(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2006-259782
(P2006-259782A)
(43)公開日　平成18年9月28日(2006.9.28)

(51)Int.Cl.		F I		テーマコード（参考）
G08B 13/14	(2006.01)	G08B 13/14	Z	5C084
H04B 5/02	(2006.01)	H04B 5/02		5K012

審査請求 未請求　請求項の数 33　ＯＬ　（全 17 頁）

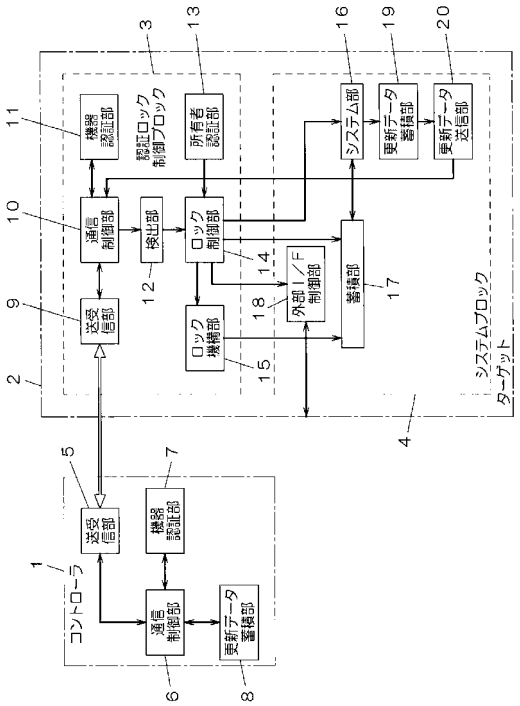
(21)出願番号　特願2005-58547(P2005-58547)
(22)出願日　平成17年3月3日(2005.3.3)
(31)優先権主張番号　特願2005-38811(P2005-38811)
(32)優先日　平成17年2月16日(2005.2.16)
(33)優先権主張国　日本国(JP)

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真１００６番地
(74)代理人　100097445
弁理士　岩橋　文雄
(74)代理人　100103355
弁理士　坂口　智康
(74)代理人　100109667
弁理士　内藤　浩樹
(72)発明者　日高　巌
大阪府門真市大字門真１００６番地　松下電器産業株式会社内

Ｆターム(参考)　5C084 AA09 AA15 BB33 CC16 CC23
CC33 DD07 EE07 FF02
5K012 AA01 AB18 BA07

(54)【発明の名称】機器盗難防止通信システム

(57)【要約】
【課題】従来の携帯情報端末のセキュリティーシステムでは、端末盗難後の不正使用や不正流通を防ぐことができない。
【解決手段】ターゲット機器とコントローラ機器で近距離の無線通信を行い、設定距離以内かまたは通信可能かを検出して機器を認証するコントローラと、前記コントローラと無線通信を行い機器の動作及び機構系を制御するターゲットと、前記ターゲットの構成として所有者によって蓄積部のデータを更新した場合にコントローラへの送信・機器の動作・データの蓄積・外部機器との通信制御を行うシステムブロック、通信不能を検出してシステムブロックのロック制御及び機器の認証及び所有者の認証を行う認証ロック制御ブロックによって実現する。
【選択図】図１



【特許請求の範囲】
【請求項１】
近距離の無線通信を行いターゲット機器と一定間隔もしくは不定期間隔の通信によって設定距離以内かまたは通信可能かを検出して機器の認証・無線通信によりターゲットの更新データを受信して蓄積を行うコントローラと、前記コントローラと無線通信を行い機器の動作及び機構系を制御するターゲットと、前記ターゲットの構成として機器の動作制御・データの蓄積・外部機器との通信制御・蓄積されたデータの更新を行った場合に更新データの蓄積するシステムブロック、前記コントローラと通信を行いコントローラとの距離を測定して一定距離以上もしくは通信不可能の検出を行いシステムブロックのロック制御を行う及び機器の認証及び所有者の認証を行う認証ロック制御ブロックを備えたことを特徴とする機器盗難防止通信システム。
【請求項２】
コントローラは、ターゲットと機器認証する為の通信とデータ蓄積から更新されたデータの蓄積データを送受信する送受信部と、前記送受信部を含む通信に関する制御と蓄積された更新データを通信する為の制御を行う通信制御部と、前記ターゲットとの送受信を行い前記コントローラの前記通信制御部からの信号によって機器認証を行う機器認証部と、前記ターゲットで蓄積された更新データを通信して蓄積する更新データ蓄積部を備えることを特徴とする請求項１記載の機器盗難防止通信システム。
【請求項３】
コントローラは、モジュールとして携帯通信機器に搭載して機能する請求項１、または２記載の機器盗難防止通信システム。
【請求項４】
認証ロック制御ブロックは、コントローラと機器認証する為の通信とデータ蓄積から更新されたデータの蓄積データを送受信する送受信部と、前記送受信部を含む通信に関する制御と蓄積された更新データを通信する制御を行う通信制御部と、前記コントローラから一定距離以上離れたことを検出または一定間隔もしくは不定期間隔の通信によって通信可能かを検出する検出部と、前記コントローラとの送受信を行い前記ターゲットの通信制御部の信号によって機器認証を行う機器認証部と、バイオメトリクス、パスワードによって所有者を特定する所有者認証部と、前記検出部によってシステムブロックに対してロックをかけるロック動作と前記機器認証部と前記所有者認証部によってロック解除動作を行うロック制御部と、前記システムブロックの蓄積部を機構的のロックするロック機構部を備えることを特徴とする請求項１記載の機器盗難防止通信システム。
【請求項５】
システムブロックは、ターゲットの動作全てを管理し検出部からの信号によってシステムブロックのロック動作を行うシステム部と、蓄積データのロック制御を行う蓄積部と、外部機器との通信をロック制御する外部Ｉ／Ｆ制御部と、所有者が前記ターゲットを操作して前記蓄積部のデータを更新した内容を更新データとして蓄積する更新データ蓄積部と、更新データ蓄積部のデータを前記認証ロック制御ブロックの通信制御部に送る更新データ送信部を備えることを特徴とする請求項１記載の機器盗難防止通信システム。
【請求項６】
更新データ蓄積部は蓄積部のデータで更新された部分のみを蓄積する事を特徴とする請求項１、または５記載の機器盗難防止通信システム。
【請求項７】
ターゲットの更新データ送信部からデータの送信をオン／オフ制御できる請求項１、または５、または６記載の機器盗難防止通信システム。
【請求項８】
システム部は、ロック制御部からの信号によって起動を停止して機器の動作をロック制御することを備えることを特徴とする請求項１、または５、または６記載の機器盗難防止通信システム。
【請求項９】

システム部は、ロック制御部からの信号によってシステム部の起動のデータを消去することを備えることを特徴とする請求項１、または５、または６記載の機器盗難防止通信システム。

【請求項１０】

蓄積部は、ロック制御部からの信号によって機構的にロックして取り外しを不可能にすることを備えることを特徴とする請求項１、または５、または６記載の機器盗難防止通信システム。

【請求項１１】

蓄積部は、ロック制御部からの信号によって蓄積データの消去を行うことを備えることを特徴とする請求項１、または５、または６記載の機器盗難防止通信システム。

【請求項１２】

蓄積部は、ロック制御部からの信号によって蓄積データの暗号化を行うことを備えることを特徴とする請求項１、または５、または６記載の機器盗難防止通信システム。

【請求項１３】

外部Ｉ／Ｆ制御部は、ロック制御部からの信号によって外部機器との通信を遮断することを備えることを特徴とする請求項１、または５、または６記載の機器盗難防止通信システム。

【請求項１４】

外部Ｉ／Ｆ制御部は、ロック制御部からの信号によって外部機器への電源供給を停止することを備えることを特徴とする請求項１、または５、または６記載の機器盗難防止通信システム。

【請求項１５】

更新データ送信部は、暗号化して通信制御部に送信する機能を備えることを特徴とする請求項１、または５記載の機器盗難防止通信システム。

【請求項１６】

コントローラとターゲットは、それぞれ機器盗難防止通信システムのオン／オフの制御が出来る構成を持つ請求項１記載の機器盗難防止通信システム。

【請求項１７】

コントローラとターゲットはそれぞれの機器盗難防止通信システムがオン状態において通常モードと盗難防止モードを設けて、通常モードではコントローラとターゲットの通信間隔を長くし、盗難防止モードにおいては通信間隔を短くすることによって盗難されても即時にターゲットのロックがかかるようにする構成の請求項１記載の機器盗難防止通信システム。

【請求項１８】

コントローラとターゲットは、任意の場所を離れた時点でそれぞれの機器盗難防止通信システムをオン状態にして強制的に盗難防止モードに設定する構成の請求項１記載の機器盗難防止通信システム。

【請求項１９】

ターゲットは、蓄積部を搭載している携帯機器である請求項１記載の機器盗難防止通信システム。

【請求項２０】

ロック制御部で脱着可能な蓄積部に対して取り出しレバーにロックをかけて取り出しを不可能にする請求項１、または４記載の機器盗難防止通信システム。

【請求項２１】

ロック制御部で脱着可能な蓄積部に対してカバーを行う構成の場合カバーにロックをかけて取り出しを不可能にする請求項１、または４記載の機器盗難防止通信システム。

【請求項２２】

ロック制御部は、蓄積部のデータを消滅させて復元出来ないようにする制御を行う請求項１、または４記載の機器盗難防止通信システム。

【請求項２３】

蓄積部が固定ハードディスクである請求項１０，または１１，または１２記載の機器盗難防止通信システム。
【請求項２４】
蓄積部が内蔵のメモリである請求項１０，または１１，または１２記載の機器盗難防止通信システム。
【請求項２５】
蓄積部が脱着可能なメモリカードである請求項１０，または１１，または１２記載の機器盗難防止通信システム。
【請求項２６】
蓄積部が脱着可能なハードディスクカードである請求項１０，または１１，または１２記載の機器盗難防止通信システム。
【請求項２７】
蓄積部がハードディスクである請求項１０，または１１，または１２記載の機器盗難防止通信システム。
【請求項２８】
蓄積部がテープメディアである請求項１０，または１１，または１２記載の機器盗難防止通信システム。
【請求項２９】
蓄積部がディスクメディアである請求項１０，または１１，または１２記載の機器盗難防止通信システム。
【請求項３０】
ロック制御部は、ターゲットにハードディスクを固定する為に準備されている部分を機構的にロックする請求項１記載の機器盗難防止通信システム。
【請求項３１】
ロック制御部によってターゲットからハードディスクが取り出せないようにｎ本（ｎ＝１、２、３、・・・）のロックバーを備えて取り外しを防止する請求項１記載の機器盗難防止通信システム。
【請求項３２】
ロック制御においては、機器認証部または所有者認証部のどちらか一方で認証ができた場合にロック解除を行う、または前記機器認証部と前記所有者認証部の両方が認証できた場合にロック解除を行う構成を持つ請求項１記載の機器盗難防止通信システム。
【請求項３３】
所有者認証部においてバイオメトリクスまたはパスワードのどちらか一方で所有者の認証を行う、またはバイオメトリクスとパスワードの両方で所有者の認証を行う構成を持つ請求項１、または４記載の機器盗難防止システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、機器盗難防止通信システムに係り、特に、所有者が携行物品にコントローラを内蔵または装着した送受信部と、所有者が鞄等に入れているターゲットに内蔵または装着した送受信部との間で短距離無線通信方式の通信をさせて送受信部間の距離を測定し、認証がとれている間に所有者がターゲットを操作して蓄積部のデータに変更を加えた場合にその更新データを蓄積していてコントローラに送受信部を介して転送を行いコントローラに蓄える。更新データはコントローラの更新されたデータの蓄積部の容量を少なくする為に蓄積部にある元データに対しての差分データでも良い。もしも盗難にあった場合でもターゲットの蓄積されたデータが会社にある場合、コントローラとの差分データと元データで復元を行うことが出来る。もしくは更新したデータを蓄積していてコントローラに送受信部を介して転送を行いコントローラに蓄える。もしも盗難にあった場合でもコントローラにある更新したデータに関しては所有者自身が身につけている為にセキュリティーとして安全である。また、コントローラの送受信部とターゲットの送受信部間で短距離無線

通信方式の通信をさせ送受信部間の距離を測定し、一定距離以上になるか、または無線信号の通信が不可能になった場合にターゲットの機器動作を停止、蓄積メディアを機構的にロック、蓄積部のデータの消滅等を行う事によって盗難にあった場合にターゲットとしての価値を無くしセキュリティーの保護及び機器の不正販売を防止する機器盗難防止システムに関する。

【背景技術】

【０００２】

近年、パーソナルコンピュータ（パソコン）及びモバイル機器は、盗難等で秘密情報の漏洩や不正販売を行う事が発生しており、パソコンに対してはパスワードの設定を行って起動の制限及びハードディスクのアクセス制限を行ってセキュリティー保護している。

【０００３】

以下に従来の盗難防止システムについてパソコンの構成を用いて説明する。

【０００４】

従来の盗難防止システムを図８に示す。図８は従来のセキュリティーシステムを搭載したパソコンのブロック図を示すものである。図８において、８０はパソコン本体である。８１はパソコンの全システムを制御するシステム部である。８２はシステム部８１で制御・作成されたデータ等を格納するハードディスクである。８３はパソコン８０を起動する為に必要なデータの入出力を制御・管理するソフトになる基本プログラムを搭載しシステム部８１とハードディスク８２を制御するＢＩＯＳ（Ｂａｓｉｃ　Ｉｎｐｕｔ　Ｏｕｔｐｕｔ　Ｓｙｓｔｅｍ）部である。

【０００５】

以上のように構成された従来の盗難防止システムについて、以下その動作について説明する。

【０００６】

まず、パソコン８０の電源を投入した後、ＢＩＯＳ部８３によりパソコンの起動が開始される。この時、ＢＩＯＳ部８３にパスワードが設定されているとシステム部８１の起動前にパスワードを要求される。これによりパソコン８０の起動の制限を行ってセキュリティー保護を行っている。また、ＢＩＯＳの設定によってはハードディスクにも制限をかけることによってハードディスクを取り外して他のパソコンに装着して内部情報を入手しようとしてもハードディスクを認識しないようになっていてセキュリティーの保護をかけている。

【特許文献１】特開２００３－１０９１２７号公報

【発明の開示】

【発明が解決しようとする課題】

【０００７】

しかしながら上記の従来の構成では、パスワード設定によって保護している為解除の可能性がある、また脱着可能なメモリカードなどにおいての保護はかけられていないという問題点を有していた。

【０００８】

本発明は上記従来の問題点を解決するもので、コントローラとターゲットとの間で認証許可にならない限りターゲットの起動を停止、起動部分のプログラムデータを消去、蓄積部のデータを消去または暗号化、蓄積部の取り外しを機構的に不可能にする、外部機器との通信の遮断等を行う事によって、セキュリティーの保護及び不正販売を防止する。ただし、コントローラとターゲット間で認証がとれている間に所有者がターゲットを操作して蓄積部のデータに変更を加えた場合にその更新データを蓄積していてコントローラに送受信部を介して転送を行いコントローラに蓄える。更新データはコントローラの更新されたデータの蓄積部の容量を少なくする為に蓄積部にある元データに対しての差分デーでも良い。もしも、盗難にあった場合でもターゲットの蓄積されたデータが会社にある場合、コントローラとの差分データと元データで復元を行うことが出来る。もしくはコントローラの蓄積部の容量が許容範囲の場合は、更新したデータを蓄積していてコントローラに送受

信部を介して転送を行いコントローラに蓄える。もしも、盗難にあった場合でもコントローラにある更新したデータに関しては所有者自身が身につけている為にセキュリティーとして安全な機器盗難防止通信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】

【０００９】

この目的を達成するために本発明の機器盗難防止通信システムは、近距離の無線通信を行いターゲット機器と一定間隔もしくは不定期間隔の通信によって設定距離以内かまたは通信可能かを検出して機器の認証・無線通信によりターゲットの更新データを受信して蓄積を行うコントローラと、前記コントローラと無線通信を行い機器の動作及び機構系を制御するターゲットと、前記ターゲットの構成として機器の動作制御・データの蓄積・外部機器との通信制御・蓄積されたデータの更新を行った場合に更新データの蓄積するシステムブロック、前記コントローラと通信を行いコントローラとの距離を測定して一定距離以上もしくは通信不可能の検出を行いシステムブロックのロック制御を行う及び機器の認証及び所有者の認証を行う認証ロック制御ブロックを有している。

【００１０】

この構成によって、コントローラとターゲットとの間で認証許可にならない限りターゲットの起動を停止、起動部分のプログラムデータを消去、蓄積部のデータを消去または暗号化、蓄積部の取り外しを機構的に不可能にする、外部機器との通信の遮断等を行う事によって、セキュリティーの保護及び不正販売を防止する。ただし、コントローラとターゲット間で認証がとれている間に所有者がターゲットを操作して蓄積部のデータに変更を加えた場合にその更新データを蓄積していてコントローラに送受信部を介して転送を行いコントローラに蓄える。更新データはコントローラの更新されたデータの蓄積部の容量を少なくする為に蓄積部にある元データに対しての差分デーでも良い。もしも、盗難にあった場合でもターゲットの蓄積されたデータが会社にある場合、コントローラとの差分データと元データで復元を行うことが出来る。もしくはコントローラの蓄積部の容量が許容範囲の場合は、更新したデータを蓄積していてコントローラに送受信部を介して転送を行いコントローラに蓄える。もしも、盗難にあった場合でもコントローラにある更新したデータに関しては所有者自身が身につけている為にセキュリティーとしては安全という効果が得られる。

【発明の効果】

【００１１】

以上のように本発明は、所有者が携行物品にコントローラを内蔵または装着した送受信部と、所有者が鞄等に入れているターゲットに内蔵または装着した送受信部との間で短距離無線通信方式の通信をさせて送受信部間の距離を測定し、認証がとれている間に所有者がターゲットを操作して蓄積部のデータに変更を加えた場合にその更新データを蓄積していてコントローラに送受信部を介して転送を行いコントローラに蓄える。更新データはコントローラの更新されたデータの蓄積部の容量を少なくする為に蓄積部にある元データに対しての差分データでも良い。もしも盗難にあった場合でもターゲットの蓄積されたデータが会社にある場合、コントローラとの差分データと元データで復元を行うことが出来る。もしくは更新したデータを蓄積していてコントローラに送受信部を介して転送を行いコントローラに蓄える。もしも盗難にあった場合でもコントローラにある更新したデータに関しては所有者自身が身につけている為にセキュリティーとして安全である。また、コントローラの送受信部とターゲットの送受信部間で短距離無線通信方式の通信をさせ送受信部間の距離を測定し、一定距離以上になるか、または無線信号の通信が不可能な場合にターゲットの機器動作を停止、蓄積メディアを機構的にロック、蓄積部のデータの消滅を行う事によって盗難にあった場合にターゲットとしての価値を無くしセキュリティーの保護及び機器の不正販売を防止するという効果が得られる。

【発明を実施するための最良の形態】

【００１２】

本発明の請求項１に記載の発明は、近距離の無線通信を行いターゲット機器と一定間隔

もしくは不定期間隔の通信によって設定距離以内かまたは通信可能かを検出して機器の認証・無線通信によりターゲットの更新データを受信して蓄積を行うコントローラと、前記コントローラと無線通信を行い機器の動作及び機構系を制御するターゲットと、前記ターゲットの構成として機器の動作制御・データの蓄積・外部機器との通信制御・蓄積されたデータの更新を行った場合に更新データの蓄積するシステムブロック、前記コントローラと通信を行いコントローラとの距離を測定して一定距離以上もしくは通信不可能の検出を行いシステムブロックのロック制御を行う及び機器の認証及び所有者の認証を行う認証ロック制御ブロックを備えたことを特徴とする機器盗難防止通信システムあり、コントローラとターゲットとの間で認証許可にならない限りターゲットの起動を停止、起動部分のプログラムデータを消去、蓄積部のデータを消去または暗号化、蓄積部の取り外しを機構的に不可能にする、外部機器との通信の遮断を行う事によって、セキュリティーの保護及び不正販売を防止する。ただし、コントローラとターゲット間で認証がとれている間に所有者がターゲットを操作して蓄積部のデータに変更を加えた場合にその更新データを蓄積していてコントローラに送受信部を介して転送を行いコントローラに蓄える。更新データはコントローラの更新されたデータの蓄積部の容量を少なくする為に蓄積部にある元データに対しての差分デーでも良い。もしも、盗難にあった場合でもターゲットの蓄積されたデータが会社にある場合、コントローラとの差分データと元データで復元を行うことが出来る。もしくはコントローラの蓄積部の容量が許容範囲の場合は、更新したデータを蓄積していてコントローラに送受信部を介して転送を行いコントローラに蓄える。もしも、盗難にあった場合でもコントローラにある更新したデータに関しては所有者自身が身につけている為にセキュリティーとしては安全という作用を有する。

【００１３】

以下、本発明の実施の形態について、図１から図７を用いて説明する。

【００１４】

（実施の形態１）

図１は本発明の機器盗難防止通信システムのブロック図であり、図１において、１は近距離の無線通信を行いターゲット機器と一定間隔もしくは不定期間隔の通信によって設定距離以内かまたは通信可能かを検出して機器認証を行うコントローラである。コントローラ１は、ターゲット２（後述）を使用する際に、ターゲット２との間で通信が可能なように、近くに配置させておく必要がある。そのために、コントローラ１を小型ユニット化して、使用者が普段ターゲットを使用する場所に設置させたり、使用者が容易に身に付けることが可能なように構成してもよい。また、使用者が身に付けることを前提とする場合は、携帯電話機や腕時計など、一般に使用者が常時身につけているものと思われる機器に、モジュール化して内蔵させてもよい。いずれにしても、設置状態や搭載状態については特に限定されるものではない。

【００１５】

２はコントローラ１と無線通信を行い機器の認証動作を行う事と機器の動作及びデータの蓄積する事と外部機器との通信を制御する事と蓄積部のデータを更新したデータを蓄積する事とコントローラ１に送信する機能を持ったターゲットであり、コントローラ１との間で用いる無線通信手段については特に限定はしないが、盗難直後にロックシステムが起動することが望ましいので、通信距離が５ｍ程度のＢｌｕｅｔｏｏｔｈ（登録商標）規格などに基づくものを用いることが考えられる。また、本実施の形態では、ターゲット２はノート型パソコンなどのモバイル機器を想定しているが、可搬できるものであればその実用範囲に入るため、ノート型パソコンに限定されるものではない。

【００１６】

３はターゲット２に搭載されていてコントローラ１との無線通信を行い機器の認証を行い通信状況によってターゲット2の動作を停止させる等の制御を行う事と、蓄積部１７（後述）等を機構的にロックして脱着を防止する事と、蓄積部１７のデータを消去または暗号化する動作を行う事と、外部機器との通信を遮断する制御を行うブロックを備える認証ロック制御ブロックである。ターゲット２の動作を停止させたり、蓄積部１７を機構的あ

るいは信号的にロックするシステムを、以下ロックシステムと称する。

【００１７】

４はターゲット２に備えられ、ターゲット2の機器動作を制御する事とデータの蓄積を行う事と外部機器との通信制御を行う事と所有者が蓄積しているデータを更新したデータを蓄える事と更新データとして蓄えられたデータを認証ロック制御ブロック３に転送するシステムブロックである。外部機器の例としては、ＩＥＥＥ１３９４，ＵＳＢ、ＬＡＮ規格を用いたハードディスク等の蓄積器やディスクドライブ等、またはＩＥＥＥ１３９４，ＵＳＢ、ＬＡＮ規格を採用した全ての機器がある。

【００１８】

５はコントローラ１に内蔵されターゲット２との無線通信を行う送受信部、６はターゲット２と無線通信する送受信部５の制御を行い、またロックシステムの機能をオン／オフ制御する通信制御部、７は通信制御部６からの情報を元にコントローラ１に登録しているターゲット２が一致しているかを認証する機器認証部、８はターゲット２から送信されて送受信部５と通信制御部６を経由して更新データとして蓄積を行う更新データ蓄積部、９はターゲット２に内蔵されコントローラ１との無線通信を行う送受信部、１０はコントローラ１と無線通信する送受信部９の制御を行うまたロックシステムの機能をオン／オフ制御する通信制御部、１１は通信制御部１０からの情報を元にターゲット２に登録しているコントローラ１が一致しているかを認証する機器認証部、１２は通信制御部１０からの情報を元にコントローラ１との距離が設定以上になっているかもしくは通信が不可能な場合を検出する検出部、１３はバイオメトリクス（指紋、網膜等の認証を行う手法）およびパスワードとの組み合わせを行って所有者を特定する所有者認証部で、本実施の形態ではバイオメトリクスとパスワードの両方を用いて所有者認証を行っているが、いずれか一方のみを用いて認証を行ってもよい。また、認証する手段はバイオメトリクスやパスワードに限らず、他の手段を用いてもよい。１４は検出部１２からの情報を元に通信が不成立になった場合または機器認証部１１の機器認証が出来ない場合または所有者認証部１３で所有者の特定が出来ない場合にシステムブロック４の起動を制御して停止するもしくは起動ブロックのデータを消去する、また蓄積部１７（脱着可能なメモリカード等を含む）を機構的にロックして取り外せないようにするもしくは蓄積部１７に格納されているデータを消去または暗号化する、また外部機器との通信を遮断するもしくは電源の供給を停止する制御（例えば１３９４、ＵＳＢ等では電源の供給を行っている）を行うロック制御部、１５はロック制御部１５からの情報を元に蓄積部１７（脱着可能なメモリカード等を含む）を機構的にロックして取り外せないようにするロック機構部、１６はターゲット2の起動と動作を制御するシステム部、１７はシステム部１６からの制御を受けてデータを蓄積する蓄積部でロック制御部１４からの情報を受けた場合には蓄積されているデータを消去または暗号化するまたはロック機構部１５の情報を元に機構的に取り外せない処理を行う、１８はシステム部１６と通信を行い外部に接続される機器との制御を行う外部Ｉ／Ｆ制御部でロック制御部１４からの情報を受けた場合には外部機器との通信の遮断または外部機器に対して電源を供給している場合には電源供給の停止を行う、１９は所有者がターゲット２において蓄積部１７のデータを更新した場合に更新データを蓄積する更新データ蓄積部、２０は更新データ蓄積部１９のデータを通信制御部１０に送り送受信部９を経由してコントローラ２に送り更新データ蓄積部８に蓄積する更新データ送信部によって構成される。

【００１９】

以上のように構成された機器盗難防止通信システムについて、図１を用いてその動作を説明する。

【００２０】

まず、コントローラ１とターゲット2のそれぞれの機器盗難防止通信システムをオンさせて動作状態にする。次に所有者の認証を行う為にバイオメトリクス、パスワードの組み合わせによって所有者認証部１３でターゲット２と所有者との認証を行う。次にコントローラ１の機器認証部７とターゲット２の機器認証部１１によって認証動作を行う事によっ

て通信が開始し始める。ターゲット2の起動にあたっては機器認証部１１と所有者認証部１３の両方が成立した場合またはどちらか一方が成立した時点で実行される。

【００２１】

認証が成立した時点で送受信部５に対して通信制御部６が通信に関する制御を行うのと並行して機器認証部７と連携をとってターゲット２との関係を保つようにする。次に送受信部９に対して通信制御部１０が通信に関する制御を行うのと並行して機器認証部１１と連携をとってコントローラ１との関係を保つようにする。コントローラ１とターゲット２との間で認証による関係が保たれている環境ではターゲット２は通常動作を行う。通常動作で所有者によって蓄積部１７のデータを更新した場合には更新データ蓄積部１９に更新したデータを格納する。更新データ蓄積部１９のデータを更新データ送信部２０に送り直接通信か、暗号化通信を行い通信制御部１０に送り認証通信と同様に送受信部９からコントローラ１の送受信部５に送る。

【００２２】

次に送受信部５で受信したデータは通信制御部６を経由して更新データ蓄積部８に蓄積される。更新データ送信部２０をオン／オフ構成により更新データの通信をオン／オフ出来る。ターゲット２を外部に持ち出す場合にはコントローラ１を所有者が携帯し、ターゲット２を鞄などに入れる場合が発生する。もしもターゲット２が盗難にあった場合、送受信部５と送受信部９の間が設定距離以上になるか正常通信不可能になるかのどちらかが発生して近距離通信が不可能になる。その時点で機器認証部７と機器認証部１１との間で認証不可になる。この情報を通信制御部１０から受信して検出部１２で認証不可という判断を行う。検出部１２で認証不可と判断された情報を受信してロック制御部１４がシステム部１６の起動回路を停止するかもしくは起動回路のプログラムを消去する。

【００２３】

次にロック制御部１４により蓄積部１７に保存しているデータを消去または暗号化する。次に外部Ｉ／Ｆ制御部に関しては通信を遮断する等の制御を行うかもしくは電源の供給を停止する。ロック制御部１４からロック機構部１５に命令して蓄積部１７を機構的にロックをかけて取り出しを不可能にする。ロック制御を解除する為にはコントローラ１とターゲット２が無線通信出来るようになった上で機器認証部７と機器認証部１１との間で認証を確立するまたはバイオメトリクスまたはパスワードとの組み合わせによって所有者認証部１３で認証の確立を行う必要がある。

【００２４】

なお、機器認証部１１と所有者認証部１３の両方の認証が確立したという構成にしても良い。認証が確立した状態で検出回路１２からロック制御部１４に情報を送りシステム部１６の起動回路のプログラムが消去されている場合、同一プログラムを格納したＲＯＭから読み出してシステム部１６が動作するようにする。

【００２５】

なお、以上の説明でコントローラ１とターゲット２の機器盗難防止通信システムをオンするということで説明したが、特定エリアからコントローラ１とターゲット２を移動させる場合には強制的に機器盗難防止通信システムをオンさせても良い。この場合には、コントローラあるいはターゲットにＧＰＳ機能を搭載し、コントローラあるいはターゲットの現在位置を把握して、特定エリア外へ移動したことを認識する方法がある。また、特定エリアにおいて特定の信号を発信して、コントローラ１とターゲット２との間で通信を行い、強制的に機器盗難防止システムをオンさせても良い。いずれにせよ、このように強制的に機器盗難防止システムをオンさせる機能の搭載要否は、あくまで任意であるとともに、搭載する場合の構成については前述の例に限るものではない。

【００２６】

図２は本発明の蓄積部１７で脱着可能なメモリカードを機構的にロックさせる図であり、図２において（ａ）の２はターゲット、２４は脱着可能なメモリカード、２５はメモリカード２４を取り出す為のプッシュ形取り出しピンを備えるモバイル機器において、（ｂ）の２６はプッシュ形取り出しピン２５を機構的に（ｂ）の矢印位置からピンを挿入して

固定するロックピンによって構成される。（ｃ）及び（ｄ）はロックピンを設けた位置の他例である。

【００２７】

以上のように構成された機器盗難防止通信システムのロック方法に関して、図２を用いてその動作を説明する。まず、メモリカード２４をターゲット２に挿入した状態でプッシュ形取り出しピン２５はターゲット2の中に押された状態になっている。メモリカードを取り出す場合はプッシュ形取り出しピン２５をターゲット２内に押し込むことによって飛び出してくるので、再度押し込むことでメモリカード２４を取り出すことが可能になる構成になっている。上記の動作に関しては機構的に（ａ）の矢印の方向に動作する。

【００２８】

メモリカード２４が挿入されてプッシュ形取り出しピン２５がターゲット２に挿入されている状況で、ロック制御部１４からの指令によって（ｂ）のロックピン２６が矢印の方向からプッシュ形取り出しピン２５に挿入されて固定する。この動作によってメモリカード２４の取り出しを不可能にする。なお、以上の説明で（ｂ）のロックピン２６の位置を説明したが、プッシュ形取り出しピン２５であればどの位置に設置しても良い。

【００２９】

なお、以上の説明でメモリカードとして説明したが、ハードディスクカード、ディスクカード等蓄積機能を備えるカードでも良い。なお、以上の説明でメモリカード２４を挿入するスロットを１個で説明しているが複数枚が挿入されるスロットで構成されていても良い。

【００３０】

図３は本発明の蓄積部１７で脱着可能なメモリカードを機構的にロックさせる図であり、同図（ａ）は本ロック機構を備えたターゲット全体構成を示す斜視図、同図（ｂ）は同図（ａ）における取り出しピン２７近傍の斜視図、同図（ｃ）～（ｅ）はロックピン３０を用いて格納レバー２８を固定する構成例を示す斜視図、同図（ｆ）～（ｈ）はロックピン３１を用いて取り出しピン２７を固定する構成例を示す斜視図である。なお、同図（ｂ）と（ｃ）は同じ構成である。図３において、２はターゲット、２４は脱着可能なメモリカード、２７はメモリカード２４を取り出す為の取り出しピン、２８はメモリカード２４を格納した時に飛び出している取り出しピン２７を回転軸によって矢印のように折り畳んでターゲット２に格納する格納レバー、２７ａはロックピン３１が挿入されるロック穴、２８ａはロックピン３０が挿入されるロック穴、２９は取り出しピン２７と格納レバー２８を接続する回転軸、３０は取り出しピン２７を機構的に固定する為に格納レバー２８を固定するロックピン、３１は取り出しピン２７を固定するロックピンによって構成される。なお、同図（ｃ）～（ｈ）はロックピンとロック穴の位置の応用例である。

【００３１】

以上のように構成された機器盗難防止通信システムのロック方法に関して、図３を用いてその動作を説明する。まず、メモリカード２４をターゲット２に挿入した時に取り出しピン２７はターゲット２から格納レバー２８の部分が飛び出した状態になっている。この格納レバー２８を回転軸２９によって図３（ａ）中の矢印イ方向に折り畳んでターゲット２内に格納する構成になっている。またメモリカード２４の取り出しに関しては、格納レバー２８を回転軸２９によって図３（ｂ）中の矢印のア方向に回転させて取り出しピン２７と真っ直ぐなるようにして、図３（ａ）中の矢印ウ方向へ押し込むことで実現できる構成になっている。この構成の場合、ロック制御部１４からの指令で（ｂ）のようにロックピン３０をロック穴２８ａに挿入して格納レバー２８の回動動作を禁止し固定する。本実施の形態ではロックピンによる固定方法として、図２（ｂ）や（ｃ）に示す構成以外に、（ｄ）及び（ｅ）に示すようにロック穴２８ａの位置やロックピン３０の挿入方向を応用した構成や、（ｆ）～（ｈ）に示すようにロックピン３１によって取り出しピン２７を固定する事によってメモリカード２４の取り出しを不可能にする構成も考えられる。

【００３２】

なお、以上の説明で（ｂ）～（ｅ）に示すようなロックピン３０の位置を説明したが、

格納レバー２８上であればどの位置に設置しても良い。なお、以上の説明で（ｆ）～（ｈ）に示すようなロックピン３１の位置を説明したが、取り出しピン２７上であればどの位置に設置しても良い。なお、以上の説明でロックピン３０とロックピン３１を個別に説明したが両方を搭載しても良い。なお、以上の説明でメモリカードとして説明したが、ハードディスクカード、ディスクカード等蓄積機能を備えるカードでも良い。なお、以上の説明でメモリカード２４を挿入するスロットを１個で説明しているが複数枚が挿入されるスロットで構成されていても良い。

【００３３】

図４は本発明の蓄積部１７で脱着可能なメモリカードのスロットに対してカバーを行う事でメモリカードの取り出しを不可能にする図であり、図４において（ａ）の２はターゲット、２４は脱着可能なメモリカード、３５はターゲット２に装着しているメモリカード２４に蓋をするためのカバー、３６はターゲット２にカバー３５を取り付ける為の回転軸を備えるモバイル機器において、（ｂ）の３７はカバー３５を固定する為のロックピン、（ｃ）の３８はカバー３５を固定する為の固定部、（ｄ）の３９は固定部３８の一部でターゲット２に装着している矢印形固定部、４０は固定部３８の一部でターゲット２に装着している矢印形固定部、４１はカバー３５の一部でターゲット２にカバー３５を固定する為の矢印形ロック部によって構成される。

【００３４】

以上のように構成された機器盗難防止通信システムのロック方法に関して、図４を用いてその動作を説明する。まず、（ａ）の動作としてメモリカード２４をターゲット２に挿入した時に回転軸３６を基点にしてカバー３５を閉じる。この回転軸３６が無い方にロック出来る仕組みを備える。（ｂ）はカバー３５で回転軸３６が無い方とターゲット２との間にロックピン３７を装着できる構成にして、ロック指令がロック制御部１４から発行されるとロックピン３７によってターゲット２とカバー３５を固定してメモリカード２４の取り出しを不可能にする。（ｃ）はカバー３５で回転軸３６が無い方とターゲット２との間に固定部３８を設置しカバー３５の開閉を行う。（ｄ）は（ｃ）の構造説明で通常は矢印形固定部３９と矢印形固定部４０を矢印のように移動させることによって矢印形ロック部４１を固定、解除を行ってカバー３５の開閉を行う。ロック指令がロック制御部１４から発行されると矢印形固定部３９と矢印形固定部４０は通常の開閉より優先してターゲット２とカバー３５を固定してメモリカード２４の取り出しを不可能にする。

【００３５】

なお、以上の説明で図（ｂ）のロックピン３７の位置を説明したが、カバー３５であればどの位置に設置しても良い。なお以上の説明で（ｄ）の矢印形固定部３９、矢印形固定部４０から構成される固定部３８とカバー３５に付随している矢印形ロック部４１によって固定するという説明をしたが、固定部の形状に関しては任意である。なお、以上の説明でメモリカードとして説明したが、ハードディスクカード、ディスクカード等蓄積機能を備えるカードでも良い。なお、以上の説明でメモリカード２４を挿入するスロットを１個で説明しているが複数枚が挿入されるスロットで構成されていても良い。

【００３６】

図５は本発明の蓄積部１７で脱着可能なメモリカードのスロットに対してカバーを行う事でメモリカードの取り出しを不可能にする図であり、図５において（ａ）の２はターゲット、２４は脱着可能なメモリカード、４２はターゲット２に装着しているメモリカード２４に蓋をするためのカバー、４３はカバー４２を開ける場合に矢印の方向にスライドさせてカバー４２の開放の補助とカバー４２がはずれないように固定するスライド部を備えるモバイル機器において、（ｂ）の４４はカバー４２を固定する為のロックピン、（ｃ）の４５はカバー４２を固定する為の固定部、（ｄ）の３９は固定部４５の一部でターゲット２に装着している矢印形固定部、４０は固定部４５の一部でターゲット２に装着している矢印形固定部、４６はカバー３５の一部でカバー４２をターゲット２に固定する為の矢印形ロック部によって構成される。

【００３７】

以上のように構成された機器盗難防止通信システムのロック方法に関して、図５を用いてその動作を説明する。まず、（ａ）の動作としてカバー４２の上部を引っ張ってスライド部４３が矢印の方向にスライドすることによってターゲット２のメモリを格納するスロット部が見える為、メモリカードの挿入を行うことができる。このスライド部分にロック出来る仕組みを備えます。（ｂ）はスライド部４３とターゲット２との間にロックピン４４を装着できる構成にして、ロック指令がロック制御部１４から発行されるとロックピン４４でターゲット２とカバー４２は通常の開閉より優先して固定しスライドできないようにしてメモリカード２４の取り出しを不可能にする。（ｃ）はスライド部４３とターゲット２との間に固定部４５を設置しカバー４２の開閉を制御する。（ｄ）は（ｃ）の構造説明で通常は矢印形固定部３９と矢印形固定部４０を矢印のように移動させることによって矢印形ロック部４６を固定、解除を行ってカバー４２の開閉を行う。ロック指令がロック制御部１４から発行されると矢印形固定部３９と矢印形固定部４０が通常の開閉より優先して矢印形ロック部４６を固定してメモリカード２４の取り出しを不可能にする。なお、以上の説明で図（ｂ）のロックピン４４の位置を説明したが、カバー４２であればどの位置に設置しても良い。（ｄ）の矢印形固定部３９、矢印形固定部４０から構成される固定部３８とカバー３５に付随している矢印形ロック部４６によって固定するという説明をしたが、固定部の形状に関しては任意である。

【００３８】

なお、以上の説明でメモリカードとして説明したが、ハードディスクカード、ディスクカード等蓄積機能を備えるカードでも良い。なお、以上の説明でメモリカード２４を挿入するスロットを１個で説明しているが複数枚が挿入されるスロットで構成されていても良い。

【００３９】

図６は本発明の蓄積部１７で脱着可能なメモリカード自身にロックを行う事でメモリカードの取り出しを不可能にする図であり、図６において２はターゲット、２４は脱着可能なメモリカード、４７はメモリカード自身に備えているカード固定部、４８はメモリカードを固定するロックピンで構成されている。メモリスロットによってはカード固定部４７を利用してメモリカード２４の固定を行っている機器が存在したり、カード固定部４７を備えているにもかかわらず固定に使用していないメモリスロットもある。

【００４０】

以上のように構成された機器盗難防止通信システムのロック方法に関して、図６を用いてその動作を説明する。まず、ターゲット２にメモリカード２４が挿入された状態で、ロック指令がロック制御部１４から発行されるとロックピン４８がカード固定部４７に挿入され、メモリカード２４の取り出しを不可能にする。またカード固定部４７でメモリカード２４を固定している機器があった場合はロック指令がロック制御部１４から発行され事が優先される構成になってメモリカード２４の取り出しを不可能にする。以上の説明でカード固定部４７はメモリカードのどの部分に設置されていても良く、またカード固定部４７が複数存在しても良い。なお、以上の説明でメモリカードとして説明したが、ハードディスクカード、蓄積機能を備えるカードでも良い。

【００４１】

図７は本発明の蓄積部１７でモバイル機器に搭載されているハードディスクを機構的にロックさせる図であり、図７において（ａ）の２はターゲット、５０はハードディスク、５１はハードディスク５０に設置されておりターゲット２との間で固定を行うハードディスク固定部を備えるモバイル機器において、（ｂ）の５２はハードディスク固定部５１をターゲット２にロックさせる為のロックピン、（ｃ）の５３はハードディスク５０をターゲットから取り外し出来ないように固定する固定バー、（ｄ）の５４はハードディスク５０をターゲットから取り外し出来ないように固定する固定バー、（ｅ）の５５はハードディスク５０をターゲットから取り外し出来ないように固定する固定バー、５６はハードディスク５０をターゲットから取り外し出来ないように固定する固定バーで構成されている。

【００４２】
以上のように構成された機器盗難防止通信システムのロック方法に関して、図７を用いてその動作を説明する。まず、（ｂ）においてロック指令がロック制御部１４から発行されるとロックピン５２がハードディスク固定部５２に挿入され、ハードディスク５０の取り外しを不可能にする。（ｃ）においてロック指令がロック制御部１４から発行されると固定バー５３がハードディスク５０の取り出し部に設置されハードディスク５０の取り外しを不可能にする。（ｄ）においてロック指令がロック制御部１４から発行されると固定バー５４がハードディスク５０の取り出し部に設置されハードディスク５０の取り外しを不可能にする。（ｅ）においてロック指令がロック制御部１４から発行されると固定バー５５と固定バー５６がハードディスク５０の取り出し部に設置されハードディスク５０の取り外しを不可能にする。

【００４３】
なお、以上の説明で（ｂ）のロックピン５２に関して全ての位置に設置するように説明したが、ロックピンの数量に関しては任意でも良い。なお、以上の説明で（ｃ）の固定バー５３，（ｄ）の固定バー５４，（ｅ）の固定バー５５，５６に関して１本で説明したが、複数本備えても良いまたハードディスク５０とほぼ同等の大きさの鉄板で構成されても良い。なお、以上の説明でハードディスク５０を１個で説明しているが複数個のハードディスクでも良く、固定バーに関してもハードディスクの個数以上で構成されても良い。

【００４４】
以上のように本実施の形態によれば、所有者が携行物品にコントローラを内蔵または装着した送受信部と、所有者が鞄等に入れているターゲットに内蔵または装着した送受信部との間で短距離無線通信方式の通信をさせて送受信部間の距離を測定し、認証がとれている間に所有者がターゲットを操作して蓄積部のデータに変更を加えた場合にその更新データを蓄積していてコントローラに送受信部を介して転送を行いコントローラに蓄える。更新データはコントローラの更新されたデータの蓄積部の容量を少なくする為に蓄積部にある元データに対しての差分データでも良い。もしも盗難にあった場合でもターゲットの蓄積されたデータが会社にある場合、コントローラとの差分データと元データで復元を行うことが出来る。もしくは更新したデータを蓄積していてコントローラに送受信部を介して転送を行いコントローラに蓄える。もしも盗難にあった場合でもコントローラにある更新したデータに関しては所有者自身が身につけている為にセキュリティーとして安全である。また、コントローラの送受信部とターゲットの送受信部間で短距離無線通信方式の通信をさせ送受信部間の距離を測定し、一定距離以上になるか、または無線信号の通信が停止した場合にターゲットの機器動作を停止、蓄積メディアを機構的にロック、蓄積部のデータの消滅等を行う事によって盗難にあった場合にターゲットとしての価値を無くしセキュリティーの保護及び機器の不正販売を防止するという効果を得ることができる。

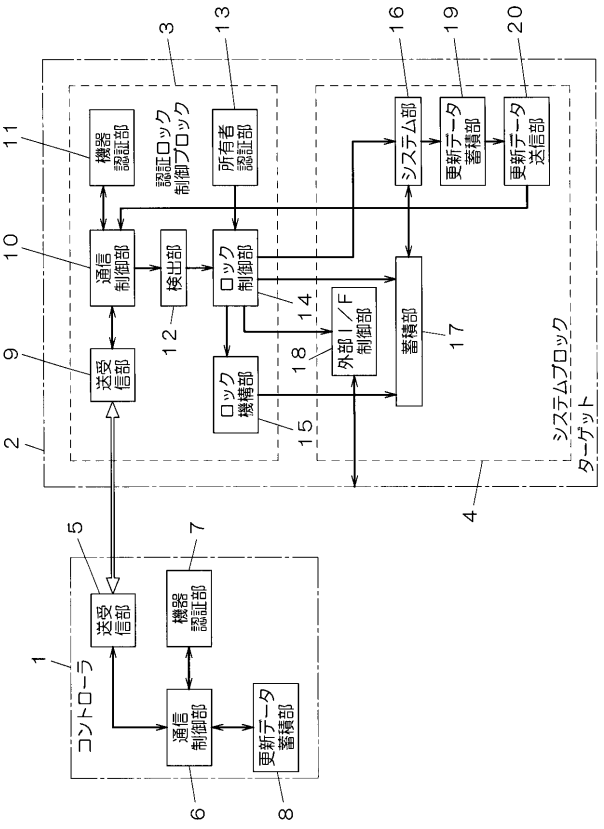
【産業上の利用可能性】
【００４５】
本発明は、コントローラとターゲットとで通信を行い、両者が所定距離離れたことで、ターゲットを動作不能にするものであり、携帯機器やモバイル機器などので、様々な応用例が考えられる。

【図面の簡単な説明】
【００４６】
【図１】本発明の実施の形態１における機器盗難防止通信システムのブロック図
【図２】同実施の形態１における機器盗難防止通信システムの脱着可能なメモリカードを機構的にロックさせる為の構成図
【図３】同実施の形態１における機器盗難防止通信システムの脱着可能なメモリカードを機構的にロックさせる為の構成図
【図４】同実施の形態１における機器盗難防止通信システムの脱着可能なメモリカードのスロットにカバーをしてメモリカードの取り出しを不可能にする構成図
【図５】同実施の形態１における機器盗難防止通信システムの脱着可能なメモリカードの

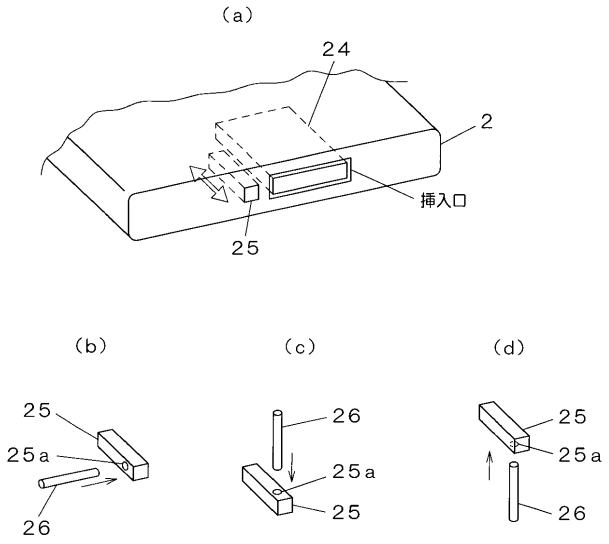
スロットにカバーをしてメモリカードの取り出しを不可能にする構成図
【図６】同実施の形態１における機器盗難防止通信システムの脱着可能なメモリカード自身にロックを行う事でメモリカードの取り出しを不可能にする構成図
【図７】同実施の形態１における機器盗難防止通信システムのハードディスクを機構的にロックさせる構成図
【図８】従来の盗難防止システムのブロック図
【符号の説明】
【００４７】
１　コントローラ
２　ターゲット
３　認証ロック制御ブロック
４　システムブロック
５　送受信部
６　通信制御部
７　機器認証部
８　更新データ蓄積部
９　送受信部
１０　通信制御部
１１　機器認証部
１２　検出部
１３　所有者認証部
１４　ロック制御部
１５　ロック機構部
１６　システム部
１７　蓄積部
１８　外部Ｉ／Ｆ制御部
１９　更新データ蓄積部
２０　更新データ送信部
２４　メモリカード
２５　プッシュ形取り出しピン
２６　ロックピン
２７　取り出しピン
２８　格納レバー
２９　回転軸
３０　ロックピン
３１　ロックピン
３５　カバー
３６　回転軸
３７　ロックピン
３８　固定部
３９　矢印形固定部
４０　矢印形固定部
４１　矢印形ロック部
４２　カバー
４３　スライド部
４４　ロックピン
４５　固定部
４６　矢印形ロック部
４７　カード固定部
４８　ロックピン

５０　ハードディスク
５１　固定部
５２　ロックピン
５３　固定バー
５４　固定バー
５５　固定バー
５６　固定バー

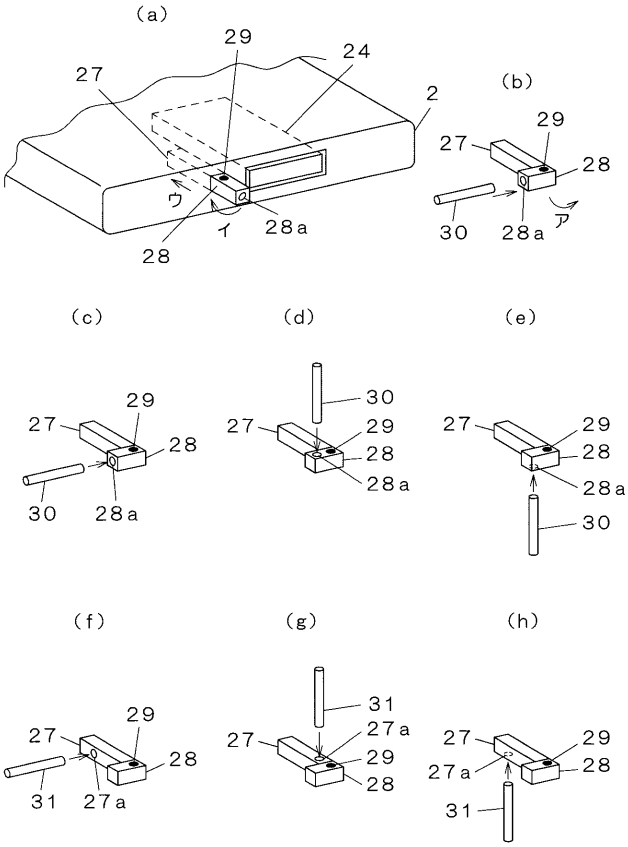
【図１】



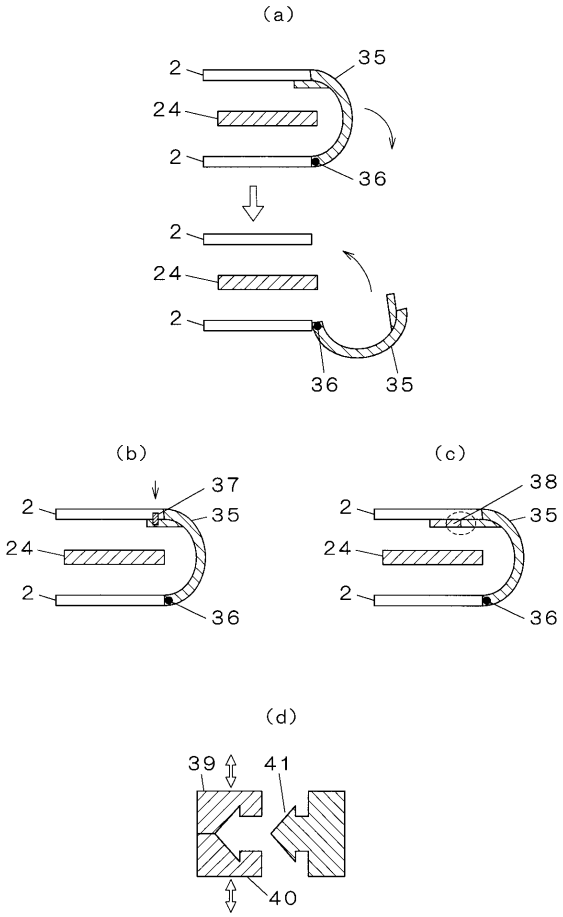
【図２】



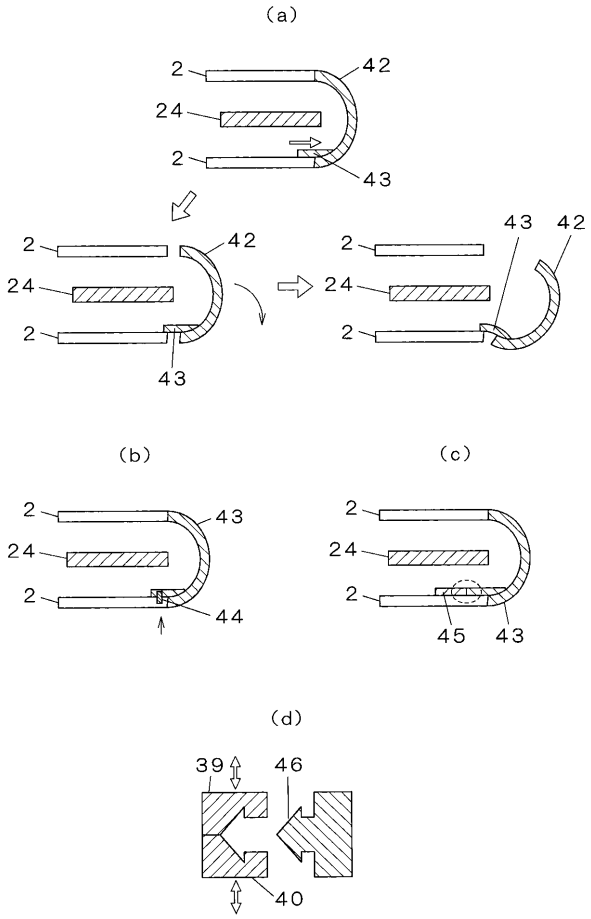
【図３】


(a)
29
24
27
2
ウ
イ
28a
28
(b)
29
27
28
30
28a
ア
(c)
(d)
(e)
(f)
(g)
(h)
31
27a

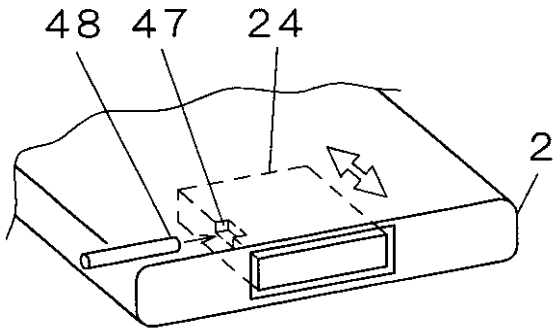
【図４】


(a)
2
35
24
36
(b)
37
(c)
38
(d)
39
41
40

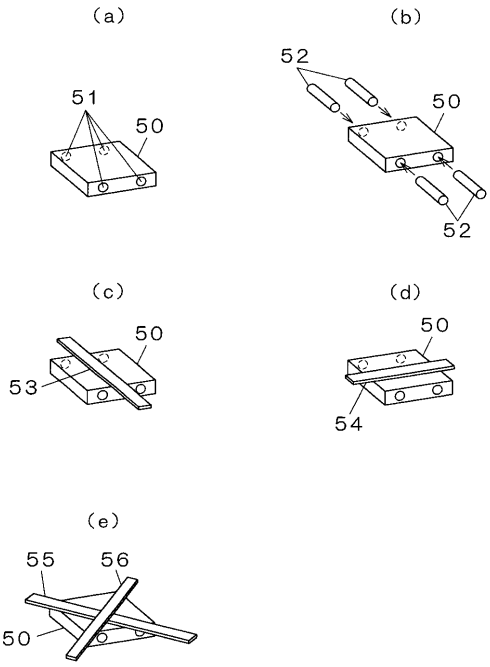
【図５】


(a)
2
42
24
43
(b)
44
(c)
45
(d)
39
46
40

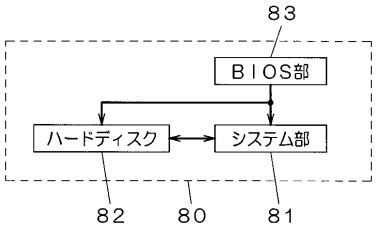
【図６】


48
47
24
2

【図７】


(a)
51
50
(b)
52
50
52
(c)
50
53
(d)
50
54
(e)
55
56
50

【図８】


83
BIOS部
ハードディスク
システム部
82
80
81