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

特許第4680489号
(P4680489)

(45)発行日　平成23年5月11日(2011.5.11)　(24)登録日　平成23年2月10日(2011.2.10)

| (51)Int.Cl. | | F I | | |
|---|---|---|---|---|
| G06F 21/24 | (2006.01) | G06F | 12/14 | 530P |
| G06K 17/00 | (2006.01) | G06F | 12/14 | 510F |
| H04L 9/32 | (2006.01) | G06K | 17/00 | S |
| G06K 19/10 | (2006.01) | H04L | 9/00 | 673E |
| | | G06K | 19/00 | R |

請求項の数 2　(全 16 頁)

(21)出願番号　特願2003-360076 (P2003-360076)
(22)出願日　平成15年10月21日 (2003.10.21)
(65)公開番号　特開2005-128592 (P2005-128592A)
(43)公開日　平成17年5月19日 (2005.5.19)
審査請求日　平成18年9月7日 (2006.9.7)

(73)特許権者　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目７番３号
(74)代理人　100099461
弁理士　溝井　章司
(74)代理人　100114878
弁理士　山地　博人
(72)発明者　小林　信博
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
(72)発明者　高島　克幸
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内

審査官　深沢　正志

最終頁に続く

(54)【発明の名称】情報記録読取システム

(57)【特許請求の範囲】
【請求項１】
秘密情報Ｓを複数の分散情報に分散する場合の分散個数ｎ（ｎは自然数）と、分散したｎ個の分散情報より少ない個数の分散情報に基づいて上記秘密情報Ｓを復元する場合の最小個数ｋ（ｋ＜ｎ）とに基づいて上記秘密情報Ｓをｎ個の分散情報に分散し、分散したｎ個の分散情報の各分散情報をｎ個のチップの各チップに記録する情報記録読取システムであって、
ｋ－１個の乱数を乱数$a_1$～$a_{(k-1)}$として生成し、素数ｒを生成し、上記秘密情報Ｓを定数項とする（ｋ－１）次の多項式をｆ（ｘ）とし、$f(x)=S+a_1\cdot x+a_2\cdot x^2+\cdots+a_{k-1}\cdot x^{k-1}\pmod r$（前記ｆ（ｘ）の式において「$a_{k-1}\cdot x^{k-1}\pmod r$」は「$a_{k-1}\cdot x^{k-1}$」の演算結果を「ｒ」で割った余りを意味する）の式に基づいてｊ＝１，…，ｎとしｆ（ｊ）を算出して算出したｆ（ｊ）を$w_j$とし、上記ｊ（ｊ＝１，…，ｎ）と$w_j$（ｊ＝１，…，ｎ）とを有するｎ個の分散情報$B_j$（ｊ＝１，…，ｎ）を出力するとともに上記乱数$a_1$～$a_{(k-1)}$と上記素数ｒとを出力する情報分散部と、
上記情報分散部が出力した乱数$a_1$～$a_{(k-1)}$と素数ｒとを入力し、入力した素数ｒで割り切ることができるｐ－１であり、かつ、上記ｐ－１のｐが素数である素数ｐを生成し、乗法群$Z^*_p$での位数が上記素数ｒとなる要素ｇを定め、$C_0=g^s\pmod p$の式と、ｊ＝１，…，ｋ－１とし$C_j=f(j)$の式とに基づいて$C_0$と$C_j$（ｊ＝１，…，ｋ－１）を算出し、上記素数ｐと上記要素ｇと算出した$C_0$と算出した$C_j$（ｊ＝１，…，ｋ－１）とを有する検証用情報Ｖであって上記ｎ個の分散情報$B_j$（ｊ＝１，…，ｎ）が正当な

分散情報であるか否かを検証する検証用情報Ｖを出力する検証用情報生成部と、
上記情報分散部により出力されたｊと$w_j$（ｊ＝１，…，ｎ）とを有するｎ個の分散情報$B_j$（ｊ＝１，…，ｎ）の各分散情報と上記検証用情報生成部により出力された素数ｐと要素ｇと$C_0$と$C_j$（ｊ＝１，…，ｋ－１）とを有する検証用情報Ｖとを有するｎ個の分散識別子(分散ＩＤ)である分散$ID_j$（ｊ＝１，…，ｎ）を生成する秘密情報分散部と、
上記秘密情報分散部により生成されたｎ個の分散ＩＤを個々にｎ個のチップに記録する情報設定部と
を備えたことを特徴とする情報記録読取システム。
【請求項２】
上記情報設定部によりｎ個の分散ＩＤの各分散ＩＤが記録されたｎ個のチップを取り付けた物品に対応する物品情報と上記秘密情報Ｓとを情報リストとしてデータベースに記憶する情報蓄積部と、
上記物品に取り付けられたｎ個のチップからｎ個の分散ＩＤを受信する読取部と、
上記読取部により受信されたｎ個の分散ＩＤの各分散ＩＤごとに、当該分散ＩＤが有する分散情報と検証用情報Ｖとに基づいて当該分散ＩＤが有する分散情報が正当な分散情報であるか否かを検証し、当該分散情報が正当な分散情報であることを検証した場合、当該分散ＩＤを出力する分散情報検証部と、
上記分散情報検証部により出力された分散ＩＤの数が上記ｋ個以上の場合、ｋ個以上の分散ＩＤのなかからｋ個の分散ＩＤを取得し、取得したｋ個の分散ＩＤの各分散ＩＤが有する分散情報に基づいて秘密情報Ｐ（０）を算出し、上記ｋ個の分散ＩＤのうちいずれかの分散ＩＤが有する検証用情報Ｖの素数ｐと要素ｇと上記秘密情報Ｐ（０）とに基づいて$g^{P(0)}$（ｍｏｄ　ｐ）の式より余りを算出し、算出した余りと当該検証用情報Ｖが有する$C_0$とが等しい場合、上記秘密情報Ｐ（０）を秘密情報Ｓとして出力する秘密情報復元部と
を備え、
上記情報蓄積部は、上記データベースに記憶された情報リストから上記秘密情報復元部により出力された秘密情報Ｓを検索し、検索した秘密情報Ｓに対応する物品情報を取得して出力する
ことを特徴とする請求項１記載の情報記録読取システム。
【発明の詳細な説明】
【技術分野】
【０００１】
この発明は、物品とＲＦＩＤとの関連付けを行い、物品の偽造や破壊などの不正行為を防ぎ、物品情報の喪失、改竄を防ぐ、安全技術に関するものである。
【背景技術】
【０００２】
ＩＥＥＥ ｍｉｃｒｏ，　ｖｏｌ．２１，　ｎｏ６，　ｐｐ．４３－４９　２００１“Ａｎ　Ｕｌｔｒａ　Ｓｍａｌｌ　Ｉｎｄｉｖｉｄｕａｌ　Ｒｅｃｏｇｎｉｔｉｏｎ　Ｓｅｃｕｒｉｔｙ　Ｃｈｉｐ”には、（株）日立製作所ミューソリューションズカンパニーの販売しているμチップに関する技術が記載されている。このチップは、ＲＦＩＤ（ｒａｄｉｏ　ｆｒｅｑｕｅｎｃｙ　ｉｄｅｎｔｉｆｉｃａｔｉｏｎ）と呼ばれる無線を用いた自動識別技術を用いており、小型化を実現するために、読み出し専用の記録部であるＲＯＭと通信用のアンテナ回路からのみ構成されている。そして、物品に取り付けられたＲＦＩＤチップ内のＩＤを、無線によりＲＦＩＤリーダが読み取り、そのＩＤをデータベースに問い合わせることで、物品に関連する物品情報が得られるようにしたＲＦＩＤシステムが構築されている。
【０００３】
図１３は従来技術におけるＲＦＩＤシステムを示す図である。図において、システムは、チップを製造するチップ製造部１０１と、チップを物品に取り付ける物品製造部１０２と、ＩＤと物品情報を保管する情報蓄積部１０３と、物品に取り付けられたＩＤを読み取

り、情報蓄積部１０３から物品情報を取り出す読取部１０４からなる。
【０００４】
上記チップ製造部１０１は、詳しくはＩＤ生成手段１０６にてＩＤを生成し、ＩＤ設定手段１１０にてＲＦＩＤチップの記録部にＩＤを設定し、ＲＦＩＤチップを物品製造部１０２へ送る。物品製造部１０２では、詳しくはＲＦＩＤチップを物品に取り付け、または埋め込み、物品情報設定手段１１４にて物品に関する物品情報を生成し、データベース登録手段１１５にて、チップ製造部１０１から受け取ったＩＤと、物品情報を、情報蓄積部１０３へ登録の為に送る。
【０００５】
情報蓄積部１０３は、物品製造部１０２より受け取ったＩＤと物品情報を情報リスト１１６としてデータベース１１７に登録し保管する。
読取部１０４は、詳しくは読取手段１１９にて物品のＲＦＩＤチップ１０７のアンテナ回路１０９からの電波により、ＲＦＩＤチップの記録部１０８に設定されているＩＤを読み取り、そのＩＤを物品情報の検索の為に情報蓄積部１０３へと送る。
情報蓄積部１０３は、詳しくは読取部１０４から受け取ったＩＤに対応する物品情報をデータベース１１７に蓄積されている情報リスト１１６から取り出し、読取部１０４へ検索結果として送る。
読取部１０４は、データベース検索手段１２０により情報蓄積部１０３から物品情報を受け取る。こうして、物品に関連付けられている物品情報を入手することが可能となっている。
【０００６】
また、特許文献１において、少なくとも２つのＩＣチップにデータを記録し、これらのＩＣを１つのアンテナに接続して、どちらかのＩＣが故障をしても、他方のデータをバックアップする構成は知られている。しかしこの場合も、データの記録内容には言及がなく、単にチップの故障のバックアップ方法が記載されているのみである。
【特許文献１】特開２００２－８３２７７号公報
【発明の開示】
【発明が解決しようとする課題】
【０００７】
従来のＲＦＩＤシステムは、上記のように構成され動作するので、物品に取り付けられているＲＦＩＤチップのＩＤ情報が読取部のＲＦＩＤリーダにより容易に読み取り可能であり、この読み取ったＩＤをもとにＲＦＩＤチップを複製し別の物品に取り付けることが容易であるという課題がある。更に、他の情報付ＩＤにするかえられることもあり得る。
また逆に、物品に取り付けられているＲＦＩＤチップが１つである為、これの故障や、これの破壊または取り外しにより、物品情報が入手不能となるという課題もある。
【０００８】
単に複数の同一ＩＤのＲＦＩＤチップを取り付けても、ＲＦＩＤチップの破壊や取り外しに関しては有効であるが、他の物品に複製したＲＦＩＤチップを取り付けて、すり替えることに対しては無力である。
また、ＩＤを単純に複数のＩＤに分割しても、全ての分割したチップから情報を得なければ、元のＩＤ情報が得られないという課題もある。
【０００９】
この発明は、上述のような課題を解決するためになされたもので、物品につけられたＲＦＩＤチップの故障や破壊や取り外しによりＩＤ情報の喪失を防ぎ、ＲＦＩＤチップの偽造による物品の成りすましや物品情報のすり替えを困難にして、ＲＦＩＤ情報の安全性を高めることを目的とする。
【課題を解決するための手段】
【００１０】
この発明に係る分散識別情報記録装置は、チップに識別情報を埋め込んで、識別情報チップを生成する識別情報記録装置において、

上記識別情報から、一部のチップが消失しても残存チップで復元可能な数以上の、所定の論理で分散情報と検証用情報とを組にした、それぞれが異なる分散識別情報を複数組、生成する秘密情報分散部と、上記各組毎にチップに上記分散識別情報を埋め込む識別情報設定部とを備えた。

またこの発明に係る分散識別情報記憶チップは、識別情報記録装置により識別情報を埋め込まれる識別情報記憶チップにおいて、

上記チップは複数組で所定の識別情報を記憶するようにし、かつ各チップは所定の論理で生成された分散情報と検証用情報とを組にして各チップに埋め込み、それぞれが異なる分散識別情報を記録部に持つ、複数組のチップで構成される。

またこの発明に係る分散識別情報読取り装置は、チップに埋め込まれた識別情報を読取る識別情報読取り装置において、

上記チップは複数のチップとして、この複数のチップが持つ分散識別情報を読取る読取部と、上記読取った複数の異なる分散情報と検証用情報を抽出し、この抽出した複数の、分散情報と検証用情報との組を基に元の識別情報を生成する秘密情報復元部とを備えた。

【発明の効果】

【００１１】

以上のように一部のチップのみでも得られる複数の秘密化分散情報をそれぞれ別々のチップに記録し、読取るようにしたので、不正な複製や不正使用を防ぐ効果がある。

また一部のチップが故障し、または取外されても、残存分散情報に基づいて安全に元の識別情報が得られる効果がある。

【発明を実施するための最良の形態】

【００１２】

実施の形態１.

本実施の形態においては、ＩＤ情報を、そのいくつかが失われても残りの分散情報から復元可能な複数の秘密情報に分散して、この複数の分散ＩＤ情報から元のＩＤ情報を得る安全化情報システムを説明する。

図１は、本発明の実施の形態１をにおけるＲＦＩＤ偽造防止システムの構成を示す図である。

図において、システムは、チップ製造部１と、物品製造部２と、情報蓄積部３と、ＩＤ読取部４からなる。更に詳しく各部の構成を説明する。

チップ製造部１は、固有情報のＩＤ５を生成するＩＤ生成部６と、ＩＤ５を分散ＩＤ２２に秘密情報として分散する秘密情報分散部２１と、この分散ＩＤ２２を記録する記録部８と、この記録部８の分散ＩＤ２２を無線にて送信するアンテナ回路９を備えた分散ＲＦＩＤチップ７と、分散ＩＤ２２を分散ＲＦＩＤチップ７の記録部８に記録するＩＤ設定部１０とを備えている。

物品製造部２は、物品１２に分散ＲＦＩＤチップ７を取り付ける取付部１１と、物品１２に関連する属性などの情報である物品情報１３を設定する物品情報設定部１４と、チップ製造部１より受け取ったＩＤ５と物品情報１３を情報蓄積部３へ登録するデータベース登録部１５とを備えている。

【００１３】

情報蓄積部３は、物品製造部２より受け取ったＩＤ５と物品情報１３を情報リスト１６として蓄積し、ＩＤ５による検索依頼に対して情報リスト１６の対応する物品情報１３を検索結果として返すデータベース１７とを備えている。

ＩＤ読取部４は、無線にて物品１２の分散ＲＦＩＤチップ７のアンテナ回路９から送信された記録部８の分散ＩＤ２２を受信する読取部１９と、読取部１９にて受信した分散ＩＤ２２からＩＤ５を復元する秘密情報復元部２３と、ＩＤ５による検索の依頼を情報蓄積部３に送り、情報蓄積部３から検索結果として物品情報１３を受け取るデータベース検索部２０とを備えている。

【００１４】

このように構成されたＲＦＩＤシステムにおいて、物品に対応するＩＤを物品１２に付

加し、またその情報を後の照合のためにデータベースに蓄積するまでの動作を説明する。
まず、チップ製造部１は、ＩＤ生成部６にてＩＤ５を生成する。そして、秘密情報分散部２１にてＩＤ５を分散ＩＤ２２として秘密情報分散する。

【００１５】

ここで秘密情報分散部２１は、図２の秘密情報分散部の詳細構成に基づいて情報分散の内部処理を実行する。即ち、まず、ＩＤ５と秘密情報を分散する個数：ｎ２６と秘密情報の復元に必要な最小個数：ｋ２７を得て、分散情報：$B_1$ ～$B_n$ ２８と、乱数$a_1$ ～$a_{(k-1)}$ ３０と素数ｒ２９を出力する。
検証用情報生成部２５は、ＩＤ５と乱数$a_1$ ～$a_{(k-1)}$ ３０と素数ｒ２９を得て、検証用情報Ｖ３１を出力する。そして、秘密情報分散部２１としては、各分散情報：$B_1$ ～$B_n$ ２８と検証用情報Ｖ３１をあわせて分散$ID_1$ ～$ID_n$ ２２として出力する。

【００１６】

ここで情報分散部２４は、図３に示す内部処理手順により処理を実行する。
まず、情報分散部の内部処理手順その１．４４にて処理を開始し、内部処理手順その２．４５にて秘密情報としてのＩＤ：Ｓ５を取得し、内部処理手順その３．４６にて秘密情報を分散する個数：ｎ２６を取得し、内部処理手順その４．４７にて秘密情報の復元に必要な最小個数：ｋを取得し、内部処理手順その５．４８にてｋ－１個の乱数$a_1$～$a_{k-1}$ ３０を生成し、手順その６．４９にて素数ｒ２９を生成し、手順その７．５０にて次式（１）を設定する。

$$f(x)=S+a_1\cdot x+a_2\cdot \underline{x}^2+\cdots+a_{k-1}\cdot \underline{x}^{k-1}\ (\mathrm{mod}\ \underline{r}) \quad (1)$$

手順その８．５１にてｊ＝１，…，ｎとして$w_j=f(j)$を算出し、手順その９．５２にて分散情報：$B_j=(j, w_j)$ ２８を出力し、手順その１０．５３にて素数ｒ２９を出力し、手順その１１．５４にて乱数$a_1$ ～$a_{k-1}$ ３０を出力し、手順その１２．５５にて処理を終了する。

【００１７】

ここで検証用情報生成部２５は、図４に示す内部処理手順により処理を実行する。
検証用情報生成部の内部処理手順その１．５６にて処理を開始し、内部処理手順その２．５７にて秘密情報としてのＩＤ：Ｓ５を取得し、内部処理手順その３．５８にて秘密情報の復元に必要な最小個数：ｋ２７を取得し、手順その４．５９にて素数ｒ２９を取得し、手順その５．６０にて乱数$a_1$ ～$a_{k-1}$ ３０を取得し、手順その６．６１にてｒ｜ｐ－１を満たす素数ｐ３３を生成し、手順その７．６２にて乗法群$Z^*_p$での位数がｒとなる要素ｇ３４を定め、手順その８．６３にて$f(j)=g^{aj}\ (\mathrm{mod}\ p)$とし、検証用情報生成部の内部処理手順その９．６４にて値Ｃを$C_0=g^s\ (\mathrm{mod}\ p)$およびｊ＝１，…，ｋ－１として、$C_j=f(j)$を算出する。更に、手順その１０．６５にて検証用情報：Ｖ＝（ｐ，ｇ，$C_0$，$C_1$，…，$C_{k-1}$）３１を出力し、手順その１１．６６にて処理を終了する。

【００１８】

次に、ＩＤ設定部１０は、分散ＩＤ２２を分散ＲＦＩＤチップ７の記録部８に記録して、ＩＤ５の情報と分散ＲＦＩＤチップ７を物品製造部２に渡す。

【００１９】

物品製造部２は、物品１２に分散ＲＦＩＤチップ７を取付部１１により取り付け、物品情報設定部１４により物品１２に関連する属性などの情報である物品情報１３を設定し、この物品情報１３を情報蓄積部３へデータベース登録部１５により登録する。データベース登録部１５は、ＩＤ５の情報も登録する。
情報蓄積部３は、受け取ったＩＤ５と物品情報１３を情報リスト１６としてデータベース１７に蓄積する。

【００２０】

次に、物品情報に対応する物品１２に取り付けられた複数の分散ＲＦＩＤチップ７から情報を取り出して確認をする動作を説明する。
まず、ＩＤ読取部４は、無線にて物品１２の分散ＲＦＩＤチップ７のアンテナ回路９か

ら送信された記録部８にある分散ＩＤ２２を読取部１９により受信し、この受信した分散ＩＤ２２からＩＤ５を秘密情報復元部２３で復元する。

【００２１】

ここで秘密情報復元部２３は、図５の秘密情報復元部の詳細構成に基づいて情報復元の内部処理手順を実行する。

まず、分散ＩＤ２２を取得して、分散情報検証部３５に入力する。分散情報検証部３５は、検証に成功した場合に秘密情報の復元に必要な最小個数：ｋ２７以上で秘密情報を分散する個数：ｎ２６以下のｍ個の検証済みの分散ＩＤ$_1$ ～ＩＤ$_m$ ３２を情報復元部３６に入力し、情報復元部３６はＩＤ５を出力する。

【００２２】

ここで、分散情報検証部３５は、図６に示す内部処理手順により処理を実行する。即ち、まず、内部処理手順その１．６７にて処理を開始し、内部処理手順その２．６８にて分散ＩＤ２２を取得し、手順その３．６９にて分散ＩＤ２２から分散情報：Ｂ２８と検証用情報：Ｖ３１を取り出し、手順その４．７０にて検証用情報：Ｖ３１から（ｐ，ｇ，$C_0$，$C_1$，…，$C_{k-1}$）を取り出し、手順その５．７１にて分散情報：$B_j$ ２８から（ｊ，$w_j$）を取り出し、手順その６．７２にて$g^{wj} \equiv C_0 \cdot C_1^{j} \cdot C_2^{j2} \cdot \cdots \cdot C_{k-1}^{jk-1}$（ｍｏｄ　ｐ）が成り立つかどうかを判断し、成り立つ場合は、手順その７．７３にて検証成功とし、手順その９．７５にて分散ＩＤ２２を出力し、処理を終了する。成り立たない場合は、手順その８．７４にて検証失敗とし、手順その１０．７６にて処理を終了する。

【００２３】

また、情報復元部３６は、図７に示す内部処理手順により処理を実行する。即ち、まず、情報復元部の内部処理手順その１．７７にて処理を開始し、内部処理手順その２．７８にてｍ個の分散ＩＤ２２を取得し、内部処理手順その３．７９にて分散ＩＤ２２から分散情報：Ｂ２８と検証用情報：Ｖ３１を取り出し、手順その４．８０にて、ｍ個の分散ＩＤ２２のなかに検証用情報：Ｖ３１の等しいｋ個の分散ＩＤ２２が存在するかを判断する。存在する場合は、手順その５．８１にて正当な分散ＩＤ２２とし、存在しない場合は、手順その６．８２にて不正な分散ＩＤとして処理を終了する。また、正当な分散とした場合は、手順その７．８３にてｋ個の分散ＩＤ２２を取得し、手順その８．８４にて分散情報：$B_j$ ２８から（ｊ，$w_j$）を取り出し、手順その９．８５にてラグランジュの補間多項式を利用し、次式（２）を用いて式（３）を得る。

【００２４】

【数１】

$$L_j(0) = \prod_{\substack{m=1 \\ j \neq m}}^{k} \frac{0 - x_m}{x_j - x_m}$$

$$= \frac{0 - x_1}{x_j - x_1} \bullet \frac{0 - x_2}{x_j - x_2} \cdots \frac{0 - x_{j+1}}{x_j - x_{j-1}} \bullet \frac{0 - x_{j+1}}{x_j - x_{j+1}} \cdots \frac{0 - x_k}{x_j - x_k} \qquad (2)$$

$$p(0) = \sum_{j=1}^{k} w_j \bullet L_j(0) \qquad (3)$$

【００２５】

手順その１０．８６にて検証用情報生成部の内部処理手順その７．６３のｆ（ｘ）において、Ｐ（０）＝ｆ（０）＝Ｓとし、手順その１１．８７にて検証用情報：Ｖ３１から（ｐ，ｇ，$C_0$，$C_1$，…，$C_{k-1}$）を取り出し、手順その１２．８８にて$C_0 = g^s \pmod p$が成り立つかどうかを判定する。判定が成り立つ場合は、手順その１３．８９にて正当な秘密情報としてのＩＤ：Ｓ５とし、手順その１５．９１にて秘密情報としてのＩＤ：Ｓ５を出力し、手順その１６．９２にて処理を終了する。また、手順８８で成り立たない場合は、手順その１４．９０にて不正な秘密情報としてのＩＤ：Ｓとし処理を終える。

こうして、ＩＤ読取部４は、ＩＤ５による検索依頼を情報蓄積部３にデータベース検索部２０を通じて送信する。

【００２６】

情報蓄積部３は、読取部からのＩＤ５による検索依頼に対して情報リスト１６の対応する物品情報１３をデータベース１７から検索し、検索結果として物品情報１３をＩＤ読取部４に返す。

ＩＤ読取部４は、情報蓄積部３から送られてきた物品情報１３をデータベース検索部２０経由で受け取る。

【００２７】

なお、チップ製造部１と物品製造部２と情報蓄積部３とＩＤ読取部４の間の情報の交換時は、必要に応じて秘匿通信技術により保護される。

また、情報伝送の分野において、誤り訂正の技術が知られていて、これは、分割したセルに冗長情報を付加し、伝送中に一部のセルに消失又は誤りが発生しても、残存セルから正しい情報を復元する技術である。しかし、この方法では、安全性に不安があり、一部のセルから少なくとも一部の情報が入手できる。更に、セル内部の誤りは訂正できても、偽りのセルは検出できない。これに対して本実施の形態による分割では、一部のＩＤチップのみからでは一部の情報も復元できず、また、偽りのＩＤチップも排除できて安全性が極めて高い。

【００２８】

以上説明したように、物品１２に取り付けられた分散ＲＦＩＤチップ７からＩＤ５を復元し、対応する物品情報１３を入手することができる。そして、ＩＤを複数の分散ＲＦＩＤチップとしたことにより、複製や別の物品への取り付けによる不正が困難になる。ＩＤをｎ個のＲＦＩＤチップに分散し、そのうちｋ個が集まればＩＤ５を復元できるので、一部のＲＦＩＤチップの故障や破壊や取り外しに対しても安全に情報を得ることができる。

なお、ＩＤチップは、ＲＦＩＤに限らず、対応した読取手段により読み取り可能なＩＤであれば、どのようなＩＤチップであってもよい。

【００２９】

実施の形態２．

本実施の形態においては、情報復元部を共通化してシステム規模を小さくした構成を説明する。

図８は、実施の形態２におけるＲＦＩＤ偽造防止システムの構成を示す図である。

図において、実施の形態１の図１の構成と異なる部分は、ＩＤ読取部４ｂを分散ＩＤを読み取るまでの構成とし、独立した情報復元部３６ｂを設けたことである。

ＩＤ読取部４ｂは、分散ＲＦＩＤチップ７から送信された分散ＩＤ２２を受信する読取部１９と、この受信した分散ＩＤ２２を情報復元部３６ｂに送信する分散ＩＤ送信部３８と、復元されたＩＤ５を受信するＩＤ受信部４０と、ＩＤ５による検索依頼と、情報蓄積部３からの検索結果として物品情報１３を受け取るデータベース検索部２０とを備えている。

また、情報復元部３６ｂは、ＩＤ読取部４ｂより分散ＩＤ２２を受信する分散ＩＤ受信部３９と、分散ＩＤ受信部３９で受信した分散ＩＤ２２からＩＤ５を復元する秘密情報復元部２３と、復元されたＩＤ５をＩＤ読取部４ｂへ送信するＩＤ送信部４１とを備えている。

【００３０】
このＲＦＩＤシステムの動作は以下の通りであるが、分散ＩＤを生成し、また、データベースに蓄積するまでの動作は実施の形態１と同様であるので、記述を省略する。
【００３１】
読み取りと復元動作を説明する。
まず、ＩＤ読取部４ｂは、物品１２のＲＦＩＤチップ７のアンテナ回路９から送信された記録部８にある分散ＩＤ２２を読取部１９により受信し、これを分散ＩＤ送信部３８により情報復元部３６ｂに送信する。
【００３２】
これを分散ＩＤ受信部３９で受けた情報復元部３６ｂは、秘密情報復元部２３で復元してＩＤ５を得る。この際の秘密情報復元の手順は、実施の形態１の図５ないし図７の手順と同じである。
【００３３】
次に、情報復元部３６ｂは、復元されたＩＤ５をＩＤ読取部４ｂへ送信する。これを受けたＩＤ読取部４ｂは、受信したＩＤ５により検索依頼を情報蓄積部３に送信する。以降の動作は、実施の形態１と同じである。
【００３４】
このようにして、秘密情報復元部を独立した情報復元部とした構成により、複数の読取部が情報復元部を共有することとなり、システム規模を縮小できる。
【００３５】
本実施の形態の変化構成をいくつか説明する。
図９は、本実施の形態における他のＲＦＩＤ偽造防止システムの構成を示す図である。
図において、図８の構成と異なる部分は、情報復元部３６ｃにデータベース検索部２０を移し、ＩＤ読取部４ｃからデータベース検索部を除いたことである。従って、ＩＤ読取部４ｃは、分散ＩＤ２２を受信する読取部１９と、分散ＩＤ送信部３８と、物品情報受信部４２とから構成される。
また、情報復元部３６ｃは、分散ＩＤ受信部３９と、秘密情報復元部２３と、データベース検索部２０と、物品情報送信部４３とから構成される。
【００３６】
図９の構成によるシステムの動作は、データベース検索部２０の場所が少し移っただけであり、図８のそれと同様であるので、記述を省略する。
【００３７】
このように、情報復元部にデータベース検索部を配置することにより、復元されたＩＤが情報復元部の外に漏れないので、他の部分におけるＩＤの不正入手を防止する効果がある。
【００３８】
図１０は、本実施の形態における他のＲＦＩＤ偽造防止システムの構成を示す図である。
図において、図９の構成と異なる部分は、図９では、独立して設けられていた情報復元部３７ｃを、情報蓄積部３ｄの内部に設けたことである。
【００３９】
この構成の動作は、既に述べた動作説明から明らかなので、ここでの記述は省略する。
この構成によれば、復元されたＩＤがＩＤを保管している情報蓄積部の外部に漏れないので、情報復元部を独立に設けた場合より更にＩＤの不正入手を困難にする効果がある。
【００４０】
実施の形態３．
本発明における複製や不正使用を防止しＩＤチップ破損にも安全であって、更に、情報の秘密性を高めたシステムを説明する。
本実施の形態におけるＲＦＩＤ偽造防止システムは、図１のそれとほぼ同じであるが、チップ製造部１ｅおよびＩＤ読取部４ｅが図１１にその詳細を示す構成となっている。即

ち、チップ製造部１ｅが、ＩＤ生成部６と、ＩＤ５とチップ製造部の署名鍵９３により署名データ９６を、一旦生成する署名部９５と、更に、この一旦生成された署名データ９６とＩＤ５とチップ製造部の電子証明書９４をあわせた署名付ＩＤ７６も署名部９５で生成し、この署名付ＩＤ９７を分散ＩＤ２２に秘密情報分散する秘密情報分散部２１と、この分散ＩＤ２２を分散ＲＦＩＤチップ７の記録部８に記録するＩＤ設定部１０とを備えている。

【００４１】

ＩＤ読取部４ｅとしては、読取部１９と、受信した分散ＩＤ２２から署名付ＩＤ９７を復元する秘密情報復元部２３と、署名付ＩＤ９７からＩＤ５と署名データ９６とチップ製造部の電子証明書９４を取り出し、これらを用いて署名検証結果９９を出力する署名検証部９８と、署名付ＩＤ９７から取り出されたＩＤ５による検索の依頼を情報蓄積部３に送り、検索結果として物品情報１３を受け取るデータベース検索部２０とを備えている。

【００４２】

このように構成されたＲＦＩＤシステムにおいて、秘密情報を分散し、ＩＤチップに記録する動作を説明する。

まず、チップ製造部１ｅは、ＩＤ生成部６にてＩＤ５を生成し、このＩＤ５とチップ製造部の署名鍵９３を用いて署名部９５でディジタル署名としての署名データ９６を一旦生成し、更に、ＩＤ５と署名データ９６とディジタル証明技術における署名の検証に用いるチップ製造部の電子証明書９４をあわせた署名付ＩＤ９７とし、秘密情報分散部２１にて署名付ＩＤ９７をＩＤ５に置き換えて分散ＩＤ２２に秘密情報分散する。

【００４３】

秘密情報分散部２１が行う内部処理手順は、データとしてＩＤ５に換えて署名付ＩＤを用いること以外は、実施の形態１と同じであり、以下の詳細記述は省略する。

【００４４】

ＩＤ読取部４ｅの動作も、秘密情報の復元までは実施の形態１と同様である。ただ、復元された情報は、署名付ＩＤ９７である。即ち、図５の情報復元部３６が出力するのは、署名付ＩＤ９７である。

【００４５】

同様に、分散情報検証部３５は、図６の内部処理手順により処理を実行し、情報復元部３６は、図７の内部処理手順により処理を実行する。

【００４６】

なお、ここでは署名付ＩＤ９７をＩＤ５に置き換えてあるので、上記したように、秘密情報復元部２３からは署名付ＩＤ９７が出力される。

【００４７】

次に、ＩＤ読取部４ｅは、署名付ＩＤ９７からＩＤ５と署名データ９６とチップ製造部の電子証明書９４を取り出し、これらにより署名検証部９８が署名検証結果９９を出力する。また、ＩＤ５による検索依頼を情報蓄積部３へデータベース検索部２０により送る。以降の動作は、実施の形態１と同様である。

【００４８】

なお、ディジタル証明技術としては、既存のＲＳＡ公開鍵暗号方式または楕円暗号方式等が利用できる。また、上記では、実施の形態１のチップ製造部と読取部を変更する構成を説明したが、実施の形態２における各システムの構成と組み合わせるようにしてもよい。つまり、各チップ製造部と読取部を変更する。

【００４９】

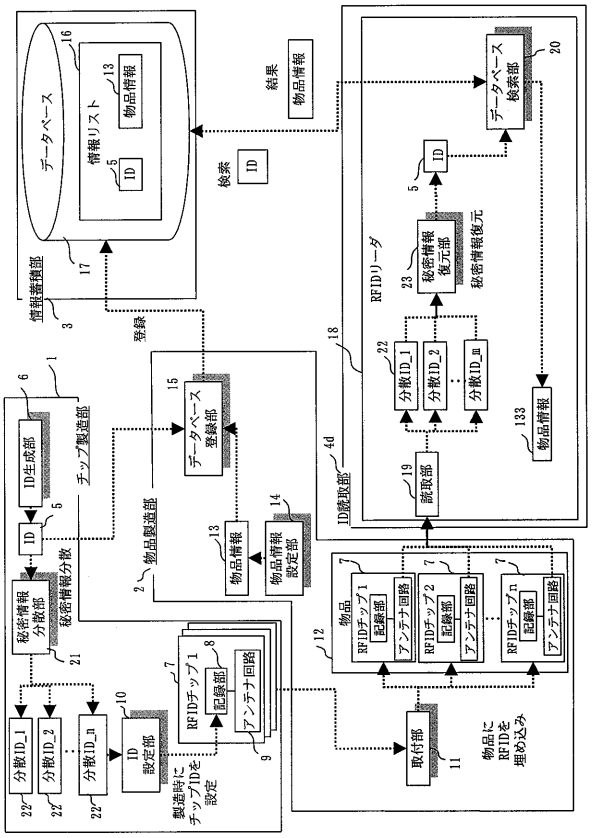
以上説明したように、先の各実施の形態と組み合わせて用いることにより、各実施の形態の効果に加えて、ＩＤに対してチップ製造部の署名を施し、復元後のＩＤに対して署名の検証を行うことで、ＩＤの偽造を防止することが可能である。

なお、上記では、署名付ＩＤとして、署名データと、その電子署名書を組み合わせたものとしているが、署名鍵のみによる署名データのみとしてもよい。その場合には、署名データの信憑性は損なわれるが、それでも偽造防止の度合いを高める不正防止効果がある。

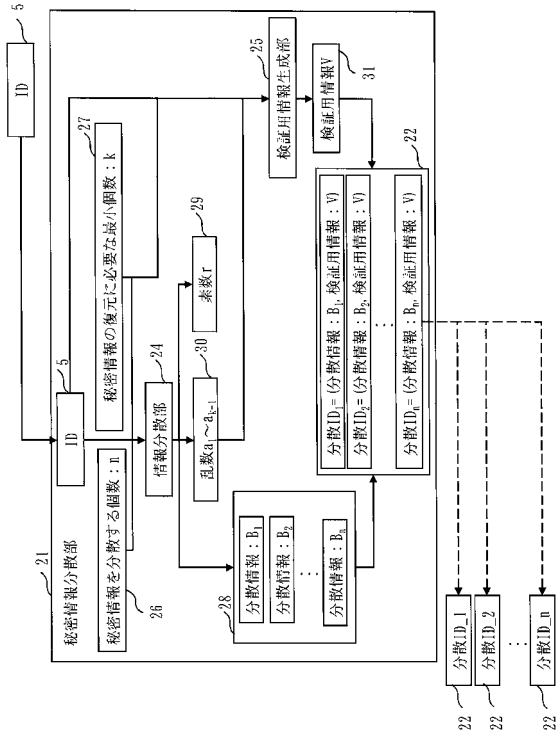
【００５０】
実施の形態４.
複製や不正使用を更に困難にしたＩＤチップの生成と、その使用システムの説明をする。
図１２は、本実施の形態における分散ＲＦＩＤチップ７ｆの構成およびＩＤ読取部４ｆの読取部１９ｆの詳細構成を示す図である。この構成を実施の形態１ないし実施の形態３における他の要素と組み合わせてシステムを構成する。
図において、分散ＲＦＩＤチップ７ｆは、分散ＩＤ２２を記録する記録部８と、記録部８の分散ＩＤ２２を特定周波数帯の１つの周波数を利用した無線にて送信する特定周波数アンテナ回路９ｆとで構成される。
対応してＩＤ読取部４ｆの読取部１９ｆは、分散ＲＦＩＤチップ７ｆの特定周波数アンテナ回路９ｆから送信された分散ＩＤ２２を受信する可変周波数アンテナ回路１９１と、乱数発生部１９３と、この得られた乱数により可変周波数アンテナ回路１９１の周波数を変更する周波数切替部１９２からなる。
【００５１】
このように構成されたＲＦＩＤシステムの動作を簡単に説明すると、以下の通りとなる。
各分散ＲＦＩＤチップ７ｆは、記録部８の分散ＩＤ２２を特定周波数帯のそれぞれ異なる１つの周波数を利用した無線にて特定周波数アンテナ回路９ｆにより送信する。
これを受けて、読取部１９ｆは、乱数発生部１９３からの乱数により特定周波数帯の１つの周波数を選び、周波数切替部１９２により可変周波数アンテナ回路１９１の周波数を変更し、分散ＲＦＩＤチップ７ｆの特定周波数アンテナ回路９ｆから送信された分散ＩＤ２２を可変周波数アンテナ回路１９１にて受信する。従って、どの周波数に対応したＲＦＩＤチップの分散ＩＤが読取部により受信されるのかが事前に明らかにされず、一部のＲＦＩＤチップを複製して成りすますことを防止できる。もちろん、必ずしも全てのチップに異なる周波数を割り当てる必要はなく、複数の周波数と、同一周波数を割り当てられたチップにおいては、発信タイムラグを異なるよう設定するようにしてもよい。
【図面の簡単な説明】
【００５２】
【図１】本発明の実施の形態１におけるＲＦＩＤ偽造防止システムの構成を示す図である。
【図２】実施の形態１における秘密情報分散部の詳細構成とその信号を示す図である。
【図３】図２に示す情報分散部が行う内部処理手順を示すフロー図である。
【図４】図２に示す検証用情報生成部が行う内部処理手順を示すフロー図である。
【図５】実施の形態１における秘密情報復元部の詳細構成とその信号を示す図である。
【図６】図５に示す分散情報検証部が行う内部処理手順を示すフロー図である。
【図７】図５に示す情報復元部が行う内部処理手順を示すフロー図である。
【図８】本発明の実施の形態２におけるＲＦＩＤ偽造防止システムの構成を示す図である。
【図９】実施の形態２における他のＲＦＩＤ偽造防止システムの構成を示す図である。
【図１０】実施の形態２における他のＲＦＩＤ偽造防止システムの構成を示す図である。
【図１１】本発明の実施の形態３におけるＲＦＩＤ偽造防止システムの構成を示す図である。
【図１２】本発明の実施の形態４におけるＲＦＩＤ偽造防止システムの構成を示す図である。
【図１３】従来のＲＦＩＤシステムの構成を示す図である。
【符号の説明】
【００５３】
１　チップ製造部、２　物品製造部、３　情報蓄積部、４，４ｂ，４ｃ，４ｅ，４ｆ　ＩＤ読取部、５　ＩＤ、６　ＩＤ生成部、７，７ｆ　ＲＦＩＤチップ、８　記録部、９

アンテナ回路、９ｆ　特定周波数アンテナ回路、１０　ＩＤ設定部、１１　取付部、１２　物品、１３　物品情報、１４　物品情報設定部、１５　データベース登録部、１６　情報リスト、１７　データベース、１８　ＲＦＩＤリーダ、１９，１９ｆ　読取部、２０　データベース検索部、２１　秘密情報分散部、２２　分散ＩＤ、２３　秘密情報復元部、２４　情報分散部、２５　検証用情報生成部、２６　秘密情報を分散する個数：ｎ、２７　秘密情報の復元に必要な最小個数：ｋ、２８　分散情報：$B_1$～$B_n$、２９　素数ｒ、３０　乱数ａ，$a_1$～$a_{k-1}$、３１　検証用情報Ｖ、３５　分散情報検証部、３６，３６ｂ，３６ｃ　情報復元部、３８　分散ＩＤ送信部、３９　分散ＩＤ受信部、４０　ＩＤ受信部、４１　ＩＤ送信部、４２　物品情報受信部、４３　物品情報送信部、４４　情報分散部の内部処理手順その１．、４５　情報分散部の内部処理手順その２．、４６　情報分散部の内部処理手順その３．、４７　情報分散部の内部処理手順その４．、４８　情報分散部の内部処理手順その５．、４９　情報分散部の内部処理手順その６．、５０　情報分散部の内部処理手順その７．、５１　情報分散部の内部処理手順その８．、５２　情報分散部の内部処理手順その９．、５３　情報分散部の内部処理手順その１０．、５４　情報分散部の内部処理手順その１１．、５５　情報分散部の内部処理手順その１２．、５６　検証用情報生成部の内部処理手順その１．、５７　検証用情報生成部の内部処理手順その２．、５８　検証用情報生成部の内部処理手順その３．、５９　検証用情報生成部の内部処理手順その４．、６０　検証用情報生成部の内部処理手順その５．、６１　検証用情報生成部の内部処理手順その６．、６２　検証用情報生成部の内部処理手順その７．、６３　検証用情報生成部の内部処理手順その８．、６４　検証用情報生成部の内部処理手順その９．、６５　検証用情報生成部の内部処理手順その１０．、６６　検証用情報生成部の内部処理手順その１１．、６７　分散情報検証部の内部処理手順その１．６８　分散情報検証部の内部処理手順その２．、６９　分散情報検証部の内部処理手順その３．、７０　分散情報検証部の内部処理手順その４．、７１　分散情報検証部の内部処理手順その５．、７２　分散情報検証部の内部処理手順その６．、７３　分散情報検証部の内部処理手順その７．、７４　分散情報検証部の内部処理手順その８．、７５　分散情報検証部の内部処理手順その９．、７６　分散情報検証部の内部処理手順その１０．、７７　情報復元部の内部処理手順その１．、７８　情報復元部の内部処理手順その２．、７９　情報復元部の内部処理手順その３．、８０　情報復元部の内部処理手順その４．、８１　情報復元部の内部処理手順その５．、８２　情報復元部の内部処理手順その６．、８３　情報復元部の内部処理手順その７．、８４　情報復元部の内部処理手順その８．、８５　情報復元部の内部処理手順その９．、８６　情報復元部の内部処理手順その１０．、８７　情報復元部の内部処理手順その１１．、８８　情報復元部の内部処理手順その１２．、８９　情報復元部の内部処理手順その１３．、９０　情報復元部の内部処理手順その１４．、９１　情報復元部の内部処理手順その１５．、９２　情報復元部の内部処理手順その１６．９３　署名鍵、９４　電子証明書、９５　署名部、９６　署名データ、９７　署名付ＩＤ、９８　署名検証部、９９　署名検証結果、１９１　可変周波数アンテナ回路、１９２　周波数切替部、１９３　乱数発生部。

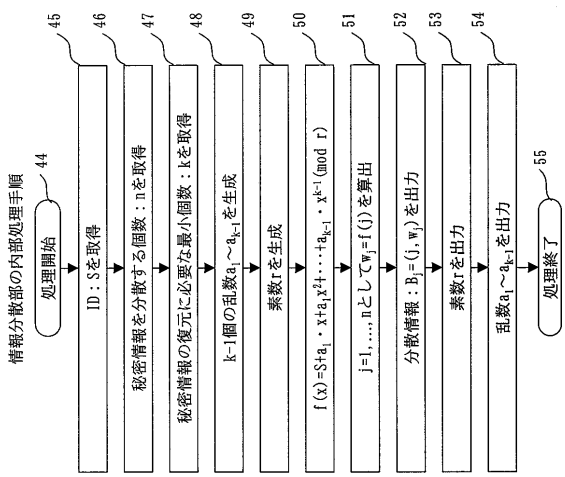
【図１】


データベース
情報リスト
物品情報
ID
検索
結果
情報蓄積部
登録
秘密情報分散部
秘密情報分散
ID生成部
チップ製造部
物品製造部
データベース登録部
物品情報
物品情報設定部
ID設定部
製造時にチップIDを設定
RFIDチップ1
記憶部
アンテナ回路
物品
RFIDチップn
取付部
物品にRFIDを埋め込み
RFIDリーダ
ID読取部
秘密情報復元部
秘密情報復元
データベース検索部
分散ID_1
分散ID_2
分散ID_n
分散ID_m

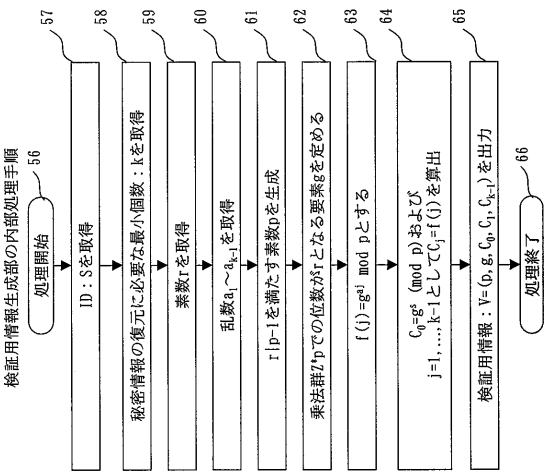
【図２】


ID
秘密情報分散部
秘密情報を分散する個数：n
秘密情報の復元に必要な最小個数：k
情報分散部
乱数a₁～a_{k-1}
素数r
分散情報：B₁
分散情報：B₂
分散情報：Bn
検証用情報生成部
検証用情報V
分散ID₁=(分散情報：B₁,検証用情報：V)
分散ID₂=(分散情報：B₂,検証用情報：V)
分散IDn=(分散情報：Bn,検証用情報：V)
分散ID_1
分散ID_2
分散ID_n

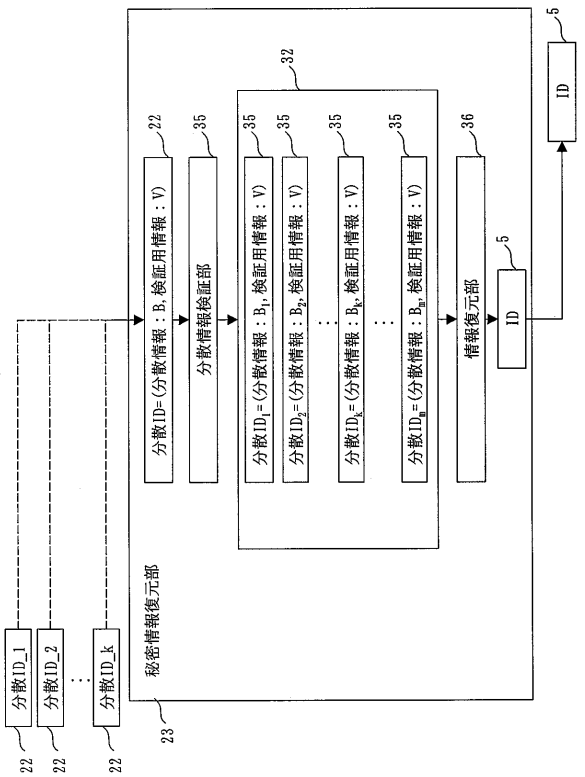
【図３】


情報分散部の内部処理手順
処理開始
ID：Sを取得
秘密情報を分散する個数：nを取得
秘密情報の復元に必要な最小個数：kを取得
k-1個の乱数a₁～a_{k-1}を生成
素数rを生成
f(x)=S+a₁・x+a₂x²+…+a_{k-1}・x^{k-1}(mod r)
j=1,…,nとしてwj=f(j)を算出
分散情報：Bj=(j,wj)を出力
素数rを出力
乱数a₁～a_{k-1}を出力
処理終了

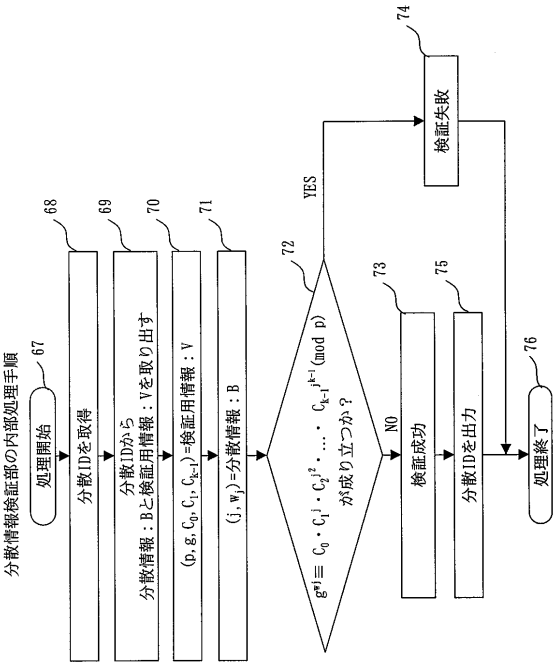
【図４】


検証用情報生成部の内部処理手順
処理開始
ID：Sを取得
秘密情報の復元に必要な最小個数：kを取得
素数rを取得
乱数a₁～a_{k-1}を取得
r以上p-1を満たす素数pを生成
乗法群Zpでの位数がrとなる要素gを定める
f(j)=g^{sj} mod pとする
C0=g^s (mod p)および
j=1,…,k-1としてCj=f(j)を算出
検証用情報：V=(p,g,C0,C1,…,Ck-1)を出力
処理終了

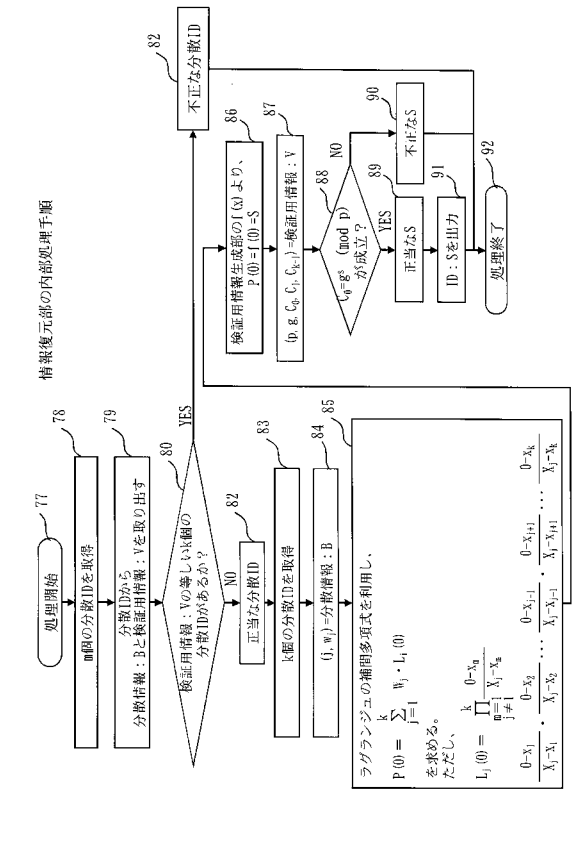
【図５】


分散ID_1
分散ID_2
分散ID_k
秘密情報復元部
分散ID=(分散情報：B，検証用情報：V)
分散情報検証部
分散ID1=(分散情報：B1，検証用情報：V)
分散ID2=(分散情報：B2，検証用情報：V)
分散IDk=(分散情報：Bk，検証用情報：V)
分散IDm=(分散情報：Bm，検証用情報：V)
情報復元部
ID

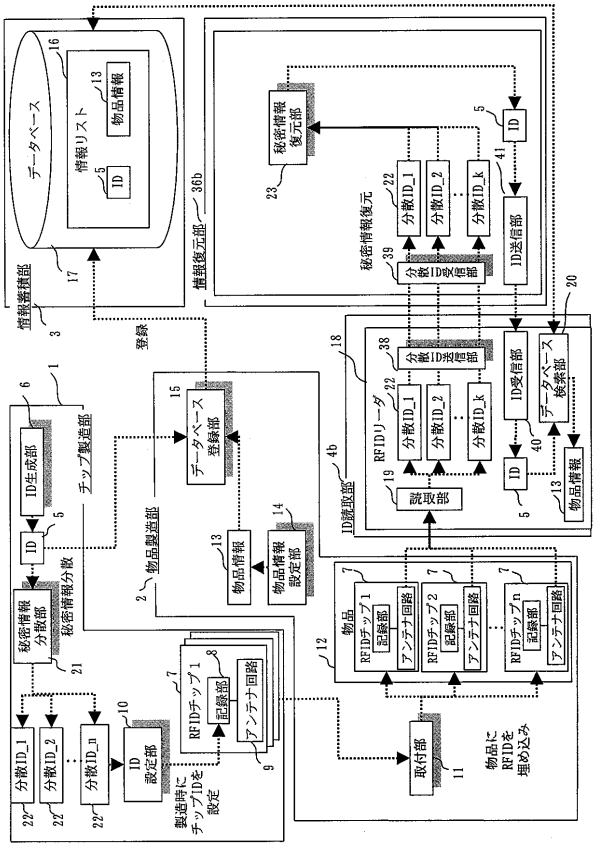
【図６】


分散情報検証部の内部処理手順
処理開始
分散IDを取得
分散IDから
分散情報：Bと検証用情報：Vを取り出す
(p, g, C0, C1, Ck-1)=検証用情報：V
(j, wj)=分散情報：B
が成り立つか？
YES
NO
検証成功
検証失敗
分散IDを出力
処理終了

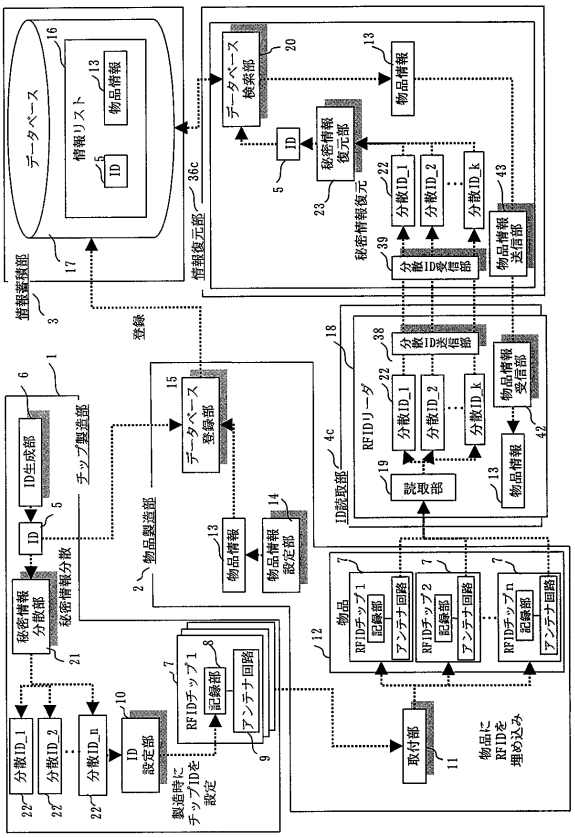
【図７】


情報復元部の内部処理手順
処理開始
m個の分散IDを取得
分散IDから
分散情報：Bと検証用情報：Vを取り出す
検証用情報：Vの等しいk個の分散IDがあるか？
YES
NO
正当な分散ID
k個の分散IDを取得
(j, wj)=分散情報：B
ラグランジュの補間多項式を利用し、
を求める。
ただし、
検証用情報生成部のf(x)より、
P(0)=f(0)=S
(p, g, C0, C1, Ck-1)=検証用情報：V
が成り立つ？
正当なS
ID：Sを出力
処理終了
不正な分散ID

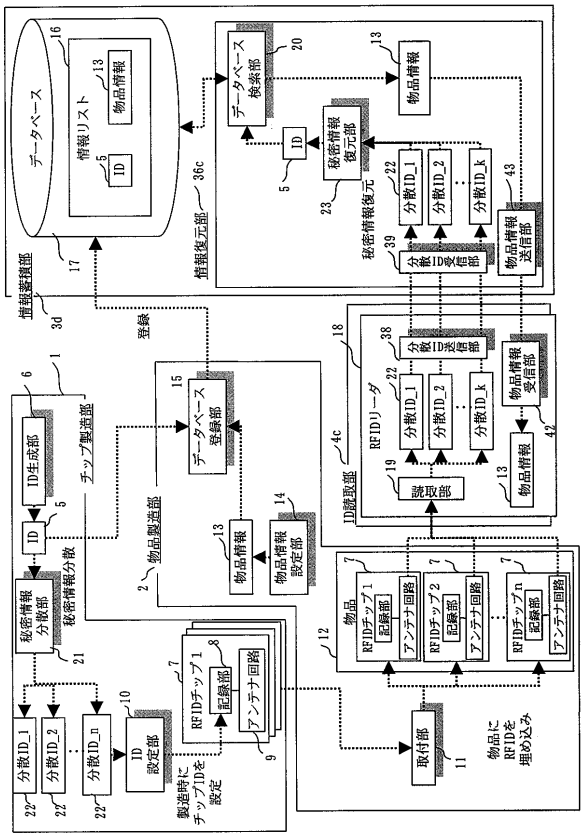
【図８】


データベース
情報リスト
物品情報
秘密情報分散部
秘密情報復元部
分散ID_1
分散ID_2
分散ID_k
分散ID_n
ID生成部
ID設定部
製造時にチップIDを設定
RFIDタグ1
RFIDタグ2
RFIDタグn
記録部
アンテナ回路
物品
取付部
物品に RFIDを 埋め込み
RFIDリーダ
読取部
ID送信部
ID受信部
データベース検索部
物品情報設定部
データベース登録部
物品製造部
チップ製造部
登録
秘密情報復元
情報復元部
ID読取部

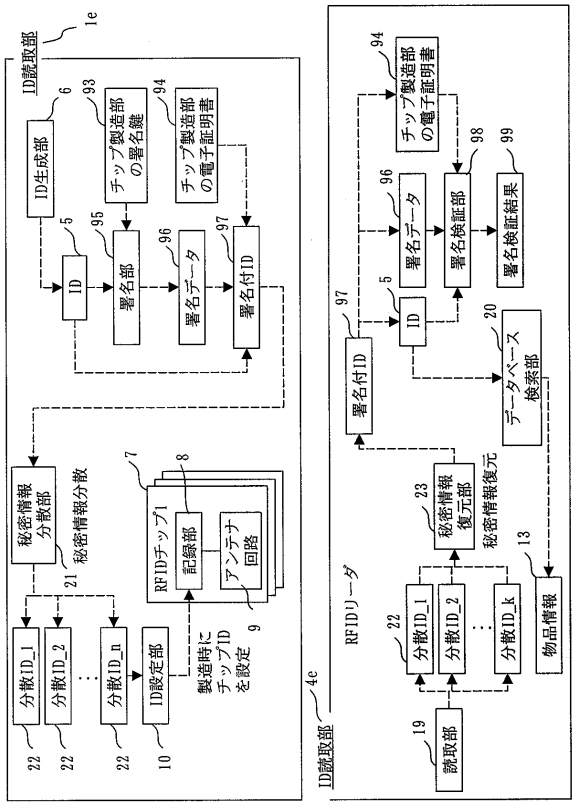
【図９】



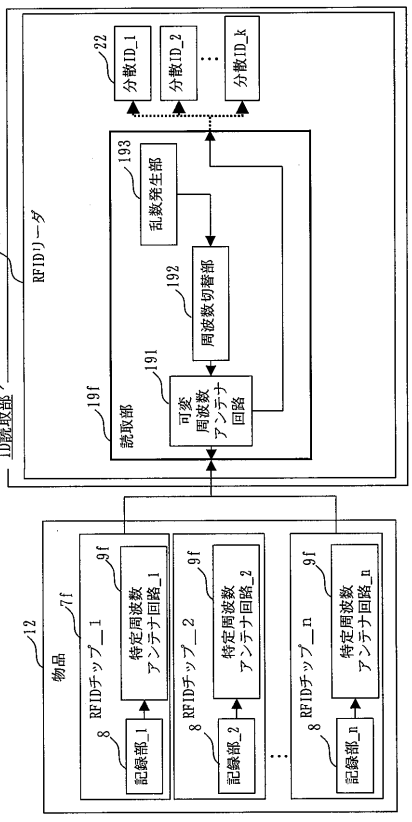

【図１０】



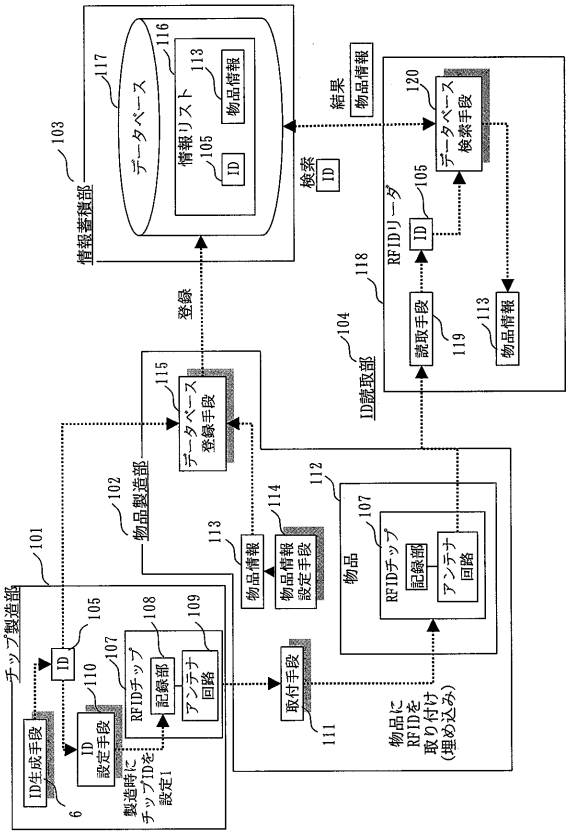

【図１１】




【図１２】



【図１３】


チップ製造部
101
ID生成手段
6
ID
105
ID
設定手段
110
製造時に
チップIDを
設定1
RFIDチップ
107
記録部
108
アンテナ
回路
109
物品製造部
102
取付手段
111
物品に
RFIDを
取り付け
(埋め込み)
物品
112
RFIDチップ
107
記録部
アンテナ
回路
物品情報
113
物品情報
設定手段
114
データベース
登録手段
115
登録
ID読取部
104
RFIDリーダ
118
読取手段
119
ID
105
物品情報
113
データベース
検索手段
120
検索
ID
結果
物品情報
情報蓄積部
103
データベース
117
情報リスト
116
ID
105
物品情報
113

フロントページの続き

(56)参考文献 特開平１１－３１７７３４（ＪＰ，Ａ）
特開平０８－１６７０１１（ＪＰ，Ａ）
Adi Shamir, How to Share a Secret, Communications of the ACM, １９７９年１１月, Volume 22, Number 11, 612-613

(58)調査した分野(Int.Cl., ＤＢ名)
Ｇ０６Ｆ ２１／００ － ２１／２４
Ｈ０４Ｌ ９／００