

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7387596号
(P7387596)

(45)発行日 令和5年11月28日(2023.11.28)

(24)登録日 令和5年11月17日(2023.11.17)

(51)国際特許分類

F I

G 0 6 T 7/00 (2017.01)

G 0 6 T 7/00 3 0 0 E

B 4 2 D 25/351 (2014.01)

B 4 2 D 25/351

G 0 6 K 7/14 (2006.01)

G 0 6 K 7/14 0 1 7

G 0 6 K 19/06 (2006.01)

G 0 6 K 19/06 0 3 7

G 0 6 T 7/00 3 0 0 F

請求項の数 20 (全96頁)

(21)出願番号 特願2020-524694(P2020-524694)

(86)(22)出願日 平成30年7月20日(2018.7.20)

(65)公表番号 特表2020-527817(P2020-527817
A)

(43)公表日 令和2年9月10日(2020.9.10)

(86)国際出願番号 PCT/IB2018/000915

(87)国際公開番号 WO2019/016602

(87)国際公開日 平成31年1月24日(2019.1.24)

審査請求日 令和3年7月19日(2021.7.19)

(31)優先権主張番号 62/535,201

(32)優先日 平成29年7月20日(2017.7.20)

(33)優先権主張国・地域又は機関
米国(US)

(73)特許権者 520021336

ラーバ アイディー プロプライアタリー
リミティドオーストラリア国, シドニー ニューサ
ウスウェールズ 2 0 0 0, ビット スト
リート 3 3 8, レベル 1 6

(74)代理人 100099759

弁理士 青木 篤

(74)代理人 100123582

弁理士 三橋 真二

(74)代理人 100114018

弁理士 南山 知広

(74)代理人 100165191

弁理士 河合 章

(74)代理人 100133835

最終頁に続く

(54)【発明の名称】 安全タグ

(57)【特許請求の範囲】

【請求項1】

数値データとスタイルシートの組み合わせに基づくタグ特徴オプションの選択によって生成されるコンピュータ読み取り可能な安全追跡タグにより物理的またはデジタルの製品または文書にラベル付けすることを含む、物理的またはデジタルの製品または文書を追跡する方法であって、

前記コンピュータ読み取り可能な安全追跡タグのタグ特徴は、所定のタイプの前記タグ特徴間の接続を含み、前記接続のためのタグ特徴オプションは、接続幅および接続非対称を含む、方法。

【請求項2】

数値データとスタイルシートの組み合わせに基づくタグ特徴オプションを選択によって生成されるコンピュータ読み取り可能な安全追跡タグにより物理的またはデジタル製品またはドキュメントをラベル付けすることを含む、製品の物理的またはデジタル製品または文書を追跡する方法であって、

前記コンピュータ読み取り可能な安全追跡タグのタグ特徴は、前記コンピュータ読み取り可能な安全追跡タグの既存のタグ特徴間の接続と、接続幅と接続非対称を含む前記接続のタグ特徴オプションを含む、方法。

【請求項3】

数値データとスタイルシートの組み合わせに基づくタグ特徴オプションを選択によって生成されるコンピュータ読み取り可能な安全追跡タグにより物理的またはデジタル製品ま

たはドキュメントをラベル付けすることを含む、製品の物理的またはデジタル製品または文書を追跡する方法であって、

第1のタグ特徴オプションは、第1のタグ特徴の有無を含み、第2のタグ特徴オプションは、前記第1のタグ特徴間の接続の有無を含む、方法。

【請求項4】

前記タグ特徴のオプションは、前記数値データと前記スタイルシートとの組み合わせによって指定される前記コンピュータ読み取り可能な安全追跡タグの位置におけるタグ特徴の有無を含む、請求項1-3のいずれか1項に記載の方法。

【請求項5】

前記タグ特徴オプションは、前記コンピュータ読み取り可能な安全追跡タグのタグ特徴のサイズ、色、または形状を含む、請求項1-3のいずれか1項に記載の方法。

10

【請求項6】

前記タグ特徴オプションは、前記数値データと前記スタイルシートとの組み合わせによって指定される位置からの逸脱を含む、請求項1-3のいずれか1項に記載の方法。

【請求項7】

前記タグ特徴オプションは、前記数値データと前記スタイルシートとの組み合わせによって指定される位置に存在するいくつかのタグ特徴を含む、請求項1-3のいずれか1項に記載の方法。

【請求項8】

前記タグ特徴オプションは、前記コンピュータ読み取り可能な安全追跡タグのタグ特徴上の、基準点または基準線から1または複数の距離に延びるタグ特徴端を含むスプラインエンコードの存在を含む、請求項1-3のいずれか1項に記載の方法。

20

【請求項9】

前記1または複数の距離は、前記数値データの1つまたは複数の空間的に多重化された部分をエンコードする、請求項8に記載の方法。

【請求項10】

前記1または複数の距離は、前記数値データの1つまたは複数の空間的に多重化された部分の繰り返しをエンコードする、請求項9に記載の方法。

【請求項11】

前記タグ特徴オプションは、前記コンピュータ読み取り可能な安全追跡タグのタグ特徴上の微細構造の存在を含む、請求項1-3のいずれか1項に記載の方法。

30

【請求項12】

前記コンピュータ読み取り可能な安全追跡タグのタグ特徴はリムを含み、前記リムのタグ特徴オプションは、リム破損、リム変形、およびリム接続を含む、請求項1-3のいずれか1項に記載の方法。

【請求項13】

前記コンピュータ読み取り可能な安全追跡タグのタグ特徴はリム破損を含み、前記リム破損のタグ特徴オプションはリム破損端形状を含む、請求項1-3のいずれか1項に記載の方法。

【請求項14】

前記コンピュータ読み取り可能な安全追跡タグのタグ特徴は中央ロゴを含み、タグ特徴オプションは、前記安全追跡タグの中心点からの前記中央ロゴの変位を含む、請求項1-3のいずれか1項に記載の方法。

40

【請求項15】

前記方法は、前記コンピュータ読み取り可能な安全追跡タグを生成することをさらに含む、請求項3に記載の方法。

【請求項16】

前記コンピュータ読み取り可能な安全追跡タグを生成することは、前記数値データの第1のサブセットに従って第1のタグ特徴オプションの1つを選択し、前記第1のタグ特徴オプションの選択は対応する前記第2のタグ特徴オプションの1つを有効にすることと、

50

前記数値データの第2のサブセットに従って前記有効にされた第2のタグ特徴オプションの1つを選択することと、を含む、請求項15に記載の方法。

【請求項17】

前記数値データの第3のサブセットをエンコードする第3のタグ特徴オプションは、前記数値データの前記第2のサブセットに従って存在する前記各接続の幅を含む、請求項16に記載の方法。

【請求項18】

前記コンピュータ読み取り可能な安全追跡タグはベクトルグラフィックファイルを含み、前記物理的またはデジタルの製品または文書を前記コンピュータ読み取り可能な安全追跡タグでラベル付けすることは前記ベクトルグラフィックファイルをラスターライズすることを含む、請求項1-3のいずれか1項に記載の方法。

10

【請求項19】

前記方法は、前記コンピュータ読み取り可能な安全追跡タグの識別情報を認証サーバに提供することをさらに含む、請求項1-3のいずれか1項に記載の方法。

【請求項20】

前記方法は、前記コンピュータ読み取り可能な安全追跡タグのハッシュを生成し、前記識別情報を前記認証サーバに提供する前に、他のコンピュータ読み取り可能な安全追跡タグのハッシュとの衝突についてハッシュをチェックすることをさらに含む、請求項19に記載の方法。

20

【発明の詳細な説明】

【技術分野】

【0001】

本出願は、2017年7月20日に提出され、参照によりその全体が本明細書に組み込まれる米国仮特許出願第62/535,201号の優先権の利益を主張する。

【背景技術】

【0002】

物事の認証は現在、ブランド、商人、消費者に多くの問題を引き起こしている。既存の在庫追跡アプローチにより、ブランドは、偽造されやすく、不正なチャネルを介した販売（「グレーマーケット」）の影響を受けやすく、サプライチェーン管理の問題に苦しみ、エンドユーザに関連する問題に対処する（例えば、販売の追跡と検証、製品リコールの管理、およびアフターサービスの実行）。小売業者および再販業者は、例えば、偽造品の識別、製品に関する情報へのアクセス、顧客との関係の管理（例：返品、領収書、顧客サポート、特別オファーまたは割引、顧客関係管理）のような同様の問題に対処する。消費者は、偽造製品の識別、製品に関する正確な情報の受信、保証の管理、購入証明の償還、製品登録、製品の本物としての再販など、既存のシステムに関する問題に直面する可能性もある。

30

【0003】

バーコードやQRコード（登録商標）などの従来のタグには、様々な弱点がある。例えば、従来のタグは主に在庫管理単位（stock-keeping unit: SKU）の識別の対象物に使用され、通常は読み取り専用である。さらに、保存された情報は、保存された二値エンコードデータとして読者が自由にアクセスできる。情報は、単一の方法を使用して従来のタグにのみ書き込むことができる。タグを読み取るときは、特定の方向に向ける必要がある。さらに、従来のタグには通常、固定サイズの情報が含まれている。これらのタグは簡単に再利用および複製できる。ウイルス／マルウェアの送信には過去にQRコード（登録商標）が使用されていたため、従来のタグにはセキュリティリスクも含まれている。

40

【発明の概要】

【発明が解決しようとする課題】

【0004】

本明細書で開示する安全タグは、個々の物の認証を取り巻くブランド、商人、および消

50

費者が直面する多くの問題を解決する。これらの安全タグにより、個々の対象物がブロックチェーンまたは同様のデータベースに接続できるようになり、個々の検証が可能になる。個々の製品には、繰り返されることのない固有の安全タグがあり、SKU識別の代わりに個々の項目識別を可能にする。安全なタグを使用して個々の項目を検証できるため、個々の項目の識別により、信頼性の証明が可能になる。この形式の一意の識別は、大きな計算能力とオンライン接続、デジタル印刷、およびブロックチェーンと安全なデータベース技術を備えた高解像度のスマートフォンに一部起因する。

【課題を解決するための手段】

【0005】

本開示の独自の安全タグは、既存のQRコード（登録商標）およびバーコードを超える大きな利点を提供するが、類似点はそれぞれが二値ベースのIDレイヤを持っていることだけである。従来のタグとは異なり、安全タグにはそれぞれ一意の目立たないキーが含まれ、動的で柔軟な保存領域があり、デジタル台帳と統合され、他の多くの利点がある。例えば、安全タグは1つの形状やフォームに限定されず、顧客のニーズに合わせて複数の設計状態で存在できる。さらに、安全タグは、デジタル、印刷、彫刻、アニメーションなどの多くのフォームファクタにまたがって存在できる。安全タグのもう1つの利点は、スマートフォンを含む様々な光学装置で読み取り可能であることであり、これにより、タグをスキャンできるユーザの数が大幅に増える。

【0006】

安全タグには、二値情報とアナログ情報との両方が含まれており、複数の方法で読み取ることができる。安全タグの独自の設計により、大量の二値をタグにエンコードでき、データを返さないがブロックチェーンで安全タグを認証するために使用できる視覚的な「指紋」も可能になる。安全タグは、安全タグを別の安全タグとペアリングおよび／またはシーケンスすることによって、または安全タグの近くで情報を使用する（つまり、近接フィンガプリンティング）などによって、追加の信頼性の層を持つことができる。サプライチェーン全体で、様々なレベルのアクセスを様々なユーザに提供できる。例えば、顧客には、信頼性、安全性、および保証の証明に関する特定の情報を表示するアクセス権を与えることができるが、小売業者には、製品データ、顧客データ、および製品追跡に関する特定の情報を表示するアクセス権を与えることができる。安全タグの使いやすさと有効性により、無数のケースで有用になり、サプライチェーン全体での物事の認証の問題を低減することができる。

【0007】

開示された実施形態は、安全タグと対話するための認証サーバを含む。認証サーバは、少なくとも1つのプロセッサと、少なくとも1つのプロセッサによって実行されたときに、タグ画像を含むタグ識別要求を受信することと、スタイルシートを使用して生成された安全タグの画像の保存されたハッシュを使用して、受信タグ画像内の安全タグを識別することと、受信タグ画像とスタイルシートを使用して生成されたタグをデコードするためのデコード規則とを使用してタグデータを生成することと、タグ識別要求に応じてタグデータを提供することと、を含む動作を認証サーバに実行させる命令を含む少なくとも1つの非一時的メモリと、を備え得る。

【0008】

いくつかの実施形態では、保存されたハッシュおよび受信タグ画像を使用して安全タグを識別することは、受信タグ画像のハッシュを生成することと、保存されたハッシュと生成されたハッシュとの間の差がしきい値基準を満たすと判定することと、をさらに含む得る。受信タグ画像のハッシュを生成することは、受信タグ画像を所定のピクセル数を有する画像に変換することをさらに含む得る。所定のピクセル数は、64ピクセル以上、かつ1,048,576ピクセル以下であり得る。保存されたハッシュを使用して、安全タグが知覚ハッシュであり、保存されたハッシュと生成されたハッシュとの差がハミング距離であることを識別できる。さらに、受信タグ画像はベクトル画像ファイルにすることができ、また、受信した画像のハッシュを生成することは、ベクトルグラフィックスファイル

10

20

30

40

50

の少なくとも一部をラスターライズすることを含み得る。

【0009】

いくつかの実施形態では、受信タグ画像内の安全タグを識別することは、受信タグ画像のハッシュを生成することと、生成されたハッシュと、第1の安全タグの画像の保存されたハッシュとの差を使用して、第1の安全タグを選択することと、受信タグ画像の所定のセグメントの第2のハッシュを生成することと、生成された第2のハッシュと、第1の安全タグの画像における所定の部分の保存された第2のハッシュとの差を使用して、第1の安全タグから安全タグを選択することと、を含み得る。他の実施形態では、受信タグ画像内の安全タグを識別することは、受信タグ画像の漸進的により小さいセグメントのハッシュを生成することを含み得る。

10

【0010】

他の実施形態では、受信タグ画像内の安全タグを識別することは、受信タグ画像のハッシュを生成することと、安全タグの第1の所定のセグメントに対応する受信タグ画像の第1のセグメントの第2のハッシュを生成することと、生成されたハッシュと安全タグの画像の保存されたハッシュとの差がしきい値基準を満たさないと判定することと、生成された第2のハッシュと安全タグの第1の所定のセグメントの画像の保存された第2のハッシュとの差を使用して安全タグを選択することと、安全タグの第2の所定のセグメントに対応する第3のハッシュを生成することと、生成された第3のハッシュと、安全タグの第2の所定のセグメントの画像の保存された第3のハッシュとの間の差を使用して、安全タグを検証することと、を含み得る。特定の態様では、第3のハッシュは、安全タグの第2の所定のセグメントに対応する受信タグ画像の第2のセグメントにわたって生成され得る。他の態様では、第3のハッシュは、安全タグの第2の所定のセグメントに対応する第2の受信タグ画像にわたって生成され得る。

20

【0011】

他の実施形態では、受信タグ画像内の安全タグを識別することは、安全タグの所定のセグメントの画像のハッシュを、受信タグ画像を含む1つ以上の受信タグ画像のセグメントのハッシュと比較し、1つ以上の受信タグ画像のセグメントは、安全タグの所定のセグメントに対応することと、比較に基づいて安全タグを選択することと、を含み得る。比較は、安全タグの所定のセグメントの画像のハッシュと、1つ以上の受信タグ画像のセグメントの対応するハッシュとの間のセグメント距離と、セグメント距離を使用した全体距離またはしきい値基準を満たすセグメント距離のカウントの少なくとも1つと、を判定することを含み得る。動作は、安全タグの所定のセグメントの画像のハッシュの数、しきい値基準を満たすセグメント距離のカウント、およびセグメント距離を使用して信頼値を判定することをさらに含み得る。さらに、1つ以上の受信タグ画像は、第1の詳細レベルでタグの少なくともいくつかを示す第1の画像と、第1の詳細レベルよりも大きい第2の詳細レベルでタグの少なくともいくつかを示す第2の画像と、を含み得る。

30

【0012】

一部の実施形態では、動作は、個人システムから画像の保存されたハッシュを受信することと、個人システムにデコード要求を提供し、デコード要求は安全タグの識別子を含む、ことと、をさらに含んでもよく、デコード規則は、デコード要求に応じて個人システムから受信されてもよい。

40

【0013】

いくつかの実施形態では、タグ識別要求は認証キーを含んでもよく、デコード要求は認証キーを含んでもよく、デコード規則は認証キーに対応し得る。他の実施形態では、タグ識別要求はクライアント装置から受信することができ、動作は、スタイルシートを使用して生成されたタグの公開部分をデコードするための公開デコード規則を受信することと、クライアント装置に公開デコード規則を提供することと、をさらに含み得る。さらに他の実施形態では、デコード規則は、スタイルシートによって規定されたタグ特徴のサブセットのデコードを可能にすることができる。さらに他の実施形態では、デコード規則は、スタイルシートによって規定された安全タグの一部のデコードを可能にすることが

50

できる。

【0014】

いくつかの実施形態では、デコード規則は、スタイルシートによって規定される安全タグの第1の部分またはスタイルシートによって規定されるタグ特徴の第1のサブセットの少なくとも1つのデコードを可能にする第1のデコード規則、および安全タグの第2の部分またはタグ特徴の第2のサブセットの少なくとも1つのデコードを可能にする第2のデコード規則を含み得る。さらに、受信タグ画像とデコード規則を使用したタグデータの生成は、第1デコード規則を使用した第1のタグデータの生成、および第1のタグデータと第2デコード規則を使用した第2のタグデータの生成を含み得る。

【0015】

一部の実施形態では、動作は、タグ識別要求の追跡をさらに含み得る。他の実施形態では、動作は、タグ識別要求情報を保存することをさらに含み得る。さらに他の実施形態では、動作は、タグデータを反映するために分散データベースを更新する命令を提供することをさらに含み得る。

【0016】

開示された実施形態は、安全タグを生成するためのシステムを含む。安全タグを生成するためのシステムは、少なくとも1つのプロセッサと、少なくとも1つのプロセッサによって実行されたときに、安全タグのクラスを説明するスタイルシートを受け取ることと、数値シードを取得することと、数値シードとスタイルシートとを使用して安全タグレイアウトを生成し、安全タグレイアウトは、数値シードとスタイルシートとに基づいてタグ特徴オプションの組み合わせを指定することと、タグデータを受信することと、タグデータの値に従ってタグ特徴オプションを選択することにより、タグデータをエンコードする安全タグを生成することと、安全タグの知覚ハッシュを生成することと、安全タグのハッシュと識別子とをデータベースに保存することと、安全タグを提供することと、を含む動作を認証サーバに実行させる命令を含む少なくとも1つの非一時的メモリと、を備え得る。

【0017】

いくつかの実施形態では、安全タグレイアウトは、データをエンコードするために、安全タグレイアウト内の1つ以上の参照位置を示す参照部分を指定することができる。他の実施形態では、安全タグレイアウトは、データをエンコードするために、安全タグレイアウト内の参照されていない部分を指定することができる。さらに他の実施形態では、安全タグレイアウトは、ランダムデータをエンコードするために、安全タグレイアウトのジャンク部分を指定することができる。さらに他の実施形態では、安全タグレイアウトは、暗号化キーをエンコードするために、安全タグレイアウトのキー部分を指定することができる。

【0018】

いくつかの実施形態では、タグ特徴オプションは、安全タグレイアウトによって指定された位置におけるタグ特徴の有無を含み得る。他の実施形態では、タグ特徴オプションは、タグ特徴のサイズ、色、または形状を含み得る。さらに他の実施形態では、タグ特徴オプションは、安全タグレイアウトによって指定された位置からの逸脱を含み得る。さらに他の実施形態では、タグ特徴オプションは、安全タグレイアウトによって指定された位置に存在するいくつかのタグ特徴を含み得る。

【0019】

いくつかの実施形態では、タグ特徴オプションは、タグ特徴上のスプラインエンコードの存在を含み得る。スプラインエンコードは、基準点または基準線から様々な距離に広がるタグ特徴単を含み得る。様々な距離は、1つ以上の空間的に多重化されたタグデータ値をエンコードできる。さらに、様々な距離は、1つ以上の空間的に多重化されたタグデータ値の繰り返しをエンコードできる。

【0020】

いくつかの実施形態では、タグ特徴オプションは、タグ特徴上の微細構造の存在を含み得る。他の実施形態では、タグ特徴はリムを含むことができ、リムのタグ特徴オプション

10

20

30

40

50

は、リム破損、リム変形、およびリム接続を含む。さらに他の実施形態では、タグ特徴はリム破損を含むことができ、リム破損のタグ特徴オプションはリム破損端形状を含む。さらに他の実施形態では、タグ特徴は、所定のタイプのタグ特徴間の接続を含むことができ、接続のタグ特徴オプションは、接続幅および接続非対称を含む。さらに他の実施形態では、タグ特徴はタグ特徴間の接続を含むことができ、接続のタグ特徴オプションは接続幅と接続非対称性を含む。

【0021】

いくつかの実施形態では、タグ特徴オプションを選択することによりタグデータをエンコードする安全タグを生成することは、第1のタグデータの値に従って第1のタグ特徴オプションを選択し、第1のタグ特徴オプションの選択は第2のタグ特徴オプションを作成することと、第2のタグデータの値に従って第2のタグ特徴オプションを選択することと、を含み得る。さらに、第1のタグ特徴オプションはポイントの有無を含んでいてもよく、第2のタグ特徴オプションは第1のタグデータの値に従って存在するポイント間の接続の有無を含んでいてもよく、第3のタグデータをエンコードする第3のタグ特徴オプションは、第2のタグデータの値に応じて存在する接続の幅を含んでいてもよい。他の実施形態では、タグデータの値に従ってタグ特徴オプションを選択することにより、タグデータをエンコードする安全タグを生成することは、暗号化キーでタグデータを暗号化することと、暗号化されたタグデータの値に従ってタグ特徴オプションを選択することと、暗号化キーを安全タグにエンコードすることと、を含み得る。

【0022】

いくつかの実施形態では、安全タグはベクトルグラフィックスファイルを含み得る。他の実施形態では、安全タグを提供することは、安全タグをラスタライズすることを含み得る。さらに他の実施形態では、安全タグを提供することは、対象物に安全タグでラベル付けすること、または安全タグをデジタル製品に組み込むことを含み得る。さらに他の実施形態では、動作は、タグデータを提供する前に、他の安全タグのハッシュとの衝突について生成されたハッシュをチェックすることをさらに含み得る。さらに他の実施形態では、スタイルシートは、公開データをエンコードするための安全タグレイアウトの一部を生成する公開部分と、個人データをエンコードする安全タグレイアウトの一部を生成する個人部分とを含み得る。さらに他の実施形態では、動作は、安全タグの異なるセグメントの知覚ハッシュを複数の詳細レベルで生成することと、安全タグの異なるセグメントの知覚ハッシュをデータベースに保存することと、をさらに含み得る。

【0023】

いくつかの実施形態では、タグデータは、1つ以上の他の安全タグに関する1つ以上の識別子を含み得る。1つ以上の識別子における第1の識別子は、1つ以上の他の安全タグにおける第1の安全タグの知覚ハッシュをさらに含み得る。他の実施形態では、タグデータは、多要素識別項目の識別子を含み得る。多要素識別項目は、画像の認証資格情報または知覚ハッシュをさらに含み得る。特定の態様では、画像はタグでラベル付けされた対象物の一部を示す。他の態様では、画像はタグに関連付けられた人物を示す。他の実施形態では、タグを提供することは、基板上にタグを印刷し、タグの少なくとも第1の部分が蛍光インクで印刷されることを含み得る。

【0024】

開示された実施形態は、安全タグ読み取り装置を含む。安全タグ読み取り装置は、少なくとも1つのプロセッサと、少なくとも1つのプロセッサによって実行されたときに、画像内の潜在的な安全タグを検出することと、画像およびスタイルシートを使用して、正規化安全タグ画像を生成することと、正規化安全タグ画像を含む識別要求を認証サーバに提供することと、安全タグにエンコードされたタグデータをタグ特徴オプションとしてデコードするための規則を受信することと、受信した規則を使用してタグデータをデコードすることと、を含む動作を安全タグ読み取り装置に実行させる命令を含む少なくとも1つの非一時的メモリと、を備え得る。いくつかの実施形態では、画像は、安全タグ読み取り装置のスキナナから受信することができる。他の実施形態では、スキナナはカメラであり得

る。

【0025】

いくつかの実施形態では、画像内の潜在的な安全タグを検出することは、潜在的な安全タグのサイズがスタイルシートから読み出されたサイズ制約を満たすと判定することを含み得る。他の実施形態では、潜在的な安全タグは、幾何学的特徴検出、カーネルベースの特徴検出、テンプレートマッチング、または畳み込みニューラルネットワークのうちの少なくとも1つを使用して検出することができる。幾何学的特徴検出を使用して画像内の潜在的な安全タグを検出することは、画像をしきい値処理して二値画像を生成することと、スタイルシートから読み出されたターゲットパラメータ値を使用して、二値画像内の幾何学的特徴を検出することと、幾何学的特徴を使用して、潜在的な安全タグの基準点を決定することと、をさらに含み得る。さらに、幾何学的特徴は同心円の楕円を含んでいてもよく、基準点は同心円の楕円の焦点を含んでいてもよい。

10

【0026】

いくつかの実施形態では、潜在的な安全タグの正規化画像を生成することは、画像を白黒画像またはグレースケール画像に変換することを含み得る。他の実施形態では、潜在的な安全タグの正規化画像を生成することは、画像ワープ変換およびスタイルシートから読み出されたターゲットパラメータ値を使用して画像を平坦化することを含み得る。画像ワープ変換を使用して画像を平坦化することは、魚眼歪み、樽型歪み、または角度歪みのうちの少なくとも1つを修正することをさらに含み得る。さらに、ターゲットパラメータ値は、内側または外側のタグリム形状を含み得る。さらに他の実施形態では、潜在的な安全タグの正規化画像を生成することは、潜在的な画像ギャップのタグ特徴オプションを決定し、タグ特徴オプション値をターゲットパラメータ値と比較することにより画像ギャップを検出することを含み得る。ターゲットパラメータ値は、内側または外側のタグリムの厚さと直径比、または内側または外側のタグリムの厚さとタグリムの破損幅比を含み得る。さらに他の実施形態では、潜在的な安全タグの正規化画像を生成することは、タグ特徴の向きを決定し、タグ特徴の決定された向きおよびスタイルシートから検索されたターゲットパラメータ値に基づいて画像を回転させることを含み得る。タグ特徴は中央ロゴにすることができ、ターゲットパラメータ値は中央ロゴの向きを含み得る。

20

【0027】

いくつかの実施形態では、潜在的な安全タグの正規化画像は、ベクトルグラフィックス画像を含み得る。他の実施形態では、画像は複数の潜在的な安全タグを含み、識別要求は、複数の潜在的な安全タグに対応するベクトルグラフィックス画像のストリームを含み得る。さらに他の実施形態では、識別要求は安全タグ読み取り装置の公開鍵を含み、識別要求の少なくとも一部は安全タグ読み取り装置の秘密鍵で暗号化される。さらに他の実施形態では、画像を使用して正規化安全タグ画像を生成することは、安全タグ読み取り装置のユーザインターフェースに、画像と潜在的な安全タグを強調する表示とを表示する指示を提供することと、潜在的な安全タグの第2のズームイン画像を生成する指示を受信することと、潜在的な安全タグの第2のズームイン画像から正規化画像を生成することと、を含み得る。

30

【0028】

いくつかの実施形態では、動作は、安全タグ読み取り装置のユーザインターフェースに、画像と潜在的な安全タグを強調する表示とを表示する指示を提供することと、潜在的な安全タグの選択を受信することと、安全タグ読み取り装置のユーザインターフェースに安全タグデータを表示する手順を提供することと、をさらに含み得る。潜在的な安全タグを強調表示する表示は、画像内の潜在的な安全タグを囲む境界ボックスであり得る。

40

【0029】

いくつかの実施形態では、スタイルシートの公的に利用可能な部分は、タグ特徴オプションとして安全タグにエンコードされた公開タグデータをデコードするための規則を提供できる。公開タグデータは、認証サーバのアドレス、製品タイプ、ブランド名、在庫番号、またはエラー訂正コードの少なくとも1つをさらに含み得る。

50

【0030】

開示された実施形態は、安全タグシステムを含む。安全タグシステムは、安全タグシステムであって、少なくとも1つのプロセッサと、少なくとも1つのプロセッサによって実行されたときに、潜在的なタグ特徴オプションの選択としてタグデータをエンコードする安全タグをスキャンすることと、認証サーバと対話して安全タグをデコードすることと、分散データベースに保存された安全タグの状態情報を受信し、状態情報は、タグの有効性ステータスを示す、ことと、を含む動作を安全タグシステムに実行させる命令を含む少なくとも1つの非一時的メモリと、を備え得る。

【0031】

いくつかの実施形態では、認証サーバと対話して安全タグをデコードすることは、安全タグの画像を認証サーバに提供することを含み得る。他の実施形態では、認証サーバと対話して安全タグをデコードすることは、安全タグの知覚ハッシュを認証サーバに提供することを含み得る。さらに他の実施形態では、認証サーバと対話して安全タグを復号することは、認証キーを認証サーバに提供することを含み得る。状態情報は認証サーバから受信でき、状態情報は認証キーに依存する。さらに他の実施形態では、安全タグをデコードするために認証サーバと対話することは、認証サーバから、タグデータをエンコードするタグ特徴オプションを示すデコード命令を受信することと、デコード命令を使用してタグデータを生成し、タグデータはタグ識別子を含む、ことと、を含み得る。さらに、分散データベースから安全タグの状態情報を受信することは、認証キーをオラクルに提供することをさらに含み、受信した状態情報は認証キーに依存し得る。特定の態様において、認証キーは製造業者に対応でき、状態情報は追跡情報、販売情報、顧客データ、使用情報、活動情報、または位置情報の少なくとも1つを含み得る。他の態様では、認証キーは卸業者に対応することができ、状態情報は信頼性情報、宛先情報、または製造業者情報のうちの少なくとも1つを含み得る。他の態様では、認証キーは小売業者に対応することができ、状態情報は信頼性情報、取引情報、製品情報、または追跡情報のうちの少なくとも1つを含み得る。他の態様では、認証キーは購入者に対応でき、状態情報は認証情報、製品情報、または所有権情報の少なくとも1つを含み得る。

【0032】

いくつかの実施形態では、動作は、分散データベースに格納するための安全タグの更新された状態情報を提供することをさらに含み得る。安全タグの更新された状態情報は、認証キーとともに分散データベースに書き込むために、オラクルにさらに提供できる。さらに、安全タグの更新された状態情報は、安全タグが無効であることを示し得る。他の実施形態では、更新された状態情報は、状態情報の更新されたアクセシビリティオプションを含み得る。さらに他の実施形態では、安全タグの状態情報は、追跡情報、販売情報、顧客データ、使用情報、活動情報、位置情報、信頼性情報、宛先情報、更新された製造者情報、取引情報、製品データ、または所有権の証明情報の少なくとも1つを示し得る。さらに他の実施形態では、安全タグの状態情報は、安全タグと別の安全タグとの間のペアリングを示すことができる。

【0033】

開示された実施形態は、安全タグシステムを含む。安全タグシステムは、少なくとも1つのプロセッサと、少なくとも1つのプロセッサによって実行されたときに、潜在的な第1の安全タグ特徴オプションの選択として第1のタグデータをエンコードする第1の安全タグに関連付けられた製品に関する取引要求を受信することと、潜在的な第2の安全タグ特徴オプションの選択として第2のタグ識別データをエンコードする製品に関する第2の安全タグを生成し、第2のタグデータは第1の安全タグの識別子および購入者の識別子を含む、ことと、購入者への所有権の移転の表示を受信することと、データベースに第2の安全タグのエントリを作成し、作成されたエントリは、所有権の移転を示す、ことと、を含む動作を安全タグシステムに実行させる命令を含む少なくとも1つの非一時的メモリと、を備え得る。

【0034】

いくつかの実施形態では、製品はデジタル製品を含み得る。第1の安全タグは、デジタル製品にさらに埋め込むか、デジタル製品と一緒に表示できる。他の実施形態では、製品は物理的製品を含み得る。第1の安全タグは、物理的製品にさらにラベルを付けることができる。

【0035】

いくつかの実施形態では、動作は、データベース内の第1の安全タグのエントリを更新することをさらに含み得る。エントリをさらに更新して、所有権の移転、第2タグの識別子、所有権の移転に関する取引情報、または第1安全タグの有効性状態の少なくとも1つを示すことができる。他の実施形態では、第1の安全タグの識別子は、少なくともいくつかの第1のタグデータのハッシュを含み得る。さらに他の実施形態では、第2の安全タグを生成することは、第1の安全タグをデコードして第1のタグデータを読み出すことを含み得る。さらに他の実施形態では、第2の安全タグは、第1の安全タグに関連付けられたスタイルシートを使用して生成され得る。さらに他の実施形態では、第2の安全タグは、一意の数値シードを使用して生成され得る。

【0036】

いくつかの実施形態では、データベースは分散データベースであってもよく、データベースに第2の安全タグのエントリを作成するには、ブロックチェーンに書き込むために、認証キーと第2のタグの識別子をオラクルに提供することが含まれる。

【0037】

開示された実施形態は、安全タグと対話するためのサーバを含む。安全タグと対話するためのサーバは、安全タグと対話するためのサーバであって、少なくとも1つのプロセッサと、少なくとも1つのプロセッサによって実行されたときに、潜在的な第1の安全タグ特徴オプションの選択として第1のタグデータをエンコードする第1の安全タグに関する要求を受信し、第1のタグデータは保存された文脈情報を含む、ことと、保存された文脈情報をデコードすることと、文脈情報を受信することと、受信した文脈情報と保存された文脈情報とを使用して要求を認証することと、要求に応じて認証が成功したことを示すことと、を含む動作をサーバに実行させる命令を含む少なくとも1つの非一時的メモリと、を備え得る。

【0038】

いくつかの実施形態では、保存された文脈情報は、認証信任状、生体認証識別子、音声ファイル、タグ識別子、または画像の知覚ハッシュのうちの少なくとも1つを含み得る。生体認証識別子は、指紋または声紋をさらに含み得る。特定の態様において、第1の安全タグは項目にラベルを付けることができ、画像は項目の一部を示すことができる。さらに、ラベル付き項目はIDカードにすることができ、項目の一部は身分証明書の身分証明写真である。他の態様では、第1の安全タグは項目にラベルを付けることができ、画像は項目に関連付けられた人物または項目のテクスチャを示すことができる。

【0039】

いくつかの実施形態では、要求を認証することは、受信した文脈情報および格納された文脈情報が類似性基準を満たすと判定することを含み得る。類似性基準の充足度は、受信した文脈情報と保存された文脈情報との間のハミング距離にさらに依存し得る。他の実施形態では、動作は、文脈情報を要求することをさらに含むことができ、受信した文脈情報は、要求に応じて受信できる。

【0040】

いくつかの実施形態では、認証成功の表示は、少なくともいくつかの第1のタグデータを含み得る。他の実施形態では、認証成功の表示は、少なくともいくつかの第1のタグデータに対するデコード命令を含み得る。さらに他の実施形態では、認証成功の表示は、分散データベースから読み出されたステータス情報を含み得る。さらに他の実施形態では、オラクルを使用して分散データベースからステータス情報を読み出すことができる。

【0041】

開示された実施形態は、2部構成のラベルを含む。2部構成ラベルは、潜在的な第1の

10

20

30

40

50

安全タグ特徴オプションの選択として第1のタグデータをエンコードする第1の安全タグでラベル付けされた基板と、基板に取り外し可能に接着されたオーバーレイであって、第1の安全タグと位置合わせされる透明部分および不透明部分を含み、第1の安全タグと位置合わせされた不透明部分とは、潜在的な第2の安全タグ特徴オプションの選択として第2のタグデータをエンコードする、オーバーレイと、を備え得る。いくつかの実施形態では、潜在的な第1の安全タグ特徴オプションは、潜在的な第2の安全タグ特徴オプションと異なり得る。他の実施形態では、位置合わせされた不透明部分は、選択された潜在的な第1の安全タグ特徴オプションを曖昧にする可能性がある。さらに他の実施形態では、位置合わせされた不透明部分は、潜在的な第1の安全タグ特徴オプションを選択することができる。さらに他の実施形態では、潜在的な第1の安全タグ特徴オプションは、第1の安全タグレイアウトによって指定される位置におけるタグ特徴の有無を含み得る。さらに、潜在的な第2安全タグ特徴オプションは、第1安全タグレイアウトとは異なる第2安全タグレイアウトで指定された位置でのタグ特徴の有無を含み得る。

【0042】

開示された実施形態は、2部構成ラベルを生成する方法を含む。二部構成ラベルを生成する方法は、第1のタグデータ、第1の数値シード、および第1のスタイルシートを使用して、潜在的な第1の安全タグ特徴オプションの選択として第1のタグデータをエンコードする第1の安全タグを生成することと、第2のタグデータ、第2の数値シード、および第2のスタイルシートを使用して、潜在的な第2の安全タグ特徴オプションの選択として第2のタグデータをエンコードする第2の安全タグを生成することと、第1の安全タグと第2の安全タグとの間の差分画像を判定することと、第1の安全タグで基板にラベルを付けることと、基板にオーバーレイを取り外し可能に接着し、差分画像で過度にラベル付けし、第1の安全タグと位置合わせされる、ことと、を含み得る。

【0043】

いくつかの実施形態では、オーバーレイは、第2の安全タグにない第1の安全タグの部分を覆い隠すことがある。他の実施形態では、オーバーレイは、第1の安全タグにない第2の安全タグの部分を示すことができる。さらに他の実施形態では、オーバーレイは、第1の安全タグに存在する第2の安全タグの部分を送信することができる。さらに他の実施形態では、基材は消費財を含み得る。第1の安全タグは消費財の購入後の状態に対応でき、第2の安全タグは消費財の購入前の状態に対応できる。

【0044】

開示された実施形態は、文書を提供する方法を含む。文書を提供する方法は、文書と対になった第1の安全タグを生成し、第1の安全タグは、潜在的なタグ特徴オプションの選択を使用して文書の識別子をエンコードすることと、第1の装置から文書へのアクセス要求を受信することと、第1の装置に第1の安全タグを提供することと、安全タグ画像を含む確認要求を第2の装置から受信することと、第1の安全タグを安全タグ画像と比較することと、比較に基づいて第1の装置に文書を提供することと、を含み得る。特定の態様では、文書の識別子は文書のハッシュを含み得る。さらに、第2の装置はモバイル装置にすることができる。

【0045】

いくつかの実施形態では、第1の安全タグを安全タグ画像と比較することは、第1の安全タグの知覚ハッシュを生成することと、安全タグ画像の知覚ハッシュを生成することと、保存された知覚ハッシュと生成された知覚ハッシュとの差がしきい値基準を満たすと判定することと、を含み得る。他の実施形態では、第1の安全タグを安全タグ画像と比較することは、安全タグ画像の知覚ハッシュを生成することと、生成された知覚ハッシュと、第1の安全タグの画像の保存された知覚ハッシュとの差を使用して、第1の安全タグを選択することと、安全タグ画像の所定のセグメントの第2の知覚ハッシュを生成することと、生成された第2の知覚ハッシュと、第1の安全タグの画像の所定の部分の保存された第2の知覚ハッシュとの差を使用して、複数の第1の安全タグから第1の安全タグを選択することと、を含み得る。

【0046】

いくつかの実施形態では、確認要求は確認要求識別子を含むことができ、比較に基づいて文書を第1の装置に提供することは、要求と対になる第2の安全タグを生成することをさらに含むことができ、第2の安全タグは、潜在的なタグ特徴オプションの選択を使用して確認要求識別子をエンコードすることと、第2の安全タグで文書に透かしを入れることと、を含み得る。

【0047】

いくつかの実施形態では、方法は、安全タグ画像の受信が認証基準を満たすと判定することをさらに含む得る。特定の側面では、認証基準は、第1の安全タグに関連付けられた多数の確認要求に関係する場合がある。他の態様では、認証基準は、第1の装置への第1の安全タグの提供からの経過時間に関係し得る。まだ他の態様では、認証基準は確認要求の地理的起源に関係し得る。まだ他の態様では、確認要求は確認要求識別子を含み得、認証基準は確認要求識別子に関係し得る。さらに、認証基準は、アクセス要求のアクセス識別子が確認要求の確認識別子と一致する場合に満たされ得る。

【0048】

開示された実施形態は、可変安全タグを生成するシステムを含む。可変安全タグを生成するシステムは、少なくとも1つのプロセッサと、少なくとも1つのプロセッサによって実行されたときに、タグデータの値に応じたタグ特徴オプションの選択として、タグデータをエンコードする第1の安全タグを生成することと、第2の装置のスキナから、第1のタグ画像を含むタグ画像のシーケンスを含む要求を受信することと、第1の安全タグと第1のタグ画像とを使用して要求を認証することと、要求の認証の表示を提供することと、を含む操作をシステムに実行させる命令を含む少なくとも1つの非一時的メモリと、を備え得る。特定の態様において、スキナはカメラであり得る。他の態様では、トリガはロールオーバーイベントまたはクリックイベントであり得る。

【0049】

いくつかの実施形態では、動作は、第1の装置のディスプレイ上に第1の安全タグを含むタグのシーケンスを表示する命令を提供することをさらに含む得る。特定の態様では、第1の安全タグを含むタグのシーケンスを表示する命令を提供することは、タグのシーケンスをデジタル製品に埋め込むことを含む得る。他の態様では、命令は、トリガに応じて第1の装置のディスプレイのタグのシーケンスを表示することを提供できる。

【0050】

いくつかの実施形態では、要求を認証することは、第1の安全タグの1つ以上の知覚ハッシュを第1のタグ画像の1つ以上の対応するハッシュと比較することを含み得る。他の実施形態では、要求を認証することは、第1の安全タグを含む複数の安全タグを、第1のタグ画像を含む複数の対応するタグ画像に一致させることを含む得る。認証は、出現の所定の順序に従って、複数の安全タグを複数の対応するタグ画像に一致させることをさらに必要とし得る。さらに他の実施形態では、タグのシーケンスを認証することはジャンクタグを含み得る。

【0051】

いくつかの実施形態では、要求の認証の表示は、タグデータの少なくともいくつかを含み得る。他の実施形態では、要求の認証の指示は、第1のタグデータの少なくともいくつかをデコードするためのデコード命令を含み得る。さらに他の実施形態では、要求の認証の指示は、データベースから読み出されたステータス情報を含み得る。さらに他の実施形態では、データベースは分散データベースであり得、ステータス情報は、オラクルを使用して分散データベースから取得される。

【0052】

開示された実施形態は、製品を追跡する方法を含む。製品を追跡する方法には、数値シードとスタイルシートとの組み合わせに基づくタグ特徴オプションの選択として製品識別データをエンコードするコンピュータ読み取り可能な安全な追跡タグにより製品にラベルを付けることが含まれる。いくつかの実施形態では、タグ特徴オプションは、数値シード

とスタイルシートとの組み合わせによって指定される位置におけるタグ特徴の有無を含み得る。他の実施形態では、タグ特徴オプションは、タグ特徴のサイズ、色、または形状を含み得る。さらに他の実施形態では、タグ特徴オプションは、数値シードとスタイルシートとの組み合わせによって指定される位置からの逸脱を含み得る。さらに他の実施形態では、タグ特徴オプションは、数値シードとスタイルシートとの組み合わせによって指定される位置に存在するいくつかのタグ特徴を含む。

【0053】

いくつかの実施形態では、タグ特徴オプションは、タグ特徴上のスプラインエンコードの存在を含む。スプラインエンコードは、基準点または基準線から様々な距離に広がるタグ特徴端をさらに含み得る。さらに、様々な距離は、1つまたは複数の空間多重タグデータ値をエンコードでき、様々な距離は、1つまたは複数の空間多重タグデータ値の繰り返しをエンコードできる。他の実施形態では、タグ特徴オプションは、タグ特徴上の微細構造の存在を含み得る。さらに他の実施形態では、タグ特徴はリムを含むことができ、リムのタグ特徴オプションは、リム破損、リム変形、およびリム接続を含む。さらに他の実施形態では、タグ特徴はリム破損を含むことができ、リム破損のタグ特徴オプションはリム破損端形状を含む。さらに他の実施形態では、タグ特徴は、所定のタイプのタグ特徴間の接続を含むことができ、接続のタグ特徴オプションは、接続幅および接続非対称を含み得る。さらに他の実施形態では、タグ特徴はタグ特徴間の接続を含むことができ、接続のタグ特徴オプションは接続幅と接続非対称性を含み得る。さらに他の実施形態では、タグ特徴は中央ロゴを含むことができ、タグ特徴オプションは安全タグの中心点からの中央ロゴの変位を含み得る。

【0054】

いくつかの実施形態では、この方法は、コンピュータ可読の安全追跡タグを生成することをさらに含み得る。特定の態様では、コンピュータ可読の安全追跡タグを生成することは、製品識別データの第1の値に従って第1のタグ特徴オプションを選択し、第1のタグ特徴オプションの選択は第2のタグ特徴オプションを作成することと、製品識別データの第2の値に従って第2のタグ特徴オプションを選択することと、をさらに含み得る。第1のタグ特徴オプションには、ポイントの有無をさらに含めることができ、第2のタグ特徴オプションには、第1の値に従って存在するポイント間の接続の有無を含めることができ、製品識別データの第3の値をエンコードする第3のタグ特徴オプションを含めることができる第2の値に従って存在する接続の幅を含めることができる。他の態様では、コンピュータ可読の安全な追跡タグを生成することは、製品識別データの少なくとも一部を暗号化キーで暗号化することと、製品識別データの暗号化された部分の値に従って第1のタグ特徴オプションを選択することと、コンピュータ可読の安全追跡タグに暗号化キーをエンコードすることと、を含み得る。

【0055】

いくつかの実施形態では、コンピュータ可読の安全追跡タグは、ベクトルグラフィックスファイルを含むことができ、コンピュータ可読の安全追跡タグで製品にラベル付けすることは、ベクトルグラフィックスファイルをラスタライズすることを含み得る。他の実施形態では、この方法は、コンピュータ可読の安全追跡タグの識別情報を認証サーバに提供することをさらに含み得る。この方法は、認証サーバに識別情報を提供する前に、コンピュータ可読の安全追跡タグのハッシュを生成し、他のコンピュータ可読の安全追跡タグのハッシュとの衝突についてハッシュをチェックすることをさらに含み得る。

【0056】

開示された実施形態は、製品を追跡するためのラベルを含む。製品を追跡するためのラベルは、数値シードとスタイルシートとの組み合わせに基づくタグ特徴オプションの選択として製品識別データをエンコードするコンピュータ可読の安全追跡タグが印刷された基材を含み得る。いくつかの実施形態では、タグ特徴オプションは、数値シードとスタイルシートとの組み合わせによって指定される位置におけるタグ特徴の有無を含み得る。他の実施形態では、タグ特徴オプションは、タグ特徴のサイズ、色、または形状を含み得る。

さらに他の実施形態では、タグ特徴オプションは、数値シードとスタイルシートとの組み合わせによって指定される位置からの逸脱を含み得る。さらに他の実施形態では、タグ特徴オプションは、数値シードとスタイルシートとの組み合わせによって指定される位置に存在するいくつかのタグ特徴を含み得る。

【0057】

いくつかの実施形態では、タグ特徴オプションは、タグ特徴上のスプラインエンコードの存在を含み得る。スプラインエンコードは、基準点または基準線から様々な距離に広がるタグ特徴端をさらに含み得る。さらに、距離が変化すると、1つまたは複数の空間多重タグデータ値をエンコードでき、様々な距離は、1つまたは複数の空間多重タグデータ値の繰り返しをエンコードできる。他の実施形態では、タグ特徴オプションは、タグ特徴上の微細構造の存在を含み得る。さらに他の実施形態では、タグ特徴はリムを含むことができ、リムのタグ特徴オプションは、リム破損、リム変形、およびリム接続を含み得る。さらに他の実施形態では、タグ特徴はリム破損を含むことができ、リム破損のタグ特徴オプションはリム破損端形状を含み得る。さらに他の実施形態では、タグ特徴は、所定のタイプのタグ特徴間の接続を含むことができ、接続のタグ特徴オプションは、接続幅および接続非対称を含み得る。さらに他の実施形態では、タグ特徴はタグ特徴間の接続を含むことができ、接続のタグ特徴オプションは接続幅と接続非対称性を含み得る。さらに他の実施形態では、タグ特徴は中央ロゴを含むことができ、タグ特徴オプションは安全タグの中心点からの中央ロゴの変位を含み得る。

【0058】

前述の一般的な説明および以下の詳細な説明の両方は、例示および説明のみであり、特許請求されるように、開示された実施形態を限定するものではないことを理解されたい。

【0059】

添付の図面は、必ずしも一定の縮尺または網羅的なものではない。代わりに、一般に、本明細書で説明する本発明の原理を説明することに重点が置かれている。本明細書に組み込まれ、その一部を構成するこれらの図面は、本開示と一致するいくつかの実施形態を示し、詳細な説明とともに、本開示の原理を説明するのに役立つ。

【図面の簡単な説明】

【0060】

【図1】安全タグと対話するための例示的なシステムを示す。

【図2】安全タグと対話するための認証サーバの例示的な概略図を示す。

【図3】タグデータの例示的な概略図を示す。

【図4】開示されたシステムおよび方法を実装するのに一般的に適した例示的なコンピュータ装置の構成要素を示す例示的な図を示す。

【図5】タグ情報を格納するためのデータベースの例示的な概略図を示す。

【図6】タグ生成の例示的なプロセスを示すフローチャートを示す。

【図7】例示的な反復エンコードプロセスを示すフローチャートを示す。

【図8】タグ読み取りの例示的なプロセスを示すフローチャートを示す。

【図9】タグ識別の例示的なプロセスを示すフローチャートを示す。

【図10】多重解像度タグ識別の例示的なプロセスを示すフローチャートを示す。

【図11】タグが変更された多重解像度タグ識別の例示的なプロセスを示すフローチャートを示す。

【図12】多重解像度タグ識別を実行するための例示的なデータ構造を示すフローチャートを示す。

【図13】タグ識別の結果を示す例示的なユーザインターフェースを示す。

【図14】タグ特徴選択をデコードするための例示的なプロセスを示す。

【図15】文脈情報を使用する例示的な認証プロセスを示す。

【図16A】ペアとシーケンスの安全タグを示す。

【図16B】文脈情報と対になった安全タグを示す。

【図17】例示的なオーバーレイタグを示す。

- 【図 1 8】安全タグを使用したマルチチャネル文書認証の例示的なプロセスを示す。
- 【図 1 9】認証のための例示的な安全タグシーケンスを示す。
- 【図 2 0】データベースを使用した在庫管理の例示的なプロセスを示す。
- 【図 2 1】タグを修正するための例示的なプロセスを示す。
- 【図 2 2】対になったタグを使用した在庫管理の例示的なプロセスを示す。
- 【図 2 3】所有権の移転を文書化するための例示的なプロセスを示す。
- 【図 2 4 A】例示的な安全タグを示す。
- 【図 2 4 B】例示的な安全タグに対応するグラフィックファイルの部分を示す。
- 【図 2 5 A】同じスタイルシートと異なるデータを使用して生成された安全タグを示す。
- 【図 2 5 B】異なるスタイルシートと同じデータを使用して生成された安全タグを示す。
- 【図 2 6 A】安全タグ特徴オプションを示す。
- 【図 2 6 B】潜在的な安全タグオプションの詳細を示す。
- 【図 2 6 C】潜在的な安全タグオプションの詳細を示す。
- 【図 2 6 D】潜在的な安全タグオプションの詳細を示す。
- 【図 2 6 E】潜在的な安全タグオプションの詳細を示す。
- 【図 2 6 F】潜在的な安全タグオプションの詳細を示す。
- 【図 2 6 G】潜在的な安全タグオプションの詳細を示す。
- 【図 2 6 H】潜在的な安全タグオプションの詳細を示す。
- 【図 2 6 I】潜在的な安全タグオプションの詳細を示す。
- 【図 2 6 J】潜在的な安全タグオプションの詳細を示す。
- 【図 2 6 K】潜在的な安全タグオプションの詳細を示す。
- 【図 2 6 L】潜在的な安全タグオプションの詳細を示す。
- 【図 2 6 M】潜在的な安全タグオプションの詳細を示す。
- 【図 2 6 N】潜在的な安全タグオプションの詳細を示す。
- 【図 2 7 A】例示的な安全タグの生成を示す。
- 【図 2 7 B】例示的な安全タグの生成を示す。
- 【図 2 7 C】例示的な安全タグの生成を示す。
- 【図 2 7 D】例示的な安全タグの生成を示す。
- 【図 2 7 E】例示的な安全タグの生成を示す。
- 【図 2 7 F】例示的な安全タグの生成を示す。
- 【図 2 7 G】例示的な安全タグの生成を示す。
- 【図 2 7 H】例示的な安全タグの生成を示す。
- 【図 2 7 I】例示的な安全タグの生成を示す。
- 【図 2 7 J】例示的な安全タグの生成を示す。
- 【図 2 8 A】例示的な安全タグの生成を示す。
- 【図 2 8 B】例示的な安全タグの生成を示す。
- 【図 2 8 C】例示的な安全タグの生成を示す。
- 【図 2 8 D】例示的な安全タグの生成を示す。
- 【図 2 8 E】例示的な安全タグの生成を示す。
- 【図 2 8 F】例示的な安全タグの生成を示す。
- 【図 2 8 G】例示的な安全タグの生成を示す。
- 【図 2 8 H】例示的な安全タグの生成を示す。
- 【図 2 8 I】例示的な安全タグの生成を示す。
- 【図 2 8 J】例示的な安全タグの生成を示す。
- 【図 2 8 K】例示的な安全タグの生成を示す。
- 【図 2 8 L】例示的な安全タグの生成を示す。
- 【図 2 8 M】例示的な安全タグの生成を示す。
- 【図 2 8 N】例示的な安全タグの生成を示す。
- 【図 2 9 A】例示的なユーザインターフェースを示す。
- 【図 2 9 B】例示的なユーザインターフェースを示す。

10

20

30

40

50

【発明を実施するための形態】

【0061】

以下の詳細な説明では、開示された例示的な実施形態の完全な理解を提供するために、多くの特定の詳細が述べられている。しかし、例示的な実施形態の原理は、すべての特定の詳細なしで実施できることを当業者は理解するであろう。例示的な実施形態の原理を不明瞭にしないために、周知の方法、手順、および構成要素は詳細には説明されていない。明示的に述べられていない限り、本明細書で説明される例示的な方法およびプロセスは、特定の順序またはシーケンスに制約されず、特定のシステム構成にも制約されない。加えて、記載された実施形態またはその要素のいくつかは、同時に、同じ時点で、または同時に発生または実行され得る。次に、開示された実施形態を詳細に参照し、その例を添付の図面に示す。明示的に述べられていない限り、本明細書で使用される送信および受信は、特定の要求に応じて、またはそのような特定の要求なしで送信または受信を含む広い意味を持つと理解される。したがって、これらの用語は、送信と受信のアクティブ形式とパッシブ形式の両方を対象としている。

【0062】

図1は、安全タグと対話するための例示的なシステム100を示している。この例示的なシステムは、安全タグ105、クライアント装置110、検証サーバ115、個人システム120、および公開データベース125を含み得る。システム100の構成要素は、ネットワーク130を使用して通信するように構成することができる。いくつかの実施形態では、安全タグの画像、スタイルシート、および数値シードを使用して、安全タグ105をデコードすることができる。これらのシステムのいずれかを侵害できる攻撃者が安全タグをデコードできる可能性を減らすために、この情報を個人システム120とクライアント装置110との間で配信することができる。例えば、個人システム120はスタイルシートと数値シードを保存するように構成でき、クライアント装置110は安全タグ105の画像を取得するように構成できる。いくつかの実施形態では、認証サーバ115は、復号を実行し、クライアント装置110から安全タグ105の画像を取得し、個人システム120から命令を復号するように構成することができる。このようにして、システムは、復号化が安全なシステム（認証サーバ115）上で行われることを保証しながら、安全タグ105を復号化するために必要な情報を配信できる。

【0063】

安全タグ105は、製品にラベルを付けるように構成されたタグであり得る。製品は、物理的な製品（靴など）またはデジタル製品（ウェブサイトやビデオスチームなど）にすることができる。本明細書で説明するように、製品は、タグ特徴オプションの選択を使用してタグデータをエンコードするように構成できる。選択のための潜在的なタグ特徴オプションは、スタイルシートと数値シードに依存する。このようにして、スタイルシートは同様の安全タグのクラスを定義できるが、異なる数値シードを使用すると、各タグが一意に保たれる。

【0064】

クライアント装置110は、スキャナを含むモバイル装置を備えてもよい。例えば、クライアント装置110は、スマートフォン、タブレットコンピュータ、またはポータブルコンピュータなどの携帯電話であってもよい。追加の例として、クライアント装置110は、ハンドヘルド光学スキャナ（例えば、SIMATICまたはMOTOROLA光学スキャナ）などの光学スキャナであり得る。クライアント装置110は、安全タグ105の画像を生成し、それらの画像を認証サーバ115に提供するように構成することができる。

【0065】

認証サーバ115は、サーバ、汎用コンピュータ、またはメインフレームコンピュータなどの1つまたは複数のコンピューティングシステムを含み得る。認証サーバ115は、スタンドアロンであってもよいし、サブシステムの一部であってもよく、サブシステムはより大きなシステムの一部であってもよい。例えば、認証サーバ115は、遠隔に配置され、公開ネットワーク（例えば、ネットワーク130）または専用プライベートネットワ

ークを介して通信する分散サーバを含み得る。一部の実施形態では、認証サーバ 115 は、ネットワーク 130 を介してシステム 100 の構成要素と通信するように構成されてもよい。いくつかの態様では、認証サーバ 115 は、アマゾンウェブサービスなどのクラウドコンピューティング環境でホストされる 1 つまたは複数のコンテナまたは仮想マシンを備えてもよい。

【0066】

認証サーバ 115 は、クライアント装置 110 から受信した画像に基づいて安全タグを識別し、個人システム 120 または別のシステムから受信した命令をデコードするように構成することができる。認証サーバ 115 は、公開データベース 130 と対話して、識別されたタグに関するステータス情報を読み書きするように構成することができる。いくつかの実施形態では、認証サーバ 115 は、オラクルを介して間接的に公開データベース 130 と対話するように構成することができる（例えば、公開データベース 130 がイーサリアムブロックチェーンである場合）。認証サーバ 115 は、識別要求に応じて、デコードされたタグ情報または特定のデコード命令をクライアント装置 110 に提供するように構成することができる。

【0067】

個人システム 120 は、サーバ、汎用コンピュータ、またはメインフレームコンピュータなどの 1 つまたは複数のコンピューティングシステムを含み得る。個人システム 120 はスタンドアロンであってもよいし、サブシステムの一部であってもよく、サブシステムはより大きなシステムの一部であってもよい。例えば、個人システム 120 は、公開ネットワーク（例えば、ネットワーク 130）または専用プライベートネットワークを介して遠隔に配置され通信する分散サーバを含み得る。いくつかの実施形態では、個人システム 120 は、ネットワーク 130 を介してシステム 100 の構成要素と通信するように構成されてもよい。いくつかの態様では、個人システム 120 は、アマゾンウェブサービスなどのクラウドコンピューティング環境でホストされる 1 つまたは複数のコンテナまたは仮想マシンを備えてもよい。

【0068】

個人システム 120 は、システム 100 が使用する安全タグを生成するように構成できる。いくつかの実施形態では、個人システム 120 は、安全タグを作成するためのスタイルシート情報および数値シードを格納するように構成することができる。開示された実施形態と一致して、個人システム 120 は、認証サーバ 115 からの要求に応答するように構成され得る。要求には、安全タグ識別子を含めることができる。個人システム 120 は、安全タグ識別子に対応する安全タグのデコード命令を提供するように構成することができる。いくつかの実施形態では、デコード命令は、少なくともいくつかのスタイルシートおよび数値シードを含み得る。デコード命令には、安全タグのタグ特徴オプションとタグデータ間の特定の対応を含めることができる。

【0069】

公開データベース 125 は、コンピュータ装置（例えば、ラップトップ、デスクトップ、ワークステーション、サーバ、汎用コンピュータ、メインフレームコンピュータ、クラウドコンピューティングプラットフォーム）によってホストされる 1 つ以上のデータベースを含み得る。公開データベース 125 は、分散データベースとすることができる。例えば、公開データベース 125 はブロックチェーンデータベースにすることができる。いくつかの実施形態では、公開データベース 125 は、イーサリアムブロックチェーン、または同様のスマートコントラクトブロックチェーンであり得る。

【0070】

図 2 は、開示された実施形態と一致する、安全タグと対話するための認証サーバの例示的な概略図を示す。認証サーバ 115 は、いくつかの態様において認証データベース 205 を含むように構成され得る。認証データベース 205 は、様々な態様でレコード 220 を含み得る。いくつかの実施形態では、記録は、安全タグの 1 つまたは複数のハッシュをタグ識別データに関連付けることができる。様々な実施形態において、認証データベース

10

20

30

40

50

に加えて、認証サーバ 115 は、一般的なアクセス規則を含むように構成され得る。一般的なアクセス規則には、アプリケーションキー要件、認証資格情報要件、セッショントークン要件、または認証サーバへのアクセスに関する同様の制限を含めることができる。

【0071】

図 3 は、開示された実施形態と一致する、タグ識別データの例示的な概略図を示している。いくつかの実施形態では、タグ識別データはタグ固有のアクセス規則 305 を含み得る。例えば、特定の安全タグには、デコードのために特定のアプリケーションキーが必要な場合がある。追加の例として、別の安全タグは、デコードに特定のアプリケーションキーを必要としない場合がある。一部の安全タグには、時間、地理的位置、ローカルネットワーク、またはユーザベースのアクセス規則が含まれる場合がある。認証サーバ 115 は、その安全タグに対する安全タグ固有のアクセス規則 305 を満たさない識別要求を拒否することによりこれらのアクセス規則を実施するように構成することができる。いくつかの実施形態では、タグ識別データはタグ識別子 310 を含み得る。いくつかの態様では、タグ識別子 310 は、特定の安全タグに固有であり得る。例えば、タグ識別子 310 は、安全タグにエンコードされた情報のハッシュであり得る。追加の例として、タグ識別子 310 は、安全タグの知覚ハッシュであり得る。そのような実施形態では、認証サーバ 115 は、タグ識別子に関連付けられたハッシュを格納するのではなく、タグ識別子 310 を単に格納するように構成されてもよい。様々な実施形態において、タグ識別子は、公開データ 315 および個人データ 320 を格納することができる。公開データ 315 は、追跡データまたは位置データなど、認証サーバ 115 のオペレータが公開に利用可能にしたい安全タグとの相互作用に関するメタデータを含み得る。個人データ 320 は、製造業者、販売業者、および小売業者によって収集された製造データまたは顧客データへのアクセスを制限したい認証サーバ 115 のオペレータが安全タグとの相互作用に関するメタデータを含み得る。照会に応じて公開データを提供できるが、認証サーバ 115 は個人データへのアクセスを制限できる。例えば、認証サーバ 115 は、適切なアプリケーションキーまたは認証証明書を含む識別要求に応じて個人データ 320 を提供するように構成され得る。提供される個人データ 320 の量とタイプは、受信したアプリケーションキーまたは認証資格情報によって異なる。いくつかの実施形態では、認証サーバ 115 は、タグ固有のアクセス規則 305、タグ識別子 310、公開データ 315、または個人データ 320 の少なくとも 1 つへのリンクを格納するように構成することができる。例えば、この情報の少なくともいくつかは、公開データベース 130 または別のデータベースに保存することができる。リンクまたは実際のタグ固有のアクセス規則 305、タグ識別子 310、公開データ 315、または個人データ 320 が認証サーバ 115 に保存されるかどうかは、パフォーマンスとセキュリティの問題に依存する。

【0072】

図 4 は、開示されたシステムおよび方法を実装するのに一般的に適した例示的なコンピュータ装置の構成要素を示す例示的な図を示す。いくつかの実施形態によれば、例示的な装置は、プロセッサ 410、メモリ 415、I/O インターフェース 420、およびネットワークアダプタ 425 を含み得る。これらのユニットは、バス 405 を介して、または無線で互いに通信してもよい。図 4 に示す構成要素は、単一の装置または複数の装置に存在する場合がある。

【0073】

プロセッサ 410 は、開示された実施形態に従って様々な方法を実行する 1 つ以上のマイクロプロセッサ、中央処理装置、またはグラフィックス処理装置であってもよい。メモリ 415 は、1 つ以上のコンピュータハードディスク、ランダムアクセスメモリ、リムーバブルストレージ、またはリモートコンピュータストレージを含み得る。様々な実施形態において、メモリ 415 は、プロセッサ 410 によって実行される様々なソフトウェアプログラムを格納する。I/O インターフェース 420 は、キーボード、マウス、オーディオ入力装置、タッチスクリーン、または同様のヒューマンインターフェース装置を含み得る。ネットワークアダプタ 425 により、例示的な装置は、ネットワーク 130 を介して

図1の構成要素と情報を交換することができる。様々な実施形態において、ネットワークアダプタ425は、無線または有線ネットワークをサポートするように構成され得る。特定の態様では、ネットワークアダプタ425は、1つまたは複数のローカルエリアネットワーク、パーソナルエリアネットワーク、または近距離ネットワークをサポートするためのモジュールで構成され得る。いくつかの態様では、ネットワークアダプタ425は、コンピュータバスをサポートするためのハブで構成されてもよい。例えば、ネットワークアダプタ425は、1つ以上のUSBハブで構成されてもよい。

【0074】

図5は、タグ情報を格納するためのデータベースの例示的な概略図を示している。いくつかの実施形態では、公開データベースは、個々のアカウント515およびバンドルアカウント520を含み得る。開示された実施形態と一致して、高価値項目は、個々のアカウント（例えば、家、宝飾品、車など）にステータス情報を格納でき、複数の低価値項目は、単一のバンドルアカウント（例えば、靴）にステータス情報を格納できる、布、パーソナルエレクトロニクス、映画などのデジタル製品など）。いくつかの態様では、高価値項目の安全タグを含む各取引を公開データベース130に書き込むことができ、低価値項目を含む取引のグループを個人データベースに保存し、対応するバンドルアカウント520に定期的書き込むことができる。いくつかの実施形態では、公開データベース130が分散データベースである場合、リクエスト501（例えば、認証サーバ115）は、公開データベースに情報を読み書きするためにオラクル510と対話しなければならない。様々な態様では、リクエストとオラクルを組み合わせる単一のプログラムにすることができる（例えば、認証サーバ115はリクエスト501とオラクル510の両方として機能できる）。いくつかの実施形態では、システム100のユーザは、認証サーバ115に連絡する必要なく、公開データベース130から直接情報を読み取ることができる。例えば、システム100は、公開データベース130に含まれる安全タグに関する情報を読むためのポータルを含み得る。

【0075】

図6は、開示される実施形態と一致する、安全タグ生成の例示的なプロセス600を示すフローチャートを示す。個人システム120によって実行されるものとして以下で説明されるが、プロセス600は、いくつかの実施形態では認証サーバ115または別のシステムによって実行され得る。プロセス600は、安全タグの生成、安全タグレイアウトの生成、安全タグレイアウトとタグデータを使用した安全タグの生成、認証サーバ115への安全タグの登録、およびタグの提供に必要な数値シードとスタイルシートの受信を含み得る製品を追跡するための適切なフォーム。このようにして、タグ特徴オプションの選択としてタグデータをエンコードする、製品に固有の識別子を生成できる。

【0076】

開始後、プロセス600はステップ601に進むことができる。ステップ601で、個人システム120はスタイルシートを受け取ることができる。スタイルシートは、安全タグのクラスを記述することができる。いくつかの実施形態では、安全タグのクラスは、外観、目的、または使用において類似している。例えば、スタイルシートは、特定の製品（靴のモデルなど）にラベルを付けるために特定のメーカ（靴メーカなど）が使用する安全タグのクラスを記述することができる。いくつかの実施形態では、製造業者は、同じスタイルシートを使用して、同じ製品のインスタンスの安全タグを生成することができる。これにより、製造業者は、製品のラベル付けに使用される安全タグ間で視覚的な均一性を達成し、個々のタグが一意であることを保証できる。

【0077】

スタイルシートは、このクラスの安全タグで利用できるタグデータの場所、タグ特徴、およびタグ特徴オプションを定義できる。いくつかの態様では、空間オプション（例えば、タグ特徴サイズ、安全タグ内のタグ特徴位置など）は、比率や角度などの正規化された値によって定義できる。非限定的な例として、スタイルシートは、ポイントの第1の直径オプションを安全タグの中心から安全タグの外縁までの距離の10%に定義できるように

構成できるが、ポイントの第2の直径オプションは安全タグの中心から安全タグの外縁までの距離の15%になる。第2の非限定的な例として、スタイルシートを構成して、タグの中心を原点とする放射状座標フレームに従って潜在的なタグ特徴の位置を定義できる。特定のタグ特徴の潜在的な位置は、オリエンテーションラインから時計回りに5度、中心点からタグの端までの距離の50%である。別の例として、タグの縁の切れ目は、タグの幅の2倍の幅になる可能性がある。タグのリムの幅は、タグの中心点から端までの距離の一部として定義できる。このようにして、スタイルシートを使用して、タグをデコードできるかどうかに関係なく、タグの認証に使用できるタグ特徴に関する一連の制約を定義できる。

【0078】

スタイルシートは、開示された実施形態と一致して、タグ特徴オプションへのデータの潜在的なマッピングを記述することができる。例えば、スタイルシートは、特定のタグ特徴オプションと2進数の特定のビットとの対応を記述することができる。いくつかの側面では、スタイルシートは、タグ特徴オプションの特定の値と2進数のビットの特定の値の間の対応を記述することができる。例えば、タグ特徴オプションに特定の値（または特定の値の範囲、または特定の潜在的な値のセットから選択された値）がある場合、2進数の対応するビットの値は1になる。タグ特徴オプションが異なる特定の値（または異なる特定の値の範囲、または異なる特定の潜在的な値のセットから選択された値）を持つ場合、2進数の対応するビットの値は0になる。様々な側面で、スタイルシートは、安全タグレイアウトの代替オプション、およびタグ特徴オプションとタグデータ値の対応を記述することができる。いくつかの側面では、スタイルシートはタグ特徴が特定の場所に存在するか存在しない可能性を記述することができる。例えば、スタイルシートは、ドットが存在する可能性のある安全タグ内の位置、またはブレークが存在する可能性がある安全タグのリム内の位置を識別できる。これらのオプションは相互に排他的である。例えば、第1のオプションでは、安全タグの特定の部分をタグデータ用に予約できるが、第2のオプションでは、安全タグの特定の部分を安全タグの別の部分への参照用に予約できる、および第3のオプションによると、安全タグの特定の部分は、不正なタグのデコードを阻止するためのランダムタグ特徴で埋めることができる。

【0079】

いくつかの実施形態において、スタイルシートは、複数の安全タグレイアウトオプション（例えば、レイアウトオプション、タグデータからタグ特徴オプション対応へのオプション、特定の場所でのタグ特徴の有無）から選択するためのデータおよび／または命令で構成することができる。この選択プロセスは、ランダムに生成された数値に依存する場合がある。例えば、スタイルシートは、安全タグの特定の場所の第1の使用（データの保存など）と、安全タグの特定の場所の2回目の使用（ジャンク値の保存など）をランダムに生成された数の値に応じて選択するように構成できる。スタイルシートは、そのようなランダムに生成された数値のベクトルを特定の安全タグレイアウトに使用するように構成できる（例えば、特定のレイアウトオプション、タグデータとオプション機能の対応をタグ付けするオプション、特定の場所でのタグ特徴の有無、等。）スタイルシートは、パラメータのベクトルを使用して構成することもできる。例えば、スタイルシートは、ランダムに生成された数値の値がパラメータ α の値を超える場合にタグデータとタグ特徴オプション間の第1の対応を選択し、そうでない場合はタグデータとタグ特徴オプション間の第2の対応を選択するように構成できる。この例を続けるには、別のランダムに生成された数値がパラメータ β の値を超えたときにタグデータをエンコードするための安全タグの第1の場所を選択し、タグをエンコードするための安全タグの第2の場所を選択するようにスタイルシートを構成できるそれ以外のデータ。この例では、 α と β はスタイルシートのパラメータである。これらのパラメータは、デフォルト値をとるか、ユーザから受け取った値、または別のシステムまたは構成ファイルから取得した値をとることができる。

【0080】

いくつかの実施形態では、スタイルシートは、タグがどのように見えるかのパラメータ

10

20

30

40

50

、プリセット、可変、またはランダムに生成された特徴の最小値、最大値、および許容値を含むように構成できる。スタイルシートは、安全タグの使用目的に応じて異なる安全タグレイアウトを生成するように構成できる（例えば、安全タグの意図したサイズ、小さなタグは携帯電話のカメラを使用して読むのが難しい場合があるため、印刷された安全タグ、安全タグの意図された色と表面仕上げ）。いくつかの実施形態では、個人システム120は、スタイルシートの生成、エクスポート、および保管を可能にする構成ツールを提供するように構成することができる。

【0081】

個人システム120は、安全タグレイアウトを作成する際にスタイルシートが使用する乱数を生成するように構成できる。乱数は、擬似乱数ジェネレータを使用して生成できる。一部の態様では、スタイルシートは、擬似乱数ジェネレータを指定できる（例えば、関数ライブラリまたはWebサービスへの参照、擬似乱数ジェネレータのスタイルシートへのエンコードなど）。様々な態様において、個人システム120は、擬似乱数生成器を指定することができる。

10

【0082】

いくつかの実施形態では、擬似乱数生成器は、初期シードに依存する一連の乱数を生成するように構成することができる。同じシードが与えられた場合、擬似乱数ジェネレータは、擬似乱数の同じシーケンスを生成するように構成できる。したがって、スタイルシートによって生成された安全タグレイアウトは、開示された実施形態と一致して、スタイルシートおよびシードの任意のパラメータに依存する可能性がある。

20

【0083】

様々な実施形態において、2進数として表される擬似乱数は、そのビットにより一連の選択を提供することができる。例えば、2進数が00110110の場合、スタイルシートによって提供される第1の2つのオプションに対して「false」オプションを選択し、スタイルシートによって提供される第3のオプションに対して「true」オプションを選択できる。複数のビットを使用して、3つ以上の選択肢を持つオプションを選択できる。例えば、2ビットを使用して、4つの可能な値を持つオプションを選択できる。

【0084】

いくつかの実施形態では、スタイルシートは公開部分を含み得る。いくつかの態様では、システム100は、クライアント装置にスタイルシートの公開部分をプロビジョニングするように構成することができる。様々な態様において、スタイルシートの公開部分は、既知の場所（例えば、既知のURLなど）で利用できる。スタイルシートの公開部分には、タグ特徴の関係を制約する比率の少なくとも一部を含めることができる。例えば、公開部分は、外側のタグリムの幅とタグの直径（または長軸または短軸など）との間の比率を含み得る。この比率を使用して、タグがさらに処理されずに、いくつかの側面で本物かどうかを判断できる。公開部分は、公開タグデータの場所とそのタグデータのデコード方法を示すこともできる。非限定的な例として、スタイルシートの公開部分は、12時の位置から6時の位置まで続く外縁の外縁に沿ったスプラインが、SKU、認証サーバのURL、またはタグの画像が正しく処理されたかどうかを判断する際に使用する既知の値。スタイルシートはタグのクラスを記述するため、この公開部分は、このタグのクラスに属するすべての安全タグでアクセス可能な情報を記述することができる。

30

40

【0085】

いくつかの実施形態では、スタイルシートはプライベート部分を含み得る。プライベート部分は、プライベートタグデータのエンコードに使用できる比率、安全タグレイアウト情報、タグデータとタグ特徴オプションの対応などを記述することができる。いくつかの態様では、スタイルシートのプライベート部分は個人システム120によって保存され得る。

【0086】

開始後、プロセス600はステップ603に進むことができる。ステップ603で、個人システム120は数値シードを取得することができる。個人システム120は、乱数ジ

50

エネレータを使用して数値シードを生成するように構成できる。個人システム120は、システム100のユーザ、構成ファイル、または別のシステムから数値シードを受信するように構成することができる。

【0087】

ステップ601および603の後、プロセス600はステップ605に進むことができる。ステップ605で、個人システム120は、数値シードとスタイルシートを使用して安全タグレイアウトを生成することができる。前述のように、スタイルシートには、タグ特徴オプションとしてデータをエンコードする複数の方法を含めることができる。データをタグ特徴オプションとしてエンコードする特定の方法（安全タグレイアウトなど）の選択は、数値シードに依存する。

【0088】

いくつかの実施形態では、乱数生成器（例えば、ギブソン・リサーチ・コーポレーションの超高エントロピー擬似乱数生成器など）は、数値シードを使用して1つまたは複数の擬似乱数を生成できる。これらの擬似乱数を使用して、データをタグ特徴オプションとしてエンコードする方法を選択できる。例えば、32の二値オプションがある場合、2つの16ビットの2進数のビット値を使用して、32の二値オプションから選択して、安全タグレイアウトを生成できる。追加の例として、ランダムに生成された数値をしきい値パラメータと比較することに基づいて、32の二値オプションを選択できる。例えば、個人システム120は、ランダムに生成された数の値が0.95を超える場合は第1のオプションを選択し、そうでない場合は第2のオプションを選択するように構成され得る。さらなるオプションとして、乱数ジェネレータをカードシャッフルアルゴリズムと組み合わせて使用して、一連の二値データ（例えば、一連の20個のタグ特徴の有無）を生成できる。非限定的な例として、個人システム120は、必要なタグ特徴の数を決定し、これらのタグ特徴の潜在的な位置の数を決定し、潜在的な位置の数に等しいサイズの配列を作成し、必要な数を埋めるように構成することができるタグ特徴の存在を示す値を持つ配列内の要素の組み合わせ。次に、配列をシャッフルしてランダムシーケンスを作成する（例えば、Fisher-Yatesシャッフルアルゴリズムなどを使用）。この方法で、安全タグレイアウトは、数値シードとスタイルシートの選択に基づいてタグ特徴オプションの組み合わせを指定できる。

【0089】

いくつかの実施形態では、安全タグレイアウトは、参照タグ部分、参照部分、参照されていないタグ部分、キー部分、またはジャンク部分のうちの少なくとも1つを指定することができる。これらの部分には、タグデータを含む安全タグの1つ以上の場所を含めることができる。例えば、参照タグ部分には、タグ上の他の場所に保存されているタグデータによって識別される安全タグ内の1つ以上の場所を含めることができる。安全タグの対応する参照部分は、安全タグの参照部分を見つけるために必要なタグデータを保存できる。したがって、安全タグの参照部分をデコードすると、安全タグの対応する参照部分をデコードできるようになる。いくつかの実施形態では、タグの参照部分をデコードするために追加情報が必要になる場合がある。例えば、参照部分に格納されたデータにより、参照部分を見つけることができるが、参照部分でタグデータをデコードするには追加のデコード命令または暗号キーが必要になる場合がある。追加の例として、参照されていない部分には、タグの他の場所に保存されているタグデータによって参照されていない安全タグ内の1つ以上の場所を含めることができる。指示（スタイルシートの関連部分など）がないと、そのような参照されていない部分を特定できず、デコードがはるかに少なくなる。さらなる例として、キー部分は、キーマテリアルが保存される安全タグ内の1つまたは複数の場所を含み得る。いくつかの態様では、そのような鍵素材を使用して、安全タグの他の部分にエンコードされたタグデータをデコードできる。様々な態様において、そのような鍵素材を使用して、タグの他の部分をデコードするための命令を要求することができる（例えば、そのような鍵素材はアプリケーション鍵などを含み得る）。キー部分は、前述のように、参照された部分でも参照されていない部分でもかまわない。いくつかの実施形態で

10

20

30

40

50

は、安全タグは、データを保存しないか、または意味的意味を欠いたランダムデータを保存するジャンク部分を含み得る。このようなジャンク部分は、攻撃者がすべてのタグ特徴に何らかの関連する意味があると単純に想定できないようにし、タグをデコードする不正な試みをより困難にする。

【0090】

いくつかの実施形態では、タグ部分は安全タグの空間領域を記述することができる。例えば、安全タグの物理象限。様々な実施形態では、タグ部分は、安全タグの論理部分を記述することができる。例えば、安全タグはベクトルグラフィックスファイルであり、タグ部分はそのベクトルグラフィックスファイル内の論理的な区分である。例えば、タグ部分には、特定の順序で安全タグのドットの潜在的な位置を記述するSVGタグを含む要素を含めることができる。要素内のタグの順序は、安全タグ内のドットの実際の位置を参照せずに、セキュア画像内のドットの有無に対する数のビットからのマッピングを記述することができる。

10

【0091】

開示された実施形態と一致して、安全タグレイアウトは、複数の異なるタイプのタグ特徴オプションを含み得る。タグ特徴オプションには、安全タグレイアウトで指定された位置にタグ特徴が存在するかどうかが含まれる。例えば、安全タグレイアウトは、安全タグ内の特定の場所にドットを配置できることを示すことができる。その場所にドットが存在することは、タグデータの対応するビットが設定されていることを示す。

【0092】

タグ特徴オプションには、タグ特徴のサイズ、色、または形状を含めることができる。例えば、安全タグレイアウトは、大きなドット（または第1の色のドット、またはゆがんだタグ特徴など）がセットビットに対応し、小さいドット（または第2の色のドット、またはゆがんだタグ特徴など）がnullビットに対応する。

20

【0093】

タグ特徴オプションには、安全タグレイアウトで指定された位置からの偏差を含めることができる。例えば、セキュアレイアウトでは、安全タグ内のタグ特徴の相対位置を指定できる。指定された場所からの偏差は、偏差の方向と大きさによって1つ以上のビットの値をエンコードできる（例えば、X方向の偏差による1つ以上のビットと、Y方向の偏差による1つ以上のビット）。

30

【0094】

タグ特徴オプションには、安全タグレイアウトで指定された位置に存在する多数のタグ特徴を含めることができる。例えば、指定された場所にある多数のドットはビットをエンコードできる。さらなる例として、エンコードは、直接的な対応（例えば、ビットの値がドットの数を含む）または何らかの間接的な対応（例えば、0～2つのドットが存在する場合にビットが設定され、3つ以上のドットが存在する）。

【0095】

タグ特徴オプションには、タグ特徴上の微細構造の存在を含めることができる。そのような微細構造には、微小印刷されたバーコード、QRコード（登録商標）、テキスト、またはその他の機能が含まれる。いくつかの実施形態では、安全タグから第1の距離にある（例えば、5～20cmの間の距離よりも大きい）スキャナがマイクロ構造を解像できないように、マイクロ構造を印刷することができ、安全タグから第2の距離にあるスキャナは（例えば、1～10cm未満の距離）微細構造を解決できる。

40

【0096】

タグ特徴オプションには、タグ特徴でのスプラインエンコーディングの存在を含めることができる。一部の実施形態では、スプラインエンコードは、タグ特徴端の拡張またはバリエーションを含み得る。この延長または変動は、基準点または線から様々な距離を延長できる。例えば、他の点では丸いドットの端は、タグレイアウトで指定されているように、ドットの中心から、またはドットの円周から様々な量だけ拡張できる。この可変距離は、空間的に多重化されたもう1つのタグデータ値をエンコードできる。

50

【0097】

例えば、基本的な空間周波数は、第1のタグ値の二値表現と多重化できる。したがって、基本的な空間周波数は、第1のタグ値のヌルビットに対応する位置ではなく、第1のタグ値のセットビットに対応する位置で端の拡張または変化に寄与する可能性がある。追加の基本空間周波数は、追加のタグ値の二値表現で多重化できる。これらの基本空間周波数は、少なくとも4倍異なる（例えば、第1の基本空間周波数の周期は 2^{12} マイクロメートル、第2の空間周波数の周期は 2^{10} マイクロメートル、第3の空間周波数は周期が 2^8 マイクロメートルなど）。安全タグレイアウトは、スプラインをデコードするための原点と繰り返し数をさらに指定するように構成できる。したがって、距離が変化すると、1つまたは複数の空間多重化タグデータ値の繰り返しをエンコードできる。

10

【0098】

タグ特徴には、内側のリムや外側のリムなど、安全タグのリムを含めることができる。リムのタグ特徴オプションには、リムの破損、リムの変形、リムの接続を含めることができる。リムにオプションとしてリムブレイクが含まれる場合、リムブレイクのタグ特徴オプションにリムブレイク端の形状を含めることができる。

【0099】

タグ特徴には、所定のタイプのタグ特徴間の接続を含めることができる。例えば、そのような接続には、ドット間の接続と、ドットとリムの間の接続（例えば、ドットと内側リムまたは外側リムとの間の接続）を含めることができる。接続のタグ特徴オプションには、接続幅と接続の非対称性を含めることができる。

20

【0100】

タグ特徴には中央のロゴを含めることができる。中央のロゴは、タグの一般的なクラスを識別するために使用できる。例えば、タグ内の公開データのデコードに使用できるスタイルシートの公開部分をユーザが識別できるようにする。中央ロゴのタグ特徴オプションには、安全タグの中心点からの中央ロゴの変位を含めることができる。例えば、安全タグのハッシュまたは安全タグに関連付けられた公開キーは、安全タグの中心点から中心のロゴをずらすことによってエンコードできる。

【0101】

開始後、プロセス600はステップ606に進むことができる。ステップ606において、個人システム120は、タグデータを受信するように構成され得る。タグデータは、ユーザ、入力ファイル、個人システム120のメモリ、別のシステムなどからユーザインターフェースを介して受信することができる。タグデータには、データや命令を含めることができる。データおよび／または命令は、1つ以上の数字で表すことができる。タグデータには、多要素識別項目の識別子を含めることができる。タグを読み取ったり、タグを使用してアクションを実行しようとする、タグをデコードし、識別子を他のデータと比較して、読み取りまたはアクションが認証または許可されているかどうかを判断できる。例えば、多要素識別項目には、認証資格情報（パスワード、APIキー、トークン、パスワードのハッシュ、APIキー、またはトークンなど）を含めることができる。追加の例として、多要素識別項目には、画像や画像の知覚ハッシュ、声紋や音声のハッシュなどの文脈情報を含めることができる。例えば、画像はタグでラベル付けされた製品の一部を表すことができる。タグでラベル付けされた製品の一部の画像の知覚ハッシュを含めて、個人システム120は、タグが別の製品に移動したり、安全タグのコピーで複数の製品にラベル付けされたりするのを防ぐように構成できる。追加の例として、画像は安全タグに関連付けられた人物を描写できる。非限定的な例として、個人はラベル付き製品の所有者になることができる。この方法で、安全タグを使用して所有権を確認できる。

30

40

【0102】

さらなる例として、タグデータは、1つ以上の他の安全タグの1つ以上の識別子を含み得る。例えば、1つ以上の識別子の第1の識別子は、1つ以上の他の安全タグの第1の安全タグの知覚ハッシュを含み得る。この方法で、追加のタグを現在のタグと対にすることができる。いくつかの実施形態では、認証サーバは、現在のタグに関する要求を認証また

50

は認可するために、これらの追加タグの画像またはこれらの追加タグの知覚ハッシュの提供を要求するように構成できる。

【0103】

ステップ606の後、プロセス600はステップ607に進むことができる。ステップ607で、個人システム120は、タグデータをエンコードする安全タグを生成することができる。いくつかの態様では、個人システム120は、タグデータの値に従ってタグ特徴オプションを選択することにより、タグデータをエンコードする安全タグを生成するように構成することができる。例えば、安全タグレイアウトが複数のドットまたはリムブレイクの潜在的な場所を含むタグ特徴オプションを提供し、タグデータに2進数が含まれる場合、2進数の対応するビットが存在するかどうかに応じて、ドットまたはリムブレイクが存在するかどうか設定されているか、`null`である。いくつかの実施形態において、タグデータの少なくとも一部は、暗号化キーを使用して暗号化され得る。暗号化されたタグデータの値に従ってタグ特徴オプションを選択することにより、安全タグを生成できる。いくつかの実施形態では、暗号化されたタグデータを解読するための暗号化キーは、安全タグにエンコードすることもできる（例えば、安全タグの参照または非参照キー部分）。いくつかの実施形態では、安全タグは、スケーラブルベクトルグラフィックスファイル、カプセル化ポストスクリプトファイル、ポータブル文書フォーマットファイルなどのベクトルグラフィックスファイルであり得る。

10

【0104】

ステップ607の後、プロセス600はステップ609に進むことができる。ステップ609で、個人システム120は、安全タグの知覚ハッシュ（`pHash`など）を生成することができる。知覚ハッシュの生成には、安全タグのラスタライズが含まれる。例えば、安全タグがベクトルグラフィックスファイルとして保存されている場合、知覚ハッシュの生成には、知覚ハッシュをラスタグラフィックスファイル形式に変換することが含まれる。いくつかの実施形態において、個人システム120は、生成された`pHash`を既存の安全タグの`pHash`のライブラリと比較することによりハッシュ衝突をチェックするように構成され得る。ハッシュ衝突が存在する場合、個人システム120は、新しい数値シードを使用して安全タグを再作成するように構成できる。様々な実施形態において、個人システム120は、複数レベルの詳細で安全タグの異なるセグメントの追加の知覚ハッシュを生成するように構成され得る。

20

30

【0105】

ステップ609の後、プロセス600はステップ611に進むことができる。ステップ611で、個人システム120は、安全タグの知覚ハッシュをデータベース（例えば、認証サーバ115のデータベース）に保存することができる。いくつかの態様では、個人システム120が安全タグの異なるセグメントの追加のハッシュを生成するように構成されている場合、これらの追加のハッシュは安全タグ全体の知覚ハッシュとともにデータベースに保存できる。個人システム120は、安全タグのハッシュとともにデータベースにセキアハッシュの識別子を格納するように構成することができる。この識別子は、個人システム120がどのスタイルシートと数値シードが安全タグを生成するために使用されたかを決定できるように構成することができる。例えば、個人システム120は、安全タグを追跡するためのデータベースを維持するように構成され得る。このデータベースには、キー値としての安全タグ識別子、各安全タグの生成に使用されるスタイルシートの指示、および各安全タグの生成に使用される数値シードを含めることができる。いくつかの実施形態では、このデータベースは、安全タグまたは安全タグの画像を生成するために使用されるタグデータを含まない。したがって、この安全なデータベースを侵害できる攻撃者は、ストア識別子、スタイルシート参照、および数値シードからタグデータを再作成することはできない。

40

【0106】

ステップ611の後、プロセス600はステップ612に進むことができる。ステップ612において、個人システム120は、安全タグを提供するように構成され得る。いく

50

つかの実施形態では、安全タグを提供することは、タグで対象物にラベル付けすること、またはビデオファイルまたはウェブページなどのデジタル製品に安全タグを組み込むことを含み得る。例えば、安全タグを提供することは、コンピュータスクリーンなどに安全タグを表示するための指示を提供することを含み得る。様々な実施形態において、タグを提供することは、基材上にタグを印刷することを含み得る。例えば、安全タグを提供することは、安全タグを製品にラベル付けする印刷システムに安全タグをベクトルファイルまたはラスタファイルとして提供することを含み得る。したがって、安全タグの提供には、安全タグのラスタライズが含まれる。いくつかの実施形態では、タグは複数のタイプのインクで提供され得る。例えば、蛍光インクで印刷されたタグの少なくとも第1の部分。この蛍光インクは、特定の照明条件下でのみ表示され、タグデータをエンコードするための追加オプションが作成される。

10

【0107】

いくつかの実施形態では、認証サーバ115は、データベース（例えば、データベース130）からタグステータス情報を取得するように構成され得る。例えば、認証サーバ115は、安全タグがまだ有効であるか、キャンセルされているか、安全タグに関するアクションに関する認証要件を含むかを決定するように構成できる（例えば、実行するためにユーザにアプリケーションキーまたは認証資格情報を提供することを要求する）安全タグを含む取引）。

【0108】

図7は、開示された実施形態と一致する、例示的な反復エンコードプロセス700を示すフローチャートを示している。以下に個人システム120によって実行されるものとして説明するが、プロセス700は、いくつかの実施形態では認証サーバ115または別のシステムによって実行することができる。プロセス700は、安全タグレイアウトを受信し、現在のタグ状態に基づいて利用可能なタグ特徴を決定し、タグデータ値を使用してタグ特徴オプションを選択し、選択したタグ特徴オプションに基づいて利用可能なタグ特徴オプションを更新することを含み得る。この方法で、タグデータの項目を安全タグに繰り返しエンコードし、各反復でタグデータの次の項目のエンコードに使用するタグ特徴オプションを作成できる。

20

【0109】

開始後、プロセス700はステップ701に進むことができる。ステップ701で、個人システム120は安全タグレイアウトを受け取ることができる。安全タグレイアウトは、安全タグを生成するプロセスの前のステップ（例えば、プロセス600のステップ605）、個人システム120のメモリ、システム100の別の構成要素、または別のシステムから受け取ることができる。安全タグレイアウトには、潜在的なタグ特徴オプションのセットを含めることができる。

30

【0110】

ステップ701の後、プロセス700はステップ703に進むことができる。ステップ703で、個人システム120は、現在のタグ状態に基づいて利用可能なタグ特徴を決定することができる。例えば、安全タグレイアウトでは、タグ特徴にドットとドット間の接続を含めることができるように指定できる。安全タグレイアウトは、潜在的なドット位置の順序を指定することができ、順序内の潜在的なドット位置の位置は、二値タグデータのビット位置に対応する。安全タグレイアウトは、ドットの存在がビット値1に対応し、ドットの非存在がビット値0に対応することを指定できる。この例では、現在のタグの状態にこれらの潜在的なドット位置を含めることができる。現在のタグの状態には、潜在的なリム破損や歪みなど、追加の利用可能なタグ特徴も含まれる場合がある。

40

【0111】

ステップ703の後、プロセス700はステップ705に進むことができる。ステップ705において、個人システム120は、タグデータ値を使用して利用可能なタグ特徴オプションからタグ特徴オプションを選択することができる。前の例を続けるために、個人システム120は、二値タグデータからビットを読み取り、ビットの値が1のときに対応

50

する潜在的なドット位置にドットを配置できる（ビットの値が0）。ドットに関して説明するが、このようなプロセスは他のタグ特徴にも同様に適用できる。

【0112】

ステップ705の後、プロセス700はステップ707に進むことができる。ステップ707において、個人システム120は、選択されたタグ特徴オプションに基づいて利用可能なタグ特徴オプションを更新することができる。前の例を続けると、潜在的なドット位置は選択可能なタグ特徴オプションを構成しなくなる可能性があるが、ドットサイズ、ドットカラー、ドット間の接続の有無、およびドットとリム間の接続の有無は、利用できる。スタイルシートは、これらのタグ特徴オプションとタグデータ項目間の対応を管理する規則を提供できる。例えば、スタイルシートは、ドット間の接続を二値タグデータの特定のビットに関連付ける規則を提供できる。

10

【0113】

個人システム120は、タグデータが完全にエンコードされるまで、タグ特徴オプションの選択を継続し、利用可能なタグ特徴オプションのセットを更新するように構成できる。例えば、個人システム120は、第1のタグデータの値に従って第1のタグ特徴オプションを選択することができる。この第1のタグ特徴オプションの選択により、第2のタグ特徴オプションを作成できる。次に、個人システム120は、第2のタグデータの値に従って第2のタグ特徴オプションを選択することができる。この第2のタグ特徴オプションの選択により、第3のタグ特徴オプションを作成できる。非限定的な例では、第1のタグ特徴オプションにはポイントの有無を含めることができ、第2のタグ特徴オプションには、第1のタグデータの値に従って存在するポイント間の接続の有無を含めることができ、第3のタグ第3のタグデータをエンコードする機能オプションには、第2のタグデータの値に応じて存在する接続の幅を含めることができる。

20

【0114】

図8は、タグ読み取りの例示的なプロセス800を示すフローチャートを示している。プロセス800は、タグ検出、タグ識別およびサーバ側復号化、およびオプションのクライアント側復号化のステップを含む。いくつかの実施形態では、タグ検出は、クライアント装置110のスキナ（例えば、モバイル装置のカメラ、またはハンドヘルド光学スキナ）から受信した画像を使用して、クライアント装置110によって実行され得る。様々な実施形態では、タグ検出は、別の装置から受信した画像を使用してクライアント装置110によって実行され得る。様々な実施形態において、タグ識別およびサーバ側復号化は、認証サーバ115、個人システム120、または別のシステムによって実行され得る。様々な実施形態では、オプションのクライアント側復号化は、クライアント装置110によって実行され得る。

30

【0115】

開始後、プロセス800はステップ801に進むことができる。ステップ801で、クライアント装置110は、安全タグ105の少なくとも一部を含むラスタ画像を受信することができる。いくつかの実施形態では、タグ検出801は、ラスタ画像を正規化されたベクトルグラフィック画像に変換し、ベクトルグラフィック画像を認証サーバ115に提供することを含み得る。様々な実施形態において、タグ検出801は、ラスタ画像を正規化されたラスタ画像に変換し、正規化されたラスタ画像を認証サーバ115に提供することを含み得る。

40

【0116】

タグ検出801は、幾何学的特徴検出、カーネルベースの特徴検出、テンプレートマッチング、または畳み込みニューラルネットワークのうちの少なくとも1つを使用して受信画像内の安全タグ105を検出することを含み得る。いくつかの実施形態では、幾何学的特徴検出を使用して受信画像内の安全タグ105を検出することは、ラスタ画像をしきい値処理して二値画像を生成することを含み得る。このしきい値処理には、カラー画像をグレースケール画像に変換し、グレースケール値に基づいて画像をしきい値処理するか、カラー画像を白黒画像に変換することが含まれる。いくつかの実施形態では、クライアント

50

装置 110 は、Image Magic、OpenCV などによって提供される画像処理機能を使用して画像変換を実行するように構成することができる。

【0117】

クライアント装置 110 は、開示された実施形態と一致して、既知のターゲットパラメータに一致する受信タグ画像内の幾何学的特徴を検出するように構成され得る。クライアント装置 110 は、幾何学的特徴を使用して潜在的な安全タグの基準点を検出するように構成することもできる。いくつかの態様では、クライアント装置 110 は、OpenCV などによって提供される幾何学的特徴検出アルゴリズムを使用するように構成することができる。いくつかの態様では、クライアント装置 110 は、二値画像内の幾何学的特徴を検出する際にスタイルシートから取得されたターゲットパラメータ値を使用するように構成され得る。例えば、スタイルシートの公開部分には、安全タグのクラスに存在する幾何学的特徴の説明を含めることができる。そのような幾何学的特徴は、内側および／または外側のタグリムの形状を含み得る。例えば、スタイルシートは、内側および外側のタグの縁が所定の寸法比を持つ円であることを示すことができる。次に、クライアント装置 110 は、幾何学的特徴検出アルゴリズムを使用して、受信タグ画像内の適切な寸法比率で同心円楕円を検出することができる。いくつかの実施形態では、基準点は同心楕円の焦点であり得る。いくつかの実施形態では、クライアント装置 110 は、安全タグ 105 の中心として基準点を登録することができる。

10

【0118】

クライアント装置 110 は、開示された実施形態と一致して、カーネルベースの特徴検出を使用して画像内の潜在的なタグ位置を検出するように構成され得る。いくつかの態様では、カーネルベースの特徴検出を使用して、安全タグ 105 または安全タグ 105 内のタグ特徴の概要を識別することができる。開示された実施形態と一致して、カーネルベースの特徴検出は、OpenCV などによって提供されるカーネルベースの特徴検出アルゴリズムを使用して実行することができる。

20

【0119】

クライアント装置 110 は、テンプレートマッチングまたは画像ステンシル検出を使用して、画像内の潜在的なタグ位置を検出するように構成することができる。いくつかの実施形態では、テンプレートまたはステンシルは、スタイルシートの公開部分を使用して含まれるか、または生成され得る。テンプレートまたはステンシルは、中央のロゴやタグの縁など、安全タグの一部を識別することに関するものである。例えば、テンプレートまたはステンシルは中央のロゴと一致させることができる。クライアント装置 110 は、OpenCV などによって提供されるテンプレートマッチングアルゴリズムを使用して、テンプレートマッチングまたは画像ステンシル検出を実行するように構成することができる。

30

【0120】

クライアント装置 110 は、畳み込みニューラルネットワークを使用して画像内の潜在的なタグ位置を検出するように構成することができる。畳み込みニューラルネットワークは、YOLO などが提供するリアルタイム対象物検出機能を使用して実装できる。畳み込みニューラルネットワークをトレーニングして、安全タグを画像内の他の特徴と区別することができる。いくつかの実施形態では、畳み込みニューラルネットワーク（または別の畳み込みニューラルネットワーク）は、画像内の安全タグの識別に続いて、安全タグのクラスを区別するように構成できる。

40

【0121】

タグ検出ステップ 801 の間に、クライアント装置 110 は、受信した画像とスタイルシートを使用して正規化された安全タグ画像を生成するように構成することができる。いくつかの実施形態では、クライアント装置 110 は、スタイルシートの公開部分を使用するように構成することができる。スタイルシートの公開部分は、タグのクラスのターゲットパラメータ値を指定できる。これらのターゲットパラメータ値には、タグのクラスにタグの共有特性を含めることができる。このような共有特性には、中央ロゴ、内側リム、外側リムなどのタグ特徴の有無、形状、向きが含まれる。ターゲットパラメータ値には、タ

50

グ特徴のディメンション間の関係を表す比率をさらに含めることができる。例えば、そのような比は、内側（または外側）タグリムの厚さとタグ直径の間の比、または内側（または外側）タグリムの厚さとタグリムの破断幅の間の比を含み得る。ターゲットパラメータ値には、タグのサイズの制約（例えば、円形の安全タグの全体の直径）も含めることができる。クライアント装置 110 は、受信した画像で識別された安全タグがスタイルシートの公開部分から検索された全体的なサイズ制約を満たすかどうかを判定するように構成することができる。スタイルシートの公開部分は、安全タグにエンコードされた公開タグデータをタグ特徴オプションとしてデコードするための規則も提供できる。例えば、スタイルシートの公開されている部分は、正規化画像から識別可能なタグ特徴オプションとエンコードされたタグデータとの間の対応を記述できる。スタイルシートの公開部分を含むスタイルシートは、エンコードされたデータのセマンティクスも記述できる。例えば、スタイルシートの公開部分は、公開アクセス可能なエンコードされた二値データを認証サーバのアドレス、製品タイプ、ブランド名、在庫番号、またはエラー修正コードとして識別できる。

【0122】

タグ検出ステップ 801 の間に、クライアント装置 110 は、画像ワープ変換を使用して受信画像を平坦化するように構成され得る。いくつかの実施形態では、クライアント装置 110 は、スタイルシートの公開部分から検索されたターゲットパラメータ値を使用してワープ変換を実行することができる。いくつかの態様では、画像ワープ変換は、受信した画像で検出されたタグ特徴を、スタイルシートの公開部分で指定された既知の位置にマッピングできる。例えば、クライアント装置 110 は、受信した画像内の潜在的な安全タグリムを検出し、検出された画像位置から既知の画像位置への変換を決定することができる。OpenCV などによって提供される画像ワーピング機能を使用して、クライアント装置 110 は、画像全体を変換して、検出された特徴をスタイルシートの公開部分によって記述される特徴位置によりよくマッピングするように構成できる。このようにして、クライアント装置 110 は、魚眼歪み、樽型歪み、または角度歪みのうちの少なくとも 1 つを補正するように構成され得る。

【0123】

タグ検出ステップ 801 の間に、クライアント装置 110 は、タグ特徴の向きを決定し、決定されたタグ特徴の向きに基づいて画像を回転させるように構成され得る。回転は、スタイルシートの公開部分から取得したターゲットパラメータ値にさらに基づくことができる。タグ特徴は、安全タグの中央のロゴにすることができる。クライアント装置 110 は、上記のテンプレートマッチングシステムを使用してタグの中心を識別するように構成され得る。クライアント装置 110 は、次いで、安全タグ全体を包含する外側卵形ラインを決定するように構成され得る。クライアント装置 110 は、安全タグの中心を決定するように構成され得る。中心と卵形の線を決定した後、クライアント装置 110 は、安全タグ画像上に複数の直角三角形を構築するように構成することができる。直角三角形は、各直角三角形の中心が安全タグの中心と重なるように配置できるが、斜辺を囲む 2 つの頂点は外側の卵形の縁と交差する。最小および／または最大の斜辺を持つ三角形を、スタイルシートの公開部分の方向情報と組み合わせて使用して、タグの方向を修正できる。クライアント装置 110 は、中央ロゴに基づいて適切なスタイルシートを決定するように構成され得る。安全タグに中央ロゴが含まれていない場合、クライアント装置 110 は、デフォルトの場所でタグ特徴オプション（例えば、スプラインエンコーディングを使用して外縁スプラインからの文字）を読み取ることにより、タグスタイルシートを決定するように構成できる。

【0124】

タグ検出ステップ 801 の間に、クライアント装置 110 は、画像ギャップを検出するように構成され得る。このような画像のギャップは、損傷、照明（例えば、周囲光のスキヤナへの反射）、または表面状態（例えば、汚れ）から発生する可能性がある。クライアント装置 110 は、潜在的な画像ギャップのタグ特徴オプションを検出し、タグ特徴オブ

10

20

30

40

50

ション値をスタイルシートの公開部分にリストされたターゲットパラメータ値と比較するように構成することができる。潜在的な画像ギャップがスタイルシートの公開部分のターゲットパラメータ値と一致しない場合、クライアント装置 110 は画像ギャップを無視し、公開のターゲットパラメータ値に基づいて画像ギャップを介して画像ギャップを囲むタグ特徴を拡張するように構成できるスタイルシートの一部。例えば、クライアント装置 110 は、認証サーバ 115 への送信のために正規化されたラスタ画像をベクトルグラフィックスファイルに変換するときにリムギャップを無視することにより、アーチファクトであると判定されたリムギャップを処理するように構成され得る。

【0125】

タグ検出ステップ 801 の間に、クライアント装置 110 は、認証サーバに識別要求を提供するように構成することができ、識別要求は正規化された安全タグ画像を含む。本明細書では「識別要求」として説明されているが、そのような要求を提供する理由または目的は、安全タグの識別に限定されない。例えば、識別要求の提供は、安全タグでラベル付けされた項目の所有権の取引、安全タグに関する規則の更新、安全タグのキャンセルなど、安全タグに関連するアクションの一部になる。上述のように、クライアント装置 110 は、受信したラスタ画像の向きを少なくとも正規化し、ラスタ画像を平坦化し、画像のギャップを修正するように構成することができる。クライアント装置 110 は、ラスタ画像を SVG、EPS、または PDF 画像などのベクトルグラフィック画像に変換することにより、正規化された安全タグ画像を生成するように構成することができる。

【0126】

いくつかの実施形態において、クライアント装置 110 は、安全タグ読み取り装置のユーザインターフェース上で画像および潜在的な安全タグを強調表示する指示を表示する命令を提供するように構成され得る。例えば、クライアント装置 110 がスマートフォンのカメラである場合、スマートフォンのディスプレイは画像を描写し、検出された安全タグの周りに境界ボックスまたは同様の表示を含み得る。いくつかの実施形態では、境界ボックスは、タグが正常に識別されたかどうかを示すことができる。例えば、境界ボックスの色、形状、線種などは、タグが正常に識別されたかどうかを示すことができる。クライアント装置 110 は、検出されたタグの領域を光学的またはデジタル的にズームするなど、境界ボックスの選択時にアクションを実行するように構成することができる。

【0127】

ステップ 801 の後、プロセス 800 はステップ 803 に進むことができる。ステップ 803 で、クライアント装置 110 は、認証サーバ 115 に識別要求を提供するように構成され得る。識別要求は、ステップ 801 で生成された正規化画像を含み得る。正規化画像は、ベクトルグラフィックス画像である。いくつかの実施形態では、ステップ 801 でクライアント装置 110 によって受信したラスタ画像は、複数の潜在的な安全タグを含み得る。そのような実施形態では、クライアント装置 110 は、複数の潜在的な安全タグの正規化画像を検出および生成するように構成することができる。クライアント装置 110 は、複数の潜在的な安全タグに対応するベクトルグラフィックス画像のストリームとして生成された正規化画像を提供するように構成され得る。いくつかの実施形態では、識別要求は安全タグ読み取り装置の公開鍵を含むことができ、識別要求の少なくとも一部はクライアント装置 110 の秘密鍵で暗号化することができる。

【0128】

いくつかの実施形態では、クライアント装置 110 は、別の画像を生成する命令を受信するように構成され得る。これらの指示は、認証サーバ 115 から受け取ることができる。命令は、潜在的な安全タグの第 2 のズームイン画像をクライアント装置 110 に自動的に生成させることができる。代替的または追加的に、命令は、潜在的な安全タグの第 2 のズームイン画像をクライアント装置 110 に生成させるようにユーザに指示することができる。次に、クライアント装置 110 は、潜在的な安全タグの第 2 のズームイン画像から別の正規化画像を生成するように構成することができる。

【0129】

ステップ 803 の後、プロセス 800 はステップ 805 に進むことができる。ステップ 805 で、クライアント装置 110 は、認証サーバ 115 からデコード命令および／またはタグデータを受信することができる。いくつかの実施形態では、デコード命令は、スタイルシートの公開部分を補足することができる。例えば、デコード命令は、スタイルシートによって開示される可能性を、タグ特徴オプションとタグデータ値の間の特定のマッピングに制限することができる。様々な実施形態において、デコード命令は、タグ特徴オプションをタグデータ値に変換するための特定の規則セットを記述することができる。例えば、デコード命令は、特定のタグデータ項目が、特定されたタグ特徴オプションのセットに依存する値を持つことを示すことができる。

【0130】

上述のように、いくつかの実施形態では、クライアント装置 110 は、安全タグ読み取り装置のユーザインターフェース上で画像および潜在的な安全タグを強調表示する指示を表示するように構成することができる。いくつかの実施形態では、クライアント装置 110 は、潜在的な安全タグを選択するユーザからの指示を受信するように構成することができる（例えば、指示は潜在的な安全タグを囲むバウンディングボックスであり、指示は、ユーザによるバウンディングボックスの選択を含み得るタッチセンサ式ディスプレイ）。クライアント装置 110 は、潜在的な安全タグの正規化画像を生成し、認証サーバ 115 に識別要求を提供し、それに応じて認証サーバ 115 からタグデータおよび／または復号命令を受信するように構成できる。クライアント装置 110 は、認証サーバ 115 から受信した任意の復号化命令を使用してタグデータを復号化するように構成することができる。次に、クライアント装置 110 は、クライアント装置 110（または別の装置）のユーザインターフェース上に安全タグデータ（例えば、受信および／またはデコードされたタグデータ）を表示する命令を提供するように構成され得る。

【0131】

図 9 は、タグ識別の例示的なプロセス 900 を示すフローチャートを示している。以下に認証サーバ 115 によって実行されるものとして説明するが、プロセス 900 は、いくつかの実施形態では、個人システム 120、クライアントシステム 110、または別のシステムによって実行することができる。開示された実施形態と一致して、プロセス 900 は、タグ識別要求を受信するステップ、タグ識別要求に基づいて安全タグを識別するステップ、検索されたタグ画像およびデコード規則を使用してタグデータを生成するステップ、およびそれに応じてデコードされたタグデータを提供するステップを含み得る要求。

【0132】

開始後、プロセス 900 はステップ 901 に進むことができる。ステップ 901 で、認証サーバ 115 はタグ識別要求を受信することができる。タグ識別要求には、タグ画像（例えば、識別されていない安全タグを含む写真またはビデオ画像）を含めることができる。認証サーバ 115 は、クライアント装置 110 からタグ識別要求を受信するように構成することができる。タグ識別要求は、ネットワーク 130 を使用して受信できる。いくつかの態様では、タグ識別要求には、認証キー（API 呼び出しを認証するための API キーなど）を含めることができる。いくつかの態様では、タグ識別要求は、セッショントークン（例えば、OAuth 2.0 ベアトークン、Kerberos トークンなど）を含み得る。いくつかの態様では、タグ識別要求は、ユーザ名またはアカウント情報などのユーザ識別情報を含み得る。いくつかの態様では、認証サーバ 115 は、セッショントークンおよび一般的なアクセス規則 210 に基づいて、識別要求が有効であるかどうかを判断するように構成することができる。例えば、認証サーバ 115 は、セッショントークンに加えてアカウント情報を要求するように一般的なアクセス規則 210 により構成され得る。代替的に、認証サーバ 115 は、アカウント情報を必要とせずにアクセスを許可するように一般的なアクセス規則 210 により構成され得る。

【0133】

ステップ 901 の後、プロセス 900 はステップ 903 に進むことができる。ステップ 903 で、認証サーバ 115 は、受信タグ画像内の安全タグ 105 を識別することができ

10

20

30

40

50

る。開示される実施形態と一致して、認証サーバ115は、安全タグの画像の保存されたハッシュを使用して安全タグ105を識別するように構成され得る。保存されたハッシュは、知覚ハッシュ（例えば、pHash、aHash、dHashなど）にすることができる。図6に関して上記で説明したように、保存されたハッシュに対応する安全タグは、スタイルシートを使用して生成された可能性がある。いくつかの実施形態では、認証サーバ115は、個人システム120から受信したハッシュを保存するように構成され得る。認証サーバ115は、保存されたハッシュを安全タグ識別子に関連付けるように構成され得る。認証サーバ115は、スタイルシートまたはスタイルシートのプライベート部分を格納するように構成されていない場合がある。したがって、攻撃者が認証サーバ115へのアクセスを取得した場合、攻撃者はハッシュと安全タグ識別子へのアクセスのみを取得する。しかし、いくつかの実施形態では、認証サーバ115は、スタイルシートの公開部分を格納するように構成されてもよい。

10

【0134】

ステップ903では、開示された実施形態と一致して、認証サーバ115は、受信タグ画像の1つ以上のハッシュを生成することができる。1つ以上の生成ハッシュは、知覚ハッシュ（例えば、pHash、aHash、dHashなど）であり得る。いくつかの態様では、受信タグ画像はベクトルグラフィックス画像であり得る。様々な態様では、受信タグ画像のハッシュを生成することは、受信したベクトルグラフィックス画像の少なくとも一部をラスタ画像に変換することを含み得る。このラスタ画像は、あらかじめ決められた数のピクセルを持つことができる。いくつかの態様では、ピクセルの所定の数、64ピクセル以上であり得る。様々な態様において、ピクセルの所定の数、1,048,576ピクセル以下であり得る。

20

【0135】

ステップ903において、開示された実施形態と一致して、認証サーバ115は、受信タグ画像の生成された1つ以上のハッシュを既知の安全タグの画像の保存ハッシュと比較することにより、受信タグ画像内の安全タグ105を識別することができる。いくつかの実施形態では、この比較は、保存されたハッシュと生成されたハッシュとの間の差を決定することを含み得る。認証サーバ115は、保存されたハッシュと生成されたハッシュとの間の差がしきい値基準を満たすとき、保存されたハッシュに対応する安全タグとして安全タグ105を識別するように構成され得る。例えば、しきい値基準では、ハッシュが一致する必要がある。追加の例として、しきい値の基準では、ハッシュが類似している必要がある。例えば、いくつかの局面では、差異は、保存されたハッシュと生成されたハッシュとの間の距離であり得る。認証サーバ115は、同様にしきい値距離内のハッシュを識別するように構成され得る。いくつかの実施形態では、距離はハミング距離であり得る。

30

【0136】

いくつかの実施形態では、認証サーバ115は、損傷したタグまたは部分的に不明瞭なタグを識別するように構成することができる。例えば、認証サーバ115は、受信タグ画像の漸進的により小さいセグメントのハッシュを生成することにより、受信タグ画像内の安全タグ105を識別するように構成することができる。受信タグ画像のこれらの漸進的により小さなセグメントは、既知の安全タグの対応するセグメントのハッシュと比較することができる。これらの生成されたハッシュと既知の安全タグの対応するハッシュ間の一致度に基づいて、破損したタグまたは部分的に不明瞭なタグの画像全体のハッシュが保存されたタグと一致しない場合でも、破損したタグまたは部分的に不明瞭なタグを識別できるハッシュ。

40

【0137】

ステップ903では、開示された実施形態と一致して、認証サーバ115は、一致する保存されたハッシュのタグ識別子を決定することができる。タグ識別子を使用して、タグのデコード規則を取得できる。

【0138】

ステップ903の後、プロセス900はステップ905に進むことができる。ステップ

50

905で、認証システム115は、受信タグ画像およびデコード規則を使用してタグデータを生成することができる。いくつかの側面では、これらのデコード規則は、特定のスタイルシートを使用して生成されたタグに固有のものにすることができる。例えば、これらのデコード規則は、タグ内のタグデータの場所を識別し、タグ特徴のデフォルトの場所を指定し、タグ特徴オプションとタグデータ値との対応を指定し、比率を提供する（例：全体の直径の比率としてのドットの直径、幅タグの特徴とタグの特徴のオプションを識別するための、リムの厚さの比率などとしてのリム破損の）。

【0139】

ステップ905で、認証システム115は、デコード要求に応じてデコード規則を受信することができる。いくつかの態様では、デコード要求は、個人システム120または別のシステムに提供され得る。デコード要求は、ネットワーク130を使用して提供できる。デコード要求は、安全タグ105の識別子を含み得る。デコード要求は、認証キー（例えば、クライアント装置110から受信した認証キー）を含み得る。いくつかの態様では、復号規則は、個人システム120または別のシステムから取得することができる。

【0140】

いくつかの実施形態では、デコード規則は、安全タグ105のサブセットの復号化を可能にすることができる。デコード規則は、安全タグ105を生成するために使用されるスタイルシートの部分を含むか、それに基づくことができる。デコード規則は認証キーに対応できる。例えば、認証システム115は、デコード要求を含む認証キーに応じて異なるデコード規則を受信することができる。追加の例として、製造業者に関連付けられた認証キーに応じて、小売業者に関連付けられた認証キーに応じて異なる規則を提供できる。安全タグには同じ情報を含めることができるが、デコード規則の違いは、その情報の様々なサブセットを製造業者と小売業者が利用できることを意味する。

【0141】

いくつかの実施形態では、復号規則は、安全タグ105の反復復号を可能にすることができる。例えば、デコード規則には、第1のデコード規則と第2のデコード規則を含めることができる。第1の復号規則は、スタイルシートによって定義された安全タグの第1の部分またはスタイルシートによって定義されたタグ特徴の第1のサブセットのうちの少なくとも1つの復号を可能にすることができる。例えば、第1のデコード規則により、安全タグの参照部分の第1のタグデータのデコードが可能になる。第2のデコード規則は、安全タグの第2の部分またはタグ特徴の第2のサブセットの少なくとも1つの復号化を可能にすることができる。例えば、第2のデコード規則は、第1のタグを使用して復号化された安全タグの参照部分でエンコードされた第1のタグデータにより参照される安全タグの部分の第2のタグデータの復号化を可能にすることができる。参照部分でエンコードされた第1のタグデータがないと、第2のデコード規則を使用して第2のタグデータをデコードできない。したがって、第1のタグデータは、第1のデコード規則を使用して生成でき、第2のタグデータは、第1のタグデータと第2のデコード規則を使用して生成できる。

【0142】

いくつかの実施形態では、認証システム115は、スタイルシートを使用して生成されたタグの公開部分を復号化するための公開デコード規則を受け取ることができる。このような規則は、在庫管理単位番号（SKU）、ブランド名、有効期限、製品名などの一般的に重要な非機密情報のデコード方法を指定できる。

【0143】

ステップ905の後、プロセス900はステップ907に進むことができる。ステップ907において、認証サーバ115は、元のタグ識別に応答して、デコードされたタグデータをクライアントシステム110に提供するように構成され得る。いくつかの実施形態では、認証システム115は、タグデータに加えて、またはタグデータの代わりにタグ復号規則を提供するように構成することができる。これにより、クライアント装置は、認証サーバ115の代わりに、または認証サーバ115によって実行されたデコードを検証するために、タグデコードを実行できる。例えば、いくつかの実施形態では、認証サーバ1

10

20

30

40

50

15は、認証サーバ115によって格納された、または個人システム120から受信した安全タグ105の公開デコード規則をクライアント装置110に提供するように構成することができる。

【0144】

いくつかの実施形態では、認証サーバ115は、タグ識別要求を追跡するように構成することができる。例えば、認証サーバ115は、識別要求タイプ、場所、IPアドレス、時刻、クライアント装置識別情報、ユーザ識別情報、取引情報などを含む追跡情報を保存するように構成することができる。いくつかの実施形態では、認証サーバ115は、認証データベース205に追跡情報を格納するように構成することができる。様々な実施形態において、認証サーバ115は、この情報を公開データベース130（イーサリアムブロックチェーンなどの分散データベースとすることができる）に書き込む命令を提供するように構成することができる。例えば、認証サーバ115は、オラクル510を使用して安全タグ105の識別要求の場所をバンドルアカウント520に書き込むように構成することができる。いくつかの実施形態では、認証サーバ115は、要求に関連付けられた1つまたは複数のアイデンティティまたは提供されるAPIキーに応じて、クライアント装置110からの要求に応答して追跡情報の少なくとも一部を提供するように構成できる要求。いくつかの実施形態では、認証サーバ115は、クライアント装置110が追跡情報を取得するために使用できる公開データベース130内のアドレスを提供するように構成することができる。

【0145】

図10は、開示される実施形態と一致する、多重解像度タグ識別の例示的なプロセス1000を示すフローチャートを示す。以下に認証サーバ115によって実行されるものとして説明するが、プロセス1000は、いくつかの実施形態では、個人システム120、クライアントシステム110、または別のシステムによって実行することができる。プロセス1000は、安全タグ105の画像のハッシュを生成するステップ、生成されたハッシュに基づいて第1の安全タグを選択するステップ、安全タグ105の所定のセグメントに対応する第2のハッシュを生成するステップ、および第1から安全タグを選択するステップを含み得る。安全タグ105に一致する安全タグとして安全タグ。このようにして、プロセス1000は、画像内の安全タグ105のハッシュが複数の保存されたハッシュと一致する場合、認証サーバ115が画像内の安全タグ105を識別できるようにすることができる。

【0146】

開始後、プロセス1000はステップ1001に進むことができる。ステップ1001において、認証サーバ115は、受信タグ画像に描かれた安全タグ（例えば、安全タグ105）のハッシュを生成することができる。ハッシュは知覚ハッシュにすることができる。

【0147】

ステップ1001の後、プロセス1000はステップ1003に進むことができる。ステップ1003で、認証サーバ115は、生成されたハッシュと第1の安全タグの保存されたハッシュとの間の差を使用して第1の安全タグを選択することができる。いくつかの実施形態では、差は、ハミング距離などのメトリックに応じた距離であり得る。いくつかの態様では、選択された第1の安全タグの保存されたハッシュは、受信タグ画像に描かれた安全タグの生成されたハッシュとしきい値未満だけ異なる可能性がある。

【0148】

ステップ1003の後、プロセス1000はステップ1005に進むことができる。ステップ1005で、認証サーバ115は、受信タグ画像に描かれた安全タグ105の所定のセグメントの第2のハッシュを生成することができる。例えば、認証サーバ115は、安全タグの1つ以上の象限のハッシュを生成するように構成され得る。

【0149】

認証サーバ115は、開示された実施形態と一致して、クライアント装置110に第2の画像を求めるように構成することができる。例えば、認証サーバ115は、安全タグ1

10

20

30

40

50

05の所定のセグメントの周りにバンディングボックスまたは同様の表示を表示する命令を提供するように構成され得る。この指示にตอบสนองして、ユーザはクライアント装置と対話して、安全タグ105の所定のセグメントを表す第2の画像を取得することができる。

【0150】

認証サーバ115は、クライアント装置110からこの第2の画像を受信するように構成され得る。第1の受信画像は、安全タグ105の少なくとも一部を第1の詳細レベルで全体として示すことができるが、第2の受信画像は、第1の詳細レベルよりも大きい第2の詳細レベルで安全タグ105の所定のセグメントを示すことができる。例えば、第1および第2の画像は同じ数のピクセルを含み得るが、クライアント装置110のカメラは、第1の画像を撮るときよりも第2の画像を撮るときの安全タグ105の所定のセグメントにより近くなり得る。

10

【0151】

ステップ1005の後、プロセス1000はステップ1007に進むことができる。ステップ1007で、認証サーバ115は、以前に選択された第1の安全タグから特定の安全タグを選択するように構成され得る。認証サーバ115は、ステップ1005で生成された第2のハッシュと第1の安全タグの画像の所定部分の記憶された第2のハッシュとの差を使用して一致する安全タグの選択を絞り込むように構成することができる。例えば、ステップ1001で生成された第1ハッシュは、第1安全タグの保存済みハッシュに広く一致するが、ステップ1005で生成された第2ハッシュは、保存された第2ハッシュの1つのみに一致する（例えば、ステップ1005で生成された第2ハッシュのみ格納されている第2のハッシュの1つが、しきい値よりも小さい場合がある）。格納された2つ以上の第2ハッシュがステップ1005で生成された第2ハッシュと十分に一致する場合、認証サーバ115は、セキュアハッシュ105の別の所定のセグメント（例えば、ステップ1005、または安全タグ105の別の象限で選択された象限のサブセグメント）とこの比較プロセスを繰り返すように構成され得る。

20

【0152】

図11は、タグが変更された多重解像度タグ識別の例示的なプロセス1100を示すフローチャートを示している。以下に認証サーバ115によって実行されるものとして説明するが、プロセス1100は、いくつかの実施形態では、個人システム120、クライアントシステム110、または別のシステムによって実行することができる。開示された実施形態と一致して、プロセス1100は、受信タグ画像に描かれた安全タグのハッシュを安全タグ画像の保存されたハッシュと比較することを含み得る。受信タグ画像に示された安全タグのハッシュが、保存されたハッシュのいずれかと所定の差の範囲内で一致しない場合、認証サーバ115は、図に示された安全タグの所定のセグメントのハッシュ安全タグの対応するセグメントの保存されたハッシュにタグ画像を受信した。認証サーバ115は、この第2の比較に基づいて潜在的に一致する安全タグを識別するように構成することができる。認証サーバ115は、受信タグ画像に示された安全タグの別の所定のセグメントのハッシュを、識別された潜在的に一致する安全タグの対応するセグメントの保存されたハッシュと比較するように構成できる。これらの追加のハッシュが所定の差の範囲内で一致する場合、認証サーバ115は、受信タグ画像に描かれた安全タグとして一致する安全タグの識別を確認するように構成できる。したがって、プロセス110によれば、認証サーバ115は、受信した画像に描かれた安全タグの部分に一致するハッシュについて認証データベース205を検索するように構成することができる。このようにして、認証サーバ115は、不完全または破損した安全タグと一致するように構成できる。

30

40

【0153】

開始後、プロセス1100はステップ1101に進むことができる。ステップ1101で、認証サーバ115は、安全タグの最初に生成されたハッシュと最初に保存されたハッシュとの差がしきい値基準を満たさないと判断することができる。第1の生成されたハッシュは、受信した画像に描かれた安全タグ（例えば、安全タグ105）のものであり得る。最初に保存されたハッシュは、認証データベース205の安全タグである場合がある。

50

差は、メトリック（ハミング距離など）に従って計算された距離である。

【0154】

ステップ1101の後、プロセス1100はステップ1103に進むことができる。ステップ1103において、認証サーバ115は、受信画像に描かれた安全タグの生成された第2のハッシュ（例えば、安全タグ105）と格納された第2のハッシュとの比較に基づいて、認証データベース205内の安全タグの1つを選択するように構成できるハッシュ。生成された第2のハッシュは、受信した画像（または同じ安全タグの別の画像）に描かれた安全タグのセグメントのハッシュにすることができる。格納された第2のハッシュは、潜在的に一致する安全タグのセグメントの認証データベース205に保存されたハッシュであり得る。潜在的に一致する安全タグのセグメントは、受信した画像に描かれている安全タグのセグメントと同じである場合がある。

10

【0155】

ステップ1103の後、プロセス1100はステップ1105に進むことができる。ステップ1105において、認証サーバ115は、最初に受信した画像に描かれた安全タグの第2セグメントのハッシュを生成するように構成され得る。いくつかの実施形態では、認証サーバ115は、クライアント装置110に別の画像を促すように構成することができる。例えば、認証サーバ115は、安全タグ105のセグメントの周りにバンディングボックスまたは同様の表示を表示する命令を提供するように構成することができる。この指示に回答して、ユーザは、クライアント装置110と対話して、安全タグ105の所望のセグメントを示す第2の画像を取得することができる。

20

【0156】

いくつかの実施形態では、第2のセグメントは、第1のセグメントとは異なり得る。例えば、第1のセグメントが安全タグの右上象限である場合、第2のセグメントは安全タグの左上象限にすることができる。様々な実施形態において、第2のセグメントは第1のセグメントと重なり合うことができる。例えば、第2のセグメントは、完全にまたは部分的に第1のセグメントに含まれる。例えば、第2のセグメントは、第1のセグメントの左下の象限にすることができる。

【0157】

ステップ1105の後、プロセス1100はステップ1107に進むことができる。ステップ1107で、認証サーバ115は、ステップ1103で識別された潜在的に一致する安全タグを検証するように構成することができる。認証サーバ115は、生成された第3のハッシュと格納された第3のハッシュとの間の差を使用して、潜在的に一致する安全タグを検証するように構成され得る。格納された第3のハッシュは、潜在的に一致する安全タグのセグメントにすることができる。セグメントは、第3のハッシュの生成に使用されるセグメントに対応できる。認証サーバ115は、第3の生成されたハッシュとこの保存されたハッシュとの間の差がしきい値基準を満たすと判断することができる。差は、メトリック（ハミング距離など）に従って計算された距離である。

30

【0158】

開示される実施形態と一致して、プロセス1000および1100は、（i）セグメント距離を使用して全体距離を決定すること、および／または（ii）セグメント距離のカウントがしきい値基準を満たすことを含み得る。例えば、認証サーバ115は、安全タグ105のセグメントの画像の複数のハッシュを、安全タグのセグメントの対応する保存されたハッシュと比較することができる。この比較は、安全タグ105のセグメントの画像の各ハッシュと安全タグのセグメントの対応する保存されたハッシュとの間の距離を決定することを含み得る。比較には、平均距離など、これらの個々の距離に基づいて全体の距離を決定することが含まれる。比較はまた、しきい値基準を満たす（例えば、特定の最大距離内に入る）個々の距離のカウントを決定することを含み得る。いくつかの実施形態では、認証サーバ115は、比較されるハッシュの数、しきい値基準を満たす個々の距離のカウント、または個々の距離または全体の距離の少なくとも1つを使用して信頼値を決定するように構成できる。

40

50

【0159】

図12は、多重解像度タグ識別を実行するための論理データベース構造の概略図を示している。いくつかの実施形態では、認証データベース205は、図12に示されるスキーマで構成され得る。認証データベース1205は、安全タグを使用して生成されたハッシュを格納するように構成できる。これらのハッシュは、図6に関して前述したように、タグ作成プロセス中に個人システム120によって生成できる。いくつかの態様では、認証データベース205は、データ構造1201に第1の安全タグに関するハッシュを格納するように構成することができる。認証データベース205は、複数の詳細レベルに対応するハッシュを保存するように構成することができる。いくつかの態様では、タグレベル1230は安全タグ全体にわたって計算されたハッシュを含み得る。この詳細レベルでは、データのエンコードに使用される小さなタグ特徴オプションが識別できない場合がある（スキャナの解像度または画像処理の損失のため）。したがって、タグ全体を表す画像上で計算されたハッシュは、認証データベースに格納されているハッシュのいずれとも一致しないか、複数のハッシュと一致する場合がある。様々な態様において、タグレベル1240は、タグ全体のセグメント（例えば、安全タグ全体の象限）にわたって計算されたハッシュを含み得る。この詳細レベルでは、データのエンコードに使用される小さなタグ特徴オプションが識別可能である。さらに、タグの1つのセグメントへの損傷は、タグの別のセグメントに影響しない場合がある。したがって、破損したタグ全体で計算されたハッシュは一致しない場合があるが（例えば、一致しないハッシュ1203）、タグの破損していないセグメントで計算されたハッシュは一致する場合がある（例えば、一致したハッシュ1211）。様々な態様では、タグレベル1250は、タグ全体のサブセグメント（例えば、安全タグ全体の象限の象限）で計算されたハッシュを含み得る。他のタグの追加のセグメントが一致する場合があるため（例えば、一致するハッシュ1213）、認証サーバ115は、追加のハッシュ（例えば、一致するハッシュ1221、一致しないハッシュ1223）をチェックするように構成できる。これらの追加のハッシュをチェックすることにより、認証サーバ115は、第1のタグハッシュ構造1201のハッシュに対応する安全タグが受信画像に描かれた安全タグであることを確認できる。いくつかの実施形態では、認証サーバ115は、チェックされたハッシュの数、類似性基準に従って一致するハッシュの数、および一致の程度に基づいてスコアを生成するように構成され得る。このスコアを使用して、クライアント装置110から受信した画像に描かれている安全タグと一致する安全タグを識別することができる。当業者によって理解されるように、図示されたツリー構造は限定することを意図していない。他のデータ構造を使用して、ハッシュや関連する情報を保存することができる。例えば、保存されたハッシュにキー付けされ、安全タグの識別子を含む連想配列やマップなどである。

【0160】

図13は、タグの信頼性を評価するための例示的なユーザインターフェースを示している。読み取り装置には、タグの信頼性の決定されたレベルを表示できるアプリを含めることができる。本物は、本明細書に開示されるシステムおよび方法を使用して決定され得る。安全タグがスキャンされると、スキャンされたタグ画像が認証サーバに送信される。タグの信頼性は、図10～図12で説明したハッシュ方法を使用して判断できる。タグが認証されると、スキャン数、レポートなど、タグに関する情報が返される。特定の側面では、認証サーバは、ハッシュプロセスに基づいて信頼性の確率を決定できる。他の側面では、認証サーバはブロックチェーンに保存されたタグ履歴に基づいて安全タグの信頼性を判断できる。

【0161】

一部の実施形態では、タグの信頼性のレベルを決定するアプリは、「認証スコア」を返すことができる。特定の側面では、完全なスコア1301を返すことができる。これは、例えば、安全タグが良好な状態にあり、読み取り装置が安全タグの適切なスキャンを取得できる場合に発生する可能性がある。さらに、安全タグが以前にスキャンされていないと認証サーバが判断した場合、またはブロックチェーン内のタグ履歴が製品が偽物ではない

10

20

30

40

50

ことを示している場合、完全なスコア1301を返すことができる。他の態様では、低スコア1303を返すことができる。これは、安全タグの状態が悪い場合、または読み取り装置が安全タグの適切なスキャンを取得できない場合に発生する可能性がある。さらに、同じタグが偽造の可能性があるとして識別されたと認証サーバが判断した場合、低スコア1303を返すことができる。例えば、タグが複数の場所で何度もスキャンされた場合、低いスコア1303が認証スコアとして返される。別の例では、タグが偽造として報告されている場合、低スコア1303が認証スコアとして返される。

【0162】

一部の実施形態では、ユーザは、図13に示される例示的なユーザインターフェースを介してタグを報告することができる。例えば、タグが何度もスキャンされており、一意ではないことを示す低スコア1303が返された場合、ユーザはタグを報告して、タグの所有者が偽造の可能性に気付くことができる。他の実施形態では、ユーザはアプリを介して製品情報を見ることができる。例えば、高スコア1301が返された場合、ユーザは製品情報を確認できる。

【0163】

図14は、タグ特徴選択をデコードするための例示的なプロセスを示している。以下に認証サーバ115によって実行されるものとして説明するが、プロセス1400は、いくつかの実施形態では、個人システム120、クライアントシステム110、または別のシステムによって実行することができる。プロセス1400には、画像を受信するステップ、デコード規則と数値シードを受信するステップ、既知のスタイルシートおよび／または既知のデータ値を使用して可能な機能を識別するステップ、受信した画像に基づいて実際の機能を識別するステップ、データ値を再構築するステップ、およびデータ値を復号化するステップを含めることができる。このようにして、認証サーバ115は、クライアント装置110と個人システム120の両方から受信した情報を使用して、安全タグに格納されたデータをデコードするように構成できる。一部の実施形態では、認証サーバ115は、画像、デコード規則、数値シードを保存しない。このようにして、システム100の機能の配置は、認証サーバ115を危険にさらす攻撃者が認証サーバ115によって管理される安全タグのコンテンツをデコードできないことを保証する。

【0164】

開始後、プロセス1400はステップ1401に進むことができる。ステップ1401では、画像を受信するように認証サーバ115を構成することができる。画像は、ラスタ画像またはベクトルグラフィックス画像である。画像は、クライアント装置110または別のシステムから受信することができる。認証サーバ115は、画像がラスタ画像である場合、画像をベクトルグラフィックス画像に変換するように構成することができる。

【0165】

ステップ1401の後、プロセス1400はステップ1403に進むことができる。ステップ1401で、認証サーバ115はデコード命令を受信することができる。いくつかの実施形態では、認証サーバ115は、個人システム120からデコード命令を受信するように構成され得る。デコード命令は、認証サーバ115から個人システム120への要求に応じて受信することができる。要求にはアプリケーションキーを含めることができ、受信したデコード命令は提供されたアプリケーションキーに依存する。

【0166】

いくつかの実施形態では、個人システム120は、安全タグを生成するために使用されるスタイルシートおよび数値シードを、ベクトルグラフィックス画像に存在するタグ特徴とタグデータ値との間の対応を直接記述する復号化命令に変換するように構成され得る。例えば、デコード命令は、タグ特徴オプションのセットと、これらのタグ特徴オプションの値からタグデータの項目の値へのマッピングを指定できる。そのような実施形態では、個人システム120は、スタイルシートのプライベート部分または数値シードを認証サーバ115に提供しなくてもよい。いくつかの実施形態において、認証サーバ115は、スタイルシートのプライベート部分の少なくとも一部を、安全タグの安全タグレイアウトを生

10

20

30

40

50

成するために使用される数値シードとともにタグを生成するために使用するように構成できる。そのような実施形態では、認証サーバ115は、ベクトルグラフィック画像に存在するタグ特徴とタグデータ値との間の対応を生成するように構成することができる。

【0167】

ステップ1403の後、プロセス1400はステップ1405に進むことができる。ステップ1405で、認証サーバ115は、復号化命令および既知のタグデータ値を使用して可能な特徴を識別することができる。例えば、認証サーバ115は、復号化命令に記載されているタグ特徴を見つけるように構成することができる。場合によっては、タグ特徴の特定は、既知のタグデータ値に依存する。例えば、安全タグは、8ビットの2進数を安全タグのドットのサイズにエンコードできる。デコード命令は、ドットのサイズと特定の8ビット2進数の値との対応を示すことができる。ただし、デコード命令では、安全タグのどの部分に関連するドットが含まれているかを指定できない場合がある。安全タグの別の部分は、タグデータの特定の値をエンコードするタグ特徴オプション（ドットサイズ）を持つタグ特徴（ドット）をエンコードするタグの部分の識別するために使用可能なリファレンスを含み得る。

10

【0168】

ステップ1405の後、プロセス1400はステップ1407に進むことができる。ステップ1407で、認証サーバ115は、受信した画像に基づいて実際のタグ特徴オプション値を識別することができる。いくつかの実施形態では、画像ファイルがベクトルグラフィックファイルである場合、認証サーバ115は、ベクトルグラフィックファイルから機能オプション値を読み取ることができる。必要に応じて、認証サーバ115は最初に受信した画像をベクトルグラフィックファイルに変換できる。あるいは、認証サーバ115は、OpenCVなどによって提供される機能を使用して、ラスト画像からタグ特徴オプション値（例えば、相対的なドットサイズ、ある位置における特徴の有無）を直接決定することができる。

20

【0169】

ステップ1407の後、プロセス1400はステップ1409に進むことができる。ステップ1409で、認証サーバ115は、実際の特徴値に基づいてタグデータ値を再構築することができる。例えば、関連するタグ特徴のタグ特徴オプションの値を決定した場合、認証サーバ115は、個人システム120から受信したデコード規則に従ってこれらのタグ特徴オプション値をタグデータに変換するように構成できる。

30

【0170】

ステップ1409の後、プロセス1400は、オプションのステップ1411に進むことができる。オプションのステップ1411では、認証サーバ115はタグデータを解読することができる。いくつかの実施形態では、認証サーバ115は、安全タグにエンコードされた鍵素材を使用して暗号化タグデータを解読するように構成することができる。

【0171】

図15は、文脈情報を使用する例示的な認証プロセスを示している。個人システム120および認証サーバ115によって実行されるように以下で説明するが、プロセス1500は、いくつかの実施形態では、個人システム120または認証サーバ115、またはクライアントシステム110または別のシステムによって完全に実行できる。プロセス1500によれば、個人システム120は、文脈データを安全タグにエンコードすることができる。次に、認証サーバ115は、識別要求に応答する際にエンコードされたデータに関する文脈条件を実施することができる。

40

【0172】

開始後、プロセス1500はステップ1501に進むことができる。ステップ1501で、個人システム120はタグデータを受信することができる。前述のように、このタグデータは、別のシステム、個人システム120のメモリ、またはユーザから受信できる。

【0173】

ステップ1501の後、プロセス1500はステップ1503に進むことができ、ステ

50

ステップ1503では、個人システム120は文脈情報を受信することができる。いくつかの実施形態では、この文脈情報は、認証資格情報（例えば、パスワード、認証トークンなど）、生体認証識別子（例えば、指紋、声紋など）、音声ファイル、タグ識別子（例えば、別の安全タグのタグ識別子）、または画像の知覚ハッシュの少なくとも1つを含み得る。例えば、項目にラベルを付けるために安全タグを作成でき（例えば、ユーザIDカード、肉、ワインのボトル、個人が所有する項目）、画像に項目の一部（例えば、身分証明書の身分証明書写真、肉の粒、ワインのボトルのラベル、項目を所有する個人の顔）を描写できる。

【0174】

ステップ1503の後、プロセス1500はステップ1505に進むことができる。ステップ1505で、個人システム120は、タグデータおよび文脈情報を安全タグにエンコードすることができる。このアプリケーションで説明されているように、タグデータと文脈情報は、タグ特徴オプションの選択として安全タグにエンコードでき、利用可能なタグ特徴オプションは数値シードに依存する。

【0175】

ステップ1505の後、プロセス1500はステップ1507に進むことができる。ステップ1505で、認証システム115は、安全タグに関する識別要求を受信することができる。このアプリケーションで説明されているように、認証サーバは、安全タグの1つ以上のハッシュを使用してタグを識別するように構成できる。認証サーバ115は、個人システム120からデコード命令を要求するように構成され得る。認証サーバ115は、復号化命令を使用して、格納された文脈情報を復号化するように構成され得る。

【0176】

ステップ1507の後、プロセス1500はステップ1509に進むことができる。ステップ1509で、認証システム115は追加の文脈情報を受け取ることができる。この追加の文脈情報は、クライアント装置110または別の装置から受信できる。追加の文脈情報は、認証システム115によって提供された要求に応じて受信できる。例えば、認証システム115は、クライアント装置110のユーザに表示するためのクライアント装置110に指示を提供することができる（例えば、クライアント装置110のユーザインターフェースに「所有者の顔の写真を撮るラバタグを解除する」というテキストを表示する指示）。

【0177】

ステップ1509の後、プロセス1500はステップ1511に進むことができる。ステップ1511で、認証システム115は、追加の文脈情報を使用して識別要求を認証することができる。いくつかの実施形態では、認証システム115は、受信した追加の文脈情報およびデコードされた文脈情報が類似性基準を満たすことを決定するように構成され得る。例えば、認証システム115は、デコードされた文脈情報を受信した文脈情報と比較するように構成され得る。文脈情報が画像の知覚ハッシュ（例えば、別のタグ、またはラベル項目の所有者、またはラベル付き項目の一部の知覚ハッシュ）である場合、認証システム115は、受信した追加の文脈情報とデコードされた文脈情報との違いを判定するよう構成され得る。いくつかの側面では、この距離はハミング距離（または同様のメトリック）になる。

【0178】

ステップ1511の後、プロセス1500はステップ1513に進むことができる。ステップ1513で、認証システム115は、ステップ1511で実行された認証の結果に基づいて指示を提供することができる。追加の文脈情報およびデコードされた文脈情報が類似性基準を満たさない場合、認証システム115は、クライアント装置110に認証失敗の表示を提供することができる。追加の文脈情報およびデコードされた文脈情報が類似性基準を満たす場合、認証システム115は、クライアント装置110に認証成功の表示を提供することができる。いくつかの実施形態では、成功した認証の表示は、ステップ1501で受信したタグデータの少なくともいくつかを含み得る。様々な実施形態において

10

20

30

40

50

、成功した認証の表示は、ステップ1501で受信したタグデータの少なくともいくつかに対するデコード命令を含み得る。様々な実施形態において、成功した認証の表示は、分散データベースから検索されたステータス情報を含み得る。このステータス情報は、Oracleを使用して分散データベースから取得できる（例えば、分散データベースはEthereumブロックチェーンになる）。

【0179】

図16Aは、対とシーケンスの安全タグを示している。安全タグは、セキュリティと信頼性のレベルを高めるために他のタグとの関係を持つことができる。例えば、第1の安全タグ1601と第2の安全タグ1603を対にすることができる。次いで、第1の安全タグ1601および第2の安全タグ1603の両方が、製品についての情報を取得するため、または製品の所有権を移転するために、ユーザについてスキャンされることを要求され得る。例えば、第1の安全タグ1601を生成して、一対の靴の一方の靴に配置し、第2の安全タグ1603を生成して、同じ対の靴の第2のショーに配置することができる。この例では、両方のタグは一意であり、ペアの特定の靴を識別するが、靴のペアを認証したり所有権を譲渡したりするには、両方のタグを読み取る必要がある。

【0180】

いくつかの実施形態では、ペア化されたタグをさらにシーケンス化して、シーケンス化されたタグ1605を作成することができる。シーケンスタグ1605は、第1の安全タグ1601と第2の安全タグ1603の組み合わせであり、ペアのタグに関する情報を提供する。特定の態様では、順序付けられたタグ1605は、所有権の購入または移転の前にスキャンできる唯一のタグであり得る。これらの態様では、シーケンスタグ1605は、製品の認証と製品に関する基本情報を提供できる。シーケンスタグ1605は、どのペアタグが存在する必要があるかを示すこともできる。前の例として、靴のペアにペアのタグが含まれている場合、タグをシーケンス化して、シーケンス化されたタグ1605を作成できる。順序付けられたタグ1605を靴箱の外側に配置して、箱内の靴に関する情報を提供することができる。開いたら、第1の安全タグ1601と第2の安全タグ1603をスキャンして、正しい靴が箱に入っていることを確認することができる。

【0181】

図16Bは、近接フィンガプリンティングを使用したIDカード1607を示している。他の安全タグとの関係を持つことに加えて、安全タグ1611は、顔の指紋1609などの外部画像との関係を持つことができる。身分証明書1607は、安全タグ1611を顔の指紋1609と組み合わせることにより、追加のレベルの信頼性を有することができる。近接フィンガプリンティングは、安全タグ1609に近接している対象物を使用して、タグをさらに認証する。いくつかの実施形態では、これにより、安全タグがコピーされる状況が他のどこかで認証されるのを防ぐことができる。例えば、安全タグ1611がIDカード1607からコピーされた場合、顔の指紋1609がないと検証されない。その結果、IDカード1607の形式で組み合わせられた保護されたIDが得られる。いくつかの実施形態では、安全タグ1611は顔の指紋1609とペアにされ、認証のために安全タグ1611と顔の指紋1609の両方が一緒に提示されなければならないことを意味する。

【0182】

いくつかの実施形態では、IDカード1607を使用して、適切な状況で識別の証明を提示することができる。例えば、警察官は市民が身分証明書1607の提示を要求して、その人が遭遇地点にいると主張する人物であることを確認することができる。他の実施形態では、アルコールを提供する施設は、人が偽の運転免許証または年齢証明のカードを使用していないことを保証するために、人に身分証明書1607の提示を要求することができる。

【0183】

図22に、サプライチェーン全体のペアタグを示す。製造業者が製品を製造するとき、第1の安全タグ2201と第2の安全タグ2203を作成し、安全タグをペアリングし、

10

20

30

40

50

製品に安全タグを貼り付けることができる。ペアになったタグは、サプライチェーンプロセス全体でブロックチェーンでシーケンス化および更新できる。例えば、シーケンスされたタグには、ペア製品自体に関する情報 2205、ペア製品が 2207 に出荷された特定のパレット、ペア製品が 2209 に送信された全体の出荷、および小売業者 2211 に関する情報を含めることができる。サプライチェーンプロセスの各段階で、ブロックチェーンはペア製品に関する情報で更新される。顧客が小売店に行って製品を購入すると、シーケンスされたタグの所有権検証 2213 を実行できる。

【0184】

いくつかの実施形態では、小売業者制御 2215 および閉じた消費者ループ 2217 は、異なるレベルの情報にアクセスすることができる。例えば、閉じた消費者ループ 2215 は、ペアになったタグ自体に関する情報のみにアクセスできる。これには、製品自体とメーカに関する情報が含まれる場合がある。クローズド消費者ループ 2215 により、消費者はペアのタグの信頼性を検証できる。この例では、小売業者の制御 2215 には、サプライチェーンプロセス全体に関する情報にアクセスする機能を含めることができる。小売業者制御 2215 は、個々の包装情報 2205、パレット情報 2207、出荷情報 2209、および小売業者情報 2211 へのアクセスを含み得る。小売業者管理 2215 は通常、ペアのタグ自体へのアクセスを含まない。小売業者の制御 2215 により、小売業者は出荷情報を追跡し、物流を管理できる。

【0185】

図 17 は、例示的な 2 部構成のラベルを示している。二部ラベルは、ベースタグ 1710 とオーバーレイ 1720 を含み得る。ベースタグ 1710 は、潜在的な第 1 のセキュアデータ機能オプションの選択として第 1 のタグデータをエンコードする第 1 の安全タグでラベル付けされた基板を含み得る。オーバーレイ 1720 は、ベースタグ 1710 を含む基板に取り外し可能に接着することができる。オーバーレイ 1720 は、透明部分 1721 および不透明部分 1723 を含み得る。透明部分 1721 および不透明部分 1723 の両方は、第 1 の安全タグと位置合わせすることができる。ベースタグ 1710 上にある第 1 の安全タグは、整列した透明部分 1721 の影響を受けないことがある。位置合わせされた不透明部分 1723 およびベースタグ 1710 上に位置する第 1 の安全タグは、潜在的な第 2 の安全タグ特徴オプションの選択として第 2 のタグデータをエンコードすることができる。

【0186】

いくつかの実施形態では、ベースタグ 1710 上の潜在的な第 1 の安全タグ特徴オプションは、不透明部分 1723 およびベースタグ 1710 によって作成される潜在的な第 2 の安全タグ特徴オプションとは異なる。他の実施形態では、位置合わせされた不透明部分 1723 は、ベースタグ 1710 上の選択された第 1 の安全タグ特徴を覆い隠すことができる。さらに他の実施形態では、位置合わせされた不透明部分 1723 は、ベースタグ 1710 上の潜在的な第 1 の安全タグ特徴オプションを選択することができる。さらに他の実施形態では、ベースタグ 1710 上の潜在的な第 1 の安全タグ特徴オプションは、第 1 の安全タグレイアウトによって指定される位置におけるタグ特徴の有無を含み得る。これらの実施形態では、位置合わせされた不透明部分 1723 によって作成される潜在的な第 2 の安全タグ特徴オプションは、第 2 の安全タグによって指定される位置でのタグ特徴の有無を含み得る。

【0187】

図 17 に示す 2 部ラベルは、第 1 のタグデータ、第 1 の数値シード、および第 1 のスタイルシートを使用して、潜在的な第 1 の安全タグ特徴オプションの選択として第 1 のタグデータをエンコードする第 1 の安全タグを最初に生成することで生成できる。次に、この方法は、第 2 のタグデータ、第 2 数値シード、および第 2 スタイルシートを使用して、潜在的な第 2 安全タグ特徴オプションの選択として第 2 のタグデータをエンコードする第 2 安全タグを生成する。次いで、この方法は、第 1 の安全タグと第 2 の安全タグとの間の差分画像を決定し、基材に第 1 の安全タグでラベル付けしてベースタグ 1710 を作成する

。次いで、この方法は、オーバーレイ 1720 をベースタグ 1710 に取り外し可能に付着させ、オーバーレイ 1720 は、差分画像でラベル付けされ、第 1 の安全タグと位置合わせされる。

【0188】

いくつかの実施形態では、オーバーレイ 1720 は、第 2 の安全タグに存在しない不透明部分 1723 により、ベースタグ 1710 上に位置する第 1 の安全タグの部分を覆い隠す。他の実施形態では、オーバーレイ 1720 は、第 1 の安全タグに存在しない第 2 の安全タグの部分を示している。さらに他の実施形態では、オーバーレイ 1720 は、透明部分 1721 を介してベースタグ 1710 上に位置する第 1 の安全タグに存在する第 2 の安全タグの部分を送信する。さらに他の実施形態では、第 1 の安全タグを生成するために使用される第 1 のスタイルシートは、第 2 の安全タグを生成するために使用される第 2 のスタイルシートと異なってもよい。さらに他の実施形態では、ベースタグ 1710 がラベル付けされ、オーバーレイ 1720 が接着される基板は、消費財を含み得る。

【0189】

例えば、ラベル付きの 2 つの部分は、製品の追加の認証とセキュリティに使用できる。販売されているボックスの外側に 2 部ラベルを配置できる。この 2 部ラベルは、ベースタグ 1710 とオーバーレイ 1720 を含んでいる。オーバーレイ 1720 は、透明部分 1721 と不透明部分 1723 の両方を含むため、タグはベースタグ 1710 とは異なる独特の外観を有する。この例では、顧客または小売業者は、オーバーレイ 1720 によって作成された第 2 のタグをスキャンして、製品に関する特定の情報を明らかにできる。製品の購入および／または所有権の譲渡後、オーバーレイ 1720 を削除してベースタグ 1710 を表示できる。現在の所有者は、ベースタグ 1710 をスキャンして、オーバーレイ 1720 とベースタグ 1710 の組み合わせによって提供される情報とは完全に異なる情報を明らかにすることができる。2 つの部分からなるラベルは、安全タグ自体の複雑さを増すことなく、セキュリティの追加レイヤを追加する。

【0190】

図 18 は、安全タグを使用して文書を提供するための例示的な方法 1800 のフローチャートである。方法 1800 は、ステップ 1801 で始まり、ここで、方法は、第 1 の安全タグ 1813 を文書 1811 に関連付ける。第 1 の安全タグ 1813 を生成し、文書 1811 とペアにすることができる。加えて、第 1 の安全タグ 1813 は、潜在的な機能オプションの選択を使用してエンコードされた文書 1811 の識別子を有する。いくつかの実施形態では、文書 1811 の識別子は文書 1811 のハッシュを含み得る。他の実施形態では、文書 1811 はブロックチェーンに暗号化される。この方法は、文書 1811 にアクセスするための要求を第 1 の装置 1821 から受信することができる。第 1 の装置 1821 は、モバイル装置（例えば、タブレット、スマートフォンなど）、デスクトップコンピュータ、ラップトップ、サーバ、ウェアラブル装置（眼鏡、時計など）、および／または装置専用ハードウェア装置であり得る。文書 1811 へのアクセスの要求に続いて、方法 1800 はステップ 1803 に移動する。

【0191】

ステップ 1803 で、この方法は、表示のために第 1 のユーザ装置 1821 を介して第 1 の安全タグ 1811 を提供する。ステップ 1805 で、この方法は、安全タグ画像を含む第 2 の装置 1831 を介して要求の確認を受け取ることができる。第 2 の装置 1831 は、モバイル装置（例えば、タブレット、スマートフォンなど）、デスクトップコンピュータ、ラップトップ、サーバ、ウェアラブル装置（眼鏡、時計など）、および／または装置専用ハードウェア装置であり得る。次いで、この方法は、第 1 の安全タグ画像 1813 を第 2 の装置 1831 から受信した安全タグ画像と比較することができる。比較により、第 1 のセキュア画像 1813 と第 2 の装置 1831 から受信した安全タグ画像との一致が明らかになった場合、方法 1800 はステップ 1807 に移動する。

【0192】

ステップ 1807 で、この方法は、表示のために文書 1811 を第 1 の装置 1821 に

提供する。いくつかの実施形態では、文書 1811 に安全タグで透かしを入れて、透かし入り文書 1843 を作成することができる。透かし入り文書 1843 は、新しい安全タグを持つことができるか、第 1 の安全タグ 1813 で透かしを入れることができる。他の実施形態では、第 1 の装置 1821 は、許可されたユーザ装置 1841 になることができる。いくつかの実施形態では、許可されたユーザ装置 1841 は、所定の期間、透かし入り文書 1843 にアクセスすることができる。所定の期間が終了すると、許可されたユーザ装置 1841 は、透かし入り文書 1843 を見るための許可を失う。他の実施形態では、透かし入り文書 1843 は、既読としてマークされた後、どの装置からもアクセスできない。さらに他の実施形態では、許可されたユーザ装置 1841 が文書に既読のマークを付けた後に、透かし入り文書 1843 を第 2 の許可されたユーザ装置によって読み取ることができる。

10

【0193】

いくつかの実施形態では、第 1 の安全タグ 1813 と第 2 のユーザ装置 1831 から受信した安全タグ画像とを比較することは、第 1 の安全タグ 1813 の知覚ハッシュを生成することと、第 2 のユーザ装置 1831 から受信した安全タグ画像の知覚ハッシュを生成することと、決定を含み得る格納された知覚ハッシュと生成された知覚ハッシュとの差がしきい値基準を満たすと判定することと、を含み得る。他の実施形態では、第 1 の安全タグ 1813 と第 2 のユーザ装置 1831 から受信した安全タグ画像を比較することは、第 2 のユーザ装置 1831 から受信した安全タグ画像の知覚ハッシュを生成することと、生成された知覚ハッシュと第 1 の安全タグの画像の保存された知覚ハッシュとの差を使用して、第 1 の安全タグを選択することと、第 2 のユーザ装置 1831 から受信した安全タグ画像の所定のセグメントの第 2 の知覚ハッシュを生成することと、生成された第 2 の知覚ハッシュと、第 1 の安全タグの画像の所定の部分の保存された第 2 の知覚ハッシュとの差を使用して、第 1 の安全タグから第 1 の安全タグ 1813 を選択することと、を含み得る。

20

【0194】

いくつかの実施形態では、ステップ 1805 の確認要求は、確認要求識別子を含み得る。この実施形態では、比較に基づいてステップ 1807 で第 1 の装置 1821 に文書を提供することは、潜在的なタグ特徴オプションの選択を使用して確認要求識別子をエンコードする、要求とペアになった第 2 の安全タグを生成することと、第 2 の安全タグで文書 1811 に透かしを入れることと、をさらに含むことができる。これらの実施形態では、透かし入り文書 1843 は、第 1 の安全タグ 1813 の透かしを含まない。

30

【0195】

いくつかの実施形態では、方法 1800 は、安全タグ画像の受信が認証基準を満たすことを決定することをさらに含み得る。特定の態様では、認証基準は、第 1 の安全タグ 1813 に関連付けられたいくつかの確認要求に関係し得る。他の態様では、認証基準は、第 1 の安全タグ 1813 が第 1 の装置 1821 に提供されてからの経過時間に関係し得る。まだ他の態様では、認証基準は確認要求の地理的起源に関係し得る。さらに他の態様では、確認要求は確認要求識別子を含むことができ、認証基準は確認要求識別子に関係し得る。これらの態様では、アクセス要求のアクセス識別子が確認要求の確認識別子と一致する場合、認証基準を満たすことができる。

40

【0196】

方法 1800 は、文書に必要な追加のセキュリティレベルがある場合に使用できる。例えば、銀行は方法 1800 を使用して、特定の文書のセキュリティを確保できる。銀行は、顧客の口座に関する文書と対になるタグを作成できる。顧客はラップトップから文書へのアクセスを要求できる。銀行は、文書に関連付けられた安全タグを顧客のラップトップに送信する。その後、顧客は携帯電話でタグをスキャンし、スキャンを銀行に送り返すことができる。その後、画像が比較され、画像が提供された安全タグと一致する場合、銀行の文書へのアクセスが許可される。

【0197】

図 19 は、例示的な可変安全タグを示している。可変タグは、グリフとタグをモーフィ

50

ングすることにより、時間の経過とともにデジタル的にアニメーション化できる。例えば、最初の時点では、変更可能なタグは、タグ特徴が追加されていない一連のドットの形式、または無効なフレーム1901である場合がある。無効なフレーム1901は、有効なフレーム1903に変化するために、所定の期間にわたって変化する可能性がある。有効なフレーム1903は、適切な読み取り装置で読み取ることができ、データを返すことができる。いくつかの実施形態では、可変タグは、可変タグプロセスの単一フレームによる認証であり得る。他の実施形態では、可変タグプロセスのいくつかのフレームによって認証されることにより、可変タグを認証することができる。さらに他の実施形態では、認証は、可変タグプロセスにおけるフレームの出現順序に基づいてのみ発生する可能性がある。他の実施形態では、無効なフレーム1901は、「ジャンクタグ」、または有効に見えても情報を返さないタグのタイプを含み得る。可変タグは、例えばカメラなど、任意の形式の読み取り可能な装置で読み取ることができる。

10

【0198】

いくつかの実施形態では、可変タグプロセスは、ロールオーバーまたはクリックイベントによってトリガされ得る。これらの実施形態では、タグは、トリガイイベントの前は静的であり、トリガイイベントの後に可変タグプロセスに入る。他の実施形態では、タグは、特定の時間枠の間に可変タグプロセスに入るように設定することができる。例えば、夜間にタグのセキュリティを強化するために、午後8時から午前8時までの間で変化するようにタグを設定できる。さらに他の実施形態では、可変タグは、別の有効なフレームとペアになっている有効なフレーム1903を含む。これらの実施形態では、ユーザは、タグを認証するために両方のペアのフレームをスキャンする必要がある場合がある。

20

【0199】

可変安全タグを生成するためのシステムは、少なくとも1つのプロセッサと、少なくとも1つのプロセッサによって実行されると、システムに第1の安全タグエンコーディングの生成を含み得る操作を実行させる命令を含む少なくとも1つの非一時的メモリを含み得るタグデータの値に応じたタグ特徴オプションの選択としてのタグデータ。第2の装置のスキナから、第1のタグ画像を含むタグ画像のシーケンスを含む要求を受信する。第1の安全タグと第1のタグ画像を使用して要求を認証する。要求の認証の表示を提供する。

【0200】

いくつかの実施形態では、動作は、有効なフレーム1903に示される第1の安全タグを含むタグのシーケンスを第1の装置のディスプレイ上に表示する命令を提供することをさらに含み得る。いくつかの態様では、有効なフレーム1903に示される第1の安全タグを含むタグのシーケンスを表示するために提供される命令は、タグのシーケンスをデジタル製品に埋め込むことを含み得る。他の態様では、命令は、トリガに応じて第1の装置のディスプレイのタグのシーケンスを表示することを提供できる。トリガは、ユーザまたは事前に定義されたイベントによって引き起こされるイベントである。どちらの側面でも、表示されるタグのシーケンスには無効なフレーム1901と有効なフレーム1903が含まれる。

30

【0201】

いくつかの実施形態では、要求を認証することは、有効なフレーム1903に表示される第1の安全タグの1つ以上の知覚ハッシュを第1のタグ画像の1つ以上の対応するハッシュと比較することを含み得る。他の実施形態では、認証は、所定の出現順序に従って複数の安全タグを複数の対応するタグ画像に一致させることをさらに要求することができる。さらに他の実施形態では、要求の認証の指示は、タグデータの少なくともいくつかを含み得る。さらに他の実施形態では、要求の認証の表示は、第1のタグデータの少なくともいくつかをデコードするためのデコード命令を含み得る。さらに他の実施形態では、要求の認証の指示は、データベースから読み出されたステータス情報を含み得る。特定の側面では、データベースは分散データベースにすることができ、Oracleを使用して分散データベースからステータス情報を取得できる。

40

【0202】

50

図20は、開示された実施形態と一致する、データベースを使用した在庫管理のための例示的なシステム2000を示す。サプライチェーン内の異なるエンティティに関連付けられたクライアントシステムによって実行されるものとして以下で説明するが、システム2000は、認証システム115、個人システム120、または別のシステムによっていくつかの実施形態で実行できる。いくつかの実施形態では、製造システム2001は、安全タグのステータス情報でデータベース（例えば、データベース130）をプロビジョニングするように構成され得る。いくつかの態様では、製造システム2001は、安全タグまたは安全タグでラベル付けされた項目に関するステータス情報でデータベースのアカウント2010の状態を更新するように構成することができる。製造システム2001または別のシステムは、キャリアシステム2003および小売業者システム2005にアプリケーションキーを提供するように構成できる。これらのアプリケーションキーにより、運送業者システム2003および／または小売業者システム2005はアカウント2010の状態を更新または変更できる。代替的または追加的に、データベースのアカウント2010の状態には、アカウントへのアクセスを管理する規則を含めることができる。いくつかの実施形態において、顧客システム2007は、アプリケーションキーを欠く可能性がある。したがって、いくつかの実施形態では、顧客システム2007は、データベースへのデフォルトレベルのアクセスを有することができる。例えば、顧客システム2007は、アカウント2010に記載されている状態情報への読み取り専用アクセス権を持つことができる。

【0203】

クライアント装置は、アカウント2010に関連付けられた安全タグをスキャンできる。安全タグをスキャンすると、クライアント装置が認証サーバ115と対話して安全タグをデコードする可能性がある。いくつかの実施形態では、クライアント装置は、認証情報（例えば、アプリケーションキーまたは認証資格情報）を提供し、認証サーバ115に情報を更新するように構成することができる。

【0204】

いくつかの実施形態では、安全タグからデコードされた情報を使用して、認証サーバ115は、アカウント2010を更新するように構成され得る。いくつかの態様では、認証サーバ115は、更新情報にアカウントのアドレスをオラクルに提供するように構成することができる。その後、Oracleはアカウント2010に更新を書き込むことができる。いくつかの実施形態では、認証サーバ115は、個人データベースに情報を提供するように構成され得る。個人データベースは、更新を収集するように構成でき、定期的にデータベースに書き込むことができる。

【0205】

様々な実施形態において、安全タグからデコードされた情報（例えば、データベース130のアカウント2010のアドレス）を使用して、認証サーバ115は、アカウント2010から情報を取得するように構成され得る。いくつかの態様では、認証サーバ115は、オラクルに状態情報の要求を提供するように構成することができる。要求には、アカウントのアドレスを含めることができる。オラクルは、アカウント2010の状態を読み取って状態情報を取得できる。状態情報は、クライアント装置に（直接または1つ以上のオラクルと認証サーバを介して）伝達される。

【0206】

いくつかの実施形態では、認証サーバ115は、データベースに対する読み取りまたは書き込みのための情報を提供するように構成することができる。例えば、認証サーバ115は、データベース130内のアカウント2010のアドレスをデコードし、そのアドレスをクライアント装置に提供するように構成され得る。クライアント装置は、オラクルに連絡して更新を提供したり、情報を読み取ったりできる。そのような実施形態では、オラクルは、クライアント装置から受信したアプリケーションキーまたはアカウント2010に格納された規則に基づいてアカウント2010へのアクセスを制限するように構成され得る。

【0207】

製造システム2001に関連付けられたクライアント装置は、開示された実施形態と一致して、安全タグをスキャンすることができる。例えば、安全タグでラベル付けされた項目が製造システム2001に関連付けられた製造施設を出るときに、作業者はクライアント装置を使用して安全タグをスキャンできる。製造システム2001は、システム2000を使用して、品目の製造に関する情報でアカウント2010を更新するように構成することができる。いくつかの実施形態では、製造システム2001は、その後、ポータルにアクセスして、安全タグに関してアカウント2010に格納された情報を読み取ることができる。例えば、製造システム2001が製造者に関連付けられたアプリケーションキーまたは資格情報を使用して（認証サーバ215またはOracleを介して）システム2000にアクセスする場合、製造システム2001は、追跡情報、販売情報、顧客データ、使用情報、活動情報、または場所情報の少なくとも1つを含む状態情報を取得できる。

10

【0208】

配布システム2003に関連付けられたクライアント装置は、開示された実施形態と一致して、安全タグをスキャンすることができる。例えば、ワーカはクライアント装置を使用して、安全タグでラベル付けされた項目を転送用に受信するときに、安全タグをスキャンできる。このスキャンに基づいて、配布システム2003は、システム2000を使用して、認証情報、宛先情報、または製造元情報の少なくとも1つに関する状態情報を取得するように構成できる。配布システム2003は、システム2000を使用して、項目の配布に関する情報でアカウント2010を更新するように構成できる。いくつかの実施形態において、配布システム2003は、続いてポータルにアクセスして、安全タグに関してアカウント2010に格納された情報を読み取ることができる。例えば、配布システム2003が卸業者に関連付けられたアプリケーションキーまたは資格情報を使用して（認証サーバ215またはOracleを介して）システム2000にアクセスする場合、配布システム2003は、信頼性情報、宛先情報、または製造元の少なくとも1つに関する状態情報を取得できる。

20

【0209】

小売業者システム2005に関連付けられたクライアント装置は、開示された実施形態と一致して、安全タグをスキャンすることができる。例えば、ワーカはクライアント装置を使用して、安全タグでラベル付けされた項目が卸業者から受信されると、安全タグをスキャンできる。このスキャンに基づいて、小売業者システム2005は、システム2000を使用して、信頼性情報、取引情報、製品情報、または追跡情報の少なくとも1つに関する状態情報を取得するように構成できる。小売業者システム2005は、システム2000を使用して、品目の受領または販売に関する情報でアカウント2010を更新するように構成できる。いくつかの実施形態では、小売業者システム2005は、その後、ポータルにアクセスして、安全タグに関してアカウント2010に格納された情報を読み取ることができる。例えば、小売業者システム2005が、販売業者に関連付けられたアプリケーションキーまたは資格情報を使用して（認証サーバ215またはOracleを介して）システム2000にアクセスする場合、小売業者システム2005は、認証情報、取引情報、製品情報の少なくとも1つに関する状態情報を取得できる、または追跡情報。

30

40

【0210】

クライアント装置2007は、開示された実施形態と一致して、安全タグをスキャンすることができる。いくつかの実施形態では、クライアント装置2007は、アプリケーションキーまたは認証証明書を欠いている場合がある。そのような実施形態では、システム2000は、安全タグ105でラベル付けされた項目に関する情報を比較的わずかに提供してもよい。例えば、クライアント装置2007は、信頼性情報、製品情報、または所有権情報の少なくとも1つを取得できる場合がある。

【0211】

本明細書で説明するように、アカウントの状態は、追跡情報、販売情報、顧客データ、使用情報、活動情報、位置情報、信頼性情報、宛先情報、更新メーカ情報、取引情報、製

50

品データ、または所有権の証明情報の少なくとも1つを示す安全タグの状態情報を含むステータス情報を保存できる。製造業者、流通業者、小売業者、および顧客の間でのこの情報へのアクセスの特定の割り当ては、例示であることを意図しており、限定するものではない。

【0212】

図21は、開示された実施形態と一致する、データベース内の安全タグ情報を変更するための例示的なシステム2100を示す。以下ではクライアントシステムによって実行されるものとして説明するが、システム2100は、認証システム115、個人システム120、または別のシステムによっていくつかの実施形態で実行することができる。図20に関して上述したように、システムは、安全タグを含む対話中またはポータルを使用してデータベースにアクセスして、安全タグの状態に関する情報を読み書きすることができる。図21に示すように、特権アカウント（例えば、特権アプリケーションキーまたは認証資格情報で示される）を持つユーザは、データベースにアクセスして状態情報を更新し、タグをキャンセルできる。これにより、その後の使用または取引でタグが無効になる可能性がある。例えば、ユーザ2103が後でタグを使用してアクションを実行しようとする、認証サーバ115はタグがキャンセルされたことを示し、タグの識別、タグの認証、またはアクションの実行を拒否できる。

【0213】

図22は、安全タグを使用して在庫を追跡するプロセスを示している。示されるように、図16Aおよび16Bに関して説明されるように、ペアのタグ（例えば、タグ2201および2203）を使用して2つの靴を一緒に結び付けることができる。靴は、タグ2201および2203のそれぞれとペアになっているタグ2205で靴箱にラベルを付けることにより、靴を含む靴箱とペアにすることができる。靴箱のボックスのタグ2207は、タグ2205とペアにすることができる。輸送用コンテナのタグ2209は、靴箱のボックスのタグ2207とペアにすることができる。小売業者タグ2211は、出荷コンテナのタグ2209とペアにすることができる。顧客への所有権の譲渡は、図23に関して以下で説明するように、タグ2213の生成に関連付けることができる。いくつかの実施形態において、タグ2213タグは、個々の靴タグ2201および2203と対にすることができる。この在庫追跡プロセス全体を通じて、記述されたタグに関連付けられたアカウントは、図20および図21に関して説明したように、追跡情報、位置情報、およびその他のステータス情報で更新できる。示されているように、小売業者が管理する（小売業者制御ループ2203内の）タグのアカウントの情報は、少なくとも小売業者がアクセスできるが、タグ2201、2203、および2213のアカウントの情報は顧客がアクセスできる。

【0214】

図23は、安全タグを使用して項目の所有権を譲渡するプロセスを示している。タグ検証プロセスには、一意に生成されたデジタル安全タグと元のメーカーの安全タグ2301のペアリングが含まれる。いくつかの実施形態では、製品は、元の製造業者の安全タグ2301を持つ販売者によって受け取られる。製造元の安全タグ2301は販売者のシステムに記録され、オンラインで製品に関連付けられている。潜在的な顧客は、製品をオンラインで表示できる。潜在的な各顧客には、スキャン時に製品を認証できるセカンダリデータを含む一意に生成されたタグが表示される。一意に生成された各タグは、元のメーカーの安全タグ2301と対になる。例えば、潜在的な購入者には、一意の安全タグ2303が提示される。一意の安全タグ2303は、元のメーカーの安全タグ2301に似ているが、一意のセカンダリデータが含まれている。さらに、一意の安全タグ2303は、元のメーカーの安全タグ2301と対になる。したがって、ユーザは、製品を見るための日時に関する情報を含み得る一意の安全タグ2303を維持しながら、製品の信頼性を確認できる。他の実施形態では、潜在的なユーザ2に一意の安全タグ2（2305）を提示でき、潜在的なユーザ3に一意の安全タグ3（2307）を提示でき、潜在的なユーザ4に一意の安全タグ4（2309）を提示でき、潜在的なユーザ5を提示できるユニークな安全タグ5（

10

20

30

40

50

2311)を使用する。各実施形態において、一意の安全タグは、元の製造業者の安全タグ2301と対にされる。

【0215】

いくつかの実施形態では、製品が買い手によって購入されると、売り手は元の製造業者安全タグ2301を買い手に割り当てることができる。他の実施形態では、元の製造業者の安全タグ2301は、購入時に買い手に自動的に割り当てることができる。いずれの実施形態でも、元の製造業者タグ2301の購入およびその後の割り当ては、ブロックチェーンで更新される。購入と割り当てに続いて、追加の一意の安全タグを生成し、元のメーカタグ2301とペアにすることはできない。特定の側面では、ペアの一意の安全タグを介して潜在的な顧客に購入を通知できる。例えば、元の製造元の安全タグ2301と一意の安全タグのペアリングを削除できる。別の例では、一意の安全タグは、ブロックチェーン上の更新された情報を介して潜在的な顧客に購入を通知できる。

10

【0216】

図24Aは、例示的な安全タグを示す。安全タグには、様々な技術構成要素を含めることができる。例えば、技術構成要素には、検証フラグメント、外枠および内枠、外枠セクション、外枠ブロック、ドット、グリフ、コネクタおよびスプライン、L a a v a ステージ1ID、中央グラフィック、中央グラフィックp u b l i cが含まれる。キー、および以下で詳細に説明する追加の技術的機能。さらに、技術構成要素を使用して、様々な形式でデータをエンコードできる。技術的な構成要素については、以下で詳しく説明する。

【0217】

中央のグラフィックは、グラフィック、ブランド、またはその他のビジュアルにすることができ、フィンガプリントされたデータも含むエンドユーザの識別可能な要素にすることができる。いくつかの実施形態では、中央のグラフィックは、安全タグの向きに使用することができる。他の実施形態では、中央のグラフィックは、データを含み得るグリフセットであり得る。例えば、中央のグラフィックには、大きなタグよりも小さな指紋署名を含めることができ、必要に応じて、読み取り可能なテキストに128文字の情報を含めることができる。さらに他の実施形態では、ブランドを表示するために中央のグラフィックを使用することができる。そのような実施形態では、中央グラフィックは任意の形状とすることができ、色を有することができる。中央のグラフィックは、コントラストの異なる線でさらに囲まれ、タグの残りの部分から分離できる。いくつかの実施形態では、線は特定の太さを有することが要求され得る。

20

30

【0218】

中央のグラフィック公開キーは、中央のグラフィックのハッシュされたS H A 2バージョンである場合があり、通常は生成された大きな数である。以下でさらに詳しく説明するように、中央のグラフィック公開キーを使用して、タグの他の部分のロックを解除できる。L a a v a ステージ1IDは、製造元IDと公開キーにすることができ、データを読み取る前にタグを識別することができる。グリフは通常、タグ内で生成された個々の形状または文字であり、ほとんどのデータ、キー、IDなどが格納される場所である。外側のフレームは、安全タグの外側の境界線であり、スキャンの形状を定義する。外側のフレームは、追加の機能とデータストレージも可能にする。内側のフレームは、中央のグラフィックを囲む安全タグの内側のオプションの境界線にすることができ、中央のグラフィックからグリフを視覚的に分離するために使用できる。さらに、内側のフレームを使用して中央のグラフィックのフィンガプリントを作成し、データを含めることができる。

40

【0219】

検証フラグメントは、特定の画像データのセットにすることができ、検証、比較、およびデータの保存に使用できる。検証フラグメントには、中央のグラフィックやその他の可変要素など、複数の要素を含めることができる。ドットは、空白が目に見える形または円になる安全タグのポイントになることができる。ドットは複数のデータ要素を保存してタグを定義でき、グリフを形成するための開始点になる。スプラインとコネクタは、2つ以上のドットを結合またはブレンドする形状にすることができ、大量のデータの保存と強力

50

な暗号化またはエンコードを可能にする。外枠セクションは、外枠の識別された部分であり、データの保存または繰り返しに使用できる。外部フレームブロックは、外部フレームセクションのブレイクのコレクションであり、データの格納に使用できる。

【0220】

図24Bは、例示的な安全タグに対応するグラフィックファイルの部分を示している。グラフィックファイルは、図24Aに示された例示的な安全タグを表す。グラフィックファイルは、タグ生成プロセス中に作成される。詳細については、以下で説明する。

【0221】

図25Aは、それぞれ同じスタイルシートであるが異なるデータを使用して生成された安全タグ2501、安全タグ2503、および安全タグ2505を示す。スタイルシートは、安全なタグ生成の第1のステップのタグテンプレートを提供する。いくつかの実施形態では、スタイルシートは安全タグのクラスを記述する。スタイルシートの受信に続いて、タグ生成プロセスは数値シードを受け取り、安全タグレイアウトを生成し、タグデータを受け取る。その後、すべてが最終的な安全タグを生成する。スタイルシートと数値シードは、データをエンコードできる場所を提供する。その後、データはタグ特徴オプションとしてエンコードされる。図25Aでは、安全タグ生成プロセスの第1のステップで同じスタイルシートを使用して安全タグ2501、2503、および2505がすべて生成されたが、最終的な安全タグが生成される前に異なるデータが提供された。タグ生成プロセス中に、タグ生成システムは、安全タグ2501、2503、および2505のスタイルシートに基づいて同じ一次および二次場所から選択できるため、安全タグ間の類似性が得られる。各例示的な安全タグのレイアウトが作成された後、データはタグ特徴オプションにエンコードされ、独自のデザインが作成された。

【0222】

図25Bは、安全タグ2511、安全タグ2513、および安全タグ2515を示し、それぞれが異なるスタイルシートであるが同じタグデータを使用して生成される。前述のように、スタイルシートはタグ生成プロセスの第1のステップで使用される。安全タグ2511、2513、および2515はそれぞれ、利用可能な異なる一次および二次場所でタグ生成プロセスを開始した。前の例と同様に、データは、一次および二次位置が識別および選択された後にエンコードされる。データは様々なタグ特徴にエンコードでき、タグ生成アルゴリズムはランダム化されたデザインを生成するため、同じタグデータによって、最終的に安全タグデザインが大きく異なる可能性がある。安全タグ2511、2513、および2515は、スキャン時にすべて同じデータを返すが、各安全タグには独自のデザインがある。

【0223】

図26A～図26Pは、潜在的な安全タグ特徴の詳細を示している。各図については、以下で詳しく説明する。

【0224】

図26Aは、例示的な安全タグの潜在的な特徴を示している。潜在的な各機能を使用して、データをエンコードしたり、フィンガプリントを作成したりできる。潜在的な機能は次のとおりである。プライマリ内部ドット、外部ブレイク、内部ブレイク、内部端ブレンド、外部水平ブレンド、内部フレーム、所有者ID、セカンダリ内部ドット、内部水平ブレンド、外部フレーム、外側のブレンド、短いブレンド、二次的な外側のドット、内側の変形、外側の変形、結節、長いブレンド。以下で詳しく説明するように、これらの潜在的な機能のそれぞれを使用して情報をエンコードできる。追加の変数資産を使用して、追加のデータを埋め込んだり、情報を暗号化したりできる。例えば、変数アセットには、インデント、くぼみ、色付きの図形、グラデーション、接続線、埋め込み記号を含めることができる。

【0225】

いくつかの実施形態では、安全タグは、製品を認証するか情報を保存するための追加の機能を含み得る。例えば、背景パターンまたはテクスチャは、タグの後ろに微妙にまたは

目に見えないように配置できる。同様に、別の例では、隣接するパターンまたはテクスチャを使用して、追加の認証を提供したり、情報を保存したりできる。別の例では、ペンローズタイルのグラフィックパターンを使用して、特定のタグセットをフィンガプリントまたは区別できる。さらに別の例では、一意の単語セットなどの隣接情報をタグの近くに配置できる。このような設計は、例えばカスタマーサポートの場合など、人間が読み取れるID確認が必要な場合に役立つ。

【0226】

図26Bは、位置ベクトル2601を示す例示的なタグを示している。位置ベクトル2601は、レイアウトおよびドットおよび形状の任意の変位が決定された後の例示的な安全タグ内のドットおよび形状の最終位置を開示する。位置ベクトル2601は、安全タグの各形状、ドット、およびタグ特徴の位置に関する情報を提供する。

10

【0227】

図26Cは、オフセットドット整列の例を示している。上記で開示されたように、例示的な安全タグのレイアウトは、安全タグのクラスおよび数値シードを記述するスタイルシートの受信に続いて決定され得る。レイアウト位置2603は、安全タグレイアウトが生成された後の例示的なドットの位置を示している。タグデータを受信すると、タグ特徴オプションとして安全タグが生成される。特定のタグ特徴オプションには、ドットとシェイプの配置と配置が含まれる。変位位置2605は、タグデータがタグ特徴オプションとしてエンコードされた後の例示的なドットの最終位置を示している。レイアウト位置2603と変位位置2605の違いは、人間の目に見分けがつかない場合があり、そのようなタグをコピーすることは困難である。タグ生成システムは、グリッドを標準グリッドよりもはるかに予測不能にするように設計されている。いくつかの実施形態では、解像度により、グリッドオフセット、ライン長、角度などに基づいて、変位位置2605をレイアウト位置2603から調整することができる。そのような実施形態では、これらの調整により、追加情報をタグにエンコードすることが可能になり得る。

20

【0228】

図26Dは、ドット接続機能オプション2608を示す例示的な安全タグを示している。ドット接続機能オプション2608は、他のドットに到達するために、安全タグの外枠内の任意の距離に広がることができる。いくつかの実施形態では、ドット接続機能オプション2608は、ドットとして直線として確立することができる。ドット接続機能オプション2608は、中央の画像を通過して別のドットに到達することはできない。

30

【0229】

図26Eは、スプラインおよび端接続を作成するためにデータがエンコードされた後のドット接続機能オプション2608を示している。スプラインを介して形成される形状は、グリフと呼ばれる。上記で説明したように、グリフはタグ内で生成された個々の形状または文字にすることができ、ほとんどのデータ、キー、IDなどが格納される場所にすることができる。いくつかの実施形態では、スプライン数学を使用して、暗号化またはエンコードされた情報を含めることができる。例えば、楕円曲線暗号を使用できる。端結合を使用してデータを保存することもできる。

【0230】

40

図26Fおよび図26Gは、同じ例示的なタグレイアウトのベクトルとしてドットおよびコネクタを示している。安全タグはベクトル形式で生成され、接続線と曲線を含む2Dポイントの観点から定義される。これらの画像のベクトルは、データのエンコードに使用できる可変スプラインの原点とスプラインの厚さ、またはコネクタを示している。図26Fは、第1の接続幅2607を示し、図26Gは、第2の接続幅2609を示す。第1の接続幅2607は、第2の接続幅2609よりも大きいものとして示されている。第1の接続幅2607および第2の接続幅2609は、同じデータまたは異なるデータでエンコードされ得る。

【0231】

図26Hは、端接続機能オプション2610を示す例示的なタグを示している。端接続

50

は、潜在的な端コネクタ機能オプション 2 6 1 0 から形成できる。端コネクタ機能オプション 2 6 1 0 は、内側フレームまたは外側フレームの間に端接続を形成する可能性を提供する。端コネクタ機能オプション 2 6 1 0 を選択して端接続に変換すると、データを形状にエンコードできる。例えば、端接続は、メーカ番号を表すために使用されるデータでエンコードできる。

【0 2 3 2】

図 2 6 H および 2 6 I は、同じ例示的なタグレイアウトのベクトルとしてドットおよび端接続を示している。これらの画像のベクトルは、データをエンコードするために使用できる可変端結合の原点と厚さを示している。図 2 6 I は、第 1 の端接続サイズ 2 6 1 1 を示し、図 2 6 H は、第 2 の端接続サイズ 2 6 1 3 を示す。第 1 の端接続サイズ 2 6 1 1 は、第 2 の端接続サイズ 2 6 1 3 よりも大きいものとして示されている。第 1 の接続サイズ 2 6 1 1 および第 2 の端接続サイズ 2 6 1 3 は、同じデータまたは異なるデータでエンコードされ得る。

【0 2 3 3】

図 2 6 J は、例示的な安全タグの様々なグリフおよび潜在的なスプライン機能を示している。グリフセットは、多数のスプラインを使用して生成し、柔軟な座標系内に配置できる。いくつかの実施形態において、グリフは、ブレンド曲率アルゴリズムを使用して数学的に生成することができる。他の実施形態では、所定の形状に基づいてグリフを生成することができる。例えば、顧客は、顧客の製品またはサービスに基づいて特定の形状のグリフを要求できる。この例では、グリフセットを明確に識別し、特別に設計できる。グリフのスプラインの太さは、部分的に各ドットのスプラインの開始位置に基づいて変化する。いくつかの実施形態において、グリフは、任意の数のドット間に形成され得る。グリフの周囲には、微細構造として、またはパスにデータを保存するアルゴリズム手法内にデータを含めることができる。図 2 6 J は、限られた数の可能なグリフとスプラインフィーチャのみを示している。

【0 2 3 4】

図 2 6 K は、第 1 のリング変形 2 6 1 5、第 2 のリング変形 2 6 1 7、および第 3 のリング変形 2 6 1 9 を示し、これらはすべてデータをエンコードするために使用することができる。第 1 のリング変形 2 6 1 5 は、外枠の内縁の変形を含み得る。第 2 のリング変形 2 6 1 7 は、内側フレームの外縁上の変形を含み得る。第 3 のリング変形 2 6 1 9 は、外枠の外縁の変形を含み得る。

【0 2 3 5】

図 2 6 L は、マイクロドット 2 6 2 1 および微小印刷 2 6 2 3 を示し、これらは両方ともデータをエンコードするために使用することができる。微小印刷 2 6 2 3 は、第 2 の二値データセットを含むことができ、これは、外枠および外枠破損データと同様の方法で解釈することができる。低解像度では、微小印刷 2 6 2 3 がノイズとして表示される場合がある。より高い解像度では、微小印刷 2 6 2 3 は指紋データのグリッド位置に関する情報を含み得る。情報には、X または Y グリッド番号とオフセット値を含めることができる。いくつかの実施形態では、十分な微小印刷 2 6 2 3 があれば、タグを暗号化することができる。他の実施形態では、微小印刷 2 6 2 3 は異なる色を含み得る。そのような実施形態では、微小印刷 2 6 2 3 は、同じ物理空間に追加情報を保存することができる。さらに他の実施形態では、外側フレームは、ラインの内側と外側の両方に微小印刷 2 6 2 3 を含み得る。そのような実施形態では、内側および外側の両方の微小印刷 2 6 2 3 を着色することができる。他の実施形態では、微小印刷 2 6 2 3 は、ブロックされたセクションの高さを変えることにより追加の二値データを保存することができる。そのような実施形態では、二値コードは、物理サイズが小さいためコピーするのが難しい場合がある。微小印刷 2 6 2 3 は高度なデータストレージに使用でき、非常に高解像度のカメラからアクセスできる。

【0 2 3 6】

図 2 6 M は、同じ場所を 3 つの異なるグラデーションの色塗りで示している。塗りつぶ

10

20

30

40

50

されていない 2 6 2 5、異なる色 2 6 2 7 で塗りつぶされ、同じ色 2 6 2 9 で塗りつぶされている。データは、場所の勾配と色に基づいて安全タグにエンコードできる。

【0 2 3 7】

図 2 6 N は、例示的なタグ特徴 2 6 3 1 と、タグ特徴 2 6 3 1 にエンコードされたデータを示している。タグ特徴 2 6 3 1 は、接続によって接続された 2 つのドット、または第 3 のビットによって接続された 2 ビットを、エンコードされたデータを含む詳細領域 2 6 3 3 とともに示す。詳細領域 2 6 3 3 は、ドットの 1 つの端の周囲を包むスプラインを含み得る。詳細領域 2 6 3 3 は、開始位置 2 6 3 5 から読み取り方向 2 6 3 7 に移動することで読み取ることができる。詳細領域 2 6 3 3 は、3 ビットのデータ（値 A）をエンコードする可能性のある第 1 空間周波数と、18 ビットのデータをエンコードする可能性のある第 2 空間周波数を持つことができる。値 A 設定ビット 2 6 3 9 は、第 1 の空間周波数で 1 を表し、値 A 未設定ビット 2 6 4 1 は、第 1 の空間周波数で 0 を表す。値 B 未設定 B は、第 2 の空間周波数で 0 を表し、値セットビット 2 6 4 5 は、第 2 の空間周波数で 1 を表す。エンコードされたデータの 3 ビットと 18 ビットに続いて、2 6 4 7 の繰り返しがある。

10

【0 2 3 8】

図 2 7 A ～ 図 2 7 K は、例示的な安全タグの生成を示している。各図について、以下で詳しく説明する。

【0 2 3 9】

図 2 7 A は、安全タグ生成のプロセスにおいてベースとして使用される例示的なグリッドを示す。グリッドは、グリフ 2 7 0 5 のベースである潜在的な一次位置 2 7 0 1 と潜在的な二次位置 2 7 0 3 を備える。グリッドの形成は、安全タグの生成における第 1 の段階であり、特定のアルゴリズムを使用してランダム化されたデザインを作成する。潜在的な一次位置 2 7 0 1 および潜在的な二次位置 2 7 0 3 は、グリフ 2 7 0 5 の最終的な位置および形状を決定する。グリフ 2 7 0 5 は、任意の数の潜在的な一次位置 2 7 0 1 および潜在的な二次位置 2 7 0 3 にまたがることのできる。

20

【0 2 4 0】

図 2 7 B は、選択された一次位置 2 7 0 7 および選択されていない一次位置 2 7 0 9 を示している。タグ生成プロセスのこの段階で、潜在的な一次位置 2 7 0 1 が識別され選択される。タグ生成アルゴリズムは、所定数の潜在的な一次位置 2 7 0 1 をランダムに選択する。次に、選択された一次位置 2 7 0 7 は、安全タグ生成プロセスでさらに使用されるが、選択されていない一次位置 2 7 0 9 は、タグ生成プロセスの一部ではなくなる。図 2 7 B では、ランダムに選択された 26 個の選択された一次位置 2 7 0 7 があり、72 億個の可能な組み合わせの 1 つをもたらす。

30

【0 2 4 1】

図 2 7 C は、潜在的な二次位置 2 7 1 1 の識別を示している。潜在的な二次位置 2 7 1 1 は、選択された一次位置 2 7 0 7 の間に位置する任意の二次位置を含み得る。図 2 7 C では、40 の潜在的な二次位置 2 7 1 1 が特定されており、約 1 兆のサブコンビネーションの可能性はある。

【0 2 4 2】

図 2 7 D は、選択されていない二次位置 2 7 1 3 および選択された二次位置 2 7 1 5 を示している。選択された二次位置 2 7 1 5 は、以前に特定された潜在的な二次位置 2 7 1 1 から選択される。選択された二次位置 2 7 1 5 は、タグ生成アルゴリズムに基づいてシステムによって選択され、選択された一次位置 2 7 0 7 を別個の選択された一次位置 2 7 0 7 に接続するために使用され得る。

40

【0 2 4 3】

図 2 7 E は、安全タグ生成のプロセスで視覚化エンジンを介して処理する直前および直後に、選択された一次位置 2 7 0 7 および選択された二次位置 2 7 1 5 を示す二次グリッドを示す。選択された一次位置 2 7 0 7 および選択された二次位置 2 7 1 5 を含む二次グリッド、または最終的な二次グリッドは、さらに安全タグ生成のために視覚化エンジンに

50

渡することができる。特定の選択された一次位置 2707 は、選択された二次位置 2715 によってブリッジされる。選択された二次位置 2715 は、選択された一次位置 2707 間の接続を作成するために使用され、グリフが生成される。一部の実施形態では、各グリフ上の曲線の形状はデータを含み得る。形状ビルドに基づいて、構造に追加のコードバリエーションを導入できる。選択された二次位置 2716 によってブリッジされなかった選択された一次位置 2707 は、個々のドットとして残ることができる。いくつかの実施形態では、ドットはデータを含み得る。

【0244】

図 27F～図 27I は、選択された一次位置 2719 および選択された二次位置 2721 に基づいて異なる可能なグリフ 2717 を示す。各図で、タグ生成アルゴリズムは、潜在的なコネクタとして二次位置のいずれかを識別している場合がある。各図は、選択された二次位置 2721 に基づいて異なる可能なグリフ 2717 を示している。図 27F および図 27H は両方とも、選択された一次位置 2719 が少なくとも 1 つであるが 3 つ以下の選択された一次位置 2719 に接続されるグリフ 2715 を示すが、図 27H は直列に接続された選択された一次位置 2719 を示す。図 27G は、選択された一次位置 2719 が選択されたすべての一次位置 2719 に接続されているグリフ 2717 を示している。この図では、選択された二次位置 2721 により、選択された一次位置 2719 が大きな円または点になる。図 27J は、5 つの選択された一次位置 2719 のうち 3 つのみが選択された二次位置 2721 によって接続されているグリフ 2717 を示している。この図では、最終タグにはグリフ 2717 と 2 つの個別のドットが含まれる。図 27F～図 27I の各グリフ 2717 には、データをエンコードできる。

【0245】

図 27J は、方向情報 2723 を有する例示的な安全タグを示している。方向情報 2723 は、中央の画像として安全タグの中央に配置できる。方向情報 2723 をタグ識別プロセスで使用して、光学式読み取り装置が正しいタグを適切に識別できるようにすることができる。いくつかの実施形態では、方向情報は、ロゴ、ブランド、または他の識別子を含み得る。

【0246】

図 28A～図 28N は、例示的な安全タグを示している。各タグの詳細については、以下で説明する。

【0247】

図 28A は、様々なフォームファクタの安全タグを示している。安全タグの外枠は、任意の形状にすることができる。例えば、特定の画像に一致するように設計されたタグを顧客が要求する場合がある。この例では、目的の画像が安全タグと商標の両方として機能する。いくつかの実施形態では、安全タグは中央画像を持たない場合がある。これらの実施形態では、タグの向きは、安全タグの外側フレームの設計に基づいて達成することができる。他の実施形態では、中央画像は、顧客により提供されるカスタム画像であり得る。図 28A は、オーストラリアの形状や Nike（商標）Swoosh など、考えられるフォームファクタの例を示している。

【0248】

図 28B は、一連の例示的なタグを示している。これらの各タグには、対称的なデザインと、コネクタまたはスプラインのない一連のドットがある。通常的安全タグ生成プロセスでは、対称安全タグが作成される可能性は非常に低くなる。しかし、安全タグ生成プロセスを制御して、図 28B に示す例のように、審美的に魅力的なタグを作成することもできる。これらの例では、デザインが選択され、選択したデザインにデータをエンコードできる。

【0249】

図 28C は、バーコードと統合された安全タグの例を示している。いくつかの実施形態では、安全タグはバーコードと一緒に読み取ることができる。他の実施形態では、安全タグとバーコードは別々に読み取ることができる。安全タグとバーコードを統合すると、S

K Uベースのバーコード読み取り装置の後方互換性と一意のアイデンティティを提供できる。安全タグには、バーコードに関連する一致データを含めることができる。これにより、バーコードと安全タグの両方の不正使用または誤用を防ぐことができる。

【0250】

図28Dは、例示的な安全タグを示す。いくつかの実施形態では、例示的な安全タグは、色付きまたは黒の背景にオーバーレイされた中央画像を有することができる。他の実施形態では、安全タグは内部フレームを有さない場合がある。さらに他の実施形態では、安全タグは、外側フレームとは異なる形状の内側フレームを有することができる。

【0251】

図28Eは、対称パターンおよびL a a v a中央画像を有する例示的な安全タグを示す。

10

【0252】

図28Fは、対称パターンとラーバ中心画像を備えた例示的な安全タグを示している。

【0253】

図28Gは、対称パターンとラーバ中心画像を備えた例示的な正方形の安全タグを示している。

【0254】

図28Hは、対称的なパターンとラーバ中心画像を備えた例示的な正方形の安全タグを示している。

【0255】

図28Iは、中心画像がなく、ドット間のコネクタがない例示的な安全タグを示す。

20

【0256】

図28Jは、L a a v a中央画像を有し、ドット間にコネクタがない例示的な正方形の安全タグを示す。

【0257】

図28Kは、L a a v a中央画像と狭い厚さのコネクタを備えた例示的な安全タグを示す。

【0258】

図28Lは、L a a v a中央画像および狭い厚さのコネクタを備えた例示的な正方形の安全タグを示す。

【0259】

図28Mは、対称パターンとラーバ中心画像を備えた例示的な安全タグを示す。

30

【0260】

図28Nは、対称パターンおよびラーバ中心画像を備えた例示的な正方形の安全タグを示す。

【0261】

図29Aは、安全タグを管理するための例示的なユーザインターフェースを示している。図29Aでは、ダッシュボードタブに24時間にわたる安全タグアクティビティが表示されている。いくつかの実施形態では、ユーザインターフェースのダッシュボードは、単一の顧客のすべての安全タグの概要、場所ごとの安全タグの数、関連するユーザ情報、および関連する再販業者情報を含む情報を提供できる。ユーザインターフェースには、ユーザインタラクションに使用できる様々なタブがある。これらのタブには、タグ管理、タグ設計、タグ印刷、レポート、統計、アカウント情報、APIセットアップ、ユーザ管理などが含まれる。

40

【0262】

図29Bは、安全タグ設計を要求するための例示的なユーザインターフェースを示している。タブデザインのユーザインターフェースは、安全タグを作成するための様々なオプションをユーザに提供できる。例えば、ユーザは、ネストされた安全タグが必要かどうか、および安全タグをペアにするかどうかを選択するオプションがある。その他の潜在的なカスタマイズ可能なオプションには、カスタマーセンタのロゴ、暗号化ID、カスタムDB同期、安全タグがユーザが読み取り可能かどうか、IDを難読化するかどうか、オフラ

50

インでの読みやすさ、場所の埋め込みの有無、リセラーが含まれる各IDへのアクセス、Laavaブロックチェーンを使用するかどうか、安全タグが強制終了可能かどうか。図30Bでは、ユーザはネストされたタグの4つのレイヤを選択しており、最上位のレイヤがペアになっている。安全タグの各レイヤには、異なる情報を含めることができる。この例では、ユーザは各レイヤが提供できる情報と、各安全タグにアクセスするために必要なキーを制御できる。

【0263】

いくつかの実施形態では、システム100（例えば、認証サーバ115または個人システム120）は、1つ以上の安全タグを許可された安全タグの許可されていないコピーとして識別するように構成され得る。システム100は、これらの不正コピーに関する情報にインデックスを付け、不正コピーに関する情報を含むレポートを生成するように構成することができる。例えば、システム100は、安全タグの不正コピーがどこでどのくらいの頻度で検出されたかを示す図29Aおよび図29Bのユーザインターフェースによって表示可能なヒートマップを生成するように構成することができる。

【0264】

例示的な使用例

【0265】

安全タグを使用して、アルコールなどの製品の販売および購入において顧客と小売業者の両方を支援できる。購入する前に、顧客は、例えばワインボトルなどのアルコールの信頼性を確認し、前の所有者、小売業者、製造業者、製造日、材料、使用説明書などのワインボトルに関する情報を受け取ることができる、安全警告、およびその他の関連情報。販売前に、小売業者はタグをスキャンして情報を確認できる。情報には、ロジスティクスでの到着の確認、ブドウ園からの小売業者のオファーの表示、メーカーと製造データの表示、ワインボトルの在庫の表示、材料の表示、顧客の販売の表示が含まれるメモ、店舗の位置の決定、返品ポリシーの設定、ボトルごとのオファーの設定、ボトルの購入時に発生する幸運な勝利の設定、安全警告の表示、使用説明書の表示、およびその他の関連アクション。チェックアウト時に、小売業者はワインボトルの所有権を顧客に譲渡することができ、顧客は安全タグを使用して追加のメリット（再注文、レビューなど）を利用できる。いくつかの実施形態において、ワインボトルは、ボトルを開けた後の追加の信頼性のためにワインボトルキャップの内側に第2の安全タグの場所を有することができ、これはワインボトルの外側の安全タグと対にすることができる。

【0266】

安全タグを使用して、Webページ、電子メール、またはその他のデジタル製品を認証できる。例えば、Webページには、Webページ自体の認証に使用されるデジタルトークンとして機能する、すべてのページに一意の安全タグを設定できる。安全タグは、所定の期間が経過すると変更される可能性がある。また、タグは、表示またはタイムアウトされると強制終了される。ユーザは、安全なプラグインを使用して、またはスマートフォンなどの光学式読み取り装置を使用して、安全タグ自体をスキャンするブラウザを使用して、Webページ、電子メールなどを認証できる。安全タグを使用して、配信日時、ウェブサイトまたはメールプロバイダ、ウェブページまたはメールのセキュリティ情報、またはウェブページまたはメールに固有のその他の情報を確認できる。

【0267】

顧客が所有し、許可されたビジネスとペアリングまたは共有する単一の保護されたタグ内で、複数の形式のメンバーシップを管理できる。顧客は、健康保険証、学生証、フィットネス会員証、旅行会員証など、様々な形式のIDおよび／または会員資格を持ち、単一の個人的な物理的またはデジタルセキュアにエンコードできる。鬼ごっこ。IDやメンバーシップのエンコードされた形式に関連付けられた各ビジネスには、関連付けられた特定のIDやメンバーシップのみについて安全タグをチェックするアクセス権を付与できる。したがって、顧客は、複数の形式のIDを持ち歩く代わりに、各状況で同じ単一の安全タグを提示できる。

【0268】

安全タグを使用して、オンラインとオフラインの両方で使用できる認証済みの保護された個人IDを作成できる。ユーザは、公式ID（クレジットカード、パスポートなど）を関連機関（銀行、パスポートオフィスなど）に持ち込み、そこでIDが検証され、確認されたIDサプライヤがユーザの個人IDブロックチェーンに接続される。認証された保護された個人IDは、適切な当局によって読み取られ、選挙や投票、銀行取引明細書のプッシュ、安全なメッセージング、安全な電子メール、建物への入場、メンバーシップ、年齢証明、その他のアプリケーションで使用できる。個人識別が必要である。保護されたIDはユーザが所有しているが、関係は正式なID発行者と対になっているため、正式なID発行者はIDを取り消すことができる。

10

【0269】

企業は、安全タグを使用して、顧客用に認証済みの個人IDを作成できる。例えば、銀行などのビジネスは、そのユーザのアカウントに関連付けられた個人IDと特定のアクセス許可を持つ読み取り装置（例えば、そのビジネスに固有のアプリを使用）の両方を顧客に提供できる。その顧客の特定の情報を含む物理的またはデジタル文書には、その文書に関連付けられた正しい個人IDを持つユーザのみが読み取ることができるタグを含めることができる。ユーザが文書に関連付けられた正しい個人IDを持っている場合、個人IDによって許可されたレベルに対応するアクセスが許可される。さらに、認証された個人IDを使用して、自動預け払い機や銀行などで顧客を確認できる。ビジネスは、正しい個人IDを持たないユーザが文書をスキャンしたとき、または顧客の確認に個人IDを使用できないときに通知を受け取ることができる。

20

【0270】

安全タグを使用して、アートやその他の貴重な商品を認証し、アーティストが継続的／将来の販売から収益を潜在的に獲得できるようにすることができる。安全タグを元のアートワークに添付し、所有権を表す第2の安全タグと、アーティストが保持する第3の安全タグの両方とペアにすることができる。アートワークの安全タグと所有権を表す第2の安全タグの両方に、アート自体、現在の所有者、アーティスト、アートディーラに関する情報を含めることができ、所有権の売却と譲渡には両方が必要である。アーティストは、ペアになったタグを保持し、所有権の譲渡時に通知を受け取ることができる。所有権の譲渡による収益の一部が含まれる可能性がある。いくつかの実施形態では、例えば、タグに近接するアートフレーム上の木目パターンを使用して、近接フィンガプリントによりアートを検証することができる。近接指紋は顧客には見えないため、タグを移動すると検証されず、信頼性が証明されない場合がある。

30

【0271】

粉ミルクなど、非常に特定の要件を持つ他の貴重な製品は、安全タグを使用して認証できる。粉ミルクには、外部の安全タグと内部の安全タグの両方を含めることができる。外部タグには、次のような重要な情報を含めることができる：使用説明書、メーカーID、市場情報、安全情報、またはすべての潜在的な顧客がスキャンできるその他の関連情報。乳児用調乳を購入して所有権を譲渡すると、所有者は内部の安全タグに含まれる情報にアクセスできる。内部の安全タグは通常、パレットまたは出荷IDを介して在庫または小売業者IDとペアになり、購入した特定の乳児用調製粉乳に関する完全なサプライチェーン情報に顧客がアクセスできるようにする。

40

【0272】

安全タグを使用して、紛失した項目を追跡し、所有者に返すことができる。ユーザは、所有者に関する情報を含む様々なフォームファクタで、独自の安全タグを印刷したり、安全タグを購入したりできる。安全タグは、アプリまたは別のプログラムを介して「遺失物」アカウントとペアリングし、項目に添付できる。タグの所有者には、タグがスキャンされるたびに、時間や場所などのスキャンに関する情報を含む通知が送信される。所有者は、他の誰かがタグをスキャンした場合に、所有者への連絡方法や項目の返品方法などの特定の情報を開示するかどうかを選択できる。

50

【0273】

保証と保険の登録は、安全タグを使用して処理できる。顧客はブロックチェーンを通じて車両を認証し、車両を購入できる。その後、所有権は顧客に譲渡され、顧客は保証のために登録され、車両は適切なデータベース（DMVなど）で顧客に正式に登録される。顧客の保険会社は、最近購入した車両の顧客IDと車両データを照合できる。顧客IDが確認されると、保険を発行できる。

【0274】

安全タグを使用して、カジノチップまたはその他のギャンブルチップを認証できる。各チップには、チップに埋め込まれたRFID IDとペアにすることができる安全タグが与えられる。安全タグとRFIDの組み合わせはブロックチェーンで管理できるため、カジノは各チップを様々な方法で追跡できる。ユーザは、自分の読み取り装置で安全タグをチェックして、正当なチップが手元にあることを確認することもできる。さらに、チップ上の一意のタグは、スプーフィングされたタグを作成するための視覚的な抑止力として機能する。

10

【0275】

宝くじやその他のプロモーションは、安全タグを使用して管理できる。会社はブロックチェーン上にチケットを作成できる。その後、顧客はブロックチェーンのチケットに関連付けられたデジタルまたは物理チケットを購入し、チケットのタグを公開できる。その後、チケットをスキャンし、顧客は勝ち負けに関する情報を受け取ることができ、勝ち負けの結果はブロックチェーンで更新できる。いくつかの実施形態では、チケットは、購入前に宝くじ会社、小売業者などに関する基本情報を明らかにするためにスキャンすることができるタグであることができ、現在の所有者がスキャンして勝ち負けの結果を明らかにできる新しいタグを明らかにするために削り取ることができる部分を持つタグにすることができる。

20

【0276】

安全タグは、特定の顧客にプロモーション広告を提供するために使用できる。顧客には、その顧客に固有の特定のタグを含むプロモーション広告をオンラインで提供できる。その後、顧客は広告に関連付けられたWebサイトにアクセスし、特定のIDとプロモーションデータが埋め込まれた安全タグ付きのクーポンを印刷できる。その後、顧客は実店舗にアクセスしてクーポンを引き換えることができ、実売は元の広告に関連付けられたデジタルCookieに関連付けられる。

30

【0277】

安全タグは、一般的なプロモーション活動にも使用できる。例えば、自動車会社は、車両の景品や試乗を予約するために使用される、公に宣伝されるカスタムタグを作成できる。安全タグは一般に公開され、誰でもスキャンできる。安全タグは、各顧客スキャンが一意になるように、すべてのビューに必要な場所、時間、およびその他のデータが含まれるように、セット式に従ってアニメーション化できる。各スキャンはブロックチェーンにアップロードされ、会社は特定のスキャンを行うためのプロモーション規則を設定できる。

【0278】

物理的な暗号通貨は、安全タグを使用して認証できる。ユーザは、「ビットコイン」などの暗号通貨を、安全タグが印刷された物理的なメモに読み込むことができる。安全タグは、アクセスキーによって特定の所有者に結び付けることも、オフラインで誰でも利用できるように公開することもできる。安全タグはチェックアウトステーションで検証でき、取引に関する情報はブロックチェーンにアップロードできる。いくつかの実施形態では、安全タグは、RFIDなどの別の形式の識別とペアにすることができる。

40

【0279】

安全タグを使用して、軍隊やその他の非公開組織で使われるような機密項目へのアクセスを制御できる。プライベートブロックチェーンに保存された情報を使用して、プライベート安全タグを作成できる。指定された担当者には、タグ付き項目をスキャンおよび読み取るための様々なアクセスレベルを付与できる。許可されていない読み取り装置によっ

50

て項目がスキャンされた場合、タグをスキャンした場所、時間、およびユーザに関するデータがプライベートブロックチェーンに返送される。許可されていない読み取り装置が項目をスキャンした場合、安全タグ所有者に向けられたアラームまたは警告がトリガされることがある。

【0280】

肉や家畜、または他の有機製品は、近接フィンガプリントにより安全タグを使用して検証できる。例えば、安全タグの近くにある牛肉の「テクスチャ」は、パッケージングの時点で安全タグと一緒に指紋を取ることができる。安全タグは、牛肉の切り身、包装の日付、輸送、および傷みやすい商品の購入に重要なその他の情報を提供できる。製品をエンドユーザに対して完全に認証するには、安全タグとテクスチャと一緒にスキャンする必要がある。タグが移動した場合、近接フィンガプリンティングでは製品が本物であると検証されない。

10

【0281】

安全タグを使用して、安全および検査レポートを確認および検証できる。検査が必要なユニットまたは装置がインストールされている場合、インストーラは、ユニット全体または個々の部品用の安全タグを作成し、インストールおよび製造元に関する情報を含めることができる。適切なアクセス権を持つ追加のユーザが検査および安全性評価中にタグをスキャンおよび更新できる。新しいユーザが安全タグをスキャンすると、検査履歴、交換履歴、以前にタグをスキャンしたユーザ、スキャンした日時、保証情報、部品が誰によって提供されたかに関する情報および関連すると見なされるその他の情報を受け取ることができる。したがって、検査のログをブロックチェーンに保存できる。

20

【0282】

安全タグを使用して、薬と処方箋を認証できる。例えば、医師は処方箋の盗難を防ぐために、すべての処方箋ページに一意的安全タグを付けることができる。医師は、処方箋を書き留めるときにスキャンして、特定の患者がその処方箋を使用する許可を与えることができる。薬局が処方箋を補充しているとき、医師が特定の処方箋ページを使用する許可を医師が実際に与えているかどうか、また適切な薬が正しい人に処方されているかどうかを確認するために安全タグを確認できる。別の例では、安全タグを医薬品の包装、ブリスターパック、さらには個々の錠剤自体に印刷できる。これらの例では、薬は患者と照合されるため、医師、看護師、または承認された他の医療提供者がスキャン時に患者情報にアクセスできる。これにより、薬が処方されたとおりに服用されているという証拠が得られ、正しい人に適切な薬が確実に提供されるようになる。

30

【0283】

安全タグを使用して、税金と経費の報告を追跡および検証できる。会社は、領収書と請求書をスキャンするための特定の読み取り装置を従業員に提供できる。領収書と請求書は一意的タグで印刷でき、このアクティビティ用に特別に設計された読み取り装置でスキャンできる。読み取り装置は、領収書または請求書の特定の安全タグのみをスキャンする機能をユーザに提供するように設計できる。スキャンされた費用はブロックチェーンに保存され、会社または税務当局が将来アクセスして費用と費用を確認できる。

【0284】

40

ユーザは、様々な構成でカスタマイズされた安全タグを作成できる。例えば、特定のブランドは、商標と同じ形でデザインされたタグを持ちたい場合がある。これにより、様々なパッケージオプションと様々なレベルのセキュリティが可能になる。いくつかの実施形態では、安全タグの形状を標準形状に固定したまま、中央ロゴをカスタマイズすることができる。

【0285】

安全タグを使用すると、灰色の製品を供給ラインから排除できる。特定の機器および車両の本物の部品には、製造業者に関する情報と、部品を使用する機器または車両の種類に関する情報を含む安全タグを付けることができる。将来、部品を検査および交換するエンジニアまたは技術者は、部品をスキャンして、部品が本物であり、正しい方法で使用され

50

ているかどうかを判断できる。

【0286】

安全タグを使用して、偽造品または偽造品を識別および報告できる。顧客は製品の安全タグをスキャンして、製造業者、認可された販売国、承認された小売業者などを確認できる。この情報のいずれかがオフになっている場合、顧客はスキャンの場所と時間に関する情報を含め、項目を偽物として報告できる。レポートはブロックチェーンにアップロードされ、タグの所有者に通知される。さらに、各安全タグは一意であるため、同じタグが複数の場所で複数回スキャンされていると報告した場合、タグの所有者に不一致が自動的に通知される。

【0287】

企業は、安全タグを使用して、靴などの製品のコピーを制限できる。この例では、コピー機は、正当なタグを持つ会社が製造した単一の靴にアクセスし、偽の靴に置くために正規のタグのコピーを作成した。その後、コピー機は靴を多数のバイヤに販売し、製品が本物であると主張する。第1のスキャンのみが認証された本物の製品になり、スキャンは靴が販売される前でなければならない。同じタグが初めてスキャンされたのではないことがタグで明らかになった場合、タグは偽造品として報告され、顧客は偽造品の購入を免れる。正当な顧客が靴を最初にスキャンしない場合、顧客は会社自体で製品を認証できる。

【0288】

開示される実施形態は、システム、方法、および／またはコンピュータプログラム製品で実装され得る。コンピュータプログラム製品は、プロセッサに本発明の態様を実行させるためのコンピュータ可読プログラム命令を有するコンピュータ可読記憶媒体を含み得る。

【0289】

コンピュータ可読記憶媒体は、命令実行装置によって使用される命令を保持および格納できる有形の装置であり得る。コンピュータ可読記憶媒体は、例えば、電子記憶装置、磁気記憶装置、光学記憶装置、電磁記憶装置、半導体記憶装置、または前述の任意の適切な組み合わせであり得るが、これらに限定されない。コンピュータで読み取り可能な記憶媒体のより具体的な例の非網羅的なリストには、ポータブルコンピュータディスク、ハードディスク、ランダムアクセスメモリ（RAM）、読み取り専用メモリ（ROM）、消去可能なプログラム可能な読み取り専用メモリのみ（EPROMまたはフラッシュメモリ）、スタティックランダムアクセスメモリ（SRAM）、ポータブルコンパクトディスク読み取り専用メモリ（CD-ROM）、デジタルバーサタイルディスク（DVD）、メモリスティック、フロッピーディスク、命令が記録されたパンチカードまたは溝内の隆起構造などのエンコードされた装置、および前述の任意の適切な組み合わせ。本明細書で使用されるコンピュータ可読記憶媒体は、電波または他の自由に伝搬する電磁波、導波管または他の伝送媒体を伝搬する電磁波（例えば、光ファイバケーブルを通過する光パルス）またはワイヤを介して送信される電気信号などの一時的な信号それ自体と解釈されるべきではない。

【0290】

本明細書で説明するコンピュータ読み取り可能なプログラム命令は、コンピュータ読み取り可能な記憶媒体からそれぞれのコンピューティング／処理装置、またはインターネット、ローカルエリアネットワーク、ワイドエリアネットワークおよび／またはワイヤレスネットワークなどのネットワークを介して外部コンピュータまたは外部ストレージ装置にダウンロードできる。ネットワークには、銅線伝送ケーブル、光伝送ファイバ、無線伝送、ルータ、ファイアウォール、スイッチ、ゲートウェイコンピュータ、および／または端サーバが含まれる。各コンピューティング／処理装置のネットワークアダプタカードまたはネットワークインターフェースは、ネットワークからコンピュータ可読プログラム命令を受信し、各コンピューティング／処理装置内のコンピュータ可読記憶媒体に格納するためにコンピュータ可読プログラム命令を転送する。

【0291】

本発明の動作を実行するためのコンピュータ可読プログラム命令は、アセンブラ命令、

10

20

30

40

50

命令セットアーキテクチャ（ISA）命令、マシン命令、マシン依存命令、マイクロコード、ファームウェア命令、状態設定データ、またはソースコードまたは対象物のいずれかであり得る。Smalltalk、C++などの対象物指向プログラミング言語、および「C」プログラミング言語または同様のプログラミング言語などの従来の手続き型プログラミング言語を含む、1つ以上のプログラミング言語の任意の組み合わせで記述されたコード。コンピュータで読み取り可能なプログラム命令は、ユーザのコンピュータ上で、ユーザのコンピュータ上で、スタンドアロンのソフトウェアパッケージとして、ユーザのコンピュータ上で、リモートコンピュータ上で、またはリモートコンピュータまたはサーバ上で完全に実行できる。後者のシナリオでは、リモートコンピュータは、ローカルエリアネットワーク（LAN）またはワイドエリアネットワーク（WAN）を含む任意のタイプのネットワークを介してユーザのコンピュータに接続できる。または、外部コンピュータ（例えば、インターネットサービスプロバイダを使用したインターネット経由）。一部の実施形態では、例えば、プログラマブルロジック回路、フィールドプログラマブルゲートアレイ（FPGA）、またはプログラマブルロジックアレイ（PLA）を含む電子回路は、コンピュータ可読プログラム命令の状態情報を利用して、本発明の態様を実行するために電子回路をパーソナライズすることによりコンピュータ可読プログラム命令を実行することができる。

【0292】

本明細書では、本発明の実施形態による方法、装置（システム）、およびコンピュータプログラム製品のフローチャート図および／またはブロック図を参照して、本発明の態様を説明する。フローチャート図および／またはブロック図の各ブロック、およびフローチャート図および／またはブロック図におけるブロックの組み合わせは、コンピュータ可読プログラム命令によって実装できることが理解されよう。

【0293】

これらのコンピュータ可読プログラム命令は、汎用コンピュータ、専用コンピュータ、またはその他のプログラム可能なデータ処理装置のプロセッサに提供され、コンピュータのプロセッサまたはその他のプログラム可能なデータを介して実行される命令がマシンを生成する処理装置、フローチャートおよび／またはブロック図のブロックで指定された機能／行為を実装するための手段を作成する。これらのコンピュータ可読プログラム命令は、コンピュータ、プログラム可能なデータ処理装置、および／または他の装置を特定の方法で機能させることができるコンピュータ可読記憶媒体に格納することもでき、その結果、コンピュータ可読記憶媒体は命令を格納するフローチャートおよび／またはブロック図ブロックで指定された機能／動作の側面を実装する命令を含む製品を含む。

【0294】

コンピュータ可読プログラム命令は、コンピュータ、他のプログラム可能なデータ処理装置、または他の装置にロードして、コンピュータ、他のプログラム可能な装置または他の装置で一連の動作ステップを実行し、コンピュータ実装プロセスを生成することもできる。そのため、コンピュータ、他のプログラム可能な装置、または他の装置で実行する命令は、フローチャートおよび／またはブロック図のブロックで指定された機能／動作を実装する。

【0295】

図中のフローチャートおよびブロック図は、本発明の様々な実施形態によるシステム、方法、およびコンピュータプログラム製品の可能な実装のアーキテクチャ、機能、および動作を示している。これに関して、フローチャートまたはブロック図の各ブロックは、指定された論理機能を実装するための1つまたは複数の実行可能な命令を含むソフトウェアプログラム、セグメント、またはコードの一部を表してもよい。また、いくつかの代替の実装では、ブロックに記載されている機能は、図に記載されている順序とは異なる順序で発生する場合があることに注意する必要がある。例えば、実際には、連続して示される2つのブロックは、実質的に同時に実行される場合がある。または、機能が関係する場合は、ブロックが逆の順序で実行される場合もある。また、ブロック図および／またはフロー

チャート図の各ブロック、およびブロック図および／またはフローチャート図のブロックの組み合わせは、指定された機能または行為を実行する専用ハードウェアベースのシステムまたは特殊用途のハードウェアとコンピュータの指示の組み合わせによって実装できることに注意されたい。

【0296】

本発明の様々な実施形態の説明は、例示の目的で提示されているが、網羅的であることまたは開示された実施形態に限定されることを意図するものではない。記載された実施形態の範囲および精神から逸脱することなく、多くの修正および変形が当業者には明らかであろう。本明細書で使用される用語は、実施形態の原理、市場で見られる技術に対する実際の応用または技術的改善を最もよく説明するか、または当業者が本明細書で開示される実施形態を理解できるように選択された。

10

【0297】

このアプリケーションから満了する特許の存続期間中に、多くの関連する仮想化プラットフォーム、仮想化プラットフォーム環境、信頼できるクラウドプラットフォームリソース、クラウドベースの資産、プロトコル、通信ネットワーク、セキュリティトークンおよび認証資格情報が開発され、範囲これらの用語のすべては、そのような新しい技術をすべて先験的に含むことを意図している。

【0298】

明確にするため別個の実施形態の文脈で説明されている本発明の特定の特徴は単一の実施形態に組み合わせて提供することもできることは分かるであろう。逆に、簡潔にするために単一の実施形態の文脈で説明される本発明の様々な特徴は、別個に、または任意の適切なサブコンビネーションで、または本発明の他の説明された実施形態で適切に提供されてもよい。様々な実施形態の文脈で説明される特定の特徴は、実施形態がそれらの要素なしで動作不能でない限り、それらの実施形態の本質的な特徴と見なされるべきではない。

20

【0299】

本発明をその特定の実施形態に関連して説明したが、多くの代替、修正、および変形が当業者には明らかであることは明らかである。したがって、添付の特許請求の範囲の精神および広い範囲内にあるそのようなすべての代替、修正、および変形を包含することが意図されている。本発明の態様の一部を以下記載する。

〔態様1〕

30

安全タグと対話するための認証サーバであって、
少なくとも1つのプロセッサと、
前記少なくとも1つのプロセッサによって実行されたときに、
タグ画像を含むタグ識別要求を受信することと、
スタイルシートを使用して生成された安全タグの画像の保存されたハッシュを使用して、
前記受信タグ画像内の安全タグを識別することと、
前記受信タグ画像と前記スタイルシートを使用して生成されたタグをデコードするためのデコード規則とを使用してタグデータを生成することと、
前記タグ識別要求に応じて前記タグデータを提供することと、を含む動作を前記認証サーバに実行させる命令を含む少なくとも1つの非一時的メモリと、
を備える認証サーバ。

40

〔態様2〕

前記保存されたハッシュおよび前記受信タグ画像を使用して前記安全タグを識別することは、
前記受信タグ画像のハッシュを生成することと、
前記保存されたハッシュと前記生成されたハッシュとの間の差がしきい値基準を満たすと判定することと、
を含む、態様1に記載の認証サーバ。

〔態様3〕

前記受信タグ画像の前記ハッシュを生成することは、前記受信タグ画像を所定のピクセ

50

ル数を有する画像に変換することを含む、態様 2 に記載の認証サーバ。

〔態様 4〕

前記所定のピクセル数は、64ピクセル以上、かつ1,048,576ピクセル以下である、態様 3 に記載の認証サーバ。

〔態様 5〕

前記ハッシュは知覚ハッシュである、態様 2 に記載の認証サーバ。

〔態様 6〕

前記差は、前記保存されたハッシュと前記生成されたハッシュとの間のハミング距離である、態様 2 に記載の認証サーバ。

〔態様 7〕

前記受信タグ画像はベクトルグラフィックスファイルであり、

前記受信タグ画像の前記ハッシュを生成することは、前記ベクトルグラフィックスファイルの少なくとも一部をラスタライズすることを含む、態様 2 に記載の認証サーバ。

〔態様 8〕

前記受信タグ画像内の前記安全タグを識別することは、

前記受信タグ画像のハッシュを生成することと、

前記生成されたハッシュと、第 1 の安全タグの画像の保存されたハッシュとの差を使用して、前記第 1 の安全タグを選択することと、

前記受信タグ画像の所定のセグメントの第 2 のハッシュを生成することと、

前記生成された第 2 のハッシュと、前記第 1 の安全タグの前記画像における前記所定の部分の保存された第 2 のハッシュとの差を使用して、前記第 1 の安全タグから前記安全タグを選択することと、

を含む、態様 1 に記載の認証サーバ。

〔態様 9〕

前記受信タグ画像内の前記安全タグを識別することは、前記受信タグ画像の漸進的により小さいセグメントのハッシュを生成することを含む、態様 1 に記載の認証サーバ。

〔態様 10〕

前記受信タグ画像内の前記安全タグを識別することは、

前記受信タグ画像のハッシュを生成することと、

前記安全タグの第 1 の所定のセグメントに対応する前記受信タグ画像の第 1 のセグメントの第 2 のハッシュを生成することと、

前記生成されたハッシュと前記安全タグの画像の保存されたハッシュとの差がしきい値基準を満たさないと判定することと、

前記生成された第 2 のハッシュと前記安全タグの前記第 1 の所定のセグメントの画像の保存された第 2 のハッシュとの差を使用して前記安全タグを選択することと、

前記安全タグの第 2 の所定のセグメントに対応する第 3 のハッシュを生成することと、

前記生成された第 3 のハッシュと、前記安全タグの前記第 2 の所定のセグメントの画像の保存された第 3 のハッシュとの間の差を使用して、前記安全タグを検証することと、

を含む、態様 1 に記載の認証サーバ。

〔態様 11〕

前記第 3 のハッシュは、前記安全タグの前記第 2 の所定のセグメントに対応する前記受信タグ画像の第 2 のセグメントにわたって生成される、態様 10 に記載の認証サーバ。

〔態様 12〕

前記第 3 のハッシュは、前記安全タグの前記第 2 の所定のセグメントに対応する第 2 の受信タグ画像にわたって生成される、態様 10 に記載の認証サーバ。

〔態様 13〕

前記受信タグ画像内の前記安全タグを識別することは、

前記安全タグの所定のセグメントの画像のハッシュを、前記受信タグ画像を含む 1 つ以上の受信タグ画像のセグメントのハッシュと比較し、前記 1 つ以上の受信タグ画像の前記セグメントは、前記安全タグの前記所定のセグメントに対応することと、

10

20

30

40

50

前記比較に基づいて前記安全タグを選択することと、
を含む、態様 1 に記載の認証サーバ。

〔態様 1 4〕

前記比較は、
前記安全タグの前記所定のセグメントの前記画像の前記ハッシュと、前記 1 つ以上の受信タグ画像のセグメントの前記対応するハッシュとの間のセグメント距離と、
前記セグメント距離を使用した全体距離またはしきい値基準を満たすセグメント距離のカウントの少なくとも 1 つと、
を判定することを含む、態様 1 3 に記載の認証サーバ。

〔態様 1 5〕

前記動作は、前記安全タグの前記所定のセグメントの前記画像の前記ハッシュの数、前記しきい値基準を満たすセグメント距離のカウント、および前記セグメント距離を使用して信頼値を判定することをさらに含む、態様 1 4 に記載の認証サーバ。

〔態様 1 6〕

前記 1 つ以上の受信タグ画像は、
第 1 の詳細レベルでタグの少なくともいくつかを示す第 1 の画像と、
前記第 1 の詳細レベルよりも大きい第 2 の詳細レベルで前記タグの少なくともいくつかを示す第 2 の画像と、
を含む、態様 1 3 に記載の認証サーバ。

〔態様 1 7〕

前記動作は、
個人システムから前記画像の前記保存されたハッシュを受信することと、
前記個人システムにデコード要求を提供し、前記デコード要求は前記安全タグの識別子を含むことと、
をさらに含み、
前記デコード規則は、前記デコード要求に応じて前記個人システムから受信される、態様 1 に記載の認証サーバ。

〔態様 1 8〕

前記タグ識別要求は認証キーを含み、
前記デコード要求は認証キーを含み、
前記デコード規則は前記認証キーに対応する、
態様 1 に記載の認証サーバ。

〔態様 1 9〕

前記タグ識別要求はクライアント装置から受信され、
動作は、
前記スタイルシートを使用して生成されたタグの公開部分をデコードするための公開デコード規則を受信することと、
前記クライアント装置に前記公開デコード規則を提供することと、
をさらに含む、態様 1 に記載の認証サーバ。

〔態様 2 0〕

前記デコード規則は、前記スタイルシートによって規定されたタグ特徴のサブセットのデコードを可能にする、態様 1 に記載の認証サーバ。

〔態様 2 1〕

前記デコード規則は、前記スタイルシートによって規定された前記安全タグの一部のデコードを可能にする、態様 1 に記載の認証サーバ。

〔態様 2 2〕

前記デコード規則は、
前記スタイルシートによって定義された前記安全タグの第 1 の部分、または前記スタイルシートによって規定されたタグ特徴の第 1 のサブセットの少なくとも 1 つのデコードを可能にする第 1 のデコード規則と、

10

20

30

40

50

前記安全タグの第2の部分または前記タグ特徴の第2のサブセットの少なくとも1つのデコードを可能にする第2のデコード規則と、

を含み、

前記受信タグ画像と前記デコード規則とを使用してタグデータを生成することは、

第1のデコード規則を使用して第1のタグデータを生成することと、

第1のタグデータと第2のデコード規則を使用して第2のタグデータを生成することと、

を含む、態様1に記載の認証サーバ。

〔態様23〕

前記動作は、タグ識別要求を追跡することをさらに含む、態様1に記載の認証サーバ。

〔態様24〕

前記動作は、タグ識別要求情報を記憶することをさらに含む、態様1に記載の認証サーバ。

〔態様25〕

前記動作は、タグデータを反映するために分散データベースを更新する命令を提供することをさらに含む、態様1に記載の認証サーバ。

〔態様26〕

安全タグを生成するためのシステムであって、

少なくとも1つのプロセッサと、

前記少なくとも1つのプロセッサによって実行されたときに、

安全タグのクラスを説明するスタイルシートを受け取ることと、

数値シードを取得することと、

前記数値シードとスタイルシートとを使用して安全タグレイアウトを生成し、前記安全タグレイアウトは、前記数値シードとスタイルシートとに基づいてタグ特徴オプションの組み合わせを指定することと、

タグデータを受信することと、

前記タグデータの値に従って前記タグ特徴オプションを選択することにより、前記タグデータをエンコードする安全タグを生成することと、

前記安全タグの知覚ハッシュを生成することと、

前記安全タグの前記ハッシュと識別子とをデータベースに保存することと、

前記安全タグを提供することと、を含む動作を認証サーバに実行させる命令を含む少なくとも1つの非一時的メモリと、

を備えるシステム。

〔態様27〕

前記安全タグレイアウトは、データをエンコードするために、前記安全タグレイアウト内の1つ以上の参照位置を示す参照部分を指定する、態様26に記載のシステム。

〔態様28〕

前記安全タグレイアウトは、データをエンコードするために、前記安全タグレイアウト内の参照されていない部分を指定する、態様26に記載のシステム。

〔態様29〕

前記安全タグレイアウトは、ランダムデータをエンコードするために、前記安全タグレイアウト内のジャンク部分を指定する、態様26に記載のシステム。

〔態様30〕

前記安全タグレイアウトは、暗号化キーをエンコードするために、前記安全タグレイアウト内のキー部分を指定する、態様26に記載のシステム。

〔態様31〕

前記タグ特徴オプションは、前記安全タグレイアウトによって指定された位置におけるタグ特徴の有無を含む、態様26に記載のシステム。

〔態様32〕

前記タグ特徴オプションは、タグ特徴のサイズ、色、または形状を含む、態様26に記載のシステム。

10

20

30

40

50

〔態様 3 3〕

前記タグ特徴オプションは、前記安全タグレイアウトによって指定された位置からの逸脱を含む、態様 2 6 に記載のシステム。

〔態様 3 4〕

前記タグ特徴オプションは、前記安全タグレイアウトによって指定された位置に存在するいくつかのタグ特徴を含む、態様 2 6 に記載のシステム。

〔態様 3 5〕

前記タグ特徴オプションは、前記タグ特徴上のスプラインエンコードの存在を含む、態様 2 6 に記載のシステム。

〔態様 3 6〕

前記スプラインエンコードは、基準点または基準線から様々な距離に延びるタグ特徴端を含む、態様 3 5 に記載のシステム。

〔態様 3 7〕

前記様々な距離は、1 つ以上の空間的に多重化されたタグデータ値をエンコードする、態様 3 6 に記載のシステム。

〔態様 3 8〕

前記様々な距離は、前記 1 つ以上の空間的に多重化されたタグデータ値の繰り返しをエンコードする、態様 3 7 に記載のシステム。

〔態様 3 9〕

前記タグ特徴オプションは、前記タグ特徴上の微細構造の存在を含む、態様 2 6 に記載のシステム。

〔態様 4 0〕

前記タグ特徴はリムを含み、前記リムの前記タグ特徴オプションは、リム破損、リム変形、およびリム接続を含む、態様 2 6 に記載のシステム。

〔態様 4 1〕

前記タグ特徴はリム破損を含み、前記リム破損の前記タグ特徴オプションはリム破損端形状を含む、態様 2 6 に記載のシステム。

〔態様 4 2〕

前記タグ特徴は、所定のタイプのタグ特徴間の接続を含み、前記接続のためのタグ特徴オプションは、接続幅および接続非対称を含む、態様 2 6 に記載のシステム。

〔態様 4 3〕

前記タグ特徴は、タグ特徴間の接続を含み、前記接続のための前記タグ特徴オプションは、接続幅および接続非対称を含む、態様 2 6 に記載のシステム。

〔態様 4 4〕

前記タグ特徴は、中央ロゴを含み、前記タグ特徴オプションは、前記安全タグの中心点からの前記中央ロゴの変位を含む、態様 2 6 に記載のシステム。

〔態様 4 5〕

前記タグ特徴オプションを選択することによりタグデータをエンコードする前記安全タグを生成することは、第 1 のタグデータの値に従って第 1 のタグ特徴オプションを選択し、前記第 1 のタグ特徴オプションの前記選択は第 2 のタグ特徴オプションを作成することと、第 2 のタグデータの値に従って前記第 2 のタグ特徴オプションを選択することと、を含む、態様 2 6 に記載のシステム。

〔態様 4 6〕

前記第 1 のタグ特徴オプションはポイントの有無を含み、前記第 2 のタグ特徴オプションは前記第 1 のタグデータの値に従って存在するポイント間の接続の有無を含み、第 3 のタグデータをエンコードする第 3 のタグ特徴オプションは、前記第 2 のタグデータの前記値に応じて存在する接続の幅を含む、態様 4 5 に記載のシステム。

〔態様 4 7〕

前記タグデータの値に従って前記タグ特徴オプションを選択することにより、前記タグデータをエンコードする前記安全タグを生成することは、

10

20

30

40

50

暗号化キーで前記タグデータを暗号化することと、
前記暗号化されたタグデータの値に従って前記タグ特徴オプションを選択することと、
前記暗号化キーを前記安全タグにエンコードすることと、
を含む、態様 2 6 に記載のシステム。
[態様 4 8]
前記安全タグは、ベクトルグラフィックスファイルを含む、態様 2 6 に記載のシステム。
[態様 4 9]
前記安全タグを提供することは、前記安全タグをラスタライズすることを含む、態様 2 6 に記載のシステム。
[態様 5 0]
前記安全タグを提供することは、前記安全タグで対象物にラベル付けすること、またはデジタル製品に前記安全タグを組み込むことを含む、態様 2 6 に記載のシステム。
[態様 5 1]
前記動作は、前記タグデータを提供する前に、前記生成されたハッシュを他の安全タグのハッシュとの衝突についてチェックすることをさらに含む、態様 2 6 に記載のシステム。
[態様 5 2]
前記スタイルシートは、公開データをエンコードするための前記安全タグレイアウトの部分生成する公開部分と、個人データをエンコードするための前記安全タグレイアウトの部分生成する個人部分とを含む、態様 2 6 に記載のシステム。
[態様 5 3]
前記動作は、
前記安全タグの異なるセグメントの知覚ハッシュを複数の詳細レベルで生成することと、
前記安全タグの異なるセグメントの前記知覚ハッシュを前記データベースに保存することと、
をさらに含む、態様 2 6 に記載のシステム。
[態様 5 4]
前記タグデータは、1 つ以上の他の安全タグに関する 1 つ以上の識別子を含む、態様 2 6 に記載のシステム。
[態様 5 5]
前記 1 つ以上の識別子における第 1 の識別子は、前記 1 つ以上の他の安全タグにおける第 1 の安全タグの知覚ハッシュを含む、態様 5 4 に記載のシステム。
[態様 5 6]
前記タグデータは、多要素識別項目の識別子を含むことを特徴とする態様 2 6 に記載のシステム。
[態様 5 7]
前記多要素識別項目は、画像の認証証明書または知覚ハッシュを含む、態様 5 6 に記載のシステム。
[態様 5 8]
前記画像は、前記タグでラベル付けされた対象物の一部を示す、態様 5 7 に記載のシステム。
[態様 5 9]
前記画像は、前記タグに関連付けられた人物を示す、態様 5 7 に記載のシステム。
[態様 6 0]
前記タグを提供することは、基板上に前記タグを印刷し、前記タグの少なくとも第 1 の部分が蛍光インクで印刷されることを含む、態様 2 6 に記載のシステム。
[態様 6 1]
安全タグ読み取り装置であって、
少なくとも 1 つのプロセッサと、
前記少なくとも 1 つのプロセッサによって実行されたときに、
画像内の潜在的な安全タグを検出することと、

10

20

30

40

50

前記画像およびスタイルシートを使用して、正規化安全タグ画像を生成することと、
前記正規化安全タグ画像を含む識別要求を認証サーバに提供することと、
前記安全タグにエンコードされたタグデータをタグ特徴オプションとしてデコードする
ための規則を受信することと、

前記受信した規則を使用して前記タグデータをデコードすることと、を含む動作を前記
安全タグ読み取り装置に実行させる命令を含む少なくとも1つの非一時的メモリと、
を備える安全タグ読み取り装置。

〔態様62〕

前記画像は、前記安全タグ読み取り装置のスキヤナから受信される、態様61に記載の
安全タグ読み取り装置。

〔態様63〕

前記スキヤナはカメラである、態様61に記載の安全タグ読み取り装置。

〔態様64〕

前記画像内の前記潜在的な安全タグを検出することは、前記潜在的な安全タグのサイズが前
記スタイルシートから読み出されたサイズ制約を満たすと判定することを含む、態様61
に記載の安全タグ読み取り装置。

〔態様65〕

前記潜在的な安全タグは、幾何学的特徴検出、カーネルベースの特徴検出、テンプレート
マッチング、または畳み込みニューラルネットワークのうちの少なくとも1つを使用して
検出される、態様61に記載の安全タグ読み取り装置。

〔態様66〕

幾何学的特徴検出を使用して前記画像内の潜在的な安全タグを検出することは、
画像をしきい値処理して二値画像を生成することと、
前記スタイルシートから読み出されたターゲットパラメータ値を使用して、前記二値画
像内の幾何学的特徴を検出することと、

前記幾何学的特徴を使用して、前記潜在的な安全タグの基準点を決定することと、
を含む、態様65に記載の安全タグ読み取り装置。

〔態様67〕

前記幾何学的特徴は同心円の楕円を含み、前記基準点は前記同心円の楕円の焦点を含む
、態様66に記載の安全タグ読み取り装置。

〔態様68〕

前記潜在的な安全タグの正規化画像を生成することは、前記画像を白黒画像またはグレイ
スケール画像に変換することを含む、態様61に記載の安全タグ読み取り装置。

〔態様69〕

前記潜在的な安全タグの正規化画像を生成することは、画像ワープ変換と前記スタイル
シートから検索されたターゲットパラメータ値とを使用して前記画像を平坦化すること
を含む、態様61に記載の安全タグ読み取り装置。

〔態様70〕

画像ワープ変換を使用して前記画像を平坦化することは、魚眼歪み、樽型歪み、または
角度歪みのうちの少なくとも1つを補正することを含む、態様69に記載の安全タグ読み
取り装置。

〔態様71〕

前記ターゲットパラメータ値は、内側または外側のタグリム形状を含む、態様69に記
載の安全タグ読み取り装置。

〔態様72〕

前記潜在的な安全タグの正規化画像を生成することは、潜在的画像ギャップのタグ特徴オ
プションを決定し、前記タグ特徴オプション値をターゲットパラメータ値と比較すること
により画像ギャップを検出することを含む、態様61に記載の安全タグ読み取り装置。

〔態様73〕

前記ターゲットパラメータ値は、内側または外側のタグリムの厚さと直径比、または内

10

20

30

40

50

側または外側のタグリムの厚さとタグリムの破断幅比を含む、態様 7 2 に記載の安全タグ読み取り装置。

〔態様 7 4〕

前記潜在的な安全タグの正規化画像を生成することは、タグ特徴の向きを決定し、前記タグ特徴の前記決定された向きおよびスタイルシートから検索されたターゲットパラメータ値に基づいて前記画像を回転させることを含む、態様 6 1 に記載の安全タグ読み取り装置。

〔態様 7 5〕

前記タグ特徴は中央ロゴであり、前記ターゲットパラメータ値は中央ロゴの向きを含む、態様 7 4 に記載の安全タグ読み取り装置。

〔態様 7 6〕

前記潜在的な安全タグの正規化画像は、ベクトルグラフィックス画像を含む、態様 6 1 に記載の安全タグ読み取り装置。

〔態様 7 7〕

前記画像は複数の潜在的な安全タグを含み、
前記識別要求は、前記複数の潜在的な安全タグに対応するベクトルグラフィックス画像のストリームを含む、態様 6 1 に記載の安全タグ読み取り装置。

〔態様 7 8〕

前記識別要求は前記安全タグ読み取り装置の公開鍵を含み、
前記識別要求の少なくとも一部は、前記安全タグ読み取り装置の秘密鍵で暗号化される、態様 6 1 に記載の安全タグ読み取り装置。

〔態様 7 9〕

前記画像を使用して正規化安全タグ画像を生成することは、
前記安全タグ読み取り装置のユーザインターフェースに、前記画像と前記潜在的な安全タグを強調する表示とを表示する指示を提供することと、
前記潜在的な安全タグの第 2 のズームイン画像を生成する指示を受信することと、
前記潜在的な安全タグの第 2 のズームイン画像から前記正規化画像を生成することと、
を含む、態様 6 1 に記載の安全タグ読み取り装置。

〔態様 8 0〕

前記動作は、
前記安全タグ読み取り装置のユーザインターフェースに、前記画像と前記潜在的な安全タグを強調する表示とを表示する指示を提供することと、
前記潜在的な安全タグの選択を受信することと、
前記安全タグ読み取り装置のユーザインターフェースに前記安全タグデータを表示する手順を提供することと、
をさらに含む、態様 6 1 に記載の安全タグ読み取り装置。

〔態様 8 1〕

前記潜在的な安全タグを強調表示する前記表示は、前記画像内の前記潜在的な安全タグを囲む境界ボックスである、態様 8 0 に記載の安全タグ読み取り装置。

〔態様 8 2〕

前記スタイルシートの前記公的に利用可能な部分は、タグ特徴オプションとして前記安全タグにエンコードされた公開タグデータをデコードするための規則を提供する、態様 6 1 に記載の安全タグ読み取り装置。

〔態様 8 3〕

前記公開タグデータは、認証サーバのアドレス、製品タイプ、ブランド名、在庫番号、またはエラー訂正コードのうちの少なくとも 1 つを含む、態様 8 2 に記載の安全タグ読み取り装置。

〔態様 8 4〕

安全タグシステムであって、
少なくとも 1 つのプロセッサと、

10

20

30

40

50

前記少なくとも1つのプロセッサによって実行されたときに、
潜在的なタグ特徴オプションの選択としてタグデータをエンコードする安全タグをスキ
ャンすることと、
認証サーバと対話して前記安全タグをデコードすることと、
分散データベースに保存された前記安全タグの状態情報を受信し、前記状態情報は、前
記タグの有効性ステータスを示す、ことと、
を含む動作を前記安全タグシステムに実行させる命令を含む少なくとも1つの非一時的
メモリと、
を備える安全タグシステム。

〔態様 8 5〕

認証サーバと対話して前記安全タグをデコードすることは、前記安全タグの画像を前記
認証サーバに提供することを含む、態様 8 4 記載の安全タグシステム。

〔態様 8 6〕

認証サーバと対話して前記安全タグをデコードすることは、前記安全タグの知覚ハッシ
ュを前記認証サーバに提供することを含む、態様 8 4 に記載の安全タグシステム。

〔態様 8 7〕

認証サーバと対話して前記安全タグをデコードすることは、前記認証サーバに認証キー
を提供することを含む、態様 8 4 に記載の安全タグシステム。

〔態様 8 8〕

前記状態情報は、前記認証サーバから受信され、前記状態情報は、前記認証キーに依存
する、態様 8 7 に記載の安全タグシステム。

〔態様 8 9〕

前記安全タグをデコードするために前記認証サーバと対話することは、
前記認証サーバから、前記タグデータをエンコードする前記タグ特徴オプションを示す
デコード命令を受信することと、
前記デコード命令を使用して前記タグデータを生成し、前記タグデータはタグ識別子を
含む、ことと、
を含む、態様 8 4 に記載の安全タグシステム。

〔態様 9 0〕

分散データベースから前記安全タグの前記状態情報を受信することは、前記タグ識別子
をオラクルに提供することを含む、態様 8 9 に記載の安全タグシステム。

〔態様 9 1〕

分散データベースから前記安全タグの前記状態情報を受信することは、認証キーをオラ
クルに提供することをさらに含み、
受信した前記状態情報は前記認証キーに依存する、態様 9 0 に記載の安全タグシステム。

〔態様 9 2〕

前記認証キーは製造業者に対応し、前記状態情報は追跡情報、販売情報、顧客データ、
使用情報、活動情報、または位置情報のうちの少なくとも1つを含む、態様 9 1 に記載の
安全タグシステム。

〔態様 9 3〕

前記認証キーは卸業者に対応し、前記状態情報は、信頼性情報、宛先情報、または製造
業者情報のうちの少なくとも1つを含む、態様 9 1 に記載の安全タグシステム。

〔態様 9 4〕

前記認証キーは小売業者に対応し、前記状態情報は、信頼性情報、取引情報、製品情報
、または追跡情報のうちの少なくとも1つを含む、態様 9 1 に記載の安全タグシステム。

〔態様 9 5〕

前記認証キーは購入者に対応し、前記状態情報は、信頼性情報、製品情報、または所有
権情報のうちの少なくとも1つを含む、態様 9 1 に記載の安全タグシステム。

〔態様 9 6〕

前記動作は、前記分散データベースに保存するために、前記安全タグの更新された状態

10

20

30

40

50

情報を提供することをさらに含む、態様 1 に記載の安全タグシステム。

〔態様 9 7〕

前記安全タグの前記更新された状態情報は、認証キーとともに前記分散データベースに書き込むためにオラクルに提供される、態様 9 6 に記載の安全タグシステム。

〔態様 9 8〕

前記安全タグの前記更新された状態情報は、前記安全タグが無効であることを示す、態様 9 7 に記載の安全タグシステム。

〔態様 9 9〕

前記更新された状態情報は、前記状態情報に対する更新されたアクセシビリティオプションを含む、態様 8 4 に記載の安全タグシステム。

〔態様 1 0 0〕

前記安全タグの前記状態情報は、追跡情報、販売情報、顧客データ、使用情報、活動情報、位置情報、信頼性情報、宛先情報、更新された製造者情報、取引情報、製品データ、または所有権の証明情報の少なくとも 1 つを示す、態様 8 4 に記載の安全タグシステム。

〔態様 1 0 1〕

前記安全タグの前記状態情報は、前記安全タグと別の安全タグとの間のペアリングを示す、態様 8 4 に記載の安全タグシステム。

〔態様 1 0 2〕

安全タグシステムであって、
少なくとも 1 つのプロセッサと、
前記少なくとも 1 つのプロセッサによって実行されたときに、
潜在的な第 1 の安全タグ特徴オプションの選択として第 1 のタグデータをエンコードする第 1 の安全タグに関連付けられた製品に関する取引要求を受信することと、
潜在的な第 2 の安全タグ特徴オプションの選択として第 2 のタグ識別データをエンコードする前記製品に関する第 2 の安全タグを生成し、第 2 のタグデータは前記第 1 の安全タグの識別子および購入者の識別子を含む、ことと、

前記購入者への所有権の移転の表示を受信することと、
データベースに前記第 2 の安全タグのエントリを作成し、前記作成されたエントリは、前記所有権の移転を示す、ことと、を含む動作を前記安全タグシステムに実行させる命令を含む少なくとも 1 つの非一時的メモリと、
を備える安全タグシステム。

〔態様 1 0 3〕

前記製品はデジタル製品を含む、態様 1 0 2 に記載の安全タグシステム。

〔態様 1 0 4〕

前記第 1 の安全タグは、前記デジタル製品に埋め込まれるか、または前記デジタル製品と共に表示される、態様 1 0 3 に記載の安全タグシステム。

〔態様 1 0 5〕

前記製品は物理的製品を含む、態様 1 0 2 に記載の安全タグシステム。

〔態様 1 0 6〕

前記第 1 の安全タグは前記物理的製品にラベル付けする、態様 1 0 5 に記載の安全タグシステム。

〔態様 1 0 7〕

前記動作は、前記データベース内の前記第 1 の安全タグのエントリを更新することをさらに含む、態様 1 0 2 に記載の安全タグシステム。

〔態様 1 0 8〕

前記エントリは、前記所有権の移転、前記第 2 のタグの識別子、前記所有権の移転に関する取引情報、または前記第 1 の安全タグの有効性状態の少なくとも 1 つを示すように更新される、態様 1 0 7 に記載の安全タグシステム。

〔態様 1 0 9〕

前記第 1 の安全タグの前記識別子は、少なくともいくつかの前記第 1 のタグデータのハ

10

20

30

40

50

ッシュを含む、態様 1 0 2 に記載の安全タグシステム。

〔態様 1 1 0〕

前記第 2 の安全タグを生成することは、前記第 1 の安全タグをデコードして前記第 1 のタグデータを読み出すことを含む、態様 1 0 2 に記載の安全タグシステム。

〔態様 1 1 1〕

前記第 2 の安全タグは、前記第 1 の安全タグに関連付けられたスタイルシートを使用して生成される、態様 1 0 2 に記載の安全タグシステム。

〔態様 1 1 2〕

前記第 2 の安全タグは、固有の数値シードを使用して生成される、態様 1 0 2 に記載の安全タグシステム。

〔態様 1 1 3〕

データベースは分散データベースであり、

前記データベースに前記第 2 の安全タグの前記エントリを作成することは、ブロックチェーンに書き込むために、前記第 2 のタグの認証キーと識別子とをオラクルに提供することを含む、態様 1 0 2 に記載の安全タグシステム。

〔態様 1 1 4〕

安全タグと対話するためのサーバであって、

少なくとも 1 つのプロセッサと、

前記少なくとも 1 つのプロセッサによって実行されたときに、

潜在的な第 1 の安全タグ特徴オプションの選択として第 1 のタグデータをエンコードする第 1 の安全タグに関する要求を受信し、前記第 1 のタグデータは保存された文脈情報を含むことと、

前記保存された文脈情報をデコードすることと、

文脈情報を受信することと、

前記受信した文脈情報と前記保存された文脈情報とを使用して前記要求を認証することと、

前記要求に応じて認証が成功したことを示すことと、を含む動作を前記サーバに実行させる命令を含む少なくとも 1 つの非一時的メモリと、

を備えるサーバ。

〔態様 1 1 5〕

前記保存された文脈情報は、認証信任状、生体認証識別子、音声ファイル、タグ識別子、または画像の知覚ハッシュのうちの少なくとも 1 つを含む、態様 1 1 4 に記載のサーバ。

〔態様 1 1 6〕

前記生体認証識別子は、指紋または声紋を含む、態様 1 1 5 に記載のサーバ。

〔態様 1 1 7〕

前記第 1 の安全タグは項目にラベル付けし、前記画像は前記項目の一部を示す、態様 1 1 5 に記載のサーバ。

〔態様 1 1 8〕

前記ラベル付き項目は身分証明書であり、

前記項目の前記一部は、身分証明書の身分証明書写真である、態様 1 1 7 に記載のサーバ。

〔態様 1 1 9〕

前記第 1 の安全タグは項目にラベル付けし、前記画像は、前記項目に関連付けられた人物または前記項目のテキストチャを示す、態様 1 1 5 に記載のサーバ。

〔態様 1 2 0〕

前記要求を認証することは、前記受信した文脈情報および前記保存された文脈情報が類似性基準を満たすと判定することを含む、態様 1 1 4 に記載のサーバ。

〔態様 1 2 1〕

前記類似性基準の充足度は、前記受信した文脈情報と前記保存された文脈情報との間のハミング距離に依存する、態様 1 2 0 に記載のサーバ。

10

20

30

40

50

〔態様 1 2 2〕

前記動作は、前記文脈情報を要求することをさらに含み、

前記受信した文脈情報は、前記要求への応答として受信される、態様 1 1 4 に記載のサーバ。

〔態様 1 2 3〕

前記認証成功の表示は、前記第 1 のタグデータの少なくとも一部を含む、態様 1 1 4 に記載のサーバ。

〔態様 1 2 4〕

前記認証成功の表示は、前記第 1 のタグデータの少なくともいくつかに対する命令をデコードすることを含む、態様 1 1 4 に記載のサーバ。

〔態様 1 2 5〕

前記認証成功の表示は、分散データベースから読み出されたステータス情報を含む、態様 1 1 4 に記載のサーバ。

〔態様 1 2 6〕

前記ステータス情報は、オラクルを使用して分散データベースから読み出される、態様 1 1 4 に記載のサーバ。

〔態様 1 2 7〕

潜在的な第 1 の安全タグ特徴オプションの選択として第 1 のタグデータをエンコードする第 1 の安全タグでラベル付けされた基板と、

前記基板に取り外し可能に接着されたオーバーレイであって、前記第 1 の安全タグと位置合わせされる透明部分および不透明部分を含み、前記第 1 の安全タグと位置合わせされた不透明部分とは、潜在的な第 2 の安全タグ特徴オプションの選択として第 2 のタグデータをエンコードする、オーバーレイと、

を備える 2 部構成ラベル。

〔態様 1 2 8〕

前記潜在的な第 1 の安全タグ特徴オプションは、前記潜在的な第 2 の安全タグ特徴オプションとは異なる、態様 1 2 7 に記載の 2 部構成ラベル。

〔態様 1 2 9〕

前記位置合わせされた不透明部分は、選択された潜在的な第 1 の安全タグ特徴オプションを隠す、態様 1 2 7 に記載の 2 部構成ラベル。

〔態様 1 3 0〕

前記位置合わせされた不透明部分が、潜在的な第 1 の安全タグ特徴オプションを選択する、態様 1 2 7 に記載の 2 部構成ラベル。

〔態様 1 3 1〕

前記潜在的な第 1 の安全タグ特徴オプションは、第 1 の安全タグレイアウトによって指定される位置におけるタグ特徴の有無を含む、態様 1 2 7 に記載のシステム。

〔態様 1 3 2〕

前記潜在的な第 2 の安全タグ特徴オプションは、前記第 1 の安全タグレイアウトとは異なる第 2 の安全タグレイアウトにより指定される位置におけるタグ特徴の有無を含む、態様 1 3 1 に記載のシステム。

〔態様 1 3 3〕

第 1 のタグデータ、第 1 の数値シード、および第 1 のスタイルシートを使用して、潜在的な第 1 の安全タグ特徴オプションの選択として第 1 のタグデータをエンコードする第 1 の安全タグを生成することと、

第 2 のタグデータ、第 2 の数値シード、および第 2 のスタイルシートを使用して、潜在的な第 2 の安全タグ特徴オプションの選択として第 2 のタグデータをエンコードする第 2 の安全タグを生成することと、

前記第 1 の安全タグと前記第 2 の安全タグとの間の差分画像を判定することと、

前記第 1 の安全タグで基板にラベルを付けることと、

前記基板にオーバーレイを取り外し可能に接着し、前記差分画像で過度にラベル付けし

10

20

30

40

50

、第1の安全タグと位置合わせされることと、
を含む、2部構成ラベルを生成する方法。

〔態様134〕

前記オーバーレイは、前記第2の安全タグに存在しない前記第1の安全タグの部分を隠す、態様133に記載の方法。

〔態様135〕

前記オーバーレイは、前記第1の安全タグに存在しない前記第2の安全タグの部分を示す、態様133に記載の方法。

〔態様136〕

前記オーバーレイは、前記第1の安全タグに存在する前記第2の安全タグの部分を送信する、態様133に記載の方法。

〔態様137〕

前記第1のスタイルシートは、前記第2のスタイルシートとは異なる、態様133に記載の方法。

〔態様138〕

前記基材は消費財を含む、態様133に記載の方法。

〔態様139〕

前記第1の安全タグは、前記消費財の購入後状態に対応し、前記第2の安全タグは、前記消費財の購入前状態に対応する、態様138に記載の方法。

〔態様140〕

文書を提供する方法であって、
文書と対になった第1の安全タグを生成し、前記第1の安全タグは、潜在的なタグ特徴オプションの選択を使用して前記文書の識別子をエンコードすることと、
第1の装置から前記文書へのアクセス要求を受信することと、
前記第1の装置に前記第1の安全タグを提供することと、
安全タグ画像を含む確認要求を第2の装置から受信することと、
前記第1の安全タグを前記安全タグ画像と比較することと、
前記比較に基づいて前記第1の装置に前記文書を提供することと、
を含む、方法。

〔態様141〕

前記文書の前記識別子は、前記文書のハッシュを含む、態様140に記載の方法。

〔態様142〕

前記第1の安全タグを前記安全タグ画像と比較することは、
前記第1の安全タグの知覚ハッシュを生成することと、
前記安全タグ画像の知覚ハッシュを生成することと、
前記保存された知覚ハッシュと前記生成された知覚ハッシュとの差がしきい値基準を満たすと判定することと、
を含む、態様140に記載の方法。

〔態様143〕

前記第1の安全タグを前記安全タグ画像と比較することは、
前記安全タグ画像の知覚ハッシュを生成することと、
前記生成された知覚ハッシュと、前記第1の安全タグの画像の保存された知覚ハッシュとの差を使用して、第1の安全タグを選択することと、
前記安全タグ画像の所定のセグメントの第2の知覚ハッシュを生成することと、
前記生成された第2の知覚ハッシュと、第1の安全タグの画像の所定の部分の保存された第2の知覚ハッシュとの差を使用して、複数の前記第1の安全タグから前記第1の安全タグを選択することと、
を含む、態様140に記載の方法。

〔態様144〕

前記確認要求は確認要求識別子を含み、

10

20

30

40

50

前記比較に基づいて前記文書を前記第1の装置に提供することは、
前記要求と対になった第2の安全タグを生成し、前記第2の安全タグは、潜在的なタグ
特徴オプションの選択を使用して前記確認要求識別子をエンコードすることと、
前記第2の安全タグで前記文書に透かしを入れることと、
をさらに含む、態様140に記載の方法。

[態様145]

前記第2の装置はモバイル装置である、態様140に記載の方法。

[態様146]

前記安全タグ画像の前記受信が認証基準を満たすと判定することをさらに含む、態様1
40に記載の方法。

[態様147]

前記認証基準は、前記第1の安全タグに関連するいくつかの確認要求に関係する、態様
146に記載の方法。

[態様148]

前記認証基準は、前記第1の装置への前記第1の安全タグの前記提供からの経過時間に
関する、態様146に記載の方法。

[態様149]

前記認証基準は、前記確認要求の地理的起源に関係する、態様146に記載の方法。

[態様150]

前記確認要求は確認要求識別子を含み、

前記認証基準は前記確認要求識別子に関係する、態様146に記載の方法。

[態様151]

前記認証基準は、前記アクセス要求のアクセス識別子が前記確認要求の確認識別子と一
致する場合に満たされる、態様150に記載の方法。

[態様152]

可変安全タグを生成するためのシステムであって、

少なくとも1つのプロセッサと、

前記少なくとも1つのプロセッサによって実行されたときに、

タグデータの値に応じたタグ特徴オプションの選択として、前記タグデータをエンコー
ドする第1の安全タグを生成することと、

第2の装置のスキャナから、第1のタグ画像を含むタグ画像のシーケンスを含む要求を
受信することと、

前記第1の安全タグと前記第1のタグ画像とを使用して前記要求を認証することと、

前記要求の前記認証の表示を提供することと、を含む操作を前記システムに実行させる
命令を含む少なくとも1つの非一時的メモリと、

を備えるシステム。

[態様153]

前記動作は、第1の装置のディスプレイ上に前記第1の安全タグを含むタグのシーケン
スを表示する命令を提供することをさらに含む、態様152に記載のシステム。

[態様154]

前記第1の安全タグを含むタグのシーケンスを表示する命令を提供することは、前記タ
グのシーケンスをデジタル製品に埋め込むことを含む、態様153に記載のシステム。

[態様155]

前記命令は、トリガに応答して、前記第1の装置のディスプレイのタグのシーケンスを
表示することを提供する、態様153に記載のシステム。

[態様156]

前記スキャナはカメラである、態様152に記載のシステム。

[態様157]

前記要求を認証することは、前記第1の安全タグの1つ以上の知覚ハッシュを、前記第
1のタグ画像の1つ以上の対応するハッシュと比較することを含む、態様152に記載の

10

20

30

40

50

システム。

〔態様 1 5 8〕

前記要求を認証することは、前記第 1 の安全タグを含む複数の安全タグを、前記第 1 のタグ画像を含む複数の対応するタグ画像に一致させることを含む、態様 1 5 2 に記載のシステム。

〔態様 1 5 9〕

前記認証は、所定の出現順序に従って、前記複数の安全タグを前記複数の対応するタグ画像に一致させることをさらに要求する、態様 1 5 8 に記載のシステム。

〔態様 1 6 0〕

前記タグのシーケンスはジャンクタグを含む、態様 1 5 2 に記載のシステム。

〔態様 1 6 1〕

前記トリガは、ロールオーバーイベントまたはクリックイベントである、態様 1 5 2 に記載のシステム。

〔態様 1 6 2〕

前記要求の認証の前記表示は、前記タグデータの少なくともいくつかを含む、態様 1 5 2 に記載のシステム。

〔態様 1 6 3〕

前記要求の認証の前記表示は、前記第 1 のタグデータの少なくともいくつかをデコードするためのデコード命令を含む、態様 1 5 2 に記載のサーバ。

〔態様 1 6 4〕

前記要求の認証の表示は、データベースから読み出されたステータス情報を含む、態様 1 5 2 に記載のサーバ。

〔態様 1 6 5〕

前記データベースは分散データベースであり、
前記ステータス情報は、オラクルを使用して分散データベースから取得される、態様 1 5 2 に記載のサーバ。

〔態様 1 6 6〕

数値シードとスタイルシートの組み合わせに基づくタグ特徴オプションの選択として製品識別データをエンコードするコンピュータ読み取り可能な安全な追跡タグにより製品にラベル付けすることを含む、製品を追跡する方法。

〔態様 1 6 7〕

前記タグ特徴オプションは、前記数値シードと前記スタイルシートとの組み合わせによって指定される位置におけるタグ特徴の有無を含む、態様 1 6 6 に記載の方法。

〔態様 1 6 8〕

前記タグ特徴オプションは、タグ特徴のサイズ、色、または形状を含む、態様 1 6 6 に記載の方法。

〔態様 1 6 9〕

前記タグ特徴オプションは、前記数値シードと前記スタイルシートとの組み合わせによって指定される位置からの逸脱を含む、態様 1 6 6 に記載の方法。

〔態様 1 7 0〕

前記タグ特徴オプションは、前記数値シードと前記スタイルシートとの組み合わせによって指定される位置に存在するいくつかのタグ特徴を含む、態様 1 6 6 に記載の方法。

〔態様 1 7 1〕

前記タグ特徴オプションは、前記タグ特徴上のスプラインエンコードの存在を含む、態様 1 6 6 に記載の方法。

〔態様 1 7 2〕

前記スプラインエンコードは、基準点または基準線から様々な距離に延びるタグ特徴端を含む、態様 1 7 1 に記載の方法。

〔態様 1 7 3〕

前記様々な距離は、1 つ以上の空間的に多重化されたタグデータ値をエンコードする、

10

20

30

40

50

態様 172 に記載の方法。

〔態様 174〕

前記様々な距離は、前記 1 つ以上の空間的に多重化されたタグデータ値の繰り返しをエンコードする、態様 173 に記載の方法。

〔態様 175〕

前記タグ特徴オプションは、前記タグ特徴上の微細構造の存在を含む、態様 166 に記載の方法。

〔態様 176〕

前記タグ特徴はリムを含み、前記リムのタグ特徴オプションは、リム破損、リム変形、およびリム接続を含む、態様 166 に記載の方法。

〔態様 177〕

前記タグ特徴はリム破損を含み、前記リム破損のタグ特徴オプションはリム破損端形状を含む、態様 166 に記載の方法。

〔態様 178〕

前記タグ特徴は、所定のタイプのタグ特徴間の接続を含み、前記接続のためのタグ特徴オプションは、接続幅および接続非対称を含む、態様 166 に記載の方法。

〔態様 179〕

前記タグ特徴は、タグ特徴間の接続を含み、前記接続のためのタグ特徴オプションは、接続幅および接続非対称を含む、態様 166 に記載の方法。

〔態様 180〕

前記タグ特徴は中央ロゴを含み、前記タグ特徴オプションは、前記安全タグの中心点からの前記中央ロゴの変位を含む、態様 166 に記載の方法。

〔態様 181〕

前記方法は、前記コンピュータ可読の安全追跡タグを生成することをさらに含む、態様 166 に記載の方法。

〔態様 182〕

前記コンピュータ可読の安全追跡タグを生成することは、前記製品識別データの第 1 の値に従って第 1 のタグ特徴オプションを選択し、前記第 1 のタグ特徴オプションの選択は第 2 のタグ特徴オプションを作成することと、前記製品識別データの第 2 の値に従って前記第 2 のタグ特徴オプションを選択することと、を含む、態様 181 の方法。

〔態様 183〕

前記第 1 のタグ特徴オプションはポイントの有無を含み、前記第 2 のタグ特徴オプションは前記第 1 の値に従って存在するポイント間の接続の有無を含み、製品識別データの第 3 の値をエンコードする第 3 のタグ特徴オプションは、前記第 2 の値に従って存在する接続の幅を含む、態様 182 に記載の方法。

〔態様 184〕

前記コンピュータ可読の安全追跡タグを生成することは、
前記製品識別データの少なくとも一部を暗号化キーで暗号化することと、
前記製品識別データの前記暗号化された部分の値に従って第 1 のタグ特徴オプションを選択することと、
コンピュータ可読の安全追跡タグに前記暗号化キーをエンコードすることと、
を含む、態様 181 に記載の方法。

〔態様 185〕

前記コンピュータ可読の安全追跡タグはベクトルグラフィックファイルを含み、前記製品をコンピュータ可読の安全追跡タグでラベル付けすることは前記ベクトルグラフィックファイルをラスタライズすることを含む、態様 166 に記載の方法。

〔態様 186〕

前記方法は、前記コンピュータ可読の安全追跡タグの識別情報を認証サーバに提供することをさらに含む、態様 166 に記載の方法。

〔態様 187〕

10

20

30

40

50

前記方法は、前記コンピュータ可読の安全追跡タグのハッシュを生成し、前記識別情報を前記認証サーバに提供する前に、他のコンピュータ可読の安全追跡タグのハッシュとの衝突についてハッシュをチェックすることをさらに含む、態様 186 に記載の方法。

〔態様 188〕

数値シードとスタイルシートとの組み合わせに基づくタグ特徴オプションの選択として製品識別データをエンコードするコンピュータ可読の安全追跡タグが印刷された基材を含む、製品を追跡するためのラベル。

〔態様 189〕

前記タグ特徴オプションは、前記数値シードと前記スタイルシートとの組み合わせによって指定される位置におけるタグ特徴の有無を含む、態様 188 に記載のラベル。

〔態様 190〕

前記タグ特徴オプションは、タグ特徴のサイズ、色、または形状を含む、態様 188 に記載のラベル。

〔態様 191〕

前記タグ特徴オプションは、前記数値シードと前記スタイルシートとの組み合わせによって指定される位置からの逸脱を含む、態様 188 に記載のラベル。

〔態様 192〕

前記タグ特徴オプションは、前記数値シードと前記スタイルシートとの組み合わせによって指定される位置に存在するいくつかのタグ特徴を含む、態様 188 に記載のラベル。

〔態様 193〕

前記タグ特徴オプションは、前記タグ特徴上のスプラインエンコードの存在を含む、態様 188 に記載のラベル。

〔態様 194〕

前記スプラインエンコードは、基準点または基準線から様々な距離に延びるタグ特徴端を含む、態様 193 に記載のラベル。

〔態様 195〕

前記様々な距離は、1つ以上の空間的に多重化されたタグデータ値をエンコードする、態様 194 に記載のラベル。

〔態様 196〕

前記様々な距離は、前記 1つまたは複数の空間多重化タグデータ値の繰り返しをエンコードする、態様 195 に記載のラベル。

〔態様 197〕

前記タグ特徴オプションは、前記タグ特徴上の微細構造の存在を含む、態様 188 に記載のラベル。

〔態様 198〕

前記タグ特徴はリムを含み、前記リムのタグ特徴オプションは、リム破損、リム変形、およびリム接続を含む、態様 188 に記載のラベル。

〔態様 199〕

前記タグ特徴はリム破損を含み、前記リム破損用の前記タグ特徴オプションはリム破損端形状を含む、態様 188 に記載のラベル。

〔態様 200〕

前記タグ特徴は、所定のタイプのタグ特徴間の接続を含み、前記接続のためのタグ特徴オプションは、接続幅および接続非対称を含む、態様 188 に記載のラベル。

〔態様 201〕

前記タグ特徴は、タグ特徴間の接続を含み、前記接続のためのタグ特徴オプションは、接続幅および接続非対称を含む、態様 188 に記載のラベル。

〔態様 202〕

前記タグ特徴は中央ロゴを含み、前記タグ特徴オプションは前記安全タグの中心点からの前記中央ロゴの変位を含む、態様 188 に記載のラベル。

10

20

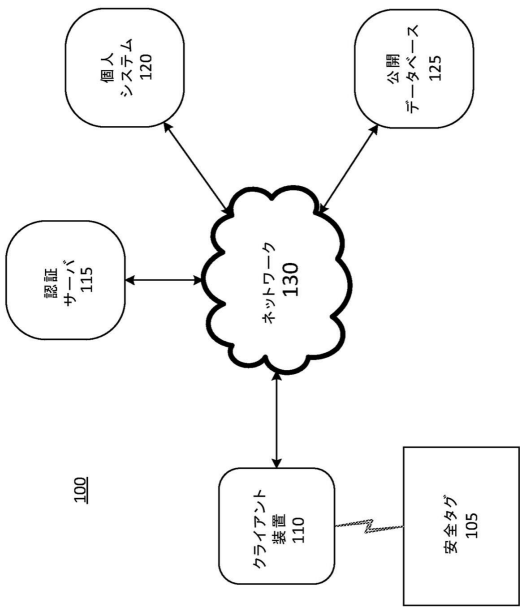
30

40

50

【図面】

【図 1】



【図 2】

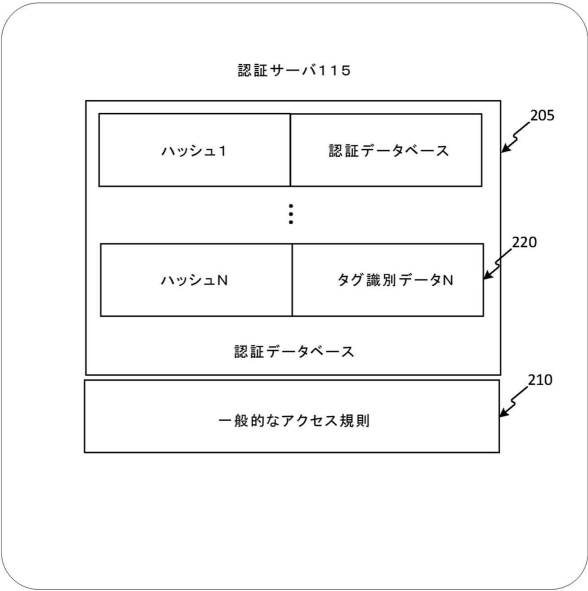


図 1

図 2

【図 3】

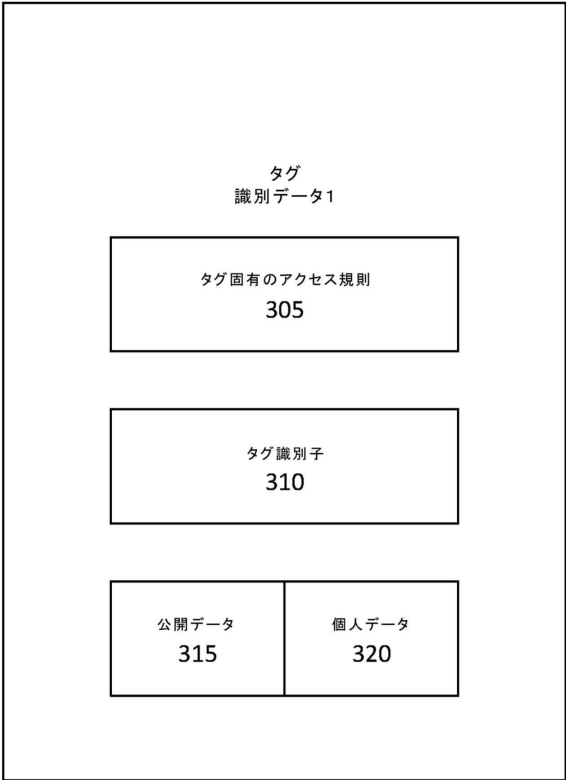


図 3

【図 4】

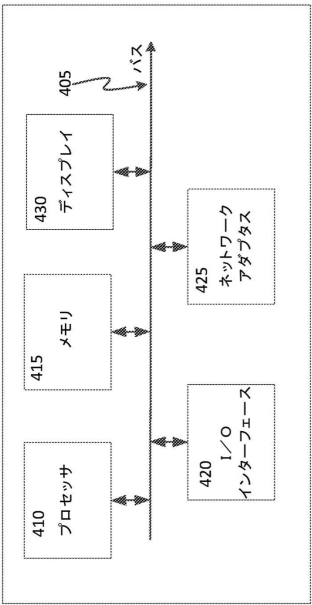


図 4

10

20

30

40

50

【図 5】

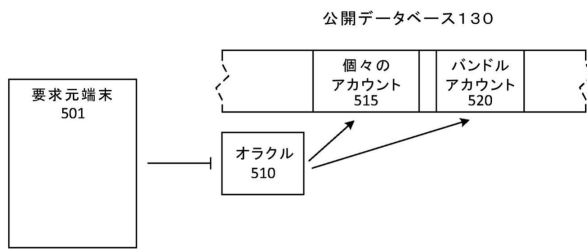


図 5

【図 6】

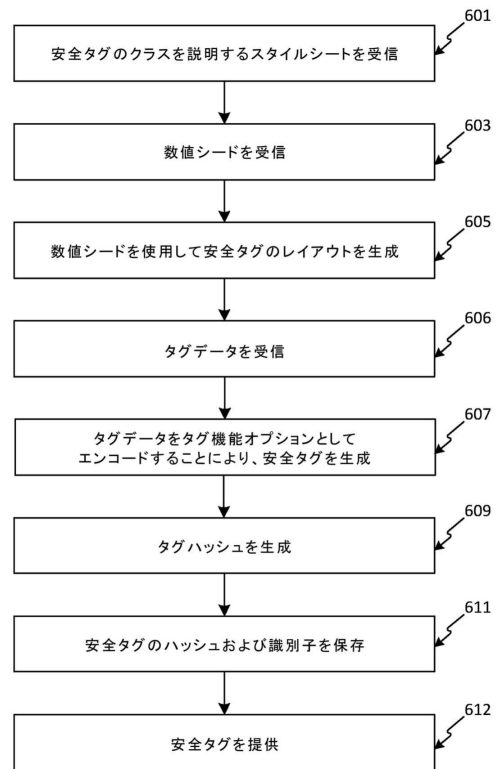


図 6

【図 7】

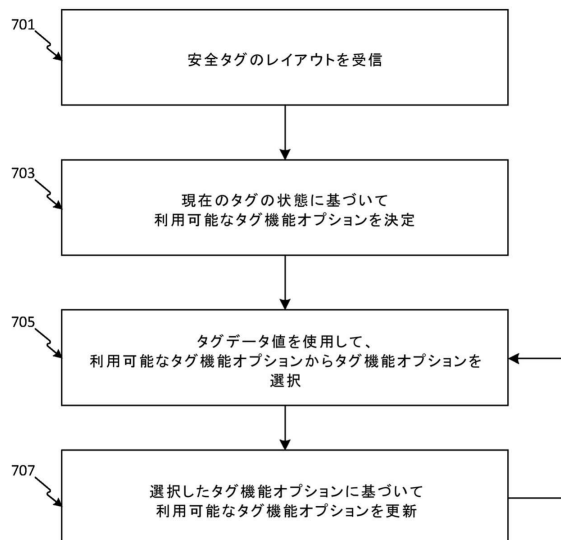


図 7

【図 8】

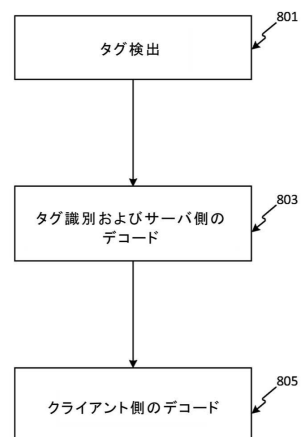


図 8

10

20

30

40

50

【図 9】

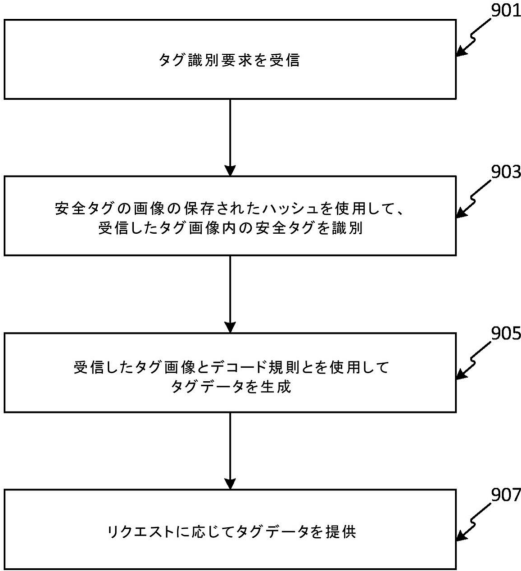


図 9

【図 10】

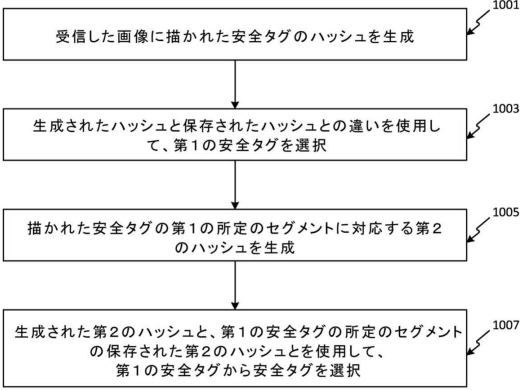


図 10

【図 11】

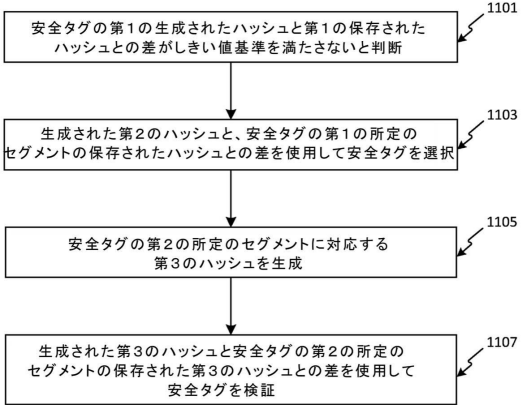


図 11

【図 12】

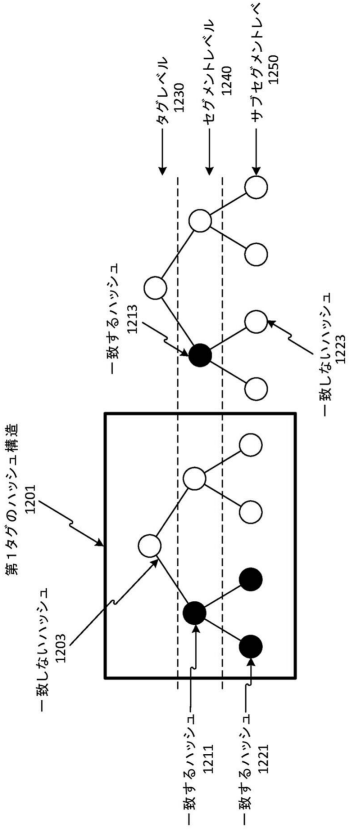


図 12

【図 13】

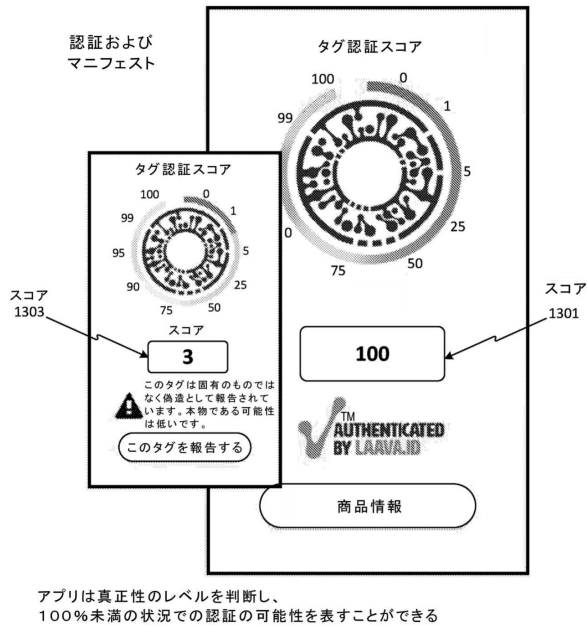


図 13

【図 14】

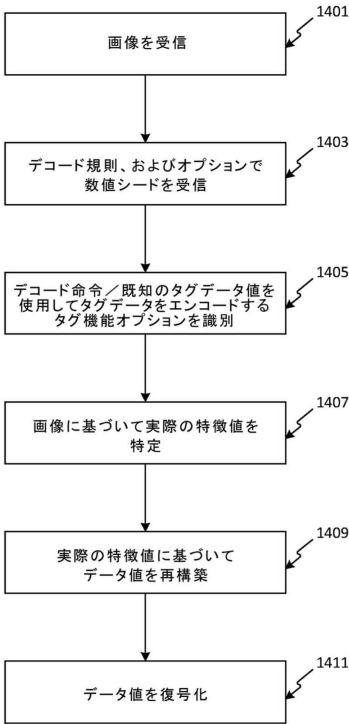


図 14

【図 15】

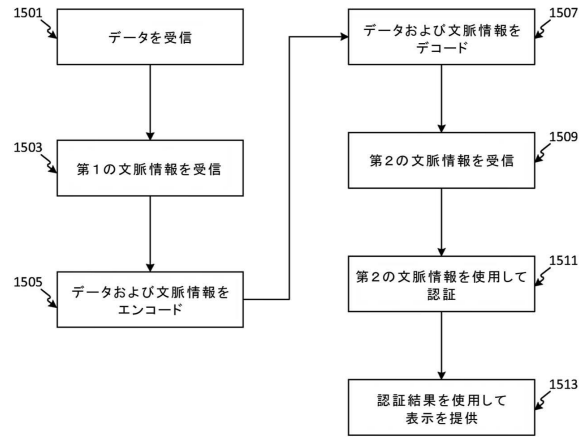


図 15

【図 16 A】

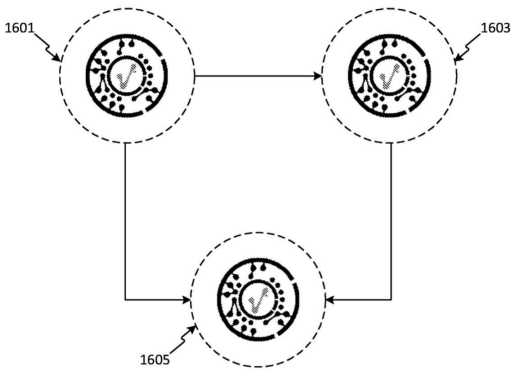


図 16A

10

20

30

40

50

【図 1 6 B】

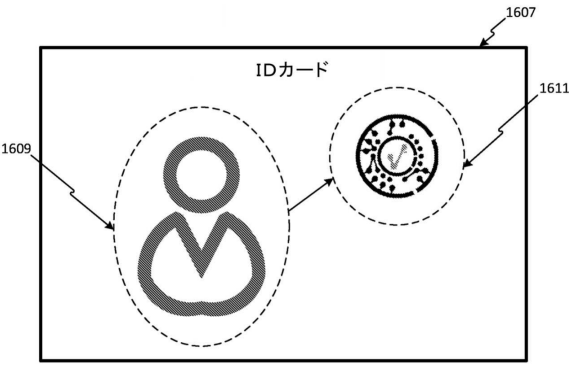


図 16B

【図 1 7】

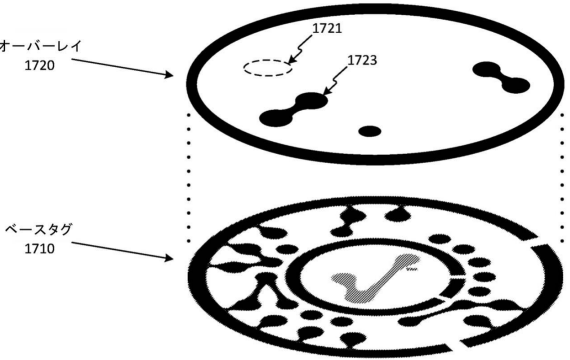


図 17

【図 1 8】

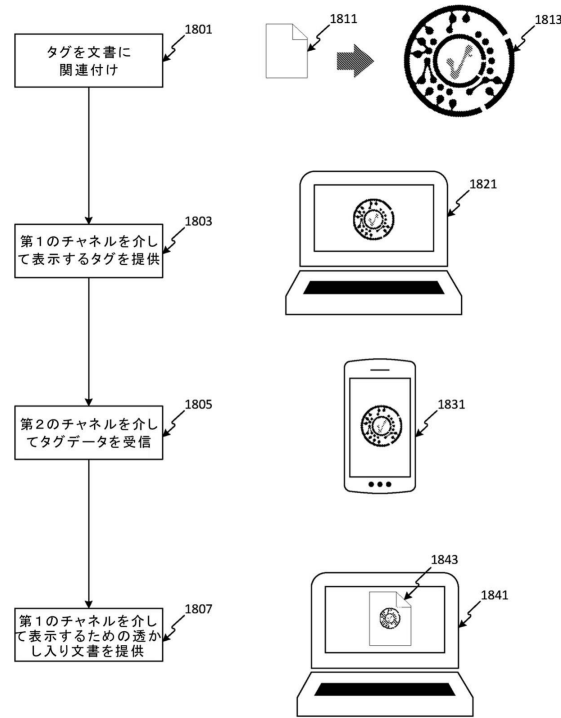


図 18

【図 1 9】

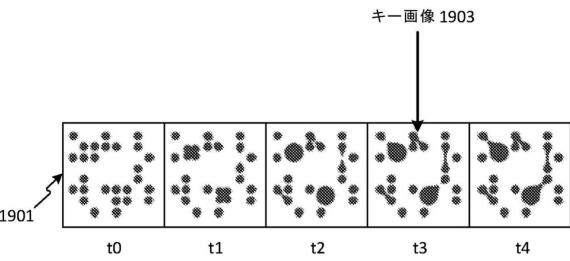


図 19

10

20

30

40

50

【図 20】

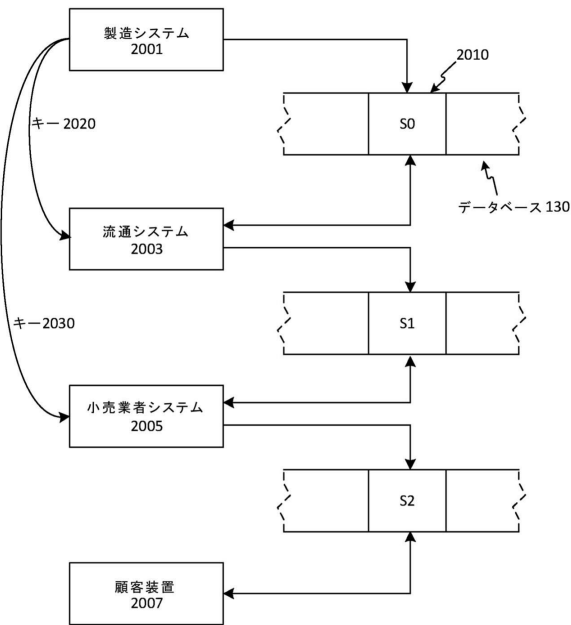


図 20

【図 21】

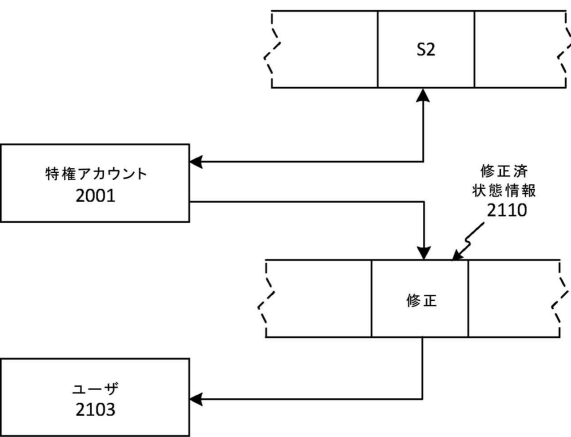


図 21

【図 22】

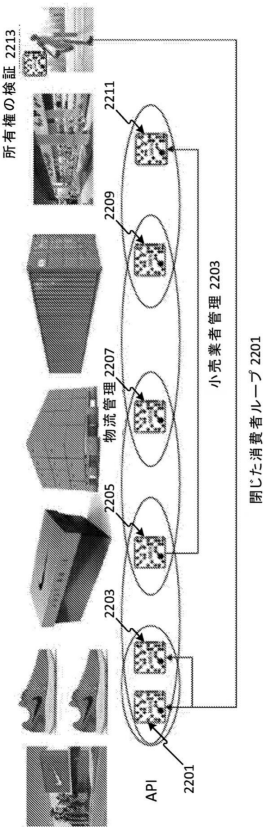


図 22

【図 23】

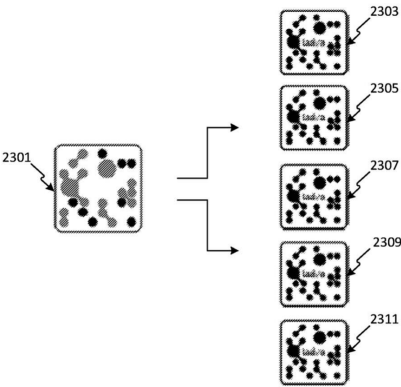


図 23

10

20

30

40

50

【図 2 4 A】

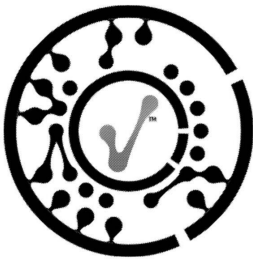


図 24A

【図 2 4 B】



図 24B

10

【図 2 5 A】

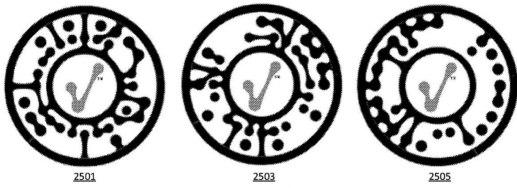


図 25A

【図 2 5 B】



図 25B

20

30

40

50

【図 2 6 A】

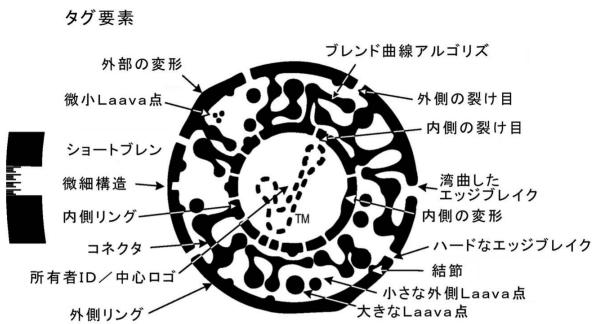


図 26A

【図 2 6 B】

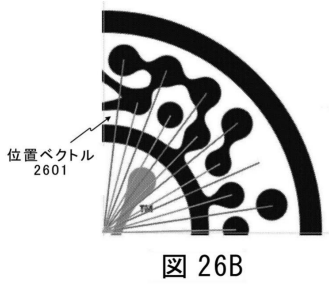


図 26B

10

【図 2 6 C】

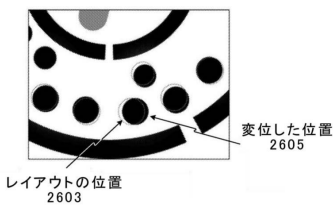


図 26C

【図 2 6 D】

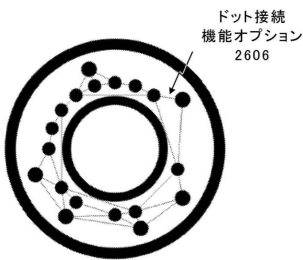


図 26D

20

30

40

50

【図 2 6 E】

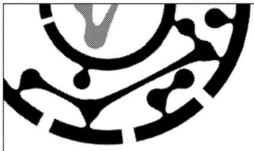


図 26E

【図 2 6 F】

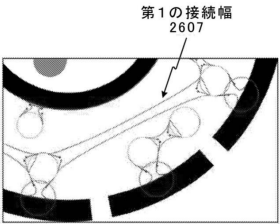


図 26F

10

【図 2 6 G】

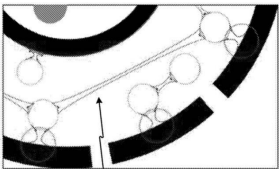


図 26G

【図 2 6 H】

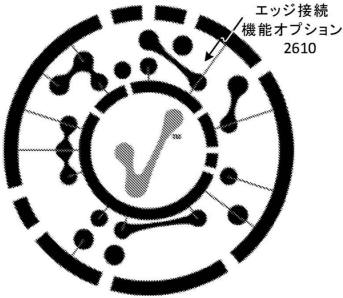


図 26H

20

30

40

50

【図 2 6 I】

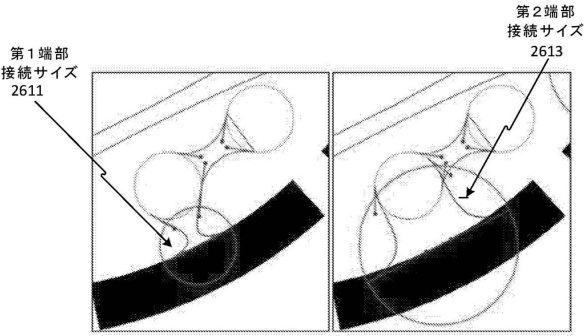


図 26I

【図 2 6 J】

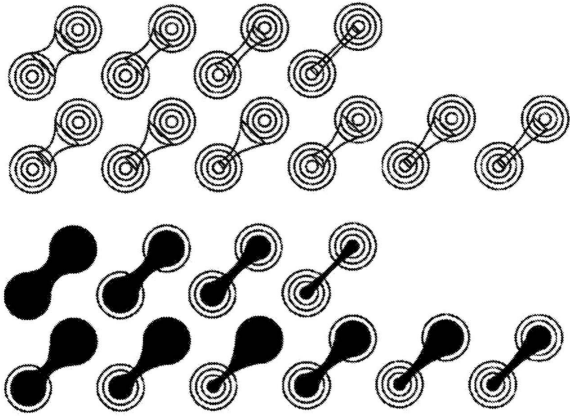


図 26J

【図 2 6 K】

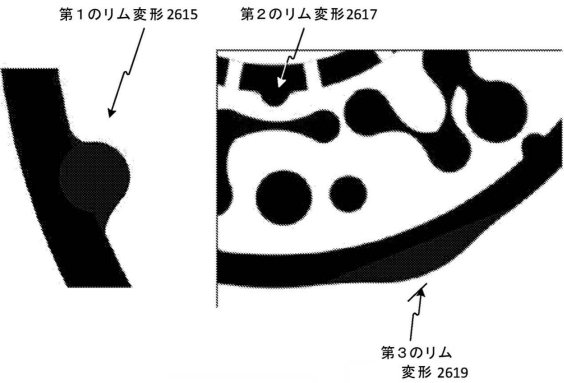


図 26K

【図 2 6 L】

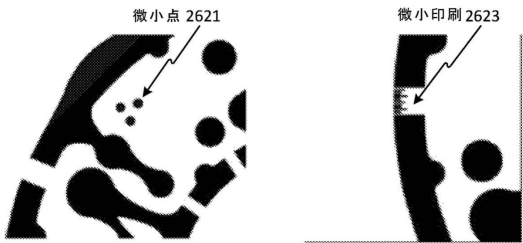


図 26L

10

20

30

40

50

【図 2 6 M】

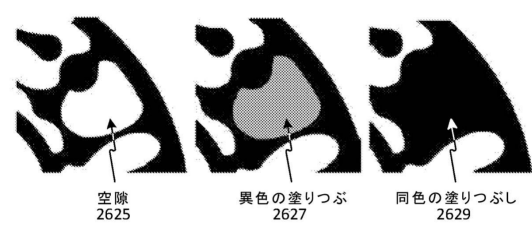


図 26M

【図 2 6 N】

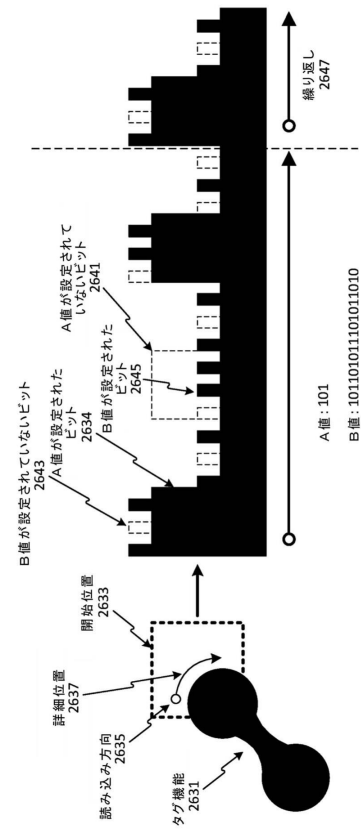


図 26N

【図 2 7 A】

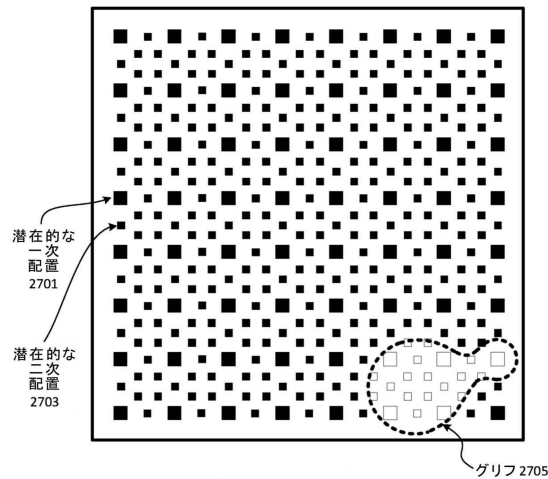


図 27A

【図 2 7 B】

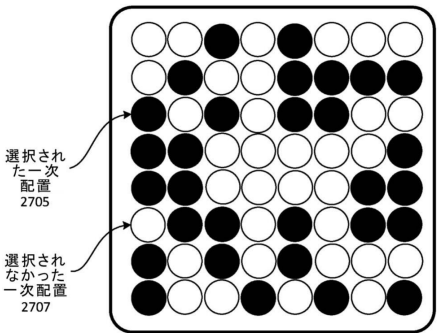


図 27B

10

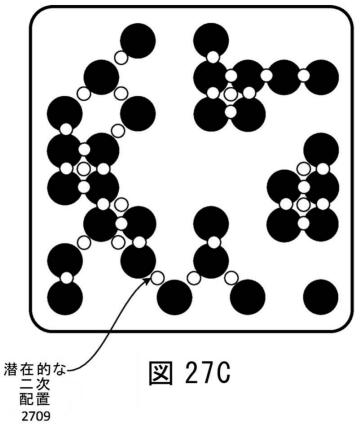
20

30

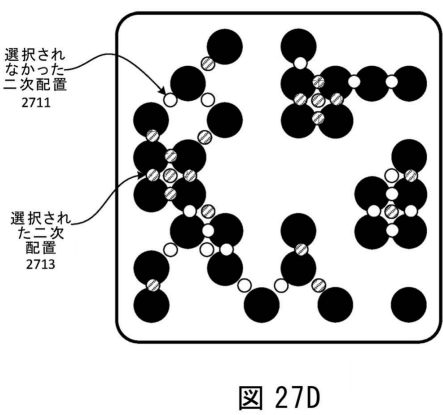
40

50

【図 2 7 C】



【図 2 7 D】



10

【図 2 7 E】

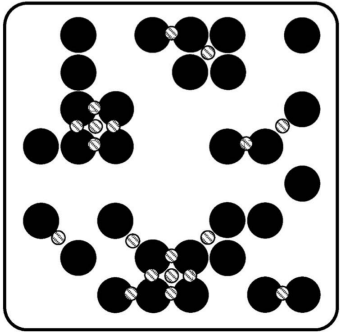
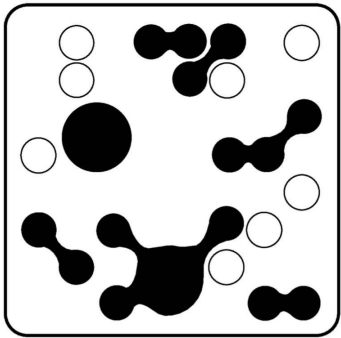
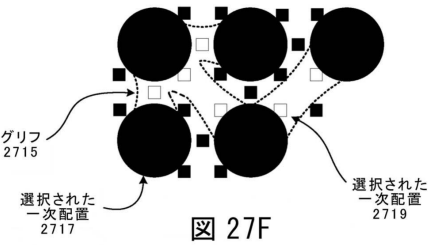


図 27E

【図 2 7 F】



選択された一次配置 2719

20

30

40

50

【図 27 G】

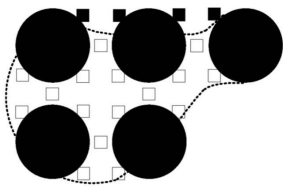


図 27G

【図 27 H】

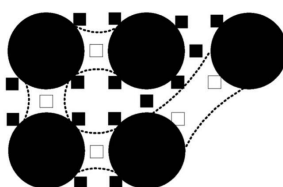


図 27H

10

【図 27 I】

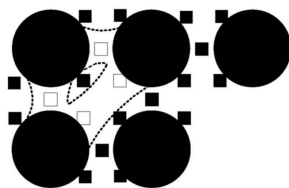


図 27I

【図 27 J】

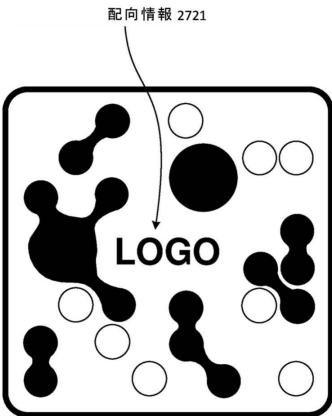


図 27J

20

30

40

50

【図 28 A】

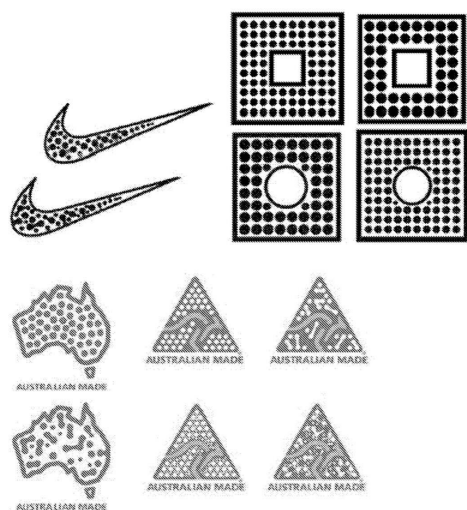


図 28A

【図 28 B】

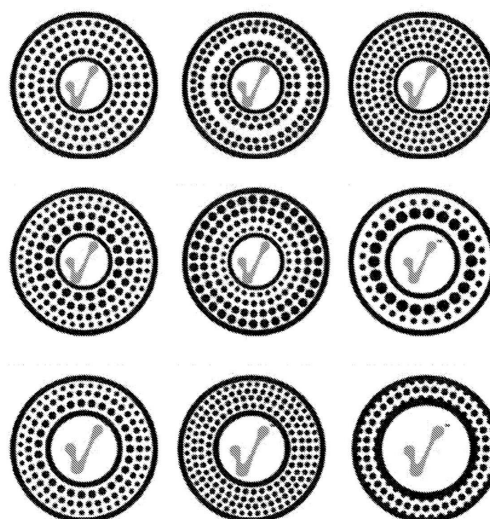


図 28B

【図 28 C】

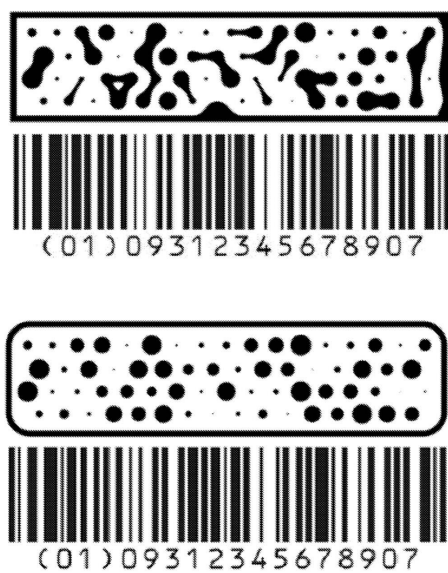


図 28C

【図 28 D】

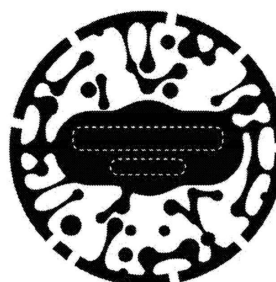


図 28D

10

20

30

40

50

【図 28 E】

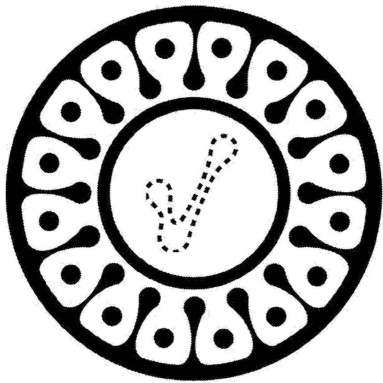


図 28E

【図 28 F】

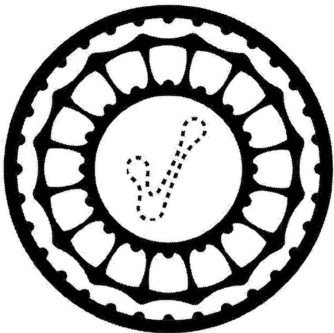


図 28F

10

【図 28 G】

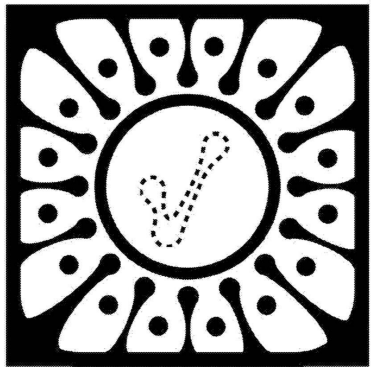


図 28G

【図 28 H】

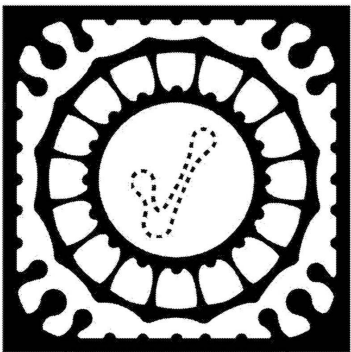


図 28H

20

30

40

50

【図 28 I】

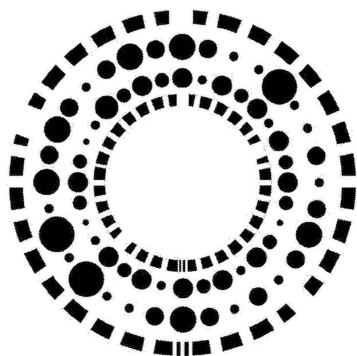


図 28I

【図 28 J】

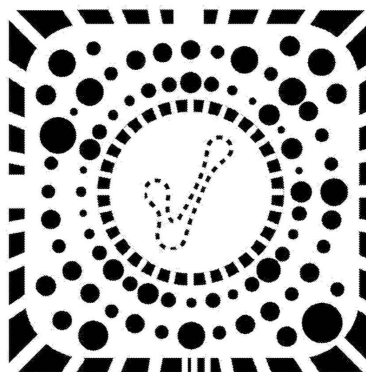


図 28J

10

【図 28 K】

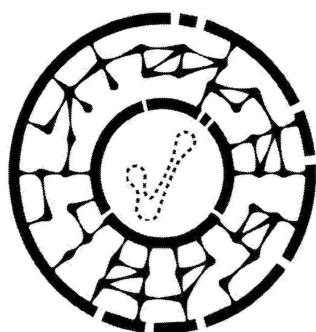


図 28K

【図 28 L】

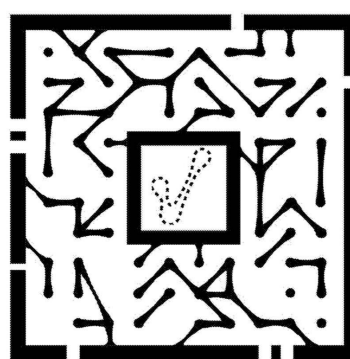


図 28L

20

30

40

50

【図 28 M】

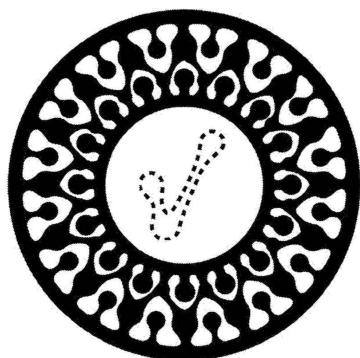


図 28M

【図 28 N】



図 28N

10

【図 29 A】



図 29A

【図 29 B】

[illegible]

29B

20

30

40

50

フロントページの続き

- 弁理士 河野 努
(74)代理人 100196601
弁理士 酒井 祐市
(72)発明者 イアン ジェイムズ マクドナルド
オーストラリア国, ニュー サウス ウェールズ 2030, ボークルーズ, キングス ロード 75
(72)発明者 パトリック ルネ フィリップ ミッシェル
オーストラリア国, ニュー サウス ウェールズ 2088, モスマン, ミドル ヘッド ロード 43
(72)発明者 アントニー サーティーズ
オーストラリア国, ニュー サウス ウェールズ 2030, ワトソンズ ベイ, ソールズベリー ス
トリート 1エー
(72)発明者 モーガン リーン
オーストラリア国, ニュー サウス ウェールズ 2043, アースキンビル, シドニー パーク ロ
ード 221
審査官 松浦 功
(56)参考文献 国際公開第2016/202827 (WO, A1)
米国特許出願公開第2007/0278316 (US, A1)
米国特許第05798514 (US, A)
特開2009-151700 (JP, A)
国際公開第2013/061468 (WO, A1)
米国特許第09331856 (US, B1)
特開2009-163720 (JP, A)
米国特許出願公開第2003/0009350 (US, A1)
米国特許出願公開第2015/0147585 (US, A1)
米国特許出願公開第2014/0263674 (US, A1)
米国特許出願公開第2012/0048936 (US, A1)
米国特許出願公開第2006/0007255 (US, A1)
米国特許第05774639 (US, A)
(58)調査した分野 (Int.Cl., DB名)
G06T 7/00 - 7/90
B42D 25/351
G06K 1/00 - 7/14
G06K 19/06
G06T 1/00
G06V 10/00 - 20/90