

リソースサーバ１０８は、セキュアコンテンツ１０８ａ、例えば、ユーザ１１８に関連するユーザ固有情報または個人識別情報（ＰＩＩ）を記憶するように構成することができる適切なロジック、回路、およびインターフェースを備えることができる。セキュアコンテンツ１０８ａは、ユーザ１１８のアイデンティティを確立するのに十分であり得る。例として、Ｏａｕｔｈ ２．０により、リソースサーバ１０８は、アプリケーションプログラミングインターフェース（ＡＰＩ）サーバとも称することができ、セキュアコンテンツ１０８ａにアクセスするための有効なアクセス認証情報を有するウェブアプリケーションの認証に関する要求を処理するように構成することができる。

【００１６】

アイデンティティプロバイダ１１０は、ウェブアプリケーション１０６がリソースサーバ１０８からのセキュアコンテンツ１０８ａにアクセスすることを可能にするために、ユーザ１１８に代わってウェブアプリケーション１０６にアクセス認証情報を発行するサーバ、サーバのネットワーク、オンラインサービス、またはウェブサイトであってよい。また、アイデンティティプロバイダ１１０は、クライアントとしてウェブアプリケーション１０６にサービスとしてのＳＳＯを提供することもできる。リソースサーバ１０８は、アイデンティティプロバイダ１１０によって管理することができる。Ｏａｕｔｈベースの認証の場合、アイデンティティプロバイダ１１０は、ウェブアプリケーション１０６に対してユーザ１１８に代わってアクセス認証情報を発行することができるＯａｕｔｈサーバであってもよい。アイデンティティプロバイダ１１０の例は、電子メールサービスプロバイダ、ソーシャルメディアネットワーク、または他のウェブベースのログインサービスを含むことができるが、これらに限定されない。

【００１７】

公開台帳１１２は、データ操作またはトランザクションの不変レコードを維持する非集中的、分散型で、公開のデータベースシステムであってもよい。データ操作のセットは、ブロックとしてともにグループ化することができ、チェーンを形成するためにデータ操作の以前のブロックにさらにリンクさせることができる。データ操作のすべてのブロックは非集中的に記憶することができ、それによってすべての参加者またはパブリックノードはすべてのブロックを記憶する。さらに、公開台帳１１２は、複数の当事者の間、例えば、ユーザとハイブリッド認証システム１０２との間のスマートコントラクトの展開を可能にするオペレーティングシステムを含むことができる。本明細書において、スマートコントラクトは、公開台帳１１２上で実行することができる自己実行可能プログラムまたはコンピュータコードとすることができ、スマートコントラクトの複数の当事者が互いに対話することに同意する条件のセットを含むことができる。スマートコントラクトは、公開台帳１１２上の特定のアドレスに記憶することができ、コンピュータコード（すなわち、関数）およびデータ（すなわち、アカウントの状態）の集合とすることができる。

【００１８】

例として、公開台帳１１２は、状態オブジェクトとしてアカウントを使用するＥｔｈｅｒｅｕｍブロックチェーンであってもよく、各アカウントの状態は、Ｅｔｈｅｒｅｕｍブロックチェーンによって追跡することができる。本明細書において、アカウントは、ユーザ、マイニングノード、または自動化エージェントのアイデンティティを表す。データ操作のすべてのブロックまたはスマートコントラクトは、Ｅｔｈｅｒｅｕｍブロックチェーン上のアカウントに関連付けられている。

【００１９】

ユーザデバイス１１４は、ユーザデバイス１１４上のウェブクライアント１１４ａを介してウェブアプリケーション１０６にアクセスするように構成することができる適切なロジック、回路、およびインターフェースを備えることができる。例えば、ウェブクライアント１１４ａは、マルチメディアストリーミングアプリケーションのクライアント側インターフェースをロードアップするウェブブラウザであってもよい。ユーザデバイス１１４上のウェブクライアント１１４ａは、例えば、ソーシャルメディアアカウントや電子メールアカウント等の、アイデンティティプロバイダ１１０によってリソースサーバ１０８上

で維持されるユーザ１１８のアイデンティティ情報／認証情報に基づいて、マルチメディアストリーミングアプリケーションへのＳＳＯアクセスに対するユーザ開始要求を生成する規定を有することができる。ユーザデバイス１１４は、ウェブクライアント１１４ａとウェブアプリケーションサーバ１０４および／またはハイブリッド認証システム１０２との通信を容易にするための適切な入出力（Ｉ／Ｏ）機能およびネットワーキング機能を含むことができる。ユーザデバイス１１４の例は、コンピューティングデバイス、携帯電話、スマートフォン、コンピュータワークステーション、および／または任意の家電（ＣＥ）デバイスを含むことができるが、これらに限定されない。

【００２０】

ウェブクライアント１１４ａは、ユーザデバイス１１４上のウェブブラウザ等のコンピュータアプリケーションであってもよい。ウェブクライアント１１４ａは、ウェブアプリケーションサーバ１０４上でホストされているウェブアプリケーション１０６のクライアント側インターフェースにアクセスするためのユーザデバイス１１４上のプラットフォームに相当することができる。

【００２１】

通信ネットワーク１１６は、ハイブリッド認証システム１０２、ウェブアプリケーションサーバ１０４、リソースサーバ１０８、アイデンティティプロバイダ１１０、公開台帳１１２、およびユーザデバイス１１４が互いに通信することができる通信媒体を含むことができる。通信ネットワーク１１６の例は、インターネット、クラウドネットワーク、ワイヤレスフィデリティ（Ｗｉ－Ｆｉ）ネットワーク、パーソナルエリアネットワーク（ＰＡＮ）、ローカルエリアネットワーク（ＬＡＮ）、またはメトロポリタンエリアネットワーク（ＭＡＮ）を含むことができるが、これらに限定されない。ネットワーク環境１００内の様々なデバイスは、様々な有線および無線通信プロトコルに従って、通信ネットワーク１１６に接続するように構成することができる。このような有線および無線通信プロトコルの例は、伝送制御プロトコルおよびインターネットプロトコル（ＴＣＰ／ＩＰ）、ユーザデータグラムプロトコル（ＵＤＰ）、ハイパーテキスト転送プロトコル（ＨＴＴＰ）、ファイル転送プロトコル（ＦＴＰ）、Ｚｉｇ Ｂｅｅ、ＥＤＧＥ、ＩＥＥＥ ８０２．１１、ライトフィデリティ（Ｌｉ－Ｆｉ）、８０２．１６、ＩＥＥＥ ８０２．１１ ｓ、ＩＥＥＥ ８０２．１１ ｇ、マルチホップ通信、無線アクセスポイント（ＡＰ）、デバイス間通信、セルラ通信プロトコル、およびＢｌｕｅｔｏｏｔｈ（ＢＴ）通信プロトコルのうちの少なくとも１つを含むことができるが、これらに限定されない。

【００２２】

動作時、ウェブアプリケーションサーバ１０４は、ウェブアプリケーション１０６等の１つまたは複数のウェブアプリケーションをホストすることができる。ユーザデバイス１１４上で、ウェブクライアント１１４ａは、ウェブアプリケーション１０６のクライアント側インターフェースにアクセスするための第１のユーザ入力（例えば、ウェブアプリケーションの統一資源位置指定子（ＵＲＬ））を受信することができる。クライアント側インターフェースがロードされ、ユーザデバイス１１４のユーザインターフェース上に表示されると、ウェブクライアント１１４ａは、クライアント側インターフェースを介して、ウェブアプリケーションへのＳＳＯアクセスを求める要求として第２のユーザ入力を受信することができる。第２のユーザ入力は、ウェブアプリケーション１０６へのＳＳＯアクセスのためのプロセスをトリガし、アイデンティティプロバイダ１１０によって提供されるシングルサインオン認証情報を使用してウェブアプリケーション１０６に関連する複数のシステムまたはサービスへのアクセスを得るために提供されてよい。

【００２３】

ウェブアプリケーションサーバ１０４は、ウェブアプリケーション１０６へのＳＳＯアクセスを求めるユーザ開始要求を受信することができる。ユーザ開始要求の受信に基づいて、ウェブアプリケーションサーバ１０４は、要求をさらに生成し、ハイブリッド認証システム１０２に送信することができる。要求は、リソースサーバ１０８上のセキュアコンテンツ１０８ａにアクセスするための認証プロセスを開始するために送信することができ

る。セキュアコンテンツ１０８ａは、ユーザ名、電子メールＩＤ、年齢、性別、誕生日（ＤＯＢ）、ユーザ位置等のユーザ固有の情報を含むことができる。ウェブアプリケーションサーバ１０４は、ウェブアプリケーション１０６にユーザがログインもしくはサインアップするために、および／またはユーザ１１８のアイデンティティを作成／検証するために、ユーザ固有の情報にアクセスする必要があり得る。

【００２４】

ハイブリッド認証システム１０２は、ウェブアプリケーションサーバ１０４から、リソースサーバ１０８上のセキュアコンテンツ１０８ａにアクセスすることを求める要求を受信するように構成することができる。ハイブリッド認証システム１０２は、ウェブアプリケーションサーバ１０４から受信される要求に基づいて、ユーザデバイス１１４のユーザインターフェース上のユーザ選択可能オプションのセットの表示を制御するようにさらに構成することができる。一例として、ユーザインターフェースは、ユーザ選択可能オプションのセットを表示するウェブページまたはポップアップウィンドウであってもよい。ユーザ選択可能オプションのセットは、ウェブベースの認証方式およびウォレットベースの認証方式に相当することができる。ウェブベースの認証方式は、Ｏａｕｔｈ（例えば、Ｏａｕｔｈ　２．０）プロトコルに基づくことができ、２要素認証オプションの第１の認証オプションに相当することができる。ウォレットベースの認証方式は、公開台帳１１２に記憶されたスマートコントラクトに基づくことができる。

【００２５】

スマートコントラクトは、ウォレットアドレス、リソースサーバ１０８のアクセストークン、ユーザ識別子、および公開台帳１１２上のステータス識別子を記憶することができる。ここで、アクセストークンは、ウェブアプリケーションサーバ１０４によって提供されるアクセス要求の認証に基づいて、アイデンティティプロバイダ１１０によって事前に共有されてもよいことが留意され得る。例として、アイデンティティプロバイダ１１０は、Ｏａｕｔｈプロトコルを使用した過去の認証に基づいて、Ｏａｕｔｈトークンをアクセストークンとしてウェブアプリケーションサーバ１０４と事前共有してもよい。アクセストークンを取得するための動作の詳細は、例えば、図３Ａおよび図３Ｂに提供されている。

【００２６】

ウォレットアドレスは、公開台帳１１２上のユーザのウォレットアカウント（すなわち、ユーザ１１８のウォレットアカウント）に利用することができる。アクセストークンは、アクセストークンのベアラがリソースサーバ１０８へのアクセスを認可されており、アクセストークンに認められた範囲に従ってリソースサーバ１０８に対して特定の操作（例えば、データ取り出し）を実行することを許可されていることを示すことができる固有の文字列を含んでもよい。さらに、アクセストークンは、ユーザ識別子にリンクさせることができ、公開台帳１１２にともに記憶することができる。アイデンティティプロバイダ１１０からアクセストークンを取得するための動作の詳細は、例えば、図３Ａおよび図３Ｂに提供されている。

【００２７】

ステータス識別子は、ユーザのウォレットアカウントのウォレットアドレスまたはウォレットアイデンティティ（ＩＤ）のうちの一方が、アイデンティティプロバイダ１１０のウェブＩＤ（またはウェブアカウント）にリンクされているか否かを示すことができる。特定の事例において、複数のウェブアカウント（またはウェブＩＤ）をユーザのウォレットアカウントにリンクさせて、ユーザ１１８がウェブアプリケーションへのＳＳＯアクセスに適した任意のウェブＩＤを選択することを可能にすることができる。ユーザのウォレットアカウントのウォレットアドレスまたはウォレットＩＤとウェブＩＤ（複数可）とのリンクは、例えば、図３Ａおよび図３Ｂに記載されている。

【００２８】

ハイブリッド認証システム１０２は、認証方式として、ウェブベースの認証方式およびウォレットベースの認証方式のうちの一方を選択するようにさらに構成することができる。認証方式は、規定のセキュリティ基準、またはユーザ選択可能オプションの表示された

セットのうちの１つを介したユーザ１１８からのユーザ入力に基づいて選択することができる。例として、規定のセキュリティ基準は、ウェブアプリケーションサーバ１０４上でホストされている１つまたは複数のウェブアプリケーションのうちの特定のウェブアプリケーションについての規定のセキュリティレベルを含むことができる。規定のセキュリティ基準は、ウェブアプリケーションサーバ１０４によって開始される要求に対して単一要素認証または２要素認証をさらに選択すべきかを判定するために使用され得る。特定の例示的なシナリオでは、２要素認証のために、例えば、ワンタイムパスワード（ＯＴＰ）ベースの認証またはピンベースの認証等の他の認証方式が、選択された認証方式を一次認証要素とする二次認証要素として選択され得る。付加的または代替的に、規定のセキュリティ基準は、特定のウェブアプリケーションのためのユーザが選好する認証方式を含むことができる。一例として、認証方式の過去のユーザ選好または過去の選択に基づいて、異なるウェブアプリケーションに対する、ユーザが選好する認証方式のレコードをハイブリッド認証システム１０２によって維持することができる。

【００２９】

付加的または代替的に、規定のセキュリティ基準は、ウェブベースの認証方式またはウォレットベースの認証方式のうちの１つに基づいて以前に試行された認証の失敗ステータスを含み得る。例えば、ウェブベースの認証方式を使用してウェブアプリケーションサーバ１０４の要求を認証するための認証失敗の過去のレコードおよび／または失敗した試行のログを分析して、選択認証方式としてウォレットベースの認証方式を選択し、ウォレットベースの認証方式に基づいて認証を再試行することができる。

【００３０】

ハイブリッド認証システム１０２は、選択認証方式に基づいて、受信された要求の認証を制御するようにさらに構成することができる。一実施形態では、ハイブリッド認証システム１０２は、ウェブベースの認証方式を選択するために、表示されているユーザ選択可能オプションのセットのうちの第１のユーザ選択可能オプションを介してユーザ入力を受信するように構成することができる。ハイブリッド認証システム１０２は、ユーザ１１８から受信されるユーザ入力に基づいて、この認証方式をウェブベースの認証方式として選択するようにさらに構成することができる。ハイブリッド認証システム１０２は、ウェブベースの認証方式に従って、受信された要求の認証を制御するようにさらに構成することができる。例として、ウェブベースの認証方式は、Ｏａｕｔｈ　２．０プロトコル（以下、Ｏａｕｔｈプロトコルと称する）に従い得る。Ｏａｕｔｈプロトコルは、トークンベースの認証および認可のためのオープン規格であり、ウェブアプリケーション１０６のためのユーザ認可ＡＰＩを必要とするサービスにアクセスするための標準的な方法を提供する。Ｏａｕｔｈプロトコルは当業者に知られており、そのため、簡潔にするためにＯａｕｔｈプロトコルの詳細は本開示から省略する。

【００３１】

ウェブベースの認証方式が選択されると、ハイブリッド認証システム１０２は、アクセストークンが期限切れであり、新しいアクセストークンが要求されるべきか否かを判定するように構成することができる。アクセストークンが期限切れになっていない場合、ハイブリッド認証システム１０２は、アイデンティティプロバイダ１１０によって生成されるアクセストークンに基づいて、受信される要求の認証を制御するように構成することができる。例として、認証は、ウェブアプリケーションサーバ１０４とリソースサーバ１０８との間でトークン交換プロセスをディスパッチすることによって制御されてもよい。より具体的には、ウェブアプリケーションサーバ１０４は、アクセストークンを取り出し、アクセストークンをリソースサーバ１０８に送信してもよい。リソースサーバ１０８は、アクセストークンの有効性を検証し、アクセストークンのベアラのアイデンティティを検証し、ウェブアプリケーションサーバ１０４がセキュアコンテンツ１０８ａにアクセスすることを認可することができる。

【００３２】

他の実施形態では、ハイブリッド認証システム１０２は、ウォレットベースの認証方式

を選択するために、表示されているユーザ選択可能オプションのセットのうちの第２のユーザ選択可能オプションを介してユーザ入力を受信するように構成することができる。ハイブリッド認証システム１０２は、ユーザ１１８から受信されるユーザ入力に基づいて、この認証方式をウォレットベースの認証方式として選択するようにさらに構成することができる。ハイブリッド認証システム１０２は、ウォレットベースの認証方式に従って、受信された要求の認証を制御するようにさらに構成することができる。ウォレットベースの認証方式が選択されると、ハイブリッド認証システム１０２は、アクセストークンが期限切れであり、新しいアクセストークンが要求されるべきか否かを判定するように構成することができる。アクセストークンが期限切れになっていない場合、ハイブリッド認証システム１０２は、ウォレットベースの認証プロセスをディスパッチすることによって、受信される要求の認証を制御するように構成することができる。

【００３３】

ウォレットベースの認証プロセスにおいて、ハイブリッド認証システム１０２は、受信されるユーザ入力に基づいてユーザデバイス１１４のウェブクライアント１１４ａ上でプロンプトをトリガするように構成され得る。プロンプトは、公開台帳１１２上のユーザのウォレットアカウントへのユーザログインを可能にするようにトリガすることができる。例えば、プロンプトは、ユーザデバイス１１４上のウェブクライアント１１４ａを介して、ユーザのウォレットアカウントへのユーザログインを可能にするようにトリガされてもよい。ユーザのウォレットアカウントへのユーザログインは、ユーザのウォレットアカウントのウォレットアドレスおよびウォレットアドレスに関連付けられた秘密鍵を使用して有効にすることができる。ユーザのウォレットアカウントに関連付けられた秘密鍵は、ユーザ１１８のみがアクセス可能であり得る。

【００３４】

ハイブリッド認証システム１０２は、公開台帳１１２上のユーザのウォレットアカウントへのユーザログインを検出するようにさらに構成することができる。ユーザ１１８は、例えば、ウェブクライアント１１４ａにおいてトリガされるプロンプトを介して、ユーザのウォレットアカウントがユーザログインを実行するためのウォレットＩＤおよび秘密鍵またはパスワードを入力することができる。ハイブリッド認証システム１０２は、ウォレットアドレスに関連付けられた公開鍵、ユーザログインの検出、およびスマートコントラクトに基づいて、受信される要求の認証を制御するようにさらに構成することができる。ウォレットアドレスに関連付けられた公開鍵は、ハイブリッド認証システム１０２に記憶することができる。

【００３５】

ハイブリッド認証システム１０２は、受信される要求の認証に基づいて認証情報をウェブアプリケーションサーバ１０４と共有するようにさらに構成することができる。認証情報は、ウェブアプリケーションサーバ１０４からのセキュアコンテンツ１０８ａへのアクセス要求が認証されたことを示すように、ハイブリッド認証システム１０２がウェブアプリケーションサーバ１０４に提供することができる認証情報に相当することができる。ウェブアプリケーションサーバ１０４は、ＳＳＯクライアント１０６ａを介してハイブリッド認証システム１０２から認証情報を受信することができる。その後、ウェブアプリケーションサーバ１０４は、共有認証情報を使用してリソースサーバ１０８上のセキュアコンテンツ１０８ａにアクセスすることができる。例として、リソースサーバ１０８Ａは、ウェブアプリケーションサーバ１０４から認証情報を受信して、セキュアコンテンツ１０８ａにアクセスすることができる。リソースサーバ１０８上のＳＳＯクライアント１０８ｂは受信される認証情報をハイブリッド認証情報によって検証することができる。リソースサーバ１０８は、共有認証情報の検証に基づいてセキュアコンテンツ１０８ａにアクセスすることを求める要求の有効性を検証することができる。付加的または代替的に、リソースサーバ１０８は、セキュアコンテンツ１０８ａにアクセスすることを求める要求が有効なトークンベアラ、すなわちウェブアプリケーション１０６からのものであることを検証することができる。

【００３６】
ウェブアプリケーションサーバ１０４は、アクセスされたセキュアコンテンツ１０８ａに基づいて、ユーザデバイス１１４のウェブクライアント１１４ａ上のウェブアプリケーション１０６のセッションを初期化することができる。ウェブアプリケーション１０６は、ユーザデバイス１１４上のウェブクライアント１１４ａ上の初期化されたセッションにセッションＩＤを割り当てることができる。割り当てられたセッションＩＤは、ウェブベースのログインに基づくサインオンのセッションＩＤと同一であり得る。換言すれば、割り当てられたセッションＩＤは、ウェブクライアント１１４ａ上でのウェブベースのログインのためにウェブアプリケーション１０６に割り当てられ得るセッションＩＤと同一であり得る。

【００３７】
いくつかの例示的な実施形態では、ハイブリッド認証システム１０２は、受信される要求の認証に基づいてユーザプロファイルイメージを構築するように構成することができる。ユーザプロファイルイメージは、ウェブアプリケーションサーバ１０４上でホストされている１つまたは複数のウェブアプリケーションのためのアプリケーション統一資源位置指定子（ＵＲＬ）、認証タイプ、アイデンティティプロバイダ名、アクセストークンに事前に割り当てられた有効期間、および再認証ステータスを含むことができる。例えば、ユーザ１１８のユーザプロファイルイメージは、ウェブクライアント１１４ａを介してウェブアプリケーションサーバ１０４上でホストされているウェブアプリケーション１０６のＵＲＬを含むことができる。ユーザ１１８のユーザプロファイルイメージは、特定のウェブアプリケーションからの要求の認証のために選択される認証方式（複数可）を指定することができる認証タイプをさらに含むことができる。例えば、認証タイプは、ウェブベースの認証、ウォレットベースの認証、またはウェブベースの認証とウォレットベースの認証の両方であり得る。ユーザ１１８のユーザプロファイルイメージは、アイデンティティプロバイダ１１０の名前およびアイデンティティプロバイダ１１０によって提供されるアクセストークンに事前に割り当てられた有効期間をさらに含むことができる。ユーザ１１８のユーザプロファイルイメージは、ＳＳＯアクセスの再認証が将来ユーザ１１８に必要かまたは不要かを示す再認証ステータスをさらに含んでよい。

【００３８】
ユーザプロファイルイメージの一例を以下の表１に示す。

【表１】

アプリケーションＵＲＬ	認証タイプ	ウェブアカウント（ウェブＩＤ）	有効期間	再認証（ＳＳＯ）
ｈｔｔｐ：／／１２３．ｃｏｍ	両方（ウェブ、ウォレット）	ＩＤ＿Ｐｒｏｖｉｄｅｒ＿１、ＩＤ＿Ｐｒｏｖｉｄｅｒ＿２	７２時間	強制
ｈｔｔｐ：／／ａｂｃ．ｃｏｍ	ウォレットのみ	ＩＤ＿Ｐｒｏｖｉｄｅｒ＿３、ＩＤ＿Ｐｒｏｖｉｄｅｒ＿２	０．５時間	なし
ｈｔｔｐ：／／ｘｙｚ．ｃｏｍ	（ウェブ、ウォレット）のうちの一方	ＩＤ＿Ｐｒｏｖｉｄｅｒ＿４	１２時間	なし

表１：ハイブリッド認証構成のユーザプロファイルイメージ

【００３９】
表１では、ウェブアカウント（ＩＤ＿Ｐｒｏｖｉｄｅｒ＿１、ＩＤ＿Ｐｒｏｖｉｄｅｒ＿２、ＩＤ＿Ｐｒｏｖｉｄｅｒ＿３、およびＩＤ＿Ｐｒｏｖｉｄｅｒ＿４）は、複数のアイデンティティプロバイダに相当し得る。複数のアイデンティティプロバイダの相当するウェブアカウント（またはウェブＩＤ）は、ユーザが異なるウェブアカウント／ウェブＩＤを介してＳＳＯ認証を選択することを可能にするように、ユーザのウォレットアカウントのウォレットＩＤまたはウォレットアドレスにリンクさせることができる。

【００４０】
いくつかの例示的な実施形態では、ハイブリッド認証システム１０２は、受信される要求の認証のための２要素認証方式を提供するようにさらに構成することができる。２要素認証方式は、受信される要求の認証のためのウェブベースの認証方式とウォレットベース

の認証方式の両方を含み得る。ハイブリッド認証システム１０２は、ウェブベースの認証方式とウォレットベースの認証方式の両方に従って、要求の認証を制御するようにさらに構成することができる。

【００４１】

図２は、本開示の一実施形態による、複数の認証オプションによるＳＳＯ認証のための例示的なハイブリッド認証システムを示すブロック図である。図２は、図１の要素と関連して説明される。図２を参照すると、ハイブリッド認証システム１０２のブロック図２００が示されている。ハイブリッド認証システム１０２は、制御回路２０２、メモリ２０４、および永続的データ記憶装置２０６を含むことができる。ハイブリッド認証システム１０２は、イベントリスナ２０８およびネットワークインターフェース２１０をさらに含むことができる。制御回路２０２は、ネットワークインターフェース２１０を使用することによって、ウェブアプリケーションサーバ１０４、リソースサーバ１０８、公開台帳１１２、アイデンティティプロバイダ１１０、およびユーザデバイス１１４と通信するように構成することができる。また、制御回路２０２は、メモリ２０４、永続的データ記憶装置２０６、イベントリスナ２０８、およびネットワークインターフェース２１０に通信可能に結合することができる。

【００４２】

制御回路２０２は、ウェブアプリケーションサーバ１０４から、リソースサーバ１０８上のセキュアコンテンツ１０８ａにアクセスすることを求める要求を受信するように構成することができる適切なロジック、回路、およびインターフェースを備えることができる。制御回路２０２は、受信される要求の認証のためにウェブベースの認証方式およびウォレットベースの認証方式のうちの一方を選択するようにさらに構成することができる。認証方式は、規定のセキュリティ基準またはユーザデバイス１１４を介したユーザ入力に基づいて選択することができる。制御回路２０２は、選択認証方式に基づいて、受信された要求の認証を制御するようにさらに構成することができる。制御回路２０２は、メモリ２０４に記憶された命令を実行するように構成された１つまたは複数のプロセッサを含むことができ、ハイブリッド認証システム１０２内の別個のプロセッサまたは回路として実装され得る１つまたは複数の専用処理ユニットを含むことができる。

【００４３】

一実施形態では、１つまたは複数の専用処理ユニットおよび制御回路２０２は、集合的に１つまたは複数の専用処理ユニットおよび制御回路２０２の機能を実行する統合プロセッサまたはプロセッサのクラスタとして実装されてもよい。制御回路２０２は、当技術分野で知られているいくつかのプロセッサ技術に基づいて実装されてもよい。制御回路２０２の実施態様の例は、ｘ８６ベースのプロセッサ、縮小命令セットコンピューティング（ＲＩＳＣ）プロセッサ、特定用途向け集積回路（ＡＳＩＣ）プロセッサ、複合命令セットコンピューティング（ＣＩＳＣ）プロセッサ、マイクロコントローラ、中央処理装置（ＣＰＵ）、グラフィック処理装置（ＧＰＵ）、および／または他の制御回路であってもよい。

【００４４】

メモリ２０４は、制御回路２０２によって実行可能なプログラム命令を記憶するように構成することができる適切なロジック、回路、およびインターフェースを備えることができる。特定の実施形態では、メモリ２０４は、オペレーティングシステムおよび関連するアプリケーション固有の情報を記憶するように構成することができる。メモリ２０４は、コンピュータ実行可能命令またはデータ構造を搬送または記憶するためのコンピュータ可読記憶媒体を含むことができる。このようなコンピュータ可読記憶媒体は、汎用または専用コンピュータによってアクセスされ得る任意の利用可能な媒体を含むことができる。このようなコンピュータ可読記憶媒体は、ランダムアクセスメモリ（ＲＡＭ）、読み出し専用メモリ（ＲＯＭ）、電気的消去可能プログラマブル読み出し専用メモリ（ＥＥＰＲＯＭ）、コンパクトディスク読み出し専用メモリ（ＣＤ－ＲＯＭ）もしくは他の光ディスク記憶装置、磁気ディスク記憶装置もしくは他の磁気記憶デバイス、フラッシュメモリデバイス（例えば、ソリッドステートメモリデバイス）、または、コンピュータ実行可能命令も

しくはデータ構造の形態で特定のプログラムコードを搬送もしくは記憶するために使用することができ、汎用もしくは専用コンピュータによってアクセスすることができる任意の他の記憶媒体を含む、有形または非一時的コンピュータ可読記憶媒体を含むことができる。上記の組み合わせもまた、コンピュータ可読記憶媒体の範囲内に含まれ得る。コンピュータ実行可能命令は、例えば、ハイブリッド認証システム１０２に関連する特定の動作または動作群を制御回路２０２に実行させるように構成された命令およびデータを含むことができる。

【００４５】

永続的データ記憶装置２０６は、制御回路２０２によって実行可能なプログラム命令、オペレーティングシステム、ならびに／またはログおよびアプリケーション固有のデータベース等のアプリケーション固有の情報を記憶するように構成することができる適切なロジック、回路、およびインターフェースを備えることができる。永続的データ記憶装置２０６は、コンピュータ実行可能命令またはデータ構造を搬送または記憶するためのコンピュータ可読記憶媒体を含むことができる。このようなコンピュータ可読記憶媒体は、汎用または専用コンピュータによってアクセスされ得る任意の利用可能な媒体を含むことができる。限定ではなく例として、このようなコンピュータ可読記憶媒体は、コンパクトディスク読み出し専用メモリ（ＣＤ－ＲＯＭ）もしくは他の光ディスク記憶装置、磁気ディスク記憶装置もしくは他の磁気記憶デバイス（例えば、ハードディスクドライブ（ＨＤＤ））、フラッシュメモリデバイス（例えば、ソリッドステートドライブ（ＳＳＤ）、セキュアデジタル（ＳＤ）カード、他のソリッドステートメモリデバイス）、または、コンピュータ実行可能命令もしくはデータ構造の形態で特定のプログラムコードを搬送もしくは記憶するために使用することができ、汎用もしくは専用コンピュータによってアクセスすることができる任意の他の記憶媒体を含む、有形または非一時的コンピュータ可読記憶媒体を含むことができる。上記の組み合わせもまた、コンピュータ可読記憶媒体の範囲内に含まれ得る。コンピュータ実行可能命令は、例えば、ハイブリッド認証システム１０２に関連する特定の動作または動作群を制御回路２０２に実行させるように構成された命令およびデータを含むことができる。

【００４６】

イベントリスナ２０８は、公開台帳１１２上の記憶されているスマートコントラクトに関連する１つまたは複数のイベントを検出するように構成することができる適切なロジック、回路、およびインターフェースを備えることができる。イベントリスナ２０８は、公開台帳１１２上の記憶されているスマートコントラクトに関連する１つまたは複数のイベントを検出するように、制御回路２０２によって公開台帳１１２上に展開することができる。１つまたは複数のイベントは、公開台帳１１２上のユーザのウォレットアカウントのスマートコントラクトに関連付けられた１つまたは複数のレコードに相当することができる。イベントリスナ２０８は、プログラムコード／ソフトウェアプログラムおよび／または当該技術分野において知られているいくつかのプロセッサ技術に基づいて実装されてもよい。

【００４７】

ネットワークインターフェース２１０は、通信ネットワーク１１６を介して、ハイブリッド認証システム１０２、ウェブアプリケーションサーバ１０４、リソースサーバ１０８、アイデンティティプロバイダ１１０、公開台帳１１２、およびユーザデバイス１１４の間の通信を容易にするように構成することができる適切なロジック、回路、およびインターフェースを備えることができる。ネットワークインターフェース２１０は、ハイブリッド認証システム１０２と通信ネットワーク１１６との有線または無線通信をサポートするための様々な既知の技術の使用によって実装されてもよい。ネットワークインターフェース２１０は、限定ではないが、アンテナ、無線周波数（ＲＦ）送受信機、１つもしくは複数の増幅器、チューナ、１つもしくは複数の発振器、デジタル信号プロセッサ、コーダ／デコーダ（ＣＯＤＥＣ）チップセット、加入者識別モジュール（ＳＩＭ）カード、またはローカルバッファ回路を含むことができる。ネットワークインターフェース２１０は、無

線通信を介して、インターネット、イントラネット、または携帯電話ネットワーク、無線ローカルエリアネットワーク（ＬＡＮ）およびメトロポリタンエリアネットワーク（ＭＡＮ）等の無線ネットワークと通信するように構成することができる。

【００４８】

無線通信は、グローバルシステムフォーモバイルコミュニケーションズ（ＧＳＭ）、拡張データＧＳＭ環境（ＥＤＧＥ）、広帯域符号分割多元接続（Ｗ－ＣＤＭＡ）、ロングタームエボリューション（ＬＴＥ）、符号分割多元接続（ＣＤＭＡ）、時分割多元接続（ＴＤＭＡ）、Ｂｌｕｅｔｏｏｔｈ、ワイヤレスフィデリティ（Ｗｉ－Ｆｉ）（ＩＥＥＥ ８０２．１１ ａ、ＩＥＥＥ ８０２．１１ ｂ、ＩＥＥＥ ８０２．１１ ｇ、またはＩＥＥＥ ８０２．１１ ｎ等）、ボイスオーバーインターネットプロトコル（ＶｏＩＰ）、ライトフィデリティ（Ｌｉ－Ｆｉ）、世界規模相互運用マイクロ波アクセス（Ｗｉ－ＭＡＸ）、電子メール、インスタントメッセージング、およびショートメッセージサービス（ＳＭＳ）のためのプロトコル等の複数の通信規格、プロトコル、および技術のうちの１つまたは複数を使用するように構成されてもよい。

【００４９】

いくつかの例示的な実施形態では、ハイブリッド認証システム１０２は、ウェブアプリケーションサーバ１０４からの要求のウォレットベースの認証を実行するように構成することができる１つまたは複数のエッジデバイス２１２をさらに含むことができる。１つまたは複数のエッジデバイス２１２の各エッジデバイスは、企業またはサービスプロバイダ基幹ネットワークへのエントリポイントを提供することができる。１つまたは複数のエッジデバイス２１２は、例えば、ルータ、ルーティングスイッチ、統合アクセスデバイス（ＩＡＤ）、マルチプレクサ、ならびに様々なＭＡＮおよびＷＡＮアクセスデバイスを含んでもよい。制御回路２０２によって実行される動作は、例えば、図３Ａ、図３Ｂ、図４Ａ、図４Ｂ、および図５に詳細に記載されている。

【００５０】

図３Ａおよび図３Ｂは集合的に、本開示の一実施形態による、アイデンティティプロバイダのウェブＩＤをユーザのウォレットアカウントにリンクさせるためのシーケンス図を示す。図３Ａおよび図３Ｂは、図１および図２の要素に関連して説明される。図３Ａおよび図３Ｂを参照すると、アイデンティティプロバイダ１１０のウェブＩＤをユーザのウォレットアカウントの公開鍵にリンクさせる方法を示すシーケンス図３００が示されている。一連の動作は、ハイブリッド認証システム１０２、ウェブアプリケーションサーバ１０４、アイデンティティプロバイダ１１０、および公開台帳１１２等のネットワーク環境１００の様々な要素によって実行され得る３０２～３２４であってもよい。

【００５１】

３０２において、ウェブアプリケーションサーバ１０４は、ユーザ１１８のアクセス要求およびユーザ登録詳細をハイブリッド認証システム１０２に送信することができる。アクセス要求は、アイデンティティプロバイダ１１０からアクセストークンを取得するために送信することができる。ウェブアプリケーションサーバ１０４、すなわちトークンベアラは、リソースサーバ１０８から、ユーザ１１８に関連するセキュアコンテンツ１０８ａにアクセスするために、ユーザ１１８に代わって認証される。また、アクセス要求およびユーザ登録詳細は、ユーザデバイス１１４のウェブクライアント１１４ａを介して、ウェブアプリケーション１０６上でのＳＳＯを求めるユーザの要求に基づいてハイブリッド認証システム１０２に送信することもできる。

【００５２】

３０４において、ハイブリッド認証システム１０２は、認証のためにアクセス要求をアイデンティティプロバイダ１１０にリダイレクトするように構成することができる。ハイブリッド認証システム１０２は、ウェブアプリケーションサーバ１０４からユーザ１１８のアクセス要求およびユーザ登録詳細を受信するように構成することができる。例えば、ハイブリッド認証システム１０２は、アクセス要求をアイデンティティプロバイダ１１０のウェブページにリダイレクトするように構成することができる。

【００５３】
３０６において、アイデンティティプロバイダ１１０は、アクセス要求の認証に基づいてアクセストークンを発行するように構成することができる。一例として、アクセストークンは、Ｏａｕｔｈプロトコルに従って、アイデンティティプロバイダ１１０によって発行されるＯａｕｔｈトークンであってもよい。アイデンティティプロバイダ１１０は、ユーザ１１８のユーザ登録詳細に基づいてアクセス要求およびユーザ１１８のアイデンティティを認証するように構成することができる。アイデンティティプロバイダ１１０は、ユーザ１１８のアクセス要求に関連付けられたアクセストークンを生成するようにさらに構成することができる。アクセストークンは、アクセストークンのベアラがリソースサーバ１０８へのアクセスを認可されており、アクセストークンに認められた範囲に従ってリソースサーバ１０８に対して特定の操作（例えば、データ取り出し）を実行することを許可されていることを表すことができる固有の文字列を含んでもよい。
【００５４】
３０８において、ハイブリッド認証システム１０２は、スマートコントラクトを介して、アクセストークンおよびユーザ登録詳細を公開台帳１１２に安全に記憶するようにさらに構成することができる。スマートコントラクトは、ウォレットアドレス、ユーザ識別子、およびステータス識別子、ならびにリソースサーバ１０８のアクセストークンを公開台帳１１２上に記憶する自己実行可能プログラムであってもよい。スマートコントラクト自体は、公開台帳１１２に記憶することができる。
【００５５】
ウォレットアドレスは、ユーザ１１８のウォレットアカウント等の、ユーザのウォレットアカウントのためのものであってもよい。スマートコントラクトに記憶されているステータス識別子は、ユーザのウォレットアカウントのウォレットアドレスまたはウォレットＩＤが、アイデンティティプロバイダ１１０のウェブＩＤにリンクされているか否かを示すことができる。本明細書において、ウェブＩＤは、統一資源識別子（ＵＲＩ）を使用して企業、組織、またはエージェントを識別するための固有の方法であり得る。アイデンティティプロバイダ１１０のウェブＩＤは、予め指定されたＵＲＩであってもよく、これは、アイデンティティプロバイダ１１０を一義的に識別するために使用され得る文字列であってもよい。公開台帳１１２上のユーザ１１８のウォレットアカウントは、公開台帳１１２上のユーザ１１８の暗号化ウォレットアカウントであってもよい。公開台帳１１２上のユーザ１１８のウォレットアカウントは、公開鍵および秘密鍵に関連付けられ得る。ユーザのウォレットアカウントのウォレットＩＤは、公開台帳１１２上のユーザのウォレットアカウントに割り当てられた一意のＩＤであり得る。
【００５６】
３１０において、ハイブリッド認証システム１０２は、スマートコントラクト内のステータス識別子をリンクされていないものとして更新するように構成することができる。リンクされていないステータス識別子は、ユーザのウォレットアカウントのウォレットＩＤ（またはウォレットアドレス）がアイデンティティプロバイダ１１０のウェブＩＤにリンクされていないことを示すことができる。最初に、ウォレットＩＤ（またはウォレットアドレス）はウェブＩＤにリンクされていなくてもよく、そのため、ステータス識別子はリンクされていないとして更新されてもよい。公開台帳１１２に記憶されたウォレットアドレス、ユーザ識別子、ステータス識別子、およびアクセストークンの例示的なレコードは、以下のように表２に提供される。
【表２】

ウェブＩＤ	アクセストークン	ウォレットＩＤ	ステータス識別子
１２３	４５ｆｆｓｄ４	０ｘ２３ｄｄｆ４	リンクされていない

表２：公開台帳上の例示的なレコード
【００５７】

３１２において、ハイブリッド認証システム１０２は、イベントリスナ２０８を公開台帳１１２に対して展開するようにさらに構成することができる。ハイブリッド認証システム１０２は、展開されたイベントリスナ２０８を使用して、公開台帳１１２上の記憶されたスマートコントラクトに関連する１つまたは複数のイベントを検出するようにさらに構成することができる。１つまたは複数のイベントは、公開台帳１１２上のユーザのウォレットアカウントのスマートコントラクトに関連付けられた１つまたは複数のレコードに相当することができる。例えば、イベントは、公開台帳１１２上のユーザのウォレットアカウントに関連付けられた現在のユーザ活動のレコードに相当することができる。

【００５８】

３１４において、イベントリスナ２０８は、記憶されたスマートコントラクトに関連するイベント情報をハイブリッド認証システム１０２に送信するように構成することができる。イベント情報は、公開台帳１１２上の記憶されたスマートコントラクトに関連する検出された１つまたは複数のイベントを含むことができる。例えば、検出されたイベントは、公開台帳１１２上のユーザのウォレットアカウントへのユーザログインに相当することができる。

【００５９】

３１６において、ハイブリッド認証システム１０２は、公開台帳１１２上の検出された１つまたは複数のイベントに基づいて、アイデンティティプロバイダ１１０による受信したアクセストークンの有効性検証要求を開始するようにさらに構成することができる。アイデンティティプロバイダ１１０は、受信されたアクセストークンが有効であるか否かを判定するように構成することができる。

【００６０】

３１８において、アイデンティティプロバイダ１１０は、開始された有効性検証要求に対する応答をハイブリッド認証システム１０２に送信するようにさらに構成することができる。応答は、アクセストークンが有効であるか否かを示すことができる情報を含むことができる。例えば、受信されるアクセストークンが有効である場合、アイデンティティプロバイダ１１０は、受信されるアクセストークンが有効であることを示す応答をハイブリッド認証システム１０２に送信するように構成されてもよい。代替的に、受信されるアクセストークンが無効である場合、アイデンティティプロバイダ１１０は、受信されるアクセストークンが無効であることを示す応答をハイブリッド認証システム１０２に送信するように構成されてもよい。ハイブリッド認証システム１０２は、アイデンティティプロバイダ１１０から応答を受信するように構成されてもよい。

【００６１】

３２０において、ハイブリッド認証システム１０２は、アイデンティティプロバイダ１１０から受信される応答に基づいて、受信されているアクセストークンの有効性を検証するようにさらに構成することができる。ハイブリッド認証システム１０２は、アイデンティティプロバイダ１１０から受信される応答がアクセストークンを有効と確認する場合、受信されているアクセストークンを有効と確認するようにさらに構成することができる。代替的に、ハイブリッド認証システム１０２は、アイデンティティプロバイダ１１０から受信される応答がユーザ１１８と関連付けられるアクセストークンを無効と確認する場合、受信されているアクセストークンを無効と確認するようにさらに構成されてもよい。

【００６２】

３２２において、ハイブリッド認証システム１０２は、受信されるアクセストークンの有効性検証に基づいて、アイデンティティプロバイダ１１０のウェブＩＤをユーザのウォレットアカウントのウォレットＩＤ（またはウォレットアドレス）とリンクさせるようにさらに構成することができる。例えば、アイデンティティプロバイダ１１０が電子メールサービスプロバイダである場合、ハイブリッド認証システム１０２は、電子メールサービスプロバイダのウェブＩＤを、公開台帳１１２上のユーザのウォレットアカウントのウォレットＩＤ（またはウォレットアドレス）とリンクさせるように構成することができる。

【００６３】

付加的または代替的に、ユーザのウォレットアカウントは、相当する複数のアイデンティティプロバイダの複数のウェブＩＤにリンクされてもよい。ハイブリッド認証システム１０２は、相当する複数のアイデンティティプロバイダの複数のウェブＩＤを、公開台帳１１２上のユーザのウォレットアカウントのウォレットＩＤ（またはウォレットアドレス）とリンクさせるようにさらに構成することができる。例えば、アイデンティティプロバイダとしての電子メールサービスプロバイダ、および１つまたは複数のソーシャルメディアネットワークプロバイダを用いて、ハイブリッド認証システム１０２は、アイデンティティプロバイダのウェブＩＤをユーザのウォレットアカウントのウォレットＩＤ（またはウォレットアドレス）とリンクさせるように構成されてもよい。

【００６４】

３２４において、ハイブリッド認証システム１０２は、アイデンティティプロバイダ１１０のウェブＩＤとユーザのウォレットアカウントのウォレットＩＤ（またはウォレットアドレス）との間のリンクに基づいて、リンクされているスマートコントラクト内のステータス識別子を更新するようにさらに構成することができる。アイデンティティプロバイダ１１０のウェブＩＤを含む更新されたステータス識別子は、公開台帳１１２に記憶することができ、ウォレットＩＤ（またはウォレットアドレス）とアイデンティティプロバイダ１１０のウェブＩＤとの間の関連付けを示すことができる。公開台帳１１２上のウェブＩＤ、アクセストークン、ウォレットＩＤ、および更新されたステータス識別子の例示的なレコードは、以下のように表３に提供される。

【表３】

ウェブＩＤ	アクセストークン	ウォレットＩＤ	ステータス識別子
１２３	４５ｆｆｓｄ４	０ｘ２３ｄｄｆ４	リンクされている

表３：公開台帳上の更新されたレコード

【００６５】

図４Ａおよび図４Ｂは集合的に、本開示の一実施形態による、複数の認証オプションによるＳＳＯ認証のためのシーケンス図を示す。図４Ａおよび図４Ｂは、図１、図２、図３Ａおよび図３Ｂの要素に関連して説明される。図４Ａおよび図４Ｂを参照すると、複数の認証オプションによるＳＳＯ認証の方法を示すシーケンス図４００が示されている。一連の動作は、ハイブリッド認証システム１０２、ウェブアプリケーションサーバ１０４、リソースサーバ１０８、およびユーザデバイス１１４等のネットワーク環境１００の様々な要素によって実行され得る４０２～４２０であってもよい。

【００６６】

４０２において、ユーザデバイス１１４はウェブアプリケーションサーバ１０４のウェブアプリケーション１０６へのＳＳＯアクセスを要求することができる。ＳＳＯアクセスを求める要求はウェブクライアント１１４ａを介してユーザ１１８によって開始でき、ウェブアプリケーションサーバ１０４に通信することができる。

【００６７】

４０４において、ウェブアプリケーションサーバ１０４は、リソースサーバ１０８上のセキュアコンテンツ１０８ａへのアクセスを要求することができる。要求は、ユーザ１１８によるウェブアプリケーション１０６へのＳＳＯアクセスを求めるユーザ要求の受信に基づいてハイブリッド認証システム１０２に提供することができる。セキュアコンテンツ１０８ａへのアクセスは、ユーザデバイス１１４のウェブクライアント１１４ａを介してユーザ１１８にウェブアプリケーション１０６の特定のサービスを提供するために必要とされ得る。

【００６８】

４０６において、ハイブリッド認証システム１０２は、ウェブアプリケーションサーバ１０４から受信される要求に基づいて、ユーザデバイス１１４のユーザインターフェース上のユーザ選択可能オプションのセットの表示を制御するように構成することができる。

ユーザ選択可能オプションのセットは、ウェブベースの認証方式およびウォレットベースの認証方式に相当することができる。

【００６９】

４０８において、要求の認証のためにウェブベースの認証方式が選択された場合、ハイブリッド認証システム１０２は、ウェブベースの認証方式に従って要求の認証を制御するように構成することができる。認証方式は、規定のセキュリティ基準、またはユーザ選択可能オプションの表示されたセットのうちの１つを介したユーザ入力に基づいて選択することができる。ウェブベースの認証方式は、Ｏａｕｔｈプロトコルに基づいてもよい。ウェブベースの認証方式の詳細は、例えば、図１に提供されている。

【００７０】

４１０において、要求の認証のためにウォレットベースの認証方式が選択された場合、ハイブリッド認証システム１０２は、受信されるユーザ入力に基づいてユーザデバイス１１４のウェブクライアント１１４ａ上でプロンプトをトリガするように構成することができる。プロンプトは、例えば、Ｅｔｈｅｒｅｕｍブロックチェーン等、公開台帳１１２上のユーザのウォレットアカウントへのユーザログインを可能にするようにトリガすることができる。例として、ユーザのウォレットアカウントへのユーザログインは、ユーザのウォレットアカウントのウォレットアドレスおよびウォレットアドレスに関連付けられた秘密鍵に基づくことができる。ハイブリッド認証システム１０２は、ウェブクライアント１１４ａを介して、公開台帳１１２上のユーザのウォレットアカウントへのユーザログインを検出するようにさらに構成することができる。

【００７１】

４１２において、ハイブリッド認証システム１０２は、ウォレットアドレスに関連付けられた公開鍵、ユーザログインの検出、およびスマートコントラクトに基づいて、要求の認証を制御するようにさらに構成することができる。例として、要求は、ユーザのウォレットアカウントへのユーザログインの有効性検証に基づいて、さらに、ユーザのウォレットアカウントに関連付けられた公開鍵、および公開台帳１１２に記憶され、スマートコントラクトにリンクされたアクセストークンに基づいて認証され得る。

【００７２】

４１４において、ハイブリッド認証システム１０２は、受信される要求の認証に基づいて認証情報をウェブアプリケーションサーバ１０４と共有するように構成することができる。認証情報は、認証情報のベアラがリソースサーバ１０８上のセキュアコンテンツ１０８ａにアクセスすることを認可されていることを表すことができる情報を含むことができる。また、認証情報は、ウェブアプリケーションサーバ１０４からのセキュアコンテンツ１０８ａへのアクセス要求が認証されたことを示すように、ハイブリッド認証システム１０２によってウェブアプリケーションサーバ１０４に提供することができる。

【００７３】

４１６において、ウェブアプリケーションサーバ１０４は、共有認証情報を使用することによってリソースサーバ１０８上のセキュアコンテンツ１０８ａにアクセスすることができる。例として、ウェブアプリケーションサーバ１０４は、認証情報をリソースサーバ１０８Ａに送信して、セキュアコンテンツ１０８ａにアクセスすることができる。リソースサーバ１０８は、受信される認証情報をハイブリッド認証システム１０２によって検証することができる。ウェブアプリケーションサーバ１０４は、リソースサーバ１０８による認証情報の有効性検証に基づいて、リソースサーバ１０８上のセキュアコンテンツ１０８ａにアクセスすることを許可され得る。

【００７４】

４１８において、ウェブアプリケーションサーバ１０４は、アクセスされたセキュアコンテンツ１０８ａに基づいて、ユーザデバイス１１４のウェブクライアント１１４ａ上のウェブアプリケーション１０６のセッションを初期化することができる。

【００７５】

４２０において、ウェブアプリケーションサーバ１０４は、ユーザデバイス１１４上の

ウェブクライアント１１４ａ上の初期化されたセッションにセッションＩＤを割り当てるようにさらに構成することができる。割り当てられたセッションＩＤは、ウェブクライアント１１４ａ上のウェブベースのログインに基づくサインオンのセッションＩＤと同一であり得る。セッションＩＤは、ウェブアプリケーションサーバ１０４が特定の期間にわたってウェブクライアント１１４ａ上のウェブアプリケーション１０６のセッションに割り当てることができる一意の番号であってもよい。セッションＩＤは、例えば、ウェブクライアント１１４ａ上のクッキー、フォームフィールド、または統一資源位置指定子（ＵＲＬ）内で指定されてもよい。

【００７６】

図５は、本開示の一実施形態による、ユーザ識別子と、複数のユーザアカウントと、複数のウェブアカウントまたは複数のウェブＩＤとの間の関連付けを示す例示的な図である。図５は、図１、図２、図３Ａおよび図３Ｂ、ならびに図４Ａおよび図４Ｂの要素に関連して説明される。図５を参照すると、例示的な図５００が示されている。

【００７７】

例示的な図５００は、ユーザ識別子５０２、複数のユーザアカウント５０４、および複数のウェブアカウント５０６を含む。図示のように、複数のユーザアカウント５０４は、例えば、公開台帳１１２上のウォレットアカウント、デジタル識別カード、または非接触スマートカードを含むことができる。同様に、複数のウェブアカウント５０６は、例えば、ＩＤ＿Ｐｒｏｖｉｄｅｒ＿１、ＩＤ＿Ｐｒｏｖｉｄｅｒ＿２、ＩＤ＿Ｐｒｏｖｉｄｅｒ＿３、およびＩＤ＿Ｐｒｏｖｉｄｅｒ＿４を含み得る。これらの複数のウェブアカウント５０６は、それぞれのウェブＩＤを有することができ、ユーザに代わってそれぞれのリソースサーバ上のセキュアコンテンツへのアクセスを要求するウェブアプリケーションにサービスとしてのＳＳＯを提供する複数のアイデンティティプロバイダに相当することができる。

【００７８】

複数のウェブアカウント５０６およびそれらのそれぞれのタイプの例を以下の表４に示す。

【表４】

ウェブアカウント	タイプ
ＩＤ＿Ｐｒｏｖｉｄｅｒ＿１	電子メールサービスプロバイダ
ＩＤ＿Ｐｒｏｖｉｄｅｒ＿２	ソーシャルメディアネットワーク
ＩＤ＿Ｐｒｏｖｉｄｅｒ＿３	ソーシャルメディアネットワーク
ＩＤ＿Ｐｒｏｖｉｄｅｒ＿４	電子メールサービスプロバイダ

表４：複数のウェブアカウントの例

【００７９】

示されるように、例えば、電子メールＩＤ等のユーザ識別子５０２は、公開台帳１１２上のウォレットアカウント、デジタル識別カード、および非接触スマートカードの各々にリンクさせることができる。ウォレットアカウントは、ＩＤ＿Ｐｒｏｖｉｄｅｒ＿１およびＩＤ＿Ｐｒｏｖｉｄｅｒ＿３にリンクさせることができる。同様に、デジタル識別カードはＩＤ＿Ｐｒｏｖｉｄｅｒ＿３にリンクさせることができ、非接触アイデンティティカードはＩＤ＿Ｐｒｏｖｉｄｅｒ＿２およびＩＤ＿Ｐｒｏｖｉｄｅｒ＿３にリンクさせることができる。複数のユーザアカウント５０４は、単一のユーザによって所有されてもよく、ユーザがそれぞれ複数のユーザアカウント５０４および複数のウェブアカウント５０６から選好するユーザアカウントおよび選好するウェブアカウントを選択することを可能にしてもよい。例えば、ユーザデバイス１１４上のウェブクライアント１１４ａを介して、公開台帳１１２上のウォレットアカウント、および、ウェブアプリケーション１０６へのＳＳＯアクセスのためのアイデンティティプロバイダ１１０としてのＩＤ＿Ｐｒｏｖｉｄｅｒ＿３を選択するためのユーザ入力が提供されてもよい。

【００８０】
図６は、本開示の一実施形態による、複数の認証オプションによるＳＳＯ認証のための例示的な方法を示す流れ図である。図６は、図１、図２、図３Ａ、図３Ｂ、図４Ａ、図４Ｂ、および図５の要素に関連して説明される。図６を参照すると、流れ図６００が示されている。流れ図６００の例示的な方法は、例えば、ハイブリッド認証システム１０２等の任意のコンピューティングシステムによって実行することができる。流れ図６００の例示的な方法は、６０２において開始し、６０４に進むことができる。
【００８１】
６０４において、ウェブアプリケーションサーバ１０４から、リソースサーバ１０８上のセキュアコンテンツ１０８ａにアクセスすることを求める要求を受信することができる。ハイブリッド認証システム１０２は、ウェブアプリケーションサーバ１０４から、リソースサーバ１０８上のセキュアコンテンツ１０８ａにアクセスすることを求める要求を受信するように構成することができる。ウェブアプリケーションサーバ１０４は、ウェブアプリケーションサーバ１０４のウェブアプリケーション１０６へのＳＳＯアクセスを求めるユーザ開始要求の受信に基づいて要求を送信するようさらに構成できる。
【００８２】
６０６において、受信される要求に基づいてユーザデバイス１１４のユーザインターフェース上のユーザ選択可能オプションのセットの表示を制御することができる。ハイブリッド認証システム１０２は、ユーザデバイス１１４のユーザインターフェース上のユーザ選択可能オプションのセットの表示を制御するようにさらに構成することができる。ユーザ選択可能オプションのセットは、ウェブベースの認証方式およびウォレットベースの認証方式に相当することができる。
【００８３】
６０８において、規定のセキュリティ基準またはユーザ選択可能オプションの表示されたセットのうちの１つを介したユーザ入力に基づいて、認証方式をウェブベースの認証方式およびウォレットベースの認証方式のうちの一方として選択することができる。規定のセキュリティ基準は、ウェブアプリケーションサーバ１０４上でホストされている１つまたは複数のウェブアプリケーションのうちの特定のウェブアプリケーションについての規定のセキュリティレベル、特定のウェブアプリケーションについてのユーザが選好する認証方式、またはウェブベースの認証方式もしくはウォレットベースの認証方式のうちの１つに基づいて以前に試みられた認証の失敗ステータスを含むことができるが、これらに限定されない。ハイブリッド認証システム１０２は、認証方式を、ウェブベースの認証方式およびウォレットベースの認証方式のうちの一方として選択するように構成することができる。
【００８４】
６１０において、選択された認証方式に基づいて、受信された要求の認証を制御することができる。ハイブリッド認証システム１０２は、選択認証方式に基づいて、受信された要求の認証を制御するようにさらに構成することができる。ウェブベースの認証方式が選択された場合、ハイブリッド認証システム１０２は、ウェブベースの認証に従って要求の認証を制御するように構成することができる。ウェブベースの認証は、Ｏａｕｔｈプロトコルに基づいてもよい。ウォレットベースの認証方式が選択された場合、ハイブリッド認証システム１０２は、ウォレットベースの認証方式に従って要求の認証を制御するように構成することができる。ウォレットベースの認証方式は、公開台帳１１２上の記憶されたスマートコントラクトに基づくことができる。受信される要求の認証の制御に関するさらなる詳細は、例えば、図１、図４Ａ、および図４Ｂに記載されている。制御は終了に進むことができる。
【００８５】
本開示の様々な実施形態は、複数の認証オプションによるシングルサインオン（ＳＳＯ）認証のための、ハイブリッド認証システム等の、機械および／またはコンピュータによって実行可能な命令を記憶されている、非一時的コンピュータ可読媒体および／もしくは

記憶媒体、ならびに／または非一時的機械可読媒体および／もしくは記憶媒体を提供することができる。少なくとも１つのコードセクションは、機械および／またはコンピュータに、ウェブアプリケーションサーバからリソースサーバ上のセキュアコンテンツにアクセスすることを求める要求を受信することを含む動作を実行させることができる。ハイブリッド認証システムは、ウェブアプリケーションサーバおよびスマートコントラクトを記憶する公開台帳に通信可能に結合することができる。動作は、受信される要求に基づいて、ユーザデバイスのユーザインターフェース上のユーザ選択可能オプションのセットの制御表示をさらに含む。ユーザ選択可能オプションのセットは、ウェブベースの認証方式およびウォレットベースの認証方式に相当することができる。ウォレットベースの認証方式は、公開台帳上の記憶されたスマートコントラクトに基づくことができる。動作は、規定のセキュリティ基準またはユーザ選択可能オプションの表示されたセットのうちの１つを介したユーザ入力に基づいて、ウェブベースの認証方式およびウォレットベースの認証方式のうちの一方を認証方式として選択することをさらに含むことができる。動作は、選択された認証方式に基づいて、受信された要求の認証を制御することをさらに含む。

【００８６】

本開示の例示的な態様は、ウェブアプリケーションサーバ１０４および公開台帳１１２に通信可能に結合された制御回路２０２を含むハイブリッド認証システム１０２を含むことができる。公開台帳１１２は、スマートコントラクトを記憶することができる。制御回路２０２は、ウェブアプリケーションサーバ１０４から、リソースサーバ１０８上のセキュアコンテンツ１０８ａにアクセスすることを求める要求を受信するように構成することができる。制御回路２０２は、受信される要求に基づいて、ユーザデバイス１１４のユーザインターフェース上のユーザ選択可能オプションのセットの表示を制御するようにさらに構成することができる。ユーザ選択可能オプションのセットは、ウェブベースの認証方式およびウォレットベースの認証方式に相当することができる。ウォレットベースの認証方式は、公開台帳１１２上の記憶されたスマートコントラクトに基づくことができる。制御回路２０２は、規定のセキュリティ基準またはユーザ選択可能オプションの表示されたセットのうちの１つを介したユーザ入力に基づいて、ウェブベースの認証方式およびウォレットベースの認証方式のうちの一方を認証方式として選択するようにさらに構成することができる。制御回路２０２は、選択認証方式に基づいて、受信された要求の認証を制御するようにさらに構成することができる。制御回路２０２は、受信される要求の認証に基づいて認証情報をウェブアプリケーションサーバ１０４と共有するようにさらに構成することができる。

【００８７】

ウェブアプリケーションサーバ１０４は、１つまたは複数のウェブアプリケーションをホストすることができ、ウェブアプリケーション１０６へのシングルサインオン（ＳＳＯ）アクセスを求めるユーザ開始要求の受信に基づいて要求を提供することができる。スマートコントラクトは、ウォレットアドレス、リソースサーバ１０８のアクセストークン、ユーザ識別子、およびステータス識別子を記憶する自己実行可能プログラムであってもよい。ウォレットアドレスは、公開台帳１１２上のユーザのウォレットアカウントのためのものであり得る。ステータス識別子は、ユーザのウォレットアカウントのウォレットアドレスまたはウォレットＩＤのうちの一方が、アイデンティティプロバイダ１１０のウェブＩＤにリンクされているか否かを示すことができる。リソースサーバ１０８は、アイデンティティプロバイダ１１０によって管理され得るアプリケーションプログラミングインターフェース（ＡＰＩ）サーバであってもよい。

【００８８】

ウェブアプリケーションサーバ１０４は、ユーザデバイス１１４のウェブクライアント１１４ａからのユーザのアクセス要求に基づいて、ハイブリッド認証システム１０２にアクセス要求およびユーザ登録詳細を送信することができる。制御回路２０２は、ウェブアプリケーションサーバ１０４によって送信されるアクセス要求およびユーザ登録詳細を受信するようにさらに構成することができる。制御回路２０２は、受信されるアクセス要求

の認証のために、受信されるアクセス要求をアイデンティティプロバイダ１１０にリダイレクトするようにさらに構成することができる。制御回路２０２は、受信されるアクセス要求の認証に基づいて、アイデンティティプロバイダ１１０からアクセストークンを受信するようにさらに構成することができる。制御回路２０２は、受信されるアクセストークンおよび受信されるユーザ登録詳細を、スマートコントラクトを介して公開台帳１１２上に安全に記憶するようにさらに構成することができる。

【００８９】

制御回路２０２は、スマートコントラクト内のステータス識別子をリンクされていないものとして更新するようにさらに構成することができる。更新されたステータス識別子は、ユーザのウォレットアカウントのウォレットアドレスまたはウォレットＩＤのうちの一方が、アイデンティティプロバイダ１１０のウェブＩＤにリンクされていないことを示すことができる。制御回路２０２は、イベントリスナを公開台帳１１２上に展開するようにさらに構成することができる。制御回路２０２は、展開されたイベントリスナによって、公開台帳１１２上の記憶されたスマートコントラクトに関連する１つまたは複数のイベントを検出するようにさらに構成することができる。

【００９０】

制御回路２０２は、公開台帳１１２上の検出された１つまたは複数のイベントに基づいて、アイデンティティプロバイダ１１０による受信したアクセストークンの有効性検証要求を開始するようにさらに構成することができる。制御回路２０２は、開始された有効性検証要求に対するアイデンティティプロバイダ１１０の応答を受信するようにさらに構成することができる。制御回路２０２は、受信される応答に基づいて、受信されるアクセストークンの有効性を検証するようにさらに構成することができる。制御回路２０２は、受信されるアクセストークンの有効性検証に基づいて、アイデンティティプロバイダ１１０のウェブＩＤを、公開台帳１１２上のユーザのウォレットアカウントの公開鍵、ウォレットアドレス、またはウォレットＩＤのうちの１つとリンクさせるようにさらに構成することができる。

【００９１】

制御回路２０２は、リンクに基づいて、スマートコントラクト内のステータス識別子をリンクされているものとして更新するようにさらに構成することができる。制御回路２０２は、相当する複数のアイデンティティプロバイダの複数のウェブＩＤを、公開台帳１１２上のユーザのウォレットアカウントの公開鍵、ウォレットアドレス、またはウォレットＩＤのうちの１つにリンクさせるようにさらに構成することができる。制御回路２０２は、リンクに基づいて、スマートコントラクト内のステータス識別子をリンクされているものとして更新するようにさらに構成することができる。

【００９２】

一実施形態によれば、制御回路２０２は、ウェブベースの認証方式を選択するために、表示されているユーザ選択可能オプションのセットのうちの第１のユーザ選択可能オプションを介してユーザ入力を受信するようにさらに構成することができる。制御回路２０２は、受信されるユーザ入力に基づいて、この認証方式をウェブベースの認証方式として選択するようにさらに構成することができる。制御回路２０２は、ウェブベースの認証方式に従って、受信された要求の認証を制御するようにさらに構成することができる。ウェブベースの認証方式は、Ｏａｕｔｈプロトコルに基づいてもよい。

【００９３】

一実施形態によれば、制御回路２０２は、ウォレットベースの認証方式を選択するために、表示されているユーザ選択可能オプションのセットのうちの第２のユーザ選択可能オプションを介してユーザ入力を受信するようにさらに構成することができる。制御回路２０２は、受信されるユーザ入力に基づいてユーザデバイス１１４のウェブクライアント１１４ａ上でプロンプトをトリガするようにさらに構成することができる。プロンプトは、ユーザのウォレットアカウントのウォレットアドレスおよびウォレットアドレスに関連付けられた秘密鍵を使用してユーザのウォレットアカウントへのユーザログインを可能にす

るようにトリガすることができる。制御回路２０２は、ユーザデバイス１１４上のウェブクライアント１１４ａを介して、ユーザのウォレットアカウントへのユーザログインを検出するようにさらに構成することができる。制御回路２０２は、ウォレットアドレスに関連付けられた公開鍵およびユーザログインの検出に基づいて、受信される要求の認証を制御するようにさらに構成することができる。公開鍵は、ハイブリッド認証システム１０２に記憶することができる。

【００９４】

制御回路２０２は、受信される要求の認証に基づいてアクセス認証情報をウェブアプリケーションサーバ１０４と共有するようにさらに構成することができる。ウェブアプリケーションサーバ１０４は、共有認証情報を使用してリソースサーバ１０８上のセキュアコンテンツ１０８ａにアクセスすることができる。ウェブアプリケーションサーバ１０４はさらに、アクセスされたセキュアコンテンツ１０８ａに基づいて、ユーザデバイス１１４のウェブクライアント１１４ａ上のウェブアプリケーション１０６のセッションを初期化することができる。ウェブアプリケーションサーバ１０４はさらに、初期化されたセッションにセッションＩＤを割り当てることができる。割り当てられたセッションＩＤは、ウェブベースのログインに基づくサインオンのセッションＩＤと同一であり得る。

【００９５】

制御回路２０２は、受信される要求の認証に基づいてユーザプロファイルイメージを構築するようにさらに構成することができる。ユーザプロファイルイメージは、ウェブアプリケーションサーバ１０４上でホストされている１つまたは複数のウェブアプリケーションのためのアプリケーション統一資源位置指定子（ＵＲＬ）、認証タイプ、アイデンティティプロバイダ名、アクセストークンに事前に割り当てられた有効期間、および再認証ステータスを含むことができる。規定のセキュリティ基準は、ウェブアプリケーションサーバ１０４上でホストされている１つまたは複数のウェブアプリケーションのうちの特定のウェブアプリケーションについての規定のセキュリティレベル、特定のウェブアプリケーションについてのユーザが選好する認証方式、またはウェブベースの認証方式もしくはウォレットベースの認証方式のうちの１つに基づいて以前に試みられた認証の失敗ステータスを含むことができる。

【００９６】

本開示は、ハードウェア、またはハードウェアとソフトウェアとの組み合わせで実現されてもよい。本開示は、少なくとも１つのコンピュータシステムにおいて集中化様式で、または、複数の異なる要素がいくつかの相互接続されたコンピュータシステムにわたって分散され得る分散様式で実現されてもよい。本明細書に記載の方法を実行するように適合されたコンピュータシステムまたは他の装置が適し得る。ハードウェアとソフトウェアの組み合わせは、ロードされ実行されるときに、コンピュータシステムが本明細書に記載の方法を実行するようにコンピュータシステムを制御することができるコンピュータプログラムを有する汎用コンピュータシステムであってもよい。本開示は、他の機能も実行する集積回路の一部を含むハードウェアにおいて実現されてもよい。

【００９７】

本開示はまた、本明細書に記載された方法の実施を可能にするすべての特徴を含み、コンピュータシステムにロードされたときにこれらの方法を実行することができるコンピュータプログラム製品に組み込まれてもよい。本明細書において、コンピュータプログラムとは、情報処理能力を有するシステムに、特定の機能を直接的に、または、ａ）別の言語、コードまたは表記法への変換、ｂ）異なる素材形式での再生のいずれかまたは両方の後に実行させるように意図された命令セットの任意の言語、コードまたは表記の表現を意味する。

【００９８】

本開示は、特定の実施形態を参照して説明されているが、本開示の範囲から逸脱することなく、様々な変更がなされ得、均等物が置換され得ることが、当業者によって理解される。その上、その範囲から逸脱することなく、特定の状況または材料を本開示の教示に適

合させるために、多くの修正がなされてもよい。そのため、本開示は、開示される特定の実施形態に限定されず、本開示は、添付の特許請求項の範囲内に入るすべての実施形態を含むことが意図される。

【図面】

【図１】

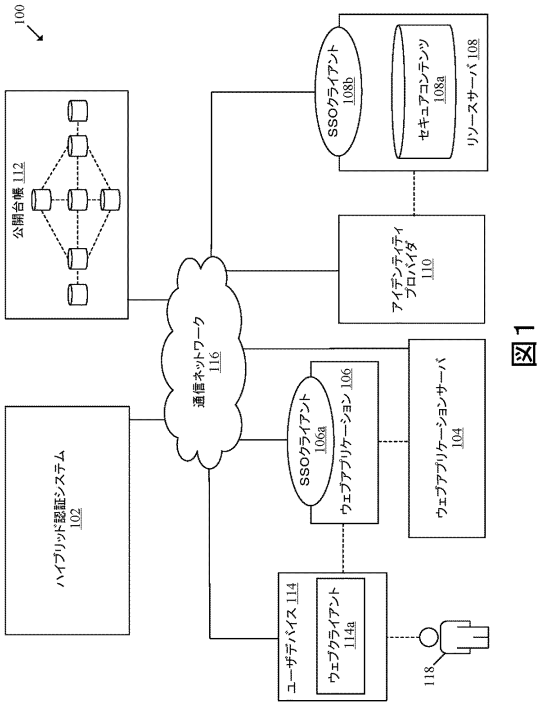


図1

【図２】

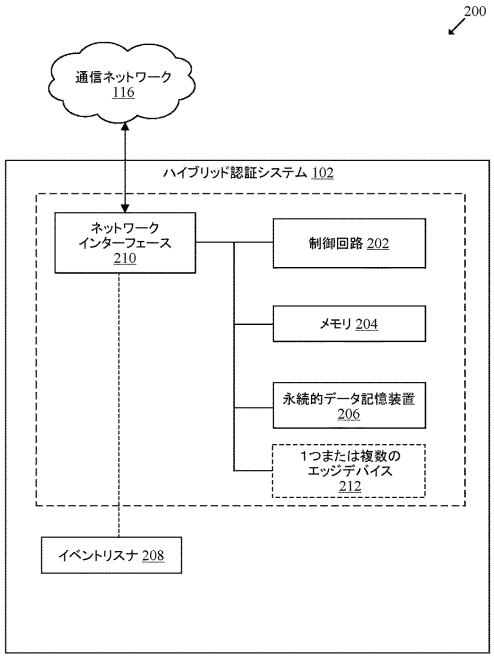


図2

【図３Ａ】

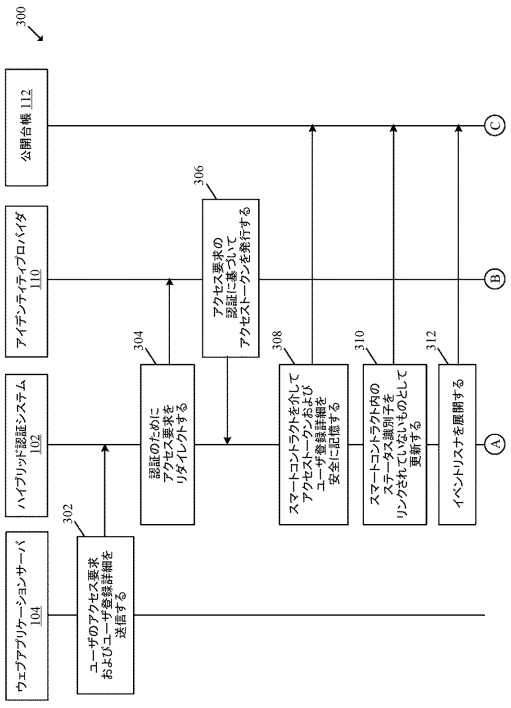


図3A

【図３Ｂ】

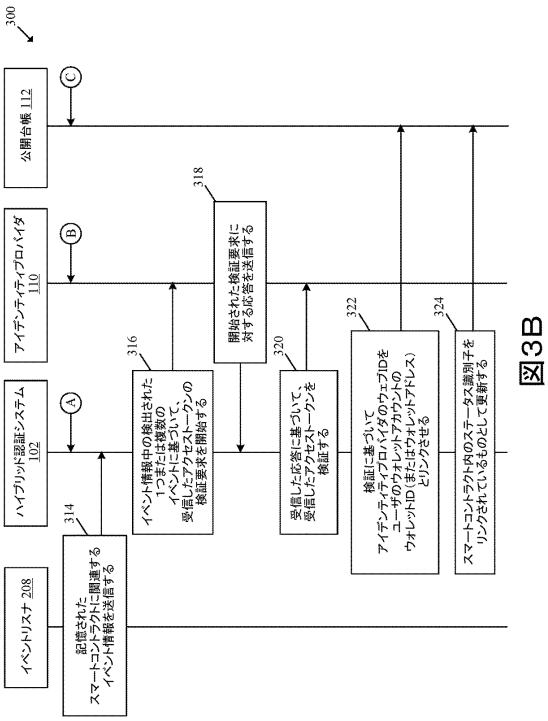


図3B

【図４Ａ】

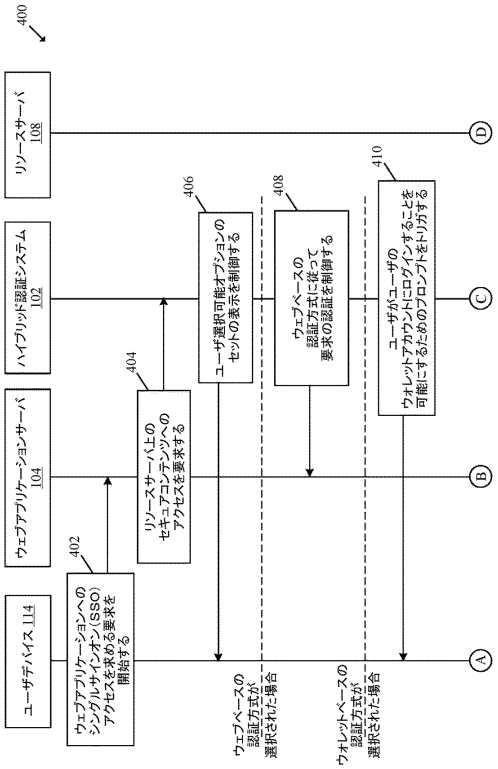


図4A

【図４Ｂ】

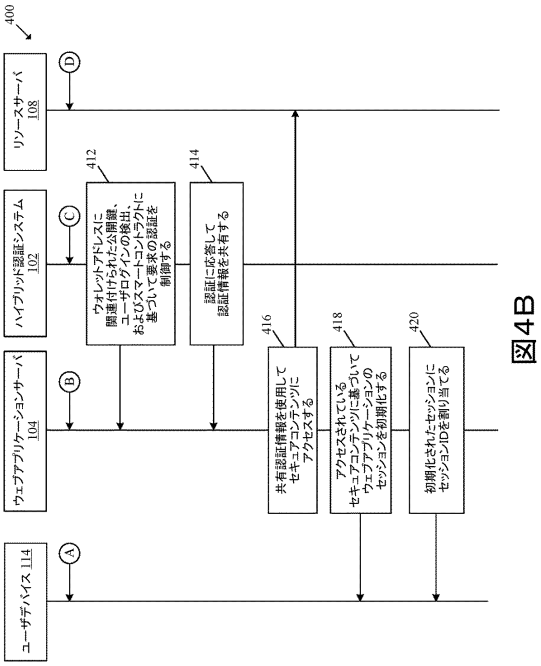


図4B

【図５】

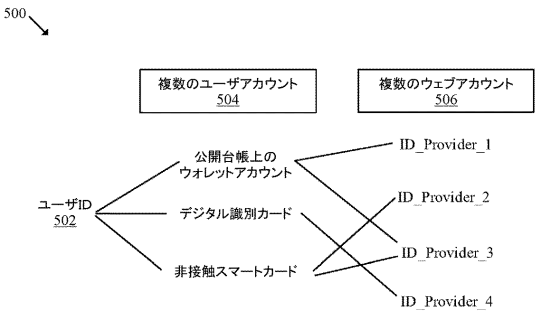


図5

【図６】

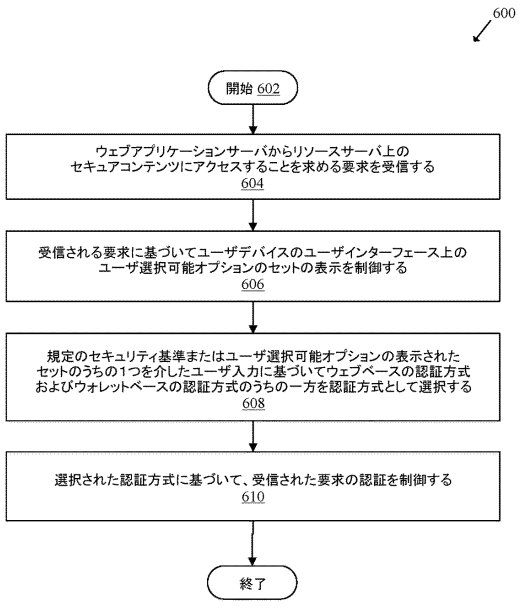


図6

フロントページの続き

ドソフトウェアセンタープライベートリミテッド内
(72)発明者　ピンギリ シュリニヴァーサ
インド カルナータカ州、５６０　１０３、バンガロール市 ヴァルツルホブリ、デヴァラベサネハリ、アウターリンクロード エンバシー テク ヴィレッジ、ハイビスカス タワー２　２階 ソニーインドソフトウェアセンタープライベートリミテッド内
(72)発明者　小野 孝一
東京都港区港南１丁目７番１号 ソニー株式会社内

審査官　平井 誠

(56)参考文献　米国特許出願公開第２０１８／０１３９１９９（ＵＳ，Ａ１）
米国特許出願公開第２０１９／０２８１０２８（ＵＳ，Ａ１）
特開２０１５－０９０６２０（ＪＰ，Ａ）

(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／４１
Ｇ０６Ｆ　２１／３３