(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2005-296489
(P2005-296489A)
(43)公開日　平成17年10月27日(2005.10.27)

(51)Int.Cl.[7]	F I			テーマコード（参考）
A63F 7/02	A63F	7/02	334	2C088
G06K 17/00	A63F	7/02	326Z	5B035
G06K 19/073	A63F	7/02	328	5B058
G06K 19/10	G06K	17/00	T	
	G06K	19/00	P	

審査請求 有　請求項の数 9　ＯＬ　（全 16 頁）　最終頁に続く

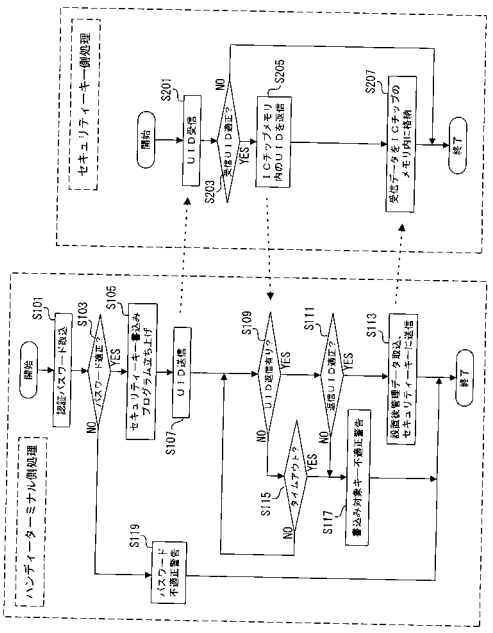
(21)出願番号　特願2004-120066 (P2004-120066)
(22)出願日　平成16年4月15日 (2004.4.15)

(71)出願人　390031772
株式会社オリンピア
東京都台東区東上野２丁目１１番７号
(74)代理人　100079119
弁理士　藤村　元彦
(72)発明者　石井　義郎
東京都台東区東上野二丁目１１番７号　株式会社オリンピア内

Ｆターム(参考)　2C088 BC45 BC47 CA08 EA10
5B035 AA15 BA02 BB09 BC00 CA01 CA23 CA38
5B058 CA17 CA27 KA33 YA13

(54)【発明の名称】遊技機のセキュリティー管理システム

(57)【要約】
【課題】　特殊な形状、及び構造を有する封緘具を用いて、遊技機及びこれに内蔵される電子回路ユニットの設置状態を管理するセキュリティー管理システムを提供する。
【解決手段】　遊技機毎に設けられており、データ記憶用のメモリーを含むＩＣチップを内蔵して遊技機毎に固有の設置後管理データを含むデータの書き込み及び読み出しが自在のセキュリティーキーと、同セキュリティーキーとの間で前記データの授受を行うハンディターミナルと、同ハンディターミナルとの間で前記ＩＣチップ毎に書き込まれたデータの授受を行うコンピュータと、通信ネットワークを介してコンピュータとの間で前記ＩＣチップ毎に書き込まれたデータの授受を行って、上記セキュリティーキーが設けられた遊技機の各々を集中して管理するデータサーバーと、を用いて遊技機のセキュリティー管理システムを構成する。
【選択図】　図４



【特許請求の範囲】
【請求項１】
遊技機毎に設けられており、データ記憶用のメモリーを含むＩＣチップを内蔵して前記遊技機毎に固有の設置後管理データを含むデータの書き込み及び読み出しが自在のセキュリティーキーと、
前記セキュリティーキーとの間で前記データの授受を行うハンディターミナルと、
前記ハンディターミナルとの間で前記ＩＣチップ毎に書き込まれたデータの授受を行うコンピュータと、
通信ネットワークを介して前記コンピュータとの間で前記ＩＣチップ毎に書き込まれたデータの授受を行って、前記セキュリティーキーが設けられた遊技機の各々を集中して管理するデータサーバーと、を含むことを特徴とする遊技機のセキュリティー管理システム。
【請求項２】
前記ハンディーターミナルは、前記セキュリティーキーとの間でその双方に固有の認証コードを介して相互認証を行いつつ、前記セキュリティーキーに内蔵されるＩＣチップへのデータの書き込み、若しくは前記ＩＣチップからのデータの読み出しを行うことを特徴とする請求項１に記載のセキュリティー管理システム。
【請求項３】
前記ハンディーターミナルは、前記コンピュータとの間でその双方に固有の認証コードを介して相互認証を行いつつ、前記セキュリティーキー毎の設置管理後データを前記コンピュータに書き込み、若しくは前記コンピュータに書き込まれた前記データを読み出すことを特徴とする請求項１に記載のセキュリティー管理システム。
【請求項４】
前記コンピュータは、前記データサーバーとの間でその双方に固有の認証コードを介して相互認証を行いつつ、前記セキュリティーキー毎の設置管理後データを前記データサーバに書き込み、若しくは前記データサーバーに書き込まれた前記データを読み出すことを特徴とする請求項１に記載のセキュリティー管理システム。
【請求項５】
前記ハンディーターミナルは、
前記ＩＣチップへ書き込まれた設置管理後データ若しくは前記コンピュータから読み出した設置管理後データを前記セキュリティーキー毎に記憶する記憶手段と、
相互認証の確認されたセキュリティーキーのＩＣチップから読み出した設置管理後データと前記コンピュータから読み出して前記記憶手段に記憶された設置管理後データとを照合する照合手段と、を含むことを特徴とする請求項１に記載のセキュリティー管理システム。
【請求項６】
前記設置後管理データは、前記遊技機の各々について少なくともその属性表示データ、及び設置場所データを含むことを特徴とする請求項１に記載のセキュリティー管理システム。
【請求項７】
前記ＩＣチップは、一旦書き込まれたデータの変更、及びデータの再書き込みを禁止する構成を有することを特徴とする請求項１に記載のセキュリティー管理システム。
【請求項８】
前記セキュリティーキーは、前記遊技機に係着することで該遊技機から取り外しができない構造を有することを特徴とする請求項１に記載のセキュリティー管理システム。
【請求項９】
前記セキュリティーキーは、前記ＩＣチップを把持する基体を破断することよって該セキュリティーキーが係着された遊技機から取り外すことが可能であり、前記基体の破断によって該セキュリティーキーに内蔵されるＩＣチップが破壊されることを特徴とする請求項８に記載のセキュリティー管理システム。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、各地の遊技場に設置される遊技機のセキュリティー管理システムに関する。
【背景技術】
【０００２】
近年におけるエレクトロニクス技術の発達により、パチンコやパチスロ機などの遊技機の性能は高機能化しており、新たな機能を有する多数の遊技機が極めて短期間の内に、全国各地のパチンコ店やゲームセンター等の遊技場に供給されている。これらの遊技機には、そのゲーム動作を制御する中枢部品であるマイクロプロセッサ、メモリー等の電子部品が実装された電子回路ユニットが内蔵されている。それ故、これらの遊技機が一旦、遊技場のホールなどに設置された後は、設置された遊技機の台間での電子回路ユニットの移動、或いは、同ユニット内の部品交換や不正回路との入れ替えなどの不正行為を厳重に防止する必要がある。
【０００３】
従来、かかる不正行為の防止対策として、例えば、特許文献１に示されるような、遊技機筐体のフレーム（台枠）と、上記の電子回路ユニットとを特殊な封緘具を用いてカシメを施して双方を固着させる方式が採用されていた。
【０００４】
しかしながら、従来のカシメ方式による固着に用いられる封緘具は、比較的に模造が容易であり、その真贋の判定には時間を要する場合が多い。それ故、封緘具が本物であるのか、或いは偽造されたものであるのかを、実際に遊戯具が設置された現場で判断することは極めて難しく不正行為の摘発が困難であった。
【０００５】
また、かかる封緘方式の不完全さから、遊技場に設置された後の遊技機に内蔵される電子回路ユニットの設置状況を正確に把握して、広域における遊技機のセキュリティー管理を厳格に行うことは極めて難しかった。
【特許文献１】特開２００２－２８２４１５号公報
【発明の開示】
【発明が解決しようとする課題】
【０００６】
本発明は、このような問題を解決するために為されたものであって、特殊な形状、及び構造を有する封緘具（以下“セキュリティーキー”と称する）を用いて、遊技機及びこれに内蔵される電子回路ユニットの設置状態を管理するセキュリティー管理システムを提供する。
【課題を解決するための手段】
【０００７】
本発明は、遊技機のセキュリティー管理システムであって、遊技機毎に設けられており、データ記憶用のメモリーを含むＩＣチップを内蔵して前記遊技機毎に固有の設置後管理データを含むデータの書き込み及び読み出しが自在のセキュリティーキーと、前記セキュリティーキーとの間で前記データの授受を行うハンディターミナルと、前記ハンディターミナルとの間で前記ＩＣチップ毎に書き込まれたデータの授受を行うコンピュータと、通信ネットワークを介して前記コンピュータとの間で前記ＩＣチップ毎に書き込まれたデータの授受を行って、前記セキュリティーキーが設けられた遊技機の各々を集中して管理するデータサーバーと、を含むことを特徴とする。
【発明を実施するための最良の形態】
【０００８】
【実施例】
【０００９】
先ず、電子的な封緘具であるセキュリティーキー（以下、単に“キー”と言う）につい

て説明する。キーは、通常のＩＣカードと同様にデータの書き込み及び読み出しが自在なメモリーを含むＩＣチップを内蔵している。このＩＣチップには、その他にも、例えば、キー外部のハンディーターミナルとの間でデータの送受信を行う無線通信回路やアンテナ回路、及びチップ全体を制御するマイクロプロセッサ等が含まれている。

【００１０】

図１に、ＩＣチップのメモリー内に記憶されるデータ構成の一例を示す。図１において、ブロックナンバー１乃至３のエリアは、ＩＣチップ毎に固有のユニーク番号であるＵＩＤ１～７や、その他のキー製造時における管理データが書き込まれるエリアである。これらの管理データは、キーの製造時にその製造メーカーによって書き込まれるものであり、一旦書き込まれた番号等を後に改変することはできない。また、後述する遊技機管理機構を管理運営する管理事業者の本店データベース上において、かかるユニーク番号が一括して管理されるものとする。

【００１１】

ブロックナンバー４の遊技機製造メーカーコードは、キーの出荷時（販売時）に管理事業者（販売者）によって書き込まれるものであり、キーが装着される遊技機の製造メーカーを表すものである。なお、一度書き込まれた当該コードは、所定の方法によりロックされてその後に変更することはできない。

【００１２】

ブロックナンバー５乃至１０の各コードは、キーが装着された遊技機が遊技場のホール等に設置されるときに、上記の管理事業者によって書き込まれるデータであり、一旦書き込まれたデータは、所定の方法でロックされてその後に変更することはできない。

【００１３】

なお、図１に示されるＩＣチップメモリー内のデータ構成は、一つの事例を表すものに過ぎず、本発明の実施がかかる事例に限定されるものでないことは言うまでもない。

【００１４】

次に、本発明による遊技機のセキュリティー管理システムについて、パチンコやパチスロ機などの遊技機に上記のキーが装着されて、それに基づくセキュリティー管理が為されまでを時系列的に説明する。

【００１５】

先ず、遊技機の製造メーカーは、キーを一括して管理する管理事業者から、ＩＣチップ固有のユニーク番号（以下、単に“ＵＩＤ”と言う）や遊技機製造メーカーコード等のデータ（図１のブロックナンバー１乃至４のデータ）が既に書き込まれたキーを購入する。そして、自社で製造した遊技機を各地の遊技場に出荷する際に、これらのキーを出荷される遊技機毎に装着する。なお、遊技機単体が全国各地の遊技場に出荷された後、現地において、製造メーカー、或いは管理事業者の監督の下に遊技機へのキーの装着を行うようにしても良い。

【００１６】

キーが遊技機に装着された状態を図２に示す。同図において、セキュリティーキー３０の基体は、円筒軸状の軸部３１、軸部に対して放射方向に設けられた可撓性を有する矢羽翼状の係止片３２、操作ツマミ部３４，及び軸部と操作ツマミ部とを連結する切断部３３から成っている。操作ツマミ部３４には、例えば、ヘリカルアンテナ等の高周波受信アンテナが内蔵されており、また、切断部３３の付近には軸部３１に把持される形で上記のＩＣチップが内蔵されている。

【００１７】

遊技機フレーム１１は、パチンコやパチスロ機等の遊技機の台（フレーム）であり、例えば、釘等が設けられた着脱自在な制御ＲＯＭ付きの遊技機盤を含む構成であっても良い。また、電子回路ユニット基台２１は、遊技機のゲーム動作を総括制御する電子回路ユニット２０を担持する部分であり、遊技盤の背面に固定され、電子回路基板が実装された回路基板ケース２２を支持すると共に、玉排出通路等を備えた遊技機の本体機構を含む構成であっても良い。なお、遊技機フレーム１１の制御ＲＯＭと、電子回路ユニット基台２１

の電子回路基板との間は、コネクタ及びケーブルを介して接続されている。

【００１８】

キー３０は、遊技機フレーム１１及び電子回路ユニット基台２１の双方を貫通する開孔部に、その軸部３１を挿通することによって遊技機に装着される。キー３０の係止は、係止片３２の可撓性による部材変形のみを利用して行うようにしても良いし、或るいはキー３０の挿通後、軸部３１を回転軸としてキーを１／４乃至１／２回転させ、係止片３２と開孔部との位置関係の変化を利用して行うようにしても良い。なお、係止片３２の形状や、軸部３１への取付位置、或いはその取付数等の条件に関しては、図２の記載に限定されるものではない。

【００１９】

キー３０が一旦、遊技機に装着されると係止片３２の作用によって、キー３０、遊技機フレーム１１、及び電子回路ユニット基台２１の三者が固着される。図２からも明らかな如く、キー３０の基体は、その切断部３３において極端に括れている。それ故、キー装着後に、操作ツマミ部３４を掴んで遊技機に装着されたキーを無理に引き抜こうとすると、切断部３３にストレスが加わりキー３０が同部分において破断される構造となっている。上述の如く、ＩＣチップは、かかる切断部３３に埋設内蔵されており、ＩＣチップ自体は脆弱なシリコン基板、或いはセラミック基板で構成されているため、キー３０の基体が切断部３３の近傍で破断されると、それに伴ってＩＣチップも同時に破壊される。

【００２０】

以上に説明した如く、キーが一旦遊技機に装着されると、キーに内蔵されているＩＣチップを破壊しない限り、遊技機からキーを取り外せない構造となっている。また、遊技機におけるキーの装着位置は、遊技機のフレームに、同遊技機に内蔵される電子回路ユニットが係止される位置に設けられている。したがって、遊技機に装着されたキーを破断して、キーに内蔵されたＩＣチップを破壊しない限り、遊技機フレームから電子回路ユニットを取り外すことができない。

【００２１】

次に、キーが装着された遊技機が遊技場に据え付けられるとき（以下、“据付検査時”と言う）の処理を説明する。

【００２２】

かかる据付検査時に、管理事業者の検査員が操作するハンディーターミナルによって、キーのＩＣチップに図１のブロックナンバー５乃至１０のデータが書き込まれる。据付検査時におけるハンディターミナルからキーへのデータ書込みの概念を図３に示す。

【００２３】

図３において、遊技機１０は、例えば、パチンコやパチスロ機等の遊技機を表している。電子回路ユニット２０は、遊技機１０におけるゲーム動作全体を総括制御する部分であり、遊技機１０のフレームにキー３０によって係止されている。キー３０は、前述の如く、メモリー等の各種の電子回路を含むＩＣチップを内蔵している。

【００２４】

一方、図３のハンディーターミナル４０（以下、単に“ターミナル４０”と言う）は、例えば、ブルートゥース(Bluetooth)やＩＥＥＥ８０２規格等の微弱ないし小電力の電波を利用して、キー３０に各種のデータを送信し、或いはキー３０から所定のデータを受信する携帯端末装置である。ターミナル４０は、キーボードやディスプレイパネル、内部メモリー回路、上記の無線送受信回路、及び各部の制御回路などの各種回路（何れも図示せず）を含んでいる。

【００２５】

ターミナル４０からキー３０へのデータの書込み処理を、図４のフローチャートに基づいて説明する。なお、図４の左側の破線に囲まれた部分がターミナル４０における動作を示すものであり、その右側の破線に囲まれた部分がキー３０の動作を示すものである。

【００２６】

先ず、検査員は、ターミナル４０の電源投入により同ターミナルを立ち上げると、その

キーボードを介して認証パスワードを入力する。認証パスワードとしては、例えば、ハンディターミナル毎に固有に設定されたハンディーターミナル番号を利用するようにしても良い。なお、かかるハンディターミナル番号も上記事業者によって一括して管理が為されるものとする。また、ハンディターミナル番号以外にも、例えば、ハンディターミナルを操作する検査員について、各個人毎に所定のパスワードを更に設けるようにしても良い。これらのパスワードを設けることによって、例えば、第三者が不正にハンディーターミナルを入手した場合でもその操作ができない仕組みとなる。

【００２７】

図４のステップＳ１０１でターミナル４０に認証パスワードが取り込まれると、次のステップＳ１０３において、かかるパスワードのチェック処理が為される。チェックの結果、パスワードが不適正であると判定されたときは、ステップＳ１１９に移行して、ターミナル４０から警報音、或いは警報表示を伴う警告出力が為され、それ以降のターミナル４０へのアクセスは禁止される。

【００２８】

一方、ステップＳ１０３でパスワードが適正であると判定された場合、次のステップＳ１０５において、キー３０にデータを書き込むアプリケーションプログラムの立ち上げ処理が実行される。これによって、ターミナル４０の無線通信回路等の各回路の機能が活性化されキー３０へのデータ送信が可能となる。

【００２９】

据付検査時においてターミナル４０は、据付検査の対象とされる遊技機１０、及びそれに装着されたキー３０の履歴を当然に把握しており、ターミナル４０の内部メモリーには、据付検査の対象とされる各々のキー３０の内蔵ＩＣチップに書き込まれたＵＩＤが予めストアされている。ステップＳ１０５の立ち上げ処理が完了すると、ターミナル４０は、ステップＳ１０７で据付検査の対象とされるキー３０に対し、当該キーに相当するＵＩＤを内部メモリーから抽出してこれを送信する。

【００３０】

一方、キー３０の側では、ステップＳ２０１でターミナル４０から送信されたＵＩＤを受信すると、次のステップＳ２０３において受信したＵＩＤが適正であるか否かを判定する。具体的には、キー３０は、受信したＵＩＤと、ＩＣチップ内メモリーのブロックナンバー１乃至２のエリアに出荷時に書き込まれたＵＩＤとを比較・判定する。

【００３１】

ステップＳ２０３において、受信したＵＩＤが不適正、つまり両者が不一致であると判定された場合、キー３０はそれ以降の動作を中止する。なお、この場合に、例えば、ターミナル４０に、ＵＩＤが不適正である旨の通報を行うようにしても良いし、或いは、キー３０に設けられた何らかの表示手段に、ＵＩＤが不適正である旨を表示させるようにしても良い。一方、ステップＳ２０３において、受信したＵＩＤが適正、つまり両者が一致したと判定された場合は次のステップＳ２０５に進み、キー３０は、ＩＣチップに書き込まれていたＵＩＤをターミナル４０に返信する。

【００３２】

一方、ターミナル４０は、上記のステップＳ１０７でキー３０へのＵＩＤ送信を行った後、ステップＳ１０９に進み、キー３０からＵＩＤの返信が有るか否かを監視して、返信が検知されないときはステップＳ１１５に移り、返信監視の待機期間が所定の時間長を経過しているか否かのタイムアウトをチェックする。タイムアウトが発生していなければ、ステップＳ１０９に戻り、キー３０からのＵＩＤの返信監視を繰り返す。

【００３３】

ステップＳ１０９において、キー３０からの返信が検知されると、ターミナル４０は次のステップＳ１１１に進み、キー３０から返信されたＵＩＤが、先に、キー３０へ送信したＵＩＤと等しいか否かを判定する。そして、キー３０から返信されたＵＩＤが適正である、即ち、通信相手先のキー３０が据付検査の対象とするキーであることが確認されると、ステップＳ１１３の処理に移行する。

【００３４】
ステップＳ１１３において、ターミナル４０は、検査員がキーボードから入力した以下のデータを取り込み、これらのデータに所定の暗号化処理を施した後、これをキー３０に送信する。
【００３５】
（１）ホール番号
（２）遊技機台番号
（３）検査日
（４）管理エリアコード
（５）管理者コード
（６）書込みハンディーターミナル番号
上記の各データを簡単に説明すれば、（１）はキー３０が装着された遊技機１０が設置されている遊技場内のホール番号を示すものであり、（２）はホール内、若しくは遊技場内における当該遊技機の台番号を表す。（３）はキー３０へのデータ書込みが行われた期日、即ち据付検査の行われた日を示すものであり、（４）は当該遊技機が設置された遊技場の地域を示す管理エリアコードを示すものである。また、（５）はセキュリティー管理システムを運営する管理者の略号を示すものであり、（６）は書込みを行ったハンディーターミナルの機器認証番号を示すものである。なお、管理エリアコードや管理者コードは、前述の管理事業者によって一括して管理されるものとする。
【００３６】
以上の各データは、据付検査が為される遊技機１０にとって固有のものであり、かつ同遊技機が遊技場に設置された後の管理情報となるので、以後“設置後管理データ”と称するものとする。なお、ターミナル４０は、暗号化された設置後管理データをキー３０に送信すると共に、当該キーのＵＩＤとリンクさせて、同データをターミナル４０の内部メモリーに保存する。
【００３７】
一方、キー３０側では、ターミナル４０から設置後管理データを受信すると、ステップＳ２０７において、これらのデータをＩＣチップ内の所定メモリーエリアに記憶する。因みに、これらの設置後管理データが記憶されるメモリーエリアは、図１に示されるブロックナンバー５乃至１０の領域に相当する。
【００３８】
なお、キー３０のＩＣチップにおいて設置後管理データの書込みは、１回のみで禁止される構成となっている。かかる構成は、例えば、フューズＲＯＭ(Read Only Memory)のような書込みセルの溶断によって書き込まれた情報を担保するハードウェアで実現しても良いし、或いは、ＩＣチップ内のマイクロプロセッサによる所定のソフトウェア処理によって実現するようにしても良い。これによって、一旦、キー３０に書き込まれた設置後管理データが変更されたり、新たな設置後管理データが上書きされる危険を回避できる。
【００３９】
ＩＣチップのメモリー内に所定の設置後管理データが書き込まれるとキー３０における据付検査時の処理は終了する。なお、キー３０は、データ書込み処理の終了をターミナル４０に通知するようにしても良いし、或いは、キー３０に設けられた何らかの表示手段に、処理が終了した旨を表示させるようにしても良い。
【００４０】
一方、ターミナル４０側では、ステップＳ１１３において、キー３０への設置後管理データの送信、及び内部メモリーへの保存を終了させると、１つのキー３０への処理を終了させる。
【００４１】
なお、ステップＳ１１１においてキー３０から返信されたＵＩＤが不適正であると判定された場合、または、ステップＳ１１５で、キー３０から返信がなくタイムアウトが判定された場合、ターミナル４０は、ステップＳ１１７に移行する。そして、据付検査対象の

遊技機に装着されたキーが不適正なものである旨の警告表示を行った後、当該キーへの処理を終了させ、次の据付検査対象の遊技機キーに処理を移行させる。

【００４２】

なお、ターミナル４０は、据付検査の対象とされる全ての遊技機１０に装着されているキー３０に対して、以上に説明した設置後管理データの書込み処理を実行する。

【００４３】

次に、管理事業者の所轄支店におけるハンディターミナルからデータ保存用コンピュータへの設置後管理データの転送、及び同データの保存・表示について説明する。

【００４４】

上記の据付検査が終了すると、検査員は、据付検査が行われた遊技場を管轄する管理事業者の支店にハンディターミナルを持ち帰る。前述の如く、ハンディターミナルは、その内部にメモリーを有しており、据付検査時に書込まれた遊技機毎の設置後管理データが暗号化されて同メモリー内に蓄積されている。ハンディターミナルに蓄積されるデータ量は、その内蔵メモリーの容量によって左右されるが、データ処理の便宜上から、例えば、１台のハンディターミナルに蓄積可能なデータ量を遊技機３０００台程度に定めるようにしても良い。なお、全ての設置後管理データは、各々のキーのＵＩＤとリンクしてメモリー内に蓄積されていることは言うまでもない。

【００４５】

所轄支店に持ち帰ったハンディターミナルからは、図５に示される如く、その内蔵メモリーに蓄積されたデータが同支店のデータ保存用コンピュータに転送される。

【００４６】

図５において、通信ユニット５０は、ターミナル４０の内蔵メモリーに蓄積された設置後管理データを読み出して、これをデータ保存用コンピュータ７０（以下、単に“コンピュータ７０”と言う）に転送する通信ユニットであり、通信ケーブル６０を介してコンピュータ７０に接続されている。また、コンピュータ７０は、例えば、デスクトップ型のパーソナルコンピュータであり、本体のＣＰＵ、キーボード、ディスプレイ、ＨＤＤ等の記録媒体から成る記憶部、及び各種の通信ポートを備えている。なお、ターミナル４０から転送された遊技機毎の設置後管理データは、かかる記憶部にデータベースとして保存される。

【００４７】

なお、図５に示される事例では、ターミナル４０とコンピュータ７０とを、通信ユニット５０及び通信ケーブル６０を介して有線接続しているが、本発明は、かかる事例に限定されるものではなく、例えば、前述したキー３０へのデータ書込み時のように、無線通信媒体を用いて両者を接続するようにしても良い。

【００４８】

次に、ターミナル４０からコンピュータ７０へのデータの転送処理を、図６のフローチャートに基づいて説明する。

【００４９】

コンピュータ７０の電源が投入されてその動作が開始されると、先ず、ステップＳ３０１において認証パスワードの取込処理がなされる。すなわち、コンピュータ７０の操作者は、当該操作者、或いはコンピュータ７０について予め設定された認証用のパスワードをコンピュータ７０のキーボードを介して入力すると、コンピュータ７０がこれを取り込む。なお、パスワードとして文字コードではなく、例えば、予め登録された操作者の指紋や血流等の個人認識情報を用いるようにしても良い。この場合、コンピュータ７０は、指紋スキャナーなどの所定のセンサー機器を用いてこれらの情報を取り込むことになる。かかる処置を講ずることにより、第三者が不正にコンピュータ７０を操作してコンピュータ内のデータベースにアクセスすることを防ぐことができる。

【００５０】

ステップＳ３０１で認証パスワードが上記いずれかの形で取り込まれると、コンピュータ７０は、ステップＳ３０３に移り、取り込んだパスワードのチェックを行う。ステップ

Ｓ３０３においてパスワードが不適正であると判定された場合、コンピュータ７０は、ステップＳ３１７に移行してパスワードが不正である旨の警告処理を実行して図６の処理を終了させる。不正警告処理は、例えば、ディスプレイ上に不正アクセスが行われている旨を表示するメッセージを出力するようにしても良いし、或いは、スピーカやブザー等から不正アクセスを示す警告音を出力しても良い。

【００５１】

一方、ステップＳ３０３においてパスワードが適正であると判定された場合、コンピュータ７０は、ステップＳ３０５に進み、ターミナル４０からのデータ取り込みアプリケーションプログラムの立ち上げ処理を実行する。これによって、コンピュータ７０からは、通信ケーブル６０及び通信ユニット５０を介して、ターミナル４０にデータの取込指令が送信され、これを受信したターミナル４０は、そのメモリー内に蓄積されているデータの転送を準備する。

【００５２】

なお、セキュリティシステムの完全性を期すべく、例えば、ターミナル４０からデータを転送する際に、コンピュータ７０からターミナル４０にそのハンディターミナル番号を送信して、ターミナル４０側においてもハンディターミナル番号の認証処理を行うようにしても良い。

【００５３】

ステップＳ３０５の処理が完了すると、コンピュータ７０は、次のステップＳ３０７に進み、ターミナル４０に蓄積されたデータの転送を開始させる。これによって、ターミナル４０の内蔵メモリーに蓄積されていた各遊技機毎の設置後管理データが、全てコンピュータ７０に転送される。

【００５４】

ステップＳ３０７が終了すると、コンピュータ７０はステップＳ３０９において、ターミナル４０から転送されたデータを、その記憶部の所定エリア内にデータベースとして格納する。すなわち、ステップＳ３０９が終了した時点で、コンピュータ７０の記憶部には、据付検査が終了した遊技機に関する設置後管理データが、各遊技機に装着されたキー３０のＵＩＤに関連づけされ保存される。このようにしてコンピュータ７０の記憶部に形成されたデータベースを利用することにより、所轄支店では、その管内に設置されている遊技機の動向を容易に把握することができる。

【００５５】

ところで、コンピュータ７０のデータベース上に保存された各遊技機の設置後管理データは、前述の如く、暗号化されたままの状態である。それ故、これらのデータをそのままコンピュータ７０のディスプレイ上に表示しても、操作者はその内容を理解することができない。そこで、保存データをディスプレイ上に操作者に理解可能な形で表示する解読表示処理が必要となり、これを図６のフローチャートに基づいて以下に説明する。

【００５６】

ステップＳ３０９のデータ保存処理が終了すると、コンピュータ７０はステップＳ３１１において、操作者からデータベースの表示要求が為されているか否かを判定する。かかる要求が為されていないときは、コンピュータ７０はその処理を終了させる。一方、表示要求があるときは、コンピュータ７０は、ステップＳ３１３に進んで再度認証パスワードの取込み並びにチェック処理を実行する。なお、同処理については、前述のステップＳ３０１、Ｓ３０３と同様であるためその説明を省略する。

【００５７】

ステップＳ３１３において、パスワードが適正であると判定された場合は、コンピュータ７０は、ステップＳ３１５に進んで、データベース上に保存された設置後管理データに所定の暗号解読処理を施して、解読後のデータをそのディスプレイ上に表示する。一方、ステップＳ３１３で、パスワードが不適正であると判定された場合は、コンピュータ７０は、ステップＳ３１７の不正警告処理を実行して図６に示される処理を終了させる。

【００５８】

次に、遊技機の確認検査時における処理について説明を行う。なお、遊技機の確認検査とは、据付検査を経て各遊技場に据え付けられた遊技機に不正行為が加えられていないかをチェックする検査のことである。確認検査では、先ず、確認検査の対象とされる遊技機に関する据付検査時の設置管理後データを、所轄支店のデータ保存用コンピュータから当該遊技機の据付検査時に使用されたハンディーターミナルにロードする。その後、管理事業者の検査員が、このハンディーターミナルを遊技場に持参して、確認検査の対象となる遊技機のセキュリティーキーから設置後管理データを読み取り、これを据付検査時のデータと照合することにより行う。

【００５９】

先ず、確認検査時の所轄支店における処理について前述の図５を参照しつつ説明を行う。確認検査を行うためには、上記の如く、検査対象とされる各遊技機に関する設置後管理データをコンピュータ７０からターミナル４０にロードする必要がある。それ故、ターミナル４０を、通信ユニット５０、及び通信ケーブル６０を介してコンピュータ７０に接続する。なお、以上の各機器についての説明は、既に記述しているため省略する。

【００６０】

次に、コンピュータ７０からターミナル４０へのデータのロード処理を、図７のフローチャートに基づいて説明する。なお、図７におけるステップＳ４０１、Ｓ４０３、及びＳ４１１に関しては、図６のステップＳ３０１、Ｓ３０３、及びＳ３１７の各ステップと同様であるためその説明を省略し、図７のステップＳ４０５以下を説明する。

【００６１】

すなわち、ステップＳ４０３において、パスワードが適正であると判定されると、コンピュータ７０は、ステップＳ４０５に進み、データの表示及び転送のアプリケーションプログラムを立ち上げる。確認検査処理の正確を期すべく、次のステップＳ４０７で、コンピュータ７０は、確認検査の対象とされる遊技機の設置後管理データを記憶部のデータベースから抽出して暗号解読を施した後、これをディスプレイ上に表示する。以上の処理が終了すると、コンピュータ７０は、ステップＳ４０９に移り、そのデータベースからターミナル４０へデータを転送する。なお、ターミナル４０では、転送されたデータ、即ち、確認検査の対象とされる各遊技機の設置後管理データを、遊技機の各々に装着されたキー３０に含まれるＩＣチップ毎のＵＩＤを基準にして内蔵メモリーにストアする。

【００６２】

次に、遊技場における確認検査処理の様子を図８のフローチャートに基づいて説明する。なお、図８の場合もハンディーターミナル側処理のステップＳ５０１、Ｓ５０３、及びＳ５１９に関しては、図４のステップＳ１０１、Ｓ１０３、及びＳ１１９の各ステップと同様であるためその説明を省略する。

【００６３】

したがって、図８に関しては、ハンディーターミナル側処理のステップＳ５０５から説明を始める。即ち、ターミナル４０は、ステップＳ５０３でパスワードが適正であると判定されるとステップＳ５０５に進み、データ照合プログラムを立ち上げ、さらに、次のステップＳ５０５で、確認検査の対象とされる遊技機１０のキー３０に対して、そのＩＣチップのＵＩＤを送信する。

【００６４】

セキュリティーキー側では、ステップＳ６０１でターミナル４０から送信されたＵＩＤを受信すると、次のステップＳ６０３において受信したＵＩＤが適正であるか否かを判定する。具体的には、キー３０は、受信したＵＩＤと、ＩＣチップ内メモリーのブロックナンバー１乃至２のエリアに出荷時に書き込まれたＵＩＤとを比較・判定する。

【００６５】

ステップＳ６０３において、受信したＵＩＤが不適正、つまり両者が不一致であると判定された場合、キー３０はそれ以降の動作を中止する。なお、この場合に、例えば、ターミナル４０に、ＵＩＤが不適正である旨の通報を行うようにしても良いし、或いは、キー３０に設けられた何らかの表示手段に、ＵＩＤが不適正である旨を表示させるようにして

も良い。一方、ステップＳ６０３において、受信したＵＩＤが適正、つまり両者が一致したと判定された場合は次のステップＳ６０５に進み、キー３０は、ＩＣチップに書き込まれていた設置後管理データをターミナル４０に返信する。

【００６６】

一方、ターミナル４０は、上記のステップＳ５０７でキー３０へのＵＩＤ送信を行った後、ステップＳ５０９に進み、キー３０からデータの返信が有るか否かを監視して、返信が検知されないときはステップＳ５１５に移り、返信監視の待機期間が所定の時間長を経過しているか否かのタイムアウトをチェックする。そして、タイムアウトが発生していなければ、ステップＳ５０９に戻り、キー３０からのデータの返信監視を繰り返す。

【００６７】

ステップＳ５０９において、キー３０からの返信が検知されると、ターミナル４０は次のステップＳ５１１に進み、キー３０から返信されたデータと内蔵メモリーにストアされているデータとの照合を行う。すなわち、確認検査対象とされる遊技機のＩＣチップから直接読み込んだ設置後管理データと、所轄支店のデータベースからロードされた当該遊技機に関する設置後管理データとを照合するわけである。キーの偽造や電子回路ユニットの交換等の不正行為が為されていなければ当然に両者のデータは一致し、その遊技機は適正なものであるとの確認が為されて、当該遊技機についての確認検査を終了する。

【００６８】

一方、ステップＳ５１１においてキー３０から返信された設置後管理データが不適正であると判定された場合、または、ステップＳ５１５で、キー３０から返信がなくタイムアウトが判定された場合、ターミナル４０は、ステップＳ５１７に移行する。そして、検査対象の遊技機に装着されたキーが不適正なものである旨の警告表示を行った後、当該キーへの処理を終了させ、次の確認検査対象の遊技機キーに処理を移行させる。

【００６９】

なお、ターミナル４０は、確認検査の対象とされる全ての遊技機１０に装着されているキー３０に対して、以上に説明した設置後管理データの照合処理を実行する。

【００７０】

次に、管理事業者の本店に設置された中央管理データサーバーによる、各遊技機の集中管理について図９を参照しつつ説明を行う。

【００７１】

図９において、コンピュータ７０は、各地の所轄支店に設置されたデータ保存用のコンピュータを表す。中央管理データサーバー９０は、遊技機管理機構を担う管理事業者の本店に設置されたデータサーバーであり、各地の所轄支店のコンピュータ７０に保存されているデータベースを一括して集中管理するものである。また、通信ネットワーク８０は、例えば、ＮＴＴやその他の通信事業者が運営管理する専用回線等の通信ネットワークである。各所轄支店のコンピュータ７０は、通信ネットワーク８０を介して本店の中央管理データサーバー９０に接続されている。

【００７２】

各支店のコンピュータ７０と本店の中央管理データサーバー９０との間において、予め所定の認証コードを定めておき双方が相互認証を行いつつ、各支店のコンピュータ７０のデータベースに格納された各遊技機の設置後管理データを本店の中央管理データサーバー９０に転送する。これによって、全国各地の遊技場に設置された遊技機の動向を本店の中央管理データサーバー９０により、一括して集中管理することが可能となる。

【００７３】

なお、図９に示される支店や本店の数は、説明の便宜上のものであり、本発明の実施がかかる事例に限定されるものでないことは言うまでもない。

【００７４】

以上に説明したように、本発明による遊技機のセキュリティー管理システムによれば、遊技場における遊技機の据付検査及び確認検査の方式を統一することが可能となり、全国各地の遊技場に設置された遊技機を中央で集中管理することができる。また、各地の支店

間における遊技機の移動も容易に把握することが可能となり、遊技機に対する不正行為の発見も容易となる。

【図面の簡単な説明】

【００７５】

【図１】図１は、セキュリティーキーのＩＣチップへ書き込まれるデータの構成を示す説明図である。

【図２】図２は、セキュリティーキーの概略構造、及び同キーが遊技機に装着された場合の状態を示す構造図である。

【図３】図３は、ハンディターミナルと遊技機に装着されたセキュリティーキーとの間におけるデータ授受の概念を示す説明図である。

【図４】図４は、ハンディターミナルからセキュリティーキーへのデータの書込みの手順を示すフローチャートである。

【図５】図５は、ハンディターミナルとデータ保存用コンピュータとの間におけるデータ授受の概念を示す説明図である。

【図６】図６は、ハンディターミナルからデータ保存用コンピュータへのデータの転送を示すフローチャートである。

【図７】図７は、データ保存用コンピュータからハンディターミナルへのデータの転送を示すフローチャートである。

【図８】図８は、ハンディターミナルとセキュリティーキーとの間におけるデータの照合手順を示すフローチャートである。

【図９】図９は、複数のデータ保存用コンピュータと中央管理データサーバからなる管理システムの構成図である。

【符号の説明】

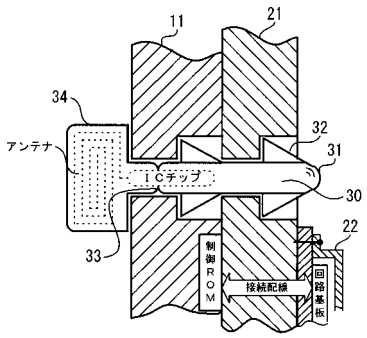
【００７６】

１０　遊技機
１１　遊技機フレーム
２０　電子回路ユニット
２１　電子回路ユニット基台
２２　電子回路基板ケース
３０　セキュリティーキー（セキュリティーキー基体）
３１　軸部
３２　係止片
３３　切断部
３４　操作ツマミ部
４０　ハンディターミナル
５０　通信ユニット
６０　通信ケーブル
７０　データ保存用コンピュータ
８０　通信ネットワーク
９０　中央管理データサーバ

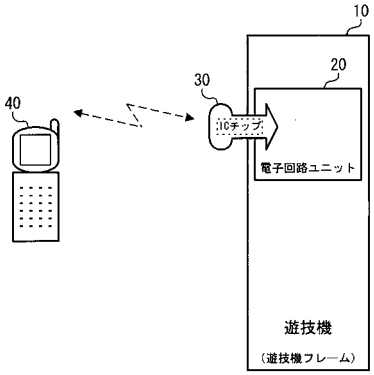
【図１】

ブロックＮｏ.	ＩＣチップメモリー内のデータ構成			
	Byte0	Byte1	Byte2	Byte3
Ｎｏ．１	UID0	UID1	UID2	UID3
Ｎｏ．２	UID4	UID5	UID6	UID7
Ｎｏ．３	内部使用	EAS	AFI	DSFID
Ｎｏ．４	遊技機製造メーカーコード			
Ｎｏ．５	ホール番号			
Ｎｏ．６	遊技機台番号			
Ｎｏ．７	検査日			
Ｎｏ．８	管理エリアコード			
Ｎｏ．９	管理者コード			
Ｎｏ．１０	書込みハンディーターミナル番号			

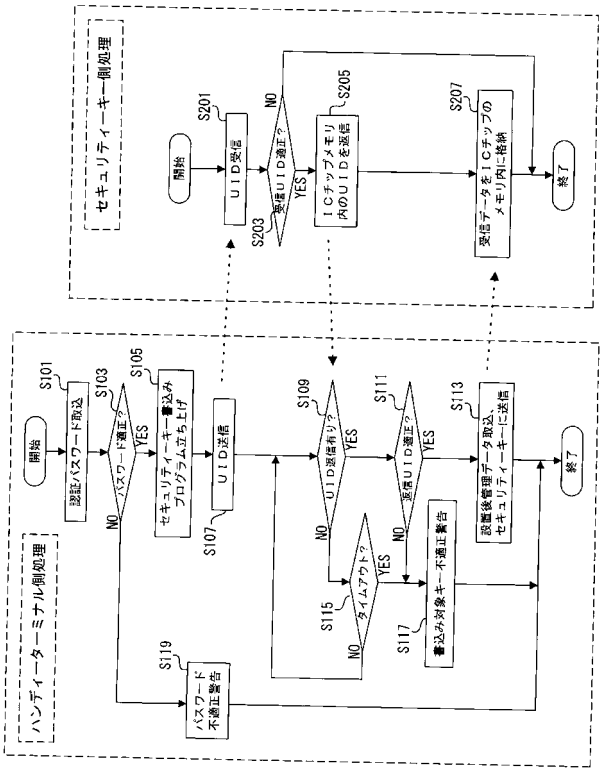
【図２】



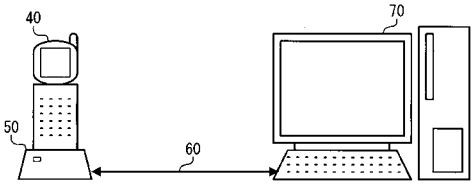
【図３】



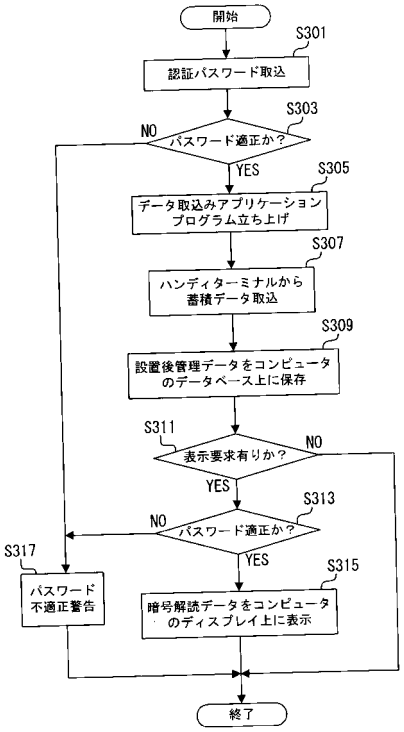
【図４】



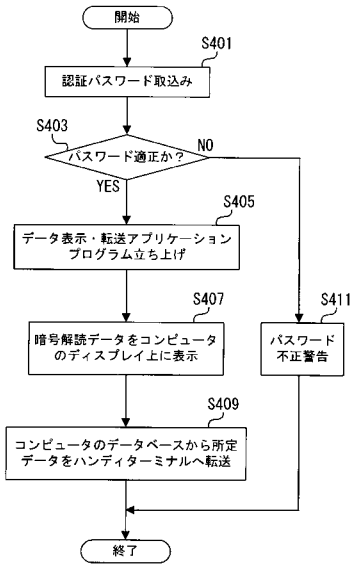
【図５】


40
70
50
60

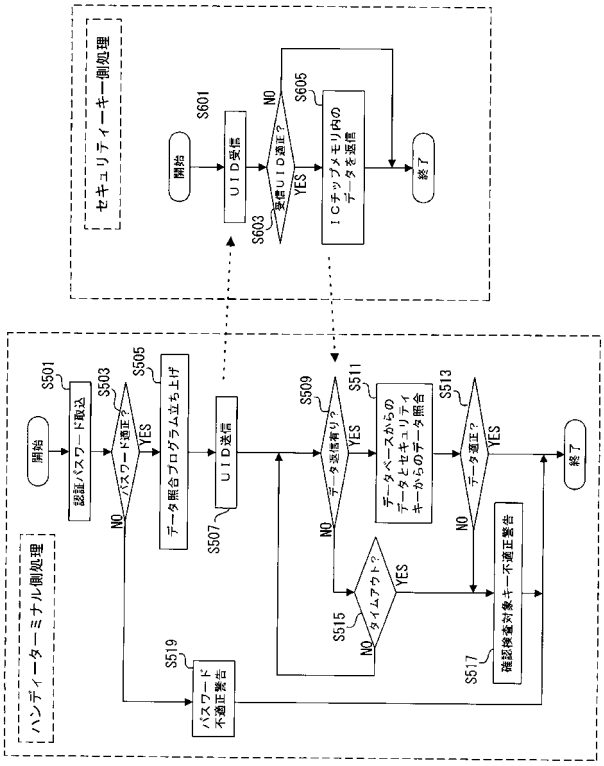
【図６】


開始
S301
認証パスワード取込
S303
NO
パスワード適正か？
YES
S305
データ取込みアプリケーション
プログラム立ち上げ
S307
ハンディターミナルから
蓄積データ取込
S309
設置後管理データをコンピュータ
のデータベース上に保存
S311
表示要求有りか？
NO
YES
S313
NO
パスワード適正か？
YES
S315
暗号解読データをコンピュータ
のディスプレイ上に表示
S317
パスワード
不適正警告
終了

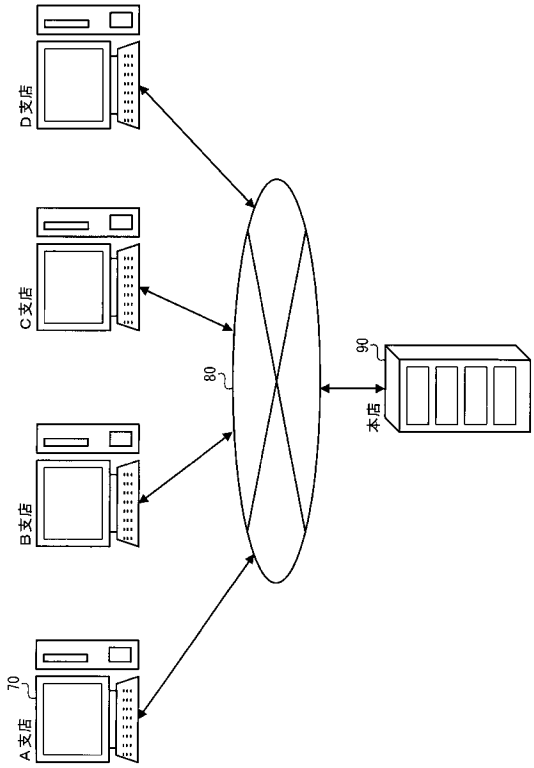
【図７】


開始
S401
認証パスワード取込み
S403
パスワード適正か？
NO
YES
S405
データ表示・転送アプリケーション
プログラム立ち上げ
S407
暗号解読データをコンピュータ
のディスプレイ上に表示
S409
コンピュータのデータベースから所定
データをハンディターミナルへ転送
S411
パスワード
不正警告
終了

【図８】


セキュリティーキー側処理
開始
S601
UID受信
S603
受信UID適正？
NO
YES
S605
ICチップメモリ内の
データを送信
終了
ハンディーターミナル側処理
開始
S501
認証パスワード取込
S503
パスワード適正？
NO
YES
S505
データ照合プログラム立ち上げ
S507
UID送信
S509
データ送信有り？
NO
YES
S511
データベースからの
データとセキュリティ
キーからのデータ照合
S513
データ適正？
NO
YES
S515
タイムアウト？
NO
YES
S517
確認検査対象キー不適正警告
S519
パスワード
不適正警告
終了

【図９】



フロントページの続き

(51)Int.Cl.[7]	FI	テーマコード（参考）
	G06K 19/00 R	