(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2006-65538
(P2006-65538A)
(43)公開日　平成18年3月9日(2006.3.9)

(51)Int.Cl.		F I			テーマコード（参考）
G06K 17/00	(2006.01)	G06K	17/00	F	5B017
G06F 21/24	(2006.01)	G06K	17/00	E	5B058
H04B 5/02	(2006.01)	G06F	12/14	540P	5J104
H04L 9/32	(2006.01)	H04B	5/02		5K012
H04L 9/08	(2006.01)	H04L	9/00	675Z	

審査請求 未請求　請求項の数 10　ＯＬ　（全 19 頁）　最終頁に続く

(21)出願番号　特願2004-246295 (P2004-246295)
(22)出願日　平成16年8月26日 (2004.8.26)

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(71)出願人　000237639
富士通フロンテック株式会社
東京都稲城市矢野口１７７６番地
(74)代理人　100101856
弁理士　赤澤　日出夫
(74)代理人　100097250
弁理士　石戸　久子
(72)発明者　橋本　繁
東京都稲城市矢野口１７７６番地　富士通フロンテック株式会社内

最終頁に続く

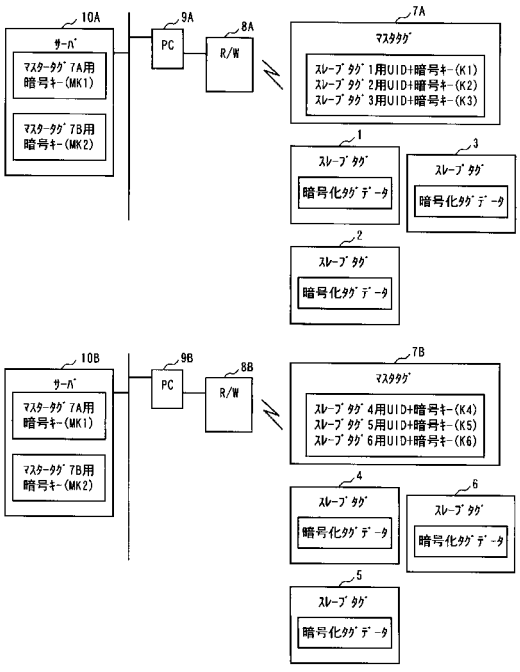
(54)【発明の名称】無線タグシステム、無線タグアクセス制御装置、無線タグアクセス制御方法、無線タグアクセス制御プログラム、及び無線タグ

(57)【要約】

【課題】　暗号キーの保管、管理が容易であり、且つセキュリティを高めることができる無線タグシステム、無線タグアクセス制御装置等を得る。

【解決手段】　複数の無線タグであって、第１の暗号キーで暗号化された情報を記憶するスレーブタグ１～３と、スレーブタグに対して設けられ、第２の暗号キーで暗号化された第１の暗号キーを記憶するマスタタグ７Ａと、マスタタグ７Ａにアクセスして該マスタタグ７Ａより取得した第１の暗号キーを第２の暗号キーを用いて復号し、該復号化された第１の暗号キーを用いてスレーブタグ１～３から取得したタグ情報を復号化する無線タグアクセス制御装置とを備えた。

【選択図】　図１



【特許請求の範囲】
【請求項１】
複数の無線タグであって、第１の暗号キーで暗号化されたタグデータを記憶するスレーブタグと、
複数の無線タグであって、第２の暗号キーで暗号化された前記第１の暗号キーを記憶するマスタタグと、
前記マスタタグにアクセスして該マスタタグより取得した前記第１の暗号キーを前記第２の暗号キーを用いて復号化し、該復号化された第１の暗号キーを用いて前記スレーブタグから取得した前記タグデータを復号化する無線タグアクセス制御装置と、
を備えてなる無線タグシステム。
【請求項２】
請求項１に記載の無線タグシステムにおいて、
前記マスタタグには、前記第１の暗号キーと、前記スレーブタグのユニークＩＤとを関連付けて記憶していることを特徴とする無線タグシステム。
【請求項３】
請求項１又は請求項２に記載の無線タグシステムにおいて、
前記第１の暗号キーと共に前記第１の暗号キーによる暗号方式が前記第２の暗号キーで暗号化されて前記マスタタグに記憶され、
前記無線タグアクセス制御装置は、前記第１の暗号キーと共に前記暗号方式を前記第２の暗号キーで復号化し、これら復号化された前記第１の暗号キーと暗号方式を用いて前記スレーブタグのタグデータを復号化することを特徴とする無線タグシステム。
【請求項４】
請求項１乃至請求項３のいずれかに記載の無線タグシステムにおいて、
前記スレーブタグに記憶されるタグデータは、複数のブロックに分けて構成されると共に、該ブロック毎に前記第１の暗号キーが設定されて該第１の暗号キーで暗号化され、
前記マスタタグに記憶される前記第１の暗号キーは、前記複数のブロック毎に対応して記憶され、且つ該ブロック毎に対応して設定される第２の暗号キーで暗号化されていることを特徴とする無線タグシステム。
【請求項５】
複数の無線タグであって、第１の暗号キーで暗号化されたタグデータを記憶するスレーブタグと、スレーブタグのユニークＩＤと前記第１の暗号キーのうち、少なくとも前記第１の暗号キーを第２の暗号キーで暗号化してなるスレーブタグ関連情報を記憶するマスタタグとにアクセスすることができる無線タグアクセス制御装置であって、
前記マスタタグにアクセスし、前記マスタタグに記憶されたスレーブタグ関連情報を取得するマスタタグ情報取得部と、
前記マスタタグ情報取得部により取得された前記スレーブタグ関連情報のうち、前記第２の暗号キーで暗号化された情報を、前記マスタタグに対応して取得された第２の暗号キーで復号化する第１復号化部と、
前記マスタタグ情報取得部により取得され、又は前記第１復号化部において復号化されて取得された前記スレーブタグのユニークＩＤを用いて前記スレーブタグにアクセスし、前記第１の暗号キーで暗号化されたタグデータを取得するスレーブタグデータ取得部と、
前記スレーブタグデータ取得部により取得されたタグデータを前記第１復号化部で復号化された第１の暗号キーで復号化する第２復号化部と
を備えてなる無線タグアクセス制御装置。
【請求項６】
請求項５に記載の無線アクセス制御装置において、
前記マスタタグに記憶されたスレーブタグ関連情報には、前記第１の暗号キーによる暗号方式が前記第２の暗号キーで暗号化されて含まれていて、
前記第１復号化部は、前記第２の暗号キーを用いて前記第１の暗号キーと共に前記暗号方式を復号化し、

前記第２復号化部は、前記第１の暗号キーと共に前記暗号方式を用いて前記スレーブタグデータ取得部により取得されたタグデータを復号化することを特徴とする無線タグアクセス制御装置。

【請求項７】

複数の無線タグであって、第１の暗号キーで暗号化されたタグデータを記憶するスレーブタグと、スレーブタグのユニークＩＤと前記第１の暗号キーのうち、少なくとも前記第１の暗号キーを第２の暗号キーで暗号化してなるスレーブタグ関連情報を記憶するマスタタグとにアクセスする無線タグアクセス制御方法であって、

前記マスタタグにアクセスし、前記マスタタグに記憶されたスレーブタグ関連情報を取得するマスタタグ情報取得ステップと、

前記マスタタグ情報取得ステップにより取得された前記スレーブタグ関連情報のうち、前記第２の暗号キーで暗号化された情報を、前記マスタタグに対応して取得された第２の暗号キーで復号化する第１復号化ステップと、

前記マスタタグ情報取得ステップにより取得された前記スレーブタグのユニークＩＤを用いて前記スレーブタグにアクセスし、前記第１の暗号キーで暗号化されたタグデータを取得するスレーブタグデータ取得ステップと、

前記スレーブタグデータ取得ステップにより取得されたタグデータを前記第１復号化ステップで復号化された第１の暗号キーで復号化する第２復号化ステップと

を備えてなる無線タグアクセス制御方法。

【請求項８】

複数の無線タグであって、第１の暗号キーで暗号化されたタグデータを記憶するスレーブタグと、スレーブタグのユニークＩＤと前記第１の暗号キーのうち、少なくとも前記第１の暗号キーを第２の暗号キーで暗号化してなるスレーブタグ関連情報を記憶するマスタタグとにアクセスする無線タグアクセス制御方法をコンピュータに実行させる無線タグアクセス制御プログラムであって、

前記マスタタグにアクセスし、前記マスタタグに記憶されたスレーブタグ関連情報を取得するマスタタグ情報取得ステップと、

前記マスタタグ情報取得ステップにより取得された前記スレーブタグ関連情報のうち、前記第２の暗号キーで暗号化された情報を、前記マスタタグに対応して取得された第２の暗号キーで復号化する第１復号化ステップと、

前記マスタタグ情報取得ステップにより取得され、又は前記第１復号化ステップにより復号化されて取得した前記スレーブタグのユニークＩＤを用いて前記スレーブタグにアクセスし、前記第１の暗号キーで暗号化されたタグデータを取得するスレーブタグデータ取得ステップと、

前記スレーブタグデータ取得ステップにより取得されたタグデータを前記第１復号化ステップで復号化された第１の暗号キーを用いて復号化する第２復号化ステップと

を備えてコンピュータに実行させる無線タグアクセス制御プログラム。

【請求項９】

請求項８に記載の無線アクセス制御プログラムにおいて、

前記マスタタグに記憶されたスレーブタグ関連情報には、前記第１の暗号キーによる暗号方式が前記第２の暗号キーにより暗号化されて含まれていて、

前記第１復号化ステップは、前記第２の暗号キーを用いて前記第１の暗号キーと共に前記暗号方式を復号化し、

前記第２復号化ステップは、復号化された前記第１の暗号キーと共に前記暗号方式を用いて前記スレーブタグ情報取得ステップにより取得されたタグデータを復号化することをコンピュータに実行させることを特徴とする無線タグアクセス制御プログラム。

【請求項１０】

無線アンテナとメモリ部を備え、リードライト装置から無線信号によりアクセスされることができる無線タグであって、

前記メモリ部に、

前記リードライト装置によってアクセスすることができる他の無線タグに係るユニークＩＤと、
前記ユニークＩＤを有する無線タグに記憶された情報を復号化するための第１の暗号キーであって、第２の暗号キーにより暗号化されてなる前記第１の暗号キーと、
を記憶してなる無線タグ。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、複数の無線タグ（ＩＣタグとも言う）とリードライト装置との間で交信を行うようにした無線タグシステム、及びこれに用いられる無線タグアクセス制御装置、無線タグアクセス制御方法、無線タグアクセス制御プログラム、並びに無線タグに関するものである。
【背景技術】
【０００２】
近年、ＩＣ技術の急速な発展に伴い、それを用いた無線タグシステムが急速に普及しつつある（例えば特許文献１参照）。
【０００３】
かかる無線タグシステムにおいては、複数の管理対象物に付された複数の無線タグをリードライト装置を介してアクセスし、必要な情報を適宜読み取り、或いは必要な情報を適宜書き込むことで、管理対象物の管理をシステム化して容易化する。
【０００４】
従来、無線タグ（以下、単にタグという）システムにおけるセキュリティのために、無線タグのメモリに書き込まれる情報（タグデータ）を暗号化することが知られている。図１０は従来の技術として、全てのタグデータを一つの暗号キーにて暗号化するようにした無線タグシステムの全体構成を示すブロック図である。
【０００５】
図１０に示す無線タグシステムは、複数のタグ１０１～１０３がリードライト装置１０８Ａを介してＰＣ（パーソナルコンピュータ）１０９Ａに接続可能とされている。また別の複数のタグ１０４～１０６がリードライト装置１０８Ｂを介してＰＣ１０９Ｂに接続可能とされている。各タグ１０１～１０６に記憶されるタグデータは、全て共通のタグ用暗号キーで暗号化されている。ＰＣ１０９Ａ，１０９Ｂにはサーバ１１０Ａ，１１０Ｂが接続されており、このサーバ１１０Ａ，１１０Ｂにタグデータを暗号化したタグ用暗号キーが記憶され、適宜ＰＣ１１０Ａ，１１０Ｂに提供される。
【０００６】
このような構成において、ＰＣ１０９Ａ，１０９Ｂによるタグ１０１～１０６との交信においては、ＰＣ１０９Ａ，１０９Ｂはサーバ１１０Ａ又は１１０Ｂより取得したタグ用暗号キーを用いて各タグより取得したタグデータを復号化し、或いはタグに書き込むデータを暗号化することにより、情報セキュリティを図っている。
【０００７】
しかしながら、このような構成においては、一つのタグ用暗号キーを共通に使用しているため、タグ用暗号キーが漏洩すると、それを用いて全てのタグにアクセスすることができるようになり、セキュリティ面で不十分である。
【０００８】
このため、他の従来技術として、図１１に示すように各タグ毎にタグ用暗号キーを異ならせると共にそれらをサーバにて管理し、ＰＣは交信を行う各タグ毎にそのタグに対応するタグ用暗号キーをサーバより取得し、復号化又は暗号化するようにした従来技術が知られている。
【０００９】
以下、図１１に示された従来の技術の動作を、図１２のフローチャート及び図１１のフロー概念図に従って説明する。なお、図１２の各ステップをＳで表し、図１３のステップ

をＰで表す。また、図１１において二つの対象物を区別して示している各符号のＡ，Ｂは説明の便宜上省略する。

【００１０】

まず、ＰＣ２０９Ａ，２０９Ｂ（以下説明の便宜上、二つの対象物を区別して示す各符号のＡ，Ｂは適宜省略する）が各タグと交信を行おうとする場合は、各タグのユニークＩＤ（以下、ＵＩＤという）取得指示（アンチコリージョン処理）をリードライト装置２０８に出力する（Ｐ１０１）。リードライト装置２０８は、この指示に従ってアンチコリージョン処理を行い（Ｐ１０２）、通信可能エリア内の全てのタグ（例えばＰＣ２０９Ａ（リードライト装置２０８Ａ）については、タグ２０１～２０３）からＵＩＤを取得する（Ｐ１０３，ステップＳ１０２）。

【００１１】

ＵＩＤを取得すると、次にＰＣ２０９は取得されたＵＩＤを用いてタグのリード指示をリードライト装置２０８に出力し（Ｐ１０４）、リードライト装置２０８は当該指示を各タグに送信する（Ｐ１０５）。タグはこのリード指示を受けてリードライト装置２０８にタグデータを送信し（Ｐ１０６）、リードライト装置２０８は当該ＵＩＤに係るタグから暗号化タグデータを受信しＰＣ２０９に取得させる（Ｐ１０７，ステップＳ１０２）。

【００１２】

ＰＣ２０９は、取得したタグデータを復号化するため、そのＵＩＤに対応する暗号キーをサーバ２１０から取得し（Ｐ１０８）、取得した暗号キーにて復号し、復号化されたタグデータを取得する（ステップＳ１０３）。

【００１３】

タグにデータを書き込む場合は、ＰＣ２０９はデータをサーバ２１０より取得したタグのＵＩＤに対応するタグ用暗号キーで暗号化し（ステップＳ１０４）、該暗号化されたデータと共にライト指示をリードライト装置２０８に出力する（Ｐ１０９，ステップＳ１０５）。リードライト装置２０８は、ライト指示と共に暗号化されたデータをタグに送信し、タグに当該指示に従って暗号化されたデータを書き込ませる（Ｐ１１０）。

【００１４】

このような構成によれば、一つのタグ用暗号キーが漏洩しても、それは一つのタグにしか適用できず、図１０に示した構成に比べて飛躍的にセキュリティを高めることが可能となる。

【特許文献１】特開２００３－１９６３６０号公報

【発明の開示】

【発明が解決しようとする課題】

【００１５】

しかしながら、例えば物流システムにおける管理において、バーコードの代りに上述した無線タグシステムを適用しようとすると、タグの個数が例えば数千万個という膨大な数となり、サーバのような上位装置が多数存在する場合は、各上位装置にて各タグのタグ用暗号キーを保管、管理するのは容易ではなくなるという問題点がある。

【００１６】

本発明は、上述した従来の問題点を解決するためになされたものであり、暗号キーの保管、管理が容易であり、且つセキュリティを高めることができる無線タグシステム、及びこれに用いられる無線タグアクセス制御装置、無線タグアクセス制御方法、無線タグアクセス制御プログラム、並びに無線タグを提供することを目的としている。

【課題を解決するための手段】

【００１７】

上述した課題を解決するため、本発明に係る無線タグシステムは、複数の無線タグであって、第１の暗号キーで暗号化されたタグデータを記憶するスレーブタグと、複数の無線タグであって、第２の暗号キーで暗号化された前記第１の暗号キーを記憶するマスタタグと、前記マスタタグにアクセスして該マスタタグより取得した前記第１の暗号キーを前記第２の暗号キーを用いて復号化し、該復号化された第１の暗号キーを用いて前記スレーブ

タグから取得した前記タグデータを復号化する無線タグアクセス制御装置とを備えてなるものである。

【００１８】

また、本発明の無線タグシステムにおいて、前記マスタタグには、前記第１の暗号キーと、前記スレーブタグのＵＩＤ（ユニークＩＤ）とを関連付けて記憶していることを特徴とする。

【００１９】

なお、本発明の無線タグシステムにおいて、前記スレーブタグのＵＩＤは前記第２の暗号キーにより暗号化されていて、前記無線タグアクセス制御装置は、前記第２の暗号キーを用いて前記第１の暗号キーと共に前記スレーブタグのＵＩＤを復号化し、該復号化されたＵＩＤを用いて前記スレーブタグにアクセスすることを特徴とすることができる。また、前記無線タグアクセス制御装置は、前記マスタタグのＵＩＤを取得して、該ＵＩＤに基づいて前記第２の暗号キーを取得することを特徴とすることができる。

【００２０】

また、本発明の無線タグシステムにおいて、前記第１の暗号キーと共に前記第１の暗号キーによる暗号方式が前記第２の暗号キーで暗号化されて前記マスタタグに記憶され、前記無線タグアクセス制御装置は、前記第１の暗号キーと共に前記暗号方式を前記第２の暗号キーで復号化し、これら復号化された前記第１の暗号キーと暗号方式を用いて前記スレーブタグのタグデータを復号化することを特徴とする。

【００２１】

この無線タグシステムにおいて、前記無線タグアクセス制御装置は、スレーブタグにアクセスする際に、マスタタグのＵＩＤを取得し、取得したマスタタグのＵＩＤに基づいて第２の暗号キーを取得すると共に、該ＵＩＤを用いて前記マスタタグにアクセスし、該マスタタグに記憶された前記スレーブタグのＵＩＤと第１の暗号キーとを取得して、少なくとも第１の暗号キーを前記第２の暗号キーで復号化し、取得されたスレーブタグのＵＩＤを用いて該スレーブタグにアクセスしてタグデータを取得し、取得したタグデータを前記第２の暗号キーで復号化された前記第１の暗号キーで復号化することを特徴とすることができる。

【００２２】

また、本発明の無線タグシステムにおいて、前記スレーブタグに記憶されるタグデータは、複数のブロックに分けて構成されると共に、該ブロック毎に前記第１の暗号キーが設定されて該第１の暗号キーで暗号化され、前記マスタタグに記憶される前記第１の暗号キーは、前記複数のブロック毎に対応して記憶され、且つ該ブロック毎に対応して設定される第２の暗号キーで暗号化されていることを特徴とする。

【００２３】

この無線タグシステムにおいて、前記ブロック毎に設定される前記第１の暗号キーによる暗号方式が前記ブロック毎に対応して前記第１の暗号キーと共に前記マスタタグに記憶され、前記無線タグアクセス制御装置は、前記第１の暗号キーと前記暗号方式とを前記ブロック毎に対応して設定された前記第２の暗号キーで復号化して取得し、これら復号化された前記第１の暗号キーと暗号方式を用いて前記スレーブタグのタグデータを復号化することを特徴とすることができる。

【００２４】

また、前記無線タグアクセス制御装置は、前記スレーブタグに記憶させるタグデータを、前記マスタタグより取得されて復号化された前記第１の暗号キーにより暗号化して記憶させることを特徴とすることができる。

【００２５】

また、本発明は、複数の無線タグであって、第１の暗号キーで暗号化されたタグデータを記憶するスレーブタグと、スレーブタグのＵＩＤと前記第１の暗号キーのうち、少なくとも前記第１の暗号キーを第２の暗号キーで暗号化してなるスレーブタグ関連情報を記憶するマスタタグとにアクセスすることができる無線タグアクセス制御装置であって、前記

マスタタグにアクセスし、前記マスタタグに記憶されたスレーブタグ関連情報を取得するマスタタグ情報取得部と、前記マスタタグ情報取得部により取得された前記スレーブタグ関連情報のうち、前記第２の暗号キーで暗号化された情報を、前記マスタタグに対応して取得された第２の暗号キーで復号化する第１復号化部と、前記マスタタグ情報取得部により取得され、又は前記第１復号化部において復号化されて取得された前記スレーブタグのＵＩＤを用いて前記スレーブタグにアクセスし、前記第１の暗号キーで暗号化されたタグデータを取得するスレーブタグデータ取得部と、前記スレーブタグデータ取得部により取得されたタグデータを前記第１復号化部で復号化された第１の暗号キーで復号化する第２復号化部とを備えてなるものである。

【００２６】

また、本発明の無線アクセス制御装置において、前記マスタタグに記憶されたスレーブタグ関連情報には、前記第１の暗号キーによる暗号方式が前記第２の暗号キーで暗号化されて含まれていて、前記第１復号化部は、前記第２の暗号キーを用いて前記第１の暗号キーと共に前記暗号方式を復号化し、前記第２復号化部は、前記第１の暗号キーと共に前記暗号方式を用いて前記スレーブタグデータ取得部により取得されたタグデータを復号化することを特徴とする。

【００２７】

また、本発明は、複数の無線タグであって、第１の暗号キーで暗号化されたタグデータを記憶するスレーブタグと、スレーブタグのＵＩＤと前記第１の暗号キーのうち、少なくとも前記第１の暗号キーを第２の暗号キーで暗号化してなるスレーブタグ関連情報を記憶するマスタタグとにアクセスする無線タグアクセス制御方法であって、前記マスタタグにアクセスし、前記マスタタグに記憶されたスレーブタグ関連情報を取得するマスタタグ情報取得ステップと、前記マスタタグ情報取得ステップにより取得された前記スレーブタグ関連情報のうち、前記第２の暗号キーで暗号化された情報を、前記マスタタグに対応して取得された第２の暗号キーで復号化する第１復号化ステップと、前記マスタタグ情報取得ステップにより取得された前記スレーブタグのＵＩＤを用いて前記スレーブタグにアクセスし、前記第１の暗号キーで暗号化されたタグデータを取得するスレーブタグデータ取得ステップと、前記スレーブタグデータ取得ステップにより取得されたタグデータを前記第１復号化ステップで復号化された第１の暗号キーで復号化する第２復号化ステップとを備えてなるものである。

【００２８】

また、本発明の無線アクセス制御方法において、前記マスタタグに記憶されたスレーブタグ関連情報には、前記第１の暗号キーによる暗号方式が前記第２の暗号キーにより暗号化されて含まれていて、前記第１復号化ステップは、前記第２の暗号キーを用いて前記第１の暗号キーと共に前記暗号方式を復号化し、前記第２復号化ステップは、復号化された前記第１の暗号キーと共に前記暗号方式を用いて前記スレーブタグ情報取得ステップにより取得されたタグデータを復号化することを特徴とすることができる。

【００２９】

また、本発明は、複数の無線タグであって、第１の暗号キーで暗号化されたタグデータを記憶するスレーブタグと、スレーブタグのＵＩＤと前記第１の暗号キーのうち、少なくとも前記第１の暗号キーを第２の暗号キーで暗号化してなるスレーブタグ関連情報を記憶するマスタタグとにアクセスする無線タグアクセス制御方法をコンピュータに実行させる無線タグアクセス制御プログラムであって、

前記マスタタグにアクセスし、前記マスタタグに記憶されたスレーブタグ関連情報を取得するマスタタグ情報取得ステップと、前記マスタタグ情報取得ステップにより取得された前記スレーブタグ関連情報のうち、前記第２の暗号キーで暗号化された情報を、前記マスタタグに対応して取得された第２の暗号キーで復号化する第１復号化ステップと、前記マスタタグ情報取得ステップにより取得され、又は前記第１復号化ステップにより復号化されて取得した前記スレーブタグのＵＩＤを用いて前記スレーブタグにアクセスし、前記第１の暗号キーで暗号化されたタグデータを取得するスレーブタグデータ取得ステップと

、前記スレーブタグデータ取得ステップにより取得されたタグデータを前記第１復号化ステップで復号化された第１の暗号キーを用いて復号化する第２復号化ステップとを備えてコンピュータに実行させるものである。

【００３０】

また、本発明の無線アクセス制御プログラムにおいて、前記マスタタグに記憶されたスレーブタグ関連情報には、前記第１の暗号キーによる暗号方式が前記第２の暗号キーにより暗号化されて含まれていて、前記第１復号化ステップは、前記第２の暗号キーを用いて前記第１の暗号キーと共に前記暗号方式を復号化し、

前記第２復号化ステップは、復号化された前記第１の暗号キーと共に前記暗号方式を用いて前記スレーブタグ情報取得ステップにより取得されたタグデータを復号化することをコンピュータに実行させることを特徴とする。

【００３１】

また、本発明は、無線アンテナとメモリ部を備え、リードライト装置から無線信号によりアクセスされることができる無線タグであって、前記メモリ部に、前記リードライト装置によってアクセスすることができる他の無線タグに係るＵＩＤと、前記ＵＩＤを有する無線タグに記憶された情報を復号化するための第１の暗号キーであって、第２の暗号キーにより暗号化されてなる前記第１の暗号キーとを記憶してなるものである。

【００３２】

また、本発明の無線タグにおいて、前記メモリ部に前記第１の暗号キーによる暗号方式を記憶してなることを特徴とすることができる。

【発明の効果】

【００３３】

本発明によれば、暗号キーの保管、管理が容易であり、且つセキュリティを高めることができるという効果を奏する。また、本発明によれば、膨大な量のスレーブタグのＵＩＤを全て一括してリードライト装置に記憶しておく必要が無く、アンチコリージョン処理などを迅速に行うこともできる。

【発明を実施するための最良の形態】

【００３４】

以下、本発明の実施の形態について、図面を参照しつつ説明する。

実施の形態１．

図１は本実施の形態１における無線タグシステムの全体構成を示すブロック図である。図１において、この無線タグシステムは、複数のスレーブタグ１～３及び４～６と、これら複数のスレーブタグ１～３及び４～６に対してそれぞれ一つずつ設けられるマスタタグ７Ａ，７Ｂと、これらマスタタグ７Ａ，スレーブタグ１～３及びマスタタグ７Ｂ，スレーブタグ４～６のそれぞれにアクセスし、交信を行うことができるリードライト装置（Ｒ／Ｗ）８Ａ，８Ｂと、リードライト装置８Ａ，８Ｂそれぞれを制御するＰＣ９Ａ，９Ｂと、ＰＣ９Ａ，９Ｂそれぞれに接続されマスタタグ７Ａ，７Ｂのマスタタグ用暗号キーを保管、管理し必要に応じてＰＣ９Ａ，９Ｂに与えることができるこれらＰＣ９Ａ，９Ｂの上位装置であるサーバ１０Ａ，１０Ｂとを備えている。

【００３５】

複数のスレーブタグ１～６は、それぞれ自己のＵＩＤを有し、それぞれのスレーブタグ用暗号キー（第１の暗号キー）で暗号化された暗号化タグデータ（タグ情報）を記憶している。マスタタグ７Ａは、自己のＵＩＤを有し、各スレーブタグ１～３のＵＩＤとそれらに対応するスレーブタグ用暗号キーＫ１～Ｋ３（各スレーブタグにより異なる）を関連付けて記憶している。また、マスタタグ７Ｂも同様に、自己のＵＩＤを有し、各スレーブタグ４～６のＵＩＤとそれらに対応するスレーブタグ用暗号キーＫ４～Ｋ６（各スレーブタグにより異なる）を関連付けて記憶している。なお、これらスレーブタグのＵＩＤとスレーブタグ用暗号キーはスレーブタグ関連情報とされる。

【００３６】

ここで、各マスタタグ７Ａ，７Ｂに記憶された各スレーブタグ用暗号キーは、それぞれ

異なるマスタタグ用暗号キーＭＫ１，ＭＫ２（第２の暗号キー）により暗号化されている。なお、各スレーブタグ１～６のＵＩＤもマスタタグ用暗号キーにより暗号化されていても良い。マスタタグ用暗号キーはサーバ１０Ａ，１０Ｂに保管、管理されている。

【００３７】

各マスタタグ７Ａ，７Ｂそれぞれは、リードライト装置８Ａ，８Ｂそれぞれの要求に応じて記憶した全てのスレーブタグ１～３，４～６それぞれのＵＩＤとそれらに対応付けて記憶したスレーブタグ用暗号キーとをリードライト装置８Ａ，８Ｂに送信することができる。リードライト装置８Ａ，８Ｂでは、送信された各スレーブタグのＵＩＤ及びスレーブタグ用暗号キーを受信して、それぞれＰＣ９Ａ，９Ｂに伝送することができる。ＰＣ９Ａ，９Ｂのそれぞれはサーバ１０Ａ，１０Ｂよりマスタタグ用暗号キーを取得し、マスタタグから得られたスレーブタグ用暗号キーを復号化することができる。なお、スレーブタグのＵＩＤが暗号化されている場合はＵＩＤも共に復号化する。そして、ＰＣ９Ａ，９Ｂはスレーブタグから得られた暗号化タグデータをマスタタグ７Ａ，７Ｂのそれぞれから取得し復号化したスレーブタグ用暗号キーにより復号化することができる。

【００３８】

図２はスレーブタグ１～３とマスタタグ７Ａの配置構造の一例を示す図であり、スレーブタグ１～３はダンボール１２内に収納される複数の衣服のそれぞれに取り付けられ、マスタタグ７Ａはそのダンボール１２壁面に例えば一つ取り付けられている。なお、このようなダンボールが二つある場合について例示したのが図１の構成に該当するが、通常このような管理体制下にあるダンボール数は数千、数万にも及び、本発明は、そのような場合にも容易に適用できる。

【００３９】

図３は、マスタタグ７Ａ，７Ｂ及びスレーブタグ１～６の基本構成を示すブロック図である。

【００４０】

これらのタグのそれぞれは、タグチップ（ＩＣチップ）１６とループ状のアンテナ１７によって構成される。タグチップ１６には、無線信号等のアナログ信号と内部処理のためのデジタル信号との変換を行うアナログ・デジタル変換部１８と、コマンドを解析し、必要な所定の処理を行うコマンド解析・処理部１９と、メモリ部２０とを備えている。そして、マスタタグにおいては、このメモリ部２０に自己のＵＩＤと、上述した各スレーブタグ１～６のＵＩＤ及びそれに対応するスレーブタグ用暗号キーＫ１～Ｋ６、その他必要な情報が暗号化されて記憶される。またスレーブタグ１においては、自己のＵＩＤと共に暗号化タグデータ（タグ情報）が記憶される。

【００４１】

ここで、ＰＣ９Ａ，９Ｂ、或いはリードライト装置８Ａ，８Ｂ、若しくはＰＣ９Ａ，９Ｂ及びリードライト装置８Ａ，８Ｂとは、無線タグ（スレーブタグ、マスタタグ）にアクセスすることができる本発明の無線タグアクセス制御装置を構成している。

【００４２】

以下、実施の形態１の動作として、無線タグアクセス制御装置（ＰＣ）において行われるスレーブタグとの交信処理を図４、図５を用いて説明する。図４は、同動作を示すフローチャートであり、図５は同動作を概念的に示した図である。なお、図１において二つの対象物を区別して示している各符号のＡ，Ｂは説明の便宜上省略する。

【００４３】

スレーブタグ１～６のいずれかとの交信を行おうとする場合、ＰＣ９はマスタタグ７のＵＩＤを取得するために、ＵＩＤ取得指示をリードライト装置８に出力する（Ｐ１）。リードライト装置８は例えばアンチコリージョン処理を行って、通信エリア内にあるマスタタグのＵＩＤを取得し（Ｐ２）、ＰＣ９はそれを取得する（Ｐ３，ステップＳ１）。

【００４４】

この場合、マスタタグ７のみをアンチコリージョン処理に参加させるため、マスタタグ専用のアンチコリージョン処理コマンドを用いるようにすることが好ましい。或いはマス

タタグのみを識別するグループアドレスをマスタタグに規定しておき、このグループアドレスを指定してアンチコリージョン処理コマンドを送信するようにしても良い。

【００４５】

次に、ＰＣ９は取得したＵＩＤに基づいて所定のマスタタグ７を指定して、そのリード指示をリードライト装置８に出力し（Ｐ４）、リードライト装置８は指定されたマスタタグ７についてそのリード指令を送信する（Ｐ５）。リード指令を受信したマスタタグ７は、それに記憶された全スレーブタグのＵＩＤとスレーブタグ用暗号キーであって、マスタタグ用暗号キーにより暗号化された情報をリードライト装置８に送信する（Ｐ６）。リードライト装置８はその情報を受信するとＰＣ９に送出し、ＰＣ９は指定したマスタタグ７からのスレーブタグに関する情報（ＵＩＤとスレーブタグ用暗号キー）を取得する（Ｐ７，ステップＳ２）。

【００４６】

スレーブタグに関する情報を取得したＰＣ９は、サーバ１０よりマスタタグ用暗号キー（第２の暗号キー）を取得し（Ｐ８）、取得したマスタタグ用暗号キーを用いて、暗号化されたスレーブタグ用暗号キー（第１の暗号キー）を復号化し（ＵＩＤも暗号化されている場合はＵＩＤも復号化する）、スレーブタグのＵＩＤとそれに対応するスレーブタグ用暗号キーを取得する（ステップＳ３）。

【００４７】

次に、ＰＣ９は取得したスレーブタグのＵＩＤを用いて所定のスレーブタグについてのリード指示をリードライト装置８に出力し（Ｐ９）、リードライト装置８はそのＵＩＤについてのスレーブタグにアクセスして（Ｐ１０）、そのスレーブタグより暗号化タグデータを取得し（Ｐ１１）、ＰＣ９に送出する。ＰＣ９はリードライト装置より送出された暗号化タグデータを取得する（Ｐ１２，ステップＳ４）。

【００４８】

ＰＣ９はマスタタグ７より取得して復号化したスレーブタグ用暗号キー（Ｋ１～Ｋ６）にてスレーブタグより取得した暗号化タグデータを復号化して当該タグデータを取得する（ステップＳ５）。

【００４９】

なお、引き続き、スレーブタグに新たなタグデータをライトする場合は、同スレーブタグ用暗号キーにより情報（タグデータ）を暗号化し（ステップＳ６）、それをスレーブタグにライトするライト指示をリードライト装置８に出力する（Ｐ１３）。リードライト装置８は、そのライト指示をスレーブタグに送信して（Ｐ１４）、一連の処理を終了する。

【００５０】

ここで、ステップＳ２は本発明における無線タグアクセス制御装置のマスタタグ情報取得部を構成し、ステップＳ３は同第１復号化部を構成し、ステップＳ４はスレーブタグデータ取得部を構成し、ステップＳ５は第２復号化部を構成している。

実施の形態２．

実施の形態２は、更にセキュリティ向上のため、マスタタグにスレーブタグ用暗号キーと共にそれによる暗号方式（例えばＤＥＳ／ＲＳＡ方式）を記憶させるようにしている。またスレーブタグデータを復号化もしくは暗号化する場合に、ＰＣはその暗号方式を暗号キーと共に用いてスレーブタグデータを復号化もしくは暗号化するようにする。

【００５１】

図６は実施の形態２におけるマスタタグの記憶部内のデータ構成を示した図である。図６に示されるように、マスタタグ７には、暗号方式である例えばＤＥＳ／ＲＳＡ方式を識別する識別子が各スレーブタグ用暗号方式識別子Ｄ１～Ｄ３としてスレーブタグ用暗号キーＫ１～Ｋ３と共にスレーブタグのＵＩＤに対応して記憶されている。この場合、スレーブタグ用暗号方式識別子Ｄ１～Ｄ３も実施の形態１で述べたマスタタグ用暗号キーにて暗号化されていることが好ましい。

実施の形態３．

図７は実施の形態３におけるマスタタグとスレーブタグのメモリ内容を示す図である。

図７に示すように、実施の形態３はさらなるセキュリティ向上のために、スレーブタグデータ（スレーブタグ情報）を複数のデータブロック（１）～（３）に分割すると共に、スレーブタグ用暗号キーをデータブロック毎に定めてなるデータブロック用暗号キーでデータブロック毎に暗号化してスレーブタグのメモリ部に記憶させる。そして、マスタタグには、それに対応させてデータブロック毎にデータブロック用暗号方式識別子（ＤＢ１～ＤＢ３）とデータブロック用暗号キー（ＫＢ１～ＫＢ３）を記憶するようにしたものである。

【００５２】

このような構成において、ＰＣ９では、マスタタグから得られたデータブロック用暗号方式識別子及びデータブロック用暗号キーを各ブロック毎にサーバから得られたマスタタグ用暗号キーでそれぞれ復号化する。そして、スレーブタグから得られた暗号化タグデータを、そのブロック毎に復号化されたデータブロック用暗号方式識別子とデータブロック用暗号キーを用いて復号化する。

【００５３】

なお、スレーブタグへのデータのライト時においても同様に、データをブロック分割して各ブロック毎にスレーブタグ用暗号キーと暗号方式を用いて暗号化し、スレーブタグにライトさせる。

【００５４】

以上に本発明の実施の形態について説明したが、ここでマスタタグに登録されているスレーブタグについてのデータ（ＵＩＤ及びスレーブタグ用暗号キー）の更新処理について説明しておく。

【００５５】

このデータの更新処理は、例えば図８に示されるように、所定時間（又は所定時刻）毎に行うことができる。ＰＣよりリードライト装置を介してマスタタグよりスレーブタグのＵＩＤを取得し（Ｐ３１）、そのＵＩＤを用いて順次各スレーブタグのデータリードを行っていく（Ｐ３２～Ｐ３４）。もし、あるスレーブタグ（図示ではＵＩＤ３）が管理下より外れた場合は、そのＵＩＤに係るスレーブタグからの応答がないため（Ｐ３４）、ＰＣはそのスレーブタグが管理下よりなくなったこと（例えばスレーブタグを付した商品が外部に移された場合等）を判断し、マスタタグにそのＵＩＤを削除するよう指示を出し、その指示を受けてマスタタグでは、そのスレーブタグについてのＵＩＤを削除する（Ｐ３５）。以下、残りのスレーブタグについて上述した実施の形態で述べた処理が行われる（Ｐ３６）。

【００５６】

次に、スレーブタグ及びマスタタグの初期設定時における処理について図９を用いて説明する。ＰＣはリードライト装置を介して、アンチコリージョン処理を行い、スレーブタグ及びマスタタグの全タグについてのＵＩＤを取得する（Ｐ４１）。そして、マスタタグのＵＩＤを判断すると（マスタタグとすべきタグは他のタグのＵＩＤと識別されるべきＵＩＤが設定されているものとする）、その他のＵＩＤに係るタグを全てスレーブタグとすると共に、各ＵＩＤに対してスレーブタグ用暗号キーを割り当てて、そのスレーブタグ用暗号キー又はそれと共にＵＩＤを第２の暗号キーで暗号化してそれらをマスタタグにライトして記憶させる（Ｐ４２）。暗号方式を使う場合は、その暗号方式も併せて記憶させるようにする。

【００５７】

また、初期設定時以降について、スレーブタグが追加された場合のマスタタグ情報の更新処理もほぼ同様に行うことができる。すなわち、スレーブタグについてアンチコリージョン処理を行い、マスタタグに登録されていないスレーブタグのＵＩＤが判断されると、それについて新たなスレーブタグ用暗号キーを割り当てて、そのスレーブタグ用暗号キー又はそれと共にＵＩＤを第２の暗号キーで暗号化してそれらをマスタタグにライトして記憶させる。

【００５８】

以上、本発明の実施の形態によれば、暗号化キーの保管、管理が容易であり、且つセキュリティを高めることができるが、それと共に、マスタタグにスレーブタグのＵＩＤを記憶させ、このＵＩＤをマスタタグのアンチコリージョン処理により取得して、各スレーブタグにアクセスするようにしたため、アンチコリージョン処理を全スレーブタグに対して行う必要がなく、アンチコリージョン処理に参加するタグの数を激減させることができて、その処理の迅速化を図ることが可能となる。

【００５９】

以上、本発明の実施の形態について説明したが、本実施の形態によれば、上述したフローチャート（図４）の処理を無線タグアクセス制御装置を構成するコンピュータに実行させるプログラムを無線タグアクセス制御プログラムとして提供することができる。上述したプログラムは、コンピュータにより読取り可能な記録媒体に記憶させることによって、無線タグアクセス制御装置を構成するコンピュータに実行させることが可能となる。ここで、上記コンピュータにより読取り可能な記録媒体としては、ＣＤ－ＲＯＭやフレキシブルディスク、ＤＶＤディスク、光磁気ディスク、ＩＣカード等の可搬型記憶媒体や、コンピュータプログラムを保持するデータベース、或いは、他のコンピュータ並びにそのデータベースや、更に回線上の伝送媒体をも含むものである。

（付記１）　複数の無線タグであって、第１の暗号キーで暗号化されたタグデータを記憶するスレーブタグと、

複数の無線タグであって、第２の暗号キーで暗号化された前記第１の暗号キーを記憶するマスタタグと、

前記マスタタグにアクセスして該マスタタグより取得した前記第１の暗号キーを前記第２の暗号キーを用いて復号化し、該復号化された第１の暗号キーを用いて前記スレーブタグから取得した前記タグデータを復号化する無線タグアクセス制御装置と、

を備えてなる無線タグシステム。

（付記２）付記１に記載の無線タグシステムにおいて、

前記マスタタグには、前記第１の暗号キーと、前記スレーブタグのユニークＩＤとを関連付けて記憶していることを特徴とする無線タグシステム。

（付記３）付記２に記載の無線タグシステムにおいて、

前記スレーブタグのユニークＩＤは前記第２の暗号キーにより暗号化されていて、前記無線タグアクセス制御装置は、前記第２の暗号キーを用いて前記第１の暗号キーと共に前記スレーブタグのユニークＩＤを復号化し、該復号化されたユニークＩＤを用いて前記スレーブタグにアクセスすることを特徴とする無線タグシステム。

（付記４）付記１乃至付記３のいずれかに記載の無線タグシステムにおいて、

前記無線タグアクセス制御装置は、前記マスタタグのユニークＩＤを取得して、該ユニークＩＤに基づいて前記第２の暗号キーを取得することを特徴とする無線タグシステム。

（付記５）付記１乃至付記４のいずれかに記載の無線タグシステムにおいて、

前記第１の暗号キーと共に前記第１の暗号キーによる暗号方式が前記第２の暗号キーで暗号化されて前記マスタタグに記憶され、

前記無線タグアクセス制御装置は、前記第１の暗号キーと共に前記暗号方式を前記第２の暗号キーで復号化し、これら復号化された前記第１の暗号キーと暗号方式を用いて前記スレーブタグのタグデータを復号化することを特徴とする無線タグシステム。

（付記６）付記１乃至付記５のいずれかに記載の無線タグシステムにおいて、

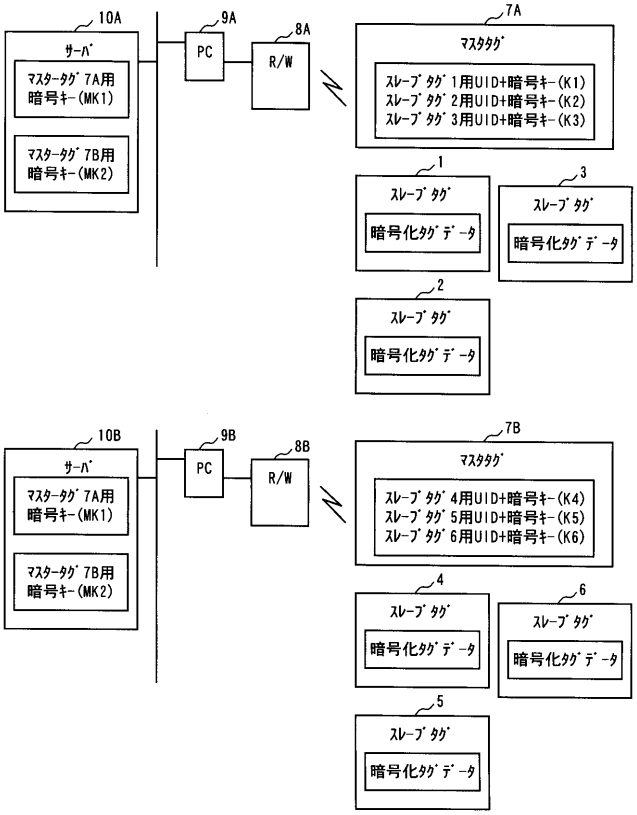
前記無線タグアクセス制御装置は、スレーブタグにアクセスする際に、マスタタグのユニークＩＤを取得し、取得したマスタタグのユニークＩＤに基づいて第２の暗号キーを取得すると共に、該ユニークＩＤを用いて前記マスタタグにアクセスし、該マスタタグに記憶された前記スレーブタグのユニークＩＤと第１の暗号キーとを取得して、少なくとも第１の暗号キーを前記第２の暗号キーで復号化し、取得されたスレーブタグのユニークＩＤを用いて該スレーブタグにアクセスしてタグデータを取得し、取得したタグデータを前記第２の暗号キーで復号化された前記第１の暗号キーで復号化することを特徴とする無線タグシステム。

（付記７）付記１乃至付記６のいずれかに記載の無線タグシステムにおいて、
前記スレーブタグに記憶されるタグデータは、複数のブロックに分けて構成されると共に、該ブロック毎に前記第１の暗号キーが設定されて該第１の暗号キーで暗号化され、
前記マスタタグに記憶される前記第１の暗号キーは、前記複数のブロック毎に対応して記憶され、且つ該ブロック毎に対応して設定される第２の暗号キーで暗号化されていることを特徴とする無線タグシステム。
（付記８）付記７に記載の無線タグシステムにおいて、
前記ブロック毎に設定される前記第１の暗号キーによる暗号方式が前記ブロック毎に対応して前記第１の暗号キーと共に前記マスタタグに記憶され、
前記無線タグアクセス制御装置は、前記第１の暗号キーと前記暗号方式とを前記ブロック毎に対応して設定された前記第２の暗号キーで復号化して取得し、これら復号化された前記第１の暗号キーと暗号方式を用いて前記スレーブタグのタグデータを復号化することを特徴とする無線タグシステム。
（付記９）付記１乃至付記８のいずれかに記載の無線タグシステムにおいて、
前記無線タグアクセス制御装置は、前記スレーブタグに記憶させるタグデータを、前記マスタタグより取得されて復号化された前記第１の暗号キーにより暗号化して記憶させることを特徴とする無線タグシステム。
（付記１０）複数の無線タグであって、第１の暗号キーで暗号化されたタグデータを記憶するスレーブタグと、スレーブタグのユニークＩＤと前記第１の暗号キーのうち、少なくとも前記第１の暗号キーを第２の暗号キーで暗号化してなるスレーブタグ関連情報を記憶するマスタタグとにアクセスすることができる無線タグアクセス制御装置であって、
前記マスタタグにアクセスし、前記マスタタグに記憶されたスレーブタグ関連情報を取得するマスタタグ情報取得部と、
前記マスタタグ情報取得部により取得された前記スレーブタグ関連情報のうち、前記第２の暗号キーで暗号化された情報を、前記マスタタグに対応して取得された第２の暗号キーで復号化する第１復号化部と、
前記マスタタグ情報取得部により取得され、又は前記第１復号化部において復号化されて取得された前記スレーブタグのユニークＩＤを用いて前記スレーブタグにアクセスし、前記第１の暗号キーで暗号化されたタグデータを取得するスレーブタグデータ取得部と、
前記スレーブタグデータ取得部により取得されたタグデータを前記第１復号化部で復号化された第１の暗号キーで復号化する第２復号化部と
を備えてなる無線タグアクセス制御装置。
（付記１１）付記１０に記載の無線アクセス制御装置において、
前記マスタタグに記憶されたスレーブタグ関連情報には、前記第１の暗号キーによる暗号方式が前記第２の暗号キーで暗号化されて含まれていて、
前記第１復号化部は、前記第２の暗号キーを用いて前記第１の暗号キーと共に前記暗号方式を復号化し、
前記第２復号化部は、前記第１の暗号キーと共に前記暗号方式を用いて前記スレーブタグデータ取得部により取得されたタグデータを復号化することを特徴とする無線タグアクセス制御装置。
（付記１２）複数の無線タグであって、第１の暗号キーで暗号化されたタグデータを記憶するスレーブタグと、スレーブタグのユニークＩＤと前記第１の暗号キーのうち、少なくとも前記第１の暗号キーを第２の暗号キーで暗号化してなるスレーブタグ関連情報を記憶するマスタタグとにアクセスする無線タグアクセス制御方法であって、
前記マスタタグにアクセスし、前記マスタタグに記憶されたスレーブタグ関連情報を取得するマスタタグ情報取得ステップと、
前記マスタタグ情報取得ステップにより取得された前記スレーブタグ関連情報のうち、前記第２の暗号キーで暗号化された情報を、前記マスタタグに対応して取得された第２の暗号キーで復号化する第１復号化ステップと、
前記マスタタグ情報取得ステップにより取得された前記スレーブタグのユニークＩＤを

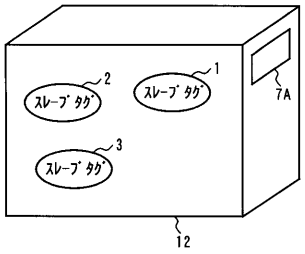
用いて前記スレーブタグにアクセスし、前記第１の暗号キーで暗号化されたタグデータを取得するスレーブタグデータ取得ステップと、
前記スレーブタグデータ取得ステップにより取得されたタグデータを前記第１復号化ステップで復号化された第１の暗号キーで復号化する第２復号化ステップと
を備えてなる無線タグアクセス制御方法。
（付記１３）付記１２に記載の無線アクセス制御方法において、
前記マスタタグに記憶されたスレーブタグ関連情報には、前記第１の暗号キーによる暗号方式が前記第２の暗号キーにより暗号化されて含まれていて、
前記第１復号化ステップは、前記第２の暗号キーを用いて前記第１の暗号キーと共に前記暗号方式を復号化し、
前記第２復号化ステップは、復号化された前記第１の暗号キーと共に前記暗号方式を用いて前記スレーブタグデータ取得ステップにより取得されたタグデータを復号化することを特徴とする無線タグアクセス制御方法。
（付記１４）複数の無線タグであって、第１の暗号キーで暗号化されたタグデータを記憶するスレーブタグと、スレーブタグのユニークＩＤと前記第１の暗号キーのうち、少なくとも前記第１の暗号キーを第２の暗号キーで暗号化してなるスレーブタグ関連情報を記憶するマスタタグとにアクセスする無線タグアクセス制御方法をコンピュータに実行させる無線タグアクセス制御プログラムであって、
前記マスタタグにアクセスし、前記マスタタグに記憶されたスレーブタグ関連情報を取得するマスタタグ情報取得ステップと、
前記マスタタグ情報取得ステップにより取得された前記スレーブタグ関連情報のうち、前記第２の暗号キーで暗号化された情報を、前記マスタタグに対応して取得された第２の暗号キーで復号化する第１復号化ステップと、
前記マスタタグ情報取得ステップにより取得され、又は前記第１復号化ステップにより復号化されて取得した前記スレーブタグのユニークＩＤを用いて前記スレーブタグにアクセスし、前記第１の暗号キーで暗号化されたタグデータを取得するスレーブタグデータ取得ステップと、
前記スレーブタグデータ取得ステップにより取得されたタグデータを前記第１復号化ステップで復号化された第１の暗号キーを用いて復号化する第２復号化ステップと
を備えてコンピュータに実行させる無線タグアクセス制御プログラム。
（付記１５）付記１４に記載の無線アクセス制御プログラムにおいて、
前記マスタタグに記憶されたスレーブタグ関連情報には、前記第１の暗号キーによる暗号方式が前記第２の暗号キーにより暗号化されて含まれていて、
前記第１復号化ステップは、前記第２の暗号キーを用いて前記第１の暗号キーと共に前記暗号方式を復号化し、
前記第２復号化ステップは、復号化された前記第１の暗号キーと共に前記暗号方式を用いて前記スレーブタグデータ取得ステップにより取得されたタグデータを復号化することをコンピュータに実行させることを特徴とする無線タグアクセス制御プログラム。
（付記１６）無線アンテナとメモリ部を備え、リードライト装置から無線信号によりアクセスされることができる無線タグであって、
前記メモリ部に、
前記リードライト装置によってアクセスすることができる他の無線タグに係るユニークＩＤと、
前記ユニークＩＤを有する無線タグに記憶されたタグデータを復号化するための第１の暗号キーであって、第２の暗号キーにより暗号化されてなる前記第１の暗号キーと、
を記憶してなる無線タグ。
（付記１７）付記１６に記載の無線タグにおいて、
前記メモリ部に前記第１の暗号キーによる暗号方式を記憶してなる無線タグ。
【図面の簡単な説明】
【００６０】

【図１】本発明の実施の形態１における無線タグシステムの全体構成を示すブロック図である。
【図２】マスタタグ及びスレーブタグの取り付け配置例を示す図である。
【図３】マスタタグ及びスレーブタグの構成を示すブロック図である。
【図４】実施の形態１の動作を示すフローチャートである。
【図５】実施の形態１の動作を示す概念図である。
【図６】実施の形態２を示すマスタタグのメモリ内容を示す図である。
【図７】実施の形態３を示すマスタタグとスレーブタグのメモリ内容を示す図である。
【図８】マスタタグに登録されているスレーブタグについてのデータ（ＵＩＤ及びスレーブタグ用暗号キー）の更新処理の動作を示す概念図である。
【図９】スレーブタグ及びマスタタグの初期設定処理の動作を示す概念図である。
【図１０】従来の技術として、全てのタグデータを一つの暗号キーにて暗号化するようにした無線タグシステムの全体構成を示すブロック図である。
【図１１】従来の技術の他の例に係る無線タグシステムの全体構成を示すブロック図である。
【図１２】図１１に示した従来の技術の動作を示すフローチャートである。
【図１３】図１１に示した従来の技術の動作を概念的に示す図である。
【符号の説明】
【００６１】
１，２，３，４，５，６　スレーブタグ、７、７Ａ，７Ｂ　マスタタグ、８Ａ，８Ｂ　リードライト装置（Ｒ／Ｗ）、９Ａ，９Ｂ　ＰＣ、１０Ａ，１０Ｂ　サーバ、１６　タグチップ（ＩＣチップ）、１７　ループアンテナ、１８　アナログ・デジタル変換部、１９　コマンド処理部、２０　メモリ部、Ｄ１　スレーブタグ１用暗号方式識別子、Ｄ２　スレーブタグ２用暗号方式識別子、Ｄ３　スレーブタグ３用暗号方式識別子、Ｋ１　スレーブタグ１用暗号キー、Ｋ２　スレーブタグ２用暗号キー、Ｋ３　スレーブタグ３用暗号キー、Ｋ４　スレーブタグ４用暗号キー、Ｋ５　スレーブタグ５用暗号キー、Ｋ６　スレーブタグ６用暗号キー、ＭＫ１　マスタタグ１用暗号キー、ＭＫ２　マスタタグ２用暗号キー、ＤＢ１　データブロック（１）用暗号方式識別子、ＤＢ２　データブロック（２）用暗号方式識別子、ＤＢ３　データブロック（３）用暗号方式識別子、ＫＢ１　データブロック（１）用暗号キー、ＫＢ２　データブロック（２）用暗号キー、ＫＢ３　データブロック（３）用暗号キー。

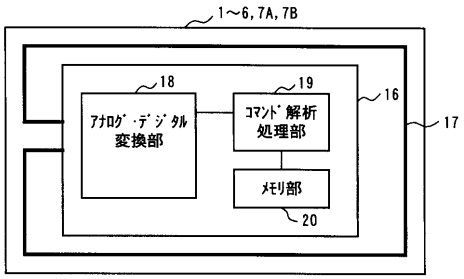
【図１】


10A
サーバ
マスタータグ 7A用 暗号キー(MK1)
マスタータグ 7B用 暗号キー(MK2)
9A
PC
8A
R/W
7A
マスタタグ
スレーブタグ 1用UID+暗号キー(K1)
スレーブタグ 2用UID+暗号キー(K2)
スレーブタグ 3用UID+暗号キー(K3)
1
スレーブタグ
暗号化タグデータ
3
スレーブタグ
暗号化タグデータ
2
スレーブタグ
暗号化タグデータ
10B
サーバ
マスタータグ 7A用 暗号キー(MK1)
マスタータグ 7B用 暗号キー(MK2)
9B
PC
8B
R/W
7B
マスタタグ
スレーブタグ 4用UID+暗号キー(K4)
スレーブタグ 5用UID+暗号キー(K5)
スレーブタグ 6用UID+暗号キー(K6)
4
スレーブタグ
暗号化タグデータ
6
スレーブタグ
暗号化タグデータ
5
スレーブタグ
暗号化タグデータ

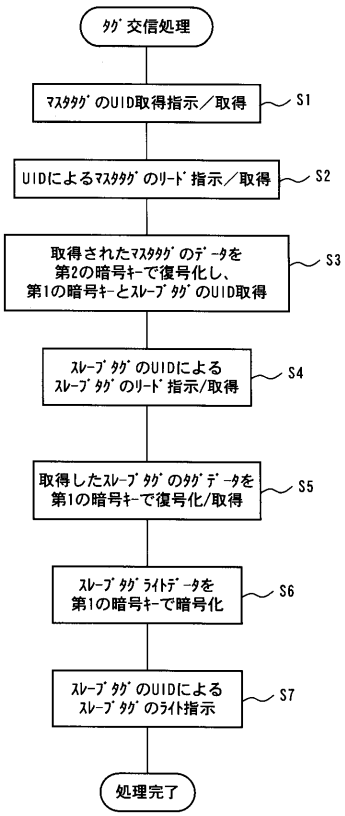
【図２】


スレーブタグ
2
スレーブタグ
1
7A
スレーブタグ
3
12

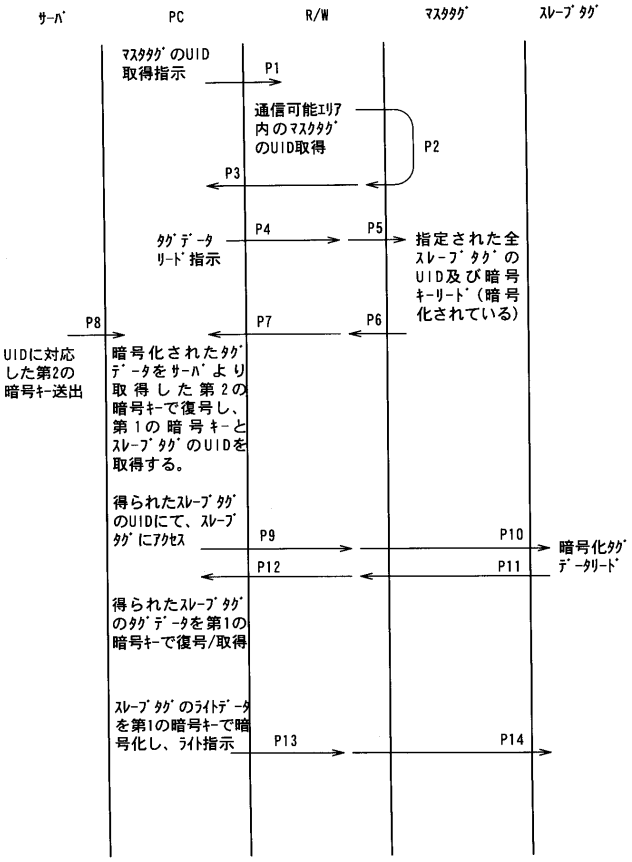
【図３】


1～6, 7A, 7B
18
アナログ・デジタル 変換部
19
コマンド解析 処理部
16
17
メモリ部
20

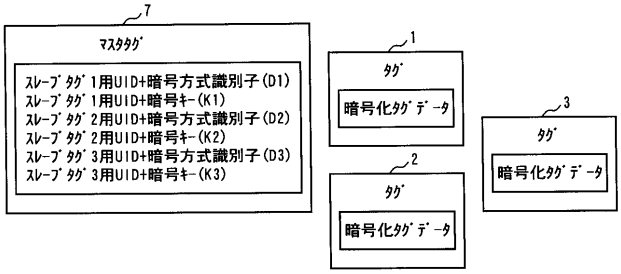
【図４】


タグ交信処理
マスタタグのUID取得指示／取得
S1
UIDによるマスタタグのリード指示／取得
S2
取得されたマスタタグのデータを 第2の暗号キーで復号化し、 第1の暗号キーとスレーブタグのUID取得
S3
スレーブタグのUIDによる スレーブタグのリード指示/取得
S4
取得したスレーブタグのタグデータを 第1の暗号キーで復号化/取得
S5
スレーブタグライトデータを 第1の暗号キーで暗号化
S6
スレーブタグのUIDによる スレーブタグのライト指示
S7
処理完了

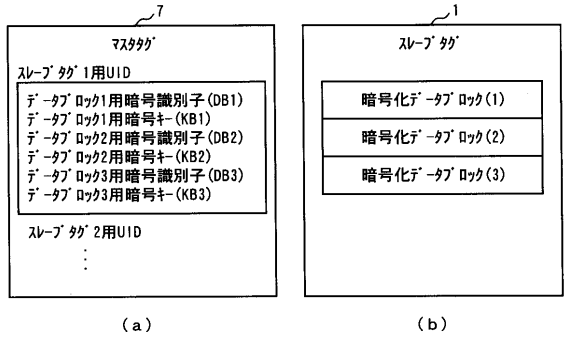
【図５】


サーバ
PC
R/W
マスタタグ
スレーブタグ
マスタタグのUID 取得指示
P1
通信可能エリア 内のマスタタグ のUID取得
P2
P3
タグデータ リード指示
P4
P5
指定された全 スレーブタグ の UID及び暗号 キーリード（暗号 化されている）
P8
P7
P6
UIDに対応 した第2の 暗号キー送出
暗号化されたタグ データをサーバより 取得した第2の 暗号キーで復号し、 第1の暗号キーと スレーブタグのUIDを 取得する。
得られたスレーブタグ のUIDにて、スレーブ タグにアクセス
P9
P10
暗号化タグ データリード
P12
P11
得られたスレーブタグ のタグデータを第1の 暗号キーで復号/取得
スレーブタグのライトデータ を第1の暗号キーで暗 号化し、ライト指示
P13
P14

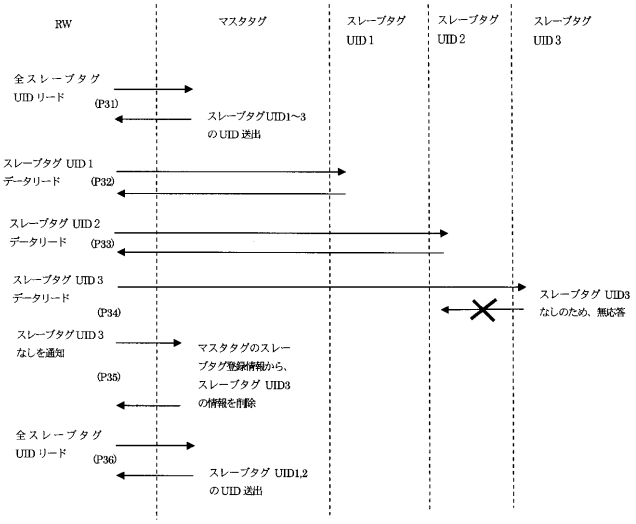
【図６】



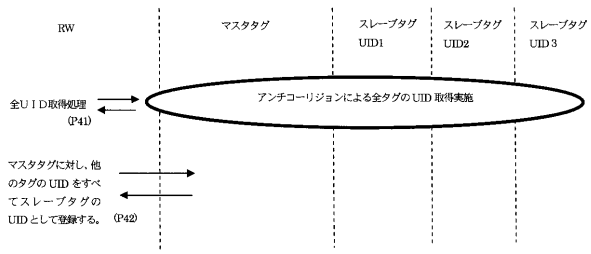
【図７】



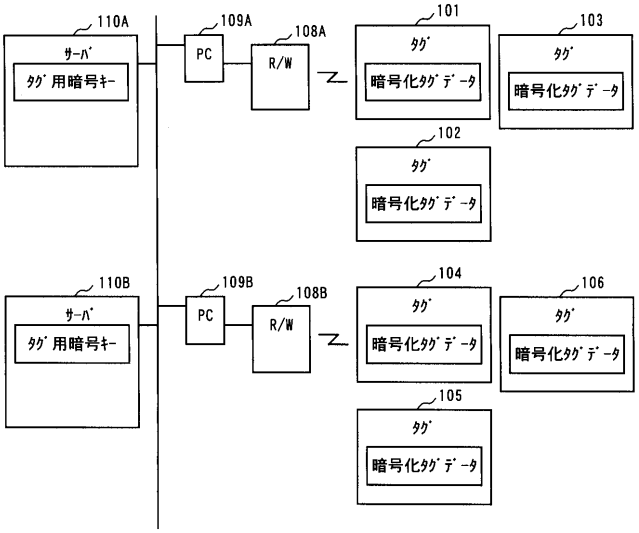
【図８】



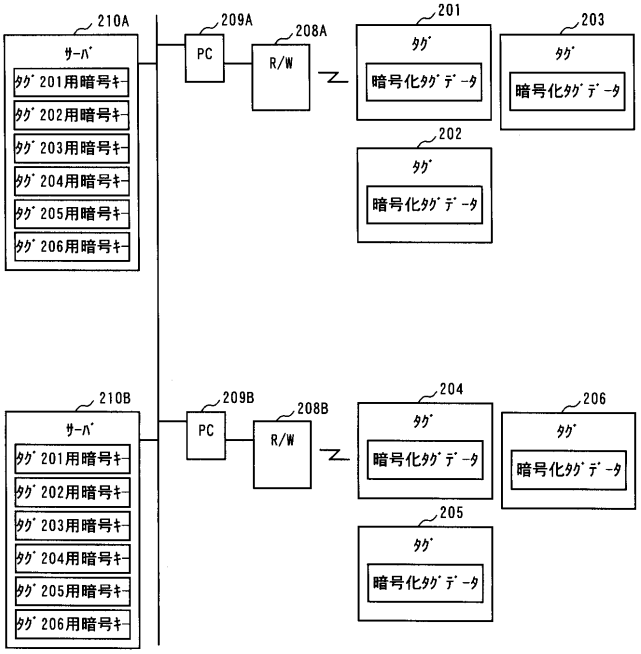
【図９】



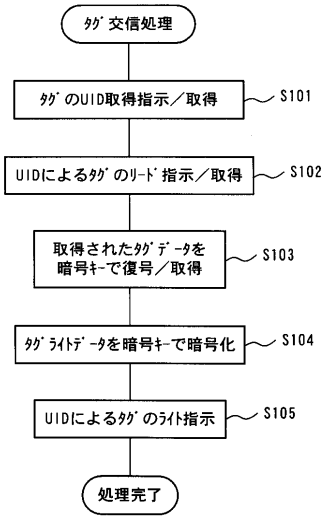
【図１０】



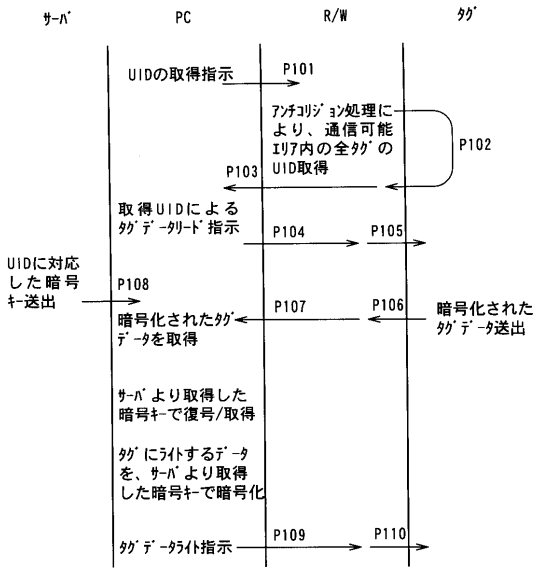
【図１１】


210A
ｻｰﾊﾞ
ﾀｸﾞ201用暗号ｷｰ
ﾀｸﾞ202用暗号ｷｰ
ﾀｸﾞ203用暗号ｷｰ
ﾀｸﾞ204用暗号ｷｰ
ﾀｸﾞ205用暗号ｷｰ
ﾀｸﾞ206用暗号ｷｰ
209A
PC
208A
R/W
201
ﾀｸﾞ
暗号化ﾀｸﾞﾃﾞｰﾀ
203
ﾀｸﾞ
暗号化ﾀｸﾞﾃﾞｰﾀ
202
ﾀｸﾞ
暗号化ﾀｸﾞﾃﾞｰﾀ
210B
ｻｰﾊﾞ
ﾀｸﾞ201用暗号ｷｰ
ﾀｸﾞ202用暗号ｷｰ
ﾀｸﾞ203用暗号ｷｰ
ﾀｸﾞ204用暗号ｷｰ
ﾀｸﾞ205用暗号ｷｰ
ﾀｸﾞ206用暗号ｷｰ
209B
PC
208B
R/W
204
ﾀｸﾞ
暗号化ﾀｸﾞﾃﾞｰﾀ
206
ﾀｸﾞ
暗号化ﾀｸﾞﾃﾞｰﾀ
205
ﾀｸﾞ
暗号化ﾀｸﾞﾃﾞｰﾀ

【図１２】


ﾀｸﾞ交信処理
ﾀｸﾞのUID取得指示／取得
S101
UIDによるﾀｸﾞのﾘｰﾄﾞ指示／取得
S102
取得されたﾀｸﾞﾃﾞｰﾀを
暗号ｷｰで復号／取得
S103
ﾀｸﾞﾗｲﾄﾃﾞｰﾀを暗号ｷｰで暗号化
S104
UIDによるﾀｸﾞのﾗｲﾄ指示
S105
処理完了

【図１３】


ｻｰﾊﾞ
PC
R/W
ﾀｸﾞ
UIDの取得指示
P101
ｱﾝﾁｺﾘｼﾞｮﾝ処理に
より、通信可能
ｴﾘｱ内の全ﾀｸﾞの
UID取得
P102
P103
取得UIDによる
ﾀｸﾞﾃﾞｰﾀﾘｰﾄﾞ指示
P104
P105
UIDに対応
した暗号
ｷｰ送出
P108
P107
P106
暗号化された
ﾀｸﾞﾃﾞｰﾀ送出
暗号化されたﾀｸﾞ
ﾃﾞｰﾀを取得
ｻｰﾊﾞより取得した
暗号ｷｰで復号/取得
ﾀｸﾞにﾗｲﾄするﾃﾞｰﾀ
を、ｻｰﾊﾞより取得
した暗号ｷｰで暗号化
ﾀｸﾞﾃﾞｰﾀﾗｲﾄ指示
P109
P110

フロントページの続き

(51)Int.Cl.	FI	テーマコード（参考）
	Ｈ０４Ｌ　9/00　６０１Ａ	

(72)発明者　波江野　正
東京都稲城市矢野口１７７６番地　富士通フロンテック株式会社内

Ｆターム(参考) 5B017 AA07 BA07 CA14
5B058 CA17 CA27 KA35
5J104 AA01 AA07 AA16 EA04 EA06 EA15 EA16 EA17 EA20 JA03
KA02 KA04 NA02 NA27 NA36 NA37 NA38 PA14
5K012 AB02 AC06 BA07