(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2004-362366
(P2004-362366A)
(43)公開日　平成16年12月24日(2004.12.24)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G06F 1/00	G06F 1/00	370E	5B017
G06F 12/14	G06F 12/14	320D	5B058
G06K 17/00	G06K 17/00	E	5K023
H04M 1/00	H04M 1/00	U	5K027
H04M 1/02	H04M 1/02	C	

審査請求 未請求　請求項の数 9　ＯＬ　（全 14 頁）

(21)出願番号　特願2003-161468(P2003-161468)
(22)出願日　平成15年6月6日(2003.6.6)

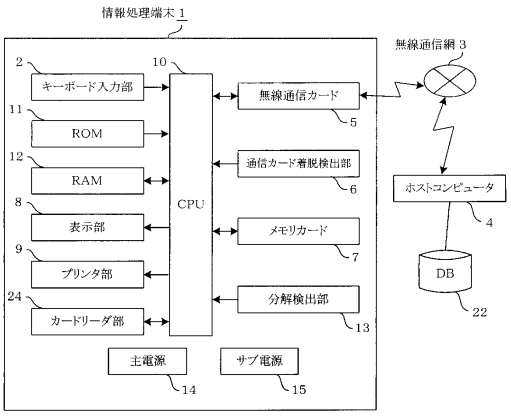
(71)出願人　000104652
キヤノン電子株式会社
埼玉県秩父市大字下影森１２４８番地
(74)代理人　100075292
弁理士　加藤　卓
(72)発明者　切手　直人
埼玉県秩父市大字下影森１２４８番地　キヤノン電子株式会社内

Ｆターム(参考)　5B017 AA03 BA08 CA14
5B058 CA04 CA27 KA31
5K023 AA07 BB02 BB23 DD06 LL06
MM25 NN06 PP01 PP12
5K027 AA11 BB09 CC08 FF22 GG01

(54)【発明の名称】情報処理端末、その制御方法、及びその制御プログラム

(57)【要約】
【課題】無線通信カードとデータの記憶手段を着脱可能に装着して使用する情報処理端末において、簡単な構成で、記憶手段の記憶データが第三者に不正に読み取られることを防止する。
【解決手段】メモリカード７と無線通信カード５が装着された状態で無線通信カード５を取り外さないとメモリカード７が取り外せないようになっている。また、キーボード入力部２からの所定の情報の入力に応じて、端末１の正規の使用者の認証を行なうためのホストコンピュータ４との通信を無線通信カード５により行なう。そして、無線通信カード５の取り外しが検出部６で検出されたときに、その前に前記の通信で使用者が正規の使用者と認証されていない場合、ＣＰＵ１０がメモリカード７の記憶データを閲覧不可能になるように処理する。
【選択図】　図１

（図１）



【特許請求の範囲】
【請求項１】
データを記憶する不揮発性の記憶手段と、無線通信を行なう無線通信カードを着脱可能に装着して使用する情報処理端末において、
情報処理端末に前記記憶手段と無線通信カードが装着された状態で無線通信カードを取り外さないと記憶手段を取り外せないように構成されており、
情報処理端末の使用者が情報を入力するための入力手段と、
該入力手段からの所定の情報の入力に応じて、情報処理端末の正規の使用者の認証を行なうための外部との通信を前記無線通信カードにより行なうように制御する制御手段と、
前記無線通信カードの取り外しを検出する検出手段と、
該検出手段により前記無線通信カードの取り外しが検出されたときに、その前に前記外部との通信で使用者が正規の使用者と認証されていない場合、前記記憶手段の記憶データを閲覧不可能になるように処理する処理手段を有することを特徴とする情報処理端末。
【請求項２】
情報処理端末の筐体の分解を検出する分解検出手段と、
該分解検出手段により前記筐体の分解が検出されたときに、前記記憶手段の記憶データを閲覧不可能になるように処理する処理手段を有することを特徴とする請求項１に記載の情報処理端末。
【請求項３】
前記分解検出手段により前記筐体の分解が検出されたときに、前記処理手段の処理の前に、前記筐体の分解を通知する情報と前記記憶手段の記憶データを前記無線通信カードにより外部に送信するように制御する制御手段を有することを特徴とする請求項２に記載の情報処理端末。
【請求項４】
情報処理端末の不正使用を検出する不正使用検出手段と、
該不正使用検出手段により情報処理端末の不正使用が検出されたときに、前記記憶手段の記憶データを閲覧不可能になるように処理する処理手段を有することを特徴とする請求項１に記載の情報処理端末。
【請求項５】
前記不正使用検出手段により情報処理端末の不正使用が検出されたときに、前記処理手段の処理の前に、情報処理端末の不正使用を通知する情報と前記記憶手段の記憶データを前記無線通信カードにより外部に送信するように制御する制御手段を有することを特徴とする請求項４に記載の情報処理端末。
【請求項６】
前記記憶手段を着脱可能に装着する第１のコネクタと、前記無線通信カードを着脱可能に装着する第２のコネクタを有し、該第１と第２のコネクタのそれぞれに前記記憶手段と無線通信カードが装着された状態で、無線通信カードを取り外さないと記憶手段を取り外せないように、無線通信カードと第２のコネクタがブロックするように構成されたことを特徴とする請求項１から５までのいずれか１項に記載の情報処理端末。
【請求項７】
少なくとも前記記憶手段と無線通信カードを着脱可能に装着する一体のコネクタを有し、該コネクタに前記記憶手段と無線通信カードが装着された状態で、無線通信カードを取り外さないと記憶手段を取り外せないように、無線通信カードとコネクタがブロックするように構成されたことを特徴とする請求項１から５までのいずれか１項に記載の情報処理端末。
【請求項８】
データを記憶する不揮発性の記憶手段と、無線通信を行なう無線通信カードを着脱可能に装着して使用する情報処理端末であって、前記記憶手段と無線通信カードが装着された状態で無線通信カードを取り外さないと記憶手段を取り外せないように構成された情報処理端末の制御方法であって、

情報処理端末の使用者からの所定の情報の入力に応じて、情報処理端末の正規の使用者の認証を行なうための外部との通信を前記無線通信カードにより行なう通信工程と、
前記無線通信カードの取り外しを検出する検出工程と、
該検出工程で前記無線通信カードの取り外しが検出されたときに、その前に前記通信工程で使用者が正規の使用者と認証されていない場合、前記記憶手段の記憶データを閲覧不可能になるように処理する処理工程を行なうように制御することを特徴とする情報処理端末の制御方法。
【請求項９】
データを記憶する不揮発性の記憶手段と、無線通信を行なう無線通信カードを着脱可能に装着して使用する情報処理端末であって、前記記憶手段と無線通信カードが装着された状態で無線通信カードを取り外さないと記憶手段を取り外せないように構成された情報処理端末の制御プログラムであって、
情報処理端末の使用者からの所定の情報の入力に応じて、情報処理端末の正規の使用者の認証を行なうための外部との通信を前記無線通信カードにより行なう通信工程と、
前記無線通信カードの取り外しを検出する検出工程と、
該検出工程で前記無線通信カードの取り外しが検出されたときに、その前に前記通信工程で使用者が正規の使用者と認証されていない場合、前記記憶手段の記憶データを閲覧不可能になるように処理する処理工程を行なうための制御手順を含むことを特徴とする情報処理端末の制御プログラム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、データを記憶する不揮発性のメモリカードなどの記憶手段と、無線通信を行なう無線通信カードを着脱可能に装着して使用する情報処理端末、その制御方法、及びその制御プログラムに関するものである。
【０００２】
【従来の技術】
従来、情報処理端末に無線通信機能を搭載するために、端末に設けられたＰＣカードスロットやＣＦカードスロット等のカードスロットに、ＰＨＳカード、パケット通信カード、無線ＬＡＮカード等の無線通信カードを装着するといった手段が多用されており、これにより複数種類の移動通信網を利用して無線通信を行なうことができる。また、近年さらなる小型化が進んでいるメモリカード等の着脱可能な記憶手段を用いることで、他の装置とのデータ交換を行うことができ、端末の故障時でも被害を受け難くなり、記憶容量の変更も容易に行なえる。
【０００３】
このような無線通信カードと記憶手段を用いる情報処理端末として例えば携帯型カード決済端末があり、クレジットカードやデビットカード等の決済に必要な各種のデータを無線で送受信する。端末から発せられた電波は各地に設置された無線基地局で受信される。無線基地局は各種のネットワークを経由して最終的に銀行やクレジットカード会社等のホストコンピュータに接続される。そのため、この種の携帯型カード決済端末は、大規模店舗内の移動での使用は勿論のこと、屋外で自由に持ち歩いて使用することもでき、例えばセールスマンによる訪問販売等に使用することもできる。しかし、その一方で置き忘れや盗難等により第三者の手に渡り、記憶手段に記憶された個人情報などのデータを不正に読み取られて悪用される可能性が高くなる。
【０００４】
そこで、このような端末の不正使用対策として、例えば端末の筐体がこじ開けられた場合に端末内部の検知スイッチによりそれを検知して、記憶データを消去、改変、もしくは暗号化処理する方法が提案されている。例えば、下記の特許文献１には、携帯型カード決済端末（クレジットカード認証端末）において、本体ケースの不正分解を検出スイッチにより検出し、その信号に応じてメモリのデータを消去すると共に、端末ＩＤと不正分解情報

を中央データ処理センターへ送信する構成が記載されている。
【０００５】
また、下記の特許文献２には、電子機器に着脱可能に実装される記憶装置において、記憶データを不正アクセスや盗難等から防御するために、電子機器からの抜き取りを検出する抜取センサと、これが抜き取りを検出した場合にデータの全部または一部を消去ないし破壊するデータ消去装置を有する構成が記載されている。
【０００６】
また、下記の特許文献３には、ＩＣカード（メモリモジュール）を着脱可能な無線端末において、ＩＣカードの不正アクセスを防止するために、ＩＣユーザがＩＣカードの取外しを要求する場合にユーザの認証を行ない、ＯＫとならない限りカードロック機構部によりＩＣカードをロックする構成が記載されている。
【０００７】
【特許文献１】
特開２０００－２９８７５５号公報
【特許文献２】
特開２００２－１８９６３５号公報
【特許文献３】
特開２００２－９９２１号公報
【０００８】
【発明が解決しようとする課題】
ところが、情報処理端末で重要なデータを記憶する記憶手段として一般のＣＦカードやＳＤカード等のメモリカードを用いる場合、これらのメモリカードの端末からの取り外しは制限されておらず、このためメモリカードへの不正アクセスを確実に防止することができないという問題がある。
【０００９】
すなわち、端末の本体ケースの不正分解を検出する特許文献１の構成でも、メモリが取り外しを制限されないメモリカードで本体ケースを分解せずに取り外せるものならば、不正アクセスを防止できない。
【００１０】
これに対して、特許文献２に記載された記憶装置の構成では、取り外し（抜き取り）による不正アクセスを防止することはできるが、特別なセキュリティ機能のための構成を有するため、これに対応する情報処理端末などの機器が限られるので、この記憶装置を使用している機器から他の機器に差し替えて使用するようなことが制限されてしまうことになる。この点を考慮すると、セキュリティ機能は機器側に持たせることが望ましい。
【００１１】
また、特許文献３の構成では、ＩＣカードの不正アクセスのための取り外しを完全に阻止するためには複雑なカードロック機構部が必要となる。
【００１２】
そこで、本発明の課題は、無線通信カードとメモリカードなどの記憶手段を着脱可能に装着して使用する情報処理端末において、簡単な構成により、前記記憶手段の記憶データが第三者により不正に読み取られて悪用されることを確実に防止できるようにすることにある。
【００１３】
【課題を解決するための手段】
上記の課題を解決するため、本発明によれば、
データを記憶する不揮発性の記憶手段と、無線通信を行なう無線通信カードを着脱可能に装着して使用する情報処理端末において、
情報処理端末に前記記憶手段と無線通信カードが装着された状態で無線通信カードを取り外さないと記憶手段を取り外せないように構成されており、
情報処理端末の使用者が情報を入力するための入力手段と、

該入力手段からの所定の情報の入力に応じて、情報処理端末の正規の使用者の認証を行なうための外部との通信を前記無線通信カードにより行なうように制御する制御手段と、
前記無線通信カードの取り外しを検出する検出手段と、
該検出手段により前記無線通信カードの取り外しが検出されたときに、その前に前記外部との通信で使用者が正規の使用者と認証されていない場合、前記記憶手段の記憶データを閲覧不可能になるように処理する処理手段を有する構成を採用した。

【００１４】

【発明の実施の形態】

以下、図を参照して本発明の実施の形態を説明する。

【００１５】

［第１の実施形態］

図１は本発明の第１の実施形態による情報処理端末の構成を示すブロック図である。なお、本実施形態の情報処理端末（以下、端末と略す）１は、利用者の個人情報や顧客の電話番号及び銀行の口座番号等の機密データをメモリカードに記憶するものとする。

【００１６】

図１において、２は端末１の使用者が操作して端末１に情報を入力するためのキーボード入力部である。

【００１７】

５は、無線通信網３を介してホストコンピュータ４等の外部装置と無線通信を行なうための無線通信装置としての着脱可能な無線通信カードであり、例えばＰＣＭＣＩＡに準拠する形状及びピン配列を持つＰＣカードやＣＦカードｔｙｐｅＩＩ等のカードとする。この無線通信カード５は、後述する図２～図４に示すように端末１の筐体２６内のプリント基板１７上に設けられたカードコネクタ１６に着脱可能に装着、接続されて使用される。

【００１８】

６は、無線通信カード５のカードコネクタ１６に対する着脱を検出する通信カード着脱検出部である。

【００１９】

７は、データを記憶する記憶手段としての不揮発性のメモリカードであり、本実施形態では、上述した個人情報などの重要な機密データを記憶させるものとする。このメモリカード７は、後述する図２～図４に示すように端末１の筐体２６内のプリント基板１７上に設けられたカードコネクタ２５に着脱可能に装着、接続されて使用される。

【００２０】

８は、キーボード入力部２から入力された情報や、無線通信カード５で受信した情報など各種情報を表示する表示部である。

【００２１】

９は、ロール紙などの印刷用紙に文字などを印刷するプリンタ部である。

【００２２】

１０は、各種演算処理、情報処理を行い、端末１の各部の動作全体を統括制御するＣＰＵである。

【００２３】

１１はＣＰＵ１０が実行する制御プログラム等のデータを格納するＲＯＭ１１、１２はワークエリアとしてデータの一時的な格納などに使用されるＲＡＭである。

【００２４】

１３は、端末１の筐体２６の分解を検出する分解検出部であり、例えば押釦スイッチを用い、筐体２６が不正に分解されて開けられると押釦スイッチが開放され、ＣＰＵ１０に不正分解があったことを信号で知らせる。これに応じてＣＰＵ１０はメモリカード７の記憶データを消去、改変、ないしは暗号化するなど閲覧不可能になるように処理する。

【００２５】

１４は主電源、１５はサブ電源である。主電源１４は、端末１の通常の使用時に電源を供給する。サブ電源１５は、通信カード着脱検出部６により無線通信カード５のカードコネ

クタ１６からの取り外しが検出されたとき、あるいは分解検出部１３により筐体２６の分解が検出されたときに、主電源１４が端末１から外されていた場合、端末１を駆動するために電源を供給する。このサブ電源１５は、筐体２６を分解しないと取り出せないように、筐体２６に内蔵する。こうすることで、筐体２６が分解されたときに、確実に電源供給が行なわれ、分解検出以後の動作を確実に行なうことができる。また、サブ電源１５は二次電池とし、主電源１４が装着されているときは、主電源１４により適宜充電されるものとする。

【００２６】

また、２２は、ホストコンピュータ４がアクセス可能なデータベースであり、このデータベースには、本実施形態の端末１を含めてホストコンピュータ４と通信を行なう複数の端末のそれぞれの固有のＩＤ番号とパスワードなどの情報のデータが含まれている。

【００２７】

なお、２４は、カードリーダ部であり、便宜上この図１に示してあるが、実際は本実施形態ではなく、後述する第３の実施形態の端末で設けられる。

【００２８】

次に、図２は端末１で無線通信カード５とメモリカード７が装着、接続されるカードコネクタ１６と２５を示す平面図、図３はカードコネクタ１６に対する無線通信カード５の着脱の様子を示す斜視図、図４は図２のＡ－Ａ線に沿った断面図である。

【００２９】

これらの図に示すように、プリント基板１７上にカードコネクタ１６が実装されており、その内側でプリント基板１７上にカードコネクタ２５が実装されている。また、図３に示すように端末１の筐体２６においてカードコネクタ１６部上の位置に蓋２７が設けられており、これを開けてメモリカード７がカードコネクタ２５に対して図２中で矢印ｂ，ｂ′方向に着脱可能に装着され、電気的に接続される。また、無線通信カード５がメモリカード７上でカードコネクタ１６に対して矢印ａ，ａ′方向に着脱可能に装着され、電気的に接続される。

【００３０】

ここで、カードコネクタ１６と無線通信カード５は、無線通信カード５とメモリカード７をカードコネクタ１６と２５に装着した状態で、無線通信カード５を取り外さないとメモリカード７を取り外せないようにブロックする物理的保護手段（ブロック手段）として構成されている。

【００３１】

すなわち、カードコネクタ１６は、プリント基板１７上で無線通信カード５をメモリカード７より僅かに上の高さに装着するために高さ方向に所定のスタンドオフ（かさ上げ）値を有している。また、カードコネクタ１６は、無線通信カード５を機械的に着脱可能に結合する結合部１８と、無線通信カード５を着脱するａ，ａ′方向に沿って案内する溝が形成された左右両側のガイド部２０，２０を有しているとともに、ガイド部２０，２０のそれぞれの結合部１８と反対側の端部間で下側に取り出し防止用の防御壁部１９が形成されており、これらが全体として長方形の枠状に形成され、プリント基板１７上でカードコネクタ２５に装着されたメモリカード７の四方を囲むように配置される。

【００３２】

また、無線通信カード５は、その取り外し方向側の端部に設けられたアンテナ部５ａの厚さが他の部分より大きく、その厚さの差の部分が装着時に下側（プリント基板１７側）となる向きに突出している。そして、図２及び図４に示すように無線通信カード５をカードコネクタ１６に装着すると、無線通信カード５がメモリカード７を覆い、自らとプリント基板１７の間に挟み込み、取り外せないように本体とアンテナ部５ａで上側と取り出し方向側をブロックするようになっている。

【００３３】

なおメモリカード７は、上記のように無線通信カード５とカードコネクタ１６で取り外せないようにブロックするために、外形が無線通信カード５より小さな例えばＳＤ／ＭＭＣ

カード等の小型のメモリカードを用いる。このようなメモリカード７をユーザファイルメモリ領域として利用すれば、万一端末１が故障してもメモリカード７を代替機に差し替えることが可能で、他の装置へのデータの受け渡しや記憶容量の変更も容易となるという利点がある。

【００３４】

次に、図５は、通信カード着脱検出部６の具体例を示している。ここでは、通信カード着脱検出部６として、カード挿抜（着脱）検出スイッチ２１をカードコネクタ１６の左右のガイド部２０の通信カード結合部１８近傍に設けてあり、無線通信カード５がカードコネクタ１６から引き抜かれると、スイッチ２１のバネ２１ａが開放されることでスイッチ２１がオフしてカード５の取り外しが検知される。そして、後述のようにＣＰＵ１０及びメモリカード７を動作させることができるように主電源１４またはサブ電源１５から電源が供給されることとなる。

【００３５】

ここで、カード挿抜検出スイッチ２１としてコネクタ１６のピンＰの内でカードディテクト用のピンを利用しても構わないが、この場合は電源部が端末１の電源オフ時を含めて常時微弱電流を流し、そのピンのカードディテクト機能を動作させておく必要がある。

【００３６】

以上の構成からなる本実施形態の端末１では、これを盗む或いは拾うなどした第三者がメモリカード７を取り外してその記憶データを不正に読み取ることを防止するために、メモリカード７の取り外しのために必要な無線通信カード５の取り外しを検出すると、メモリカード７の記憶データを消去、変更あるいは暗号化処理するなどして閲覧不可能にする。ただし、無線通信カード５の取り外し時に、端末１の使用者が正規の使用者であると認証されていてメモリカード７の取り外しが許可されている場合は、上記の閲覧不可能にする処理を行なわない。これは、正規の使用者がメモリカード７の記憶データを端末１以外の機器で利用するなどのためにメモリカード７を取り外すことができるようにするためである。

【００３７】

使用者の認証は、無線通信カード５によるホストコンピュータ４との無線通信で行なう。その処理は、図６のフローチャートに示す手順で以下のように行なわれる。

【００３８】

まず、ステップＳ１で端末１の使用者がキーボード入力部２の操作によりメモリカード７の取り外しの許可の要求と、認証のための例えば端末１の固有のＩＤ番号とパスワードなどの情報を入力し、その入力に応じてＣＰＵ１０が無線通信カード５を制御し、前記の入力された情報をホストコンピュータ４に送信させる。

【００３９】

その情報を受信したホストコンピュータ４は、ステップＳ２でデータベース２２にアクセスし、上記許可要求を受けた端末の固有ＩＤ番号とパスワードなどの情報を抽出し、それぞれ受信した情報と一致するか否か照合する。

【００４０】

そして、ステップＳ３で上記照合の結果として一致するか否かにより使用者を正規の使用者と認証するか否か判断する。そして、一致せず認証しない場合はステップＳ４でメモリカード取り外しの不許可情報を端末１へ送信する。これを受信した端末１では、ＣＰＵ１０の制御により、表示部８にメモリカードの取り外しが不許可である旨が表示される。

【００４１】

また、ステップＳ３で照合の結果として一致し、使用者が正規の使用者であると認証した場合はステップＳ５で１回のメモリカードの取り外しを許可する許可情報を端末１に送信する。これを受信した端末１では、ＣＰＵ１０の制御により前記の許可情報がＲＡＭ１２に記憶され、これにより無線通信カード５を取り外してメモリカード７を取り外せる状態になる。すなわち、無線通信カード５を取り外してもメモリカード７の記憶データを閲覧不可能にする処理が行なわれない状態になる。なお、その後、ＣＰＵ１０は、所定時間が

経過しても無線通信カード５の取り外しが検知されない場合はタイムアウトとしてＲＡＭ１２に記憶していた上記の許可情報を無効化（消去）する処理を行う。

【００４２】

次に、図７は端末１で無線通信カード５が取り外されたときにメモリカード７に対する不正アクセスを防止するために行なわれるセキュリティ処理の手順を示すフローチャートである。

【００４３】

まず、ステップＳ６で端末１の使用者（本来の正規の使用者または不正アクセスを行なおうとする悪意のある第３者）が端末１からメモリカード７を取り外そうとして、その前に無線通信カード５を取り外すと、ステップＳ７でカード挿抜検出スイッチ２１がオフして無線通信カード５の取り外しが検出される。

【００４４】

それに応じて主電源１４から（主電源１４が外されていた場合はサブ電源１５から）ＣＰＵ１０へ電源が供給され、ＣＰＵ１０はステップＳ８で前述したメモリカード取り外しの許可情報がＲＡＭ１２に記憶されているか否か調べる。

【００４５】

そして、許可情報が記憶されていない場合はステップＳ９で不正な取り外しと判断してメモリカード７の記憶データを消去、変更あるいは暗号化するなどして閲覧不可能にし、その後、処理を終了する。

【００４６】

また、ステップＳ８で許可情報が記憶されている場合は、そのまま処理を終了する。すなわち、この場合は、正当な取り外しと判断してメモリカード７の記憶データを閲覧不可能にする処理は行わない。

【００４７】

以上のように無線通信カード５が取り外されたときにセキュリティ処理が行なわれるとともに、端末１の筐体２６が不正に分解されたときには、前述した分解検出部１３がそれを検出し、その信号に応じてＣＰＵ１０がメモリカード７の記憶データを閲覧不可能になるように処理するセキュリティ処理が行なわれる。

【００４８】

以上のような本実施形態の端末１によれば、無線通信カード５を取り外さないとメモリカード７を取り外せず、無線通信カード５を取り外すと図７のセキュリティ処理が行なわれ、その前に無線通信カード５による無線通信で使用者が認証されていない場合は、メモリカード７の記憶データが閲覧不可能になるように処理される。

【００４９】

従って端末１を盗む或いは拾うなどした第三者がメモリカード７を取り外して記憶データを不正に読み取ろうとする場合、使用者の認証に必要な端末のＩＤ番号とパスワードなどの情報を知っていて認証を行なわない限り、無線通信カード５を取り外してメモリカード７を取り外すと、既にその記憶データが閲覧不可能に処理されていることになるので、記憶データの不正な読み取りを確実に防止することができる。

【００５０】

また、第三者がメモリカード７を取り外さずに、端末１の筐体２６を分解してメモリカード７の記憶データを読み取ろうとした場合は、その分解が分解検出部１３により検出されて記憶データが閲覧不可能に処理されるので、この場合も不正な読み取りを確実に防止することができる。

【００５１】

しかも、本実施形態の端末１では、特許文献３の場合のようにメモリカードを取り外せないようにロックする複雑なロック機構を必要とせず、簡単な構成で安価なものにすることができる。

【００５２】

また、メモリカード７として着脱可能で汎用のものを用いることができるので、他の機器

へ差し替えて記憶データを移し替えるような作業も容易に行なえ、端末１の故障などにも対応できる。また、無線通信カード５も着脱可能であるので、無線通信カード５を複数種類のものに差し替えることにより、複数種類の通信規格に対応可能である。

【００５３】

［第２の実施形態］

次に、本発明の第２の実施形態を説明する。本実施形態では、先述した第１の実施形態の構成において、カードコネクタ１６の代わりに、図８の平面図、及びそのＢ－Ｂ線断面図である図９に示すように、２枚のカードを上下に装着する２段式のカードコネクタ２３を用いる。

【００５４】

このカードコネクタ２３は、上下２段のスロットを有しており、その上段スロットに、無線通信カード５として、例えばＣＦカードに準拠したコネクタ形状及びピン配列としたＣＦカードタイプのカードを図８中で矢印ａ，ａ´方向に着脱可能に装着し、下段スロットに、メモリカード７として例えばＣＦカードよりも外形の小さいＳＤカードを同じくａ，ａ´方向に着脱可能に装着する。無線通信カード５は、第１の実施形態と同様にアンテナ部５ａの厚みが大きくなっているものが望ましい。

【００５５】

これにより、カードコネクタ２３にメモリカード７と無線通信カード５を装着した状態で、無線通信カード５を取り外さないとメモリカード７が取り外せないように無線通信カード５とカードコネクタ２３がブロックすることになる。

【００５６】

なお、第１の実施形態のカードコネクタ１６の防御壁部１９に相当するものをカードコネクタ２３に設けてもよい。また、カードコネクタ２３にメモリカード７と無線通信カード５を装着した状態で、無線通信カード５を取り外さないとメモリカード７が取り外せないようにブロックされる構造であれば、メモリカード７と無線通信カード５として互いに外形の大きさが同じものが装着されるものとしてもよい。また、カードコネクタ２３を３枚以上のカードを上下に装着する３段以上の多段式のコネクタとしてもよい。

【００５７】

このような本実施形態によれば、第１の実施形態に比べてカードコネクタが１つ少なくて済み、端末１の部品点数を減らし、組み立て工程を簡単にすることができる。

【００５８】

［第３の実施形態］

次に、本発明の第３の実施形態を説明する。本実施形態の端末は、携帯型カード決済端末とし、そのハードウェアの構成は、第１の実施形態の図１に示した端末１の構成でカードリーダ部２４を設けたものとする。カードリーダ部２４は、磁気カードやＩＣカードからなるクレジットカードやデビットカード等に書き込まれたデータを読み取るリーダライタとして構成される。このカードリーダ部２４で読み取ったクレジットカードなどの機密データをメモリカード７に記憶するものとする。

【００５９】

そして、本実施形態の端末１では、第１の実施形態の図６及び図７で説明した使用者の認証による無線通信カード取り外し時のセキュリティ動作を同様に行なうとともに、端末を盗んだ或いは拾った第三者が端末１の筐体２６を分解してメモリカード７の記憶データを不正に読み取ることを防止するために、図１０のフローチャートに手順を示すセキュリティ動作を以下のように行なう。

【００６０】

すなわち、まず筐体２６が分解されると、ステップＳ１１で分解検出部１３が分解を検出し、それに応じて主電源１４から（主電源１４が外されている場合はサブ電源１５から）ＣＰＵ１０へ電源が供給され、分解検出部１３からＣＰＵ１０に不正分解があったことを知らせる信号が入力される。

【００６１】

それに応じてＣＰＵ１０は、ステップＳ１２で無線通信カード５による無線通信が可能か否かを判断し、可能ならば、ステップＳ１３でカード会社や銀行等のホストコンピュータ４に対して、端末１の筐体２６が不正に分解されたことを通知する不正分解情報として、不正分解と端末１のＩＤ、時刻、及び位置等の情報を無線通信カード５により送信する。

【００６２】

これによりホストコンピュータ４はどの端末が不正分解されたかを即座にオンラインで把握して対処できるようになり、盗難端末を用いたクレジットカード等によるオンライン決済もできなくなる。

【００６３】

また、ステップＳ１３に続いてステップＳ１４でメモリカード７に記憶された所定の重要データ（全データでもよい）を予め指定された送信先（ホストコンピュータ４でもよい）へ送信させる。これにより重要データを失うことなく指定された送信先へ移動させ、後で利用することができる。

【００６４】

ステップＳ１４の後、あるいはステップＳ１２で無線通信が不可能であった場合、ＣＰＵ１０はステップＳ１５でメモリカード７の記憶データを消去するなどして閲覧不可能にした後、端末の動作を停止し端末の使用を不可能にし、処理を終了する。

【００６５】

以上のような本実施形態によれば、第三者がメモリカード７の記憶データを不正に読み取ろうとして筐体２６を分解した場合、無線通信が可能であれば、不正分解情報とメモリカード７の重要データをホストコンピュータ４と予め指定された送信先へ送信するので、ホストコンピュータ４が端末１の不正分解を把握して対処できるとともに、重要データが失われることがない。また、無線通信が可能な場合も、不可能な場合（第三者が上記の送信を妨害しようとして無線通信カード５を取り外す、ないしは取り外さないで壊した場合）もメモリカード７の記憶データを消去するなどして閲覧不可能にするので、不正な読み取りを防止することができる。

【００６６】

なお、本実施形態では、端末１の筐体２６の分解を検出して図１０の処理を行なうものとしたが、第三者による端末１の不正使用を検出して図１０と同様の処理を行なうようにしてもよい。不正使用の検出方法としては、例えば端末１の起動時などのパスワードの入力時において複数回の誤入力があった場合に不正操作であり不正使用であると検出する。そして、図１０と同様の処理を行なうが、その場合にステップＳ１１の「筐体の分解の検出」を「端末の不正使用の検出」に置き換えるとともに、ステップＳ１３の「不正分解情報の送信」を「端末の不正使用を通知する情報の送信」に置き換える。

【００６７】

また、筐体２６の分解の検出に応じた処理と、不正使用の検出に応じた処理を共に行なうようにしてもよい。

【００６８】

なお、上述した第１と第３の実施形態で図６，図７，図１０の処理における動作を含むＣＰＵ１０の動作はＣＰＵ１０が実行するＲＯＭ１１に格納された制御プログラムに従って行なわれる。すなわち、ＣＰＵ１０の本発明に係る機能は、その制御プログラムにより実現されることは勿論である。

【００６９】

【発明の効果】

以上の説明から明らかなように、本発明によれば、データを記憶する不揮発性の記憶手段と、無線通信を行なう無線通信カードを着脱可能に装着して使用する情報処理端末において、情報処理端末に前記記憶手段と無線通信カードが装着された状態で無線通信カードを取り外さないと記憶手段を取り外せないようにし、さらに、使用者からの所定の情報の入力に応じて、情報処理端末の正規の使用者の認証を行なうための外部との通信を無線通信カードにより行なうようにし、無線通信カードの取り外しが検出されたときに、その前に

前記の通信で使用者が正規の使用者と認証されていない場合、前記記憶手段の記憶データを閲覧不可能になるように処理するようにしたので、簡単で安価に実施できる構成により、情報処理端末を盗んだ或いは拾った第三者が端末から記憶手段を取り外して、その記憶データを不正に読み取って悪用することを確実に防止することができる。

【００７０】

さらに、情報処理端末の筐体の分解、或いは情報処理端末の不正使用が検出されたときに、記憶手段の記憶データを閲覧不可能になるように処理するようにしたので、第三者が筐体の分解、或いは端末の不正使用により、記憶手段の記憶データを不正に読み取って悪用することを確実に防止することができる。

【００７１】

さらに、筐体の分解、或いは端末の不正使用が検出されたときに、記憶データを閲覧不可能にする処理の前に、筐体の分解、或いは端末の不正使用を通知する情報と記憶手段の記憶データを無線通信カードにより外部に送信するようにしたので、送信先の外部で筐体の分解、或いは端末の不正使用を知り、適切に対処することができるとともに、記憶手段の記憶データが外部で保存され失われることがないという優れた効果が得られる。

【図面の簡単な説明】

【図１】本発明の第１の実施形態における情報処理端末の構成を示すブロック図である。

【図２】同端末の無線通信カードとメモリカードを装着するカードコネクタ部の平面図である。

【図３】同端末のカードコネクタ部周辺の構造と無線通信カードの着脱の様子を示す斜視図である。

【図４】図２のＡ－Ａ線に沿った断面図である。

【図５】同端末の無線通信カード用のカードコネクタに設けられたカード挿抜検出スイッチを説明する平面図である。

【図６】同端末とホストコンピュータ間の無線通信で行なわれる端末の使用者の認証処理の手順を示すフローチャート図である。

【図７】同端末で無線通信カードが取り外されたときに行なわれるセキュリティ処理の手順を示すフローチャート図である。

【図８】第２の実施形態で用いられる２段式のカードコネクタ部の平面図である。

【図９】図８のＢ－Ｂ線に沿った断面図である。

【図１０】第３の実施形態で端末の筐体の分解に応じてなされるセキュリティ処理の手順を示すフローチャート図である。

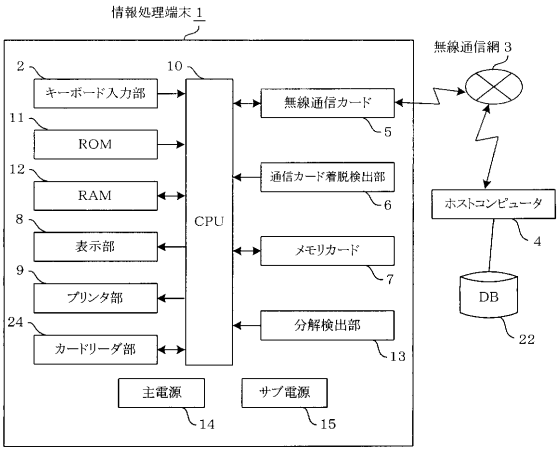
【符号の説明】

１　情報処理端末
２　キーボード入力部
３　無線通信網
４　ホストコンピュータ
５　無線通信カード
６　通信カード着脱検出部
７　メモリカード
８　表示部
９　プリンタ部
１０　ＣＰＵ
１１　ＲＯＭ
１２　ＲＡＭ
１３　分解検出部
１４　主電源
１５　サブ電源
１６　カードコネクタ
１７　プリント基板

１８　結合部
１９　防御壁部
２０　ガイド部
２１　カード挿抜検出スイッチ
２２　データベース
２３　２段式カードコネクタ
２４　カードリーダ部
２５　カードコネクタ
２６　筐体

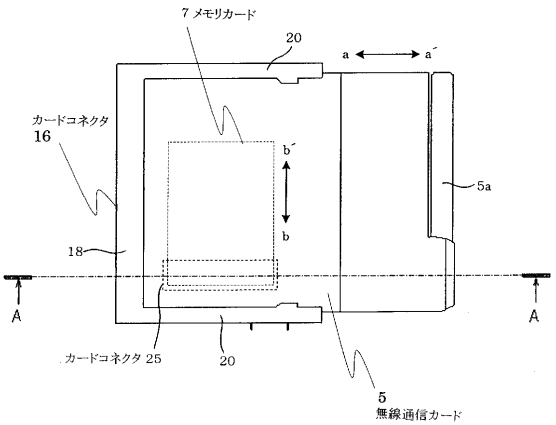
【図１】

（図１）



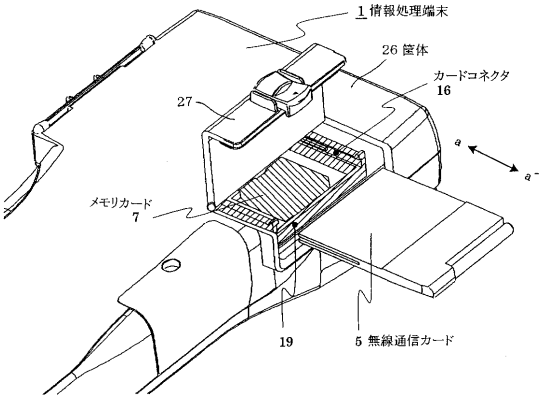
【図２】

（図２）



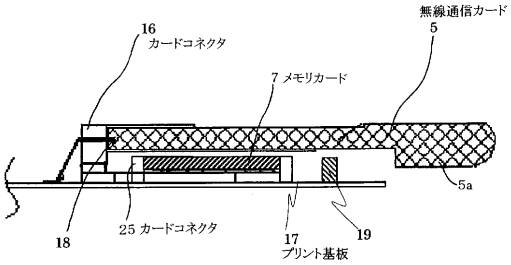
【図３】

（図３）



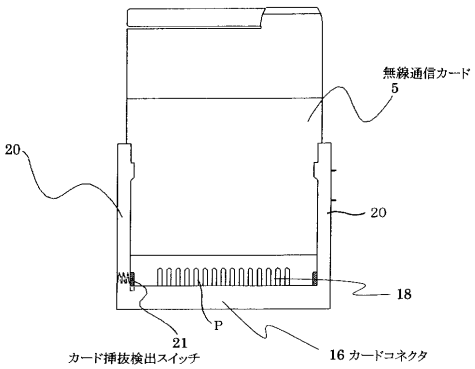
【図４】

（図４）



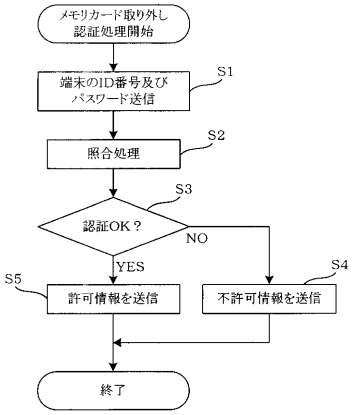
【図５】

（図５）



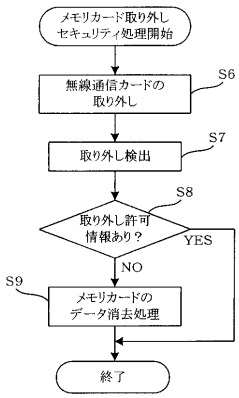
【図６】

（図６）

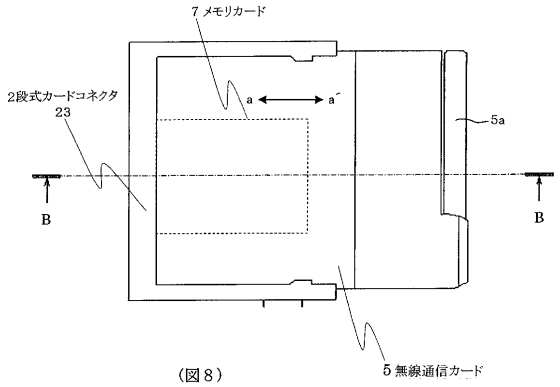


【図７】

(図７)



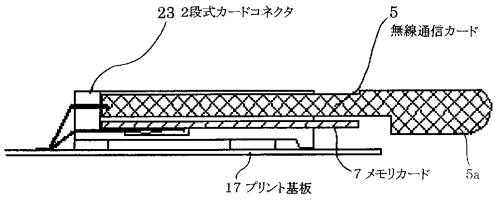
【図８】



(図８)

【図９】

(図９)



【図１０】

(図１０)