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

特許第4139382号
(P4139382)

(45)発行日　平成20年8月27日(2008.8.27)　(24)登録日　平成20年6月13日(2008.6.13)

(51)Int.Cl.		F I		
H04L 9/32	(2006.01)	H04L	9/00	675A
G06K 17/00	(2006.01)	H04L	9/00	673E
G06F 21/20	(2006.01)	G06K	17/00	S
		G06F	15/00	330B

請求項の数 18　(全 15 頁)

(21)出願番号　特願2004-380867(P2004-380867)
(22)出願日　平成16年12月28日(2004.12.28)
(65)公開番号　特開2006-186903(P2006-186903A)
(43)公開日　平成18年7月13日(2006.7.13)
審査請求日　平成19年12月10日(2007.12.10)

早期審査対象出願

(73)特許権者　390009531
インターナショナル・ビジネス・マシーンズ・コーポレーション
ＩＮＴＥＲＮＡＴＩＯＮＡＬ　ＢＵＳＩＮＥＳＳ　ＭＡＳＣＨＩＮＥＳ　ＣＯＲＰＯＲＡＴＩＯＮ
アメリカ合衆国１０５０４　ニューヨーク州　アーモンク　ニュー　オーチャード　ロード
(74)代理人　100086243
弁理士　坂口　博
(74)代理人　100091568
弁理士　市位　嘉宏
(74)代理人　100108501
弁理士　上野　剛史

最終頁に続く

(54)【発明の名称】製品／サービスに係る所有権限を認証する装置、製品／サービスに係る所有権限を認証する方法、及び製品／サービスに係る所有権限を認証するプログラム

(57)【特許請求の範囲】
【請求項１】
識別子を備える製品より提供される前記識別子と、前記識別子、前記製品に係る情報および前記情報へのアクセス権限を認証するためのワンタイム認証キーをそれぞれ記憶する製品ＤＢ（データベース）より提供される前記ワンタイム認証キーと、前記情報へのアクセス権限を認証するためのワンタイム認証キーを作成・保持する端末より提供される前記ワンタイム認証キーとにより、前記情報へのアクセス権限を認証する装置であって、
前記製品より提供される前記識別子と、前記端末より提供される前記ワンタイム認証キーを受け取る手段と、
前記受け取った前記識別子により、前記製品ＤＢより提供される前記ワンタイム認証キーを取得する手段と、
前記受け取った前記端末より提供される前記ワンタイム認証キーと、前記取得した前記製品ＤＢより提供される前記ワンタイム認証キーから、前記情報へのアクセス権限があるか否かを判定する手段と
を含む、前記装置。
【請求項２】
前記判定する手段が、前記ワンタイム認証キーとして、所定の方法で得た数値に一方向ハッシュ関数をｔ（１以上の整数）回適用して得られるハッシュ値を使用して判定し、次回の認証において、前記ワンタイム認証キーとして、前記数値に前記一方向ハッシュ関数をｔ－１回適用して得られるハッシュ値を使用して判定する手段を含む、請求項１に記載

の装置。
【請求項３】
前記受け取る手段が、前記識別子を前記製品より読み込んだ前記端末から前記識別子を受け取る、請求項１または２に記載の装置。
【請求項４】
前記製品ＤＢより、１つの前記製品につき前記情報への複数のアクセス権限に対応した複数のワンタイム認証キーが提供される、請求項１から３のいずれかに記載の装置。
【請求項５】
前記製品が、サービスの提供を受けるためのサービス券である、請求項１から４のいずれかに記載の装置。
【請求項６】
識別子を備える製品より提供される前記識別子と、前記識別子、前記製品に係る情報および前記情報へのアクセス権限を認証するためのワンタイム認証キーをそれぞれ記憶する製品ＤＢ（データベース）より提供される前記ワンタイム認証キーと、前記情報へのアクセス権限を認証するためのワンタイム認証キーおよび前記情報へのアクセス権限移転後の前記情報へのアクセス権限を認証するための別のワンタイム認証キーを作成・保持する端末より提供される前記ワンタイム認証キーおよび別のワンタイム認証キーとにより、前記情報へのアクセス権限を認証する装置であって、
前記製品より提供される前記識別子と、前記端末より提供される前記ワンタイム認証キーおよび別のワンタイム認証キーを受け取る手段と、
前記受け取った前記識別子により、前記製品ＤＢより提供される前記ワンタイム認証キーを取得する手段と、
前記受け取った前記端末より提供される前記ワンタイム認証キーと、前記取得した前記製品ＤＢより提供される前記ワンタイム認証キーから、前記情報へのアクセス権限があるか否かを判定する手段と、
前記情報へのアクセス権限があると判定されたことを条件に、前記製品ＤＢに記憶された前記ワンタイム認証キーの代わりに、前記受け取った前記端末より提供される前記別のワンタイム認証キーを前記製品ＤＢに記憶する手段と
を含む、前記装置。
【請求項７】
前記判定する手段が、前記ワンタイム認証キーとして、所定の方法で得た数値に一方向ハッシュ関数をｔ（１以上の整数）回適用して得られるハッシュ値を使用して判定し、次回の認証に、前記別のワンタイム認証キーとして、所定の方法で得た数値に前記一方向ハッシュ関数をｕ（１以上の整数）回適用して得られるハッシュ値を使用して判定する手段を含む、請求項６に記載の装置。
【請求項８】
前記受け取る手段が、前記識別子を前記製品より読み込んだ前記端末から前記識別子を受け取る、請求項６または７に記載の装置。
【請求項９】
前記製品ＤＢより、１つの前記製品につき前記情報への複数のアクセス権限に対応した複数のワンタイム認証キーが提供される、請求項６から８のいずれかに記載の装置。
【請求項１０】
前記製品が、サービスの提供を受けるためのサービス券である、請求項６から９のいずれかに記載の装置。
【請求項１１】
製品に係る情報へのアクセス権限に関する認証情報を管理する端末であって、
製品の識別子とは別個に管理される所定の方法で得た数値およびｔ（１以上の整数）を記憶する手段と、
製品ＤＢ（データベース）に記憶される前記製品に係る情報へのアクセス権限を認証する装置で認証するために使用されるワンタイム認証キーを、前記数値に一方向ハッシュ関

数をｔ回適用して得られるハッシュ値で作成し、暗号キーを、前記数値に前記一方向ハッシュ関数をｔ－１回適用して得られるハッシュ値で作成する手段と、
前記作成したワンタイム認証キーを前記作成した暗号キーで暗号化する手段と、
を含む前記端末。
【請求項１２】
次回の認証のために使用される前記ワンタイム認証キーが、前記一方向ハッシュ関数を前記数値にｔ－１回適用して得られるハッシュ値で作成される、請求項１１に記載の端末。
【請求項１３】
前記製品の識別子を読み込むための手段をさらに含む、請求項１１または１２に記載の端末。
【請求項１４】
前記製品が、サービスの提供を受けるためのサービス券である、請求項１１から１３のいずれかに記載の端末。
【請求項１５】
識別子を備える製品と、
前記識別子、前記製品に係る情報および前記情報へのアクセス権限を認証するためのワンタイム認証キーをそれぞれ記憶する製品ＤＢ（データベース）と、
前記製品ＤＢに記憶された前記情報へのアクセス権限を認証するためのワンタイム認証キーを作成・保持する端末と、
前記製品より提供される前記識別子および前記端末より提供される前記ワンタイム認証キーを受け取り、前記受け取った前記識別子により前記製品ＤＢより提供される前記ワンタイム認証キーを取得し、前記端末より提供される前記ワンタイム認証キーおよび前記製品ＤＢより提供される前記ワンタイム認証キーから前記情報へのアクセス権限があるか否かを判定する認証装置と、
を含む、製品に係る情報へのアクセス権限を認証するシステム。
【請求項１６】
識別子を備える製品より提供される前記識別子と、前記識別子、前記製品に係る情報および前記情報へのアクセス権限を認証するためのワンタイム認証キーをそれぞれ記憶する製品ＤＢ（データベース）より提供される前記ワンタイム認証キーと、前記情報へのアクセス権限を認証するためのワンタイム認証キーを作成・保持する端末より提供される前記ワンタイム認証キーとにより、前記情報へのアクセス権限を認証する方法であって、
インタフェース手段により、前記製品より提供される前記識別子と、前記端末より提供される前記ワンタイム認証キーを受け取るステップと、
ＣＰＵにより、前記受け取った前記識別子で前記製品ＤＢを検索して、前記製品ＤＢより提供される前記ワンタイム認証キーを取得するステップと、
前記ＣＰＵにより、前記受け取った前記端末より提供される前記ワンタイム認証キーと前記取得した前記製品ＤＢより提供される前記ワンタイム認証キーを比較して、一致するか否かで前記情報へのアクセス権限があるか否かを判定するステップと
を含む、前記方法。
【請求項１７】
識別子を備える製品より提供される前記識別子と、前記識別子、前記製品に係る情報および前記情報へのアクセス権限を認証するためのワンタイム認証キーをそれぞれ記憶する製品ＤＢ（データベース）より提供される前記ワンタイム認証キーと、前記情報へのアクセス権限を認証するためのワンタイム認証キーおよび前記情報へのアクセス権限移転後の前記情報へのアクセス権限を認証するための別のワンタイム認証キーを作成・保持する端末より提供される前記ワンタイム認証キーおよび別のワンタイム認証キーとにより、前記情報へのアクセス権限を認証する方法であって、
インタフェース手段により、前記製品より提供される前記識別子と、前記端末より提供される前記ワンタイム認証キーおよび別のワンタイム認証キーを受け取るステップと、

ＣＰＵにより、前記受け取った前記識別子で前記製品ＤＢを検索して、前記製品ＤＢより提供される前記ワンタイム認証キーを取得するステップと、
前記ＣＰＵにより、前記受け取った前記端末より提供される前記ワンタイム認証キーと前記取得した前記製品ＤＢより提供される前記ワンタイム認証キーを比較して、一致するか否かで前記情報へのアクセス権限があるか否かを判定するステップと、
前記情報へのアクセス権限があると判定されたことを条件に、前記ＣＰＵにより、前記製品ＤＢに記憶された前記ワンタイム認証キーの代わりに、前記受け取った前記端末より提供される前記別のワンタイム認証キーを前記製品ＤＢに記憶するステップと
を含む、前記方法。
【請求項１８】
製品に係る情報へのアクセス権限に関する認証情報を管理する方法であって、
製品の識別子とは別個に管理される所定の方法で得た数値およびｔ（１以上の整数）をインタフェース手段より入力して記憶手段に記憶するステップと、
ＣＰＵにより、製品ＤＢ（データベース）に記憶される前記製品に係る情報へのアクセス権限を認証する装置で認証するために使用されるワンタイム認証キーを、前記数値に一方向ハッシュ関数をｔ回適用して得られるハッシュ値で作成し、暗号キーを、前記数値に前記一方向ハッシュ関数をｔ－１回適用して得られるハッシュ値で作成するステップと、
前記ＣＰＵにより、前記作成したワンタイム認証キーを前記作成した暗号キーで暗号化するステップと、
を含む前記方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ＲＦＩＤ（Radio Frequency Identification）、ＩＣタグ、二次元バーコードやその他の識別子で製品やサービスを管理する場合において、当該製品またはサービスの製造過程や流通等に関する情報にアクセスする権限を所有する者か否かを、認証する装置、認証する方法、及び認証するプログラムに関する。
【背景技術】
【０００２】
近年、流通業界では、製品（商品）の管理をバーコード等から、無線ＩＣチップを利用したＲＦＩＤ（Radio Frequency Identification）等にシフトしているが、ＲＦＩＤの利用は、製品の在庫・流通の効率性の向上に留まらず、あらゆる製品に無線ＩＣチップを添付することで、社会のＩＴ化、自動化を推進する重要な技術として注目が集まってきている。例えば、購入した食品の産地や生産者、加工者等の情報を、ＲＦＩＤのデータを基に検索できるようにしたり、また、冷蔵庫に入れた食品のリストをＲＦＩＤにより自動作成し、消費期限を知らせたりするのに利用することが考えられている。これらを社会全般に浸透させて実現するためには、ＲＦＩＤを安価に供給し使用できるようにする必要がある。
【０００３】
ＲＦＩＤを安価に供給し使用できるようにするために、ＲＦＩＤには、製品のＩＤ情報等の識別情報のみを保持し、製品の生産者や流通経路の追跡情報等の製品に関する情報は、製品データベース（ＤＢ）サーバ等に記録し、製品ＩＤ情報により、製品に関する情報を参照する形式が、一つの有力な選択肢として考えられている。実際には、タグ・リーダ等から製品のＩＤ情報を読み取り、製品ＤＢサーバにＩＤ情報を送信して、その製品情報に関する情報にアクセスすることになる。この時、正しい権限所有者のアクセスを確保し、不正者による製品情報の取得、偽造製品の流通や、偽造品等によるトレーサビリティシステムの阻害を防止する必要がある。
【０００４】
特許文献１は、タグチップにタグアドレスとセキュリティブロックという２つの記憶領域を持たせ，通常ＲＦＩＤとして読み取られるタグアドレスに対しての認証を、２番目の

セキュリティブロックとの比較によって行う方法を示している。タグ・リーダは、まずタグ・アドレスを読み取ると、これを自ら保持している秘密鍵によって暗号化し、その結果とセキュリティブロックの値を比較することによって認証する。特許文献２は、認証情報をタグ自体に保管し，それによってリーダが所有者認証する方法が開示されている。顔画像、サインやパスワード情報をタグに保存し，ローカルに所有者認証をするものである。特許文献２は、ユーザと機密文書両方にＲＦＩＤを付与し、ユーザの持つＲＦＩＤのセキュリティレベルが機密文書に付加されたＲＦＩＤタグのセキュリティレベルより高いときに限りコピーなどができる仕組みを示している。特許文献４は、無線タグが、物品識別子と物品秘密鍵を格納し、物品秘密鍵等を利用して物品デジタル署名を作成し、認証者コンピュータに送信して認証してもらうことを示している。非特許文献１は、リーダのマルチアクセス機能を用いて、製品に付加されたＲＦＩＤの読み取りを、Ｂｌｏｃｋｅｒタグとよばれる別のＲＦＩＤタグによって制御する方法が示されている。

【０００５】

【特許文献１】特表２００３－５２４２４２号公報
【特許文献２】特開２００１－１８４３１２号公報
【特許文献３】特開２００１－１６０１７７号公報
【特許文献４】特開２００１－１６０１７７号公報
【非特許文献１】A.Juels and J.Brainard, “Soft Blocking: Flexible Blocker Tags on the Cheap,” URL：http://www.rsasecurity.com/rsalabs/staff/bios/ajuels/publications/softblocker/softblocker.pdf.

【発明の開示】

【発明が解決しようとする課題】

【０００６】

しかしながら、上記従来技術では、ＲＦＩＤタグの不正コピー等による、製品ＤＢへのアクセスを十分に防止できず、また、不正コピーが防止できても、コストがかかりすぎるという欠点がある。特許文献１では、タグアドレスとセキュリティブロックの両方をコピーしてタグを複製する攻撃に対しては無力である。また，常に同じタグアドレスとセキュリティブロックが使用されるので，リプレイ攻撃も簡単にできてしまう。特許文献２では、認証情報をタグ自体に保管するので、タグの所有者が変化しない銀行カードなどには適当であるが、流通業で使用される製品タグのように所有者が変化する用途には向かない。また、タグの記憶域やリーダ機能の増大を招き、安価にＲＦＩＤを利用することが困難になる。特許文献１と特許文献２で指摘される同様の問題は、特許文献４についても言える。特許文献３では、ユーザと機密文書両方にＲＦＩＤを付与しているが、流通過程で製品が移動する所有者移譲の仕組みや、リプレイアタックに対するセキュリティ対策がない。たとえば，不正者が別のタグ・リーダによって、ユーザ用のＲＦＩＤタグを読み取って同じものをコピーすれば、正規の利用者として振舞うことができてしまうという問題点が生じる。非特許文献１では、Ｂｌｏｃｋｅｒタグにより、タグ・リーダによるタグ情報の読み取りを制御するだけで、流通過程で製品が移動する場合に適応させるのは困難である。

【課題を解決するための手段】

【０００７】

上記課題を解決するために、本発明においては、　製品の識別子と、前記製品に係る権限の所有者の端末において保持される権限を認証するための第１の認証情報と、製品ＤＢ（データベース）に記憶される前記製品の識別子に係る権限を認証するための第２の認証情報とにより権限を認証する装置を提供する。前記装置は、前記識別子と、前記第１の認証情報を受け取る手段と、前記製品ＤＢから、前記第２の認証情報を取得する手段と、前記第１の認証情報と、前記第２の認証情報から、権限があるか否かを判定する手段と、を備える。別々に管理されている製品の識別子であるＲＦＩＤ等と、権限所有者を認証するための情報を、製品／サービスＤＢサーバで認証することで、ＲＦＩＤのコピーによる偽造製品が出てきても、不正者によるアクセスを防止し、偽造品等によるトレーサビリティシステムの阻害を安価に防ぐことができる。

【０００８】
また、本発明においては、　前記判定する手段が、認証情報の認証キーとして、所定の方法で得た数値に一方向ハッシュ関数をｔ（１以上の整数）回適用して得られるハッシュ値を使用することで判定し、次回の認証において、認証情報の認証キーとして前記数値に前記一方向ハッシュ関数をｔ－１回適用して得られるハッシュ値を使用して判定するので、いわゆるワンタイム認証キーで、認証キーの漏洩に対し、高度な安全性が確保できる。さらに、権限所有者の端末から、前記権限を認証するための認証情報を受取る場合に、前記ｔ－１回適用して得られるハッシュ値を暗号キーとすれば、さらに、安全性が高くなる。
【０００９】
なお、上記の発明の概要は、本発明の必要な特徴の全てを列挙したものではなく、これらの特徴群のサブコンビネーションもまた、発明となりうる。
【発明を実施するための最良の形態】
【００１０】
以下、発明の実施の形態を通じて本発明を説明するが、以下の実施形態は特許請求の範囲にかかる発明を限定するものではなく、また実施形態の中で説明されている特徴の組み合わせは、発明の内容を理解しやすくするためのものもあり、その全てが発明の解決手段に必須であるとは限らない。
【００１１】
図１は、製品／サービスに係る権限を認証するシステムが動作する環境の概略を示している。製品／サービス・データベース（ＤＢ）サーバ１０１は、製品／サービスに関する情報の送信要求に対応する。製品／サービスＤＢサーバは、製品に関する情報を要求する者の権限の認証を行い、また、製品／サービスに係る権限の移転処理も行う。製品／サービスＤＢ１０２は、製品またはサービスに関する情報を保持し、さらに権限を認証するための情報を保持している。このＤＢ１０２には、製品だけの情報でもよく、またサービスだけの情報でもよく、さらには、製品とサービスの両方の情報を登録していてもよい。製品／サービスＤＢサーバ１０１は、生産者または流通業者等が管理するサーバなので、複数存在する。また、製品／サービスに係る権限を所有する者が、過去の製品の流通経路や、サービスの履歴等を見る必要があるため、製品／サービスが市場を流通するに従って、同一の製品／サービスに係る情報が、複数の製品／サービスＤＢ１０２に存在する場合も発生することになる。製品／サービスＤＢは、製品に関する情報、またはサービスに関する情報、またはその両方の情報を保持している。ネットワーク１０３は、製品／サービスＤＢサーバ１０１、タグ・リーダ１０４またはユーザ端末１０７を通信回線で結びもので、有線、無線を問わず、通信ができれば特に限定されるものではない。
【００１２】
タグ・リーダ１０４は、製品／サービスＩＤ１０６や、認証情報１０８を読み取り、製品／サービスＤＢサーバ１０１に送信するためのもの機器である。タグ・リーダ１０４は、通信機能を持って、製品／サービスＤＢサーバ１０１に直接データを送受信してもよく、または、パソコンなどの通信機器を持ったものに接続されて単にデータを読み込むだけの機能を持つものでもよい。ここでは、タグ・リーダ１０４は、通信機能をもつ例を示している。そして、タグ・リーダ１０４は、製品／サービスに付加されたタグと、ユーザ端末に付加されているタグの両方を読むことができる、マルチ・タグ・リーダであることが望ましい。なお、マルチ・タグ・リーダは、読み取ったＩＤが、製品／サービスＩＤ、所有者ＩＤ（認証キー）、または後述する図６の譲受者の新所有者ＩＤ（認証キー）等のいずれかであるかの区別は、ＲＦＩＤコード等のヘッダ部で識別することで（例えば、製品／サービスＩＤ：00、所有者ＩＤ：01、新所有者ＩＤ：11）、容易に対応可能である。１０５は製品／サービス券であり、これは、市場を流通するような製品であってもよく、また例えば、サービスを受けるための、メンバーズ・カードやクーポン券であってもよい。
【００１３】
製品／サービス券１０５には、製品／サービスＩＤ１０６が添付され、当該製品、また

はサービスを特定するための識別子となっている。製品／サービスＩＤ１０６は、無線ＩＣタグ、ＲＦＩＤ、１次元バーコードまたは２次元バーコード等、製品／サービスを特定できる識別子であれば特に限定するものではない。製品／サービスＩＤ１０６は、製品には直接添付できるが、サービスには直接添付できないので、サービスの提供を受けるためのクーポン券やチケット等を含むサービス券等に付随することになる。また、サービス券は紙に印刷されたものの他、電子的なコードからなるものも含まれる。１０７は、ユーザ端末であり、所有権限を認証するための認証情報を含んでいる。この認証情報は、所有権限を認証する認証キーに関するもので認証情報１０８である。認証情報１０８は、製品またはサービスに関する所有権限を、製品／サービスＤＢで認証する際に使用される。ユーザ端末１０７は、ＰＤＡ（Personal Digital Assistance）や携帯電話でもよく、また、ノート型パソコンやデスクトップ・パソコン等の端末装置であればよい。ユーザ端末１０８は、製品／サービスＤＢサーバから、情報を取得する場合は、通信機能を備えていることが望ましい。また、ユーザ端末１０７は、タグ・リーダ１０４の機能と一体になったものでもよい。

【００１４】

図２は、製品／サービスＤＢサーバ１０１、またはユーザ端末のハード構成２００の概要である。中央演算処理装置であるＣＰＵ２０１は各種ＯＳの制御下で様々なプログラムを実行する。ＣＰＵ２０１はバス２０２を介して、メモリ２０３、ディスク２０４、ユーザ・インタフェース２０５およびネットワーク・インタフェース２０６と相互接続される。ユーザ・インタフェース２０５を通して、ディスプレイ装置２０７、キーボード２０８およびマウス２０９に接続され、ネットワーク・インタフェース２０６を通してネットワークに接続される。ユーザからの入力は、キーボード２０８およびマウス２０９以外に、タッチペン２１０からも行える。従って、２０８～２１０は、いずれかを備えていればよくすべてを必要としているわけではない。メモリ２０３は、主メモリやキャッシュ・メモリを含み、キャッシュ・メモリは、ディスク２０４等に保持される製品／サービスＤＢから検索された製品／サービスのデータや、所有者情報などを記憶するのに使用される。

【００１５】

ディスク２０４には、製品／サービスＤＢサーバで、製品／サービスに係る権限の認証処理等を行うプログラムが記憶されている。このプログラムがＣＰＵ２０１により主メモリに読み込まれ実行される。また、ディスク２０４には製品／サービスＤＢが保持される。製品／サービスＤＢは、製品／サービスに係る権限の認証処理等を行うプログラムと同一のディスクで保持される必要はないので、ディスク２０４は複数存在する場合もある。また、ハード構成２００がユーザ端末である場合は、ディスク２０４には、ユーザ端末で動作するプログラムが記録され、認証情報も保持されている。そして、ユーザ端末がタグ・リーダと一体となっている場合は、タグ・リーダ２１１がバス２０２に接続される。

【００１６】

ユーザ端末がＰＤＡである場合は、通常はキーボード２０８とマウス２０９がなくて、タッチペン２１０での入力となる。また、ユーザ端末が携帯電話である場合は、キーボード２０８が携帯電話のプッシュボタンで代用される。製品／サービスＤＢサーバとユーザ端末が直接データをやり取りする場合は、ネットワーク・インタフェース２０６を利用する。ここで開示したハード構成２００は、コンピュータ・システムおよびバス配置の一実施形態の例にすぎず、本発明の特徴は、さまざまなシステム構成で、同一の構成要素を複数有する形態で、または、ネットワーク上に分散された形態でも実現することができる。

【００１７】

図３は、製品／サービスＤＢサーバ３００および、ユーザ端末３５０の機能を模式的に示したものである。まず、製品／サービスＤＢ３００から説明する。３０１はユーザ端末やタグ・リーダとデータの送受信を行うためのインタフェースである。ブロックを模式的に示している。３０２はハッシュ関数を用いてハッシュ値を計算するハッシュ値計算部である。ハッシュ値計算部３０２で使用されるハッシュ関数は、一方向ハッシュ関数が望ましい。３０３は、排他的論理和を計算するための排他的論理和エンコーダである。また、

排他的論理和エンコーダ３０３は、排他的論理和で暗号化されたタグ・リーダやユーザ端末から受取った認証キー等に関するデータから、秘密鍵等を用いてデコードもする。

【００１８】

３０４は、製品／サービスに係る権限保有を認証する権限認証部である。所有権限判定部３０４は、ユーザ端末に保持される認証キー等（第１の認証情報）と、製品／サービス情報検索部３０５から受取った認証キー等（第２の認証情報）を用いて所有権限の有無を判定する。製品／サービス情報検索部３０５は、製品／サービスＤＢ３０６にアクセスするためのＤＢＭＳ（DataBase Management System）である。製品／サービスＤＢ３０６は、製品／サービスＩＤ３１１、権限の認証キー３１２や、製品／サービスの属性、名称等の製品／サービス関連情報３１３が含まれる。

【００１９】

次に、ユーザ端末３５０の機能について説明する。インタフェース３５１は、製品／サービスＤＢサーバとデータをやり取りするための、インタフェースである。インタフェース３５１は、ユーザ端末にタグ・リーダが付いている場合は、タグから読み取ったＩＤ等を製品／サービスＤＢに送信し、また、製品／サービスＤＢサーバから送られてくる製品／サービスに関する情報を受取るときに使用される。３５２はハッシュ関数を用いてハッシュ値を計算するハッシュ値計算部である。ハッシュ値計算部３５２で使用されるハッシュ関数は、製品／サービスＤＢサーバと同様に一方向ハッシュ関数が望ましい。３５３は、排他的論理和を計算するための排他的論理和エンコーダである。また、排他的論理和エンコーダ３５３は、製品／サービスＤＢから受取った排他的論理和により暗号化された製品／サービス関連情報等のデータをデコードする。

【００２０】

３５４は、タグ・リーダである。タグ・リーダ３５５は、ユーザ端末に必須ではなく、付近にあるタグ・リーダから、製品／サービスＩＤと、権限の認証キーを読み込む形態でもよい。３５５は、ユーザ端末のディスク（記憶装置）である。ここには、所有権限を証明するための、製品／サービスＩＤ３６１と、一方向ハッシュ値を適用する数値Ｓ（乱数等で作成）３６２、ハッシュ関数の適用回数ｔ３６２を保持する。３６１～３６２は、ユーザ端末１台で複数の製品／サービスに対応可能とするために、複数のレコードが製品／サービスごとに存在する。なお、製品／サービスＩＤが複数存在しても、製品／サービスＩＤのＭＡＣ（ハッシュの短いもの、あるいはチェックサムでもよい）等を認証キーの一部に採用するようにすれば、タグ・リーダ３７１は、容易に製品／サービス毎に、認証キーを識別できる。このように、ユーザ端末３５０は、ディスク３５５の情報を用いて、製品／サービスごとに認証キーの作成を行うなどして、認証情報を管理している。通常は、マルチ・タグ・リーダ３７１が、製品／サービス券に付随する、製品／サービスＩＤ３７２と、ユーザ端末３５０で管理される認証情報を読み込む。ちなみに、図３は各機能をブロックで表し配置しているが、各機能のブロック化は様々範囲で行い得るので、これらの機能を結果的に有すれば、他の機能ブロック形態で実現されてもよく、このブロック構成に限定されるものではない。

【００２１】

図４は、製品／サービスに係る所有権限認証の基本概要を説明したものである。権限の認証は、一方向ハッシュ関数を用いたワンタイム認証キーを用いる、いわゆるＳ／Ｋｅｙ認証方式を用い、さらに、認証キーを伝送する場合、安全のため、排他的論理和による暗号化を行う。一方向ハッシュ関数とは、ある値にハッシュ関数を適用して得たハッシュ値から、ハッシュ関数を適用するまえの値（ある値）を求めることができないハッシュ関数である。その認証方式の内容は、図４に概略する。ｔを１以上の整数とした場合に、T^{old}は、乱数Ｓに一方向ハッシュ関数ｈをｔ回適用したもので、$T^{old}=h^{t}(S)$となる。ここでは、Ｓを乱数としているが、予め決められた数値等を含む所定の方法で得られた数値でもよい。

【００２２】

ｈは一方向ハッシュ関数なので、ハッシュ値から、ハッシュ関数を適用する前の数値を

求めることはできない。そして、T^{new}を、ハッシュ関数ｈにｔ－１回適用したものとすると、$T^{new}=h^{t-1}$（Ｓ）となる。また、$T^{old}=h(T^{new})$となり、T^{new}にハッシュ関数ｈを１回適用したものが、T^{old}となる。これは、T^{new}からT^{old}を求められるが、逆にT^{old}からT^{new}は求められないことを意味している。ここで、ユーザおよび認証者は、T^{old}を認証キーとして使用する（ブロック４０１、４５１）。実際には、ユーザは、乱数Ｓとハッシュ関数の適用回数ｔを保持する。ブロック４５２で、ユーザは認証キー、暗号キーおよびそれらの排他的論理和を計算し、認証者に送信する。認証キーT^{old}は乱数Ｓから、ハッシュ関数ｈをt回適用した値h^{t}（Ｓ）で求める。また、ユーザは認証キーT^{old}を暗号化するために、$T^{new}=h^{t-1}$（Ｓ）を求め、T^{old}とT^{new}との排他的論理和$E_T=(T^{new}\ \mathrm{xor}\ T^{old})$をさらに求めて、認証者に送信する。

【００２３】

認証者はブロック４０２で認証処理を行う。認証者は、保持している認証キーT^{old}で、排他的論理和$E_T\ \mathrm{xor}\ T^{old}=T^{new}\ \mathrm{xor}\ T^{old}\ \mathrm{xor}\ T^{old}=T^{new}$を求める。そして、$T^{new}$にハッシュ関数を１回適用したｈ（$T^{new}$）から$T^{old}$を求めて、サーバが保持する$T^{old}$と比較し一致すれば、認証する。次に、サーバとユーザはT^{new}を認証キーとして使用する（ブロック４０３、４５３）。実際には、ユーザは、乱数Ｓとハッシュ関数の適用回数ｔを保持する。次回の認証処理（ブロック４３０）が終了すると、新たな認証キーは、Ｔ（＝h^{t-2}（Ｓ））となる（ブロック４０４、４５４）。さらにその次の認証キーはＴ（＝h^{t-3}（Ｓ））となる。このように毎回新しい認証キーを用いて認証していく。その際に、古い認証キーが漏洩しても、新しい認証キーは、古い認証キーから求めることはできないので、安全性は高く確保できる。

【００２４】

図５は、製品／サービスＤＢサーバと、ユーザ端末で行われる、製品／サービスに係る所有権限の認証処理フロー５００を示したものである。左側がユーザ端末、右側が製品／サービスＤＢサーバの処理を示している。ステップ５５１で処理が開始される。ステップ５５２でT_A^{new}とT_A^{old}を取得する。ここでは、図３のユーザ端末のハッシュ値計算部３５２が、ハッシュ関数ｈ、ｔ（１以上の整数）および乱数S_Aを用いて、T_A^{new}とT_A^{old}を計算する。T_A^{old}は、S_Aにハッシュ関数をｔ回適用した値である。また、T_A^{new}は、S_Aにハッシュ関数を（ｔ－１）回適用した値である。ステップ５５３で、製品／サービスＩＤとともに、T_A^{new}とT_A^{old}の排他的論理和E_Tを計算して、製品／サービスＤＢサーバに送信する。この送信は、通常はマルチ・タグ・リーダが行うことになる。排他的論理和E_Tの計算は、T_A^{old}の暗号化処理になる。このステップ５５３は、タグ・リーダがユーザ端末と別個になっているものでは、送信処理の部分はタグ・リーダが行うことになる。

【００２５】

その後、処理は製品／サービスＤＢサーバに移る。ステップ５０１で、製品／サービスＩＤを検索キーとして、製品／サービスＤＢから該当する認証キー（T_A^{old}）を検索する。ステップ５０２で、該当する製品／サービスＩＤが存在するか否か判断する。該当する製品／サービスＩＤがないと判断される場合（Ｎｏ）、ステップ５０３で該当する製品／サービスＩＤがない旨を、ユーザ端末に送信する。ユーザ端末では、ステップ５５４で、該当する製品／サービスＩＤが無い旨を受信し、ステップ５５８に進み、処理を終了する。一方、ステップ５０２で、該当する製品／サービスＩＤがあると判断される場合（Ｙｅｓ）、すなわち、認証に成功したことに応答して、ステップ５０４に進む。ステップ５０４で、検索した認証キー（T_A^{old}）と、E_Tの排他的論理和からT_A^{new}を求めて、これにハッシュ関数を適用した値と、検索された認証キー（T_A^{old}）とが、一致するか否かを判断する。一致しないと判断される場合（Ｎｏ）、ステップ５０５に進み、所有者権限が無い旨を、ユーザ端末に送信する。

【００２６】

ユーザ端末はステップ５５５で、所有者権限が無い旨を受信し、ステップ５５８に進んで処理を終了する。ステップ５０４で、一致すると判断される場合は（Ｙｅｓ）、ステッ

プ５０６に進み、新たな認証キーにT_A^{new}を設定し、製品／サービスに係る情報等に必要な暗号化処理をして、ユーザ端末に送信する。ここでの暗号化処理は、T_A^{new}またはT_A^{old}で排他的論理和を求めるものが好ましい。なお、T_A^{new}で排他的論理和を計算する暗号化処理にすると、ユーザ端末はサーバ側が正しくT_A^{new}を計算できたことを確認できる。ユーザ端末では、ステップ５５６で製品／サービスに係る情報等を取得し、必要な複合化処理をする。次にステップ５５７で、認証キーをT_A^{new}に置き換えるが、ここでは、実際にはハッシュ適用回数をｔ－１で記憶すれば次回の認証キーがT_A^{new}になるのと同じことである。ステップ５５８で処理を終了する。この処理フロー５００では、製品／サービスＤＢサーバにおいて、S_Aを持つ必要はなく、T_A^{old}のみ保持していれば、ユーザ端末（タグ・リーダ）から送られてきたE_Tから、T_A^{new}も求めることができる。

【００２７】

図６は、製品／サービスに係る所有権限を移転する処理フローを示したものである。所有権限の移転は、ユーザＡ（譲渡者）からユーザＢ（譲受者）に移転する場合を想定している。従って、所有権限の移転処理を開始する前は、ユーザＡが所有権限を有していて、製品／サービスＤＢには、ユーザＡの認証情報（認証キー：T_A^{old}）が入っている。ユーザＡから、製品／サービスに係る所有権限の移転を承諾されたユーザＢのユーザ端末は、ステップ６８１で処理を開始する。ステップ６８２で、乱数等を使ってS_Bを求める。S_Bにハッシュ関数ｈをｕ（１以上の整数）回適用して、T_B^{new}を計算する。ステップ６８３で、所有権の移転を承諾しているユーザＡのユーザ端末に送信する。

【００２８】

ステップ６５１で、ユーザＡのユーザ端末は、ユーザＢのユーザ端末から、T_B^{new}を受信する。ステップ６５２で、ハッシュ関数ｈ、ｔおよびS_Aを用いて、T_A^{new}とT_A^{old}を計算する。T_A^{old}はS_Aにハッシュ関数ｈをｔ回適用し、T_A^{new}はS_Aにハッシュ関数ｈをｔ－１回適用して求める。ステップ６５３で、T_A^{new}とT_A^{old}の排他的論理和E_{TA}を求め、T_B^{new}とT_A^{old}の排他的論理和E_{TB}を求めて、所有権限の移転に係る製品／サービスＩＤと共に、製品／サービスＤＢサーバに送信する。この送信は、マルチ・タグ・リーダが行ってもよい。ステップ６０１で、製品／サービスＩＤを検索キーとして、製品／サービスＤＢから該当する認証キー（T_A^{old}）を検索する。ステップ６０２で、該当する製品／サービスＩＤが存在するか否か判断する。該当する製品／サービスＩＤが存在しないと判断した場合（Ｎｏ）、ステップ６０３に進み、製品／サービスＩＤが無い旨を送信する。ユーザＡのユーザ端末およびユーザＢのユーザ端末は、ステップ６５４とステップ６８４で、通知を受信して終了する。一方、ステップ６０２で、該当する製品／サービスＩＤが存在すると判断した場合（Ｙｅｓ）、ステップ６０４に進む。

【００２９】

ステップ６０４では、検索した認証キー（T_A^{old}）と、E_{TA}の排他的論理和からT_A^{new}を求めて、ハッシュ関数を１回適用した値と、検索された認証キー（T_A^{old}）とが、一致するかを判断する。一致しないと判断される場合（Ｎｏ）、ステップ６０５に進み、所有者権限が無い旨または該当なしを、ユーザＡのユーザ端末とユーザＢのユーザ端末に送信する。ユーザＡのユーザ端末およびユーザＢのユーザ端末は、ステップ６５４とステップ６８４で、通知を受信して終了する。一方、ステップ６０４で、一致すると判断される場合（Ｙｅｓ）、すなわち、認証に成功したことを条件として、ステップ６０６に進み、T_A^{old}とE_{TB}の排他的論理和からT_B^{new}を求めて、新たな認証キーにT_B^{new}を設定する。ステップ６０７で、完了した旨を、ユーザＡのユーザ端末とユーザＢのユーザ端末に送信する。ユーザＡのユーザ端末およびユーザＢのユーザ端末は、ステップ６５４とステップ６８４で、通知を受信して終了する。

【００３０】

処理フロー６００により、セキュリティを保ったまま、ユーザＡからユーザＢに所有権限の移転をすることができる。また、正規の権限所有者ユーザＡのみしか、他者にその所有権限を移転することができない。そして、製品／サービスＤＢに、製品／サービスに係る情報のレコードが記録される最初の段階において、製品／サービスに係る権限の所有者

を、製品／サービスＤＢサーバと同一にしておけば、すなわち、ユーザＡを製品／サービスＤＢサーバにしておいて、実際に製品等を顧客（ユーザＢ）に移転する場合に、この処理フロー６００を利用すれば、製品／サービスを簡単に流通過程に移すことができる。さらに、異なる会社の製品／サービスＤＢサーバ間でのデータ移転も、この処理フロー６００を用いて行うことができる。例えば、製造業者を、ユーザＡとして、流通業者をユーザＢとすれば、セキュリティを保ったまま所有権限を移転することができる。

【００３１】

ワンタイム認証情報は、乱数Ｓにｔ回ハッシュ関数を適用した認証キーを使用し、その次には、ｔ－１回ハッシュ関数を適用した認証キーを使用する。さらに、その次は、ｔ－２回ハッシュ関数を適用した認証キーを使用することになる。認証の回数が増えれば、ハッシュ関数の適用回数が最終的に０になってしまう。この場合、処理フロー６００を用いて、リセットすることが可能である。これは、単にユーザＡとユーザＢの処理を同一ユーザ端末内で行うだけでよい。これにより、新しい乱数に整数回ハッシュ関数を適用した認証キーを採用して、再び認証が可能となる。

【００３２】

実施の形態を変形した応用例を説明する。図７は、応用例で使用される製品／サービスＤＢの概要７００である。図３の製品／サービスＤＢ３０６を一部変更している。一つの製品／サービスにつき、複数のユーザがアクセスする場合過去の履歴を見る必要がある場合には、製品／サービスＤＢには、オーナー・リストの項目を儲け、各オーナーの認証キーを別に持つ形態が考えられる。７０１は、製品／サービスＩＤである。７０２はオーナー・リストで、複数のオーナーを入れることが可能になっている。７０３は、製品／サービスに関連する情報である。７０４は、各オーナーの認証キーを管理するテーブルである。製品／サービスＤＢ７００の構成により、一つの製品／サービスにつき、各オーナーの認証キーを、共同オーナーに知られることなく、それぞれが、セキュリティを保って、製品／サービスに関する情報にアクセスすることができる。

【００３３】

図８は、ユーザ端末が、製品／サービスＩＤと認証キーの両方を保持する応用例である。ここでは、ユーザ端末が、図１の製品／サービスＩＤ１０６と認証情報１０８の両方を持つ形態になる。ユーザ端末８０１は、製品／サービスＩＤ８０２と、認証情報８０３を保持する。この形態で特に便利なのは、製品／サービスが、電子チケット等の場合である。製品／サービスＩＤが、電子チケット等であれば、製品／サービスＩＤを、ユーザ端末に持つことも可能である。現在、携帯電話に電子チケットの機能を持った形態が広がりつつある。この応用形態により、チケット販売所から、また、インターネットからでも、直接電子チケットを購入することができ、また、ユーザ間での流通も高度なセキュリティを保ったまま可能になる。この電子チケットの購入は、図６のフロー６００を利用すれば、容易に行える。ステップ６０７からユーザＢのユーザ端末に通知する際に、電子チケットの情報を含めればいいだけである。

【００３４】

また、一時的に、ユーザＡからユーザＢに所有権限を移転する場合、例えば、ユーザＡが長期に出張し、その期間ユーザＢに、製品等の管理を任せる場合等は、処理フロー６００を用いて所有権限を移転し、時限的に認証キーをT_B^{old}として、所定時間経過後に認証キーがT_A^{new}に戻るようにする応用例も可能である。ここで、認証キーがT_A^{old}に戻るのではなくT_A^{new}になるのは、T_A^{old}はユーザＡからユーザＢに所有権限を移転する際に使用したため、ワンタイム認証キーとしては、もう使用できないからである。

【００３５】

また、製品／サービスＤＢサーバを持たない製造業者などは、第三者の管理する製品／サービスＤＢに登録する必要があるが、この場合は、製品／サービスＩＤ、認証キーや製品／サービスの属性等を、ユーザ端末から送信して登録できるようにしてもよい。

【００３６】

以上、本発明を実施の形態を用いて説明したが、本発明の技術的範囲は上記実施の形態

に記載の範囲には限定されない。上記実施の形態に、多様な変更または改良を加えることが可能であることが当業者に明らかである。その様な変更または改良を加えた形態も本発明の技術的範囲に含まれ得ることが、特許請求の範囲の記載から明らかである。

【図面の簡単な説明】

【００３７】

【図１】製品／サービスに係る権限を認証するシステムの概略を示す。

【図２】製品／サービスＤＢサーバ、またはユーザ端末のハード構成図の一例を示す。

【図３】製品／サービスＤＢサーバおよび、ユーザ端末の機能の機能ブロック図の一例を示す。

【図４】製品／サービスに係る所有権限認証の基本概要を示す。

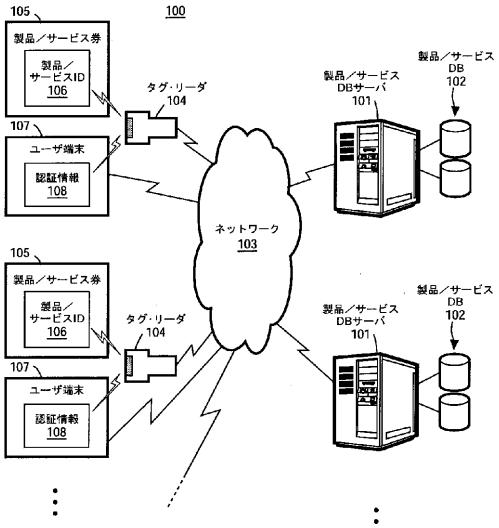
【図５】製品／サービスＤＢサーバと、ユーザ端末で行われる、製品／サービスに係る所有権限の認証処理フローの一例を示す。

【図６】製品／サービスに係る所有権限を移転する処理フローの一例を示す。

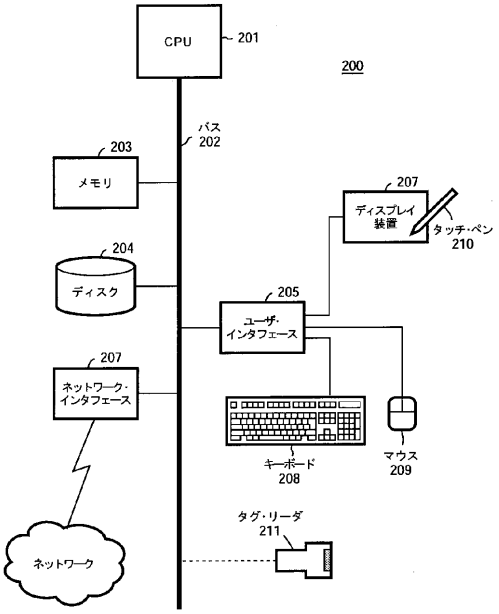
【図７】応用例で使用される製品／サービスＤＢの概要を示す。

【図８】ユーザ端末が、製品／サービスＩＤと認証キーの両方を保持する例を示す。

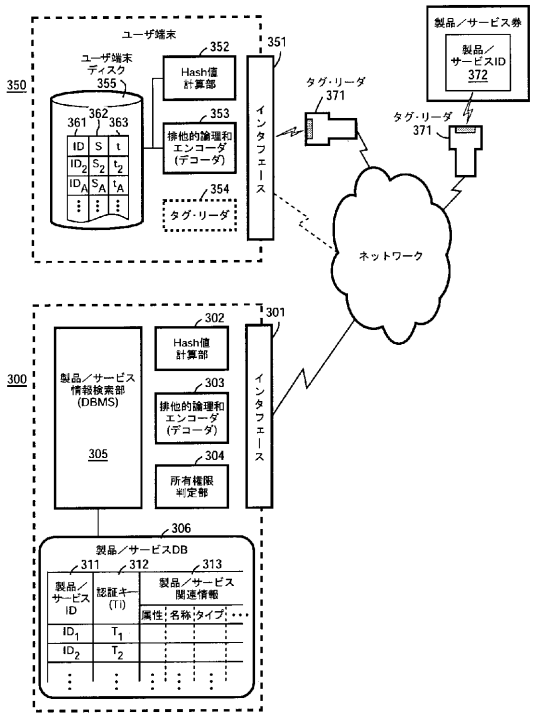
【図１】



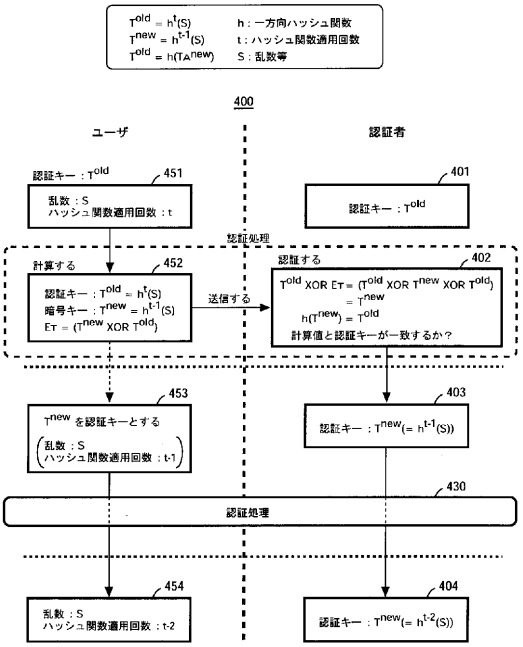
【図２】



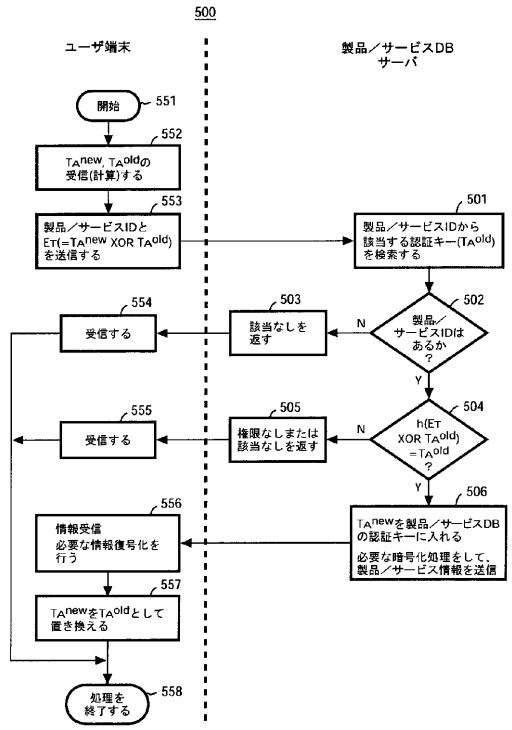
【図３】


ユーザ端末
ユーザ端末ディスク
Hash値計算部
排他的論理和エンコーダ(デコーダ)
タグ・リーダ
インタフェース
製品／サービス券
製品／サービスID
タグ・リーダ
タグ・リーダ
ネットワーク
製品／サービス情報検索部(DBMS)
Hash値計算部
排他的論理和エンコーダ(デコーダ)
所有権限判定部
インタフェース
製品／サービスDB
製品／サービスID
認証キー(Ti)
製品／サービス関連情報
属性
名称
タイプ

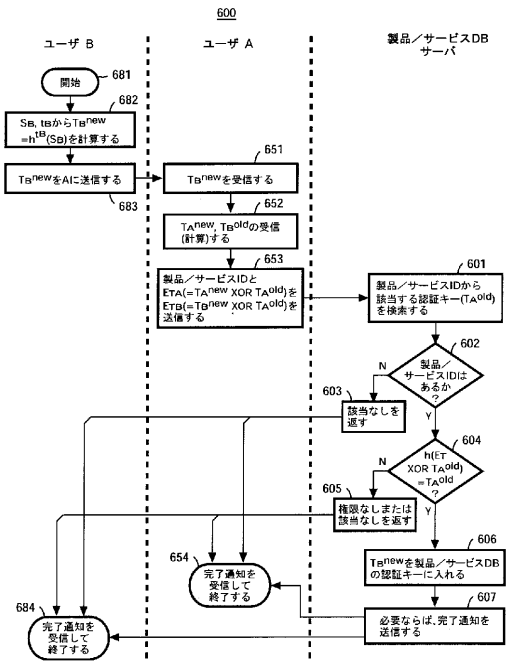
【図４】


h：一方向ハッシュ関数
t：ハッシュ関数適用回数
S：乱数等
ユーザ
認証者
認証キー：Told
乱数：S
ハッシュ関数適用回数：t
認証キー：Told
認証処理
計算する
認証する
認証キー：Told = ht(S)
暗号キー：Tnew = ht-1(S)
ET = (Tnew XOR Told)
送信する
Told XOR ET = (Told XOR Tnew XOR Told) = Tnew
h(Tnew) = Told
計算値と認証キーが一致するか？
Tnewを認証キーとする
乱数：S
ハッシュ関数適用回数：t-1
認証キー：Tnew(= ht-1(S))
認証処理
乱数：S
ハッシュ関数適用回数：t-2
認証キー：Tnew(= ht-2(S))

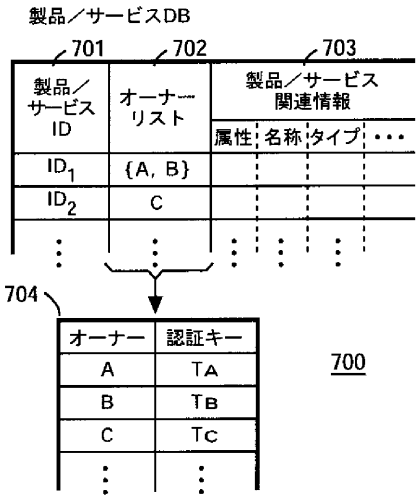
【図５】


ユーザ端末
製品／サービスDBサーバ
開始
TAnew, TAoldの受信(計算)する
製品／サービスIDとET(=TAnew XOR TAold)を送信する
製品／サービスIDから該当する認証キー(TAold)を検索する
製品／サービスIDはあるか？
該当なしを返す
受信する
h(ET XOR TAold) =TAold ？
権限なしまたは該当なしを返す
受信する
TAnewを製品／サービスDBの認証キーに入れる
必要な暗号化処理をして、製品／サービス情報を送信
情報受信
必要な情報復号化を行う
TAnewをTAoldとして置き換える
処理を終了する

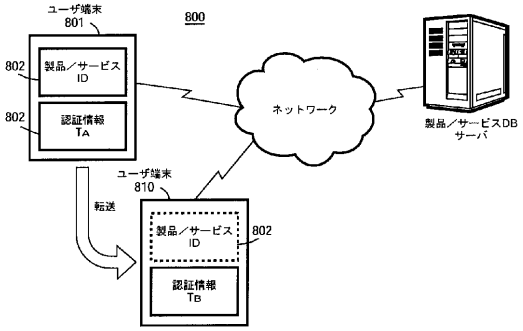
【図６】


ユーザ B
ユーザ A
製品／サービスDBサーバ
開始
SB, tBからTBnew =htB(SB)を計算する
TBnewをAIに送信する
TBnewを受信する
TAnew, TBoldの受信(計算)する
製品／サービスIDとETA(=TAnew XOR TAold)をETB(=TBnew XOR TAold)を送信する
製品／サービスIDから該当する認証キー(TAold)を検索する
製品／サービスIDはあるか？
該当なしを返す
h(ET XOR TAold) =TAold ？
権限なしまたは該当なしを返す
完了通知を受信して終了する
TBnewを製品／サービスDBの認証キーに入れる
必要ならば、完了通知を送信する
完了通知を受信して終了する

【図７】


製品／サービスDB
701
702
703
製品／サービスID
オーナーリスト
製品／サービス関連情報
属性
名称
タイプ
ID1
{A, B}
ID2
C
704
オーナー
認証キー
A
TA
B
TB
C
TC
700

【図８】


ユーザ端末
801
800
802
製品／サービスID
認証情報
TA
ネットワーク
製品／サービスDBサーバ
ユーザ端末
810
転送
製品／サービスID
802
認証情報
TB

フロントページの続き

(72)発明者　沼尾　雅之
神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　東京基礎研究所内
(72)発明者　石垣　良信
神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　東京基礎研究所内
(72)発明者　渡邊　裕治
神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　東京基礎研究所内

審査官　青木　重徳

(56)参考文献　特開２００３－０９９６６２（ＪＰ，Ａ）
特開平１１－２９６０７６（ＪＰ，Ａ）
渡邊裕治，吉澤武郎，百合山まどか，沼尾雅之，“個人の選択を考慮したプライバシー保護のための情報管理”，コンピュータセキュリティシンポジウム２００４論文集　Ｖｏｌｕｍｅ　１ｏｆ　２，日本，社団法人情報処理学会，２００４年10月20日，Ｖｏｌ．２００４，Ｎｏ．１１，ｐ．１４５－１５０，情報処理学会シンポジウムシリーズ
木下真吾，星野文学，小室智之，藤村明子，大久保美也子，“ローコストＲＦＩＤプライバシ保護方法”，情報処理学会論文誌，日本，社団法人情報処理学会，２００４年　8月１５日，第４５巻，第8号，ｐ．２００７－２０２１
沼尾雅之，渡邊裕治，“ＲＦＩＤトレーサビリティのための所有権移転可能な所有者認証方法”，２００５年暗号と情報セキュリティシンポジウム　ＳＣＩＳ２００５　予稿集付録ＣＤ－ＲＯＭ，２００５年　1月２５日
沼尾雅之，渡邊裕治，石垣良信，“流通トレーサビリティにおけるセキュリティの考察”，２００６年暗号と情報セキュリティシンポジウム　ＳＣＩＳ２００６　予稿集ＣＤ－ＲＯＭ，日本，２００６年暗号と情報セキュリティシンポジウム実行委員会事務局，２００６年　1月１７日

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／３２
Ｇ０６Ｋ　１７／００
Ｇ０６Ｆ　２１／２０