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

特許第4867760号
(P4867760)

(45)発行日　平成24年2月1日(2012.2.1)　(24)登録日　平成23年11月25日(2011.11.25)

(51)Int.Cl.		F I		
G06F 21/24	(2006.01)	G06F	12/14	530D
H04L 9/32	(2006.01)	G06F	12/14	540B
G06F 3/06	(2006.01)	G06F	12/14	520P
		H04L	9/00	673A
		G06F	3/06	304H

請求項の数 21　(全 32 頁)

(21)出願番号　特願2007-94172(P2007-94172)
(22)出願日　平成19年3月30日(2007.3.30)
(65)公開番号　特開2008-250874(P2008-250874A)
(43)公開日　平成20年10月16日(2008.10.16)
審査請求日　平成22年3月15日(2010.3.15)

(73)特許権者　000002185
ソニー株式会社
東京都港区港南１丁目７番１号
(74)代理人　100082131
弁理士　稲本　義雄
(72)発明者　岡上　拓己
東京都港区港南１丁目７番１号　ソニー株式会社内

審査官　児玉　崇晶

最終頁に続く

(54)【発明の名称】情報処理装置および方法、並びに情報処理システム

(57)【特許請求の範囲】
【請求項１】
記憶媒体への外部からのアクセスを制限する情報処理装置であって、
前記情報処理装置と別体として構成される認証ユニットより、前記記憶媒体へのアクセス禁止の解除を要求するコマンドであるロック解除コマンドとともに、前記認証ユニットの認証方式を識別する認証方式IDを取得するロック解除コマンド取得手段と、
前記記憶媒体へのアクセスを指示するユーザの認証処理において正当なユーザであることを示す見本のデータとして利用される認証データであって、前記ロック解除コマンド取得手段により前記ロック解除コマンドとともに取得された前記認証方式IDに対応する認証データを前記認証ユニットに供給する認証データ供給手段と、
前記認証ユニットより、前記認証データ供給手段が供給した前記認証データを用いて行われた前記認証処理の認証結果を取得する認証結果取得手段と、
前記認証結果の内容を確認する認証結果確認手段と、
前記認証結果確認手段による確認の結果、前記ユーザが正当であると認証された場合、前記記憶媒体への外部からのアクセスの禁止を解除する解除手段と
を備える情報処理装置。
【請求項２】
所定の方法で乱数を発生する乱数発生手段をさらに備え、
前記認証データ供給手段は、前記認証データとともに、前記乱数発生手段により発生された乱数も前記認証ユニットに供給し、

前記認証結果取得手段は、前記認証ユニットより、前記認証結果とともに前記乱数も取得し、
前記認証結果確認手段は、さらに、前記認証結果取得手段により取得された前記乱数が、前記乱数発生手段により発生された乱数と一致するか否かを確認する
請求項１に記載の情報処理装置。
【請求項３】
前記認証結果取得手段により取得された前記認証結果は、前記認証ユニットにおいて、所定の電子鍵情報である秘密鍵により暗号化されており、
前記認証結果を、前記秘密鍵に対応する公開用の電子鍵情報である公開鍵を用いて復号する復号手段をさらに備える
請求項１に記載の情報処理装置。
【請求項４】
前記記憶媒体に情報を記憶させる記憶制御手段をさらに備え、
前記記憶制御手段は、前記記憶媒体の所定の記憶領域に、前記認証データ、前記認証方式ID、および前記公開鍵を記憶させる
請求項３に記載の情報処理装置。
【請求項５】
記憶媒体への外部からのアクセスを制限する情報処理装置の情報処理方法であって、
前記情報処理装置と別体として構成される認証ユニットより、前記記憶媒体へのアクセス禁止の解除を要求するコマンドであるロック解除コマンドとともに、前記認証ユニットの認証方式を識別する認証方式IDを取得し、
前記記憶媒体へのアクセスを指示するユーザの認証処理において正当なユーザであることを示す見本のデータとして利用される認証データであって、前記ロック解除コマンドとともに取得された前記認証方式IDに対応する認証データを前記認証ユニットに供給し、
前記認証ユニットより、供給した前記認証データを用いて行われた前記認証処理の認証結果を取得し、
前記認証結果の内容を確認し、
確認の結果、前記ユーザが正当であると認証された場合、前記記憶媒体への外部からのアクセスの禁止を解除する
ステップを含む情報処理方法。
【請求項６】
記憶媒体への外部からのアクセスを制限する情報処理装置であって、
前記情報処理装置と別体として構成される認証ユニットより、前記記憶媒体へのアクセス禁止の解除を要求するコマンドであるロック解除コマンドを取得するロック解除コマンド取得手段と、
所定の方法で乱数を発生する乱数発生手段と、
前記記憶媒体へのアクセスを指示するユーザの認証処理において正当なユーザであることを示す見本のデータとして利用される認証データ、および前記乱数発生手段により発生した前記乱数を前記認証ユニットに供給する認証データ供給手段と、
前記認証ユニットより、前記認証データ供給手段が供給した前記認証データを用いて行われた前記認証処理の認証結果、および乱数を取得する認証結果取得手段と、
前記認証結果の内容、並びに、前記認証結果取得手段により取得された前記乱数が前記乱数発生手段により発生された前記乱数とで値が一致するか否かを確認する確認手段と、
前記確認手段による確認の結果、前記乱数同士の値が一致し、かつ、前記ユーザが正当であると認証された場合、前記記憶媒体への外部からのアクセスの禁止を解除する解除手段と
を備える情報処理装置。
【請求項７】
前記ロック解除コマンド取得手段は、前記ロック解除コマンドとともに、前記認証ユニットの認証方式を識別する認証方式IDを取得し、

前記認証データ供給手段は、前記ロック解除コマンド取得手段により前記ロック解除コマンドとともに取得された前記認証方式IDに対応する認証データ、および前記乱数発生手段により発生した前記乱数を前記認証ユニットに供給する
請求項６に記載の情報処理装置。
【請求項８】
前記認証結果取得手段により取得された前記認証結果は、前記認証ユニットにおいて、所定の電子鍵情報である秘密鍵により暗号化されており、
前記認証結果を、前記秘密鍵に対応する公開用の電子鍵情報である公開鍵を用いて復号する復号手段をさらに備える
請求項７に記載の情報処理装置。
【請求項９】
記憶媒体への外部からのアクセスを制限する情報処理装置の情報処理方法であって、
前記情報処理装置と別体として構成される認証ユニットより、前記記憶媒体へのアクセス禁止の解除を要求するコマンドであるロック解除コマンドを取得し、
所定の方法で乱数を発生し、
前記記憶媒体へのアクセスを指示するユーザの認証処理において正当なユーザであることを示す見本のデータとして利用される認証データ、および発生した前記乱数を前記認証ユニットに供給し、
前記認証ユニットより、供給した前記認証データを用いて行われた前記認証処理の認証結果、および乱数を取得し、
前記認証結果の内容、並びに、取得された前記乱数と発生された前記乱数とで値が一致するか否かを確認し、
確認の結果、前記乱数同士の値が一致し、かつ、前記ユーザが正当であると認証された場合、前記記憶媒体への外部からのアクセスの禁止を解除する
ステップを含む情報処理方法。
【請求項１０】
外部からのアクセスが制限される記憶媒体へのアクセスに関する指示を行うユーザを認証する情報処理装置であって、
前記ユーザの認証のために前記ユーザが入力する認証データを受け付ける認証データ受付手段と、
前記記憶媒体へのアクセス禁止の解除を要求するコマンドであるロック解除コマンドとともに、前記情報処理装置において行われる前記ユーザの認証の認証方式を識別する認証方式IDを、前記記憶媒体のアクセスを制限する、前記情報処理装置と別体の入出力制御装置に供給するロック解除コマンド供給手段と、
前記入出力制御装置より、正当なユーザであることを示す見本のデータとして利用される認証データであって、前記ロック解除コマンド供給手段が前記ロック解除コマンドとともに供給した前記認証方式IDに対応する認証データを取得する認証データ取得手段と、
前記認証データ受付手段により受け付けられた前記認証データを、前記認証データ取得手段により取得された前記認証データと比較することにより、前記ユーザの認証を行う認証手段と、
前記認証手段による前記ユーザの認証の認証結果を前記入出力制御装置に供給する認証結果供給手段と
を備える情報処理装置。
【請求項１１】
前記認証データ取得手段により取得された前記認証データは、所定の暗号化方式により暗号化されている暗号化認証データであり、
前記暗号化認証データを前記所定の暗号化方式に対応する復号方式により復号する復号手段をさらに備える
請求項１０に記載の情報処理装置。
【請求項１２】

前記認証データ取得手段は、前記認証データとともに所定の乱数を取得し、
前記認証結果供給手段は、前記認証結果とともに、前記認証データ取得手段により取得された前記乱数を供給する
請求項１０に記載の情報処理装置。
【請求項１３】
所定の電子鍵情報である秘密鍵を保持する鍵保持手段と、
前記鍵保持手段により保持されている前記秘密鍵を用いて、前記認証結果を暗号化する認証結果暗号化手段と
をさらに備える請求項１０に記載の情報処理装置。
【請求項１４】
外部からのアクセスが制限される記憶媒体へのアクセスに関する指示を行うユーザを認証する情報処理装置の情報処理方法であって、
前記ユーザの認証のために前記ユーザが入力する認証データを受け付け、
前記記憶媒体へのアクセス禁止の解除を要求するコマンドであるロック解除コマンドとともに、前記情報処理装置において行われる前記ユーザの認証の認証方式を識別する認証方式IDを、前記記憶媒体のアクセスを制限する、前記情報処理装置と別体の入出力制御装置に供給し、
前記入出力制御装置より、正当なユーザであることを示す見本のデータとして利用される認証データであって、前記ロック解除コマンドとともに供給した前記認証方式IDに対応する認証データを取得し、
受け付けた前記認証データを、取得した前記認証データと比較することにより、前記ユーザの認証を行い、
前記ユーザの認証の認証結果を前記入出力制御装置に供給する
ステップを含む情報処理方法。
【請求項１５】
外部からのアクセスが制限される記憶媒体へのアクセスに関する指示を行うユーザを認証する情報処理装置であって、
前記ユーザの認証のために前記ユーザが入力する認証データを受け付ける認証データ受付手段と、
前記記憶媒体へのアクセス禁止の解除を要求するコマンドであるロック解除コマンドを、前記記憶媒体のアクセスを制限する、前記情報処理装置と別体の入出力制御装置に供給するロック解除コマンド供給手段と、
前記入出力制御装置より、正当なユーザであることを示す見本のデータとして利用される認証データとともに所定の乱数を取得する認証データ取得手段と、
前記認証データ受付手段により受け付けられた前記認証データを、前記認証データ取得手段により取得された前記認証データと比較することにより、前記ユーザの認証を行う認証手段と、
前記認証手段による前記ユーザの認証の認証結果を、前記認証データ取得手段により取得された前記乱数とともに前記入出力制御装置に供給する認証結果供給手段と
を備える情報処理装置。
【請求項１６】
前記認証データ取得手段により取得された前記認証データは、所定の暗号化方式により暗号化されている暗号化認証データであり、
前記暗号化認証データを前記所定の暗号化方式に対応する復号方式により復号する復号手段をさらに備える
請求項１５に記載の情報処理装置。
【請求項１７】
前記ロック解除コマンド供給手段は、前記ロック解除コマンドとともに、前記情報処理装置において行われる前記ユーザの認証の認証方式を識別する認証方式IDを、前記入出力制御装置に供給する

請求項１５に記載の情報処理装置。
【請求項１８】
所定の電子鍵情報である秘密鍵を保持する鍵保持手段と、
前記鍵保持手段により保持されている前記秘密鍵を用いて、前記認証結果を暗号化する認証結果暗号化手段と
をさらに備える請求項１５に記載の情報処理装置。
【請求項１９】
外部からのアクセスが制限される記憶媒体へのアクセスに関する指示を行うユーザを認証する情報処理装置の情報処理方法であって、
前記ユーザの認証のために前記ユーザが入力する認証データを受け付け、
前記記憶媒体へのアクセス禁止の解除を要求するコマンドであるロック解除コマンドを、前記記憶媒体のアクセスを制限する、前記情報処理装置と別体の入出力制御装置に供給し、
前記入出力制御装置より、正当なユーザであることを示す見本のデータとして利用される認証データとともに所定の乱数を取得し、
受け付けた前記認証データを、取得した前記認証データと比較することにより、前記ユーザの認証を行い、
前記ユーザの認証の認証結果を、取得した前記乱数とともに前記入出力制御装置に供給する
ステップを含む情報処理方法。
【請求項２０】
記憶媒体への外部からのアクセスを制限する入出力制御装置と、前記入出力制御装置とは別体の、前記記憶媒体へのアクセスに関する指示を行うユーザを認証する認証ユニットとを有する情報処理システムであって、
前記入出力制御装置は、
前記認証ユニットより、前記記憶媒体へのアクセス禁止の解除を要求するコマンドであるロック解除コマンドとともに、前記認証ユニットの認証方式を識別する認証方式IDを取得するロック解除コマンド取得手段と、
前記ユーザの認証において正当なユーザであることを示す見本のデータとして利用される認証データであって、前記ロック解除コマンド取得手段により前記ロック解除コマンドとともに取得された前記認証方式IDに対応する認証データを前記認証ユニットに供給する認証データ供給手段と、
前記認証ユニットより、前記認証データ供給手段が供給した前記認証データを用いて行われた前記ユーザの認証結果を取得する認証結果取得手段と、
前記認証結果の内容を確認する認証結果確認手段と、
前記認証結果確認手段による確認の結果、前記ユーザが正当であると認証された場合、前記記憶媒体への外部からのアクセスの禁止を解除する解除手段と
を備え、
前記認証ユニットは、
前記ユーザの認証のために前記ユーザが入力する認証データを受け付ける認証データ受付手段と、
前記ロック解除コマンドおよび前記認証方式IDを前記入出力制御装置に供給するロック解除コマンド供給手段と、
前記入出力制御装置より、前記ロック解除コマンド供給手段が前記ロック解除コマンドとともに供給した前記認証方式IDに対応する認証データを取得する認証データ取得手段と、
前記認証データ受付手段により受け付けられた前記認証データを、前記認証データ取得手段により取得された前記認証データと比較することにより、前記ユーザの認証を行う認証手段と、
前記認証手段による前記ユーザの認証の認証結果を前記入出力制御装置に供給する認

証結果供給手段と
を備える情報処理システム。
【請求項２１】
記憶媒体への外部からのアクセスを制限する入出力制御装置と、前記入出力制御装置とは別体の、前記記憶媒体へのアクセスに関する指示を行うユーザを認証する認証ユニットとを有する情報処理システムであって、
前記入出力制御装置は、
前記認証ユニットより、前記記憶媒体へのアクセス禁止の解除を要求するコマンドであるロック解除コマンドを取得するロック解除コマンド取得手段と、
所定の方法で乱数を発生する乱数発生手段と、
前記ユーザの認証において正当なユーザであることを示す見本のデータとして利用される認証データ、および前記乱数発生手段により発生した前記乱数を前記認証ユニットに供給する認証データ供給手段と、
前記認証ユニットより、前記認証データ供給手段が供給した前記認証データを用いて行われた前記ユーザの認証結果、および乱数を取得する認証結果取得手段と、
前記認証結果の内容、並びに、前記認証結果取得手段により取得された前記乱数が前記乱数発生手段により発生された前記乱数とで値が一致するか否かを確認する確認手段と、
前記確認手段による確認の結果、前記乱数同士の値が一致し、かつ、前記ユーザが正当であると認証された場合、前記記憶媒体への外部からのアクセスの禁止を解除する解除手段と
を備え、
前記認証ユニットは、
前記ユーザの認証のために前記ユーザが入力する認証データを受け付ける認証データ受付手段と、
前記ロック解除コマンドを、前記入出力制御装置に供給するロック解除コマンド供給手段と、
前記入出力制御装置より、前記認証データとともに前記乱数を取得する認証データ取得手段と、
前記認証データ受付手段により受け付けられた前記認証データを、前記認証データ取得手段により取得された前記認証データと比較することにより、前記ユーザの認証を行う認証手段と、
前記認証手段による前記ユーザの認証結果を、前記認証データ取得手段により取得された前記乱数とともに前記入出力制御装置に供給する認証結果供給手段と
を備える情報処理システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、情報処理装置および方法、並びに情報処理システムに関し、特に、より安全性および利便性を向上させたストレージメディアを実現することができるようにした情報処理装置および方法、並びに情報処理システムに関する。
【背景技術】
【０００２】
従来、パスワード認証や指紋認証等の認証技術によって、内蔵するハードディスクやフラッシュメモリ等よりなる記憶媒体について、情報の読み出しや書き込みを制限するストレージメディアが存在する（例えば特許文献１参照）。
【０００３】
このようなストレージメディアには、指紋採取部やキーボード等のような、指紋やパスワード等の認証情報を受け付ける構成が設けられており、その構成より入力された認証情報と、予め登録されている認証情報が照合され、正当なユーザであると判定された場合の

み、記憶媒体へのアクセスが許可（アンロック）され、それ以外については記憶媒体へのアクセスが禁止（ロック）される（データの読み出しや書き込みが禁止される）。このようにすることにより、記憶媒体に記憶される情報の第３者への情報の漏洩を抑制し、安全性を高めている。

【０００４】

近年、情報処理技術の向上とともに、記憶媒体の大容量化、ストレージメディアの小型化が進んでいる。

【０００５】

【特許文献１】特開２０００－７６４４３号公報

【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、上述したように、このようなストレージメディアには認証情報を受け付ける構成が設けられており、例えば、指紋パターンを採取する機構やキーボード等、その構成のためにある程度の大きさを確保する必要があり、ストレージメディアのさらなる小型化が困難になる恐れがあった。

【０００７】

また、秘密情報を記憶する記憶媒体と認証情報を受け付ける構成が１つの筐体に一体化されているため、他の認証技術を容易に適用することができない恐れがあった。認証技術の開発は恒常的に行われており、その技術レベルは日進月歩で向上している。換言するに、古い認証技術の安全性は日々低下しているともいえる。しかしながら、上述したように従来のストレージメディアの場合、予め設けられている以外の認証技術を適用することは困難であるので、将来情報技術が向上し、より安全な新たな認証技術が開発されたとしても、その認証技術を適用することができない恐れがあった。つまり、従来のストレージメディアにおいては、将来的に十分な安全性が確保できなくなる恐れがあった。

【０００８】

さらに、秘密情報を記憶する記憶媒体と認証情報を受け付ける構成が１つの筐体に一体化されていることにより、仮に認証情報が第３者に漏洩した場合、その第３者がそのストレージメディアを取得することにより、容易に秘密情報を得ることができてしまう恐れがあった。

【０００９】

本発明は、このような従来の実情に鑑みて提案されたものであり、ストレージメディアの安全性および利便性をより向上させることができるようにするものである。

【課題を解決するための手段】

【００１０】

本発明の第１の側面は、記憶媒体への外部からのアクセスを制限する情報処理装置であって、前記情報処理装置と別体として構成される認証ユニットより、前記記憶媒体へのアクセス禁止の解除を要求するコマンドであるロック解除コマンドとともに、前記認証ユニットの認証方式を識別する認証方式IDを取得するロック解除コマンド取得手段と、前記記憶媒体へのアクセスを指示するユーザの認証処理において正当なユーザであることを示す見本のデータとして利用される認証データであって、前記ロック解除コマンド取得手段により前記ロック解除コマンドとともに取得された前記認証方式IDに対応する認証データを前記認証ユニットに供給する認証データ供給手段と、前記認証ユニットより、前記認証データ供給手段が供給した前記認証データを用いて行われた前記認証処理の認証結果を取得する認証結果取得手段と、前記認証結果の内容を確認する認証結果確認手段と、前記認証結果確認手段による確認の結果、前記ユーザが正当であると認証された場合、前記記憶媒体への外部からのアクセスの禁止を解除する解除手段とを備える情報処理装置である。

【００１１】

所定の方法で乱数を発生する乱数発生手段をさらに備え、前記認証データ供給手段は、前記認証データとともに、前記乱数発生手段により発生された乱数も前記認証ユニットに

供給し、前記認証結果取得手段は、前記認証ユニットより、前記認証結果とともに前記乱数も取得し、前記認証結果確認手段は、さらに、前記認証結果取得手段により取得された前記乱数が、前記乱数発生手段により発生された乱数と一致するか否かを確認することができる。

【００１２】

前記認証結果取得手段により取得された前記認証結果は、前記認証ユニットにおいて、所定の電子鍵情報である秘密鍵により暗号化されており、前記認証結果を、前記秘密鍵に対応する公開用の電子鍵情報である公開鍵を用いて復号する復号手段をさらに備えることができる。

【００１３】

前記記憶媒体に情報を記憶させる記憶制御手段をさらに備え、前記記憶制御手段は、前記記憶媒体の所定の記憶領域に、前記認証データ、前記認証方式ID、および前記公開鍵を記憶させることができる。

【００１６】

本発明の第１の側面はまた、記憶媒体への外部からのアクセスを制限する情報処理装置の情報処理方法であって、前記情報処理装置と別体として構成される認証ユニットより、前記記憶媒体へのアクセス禁止の解除を要求するコマンドであるロック解除コマンドとともに、前記認証ユニットの認証方式を識別する認証方式IDを取得し、前記記憶媒体へのアクセスを指示するユーザの認証処理において正当なユーザであることを示す見本のデータとして利用される認証データであって、前記ロック解除コマンドとともに取得された前記認証方式IDに対応する認証データを前記認証ユニットに供給し、前記認証ユニットより、供給した前記認証データを用いて行われた前記認証処理の認証結果を取得し、前記認証結果の内容を確認し、確認の結果、前記ユーザが正当であると認証された場合、前記記憶媒体への外部からのアクセスの禁止を解除するステップを含む情報処理方法である。

【００１８】

本発明の第２の側面は、記憶媒体への外部からのアクセスを制限する情報処理装置であって、前記情報処理装置と別体として構成される認証ユニットより、前記記憶媒体へのアクセス禁止の解除を要求するコマンドであるロック解除コマンドを取得するロック解除コマンド取得手段と、所定の方法で乱数を発生する乱数発生手段と、前記記憶媒体へのアクセスを指示するユーザの認証処理において正当なユーザであることを示す見本のデータとして利用される認証データ、および前記乱数発生手段により発生した前記乱数を前記認証ユニットに供給する認証データ供給手段と、前記認証ユニットより、前記認証データ供給手段が供給した前記認証データを用いて行われた前記認証処理の認証結果、および乱数を取得する認証結果取得手段と、前記認証結果の内容、並びに、前記認証結果取得手段により取得された前記乱数が前記乱数発生手段により発生された前記乱数とで値が一致するか否かを確認する確認手段と、前記確認手段による確認の結果、前記乱数同士の値が一致し、かつ、前記ユーザが正当であると認証された場合、前記記憶媒体への外部からのアクセスの禁止を解除する解除手段とを備える情報処理装置である。

【００１９】

前記ロック解除コマンド取得手段は、前記ロック解除コマンドとともに、前記認証ユニットの認証方式を識別する認証方式IDを取得し、前記認証データ供給手段は、前記ロック解除コマンド取得手段により前記ロック解除コマンドとともに取得された前記認証方式IDに対応する認証データ、および前記乱数発生手段により発生した前記乱数を前記認証ユニットに供給することができる。

【００２０】

前記認証結果取得手段により取得された前記認証結果は、前記認証ユニットにおいて、所定の電子鍵情報である秘密鍵により暗号化されており、前記認証結果を、前記秘密鍵に対応する公開用の電子鍵情報である公開鍵を用いて復号する復号手段をさらに備えることができる。

【００２４】

本発明の第２の側面はまた、記憶媒体への外部からのアクセスを制限する情報処理装置の情報処理方法であって、前記情報処理装置と別体として構成される認証ユニットより、前記記憶媒体へのアクセス禁止の解除を要求するコマンドであるロック解除コマンドを取得し、所定の方法で乱数を発生し、前記記憶媒体へのアクセスを指示するユーザの認証処理において正当なユーザであることを示す見本のデータとして利用される認証データ、および発生した前記乱数を前記認証ユニットに供給し、前記認証ユニットより、供給した前記認証データを用いて行われた前記認証処理の認証結果、および乱数を取得し、前記認証結果の内容、並びに、取得された前記乱数と発生された前記乱数とで値が一致するか否かを確認し、確認の結果、前記乱数同士の値が一致し、かつ、前記ユーザが正当であると認証された場合、前記記憶媒体への外部からのアクセスの禁止を解除するステップを含む情報処理方法である。

【００２６】

本発明の第３の側面は、外部からのアクセスが制限される記憶媒体へのアクセスに関する指示を行うユーザを認証する情報処理装置であって、前記ユーザの認証のために前記ユーザが入力する認証データを受け付ける認証データ受付手段と、前記記憶媒体へのアクセス禁止の解除を要求するコマンドであるロック解除コマンドとともに、前記情報処理装置において行われる前記ユーザの認証の認証方式を識別する認証方式IDを、前記記憶媒体のアクセスを制限する、前記情報処理装置と別体の入出力制御装置に供給するロック解除コマンド供給手段と、前記入出力制御装置より、正当なユーザであることを示す見本のデータとして利用される認証データであって、前記ロック解除コマンド供給手段が前記ロック解除コマンドとともに供給した前記認証方式IDに対応する認証データを取得する認証データ取得手段と、前記認証データ受付手段により受け付けられた前記認証データを、前記認証データ取得手段により取得された前記認証データと比較することにより、前記ユーザの認証を行う認証手段と、前記認証手段による前記ユーザの認証の認証結果を前記入出力制御装置に供給する認証結果供給手段とを備える情報処理装置である。

【００２７】

前記認証データ取得手段により取得された前記認証データは、所定の暗号化方式により暗号化されている暗号化認証データであり、前記暗号化認証データを前記所定の暗号化方式に対応する復号方式により復号する復号手段をさらに備えることができる。

【００２８】

前記認証データ取得手段は、前記認証データとともに所定の乱数を取得し、前記認証結果供給手段は、前記認証結果とともに、前記認証データ取得手段により取得された前記乱数を供給することができる。

【００２９】

所定の電子鍵情報である秘密鍵を保持する鍵保持手段と、前記鍵保持手段により保持されている前記秘密鍵を用いて、前記認証結果を暗号化する認証結果暗号化手段とをさらに備えることができる。

【００３１】

本発明の第３の側面はまた、外部からのアクセスが制限される記憶媒体へのアクセスに関する指示を行うユーザを認証する情報処理装置の情報処理方法であって、前記ユーザの認証のために前記ユーザが入力する認証データを受け付け、前記記憶媒体へのアクセス禁止の解除を要求するコマンドであるロック解除コマンドとともに、前記情報処理装置において行われる前記ユーザの認証の認証方式を識別する認証方式IDを、前記記憶媒体のアクセスを制限する、前記情報処理装置と別体の入出力制御装置に供給し、前記入出力制御装置より、正当なユーザであることを示す見本のデータとして利用される認証データであって、前記ロック解除コマンドとともに供給した前記認証方式IDに対応する認証データを取得し、受け付けた前記認証データを、取得した前記認証データと比較することにより、前記ユーザの認証を行い、前記ユーザの認証の認証結果を前記入出力制御装置に供給するステップを含む情報処理方法である。

【００３３】

本発明の第４の側面は、外部からのアクセスが制限される記憶媒体へのアクセスに関する指示を行うユーザを認証する情報処理装置であって、前記ユーザの認証のために前記ユーザが入力する認証データを受け付ける認証データ受付手段と、前記記憶媒体へのアクセス禁止の解除を要求するコマンドであるロック解除コマンドを、前記記憶媒体のアクセスを制限する、前記情報処理装置と別体の入出力制御装置に供給するロック解除コマンド供給手段と、前記入出力制御装置より、正当なユーザであることを示す見本のデータとして利用される認証データとともに所定の乱数を取得する認証データ取得手段と、前記認証データ受付手段により受け付けられた前記認証データを、前記認証データ取得手段により取得された前記認証データと比較することにより、前記ユーザの認証を行う認証手段と、前記認証手段による前記ユーザの認証の認証結果を、前記認証データ取得手段により取得された前記乱数とともに前記入出力制御装置に供給する認証結果供給手段とを備える情報処理装置である。

【００３４】

前記認証データ取得手段により取得された前記認証データは、所定の暗号化方式により暗号化されている暗号化認証データであり、前記暗号化認証データを前記所定の暗号化方式に対応する復号方式により復号する復号手段をさらに備えることができる。

【００３５】

前記ロック解除コマンド供給手段は、前記ロック解除コマンドとともに、前記情報処理装置において行われる前記ユーザの認証の認証方式を識別する認証方式IDを、前記入出力制御装置に供給することができる。

【００３６】

所定の電子鍵情報である秘密鍵を保持する鍵保持手段と、前記鍵保持手段により保持されている前記秘密鍵を用いて、前記認証結果を暗号化する認証結果暗号化手段とをさらに備えることができる。

【００３８】

本発明の第４の側面はまた、外部からのアクセスが制限される記憶媒体へのアクセスに関する指示を行うユーザを認証する情報処理装置の情報処理方法であって、前記ユーザの認証のために前記ユーザが入力する認証データを受け付け、前記記憶媒体へのアクセス禁止の解除を要求するコマンドであるロック解除コマンドを、前記記憶媒体のアクセスを制限する、前記情報処理装置と別体の入出力制御装置に供給し、前記入出力制御装置より、正当なユーザであることを示す見本のデータとして利用される認証データとともに所定の乱数を取得し、受け付けた前記認証データを、取得した前記認証データと比較することにより、前記ユーザの認証を行い、前記ユーザの認証の認証結果を、取得した前記乱数とともに前記入出力制御装置に供給するステップを含む情報処理方法である。

【００４０】

本発明の第５の側面は、記憶媒体への外部からのアクセスを制限する入出力制御装置と、前記入出力制御装置とは別体の、前記記憶媒体へのアクセスに関する指示を行うユーザを認証する認証ユニットとを有する情報処理システムであって、前記入出力制御装置は、前記認証ユニットより、前記記憶媒体へのアクセス禁止の解除を要求するコマンドであるロック解除コマンドとともに、前記認証ユニットの認証方式を識別する認証方式IDを取得するロック解除コマンド取得手段と、前記ユーザの認証において正当なユーザであることを示す見本のデータとして利用される認証データであって、前記ロック解除コマンド取得手段により前記ロック解除コマンドとともに取得された前記認証方式IDに対応する認証データを前記認証ユニットに供給する認証データ供給手段と、前記認証ユニットより、前記認証データ供給手段が供給した前記認証データを用いて行われた前記ユーザの認証結果を取得する認証結果取得手段と、前記認証結果の内容を確認する認証結果確認手段と、前記認証結果確認手段による確認の結果、前記ユーザが正当であると認証された場合、前記記憶媒体への外部からのアクセスの禁止を解除する解除手段とを備え、前記認証ユニットは、前記ユーザの認証のために前記ユーザが入力する認証データを受け付ける認証データ受付手段と、前記ロック解除コマンドおよび前記認証方式IDを前記入出力制御装置に供給す

るロック解除コマンド供給手段と、前記入出力制御装置より、前記ロック解除コマンド供給手段が前記ロック解除コマンドとともに供給した前記認証方式IDに対応する認証データを取得する認証データ取得手段と、前記認証データ受付手段により受け付けられた前記認証データを、前記認証データ取得手段により取得された前記認証データと比較することにより、前記ユーザの認証を行う認証手段と、前記認証手段による前記ユーザの認証の認証結果を前記入出力制御装置に供給する認証結果供給手段とを備える情報処理システムである。

【００４１】

本発明の第６の側面は、記憶媒体への外部からのアクセスを制限する入出力制御装置と、前記入出力制御装置とは別体の、前記記憶媒体へのアクセスに関する指示を行うユーザを認証する認証ユニットとを有する情報処理システムであって、前記入出力制御装置は、前記認証ユニットより、前記記憶媒体へのアクセス禁止の解除を要求するコマンドであるロック解除コマンドを取得するロック解除コマンド取得手段と、所定の方法で乱数を発生する乱数発生手段と、前記ユーザの認証において正当なユーザであることを示す見本のデータとして利用される認証データ、および前記乱数発生手段により発生した前記乱数を前記認証ユニットに供給する認証データ供給手段と、前記認証ユニットより、前記認証データ供給手段が供給した前記認証データを用いて行われた前記ユーザの認証結果、および乱数を取得する認証結果取得手段と、前記認証結果の内容、並びに、前記認証結果取得手段により取得された前記乱数が前記乱数発生手段により発生された前記乱数とで値が一致するか否かを確認する確認手段と、前記確認手段による確認の結果、前記乱数同士の値が一致し、かつ、前記ユーザが正当であると認証された場合、前記記憶媒体への外部からのアクセスの禁止を解除する解除手段とを備え、前記認証ユニットは、前記ユーザの認証のために前記ユーザが入力する認証データを受け付ける認証データ受付手段と、前記ロック解除コマンドを、前記入出力制御装置に供給するロック解除コマンド供給手段と、前記入出力制御装置より、前記認証データとともに前記乱数を取得する認証データ取得手段と、前記認証データ受付手段により受け付けられた前記認証データを、前記認証データ取得手段により取得された前記認証データと比較することにより、前記ユーザの認証を行う認証手段と、前記認証手段による前記ユーザの認証結果を、前記認証データ取得手段により取得された前記乱数とともに前記入出力制御装置に供給する認証結果供給手段とを備える情報処理システムである。

【００４２】

本発明の第１の側面においては、情報処理装置と別体として構成される認証ユニットより、記憶媒体へのアクセス禁止の解除を要求するコマンドであるロック解除コマンドとともに、認証ユニットの認証方式を識別する認証方式IDが取得され、記憶媒体へのアクセスを指示するユーザの認証処理において正当なユーザであることを示す見本のデータとして利用される認証データであって、ロック解除コマンドとともに取得された認証方式IDに対応する認証データが認証ユニットに供給され、認証ユニットより、供給した認証データを用いて行われた認証処理の認証結果が取得され、認証結果の内容が確認され、その確認の結果、ユーザが正当であると認証された場合、記憶媒体への外部からのアクセスの禁止が解除される。

【００４３】

本発明の第２の側面においては、情報処理装置と別体として構成される認証ユニットより、記憶媒体へのアクセス禁止の解除を要求するコマンドであるロック解除コマンドが取得され、所定の方法で乱数が発生され、記憶媒体へのアクセスを指示するユーザの認証処理において正当なユーザであることを示す見本のデータとして利用される認証データ、および発生した乱数が認証ユニットに供給され、認証ユニットより、供給した認証データを用いて行われた認証処理の認証結果、および乱数が取得され、認証結果の内容、並びに、取得された乱数が発生された乱数とで値が一致するか否かが確認され、その確認の結果、乱数同士の値が一致し、かつ、ユーザが正当であると認証された場合、記憶媒体への外部からのアクセスの禁止が解除される。

【００４４】
本発明の第３の側面においては、ユーザの認証のためにユーザが入力する認証データが受け付けられ、記憶媒体へのアクセス禁止の解除を要求するコマンドであるロック解除コマンドとともに、情報処理装置において行われるユーザの認証の認証方式を識別する認証方式IDが、記憶媒体のアクセスを制限する、情報処理装置と別体の入出力制御装置に供給され、入出力制御装置より、正当なユーザであることを示す見本のデータとして利用される認証データであって、ロック解除コマンドとともに供給した認証方式IDに対応する認証データが取得され、受け付けられた認証データが、取得された認証データと比較されることにより、ユーザの認証が行われ、そのユーザの認証の認証結果が入出力制御装置に供給される。
【００４５】
本発明の第４の側面においては、ユーザの認証のためにユーザが入力する認証データが受け付けられ、記憶媒体へのアクセス禁止の解除を要求するコマンドであるロック解除コマンドが、記憶媒体のアクセスを制限する、情報処理装置と別体の入出力制御装置に供給され、入出力制御装置より、正当なユーザであることを示す見本のデータとして利用される認証データとともに所定の乱数が取得され、受け付けられた認証データが、取得された認証データと比較されることにより、ユーザの認証が行われ、そのユーザの認証の認証結果が、取得された乱数とともに入出力制御装置に供給される。
【００４６】
本発明の第５の側面においては、入出力制御装置において、認証ユニットより、記憶媒体へのアクセス禁止の解除を要求するコマンドであるロック解除コマンドとともに、認証ユニットの認証方式を識別する認証方式IDが取得され、ユーザの認証において正当なユーザであることを示す見本のデータとして利用される認証データであって、ロック解除コマンドとともに取得された認証方式IDに対応する認証データが認証ユニットに供給され、認証ユニットより、供給した認証データを用いて行われたユーザの認証結果が取得され、認証結果の内容が確認され、確認の結果、ユーザが正当であると認証された場合、記憶媒体への外部からのアクセスの禁止が解除され、認証ユニットにおいて、ユーザの認証のためにユーザが入力する認証データが受け付けられ、ロック解除コマンドおよび認証方式IDが入出力制御装置に供給され、入出力制御装置より、ロック解除コマンドとともに供給した認証方式IDに対応する認証データが取得され、受け付けられた認証データが取得された認証データと比較されることにより、ユーザの認証が行われ、そのユーザの認証の認証結果が入出力制御装置に供給される。
【００４７】
本発明の第６の側面においては、入出力制御装置において、認証ユニットより、記憶媒体へのアクセス禁止の解除を要求するコマンドであるロック解除コマンドが取得され、所定の方法で乱数が発生され、ユーザの認証において正当なユーザであることを示す見本のデータとして利用される認証データ、および発生した乱数が認証ユニットに供給され、認証ユニットより、供給した認証データを用いて行われたユーザの認証結果、および乱数が取得され、認証結果の内容、並びに、取得された乱数が発生された乱数とで値が一致するか否かが確認され、その確認の結果、乱数同士の値が一致し、かつ、ユーザが正当であると認証された場合、記憶媒体への外部からのアクセスの禁止が解除され、認証ユニットにおいて、ユーザの認証のためにユーザが入力する認証データが受け付けられ、ロック解除コマンドが、入出力制御装置に供給され、入出力制御装置より、認証データとともに乱数が取得され、受け付けられた認証データが、取得された認証データと比較されることにより、ユーザの認証が行われ、ユーザの認証結果が、取得された乱数とともに入出力制御装置に供給される。
【発明の効果】
【００４８】
本発明によれば、記憶媒体へのアクセスを制限することができる。特に、認証ユニットと記憶媒体を別体とすることにより、安全性および利便性をより向上させることができる

。
【発明を実施するための最良の形態】
【００８２】
以下、本発明の実施の形態について説明する。
【００８３】
図１は、本発明を適用した、記憶媒体のデータの入出力を制御する制御システムの構成例を示す図である。この制御システムは、認証ユニット１０１、認証ユニット１０２、または認証ユニット１０３を用いて、それらとは別体のストレージメディア１１１に内蔵される記憶部１１２への、リーダライタ１２１によるデータの入出力を制御するシステムである。
【００８４】
認証ユニット１０１は、ユーザの指紋パターンを検出する機構を有し、検出した指紋パターンをユーザ認証に利用する認証データとする指紋認証方式を採用した認証ユニットである。認証ユニット１０２は、例えばキーボード等を有し、入力されたパスワードをユーザ認証に利用する認証データとするパスワード認証方式を採用した認証ユニットである。認証ユニット１０３は、例えば、虹彩を採取するためのCCDカメラ等を有し、採取した虹彩をユーザ認証に利用する認証データとする虹彩認証方式を採用した認証ユニットである。
【００８５】
ストレージメディア１１１は、例えばフラッシュメモリ等により構成される記憶部１１２を内蔵し、各種情報を記憶する。リーダライタ１２１は、所定の状態においてこのストレージメディア１１１と通信を行うことができるようになされており、通信可能な状態において、記憶部１１２に記憶されているデータを読み出したり、記憶部１１２にデータを書き込んだりする。なお、ここでいうデータとは、記憶部１１２に記憶されている情報全般を示しており、ストレージメディア１１１や認証ユニット１０１等において実行されないプログラム等も含まれるものとする。
【００８６】
ストレージメディア１１１は、許可（アンロック）と禁止（ロック）の２つのモードを有しており、リーダライタ１２１は、ストレージメディア１１１が許可（アンロック）の状態にあるとき、記憶部１１２にアクセスすることができ、記憶部１１２よりデータを読み出したり、記憶部１１２にデータを書き込んだりすることができる。逆に、ストレージメディア１１１が禁止（ロック）の状態にあるときは、リーダライタ１２１は、記憶部１１２にアクセスすることはできず、記憶部１１２よりデータを読み出したり、記憶部１１２にデータを書き込んだりすることはできない。
【００８７】
認証ユニット１０１乃至認証ユニット１０３は、所定の状態においてこのストレージメディア１１１と通信を行うことができるようになされており、それぞれ認証技術により、リーダライタ１２１によるストレージメディア１１１の記憶部１１２へのアクセスを制限する。ストレージメディア１１１は、これらの認証ユニットによりユーザが認証された場合のみ、つまり、正当なユーザが承認する場合のみ、リーダライタ１２１による記憶部１１２へのアクセスを許可する。
【００８８】
詳細については後述するが、リーダライタ１２１からのアクセスが禁止されたストレージメディア１１１の記憶部１１２には、照合用の認証データが記憶（登録）されている。ストレージメディア１１１は、例えば認証ユニットに接続される等して認証ユニットと通信可能な状態にされると、認証ユニットからの要求に基づいて、記憶している認証データを認証ユニットに供給する。認証ユニットは、ユーザにより入力された認証データと、ストレージメディア１１１より取得した認証データとを比較してユーザ認証を行う。その認証結果はストレージメディア１１１に供給され、ユーザが正当であると認証された場合、リーダライタ１２１からの記憶部１１２へのアクセスが許可（アンロック）される。

【００８９】
従って、ストレージメディア１１１は、認証方式によらず、認証ユニット１０１乃至認証ユニット１０３のいずれも利用することができる。つまり、ストレージメディア１１１は、指紋認証やパスワード認証以外にも、例えば、眼球の黒目に現れる皺のパターンを識別して本人確認を行う認証方式である虹彩認証、手のひらや指先の静脈パターンにより本人確認を行う認証方式である静脈認証、顔の輪郭の形状により本人確認を行う認証方式である輪郭認証、声の特徴で本人確認を行う認証方式である声紋認証、DNA（Deoxyribonucleic acid）の塩基配列のパターンにより本人確認を行う認証方式であるDNA認証、利用の度に変化するパスワードを用いて本人確認を行う認証方式であるワンタイムパスワード認証、第３者による証明を利用して本人確認を行う認証方式である電子認証、またはデバイスにより本人確認を行う認証方式であるハードウェアキー等、どのような認証方式にも対応することができる。図１の認証ユニット１０１乃至認証ユニット１０３は、認証ユニットの例を示したものであり、ストレージメディア１１１は、これら以外の認証ユニットでも同様にユーザ認証を行うことができる。
【００９０】
各認証ユニットとストレージメディア１１１との間の通信方式は任意である。例えば、ストレージメディア１１１が、認証ユニットに設けられたストレージメディア用のスロットに通信可能に装着されるようにしてもよいし、有線のケーブルを介して通信可能に認証ユニットと接続されるようにしてもよい。そのような場合、ストレージメディア１１１は、例えば、PCIExpress（Peripheral Components Interconnect Express bus）、USB（Universal Serial Bus）、若しくはIEEE（Institute of Electrical and Electronic Engineers）１３９４のような有線のバス、またはLAN（Local Area Network）のようなネットワークを介して認証ユニットと通信を行う。また、例えば、ストレージメディア１１１および各認証ユニットが、IEEE802.11xや、RF（Radio Frequency）、ブルートゥース（Bluetooth）のような近距離無線通信機能、またはIrDA（Infrared Data Association）のような赤外線通信機能を有し、互いに通信可能な範囲内に位置する状態で、無線通信または赤外線通信を行うようにしてもよい。
【００９１】
同様に、ストレージメディア１１１とリーダライタ１２１との間の通信方式も任意である。例えば、ストレージメディア１１１が、リーダライタ１２１に設けられたストレージメディア用のスロットに通信可能に装着されるようにしてもよいし、有線のケーブルを介して通信可能にリーダライタ１２１と接続されるようにしてもよい。そのような場合、ストレージメディア１１１は、例えば、PCIExpress、USB、若しくはIEEE１３９４のような有線のバス、またはLANのようなネットワークを介してリーダライタ１２１と通信を行う。また、例えば、ストレージメディア１１１およびリーダライタ１２１が、IEEE802.11xや、RF、ブルートゥースのような近距離無線通信機能、またはIrDAのような赤外線通信機能を有し、互いに通信可能な範囲内に位置する状態で、無線通信または赤外線通信を行うようにしてもよい。
【００９２】
なお、認証ユニットとリーダライタ１２１は、一体として構成されてもよいが、ストレージメディア１１１はそれらと別体に構成される。認証ユニットとリーダライタ１２１が一体として構成される場合、認証ユニットとストレージメディア１１１を接続するバスと、リーダライタ１２１とストレージメディア１１１を接続するバスは、互いに同一（共通）であってもよいが、その通信は互いに独立している。また、図１に示される制御システムにおいて、認証ユニット１０１、ストレージメディア１１１、およびリーダライタ１２１の数はそれぞれ任意である。
【００９３】
次に、各デバイスの構成例について説明する。なお、以下においては、認証ユニット１０１についてのみ説明し、認証ユニット１０２および認証ユニット１０３についての説明は、必要な場合を除いて省略する。

【００９４】
図２は、図１の認証ユニット１０１の内部の構成例を示すブロック図である。
【００９５】
図２において、認証ユニット１０１は、認証データ受付部２０１、暗号化部２０２、認証方式ID提供部２０３、鍵保持部２０４、入出力制御部２０５、ストレージメディアインタフェース部２０６、ロック解除コマンド供給部２２１、復号部２２２、比較部２２３、および暗号化部２２４を有する。
【００９６】
認証データ受付部２０１は、ユーザの指紋パターンを検出してデータ化する。認証データをストレージメディア１１１に登録し、アクセスの制限を開始する場合、認証データ受付部２０１は、得られた指紋パターンのデータを認証データとして暗号化部２０２に供給する。また、記憶部１１２へのアクセスを許可（アンロック）する場合、認証データ受付部２０１は、得られた指紋パターンのデータを認証データとして比較部２２３に供給するとともに、ロック解除コマンド供給部２２１に、ユーザの指紋パターンを検出して認証データを生成した旨を通知する。
【００９７】
暗号化部２０２は、通信時、または、ストレージメディア１１１で保存する際に、認証データの漏洩の危険性を低下させるために、認証データ受付部２０１において受け付けられた認証データを独自の方式で暗号化し、暗号化認証データを生成する。
【００９８】
この暗号化の方式は任意であるが、一般的でない専用の暗号化方式を用いることにより、認証データ漏洩の危険性を更に低下させることができる。ただし、本発明を適用した制御システムにおいて適用される、同じ認証方式の認証ユニット間において暗号化方式（暗号鍵）を共通とすることにより、ストレージメディア１１１は、ユーザの認証データを登録した認証ユニット以外の認証ユニットでもユーザ認証を行うことができるようになり、利便性が向上する。
【００９９】
暗号化部２０２は、認証データを暗号化して得られた暗号化認証データを入出力制御部２０５に供給する。
【０１００】
認証方式ID提供部２０３は、この認証ユニットが採用する認証方式を識別する認証方式IDを提供する。つまり、認証方式ID提供部２０３は、指紋認証を示す認証方式IDを保持しており、必要に応じてその認証方式IDを入出力制御部２０５に供給する。
【０１０１】
鍵保持部２０４は、他のデバイスに供給するための所定の電子鍵データである公開鍵２１１およびその公開鍵２１１に対応する秘密鍵２３１を保持しており、必要に応じて、その公開鍵２１１を入出力制御部２０５に供給する。
【０１０２】
入出力制御部２０５は、認証ユニット１０１とストレージメディア１１１との間の情報の授受を制御する。入出力制御部２０５は、暗号化部２０２より暗号化認証データを供給されると、認証方式ID提供部２０３より認証方式IDを取得し、さらに鍵保持部２０４より公開鍵２１１を取得する。そして入出力制御部２０５は、その暗号化認証データ、認証方式ID、および公開鍵２１１を、ストレージメディアインタフェース部２０６を介してストレージメディア１１１に供給する。また、入出力制御部２０５は、ロック解除コマンド供給部２２１より供給されたロック解除コマンドを、ストレージメディアインタフェース部２０６を介してストレージメディア１１１に供給する。さらに、入出力制御部２０５は、ストレージメディアインタフェース部２０６を介して取得した、ストレージメディア１１１より供給された認証データおよび乱数を復号部２２２に供給する。また、入出力制御部２０５は、暗号化部２２４より供給された暗号化データを、ストレージメディアインタフェース部２０６を介してストレージメディア１１１に供給する。

【０１０３】
ストレージメディアインタフェース部２０６は、ストレージメディア１１１用のインタフェースであり、所定の通信方式によりストレージメディア１１１と通信を行い、ストレージメディア１１１より供給されるデータを入出力制御部２０５に供給したり、入出力制御部２０５より供給されたデータをストレージメディア１１１に供給したりする。
【０１０４】
ロック解除コマンド供給部２２１は、認証データ受付部２０１より、ユーザの指紋パターンを検出して認証データを生成した旨を通知されると、ロック解除コマンドを、入出力制御部２０５を介してストレージメディア１１１に供給する。
【０１０５】
復号部２２２は、ストレージメディア１１１より供給された暗号化認証データおよび乱数を、入出力制御部２０５を介して取得すると、暗号化認証データを、暗号化部２０２の暗号化方式に対応する独自の復号方式により復号し、平文の認証データを得る。復号部２２２は、その認証データおよび乱数を比較部２２３に供給する。
【０１０６】
比較部２２３は、認証データ受付部２０１より供給された認証データと、復号部２２２より供給された認証データとを比較し、それらが一致するか否かを判定し、その判定結果を認証結果として、乱数とともに暗号化部２２４に供給する。暗号化部２２４は、比較部２２３より供給された認証結果および乱数を、第３者に漏洩しないように安全にストレージメディア１１１に供給するために、鍵保持部２０４より供給された秘密鍵２３１を用いて暗号化し、得られた暗号化データを、入出力制御部２０５を介してストレージメディア１１１に供給する。
【０１０７】
なお、認証ユニット１０２および認証ユニット１０３も、認証データ受付部２０１が受け付けるデータや、その受け付けたデータより生成する認証データが異なることと、認証方式ID提供部２０３が提供する認証方式IDの値が異なることを除けば、図２に示される認証ユニット１０１の構成と同様の構成を有する。すなわち、本発明を適用した認証ユニットはその認証方式によらず、図２に示される構成を有する。
【０１０８】
次に、ストレージメディア１１１の構成例について説明する。図３は、ストレージメディア１１１の内部の構成例を示すブロック図である。ここでは、認証処理を行う認証ユニットとして認証ユニット１０１を例に説明する。以下の説明は、認証方式によらないので、認証ユニット１０１以外の認証ユニットにより認証を行う場合も基本的に同様である。
【０１０９】
図３に示されるように、ストレージメディア１１１は、記憶部１１２の他に、リーダライタ１２１からの記憶部１１２へのアクセスを許可したり禁止したりする制御部３０１、および、リーダライタ１２１用のインタフェースであるデータバスインタフェース部３０２を有する。
【０１１０】
制御部３０１は、認証ユニットインタフェース部３１１、入出力制御部３１２、ロック制御部３１３、エラー処理部３１４、乱数発生部３１５、復号部３１６、および一致判定部３１７を有する。
【０１１１】
認証ユニットインタフェース部３１１は、認証ユニット１０１用のインタフェースであり、所定の通信方式により認証ユニット１０１と通信を行い、認証ユニット１０１より供給されるデータを入出力制御部３１２に供給したり、入出力制御部３１２より供給されたデータを認証ユニット１０１に供給したりする。
【０１１２】
入出力制御部３１２は、認証ユニット１０１とストレージメディア１１１との間のデータの授受を制御する。入出力制御部３１２は、認証ユニットインタフェース部３１１を介

して取得した、認証ユニット１０１より供給された暗号化認証データ、認証方式ID、および公開鍵２１１を、記憶部１１２に供給し、その秘匿エリア３２１にそれらのデータを保存させる。また、入出力制御部３１２は、暗号化認証データを記憶部１１２に保存させた旨をロック制御部３１３に通知する。

【０１１３】

さらに、入出力制御部３１２は、認証ユニット１０１より供給されたロック解除コマンドを、認証ユニットインタフェース部３１１を介して取得すると、その旨をロック制御部３１３に通知し、リーダライタ１２１による記憶部１１２へのアクセスが禁止（ロック）されていることを確認し、乱数発生部３１５に乱数を発生させて取得し、さらに記憶部１１２より、供給した認証方式IDに対応する暗号化認証データを取得すると、その暗号化認証データと乱数を、認証ユニットインタフェース部３１１を介して認証ユニット１０１に供給する。また、入出力制御部３１２は、認証ユニットインタフェース部３１１を介して取得した、認証ユニット１０１より供給された暗号化データを復号部３１６に供給する。

【０１１４】

ロック制御部３１３は、リーダライタ１２１からの記憶部１１２へのアクセスを禁止（ロック）したり、その禁止を解除（アンロック）したりする。例えば、ロック制御部３１３は、入出力制御部３１２より、ロックコマンドとともに、暗号化認証データ、認証方式ID、および公開鍵２１１の保存を通知されると、リーダライタ１２１からの記憶部１１２へのアクセスを禁止（ロック）する。また、ロック制御部３１３は、入出力制御部３１２よりロック解除コマンドの取得を通知されると、現在、リーダライタ１２１からの記憶部１１２へのアクセスが禁止（ロック）されているのであれば、その旨を入出力制御部３１２に通知する。例えば、暗号化認証データが登録されていなかったり、既にロックが解除（アンロック）されていたりして、リーダライタ１２１からの記憶部１１２へのアクセスが禁止されていない場合、エラー処理部３１４にその旨を通知し、エラー処理を実行させる。さらに、ロック制御部３１３は、一致判定部３１７の判定結果に基づいて、認証データが一致するのであれば、記憶部１１２の情報の入出力の禁止を解除（アンロック）する。

【０１１５】

エラー処理部３１４は、ロック制御部３１３または一致判定部３１７のエラー判定に基づいてエラー処理を行う。乱数発生部３１５は、認証ユニット１０１との通信を識別するセッションIDとして利用される乱数を発生し、入出力制御部３１２および一致判定部３１７に供給する。復号部３１６は、認証ユニット１０１より供給された暗号化データを、入出力制御部３１２より供給されると、記憶部１１２より公開鍵２１１を取得し、その公開鍵２１１を用いて暗号化データを復号する。復号部３１６は、その復号結果である認証結果と乱数を一致判定部３１７に供給する。

【０１１６】

一致判定部３１７は、復号部３１６より供給された乱数と、乱数発生部３１５より供給された乱数とを比較し、それらの値が一致するか否かを判定する。乱数の値が一致する場合、一致判定部３１７は、さらに、復号部３１６より供給された認証結果を参照し、認証データが一致したか否かを判定する。認証データが一致したと判定した場合、一致判定部３１７は、その旨をロック制御部３１３に通知する。また、乱数の値が一致しない場合、または、認証データが一致しなかったと判定した場合、一致判定部３１７は、エラー処理部３１４にその旨を通知し、エラー処理を実行させる。

【０１１７】

データバスインタフェース部３０２は、リーダライタ１２１用のインタフェースであり、上述した制御部３０１によりリーダライタ１２１からの記憶部１１２へのアクセスが制限されるデータバスのインタフェースである。つまり、データバスインタフェース部３０２を介して授受されるデータは、記憶部１１２に記憶される、制御部３０１により入出力の可否が制限される通常のデータである。データバスインタフェース部３０２は、所定の通信方式によりリーダライタ１２１と通信を行い、リーダライタ１２１より供給されるデ

ータを記憶部１１２に供給して記憶させたり、記憶部１１２より供給されたデータをリーダライタ１２１に供給したりする。なお、この通常のデータは、漏洩を抑制するために、所定の暗号化方式で暗号化されているようにしてもよい。

【０１１８】

記憶部１１２には、通常のデータを記憶する領域の他に、ユーザ認証に用いられるデータが記憶される領域である秘匿エリア３２１が設けられている。この秘匿エリア３２１は、情報漏洩抑制のために、リーダライタ１２１からアクセスすることが出来ないようになされている。この秘匿エリア３２１には、認証ユニット１０１より供給される暗号化認証データ３３１、認証方式ID、および公開鍵２１１が記憶される。

【０１１９】

次に、以上のようなシステムの各装置による処理の流れを説明する。最初に、図４のフローチャートを参照して、認証データ登録時の認証ユニット１０１およびストレージメディア１１１により実行されるロック処理の流れの例を説明する。必要に応じて図５乃至図８を参照して説明する。

【０１２０】

例えば、リーダライタ１２１による記憶部１１２へのアクセスを制限する場合、最初に正当なユーザの認証データをストレージメディア１１１に登録する（記憶させる）必要がある。そのとき、認証ユニット１０１およびストレージメディア１１１は、図４に示されるように処理を行う。

【０１２１】

最初に、認証ユニット１０１の認証データ受付部２０１は、ステップＳ１において、認証データを受け付ける。例えば、認証データが登録されていないストレージメディア１１１が認証ユニット１０１と通信可能な状態になされると、認証データ受付部２０１は、所定の方法でユーザに指紋パターンを入力させるように促し、例えば図５に示されるように、入力されたユーザの指紋パターンを検出してデータ化し、そのデータを認証データとする。

【０１２２】

ステップＳ２において、暗号化部２０２は、例えば図６に示されるように、認証データ受付部２０１において受け付けられた認証データを独自方式で暗号化する。

【０１２３】

認証ユニット１０１は、例えば図７に示されるように、公開鍵（Ｋｐ）２１１と秘密鍵（Ｋｓ）２３１、並びに認証方式ID３３２を保持している。入出力制御部２０５は、ステップＳ３において、例えば図８に示されるように、暗号化部２０２が認証データを暗号化して生成した暗号化認証データ３３１、認証方式ID提供部２０３より提供された、指紋認証方式を示す値の認証方式ID３３２、および鍵保持部２０４より取得した電子鍵データである公開鍵（Ｋｐ）２１１を、記憶部１１２のデータの入出力を禁止するように要求するロックコマンドとともに、ストレージメディアインタフェース部２０６を介してストレージメディア１１１に供給する。

【０１２４】

ストレージメディア１１１の入出力制御部３１２は、ステップＳ２１において、そのストレージメディア１１１より供給された暗号化認証データ３３１、認証方式ID３３２、および公開鍵（Ｋｐ）２１１を取得すると、記憶部１１２は、ステップＳ２２において、その入出力制御部３１２が取得した暗号化認証データ３３１、認証方式ID３３２、および公開鍵（Ｋｐ）２１１を秘匿エリア３２１に保存する。ステップＳ２３において、ロック制御部３１３は、リーダライタ１２１からの記憶部１１２へのアクセスを禁止（ロック）する。

【０１２５】

以上のように、認証データが登録されると、リーダライタ１２１からの記憶部１１２へのアクセスが禁止（ロック）される。

【０１２６】

次に、図９のフローチャートを参照して、記憶部１１２のロック解除時の認証ユニット１０１およびストレージメディア１１１により実行されるロック解除処理の流れの例を説明する。必要に応じて図１０および図１１を参照して説明する。

【０１２７】

例えば、リーダライタ１２１による記憶部１１２へのアクセスを許可する場合、アクセスを行うユーザの認証が必要になる。そのとき、認証ユニット１０１およびストレージメディア１１１は、図９に示されるように処理を行う。

【０１２８】

最初に、認証ユニット１０１の認証データ受付部２０１は、ステップＳ４１において、認証データを受け付ける。例えば、認証データが登録されているストレージメディア１１１が認証ユニット１０１と通信可能な状態になされると、認証データ受付部２０１は、所定の方法でユーザに指紋パターンを入力させるように促し、例えば図１０に示されるように、入力されたユーザの指紋パターンを検出してデータ化し、そのデータを認証データとする。

【０１２９】

認証データが受け付けられると、ロック解除コマンド供給部２２１は、ステップＳ４２において、ロック解除コマンドを、認証ユニット１０１の認証方式IDとともに、入出力制御部２０５を介してストレージメディア１１１に供給する。ストレージメディア１１１の入出力制御部３１２は、ステップＳ６１において、そのロック解除コマンドを取得する。ステップＳ６２において、乱数発生部３１５は、乱数Ｒｍを発生する。入出力制御部３１２は、ステップＳ６３において、認証ユニット１０１の認証方式IDに対応する暗号化認証データ３３１を秘匿エリア３２１より取得すると、例えば図１１に示されるように、その暗号化認証データ３３１、および、ステップＳ６２の処理により生成された乱数Ｒｍを、ロック解除コマンドの供給元である認証ユニット１０１に供給する。

【０１３０】

認証ユニット１０１の入出力制御部２０５は、ステップＳ４４において、その暗号化認証データ３３１および乱数Ｒｍを取得する。ステップＳ４５において、復号部２２２は、ステップＳ４４において取得された暗号化認証データ３３１を独自復号方式で復号する。ステップＳ４６において、比較部２２３は、ステップＳ４１において取得した認証データと、ステップＳ４５において復号された認証データを比較する。

【０１３１】

ステップＳ４７において、暗号化部２２４は、第３者に情報が漏洩しないように、ステップＳ４６における比較結果である認証結果と、ステップＳ４４において取得した乱数Ｒｍとを、秘密鍵（Ｋｓ）２３１を用いて暗号化する。ステップＳ４８において、入出力制御部２０５は、ステップＳ４７の処理において暗号化された暗号化データをストレージメディア１１１に供給する。ストレージメディア１１１の入出力制御部３１２は、ステップＳ６４において、その暗号化データを取得する。

【０１３２】

復号部３１６は、ステップＳ６５において、ステップＳ６４の処理において取得された暗号化データを、公開鍵（Ｋｐ）２１１を用いて復号する。一致判定部３１７は、ステップＳ６６において、ステップＳ６４の処理において取得された乱数Ｒｍと、ステップＳ６２において発生した乱数とが一致するか否かを確認する。また、ステップＳ６７において、一致判定部３１７は、ステップＳ６５において復号されて得られた平文の認証結果を参照し、正当なユーザであると認証されたか否かを判定する。

【０１３３】

乱数Ｒｍが一致し、認証結果が真である場合、ロック制御部３１３は、ステップＳ６８において、リーダライタ１２１による記憶部１１２へのアクセスを許可する（ロックを解除する）。

【０１３４】

なお、以上のようにして許可されたアクセスは、所定の条件が満たされた場合に、ロッ

ク制御部３１３によって再度禁止される（ロックされる）。例えばリーダライタ１２１とストレージメディア１１１が有線のデータバスで接続されている場合、そのデータバスが電気的に切断されると、ロック制御部３１３は、リーダライタ１２１による記憶部１１２へのアクセスを再度禁止にする（ロックする）。この場合、再度、データバスを接続してもリーダライタ１２１による記憶部１１２へのアクセスは禁止されたまま（ロックされた状態）であり、ロックを解除するためには、改めて図９のフローチャートのようなユーザ認証を行う必要がある。リーダライタ１２１とストレージメディア１１１が無線通信により通信を行う場合も同様であり、リーダライタ１２１とストレージメディア１１１の無線通信が切断されると、ロック制御部３１３は、リーダライタ１２１による記憶部１１２へのアクセスを再度禁止にする（ロックする）。なお、ロック制御部３１３がリーダライタ１２１による記憶部１１２へのアクセスを禁止にする条件は任意でありこれ以外でもよい。例えば、ロックが解除されてから所定の時間が経過すると、ロック制御部３１３がリーダライタ１２１による記憶部１１２へのアクセスを禁止にするようにしてもよい。

【０１３５】

次に、以上のようなロック時、アンロック時のストレージメディア１１１の制御部３０１において実行される処理の具体的な流れについて説明する。

【０１３６】

最初に、図１２のフローチャートを参照して、制御部３０１が、認証データの登録時に行うロック処理の流れの例を説明する。

【０１３７】

ステップＳ８１において、入出力制御部３１２は、認証ユニット１０１よりコマンドを取得したか否かを判定し、コマンドが供給されるまで待機する。コマンドを取得したと判定されると、処理はステップＳ８２に進む。ステップＳ８２において、入出力制御部３１２は、取得したコマンドがロックコマンドであるか否かを判定する。ロックコマンドであると判定された場合、処理はステップＳ８３に進む。ステップＳ８３において、ロック制御部３１３は、記憶部１１２が既にロックされているか否かを判定する。リーダライタ１２１による記憶部１１２へのアクセスがまだ禁止されていないと判定された場合、処理はステップＳ８４に進む。

【０１３８】

ステップＳ８４において、入出力制御部３１２は、さらに、暗号化認証データ３３１、認証方式ID３３２、および公開鍵２１１が供給されたか否かを判定し、供給されるまで待機する。暗号化認証データ３３１、認証方式ID３３２、および公開鍵２１１を取得したと判定された場合、処理はステップＳ８５に進む。ステップＳ８５において、入出力制御部３１２は、取得した暗号化認証データ３３１、認証方式ID３３２、および公開鍵２１１を記憶部１１２の秘匿エリア３２１に供給し、保存させる。ステップＳ８６において、ロック制御部３１３は、リーダライタ１２１による記憶部１１２へのアクセスを禁止する（ロックする）。ステップＳ８６の処理が終了すると、処理は、ステップＳ８１に戻る。

【０１３９】

また、ステップＳ８２において、入出力制御部３１２が取得したコマンドがロックコマンドでないと判定された場合、処理は、ステップＳ８７に進む。ステップＳ８７において、入出力制御部３１２は、他のコマンド処理を実行させる。ステップＳ８７の処理が終了すると、ロック処理が終了される。

【０１４０】

また、ステップＳ８３において、記憶部１１２が既にロックされていると判定された場合、処理はステップＳ８８に進む。ステップＳ８８において、エラー処理部３１４は、エラー処理を行う。ステップＳ８８の処理が終了すると、ロック処理は終了される。

【０１４１】

次に、図１３のフローチャートを参照して、制御部３０１が、ロック解除を要求された時に行うアンロック処理の流れの例を説明する。

【０１４２】

ステップＳ１０１において、入出力制御部３１２は、認証ユニット１０１よりコマンドを取得したか否かを判定し、取得したと判定するまで待機する。コマンドを取得したと判定された場合、処理はステップＳ１０２に進む。ステップＳ１０２において、入出力制御部３１２は、取得したコマンドがロック解除コマンドであるか否かを判定する。ロック解除コマンドであると判定された場合、処理はステップＳ１０３に進む。ステップＳ１０３において、ロック制御部３１３は、記憶部１１２がロックされているか否かを判定する。リーダライタ１２１による記憶部１１２へのアクセスが禁止されていると判定された場合、処理はステップＳ１０４に進む。

【０１４３】

ステップＳ１０４において、乱数発生部３１５は乱数を発生する。ステップＳ１０５において、入出力制御部３１２は、ステップＳ１０４の処理により発生した乱数、および、ステップＳ１０１においてロック解除コマンドとともに取得した、認証ユニット１０１の認証方式IDに対応する暗号化認証データを認証ユニット１０１に供給する。ステップＳ１０６において、入出力制御部３１２は、認証ユニット１０１より供給される暗号化データを取得したか否かを判定し、取得したと判定するまで待機する。暗号化データを取得したと判定された場合、入出力制御部３１２は、処理をステップＳ１０７に進める。

【０１４４】

ステップＳ１０７において、復号部３１６は、暗号化データを公開鍵で復号する。ステップＳ１０８において、一致判定部３１７は、認証ユニット１０１より供給された乱数がステップＳ１０４の処理により発生された乱数と一致したか否かを判定する。乱数が一致したと判定された場合、処理は、ステップＳ１０９に進む。ステップＳ１０９において、一致判定部３１７は、認証ユニット１０１より供給された認証結果が真であるか否かを判定する。認証結果が真であると判定された場合、処理はステップＳ１１０に進む。

【０１４５】

ステップＳ１１０において、ロック制御部３１３は、リーダライタ１２１による記憶部１１２へのアクセスの禁止（ロック）を解除する。ステップＳ１１０の処理が終了すると処理はステップＳ１０１に戻る。

【０１４６】

ステップＳ１０２において、取得したコマンドがロック解除コマンドではないと判定された場合、処理はステップＳ１１１に進む。ステップＳ１１１において、入出力制御部３１２は、他のコマンド処理を実行させる。ステップＳ１１１の処理が終了すると、アンロック処理が終了される。

【０１４７】

また、ステップＳ１０３において、記憶部１１２がロックされていないと判定された場合、処理はステップＳ１１２に進む。また、ステップＳ１０８において、乱数が一致しないと判定された場合も、処理はステップＳ１１２に進む。さらに、ステップＳ１０９において、認証結果が偽であると判定された場合も、処理はステップＳ１１２に進む。ステップＳ１１２において、エラー処理部３１４は、エラー処理を行う。ステップＳ１１２の処理が終了すると、アンロック処理は終了される。

【０１４８】

以上のように、認証方式IDを利用することにより、暗号化認証データを要求する認証ユニットに対して、ストレージメディア１１１が容易に適切な暗号化認証データを供給することができる。

【０１４９】

なお、ストレージメディア１１１が１つの暗号化認証データを保持しない場合、どの認証ユニットに対しても唯一の暗号化認証データを供給すれば、認証ユニットが認証処理を行うことは可能であるが、不要なデータの授受が増大するので、認証処理の負荷が増大し、処理時間が長くなる恐れがある。また、場合によっては、未対応の暗号化認証データを処理することにより認証ユニットが故障してしまう恐れもある。

【０１５０】

これに対して、認証方式IDを利用して、認証ユニットの認証方式に対応する場合のみ、ストレージメディア１１１が保持している暗号化認証データを認証ユニットに供給するようにすることにより、ストレージメディア１１１が複数種類の認証方式の認証ユニットに対応することができるだけでなく、不要なデータの授受を低減し、認証処理の負荷を軽減させることができる。これにより認証処理の高速化を実現することができる。また、認証ユニットの故障発生の可能性を低減させ、認証処理の安全性を向上させることができる。

【０１５１】

また、ユーザを認証する認証ユニットと、データを記憶するストレージメディア１１１とを別体として構成するようにしたので、ストレージメディア１１１の小型化を容易に実現することができる。このような小型化により、ストレージメディア１１１の携帯がさらに容易になり、ストレージメディア１１１を適用可能な装置の種類も増加し、さらに、製造コストや消費電力を低減させることも出来る。このようにストレージメディア１１１の利便性が向上する。

【０１５２】

また、認証ユニットとストレージメディア１１１を別体とすることにより、ストレージメディア１１１が第３者に取得された場合の、情報漏洩の危険性を低減させることができる。また、上述したように、ストレージメディア１１１が認証ユニットの認証方式によらず、認証結果のみに基づいてロックまたはロックの解除を行うことができるので、現時点において未確認の認証方式であっても容易に適用することができる。例えば、より安全でより利便性の高い認証方式が今後新たに開発された場合、その認証方式の認証ユニットを、上述したようにストレージメディア１１１とデータの授受を行うようにすることにより、ストレージメディア１１１の変更は不要になる。

【０１５３】

また、ストレージメディア１１１は、ロック解除時に、乱数を発生して、その乱数を授受することにより通信相手となる認証ユニットの確認を行うので、なりすまし等による情報漏洩の危険性を低減させることができる。

【０１５４】

以上のように、より安全性および利便性を向上させたストレージメディアを実現することができる。

【０１５５】

なお、図３においては、記憶部１１２の秘匿エリア３２１に暗号化認証データ３３１、認証方式ID、および公開鍵（Ｋｐ）２１１が１つずつ記憶されている例の様子を示したが、秘匿エリア３２１に記憶される暗号化認証データ３３１、認証方式ID、および公開鍵（Ｋｐ）２１１の数はいずれも任意であり、複数であってもよい。図１４に、複数の暗号化認証データ３３１および認証方式IDが秘匿エリアに格納される例を示す。

【０１５６】

図１４において、ストレージメディア５１１の記憶部５１２の秘匿エリア５２１には、複数の暗号化認証データ（暗号化認証データ３３１－１、暗号化認証データ３３１－２、・・・）と、複数の認証方式ID（認証方式ID３３２－１、認証方式ID３３２－２、・・・）と、１つの公開鍵２１１が格納されている。また、秘匿エリア５２１において、暗号化認証データと認証方式IDは、互いに関連付けられており、

【０１５７】

このようにすることにより、ストレージメディア５１１は、登録されている暗号化認証データを、認証方式IDによって、登録時に使用された認証ユニットの認証方式毎に識別することができる。これにより、ストレージメディア５１１は、認証ユニットから暗号化認証データを要求されたときに、その認証ユニットの認証方式IDと関連付けられた暗号化認証データを供給することができる。つまり、認証ユニットに対して正当な形式の暗号化認証データを供給することができる。

【０１５８】

なお、このように暗号化認証データを複数登録することができるようにすることにより

、複数のユーザを正当なユーザとして登録することができる。つまり、秘匿エリア５２１に複数記憶されている暗号化認証データが互いに異なるユーザのものであってもよい。

【０１５９】

なお、図１４においては、公開鍵２１１が全認証ユニットにおいて共通である場合について説明したが、例えば認証方式毎に公開鍵２１１が異なるようにしてもよい。つまり、秘匿エリア５２１には、複数の公開鍵が保存されるようにしてもよい。なお、この場合、認証方式IDにその認証方式IDに対応する公開鍵２１１が暗号化認証データのように関連付けられるようにしてもよい。

【０１６０】

図１５を参照して、以上のようなシステムの具体的な構成例を説明する。

【０１６１】

図１５Ａの例の場合、認証ユニット１０１とリーダライタ１２１は、パーソナルコンピュータ６０１の周辺機器である認証デバイス６０２として構成され、パーソナルコンピュータより制御可能に接続されている。

【０１６２】

この場合、例えば、ストレージメディア１１１がリーダライタ１２１と、物理的に接続されたり近接されたりして通信可能な状態にされると、リーダライタ１２１は、そのストレージメディア１１１を検出し、パーソナルコンピュータ６０１で実行される制御ソフトウェアに通知する。制御ソフトウェアは、例えばディスプレイに案内文や画像を表示させてユーザに指紋パターンの入力を促すとともに、認証ユニット１０１を制御し、ユーザの指紋パターンを検出するように動作させる。認証ユニット１０１は、上述したようにストレージメディア１１１と通信を行い、ロックの解除、または認証データの登録に関する処理を行う。ロックが解除された場合、パーソナルコンピュータ６０１は、リーダライタ１２１を介してストレージメディア１１１にアクセスすることができる。

【０１６３】

なお、認証ユニット１０１とリーダライタ１２１は、それぞれ、パーソナルコンピュータ６０１に内蔵されるようにしても良い。パーソナルコンピュータ６０１は、一般的な情報処理装置を示すものであり、認証デバイス６０２と上述したように通信可能であればどのような装置であってもよい。

【０１６４】

この場合、ストレージメディア１１１は、認証ユニット１０１を有していないので、容易に小型化することができ、コストや消費電力を低減させることができるとともに、携帯性を向上させることができる。また、例えば、パーソナルコンピュータ６０１および認証デバイス６０２が、例えば、自動販売機や現金自動預入支払機（ATM(Automatic Teller Machine)）のような各所に設置された設備である場合、ユーザは、このストレージメディア１１１を携帯するだけで、どの認証デバイス６０２も利用することができる。さらに、ストレージメディア１１１は認証方式によらず利用可能であるので、多様なシステムに応用することができるとともに、システムに新たな認証技術を導入することも容易になり、容易に安全性を向上させることができる。

【０１６５】

また、図１５Ｂに示されるように、リーダライタ１２１と認証ユニット１０１は、互いに別体として構成されるようにしてもよい。図１５Ｂの例の場合、リーダライタ１２１は、パーソナルコンピュータ６０１に内蔵されている。認証ユニット１０１は、ストレージメディア１１１とは別体の携帯用デバイスとして構成される。ユーザは、ストレージメディア１１１と認証ユニット１０１の２つのデバイスを携帯し、使用時には、ストレージメディア１１１をリーダライタ１２１と通信可能な状態にする。そして、認証データ登録時やロック解除のときのみ、ユーザは、認証ユニット１０１をストレージメディア１１１と通信可能な状態にし、上述したような処理を実行させる。

【０１６６】

なお、リーダライタ１２１を図１５Ａの認証デバイス６０２のように、パーソナルコン

ピュータ６０１とは別体の、パーソナルコンピュータ６０１に接続される周辺機器として構成されるようにしてもよい。また、ストレージメディア１１１がパーソナルコンピュータ６０１に内蔵されるようにしてもよい。

【０１６７】

この場合、ユーザは、必要なときのみ認証ユニット１０１を使用し、必要でないときは、ストレージメディア１１１と認証ユニット１０１を通信不可能な状態にすることができるので、第３者への情報漏洩の危険性を抑制することができる。また、例えば、ストレージメディア１１１が特定の認証ユニット１０１に対してのみ通信可能とすることにより、正当なユーザが正当な認証ユニット１０１を用いないとストレージメディア１１１のロックを解除することができないようにすることができる。つまり、ユーザは、認証ユニット１０１をストレージメディア１１１のハードウェアキーのように使用することができる。

【０１６８】

また、図１５Ｃに示されるように、ストレージメディア１１１を、図３の制御部３０１とデータバスインタフェース部３０２を有する制御アダプタ６１１と、記憶部１１２を有するストレージメディア６１２の２つのデバイスとして構成されるようにしてもよい。

【０１６９】

この場合、ストレージメディア６１２は、従来のロック機能を有さない記憶媒体と同等である。制御アダプタ６１１は、ストレージメディア６１２のインタフェースとして動作し、外部からのストレージメディア６１２へのアクセスを制限する。つまり、制御アダプタ６１１は、従来のロック機能を有さない記憶媒体に、上述したようなロックアンロック機能（アクセス制限機能）を付与するデバイスである。

【０１７０】

制御アダプタ６１１とストレージメディア６１２が通信可能な状態にあるとき、ストレージメディア１１１と同等となる。つまり、図１５Ｃの構成は図１５Ａの構成と同等である。

【０１７１】

この場合、記憶部１１２が含まれない分、制御アダプタ６１１の方がストレージメディア１１１より製造コストを低減させることが出来る。また、従来のロック機能を有さない記憶媒体を利用することができるので、ユーザは、所有する資産を有効に活用することができる。

【０１７２】

認証ユニット１０１とストレージメディア１１１を別体とすることにより、認証ユニット１０１とストレージメディア１１１は、通信可能であれば、互いの物理的距離は任意となるのでより多様なシステムに応用することができる。例えば、図１５Ｄに示されるように、ネットワーク６２０を介して接続されるようにすることもできる。

【０１７３】

図１５Ｄの例の場合、例えばインターネットやLAN等に代表される任意のネットワーク６２０を介してパーソナルコンピュータ６２１およびパーソナルコンピュータ６２２が互いに通信可能に接続されている。パーソナルコンピュータ６２１およびパーソナルコンピュータ６２２は、一般的な情報処理装置を示しており、どのような装置であってもよい。

【０１７４】

パーソナルコンピュータ６２１には、認証ユニット１０１が通信可能に接続され、パーソナルコンピュータ６２２には、リーダライタ１２１を介してストレージメディア１１１が通信可能に接続される。すなわち、認証ユニット１０１とストレージメディア１１１は、パーソナルコンピュータ６２１、ネットワーク６２０、パーソナルコンピュータ６２２およびリーダライタ１２１を介して接続される。

【０１７５】

このような場合であっても、認証ユニット１０１は、ストレージメディア１１１と通信可能に接続されているので、図１５Ａの場合と同様の通信により、ストレージメディア１１１のロックやアンロックを行うことができる。例えば、ユーザは、自宅に設置されるパ

ーソナルコンピュータ６２２のリーダライタ１２１とストレージメディア１１１を通信可能な状態にしておき、外出先のパーソナルコンピュータ６２１に接続されている認証ユニット１０１を用いて、外出先から自宅のストレージメディア１１１のロックを解除し、アクセスを許可することができる。このような場合、ユーザは、認証ユニット１０１およびストレージメディア１１１のいずれも携帯しなくても、任意の場所に設けられた、ストレージメディア１１１と通信可能に設置された認証ユニット１０１を用いてストレージメディア１１１にアクセスすることができる。

【０１７６】

以上のように、認証ユニットと記憶媒体であるストレージメディアを別体とすることにより、安全性および利便性をより向上させることができるだけでなく、多用なシステムに適用することができる。

【０１７７】

なお、以上においては、ユーザが認証ユニット１０１を用いてストレージメディア１１１に認証データを登録するように説明したが、これに限らず、認証データは、ストレージメディア１１１に製造時に記憶させるようにしてもよい。例えばストレージメディア内に暗号化認証データを記憶するROMを設けようにし、更新や消去を不可能とするようにしてもよい。この場合、ユーザや用途が限定されるが、データの改ざんを抑制することができ安全性をより向上させることができる。

【０１７８】

また、ストレージメディア１１１へのアクセスの許可等の際に、複数の認証方式により、ユーザ認証を複数回行う必要があるようにしてもよい。この場合、ユーザは、複数の認証方式により、ユーザ認証を複数回行い、全ての認証方式において認証されない限りストレージメディア１１１のロックを解除することができない。このように複数の認証方式によりロックを多重化することにより、ストレージメディア１１１のデータの漏洩に対する安全性をより向上させることができる。

【０１７９】

また、例えば、上述したようにストレージメディア１１１に所定のパスワードを記憶するROMを設け、ユーザが指紋パターン等の認証データをストレージメディア１１１に登録する際に、ROMに記憶されているパスワードを用いた認証を行う必要があるようにしてもよい。このようにすることにより、第３者が勝手に認証データを登録してしまうことを抑制することができ、ストレージメディア１１１のデータの漏洩に対する安全性をより向上させることができる。

【０１８０】

なお、複数のユーザの認証データを登録することができるようにする場合、ストレージメディア１１１は、その認証データ毎に、記憶部１１２のアクセスを許可する領域や、実行権限を割り当てるようにしてもよい。すなわち、認証に用いられる認証データによって、記憶部１１２のアクセス可能な領域や実行可能な処理を区別または制限することができるようにしてもよい。

【０１８１】

例えば、工場出荷時等からROMに記憶されている認証データには、無制限の管理者権限を付与し、その後登録される認証データには、更新可能なデータや領域が制限されるユーザ権限を付与するようにしてもよい。

【０１８２】

また、例えば、認証データを新たに登録する際にそのユーザが以前登録した認証データでロックを解除してから登録を行うことにより、ストレージメディア１１１が、認証データをユーザ毎に管理することができるようにしてもよい。その場合、記憶部１１２のアクセス可能な領域や実行権限を、ユーザ毎に区別または制限することもできる。

【０１８３】

なお、以上においては、認証データを暗号化するように説明したが、これに限らず、認証データが平文のまま、認証ユニット１０１とストレージメディア１１１との間で授受さ

れるようにしてもよい。その場合、暗号化部２０２および復号部２２２、並びに、図４のステップＳ２の処理および図９のステップＳ４５の処理を省略することができるので、認証ユニット１０１の回路規模の縮小や処理の負荷の低減を実現することができる。ただし、この場合、情報漏洩に対する安全性は低下する。

【０１８４】

同様に、認証ユニット１０１が認証結果および乱数を秘密鍵２３１で暗号化し、ストレージメディア１１１がその暗号化データを公開鍵２１１で復号するように説明したが、認証結果や乱数が平文のまま授受されるようにしてもよい。その場合、鍵保持部２０４、暗号化部２２４、および復号部３１６、並びに、図９のステップＳ４７の処理およびステップＳ６５の処理等を省略することができるので、認証ユニット１０１やストレージメディア１１１の回路規模の縮小や処理の負荷の低減を実現することができる。ただし、この場合、情報漏洩に対する安全性は低下する。

【０１８５】

上述した一連の処理は、ハードウェアにより実行させることもできるし、ソフトウェアにより実行させることもできる。この場合、例えば、図１６に示されるようなパーソナルコンピュータとして構成されるようにしてもよい。

【０１８６】

図１６において、パーソナルコンピュータ７００のCPU７０１は、ROM（Read Only Memory）７０２に記憶されているプログラム、または記憶部７１３からRAM（Random Access Memory）７０３にロードされたプログラムに従って各種の処理を実行する。RAM７０３にはまた、CPU７０１が各種の処理を実行する上において必要なデータなども適宜記憶される。

【０１８７】

CPU７０１、ROM７０２、およびRAM７０３は、バス７０４を介して相互に接続されている。このバス７０４にはまた、入出力インタフェース７１０も接続されている。

【０１８８】

入出力インタフェース７１０には、キーボード、マウスなどよりなる入力部７１１、CRT（Cathode Ray Tube）、LCD（Liquid Crystal Display）などよりなるディスプレイ、並びにスピーカなどよりなる出力部７１２、ハードディスクなどより構成される記憶部７１３、モデムなどより構成される通信部７１４が接続されている。通信部７１４は、インターネットを含むネットワークを介しての通信処理を行う。

【０１８９】

入出力インタフェース７１０にはまた、必要に応じてドライブ７１５が接続され、磁気ディスク、光ディスク、光磁気ディスク、或いは半導体メモリなどのリムーバブルメディア７２１が適宜装着され、それらから読み出されたコンピュータプログラムが、必要に応じて記憶部７１３にインストールされる。

【０１９０】

上述した一連の処理をソフトウェアにより実行させる場合には、そのソフトウェアを構成するプログラムが、ネットワークや記録媒体からインストールされる。

【０１９１】

この記録媒体は、例えば、図１６に示されるように、装置本体とは別に、ユーザにプログラムを配信するために配布される、プログラムが記録されている磁気ディスク（フレキシブルディスクを含む）、光ディスク（CD-ROM(Compact Disk-Read Only Memory),DVD(Digital Versatile Disk)を含む）、光磁気ディスク（ＭＤ（Mini-Disk）（登録商標）を含む）、もしくは半導体メモリなどよりなるリムーバブルメディア７２１により構成されるだけでなく、装置本体に予め組み込まれた状態でユーザに配信される、プログラムが記録されているROM７０２や、記憶部７１３に含まれるハードディスクなどで構成される。

【０１９２】

なお、本明細書において、記録媒体に記録されるプログラムを記述するステップは、記載された順序に沿って時系列的に行われる処理はもちろん、必ずしも時系列的に処理され

なくとも、並列的あるいは個別に実行される処理をも含むものである。

【０１９３】

また、本明細書において、システムとは、複数のデバイス（装置）により構成される装置全体を表すものである。

【０１９４】

なお、以上において、１つの装置として説明した構成を分割し、複数の装置として構成するようにしてもよい。逆に、以上において複数の装置として説明した構成をまとめて１つの装置として構成されるようにしてもよい。また、各装置の構成に上述した以外の構成を付加するようにしてももちろんよい。さらに、システム全体としての構成や動作が実質的に同じであれば、ある装置の構成の一部を他の装置の構成に含めるようにしてもよい。つまり、本発明の実施の形態は、上述した実施の形態に限定されるものではなく、本発明の要旨を逸脱しない範囲において種々の変更が可能である。

【産業上の利用可能性】

【０１９５】

本発明は、ストレージメディアの入出力を制御する情報処理装置に適用することが可能である。

【図面の簡単な説明】

【０１９６】

【図１】本発明を適用した記憶媒体のデータの入出力を制御する制御システムシステムの構成例を示すブロック図である。

【図２】図１の認証ユニット１０１の内部の構成例を示すブロック図である。

【図３】図１のストレージメディア１１１の内部の構成例を示すブロック図である。

【図４】ロック処理の流れの例を説明するフローチャートである。

【図５】認証データ取得の様子の例を説明する図である。

【図６】認証データの暗号化の様子の例を説明する図である。

【図７】公開鍵と秘密鍵と認証方式IDの例を説明する図である。

【図８】ロックコマンドの供給の様子の例を説明する図である。

【図９】ロック解除処理の流れの例を説明するフローチャートである。

【図１０】認証データ取得の様子の例を説明する図である。

【図１１】乱数の供給の様子の例を説明する図である。

【図１２】ロック処理の流れの例を説明するフローチャートである。

【図１３】アンロック処理の流れの例を説明するフローチャートである。

【図１４】秘匿エリアの様子の例を説明する図である。

【図１５】システムの具体的な構成例を説明する図である。

【図１６】本発明を適用したパーソナルコンピュータの構成例を示すブロック図である。

【符号の説明】

【０１９７】

１０１乃至１０３　認証ユニット，　１１１　ストレージメディア，　１１２　記憶部，　１２１　リーダライタ，　２０１　認証データ受付部２０１，　２０２　暗号化部，　２０３　認証方式ID提供部，　２０４　鍵保持部部，　２０５　入出力制御部，　２０６　ストレージメディアインタフェース部，　２１１　公開鍵，　２２１　ロック解除コマンド供給部，　２２２　復号部，　２２３　比較部，　２２４　暗号化部，　２３１　秘密鍵，　３０１　制御部，　３０２　データバスインタフェース部，　３１１　認証ユニットインタフェース部，　３１２　入出力制御部，　３１３　ロック制御部，　３１４　エラー処理部，　３１５　乱数発生部，　３１６　復号部，　３１７　一致判定部，　３２１　秘匿エリア，　３３１　暗号化認証データ，　３３２　認証方式ID，　５１１　ストレージメディア，　５１２　記憶部，　５２１　秘匿エリア，　６０１　パーソナルコンピュータ，　６０２　認証デバイス，　６１１　制御アダプタ，　６１２　ストレージメディア，　６２０　ネットワーク，　６２１および６２２　パーソナルコンピュータ

【図１】

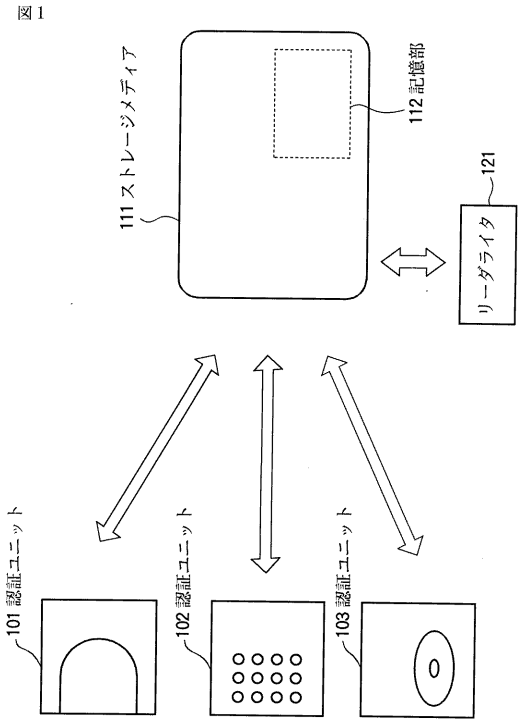


図1
111 ストレージメディア
112 記憶部
121
リーダライタ
101 認証ユニット
102 認証ユニット
103 認証ユニット

【図２】

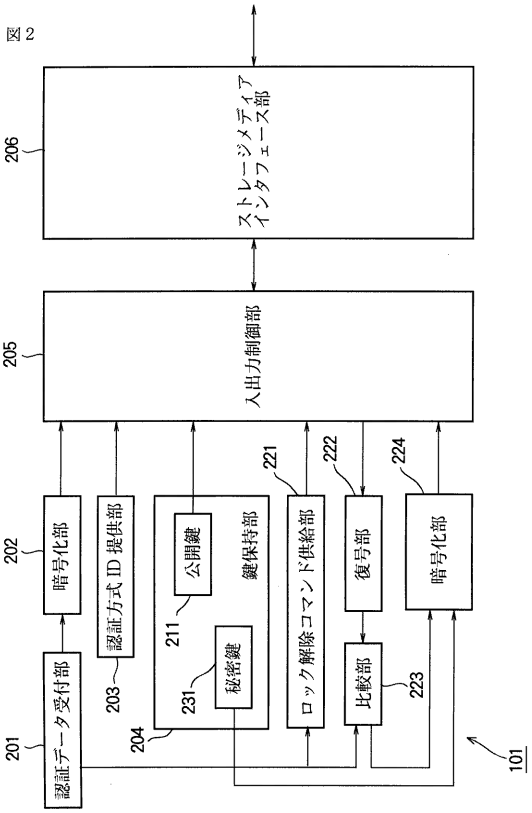


図2
206
ストレージメディア
インタフェース部
205
入出力制御部
202
暗号化部
認証方式 ID 提供部
203
認証データ受付部
201
204
211
公開鍵
231
秘密鍵
鍵保持部
221
ロック解除コマンド供給部
222
復号部
224
暗号化部
223
比較部
101

【図３】

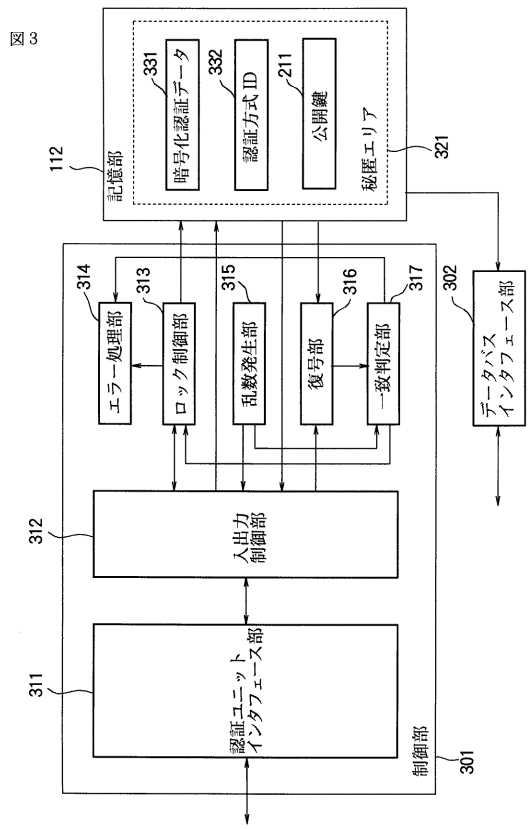


図3
112
記憶部
331
暗号化認証データ
332
認証方式 ID
211
公開鍵
秘匿エリア
321
314
エラー処理部
313
ロック制御部
315
乱数発生部
316
復号部
317
一致判定部
302
データバス
インタフェース部
312
入出力
制御部
311
認証ユニット
インタフェース部
制御部
301

【図４】

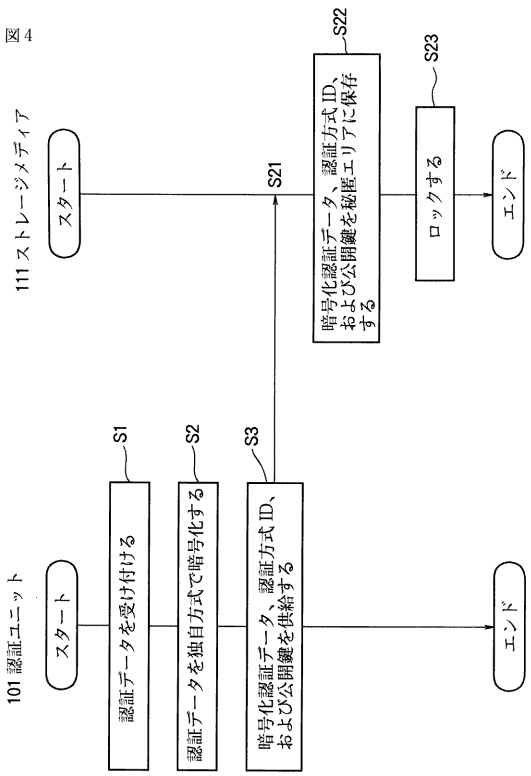
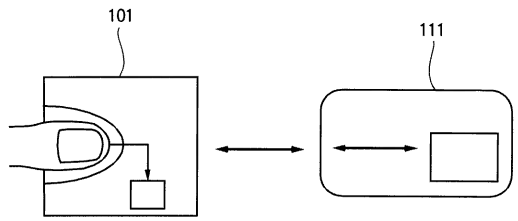


図4
111 ストレージメディア
スタート
S21
S22
暗号化認証データ、認証方式 ID、
および公開鍵を秘匿エリアに保存
する
S23
ロックする
エンド
101 認証ユニット
スタート
S1
認証データを受け付ける
S2
認証データを独自方式で暗号化する
S3
暗号化認証データ、認証方式 ID、
および公開鍵を供給する
エンド

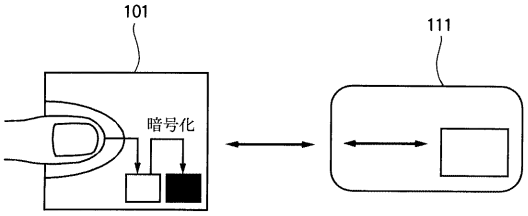
【図５】

図５



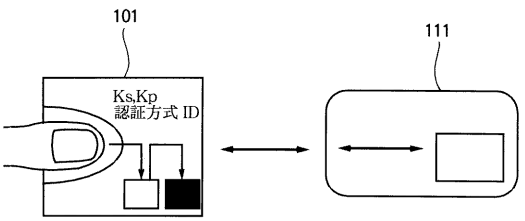
【図６】

図６



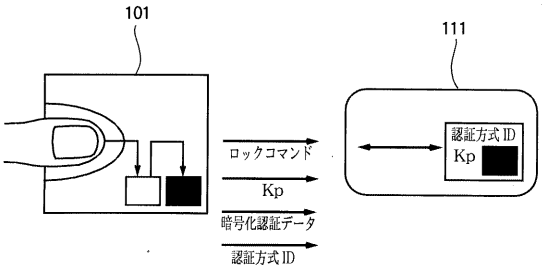
【図７】

図７



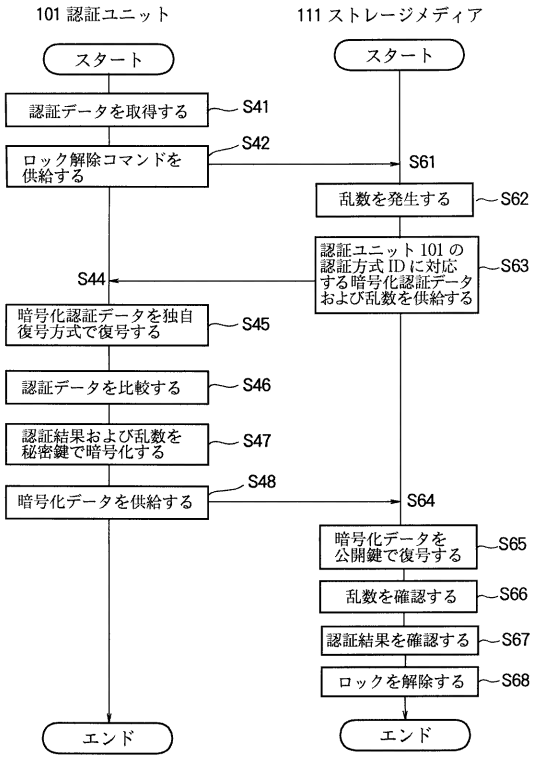
【図８】

図８



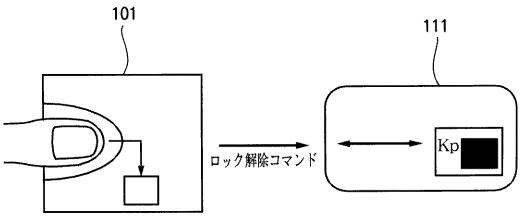
【図９】

図９



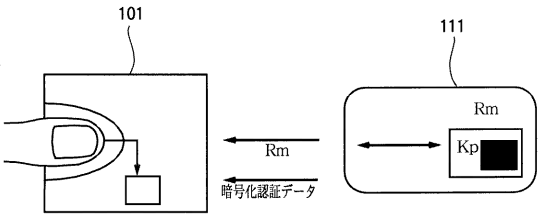
【図１０】

図１０

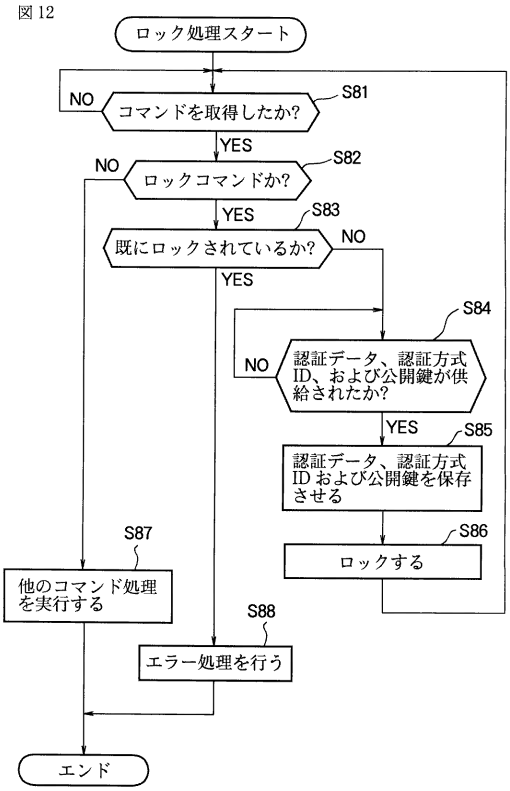


【図１１】

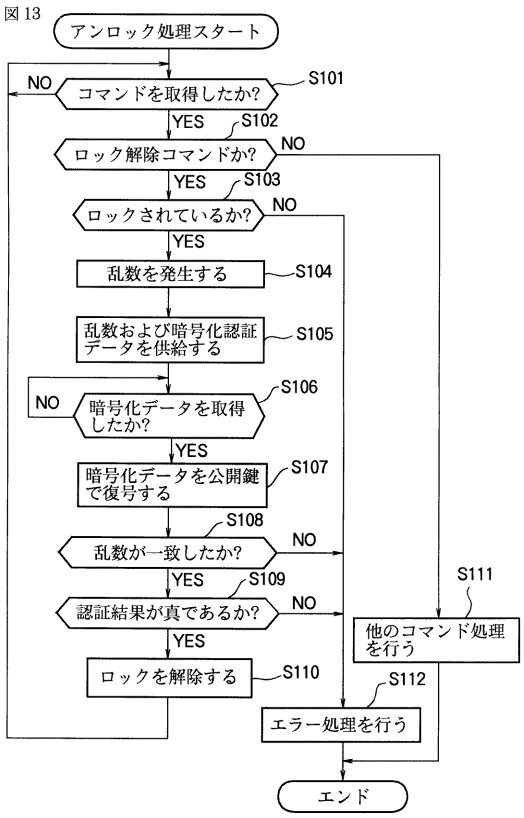
図１１



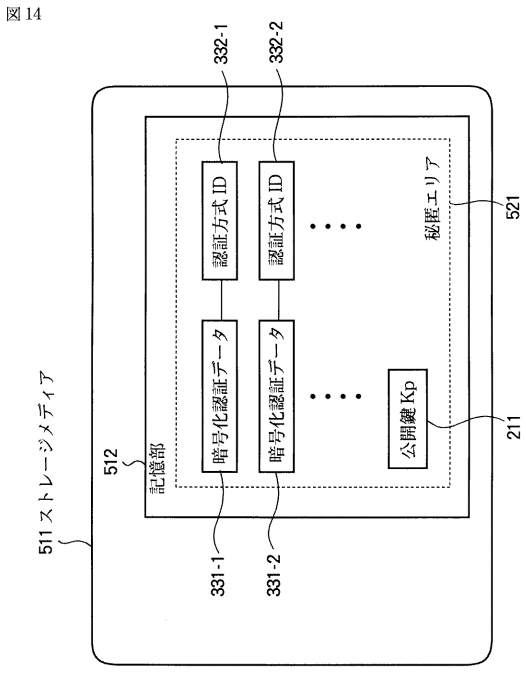
【図１２】



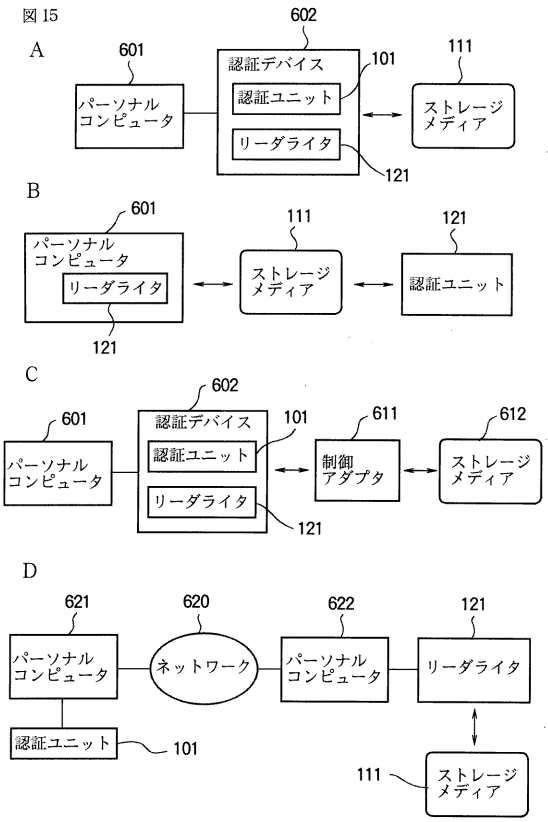
【図１３】



【図１４】

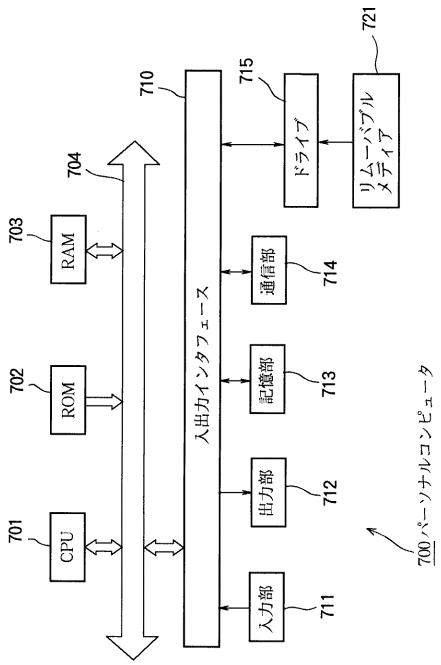


【図１５】



【図１６】

図16


700 パーソナルコンピュータ
701 CPU
702 ROM
703 RAM
704
710 入出力インタフェース
711 入力部
712 出力部
713 記憶部
714 通信部
715 ドライブ
721 リムーバブルメディア

フロントページの続き

(56)参考文献 特開２００５－５０１４８（ＪＰ，Ａ）
特開２００６－３５１０１５（ＪＰ，Ａ）
特開２００５－１６６０４９（ＪＰ，Ａ）
特開昭６１－３２５４（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／２４
Ｇ０６Ｆ　３／０６
Ｈ０４Ｌ　９／３２