(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2010-141639
(P2010-141639A)
(43)公開日　平成22年6月24日(2010.6.24)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/32	(2006.01)	H04L	9/00	675A	5B017
G06K 17/00	(2006.01)	G06K	17/00	S	5B058
G06F 21/24	(2006.01)	G06F	12/14	560C	5J104
		H04L	9/00	673E	

審査請求 未請求　請求項の数 6　ＯＬ　（全 11 頁）

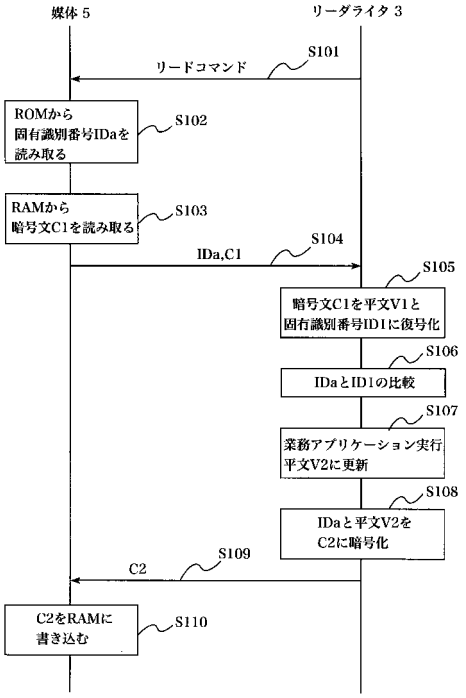
(21)出願番号　特願2008-316478 (P2008-316478)
(22)出願日　平成20年12月12日 (2008.12.12)

(71)出願人　000002897
大日本印刷株式会社
東京都新宿区市谷加賀町一丁目１番１号
(74)代理人　100096091
弁理士　井上　誠一
(72)発明者　小林　史陽
東京都新宿区市谷加賀町一丁目１番１号
大日本印刷株式会社内

Ｆターム(参考)　5B017 AA08　BA09
5B058 CA01　KA31　KA32　KA35
5J104 AA08　LA02　NA36　PA07

(54)【発明の名称】通信システムおよび通信方法

(57)【要約】
【課題】暗号演算用のプロセッサを搭載しないＩＣチップが内蔵された媒体に記憶されたデータが、不正に書き換えられたことを検知できる通信システム等を提供する。
【解決手段】媒体５は、リーダライタ３が送信したリードコマンドを受信し（Ｓ１０１）、そのコマンドに対応して、ＲＯＭ４３に記憶している固有識別番号ＩＤａを読み取り（Ｓ１０２）、さらにＲＡＭ４５に記憶している暗号文Ｃ１を読み取る（Ｓ１０３）。読み取った固有識別番号ＩＤａと暗号文Ｃ１をリーダライタ３に送信する（Ｓ１０４）。リーダライタ３は、媒体５が送信したＩＤａ、Ｃ１を受信し、暗号文Ｃ１を復号部２５で平文Ｖ１と固有識別番号ＩＤ１に復号化する（Ｓ１０５）。リーダライタ３は、媒体５が送信したＩＤａと復号化して得られたＩＤ１を比較し（Ｓ１０６）、一致した場合、媒体５のデータに改ざんがないものと判断し、業務アプリケーションを実行する。
【選択図】図６



【特許請求の範囲】
【請求項１】
暗号演算用のプロセッサを搭載しないＩＣチップが内蔵された媒体と、媒体内のデータを読み書きする情報処理装置とがデータの通信を行う通信システムであって、
前記媒体は、
固有識別番号を書き換え不可能なものとして記憶する第１の記憶手段と、
前記情報処理装置から受信するデータを書き換え可能なものとして記憶する第２の記憶手段と、
を備え、
前記情報処理装置は、
前記第１の記憶手段に記憶されている固有識別番号および前記第２の記憶手段に記憶されているデータを前記媒体から受信する受信手段と、
前記第１の記憶手段に記憶されている固有識別番号に基づいて、受信した前記第２の記憶手段に記憶されているデータが不正に書き換えられているか否かを検知する不正書換検知手段と、
を備えることを特徴とする通信システム。
【請求項２】
前記情報処理装置は、
固有識別番号および所定のデータを連結したものを暗号文に暗号化する暗号化手段と、
前記暗号文を復号化し、固有識別番号および所定のデータを取得する復号化手段と、
を更に備え、
前記受信手段は、前記第１の記憶手段に記憶されている固有識別番号および前記第２の記憶手段に記憶されている暗号文を前記媒体から受信し、
前記不正書換検知手段は、受信した暗号文を復号化することによって取得された固有識別番号と、前記媒体から受信した前記第１の記憶手段に記憶されている固有識別番号とを比較し、一致しない場合には、前記媒体から受信した暗号文が不正に書き換えられていると判定することを特徴とする請求項１に記載の通信システム。
【請求項３】
前記情報処理装置は、
固有識別番号および所定のデータを連結したものから署名を生成する署名生成手段、
を更に備え、
前記受信手段は、前記第１の記憶手段に記憶されている固有識別番号および前記第２の記憶手段に記憶されている署名と平文を前記媒体から受信し、
前記不正書換検知手段は、受信した固有識別番号および平文から前記署名生成手段によって生成された署名と、前記媒体から受信した前記第２の記憶手段に記憶されている署名とを比較し、一致しない場合には、前記媒体から受信した平文が不正に書き換えられていると判定することを特徴とする請求項１に記載の通信システム。
【請求項４】
前記情報処理装置は、
前記媒体から送信された固有識別番号と鍵を連結したものを暗号化して派生鍵を生成し、前記派生鍵を前記暗号化手段、前記復号化手段に利用する、
ことを特徴とする請求項２に記載の通信システム。
【請求項５】
前記情報処理装置は、
前記媒体から送信された固有識別番号と鍵を連結したものを暗号化して派生鍵を生成し、前記派生鍵を前記署名生成手段に利用する、
ことを特徴とする請求項３に記載の通信システム。
【請求項６】
暗号演算用のプロセッサを搭載しないＩＣチップが内蔵された媒体と、媒体内のデータを読み書きする情報処理装置とがデータの通信を行う通信方法であって、

前記媒体は、
固有識別番号を書き換え不可能なものとして記憶する第１の記憶手段と、
前記情報処理装置から受信するデータを書き換え可能なものとして記憶する第２の記憶手段と、
を備えるものであって、
前記情報処理装置が、前記第１の記憶手段に記憶されている固有識別番号および前記第２の記憶手段に記憶されているデータを前記媒体から受信するステップと、
前記第１の記憶手段に記憶されている固有識別番号に基づいて、受信した前記第２の記憶手段に記憶されているデータが不正に書き換えられているか否かを検知するステップと、
を備えることを特徴とする通信方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、暗号演算用のプロセッサを搭載しないＩＣチップが内蔵された媒体と、媒体内のデータを読み書きする情報処理装置とによって構成される、通信システム、およびその通信方法に関する。
【背景技術】
【０００２】
現在さまざまな媒体（ＩＣカード、携帯電話など）と情報処理端末の間では所定の伝送路を介して大量の情報が通信されている。情報が通信される伝送路では、第三者（送信者および受信者以外の者）が、通信されているデータを盗聴、改ざんする可能性がある。
【０００３】
そこで、データのセキュリティを強化するために、情報を暗号化する方法が用いられる。暗号化されたデータを通信することにより、暗号化されたデータを盗聴することができても、第三者がそのデータから通信された情報を読み出すことは困難である。
【０００４】
暗号化の方法としては、特定の暗号化手法と鍵を利用して、平文（送信される情報）から暗号（実際に送信されるデータ）を生成するものが利用されることが多い。受信者は同じ暗号化手法と鍵を利用して復号して送信された情報を入手する。
【０００５】
このような暗号化には、共通鍵暗号化方式と公開鍵暗号化方式の２種類がある。
共通鍵暗号では、暗号化するときの鍵（暗号化鍵データ）と復号化するときの鍵（復号化データ）が同一である。一方、公開鍵暗号では、暗号化鍵データと復号化鍵データが異なる。送信者は個人鍵と公開鍵の二つの鍵を持ち、受信者に公開鍵を送信する。送信者は個人鍵を使って暗号化し、受信者は公開鍵を使って復号化する。
【０００６】
図１０は、このような鍵を利用した秘密通信の一例を示している。送信者８１は、送信する情報（平文Ｍ）を、鍵Ｋを利用して暗号Ｃに暗号化する。そして、送信者８１は暗号Ｃを所定の伝送路を介して受信者８３に送信する。受信者８３は、暗号Ｃを受け取り、送信者８１が有する鍵Ｋと同一の鍵Ｋを利用して暗号Ｃを復号化し、送信者８１より送信された情報を取得する。
【０００７】
このように、暗号化することによってデータの秘匿性を確保することはできるが、さらに送信データの改ざんがないことを保証する必要がある。そのためにメッセージダイジェストを利用する。メッセージダイジェストとは特殊な計算式を使用した計算結果を比較する方法で、送信者は、平文の状態で計算式を使って計算したあとに暗号化し、その計算結果と暗号を送信する。受信者は復号後、送信者と同じ計算式を使って計算する。その計算結果と送信された計算結果を比較し一致すればデータの改ざんはないものとする。
【０００８】

図１１は、メッセージダイジェストを利用した改ざんの検知の一例を示している。送信者８５は、平文Ｍを、特殊な計算式Ｘを使って計算し計算結果Ａを得る。送信者８５は、平文Ｍと計算結果Ａを受信者８７に送信する。受信者８７は、送信者８５が有する計算式Ｘと同一の計算式Ｘを使って平文Ｍを計算し、計算結果Ｂを得る。計算結果Ａと計算結果Ｂを比較し、一致すれば平文Ｍの改ざんはないものとする。

【０００９】

さらに、上記の公開鍵暗号とメッセージダイジェストを組み合わせることによって、本人から送信されたデータであることを証明することが可能となる。これを電子署名と呼び、電子商取引やオンラインショッピングなどの際のデータの信頼性が保証される。

【００１０】

このように、非接触媒体と情報処置端末との間のデータの送受信のセキュリティ強化を実現するため、媒体にＩＣチップが搭載されるようになってきた（特許文献１参照）。特許文献１では、ＩＣチップには暗号演算用のプロセッサ装置が搭載されたＩＣカードが開示されており、リーダライタとの間で認証を行ったり、暗号通信などを行ったりしている。

【００１１】

【特許文献１】特許第３７０９９４６号公報

【発明の開示】

【発明が解決しようとする課題】

【００１２】

しかしながら、最近では特許文献１に開示されているＩＣカードに内蔵されるＩＣチップ等ではなく、コストを下げるために暗号演算等用のプロセッサを搭載しない安価なＩＣチップも出てきている。このようなＩＣチップが内蔵された媒体では、従来の暗号処理やメッセージダイジェストが行えない。その結果、伝送路における盗聴、等を防止する媒体の認証や暗号通信が行えないことに加えて、媒体内に記憶されたデータが不正に書き換えられても検知することができない。

【００１３】

本発明は、このような状況に鑑みてなされたものであり、その目的は、暗号演算用のプロセッサを搭載しないＩＣチップが内蔵された媒体に記憶されたデータが、不正に書き換えられたことを検知できる通信システム等を提供することである。

【課題を解決するための手段】

【００１４】

前述した目的を達成するために、第１の発明は、暗号演算用のプロセッサを搭載しないＩＣチップが内蔵された媒体と、媒体内のデータを読み書きする情報処理装置とがデータの通信を行う通信システムであって、前記媒体は、固有識別番号を書き換え不可能なものとして記憶する第１の記憶手段と、前記情報処理装置から受信するデータを書き換え可能なものとして記憶する第２の記憶手段と、を備え、前記情報処理装置は、前記第１の記憶手段に記憶されている固有識別番号および前記第２の記憶手段に記憶されているデータを前記媒体から受信する受信手段と、前記第１の記憶手段に記憶されている固有識別番号に基づいて、受信した前記第２の記憶手段に記憶されているデータが不正に書き換えられているか否かを検知する不正書換検知手段と、を備えることを特徴とする通信システムである。第１の発明に係る通信システムを使用することによって、暗号演算用のプロセッサを搭載しないＩＣチップが内蔵された媒体に対しても、データが不正に書き換えられたことを検知することができる。

【００１５】

前記第１の発明は、前記情報処理装置が、固有識別番号および所定のデータを連結したものを暗号文に暗号化する暗号化手段と、前記暗号文を復号化し、固有識別番号および所定のデータを取得する復号化手段と、を更に備え、前記受信手段は、前記第１の記憶手段に記憶されている固有識別番号および前記第２の記憶手段に記憶されている暗号文を前記媒体から受信し、前記不正書換検知手段は、受信した暗号文を復号化することによって取

得された固有識別番号と、前記媒体から受信した前記第１の記憶手段に記憶されている固有識別番号とを比較し、一致しない場合には、前記媒体から受信した暗号文が不正に書き換えられていると判定するものが望ましい。これによる効果は、第１の発明の説明において前述したとおりである。

【００１６】

また、前記第１の発明は、前記情報処理装置が、固有識別番号および所定のデータを連結したものから署名を生成する署名生成手段、を更に備え、前記受信手段は、前記第１の記憶手段に記憶されている固有識別番号および前記第２の記憶手段に記憶されている署名と平文を前記媒体から受信し、前記不正書換検知手段は、受信した固有識別番号および平文から前記署名生成手段によって生成された署名と、前記媒体から受信した前記第２の記憶手段に記憶されている署名とを比較し、一致しない場合には、前記媒体から受信した平文が不正に書き換えられていると判定するものが望ましい。これによる効果は、第１の発明の説明において前述したとおりである。

【００１７】

また、第１の発明は、前記情報処理装置が、前記媒体から送信された固有識別番号と鍵を連結したものを暗号化して派生鍵を生成し、前記派生鍵を前記暗号化手段、前記復号化手段に利用することが望ましい。これによって、前記派生鍵が解読されても、他の媒体で悪用されることがなく、安全である。

【００１８】

また、第１の発明は、前記情報処理装置が、前記媒体から送信された固有識別番号と鍵を連結したものを暗号化して派生鍵を生成し、前記派生鍵を前記署名生成手段に利用するものが望ましい。これによって、前記派生鍵が解読されても、他の媒体で悪用されることがなく、安全である。

【００１９】

第２の発明は、暗号演算用のプロセッサを搭載しないＩＣチップが内蔵された媒体と、媒体内のデータを読み書きする情報処理装置とがデータの通信を行う通信方法であって、前記媒体は、固有識別番号を書き換え不可能なものとして記憶する第１の記憶手段と、前記情報処理装置から受信するデータを書き換え可能なものとして記憶する第２の記憶手段と、を備えるものであって、前記情報処理装置が、前記第１の記憶手段に記憶されている固有識別番号および前記第２の記憶手段に記憶されているデータを前記媒体から受信するステップと、前記第１の記憶手段に記憶されている固有識別番号に基づいて、受信した前記第２の記憶手段に記憶されているデータが不正に書き換えられているか否かを検知するステップと、を備えることを特徴とする通信方法である。第２の発明に係る通信方法を使用することによって、暗号演算用のプロセッサを搭載しないＩＣチップが内蔵された媒体に対しても、データが不正に書き換えられたことを検知することができる。

【発明の効果】

【００２０】

本発明により、暗号演算用のプロセッサを搭載しないＩＣチップが内蔵された媒体に記憶されたデータが、不正に書き換えられたことを検知できる通信システム等を提供することができる。

【発明を実施するための最良の形態】

【００２１】

以下図面に基づいて、本発明の実施形態を詳細に説明する。

【００２２】

最初に、第１の実施の形態について説明する。図１は、通信システム１の一例を示す図である。図１に示すように、通信システム１は、リーダライタ３、媒体５、コンピュータ７等から構成される。媒体５は、例えば、ＩＣカード、携帯電話等である。リーダライタ３と媒体５は、電磁波を利用してデータの送受信を行う。リーダライタ３が、リードコマンドを媒体５に送信すると、媒体５は、そのリードコマンドを受信し、リードコマンドで指示されたデータをリーダライタ３に送信する。

【００２３】
また、リーダライタ３が、データを媒体５に送信すると、媒体５は、そのデータを受信して、受信したデータを、内蔵する書き換え可能なＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）４５（図５）に記憶させる。
【００２４】
図２は、リーダライタ３の構成を示すブロック図である。尚、図２のハードウエア構成は一例であり、用途、目的に応じて様々な構成をとることが可能である。
【００２５】
リーダライタ３においては、制御部１１は、内蔵するプログラムに応じて、各種処理を行う。また、メモリ１５から、データを呼び出し、メモリ１５に、データを記憶させる。
【００２６】
さらに、制御部１１は、インタフェース１３を介して、コンピュータ７と通信を行う。
【００２７】
メモリ１５は、制御部１１における処理に使用されるデータ、暗号化および復号化に使用される鍵などを記憶している。
【００２８】
暗号部１７は、制御部１１より供給されたデータを、所定の鍵で暗号化し、暗号化したデータ（暗号）を送信部１９に出力する。
【００２９】
送信部１９は、暗号部１７より供給されたデータ（暗号）を、所定の変調方式で変調し、生成された変調波を、アンテナ部２１を介して媒体５に送信する。
【００３０】
受信部２３は、アンテナ部２１を介して、媒体５より送信された変調波を受信し、その変調波に対応する復調方式で復調し、復調したデータ（暗号）を復号部２５に出力する。
【００３１】
図３は、図２の暗号部１７の一構成例を示すブロック図である。鍵保存部２９は、制御部１１より供給された鍵を保持する。
【００３２】
データランダム化部２７は、鍵保存部２９から鍵を読み出し、その鍵で、制御部１１より供給されたデータを暗号化し、生成された暗号を送信部１９に出力する。
【００３３】
図４は、図２の復号部２５の一構成例を示すブロック図である。変換部３１は、鍵保存部２９から鍵を読み出し、その鍵で、受信部２３より供給されたデータ（暗号）を復号化し、復号化したデータを制御部１１に出力する。
【００３４】
図５は、本発明の一実施例である媒体５の構成を示すブロック図である。制御部４１は、リーダライタ３により供給されるコマンドをアンテナ部４９、受信部５１を介して受け取り、そのコマンドに対応した処理を行う。そして、その処理の結果に対応する応答データを送信部４７に出力する。
【００３５】
また、制御部４１は、コマンドに対応してＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）４３に記憶されている固有識別番号ＩＤａや、ＲＡＭ４５に記憶されているデータを読み出す。
【００３６】
ＲＯＭ４３は、不揮発メモリであり、媒体５ごとに決められている固有識別番号ＩＤａを書き換え不可能なものとして記憶している。
【００３７】
ＲＡＭ４５は、制御部４１が処理したデータを書き換え可能なものとして記憶する。
【００３８】
次に、図６を参照しながら、第１の実施の形態に係る通信処理の詳細について説明する

。
【００３９】
図６は、第１の実施の形態に係る通信処理の詳細を示すシーケンス図である。図６に示すように、リーダライタ３と媒体５が、お互いにメッセージ（矢印で示す。）をやり取りしながら、自らの処理（ボックスで示す。）を行う。尚、処理に用いる具体的なデータについては、記号で示すこととする。
【００４０】
媒体５は、リーダライタ３が送信したリードコマンドを受信し（Ｓ１０１）、そのコマンドに対応して、ＲＯＭ４３に記憶している固有識別番号ＩＤａを読み取り（Ｓ１０２）、さらにＲＡＭ４５に記憶している暗号文Ｃ１を読み取る（Ｓ１０３）。読み取った固有識別番号ＩＤａと暗号文Ｃ１をリーダライタ３に送信する（Ｓ１０４）。
【００４１】
リーダライタ３は、媒体５が送信したＩＤａ、Ｃ１を受信し、暗号文Ｃ１を復号部２５で平文Ｖ１と固有識別番号ＩＤ１に復号化する（Ｓ１０５）。リーダライタ３は、媒体５が送信したＩＤａと復号化して得られたＩＤ１を比較し（Ｓ１０６）、一致した場合、媒体５のデータに改ざんがないものと判断し、業務アプリケーションを実行する。ＩＤａとＩＤ１が一致しなかった場合は、リーダライタ３は、ステップＳ１０７以降の処理を行わない。ここで、業務アプリケーションとは、例えば、電子マネーの決済、ポイントカードのポイント加算などを行うアプリケーションである。
【００４２】
リーダライタ３は、業務アプリケーションを実行し、平文Ｖ１を平文Ｖ２に更新する（Ｓ１０７）。リーダライタ３は、ＩＤａとＶ２を連結させて暗号部１７にて暗号化し、暗号文Ｃ２を生成し（Ｓ１０８）、Ｃ２を送信部より送信する（Ｓ１０９）。
【００４３】
媒体５は、リーダライタ３が送信した暗号Ｃ２を受信し、受信したＣ２をＲＡＭ４５に書き込む（Ｓ１１０）。
【００４４】
第１の実施の形態では、媒体５のデータが不正に書き換えされているか否かを検知する手段（＝不正書換検知手段）として、暗号化を利用する。第１の実施の形態によって、暗号演算用のプロセッサを搭載しないＩＣチップが内蔵された媒体５に対しても、データが不正に書き換えられたことを検知することができる。
【００４５】
尚、リーダライタ３は、メモリ１５に記憶している鍵を利用して暗号化及び復号化を行うと説明したが、これに限定されない。例えば、リーダライタ３は、媒体５が送信した固有識別番号ＩＤａとメモリ１５に記憶している鍵を連結して暗号化し生成した派生鍵を利用して、暗号化と復号化を行ってもよい。これによって、仮に派生鍵を解読されても、他の媒体５において悪用される心配がない。
【００４６】
次に、第２の実施の形態について説明する。第２の実施の形態では、不正書換検知手段として、署名を利用する。以下、第１の実施の形態と同じ要素については同じ符号を付し、重複した説明を省略する。
【００４７】
図７は、リーダライタ３の構成を示すブロック図である。署名生成部６１は、制御部１１より供給されたデータを、所定の計算式で計算し、生成した署名を送信部１９に出力する。
【００４８】
図８は、図７の署名生成部６１の構成例を示すブロック図である。鍵保存部６３は、署名生成に必要な鍵を記憶し、署名生成部６１は、鍵保存部６３から鍵を読み出し、制御部１１から供給されたデータで署名を生成し、送信部１９に出力する。
【００４９】

次に、図９を参照しながら、第２の実施の形態に係る通信処理の詳細について説明する。

【００５０】

図９は、第２の実施の形態に係る通信処理の詳細を示すシーケンス図である。リーダライタ３は、リードコマンドを媒体５に送信する（Ｓ１１１）。媒体５は、リーダライタ３が送信したコマンドを受信し、コマンドに対応して、ＲＯＭ４３から固有識別番号ＩＤａを読み出す（Ｓ１１２）。さらに、ＲＡＭ４５から平文Ｖ１と署名Ｔ１ａを読み出す（Ｓ１１３）。媒体５は、ＩＤａ、Ｖ１、Ｔ１ａをリーダライタ３に送信する（Ｓ１１４）。リーダライタ３は、Ｖ１とＩＤａを連結させて署名Ｔ１ｂを生成する（Ｓ１１５）。リーダライタ３は、媒体５が送信したＴ１ａと生成したＴ１ｂを比較し（Ｓ１１６）、一致した場合、媒体５のデータが改ざんされていないと判断し、業務アプリケーションを実行する。一致しなかった場合は、ステップＳ１１７以降の処理を行わない。リーダライタ３は、業務アプリケーションを実行して、平文Ｖ１を平文Ｖ２に更新する（Ｓ１１７）。ＩＤａとＶ２を連結して署名Ｔ１ｃを生成し（Ｓ１１８）、媒体５に、Ｖ２とＴ１ｃを送信する（Ｓ１１９）。

【００５１】

媒体５は、リーダライタ３が送信したＶ２とＴ１ｃを受信し、ＲＡＭ４５に記憶させる（Ｓ１２０）。

【００５２】

第２の実施の形態では、不正書換検知手段として、署名を利用する。第２の実施の形態によって、暗号演算等用のプロセッサを搭載しないＩＣチップが内蔵された媒体５においても、データが改ざんされたか否かを検知することができる。

【００５３】

尚、リーダライタ３は、メモリ１５に記憶している鍵を利用して署名処理を行うと説明したが、これに限定されない。例えば、リーダライタ３は、媒体５が送信した固有識別番号ＩＤａとメモリ１５に記憶している鍵を連結して暗号化し生成した派生鍵を利用して、署名処理を行ってもよい。これによって、仮に派生鍵を解読されても、他の媒体５において悪用される心配がない。

【００５４】

更に、リーダライタ３は、第１の実施の形態における暗号化処理と、第２の実施の形態における署名処理の両方を行っても良い。そして、リーダライタ３は、両方の処理において媒体５のデータの改ざんがないと判断した場合にのみ、業務アプリケーションを実行するようにしても良い。これによって、不正書換を検知する精度が高くなる。

【００５５】

また、本発明の実施の形態では、リーダライタ３単体が、情報処理装置として、不正な書き換えの検知、及び業務アプリケーションの実行を行うと説明したが、これに限定されない。例えば、リーダライタ３は、媒体５とのデータの送受信のみを行い、コンピュータ７が不正な書き換えの検知、及び業務アプリケーションの実行を行うようにしても良い。この場合、リーダライタ３およびコンピュータ７が一体となって、情報処理装置を構成する。

【００５６】

以上、添付図面を参照しながら、本発明に係る通信システム１等の好適な実施形態について説明したが、本発明はかかる例に限定されない。当業者であれば、本願で開示した技術的思想の範疇内において、各種の変更例又は修正例に想到し得ることは明らかであり、それらについても当然に本発明の技術的範囲に属するものと了解される。

【図面の簡単な説明】

【００５７】

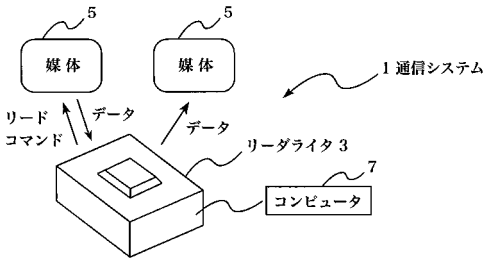
【図１】通信システム１の一例を示す図

【図２】暗号化処理を行うリーダライタ３の構成を示す図

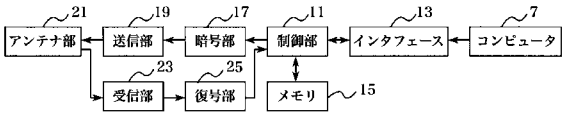
【図３】暗号部１７の構成例を示すブロック図

【図４】復号部２５の構成例を示すブロック図
【図５】媒体５の構成例を示すブロック図
【図６】第１の実施の形態に係る通信処理の詳細を示すシーケンス図
【図７】署名処理を行うリーダライタ３の構成を示す図
【図８】署名生成部６１の構成例を示すブロック図
【図９】第２の実施の形態に係る通信処理の詳細を示すシーケンス図
【図１０】秘密暗号を利用した通信の一例を示すブロック図
【図１１】メッセージダイジェストを利用した通信の一例を示すブロック図
【符号の説明】
【００５８】
１……通信システム
３……リーダライタ
５……媒体
７……コンピュータ
１１……制御部
１３……インタフェース
１５……メモリ
１７……暗号部
１９……送信部
２１……アンテナ部
２３……受信部
２５……復号部
２７……データランダム化部
２９……鍵保存部
３１……変換部
４１……制御部
４３……ＲＯＭ
４５……ＲＡＭ
４７……送信部
４９……アンテナ部
５１……受信部
６１……署名生成部
６３……鍵保存部

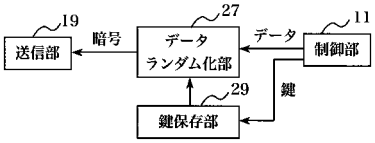
【図１】



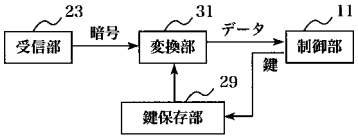
【図２】



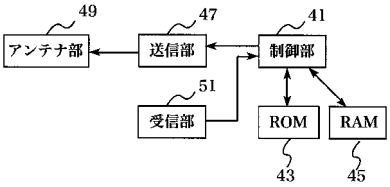
【図３】



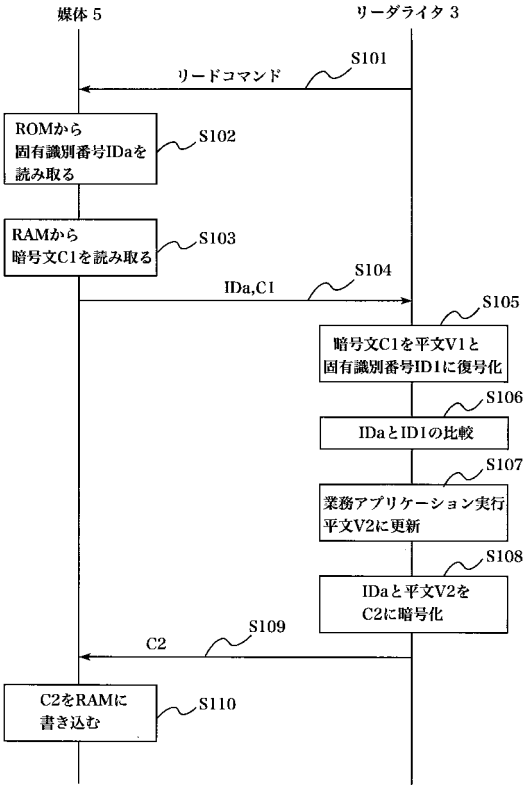
【図４】



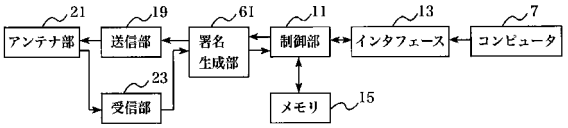
【図５】



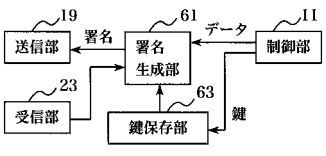
【図６】



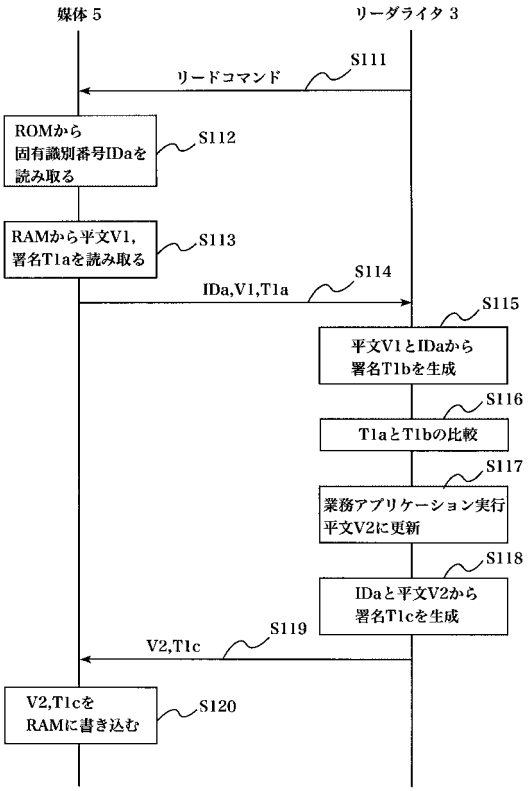
【図７】



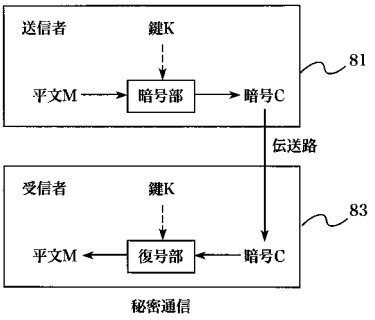
【図８】



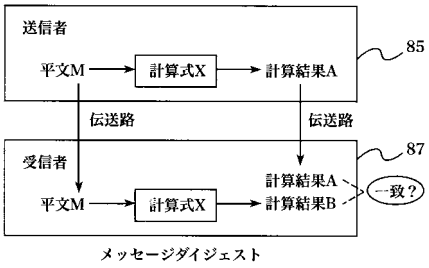
【図９】


媒体 5
リーダライタ 3
S111
リードコマンド
ROMから
固有識別番号IDaを
読み取る
S112
RAMから平文V1,
署名T1aを読み取る
S113
S114
IDa,V1,T1a
S115
平文V1とIDaから
署名T1bを生成
S116
T1aとT1bの比較
S117
業務アプリケーション実行
平文V2に更新
S118
IDaと平文V2から
署名T1cを生成
S119
V2,T1c
V2,T1cを
RAMに書き込む
S120

【図１０】


送信者
鍵K
平文M
暗号部
暗号C
81
伝送路
受信者
鍵K
平文M
復号部
暗号C
83
秘密通信

【図１１】


送信者
平文M
計算式X
計算結果A
85
伝送路
伝送路
受信者
計算結果A
平文M
計算式X
計算結果B
一致？
87
メッセージダイジェスト