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

特許第4897704号
(P4897704)

(45)発行日　平成24年3月14日(2012.3.14)　(24)登録日　平成24年1月6日(2012.1.6)

(51)Int.Cl.		F I		
G06F 21/20	(2006.01)	G06F	15/00	330D
G06K 17/00	(2006.01)	G06K	17/00	L
G06K 19/07	(2006.01)	G06K	17/00	T
G06K 19/10	(2006.01)	G06K	19/00	H
G06F 21/24	(2006.01)	G06K	19/00	R

請求項の数 20　(全 24 頁)　最終頁に続く

(21)出願番号　特願2007-548894 (P2007-548894)
(86)(22)出願日　平成17年12月23日 (2005.12.23)
(65)公表番号　特表2008-527484 (P2008-527484A)
(43)公表日　平成20年7月24日 (2008.7.24)
(86)国際出願番号　PCT/GB2005/005075
(87)国際公開番号　WO2006/070189
(87)国際公開日　平成18年7月6日 (2006.7.6)
審査請求日　平成20年12月22日 (2008.12.22)
(31)優先権主張番号　0428543.3
(32)優先日　平成16年12月31日 (2004.12.31)
(33)優先権主張国　英国 (GB)

(73)特許権者　390028587
ブリティッシュ・テレコミュニケーションズ・パブリック・リミテッド・カンパニー
ＢＲＩＴＩＳＨ　ＴＥＬＥＣＯＭＭＵＮＩＣＡＴＩＯＮＳ　ＰＵＢＬＩＣ　ＬＩＭＩＴＥＤ　ＣＯＭＰＡＮＹ
イギリス国，イーシー１エー・７エー　ジェイ，ロンドン，ニューゲート・ストリート　８１
(74)代理人　100091351
弁理士　河野　哲
(74)代理人　100088683
弁理士　中村　誠
(74)代理人　100108855
弁理士　蔵田　昌俊

最終頁に続く

(54)【発明の名称】データ交換の制御

(57)【特許請求の範囲】
【請求項１】
団体と、制御装置に関連付けられている商品識別装置との間のデータ交換を制御する制御装置であって、
前記団体のそれぞれは、前記制御装置が関連付けられている複数の商品識別装置の１以上とデータを交換するデータ交換手段と関連付けられており、
前記データ交換手段は、前記データ交換手段が関連付けられている前記団体を示す、あるいは前記データ交換手段が関連付けられている団体のカテゴリを示す認証データを提供するように構成されており、
１つ以上の団体又は団体のカテゴリのためのアクセス方針であって、団体又は団体のカテゴリが、前記制御装置が関連付けられている複数の商品識別装置の１つ以上とデータを交換できる範囲に関する前記アクセス方針を示すデータを記憶するアクセス方針記憶手段と、
データ交換手段から認証データを受信する通信受信手段と、
受信された認証データと前記記憶されているアクセス方針を示すデータとから、前記データ交換手段が関連付けられている前記団体又は団体のカテゴリに適用可能なアクセス方針を確立する認証手段と、
前記団体に対する前記適用可能なアクセス方針に従って、前記商品識別装置と、前記データ交換手段が関連付けられている前記団体との間でデータの交換を可能にするアクセスデータを前記データ交換手段に提供する通信提供手段と、

を備える制御装置。
【請求項２】
前記制御装置は、無線周波数信号を用いたデータを提供する、及び／又は受信するように構成されている、請求項１に記載の制御装置。
【請求項３】
前記制御装置はアクティブＲＦＩＤ装置である、請求項１又は請求項２に記載の制御装置。
【請求項４】
前記商品識別装置は無線周波数識別（ＲＦＩＤ）装置である、請求項１乃至請求項３のいずれか１項に記載の制御装置。
【請求項５】
前記商品識別装置はパッシブＲＦＩＤ装置又は準アクティブＲＦＩＤ装置である、請求項１乃至請求項４のいずれか１項に記載の制御装置。
【請求項６】
前記商品識別装置は、前記商品識別装置が関連付けられている１つ以上の商品に関係するデータを提供するように構成されている、請求項１乃至請求項５のいずれか１項に記載の制御装置。
【請求項７】
前記商品識別装置は商品識別データを提供するように構成されている、請求項６に記載の制御装置。
【請求項８】
前記商品識別装置は商品ステータスデータを提供するように構成されている、請求項６又は請求項７に記載の制御装置。
【請求項９】
前記データ交換手段はＲＦ読み取り装置である、請求項１乃至請求項８のいずれか１項に記載の制御装置。
【請求項１０】
前記データ交換手段はＲＦ書き込み装置である、請求項１乃至請求項８のいずれか１項に記載の制御装置。
【請求項１１】
前記データ交換手段はＲＦ読み取り／書き込み装置である、請求項１乃至請求項８のいずれか１項に記載の制御装置。
【請求項１２】
提供される前記アクセスデータは、商品識別装置により提供された符号化データの復号を可能にする、請求項１乃至請求項１１のいずれか１項に記載の制御装置。
【請求項１３】
提供される前記アクセスデータは、商品識別装置にデータを提供させることを可能にする、請求項１乃至請求項１２のいずれか１項に記載の制御装置。
【請求項１４】
提供される前記アクセスデータは、前記商品識別装置にデータを記憶させる、請求項１乃至請求項１３のいずれか１項に記載の制御装置。
【請求項１５】
商品識別装置と団体との間で交換される前記データは、複数の属性の１つ以上に関するデータを備える、請求項１乃至請求項１４のいずれか１項に記載の制御装置。
【請求項１６】
前記アクセス方針は、団体又は団体のカテゴリが、前記制御装置が関連付けられている商品識別装置とデータを交換できるかについての前記属性又は前記属性の組み合わせを示す、請求項１５に記載の制御装置。
【請求項１７】
前記アクセス方針は、団体又は団体のカテゴリが、前記１つ以上の属性に関するデータ

に関して読み取り、書き込み、又は読み書きのアクセスを許されるかどうかを示す、請求項１５に記載の制御装置。

【請求項１８】

前記アクセス方針は、団体又は団体のカテゴリが権利を委任することを許されるかどうかを示す、請求項１乃至請求項１７のいずれか１項に記載の制御装置。

【請求項１９】

団体と、制御装置に関連付けられている商品識別装置との間のデータ交換を制御する方法であって、

前記団体のそれぞれには、前記制御装置が関連付けられている複数の商品識別装置の1つ以上とデータを交換するデータ交換手段が関連付けられており、

前記データ交換手段は、前記データ交換手段が関連付けられている前記団体を示す、あるいは前記データ交換手段が関連付けられている前記団体のカテゴリを示す認証データを提供するように構成されており、

１つ以上の団体あるいは団体のカテゴリのためのアクセス方針であって、団体又は団体のカテゴリが、前記制御装置が関連付けられている複数の商品識別装置の１つ以上とデータを交換できる範囲に関する前記アクセス方針を示すデータを記憶するステップと、

データ交換手段から認証データを受信するステップと、

受信された認証データと前記記憶されているアクセス方針を示すデータとから、前記データ交換手段が関連付けられている前記団体又は該団体のカテゴリに適用可能なアクセス方針を確立するステップと、

前記団体に対して前記適用可能なアクセス方針に従って、前記商品識別装置と、前記データ交換手段が関連付けられている前記団体との間でデータの交換を可能にするアクセスデータを前記データ交換手段に提供するステップと、

を備える方法。

【請求項２０】

団体と商品識別装置との間のデータ交換を制御するシステムであって、

前記システムは、

複数の商品識別装置と関連付けられている制御装置と、

それぞれが１つ以上の団体又は団体のカテゴリと関連付けられている１つ以上のデータ交換手段と、

を備え、

前記データ交換手段又はデータ交換手段の各々は、

前記制御装置が関連付けられている複数の商品識別装置の1つ以上とデータを交換する手段と、

前記データ交換手段が関連付けられている団体を示す、あるいは前記データ交換手段が関連付けられている団体のカテゴリを示す認証データを提供する手段と、

を備え、

前記制御装置は、

１つ以上の団体あるいは団体のカテゴリに関するアクセス方針であって、団体又は団体のカテゴリが、前記制御装置が関連付けられている前記商品識別装置の1つ以上とデータを交換できる範囲に関する前記アクセス方針を示すデータを記憶するアクセス方針記憶手段と、

前記データ交換手段から認証データを受信する通信受信手段と、

受信された認証データと前記記憶されているアクセス方針を示すデータとから、前記データ交換手段が関連付けられている団体又は団体のカテゴリに適用可能なアクセス方針を確立する認証手段と、

前記団体に対して適用可能なアクセス方針に従って、前記商品識別装置と、前記データ交換手段が関連付けられている前記団体との間でデータの交換を可能にするアクセスデータを前記データ交換手段に提供する通信提供手段と、

を備えるシステム。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ＲＦＩＤタグ読み取り装置及び／又は書き込み装置等のデータ交換手段を介した商業組織等の団体と、ＲＦＩＤタグのような商品識別装置の間でのデータ交換の制御に関する。
【背景技術】
【０００２】
無線周波数識別（ＲＦＩＤ）は、現在、情報を処理する方法を根本的に変更し得る、実現可能性の高い技術として提示されている。ＲＦＩＤタグは主に、読み取り動作中に視認を必要とせず、識別プロセスを自動化するためにサプライチェーンで使用されている。アイデンティティ情報は多くの適用の領域で潜在的な利点を有するであろう。
【発明の開示】
【０００３】
通常、ＲＦＩＤタグは小さな記憶容量及びアンテナを備えた集積回路から成る。「アクティブタグ」と呼ばれる、内蔵電源を有するタグもあり、通常は処理回路網に電力を供給し、出力信号を生成させるために使用される。「パッシブタグ」と呼ばれる他のタグは、内蔵電源を有していない。パッシブタグは、一般的には、読み取り装置によって生成される電磁場から電力を収集することによって、入信信号に応答し、出力信号を発生させるために必要とされるエネルギーを取得する。また、「準アクティブ」（またあるいはときには「準パッシブ」）タグとして知られる、タグも存在し、一般的には、小さな電源を有し、タグの処理回路網が絶えず電力の供給を受けることができるようにする。したがって、これらのタグは任意の処理を開始する前に入信信号から電力を収集する必要はなく、通常これらのタグはパッシブタグよりも速い応答を提供できる。
【０００４】
ＲＦＩＤタグは、通常、商用製品のような、関連付けられた物理オブジェクトに関するアイデンティティ情報を保持する。読み取り装置によって照会されると、タグは通常、有効期限、製造場所、現在位置等のオブジェクトについての詳細な情報を記憶するバックエンドデータベース上の一意の位置を指すことができるアイデンティティ情報で応答する。この情報は、本来リアルタイムでユーザに利用可能とすることができる。
【０００５】
調査において、商用製品にタグを付けるためのＲＦＩＤ技術の展開に関連している最も重要な懸案事項の１つとして、プライバシーが繰り返し挙げられてきた。簡略には、オブジェクトにタグが付けられると、ＲＦＩＤ読み取り装置を持った誰もが該オブジェクト、該オブジェクトの所有者、又は該オブジェクトのユーザに関する情報を、該所有者又は該ユーザの許可なしに発見できる可能性がある。ＲＦＩＤタグを保持する個人は不正な追跡によって影響を受け、タグ情報は、個人情報を収集し、ユーザの好みを分析するために使用され得るであろう。同様に、ＲＦＩＤタグ付き製品を所有する企業はスパイ行為に対して弱くなるであろう。競合他社はタグＩＤを監視するだけで該企業の製品を追跡できるであろう。
【０００６】
すべてのＲＦＩＤタグは、範囲内の誰もが受信できる無線スペクトルを通して動作する。タグの現在の生成の多くはアクセス制御機能が欠け、したがって悪意のあるユーザを含む誰もがタグに記憶されている情報を読み取ることができる。タグに記憶されている静的な「一意識別子」は、タグが付けられているオブジェクトを該オブジェクトを所有している個人又は企業と関連付ける。ＲＦＩＤタグのプライバシー懸念の具体的な証拠は主に以下の問題点に関する。
【０００７】
－トレーサビリティ：一意の識別番号は、製品がある読み取り装置から別の読み取り装置に移動するにつれ、認証されていない読み取り装置が該製品を追跡することを可能にする

。
【０００８】
－情報漏洩：ＲＦＩＤタグは、タグが関連付けられている製品についての情報を伝える。悪意のある、隠れた読み取り装置が所有者の承認なしに製品情報を収集できるであろう（例えば、ユーザによって所有されるＲＦＩＤタグ付き製品は、このようにしてユーザの好みについての潜在的に貴重な情報を提供する）。
【０００９】
研究者及び産業活動家はＲＦＩＤプライバシー問題を軽減するための異なる手法を研究してきた。手法のほとんどは、何らかの追加の機能をタグに組み込み、読み取り装置－タグ通信プロトコルを変更し、あるいは暗号化装置又は特殊タグ等の新しいインフラストラクチャを追加することによりタグに負担をかける。理想的には、解決策は最小の費用で適切なプライバシーの保護を提供するべきである。
【００１０】
Ｊｕｅｌｓ及びＰａｐｐｕ［１］は、ＲＦＩＤが使用可能にされた紙幣のための方法を提案した。「ユーロ」紙幣の連続番号がＲＦＩＤタグによって伝えられ、暗号化方式によって保護されている。連続番号は計算装置による再暗号化を受け、これにより紙幣のトレーサビリティが難しくなる。この方式は単一の認証団体を必要とし、サプライチェーンのシナリオでよくあるような、複数ドメインシステムには合わない。
【００１１】
［１］Ａ．Ｊｕｅｌｓ及びＲ．Ｐａｐｐｕ。「密告するユーロ：ＲＦＩＤが使用可能にされた紙幣におけるプライバシー保護（Squealing Euros: Privacy-Protection in RFID-Enabled Banknotes）」。Ｒ．Ｗｒｉｔｅ編集の、金融暗号学（Financial Cryptography）２００３年、１０３から１２１ページ、Ｓｐｒｉｎｇｅｒ－Ｖｅｒｌａｇ。２００３年。ＬＮＣＳ第２７４２番。
【００１２】
Ｗｅｉｓ、Ｓａｒｍａ、Ｒｉｖｅｓｔ及びＥｎｇｅｌｓ［２］は、ＲＦＩＤシステムにおいてセキュリティを改善するための複数のセキュリティ機構を提案してきた。彼らは盗聴に基づいた攻撃の問題を特定し、タグから読み取り装置への通信の電力が読み取り装置からタグへの通信の電力よりはるかに弱いことを認識した。提案された方式には、タグ上でのハッシュ関数及び擬似乱数生成器の使用が含まれる。該システムは、バックエンドサーバで実行される逆ハッシュ関数探索に基づく。
【００１３】
これらの特性に起因して、該方式は大規模な小売業者にとっては実用的ではなく、比較的少数のタグの所有者にとってのみ有効であり得る。さらに、擬似乱数生成器は現在のＲＦＩＤタグ技術では実現できない。
【００１４】
［２］Ｓａｎｊａｙ Ｅ．Ｓａｒｍａ、Ｓｔｅｐｈｅｎ Ａ．Ｗｅｉｓ、及びＤａｎｉｅｌ Ｗ．Ｅｎｇｅｌｓ。「ＲＦＩＤシステム及びセキュリティとプライバシーの影響（RF ID Systems and Security and Privacy Implications）」。暗号ハードウェア及び埋め込みシステムに関するワークショップ（Workshop on Cryptographic Hardware and Embedded Systems）において、４５４から４７０ページ。コンピュータサイエンスの講義ノート、２００２年。
【００１５】
「必要最低限度の暗号学（minimalist cryptography）」［３ａ］の中で、Ｊｕｅｌｓは、タグが、異なる、事前にプログラミングされた仮名を含む方法を提案している。各読み取り動作の間に異なる匿名を開示することによって、追跡を回避することができる。認証された読み取り装置は、匿名を正しいＩＤに関連付けるデータベースにリンクされる必要がある。この方式の主要な弱点は、タグ内の匿名の集合を更新する必要性である。ＮＴＴ実験室（NTT laboratories）からのさらに複雑な手法［３ｂ］は、タグに含まれている秘密情報を自動的に更新するためにセキュアハッシュチェーン(secure hash chain)機能

を使用することを含む。この方式の背景にある論理的根拠は、タグが読み取り装置の照会に予想通りに応答してはならないという点である。タグは、２つのハッシュ（ＨとＧ）関数を使用することにより自立的にタグの識別子をリフレッシュし、読み取りのたびに異なる匿名を出力する。セキュアなデータベースは、タグ出力のシーケンスを生成するために使用される秘密値にアクセスできるため、該データベースは、タグ出力を製品情報にマッピングできる。明示された階層的な命名構造なしに匿名を正しいＩＤにリンクさせることが高価であるため、この解決策にはスケーラビリティの問題がある。

【００１６】

［３ａ］Ａ．Ｊｕｌｅｓ、「ＲＦＩＤタグのための必要最低限度の暗号学（Minimalist Cryptography for RFID Tags）」、Ｃ．Ｂｌｕｎｄｏ編集において、通信ネットワークのセキュリティ（Security of Communication Networks）（SCN）、２００４年

［３ｂ］Ｍｉｙａｋｏ　Ｏｈｋｕｂｏ、Ｋｏｕｔａｒｏｕ　Ｓｕｚｕｋｉ及びＳｈｉｎｇｏ　Ｋｉｎｏｓｈｉｔａ：２００３年１１月にＭＩＴで提示されたと考えられている「「プライバシーフレンドリ」なタグに対する暗号手法（Cryptographic Approach to “Privacy-Friendly" Tags）」。http://lasecwww.epfl.ch/~gavoine/download/papers/OhkuboSK-2003-mit-paper.pdfを参照せよ。

【００１７】

これらの方式はアクセス制御が欠如していることに対処するためにタグに何らかの追加の機能を組み込む。しかしながら、該方式の技術の想定は明らかに適用できるものではない。ＲＦＩＤタグ、特に広範に配置される可能性があるものは、リソースとアーキテクチャのさまざまな制約がある。

【００１８】

（１）「Ｊｕｅｌｓ及びＰａｐｐｕ」の提案は、信頼できるサードパーティ手法を必要とするが、これは非常に限られた状況でのみ有効であり得る。

【００１９】

（２）「Ｗｅｉｓら」の解決策は、現在のパッシブＲＦＩＤタグにおいて使用できるリソースの量が制限されていることにより、制限される。

【００２０】

（３）匿名解決策は、タグ上に追加のメモリを必要とする。

【００２１】

ＲＦＩＤタグが遭遇するプライバシーとセキュリティの問題に対する２つの代替手法は、ＲＦＩＤブロッカータグに関するＪｕｅｌｓ、Ｒｉｖｅｓｔ及びＳｚｙｄｌｏの研究［４］、及びソフトブロッキング手法に関するＪｕｅｌｓ及びＢｒａｉｎａｒｄの研究［５］に概略されている。該研究はともに、特定の潜在的なプライバシー問題を軽減できるプライバシー機能強化解決策を説明している。

【００２２】

「ブロッカータグ」は、ＲＦＩＤタグの大きな集合の存在をシミュレーションすることによって読み取り動作を妨害する破壊的な方式である。ブロッカータグは、「木探索（tree-walking）」方式又はＡＬＯＨＡ方式と相互作用する現在のタグ読み取り基準で実現されるシンギュレーション（singulation）プロセスに作用する。ブロッカータグは、ユーザがプライバシー保護のために持ち歩く特定目的装置であり、該装置は個人的な（private）タグが読み取られるのを防ぐ。この解決策の主要な欠点は読み取り動作が破壊されることである。この弱点は該解決策の実用性を傷つける。

【００２３】

［４］「ブロッカータグ：消費者のプライバシーのためのＲＦＩＤタグの選択的ブロッキング（The Blocker Tag:Selective Blocking of RFID Tags for Consumer Privacy）」。Ｖ．Ａｔｌｕｒｉ編集において、第８回コンピュータ及び通信セキュリティに関するＡＣＭ会議（8th ACM Conference on Computer and Communications Security）、１０３から１１１ページ。ＡＣＭ出版、２００３年。

【００２４】

「ソフトブロッカー」手法は、ＲＦＩＤタグのプライバシー優先度を読み取り装置に表明する単純な手法である。これは、読み取り装置にプライバシーエージェントを必要とし、またタグの分類を必要とする。例えば、プライベートと分類されるタグは、読み取り装置上のプライバシーエージェントにタグの値を開示させない。同じ状況で、ブロッカーと分類されたタグが読み取られると、プライバシーエージェントは秘密のタグデータをフィルタで除去する。この解決策の主要な優位点は、方針の実現に関する柔軟性である。異なるシナリオに対して新しいプライバシー方針が任意に作成できるであろう。主要な弱点は、読み取り装置で実現されるプライバシーエージェントがタグ分類を遵守することを検証する監査機構又は機能強化サービスが必要とされることである。

【００２５】

［５］Ａ．Ｊｕｅｌｓ及びＪ．Ｂｒａｉｎａｒｄ：「ソフトブロッキング：安価で柔軟なブロッカータグ（Soft Blocking:Flexible Blocker Tag on the Cheap）」。Ｓ．Ｄｅ Ｃａｐｉｔａｎｉ ｄｉ Ｖｉｍｅｒｃａｔｉ及びＰ．Ｓｙｖｅｒｓｏｎ、編集において、電子社会におけるプライバシーに関するワークショップ（Workshop on Privacy in the Electronic Society）（WPES）、２００４年

「監視（watchdog）」タグと呼ばれる別の手法がＦｌｏｅｒｋｅｍｅｉｅｒ、Ｓｃｈｎｅｉｄｅｒ及びＬａｎｇｈｅｉｎｒｉｃｈによって説明されている［６］。これは、読み取り装置とタグの間の通信を立ち聞きするアクティブタグである。監視タグは読み取り装置、読み取り動作の目的及び、おそらくは読み取り装置の位置に関する識別情報を記録できる。収集されたデータは、検査及び検証の目的のために最終的なユーザに使用されることができる。監視タグはプライバシー強化方法を提供しないが、読み取り装置－タグ間のやり取りの可視性を強化することができる。

【００２６】

［６］「目的のある走査－ＲＦＩＤプロトコルにおける公正な情報の原則のサポート（Scanning with a Purpose-Supporting the Fair Information Principles in RFID Protocols)」、Ｃｈｒｉｓｔｉａｎ Ｆｌｏｅｒｋｅｍｅｉｅｒ、Ｒｏｌａｎｄ Ｓｃｈｎｅｉｄｅｒ、Ｍａｒｃ Ｌａｎｇｈｅｉｎｒｉｃｈ、パーベイシブコンピューティング研究所(Institute for Pervasive Computing)ＥＴＨ、スイス、チューリッヒ（Zurich, Switzerland）

国際特許出願第２００４／０８６２９０号は、「認証装置」と呼ばれる装置を使用して、ＲＦＩＤシステム内のトランスポンダ等のトランスポンダを認証するための方法及びシステムに関する。電子「ウォーターマーク」がトランスポンダのために計算され、トランスポンダに書き込まれる。トランスポンダは、読み取られるときにウォーターマークとともにトランスポンダ自体のデータを提供する。別の装置は、無関係に正しいウォーターマークを計算する。トランスポンダを認証するために、認証装置が該２つを比較し、読み取り装置に知らせるか、あるいは読み取り装置自体が比較を行うかのどちらかである。

【００２７】

本発明によると、請求項１に述べられているような制御装置が提供される。

【００２８】

また、本発明によると、請求項２０に述べられているようなデータ交換を制御するための方法が提供される。

【００２９】

さらに本発明によると、請求項２１に述べられているようなデータ交換を制御するためのシステムが提供される。

【００３０】

本発明の実施形態によると、前述された従来のシステムの不利な点はなく、特にありとあらゆる商品識別装置に複雑さを付加する必要なく、必要なセキュリティとプライバシーの要件を維持することが可能である。本発明の好ましい実施形態による制御装置を有するシステムは柔軟であり、異なるＲＦＩＤタグ方式と互換性があるという優位点を有することができる。該システムは異なる領域間での製品の輸送（例えば、出荷）又は取引の間に

有効なプライバシー保護を提供することができ、秘密の読み取り及び製品スパイ行為を防ぐために大規模なサプライチェーンのシナリオに関して特に有効であり得る。

【００３１】

本発明の好ましい実施形態は、公知の種々のＲＦＩＤタグ等のＲＦＩＤ商品識別装置と関連して使用される制御装置に関するが、本発明のある実施形態による制御装置が他のタイプの商品識別装置と関連して使用され得ることは予測できる。

【００３２】

現在のＲＦＩＤタグの不利な点の１つは、有用なレベルの処理を実行できるアクティブタグのコストが、アクティブタグを大量の低コストの商品に個々に適用するには高すぎると考えられているのに対し、より安価で使用可能なパッシブＲＦＩＤタグは、所定の応答で特定の照会に応答する等の、はるかに基本的な機能しかを実行できないという点である。本発明の特に有利な実施形態によれば、商品識別装置は簡単で低コストのパッシブタグであってもよいが、本発明による制御装置の機能のため、セキュリティ、プライバシー等のレベルは、各商品識別装置が、あたかもより複雑なアクティブタグの機能を有するかのように制御可能且つ柔軟であることができる。

【００３３】

特定の好ましい実施形態に関連して、制御装置はＲＦＩＤタグ自体であってもよく、その場合、該タグは制御タグと呼ばれることができる。このような実施形態によれば、該タグが制御タグの必要な機能を実行できるため、該タグは一般的には、アクティブ、あるいは少なくとも準アクティブなタグとなるが、本発明がアクティブ又は準アクティブな制御装置に限定されることは意図されていない。

【００３４】

前述された従来の技術のシステムの多くの問題が、多くの場合プライバシーという言葉で表されるが、実際には制御の問題とみなすことができることに留意すべきである。

【００３５】

本発明による制御装置は、「ブロッカータグ(blocker tag)」によって使用される「オプトアウト(opt-out)」手法とは対照的に「オプトイン(opt-in)」手法を実現すると考えることができる。制御装置は、団体がパッシブタグのような大多数の商品識別装置に含まれている情報に対するアクセスを得るために有効にオプトインすることを可能にするアクセス制御を提供するものと考えられ得る。該制御装置は、アクセス制御機能を信頼できるサードパーティシステムから、制御装置に置き換えることを可能にし、該制御装置は、信頼できるサードパーティとは異なり、商品識別装置が関連付けられている商品とともに便利に（物理的に）移動することができる。

【００３６】

本発明の実施形態による制御装置の役割は、製品に付けられているパッシブタグのグループに記憶されているアイデンティティ情報と、バックエンドデータベースに記憶され得る該製品の実際のアイデンティティもしくは該アイデンティティに関係する他の情報との間のリンクをセキュアにするための方法を提供することであってもよい。タグアイデンティティ情報は、暗号化又は匿名等のセキュアな方式を通して保護され得る。制御装置は、最初に読み取り装置を認証してから、該読み取り装置にパッシブタグに含まれている情報にアクセスするために必要とされるプロトコル情報を与えてもよい。

【００３７】

タグ又は他のこのような商品識別装置は、「プライベート」又は「パブリック」として分類できると考えることができる。該分類によって、読み取り装置は、どのプライバシー方針が特定のタグに利用できるのかを判断できる。パブリックタグは、該パブリックタグが制御装置とやり取りすることを必要とせずに該パブリックタグ自体の情報を読み取り装置に送信してよい。プライベートタグは、暗号化されたフォーマットでアイデンティティ情報を送信してよい。読み取り装置は、暗号化された情報にアクセスできるようになる前に該制御装置によって読み取り装置自体が認証される必要があるであろう。

【００３８】

以下の２つのシナリオは、本発明の実施形態がどのようにして２つの例の状況、つまり「出荷環境」及び「消費者環境」に適用できるのかを図解するために役立つ。

【００３９】

出荷環境

配置例として、「Ａ」社から「Ｂ」社に出荷されている１００個の製品を有するパレットを考えてもよい。それぞれの製品にはＲＦＩＤタグでタグが付けられている。「Ａ」社はパレット上に含まれたすべてのタグをプライベートと分類するであろう。プライベートタグは認証された読み取り装置にだけ情報を開示するであろうことを念頭に置かなければならない。本発明の実施形態による制御装置は、物理的にパレットの上に取り付けられている。制御装置の主要な役割は、認証された読み取り装置がタグ上の情報にアクセスできるようにすることである。

【００４０】

Ａ社は、制御装置をプログラミングする。Ａ社は「Ｂ」社の証明書、及び製品アイデンティティにアクセスするために必要とされるデータで制御装置をプログラミングするであろう。パレットが「Ｂ」社に届けられると、制御装置は該証明書を使用して「Ｂ」社の読み取り装置を認証し、セキュアな情報を開示する。この動作により、パレットに含まれたタグを読み取るために必要な情報が「Ｂ」社に提供されるであろう。トランザクションの間にプライベートと分類されたタグは、もはや「Ｂ」社の領域内でパブリックと分類され得る。

【００４１】

もちろん、制御装置の挙動はこれよりもさらに複雑ともなり得る。例えば、税関当局及び輸送会社は、制御及び出荷情報のために製品又は製品に関する情報にアクセスできるであろう。このためには、「Ａ」社が制御装置を通して部分的な情報に対するアクセスを委任することを必要としてもよい。

【００４２】

消費者環境

Ｊｕｅｌｓによる研究［５］は別として、過去のプライバシー技法は「オプトイン」手法に何の解決策も提供しない。制御装置手法は、販売時に（暗号化を通じて）タグをブロックできるようにし、タグが消費者領域に入るとタグをアンブロックできるようにする。このようにして、当初ブロックされていたタグが再利用できる。新しいサービスの潜在的な範囲は、消費者環境で使用可能にされるであろう。

【００４３】

図１を参照して医薬品小売環境を考えることができる。医薬品環境の内部では、すべてのタグはプライベートであって、在庫のために使用されることができる。製品が購入されると、該タグの「所有権」が小売業者から消費者に渡されることができる。そして、消費者の制御装置は、タグにアクセスするために必要とされる情報で更新されることができる。すると、ユーザは、医療や遠隔医療への適用においてタグを使用できるであろう。

【００４４】

このシナリオでは、制御装置は、ユーザのプライバシー及びタグの機能を維持しながら、医療情報及び健康記録の認証されていない関係者への開示を妨げることができる。

【００４５】

前記シナリオを考慮して、ＲＦＩＤタグのための以前のプライバシー強化技術を振り返り、該技術がなぜ失敗したのかを評価することが有益である。該技術は多くの場合、実際には実現できない機能、及び単一の制御団体を想定した解決策に依存している。さらに優れた解決策がより簡単に利用できるようになるまで、小売業者は販売時点でタグを「キルする」オプションをサポートしなければならない。しかしながら、このオプションはタグをキルするための技術に対する投資を必要とし、販売後の適用の機会を妨げるため、高価である。さらに、ユーザは、タグがキルされたことを手動で検証することはできず、製品情報を制御するオプションを有することを好む可能性がある。

【００４６】

製品はサプライチェーンに沿って分散されるので、複数の関係者が在庫のために、あるいは販売後の応用のために製品タグにアクセスし、再利用することを希望する可能性がある。会社は、該会社がある特定の製品を在庫情報に自動的にリンクさせるのに役立つレガシー識別子で自らの所有物にタグを付けることを希望することがある。例えば、薬物製造者は特定の薬物情報とともに一意の薬物識別子をタグの中に記憶できるであろう。この情報は、薬局、医療サービス、最終ユーザ及び処理会社等の特定の関係者によってだけアクセス可能であるべきである。複数の関係者（例えば、薬局、病院等）がタグによりプライベートな在庫情報を追加することを希望する場合がある。問題は、タグが許可された関係者によってだけアクセスされ、読み取られることができることをどのように保証するか、及びプライバシーが維持されていることをどのように保証するかという点である。

【００４７】

現在の解決策が何をできるのかを評価しよう。

【００４８】

（１）１つの手法は、チェックされるたびに情報の新しい集合でタグを書き換え、次のオーナだけがこの情報にアクセスできるようにすることであろう。これは約束できる解決策であるが、図書館、レンタル事業、又は在庫が回転するサプライチェーン向けのオプションではない。製造情報はリサイクル会社に対しても依然として有用となるであろうため、この情報は消去されるべきではない。

【００４９】

（２）別の手法は、読み取り者を認証するパスワードを導入することであるが、残念なことにパスワードの立ち聞きや収集が可能である。また、パスワード方式は他の問題も提起する。つまり、タグの集合に対する単一のパスワードは容易に打ち負かすことができ、回復するのが困難である。

【００５０】

上記の理由から、現在の解決策は複数の関係者にわたってタグの制御を移動させるのには実際的ではない。製品の所有権は製品のライフサイクルに沿って複数回変化することがあるため、製品情報を開示するためのセキュリティ及びプライバシーの要件も変化するであろう。必要な範囲までオーナとタグの間の関連はセキュア(secure)である必要がある。上記に開示されたプライバシー保護の実現例によれば、タグは、ＩＤ及び製品情報を含み得る「データセット」と、該データセットの開示を制御するためのプライバシー方針を含み得る「制御セット」の組み合わせを有するとみなすことができる。

【００５１】

本発明の実施形態は、制御装置を通してＲＦＩＤタグのプライバシーを管理する。該制御装置は「制御セット」（アクセス方針又はプライバシー方針）をアップロードしてよく、タグ情報の開示及び／又は解釈を制御する。タグ及び／又は製品の所有権が変更される、又は一時的に移管されるとき、制御装置は新たに認証された読み取り装置をタグと関連付けてもよい。このモデルは種々の異なる状況で使用することができ、現在のＲＦＩＤプライバシー解決策及びセキュリティ解決策と比較して一連の優位点を導入することができる。

【００５２】

以下のいくつかのパラグラフは、セキュリティに関連性のあるＲＦＩＤタグの特性、及びこれらが本発明の実施形態にどのように関連しているのかに関する。

【００５３】

１．関連付け及びデータ秘密性　タグは、アイデンティティ、製品又は在庫の情報を不正な又は認証されていないリーダー（reader）に漏洩してはならない。好ましい実施形態よれば、読み取り装置（reader device）はタグ情報にアクセスできるようになる前に制御装置によって認証されなければならず、その後関連のあるプライバシー方針を遵守させられる。

【００５４】

２．経済的実現可能性　手法のほとんどは、何らかの追加の機能をタグに組み込み、

読み取り装置－タグ通信、プロトコルを変更し、あるいは暗号化装置又は特殊タグ等の新しいインフラストラクチャを追加することによってタグに負担をかける。これらの方式はパッシブ(passive)タグのコストを大幅に増加させ得る。理想的には、プライバシー解決策は、追加コストを加算することなく追加の保護を提供するべきである。本発明の実施形態による制御装置の２つの重要な特長は以下の通りである。

【００５５】

（１）制御装置は、タグに技術的な複雑さを付加することなくアクセス制御機能を提供するためのすべてのセキュリティプリミティブを実現することができる。

【００５６】

（２）制御装置は大多数のパッシブタグを「保護」することができる。制御装置が通常のパッシブタグよりはるかに高価であっても、この特性はその経済的な優位点を維持する。

【００５７】

（３）制御装置は、サプライチェーンの任意の点で取り外すことができる。読み取り装置が特定のタグにアクセスすることを認証されているとき、該タグは該読み取り装置にとってパブリックとみなすことができる。

【００５８】

３．信頼性　追加の装置又は前述された「ブロッカータグ」提案等の特殊なタグを組み込む従来の手法はタグの向き(orientation)に敏感である場合がある。走査時のタグの伝送電力は、アンテナに垂直な領域であって、該タグが存在する領域に依存する。ブロッカータグ等のプライバシー機能強化装置がうまく整列されていない場合には、該装置は失敗することがあり、パッシブタグはそのアイデンティティ情報を漏洩する可能性がある。本発明の好ましい実施形態による制御装置を使用するシステムは、タグをデフォルトで「保護」できるようにする。もし走査問題が存在するとすれば、情報は開示されないであろう。この手法はプライバシーを保護するが、「プライベート」タグが使用されるのを妨げるケースもあるであろう。

【００５９】

４．柔軟なプライバシー方針　タグ情報は製品のライフサイクルに沿って異なるプレーヤ（会社、ユーザ等）によってアクセス可能となることがある。特定の適用では、特定の読み取り装置が限られた量のタグ情報にアクセスすることだけを認証されている可能性が高い。制御装置は同時に複数の関係者に対するアクセス方針を伝えるように構成されてもよい。ある実施形態によれば、制御装置があるプレーヤから別のプレーヤに移される際に新しいアクセス方針がアップロードされ得る。アイデンティティが認証され、アクセス方針によって（委任の目的のために、又はそれ以外のために）アクセス方針の書き込みが許される読み取り装置によって、追加のアクセス方針が制御装置に書き込まれることができるようにシステムが構築されてもよい。

【００６０】

ＲＦＩＤタグ／読み取り装置通信の性質は、多くの場合、有効なプライバシー機能強化解決策の作成を困難にしてきた。ＲＦＩＤのやり取りがオンラインのやり取りと根本的に異なる１つの点は、アクセス制御、認証及びキー確立等の機能がないことである。ＲＦＩＤ規格はタグ読み取り装置の識別を可能にしない。識別プロセスの実施なしには、タグ情報の開示を制御することは不可能であった。

【００６１】

一般的には、読み取り装置は、近傍のタグを検出し、パブリックタグに関する平文情報にアクセスしてもよいが、プライベートタグに関する情報にアクセスすることはできない。プライベートタグは暗号化されている、及び／又は保護されている情報を含み得る。タグは、通常、一意のＩＤ（ＵＤＩ）及び該ＩＤが（物理的に又は単に概念的に）関連付けられている製品についての情報を記憶する。概して２つの手法を区別できる。

【００６２】

（ｉ）タグが一意のＩＤだけを伝え、製造者及び製品タイプについての情報はこの識別

子に符号化されているＥＰＣ手法、及び
（ｉｉ）タグメモリが製品を識別するＩＤ、及び該タグが付けられているオブジェクトについての情報を記憶するための追加フィールドを含む分割メモリ手法
本発明の実施形態によると、読み取り装置はプライベートタグに対するアクセス（「読み取り」アクセス、「書き込み」アクセス、あるいは「読み書きアクセス」さえも）を取得するために制御装置とのセキュアな通信を確立する。すると制御装置は認証方式に基づいて役割を実現し、プライバシー方針を検証することができる。これは、「ＲＦＩＤ読み取り装置」のアイデンティティ及び役割についての情報を記憶することを必要とする。役割は組織との関連における機能のセットを表す。このような機能は、タグの中の情報を読み取り、書き込み、追加、あるいは修正する能力を含み得て、タグのプライバシー方針に依存する。例えば、出荷のシナリオでは、国の国境にある税関当局は製品情報を制御し、支払われた税金又は関税についての情報を追加する権利及び能力を与えられるであろう。輸送会社の役割は、輸送及び目的地情報にアクセスするが、出荷された荷物についての情報を修正しない機能を含み得る。
【００６３】
したがって、制御装置はＲＦＩＤシステムにおける追加の機能を可能にする大きな柔軟性を提供し得る。例えば、プライバシー方針は、タグ情報にアクセスしたことのある異なる組織のログファイルを維持することを制御装置に要求し得る。これは、出荷先又は監査役が製品の出荷を検証することを可能にし、認証されていない読み取り装置がプライベート情報にアクセスしていないことを保証することを可能にする。タグ読み取りにおける将来の規制及び制約を考慮すると、このロギング機能は不正な走査動作を防止し、制御するインセンティブを生じさせることができるであろう。
【００６４】
前述されたように、役割に基づく方針は、タグ付きの製品がサプライチェーンに沿って移動するにつれて、異なる役割に異なるアクセス権を与えることができる。さらに、製品が新しいオーナのところへ行く（visit）と、新しいセキュアな方針が制御装置に追加され、新しい製品情報が１つ以上の製品タグに追加され得る。これにより、ネスト化された(nested)領域が、タグ情報にアクセスできる読み取り装置を有することを可能にする。この委任機能は、承認された読み取り装置は信頼できるという仮定の元でセキュアである。
【００６５】
役割のアクセス権は、製品が組織及びカスタマの領域を変更するにつれて、制御装置によって、又はシステム管理者によって直接的に許可され、取り消され得る。読み取り装置が限られた時間の間、タグにアクセスできることが必要とされるケースがある。この場合には、制御装置は、限られた時間の間、有効であり、数回の読み取り動作の後に無効となる特定のキーを配布してもよい。
【００６６】
本発明の実施形態の主要な特性のいくつかは以下のように要約される。
【００６７】
－制御装置は、標準的なＲＦＩＤタグ－読み取り装置間のやり取りを拡張し、ＲＦＩＤタグで、前述された「ブロッカータグ」によって使用される「オプトアウト」手法とは対照的な「オプトイン」手法を実現してよい。
【００６８】
－セキュアで、短期的な関連。パッシブタグは、該タグが認証されていない領域を渡るときに保護され得るが、制御装置によって実行される役割に基づく認証プロセスを通して承認された読み取り装置と容易に関連付けられ得る。
【００６９】
－制御装置は、役割に基づいた認証方式を実現してよい。さらなる任意のアクセス制御手法のかわりに、役割に対してアクセスを許可し、機能を指定する動作によって、アクセス制御権のさらにスケーラブルな管理が可能になる。役割は、複数の組織及び複数の機能に関連付けることができる。

【００７０】
－制御装置は、（前述された）ロギング等の追加の機能を実現する基本的なセキュリティプラットホーム、走査プロセスに関連付けらた追加情報の開示、及び特定の役割に対するアクセスを許可し、取り消す機能を提供することができる。
【００７１】
本発明による制御装置の概念は、無線センサネットワーク及び低リソース装置を含むさまざまな応用例に適用可能であることが留意されるべきである。例えば軍事応用例における秘密の読み取り値を収集する複数のノードから構成されている無線センサネットワークでは、該概念は、これらのノードが、敵ではない、正当な受信機だけにデータを配信することを保証するために使用され得る。
【００７２】
センサネットワーク上の情報にアクセスする前に、読み取り装置は制御装置によって認証される必要があるであろう。認証段階の際、制御装置はセンサネットワーク内の情報にアクセスするために必要なセキュアな情報を配信するであろう。
【発明を実施するための最良の形態】
【００７３】
前述の図に関して、本発明の好ましい実施形態がさらに詳細に説明される。ここで説明される実施形態によれば、制御装置は制御タグと呼ばれ、後述されるＲＦＩＤシステムに関して説明される。第１に、制御タグ特性に関する具体的な説明、及びアクセス－制御プロセスがどのように行なわれるかの説明を提供する。第２の部分は技術設計に関する。
【００７４】
（前述された）図１は２つの態様、つまりデータと制御の分離を描いている。一般的には、商品識別タグは、商品のアイデンティティ、価格、日付、原産地、目的地等の商品の特徴、商品の現在の状況、商品に関する履歴データ等の属性に関する、商品についてのデータ又は情報を含んでもよい。情報がパスワードで保護されているか、もしくは符号化されているか、又は別の方法で保護されているか、守られているのかに応じて、タグ読み取り装置が情報にアクセスできる場合とできない場合とがある。従来技術のシステムによれば、正しいパスワード、復号キー、又は他のアクセスデータを有する任意の読み取り装置はタグに記憶されている情報を読み取り、及び／又は復号／解読することができる。単純で、安価な、特にパッシブＲＦＩＤタグ等の識別タグは、一般的には、異なるタグ読み取り装置を認識したり、識別したり、異なるタグ読み取り装置に異なる応答を提供したりするための十分な処理能力を備えていない。本発明の実施形態による制御装置を、このような単純な識別タグに関連付け、このような制御装置は、異なる読み取り装置が該識別タグとデータを交換すること（つまり、読み取り及び／又は書き込み）ができる範囲を管理できる。該「範囲」は、異なるレベルのデータへのアクセス、あるいは異なる属性又は属性の組み合わせに関するデータへのアクセスを異なる読み取り装置に許可することを含んでもよい。代わりに、該「範囲」は「読み取り専用」、「読み書き」、「委任」（以下を参照すること）等の異なるタイプの権利を異なる読み取り装置に許可することを含んでもよい。
【００７５】
制御タグの詳細及び特性
図２に関して、以下の４つの要素から成るＲＦＩＤシステムが図示されている。
【００７６】
（１）それぞれが製品（不図示）に取り付けられている、あるいはそれ以外の場合製品と関連付けられており、それぞれが一意のＩＤ（ＵＩＤ）及び該製品についての情報を伝える複数の無線周波数ＩＤタグ１０。ＩＤタグは好ましくは安価であり、したがってパッシブタグである可能性が高い。該タグは暗号化又は匿名方式によってデータの秘密性を維持してもよい。
【００７７】
（２）ＩＤタグ１０に関するデータに対するアクセスを制御する機能を有する、アクテ

ィブタグである制御タグ２０。制御タグ２０は読み取り装置３０を認証する暗号プリミティブを含み、パッシブタグ上の情報の読み取り及び／又は書き込みアクセスを可能にすることがある暗号化キーを選択的に分配できる。

【００７８】

（３）ＩＤタグデータの読み取り、及び／又は書き込み、及び、制御タグを用いて適切な認証手順を実行できる読み取り装置、又は読み取り装置／書き込み装置３０。

【００７９】

（４）該読み取り装置は、読み取り装置によって収集されるＩＤタグ情報と記録を関連付け得るバックエンドデータベース４０と連絡を取ってもよい。

【００８０】

制御タグ方式はＩＤタグ－読み取り装置間のやり取りを拡張し、ＩＤタグの情報を保護するために低リソースＩＤタグによって要求されるアクセス制御機能を実現する。読み取り装置３０は、認証を得るため、及び、ＩＤタグ上の秘密の（private）情報にアクセスすることを可能にするデータ又はコードを受け取るために制御タグ２０と保護された通信を確立する必要がある。

【００８１】

制御タグ２０は、考えられる読み取り装置３０のアイデンティティ及び役割についての情報を記憶することによって役割に基づいた認証を実現する。アクセスが許可されると、ＩＤタグ情報にアクセスすること、及び／又は復号することができる。

【００８２】

制御タグがアクセス方針の適切なセットをどのようにして実現する及び／又は施行してよいかをさらに説明する前に、「サプライチェーンシナリオ」を示す図３に関して商品の出荷を再び検討することは有益である。

【００８３】

この例では、制御タグ方式によって、製品が製品に関連付けられたＩＤタグとともに複数の領域にわたり移動する際に製品情報をリリースする制御が可能となる。アクセス情報は製品と組み合わされてサプラインチェーンに沿って配布される。製品情報にアクセスする権利は、役割をベースにした認証プロセスを利用する制御タグによって制御される。制御タグは、アクセスの許可又は拒否に関する規則の組を含み、該アクセスには読み取り及び／又は書き込みアクセスが含まれ得る。

【００８４】

ここで図４を参照すると、初期の団体(entity)から最終的な団体に、輸送組織、倉庫、税関当局等の他の団体を介して出荷される商業製品のような商品（個別に図示されていない）の積送品１が示されている。商品のそれぞれは、商品に付けられている、あるいはそうでなければ商品と関連付けられているＲＦＩＤタグ等の商品識別装置１０を有する。積送品１には制御装置２０が関連付けられている。現在積送品１を保有している団体（不図示）は、ＲＦＩＤ読み取り装置／書き込み装置、又はＲＦ通信手段３２とデータ処理手段３４とを有する「データ交換装置」３０を有する。通信手段３２は送信機２１及び受信機３２２を備える。制御装置２０は同様に、送信機２２１と受信機２２２を備えるＲＦ通信手段２２を有し、データ認証装置２６とアクセス方針記憶装置２８も有する。アクセス方針記憶装置は１以上の団体に対する、あるいは団体のカテゴリに対するものでもあり得る「アクセス方針」を示すデータを記憶し、該「アクセス方針」は、団体（又は団体のカテゴリ）が、制御装置２０が関連付けられている商品識別装置１０とデータを交換するのを許されるべき範囲に関する。

【００８５】

データ交換装置３０の送信機３２１は、自身を「認証する」ために、データ交換装置３０が関連付けられている団体を示す認証データを制御装置２０に提供する。これは制御装置２０の受信機２２２によって受信される。該認証データから、認証装置２６は、アクセス方針記憶装置を参照し、どのアクセス方針が現在の団体（又は団体のカテゴリ）に適用できるのかを確立する。通信手段２２の送信機２２１は、次に、関連付けられている団体

の代りに、その団体に対して適用可能なアクセス方針に従って、データ交換装置３０が商品識別装置１０とデータを交換できるようにするほど十分なアクセスデータをデータ交換装置３０に提供する。意図された範囲のアクセスを可能にするために適切なアクセスデータを、制御装置２０とのやり取りから取得することで、データ交換装置３０は、許可されている範囲まで商品識別装置１０と直接的にやり取りすることができる。該許可されている範囲には、読み取り及び／又は書き込み要求を該商品識別装置１０に送信すること、商品識別装置１０から応答を受信すること、又は他の考えられるやり取りが含まれ得る。

【００８６】

制御装置２０によって提供されるアクセスデータは、秘密の「パスワード」の形式であってもよく、該「パスワード」は、商品識別装置１０からの応答を「トリガする」ために、又は該「パスワード」なしにはセキュアなデータを公開しない商品識別装置１０をアンロックするために必要なものである。この場合、データ交換装置３０と制御装置２０の間の上記のやり取りは、データ交換装置３０と商品識別装置１０間のやり取りの前に発生する。代わりに、制御装置２０によって提供されるアクセスデータは、秘密「キー」の形であってもよく、該「キー」は該「キー」を持たない読み取り装置及び／又は団体にとって意味のない形式でしかデータを明らかにしない商品識別装置１０からからの応答を復号するために必要なものである。この場合には、データ交換装置３０と制御装置２０の間の上記やり取りは、データ交換装置３０と商品識別装置１０間のやり取りの前又は後に発生してよい。さらに高いセキュリティのために、アクセスデータは、上記タイプのデータの両方を備えてもよいし、もしくは他の形式のセキュリティ保護を可能にする他のタイプを含んでよい。

【００８７】

図５は、読み取り装置Ｒと制御タグＡの間、及び読み取り装置Ｒと複数のＩＤタグＴのどれかの間で発生し得るやり取りのプロセスをさらに詳細に描いている。本実施形態によれば、読み取り装置Ｒは、制御タグＡとのやり取りの後ではなくむしろ前にＩＤタグＴとやり取りしてもよい。

【００８８】

図５ａは、以下に使用されるラベルＳ１、Ｓ２、Ｓ３及びＳ４を導入し、これらのやり取りが図４に関して前述されたやり取りとそれぞれのどのように対応するのかを示している。やり取りＳ３とＳ４は読み取り装置Ｒと制御タグＡの間の交換に関する。やり取りＳ１とＳ２は、読み取り装置Ｒと、制御タグＡが関連付けられている複数のＩＤタグＴのどれかの間の交換に関する。

【００８９】

図５ｂは、図５ａをさらに説明するための流れ図を示す。この流れ図のステップがここで説明される。

【００９０】

ステップＺ１．第１の接続Ｓ１が、読み取り装置ＲとＩＤタグＴのそれぞれの通信手段の間で確立される。

【００９１】

ステップＺ２．情報コードワードＳ２が保護されているＩＤタグＴから読み取り装置Ｒに送信される。

【００９２】

送信されたコードワードがセキュリティ方式によって保護されるべきことが判明すると、プロセスは認証ステップに移行する。

【００９３】

ステップＺ３．ステップＳ３では、例えばタグによって送信されたコードワードに関連付けられている読み取り装置Ｒの役割証明書情報によって認証要求が生成される。しかしながら、コードワードの一部を送信することだけが必要な場合もある。

【００９４】

ステップＺ４．認証要求は読み取り装置Ｒから制御装置Ａに送信される。

【００９５】
ステップＺ５．以後のステップでは、ステップＳ３の情報が有効であると制御装置Ａにより判明されると、アクセスデータが制御装置Ａによって読み取り装置Ｒにリリースされる。
【００９６】
ステップＺ６．すると、データ又は関数に対するこのアクセスは、読み取り装置Ｒによって実行されることができる。
【００９７】
図５ｃは、アクセスデータが制御装置Ａによって読み取り装置Ｒに対してすでにリリースされた状況を描いている。
【００９８】
図５ｄは、読み取り装置Ｒが１回以上ＩＤ－タグＴの１つにアクセスしようとするときに、あるいは１以上のＩＤタグにアクセスしようとするときに必要とされる動作を描いている。
【００９９】
図５ｄに示されているように、制御装置Ａとの認証プロセスは最初のときだけ実行される必要がある実施形態もある。この場合、読み取り装置Ｒは制御装置Ａと複数回接触する必要がなく、したがって読み取り動作の効率が改善される。
【０１００】
それぞれのやり取りに対して、異なるレベルのセキュリティが選択され得るし、又は必要とされ得る。例えば、以下のレベルのセキュリティが使用されてもよい。
【０１０１】
－Ｓ１接続及び平文（セキュリティは使用されていない）のメッセージ
－Ｓ２コードワードがセキュリティ付きで送信される
－ＩＤ情報のための匿名
－他のデータ情報のための暗号化
－Ｓ３及びＳ４は保護された通信チャネルを通して送信される。使用されてるプロトコルは制御タグの通信プロトコルに依存する。制御タグは、８０２．１１ａ，ｂ，ｇ、ブルーツース、８０２．１５．４又はその他のプロトコルを使用できるであろう。
【０１０２】
制御タグ要約
最初に、制御タグはＩＤタグの制御を取得する。方針及びＩＤタグと関連づけられた共有される秘密は、制御タグ内にアップロードされる。方針の関連が制御タグをＩＤタグの制御下に入れる。方針は異なる方法でアップロードされ得る。例えば、制御タグはブルーツースの装置のようであると仮定してよい。制御タグが無線通信チャネルを通して関連付けられると仮定できる。この場合、認証交換プロトコルが必要とされる。したがって、制御タグをＩＤタグに関連付けるための機構を必要とする。消費者シナリオの適用では、タグは、ＩＤタグを検証し、データベースに関する、又は以前の制御タグに関する方針を調べる特殊な読み取り装置の近くにくるであろう。その結果、新しい制御タグは無線チャネルを通して正しい情報を取得する。
【０１０３】
第２に、制御タグはアクセスを委任する。制御タグの主要な特長はアクセスを委任し、アクセス制御を管理する能力である。タグが読み取り装置によって読み取られる必要があるとき、該読み取り装置は制御タグから、可変量の時間の間、タグを読み取る権利を受け取ることができる。例えば、アクセスパスワード又は暗号化によって保護されているＩＤタグの場合、制御タグはパスワード又は暗号化キーに対するアクセスを委任できる。この方式は、タグが新しい読み取り装置に委任されるたびに制御タグ及び読み取り装置がタグのアクセスパスワードを書き換えることをサポートする。
【０１０４】
ＲＦＩＤタグ特性

制御タグのさらなる詳細を説明する前に、ＲＦＩＤタグ技術のいくつかの一般的な特性及び特長が図６に関して説明される。現在の適用では、ＵＨＦバンド（８６０から９６０ＭＨｚ）のＲＦＩＤシステムは約７メートまでの範囲を有することができる。ＨＦバンド（１３．５６ＭＨｚ）では、この範囲は１又は２メートルに下がる。いったんタグが読み取り装置の範囲内に入ると、タグは自らのメモリに記憶されている情報を送信する準備を完了することができる。複数のタグが存在する場合、読み取り動作を可能にするために、衝突防止アルゴリズムが必要とされる場合がある。現在の技術には、「Ａｌｏｈａ」タイプの手法、又は「バイナリツリーウォーキング(binary-tree walking)」プロトコル等の決定論的方法を使用するものもある。

【０１０５】

ＩＳＯ／ＩＥＣ　１８０００規格により説明されているように、タグは、質問機(interrogator)によって書き込み、読み取ることのできるレジスタのセット、及び特定の目的のために使用できるであろうフラグのセット（ｓｌｅｅｐ、ｗｒｉｔｅ＿ｅｒｒ、ｗｒｉｔｅ＿ｐｒｏｔ等）を含むであろう。読み取りコマンドはタグに記憶されている情報にアクセスするためにスキャナによって使用され得る。

【０１０６】

１つのレジスタが「ｓｅｓｓｉｏｎ＿ｉｄ」（又はｐｏｌｉｃｙ＿ｉｄ）情報を含むと仮定してよい。該情報は商品識別タグと制御タグの間のリンクを維持することができる。その他のレジスタは暗号化されたフォーマットの製品情報及び汎用ＩＤコードを含んでもよい。フラグは読み取り装置に、情報がパブリックであるのか、あるいはプライベートであるのかを通知することができる。

【０１０７】

ＲＦＩＤタグに含まれているフィールドは制御タグと結び付けられる必要があり、したがってタグの中の情報は、セキュアな関係が確立されるまでプライベートとして維持されてよい。次の項目で分かるように、異なるレベルのセキュリティ及びプライバシーが、実現されている機構に応じて使用可能である。

【０１０８】

制御タグ－プライバシー方針アップロード

前述されたように、読み取り装置がタグ上の情報にアクセスを希望するとき、制御タグにコンタクトしなければならない。いったん読み取り装置のアイデンティティが認証されると、読み取り装置はタグにアクセスするためにセキュアな情報を要求できる。

【０１０９】

制御タグとＩＤタグのオーナが、制御タグにＩＤタグを制御させることを望むと、制御タグは制御動作を実行するために必要なすべての情報を取得しなければならない。この情報は暗号化／匿名のためのキー、アクセス制御のためのパスワード、コマンドをキルするためのキリング(killing)パスワード、及び読み取り装置のためのアクセス制御方針を含むことができ、安全な方式で転送されなければならない。

【０１１０】

読み取り装置の適用のためのアクセス権を管理する、役割に基づいた認証方式が使用されてよい。各読み取り装置は１つ以上の役割に関連付けられることができ、各役割は、ＩＤタグ内の情報の１つ以上のタイプ又はフィールドに関するデータの読み取り、又は書き込みに割り当てることができる。読み取り装置証明書は読み取り装置のアイデンティティ、該読み取り装置の役割、及び該読み取り装置の物理的なオペレータ（例えば、会社又は他のこのような団体）についての情報を運ぶことができる。この証明書は大局的に一意である必要があり、これにより制御タグが読み取り装置とセキュアな関係性を確立できる。

【０１１１】

読み取り装置と制御タグの間の通信は、Ｚｉｇｂｅｅ又はブルーツース等の低電力装置用の標準的な通信プロトコル、あるいは十分な電池電力が利用できる場合には８０２．１１ａ／ｂ／ｇ上で行なわれてもよい。通信チャネルは保護されていると仮定されている（秘密性及び認証特性）。

【０１１２】
制御タグが作成される、あるいは例えば商品の積送品に割り当てられると、ルート証明書がインストールされる必要がある。このようなルート証明書は管理目的のために常に存在する必要がある。ルート証明書の「オーナ」は信頼できるサードパーティであってもよい。したがって、異なるプライバシー方針及び異なるタグのキー情報をアップロードすることが必要となり得る。特定のＲＦＩＤタグに対するアクセスを必要とする役割は、該証明書がロードされ、該特定のタグと関連付けられていることを必要とし得る。
【０１１３】
制御タグは、一連の関連する方法を備えたオブジェクト、つまりＲＦＩＤタグにアクセスする権利とみなされ得る。役割に基づいた方針は、ＲＦＩＤタグ情報に対するアクセスを許可するように制御タグを説得するために、読み取り装置／スキャナがどの信用証明物を提供する必要があるのかを、使用可能なアクションのそれぞれに指定する命令文である。
【０１１４】
委任
図７に関して、特定のＩＤタグ及び／又は該ＩＤタグの情報に関して権利を有する役割が、別の役割に対して該権利の一部又はすべてを委任する権利を与えられてよい。この委任の権限は注意して管理される必要がある。新しい方針をアップロードするときの役割は、一般的には該役割がアクセスできる情報に対するアクセス、あるいは役割が自身で有する権利を委任できるに過ぎない。したがって、委任される役割は一般的には、許可側の役割と比較して同じ（又はより少ない）量の権利、あるいは情報に対するアクセスを許可されるに過ぎない。この手法はピア間のやり取りを可能にし、提案されている方式の柔軟性を強化する。
【０１１５】
図３に関して前述された出荷環境では、例えば「Ａ」社は個々の製品上のＩＤタグのプライバシー方針をアップロードしてもよい。
【０１１６】
（１）「Ａ」社は、「Ｓｅｓｓｉｏｎ＿ｉｄ」情報に関連付けられた「Ｂ」社の証明書及びタグにアクセスするためのセキュアな情報とともに制御タグをアップロードできるであろう。「Ｂ」社は最終的な目的地であるので、おそらくＢ社がＡ社と同じアクセス権を有するであろうと想像できるであろう。
【０１１７】
（２）プライバシー方針は輸送会社に対するアクセスも許可できるであろう。輸送会社がどの情報にアクセスするべきであるのかを指定する役割証明書がアップロードされる。輸送会社はサードパーティ輸送会社にこのアクセスを委任できるであろう。
【０１１８】
（３）プライバシー方針は、製品が国境を越えるときに自動的にチェックされ得るように税関当局にアクセス権利を与えてもよい。この役割は、例えば、関税又は税金が支払われていることを示すために、例えばＩＤタグの中に情報を書き込む権利を与えてよい。
【０１１９】
読み取り装置認証及びデータ開示
前述されたように、本発明者らのシステムの好ましい実施形態では、個々の商品のタグ上のタグ情報が別々のセキュリティキーによって保護されており、制御タグが読み取り装置に正しいデータにアクセスするための正しいキー又はパスワードを与えていると仮定している。図８に関して、該方式は以下のように動作し得る。
【０１２０】
セットアップ時、Ｓｅｓｓｉｏｎ＿ＩＤが各商品タグに与えられ、これは在庫情報又は製品情報という点では意味がないが、制御タグと商品タグをリンクすることを可能にする番号である。これにより、どのキーを開示べきであるかを知らなければならないという問題が解決される。ｓｅｓｓｉｏｎ＿ＩＤは商品タグと制御タグの間のリンクを維持するた

めに使用されることができる。静的なｓｅｓｓｉｏｎ＿ＩＤが追跡を可能にしてよいことが考えられる。追跡が問題とみなされる場合、読み取り動作のたびに、前記［３］に概略されている「匿名」手法にいくつかの点で類似したようにリフレッシュする動的なｓｅｓｓｏｎ＿ＩＤが使用できるであろう。

【０１２１】

（１）読み取り動作中、（ＲＦＩＤ商品タグのような）ＩＤタグは「Ｓｅｓｓｉｏｎ＿ＩＤ」情報から成るメッセージ（Ｓ＿ＩＤ,Ｐｒｉｖａｔｅ）を送信する。

【０１２２】

（２）読み取り装置は、次に、「組」（証明書、Ｓ＿ＩＤ）（つまり、２種類の情報：アクセス方針に対応する証明書、及び「Ｓｅｓｓｉｏｎ＿ＩＤ」情報であるＳ＿ＩＤ）を用いてセキュアな通信チャネルを通して制御タグを照会するであろう。証明書が認識されると、制御タグはＩＤタグに記憶されている秘密情報にアクセスするためのキー（Ｓ＿ＩＤ,Ｋ１,Ｋ２,Ｋ３,．．．,Ｋｎ）を開示するであろう。

【０１２３】

（３）次に、読み取り装置は異なるレジスタに含まれている情報を取得するためにＩＤタグ（Ｓ＿ＩＤ）を照会するであろう。該情報は暗号化された形式で送信され、該情報は読み取り動作で開示されないであろう（Ｓ＿ＩＤ,ｄａｔａ－１,ｄａｔａ－２,ｄａｔａ－３,．．．,ｄａｔａ－ｎ）。情報を受信すると、読み取り装置は制御タグによって開示されたキーを使用して情報を復号するであろう。

【０１２４】

要約すれば、好ましい実施形態による制御タグは、タグ－読み取り装置間のやり取りを拡張できるようにし、ＩＤタグに記憶されている情報を保護するために「オプトイン」手法を実現する。このようにして、セキュアで、短期的な関連を確立するための方法が提供され、これにより、タグ情報は、認証される役割によってだけアクセスされ得る。この方式の特に優位な点は、現在のＲＦＩＤ技術に対する修正が必要ではないという点である。適切な方法は、ＲＦＩＤタグのクラス０、１、２等と互換性があるように使用され得る。

【０１２５】

さらなる注意が必要ないくつかの問題点がある。静的な「Ｓｅｓｓｉｏｎ＿ＩＤ」フィールドとレジスタに記憶されている静的なデータ情報の両方を通してタグ付きの製品を追跡することも可能である。さらに、取り消し問題はこれまで対処されてこなかった。制御タグがセキュアなキー情報を開示するとき、ＩＤタグは、該ＩＤタグを受け取る読み取り装置に公開され、この権利を取り消すことはできない。

【０１２６】

局所キー手法－追跡保護及び取り消し制御に対して

前述の問題を解決するために、該方式に何らかの形の動的処理が加えられ得る。これは商品ＩＤタグに何らかの基本的なセキュア機能を追加する必要がある。タグは、追加のキーを記憶し、簡略な暗号化機能を実行できるであろう。

【０１２７】

図９を参照すると、解決策は、読み取り装置、制御タグ、及び商品タグの間で共有される局所キーを追加することである。商品タグが新しい領域に移管されると（タグ所有権の変更）、局所キーは変更される。この手法の基本的な考え方は、タグの「暗号文テキスト（cyphetexts）」の外観を変化させるために再暗号化を利用しつつ、暗号文テキストの元である平文は同じままとすることである。この手法を利用すると、タグ情報は局所キーを共有する読み取り装置にだけ開示され得る。

【０１２８】

局所キーは、セキュアな通信チャネルを介して読み取り装置と制御タグの間で容易に共有され得る。それにも関わらず、商品タグと秘密を共有することはさらに困難な問題であり得る。

【０１２９】

「秘密」を共有することの問題の１つは、受動的な盗聴者がキー共有動作を立ち聞きす

ることができるという点である。ここに概略されているのは、この問題に対する２つの考えられる解決策である。

【０１３０】

－読み取り装置は非常に短い範囲のプロトコルを通してタグの読み取り専用レジスタにパスワードを書き込む（表面接触読み取り装置）。したがって、盗聴者はこの通信を立ち聞きすることはできない。

【０１３１】

－Ｍｏｌｎａｒ及びＷａｇｎｅｒ［７］は、タグと読み取り装置間の非対称通信を利用する方法を提案した。タグは、読み取り装置のみが聞くことができる乱数を用いて通信を開始し、この乱数に基づいて、局所キーが共有される。

【０１３２】

この手法は以下の特長を提供し得る。

【０１３３】

（１）読み取り装置とタグの間の１対１のセキュアな通信が可能となる。他の役割に対するアクセス権は一時的に取り消される。

【０１３４】

（２）局所キーを変更により、追跡の防止が改善される。局所キーを頻繁に変更すればするほど、追跡の可能性が下がる。

【０１３５】

ここで、局所キーＸが読み取り装置、商品ＩＤタグ、及び制御タグの間で共有されていると仮定してみよう。Ｘを局所レジスタに記憶させ、ＥがＩＤタグで実現される単純な低リソース暗号化関数であると仮定する。

【０１３６】

従来のプロトコルは次のように修正できるであろう。

【０１３７】

ａ．読み取り動作中、ＩＤタグは局所キーＸで暗号化されている「Ｓｅｓｓｉｏｎ＿ＩＤ」情報から成るメッセージ（Ｅ（Ｓ＿ＩＤ），Ｐｒｉｖａｔｅ）を送信する。局所的なキーＸは、前記説明された２つの方法の一方を使用して読み取り装置とＩＤタグの間で共有されている。

【０１３８】

ｂ．次に、読み取り装置は組（ｃｅｒｔｉｆｉｃａｔｅ，Ｓ＿ＩＤ）を用いてセキュアな通信チャネルを通して制御タグを照会する。読み取り装置は（Ｓ＿ＩＤ，Ｋ１，Ｋ２，Ｋ３，．．．，Ｋｎ）を取得する。Ｋ１，Ｋ２，．．．，Ｋｎはｄａｔａ－１，ｄａｔａ－２，．．．，ｄａｔａ－ｎに含まれている情報を復号するために使用されるキーであることに留意する。

【０１３９】

ｃ．（３）次に読み取り装置はＩＤタグを照会する。ＩＤタグは、悪意のある読み取り装置が該タグを追跡できないように、局所キーで再暗号化された情報を送信する。ＩＤタグはメッセージ、つまり（Ｅ（Ｓ＿ＩＤ），Ｅ（ｄａｔａ－１），Ｅ（ｄａｔａ－２），Ｅ（ｄａｔａ－３，．．．，Ｅ（ｄａｔａ－ｎ））を送信する。情報を受信すると、読み取り装置は制御タグによって開示されているキーを使用して情報を復号する。

【０１４０】

［７］ライブラリＲＦＩＤにおけるプライバシー及びセキュリティ（Privacy and Security in Library RFID）、Ｄａｖｉｄ　Ｍｏｌｎａｒ、Ｄａｖｉｄ　Ｗａｇｎｅｒ、カリフォルニア大学バークレー校（University of California of Berkeley）

【図面の簡単な説明】

【０１４１】

【図１】医薬品又は他の消費者製品等の商品に関連して「データ」及び「制御」情報の考え方を描く。

【図２】制御タグ、複数のＩＤタグ、読み取り装置、及びバックエンドデータベースを含

むシステム内の主要な要素及びやり取りを描く。
【図３】サプライチェーンシナリオ、又は出荷環境における制御タグの可能な使用を描く。
【図４】本発明の好ましい実施形態による制御装置を含むシステムを描く。
【図５】読み取り装置と制御タグの間、及び読み取り装置と複数のＩＤタグの間で発生し得るやり取りのプロセスをさらに詳細に描く。
【図６】ＲＦＩＤタグの可能な特性を示す図である。
【図７】制御タグに記憶されているアクセス方針の可能な構造を示す。
【図８】本発明の実施形態による制御タグを使用する読み取り装置認証及びデータ開示のための可能なシステムを示す。
【図９】局所的な領域を保護するための局所的なキーの使用を描く。

【図１】

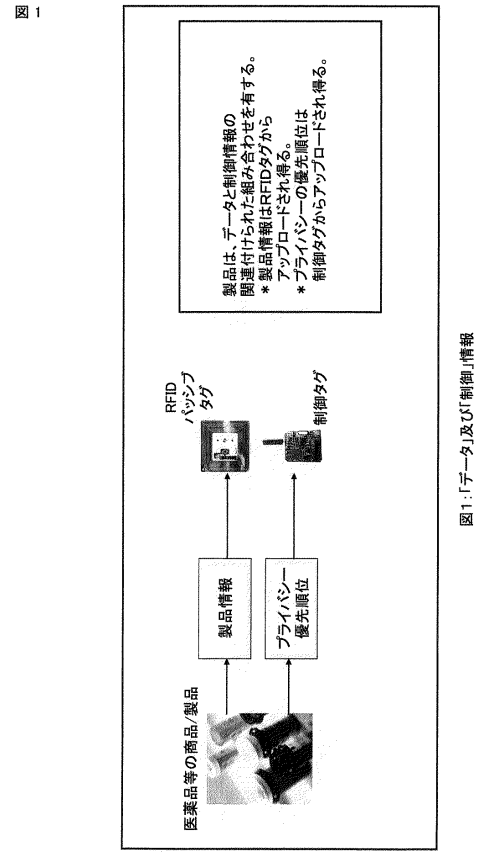

図1：「データ」及び「制御」情報

【図２】

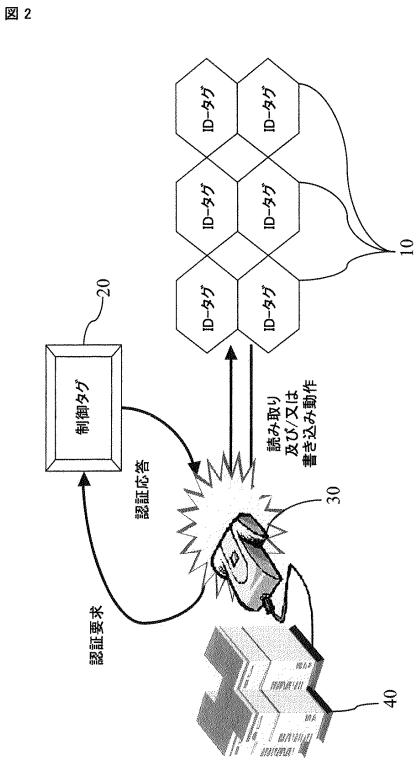

図2：読み取り装置－タグシステムにおける要素及びやり取り

【図３】

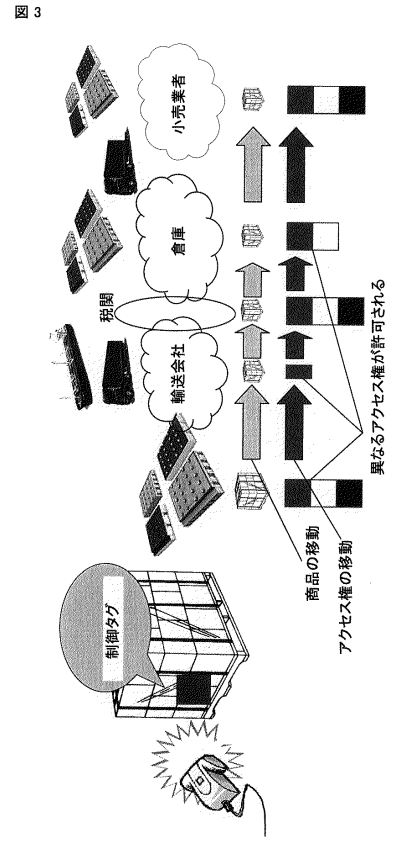

図3：「サプライチェーンシナリオ」又は出荷環境

【図４】

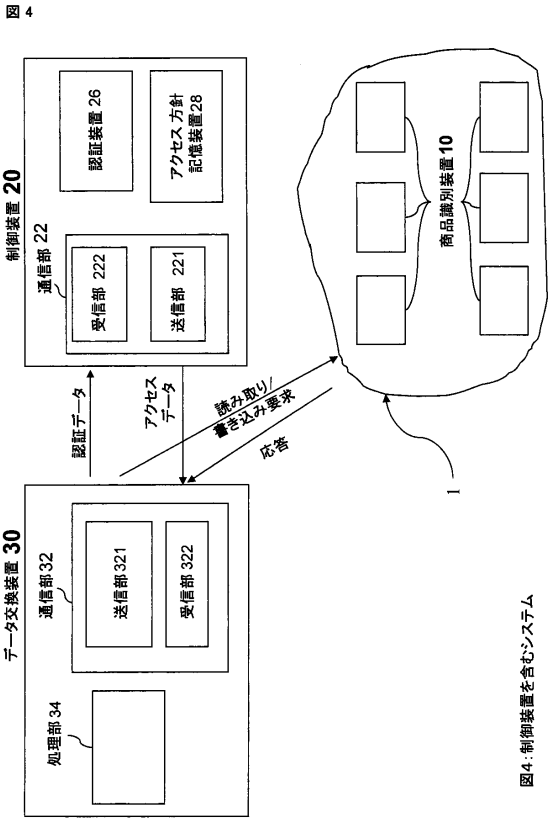

図4：制御装置を含むシステム

【図５】

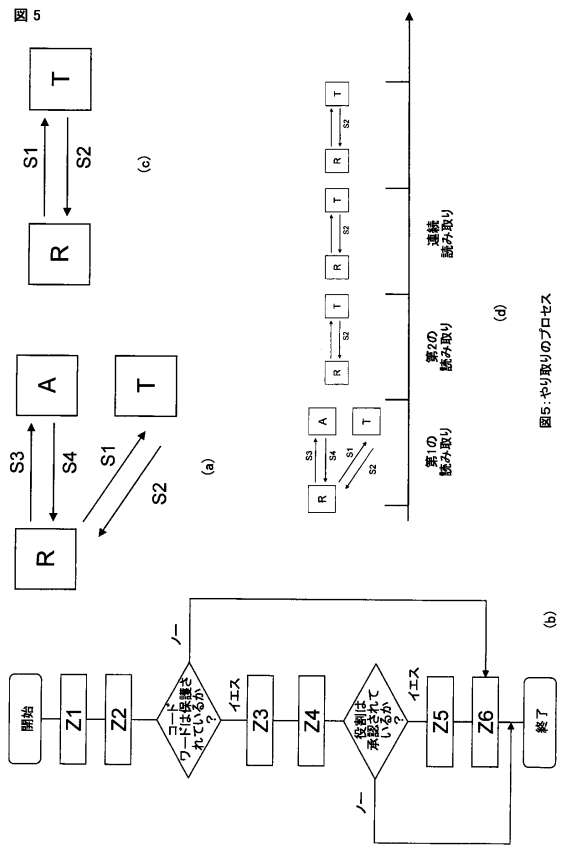

図5：やり取りのプロセス

【図６】

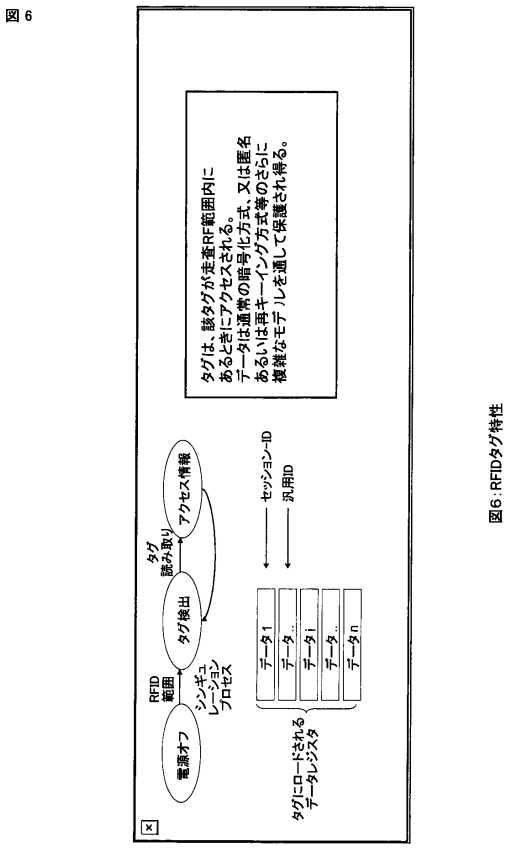

図6：RFIDタグ特性

【図７】

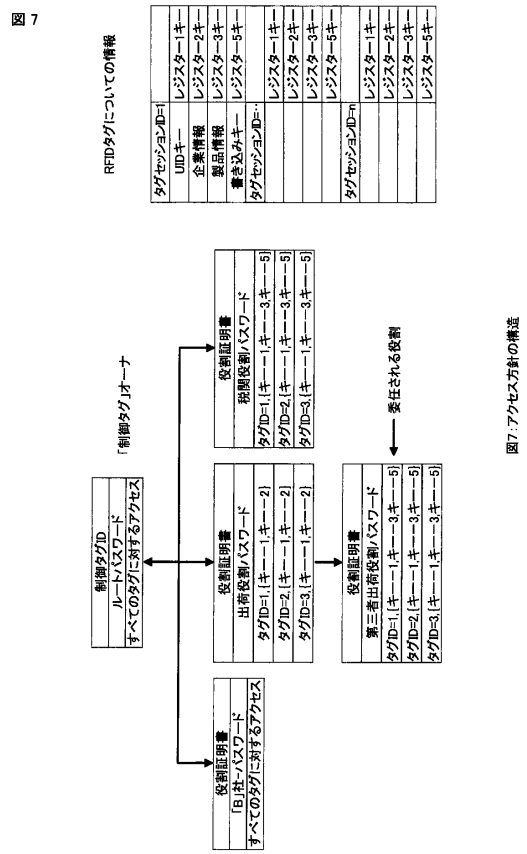

図7：アクセス方針の構造

【図８】

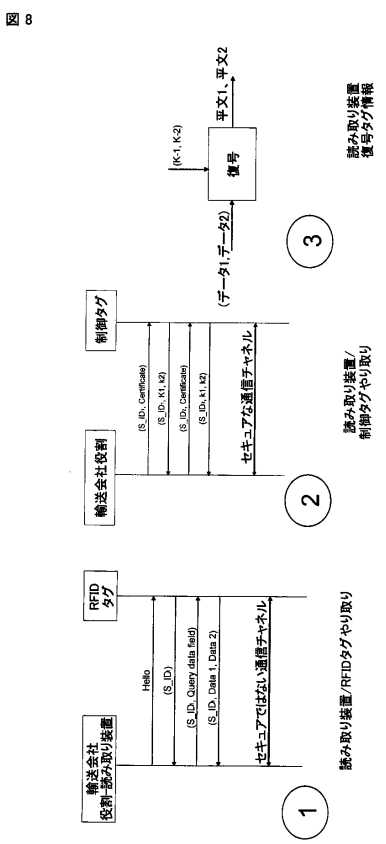

図8：読み取り装置認証のためのシステム

【図９】

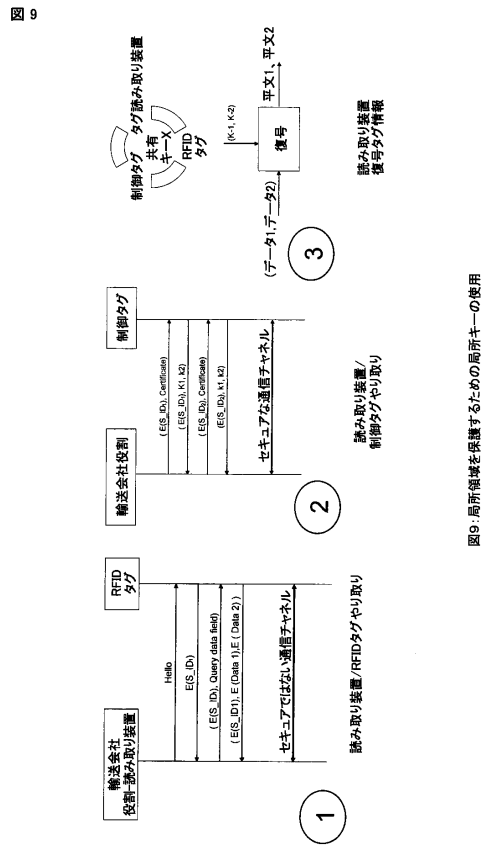

図9：局所領域を保護するための局所キーの使用

フロントページの続き

(51)Int.Cl. FI
G06F 12/14 560B

(74)代理人 100075672
弁理士 峰 隆司
(74)代理人 100109830
弁理士 福原 淑弘
(74)代理人 100095441
弁理士 白根 俊郎
(74)代理人 100084618
弁理士 村松 貞男
(74)代理人 100103034
弁理士 野河 信久
(74)代理人 100140176
弁理士 砂川 克
(74)代理人 100092196
弁理士 橋本 良郎
(74)代理人 100100952
弁理士 風間 鉄也
(72)発明者 ソッペラ、アンドリー
イギリス国、アイピー４・２ジェイエー、サフォーク、イプスウィッチ、セメテリー・ロード ４９
(72)発明者 バーブリッジ、トレバー
イギリス国、アイピー４・４エイチビー、サフォーク、イプスウィッチ、ロンズデール・クロース ４
(72)発明者 コーガオンカー、ビベカナンド
イギリス国、アイピー１・１エックスエフ、サフォーク、イプスウィッチ、エスティー・ピーターズ・ストリート １９

審査官 市川 武宜

(56)参考文献 特開２００１－１９５５４８（ＪＰ，Ａ）
特開２００２－３１２７２３（ＪＰ，Ａ）
特開平１０－３２４４０５（ＪＰ，Ａ）
特開２００２－３１９００１（ＪＰ，Ａ）
特開２００１－３０７０５５（ＪＰ，Ａ）
特開２００１－１３４６７２（ＪＰ，Ａ）
特開２００４－２４７７９９（ＪＰ，Ａ）
特開２００１－２８３１７１（ＪＰ，Ａ）
特開２００５－０９２７９６（ＪＰ，Ａ）

(58)調査した分野(Int.Cl., ＤＢ名)
G06F 21/20
G06F 21/24
G06K 17/00
G06K 19/07
G06K 19/10