

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第6811285号
(P6811285)

(45) 発行日 令和3年1月13日 (2021.1.13)

(24) 登録日 令和2年12月16日 (2020.12.16)

(51) Int. Cl.

F I

G06F 21/60 (2013.01)

H04L 9/10 (2006.01)

H04L 9/32 (2006.01)

G06F 21/62 (2013.01)

G06F 21/32 (2013.01)

G06F 21/60 320

H04L 9/00 621A

H04L 9/00 673D

G06F 21/62

G06F 21/32

請求項の数 8 (全 13 頁)

(21) 出願番号 特願2019-105471 (P2019-105471)
 (22) 出願日 令和1年6月5日 (2019.6.5)
 (65) 公開番号 特開2020-98560 (P2020-98560A)
 (43) 公開日 令和2年6月25日 (2020.6.25)
 審査請求日 令和1年6月5日 (2019.6.5)
 (31) 優先権主張番号 107145630
 (32) 優先日 平成30年12月18日 (2018.12.18)
 (33) 優先権主張国・地域又は機関 台湾 (TW)

(73) 特許権者 509092878
 ウォルトン アドバンスド エンジニアリ
 ング インク
 WALTON ADVANCED ENG
 INEERING INC.
 台湾 806 カオシュンシティ カオシ
 ユン エクスポート プロセッシング ゾー
 ン (ケー・イー・ピー・ゼット) ノー
 スファーストロード 18
 (74) 代理人 110000419
 特許業務法人太田特許事務所
 (72) 発明者 ユ ホンーチ
 台湾 高雄市 ノースファーストロード
 カオシュン エクスポート プロセッシング
 ゾーン

最終頁に続く

(54) 【発明の名称】 データストレージデバイス

(57) 【特許請求の範囲】

【請求項 1】

専用ストレージモジュールと暗号モジュールと取付モジュールを備えるデータストレ
 ジデバイスであって、

前記専用ストレージモジュールは、情報端子プラグ、ロック孔、コントロール素子、ス
 トレージ素子及び基板を備えて、前記基板により前記専用ストレージモジュールの各素子
 に電氣的に接続され、

前記暗号モジュールは、情報端子ジャック、外部素子、暗号化素子、電源素子及び回路
 基板を備えて、前記回路基板により、前記暗号モジュールの各素子に電氣的に接続され、

前記取付モジュールは、ロック素子、動力素子及び指紋認証スイッチを備えて、前記暗
 号モジュールの前記電源素子により前記動力素子に電気エネルギーが提供されて、前記ロ
 ック素子を駆動して位置を移動させ、

前記電源素子は、外付け電源方式により作動電力を取得し、前記専用ストレージモジュ
 ール、前記暗号モジュール、及び前記取付モジュールが作動に必要な電力を提供し、

前記指紋認証スイッチにより前記電源素子が ON になり、前記情報端子プラグが前記情
 報端子ジャックに挿入されると、前記ロック素子が前記ロック孔を固定し、前記暗号モジ
 ュールは、前記情報端子ジャックを介して前記専用ストレージモジュールに電氣的に接続
 され、前記暗号モジュールの前記外部素子は、外部デバイスに電氣的に接続されて機密デ
 ータを取得し、前記暗号モジュールが前記機密データを暗号化して、さらに、暗号化され
 た前記機密データを前記ストレージ素子内に保存することを特徴とするデータストレージ

10

20

デバイス。

【請求項 2】

前記ロック孔の受電箇所は、前記ロック素子を含む電力供給箇所に電氣的に接続されて、前記専用ストレージモジュールが必要とする電気エネルギーを提供することを特徴とする請求項 1 に記載のデータストレージデバイス。

【請求項 3】

前記暗号モジュールは表示ランプを備えることを特徴とする請求項 1 に記載のデータストレージデバイス。

【請求項 4】

前記暗号モジュールが暗号化するキーは前記指紋認証スイッチを介することが可能であることを特徴とする請求項 1 に記載のデータストレージデバイス。

10

【請求項 5】

前記暗号モジュールに電氣的に接続される一般のストレージデバイスをさらに備え、前記一般のストレージデバイスが前記暗号モジュールに電氣的に接続することにより、二番目のデータセキュリティ機能を提供する、請求項 1 に記載のデータストレージデバイス。

【請求項 6】

上部カバー、下部カバー、固定モジュールを備えて、前記固定モジュールは、少なくとも一個の脚部、ベース、スプリング及び位置固定柱を備えることを特徴とする請求項 1 に記載のデータストレージデバイス。

【請求項 7】

20

前記下部カバーは放熱フィンを備えることを特徴とする請求項 6 に記載のデータストレージデバイス。

【請求項 8】

前記固定モジュールは解錠パーツを備えることを特徴とする請求項 6 に記載のデータストレージデバイス。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、暗号データ保護のデバイスに関し、特に、機密データを移動保存することが可能な実体モジュールであり、外部素子を介して外部デバイスに電氣的に接続して機密データを保存し、暗号化モジュールを介して、暗号データを保存して移動させることができる専用ストレージモジュールに関する。

30

【背景技術】

【0002】

現在プライベートネットワークにおいて個人向けのクラウドストレージを使用する状況は普及の傾向にある。同時に、プライベートのストレージデバイスは、集中管理化される傾向があり、プライベートネットワークが独立したネットワークストレージデバイスにアクセスして、データを集中管理したり、バックアップを行ったりする。しかしながら、それに伴い、個人のデータに関するプライバシー保護の問題も顕著になっている。

【0003】

40

以下に、保存システムに関する特許を開示する。

【0004】

J P 2002 - 236380では、データ保管システムを開示している。前記保管システムは、ネットワーク上に保存されているユーザー端末デバイス内のデータを、前記ユーザーまたはその他のユーザーの利用に提供する時、複数の端末デバイス上でデータが利用できるようにするものである。ユーザー端末の種類にかかわらず、コンピュータネットワークNTを介して、ユーザー端末とサービス提供者のデータ保管部にアクセスする統合接続インターフェースサーバー及びデータサーバー内に保存されたデータファイルにデータ形式変換処理を行なうデータ形式変換コンピュータからなる本システムを備えることで、ユーザーがデータファイルを使用保存する時、異なる種類のユーザー端末が本システム

50

内のデータファイルを利用保存する場合、その必要に応じて、データ形式変換コンピュータ内において ユーザー端末に適合する種類のデータファイルに変換して、前記変換後のデータをユーザー端末に送る。

【0005】

TW 526643では、データ読み取り制御管理システム及びその方法を開示する。まず、秘密シェア方式により、メインキーを n 個のサブキーに分けて n 個のサブキー保管者に渡す。メインキー復元プログラムは、サブキー保管者とシェアする秘密を利用して、 m ($1 < m < n$) 個のサブキーを獲得し、さらに、 (m, n) に適合する条件でふるいにかけてメインキーを復元し、システムがこのメインキーにより保護されたデータに対して解錠して読み取る。このため、 m 個のキーの組合せによりメインキーを復元させて、システム中のデータを変更したり読み取ったりする必要がある。このように、システム中のデータの機密性と安全性を保護する効果を有すると同時に、サブキーを保管する者が離職や転勤した時、サブキーを交換しさえすれば、メインキーを復元でき、メインキーを交換する必要がなく、パスワードを交換することによる機密データの読み取りに対して影響を及ぼすことがない。

10

【0006】

EP 12217889.7は、定義された信任可能な環境において、あるサービスに対して安全に読み取ることができる方法を開示する。少なくとも一個のネットワークアセンブリが、前記定義された信任可能な環境において、パスワードを前記ネットワークアセンブリに保存する。ユーザーデバイスが前記信任可能な環境において導入され、さらに、前記ユーザーデバイスが、前記ネットワークアセンブリに連絡し且つ前記ネットワークアセンブリ中の前記パスワードを読み取って保存する。前記ユーザーデバイスは、前記パスワードを前記サービスに伝達し、且つ、前記サービス中に保存されたパスワードが、前記ユーザーデバイスから前記サービスに伝達された前記パスワードと合致すれば、前記ユーザーデバイスが前記サービスを使用開始することが可能となる。

20

【0007】

しかしながら、データのプライバシー面において、やはり不安材料が残る。したがって、機密データ保護の安全性を高めるために、従来の欠点を改善するデータストレージデバイスを提供する必要がある。

【先行技術文献】

30

【特許文献】

【0008】

【特許文献1】特開2004-080245号公報

【発明の概要】

【発明が解決しようとする課題】

【0009】

したがって、本発明は、従来の欠点を改善するデータストレージデバイスを提供することを課題とする。

【課題を解決するための手段】

【0010】

40

上記課題を解決するために、本発明は、データを暗号化し、且つ、分離式の専用ストレージモジュール方式により安全性を高めるデータストレージデバイスを提供する。

【0011】

このため、本発明のデータストレージデバイスは、多種のセキュリティ措置を組み合わせることで、安全性を高めることを特徴とする。

【0012】

さらに、本発明データストレージデバイスは、指紋認証方式を採用して;動電源を起動させる方式により、部外者が接触機密データに接触するリスクを回避することを特徴とする。

【0013】

50

またさらに、本発明のデータストレージデバイスは、専属の情報端子プラグと情報端子ジャックの組合せにより、不必要な電氣的接続を簡単に回避することを特徴とする。

【 0 0 1 4 】

またさらに、本発明のデータストレージデバイスは、ロック素子により専用モジュール電力を提供して、安易な専用モジュールへの電力導通を回避することを特徴とする。

【 0 0 1 5 】

またさらに、本発明のデータストレージデバイスは、外部素子と外部デバイスの電氣的接続により、本発明とのシンプルでスピーディーなデータ交換が可能であることを特徴とする。

10

【 0 0 1 6 】

またさらに、本発明のデータストレージデバイスは、暗号化素子に搭配指紋認証スイッチを組み合わせてデータの暗号化を図ると同時に、専用ストレージモジュールに移すことを特徴とする。

【 0 0 1 7 】

またさらに、本発明のデータストレージデバイスは、専用ストレージモジュールのみを有する時、対応する指紋がない場合に機密データを取得することができないことを特徴とする。

【 0 0 1 8 】

またさらに、本発明のデータストレージデバイスは、放熱フィンを提供して、暗号化する時の安定度を高めることを特徴とする。

20

【 0 0 1 9 】

上記目的を達成するために、本発明が使用する主な技術手段は、以下の技術方法を採用して実現させる。本発明は、データストレージデバイスであり、専用ストレージモジュール、暗号モジュール、取付モジュールを備える。前記専用ストレージモジュールは、情報端子プラグ、ロック孔、コントロール素子、ストレージ素子及び基板を備えて、前記基板により前記専用ストレージモジュールの各素子に電氣的に接続される。前記暗号モジュールは、情報端子ジャック、外部素子、暗号化素子、電源素子及び回路基板を備えて、前記回路基板により、前記暗号モジュールの各素子に電氣的に接続される。前記取付モジュールは、ロック素子、動力素子及び指紋認証スイッチを備えて、前記電源素子により前記動力素子に電気エネルギーが提供されて、前記ロック素子を駆動して位置を移動させる。その特徴は、以下のとおりである。前記指紋認証スイッチにより前記電源素子がONになり、前記情報端子プラグが前記情報端子ジャックに挿入されると、前記ロック素子が前記ロック孔を固定する。前記暗号モジュールは、前記情報端子ジャックを介して前記専用ストレージモジュールに電氣的に接続される。前記暗号モジュールの前記外部素子は、外部デバイスに電氣的に接続されて機密データを取得する。前記暗号モジュールが前記機密データを暗号化して、さらに、暗号化された前記機密データを前記ストレージ素子内に保存する。

30

【 0 0 2 0 】

本発明の目的及びその技術的な課題を解決する方法は、以下の技術内容を採用して実現させる。

40

【 0 0 2 1 】

前記デバイスにおいて、前記ロック孔の受電箇所は、前記ロック素子を含む電力供給箇所に電氣的に接続されて、前記専用ストレージモジュールが必要とする電気エネルギーを提供する。

【 0 0 2 2 】

前記デバイスにおいて、前記暗号モジュールは表示ランプを備える。

【 0 0 2 3 】

前記デバイスにおいて、前記暗号モジュールが暗号化するキーは前記指紋認証スイッチを介することが可能である。

50

【 0 0 2 4 】

前記デバイスにおいて、一般のストレージデバイスを備えることが可能で、前記一般デバイスは前記暗号モジュールに電氣的に接続される。

【 0 0 2 5 】

前記デバイスにおいて、上部カバー、下部カバー、固定モジュールを備えて、前記固定モジュールは、少なくとも一個の脚部、ベース、スプリング及び位置固定柱を備える。

【 0 0 2 6 】

前記デバイスにおいて、前記下部カバーは放熱フィンを備える。

【 0 0 2 7 】

前記デバイスにおいて、前記固定モジュールは解錠パーツを備える。

10

【 0 0 2 8 】

従来の技術と比較して、本発明は、以下の特徴を有する。(1) 専用の情報端子プラグと情報端子ジャックの組み合わせにより、簡単に不要な電氣的接続を回避する。(2) 指紋認証方式による電源起動方式により、部外者が機密データに接触するリスクを回避する。(3) データの暗号化と同時に、分離式の専用ストレージモジュール方式により、安全性を高める。

【 発明の効果 】

【 0 0 2 9 】

本発明のデータストレージデバイスは、専用の情報端子プラグと情報端子ジャックの組み合わせにより、簡単に不要な電氣的接続を回避する。指紋認証方式による電源起動方式により、部外者が機密データに接触するリスクも回避する。さらに、データの暗号化と同時に、分離式の専用ストレージモジュール方式により、安全性を高める。

20

【 図面の簡単な説明 】

【 0 0 3 0 】

【 図 1 a 】 本発明の好適な実施形態における専用ストレージモジュールの側面図である。

【 図 1 b 】 本発明の好適な実施形態における全体的外観の側面図である。

【 図 2 a 】 本発明の好適な実施形態における分解図である。

【 図 2 b 】 本発明の好適な実施形態における専用ストレージモジュールの使用状態を示した第一図である。

【 図 2 c 】 本発明の好適な実施形態における専用ストレージモジュールの使用状態を示した第二図である。

30

【 図 2 d 】 本発明の好適な実施形態における専用ストレージモジュールの使用状態を示した第三図である。

【 図 2 e 】 本発明の好適な実施形態における専用ストレージモジュールの使用状態を示した第四図である。

【 図 3 a 】 本発明の好適な実施形態における固定モジュールの使用状態を示した第一図である。

【 図 3 b 】 本発明の好適な実施形態における固定モジュールの使用状態を示した第二図である。

【 図 3 c 】 本発明の好適な実施形態における固定モジュールの断面図である。

40

【 図 4 】 本発明の好適な実施形態における固定モジュールの放熱フィンを示した図である。

【 図 5 a 】 本発明の好適な実施形態における固定モジュールの専用ストレージモジュールを示した図である。

【 図 5 b 】 本発明の好適な実施形態における固定モジュールの暗号モジュールを示した図である。

【 図 5 c 】 本発明の好適な実施形態における外部デバイスと外部素子の機密データ交換を示した図である。

【 発明を実施するための形態 】

【 0 0 3 1 】

50

本発明の目的、特徴、効果を明確にするために、以下に本発明の好適な実施形態を例として説明する。

【0032】

まず、図1bを参照しながら説明する。本発明はデータストレージデバイスであり、専用ストレージモジュール10、暗号モジュール20及び取付モジュール30を備える。

【0033】

このうち、図1a及び図5aに示したように、前記専用ストレージモジュール10は、情報端子プラグ11、ロック孔12、コントロール素子13、ストレージ素子14及び基板15を備えて、前記基板15により前記専用ストレージモジュール10の各素子に電氣的に接続される。

10

【0034】

一般に、前記情報端子プラグ11は、特殊定義の実体規格の電氣的接触ポートの形態を呈する(図1aに図示)。その目的は、普及している規格を使用することで発生する設計外の電氣的接触を避けることにある。また、ロック孔12は、前記専用ストレージモジュール10一側に設計され(図1aに図示)、その主な目的は、前記専用ストレージモジュール10を指定の位置に固定して、情報端子プラグ11と情報端子ジャック21間において安定した位置を保持するためである。さらに、コントロール素子13は、複雑なコンピュータプログラムを実行するロジックデバイスである。ストレージ素子14は、不揮発メモリ(Non-volatile memory, NVRAM)で、電流がOFFになった後、保存されたデータが消えないという特性を有し、これにより、関連する設定及び記録データを保存することができる。前記基板15は、通常回路基板(circuit board)で、例えば、基板は、単層または多層回路を有するプリント基板である。また、リードフレーム、回路フィルム(Polyimide)、BT回路板または各種チップ基板でも可能である。前記基板15内部には回路(図示はされない)が形成されて、電氣的伝達インターフェースとなる。

20

【0035】

このうち、図2a及び図5bに示したように、前記暗号モジュール20は、情報端子ジャック21、外部素子22、暗号化素子23、電源素子24及び回路基板25を備え、前記回路基板25により、前記暗号モジュール20の各素子に電氣的に接続される。

【0036】

30

具体的には、前記情報端子ジャック21は、特殊定義の実体規格の電氣的接触端を指し、コンセントの形態を呈する(図2cに示している)。その目的は、普及している規格を使用することによる設計外の電氣的接触を回避するものである。また、外部素子22は、インターネット接続機能を提供するための集合体である。例えば、ネットワークインターフェースコントローラ(network interface controller, NIC)は、デバイスがネットワーク上において通信を行なうことを許すために設計されたハードウェアである。それは無線または有線で、その場所と外部間においてデータの交換を提供するインターフェースである。暗号化素子23は、内部で集成された各タイプの対称と非対称の演算法に対して、自らが極めて高いセキュリティレベルを有し、内部保存されたキーとメッセージデータが不法に読み取られたり、改ざんされたりしないようにするための、セキュリティチップの総称であり、前記暗号モジュール20が暗号化(Encryption)を経て、文字化された情報を読み取りが困難な暗号内容に変更させることで、読み取りにくくする過程であり、復号キーを有する対象のみが、復号の過程を経て、初めて暗号文を正常に読み取れる内容に復元できる。前記電源素子24は、外付け電源方式により、作動電力を取得し、前記専用ストレージモジュール10、前記暗号モジュール20と前記取付モジュール30が作動に必要とする電力を提供する。さらに、回路基板25は、回路基板(circuit board)である。例えば、基板は、単層または多層回路を有するプリント基板である。また、リードフレーム、回路フィルム(Polyimide)、BT回路基板または各種チップ基板でも可能で、前記回路基板25内部には、回路(図示はされない)が形成されて、電氣的伝達インターフェースとなる。

40

50

【 0 0 3 7 】

図 2 a 及び図 2 b を参照しながら説明する。このうち、前記取付モジュール 3 0 は、ロック素子 3 1、動力素子 3 2 及び指紋認証スイッチ 3 3 を備えて、前記電源素子 2 4 により前記動力素子 3 2 に電気エネルギーを提供して前記ロック素子 3 1 を駆動して移動させる。

【 0 0 3 8 】

詳しく言えば、前記ロック素子 3 1 は、前記専用ストレージモジュール 1 0 の一側（図 2 b に図示）に設計されて、主に前記専用ストレージモジュール 1 0 を指定の位置に固定させて、情報端子プラグ 1 1 と情報端子ジャック 2 1 間において位置を安定させる。さらに、前記動力素子 3 2 は、モータ（Electric motor）を有し、電気エネルギーを機械エネルギーに変換して、機械エネルギーを利用して運動エネルギーを発生させて外部パーツを動かすことで、前記専用ストレージモジュール 1 0 の電気設備を駆動させるものである。前記指紋認証スイッチ 3 3 は、指紋認証及び電力スイッチの二重機能を有する素子であり、指紋を読み取り、指紋を押すことにより前記電源素子 2 4 を触発して電源を導通させるかどうかを確認する。

【 0 0 3 9 】

好適には、前記ロック孔 1 2 の受電箇所（図示はされない）と前記 3 1 を含むロック素子の一電気供給箇所（図示はされない）は電氣的に接続されて、前記専用ストレージモジュール 1 0 が必要とする電気エネルギーを提供することにより、前記専用ストレージモジュール 1 0 が自ら電氣的接続する状況を困難にする。

【 0 0 4 0 】

さらに、前記暗号モジュール 2 0 は、表示ランプ 2 6 を備えて、この表示ランプ 2 6 により、本発明との相互作用状況を知ることが可能である。

【 0 0 4 1 】

また、前記暗号化素子 2 3 が暗号化したキーは、前記指紋認証スイッチ 3 3 の定義を通して、前記専用ストレージモジュール 1 0 のみで、対応する指紋がない状況においては、機密データを取得することができない。

【 0 0 4 2 】

さらに、一般のストレージデバイス 5 0 を備えることも可能で、前記一般のストレージデバイス 5 0 は、前記暗号モジュール 2 0 に電氣的に接続することにより、二番目のデータセキュリティ機能を提供することが可能である。

【 0 0 4 3 】

さらに、前記専用ストレージモジュール 1 0 と前記暗号モジュール 2 0 間の使用時の変化を理解するために、まず、図 2 b 及び図 2 c を参照しながら説明する。前記専用ストレージモジュール 1 0 は、前記該暗号モジュール 2 0 の向きに挿入される。前記情報端子プラグ 1 1 と前記情報端子ジャック 2 1 は同時に移動する。次に、前記情報端子プラグ 1 1 と前記情報端子ジャック 2 1 は相互に接触しない（図示はされない）。この時、前記ロック素子 3 1 を触発してロック孔 1 2 を固定し、情報端子プラグ 1 1 と情報端子ジャック 2 1 間において位置を安定させる。前記専用ストレージモジュール 1 0 を離脱させる場合は、図 2 c と図 2 d に示したように、前記ロック素子 3 1 を触発して、ロック孔 1 2 におけるロック状態を解除する。動力素子 3 2 が前記専用ストレージモジュール 1 0 を押し出すことで、情報端子プラグ 1 1 と情報端子ジャック 2 1 を分離させ、さらに、前記専用ストレージモジュール 1 0 を離脱させることができる。

【 0 0 4 4 】

次に、本発明を保護するために、上部カバー 5 1、下部カバー 5 2、固定モジュール 5 3 を追加することも可能である。前記固定モジュール 5 3 は、少なくとも一個の脚部 5 3 1、ベース 5 3 2、スプリング 5 3 3 及び位置固定柱 5 3 4 を備える。

【 0 0 4 5 】

好適には、前記下部カバー 5 2 は、放熱フィン 5 2 1 を備え、前記放熱フィン 5 2 1 は、暗号化素子 2 3 を追加して暗号化する時の安定度を高めることができる。さらに、前記固

定モジュール５３は、解錠パーツ５３５を備え、前記解錠パーツ５３５は、上部カバー５１と下部カバー５２をそれぞれ取り外せるようにすることで、一般のストレージデバイス５０に変更しやすいようにしている。

【００４６】

このうち、前記上部カバー５１と下部カバー５２は、本発明を保護する効果を有する。さらに、図２ａを参照しながら説明する。前記固定モジュール５３は、それぞれ前記上部カバー５１と下部カバー５２の二者に固定される。次に、図３ａと図３ｃを参照しながら説明する。位置固定柱５３４は、前記上部カバー５１に突起した状態で取り付けられる。前記脚部５３１は、固定於下部カバー５２に固定される。前記位置固定柱５３４の側辺の突出部分は、前記ベース５３２の固定構造に固定される。図３ｃに示したように、前記解錠素子５３５は、前記位置固定柱５３４に挿入され、底部のピン構造は、図３ａを図３ｂの状態に変更し、この時、位置固定柱５３４が突起して下がり、前記上部カバー５１に取り付けられた状態を解除する。前記脚部５３１は下部カバー５２に固定され、前記位置固定柱５３４の側辺の突起構造は前記ベース５３２の固定構造の一側に移動する。

10

【００４７】

以下に、本発明のデータストレージデバイスの好適な実施形態を例に説明する。本発明の実施の過程に関する詳細な説明は以下のとおりである。

【００４８】

まず、図１ｂ及び図２ａを参照しながら説明する。上部カバー５１と下部カバー５２により本発明が保護されている状況において、前記電源素子２４から外部接続電源方式を介して作動電力を取得して、前記指紋認証スイッチ３３を通して前記電源素子２４をＯＮにすることで、前記専用ストレージモジュール１０、前記暗号モジュール２０と前記取付モジュール３０が作動に必要な電気エネルギーを有して、表示ランプ２６によって本発明との起動状態を知る。

20

【００４９】

前記情報端子プラグ１１が前記資訊插座情報端子ジャック２１に挿入された時、前記情報端子プラグ１１と前記情報端子ジャック２１は同時に移動する。図１ｂ、図２ｂ及び図２ｃに示したとおりである。

【００５０】

さらに、前記情報端子プラグ１１と前記情報端子ジャック２１は相互に接触する（図示はされない）。この時、前記ロック素子３１を触発して、ロック孔１２を固定し、情報端子プラグ１１と情報端子ジャック２１間において位置の安定させるのに役立つと同時に、前記ロック孔１２の一受電箇所（図示はされない）と前記３１を含むロック素子の一電気供給箇所（図示はされない）を電氣的に接続させて、前記専用ストレージモジュール１０が必要とする電気エネルギーを提供して、表示ランプ２６により本発明との使用状態を知る。

30

【００５１】

また、図５ｃに示したように、前記暗号モジュール２０は、前記情報端子ジャック２１を介して前記専用ストレージモジュール１０に電氣的に接続される。前記暗号モジュール２０の前記外部素子２２は、外部デバイス４０に電氣的に接続されて、機密データ４１を取得する。前記暗号化素子２３は、前記機密データ４１を暗号化し、さらに、暗号化された前記機密データ４１を前記ストレージ素子１４内に保存して、表示ランプ２６により本発明との読み取り状態を知る。

40

【００５２】

最後に、図２ｂ及び図２ｃを参照しながら説明する。前記専用ストレージモジュール１０を離脱させる場合は、図２ｃと図２ｄに示したように、前記ロック素子３１を触発してロック孔１２を固定した状態を解除し、動力素子３２により前記専用ストレージモジュール１０が押し出されて、情報端子プラグ１１と情報端子ジャック２１を分離させて、前記専用ストレージモジュール１０を離脱させることができる。

【００５３】

50

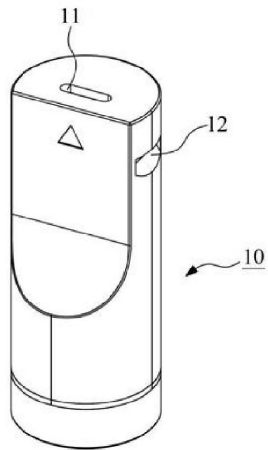
以上、本発明の実施例を図面を参照して詳述してきたが、具体的な構成は、これらの実施例に限られるものではなく、本発明の要旨を逸脱しない範囲の設計変更などがあっても、本発明に含まれる。

【符号の説明】

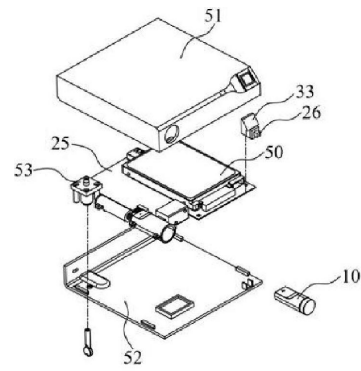
【 0 0 5 4 】

1 0	専用ストレージモジュール	
1 1	情報端子プラグ	
1 2	ロック孔	
1 3	コントロール素子	
1 4	ストレージ素子	10
1 5	基板	
2 0	暗号モジュール	
2 1	情報端子ジャック	
2 2	外部素子	
2 3	暗号化素子	
2 4	電源素子	
2 5	回路基板	
2 6	表示ランプ	
3 0	取付モジュール	
3 1	ロック素子	20
3 2	動力素子	
3 3	指紋認証スイッチ	
4 0	外部デバイス	
4 1	機密データ	
5 0	一般のストレージデバイス	
5 1	上部カバー	
5 2	下部カバー	
5 2 1	放熱フィン	
5 3	固定モジュール	
5 3 1	脚部	30
5 3 2	ベース	
5 3 3	スプリング	
5 3 4	位置固定柱	
5 3 5	解錠パーツ	

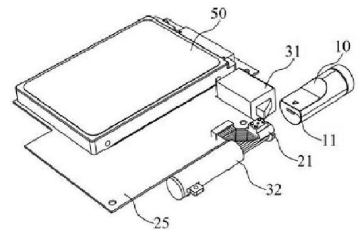
【図 1 a】



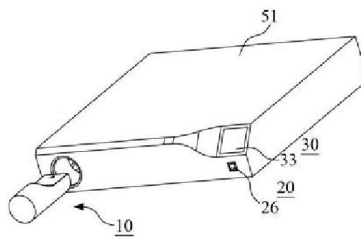
【図 2 a】



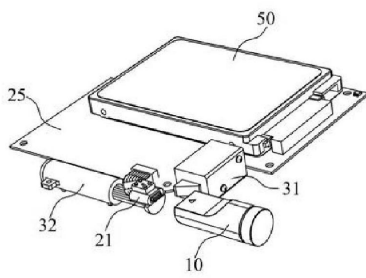
【図 2 b】



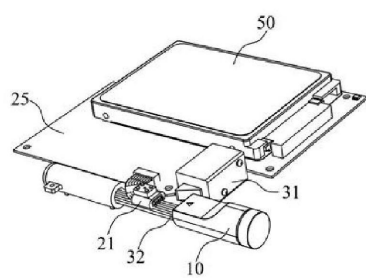
【図 1 b】



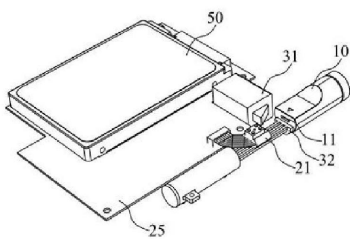
【図 2 c】



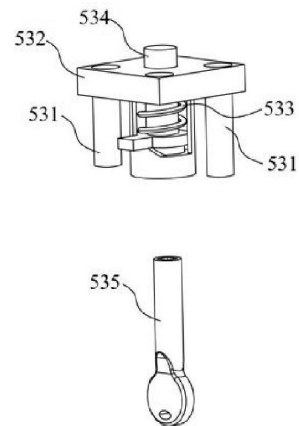
【図 2 e】



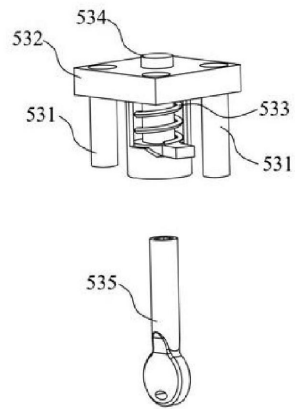
【図 2 d】



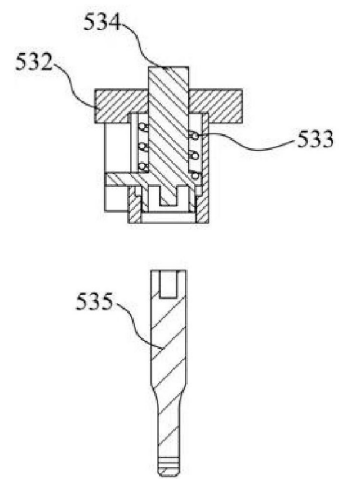
【図 3 a】



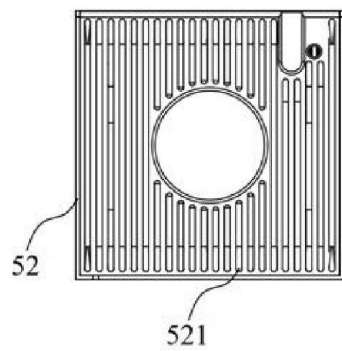
【図 3 b】



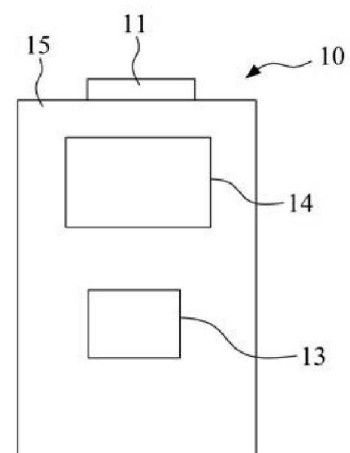
【図 3 c】



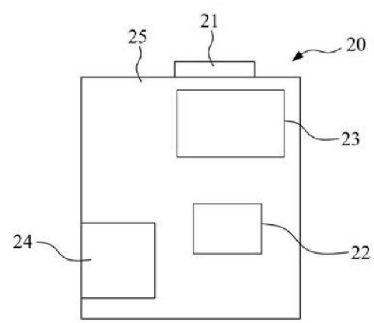
【図 4】



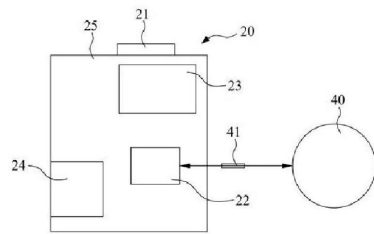
【図 5 a】



【図 5 b】



【図 5 c】



フロントページの続き

(72)発明者 チャン マオ - ティン

台湾 高雄市 ノースファーストロード カオシュン エクスポート プロセシング ゾーン

審査官 岸野 徹

(56)参考文献 米国特許出願公開第2008/0280490(US, A1)

米国特許第08928455(US, B1)

米国特許出願公開第2002/0073340(US, A1)

米国特許出願公開第2011/0163845(US, A1)

特開2001-035371(JP, A)

(58)調査した分野(Int.Cl., DB名)

G06F 21/60

G06F 21/32

G06F 21/62

H04L 9/10

H04L 9/32