(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第6430396号
(P6430396)

(45)発行日　平成30年11月28日(2018.11.28)　(24)登録日　平成30年11月9日(2018.11.9)

(51)Int.Cl.　　F I
H04L 9/32 (2006.01)　　H04L 9/00 675A
H04L 9/08 (2006.01)　　H04L 9/00 601C
　　H04L 9/00 673D

請求項の数 17　(全 17 頁)

(21)出願番号　特願2015-548407(P2015-548407)
(86)(22)出願日　平成25年12月16日(2013.12.16)
(65)公表番号　特表2016-503988(P2016-503988A)
(43)公表日　平成28年2月8日(2016.2.8)
(86)国際出願番号　PCT/EP2013/076725
(87)国際公開番号　WO2014/095737
(87)国際公開日　平成26年6月26日(2014.6.26)
審査請求日　平成28年11月30日(2016.11.30)
(31)優先権主張番号　12197525.4
(32)優先日　平成24年12月17日(2012.12.17)
(33)優先権主張国　欧州特許庁(EP)

(73)特許権者　516385952
イネクスト　ソシエテ　アノニム
スイス　１００６　ローザンヌ　アヴェニュー　エドワール－ダプル　７
(74)代理人　100094569
弁理士　田中　伸一郎
(74)代理人　100088694
弁理士　弟子丸　健
(74)代理人　100103610
弁理士　▲吉▼田　和彦
(74)代理人　100067013
弁理士　大塚　文昭
(74)代理人　100086771
弁理士　西島　孝喜

最終頁に続く

(54)【発明の名称】物理的特性を使用して製造品目をマーク付けする方法および装置

(57)【特許請求の範囲】
【請求項１】
マーク付け装置を用いて、製造品目をマーク付けする方法であって、
製造品目のための独特の製品識別子を生成する段階と、
一つ以上の暗号化鍵を生成する段階と、
前記独特の製品識別子および前記一つ以上の暗号化鍵を使用して秘密鍵を生成する段階と、
前記秘密鍵および前記独特の製品識別子を使用してシステムノイズ値を生成する段階と、
前記製造品目の測定された物理的特性から物理的鍵を生成する段階と、
前記物理的鍵および前記独特の製品識別子を使用して物理的ノイズ値を生成する段階であって、前記システムノイズ値及び前記物理的ノイズ値を生成するために、前記秘密鍵と前記独特の製品識別子との組み合わせ及び前記物理的鍵と前記独特の製品識別子との組み合わせで、前記方法は、転置式、換字式、テーブル換字式および索引付けを使用し、または、暗号ハッシュ関数を使用する、段階と、
前記秘密鍵および前記物理的鍵から導き出されたセキュア識別子を生成するか、または前記秘密鍵および前記物理的鍵を組み込む段階であって、前記セキュア識別子は、前記システムノイズ値から導き出され、または、前記システムノイズ値を組み込み、前記セキュア識別子は、前記物理的ノイズ値から導き出され、または、前記物理的ノイズ値を組み込む、段階と、

前記製造品目にマークを付ける段階であって、前記マークが前記セキュア識別子または前記セキュア識別子から導き出された識別子を含む段階とを含む、方法。

【請求項２】

前記セキュア識別子が前記独特の製品識別子から導き出され、または、前記独特の製品識別子を組み込む、請求項1に記載の方法。

【請求項３】

前記セキュア識別子を生成する前記段階が、前記独特の製品識別子を前記システムノイズ値とともに暗号化することにより第一の識別子を生成する段階、および前記第一の識別子を前記物理的ノイズ値とともに暗号化することにより前記セキュア識別子を生成する段階を含む、請求項2に記載の方法。

【請求項４】

前記独特の製品識別子を前記システムノイズ値とともに暗号化することにより前記第一の識別子を生成する前記段階は、コード生成難読化鍵による暗号化によって実行され、

前記第一の識別子は、前記物理的ノイズ値及びコード生成装置識別子と組み合わされ、

前記第一の識別子、前記物理的ノイズ値及び前記コード生成装置識別子の組み合わせは、グローバル鍵を用いて暗号化され、前記セキュア識別子が生成される、請求項3に記載の方法。

【請求項５】

前記コード生成難読化鍵は、コード生成装置に特定のものであり、前記コード生成装置に予めロードされており、前記グローバル鍵は、一又は二以上の製造センタの全てで共通である、請求項４に記載の方法。

【請求項６】

確認センターで前記製造品目を認証する段階をさらに含む、請求項3に記載の方法であって、その認証の段階が、

前記品目上の前記マークを識別する段階と、

前記マークを復号化して前記第一の識別子および前記物理的ノイズ値を導き出す段階と、

前記第一の識別子を復号化して前記独特の製品識別子および前記システムノイズ値を導き出す段階と、

前記製造品目の測定された物理的特性から新しい物理的鍵を生成する段階と、

前記新しい物理的鍵および前記導き出された独特の製品識別子に対してハッシュ関数を実行することにより、前記物理的ノイズ値の新しいコピーを生成する段階と、

前記物理的ノイズ値の前記新しいコピーを前記導き出された物理的ノイズ値と比較する段階と、

前記導き出された物理的ノイズ値が、前記物理的ノイズ値の前記新しいコピーと同一であるか、またはそれらに関連性があるかどうかの表示を提供する段階とを含む、方法。

【請求項７】

請求項6に記載の方法であって、さらに、

前記独特の製品識別子および前記一つ以上の暗号化鍵から前記秘密鍵の新しいコピーを生成する段階と、

前記秘密鍵および前記独特の製品識別子の前記新しいコピーに対してハッシュ関数を実行することにより、前記システムノイズ値の新しいコピーを生成する段階と、

前記システムノイズ値の前記新しいコピーを前記導き出されたシステムノイズ値と比較する段階と、

前記システムノイズ値の前記新しいコピーおよび前記導き出されたシステムノイズ値が同一であるかどうかの表示を提供する段階とを含む、方法。

【請求項８】

前記セキュア識別子を生成する前記段階が、前記独特の製品識別子を前記システムノイズ値とともに暗号化することにより第一の識別子を生成する段階と、

前記独特の製品識別子を前記物理的ノイズ値とともに暗号化することによりセキュア

な第二の識別子を生成する段階と、
前記製造品目にマークを付ける段階であって、前記マークが、前記第一および第二のセキュア識別子、または前記第一および第二のセキュア識別子から導き出された識別子（単一または複数）を含む段階とを含む、請求項2に記載の方法。
【請求項９】
前記システムノイズ値は、前記独特の製品識別子で組み合わされ、
前記システムノイズ値及び前記独特の製品識別子の組み合わせは、コード生成難読化鍵で暗号化され、第一の識別子が生成され、
前記第一の識別子は、コード生成装置識別子と組み合わされ、グローバル鍵で暗号化され、第一のセキュア識別子が生成され、
前記物理的ノイズ値は、前記独特の製品識別子と組み合わされ、第二の識別子が生成され、
前記第二の識別子は、グローバル鍵で暗号化され、第二のセキュア識別子が生成される、請求項8に記載の方法。
【請求項１０】
確認センターで前記製造品目を認証する段階をさらに含む、請求項8に記載の方法であって、その認証の段階が、
前記品目上の前記マークを識別する段階と、
前記マークを復号化して、前記独特の製品識別子、前記システムノイズおよび前記物理的ノイズを導き出す段階と、
前記独特の製品識別子および前記一つ以上の暗号化鍵から前記秘密鍵の新しいコピーを生成する段階と、
前記秘密鍵および前記独特の製品識別子の前記新しいコピーに対してハッシュ関数を実行することにより、前記システムノイズ値の新しいコピーを生成する段階と、
前記システムノイズ値の前記新しいコピーを前記導き出されたシステムノイズ値と比較する段階と、
前記製造品目の測定された物理的特性から新しい物理的鍵を生成する段階と、
前記新しい物理的鍵および前記導き出された独特の製品識別子に対してハッシュ関数を実行することにより、前記物理的ノイズ値の新しいコピーを生成する段階と、
前記物理的ノイズ値の前記新しいコピーを前記導き出された物理的ノイズ値と比較する段階と、
前記システムノイズ値の前記新しいコピーと前記導き出されたシステムノイズ値が同一であるかどうか、また前記物理的ノイズ値の前記新しいコピーと前記導き出された物理的ノイズ値と同一であるか、またはそれらに関連性があるかどうかの両方について表示を提供する段階とを含む、方法。
【請求項１１】
前記一つ以上の暗号化鍵が静止鍵および動的鍵を含み、また新しい動的鍵が製造品目の各バッチについて作成される、請求項1～10のいずれか1項に記載の方法。
【請求項１２】
前記独特の製品識別子が前記品目が属する品目のバッチを識別する情報を含む、請求項1～11のいずれか1項に記載の方法。
【請求項１３】
ノイズ値は、ハッシュ値又は鍵付きハッシュ値、ないしは、ハッシュ値及び秘密鍵から直接導き出される値又はキャラクタの配列を含む、請求項1～12のいずれか1項に記載の方法。
【請求項１４】
前記製造品目の前記測定された物理的特性は、前記製造品目の表面の質感に基づいている、請求項1～12のいずれか1項に記載の方法。
【請求項１５】
製造品目をマーク付けするための装置であって、

暗号化鍵を生成するように構成された鍵生成装置と、
各製造品目について独特の製品識別子を生成するよう構成されたコード生成装置と、
各製造品目の測定された物理的特性から物理的鍵を生成するように構成された物理的鍵の生成装置と、
処理手段とを含み、
前記処理手段は、
前記独特の製品識別子および一つ以上の暗号化鍵を使用して各製造品目について秘密鍵を生成するよう構成され、
前記秘密鍵および独特の製品識別子に対してハッシュ関数を実行することにより各製造品目についてのシステムノイズ値を生成するように構成され、
前記物理的鍵および前記独特の製品識別子に対してハッシュ関数を実行することにより各製造品目についての物理的ノイズ値を生成するように構成され、
前記秘密鍵および前記物理的鍵から導き出されたかまたはそれらを組み込んだセキュア識別子を生成するように構成され、前記セキュア識別子が、前記システムノイズ値から導かれたものか、または前記システムノイズ値を組み込むものであり、前記セキュア識別子が、前記物理的ノイズ値から導かれたものか、または前記物理的ノイズ値を組み込むものであり、
製造品目をマーク付けするための装置は、さらに、
前記セキュア識別子または前記セキュア識別子から導き出した識別子を用いて各製造品目にマークを付けるためのマーカーとを含む。

【請求項１６】
前記製造品目がたばこ製品を含む容器である、請求項15のいずれか1項に記載の装置。

【請求項１７】
前記製造品目の前記測定された物理的特性は、前記製造品目の表面の質感に基づいている、請求項15又は16に記載の装置。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、製造品目をマーク付けするための方法および装置に関連する。特に、本発明は包装物品のマーク付けに関連する。

【背景技術】
【０００２】
偽造品および密輸品は、顧客、製造者、および政府当局にとって世界的な問題である。大抵の場合において品質不良である物品を無断に生産した偽造品が、世界中で違法に販売されている。これらの物品は、危険性を伴う品質不良である可能性があるため、顧客にとって有害である（これは医薬品またはその他の消費財などの製品にとって特に重要である）。偽造品は、評判の失墜、それらの製品を製造する不法製造者による競争の増加、およびその他の法的権利の侵害を被ることになりうるため、製造者にとって有害である。課税または政府規制を避ける目的で製造された物品である密輸品も、製造者および政府当局にとって相当な問題である。これらの物品は、不法に転用、売買、または輸入され、その結果、関税または税金の不適切な徴収により政府当局の収入に対してかなりの損失をもたらす。

【０００３】
品目が認証される場所ですべての独特のマーキングを保存する必要なしに、品目上の独特のマーキングを使用して製造品目を認証できることには利点がある。また、それぞれの独特のマーキングの認証記録を保存する必要なしに、偽造品目、または真正製品の独特のマーキングがコピーされた品目を検出できることが望ましい。

【発明の概要】
【０００４】
本開示の一態様で、製造品目をマーク付けする方法が提供されているが、これは、

製造品目のための独特の製品識別子を生成する段階と、
一つ以上の暗号化鍵を生成する段階と、
独特の製品識別子および一つ以上の暗号化鍵を使用して秘密鍵を生成する段階と、
製造品目の測定された物理的特性から物理的鍵を生成する段階と、
秘密鍵および物理的鍵から導き出されたか、またはそれらを組み込んだセキュア識別子を生成する段階と、
製造品目にマークを付ける段階であって、マークがセキュア識別子またはセキュア識別子から導き出された識別子を含む段階を含む。

【０００５】
セキュア識別子は、独特の製品識別子に組み込みうる。

【０００６】
方法はさらに、秘密鍵および独特の製品識別子を使用してシステムノイズ値を生成する段階も含むことが好ましいが、ここで、セキュア識別子は、システムノイズ値から導かれたものか、またはそれを組み込むものである。システムノイズ値を生成する段階は、秘密鍵および独特の製品識別子に対してハッシュ関数を実行する段階を含むことが好ましい。

【０００７】
方法はさらに、物理的鍵および独特の製品識別子を使用して物理的ノイズ値を生成する段階も含むことが好ましいが、ここで、セキュア識別子は、システムノイズ値から導かれたものか、またはそれを組み込むものである。物理的ノイズ値を生成する段階は、物理的鍵および独特の製品識別子に対してハッシュ関数を実行する段階を含むことが好ましい。

【０００８】
本明細書で使用される場合、「独特の製品識別子」は、製造品目を独特に識別する識別子を意味する。各製造品目には、異なる独特の製品識別子が与えられる。独特の製品識別子は通常、数字または英数字の配列または値である。

【０００９】
「暗号化」は本明細書で使用されるとき、アルゴリズムを使用して情報を変化させ、その情報を暗号鍵という形態の特別な知識を所有する人物以外には誰にも読み取ることができないようにするプロセスを意味する。復号化は、その反対のプロセスである。「暗号鍵」は、暗号化アルゴリズムとともに使用して、情報を暗号化または復号化する一片の情報である。暗号鍵は通常、数字または英数字の配列または値である。

【００１０】
「秘密鍵」という用語は本明細書で使用されるとき、独特の製品識別子および一つ以上の追加的な鍵またはデータ片を使用して生成された鍵付きハッシュで使用される鍵を説明するのに使用される。生成された時点で、秘密鍵は、その秘密鍵を作成した当事者以外のいかなる当事者にも知られていない。この文脈では、「秘密鍵（secret key）」という用語は、非対称暗号化方式の文脈での秘密鍵（private key）の意味に限定されない。

【００１１】
「ハッシュ関数」は本明細書で使用されるとき、ハッシュ値と呼ばれる固定サイズの出力（通常は入力データよりも小さい）に入力データをマッピングする関数である。ハッシュ関数は通常、情報の換字または転置、もしくは換字および転置をしてハッシュ値またはノイズ値を生成する。ハッシュ関数は、暗号ハッシュ関数であることが好ましい。暗号ハッシュ関数は、入力データのフィンガープリントまたはチェックサムを生成する。2片のデータは、同一の暗号ハッシュ関数を使用したときに同一のハッシュ値が生成される場合、同一であると見なすことができる。有利なことに、ハッシュ関数は一方向のハッシュ関数であり、これはハッシュ値から入力データを導き出すことが計算的に不可能なことを意味する。これらの属性は、以下で説明する通り、認証プロセスで使用できる。ハッシュ関数は、鍵付きハッシュ値またはノイズを生成する目的で、秘密鍵および入力メッセージを組み合わせることにより鍵化できる。

【００１２】
「ノイズ値」という用語は本明細書で使用されるとき、ハッシュ値、または鍵付きハッ

シュ値、またはハッシュ値および秘密鍵から直接的に導かれた値もしくは文字配列を意味する。

【００１３】

製造品目の測定された物理的特性は、測定された任意の物理的特性としうるが、質量、サイズ、形状、表面の質感またはパターン、色、化学組成、または電気的刺激、磁気的刺激または光学的刺激に対する反応など、刺激に対する反応に基づくものとしうる。測定された物理的特性は、各製造品目にとって独特のものとなる可能性が高くなるような、または少なくとも任意の2つの製造品目が同じであるよりは異なる可能性がより高くなるような分解能となるように選択され測定されることが好ましい。測定された物理的特性は、製造品目について物理的な署名を提供することが好ましい。一つの好ましい実施形態で、測定された物理的特性は、製造品目の包装の一部の画像である。

【００１４】

セキュア識別子は任意の種類の識別子としうるが、数字または英数字の配列または値であることが好ましい。マークは、文字または数字の配列とすることも、一次元または二次元のバーコードなどの図式的表示とすることもできる。

【００１５】

一つの実施形態で、セキュア識別子を生成する段階は、独特の製品識別子をシステムノイズ値とともに暗号化することにより第一の識別子を生成する段階と、第一の識別子を物理的ノイズ値とともに暗号化することによりセキュア識別子を生成する段階とを含む。

【００１６】

この実施形態で、方法はさらに、確認センターで製造品目を認証する段階であって、その認証の段階が、品目上のマークを識別する段階と、マークを復号化して第一の識別子および物理的ノイズ値を導き出す段階と、第一の識別子を復号化して独特の製品識別子およびシステムノイズ値を導き出す段階と、製造品目の測定された物理的特性から新しい物理的鍵を生成する段階と、新しい物理的鍵および導き出された独特の製品識別子に対してハッシュ関数を実行することにより物理的ノイズ値の新しいコピーを生成する段階と、物理的ノイズ値の新しいコピーを導き出された物理的ノイズ値と比較する段階と、導き出された物理的ノイズ値が物理的ノイズ値の新しいコピーと同一であるか、またはそれらに関連性があるかどうかの表示を提供する段階とを含む、段階を含みうる。

【００１７】

比較する段階は相関性のスコアを導き出す段階を含むことができ、また表示を提供する段階はその相関性のスコアが閾値よりも大きいかどうかの表示を提供する段階を含む。

【００１８】

この実施形態で、認証の段階は、独特の製品識別子および一つ以上の暗号化鍵から新しいコピーを生成する段階と、秘密鍵および独特の製品識別子の新しいコピーに対してハッシュ関数を実行することによりシステムノイズ値の新しいコピーを生成する段階と、システムノイズ値の新しいコピーを導き出されたシステムノイズ値と比較する段階と、システムノイズ値の新しいコピーおよび導き出されたシステムノイズ値が同一であるかどうかの表示を提供する段階とをさらに含みうる。

【００１９】

別の実施形態において、セキュア識別子を生成する段階は、独特の製品識別子をシステムノイズ値とともに暗号化することにより第一の識別子を生成する段階と、独特の製品識別子を物理的ノイズ値とともに暗号化することにより第二のセキュア識別子を生成する段階と、製造品目にマークを付ける段階であって、そのマークが第一および第二のセキュア識別子、または第一および第二のセキュア識別子から導き出された識別子（単一または複数）を含む段階とを含む。

【００２０】

この実施形態で、方法は、確認センターで製造品目を認証する段階であって、その認証の段階が、品目上のマークを識別する段階と、マークを復号化して独特の製品識別子、システムノイズ値および物理的ノイズ値を導き出す段階と、独特の製品識別子および一つ以

上の暗号化鍵から新しいコピーを生成する段階と、秘密鍵および独特の製品識別子の新しいコピーに対してハッシュ関数を実行することによりシステムノイズ値の新しいコピーを生成する段階と、システムノイズ値の新しいコピーを導き出されたシステムノイズ値と比較する段階と、製造品目の測定された物理的特性から新しい物理的鍵を生成する段階と、新しい物理的鍵および導き出された独特の製品識別子に対してハッシュ関数を実行することにより、物理的ノイズ値の新しいコピーを生成する段階と、物理的ノイズ値の新しいコピーを導き出された物理的ノイズ値と比較する段階と、システムノイズ値の新しいコピーと導き出されたシステムノイズ値が同一であるかどうかと、物理的ノイズ値の新しいコピーと導き出された物理的ノイズ値が同一であるか、またはそれらに関連性があるかどうかの両方について表示を提供する段階とを含む段階をさらに含みうる。

【００２１】

いずれかの実施形態で、第一のセキュア識別子を生成する段階は、コード生成装置の鍵を使用して独特の製品識別子およびシステムノイズ値を暗号化する段階であって、その第二のセキュア識別子を生成する段階が第一のセキュア識別子と物理的ノイズ値とを組み合わせてコード生成装置IDと組み合わせる段階を含み、また確認センターのルックアップテーブルでコード生成装置IDを使用してコード生成装置の鍵を導き出すかまたは獲得することができる段階を含みうる。

【００２２】

いずれかの実施形態で、方法はさらに、確認センターで一つ以上の暗号化鍵を記憶する段階を含みうる。一つ以上の暗号化鍵は静止鍵および動的鍵を含みうるが、ここで製造品目の各バッチについて新しい動的鍵が作成されるのに対して、製造品目の複数のバッチについて同一の静止鍵が使用される。

【００２３】

独特の製品識別子は、その品目が属する品目のバッチを識別する情報を含みうる。

【００２４】

本発明は、製造者からの情報、すなわち様々な暗号化鍵、および品目の物理的特性の両方に基づき認証する能力を提供する。これにより2層による認証が提供され、また真正品目についての識別子のクローン作成の検出ができるが、大規模な認証コードの記憶は要求されない。

【００２５】

本発明の別の態様で、製造品目をマーク付けするための装置が提供されており、この装置は、

暗号化鍵を生成するように構成された鍵生成装置と、

各製造品目について独特の製品識別子を生成するよう構成されたコード生成装置と、

各製造品目の測定された物理的特性から物理的鍵を生成するように構成された物理的鍵生成装置と、

処理手段であって、

独特の製品識別子および一つ以上の暗号化鍵を使用して各製造品目について秘密鍵を生成し、

秘密鍵および物理的鍵から導き出されたか、またはそれらを組み込んだセキュア識別子を生成するように構成されたものと、

セキュア識別子またはセキュア識別子から導き出した識別子を用いて各製造品目にマークを付けるためのマーカーとを含む。

【００２６】

プロセッサは、秘密鍵および独特の製品識別子を使用してシステムノイズ値を生成するように構成されていることが好ましいが、ここでセキュア識別子は、システムノイズ値から導かれたものか、またはそれを組み込むものである。プロセッサは、秘密鍵および独特の製品識別子に対してハッシュ関数を実行することにより、各製造品目についてのシステムノイズ値を生成するように構成されていることが好ましい。

【００２７】

プロセッサは、物理的鍵および独特の製品識別子を使用して物理的ノイズ値を生成するように構成されていることが好ましいが、ここでセキュア識別子は、物理的ノイズ値から導かれたものか、またはそれを組み込むものである。プロセッサは、物理的鍵および独特の製品識別子に対してハッシュ関数を実行することにより、各製造品目についての物理的ノイズ値を生成するように構成されていることが好ましい。

【００２８】

一つの実施形態で、処理段階は、独特の製品識別子を秘密鍵またはシステムノイズ値とともに暗号化することにより各製造品目について第一の識別子を生成する段階と、第一の識別子を物理的ノイズ値とともに暗号化することにより各製造品目についてセキュア識別子を生成する段階とを含む。

【００２９】

別の実施形態において、処理手段は、独特の製品識別子を秘密鍵またはシステムノイズ値とともに暗号化することにより各製造品目について第一の識別子を生成する段階と、独特の製品識別子を物理的鍵または物理的ノイズ値とともに暗号化することにより各製造品目について第二のセキュア識別子を生成する段階とを含むように構成され、マーカーは、第一のセキュア識別子および第二のセキュア識別子、または第一および第二のセキュア識別子から導き出された識別子（単一または複数）を用いて製造品目にマークを付けるように構成される。

【００３０】

製造品目は、たばこ製品を含む容器としうる。たばこ製品の例は、紙巻たばこ、ルーズリーフたばこ、葉巻たばこ、および電気加熱された喫煙システム用またはその他のe-シガレットシステム用のカートリッジまたは詰め替えである。

【００３１】

本発明により、大量の情報を記憶する必要なく、製造品目を認証できるようになる。これは、大量に生産される品目の認証に適した任意の実用的なシステムにとって重要である。その上、独特の製品識別子（UPI）との組み合わせで物理的鍵を使用することでセキュリティが高まり、偽造品および密輸品の製造がより困難なものとなる。物理的鍵を追加することで、クローン作成の検出ができ、かつ複製が困難なシステムが提供される。偽造者に物理的鍵の生成に使用される特定のツールについての知識があった場合でも、識別子の生成に物理的鍵とUPIの組み合わせを用いることにより、クローン作成がほとんど不可能なものとなる。また、本発明により、認証はシステムノイズ値に基づき、オンラインで、すなわち通信ネットワークを通して確認センターに接続して遂行でき、また同様に、認証は物理的ノイズ値に基づきオフラインで遂行できるようになる。各品目に必要なマーク付けは単に一つ以上のコードであり、そのため、技術的に複製が困難な高価なラベルに依存するその他の一部のソリューションと比較して、各品目に対してほんのわずかな費用しか加算しない。

【００３２】

ここで本発明の実施形態を、以下の添付図面を参照しながら、例証としてのみであるが説明する。

【図面の簡単な説明】

【００３３】

【図１】図1は、本発明の一実施形態によるマーキングシステムの概略図である。

【図２】図2は、システムノイズ値と物理的ノイズ値がどのように導き出されるかを図示する。

【図３】図3は、図1のシステム上で遂行されうる、本発明の一実施形態のマーキング方法を示すフローチャートである。

【図４】図4は、図1のシステム上で遂行されうる、図3に示す本発明の実施形態のための認証方法を示すフローチャートである。

【図５】図5は、図1のシステム上で遂行されうる、本発明の別の実施形態のマーキング方法を示すフローチャートである。

【図６】図6は、図1のシステム上で遂行されうる、図5に示す本発明の実施形態のための認証方法を示すフローチャートである。

【発明を実施するための形態】

【００３４】

製造品目上の独特のマーキングは、品目のトラッキングに使用できる。例えば、顧客の注文を、注文された物品を含む特定の発送ケース（単数または複数）の識別用ラベル（単数または複数）にリンク付けしうる。この文脈での「物品」は、顧客への流通または販売が意図された製造品目またはその他の品物を意味する。これにより、顧客、製造者および任意の中間業者は、要求される物品の場所を常にトラッキングできる。これは、識別子の走査用のスキャナーを使用して、確認センターに通信することにより達成しうる。別の方法として、識別子は人が読むことができ、その人はその後、手作業で確認センターに通信することができる。識別子はまた、顧客、国内当局およびその他の当事者によって、特定の品目に真正な製品が含まれていることを確認するために使用されうる。例えば、当事者は、発送ケースにある識別子を読み取るためにスキャナーを使用しうる（または識別子は上記の通り、人が読み取ることもできる）。識別子の詳細は、確認センターに送信されうる。次に、確認センターが識別子の詳細を調べるか、またはその他の方法で処理し、発送ケースの製造詳細を判断し、それらの詳細をスキャナーに送信し、それによって、当事者は発送ケースおよびその中に含まれている製品が真正なものとして確認できる。中央データベースが識別子を認識しない場合には、当事者はその問題の物品は偽造品であると推量しうる。識別子はまた、品目の追跡にも使用しうる。例えば、製造者が特定の数の発送ケースからの製品をリコールする必要がある場合、それらの発送ケースはその識別子を使用して追跡することができる。

【００３５】

図1は、本発明の一実施形態によるマーキングシステムの概略図である。この実施形態で、システム101は、製造品目109を製造するための一つ以上の製造センター103、105、107を含む。各製造センターは、紙巻たばこの製造および包装ラインでありうる生産ラインまたは施設を備えうる。製造はバッチで遂行され、各バッチが一定数の個別製造品目の製造専用であることが好ましい。二つ以上の製造センターがある場合、これらは同一または異なる製造サイトに物理的に位置しうる。この好ましい実施形態で、システムは製造センター103、105、107を含むが、本発明は、実際は、輸入ポイント、流通ポイント、購入者、卸売業者またはサプライチェーン内のその他の任意のポイントで実施されうる。

【００３６】

各製造センターは、製造品目109のためのコードを生成するためのコード生成装置111を含む。コード生成装置111は、特定の製造センター専用の完全に自律的なコンピュータまたはマイクロコントローラであることが好ましい。各製造センターはまた、各製造品目の物理的特性を測定または符号化し、それを物理的鍵207に変換する物理的鍵生成装置112を含む。コード生成装置111は、物理的鍵を使用して品目にマークを付けるためのコードを生成する。

【００３７】

この実施形態で、物理的鍵生成装置はWO2007/071788号に記載のある種類のものである。各品目の包装の一部に光が照らされ、照らされた部分の画像がデジタル画像センサーにより捕捉される。包装のその部分は、その時間的に安定した無秩序な微細構造となるように選択される。紙および厚紙などの材料は、その品目の「フィンガープリント」として使用できる無秩序な微細構造を持つ。品目のその部分の微細構造の画像は、WO2007/071788号に記載されている通り、英数字の値または行列の形態の物理的鍵または署名に変換される。この種類の物理的鍵の生成装置は、Signoptic Technologies（Savoie Technolac, 5 allee Lac d’Aiguebelette BP340 F-73375, LE BOURGET-DU-LAC, France）から入手できる。ただし、任意の種類の物理的鍵の生成装置を使用することができ、また、質量または形状など、品目のその他の物理的属性に依存することや、あるいは品目の化学的属性または生物学的属性に依存することさえもありうる。

【００３８】
この実施形態で、各製造センターはまた、製造品目109上に生成されたコードにマーク付けするためのマーカー113を含む。マーカー113は、適切な任意のマーク付け手段、例えば、連続的インクジェットプリンター、ドロップ・オン・デマンド式インクジェットプリンター、ホログラフィープリンター、レーザープリンター、または個別の製造品目上に生成されたコードの印刷またはマーク付けができるその他の任意のプリンターまたはマーカーを含みうるが、これに限定されない。生成されたコードの印刷またはマーク付けは、各品目上に、外側パッケージ上に、ラベル上に、またはその他の任意の好都合な方法で行いうる。一つの実施形態で、生成されたコードは、製造品目に、好ましくは除去できないように貼り付けられる接着タグまたはラベル上に印刷される。一つの実施形態で、生成されたコードは、製造品目上または品目の包装上に蒸着されたレーザー感受性材料の層上にレーザービームによって印刷される。この方法により、コードが透明なラッピング層を通して押印される。

【００３９】
システム101はさらに、製造品目のマーク付けおよび認証に使用するための鍵209、211を生成する鍵生成装置115を含む確認センター114と、中央サーバー117とを備える。この実施形態で、コード生成装置111は、セキュアなインターネット接続119および製造センターの近くのサーバー121を通して、またはその他のデータ通信手段により、確認センター114と通信ができる。別の方法として、コード生成装置111は、一つ以上の製造センター専用の製造ポータルを通して確認センターと通信することもできる。

【００４０】
鍵生成装置115は暗号化鍵を生成するが、本明細書では静止鍵と呼ぶ。鍵生成装置115は、暗号化されていないバージョンの静止鍵および暗号化されたバージョンの静止鍵を生成する。暗号化されていないバージョンの静止鍵は、本明細書では有効な静止鍵209と呼び、図1では実線の輪郭で示されている。暗号化されているバージョンの静止鍵は、本明細書では無効な静止鍵211と呼び、図1では点線の輪郭で示されている。有効な静止鍵209、すなわち暗号化されていないバージョンの静止鍵は、鍵生成装置115内に生成され、従って中央サーバー117にアクセス可能である。鍵生成装置115は、無効な静止鍵211を製造センター103、105、107でコード生成装置111に送信する。

【００４１】
無効な静止鍵211は、鍵生成装置115から、例えばCD-Rom、DVD-Romまたは取り外し可能ハードディスクなどの不揮発性データサポート上にあるコード生成装置111に送信されうる。データサポートは、製造センター103、105、107でコード生成装置111に物理的に転送される。別の方法として、無効な静止鍵211は、例えば暗号化に関与したものなどセキュアなネットワーク接続を通して、鍵生成装置115からコード生成装置111へ送信されうる。これは、コード生成装置111からの要求に応じたものとしうる。これによって、静止鍵の真正性、機密性および保全性が確保される。

【００４２】
鍵生成装置115はまた、無効な静止鍵211を復号化して有効な静止鍵209を形成するための鍵またはコードを含む、アクティベーションコード213を生成する。このアクティベーションコード213はまた、中央サーバー117にアクセス可能である。有効な静止鍵209およびアクティベーションコード213は、それらが割り当てられている製造センター103、105、107の識別と一緒に保存されることが好ましい。

【００４３】
一つの実施形態で、静止鍵はいくつかの部分を含む。主要な部分は、例えばソルト・マトリクス（salt matrix）などの多数の秘密コードとしうる。ソルト・マトリクスは、例えば、ランダムまたは疑似ランダムな桁数の長い文字列としうる。多くの部分には、静止鍵のための独特の識別子、静止鍵が動的鍵とどのように組み合わされるかを定めた順番に並べたコード（下記で考察）、静止鍵の独特の識別子に関連付けられたデジタル暗号証明書、および上記で生成されたデジタル暗号証明書を含む静止鍵ポリシーまたはライセンス

がさらに含まれる。

【００４４】

無効な静止鍵、すなわち、暗号化されたバージョンの静止鍵、および特に複数の秘密コードは、強力な暗号を使用して暗号化されることが好ましい。適切な暗号の一例は、Triple DES（Data Encryption Standard）ブロック暗号またはTriple DES/ Rijandelブロック暗号である。どちらも、Data Encryption Standard暗号アルゴリズムを各データブロックに3回適用し、またTriple DES/ RijandelはIBMによって開発されたTriple DESをわずかに変形したものである。その場合、Triple DESまたはTriple Des/Rijandelの鍵はアクティベーションコード213を含む。こうして、一つの好ましい実施形態で、有効な静止鍵209は暗号化されず、無効な鍵211はTriple DESまたはTriple Des/Rijandelの鍵を使用して暗号化され、アクティベーションコード213はそのTriple DESまたはTriple Des/Rijandelの鍵を含む。

【００４５】

次の段階203で、コード生成装置111により受信された無効な静止鍵211が登録される。これは、コード生成装置111によって、受信した静止鍵および関連性のある任意のマシン情報（図示せず）についての情報215を確認センター114に送信することにより実行される。これは、図1に示す通り、セキュアなインターネット接続119を経由して送信されることが好ましいが、別の適切な経路によっても送信されうる。確認センター114は、コード生成装置111にアクティベーションコード213を送り返す。アクティベーションコード213により、無効な静止鍵211が有効化されるようになり、これは217に図解的に示されている。アクティベーションコード213は、図1に示す通りセキュアなインターネット接続119を通しても送信されることが好ましい。登録手順は、有効な静止鍵209がインターネットを経由して絶対に転送されないように準備することが好ましい。

【００４６】

登録手順は、従来的な公開／秘密鍵ペアの交換メカニズムの形態を取りうる。これは、上述の通り、静止鍵の一部分を形成するデジタル暗号証明書に関連付けられた非対称鍵ペアを使用しうる。その場合、非対称鍵ペアの公開鍵は、第三者、例えば政府当局によって発行された形態としうる。コード生成装置111から確認センター114に送信された受信済み静止鍵についての情報215は、上述の通り、静止鍵の部分を形成する静止鍵のための独特の識別子を含みうる。これもコード生成装置111から確認センター114に送信されたものであるが、関連性のあるマシン情報（図示せず）は、コード生成装置111または製造センターのための独特の識別子または証明書を備えうる。独特の識別子は、製造のために予め許可された、コード生成装置または製造センターの位置およびアイデンティティについての情報を含みうる。静止鍵の独特の識別子およびコード生成装置または製造センター識別子は、静止鍵の証明書に関連付けられた非対称鍵ペアの公開鍵を使用して暗号化されることが好ましい。

【００４７】

確認センター114が暗号化された静止鍵の独特の識別子およびコード生成装置または製造センター識別子を受信すると、確認センター114は静止鍵の証明書と関連付けられた非対称鍵ペアの秘密鍵を使用して復号化できる。次に、確認センターは、静止鍵の独特の識別子およびコード生成装置または製造センター識別子が有効であることをチェックしうる。次に、確認センター114は、コード生成装置111にアクティベーションコード213を送り返す。既に言及した通り、アクティベーションコード213は、Triple DESまたはTriple DES/Rijandel暗号の形態であることが好ましい。確認センターは、アクティベーションコード（例えば、Triple DESまたはTriple DES/Rijandel暗号）を、静止鍵の証明書に関連付けられた非対称鍵ペアの公開鍵で暗号化する。これにより、アクティベーションコード（例えば、Triple DESまたはTriple DES/Rijandel暗号）が、静止鍵の証明書と関連付けられた非対称鍵ペアの秘密鍵を使用してコード生成装置により復号化されるようになる。次に、無効な静止鍵211は、有効な静止鍵209を形成するために、復号化されたアクティベーションコード213を使用して有効化できる。

【００４８】
コード生成装置111で無効な静止鍵211が有効化されると、製造センターは品目を製造でき、コード生成装置111で製造品目のためのコードを生成できる。
【００４９】
コード生成装置111は、本明細書では動的鍵219と呼ぶ新しい鍵を、製造品目の各バッチについて生成する。動的鍵219は、ランダムな数字などランダムな秘密コードであることが好ましい。コード生成装置は、バッチについての動的鍵219を有効な静止鍵209とともに使用して、秘密鍵223を生成する。次に、秘密鍵223は、各品目について物理的鍵および独特の製品識別子（UPI）との組み合わせで使用され、そのバッチ内の製造品目上にマーク付けされるコード221（例えば英数字コード）を生成する。この実施形態で、各品目についてのUPIは、製造時間を識別する製造詳細と、同一の製造センターによって単一の時間間隔内に製造された品目を区別するための増分カウンター値とを備える。
【００５０】
コード生成装置は、UPIと秘密鍵の組み合わせ、およびUPIと物理的鍵の組み合わせについて暗号ハッシュ関数を使用する。これにより、品目についてデジタルフィンガープリント（本明細書では「ノイズ値」と呼ぶ）が作成されるが、これらのノイズ値は、マーカー113によって品目上にマーク付けされるコード221を生成するために使用される。共通して使用される暗号ハッシュ関数に加えて、ハッシュ値またはノイズ値の生成には、転置式、換字式、テーブル換字式および索引付けなどを含み、それらに限定されない様々な技法が利用できる。
【００５１】
図2は、コード生成装置111により遂行されるノイズ値の生成方法を図示する。システムノイズ値225を生成するために、秘密鍵がまず、有効な静止鍵209、動的鍵219およびUPI 221から導き出される。動的鍵219および有効な静止鍵209は、確認センター114およびコード生成装置111にのみ知られている。段階301で、静止鍵内でシリアル化されたコードに従い、動的鍵およびUPIが静止鍵内に含まれる秘密鍵をソルト・マトリクスから抽出するために使用される。次に、秘密鍵223およびUPI 221は段階303でハッシュ化されて、品目についてのシステムノイズが生成される。物理的ノイズ値227を生成するために、物理的鍵207は段階305でUPI 221を用いてハッシュ化される。システムノイズ値を生成するために使用されるハッシュ関数は、物理的ノイズ値を生成するために使用されるハッシュ関数と同一でも異なるものでもよい。
【００５２】
図3は、本発明の第一の実施形態に従い、システムノイズ値と物理的ノイズ値を使用して、各品目についてセキュア識別子を生成する方法を図示する。段階311で、システムノイズ値225およびUPI 221は組み合わされる。段階313で、組み合わされたシステムノイズ値およびUPIは、コード生成器難読化コード（CGOK）231によって暗号化され、第一の識別子241が生成される。CGOKはコード生成装置に特定のもので、コード生成装置に予めロードされている。次に、第一の識別子241は、物理的ノイズ値227およびコード生成装置識別子233と組み合わされる。コード生成装置識別子（CGID）233により、認証中にCGOKを取得できるようになる。次に、第一の識別子、物理的ノイズ値およびCGIDの組み合わせが、段階317でグローバル鍵235を使用して暗号化され、セキュア識別子251が生成される。グローバル鍵235は、すべての製造センターに対して共通であり、確認センターで分かっている対称鍵または非対称鍵のペアの一部としうる。次に、セキュア識別子251は、段階319でマーカー113によって品目にマーク付けされる。
【００５３】
コード生成装置111または製造センター103、105、107は、製造品目にマーク付けされたコード数を保持する。さらに、コード生成装置111は、各バッチについて動的鍵219を、バッチ（図示せず）についての情報とともに確認センター114に送信する。これは、セキュアなインターネット接続119を通して実行されうる。バッチについての情報は、例えば、ブランド、意図された市場または意図された目的地などの様々な情報片を含みうるが、こ

れに限定されない。動的鍵219は、確認センター114にリアルタイムで送信される必要がなく、適切な任意の時間（例えば、毎月一回）に確認センターに通信できる。確認センター114に送信された動的鍵219は、確認センター114にあるか、またはそこからアクセスが可能なデータベース内に（例えば、中央サーバー117で）記憶される。各バッチについての動的鍵219は、同じ時点で確認センター114に送信されたバッチ情報とともに記憶されることが好ましい。

【００５４】

有効な静止鍵209は、特定の製造センター103、105、107でのコード生成装置111が非稼働となったときに削除されることが好ましい。これにより、悪意あるユーザーが、適切な登録なしに有効な静止鍵209に対するアクセスを得ることが防止される。コード生成装置111を無効化してコード生成装置111および製造センターの無断使用を防止するための追加的な手段が提供されうる。

【００５５】

図4は、確認センター114によって遂行される段階、およびユーザー601が図3の段階に従ってマーク付けされた個別の製造品目の認証を希望するときにユーザー601によって遂行される段階を図示する。ユーザー601は、品目上のコード221を読み取り、それを確認センター114に送信する。これは、図1に図示されている。ユーザー601は、セキュアまたは非セキュアなインターネット接続などの適切な任意の手段により、コードを確認センター114に送信しうる。

【００５６】

確認センターは、段階321でセキュア識別子を受信する。セキュア識別子は、段階323でグローバル鍵235（または非対称鍵を使用する場合は鍵ペア中の対応する鍵）を使用して復号化され、物理的ノイズ値227および第一の識別子241が明らかにされる。CGIDもまた明らかにされる。次に、ルックアップテーブルを使用して、CGOK 231がCGIDから取得される。次に、第一のIDが段階325でCGOK 231を使用して復号化され、システムノイズ225およびUPI 221が明らかにされる。この情報と、有効な静止鍵209および動的鍵219および新しい物理的鍵を合わせて、品目を認証するために物理的ノイズ値およびシステムノイズ値の両方を再現できる。

【００５７】

物理的ノイズ値を再現するには、段階327で、オリジナルの物理的鍵207を生成するために使用されたのと同一の方法および同一の条件下で品目の一部分の画像を記録することにより、新しい物理的鍵がユーザー601によって取得される必要がある。次に段階329で、UPIおよび新しい物理的鍵がハッシュ化され、新しい物理的ノイズ値が生成される。段階331で、新しい物理的ノイズが段階323で明らかにされた抽出済み物理的ノイズ値と比較される。新しい物理的ノイズ値が、抽出された物理的ノイズ値と十分に類似している場合には、認証過程の一部が完了する。新しい物理的ノイズ値が、抽出された物理的ノイズ値と十分に類似していない場合には、段階339で品目は真正性がないことが判断される。

【００５８】

その品目が真正性があると見なされるには、新しい物理的ノイズ値は抽出された物理的ノイズ値と同一であることが必要な場合がある。ただし、品目が真正性があると見なされるために、相関性スコアを使用して閾値の相関性スコアを要求することにより、新しい物理的ノイズ値と抽出された物理的ノイズ値との間にいくらかの差異を許容することが可能である。US2005/0257064号は、繊維質の媒体の測定された物理的属性から導き出された2つのデジタル署名間の相関性または類似性の度合いを計算する適切な統計的方法を記載している。

【００５９】

ユーザー601または確認センター114のいずれかが、段階329および331を遂行することが可能である。ユーザー601に確認センターによってUPIが供給されている場合、エンドユーザーは物理的ノイズ値に基づき品目を認証できる。同様に、新しい物理的鍵が確認センター114に供給されている場合、確認センターは物理的ノイズ値に基づき品目を認証できる

。

【００６０】

システムノイズ値を再現するには、秘密鍵が再生成されなければならない。段階333で、UPIおよびCGIDを使用して、確認センター114は、確認センターで保持されている記録から動的鍵219および有効な静止鍵209を取り出すことができる。次に、UPI 221、動的鍵219および有効な静止鍵209を使用して、秘密鍵を再生成できる。段階335で、UPIおよび秘密鍵をハッシュ化することにより、新しいシステムノイズ値が再現される。段階337で、新しいシステムノイズ値が、段階325で抽出されたシステムノイズ値と比較される。新しいシステムノイズ値および抽出されたシステムノイズ値が同一の場合、段階339で品目は真正性があると判断できる。

【００６１】

一つの実施形態で、ある品目が真正性があると見なされるために、物理的ノイズ値とシステムノイズ値の両方の比較が必要とされる。ただし、希望に応じてそれらの一方のチェックに基づき認証を許容することが可能である。

【００６２】

有効な静止鍵は、その関連付けられた製造センターの詳細とともに確認センターに保存されることが好ましいため、抽出された有効な静止鍵209から、品目が製造された製造センター103、105、107を判断できる。動的鍵は確認センターに関連付けられたバッチ情報とともに保存されることが好ましいため、抽出された動的鍵219から、品目についてのバッチ情報を判断できる。こうして、確認センター114は、ユーザー601から送信されたコード221を元に、個別の品目および品目の真正性のチェックについての様々な情報片603を抽出できる。次に、品目に真正性があるかどうかの表示を含めて、情報603のすべてまたはその選択した部分をユーザー601に送信できる。これは、図1に図示されている。情報603は、オリジナルのコードが送信されたのと同一の手段によってユーザー601に送信されることが好ましい。

【００６３】

図5は、本発明の第二の実施形態によるマーク付けのプロセスを図示したものである。図5の方法で、2つのセキュア識別子が生成されるが、一方はシステムノイズ値225に基づき、もう一方は物理的ノイズ値227に基づく。段階341で、システムノイズ値225はUPI 221と組み合わされる。次に段階343で、システムノイズ値と物理的ノイズ値の組み合わせがCGOK 231とともに暗号化され、図3の第一の実施形態にある通り第一のID 241が生成される。次に段階345で、第一のID 241がCGIDと組み合わせられ、段階347でグローバル鍵235を使用して暗号化されて、第一のセキュアID 271が生成される。物理的ノイズ値227は段階221でUPIと組み合わされ、第二のID 261が生成される。第二のIDは段階353でグローバル鍵235を使用して暗号化され、第二のセキュアIDが生成される。次に段階355で、第一のセキュアID 271および第二のセキュアID 281で品目をマーク付けできるか、または第一のセキュアID 271と第二のセキュアID 281の組み合わせから導き出されたマーク（単一または複数）で品目をマーク付けできる。

【００６４】

図6は、図5に図示したプロセスを使用してマーク付けされた品目の認証を遂行する段階を図示したものである。段階401で、マーク（単一または複数）はユーザーによって読み取られ、ユーザーは第一のセキュア識別子271および第二のセキュア識別子281を導き出す。段階403で、グローバル鍵235は、物理的ノイズ値227、UPI 221の第一のコピー、第一のID 241およびCGID 233を導き出すために使用される。ユーザーがグローバル鍵235を持っている場合、ユーザーは、第二のセキュア識別子に基づき、オフラインで、すなわち確認センターとの接続を必要とすることなく、品目を認証できる。ユーザーは、段階407で新しい物理的鍵を生成し、これが段階409でUPIを使用してハッシュ化され、新しい物理的ノイズ値が生成される。ユーザーは、段階411で、新しい物理的ノイズ値を、段階403で抽出された物理的ノイズ値と比較できる。図3に関連して説明した通り、新しい物理的ノイズ値が、抽出された物理的ノイズ値と同様であるか、または十分に類似している場合に、品

目は段階419で真正性があると見なすことができる。

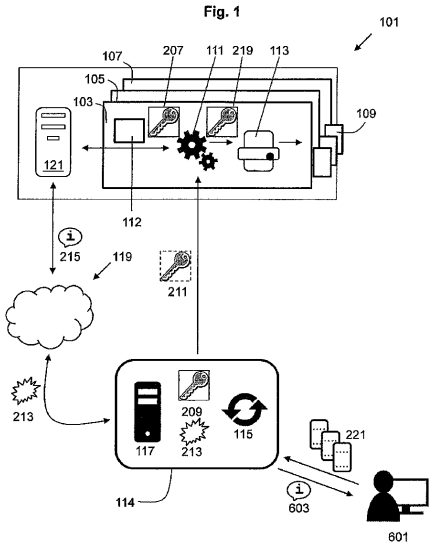
【００６５】

段階405で、確認センターによりCGIDが使用されてCGOK 231が取り出され、そのCGOKが第一のID 241を復号化して、システムノイズおよびUPIの第二のコピーを明らかにするために使用される。段階408で、UPIの第二のコピーをチェックとしてのUPIの第二のコピーと随意に比較できる。段階423で、確認センター114は、CGIDおよびUPIを使用して動的鍵219および有効な静止鍵209を取り出す。段階415で、新しいシステムノイズ値は、まずUPI、動的鍵および静止鍵から秘密鍵を再生成してから、秘密鍵をUPIでハッシュ化することにより生成される。段階417で、新しいシステムノイズ値が、段階405で抽出されたシステムノイズ値と比較される。それらが同一である場合、段階419で品目を認証することができる。図3の実施形態でと同様に、品目が真正性があると見なされるには、システムノイズ値と物理的ノイズ値の両方に基づく認証が必要とされうる。

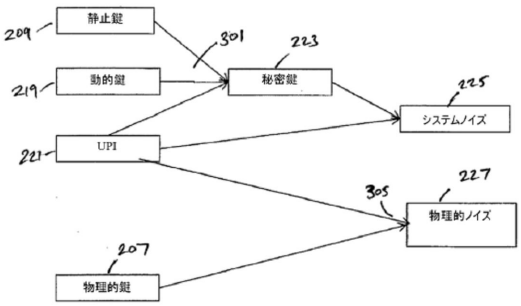
【００６６】

本発明は、紙巻たばこの製造に関連して説明してきたが、本発明は、医薬品、アルコール飲料および贅沢品など、認証を要する任意の製品に適用されることが明らかであるべきである。

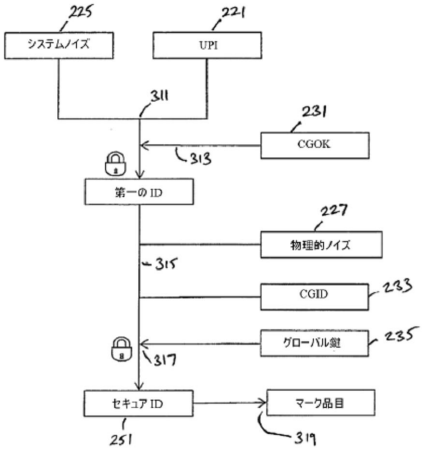
【図１】



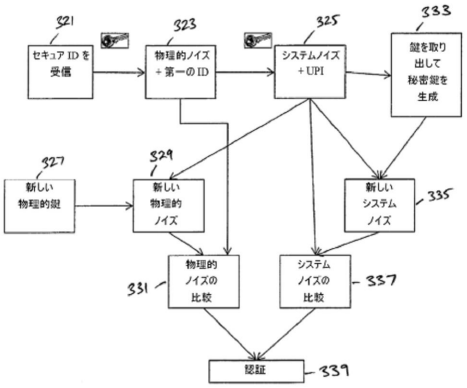
【図２】



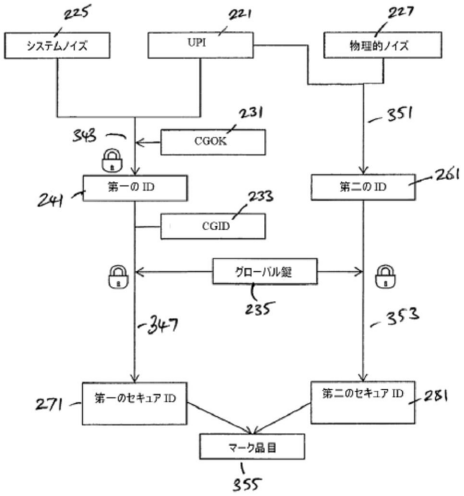
【図３】



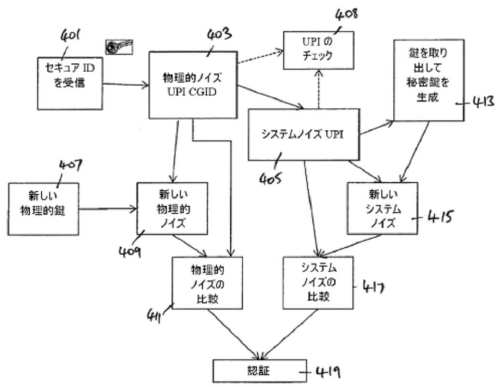
【図４】


321
セキュア ID を受信
323
物理的ノイズ＋第一の ID
325
システムノイズ＋UPI
333
鍵を取り出して秘密鍵を生成
327
新しい物理的鍵
329
新しい物理的ノイズ
335
新しいシステムノイズ
331
物理的ノイズの比較
337
システムノイズの比較
339
認証

【図５】


225
システムノイズ
221
UPI
227
物理的ノイズ
231
CGOK
343
351
241
第一の ID
233
CGID
261
第二の ID
グローバル鍵
235
347
353
271
第一のセキュア ID
第二のセキュア ID
281
マーク品目
355

【図６】


401
セキュア ID を受信
403
物理的ノイズ UPI CGID
408
UPI のチェック
鍵を取り出して秘密鍵を生成
413
システムノイズ UPI
405
407
新しい物理的鍵
新しい物理的ノイズ
409
新しいシステムノイズ
415
物理的ノイズの比較
411
システムノイズの比較
417
認証
419

フロントページの続き

(74)代理人 100109070
弁理士 須田 洋之
(74)代理人 100109335
弁理士 上杉 浩
(74)代理人 100120525
弁理士 近藤 直樹
(72)発明者 チャネス パトリック
スイス ツェーハー１４６８ シェル ルート ディヴェルドン レ バン ４０５
(72)発明者 フラデット エルワン
スイス ツェーハー１０９１ グランヴォー シュマン デュ グラブ 3アー

審査官 青木 重徳

(56)参考文献 特表２００８－５１５７４１（ＪＰ，Ａ）
特開２００３－１９８５２８（ＪＰ，Ａ）
特表２００８－５４５２８２（ＪＰ，Ａ）
特開２０００－１４８９５０（ＪＰ，Ａ）
特表２００７－５０７１２０（ＪＰ，Ａ）
特表２００６－５２４０１１（ＪＰ，Ａ）
特表２００８－５４１２６０（ＪＰ，Ａ）
国際公開第２０１２／０４０４８１（WO，Ａ1）
欧州特許出願公開第０２４７２４５１（ＥＰ，Ａ1）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ 9／３２
Ｈ０４Ｌ 9／０８