(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2018-72977
(P2018-72977A)
(43)公開日　平成30年5月10日(2018.5.10)

(51)Int.Cl.		F I			テーマコード（参考）
G06Q 30/00	(2012.01)	G06Q	30/00	３４２	５Ｌ０４９
G06K 19/077	(2006.01)	G06Q	30/00	ＺＩＴ	
G06K 7/10	(2006.01)	G06K	19/077	３０４	
G06K 17/00	(2006.01)	G06K	7/10	２５２	
		G06K	17/00	Ｏ２２	

審査請求 未請求　請求項の数 6　ＯＬ　（全 30 頁）

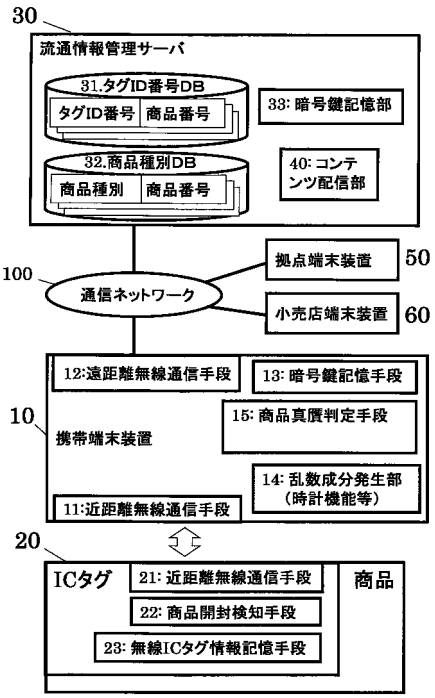
(21)出願番号　特願2016-209485 (P2016-209485)
(22)出願日　平成28年10月26日 (2016.10.26)

(71)出願人　000003193
凸版印刷株式会社
東京都台東区台東１丁目５番１号
(72)発明者　久保　高志
東京都台東区台東１丁目５番１号　凸版印刷株式会社内

Ｆターム(参考)　5L049 BB72

(54)【発明の名称】商品の真贋判定システム

(57)【要約】
【課題】商品の開封後も継続してコンテンツが配信される、商品の真贋判定システムを得る。
【解決手段】流通情報管理サーバと、商品に取り付けられ商品開封検知手段を有する無線ＩＣタグと、前記無線ＩＣタグを用いた商品真贋判定手段を有する携帯端末装置を用い、前記無線ＩＣタグが前記携帯端末装置を介して送信したタグＩＤ番号を該流通情報管理サーバが受信して商品の正当性を判定し、前記無線ＩＣタグの正当ユーザコードの記憶が固定されていない場合に前記携帯端末装置が新たな正当ユーザコードを作成して前記無線ＩＣタグの記憶を更新し、該無線ＩＣタグは、商品の開封を検知した場合に正当ユーザコードの記憶を固定し、前記無線ＩＣタグと前記携帯端末装置が記憶している前記正当ユーザコードが一致しているときにコンテンツの配信要求を受信した前記流通情報管理サーバが、前記商品に関するコンテンツを配信する商品の真贋判定システムを用いる。
【選択図】図１



【特許請求の範囲】
【請求項１】
商品に取り付けた無線ＩＣタグと携帯端末装置と流通情報管理サーバを用いる商品の真贋判定システムであり、
前記無線ＩＣタグが商品開封検知手段を有し、前記携帯端末装置が、前記無線ＩＣタグと通信する近距離無線通信手段と、前記無線ＩＣタグを用いた商品真贋判定手段を有し、
前記無線ＩＣタグが前記携帯端末装置を介して送信したタグＩＤ番号を前記流通情報管理サーバが受信して商品の正当性を判定し、
前記無線ＩＣタグの正当ユーザコードの記憶が固定されていない場合に前記携帯端末装置が新たな正当ユーザコードを作成して前記無線ＩＣタグの記憶を更新し、該無線ＩＣタグは、商品の開封を検知した場合に正当ユーザコードの記憶を固定し、
前記無線ＩＣタグと前記携帯端末装置が記憶している前記正当ユーザコードが一致しているときにコンテンツの配信要求を受信した前記流通情報管理サーバが、前記商品に関するコンテンツを配信することを特徴とする商品の真贋判定システム。
【請求項２】
請求項１記載の商品の真贋判定システムであって、前記商品真贋判定手段がプログラムの正当性検証プログラムを内在させ、前記プログラムの正当性検証プログラムが、前記商品真贋判定手段を流通情報管理サーバに認証させることを特徴とする商品の真贋判定システム。
【請求項３】
請求項１記載の商品の真贋判定システムであって、前記無線ＩＣタグが前記タグＩＤ番号を暗号化して前記流通情報管理サーバに送信し、
前記コンテンツの配信要求の際に、前記流通情報管理サーバが、前記無線ＩＣタグ及び前記携帯端末装置から暗号化された正当ユーザコードを受信し、両方の正当ユーザコードが一致している場合に商品に関するコンテンツを配信することを特徴とする商品の真贋判定システム。
【請求項４】
請求項１乃至３の何れか一項に記載の真贋判定システムであって、前記流通情報管理サーバが、前記タグＩＤ番号を記憶するデータベースを有し、該データベースを検索して前記無線ＩＣタグを取り付けた商品の正当性を判定することを特徴とする商品の真贋判定システム。
【請求項５】
請求項１乃至４の何れか一項に記載の真贋判定システムであって、前記無線ＩＣタグの前記正当ユーザコードの記憶が固定された後に、前記携帯端末装置が記憶する前記正当ユーザコードを他の携帯端末装置に移譲する処理が可能なことを特徴とする商品の真贋判定システム。
【請求項６】
請求項１乃至５の何れか一項に記載の商品の真贋判定システムであって、前記流通情報管理サーバが配信する前記商品に関するコンテンツは暗号化されており、前記正当ユーザコードを有する携帯端末装置でのみ視聴が可能であることを特徴とする商品の真贋判定システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、消費者が商品の真贋を判定できるコンテンツを受信できる商品の真贋判定システムに関する。
【背景技術】
【０００２】
従来から、商品は、例えば、工場において生産され、配売店において消費者に販売されている。販売店における販売業者は、消費者に対して、その商品が正規の工場で生産され

、正規の流通ルートを経て販売された商品に関して、商品の品質を保証している。すなわち、正規に販売された商品を偽造された商品と区別し、一定以上の品質を保つことにより、消費者に対して商品への信頼を向上している。

【０００３】

特に、商品が著名なブランド品である場合、例えば、高級酒などの高価な商品や電化製品の消耗品など、偽造防止を要する物品などにおいては、それらの真贋を判定するために、商品本体やそれを包装したケース等に封印ラベルが貼り付けられる。

【０００４】

特許文献１や特許文献２では、高いセキュリティ機能を有するＩＣタグを搭載することで、偽造防止機能を持つ封印ラベル等が提案されている。特に、固有のタグＩＤ番号が記憶されたＩＣチップを埋め込むことで、個々の商品が判別でき、商品の真贋判定をすることができる。

【０００５】

これらの特許文献の封印ラベルは、商品が開封されると封印ラベルの基材が破壊、同時にＩＣタグのアンテナも断線して通信不能になることで開封を確認している。しかし、その開封もアンテナ等の結線を戻すことによりまた未開封の状態に戻すことは物理的には可能であるので、未開封状態を偽装できる問題があった。

【０００６】

それに対し、特許文献３では、一度開封された開封済み情報を開封と同時にＩＣタグに書き込むことができる封印ラベルが提案されている。それにより、その後の開封を戻す操作を行っても未開封とならないようにでき、未開封状態が偽装されることを防ぐことができる。

【先行技術文献】

【特許文献】

【０００７】

【特許文献１】特開２０００－１１１１４号公報

【特許文献２】特開２００３－１５０９２４号公報

【特許文献３】特開２０１４－１１４０６６号公報

【発明の概要】

【発明が解決しようとする課題】

【０００８】

上述した特許文献１から３の技術では、商品のＩＣタグは、例えば酒類の商品の空き瓶やＩＣタグそのものの使い回し防止のために、商品が開封された場合にＩＣタグを破損させる機構を設けるか、開封済みフラグをＩＣタグが記憶することで、そのＩＣタグを用いてはコンテンツ情報を取得することができない様にしている。

【０００９】

しかし、商品を購入したユーザには、商品の開封後も、商品の品質の確認のためのコンテンツや商品購入の特典として与えられたコンテンツが配信される必要がある。

【００１０】

そのため、本発明の課題は、ユーザが小売店等で、販売以前の商品に関するコンテンツを受信して商品の真贋が判定でき、かつ、商品を購入したユーザには、商品の開封後も、その商品に関して継続してコンテンツが配信される、商品の真贋判定システムを提供することにある。

【課題を解決するための手段】

【００１１】

本発明は上記の課題を解決するために、商品に取り付けた無線ＩＣタグと携帯端末装置と流通情報管理サーバを用いる商品の真贋判定システムであり、

前記無線ＩＣタグが商品開封検知手段を有し、前記携帯端末装置が、前記無線ＩＣタグと通信する近距離無線通信手段と、前記無線ＩＣタグを用いた商品真贋判定手段を有し、

前記無線ＩＣタグが前記携帯端末装置を介して送信したタグＩＤ番号を前記流通情報管理

サーバが受信して商品の正当性を判定し、
前記無線ＩＣタグの正当ユーザコードの記憶が固定されていない場合に前記携帯端末装置が新たな正当ユーザコードを作成して前記無線ＩＣタグの記憶を更新し、該無線ＩＣタグは、商品の開封を検知した場合に正当ユーザコードの記憶を固定し、
前記無線ＩＣタグと前記携帯端末装置が記憶している前記正当ユーザコードが一致しているときにコンテンツの配信要求を受信した前記流通情報管理サーバが、前記商品に関するコンテンツを配信することを特徴とする商品の真贋判定システムである。

【００１２】

本発明は、この構成により、商品が開封された後にも、正当ユーザコードを記憶するユーザの携帯端末装置が流通情報管理サーバから商品に関するコンテンツを受信することができる効果がある。

【００１３】

また、本発明は、上記の商品の真贋判定システムであって、前記商品真贋判定手段がプログラムの正当性検証プログラムを内在させ、前記プログラムの正当性検証プログラムが、前記商品真贋判定手段を流通情報管理サーバに認証させることを特徴とする商品の真贋判定システムである。

【００１４】

また、本発明は、上記の商品の真贋判定システムであって、前記無線ＩＣタグが前記タグＩＤ番号を暗号化して前記流通情報管理サーバに送信し、
前記コンテンツの配信要求の際に、前記流通情報管理サーバが、前記無線ＩＣタグ及び前記携帯端末装置から暗号化された正当ユーザコードを受信し、両方の正当ユーザコードが一致している場合に商品に関するコンテンツを配信することを特徴とする商品の真贋判定システムである。

【００１５】

また、本発明は、上記の商品の真贋判定システムであって、前記流通情報管理サーバが、前記タグＩＤ番号を記憶するデータベースを有し、該データベースを検索して前記無線ＩＣタグを取り付けた商品の正当性を判定することを特徴とする商品の真贋判定システムである。

【００１６】

また、本発明は、上記の商品の真贋判定システムであって、前記無線ＩＣタグの前記正当ユーザコードの記憶が固定された後に、前記携帯端末装置が記憶する前記正当ユーザコードを他の携帯端末装置に移譲する処理が可能なことを特徴とする商品の真贋判定システムである。

【００１７】

また、本発明は、上記の商品の真贋判定システムであって、前記流通情報管理サーバが配信する前記商品に関するコンテンツは暗号化されており、前記正当ユーザコードを有する携帯端末装置でのみ視聴が可能であることを特徴とする商品の真贋判定システムである。

【発明の効果】

【００１８】

本発明によれば、携帯端末装置の商品真贋判定手段が作成した正当ユーザコードを携帯端末装置が記憶するとともに、近距離無線通信手段を介して、無線ＩＣタグに送信して記憶させる。無線ＩＣタグは、商品の開封を検知した場合は正当ユーザコードの記憶を固定する。商品に関するコンテンツを表示させる際には、携帯端末装置を無線ＩＣタグに再度かざし、無線ＩＣタグ内に記憶している正当ユーザコードと携帯端末装置が記憶している正当ユーザコードが一致していることを確認することにより、流通情報管理サーバが、携帯端末装置に暗号化されたコンテンツを配信し、携帯端末装置はそのコンテンツを復号して表示する、商品の真贋判定システムが得られる。

【００１９】

この構成によって、本発明の商品の真贋判定システムが、商品が開封された後にも、正

当ユーザコードを記憶するユーザの携帯端末装置が流通情報管理サーバから商品に関するコンテンツを受信することができる効果がある。

【００２０】

また、本発明では、上記流通情報管理サーバが配信するコンテンツは暗号化されていて、正当な商品真贋判定アプリケーションプログラムによって構成した正当な商品真贋判定手段にのみ復号でき、また、その正当な商品真贋判定手段を有する携帯端末装置のみが、正当ユーザコードを有する場合にコンテンツを視聴することが可能である。

【００２１】

それにより、本発明は、ユーザの携帯端末装置に不正な商品真贋判定アプリケーションプログラムがダウンロードされることによる偽の真贋判定が成される問題が無い効果がある。

【図面の簡単な説明】

【００２２】

【図１】本発明の第１の実施形態の商品の真贋判定システムの構成を示すブロック図である。

【図２】本発明の第１の実施形態の携帯端末装置の構成を示すブロック図である。

【図３】本発明の第１の実施形態の無線ＩＣタグの構成を示すブロック図である。

【図４】本発明の第１の実施形態の流通情報管理サーバ３０の構成を示すブロック図である。

【図５】本発明の第１の実施形態の商品の真贋判定システムの動作を示すフローチャート（その１）である。

【図６】本発明の第１の実施形態の商品の真贋判定システムの動作を示すフローチャート（その２）である。

【図７】本発明の第１の実施形態の商品の真贋判定システムの動作を示すフローチャート（その３）である。

【図８】本発明の第１の実施形態の商品の真贋判定システムの動作を示すフローチャート（その４）である。

【図９】本発明の第１の実施形態の商品の真贋判定システムの動作を示すフローチャート（その５）である。

【図１０】本発明の第２の実施形態の携帯端末装置の構成を示すブロック図である。

【図１１】本発明の第２の実施形態の無線ＩＣタグの構成を示すブロック図である。

【図１２】本発明の第２の実施形態の流通情報管理サーバ３０の構成を示すブロック図である。

【図１３】本発明の第２の実施形態の商品の真贋判定システムの動作を示すフローチャート（その１）である。

【図１４】本発明の第２の実施形態の商品の真贋判定システムの動作を示すフローチャート（その２）である。

【図１５】本発明の第２の実施形態の商品の真贋判定システムの動作を示すフローチャート（その３）である。

【図１６】本発明の第２の実施形態の商品の真贋判定システムの動作を示すフローチャート（その４）である。

【発明を実施するための形態】

【００２３】

＜第１の実施形態＞

図１は、この発明の第１の実施形態による商品の真贋判定システムの構成を示す概略ブロック図である。以下で図１から図９を用いて、本発明の第１の実施形態を説明する。

【００２４】

（システム構成）

第１の実施形態の商品の真贋判定システムは、図１の様に、携帯端末装置１０と、商品に添付した無線ＩＣタグ２０と、携帯電話網や無線ＬＡＮ網などの無線通信網の通信ネッ

トワーク１００で接続した流通情報管理サーバ３０を用いる。本実施形態では、商品に添付する無線ＩＣタグ２０は、商品の開封により、回路の特定箇所が切断や除去されて無線ＩＣタグ２０の状態が変化するように構成し、商品の開封後は開封状態が無線ＩＣタグ２０のチップ内に書き込まれ（格納され）、開封状態が判定できる様にする。

【００２５】

（携帯端末装置１０）

携帯端末装置１０の構成を、図２を参照して説明する。携帯端末装置１０は、近距離無線通信手段１１と遠距離無線通信手段１２と、暗号鍵記憶手段１３と、時計機能部のような乱数成分発生部１４と、記憶手段に記憶した商品真贋判定アプリケーションプログラムで構成する商品真贋判定手段１５を有する。

【００２６】

（近距離無線通信手段１１）

携帯端末装置１０は近距離無線通信手段１１を用いて、商品に添付した無線ＩＣタグ２０とデータ通信する。近距離無線通信手段１１の通信方式は、例えば、ＮＦＣ通信やＢｌｕｅｔｏｏｔｈ（登録商標）や赤外線通信などを用いることが可能である。

【００２７】

（遠距離無線通信手段１２）

携帯端末装置１０の遠距離無線通信手段１２は、携帯電話網の無線通信方式や、無線ＬＡＮに用いられる通信方式の通信ネットワーク１００を介して流通情報管理サーバ３０と通信する。

【００２８】

（暗号鍵記憶手段１３）

携帯端末装置１０の暗号鍵記憶手段１３には、流通情報管理サーバ３０に無線ＩＣタグ２０の識別コード（タグＩＤ番号ＩＤ１）を送付するために流通情報管理サーバ３０と共有するタグＩＤ番号暗号鍵Ｗｓ、及び、ワンタイムのコンテンツ復号鍵ＣＣｓを記憶する。

【００２９】

流通情報管理サーバ３０と共有するタグＩＤ番号暗号鍵Ｗｓは、共通鍵暗号方式の共通鍵を共有して記憶してもよいが、公開鍵暗号方式の秘密鍵と公開鍵とを組み合わせた鍵の一方の公開鍵のタグＩＤ番号暗号鍵Ｗｓを記憶する事がより望ましい。

【００３０】

また、ワンタイムのコンテンツ復号鍵ＣＣｓは、流通情報管理サーバ３０から暗号化されて送付されたコンテンツを復号するために用いる。

【００３１】

（商品真贋判定手段１５）

携帯端末装置１０は先ず、流通情報管理サーバ３０から、商品真贋判定アプリケーションプログラムと、タグＩＤ番号暗号鍵Ｗｓを受信し、その商品真贋判定アプリケーションプログラムとタグＩＤ番号暗号鍵Ｗｓによって商品真贋判定手段１５を構成する。

【００３２】

商品真贋判定手段１５は、正当ユーザコード固定フラグＦＩＸが立っていない無線ＩＣタグ２０と通信した際に、正当ユーザコードＩＤ２を更新して無線ＩＣタグ２０の記憶を更新させる。

【００３３】

商品真贋判定アプリケーションプログラムは、商品毎に流通情報管理サーバ３０から携帯端末装置１０に配信するか、又は、複数の商品で共通して使用する商品真贋判定アプリケーションプログラムを流通情報管理サーバ３０から携帯端末装置１０に配信する。

【００３４】

（変形例１）

変形例１として、商品真贋判定アプリケーションプログラムを流通情報管理サーバ３０内に持たせ、携帯端末装置１０は、その流通情報管理サーバ３０内の商品真贋判定アプリ

ケーションプログラムを動作させることで、携帯端末装置１０用の商品真贋判定手段１５を構成することができる。

【００３５】

（プログラムの正当性検証プログラム）

商品真贋判定アプリケーションプログラムを受信した携帯端末装置１０が構成した商品真贋判定手段１５内に、プログラムの正当性検証プログラムを内在させる。

【００３６】

流通情報管理サーバ３０は、携帯端末装置１０の商品真贋判定手段１５との間に、セキュア・ソケット・レイヤ（Secure Socket Layer：ＳＳＬ）等の暗号化通信の体制を整えて暗号化した情報を交換する。

【００３７】

そうして通信のセキュリティを確保した上で、商品真贋判定手段１５内のプログラムの正当性検証プログラムは、携帯端末装置１０の商品真贋判定手段１５の正当性を証明するデータを流通情報管理サーバ３０に送信して、流通情報管理サーバ３０に商品真贋判定手段１５（商品真贋判定アプリケーションプログラム）の正当性を確認させる。

【００３８】

こうして、プログラムの正当性検証プログラムが、流通情報管理サーバ３０に商品真贋判定手段１５の正当性を確認させることで、偽の商品真贋判定アプリケーションプログラムが携帯端末装置１０にインストールされても、その偽のプログラムが流通情報管理サーバ３０から不正に商品真贋判定の為のコンテンツデータを取得することを防ぐことができる効果がある。

【００３９】

すなわち、携帯端末装置１０にインストールされた偽のプログラムが、携帯端末装置１０が読み取らなかったタグＩＤ番号ＩＤ１を不正に使用した不正な端末装置暗号化データＤＭＢを作成して流通情報管理サーバ３０に送信しても、流通情報管理サーバ３０から商品真贋判定の為のコンテンツデータを取得できないように、防衛することができる効果がある。

【００４０】

流通情報管理サーバ３０は、こうして、携帯端末装置１０の商品真贋判定手段１５の正当性を確認した上で、携帯端末装置１０の商品真贋判定手段１５にワンタイムのコンテンツ復号鍵ＣＣｓを送信して記憶させる。

【００４１】

このワンタイムのコンテンツ復号鍵ＣＣｓは、流通情報管理サーバ３０と携帯端末装置１０の商品真贋判定手段１５との間のＳＳＬ等の暗号化通信におけるセッション鍵をワンタイムのコンテンツ復号鍵ＣＣｓとして用いることもできる。

【００４２】

（暗号化されたコンテンツデータＣＮＤ）

また、流通情報管理サーバ３０が、携帯端末装置１０に、暗号化されたコンテンツデータＣＮＤを送信する。携帯端末装置１０は受信した暗号化されたコンテンツデータＣＮＤを、コンテンツ復号鍵ＣＣｓを用いて復号してユーザに視聴させる。

【００４３】

ここで、携帯端末装置１０が、流通情報管理サーバ３０から暗号化されたコンテンツデータＣＮＤを受信し、商品真贋判定アプリケーションプログラムが、ワンタイムのコンテンツ復号鍵ＣＣｓを用いて復号してコンテンツデータを得てユーザに提示することで、不正な商品真贋判定アプリケーションプログラムがユーザの携帯端末装置１０に格納されて偽者の商品を本物と表示する問題を防ぐことができる効果がある。

【００４４】

不正な商品真贋判定アプリケーションプログラムは、流通情報管理サーバ３０からワンタイムのコンテンツ復号鍵ＣＣｓを入手することができない。そのため、不正な者が、通信を傍受するなどで暗号化されたコンテンツデータＣＮＤを不正に入手しても、それをワ

ンタイムのコンテンツ復号鍵ＣＣｓを用いて復号できないので、正当な商品真贋判定アプリケーションプログラムによる商品の真贋判定の正当性を高めることができる効果がある。

【００４５】

（商品真贋判定手段１５の処理の概要）

携帯端末装置１０の商品真贋判定手段１５は、近距離無線通信手段１１を用いて、商品に添付された無線ＩＣタグ２０が記憶するユニークなＩＤ番号（以下、タグＩＤ番号ＩＤ１）を読出し、そのタグＩＤ番号ＩＤ１を流通情報管理サーバ３０に問い合わせる。

【００４６】

また、商品真贋判定手段１５は、無線ＩＣタグ２０の記憶している正当ユーザコード固定フラグＦＩＸが立っていない無線ＩＣタグ２０と通信した際に、無線ＩＣタグ２０の記憶する正当ユーザコードＩＤ２を新しい値に更新する。

【００４７】

一方、無線ＩＣタグ２０の正当ユーザコード固定フラグＦＩＸが立って無線ＩＣタグ２０の記憶が固定された場合は、商品真贋判定手段１５は、携帯端末装置１０の記憶している正当ユーザコードＩＤ２と、無線ＩＣタグ２０の記憶している正当ユーザコードＩＤ２が一致しない場合には流通情報管理サーバ３０にコンテンツの配信要求を出さずに処理を終了する。

【００４８】

こうして、携帯端末装置１０の商品真贋判定手段１５が、正しい正当ユーザコードＩＤ２を持つ携帯端末装置１０のみが流通情報管理サーバ３０からコンテンツデータＣＮＤを配信されるように、コンテンツデータＣＮＤの配信の可否を定める。

【００４９】

先ず、商品真贋判定手段１５は、以下の様にして、流通情報管理サーバ３０に、商品に添付される無線ＩＣタグ２０のタグＩＤ番号ＩＤ１を問い合わせる。

【００５０】

（端末装置暗号化データＤＭＢ）

すなわち、携帯端末装置１０の商品真贋判定手段１５は、その伝文が傍受されず、偽造・改ざんされない為に、図２に示す様なデータ構造の端末装置暗号化データＤＭＢを作成して、通信ネットワーク１００を介して、流通情報管理サーバ３０に送信して、流通情報管理サーバ３０にタグＩＤ番号ＩＤ１を問い合わせる。

【００５１】

端末装置暗号化データＤＭＢを作成する元の情報は、読み出した無線ＩＣタグ２０のタグＩＤ番号ＩＤ１と、乱数成分発生部１４が作成した時刻データのような乱数成分ｔが最低限必要な情報となる。それ以外に、携帯端末装置のメールアドレスＥｍａｉｌを合わせたデータなどを追加することも可能である。

【００５２】

商品真贋判定手段１５は、その情報を、携帯端末装置１０が流通情報管理サーバ３０と共有するタグＩＤ番号暗号鍵Ｗｓ（公開鍵）で暗号化して、その端末装置暗号化データＤＭＢを作成して流通情報管理サーバ３０へ送信する。

【００５３】

流通情報管理サーバ３０は、受信した端末装置暗号化データＤＭＢを、流通情報管理サーバ３０が記憶するタグＩＤ番号暗号用秘密鍵Ｃｓ（公開鍵であるタグＩＤ番号暗号鍵Ｗｓと組になる秘密鍵）を用いて復号してタグＩＤ番号ＩＤ１を得る。

【００５４】

流通情報管理サーバ３０は、タグＩＤ番号データベース３１から、そのタグＩＤ番号ＩＤ１を記録した商品流通情報３１ａを検索する。流通情報管理サーバ３０は、その検索結果に応じた処理を行う。

【００５５】

すなわち、流通情報管理サーバ３０は、その商品流通情報３１ａがタグＩＤ番号データ

ベース３１に登録されている場合は、その商品の真贋判定用の、暗号化されたコンテンツデータＣＮＤを携帯端末装置１０の商品真贋判定手段１５に返信する。

【００５６】

携帯端末装置１０の商品真贋判定手段１５は、その暗号化されたコンテンツデータＣＮＤを、ワンタイムのコンテンツ復号鍵ＣＣｓを用いて復号してその商品の真贋判定用のコンテンツが得られることで、商品の真贋判定を行う。

【００５７】

（無線ＩＣタグ２０）

無線ＩＣタグ２０は、図３の様に、ＮＦＣ通信や無線ＬＡＮ等の近距離無線通信手段２１と、商品開封検知手段２２と、無線ＩＣタグ情報記憶手段２３を有する。

【００５８】

本実施形態では、無線タグ暗号化データ作成手段２４を持たない無線ＩＣタグ２０を用いることで、無線ＩＣタグ２０を安価にすることでコストを低く抑えることができる効果がある。

【００５９】

（商品開封検知手段２２）

無線ＩＣタグ２０の商品開封検知手段２２は、商品が開封される際に無線ＩＣタグ２０の回路の特定箇所が切断や除去されるように構成し無線ＩＣタグ２０の回路に電気的な変化を生じさせ、その電気的な変化を検出する。そして、商品の開封後は、無線ＩＣタグ情報記憶手段２３に、検出結果の開封フラグＯＰＦを開封情報として記憶し、開封がわかる様に構成する。

【００６０】

すなわち、無線ＩＣタグ２０は、商品開封検知手段２２が商品が未開封と判定した場合は、開封フラグＯＰＦを「商品未開封」に設定し、商品が開封済みと判定した場合は、開封フラグＯＰＦを「商品開封済み」に設定して開封フラグを立てる。

【００６１】

（無線ＩＣタグ情報記憶手段２３）

無線ＩＣタグ２０は、無線ＩＣタグ情報記憶手段２３に、その無線ＩＣタグ２０用のユニークなＩＤ番号（タグＩＤ番号ＩＤ１）を記憶するとともに、正当ユーザコードＩＤ２と、開封フラグＯＰＦと正当ユーザコード固定フラグＦＩＸを記憶する。

【００６２】

（無線ＩＣタグ２０のタグＩＤ番号ＩＤ１）

無線ＩＣタグ２０のタグＩＤ番号ＩＤ１は、流通情報管理サーバ３０と無線ＩＣタグ２０のみで共有させ、以って、無線ＩＣタグ２０が正当であることを確認させるために用いる。

【００６３】

このタグＩＤ番号ＩＤ１は、無線ＩＣタグ２０が流通情報管理サーバ３０以外には通知しない様に構成する必要がある。タグＩＤ番号ＩＤ１は、携帯端末装置１０の商品真贋判定手段１５が暗号化して端末装置暗号化データＤＭＢを作成し、流通情報管理サーバ３０へ送信する。

【００６４】

（正当ユーザコードＩＤ２）

無線ＩＣタグ１０は、無線ＩＣタグ情報記憶手段２３に正当ユーザコードＩＤ２を記憶する。その正当ユーザコードＩＤ２は、正当ユーザコード固定フラグＦＩＸが立っていない間は、携帯端末装置１０から新しい正当ユーザコードＩＤ２を受信する毎に、その新しい正当ユーザコードＩＤ２に更新し続ける。

【００６５】

無線ＩＣタグ１０は、無線ＩＣタグ情報記憶手段２３の開封フラグＯＰＦに「商品開封済み」が設定されて開封フラグが立っている場合は、その後に最初に携帯端末装置１０から受信した正当ユーザコードＩＤ２により無線ＩＣタグ情報記憶手段２３の記憶を更新し

、それ以降は、正当ユーザコード固定フラグＦＩＸを立てて正当ユーザコードＩＤ２の記憶を固定する。

【００６６】

こうすることで、以下の様な場合にも問題を生じ無いようにすることができる。例えば、商品を購入したユーザが、携帯端末装置１０から正当ユーザコードＩＤ２を無線ＩＣタグ２０に登録しないで商品を開封する場合が有り得る。一方で、それ以前に、その商品を購入しなかった他のユーザが、そのユーザの携帯端末装置１０が作成した正当ユーザコードＩＤ２を無線ＩＣタグ２０に登録している場合があり得る。

【００６７】

その場合に、商品を購入したユーザが、商品を開封した後に最初に携帯端末装置１０から正当ユーザコードＩＤ２を無線ＩＣタグ２０に送信した際に、無線ＩＣタグ情報記憶手段２３が正当ユーザコードＩＤ２の記憶を更新し、以降は正当ユーザコードＩＤ２の記憶を固定し更新しない様にする。こうすることで、その商品を購入したユーザが、正当ユーザコードＩＤ２を所有できる。

【００６８】

（流通情報管理サーバ３０）

流通情報管理サーバ３０は、図４に示すように、タグＩＤ番号データベース３１と、商品種別データベース３２と、暗号鍵記憶部３３と、コンテンツ配信部４０を有する。

【００６９】

また、流通情報管理サーバ３０は、公開鍵暗号方式のタグＩＤ番号暗号用秘密鍵ＣｓとタグＩＤ番号暗号鍵Ｗｓを作成し、タグＩＤ番号暗号用秘密鍵Ｃｓは流通情報管理サーバ３０のみが暗号鍵記憶部３３で記憶し、タグＩＤ番号暗号鍵Ｗｓを携帯端末装置１０に記憶させて、携帯端末装置１０の商品真贋判定手段１５が含むプログラムの正当性検証プログラムと暗号化通信を行う。

【００７０】

（変形例２）

変形例２として、この暗号化通信における公開鍵暗号方式のタグＩＤ番号暗号用秘密鍵ＣｓとタグＩＤ番号暗号鍵Ｗｓを共通鍵暗号方式の共通暗号鍵に置き換え、情報管理サーバと、携帯端末装置１０とのあいだで共通暗号鍵を共有することによる暗号通信を実施することができる。

【００７１】

流通情報管理サーバ３０が携帯端末装置１０と行う暗号化通信は、例えば、セキュア・ソケット・レイヤ（Secure Socket Layer：ＳＳＬ）等の暗号化通信の体制を整えて、流通情報管理サーバ３０と携帯端末装置１０のプログラムの正当性検証プログラムが暗号化した情報を交換することで、流通情報管理サーバ３０が携帯端末装置１０の商品真贋判定手段１５を認証する。

【００７２】

そうして通信のセキュリティを確保して、携帯端末装置１０の商品真贋判定手段１５を認証した上で、流通情報管理サーバ３０が、ワンタイムのコンテンツ復号鍵ＣＣｓを作成して、携帯端末装置１０に送信する。

【００７３】

これにより、後に、携帯端末装置１０から要求があった場合に、流通情報管理サーバ３０が、コンテンツ配信部４０を用いて、暗号化されたコンテンツデータＣＮＤを携帯端末装置１０に配信し、携帯端末装置１０は、受信した暗号化されたコンテンツデータＣＮＤを、このコンテンツ復号鍵ＣＣｓを用いて復号してユーザに視聴させる。

【００７４】

（商品種別データベース３２）

流通情報管理サーバ３０は、図４の様に、商品種別データベース３２に、商品種別に対する商品番号ＮＰを登録しておく。すなわち、商品種別を商品番号ＮＰで特定できるようにしておく。

【００７５】
（タグＩＤ番号データベース３１）
流通情報管理サーバ３０は、工場などの製造拠点において商品を生産した際に、あるいは、商品の流通拠点において商品の流通管理を開始するために各商品に無線ＩＣタグ２０を取り付ける際などに、図４の様に、タグＩＤ番号データベース３１に、その無線ＩＣタグ２０のタグＩＤ番号ＩＤ１に商品番号ＮＰを紐付ける商品流通情報３１ａを作成して登録する。また、商品流通情報３１ａに、商品の販売後にフラグを立てる商品の販売済みフラグＳＦを設ける。
【００７６】
流通情報管理サーバ３０は、携帯端末装置１０が作成した端末装置暗号化データＤＭＢを受信すると、携帯端末装置１０と共有した復号鍵（タグＩＤ番号暗号用秘密鍵Ｃｓ）を用いて端末装置暗号化データＤＭＢを復号する。
【００７７】
そして、流通情報管理サーバ３０は、端末装置暗号化データＤＭＢを復号して得たタグＩＤ番号ＩＤ１を記録した商品流通情報３１ａをタグＩＤ番号データベース３１から検索する。流通情報管理サーバ３０は、その商品流通情報３１ａが存在する場合に、無線ＩＣタグ２０を正当と判定したメッセージを携帯端末装置１０に返信するなど、その受信した端末装置暗号化データＤＭＢに応じた処理を行う。
【００７８】
すなわち、流通情報管理サーバ３０は、端末装置暗号化データＤＭＢを復号して得たタグＩＤ番号ＩＤ１を記録した商品流通情報３１ａがタグＩＤ番号データベース３１に存在する場合には、商品種別データベース３２から、商品流通情報３１ａにおいてそのタグＩＤ番号ＩＤ１に紐付けて記録されていた商品番号ＮＰを検索し、その商品番号ＮＰに紐付いた商品種別を読出す。
【００７９】
次に、流通情報管理サーバ３０は、コンテンツ配信部４０を用いて、その商品種別に応じたコンテンツを暗号化して、暗号化されたコンテンツデータＣＮＤを作成し、携帯端末装置１０にダウンロードさせる等して配信する。
【００８０】
携帯端末装置１０は、流通情報管理サーバ３０から受信した暗号化されたコンテンツデータＣＮＤを、コンテンツ復号鍵ＣＣｓを用いて復号して登録商品の解説情報を得て、又は、購入者向けのコンテンツを得てユーザに視聴させる。
【００８１】
（商品の真贋判定システムの動作手順）
次に、商品の真贋判定システムの詳細な動作手順を、図５から図９のフローチャートを参照して説明する。
【００８２】
（流通情報管理サーバ３０への無線ＩＣタグ２０の登録処理手順）
図５は、無線ＩＣタグ２０が有するタグＩＤ番号ＩＤ１を流通情報管理サーバ３０に登録し、商品に取り付けた正当な無線ＩＣタグ２０を記憶させる処理の流れを示すフローチャートである。
【００８３】
（ステップＳ１）
まず、工場などの製造拠点において商品を生産した際に、あるいは、商品の流通拠点において商品の流通管理を開始する際に、各商品に無線ＩＣタグ２０を取り付ける。その際に、拠点端末装置５０がリーダライタによって無線ＩＣタグ２０のタグＩＤ番号ＩＤ１を読み取り、そのタグＩＤ番号ＩＤ１と商品種別を結び付ける情報を記録する要求を流通情報管理サーバ３０に送信する。
【００８４】
（ステップＳ２）

タグＩＤ番号ＩＤ１と商品種別の登録要求を受信した流通情報管理サーバ３０は、商品種別データベース３２に、その商品種別に対する商品番号ＮＰを登録する。そして、流通情報管理サーバ３０は、タグＩＤ番号データベース３１に、そのタグＩＤ番号ＩＤ１に商品番号ＮＰを紐付ける商品流通情報３１ａを登録する。

【００８５】

こうして、流通情報管理サーバ３０は、商品種別データベース３２に商品種別とその番号を追加するとともに、タグＩＤ番号ＩＤ１を商品番号ＮＰと一緒にタグＩＤデータベース３１に登録することで、タグＩＤ番号ＩＤ１を商品種別に紐づける

【００８６】

（ステップＳ３）

そして、流通情報管理サーバ３０は、拠点端末装置５０に、必要に応じて、商品流通情報の作成が完了した通知を行う。

【００８７】

これにより、製造拠点の拠点端末装置５０や小売店端末装置６０が、必要に応じて商品に添付した無線ＩＣタグ２０のタグＩＤ番号ＩＤ１の正当性を流通情報管理サーバ３０に問い合わせることで無線ＩＣタグ２０の正当性を確認することが可能になる。

【００８８】

（ステップＳ４）

そして、製造拠点において、生産した商品に、タグＩＤデータベース３１が指定した無線ＩＣタグ２０を取り付ける。なお、ステップＳ４による無線ＩＣタグ２０の商品への取り付け処理は、ステップＳ１よりも先に行い、商品に無線ＩＣタグ２０を取り付けた状態でステップＳ１からＳ３の処理を行うこともできる。

【００８９】

（変形例３）

変形例３として、複数の無線ＩＣタグ２０の生産時に、タグＩＤ番号ＩＤ１をシリアルに番号を変えて複数の無線ＩＣタグ２０に付与することが可能である。変形例３では、その様にシリアルに番号を付した無線ＩＣタグ２０の群（シリアル番号なら先頭のタグＩＤ番号ＩＤ１と、無線ＩＣタグ２０を貼り付ける商品の数）を、拠点端末装置５０を通して流通情報管理サーバ３０に送信して、タグＩＤ番号ＩＤ１と商品種別を結び付ける情報を記録する要求をする。

【００９０】

流通情報管理サーバ３０は、商品種別データベース３２に、その商品種別に対する商品番号ＮＰを登録する。次に、流通情報管理サーバ３０は、タグＩＤ番号データベース３１に、そのタグＩＤ番号ＩＤ１に商品番号ＮＰを紐付ける商品流通情報３１ａを登録する。

【００９１】

次に、製造拠点がその同一の商品種別の商品群の各商品を生産する毎に、その商品に、既に流通情報管理サーバ３０にタグＩＤ番号ＩＤ１を登録した無線ＩＣタグ２０から順に、登録した商品数に至るまで貼りつけていく。大量生産の場合は、一般的にこちらの方式をとる方が望ましい。

【００９２】

（ユーザによる商品の真贋判定処理手順）

次に、図６から図８のフローチャートを参照して、流通情報管理サーバ３０を用いた商品の真贋判定処理手順を説明する。商品の真贋判定処理では、先ず、ユーザが小売店等において、携帯端末装置１０を用いて、無線ＩＣタグ２０及び流通情報管理サーバ３０と情報を交換して真贋を判定する。

【００９３】

（商品真贋判定アプリケーションプログラムのインストール）

先ず、ユーザが、最初に小売店で商品の真贋判定処理をしようとする場合等に、携帯端末装置１０に商品真贋判定アプリケーションプログラムがインストールされていない場合は、以下のステップＳ１０の処理により商品真贋判定アプリケーションプログラムをイン

ストールする。
【００９４】
（ステップＳ１０）
すなわち、携帯端末装置１０は、流通情報管理サーバ３０から、商品真贋判定アプリケーションプログラムと、タグＩＤ番号暗号鍵Ｗｓを受信する。そして、携帯端末装置１０は、この商品真贋判定アプリケーションプログラムをインストールして商品真贋判定手段１５を構成する。このインストール処理は速やかに行うことができる。
【００９５】
（ステップＳ１１）
次に、ユーザが携帯端末装置１０の商品真贋判定アプリケーションプログラムを起動する。起動された商品真贋判定アプリケーションプログラムが商品真贋判定手段１５を構成する。商品真贋判定手段１５は、近距離無線通信手段１１を用いて、無線ＩＣタグ２０と通信して、無線ＩＣタグ２０のタグＩＤ番号ＩＤ１を受信する。
【００９６】
携帯端末装置１０の商品真贋判定手段１５は、無線ＩＣタグ２０と通信できない場合は、無線ＩＣタグ２０が存在しないとして、不正商品としてエラー終了する。この場合、無線ＩＣタグ２０が壊れている場合や何らかの通信エラーにより読み出せない場合もあり得るが、特に考慮せず不正として扱い、処理を終了する。
【００９７】
（ステップＳ１２）
携帯端末装置１０の商品真贋判定手段１５は、無線ＩＣタグ２０と通信できた場合は、次に、商品真贋判定手段１５のプログラムの正当性検証プログラムが、携帯端末装置１０の商品真贋判定手段１５を流通情報管理サーバ３０に認証させる。流通情報管理サーバ３０は、認証した商品真贋判定手段１５のプログラムとの間に、セキュア・ソケット・レイヤ（Secure Socket Layer：ＳＳＬ）等の暗号化通信の体制を整えて暗号化した情報を交換する。
【００９８】
（ステップＳ１２’）
そうして通信のセキュリティを確保し、商品真贋判定手段１５の正当性を検証した上で、流通情報管理サーバ３０が、携帯端末装置１０に、ワンタイムのコンテンツ復号鍵ＣＣｓを暗号化して送信する。携帯端末装置１０は、このコンテンツ復号鍵ＣＣｓを用いることで、流通情報管理サーバ３０から受信する暗号化したコンテンツデータＣＮＤを復号してユーザに視聴させることができる。
【００９９】
（ステップＳ１３）
次に、携帯端末装置１０の乱数成分発生部１４が、時刻データのような乱数成分ｔを作成する。次に、商品真贋判定手段１５が、作成した乱数成分ｔ（生成した乱数、または、日付時間等）と、無線ＩＣタグ２０のタグＩＤ番号ＩＤ１を合わせたデータを、携帯端末装置１０が流通情報管理サーバ３０と共有しているタグＩＤ番号暗号鍵Ｗｓ（公開鍵または共通鍵）で暗号化して端末装置暗号化データＤＭＢを作成して、流通情報管理サーバ３０へ送信する。
【０１００】
ここで、この乱数成分ｔは、携帯端末装置１０が流通情報管理サーバ３０から受信した乱数成分ｔを使う様にすることもできる。そうすると、流通情報管理サーバ３０がより確実に端末装置暗号化データＤＭＢを認証できる効果がある。
【０１０１】
（ステップＳ１４）
流通情報管理サーバ３０は、受信した端末装置暗号化データＤＭＢを復号し、タグＩＤ番号ＩＤ１を取り出す。そして、流通情報管理サーバ３０のタグＩＤ番号データベース３１を検索して、そのタグＩＤ番号ＩＤ１を記録した商品流通情報３１ａの有無を確認する

。
【０１０２】
（ステップＳ１５）
流通情報管理サーバ３０は、タグＩＤ番号データベース３１から、タグＩＤ番号ＩＤ１を記録した商品流通情報３１ａを抽出できた場合は、その無線ＩＣタグ２０を正当なものと判定し、それが張り付いている商品を正当な商品であると判定する。その商品流通情報３１ａを抽出できなかった場合は、携帯端末装置１０の商品真贋判定手段１５の処理を終了させる。
【０１０３】
（ステップＳ１６）
流通情報管理サーバ３０から、無線ＩＣタグ２０を正当なものと判定した判定結果を受信した携帯端末装置１０の商品真贋判定手段１５は、無線ＩＣタグ２０と通信して、無線ＩＣタグ２０の開封フラグＯＰＦと正当ユーザコード固定フラグＦＩＸをチェックする。
【０１０４】
携帯端末装置１０は、ユーザに無線ＩＣタグ２０の開封フラグＯＰＦの状況を通知する。これにより、ユーザが、栓がしてあるにもかかわらず開封フラグＯＰＦが立っている場合を発見できる。
【０１０５】
それにより、ユーザが、使いまわされた無線ＩＣタグ２０が使われている偽装商品であると判別することができる効果がある。また、ユーザは、開栓・開封されている商品の無線ＩＣタグ２０の開封フラグＯＰＦが立っている場合は、無線ＩＣタグ２０が通常の状態であると判断できる。
【０１０６】
（ステップＳ１７）
携帯端末装置１０の商品真贋判定手段１５は、無線ＩＣタグ２０の正当ユーザコード固定フラグＦＩＸが立っている場合は、ステップＳ２１に進む。正当ユーザコード固定フラグＦＩＸが立っていない場合はステップＳ１８に進む。
【０１０７】
（ステップＳ１８）
携帯端末装置１０の商品真贋判定手段１５は、新たな正当ユーザコードＩＤ２を生成し、自らの記憶を更新する。
【０１０８】
次に、商品真贋判定手段１５が、生成した正当ユーザコードＩＤ２を携帯端末装置１０から無線ＩＣタグ２０に送信する。
【０１０９】
この処理により、正当ユーザコード固定フラグＦＩＸが立っていない場合は、常に、最近に無線ＩＣタグ２０が通信した携帯端末装置１０と無線ＩＣタグ２０の正当ユーザコードＩＤ２を一緒に更新する。
【０１１０】
（ステップＳ１９）
無線ＩＣタグ２０は、正当ユーザコードＩＤ２を無線ＩＣタグ情報記憶手段２３に記憶する（記憶更新）。
【０１１１】
（ステップＳ２０）
次に、無線ＩＣタグ２０は、無線ＩＣタグ２０の開封フラグＯＰＦが「商品開封済み」であり開封フラグが立っている場合は、正当ユーザコード固定フラグＦＩＸを立てて無線ＩＣタグ情報記憶手段２３に記憶する。これ以降は、無線ＩＣタグ２０は、正当ユーザコードＩＤ２の記憶を固定する。
【０１１２】
以上のステップＳ１６からステップＳ２０の処理によって、商品が開封された後に最初

に正当ユーザコードＩＤ２の設定がされた後に無線ＩＣタグ２０に正当ユーザコード固定フラグＦＩＸを立て、それ以降は正当ユーザコードＩＤ２の記憶を固定する。

【０１１３】

これにより、商品を購入したユーザの携帯端末装置１０の正当ユーザコードＩＤ２が確実に無線ＩＣタグ２０に設定される効果がある。

【０１１４】

（ステップＳ２１）コンテンツの配信処理

ユーザが、コンテンツの視聴の要求有無の指令を携帯端末装置１０から入力する。コンテンツの視聴の要求有りの場合、携帯端末装置１０の商品真贋判定手段１５が以降の処理を行う。コンテンツの視聴の要求が無い場合は、処理を終了する。

【０１１５】

（ステップＳ２２）

コンテンツの視聴の要求有りの場合、携帯端末装置１０の商品真贋判定手段１５は、無線ＩＣタグ２０と通信して、無線ＩＣタグ２０から正当ユーザコードＩＤ２を読み出す。

【０１１６】

携帯端末装置１０の商品真贋判定手段１５は、無線ＩＣタグ２０と通信できない場合は、無線ＩＣタグ２０が存在しないとして、不正商品としてエラー終了する。

【０１１７】

（ステップＳ２３）

携帯端末装置１０の商品真贋判定手段１５は、無線ＩＣタグ２０から読み出した正当ユーザコードＩＤ２が、携帯端末装置１０に記憶されている正当ユーザコードＩＤ２と同一の場合、ステップＳ２４以降の処理を行う。

【０１１８】

一致していない場合、正当な携帯端末装置１０ではない。つまり、他のユーザに正当ユーザコードＩＤ２が正式に譲渡されないまま、無線ＩＣタグが使いまわされた可能性がある。この場合は、携帯端末装置１０の商品真贋判定手段１５は処理を終了する。

【０１１９】

（ステップＳ２４）

次に、商品真贋判定手段１５が、無線ＩＣタグ２０の正当ユーザコード固定フラグＦＩＸが立っているかどうかをチェックする。

【０１２０】

（ステップＳ２５）

携帯端末装置１０の商品真贋判定手段１５は、正当ユーザコード固定フラグＦＩＸが立っていない場合は、流通情報管理サーバ３０に、商品購入以前の一般の者向けの商品真贋判定用コンテンツの配信要求を出す。次にステップＳ２８に進む。

【０１２１】

（ステップＳ２６）

無線ＩＣタグ２０の正当ユーザコード固定フラグＦＩＸが立っている場合は、商品真贋判定手段１５は、流通情報管理サーバ３０に、商品の購入者向けのコンテンツの配信要求を出す。

【０１２２】

その際に、商品真贋判定手段１５が、流通情報管理サーバ３０に、ユーザの携帯端末装置のメールアドレスＥｍａｉｌ等のユーザ情報を追加登録することもできる。

【０１２３】

（ステップＳ２７）

流通情報管理サーバ３０は、ユーザの携帯端末装置１０の商品真贋判定手段１５から、商品の購入者向けのコンテンツの配信要求を受信した場合は、ユーザの携帯端末装置１０に、商品の購入者向けのワンタイムのコンテンツ復号鍵ＣＣｓを暗号化して送信する。

【０１２４】

このワンタイムのコンテンツ復号鍵ＣＣｓは、流通情報管理サーバ３０がユーザの携帯

端末装置１０のメールアドレスＥｍａｉｌ宛てに問合せをしてユーザを確認した上で送信するようにすることもできる。

【０１２５】

その際に、流通情報管理サーバ３０は、タグＩＤ番号データベース３１の、商品流通情報３１ａに、商品の販売済みフラグＳＦを立てて記憶する。次にステップＳ２８に進む。

【０１２６】

（ステップＳ２８）

流通情報管理サーバ３０は、携帯端末装置１０からのコンテンツの配信要求に基づき、暗号化したコンテンツデータＣＮＤを配信する。

【０１２７】

（変形例４）

変形例４として、ユーザが携帯端末装置１０から、流通情報管理サーバ３０に、コンテンツの配信を要求する場合に、コンテンツの配信先のコンピュータ端末を指定する事ができる様にできる。その場合に、流通情報管理サーバ３０は、ユーザの携帯端末装置１０から指定されたコンピュータ宛に、コンテンツ復号鍵ＣＣｓと暗号化されたコンテンツデータＣＮＤを配信する。

【０１２８】

（ステップＳ２９）

携帯端末装置１０は、又は、ユーザがコンテンツの配信先を指定したコンピュータ端末は、暗号化されたたコンテンツデータＣＮＤをコンテンツ復号鍵ＣＣｓを用いて復号してユーザに視聴させる。

【０１２９】

コンテンツデータＣＮＤは暗号化されており、ステップＳ１２’で正当なコンテンツ復号鍵ＣＣｓを受信しなかった携帯端末装置１０ではコンテンツを視聴できない。また、ステップＳ２７で正当な商品の購入者向けのワンタイムのコンテンツ復号鍵ＣＣｓを受信しなかった携帯端末装置１０では商品の購入者向けのコンテンツを視聴できない。

【０１３０】

（変形例５）

変形例５として、無線ＩＣタグ２０の無線ＩＣタグ情報記憶手段２３に、商品購入済みフラグを記憶させる。

【０１３１】

無線ＩＣタグ２０の商品購入済みフラグは、その商品を販売する小売店の小売店端末装置６０が設定する。無線ＩＣタグ２０の商品購入済みフラグは、ユーザの携帯端末装置１０からは設定できないようにする。

【０１３２】

小売店端末装置６０が、未開封状態の商品の無線ＩＣタグ２０に商品購入済みフラグを書き込むと、その無線ＩＣタグ２０は、その後に最初にユーザの携帯端末装置１０から受信した正当ユーザコードＩＤ２を固定して記憶し、正当ユーザコード固定フラグＦＩＸを立て、それ以降は、正当ユーザコードＩＤ２のデータを更新しない様にする。

【０１３３】

これにより、商品を購入したユーザが、商品を開封しないでも、商品の購入者向けのコンテンツデータＣＮＤを受信することができる効果がある

【０１３４】

変形例５では、以上の処理のステップＳ１６、Ｓ２０を以下のステップＳ１６ａ、Ｓ２０ａに変えて処理する。

【０１３５】

（ステップＳ１６ａ）

ステップＳ１６ａにおいて、携帯端末装置１０は、無線ＩＣタグ２０の開封フラグＯＰＦと正当ユーザコード固定フラグＦＩＸをチェックするとともに、無線ＩＣタグ２０の商品購入済みフラグが立っているかどうかをチェックする。

【０１３６】
（ステップＳ２０ａ）
ステップＳ２０ａにおいて、無線ＩＣタグ２０は、無線ＩＣタグ２０の開封フラグＯＰＦが「商品開封済み」である（開封フラグが立っている）場合、又は、商品購入済みフラグが立っている場合は、正当ユーザコード固定フラグＦＩＸを立てて無線ＩＣタグ情報記憶手段２３に記憶する。これ以降は、無線ＩＣタグ２０は、正当ユーザコードＩＤ２の記憶を固定する。次にステップＳ２１に進む。
【０１３７】
変形例５は、これにより、商品が開封された後、及び、無線ＩＣタグ２０に商品購入済みフラグが書き込まれた後には、最初に正当ユーザコードＩＤ２の設定がされた後に、無線ＩＣタグ１０に正当ユーザコード固定フラグＦＩＸを立てて、それ以降は、無線ＩＣタグ２０の正当ユーザコードＩＤ２の記憶を固定する。
【０１３８】
（変形例６）
変形例６として、小売店で商品を販売した後に、小売店の小売店端末装置６０を用いて、流通情報管理サーバ３０に、商品の販売済み情報を送信し、商品の販売済みフラグＳＦを商品流通情報３１ａに記録させる。
【０１３９】
流通情報管理サーバ３０が、その商品の販売済みフラグＳＦを参照して、商品の販売前は、商品の真贋を判定するための商品の品質情報等に限ったコンテンツデータＣＮＤを携帯端末装置１０に送信する。
【０１４０】
そして、流通情報管理サーバ３０は、商品の販売後は、商品の販売済みフラグＳＦによってその商品の販売を確認した後に、ユーザの携帯端末装置１０に、新たな特典映像やその他の景品コンテンツを含む、商品の購入者向けのコンテンツデータＣＮＤを配信することができる。
【０１４１】
変形例６では、第１の実施形態の処理のステップＳ２４からＳ２８の処理を、以下のステップＳ２４ａからＳ２６ａの処理に変えて処理する。
【０１４２】
（ステップＳ２４ａ）
商品真贋判定手段１５が、流通情報管理サーバ３０に、商品真贋判定用コンテンツの配信要求を出す。
【０１４３】
（ステップＳ２５ａ）
流通情報管理サーバ３０は、商品流通情報３１ａに商品の販売済みフラグＳＦが立っているか否かを確認する。
【０１４４】
流通情報管理サーバ３０は、商品の販売済みフラグＳＦが立っている場合は、ユーザの携帯端末装置１０に、商品の購入者向けのワンタイムのコンテンツ復号鍵ＣＣｓを暗号化して送信する。
【０１４５】
このワンタイムのコンテンツ復号鍵ＣＣｓは、流通情報管理サーバ３０がユーザの携帯端末装置１０のメールアドレスＥｍａｉｌ宛てに問合せをしてユーザを確認した上で送信するようにすることもできる。
【０１４６】
（ステップＳ２６ａ）
次に、流通情報管理サーバ３０は、商品の販売済みフラグＳＦが立っている場合は、商品の購入者向けのコンテンツを暗号化したコンテンツデータＣＮＤを配信する。次に、ステップＳ２９に進む。

【０１４７】
流通情報管理サーバ３０は、商品の販売済みフラグＳＦが立っていない場合は、商品購入以前の一般の者向けの商品真贋判定用コンテンツを暗号化したコンテンツデータＣＮＤを配信する。次に、ステップＳ２９に進む。
【０１４８】
以上の、ステップＳ１０からＳ２９の処理により、無線ＩＣタグ２０と正当ユーザコードＩＤ２とを所持しているユーザに限って暗号化したコンテンツデータＣＮＤを配信する。そうすることで、商品の開封後には廃棄される可能性もある無線ＩＣタグ２０を所持しているだけでは、正当ユーザコードＩＤ２を持っていないユーザには景品コンテンツデータＣＮＤを配信することが無い、コンテンツの配信管理を適切に行える効果がある。
【０１４９】
（正当ユーザコードＩＤ２の移譲処理手順）
次に、図９のフローチャートを参照して、携帯端末装置１０が他の携帯端末装置１０ａに正当ユーザコードＩＤ２を移譲する処理手順を説明する。
【０１５０】
（ステップＳ３１）
正当ユーザコードＩＤ２の移譲先の携帯端末装置１０ａには、予め、商品真贋判定手段１５用の商品真贋判定アプリケーションプログラムを、ステップＳ１０の処理により設定する。
【０１５１】
（ステップＳ３２）
携帯端末装置１０の商品真贋判定手段１５は、ユーザの指示に従い、正当ユーザコードＩＤ２の移譲処理を開始し、移譲先の携帯端末装置１０ａに、正当ユーザコードＩＤ２を送信する。
【０１５２】
（ステップＳ３３）
移譲先の携帯端末装置１０ａの商品真贋判定手段１５は、受信した正当ユーザコードＩＤ２を記憶し、移譲完了通知を移譲元の携帯端末装置１０に返信する。また、その際に、流通情報管理サーバ３０に登録されていたユーザの携帯端末装置のメールアドレスＥｍａｉｌ等のユーザに固有な情報を、移譲先のユーザに固有な情報に更新する。
【０１５３】
（ステップＳ３４）
移譲元の携帯端末装置１０の商品真贋判定手段１５は、移譲先の携帯端末装置１０ａから移譲完了通知を受信した場合は、所定時間の経過後に、正当ユーザコードＩＤ２の記憶を消去して移譲を終了させる。
【０１５４】
正当ユーザコードＩＤ２を共有している複数の携帯端末装置１０がコンテンツデータＣＮＤを受信できる。あるいは、商品が未開封の場合には、任意の携帯端末装置１０がコンテンツデータＣＮＤを受信できる。それらの携帯端末装置１０が流通情報管理サーバ３０に端末装置暗号化データＤＭＢを送信する毎に、流通情報管理サーバ３０が、その携帯端末装置１０にコンテンツデータＣＮＤを配信する。
【０１５５】
＜第２の実施形態＞
この発明の第２の実施形態による商品の真贋判定システムは、第１の実施形態と同様に図１のブロック構成図であらわすことができ、携帯端末装置１０と、商品に添付した無線ＩＣタグ２０と、通信ネットワーク１００で接続した流通情報管理サーバ３０で構成する。以下で図１０から図１６を参照して、本発明の第２の実施形態を説明する。
【０１５６】
（システム構成）
第２の実施形態が第１の実施形態と相違する点は、図１１の様に、商品に添付する無線

ＩＣタグ２０が無線タグ暗号化データ作成手段２４を持ち、暗号鍵記憶手段２５を持つ点である。第２の実施形態では、無線ＩＣタグ２０が無線タグ暗号化データ作成手段２４を用いて、無線ＩＣタグ２０内で暗号化した無線タグ暗号化データＤＴＧを作成する。

【０１５７】

第２の実施形態では、無線ＩＣタグ２０自身が無線タグ暗号化データ作成手段２４を用いて暗号化するので、暗号通信のセキュリティを高くできる効果がある。

【０１５８】

第２の実施形態は、流通情報管理サーバ３０が、無線タグ暗号化データＤＴＧを作成する無線ＩＣタグ２０を直接に認証することができるので、携帯端末装置１０に偽のアプリケーションプログラムがインストールされて構成された偽の商品真贋判定手段がその場に存在しない無線ＩＣタグ２０が存在するものと偽装する事を防ぐことができる効果がある。

【０１５９】

そのため、第２の実施形態では、流通情報管理サーバ３０が、携帯端末装置１０の商品真贋判定手段１５を、それに内在させたプログラムの正当性検証プログラムによって検証する処理を省略することができる効果がある。それにより、商品真贋判定手段１５を構成するために携帯端末装置１０にインストールするアプリケーションプログラムの規模を小さくできる効果がある。

【０１６０】

（携帯端末装置１０）

携帯端末装置１０は図１０の様に構成する。携帯端末装置１０は、第１の実施形態と同様に、近距離無線通信手段１１と遠距離無線通信手段１２と、暗号鍵記憶手段１３と、時計機能部のような乱数成分発生部１４と、記憶手段に記憶した商品真贋判定アプリケーションプログラムで構成する商品真贋判定手段１５を有する。

【０１６１】

（商品真贋判定手段１５）

第２の実施形態の携帯端末装置１０の商品真贋判定手段１５は、プログラムの正当性検証プログラムを省略できる。

【０１６２】

（端末装置暗号化データＤＭＢ）

第２の実施形態の携帯端末装置１０の商品真贋判定手段１５は、流通情報管理サーバ３０に送信するために作成する端末装置暗号化データＤＭＢの内容に、無線ＩＣタグ２０のタグＩＤ番号ＩＤ１を入れない。線ＩＣタグ２０のタグＩＤ番号ＩＤ１は、無線ＩＣタグ２０内で暗号化した無線タグ暗号化データＤＴＧに情報が格納されて流通情報管理サーバ３０に送信する。そのため、携帯端末装置１０には無線ＩＣタグ２０のタグＩＤ番号ＩＤ１は知らされない。

【０１６３】

第２の実施形態では、商品真贋判定手段１５は、端末装置暗号化データＤＭＢの内容に、携帯端末装置１０が記憶する正当ユーザコードＩＤ２を格納して流通情報管理サーバ３０に送信する。

【０１６４】

商品真贋判定手段１５が作成する端末装置暗号化データＤＭＢは、乱数成分ｔと、正当ユーザコードＩＤ２と、ユーザに追加入力されたメールアドレスＥｍａｉｌ等の追加ユーザ情報を合わせたデータを、タグＩＤ番号暗号鍵Ｗｓで暗号化して作成する。

【０１６５】

ここで、携帯端末装置１０が端末装置暗号化データＤＭＢを作成するために用いる、暗号鍵記憶手段１３に記憶する暗号鍵を、無線ＩＣタグ２０が無線タグ暗号化データＤＴＧを作成するために用いるタグＩＤ番号暗号鍵Ｗｓと同じ暗号鍵にした場合を示した。

【０１６６】

しかし、携帯端末装置１０が端末装置暗号化データＤＭＢを作成するために用いる暗号

鍵は、無線ＩＣタグ２０が用いるタグＩＤ番号暗号鍵Ｗｓと異なる暗号鍵を使うこともできる。携帯端末装置１０と無線ＩＣタグ２０の暗号鍵を異ならせることで、暗号通信のセキュリティをより高くできる効果がある。

【０１６７】

（正当ユーザコードＩＤ２の照合チェック）

本実施形態でも第１の実施形態と同様に、携帯端末装置１０の商品真贋判定手段１５は、無線ＩＣタグ２０の記憶する正当ユーザコードＩＤ２と自身の記憶する正当ユーザコードＩＤ２の照合チェックを行うが、この処理は以下の理由により、省略することができる。

【０１６８】

すなわち、流通情報管理サーバ３０が、携帯端末装置１０での照合チェックにかかわらず、無線ＩＣタグ２０の記憶する正当ユーザコードＩＤ２を無線タグ暗号化データＤＴＧから取得し、携帯端末装置１０の記憶する正当ユーザコードＩＤ２を端末装置暗号化データＤＭＢから取得し、両者の正当ユーザコードＩＤ２を流通情報管理サーバ３０が照合チェックすることを主要な照合チェックとする。

【０１６９】

流通情報管理サーバ３０が、無線ＩＣタグ２０の記憶する正当ユーザコードＩＤ２と、携帯端末装置１０の記憶する正当ユーザコードＩＤ２を照合チェックする。これにより、携帯端末装置１０に偽の商品真贋判定手段１５が格納されて、そのプログラムが偽の照合チェックの判定をしても、その判定にかかわらず、流通情報管理サーバ３０が、無線ＩＣタグ２０と携帯端末装置１０の記憶する正当ユーザコードＩＤ２を正しく照合チェックする。

【０１７０】

そのため、第２の実施形態では、商品真贋判定手段１５による、無線ＩＣタグ２０の記憶する正当ユーザコードＩＤ２と自身の記憶する正当ユーザコードＩＤ２の照合チェック処理を省略することもできる。

【０１７１】

（無線ＩＣタグ２０）

本実施形態の無線ＩＣタグ２０は、図１１の様に、ＮＦＣ通信や無線ＬＡＮ等の近距離無線通信手段２１と、商品開封検知手段２２と、無線ＩＣタグ情報記憶手段２３と、無線タグ暗号化データ作成手段２４と、暗号鍵記憶手段２５を有する。

【０１７２】

（暗号鍵記憶手段２５）

無線ＩＣタグ２０の暗号鍵記憶手段２５は、タグＩＤ番号暗号鍵Ｗｓを記憶する。無線タグ暗号化データ作成手段２４が、そのタグＩＤ番号暗号鍵Ｗｓを用いて暗号化した無線タグ暗号化データＤＴＧを作成して携帯端末装置１０と通信ネットワーク１００を介して、流通情報管理サーバ３０に送信する。

【０１７３】

このタグＩＤ番号暗号鍵Ｗｓは、商品に無線ＩＣタグ２０を取り付ける際に、拠点端末装置５０が、リーダライタによって無線ＩＣタグ２０に書き込んでおく。

【０１７４】

無線ＩＣタグ２０に最初からタグＩＤ番号暗号鍵Ｗｓを記憶させることにより、無線ＩＣタグ２０に偽の暗号鍵が記憶させられて無線ＩＣタグ２０の暗号化データが不正に読み取られて不正に使用される問題を避けることができる。

【０１７５】

また、このタグＩＤ番号暗号鍵Ｗｓは、携帯端末装置１０が暗号化通信に用いる暗号鍵と異なる暗号鍵を使うこともできる。それにより、暗号通信のセキュリティをより高くできる効果がある。

【０１７６】

（無線タグ暗号化データＤＴＧ）

無線ＩＣタグ２０の無線タグ暗号化データ作成手段２４は、タグＩＤ番号暗号鍵Ｗｓで暗号化した無線タグ暗号化データＤＴＧを作成して、携帯端末装置１０と通信ネットワーク１００を介して、流通情報管理サーバ３０に送信する。

【０１７７】

この無線タグ暗号化データＤＴＧは、無線ＩＣタグ２０が携帯端末装置１０から受信した時刻データ等の乱数成分ｔと、タグＩＤ番号ＩＤ１と、正当ユーザコードＩＤ２と、開封フラグＯＰＦと正当ユーザコード固定フラグＦＩＸのデータを合わせたデータを、タグＩＤ番号暗号鍵Ｗｓで暗号化して作成する。

【０１７８】

（流通情報管理サーバ３０）

第２の実施形態の流通情報管理サーバ３０も、第１の実施形態と同様に構成する。流通情報管理サーバ３０は、図１２に示すように、タグＩＤ番号データベース３１と、商品種別データベース３２と、暗号鍵記憶部３３と、サーバ側同期乱数発生部３４と、正当ユーザコード照合手段３５と、コンテンツ配信部４０を有する。

【０１７９】

（サーバ側同期乱数発生部３４）

サーバ側同期乱数発生部３４は、携帯端末装置１０の乱数成分発生部１４と同期する乱数を発生する。サーバ側同期乱数発生部３４と携帯端末装置１０の乱数成分発生部１４を時計機能にし、時刻データを乱数成分ｔとすることができる。

【０１８０】

（変形例７）

変形例７として、流通情報管理サーバ３０のサーバ側同期乱数発生部３４が作成した乱数成分ｔを携帯端末装置１０の乱数成分発生部１４が受信して使うこともできる。そうすると、流通情報管理サーバ３０が、携帯端末装置１０から送信された、無線タグ暗号化データＤＴＧ及び端末装置暗号化データＤＭＢをより確実に認証することができる効果がある。

【０１８１】

流通情報管理サーバ３０は、無線ＩＣタグ２０が作成した無線タグ暗号化データＤＴＧ及び携帯端末装置１０が作成した端末装置暗号化データＤＭＢを受信すると、タグＩＤ番号暗号用秘密鍵Ｃｓを用いて復号し、復号して得たデータに一致する商品流通情報３１ａが存在する場合に、それぞれの暗号化データに応じた処理を行う。

【０１８２】

（正当ユーザコード照合手段３５）

流通情報管理サーバ３０の正当ユーザコード照合手段３５は、無線ＩＣタグ２０が作成した無線タグ暗号化データＤＴＧの含む正当ユーザコードＩＤ２と端末装置暗号化データＤＭＢの含む正当ユーザコードＩＤ２を照合し、両データが異なる場合は、ユーザを認証せず、処理を終了する。

【０１８３】

この様に、流通情報管理サーバ３０が、無線タグ暗号化データＤＴＧを受信することで、無線ＩＣタグ２０の記憶する正当ユーザコードＩＤ２を、携帯端末装置１０の記憶する正当ユーザコードＩＤ２と直接比較して携帯端末装置１０を認証することができる。

【０１８４】

それにより、流通情報管理サーバ３０が、携帯端末装置１０にインストールされた偽の商品真贋判定手段による嘘の正当ユーザコードＩＤ２の判定結果により欺かれる危険が無い効果がある。

【０１８５】

（商品の真贋判定システムの動作手順）

第２の実施形態の商品の真贋判定システムの動作手順は、図１３から図１６のフローチャートに従う。

【０１８６】

（流通情報管理サーバ３０への無線ＩＣタグ２０の登録処理手順）
流通情報管理サーバ３０への無線ＩＣタグ２０の登録処理手順は、第１の実施形態と同様に、図５のフローチャートに従う。
【０１８７】
（ユーザによる商品の真贋判定処理手順）
次に、図１３から図１６のフローチャートを参照して、第２の実施形態の商品の真贋判定処理手順を説明する。
【０１８８】
（ステップＳ４０）
商品真贋判定アプリケーションプログラムのインストール。
携帯端末装置１０は、流通情報管理サーバ３０から、商品真贋判定アプリケーションプログラムと、タグＩＤ番号暗号鍵Ｗｓを受信し、インストールして商品真贋判定手段１５を構成する。
【０１８９】
（ステップＳ４１）
携帯端末装置１０の商品真贋判定手段１５は、無線ＩＣタグ２０に、無線タグ暗号化データＤＴＧ要求コマンドと、携帯端末装置１０の乱数成分発生部１４の出力した時刻データ等の乱数成分ｔを送信する。
【０１９０】
（ステップＳ４２）
無線タグ暗号化データＤＴＧ要求コマンドを受信した無線ＩＣタグ２０は、無線タグ暗号化データ作成手段２４により、無線タグ暗号化データＤＴＧを作成し、携帯端末装置１０に送信する。
【０１９１】
無線タグ暗号化データＤＴＧは、携帯端末装置１０から受信した時刻データ等の乱数成分ｔに、タグＩＤ番号ＩＤ１と正当ユーザコードＩＤ２と、開封フラグＯＰＦと正当ユーザコード固定フラグＦＩＸのデータを合わせたデータを、タグＩＤ番号暗号鍵Ｗｓで暗号化して作成する。無線タグ暗号化データＤＴＧは、そのデータを作成する時刻での送信のみに適用される、毎回異なる暗号化データになる。
【０１９２】
なお、ステップＳ４２で作成する無線タグ暗号化データＤＴＧは、その内容に、少なくとも、乱数成分ｔに、タグＩＤ番号ＩＤ１が存在すれば十分であり、その内容から、正当ユーザコードＩＤ２と、開封フラグＯＰＦと正当ユーザコード固定フラグＦＩＸを省略することもできる。
【０１９３】
この様に、無線ＩＣタグ２０が、無線タグ暗号化データＤＴＧ内にタグＩＤ番号ＩＤ１を暗号化させて含ませて、携帯端末装置１０を介して流通情報管理サーバ３０に通知する。これにより、流通情報管理サーバ３０以外の携帯端末装置１０にはタグＩＤ番号ＩＤ１を知らせないことで、タグＩＤ番号ＩＤ１が悪意のある者に知られて無線ＩＣタグ２０が偽装される問題を避けることができる効果がある。
【０１９４】
（ステップＳ４３）
携帯端末装置１０の商品真贋判定手段１５は、無線ＩＣタグ２０と通信できない場合は、無線ＩＣタグ２０が存在しないとして、不正商品としてエラー終了する。この場合、無線ＩＣタグ２０が壊れている場合や何らかの通信エラーにより読み出せない場合もあり得るが、特に考慮せず不正として扱い、処理を終了する。
【０１９５】
（ステップＳ４４）
次に、携帯端末装置１０の商品真贋判定手段１５は、流通情報管理サーバ３０と通信して、携帯端末装置１０を流通情報管理サーバ３０に認証させる。流通情報管理サーバ３０

は、認証した携帯端末装置１０との間に、セキュア・ソケット・レイヤ（Secure Socket Layer：ＳＳＬ）等の暗号化通信の体制を整える。

【０１９６】

（ステップＳ４５）

携帯端末装置１０の商品真贋判定手段１５は、無線ＩＣタグ２０から受信した無線タグ暗号化データＤＴＧを流通情報管理サーバ３０に送信する。

【０１９７】

（ステップＳ４６）

流通情報管理サーバ３０は、受信した無線タグ暗号化データＤＴＧを復号し、タグＩＤ番号ＩＤ１を取り出す。そして、流通情報管理サーバ３０のタグＩＤ番号データベース３１を検索して、そのタグＩＤ番号ＩＤ１を記録した商品流通情報３１ａの有無の確認を行う。

【０１９８】

（ステップＳ４７）

流通情報管理サーバ３０は、タグＩＤ番号データベース３１から、タグＩＤ番号ＩＤ１を記録した商品流通情報３１ａを抽出できた場合は、その無線ＩＣタグ２０を正当なものと判定し、それが張り付いている商品を正当な商品であると判定する。その商品流通情報３１ａを抽出できなかった場合は、携帯端末装置１０の商品真贋判定手段１５の処理を終了させる。

【０１９９】

（ステップＳ４８）

流通情報管理サーバ３０から、無線ＩＣタグ２０を正当なものと判定した判定結果を受信した携帯端末装置１０の商品真贋判定手段１５は、無線ＩＣタグ２０と通信して、無線ＩＣタグ２０の開封フラグＯＰＦと正当ユーザコード固定フラグＦＩＸをチェックする。

【０２００】

（ステップＳ４９からＳ５５）

第１の実施形態のステップＳ１７からＳ２３と同じ処理により、携帯端末装置１０の商品真贋判定手段１５が正当ユーザコードＩＤ２を生成し、無線ＩＣタグ２０に送信する処理を行う。また、無線ＩＣタグ２０は、正当ユーザコードＩＤ２を記憶する処理と、開封フラグＯＰＦが立っている場合は、正当ユーザコード固定フラグＦＩＸを立てる処理を行う。

【０２０１】

（ステップＳ５６）

次に、商品真贋判定手段１５が、無線ＩＣタグ２０の正当ユーザコード固定フラグＦＩＸが立っているかどうかをチェックする。

【０２０２】

（ステップＳ５７）

携帯端末装置１０の商品真贋判定手段１５は、正当ユーザコード固定フラグＦＩＸが立っている場合は、商品真贋判定手段１５は、流通情報管理サーバ３０に追加して登録する、ユーザの携帯端末装置のメールアドレスＥｍａｉｌ等のユーザ情報を入力することができる。

【０２０３】

（ステップＳ５８）

携帯端末装置１０の商品真贋判定手段１５は、無線ＩＣタグ２０に、無線タグ暗号化データＤＴＧ要求コマンドと、携帯端末装置１０の乱数成分発生部１４の出力した時刻データ等の乱数成分ｔを送信する。この乱数成分ｔは、流通情報管理サーバ３０のサーバ側同期乱数発生部３４が作成した乱数成分ｔを携帯端末装置１０の乱数成分発生部１４が受信して使うこともできる。

【０２０４】

（ステップＳ５９）

無線タグ暗号化データＤＴＧ要求コマンドを受信した無線ＩＣタグ２０は、無線タグ暗号化データ作成手段２４により、無線タグ暗号化データＤＴＧを作成し、携帯端末装置１０に送信する。

【０２０５】

ステップＳ５９で作成する無線タグ暗号化データＤＴＧは、携帯端末装置１０から受信した時刻データ等の乱数成分ｔに、タグＩＤ番号ＩＤ１と正当ユーザコードＩＤ２と、開封フラグＯＰＦと正当ユーザコード固定フラグＦＩＸのデータを合わせたデータを、タグＩＤ番号暗号鍵Ｗｓで暗号化して作成する。無線タグ暗号化データＤＴＧは、そのデータを作成する時刻での送信のみに適用される、毎回異なる暗号化データになる。

【０２０６】

（ステップＳ６０）

携帯端末装置１０は、端末装置暗号化データＤＭＢを作成する。端末装置暗号化データＤＭＢは、携帯端末装置１０が、乱数成分ｔと、正当ユーザコードＩＤ２と、ユーザに追加入力されたメールアドレスＥｍａｉｌ等の追加ユーザ情報を合わせたデータを、タグＩＤ番号暗号鍵Ｗｓで暗号化して作成する。この端末装置暗号化データＤＭＢは、このデータを作成する時刻での送信のみに適用される、毎回異なる暗号化データになる。

【０２０７】

携帯端末装置１０は、携帯端末装置１０が作成した端末装置暗号化データＤＭＢを、無線ＩＣタグ２０から受信した無線タグ暗号化データＤＴＧと一緒に流通情報管理サーバ３０に送信する。

【０２０８】

（ステップＳ６１）

流通情報管理サーバ３０は、無線タグ暗号化データＤＴＧと端末装置暗号化データＤＭＢを受信すると、両暗号化データをタグＩＤ番号暗号用秘密鍵Ｃｓを用いて復号する。

【０２０９】

（ステップＳ６２）

流通情報管理サーバ３０は、復号した無線タグ暗号化データＤＴＧと端末装置暗号化データＤＭＢの、時刻データによる乱数成分ｔがサーバ側同期乱数発生部３４の出力する時刻データと整合しない不適切な乱数成分ｔである場合は、ユーザを認証せず、処理を終了する。

【０２１０】

乱数成分ｔが適切な場合は、流通情報管理サーバ３０の正当ユーザコード照合手段３５が、復号した無線タグ暗号化データＤＴＧの正当ユーザコードＩＤ２と端末装置暗号化データＤＭＢの正当ユーザコードＩＤ２を照合し、両データが異なる場合は、ユーザを認証せず、処理を終了する。

【０２１１】

なお、流通情報管理サーバ３０は、復号した端末装置暗号化データＤＭＢに、ユーザに追加入力されたメールアドレスＥｍａｉｌ等の追加ユーザ情報がある場合は、その追加ユーザ情報を商品流通情報３１ａに記憶させる。

【０２１２】

（ステップＳ６３）

次に、流通情報管理サーバ３０は、復号した無線タグ暗号化データＤＴＧの通知した正当ユーザコード固定フラグＦＩＸが立っているかどうかをチェックする。

【０２１３】

（ステップＳ６４）

流通情報管理サーバ３０は、正当ユーザコード固定フラグＦＩＸが立っていない場合は、ユーザの携帯端末装置１０に、一般者向けのワンタイムのコンテンツ復号鍵ＣＣｓを暗号化して送信する。

【０２１４】

（ステップＳ６５）

流通情報管理サーバ３０は、正当ユーザコード固定フラグＦＩＸが立っている場合は、タグＩＤ番号データベース３１の、商品流通情報３１ａに、商品の販売済みフラグＳＦを立てて記憶する。また、通情報管理サーバ３０は、ユーザの携帯端末装置１０に、商品の購入者向けのワンタイムのコンテンツ復号鍵ＣＣｓを暗号化して送信する。

【０２１５】

この商品の購入者向けのワンタイムのコンテンツ復号鍵ＣＣｓは、流通情報管理サーバ３０がユーザの携帯端末装置１０のメールアドレスＥｍａｉｌ宛てに問合せをしてユーザを確認した上で送信するようにすることもできる。

【０２１６】

（ステップＳ６６）

次に、流通情報管理サーバ３０は、暗号化したコンテンツデータＣＮＤを配信する。商品流通情報３１ａに商品の販売済みフラグＳＦが立っている場合は、商品の購入者向けの暗号化されたコンテンツデータＣＮＤを配信し、商品の販売済みフラグＳＦが立っていない場合は、一般者向けの暗号化されたコンテンツデータＣＮＤを配信する。

【０２１７】

（変形例８）

変形例８として、流通情報管理サーバ３０は、暗号化されたコンテンツデータＣＮＤを商品流通情報３１ａが記憶している携帯端末装置１０のメールアドレスＥｍａｉｌ宛てに送信することができる。

【０２１８】

（ステップＳ６７）

携帯端末装置１０は、暗号化されたたコンテンツデータＣＮＤをコンテンツ復号鍵ＣＣｓを用いて復号してユーザに視聴させる。

【０２１９】

コンテンツデータＣＮＤは暗号化されており、正当なコンテンツ復号鍵ＣＣｓを受信しなかった携帯端末装置１０ではコンテンツを視聴できない。

【０２２０】

（正当ユーザコードＩＤ２の移譲処理手順）

第２の実施形態における、携帯端末装置１０と携帯端末装置１０ａの間での正当ユーザコードＩＤ２の移譲処理は、第１の実施形態と同様に、図９のフローチャートの手順で行う。

【０２２１】

なお、本発明は、以上の実施形態に限定されず、正当ユーザコードＩＤ２を無線ＩＣタグ２０に固定して記憶させる以前には、携帯端末装置１０の商品真贋判定手段１５の処理は、正当ユーザコードＩＤ２を作成せず、正当ユーザコードＩＤ２を照合チェックをしない様にすることもできる。

【０２２２】

そして、無線ＩＣタグ２０の商品開封検知手段２２が商品の開封を検知して開封フラグＯＰＦを立てた場合に、携帯端末装置１０の商品真贋判定手段１５が正当ユーザコードＩＤ２を作成して、無線ＩＣタグ２０に固定して記憶させて無線ＩＣタグ２０に正当ユーザコード固定フラグＦＩＸを立たせる。それ以降は携帯端末装置１０と無線ＩＣタグ２０の記憶する正当ユーザコードＩＤ２を照合チェックする。

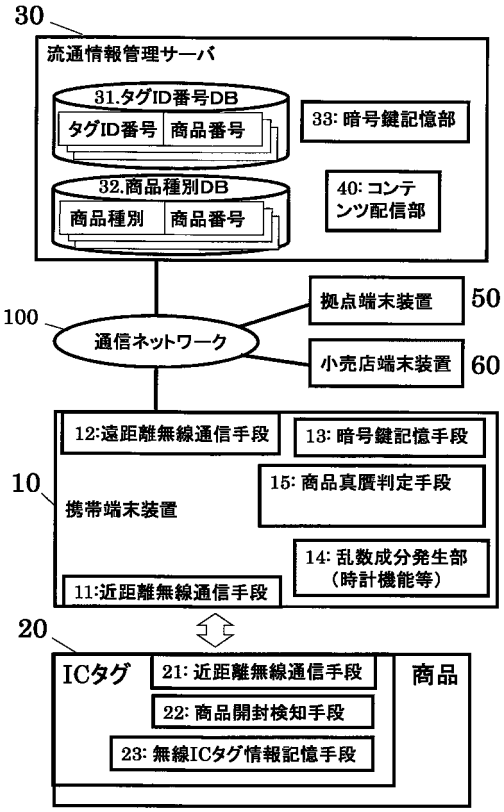
【符号の説明】

【０２２３】

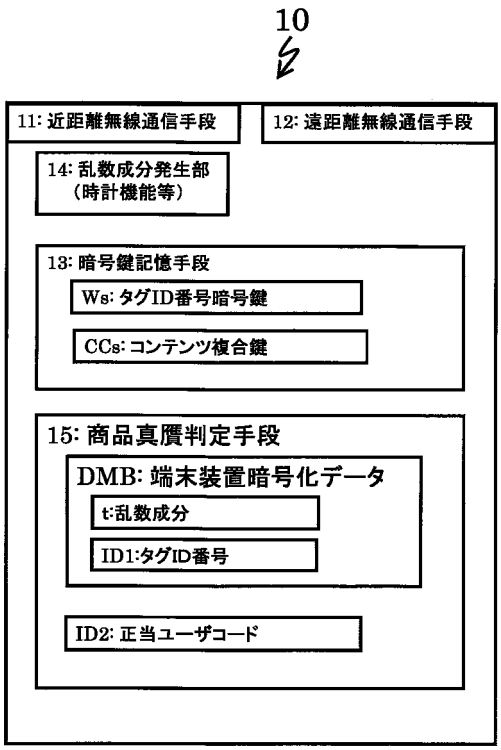
１０、１０ａ・・・携帯端末装置
１１・・・近距離無線通信手段
１２・・・遠距離無線通信手段
１３・・・暗号鍵記憶手段
１４・・・乱数成分発生部
１５・・・商品真贋判定手段

２０・・・無線ＩＣタグ
２１・・・近距離無線通信手段
２２・・・商品開封検知手段
２３・・・無線ＩＣタグ情報記憶手段
２４・・・無線タグ暗号化データ作成手段
２５・・・暗号鍵記憶手段
３０・・・流通情報管理サーバ
３１・・・タグＩＤ番号データベース
３１ａ・・・商品流通情報
３２・・・商品種別データベース
３３・・・暗号鍵記憶部
３４・・・サーバ側同期乱数発生部
３５・・・正当ユーザコード照合手段
４０・・・コンテンツ配信部
５０・・・拠点端末装置
６０・・・小売店端末装置
１００・・・通信ネットワーク
ＣＮＤ・・・コンテンツデータ
ＣＣｓ・・・コンテンツ復号鍵
Ｃｓ・・・タグＩＤ番号暗号用秘密鍵
ＤＭＢ・・・端末装置暗号化データ
ＤＴＧ・・・無線タグ暗号化データ
Ｅｍａｉｌ・・・携帯端末装置のメールアドレス
ＦＩＸ・・・正当ユーザコード固定フラグ
ＩＤ１・・・タグＩＤ番号
ＩＤ２・・・正当ユーザコード
ＮＰ・・・商品番号
ＯＰＦ・・・開封フラグ
ＳＦ・・・商品の販売済みフラグ
ｔ・・・乱数成分
Ｗｓ・・・タグＩＤ番号暗号鍵

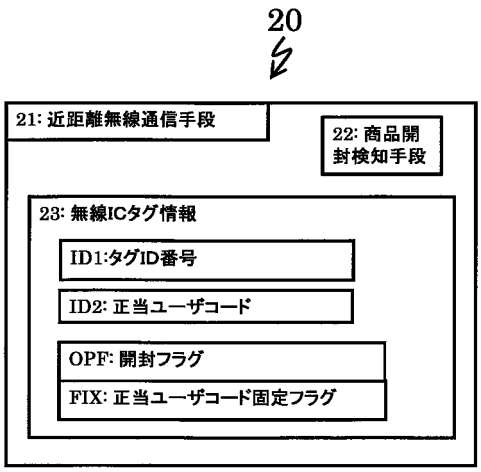
【図１】


30
流通情報管理サーバ
31.タグID番号DB
タグID番号
商品番号
33: 暗号鍵記憶部
32.商品種別DB
商品種別
商品番号
40: コンテンツ配信部
100
通信ネットワーク
拠点端末装置
50
小売店端末装置
60
12:遠距離無線通信手段
13: 暗号鍵記憶手段
10
携帯端末装置
15: 商品真贋判定手段
14: 乱数成分発生部（時計機能等）
11:近距離無線通信手段
20
ICタグ
21: 近距離無線通信手段
22: 商品開封検知手段
23: 無線ICタグ情報記憶手段
商品

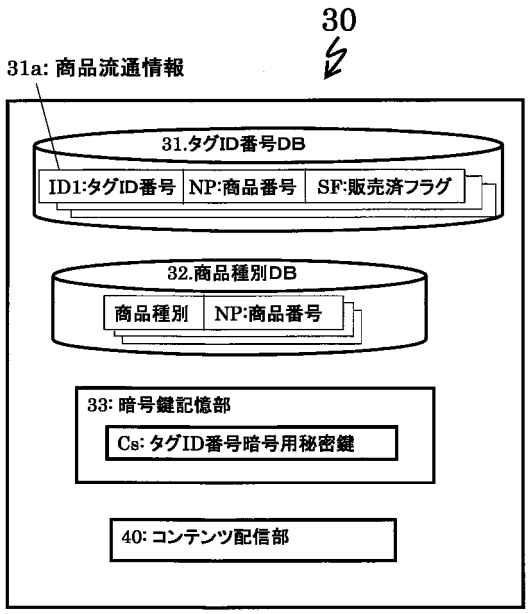
【図２】


10
11: 近距離無線通信手段
12: 遠距離無線通信手段
14: 乱数成分発生部（時計機能等）
13: 暗号鍵記憶手段
Ws: タグID番号暗号鍵
CCs: コンテンツ複合鍵
15: 商品真贋判定手段
DMB: 端末装置暗号化データ
t:乱数成分
ID1:タグID番号
ID2: 正当ユーザコード

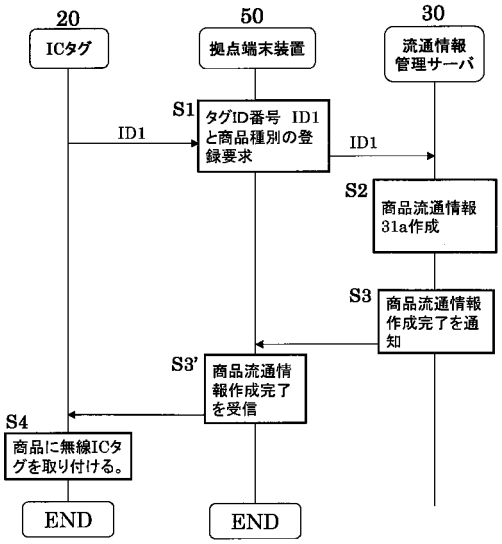
【図３】


20
21: 近距離無線通信手段
22: 商品開封検知手段
23: 無線ICタグ情報
ID1:タグID番号
ID2: 正当ユーザコード
OPF: 開封フラグ
FIX: 正当ユーザコード固定フラグ

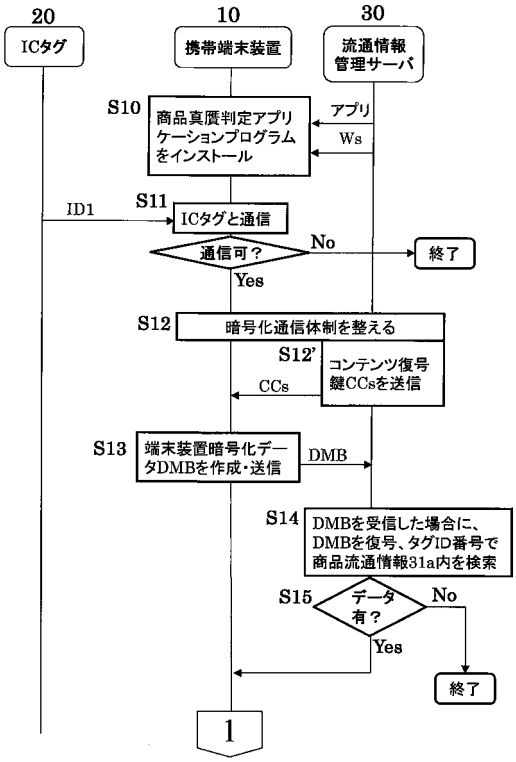
【図４】


30
31a: 商品流通情報
31.タグID番号DB
ID1:タグID番号
NP:商品番号
SF:販売済フラグ
32.商品種別DB
商品種別
NP:商品番号
33: 暗号鍵記憶部
Cs: タグID番号暗号用秘密鍵
40: コンテンツ配信部

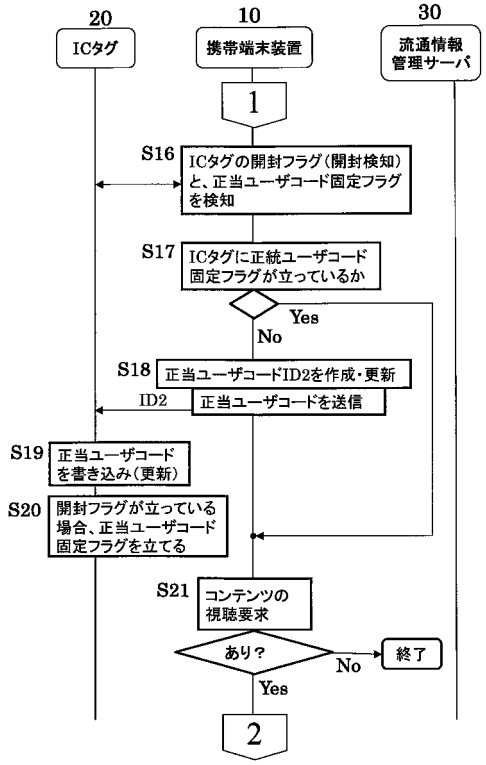
【図５】


20
ICタグ
50
拠点端末装置
30
流通情報管理サーバ
S1
タグID番号 ID1と商品種別の登録要求
ID1
ID1
S2
商品流通情報31a作成
S3
商品流通情報作成完了を通知
S3'
商品流通情報作成完了を受信
S4
商品に無線ICタグを取り付ける。
END
END

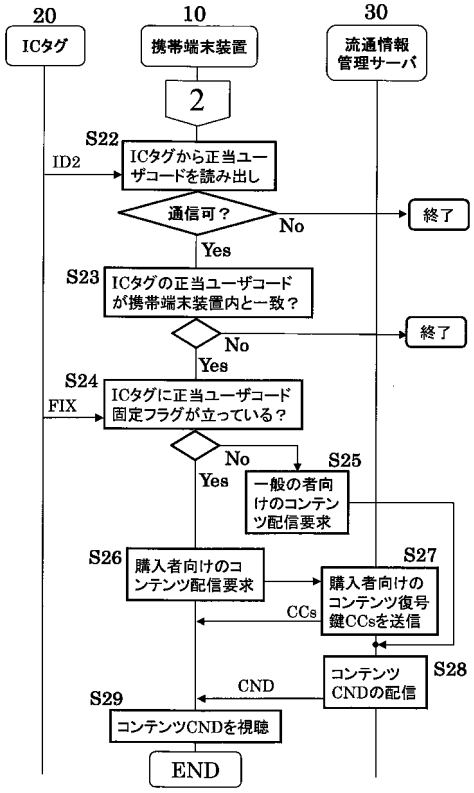
【図６】


20
ICタグ
10
携帯端末装置
30
流通情報管理サーバ
S10
商品真贋判定アプリケーションプログラムをインストール
アプリ
Ws
ID1
S11
ICタグと通信
通信可？
No
終了
Yes
S12
暗号化通信体制を整える
S12'
コンテンツ復号鍵CCsを送信
CCs
S13
端末装置暗号化データDMBを作成・送信
DMB
S14
DMBを受信した場合に、DMBを復号、タグID番号で商品流通情報31a内を検索
S15
データ有？
No
Yes
終了
1

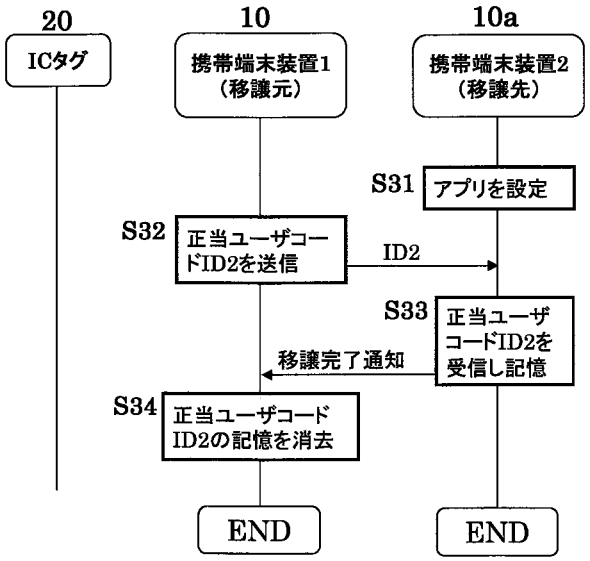
【図７】


20
ICタグ
10
携帯端末装置
30
流通情報管理サーバ
1
S16
ICタグの開封フラグ（開封検知）と、正当ユーザコード固定フラグを検知
S17
ICタグに正統ユーザコード固定フラグが立っているか
Yes
No
S18
正当ユーザコードID2を作成・更新
ID2
正当ユーザコードを送信
S19
正当ユーザコードを書き込み（更新）
S20
開封フラグが立っている場合、正当ユーザコード固定フラグを立てる
S21
コンテンツの視聴要求
あり？
No
終了
Yes
2

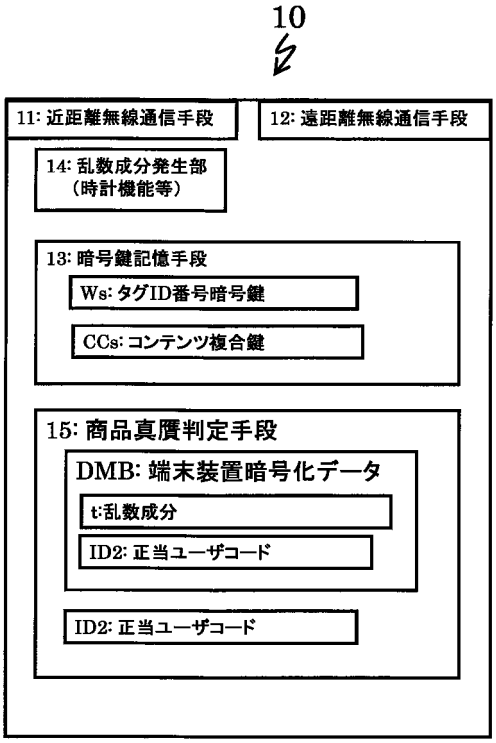
【図８】


20
ICタグ
10
携帯端末装置
30
流通情報管理サーバ
2
S22
ID2
ICタグから正当ユーザコードを読み出し
通信可？
No
終了
Yes
S23
ICタグの正当ユーザコードが携帯端末装置内と一致？
No
終了
Yes
S24
FIX
ICタグに正当ユーザコード固定フラグが立っている？
No
S25
Yes
一般の者向けのコンテンツ配信要求
S26
購入者向けのコンテンツ配信要求
S27
購入者向けのコンテンツ復号鍵CCsを送信
CCs
S28
コンテンツCNDの配信
CND
S29
コンテンツCNDを視聴
END

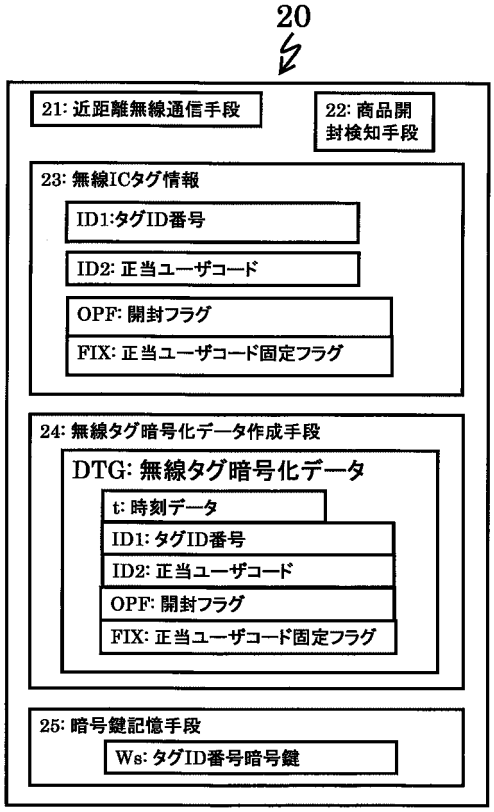
【図９】



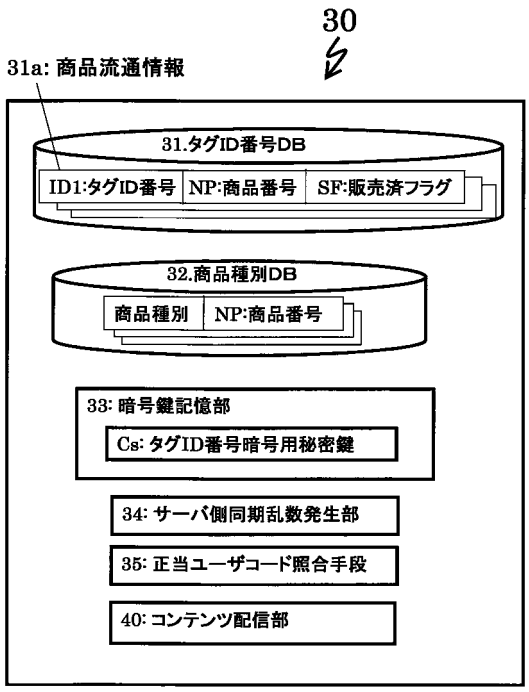
【図１０】



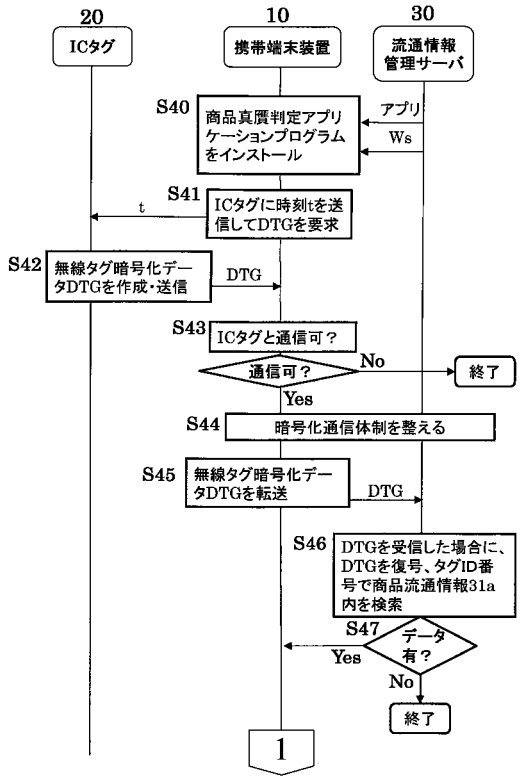
【図１１】



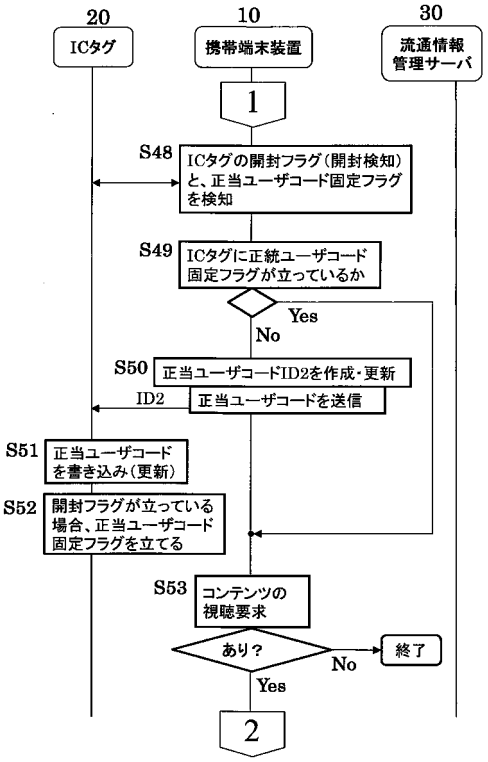
【図１２】



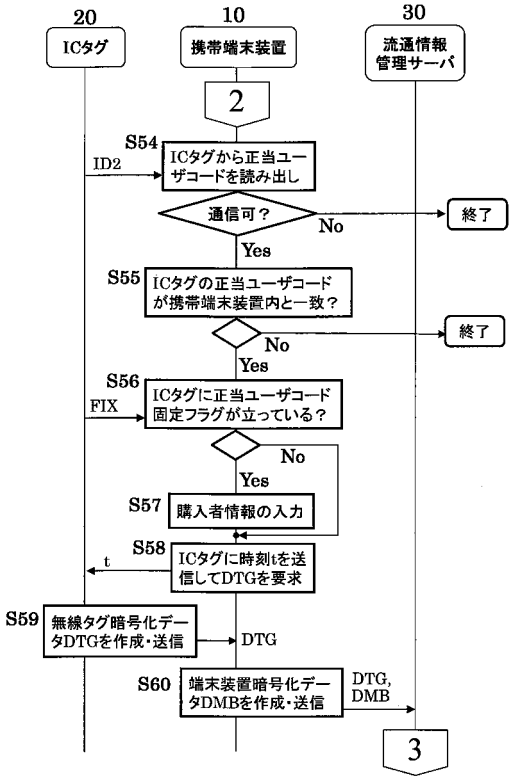
【図１３】



【図１４】



【図１５】



【図１６】