(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2006-53800
(P2006-53800A)
(43)公開日　平成18年2月23日(2006.2.23)

(51)Int.Cl.		F I			テーマコード（参考）
G06K 17/00	(2006.01)	G06K	17/00	D	5B058
H04L 9/32	(2006.01)	G06K	17/00	F	5J104
		H04L	9/00	673E	

審査請求 未請求　請求項の数 7　ＯＬ　（全 15 頁）

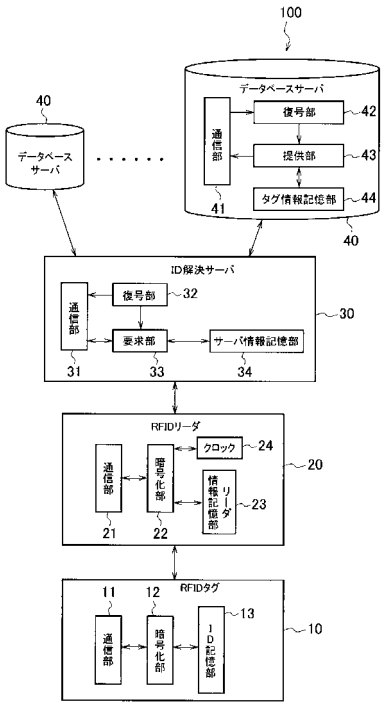
(21)出願番号　特願2004-235596 (P2004-235596)
(22)出願日　平成16年8月12日 (2004.8.12)

(71)出願人　392026693
株式会社エヌ・ティ・ティ・ドコモ
東京都千代田区永田町二丁目１１番１号
(74)代理人　100083806
弁理士　三好　秀和
(74)代理人　100100712
弁理士　岩▲崎▼　幸邦
(74)代理人　100095500
弁理士　伊藤　正和
(74)代理人　100101247
弁理士　高橋　俊一
(74)代理人　100117064
弁理士　伊藤　市太郎

最終頁に続く

(54)【発明の名称】情報提供方法、情報提供システム及び中継装置

(57)【要約】
【課題】ＲＦＩＤタグと、ＲＦＩＤリーダと、データベースサーバとが関与する情報提供の過程において、安全な情報提供を容易に実現する。
【解決手段】ＩＤ解決サーバ３０が、ＲＦＩＤリーダ２０から、暗号化ＲＦＩＤ１及び暗号化ユーザＩＤ２ｃを受信する。ＩＤ解決サーバ３０は、暗号化ＲＦＩＤ１を復号し、復号結果に基づいて、タグ情報を提供するデータベースサーバ４０を判断し、タグ情報を要求する。ＩＤ解決サーバ３０は、データベースサーバ４０からタグ情報を受信し、ＲＦＩＤリーダ２０に送信する。
【選択図】図１



【特許請求の範囲】
【請求項１】
中継装置が、暗号化された発信装置識別子を発信装置から受信する受信装置から、受信装置識別子及び前記暗号化された発信装置識別子を受信し、
前記暗号化された発信装置識別子を復号し、
該復号結果に基づいて、前記発信装置に関する発信装置情報を提供する情報提供装置を判断し、前記発信装置情報を前記情報提供装置に要求し、
該情報提供装置から前記発信装置情報を受信し、前記受信装置に送信することを特徴とする情報提供方法。
【請求項２】
前記受信装置は、前記情報提供装置の暗号鍵を用いて前記受信装置識別子を暗号化し、該暗号化された受信装置識別子を前記中継装置に送信し、
前記中継装置は、前記暗号化された受信装置識別子を前記情報提供装置に送信して前記発信装置情報を要求し、
前記情報提供装置は、前記暗号化された受信装置識別子を復号し、該復号結果に応じて前記発信装置情報を前記中継装置に送信することを特徴とする請求項１に記載の情報提供方法。
【請求項３】
前記発信装置は、前記暗号化された発信装置識別子を、暗号化する毎に変化させることを特徴とする請求項１又は２に記載の情報提供方法。
【請求項４】
暗号化された発信装置識別子を発信装置から受信する受信装置から、受信装置識別子及び前記暗号化された発信装置識別子を受信し、前記暗号化された発信装置識別子を復号し、該復号結果に基づいて、前記発信装置に関する発信装置情報を提供する情報提供装置を判断し、前記発信装置情報を前記情報提供装置に要求し、該情報提供装置から前記発信装置情報を受信し、前記受信装置に送信する中継装置と、
該中継装置の要求に応じて前記発信装置情報を前記中継装置に送信する情報提供装置とを備えることを特徴とする情報提供システム。
【請求項５】
前記受信装置は、前記情報提供装置の暗号鍵を用いて前記受信装置識別子を暗号化し、該暗号化された受信装置識別子を前記中継装置に送信し、
前記中継装置は、前記暗号化された受信装置識別子を前記情報提供装置に送信して前記発信装置情報を要求し、
前記情報提供装置は、前記暗号化された受信装置識別子を復号し、該復号結果に応じて前記発信装置情報を前記中継装置に送信することを特徴とする請求項４に記載の情報提供システム。
【請求項６】
前記発信装置は、前記暗号化された発信装置識別子を、暗号化する毎に変化させることを特徴とする請求項４又は５に記載の情報提供システム。
【請求項７】
暗号化された発信装置識別子を発信装置から受信する受信装置から、受信装置識別子及び前記暗号化された発信装置識別子を受信する受信手段と、
前記暗号化された発信装置識別子を復号する復号手段と、
該復号手段による復号結果に基づいて、前記発信装置に関する発信装置情報を提供する情報提供装置を判断し、前記発信装置情報を前記情報提供装置に要求する要求手段と、
前記情報提供装置から前記発信装置情報を受信し、前記受信装置に送信する転送手段とを備えることを特徴とする中継装置。

【発明の詳細な説明】
【技術分野】

【０００１】
本発明は、情報提供方法、情報提供システム及び中継装置に関する。
【背景技術】
【０００２】
従来、ＲＦＩＤ（Radio Frequency Identification）を発信するＲＦＩＤタグと、ＲＦＩＤを受信するＲＦＩＤリーダを用いたシステムでは、ＲＦＩＤリーダが、ＲＦＩＤについてデータベースサーバに問い合わせることにより、ＲＦＩＤタグが貼付されている物体を識別することができる。よって、ＲＦＩＤタグを追跡することにより、ＲＦＩＤタグが貼付されている物体を追跡することができる。そのため、物体と同様にしてＲＦＩＤと人を関連付けることによって、人を追跡することが可能となる問題が生じている。
【０００３】
具体的には、目視やその他の方法によりユーザＩＤとＲＦＩＤタグの関連付けが容易な場合に、ＲＦＩＤの追跡によるユーザの追跡が容易になる。例えば、図４に示すように、ＲＦＩＤリーダ２２０が、ユーザ２５０ａのユーザＩＤ「Ａ」とＲＦＩＤタグ２１０ａのＲＦＩＤ「α」とを関連付け、ユーザ２５０ｂのユーザＩＤ「Ｂ」とＲＦＩＤタグ２１０ｂのＲＦＩＤ「β」とを関連付けることにより、ユーザ２５０ａ，２５０ｂを容易に追跡できてしまう。
【０００４】
このようなＲＦＩＤタグによるプライバシー侵害を防ぐために、ＲＦＩＤを変更する方式が提案されている（例えば、非特許文献１、非特許文献２、特許文献１参照）。非特許文献１には、ＲＦＩＤタグが記憶するＲＦＩＤを書き換え可能とすることにより、継続的なＲＦＩＤタグの追跡を回避する方法が提案されている。この方法では、本来のＲＦＩＤと書き換えたＲＦＩＤとの対応付けをデータベースサーバに蓄積し、両者の関連性を保っている。非特許文献２には、ＲＦＩＤタグがＲＦＩＤを用いてハッシュ値を求め、毎回発信する情報を変更することで追跡を回避する方法が提案されている。この方法では、データベースサーバがＲＦＩＤタグと同様の計算を行い、ＲＦＩＤタグとデータベースサーバが同期をとることで、同一性を確保している。
【非特許文献１】木下真吾，星野文学，小室智之，藤村明子，大久保美也子，“ＲＦＩＤプライバシー保護を実現する可変秘匿ＩＤ方式”，ＮＴＴ情報流通プラットフォーム研究所，Computer Security Symposium 2003
【非特許文献２】大久保美也子，鈴木幸太郎，木下真吾，“Forward－secure RFID Privacy Protection for Low－cost ＲＦＩＤ”，ＮＴＴ情報流通プラットフォーム研究所，Computer Security Symposium 2003
【特許文献１】特開２００４－１９２６４５号公報
【発明の開示】
【発明が解決しようとする課題】
【０００５】
しかしながら、従来方法では、ＲＦＩＤリーダがＲＦＩＤについてデータベースサーバに問い合わせるために、ＲＦＩＤリーダがデータベースサーバに関するサーバ情報を知る必要があった。しかし、例えば、データベースサーバが個人の所有物の場合等には、サーバ情報そのものが個人情報等の他人に知られたくない情報の場合がある。このように従来方法では、ＲＦＩＤリーダに、個人情報等のサーバ情報が知られてしまう問題があった。
【０００６】
又、非特許文献１の方法では、ＲＦＩＤタグが認証機能等を備えない限り、ＲＦＩＤをだれでも書き換えることができ、データベースサーバが関連性を保持できなくなるおそれがある。又、書き換えを行わない間は追跡が可能となってしまう。非特許文献２の方法では、ＲＦＩＤタグとデータベースサーバが同期をとれなくなってしまうと機能しない。しかし、ＲＦＩＤタグの利用形態を考慮した場合、完全な同期を実現するのは困難である。又、同期維持には膨大な計算が必要となる。このように、従来の方法では、追跡回避のためにＲＦＩＤを変更することで、複雑な管理が必要となり、追跡回避を容易に実現するこ

とができなかった。

【０００７】

又、図５に示すように、ＲＦＩＤリーダ２２０ａが、ＲＦＩＤタグ２１０ａからＲＦＩＤ「α」を受信し、データベースサーバ２４０にＲＦＩＤ「α」を提示してＲＦＩＤタグ２１０ａに関する情報を問い合わせる際に、ＲＦＩＤリーダ２２０ａを所有するユーザのユーザＩＤ「Ａ」を送信する場合がある。このとき、データベースサーバ２４０は、ＲＦＩＤリーダ２２０ａのユーザＩＤ「Ａ」と、ＲＦＩＤタグ２１０ａのＲＦＩＤ「α」と、ＲＦＩＤタグ２１０ａの位置情報「Ｘ」等を対応付けることができる。同様に、データベースサーバ２４０は、ＲＦＩＤリーダ２２０ｂのユーザＩＤ「Ｂ」と、ＲＦＩＤタグ２１０ｂのＲＦＩＤ「β」と、ＲＦＩＤタグ２１０ｂの位置情報「Ｙ」を対応付けることができる。そのため、データベースサーバ２４０は、ＲＦＩＤリーダ２２０ａ，２２０ｂを追跡することができ、ＲＦＩＤリーダ２２０ａ，２２０ｂのユーザを追跡することができる。これは、データベースサーバ２４０が、ＲＦＩＤリーダ２２０ａ，２２０ｂのユーザがユーザＩＤ等の情報を開示したくない相手の場合に問題となる。

【０００８】

以上のように、従来方法では、ＲＦＩＤタグ等の発信装置と、ＲＦＩＤリーダ等の受信装置と、データベースサーバ等の発信装置に関する発信装置情報を提供する情報提供装置を利用した情報提供の過程において、情報を秘匿化したい相手に対しては秘匿化し、情報提供を安全に行うことが困難であった。

【０００９】

そこで、本発明は、発信装置と、受信装置と、情報提供装置とが関与する情報提供の過程において、安全な情報提供を容易に実現することを目的とする。

【課題を解決するための手段】

【００１０】

本発明に係る情報提供方法は、中継装置が、暗号化された発信装置識別子を発信装置から受信する受信装置から、受信装置識別子及び暗号化された発信装置識別子を受信し、暗号化された発信装置識別子を復号し、復号結果に基づいて、発信装置に関する発信装置情報を提供する情報提供装置を判断し、発信装置情報を情報提供装置に要求し、情報提供装置から発信装置情報を受信し、受信装置に送信することを特徴とする。発信装置識別子は、発信装置を一意に特定可能な情報である。受信装置識別子は、受信装置を一意に特定可能な情報である。

【００１１】

このような情報提供方法によれば、発信装置識別子を暗号化した場合であっても、中継装置は、暗号化された発信装置識別子を復号し、受信装置が希望する発信装置情報を提供する情報提供装置を判断できる。そして、中継装置は、情報提供装置と受信装置との間で発信装置情報を中継できる。よって、受信装置に対して、発信装置識別子及び情報提供装置に関する提供装置情報を秘匿化することが可能となる。従って、発信装置と、受信装置と、情報提供装置とが関与する情報提供の過程において、安全な情報提供を容易に実現することができる。

【００１２】

更に、受信装置は、情報提供装置の暗号鍵を用いて受信装置識別子を暗号化し、その暗号化された受信装置識別子を中継装置に送信することが好ましい。この場合、中継装置は、暗号化された受信装置識別子を情報提供装置に送信して発信装置情報を要求することが好ましい。又、情報提供装置は、暗号化された受信装置識別子を復号し、その復号結果に応じて発信装置情報を中継装置に送信することが好ましい。

【００１３】

これによれば、受信装置識別子を知ることができる情報提供装置を、暗号化された受信装置識別子を復号可能な、受信装置が暗号化に用いた暗号鍵の復号鍵を持つ情報提供装置に限定できる。よって、受信装置は、受信装置識別子を知られたくない情報提供装置に対して受信装置識別子を秘匿化できる。更に、情報提供装置は、復号結果に応じて、即ち、

受信装置が情報提供装置に対して受信装置識別子を秘匿化するか開示するかに応じて、送信する発信装置情報を制御することができる。又、発信装置は、暗号化された発信装置識別子を、暗号化する毎に変化させることが好ましい。これによれば、より安全性を高めることができる。

【００１４】

本発明に係る情報提供システムは、暗号化された発信装置識別子を発信装置から受信する受信装置から、受信装置識別子及び暗号化された発信装置識別子を受信し、暗号化された発信装置識別子を復号し、復号結果に基づいて、発信装置に関する発信装置情報を提供する情報提供装置を判断し、発信装置情報を情報提供装置に要求し、情報提供装置から発信装置情報を受信し、受信装置に送信する中継装置と、中継装置の要求に応じて発信装置情報を中継装置に送信する情報提供装置とを備えることを特徴とする。

【００１５】

本発明に係る中継装置は、暗号化された発信装置識別子を発信装置から受信する受信装置から、受信装置識別子及び暗号化された発信装置識別子を受信する受信手段と、暗号化された発信装置識別子を復号する復号手段と、復号手段による復号結果に基づいて、発信装置に関する発信装置情報を提供する情報提供装置を判断し、発信装置情報を情報提供装置に要求する要求手段と、情報提供装置から発信装置情報を受信し、受信装置に送信する転送手段とを備えることを特徴とする。

【００１６】

このような中継装置によれば、発信装置識別子を暗号化した場合であっても、暗号化された発信装置識別子を復号し、受信装置が希望する発信装置情報を提供する情報提供装置を判断できる。そして、中継装置は、情報提供装置と受信装置との間で発信装置情報を中継できる。よって、受信装置に対して、発信装置識別子及び提供装置情報を秘匿化することが可能となる。従って、発信装置と、受信装置と、情報提供装置とが関与する情報提供の過程において、安全な情報提供を容易に実現することができる。

【発明の効果】

【００１７】

以上説明したように、本発明によれば、発信装置と、受信装置と、情報提供装置とが関与する情報提供の過程において、安全な情報提供を容易に実現することができる。

【発明を実施するための最良の形態】

【００１８】

（情報提供システム）

図１に示すように、情報提供システム１００は、ＲＦＩＤタグ１０と、ＲＦＩＤリーダ２０と、ＩＤ解決サーバ３０と、複数のデータベースサーバ４０とを備える。ＲＦＩＤタグ１０は、発信装置識別子を受信装置に送信する発信装置である。ＲＦＩＤリーダ２０は、発信装置識別子を受信する受信装置である。データベースサーバ４０は、発信装置に関する発信装置情報を提供する情報提供装置である。ＩＤ解決サーバ３０は、受信装置と情報提供装置とのやりとりを中継する中継装置である。

【００１９】

ＲＦＩＤタグ１０は、通信部１１と、暗号化部１２と、ＩＤ記憶部１３とを備える。ＩＤ記憶部１３は、ＲＦＩＤを記憶する。ＲＦＩＤは、発信装置識別子であり、ＲＦＩＤタグ１０を一意に特定可能な情報である。

【００２０】

暗号化部１２は、発信装置識別子としてＲＦＩＤを暗号化する。暗号化部１２は、ＩＤ記憶部１３からＲＦＩＤを取得する。暗号化部１２は、ＩＤ解決サーバ３０の暗号鍵（以下、「ＩＤＲＳ鍵（ＩＤ Resolution Server鍵）」という）を用いてＲＦＩＤを暗号化する。ＩＤＲＳ鍵には、ＲＦＩＤタグ１０がＩＤ解決サーバ３０と共有している共有鍵、又は、ＩＤ解決サーバ３０の公開鍵がある。ＩＤＲＳ鍵は、ＩＤ解決サーバ３０により発行される。暗号化部１２は、ＩＤＲＳ鍵を記憶しておく。具体的には、暗号化部１２は、図２（ａ）に示すように、乱数又は乱数に相当する文字列と、ＲＦＩＤを含む平文を、Ｉ

ＤＲＳ鍵を用いて暗号化する。このようにして、暗号化部１２は、暗号化された発信装置識別子として、暗号化ＲＦＩＤ１を生成し、通信部１１に入力する。

【００２１】

このように、暗号化部１２は、乱数又は乱数に相当する文字列をＲＦＩＤに付加して暗号化することにより、暗号化ＲＦＩＤを暗号化する度に変化させることができる。暗号化部１２は、ＲＦＩＤを暗号化して得られる文字列がランダムに見えるように、ある程度の間隔において暗号化ＲＦＩＤが変化するように暗号化し、ランダムな暗号化ＲＦＩＤを生成する。

【００２２】

通信部１１は、暗号化された発信装置識別子として、暗号化ＲＦＩＤ１をＲＦＩＤリーダ２０に送信する。通信部１１は、暗号化部１２から暗号化ＲＦＩＤ１を取得する。通信部１１は、ＲＦＩＤリーダ２０からＩＤ要求を受信し、そのＩＤ要求に応じて暗号化ＲＦＩＤ１を送信してもよく、定期的に暗号化ＲＦＩＤ１を送信してもよい。このように、ＲＦＩＤタグ１０は、ＲＦＩＤリーダ２０が解読できない状態でＲＦＩＤをＲＦＩＤリーダ２０に送信する。尚、通信部１１は、赤外線や電波等の無線によりＲＦＩＤリーダ２０と送受信を行うことができる。

【００２３】

ＲＦＩＤリーダ２０は、通信部２１と、暗号化部２２と、リーダ情報記憶部２３と、クロック２４とを備える。リーダ情報記憶部２３は、ＲＦＩＤリーダ２０に関するリーダ情報を記憶する。リーダ情報には、ＲＦＩＤリーダ２０のユーザＩＤやパスワード等がある。ユーザＩＤは、受信装置識別子であり、ＲＦＩＤリーダ２０を一意に特定可能な情報である。パスワードは、ＲＦＩＤリーダ２０の認証に用いられる認証情報である。

【００２４】

暗号化部２２は、受信装置識別子としてユーザＩＤを暗号化する。暗号化部２２は、リーダ情報記憶部２３からユーザＩＤ及びパスワードを取得する。又、暗号化部２２は、クロック２４から現在時刻をタイムスタンプとして取得する。暗号化部２２は、データベースサーバ４０の暗号鍵（以下、「ＤＢ鍵（DataBase server鍵）」を用いてユーザＩＤ及びパスワードを暗号化する。ＤＢ鍵には、ＲＦＩＤリーダ２０がデータベースサーバ４０と共有している共有鍵、又は、データベースサーバ４０の公開鍵がある。各データベースサーバのＤＢ鍵は、各データベースサーバ４０によりそれぞれ発行される。

【００２５】

暗号化部２２は、ＲＦＩＤリーダ２０が信頼し、ＲＦＩＤリーダ２０のユーザＩＤを開示してもよいデータベースサーバ４０のＤＢ鍵を記憶しておく。具体的には、暗号化部２２は、図２（ｂ）に示すように、乱数又は乱数に相当する文字列と、ユーザＩＤと、パスワードと、タイムスタンプを含む平文を、ＤＢ鍵を用いて暗号化する。このようにして、暗号化部２２は、暗号化された受信装置識別子及び認証情報として、暗号化ユーザＩＤ２ｃを生成し、通信部２１に入力する。

【００２６】

このように、暗号化部２２は、タイムスタンプのように変化する値をユーザＩＤに付加して暗号化することにより、暗号化ユーザＩＤを暗号化する度に変化させることができる。暗号化部２２は、ユーザＩＤを暗号化して得られる文字列がランダムに見えるように、ある程度の間隔において暗号化ユーザＩＤが変化するように暗号化し、ランダムな暗号化ユーザＩＤを生成する。

【００２７】

通信部２１は、暗号化された発信装置識別子として、暗号化ＲＦＩＤ１をＲＦＩＤタグ１０から受信する。通信部２１は、ＲＦＩＤタグ１０にＩＤ要求を送信し、そのＩＤ要求に応じて送信される暗号化ＲＦＩＤ１を受信してもよく、ＲＦＩＤタグ１０から定期的に送信される暗号化ＲＦＩＤ１を受信してもよい。通信部２１は、暗号化された発信装置識別子及び暗号化された受信装置識別子として、暗号化ＲＦＩＤ１及び暗号化ユーザＩＤ２ｃを、ＩＤ解決サーバ３０に送信する。

【００２８】
通信部２１は、暗号化部２２から暗号化ユーザＩＤ２ｃを取得する。通信部２１は、暗号化部２２から取得した暗号化ユーザＩＤ２ｃに、ＲＦＩＤタグ１０から受信した暗号化ＲＦＩＤ１と、ヘッダ２ａとを付加し、判断情報２を生成する。ヘッダ２ａには、ＩＤ解決サーバ３０のアドレスが設定される。このように、ＲＦＩＤリーダ２０は、ＲＦＩＤリーダ２０が信頼し、ＲＦＩＤリーダ２０のユーザＩＤを開示してもよいと判断したデータベースサーバ４０以外には解読できない状態でユーザＩＤをＩＤ解決サーバ３０に送信する。
【００２９】
又、通信部２１は、ＩＤ解決サーバ３０から、データベースサーバ４０からの発信装置情報として、ＲＦＩＤタグ１０に関するタグ情報を受信する。このように、通信部２１は、ＩＤ解決サーバ３０を介してデータベースサーバ４０からのタグ情報を受信する。尚、通信部２１は、ＲＦＩＤリーダ１０とは、赤外線や電波等の無線により送受信を行うことができる。通信部２１は、ＩＤ解決サーバ３０とは、移動通信網やインターネット等のネットワークを介して送受信を行うことができる。
【００３０】
ＩＤ解決サーバ３０は、通信部３１と、復号部３２と、要求部３３と、サーバ情報記憶部３４とを備える。通信部３１は、受信装置から、受信装置識別子及び暗号化された発信装置識別子を受信する受信手段である。通信部３１は、暗号化された受信装置識別子を受信することが好ましい。具体的には、通信部３１は、ＲＦＩＤリーダ２０から、暗号化された受信装置識別子として暗号化ユーザＩＤ２ｃを、暗号化された発信装置識別子として暗号化ＲＦＩＤ１を含む判断情報２を受信する。通信部３１は、受信した判断情報２を復号部３２に入力する。
【００３１】
更に、通信部３１は、情報提供装置から発信装置情報を受信し、受信装置に送信する転送手段としても機能する。通信部３１は、データベースサーバ４０から、発信装置情報としてタグ情報を受信する。通信部３１は、受信したタグ情報をＲＦＩＤリーダ２０に送信する。尚、通信部３１は、ＲＦＩＤリーダ２０、データベースサーバ４０と、移動通信網やインターネット等のネットワークを介して送受信を行うことができる。
【００３２】
復号部３２は、暗号化された発信装置識別子を復号する復号手段である。復号部３２は、通信部３１から判断情報２を取得する。復号部３２は、判断情報２に含まれる暗号化ＲＦＩＤ１を復号する。具体的には、復号部３２は、ＲＦＩＤの暗号化に用いたＩＤＲＳ鍵が共有鍵の場合にはＩＤＲＳ鍵を復号鍵として用い、ＩＤＲＳ鍵が公開鍵の場合にはその公開鍵に対する復号鍵を用いて、暗号化ＲＦＩＤ１を復号する。復号部３２は復号鍵を記憶しておく。復号部３２は、復号結果として、復号したＲＦＩＤ又は復号に失敗した旨の通知を要求部３３に入力する。このとき、復号部３２は、復号結果と共に、判断情報２に含まれる暗号化ユーザＩＤ２ｃを要求部３３に入力する。
【００３３】
サーバ情報記憶部３４は、複数のデータベースサーバ４０に関するサーバ情報を記憶する。サーバ情報記憶部３４は、サーバ情報として、各データベースサーバ４０のアドレスと、各データベースサーバ４０が提供するタグ情報がどのＲＦＩＤタグ１０に関するタグ情報であるかを示すＲＦＩＤとを対応付けて記憶する。１つのデータベースサーバ４０が複数のＲＦＩＤタグ１０に関する情報を提供できるため、データベースサーバ４０のアドレスには複数のＲＦＩＤが対応付けられる。
【００３４】
要求部３３は、復号部３２による復号結果に基づいて、発信装置情報を提供する情報提供装置を判断し、発信装置情報を情報提供装置に要求する要求手段である。要求部３３は、復号部３２から復号結果として、暗号化ＲＦＩＤ１を復号して得られたＲＦＩＤ又は復号に失敗した旨の通知を取得する。要求部３３は、取得したＲＦＩＤに基づいてサーバ情

報記憶部３４を検索し、そのＲＦＩＤを持つＲＦＩＤタグ１０に関するタグ情報を提供するデータベースサーバ４０を判断し、特定する。要求部３３は、特定したデータベースサーバ４０のアドレスをサーバ情報記憶部３４から取得する。

【００３５】

要求部３３は、特定したデータベースサーバ４０にタグ情報を要求する情報要求を生成する。情報要求には、復号により得られたＲＦＩＤと、復号部３２から復号結果と共に取得した暗号化ユーザＩＤ２ｃが含まれる。要求部３３は、通信部３１を介して、特定したデータベースサーバ４０のアドレスに、生成した情報要求を送信する。このように、要求部３３は、暗号化された受信装置識別子を情報提供装置に送信して発信装置情報を要求する。要求部３３は、復号に失敗した場合には、データベースサーバ４０を特定できないため、処理を終了する。以上説明したように、ＩＤ解決サーバ３０は、暗号化ＲＦＩＤ１のみを復号し、データベースサーバ４０にアクセスを行うプロキシサーバとして機能する。

【００３６】

データベースサーバ４０は、通信部４１と、復号部４２と、提供部４３と、タグ情報記憶部４４とを備える。通信部４１は、ＩＤ解決サーバ３０から情報要求を受信する。通信部４１は、受信した情報要求を復号部４２に入力する。又、通信部４１は、ＩＤ解決サーバ３０にタグ情報を送信する。通信部４１は、提供部４３からタグ情報を取得する。尚、通信部４１は、ＩＤ解決サーバ３０と、移動通信網やインターネット等のネットワークを介して送受信を行うことができる。

【００３７】

復号部４２は、暗号化された受信装置識別子を復号する。復号部４２は、通信部４１から情報要求を取得する。復号部４２は、情報要求に含まれる暗号化ユーザＩＤ２ｃを復号する。具体的には、復号部４２は、ユーザＩＤ及びパスワードの暗号化に用いたＤＢ鍵が共有鍵の場合にはＤＢ鍵を復号鍵として用い、ＤＢ鍵が公開鍵の場合にはその公開鍵に対する復号鍵を用いて、暗号化ユーザＩＤ２ｃを復号する。復号部４２は、ＤＢ鍵の復号鍵を記憶しておく。復号部４２は、復号結果として、暗号化ユーザＩＤ２ｃを復号して得られたユーザＩＤ及びパスワード、又は、復号に失敗した旨の通知を提供部４３に入力する。

【００３８】

タグ情報記憶部４４は、ＲＦＩＤタグ１０に関するタグ情報を記憶する。タグ情報には、ＲＦＩＤタグ１０に関するＲＦＩＤ以外の付加的な情報がある。例えば、タグ情報には、ＲＦＩＤタグ１０の位置情報、ＲＦＩＤタグ１０が付加されている物体に関する情報、ＲＦＩＤタグ１０の周辺環境の情報等がある。タグ情報記憶部４４は、タグ情報を、特定のＲＦＩＤリーダ２０にだけ提供を制限した制限情報と、全てのＲＦＩＤリーダに提供可能な公開情報の２種類に区別して記憶してもよい。制限情報を提供する特定のＲＦＩＤリーダ２０としては、例えば、データベースサーバ４０にユーザＩＤを開示するＲＦＩＤリーダや、データベースサーバ４０が信頼できるＲＦＩＤリーダとして、予めデータベースサーバ４０がそのユーザＩＤとパスワードを記憶したり、データベースサーバ４０との共有鍵を提供したりしているＲＦＩＤリーダ等がある。以下、タグ情報のうち、制限情報だけや公開情報だけを指すときには特に「制限情報」、「公開情報」といい、タグ情報全体を指すときは、「タグ情報」という。

【００３９】

提供部４３は、中継装置の要求に応じて発信装置情報を中継装置に提供する。提供部４３は、復号結果に応じて発信装置情報を中継装置に提供することが好ましい。提供部４３は、復号部４２から復号結果を取得する。提供部４３は、タグ情報が制限情報と公開情報に区別されている場合には、復号結果に応じて制限情報又は公開情報のいずれを提供するかを決定できる。又、提供部４３は、タグ情報が制限情報と公開情報に区別されていない場合には、復号結果に応じてタグ情報を提供するか一切提供しないかを決定できる。

【００４０】

復号結果が復号により得られたユーザＩＤ及びパスワードのとき、提供部４３は、制限

情報の提供が許可されているＲＦＩＤリーダのユーザＩＤ及びパスワードを記憶している場合は、復号により得られたユーザＩＤ及びパスワードを持つＲＦＩＤリーダが、制限情報の提供を許可されているか否かを、記憶している情報を参照して認証する。又、タグ情報の提供が許可されているＲＦＩＤリーダのユーザＩＤを記憶している場合は、復号により得られたユーザＩＤ及びパスワードを持つＲＦＩＤリーダがタグ情報の提供を許可されているか否かを、記憶している情報参照して認証する。そして、提供部４３は、認証結果に応じて、制限情報又は公開情報のいずれを提供するか、あるいは、タグ情報を提供するか一切提供しないかを決定できる。又、復号結果が復号により得られたユーザＩＤのとき、提供部４３は、データベースサーバ４０にユーザＩＤを開示するＲＦＩＤリーダと判断し、制限情報又はタグ情報を提供すると決定できる。

【００４１】

又、復号結果が復号に失敗した旨の通知の場合には、提供部４３は、データベースサーバ４０にユーザＩＤを秘匿化するＲＦＩＤリーダと判断し、公開情報のみを提供するか、タグ情報を一切提供しないことを決定できる。更に、提供部４３は、タグ情報の提供が許可されているユーザＩＤを記憶せずに、提供を許可するＲＦＩＤリーダにだけＤＢ鍵としてデータベースサーバ４０との共有鍵を提供するようにしてもよい。この場合、提供部４３は、復号結果がユーザＩＤの場合には、提供可能なＲＦＩＤリーダであることを認証できる。よって、提供部４３は、復号結果がユーザＩＤの場合には、制限情報又はタグ情報を提供することを決定できる。

【００４２】

そして、提供部４３は、復号結果に基づく決定に応じて、タグ情報記憶部４４から該当するタグ情報を取得する。提供部４３は、通信部４１を介してＩＤ解決サーバ３０にタグ情報を送信する。提供部４３は、タグ情報を提供しない場合には、提供の拒否をＩＤ解決サーバ３０に通知してもよい。又、公開情報を提供すると決定したときに、公開情報が存在しない場合には、提供部４３は、現在公開情報が存在しないことを通知してもよい。以上のようにして、データベースサーバ４０は、ＩＤ解決サーバ３０の要求に応じてタグ情報ＩＤ解決サーバ３０に送信する。

【００４３】

尚、情報提供システム１００において、例えば、ＲＦＩＤタグ１０は、個人が設け、管理することができる。ＲＦＩＤリーダ２０は、個人が所有し、管理することができる。データベースサーバ４０は、個人やグループが設け、管理することができる。ＩＤ解決サーバ３０は、信頼できる第三者機関が設け、管理することができる。又、情報提供システム１００では、複数のデータベースサーバ４０が分散配置される。更に、ＲＦＩＤタグ１０とＩＤ解決サーバ３０との間の暗号化、復号には、公開鍵を用いることがスケーラビリティの観点から好ましい。

【００４４】

（情報提供方法）

図１に示す情報提供システム１００を用いた情報提供方法の手順を図３を用いて説明する。ＲＦＩＤリーダ２０が、ＲＦＩＤタグ１０にＩＤ要求を送信する（Ｓ１０１）。ＲＦＩＤタグ１０は、自身のＲＦＩＤをＩＤＲＳ鍵により暗号化し、暗号化ＲＦＩＤ１をＲＦＩＤリーダ２０に送信する（Ｓ１０２）。

【００４５】

ＲＦＩＤリーダ２０は、暗号化ＲＦＩＤ１をＲＦＩＤタグ１０から受信する。ＲＦＩＤリーダ２０は、ユーザＩＤ及びパスワードをＤＢ鍵により暗号化する。ＲＦＩＤリーダ２０は、暗号化ユーザＩＤ２ｃを受信した暗号化ＲＦＩＤ１と共に、判断情報２としてＩＤ解決サーバ３０に送信する（Ｓ１０３）。

【００４６】

ＩＤ解決サーバ３０は、判断情報２をＲＦＩＤリーダ２０から受信し、判断情報２に含まれる暗号化ＲＦＩＤ１を復号する。ＩＤ解決サーバ３０は、復号により得られたＲＦＩＤに基づいて、そのＲＦＩＤを持つＲＦＩＤタグ１０のタグ情報を提供するデータベース

サーバ４０を特定する（Ｓ１０４）。ＩＤ解決サーバ３０は、復号したＲＦＩＤと、暗号化ユーザＩＤ２ｃを含む情報要求を、特定したデータベースサーバ４０に送信し、タグ情報を要求する（Ｓ１０５）。

【００４７】

データベースサーバ４０は、情報要求に含まれる暗号化ユーザＩＤ２ｃの復号を試みる（Ｓ１０６）。データベースサーバ４０は、復号結果を用いてＲＦＩＤリーダを認証する（Ｓ１０７）。具体的には、データベースサーバ４０は、復号によりユーザＩＤ及びパスワードが得られた場合には、そのユーザＩＤ及びパスワードを持つＲＦＩＤリーダが、制限情報の提供、あるいは、タグ情報の提供を許可されているか否かを、記憶しているユーザＩＤ及びパスワードを参照して認証する。又、データベースサーバ４０は、提供を許可するＲＦＩＤリーダにだけＤＢ鍵としてデータベースサーバ４０との共有鍵を提供している場合には、復号に成功したか否かにより、提供可能なＲＦＩＤリーダか否かを認証する。あるいは、データベースサーバ４０は、復号に成功した場合には、データベースサーバ４０にユーザＩＤを開示するＲＦＩＤリーダであると判断し、制限情報又はタグ情報の提供を許可し、復号に失敗した場合には、データベースサーバ４０にユーザＩＤを秘匿化するＲＦＩＤリーダと判断し、公開情報のみを提供するか、タグ情報を提供しないことを決定してもよい。このようにして、データベースサーバ４０は、ＲＦＩＤリーダ２０がデータベースサーバ４０にとって信頼できるか否かを確認する。

【００４８】

ステップ（Ｓ１０７）において、認証に成功した場合等、制限情報やタグ情報をＲＦＩＤリーダ２０に提供することを決定した場合には、データベースサーバ４０は、制限情報、又は、タグ情報をＩＤ解決サーバ３０に送信する（Ｓ１０８）。一方、ステップ（Ｓ１０７）において、認証に失敗した場合等、公開情報のみを提供することや、タグ情報を一切提供しないことを決定した場合には、データベースサーバ４０は、公開情報、又は、提供の拒否や公開情報が存在しないことの通知をＩＤ解決サーバ３０に送信する（Ｓ１０９）そして、ＩＤ解決サーバ３０は、データベースサーバ４０から受信したタグ情報、公開情報、制限情報、通知をＲＦＩＤリーダ２０に送信し、転送する（Ｓ１１０）。

【００４９】

（効果）

このような情報提供システム１００、ＲＦＩＤタグ１０、ＲＦＩＤリーダ２０、ＩＤ解決サーバ３０、データベースサーバ４０及び情報提供方法によれば、ＲＦＩＤを暗号化した場合であっても、ＩＤ解決サーバ３０は、暗号化ＲＦＩＤ１を復号し、ＲＦＩＤリーダ２０が希望するタグ情報を提供するデータベースサーバ４０を判断できる。そして、ＩＤ解決サーバ３０は、データベースサーバ４とＲＦＩＤリーダ２０との間でタグ情報を中継できる。よって、ＲＦＩＤリーダ２０に対して、ＲＦＩＤ及びデータベースサーバ４０に関するサーバ情報を秘匿化することが可能となる。従って、ＲＦＩＤタグ１０と、ＲＦＩＤリーダ２０と、データベースサーバ４０とが関与する情報提供の過程において、安全な情報提供を容易に実現することができる。又、データベースサーバ４０がどのＲＦＩＤタグ１０に関するタグ情報を提供するかを、ＲＦＩＤリーダ２０によって特定されない状態で分散配置することができる。

【００５０】

更に、ＲＦＩＤリーダ２０は、ＤＢ鍵を用いてユーザＩＤを暗号化し、暗号化ユーザＩＤ２ｃをＩＤ解決サーバ３０に送信する。この場合、ＩＤ解決サーバ３０が、暗号化ユーザＩＤ２ｃをデータベースサーバ４０に送信してタグ情報を要求する。そして、データベースサーバ４０は、暗号化ユーザＩＤ２ｃを復号し、その復号結果に応じてタグ情報をＩＤ解決サーバ３０に送信する。

【００５１】

これによれば、ＲＦＩＤリーダ２０に関する情報を知ることができるデータベースサーバ４０を、暗号化ユーザＩＤ２ｃを復号可能な、ＲＦＩＤリーダ２０が暗号化に用いたＤＢ鍵の復号鍵を持つデータベースサーバ４０に限定できる。よって、ＲＦＩＤリーダ２０

は、ユーザＩＤを知られたくないデータベースサーバ４０に対してユーザＩＤを秘匿化できる。

【００５２】

即ち、ＲＦＩＤリーダ２０が信頼できるデータベースサーバ４０に限ってユーザＩＤを公開し、意図しない相手に公開されないようにできる。ＲＦＩＤリーダ２０は、ＩＤ解決サーバ３０を介してデータベースサーバ４０とやりとりし、サーバ情報を把握できない。そのため、ユーザＩＤのような身元判断に利用できる情報を任意のデータベースサーバ４０に公開することを避けるこのような仕組みは、安全な情報提供において有用である。又、これにより、図５に示したようなＲＦＩＤと、ユーザＩＤと、タグ情報の対応付けは、ＲＦＩＤリーダ２０がユーザＩＤを開示してもよいと判断した信頼できるデータベースサーバ４０に限って可能となる。そのため。ＲＦＩＤリーダ２０のユーザが情報を秘匿化したいデータベースサーバによる対応付けを防止することができる。

【００５３】

更に、データベースサーバ４０は、復号結果に応じて、即ち、ＲＦＩＤリーダ２０がデータベースサーバ４０に対してユーザＩＤを秘匿化するか開示するかに応じて、送信するタグ情報を制御することができる。即ち、データベースサーバ４０は、復号結果に応じて、タグ情報のＲＦＩＤリーダ２０に対する開示、非開示を制御することができ、タグ情報に対するアクセスコントロールができる。よって、データベースサーバ４０が、ＲＦＩＤリーダ２０からの問い合わせによりタグ情報を提供してしまい、タグ情報を知られたくない相手にタグ情報が知られてしまうことを回避できる。

【００５４】

又、ＲＦＩＤタグに関与するユーザの追跡には（１）ユーザに関与するＲＦＩＤと、（２）追跡者が設置するＲＦＩＤリーダの識別子と、（３）追跡されるユーザと、ＲＦＩＤと、ＲＦＩＤリーダの識別子と、それらの位置情報等の物理情報との対応情報が必要となる。情報提供システム１００では、このうち、追跡されるユーザが操作可能な（１）ＲＦＩＤを暗号化し、秘匿化できる。ＲＦＩＤリーダに関与するユーザの追跡には、（ａ）追跡されるユーザのＲＦＩＤリーダの識別子（ユーザＩＤ）と、（ｂ）追跡者が設置するＲＦＩＤタグのＲＦＩＤと、（ｃ）追跡されるユーザと、ＲＦＩＤリーダのユーザＩＤと、ＲＦＩＤと、それらの位置情報等の物理情報との対応情報が必要となる。情報提供システム１００では、このうち、追跡されるユーザが操作可能な（ａ）ＲＦＩＤリーダの識別子（ユーザＩＤ）を暗号化し、秘匿化できる。

【００５５】

そのため、情報提供システム１００では、ＲＦＩＤタグ１０のＲＦＩＤやＲＦＩＤリーダ２０のユーザＩＤと、ユーザとを関連付けを困難にできる。即ち、情報提供システム１００では、ＲＦＩＤの秘匿化によりＲＦＩＤを用いたユーザ追跡の危険性を低減でき、ＲＦＩＤリーダ２０のユーザＩＤの秘匿化によりユーザＩＤを用いたユーザ追跡の危険性を低減できる。又、意図しないＲＦＩＤタグ１０やＲＦＩＤリーダ２０に、ＲＦＩＤやユーザＩＤが知られないようにでき、ＲＦＩＤ１０とＲＦＩＤリーダ２０との間で適切に情報交換ができる。更に、ＲＦＩＤリーダ２０の識別子としてユーザＩＤをデータベースサーバ４０に送信する過程においても、ユーザＩＤは秘匿化されており、ユーザ追跡の危険性を低減できる。

【００５６】

特に、ＲＦＩＤタグ１０は、乱数又は乱数に相当する文字列を用い、暗号化ＲＦＩＤを暗号化する度に変化させる。又、ＲＦＩＤリーダ２０は、タイムスタンプを用い、暗号化ユーザＩＤを暗号化する度に変化させる。そのため、ＲＦＩＤやユーザＩＤの特定をより困難できる。その結果、安全性をより高めることができ、追跡をより困難することができる。

【００５７】

このような情報提供システム１００及び情報提供方法は、ＲＦＩＤタグ１０、ＲＦＩＤリーダ２０、データベースサーバ４０を広く個人で利用する場合に、様々な情報を個人と

結びつけて個人の追跡が行われる危険性を低減するために、特に有用である。尚、本発明は上記実施形態に限定されず、種々の変更が可能である。

【図面の簡単な説明】

【００５８】

【図１】本発明の実施形態に係る情報提供システムの構成を示すブロック図である。

【図２】本発明の実施形態に係る暗号化ＲＦＩＤ及び判断情報を示す図である。

【図３】本発明の実施形態に係る情報提供方法の手順を示すフロー図である。

【図４】従来方法の課題を説明する図である。

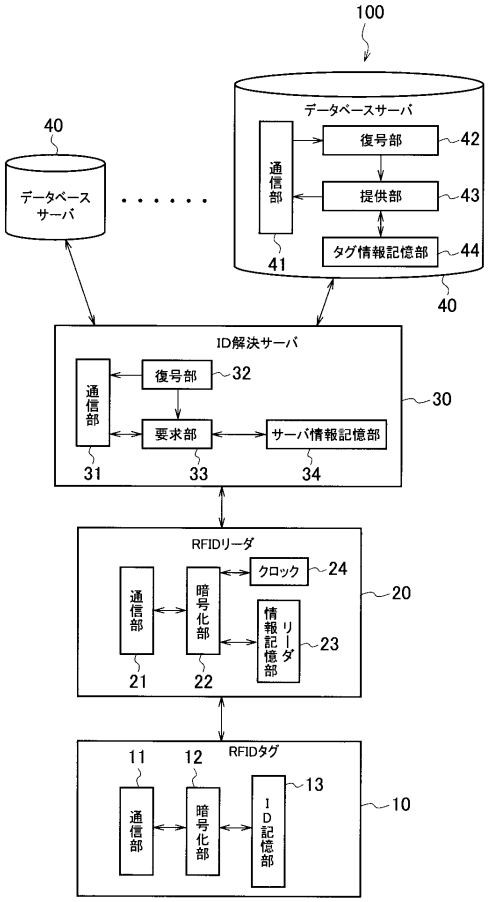
【図５】従来方法の課題を説明する図である。

【符号の説明】

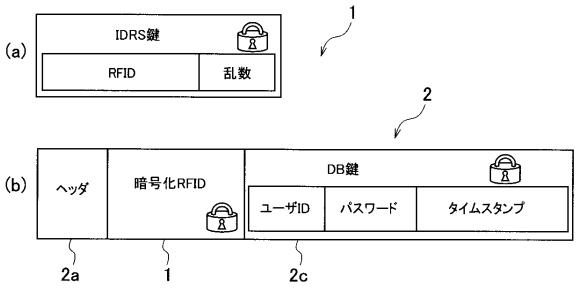
【００５９】

１０，２１０ａ，２１０ｂ　ＲＦＩＤタグ
１１，２１，３１，４１　通信部
１２，２２　暗号化部
１３　ＩＤ記憶部
２０，２２０，２２０ａ，２２０ｂ　ＲＦＩＤリーダ
２３　リーダ情報記憶部
２４　クロック
３０　ＩＤ解決サーバ
３２，４２　復号部
３３　要求部
３４　サーバ情報記憶部
４０，２４０　データベースサーバ
４３　提供部
４４　タグ情報記憶部
１００　情報提供システム
２５０ａ，２５０ｂ　ユーザ

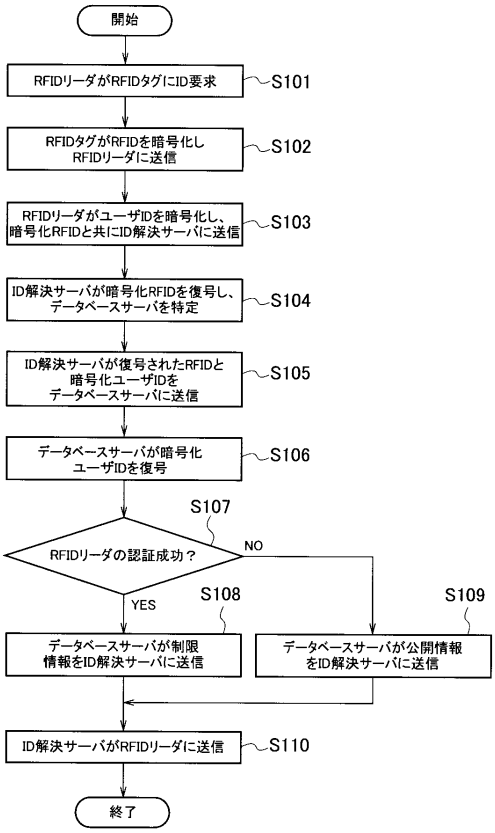
【図１】


100
データベースサーバ
通信部
復号部
提供部
タグ情報記憶部
42
43
44
41
40
40
データベースサーバ
ID解決サーバ
通信部
復号部
要求部
サーバ情報記憶部
32
30
31
33
34
RFIDリーダ
通信部
暗号化部
クロック
情報記憶部
リーダ
24
20
23
21
22
RFIDタグ
11
12
13
10
通信部
暗号化部
ID記憶部

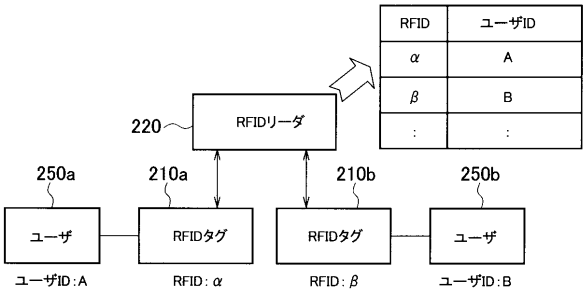
【図２】


(a)
IDRS鍵
RFID
乱数
1
2
(b)
ヘッダ
暗号化RFID
DB鍵
ユーザID
パスワード
タイムスタンプ
2a
1
2c

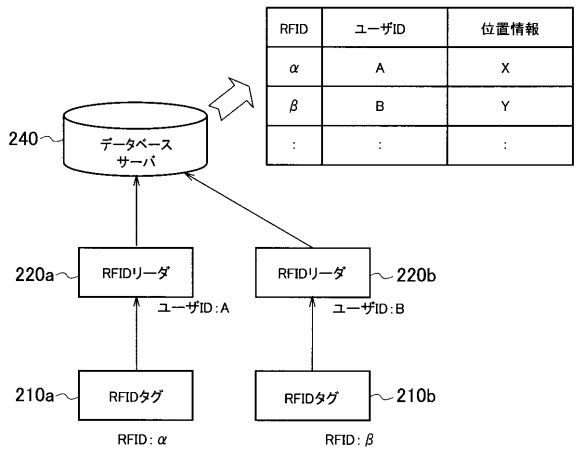
【図３】


開始
RFIDリーダがRFIDタグにID要求
S101
RFIDタグがRFIDを暗号化し
RFIDリーダに送信
S102
RFIDリーダがユーザIDを暗号化し、
暗号化RFIDと共にID解決サーバに送信
S103
ID解決サーバが暗号化RFIDを復号し、
データベースサーバを特定
S104
ID解決サーバが復号されたRFIDと
暗号化ユーザIDを
データベースサーバに送信
S105
データベースサーバが暗号化
ユーザIDを復号
S106
S107
RFIDリーダの認証成功？
NO
YES
S108
S109
データベースサーバが制限
情報をID解決サーバに送信
データベースサーバが公開情報
をID解決サーバに送信
ID解決サーバがRFIDリーダに送信
S110
終了

【図４】


RFID
ユーザID
α
A
β
B
:
:
220
RFIDリーダ
250a
210a
210b
250b
ユーザ
RFIDタグ
RFIDタグ
ユーザ
ユーザID:A
RFID:α
RFID:β
ユーザID:B

【図５】


RFID
ユーザID
位置情報
α
A
X
β
B
Y
:
:
:
240
データベース
サーバ
220a
RFIDリーダ
ユーザID：A
RFIDリーダ
220b
ユーザID：B
210a
RFIDタグ
RFID：α
RFIDタグ
210b
RFID：β

フロントページの続き

(72)発明者　杉山　俊春
東京都千代田区永田町二丁目１１番１号　株式会社エヌ・ティ・ティ・ドコモ内
(72)発明者　萩野　浩明
東京都千代田区永田町二丁目１１番１号　株式会社エヌ・ティ・ティ・ドコモ内
(72)発明者　山崎　憲一
東京都千代田区永田町二丁目１１番１号　株式会社エヌ・ティ・ティ・ドコモ内

Ｆターム(参考) 5B058 CA17　KA35　YA20
5J104 AA07　KA02　NA36　NA38　PA07