(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6069876号
(P6069876)
(45)発行日　平成29年2月1日(2017.2.1)　(24)登録日　平成29年1月13日(2017.1.13)

(51)Int.Cl.		F I		
H04L 9/10	(2006.01)	H04L	9/00	621Z
G06F 21/44	(2013.01)	G06F	21/44	
G06K 19/10	(2006.01)	G06K	19/10	

請求項の数 4　(全 17 頁)

(21)出願番号　特願2012-87659(P2012-87659)
(22)出願日　平成24年4月6日(2012.4.6)
(65)公開番号　特開2013-218483(P2013-218483A)
(43)公開日　平成25年10月24日(2013.10.24)
審査請求日　平成27年3月19日(2015.3.19)

前置審査

(73)特許権者　000003193
凸版印刷株式会社
東京都台東区台東１丁目５番１号
(72)発明者　小林　燃
東京都台東区台東１丁目５番１号　凸版印刷株式会社内
(72)発明者　横山　貴一
東京都台東区台東１丁目５番１号　凸版印刷株式会社内
(72)発明者　荒井　和重
東京都台東区台東１丁目５番１号　凸版印刷株式会社内
(72)発明者　増永　優作
東京都台東区台東１丁目５番１号　凸版印刷株式会社内

最終頁に続く

(54)【発明の名称】ＩＣチップ認証システム

(57)【特許請求の範囲】
【請求項１】
ＩＣチップと、上記ＩＣチップと通信手段を介して情報の授受を行い上記ＩＣチップの正当性を認証する認証装置と、を備えるＩＣチップ認証システムであって、
上記ＩＣチップは、当該ＩＣチップに固有の情報である固有情報、及びＰＵＦ回路を有し、
上記認証装置は、上記ＰＵＦ回路の特徴が上記固有情報に対応したデータに紐付けられた状態で記憶された記憶装置を備え、
更に、上記認証装置は、上記ＩＣチップから上記固有情報とチャレンジを入力すると、入力した固有情報に対応する上記ＰＵＦ回路の特徴と入力したチャレンジとから、上記ＩＣチップが有するＰＵＦ回路が返すと推定されるレスポンスを計算して上記ＩＣチップに向けて送信するレスポンス計算手段を有し、
上記ＩＣチップは、上記認証装置に上記固有情報とチャレンジを送信する送信手段と、上記レスポンス計算部が送信したレスポンスと、上記チャレンジを上記ＰＵＦ回路に与えて得たレスポンスとを比較することで、上記認証装置が正当であるかどうか検証する認証装置検証部とを備えることを特徴とするＩＣチップ認証システム。
【請求項２】
上記認証装置は、
上記記憶装置に記憶されているＰＵＦ回路の特徴をパラメータの一つとして認証情報を生成する認証情報生成手段と、認証情報生成手段が生成した認証情報を上記ＩＣチップに

送信する認証情報送信手段と、を備え上記認証情報を記憶する
ことを特徴とする請求項１に記載したＩＣチップ認証システム。
【請求項３】
　ＩＣチップは、チャレンジを受信すると該受信したチャレンジを上記ＰＵＦ回路に与えてレスポンスを取得し該取得したレスポンスを送信するレスポンス送信手段を備え、
　上記認証装置は、
　チャレンジを生成してＩＣチップに送信するチャレンジ送信手段と、
　ＩＣチップから受信したレスポンスと、上記チャレンジ送信手段が送信したチャレンジと上記ＩＣチップに紐付けられたＰＵＦ回路の特徴とに基づくレスポンスとの比較によってＩＣチップの正当性を検証する正当性検証手段と、を備えることを特徴とする請求項１又は請求項２に記載したＩＣチップ認証システム。
【請求項４】
　ＩＣチップ内の情報を読み取り及び書き込みを行うリーダライタ装置を備え、ＩＣチップと認証装置とは、リーダライタ装置を介して情報の授受を行うことを特徴とする請求項１～請求項３のいずれか１項に記載のＩＣチップ認証システム。
【発明の詳細な説明】
【技術分野】
【０００１】
　本発明は、ＩＣチップの正当性を検証する認証技術に関する。
【背景技術】
【０００２】
データの書換えが可能なＩＣチップは、様々な用途に用いられる。ＩＣチップは、例えば、ＩＣタグやＩＣカードなどの形式で、クレジット機能や、電子マネーなどに用いることも検討されており、ＩＣチップの不正利用を防ぐことは重要な課題である。
　上記課題に対応した従来のＩＣチップ認証システムとしては、例えば特許文献１や特許文献２に記載の技術がある。
【０００３】
　特許文献１に記載の技術は、各ＩＣタグに固有の情報であり、書き換えの出来ない固有情報と、タイムスパンとを用いて生成された認証情報をＩＣタグ内に保持することで、ＩＣタグ内の認証情報の一意性を確保する。
　特許文献２に記載の技術は、認証されることになるＰＵＦデバイスが、実際に認証された認証装置から問い合わせを受けているかどうかを確認する。例えば、ＰＵＦを有するＲＦＩＤタグが、銀行が認証を行いたい紙幣に配置される。この認証は、暗号化されたデータを復号化する銀行のユニークな能力に基づかれる。暗号化されたデータは、例えば、そのＲＦＩＤタグ（又は実際にはＰＵＦ）が銀行に登録される登録フェーズにおいて作成されたデータである。ここで、認証装置に送られるレスポンスデータを作成するためＲＦＩＤタグは再度、ＰＵＦにチャレンジする。認証装置は、そのレスポンスデータが正しいかどうかチェックし、もし正しければ、その物理トークンを有するデバイスを認証する。これによって、そのデバイスは、登録フェーズで暗号化されて格納されたレスポンスデータに対応するレスポンスデータを生成できることになる。
　また　特許文献３には、ＰＵＦを用いた技術が開示されている。
【先行技術文献】
【特許文献】
【０００４】
【特許文献１】特許第４８４３９６０号公報
【特許文献２】特表２００９－５３３７４２号公報
【特許文献３】特開２０１１－１９８３１７号公報
【発明の概要】
【発明が解決しようとする課題】
【０００５】

特許文献１の技術では、ＩＣチップ毎複製された場合、正当性の検出が出来ないという課題がある。特許文献２の技術では、認証に使用できるのは予め登録された２つのチャレンジのみでアタックを受けやすいという課題がある。また、特許文献３では、動的パラメータを用いるため、測定に時間がかかる、特別な装置が必要などの課題がある。

本発明は、上記のような点に着目してなされたもので、個人情報も含めＩＣチップごと複製された場合でもタグの正当性の検証が可能な認証システムを提供することを目的とする。

【課題を解決するための手段】

【０００６】

上記課題を解決するために、本発明のうち請求項１に記載の発明は、ＩＣチップと、上記ＩＣチップと通信手段を介して情報の授受を行い上記ＩＣチップの正当性を認証する認証装置と、を備えるＩＣチップ認証システムであって、

上記ＩＣチップは、当該ＩＣチップに固有の情報である固有情報、及びＰＵＦ回路を有し、

上記認証装置は、上記ＰＵＦ回路の特徴が上記固有情報に対応したデータに紐付けられた状態で記憶された記憶装置を備え、

更に、上記認証装置は、上記ＩＣチップから上記固有情報とチャレンジを入力すると、入力した固有情報に対応する上記ＰＵＦ回路の特徴と入力したチャレンジとから、上記ＩＣチップが有するＰＵＦ回路が返すと推定されるレスポンスを計算して上記ＩＣチップに向けて送信するレスポンス計算手段を有し、

上記ＩＣチップは、上記認証装置に上記固有情報とチャレンジを送信する送信手段と、上記レスポンス計算部が送信したレスポンスと、上記チャレンジを上記ＰＵＦ回路に与えて得たレスポンスとを比較することで、上記認証装置が正当であるかどうか検証する認証装置検証部とを備えることを特徴とする。

【０００７】

次に、請求項２に記載した発明は、請求項１に記載した構成に対し、上記認証装置は、

上記記憶装置に記憶されているＰＵＦ回路の特徴をパラメータの一つとして認証情報を生成する認証情報生成手段と、認証情報生成手段が生成した認証情報を上記ＩＣチップに送信する認証情報送信手段と、を備え、

上記ＩＣチップは、認証装置からの上記認証情報を記憶することを特徴とする。

【０００８】

次に、請求項３に記載した発明は、請求項１又は請求項２に記載した構成に対し、ＩＣチップは、チャレンジを受信すると該受信したチャレンジを上記ＰＵＦ回路に与えてレスポンスを取得し該取得したレスポンスを送信するレスポンス送信手段を備え、

上記認証装置は、

チャレンジを生成してＩＣチップに送信するチャレンジ送信手段と、

ＩＣチップから受信したレスポンスと、上記チャレンジ送信手段が送信したチャレンジと上記ＩＣチップに紐付けられたＰＵＦ回路の特徴とに基づくレスポンスとの比較によってＩＣチップの正当性を検証する正当性検証手段と、を備えることを特徴とする。

【０００９】

次に、請求項４に記載した発明は、請求項１～請求項３のいずれか１項に記載の構成に対し、ＩＣチップ内の情報を読み取り及び書き込みを行うリーダライタ装置を備え、ＩＣチップと認証装置とは、リーダライタ装置を介して情報の授受を行うことを特徴とする。

次に、請求項５に記載した発明は、ＩＣチップと、上記ＩＣチップと通信手段を介して情報の授受を行い上記ＩＣチップの正当性を認証する認証装置と、を備えるＩＣチップ認証システムであって、上記ＩＣチップは、当該ＩＣチップに固有の情報である固有情報、及びＰＵＦ回路を有し、上記認証装置は、上記ＰＵＦ回路の特徴が上記固有情報に対応したデータに紐付けられた状態で記憶された記憶装置を備え、更に、上記ＩＣチップ内の情報を読み取り及び書き込みを行うリーダライタ装置を備え、上記ＩＣチップと上記認証装置とは、リーダライタ装置を介して情報の授受を行い、上記リーダライタ装置がプリンタ

に設けられ、上記ＩＣチップが上記プリンタに使用されるトナーに設けられることを特徴とする。

【発明の効果】

【００１０】

本発明によれば、対象とするＩＣチップのＰＵＦ回路の特徴を認証装置側で参照出来るため、個人情報を含めＩＣチップごと複製された場合でも、当該ＩＣチップの正当性の検証が可能となる。

【図面の簡単な説明】

【００１１】

【図１】本発明に基づく実施形態に係るタグ認証システムの構成図である。

【図２】タグ内の記憶部のデータ構成を説明する図である。

【図３】本発明に基づく実施形態に係るＲ／Ｗ装置の構成を示すブロック図である。

【図４】Ｒ／Ｗ制御部の構成を示すブロック図である。

【図５】本発明に基づく実施形態に係る認証装置の構成を示すブロック図である。

【図６】認証制御部の構成を示すブロック図である。

【図７】本発明に基づく実施形態に係る署名生成手順を示す図である。

【図８】本発明に基づく実施形態に係る機器認証Ａの処理手順を示す図である。

【図９】本発明に基づく実施形態に係るデバイス認証Ｂの処理手順を示す図である。

【図１０】本発明に基づく実施形態に係る署名検証Ｃの処理手順を示す図である。

【発明を実施するための形態】

【００１２】

次に、本発明の実施形態について図面を参照して説明する。

図１は、本実施形態における、ＩＣチップ認証システムの一例であるタグ認証システムの例を示す概要構成図である。

以下の説明では、ＩＣチップ認証システムの一例として、ＩＣチップを有する媒体であるＩＣタグに関する認証を行うタグ認証システムを例にして説明する。なお、本発明のＩＣチップ認証システムは、タグ認証システムに限定されるものではなく、ＩＣカード認証システム等、ＩＣチップを有する媒体若しくはＩＣチップ自体についての認証システムであれば適用可能である。

【００１３】

本実施形態のタグ認証システムは、図１に示すように、ＩＣタグ１、リーダライタ装置２、通信手段、記憶装置５Ａを有する認証装置５を備える。通信手段は、ゲートウェイ装置３、及びインターネットその他のネットワーク４を備え、リーダライタ装置２と認証装置５との間の通信を可能とする装置である。すなわち、図１に示すタグ認証システムでは、ＩＣタグ１と認証装置５とは、リーダライタ装置２、ゲートウェイ装置３、ネットワーク４を介して情報（データ）の授受を行う。

【００１４】

上記リーダライタ装置２（以下、「Ｒ／Ｗ装置２」とも呼ぶ。）は、ＩＣタグ１内の情報の読み取り及び書き込みを行う装置である。このリーダライタ装置２は、ゲートウェイ装置３とローカルに接続する。

ゲートウェイ装置３は、インターネットなどのネットワーク４を介して認証局の備える認証装置５と無線通信を行う。すなわち、ゲートウェイ装置３は、ネットワーク４を介して認証装置５との間で暗号化通信によりデータの送受信を行う。ゲートウェイ装置３には、例えば、ゲートウェイサーバ、ルータ、ＰＤＡ（Ｐｅｒｓｏｎａｌ　Ｄｉｇｉｔａｌ　Ａｓｓｉｓｔａｎｔｓ：情報携帯端末）、携帯電話、などを用いることができる。本実施の形態においては、暗号化通信に、インターネット上でデータを暗号化して送受信するためのプロトコルであるＳＳＬ（Ｓｅｃｕｒｅ　Ｓｏｃｋｅｔ　Ｌａｙｅｒ）を用いる。なお、リーダライタ装置２とゲートウェイ装置３とは、有線接続でも無線接続でも構わない。

【００１５】

（ＩＣタグ１の構成）
ＩＣタグ１は、ＩＣ（Ｉｎｔｅｇｒａｔｅｄ　Ｃｉｒｃｕｉｔ）タグであり、ここでは、非接触ＩＣタグであるＲＦＩＤ（Ｒａｄｉｏ　Ｆｒｅｑｕｅｎｃｙ　Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ）タグを例に挙げて説明する。主として無線周波数を通信に利用するＲＦＩＤタグ１は、図１に示すように、データを無線周波数で搬送するためのアンテナ１１とＩＣチップ１０とを備える。このＲＦＩＤタグは、樹脂製や紙製の容器に入れられたもの、全体を樹脂封止されたものや、樹脂や紙からなるシートに挟持したラベルなど、多様な形状に製作されたものである。ＲＦＩＤタグの電源は、外部からデータの搬送波として利用する電磁波から必要な電力を取り出すか、ＲＦＩＤタグに内蔵する電池に依存する。
る。

【００１６】
ＩＣチップ１０は、図１に示すように、データ記録用の記憶部１０Ａと、データ制御部１０Ｃと、ＰＵＦ回路１０Ｂとを備える。ＩＣチップ１０は、物理的には２以上のＩＣチップで構成されていても良い。ここで、本実施形態のＩＣタグ１は、上記ＩＣチップ１０と上記アンテナ１１を少なくとも備えていれば、その他の構成になんら限定はなく、ＲＦＩＤタグの形式の他、ＩＣカードその他の一部として使用されていても良い。

【００１７】
ここで、本実施形態では、ＩＣチップを有する媒体としてＩＣタグを例にしているため、アンテナ１１を使用して近接触通信、つまり非接触通信でリーダライタ装置２と通信を行う構成となっている。しかしながら、ＩＣチップとリーダライタ装置２との通信方式は、非接触通信に限定されず、有線その他を利用した接触通信で通信する方式であっても、本発明は適用可能である。

【００１８】
上記データ記録用の記憶部１０Ａは、図２に示すように、書換えが出来ないプロテクト領域と、書換えが可能な書換え可能領域とを有する。プロテクト領域には、各ＩＣタグ１に固有の情報を示す固有情報が記憶されている。本実施形態の固有情報は、ＩＣタグ１を一意に識別する情報であるタグＩＤ（ユニークＩＤ）とする。この固有情報の書込は、ＩＣタグ１の発行段階でのみ可能である。また書換え可能領域には、ユーザデータ、認証情報、タイムスタンプ、及び、公開鍵等からなる鍵データが記憶される。ユーザデータは、ＩＣタグ１を使用するユーザに用いられる任意のデータである。例えば、ＩＣタグ１が商品に添付されている場合は、その商品のコードが、電子マネーとして使用されている場合は、金額の情報などがユーザデータとして記憶されうる。認証情報とは、ＩＣタグ１の正当性を検証するために用いられる情報であり、ここでは、デジタル署名を示す署名データが用いられる。タイムスタンプは、認証情報を生成した日時の情報を示すデータである。鍵データは、認証情報に対応した鍵のコードである。

【００１９】
データ制御部１０ＣはＩＣタグ１内のデータの演算処理等を実施する。データ制御部１０Ｃは、例えば、チャレンジを受信すると該受信したチャレンジを上記ＰＵＦ回路１０Ｂに与えてレスポンスを取得し該取得したレスポンスを、Ｒ／Ｗ装置２に送信する。

【００２０】
（リーダライタ装置２の構成）
図３は、リーダライタ装置２の構成を示すブロック図であり、本発明と関係する機能ブロックのみ抽出してある。リーダライタ装置２としては、サーバ、パーソナルコンピュータ、プリンタ、家電、ＰＤＡ、携帯電話などを例示することが出来る。
リーダライタ装置２は、図３に示すように、読取書込部２０、通信処理部２２、及びＲ／Ｗ制御部２１を備える。
読取書込部２０は、ＩＣタグ１と近接触通信を行うことで、ＩＣタグ１内の情報の読み出し及び書き込みを行う機能部であり、具体的には、ＲＦＩＤタグリーダ・ライタ装置である。

【００２１】

通信処理部２２は、ゲートウェイ装置３との間で、イントラネットやケーブル、無線通信などによってデータの送受信の処理を行う。

Ｒ／Ｗ制御部２１は、上記読取書込部２０及び通信処理部２２を通じてＩＣタグ１や認証装置５との間のデータの授受の処理やデータ処理を行う。そのＲ／Ｗ制御部２１は、図４に示すように、タグ検出部２１Ａ、Ａ認証チャレンジ生成要求部２１Ｂ、Ａ認証チャレンジ受信・レスポンス要求受信部２１Ｃ、Ａ認証レスポンス受信送信部２１Ｄ、Ｂ認証チャレンジ生成要求部２１Ｅ、Ｂ認証チャレンジ受信・レスポンス要求受信部２１Ｆ、Ｂ認証レスポンス受信・レスポンス検証要求部２１Ｇ、Ｂ認証レスポンス検証結果受信部２１Ｈ、Ｃ認証情報要求部２１Ｉ、Ｃ認証情報受信部２１Ｊ、Ｃ認証検証要求部２１Ｋ、Ｃ認証検証結果受信部２１Ｌ、及び、動作制御部２１Ｍを備える。

【００２２】

タグ検出部２１Ａは、検出範囲にＩＣタグ１が存在することを検出する。

Ａ認証チャレンジ生成要求部２１Ｂは、認証装置５からのチャレンジ要求信号を受信すると、固有情報とチャレンジを要求する信号をＩＣタグ１に送信する。

Ａ認証チャレンジ受信・レスポンス要求受信部２１Ｃは、ＩＣタグ１からの固有情報及びチャレンジを受信し、その受信した固有情報及びチャレンジを、認証装置５に送信する。

【００２３】

Ａ認証レスポンス受信送信部２１Ｄは、認証装置５からのレスポンスを受信し、受信したレスポンスを読取書込部２０を通じてＩＣタグ１に送信する。

Ｂ認証チャレンジ生成要求部２１Ｅは、チャレンジ（乱数等）要求信号を通信処理部２２及びゲートウェイ装置３を介して認証装置５に送信する。

Ｂ認証チャレンジ受信・レスポンス要求受信部２１Ｆは、認証装置５からのチャレンジを受信し、その受信したチャレンジをＩＣタグ１へ伝える機能を有し、ＩＣタグ１宛のレスポンス要求信号を読取書込部２０を通じてＩＣタグ１へ送信する。

【００２４】

Ｂ認証レスポンス受信・レスポンス検証要求部２１Ｇは、ＩＣタグ１からのレスポンスを読取書込部２０を通じて受信し、レスポンスとともに検証要求信号を通信処理部２２及びゲートウェイ装置３を介して認証装置５に送信する。

Ｂ認証レスポンス検証結果受信部２１Ｈは、通信処理部２２及びゲートウェイ装置３を介して、認証装置５からレスポンス検証結果の情報を受信する。

【００２５】

Ｃ認証情報要求部２１Ｉは、認証情報の生成要求信号を通信処理部２２及びゲートウェイ装置３を介して認証装置５に送信する。認証情報の生成要求信号には、認証情報の生成要求であることを示す情報と、読取書込部２０を介してＩＣタグ１の記憶部１０Ａから読み出した固有情報及びユーザデータとが含まれる。

Ｃ認証情報受信部２１Ｊは、通信処理部２２及びゲートウェイ装置３を介して、認証装置５から、認証装置５が生成した認証情報と、当該認証情報を生成した日時を示すデータであるタイムスタンプと、当該認証情報に対応した鍵データとを受信する。更に、Ｃ認証情報受信部２１Ｊは、上述の受信した各データを、読取書込部２０を介してＩＣタグ１に送信し、ＩＣタグ１の記憶部１０Ａ内の書換え可能領域に書き込む。

【００２６】

Ｃ認証検証要求部２１Ｋは、検証要求信号を通信処理部２２及びゲートウェイ装置３を介して認証装置５に送信する。検証要求信号には、検証要求であることを示す情報と、読取書込部２０を介してＩＣタグ１の備える記憶部１０Ａから読み出した固有情報、ユーザデータ、認証情報、タイムスタンプ、及び、鍵データからなる検証要求データとが含まれる。

【００２７】

Ｃ認証検証結果受信部２１Ｌは、通信処理部２２及びゲートウェイ装置３を介して、認証装置５からの検証結果の情報を受信する。

動作制御部２１Ｍは、Ｂ認証レスポンス検証結果受信部２１Ｈが受信した検証結果の情報と、Ｃ認証検証結果受信部２１Ｌが受信した検証結果の情報とに応じて、リーダライタ装置２が実行する機能を制御する。

【００２８】

（認証装置５の構成）

図５は、認証装置５の構成を示すブロック図であり、本発明と関係する機能ブロックのみ抽出して示してある。

認証装置５は、例えば、サーバで構成することができる。認証装置５は、図５に示すように、通信処理部５１、認証制御部５２、時計５３、及び記憶装置５Ａを備える。

記憶装置５Ａには、各ＩＣタグ１の固有情報に対応したデータに紐付けて対応するＩＣタグ１内のＰＵＦ回路の特徴が、予め記憶されている。固有情報に対応したデータは固有情報自体であっても良い。

【００２９】

通信処理部５１は、ネットワーク４を介してゲートウェイ装置３との間で暗号化通信によりデータの送受信を行う。

認証制御部５２は、図６に示すように、Ａ認証チャレンジ要求部５２Ａ、Ａ認証レスポンス計算部５２Ｂ、Ｂ認証チャレンジ要求受信部５２Ｃ、Ｂ認証チャレンジ生成部５２Ｄ、Ｂ認証チャレンジ送信・レスポンス要求部５２Ｅ、Ｂ認証レスポンス認証検証情報受信部５２Ｆ、Ｂ認証レスポンス検証部５２Ｇ、Ｂ認証レスポンス認証検証結果送信部５２Ｈ、Ｃ認証情報要求受信部５２Ｉ、Ｃ認証情報生成部５２Ｊ、Ｃ認証情報送信部５２Ｋ、Ｃ認証検証情報受信部５２Ｌ、Ｃ認証検証部５２Ｍ、及び、Ｃ認証検証結果送信部５２Ｎを備える。

【００３０】

Ａ認証チャレンジ要求部５２Ａは、固有情報とチャレンジを要求するチャレンジ要求信号を、ネットワーク４を介してＩＣタグ１に送信する。

Ａ認証レスポンス計算部５２Ｂは、ＩＣタグ１からチャレンジと固有情報を受信すると、固有情報に対応するＰＵＦ回路の特徴を記憶装置５Ａから取得し、取得したＰＵＦ回路の特徴と受信したチャレンジとからレスポンスを計算し、計算したレスポンスを、ネットワーク４を介してＩＣタグ１に送信する。

【００３１】

Ｂ認証チャレンジ要求受信部５２Ｃは、通信処理部５１を通じて、チャレンジの生成要求信号を受信する。

Ｂ認証チャレンジ生成部５２Ｄは、Ｂ認証チャレンジ生成要求受信部がチャレンジの生成要求信号を受信すると、チャレンジを生成する。

Ｂ認証チャレンジ送信・レスポンス要求部５２Ｅは、Ｂ認証チャレンジ生成部５２Ｄにより生成されたチャレンジを通信処理部５１を介してリーダライタ装置２に送信する。

【００３２】

Ｂ認証レスポンス認証検証情報受信部５２Ｆは、レスポンス検証要求信号を受信する。

Ｂ認証レスポンス検証部５２Ｇは、Ｂ認証レスポンス認証検証情報受信部５２Ｆがレスポンス検証要求信号を受信すると、レスポンス検証要求信号に含まれる検証要求データ内のレスポンスを用いてレスポンスの正当性を検証する。

Ｂ認証レスポンス認証検証結果送信部５２Ｈは、Ｃ認証検証部５２Ｍによる検証結果を示す情報を、通信処理部５１を通じて、リーダライタ装置２に送信する。

【００３３】

Ｃ認証情報要求受信部５２Ｉは、認証情報の生成要求信号を受信する。

Ｃ認証情報生成部５２Ｊは、Ｃ認証情報要求受信部５２Ｉが受信した生成要求信号に含まれる固有情報を使用して、記憶装置５Ａから上記固有情報に対応するＰＵＦ回路の特徴を取得する。そして、Ｃ認証情報生成部５２Ｊは、Ｃ認証情報要求受信部５２Ｉが受信した生成要求信号に含まれる固有情報及びユーザデータと、上記固有情報に紐付く数値化されたＰＵＦ回路の特徴とを用いて認証情報を生成すると共に、認証情報を生成した時刻を

時計５３から取得した現在の時刻を示すデータであるタイムスタンプを生成し、さらに、上記認証情報に対応した鍵とを生成する。認証情報及び鍵の生成には、例えば公開鍵型の暗号方式の１つである楕円曲線暗号（ＥＣＣ：Ｅｌｌｉｐｔｉｃ Ｃｕｒｖｅ Ｃｒｙｐｔｏｓｙｓｔｅｍ）を使用する。この場合、認証情報に対応する鍵とは、楕円曲線暗号の公開鍵である。

【００３４】

Ｃ認証情報送信部５２Ｋは、Ｃ認証情報生成部５２Ｊにより生成された認証情報とタイムスタンプ及び鍵のデータとを、通信処理部５１を介してリーダライタ装置２に送信する。

Ｃ認証検証情報受信部５２Ｌは、検証要求信号を受信する。

Ｃ認証検証部５２Ｍは、検証要求信号に含まれる検証要求データ内の固有情報、ユーザデータ、認証情報、タイムスタンプ及び鍵データを用いて、認証情報の正当性を検証する。

Ｃ認証検証結果送信部５２Ｎは、Ｃ認証検証部５２Ｍによる検証結果を示す情報をリーダライタ装置２に送信する。

【００３５】

（署名生成手順）

図７は、本実施形態のタグ認証システムで認証情報として署名を用いた場合の例による署名生成手順を示すシーケンス図である。

次に、本実施形態のタグ認証システムにおける署名生成処理について、図５を参照して説明する。

リーダライタ装置２のＣ認証情報要求部２１Ｉは、読取書込部２０を介してＩＣタグ１に固有情報及びユーザデータの読み出し要求を送信する（ステップＳ１１０）。ＩＣタグ１は、読み出し要求を受信すると、記憶部１０Ａ内のプロテクト領域に記憶している固有情報と、書換え可能領域に記憶しているユーザデータとをリーダライタ装置２へ送信する（ステップＳ１１５）。

【００３６】

リーダライタ装置２のＣ認証情報要求部２１Ｉは、認証情報の生成要求信号としての署名生成要求信号を通信処理部５１によりゲートウェイ装置３へ送信する（ステップＳ１２０）。署名生成要求信号には、署名生成要求であることを示す情報と、読取書込部２０を介してＩＣタグ１から受信した固有情報及びユーザデータとが含まれる。

ゲートウェイ装置３は、リーダライタ装置２から署名生成要求信号を受信すると、ネットワーク４を介して認証装置５へＳＳＬ通信の確立を要求するためのＳＳＬ要求を送信する（ステップＳ１２５）。認証装置５の通信処理部５１は、ＳＳＬ通信の確立を行う場合、ＳＳＬ応答をゲートウェイ装置３へ返送する（ステップＳ１３０）。これにより、ゲートウェイ装置３と認証装置５の間では、ＳＳＬ通信を用いたセキュアセッションが確立される。

【００３７】

ゲートウェイ装置３は、ステップＳ１２０においてリーダライタ装置２から受信した署名生成要求信号を、ＳＳＬパケットにより認証装置５に送信する（ステップＳ１３５）。

認証装置５のＣ認証情報要求受信部５２Ｉは、通信処理部５１を介して署名生成要求信号を受信する。

Ｃ認証情報生成部５２Ｊは、受信した署名生成要求信号内の固有情報に対応するＰＵＦ回路の特徴を取り出す（ステップＳ１３７）。また、Ｃ認証情報生成部５２Ｊは、時計５３から現在の時刻の情報を読出し、この取得した時刻を示すタイムスタンプを生成する（ステップＳ１４０）。次に、Ｃ認証情報生成部５２Ｊは、取得したＰＵＦ回路の特徴と、Ｃ認証情報要求受信部５２Ｉが受信した署名生成要求信号内の固有情報及びユーザデータと、生成したタイムスタンプとをパラメータとしたハッシュ関数により、ハッシュ値を算出する（ステップＳ１４５）。Ｃ認証情報生成部５２Ｊは、生成したハッシュ値と、乱数とから、楕円曲線暗号を用いて、認証情報としての署名データと、この署名データに対応

した公開鍵を生成する（ステップＳ１５０）。Ｃ認証情報送信部５２Ｋは、タイムスタンプ、署名データ、及び、公開鍵をＳＳＬパケットによりゲートウェイ装置３へ送信する（ステップＳ１５５）。

【００３８】

ゲートウェイ装置３は、認証装置５から受信したタイムスタンプ、署名データ、及び、公開鍵をＳＳＬパケットから取り出してリーダライタ装置２へ送信する（ステップＳ１６０）。

リーダライタ装置２のＣ認証情報受信部２１Ｊは、通信処理部５１を介してタイムスタンプ、署名データ、及び、公開鍵を受信すると、読取書込部２０を通じて、受信したタイムスタンプ、署名データ、及び、公開鍵を、ＩＣタグ１の備える記憶部１０Ａ内の書換え可能領域に書き込む（ステップＳ１６５）。

【００３９】

ＩＣタグ１は、記憶部１０Ａの書換え可能領域へのタイムスタンプ、署名データ、及び、公開鍵の書き込みが成功したか失敗したかの書き込み状態を示す確認情報を、リーダライタ装置２へ送信する（ステップＳ１７０）。

以上の署名生成の処理によって、認証装置５は、受信したＩＣタグ１の固有情報に紐付けられたＰＵＦ回路の特徴をパラメータの一つとして認証情報を生成し、生成した認証情報をＩＣタグ１に送信する。ＩＣタグ１は、受信した認証情報をＩＣタグ１の記憶部１０Ａに記憶する。

【００４０】

「認証処理」

本実施形態のタグ認証システムの認証処理としては、機器認証（外部認証）Ａ、デバイス認証（内部認証）Ｂ、及び署名検証Ｃを備える。そして、セキュリティレベルに応じて、デバイス認証（内部認証）Ｂ及び署名検証Ｃの２つの認証処理を実施したり、機器認証（外部認証）Ａ、デバイス認証（内部認証）Ｂ、及び署名検証Ｃの３つの認証処理を実施したりする。このとき、認証に失敗した場合に、ＩＣタグ１からの読み出しを固有情報だけに制限することも可能である。

【００４１】

ここで、本実施形態のＩＣタグ１は、パッシブ型で電池等の電源をＩＣタグ１自身に持たないため、ＩＣタグ１への電力供給はリーダライタ装置２からの電磁波によって行われる。上記タグ検出部２１Ａは、一般的に、リーダライタ装置２は電磁波を出し続けて、その電磁波の範囲内にＩＣタグ１が存在するかを確認している（ポーリング）。リーダライタ装置２の電磁波範囲内にＩＣタグ１が入ることでＩＣタグ１が起動してリーダライタ装置２はＩＣタグ１の固有情報等を検出する。

【００４２】

このようにＩＣタグ１の存在をリーダライタ装置２が検出し、リーダライタ装置２がその検出信号を認証装置５へ通知することが後述の認証開始のタイミングとなる。

次に、各認証処理Ａ～Ｃについて説明する。

【００４３】

（機器認証Ａ）

図８は、機器認証Ａの処理手順を示すシーケンス図である。

次に、本実施形態のタグ認証システムにおける機器認証Ａの処理について、図８を参照して説明する。

認証装置５のＡ認証チャレンジ要求部５２Ａは、リーダライタ装置２のタグ検出部２１Ａから認証開始の通知を受けると、リーダライタ装置２のＡ認証チャレンジ生成要求部２１Ｂを通じて、ＩＣタグ１へ固有情報とチャレンジ（乱数）を要求するチャレンジ要求信号を送信する（ステップＳ３００～Ｓ３２０）。

【００４４】

ＩＣタグ１は、チャレンジ要求信号を受信すると、リーダライタ装置２のＡ認証チャレンジ受信・レスポンス要求受信部２１Ｃを通じて、固有情報とチャレンジを認証装置５に

送信する（ステップＳ３３０～Ｓ３５０）。
認証装置５のＡ認証レスポンス計算部５２Ｂは、受信した固有情報に基づき、当該固有情報に紐付くＰＵＦ回路の特徴（数値化されている）を記憶部１０Ａから取得する。更に、認証装置５は、取得したＰＵＦ回路の特徴と受信したチャレンジによって、上記ＩＣタグ１内のＰＵＦ回路１０Ｂが返すと推定されるレスポンスを計算する（ステップＳ３６０）。
【００４５】
認証装置５のＡ認証レスポンス計算部５２Ｂは、リーダライタ装置２のＡ認証レスポンス受信送信部２１Ｄを通じて、計算したレスポンスをリーダライタ装置２を通じてＩＣタグ１へ送信する（ステップＳ３７０，Ｓ３８０）。
ＩＣタグ１は、上記認証装置５に送信したチャレンジを自身のＰＵＦ回路１０Ｂに与えて取得したレスポンスと、認証装置５から受信したレスポンスとを比較して、認証装置５が正当であることを検証する。上記２つのレスポンスが、予め設定した条件に基づき一致している場合には、正当な認証装置５と判定する。
そして、ＩＣタグ１は、例えば、上記認証装置５が正当でないと判定すると、固有情報以外の領域をリーダライタ装置２から読めないよう制限する。この制限は、認証できたときに解除する。
【００４６】
（デバイス認証Ｂ）
図９は、デバイス認証Ｂの処理手順を示すシーケンス図である。
次に、本実施形態のタグ認証システムにおけるデバイス認証Ｂの処理について、図９を参照して説明する。なお、デバイス認証Ｂの処理は、機器認証Ａの処理を実施する場合には、機器認証Ａの処理による認証ができた場合に実施する。機器認証Ａの処理を実施しない構成の場合には、上述のように、リーダライタ装置２から認証開始の通知を受けることが認証開始のタイミングとなる。
【００４７】
認証装置５のＢ認証チャレンジ生成部５２Ｄは、Ｂ認証チャレンジ要求受信部５２Ｃがチャレンジ要求信号を入力すると、チャレンジ（乱数）を生成し、リーダライタ装置２のＢ認証チャレンジ受信・レスポンス要求受信部２１Ｆを通じて、生成したチャレンジをＩＣタグ１に送信する（ステップＳ４１０～Ｓ４３０）。
ＩＣタグ１は、チャレンジを受信すると、受け取ったチャレンジを自身のＰＵＦ回路１０Ｂに与えてレスポンスを取得し、取得したレスポンスをリーダライタ装置２のＢ認証レスポンス受信・レスポンス検証要求部２１Ｇを通じて、認証装置５のＢ認証レスポンス検証部５２Ｇへ送信する（ステップＳ４４０～Ｓ４６０）。
【００４８】
そして、認証装置５のＢ認証レスポンス検証部５２Ｇは、上記生成したチャレンジに対するレスポンスを、上記取得したＰＵＦ回路の特徴を使用して計算し、その計算したレスポンスと、ＩＣタグ１から受信したレスポンスとを比較して、電磁波範囲内に入ったＩＣタグ１が正当であるか否かを検証する。なお、機器認証Ａを実施しない場合には、予めリーダライタ装置２を通じて、上記ＩＣタグ１から固有情報を受信し、受信した固有情報に基づき、当該固有情報に紐付くＰＵＦ回路の特徴（数値化されている）を記憶部１０Ａから取得しておく。
認証装置５のＢ認証レスポンス認証検証結果送信部５２Ｈは、検証結果をリーダライタ装置２に送信する（ステップＳ４７０，Ｓ４８０）。
【００４９】
（署名検証Ｃ）
図１０は、署名検証Ｃの処理手順を示すシーケンス図である。
次に、本実施形態のタグ認証システムにおける署名検証Ｃの処理について、図１０を参照して説明する。署名検証Ｃは、上記デバイス認証Ｂを実施した後に実施される。
リーダライタ装置２のＣ認証検証要求部２１Ｋは、ＩＣタグ１に固有情報、ユーザデー

タ、タイムスタンプ、署名データ、及び、公開鍵の読み出し要求を送信する（ステップＳ２１０）。

ＩＣタグ１は、読み出し要求を受信すると、記憶部１０Ａ内のプロテクト領域に記憶している固有情報と、書換え可能領域に記憶しているユーザデータ、タイムスタンプ、署名データ、及び、公開鍵とをリーダライタ装置２へ送信する（ステップＳ２１５）。

【００５０】

リーダライタ装置２のＣ認証検証要求部２１Ｋは、認証装置５宛の検証要求信号を通信処理部５１によりゲートウェイ装置３へ送信する（ステップＳ２２０）。検証要求信号には、検証要求であることを示す情報と、読取書込部２０を介してＩＣタグ１から受信した固有情報、ユーザデータ、タイムスタンプ、署名データ、及び、公開鍵からなる検証要求データとを含む。ゲートウェイ装置３は、リーダライタ装置２から検証要求信号を受信すると、図７のステップＳ１２５～Ｓ１３０と同様の手順により、ゲートウェイ装置３と認証装置５の間で、ＳＳＬ通信を用いたセキュアセッションを確立する（ステップＳ２２５～２３０）。

【００５１】

ゲートウェイ装置３は、ステップＳ２２０においてリーダライタ装置２から受信した検証要求信号をＳＳＬパケットにより認証装置５に送信する（ステップＳ２３５）。

認証装置５のＣ認証検証情報受信部５２Ｌは、通信処理部５１を介して検証要求信号を受信する。

Ｃ認証検証部５２Ｍは、受信した検証要求信号に含まれる固有情報に対応するＰＵＦ回路の特徴を記憶装置５Ａから取得する（ステップＳ２３７）。またＣ認証検証部５２Ｍは、Ｃ認証検証情報受信部５２Ｌが受信した検証要求信号に含まれる検証要求データからタイムスタンプを取り出す（ステップＳ２４０）。次に、Ｃ認証検証部５２Ｍは、取得したＰＵＦ回路の特徴と、取り出したタイムスタンプと、検証要求データ内の固有情報及びユーザデータとをパラメータとしたハッシュ関数を用いて、ハッシュ値を算出する（ステップＳ２４５）。続いて、Ｃ認証検証部５２Ｍは、検証要求データから公開鍵を取り出す（ステップＳ２５０）。Ｃ認証検証部５２Ｍは、ステップＳ２４５で算出したハッシュ値と、ステップＳ２５０において取り出した公開鍵と、署名データに含まれる成分とをパラメータとして楕円曲線暗号の検証関数を用いて算出した値が、当該署名データに含まれる他の成分と一致した場合に、署名データが正当であると判断し、一致しない場合に不正であると判断する（ステップＳ２５５）。

【００５２】

Ｃ認証検証結果送信部５２Ｎは、Ｃ認証検証部５２Ｍによる検証結果を示す情報をＳＳＬパケットによりゲートウェイ装置３へ送信する（ステップＳ２６０）。

ゲートウェイ装置３は、認証装置５から受信した検証結果の情報をリーダライタ装置２へ送信する（ステップＳ２６５）。

リーダライタ装置２のＣ認証検証結果受信部２１Ｌは、通信処理部５１を介して検証結果の情報を受信すると、リーダライタ装置２の備えるディスプレイ（図示せず）などに検証結果を表示する（ステップＳ２７０）。動作制御部２１Ｍは、検証結果に応じて、リーダライタ装置２が実行する機能を制御する。

以上のように、署名情報（認証情報）を検証することで、ＩＣタグ１が、書き込まれるＩＣタグ１に書き込まれているデータであることを確認することが出来る。

【００５３】

（認証例）

例えば、リーダライタ装置２をプリンタとし、そのプリンタに使用されるトナーにＩＣタグ１を備えておく。

そして、デバイス認証及び署名検証の各検証結果の情報が正当であることを示している場合、リーダライタ装置２の動作制御部２１Ｍは、フルカラー印刷などの全ての印刷機能を提供する。一方、上記検証結果の情報が不正を示している場合、動作制御部２１Ｍは、白黒印刷などの一部の印刷機能のみを提供する。このように、ある製品の純製品の部品や

消耗品にＩＣタグ１を備えておくことにより、純正品として検証された場合は全機能を提供し、純正品以外を使用した場合は、一部の機能のみを提供する、あるいは、全ての機能の提供を制限することができ、ユーザに純正品の部品や消耗品の使用を促進することができる。

【００５４】

（作用効果）

本実施形態のＩＣタグ１は、ＰＵＦ回路１０Ｂを有する。また、ＩＣタグ１の記憶部１０Ａは、タグ認証システムで使用するデータを書込可能領域にユーザデータとして保持する。

しかし、上記ユーザデータは改ざんされる恐れがある。または、ユーザデータをコピーして正当でないＩＣタグ１に書き込むことによる不正タグが作成される恐れがある。

更に、固有情報も含めてＩＣチップ１０ごと複製されて不正タグが作成される恐れがある。

上記ＩＣタグ１が保持するユーザデータの改ざんを検出するため、認証情報として例えば署名データを作成してＩＣタグ１に保持する。

【００５５】

このとき、ユーザデータと署名データをコピーして別のＩＣタグ１へ書き込まれて不正タグを作成される恐れがあるので、署名データ作成時のパラメータとしてＩＣタグ１に一意に振り分けられた固有情報を使用する。

しかし、固有情報も含めてＩＣチップ１０ごと複製されて不正タグが作成される恐れがある。

【００５６】

これに対し、本実施形態では、ＩＣタグ１に格納されているＰＵＦ回路１０Ｂに対応する、数値化されたＰＵＦ回路の特徴を認証装置５側で予め記憶することで、該認証装置５で参照可能としておく。そして、本実施形態では、署名データ作成時のパラメータの一つとして、数値化されたＩＣタグ１のチップのＰＵＦ回路の特徴を使用する。

これによって、固有情報も含めてＩＣチップ１０ごと複製されて不正タグが作成されても、物理的複製が困難なＰＵＦ回路１０Ｂが異なるために、不正タグであることを検証することが可能となる。

【００５７】

以上の事から、本実施形態では、次の効果を奏する。

（１）各ＩＣタグ１が有するＰＵＦ回路の特徴をパラメータの１つとして認証情報を生成する。

この結果、ＩＣタグ１内のデータの改ざんだけでなく、そのデータが書き込まれるべきＩＣタグ１に書き込まれていることを検証できる。

（２）複製困難であるＰＵＦを利用する。

この結果、ＩＣタグ１がＩＣチップ１０ごと複製されたとしても検出することができる。

（３）認証情報生成のパラメータとして、ＩＣタグ１のメモリ内に保持しなくてもよい数値化されたＰＵＦ回路の特徴も使用する。

この結果、認証情報の安全性を高める。

【００５８】

（４）ＰＵＦ回路１０Ｂを使用する。

この結果、高価な暗号処理機能を持つことなく安全性の高いＩＣタグ１とすることができる。

（５）数値化されたＰＵＦ回路の特徴をパラメータの１つとして認証情報を生成する。

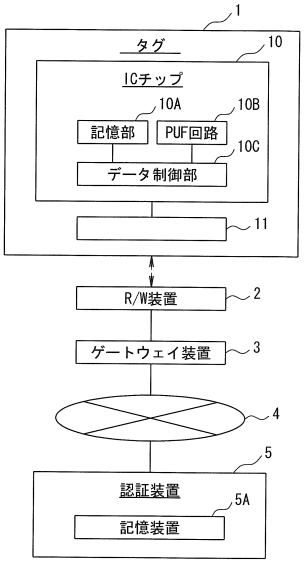
この結果、ＩＣチップ１０としては偽物でない別用途で使用されたＩＣチップ１０を使って、データのみコピーされたとしても、ＩＣチップ１０と書き込まれたデータの組み合わせがおかしいことを検出できる。

ここで、書換え可能領域に、公開鍵のコードを示す鍵データの代わりに、公開鍵を特定

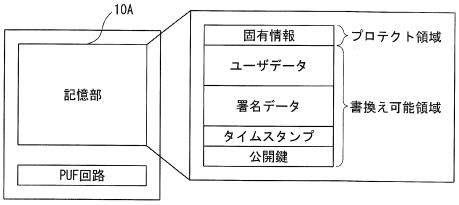
する鍵ＩＤを記憶して認証処理をしても良い。
　また、楕円曲線暗号を用いた署名の生成及び検証については、特許第４８４３９６０号公報などに記載の公知の処理を採用すればよい。又、認証情報の生成についても、パラメータの一つとしてＰＵＦ回路の特徴を採用できれば、ＲＳＡ署名、ＤＳＡ署名などの他の公知の署名生成処理を採用しても構わない。
【００５９】
　また、ＰＵＦ回路は、ＩＣチップに固有の物理的特徴を利用して固有の値を出力する関数を構成する回路である。ＩＣチップに固有な物理的特徴としては、例えばチップ毎の回路パターンのばらつき（位置のずれなど）や線幅の太さのばらつき、電気的特性などが例示できる。なお、ＰＵＦ回路としては、特許文献３などに記載されている、Ａｒｂｉｔｅｒ　ＰＵＦその他の回路を採用すれば良い。
【００６０】
　また、上述のリーダライタ装置２、ゲートウェイ装置３、認証装置５は、内部にコンピュータシステムを有している。そして、上述したリーダライタ装置２の制御部、ゲートウェイ装置３、認証装置５の認証制御部５２の処理は、プログラムの形式でコンピュータ読み取り可能な記録媒体に記憶されており、このプログラムをコンピュータシステムが読み出して実行することによって、上記処理が行われる。ここでいうコンピュータシステムとは、ＯＳや周辺機器等のハードウェアを含むものである。
【００６１】
　また、「コンピュータ読み取り可能な記録媒体」とは、ＲＯＭの他に、磁気ディスク、光磁気ディスク、ＣＤ－ＲＯＭ、ＤＶＤ－ＲＯＭ等の可搬媒体、コンピュータシステムに内蔵されるハードディスク、不揮発性記憶部等の記憶装置のことをいう。さらに「コンピュータ読み取り可能な記録媒体」とは、インターネット等のネットワーク４や電話回線等の通信回線を介してプログラムが送信された場合のシステムやクライアントとなるコンピュータシステム内部の揮発性記憶部（ＲＡＭ）のように、一定時間プログラムを保持しているものも含むものとする。
【００６２】
　また、「コンピュータシステム」は、ＷＷＷシステムを利用している場合であれば、ホームページ提供環境（あるいは表示環境）も含むものとする。
　また、「コンピュータ読み取り可能な記録媒体」とは、フレキシブルディスク、光磁気ディスク、ＲＯＭ、ＣＤ－ＲＯＭ等の可搬媒体、コンピュータシステムに内蔵されるハードディスク等の記憶装置のことをいう。さらに「コンピュータ読み取り可能な記録媒体」とは、インターネット等のネットワーク４や電話回線等の通信回線を介してプログラムを送信する場合の通信線のように、短時間の間、動的にプログラムを保持するもの、その場合のサーバやクライアントとなるコンピュータシステム内部の揮発性記憶部のように、一定時間プログラムを保持しているものも含むものとする。また上記プログラムは、前述した機能の一部を実現するためのものであっても良く、さらに前述した機能をコンピュータシステムにすでに記録されているプログラムとの組み合わせで実現できるものであっても良い。
【００６３】
　ここで、Ｃ認証情報生成部５２Ｊは認証情報生成手段を構成する。Ｃ認証情報送信部５２Ｋは認証情報送信手段を構成する。Ｂ認証チャレンジ生成部５２Ｄ、Ｂ認証チャレンジ送信・レスポンス要求部５２Ｅはチャレンジ送信手段を構成する。Ｂ認証レスポンス検証部５２Ｇは正当性検証手段を構成する。ＩＣチップ１０はレスポンス送信手段を構成する。
【符号の説明】
【００６４】
１　　ＩＣタグ
２　　リーダライタ装置（Ｒ／Ｗ装置）
３　　ゲートウェイ装置

４　　ネットワーク
５　　認証装置
５Ａ　記憶装置
１０　ＩＣチップ
１０Ａ 記憶部
１０Ｂ ＰＵＦ回路
１０Ｃ データ制御部
１１　アンテナ
２０　読取書込部
２１　Ｒ／Ｗ制御部
２１Ａ タグ検出部
２１Ｂ Ａ認証チャレンジ生成要求部
２１Ｃ Ａ認証チャレンジ受信・レスポンス要求受信部
２１Ｄ Ａ認証レスポンス受信送信部
２１Ｅ Ｂ認証チャレンジ生成要求部
２１Ｆ Ｂ認証チャレンジ受信・レスポンス要求受信部
２１Ｇ Ｂ認証レスポンス受信・レスポンス検証要求部
２１Ｇ Ｂ認証レスポンス受信・レスポンス検証要求部
２１Ｈ Ｂ認証レスポンス検証結果受信部
２１Ｉ　Ｃ認証情報要求部
２１Ｊ　Ｃ認証情報受信部
２１Ｋ Ｃ認証検証要求部
２１Ｌ　Ｃ認証検証結果受信部
２１Ｍ 動作制御部
２２　通信処理部
５１　通信処理部
５２　認証制御部
５２Ａ Ａ認証チャレンジ要求部
５２Ｂ Ａ認証レスポンス計算部
５２Ｃ Ｂ認証チャレンジ要求受信部
５２Ｄ Ｂ認証チャレンジ生成部
５２Ｅ Ｂ認証チャレンジ送信・レスポンス要求部
５２Ｆ Ｂ認証レスポンス認証検証情報受信部
５２Ｇ Ｂ認証レスポンス検証部
５２Ｈ Ｂ認証レスポンス認証検証結果送信部
５２Ｉ　Ｃ認証情報要求受信部
５２Ｊ　Ｃ認証情報生成部
５２Ｋ Ｃ認証情報送信部
５２Ｌ　Ｃ認証検証情報受信部
５２Ｍ Ｃ認証検証部
５２Ｎ Ｃ認証検証結果送信部
５３　時計
Ａ　　機器認証
Ｂ　　デバイス認証
Ｃ　　署名検証

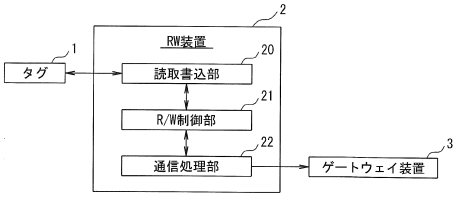
【図１】



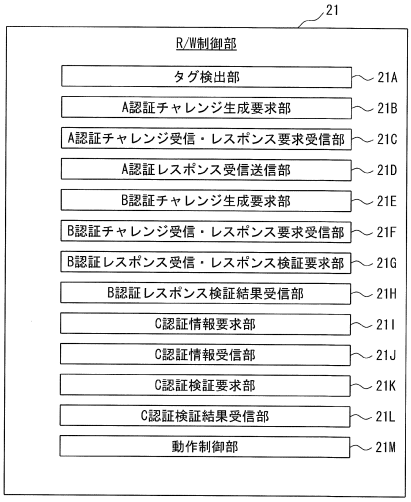
【図２】



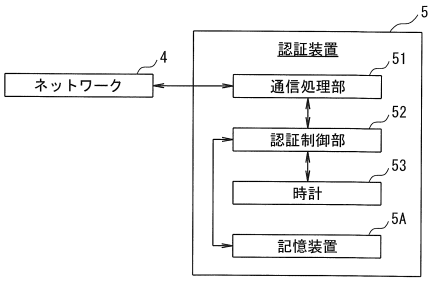
【図３】



【図４】



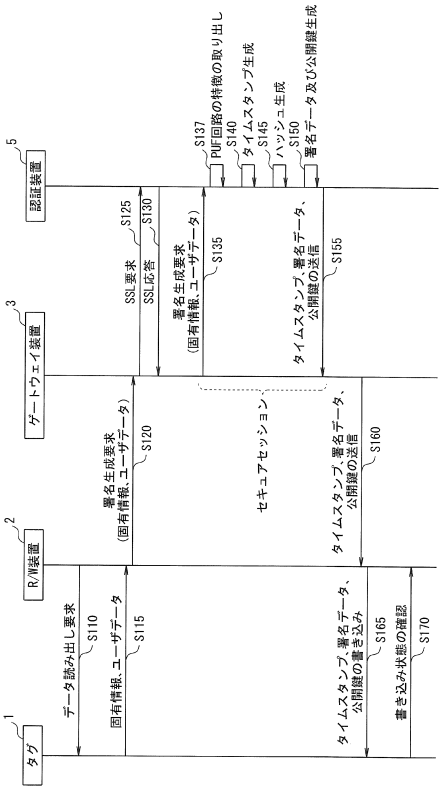
【図５】



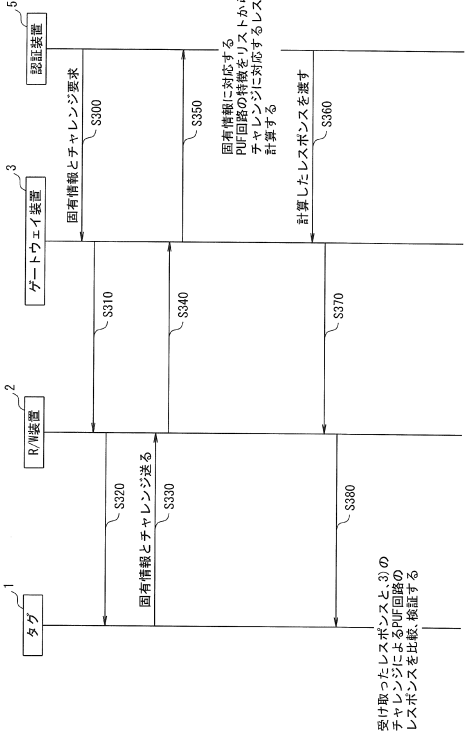
【図６】



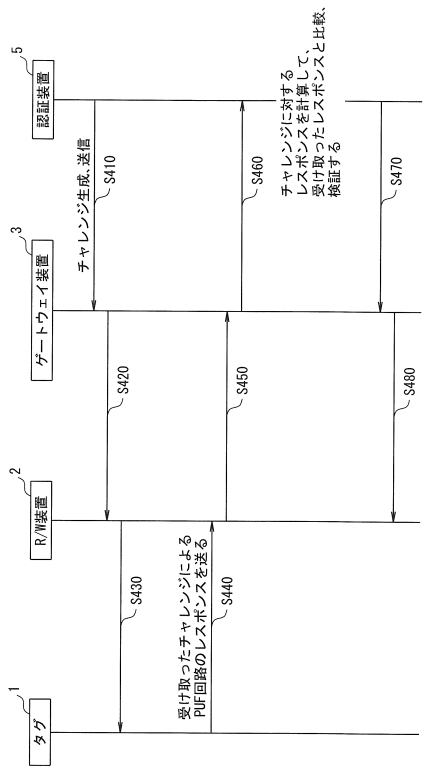
【図７】


1 タグ
2 R/W装置
3 ゲートウェイ装置
5 認証装置
データ読み出し要求 S110
固有情報、ユーザデータ S115
署名生成要求 (固有情報、ユーザデータ) S120
SSL要求 S125
SSL応答 S130
署名生成要求 (固有情報、ユーザデータ) S135
S137 PUF回路の特徴の取り出し
S140 タイムスタンプ生成
S145 ハッシュ生成
S150 署名データ及び公開鍵生成
タイムスタンプ、署名データ、公開鍵の送信 S155
セキュアセッション
タイムスタンプ、署名データ、公開鍵の送信 S160
タイムスタンプ、署名データ、公開鍵の書き込み S165
書き込み状態の確認 S170

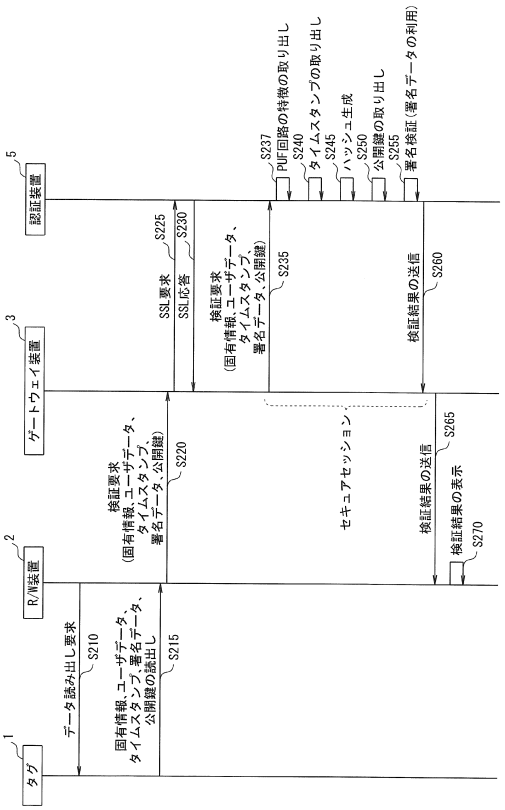
【図８】


1 タグ
2 R/W装置
3 ゲートウェイ装置
5 認証装置
固有情報とチャレンジ要求 S300
固有情報に対応するPUF回路の特徴をリストから探すチャレンジに対応するレスポンスを計算する S350
計算したレスポンスを渡す S360
S310
S340
S370
S320
固有情報とチャレンジ送る S330
S380
受け取ったレスポンスと、3)のチャレンジによるPUF回路のレスポンスを比較、検証する

【図９】


1 タグ
2 R/W装置
3 ゲートウェイ装置
5 認証装置
チャレンジ生成、送信 S410
S420
S430
受け取ったチャレンジによるPUF回路のレスポンスを送る S440
S450
S460
チャレンジに対するレスポンスを計算して、受け取ったレスポンスと比較、検証する
S470
S480

【図１０】


1 タグ
2 R/W装置
3 ゲートウェイ装置
5 認証装置
データ読み出し要求 S210
固有情報、ユーザデータ、署名データ、公開鍵の読出し S215
検証要求 (固有情報、ユーザデータ、タイムスタンプ、署名データ、公開鍵) S220
SSL要求 S225
SSL応答 S230
検証要求 (固有情報、ユーザデータ、タイムスタンプ、署名データ、公開鍵) S235
S237 PUF回路の特徴の取り出し
S240 タイムスタンプの取り出し
S245 ハッシュ生成
S250 公開鍵の取り出し
S255 署名検証 (署名データの利用)
検証結果の送信 S260
セキュアセッション
検証結果の送信 S265
検証結果の表示 S270

フロントページの続き

審査官　青木　重徳

(56)参考文献　特表２００８－５４２８９９（ＪＰ，Ａ）
特表２００５－５２３４８１（ＪＰ，Ａ）
特表２００９－５３３７４２（ＪＰ，Ａ）
特開２０１１－１９８３１７（ＪＰ，Ａ）
特表２００７－５００９１０（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／１０
Ｇ０６Ｆ　２１／４４
Ｇ０６Ｋ　１９／１０