(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2016-512675
(P2016-512675A)
(43)公表日　平成28年4月28日(2016.4.28)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/32	***(2006.01)***	H04L	9/00	675B	5J104
G06F 21/44	***(2013.01)***	H04L	9/00	675A	
		G06F	21/44		

審査請求 未請求　予備審査請求 未請求　（全 50 頁）

(21)出願番号　特願2016-501739 (P2016-501739)
(86)(22)出願日　平成26年3月12日 (2014.3.12)
(85)翻訳文提出日　平成27年10月23日 (2015.10.23)
(86)国際出願番号　PCT/US2014/025085
(87)国際公開番号　WO2014/165284
(87)国際公開日　平成26年10月9日 (2014.10.9)
(31)優先権主張番号　61/778,122
(32)優先日　平成25年3月12日 (2013.3.12)
(33)優先権主張国　米国 (US)
(31)優先権主張番号　61/835,069
(32)優先日　平成25年6月14日 (2013.6.14)
(33)優先権主張国　米国 (US)
(31)優先権主張番号　61/878,195
(32)優先日　平成25年9月16日 (2013.9.16)
(33)優先権主張国　米国 (US)

(71)出願人　397072765
インタートラスト　テクノロジーズ　コーポレイション
アメリカ合衆国，カリフォルニア　９４０８５，サニーベール，ステュアート　ドライブ　９２０
(74)代理人　100099759
弁理士　青木　篤
(74)代理人　100092624
弁理士　鶴田　準一
(74)代理人　100141162
弁理士　森　啓
(74)代理人　100141254
弁理士　榎原　正巳

最終頁に続く

(54)【発明の名称】安全な取引システム及び方法

(57)【要約】
【課題】本発明は、様々な取引と関連してタグ認証や存在検証技術を用いるシステム及び方法を提供する。
【解決手段】ある実施形態では、認証装置は、信頼できるオーソリティによって供給される秘密情報をセキュアタグが記憶するかを決定することでセキュアタグの信憑性を検証してもよい。幾つかの実施形態では、認証処理は、認証装置に秘密情報を曝すことなく実施され得るため、セキュアタグのインテグリティが維持される。他の実施形態では、インセキュアタグ及び／又は秘密情報を含まないタグが使用されてもよい。
【選択図】図４

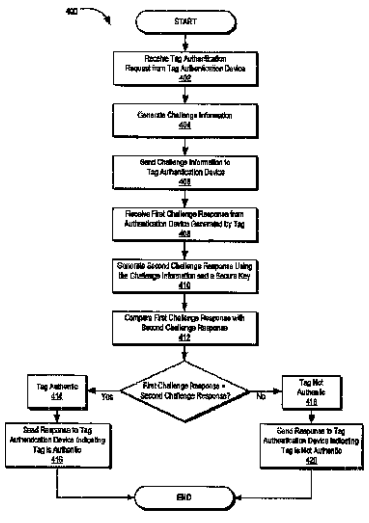

Figure 4

【特許請求の範囲】
【請求項１】
プロセッサと、命令を記憶する非一過性のコンピュータ読み取り可能な記憶媒体とを備える信頼できるシステムによって実施され、前記命令が実行されると前記システムに実施される方法であって、
認証装置からの前記信頼できるシステムのインタフェースにおいて、セキュアタグによって生成される第１のチャレンジ応答を受信する段階と、
前記信頼できるシステムによって記憶されるチャレンジ情報及び秘密情報に基づいて、第２のチャレンジ応答を生成する段階と、
前記第１のチャレンジ応答と前記第２のチャレンジ応答とを比較する段階と、
前記第１のチャレンジ応答と前記第２のチャレンジ応答が一致すると決定する段階と、
前記認証装置への前記信頼できるシステムの前記インタフェースを介して、前記セキュアタグを認証する応答を送る段階と、を備える方法。
【請求項２】
前記チャレンジ情報を生成する段階と、
前記信頼できるシステムの前記インタフェースを介して、前記チャレンジ情報を前記認証装置に送る段階と、を更に備える請求項１に記載の方法。
【請求項３】
前記認証装置からの前記信頼できるシステムのインタフェースにおいて、前記チャレンジ情報を受信する段階を更に備える、請求項１に記載の方法。
【請求項４】
前記チャレンジ情報はランダムに生成された値を有する、請求項１に記載の方法。
【請求項５】
前記チャレンジ情報は暗号的なノンスを有する、請求項１に記載の方法。
【請求項６】
前記セキュアタグは安全な近距離無線通信（「ＮＦＣ」）タグを有する、請求項１に記載の方法。
【請求項７】
前記第２のチャレンジ応答を生成する段階は、前記信頼できるシステムによって記憶される前記チャレンジ情報と前記秘密情報に基づいて暗号関数の結果を計算する段階を含む、請求項１に記載の方法。
【請求項８】
前記暗号関数は、前記信頼できるシステムによって記憶される前記秘密情報を用いて前記チャレンジ情報を電子的に署名することを含む、請求項７に記載の方法。
【請求項９】
前記暗号関数は、前記信頼できるシステムによって記憶される前記秘密情報に基づいて前記チャレンジ情報のハッシュ値を計算することを含む、請求項７に記載の方法。
【請求項１０】
前記秘密情報は秘密キーを有する、請求項１に記載の方法。
【請求項１１】
前記第２のチャレンジ応答を生成する段階は、更に、
前記第１のチャレンジ応答に含まれる前記セキュアタグと関連付けられた識別情報を用いて、前記信頼できるシステムによって記憶される前記秘密情報を読み出す段階を含み、
前記信頼できるシステムによって記憶される前記秘密情報は前記セキュアタグと関連付けられる、請求項１に記載の方法。
【請求項１２】
前記セキュアタグを認証する応答は、更に、前記セキュアタグと関連付けられる製品に関する情報を有する、請求項１に記載の方法。
【請求項１３】

前記製品に関する前記情報は、前記第１のチャレンジ応答に含まれる前記セキュアタグと関連付けられる識別情報に基づいて、前記信頼できるシステムによって読み出される、請求項１２に記載の方法。

【発明の詳細な説明】

【技術分野】

【０００１】

［関連出願］

本出願は、「物体識別システム及び方法」なる名称の２０１３年3月１２日に出願された米国仮特許出願第６１／７７８，１２２号、「安全な取引システム及び方法」なる名称の２０１３年6月１４日に出願された米国仮特許出願第６１／８３５，０６９号、「安全な取引システム及び方法」なる名称の２０１３年9月１６に出願された米国仮特許出願第６１／８７８，１９５号、「安全な取引システム及び方法」なる名称の２０１３年１２月１０に出願された米国仮特許出願第６１／９１４，２１２号、「安全な取引システム及び方法」なる名称の２０１３年１２月１９に出願された米国仮特許出願第６１／９１８，５０６号、及び、「文書実行システム及び方法」なる名称の２０１４年1月２９日に出願された米国仮特許出願第Ｎｏ．６１／９３２，９２７号に対して、米国特許法第１１９条（ｅ）に基づいて優先権の利益を主張し、これら全ての開示が参照により本明細書によりその全体に組み込まれている。

著作権の許諾

【０００２】

本特許文書の開示の一部分は、著作権保護されている材料を含む場合がある。著作権の所有者は、米国特許及び商標局の特許ファイル又は記録に表れる形態での特許文献又は特許情報開示が誰かによって複製されても異論はないが、その他の面では、全ての著作権を留保する。

【背景技術】

【０００３】

本開示は、一般的に、様々な安全な取引を行うシステム及び方法に関わる。排他的ではないが、より具体的には、本開示は、様々な取引と関連して電子タグ及び／又は存在検証を用いるシステム及び方法に関わる。

【発明の概要】

【０００４】

電子タグは、製品在庫管理、バリュー及び／又はポイントカードシステム、個人識別システム等を含む、様々な有益な用途で使用され得る。しかしながら、従来の電子タグは、特に頑丈ということはない。例えば、従来の電子タグを利用するバリュー及び／又はポイントカードシステムでは、カードの残高がタグに記憶されてもよい。このようなカードが盗まれた場合、ユーザーは、一時的に不便になり、カードと関連付けられたバリューを回復するために償還請求をたとえあったとしても僅かに有する。電子タグを利用する従来のシステムは、電子タグリーダー及び／又は関連する通信チャネルの著しいセキュリティ強化も必要とする。このようなシステムは、従来のタグリーダーに含まれる安全なハードウェアと関連付けられるコストにより、幅広く採用されない。更に、電子タグを利用する既存のシステムは、タグの信憑性及び／又は有効性をしっかりと証明し、及び／又は、タグが特定の時間において特定の場所に位置することを決定することに、能力が制限されている場合もある。これらの問題を幾つかあるいは全て改善するシステム及び方法を本願で説明する。例えば、制限なく、幾つかの既存の電子タグベースのシステムにおいて、電子タグは、比較的高機能である及び／又は高価な技法が使用されていない限り、比較的簡単に複製できる。本願記載のシステム及び方法の幾つかの実施形態では、サーバー側方法が、タグおよぶ／又はタグリーダーにおけるセキュリティの必要性を取り除く又は低下させるエンドツーエンドシステムにおいて使用される。

【０００５】

本願で開示するシステム及び方法は、電子タグ及び／又は存在検証を容易化する。幾つ

かの実施形態では、物理的なタグよりもむしろ、携帯電話やタブレット等の消費者装置に常駐し得る仮想タグが使用される。文脈から明らかでない限り、セキュア電子タグ、電子タグ、タグ等に対する参照は、全ての好適な実施（例えば、安全なチップ、ユーザーの装置に記憶される仮想タグ又はバリュー、等）を網羅することを意図する。ある実施形態では、開示するシステム及び方法は、信頼できるオーソリティによって供給される秘密情報を記憶するよう構成されるセキュア電子タグを使用してもよい。タグによる該秘密情報の認識は、信頼できるオーソリティが、タグ認証装置に近接してタグの存在を認証することで検証される。開示するシステム及び方法の実施形態は、電子タグが、特定の時間にタグ認証装置に近接して物理的に存在するといった信頼できる検証を必要とする様々な安全な取引と関連して使用されてもよい。

【０００６】

セキュア電子タグを認証するために、タグ認証装置は、全ての好適な通信方法を介して認証装置に近接するタグの存在を検出してもよい。タグの存在を検出する際、認証装置は、タグと関連付けられる信頼できるオーソリティと通信し、信頼できるオーソリティによるタグの認証を要求してもよい。これに応じて、信頼できるオーソリティは、チャレンジ情報を生成し、該チャレンジ情報を認証装置に通信してもよい。ある実施形態では、チャレンジ情報は、ランダムに生成された値を有してもよいが、開示するシステムおよび方法と関連して他のタイプのチャレンジ情報が使用されてもよい。認証装置は、チャレンジ情報を電子タグに通信し、チャレンジ情報に基づきタグが応答を生成することを要求してもよい。ある実施形態では、要求された応答は、チャレンジ情報と秘密情報（例えば、秘密情報を用いるチャレンジ情報のデジタル署名、ハッシュおよび／または暗号化バージョン等）を用いて、電子タグによって実施される計算の結果を有してもよい。

【０００７】

タグは、認証装置に応答を通信してもよく、認証装置は、反対に、該応答を信頼できるオーソリティに転送してもよい。応答を受信すると、信頼できるオーソリティは、タグと関連付けられる信頼できるオーソリティが記憶する及び／またはさもなければ所有するチャレンジ情報と秘密情報に基づき、自身の応答を生成してもよい。タグによって生成された応答と、信頼できるオーソリティによって生成された応答が一致する場合、タグによって記憶された秘密情報の認識が信頼できるオーソリティによって検証され、タグが認証されてもよい。応答が一致しない場合、タグは、信頼できるオーソリティによって検証されないこともある。信頼できるオーソリティによってタグが認証されたかの表れは、認証装置及び／または一つ以上の他のサービスプロバイダに通信され、タグと関連付けられるサービスを提供することに関連して使用される。

【０００８】

本願で開示する認証システムおよび方法のある実施形態は、タグ、リーダー、及び／または、信頼できるオーソリティまたは信頼できるサービスの間でタグ並びに文脈的相互作用それぞれの認証を提供し得る。例として、幾つかの実施形態では、チャレンジ応答を生成する際に使用されるチャレンジ情報は、チャレンジ応答に加えて、タグによって認証装置及び／又は信頼できるオーソリティに通信されてもよい。チャレンジ応答は、タグによるある秘密情報の所有を表し得るが、タグが関連付けられたチャレンジ情報を認証装置及び／又は信頼できるオーソリティに通信することに失敗した場合、本願記載の実施形態によるタグ、認証装置、及び／又は信頼できるオーソリティの間の正しい相互作用が認証され得ない。例えば、このような状況では、タグ応答が加工された、及び／又は、さもなければ、本願記載の実施形態による所定のタグ、認証装置、及び／又は信頼できるオーソリティの相互作用以外の何等かの他の文脈で生成されたと疑われる。

【０００９】

本願で開示するシステム及び方法の実施形態により、タグ及び／又は信頼できるオーソリティによって記憶された秘密情報は、認証装置及び／又は関連するサービスプロバイダシステムに曝されず、及び／又は、タグ又は信頼できるオーソリティから直接的に通信されない。ある実施形態では、これにより、認証装置及び／又は関連付けられたハードウェ

ア、ソフトウェア、及び／又は、通信チャネルのセキュリティの複雑性が低下される。本願で開示するシステム及び方法は、セキュア電子タグを利用する様々な安全な取引と関連して使用されてもよい。例えば、制限的でなく、製品認証、在庫管理、及び／又は、所有者サービス、製品情報配信サービス、バリュー及び／又はポイントカードシステム（例えば、私的通貨システム）、チケット発行システム、電子決済システム、ユーザー認証サービス、文書署名サービス、電子商取引サービス（例えば、オークションサービス）等が挙げられる。幾つかの実施形態では、タグと物理的なアイテムとの間で一対一の対応を安全に維持するサービスを構成し、末端消費者までの流通網を通じて安全なアイテムトラッキング及び追跡を可能にし、それにより、窃盗や詐欺を防止することを補助するために使用されるシステム及び方法が開示される。

【図面の簡単な説明】

【００１０】

本発明は、添付の図面と共に以下の詳細な説明を参照することで容易に理解されるであろう。

【図１】図１は、本開示の実施形態による電子タグの供給を示す。

【図２】図２は、本開示の実施形態による電子タグの認証を示す。

【図３】図３は、本開示の実施形態による、認証装置によりセキュア電子タグを認証する模範的な方法のフローチャートを示す。

【図４】図４は、本開示の実施形態による、信頼できるオーソリティによりセキュア電子タグを認証する模範的な方法のフローチャートを示す。

【図５】図５は、本開示の実施形態によるセキュア電子タグを含むシリアル化された製品の有効性を示す。

【図６】図６は、本開示の実施形態による、電子タグを含む製品に関する情報の配信を示す。

【図７Ａ】図７Ａは、本開示の実施形態による、電子タグを含むポイントカードの供給を示す。

【図７Ｂ】図７Ｂは、本開示の実施形態による、ポイントカード認証処理を示す。

【図７Ｃ】図７Ｃは、本開示の実施形態による、ポイントカード換金処理を示す。

【図８】図８は、本開示の実施形態による、バリューカード認証及び取引処理を示す。

【図９】図９は、本開示の実施形態による、交通カードの認証を示す。

【図１０】図１０は、本開示の実施形態による、再生攻撃を緩和するセキュアタグ認証処理を示す。

【図１１】図１１は、本開示の実施形態による、電子商取引サービスと関連して製品の有効性を示す。

【図１２】図１２は、本開示の実施形態による、電子商取引サービスと関連して別の製品の有効性処理を示す。

【図１３】図１３は、本開示の実施形態による、レビュー・サービスと関連して存在の有効性を示す。

【図１４】図１４は、本開示の実施形態による、文書署名サービスと関連してユーザーの認証を示す。

【図１５】図１５は、本開示の実施形態による、文書署名サービスと関連してユーザー認証処理を示す。

【図１６】図１６は、本開示の実施形態による、装置ベースのタグの初期化処理を示す。

【図１７】図１７は、本開示の実施形態による、装置ベースのタグの認証処理を示す。

【図１８】図１８は、本開示のシステム及び方法のある実施形態を実施するために使用され得るシステムを示す。

【発明を実施するための形態】

【００１１】

以下に、本開示の実施形態によるシステム及び方法を詳細に説明する。幾つかの実施形態を説明するが、本開示はどの実施形態にも制限されず、多数の変形例、変更態様、及び

、等価物を包含することは理解されるであろう。更に、本願で説明する実施形態をよりよく理解するために、以下の説明では多数の特定の詳細が説明されるが、幾つかの実施形態はこれらの詳細が幾つか又は全てなくても実施され得る。更に、本開示を不必要に不明瞭にすることを避け、明確にするために、従来技術において公知のある技術的材料は詳細に説明しない。

【００１２】

本開示の幾つかの実施形態は、図面を参照して理解され、図中、同様の参照番号が同様の構成要素に付与される。本願の図面で一般的に説明され例示されるように、開示する実施形態の構成要素は、様々な異なる構成において配置され設計され得る。それにより、ある例示的な実施形態の以下の詳細な説明は、請求する開示の範囲を制限することを意図せず、開示の可能な実施形態を表しているに過ぎない。更に、本願に記載するどの方法の段階も、必ずしも具体的な順番、又は、順次的に実行される必要がなく、また、段階は特定されない限り一回だけ実行されることに留まらない。

【００１３】

本願に開示する実施形態により、電子タグの存在を安全に検証することが可能となる。このような検証は、様々な安全な取引と関連して使用されてもよい。例えば、シリアル化された製品が本願記載の実施形態を実施するタグと関連付けられてもよい。タグ認証装置と通信する信頼できるオーソリティは、タグの信憑性を検証することで、関連するシリアル化された製品の信憑性を検証してもよい。同様にして、本願記載の実施形態は、バリューカード（例えば、アクセスパス、交通パス等の私的通貨カード）又はカード取引と関連してタグを含む同様の装置の信憑性及び／又はステータスを検証するために使用され得る。開示する実施形態のこのような実施は、中でも、権限のない人による偽造品及び／又はバリューカードの生産及び／又は配布を減少させる。

【００１４】

開示する実施形態により、例えば、携帯スマートフォン及び／又はタブレット計算装置等のセキュアタグ認証と関連して、比較的低コストのタグ認証装置の使用が可能となる。幾つかの実施形態では、タグ認証と関連して使用される秘密情報が認証装置に曝されることがないため、認証装置のハードウェア及び／又はソフトウェアセキュリティ要件が減少され得る。タグ認証装置のコスト及び／又は複雑性を下げることにより、開示するシステム及び方法は様々なサービスと関連してセキュアタグ及び／又は存在認証の採用を増加し得る。更に、開示する実施形態により、様々なサービスプロバイダによるセキュアタグ認証のために共通の信頼できるオーソリティの使用が可能となり、それにより、様々なサービスと関連してタグの権限付与及び／又は存在検証をより簡単に一体化することが容易化される。

【００１５】

ある実施形態では、本願記載のシステム及び方法は、例えば、２００６年１０月１８日に出願され、米国特許出願第２００７／０１８０５１９　Ａ１号（「‘６９３出願」）として公開された「デジタル著作権管理エンジンシステム及び方法」なる名称の同一出願人による同時係属米国特許出願第１１／５８３，６９３号に記載されるデジタル著作権管理（「ＤＲＭ」）技術、「ピア・ツー・ピアサービス編成に対する相互運用可能なシステム及び方法」（「’３８７特許」）なる名称の同一出願人による米国特許第８，２３４，３８７号に記載されるサービス編成及びＤＲＭ技術、同一出願人による同時係属米国特許出願第１３／９１４，５３８号（「‘５３８出願」）に記載されるデータ収集及び分析技術、同一出願人による同時係属米国特許出願第１３／９４６，７５０号（「‘７５０出願」）に記載される情報ターゲット化技術、及び／又は、同一出願人による同時係属米国特許出願第１２／７８５，４０６号（「’４０６出願」）（‘６９３出願、‘３８７特許、‘５３８出願、‘７５０出願、及び、‘４０６出願の内容は全体的に本明細書では参照として組み込む）、並びに、他の文脈に記載されるコンテンツ配信技術と関連して使用され得る。

【００１６】

［セキュアタグ供給］

【００１７】

図１は、本開示の実施形態によるセキュア電子タグ１００の供給を例示する。セキュア電子タグ１００は、供給された情報１０４（例えば、秘密情報）を安全に記憶し、タグ認証装置からの問い合わせ（例えば、符号付きの値、ハッシュ値、暗号化された値、及び／又は他の計算、導出、又は、変換等）に応答して該情報に基づき一つ以上の応答を生成するよう構成される全ての好適な電子的ハードウェア及び／又はソフトウェアを有し得る。情報１０４を記憶することに加え、セキュアタグ１００は、本願記載の実施形態と関連して使用される様々な他の情報を記憶するよう構成されてもよい。セキュア電子タグ１００は、全ての好適な有線及び／又は無線通信プロトコルを用いてタグ認証装置及び／又は他の関連するシステム（例えば、タグ供給処理中は信頼できるオーソリティ１０２）と通信するよう構成されてもよい。説明を簡略化するために、ここではセキュアタグをしばしば参照するが、幾つかの実施形態では、タグに本来備わっているセキュリティ能力とは対照的に、サーバーのセキュリティ能力からタグセキュリティが導出されてもよいことは理解されるであろう。このため、タグは、エンドツーエンドシステムのセキュリティを提供するサービスの識別可能な部分であることにより、安全と考えられる。文脈から明らかでない限り、本願におけるセキュアタグの参照は、少なくとも両方のシナリオ（例えば、強化された／セキュアタグを使用するシステム、及び／又は、参加するサービスとの関連で遠隔サーバーとの相互作用からセキュリティを導出するタグを使用するシステム）を含むと考えられる。

【００１８】

ある実施形態では、セキュアタグ１００は、安全な情報等を記憶する近距離無線通信（「ＮＦＣ」）タグ、無線自動識別（「ＲＦＩＤ」）タグ、ユニバーサル・シリアル・バス（「ＵＳＢ」）トークン、ブルートゥース（登録商標）可能（「ＢＬＥ」）装置を有する。更なる実施形態では、セキュアタグ１００は、関連付けられた装置に含まれるハードウェア及び／又はソフトウェアを介して実行される。例えば、セキュアタグ１００は、装置（例えば、スマートフォン）で実行される安全なソフトウェアアプリケーション（又は「アップ」）を用いて実行されてもよい、及び／又は、装置の安全なハードウェア（例えば、スマートフォンに含まれる安全なハードウェア）に含まれてもよい。本願記載のタグ認証及び／又は存在検証処理と関連して様々な他のタイプのタグが使用されてもよく、また、開示する実施形態と関連して全てのタイプの電子タグが使用されてもよいことは理解されるであろう。

【００１９】

ある実施形態では、タグ１００には、信頼できるオーソリティ１０２によって秘密情報１０４が供給されてもよい。秘密情報１０４は、本願記載の実施形態と関連して使用され得る全ての好適な情報及び／又は値を有し得る。ある実施形態では、秘密情報１０４は、電子キー、デジタル署名、ハッシュ値を計算するために用いられる情報、信頼できる認証情報等を有してもよい。幾つかの実施形態では、信頼できるオーソリティ１０２によって供給される秘密情報１０４は、特定のタグ１００に対して固有である。他の実施形態では、タグには秘密情報１０４が供給されなくてもよいが、例えば、認証された情報を記憶してもよく、認証に用いられた秘密は、例えば、サーバー（例えば、信頼できるオーソリティ１０２と関連付けられるサーバー）に記憶され得る。

【００２０】

信頼できるオーソリティ１０２によって秘密情報１０４が供給された場合、タグ１００は、開示するタグ認証及び／又は存在検証処理と関連して使用するために秘密情報１０４を持続して記憶してもよい。更なる実施形態では、信頼できるオーソリティ１０２及び／又は一つ以上の第三者（例えば、第三者サービスプロバイダ）は、タグ１００によって記憶されるよう他の情報を供給してもよい。例えば、タグ１００と関連付けられる様々なメタデータ及び／又は取引情報（例えば、タグ識別情報、関連付けられた製品及び／又は装置のメタデータ情報、サービスプロバイダ情報等）は、開示する実施形態と関連して使用

されるようセキュアタグ１００に供給され、セキュアタグ１００に記憶される。このようなメタデータ及び／又は取引情報は、情報及び／又はタグ１００と関連付けられるセキュリティ要件及び／又は好みに依存して、タグ１００によって安全に及び／又は不安全に記憶され得る。他の実施形態では、タグ１００にはシリアル化された識別子が供給され、該シリアル化された識別子は、トラッキングされる及び／又はさもなければ追跡されるべきアイテムのセットと一対一対応している。識別子自体は、個々のシリアル化されたアイテムと一対一の関連性を有するランダムに選択された値でもよく、それにより、詐欺師がこれらの値を予想することが困難となる。

【００２１】

［セキュアタグ認証］

【００２２】

図２は、本開示の実施形態による電子タグ１００の認証を例示する。信頼できるオーソリティ１０２によって秘密及び／又は認証情報１０４がタグ１００に供給された後、タグ認証装置２００はタグ１００の信憑性を検証するために使用され得る。つまり、タグ認証装置２００は、タグ１００が信頼できるオーソリティ１０２によって供給された真正のタグである、及び／又は、タグ１００が認証装置２００に近接して物理的に位置する及び／又は特定の時間に存在することを決定するために使用され得る。以下により詳細に説明するように、このような情報は、様々な安全な取引と関連して、互いに対するタグ１００、タグ認証装置２００、及び／又は関連付けられたアイテム（例えば、製品、バリュー及び／又はポイントカード、身分証明書又はアイテム、等）の存在あるいは近接の証明として使用され得る。

【００２３】

タグ認証装置２００、信頼できるオーソリティ１０２、及び／又は、一つ以上の他のサービスプロバイダ（図示せず）は、本願記載のシステム及び方法の実施形態を実施するよう構成される全ての好適な計算システム又はシステムの組み合わせを有し得る。ある実施形態では、タグ認証装置２００、信頼できるオーソリティ１０２、及び／又は、他のサービスプロバイダは、関連する非一過性のコンピュータ読み取り可能な記憶媒体に記憶されている命令を実行するよう構成される少なくとも一つのプロセッサシステムを有してもよい。以下により詳細に説明するように、タグ認証装置２００、信頼できるオーソリティ１０２、及び／又は、他のサービスプロバイダは、更に、信頼できる認証情報及び／又はキー管理、安全な政策管理、及び／又は、本願記載のシステム及び方法の他の面等の慎重に扱うべキー動作を実施するよう構成されるセキュア処理ユニット（「ＳＰＵ」）を有してもよい。タグ認証装置２００、信頼できるオーソリティ１０２、及び／又は、他のサービスプロバイダは、更に、一つ以上の関連するネットワーク接続（例えば、ネットワーク２０２）を介して装置及び／又はシステム１０２、２００間の情報の電子的通信を可能にするよう構成されるソフトウェア及び／又はハードウェアを有し得る。

【００２４】

タグ認証装置２００は、本願記載のシステム及び方法の実施形態を実施するよう構成される一つ以上のアプリケーションを実行する計算装置を有してもよい。ある実施形態では、タグ認証装置２００は、ラップトップコンピュータシステム、デスクトップコンピュータシステム、スマートフォン、タブレット・コンピュータ、タグ認証端末システム、及び／又は、開示するシステム及び方法と関連して使用され得る全ての他の計算システム及び／又は装置を有してもよい。ある実施形態では、タグ認証装置２００は、中でも、セキュアタグ１００が信頼できるオーソリティ１０２によって供給された真正タグであり、セキュアタグ１００が認証装置２００に近接して物理的に位置する及び／又は特定の時間に存在することを決定するよう構成されるソフトウェア及び／又はハードウェアを有してもよい。幾つかの実施形態では、このような機能性は、信頼できるオーソリティ１０２及び／又は一つ以上のサービスプロバイダと関連するタグ認証装置２００で実行される一つ以上のアプリケーション（例えば、タグ認証アプリケーション２０４）を用いて実施されてもよい。

【００２５】
開示する実施形態うちのある実施形態は、セキュアタグ認証及び／又は存在検証と関連して比較的低コストの汎用タグ認証装置２００を使用することを可能にする。開示するシステム及び方法と関連して使用される情報１０４にタグ認証装置２００が曝されていない場合もあるため、ある実施形態では、認証装置２００は該情報１０４と関連する全てのセキュリティを維持するために必要なセキュアソフトウェア及び／又はハードウェアを含む必要がない。例えば、ある実施形態では、タグ認証アプリケーション（又は「アップ」）２０４（例えば、信頼できるオーソリティ１０２及び／又は別のサービスプロバイダによって供給される認証アプリケーション）を実行する汎用スマートフォン及び／又はタブレット計算装置が、開示する実施形態のある態様を実施するために使用されてもよい。更なる実施形態では、タグ認証装置２００は、開示するシステム及び方法と関連して使用されるセキュアソフトウェア及び／又はハードウェアを含んでもよい。

【００２６】
タグ認証装置２００は、全ての好適な数のネットワーク及び／又はネットワーク接続を有するネットワーク２０２を介して信頼できるオーソリティ１０２及び／又はサービスプロバイダと通信し得る。ネットワーク接続は、様々なネットワーク通信装置及び／又はチャネルを有してもよく、接続された装置やシステム間の通信を容易にする全ての好適な通信プロトコル及び／又は標準を使用し得る。例えば、幾つかの実施形態では、ネットワークは、インターネット、ローカルエリアネットワーク、仮想プライベートネットワーク、及び／又は、一つ以上の電子通信技術及び／又は標準（例えば、イーサネット（登録商標）等）を利用する全ての他の通信ネットワークを含み得る。幾つかの実施形態では、ネットワーク接続は、パーソナルコミュニケーションシステム（「ＰＣＳ」）及び／又は全ての好適な通信標準及び／又はプロトコルを組み込む全ての他の好適な通信システム等の無線搬送システムを含み得る。更なる実施形態では、ネットワーク接続は、例えば、符号分割多重アクセス方式（「ＣＤＭＡ」）、グローバル・システム・フォー・モバイル・コミュニケーションズ又はグループ・スペシャル・モバイル（「ＧＳＭ（登録商標）」）、周波数分割多重アクセス方式（「ＦＤＭＡ」）及び／又は時間分割多重アクセス方式（「ＴＤＭＡ」）標準を利用するアナログ移動通信ネットワーク及び／又はデジタル移動通信ネットワークを有し得る。ある実施形態では、ネットワーク接続は、一つ以上の衛星通信回線を組み込んでもよい。更なる実施形態では、ネットワーク接続は、ＩＥＥＥ　８０２．１１標準、ブルートゥース（登録商標）、超広帯域（「ＵＷＢ」）、ジグビー（登録商標）、及び／又は、全ての他の好適な通信プロトコルを使用してもよい。

【００２７】
タグ認証装置２００は、全ての好適なタイプの有線及び／又は無線通信プロトコルを介してセキュアタグ１００と通信するよう構成される。幾つかの実施形態では、タグ認証装置２００は、ＮＦＣ、ＲＦＩＤ、トランスファージェット、ジグビー（登録商標）、ブルートゥース（登録商標）、ＩＥＥＥ　８０２．１１標準、及び／又は、本願記載の全ての通信プロトコルを含む他の好適な無線通信プロトコルを用いてセキュアタグ１００と通信してもよい。ある実施形態では、タグ認証装置２００は、セキュアタグ１００にチャレンジ情報２０８を含む一つ以上の問い合わせを通信してもよく、及び／又は、セキュアタグ１００から一つ以上の応答２１０及び／又は他の情報を受信してもよい。

【００２８】
タグ認証装置２００は、本願記載の実施形態によるタグ認証及び／又は存在検証処理と関連して使用されるタグ認証アプリケーション２０４を実行してもよい。ある実施形態では、タグ認証アプリケーション２０４は、タグ認証及び／又は存在検証処理を実施する信頼できるオーソリティ１０２によってタグ認証装置２００に供給されてもよい。更なる実施形態では、タグ認証アプリケーション２０４は、例えば、本願記載のタグ認証及び／又は存在検証処理を利用してサービスを提供するサービスプロバイダを含む一つ以上の第三者によってタグ認証装置２００に供給されてもよい。

【００２９】

ある実施形態では、タグ認証アプリケーション２０４は、全ての好適な通信方法（例えば、ＮＦＣ、ＲＦＩＤ通信等）を介して近接して位置するセキュアタグ１００を検出するためにタグ認証装置２００とポーリング処理を実施してもよい。しかしながら、全ての好適なタグ検出処理が、開示する実施形態（例えば、タグがタグ認証装置に警報を発することができる、等）と関連して使用され得ることは理解されるであろう。タグ認証アプリケーション２０４が近接して位置するタグ１００を検出した場合、タグ認証アプリケーション２０４は、タグ認証要求２０６を生成し、該タグ認証要求２０６を信頼できるオーソリティ１０２に通信してタグ１００の認証を要求する。

【００３０】

幾つかの実施形態では、セキュアタグ１００は、タグ認証アプリケーション２０４及び／又は認証装置２００によって実施されるポーリング処理を伴わない方法を用いることを含む、様々な方法でタグ認証装置２００によって検出されてもよい。幾つかの実施形態では、タグ認証装置２００は、エネルギーバースト及び／又は他の電磁信号（例えば、電波信号等）を送信してもよく（例えば、定期的に送信してもよく）、近接して位置するタグ１００がこれらを受信すると、タグ１００は応答を生成する。代替的には、タグ認証装置２００は、低エネルギー電磁場を放出してもよい。タグ認証装置２００によって放出された磁場の範囲内にタグ１００が入ると、磁場は認証装置２００によって検出可能な何等かの方法で変化し、それにより、認証装置２００は近接して位置するタグ１００を識別することができるようになる。

【００３１】

更なる実施形態では、タグ１００はその存在を示すよう近接して位置するタグ認証装置２００に信号を積極的に送信してもよい。例えば、ＮＦＣベースのタグ及び／又はスマートフォン・アプリケーションを用いて電子的に実施されたタグは、タグ認証装置２００に近接するその存在を示す信号及び／又はビーコンを送信してもよい。様々な他の好適なタグ検出処理が使用されてもよく、本願記載の実施形態と関連してタグ１００及び／又は認証装置２００によって全ての好適なタイプのタグ検出処理が実施されてもよいことは理解されるであろう。例えば、本願ではタグ検出のためにポーリング処理を用いるとしてある実施形態及び／又は例が説明されるが、非制限的に本願記載の全てのタグ検出処理を含む全ての好適なタグ検出処理が開示する実施形態及び／又は例と関連して使用されてもよいことは理解されるであろう。

【００３２】

タグ認証要求２０６を受信すると、信頼できるオーソリティ１０２は、その上で実行されるチャレンジ生成部２１２を用いてチャレンジ情報２０８を生成してもよい。ある実施形態では、チャレンジ情報２０８は、暗号的なノンス等のランダムに及び／又は疑似ランダムに生成された値を有してもよいが、他のタイプのチャレンジ情報が開示するシステム及び方法と関連して使用されてもよい。信頼できるオーソリティ１０２は、生成されたチャレンジ情報２０８をタグ認証装置２００に通信してもよく、タグ認証装置２００は、反対に、チャンレジ情報２０８をチャレンジ問い合わせの一部としてタグ１００に通信してもよい。

【００３３】

チャレンジ問い合わせは、タグ１００が少なくとも部分的にチャレンジ情報２０８に基づいて応答を返すことを要求してもよい。ある実施形態では、要求された応答は、チャレンジ情報２０８及びタグ１００によって記憶された秘密情報１０４に基づいてタグ１００によって実施される計算の結果を含んでもよい。例えば、計算は、少なくとも部分的に秘密情報１０４を用いて、チャレンジ情報２０８に含まれる暗号的なノンスのデジタル署名値、暗号化された値、ＭＡＣ値、及び／又は、ハッシュ値を計算することを含む。ある実施形態では、計算は、チャレンジ情報２０８だけに基づいては、秘密情報１０４を識別するために使用されず、及び／又は、さもなければ計算と関連して使用される秘密情報１０４を難読化するといった結果を返し得る。

【００３４】

タグ１００は、チャレンジ問い合わせに応答して生成されるチャレンジ応答２１０を認証装置２００に通信してもよい。ある実施形態では、チャレンジ応答２１０はチャレンジ情報２０８及び秘密情報１０４に基づいてタグ１００によって実施された計算の結果を含む。続いて、認証装置２００は、信頼できるオーソリティ１０２にチャレンジ応答２１０を転送してもよい。チャレンジ応答２１０を受信すると、信頼できるオーソリティ１０２は、その上で実行されるタグ認証モジュール２１４を用いてタグ認証処理を実施する。タグ認証処理の一部として、タグ認証モジュール２１４は、信頼できるオーソリティ１０２によって記憶されたチャレンジ情報２０８及び秘密情報に少なくとも部分的に基づいて応答を生成してもよい。例えば、タグ認証モジュール２１４は、チャレンジ情報２０８に含まれる暗号的なノンスのデジタル署名値、暗号化された値、ＭＡＣ値、ハッシュ値、及び／又は、他の微分又は変換を計算してもよい。ある実施形態では、タグ認証モジュール２１４によって実施される計算は、チャレンジ問い合わせに応答してタグ１００によって実施される計算と同じあるいは類似していてもよい。

【００３５】

応答を生成した後、タグ認証モジュール２１４は、生成された応答をセキュアタグ１００によって生成されたチャレンジ応答２１０と比較してもよい。タグ認証モジュール２１４によって生成された応答とセキュアタグ１００によって生成されたチャレンジ応答２１０とが一致する場合、タグ認証モジュール２１４は、セキュアタグ１００及び信頼できるオーソリティ１０２の両方が同じ秘密情報１０４を所有し、したがって、セキュアタグ１００が真正のセキュアタグ１００であると検証してもよい。しかしながら、応答が一致しない場合、タグ認証モジュール２１４は、セキュアタグ１００によって所有される秘密情報１０４の信憑性及び／又は妥当性を検証しなくてもよい。したがって、このような場合には、タグ認証モジュール２１４はセキュアタグ１００が真正ではないと決定してもよい。このようにして、セキュアタグ１００は、信頼できるオーソリティ１０２によって秘密情報１０４が供給されているため真正である、あるいは、供給されていないため真正でないと決定される。他の実施形態では、応答２１０を検証するために非対称暗号化技術が使用されてもよく、それにより、タグ認証モジュール２１４はタグ１００によって維持される情報の心得がある必要はないが、対応する非対称暗号化値（例えば、タグの秘密鍵に対応する公開鍵、あるいはその逆）を代わりに所有してもよい。

【００３６】

認証応答２１８は、タグ認証モジュール２１４によって実施される決定に基づいて認証装置２００及び／又は一つ以上の他の第三者のサービス（図示せず）に戻されてもよい。例えば、タグ認証モジュール２１４が、セキュアタグ１００は真正であると決定した場合、認証応答２１８はセキュアタグ１００が真正であるという表れを含んでもよい。同様にして、タグ認証モジュール２１４が、セキュアタグ１００は真正でないと決定した場合、認証応答２１８はセキュアタグ１００が真正でないという表れを含んでもよい。ある実施形態では、認証応答２１８に含まれる情報は認証装置２００（例えば、タグ認証アプリケーション２０４を介して）に表示されてもよく、それにより、認証装置２００のユーザーは、様々な安全な取引と関連して、信頼できるオーソリティ１０２によってセキュアタグ１００が認証されたか否かの表れを受信することができる。幾つかの実施形態では、認証装置２００及び／又は信頼できるオーソリティ１０２は、サービスプロバイダが存在の証明を確認できるようサービスプロバイダに認証応答２１８を転送してもよい。

【００３７】

幾つかの実施形態では、タグ認証モジュール２１４がセキュアタグ１００は真正であると決定した場合、認証応答２１８はセキュアタグ１００と関連するあるタグメタデータ２１６及び／又は取引情報を更に有してもよい。例えば、ある実施形態では、タグメタデータ２１６は、タグ識別情報、セキュアタグ１００と関連付けられる製品及び／又は装置に関する情報、及び／又は、セキュアタグ１００及び／又は認証する手段としてセキュアタグ１００を利用する取引と関連付けられ得る全ての他の情報を有してもよい。認証応答２１８に含まれるメタデータ及び／又は他の情報は、タグ認証装置２００のユーザーに更に

表示されてもよい。例えば、認証されたセキュアタグ１００と関連付けられるユーザーの写真は、認証応答２１８に含まれ認証装置２００に表示されてもよく、それにより認証装置２００のユーザーは、信頼できるオーソリティ１０２によって示されるように、認証装置２００にセキュアタグ１００を提示している人がセキュアタグ１００と関連していることを検証することができる。

【００３８】

本願記載のシステム及び方法の実施形態により、セキュアタグ１００及び／又は信頼できるオーソリティ１０２によって記憶された秘密情報１０４が、認証装置２００及び／又は関連するサービスプロバイダシステムに曝され、及び／又は、セキュアタグ１００又は信頼できるオーソリティ１０２から直接的に通信されないようにすることができる。秘密情報１０４が認証装置２００に曝されないため、認証装置２００はこのような秘密情報１０４の妥当性を保護するために設計されるセキュリティ強化ソフトウェア及び／又はハードウェア構成要素を含む必要がなくなり、それにより、認証装置を実施するために必要なコスト及び複雑性が少なくなる。更に、秘密情報１０４がタグ１００に供給された後、秘密情報１０４は、タグ１００と様々な他のシステム及び／又は装置（例えば、認証装置２００及び／又は信頼できるオーソリティ１０２）との間で通信される必要がない。したがって、このような通信チャネルは、比較的負安全な通信チャネルでもよい。幾つかの実施形態では、これにより、例えば、オープンモバイル装置データネットワーク、インターネット等を含む既存のデータネットワークが様々な開示する実施形態と関連して使用され得る。

【００３９】

幾つかの実施形態では、タグ１００及び／又は信頼できるオーソリティ１０２はセキュリティ強化され（例えば、安全なソフトウェア及び／又はハードウェアベースのセキュリティ技術を用いる）てもよく、認証装置２００はセキュリティ強化されていない及び／又はより低い度合でセキュリティ強化されている。幾つかの実施形態では、認証装置２００の信用性は、装置２００と関連付けられる信頼できるエンティティ及び／又は起源制御機構による発行に基づいて文脈上確立されてもよい。例えば、認証装置２００の所有者は、確立された起源制御機構によって厳しく制御されているユーザーに対する装置２００の発行及び／又は所有に基づいて装置２００にある程度の信用を予め定めてもよい。

【００４０】

更なる実施形態では、本願記載のシステム及び方法は、比較的インセキュアな（不安全な）タグ１００及び／又は認証装置２００（例えば、信頼できるオーソリティ１０２よりも低いセキュリティ強化を実施するタグ１００及び／又は装置２００）を用いて実施されてもよい。信頼できるオーソリティ１０２は、より強固なセキュリティ対策（例えば、安全なソウトウェア及び／又はハードウェアベースのセキュリティ技術を用いる、データへのアクセス及び／又はプロセスを制限するためにその遠隔な場所を利用する、等）を実施してもよい。ある実施形態では、このような構造により、中央化セキュリティの利用、比較的低コストの既存のタグ認証装置２００（例えば、タグ認証アプリケーション２０４を実行する携帯スマートフォン、及び／又はタブレット計算装置）及び／又は比較的インセキュアなタグ１００の使用が可能となる。例えば、幾つかの実施形態では、タグ１００は秘密情報１０４及び／又はさもなければセキュアな情報を記憶しないこともあるが、タグ１００に固有の供給された識別子を記憶する。信頼できるオーソリティ１０２は、認証装置２００と関連して、タグ１００が固有の識別子を記憶しているといった決定に基づいてタグ１００を認証してもよい。以下により詳細に説明するように、製品の有効性と関連して、タグと関連付けられたアイテムとの一対一対応が信頼できるオーソリティ１０２によって維持されてもよい。この対応に基づき、信頼できるオーソリティ１０２は偽造のタグ１００及び／又はアイテムを（例えば、二重の識別子を有するタグを識別することによって、等）検出することができ、及び／又は、これに応答して適当なアクションを取ることができる（例えば、オーソリティ等に通知する）。

【００４１】

本発明の範囲内で図２と関連して提示されるアーキテクチャ及び関係に対して幾つかの変更がなされ得ることは理解されるであろう。例えば、制限的でなく、幾つかの実施形態では、認証装置２００によって実施される幾つかの又は全ての機能は、信頼できるオーソリティ１０２によって実施されてもよい。同様にして、信頼できるオーソリティ１０２によって実施される幾つかの又は全ての機能は、認証装置２００によって実施されてもよい。以下により詳細に説明するように、図２に例示するセキュアタグ認証及び／又は存在検証処理のある態様は、セキュア電子タグを利用する様々な安全な取引と関連して使用されてもよい。例えば、制限的でなく、製品認証、在庫管理、及び／又は、所有者サービス、製品情報配信サービス、バリュー及び／又はポイントカードシステム（例えば、私的通貨システム）、ユーザー認証サービス、文書署名サービス、電子商取引サービス（例えば、オークションサービス）、識別サービス、電子通貨システム、等が挙げられる。そのため、図２が例示及び説明目的のために提供され、制限するために提供されないことは理解されるであろう。

【００４２】

図３は、本開示の実施形態による、認証装置によりセキュア電子タグを認証する模範的な方法３００のフローチャートを示す。例示する方法３００は、様々な方法で実施され、例えば、ソフトウェア、ファームウェア、ハードウェア、及び／又は、その組み合わせを用いて実施される。ある実施形態では、方法３００は、上述の通り認証装置で実行されるタグ認証アプリケーションによって少なくとも部分的に実施される。

【００４３】

３０２において、タグ認証装置の近傍に位置するセキュアタグが装置によって検出される。ある実施形態では、セキュアタグは、認証装置によって実施されるポーリング処理に応答して検出されてもよい。例えば、認証装置は、関連する無線通信システム（例えば、ＮＦＣ、ＲＦＩＤ通信等）とポーリング処理を実施してもよい。ある実施形態では、無線通信システムは、認証装置から広がる特定の範囲を有してもよい。それに応じて、セキュアタグは、無線通信システムの範囲内で検出されると、タグ認証装置に近接して位置すると決定され得る。このようにして、本願記載の実施形態は、セキュアタグが信頼できるオーソリティによって供給される真正タグである、真正タグが認証装置に近接して位置する（例えば、存在検証）の両方を決定するために使用され得る。

【００４４】

セキュアタグが検出されると、３０４においてセキュアタグの認証を要求するタグ認証要求がタグ認証装置から信頼できるオーソリティに通信されてもよい。ある実施形態では、タグ認証要求は、例えば、タグ識別情報、取引情報等を含む、近接するセキュアタグから認証装置によって受信される情報を含んでもよい。ある実施形態では、このような情報は、タグ認証処理の一部としてセキュアタグに後に通信されるチャレンジ情報を生成する際に信頼できるオーソリティによって使用されてもよい。

【００４５】

タグ認証装置は、３０６において、タグ認証要求に応答して信頼できるオーソリティからチャレンジ情報を受信してもよい。ある実施形態では、チャレンジ情報は、暗号的なノンス等のランダムに及び／又は疑似ランダムに生成された値を有してもよいが、他のタイプのチャレンジ情報が開示するシステム及び方法と関連して使用されてもよい。他の実施形態では、タグ認証装置及び／又は別の第三者のサービスがチャレンジ情報を生成し、該チャレンジ情報をタグ及び／又は信頼できるオーソリティに通信してもよい。

【００４６】

３０８において、タグ認証装置は、チャレンジ情報に少なくとも部分的に基づいてセキュアタグが応答を返すことを要求するチャレンジ問い合わせの一部として、近接して位置するタグにチャレンジ情報を通信してもよい。ある実施形態では、要求された応答は、チャレンジ情報及びセキュアタグによって記憶された秘密情報に基づいてセキュアタグによって実施される計算（例えば、デジタル署名動作、ハッシュ計算、等）の結果を有してもよい。

【００４７】
チャレンジ問い合わせに対する応答は、３１０において、近接して位置するセキュアタグからタグ認証装置によって受信され、３１２において、信頼できるオーソリティによる認証のために信頼できるオーソリティに転送される。３１４において、タグ認証応答は信頼できるオーソリティから受信されてもよく、タグが信頼できるオーソリティによって供給される真正セキュアタグか否かが示される。該応答に含まれる情報に基づき、タグが真正であるか否かの表れがタグ認証装置のユーザーに提供されてもよい。
【００４８】
更なる実施形態では、タグ認証応答は、追加的なメタデータ（例えば、セキュアタグの登録ユーザーと関連付けられるユーザー情報）及び／又は他の取引情報（例えば、セキュアタグと関連付けられる勘定残高の表れ）を含んでもよい。セキュアタグと関連付けられる様々なメタデータ及び／又は取引情報がタグ認証応答に含まれてもよく、セキュアタグ認証処理及び／又は存在検証を伴う取引において使用され得る全ての好適なタイプの情報が本願記載の実施形態と関連して使用されてもよいことは理解されるであろう。
【００４９】
図４は、本開示の実施形態による、信頼できるオーソリティによりセキュア電子タグを認証する模範的な方法４００のフローチャートを示す。例示する方法４００は、様々な方法で実施され、例えば、ソフトウェア、ファームウェア、ハードウェア、及び／又は、その組み合わせを用いて実施される。ある実施形態では、方法４００は、上述の通り信頼できるオーソリティで実行されるチャレンジ生成部及び／又はタグ認証モジュールによって少なくとも部分的に実施される。
【００５０】
４０２において、タグ認証要求が、近接して位置するタグを検出したタグ認証装置から受信される。ある実施形態では、タグ認証要求は、例えば、タグ識別情報、取引情報等を含み、近接タグから認証装置によって受信される情報を含んでもよい。タグ認証要求を受信すると、４０４において、信頼できるオーソリティはチャレンジ情報を生成する。チャレンジ情報は、暗号的なノンス等のランダムに及び／又は疑似ランダムに生成された値を有してもよい。他の実施形態では、タグ認証装置及び／又は別の第三者のサービスがチャレンジ情報を生成し、該チャレンジ情報をセキュアタグ及び／又は信頼できるオーソリティに通信してもよい。
【００５１】
４０６において、生成されたチャレンジ情報はタグ認証装置に通信されてもよい。タグ認証装置は、チャレンジ情報をチャレンジ問い合わせの一部としてタグに通信してもよい。４０８において、チャレンジ問い合わせに応答してタグによって生成された第１のチャレンジ応答が認証装置及び／又はタグから信頼できるオーソリティによって受信されてもよい。４１０において、信頼できるオーソリティは、４０４において生成されたチャレンジ情報と、信頼できるオーソリティによって所有される秘密情報を用いて第２のチャレンジ応答を生成してもよい。ある実施形態では、４１０において使用される信頼できるオーソリティによって所有される秘密情報は、特定のセキュアタグと関連付けられてもよい。幾つかの実施形態では、信頼できるオーソリティによって使用される秘密情報は、タグ認証装置から（例えば、タグ認証要求の一部として等）通信されるセキュアタグと関連付けられるタグ識別情報を用いて秘密情報の多数のインスタンスの中から識別されてもよい。
【００５２】
ある実施形態では、第２のチャレンジ応答は、信頼できるオーソリティによって実施された計算の結果を含んでもよい。例えば、幾つかの実施形態では、第２のチャレンジ応答は、チャレンジ情報に含まれる暗号的なノンスのデジタル署名された及び／又はハッシュされた値を含んでもよい。ある実施形態では、信頼できるオーソリティによって実施される計算は、チャレンジ問い合わせに応答してセキュアタグによって実施される計算と同じでもよい。
【００５３】

４１２において、タグ認証装置から受信された第１のチャレンジ応答と信頼できるオーソリティによって生成された第２のチャレンジ応答が比較される。第１のチャレンジ応答と第２のチャレンジ応答が同じである場合、４１４においてタグは真正であると決定される（例えば、タグは信頼できるオーソリティによって供給される秘密情報を所有する）。４１６において、タグが真正であることを示す応答が信頼できるオーソリティによってタグ認証装置に送られる。第１のチャレンジ応答と第２のチャレンジ応答が同じでない場合、４１８においてタグは真正でないと決定される（例えば、タグは信頼できるオーソリティによって供給される秘密情報を所有しない）。４２０において、タグが真正でないことを示す応答が信頼できるオーソリティによってタグ認証装置に送られる。

【００５４】

特に図示しないが、４１４においてタグが真正であると決定された場合、４１６において送られる応答はタグと関連付けられる追加的な情報を更に含んでもよい。例えば、送られる応答は、制限的でなく、例えば、タグ識別情報、製品、装置、及び／又はセキュアタグと関連付けられるユーザーに関する情報、タグと関連付けられる取引情報（例えば、勘定残高等）、取引を進める権限、及び／又は、全ての好適な情報を含む、タグと関連付けられるタグメタデータ及び／又は取引情報を更に有してもよい。幾つかの実施形態では、４１６において送られる応答のデータは、信頼できるオーソリティによって署名されてもよく、それにより、装置又は信頼できるオーソリティが４１６を第三者（例えば、サービスプロバイダ）に４１６を転送した場合でも、第三者は信頼できるオーソリティの署名を検証することで該データを存在の証拠として使用することができる。

【００５５】

図４は制限的でなく例示目的のために提供され、本発明の原理から逸脱することなく本願で例示する処理に幾つかの変更がなされ得ることは理解されるであろう。例えば、あるステップは異なる順番で実施されてもよく、又は、他のステップと組み合わされてもよい。例えば、幾つかの実施形態では、信頼できるオーソリティは、例えば、（例えば、暗号化することで）キー値で変換され得る所望のチャレンジ応答を生成することができる。チャレンジ応答が受信されると、該チャレンジ応答は、最初に選択された値（即ち、本実施形態では、サーバー側でチャレンジ応答を再計算する必要がない）と単に比較される。このため全ての好適なチャレンジ／応答プロトコル（単数又は複数）が使用され得ることは理解されるであろう。

【００５６】

［シリアル化された製品の有効性］

【００５７】

開示するシステム及び方法のある実施形態は、様々な製品及び／又はアイテムを識別及び／又は検出することと関連して使用されてもよい。例えば、美術品、デザイナー服やアクセサリー、相手先商標製品の製造会社（「ＯＥＭ」）の部品、薬剤等を含む偽造アイテムの検出は、オリジナルに類似するように見えるオブジェトの複製品を製造することを容易にする三次元印刷及び他の技術により次第に難しくなり得る。本願記載のシステム及び方法は、偽造活動を阻止する及び／又はさもなければ検出するようセキュアタグやタグ認証及び／又は存在検証を使用してもよい。本願記載のシステム及び方法のある態様は、一つ以上の実行可能なアプリケーションを用いて既存の消費者装置に一体化されてもよく、それにより、消費者は、偽造物体を識別し、識別を簡単にすることで偽造を阻止し、製造会社及び／又は捜査当局が偽造活動のパターンを識別し、証拠を集める等を行うことを補助する。

【００５８】

電子タグを利用する、ある従来のシステムは、オンラインーツゥーオフライン（「Ｏ２Ｏ」）プロトコルとして公知の技術を使用してもよい。このようなシステムでは、タグは物体（例えば、製品又はイベントを宣伝するポスター）と関連付けられてもよい。消費者は、タグリーダーを含む携帯装置（例えば、スマートフォン）を物体にタップすることで、製品又はイベントに関する追加的な情報を提供するウェブサイト（例えば、タグに埋め

込まれたＵＲＬに対応するページ）に移動され得る。しかしながら、このようなシステムでは、タグは、消費者が自身の携帯装置をタグにタップすると、タグが、不正な詐欺まがいの電子メールキャンページで使用される「フィッシング詐欺」と類似する方法で偽造者が選ぶウェブサイトに消費者を移動させるように、偽造される。

【００５９】

本願記載のシステム及び方法は、セキュア電子タグを用いることで、電子タグの偽造を防止するために及び／又はフィッシング詐欺の活動を緩和するために使用され得る。幾つかの実施形態では、セキュアタグの製造会社Ｍは、固有の秘密文字列Ｓ（Ｍ）又は他の秘密情報と固有の識別子ＩＤ（Ｍ）を得る及び／又はさもなければ生成する。製造会社は、ＵＲＬが埋め込まれたタグを生産する際、暗号関数Ｈ（．．．）（例えば、一方向性ハッシュ関数）を用いて、選択する（例えば、メタデータ情報）ＵＲＬを超える全ての情報を含むＨ（Ｓ（Ｍ），ＩＤ（Ｍ），ＵＲＬ．．．）を計算し、計算の結果をセキュアタグに安全に埋め込んでもよい。セキュアタグが携帯装置によって（例えば、その上で実行されるタグ認証アプリケーションを介して）読み出されると、携帯装置は、暗号関数の計算の結果及び製造会社の識別子を信頼できるオーソリティとして動作する信頼できるサービスプロバイダで確認してもよく、該信頼できるオーソリティも暗号関数の結果を計算してもよい。結果（例えば、ハッシュ）が一致しない場合、信頼できるオーソリティは、偽造タグ及び／又はフィッシング攻撃が疑われていることを携帯装置及び／又はそのユーザーに通知し得る。更なる実施形態は、上述の方法を拡大して、セキュアタグと関連付けられる物体自体が偽造されたか否かの検出を容易にすることができる。

【００６０】

ある実施形態により、物理的アイテム及び／又は製品の製造会社はアイテム及び／又は製品のシリアル化された複製品とシリアル化されたセキュアタグを安全に関連付けることができる。ある実施形態では、セキュアタグは、製品からセキュアタグを取り除くとセキュアタグ及び／又は製品が結果として損傷するようにして、製品と関連付けられ得る。例えば、セキュアタグは、製品、製品の容器等に貼られる及び／又はさもなければ物理的に関連付けられ（例えば、パッケージングを介して）てもよい。信頼できるサービスプロバイダ（例えば、信頼できるオーソリティ）Ｔは、正当な製品製造会社Ｍを有効化してもよい。信頼できるサービスプロバイダは、製造会社Ｍと関連付けられる固有の秘密文字列Ｓ（Ｍ）又は他の秘密情報と固有の識別子ＩＤ（Ｍ）を製造会社に供給してもよい。製造会社が、シリアルナンバーｎを有するシリアル化された製品Ｐを生産すると（Ｐ（ｎ）は製品Ｐの正当なバージョンとのシリアルナンバーの割り当て）、製造会社Ｍは製品と関連付けられるＵＲＬであるＵＲＬ（Ｐ）及び／又は信頼できるサービスＵＲＬ（Ｔ）を記憶するシリアル化されたセキュアタグを生産することができる。

【００６１】

ハッシュ関数等の暗号関数Ｈ（．．．）は、結果Ｈ（Ｓ（Ｍ），ＩＤ（Ｍ），ＵＲＬ（Ｐ），ＵＲＬ（Ｔ），Ｐ（ｎ），…）を計算するために使用されてもよい。この結果が各セキュアタグに記憶されることにより、シリアル化されたセキュアタグとシリアル化された製品との間で一対一の対応が得られる。セキュアタグのセキュリティは、固有の秘密文字列Ｓ（Ｍ）又は他の秘密情報が他の第三者に曝されないことを確実にすることにより、セキュアタグの製造会社によって維持される。関連付けられた製品の有効性及び／又は信憑性を識別するためにセキュアタグが使用され得るため、関連付けられた製品の本質的価値はセキュアタグと結び付けられる。

【００６２】

開示するシステム及び方法の実施形態は、購入取引と関連して製品の信憑性を立証するために使用されてもよい。購入取引の一部として、ユーザーは、スマートフォンや他の携帯装置を用いて製品と関連付けられるセキュアタグによって記憶されている情報を読み出すことができる。携帯装置上のアプリケーションは、ユーザーが製品を新製品として又は使用済製品として購入するかを問い合わせることがある。新製品の場合、本システム及び方法の実施形態は、製品の特定のシリアル化されたバージョンが別の第三者によって以前

新しく購入されたか否かを確認するために使用され得る。アプリケーションは、取引と関連してどこでセキュアタグが携帯装置によって読み取られたかといった場所と関連する他のデータ（例えば、ＧＰＳ位置情報等）を収集してもよい。本システム及び方法の実施形態は、使用済製品の場合、いつ、どこで、誰によって製品が以前購入されたかを確認してもよい。幾つかの実施形態では、関連するサービスが、該情報及び／又は製造会社によって得られた以前に収集された情報（例えば、使用及び／又は転売パターンに関する情報）を用いて、製品が公認された複製品である可能性があることを決定してもよい。

【００６３】

図５は、本開示の実施形態によるセキュアな電子タグ１００を含むシリアル化された製品５００の有効性を示す。セキュアタグ１００は、信頼できるオーソリティ１０２及び／又は別の信頼できるサービスプロバイダによって秘密情報１０４と共に供給されてもよい。供給された後、セキュアタグ１００は製品５００と（例えば、製品の製造会社又は別の第三者によって）安全に関連付けられる。製品５００は、制限なく、美術品、デザイナー服やアクセサリー、ＯＥＭの部品、車両、薬剤、バリュー及び／又はポイントカード、携帯電話等を含む全ての製品及び／又はアイテムを含んでもよい。ある実施形態では、製品５００は独自の製品でもよい。更なる実施形態では、製品５００はシリアル化された製品５００でもよい。つまり、製品５００は、関連付けられたシリアルナンバー又は他の固有の識別子を有する製品の複数の複製品のうちの一つでもよい。

【００６４】

ある実施形態では、セキュアタグ１００は、シリアル化された製品５００と物理的に関連付けられてもよい。例えば、セキュアタグ１００は、製品５００からセキュアタグ１００を取り除くと、結果としてセキュアタグ１００及び／又は製品５００が損傷する、及び／又は、セキュアタグ１００及び／又は製品５００と関連付けられるバリューが低下するようにして、製品５００と関連付けられてもよい。更なる実施形態では、セキュアタグ１００は、セキュアタグ１００の存在が見えない、又は、さもなければ、製品５００上で明らかとならないようにして、製品５００及び／又は製品５００と関連付けられる容器に貼られる及び／又は物理的に関連付けられてもよい。

【００６５】

ユーザーは、製品５００に関する情報を取得することに関心を持つこともある。ある状況では、ユーザーは、購入等、製品５００に関わる取引と関連して製品５００関する情報を取得することに関心を持つことがある。例えば、購入取引と関連して、ユーザーは、中でも、製品５００が偽造品でなく製造会社からの真正製品であることを立証し、製品５００が新品か、新品として以前に販売されてないことを確認し、製品５００に関して所有者履歴情報を取得する等、を行うことを望む。本願記載の実施形態によると、ユーザーは製品５００と関連付けられるセキュアタグ１００を伴う認証処理を通じて、このような情報を取得することができる。

【００６６】

ユーザーは、製品５００を有効化する及び／又は関連付けられた情報を取得するために、認証装置２００を使用してもよい。中でも、認証装置２００は、セキュアタグ１００が信頼できるオーソリティ１０２によって供給された真正タグであることを立証してもよく、拡大解釈すれば、セキュアタグ１００と関連付けられた製品５００は認証装置２００に近接して位置する真正の及び／又は有効な製品５００であると立証してもよい。ある実施形態では、認証装置２００上で実行される製品有効化アプリケーション５０２（例えば、信頼できるオーソリティ１０２、製品５００の製造会社、及び／又は、全ての対の第三者によって提供されるアプリケーション）が、本願記載の実施形態によるタグ認証及び／又は存在検証処理と関連して使用されてもよい。

【００６７】

幾つかの実施形態では、製品有効化アプリケーション５０２は、セキュアタグ１００を含む近接して位置する製品５００を検出するためにタグ認証装置２００とポーリング処理を実施してもよい。他の実施形態では、他のタグ検出技術が使用され得る。製品有効化ア

プリケーション５０２がセキュアタグ１００を含む近接して位置する製品５００を検出すると、製品有効化アプリケーション５０２は製品有効化要求５０４を生成し、該製品有効化要求５０４を製品５００の有効化を要求している信頼できるオーソリティ１０２に通信してもよい。

【００６８】

図２を参照して上述したタグ認証処理と同様にして、信頼できるオーソリティ１０２は、チャレンジ生成部２１２を用いてチャレンジ情報２０８を生成し、チャレンジ情報２０８を製品５００に含まれるセキュアタグ１００に通信してもよい。セキュアタグ１００は、チャレンジ情報２０８及びセキュアタグ１００によって記憶された秘密情報１０４を用いてセキュアタグ１００によって実施される計算（例えば、ハッシュ計算等）の結果を含み得るチャレンジ応答２１０を通信してもよい。チャレンジ応答２１０は、更に、例えば、タグ１００及び／又は製品５００と関連付けられるシリアル及び／又は他の識別情報等の、セキュアタグ１００と関連付けられる他の情報を含んでもよい。

【００６９】

信頼できるオーソリティ１０２は、チャレンジ応答２１０に含まれる結果を、チャレンジ情報２０８と所有する秘密情報１０４に基づきタグ認証モジュール２１４を用いて実施する同様の計算の結果と比較してもよい。結果が一致した場合、又は、幾つかの所定の関係を満たした場合、信頼できるオーソリティ１０２はセキュアタグ１００が信頼できるオーソリティ１０２によって供給された真正のタグであり、したがって、関連する製品５００が有効であると決定してもよい。結果が一致しない場合、信頼できるオーソリティ１０２はセキュアタグ１００が信頼できるオーソリティ１０２によって供給された真正のタグでなく、したがって、関連する製品５００が有効でない又は偽造タグと関連付けられていると決定してもよい。信頼できるオーソリティ１０２は、製品５００が信頼できるオーソリティによって有効であると確認されたか否かを示す製品有効化応答５０６を認証装置２００に通信してもよい。認証装置２００のユーザーには、有効化応答５０６（例えば、「製品有効」）の内容に基づき製品５００が有効か否か装置２００上で提示されてもよい。更なる実施形態では、有効な場合、製品５００に関する追加的な情報（例えば、信頼できるオーソリティ１０２及び／又は別のサービスによって維持される製品メタデータ５０８）が有効化応答５０６に含まれ、認証装置２００のユーザーに提示されてもよい。

【００７０】

本願記載の実施形態によると、セキュアタグ１００によって記憶された関連付けられたシリアルナンバー又は他の固有識別子が信頼できるオーソリティ１０２に通信されてもよい。シリアルナンバー又は識別子は、チャレンジ応答２１０に含まれる結果を計算することと関連してセキュアタグ１００によって使用されてもよい。同様にして、シリアルナンバー又は識別子は、セキュアタグ１００からのチャレンジ応答２１０に含まれる結果と比較するために結果を計算することにおいて、信頼できるオーソリティ１０２によって更に使用されてもよい。このようにして、本願記載の認証処理は、セキュアタグ１００及び／又は製品５００と関連付けられた固有のシリアル化された情報を使用してもよい。シリアルナンバー又は識別子は、信頼できるオーソリティ１０２によって維持される製品メタデータのデータベースから、セキュアタグ１００及び／又は製品５００と関連付けられる製品メタデータ５０８を識別し配信する際に信頼できるオーソリティ１０２によって使用されてもよい。

【００７１】

有効な又は正当な製品５００に対するセキュアタグ１００の一対一対応を維持することにより、偽造を緩和する開示するシステム及び方法の能力が強化される。シリアル化されたセキュアタグ１００は、偽造者によって簡単に製造され得ないが、個々のセキュアタグ１００は複製され得る（製品自体よりも簡単ではない）ため、所与のシリアル化されタグの複製品が一つ以上存在し得る。したがって、幾つかの実施形態では、偽造活動を緩和するために追加的な技術が使用されてもよい。例えば、ある実施形態では、信頼できるオーソリティ１０２は、製造会社及びその製品５００に対して登録オーソリティとして機能し

てもよい。

【００７２】

幾つかの実施形態では、信頼できるオーソリティ１０２は、正当な製造会社を入念に検査し製品有効かサービスを提供することで貴重なサービスを消費者や製造会社に提供してもよい。更に、信頼できるオーソリティ１０２は、違法の製品複製及び／又は販売計画のパターンを識別するために機械学習ベースのパターン検出サービスを提供してもよい。信頼できるオーソリティ１０２は、製品５００の導入前にデータを収集してもよく、また、製品５００が導入された後にユーザーから（例えば、ユーザーやその後のユーザーの使用パターンを収集することで）データを収集してもよい。不正行動は、本願記載の製品有効か技術及び／又はＧＰＳ位置、時間、日付、所有者、及び／又は、製品分類情報と関連して識別される使用パターンを利用して信頼できるオーソリティ１０２によって識別されてもよい。

【００７３】

［盗難商品識別］

【００７４】

開示されたシステム及び方法のある実施形態は、窃盗の抑制及び／又は検出に関連して利用されてもよい。消費者及び／又は販売者は、新品又は中古品を購入又は他の場合では取得すると、このような情報を維持し得る信頼できる第三者機関に製品の所有権を記録し、登録し且つ／又は他の場合では主張することができる。例えば、信頼できる第三者機関は、ある製品が新品であるか或いは以前に販売されたものであるかに関する情報を維持してもよい（例えば、製品は、該信頼できる第三者機関に「新品」、「中古品」、「最初の販売」、「中古販売」及び／又は同種のものとして登録され得る）。利用者識別子を各登録取引に関連付けることで、特定利用者に関連付けられた製品目録及び／又は製品製造番号が、信頼できる第三者機関によって維持されてもよい。後日、仮に利用者が窃盗により製品の損害を被った場合には、利用者は、信頼できる第三者機関から製品目録を検索し且つこれらの製品のうちのどれが盗難及び／又は他の場合には紛失に遭ったかを知らせてもよい。

【００７５】

盗難製品の信頼できる第三者機関への報告は、直接利用者によって及び／又は法執行当局（例えば、公式の警察報告プロセスの一部又は同種のもの）等の別の当事者によって実施されてもよい。例えば、法執行当局は、信頼できる第三者機関に維持される製品データベース（例えば、製品メタデータデータベース）に、ある製品が盗難に遭ったとして報告し且つ／又は認定することを該法執行当局に許可し得る、信頼できる第三者機関に関連付けられた特別な報告を受け得る。製品にはフラグ設定してもよく、該フラグ設定は、仮に利用者が例えば、製品タグの認証（例えば走査）、該製品の所有権主張、認証デバイスの近接領域内通過及び／又は同種のものを試みることで製品の状態について問い合わせした場合、信頼できる第三者機関、法執行当局及び／又は他の利害関係者（例えば、該製品の所有権を主張する別の利用者）への通知が提供できるようになされる。

【００７６】

通知は、製品を盗難に遭ったとして分類した第三者機関に通知すること、報告された該製品が盗難に遭ったことを利用者に通知すること、（例えば、認証デバイス及び／又はセル無線三角測量、ＧＰＳ、報告利用者位置、ＩＰアドレス追跡等の他の位置識別手段の位置検索により判定された通りの）走査製品位置付近の第三者機関（例えば法執行当局）に通知すること及び／又は潜在的購入者（例えば、該製品を走査又は他の場合では認証するように試みた人物）に通知することを含み得るが、これらに限定されない。ある実施形態において、通知は、例えば、認証要求、走査発生位置（例えばＧＰＳ位置）、セキュアタグ及び／若しくは認証デバイスに対応する他の環境データ、製品が盗難に遭ったと報告された日付及び／若しくは位置に関連付けられた利用者アカウント並びに／又は同種のもの等の追加データを含んでもよい。盗難品の潜在的購入者が購入前に該商品の妥当性を確認できるようにすることで、法執行の及ぶ範囲は、商品のグレーマーケット内の多くの店頭

販売時点情報管理へと著しく増加し、その結果、窃盗未遂犯にとっての再販市場を低減し且つ盗難製品の洗浄（ロンダリング）に関与し得る個人を捜し出すのに役立ち得る。

【００７７】

［製品情報分布］

【００７８】

図６は、本開示の実施形態に従うセキュア電子タグ１００を備える製品６００に関する情報の分布を例示する。上述したように、セキュア電子タグ１００は、信頼できる第三者機関１０２及び／又は別の信頼できるサービスプロバイダによって秘密情報１０４をプロビジョニングされ且つ（該製品の製造業者又は別の当事者によって）製品６００に安全に関連付けられてもよい。製品６００は車両として例示されているが、製品６００は、ここで詳述されるいかなる種類の品目及び／又は製品も含む、あらゆる種類の品目及び／又は製品を含み得る。別の実施形態において、製品６００は、利用者が製品及び／又はサービスに関する情報を受け取るためにここで開示されたシステム及び方法を利用して対話し得る広告及び／又は他のシステム（例えば情報キオスク又は同種のもの）等の製品であってもよい。

【００７９】

顧客が関心のある多様な情報は、製品６００に関連付けられ得る。例えば、安全性又は他の点での懸念に起因して、製造業者は、所定の製品機種番号又はある機種番号に対する所定の特定製造番号セットに対して安全のための自主回収を発表してもよい。この場合、製造業者は、顧客が有害製品６００を破壊若しくはサービスから除外し且つ／又は修理のために該製品を持ち込むのと引き換えに該顧客に対してある種の補償を施し得る。いくつかの事情において、所定の製品機種番号又は製造番号のみが影響を受け且つ製品回収における補償の対象となり得るため、製造番号が振られた製品６００の安全認証は、製品回収のサービス提供に関連して利用され得る。

【００８０】

開示されたシステム及び方法の実施形態は、このような製品情報を収集及び報告し且つ／又は回収要求（例えばサービス提供、交換等）の順守を登録及び／又は他の場合では規定するのに便利な機構を提供することで、このような努力を容易にできる。例えば、安全関連回収の場合、潜在的有害製品６００が疑いを持たない個人に転売されないように保証することが望ましい。製品回収情報を包含するようにここで開示された報告能力を拡張することで、該能力が認証デバイス２００で走査し得る製品６００の特定機種及び／又は製造番号の回収を潜在的顧客に変更させることもできる。このようなデータを収集し且つ／又は監査することで、製造業者は、正しく回収を実現し得た公認の再販売業者又は小売業者か或いは営利目的で該回収を無視し得る評判の悪い販売員かを識別するように支援され得る。

【００８１】

利用者は、製品６００に関する情報を取得することに関心があり得る。例えば、購入取引に関連して、利用者は、とりわけ、製品６００が未解決の製造業者回収の対象ではないこと、製品６００が製品回収及び／若しくは保守計画に従ってサービス提供されたことを確証し且つ／又は製品６００に関する他のいかなる情報も受け取りたいと欲し得る。ここで開示された実施形態に従って、利用者は、製品６００に関連付けられたセキュアタグ１００を必要とする認証プロセスを経て、このような情報を取得してもよい。

【００８２】

製品６００を検証し且つ／又は関連情報を取得するために、利用者は、認証デバイス２００を利用してもよい。例えば、いくつかの実施形態において、認証デバイス２００は、ここで述べられた信頼できる第三者機関１０２と対話するアプリケーションが読み込まれた利用者のスマートフォン又はタブレットであり得るが、これには限定されない。とりわけ、認証デバイス２００は、セキュアタグ１００が信頼できる第三者機関１０２によってプロビジョニングされた本物のタグであること、タグ１００がある特定の時間には認証デバイス２００の物理的に近接した位置にあること、ひいては、セキュアタグ１００に関連

付けられた製品６００が認証デバイス２００の近接位置にある本物で且つ／又は妥当な製品６００であることを確証してもよい。ある実施形態において、認証デバイス２００上で実行される製品情報アプリケーション６０２（例えば、信頼できる第三者機関１０２、製品６００の製造業者及び／又は他のあらゆる当事者によって提供されるアプリケーション）は、ここで開示された実施形態に従うタグ認証及び／又は存在検証プロセスに関連して利用されてもよい。

【００８３】

製品情報アプリケーション６０２がセキュアタグ１００を備える近接位置製品６００を検出する場合、製品情報アプリケーション６０２は、情報要求６０４を生成し且つ該情報要求６０４を製品６００の検証を要求する信頼できる第三者機関１０２へ伝達してもよい。ある実施形態において、情報要求６０４は、製品６００に関する情報（例えば、製品６００に関連する回収情報、サービス情報、所有権情報及び／又は他のあらゆる情報）に対する要求を含んでもよい。

【００８４】

上述したタグ認証プロセスと同様に、信頼できる第三者機関１０２は、チャレンジ情報２０８を生成し且つ該チャレンジ情報２０８を製品６００に含まれるセキュアタグ１００へ伝達してもよい。セキュアタグ１００は、チャレンジ情報２０８及びセキュアタグ１００によって格納された秘密情報１０４を利用してセキュアタグ１００によって実行される計算（例えばハッシュ計算又は同種のもの）の結果を含み得るチャレンジ応答６０６を伝達してもよい。チャレンジ応答６０６は、例えば、セキュアタグ１００及び／若しくは製品６００（例えば製品識別子）に関連付けられた製造番号並びに／又は他の識別情報等のセキュアタグ１００に関連付けられた他の情報を更に含んでもよい。

【００８５】

信頼できる第三者機関１０２は、チャレンジ応答６０６に含まれる結果を、複数の暗号鍵（例えば、秘密鍵、非対称鍵等）を複数の製品識別子に関連付けたデータベース６０８に格納され且つ信頼できる第三者機関１０２が所有する秘密情報、及び、チャレンジ情報２０８に基づいて、信頼できる第三者機関１０２がタグ認証モジュール２１４を使用して実行する類似の計算の結果と比較してもよい。結果が一致する場合、信頼できる第三者機関１０２は、セキュアタグ１００が信頼できる第三者機関１０２にプロビジョニングされた本物のタグであるため、製品６００が本物であることを判定し得る。結果が一致しない場合、信頼できる第三者機関１０２は、セキュアタグ１００が信頼できる第三者機関１０２にプロビジョニングされた本物のタグではないため、関連製品６００が本物ではないことを判定し得る。

【００８６】

製品６００が本物であることを判定すると、信頼できる第三者機関１０２は、信頼できる第三者機関及び／又は（例えば、製品メタデータデータベース５０８及び／又は同種のもの内の）別のサービスによって維持される製品６００に関連付けられた情報６１０を認証デバイス２００に提供してもよい。ある実施形態において、認証デバイス２００に提供された情報６１０は、情報要求６０４に関連して認証デバイス２００によって要求された情報を含んでもよい。例えば、情報６１０は、製品６００に関連付けられたいかなる製造業者回収の指示、製品６００に関連付けられたサービス履歴、製品６００に関連付けられた仕様及び／若しくは他の情報、製品６００に関連付けられた広告用材料、製品６００に関連付けられた所有権情報（例えば、ある製品が盗難に遭ったか否かの情報、所有権履歴情報等）並びに／又は製品６００に関連付けられた他のいかなる情報も含み得る。認証デバイス２００の利用者は、受け取った製品情報６１０（例えば「製品回収」）の指示をデバイス２００上で提示されてもよい。製品情報６１０は、法執行機関、製品製造業者及び／又は同種のもの等の一以上の第三者に更に提供されてもよい。

【００８７】

［出所制御及び製品登録］

【００８８】

ここで開示されたシステム及び方法のある実施形態は、価値連鎖及び／又はアフターマーケットにおける製品の登録所有者間での受け渡しをより厳重に制御及び／又は管理するために利用されてもよい。高価品目に関しては、現在の所有者は、特定製造番号が振られた製品の登録状態の変更を制限し且つ／又はかなりの確実さで該製品の全ての所有者の正確な記録を維持することが有利であり得る。例えば、高級品の所有者には該所有者の不動産への多数の招待客がおり、且つ／又は、高級品小売業者は多数の潜在的顧客に実際の顧客がある製品を購入する前に該製品を眺めさせる可能性がある。

【００８９】

一時的利用者が店内の新製品を購入したと「主張する」こと又はある住宅で客が自分のものではない製品の「権利を主張する」ことを防止するために、このような製品の現在の所有者は、信頼できる第三者機関及び／又は他のサービスによって維持された該所有者の製品に関連付けられた一部又は全てのデータ（例えば製品メタデータ）を施錠してもよい。例えば、管理された製品メタデータに包含される製品購入属性（例えば「新品」、「最初の販売」等）及び所有者属性（例えば現在の所有者属性）は、ある製品が店内で展示される場合、現在の所有者（例えば小売業者）によって施錠されてもよい。購入取引中、小売業者又は他の公認の当事者は、製品に関連付けられた購入属性を解錠し且つ該属性を（例えば「販売済み」に）変更し、所有者属性を解錠し且つ所有者の名前又は他の識別子を除外する或いは他の場合では該所有者属性を新規当事者（例えば購入者）に変更してもよい。この際、該購入者は、製品に関連付けられたタグを走査し且つ該製品の所有権を主張し得る。その後、該製品が再販売される場合、各取引が記録され且つ信頼できる第三者機関及び／又は他の信頼できるサービスによって安全に格納されてプロセスが繰り返され得る。このように、製品の出所は、該製品の固有部分として追跡及び／又は報告できる。いくつかの実施形態において、製品は、ここで開示されたシステム及び方法（例えば、著名な野球選手によって所有された最初の野球用バット、有名な俳優によって寄贈された専門デザイナーによる宝石類等）を利用して管理されたその検証可能な出所に基づいて価値が増し得る。

【００９０】

開示されたシステム及び方法の別の実施形態は、製品登録、保証管理、製品回収管理、製品寿命管理及び／又は同種のものと関連して利用されてもよい。例えば、製品（例えば新品又は中古品）が購入された後、新規所有者は、製造番号及び／若しくは機種番号、購入年月日並びに／又は同種のものをログ記録するためにある製品に添付された関連セキュアタグを走査し且つ自身の個人識別情報を（例えば、このような情報を信頼できる第三者機関及び／若しくは他の信頼できるサービスによって管理される製品メタデータ及び／又は他の情報に包含することで）該製品に関連付けてもよい。特定製品及び／又は製造番号に将来の回収（例えば安全のための自主回収）の見込みがある場合、製造業者は、製品の最初及び／又は現在の所有者の管理目録にアクセスし、該回収の関連当事者に情報提供してもよい。

【００９１】

ある製品に関連付けられたセキュアタグがここで開示された実施形態に従う認証デバイスを使用して走査される場合、利用者は、該製品に関連付けられた多様な情報を提供され得る。例えば、利用者は、該製品、該製品の製造番号、安全性考察、該製品に対してまだ有効であり得る保証若しくは保証書、特定製品、機種及び／若しくは製造番号に対するサポート又はサービスの終了、利用者が関心を持ち得る関連製品及び／若しくは提案並びに／又は該製品に関する他のいかなる関連情報に関連付けられた過去の回収に関する情報を提供されてもよい。製品回収及び／又は保証目的のため、ここで開示されたシステム及び方法の実施形態は、製造業者が偽造品の購入者に対して誤って補償しないことを保証するのに役立ち、且つ／又は、顧客が検証可能なセキュアタグが添付された純正品を所有していない場合、製造業者が顧客補償を拒否する検証可能な理由を提供し得る。

【００９２】

いくつかの実施形態において、信頼できる第三者機関及び／又は他のサービスは、どの

当事者が該信頼できる第三者機関及び／又はサービスによって管理される製品に関連付けられた各種属性及び／又は他のメタデータ若しくは情報を変更し得るかに関する認可を管轄してもよい。例えば、いくつかの実施形態において、信頼できる第三者機関及び／又はサービスは、ある製造業者のみが特定製造番号が振られた製品に対する回収状態を変更できること、ある製造業者のみが製品の購入状態を「新品」に変更できること、ある製造業者又は公認の修理センターのみが状態を工場標準に対して「改装済み」又は「修理済み」に変更できること、公認の再販売業者のみが購入状態を「最初の販売」に変更できること、登録所有者又は政府管轄機関のみが所有権を解消／変更できること、登録所有者のみが該製品に関する表明を追加でき且つ該製品を所有する場合にのみそれを追加できること（例えば、「２０２０ワールドシリーズで使用された幸運なバット」）並びに／又は同種のものを規定してもよい。このような方針は、従来のパスワード認証、‘６９３アプリケーションで記述されたようなＤＲＭ技術及び／又は同種のものを含むがこれに限定されない、いかなる適切な技術によっても実施できる。

【００９３】

有価、ロイヤルティ及び識別カード取引

【００９４】

民間通貨及び／若しくは小売業者ポイント、報酬ポイント並びに／又は同種のものは、有価、ロイヤルティ及び／又は他の識別カードに基づくシステムを使用して実現されてもよい。例えば、喫茶店等の小売業者は、顧客がロイヤルティ報酬（例えば報酬ポイント）を取引に関連して貯め且つそれを所定の製品及び／又はサービス（例えば、一杯分の無料コーヒー又は同種のもの）と交換できる報酬ポイントシステムを実現してもよい。しかしながら、このような民間通貨システムの安全を構築し且つ維持するためには、従来システムが典型的には民間通貨を流通させるための固有の顧客本人確認証発行、顧客識別認証及びバックエンドサービスを含む多数の要素を利用するのと同様に、多大な努力及び投資が必要とされ得る。更に、多数の異なる小売業者によって利用できる安全な民間通貨システムを構築するのは困難であり得る。

【００９５】

ここで開示されたシステム及び方法の実施形態は、有価、ロイヤルティ及び／又は他の識別カードに基づく民間通貨システムに関連して利用されてもよい。特に、ここで開示されたセキュアタグ認証技術の実施形態は、多様な機密保護取引に関連してセキュアタグを含む有価、ロイヤルティ及び／又は他の識別カードの存在証明を判定することに関連して利用されてもよい。とりわけ、取引に関連付けられた場所で本物のセキュアタグがプロビジョニングされた本物の有価、ロイヤルティ及び／又は他の識別カードの存在を検証することで、関連利用者が実際に該場所に存在することを判定してもよい。

【００９６】

図７Ａは、本開示の実施形態に従うセキュア電子タグを含むロイヤルティカードのプロビジョニングを例示する。ある実施形態において、有価、ロイヤルティ及び／又は他の識別カードに基づく民間通貨システムの実現に関心を持つ小売業者（例えば店舗所有者）７００又は他の当事者は、信頼できる第三者機関１０２又は民間通貨サービス（例えば、ウェブ基盤サービス又は同種のもの）を提供する他の信頼できるサービスプロバイダと対話してもよい。いくつかの実施形態において、信頼できる第三者機関１０２は、複数の当事者（例えば多数のレストラン又は同種のもの）に対してカードに基づく民間通貨サービスを提供してもよい。

【００９７】

小売業者７００又は他の当事者は、信頼できる第三者機関１０２と契約を結んでもよい。信頼できる第三者機関１０２との取引を開設することで、小売業者７００は、信頼できる第三者機関１０２によってサービス提供される得意客向けに民間通貨を生成してもよい。別の実施形態において、小売業者７００は、信頼できる第三者機関１０２によってサービス提供される民間通貨の可用性を一以上の他の当事者に拡張してもよい。更に別の実施形態（例えば、カードに関連付けられた価値が比較的小さい状況）において、セキュア及

び／又は秘密タグを利用する必要がない。その代わりに、例えば利用者所有物（例えば、カード上及び／又はスマートフォン・アプリケーション内）の単純なバーコードを利用してもよい。

【００９８】

小売業者７００は、ここで開示された実施形態に従うタグ及び／又は価値を含む一つ以上のカード及び／又は他のデバイス（例えば、キーホルダデバイス又は同種のもの）を提供されてもよい。該カードは、信頼できる第三者機関１０２を介してサービス提供される小売業者７００によって提供された民間通貨を利用したいと欲する一人以上の顧客に小売業者７００によって配布されてもよい。他の実施形態において、小売業者７００は、利用者にカードを配布するよりもむしろ、利用者のデバイス上に格納された値（例えば、製造時に組み込まれた機密保護及び／若しくは秘密値（並びに／又は該機密保護値及び／若しくは秘密値から導出した値）、信頼できる第三者機関１０２によって組み込まれた値、非機密保護値並びに／又は同種のもの）を利用してここで開示された技術を実装する利用者のスマートフォン又は他のデバイスにアプリケーションを配信してもよい。説明を簡単にするために、ここで述べられた例のいくつかはカードに基づくシステムに係るが、これらのシステムが利用者のスマートフォン又は他のデバイス上で実行されるアプリケーションをその代案として或いは追加として利用できる（これにより利用者が別途カードを携帯する必要がなくなる）ことは理解されるであろう。

【００９９】

図７Ｂは、本開示の実施形態に従うロイヤルティカード７０２認証プロセスを例示する。ロイヤルティカード７０２を小売業者の民間通貨を利用したいと欲する一人以上の顧客に配布した後、顧客は、認証デバイス２００を利用して小売業者所在地でのその実際の存在を認証するためにロイヤルティカード７０２を使用してもよい。例えば、小売業者は、顧客が一杯のコーヒーを購入する度にポイントに基づく民間通貨におけるある数のポイントを顧客に付与してもよい。顧客が小売業者を訪れる時、顧客は、（例えば、チェックインにより）小売業者の認証デバイス２００上で実行される民間通貨アプリケーションを利用してロイヤルティカード７０２を認証することでその物理的存在を確証し得る。ある実施形態において、認証デバイス２００に近接したロイヤルティカード７０２の存在の認証による顧客存在の確証は、ここで開示されたセキュアタグ認証技術の実施形態を利用して実行されてもよい。上述したように、認証デバイス２００は、開示されたセキュアタグ認証技術を実装するために使用され得るアプリケーションを実行するように構成されたいかなる適切なデバイス（例えばスマートフォン、タブレットコンピューティングシステム等）を備えてもよい。顧客存在を確証後、認証デバイス２００上にメッセージを表示し、チェックインプロセスの結果（例えば、顧客に関連付けられた民間通貨口座へのポイント付与）を示してもよい。

【０１００】

図７Ｃは、本開示の実施形態に従うロイヤルティカード７０２引き換えプロセスを例示する。ある実施形態において、顧客は、小売業者所在地を訪れる際に累積ポイント／通貨を引き換えてもよい。例えば、顧客は、小売業者から累積ポイント／通貨を使用して一杯のコーヒーを購入したいと欲し得る。累積ポイント／通貨と引き換えるために、顧客は、小売業者所在地に関連付けられた認証デバイス２００に近接したロイヤルティカード７０２の存在を認証することで小売業者存在を確証してもよい。ある実施形態において、小売業者は、認証デバイス２００上で実行される民間通貨アプリケーションを使用して、（例えば、引き換えられるポイント／通貨量又は同種のものを指定することで）民間通貨サービスを実現する信頼できる第三者機関に対してポイント／通貨引き換えプロセスを要求してもよい。ロイヤルティカード７０２認証プロセスの一部として、信頼できる第三者機関は、民間通貨アプリケーションを使用して小売業者によって指定された分だけロイヤルティカード７０２に関連付けられた勘定を借方に記入してもよく、且つ、成功した勘定借方を示す認証デバイス２００への指示を提供してもよい。

【０１０１】

ロイヤルティカードシステムに関連して以上のように述べられたが、類似プロセスが有価カード、識別カード及び／又は他のいかなるカードに基づく民間通貨システムに関連して開示され得ることは理解されるであろう。ある実施形態において、カードに関連付けられた口座残高は、ここで開示されたセキュアタグ認証操作を実行する、信頼できる第三者機関によって維持及び／又は他の場合では管理されてもよい。別の実施形態において、信頼できる第三者機関を利用してある開示されたセキュアタグ認証アプリケーションを実行してもよく、民間通貨を提供する別の第三者サービスを利用して口座残高を維持及び／又は他の場合では管理してもよい。

【０１０２】

［民間通貨取引］

【０１０３】

図８は、本開示の実施形態に従う有価カード８００認証及び取引プロセスを例示する。例示された実施形態において、信頼できる第三者機関１０２は、ここで開示されたセキュアタグ認証プロセスの実施形態を利用して有価カード８００を認証するための認証デバイス２００に関連して利用されてもよく、民間通貨サービス８０２は、有価カード８００に関連付けられた口座残高８０４を維持及び／又は他の場合では管理するために利用されてもよい。個別のシステムとして例示されているが、他の実施形態において、認証デバイス２００、信頼できる第三者機関１０２及び／又は民間通貨サービス８０２の一定の機能が単一システム及び／又はいかなる適切なシステムの組み合わせによって実行されてもよいことは理解されるであろう。

【０１０４】

有価カード８００は、信頼できる第三者機関１０２及び／又は別の信頼できるサービスによって秘密情報がプロビジョニングされたセキュアタグを備えてもよい。信頼できる第三者機関１０２は、とりわけセキュアタグの識別情報（例えばタグＩＤ）、対応するプロビジョニングされた秘密情報（例えば秘密鍵又は同種のもの）及び／又はセキュアタグに関連付けられた顧客アカウント情報（例えばアカウントＩＤ）を関連付けたデータベースを維持してもよい。いくつかの実施形態において、有価カード８００（及び／若しくはスマートフォン・アプリケーション並びに／又は同種のもの）は、セキュアタグを備える必要はなく、その代わりとして口座番号を含んでもよく、仮に例えばカードに関連付けられた金額を借方に記入するように要求された場合、認証のある追加形態（例えば、認証デバイス２００に入力するパスワード）は、要求が許可されたことを確証するために利用できる。

【０１０５】

認証デバイス２００上で実行される民間通貨アプリケーションは、ここで開示された実施形態に従うタグ又は値を備える近接位置有価カード８００を（例えば、ポーリングプロセス又は同種のものに応答して）検出してもよい。近接位置有価カード８００を検出すると、タグ認証デバイス２００は、チャレンジ情報Ｒを生成し且つ有価カード８００に含まれるセキュアタグへ伝達されてもよい。ある実施形態において、該チャレンジ情報は、暗号ノンス等のランダム及び／又は擬似ランダムに生成された値（説明を簡単にするために、ここでは「ランダム」値は真にランダムな値、擬似ランダムな値及び／又は同種のものの意味を包含する）を含んでもよいが、他の種類のチャレンジ情報は、開示されたシステム及び方法に関連して使用されてもよい。別の実施形態において、該チャレンジ情報は、（例えば、認証デバイス２００又は同種のものからの認証要求に応答して）信頼できる第三者機関１０２及び／又は別の信頼できるサービスによって生成され且つセキュアタグへ伝達されてもよい。

【０１０６】

チャレンジ情報Ｒを受け取った後、有価カード８００のセキュアタグは、少なくとも部分的には、セキュアタグによって格納された秘密情報に基づいて、ＭＡＣ及び／又は他の計算結果を生成してもよい。別の実施形態において、ＭＡＣは、他のデータ（例えば任意メッセージデータＭｓｇ）に更に基づいて生成されてもよい。ＭＡＣ、タグ識別情報、チ

ャレンジ情報及び／又は他のデータは、有価カード８００のセキュアタグから近接位置認証デバイス２００へ伝達されてもよく、該デバイス２００は、順繰りに該情報を信頼できる第三者機関１０２へ伝達してもよい。

【０１０７】

信頼できる第三者機関１０２は、受け取った情報（即ちタグＩＤ、Ｒ、ＭＡＣ、Ｍｓｇ等）に基づいてここで開示された実施形態に従うタグ認証プロセスを実行してもよい。例えば、信頼できる第三者機関１０２は、受け取ったタグ識別情報に基づいて有価カード８００のセキュアタグに関連付けられた機密保護鍵を取得してもよい。取得した機密保護鍵は、機密保護鍵及びチャレンジ情報並びに／又は認証デバイス２００（例えばＭｓｇ）から取得された他の情報に基づいてＭＡＣ及び／又は他の計算結果のコンピューティングに関連して使用されてもよい。一たび計算されれば、信頼できる第三者機関１０２は、計算されたＭＡＣを有価カード８００のセキュアタグによって生成された認証デバイス２００から受け取ったＭＡＣと比較してもよい。二つのＭＡＣ値が一致する場合、信頼できる第三者機関１０２は、セキュアタグ（ひいては有価カード８００）が本物であり且つ認証デバイス２００の近接位置にあることを示す認証結果を認証デバイス２００に返してもよい。二つのＭＡＣ値が一致しない場合、信頼できる第三者機関１０２は、セキュアタグ及び／又は有価カード８００が本物ではないことを示す認証結果を認証デバイス２００に返してもよい。

【０１０８】

受け取った認証結果がセキュアタグ及び／又は有価カード８００が本物であることを示す場合、認証デバイス２００は、該結果を有価カード８００に関連付けられた民間通貨サービス８０２へ転送してもよい。上述したように、民間通貨サービス８０２は、とりわけ、有価カード８００及び有価カード８００を必要とする取引に関連付けられた口座残高８０４を維持及び／又は他の場合では管理するために利用されてもよい。認証結果に加えて、認証デバイス２００は、有価カード８００の利用者が実行したいと欲する取引に関連する取引情報を民間通貨サービス８０２へ伝達してもよい。例えば、該取引情報は、有価カード８００に関連付けられた口座残高８０４に含まれるある量のポイントが減算及び／若しくは加算され且つ／又は別の口座（例えば、認証デバイス２００の利用者に関連付けられた口座又は同種のもの）へ転送されることを要求してもよい。このような情報を利用して、民間通貨サービス８０２は、関連取引プロセスを実行してもよい。

【０１０９】

口座取引プロセスを実行した後で、民間通貨サービス８０２は、該取引が成功したことの確認書を認証デバイス２００へ伝達してもよい。認証デバイス２００の利用者は、該取引が実行されたことを認証するためのこのような確認書を利用してもよく、且つ、取引の他の態様（例えば、有価カード８００の利用者に購入製品又は同種のものを提供すること）を発効させるための行為を行ってもよい。

【０１１０】

別の実施形態において、利用者及び／又は有価カード８００に関連付けられた口座識別は、有価カード８００及び／又は認証デバイス２００によって民間通貨サービス８０２へ伝達されてもよい。このような口座情報を認証した後、民間通貨サービス８０２は、とりわけ、有価カード８００及び／若しくは有価カード８００の利用者に関連付けられた利用可能な残高を判定するために使用され得る認証デバイス２００並びに／又は有価カード８００へ口座残高情報を伝達してもよい。特に例示していないが、ある実施形態において、認証デバイス２００の利用者が民間通貨サービス８０２によって提供された民間通貨を利用する権限があることを認証するために、認証プロセスが認証デバイス２００及び民間通貨サービス８０２間で実行されてもよい。

【０１１１】

［アクセスカード照合］

【０１１２】

ここで開示されたシステム及び方法の実施形態は、アクセスカード（例えばアクセスパ

ス、交通パス及び／又は同種のもの）の信憑性及び／又は状態を検証するために利用されてもよい。開示されたシステム及び方法は、とりわけ、セキュアタグを備えるアクセスカードが信頼できる第三者機関によってプロビジョニングされた本物のカードであることを検証するために利用されてもよい。更に、開示されたシステム及び方法は、認証されたアクセスカードに関連付けられた口座が有効で且つ／又は特定取引には充分な金額を有するか否かを判定するために利用されてもよい。例えば、開示されたシステム及び方法の実施形態は、公共交通機関管理所によって発行された認証アクセスカード（例えば交通カード）が関連認証デバイスに提示されたこと及び提示されたアクセスカードに関連付けられた口座が有効であり且つ／又は特定旅行用に利用可能な充分な預金を有することを判定するために利用されてもよい。

【０１１３】

図９は、本開示の実施形態に従う交通カード９００の認証を例示する。上述したように、セキュアタグ１００は、信頼できる第三者機関１０２及び／又は別の信頼できるサービスプロバイダによって秘密情報１０４がプロビジョニングされてもよく、且つ、顧客に関連付けられたカード９００又は他のデバイスに安全に関連付けられてもよい。カード９００は、交通カード（例えばバスカード、鉄道カード及び／又は同種のもの）として例示されるが、カード９００は、例えば建物アクセスカード、スキーパスカード及び／又は同種のものを含むいかなる種類のアクセスカードも含み得る。

【０１１４】

公共交通機関管理所は、交通カード９００をその運賃システムに関連して利用したいと欲し得る。運賃取引に関連して、公共交通機関管理所は、利用者によって提示された交通カード９００が公共交通機関管理所又は別の信頼できる当事者によって発行された本物のカードであって偽造物ではないこと、交通カード９００が取引のターミナルで物理的に存在すること並びに交通カード９００が特定運賃には充分な活性状態及び／又は関連残高を有することを確証したいと欲し得る。開示されたシステム及び方法の実施形態は、このような行為を運賃取引に関連して実行するために公共交通機関管理所によって利用されてもよい。

【０１１５】

公共交通機関管理所は、該管理局が利用者に運賃取引を許可したいと欲する場所において、ここで開示された実施形態に従うカード照合アプリケーション９０２を実行する複数の認証デバイス２００を配布してもよい。例えば、認証デバイス２００は、公共交通機関管理所バス、鉄道車両、乗り換え拠点及び／又は同種のもので配布されてもよい。ここで開示された実施形態が、セキュアタグ認証及び／又は存在検証に関連して比較的低費用の汎用タグ認証デバイス２００（例えばスマートフォン又はタブレットコンピューティングデバイス）の利用を許可するため、公共交通機関管理所は、従来の運賃取引システムよりも概して低費用で開示された実施形態に従う運賃取引を実現し得る。

【０１１６】

運賃取引を開始するために、利用者は、秘密情報１０４をプロビジョニングされたセキュアタグ１００を備える交通カード９００を近接位置認証デバイス２００へ提示してもよい。いくつかの実施形態において、カード照合アプリケーション９０２は、セキュアタグ１００を備える近接位置交通カード９００を検出するためにタグ認証デバイス２００を利用してポーリング又は他のプロセスを実行してもよい。カード照合アプリケーション９０２がセキュアタグ１００を備える近接位置交通カード９００を検出する場合、カード照合アプリケーション９０２は、カード照合要求９０４を生成し且つ該カード照合要求９０４を交通カード９００の検証を要求する信頼できる第三者機関１０２へ伝達してもよい。

【０１１７】

ここで開示されたタグ認証プロセスに従って、公共交通機関管理所に関連付けられた信頼できる第三者機関１０２は、チャレンジ情報２０８を生成し且つ該チャレンジ情報２０８を交通カード９００に含まれるセキュアタグ１００へ（例えば、認証デバイス２００を介して）伝達してもよい。別の実施形態において、該チャレンジ情報２０８は、認証デバ

イス２００によって生成され且つ交通カード９００及び信頼できる第三者機関１０２へ伝達されてもよい。セキュアタグ１００は、チャレンジ情報２０８及びセキュアタグ１００によって格納された秘密情報１０４を使用してセキュアタグ１００によって実行された計算（例えばハッシュ計算又は同種のもの）の結果を含み得るチャレンジ応答９０６を生成してもよい。チャレンジ応答９０６は、交通カード９００及び／又はセキュアタグ１００に関連付けられた識別子を更に含んでもよい。チャレンジ応答９０６は、認証デバイス２００に伝達されてもよく、且つ、認証のために信頼できる第三者機関１０２へ転送されてもよい。

【０１１８】

信頼できる第三者機関１０２は、チャレンジ応答９０６に含まれる結果を、データベース９０８に格納され且つ信頼できる第三者機関１０２が所有する秘密情報、及び、チャレンジ情報２０８に基づいて、信頼できる第三者機関１０２がタグ認証モジュール２１４を使用して実行する類似の計算の結果と比較してもよい。いくつかの実施形態において、特定セキュアタグ１００に関連付けられたデータベース９０８に格納された秘密情報は、交通カード９００及び／又はチャレンジ応答９０６に含まれるセキュアタグ１００に関連付けられた識別子を使用して信頼できる第三者機関１０２によって識別されてもよい。チャレンジ応答９０６に含まれる結果が信頼できる第三者機関によって生成された結果と一致する場合、信頼できる第三者機関１０２は、セキュアタグ１００が信頼できる第三者機関１０２によってプロビジョニングされた本物のタグであるため、交通カード９００が本物であって偽造物ではないことを判定してもよい。結果が一致しない場合、信頼できる第三者機関１０２は、セキュアタグ１００が信頼できる第三者機関１０２によってプロビジョニングされた本物のタグではないため、関連交通カード９００が本物ではないことを判定してもよい。

【０１１９】

交通カード９００が本物ではないと判定された場合、信頼できる第三者機関１０２は、カード９００が本物ではないことを示すカード照合応答９１６を認証デバイス２００へ伝達してもよい。別の実施形態において、一以上の他の当事者（例えば法執行当局又は同種のもの）は、信頼できる第三者機関１０２によって交通カード９００が本物ではないと識別されたことを通知してもよく、そのように判定が偽造行為を示してもよい。

【０１２０】

交通カード９００が本物であると判定された場合、信頼できる第三者機関１０２及び／又は別のシステムは、交通カード９００が（例えば、管理カード状態データベース９１２又は同種のものにおいて識別された通りに）活性状態である口座に関連付けられているか否かを判定し、カード９００の所有者が運賃取引に関連して交通システムにアクセスすることを許可してもよい。別の実施形態において、信頼できる第三者機関１０２及び／又は別のシステムは、交通カード９００に関連付けられた口座が運賃取引に関連して特定運賃には（例えば、管理カード価値データベース９１４に反映された通りに）充分な残高又は同種のものを有するか否かを判定してもよい。交通カード９００の利用者は、（例えば、信頼できる第三者機関、公共交通機関管理所等の関連サービスプロバイダ及び／又は同種のものによって提供されたウェブインタフェースを介して）交通カード９００に関連付けられた口座に預金することで交通カード９００のカード状態及び／又はカード価値を管理するために信頼できる第三者機関１０２と対話してもよい。

【０１２１】

信頼できる第三者機関１０２が、交通カード９００に関連付けられた口座が充分な残高及び／又は活性状態を有すると判定した場合、認証デバイス２００に送信されたカード照合応答９１６は、運賃取引が成功したという指示を含み得る。信頼できる第三者機関１０２が、交通カード９００に関連付けられた口座が不充分な残高及び／又は不活性状態を有すると判定した場合、認証デバイス２００に送信されたカード照合応答９１６は、運賃取引が失敗したという指示を含み得る。認証デバイス２００の利用者は、受け取ったカード照合応答９１６の内容の指示（例えば「カードは有効」又は同種のもの）をデバイス２０

０上で提示されてもよい。
【０１２２】
交通カード９００に関連付けられた状態及び／又は口座残高は、運賃取引に従って信頼できる第三者機関１０２によって更新されてもよい。例えば、交通カード９００に関連付けられた勘定は借方に記入される又は同種のものが実施されてもよい。同様に、交通カード９００に関連付けられた状態は、運賃取引に関連して変更されてもよい。
【０１２３】
いくつかの実施形態において、信頼できる第三者機関１０２によってカードメタデータデータベース９１０に格納され且つ交通カード９００に関連付けられたメタデータは、信頼できる第三者機関１０２によって認証デバイス２００へ伝達されたカード照合応答９１６に含まれてもよい。例えば、交通カードに関連付けられた利用者の写真、パスコード及び／又は他の接触情報は、カード照合応答９１６に関連して信頼できる第三者機関１０２によって認証デバイス２００へ伝達されてもよい。とりわけ、交通カード９００が充分な口座残高及び／若しくは有効な関連状態を有する本物のカードであることだけでなく、運賃取引に関連して交通カード９００を提示する個人が該カードを利用する権限を有し且つ／又は他の場合では該カードに関連付けられていることを判定する際に、カードメタデータが認証デバイス２００の利用者によって使用されてもよい。
【０１２４】
［反射攻撃の緩和］
【０１２５】
図１０は、本開示の実施形態に従う反射攻撃を緩和し得るセキュアタグ認証プロセスを例示する。例示された実施形態において、信頼できる第三者機関１０２は、ここで開示されたタグ認証プロセスの実施形態を利用してセキュアタグ１００を認証するための認証デバイス２００及び店舗サービス１０００に関連して使用されてもよい。個別のシステムとして例示されているが、他の実施形態において、認証デバイス２００、信頼できる第三者機関１０２及び／又は店舗サービス１０００の一定の機能が単一システム及び／又はいかなる適切なシステムの組み合わせによって実行されてもよいことは理解されるであろう。
【０１２６】
セキュアタグ１００は、信頼できる第三者機関１０２及び／又は別の信頼できるサービスによって秘密情報をプロビジョニングされてもよい。認証デバイス２００（例えば、店舗又は他の小売店に関連付けられた認証デバイス）上で実行されるタグ認証アプリケーションは、いかなる適切な方式で近接位置セキュアタグ１００を検出してもよい。
【０１２７】
近接位置セキュアタグ１００を検出すると、サービスアプリケーション（例えば、店舗に関連付けられたサービス）は、認証デバイス２００上で起動されてもよい。いくつかの実施形態において、該サービスアプリケーションは、店舗サービス１０００によって提供される遠隔サービスにログインしてもよい。店舗サービス１０００は、チャレンジ情報を生成し且つ認証デバイス２００を介して該チャレンジ情報をセキュアタグ１００へ伝達してもよい。ある実施形態において、該チャレンジ情報は、暗号ノンス等のランダム及び／又は擬似ランダムに生成された値を含んでもよいが、他の種類のチャレンジ情報は、開示されたシステム及び方法に関連して使用されてもよい。別の実施形態において、該チャレンジ情報は、信頼できる第三者機関１０２及び／又は認証デバイス２００によって生成され且つセキュアタグ１００へ伝達されてもよい。
【０１２８】
チャレンジ情報を受け取った後、セキュアタグ１００は、少なくとも部分的には、セキュアタグによって格納された秘密情報に基づいて、ＭＡＣ及び／又は他の計算結果を生成してもよい。別の実施形態において、ＭＡＣは、他のデータに基づいて更に生成されてもよい。ＭＡＣ、タグ識別情報、チャレンジ情報及び／又は他のデータは、セキュアタグ１００から近接位置認証デバイス２００へ伝達されてもよく、該デバイス２００は、順繰りに該情報を信頼できる第三者機関１０２へ伝達してもよい。

【０１２９】
信頼できる第三者機関１０２は、受け取った情報（例えば、タグＩＤ、ノンス、ＭＡＣ等）に基づいてここで開示された実施形態に従うタグ認証プロセスを実行してもよい。例えば、信頼できる第三者機関１０２は、受け取ったタグ識別情報に基づいてセキュアタグ１００に関連付けられた機密保護鍵を取得してもよい。取得した機密保護鍵は、機密保護鍵及びチャレンジ情報並びに／又は認証デバイス２００から取得された他の情報に基づいてＭＡＣ及び／又は他の計算結果のコンピューティングに関連して使用されてもよい。一たび計算されれば、信頼できる第三者機関１０２は、計算されたＭＡＣをセキュアタグ１００によって生成された認証デバイス２００から受け取ったＭＡＣと比較してもよい。二つのＭＡＣ値が一致する場合、信頼できる第三者機関１０２は、セキュアタグ１００が本物であり且つ認証デバイス２００の近接位置にあることを示す認証結果（例えば状態）を認証デバイス２００に返してもよい。二つのＭＡＣ値が一致しない場合、信頼できる第三者機関１０２は、セキュアタグ１００が本物ではないことを示す認証結果（例えば状態）を認証デバイス２００に返してもよい。
【０１３０】
ある実施形態において、状態（例えば「本物である」或いは「本物ではない」）に加えて、認証デバイス２００に返された認証結果は、信頼できる第三者機関１０２によって署名されたチャレンジ情報、認証時間及びタグ識別情報を更に含んでもよい。認証デバイス２００は、署名されたチャレンジ情報、認証時間及びタグ識別情報を店舗サービス１０００へ転送してもよい。ある実施形態において、店舗サービス１０００は、ロイヤルティポイントを報酬として付与し且つ／又はセキュアタグ１００の認証成功に関連付けられた他のいかなる機能を実行してもよい。
【０１３１】
店舗サービス１０００は、該認証時間が特定期間内にあることを確認してもよい。換言すれば、店舗サービス１０００は、署名された認証時間が「真新しいもの」であることを確認してもよい。店舗サービス１０００は、署名されたチャレンジ情報の「真新しさ」を更に確認し、該情報が特定期間内に発行されたことを判定してもよい。これらの値が特定期間内ではない（即ち真新しいものではない）場合、店舗サービス１０００は、ロイヤルティポイントを報酬として付与すべきでない又はセキュアタグ１００の認証に関連付けられた他の機能を実行すべきであることを判定してもよく、それは署名された認証時間及び／又はチャレンジ情報の年数が可能な反射攻撃を示す可能性があるからである。ある実施形態において、認証時間及び／又はチャレンジ情報が信頼できる第三者機関１０２によって署名され得るため、この機構は認証デバイス２００の安全性に依存しなくてもよいことから、潜在的反射攻撃を防止するための開示された実施形態の能力を向上できる。
【０１３２】
［タグ確認及び存在確認サービス］
【０１３３】
本明細書に開示されるシステム及び方法のある実施形態は、消費者間（「Ｃ２Ｃ」）ビジネスなど（例えば、オンライン競売サービス、クラシファイド広告サービスなど）の電子商取引サービスに関連して使用されてもよい。例えば、オンライン競売サービスにおいて、入札者が、売り手が選択してアップする、製品に関して限られた情報（例えば、画像及び／又は説明）にアクセスするだけで、オンライン競売サービスにおいて売り物の製品の真正性を保証することは、入札者及び／又はサービスにとって困難だろう。本明細書に開示される実施形態に合わせて、セキュアなタグは製品と関連させてもよく、それによってセキュアなタグを使用して、信頼される権限を有する製品、及び／又は他のサービス提供者、の認証を可能にする。製品が信頼される権限によって認証される場合、表示は、電子商取引サービスに提供されてもよく、サービスが、売り手が与えられた製品を実際に物理的に所有することを検証し、品目に関連して売り手から提供される製品情報が製造業者等からの製品情報と一致するかどうかを決定することを可能にする。
【０１３４】

図１１は、本開示の実施形態に合わせて、電子商取引サービス１１００に関する製品確認を例示する。ある実施形態において、電子商取引サービス１１００は、例えば、オンライン競売サービス、クラシファイド広告サービス等などのＣ２Ｃサービスを含んでもよい。様々な他のタイプ電子商取引サービスが、本明細書に開示されるタグ認証及び／又は存在確認プロセスを使用してもよく、任意の好適なタイプの電子商取引又は他のサービスが、開示された実施形態を実装してもよいことは、理解されるだろう。

【０１３５】

電子商取引サービス１１００を使用する、購入トランザクションに関連して、ユーザーは、とりわけ、売り手によって販売のために提供される製品５００が、模造品でない、且つその製造業者からの真正な製品であることを確認し、製品５００が新しいか又は以前に新品として販売されなかったことを確かめ、製品５００等に関して所有履歴情報を取得することを望んでもよい。本明細書に開示される実施形態に合わせて、そのような情報は、製品５００、認証装置２００、及び／又は信頼される権限１０２と関連するセキュアなタグ１００を要する、認証プロセスを通して取得されてもよい。そのような情報は、電子商取引サービス１１００によって潜在的な買い手に提供されるインタフェース１１０２に関連して、更に提示されてもよい。

【０１３６】

製品５００の真正性を確認することは、図５に関連して上記に詳述されるように、認証装置２００及び／又は信頼される権限１０２を使用して、実施されてもよい。例えば、売り手は、電子商取引サービス１１００によって管理されるオンライン競売において売物の製品５００を提供したい場合、ユーザーは、電子商取引サービス１１００によって製品５００の真正性を確認することを選択してもよい。ある実施形態において、電子商取引サービス１１００によって製品５００を確認することは、とりわけ、結果として、潜在的な買い手がその確認によって製品５００により高い価値がつくと考えることになる。

【０１３７】

製品５００を確認するために、売り手は、認証装置２００（例えば、スマートフォン又はタブレット・コンピュータ装置）で実行する製品確認アプリケーション５０２を使用してもよい。上記に詳述されるように、セキュアなタグ１００、認証装置２００、及び／又は信頼される権限１０２を利用する、確認プロセスが実施されてもよく、結果として、確認応答５０６が信頼される権限１０２によって発行され、認証装置２００に伝送される。ある実施形態において、確認応答５０６は、電子商取引サービス１１００に更に伝送されてもよい。確認応答５０６を受けると、電子商取引サービス１１００は、関連するインタフェース１１０２を介して関連する製品５００に関連して潜在的な買い手に確認情報を提示してもよい。更なる実施形態において、確認応答５０６は、インタフェース１１０２を介して電子商取引サービス１１００によって潜在的な買い手に提示されるだろう製品５００（例えば、信頼される権限１０２及び／又は別のサービスによって維持される製品メタデータ５０８）に関して、付加情報を更に含んでもよい。

【０１３８】

図１２は、本開示の実施形態に合わせて、電子商取引サービス１１００に関連して別の製品確認プロセスを例示する。例示された実施形態において、信頼される権限１０２は、本明細書に開示されるタグ認証プロセスの実施形態を使用して、セキュアなタグを含む製品を認証するための、認証装置２００及び電子商取引サービス１１００に関連して使用されてもよい。単独のシステムとして例示されているが、他の実施形態において、認証装置２００、信頼される権限１０２、及び／又は電子商取引サービス１１００のある機能が、単一のシステム、及び／又はシステムの任意の好適な組み合わせによって実施されてもよいことは理解されるだろう。

【０１３９】

製品と関連するセキュアなタグ１００は、信頼される権限１０２及び／又は別の信頼されるサービスによって、秘密情報を供給されてもよい。売り手と関連する認証装置２００で実行する、製品確認アプリケーション（例えば、電子商取引サービス１１００によって

提供されるアプリケーション）は、本明細書に開示される実施形態に合わせて、最も近くに位置するセキュアなタグ１００を検出してもよい。

【０１４０】

最も近くに位置するセキュアなタグ１００を検出すると、アプリケーションは、電子商取引サービス１１００によって提供されるサービスにログインするだろう、装置２００で起動されてもよい。電子商取引サービス１１００は、チャレンジ情報を生成し、認証装置２００を介してそれをセキュアなタグ１００に伝送してもよい。ある実施形態において、チャレンジ情報は、ランダム及び／又は疑似ランダムに生成した、暗号ノンスなどの値を含んでもよいが、他のタイプのチャレンジ情報は、開示されたシステム及び方法に関連して、更に使用されてもよい。更なる実施形態において、チャレンジ情報は、信頼される権限１０２及び／又は認証装置２００によって、生成され、セキュアなタグ１００に伝送されてもよい。

【０１４１】

チャレンジ情報を受信した後に、セキュアなタグ１００は、セキュアなタグによって記憶される秘密情報に、少なくとも部分的には基づいて、ＭＡＣ、ハッシュ、及び／又は他の計算結果を生成してもよい。更なる実施形態において、計算は、他のデータに基づいて更に生成されてもよい。計算結果、タグ識別情報、チャレンジ情報、及び／又は他のデータは、セキュアなタグ１００から、次に信頼される権限１０２に情報を伝送されるだろう、最も近くに位置される認証装置２００に伝送されてもよい。

【０１４２】

信頼される権限１０２は、受信される情報（例えば、タグＩＤ、ノンス、ＭＡＣなど）に基づいて、本明細書に開示される実施形態に沿ったタグ認証プロセスを実施してもよい。例えば、信頼される権限１０２は、受信されるタグ識別情報に基づいて、セキュアなタグ１００と関連するセキュアなキーを取り出してもよい。取り出されたセキュアなキーは、認証装置２００から受信される、セキュアなキー及びチャレンジ情報及び／又は他の情報に基づいて、ＭＡＣ、ハッシュ、及び／又は他の計算結果を計算することに関して使用されてもよい。一旦計算されると、信頼される権限１０２は、その計算結果と、認証装置２００から受信され、且つセキュアなタグ１００によって生成される計算結果とを比較してもよい。２つの値が一致する場合、信頼される権限１０２は、認証装置２００に認証結果（例えば、ステータス）を戻し、セキュアなタグ１００が真正であることを示す。２つの値が一致しない場合、信頼される権限１０２は、認証装置２００に認証結果（例えば、ステータス）を戻し、セキュアなタグ１００が真正でないことを示。

【０１４３】

ある実施形態において、ステータス（例えば、「真正である」又は「真正でない」）に加えて、認証装置２００に戻された認証結果は、チャレンジ情報、認証時間、及び／又は、信頼されるサービス１０２によって署名される、タグ識別情報を更に含んでもよい。認証装置２００は、電子商取引サービス１１００に、署名付きチャレンジ情報、認証時間、及びタグ識別情報を送ってもよい。いくつかの実施形態において、電子商取引サービス１１００は、売り手が認証を実施したことを確かめる、署名付きチャレンジ情報、売り手がいつ認証を実施したかを確かめる、署名付き認証時間、及び、売り手がどの製品を認証したかを確かめる、署名付きタグ識別情報を更にチェックしてもよい。更なる実施形態において、電子商取引サービス１１００は、製品の確認の表示を潜在的な買い手に提供し、且つ／又は、セキュアなタグ１００の成功している認証と関連する任意の他の機能を実施してもよい。

【０１４４】

［レビュー・サービスの存在確認］

【０１４５】

本明細書に開示される、ある実施形態は、オンラインレビュー・サービスに関連してアップされる、特定の製品及び／又はビジネスの、個人のコメント、意見、及び／又はレビューの妥当性を向上させるために使用されてもよい。例えば、レストランに関してオンラ

インレビュー・サービスにアップされる、個人によるレビューは、レビュアがレストランを実際に訪れたことが認証できる場合、レビュー・サービスのユーザーにとってより価値が高いと考えられるだろう。同様に、製品のレビュアが、彼らがレビューをアップした時点で、レビューされた製品を実際に所有していたという製品レビューに関する表示を提供されることは、製品レビュー・サービスのユーザーにとって有益であろう。

【０１４６】

本明細書に開示されるシステム及び方法の実施形態は、特定の時間に特定の場所において真正な電子タグが存在するというセキュアな検証を提供してもよい。ビジネスの位置における認証装置に関連して使用される場合に、位置におけるユーザーの存在を検証するために使用されるだろう、セキュアな電子タグ及び／又は秘密の値を含む、カード、スマートフォン・アプリケーション、又は他の装置を、レビュー・システムのユーザーは提供されてもよい。例えば、そのような検証は、アップされたレビューに関連する、ビジネス及び／又は製品のレビュアが、実際にビジネスを訪れ、及び／又は製品を所有したことを検証するために使用されてもよい。レビューされた位置におけるレビュアの存在及び／又はレビューされた製品の所有の検証は、信頼性がより低いレビューとビジネス及び／又は製品の直接の知識に基づいたレビューとを区別するため、レビュー・サービスのユーザーの能力を向上させるだろう。

【０１４７】

図１３は、本開示の実施形態に沿ったレビュー・サービス１３００に関連して、存在確認を例示する。製品レビュー・サービス１３００に関連して、製品レビュア１３０２は、とりわけ、彼らがレビューされた真正な製品を実際に所有していることを確認することを望むだろう。同様に、ビジネス・レビュー・サービス１３００に関連して、ビジネス・レビュア１３０２は、とりわけ、彼らがレビューされたビジネスを実際に訪れていることを確認することを望むだろう。本明細書に開示されるセキュアなタグ認証技術の実施形態は、様々なレビュー・サービス１３００に関連して、レビュアに関連する製品及び／又はビジネスの存在の証明を決定する際に使用されてもよい。

【０１４８】

レビュア１３０２が、真正な製品を所有し、及び／又は特定のビジネスに身体的に出席していることの確認は、本明細書に開示されるセキュアなタグの許可及び／又は存在検証技術を使用して、認証装置２００及び／又は信頼される権限１０２を使用して実施されてもよい。例えば、レビュア１３０２が、彼らが実際にレストランを訪れたレビュー１３０４に関して検証したい場合、レビュアは、信頼される権限１０２によって、レストランにおける彼らの存在を確認することを選択してもよい。彼らの存在を確認するために、レビュア１３０２は、レビュア１３０２と関連するセキュアなタグ１００を、レストランの位置と関連する認証装置２００（例えば、出入り口等に又はその近くに位置する装置）で実行するチェックイン・アプリケーション１３０６に、提示してもよい。他の実施形態に関連して上記に述べられるように、セキュアなタグ１００、認証装置２００、及び／又は信頼される権限１０２を利用する確認のプロセスが実施されてもよく、結果として、認証応答２１８が、信頼される権限１０２によって発行され、装置２００に近接するセキュアなタグ１００の存在を確認する認証装置２００に伝送されることになる。いくつかの実施形態において、タグは、レストランに（例えば、レストランのテーブルに封止され）置くことができ、レビュアが信頼される権限１０２からタグ認証応答２１８を得るために認証装置２００を使用する場合、装置２００又は信頼される権限１０２は、存在の証明として、レビュー・サービス１３００にそれを送ってもよい。

【０１４９】

ある実施形態において、認証応答２１８は、レビュー・サービス１３００に更に伝送されてもよい。認証応答２１８を受けると、レビュー・サービス１３００は、レビュア１３０２がレビューされたレストラン（例えば、「検証されたユーザーレビュー」等）を実際に訪れたことを示しているアップされたレビュー１３０４に関連して、確認情報を与えてもよい。類似する実施形態が、製品レビュー・サービス１３００に関連して使用されても

よく、ここで、製品レビュア１３０２が、認証装置２００を使用して、信頼される権限１０２によってレビューされた製品の彼らの所有を確認し、製品のレビューに関連する存在について製品レビュー・サービス１３００に伝送されるような確認を有してもよいことは理解されよう。

【０１５０】

上記に述べられるように、代わりの実施形態では、レビュア１３０２は、チェックイン・アプリケーション１３０６を実行する認証装置２００を所有していてもよい。認証可能なタグ１００は、レストランの位置（例えば、出入り口に又は近くに、テーブルの中又は上に、等に位置するタグ）と関連させてもよい。レビュア１３０２は、認証装置２００、セキュアなタグ１００、及び／又は信頼される権限１０２を利用して、確認プロセスを実施してもよく、結果として、認証応答２１８が、信頼される権限１０２によって発行され、ユーザーの認証装置２００に伝送され、装置２００に近接するセキュアなタグ１００の存在を確認することになる。この応答２１８は、レストランの位置におけるレビュア１３０２の存在の証明として利用されてもよい。

【０１５１】

更なる実施形態において、応答２１８は、信頼される権限１０２からレビュー・サービス１３００に伝送されてもよい。いくつかの実施形態において、応答２１８は、認証装置２００からレビュー・サービス１３００に伝送されてもよい。レビュー・サービス１３００は、レストランの位置におけるレビュア１３０２の存在の証明として、受信された応答２１８を利用してもよく、レビュア１３０２がレビューしたレストラン（例えば、「検証されたユーザーレビュー」等）を実際に訪れたことを示す、アップされたレビュー１３０４に関する情報を提示する。

【０１５２】

［文書の署名サービス］

【０１５３】

本明細書に開示されるシステム及び方法は、信頼される文書の署名サービスに関連して、更に使用されてもよい。ある管轄において、署名、印鑑、及び／又は封印は、法的効力を有する文書向けに、文書に適用されることを要求されるだろう。文書に適用される場合、署名、印鑑、及び／又は封印は、任意の好適な記号、画像、及び／又はそれらの組み合わせを含む、ユニークなマーク（例えば、グラフィック・マーク）を表してもよい。ある実施形態において、署名、印鑑、及び／又は封印は、組織と関連してもよく、文書に適用されるときに、文書についての組織の賛成、文書の内容の認証、文書等の署名者としての権限（例えば、組織を代表して行為を行う権限）を意味してもよい。

【０１５４】

とりわけ、開示され、信頼される文書の署名サービスの実施形態は、電子の署名、印鑑、及び／又は封印を利用している当事者が、そうするために権限を有することを保証してもよい。ある実施形態において、開示された実施形態を使用している、電子の署名、押印、及び／又は封印は、彼らが文書を作成するだろう前に秘密情報の所有を明示しているユーザーを関わらせてもよい。ある実施形態において、秘密情報の所有は、秘密情報を記憶している、セキュアなタグ、又は他の関連品目（例えば、物理的な印鑑、封印、許可カードなど）の所有を明示することを通して明示されてもよい。セキュアなタグの所有を明示することによって、ユーザーは彼らの許可を、文書の署名サービスを用いて電子の署名、印鑑、及び／又は封印を適用するために、認証してもよい。

【０１５５】

図１４は、本開示の実施形態に合わせて、文書署名サービス１４０２に関連して、ユーザーの認証を例示する。ある実施形態において、認証は、ユーザーが、セキュアなタグ１００に記憶される、ある秘密情報１０４を所有するかどうか、且つ、拡張して、文書に署名、印鑑、及び／又は封印を電子的に適用することを許可するかどうかの決定を含んでもよい。いくつかの実施形態において、セキュアなタグ１００は、関連する署名、印鑑、及び／又は封印を適用するために、ユーザーが彼らの権限によって所有する、物理的な印鑑

、封印１４００、ペン、許可カード、モバイル装置等などの物理的な品目に含まれてもよい。様々な他のタイプの品目が、本明細書に開示されるプロセスに関連して使用されてもよく、且つ、セキュアなタグ１００（又は、例えば、スマートフォンのメモリに記憶される秘密の値を利用する、セキュアなアプリケーションを走らせているスマートフォン）を含む任意のタイプの品目が、開示された実施形態で使用されてもよいことは理解されるだろう。

【０１５６】

ユーザーが、供給された秘密情報１０４を記憶しているセキュアなタグ１００を含む、封印１４００を所有することの確認は、本明細書に開示される、セキュアなタグ許可及び／又は存在検証の技術を実装している、認証装置２００及び／又は信頼される権限１０２を使用して実施されてもよい。例えば、ユーザーが電子の署名、印鑑、及び／又は封印を文書に適用したい場合、ユーザーは、彼らが信頼される権限１０２によって封印１４００を所有していることを確認することを選択してもよい。封印１４００の彼らの所有を確認するために、ユーザーは、認証装置２００（例えば、ユーザー及び／又は文書署名サービス１４０２と関連する装置）で実行する封印認証アプリケーション１４０４に、封印１４００を与えてもよい。他の実施形態に関する上述のプロセスと類似して、封印認証要求１４０６は、認証装置２００から信頼される権限１０２に伝送されてもよく、セキュアなタグ１００、認証装置２００、及び／又は信頼される権限１０２を利用して、認証プロセスを初期化する。認証プロセスは、結果として、封印認証応答１４０８が、信頼される権限１０２によって発行され、装置２００に近接するセキュアなタグ１００の存在を確認する認証装置２００に伝送されることになるだろう。ある実施形態において、封印認証応答１４０８は、関連する署名、印鑑、及び／又は封印を適用するために、ユーザーの許可の証明として、文書署名サービス１４０２に更に伝送されてもよい。

【０１５７】

図１５は、本開示の実施形態に合わせて、文書署名サービス１４０２に関連して、ユーザー認証プロセスを例示する。文書署名サービス１４０２とやり取りをする際に、ユーザーは、とりわけ、彼らが、物理的な封印１４００などのような許可を示す品目の所有を明示することによって、文書に署名、印鑑、及び／又は封印の電子的な適用を許可されることの認証を望んでもよい。本明細書に開示されるセキュアなタグ認証技術の実施形態は、そのような封印１４００のユーザーの所有を認証するために使用されてもよい。

【０１５８】

署名、印鑑、及び／又は封印を適用するために彼らの許可を明示する物理的な封印１４００をユーザーが所有することの認証は、本明細書に開示される、セキュアなタグ許可及び／又は存在検証の技術を使用する、物理的な封印１４００、認証装置２００、及び／又は信頼される権限１０２を使用して実施されてもよい。単独のシステムとして例示されているが、他の実施形態において、認証装置２００、信頼される権限１０２、及び／又は文書署名サービス１４０２の、ある機能が、単一のシステム、及び／又はシステムの任意の好適な組み合わせによって実施されてもよいことは理解されるだろう。

【０１５９】

署名、印鑑、及び／又は封印を適用するために彼らの許可を文書署名サービス１４０２に明示する場合、ユーザーは、信頼される権限１０２によって物理的な封印１４００の彼らの所有を確認してもよい。物理的な封印１４００は、信頼される権限１０２及び／又は別の信頼されるサービスによって、セキュアなタグ１００に含まれる秘密情報１０４を供給されてもよい。ユーザーは、認証装置２００の文書署名サービス１４０２と関連するアプリケーション（例えば、封印認証アプリケーション）を最初に起動してもよい。封印認証アプリケーションは、本明細書に開示される実施形態に合わせて（例えば、ポーリングプロセス等に応じて）、最も近くに位置するセキュアなタグ１００を検出してもよい。認証装置２００は、それから文書署名サービス１４０２によって提供される署名サービスにログインしてもよい。

【０１６０】

文書署名サービス１４０２は、認証装置２００に暗号ノンスなどのチャレンジ情報を発行してもよく、チャレンジ情報とユーザー要求認証とを関連させてもよい。あるいは、認証装置２００、信頼されるサービス１０２、及び／又は別の信頼されるサービスは、チャレンジ情報を生成してもよい。認証装置２００は、応答して、チャレンジ情報に基づいて計算されたタグ識別子及びＭＡＣを返すだろうセキュアなタグ１００に、チャレンジ情報を伝送してもよい。認証装置２００は、それから、タグ識別子、ＭＡＣ、及びチャレンジ情報を信頼される権限１０２に送信してもよい。この情報を使用して、信頼される権限１０２は、受信されたタグ識別子及びチャレンジ情報を使用して、ＭＡＣを引き出してもよい。

【０１６１】

信頼される権限１０２に伝送されるＭＡＣと、信頼される権限１０２によって引き出されるＭＡＣが一致する場合、信頼される権限１０２は、認証装置２００に一致の証明を戻してもよい。ある実施形態において、この証明は、チャレンジ情報、タグ識別子、及びタイムスタンプを含む、署名付きデータを含んでもよい。認証装置２００は、文書署名サービス１４０２にこの証明を送ってもよい。文書署名サービス１４０２は、認証のための証明の署名を検証してもよい。文書署名サービス１４０２は、それから、認証されたユーザーによる使用のための署名、印鑑、及び／又は封印データを取り出すために、タグの識別を使用してもよい。ある実施形態において、適用される署名、印鑑、及び／又は封印は、返されたタイムスタンプによって示される、日付及び／又は時間と関連させてもよい。

【０１６２】

装置ベースのセキュアな電子タグ

【０１６３】

ある実施形態において、セキュアなタグは、装置ベースであり、及び／又はそうでない場合に、本明細書に開示される任意の装置を含む任意の好適な装置に統合されてもよい。装置ベースのセキュアなタグは、様々な状況において使用されてもよい。例えば、セキュリティ会社は、警備員の巡回がある指定されたチェックポイントを訪れることを確かめるために、装置ベースのセキュアなタグを使用してもよい。会社は、巡回チェックポイントに認証装置を置いてもよく、警備員は、各巡回チェックポイントでの存在の証明を提供するために、装置ベースのセキュアな電子タグを使用してもよい。セキュリティ会社は、巡回警備の記録として、この存在の証明を使用してもよい。

【０１６４】

同様に、会社は、職場に来ていて、そこから外出する従業員を管理することを望むだろう。会社は、チェックイン・ポイントに認証装置を置いてもよく、従業員は、職場の中及び外での彼らの署名によって存在の証明を提供するために、装置ベースのセキュアな電子タグを使用してもよい。会社は、各従業員が働く、多くの時間の記録として、この存在の証明を使用してもよい。装置ベースのセキュアな電子タグに関して述べているが、上述の例が、（例えば、カード・ベースのタグ、セキュアでないタグなど）本明細書に開示される任意の他のタイプのタグを更に使用してもよいことは理解されるだろう。

【０１６５】

図１６は、本開示の実施形態に合わせて、装置ベースのセキュアなタグの初期化プロセスを例示する。ある実施形態において、ＢＬＥ装置１６０２（例えば、スマートフォン等）及び／又は任意の他の好適な装置は、セキュアに組み込まれた秘密情報（例えば、ユニークな鍵）を供給されてもよい。ある実施形態において、情報は、セキュアなハードウェア、ソフトウェア、及び／又はそれらの組み合わせを介して、ＢＬＥ装置１６０２にセキュアに組み込まれてもよい。いくつかの実施形態において、事前設定は、ＢＬＥ装置１６０２にユニークな鍵を提供するだろう初期化装置１６００によって初期化されてもよい。ＢＬＥ装置１６０２と関連する、ユニークな鍵及び／又は識別情報は、開示された実施形態に合わせて、セキュアなタグ認証及び／又は存在検証プロセスを実施するように構成された、信頼される権限１０２に配布されてもよい。多くの変更が、例示された初期化プロセスに対して行うことができることは理解されるだろう。例えば、いくつかの実施形態に

おいて、ＢＬＥ装置１６０２は、個々の初期化装置１６００を用いることなく、信頼される権限１０２によって初期化されてもよい。

【０１６６】

図１７は、本開示の実施形態に合わせて装置ベースのセキュアなタグの認証プロセスを例示する。上記に述べられるように、ある実施形態において、装置ベースのセキュアなタグは、供給されたＢＬＥ装置１６０２を使用して実装されてもよい。ある種の実施形態において、例示される認証プロセスは、信頼される権限１０２を使用して、認証装置２００と関連する物理的な位置において、ＢＬＥ装置１６０２の存在を検証するために使用されてもよい。検証された場合、ＢＬＥ装置１６０２の存在の証明は、存在検証を利用するサービスを実装しているアプリケーション・サービス１７００に、伝送されてもよい。単独のシステムとして例示されているが、他の実施形態において、ＢＬＥ装置１６０２、認証装置２００、信頼される権限１０２、及び／又はアプリケーション・サービス１７００の、ある機能が、単一のシステム、及び／又はシステムの任意の好適な組み合わせによって実施されてもよいことは理解されるだろう。

【０１６７】

認証装置２００は、ＢＬＥ装置１６０２に近接して位置するために、ＢＬＥ装置・ディスカバリープロセスに従事してもよい。最も近くに位置するＢＬＥ装置１６０２を検出すると、認証装置２００は、チャレンジ情報（例えば、ノンス）を生成し、それをＢＬＥ装置１６０２に伝送してもよい。ある実施形態において、チャレンジ情報は、暗号ノンスなどのランダム及び／又は疑似ランダムに生成した値を含んでもよいが、他のタイプのチャレンジ情報が、開示されたシステム及び方法に関連して、更に使用されてもよい。更なる実施形態において、チャレンジ情報は、信頼される権限１０２によって、生成され、ＢＬＥ装置１６０２に伝送されてもよい。

【０１６８】

チャレンジ情報を受信した後に、ＢＬＥ装置１６０２は、ＢＬＥ装置１６０２によって記憶される、供給された秘密情報に、少なくとも部分的には基づいて、ＭＡＣ及び／又は他の計算結果を生成してもよい。更なる実施形態において、ＭＡＣは他のデータに基づいて更に生成されてもよい。ＢＬＥ装置１６０２と関連するＭＡＣ及び識別情報は、認証装置２００に伝送されてもよい。次に、認証装置２００は、ＢＬＥ装置１６０２に発行されたチャレンジ情報に加えて、そのような情報を信頼される権限１０２に伝送してもよい。

【０１６９】

信頼される権限１０２は、受信された情報（すなわち、装置ＩＤ、ノンス、ＭＡＣなど）に基づいて、本明細書に開示される実施形態に沿ったタグ認証プロセスを実施してもよい。例えば、信頼される権限は、受信した装置識別情報に基づいて、ＢＬＥ装置１６０２と関連する、自らが所有する秘密情報を取り出してもよい。取り出された秘密情報は、認証装置２００から受信される、秘密情報及びチャレンジ情報及び／又は他の情報に基づいて、ＭＡＣ及び／又は他の計算結果を計算することに関連して使用されてもよい。一旦計算されると、信頼される権限１０２は、その計算されたＭＡＣと、ＢＬＥ装置１６０２によって生成され、認証装置２００から受信されるＭＡＣとを比較してもよい。２つのＭＡＣ値が一致する場合、信頼される権限１０２は、認証装置２００の位置においてＢＬＥ装置の存在を認証する存在の証明を戻してもよい。２つのＭＡＣ値が一致しない場合、信頼される権限１０２は、存在の証明を戻さないだろう。ある実施形態では、存在の証明は、信頼される権限１０２及び／又は認証装置２００から、様々な存在検証に基づいたサービスに関連する情報を使用するアプリケーション・サービス１７００に伝送されてもよい。

【０１７０】

［ユーザー認証プロセス］

【０１７１】

ある実施形態において、ユーザー認証技術は、本明細書に開示されるセキュアなタグ認証技術に加えて、使用されてもよい。例えば、ユーザー名、及び／又はパスワード認証、生体認証、個人識別番号認証、及び／又は任意の他の好適なタイプの使用される認証技術

は、開示されたセキュアなタグ認証技術に加えて使用されてもよい。ある実施形態において、セキュアなタグ認証に加えてユーザー認証の実装は、セキュアなタグが、信頼される権限によって供給される真正なセキュアなタグであるだけでなく、セキュアなトランザクションに関連してセキュアなタグを提示する個人が、使用を許可され、及び／又はそうでない場合にセキュアなタグと関連させるという決定を促進するだろう。

【０１７２】

ある実施形態において、ユーザー認証はアクティブであってよく、ここで、セキュアなタグのユーザーは、ユニークなパスワード、識別番号、及び／又は生体情報などのある秘密情報の知識及び／又は所有を明示することによって、信頼される権限及び／又は他のサービスにより、彼らが本人であることを認証するだろう。いくつかの実施形態において、そのような情報は、トランザクションと関連する、セキュアなタグ認証プロセス、及び／又は１つ又は複数の他の装置及び／又はサービスに関連して、認証装置に提供されてもよい。更なる実施形態において、ユーザー認証は受動的でもよく、それによって、情報は、セキュアなタグを提示する個人がセキュアなタグと関連していることを確かめるために、装置のユーザーによって使用されるだろう、セキュアなタグ認証プロセスに関連して認証装置に提供されてもよい。例えば、認証されたセキュアなタグの許可されたユーザーと関連する、写真及び／又は他の個人情報（例えば、伸長、体重、毛髪の色など）は、認証装置に表示されてもよい。認証装置のユーザーは、トランザクションに関するセキュアなタグを提示する人が関連情報と一致することを確かめるために、そのような情報を使用してもよい。

【０１７３】

ある実施形態では、ユーザー認証は、認証装置を使用して実施されてもよい。更なる実施形態において、１つ又は複数の他のシステムは、限定はされないが、信頼される権限、及び／又は１つ又は複数の他の信頼されるサービスを含む、ユーザー認証に関連して使用されてもよい。

【０１７４】

［パーソナライズされた広告及び情報サービス］

【０１７５】

更なる実施形態において、開示されたセキュアなタグ認証技術は、消費者製品広告宣伝及びブランド管理を促進するために使用されてもよい。本明細書に開示される実施形態によって、ユーザーは、認証装置を使用して製品に含まれる、セキュアなタグを認証でき、製品に関する有益な情報を受信できるだろう。そのような実施形態は、信頼される供給源から豊かな製品情報と共に製品の真正性の保証を消費者に提供してもよい。

【０１７６】

’４０６アプリケーション、’５３８アプリケーション、及び’７５０アプリケーションにおいて説明される技術を含む、ある特定の技術は、健全な消費者が、プライバシーが保護された（例えば、彼らの個人プロファイルを対象にした）彼らの情報を受信し、彼らが、彼らの製品を購買し及び／又は購買することを考えている消費者の特性について、詳細な且つタイムリな分析報告を取り出すことが可能だろうという保証を製品広告宣伝担当者及びブランド・マネージャに提供するために、開示された実施形態に関連して使用されてもよい。ブランド・マネージャは、開示されたシステム及び方法によって提供されるだろう、真正性、偽の及び／又は盗まれた品目の検出、（例えば、位置通報による）未許可のチャネルを通しての売上げの識別、及び／又は販売後のサポート及び／又はマーケティングのための製品登録の確実性を更に評価するだろう。

【０１７７】

ブランディング及びメッセージングが他者によって乗っ取られず、ある特定の消費者に適切なメッセージングが提供され、且つ小売業者（例えば、店員、販売員など）に適切なメッセージングが消費者にではなく、そのような当事者に提供されることを保証する、信頼される権限と共に、消費者のモバイル装置から読める安価なセキュアなタグの使用を通して、開示されたシステム及び方法の実施形態は上述の機能を提供してもよい。本明細書

に開示される実施形態に沿った信頼されるサービスは、位置の特定によって、偽造者を失敗させ、及び／又は未許可の販売チャネルを識別することを助けてもよい。

【０１７８】

ある実施形態は、消費者のプライバシーを侵害することなく、製品マネージャに、豊富なバックチャネル情報が提供されることを可能にするだろう。例えば、開示されたシステム及び方法は、流通チェーンを通して製品の追尾及び／又は追跡を可能にしてもよい。これは、とりわけ、製品の真正性、及び偽の製品の検出、及びそれらの位置の特定（それによって偽造を防止する）に関して消費者に保証を提供し、盗まれた製品の検出及び／又は位置の特定を促進し、地理、人口統計、及び／又は消費者の興味によって、消費者販売の簡便な、プライバシーが保護された追尾を可能にし、売り場においてプライバシーが保護された接客を提供し、及び／又は、プライバシーが保護された販売後のサポート及びターゲティングを促進するだろう。

【０１７９】

情報は、セキュアなタグが認証される際に、消費者及び／又は小売業者に提供されてもよい。例えば、消費者認証装置を使用する個人がセキュアなタグを認証する際に、消費者向け情報が提供されてもよい。そのような情報は、彼らのプライバシーを侵害することなく、消費者の個人的特徴に対応させられ、及び／又はそれによって優先順位をつけられてもよい。いくつかの実施形態において、情報は、限定はされないが、ビデオ、オーディオ、テキストなどを含む、様々なフォーマットであってもよい。

【０１８０】

小売業者向け情報は、小売業者認証装置を使用している小売業者がセキュアなタグを認証する際に、提供されてもよい。小売業者の情報は、消費者に対しては混乱させ、又は圧倒的だろうが、製品の販売において小売業者を助けることができる情報などの、製品に関する小売業者に特有の情報を含んでもよい。同様に、より多くの特有の情報は、特別の要望及び／又は要求によりセキュアなタグを認証させるユーザーに提供されてもよい。例えば、特別な要求を有する消費者、中古品目を合法的に再販する個人、棚卸しを実施する従業員等は、彼らがセキュアなタグを認証する際に、彼らの要求に関する特有の情報を提供されてもよい。

【０１８１】

ある実施形態において、適切な情報が、特有の状況下において健全な人々に提供されることを保証する、信頼基盤は使用されてもよい。ある実施形態において、基盤は、様々な装置及び／又はアプリケーションをサポートする、スケーラブル及び効率的であってよい。とりわけ、これは、消費者が、認証装置で実行する、適切に許可されたアプリケーションを用いて、任意の小売店舗に入り、製品を認証するために彼らの装置を使用し、セキュアなタグを含み、信頼される供給源からの真正性及び製品情報を確実に受信するだろうことを保証してもよい。更に、製品生産者には、消費者が、彼らの製品についての適正なメッセージ及び／又は情報を受信するはずであり、彼らの製品と消費者のやり取りについて収集される情報が、許可されたエンティティによって伝送され、アクセスされることを保証してもよい。

【０１８２】

いくつかの実施形態において、異なる小売業者及び／又は製品にとって多くのアプリケーションの中から選択しなければならないよりはむしろ、相互運用性が提供されてもよく、それによって、様々なブランド及び／又は製品間で経費の流通を可能にして、消費者がちょうど１つ又は２、３の許可されたアプリケーションに依存できることを保証する。他の実施形態において、本明細書に説明されるシステム及び方法は、単一のブランド、製品、ビジネス、又はサービスをサポートするために、又はその閉部分集合をサポートするために、展開されることができる。いくつかの実施形態において、ブランドを所有し及び／又は管理する人々が、ブランド製品に関して情報を提供するために許可された唯一の人であることを保証する、登録権限は提供されてもよい。

【０１８３】

ブランド製品を有する会社がどのように開示されたシステム及び方法の実施形態を実装するのかという例として、会社は、最初に、互換性を持つセキュアなタグ供給者を（例えば、信頼される権限等を介して）識別してもよい。会社は、信頼される権限によって登録してもよく、該当する連絡先の情報、ブランド情報等を提供する。会社は、供給者からセキュアなタグを取得し（例えば、それらを彼らの製品及び／又は彼らの製品パッケージに統合することによって）、それらを彼らの製品に関連させてもよい。会社は、各製品のためにタグ情報（例えば、製品に通し番号を振る場合、通し番号を振られたタグ識別情報）を信頼される権限にアップロードしてもよい。加えて、会社は、製品情報、及び／又は媒体、又はリンクを、彼らの製品と関連するタグをセキュアに認証する、消費者、小売業者、及び／又は他の当事者に提供される同一のものにアップロードしてもよい。ある実施形態において、会社は、そのような情報が、消費者属性、小売環境、位置などに基づいて、どのように表示されるかを指定してもよい。

【０１８４】

実装の後、会社は、（例えば、ダッシュボード等を介して、）彼らの情報を管理するために信頼される権限にログインしてもよい。会社は、その製品に関する様々な情報を見てもよい。例えば、会社は、会社の製品と消費者のやり取り（例えば、消費者プロフィール、購入／パス比率、位置情報など）に基づく報告（例えば、リアルタイム報告）を見てもよく、消費者登録、コメント等を集めてもよい。会社は、起こり得る偽造、無免許の製品流通、無許可販売の位置等についての情報を取得するために、信頼される権限によって提供される不正行為管理サービスにアクセスしてもよい。

【０１８５】

消費者は、様々な方法で本明細書に開示される実施形態に合わせて、セキュアなタグを供給される製品とやり取りをしてもよい。例えば、消費者は、彼らが認証するセキュアなタグを含む、任意の製品に関して情報を収集し、見るために、ショッピング・アプリケーションを彼らのモバイル装置にダウンロードできるだろう。セキュアなタグを認証することによって、消費者は、製品に関する製品真正性及び／又はパーソナライズされた情報の保証を受信してもよい。いくつかの実施形態において、消費者は、彼らのモバイル装置に製品に関する情報及び／又はメモを記憶できるだろう。

【０１８６】

消費者がセキュアなタグを供給される製品を購入することを決定する場合、消費者は、信頼される権限によって彼らの購入を登録でき、及び／又は、開示されたシステム及び方法を使用して、製品（例えば、保証情報、アクセサリー情報、ユーザーガイドなど）に関する付加情報を受信できる。消費者は、製品生産者によって提供される製品ウェブサイトとやり取りをすることを選択してもよい。ある実施形態において、ショッピング・アプリケーションは、消費者の購入品に関する情報を維持してもよく、後程、消費者が援助を必要とし、又は、付加的な商品及び／又はサービスを購入したい場合、消費者を適切な供給源に接続するだろう。ある実施形態では、消費者のそのような資産在庫表は、とりわけ、保険目的、盗品の回収のために有効であり、及び／又は、パーソナライズされた製品マッチング及び／又は推薦サービスをより適切に提供する、好ましい口出し及び／又は属性を引き出す。

【０１８７】

［システム及び装置構成］

【０１８８】

図１８は、本開示のシステム及び方法のある実施形態を実装するために使用されるだろうシステム１８００を例示する。システム１８００は、セルラ電話、ＰＤＡ、スマートフォン、携帯用オーディオ又はビデオプレーヤ、タブレット・コンピュータシステム、サーバコンピュータシステム、及び／又は、本明細書に説明されるシステム及び方法を実装するように構成された任意の他のシステムを含んでもよい。ある実施形態において、本明細書に開示されるように、システム１８００は、認証装置、信頼される権限、及び／又は別の関連サービスと関連する、ある特定の機能を実施してもよい。

【０１８９】
図１８に例示されるように、システム１８００は、以下を含んでもよい：プロセッサ１８０２；プロセッサ１８０２による、使用及び実行のための記憶プログラム及び他のデータのための、高速ＲＡＭ、不揮発性メモリ、及び／又は１つ又は複数の大容量不揮発性コンピュータ可読記憶媒体（例えば、ハードディスク、フラッシュメモリなど）を含んでもよいシステム・メモリ１８０４；ディスプレー、及び／又は、例えば、タッチスクリーン、キーボード、マウス、トラックパッド、等などの１つ又は複数の入力装置を含んでもよいインタフェース１８１６（例えば、入出力インタフェース）；もう１つのディスケット、光学記憶媒体、及び／又は他のコンピュータ可読記憶媒体（例えば、フラッシュメモリ、サムドライブ、ＵＳＢドングル、コンパクトディスク、ＤＶＤなど）を含んでもよい着脱可能なメモリ１８０８とインタフェースするためのポート１８０６；１つ又は複数の通信技術を使用して、ネットワーク１８１２を介して他のシステムと通信するネットワーク・インタフェース１８１０；１つ又は複数の位置センサ、セキュアな電子タグ・センサ、及び／又は本明細書に開示される任意のセンサシステムを含む任意の他のセンサシステムを含んでもよい１つ又は複数のセンサ１８１８；及び、上述の素子と通信可能に連結するための１つ又は複数のバス１８３２。

【０１９０】
ある実施形態において、ネットワーク１８３２は、インターネット、ＬＡＮ、仮想私設網、及び／又は１つ又は複数の電子回路通信技術及び／又は標準（例えば、イーサネット（登録商標）等）を利用している任意の他の通信網を含んでもよい。いくつかの実施形態において、ネットワーク・インタフェース１８１０及び／又はネットワーク１８３２は、ＰＣＳなどの無線搬送方式、及び／又は任意の好適な通信標準及び／又はプロトコルを組み込んでいる任意の他の好適な通信システムの部分であってもよい。更なる実施形態において、ネットワーク・インタフェース１８１０及び／又はネットワーク１８３２は、アナログ移動通信ネットワーク、及び／又は、例えば、ＣＤＭＡ、ＧＳＭ、ＦＤＭＡ及び／又はＴＤＭＡ標準を利用している、デジタル移動通信ネットワークの部分であってもよい。尚、更なる実施形態において、ネットワーク・インタフェース１８１０及び／又はネットワーク１８３２は、１つ又は複数の衛星通信リンクを組み込んでもよく、及び／又はＩＥＥＥの８０２．１１の標準、近接場通信、Ｂｌｕｅｔｏｏｔｈ（登録商標）、ＵＷＢ、Ｚｉｇｂｅｅ（登録商標）、及び／又は任意の他の好適な標準又は標準を使用してもよい。

【０１９１】
いくつかの実施形態において、システム１８００は、あるいは又は加えて、システム１８００のユーザーによる不正操作、又はセキュアな物理的及び／又は仮想セキュリティ技術を利用することよる他のエンティティから保護されているＳＰＵ１８１４を含んでもよい。ＳＰＵ１８１４は、秘密又は他のセキュアな情報の個人的管理などの慎重を要する運用のセキュリティ、及び本明細書に開示されるシステム及び方法の他の態様を向上及び／又は促進することを助けることができる。ある実施形態において、ＳＰＵ１８１４は、論理的にセキュアなプロセス領域において動作し、秘密情報に基づいて保護及び動作するように構成されてもよい。いくつかの実施形態において、ＳＰＵ１８１４は、ＳＰＵ１８１４がセキュアな動作を実施することを可能にするように構成される、実行命令又はプログラムを記憶している内部記憶装置を含んでもよい。

【０１９２】
システム１８００の動作は、通常、システム・メモリ１８０４（及び／又は着脱可能なメモリ１８０８などの他のコンピュータ可読媒体）に記憶されたソフトウェア命令及びプログラムを実行することによって動作する、プロセッサ１８０２によって制御されてもよい。システム・メモリ１８０４は、システム１８００の動作を制御するための様々な実行可能なプログラム又はモジュールを記憶してもよい。例えば、システム・メモリ１８０４はオペレーティング・システム（「ＯＳ」）１８２０を含み、それは、システム・ハードウェア・リソースを少なくとも部分的には管理及び調整してもよく、且つ、様々なアプリケーション、及び秘密情報の保護及び／又は管理を含む信頼及びプライバシー管理機能を

実装するための信頼及びプライバシー管理システム１８２２、の実行のための共通サービスを提供してもよい。システム・メモリ１８０４は、本明細書に開示されるシステム及び方法の実施形態を実装するように構成された、システム１８００との通信をそれによって部分的に可能にするように構成された通信ソフトウェア１８２４、アプリケーション１８２６（例えば、タグ及び／又は製品確認アプリケーション）、タグ認証モジュール１８２８、チャレンジ発生器１８３０、及び／又は、任意の他の情報及び／又はアプリケーションを、限定はされないが、更に含んでもよい。

【０１９３】

本明細書に説明されるシステム及び方法が、図１８に例示されるものに類似又は同一の計算装置によって、又は、図１８に示される、いくつかの構成要素を所有しないコンピュータ装置を含む、仮想的に任意の他の好適な計算装置、及び／又は、図示されない他の構成要素を所有する計算装置によって、実施できることを、当業者は理解するだろう。従って、図１８が、説明のために且つ限定のためでなく、提供されることは理解されるべきである。

【０１９４】

本明細書に開示されるシステム及び方法は、任意の特定のコンピュータ、電子制御ユニット、又は他の機器に本質的に関係がなく、ハードウェア、ソフトウェア、及び／又はファームウェアの好適な組み合わせによって実装されてもよい。ソフトウェア実装は、プロセッサによって実行される場合に、プロセッサに実行命令によって少なくとも部分的に定められる方法を実施させるだろう、実行可能なコード／命令を含む１つ又は複数のコンピュータプログラムを含んでもよい。コンピュータプログラムは、コンパイル又はインタープリットされた言語を含む、プログラム言語の任意の形式で書かれることができ、スタンドアロンのプログラムとして、又はコンピューティング環境での使用に好適な、モジュール、構成要素、サブルーチン、又は他のユニットとして含んでいる、任意の形式で展開することができる。更に、コンピュータプログラムは、１台のコンピュータにおいて又は１つのサイトでの複数のコンピュータにおいて実行されるように展開でき、複数のサイト全体にわたって配布され、且つ通信ネットワークによって相互接続される。ソフトウェアの実施形態は、コンピュータプログラム及び命令を記憶するように構成された非一時的な記憶媒体を含み、プロセッサによって実行される場合に、プロセッサに命令に従って方法を実施させるように構成される、コンピュータプログラム製品として実装されてもよい。ある実施形態において、非一時的な記憶媒体は、プロセッサ可読命令を非一時的な記憶媒体に記憶することが可能な任意の形式であってもよい。非一時的な記憶媒体は、コンパクトディスク、ディジタルビデオ・ディスク、磁気テープ、磁気ディスク、フラッシュメモリ、集積回路、又は任意の他の非一時的なデジタル処理機器のメモリ装置によって具体化されてもよい。

【０１９５】

前述のことは、明確さのためにいくつかの詳細において説明されたが、ある変更及び修正が、その原理を逸脱しない範囲でなされてもよいことは明らかだろう。本明細書に説明される両方のシステム及び方法を実装する多くの代替方法があることに注意されたい。従って、本実施形態は、例示的であって限定的はでないと考えられるべきであり、本発明は、本明細書に与えられた詳細に限定されるべきでないが、添付の特許請求の範囲及びその均等の範囲内で修正されてもよい。

【図１】

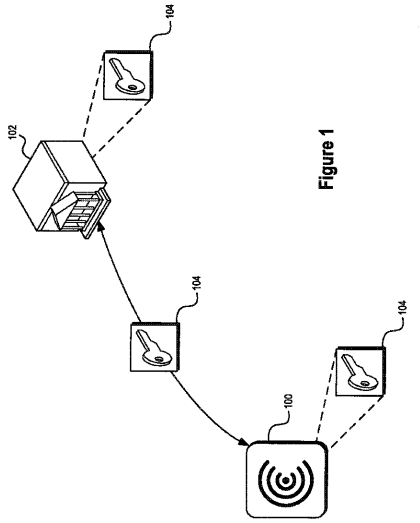

Figure 1

【図７Ａ】

Figure 7A

【図２】

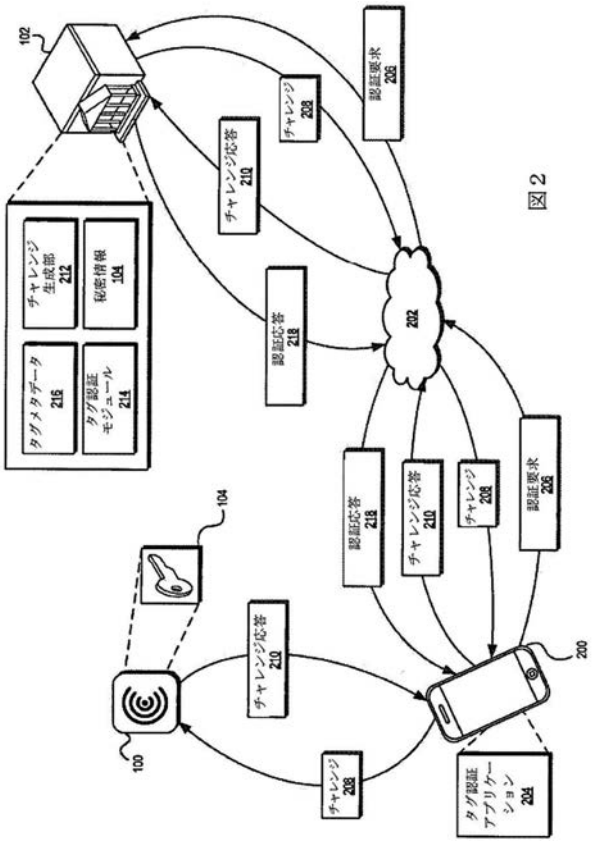

図２

【図３】

図３

【図４】

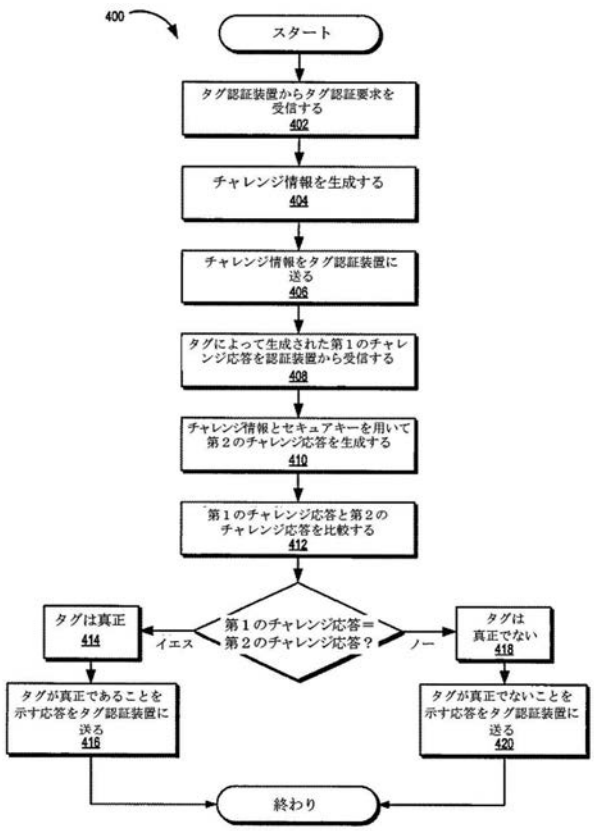

図４

【図５】

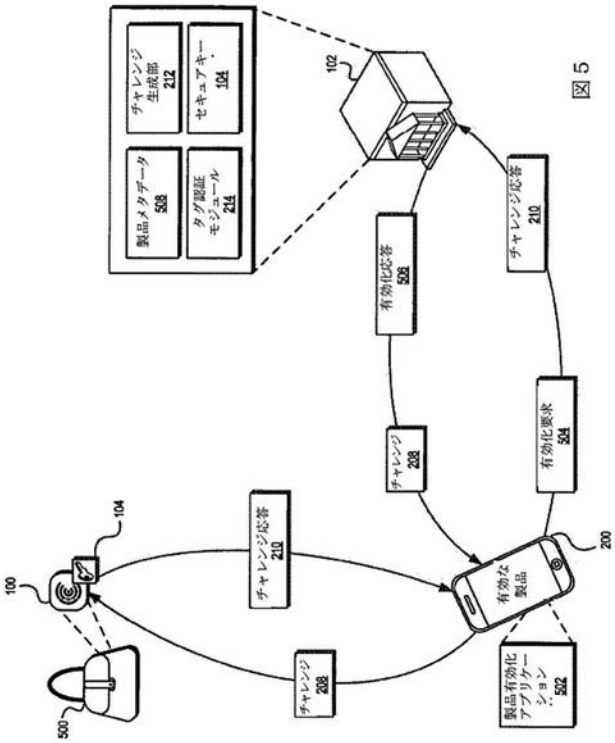

図５

【図６】

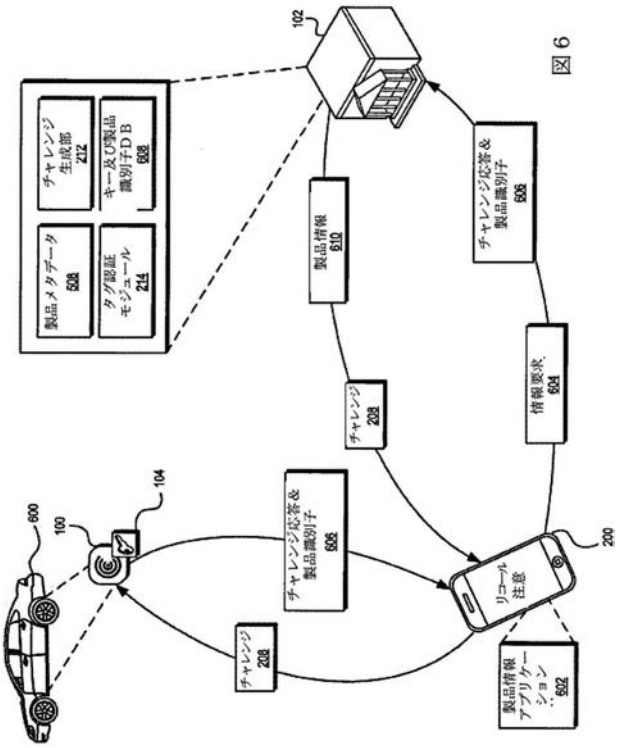

図６

【図７Ｂ】

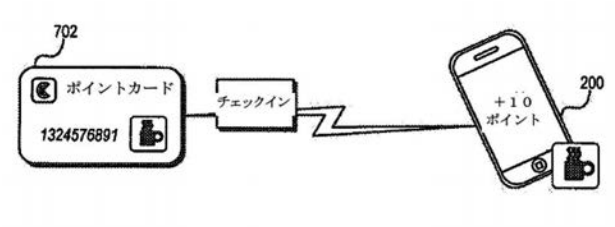

図７Ｂ

【図７Ｃ】

図７Ｃ

【図８】

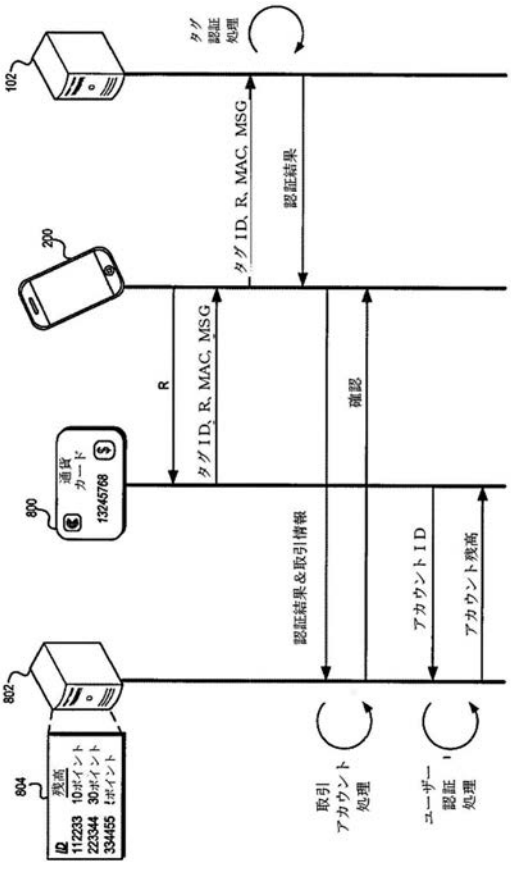

図８

【図９】

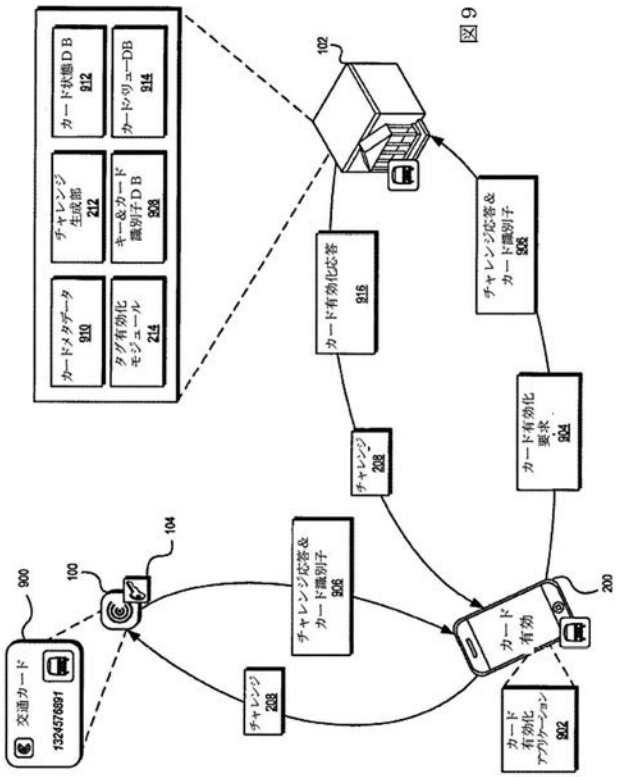

図９

【図１０】

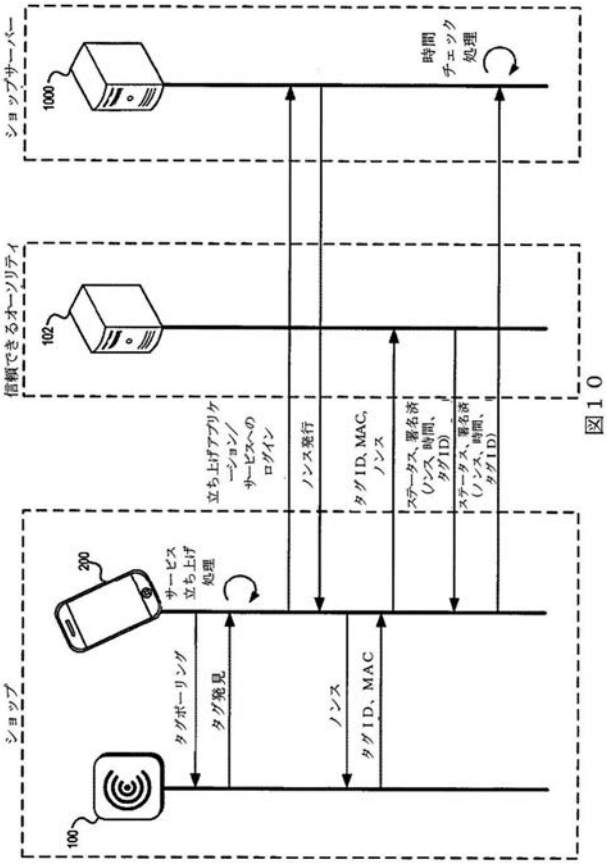

図１０

【図１１】

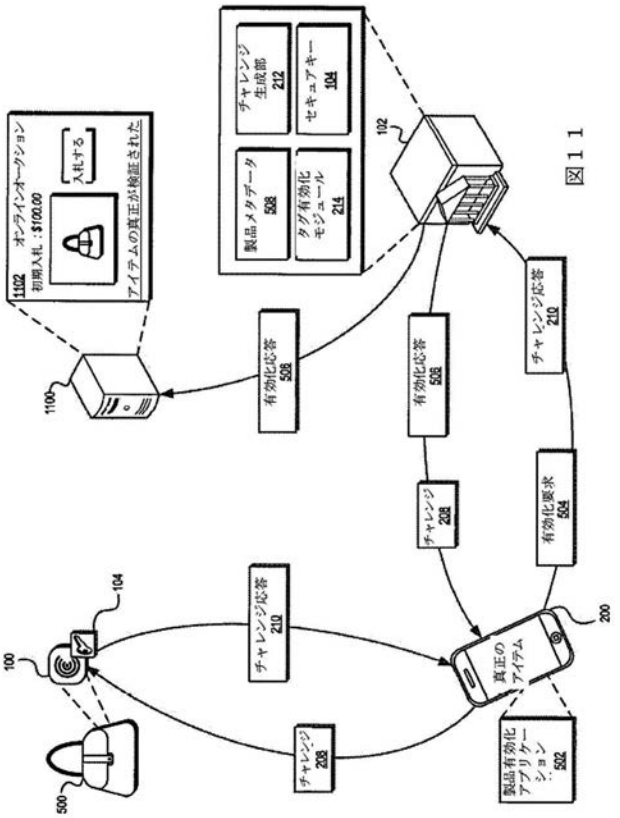

図１１

【図１２】

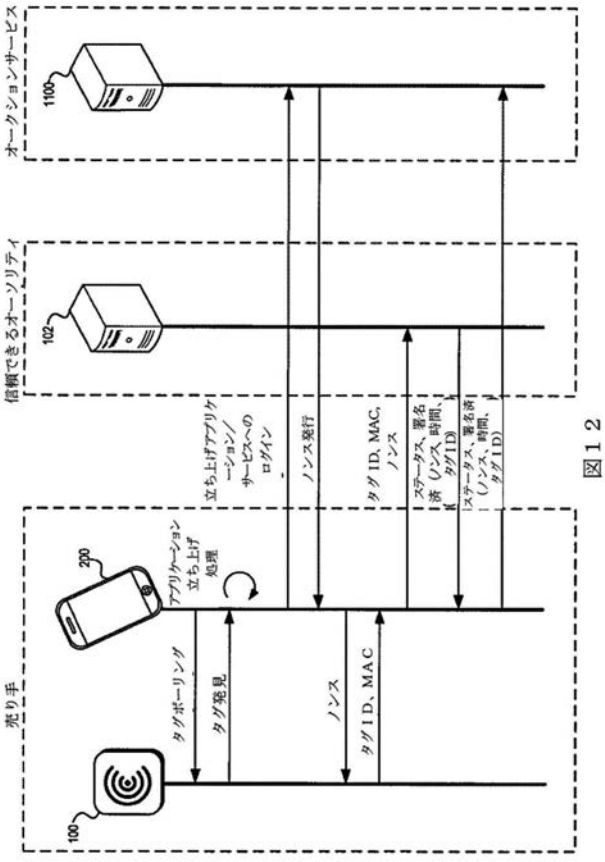

図１２

【図１３】

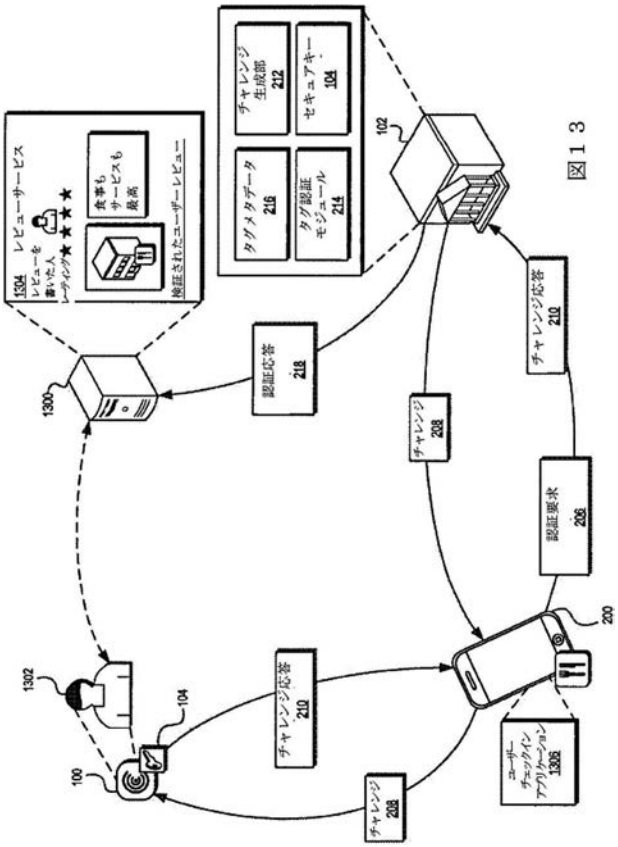

図１３

【図１４】

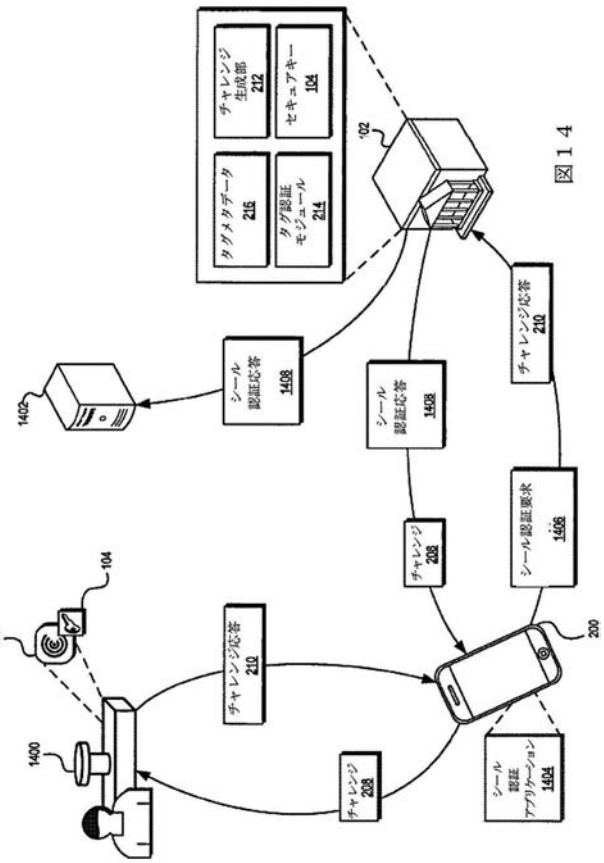

図１４

【図１５】

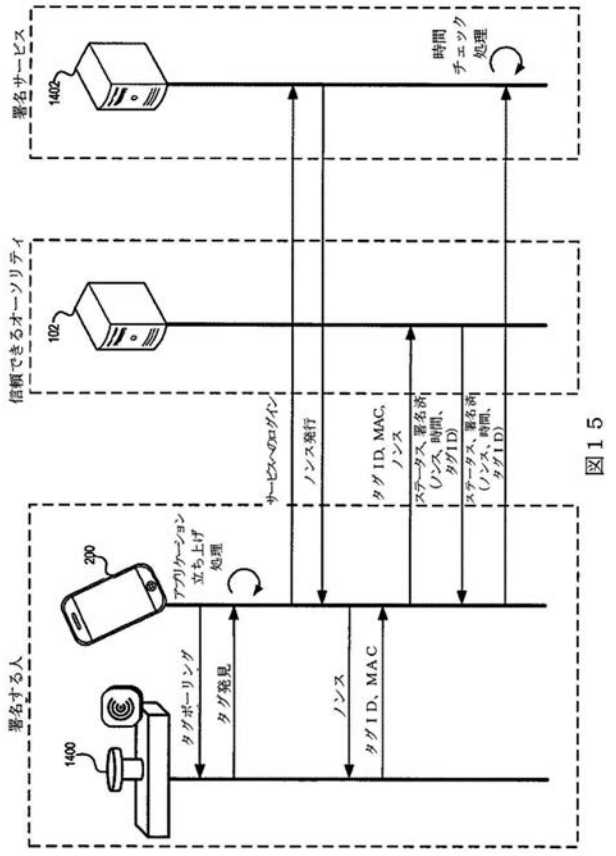

図１５

【図１６】

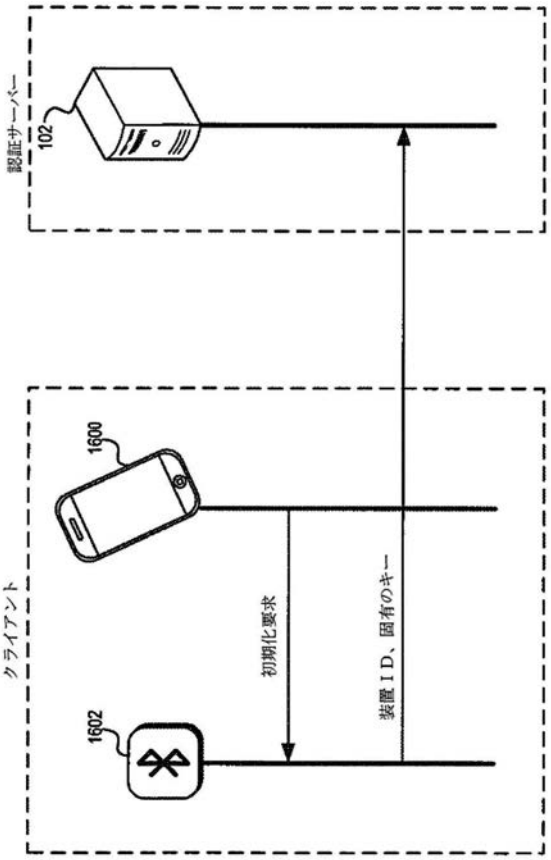

図１６

【図１７】

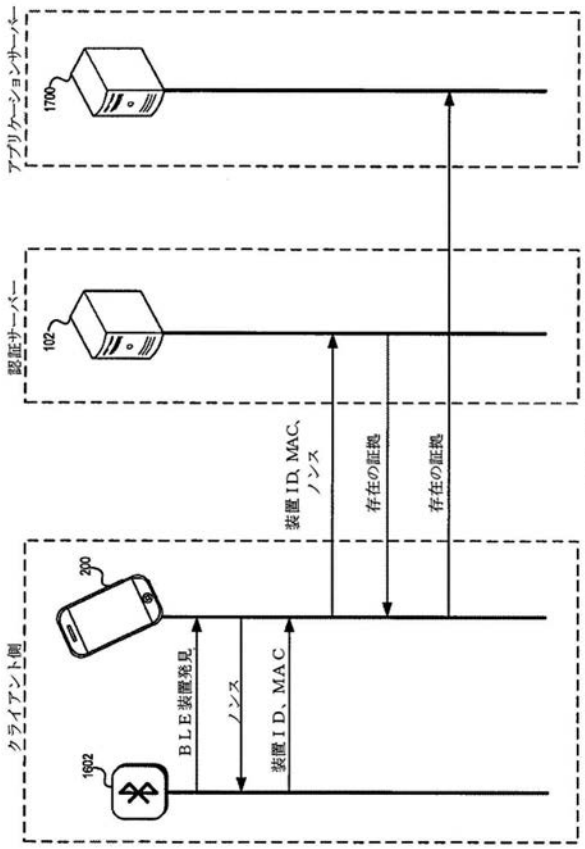

図１７

【図１８】

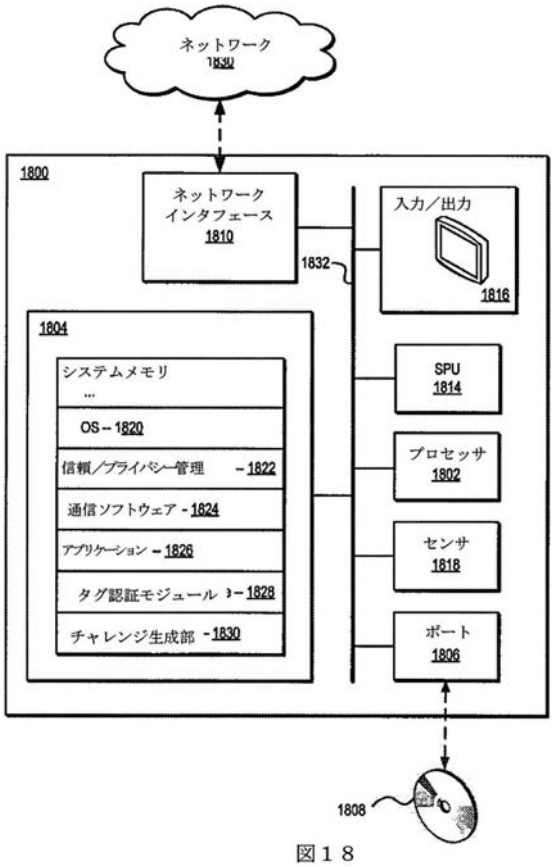

図１８

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2014/025085

A. CLASSIFICATION OF SUBJECT MATTER

G06Q 20/40(2012.01)i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06Q 20/40; G06F 19/00; A63F 9/24; G06F 12/14; G06Q 10/00; H04Q 5/22; G06F 21/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean utility models and applications for utility models
Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
eKOMPASS(KIPO internal) & Keywords: secure tag, authentication device, challenge response, match

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2008-0214312 A1 (CHRISTIAN RICHARD) 04 September 2008 See abstract, paragraphs [0034], [0039], [0041] and claims 1, 3, 4, 8.	1-13
Y	WO 2007-128966 A1 (ITI SCOTLAND LIMITED et al.) 15 November 2007 See abstract, page 7, lines 4-12, page 29, line 32-page 30, line 1 and claims 1, 6.	1-13
A	US 2008-0109899 A1 (SANDER MATTHIJS RIJNSWOU VAN et al.) 08 May 2008 See abstract, paragraph [0044] and claim 1.	1-13
A	US 2010-0161994 A1 (JAVIER SERRET AVILA et al.) 24 June 2010 See abstract, paragraphs [0081], [0085] and claims 3, 5.	1-13
A	US 2004-0066278 A1 (MICHAEL A. HUGHES et al.) 08 April 2004 See abstract and claims 1, 4, 7.	1-13

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

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents,such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
10 July 2014 (10.07.2014)	**10 July 2014 (10.07.2014)**

Name and mailing address of the ISA/KR
International Application Division
Korean Intellectual Property Office
189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan City, 302-701,
Republic of Korea
Facsimile No. +82-42-472-7140

Authorized officer
PARK, Hye Lyun
Telephone No. +82-42-481-3463

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/US2014/025085

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2008-0214312 A1	04/09/2008	AU 2005-291797 A1	13/04/2006
		CA 2578983 A1	13/04/2006
		CN 101031940 A0	05/09/2007
		EP 1805735 A1	11/07/2007
		EP 1805735 A4	11/11/2009
		WO 2006-037220 A1	13/04/2006
WO 2007-128966 A1	15/11/2007	EP 2011061 A1	07/01/2009
		JP 2009-532792 A	10/09/2009
		US 2010-0019026 A1	28/01/2010
US 2008-0109899 A1	08/05/2008	AT 510270 T	15/06/2011
		CN 100555316 C	28/10/2009
		CN 101006456 A	25/07/2007
		EP 1759338 A2	07/03/2007
		EP 1759338 B1	18/05/2011
		JP 2008-502068 A	24/01/2008
		US 8621602 B2	31/12/2013
		WO 2005-122071 A2	22/12/2005
		WO 2005-122071 A3	16/03/2006
US 2010-0161994 A1	24/06/2010	CN 101405805 A	08/04/2009
		EP 1999751 A2	10/12/2008
		JP 2009-530945 A	27/08/2009
		RU 2008141690 A	27/04/2010
		WO 2007-107928 A2	27/09/2007
		WO 2007-107928 A3	21/12/2007
US 2004-0066278 A1	08/04/2004	AU 2003-270786 A1	04/05/2004
		CA 2500779 A1	22/04/2004
		EP 1547008 A1	29/06/2005
		MX PA05003546 A	30/09/2005
		US 6842106 B2	11/01/2005
		WO 2004-034321 A1	22/04/2004
		WO 2004-034321 B1	10/06/2004

フロントページの続き

(31)優先権主張番号 61/914,212
(32)優先日 平成25年12月10日(2013.12.10)
(33)優先権主張国 米国(US)
(31)優先権主張番号 61/918,506
(32)優先日 平成25年12月19日(2013.12.19)
(33)優先権主張国 米国(US)
(31)優先権主張番号 61/932,927
(32)優先日 平成26年1月29日(2014.1.29)
(33)優先権主張国 米国(US)

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

(72)発明者 デイビッド ピー. マハー
アメリカ合衆国, カリフォルニア ９４５５０, リバーモア, ウェットモア ロード １５６６
(72)発明者 ピエール シャバンヌ
アメリカ合衆国, カリフォルニア ９５６１６, デイビス, ダッチャンプ ストリート ２１６６
(72)発明者 長尾 豊
アメリカ合衆国, カリフォルニア ９５０１４, クパチーノ, スティーブンス クリーク ブールバード ２０４８８, ＃２３０９
(72)発明者 マイケル マネンテ
アメリカ合衆国, マサチューセッツ ０１７７６, サドベリー, ウェブスター サークル ２３

Ｆターム(参考) 5J104 AA07 AA08 AA16 AA32 EA04 EA08 EA18 EA19 JA03 JA21
KA02 LA06 NA02 NA12 NA33 NA37 NA38 PA10