(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7586818号
(P7586818)

(45)発行日　令和6年11月19日(2024.11.19)

(24)登録日　令和6年11月11日(2024.11.11)

(51)国際特許分類

Ｇ０６Ｆ　21/31　(2013.01)		Ｇ０６Ｆ	21/31
Ｇ０６Ｆ　21/32　(2013.01)		Ｇ０６Ｆ	21/32

ＦＩ

請求項の数　15　（全28頁）

(21)出願番号　特願2021-533228(P2021-533228)
(86)(22)出願日　令和1年12月10日(2019.12.10)
(65)公表番号　特表2022-512202(P2022-512202A)
(43)公表日　令和4年2月2日(2022.2.2)
(86)国際出願番号　PCT/US2019/065521
(87)国際公開番号　WO2020/123535
(87)国際公開日　令和2年6月18日(2020.6.18)
審査請求日　令和4年8月23日(2022.8.23)
(31)優先権主張番号　62/778,106
(32)優先日　平成30年12月11日(2018.12.11)
(33)優先権主張国・地域又は機関
米国(US)
前置審査

(73)特許権者　505468864
ビザ インターナショナル サービス アソシエーション
アメリカ合衆国、９４１２８－８９９９　カリフォルニア州、サン フランシスコ、ピー．オー． ボックス ８９９９
(74)代理人　110000855
弁理士法人浅村特許事務所
(72)発明者　フレンド、エリック クリストファー
アメリカ合衆国、カリフォルニア、マウンテンビュー、バーバラ アベニュー ２９７
(72)発明者　バンクストン、マイケル スティーブン
アメリカ合衆国、カリフォルニア、オークランド、ブルネル ドライブ ３３５３

最終頁に続く

(54)【発明の名称】　リソースアクセスのための信頼トークン

(57)【特許請求の範囲】

【請求項１】

ユーザーデバイス上の第１のアプリケーションからサーバーコンピュータによって、ユーザーが認証されたという表示を受信することと、

前記ユーザーデバイス上の第２のアプリケーションから前記サーバーコンピュータによって、前記ユーザーが検出されたという表示を受信することであって、前記ユーザーデバイスが前記ユーザー上のウェアラブルデバイスから前記ユーザーが検出されたという表示を受信する、受信することと、

前記サーバーコンピュータによって、前記ユーザーが、前記ユーザーのデジタルアイデンティティに関連付けられたユーザーデータへのアクセスを承認されたと判定することと、

前記２つの表示をある期間内に受信することに基づいて及び前記ユーザーが前記ユーザーの前記デジタルアイデンティティに関連付けられた前記ユーザーデータへの前記アクセスを承認されたとの前記判定に基づいて、前記ユーザーに対して信頼トークンを生成または維持することと、

前記サーバーコンピュータによって、定期的に受信される前記ユーザーが検出されたとの表示に基づいて記録を定期的に更新することであって、前記信頼トークンが前記記録に基づいて維持される、更新することと、

を含み、

前記信頼トークンは、リソースへのアクセスを許可するために使用されるインジケータである、方法。

【請求項２】
前記ユーザーデバイス上の前記第２のアプリケーションから前記サーバーコンピュータによって、前記ユーザーが検出されないという表示を受信することと、
前記ユーザーが検出されないという前記表示を受信することに基づいて、前記信頼トークンを無効にすることと、さらに含む、請求項１に記載の方法。
【請求項３】
前記サーバーコンピュータによって、前記ユーザーが、前記ユーザーの前記デジタルアイデンティティに関連付けられた前記ユーザーデータへのアクセスを無効にされたと判定することと、
前記ユーザーが前記アクセスを無効にされたと判定することに基づいて、前記サーバーコンピュータによって前記信頼トークンを無効にすることと、をさらに含む、請求項１に記載の方法。
【請求項４】
前記期間が第１の期間であり、かつ前記ユーザーが、第２の期間の間、前記ユーザーの前記デジタルアイデンティティに関連付けられた前記ユーザーデータへのアクセスを承認され、前記方法が、
前記サーバーコンピュータによって、前記第２の期間が期限切れになったと判定することと、
前記第２の期間が期限切れになったと判定することに基づいて、前記サーバーコンピュータによって前記信頼トークンを無効にすることと、をさらに含む、請求項１に記載の方法。
【請求項５】
前記サーバーコンピュータによって、前記ユーザーのデジタルアイデンティティを識別することであって、前記信頼トークンが前記ユーザーの前記デジタルアイデンティティと関連付けて保存されることと、をさらに含む、請求項１に記載の方法。
【請求項６】
前記ユーザーが検出されたという前記表示が、前記ユーザーの検出された心拍に対応する、請求項１に記載の方法。
【請求項７】
前記サーバーコンピュータによって、前記ユーザーの前記検出された心拍を前記ユーザーの保存された心拍と比較することと、
前記比較に基づいて、前記サーバーコンピュータによって、前記検出された心拍が前記保存された心拍と一致することを判定することであって、前記信頼トークンが、前記検出された心拍が前記保存された心拍と一致するという前記判定に基づいてさらに生成または維持される、判定することと、をさらに含む、請求項６に記載の方法。
【請求項８】
サーバーコンピュータであって、
プロセッサと、
前記プロセッサに動作可能に連結された、コンピュータ可読媒体と、を備え、
ユーザーデバイス上の第１のアプリケーションから、ユーザーが認証されたという表示を受信することと、
前記ユーザーデバイス上の第２のアプリケーションから、前記ユーザーが検出されたという表示を受信することであって、前記ユーザーデバイスが、前記ユーザー上のウェアラブルデバイスから前記ユーザーが検出されたという表示を受信する、受信することと、
前記サーバーコンピュータによって、前記ユーザーが、前記ユーザーのデジタルアイデンティティに関連付けられたユーザーデータへのアクセスを承認されたと判定することと、
前記２つの表示をある期間内に受信することに基づいて及び前記ユーザーが前記ユーザーのデジタルアイデンティティに関連付けられた前記ユーザーデータへの前記アクセスを承認されたとの前記判定に基づいて、前記ユーザーに対して信頼トークンを生成または維持することと、

定期的に受信される前記ユーザーが検出されたとの表示に基づいて記録を定期的に更新することであって、前記信頼トークンが前記記録に基づいて維持される、更新することと、を含み、前記信頼トークンは、リソースへのアクセスを許可するために使用されるインジケータである、方法を実施するための、サーバーコンピュータ。

【請求項９】

前記方法が、

前記ユーザーデバイス上の前記第２のアプリケーションから、前記ユーザーが検出されないという表示を受信することと、

前記ユーザーが検出されないという前記表示を受信することに基づいて、前記信頼トークンを無効にすることと、をさらに含む、請求項８に記載のサーバーコンピュータ。

【請求項１０】

前記方法が、

前記サーバーコンピュータによって、前記ユーザーが、前記ユーザーの前記デジタルアイデンティティに関連付けられた前記ユーザーデータへの前記アクセスを無効にされたと判定することと、

前記ユーザーが前記アクセスを無効にされたと判定することに基づいて、前記サーバーコンピュータによって前記信頼トークンを無効にすることと、をさらに含む、請求項８に記載のサーバーコンピュータ。

【請求項１１】

前記期間が第１の期間であり、かつ前記ユーザーが、第２の期間の間、前記ユーザーの前記デジタルアイデンティティに関連付けられた前記ユーザーデータへのアクセスを承認され、前記方法が、

前記サーバーコンピュータによって、前記第２の期間が期限切れになったと判定することと、

前記第２の期間が期限切れになったと判定することに基づいて、前記サーバーコンピュータによって前記信頼トークンを無効にすることと、を含む、請求項８に記載のサーバーコンピュータ。

【請求項１２】

前記信頼トークンが、前記ユーザーの前記デジタルアイデンティティと関連付けて保存される、請求項８に記載のサーバーコンピュータ。

【請求項１３】

前記ユーザーが検出されたという前記表示が、前記ユーザーの検出された心拍に対応し、

前記方法が、

前記ユーザーの前記検出された心拍を前記ユーザーの保存された心拍と比較することと、

前記比較に基づいて、前記検出された心拍が前記保存された心拍と一致することを判定することであって、前記信頼トークンが、前記検出された心拍が前記保存された心拍と一致するという前記判定に基づいてさらに生成または維持される、判定することと、をさらに含む、請求項８に記載のサーバーコンピュータ。

【請求項１４】

ユーザーデバイスによって、ユーザーが認証されたと判定することと、

前記ユーザーデバイスによってサーバーコンピュータへと、前記ユーザーが認証されたという表示を送信することと、

前記ユーザーデバイスによって、前記ユーザーが検出されたことを判定することであって、前記ユーザーデバイスが、前記ユーザーの心拍を検出することに基づいてウェアラブルデバイスによって生成された情報に基づいて前記ユーザーが検出されたことを判定することと、

前記ユーザーデバイスによって前記サーバーコンピュータへと、前記ユーザーが検出されたという表示を送信することと、を含む方法であり、

前記サーバーコンピュータが、前記ユーザーのデジタルアイデンティティに関連付けら

れたユーザーデータへのアクセスを承認されたと判定し、ある期間内に前記２つの表示を受信することに基づいて及び前記ユーザーが前記ユーザーのデジタルアイデンティティに関連付けられた前記ユーザーデータへの前記アクセスを承認されたとの前記判定に基づいて、前記ユーザーに対して信頼トークンを生成または維持し、前記信頼トークンは、リソースへのアクセスを許可するために使用されるインジケータであり、
さらに、前記方法は、前記ユーザーが検出されたという追加的な表示を、前記ユーザーデバイスによって前記サーバーコンピュータへと定期的に送信することであって、前記追加的な表示が前記信頼トークンを維持するために使用される、送信することを含み、
前記サーバーコンピュータが、定期的に受信される前記ユーザーが検出されたとの表示に基づいて記録を定期的に更新することであって、前記信頼トークンが前記記録に基づいて維持される、方法。

【請求項１５】

前記ユーザーデバイスによって前記ウェアラブルデバイスから、前記ユーザーが検出されないという表示を受信することと、

前記ユーザーデバイスによって前記サーバーコンピュータへと、前記ユーザーが検出されないという前記表示を送信することであって、前記信頼トークンが前記ユーザーが検出されないという前記表示に基づいて無効にされる、送信することと、をさらに含む請求項１４に記載の方法。

【発明の詳細な説明】

【技術分野】

【０００１】

関連出願の相互参照

本出願は、２０１８年１２月１１日に出願された米国仮特許出願第６２／７７８，１０６号の優先権を主張するＰＣＴ出願であり、その全体は参照により本明細書に組み込まれる。

【背景技術】

【０００２】

セキュアなリソースへのアクセスは、１つ以上の認証方法に基づいて許可される。例えば、ユーザーはセキュアなウェブサイトまたはアプリケーションにログインしてもよい。別の例として、ユーザーは、セキュアな建物へのアクセスを得るために認証情報または生体認証を提示してもよい。リソースがよりセキュアであるほど、より多くの認証が必要とされる場合がある。例えば、セキュアなリソースは、ステップアップ認証、または複数の形態の身分証明を必要とする場合がある。これらの認証方法がより煩わしくなるにつれて、ユーザーがリソースへのアクセスを取り戻すためにますます手間がかかるようになる場合がある。例えば、ユーザーは、ユーザー名とパスワードで銀行のウェブサイトにログインしてもよい。次いで、ユーザーは、テキストメッセージで受信したアクセスコードを入力することによって、ステップアップ認証プロセスを実行しなければならない場合がある。セッションが期限切れになった後に、ユーザーが再度ログインしなければならない場合、ユーザーは、複数の認証フェーズを再度受けなければならないことにわずらわしさを経験する場合がある。

【０００３】

ユーザーを過度に再認証する必要性を回避するために、リソースへのアクセスがある時間の間長くなる場合がある。ウェブサイトへのユーザーのログインを保持する１つのやり方は、クッキーの使用を通したやり方である。クッキーは、セッションの開始時に発行され、そしてセッションの終了時に期限切れになる。例えば、ユーザーが手動でログアウトしたとき、および／またはある期間（例えば、５分間）が経過した後、クッキーが期限切れになる場合がある。セッションを延長するためのクッキーの使用は、セキュリティを欠いている。クッキーは、改ざんおよび複数のエンティティへの曝露に対して脆弱である。

【０００４】

実施形態は、これらのおよびその他の問題に、個別に、および総合的に対処する。

【発明の概要】
【課題を解決するための手段】
【０００５】
本明細書に記載される方法は、リソースにセキュアにアクセスし、かつ限られたコンピューティングリソースを使用するユーザーの能力を拡張する方法を提供する。
【０００６】
実施形態は、ユーザーデバイス上の第１のアプリケーションからサーバーコンピュータによって、ユーザーが認証されたという表示を受信することと、ユーザーデバイス上の第２のアプリケーションからサーバーコンピュータによって、ユーザーが検出されたという表示を受信することであって、ユーザーが検出されたという表示をユーザー上のウェアラブルデバイスからユーザーデバイスが受信する、受信することと、これらの２つの表示をある期間内に受信することに基づいて、ユーザーのために信頼トークンを生成または維持することと、を含む方法を含む。
【０００７】
一部の態様では、方法は、ユーザーデバイス上の第２のアプリケーションからサーバーコンピュータによって、ユーザーが検出されないという表示を受信することと、ユーザーが検出されないという表示を受信することに基づいて、信頼トークンを無効にすることと、をさらに含む。一部の態様では、方法は、サーバーコンピュータによって、ユーザーがユーザーのデジタルアイデンティティに関連付けられたユーザーデータへの承認されたアクセスを有することを判定することをさらに含み、ユーザーがユーザーのデジタルアイデンティティに関連付けられたユーザーデータへのアクセスを承認されたことを判定することに基づいて、信頼トークンが生成される。一部の態様では、方法は、サーバーコンピュータによって、ユーザーがユーザーのデジタルアイデンティティに関連付けられたユーザーデータへのアクセスを無効にされたことを判定することと、サーバーコンピュータによって、ユーザーがアクセスを無効にされたと判定することに基づいて信頼トークンを無効にすることと、をさらに含む。
【０００８】
一部の態様では、期間は第１の期間であり、またユーザーは、第２の期間の間、ユーザーのデジタルアイデンティティに関連付けられたユーザーデータへの承認されたアクセスを有し、方法は、サーバーコンピュータによって、第２の期間が期限切れになったことを判定することと、サーバーコンピュータによって、第２の期間が期限切れになったことを判定することに基づいて信頼トークンを無効にすることと、をさらに含む。一部の態様では、方法は、サーバーコンピュータによって、ユーザーのデジタルアイデンティティを識別することをさらに含み、信頼トークンはユーザーのデジタルアイデンティティに関連付けられて保存される。一部の態様では、方法は、サーバーコンピュータによって、定期的に受信されるユーザーが検出されたという表示に基づく記録を定期的に更新することをさらに含むものであって、信頼トークンは、記録に基づいて維持される。
【０００９】
一部の態様では、ユーザーが検出されたという表示は、検出されたユーザーの心拍に対応する。一部の態様では、方法は、サーバーコンピュータによって、検出されたユーザーの心拍を、保存されたユーザーの心拍と比較することと、サーバーコンピュータによって、比較に基づいて、検出された心拍が保存された心拍と一致することを判定することと、をさらに含み、検出された心拍が保存された心拍と一致するという判定に基づいて信頼トークンがさらに生成または維持される。
【００１０】
実施形態は、プロセッサと、プロセッサに動作可能に連結されたコンピュータ可読媒体と、を備える、上述の方法を実行するためのサーバーコンピュータを含む。
【００１１】
実施形態は、ユーザーデバイスによって、ユーザーが認証されたことを判定することと、ユーザーデバイスによってサーバーコンピュータへと、ユーザーが認証されたという表

示を送信することと、ユーザーデバイスによって、ユーザーが検出されたことを判定することであって、ユーザーデバイスが、ユーザーの心拍を検出することに基づいてウェアラブルデバイスによって生成された情報に基づいてユーザーが検出されたことを判定する、判定することと、ユーザーデバイスによってサーバーコンピュータへと、ユーザーが検出されたという表示を送信することと、を含み、サーバーコンピュータが、ある期間内に２つの表示を受信することに基づいて、ユーザーのために信頼トークンを生成または維持する方法を含む。

【００１２】

一部の態様では、方法は、ユーザーデバイスによってウェアラブルデバイスから、ユーザーが検出されないという表示を受信することと、ユーザーデバイスによってサーバーコンピュータへと、ユーザーが検出されないという表示を送信することと、をさらに含み、信頼トークンは、ユーザーが検出されないという表示に基づいて無効にされる。一部の態様では、方法は、ユーザーデバイスによってサーバーコンピュータへと、ユーザーが検出されたという追加的な表示を定期的に送信することをさらに含み、追加的な表示は信頼トークンを維持するために使用される。

【００１３】

実施形態は、プロセッサと、プロセッサに動作可能に連結されたコンピュータ可読媒体と、を備える、上述の方法を実行するためのユーザーデバイスを含む。

【図面の簡単な説明】

【００１４】

【図１】図１は、一部の実施形態による信頼トークンを管理するためのシステムおよび方法の概略図を示す。

【図２】図２は、一部の実施形態によるサーバーコンピュータのブロック図を示す。

【図３】図３は、一部の実施形態によるユーザーデバイスのブロック図を示す。

【図４】図４は、一部の実施形態によるデジタルアイデンティティプラットフォームのブロック図を示す。

【図５】図５は、一部の実施形態による信頼トークンを使用する例示的な使用を示す。

【図６】図６は、一部の実施形態による信頼トークンを使用してリソースへのアクセスを許可するための技法のフローチャートを示す。

【発明を実施するための形態】

【００１５】

様々な実施形態を論じる前に、一部の用語をさらに詳細に説明することができる。

【００１６】

「ユーザー」は、個人を含んでもよい。一部の実施形態では、ユーザーは、１つ以上の個人のアカウントおよび／またはユーザーデバイスと関連付けられてもよい。ユーザーはまた、一部の実施形態では、カード保有者、アカウント保有者、または消費者と称されてもよい。

【００１７】

「ユーザーデバイス」は、ユーザーによって操作されるうる任意の好適なデバイスであってもよい。ユーザーデバイスには、携帯電話、携帯情報端末（ＰＤＡ）、ポケベル、タブレット、パソコン、およびこれに類するものが含まれてもよい。追加的な例として、ユーザーデバイスは、ウェアラブルデバイス（例えば、時計、リング等）を含んでもよい。ユーザーデバイスは、こうした機能を実行するための任意の好適なハードウェアおよびソフトウェアを備えてもよく、また複数のデバイスまたは構成要素を含んでもよい。

【００１８】

「リソースプロバイダー」は、物品、サービス、情報、および／またはアクセスなどの、リソースを提供することができるエンティティであってもよい。リソースプロバイダーの例としては、小売業者、データプロバイダー、輸送機関、政府機関、会場、住宅運営業者などが挙げられる。リソースプロバイダーは、リソースプロバイダーのコンピュータを操作してもよい。

【００１９】
「認証」という用語とその派生語は、明らかにされるべきエンドポイントの認証情報（アプリケーション、人、デバイス、プロセス、システムが挙げられるが、これらに限定されない）を検証し、エンドポイントが誰であるかを確認するプロセスを指す。
【００２０】
「識別子」という用語は、何かを識別するために使用されてもよい任意の情報を指す場合がある。一部の実施形態では、識別子は、ランダムに、または所定のアルゴリズム、コード、または共有シークレットに従って生成された特別な値であってもよい。例えば、個人は、運転免許証番号または暗号化キーを使用して識別されてもよい。一部の実施形態では、識別子は、１つ以上のグラフィック、トークン、バーコード、クイックレスポンス（ＱＲ）コード、またはエンティティを一意に識別するために使用されてもよい任意の他の情報の形態であってもよい。
【００２１】
「識別属性」は、エンティティ（例えば、個人、組織、物、またはこれに類するもの）についての情報の特定の一部を指す場合がある。識別属性の例としては、社会保障番号、年齢、電話番号、および個人に関連付けられた銀行口座番号が挙げられる。
【００２２】
「デジタルアイデンティティ」（ＤＩ）は、エンティティ（例えば、個人、組織、または物）についてのセキュアな情報の組を含んでもよい。ＤＩは、複数の識別属性だけでなく、デジタルアイデンティティを識別するデジタルアイデンティティ識別子も含んでもよい。例えば、ユーザーに対するＤＩであるＪｏｅ　Ｓｍｉｔｈは、ユーザーの生年月日、社会保障番号、住所、運転免許証番号などの識別属性だけでなく、Ｊｏｅ　Ｓｍｉｔｈのデジタルアイデンティティを識別するために使用されるＪｏｅ＿Ｓｍｉｔｈ＿１２３４などの識別子を含んでもよい。ＤＩは、セキュアな様態で別のエンティティに対して利用可能にされてもよい。ＤＩは、利害関係者間の合意および暗号化などのセキュリティ対策に依拠する場合がある。
【００２３】
「信頼トークン」は、リソースへのアクセスを許可するために使用することができるインジケータを含んでもよい。信頼トークンは、例えば、ユーザーがセキュアなシステムに認証されたままである期間を延長するために使用されてもよい。信頼トークンは、サーバーコンピュータによって管理されるクラウドストレージシステムなどのデータストアに保存されてもよい。信頼トークンは、バイナリであってもよく、またはコード化された情報を含んでもよい。信頼トークンは、ユーザー識別子、エンティティ識別子、タイムスタンプ、デジタルアイデンティティなどの追加的な情報を含んでもよく、または追加的な情報に関連付けて保存されてもよい。一部の実施形態では、信頼トークンは、１つ以上のそれぞれのリソースへのアクセスを許可するかどうかを判定するために、１つ以上のエンティティによって見ることができてもよい。データストアは、各々を特定のユーザーおよび／またはエンティティと関連付けて、複数の信頼トークンを保存してもよい。例えば、信頼トークンは、認証されたユーザーに対するユーザー識別子およびユーザーが認証されているエンティティに対するエンティティ識別子と関連付けて保存されてもよい。
【００２４】
「アクセスデバイス」は、リソースへのアクセスを得るための任意の好適なデバイスであってもよい。アクセスデバイスは、一般に、小売業者の場所など、任意の好適な場所に位置付けられてもよい。アクセスデバイスは、任意の好適な形態であってもよい。アクセスデバイスの一部の例としては、販売時点情報管理（ＰＯＳ）デバイス、携帯電話、携帯情報端末（ＰＤＡ）、パソコン（ＰＣ）、タブレットＰＣ、ハンドヘルド専用リーダ、セットトップボックス、電子キャッシュレジスタ（ＥＣＲ）、現金自動預入支払機（ＡＴＭ）、仮想キャッシュレジスタ（ＶＣＲ）、キオスク、セキュリティシステム、アクセスシステム、ウェブサイト、およびこれに類するものが挙げられる。アクセスデバイスは、任意の好適な接触または非接触の動作モードを使用して、支払デバイスおよび／またはポー

タブルデバイスにデータを送信もしくはこれらから受信し、または支払デバイスおよび／またはポータブルデバイスと関連付けられたデータを送信もしくは受信してもよい。

【００２５】

「プロセッサ」は、任意の好適なデータ計算デバイス（複数可）を指す場合がある。プロセッサは、所望の機能を達成するために協働する１つ以上のマイクロプロセッサを備えてもよい。プロセッサは、ユーザー要求および／またはシステム生成要求を実行するためのプログラムコンポーネントを実行するために適切な、少なくとも１つの高速データプロセッサを備えるＣＰＵを含んでもよい。ＣＰＵは、ＡＭＤのＡｔｈｌｏｎ、Ｄｕｒｏｎ、および／またはＯｐｔｅｒｏｎ、ＩＢＭおよび／またはＭｏｔｏｒｏｌａのＰｏｗｅｒＰＣ、ＩＢＭおよびＳｏｎｙのＣｅｌｌ ｐｒｏｃｅｓｓｏｒ、ＩｎｔｅｌのＣｅｌｅｒｏｎ、Ｉｔａｎｉｕｍ、Ｐｅｎｔｉｕｍ、Ｘｅｏｎ、および／またはＸＳｃａｌｅ、および／またはこれに類するプロセッサ（複数可）などのマイクロプロセッサであってもよい。

【００２６】

「メモリ」は、電子データを保存することができる、任意の好適なデバイス（複数可）であってもよい。好適なメモリは、所望の方法を実施するためにプロセッサによって実行することができる命令を保存する、非一時的コンピュータ可読媒体を含んでもよい。メモリの例として、１つ以上のメモリチップ、ディスクドライブ等が挙げられる場合がある。こうしたメモリは、任意の好適な電気的、光学的、および／または磁気的な動作モードを使用して動作してもよい。

【００２７】

「サーバーコンピュータ」は、強力なコンピュータ、またはコンピュータのクラスタを含んでもよい。例えば、サーバーコンピュータは、大型メインフレーム、ミニコンピュータクラスタ、またはユニットとして機能するサーバー群とすることができる。一例では、サーバーコンピュータは、ウェブサーバーに連結されたデータベースサーバーであってもよい。サーバーコンピュータは、データベースに連結されてもよく、また１つ以上のクライアントのコンピュータからの要求にサービスを提供する、任意のハードウェア、ソフトウェア、他のロジック、または前述の組み合わせを含んでもよい。サーバーコンピュータは、１つ以上の計算装置を含んでもよく、また１つ以上のクライアントコンピュータからの要求にサービスを提供するための、様々な計算構造、配設、およびコンパイルのうちのいずれを使用してもよい。

【００２８】

「リソースプロバイダー」は、取引中にリソース（例えば、物品、サービス、セキュアなデータへのアクセス、場所へのアクセス、またはこれに類するもの）を提供する任意の好適なエンティティとすることができる。例えば、リソース提供機関は、小売業者、施設運営者、建物所有者、政府機関などとすることができる。「小売業者」は典型的に、取引に従事し、かつ物品もしくはサービスを販売する、または物品もしくはサービスへのアクセスを提供することができるエンティティであってもよい。

【００２９】

実施形態は、リソースへのユーザーアクセスを許可するために使用されてもよい信頼トークンを提供する。信頼トークンは、ある期間内に２つのアプリケーションから確認を受信したときに生成されてもよい。例えば、第１のアプリケーションは、ユーザーが認証プロセス（例えば、安全な場所へのアクセスを得るために銀行のウェブサイト上のステップアップ認証を介して、網膜スキャンを介して等）を受けたという通知を送信してもよい。第２のアプリケーションは、ユーザーがウェアラブルデバイスを着用していること、およびウェアラブルデバイスがユーザーの心拍を検出するという表示を送信してもよい。両方の通知が閾値期間内に受信された場合、サーバーコンピュータは、ユーザーが信頼されており、かつリソースへのアクセスを許可することができることを示す信頼トークンを発行してもよい。例えば、信頼トークンは、当面はステップアップすることなく、ユーザーの銀行のウェブサイトへのログインを保持してもよく、またはユーザーが、当面は別の網膜スキャンを行うことなく、セキュアな場所にアクセスを得ることを可能にしてもよい。別

の方法として、または追加的に、ユーザーは、その期間中に他のリソースへのアクセスを許可される場合がある。

【００３０】

図１は、一部の実施形態による信頼トークンを管理するためのシステムおよび方法の概略図を示す。システム１００は、サーバーコンピュータ１０６、第１のユーザーデバイス１０２、第２のユーザーデバイス１０４、エンティティコンピュータ１０８、およびデータストア１０９を含んでもよい。

【００３１】

図１に図示したシステムの構成要素は、任意の好適な通信チャネルまたは通信ネットワークを通して互いに動作可能に通信することができる。好適な通信ネットワークは、直接相互接続、インターネット、ローカルエリアネットワーク（ＬＡＮ）、メトロポリタンエリアネットワーク（ＭＡＮ）、インターネット上のノードとしてのオペレーティングミッション（Ｏｐｅｒａｔｉｎｇ Ｍｉｓｓｉｏｎｓ ａｓ Ｎｏｄｅｓ ｏｎ ｔｈｅ Ｉｎｔｅｒｎｅｔ （ＯＭＮＩ））、セキュアなカスタム接続、ワイドエリアネットワーク（ＷＡＮ）、無線ネットワーク（例えば、ワイヤレスアプリケーションプロトコル（ＷＡＰ）、Ｉ－モード、および／またはこれに類するものなど、しかしこれらに限定されないのプロトコルを採用する）および／またはこれに類するもののうちのいずれか１つおよび／またはそれらの組み合わせであってもよい。コンピュータ、ネットワーク、およびデバイス間のメッセージは、ファイル転送プロトコル（ＦＴＰ）、ハイパーテキスト転送プロトコル（ＨＴＴＰ）、セキュアハイパーテキスト転送プロトコル（ＨＴＴＰＳ）、セキュアソケットレイヤー（ＳＳＬ）、ＩＳＯ（例えば、ＩＳＯ ８５８３）、および／またはこれに類するものなどの、しかしこれらに限定されないセキュアな通信プロトコルを使用して送信されてもよい。

【００３２】

説明の単純化のために、ある特定の数の構成要素が図１に示されている。しかしながら、実施形態は、２つ以上の各構成要素を含んでもよいことが理解される。例えば、エンティティコンピュータ１０８および／またはサーバーコンピュータ１０６と動作可能な通信にある第１のユーザーデバイス１０２を含む、複数のユーザーデバイスあるものとすることができる。

【００３３】

第１のユーザーデバイス１０２は、ユーザーによって操作可能であり、かつアプリケーションを実行する能力を有するデバイスであってもよい。例として、第１のユーザーデバイス１０２は、スマートフォン、コンピュータ、タブレット、またはこれに類するものであってもよい。第１のユーザーデバイス１０２は、様々なアプリケーションを実行してもよい。第１のユーザーデバイス１０２などの例示的なユーザーデバイスの構成要素および機能は、下記で図３に関してさらに説明される。

【００３４】

エンティティコンピュータ１０８は、リソースプロバイダーなどのエンティティに関連付けられたサーバーコンピュータであってもよい。エンティティコンピュータ１０８は、第１のアプリケーション１０２Ａを管理する同一のエンティティに関連付けられてもよい。例えば、第１のアプリケーション１０２Ａは銀行のアプリケーションであり、またエンティティコンピュータ１０８は対応する銀行のサーバーコンピュータである。別の例として、第１のアプリケーション１０２Ａは、小売業者のアプリケーション（例えば、オンラインショッピング用）であり、エンティティコンピュータ１０８は、対応する小売業者のサーバーコンピュータである。別の例として、第１のアプリケーション１０２Ａは、（例えば、輸送システムへのアクセスを制御するための）輸送アプリケーションであり、またエンティティコンピュータ１０８は、対応する輸送機関のサーバーコンピュータである。

【００３５】

第２のユーザーデバイス１０４は、ユーザーを検出する能力を有するデバイスであってもよい。第２のユーザーデバイスは、スマートウォッチ、光学式ヘッドマウントディスプ

レイ、スマートリング、またはこれに類するものなどのウェアラブルデバイスであってもよい。別の方法として、第２のユーザーデバイスは、ユーザーを検出する能力を有する別のタイプのデバイスであってもよい。例えば、移動電話は、触覚を介してユーザーの動きを検出してもよい。別の例として、１つ以上の監視カメラを使用して、ユーザーを検出してもよい。第２のユーザーデバイス１０４は、（例えば、検出された脈に基づいて）心拍を検出する機能を含んでもよい。第２のユーザーデバイス１０４は、経時的な心拍の特性をモニターする機能を含んでもよい。第２のユーザーデバイス１０４は、デバイスを着用するユーザーについての脈または他のデータを検出および／またはモニターする機能を含んでもよい。第２のユーザーデバイス１０４は、第１のユーザーデバイス１０２および／またはサーバーコンピュータ１０６に通信可能に連結されてもよい。第２のユーザーデバイス１０４は、ユーザーが検出された（またはもはや検出されなくなった）ときに、第１のユーザーデバイス１０２上のアプリケーションに通知する機能を含んでもよい。別の方法として、または追加的に、第２のユーザーデバイス１０４は、ユーザーが検出された（またはもはや検出されなくなった）ときにサーバーコンピュータ１０６に通知する機能を含んでもよい。

【００３６】

第１のユーザーデバイス１０２上で実行されるアプリケーションは、第１のアプリケーション１０２Ａを含んでもよい。第１のアプリケーション１０２Ａは、ユーザーを認証する機能を含んでもよい。例えば、第１のアプリケーション１０２Ａは、銀行のアプリケーションであってもよい。銀行のアプリケーションは、パスワード、個人識別番号（ＰＩＮ）、生体認証データ、またはこれに類するものを入力するようにユーザーに促す場合がある。次いで、このデータは、ユーザーを認証するために使用されてもよい。別の例として、第１のアプリケーション１０２Ａは、車両をキーレスで始動するためのアプリケーションであってもよい。一部では初回に車両をキーレスで始動する前に、アプリケーションは、生体認証、パスワード、またはこれに類するものを使用してユーザーを認証することを必要とする場合がある。

【００３７】

第１のアプリケーション１０２Ａは、サーバーコンピュータ１０６と通信する機能をさらに含んでもよい。第１のアプリケーション１０２Ａは、ユーザーが認証されたことを示す通知をサーバーコンピュータ１０６に送信してもよい。

【００３８】

第１のユーザーデバイス１０２上で実行されるアプリケーションは、第２のアプリケーション１０２Ｂを含んでもよい。第２のアプリケーション１０２Ｂは、第２のユーザーデバイス１０４と通信する（例えば、ユーザーが検出されるかどうかに関するメッセージを送信および／または受信する）機能を含んでもよい。一部の実施形態では、第２のアプリケーション１０２Ｂは、第２のユーザーデバイス１０４から生データ（例えば、脈拍数）を受信し、ユーザーが検出されるかどうかを判定するために生データを解析してもよい。第２のアプリケーション１０２Ｂは、サーバーコンピュータ１０６と通信する（例えば、ユーザーが検出されるかどうかに関するメッセージを送信および／または受信する）ための機能を含んでもよい。

【００３９】

一部の実施形態では、第１のアプリケーション１０２Ａおよび第２のアプリケーション１０２Ｂは、互いに直接的に通信することができない場合がある。例えば、スマートフォンでは、セキュリティの目的で、アプリケーションが互いに仕切られる場合がある。第１のアプリケーション１０２Ａおよび第２のアプリケーション１０２Ｂは、互いに直接的な通信が部分的または完全に妨げられる場合がある。よって、回避策として、１つのアプリケーションはサーバーコンピュータに情報を送信し、そしてサーバーコンピュータはもう１つのアプリケーションに情報を戻すように送信してもよい。別の方法として、アプリケーションが直接的に通信することができる場合、サーバーコンピュータに関して本明細書に記載される動作の一部は、第１のユーザーデバイス１０２上で実行されてもよい。

【００４０】
サーバーコンピュータ１０６は、信頼トークンを生成および管理するための機能を含んでもよい。一部の実施形態では、サーバーコンピュータ１０６は、記録１０６Ａに基づいて信頼トークンを生成してもよい。サーバーコンピュータ１０６などのサーバーコンピュータについてのさらなる詳細は、下記で図２に関してさらに詳細に説明される。サーバーコンピュータ１０６は、下記で図２に関してさらに説明されるように、信頼トークン１１０をデータストア１０９内に保存してもよい。
【００４１】
記録１０６Ａは、複数の条件に基づいてリソースへのアクセスを制御するために使用されてもよい。記録１０６Ａはセマフォとも呼ばれる場合があり、その記録１０６Ａは２つ以上のプロセスの同期を表す場合がある。記録１０６Ａは、変数、オブジェクト、またはこれに類するものとして表されてもよい。記録１０６Ａは、２つの肯定的な表示がある期間内に受信されたかどうかを判定するために使用されてもよい。図１に示すように、記録１０６Ａは、ユーザーが（ａ）認証され、かつ（ｂ）検出された（例えば、心拍、脈、監視システム等を用いて）場合、肯定的である（２つのチェックボックスによって示される）。記録１０６Ａは、例えば、１の値または「はい」を割り当てることによって肯定として表される。記録１０６Ａは、例えば、例えば、０の値または「いいえ」によって否定として表されてもよい（例えば、ユーザーは認証されない、かつ／または検出されない）。
【００４２】
一部の実施形態では、記録１０６Ａは、ユーザーが認証され、かつある期間内に検出される場合、肯定的であってもよい。例えば、ユーザーが認証から１秒以内に検出される。別の例として、ユーザーは、認証時間の周囲の３０秒の時間枠の間、連続的に検出される。サーバーコンピュータ１０６は、タイマーを使用して、ユーザーが特定の期間の間に、検出されるかどうかを判定してもよい。記録１０６Ａは、ユーザーが検出されない場合、もはや肯定的ではないように修正されてもよい。記録１０６Ａが肯定的である場合、システムは信頼トークン１１０を生成してもよい。
【００４３】
信頼トークン１１０は、記録１０６Ａに基づいて確立されたインジケータであってもよい。信頼トークン１１０は、下記で図６に関してさらに詳述するように、ユーザーがリソースへのアクセスを許可されるべきであることを示すために使用されてもよい。信頼トークン１１０は、サーバーコンピュータ１０６によって管理されるクラウドストレージシステムなどのデータストア１０９に保存されてもよい。信頼トークン１１０は、ユーザー識別子、エンティティ識別子、タイムスタンプ、デジタルアイデンティティなどの追加的な情報を含んでもよく、またはそれらに関連付けられて保存されてもよい。一部の実施形態では、信頼トークン１１０は、１つ以上のそれぞれのリソースへのアクセスを許可するかどうかを判定するために、１つ以上のエンティティによって見ることができてもよい。
【００４４】
信頼トークン１１０は、ユーザーが閾値期間の間に検出されない場合、無効にされる場合がある。閾値期間は、例としては、３０秒、３０分、または２時間であってもよい。具体的な例として、短いユーザーの心拍が検出されない期間は許可されてもよいが、ユーザーの心拍が１時間以上検出されない場合は、信頼トークンは無効にされる場合がある。
【００４５】
図２は、一部の実施形態によるサーバーコンピュータ２００のブロック図を示す。サーバーコンピュータ２００は、プロセッサ２０４を備えてもよい。プロセッサ２０４は、メモリ２０２、ネットワークインターフェース２０６、およびコンピュータ可読媒体２０８に連結されていてもよい。サーバーコンピュータ２００は、データストア２２０を含んでもよく、またはデータストア２２０に通信可能に連結されてもよい。
【００４６】
データストア２２０は、データを保存するためのストレージユニットおよび／またはデバイス（例えば、ファイルシステム、データベース、テーブルの集まり、または他のスト

レージ機構）であってもよい。データストア２２０は、複数の異なるストレージユニットおよび／またはデバイスを含んでもよい。例えば、データストア２２０は、１つ以上のエンティティコンピュータによって制限付きで（例えば、アクセスは、下記で図４に関してさらに説明されるように、サーバーコンピュータ２００によって管理される暗号化キーによって制御されてもよい）アクセス可能なクラウドストレージシステムであってもよい。

【００４７】

データストア２２０は、信頼トークン２２２を保存してもよい。図１に関して上述したように、信頼トークンは、記録に基づいてユーザーのための認証期間を延長するために使用されてもよい。データストア２２０は、各々が特定のユーザーおよび／またはエンティティと関連付けられている、複数の信頼トークン２２２を保存してもよい。例えば、信頼トークン２２２は、認証されたユーザーに対するユーザー識別子およびユーザーが認証されているエンティティに対するエンティティ識別子と関連付けて保存されてもよい。信頼トークン２２２は、ユーザーのデジタルアイデンティティと関連付けて保存されてもよい。

【００４８】

プロセッサ２０４は、１つ以上の集積回路（例えば、１つ以上のシングルコアもしくはマルチコアマイクロプロセッサおよび／またはマイクロコントローラ）として実装されてもよい。プロセッサ２０４は、サーバーコンピュータ２００の動作を制御するために使用されてもよい。プロセッサ２０４は、メモリ内に保存されたプログラムコードまたはコンピュータ可読コードに応答して、様々なプログラムを実行することができる。プロセッサ２０４は、同時に実行される複数のプログラムまたはプロセスを維持する機能を含んでもよい。

【００４９】

メモリ２０２は、データおよびコードを記憶するために使用することができる。メモリ２０２は、プロセッサ２０４に内部または外部で（例えば、クラウドベースのデータストレージ）連結されていてもよく、ＲＡＭ、ＤＲＡＭ、ＲＯＭ、フラッシュ、もしくは任意の他の好適なメモリデバイスなどの、揮発性メモリおよび／または不揮発性メモリの任意の組み合わせを備えてもよい。

【００５０】

ネットワークインターフェース２０６は、サーバーコンピュータ２００が外部コンピュータと通信することを可能にすることができるインターフェースを含んでもよい。ネットワークインターフェース２０６は、サーバーコンピュータ２００が、別のデバイス（例えば、エンティティコンピュータ１０８、承認コンピュータ等）との間でデータを通信することを可能にする場合がある。ネットワークインターフェース２０６のいくつかの例は、モデム、物理ネットワークインターフェース（イーサネットカードもしくは他のネットワークインターフェースカード（ＮＩＣ）など）、仮想ネットワークインターフェース、通信ポート、ＰＣメモリーカード国際協会（ＰＣＭＣＩＡ）スロットおよびカード、またはこれに類するものを含んでもよい。ネットワークインターフェース２０６によって有効になる無線プロトコルには、Ｗｉ－Ｆｉ（商標）を含んでもよい。ネットワークインターフェース２０６を介して転送されるデータは、電気信号、電磁信号、光信号、または外部通信インターフェースによって受信される能力を有する任意の他の信号（総称して「電子信号」または「電子メッセージ」と呼ばれる）であってもよい信号の形態であってもよい。データまたは命令を含んでもよいこれらの電子メッセージは、通信経路またはチャネルを介して、ネットワークインターフェース２０６と他のデバイスとの間に提供されてもよい。上述のように、例えば、ワイヤもしくはケーブル、光ファイバ、電話回線、セルラーリンク、無線周波数（ＲＦ）リンク、ＷＡＮもしくはＬＡＮネットワーク、インターネット、または任意の他の好適な媒体など、任意の好適な通信経路またはチャネルを使用してもよい。ネットワークインターフェース２０６は、長距離通信チャネルだけでなく、短距離通信チャネルも利用することができる。

【００５１】

コンピュータ可読媒体２０８は、記憶および／または送信のための１つ以上の非一時的

媒体を備えてもよい。好適な媒体としては、例として、ランダムアクセスメモリ（ＲＡＭ）、読み出し専用メモリ（ＲＯＭ）、ハードドライブもしくはフロッピーディスクなどの磁気媒体、またはコンパクトディスク（ＣＤ）もしくはＤＶＤ（デジタル多目的ディスク）などの光媒体、フラッシュメモリ、およびこれに類するものが挙げられる。コンピュータ可読媒体は、こうした記憶または送信デバイスの任意の組み合わせであってもよい。

【００５２】

コンピュータ可読媒体２０８は、一連の命令またはコマンドとして保存されるソフトウェアコードを含んでもよい。コンピュータ可読媒体２０８は、ユーザーデバイス上の第１のアプリケーションからサーバーコンピュータによって、ユーザーが認証されたという表示を受信することと、ユーザーデバイス上の第２のアプリケーションからサーバーコンピュータによって、ユーザーが検出されたという表示を受信することであって、ユーザーが検出されたという表示をユーザー上のウェアラブルデバイスからユーザーデバイスが受信する、受信することと、これらの２つの表示をある期間内に受信することに基づいて、ユーザーのために信頼トークンを生成または維持することと、を含む方法を実施するためのプロセッサ２０４によって実行可能なコードを含んでもよい。

【００５３】

コンピュータ可読媒体２０８は、通信モジュール２１０と、記録管理モジュール２１２と、信頼トークン生成モジュール２１４と、信頼トークン更新モジュール２１６と、を含んでもよい。これらのモジュールの各々は、プロセッサ２０４と併せて、下記で説明される機能を実行するように構成されたコードを含んでもよい。

【００５４】

通信モジュール２１０は、プロセッサ２０４にメッセージの生成、メッセージの転送、メッセージの再フォーマット、および／またはそうでなければ他のエンティティとの通信を行わせるコードを含んでもよい。

【００５５】

記録管理モジュール２１２は、プロセッサ２０４に記録を生成および維持させるコードを含んでもよい。記録管理モジュール２１２は、プロセッサ２０４と連携して、ユーザーデバイスから受信した情報に基づいて、記録（例えば、図１に関して上述した記録１０６Ａ）を生成してもよい。記録管理モジュール２１２は、プロセッサ２０４および通信モジュール２１０と連携して、ユーザー認証ステータスを特定するユーザーデバイスから表示を受信してもよい（例えば、ユーザーはユーザーデバイス上のセキュアなアプリケーションに最近ログインした）。記録管理モジュール２１２は、プロセッサ２０４および通信モジュール２１０と連携して、ユーザー検出ステータスを特定するユーザーデバイスから表示を受信してもよい（例えば、ユーザーの心拍は、ウェアラブルデバイスに連結されたアプリケーションによって検出される）。こうした情報に基づいて、記録管理モジュール２１２は、プロセッサ２０４と連携して、記録を更新してもよい。記録管理モジュール２１２は、さらに、記録についての情報を信頼トークン生成モジュール２１４および／または信頼トークン更新モジュール２１６に提供してもよい。

【００５６】

信頼トークン生成モジュール２１４は、プロセッサ２０４に信頼トークンを生成させるコードを備えてもよい。信頼トークン生成モジュール２１４は、プロセッサ２０４および記録管理モジュール２１２と連携して、記録（例えば、図１に関して上述の記録１０６Ａ）をモニターする。記録が肯定的である（例えば、ユーザーがある期間内に認証され、かつ検出される）場合、信頼トークン生成モジュール２１４は、プロセッサ２０４と連携して信頼トークン２２２を生成してもよい。信頼トークン生成モジュールは、特定のユーザーと関連付けて信頼トークン２２２を生成し、そしてデータストア２２０に保存することによって、プロセッサ２０４に信頼トークン２２２を生成させるコードを含んでもよい。

【００５７】

信頼トークン更新モジュール２１６は、プロセッサ２０４に信頼トークン２２２を更新させるコードを含んでもよい。信頼トークン更新モジュール２１６は、プロセッサ２０４

と連携して、記録（例えば、図１に関する記録１０６Ａ）をモニターしてもよい。記録が変更される場合、信頼トークン更新モジュール２１６は、プロセッサ２０４と連携して、信頼トークン２２２を更新してもよい。例えば、記録が肯定から否定へと変更される場合、信頼トークン更新モジュール２１６は、プロセッサ２０４と連携して信頼トークン２２２を無効にする場合がある。信頼トークン２２２を無効にすることは、信頼トークン２２２を削除すること、または信頼トークン２２２が現在無効であることを示すように信頼トークン２２２を修正することを含んでもよい。記録が否定から肯定に変わった場合、信頼トークン更新モジュール２１６は、プロセッサ２０４と連携して、信頼トークン２２２を回復させてもよい。信頼トークン２２２を回復させることは、無効にされた以前の信頼トークン２２２に基づいて新しい信頼トークン２２２を生成すること、または信頼トークン２２２が現在有効であることを示すように無効な信頼トークン２２２を修正することを含んでもよい。信頼トークン更新モジュール２１６は、プロセッサ２０４と連携して、信頼トークンを維持するための行為を実行してもよい（例えば、信頼トークン２２２を保存したまま保持すること、および／または信頼トークン２２２に関連付けて保存された時間を更新することによって）。

【００５８】

サーバーコンピュータ２００は、１つ以上のタイマー（図示せず）をさらに含んでもよい。タイマーは、ソフトウェアタイマーおよび／またはハードウェアタイマーであってもよい。サーバーコンピュータ２００は、タイマーを使用して、上述の様々な期間を追跡してもよい。例えば、サーバーコンピュータ２００は、ユーザーが認証されたときにタイマーを開始してもよく、またタイマーのカウントが１０秒未満である場合、サーバーコンピュータ２００がユーザーが検出されたことを確認したときに、サーバーコンピュータ２００は、信頼トークン２２２の生成へと進んでもよい。別の例として、サーバーコンピュータ２００は、ユーザーが認証されたときにタイマーを開始してもよく、またタイマーが１０日に達した場合、ユーザーをグリッドからオフにしてもよい。

【００５９】

図３は、一部の実施形態によるユーザーデバイス３００のブロック図を示す。ユーザーデバイス３００は、プロセッサ３０４を備えてもよい。プロセッサ３０４は、メモリ３０２、ネットワークインターフェース３０６、およびコンピュータ可読媒体３０８に連結されていてもよい。

【００６０】

メモリ３０２、プロセッサ３０４、およびネットワークインターフェース３０６は、図２に関して上述されるようなメモリ２０２、プロセッサ２０４、およびネットワークインターフェース３０６と実質的に同様であってもよい。

【００６１】

コンピュータ可読媒体３０８は、記憶および／または送信のための１つ以上の非一時的媒体を備えてもよい。好適な媒体としては、例として、ランダムアクセスメモリ（ＲＡＭ）、読み出し専用メモリ（ＲＯＭ）、ハードドライブもしくはフロッピーディスクなどの磁気媒体、またはコンパクトディスク（ＣＤ）もしくはＤＶＤ（デジタル多目的ディスク）などの光媒体、フラッシュメモリ、およびこれに類するものが挙げられる。コンピュータ可読媒体は、こうした記憶または送信デバイスの任意の組み合わせであってもよい。

【００６２】

コンピュータ可読媒体３０８は、一連の命令またはコマンドとして保存されるソフトウェアコードを含んでもよい。コンピュータ可読媒体３０８は、ユーザーデバイスによって、ユーザーが認証されたことを判定することと、ユーザーデバイスによってサーバーコンピュータへと、ユーザーが認証されたという表示を送信することと、ユーザーデバイスによって、ユーザーが検出されたことを判定することであって、ユーザーデバイスが、ユーザーの心拍を検出することに基づいてウェアラブルデバイスによって生成された情報に基づいてユーザーが検出されたことを判定する、判定することと、ユーザーデバイスによってサーバーコンピュータへと、ユーザーが検出されたという表示を送信することと、を含

み、サーバーコンピュータが、ある期間内に２つの表示を受信することに基づいて、ユーザーに対して信頼トークンを生成または維持する方法を実施するためにプロセッサ３０４によって実行可能なコードを含んでもよい。

【００６３】

コンピュータ可読媒体３０８は、通信モジュール３１０と、セキュアなアプリケーション３１２と、ユーザー検出アプリケーション３１４と、を含んでもよい。これらのモジュールの各々は、プロセッサ３０４と併せて、下記で説明される機能を実行するように構成されたコードを含んでもよい。

【００６４】

通信モジュール３１０は、プロセッサ３０４にメッセージの生成、メッセージの転送、メッセージの再フォーマット、および／またはそうでなければ他のエンティティとの通信を行わせるコードを含んでもよい。

【００６５】

セキュアなアプリケーション３１２は、プロセッサ３０４にユーザーを認証させるコードを含んでもよい。セキュアなアプリケーション３１２は、図１に関して上述の第１のアプリケーション１０２Ａと実質的に同様であってもよい。セキュアなアプリケーション３１２は、銀行のアプリケーション、車両をキーレスで始動するためのアプリケーション、またはセキュアなファイルシステムにログインするためのアプリケーションなど、ユーザーが継続的に認証されるべきアプリケーションであってもよい。

【００６６】

ユーザー検出アプリケーション３１４は、プロセッサ３０４にユーザーが検出されたかどうかについての情報を通信させるコードを含んでもよい。ユーザー検出アプリケーション３１４は、図１に関して上述の第２のアプリケーション１０２Ｂと実質的に同様であってもよい。ユーザー検出アプリケーション３１４は、例えば、スマートウォッチなどのウェアラブルデバイスに関連付けられたアプリケーションであってもよい。ユーザー検出アプリケーション３１４は、ウェアラブルデバイスから受信した情報を、取得、解析、および送信してもよい。

【００６７】

図４は、一部の実施形態によるデジタルアイデンティティ管理のための例示的なシステム４００の概略図を図示する。下記で説明するように、デジタルアイデンティティ管理システム４００は、前述の信頼トークンシステムと併せて使用して、機密性の高いユーザー情報を保護するだけでなく、ユーザーが支払取引などのやり取りを便利に行えるようにすることができる。システム４００は、本明細書に記載のプログラミングを実行するために構成された構成要素の数多くの可能な配設のうちの１つのみを図示する。他の配設は、より少ない構成要素、または異なる構成要素が含まれてもよく、また構成要素間の作業の分割は、配設に応じて変化してもよい。

【００６８】

システム４００は、少なくとも１つのデジタルアイデンティティ（ＤＩ）プロバイダー４１０、サーバーコンピュータ４０２、依存エンティティ４０８、イベントログ４０４、ターゲットエンティティ４１１、およびキーロッカー４０６を含むことができる。システム４００の構成要素は、通信ネットワークを通して互いに動作可能に通信してもよい。

【００６９】

通信ネットワークは、任意の好適な通信媒体を含んでもよい。通信ネットワークは、以下の直接相互接続、インターネット、ローカルエリアネットワーク（ＬＡＮ）、メトロポリタンエリアネットワーク（ＭＡＮ）、インターネット上のノードとしてのオペレーティングミッション（ＯＭＮＩ）、セキュリティ保護カスタム接続（ｓｅｃｕｒｅｄ　ｃｕｓｔｏｍ　ｃｏｎｎｅｃｔｉｏｎ）、ワイドエリアネットワーク（ＷＡＮ）、無線ネットワーク（例えば、ワイヤレスアプリケーションプロトコル（ＷＡＰ）、Ｉ－モード、および／またはこれに類するものなどの、しかしこれらに限定されないプロトコルを採用する）、および／またはこれに類するもののうちの一つおよび／もしくはそれらの組み合わせで

あってもよい。図４に図示されるエンティティ、プロバイダー、ネットワーク、およびデバイス間のメッセージは、ファイル転送プロトコル（ＦＴＰ）、ハイパーテキスト転送プロトコル（ＨＴＴＰ）、セキュアハイパーテキスト転送プロトコル（ＨＴＴＰＳ）、セキュアソケットレイヤー（ＳＳＬ）、ＩＳＯ（例えば、ＩＳＯ　８５８３）、および／またはこれに類するものなどの、しかしこれらに限定されないセキュアな通信プロトコルを使用して送信されてもよい。

【００７０】

一部の実施形態では、ターゲットエンティティ４１１は、デジタルアイデンティティが提供されるエンティティである（すなわち、ターゲットエンティティ４１１についてのデジタルアイデンティティ）。ターゲットエンティティ４１１は、ターゲットエンティティのユーザー４１１Ａおよび／またはクライアントデバイス４１１Ｂを含んでもよい。「ターゲットエンティティ」という用語は、個人（例えば、顧客、消費者、および／またはこれに類するもの）、企業もしくは他の法的組織、政府機関、および／またはこれに類するものを指す場合がある。追加的に、または別の方法として、「ターゲットエンティティ」という用語は、物（例えば、物体、機器の一部、電子構成要素、コンピュータシステム、および／またはこれに類するもの）を指す場合がある。

【００７１】

一部の非限定的な実施形態では、ターゲットエンティティ４１１は、識別子（「ターゲットエンティティの識別子」）が割り当てられる場合がある。ターゲットエンティティの識別子は、ターゲットエンティティ４１１のデジタル署名および／または暗号化キーに関連付けられたデータを含んでもよい。別の方法として、または追加的に、ターゲットエンティティの識別子は、ＩＤ番号、クイックレスポンス（ＱＲ）コード、および／またはこれに類するものを含んでもよい。

【００７２】

ターゲットエンティティについての情報は、ソースから取得することができる。ソースの１つのタイプは、ＤＩプロバイダー４１０である。ＤＩプロバイダー４１０は、ターゲットエンティティ４１１に関連付けられた１つ以上のデジタルアイデンティティ（ＤＩ）を生成する。上述のように、ＤＩは、別のエンティティと共有することができるエンティティについての一組の情報に関連付けられたデータを含むことができる。ＤＩプロバイダー４１０は、発行者、取得者、取引サービスプロバイダー、政府機関、および／またはこれに類するものであってもよい。ＤＩプロバイダー４１０は、ＤＩを作成および保存するように構成される。

【００７３】

一部の非限定的な実施形態では、依存エンティティ４０８は、ユーザーのデジタルアイデンティティに関連付けられた情報を受信するエンティティである。一部の実施形態では、依存エンティティ４０８は、図１に関して上述される、エンティティコンピュータ１０８に対応してもよい。依存エンティティ４０８は、ターゲットエンティティ４１１についての情報を要求する任意のエンティティとすることができる。例えば、依存エンティティ４０８は、支払取引を開始するターゲットエンティティ４１１についての情報を要求する小売業者とすることができる。追加的に、または別の方法として、依存エンティティ４０８は、支払のないやり取り（例えば、ターゲットエンティティ４１１に対するセキュアなエリアまたはイベント会場へのアクセスの許可する）に関してターゲットエンティティ４１１についての情報を要求するエンティティ（例えば、政府機関または企業組織）とすることができる。

【００７４】

一部の非限定的な実施形態では、依存エンティティ４０８は、識別子（「依存エンティティの識別子」）が割り当てられてもよい。依存エンティティの識別子は、依存エンティティ４０８のデジタル署名および／または暗号化キーに関連付けられたデータを含んでもよい。

【００７５】

イベントログ４０４は、紛争解決、不正検出、および／またはユーザー挙動の解析などのタスクのためのイベントメタデータにアクセスするために使用されてもよい。１つ以上のイベントにアクセスするために必要な暗号化キーへのアクセスを制限することによって、イベント構造は、ターゲットエンティティに関連付けられたデータを非公開に保持する役に立つ。例えば、ターゲットエンティティによって保持されるプライベートキーが、イベントデータにアクセスするために必要とされる場合があり、イベントデータは、ターゲットエンティティからの明示的な許可がある場合にのみ利用可能になることを確実にする。イベントデータへのアクセス経路は、共通のアプリケーションプログラミングインタフェース（ＡＰＩ）構造を介して定義されてもよい。アクセス経路は、限られたエンティティが限られたデータ量でイベントにアクセスしうるように確立されてもよい。

【００７６】

イベントログ４０４は、任意の好適なコンピュータ可読記憶媒体および／または任意の好適なコンピュータ可読記憶媒体の組み合わせに保存することができる。例えば、イベントログ４０４は、データベース内に保存することができる。追加的に、または別の方法として、イベントログ４０４は、ブロックチェーンおよび／またはこれに類するものを含むがこれらに限定されない、分散型台帳に維持および保存することができる。

【００７７】

システム４００は、キーロッカー４０６をさらに含んでもよい。キーロッカー４０６は、ファイル、ファイルの集まり、または暗号化キーを保存するためのデータベースであってもよい。キーロッカー４０６は、クラウドベースであってもよい。キーロッカー４０６は、様々なエンティティ（例えば、ターゲットエンティティ４１１に割り当てられた暗号化キー、ＤＩプロバイダー４１０、依存エンティティ４０８等）に割り当てられた暗号化キーを保存してもよい。キーロッカー４０６は、ターゲットエンティティ４１１と関連付けたイベントに関与してきた当事者のキーが、そのターゲットエンティティ４１１に基づいて構造内に保存されるように、ターゲットエンティティ４１１に基づいてキーを組織化してもよい。このキーの組は、ターゲットエンティティ４１１のキーを使用して暗号化されてもよく、これによりキーの組を解放するためには、ターゲットエンティティ４１１によって保持されるプライベートキーが必要とされる。別の方法として、または追加的に、ペアワイズキーの組を、各関係に対して割り当ててもよい。例として、ペアワイズキーの組は、ターゲットエンティティ４１１および依存エンティティ４０８に対して割り当てられてもよい。キーロッカー４０６は、ターゲットエンティティ４１１が関与する以前のイベントと関連付けられていた暗号化キーを保存してもよい。

【００７８】

一部の実施形態では、キーのうちの１つ以上は、Ｂａｓｅ５８モデルに基づいてコード化されてもよい。Ｂａｓｅ５８は、簡単に区別される５８個の英数字記号および恣意的なサイズのペイロードを使用する、バイナリからテキストへのコード化のタイプである。追加的に、１つ以上のキーをウォレットインポートフォーマット（ＷＩＦ）でコード化することもできる。ＷＩＦは、キーのコピーを容易にし、かつ圧縮を可能にする、キーをコード化する方法である。一部のキーは、適切なセキュリティレベルに基づいてコード化されてもよく、またはコード化されなくてもよく、かつ／または暗号化されてもよい。

【００７９】

システム４００は、「グリッド上」ステータスを管理してもよい。「グリッド上」は、コンピュータネットワークインフラストラクチャに接続され、かつ通信することを含んでもよい。グリッド上ステータスは、ユーザーがユーザーのデジタルアイデンティティに関連付けられたユーザーデータへのアクセスを承認されたことを示してもよい。例えば、グリッド上にあることは、ネットワーク通信システムに接続されていることを含み得る。ユーザーデバイスがネットワーク通信システムに接続されているとき、他のデバイスは、デジタルアイデンティティ、ユーザーデータ、およびこれに類するものなどのユーザーに関する情報にアクセスするために、ユーザーデバイスと通信することができる。例えば、デバイスは、ユーザーデバイスと通信して、その後ユーザーについてのアサーションを復号

するために使用される暗号化キーを、ユーザーデバイスから取得することができる。実施形態では、ユーザーは、「グリッド上」に行く前に認証されてもよい。一部の実施形態では、ユーザー認証ステータスは、「グリッド上」にある間は、「グリッド上」に留まり続けるために、「グリッド上」でモニターされてもよい。この態様に関するさらなる詳細は、２０１９年１２月３日に出願されたＰＣＴ出願第ＰＣＴ／ＵＳ２０１９／０６４１３２号（本出願と同一の譲受人に割り当てられる）に見出すことができる。

【００８０】

モバイルアプリケーションなどのアプリケーションを、グリッドをオンまたはオフにするために使用してもよい。例えば、アプリケーションは、グリッドステータス上に表示するためのユーザーインターフェースを含んでもよい。ユーザーインターフェースは、ユーザーが第１の状態ではグリッド上にあり、またユーザーが第２の状態ではグリッドから外れていることを表す場合がある。ユーザーインターフェースは、ユーザーがグリッド上にあるか、またはグリッドから外れているかを表すこと、および／または制御することができるグラフィカル要素を含んでもよい。別の例として、ユーザーは、グリッドステータスを制御するために、ウェブサイトを介してユーザー入力を受け入れるためのチェックボックスまたはその他の要素とやりとりしてもよい。

【００８１】

グリッド上に移動するために、ユーザーは、まず認証操作を実行し、そしてグリッド上に移動してもよい。グリッドから外れる前に時間が残っているタイマーは、その後、８時間などの最大値で初期化されてもよい。

【００８２】

ユーザーがグリッド上にある間に、ユーザーデータは、ユーザーのデジタルアイデンティティと関連付けられて、１つ以上の依存エンティティに対してアクセス可能であってもよい。例えば、ユーザーデータは、ユーザーに関連付けられたイベントデータであってもよい。ユーザーデータは、暗号化された形態であってもよく、またイベントログ４０４などのデータベースに保存されてもよい。

【００８３】

ユーザーがグリッド上にある間、サーバーコンピュータ４０２は、セキュアなイベントデータへのアクセスを許可する場合がある。サーバーコンピュータ４０２は、ユーザーに関連付けられたユーザーデバイス（例えば、図１の第１のユーザーデバイス１０２）上のセキュアな要素からユーザーに関連付けられた暗号化キーを取得することができる。暗号化キーを取得する前に、サーバーコンピュータ４０２は、ユーザーがユーザーデータへのアクセスを承認されていた期間中にユーザーデータ要求が発生したと判定することができる。例えば、サーバーコンピュータ４０２は、アクセス要求のタイムスタンプが、ユーザーが様々な当事者によってユーザーデータへのアクセスを承認された期間内に発生したと判定することができる。サーバーコンピュータ４０２は、キーロッカー４０６にアクセスするために、ユーザーの暗号化キーを使用してもよい。記録（例えば、図１の記録１０６Ａ）を制御するために第１の期間を使用してしてもよく、またグリッドステータス上の制御のために別の第２の期間を使用してしてもよい。

【００８４】

ユーザーは、グリッド上に移動した後の任意の時点で、グリッドから外れることを決定してもよい。また、ユーザーは、グリッド上に無期限に留まることが妨げられる場合もある。一部の実施形態では、タイマーは、ユーザーがグリッド上に移動するときに初期化されてもよい。タイマーが期限切れになった後、ユーザーはグリッドから外れてもよい。例えば、認証後で、かつグリッド上に移動した後、ユーザーは、グリッドから外れるまで８時間（例えば、第２の期間）を有してもよい。タイマーの長さは、調整可能なシステムパラメータであってもよい。グリッドから外された後、ユーザーは、グリッド上に戻るために自身を再認証してもよい。

【００８５】

図５は、信頼トークンを用いて取引を行う例示的な使用の事例を示す。この例では、ユ

ーザーの銀行のアプリケーションへのログインを保持するために、信頼トークンが使用される。

【００８６】

ステップＳ１では、第２のユーザーデバイス５０４（例えば、心拍を検出するためのハードウェアおよびソフトウェアを含むウェアラブルデバイス）は、第１のユーザーデバイス上で実行されるセキュアなアプリケーション５０２Ａと同期する。第２のユーザーデバイス５０４およびセキュアなアプリケーション５０２Ａは、実質的に同時に（例えば、ユーザーが数秒以内に認証され、かつ検出されるという表示を送信することによって）ユーザーのアクティビティを確認することによって同期してもよい。この実施例では、第１のユーザーデバイスはモバイルデバイスであり、そして図３に関して上述のユーザーデバイス３００と実質的に同様であってもよい。セキュアなアプリケーション５０２Ａは、銀行のアプリケーション（例えば、図５に示すように、ＫＢＢ銀行のための）であり、図３に関して上述のセキュアなアプリケーション３１２と実質的に同様であってもよい。

【００８７】

第１のユーザーデバイス５０２は、ユーザーから、セキュアなアプリケーション５０２Ａのインターフェース要素５０２Ｂを介してユーザーログイン情報を受信してもよい。第１のユーザーデバイス５０２は、ログイン情報を、セキュアなアプリケーション５０２Ａに関連付けられたリモートエンティティコンピュータ５１２に送信してもよい（例えば、エンティティコンピュータ５１２は、セキュアなアプリケーション５０２Ａを提供する銀行のサーバーコンピュータであってもよい）。エンティティコンピュータ５１２は、認証確認を第１のユーザーデバイス５０２に送信してもよい。第１のユーザーデバイス５０２は、次に、ユーザーがステップＳ２において認証されたことを示す信号をサーバーコンピュータ５０６に送信してもよい。

【００８８】

サーバーコンピュータ５０６は、図２に関して上述のサーバーコンピュータ２００と実質的に同様である。第２のユーザーデバイス５０４およびセキュアなアプリケーション５０２Ａの同期は、サーバーコンピュータ５０６を介して実行されてもよい。例えば、第２のユーザーデバイス５０４およびセキュアなアプリケーション５０２Ａは、サーバーコンピュータ５０６を各々ｐｉｎｇしてもよく、そして同期はサーバーコンピュータ５０６上で行われてもよい。サーバーコンピュータは、こうした同期を表すために、記録（例えば、図１の記録１０６Ａ）を使用してもよい。

【００８９】

ステップＳ２では、サーバーコンピュータ５０６は、信頼トークン５１０を発行し、そしてユーザーが認証され、かつ検出されたことを示す信号を受信することに応答して、信頼トークン５１０をデータストア５０８に保存する。データストア５０８は、クラウドストレージシステム（例えば、「クラウド（ｔｈｅ　ｃｌｏｕｄ）」）であってもよく、図２に関して上述のデータストア２２０と実質的に同様であってもよい。信頼トークン５１０は、図２に関して上述の信頼トークン２２２と実質的に同様であってもよい。信頼トークン５１０は、図１に関して上述したように、肯定的な記録を検出することに基づいて生成されてもよい。別の方法として、または追加的に、信頼トークン２２２は、ユーザーがグリッド上にあると判定することに基づいて生成されてもよい。例えば、信頼トークン２２２を生成する前触れとして、サーバーコンピュータ５０６は、図４に関して上述のデジタルアイデンティティプラットフォームを使用して、ユーザーがグリッド上にあるかどうかを判定してもよい。信頼トークン２２２はまた、ウェアラブルデバイスを介してユーザーを検出することに基づいて生成されてもよい。第２のユーザーデバイス５０４を介したユーザーの継続的な検出は、信頼トークン２２２を経時的に維持することを可能にする場合がある。

【００９０】

ステップＳ３では、リソースへのユーザーアクセスを許可するかどうかを判定するために、クラウド内の信頼トークン５１０が使用される。信頼トークン５１０は、ユーザー経

験を効率化することができる。ユーザーは、例えば、自身を再認証することなく、または自分の支払認証情報を入力することなく、セキュアなアプリケーション５０２Ａを介して資金の送金を開始することを許可されてもよい。例えば、信頼トークン５１０は、ワンタイムパスワードなどの情報を入力することによって、ユーザーが自身を認証する必要性を回避するために使用することができる。信頼トークン５１０は、デジタルアイデンティティと併せて、有利なことに、個人識別情報などの機密データを入力する必要性を回避するために使用することができる。

【００９１】

図６は、一部の実施形態による信頼トークンを使用してリソースへのアクセスを制御するための方法６００のフローチャートを示す。図６の操作は、図１～３に関して上述のシステム、そして特にサーバーコンピュータによって実行されてもよい。

【００９２】

ステップ６０２では、サーバーコンピュータは、ユーザーデバイス上の第１のアプリケーションから、ユーザーが認証されたという表示を受信してもよい。第１のアプリケーションおよび／または第１のアプリケーションと関連付けられたリモートエンティティコンピュータは、例えば、ユーザーのログイン認証情報を受け入れ、かつ検証することによって、ユーザーを認証してもよい。ログイン認証情報は、ユーザーデバイス上のメタデータおよび／またはステップアップ認証を介してなど、追加的な認証の層で補足されてもよい。別の方法として、または追加的に、第１のアプリケーションは、外部アクセスデバイスから受信した認証されたユーザーの表示を転送してもよい。例えば、ユーザーは、セキュアな施設に初めて入る際に、自身の電話および２つの形態の身分証明をアクセスデバイスへとスキャンしてもよい。アクセスデバイスは、接続されたエンティティデバイスと併せて、ユーザーを認証し、そしてその通知を第１のアプリケーションに送信してもよい。いずれにしても、サーバーコンピュータは、ネットワーク上でサーバーコンピュータに送信されたメッセージを介してユーザーが認証されたという表示を受信してもよい。メッセージは、ユーザーが認証された時間を示すタイムスタンプをさらに含んでもよい。

【００９３】

ステップ６０４では、サーバーコンピュータは、ユーザーデバイス上で実行される第２のアプリケーションから、ユーザーが検出されたという表示を受信してもよい。ユーザーデバイスは、ユーザー上のウェアラブルデバイスから、ユーザーが検出されたという表示を受信してもよい。例として、ユーザーデバイスは、ユーザーによって着用されているウェアラブルデバイス（例えば、図１の第２のユーザーデバイス１０４）と通信してもよい。ウェアラブルデバイスは、心拍を検出し、そしてユーザーデバイス上のアプリケーション（例えば、図１の第２のアプリケーション１０２Ｂ）に、ユーザー心拍が検出されたことを連続的にまたは定期的に通知してもよい。ウェアラブルデバイスは、ユーザーが生存していて、かつ健在であり、そして実質的に連続的な様式でウェアラブルデバイスを着用していることを保証するために活用されてもよい。

【００９４】

一部の実施形態では、高度なセキュリティ対策として、ウェアラブルデバイスおよび／またはユーザーデバイス上の関連付けられたアプリケーションは、検出された心拍を解析してもよい。例えば、ユーザーデバイスは、ユーザー心拍に関連付けられた収集された履歴データに基づいて、心拍のパターンおよび連続性を解析して、それが承認されたユーザーのものと一致することを保証してもよい。履歴データは、ユーザーの保存された心拍に対応してもよい。システムは、ユーザーのこうした保存された心拍と検出された心拍との比較を実行してもよい。ユーザーデバイスは、保存された心拍データおよび検出された心拍データの特性を解析して、ユーザーが覚醒しているかどうか、および／または検出された心拍がユーザーに関連付けられた特性パターンを含むかどうかを判定してもよい。ユーザーが覚醒していると判定することは、ユーザーが検出されたことを示す前に、追加的な必要条件であってもよい。別の方法として、または追加的に、ユーザーは、脈、触覚、ビデオ録画当によって検出されてもよい。いずれにしても、サーバーコンピュータは、ネッ

トワーク上でサーバーコンピュータに送信されたメッセージを介してユーザーが検出されたという表示を受信してもよい。メッセージは、ユーザーが検出された時間を示すタイムスタンプをさらに含んでもよい。

【００９５】

ステップ６０６では、サーバーコンピュータは、ステップ６０２および６０４の表示が閾値期間内に受信されるかどうかを判定してもよい。サーバーコンピュータは、ユーザーが認証された時間を示すタイムスタンプを、ユーザーが検出された時間を示すタイムスタンプと比較してもよい（例えば、２つのタイムスタンプを減算して、２つの表示の受信の間に経過した期間を識別することによって）。サーバーコンピュータは、所定の閾値期間を識別してもよい。サーバーコンピュータは、異なるコンテキストに対する閾値期間を保存してもよい。例えば、サーバーコンピュータは、信頼トークンを生成するための閾値期間、信頼トークンを維持するための閾値期間、および／または異なるエンティティのための閾値期間（例えば、銀行のアプリケーションは、小売業者アプリケーションよりも短い時間枠を必要とする場合がある）を保存してもよい。信頼トークンを生成する目的では、閾値期間は、例えば、１秒であってもよい。サーバーコンピュータは、タイムスタンプ間の差が閾値以下である場合、ステップ６０２および６０４の表示が閾値期間内に受信されたこと（「はい」の結果）を判定してもよい。サーバーコンピュータは、タイムスタンプ間の差が閾値より大きい場合、ステップ６０２および６０４の表示が閾値期間内に受信されなかったこと（「いいえ」の結果）を判定してもよい。

【００９６】

表示が閾値期間内に受信されない場合、サーバーコンピュータは、信頼トークンの生成を控え、そしてフローを終了してもよい。表示が閾値期間内に受信された場合、フローは任意選択でステップ６０８に進んでもよく、または別の方法として、ステップ６１０に直接進んでもよい。

【００９７】

ステップ６０８では、サーバーコンピュータは、任意選択で、ユーザーがグリッド上にあるかどうか（例えば、ユーザーのデジタルアイデンティティがオンになっているかどうか）を判定してもよい。サーバーコンピュータは、図４に関して上述したように、デジタルアイデンティティプラットフォームに保存された記録に基づいてユーザーがグリッド上にあるかどうかを識別してもよい。グリッド上にあることは、ユーザーが、ユーザーのデジタルアイデンティティに関連付けられたユーザーデータへのアクセスを承認されたことを示してもよい。一部の事例では、ユーザーは、ある期間（例えば、１日間「グリッド上」に行くことによって）こうしたアクセスを承認してもよい。ユーザーは、ユーザーのデジタルアイデンティティに関連付けられたユーザーデータへのアクセスを無効にすることによって「グリッドから外れ」てもよい。ユーザーがグリッド上にある場合、フローはステップ６１０に進んでもよい。ユーザーがグリッド上にない場合、フローは終了してもよい。

【００９８】

ステップ６１０では、サーバーコンピュータは、ユーザーに対して信頼トークンを生成してもよい。サーバーコンピュータは、ステップ６０２および６０４での閾値期間内の表示の受信に基づいて、信頼トークンを生成してもよい。例えば、信頼トークンは、ユーザーが第１のアプリケーションを介して認証された時点から１０秒以内にユーザーの心拍が検出された場合に発行されてもよい。サーバーコンピュータは、図１に関して上述したように、信頼トークンを生成するかどうかを判定するために、保存された記録を使用してもよい。

【００９９】

ステップ６１２では、サーバーコンピュータは、ユーザーに対して信頼トークンを維持するための条件が満たされているかどうかを連続的または定期的に判定してもよい。信頼トークンを維持するかどうかの判定は、例えば、ステップ６０４～６０８を繰り返すことによって、信頼トークンを生成するかどうかの判定と同様の様式で実行されてもよい。信

頼トークンを生成するために使用される初期表示に加えて、ユーザーデバイスは、ユーザーが検出された（または検出されない）という追加的な表示を定期的にサーバーコンピュータに送信してもよい。追加的な表示は、信頼トークンを維持するかどうかを判定するために使用されてもよい。例えば、サーバーコンピュータは、ユーザーデバイスから３０秒ごとにユーザーが検出されたという表示を受信してもよく、またその表示に基づいて、記録を更新する。記録を更新することは、特定の時間に心拍が検出される、または検出されないことを示すことの記録を変えること、記録を変えるのを控えること、または記録を変更することを含んでもよい。

【０１００】

サーバーコンピュータは、ステップ６０２および６０４での閾値期間内の表示の受信に基づいて、信頼トークンを維持するように判定してもよい。信頼トークンを維持するための閾値期間は、信頼トークンを生成するための閾値期間とは異なる場合がある。例えば、サーバーコンピュータは、ユーザーが第１のアプリケーションを介して認証された時間から４時間以内にユーザーの心拍が検出された場合、信頼トークンを維持するための条件が満たされていると判定してもよいが、一方で信頼トークンを生成するための閾値期間は、はるかに短くてもよい。サーバーコンピュータは、図１に関して上述したように、信頼トークンを維持するための条件を満たしているかどうかを判定するために保存された記録を使用してもよい。信頼トークンを維持するための条件は、ステップ６０８に関して上述したように、ユーザーがグリッド上にあるかどうかにさらに基づいてもよい。したがって、サーバーコンピュータは、ユーザーがユーザーのデジタルアイデンティティへのアクセスを許可しされたと判定することに基づいて信頼トークンを維持してもよく、またはユーザーがユーザーのデジタルアイデンティティへのアクセスを無効にされたと判定することに基づいて信頼トークンを無効にしてもよい。また、グリッド上に留まっていることに関連付けられた期間が経過すると、サーバーコンピュータは、信頼トークンをさらに無効にする場合がある。

【０１０１】

ステップ６１４では、サーバーコンピュータは、信頼トークンを維持してもよい。サーバーコンピュータは、ステップ６１２で「はい」を判定する際に信頼トークンを維持してもよい。信頼トークンを維持することは、信頼トークンを無効にしないことを含んでもよい。別の方法として、または追加的に、信頼トークンを維持することは、信頼トークンのステータスを積極的に更新すること（例えば、特定の時点でアクティブに）が関与してもよい。

【０１０２】

ステップ６１６では、サーバーコンピュータは、信頼トークンを無効にしてもよい。サーバーコンピュータは、ステップ６１２で「いいえ」を判定する際に信頼トークンを無効にしてもよい。信頼トークンを無効にすることは、信頼トークンを削除することを含んでもよい。別の方法として、信頼トークンを無効にすることは、信頼トークンのステータスを更新すること（例えば、特定の時点で非アクティブに）が関与してもよい。例として、サーバーコンピュータは、ユーザーデバイス上の第２のアプリケーションから、ユーザーが検出されないという表示を受信してもよい。ユーザーが、ウェアラブルデバイスを取り外している場合があり、ウェアラブルデバイスをユーザーデバイスから過度に長い期間分離している場合があり、または死亡した場合さえある。ユーザーが検出されないという表示を受信することに基づいて、サーバーコンピュータは信頼トークンを無効にしてもよい。

【０１０３】

ステップ６１８では、サーバーコンピュータは、信頼トークンを識別するか、またはエンティティコンピュータが信頼トークンを識別することを許可してもよい。信頼トークンは、リソースへのアクセス要求に基づいて識別されてもよい。例えば、ユーザーは、ユーザーデバイスおよび／またはエンティティコンピュータ上のアプリケーションを介して、購入を試み、資金を送金し、セキュアなウェブサイトまたはアプリケーションにログインしたままにし、セキュアな場所にアクセスする、などをしてもよい。リソースにアクセス

することは、ユーザーが認証されることを必要とする場合がある。したがって、ユーザーが信頼トークンを介して認証された状態に留まってもよいように、信頼トークンが有効な状態にあるかどうかの判定がなされる。一部の実施形態では、エンティティは、認証要求メッセージをサーバーコンピュータに送信してもよく、サーバーコンピュータは、認証要求メッセージの情報に基づいて信頼トークンを取得してもよい。別の方法として、または追加的に、サーバーコンピュータは、エンティティが信頼トークンにアクセスすることを許可してもよい。例えば、サーバーコンピュータは、エンティティが、エンティティが信頼トークンを取得するために使用することができる暗号化キーへとアクセスすることを許可してもよい。一部の実施形態では、信頼トークンを識別することは、ユーザーのデジタルアイデンティティを識別することを含んでもよく、信頼トークンは、ユーザーのデジタルアイデンティティに関連付けて保存される。

【０１０４】

サーバーコンピュータおよび／またはエンティティコンピュータは、識別された信頼トークンを解析して、信頼トークンが有効であるかどうかを判定してもよい。クラウド内に信頼トークンが存在する場合、信頼トークンは有効になり、クラウド内に信頼トークンが存在しない場合、無効になる。別の方法として、または追加的に、信頼トークンは、特定の値（例えば、有効または１）を有する場合、信頼トークンは有効になってもよく、また信頼トークンが別の値（例えば、無効または０）を有する場合、無効になってもよい。

【０１０５】

ステップ６２０では、ステップ６１８で有効な信頼トークンを識別することに基づいて、リソースへのアクセスは許可されてもよい。信頼トークンは、ユーザーが認証され、かつ通常の様式で行動する、すなわち認証されたままであるべきであることをエンティティに保証するために使用されてもよい。エンティティコンピュータは、有効な信頼トークンに基づいて、要求されたリソースへのアクセスを許可してもよい。例えば、エンティティコンピュータは、ユーザーが資金を送金すること、商品およびサービスを購入すること、セキュアな場所に入ることなどを許可してもよい。

【０１０６】

一例として、本来ユーザーを認証したアプリケーションに関連付けられたエンティティによって、リソースへのアクセスが許可される場合がある。これは、クッキーの使用によってユーザーログインが長くなる状況といくらか類似している。しかしながら、この場合には、信頼トークンはよりセキュアであり、また本来の認証に基づいてより長い時間アクセスを許可するために使用することができる。ユーザーは、銀行のウェブサイトにログインするために認証されてもよい。信頼トークンが有効なままである限り（例えば、ウェアラブルデバイスを介してユーザーの心拍が検出される限り）、ユーザーはログインしたままになり、再認証の必要性を回避する場合がある。

【０１０７】

別の例として、アクセスは、ユーザーを本来認証したアプリケーションとは異なる１つ以上のエンティティによって許可されてもよい。例えば、実質的に連続的な心拍数の確認と併せて、信頼されたアプリケーション（例えば、セキュアな銀行のアプリケーション）から取得した認証情報に基づいて、異なるエンティティはユーザーがリソースへのアクセスを受信することを許可してもよい。異なるエンティティは、例えば、ソーシャルメディアアプリケーション、小売業者ウェブサイト、またはこれに類するものであってもよい。信頼トークンが有効である限り、複数の異なるエンティティがリソースへのユーザーのアクセスを許可してもよい。異なるエンティティおよびリソースは、ユーザーのデジタルアイデンティティを使用して管理されてもよい。デジタルアイデンティティは、ユーザーに関連付けられたイベントを管理するために使用されてもよい。ユーザーについての詳細情報により、システムは、ユーザーが有効な信頼トークンによってアクセスできるリソースを識別することができる。

【０１０８】

別の例として、信頼トークンに基づいて輸送サービスへのアクセスが許可されてもよい

。ユーザーは、地下鉄の一週間定期券を購入し、そしてこの定期券を用いて最初に地下鉄に乗車するときに定期券と併せて自身を認証するために、身分証明をスキャンして取り込んでもよい。ユーザーが、自身のウェアラブルデバイスによって検出される限り、ユーザーは、信頼トークンを使用して地下鉄システムに再入場することができる場合がある。

【０１０９】

一部の実施形態では、信頼トークンは、限定された状況でリソースへのアクセスを許可するために受け入れ可能である場合がある。例として、信頼トークンは、最高１００ドルまでの取引に対して、ユーザーがさらなる入力を行わずに購入を可能にする場合がある。取引額が１００ドルを超える場合、ユーザーは追加的な情報の入力を促される場合がある。信頼トークンは、こうした制限を強制するために、構成データ（例えば、金銭上の限度または時間の限度）に関連付けて保存されてもよい。別の例として、信頼トークンは、ユーザーが２４時間、セキュアな施設へのアクセスを得ることを可能にする場合がある。２４時間後、信頼トークンは無効にされ、そしてユーザーは再認証を受ける必要がある。

【０１１０】

工程６２２では、工程Ｓ６１８で有効な信頼トークンを検出しないことに基づいて、ステップアップまたは取り下げが実行されてもよい。例えば、信頼トークンが無効にされた場合、ユーザーは再度サインインするか、ユーザーに送信されるコード番号を確認することによってステップアップするように促される。別の方法として、または追加的に、リソースへのアクセスは、取り下げられてもよい（例えば、ユーザーがステップアップ認証に失敗する場合）。

【０１１１】

実施形態は、いくつかの利点を提供する。１つ以上のリソースにアクセスするためにユーザーが再認証しなければならない回数を制限することによって、ユーザーのわずらわしさは軽減される。さらに、信頼トークンの使用は、アクセスがいつ許可されるかを判定するセキュアな手段を容易にすることができる。改ざんに対して脆弱なクッキーとは異なり、信頼トークンは改ざんに対して安全であるように管理されうる。例えば、信頼トークンは暗号的に保護されてもよく、また信頼できるエンティティのみが管理された条件下でアクセス可能であってもよい。さらに、デジタルアイデンティティと併せた信頼トークンの使用は、ユーザーの個人識別情報を損なうことなく、ユーザーのリソースへのアクセスを許可し、それ故にユーザーのプライバシーを保護するために使用することができる。

【０１１２】

認証を維持するための信頼トークンの使用は、処理リソースをさらに削減し、かつリソースへのアクセスを許可するかどうかを判定するために必要とされる時間を短縮する場合がある。ユーザーは、繰り返しログインまたはステップアップする必要はなく、こうした機能を実行するために必要とされるメッセージングおよび処理を排除、もしくは大幅に低減する場合がある。さらに、信頼トークンは、ユーザー認証を拡張する一部の以前の技法より低い処理要件を用いて維持することができる。心拍数などの単一のバイタルパラメータを介してユーザーをモニターすることによって、信頼トークンのステータスを単純なデータセットを用いて管理することができる。これは、リソースへのアクセスを許可するかどうかを判定するために必要とされる演算能力の量を低減することができる（例えば、非常に複雑である可能であるユーザーの挙動を追跡するのとは対称的に）。

【０１１３】

本出願に記載されるソフトウェア構成要素または機能のいずれかは、例えば、オブジェクト指向の技法を使って、例えば、Ｊａｖａ、Ｃ＋＋、またはＰｅｒｌなどの任意の好適なコンピュータ言語を使用する、プロセッサによって実行されるソフトウェアコードとして実装されてもよい。ソフトウェアコードは、ランダムアクセスメモリ（ＲＡＭ）、読み出し専用メモリ（ＲＯＭ）、ハードドライブもしくはフロッピーディスクなどの磁気媒体、またはＣＤ－ＲＯＭなどの光媒体などの、コンピュータ可読媒体上の一連の命令またはコマンドとして保存されてもよい。任意のこうしたコンピュータ可読媒体は、単一の計算装置上またはその内部にあってもよく、またシステムまたはネットワーク内の異なる計算

装置上もしくはその内部に存在してもよい。

【０１１４】

上記の説明は例示であり、限定するものではない。本開示の検討に伴い、本発明の数多くの変形が、当業者には明らかになる場合がある。したがって、本発明の範囲は、上記の説明を参照して判定されるのではなく、それらの全範囲または均等物とともに、係属中の請求項を参照して判定することができる。

【０１１５】

任意の実施形態からの１つ以上の特徴は、本発明の範囲から逸脱することなく、任意の他の実施形態の１つ以上の特徴と組み合わされてもよい。

【０１１６】

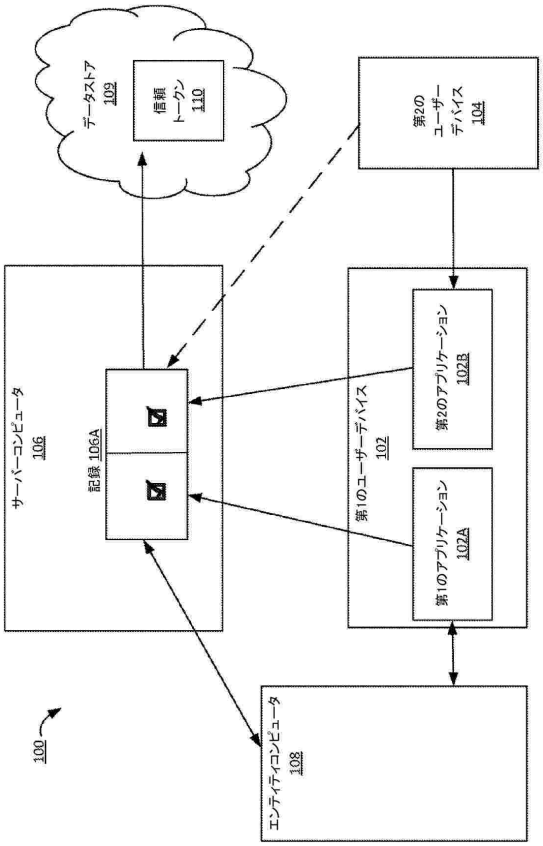
「一つの（ａ）」、「一つの（ａｎ）」、または「その（ｔｈｅ）」の列挙は、特に反対の指示がない限り、「一つ以上」を意味することを意図している。

【０１１７】

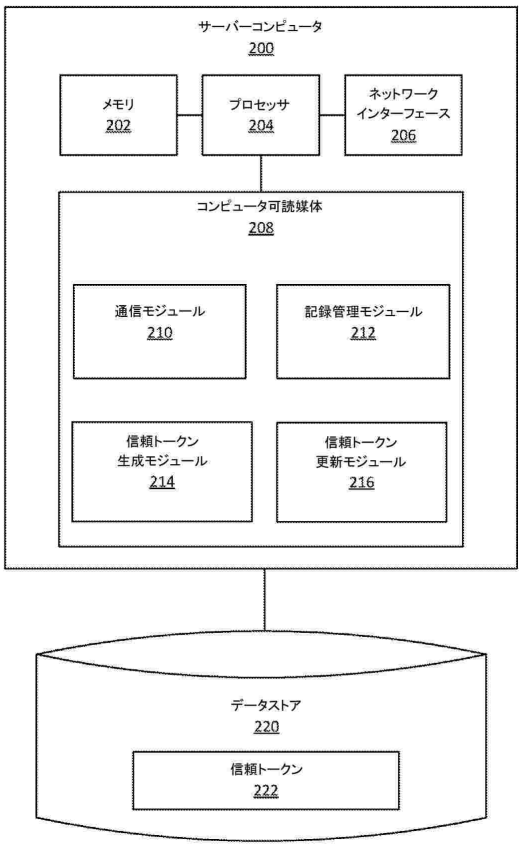
上記で言及したすべての特許、特許出願、刊行物および記載は、あらゆる目的のためにその全体が参照により本明細書に組み込まれる。いずれも先行技術とは認められない。

【図面】

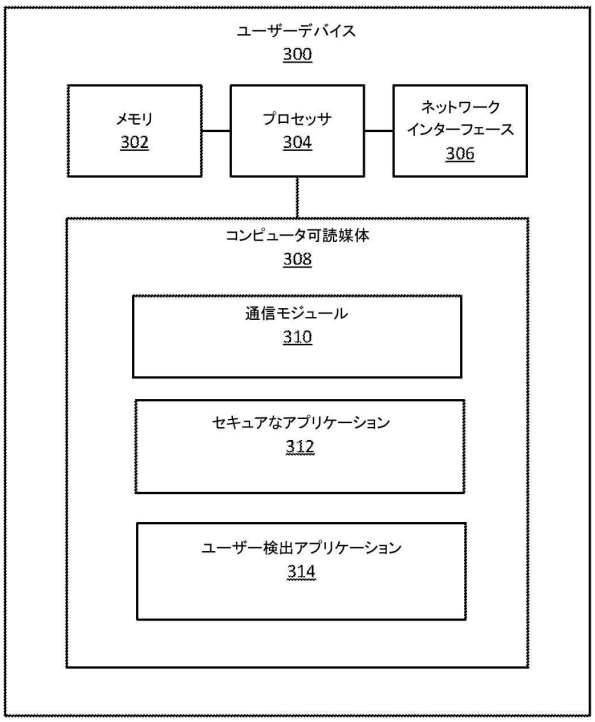
【図１】


データストア
109
信頼
トークン
110
第2の
ユーザー
デバイス
104
サーバーコンピュータ
106
記録 106A
第1のユーザーデバイス
102
第2のアプリケーション
102B
第1のアプリケーション
102A
100
エンティティコンピュータ
108

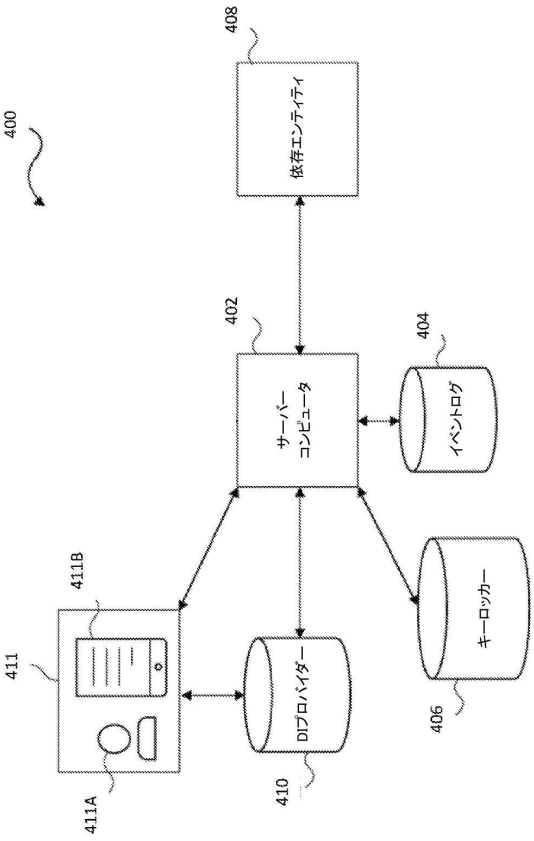
【図２】


サーバーコンピュータ
200
メモリ
202
プロセッサ
204
ネットワーク
インターフェース
206
コンピュータ可読媒体
208
通信モジュール
210
記録管理モジュール
212
信頼トークン
生成モジュール
214
信頼トークン
更新モジュール
216
データストア
220
信頼トークン
222

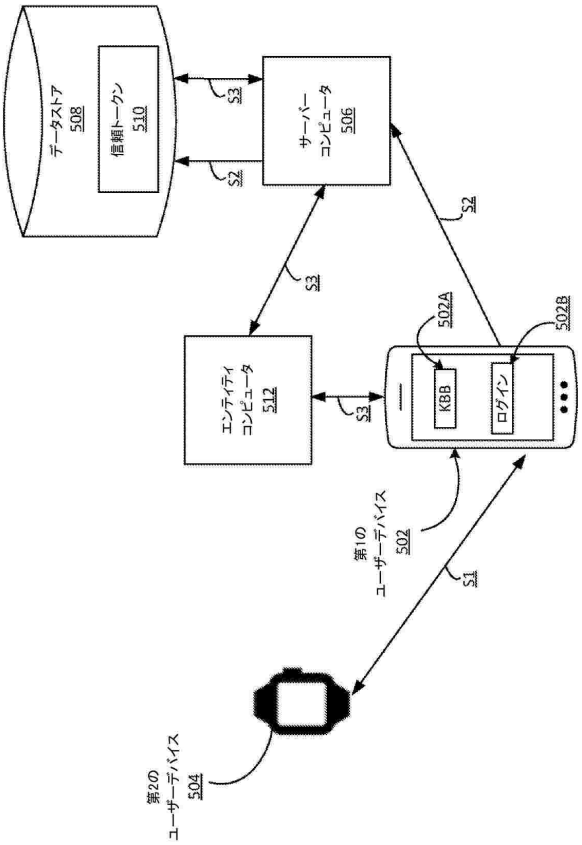
【図３】


ユーザーデバイス
300
メモリ
302
プロセッサ
304
ネットワーク
インターフェース
306
コンピュータ可読媒体
308
通信モジュール
310
セキュアなアプリケーション
312
ユーザー検出アプリケーション
314

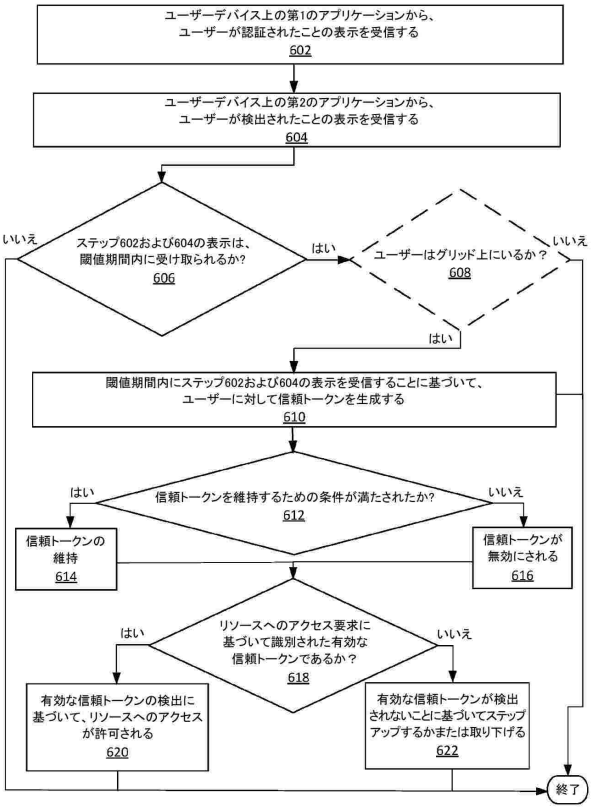
【図４】


400
408
依存エンティティ
402
サーバー
コンピュータ
404
イベントログ
411B
411
411A
DIプロバイダー
410
キーロッカー
406

【図５】


データストア
508
信頼トークン
510
サーバー
コンピュータ
506
S3
S2
S2
S3
エンティティ
コンピュータ
512
S3
502A
502B
KBB
ログイン
第1の
ユーザーデバイス
502
S1
第2の
ユーザーデバイス
504

【図６】


ユーザーデバイス上の第1のアプリケーションから、
ユーザーが認証されたことの表示を受信する
602
ユーザーデバイス上の第2のアプリケーションから、
ユーザーが検出されたことの表示を受信する
604
ステップ602および604の表示は、
閾値期間内に受け取られるか?
606
いいえ
はい
ユーザーはグリッド上にいるか？
608
いいえ
はい
閾値期間内にステップ602および604の表示を受信することに基づいて、
ユーザーに対して信頼トークンを生成する
610
信頼トークンを維持するための条件が満たされたか?
612
はい
いいえ
信頼トークンの
維持
614
信頼トークンが
無効にされる
616
リソースへのアクセス要求に
基づいて識別された有効な
信頼トークンであるか？
618
はい
いいえ
有効な信頼トークンの検出に
基づいて、リソースへのアクセス
が許可される
620
有効な信頼トークンが検出
されないことに基づいてステップ
アップするかまたは取り下げる
622
終了

フロントページの続き

審査官　吉田 歩
(56)参考文献　特開２０１８－１４７３２７（ＪＰ，Ａ）
特表２０１７－５２００３３（ＪＰ，Ａ）
特開２０１７－１５７２２３（ＪＰ，Ａ）
(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／３１
Ｇ０６Ｆ　２１／３２