(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2004-30681
(P2004-30681A)
(43)公開日　平成16年1月29日(2004.1.29)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G06K 19/07	G06K 19/00	H	5B035
G06F 17/60	G06F 17/60	106	
	G06F 17/60	502	
	G06F 17/60	510	
	G06F 17/60	512	

審査請求 未請求　請求項の数 42　OL　（全 32 頁）

(21)出願番号　特願2003-207421(P2003-207421)
(22)出願日　平成15年8月13日(2003.8.13)
(62)分割の表示　特願2000-210689(P2000-210689)の分割
原出願日　平成12年7月6日(2000.7.6)

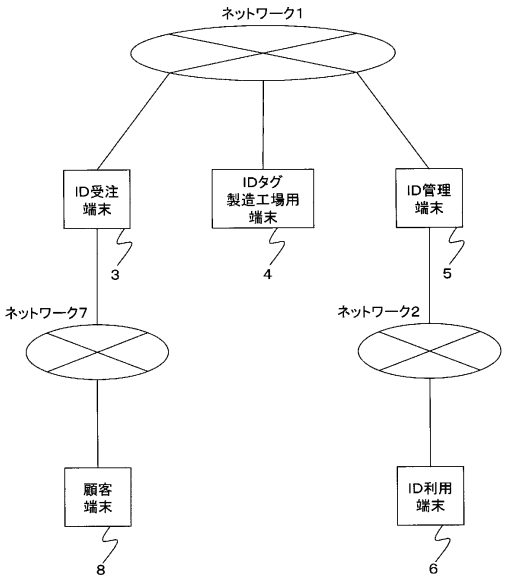
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(74)代理人　100075096
弁理士　作田　康夫
(72)発明者　岡本　周之
神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内
(72)発明者　宝木　和夫
神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内

最終頁に続く

(54)【発明の名称】ＩＤの管理方法及び管理システム

(57)【要約】
【課題】改竄検知符号を備えたＩＤの発行と流通を管理し、ＩＤを利用した物品管理を効率よく、かつ、信頼性高く行うことが可能な仕組みを提供する。
【解決手段】改竄検知符号を備えたＩＤを書き換え不可領域に格納した電子回路チップをＩＤタグとして用いる。ＩＤ受注端末とＩＤタグ製造工場用端末の情報をＩＤ管理端末に集約し、一括管理する。ＩＤ利用端末に機密性の高い情報を格納しておかなくてもいいように、前記情報をＩＤ管理端末に問い合わせる、または、前記情報の必要な処理をＩＤ管理端末に依頼する手段を構築する。
【選択図】　図３

図3



【特許請求の範囲】
【請求項１】
ＩＤ発行の受注を行なうＩＤ受注端末と、前記ＩＤが格納されたＩＤタグの製造を行なう製造工場用端末と、ネットワークを介して前記ＩＤ受注端末および製造工場用端末に接続されたＩＤ管理端末とを含むＩＤ管理システムを用いて、ＩＤの管理を行うＩＤ管理方法であって、
前記ＩＤタグには、外部からデータを読取り可能な電子回路チップが装着されており、
前記電子回路チップは、書き換え不可の記憶領域を有し、且つ当該領域に、外部から読取り可能なデータとして、受注したＩＤと、ＩＤの属性情報と、改竄検知符号、とを含む、拡張ＩＤを格納しており、
前記ＩＤ管理端末において、
前記ＩＤ受注端末から、前記拡張ＩＤを含む受注ＩＤ登録要求が送られてきた場合に、当該拡張ＩＤが登録済みであるとして、データベースに登録する受注ＩＤ登録ステップと、
前記製造工場用端末から、製造済みの前記ＩＤタグに格納されている前記拡張ＩＤを含む、製造済みＩＤ登録要求が送られてきた場合に、当該拡張ＩＤを格納した前記ＩＤタグが製造済みであるとして、前記データベースに登録する製造済みＩＤ登録ステップと、を有するＩＤ管理方法。
【請求項２】
請求項１記載のＩＤ管理方法であって、
前記ＩＤ管理端末において、
前記ＩＤ受注端末から、前記拡張ＩＤを含むＩＤ重複確認要求が送られてきた場合に、当該拡張ＩＤが受注済みであるとして前記データベースに登録されているか否かを調べ、その結果を前記ＩＤ受注端末に通知するＩＤ重複確認ステップをさらに有するＩＤ管理方法。
【請求項３】
請求項１記載のＩＤ管理方法であって、
前記ＩＤ管理端末において、
前記ＩＤタグ製造工場用端末から、前記ＩＤタグに格納されている前記拡張ＩＤを含む、欠番ＩＤ登録要求が送られてきた場合に、当該要求に含まれる拡張ＩＤが欠番ＩＤであるとして、前記データベースに登録する欠番ＩＤ登録ステップをさらに有するＩＤ管理方法。
【請求項４】
請求項１記載のＩＤ管理方法であって、
前記ＩＤ管理システムは、
ネットワークを介して前記ＩＤ管理端末に接続された、ＩＤ利用端末を含んでおり、
前記ＩＤ管理端末において、
前記ＩＤ利用端末から、前記拡張ＩＤを含む検証要求が送られてきた場合に、当該拡張ＩＤを、データベースに格納してある拡張ＩＤと比較し、送られてきた拡張ＩＤに含まれる前記改竄検知符号が正当か否かを検証する検証ステップをさらに有するＩＤ管理方法。
【請求項５】
請求項１記載のＩＤ管理方法であって、
前記ＩＤ管理システムは、
ネットワークを介して前記ＩＤ管理端末に接続された、ＩＤ利用端末を含んでおり、
前記ＩＤ管理端末において、
前記ＩＤ利用端末から、前記ＩＤの属性情報を含む検証用鍵要求が送られてきた場合に、当該属性情報と対応づけられてデータベースに格納してある、前記改竄検知符号の検証用の鍵を、前記ＩＤ利用端末に送信するステップをさらに有するＩＤ管理方法。
【請求項６】
請求項１記載のＩＤ管理方法であって、
前記ＩＤ管理システムは、

ネットワークを介して前記ＩＤ管理端末に接続された、ＩＤ利用端末を含んでおり、
前記ＩＤ管理端末において、
前記ＩＤ利用端末から、復号化用鍵要求が送られてきた場合に、データベースに格納してある、暗号化された拡張ＩＤの復号化用の鍵を、前記ＩＤ利用端末に送信するステップをさらに有するＩＤ管理方法。
【請求項７】
請求項１記載のＩＤ管理方法であって、
前記ＩＤ管理システムは、
ネットワーク２を介して前記ＩＤ管理端末に接続された、ＩＤ利用端末を含んでおり、
前記ＩＤ管理端末において、
前記ＩＤ利用端末から、前記拡張ＩＤを含む、失効ＩＤ登録要求が送られてきた場合に、当該要求に含まれる拡張ＩＤが失効ＩＤであるとして、前記データベースに登録する失効ＩＤ登録ステップをさらに有するＩＤ管理方法。
【請求項８】
請求項１記載のＩＤ管理方法であって、
前記ＩＤ管理システムは、
ネットワークを介して前記ＩＤ受注端末に接続された、顧客端末を含んでおり、
前記ＩＤ受注端末において、
前記顧客端末から、前記ＩＤタグを発注する顧客の情報と、前記ＩＤタグへの格納を希望するＩＤと、前記ＩＤの改竄検知符号を生成するための鍵と、を含む発注情報が送られてきた場合に、当該発注情報を用いて、前記ＩＤの属性情報と、前記改竄検知符号と、を生成し、前記拡張ＩＤを生成する拡張ＩＤ生成ステップと、前記顧客端末からの要求に応じて、前記発注情報と、前記拡張ＩＤと、を含む受注情報を送信するステップと、
前記受注情報を含む受注ＩＤ登録要求をＩＤ管理端末に送信する受注ＩＤ登録要求ステップと、
前記拡張ＩＤを含むＩＤタグ製造要求を前記ＩＤタグ製造工場用端末に送信するＩＤタグ製造要求ステップと、を有するＩＤ管理方法。
【請求項９】
請求項１記載のＩＤ管理方法であって、
前記ＩＤタグ製造工場用端末において、
前記ＩＤ受注端末から、前記拡張ＩＤを含むＩＤタグ製造要求が送られてきた場合に、前記ＩＤタグを製造させるステップと、
製造された前記ＩＤタグを検査させるステップと,
前記検査ステップの結果が合格の場合に、前記ＩＤタグに格納されている前記拡張ＩＤを含む、製造済みＩＤ登録要求を前記ＩＤ管理端末に送信する製造済みＩＤ登録要求ステップと、を有するＩＤ管理方法。
【請求項１０】
請求項１記載のＩＤ管理方法であって、
前記ＩＤ利用端末において、
処理動作の指示を受け入れる指示入力ステップと、
前記ＩＤタグに装着されている前記電子回路チップから前記拡張ＩＤを取得するＩＤ読み取りステップと、
前記読み取りステップで取得した前記拡張ＩＤの正当性を、当該拡張ＩＤに含まれる前記改竄検知符号を用いて検証する検証ステップと、
前記指示入力ステップで受け入れた指示が情報読取指示である場合に、前記ＩＤ読み取りステップで取得した前記拡張ＩＤと対応づけられている情報をデータベースから取り出し、当該情報に応じて定められた処理を行なうステップと、
前記指示入力ステップで受け入れた指示が更新指示である場合に、更新情報を入手し、当該更新情報で、前記ＩＤ読み取りステップで取得した前記拡張ＩＤと対応づけられている情報を更新するステップと、

前記指示入力ステップで受け入れた指示が新規登録指示である場合に、新規情報を入手し、当該新規情報を、前記ＩＤ読み取りステップで取得した前記拡張ＩＤと対応づけてデータベースに格納するステップと、
前記指示入力ステップで受け入れた指示が失効ＩＤ登録指示である場合に、前記ＩＤタグの情報と対応づけられている前記拡張ＩＤをデータベースから取り出し、当該拡張ＩＤを含む失効ＩＤ登録要求をＩＤ管理端末に送信する失効ＩＤ登録要求ステップと、
を有するＩＤ管理方法。
【請求項１１】
ＩＤ発行の受注を行なうＩＤ受注端末と、前記ＩＤが格納されたＩＤタグの製造を行なう製造工場用端末と、ネットワークを介して前記ＩＤ受注端末および製造工場用端末に接続されたＩＤ管理端末とを含むＩＤ管理システムであって、
前記ＩＤタグは、外部からデータを読取り可能な電子回路チップを備え、
前記電子回路チップは、書き換え不可の記憶領域を有し、且つ当該領域に、外部から読取り可能なデータとして、受注したＩＤと、ＩＤの属性情報と、改竄検知符号、とを含む、拡張ＩＤを格納しており、
前記ＩＤ受注端末は、受注時に受け入れた発注情報から生成した受注情報を含む受注ＩＤ登録要求を、前記ＩＤ管理端末に送る受注ＩＤ登録要求処理部を備え、
前記ＩＤ管理端末は、前記受注ＩＤ登録要求が送られてきた場合に、当該拡張ＩＤが登録済みであるとして、データベースに登録する受注ＩＤ登録処理部を備え、
前記製造工場用端末は、製造済みの前記ＩＤタグに格納されている前記拡張ＩＤを含む、製造済みＩＤ登録要求を、前記ＩＤ管理端末に送らせる製造済みＩＤ登録要求処理部を備え、
前記ＩＤ管理端末は、前記製造済みＩＤ登録要求が送られてきた場合に、当該拡張ＩＤを格納した前記ＩＤタグが製造済みであるとして、前記データベースに登録する製造済みＩＤ登録処理部を備えるＩＤ管理システム。
【請求項１２】
請求項１１記載のＩＤ管理システムであって、
前記ＩＤ管理端末において、
前記ＩＤ受注端末から、前記拡張ＩＤを含むＩＤ重複確認要求が送られてきた場合に、当該拡張ＩＤが受注済みであるとして前記データベースに登録されているか否かを調べ、その結果を前記ＩＤ受注端末に通知するＩＤ重複確認処理部をさらに有するＩＤ管理システム。
【請求項１３】
請求項１１記載のＩＤ管理システムであって、
前記ＩＤ管理端末において、
前記ＩＤタグ製造工場用端末から、前記ＩＤタグに格納されている前記拡張ＩＤを含む、欠番ＩＤ登録要求が送られてきた場合に、当該要求に含まれる拡張ＩＤが欠番ＩＤであるとして、前記データベースに登録する欠番ＩＤ登録処理部をさらに有するＩＤ管理システム。
【請求項１４】
請求項１１記載のＩＤ管理システムであって、
前記ＩＤ管理システムは、
ネットワークを介して前記ＩＤ管理端末に接続された、ＩＤ利用端末を含んでおり、
前記ＩＤ管理端末において、
前記ＩＤ利用端末から、前記拡張ＩＤを含む検証要求が送られてきた場合に、当該拡張ＩＤを、データベースに格納してある拡張ＩＤと比較し、送られてきた拡張ＩＤに含まれる前記改竄検知符号が正当か否かを検証する検証処理部をさらに有するＩＤ管理システム。
【請求項１５】
請求項１１記載のＩＤ管理システムであって、
前記ＩＤ管理システムは、

ネットワークを介して前記ＩＤ管理端末に接続された、ＩＤ利用端末を含んでおり、
前記ＩＤ管理端末において、
前記ＩＤ利用端末から、前記ＩＤの属性情報を含む検証用鍵要求が送られてきた場合に、当該属性情報と対応づけられてデータベースに格納してある、前記改竄検知符号の検証用の鍵を、前記ＩＤ利用端末に送信する処理部をさらに有するＩＤ管理システム。
【請求項１６】
請求項１１記載のＩＤ管理システムであって、
前記ＩＤ管理システムは、
ネットワークを介して前記ＩＤ管理端末に接続された、ＩＤ利用端末を含んでおり、
前記ＩＤ管理端末において、
前記ＩＤ利用端末から、復号化用鍵要求が送られてきた場合に、データベースに格納してある、暗号化された拡張ＩＤの復号化用の鍵を、前記ＩＤ利用端末に送信する処理部をさらに有するＩＤ管理システム。
【請求項１７】
請求項１１記載のＩＤ管理システムであって、
前記ＩＤ管理システムは、
ネットワーク２を介して前記ＩＤ管理端末に接続された、ＩＤ利用端末を含んでおり、
前記ＩＤ管理端末において、
前記ＩＤ利用端末から、前記拡張ＩＤを含む、失効ＩＤ登録要求が送られてきた場合に、当該要求に含まれる拡張ＩＤが失効ＩＤであるとして、前記データベースに登録する失効ＩＤ登録処理部をさらに有するＩＤ管理システム。
【請求項１８】
請求項１１記載のＩＤ管理システムであって、
前記ＩＤ管理システムは、
ネットワークを介して前記ＩＤ受注端末に接続された、顧客端末を含んでおり、
前記ＩＤ受注端末において、
前記顧客端末から、前記ＩＤタグを発注する顧客の情報と、前記ＩＤタグへの格納を希望するＩＤと、前記ＩＤの改竄検知符号を生成するための鍵と、を含む発注情報が送られてきた場合に、当該発注情報を用いて、前記ＩＤの属性情報と、前記改竄検知符号と、を生成し、前記拡張ＩＤを生成する拡張ＩＤ生成処理部と、
前記顧客端末からの要求に応じて、前記発注情報と、前記拡張ＩＤと、を含む受注情報を送信する受注情報送信処理部と、
前記受注情報を含む受注ＩＤ登録要求をＩＤ管理端末に送信する受注ＩＤ登録要求処理部と、
前記拡張ＩＤを含むＩＤタグ製造要求を前記ＩＤタグ製造工場用端末に送信するＩＤタグ製造要求処理部と、を有するＩＤ管理システム。
【請求項１９】
請求項１１記載のＩＤ管理システムであって、
前記ＩＤタグ製造工場用端末は、
前記ＩＤ受注端末から、前記拡張ＩＤを含むＩＤタグ製造要求が送られてきた場合に、前記ＩＤタグの製造と、
製造された前記ＩＤタグの検査を指示する制御部と、
前記検査処理部の結果が合格の場合に、前記ＩＤタグに格納されている前記拡張ＩＤを含む、製造済みＩＤ登録要求を前記ＩＤ管理端末に送信する製造済みＩＤ登録要求処理部と、を有するＩＤ管理システム。
【請求項２０】
請求項１１記載のＩＤ管理システムであって、
前記ＩＤ利用端末において、
処理動作の指示を受け入れる指示入力処理部と、
前記ＩＤタグに装着されている前記電子回路チップから前記拡張ＩＤを取得するＩＤ読み

取り処理部と、
前記読み取り処理部で取得した前記拡張ＩＤの正当性を、当該拡張ＩＤに含まれる前記改竄検知符号を用いて検証する検証処理部と、
前記指示入力処理部で受け入れた指示が情報読取指示である場合に、前記ＩＤ読み取り処理部で取得した前記拡張ＩＤと対応づけられている情報をデータベースから取り出し、当該情報に応じて定められた処理を行なう処理部と、
前記指示入力処理部で受け入れた指示が更新指示である場合に、更新情報を入手し、当該更新情報で、前記ＩＤ読み取り処理部で取得した前記拡張ＩＤと対応づけられている情報を更新する処理部と、
前記指示入力処理部で受け入れた指示が新規登録指示である場合に、新規情報を入手し、当該新規情報を、前記ＩＤ読み取り処理部で取得した前記拡張ＩＤと対応づけてデータベースに格納する処理部と、
前記指示入力ステップで受け入れた指示が失効ＩＤ登録指示である場合に、前記ＩＤタグの情報と対応づけられている前記拡張ＩＤをデータベースから取り出し、当該拡張ＩＤを含む失効ＩＤ登録要求をＩＤ管理端末に送信する処理部と、
を有するＩＤ管理システム。
【請求項２１】
ネットワークに接続されて用いられ、ＩＤタグに格納された拡張ＩＤの管理を行うＩＤ管理端末であって、
前記ＩＤタグは、外部からデータを読取り可能な、書き換え不可の記憶領域を有し、且つ当該領域に、受注したＩＤと、ＩＤの属性情報と、改竄検知符号、とを含む、拡張ＩＤを格納しており、
前記拡張ＩＤと、当該拡張ＩＤに関連する情報と、を登録するデータベースを記憶する記憶手段と、
前記ネットワークに接続された他の端末と、通信を行う通信手段と、
前記通信手段により、前記他の端末から、受注時に受け入れた発注情報から生成した受注情報を含む受注ＩＤ登録要求が送られてきた場合に、当該拡張ＩＤが登録済みであるとして、データベースに登録する受注ＩＤ登録手段と、
前記通信手段により、前記他の端末から、製造済みの前記ＩＤタグに格納されている前記拡張ＩＤを含む、製造済みＩＤ登録要求が送られてきた場合に、当該拡張ＩＤを格納した前記ＩＤタグが製造済みであるとして、前記データベースに登録する製造済みＩＤ登録手段と、を有するＩＤ管理端末。
【請求項２２】
請求項２１記載のＩＤ管理端末であって、
前記通信手段により、前記他の端末から、前記拡張ＩＤを含むＩＤ重複確認要求が送られてきた場合に、当該拡張ＩＤが受注済みであるとして前記データベースに登録されているか否かを調べるＩＤ重複確認手段をさらに有し、
前記通信手段は、
前記ＩＤ重複確認手段での確認結果を前記他の端末に送信するＩＤ管理端末。
【請求項２３】
請求項２１記載のＩＤ管理端末であって、
前記通信手段により、前記他の端末から、前記ＩＤタグに格納されている前記拡張ＩＤを含む、欠番ＩＤ登録要求が送られてきた場合に、当該拡張ＩＤが欠番ＩＤであるとして、前記データベースに登録する欠番ＩＤ登録手段をさらに有するＩＤ管理端末。
【請求項２４】
請求項２１記載のＩＤ管理端末であって、
前記通信手段により、前記他の端末から、前記拡張ＩＤを含む検証要求が送られてきた場合に、当該拡張ＩＤを、データベースに格納してある拡張ＩＤと比較し、送られてきた拡張ＩＤに含まれる前記改竄検知符号が正当か否かを検証する検証手段をさらに有し、
前記通信手段は、

前記検証手段での検証結果を前記他の端末に送信するＩＤ管理端末。
【請求項２５】
請求項２１記載のＩＤ管理端末であって、
前記通信手段により、前記他の端末から、前記ＩＤの属性情報を含む検証用鍵要求が送られてきた場合に、当該属性情報と対応づけられてデータベースに格納してある、前記改竄検知符号の検証用の鍵を入手する検証用鍵入手手段をさらに有し、
前記通信手段は、
前記改竄検知符号の検証用の鍵を前記端末に送信するＩＤ管理端末。
【請求項２６】
請求項２１記載のＩＤ管理端末であって、
前記通信手段により、前記他の端末から、復号化用鍵要求が送られてきた場合に、データベースに格納してある、暗号化された拡張ＩＤの復号化用の鍵を入手する復号化用鍵入手手段をさらに有し、
前記通信手段は、
前記暗号化された拡張ＩＤの復号化用の鍵を前記端末に送信するＩＤ管理端末。
【請求項２７】
請求項２１記載のＩＤ管理端末であって、
前記通信手段により、前記他の端末から、前記拡張ＩＤを含む失効ＩＤ登録要求が送られてきた場合に、当該要求に含まれる拡張ＩＤが失効ＩＤであるとして、前記データベースに登録する失効ＩＤ登録手段をさらに有するＩＤ管理端末。
【請求項２８】
ネットワークに接続されて用いられ、ＩＤタグに格納されるＩＤの発行を受注するＩＤ受注端末であって、
前記ＩＤタグには、外部からデータを読取り可能な，書き換え不可の記憶領域を有し、且つ当該領域に、受注したＩＤと、ＩＤの属性情報と、改竄検知符号、とを含む、拡張ＩＤを格納しており、
前記ネットワークに接続された他の端末と，通信を行う通信手段と、
前記他の端末から、前記ＩＤタグを発注する顧客の情報と、前記ＩＤタグへの格納を希望するＩＤと、前記ＩＤの改竄検知符号を生成するための鍵と、を含む発注情報が送られてきた場合に、当該発注情報を用いて、前記ＩＤの属性情報と、前記改竄検知符号と、を生成し、前記拡張ＩＤを生成する拡張ＩＤ生成部と、
前記通信手段により、前記発注情報から生成した受注情報を含む受注ＩＤ登録要求をＩＤ管理端末に送信する受注ＩＤ登録要求手段と、
前記通信手段により、前記拡張ＩＤを含むＩＤタグ製造要求を前記ＩＤタグ製造工場用端末に送信するＩＤタグ製造要求手段と、を有するＩＤ受注端末。
【請求項２９】
請求項２８記載のＩＤ受注端末であって、
前記通信手段により、前記拡張ＩＤを含むＩＤ重複確認要求を前記他の端末に送信して、前記拡張ＩＤが前記ＩＤ管理端末に登録してある拡張ＩＤと重複しているか否かを確認させるＩＤ重複確認要求処理部をさらに有するＩＤ受注端末。
【請求項３０】
請求項２８記載のＩＤ受注端末であって、
乱数を生成し、当該乱数を前記改竄検知符号の生成用の鍵とする手段をさらに有するＩＤ受注端末。
【請求項３１】
請求項２８記載のＩＤ受注端末であって、
前記拡張ＩＤを暗号化し、暗号化してあることを示す暗号化符号を添付する手段をさらに有するＩＤ受注端末。
【請求項３２】
ネットワークに接続されて用いられ、ＩＤタグを製造するＩＤタグ製造工場で用いるＩＤ

タグ製造工場用端末であって、
前記ＩＤタグは、外部からデータを読取り可能な、書き換え不可の記憶領域を有し、且つ当該領域に、受注したＩＤと、ＩＤの属性情報と、改竄検知符号、とを含む、拡張ＩＤを格納しており、
前記ネットワークに接続された他の端末と、通信を行う通信手段と、
前記通信手段により、前記他の端末から、前記拡張ＩＤを含むＩＤタグ製造要求が送られてきた場合に、当該製造要求に従った前記ＩＤタグの製造と、製造された前記ＩＤタグの検査を実施させる制御手段と、
前記検査の結果が合格の場合に、前記通信手段により、前記ＩＤタグに格納されている前記拡張ＩＤを含む、製造済みＩＤ登録要求を前記他の端末に送信して、当該他の端末に、前記拡張ＩＤを格納したＩＤタグが製造済みであるとして登録させる製造済みＩＤ登録要求手段と、
を有するＩＤタグ製造工場用端末。
【請求項３３】
請求項３２記載のＩＤタグ製造工場用端末であって、
前記検査の結果が不合格であり、かつ、前記ＩＤタグの再製造が不要な場合に、前記通信手段により、前記ＩＤタグに格納されている前記拡張ＩＤを含む、欠番ＩＤ登録要求を前記他の端末に送信して、当該他の端末に、前記拡張ＩＤが欠番ＩＤであるとして登録させる欠番ＩＤ登録要求手段をさらに有するＩＤタグ製造工場用端末。
【請求項３４】
ネットワークに接続されて用いられ、ＩＤタグを利用する際に用いるＩＤ利用端末であって、
前記ＩＤタグには、外部からデータを読取り可能な，書き換え不可の記憶領域を有し、且つ当該領域に、受注したＩＤと、ＩＤの属性情報と、改竄検知符号、とを含む、拡張ＩＤを格納しており、
前記拡張ＩＤと、当該拡張ＩＤに関連する情報と、当該拡張ＩＤが格納されている前記ＩＤタグと対応づけられている情報と、を登録するデータベースを記憶する記憶手段と、
前記ネットワークに接続された、前記他の端末と通信を行う通信手段と、
処理動作の指示を受け入れる指示入力手段と、
前記ＩＤタグに装着されている前記電子回路チップから前記拡張ＩＤを取得するＩＤ読み取り手段と、
前記読み取り手段で取得した前記拡張ＩＤの正当性を、当該拡張ＩＤに含まれる前記改竄検知符号を用いて検証する検証手段と、
前記指示入力手段で受け入れた指示が情報読取指示である場合に、前記ＩＤ読み取り手段で取得した前記拡張ＩＤと対応づけられている情報をデータベースから取り出し、当該情報に応じて定められた処理を行なう手段と、
前記指示入力手段で受け入れた指示が更新指示である場合に、更新情報を入手し、当該更新情報で、前記ＩＤ読み取り手段で取得した前記拡張ＩＤと対応づけられている情報を更新する手段と、
前記指示入力手段で受け入れた指示が新規登録指示である場合に、新規情報を入手し、当該新規情報を、前記ＩＤ読み取り手段で取得した前記拡張ＩＤと対応づけてデータベースに格納する手段と、
前記指示入力手段で受け入れた指示が失効ＩＤ登録指示である場合に、前記ＩＤタグの情報と対応づけられている前記拡張ＩＤをデータベースから取り出し、当該拡張ＩＤを含む失効ＩＤ登録要求をＩＤ管理端末に送信する手段と、
を有するＩＤ利用端末。
【請求項３５】
請求項３４記載のＩＤ利用端末であって、
前記ＩＤ読み取り手段で取得した前記拡張ＩＤが暗号化されている場合に、前記記憶手段に格納されている復号化用の鍵を用いて復号化を行なう手段をさらに有するＩＤ利用端末

。
【請求項３６】
請求項３４記載のＩＤ利用端末であって、
前記ＩＤ読み取り手段で取得した前記拡張ＩＤが暗号化されており、かつ、前記記憶手段に復号化用の鍵を所有していない場合に、前記通信手段により、復号化用鍵要求を前記他の端末に送信して、当該他の端末に、前記復号化用の鍵を送信させる手段をさらに有するＩＤ利用端末。
【請求項３７】
請求項３４記載のＩＤ利用端末であって、
前記ＩＤ読み取り手段で取得した前記拡張ＩＤに含まれる前記改竄検知符号を検証する鍵を所有していない場合に、前記通信手段により、前記拡張ＩＤを含む検証用鍵鍵要求を前記他の端末に送信して、当該他の端末に、前記検証用鍵を送信させる手段をさらに有するＩＤ利用端末。
【請求項３８】
請求項３４記載のＩＤ利用端末であって、
前記通信手段により、前記ＩＤ読み取り手段で取得した前記拡張ＩＤを含む、検証要求を前記他の端末に送信して、当該他の端末に、前記拡張ＩＤの正当性を検証させる検証要求手段をさらに有し、
前記検証手段は、
検証結果として、前記他の端末から送られてくる前記検証要求に対する結果を用いるＩＤ利用端末。
【請求項３９】
ネットワークに接続可能な複数の計算機に、ＩＤ発行の受注を行なうＩＤ受注端末と、前記ＩＤが格納されたＩＤタグの製造を行なう製造工場用端末と、ＩＤ管理端末とからなるＩＤ管理システムを実現させるプログラム製品であって、
前記計算機が読みとり可能な媒体と、
前記ＩＤ受注端末となる前記計算機に、受注時に受け入れた発注情報から生成した受注情報を含む受注ＩＤ登録要求を、前記ＩＤ管理端末に送らせる受注ＩＤ登録要求処理部を実現させるモジュールと、
前記ＩＤ管理端末となる前記計算機に、前記受注ＩＤ登録要求が送られてきた場合に、当該拡張ＩＤが登録済みであるとして、データベースに登録する受注ＩＤ登録処理部を実現させるモジュールと、
前記製造工場用端末となる前記計算機に、製造済みの前記ＩＤタグに格納されている前記拡張ＩＤを含む、製造済みＩＤ登録要求を、前記ＩＤ管理端末に送らせる製造済みＩＤ登録要求処理部を実現させるモジュールと、
前記ＩＤ管理端末となる前記計算機に、前記製造済みＩＤ登録要求が送られてきた場合に、当該拡張ＩＤを格納した前記ＩＤタグが製造済みであるとして、前記データベースに登録する製造済みＩＤ登録処理部を実現させるモジュールと、を備えるプログラム製品。
【請求項４０】
流通を管理するためのＩＤタグを備える物品であって，
前記ＩＤタグは，前記物品のＩＤと前記物品に関わる属性情報と，前記ＩＤと前記属性情報に対する改竄検知符号とからなる拡張ＩＤを格納し，
前記ＩＤと、前記属性情報と、前記改竄検知符号と、前記改竄検知符号の検証用の鍵を、関連付けて格納するデータベースを用いて，前記拡張ＩＤの正当性を確認可能としたＩＤタグを備える物品。
【請求項４１】
請求項４０記載のＩＤタグを備える物品であって、
前記拡張ＩＤは，さらに，前記ＩＤと前記属性情報との割り当てを制御するクラス情報をさらに含むＩＤタグを備える物品。
【請求項４２】

請求項４０記載のＩＤタグを備える物品であって、
前記拡張ＩＤは，さらに，拡張ＩＤの桁数、改竄検知符号の桁数と計算方法を示すバージョン情報を含み，前記改竄検知符号は，前記バージョン情報に対する改竄をも検知するものであるＩＤタグを備える物品。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、ＩＤの管理を行う技術に関し、特に、改竄検知符号を備えたＩＤの、発行と流通の管理を行う技術に関する。
【０００２】
【従来の技術】
従来より、ＪＡＮコードなどの様々なＩＤが物品に付与され、物品の管理に利用されている。物品に関する情報を、物品に付与したＩＤ（物品識別子）と関連付けて管理することにより、物品を個別に管理することができる。
【０００３】
例えば、コンビニエンスストアなどでは、商品の製造会社や名前や価格を、商品の包装に印字されているＪＡＮコードと関連付けて管理しておき、バーコードを読み取ることでＪＡＮコードを入力すれば商品の情報を参照できるシステムを利用している。
【０００４】
また、値が正しいものであることを保証するため、ＩＤに誤り検知符号を備える。読み取ったＩＤの誤り検知符号を所定の計算手順により検証することで、読み取りが正常に行われたか否かが判断できる。さらに、鍵となる数値を利用して計算する誤り検知符号には、鍵を知らない者によるＩＤの改竄を検知する機能がある。以下では、鍵を利用して計算する誤り検知符号のことを改竄検知符号と呼ぶ。
【０００５】
ＩＤに高い安全性が求められる場合、改竄検知符号を備えたＩＤを利用する。例えば、身分証明証などのようなＩＤの付与された物品を人と関連付けることにより、人を個別に管理する場合や、株券や商品券などの有価証券にＩＤを付与して管理する場合などがある。
【０００６】
【発明が解決しようとする課題】
上記従来のＩＤの管理方法には、以下のような問題がある。
【０００７】
すなわち、上記コンビニエンスストアの例の様にＪＡＮコードを物品のＩＤとして利用する場合、ＩＤの桁数制限により物品の種類別にＩＤを振り分けているため、同じ種類の物品において，１つ１つ個別に管理することはできない。また、個別管理ができるようにＪＡＮコードよりも桁数を増やしたＩＤがあるが、バーコードで表示する場合、スペースの都合により適用できない物品もある。
【０００８】
また、ＪＡＮコードは誤り検知符号しか備えておらず、鍵を用いた改竄検知符号は備えていない。このため、ＩＤを偽造されるおそれがある。偽造防止のため、ＩＤに改竄検知符号を用いる場合は、安全のため、いくつかのＩＤ毎に異なる鍵を利用する必要がある。このため、上記コンビニエンスストアの例の様に、様々な種類のＩＤを扱う場合、扱うＩＤ全ての改竄検知符号の検証用の鍵をあらかじめ用意しておかねばならない。
【０００９】
また、改竄検知符号を備えたＩＤを利用した物品管理を個人が行なう場合、ＩＤが付与されたシールやテープを入手し、任意の物品に貼り付けて管理する方法などが考えられるが、改竄検知符号の検証用の鍵も管理する必要があり、困難である。
【００１０】
また、ＩＤに高い安全性が求められる場合、ＩＤが重複しないように発行の管理を行なうか、もしくは、同一ＩＤの個数の管理を行なう必要がある。このためには、物品やシール

へのＩＤの印字や、電子タグに利用するメモリへの書き込みも、管理しなければならない。

【００１１】

また、ＩＤが重複しないように安全性高く発行の管理を行なっているものとして、クレジットカードのＩＤが挙げられる。しかし、クレジットカードのＩＤのように、サービスや、サービスを受ける人・法人に対して与えられているＩＤは、物品としての実体がなく情報にすぎないため、発行後に不正に複製されてしまう恐れがある。

【００１２】

本発明は、上記事情に鑑みてなされたものであり、本発明の目的は、改竄検知符号を備え、物品個別に割り当て可能なＩＤの発行と流通を管理し、ＩＤを利用した物品管理を効率よく、かつ、信頼性高く行うことが可能な仕組みを提供することにある。

【００１３】

【課題を解決するための手段】

上記目的を達成するために、本発明では、同じ種類の物品であっても異なるＩＤを個別に割り当て可能であり，さらに属性情報と改竄検知符号を備えた拡張型物品識別子（以下，拡張ＩＤという）を利用する。属性情報とはＩＤを分類する情報で、ＩＤの利用分野や、発行を依頼した会社名などを表わす情報である。そして、ＩＤの備える改竄検知符号は、属性情報ごとに異なる鍵を用いて生成する。

【００１４】

また、本発明では、ＩＤの発行と流通を管理するためのＩＤ管理端末を設け、ネットワークを介して、ＩＤを利用するためのＩＤ利用端末に接続する。ＩＤ管理端末には、発行したＩＤと、ＩＤの属性情報と、改竄検知符号と、改竄検知符号の検証用の鍵を、関連付けて格納する。そして、ＩＤ管理端末は、ＩＤとＩＤの属性情報と改竄検知符号とを含む改竄検知符号１０２の検証要求が、ＩＤ利用端末から送られてきた場合、格納しているＩＤと、それに関連付けられている改竄検知符号とを用いて検証し、結果を端末に返す。以下、検証要求とは、改竄検知符号１０２の検証要求を指す。また、ＩＤの属性情報を含む検証用鍵要求がＩＤ利用端末から送られてきた場合、ＩＤの属性情報と関連づけられている検証用の鍵を、端末に返す。ＩＤ利用端末は、ＩＤを読み取る機能と、読み取ったＩＤとＩＤが付与されている物品の情報とを関連付けて管理する機能と、物品の情報が処理を示すものであった場合にその処理を行なう機能を有している。

【００１５】

また、本発明では、ＩＤ受注端末とＩＤタグ製造工場用端末を設け、ネットワークを介してＩＤ管理端末と接続する。ＩＤ受注端末は、ＩＤの発行を依頼された日付け、個数、改竄検知符号の生成用の鍵などを格納し、生成用の鍵を用いて改竄検知符号の生成を行なう。ＩＤと、ＩＤの属性情報と、改竄検知符号をひとつにまとめる。暗号通信を利用してＩＤ管理端末に送信し、ＩＤ管理センタで管理している情報から、発行済みのＩＤと重複していないことを確認した後、同様に暗号通信を利用してＩＤタグ製造工場用端末に送信する。ここで、ＩＤがバーコードと同じ情報を示している旨を属性情報に含ませて、複数個の同一ＩＤを発行してもよい。

【００１６】

一方、ＩＤタグ製造工場用端末は、バーコードラベルや電子タグなどのＩＤタグを製造する製造部に対し、ＩＤと、ＩＤの属性情報と、改竄検知符号を、ＩＤタグ上に印字、もしくは、ＩＤタグ内に格納するよう、指示する。また、ＩＤタグの検査部に対し、完成したＩＤタグに情報が正しく格納されているかどうかを検査するよう、指示する。そして、製造したＩＤタグの情報と検査結果を、暗号通信を利用してＩＤ管理端末に送信する。

【００１７】

本発明によれば、ＩＤを重複すること無く発行し、物品の個別管理を行なうことが可能となる。また、複数個の同一ＩＤを発行し、ＩＤを既存のバーコードシステムで利用することが可能となる。

【００１８】

また、本発明によれば、ＩＤの利用者は、検証用の鍵や装置を保持していなくても、ＩＤ利用端末からＩＤ管理端末に、ネットワークを通じてＩＤタグから読みとった情報（例えば，ＩＤとＩＤの属性情報と改竄検知符号）を用いた検証要求を送信すれば、検証結果を得ることができる。

【００１９】

また、本発明によれば、ＩＤの利用者は、検証用の鍵を保持していなくても、ＩＤ利用端末からＩＤ管理端末に、ネットワークを通じてＩＤの属性情報を含む検証用鍵要求を送信すれば、検証用の鍵を得ることができ、改竄検知符号の検証を行なうことができる。

【００２０】

また、本発明によれば、改竄検知符号の生成用および検証用の鍵や、ＩＤの発行依頼者の情報などの、機密性の高い情報を秘密裏に管理することができる。

【００２１】

また、本発明において、ＩＤタグとして電子回路チップを用いる場合を考える。電子回路チップを製造するには、十分な設備が必要である。そして、電子回路チップを小型・薄型にするほど、電子回路チップを製造できる者が限られてくる。このため、不正な第三者がＩＤタグの複製を製造する可能性が低くなる。また、ＩＤを電子回路チップの書き換え不可領域に格納すれば、不正な第三者がＩＤを改変することはできない。したがって、本発明によれば、ＩＤ管理端末が市場に流通するＩＤタグの個数を管理することができる。

【００２２】

【発明の実施の形態】

以下、本発明の一実施形態が適用されたＩＤ管理システムについて説明する。

【００２３】

まず、本実施形態のＩＤ管理システムで用いるＩＤおよびＩＤタグについて説明する。

【００２４】

図１は本実施形態のＩＤ管理システムで用いるＩＤの一例を示した図である。

【００２５】

図１（ａ）に示すように、本実施形態で用いるＩＤ１００は、ＩＤの属性情報１０１と、改竄検知符号１０２を伴ない、拡張ＩＤ２００として一まとめで利用される。属性情報１０１とはＩＤ１００を分類する情報で、ＩＤ１００の利用分野や、発行を依頼した会社名などを表わす情報である。また、改竄検知符号１０２は、属性情報１０１ごとに異なる鍵を用いて、ＩＤ１００と属性情報１０１に対して所定の計算を行ない生成される。改竄検知符号１０２を生成するための計算には、公開鍵暗号、共通鍵暗号、ハッシュ生成関数などを組み合わせたものを利用するとよい。

【００２６】

図１（ｂ）は、図１（ａ）の３要素にクラス情報１０３が付随する場合を示している。クラス情報とは、ＩＤ１００と属性情報１０１の切り分け位置、すなわち、それぞれの桁数を示す情報である。図１（ｃ）、（ｄ）、（ｅ）に示すように、クラス情報１０３を用いれば、拡張ＩＤ２００と改竄検知符号１０２が同じ桁数でありながら、ＩＤ１００と属性情報１０１の桁数や個数を様々に変えた拡張ＩＤ２００を構築することができる。このため、拡張ＩＤ２００の受け渡しや、改竄検知符号１０２の生成および検証に用いる仕組みを変えることなく、用途に応じて、ＩＤ１００と属性情報１０１の桁数や個数の組み合わせが最適な拡張ＩＤ２００を利用できる。

【００２７】

また、図１（ｆ）は、図１（ａ）の３要素にバージョン情報１０４が付随する場合を示している。バージョン情報とは、拡張ＩＤ２００のバージョンを示す情報である。バージョン情報１０４から、拡張ＩＤ２００の桁数、改竄検知符号１０２の桁数と計算方法などが分かる。

【００２８】

また、図１（ｇ）は、拡張ＩＤ２００が暗号化してある場合を示している。暗号化してあることを示す暗号化符号１０５と、図１（ａ）の３要素を暗号化した情報１０６からなる

。拡張ＩＤ２００を暗号化して用いると、復号化用の鍵を知らない者には拡張ＩＤ２００の構成要素が判別できないため、不正な解読を防止することができる。

【００２９】

なお、拡張ＩＤ２００は上記に限らず、クラス情報１０３の追加、バージョン情報１０４の追加、暗号化、のうちの任意の２つ、または、全てを組み合わせたものでも良い。

【００３０】

図２は本実施形態のＩＤ管理システムで用いるＩＤタグの一例を示した図である。

【００３１】

図２（ａ）は、テープ状のＩＤタグ３００に電子回路チップ３０１が複数個装着されている様子を示す。適切な位置でテープを切断することで、任意の個数の電子回路チップが装着されたテープ片を得ることができる。

【００３２】

なお、ＩＤタグ３００は、電子回路チップ３０１が装着されているテープ状のものとしたが、シート状のものであってもよいし、電子回路チップ３０１そのものでもよい。また、ＩＤが印刷されたラベルであってもよい。

【００３３】

電子回路チップ３０１は、たとえば、十分な設備を有する半導体製造メーカでなければ製造できない０．３ｍｍ角程度の小型電子回路チップであり、薄型の略直方体の形状を有している。また、図２（ｂ）に示すように、シリコンチップ３０２上に、メモリおよびその読み出し回路として機能する電子回路３０３と、コンデンサ３０４と、アンテナ３０５とが、形成されて構成されている。メモリは、書き換え不可能なメモリ部分を含むものとする。また、書き換え不可能なメモリ部分には、拡張ＩＤ２００が格納されている。

【００３４】

なお、電子回路３０３の書き換え不可能なメモリ部分への拡張ＩＤ２００の格納は、電子回路チップ３０１の製造業者が、当該チップ３０１をＩＤタグ３００の製造業者へ出荷する前に、予め行っておくようにする。電子回路３０３の書き換え不可能なメモリ部分とは、ＲＯＭなどの書き換え不可能なメモリの他、たとえば、拡張ＩＤ２００が書き込まれた部分が書き換え不可に設定されている、ＥＥＰＲＯＭなどの書き換え可能なメモリも含むものとする。

【００３５】

電子回路３０３とコンデンサ３０４とアンテナ３０５は、図２（ｃ）に示すような回路を形成している。この回路は、外部から与えられた電波により、アンテナ３０５にて電流を誘起し、電荷をコンデンサ３０４に蓄積する。そして、コンデンサ３０４に蓄積した電荷から得た電力を用いて、電子回路３０３に記憶されている情報を、アンテナ３０５より電波を用いて送信する。すなわち、この電子回路チップ３０１に電波を与えることにより、外部より非接触で電子回路チップ３０１の電子回路３０３に格納されている拡張ＩＤ２００を読み出すことができる。

【００３６】

次に、以上のようなＩＤタグ３００を利用して拡張ＩＤ２００の管理を行う、ＩＤ管理システムの構成について説明する。

【００３７】

図３は、本実施形態が適用されたＩＤ管理システムの概略図である。

【００３８】

図示するように、本実施形態のＩＤ管理システムは、ＩＤ受注端末３と、ＩＤタグ製造工場用端末４と、ＩＤ管理端末５とが、専用ネットワークやインターネットなどのネットワーク１に接続されて構成される。なお、図３に示す例では、端末３および４をそれぞれ１つ示しているが、複数であってもかまわない。また、顧客端末８は、専用ネットワークやインターネットなどのネットワーク７を介して、ＩＤ受注端末３に接続されている。また、ＩＤ管理端末５は、専用ネットワークやインターネットなどのネットワーク２を介して、ＩＤ利用端末６に接続されている。ネットワーク１とネットワーク２とネットワーク７

とは、同じネットワークであってもよい。
【００３９】
顧客端末８は、ＩＤタグ３００を発注するために必要な発注情報を、顧客が入力する端末であり、発注情報をＩＤ受注端末３に送信する。
【００４０】
ＩＤ受注端末３は、拡張ＩＤ２００の発行を受注するための端末であり、顧客端末８から送られてきた発注情報から、ＩＤ１００、属性情報１０１、改竄検知符号１０２などを含む拡張ＩＤ２００を生成し、ＩＤタグ製造工場用端末４に送信する。
【００４１】
また、ＩＤタグ製造工場用端末４は、ＩＤタグ３００の製造を管理する端末であり、ＩＤ受注端末３から送られてきた拡張ＩＤ２００が付与されたＩＤタグ３００の製造状況をＩＤ管理端末５に送信する。
【００４２】
また、ＩＤ管理端末５は、ＩＤ受注端末３とＩＤタグ製造工場用端末４から送られてくる情報を管理し、ＩＤ利用端末６から送られてくる要求に応える。
【００４３】
また、ＩＤ利用端末６は、ＩＤタグ３００から拡張ＩＤ２００を読み取り、拡張ＩＤ２００と関連付けて管理している情報を利用するための端末であり、必要に応じて、ＩＤ管理端末５に要求を送信する。
【００４４】
なお、ＩＤ管理端末５に、ＩＤ受注端末３としての機能を持たせるようにすることで、ＩＤ受注端末３を省略してもよい。また、ＩＤ管理端末５に、ＩＤタグ製造工場用端末４としての機能を持たせるようにすることで、ＩＤタグ製造工場用端末４を省略してもよい。また、ＩＤ管理端末５に、ＩＤ利用端末６としての機能を持たせるようにすることで、ＩＤ利用端末６を省略してもよい。また、ＩＤ受注端末３に、顧客端末８としての機能を持たせるようにすることで、顧客端末８を省略してもよい。
【００４５】
なお、顧客端末８とＩＤ利用端末６は複数個あってもよい。
【００４６】
なお、顧客端末８とＩＤ受注端末３間、および、ＩＤ受注端末３とＩＤタグ製造工場用端末４間、および、ＩＤ受注端末３とＩＤ管理端末５間、および、ＩＤタグ製造工場用端末４とＩＤ管理端末５間、および、ＩＤ管理端末５とＩＤ利用端末６間の通信には、暗号を用いることが望ましいが、暗号通信の方式は、それぞれ２つの端末間で通信できれば，異なる方式であってもよい。また、暗号通信を行なう代わりに、あらかじめ認証を行なった後で通信を行なってもよい。
【００４７】
次に、上記のＩＤ管理システムを構成する各装置について説明する。
【００４８】
図１６は、顧客端末８の機能構成を示す概略図である。
【００４９】
図示するように、顧客端末８は、入出力部８１と、通信部８２を有する。
【００５０】
入出力部８１は、ＩＤタグ３００の発注に必要な発注情報を受け入れる。発注情報とは、ＩＤタグ３００に格納したいＩＤ１００、暗号化した拡張ＩＤ２００の復号化用の鍵、など拡張ＩＤ２００の生成と管理に必要な情報と、発注者情報、発注日時、納入期限、納入方法指定、などＩＤタグ３００の発注に必要な情報と、を指す。
【００５１】
また、ＩＤ受注端末３から受け取った受注情報を出力する。受注情報とは、前記発注情報と、ＩＤタグ３００に格納される拡張ＩＤ２００、ＩＤ受注端末３が改竄検知符号を生成するために用いた鍵と、検証するために用いる鍵、自動生成された暗号化用及び復号化用

の鍵、など拡張ＩＤ２００の管理に必要な情報と、受注日時、納入日時、納入方法、などＩＤタグ３００の納入に必要な情報と、を指す。

【００５２】

通信部８２は、入出力部８１より受け取った発注情報を含む受注情報要求を、通信用に暗号化し、ネットワーク７を介してＩＤ受注端末３に送信する。また、ＩＤ受注端末３より、暗号化された受注情報を受け取り、復号化する。通信用の暗号化には、共通鍵暗号、もしくは、公開鍵暗号、もしくは、共通鍵暗号と公開鍵暗号を組み合わせたもの、を利用する。

【００５３】

図４は、ＩＤ受注端末３の機能構成を示す概略図である。

【００５４】

図示するように、ＩＤ受注端末３は、入出力部３１と、拡張ＩＤ生成部３２と、改竄検知符号生成部３３と、通信部３４を有する。

【００５５】

通信部３４は、ネットワーク７を介して顧客端末８より受信した暗号文の復号化を行ない、発注情報を含む受注情報要求を得る。利用する暗号方式は、顧客端末８の通信部８２で利用しているものと同じとする。

【００５６】

入出力部３１は、エラー情報などを出力する。また、発注情報をネットワーク７を介して顧客端末８から受け入れず、直接入力受付する場合に用いる。

【００５７】

拡張ＩＤ生成部３２は、通信部３４より受け取った発注情報から、ＩＤの属性情報１０１を生成する。また、改竄検知符号生成部３３に、ＩＤ１００と属性情報１０１と改竄検知符号生成用の鍵を渡し、生成された改竄検知符号１０２と検証用の鍵を受け取る。発注情報に改竄検知符号生成用の鍵が含まれていない場合、乱数を生成し、生成した値を改竄検知符号生成用の鍵とする。さらに、ＩＤ１００と属性情報１０１と改竄検知符号１０２から、拡張ＩＤ２００を生成する。なお、属性情報１０１は、クラス情報１０３であってもよいし、バージョン情報１０４であってもよい。また、発注情報に拡張ＩＤ２００の暗号化用の鍵が含まれていない場合、乱数を生成し、生成した値を暗号化用の鍵とする。また、拡張ＩＤ２００を暗号化し、暗号化符号１０５を生成し、復号化用の鍵を生成する機能も有する。発注情報に、拡張ＩＤ、生成した鍵などを加え、受注情報とする。

【００５８】

改竄検知符号生成部３３は、拡張ＩＤ生成部３２より受け取ったＩＤ１００と属性情報１０１と改竄検知符号生成用の鍵から、改竄検知符号１０２と検証用の鍵とを生成し、拡張ＩＤ生成部３２に渡す。

【００５９】

通信部３４は、ネットワーク７を介して顧客端末８より受け取った発注情報を含むＩＤ重複確認要求を、通信用に暗号化し、ネットワーク１を介してＩＤ管理端末５に送信する。なお、発注情報の代わりに入出力部３１より受け取った拡張ＩＤ２００を送信してもよい。ＩＤ管理端末５より、発行済みＩＤとの重複がない旨の通知を受け取った後、入出力部３１より受け取った受注情報を含む受注ＩＤ登録要求を通信用に暗号化し、ネットワーク１を介してＩＤ管理端末５に送信する。なお、ＩＤの重複を許可する場合は、ＩＤ重複確認要求の送信を省略しても良い。

【００６０】

また、入出力部３１より受け取った受注情報を含むＩＤタグ製造要求を通信用に暗号化し、ネットワーク１を介してＩＤタグ製造工場用端末４に送信する。通信用の暗号化には、共通鍵暗号、もしくは、公開鍵暗号、もしくは、共通鍵暗号と公開鍵暗号を組み合わせたもの、を利用する。また、入出力部３１より受け取った受注情報を通信用に暗号化し、ネットワーク７を介して顧客端末８に送信する。利用する暗号方式は、顧客端末８の通信部８２で利用しているものと同じとする。

【００６１】
図５は、ＩＤタグ製造工場４６の機能構成を示す概略図である。
【００６２】
図示するように、ＩＤタグ製造工場４６は、ＩＤタグ製造工場用端末４と、製造部４２と、検査部４３と、納入部４５とを有する。また、ＩＤタグ製造工場用端末４は、通信部４１と、制御部４４とを有する。
【００６３】
通信部４１は、ネットワーク１を介してＩＤ受注端末３より受信した暗号文の復号化を行ない、受注情報を含むＩＤタグ製造要求を得る。利用する暗号方式は、ＩＤ受注端末３の通信部３４で利用しているものと同じとする。
【００６４】
制御部４４は、通信部４１で得た受注情報を受け取り、該受注情報に含まれる拡張ＩＤ２００を格納したＩＤタグ３００を、該受注情報に従って製造するよう、製造部４２に指示する。また、拡張ＩＤ２００を検査部４３に送り、完成したＩＤタグ３００の機能が正常か否かを検査するよう、検査部４３に指示する。検査結果が不良であった場合、拡張ＩＤ２００を製造部４２に渡し、再度、ＩＤタグ３００を製造させる。検査結果が不良であった拡張ＩＤ２００を、欠番ＩＤとして通信部４１に渡してもよい。また、検査結果が正常であったＩＤタグ３００に付与されている拡張ＩＤ２００を製造済みＩＤとして通信部４１に渡す。
【００６５】
通信部４１は、欠番ＩＤを含む欠番ＩＤ登録要求と、製造済みＩＤを含む製造済みＩＤ登録要求と、を作成し、通信用に暗号化し、ネットワーク１を介してＩＤ管理端末５に送信する。通信用の暗号化には、共通鍵暗号、もしくは、公開鍵暗号、もしくは、共通鍵暗号と公開鍵暗号を組み合わせたもの、を利用する。
【００６６】
製造部４２は、制御部４４より受け取った拡張ＩＤ２００を格納したＩＤタグ３００を製造する。そして、製造したＩＤタグ３００を検査部４３に渡す。
【００６７】
検査部４３は、製造部４２から受け取ったＩＤタグ３００を検査し、制御部４４より受け取った拡張ＩＤ２００が正しく格納されていることなどを確認する。そして、検査結果を制御部４４に送る。
【００６８】
納入部４５は、検査部４３で検査結果が合格であったＩＤタグ３００を受け取る。そして、受注情報に含まれる納入方法に従って、顧客に対して発送・引き渡しなどを行ない、納入する。
【００６９】
図６は、ＩＤ管理端末５の機能構成を示す概略図である。
【００７０】
図示するように、ＩＤ管理端末５は、通信部５１と、ＩＤ関連情報管理部５２と、ＩＤ関連情報管理データベース５３とを有する。
【００７１】
通信部５１は、ネットワーク１を介してＩＤ受注端末３より受信した暗号文の復号化を行ない、受注情報を含むＩＤ重複確認要求、もしくは、受注情報を含む受注ＩＤ登録要求を得る。利用する暗号方式は、ＩＤ受注端末３の通信部３４で利用しているものと同じとする。また、ネットワーク１を介してＩＤタグ製造工場用端末４より受信した暗号文の復号化を行ない、欠番ＩＤを含む欠番ＩＤ登録要求と、製造済みＩＤを含む製造済みＩＤ登録要求と、を得る。利用する暗号方式は、ＩＤタグ製造工場用端末４の通信部４１で利用しているものと同じとする。また、ネットワーク２を介してＩＤ利用端末６より受信した暗号文の復号化を行ない、拡張ＩＤ２００を含む検証要求、もしくは、属性情報１０１を含む検証用鍵要求、もしくは、復号化用鍵要求を得る。利用する暗号方式は、ＩＤ利用端末

６の通信部６１で利用しているものと同じとする。

【００７２】

ＩＤ関連情報管理部５２は、通信部５１より受け取った要求が、ＩＤ重複確認要求である場合、共に受け取った受注情報に含まれる拡張ＩＤ２００と、ＩＤ関連情報管理データベース５３に格納してある拡張ＩＤ２００とを用いて、発行済みＩＤと重複するか否かを確認する。そして、確認の結果を通信部５１で暗号化し、ネットワーク１を介してＩＤ受注端末３に送信する。また、通信部５１より受け取った要求が、受注ＩＤ登録要求である場合、共に受け取った受注情報をＩＤ関連情報管理データベース５３に格納する。また、通信部５１より受け取った要求が、欠番ＩＤ登録要求である場合、共に受け取った欠番ＩＤをＩＤ関連情報管理データベース５３に格納する。また、通信部５１より受け取った要求が、製造済みＩＤ登録要求である場合、共に受け取った製造済みＩＤをＩＤ関連情報管理データベース５３に格納する。また、通信部５１より受け取った要求が、検証要求である場合、共に受け取った拡張ＩＤ２００と、ＩＤ関連情報管理データベース５３に格納してある拡張ＩＤ２００とを比較し、検証を行なう。そして、検証結果を通信部５１で暗号化し、ネットワーク２を介してＩＤ利用端末６に送信する。また、通信部５１より受け取った要求が、検証用鍵要求である場合、共に受け取った属性情報１０１から、ＩＤ関連情報管理データベース５３に格納してある改竄検知符号１０２の検証用の鍵を取り出し、通信部５１で暗号化し、ネットワーク２を介してＩＤ利用端末６に送信する。また、通信部５１より受け取った要求が、復号化用鍵要求である場合、ＩＤ関連情報管理データベース５３より復号化用の鍵を取り出し、通信部５１で暗号化し、ネットワーク２を介してＩＤ利用端末６に送信する。通信用の暗号化には、共通鍵暗号、もしくは、公開鍵暗号、もしくは、共通鍵暗号と公開鍵暗号を組み合わせたもの、を利用する。また、通信部５１より受け取った要求が、失効ＩＤ登録要求である場合、共に受け取った失効ＩＤ２００を、ＩＤ関連情報管理データベース５３に格納する。

【００７３】

ＩＤ関連情報管理データベース５３には、ＩＤタグ３００に関連する管理情報が格納される。図１７は、ＩＤ関連情報管理データベース５３に格納されるＩＤタグ３００に関連する管理情報を説明するための図である。図示するように、ＩＤタグ３００に関連する管理情報は、ＩＤ受注端末３から送られてきた受注情報５３０と、発行／納入済み・欠番扱い・製造中・失効などのＩＤの発行状況５３８と、その他の管理情報である備考５３９と、を含んで構成される。

【００７４】

ここで、受注情報５３０は、顧客端末８において受け入れた発注情報５３１と、ＩＤ受注端末３において前記発注情報５３１から生成された拡張ＩＤ２００と、を含む。ここで、発注情報５３１は、顧客情報５３２と、顧客が発注したＩＤの個数５３３と、欠番や重複などの発行条件５３４と、ＩＤ３００の指定納入日５３５と、ＩＤの属性情報１０１と対応づけられた改竄検知コード１０２の検証用の鍵５３６と、拡張ＩＤ２００が暗号化されてＩＤタグ３００に付与されている場合の復号化用の鍵５３７と、顧客が発行を希望したＩＤ１００と、を含んで構成される。

【００７５】

図７は、ＩＤ利用端末６の機能構成を示す概略図である。図示するように、ＩＤ利用端末６は、ＩＤ読み取り部６１と、入出力部６２と、制御部６３と、データベース６４と、通信部６５とを有する。

【００７６】

ＩＤ読み取り部６１は、ＩＤタグ３００に付与された拡張ＩＤ２００を読み取る。たとえば、拡張ＩＤが電子回路チップ３０１のメモリに格納されている場合、電波を送信してＩＤタグ３００に装着された電子回路チップ３０１を駆動する。そして、当該電子回路チップ３０１から送信されるデータを読み取る。受信したデータに暗号化符号１０５がある場合は、受信したデータを復号化し、拡張ＩＤ２００を得る。復号化に用いる鍵は、あらかじめデータベース６４に格納しておいてもよいし、通信部６５を通じてＩＤ管理端末５に

復号化用鍵要求を送信してＩＤ管理端末５から入手してもよい。また、読み取った拡張ＩＤ２００を含む検証要求を通信部６５を通じてＩＤ管理端末５に送信し、ＩＤ管理端末５から検証結果を入手してもよい。

【００７７】

入出力部６２は、データベース６４に対し、新規に登録する情報、または、更新する情報の入力、及び、読み出した情報の表示を行なう。また、ＩＤの読み取り、データベースの読み書き、通信、などの指示を受け入れ、結果を出力する。

【００７８】

制御部６３は、ＩＤ読み取り部６１と、入出力部６２と、データベース６４と、通信部６５とを制御する。また、読み取った拡張ＩＤ２００の改竄検知符号１０２の検証を行なう。検証用の鍵は、データベース６４に格納しておいてもよいし、属性情報１０１を含む検証用鍵要求をＩＤ管理端末５に対して送信して、ＩＤ管理端末５から入手してもよい。改竄検知符号１０２の検証は、拡張ＩＤ２００を含む検証要求をＩＤ管理端末５に送信して、検証結果をＩＤ管理端末５から入手してもよい。改竄検知符号１０２の検証に成功したならば、対応づけて格納してある情報をデータベース６４から取り出し、入出力部６２で出力する。なお、取り出した情報が処理を示すものである場合、当該処理を行なう。当該処理には、たとえば、決済処理、他の端末への転送、情報が示すＵＲＬに対する問い合わせ、などがある。ＩＤの読み取りに失敗した場合は、ＩＤ読み取り部６１に再度読み取り作業を行なわせるか、または、当該ＩＤを失効ＩＤとし、電子署名を付加し、通信部６５に失効ＩＤ登録要求をＩＤ管理端末５に送信させる。

【００７９】

データベース６４は、拡張ＩＤ２００と、拡張ＩＤ２００が付与されたＩＤタグ３００と対応づけられて管理されている物品の情報とを格納する。また、ＩＤの属性情報１０１と、対応する改竄検知符号１０２の検証用の鍵とを、関連付けて格納する。また、ＩＤタグ３００に付与された暗号化した拡張ＩＤ２００を復号化するための鍵を格納する。

【００８０】

通信部６５は、復号化用鍵要求と、属性情報１０１を含む検証用鍵要求と、拡張ＩＤ２００を含む検証要求と、失効ＩＤを含む失効ＩＤ登録要求と、を作成し、通信用に暗号化し、ネットワーク２を介してＩＤ管理端末５に送信する。通信用の暗号化には、共通鍵暗号、もしくは、公開鍵暗号、もしくは、共通鍵暗号と公開鍵暗号を組み合わせたもの、を利用する。

【００８１】

なお、ＩＤ読み取り部６１と入出力部６２は、ＩＤ利用端末６以外の他の端末のものを利用し、ＩＤ利用端末６とネットワークを介して接続してもよい。また、ＩＤ読み取り部６１と入出力６２は、それぞれ複数個あってもよい。

【００８２】

なお、上記の顧客端末８、ＩＤ受注端末３、ＩＤタグ製造工場用端末４、およびＩＤ管理端末５は、図８に示すように、ＣＰＵ７１と、メモリ７２と、ハードディスク装置などの外部記憶装置７３と、ＦＤ、ＣＤ－ＲＯＭ、ＤＶＤ－ＲＯＭなどの記憶媒体７４からデータを読み取る記憶媒体読取装置７５と、キーボード、マウスなどの入力装置７６と、モニタなどの出力装置７７と、ネットワークを介して他の装置と通信を行うための通信装置７８と、これら装置間のデータ送受を司るインターフェース７９と、を備えた一般的な構成を有する電子計算機上に、構築することができる。

【００８３】

上記のＩＤ受注端末３の入出力部３１、拡張ＩＤ生成部３２、改竄検知符号生成部３３、通信部３４、ＩＤ管理端末５の通信部５１、ＩＤ関連情報管理部５２およびＩＤ関連情報管理データベース５３は、ＣＰＵ７１がメモリ７２上にロードされたプログラムを実行することで、電子計算機上に具現化されるプロセスとして実現される。また、ＩＤ管理端末５の場合、メモリ７２や外部記憶装置７３がＩＤ関連情報管理データベース５３として使用される。

【００８４】
この、ＣＰＵ７１により実行されることで電子計算機上に上記のＩＤ受注端末３を具現化するためのプログラムは、予め外部記憶装置７３に記憶され、必要に応じてメモリ７２上にロードされ、ＣＰＵ７１により実行される。あるいは、記憶媒体読取装置７５を介して記憶媒体７４からメモリ７２上にロードされ、ＣＰＵ７１により実行される。もしくは、一旦、記憶媒体読取装置７５を介して記憶媒体７４から外部記憶装置７３にインストールされた後、必要に応じて、外部記憶装置７３からメモリ７２上にロードされ、ＣＰＵ７１により実行される。さらには、他の計算機から、ネットワーク上の伝送媒体と通信装置７８を介して、いったん外部記憶装置７３にダウンロードされ、それからメモリ７２上にロードされ、あるいは直接ネットワークからメモリ７２上にロードされて、ＣＰＵ７１により実行される。

【００８５】
また、上記のＩＤ利用端末６は、図８に示す電子計算機、および、電子回路チップ読取装置、バーコード読取装置、ＯＣＲ、電子スキャナなどのＩＤ読取装置７１０を有するシステム上に、構築することができる。上記のＩＤ利用端末６のＩＤ読み取り部６１、入出力部６２、制御部６３、データベース６４および通信部６５は、ＣＰＵ７１がメモリ７２上にロードされたプログラムを実行することで、システム上に具現化されるプロセスとして実現される。また、この場合、メモリ７２や外部記憶装置７３がデータベース６４として使用される。この、ＣＰＵ７１により実行されることでシステム上に上記のＩＤタグ製造工場用端末４を具現化するためのプログラムは、予め外部記憶装置７３に記憶され、必要に応じてメモリ７２上にロードされ、ＣＰＵ７１により実行される。あるいは、記憶媒体読取装置７５を介して記憶媒体７４からメモリ７２上にロードされ、ＣＰＵ７１により実行される。もしくは、一旦、記憶媒体読取装置７５を介して記憶媒体７４から外部記憶装置７３にインストールされた後、必要に応じて、外部記憶装置７３からメモリ７２上にロードされ、ＣＰＵ７１により実行される。さらには、他の計算機から、ネットワーク上の伝送媒体と通信装置７８を介して、いったん外部記憶装置７３にダウンロードされ、それからメモリ７２上にロードされ、あるいは直接ネットワークからメモリ７２上にロードされて、ＣＰＵ７１により実行される。

【００８６】
次に、上記のＩＤ管理システムの動作について説明する。

【００８７】
まず、顧客端末８の動作について説明する。

【００８８】
図１８は、顧客端末８の動作の概略を説明するためのフロー図である。

【００８９】
まず、入出力部８１において、ＩＤタグ３００の発注情報を受け入れる（ステップ１８０１（Ｓ１８０１という，以下同様））。

【００９０】
次に、通信部８２は、Ｓ１８０１で受け入れた発注情報を含む、受注情報要求を作成し、通信用に暗号化してネットワーク７を介してＩＤ受注端末３に送信する（Ｓ１８０２）。そして、ＩＤ受注端末３から、受注情報を受信するまで待機する（Ｓ１８０３）。受信したならば（Ｓ１８０３のＹｅｓ）、通信部８２は受信した暗号文の復号化を行ない、入出力部８１は、通信部８２で得た受注情報を出力する（Ｓ１８０４）。

【００９１】
次に、ＩＤ受注端末３の動作について説明する。

【００９２】
図９は、ＩＤ受注端末３の動作の概略を説明するためのフロー図である。

【００９３】
まず、通信部４１は、ネットワーク７を介して顧客端末８から発注情報を含む受注情報要求を受信するまで、待機する（Ｓ１３１６）。受信したならば（Ｓ１３１６のＹｅｓ）、

通信部４１は、受信した暗号文の復号化を行ない、発注情報を入手する（Ｓ１３０１）。
【００９４】
次に、通信部３４は、Ｓ１３０１で受け入れた発注情報を含む、ＩＤ重複確認要求を作成し、通信用に暗号化してネットワーク１を介してＩＤ管理端末５に送信する（Ｓ１３０２）。そして、ＩＤ管理端末５から、前記ＩＤ重複確認要求に対する処理結果を受信するまで待機する（Ｓ１３０３）。
【００９５】
次に、発注情報が示すＩＤとＩＤ管理端末５に登録済みのＩＤとが重複していた場合（Ｓ１３０４のＹｅｓ）、入出力部３１は、エラーを出力する（Ｓ１３０５）。重複していない場合（Ｓ１３０４のＮｏ）、拡張ＩＤ生成部３２は、発注情報からＩＤの属性情報１０１、クラス情報１０３、バージョン情報１０４を生成する（Ｓ１３０６）。発注情報に、改竄検知符号１０２生成用の鍵、または拡張ＩＤ２００の暗号化用の鍵、のいずれかが含まれていない場合（Ｓ１３０７のＮｏ）は、拡張ＩＤ生成部３２は、乱数を生成する（Ｓ１３０８）。
【００９６】
次に、改竄検知符号生成部３３は、発注情報に含まれる改竄検知符号１０２生成用の鍵と、ＩＤ１００と、Ｓ１３０６で生成された属性情報１０１、クラス情報１０３またはバージョン情報１０４と、を用いて改竄検知符号１０２と、検証用の鍵と、を生成する（Ｓ１３０９）。発注情報に、改竄検知符号１０２生成用の鍵が含まれていない場合は、改竄検知符号１０２生成用の鍵として、Ｓ１３０８で入手した乱数値を用いる。
【００９７】
次に、拡張ＩＤ生成部３２は、発注情報に含まれるＩＤ１００と、Ｓ１３０６で生成された属性情報１０１、クラス情報１０３またはバージョン情報１０４と、Ｓ１３０９で生成された改竄検知符号１０２と、を用いて拡張ＩＤ２００を生成する（Ｓ１３１０）。拡張ＩＤ２００の暗号化が必要であった場合（Ｓ１３１１のＹｅｓ）は、拡張ＩＤ生成部３２は、発注情報に含まれる暗号化用の鍵を用いて暗号化を行ない（Ｓ１３１２）、暗号化符号１０５を添付する（Ｓ１３１３）。発注情報に、暗号化用の鍵が含まれていない場合は、暗号化用の鍵として、Ｓ１３０８で入手した乱数値を用いる。
【００９８】
次に、通信部３４は、Ｓ１３０１で受け入れた発注情報と、Ｓ１３１０で作成した拡張ＩＤ２００、もしくは、Ｓ１３１３で作成した暗号化した拡張ＩＤ２００と、Ｓ１３０８で生成した乱数値から得た鍵と、を含む受注情報を生成する（Ｓ１３１７）。
【００９９】
次に、通信部３４は、Ｓ１３１７で生成した受注情報を含む、受注ＩＤ登録要求を作成し、通信用に暗号化してネットワーク１を介してＩＤ管理端末５に送信する（Ｓ１３１４）。また、通信部３４は、Ｓ１３１７で生成した受注情報を含む、ＩＤタグ製造要求を作成し、通信用に暗号化してネットワーク１を介してＩＤタグ製造工場用端末４に送信する（Ｓ１３１５）。また、通信部３４は、Ｓ１３１７で生成した受注情報を、通信用に暗号化してネットワーク７を介して顧客端末８に送信する（Ｓ１３１８）。
【０１００】
なお、Ｓ１３１４、Ｓ１３１５、およびＳ１３１８の順番は入れ替わってもよい。
【０１０１】
なお、Ｓ１３０６～Ｓ１３１０の処理を、Ｓ１３０１の直後に行なってもよい。この場合は、Ｓ１３０２において作成するＩＤ重複確認要求には、Ｓ１３１０で生成された拡張ＩＤ２００が含まれる。
【０１０２】
次に、ＩＤタグ製造工場用端末４の動作について説明する。
【０１０３】
図１０は、ＩＤタグ製造工場用端末４の動作を説明するためのフロー図である。
【０１０４】

まず、通信部４１は、ネットワーク１を介してＩＤ受注端末３からＩＤタグ製造要求を受信するまで、待機する（Ｓ１４０１）。受信したならば（Ｓ１４０１のＹｅｓ）、通信部４１は、受信した暗号文の復号化を行ない、受注情報を入手する（Ｓ１４０２）。

【０１０５】

次に、制御部４４は、Ｓ１４０２で入手した受注情報に含まれる拡張ＩＤ２００を格納したＩＤタグ３００を製造するよう、製造部４２に指示し、製造部４２は、該受注情報に従ってＩＤタグ３００を製造する（Ｓ１４０３）。

【０１０６】

次に、制御部４４は、Ｓ１４０３で製造されたＩＤタグ３００の機能が正常か否かを検査するよう、検査部４３に指示し、検査部４３は、製造部４２から受け取ったＩＤタグ３００を検査し、制御部４４より受け取った拡張ＩＤ２００が正しく格納されていることなどを確認する。（Ｓ１４０４）。

【０１０７】

制御部４４は、検査部４３から受け取った検査結果が正常であったならば（Ｓ１４０５のＹｅｓ）、ＩＤタグ３００に付与されている拡張ＩＤ２００を、製造済みＩＤとする（Ｓ１４０６）。通信部４１は、Ｓ１４０６で得た製造済みＩＤを含む、製造済みＩＤ登録要求を作成し、通信用に暗号化してネットワーク１を介してＩＤ管理端末５に送信する（Ｓ１４０７）。

【０１０８】

次に、納入部４５は、検査部４３で検査結果が合格であったＩＤタグ３００を受け取り、受注情報に含まれる納入方法に従って、顧客に対して発送・引き渡しなどを行ない、納入する（Ｓ１４１１）。

【０１０９】

一方、検査部４３から受け取った検査結果が異常であったならば（Ｓ１４０５のＮｏ）、制御部４４は、ＩＤタグ３００に付与されている拡張ＩＤ２００を、欠番ＩＤとする（Ｓ１４０８）。検査結果が異常であったＩＤタグ３００の再製造が必要な場合（Ｓ１４０９のＹｅｓ）、制御部４４は、製造部４２にＩＤタグ３００の再製造を行なわせ、Ｓ１４０８で得た欠番ＩＤを付与する（Ｓ１４０３）。一方、再製造が必要ない場合（Ｓ１４０９のＮｏ）、通信部４１は、欠番ＩＤを含む欠番ＩＤ登録要求を作成し、通信用に暗号化してネットワーク１を介してＩＤ管理端末５に送信する（Ｓ１４１０）。

【０１１０】

次に、ＩＤ管理端末５の動作について説明する。

【０１１１】

図１１は、ＩＤ管理端末５の動作を説明するためのフロー図である。

【０１１２】

まず、通信部５１は、ＩＤ受注端末３またはＩＤタグ製造工場用端末４からネットワーク１を介した要求、もしくは、ＩＤ利用端末６からネットワーク２を介した要求、を受信するまで、待機する（Ｓ１５０１）。受信したならば（Ｓ１５０１のＹｅｓ）、通信部５１は、受信した暗号文の復号化を行ない、後述する各種情報を含んだ要求を得る（Ｓ１５０２）。

【０１１３】

次に、ＩＤ関連情報管理部５２は、Ｓ１５０２で入手した要求内容を解析する。

【０１１４】

入手した要求内容が、ＩＤ受注端末３からのＩＤ重複確認要求であるならば、ＩＤ関連情報管理部５２は、前記ＩＤ重複確認要求に含まれる発注情報を入手する（Ｓ１５１１）。次に、Ｓ１５１１で入手した発注情報に含まれる拡張ＩＤ２００と、ＩＤ関連情報管理データベース５３に格納してある拡張ＩＤ２００と、を用いて、ＩＤが重複するか否かを確認する（Ｓ１５１２）。ＩＤ関連情報管理データベース５３に同一の拡張ＩＤ２００が格納されていても、該拡張ＩＤ２００が失効扱いであるならば、重複していないものとする。そして、確認の結果を通信部５１で暗号化し、ネットワーク１を介してＩＤ受注端末３

に送信する（Ｓ１５１３）。
【０１１５】
入手した要求内容が、ＩＤ受注端末３からの受注ＩＤ登録要求であるならば、ＩＤ関連情報管理部５２は、前記受注ＩＤ登録要求に含まれる、受注情報を入手する（Ｓ１５２１）。次に、Ｓ１５２１で入手した受注情報を、ＩＤ関連情報管理データベース５３に格納する（Ｓ１５２２）。
【０１１６】
入手した要求内容が、ＩＤタグ製造工場用端末４からの製造済みＩＤ登録要求であるならば、ＩＤ関連情報管理部５２は、前記製造済みＩＤ登録要求に含まれる製造済みＩＤを入手する（Ｓ１５３１）。次に、Ｓ１５３１で入手した製造済みＩＤを、ＩＤ関連情報管理データベース５３に格納する（Ｓ１５３２）。
【０１１７】
入手した要求内容が、ＩＤタグ製造工場用端末４からの欠番ＩＤ登録要求であるならば、ＩＤ関連情報管理部５２は、前記欠番ＩＤ登録要求に含まれる欠番ＩＤを入手する（Ｓ１５４１）。次に、Ｓ１５４１で入手した欠番ＩＤを、ＩＤ関連情報管理データベース５３に格納する（Ｓ１５４２）。
【０１１８】
入手した要求内容が、ＩＤ利用端末６からの検証要求であるならば、ＩＤ関連情報管理部５２は、検証要求に含まれる拡張ＩＤ２００を入手する（Ｓ１５５１）。次に、Ｓ１５５１で入手した拡張ＩＤ２００と、ＩＤ関連情報管理データベース５３に格納してある拡張ＩＤ２００と、を比較して、改竄検知符号１０２が正当なものであるか否かを検証する（Ｓ１５５２）。そして、検証の結果を通信部５１で暗号化し、ネットワーク２を介してＩＤ利用端末６に送信する（Ｓ１５５３）。
【０１１９】
入手した要求内容が、ＩＤ利用端末６からの検証用鍵要求であるならば、ＩＤ関連情報管理部５２は、前記改竄検知符号１０２の検証用鍵要求に含まれる属性情報１０１を入手する（Ｓ１５６１）。次に、Ｓ１５６１で入手した属性情報１０１と関連付けられてＩＤ関連情報管理データベース５３に格納してある、改竄検知符号１０２の検証用の鍵を取り出す（Ｓ１５６２）。そして、Ｓ１５６２で取り出した改竄検知符号１０２の検証用の鍵を通信部５１で暗号化し、ネットワーク２を介してＩＤ利用端末６に送信する（Ｓ１５６３）。
【０１２０】
入手した要求内容が、ＩＤ利用端末６からの復号化用鍵要求であるならば、ＩＤ関連情報管理部５２は、ＩＤ関連情報管理データベース５３に格納してある、暗号化拡張ＩＤ２００の復号化用の鍵を取り出す（Ｓ１５７１）。次に、Ｓ１５７１で取り出した暗号化拡張ＩＤ２００の復号化用の鍵を、通信部５１で暗号化し、ネットワーク２を介してＩＤ利用端末６に送信する（Ｓ１５７２）。
【０１２１】
入手した要求内容が、ＩＤ利用端末６からの失効ＩＤ登録要求であるならば、ＩＤ関連情報管理部５２は、前記失効ＩＤ登録要求に含まれる、失効ＩＤと電子署名を入手する（Ｓ１５８１）。次に、Ｓ１５８１で入手した電子署名により正当な失効ＩＤ登録要求であることを確認し、Ｓ１５８１で入手した失効ＩＤを、ＩＤ関連情報管理データベース５３に格納する（Ｓ１５８２）。
【０１２２】
次に、ＩＤ利用端末６の動作について説明する。
【０１２３】
図１２は、ＩＤ利用端末６の動作の概略を説明するためのフロー図である。
【０１２４】
まず、入出力部６２において、指示入力を受け入れる（Ｓ１６０１）。
【０１２５】

次に、制御部６３は、Ｓ１６０１で受け入れた指示の解析を行なう（Ｓ１６０２）。

【０１２６】

Ｓ１６０１で受け入れた指示が、情報の読み取り指示、または、情報の更新指示、または、情報の新規登録指示の場合、読み取り部６１、制御部６３、データベース６４および通信部６５は、ＩＤ読取手続（Ｓ１６０３）を行なう。Ｓ１６０３についての詳細は図１３～１５で説明する。

【０１２７】

Ｓ１６０１で受け入れた指示が、失効登録指示の場合、制御部６３、データベース６４および通信部６５は、読み取ろうとしたＩＤタグ３００に付与されている拡張ＩＤ２００を失効扱いとするための失効手続（Ｓ１６０４）を行なう。Ｓ１６０４についての詳細は図１９で説明する。

【０１２８】

Ｓ１６０１で受け入れた指示が、情報の読み取り指示の場合、Ｓ１６０３の後、制御部６３は、データベース６４より、Ｓ１６０３で入手した拡張ＩＤ２００と対応づけられて格納されている情報を取り出す（Ｓ１６０５）。そして、Ｓ１６０５で取り出した情報を入出力部６２で出力する、情報の指示に従い決済処理を行なう、情報が示す端末へ転送処理を行なう、など、情報に応じた処理を行なう（Ｓ１６０６）。

【０１２９】

Ｓ１６０１で受け入れた指示が、更新情報を含む、情報の更新指示の場合、Ｓ１６０３の後、制御部６３は、更新情報を入手する（Ｓ１６０７）。そして、データベース６４に、Ｓ１６０３で入手した拡張ＩＤ２００と対応づけられて格納されている情報を、Ｓ１６０７で入手した更新情報で更新する（Ｓ１６０８）。

【０１３０】

Ｓ１６０１で受け入れた指示が、対応情報を含む、情報の新規登録指示の場合、Ｓ１６０３の後、制御部６３は、対応情報を入手する（Ｓ１６０９）。そして、Ｓ１６０９で入手した対応情報と、Ｓ１６０３で入手した拡張ＩＤ２００と、を対応づけて、データベース６４に格納する（Ｓ１６１０）。

【０１３１】

図１３は、図１２に示すＳ１６０３（ＩＤ読取手続）の処理の概要を説明するためのフロー図である。

【０１３２】

まず、ＩＤ読み取り部６１は、電波を送信してＩＤタグ３００に装着された電子回路チップ３０１を駆動する。そして、当該電子回路チップ３０１から送信されるデータを読み取る（Ｓ１６１１）。

【０１３３】

次に、制御部６３は、Ｓ１６１１で読み取ったデータに暗号化符号１０５がある場合（Ｓ１６１２のＹｅｓ）、復号化手続を行なう（Ｓ１６１３）。なお、Ｓ１６１３についての詳細は図１４で説明するため、ここでは省略する。

【０１３４】

次に、制御部６３は、Ｓ１６１１で読み取ったデータ、もしくは、Ｓ１６１３で復号化を行なって入手したデータ、の検証手続を行なう（Ｓ１６１４）。なお、Ｓ１６１４についての詳細は図１５で説明するため、ここでは省略する。

【０１３５】

Ｓ１６１４の結果がエラーの場合（Ｓ１６１５のＹｅｓ）、制御部６３は、再読み取りの規定回数内か否かを判断する。（Ｓ１６１８）。規定回数内の場合（Ｓ１６１８のＹｅｓ）は、再度、ＩＤの読み取りを行なう（Ｓ１６１１）。読み取り回数が規定回数に達している場合（Ｓ１６１８のＮｏ）、入出力部６２にエラーを出力する（Ｓ１６１６）。

【０１３６】

一方、Ｓ１６１４の結果がエラーでない場合（Ｓ１６１５のＮｏ）、制御部６３は、正当に検証された拡張ＩＤ２００を入手する（Ｓ１６１７）。

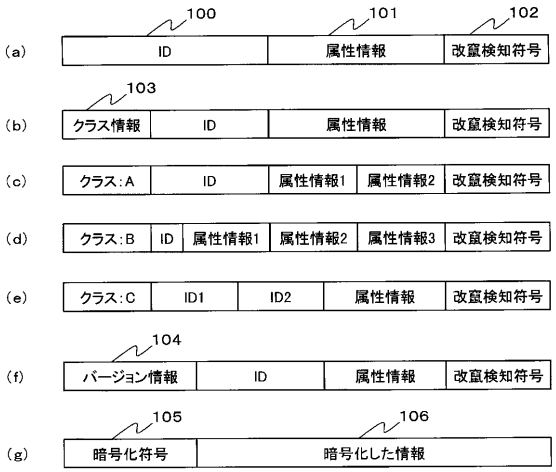
【０１３７】
図１４は、図１３に示すＳ１６１３（復号化手続）の処理を説明するためのフロー図である。
【０１３８】
まず、制御部６３は、データベース６４に、復号化用の鍵が格納されているか否かを確認する（Ｓ１６２１）。格納されていない場合（Ｓ１６２１のＮｏ）は、通信部６５は、復号化用鍵要求を作成し、通信用に暗号化してネットワーク２を介してＩＤ管理端末５に送信する（Ｓ１６２２）。そして、ＩＤ管理端末５から復号化用の鍵を受信するまで待機する（Ｓ１６２３）。
【０１３９】
次に、制御部６３は、データベース６４に格納されている復号化用の鍵、もしくは、Ｓ１６２３で得た復号化用の鍵、を用いて、暗号化拡張ＩＤ２００を復号化する（Ｓ１６２４）。
【０１４０】
図１５は、図１３に示すＳ１６１４（検証手続）の処理を説明するためのフロー図である。
【０１４１】
図１３に示すＳ１６１４（検証手続）の処理の一例として、まず、図１５（ａ）を説明する。
【０１４２】
まず、制御部６３は、データベース６４に、検証用の鍵が格納されているか否かを確認する（Ｓ１６３１）。格納されていない場合（Ｓ１６３１のＮｏ）は、通信部６５は、属性情報１０１を含む検証用鍵要求を作成し、通信用に暗号化してネットワーク２を介してＩＤ管理端末５に送信する（Ｓ１６３２）。そして、ＩＤ管理端末５から検証用の鍵を受信するまで待機する（Ｓ１６３３）。
【０１４３】
次に、制御部６３は、データベース６４に格納されている検証用の鍵、もしくは、Ｓ１６３３で得た検証用の鍵、を用いて、改竄検知符号１０２の検証を行なう（Ｓ１６３４）。
【０１４４】
図１３に示すＳ１６１４（検証手続）の処理のもう一つの例として、図１５（ｂ）を説明する。
【０１４５】
通信部６５は、拡張ＩＤ２００を含む検証要求を作成し、通信用に暗号化してネットワーク２を介してＩＤ管理端末５に送信する（Ｓ１６３５）。そして、ＩＤ管理端末５から検証結果を受信するまで待機する（Ｓ１６３６）。
【０１４６】
図１９は、図１２に示すＳ１６０４（失効手続）の処理を説明するためのフロー図である。
【０１４７】
まず、入出力部６２において、読み取りに失敗したＩＤタグ３００に関して、該ＩＤタグ３００の表面に印字されている記号や、該ＩＤタグ３００が付与されていた物品の情報、など、該ＩＤタグ３００に付与されている拡張ＩＤ２００を推定するためのタグ情報の入力を得る（Ｓ１６４１）。
【０１４８】
次に、制御部６３は、Ｓ１６４１で受け入れたタグ情報をデータベース６４で検索し、対応づけられている拡張ＩＤ２００を取り出す（Ｓ１６４２）。取り出した拡張ＩＤ２００を失効ＩＤとする（Ｓ１６４３）。
【０１４９】
次に、通信部６５は、電子署名を生成する（Ｓ１６４４）。該電子署名と失効ＩＤとを含む、失効ＩＤ登録要求を作成し、通信用に暗号化してネットワーク２を介してＩＤ管理端

末５に送信する（Ｓ１６４５）。
【０１５０】
以上、本発明の一実施形態について説明した。
【０１５１】
本実施形態によれば、ＩＤ受注端末３と、ＩＤ製造工場用端末４およびＩＤ管理端末５は、ネットワーク１を介して暗号通信を行なっている。また、受注情報、発行済みＩＤ、欠番ＩＤなどの情報をＩＤ管理端末５において一括管理している。また、ＩＤタグ３００として、拡張ＩＤ２００が書き換え不可領域に格納された電子回路チップ３０１を利用しているため、不正な第三者が、ＩＤタグ３００に付与されている拡張ＩＤ２００を改変することはできない。また、電子回路チップ３０１を製造するには、十分な設備が必要である。そして、電子回路チップ３０１を小型・薄型にするほど、電子回路チップ３０１を製造できる者が限られてくるため、不正な第三者がＩＤタグの複製を製造する可能性が低くなる。また、ＩＤを失効扱いとする際には、その旨を要求してきたＩＤ利用端末６の電子署名を確認し、正当な権利を有する場合のみ、ＩＤを失効扱いとする。以上のことより、ＩＤ管理端末５が市場に流通するＩＤタグ３００の個数を管理することができる。また、機密性の高い情報を秘密裏に管理することができる。
【０１５２】
また、本実施形態では、ＩＤ利用端末６に、検証用の鍵や装置を保持していなくても、ＩＤ管理端末５に、ネットワーク２を通じてＩＤ１００とＩＤの属性情報１０１と改竄検知符号１０２とを含む検証要求を送信すれば、検証結果を得ることができる。
【０１５３】
また、本実施形態では、ＩＤ利用端末６に、検証用の鍵を保持していなくても、ＩＤ管理端末５に、ネットワーク２を通じてＩＤの属性情報１０１を含む検証用鍵要求を送信すれば、検証用の鍵を得ることができる。
【０１５４】
なお、本発明は、上記の実施形態に限定されるものではなく、その要旨の範囲内で数々の変形が可能である。
【０１５５】
たとえば、上記の実施形態において、ＩＤ利用端末６は、必ずしも１つの装置上に構築されているものである必要はない。たとえば、拡張ＩＤ２００の読み取りや、情報または指示の入出力に係わる部分と、データベース６４に係わる部分とを、それぞれ別個の装置上に構築し、これらの装置をネットワークで接続するような構成としてもよい。また、それとは逆に、ＩＤ利用端末６のデータベース６４に係わる部分の機能をＩＤ管理端末５に持たせてもかまわない。
【０１５６】
また、たとえば、上記の実施形態において、顧客端末８からＩＤ受注端末３に送られてくる受注情報要求に含まれる発注情報に、検証用鍵または暗号用鍵が含まれていない場合、ＩＤ受注端末３で乱数を生成し、該乱数を鍵として扱うことにしているが、乱数生成機能を顧客端末８に持たせてもよい。この場合、顧客端末８において、生成した乱数を検証用鍵または暗号用鍵として発注情報に含ませ、ＩＤ受注端末３に送る。
【０１５７】
【発明の効果】
以上説明したように、本発明によれば、改竄検知符号を備えたＩＤの発行と流通を管理し、ＩＤを利用した物品管理を効率よく、かつ、信頼性高く行うことが可能な仕組みを提供できる。
【図面の簡単な説明】
【図１】本実施形態のＩＤ管理システムで用いるＩＤの一例を示した図である。
【図２】本実施形態のＩＤ管理システムで用いるＩＤタグの一例を示した図である。
【図３】本実施形態が適用されたＩＤ管理システムの概略図である。
【図４】図３に示すＩＤ受注端末３の機能構成を示す概略図である。

【図５】図３に示すＩＤタグ製造工場４６の機能構成を示す概略図である。
【図６】図３に示すＩＤ管理端末５の機能構成を示す概略図である。
【図７】図３に示すＩＤ利用端末６の機能構成を示す概略図である。
【図８】図３に示すＩＤ管理システムを構成する各装置３～６、および８のハードウエア構成例を示す図である。
【図９】図４に示すＩＤ受注端末３の動作を説明するためのフロー図である。
【図１０】図５に示すＩＤタグ製造工場用端末４の動作を説明するためのフロー図である。
【図１１】図６に示すＩＤ管理端末５の動作を説明するためのフロー図である。
【図１２】図７に示すＩＤ利用端末６の動作の概要を説明するためのフロー図である。
【図１３】図１２に示すＳ１６０２（ＩＤ読取手続）の処理の概要を説明するためのフロー図である。
【図１４】図１３に示すＳ１６１３（復号化手続）の処理を説明するためのフロー図である。
【図１５】図１３に示すＳ１６１４（検証手続）の処理を説明するためのフロー図である。
【図１６】図３に示す顧客端末８の機能構成を示す概略図である。
【図１７】図６に示すＩＤ管理端末５のＩＤ関連情報管理データベース５３に格納される、ＩＤタグ３００に関連する管理情報を説明するための図である。
【図１８】図１６に示す顧客端末８の動作を説明するためのフロー図である。
【図１９】図１２に示すＳ１６０４（失効手続）の処理の概要を説明するためのフロー図である。
【符号の説明】
１…ネットワーク，　３…ＩＤ受注端末，４…製造工場用端末，５…ＩＤ管理端末，　１００…ＩＤ，１０１…ＩＤの属性情報，１０２…改竄検知符号，　２００…拡張ＩＤ，３００…ＩＤタグ，３０１…電子回路チップ。

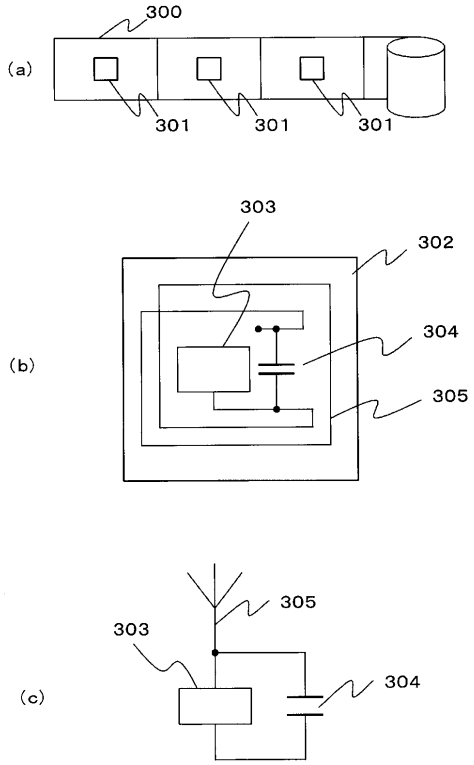
【図１】

図1



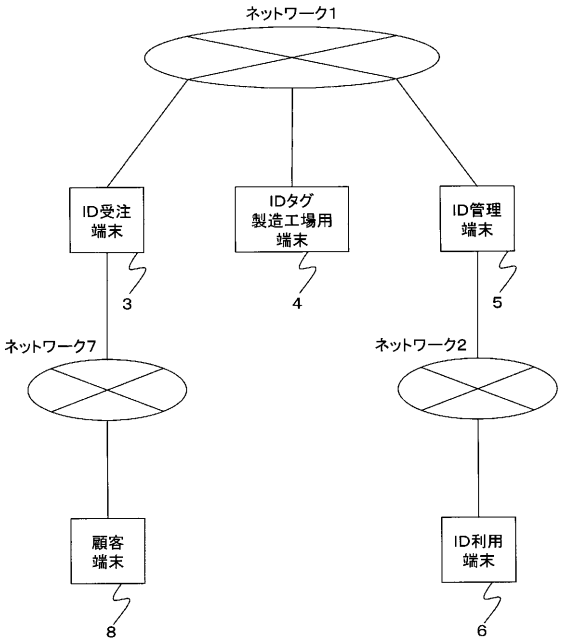
【図２】

図2



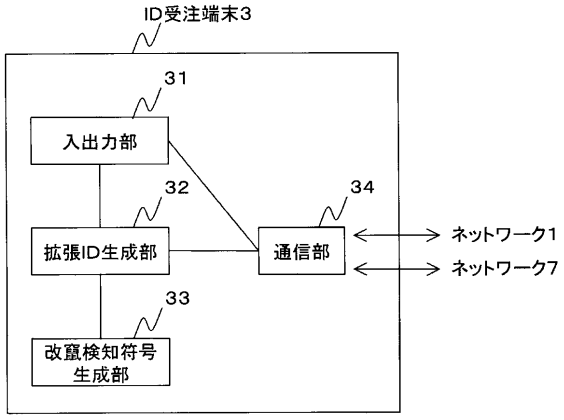
【図３】

図3



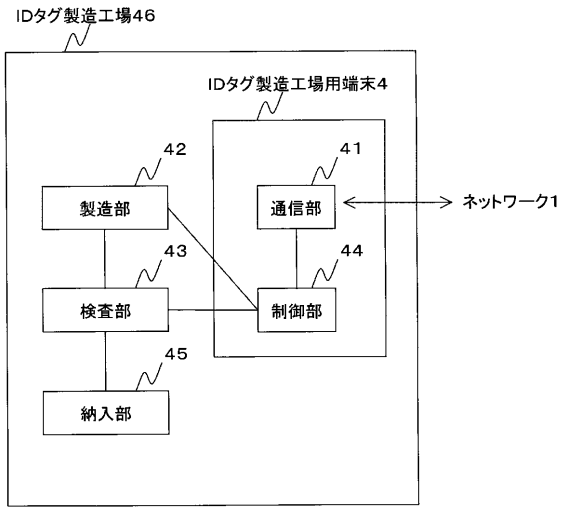
【図４】

図4



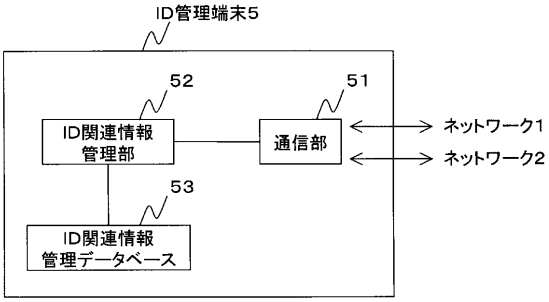
【図５】

図5



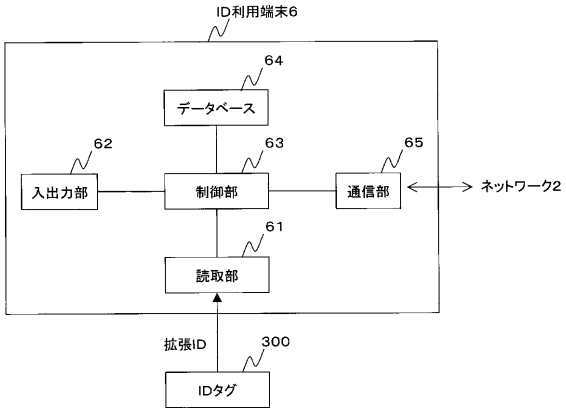
【図６】

図6



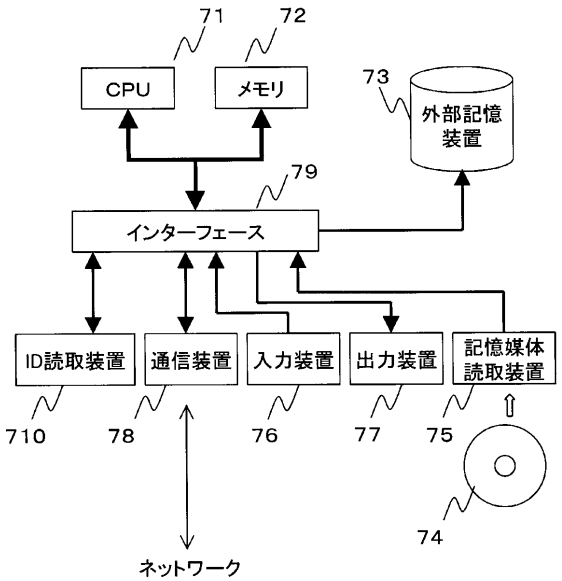
【図７】

図7



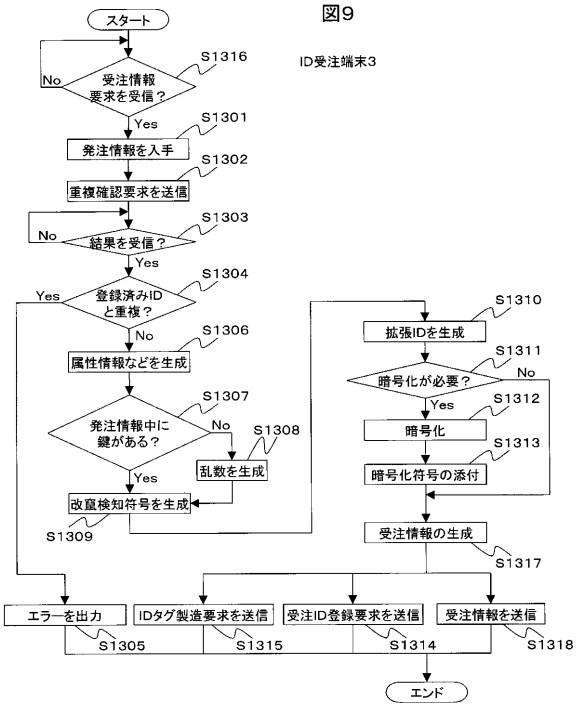
【図８】

図8



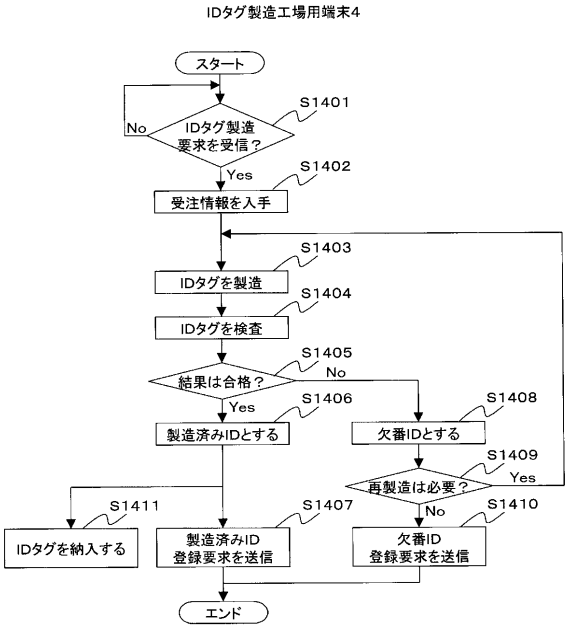
【図９】

図9



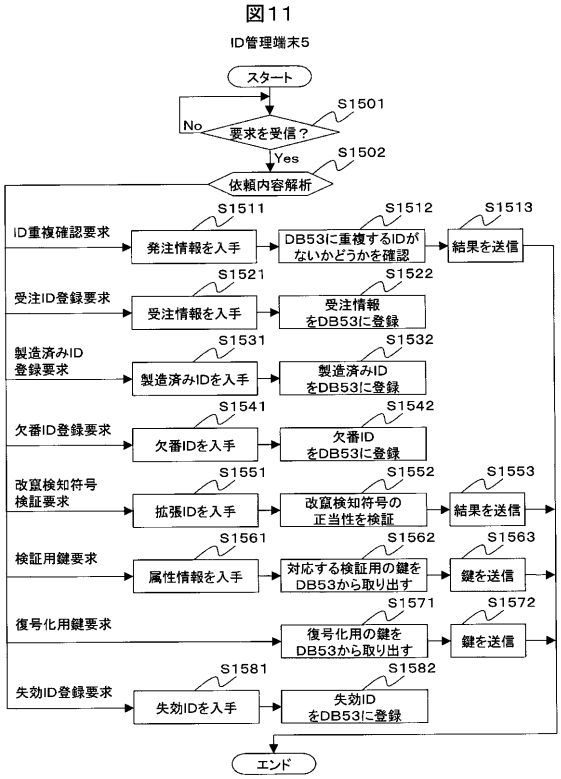
【図１０】

図10



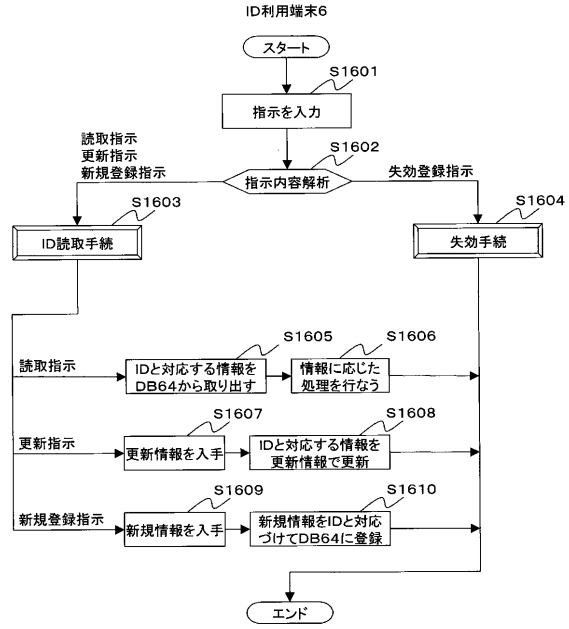
【図１１】

図11



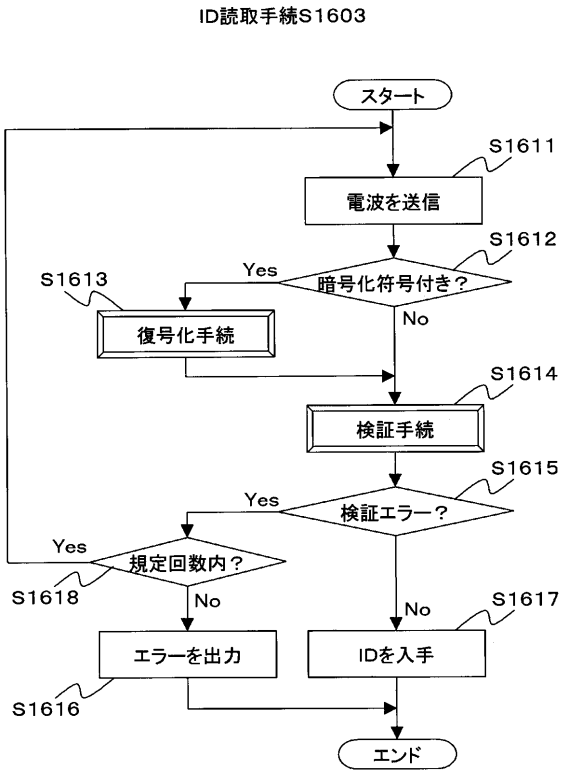
【図１２】

図12



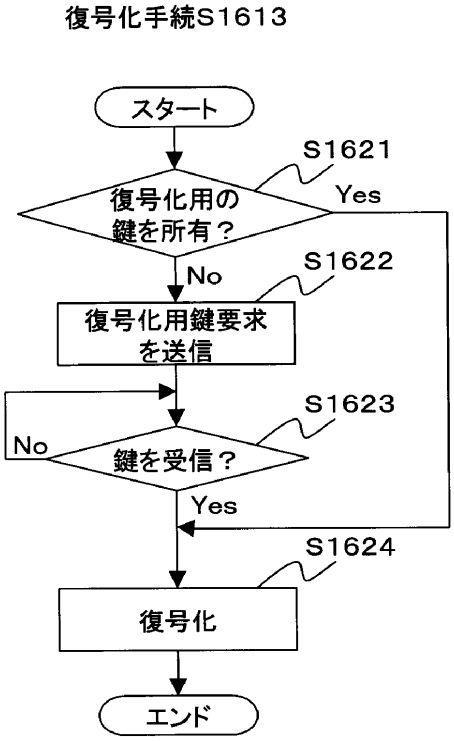
【図１３】

図13



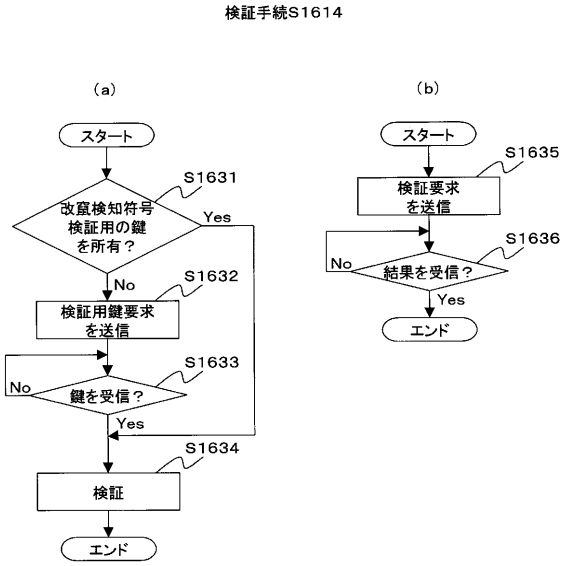
【図１４】

図14



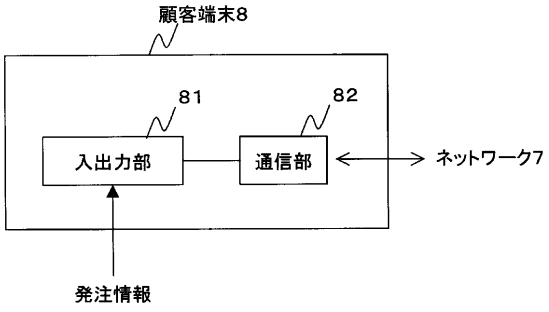
【図１５】

図15



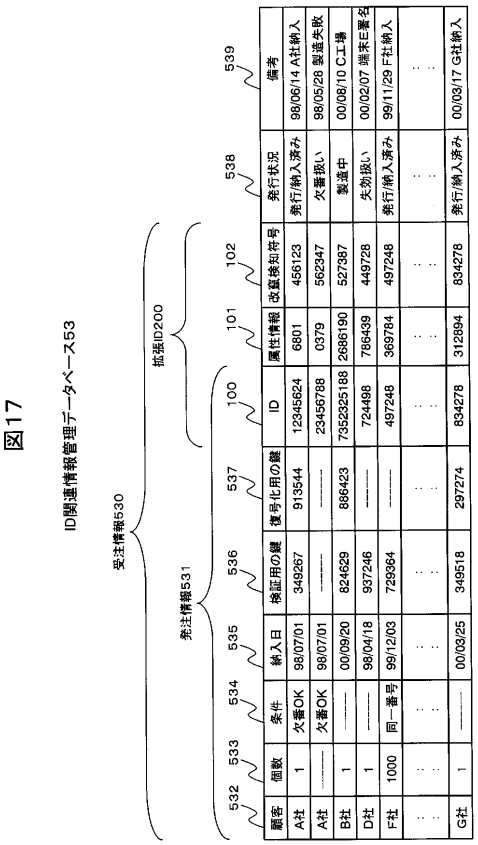
【図１６】

図16



【図１７】

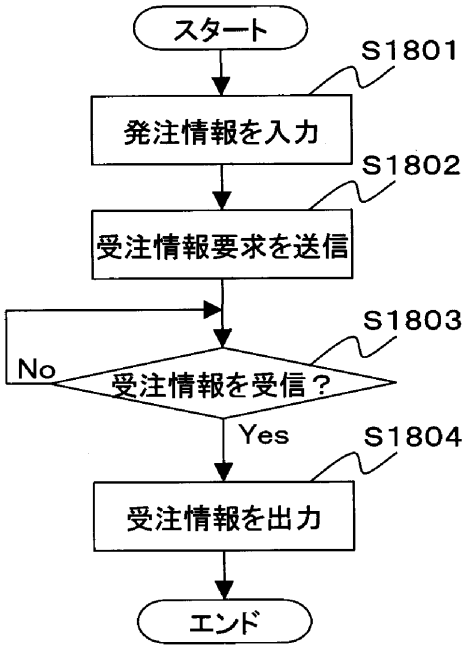
図17



顧客	個数	条件	納入日	検証用の鍵	復号化用の鍵	ID	属性情報	改竄検知符号	発行状況	備考
A社	1	欠番OK	98/07/01	349267	913544	12345624	6801	456123	発行/納入済み	98/06/14 A社納入
A社	——	欠番OK	98/07/01	——	——	23456788	0379	562347	欠番扱い	98/05/28 製造失敗
B社	1	——	00/09/20	824629	886423	73523251 88	2686190	527387	製造中	00/08/10 C工場
D社	1	——	98/04/18	937246	——	724498	786439	449728	失効扱い	00/02/07 端末E署名
F社	1000	同一番号	99/12/03	729364	——	497248	369784	497248	発行/納入済み	99/11/29 F社納入
：：	：：	：：	：：	：：	：：	：：	：：	：：	：：	：：
G社	1	——	00/03/25	349518	297274	834278	312894	834278	発行/納入済み	00/03/17 G社納入

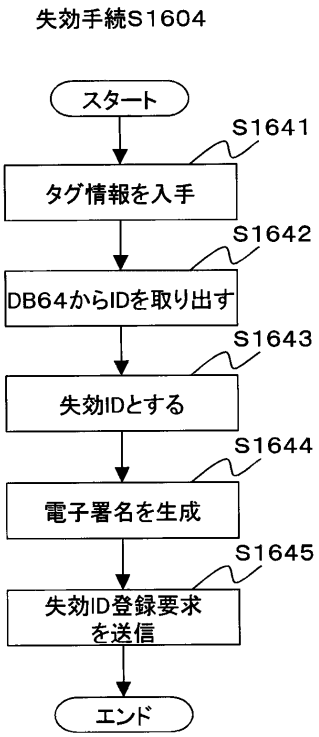
【図１８】

図18



【図１９】

図19



フロントページの続き

(72)発明者　福澤　寧子
神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内

Ｆターム(参考) 5B035 AA06　AA15　BB09　CA23