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

特許第5137552号
(P5137552)

(45)発行日　平成25年2月6日(2013.2.6)　(24)登録日　平成24年11月22日(2012.11.22)

(51)Int.Cl.		F I		
G06Q 50/10	(2012.01)	G06F	17/60	118
G06Q 10/00	(2012.01)	G06F	17/60	512
G06K 17/00	(2006.01)	G06K	17/00	F
G06K 19/07	(2006.01)	G06K	17/00	L
G06K 19/00	(2006.01)	G06K	17/00	T

請求項の数 4　(全 16 頁)　最終頁に続く

(21)出願番号　特願2007-322094 (P2007-322094)
(22)出願日　平成19年12月13日 (2007.12.13)
(65)公開番号　特開2008-217761 (P2008-217761A)
(43)公開日　平成20年9月18日 (2008.9.18)
審査請求日　平成19年12月13日 (2007.12.13)
審判番号　不服2011-13091 (P2011-13091/J1)
審判請求日　平成23年6月20日 (2011.6.20)
(31)優先権主張番号　10-2007-0020602
(32)優先日　平成19年2月28日 (2007.2.28)
(33)優先権主張国　韓国 (KR)

(73)特許権者　505176556
コリア　ユニバーシティ　インダストリアル　アンド　アカデミック　コラボレイション　ファウンデーション
大韓民国，ソウル　１３６－７０１，ソンブク－ク，アナム－ドン，５－カ，１，コリア　ユニバーシティ内
(74)代理人　110000338
特許業務法人原謙三国際特許事務所
(72)発明者　ドン　フン，イ
大韓民国，４１０－３１４，キョンギ－ド，コヤン－シ，イルサンドン－グ，チョンバルサン－ドン，バムガシ　マウル，＃９０１－２０１

最終頁に続く

(54)【発明の名称】無線識別システムを利用した陳列された品物の情報確認方法、無線識別システムを利用した購買された品物の情報確認方法、その記録媒体及びそのシステム

(57)【特許請求の範囲】
【請求項１】
売場内に進入したユーザーのモバイルリーダーに、前記売場内のローカルサーバーがＯＩＳサーバーの位置情報と認証用の値とを含んだ認証書を伝送する段階と、
品物に付着されたタグが、前記モバイルリーダーから前記品物のＩＤを要請される段階と、
前記ＩＤの要請を受信したタグが、前記タグのＩＤを前記認証用の値に暗号化した情報を前記モバイルリーダーに伝送する段階と、
前記認証書内の位置情報によるＯＩＳサーバーが、前記タグのＩＤを暗号化した情報及び前記認証用の値を前記モバイルリーダーから受信する段階と、
前記ＯＩＳサーバーに前記モバイルリーダーから受信した前記認証用の値がデータベースに存在すれば、前記ＯＩＳサーバーが前記タグのＩＤに該当するデータを前記データベースから検索して前記モバイルリーダーに伝送する段階と、を含む無線識別システムを利用した陳列された品物の情報確認方法であって、
前記タグのＩＤを前記認証用の値に暗号化した情報は、
ハッシュ関数及び前記タグが前記ローカルサーバーから前記モバイルリーダーを介して取得した認証用の値C_iを用いて$h_K(C_i)$を演算した後で、前記$h_K(C_i)$と前記タグのＩＤとを排他的論理和演算した値であることを特徴とする無線識別システムを利用した陳列された品物の情報確認方法。
【請求項２】

前記ＯＩＳサーバーは、
ＥＰＣ（Ｅｌｅｃｔｒｏｎｉｃ　Ｐｒｏｄｕｃｔ　Ｃｏｄｅ）に該当する情報を貯蔵するサーバーであることを特徴とする請求項１に記載の無線識別システムを利用した陳列された品物の情報確認方法。
【請求項３】
モバイルリーダーで無線識別システムを利用した陳列された品物の情報確認方法において、
売場内に進入した前記モバイルリーダーが、ＯＩＳサーバーの位置情報と認証用の値とを含んだ認証書を前記売場内のローカルサーバーから受信する段階と、
品物に付着されたタグに前記品物のＩＤを要請する段階と、
前記タグのＩＤを前記認証用の値に暗号化した情報を前記タグから受信する段階と、
前記タグのＩＤを暗号化した情報及び前記認証用の値を前記認証書内の位置情報によるＯＩＳサーバーに伝送する段階と、
前記タグのＩＤに該当するデータを前記ＯＩＳサーバーから受信する段階と、を含む無線識別システムを利用した陳列された品物の情報確認方法であって、
前記タグのＩＤを前記認証用の値に暗号化した情報は、
ハッシュ関数及び前記タグが前記ローカルサーバーから前記モバイルリーダーを介して取得した認証用の値C_iを用いて$h_K(C_i)$を演算した後で、前記$h_K(C_i)$と前記タグのＩＤとを排他的論理和演算した値であることを特徴とする無線識別システムを利用した陳列された品物の情報確認方法。
【請求項４】
ＯＩＳサーバーの位置情報と認証用の値とを含んだ認証書をローカルサーバーから売場内で受信し、ユーザーが売場に陳列された品物についての情報を要請すれば、タグに品物のＩＤを要請し、前記タグのＩＤを暗号化した情報及び前記認証用の値を前記認証書内の位置情報によるＯＩＳサーバーに伝送するモバイルリーダーと、
前記モバイルリーダーから前記ＩＤの要請を受信すれば、前記認証用の値にタグのＩＤを暗号化した情報を前記モバイルリーダーに伝送する品物に付着されたタグと、
前記モバイルリーダーから受信した認証用の値がデータベースに存在すれば、前記タグのＩＤに該当するデータを前記データベースから検索して前記モバイルリーダーに伝送するＯＩＳサーバーと、
前記ＯＩＳサーバーの位置情報と前記認証用の値とを含んだ認証書を貯蔵するローカルサーバーと、を含み、
前記タグのＩＤを前記認証用の値に暗号化した情報は、
ハッシュ関数及び前記タグが前記ローカルサーバーから前記モバイルリーダーを介して取得した認証用の値C_iを用いて$h_K(C_i)$を演算した後で、前記$h_K(C_i)$と前記タグのＩＤとを排他的論理和演算した値であることを特徴とする無線識別システムを利用した陳列された品物の情報確認システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、無線周波数認識（ＲＦＩＤ：Ｒａｄｉｏ　Ｆｒｅｑｕｅｎｃｙ　ＩＤｅｎｔｉｆｉｃａｔｉｏｎ、以下‘ＲＦＩＤ’と称する）システムに係り、特に、無線識別システムを利用した陳列された品物の情報確認方法、無線識別システムを利用した購買された品物の情報確認方法、その記録媒体及びそのシステムに関する。
【背景技術】
【０００２】
無線識別（Ｒａｄｉｏ　Ｆｒｅｑｕｅｎｃｙ　Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ、ＲＦＩＤ）システムは、ＲＦ通信を用いて遠距離から個体の情報を読み取る自動認識技術である。このシステムは、物理的な接触なしにも事物の情報を迅速に読み取り可能なので、バーコードシステムを取り替えるシステムとして注目されている。最近、このシステムは、物

流システム、交通管理システム、動物管理システムなどで部分的に使われている。
【０００３】
現在、類似したサービスとして２Ｄバーコードを利用したチケットサービスがあるが、認識距離が非常に短くてユーザーがサービスを利用する時、非常に不便な短所がある。
【０００４】
ＲＦＩＤリーダー（以下“リーダー”と称する）が、ＲＦＩＤタグ（以下“タグ”と称する）に質疑（ｑｕｅｒｙ）を送れば、タグは自身の情報をリーダーに伝送し、その情報はデータベースに伝送される。このような方式でサービス供給者は、タグを有している消費者の情報をいつでもどこでも容易に得ることができ、そのような消費者にいろいろ便利なサービスを提供する。しかし、タグとリーダーは、公開されたチャンネル（ｉｎｓｅｃｕｒｅ　ｃｈａｎｎｅｌ）で通信するために、攻撃者は伝送されるメッセージを盗聴することができ、このメッセージを用いて信用情報、購買パターン、健康情報のような消費者の敏感な情報が露出されうる。また、攻撃者は、このメッセージを分析することによって、タグを有している消費者の位置を追跡することができる。
【０００５】
モバイルリーダーが、タグ付き品物の情報を確認する時、購買前には誰も品物の情報を確認しなければならないが、品物を購買した後には状況が異なる。
【０００６】
従来のタグ付き品物の情報を確認する方法は、品物を購買した後には購買者が有した品物の情報を誰も確認できて購買者の品物についての情報流出、ユーザー追跡可能性のようなユーザーのプライバシー侵害が発生することができ、何らの保安認証もなしに品物の固有番号（ＥＰＣ）を伝達するために、品物の固有番号（ＥＰＣ）が分かった攻撃者は容易にタグを偽造することができるという問題点がある。
【発明の開示】
【発明が解決しようとする課題】
【０００７】
本発明が果そうとする一番目の技術的課題は、品物の購買前の商品情報に対する信頼性を保障し、購買前にタグについての情報流出を防止することができ、タグの偽造を防止し、演算の効率性を向上させうる無線識別システムを利用した陳列された品物の情報確認方法を提供することである。
【０００８】
本発明が果そうとする二番目の技術的課題は、品物の購買後にタグについての情報流出を防止することができ、購買された品物に対するタグのＩＤを追跡不能にしてプライバシーを保護し、タグの偽造を防止し、演算の効率性を向上させうる無線識別システムを利用した購買された品物の情報確認方法を提供することである。
【０００９】
本発明が果そうとする三番目の技術的課題は、前記の無線識別システムを利用した陳列された品物の情報確認方法及び無線識別システムを利用した購買された品物の情報確認方法をコンピュータで実行させるためのプログラムを記録したコンピュータで読み取り可能な記録媒体を提供することである。
【００１０】
本発明が果そうとする四番目の技術的課題は、前記の無線識別システムを利用した陳列された品物の情報確認方法が適用された無線識別システムを利用した陳列された品物の情報確認システムを提供することである。
【００１１】
本発明が果そうとする五番目の技術的課題は、前記の無線識別システムを利用した購買された品物の情報確認方法が適用された無線識別システムを利用した購買された品物の情報確認システムを提供することである。
【課題を解決するための手段】
【００１２】

前記の目的を果たすための本発明の一態様による無線識別システムを利用した陳列された品物の情報確認方法は、ユーザーのモバイルリーダーが売場内に進入すれば、前記売場内のローカルサーバーがＯＩＳサーバーの位置情報と認証用の値とを含んだ認証書を前記モバイルリーダーに伝送する段階と、品物に付着されたタグが、前記モバイルリーダーから前記品物のＩＤを要請される段階と、前記ＩＤの要請を受信したタグが、前記タグのＩＤを前記認証用の値に暗号化した情報を前記モバイルリーダーに伝送する段階と、前記認証書内の位置情報によるＯＩＳサーバーが、前記タグのＩＤを暗号化した情報及び前記認証用の値を前記モバイルリーダーから受信する段階と、前記ＯＩＳサーバーに前記モバイルリーダーから受信した前記認証用の値がデータベースに存在すれば、前記ＯＩＳサーバーが前記タグのＩＤに該当するデータを前記データベースから検索して前記モバイルリーダーに伝送する段階と、を含んでなる。

【００１３】

前記の目的を果たすための本発明の他の態様によるモバイルリーダーで無線識別システムを利用した陳列された品物の情報確認方法は、前記モバイルリーダーが売場内に進入すれば、ＯＩＳサーバーの位置情報と認証用の値とを含んだ認証書を前記売場内のローカルサーバーから受信する段階と、品物に付着されたタグに前記品物のＩＤを要請する段階と、前記タグのＩＤを前記認証用の値に暗号化した情報を前記タグから受信する段階と、前記タグのＩＤを暗号化した情報及び前記認証用の値を前記認証書内の位置情報によるＯＩＳサーバーに伝送する段階と、前記タグのＩＤに該当するデータを前記ＯＩＳサーバーから受信する段階と、を含んでなる。

【００１４】

前記の目的を果たすための本発明のまた他の態様による無線識別システムを利用した購買された品物の情報確認方法は、タグ付き品物が購買されれば、モバイルリーダーがＯＩＳサーバーから前記品物に対するキーを受信する段階と、前記モバイルリーダーで生成された第１乱数を前記タグにデータを要請する信号とともに伝送する段階と、前記タグが前記タグのＩＤを前記タグで生成された第２乱数に暗号化した第１値及び前記第２乱数を前記タグのキーに暗号化した第２値を前記モバイルリーダーに伝送する段階と、前記モバイルリーダーが貯蔵するキーを用いて前記第２値から前記第２乱数を抽出し、前記第２乱数を用いて第１値から前記タグのＩＤを抽出する段階と、前記抽出されたＩＤの中にＥＰＣの構造を有するＩＤを前記ＯＩＳサーバーに伝送すれば、前記ＯＩＳサーバーが受信したＩＤに該当するデータを前記モバイルリーダーに伝送する段階と、を含んでなる。

【００１５】

前記の目的を果たすための本発明のさらに他の態様によるモバイルリーダーで無線識別システムを利用した購買された品物の情報確認方法は、タグ付き品物が購買されれば、ＯＩＳサーバーから前記品物に対するキーを受信する段階と、第１乱数を生成させ、前記第１乱数を前記タグにデータを要請する信号とともに伝送する段階と、前記タグのＩＤを第２乱数に暗号化した第１値と、前記第２乱数を前記タグのキーに暗号化した第２値とを前記タグから受信する段階と、前記モバイルリーダーに貯蔵されたキーを用いて前記第２値から前記第２乱数を抽出し、前記第２乱数を用いて前記第１値から前記タグのＩＤを抽出する段階と、前記抽出されたＩＤの中にＥＰＣの構造を有するＩＤを前記ＯＩＳサーバーに伝送する段階と、前記ＯＩＳサーバーに伝送された前記ＩＤに該当するデータを前記ＯＩＳサーバーから受信する段階と、を含んでなる。

【００１６】

前記の目的を果たすための本発明のさらに他の態様による無線識別システムを利用した陳列された品物の情報確認システムは、売場内に進入すれば、ＯＩＳサーバーの位置情報と認証用の値とを含んだ認証書をローカルサーバーから受信し、ユーザーが売場に陳列された品物についての情報を要請すれば、タグに品物のＩＤを要請し、前記タグのＩＤを暗号化した情報及び前記認証用の値を前記認証書内の位置情報によるＯＩＳサーバーに伝送するモバイルリーダーと、前記モバイルリーダーから前記ＩＤの要請を受信すれば、前記認証用の値にタグのＩＤを暗号化した情報を前記モバイルリーダーに伝送する品物に付着

されたタグと、前記モバイルリーダーから受信した認証用の値がデータベースに存在すれば、前記タグのＩＤに該当するデータを前記データベースから検索して前記モバイルリーダーに伝送するＯＩＳサーバーと、前記ＯＩＳサーバーの位置情報と前記認証用の値とを含んだ認証書を貯蔵するローカルサーバーと、を含んでなる。

【００１７】

前記の目的を果たすための本発明のさらに他の態様による無線識別システムを利用した購買された品物の情報確認システムは、任意の第２乱数を生成させ、タグのＩＤを前記第２乱数に暗号化した第１値及び前記第２乱数をタグのキーに暗号化した第２値をモバイルリーダーに伝送する品物に付着されたタグと、ユーザーが前記タグ付き品物を購買すれば、ＯＩＳサーバーから前記品物に対するキーを受信し、任意の第１乱数を生成させて前記タグにデータを要請する信号とともに伝送し、貯蔵するキーを用いて前記第２値から前記第２乱数を抽出し、前記第２乱数を用いて第１値から前記タグのＩＤを抽出するモバイルリーダーと、前記モバイルリーダーで抽出されたＩＤの中にＥＰＣの構造を有するＩＤを受信すれば、前記受信したＩＤに該当するデータを前記モバイルリーダーに伝送するＯＩＳサーバーと、を含んでなる。

【発明の効果】

【００１８】

本発明によれば、タグ付き品物の購買前の商品情報に対する信頼性を保障し、購買前後にタグについての情報流出を防止することができ、購買された品物に対するタグのＩＤを追跡不能にしてプライバシーを保護し、タグの偽造を防止し、演算の効率性を向上させうる。

【発明を実施するための最良の形態】

【００１９】

本発明は、モバイルＲＦＩＤシステム環境での品物購買前に品物についての信頼性ある情報を確認することができ、品物を購買後には信頼性ある品物の情報を確認すると同時にユーザーのプライバシーを保護することに関する。

【００２０】

本発明は、モバイルＲＦＩＤシステム環境でユーザーが品物を購買する前と購買した後とに品物の情報を獲得する方法である。本発明によれば、購買する前には、品物の製造会社で発行した認証書を通じて信頼性ある情報を獲得して本物であることを識別する。購買後には、品物の購買者以外には品物の情報を読み取らないようにしてユーザーのプライバシー侵害を予防する。

【００２１】

モバイルＲＦＩＤシステムでは、タグの固有情報をＥＰＣ（Ｅｌｅｃｔｒｏｎｉｃ　Ｐｒｏｄｕｃｔ　Ｃｏｄｅ）構造で貯蔵する。ＥＰＣは、ヘッダ（Ｈｅａｄｅｒ）、ＥＰＣ管理者（ＥＰＣ　Ｍａｎａｇｅｒ）、商品分類番号（Ｏｂｊｅｃｔ　Ｃｌａｓｓ）、一連番号（Ｓｅｒｉａｌ　Ｎｕｍｂｅｒ）に図１Ａの構造を有する。

【００２２】

各項目に対する内容は、表１のようである。

【００２３】

【表１】

項目	内容
ヘッダ (8bit)	ﾃﾞｰﾀ類型及び長さを定義
EPC管理者 (28bit)	商品に対する分類と一連番号を管理する機関や企業を表示
商品分類番号 (24bit)	ﾊﾞｰｺｰﾄﾞの商品品目ｺｰﾄﾞに該当するものであって,各品目または単位を表示
一連番号 (36bit)	各商品に対して付与される固有の識別番号

【００２４】

表２は、以下で使われる記号の定義を表わしたものである。

【００２５】

【表２】

記号	定義
$request_p$	商品を購買する前に,売場内でﾓﾊﾞｲﾙﾘｰﾀﾞｰがﾀｸﾞからIDを読み取る時に使う要請信号
$request_c$	商品の購買後,ﾀｸﾞからPID,KIDを受信するための要請信号
ID	ﾀｸﾞのEPC
K	ﾀｸﾞのｷｰ(Key)値
K_j	ﾓﾊﾞｲﾙﾘｰﾀﾞｰが所有したｷｰ
r_i	ﾓﾊﾞｲﾙﾘｰﾀﾞｰの乱数生成器(PRNG)で生成したﾗﾝﾀﾞﾑ値
r_T	ﾀｸﾞが生成したﾗﾝﾀﾞﾑ値
h_K ( )	鍵付きﾊｯｼｭ(keyed hash function)
CerTficate(C_i)	商品についての信頼性ある情報を確認するのに使われる認証書で認証用の値(C),EPCに該当する情報を有しているｻｰﾊﾞｰの位置情報含む
$list_c$	認証用の値のﾘｽﾄ
$\oplus$	exclusive－OR

【００２６】

このとき、ｉ、ｊは、任意のインデックスである。一方、以下では、ＮＩＤは、品物購買前の品物の暗号化されたＩＤ情報、ＰＩＤは、品物購買後の品物の暗号化されたＩＤ情報を表わす。

【００２７】

以下では、図面を参照して、本発明の望ましい実施形態を説明する。しかし、次に例示する本発明の実施形態は、多様な他の形態に変形されることができ、本発明の範囲が次に詳述する実施形態に限定されるものではない。

【００２８】
図１Ｂは、本発明による無線識別システムを利用した陳列された品物の情報確認システムのブロック図である。また、図１Ｂは、本発明による無線識別システムを利用した購買された品物の情報確認システムのブロック図である。
【００２９】
タグ（Ｔａｇ）１１０は、モバイルリーダー１２０から質疑を受けて商品についての固有情報（ＥＰＣ）をＲＦ信号を用いて伝送する。タグ１１０は、ＲＦ通信のためのアンテナと演算と固有情報とを貯蔵するマイクロチップで構成される。タグ１１０は、電力供給方法によって能動型タグ（Ａｃｔｉｖｅ Ｔａｇ）と受動型タグ（Ｐａｓｓｉｖｅ Ｔａｇ）とに区分される。
【００３０】
受動型タグ（Ｐａｓｓｉｖｅ Ｔａｇ）は、モバイルリーダーから受けたＲＦ信号から電力を供給されて動作する。近距離通信が可能で複雑な演算を実行しにくい。受動型タグは、能動型タグとは異なってバッテリーを内蔵していなくて寿命が半永久的であり、能動型タグに比べて安値である。本発明に使われるタグは、ＥＰＣ ｇｌｏｂａｌ Ｃｌａｓｓ１Ｇｅｎｅｒａｔｉｏｎ２の標準でＰＲＮＧ（Ｐｓｅｕｄｏ Ｒａｎｄｏｍ Ｎｕｍｂｅｒ Ｇｅｎｅｒａｔｏｒ）がタグ内に含まれうる。本発明に使われるタグは、擬似乱数を生成させるように構成されうる。
【００３１】
能動型タグ（Ａｃｔｉｖｅ Ｔａｇ）は、タグ自体に内蔵されているバッテリーを通じて電力を供給される。リーダーと遠距離通信が可能であるが、バッテリーが内蔵されていて高価でバッテリーが全部消耗されれば、タグの使用が不可能である。
【００３２】
モバイルリーダー（Ｍｏｂｉｌｅ Ｒｅａｄｅｒ）１２０は、ＲＦＩＤシステムのリーダーをモバイル機器に内蔵したものである。タグ１１０に質疑を伝送し、タグ１１０から伝送されたデータを認識するか、タグ１１０に新たな情報をまた書き込む役割を果たす。
【００３３】
ネットワークサーバー（Ｎｅｔｗｏｒｋ Ｓｅｒｖｅｒ）のうちＯＩＳサーバー（Ｏｂｊｅｃｔ Ｉｎｆｏｒｍａｔｉｏｎ Ｓｅｒｖｉｃｅ Ｓｅｒｖｅｒ）１３０は、タグ１１０のＥＰＣとマッチングされるコンテンツ（Ｃｏｎｔｅｎｔ）を貯蔵しており、コンテンツの要請がある時にコンテンツを提供する。
【００３４】
ネットワークサーバーのうちＯＮＳサーバー１４０は、ＤＮＳサーバー（Ｄｏｍａｉｎ Ｎａｍｅ Ｓｅｒｖｉｃｅ Ｓｅｒｖｅｒ）と類似している形態に該当ＥＰＣの情報を有しているサーバーのＵＲＬ（Ｕｎｉｆｏｒｍ Ｒｅｓｏｕｒｃｅ Ｌｏｃａｔｉｏｎ）を知らせる役割を果たす。
【００３５】
図１Ｂと関連して、本発明による無線識別システムを利用した陳列された品物の情報確認システムを説明すれば、次のようである。
【００３６】
モバイルリーダー１２０は、売場内に進入すれば、ＯＩＳサーバー１３０の位置情報と認証用の値とを含んだ認証書をローカルサーバー１５０から受信する。また、モバイルリーダー１２０は、ユーザーが売場に陳列された品物についての情報を要請すれば、タグ１１０に品物のＩＤを要請し、タグ１１０のＩＤを暗号化した情報及び認証用の値を認証書内の位置情報によるＯＩＳサーバー１３０に伝送する。
【００３７】
タグ１１０は、前述したように品物にそれぞれ付着される。タグ１１０は、モバイルリーダー１２０からＩＤの要請を受信すれば、モバイルリーダー１２０から受信した認証用の値にタグ１１０のＩＤを暗号化した情報をモバイルリーダー１２０に伝送する。
【００３８】

ＯＩＳサーバー１３０は、モバイルリーダー１２０から受信した認証用の値がデータベースに存在すれば、タグ１１０のＩＤに該当するデータをＯＩＳサーバー１３０のデータベースから検索してモバイルリーダー１２０に伝送する。

【００３９】

ローカルサーバー１５０は、ＯＩＳサーバー１３０の位置情報と認証用の値とを含んだ認証書を貯蔵する。

【００４０】

図１Ｂと関連して、本発明による無線識別システムを利用した購買された品物の情報確認システムを説明すれば、次のようである。

【００４１】

タグ１１０は、前述したように品物にそれぞれ付着される。タグ１１０は、任意の第２乱数を生成させ、タグのＩＤを第２乱数に暗号化した第１値を演算する。また、タグ１１０は、第２乱数をタグのキーに暗号化した第２値と第１値とをモバイルリーダー１２０に伝送する。

【００４２】

モバイルリーダー１２０は、ユーザーがタグ１１０付き品物を購買すれば、ＯＩＳサーバー１３０から品物に対するキーを受信する。モバイルリーダー１２０は、ＯＩＳサーバー１３０から受信して累積されたキーを購買品物リストに利用できる。モバイルリーダー１２０は、購買された品物についての情報要請がある場合、任意の第１乱数をタグ１１０にデータを要請する信号とともに伝送する。以後に、モバイルリーダー１２０は、タグ１１０から第１値及び第２値を受信して貯蔵するキー（ＯＩＳサーバー１３０から受信して累積されたキー）を用いて第２値から第２乱数を抽出し、第２乱数を用いて第１値からタグのＩＤを抽出する。

【００４３】

望ましくは、モバイルリーダー１２０は、抽出されたＩＤの中でＥＰＣの構造を有したＩＤをＯＮＳサーバー１４０に伝送し、ＯＮＳサーバー１４０から受信したＯＩＳサーバー１３０のＵＲＬ及び確認されたＩＤを用いてＯＩＳサーバー１３０にＥＰＣに対するデータを要請するように構成されうる。このとき、ＯＮＳサーバー１４０は、モバイルリーダー１２０から受信されたＩＤを確認し、該確認されたＩＤに対して当該データを所有したＯＩＳサーバーのＵＲＬをモバイルリーダーに伝送する。

【００４４】

ＯＩＳサーバー１３０は、モバイルリーダー１２０で抽出されたＩＤの中にＥＰＣの構造を有するＩＤを受信すれば、該受信したＩＤに該当するデータをモバイルリーダー１２０に伝送する。

【００４５】

図１Ｂによる本発明の動作順序は、品物を購買前に売場内で品物の情報を確認する過程と、品物を購買後の初期設定、品物を購買後の品物の情報をモバイルリーダーを使って得られる過程とに分けられる。

【００４６】

図２で、品物を購買する前に売場内で品物の情報を確認する過程を説明する。

【００４７】

まず、各売場のローカルサーバー２５０は、商品に対する認証用の値を含んだ認証書をＯＩＳサーバー２３０から予め受信して貯蔵する。

【００４８】

モバイルリーダー２２０を所持したユーザーが売場に入れば、モバイルリーダー２２０は、売場のローカルサーバー２５０からＥＰＣに該当する情報を有しているサーバーの位置情報と認証用の値Ｃｉとを含んだ認証書ＣｅｒＴｆｉｃａｔｅ（Ｃｉ）を受信する。

【００４９】

次に、モバイルリーダー２２０は、（ｒｅｑｕｅｓｔｐ、Ｃｉ）をタグ２１０に伝送して商品にＩＤを要請する。

【００５０】
タグ２１０は、ｈＫ（Ｃｉ）を生成させてＩＤを排他的論理和（ＸＯＲ）してＮＩＤを生成させた後、ＮＩＤをモバイルリーダーに伝送する。
【００５１】
次に、モバイルリーダー２２０は、認証書ＣｅｒＴｆｉｃａｔｅ（Ｃｉ）の内のＯＩＳサーバー２３０の位置情報を用いてタグ２１０から受信したＮＩＤとＣｉとをＯＩＳサーバー２３０に伝送する。
【００５２】
最後に、ＯＩＳサーバー２３０は、モバイルリーダー２２０が送ったＣｉ、ＮＩＤと貯蔵しているキー値Ｋとを用いてＩＤを生成させる。ＯＩＳサーバー２３０は、生成したＩＤに該当するデータＤａｔａＴをデータベースで捜す。ＯＩＳサーバー２３０は、モバイルリーダー２２０から受信したＣｉがデータベースのｌｉｓｔＣ（＝｛Ｃ｝）に属するかどうかを確認して属すれば、ＯＩＳサーバー２３０は、タグ２１０のＥＰＣに該当するデータＤａｔａＴをモバイルリーダー２２０に伝送する。
【００５３】
これにより、モバイルリーダー２２０は、ＯＩＳサーバー２３０から受信したデータＤａｔａＴで品物の情報を確認する。
【００５４】
図３で、品物を購買後にＯＩＳサーバー２３０から品物に対するキーＫを受信して貯蔵する初期設定について説明する。
【００５５】
モバイルリーダー３２０とＯＩＳサーバー３３０との間の通信は、従来に使われている安全な無線保安通信を使う。品物を購買後のユーザーは、ＯＩＳサーバー３３０から安全なチャンネルを通じて品物に対するキーＫをモバイルリーダー３２０に受信する。ユーザーは、ＯＩＳサーバー３３０から受信したキーＫをモバイルリーダー３２０に貯蔵して購買された品物情報を読み取る時に使う。モバイルリーダー３２０を所有したユーザーは、ＯＩＳサーバー３３０から受信したキーＫを使って自身のプライバシーを保護させうる。
【００５６】
図４で、品物購買後のユーザーのプライバシーを保護しながら品物の情報を確認する過程を説明する。
【００５７】
まず、モバイルリーダー４２０は、乱数生成器（ＰＲＮＧ）を用いて第１乱数ｒｉを生成させてタグ４１０にデータを要請する信号とともに伝送する（ｒｅｑｕｅｓｔＣ、ｒｉ）。
【００５８】
次に、タグ４１０は、モバイルリーダー４２０から受信したｒｉをＫとハッシュ関数とを用いてｈＫ（ｒｉ）を生成させる。タグ４１０は、第２乱数ｒＴを生成させてこれを用いて第１値ＰＩＤ、第２値ＫＩＤを生成させた後、モバイルリーダー４２０に伝送する。
【００５９】
次に、モバイルリーダー４２０は、有しているすべてのキーＫｊを用いて第２値ＫＩＤから第２乱数ｒＴを抽出し、ｒＴを用いて第１値ＰＩＤからタグ４１０のＩＤを抽出する。モバイルリーダー４２０は、抽出したタグのＩＤの中にＥＰＣの構造を有したＩＤをＯＮＳサーバー４３０に伝送する。
【００６０】
ＯＮＳサーバー（図示せず）は、ＯＮＳサーバー（図示せず）で確認されたＩＤ、すなわち、正しいＩＤに対して当該データを所有したＯＩＳサーバー４３０のＵＲＬをモバイ__ルリーダー４２０に伝送する。
【００６１】
次に、モバイルリーダー４２０は、ＯＮＳサーバー４３０から受けたＯＩＳサーバー４３０のＵＲＬを用いてＯＩＳサーバー４３０にＥＰＣに対するデータを要請する。

【００６２】
最後に、ＯＩＳサーバー４３０は、ＥＰＣに該当するデータＤａｔａＴをモバイルリーダー４２０に伝送する。
【００６３】
図５は、本発明による無線識別システムを利用した陳列された品物の情報確認方法のフローチャートである。
【００６４】
まず、ユーザーのモバイルリーダーが売場内に進入するかどうかを判断する（５１０過程）。
【００６５】
このとき、モバイルリーダーが売場内に進入すれば、ＯＩＳサーバーの位置情報と認証用の値とを含んだ認証書をモバイルリーダーが売場内のローカルサーバーから受信する（５２０過程）。一方、モバイルリーダーが売場内に進入しなければ、待機状態を維持する。
【００６６】
次に、ユーザーが売場内に陳列された品物を見て、ボタン操作やタグとリーダーの接近などの方法で特定品物についての情報をモバイルリーダーに要請するかどうかを判断する（５３０過程）。このとき、ユーザーが品物についての情報を要請すれば、モバイルリーダーが品物に付着されたタグに品物のＩＤを要請し（５４０過程）、そうでなければ待機状態を維持する。
【００６７】
また、タグに品物のＩＤを要請した場合、ＩＤの要請を受信したタグがタグのＩＤを認証用の値に暗号化した情報をモバイルリーダーに伝送する（５４０過程）。
【００６８】
次に、モバイルリーダーがタグのＩＤを暗号化した情報及び認証用の値をＯＩＳサーバーに伝送する（５５０過程）。このとき、ＯＩＳサーバーは、認証書内の位置情報によるサーバーである。
【００６９】
次に、ＯＩＳサーバーでモバイルリーダーから受信した認証用の値がデータベースに存在するかどうかを判断する（５６０過程）。
【００７０】
このとき、認証用の値がデータベースに存在すれば、タグのＩＤに該当するデータをデータベースから検索してモバイルリーダーに伝送する（５７０過程）。一方、モバイルリーダーから受信した認証用の値がデータベースに存在しなければ、すべての過程を終了する。
【００７１】
図６は、本発明によって品物を購買した場合の初期設定過程のフローチャートである。まず、タグ付き品物を購買するかどうかを判断する（６１０過程）。このとき、品物を購買しなければ、待機状態を維持する。
【００７２】
次に、品物を購買すれば、モバイルリーダーがＯＩＳサーバーから購買された品物に対するキーを受信して貯蔵する（６２０過程）。これにより、モバイルリーダーには、購買品物リストを生成させるためのキーが収集される。
【００７３】
図７は、本発明による無線識別システムを利用した購買された品物の情報確認方法のフローチャートである。
【００７４】
まず、ユーザーが購買品物についての情報を要請するかどうかを判断する（７３０過程）。この過程（７３０）は、ユーザーがモバイルリーダーのボタンを操作するなどがある場合、購買品物についての情報を要請があると判断する過程であり得る。

【００７５】
次に、モバイルリーダーで生成された第１乱数をタグにデータを要請する信号とともに伝送する（７４０過程）。
【００７６】
次に、タグがタグのＩＤを第２乱数に暗号化した第１値及び第２乱数をタグのキーに暗号化した第２値をモバイルリーダーに伝送する（７５０過程）。このとき、第２乱数は、タグで生成された乱数値である。
【００７７】
次に、モバイルリーダーが貯蔵するキーを用いて第２値から第２乱数を抽出し、第２乱数を用いて第１値からタグのＩＤを抽出する（７６０過程）。
【００７８】
最後に、抽出されたＩＤの中にＥＰＣの構造を有するＩＤをＯＩＳサーバーに伝送すれば、ＯＩＳサーバーが受信したＩＤに該当するデータをモバイルリーダーに伝送する（７７０過程）。望ましくは、この過程（７７０過程）は、モバイルリーダーがＯＩＳサーバーから受信されたデータを用いて購買された品物に関する情報をモバイルリーダーの画面に表示する過程を含みうる。
【００７９】
本発明は、モバイルＲＦＩＤシステム環境で購買前には、品物の製造会社で発行した認証書を基盤で品物についての正確で信頼性ある情報を獲得することができ、品物購買後には、安全で効率的にユーザーのプライバシーを保護する方法を提供する。
【００８０】
本発明は、購買前の商品情報に対する信頼性を提供する。本発明では、商品の企業で発行する認証書を売場のローカルサーバーが所有してユーザーのモバイルリーダーに与える。モバイルリーダーは、ローカルサーバーから受けた認証書の認証用の値Ｃｉと商品の情報を有したサーバーの位置情報とを用いて商品の情報を得られるようになって商品の情報に対する信頼性を保障される。
【００８１】
本発明は、情報の流出を防止する。本発明は、タグが自身のＩＤ（ＥＰＣ）ではないＩＤを含んだランダムな値をモバイルリーダーに応答する。購買前には、Ｃｉの鍵付きハッシュ関数でＩＤを隠してＮＩＤを伝送し、購買後には、モバイルリーダーとタグが生成したランダム値と鍵付きハッシュ値でＩＤを隠してＰＩＤを伝送する。攻撃者は、ＮＩＤ、ＰＩＤのみではユーザーが所持した商品に対するＩＤが分からず、また情報も分からない。
【００８２】
本発明は、追跡不可能性を提供する。この特性は、ユーザーが商品を購買した後に必ず提供されなければならない特性である。本発明では、ユーザーが商品を購買後にはタグの固有のキーを受けてモバイルリーダーで管理する。タグの固有のキーと鍵付きハッシュ関数とを使ってタグがモバイルリーダーの応答に常に異なる値ＰＩＤ、ＫＩＤで応答するようにしてキーが分からないユーザーはタグのＩＤが分からなくなる。具体的に説明すれば、モバイルリーダーの要請によってタグは、ＰＩＤ、ＫＩＤを常に異なる値で伝送するために特定商品に対して追跡が不可能であるのでユーザーを追跡することができない。
【００８３】
従来の無線識別システムでは、タグのＲＦＩＤコード情報が携帯電話に暗号化過程なしに伝送されてユーザーの追跡性に対するプライバシーが保護されない。そして、政策サーバーを使うために、政策サーバーが攻撃されたらすべてのシステムが安全ではなくなる。本発明では、タグの固有コードがランダム値に隠されて他のユーザーが分からない。そして、外部サーバーのなしにも安全で効率的にユーザーのプライバシーを保護する。
【００８４】
本発明は、従来の発明と異なってモバイル機器をリーダーとして使ってタグの情報を追加的な装備が必要せずに安全に伝送が可能でユーザーのプライバシー侵害問題を予防する

。外部のサーバーを利用しなくてもユーザーが購買した品物を管理することができ、他のユーザーによって品物の情報が流出されてプライバシーが侵害されることを予防できる。

【００８５】

本発明は、タグの偽造を不可能にする。本発明では、商品を購買後にモバイルリーダーが所有したタグの固有キーＫを通じて偽造攻撃に安全である。第三者（攻撃者）がスプーフィング攻撃や再伝送攻撃でリーダーとタグと間の通信を盗聴して情報ＰＩＤ、ＫＩＤを得てもタグの固有キーＫが分からなければ、毎セッションのランダム値ｒｉに対するｈＫ（ｒｉ）が分からないためにタグの情報が露出されない。

【００８６】

一方、従来のＭＡＲＰ技法は、プロキシをＲＦＩＤシステムに使ってユーザーのプライバシー問題と保安問題とを保安する。この方法は、タグとモバイル（ＭＲＡＰ）、モバイル（ＭＡＲＰ）とリーダー、リーダーとデータベースと間にランダムな値を取り交わすことによって、従来にＲＦＩＤシステムで発生したプライバシー侵害問題と保安問題とを解決する。

【００８７】

しかし、ＭＡＲＰは、追加的なプロキシが必要であり、タグとリーダーと間の通信を全部感知しなければならない。そして、安全な通信のために使うリーダー、タグ、サーバー、プロキシのキーを管理する公開キーセンターが必要である。本発明では、モバイル機器がＲＦＩＤリーダーの役割をして追加的な装備が必要ではなく公開キーセンターのような外部サーバーやセンターが必要なしにも効率的にユーザーのプライバシー問題と保安問題とを解決する。

【００８８】

表３は、従来のＭＡＲＰと本発明の効率性とを比べた表である。

【００８９】

【表３】

プロトコル		MARP技法	提案技法
貯蔵空間	ﾀｸﾞ	3l	2l
	ﾓﾊﾞｲﾙﾘｰﾀﾞｰ	7l	1l
	ﾃﾞｰﾀﾍﾞｰｽ	5l	2l
計算量	ﾀｸﾞ	2H+3X	1H+1X(購買前) 1H+2X(購買後)
	ﾓﾊﾞｲﾙﾘｰﾀﾞｰ	(3E+1D+2V+2S+1H+1X)*M	-(購買前) (1H+2X)*N(購買後)
	ﾃﾞｰﾀﾍﾞｰｽ	1E+3D+2V+1S+2H+1X	1H+1X(購買前) -(購買後)

【００９０】

表３で、ｌはハッシュ関数の出力長やキー長またはＩＤ長、Ｈは一回のハッシュ演算、ＸはＸＯＲビット演算、Ｅは一回の暗号化演算、Ｄは一回の復号化演算、Ｖは一回の署名検証演算、Ｓは一回の署名演算、ＭはＭＡＲＰが感知できる領域内に存在するタグの数、Ｎはモバイルリーダーが所有したキーの数、“－”の表示は考慮事項ないということを表わす。

【００９１】

表３を参考にすれば、本発明が、従来のＭＡＲＰ技法より効率的であるということが分かる。

【００９２】

望ましくは、本発明の無線識別システムを利用した陳列された品物の情報確認方法をコンピュータで実行させるためのプログラムをコンピュータで読み取り可能な記録媒体に記録して提供できる。

【００９３】

望ましくは、本発明の無線識別システムを利用した購買された品物の情報確認方法をコンピュータで実行させるためのプログラムをコンピュータで読み取り可能な記録媒体に記録して提供できる。

【００９４】

本発明は、ソフトウェアを通じて実行可能である。ソフトウェアで実行される時、本発明の構成手段は、必要な作業を行うコードセグメントである。プログラムまたはコードセグメントは、プロセッサ判読可能媒体に貯蔵されるか伝送媒体または通信網で搬送波と結合されたコンピュータデータ信号によって伝送されうる。

【００９５】

コンピュータで読み取り可能な記録媒体は、コンピュータシステムによって読み取れるデータが貯蔵されるあらゆる種類の記録装置を含む。コンピュータで読み取り可能な記録装置の例としては、ＲＯＭ、ＲＡＭ、ＣＤ－ＲＯＭ、ＤＶＤ±ＲＯＭ、ＤＶＤ－ＲＡＭ、磁気テープ、フロッピー（登録商標）ディスク、ハードディスク（ｈａｒｄ　ｄｉｓｋ）、光データ貯蔵装置などがある。また、コンピュータで読み取り可能な記録媒体は、ネットワークで連結されたコンピュータ装置に分散され、分散方式でコンピュータで読み取り可能なコードが貯蔵されて実行可能である。

【００９６】

本発明は、図面に図示された一実施形態を参考にして説明したが、これは例示的なものに過ぎず、当業者ならば、これより多様な変形及び実施形態が可能であるという点を理解できるであろう。しかし、このような変形は、本発明の技術的保護範囲内にあると思わなければならない。したがって、本発明の真の技術的保護範囲は、特許請求の範囲の技術的思想によって決まるべきである。

【産業上の利用可能性】

【００９７】

無線識別システムを利用した陳列された品物の情報確認方法、無線識別システムを利用した購買された品物の情報確認方法、その記録媒体及びそのシステムに関連する技術分野に適用可能である。

【図面の簡単な説明】

【００９８】

【図１Ａ】本発明に適用されるＥＰＣの構造の一例を図示したものである。

【図１Ｂ】本発明が動作するモバイルＲＦＩＤネットワーク環境を図示したものである。

【図２】図１Ｂで品物を購買する前にモバイルリーダー１２０を用いて信頼性あるように品物の情報を獲得する過程を図示したものである。

【図３】図１Ｂで品物を購買した後にモバイルリーダー１２０で品物に対するキーを受信して貯蔵する過程を図示したものである。

【図４】図１Ｂで品物を購買した後にモバイルリーダー１２０を用いてプライバシーを保護しながら品物の情報を獲得する過程を図示したものである。

【図５】本発明による無線識別システムを利用した陳列された品物の情報確認方法のフローチャートである。

【図６】本発明によって品物を購買した場合の初期設定過程のフローチャートである。

【図７】本発明による無線識別システムを利用した購買された品物の情報確認方法のフローチャートである。

【符号の説明】

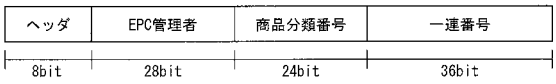
【００９９】

１１０　タグ

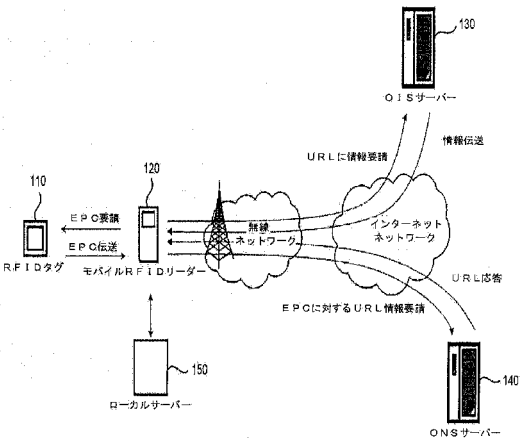
１２０　モバイルリーダー

１３０　ＯＩＳサーバー
１４０　ＯＮＳサーバー
１５０　ローカルサーバー
２１０　タグ
２２０　モバイルリーダー
２３０　ＯＩＳサーバー
２５０　ローカルサーバー
３１０　タグ
３２０　モバイルリーダー
３３０　ＯＩＳサーバー
４１０　タグ
４２０　モバイルリーダー
４３０　ＯＩＳサーバー

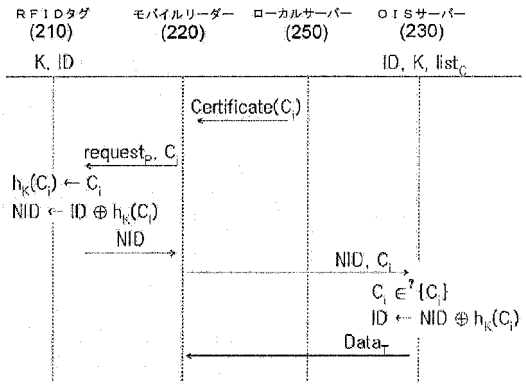
【図１Ａ】



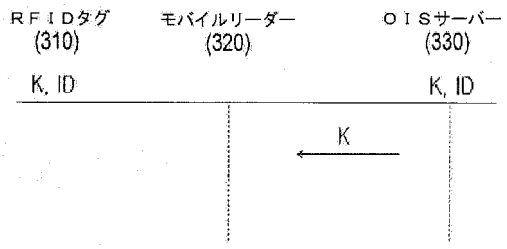
【図１Ｂ】



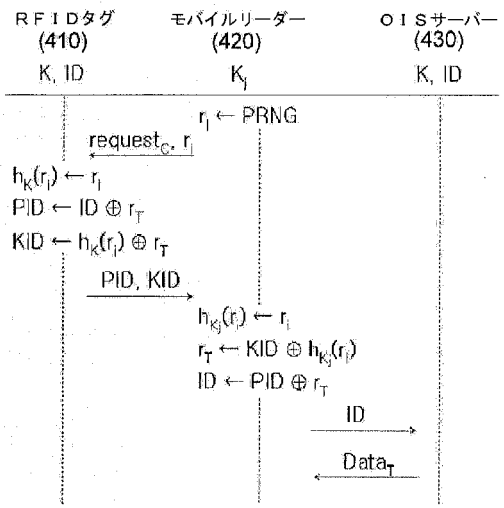
【図２】



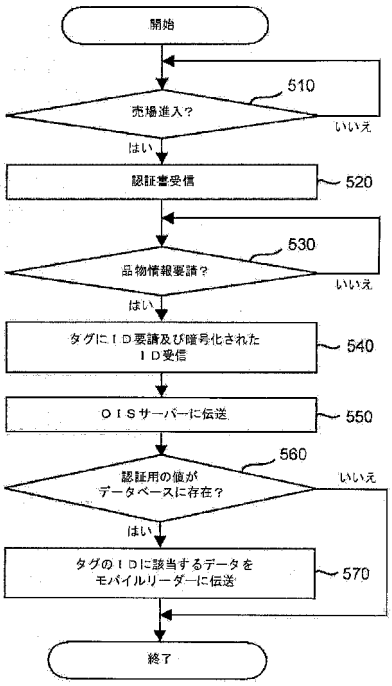
【図３】



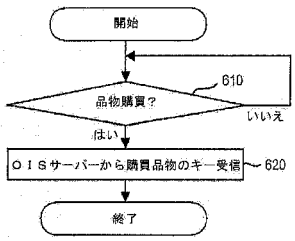
【図４】


RFIDタグ
(410)
K, ID
モバイルリーダー
(420)
K_j
OISサーバー
(430)
K, ID
r_j ← PRNG
request_C, r_j
h_K(r_j) ← r_j
PID ← ID ⊕ r_T
KID ← h_K(r_j) ⊕ r_T
PID, KID
h_Kj(r_j) ← r_j
r_T ← KID ⊕ h_Kj(r_j)
ID ← PID ⊕ r_T
ID
Data_T

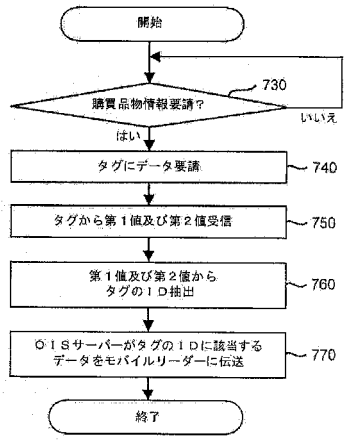
【図５】


開始
510
市場進入？
いいえ
はい
認証書受信
520
530
品物情報要請？
いいえ
はい
タグにＩＤ要請及び暗号化された
ＩＤ受信
540
ＯＩＳサーバーに伝送
550
560
認証用の値が
データベースに存在？
いいえ
はい
タグのＩＤに該当するデータを
モバイルリーダーに伝送
570
終了

【図６】


開始
610
品物購買？
いいえ
はい
ＯＩＳサーバーから購買品物のキー受信
620
終了

【図７】


開始
730
購買品物情報要請？
いいえ
はい
タグにデータ要請
740
タグから第１値及び第２値受信
750
第１値及び第２値から
タグのＩＤ抽出
760
ＯＩＳサーバーがタグのＩＤに該当する
データをモバイルリーダーに伝送
770
終了

フロントページの続き

(51)Int.Cl.			FI		
G06K	***19/10***	***(2006.01)***	G06K	19/00	H
G07G	***1/00***	***(2006.01)***	G06K	19/00	Q
G07G	***1/01***	***(2006.01)***	G06K	19/00	R
G07G	***1/14***	***(2006.01)***	G07G	1/00	311Z
H04L	***9/32***	***(2006.01)***	G07G	1/01	301D
			G07G	1/14	
			H04L	9/00	673C

(72)発明者 ウン ヨン, チェ
大韓民国, １３６－０７５, ソウル, ソンブクーク, アナムードン ５－カ, １１－１, ＃５０２
(72)発明者 イル ジョン, キム
大韓民国, １３０－０６０, ソウル, トンデムンーグ, チェギードン, １４８－２９

合議体
審判長 金子 幸一
審判官 須田 勝巳
審判官 井上 信一

(56)参考文献 特開２００７－２５９０３（ＪＰ, Ａ）
特開２００５－３４８３０６（ＪＰ, Ａ）
特開２００６－７２５８１（ＪＰ, Ａ）
特開２００５－１７４３１５（ＪＰ, Ａ）
特開２００４－３２６５８０（ＪＰ, Ａ）
伊藤忠商事株式会社情報産業部門ユビキタス戦略室, ポイント図解式 ＲＦＩＤ教科書, 株式会社アスキー, ２００６年8月３１日, 第1版, ｐ. １７１－１８０

(58)調査した分野(Int.Cl., ＤＢ名)
G06Q10/00-50/00
G06K17/00
G06K19/00
H04L9/00