(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4007518号
(P4007518)
(45)発行日　平成19年11月14日(2007.11.14)　(24)登録日　平成19年9月7日(2007.9.7)

(51)Int.Cl.　　F I
A63F 7/02 (2006.01)　　A63F 7/02 334
G06F 11/30 (2006.01)　　G06F 11/30 E

請求項の数 2　(全 63 頁)

(21)出願番号　特願平8-317021
(22)出願日　平成8年11月13日(1996.11.13)
(65)公開番号　特開平10-137419
(43)公開日　平成10年5月26日(1998.5.26)
審査請求日　平成15年10月24日(2003.10.24)

(73)特許権者　000132747
株式会社ソフィア
群馬県桐生市境野町７丁目２０１番地
(73)特許権者　390025601
株式会社西陣
東京都千代田区平河町１丁目４番３号
(74)代理人　100096699
弁理士　鹿嶋　英實
(72)発明者　井置　定男
群馬県桐生市宮本町３－７－２８

審査官　柴田　和雄

最終頁に続く

(54)【発明の名称】遊技装置の監視装置

(57)【特許請求の範囲】

【請求項１】

遊技装置の遊技制御を行うとともに、ＣＰＵ、ＲＡＭ、遊技プログラムを格納したＲＯＭ、識別情報を記録する不揮発性メモリ等を内蔵してワンチップ化した遊技用演算処理装置を有する役物制御装置を監視する遊技装置の監視装置であって、

前記遊技装置の監視装置は、該監視装置からの情報の収集および管理を行う情報管理装置と情報転送可能に接続され、

前記役物制御装置の不揮発性メモリに記録されている識別情報を読み込む識別情報読込手段と、

前記識別情報読込手段により読み込まれた識別情報の正当性を判別する識別情報判別手段と、

前記識別情報判別手段によって識別情報の正当性が認められた場合に、前記役物制御装置へ遊技制御の動作許可の指令をするとともに、識別情報形式を変更した新識別情報を作成して送信し、該新識別情報の前記不揮発性メモリへの記録を指令する遊技制御許可手段と、

第３者機関によって前記識別情報形式を変更するための識別情報形式情報が提供され、提供された前記識別情報形式情報を遊技店の前記情報管理装置で受信し、該情報管理装置より送信される前記識別情報形式を変更するための識別情報形式情報を記憶する揮発性メモリにより構成した記憶手段と、

を備え、

前記識別情報読込手段は、前記情報管理装置で開店操作された際に送信された前記識別情報形式情報である前回の識別情報、該前回の識別情報を復号化するための今回の復号化情報、次回の識別情報および該次回の識別情報を暗号化するための次回の暗号化情報を前記記憶手段に記憶した場合に、前記役物制御装置の不揮発性メモリに記憶されている暗号化された識別情報を読み込み、

前記識別情報判別手段は、前記役物制御装置から読み込んだ暗号化された識別情報を前記今回の復号化情報により復号化し、該復号化した識別情報と、前記前回の識別情報とを比較して正当性を判別し、

前記遊技制御許可手段は、前記識別情報判別手段により正当性が認められた場合に、前記次回の識別情報を前記次回の暗号化情報で暗号化した新識別情報の前記不揮発性メモリへの記録を指令するようにしたことを特徴とする遊技装置の監視装置。

【請求項２】

前記情報管理装置で閉店操作された際に、前記記憶手段に記憶された前記識別情報形式情報を消去する消去手段を備えたことを特徴とする請求項１に記載の遊技装置の監視装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、遊技装置の監視装置に係わり、詳しくは遊技装置（例えば、パチンコ遊技機）の遊技制御を行う役物制御装置に正当性を判別する識別情報を記録しておき、その識別情報を毎回の動作開始時にチェックして変更することにより、役物制御装置の改竄等の不正を有効に防止できるようにした遊技装置の監視装置に関する。

【０００２】

【従来の技術】

従来、遊技装置（例えば、パチンコ遊技機）の遊技制御を行う役物制御装置は、演算処理装置としてのＣＰＵと遊技プログラムを格納したＲＯＭとが別体で構成され、所定の機関により大当り確率等の遊技性能が基準を満たしているか否かを検査し、検査に適合した遊技装置が市場にて販売されている。

そして、遊技店設置後においても、第３者機関によるＲＯＭ検査、すなわち遊技プログラムが改竄されているか否かを検査するためにＲＯＭは着脱可能にソケットに装着され、検査（正規の遊技プログラムか否かの検査）が可能なようにしている。

【０００３】

しかし、ＲＯＭの着脱が容易となっているため、不正ＲＯＭ（遊技プログラムの改竄）の作成もまた容易になっている。不正の手口としては、例えば閉店後にホールに忍び込み、役物制御装置のＲＯＭを不正ＲＯＭ（例えば、大当り確率を良くするように改竄したもの）と交換し、翌日、当該遊技機で遊技を行い不当な利益を得る等がある。

そこで、このような不正なＲＯＭの改竄を防止するために、遊技プログラムを格納したＲＯＭ、ＲＡＭ、ＣＰＵ等をワンチップ化した遊技用演算処理装置の使用が要望されている。

【０００４】

【発明が解決しようとする課題】

しかしながら、ワンチップ化した遊技用演算処理装置であっても、以下のような問題点があった。

（イ）ワンチップ化した遊技用演算処理装置も遊技店設置後においても、第３者機関による内蔵ＲＯＭの検査（すなわち、遊技プログラムが改竄されているか否かの検査）のために、遊技用演算処理装置がソケット差しとなり、上述したように着脱が容易となって交換されることにより、遊技プログラムを改竄するという不正を誘発する恐れがあった。

実際上は、遊技用演算処理装置のチップ自体を新たに作成する必要があり、困難ではあるものの、不正交換の可能性がある。

【０００５】

（ロ）遊技装置製造メーカーが射幸心を抑制する遊技装置を開発しても、遊技用演算処理装置が改竄されたのでは、間接的に遊技者に不当にギャンブル性の高い遊技機を提供してしまう結果となり、射幸心を抑制するという最近のホールの営業方針にも反することになってしまう。

（ハ）最近、遊技用演算処理装置に識別情報を記録しておき、その識別情報を判別して遊技用演算処理装置の正当性を判断することも考えられている。しかし、その識別情報も固定化されたデータであったため、極めて困難ではあるものの、一度、解読されると、やはり遊技用演算処理装置の改竄が可能になり、この点で不正を有効に防止できるシステムが望まれている。

【０００６】

そこで本発明は、上述した問題点に鑑みてなされたもので、識別情報を毎回の動作開始時にチェックして変更することにより、役物制御装置の改竄等の不正を有効に防止できるようにした遊技装置の監視装置を提供することを目的としている。

【０００７】

【課題を解決するための手段】

上記目的達成のため、請求項１記載の発明による遊技装置の監視装置は、遊技装置の遊技制御を行うとともに、ＣＰＵ、ＲＡＭ、遊技プログラムを格納したＲＯＭ、識別情報を記録する不揮発性メモリ等を内蔵してワンチップ化した遊技用演算処理装置を有する役物制御装置を監視する遊技装置の監視装置であって、

前記遊技装置の監視装置は、該監視装置からの情報の収集および管理を行う情報管理装置と情報転送可能に接続され、

前記役物制御装置の不揮発性メモリに記録されている識別情報を読み込む識別情報読込手段と、

前記識別情報読込手段により読み込まれた識別情報の正当性を判別する識別情報判別手段と、

前記識別情報判別手段によって識別情報の正当性が認められた場合に、前記役物制御装置へ遊技制御の動作許可の指令をするとともに、識別情報形式を変更した新識別情報を作成して送信し、該新識別情報の前記不揮発性メモリへの記録を指令する遊技制御許可手段と、

第３者機関によって前記識別情報形式を変更するための識別情報形式情報が提供され、提供された前記識別情報形式情報を遊技店の前記情報管理装置で受信し、該情報管理装置より送信される前記識別情報形式を変更するための識別情報形式情報を記憶する揮発性メモリにより構成した記憶手段と、

を備え、

前記識別情報読込手段は、前記情報管理装置で開店操作された際に送信された前記識別情報形式情報である前回の識別情報、該前回の識別情報を復号化するための今回の復号化情報、次回の識別情報および該次回の識別情報を暗号化するための次回の暗号化情報を前記記憶手段に記憶した場合に、前記役物制御装置の不揮発性メモリに記憶されている暗号化された識別情報を読み込み、

前記識別情報判別手段は、前記役物制御装置から読み込んだ暗号化された識別情報を前記今回の復号化情報により復号化し、該復号化した識別情報と、前記前回の識別情報とを比較して正当性を判別し、

前記遊技制御許可手段は、前記識別情報判別手段により正当性が認められた場合に、前記次回の識別情報を前記次回の暗号化情報で暗号化した新識別情報の前記不揮発性メモリへの記録を指令するようにしたことを特徴とする。

【０００８】

好ましい態様として、例えば請求項２記載のように、前記情報管理装置で閉店操作された際に、前記記憶手段に記憶された前記識別情報形式情報を消去する消去手段を備えるようにしてもよい。

【００１２】

【発明の実施の形態】
以下、本発明の実施の形態を、多数のパチンコ遊技機を設置した遊技場設備に適用した実施例として図面を参照して説明する。すなわち、本実施例はネットワーク監視装置を介してパチンコ遊技機および遊技場内の各端末装置の各種情報を収集し、情報管理装置によって遊技場の情報管理を行っており、遊技装置としてのパチンコ遊技機の内部に遊技装置の監視装置としての情報収集基板を設けて役物制御装置の改竄等の不正を有効に防止できるようにした遊技場設備に本発明を適用した例である
（I）遊技場設備の全体構成
図１は遊技場設備の全体構成を示すブロック図である。図１において、１は遊技店（パチンコホール）であり、遊技店１には情報管理装置２、情報処理装置３、景品ＰＯＳ（景品交換装置）４、ＡＴＭ交換機５、中継装置６～８、局管理装置９、１０、玉貸カード発行装置１１、玉計数装置１２、空調制御装置１３、照明制御装置１４、監視カメラ制御装置１５、パチンコ遊技機（以下、適宜単に、遊技機という）２１ａ～２１ｎ（以下、２１で代表する）が配置されている。局管理装置１０および遊技機２１は、全体として島設備２２を構成している。島設備２２は遊技店１内に複数配置されるのが通常であるが、説明の都合上、１つの場合を例にしている。
【００１３】
情報管理装置２はホールの管理室に配置され、管理コンピュータ（主にパーソナルコンピュータで構成）を含んで構成され、遊技店１における情報管理（例えば、遊技機２１および各端末装置（景品ＰＯＳ４、玉貸カード発行装置１１、玉計数装置１２等）における遊技情報や必要な管理情報の収集管理）、ネットワーク管理等を行うもので、ＡＴＭ交換機５を経由し電話回線２３を介して第３者機関２４との間で情報転送（例えば、後述の遊技機２１の役物制御装置に記録される識別情報の授受等）が可能になっている。第３者機関２４は内部に情報処理装置２４Ａを有しており、電話回線２３を介して遊技店１内の監視情報（例えば、遊技機２２に関する情報、ネットワークに関する情報等）を受け取ったり、遊技店１にＩＤ情報を転送する。この場合、情報処理装置２４Ａは情報管理装置２により収集される情報を取得するとともに、情報管理装置２、後述の局管理装置９、１０、遊技機２１（遊技装置の監視装置）を管理する機能を実現する。なお、情報管理装置２は第３者機関２４における情報処理装置２４Ａの管轄下にある。
【００１４】
情報処理装置３は情報管理装置２から必要な情報を受信して、遊技店１における営業上の遊技情報等を収集管理したり、店内の付帯設備（空調制御装置１３、照明制御装置１４、監視カメラ制御装置１５等）の制御を行ったりする。情報処理装置３も同様に管理コンピュータ（主にパーソナルコンピュータで構成）を含んで構成される。景品ＰＯＳ４は景品の交換処理を行うもので、例えば景品交換カード（例えば、磁気カード）に記録された遊技者の持ち玉数（遊技価値）に基づいて希望の景品と精算する処理を行う。
ＡＴＭ交換機５は遊技店１内に設置された情報管理装置２、情報処理装置３、景品ＰＯＳ４、中継装置６からの情報の伝送を制御する情報交換装置であり、光ファイバーからなる情報伝送路を介して、例えば１５５Ｍｂｐｓの情報量の伝送をＡＴＭ（Asynchronous Transfer Mode：非同期転送モード）交換で行う。
【００１５】
中継装置６～８は、光通信（例えば、赤外通信）によるＬＡＮを構成し、ＡＴＭ交換機５と局管理装置９、１０との間における情報連絡を中継する。中継装置６～８による通信はＬＡＮでなく、例えば有線通信、その他の通信方式でもよい。
局管理装置９は中継装置７と各端末装置（玉貸カード発行装置１１、玉計数装置１２、空調制御装置１３、照明制御装置１４、監視カメラ制御装置１５）との間の情報連絡の中継を行うもので、光送受信部３１、通信制御装置３２、ネットワーク監視装置３３を備えている。光送受信部３１は赤外線を使用して中継装置７との間で情報の送信／受信を行い、ネットワーク監視装置３３は各端末装置との間で電源ライン４１を使用したＬＯＮ（詳細は後述）によるポーリング方式の通信プロトコルによる通信を行う。通信制御装置３２は

光送受信部３１により情報管理装置２と赤外線通信を行う。玉貸カード発行装置１１、玉計数装置１２、空調制御装置１３、照明制御装置１４、監視カメラ制御装置１５にはそれぞれＬＯＮ通信を行うためのＮボード（詳細は後述）４２ａ～４２ｅ（以下、４２で代表する）が配置され、電源ライン４１を介してネットワーク監視装置３３と相互に接続されている。

【００１６】

玉貸カード発行装置１１は玉貸カードとしてのプリペイドカードを発行する。玉計数装置１２は遊技者の獲得した球を計数し、計数値の記録（例えば、磁気記録あるいは印字でもよい）された景品交換カードを発行する。空調制御装置１３は遊技店１内の空調設備の制御管理を行う。照明制御装置１４は遊技店１内の照明設備の制御管理を行う。監視カメラ制御装置１５は遊技店１内をカメラで監視する制御を行う。

島設備２２に配置された局管理装置１０は中継装置８と各遊技機２１ａ～２１ｎとの間の情報連絡の中継を行うもので、光送受信部３４、通信制御装置３５、ネットワーク監視装置３６を備えている。光送受信部３４は赤外線を使用して中継装置８との間で情報の送信／受信を行い、ネットワーク監視装置３６は各遊技機２１ａ～２１ｎとの間で電源ラインを使用したＬＯＮによるポーリング方式の通信プロトコルによる通信を行う。通信制御装置３５は光送受信部３４により情報管理装置２と赤外線通信を行う。各遊技機２１ａ～２１ｎは玉貸装置２５ａ～２５ｎ（以下、２５で代表する）をそれぞれ併設しており、いわゆるカードリーディング機（ＣＲ機）となっている。また、各遊技機２１ａ～２１ｎの内部には詳細を後述する役物制御装置１６１ａ～１６１ｎ（以下、１６１で代表する）が設けられている。

【００１７】

ここで、情報管理装置２は局管理装置９、１０全体の情報収集および管理を行う機能を実現するとともに、所定の通信回線（ここでは電話回線２３）を介して第３者機関２４の情報処理装置２４Ａと情報転送可能に接続され、遊技機２１の役物制御装置に記録される識別情報の識別情報形式を変更するための識別情報形式情報を送信可能である。また、局管理装置１０は遊技装置の監視装置（すなわち、遊技機２１）の一群よりの情報収集および管理を行う機能を実現する。

【００１８】

（II）情報管理装置の構成

図２は情報管理装置２の構成を示すブロック図である。図２において、情報管理装置２はパーソナルコンピュータで構成され、主要なものとして、ＣＰＵ５１、ＢＩＯＳＲＯＭ５２、タイマ５３、ＲＯＭ５４、ＲＡＭ５５、Ｉ／Ｏポート５６、ＳＣＳＩホストアダプタ５７、ＳＣＳＩバス５８、ＨＤＤ５９、ＡＴＭインターフェース６０、バス６１、表示装置６２、開店ＳＷ６３、閉店ＳＷ６４を有している。

ＣＰＵ５１はＢＩＯＳＲＯＭ５２に格納されている起動プログラムを読み出して起動し、遊技店１における情報管理や、遊技機２１の役物制御装置に記録されている識別情報の識別情報形式を変更するための識別情報形式情報の送信、ネットワーク管理（ここでは局管理装置９、１０全体の情報収集および管理）に関する演算処理、記録等を行うプログラムをＲＯＭ５４よりメモリ（ＲＡＭ５５）に読み込み、処理を実行する。ＢＩＯＳＲＯＭ５２は起動プログラムを格納し、ＲＡＭ５５はワークエリアとしても用いられる。また、ＲＯＭ５４は情報管理やネットワーク管理に必要なデータを格納している。タイマ５３はＣＰＵ５１の演算処理に必要な時間計測を行う。

【００１９】

ＳＣＳＩホストアダプタ５７はバス６１とＳＣＳＩバス５８との間のデータ転送に関するインターフェース処理を行い、ＳＣＳＩバス５８を介してＨＤＤ５９が接続される。ＨＤＤ５９は遊技機２１よりの遊技データ等を記憶する。なお、ＨＤＤ５９は外部記憶装置として使用されるが、外部記憶装置としてはＨＤＤに限らず、例えば光磁気ディスク装置（ＭＯ）、デジタルテープ記憶装置（ＤＡＴ）、ＣＤ－ＲＯＭドライブ装置等のその他の記憶装置（および記憶媒体）を使用してもよい。

【００２０】
ＡＴＭインターフェース６０はＡＴＭ交換機５との間でＡＴＭでの転送を行う場合の接続部であり、Ｉ／Ｏポート５６はバス６１と表示装置６２、開店ＳＷ６３、閉店ＳＷ６４との間のインターフェース処理を行う。
表示装置６２は、例えばカラーの液晶装置（ＬＣＤ）からなり、遊技店１の情報管理やネットワーク管理に関して必要な情報を表示する。開店ＳＷ６３は遊技店１を開店する際に係員により操作され、閉店ＳＷ６４は遊技店１を閉店する際に操作される。
【００２１】
（III）ネットワーク監視装置の構成
次に、局管理装置９、１０におけるネットワーク監視装置３３、３６の構成について説明する。ネットワーク監視装置３３、３６は何れも同様の構成であり、ここでは局管理装置９のネットワーク監視装置３３について説明する。ネットワーク監視装置３３はＡＣ２４Ｖの電源ライン４１で各端末装置（玉貸カード発行装置１１、玉計数装置１２、空調制御装置１３、照明制御装置１４、監視カメラ制御装置１５）のＮボード４２ａ～４２ｅと相互に接続され、ＬＯＮの通信ネットワークを構成している。電源ライン４１は各部にＡＣ２４Ｖの電源を供給するとともに、ＬＯＮの通信ネットワークにより相互にデータの転送が可能なようになっている。
ここで、ネットワーク監視装置３３で使用されるＬＡＮは、米国エシャロン社によって開発されたＬＯＮ（Local Operating Network：エシャロン社登録商標）という技術に基づいている。以下、ネットワーク監視装置３３で使用されるＬＡＮをＬＯＮとして説明する。一般的に、ＬＯＮ技術は各種センサと、各種アクチュエータとの通信（例えば、最大３２３８５ノード）により検知、監視、制御その他のアプリケーションを容易に、高信頼度をもって、かつ低コストで実現できるというインテリジェント分散型ネットワークシステム技術である。本実施例では、このＬＯＮ技術をネットワーク監視装置３３、３６、Ｎボード４２、遊技機２１に適用している。
【００２２】
図３は局管理装置９におけるネットワーク監視装置３３の構成を示すブロック図である。
図３において、ネットワーク監視装置３３は分散形知的制御ネットワークＬＯＮシステム用のニューロンチップ１０１、クロック回路１０２、トランシーバ１０３、カップリング回路１０４、バス１０５、ＲＯＭ１０６、不揮発性メモリ１０７、ＤＰＲＡＭ１０８、ＲＡＭ１０９、異常表示装置１１１を有している。
ニューロンチップ１０１は複数のＣＰＵによりＬＯＮシステムの通信管理を行うもので、ＭＡＣＣＰＵ１２１、ネットワークＣＰＵ１２２、アプリケーションＣＰＵ１２３、ＲＡＭ１２４、ＥＥＰＲＯＭ１２５、ネットワーク通信ポート１２６、バス１２７およびＩ／Ｏポート１１０により構成される。
【００２３】
ＭＡＣＣＰＵ１２１はメディアアクセスコントロール用で、７層あるＬＯＮＴＡＬＫプロトコルの第１層と第２層の処理を行う。ネットワークＣＰＵ１２２はネットワーク用で、ＬＯＮＴＡＬＫプロトコルの第３層から第６層までの処理を行う。アプリケーションＣＰＵ１２３はユーザーが書いたコードと、オペレーティングシステム（アプリケーションコードで呼び出したオペレーティングシステム）とを同時に実行し、アプリケーションプログラムに使用するプログラム言語はＮＥＵＲＯＮ　Ｃである。
ＲＡＭ１２４はワークエリアとして使用され、ＥＥＰＲＯＭ１２５はネットワーク構成およびアドレス指定情報、ニューロンチップ識別コード、ユーザー作成のアプリケーションコードおよび読み出し主体データ等のデータを記憶する。ネットワーク通信ポート１２６はネットワーク通信のインターフェース処理を行い、バス１２７は内部の各素子を接続するとともに、Ｉ／Ｏポート１１０と接続する。
【００２４】
クロック回路１０２はニューロンチップ１０１の処理に必要なクロック信号を生成する。
ＲＯＭ１０６はニューロンチップ１０１の制御プログラムやネットワーク通信を行うとき

に必要なデータを格納している。不揮発性メモリ１０７はネットワーク通信を行うときの必要なデータを一時的に格納するワークエリアとして用いられる。
トランシーバ１０３はニューロンチップ１０１とカップリング回路１０４の間に配置されており、ＬＯＮを構成する各ノードと通信メディア間の物理的な接続を行うモジュールで、データの変調および復調を行う。カップリング回路１０４はＡＣ２４Ｖの電源ライン４１に介挿され、電源ライン４１に重畳するデータを変調／復調するトランシーバ１０３に接続される。
【００２５】
ＤＰＲＡＭ（デュアルポートＲＡＭ）１０８はネットワーク監視装置３３上のバス１０５と、通信制御装置３２側との間の何れからでも内部のメモリ（双方向メモリ）へのデータの書き込み、メモリからのデータの読み出しが可能であり、この双方向メモリを介してネットワーク監視装置３３と通信制御装置３２との間で相互にデータ転送が行われる。また、ＤＰＲＡＭ１０８からは通信制御装置３２の方に割り込みをかけるとき接続回路（ここでは通信制御装置３２）への割り込み信号ＳＰ１が出力され、接続回路（ここでは通信制御装置３２）からの割り込みをＤＰＲＡＭ１０８が受けるときは接続回路からの信号ＳＰ２がＤＰＲＡＭ１０８に入力され、Ｉ／Ｏポート１１０に送られる。
【００２６】
ＲＡＭ１０９は上位のネットワークから送信されてきた情報（例えば、情報管理装置２を経由して第３者機関２４から送信された遊技機２１の役物制御装置の正当性を判断するための識別情報等）を一時的に格納しておくもので、電源がオフすると、記憶していた情報（例えば、識別情報）は消滅し、盗用等を防止するようになっている。異常表示装置１１１はネットワーク監視装置３３における異常状態を表示する。
このようなＬＯＮを構成するネットワーク監視装置３３を使用することにより、ＡＣ２４Ｖの電源ライン４１の上に重畳してＮボード４２との間で相互にデータの転送を行うことが可能で、したがって、特にデータ転送用の信号線を設けなくても、電源ライン４１を使用してデータ転送ができるという利点がある。
また、ＬＯＮではＮボード４２との間では電源ライン４１は共通であるが、信号上は絶縁されている。したがって、Ｎボード４２との間で信号が原因でトラブルすることはない。
【００２７】
（Ⅳ）Ｎボードの構成
次に、Ｎボード４２の構成について説明する。Ｎボード４２ａ～４２ｅは何れも同様の構成であり、ここでは玉貸カード発行装置１１に付属するＮボード４２ａについて説明する。図４はＬＯＮ対応のＮボード４２ａの構成を示すブロック図である。図４において、Ｎボード４２ａは分散形知的制御ネットワークＬＯＮシステム用のニューロンチップ１３１、クロック回路１３２、トランシーバ１３３、カップリング回路１３４、バス１３５、ＲＯＭ１３６、不揮発性メモリ１３７、ＤＰＲＡＭ１３８、ＲＡＭ１３９を有している。
ニューロンチップ１２１は図３の場合と同様に、ＭＡＣＣＰＵ１４１、ネットワークＣＰＵ１４２、アプリケーションＣＰＵ１４３、ＲＡＭ１４４、ＥＥＰＲＯＭ１４５、ネットワーク通信ポート１４６、バス１４７およびＩ／Ｏポート１４０により構成される。
【００２８】
クロック回路１３２、トランシーバ１３３、カップリング回路１３４、ＲＯＭ１３６、不揮発性メモリ１３７の機能は図３の場合と同様である。
ＤＰＲＡＭ（デュアルポートＲＡＭ）１３８はＮボード４２ａ上のバス１３５と、接続制御装置１４８（例えば、玉貸カード発行装置１１）側との間の何れからでも内部のメモリ（双方向メモリ）へのデータの書き込み、メモリからのデータの読み出しが可能であり、この双方向メモリを介してＮボード４２ａと接続制御装置１４８との間で相互にデータ転送が行われる。また、ＤＰＲＡＭ１３８からは接続制御装置１４８の方に割り込みをかけるとき接続制御装置１４８への割り込み信号ＳＰ３が出力され、接続制御装置１４８からの割り込みをＤＰＲＡＭ１３８が受けるときは接続制御装置１４８からの信号ＳＰ４がＤＰＲＡＭ１３８に入力され、Ｉ／Ｏポート１４０に送られる。

ＲＡＭ１３９は上位のネットワークから送信されてきた情報を一時的に格納し、電源がオフすると、格納していた情報は消滅する。

【００２９】

（Ｖ）遊技機の構成

次に、遊技機２１の構成について説明する。図５は遊技機２１の構成を示すブロック図である。図５において、遊技機２１はカード式玉貸装置２５を併設しており、カード式玉貸装置２５はカードリーダライタ１５１、玉貸制御装置１５２を含んで構成される。カードリーダライタ１５１はプリペイドカードの情報（例えば、金額情報）の読み出しや必要な情報の書き込みを行い、玉貸制御装置１５２は玉貸しやカード返却等の制御を行うとともに、遊技機２１の後述の情報収集基板に対して玉貸信号を出力したりする。

遊技機２１は役物制御装置１６１、発射制御装置１６２、排出装置１６３、排出制御装置１６４、インターフェース回路１６５、玉貸しスイッチ１６６、カード返却スイッチ１６７、カード度数表示器１６８、玉貸し可能ＬＥＤ１６９を含んで構成される。

【００３０】

役物制御装置１６１は遊技機２１における役物の制御を行う役物制御基板１７１と、電源ライン１７２を介してネットワーク監視装置３６との間でＬＯＮによる情報転送を行う情報収集基板１７３（詳細は後述）とを有している。発射制御装置１６２は玉の発射を制御し、排出装置１６３は排出制御装置１６４からの信号に基づいて玉の排出を行う。排出制御装置１６４は玉貸信号や賞球信号に基づいて玉の排出を制御する。インターフェース回路１６５はカード式玉貸装置２５と遊技機２１における排出制御装置１６４、玉貸しスイッチ１６６等との間のインターフェース処理を行う。玉貸しスイッチ１６６は玉を購入するときに操作され、カード返却スイッチ１６７はプリペイドカードの返却を要望するときに操作される。カード度数表示器１６８はプリペイドカードの残高を表示し、玉貸し可能ＬＥＤ１６９はプリペイドカードの受け付けが有効であることを表示する。

【００３１】

（VI）情報収集基板の構成

次に、情報収集基板１７３の構成について説明する。図６は情報収集基板１７３の構成を示すブロック図である。図６において、情報収集基板１７３は電源ライン１７２を介してＬＯＮに接続されるため、前述したＬＯＮ対応のＮボード４２ａと同様の構成を有している。すなわち、情報収集基板１７３は分散形知的制御ネットワークＬＯＮシステム用のニューロンチップ２０１、クロック回路２０２、トランシーバ２０３、カップリング回路２０４、バス２０５、ＲＯＭ２０６、不揮発性メモリ２０７、ＤＰＲＡＭ２０８、ＲＡＭ２０９を有している。

ニューロンチップ２０１はＭＡＣＣＰＵ２１１、ネットワークＣＰＵ２１２、アプリケーションＣＰＵ２１３、ＲＡＭ２１４、ＥＥＰＲＯＭ２１５、ネットワーク通信ポート２１６、バス２１７およびＩ／Ｏポート２１０により構成される。

【００３２】

クロック回路２０２、トランシーバ２０３、カップリング回路２０４、ＲＯＭ２０６の機能は図３の場合と同様である。、不揮発性メモリ２０７は遊技情報（例えば、大当り情報等）を一時的に格納する（例えば、１日分の遊技情報を格納する）。

ＤＰＲＡＭ（デュアルポートＲＡＭ）２０８は情報収集基板１７３上のバス２０５と、役物制御基板１７１に配置されている後述の遊技用演算処理装置２２１（図７参照）との間の何れからでも内部のメモリ（双方向メモリ）へのデータの書き込み、メモリからのデータの読み出しが可能であり、この双方向メモリを介して情報収集基板１７３と遊技用演算処理装置２２１との間で相互にデータ転送が行われる。

また、ＤＰＲＡＭ２０８からは遊技用演算処理装置２２１の方に割り込みをかけるとき遊技用演算処理装置２２１への割り込み信号ＳＰ５が出力され、遊技用演算処理装置２２１からの割り込みをＤＰＲＡＭ２０８が受けるときは接続回路からの信号ＳＰ６がＤＰＲＡＭ２０８に入力され、Ｉ／Ｏポート２１０に送られる。

ＲＡＭ２０９は上位のネットワークから送信されてきた情報（識別情報等）を一時的に格

納し、電源がオフすると、格納していた情報は消滅する。

【００３３】

Ｉ／Ｏポート２１０にはカード式玉貸装置２５から玉貸信号ＳＰ７が入力されるとともに、回収玉ＳＷ２１８からの回収玉信号ＳＰ８が入力される。回収玉ＳＷ２１８は回収玉（アウト玉＋セーフ玉）を検出する。これらの信号ＳＰ７、ＳＰ８が入力されるのは、玉貸し情報（例えば、使用金額）や回収玉情報を遊技店１内のネットワークを介して情報管理装置２に送信するためであり、情報管理装置２に一旦蓄えられた情報は、さらに上位の第３者機関２４に送信されることになる。そして、第３者機関２４で当該遊技店１の情報（例えば、プリペイドカードの使用金額で、プリペイドカードの決済に関する情報等）が把握、管理される。第３者機関２４は全国共通のプリペイドカードを発行したり、遊技店１におけるプリペイドカードに関する精算を行ったりする。

【００３４】

（VII）役物制御基板の構成

次に、役物制御基板１７１の構成について説明する。図７は役物制御基板１７１の構成を示すブロック図である。図７において、役物制御基板１７１は遊技プログラムを格納したＲＯＭ、ＣＰＵ、ＲＡＭ等を内蔵してワンチップ化された遊技用演算処理装置２２１と、遊技用演算処理装置２２１の処理に必要なクロック信号を生成するクロック回路２２２と、各種情報信号を受け入れるフィルタ２２３と、フィルタ２２３からの信号をバス２２４を介して遊技用演算処理装置２２１に出力する入力ポート２２５と、遊技用演算処理装置２２１からの信号をバス２２４を介して受ける出力ポート２２６と、出力ポート２２６を介して入力される制御信号をドライブして各種駆動信号を生成して各機器に出力するドライバ２２７と、遊技に必要な効果音を生成する（あるいは音声合成を行ってもよい）サウンドジェネレータ２２８と、サウンドジェネレータ２２８からの音声信号を増幅して遊技機２１の所定箇所に配設されたスピーカー２２９に出力するアンプ２３０とによって構成される。

【００３５】

フィルタ２２３には第１種始動スイッチ２３１、カウントスイッチ２３２、継続スイッチ２３３、排出制御装置１６４からの賞球信号および情報収集基板１７３からの割り込み信号ＳＰ５が入力されている。第１種始動スイッチ２３１は特別図柄表示装置の図柄（特図）の変動表示を開始させる始動入賞口に玉が入賞したことを検出し、カウントスイッチ２３２は後述の変動入賞装置（アタッカー）に入った玉を検出する。継続スイッチ２３３は変動入賞装置に入った玉のうちいわゆる継続入賞（Ｖ入賞）した玉を検出する。

ドライバ２２７からは大入賞口としての変動入賞装置２４１の開閉動作を駆動するソレノイド、特図の始動記憶表示器２４２、装飾表示器２４３（例えば、各種装飾ランプやサイドランプ等）、表示制御装置２４４に制御信号が出力されるとともに、排出制御装置１６４に賞球数を知らせる信号が出力される。始動記憶表示器２４２は特図始動口が玉が入賞したとき４個の範囲内でその入賞玉数が記憶されたことを点灯させることで表示する。表示制御装置２４４は特別図柄表示装置の表示制御を行い、特別図柄表示装置は表示制御装置２４４からの表示制御用の信号に基づいて複数の識別情報（特図）を複数列で変動表示する。

【００３６】

（VIII）遊技用演算処理装置の構成

次に、遊技用演算処理装置２２１の構成について説明する。図８は遊技用演算処理装置２２１の構成を示すブロック図である。図８において、遊技用演算処理装置２２１は、遊技制御のための演算処理を行うＣＰＵコア３０１、遊技プログラムを格納したＲＯＭ３０２、ワークエリアの設定や制御に必要なデータの一時記憶等を行うＲＡＭ３０３、識別情報（ＩＤ）を記録するＥＥＰＲＯＭ３０４、各メモリにおけるデータの書き込み／読み出しを制御するメモリ制御回路３０５、外部バスのインターフェース処理を行う外部バスインターフェース３０６、所定のクロック信号を生成するクロックジェネレータ３０７、システムリセット、ユーザリセットや割り込み要求を検出してＣＰＵコア３０１に知らせるリ

セット／割込制御回路３０８、リセット／割込制御回路３０８からの信号およびクロックジェネレータ３０７からの信号の制御を行って外部端子より外部に出力する出力制御回路３０９、２本の外部クロック／タイマトリガ入力や２本のタイマ出力を内蔵してタイマモードおよびカウンタモードで作動するＣＴＣ３１０、内蔵デバイスおよび内蔵コントロール／ステータスレジスタ群のロケーションをメモリマップドＩ／Ｏ方式およびＩ／Ｏマップドド Ｉ／Ｏ方式によりデコードするアドレスデコーダ３１１、入出力ポートとしてのＰＩＯ３１２、アドレスデコーダ３１１からの信号やＰＩＯ３１２からの信号の制御を行って外部端子より外部に出力する出力制御回路３１３、８つのタイムアウト時間の中から選択しタイムアウトになると、ユーザリセットを発生させるウォッチドッグタイマ３１４およびバス３１５により構成される。

【００３７】

ここで、情報収集基板１７３は遊技装置の監視装置を構成する。ここでの遊技装置とは、遊技機２１のことである。また、情報収集基板１７３は役物制御装置に記録されている識別情報を読み込む識別情報読込手段、識別情報読込手段により読み込まれた識別情報の正当性を判別する識別情報判別手段、識別情報判別手段によって識別情報の正当性が認められた場合に役物制御装置へ遊技制御の動作許可の指令をするとともに、識別情報形式を変更した新識別情報を作成して送信し、該新識別情報の記録を指令する遊技制御許可手段を構成する。遊技制御許可手段は識別情報判別手段によって識別情報の非正当性が認められた場合に役物制御装置へ遊技制御の動作不許可を指令する。

また、情報収集基板１７３は遊技において発生した遊技情報を収集する遊技情報収集手段を構成する。

さらに、本実施例では役物制御装置に記録される識別情報は暗号化されており、識別判別手段は読み込まれた識別情報を判別可能に復号化して判別する。

また、情報収集基板１７３のＲＡＭ２０９は揮発性メモリであり、情報管理装置２より送信される識別情報形式情報を記憶する記憶手段を構成する。

【００３８】

次に、作用を説明する。

遊技店１における情報の管理、ネットワーク管理等は情報管理装置２によって行われ、情報管理装置２は遊技機２１の役物制御装置１７１に記録される識別情報の管理も行う。また、第３者機関２４に対しては遊技店１に関する必要な情報の転送が情報管理装置２を介して可能である。なお、以下の説明では各装置の符号は、適宜図面上あるいは説明上で都合により省略し、必要と思われる場合には各装置に符号を付して説明することにする。

【００３９】

Ａ．情報管理装置のメインルーチン

図９は情報管理装置２のメインルーチンを示すフローチャートである。このプログラムは情報管理装置２の電源投入（パワーオン）と同時に開始される。

図９に示すプログラムがスタートすると、まずステップＳ１０でＯＳブート処理を行う。これは、例えばシステムチェックを行った後、ＯＳ（オペレーティングシステム）のローディング等を行ってシステムを立上げる処理を行うものである。次いで、ステップＳ１２でメモリの初期化およびプログラムスタート処理を行う。これにより、ＲＡＭ５５のイニシャライズが行われ、ユーザプログラム（情報管理装置２で実行する遊技店１における情報の管理、ネットワーク管理等の処理プログラム）の処理が開始されることになる。次いで、ステップＳ１４で情報管理処理を行う（詳細はサブルーチンで後述）。次いで、ステップＳ１６でパワーオフ処理を行い、プログラムを終了する。パワーオフ処理では第３者機関２４から電源オフ指令が来た場合に情報管理装置２の電源をシャットダウンする。これにより、情報管理装置２の処理が停止する。

【００４０】

Ｂ．情報管理処理

図１０は情報管理装置２のメインルーチンにおける情報管理処理のサブルーチンを示すフローチャートである。このサブルーチンがスタートすると、まずステップＳ２０で第３者

機関処理を行う。これは、第３者機関との間における情報の送受信制御を行うものである（詳細はサブルーチンで後述）。次いで、ステップＳ２２でホール内装置処理を行う。これは、情報処理装置３および景品ＰＯＳ４からのデータ要求に基づいてデータを送信する処理を行うものである（詳細はサブルーチンで後述）。次いで、ステップＳ２４でネットワーク監視装置処理を行う。これは、主にネットワーク監視装置３３、３６に関する処理を行うものである（詳細はサブルーチンで後述）。次いで、ステップＳ２６で異常監視処理を行う。これは、ＩＤ情報等の異常、ネットワークの異常状態を表示する等の処理を行うものである（詳細はサブルーチンで後述）。次いで、ステップＳ２８でＡＴＭ送受信処理を行う。これは、ＡＴＭ交換機５に接続される各装置との間でデータのＡＴＭ送受信を行うものである。例えば、第３者機関２４との間もＡＴＭ送受信処理でデータ転送が行われる。

【００４１】

次いで、ステップＳ３０で閉店中であるか否かを判別する。閉店中かどうかは、閉店スイッチ６４が操作されたか否かで判断する。閉店スイッチ６４が操作されていなければ、ステップＳ２０に戻って上記ループを繰り返し、閉店スイッチ６４が操作されると、ステップＳ３２に進んでパワーオフ情報があるか否かを判別する。パワーオフ情報は第３者機関２４から送信されるものである。パワーオフ情報がなければ、ステップＳ２０に戻って上記ループを繰り返す。パワーオフ情報があると、今回のルーチンを終了し、メインルーチンにリターンする。これにより、情報管理装置２の電源がシャットダウンすることになる。

【００４２】

Ｃ．第３者機関処理

図１１は情報管理装置２のメインルーチンにおける第３者機関処理のサブルーチンを示すフローチャートである。このサブルーチンがスタートすると、まずステップＳ４０で第３者機関（特に、情報処理装置２４Ａ、以下同様）からデータ要求があるか否かを判別する。これは、第３者機関２４から当該遊技店１の情報管理装置２に対して必要なデータ要求があるかどうかを判断するものである。第３者機関からデータ要求があれば、ステップＳ４２に進んで第３者機関２４に要求のあった情報を記憶装置（ＨＤＤ５９）から取り出して送信設定する。送信設定すると、メインルーチンのステップＳ２８におけるＡＴＭ送受信処理で第３者機関２４に対して情報が送信されることになる。ステップＳ４２を経ると、ステップＳ４４に進む。また、ステップＳ４０で第３者機関からデータ要求がなければ、ステップＳ４４にジャンプする。

【００４３】

ステップＳ４４では、第３者機関からＩＤ等の受信があるか否かを判別する。ＩＤ等とは、遊技用演算処理装置２２１に記録されるチップＩＤ（以下、アミューズチップ用ＩＤという）、暗号鍵情報（以下、ＩＤ暗号鍵という）、復号鍵情報（以下、ＩＤ復号鍵という）、認証ＩＤをいう。第３者機関からＩＤ等の受信があれば、ステップＳ４６に進んで各機種のアミューズチップ用前回と次回のＩＤコードと、今回のＩＤ復号鍵と、次回のＩＤ暗号鍵と、認証ＩＤ等とをＲＡＭ５５に記憶する。アミューズチップ用のＩＤとは識別情報のことであり、開店時に毎回異ならせる処理が行われる。ＩＤ暗号鍵とは、アミューズチップ用のＩＤを暗号化するための暗号化情報、ＩＤ復号鍵とは、暗号化されたアミューズチップ用のＩＤを復号化するための復号化情報、認証ＩＤとは、情報管理装置２と第３者機関２４との間を相互認証するための第３者機関の認証ＩＤである。

ここで、遊技機２１の各機種毎にアミューズチップ用ＩＤが異なるので、機種毎に第３者機関２４から送信される。前回ＩＤコードとは、現時点で遊技用演算処理装置２２１に既に記録されているアミューズチップ用ＩＤのことである。次回ＩＤとは、今回のアミューズチップ用ＩＤが正当な場合に、それを更新するためのＩＤである。今回のＩＤ復号鍵とは、現時点で遊技用演算処理装置２２１に既に記録されているアミューズチップ用ＩＤ（すなわち、前回のＩＤ）を復号化するためのものである。次回のＩＤ暗号鍵とは、現時点で遊技用演算処理装置２２１に既に記録されているアミューズチップ用ＩＤ（前回のＩ

Ｄ）が正当な場合に、更新された次回ＩＤを暗号化するためのものである。
ステップＳ４６を経ると、ステップＳ４８に進む。また、ステップＳ４４で第３者機関からＩＤ等の受信がなければ、ステップＳ４８にジャンプする。

【００４４】

ステップＳ４８では第３者機関からパワーオフの受信があるか否かを判別する。パワーオフの受信があると、ステップＳ５０に進んでパワーオフ情報と時間を記憶装置（ＨＤＤ５９）に記憶する。これにより、メインルーチンにおいて情報管理装置２の電源がオフして停止し、そのオフ時間がＨＤＤ５９に記録されることになる。ステップＳ５０を経ると、ステップＳ５２に進む。また、ステップＳ４８で第３者機関からパワーオフの受信がなければ、ステップＳ５２にジャンプする。

ステップＳ５２では第３者機関からＩＤ異常時の部分復帰を受信したか否かを判別する。ＩＤ異常時の部分復帰とは、異常の端末（例えば、異常の遊技機）を除去し、正常な装置だけを開店させることである。ＩＤ異常時の部分復帰を受信していれば、ステップＳ５４に進んで異常な端末のアドレスを一時的に消去し、ステップＳ５６でＩＤ異常フラグをリセットする。これにより、例えば異常な遊技機のアドレスが一時的に消去され、その他の正常な遊技機で開店（すなわち、営業）することになる。ステップＳ５６を経ると、ステップＳ５８に進む。また、ステップＳ５２で第３者機関からＩＤ異常時の部分復帰を受信していなければ、ステップＳ５８にジャンプする。

【００４５】

ステップＳ５８ではネットワークに異常が発生（例えば、遊技機へのポーリングに応答が無いとき、あるいは通信異常等）したか否かを判別する。ネットワークに異常が発生していると、ステップＳ６０に進んで第３者機関に異常場所を記憶装置（ＨＤＤ５９）から取り出して送信設定する。これにより、ネットワークの異常場所が第３者機関に送信されることになる。ステップＳ６０を経ると、ステップＳ６２に進む。また、ステップＳ５８でネットワークに異常が発生していなければ、ステップＳ６２にジャンプする。

ステップＳ６２ではネットワークは異常から復帰したか否かを判別する。ネットワークが異常から復帰していれば、ステップＳ６４に進んで第３者機関に異常復帰場所を記憶装置（ＨＤＤ５９）から取り出して送信設定する。これにより、ネットワークの異常復帰場所が第３者機関に送信されることになる。ステップＳ６４を経ると、ステップＳ６６に進む。また、ステップＳ６２でネットワークが異常から復帰していなければ、ステップＳ６６にジャンプする。

【００４６】

ステップＳ６６ではＩＤに異常が発生したか否かを判別する。ＩＤに異常発生とは、例えばアミューズチップ用のＩＤが不当なものであるとか、認証ＩＤが不当で情報管理装置２と第３者機関２４との間が相互認証されない等の状態である。なお、ＩＤに異常が発生した場合、後述のＩＤチェック確認終了待ち処理でＩＤ異常フラグがセットされるから、ステップＳ６６ではＩＤ異常フラグをみて、判断することになる。

ＩＤに異常が発生していると、ステップＳ６８に進んで第３者機関にＩＤ異常を送信設定する。これにより、ＩＤに異常が発生したことが第３者機関に送信されることになる。ステップＳ６８を経ると、メインルーチンにリターンする。また、ステップＳ６６でＩＤに異常が発生していなければ、そのままメインルーチンにリターンする。

【００４７】

Ｄ．ホール内装置処理

図１２は情報管理装置２のメインルーチンにおけるホール内装置処理のサブルーチンを示すフローチャートである。このサブルーチンがスタートすると、まずステップＳ７０で情報処理装置３からデータ要求があるか否かを判別する。これは、遊技データ等が情報管理装置２にて収集されるので、収集元である情報管理装置２に必要なデータを情報処理装置３から要求するためである。情報処理装置３からデータ要求があると、ステップＳ７２に進んで要求のある遊技機２１に関するデータ（例えば、遊技データ）を記憶装置（ＨＤＤ５９）から取り出して送信設定する。送信設定すると、メインルーチンのステップＳ２８

におけるＡＴＭ送受信処理で情報処理装置３に対してデータが送信されることになる。ステップＳ７２を経ると、ステップＳ７４に進む。また、ステップＳ７０で情報処理装置３からデータ要求がなければ、ステップＳ７４にジャンプする。

【００４８】

ステップＳ７４では景品ＰＯＳ４からデータ要求があるか否かを判別する。これは、同様に景品交換データ等が情報管理装置２にて収集されるので、収集元である情報管理装置２に必要なデータを景品ＰＯＳ４から要求するためである。景品ＰＯＳ４からデータ要求があると、ステップＳ７６に進んで要求のあった景品ＰＯＳ４に関するデータ（例えば、景品交換データ）を記憶装置（ＨＤＤ５９）から取り出して送信設定する。送信設定すると、メインルーチンのステップＳ２８におけるＡＴＭ送受信処理で景品ＰＯＳ４に対してデータが送信されることになる。ステップＳ７６を経ると、次いで、ステップＳ７８へ進み、情報処理装置指令処理を行う。これは、情報処理装置３より遊技機２１（特に、役物制御装置１６１）への制御要求（打ち止め指令）があると、該当する遊技機へ制御コマンドを送信する処理を行うものである。ステップＳ７８を経ると、メインルーチンにリターンする。また、ステップＳ７４で景品ＰＯＳ４からデータ要求がなければ、ステップＳ７８へジャンプする。

【００４９】

Ｅ．ネットワーク監視装置処理

図１３は情報管理装置２のメインルーチンにおけるネットワーク監視装置処理のサブルーチンを示すフローチャートである。このサブルーチンがスタートすると、まずステップＳ８０でネットワーク監視装置との開店処理を行う。これは、第３者機関２４とのＩＤ認証、ネットワーク監視装置ＩＤ認証、情報収集基板ＩＤ認証、アミューズチップ用のＩＤ認証等を行うものである（詳細はサブルーチンで後述）。次いで、ステップＳ８２でネットワーク監視装置との閉店処理を行う。これは、アミューズチップ用のＩＤ消去等を行うものである（詳細はサブルーチンで後述）。次いで、ステップＳ８４でネットワーク監視装置のポーリング処理を行う。これは、情報管理装置２とネットワーク監視装置３３、３６との間でポーリングによる情報の送受信処理を行うものである（詳細はサブルーチンで後述）。次いで、ステップＳ８６でネットワーク監視装置の受信処理を行う。これは、ネットワーク監視装置３３、３６からデータを受信した場合に、データの記憶処理等を行うものである（詳細はサブルーチンで後述）。ステップＳ８６を経ると、メインルーチンにリターンする。

【００５０】

Ｅ－１．ネットワーク監視装置との開店処理

図１４はネットワーク監視装置処理におけるネットワーク監視装置との開店処理のサブルーチンを示すフローチャートである。このサブルーチンがスタートすると、まずステップＳ１００で処理番号によるステップ分岐の判断処理を行う。これは、分岐先に対応してセットされた処理番号に基づいて分岐先を決定するものである。分岐先のステップとしては、ステップＳ１０２～ステップＳ１２２があり、以下の通りである。なお、各処理の詳細は何れもサブルーチンで後述する。

ステップＳ１０２（開店確認処理）：処理Ｎｏ．０

ステップＳ１０４（第３者機関へ認証ＩＤ送信処理）：処理Ｎｏ．１

ステップＳ１０６（第３者機関からの認証ＩＤ受信処理）：処理Ｎｏ．２

ステップＳ１０８（第３者機関との認証ＩＤ比較処理）：処理Ｎｏ．３

ステップＳ１１０（ネットワーク監視装置へ認証ＩＤ送信処理）：処理Ｎｏ．４

【００５１】

ステップＳ１１２（ネットワーク監視装置からの認証ＩＤ受信待ち処理）：処理Ｎｏ．５

ステップＳ１１４（ネットワーク監視装置との認証ＩＤ比較処理）：処理Ｎｏ．６

ステップＳ１１６（ネットワーク監視装置からの情報収集基板の認証状態受信待ち処理）：処理Ｎｏ．７

ステップＳ１１８（ネットワーク監視装置からの情報収集基板の認証ＩＤ比較結果処理）

：処理Ｎｏ．８
ステップＳ１２０（アミューズチップ用のＩＤ等の送信処理）：処理Ｎｏ．９
ステップＳ１２２（ＩＤチェック確認終了待ち処理）：処理Ｎｏ．１０
上記ステップＳ１０２～ステップＳ１２２のうちの何れかのステップを経ると、ネットワーク監視装置処理にリターンする。
【００５２】
Ｅ－１－１．開店確認処理（処理Ｎｏ．０）
図１５はネットワーク監視装置との開店処理における開店確認処理のサブルーチンを示すフローチャートである。このサブルーチンがスタートすると、まずステップＳ１３０でカギから開店入力があるか否かを判別する。これは、情報管理装置２の開店スイッチ６３のカギが操作されて開店入力があるかどうかを判断するものである。カギから開店入力があると、ステップＳ１３２で処理番号を１にしてリターンする。これにより、次回ネットワーク監視装置との開店処理ではステップＳ１００の分岐処理で処理番号１に判断され、ステップＳ１０４の第３者機関へ認証ＩＤ送信処理（処理Ｎｏ．１）に分岐することになる。
ステップＳ１３０でカギから開店入力がなければ、今回のルーチンを終了してリターンする。
【００５３】
Ｅ－１－２．第３者機関へ認証ＩＤ送信処理（処理Ｎｏ．１）
図１６はネットワーク監視装置との開店処理における第３者機関へ認証ＩＤ送信処理のサブルーチンを示すフローチャートである。このサブルーチンがスタートすると、まずステップＳ１３４で第３者機関へ認証ＩＤの送信を設定する。これにより、情報管理装置２の認証ＩＤが第３者機関２４に送信されることになる。次いで、ステップＳ１３６で処理番号を２にしてリターンする。これにより、次回ネットワーク監視装置との開店処理ではステップＳ１００の分岐処理で処理番号２に判断され、ステップＳ１０６の第３者機関からの認証ＩＤ受信待ち処理（処理Ｎｏ．２）に分岐することになる。
【００５４】
Ｅ－１－３．第３者機関からの認証ＩＤ受信待ち処理（処理Ｎｏ．２）
図１７はネットワーク監視装置との開店処理における第３者機関からの認証ＩＤ受信待ち処理のサブルーチンを示すフローチャートである。このサブルーチンがスタートすると、まずステップＳ１３８で第３者機関からの認証ＩＤを受信したか否かを判別する。これは、情報管理装置２で第３者機関２４から送信されてくる認証ＩＤ（すなわち、第３者機関２４の認証ＩＤ）を受け取ったかどうかを判断するものである。第３者機関からの認証ＩＤを受信していると、ステップＳ１４０で処理番号を３にしてリターンする。すなわち、送信した情報管理装置２の認証ＩＤが正常であれば、第３者機関から認証ＩＤが送られてくる。これにより、次回ネットワーク監視装置との開店処理ではステップＳ１００の分岐処理で処理番号３に判断され、ステップＳ１０８の第３者機関との認証ＩＤ比較処理（処理Ｎｏ．３）に分岐することになる。
ステップＳ１３８で第３者機関からの認証ＩＤを受信していなければ、今回のルーチンを終了してリターンする。
【００５５】
Ｅ－１－４．第３者機関との認証ＩＤ比較処理（処理Ｎｏ．３）
図１８はネットワーク監視装置との開店処理における第３者機関との認証ＩＤ比較処理のサブルーチンを示すフローチャートである。このサブルーチンがスタートすると、まずステップＳ１５０で第３者機関の認証ＩＤは正常であるか否かを判別する。これは、情報管理装置２において第３者機関２４から受け取った認証ＩＤ（すなわち、第３者機関２４の認証ＩＤ）が正当なものであるかどうかを判断するものである。偽りの第３者機関２４ということも考えられるからである。例えば、いわゆるハッカーが第３者機関２４になりすまして、情報管理装置２にアクセスするような場合である。第３者機関の認証ＩＤが正常であれば、ステップＳ１５２に進んで処理番号を４にする。これにより、第３者機関の認

証ＩＤが正常である場合には、次回ネットワーク監視装置との開店処理ではステップＳ１００の分岐処理で処理番号４に判断され、ステップＳ１１０のネットワーク監視装置へ認証ＩＤ送信処理（処理Ｎｏ．４）に分岐することになる。次いで、ステップＳ１５４でＩＤ異常フラグをリセットしてリターンする。

【００５６】

一方、ステップＳ１５０で第３者機関の認証ＩＤが正常でなければ、ステップＳ１５６に分岐してＩＤ異常と、時間と、アドレスを記憶装置（ＨＤＤ５９）へ記憶する。これにより、第３者機関の認証ＩＤが異常であること、その異常を認識した時間および第３者機関２４のアドレスがＨＤＤ５９に記憶され、後で解析等のデータにされる。次いで、ステップＳ１５８で処理番号を０にする。これにより、第３者機関の認証ＩＤが異常である場合には、次回ネットワーク監視装置との開店処理ではステップＳ１００の分岐処理で処理番号０に判断され、ステップＳ１０２の開店確認処理（処理Ｎｏ．０）に分岐することになる。次いで、ステップＳ１６０でＩＤ異常フラグをセットしてリターンする。これにより、情報管理装置２と第３者機関２４が相互認証しないことになり、情報管理装置２からネットワーク監視装置３３、３６へのポーリングは中止されることになる。すなわち、遊技店内のネットワークは機能しなくなる。

【００５７】

Ｅ－１－５．ネットワーク監視装置へ認証ＩＤ送信処理（処理Ｎｏ．４）

図１９はネットワーク監視装置との開店処理におけるネットワーク監視装置へ認証ＩＤ送信処理のサブルーチンを示すフローチャートである。このサブルーチンがスタートすると、まずステップＳ１６２でネットワーク監視装置へ情報管理装置の認証ＩＤと情報収集基板用の認証ＩＤを送信設定する。これにより、ネットワーク監視装置３３、３６に対して情報管理装置の認証ＩＤが送信されるとともに、ネットワーク監視装置３６が受け持つ各遊技機２１の情報収集基板１７３に対応した情報収集基板用認証ＩＤがネットワーク監視装置３６に送信されることになる。次いで、ステップＳ１６４で処理番号を５にしてリターンする。これにより、次回ネットワーク監視装置との開店処理ではステップＳ１００の分岐処理で処理番号５に判断され、ステップＳ１１２のネットワーク監視装置からの認証ＩＤ受信待ち処理（処理Ｎｏ．５）に分岐することになる。

【００５８】

Ｅ－１－６．ネットワーク監視装置からの認証ＩＤ受信待ち処理（処理Ｎｏ．５）

図２０はネットワーク監視装置との開店処理におけるネットワーク監視装置からの認証ＩＤ受信待ち処理のサブルーチンを示すフローチャートである。このサブルーチンがスタートすると、まずステップＳ１７０でネットワーク監視装置からの認証ＩＤを受信したか否かを判別する。これは、情報管理装置２でネットワーク監視装置３３、３６から送信されてくる認証ＩＤ（すなわち、ネットワーク監視装置の認証ＩＤ）を受け取ったかどうかを判断するものである。ネットワーク監視装置３３、３６からの認証ＩＤを受信していると、ステップＳ１７２で処理番号を６にしてリターンする。これにより、次回ネットワーク監視装置との開店処理ではステップＳ１００の分岐処理で処理番号６に判断され、ステップＳ１１４のネットワーク監視装置との認証ＩＤ比較処理（処理Ｎｏ．６）に分岐することになる。

ステップＳ１７０でネットワーク監視装置からの認証ＩＤを受信していなければ、今回のルーチンを終了してリターンする。

【００５９】

Ｅ－１－７．ネットワーク監視装置との認証ＩＤ比較処理（処理Ｎｏ．６）

図２１はネットワーク監視装置との開店処理におけるネットワーク監視装置との認証ＩＤ比較処理のサブルーチンを示すフローチャートである。このサブルーチンがスタートすると、まずステップＳ１８０で各ネットワーク監視装置の認証ＩＤは正常であるか否かを判別する。これは、情報管理装置２において各ネットワーク監視装置３３、３６から受け取った認証ＩＤ（すなわち、ネットワーク監視装置の認証ＩＤ）が正当なものであるかどうかを判断するものである。偽りのネットワーク監視装置３３、３６ということも考えられ

るからである。最初のルーチンでは、１台目のネットワーク監視装置３３についての認証ＩＤから判断する。ネットワーク監視装置３３の認証ＩＤが正常であれば、ステップＳ１８２に進んで受信したネットワークアドレスを記憶装置（ＨＤＤ５９）へ記憶する。次いで、ステップＳ１８４に進む。

【００６０】

一方、ステップＳ１８０で各ネットワーク監視装置の認証ＩＤが異常であれば、ステップＳ１８６に分岐してＩＤ異常と、時間と、異常であるネットワーク監視装置のアドレスを記憶装置（ＨＤＤ５９）へ記憶する。これにより、ネットワーク監視装置３３の認証ＩＤが異常であること、その異常を認識した時間および各ネットワーク監視装置３３のアドレスがＨＤＤ５９に記憶され、後で解析等のデータにされる（第３者機関２４へ送信される）。次いで、ステップＳ１８４に進む。

ステップＳ１８４では全ネットワーク監視装置を確認したか否かを判別し、ＮＯのときはステップＳ１８８に進んで処理番号を５にする。これにより、次回のネットワーク監視装置との開店処理では再びステップＳ１１２のネットワーク監視装置からの認証ＩＤ受信待ち処理（処理Ｎｏ．５）に分岐し、次のネットワーク監視装置３６についての認証ＩＤを受信する。そして、本ルーチン（処理Ｎｏ．５）を繰り返し、ネットワーク監視装置３６について認証ＩＤの正当性の確認を行う。

【００６１】

ステップＳ１８４で全ネットワーク監視装置を確認すると、ステップＳ１９０に進んで処理番号を７にしてリターンする。これにより、全てのネットワーク監視装置３３、３６の認証ＩＤのチェックが終了すると、次回のネットワーク監視装置との開店処理ではステップＳ１００の分岐処理で処理番号７に判断され、ステップＳ１１６のネットワーク監視装置からの情報収集基板の認証状態受信待ち処理（処理Ｎｏ．７）に分岐することになる。

【００６２】

Ｅ－１－８．ネットワーク監視装置からの情報収集基板の認証状態受信待ち処理（処理Ｎｏ．７）

図２２はネットワーク監視装置との開店処理におけるネットワーク監視装置からの情報収集基板の認証状態受信待ち処理のサブルーチンを示すフローチャートである。このサブルーチンがスタートすると、まずステップＳ１９２でネットワーク監視装置から情報収集基板との認証状態を受信したか否かを判別する。これは、ネットワーク監視装置３６が受け持つ各遊技機２１の情報収集基板１７３とネットワーク監視装置３６との相互認証が正常に行われたか否かの情報を受信したかどうかを判断するものである。ＮＯのときは、ルーチンを終了してリターンする。したがって、ネットワーク監視装置３６から認証状態を受信するまで待つことになる。

ステップＳ１９２でＹＥＳのときは、ステップＳ１９４に進んで処理番号を８にしてリターンする。これにより、次回のネットワーク監視装置との開店処理ではステップＳ１００の分岐処理で処理番号８に判断され、ステップＳ１１８のネットワーク監視装置からの情報収集基板の認証ＩＤ比較結果処理（処理Ｎｏ．８）に分岐することになる。

【００６３】

Ｅ－１－９．ネットワーク監視装置からの情報収集基板の認証ＩＤ比較結果処理（処理Ｎｏ．８）

図２３はネットワーク監視装置との開店処理におけるネットワーク監視装置からの情報収集基板の認証ＩＤ比較結果処理のサブルーチンを示すフローチャートである。このサブルーチンがスタートすると、まずステップＳ２００でネットワーク監視装置と情報収集基板との認証結果は正常であるか否かを判別する。これは、情報管理装置２においてネットワーク監視装置３６と各遊技機２１の情報収集基板１７３の相互認証が正常であったかどうかを判断するものである。最初のルーチンでは、１台目の遊技機２１の情報収集基板１７３についての認証結果から判断する。１台目の遊技機２１の情報収集基板１７３の認証結果が正常であれば、ステップＳ２０２に進んで受信した情報収集基板アドレスを記憶装置（ＨＤＤ５９）へ記憶する。次いで、ステップＳ２０４に進む。

【００６４】
一方、ステップＳ２００で各情報収集基板の認証結果が異常であれば（最初のルーチンでは、１台目の遊技機２１の情報収集基板１７３についての認証結果が異常であれば）、ステップＳ２０６に分岐してＩＤ異常と、時間と、異常である情報収集基板のアドレスを記憶装置（ＨＤＤ５９）へ記憶する。これにより、当該情報収集基板の認証ＩＤが異常であること、その異常を認識した時間および当該情報収集基板のアドレスがＨＤＤ５９に記憶され、後で解析等のデータにされる（第３者機関２４へ送信される）。次いで、ステップＳ２０４に進む。
【００６５】
ステップＳ２０４では全情報収集基板の認証結果を確認したか否かを判別し、ＮＯのときはステップＳ２０８に進んで処理番号を７にする。これにより、次回のネットワーク監視装置との開店処理では再びステップＳ１１６のネットワーク監視装置からの情報収集基板の認証状態受信待ち処理（処理Ｎｏ．７）に分岐し、次の情報収集基板についての認証結果を受信する。そして、本ルーチン（処理Ｎｏ．８）を繰り返し、情報収集基板について認証結果の正当性の確認を行う。例えば、１台目の情報収集基板の認証結果の正当性の確認後は、２台目の情報収集基板の認証結果の正当性の確認を行う。このようにして、ネットワーク監視装置３６によって行われるネットワーク監視装置３６と情報収集基板１７３との相互認証結果について、全ての情報収集基板の認証ＩＤの正当性の確認を行う。
そして、ステップＳ２０４で全情報収集基板を確認すると、ステップＳ２１０に進んで処理番号を９にしてリターンする。これにより、全ての情報収集基板１７３の認証結果の確認後に、次回のネットワーク監視装置との開店処理ではステップＳ１００の分岐処理で処理番号９に判断され、ステップＳ１２０のアミューズチップ用のＩＤ等の送信処理（処理Ｎｏ．９）に分岐することになる。
【００６６】
Ｅ－１－１０．アミューズチップ用のＩＤ等の送信処理（処理Ｎｏ．９）
図２４はネットワーク監視装置との開店処理におけるアミューズチップ用のＩＤ等の送信処理のサブルーチンを示すフローチャートである。このサブルーチンがスタートすると、まずステップＳ２２０でＲＡＭメモリにアミューズチップ用のＩＤ等があるか否かを判別する。これは、情報管理装置２に対して第３者機関２４から送信されてきたＩＤ等がＲＡＭ５５に格納されているかどうかを判断するものである。ＲＡＭメモリにアミューズチップ用のＩＤ等があれば、ステップＳ２２２に進んでネットワーク監視装置を介して情報収集基板へアミューズチップ用ＩＤ等を送るため、対応するネットワーク監視装置へ機種毎のアミューズチップ用の前回と次回のＩＤと、今回のＩＤ復号鍵と、次回のＩＤ暗号鍵とをＲＡＭメモリ（ＲＡＭ５５）から取り出して送信設定する。これにより、島設備２２の中の遊技機２１の機種毎に対応するネットワーク監視装置３６（すなわち、情報収集基板）に、情報管理装置２から上記ＩＤ等が送信されることになる。
【００６７】
なお、本実施例では、島設備２２の中の遊技機２１に対応するネットワーク監視装置３６は１台の例であるが、ネットワーク監視装置が複数ある場合には、島設備２２の中の遊技機２１の機種毎に対応するネットワーク監視装置に情報管理装置２から上記ＩＤ等が送信される。
次いで、ステップＳ２２４で処理番号を１０にしてリターンする。これにより、次回のネットワーク監視装置との開店処理ではステップＳ１００の分岐処理で処理番号１０に判断され、ステップＳ１２２のＩＤチェック確認終了待ち処理（処理Ｎｏ．１０）に分岐することになる。
ステップＳ２２０でＲＡＭメモリに第３者機関より受信したアミューズチップ用のＩＤ等がなければ、今回のルーチンを終了してリターンする（すなわち、次の処理へは移行できない）。
【００６８】
Ｅ－１－１１．ＩＤチェック確認終了待ち処理（処理Ｎｏ．１０）

図２５はネットワーク監視装置との開店処理におけるＩＤチェック確認終了待ち処理のサブルーチンを示すフローチャートである。このサブルーチンがスタートすると、まずステップＳ２３０で情報収集基板から確認終了情報があるか否かを判別する。これは、情報収集基板１７３が役物制御基盤１７１に設けられている遊技用演算処理装置２２１のＩＤの正当性判断（チェック）の確認の終了をネットワーク監視装置３６を介して送ってくるので、その情報があるかどうかを判断するものである。各情報収集基板から確認終了情報があれば、ステップＳ２３２に進んで情報収集基板アドレスと、確認したときの時間と、遊技用演算処理装置の正当性の確認終了結果がＯＫであるか又はＮＧ（ＩＤ異常を含む）であるかの情報（すなわち、ＯＫ情報又はＮＧ情報）を記憶装置（ＨＤＤ５９）に記憶し、ステップＳ２３４に進む。また、ステップＳ２３０で各ネットワーク監視装置から確認終了情報がなければ、ステップＳ２３２をジャンプしてステップＳ２３４に進む。

【００６９】

ステップＳ２３４では全ネットワーク監視装置（すなわち、全情報収集基板）からＩＤチェック情報を取得したか否かを判別する。これは、遊技機２１の配置されている島設備２２に対応するネットワーク監視装置３６から全情報収集基板の情報を取得したかどうかを判断するものである。全ネットワーク監視装置（全情報収集基板）から情報を取得していない場合には、そのままリターンする。これにより、本ルーチンが繰り返される。そして、本ルーチンを繰り返すことにより、全ネットワーク監視装置（全情報収集基板）から情報を取得すると、ステップＳ２３６に進んでＩＤの異常等があるか否かを記憶装置（ＨＤＤ５９）に記憶されるＩＤ異常情報より判別し、ＩＤの異常があればステップＳ２３８でＩＤ異常フラグをセットする。ＩＤ異常フラグがセットされることにより、例えば第３者機関処理（図１１）等でＩＤに異常が発生したかどうかを判断することが可能になるとともに、各装置間の相互認証、アミューズチップのＩＤ確認が異常であるので、店内のネットワークは機能を停止する。

次いで、ステップＳ２４０で処理番号を０にしてリターンする。これにより、次回のネットワーク監視装置との開店処理ではステップＳ１００の分岐処理で処理番号０に判断され、ステップＳ１０２の開店確認処理（処理Ｎｏ．０）に分岐することになる。したがって、ＩＤ異常フラグがセットされると、安全のため他の処理を停止する。すなわち、ネットワーク監視装置３６ではポーリングを中止し、ネットワーク監視装置３６より下位側の通信ネットワークが不能動化されることになる。

また、ステップＳ２３６でＩＤの異常等がなければ、ステップＳ２３８をジャンプしてステップＳ２４０に進む。

【００７０】

Ｅ－２．ネットワーク監視装置との閉店処理

図２６はネットワーク監視装置処理におけるネットワーク監視装置との閉店処理のサブルーチンを示すフローチャートである。このサブルーチンがスタートすると、まずステップＳ２５０で処理番号によるステップ分岐の判断処理を行う。これは、分岐先に対応してセットされた処理番号に基づいて分岐先を決定するものである。分岐先のステップとしては、ステップＳ２５２～ステップＳ２５６があり、以下の通りである。なお、各処理の詳細は何れもサブルーチンで後述する。

ステップＳ２５２（閉店確認処理）：処理Ｎｏ．０

ステップＳ２５４（アミューズチップ用のＩＤ消去の送信処理）：処理Ｎｏ．１

ステップＳ２５６（アミューズチップ用のＩＤ消去ＡＣＫ待ち処理）：処理Ｎｏ．２

上記ステップＳ２５２～ステップＳ２５６のうちの何れかのステップを経ると、ネットワーク監視装置処理にリターンする。

【００７１】

Ｅ－２－１．閉店確認処理（処理Ｎｏ．０）

図２７はネットワーク監視装置との閉店処理における閉店確認処理のサブルーチンを示すフローチャートである。このサブルーチンがスタートすると、まずステップＳ２６０でカギから閉店入力があるか否かを判別する。これは、情報管理装置２の閉店ＳＷ６４のカギ

が操作されて閉店入力があるかどうかを判断するものである。カギから閉店入力があると、ステップＳ２６２で処理番号を１にしてリターンする。これにより、次回ネットワーク監視装置との閉店処理ではステップＳ２５０の分岐処理で処理番号１に判断され、ステップＳ２５６のアミューズチップ用のＩＤ消去の送信処理（処理Ｎｏ．１）に分岐することになる。
ステップＳ２６０でカギから閉店入力がなければ、今回のルーチンを終了してリターンする。
【００７２】
Ｅ－２－２．アミューズチップ用のＩＤ消去の送信処理（処理Ｎｏ．１）
図２８はネットワーク監視装置との閉店処理におけるアミューズチップ用のＩＤ消去の送信処理のサブルーチンを示すフローチャートである。このサブルーチンがスタートすると、まずステップＳ２７０でアミューズチップ用のＩＤ消去を対応するネットワーク監視装置へ送信設定する。これにより、遊技機２１の配置されている島設備２２に対応するネットワーク監視装置３６にアミューズチップ用のＩＤ消去指令が送られ、対応するネットワーク監視装置３６のＲＡＭ１０９に格納されているアミューズチップ用のＩＤ等が消去されることになるとともに、アミューズチップ用ＩＤ消去は情報収集基板１７３に送られ、情報収集基板１７３のＲＡＭ２０９に格納されているアミューズチップ用のＩＤ等が消去される。次いで、ステップＳ２７２で処理番号を２にしてリターンする。これにより、次回ネットワーク監視装置との閉店処理ではステップＳ２５０の分岐処理で処理番号２に判断され、ステップＳ２５６のアミューズチップ用のＩＤ消去ＡＣＫ待ち処理（処理Ｎｏ．２）に分岐することになる。
【００７３】
Ｅ－２－３．アミューズチップ用のＩＤ消去ＡＣＫ待ち処理（処理Ｎｏ．２）
図２９はネットワーク監視装置との閉店処理におけるアミューズチップ用のＩＤ消去ＡＣＫ待ち処理のサブルーチンを示すフローチャートである。このサブルーチンがスタートすると、まずステップＳ２８０で各ネットワーク監視装置からＩＤ消去ＡＣＫがあるか否かを判別する。これは、情報管理装置２で各ネットワーク監視装置等へ指令したＩＤ消去に対して、そのＡＣＫが返ってきたかどうかを判断するものである。各ネットワーク監視装置からＩＤ消去ＡＣＫがあると、ステップＳ２８２でネットワーク監視装置アドレスと、時間とを記憶装置（ＨＤＤ５９）へ記憶し、ステップＳ２８４に進む。これにより、ＩＤ消去指令に対してそのＡＣＫが返ってきたネットワーク監視装置と、ＡＣＫが返ってきた時間がＨＤＤ５９に記憶され、第３者機関２４で把握することが可能になる。また、ステップＳ２８０で各ネットワーク監視装置からＩＤ消去ＡＣＫがなければ、ステップＳ２８２をジャンプしてステップＳ２８４に進む。
【００７４】
ステップＳ２８４では対応するネットワーク監視装置（すなわち、情報収集基板）から情報を取得したか否かを判別する。これは、遊技機２１の配置されている島設備２２に対応するネットワーク監視装置から全情報収集基板について、ＩＤ消去ＡＣＫという情報を取得したか否かを判断するものである。本実施例では遊技機２１の配置されている島設備２２に対応するネットワーク監視装置３６は１台であるため、ネットワーク監視装置３６から全情報収集基板についてＩＤ消去ＡＣＫという情報を取得したかどうかで判断する。
【００７５】
対応するネットワーク監視装置（情報収集基板）から情報を取得していなければ、そのままリターンする。これにより、本ルーチンが繰り返される。そして、本ルーチンを繰り返すことにより、全ネットワーク監視装置（情報収集基板）からＩＤ消去ＡＣＫを取得すると、ステップＳ２８６に進んでアミューズチップ用のＩＤ等をＲＡＭメモリ（ＲＡＭ５５）から消去する。これにより、情報管理装置２で格納しておいたアミューズチップ用のＩＤ等が消去され、仮に情報管理装置２の情報が盗用にあっても、重要なアミューズチップ用のＩＤ等が盗まれることはない。次いで、ステップＳ２８８で処理番号を０にしてリターンする。これにより、次回のネットワーク監視装置との閉店処理ではステップＳ２５０

の分岐処理で処理番号０に判断され、ステップＳ２５２の閉店確認処理（処理Ｎｏ．０）に再び分岐することになる。

【００７６】

このように、遊技店１の閉店時には端末側（遊技機２１の情報収集基板１７３）から順次アミューズチップ用のＩＤを消去していき、そして、最後に当該情報管理装置２のＩＤも消去する。したがって、閉店後は、遊技店１には重要な情報は残っていないことになる。これは、遊技装置の監視装置としての情報収集基板１７３が情報管理装置２より送信される識別情報形式情報を記憶する記憶手段（揮発性メモリのＲＡＭ２０９）を備えており、遊技装置の監視装置が動作を停止するとき（例えば、遊技店１の閉店時）には、当該記憶手段（ＲＡＭ２０９）に記憶していた識別情報形式情報を消去する消去手段の機能を実現することに相当する。

【００７７】

Ｅ－３．ネットワーク監視装置のポーリング処理

図３０はネットワーク監視装置処理におけるネットワーク監視装置のポーリング処理のサブルーチンを示すフローチャートである。このサブルーチンがスタートすると、まずステップＳ３００で処理番号によるステップ分岐の判断処理を行う。これは、分岐先に対応してセットされた処理番号に基づいて分岐先を決定するものである。分岐先のステップとしては、ステップＳ３０２～ステップＳ３１０があり、以下の通りである。なお、各処理の詳細は何れもサブルーチンで後述する。

ステップＳ３０２（ポーリング処理）：処理Ｎｏ．０

ステップＳ３０４（ポーリング応答確認処理）：処理Ｎｏ．１

ステップＳ３０６（セレクティング処理）：処理Ｎｏ．２

ステップＳ３０８（データ送信処理）：処理Ｎｏ．３

ステップＳ３１０（送信に対するＡＣＫ待ち処理）：処理Ｎｏ．４

上記ステップＳ３０２～ステップＳ３１０のうちの何れかのステップを経ると、ネットワーク監視装置処理にリターンする。

【００７８】

Ｅ－３－１．ポーリング処理（処理Ｎｏ．０）

図３１はネットワーク監視装置のポーリング処理におけるポーリング処理のサブルーチンを示すフローチャートである。このサブルーチンがスタートすると、まずステップＳ３２０でＩＤ異常フラグがセット中であるか否かを判別する。ＩＤ異常フラグがセット中とは、例えば認証エラー、アミューズチップ用ＩＤの異常等がある。ＩＤ異常フラグがセット中であれば、以後の処理は行わずにリターンする。

ＩＤ異常フラグがセット中でなければ、ステップＳ３２２に進んでアミューズチップ用ＩＤ等は消去されているか否かを判別する。これは、閉店することにより、情報管理装置２におけるＲＡＭ５５からアミューズチップ用ＩＤ等が消去されているかどうかを判断するものである。アミューズチップ用ＩＤ等が既に消去されていれば、ポーリング処理を行わずそのままリターンする。すなわち、閉店後ポーリングを停止するためである。一方、アミューズチップ用ＩＤ等が消去されていなければ、ステップＳ３２４でポーリングポインタを更新する。ポーリングポインタは複数のネットワーク監視装置３３、３６を順次指定していくものである。したがって、ポーリングポインタの更新とは、次のネットワーク監視装置を指定するように、ポーリングポインタの値をインクリメントするものである。

【００７９】

次いで、ステップＳ３２６でポーリングポインタによりネットワーク監視装置のアドレスを取り出す。これは、更新されたポーリングポインタによって次のネットワーク監視装置を指定するものである。次いで、ステップＳ３２８でアドレスを設定したポーリング要求を送信する。これにより、更新されたポーリングポインタによって指定された次のネットワーク監視装置に対してポーリング要求が送信される。次いで、ステップＳ３３０でポーリング応答確認タイマをクリアする。ポーリング応答確認タイマは、ポーリング要求を送信したネットワーク監視装置に対して所定時間内に応答があるかどうかを判断するための

タイマである。次いで、ステップＳ３３２で処理番号を１にしてリターンする。これにより、次回のネットワーク監視装置のポーリング処理ではステップＳ３００の分岐処理で処理番号１に判断され、ステップＳ３０２のポーリング処理（処理Ｎｏ．１）に分岐することになる。

【００８０】

Ｅ－３－２．ポーリング応答確認処理（処理Ｎｏ．１）

図３２はネットワーク監視装置のポーリング処理におけるポーリング応答確認処理のサブルーチンを示すフローチャートである。このサブルーチンがスタートすると、まずステップＳ３４０で要求したネットワーク監視装置（例えば、ポーリングをかけたネットワーク監視装置）からポーリングＡＣＫ又はデータを受信したか否かを判別する。これは、正常であればポーリングをかけたネットワーク監視装置から情報管理装置２に対して必ずポーリングＡＣＫ又はデータが返ってくるからである。要求したネットワーク監視装置からポーリングＡＣＫ又はデータを受信した場合には、ステップＳ３４２に進んでネットワークに前回異常がありか否かを判別する。異常がなければ、ステップＳ３４６にジャンプして処理番号を２にしてリターンする。これにより、次回のネットワーク監視装置のポーリング処理ではステップＳ３００の分岐処理で処理番号２に判断され、ステップＳ３０６のセレクティング処理（処理Ｎｏ．２）に分岐することになる。

【００８１】

一方、ステップＳ３４２でネットワークに前回異常があれば、ステップＳ３４４に進んで異常解除のネットワークアドレスと時間を記憶装置（ＨＤＤ５９）へ記憶してステップＳ３４６に進む。これは、今回のルーチンで要求したネットワーク監視装置から正常にポーリングＡＣＫ又はデータを受信したことから、ネットワークの異常が解除されたと判断して、異常が解除されたネットワークアドレスおよび解除の時間をＨＤＤ５９に記憶するものである。

【００８２】

ステップＳ３４０で要求したネットワーク監視装置からポーリングＡＣＫ又はデータを受信しない場合には、ステップＳ３４８に進んでポーリング応答確認タイマはオーバーしているか否かを判別する。ポーリング応答確認タイマはポーリング要求を送信したネットワーク監視装置に対して所定時間内に応答があるかどうかを判断するためのタイマであるから、ポーリング応答確認タイマがオーバーしていれば、応答不能と判断してステップＳ３５０に進み、応答不能のネットワークアドレスと時間を記憶装置（ＨＤＤ５９）へ記憶する。これにより、応答不能のネットワーク監視装置が記録される。なお、応答不能のネットワーク監視装置の記録は第３者機関２４によって把握される。次いで、ステップＳ３５２で処理番号を０にしてリターンする。これにより、次回のネットワーク監視装置のポーリング処理ではステップＳ３００の分岐処理で処理番号０に判断され、ステップＳ３０２のポーリング処理（処理Ｎｏ．０）に分岐することになる。

一方、ステップＳ３４８でポーリング応答確認タイマがオーバーしていなければ、今回のルーチンを終了しリターンする。

【００８３】

Ｅ－３－３．セレクティング処理（処理Ｎｏ．２）

図３３はネットワーク監視装置のポーリング処理におけるセレクティング処理のサブルーチンを示すフローチャートである。このサブルーチンがスタートすると、まずステップＳ３６０で要求したネットワーク監視装置（例えば、情報管理装置２の要求によりポーリングをかけたネットワーク監視装置）へ送信データがあるか否かを判別する。送信データがなければステップＳ３６２に分岐して処理番号を０にしてリターンする。これにより、次のポーリングポインタで指定されるネットワーク監視装置に移行することになる。

【００８４】

ステップＳ３６０で要求したネットワーク監視装置へ送信データがある場合には、ステップＳ３６４に進んでポーリングポインタによりアドレスを取り出す。これにより、ポーリングポインタに対応したネットワーク監視装置のアドレスが取り出される。次いで、ステ

ップＳ３６６でアドレスを設定し、セレクティング要求を送信する。セレクティング要求を送信することにより、アドレスで指定されたネットワーク監視装置が受信待ちになる。次いで、ステップＳ３６８でセレクティング応答確認タイマをクリアする。セレクティング応答確認タイマは、セレクティング要求を送信したネットワーク監視装置に対して所定時間内に応答があるかどうかを判断するためのタイマである。次いで、ステップＳ３７０で処理番号を３にしてリターンする。これにより、次回のネットワーク監視装置のポーリング処理ではステップＳ３００の分岐処理で処理番号３に判断され、ステップＳ３０８のデータ送信処理（処理Ｎｏ．３）に分岐することになる。

【００８５】

Ｅ－３－４．データ送信（処理Ｎｏ．３）

図３４はネットワーク監視装置のポーリング処理におけるデータ送信のサブルーチンを示すフローチャートである。このサブルーチンがスタートすると、まずステップＳ３８０で要求したネットワーク監視装置（例えば、情報管理装置２の要求によりセレクティングをかけたネットワーク監視装置）からセレクティングＡＣＫを受信したか否かを判別する。これは、セレクティング要求をかけたネットワーク監視装置が確実にセレクティングを受けたかどうかを判断するものである。要求したネットワーク監視装置からセレクティングＡＣＫを受信した場合には、ステップＳ３８２に進んでポーリングポインタよりアドレスを取り出す。これにより、ポーリングポインタに対応したネットワーク監視装置のアドレスが取り出される。次いで、ステップＳ３８４でアドレスを設定し、データを送信設定する。これにより、アドレスで指定されたネットワーク監視装置に対して情報管理装置２からデータが送信されることになる。

【００８６】

次いで、ステップＳ３８６でデータ応答確認タイマをクリアする。データ応答確認タイマは、データを送信したネットワーク監視装置に対して所定時間内に応答があるかどうかを判断するためのタイマである。次いで、ステップＳ３８８で処理番号を４にしてリターンする。これにより、次回のネットワーク監視装置のポーリング処理ではステップＳ３００の分岐処理で処理番号４に判断され、ステップＳ３１０の送信に対するＡＣＫ待ち処理（処理Ｎｏ．４）に分岐することになる。

一方、ステップＳ３８０で要求したネットワーク監視装置からセレクティングＡＣＫを受信しない場合には、ステップＳ３９０に進んでセレクティング応答確認タイマはオーバーしているか否かを判別する。セレクティング応答確認タイマはセレクティング要求を送信したネットワーク監視装置に対して所定時間内に応答があるかどうかを判断するためのタイマであるから、セレクティング応答確認タイマがオーバーしていれば、応答不能と判断してステップＳ３９２に進み、セレクティング応答不能のネットワークアドレスと時間を記憶装置（ＨＤＤ５９）へ記憶する。これにより、セレクティング応答不能のネットワーク監視装置が記録される。同様に、セレクティング応答不能のネットワーク監視装置の記録は第３者機関２４によって把握される。

次いで、ステップＳ３９４で処理番号を０にしてリターンする。これにより、次回のネットワーク監視装置のポーリング処理ではステップＳ３００の分岐処理で処理番号０に判断され、ステップＳ３０２のポーリング処理（処理Ｎｏ．０）に分岐することになる。

【００８７】

Ｅ－３－５．送信に対するＡＣＫ待ち処理（処理Ｎｏ．４）

図３５はネットワーク監視装置のポーリング処理における送信に対するＡＣＫ待ち処理のサブルーチンを示すフローチャートである。このサブルーチンがスタートすると、まずステップＳ４００で送信したネットワーク監視装置からＡＣＫを受信したか否かを判別する。これは、今回送信したデータ（例えば、相互認証のデータや通常の送信情報等）をネットワーク監視装置が受けたか否かを判断するものである。送信したネットワーク監視装置からＡＣＫを受信していれば、ステップＳ４０２で処理番号を０にしてリターンする。これにより、次回のネットワーク監視装置のポーリング処理ではステップＳ３００の分岐処理で処理番号０に判断され、ステップＳ３０２のポーリング処理（処理Ｎｏ．０）に分岐

することになる。
【００８８】
ステップＳ４００で送信したネットワーク監視装置からＡＣＫを受信していない場合には、ステップＳ４０４に分岐してデータ応答確認タイマはオーバーしているか否かを判別する。データ応答確認タイマはデータを送信したネットワーク監視装置に対して所定時間内に応答があるかどうかを判断するためのタイマであるから、データ応答確認タイマがオーバーしていれば、応答不能と判断してステップＳ４０６に進み、データ応答確認不能のネットワークアドレスと時間を記憶装置（ＨＤＤ５９）へ記憶する。これにより、データ応答確認不能のネットワーク監視装置が記録される。データ応答確認不能のネットワーク監視装置の記録は第３者機関２４によって把握される。
次いで、ステップＳ４０８で処理番号を０にしてリターンする。これにより、次回のネットワーク監視装置のポーリング処理ではステップＳ３００の分岐処理で処理番号０に判断され、ステップＳ３０２のポーリング処理（処理Ｎｏ．０）に分岐することになる。
【００８９】
Ｅ－４．ネットワーク監視装置の受信処理
図３６はネットワーク監視装置処理におけるネットワーク監視装置の受信処理のサブルーチンを示すフローチャートである。このサブルーチンがスタートすると、まずステップＳ４１０でネットワーク監視装置からデータ（例えば、相互認証のデータや通常の送信情報等）を受信したか否かを判別する。データを受信していなければ、今回のルーチンを終了してリターンする。
ネットワーク監視装置からデータを受信した場合には、ステップＳ４１２に進んで今回受信したデータを記憶装置（ＨＤＤ５９）に記憶する。次いで、ステップＳ４１４でネットワーク異常パケットがあるか否かを判別する。これは、今回受信したデータを全てサーチしてネットワーク異常パケットがあるか否かを判断するものである。ネットワーク異常パケットがあれば、ステップＳ４１４でネットワーク監視装置と情報収集基板間のネットワークの異常（例えば、ポーリングの無応答のような異常）を設定し、ステップＳ４１８に進む。ネットワークの異常の設定では、例えばネットワーク異常設定フラグを立てて、情報管理装置２で把握できるようにする。また、ネットワーク異常パケットがなければ、ステップＳ４１６をジャンプしてステップＳ４１８に進む。
【００９０】
ステップＳ４１８ではネットワーク復帰パケットがあるか否かを判別する。これは、今回受信したデータを全てサーチしてネットワーク復帰パケットがあるか否かを判断するものである。ネットワーク復帰パケットがあれば、ステップＳ４２０でネットワーク監視装置と情報収集基板間のネットワークの復帰（例えば、ポーリングの無応答が解消した後の復帰）を設定し、リターンする。ネットワークの復帰の設定では、例えばネットワーク異常設定フラグをクリアして、情報管理装置２で把握できるようにする。
ステップＳ４１８でネットワーク復帰パケットがなければ、今回のルーチンを終了してリターンする。
【００９１】
Ｆ．異常表示処理
図３７は情報管理装置２のメインルーチンにおける異常表示処理のサブルーチンを示すフローチャートである。このサブルーチンがスタートすると、まずステップＳ４３０でネットワークに異常があるか否かを判別する。ここでのネットワークとは、情報管理装置２で管理可能なネットワーク（例えば、情報管理装置２とネットワーク監視装置３３、３６間のネットワーク）のことである。ネットワークに異常があれば、ステップＳ４３２で異常場所の表示を行い、ステップＳ４３４に進む。これは、ネットワークの異常場所のアドレスを表示装置６２に表示することにより行う。
【００９２】
ネットワークに異常がなければ、ステップＳ４３２をジャンプしてステップＳ４３４に進む。ステップＳ４３４ではネットワーク監視装置と情報収集基板間のネットワークに異常

（例えば、送信不良等）があるか否かを判別する。ネットワーク監視装置と情報収集基板間のネットワークに異常があれば、ステップＳ４３６で異常場所の表示を行い、ステップＳ４３８に進む。異常場所の表示では、ネットワーク監視装置と情報収集基板間における異常場所のアドレスを表示装置６２に表示する。
ネットワーク監視装置と情報収集基板間のネットワークに異常がなければ、ステップＳ４３６をジャンプしてステップＳ４３８に進む。ステップＳ４３８ではその他の異常（例えば、相互認証異常、アミューズチップの非正当性）があるか否かを判別する。その他の異常があれば、ステップＳ４４０でその他の異常場所の表示を行い、リターンする。その他の異常場所の表示では、例えば相互認証異常あるいはアミューズチップの非正当性が発生した場所のアドレスを表示装置６２に表示する。その他の異常がなければ、ステップＳ４４０をジャンプしてリターンする。

【００９３】
以上で、情報管理装置２のプログラムの説明を終了し、次いで、ネットワーク監視装置３３、３６のプログラムについて説明する。
Ｇ．ネットワーク監視装置のメインルーチン
図３８はネットワーク監視装置３３、３６のメインルーチンを示すフローチャートである。このプログラムはネットワーク監視装置３３、３６の電源投入（パワーオン）と同時に開始される。
図３８に示すプログラムがスタートすると、まずステップＳ４５０でリセットタスクを実行する。これは、タイマタスクのタイマ設定、ＤＰＲＡＭ１０８のクリア、Ｉ／Ｏポート１１０のイニシャライズ等を行うものである。次いで、ステップＳ４５２で時分割処理を行う。これは、以下の何れかのタスクに時分割で分岐するもので、どこに分岐するかは、行き先タスクの起動がかかることよって決定される。分岐先タスクとしては、以下のものがある。

【００９４】
ステップＳ４５４：情報管理装置送受信タスク
情報管理装置２との間でＤＰＲＡＭ１０８を介して通信制御装置３２、３５との情報の転送を行うもので、通信制御装置３２、３５からの割り込み要求で、このタスクが起動する（詳細はサブルーチンで後述）。
ステップＳ４５６：情報収集基板受信タスク
情報収集基板１７３を介して各台の遊技データおよび情報収集基板１７３からのデータを受信するもので、ＬＯＮで各情報収集基板からデータを受け取ったときにタスク起動要求がかかり、このタスクが起動する（詳細はサブルーチンで後述）。
ステップＳ４５８：タイマタスク
相互認証、アミューズチップＩＤ消去、異常表示等を行うもので、内部割込タイマで設定された時間による所定の時間毎の割り込みによりタスク起動要求がかかり、このタスクが起動する（詳細はサブルーチンで後述）。
上記ステップＳ４５４～ステップＳ４５８の何れかのタスクを経ると、ステップＳ４５２に戻って処理を繰り返す。

【００９５】
Ｈ．情報管理装置送受信タスク
図３９はネットワーク監視装置３３、３６のメインルーチンにおける情報管理装置送受信タスクのサブルーチンを示すフローチャートである。このタスクがスタートすると、まずステップＳ４６０でタスクの起動要求があるか否かを判別する。この場合のタスク起動要求は、通信制御装置３２、３５からの割り込み要求でかかる。タスクの起動要求がなければ、以後の処理を行わずにタスクを終了する。
タスクの起動要求があると、ステップＳ４６２でタスクの起動要求をかけた割り込み信号をリセットし、ステップＳ４６４でＤＰＲＡＭ１０８のデータを読み込む。ＤＰＲＡＭ１０８のデータとは、通信制御装置３２、３５を介して送られてきた情報管理装置２からの送信データである。次いで、ステップＳ４６６でＤＰＲＡＭ１０８から読み込んだデータ

はポーリング要求であるか否かを判別し、ポーリング要求であればステップＳ４６８で情報管理装置２へ送信データありか否かを判別する。これは、情報管理装置２への未送信のデータがあるかどうかを判断するものである。情報管理装置２へ送信データがある場合には、ステップＳ４７０でＤＰＲＡＭ１０８へ送信メモリ（ＲＡＭ１０９）の送信データを書き込み、ステップＳ４７４に進む。これにより、ＲＡＭ１０９に格納されている送信データがＤＰＲＡＭ１０８に書き込まれ、通信制御装置３２、３５に送信する前の準備が行われる。

【００９６】

ステップＳ４６８で情報管理装置２への送信データがなければ、ステップＳ４７２に分岐してＤＰＲＡＭ１０８へポーリングＡＣＫを書き込み、ステップＳ４７４に進む。ステップＳ４７４ではＤＰＲＡＭ１０８に割り込みを発生させ、ＤＰＲＡＭ１０８に書き込んだデータを送信し、ステップＳ４７６に進む。これにより、ネットワーク監視装置３３、３６から通信制御装置３２、３５に対してＤＰＲＡＭ１０８に書き込んだデータが送信される。すなわち、情報管理装置２へデータが送信される。

一方、ステップＳ４６６でＤＰＲＡＭ１０８から読み込んだデータがポーリング要求でなければ、ステップＳ４７６にジャンプする。

【００９７】

ステップＳ４７６ではセレクティング要求であるか否かを判別し、セレクティング要求であればステップＳ４７８で受信可能フラグをセットする。これは、情報管理装置２からネットワーク監視装置３３（あるいは３６）がセレクトされた場合に、データを受信可能であるとするフラグを立てるものである。次いで、ステップＳ４８０でＤＰＲＡＭ１０８へセレクティングＡＣＫを書き込み、ステップＳ４８２でＤＰＲＡＭ１０８に割り込みを発生させて送信し、ステップＳ４８４に進む。これにより、ネットワーク監視装置３３（あるいは３６）から通信制御装置３２（あるいは３５）に対してＤＰＲＡＭ１０８に書き込んだセレクティングＡＣＫが送信される（通信制御装置３２、３５を介して情報管理装置２へ送信される）。一方、ステップＳ４７６でセレクティング要求がなければ、ステップＳ４８４にジャンプする。

【００９８】

ステップＳ４８４では、データ（つまり通信制御装置３２、３５を介して情報管理装置２から送られてきた送信データ）はパケットであるか否かを判別する。データがパケットでなければ、今回のタスクを終了し、データがパケットであると、ステップＳ４８５で受信可能フラグはセットされているか否かを判別する。受信可能フラグがセットされていなければ、今回のタスクを終了する。受信可能フラグがセットされていると、情報管理装置２からネットワーク監視装置３３（あるいは３６）がセレクトされた場合にデータを受信可能である状態が整っていると判断する。次いで、ステップＳ４８６で受信可能フラグをリセットし、ステップＳ４８７で情報管理装置２へ送信ＡＣＫを送信するため、ＤＰＲＡＭ１０８に送信ＡＣＫを書き込むとともに、ステップＳ４８８でＤＰＲＡＭ１０８に割り込みを発生させて送信する。これにより、情報管理装置２へ送信ＡＣＫが送信される。

次いで、ステップＳ４８９でデータはＩＤ等以外であるか否かを判別する。データがＩＤ等以外であれば、ステップＳ４９０に進んで不揮発性メモリに記憶し、対応する情報収集基板へデータを送信設定する。これにより、情報管理装置２から送られてきて受信したＩＤ等以外のデータが不揮発性メモリ１０７に一旦記憶され、その後、対応する情報収集基板へ記憶したデータが送信されることになる。

【００９９】

次いで、ステップＳ４９１では情報管理装置２から受信したＩＤ等以外のデータで不揮発性メモリ１０７に一旦記憶したものがアミューズチップ用ＩＤ消去であるか否かを判別する。アミューズチップ用ＩＤ消去あれば、ステップＳ４９２に進んでポーリング可能フラグをリセットする。これにより、ネットワーク監視装置から下位の端末に対してポーリングが停止されることになる。次いで、ステップＳ４９３で最終ポーリングカウンタに情報収集基板端末数をセットする。最終ポーリングカウンタに情報収集基板端末数をセットす

るのは、ポーリング動作可能な全ての情報収集基板端末をカウントしていくためである。次いで、ステップＳ４９４でＲＡＭ１０９に格納されているアミューズチップ用ＩＤを消去する。上記より（すなわち、ステップＳ４９０～ステップＳ４９４より）、ネットワーク監視装置３６から今回のルーチンで指定されている情報収集基板１７３に対してアミューズチップ用ＩＤ消去命令が送信されることになる。これを受けて後述するように情報収集基板１７３はアミューズチップ用ＩＤの消去を行うことになる。ステップＳ４９４を経ると、今回のルーチンを終了してリターンする。

【０１００】

一方、ステップＳ４８９でデータがＩＤ等であれば、ステップＳ４９５に分岐してＲＡＭメモリに当該ＩＤ等を記憶する。これにより、情報管理装置２から送られてきて受信したＩＤ等のデータはＲＡＭ１０９に記憶される。次いで、ステップＳ４９６でＲＡＭメモリに記憶したデータはアミューズチップ用ＩＤ（この場合は、前回ＩＤ、次回ＩＤ、復号鍵、暗号鍵）であるか否かを判別し、アミューズチップ用ＩＤでなければ今回のタスクを終了し、アミューズチップ用ＩＤであればステップＳ４９７に進んでアミューズチップ用ＩＤを対応する情報収集基板へ送信設定し、タスクを終了する。これにより、情報管理装置２から送られてきて受信したアミューズチップ用ＩＤはＲＡＭ１０９に一旦記憶され、その後、対応する情報収集基板へ記憶したアミューズチップ用ＩＤが送信されることになる。

【０１０１】

Ｉ．情報収集基板通信受信タスク

図４０はネットワーク監視装置３３、３６のメインルーチンにおける情報収集基板通信受信タスクのサブルーチンを示すフローチャートである。このタスクがスタートすると、まずステップＳ５００でタスクの起動要求があるか否かを判別する。この場合のタスクの起動要求は、ＬＯＮで情報収集基板１７３からデータを受け取ったときにかかる。タスクの起動要求がなければ、以後の処理を行わずにタスクを終了する。

タスクの起動要求があると、ステップＳ５０２でタスクの起動要求をかけた受信域から情報収集基板からのデータ（例えば、情報管理装置２に送る大当りデータ、玉貸金額データ等、又はデータ（認証ＩＤ等））を不揮発メモリ１０７に記憶する。次いで、ステップＳ５０４で情報収集基板からのデータが情報管理装置へ送信するデータであるか否かを判別し、ＹＥＳのときはステップＳ５０６に進んで情報収集基板からのデータを情報管理装置へ送信するため不揮発メモリ１０７から送信メモリ（ＲＡＭ１０９）へ書き込み、タスクを終了する。これにより、情報収集基板からのデータがネットワーク監視装置３６を介して情報管理装置２へ送信されることになる。一方、ステップＳ５０４でＮＯのとき（情報収集基板からのデータが情報管理装置へ送信するデータでないとき）は、ステップＳ５０６をジャンプして今回のタスクを終了する。

【０１０２】

Ｊ．タイマタスク

図４１はネットワーク監視装置３３、３６のメインルーチンにおけるタイマタスクのサブルーチンを示すフローチャートである。このタスクがスタートすると、まずステップＳ５１０でタスクの起動要求があるか否かを判別する。この場合のタスク起動要求は、内部割込タイマで設定された時間により所定の時間毎の割り込みによりタスク起動要求がかかる。タスクの起動要求がなければ、以後の処理を行わずにタスクを終了する。

タスクの起動要求があると、ステップＳ５１２でタイマ処理用タイマを設定する。次いで、ステップＳ５１４で認証ＩＤ処理を行う。これは、情報管理装置２とネットワーク監視装置３３、３６および情報収集基板１７３とネットワーク監視装置３３、３６の間でそれぞれ相互認証を行うものである（詳細はサブルーチンで後述）。次いで、ステップＳ５１６でアミューズチップ用ＩＤ消去確認処理を行う。これは、閉店時に情報収集基板１７３よりアミューズチップ用ＩＤ消去終了を受け、情報管理装置２へアミューズチップ用ＩＤ消去ＡＣＫを送信するものである（詳細はサブルーチンで後述）。次いで、ステップＳ５１８で異常表示処理を行う。これは、ネットワーク異常等が発生したかどうかを判断し、

異常発生の場合に表示を行うものである（詳細はサブルーチンで後述）。次いで、ステップＳ５２０で情報収集基板のポーリング処理を行う。これは、情報収集基板１７３に対してＬＯＮのポーリングを行うものである（詳細はサブルーチンで後述）。ステップＳ５２０を経ると、タスクを終了する。

【０１０３】

Ｊ－１．認証ＩＤ処理

図４２はタイマタスクにおける認証ＩＤ処理のサブルーチンを示すフローチャートである。このサブルーチンがスタートすると、ステップＳ５３０で処理番号によるステップ分岐の判断処理を行う。これは、分岐先に対応してセットされた処理番号に基づいて分岐先を決定するものである。分岐先のステップとしては、ステップＳ５３２、ステップＳ５３４があり、以下の通りである。なお、各処理の詳細は何れもサブルーチンで後述する。

ステップＳ５３２（情報管理装置との認証ＩＤ比較処理）：処理Ｎｏ．０

ステップＳ５３４（情報収集基板との認証ＩＤ比較処理）：処理Ｎｏ．１

上記ステップＳ５３２あるいはステップＳ５３４の何れかのステップを経ると、タイマタスクにリターンする。

【０１０４】

Ｊ－１－１．情報管理装置との認証ＩＤ比較処理（処理Ｎｏ．０）

図４３は認証ＩＤ処理における情報管理装置との認証ＩＤ比較処理のサブルーチンを示すフローチャートである。このサブルーチンがスタートすると、ステップＳ５４０で情報管理装置の認証ＩＤを受信したか否かを判別し、受信していなければ今回のルーチンを終了して認証ＩＤ処理にリターンする。情報管理装置の認証ＩＤを受信した場合（受信するとＲＡＭ１０９に格納される）には、ステップＳ５４２に進んで情報管理装置の認証ＩＤ（ＲＯＭ１０６に格納されている）は正常であるか否かを判別する。情報管理装置の認証ＩＤが正常であれば、上位局（ここでは情報管理装置２）との相互認証が正常であると判断し、相互認証を行うために、ステップＳ５４４でネットワーク監視装置の正常な認証ＩＤを情報管理装置へ送るため送信メモリ（ＲＡＭ１０９）に書き込む。次いで、ステップＳ５４６でポーリング可能フラグをセットし、ステップＳ５４８でネットワーク監視装置の認証ＩＤ（ＲＯＭ１０６に格納されている）を送信設定する。これにより、下位の端末にネットワーク監視装置の認証ＩＤが送信されることになる。次いで、ステップＳ５５０で処理番号を１にしてリターンする。これにより、次回の認証ＩＤ処理ではステップＳ５３０の分岐処理で処理番号１に判断され、ステップＳ５３４の情報収集基板との認証ＩＤの比較処理（処理Ｎｏ．１）に分岐することになる。

【０１０５】

一方、ステップＳ５４２で情報管理装置の認証ＩＤが正常でなければ、ステップＳ５５２に分岐してネットワーク監視装置用の偽りの認証ＩＤを送信メモリ（ＲＡＭ１０９）に書き込む。これにより、情報管理装置２に偽りのネットワーク監視装置用認証ＩＤが送信されることになり、正常な相互認証は行われない。次いで、ステップＳ５５４でポーリング可能フラグをリセットしてリターンする。したがって、情報管理装置の認証ＩＤが異常である場合には、ネットワーク監視装置との間で相互認証が行われず、ポーリングも停止されて下位端末との間ではネットワークが不能動化される。

【０１０６】

Ｊ－１－２．情報収集基板との認証ＩＤ比較処理（処理Ｎｏ．１）

図４４は認証ＩＤ処理における情報収集基板との認証ＩＤ比較処理のサブルーチンを示すフローチャートである。このサブルーチンがスタートすると、ステップＳ５６０で各情報収集基板から認証ＩＤを受信したか否かを判別する。各情報収集基板とは、ネットワーク監視装置３６がポーリングによってネットワークを形成している各遊技機２１に配置された情報収集基板１７３のことである。各情報収集基板から認証ＩＤを受信すると、ステップＳ５６２で情報収集基板の認証ＩＤは正常であるか否かを判別する（判定用の情報収集基板１７３の認証ＩＤは情報管理装置２より送られ、ＲＡＭ１０９に格納されている）。情報収集基板の認証ＩＤが正常であれば、ステップＳ５６４で情報収集基板のアドレスと

ＯＫ（認証結果正常）を送信メモリ（ＲＡＭ１０９）へ書き込み送信設定しステップＳ５６６に進む。これにより、今回のルーチンで認証ＩＤを比較した情報収集基板のアドレスと認証ＩＤ結果がＯＫであることが上位局である情報管理装置２に送信されることになる。

【０１０７】

一方、ステップＳ５６２で情報収集基板の認証ＩＤが異常であれば、ステップＳ５６８に分岐して情報収集基板のアドレスとＮＧ（認証結果異常）を送信メモリ（ＲＡＭ１０９）へ書き込み送信設定しステップＳ５６６に進む。これにより、今回のルーチンで認証ＩＤを比較した情報収集基板のアドレスと認証ＩＤ結果がＮＧ（異常）であることが上位局である情報管理装置２に送信されることになる。

また、ステップＳ５６０で情報収集基板から認証ＩＤを受信しない場合には、ステップＳ５６６にジャンプする。

ステップＳ５６６では全情報収集基板から情報収集したか（つまり、全ての情報収集基板の認証ＩＤを比較したか）否かを判別し、全情報収集基板から情報収集していなければ今回のルーチンを終了してリターンし、次回以降のルーチンを繰り返す。そして、ルーチンを繰り返すことにより、全情報収集基板から情報収集すると、ステップＳ５７０で処理番号を０にしてリターンする。これにより、次回の認証ＩＤ処理ではステップＳ５３０の分岐処理で処理番号０に判断され、ステップＳ５３２の情報管理装置との認証ＩＤの比較処理（処理Ｎｏ．０）に分岐することになる。

【０１０８】

Ｊ－２．アミューズチップ用のＩＤ消去確認処理

図４５はタイマタスクにおけるアミューズチップ用のＩＤ消去確認処理のサブルーチンを示すフローチャートである。このサブルーチンがスタートすると、ステップＳ５８０で情報収集基板からアミューズチップ用のＩＤ消去終了を受信したか否かを判別し、ＹＥＳのときはステップＳ５８２で受信した情報収集基板のアドレス（すなわち、端末アドレス）を記憶してステップＳ５８４に進む。一方、情報収集基板からアミューズチップ用のＩＤ消去終了を受信していない場合（ＮＯのとき）は、ステップＳ５８２をジャンプしてステップＳ５８４に進む。

ステップＳ５８４では全情報収集基板からアミューズチップ用のＩＤ消去終了を受信したか否かを判別し、受信していなければ今回のルーチンを終了してリターンする。そして、このサブルーチンを繰り返し、全情報収集基板からアミューズチップ用のＩＤ消去終了を受信すると、ステップＳ５８６に進んで端末アドレス（すなわち、情報収集基板のアドレス）をクリアし、続くステップＳ５８８で全情報収集基板のアミューズチップ用のＩＤが消去されたことを情報管理装置へ送信するため、送信メモリ（ＲＡＭ１０９）にアミューズチップ用ＩＤ消去ＡＣＫを書き込み、今回のルーチンを終了してリターンする。

【０１０９】

Ｊ－３．異常表示処理

図４６はタイマタスクにおける異常表示処理のサブルーチンを示すフローチャートである。このサブルーチンがスタートすると、ステップＳ５９０でネットワーク監視装置と情報収集基板間のネットワークに異常があるか否かを判別する。異常とは、例えばポーリングに無応答のような場合である。ネットワーク監視装置と情報収集基板間のネットワークに異常があれば、ステップＳ５９２で異常場所の表示を行い、ステップＳ５９４に進む。これは、例えばネットワーク監視装置と情報収集基板間のネットワークの異常場所のアドレスを表示装置６２に表示することにより行う。ネットワーク監視装置と情報収集基板間のネットワークに異常がなければ、ステップＳ５９２をジャンプしてステップＳ５９４に進む。

ステップＳ５９４ではその他の異常（例えば、認証ＩＤの異常、アミューズチップ用ＩＤの異常等）があるか否かを判別する。その他の異常があれば、ステップＳ５９６でその他の異常場所の表示を行い、リターンする。その他の異常場所の表示では、例えば認証ＩＤ異常が発生した場所のアドレスを表示装置６２に表示する。その他の異常がなければ、ス

テップＳ５９６をジャンプしてリターンする。
【０１１０】
Ｊ－４．情報収集基板とのポーリング処理
図４７はタイマタスクにおける情報収集基板とのポーリング処理のサブルーチンを示すフローチャートである。このサブルーチンがスタートすると、ステップＳ６００で処理番号によるステップ分岐の判断処理を行う。これは、分岐先に対応してセットされた処理番号に基づいて分岐先を決定するものである。分岐先のステップとしては、ステップＳ６０２～ステップＳ６１０があり、以下の通りである。なお、各処理の詳細は何れもサブルーチンで後述する。
ステップＳ６０２（ポーリング開始処理）：処理Ｎｏ．０
ステップＳ６０４（ポーリング端末応答確認処理）：処理Ｎｏ．１
ステップＳ６０６（セレクティング処理）：処理Ｎｏ．２
ステップＳ６０８（データ送信処理）：処理Ｎｏ．３
ステップＳ６１０（送信に対するＡＣＫ待ち処理）：処理Ｎｏ．４
上記ステップＳ６０２～ステップＳ６１０のうちの何れかのステップを経ると、タイマタスクにリターンする。
【０１１１】
Ｊ－４－１．ポーリング開始処理（処理Ｎｏ．０）
図４８は情報収集基板とのポーリング処理におけるポーリング開始処理のサブルーチンを示すフローチャートである。このサブルーチンがスタートすると、まずステップＳ６２０でポーリング可能フラグがセット中であるか否かを判別する。ポーリング可能フラグがセット中とは、ネットワーク監視装置から情報収集基板に対してポーリングによる通信が可能な状態である。ポーリング可能フラグがセット中でなければ（ポーリング可能フラグがリセットされているとき）、ステップＳ６２２に進んで最終ポーリングカウンタは［０］であるか否かを判別する。このとき最終ポーリングカウンタが［０］であれば、ポーリングが停止してネットワークが不能動化されていると判断し、ルーチンを終了してリターンする。
【０１１２】
ステップＳ６２２で最終ポーリングカウンタが［０］でなければ、ステップＳ６２４で最終ポーリングカウンタを更新する。これにより、ポーリング動作可能な全ての情報収集基板端末数が更新される。
また、ステップＳ６２０でポーリング可能フラグがセット中であれば、ステップＳ６２６にジャンプする。
ステップＳ６２６ではポーリングカウンタを更新する。ポーリングポインタは複数の情報収集基板を順次指定していくものである。したがって、ポーリングポインタの更新とは、次の情報収集基板を指定するように、ポーリングポインタの値をインクリメントするものである。次いで、ステップＳ６２８でポーリングカウンタにより情報収集基板のアドレスを取り出し、ステップＳ６３０でアドレスを設定したポーリング要求を送信する。これにより、次のアドレスの情報収集基板に対してポーリング要求が送信されることになる。
【０１１３】
次いで、ステップＳ６３２でポーリング応答確認タイマをクリアする。ポーリング応答確認タイマは、ポーリング要求を送信した情報収集基板に対して所定時間内に応答があるかどうかを判断（つまり無応答の判断）するためのタイマである。次いで、ステップＳ６３４で処理番号を１にしてリターンする。これにより、次回の情報収集基板とのポーリング処理ではステップＳ６００の分岐処理で処理番号１に判断され、ステップＳ６０２のポーリング端末応答確認処理（処理Ｎｏ．１）に分岐することになる。
【０１１４】
Ｊ－４－２．ポーリング端末応答確認処理（処理Ｎｏ．１）
図４９は情報収集基板とのポーリング処理におけるポーリング端末応答確認処理のサブルーチンを示すフローチャートである。このサブルーチンがスタートすると、まずステップ

Ｓ６４０で要求した情報収集基板（例えば、ポーリングをかけた情報収集基板）からポーリングＡＣＫ又はデータを受信したか否かを判別する。これは、正常であればポーリングをかけた情報収集基板からネットワーク監視装置に対して必ずポーリングＡＣＫ又はデータが返ってくるからである。要求した情報収集基板からポーリングＡＣＫ又はデータを受信した場合には、ステップＳ６４２に進んでネットワークに前回異常ありか否かを判別する。ネットワークに前回異常があれば、ステップＳ６４４で異常解除のネットワークアドレスと時間を記憶装置（不揮発性メモリ１０７）へ記憶し、情報管理装置へ送信設定してステップＳ６４６へ進む。

【０１１５】

これは、ネットワークに前回異常があっても、今回、情報収集基板からポーリングＡＣＫ又はデータを受信したので、ネットワーク異常が解除されたと判断するものである。これにより、ネットワークに前回異常があっても、今回ネットワークが正常に復帰した場合には、復帰して応答があった情報収集基板のアドレスとその発生時間が情報管理装置２に送信されることになり、結局、第３者機関２４で把握される。

一方、ステップＳ６４２でネットワークに前回異常がなければ、ステップＳ６４４をジャンプしてステップＳ６４６に進む。

次いで、ステップＳ６４６で処理番号を２にしてリターンする。これにより、次回の情報収集基板とのポーリング処理ではステップＳ６００の分岐処理で処理番号２に判断され、ステップＳ６０６のセレクティング処理（処理Ｎｏ．２）に分岐することになる。

【０１１６】

一方、ステップＳ６４０で要求した情報収集基板からポーリングＡＣＫ又はデータを受信しない場合には、ステップＳ６４８に分岐してポーリング応答確認タイマはオーバーしているか否かを判別する。ポーリング応答確認タイマはポーリング要求を送信した情報収集基板に対して所定時間内に応答があるかどうかを判断するためのタイマであるから、ポーリング応答確認タイマがオーバーしていれば、無応答と判断してステップＳ６５０に進み、無応答のネットワークアドレスと時間を不揮発性メモリ１０７へ記憶し、情報管理装置２（送信メモリ）へ送信設定する。これにより、無応答の情報収集基板のアドレスとその発生時間が情報管理装置２に送信されることになり、結局、第３者機関２４で把握される。次いで、ステップＳ６５２で処理番号を０にしてリターンする。これにより、次回の情報収集基板とのポーリング処理ではステップＳ６００の分岐処理で処理番号０に判断され、ステップＳ６０２のポーリング開始処理（処理Ｎｏ．０）に分岐することになる。

【０１１７】

Ｊ－４－３．セレクティング処理（処理Ｎｏ．２）

図５０は情報収集基板とのポーリング処理におけるセレクティング処理のサブルーチンを示すフローチャートである。このサブルーチンがスタートすると、まずステップＳ６６０で要求した情報収集基板（例えば、ネットワーク監視装置の要求によりポーリングをかけた情報収集基板）へ送信データがあるか否かを判別する。送信データがなければステップＳ６６２に分岐して処理番号を０にしてリターンする。これにより、次のポーリングポインタで指定される情報収集基板に移行することになる。

【０１１８】

ステップＳ６６０で要求した情報収集基板へ送信データがある場合には、ステップＳ６６４に進んでポーリングポインタによりアドレスを取り出す。これにより、ポーリングポインタに対応した情報収集基板のアドレスが取り出される。次いで、ステップＳ６６６でアドレスを設定し、セレクティング要求を送信する。セレクティング要求を送信することにより、アドレスで指定された情報収集基板が受信待ちになる。次いで、ステップＳ６６８でセレクティングＡＣＫ応答確認タイマをクリアする。セレクティングＡＣＫ応答確認タイマは、セレクティング要求を送信した情報収集基板に対して所定時間内にＡＣＫ応答があるかどうかを判断するためのタイマである。次いで、ステップＳ６７０で処理番号を３にしてリターンする。これにより、次回の情報収集基板とのポーリング処理ではステップＳ６００の分岐処理で処理番号３に判断され、ステップＳ６０８のデータ送信処理（処理

Ｎｏ．３）に分岐することになる。
【０１１９】
Ｊ－４－４．データ送信処理（処理Ｎｏ．３）
図５１は情報収集基板とのポーリング処理のポーリング処理におけるデータ送信処理のサブルーチンを示すフローチャートである。このサブルーチンがスタートすると、まずステップＳ６７２で要求した情報収集基板（例えば、ネットワーク監視装置の要求によりセレクティングをかけた情報収集基板）からセレクティングＡＣＫを受信したか否かを判別する。これは、セレクティング要求をかけた情報収集基板が確実にセレクティングを受けたかどうかを判断するものである。要求した情報収集基板からセレクティングＡＣＫを受信した場合には、ステップＳ６７４に進んでポーリングポインタよりアドレスを取り出す。これにより、ポーリングポインタに対応した情報収集基板のアドレスが取り出される。次いで、ステップＳ６７６でアドレスを設定し、データを送信する。これにより、アドレスで指定された情報収集基板に対してネットワーク監視装置からデータが送信される。
【０１２０】
次いで、ステップＳ６７８でデータ応答確認タイマをクリアする。データ応答確認タイマは、データを送信した情報収集基板に対して所定時間内に応答があるかどうかを判断するためのタイマである。次いで、ステップＳ６８０で処理番号を４にしてリターンする。これにより、次回の情報収集基板とのポーリング処理のポーリング処理ではステップＳ６００の分岐処理で処理番号４に判断され、ステップＳ６１０の送信に対するＡＣＫ待ち処理（処理Ｎｏ．４）に分岐することになる。
一方、ステップＳ６７２で要求した情報収集基板からセレクティングＡＣＫを受信しない場合には、ステップＳ６８４に進んでセレクティング応答確認タイマはオーバーしているか否かを判別する。
【０１２１】
セレクティング応答確認タイマはセレクティング要求を送信した情報収集基板に対して所定時間内に応答があるかどうかを判断するためのタイマであるから、セレクティング応答確認タイマがオーバーしていれば、応答不能（例えば、無応答）と判断してステップＳ６８６に進み、セレクティング応答不能のネットワークアドレスと時間を不揮発性メモリ１０７へ記憶し、情報管理装置へ送信設定する。これにより、セレクティング応答不能の情報収集基板が記録され、セレクティング応答不能の情報収集基板の記録は第３者機関２４によって把握されることになる。
次いで、ステップＳ６８８で処理番号を０にしてリターンする。これにより、次回の情報収集基板とのポーリング処理ではステップＳ６００の分岐処理で処理番号０に判断され、ステップＳ６０２のポーリング開始処理（処理Ｎｏ．０）に分岐することになる。
一方、ステップＳ６８４でセレクティング応答確認タイマがオーバーしていなければ、今回のルーチンを終了してリターンする。
【０１２２】
Ｊ－４－５．送信に対するＡＣＫ待ち処理（処理Ｎｏ．４）
図５２は情報収集基板とのポーリング処理における送信に対するＡＣＫ待ち処理のサブルーチンを示すフローチャートである。このサブルーチンがスタートすると、まずステップＳ６９０で送信した情報収集基板から送信ＡＣＫを受信したか否かを判別する。これは、今回送信したデータ（例えば、相互認証のデータ）を情報収集基板が受けたか否かを判断するものである。送信した情報収集基板から送信ＡＣＫを受信していれば、ステップＳ６９２で処理番号を０にしてリターンする。これにより、次回の情報収集基板とのポーリング処理ではステップＳ６００の分岐処理で処理番号０に判断され、ステップＳ６０２のポーリング開始処理（処理Ｎｏ．０）に分岐することになる。
【０１２３】
ステップＳ６９０で送信した情報収集基板からＡＣＫを受信していない場合には、ステップＳ６９４に分岐してデータ応答確認タイマはオーバーしているか否かを判別する。データ応答確認タイマはデータを送信した情報収集基板に対して所定時間内に応答があるかど

うかを判断するためのタイマであるから、データ応答確認タイマがオーバーしていれば、応答不能（例えば、無応答）と判断してステップＳ６９６に進み、データ応答不能のネットワークアドレスと時間を不揮発性メモリ１０７へ記憶し、情報管理装置へ送信設定する。これにより、データ応答不能の情報収集基板が記録され、データ応答確認不能の情報収集基板の記録は第３者機関２４によって把握される。
次いで、ステップＳ６９８で処理番号を０にしてリターンする。これにより、次回の情報収集基板とのポーリング処理ではステップＳ６００の分岐処理で処理番号０に判断され、ステップＳ６０２のポーリング開始処理（処理Ｎｏ．０）に分岐することになる。
一方、ステップＳ６９４でデータ応答確認タイマがオーバーしていなければ、今回のルーチンを終了してリターンする。

【０１２４】
以上で、ネットワーク監視装置３３、３６のプログラムの説明を終了し、次いで、情報収集基板１７３のプログラムについて説明する。
Ｋ．情報収集基板のメインルーチン
図５３は情報収集基板１７３のメインルーチンを示すフローチャートである。このプログラムは情報収集基板１７３の電源投入（パワーオン）と同時に開始される。
図５３に示すプログラムがスタートすると、まずステップＳ７００でリセットタスクを実行する。これは、タイマタスクのタイマ設定、ＤＰＲＡＭ２０８のクリア、Ｉ／Ｏポート２１０のイニシャライズ等を行うものである。次いで、ステップＳ７０２で時分割処理を行う。これは、以下の何れかのタスクに時分割で分岐するもので、どこに分岐するかは、行き先タスクの起動がかかることよって決定される。分岐先タスクとしては、以下のものがある。

【０１２５】
ステップＳ７０４：役物回路からの受信タスク
役物回路（役物制御基板１７１のこと、以下同様）との間でＤＰＲＡＭ２０８を介して情報の転送を行うもので、役物回路側のＤＰＲＡＭからの割り込み要求で、このタスクが起動する（詳細はサブルーチンで後述）。
なお、本フローチャートにおいて役物回路とは、役物制御基板１７１のことであり、フローチャートでは、以後適宜、役物制御基板１７１を役物回路と記述して説明する。
ステップＳ７０６：ネットワーク監視装置からの受信タスク
ネットワーク監視装置３６からのデータを受信するもので、ＬＯＮでネットワーク監視装置３６からデータを受け取ったときにタスク起動要求がかかり、このタスクが起動する（詳細はサブルーチンで後述）。
ステップＳ７０８：タイマタスク
ＬＯＮによるネットワーク監視装置３６とのデータ送受信、ＤＰＲＡＭ２０８を介して役物回路との情報転送、ＩＤ処理、ＩＤ消去処理等を行うもので、内部割込タイマで設定された時間による所定の時間毎の割り込みによりタスク起動要求がかかり、このタスクが起動する（詳細はサブルーチンで後述）。

【０１２６】
ステップＳ７１０：役物回路のアウト玉入力タスク
アウト玉のカウントを行うもので、回収玉ＳＷ２１８の信号により、このタスクが起動する（詳細はサブルーチンで後述）。
ステップＳ７１２：玉貸機の玉貸入力タスク
玉貸のカウントを行うもので、玉貸信号によりこのタスクが起動する（詳細はサブルーチンで後述）。
上記ステップＳ７０４～ステップＳ７１２の何れかのタスクを経ると、ステップＳ７０２に戻って処理を繰り返す。

【０１２７】
Ｋ－１．役物回路からの受信タスク
図５４は情報収集基板１７３のメインルーチンにおける役物回路からの受信タスクのサブ

ルーチンを示すフローチャートである。このタスクがスタートすると、まずステップＳ７２０でタスクの起動要求があるか否かを判別する。この場合のタスク起動要求は、役物回路側のＤＰＲＡＭからの割り込み要求でかかる。タスクの起動要求がなければ、以後の処理を行わずにタスクを終了する。
タスクの起動要求があると、ステップＳ７２２でタスクの起動要求をかけた割り込み信号をリセットし、ステップＳ７２４で役物回路との送受信禁止中（例えば、ネットワーク監視装置との認証ＩＤが異常のとき）であるか否かを判別する。役物回路との送受信禁止中であれば、以後の処理を行わずにタスクを終了する。役物回路との送受信禁止中でなければ、ステップＳ７２６に進んで受信データ（役物回路から受信したデータ）はアミューズチップ用ＩＤであるか否かを判別する。

【０１２８】
役物回路から受信したデータがアミューズチップ用ＩＤであれば、ステップＳ７２８で受信したアミューズチップ用ＩＤをＤＰＲＡＭ２０８から読み込み、ＲＡＭメモリ（ＲＡＭ２０９）に記憶する。これにより、役物回路から受信したアミューズチップ用ＩＤが一旦ＲＡＭ２０９に記憶される。ただし、ＲＡＭ２０９の電源供給が停止すると、記憶したアミューズチップ用ＩＤは消失する。ステップＳ７２８を経ると、今回のタスクを終了する。
一方、ステップＳ７２６で役物回路から受信したデータがアミューズチップ用ＩＤでなければ、ステップＳ７３０に分岐してＤＰＲＡＭ２０８から遊技データ（例えば、大当りデータ等）を読み込み、不揮発性メモリ２０７に記憶する。遊技データは不揮発性メモリ２０７に記憶されるから、アミューズチップ用のＩＤと異なり、電源供給が停止しても記憶内容は消失しない。次いで、ステップＳ７３２で情報管理装置へ（ネットワーク監視装置を介して情報管理装置へ）データを送信設定（送信メモリとしてのＲＡＭ２０９に設定）する。これにより、不揮発性メモリ２０７に記憶した遊技データが情報管理装置２に送信されることになる。ステップＳ７３２を経ると、今回のタスクを終了する。

【０１２９】
Ｋ－２．ネットワーク監視装置からの受信タスク
図５５は情報収集基板１７３のメインルーチンにおけるネットワーク監視装置からの受信タスクのサブルーチンを示すフローチャートである。このタスクがスタートすると、まずステップＳ７４０でタスクの起動要求があるか否かを判別する。この場合のタスク起動要求は、ＬＯＮでネットワーク監視装置からデータを受けたときにタスク起動要求がかかる。タスクの起動要求がなければ、以後の処理を行わずにタスクを終了する。

【０１３０】
タスクの起動要求があると、ステップＳ７４２でタスクの起動要求をかけたネットワーク監視装置からの受信データはパケットであるか否かを判別し、パケット（データ）であれば、ステップＳ７４４に進んでパケットを受け取ったことを知らせるためにネットワーク監視装置へ送信ＡＣＫを送信する。次いで、ステップＳ７４６でタスクの起動要求をかけたネットワーク監視装置からの受信データは認証ＩＤ又はアミューズチップ用ＩＤ等であるか否かを判別する。受信データが認証ＩＤ又はアミューズチップ用ＩＤ等であれば、ステップＳ７４７でタスクの起動要求をかけた受信域から認証ＩＤ又はアミューズチップ用ＩＤ等をＲＡＭメモリ（ＲＡＭ２０９）に記憶する。これにより、ネットワーク監視装置３６から受信した認証ＩＤ又はアミューズチップ用ＩＤ等が一旦ＲＡＭ２０９に記憶される。ただし、ＲＡＭ２０９の電源供給が停止すると、又はアミューズチップ用ＩＤ消去を受信すると、記憶した認証ＩＤ又はアミューズチップ用ＩＤ等は消失する。ステップＳ７４７を経ると、今回のタスクを終了する。
一方、ステップＳ７４６で受信データが認証ＩＤ又はアミューズチップ用ＩＤ等でなければ、ステップＳ７４８でタスクの起動要求をかけた受信域からデータ（例えば、情報管理装置２、ネットワーク監視装置３６からのデータ等）を不揮発性メモリ２０７に記憶し、今回のタスクを終了する。

【０１３１】

Ｋ－３．タイマタスク
図５６は情報収集基板１７３のメインルーチンにおけるタイマタスクのサブルーチンを示すフローチャートである。このタスクがスタートすると、まずステップＳ７５０でタスクの起動要求があるか否かを判別する。この場合のタスク起動要求は、内部割込タイマで設定された時間による所定の時間毎の割り込みによりタスク起動要求がかかる。タスクの起動要求がなければ、以後の処理を行わずにタスクを終了する。
【０１３２】
タスクの起動要求があると、ステップＳ７５２でタイマ処理用タイマを設定する。次いで、ステップＳ７５４でネットワーク監視装置送信処理を行う。これは、ネットワーク監視装置３３、３６に対してＬＯＮによる送信を行うものである（詳細はサブルーチンで後述）。次いで、ステップＳ７５６で役物回路への送信処理を行う。これは、ＤＰＲＡＭ２０８を介して役物回路にデータを送信するものである（詳細はサブルーチンで後述）。次いで、ステップＳ７５８でＩＤ確認処理を行う。これは、ＩＤの認証とアミューズチップ用ＩＤの確認を行うものである（詳細はサブルーチンで後述）。次いで、ステップＳ７６０でアミューズチップ用ＩＤ消失処理を行う。これは、ＲＡＭ２０９に記憶しているアミューズチップ用ＩＤ等を消去するものである（詳細はサブルーチンで後述）。ステップＳ７６０を経ると、タスクを終了する。
【０１３３】
Ｋ－３－１．ネットワーク監視装置送信処理
図５７はタイマタスクにおけるネットワーク監視装置送信処理のサブルーチンを示すフローチャートである。このサブルーチンがスタートすると、ステップＳ７７０でネットワーク監視装置からのポーリング応答処理を行う。これは、ネットワーク監視装置３６からのポーリングに応答してデータ等を送信するもので、詳細はサブルーチンで後述する。次いで、ステップＳ７７２でネットワーク監視装置からのセレクティング応答処理を行う。これは、ネットワーク監視装置３６からのセレクティングに応答し、データ受信可能であればセレクティングＡＣＫを返すもので、詳細はサブルーチンで後述する。ステップＳ７７２を経ると、今回のサブルーチンを終了してリターンする。
【０１３４】
Ｋ－３－１ａ．ネットワーク監視装置からのポーリング応答処理
図５８はネットワーク監視装置送信処理におけるネットワーク監視装置からのポーリング応答処理のサブルーチンを示すフローチャートである。このサブルーチンがスタートすると、ステップＳ７８０でネットワーク監視装置からポーリング要求があるか否かを判別し、ポーリング要求がなければ以後の処理を行わずにリターンする。ポーリング要求があると、ステップＳ７８２でネットワーク監視装置へ送信メモリ（ＲＡＭ２０９）から送信データを送信しリターンする。この場合、送信するデータがないときはポーリングＡＣＫを送信する。これにより、ネットワーク監視装置３６からのポーリングに応答して情報収集基板１７３から送信データ（送信メモリに設定）がネットワーク監視装置３６（又は、ネットワーク監視装置３６を介して情報管理装置２）に送信される。
【０１３５】
Ｋ－３－１ｂ．ネットワーク監視装置からのセレクティング応答処理
図５９はネットワーク監視装置送信処理におけるネットワーク監視装置からのセレクティング応答処理のサブルーチンを示すフローチャートである。このサブルーチンがスタートすると、ステップＳ７９０でネットワーク監視装置からセレクティング要求があるか否かを判別し、セレクティング要求がなければ以後の処理を行わずにリターンする。セレクティング要求があると、ステップＳ７９２で現在受信可能状態であるか否かを判別する。これは、情報収集基板１７３が受信体制になっているかどうかを判断するものである。現在受信可能状態でなければ（例えば、受信メモリ（ＲＡＭ２０９、不揮発性メモリ２０７）が一杯のとき）、セレクティング要求に応答できないとしてリターンする。現在受信可能状態であれば、ステップＳ７９４でネットワーク監視装置へセレクティングＡＣＫを送信（送信メモリに設定）しリターンする。

【０１３６】
Ｋ－４．役物回路への送信処理
図６０はタイマタスクにおける役物回路への送信処理のサブルーチンを示すフローチャートである。このサブルーチンがスタートすると、ステップＳ８００でネットワーク監視装置から（上位の情報管理装置から）役物回路（すなわち、役物制御基板１７１）への制御コマンド（例えば、打ち止め指令等）を受信したか否かを判別する。ネットワーク監視装置（情報管理装置）から役物回路への制御コマンドを受信していなければ、以後の処理は行わずにリターンする。
ネットワーク監視装置（情報管理装置）から役物回路への制御コマンドを受信すると、ステップＳ８０２に進んで役物回路との送受信禁止中であるか否かを判別し、役物回路との送受信禁止中であれば、以後の処理を行わずにタスクを終了する。役物回路との送受信禁止中でなければ、ステップＳ８０４に進んでネットワーク監視装置（情報管理装置）から受信した役物回路への制御コマンドを不揮発性メモリ２０７から読み出してＤＰＲＡＭ２０８へ書き込む。次いで、ステップＳ８０６でＤＰＲＡＭ２０８に割り込みを発生させ、ＤＰＲＡＭ２０８に書き込んだデータを役物回路へ送信しリターンする。これにより、ネットワーク監視装置３６（情報管理装置２）から受信した役物回路への制御コマンド（例えば、打ち止め指令等）がＤＰＲＡＭ２０８を介して役物制御基板１７１に送信される。
【０１３７】
Ｋ－５．ＩＤ確認処理
図６１はタイマタスクにおけるＩＤ確認処理のサブルーチンを示すフローチャートである。このサブルーチンがスタートすると、ステップＳ８１０で処理番号によるステップ分岐の判断処理を行う。これは、分岐先に対応してセットされた処理番号に基づいて分岐先を決定するものである。分岐先のステップとしては、ステップＳ８１２～ステップＳ８２８があり、以下の通りである。なお、各処理の詳細は何れもサブルーチンで後述する。
ステップＳ８１２（ネットワーク監視装置からの認証ＩＤ受信処理待ち処理）：処理Ｎｏ．０
ステップＳ８１４（ネットワーク監視装置との認証ＩＤ比較処理）：処理Ｎｏ．１
ステップＳ８１６（ネットワーク監視装置からのアミューズチップ用ＩＤ受信待ち処理）：処理Ｎｏ．２
【０１３８】
ステップＳ８１８（役物回路へアミューズチップ用のＩＤ要求処理）：処理Ｎｏ．３
ステップＳ８２０（役物から前回のアミューズチップ用のＩＤ受信待ち処理）：処理Ｎｏ．４
ステップＳ８２２（前回のアミューズチップ用ＩＤの復号化処理）：処理Ｎｏ．５
ステップＳ８２４（アミューズチップ用のＩＤ比較処理）：処理Ｎｏ．６
ステップＳ８２６（役物回路へ次回のアミューズチップ用ＩＤの暗号化と送信処理）：処理Ｎｏ．７
ステップＳ８２８（役物回路からの次回のアミューズチップ用ＩＤ受信ＡＣＫ待ち処理）：処理Ｎｏ．８
上記ステップＳ８１２～ステップＳ８２８のうちの何れかのステップを経ると、タイマタスクにリターンする。
【０１３９】
Ｋ－５－１．ネットワーク監視装置からの認証ＩＤ受信処理待ち処理（処理Ｎｏ．０）
図６２はＩＤ確認処理におけるネットワーク監視装置からの認証ＩＤ受信処理待ち処理のサブルーチンを示すフローチャートである。このサブルーチンがスタートすると、まずステップＳ８３０でネットワーク監視装置から認証ＩＤを受信したか否かを判別する。これは、ネットワーク監視装置から認証ＩＤを受信してＲＡＭ２０９に取り込まれているかどうかを判断するものである。ネットワーク監視装置から認証ＩＤを受信していなければ、以後の処理は行わずにリターンする。ネットワーク監視装置から認証ＩＤを受信した場合には、ステップＳ８３２に進んで処理番号を１にしてリターンする。これにより、次回の

ＩＤ確認処理ではステップＳ８１０の分岐処理で処理番号１に判断され、ステップＳ８１４のネットワーク監視装置との認証ＩＤ比較処理（処理Ｎｏ．１）に分岐することになる。

【０１４０】

Ｋ－５－２．ネットワーク監視装置との認証ＩＤ比較処理（処理Ｎｏ．１）

図６３はＩＤ確認処理におけるネットワーク監視装置との認証ＩＤ比較処理のサブルーチンを示すフローチャートである。このサブルーチンがスタートすると、まずステップＳ８４０でネットワーク監視装置の認証ＩＤは正常であるか否かを判別し、正常であればステップＳ８４２でネットワーク監視装置へ正常な認証ＩＤ（すなわち、情報収集基板１７３の認証ＩＤ）を送信設定（送信メモリに設定）する。これにより、情報収集基板１７３の認証ＩＤがネットワーク監視装置３６に送信され、相互認証が行われることになる。次いで、ステップＳ８４４で処理番号を２にする。これにより、次回のＩＤ確認処理ではステップＳ８１０の分岐処理で処理番号２に判断され、ステップＳ８１６のネットワーク監視装置からのアミューズチップ用ＩＤ受信待ち処理（処理Ｎｏ．２）に分岐することになる。次いで、ステップＳ８４６で役物回路との送受信禁止フラグをリセットしてリターンする。送受信禁止フラグは、後述のようにネットワーク監視装置３６が正常でない場合に、役物回路との送受信を禁止するフラグである。役物回路との送受信禁止フラグがリセットされることにより、情報収集基板１７３と役物回路との間でデータの送受信が可能になる。

【０１４１】

一方、ステップＳ８４０でネットワーク監視装置の認証ＩＤが正常でない場合には、ステップＳ８４８に分岐してネットワーク監視装置へ偽りの認証ＩＤを送信設定（送信メモリに設定）する。これにより、例えばネットワーク監視装置が偽物である場合には、情報収集基板１７３から偽りの認証ＩＤがネットワーク監視装置に送信され、相互認証は行われない。次いで、ステップＳ８５０で処理番号を０にしてリターンする。これにより、次回のＩＤ確認処理ではステップＳ８１０の分岐処理で処理番号０に判断され、ステップＳ８１２のネットワーク監視装置からの認証ＩＤ受信待ち処理（処理Ｎｏ．０）に再び戻ることになる。次いで、ステップＳ８５２で役物回路との送受信禁止フラグをセットしてリターンする。これにより、ネットワーク監視装置が偽物である場合には、情報収集基板１７３と役物回路との間ではデータの送受信ができなくなる。

【０１４２】

Ｋ－５－３．ネットワーク監視装置からのアミューズチップ用ＩＤ受信待ち処理（処理Ｎｏ．２）

図６４はＩＤ確認処理におけるネットワーク監視装置からのアミューズチップ用ＩＤ受信待ち処理のサブルーチンを示すフローチャートである。このサブルーチンがスタートすると、まずステップＳ８６０でネットワーク監視装置（すなわち、上位の情報管理装置：これは上位局からアミューズチップ用ＩＤ等が送信されるからである）からＩＤ（すなわち、アミューズチップ用ＩＤ等：例えば、アミューズチップ用の前回と次回のＩＤコード、今回のＩＤ復号鍵、次回のＩＤ暗号鍵）を受信したか否かを判別する。ネットワーク監視装置からＩＤを受信していなければリターンし、ネットワーク監視装置からＩＤを受信すると、ステップＳ８６２に進んで処理番号を３にしてリターンする。これにより、次回のＩＤ確認処理ではステップＳ８１０の分岐処理で処理番号３に判断され、ステップＳ８１８の役物回路へアミューズチップ用ＩＤ要求処理（処理Ｎｏ．３）に分岐することになる。このように、ネットワーク監視装置３６からＩＤを受信すると、役物制御基板１７１にアミューズチップ用ＩＤを要求する処理に移行する。

【０１４３】

Ｋ－５－４．役物回路へアミューズチップ用ＩＤ要求処理（処理Ｎｏ．３）

図６５はＩＤ確認処理における役物回路へアミューズチップ用ＩＤ要求処理のサブルーチンを示すフローチャートである。このサブルーチンがスタートすると、まずステップＳ８７０でＤＰＲＡＭ２０８へアミューズチップ用ＩＤ要求を書き込み、ステップＳ８７２で

ＤＰＲＡＭ２０８へ割り込みを発生させ送信する。これにより、ＤＰＲＡＭ２０８に書き込まれたアミューズチップ用ＩＤ要求が情報収集基板１７３から役物制御基板１７１に送信される。次いで、ステップＳ８７４で処理番号を４にしてリターンする。これにより、次回のＩＤ確認処理ではステップＳ８１０の分岐処理で処理番号４に判断され、ステップＳ８２０の役物からの前回のアミューズチップ用ＩＤ受信待ち処理（処理Ｎｏ．４）に分岐することになる。

【０１４４】

Ｋ－５－５．役物からの前回のアミューズチップ用ＩＤ受信待ち処理（処理Ｎｏ．４）

図６６はＩＤ確認処理における役物からの前回のアミューズチップ用ＩＤ受信待ち処理のサブルーチンを示すフローチャートである。このサブルーチンがスタートすると、まずステップＳ８８０で役物回路からＩＤ（すなわち、アミューズチップ用ＩＤ）を受信したか否かを判別する。役物回路からＩＤを受信していなければリターンし、役物回路からＩＤを受信すると、ステップＳ８８２に進んで処理番号を５にしてリターンする。これにより、次回のＩＤ確認処理ではステップＳ８１０の分岐処理で処理番号５に判断され、ステップＳ８２２の前回のアミューズチップ用ＩＤの復号化処理（処理Ｎｏ．５）に分岐することになる。このように、役物回路からＩＤを受信すると、前回のアミューズチップ用ＩＤを復号化する処理に移行する。

【０１４５】

Ｋ－５－６．前回のアミューズチップ用ＩＤの復号化処理（処理Ｎｏ．５）

図６７はＩＤ確認処理における前回のアミューズチップ用ＩＤの復号化処理のサブルーチンを示すフローチャートである。このサブルーチンがスタートすると、まずステップＳ８９０でＲＡＭメモリ（ＲＡＭ２０９）から役物回路（すなわち、役物制御基板盤における遊技用演算処理装置２２１に記憶されていたＩＤ）より受信した前回のＩＤ（アミューズチップ用ＩＤ）を取り出す。これにより、役物回路から受信してＲＡＭ２０９に記憶されている前回のＩＤが取り出される。次いで、ステップＳ８９２で役物回路の前回のＩＤを復号鍵で復元する。これにより、情報管理装置２から送信されてきた復号鍵で役物回路の前回のＩＤが復号化される。次いで、ステップＳ８９４で処理番号を６にしてリターンする。これにより、次回のＩＤ確認処理ではステップＳ８１０の分岐処理で処理番号６に判断され、ステップＳ８２４のアミューズチップ用ＩＤ比較処理（処理Ｎｏ．６）に分岐することになる。

【０１４６】

Ｋ－５－７．アミューズチップ用ＩＤ比較処理（処理Ｎｏ．６）

図６８はＩＤ確認処理におけるアミューズチップ用ＩＤ比較処理のサブルーチンを示すフローチャートである。このサブルーチンがスタートすると、まずステップＳ９００でネットワーク監視装置（情報管理装置）から受信したＩＤと復号鍵で復号化された役物回路の前回のＩＤ（アミューズチップ用ＩＤ）とを比較し、ステップＳ９０２でＩＤ（役物回路の前回のＩＤ）は正常であるか否かを判別する。ＩＤが正常であれば、ステップＳ９０４でＤＰＲＡＭ２０８へ動作許可（動作許可コマンド）を書き込み、ステップＳ９０６でＤＰＲＡＭ２０８へ割り込みを発生させ送信する。これにより、ＤＰＲＡＭ２０８に書き込まれた動作許可コマンドが情報収集基板１７３から役物制御基板１７１（遊技用演算処理装置２２１）に送信されて役物制御基板１７１の動作が許可され、遊技が可能になる。なお、後述するように、役物制御基板１７１は動作許可コマンドを受けると、動作許可ＡＣＫを情報収集基板１７３に返す。

【０１４７】

次いで、ステップＳ９０８で情報管理装置へ確認終了情報としてＩＤ　ＯＫを送信設定（送信メモリに設定）する。これにより、情報収集基板１７３から情報管理装置２へネットワーク監視装置３６を介して役物制御基板１７１（遊技用演算処理装置２２１）のＩＤがＯＫ（正常）であることが送信されることになる。次いで、ステップＳ９１０で処理番号を７にしてリターンする。これにより、次回のＩＤ確認処理ではステップＳ８１０の分岐処理で処理番号７に判断され、ステップＳ８２６の役物回路へ次回のアミューズチップ用

ＩＤの暗号化と送信処理（処理Ｎｏ．７）に分岐することになる。
一方、ステップＳ９０２でＩＤが正常でなければ、ステップＳ９１２に分岐してＤＰＲＡＭ２０８へ動作不許可（動作不許可コマンド）を書き込み、ステップＳ９１４でＤＰＲＡＭ２０８へ割り込みを発生させ送信する。これにより、ＤＰＲＡＭ２０８に書き込まれた動作不許可コマンドが情報収集基板１７３から役物制御基板１７１に送信されて役物制御基板１７１の動作が不許可になり、遊技を行うことができない状態になる。
【０１４８】
次いで、ステップＳ９１６で情報管理装置へ確認終了情報としてＩＤ　ＮＧを送信設定（送信メモリに設定）する。これにより、情報収集基板１７３から情報管理装置２へネットワーク監視装置３６を介して役物制御基板１７１（遊技用演算処理装置２２１）のＩＤがＮＧ（異常）であることが送信されることになる。次いで、ステップＳ９１８で処理番号を０にしてリターンする。これにより、次回のＩＤ確認処理ではステップＳ８１０の分岐処理で処理番号０に判断され、ステップＳ８１２のネットワーク監視装置からの認証ＩＤ受信待ち処理（処理Ｎｏ．０）に再び分岐することになる。
このように、情報管理装置２からネットワーク監視装置３６を介して受信したＩＤと復号鍵で復号化した役物回路の前回のＩＤとが比較され、ＩＤが正常であれば遊技が許可され、異常であれば遊技が不許可になる。したがって、役物制御基板１７１の改竄が行われたような場合には、遊技が不許可になる。また、役物制御基板１７１のＩＤの比較結果は対応するネットワーク監視装置３６に送信され、ネットワーク監視装置３６から情報管理装置２に送信されて把握されることになる。
【０１４９】
Ｋ－５－８．役物回路へ次回のアミューズチップ用ＩＤの暗号化と送信処理（処理Ｎｏ．７）
図６９はＩＤ確認処理における役物回路へ次回のアミューズチップ用ＩＤの暗号化と送信処理のサブルーチンを示すフローチャートである。このサブルーチンがスタートすると、まずステップＳ９２０で動作許可ＡＣＫを受信したか否かを判別する。これは、情報収集基板１７３から動作許可コマンドを役物制御基板１７１に送信したことに応答して、役物制御基板１７１から動作許可ＡＣＫが返されるので、そのＡＣＫを受信したかどうかを判断するものである。動作許可ＡＣＫを受信していなければ、今回のルーチンを終了してリターンする。
【０１５０】
動作許可ＡＣＫを受信すると、ステップＳ９２２に進んで次回の暗号鍵で次回のＩＤ（アミューズチップ用ＩＤ）を暗号化する。次いで、ステップＳ９２４で暗号化したＩＤ（次回のＩＤ）をＤＰＲＡＭ２０８へ書き込み、ステップＳ９２６でＤＰＲＡＭ２０８へ割り込みを発生させ送信する。これにより、ＤＰＲＡＭ２０８に書き込まれた暗号化した次回のＩＤが情報収集基板１７３から役物制御基板１７１に送信される。次いで、ステップＳ９２８で処理番号を８にしてリターンする。これにより、次回のＩＤ確認処理ではステップＳ８１０の分岐処理で処理番号８に判断され、ステップＳ８２８の役物回路からの次回のアミューズチップ用ＩＤ受信ＡＣＫ待ち処理（処理Ｎｏ．８）に分岐することになる。
【０１５１】
Ｋ－５－９．役物回路からの次回のアミューズチップ用ＩＤ受信ＡＣＫ待ち処理（処理Ｎｏ．８）
図７０はＩＤ確認処理における役物回路からの次回のアミューズチップ用ＩＤ受信ＡＣＫ待ち処理のサブルーチンを示すフローチャートである。このサブルーチンがスタートすると、まずステップＳ９３０でＩＤ受信ＡＣＫを受信したか否かを判別する。これは、情報収集基板１７３から次回のＩＤを役物制御基板１７１に送信したことに応答して、役物制御基板１７１（遊技用演算処理装置２２１）からＩＤ受信ＡＣＫが返されるので、そのＡＣＫを受信したかどうかを判断するものである。ＩＤ受信ＡＣＫを受信していなければ、今回のルーチンを終了してリターンする。ＩＤ受信ＡＣＫを受信すると、ステップＳ９３２で処理番号を０にしてリターンする。これにより、次回のＩＤ確認処理ではステップＳ

８１０の分岐処理で処理番号０に判断され、ステップＳ８１２のネットワーク監視装置からの認証ＩＤ受信待ち処理（処理Ｎｏ．０）に分岐することになる。

【０１５２】

Ｋ－６．アミューズチップ用ＩＤ消去処理

図７１はタイマタスクにおけるアミューズチップ用ＩＤ消去処理のサブルーチンを示すフローチャートである。このサブルーチンがスタートすると、まずステップＳ９４０でネットワーク監視装置（情報管理装置）からＩＤ（アミューズチップ用ＩＤ）消去を受信したか否かを判別する。これは、閉店時にネットワーク監視装置３６（情報管理装置２）からＩＤ消去コマンドが情報収集基板１７３に送信されるので、そのＩＤ消去コマンドを受信したかどうかを判断するものである。ネットワーク監視装置からＩＤ消去を受信していなければ、今回のタスクを終了する。

ネットワーク監視装置からＩＤ消去を受信した場合には、ステップＳ９４２に進んでＲＡＭメモリ（ＲＡＭ２０９）の前回と次回のＩＤと、復号鍵と、暗号鍵とをクリアし、ステップＳ９４４でネットワーク監視装置３６へアミューズチップ用ＩＤ消去終了を送信し（送信メモリに設定）タスクを終了する。これにより、ＲＡＭ２０９に記憶されていた前回と次回のＩＤ、復号鍵および暗号鍵が消去される。したがって、情報収集基板１７３が盗用にあっても、前回と次回のＩＤ、復号鍵および暗号鍵が判明することはなく、不正が有効に防止される。

【０１５３】

Ｌ．役物回路のアウト玉入力タスク

図７２は情報収集基板１７３のメインルーチンにおける役物回路のアウト玉入力タスクのサブルーチンを示すフローチャートである。このタスクがスタートすると、まずステップＳ９５０でタスクの起動（入力）要求があるか否かを判別する。この場合のタスク起動要求は、回収玉ＳＷ２１８からの信号による割り込み要求によってかかる。タスクの起動要求がなければ、以後の処理を行わずにタスクを終了する。タスクの起動要求があると、ステップＳ９５２でアウト玉カウンタを更新し、不揮発性メモリ２０７へ記憶するとともに、送信メモリに設定してタスクを終了する。これにより、回収玉（アウト玉＋セーフ玉）がカウントされて不揮発性メモリ２０７へ記憶され、記憶されたアウト玉カウンタ値はネットワーク監視装置３６を介して情報管理装置２へ送信されることになる。

【０１５４】

Ｍ．玉貸機の玉貸入力タスク

図７３は情報収集基板１７３のメインルーチンにおける玉貸機の玉貸入力タスクのサブルーチンを示すフローチャートである。このタスクがスタートすると、まずステップＳ９６０でタスクの起動（入力）要求があるか否かを判別する。この場合のタスク起動要求は、玉貸機２５からの玉貸信号ＳＰ７による割り込み要求によってかかる。タスクの起動要求がなければ、以後の処理を行わずにタスクを終了する。タスクの起動要求があると、ステップＳ９６２で玉貸カウンタを更新し、不揮発性メモリ２０７へ記憶するとともに、送信メモリに設定してタスクを終了する。これにより、玉貸単位数（すなわち、玉貸金額に対応）がカウントされて不揮発性メモリ２０７へ記憶され、記憶された玉貸カウンタ値はネットワーク監視装置３６を介して情報管理装置２へ送信されることになる。

【０１５５】

以上で、情報収集基板１７３のプログラムの説明を終了し、次いで、遊技用演算処理装置（アミューズチップ）２２１のプログラムについて説明する。

Ｎ．アミューズチップのプログラム

図７４は遊技用演算処理装置（アミューズチップ）２２１のプログラムを示すフローチャートである。このプログラムは遊技用演算処理装置（アミューズチップ）２２１の電源投入（パワーオン）と同時に開始される。

図７４に示すプログラムがスタートすると、まずステップＳ９７０で初期化処理を行う。これは、フラグのクリア、メモリエリアのクリア、入力ポート２２５、出力ポート２２６のイニシャライズ等を行うとともに、セキュリティプログラムを起動するものである。次

いで、ステップＳ９７２でＩＤ要求があるか否かを判別する。これは、情報収集基板１７３からアミューズチップ用ＩＤの要求があるかどうかを判断するものである。ＩＤ要求がなければ、このステップＳ９７２に待機し、ＩＤ要求があると、ステップＳ９７４に進んでＥＥＰＲＯＭ３０４に格納されているＩＤを送信する。これにより、ＩＤが情報収集基板１７３に送信される。

【０１５６】

次いで、ステップＳ９７６で動作許可コマンドがあるか否かを判別する。これは、情報収集基板１７３が遊技用演算処理装置（アミューズチップ）２２１の正当性を認めた場合に、情報収集基板１７３から送信されてくるものであり、動作許可コマンドがあると遊技用演算処理装置２２１の動作が許可になるものである。動作許可コマンドがなければステップＳ９７８で動作不許可コマンドがあるか否かを判別する。動作不許可コマンドは、情報収集基板１７３が遊技用演算処理装置（アミューズチップ）２２１の正当性を認めない場合に、情報収集基板１７３から送信されてくるものであり、動作不許可コマンドがあると遊技用演算処理装置２２１の動作が不許可になるものである。

ステップＳ９７８で動作不許可コマンドがあると、以後の処理を行わずに動作を停止する。したがって、遊技用演算処理装置（アミューズチップ）２２１のプログラムは停止し、遊技は行われない。

【０１５７】

一方、動作不許可コマンドがなければ、ステップＳ９７６に戻ってループを繰り返し、動作許可コマンドがくると遊技用演算処理装置２２１の動作が許可になって遊技が可能になり、ステップＳ９８０に分岐する。ステップＳ９８０では動作許可ＡＣＫを情報収集基板１７３に送信する。これにより、情報収集基板１７３から動作許可コマンドが遊技用演算処理装置２２１に送信されてきたことに応答して、遊技用演算処理装置２２１から動作許可ＡＣＫが返される。次いで、ステップＳ９８２で新しいＩＤがあるか否かを判別する。これは、今回の正当性の判断が正当に終ったので、次回の正当性の判断のために、次回のＩＤ（すなわち、新しいＩＤ）が情報収集基板１７３から送信されてきて、受信したかどうかを判断するものである。新しいＩＤがなければ、このステップＳ９８２に待機し、新しいＩＤが送信されてくると、ステップＳ９８４に進んで新識別情報（新しいＩＤ）を不揮発性メモリ（ＥＥＰＲＯＭ３０４）に記憶する。次いで、ステップＳ９８６でＩＤ受信ＡＣＫを情報収集基板１７３に送信する。これにより、情報収集基板１７３では新しいＩＤを遊技用演算処理装置２２１が受け取ったことを確認する。

【０１５８】

次いで、ステップＳ９８８で内蔵ＲＯＭよりユーザープログラムを読み込み、暗号化データを算出する。これは、遊技用演算処理装置２２１に内蔵のＲＯＭ３０２よりユーザープログラム（すなわち、当該機種の遊技プログラム）を読み出して、後述のように正規のユーザープログラムであるかどうかの判断を行うべく、所定の暗号化データを作成するために暗号化するものである。次いで、ステップＳ９９０で内蔵ＲＯＭのユーザープログラム領域より暗号化データを読み込む。これは、遊技用演算処理装置２２１に内蔵のＲＯＭ３０２における所定のユーザープログラム領域に正規のユーザープログラムであるかどうかの判断を行うための所定の暗号化データがあるので、それを読み出すものである。次いで、ステップＳ９９２で暗号化データは正常であるか否かを判別する。これは、ステップＳ９８８で作成した所定の暗号化データと、ステップＳ９９０で読み出した所定のユーザープログラム領域にある暗号化データとを比較して、内蔵ＲＯＭ３０２に格納されているユーザープログラム（当該機種の遊技プログラム）が正当なものであるかどうかを判断するものである。

【０１５９】

ステップＳ９９２の判別結果で、暗号化データが正常でなく、異常であれば、以後の処理を行わずに動作を停止する。したがって、遊技用演算処理装置（アミューズチップ）２２１のプログラムは停止し、遊技は行われない。一方、ステップＳ９９２の判別結果で、暗号化データが正常であれば、ステップＳ９９４に進んでプログラム領域をユーザー領域に

切り換える。これにより、遊技用演算処理装置２２１に内蔵のＲＯＭ３０２におけるユーザープログラム（当該機種の遊技プログラム）によって遊技が行われる。

【０１６０】

以上のプログラムを実行することによるアミューズチップ用ＩＤ（識別情報）を毎回の動作開始時に変更してチェックする動作について、図７５を参照して説明する。

図７５に示すように、情報収集基板１７３には上位ネット局であるネットワーク監視装置３６から識別情報（アミューズチップ用ＩＤ）が送信され、格納されている。さらに、ネットワーク監視装置３６はその上位局である情報管理装置２から識別情報を受信している。したがって、情報収集基板１７３は遊技店１の開店時に毎回識別情報を上位局から受信することになる。

なお、情報収集基板１７３が識別情報を得るのは、ネットワークを介して上位局の情報管理装置２からであるが、これに限らず、例えば識別情報を情報収集基板１７３の中に格納しておいてもよい。

【０１６１】

開店時には、次いで、情報収集基板１７３から役物制御基板１７１の遊技用演算処理装置（アミューズチップ）２２１に識別情報読出コマンドが送信される。識別情報読出コマンドは暗号化していてもよいし、暗号化していなくてもよい。識別情報読出コマンドを受信すると、遊技用演算処理装置２２１は不揮発性メモリ（ＥＥＰＲＯＭ３０４）より識別情報を読み込み、情報収集基板１７３に送信する。情報収集基板１７３では、遊技用演算処理装置２２１から送信されてきた識別情報の正当性を判定し（判定処理を行い：暗号化されていれば復号化して判定し）、ＯＫあるいはＮＧを判断する。そして、識別情報の正当性の判定結果がＮＧであれば、遊技用演算処理装置２２１に動作不許可コマンドを送信し、これにより、遊技用演算処理装置２２１は動作を停止する。

【０１６２】

識別情報の正当性の判定結果がＯＫであれば、次いで、識別情報形式変更処理を行う。識別情報形式変更処理とは、識別情報あるいは識別情報を暗号化する暗号化情報のうち、少なくとも１つ以上を前回の情報と異ならせて処理を行うものである。

ここで、識別情報形式変更処理には、識別情報の解読を困難にする方法として、以下の４つの処理方法がある。

（ａ）識別情報は一定で、暗号化情報を異ならせるもの

識別情報は一定であり暗号化情報によって暗号化しておき、遊技用演算処理装置２２１の不揮発性メモリ（ＥＥＰＲＯＭ３０４）に記憶させておく。開店時に遊技用演算処理装置２２１より暗号化されている識別情報を読み込み、情報収集基板１７３の「判定処理」で復号化情報を用いて復号化し、識別情報を判定する。そして、ＯＫであれば、「識別情報形式変更処理」で新たな暗号化情報で暗号化し、新識別情報を遊技用演算処理装置２２１に送信して記憶させる。

このように、識別情報は常に一定で、暗号化情報を毎回（すなわち、遊技機の電源オン動作時）異ならせることにより、識別情報の解読を困難にする。

【０１６３】

（ｂ）暗号化情報は一定で、識別情報を異ならせるもの

暗号化情報は一定であり、一定の暗号化情報によって識別情報を暗号化しておき、遊技用演算処理装置２２１の不揮発性メモリ（ＥＥＰＲＯＭ３０４）に記憶させておく。開店時に遊技用演算処理装置２２１より暗号化されている識別情報を読み込み、情報収集基板１７３の「判定処理」では一定の復号化情報を用いて復号化し、識別情報を判定する。そして、ＯＫであれば、「識別情報形式変更処理」で新たな識別情報を一定の暗号化情報で暗号化し、新識別情報を遊技用演算処理装置２２１に送信して記憶させる。

このように、暗号化情報は常に一定で、識別情報を毎回（すなわち、遊技機の電源オン動作時）異ならせることにより、識別情報の解読を困難にする。

【０１６４】

（ｃ）識別情報および暗号化情報を異ならせるもの

暗号化情報によって識別情報を暗号化しておき、遊技用演算処理装置２２１の不揮発性メモリ（ＥＥＰＲＯＭ３０４）に記憶させておく。開店時に遊技用演算処理装置２２１より暗号化されている識別情報を読み込み、情報収集基板１７３の「判定処理」では復号化情報を用いて復号化し、識別情報を判定する。そして、ＯＫであれば、「識別情報形式変更処理」で新たな識別情報を新たな暗号化情報で暗号化し、新識別情報を遊技用演算処理装置２２１に送信して記憶させる。
このように、識別情報および暗号化情報をそれぞれ毎回（すなわち、遊技機の電源オン動作時）異ならせることにより、識別情報の解読を困難にする。本実施例では、（ｃ）の方法を採用している。この方法では、識別情報および暗号化情報が毎回異なるので、最も識別情報の解読を困難にできるという特長がある。

【０１６５】
（ｄ）識別情報を暗号化せず生のデータとし、識別情報を異ならせるもの
識別情報は暗号化せずに、遊技用演算処理装置２２１の不揮発性メモリ（ＥＥＰＲＯＭ３０４）に記憶させておく。開店時に遊技用演算処理装置２２１より暗号化されていない識別情報を読み込み、情報収集基板１７３の「判定処理」で識別情報を判定する。そして、ＯＫであれば、「識別情報形式変更処理」で新たな識別情報（つまり新識別情報）を暗号化せずに遊技用演算処理装置２２１に送信して記憶させる。
このように、識別情報を暗号化せず、識別情報を毎回（すなわち、遊技機の電源オン動作時）異ならせることにより、識別情報の解読を困難にする。この方法であると、処理が簡単で済むという利点がある。
さて、識別情報形式変更処理を行うと、次いで、新識別情報を遊技用演算処理装置２２１に送信して、その不揮発性メモリ（ＥＥＰＲＯＭ３０４）に記憶させ、遊技用演算処理装置２２１の動作を許可する。これにより、遊技用演算処理装置２２１を使用した遊技が可能になる。

【０１６６】
次に、本実施例では第３者機関２４の情報処理装置より遊技店１の情報管理装置２に電話回線２３を介して識別情報形式情報を送信し、さらに情報管理装置２よりネットワークを介してネットワーク監視装置３６に識別情報形式情報を送信し、次いで、ネットワーク監視装置３６よりＬＯＮを介して遊技機２１の情報収集基板１７３に識別情報形式情報を送信する構成になっている。これにより、一元的に第３者機関２４から一元的に情報収集基板１７３に識別情報形式情報を配信する構成となる。
この場合、送信される識別情報形式情報は上述した識別情報の解読を困難にする４つの処理方法に対応して、以下のような内容になる。

【０１６７】
・処理方法（ａ）の場合（識別情報は一定で、暗号化情報を異ならせるもの）
識別情報は一定なので、更新用および判別用の識別情報は不要であり、暗号化するための新たな暗号化情報、復号化するための復号化情報を送信することになる。
・処理方法（ｂ）の場合（暗号化情報は一定で、識別情報を異ならせるもの）
更新された識別情報、判別するための識別情報、暗号化するための暗号化情報、復号化するための復号化情報を送信することになる。
・処理方法（ｃ）の場合（識別情報および暗号化情報を異ならせるもの）
更新した識別情報、判別するための識別情報、暗号化するための新たな暗号化情報、復号化するための復号化情報を送信することになる。
・処理方法（ｄ）の場合（識別情報を暗号化せず生のデータとし、識別情報を異ならせるもの）
更新した識別情報と、判別するための識別情報のみを送信することになる。

【０１６８】
このように、本実施例では役物制御基板１７１を管理する遊技用演算処理装置（アミューズチップ）２２１を認識するアミューズチップ用ＩＤを、遊技用演算処理装置２２１の不揮発性メモリ（ＥＥＰＲＯＭ３０４）に記録し、遊技用演算処理装置２２１を含む役物制

御基板１７１を監視するとともに役物制御基板１７１よりの遊技情報（例えば、大当り情報、特図回転信号、始動口信号等）を収集する情報収集基板１７３を設け、情報収集基板１７３が遊技用演算処理装置２２１の不揮発性メモリ（ＥＥＰＲＯＭ３０４）に記録されている識別情報を読み出して、遊技用演算処理装置２２１の正当性を判断し正当な場合に遊技を許可し、識別情報の判別が正当に完了したら、新たな識別情報を遊技用演算処理装置２２１に送信してその不揮発性メモリ（ＥＥＰＲＯＭ３０４）に記録させ、次回の判定時（例えば、次の日の開店時）には、記録させた新たな識別情報を用いて正当性の判定を行う。すなわち、識別情報が毎回（例えば、遊技機２１の電源オン動作時）変更される。したがって、以下の効果を得ることができる。

【０１６９】

（１）遊技用演算処理装置２２１の識別情報を毎回の動作開始（遊技用演算処理装置２２１の動作開始）時にチェックして変更することにより、遊技用演算処理装置２２１の改竄を極めて困難にすることができる。

従来、遊技用演算処理装置に識別情報を記録しておき、その識別情報を判別して遊技用演算処理装置の正当性を判断するシステムでは、識別情報が固定化されたデータであったため、一度、解読されると、遊技用演算処理装置の改竄が可能になっていたが、これに対して本実施例では、識別情報が固定化されておらず、遊技用演算処理装置２２１の毎回の動作開始時に変更されるので、解読が極めて困難であり、不正を有効に防止することができる。

【０１７０】

（２）遊技用演算処理装置２２１のユーザープログラムを改竄した偽造品の量産を極めて困難にすることができる。

特に、ワンチップ化した遊技用演算処理装置の場合、ソケット差しで、着脱が容易となって交換されることにより、遊技プログラム（ユーザープログラム）を改竄するという不正を誘発する恐れがあったが、本実施例では遊技プログラム（ユーザープログラム）の改竄を極めて困難にすることができる。

【０１７１】

（３）識別情報を暗号化することにより、最悪、遊技用演算処理装置２２１が遊技店１から盗用されてユーザープログラム等を改竄しようとする行為があっても、改竄しようとする暗号を解読するのに時間を要し、改竄を事実上不可能にすることができる。

【０１７２】

（４）遊技用演算処理装置２２１の識別情報を毎回の動作開始時にチェックし、識別情報の非正当性が認められた場合、情報収集基板１７３から役物制御基板１７１に遊技制御の動作不許可を指令することにより、遊技を実行できなくし、不正を有効に防止することができる。

（５）情報収集基板１７３により遊技機２１における遊技において発生した遊技情報を収集することにより、情報収集基板１７３は遊技用演算処理装置２２１の監視を行うだけでなく、遊技情報を収集する機能も併せて実行することができ、遊技情報を収集する部品を別に配置する必要がなく、遊技機２１における省スペース化やパーツの有効利用化を図ることができる。

【０１７３】

（６）情報管理装置２よりネットワークを介してネットワーク監視装置３６に識別情報形式情報を送信し、さらにネットワーク監視装置３６よりＬＯＮを介して情報収集基板１７３に識別情報形式情報を送信することにより、一元的に情報管理装置２から情報収集基板１７３に識別情報形式情報を配信するので、情報管理装置２において一括して識別情報の監視、管理を行うことができ、不正に有効に対処することができる。

（７）第３者機関２４により遊技店１の情報管理装置２に識別情報形式情報を送信し、さらにネットワークを介して情報収集基板１７３に識別情報形式情報を送信することにより、第３者機関２４から一元的に情報収集基板１７３に識別情報形式情報を配信するので、第３者機関２４において一括して識別情報の監視、管理を行うことができ、不正に有効に

対処することができる。

【０１７４】

（８）第３者機関２４より送信される識別情報形式情報を記憶する情報収集基板１７３における記憶手段として揮発メモリであるＲＡＭ２０９を使用しているので、情報収集基板１７３の電源がオフすると、当該識別情報形式情報は消失する。したがって、情報収集基板１７３を盗用すると、電源がオフし、重要である識別情報形式情報が消去されるので、改竄に対する安全性を高めることができる。

（９）従来、遊技装置製造メーカーが射幸心を抑制する遊技装置を開発しても、遊技用演算処理装置が改竄されたのでは、間接的に遊技者に不当にギャンブル性の高い遊技機を提供してしまう結果となり、射幸心を抑制するという最近のホールの営業方針にも反することになっていたが、これに対して、本実施例では遊技用演算処理装置２２１の改竄が困難であるので、遊技者に不当にギャンブル性の高い遊技機（遊技プログラムが改竄されたもの）を提供することを防止でき、射幸心を抑制するという最近のホールの営業方針に沿わせることができる。また、本実施例では上述したように、識別情報を毎回異ならせることにより、改竄を困難にするのが目的であり、識別情報の変更は開店時に行うのに限らず、例えば所定時間毎に行ってもよい。

【０１７５】

本発明の実施の形態は、上記実施例に限らず、以下に述べるような各種の変形実施が可能である。

（ａ）遊技装置はパチンコ遊技機に限らず、パチスロ遊技機への適用が可能である。

（ｂ）本発明はパチンコ遊技機でなく、例えば映像式ゲーム機のようにものにも適用できる。

（ｃ）遊技装置としての遊技機は実球式に限るものではなく、封入球式の遊技機であってもよい。すなわち、遊技装置としての遊技機は、役物制御装置を備え、識別情報を記録可能なものであれば、どのような種類の遊技機でも本発明を適用できる。例えば、磁気カードで玉貸しを行うもの、ＩＣカードで玉貸しを行う等の遊技装置のタイプに限定されずに、本発明を適用することができる。

（ｄ）遊技店内の通信ネットワークは識別情報の転送が可能なものであれば、光通信、ＬＡＮ、ＬＯＮ等の種類に限らず、どのようなネットワークシステムを使用してもよい。

【０１７６】

【発明の効果】

本発明によれば、ＣＰＵ、ＲＡＭ、遊技プログラムを格納したＲＯＭ、識別情報を記録する不揮発性メモリ等を内蔵してワンチップ化した遊技用演算処理装置を有する役物制御装置の不揮発性メモリに記録されている識別情報を読み込んで正当性を判断し、正当な場合に役物制御装置へ遊技制御の許可を指令するとともに、識別情報形式情報を変更した新識別情報を送信し、新識別情報の不揮発性メモリへの記録を指令し、第３者機関によって識別情報形式を変更するための識別情報形式情報が提供され、提供された識別情報形式情報を遊技店の情報管理装置で受信し、該情報管理装置より送信される識別情報形式を変更するための識別情報形式情報を記憶しておき、情報管理装置で開店操作された際に送信された識別情報形式情報である前回の識別情報、該前回の識別情報を復号化するための今回の復号化情報、次回の識別情報および該次回の識別情報を暗号化するための次回の暗号化情報を記憶手段に記憶した場合に、役物制御装置の不揮発性メモリに記憶されている暗号化された識別情報を読み込み、役物制御装置から読み込んだ暗号化された識別情報を前記今回の復号化情報により復号化し、該復号化した識別情報と、前記前回の識別情報とを比較して正当性を判別し、識別情報判別手段により正当性が認められた場合に、前記次回の識別情報を前記次回の暗号化情報で暗号化した新識別情報の前記不揮発性メモリへの記録を指令するようにしているので、以下の効果を得ることができる。

役物制御装置の識別情報を毎回の動作開始（例えば、役物制御装置の動作開始）時にチェックして変更することにより、役物制御装置の改竄を極めて困難にすることができる。

従来、遊技用演算処理装置に識別情報を記録しておき、その識別情報を判別して遊技用

演算処理装置の正当性を判断するシステムでは、識別情報が固定化されたデータであったため、一度、解読されると、遊技用演算処理装置の改竄が可能になっていたが、これに対して本発明では、識別情報が固定化されておらず、役物制御装置のユーザープログラムを改竄した偽造品の量産を極めて困難にすることができる。

特に、ワンチップ化した遊技用演算処理装置の場合、ソケット差しで、着脱が容易となって交換されることにより、遊技プログラム（ユーザープログラム）を改竄するという不正を誘発する恐れがあったが、本発明では遊技プログラム（ユーザープログラム）の改竄を極めて困難にすることができる。

従来、遊技装置製造メーカーが射幸心を抑制する遊技装置を開発しても、遊技用演算処理装置が改竄されたのでは、間接的に遊技者に不当にギャンブル性の高い遊技機を提供してしまう結果となり、射幸心を抑制するという最近のホールの営業方針にも反することになっていたが、これに対して、本発明では遊技用演算処理装置の改竄が困難であるので、遊技者に不当にギャンブル性の高い遊技機（遊技プログラムが改竄されたもの）を提供することを防止でき、射幸心を抑制するという最近のホールの営業方針に沿わせることができる。

また、役物制御装置に記録される識別情報の暗号化、読み込まれた識別情報判別する際の復号化、および新識別情報の暗号化／復号化を行うことにより、すなわち暗号化して役物制御装置へ記録することにより、識別情報の形式が分からず（例えば、どのような情報が識別情報であるということ自体が暗号化情報を見ただけでは不明である）、盗用されることがない。また、暗号化情報を毎回異ならせることから、上述と同様の効果がある。

【図面の簡単な説明】

【図１】本発明に係る遊技装置の監視装置を適用した遊技場設備の一実施例を示す全体構成図である。

【図２】情報管理装置の構成を示すブロック図である。

【図３】ネットワーク監視装置の構成を示すブロック図である。

【図４】Ｎボードの構成を示すブロック図である。

【図５】遊技機の構成を示すブロック図である。

【図６】情報収集基板の構成を示すブロック図である。

【図７】役物制御基板の構成を示すブロック図である。

【図８】遊技用演算処理装置の構成を示すブロック図である。

【図９】情報管理装置のメインルーチンを示すフローチャートである。

【図１０】情報管理処理のサブルーチンを示すフローチャートである。

【図１１】第３者機関処理のサブルーチンを示すフローチャートである。

【図１２】ホール内装置処理のサブルーチンを示すフローチャートである。

【図１３】ネットワーク監視装置処理のサブルーチンを示すフローチャートである。

【図１４】ネットワーク監視装置との開店処理のサブルーチンを示すフローチャートである。

【図１５】開店確認処理のサブルーチンを示すフローチャートである。

【図１６】第３者機関へ認証ＩＤ送信処理のサブルーチンを示すフローチャートである。

【図１７】第３者機関からの認証ＩＤ受信待ち処理のサブルーチンを示すフローチャートである。

【図１８】第３者機関との認証ＩＤ比較処理のサブルーチンを示すフローチャートである。

【図１９】ネットワーク監視装置へ認証ＩＤ送信処理のサブルーチンを示すフローチャートである。

【図２０】ネットワーク監視装置からの認証ＩＤ受信待ち処理のサブルーチンを示すフローチャートである。

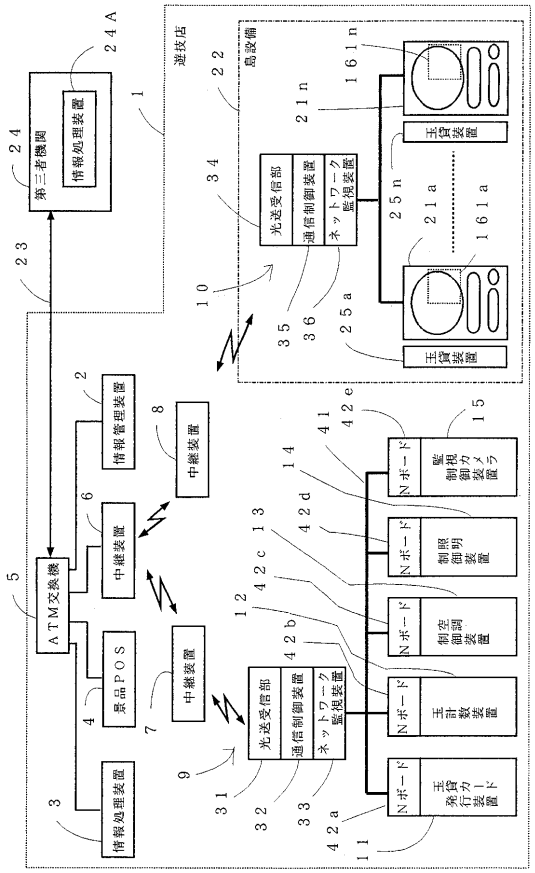
【図２１】ネットワーク監視装置との認証ＩＤ比較処理のサブルーチンを示すフローチャートである。

【図２２】ネットワーク監視装置からの情報収集基板の認証状態受信待ち処理のサブルー

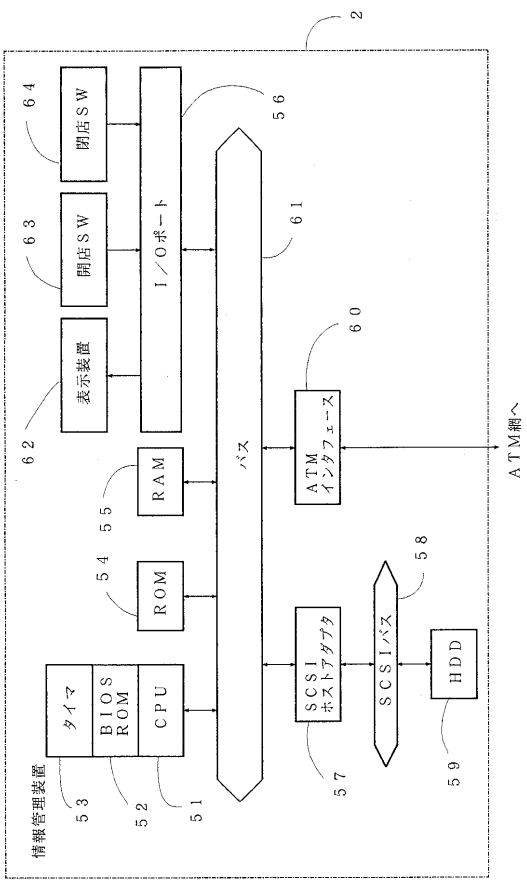
チンを示すフローチャートである。
【図２３】ネットワーク監視装置からの情報収集基板の認証ＩＤ比較結果処理のサブルーチンを示すフローチャートである。
【図２４】アミューズチップ用のＩＤ等の送信処理のサブルーチンを示すフローチャートである。
【図２５】ＩＤチェック確認終了待ち処理のサブルーチンを示すフローチャートである。
【図２６】ネットワーク監視装置との閉店処理のサブルーチンを示すフローチャートである。
【図２７】閉店確認処理のサブルーチンを示すフローチャートである。
【図２８】アミューズチップ用のＩＤ消去の送信処理のサブルーチンを示すフローチャートである。
【図２９】アミューズチップ用のＩＤ消去ＡＣＫ待ち処理のサブルーチンを示すフローチャートである。
【図３０】ネットワーク監視装置のポーリング処理のサブルーチンを示すフローチャートである。
【図３１】ポーリング処理のサブルーチンを示すフローチャートである。
【図３２】ポーリング応答確認処理のサブルーチンを示すフローチャートである。
【図３３】セレクティング処理のサブルーチンを示すフローチャートである。
【図３４】データ送信のサブルーチンを示すフローチャートである。
【図３５】送信に対するＡＣＫ待ち処理のサブルーチンを示すフローチャートである。
【図３６】ネットワーク監視装置の受信処理のサブルーチンを示すフローチャートである。
【図３７】異常表示処理のサブルーチンを示すフローチャートである。
【図３８】ネットワーク監視装置のメインルーチンを示すフローチャートである。
【図３９】情報管理装置送受信タスクのサブルーチンを示すフローチャートである。
【図４０】情報収集基板通信受信タスクのサブルーチンを示すフローチャートである。
【図４１】タイマタスクのサブルーチンを示すフローチャートである。
【図４２】認証ＩＤ処理のサブルーチンを示すフローチャートである。
【図４３】情報管理装置との認証ＩＤ比較処理のサブルーチンを示すフローチャートである。
【図４４】情報収集基板との認証ＩＤ比較処理のサブルーチンを示すフローチャートである。
【図４５】アミューズチップ用のＩＤ消去処理のサブルーチンを示すフローチャートである。
【図４６】異常表示処理のサブルーチンを示すフローチャートである。
【図４７】情報収集基板とのポーリング処理のサブルーチンを示すフローチャートである。
【図４８】ポーリング開始処理のサブルーチンを示すフローチャートである。
【図４９】ポーリング端末応答確認処理のサブルーチンを示すフローチャートである。
【図５０】セレクティング処理のサブルーチンを示すフローチャートである。
【図５１】データ送信処理のサブルーチンを示すフローチャートである。
【図５２】ＡＣＫ待ち処理のサブルーチンを示すフローチャートである。
【図５３】情報収集基板のメインルーチンを示すフローチャートである。
【図５４】役物回路からの受信タスクのサブルーチンを示すフローチャートである。
【図５５】ネットワーク監視装置からの受信タスクのサブルーチンを示すフローチャートである。
【図５６】タイマタスクのサブルーチンを示すフローチャートである。
【図５７】ネットワーク監視装置送信処理のサブルーチンを示すフローチャートである。
【図５８】ネットワーク監視装置からのポーリング応答処理のサブルーチンを示すフローチャートである。

【図５９】ネットワーク監視装置からのセレクティング応答処理のサブルーチンを示すフローチャートである。
【図６０】役物回路への送信処理のサブルーチンを示すフローチャートである。
【図６１】ＩＤ確認処理のサブルーチンを示すフローチャートである。
【図６２】ネットワーク監視装置からの認証ＩＤ受信処理待ち処理のサブルーチンを示すフローチャートである。
【図６３】ネットワーク監視装置との認証ＩＤ比較処理のサブルーチンを示すフローチャートである。
【図６４】ネットワーク監視装置からのアミューズチップ用ＩＤ受信待ち処理のサブルーチンを示すフローチャートである。
【図６５】役物回路へアミューズチップ用ＩＤ要求処理のサブルーチンを示すフローチャートである。
【図６６】役物からの前回のアミューズチップ用ＩＤ受信待ち処理のサブルーチンを示すフローチャートである。
【図６７】前回のアミューズチップ用ＩＤの復号化処理のサブルーチンを示すフローチャートである。
【図６８】アミューズチップ用ＩＤ比較処理のサブルーチンを示すフローチャートである。
【図６９】役物回路へ次回のアミューズチップ用ＩＤの暗号化と送信処理のサブルーチンを示すフローチャートである。
【図７０】役物回路からの次回のアミューズチップ用ＩＤ受信ＡＣＫ待ち処理のサブルーチンを示すフローチャートである。
【図７１】アミューズチップ用ＩＤ消去処理のサブルーチンを示すフローチャートである。
【図７２】役物回路のアウト玉入力タスクのサブルーチンを示すフローチャートである。
【図７３】玉貸機の玉貸入力タスクのサブルーチンを示すフローチャートである。
【図７４】遊技用演算処理装置のプログラムを示すフローチャートである。
【図７５】アミューズチップ用ＩＤのチェック動作を説明する図である。
【符号の説明】
１　遊技店
２　情報管理装置
３　情報処理装置
９、１０　局管理装置
２１　パチンコ遊技機（遊技機：遊技装置）
２４　第３者機関
３３、３６　ネットワーク監視装置
４２ａ～４２ｅ　Ｎボード
１６１　役物制御装置
１７１　役物制御基板
１７３　情報収集基板（遊技装置の監視装置：識別情報読込手段、識別情報判別手段、遊技制御許可手段、遊技情報収集手段）
２０９　ＲＡＭ（記憶手段）
２２１　遊技用演算処理装置

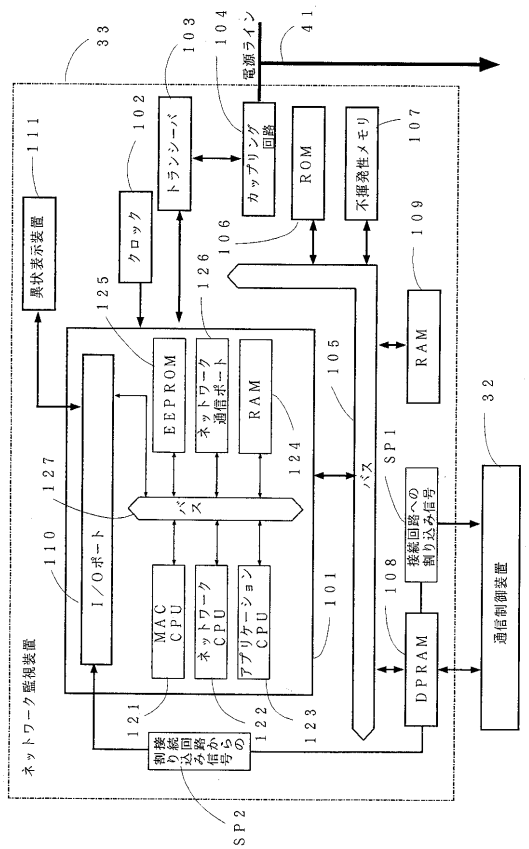
【図１】


遊技店
島設備
第三者機関
情報処理装置
ＡＴＭ交換機
情報管理装置
中継装置
景品ＰＯＳ
光送受信部
通信制御装置
ネットワーク監視装置
玉貸装置
Ｎボード
玉計数装置
発信カード装置
制空部調装置
制照部明装置
監視制御カメラ装置

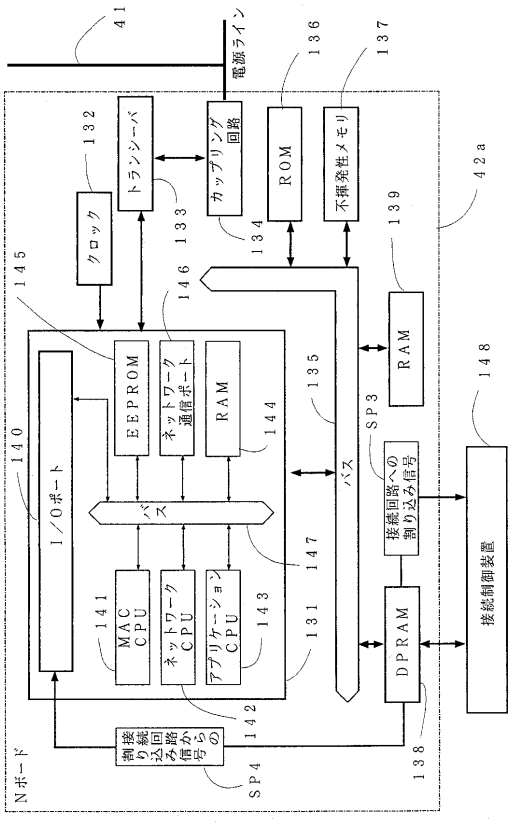
【図２】


情報管理装置
ＣＰＵ
ＢＩＯＳ ＲＯＭ
タイマ
ＲＯＭ
ＲＡＭ
バス
Ｉ／Ｏポート
閉店ＳＷ
開店ＳＷ
表示装置
ＡＴＭインタフェース
ＳＣＳＩホストアダプタ
ＳＣＳＩバス
ＨＤＤ
ＡＴＭ網へ

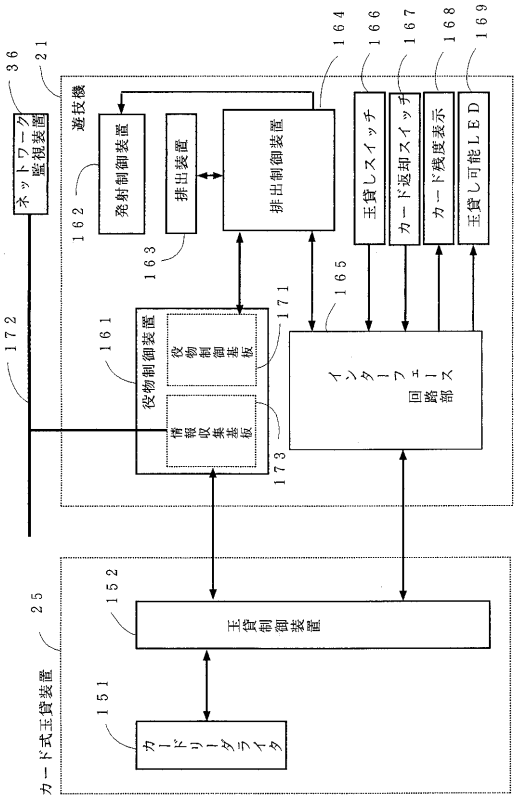
【図３】


ネットワーク監視装置
異状表示装置
Ｉ／Ｏポート
ＭＡＣ ＣＰＵ
ネットワーク ＣＰＵ
アプリケーション ＣＰＵ
ＥＥＰＲＯＭ
ネットワーク通信ポート
ＲＡＭ
バス
クロック
トランシーバ
カップリング回路
ＲＯＭ
不揮発性メモリ
ＲＡＭ
ＤＰＲＡＭ
電源ライン
接続回路への割り込み信号
割り込み信号からの接続回路
通信制御装置

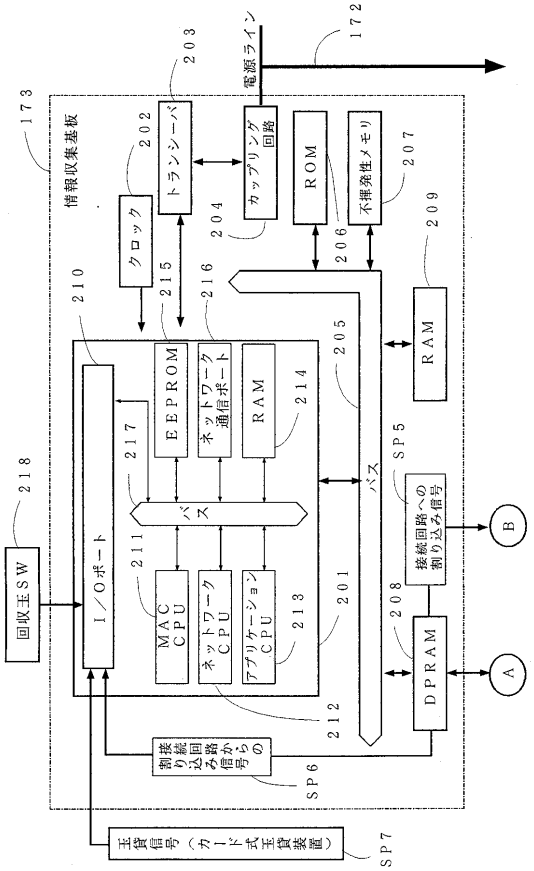
【図４】


Ｎボード
Ｉ／Ｏポート
ＭＡＣ ＣＰＵ
ネットワーク ＣＰＵ
アプリケーション ＣＰＵ
ＥＥＰＲＯＭ
ネットワーク通信ポート
ＲＡＭ
バス
クロック
トランシーバ
カップリング回路
ＲＯＭ
不揮発性メモリ
ＲＡＭ
ＤＰＲＡＭ
電源ライン
接続回路への割り込み信号
割り込み信号からの接続回路
接続制御装置

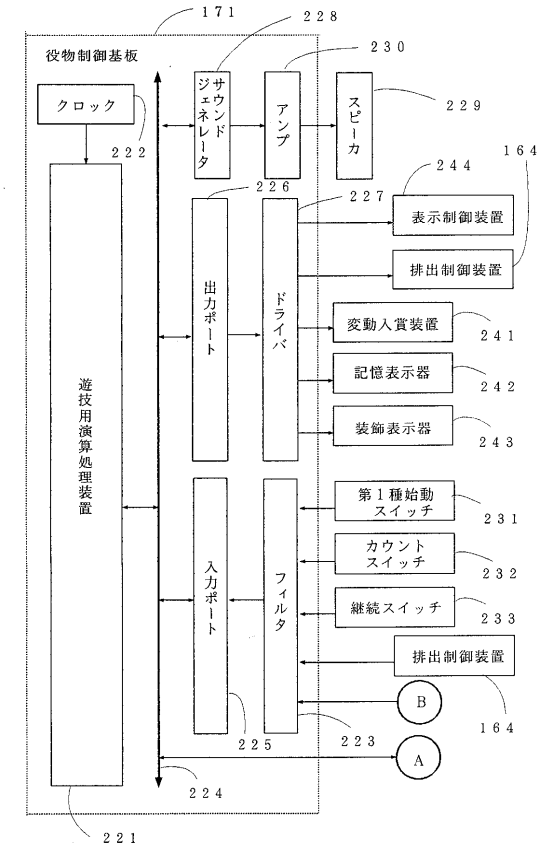
【図５】


遊技機
ネットワーク監視装置
発射制御装置
排出装置
排出制御装置
玉貸しスイッチ
カード返却スイッチ
カード残度表示
玉貸し可能ＬＥＤ
役物制御装置
役物制御基板
情報収集基板
インターフェース回路部
カード式玉貸装置
玉貸制御装置
カードリーダライタ

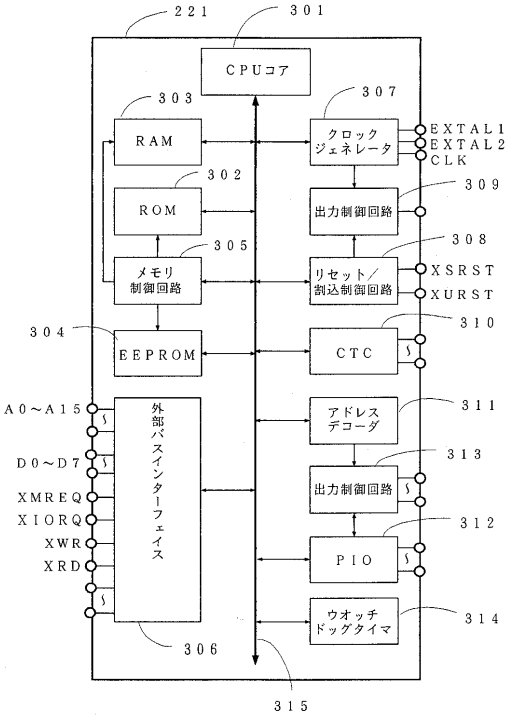
【図６】


電源ライン
情報収集基板
トランシーバ
クロック
カップリング回路
ROM
不揮発性メモリ
RAM
EEPROM
ネットワーク通信ポート
RAM
バス
I／Oポート
回収玉SW
MAC CPU
ネットワーク CPU
アプリケーション CPU
DPRAM
接続回路への割り込み信号
割り込み信号
玉貸信号（カード式玉貸装置）

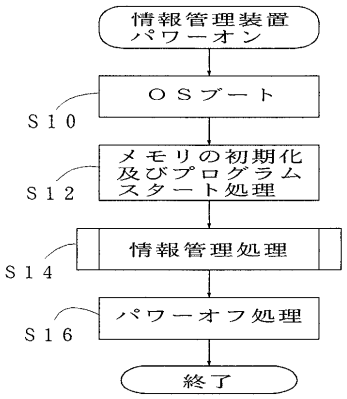
【図７】


役物制御基板
クロック
サウンドジェネレータ
アンプ
スピーカ
出力ポート
ドライバ
表示制御装置
排出制御装置
変動入賞装置
記憶表示器
装飾表示器
入力ポート
フィルタ
第１種始動スイッチ
カウントスイッチ
継続スイッチ
排出制御装置
遊技用演算処理装置

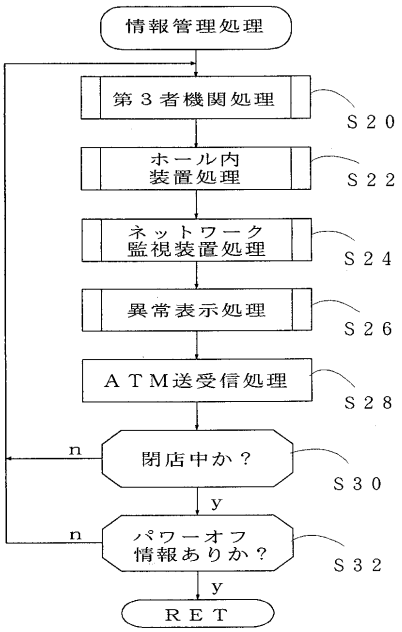
【図８】


CPUコア
RAM
ROM
メモリ制御回路
EEPROM
外部バスインターフェイス
クロックジェネレータ
出力制御回路
リセット／割込制御回路
CTC
アドレスデコーダ
出力制御回路
PIO
ウオッチドッグタイマ
EXTAL1
EXTAL2
CLK
XSRST
XURST
A0～A15
D0～D7
XMREQ
XIORQ
XWR
XRD

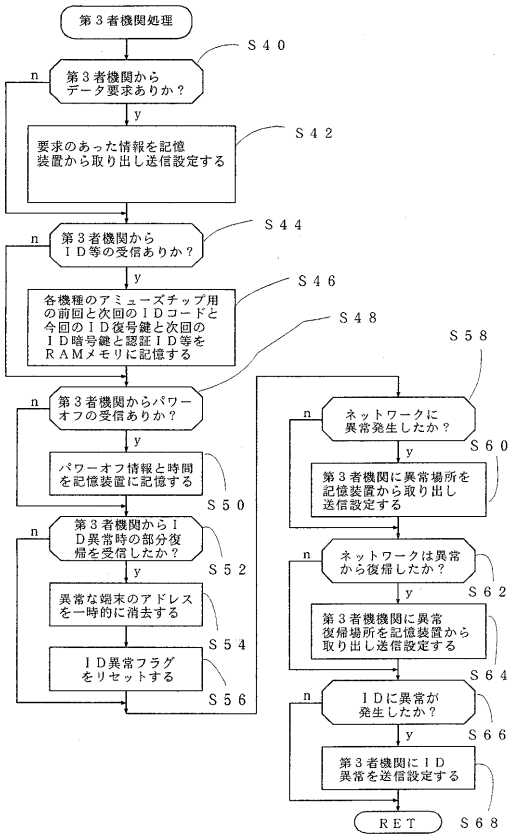
【図９】



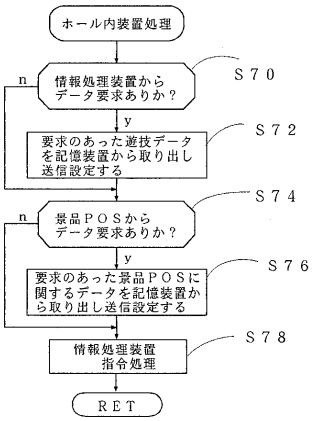
【図１０】



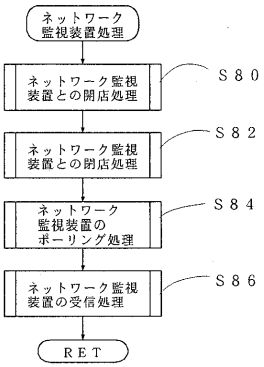
【図１１】



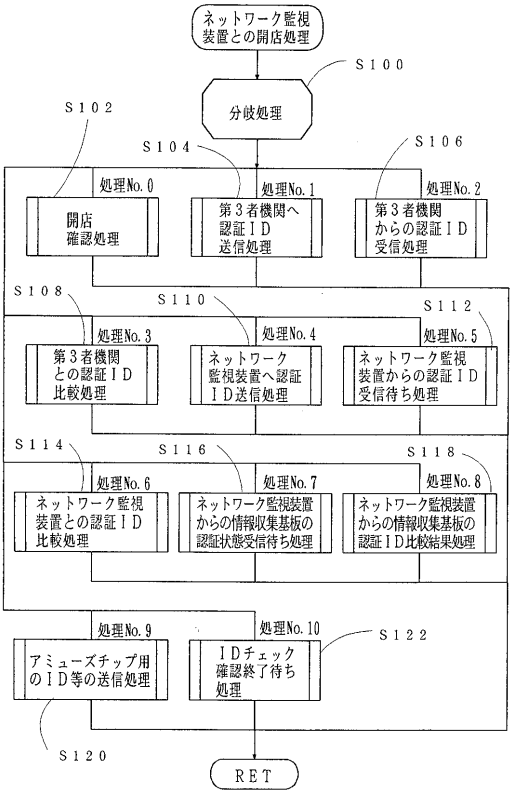
【図１２】



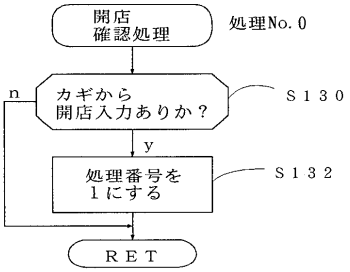
【図１３】



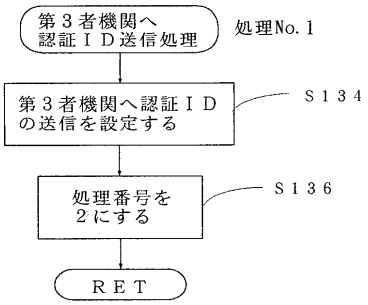
【図１４】



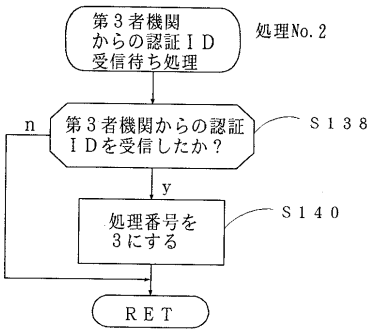
【図１５】



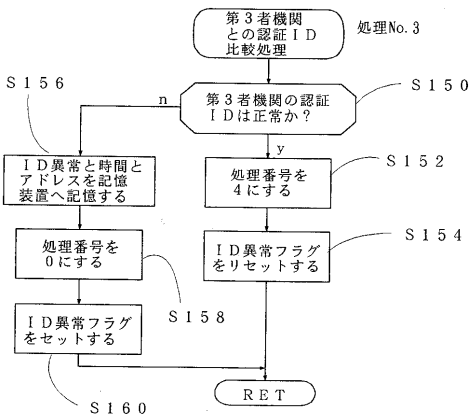
【図１６】



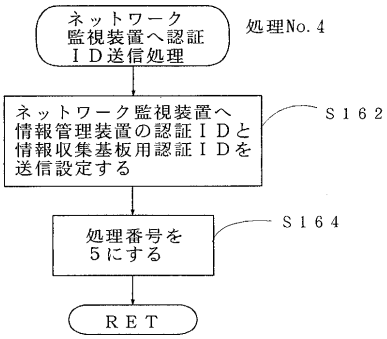
【図１７】



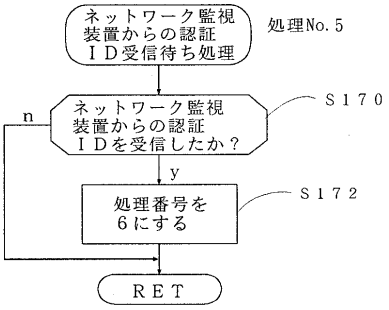
【図１８】



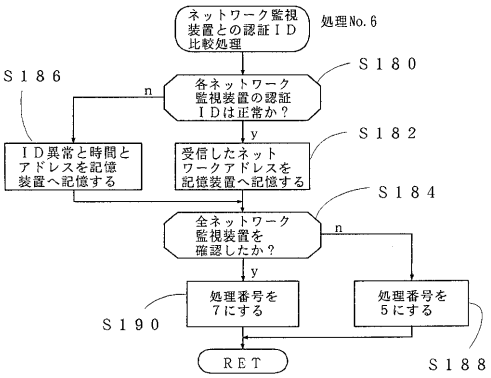
【図１９】



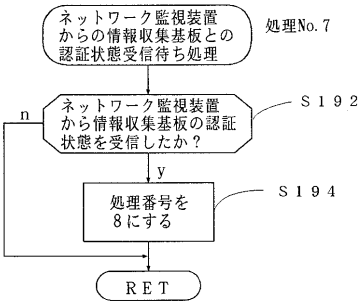
【図２０】



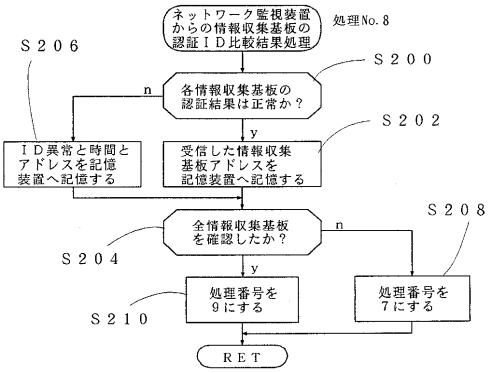
【図２１】



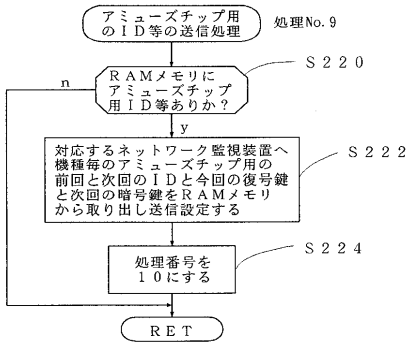
【図２２】



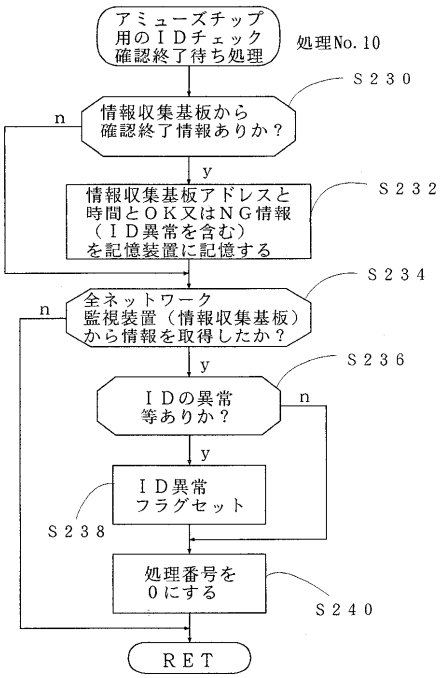
【図２３】



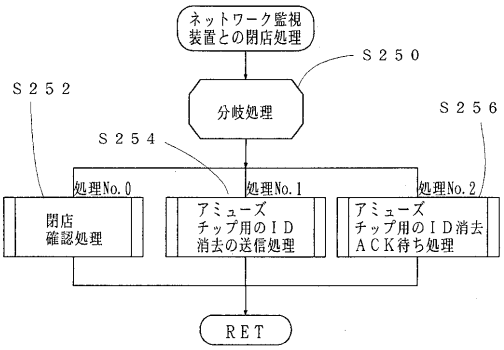
【図２４】



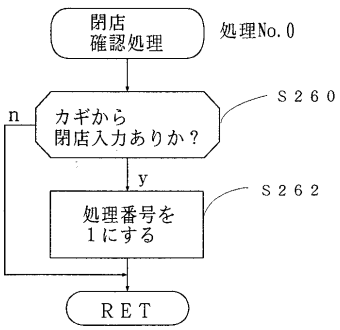
【図２５】



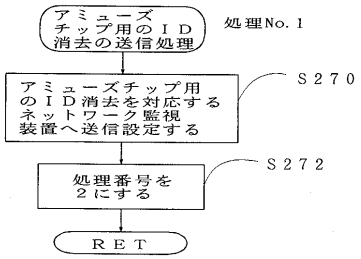
【図２６】



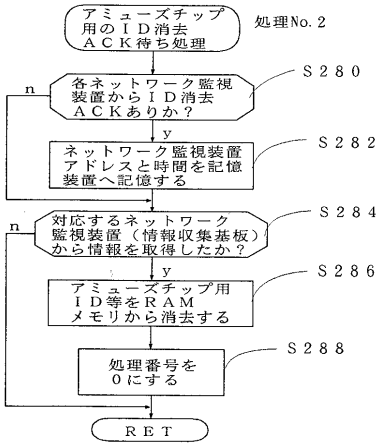
【図２７】



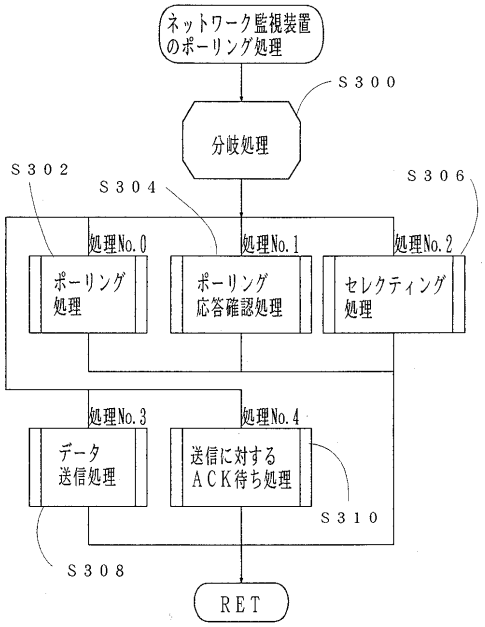
【図２８】



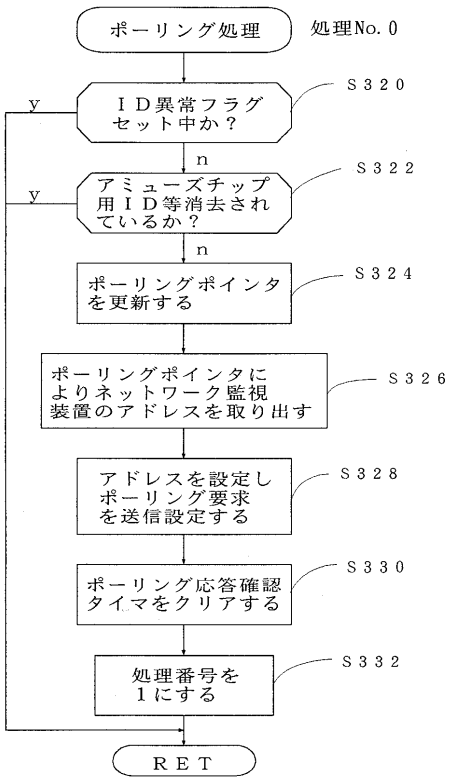
【図２９】



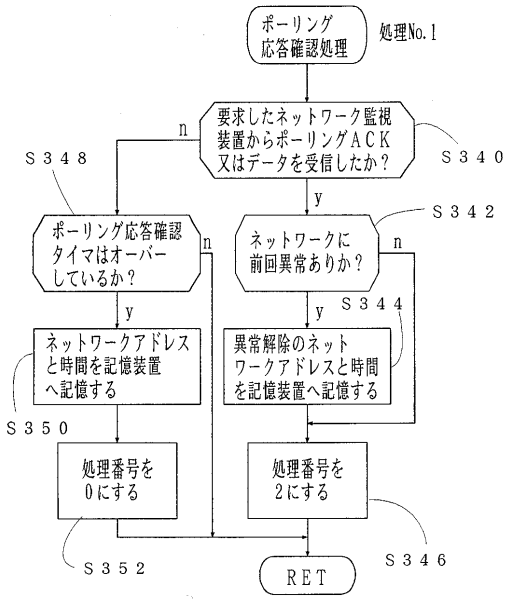
【図３０】



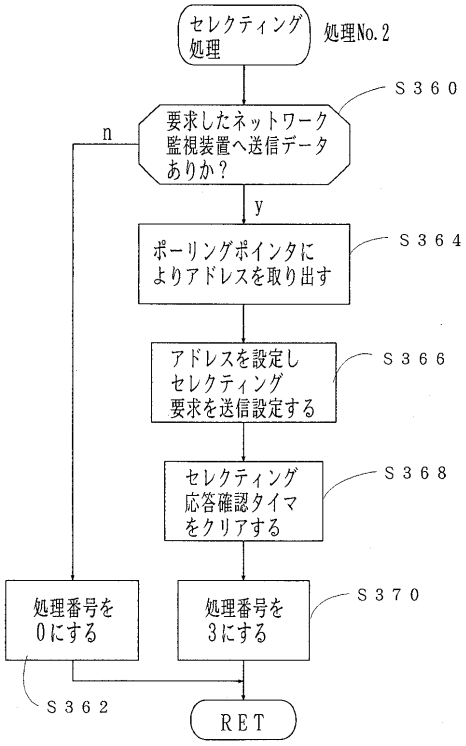
【図３１】



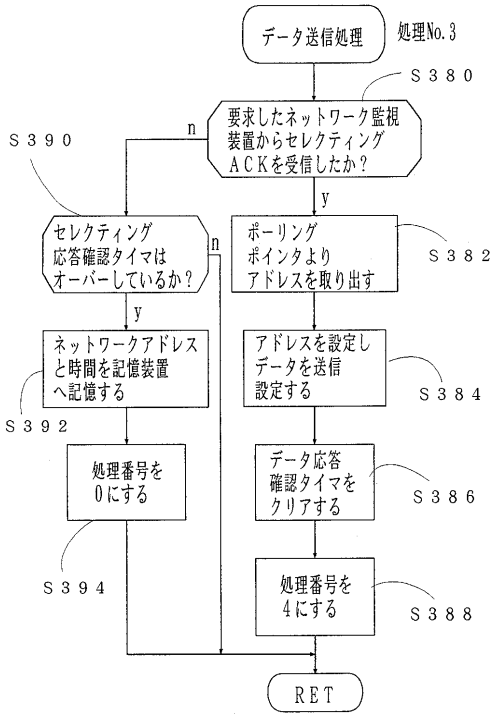
【図３２】



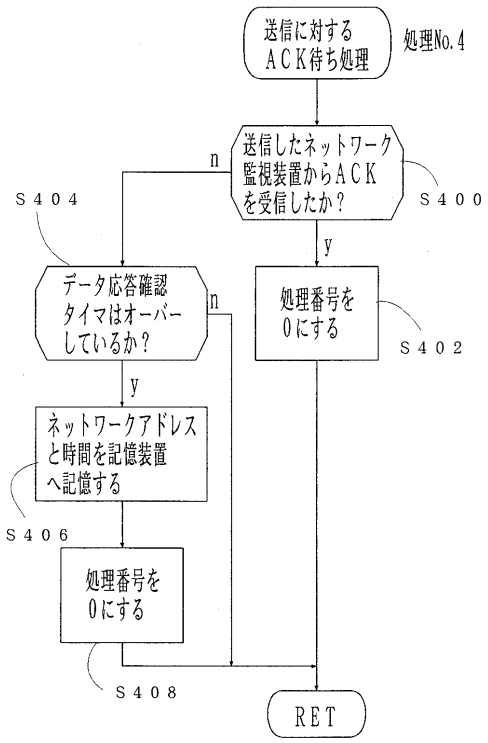
【図３３】



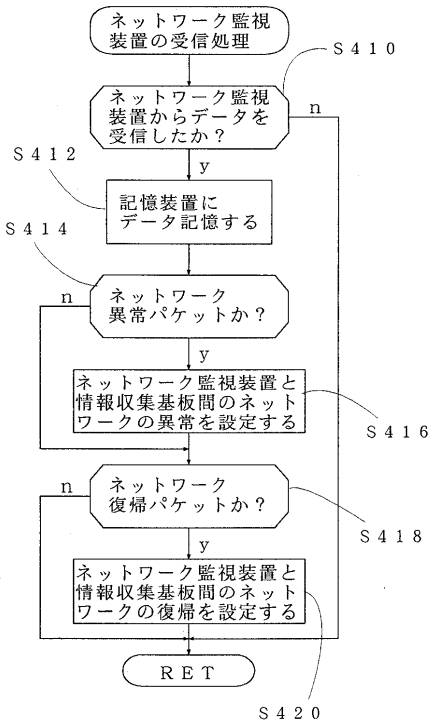
【図３４】



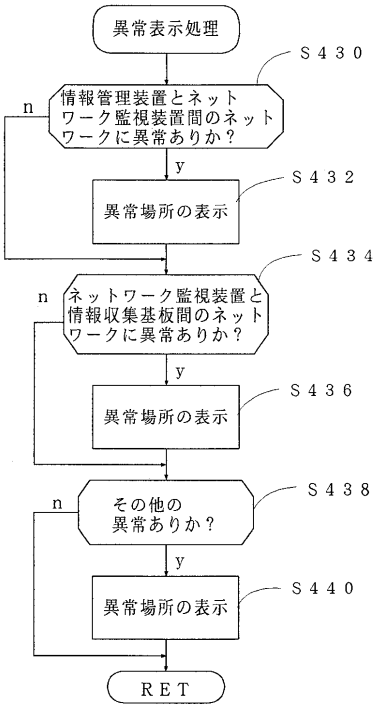
【図３５】



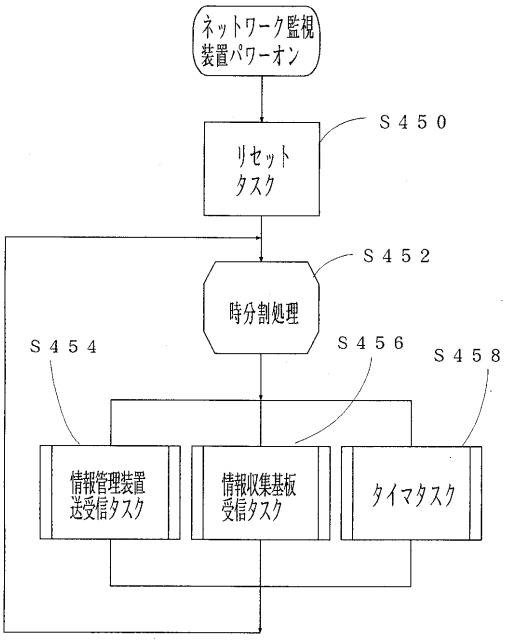
【図３６】



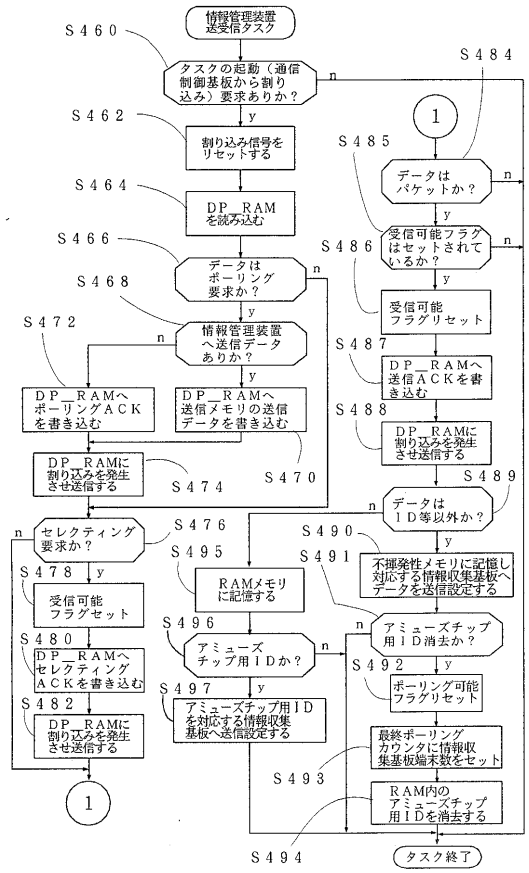
【図３７】



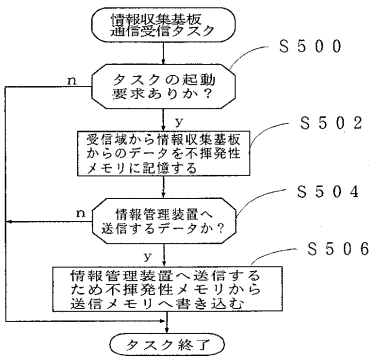
【図３８】



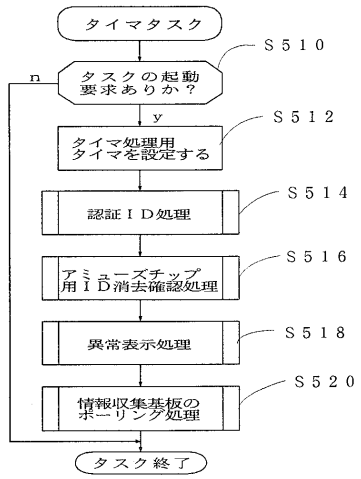
【図３９】



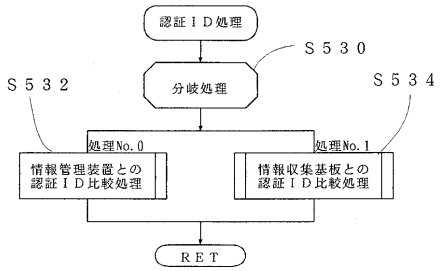
【図４０】



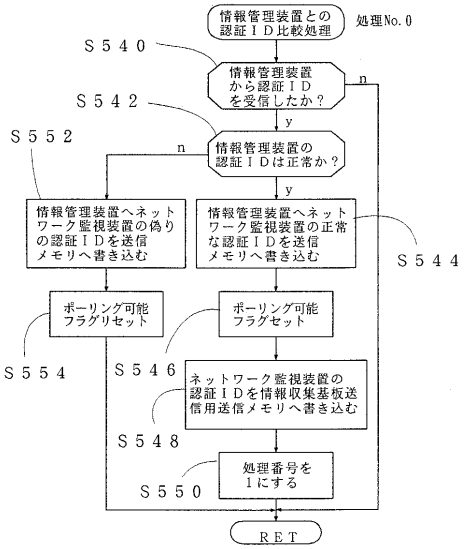
【図４１】



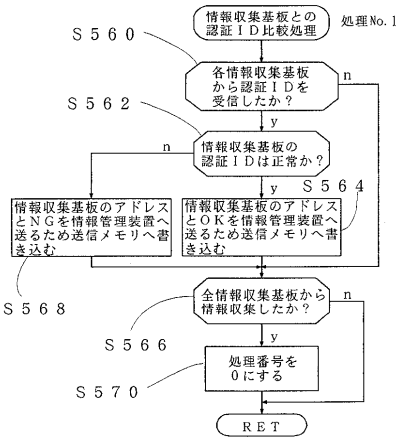
【図４２】



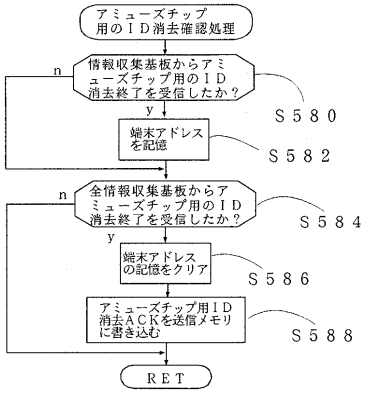
【図４３】



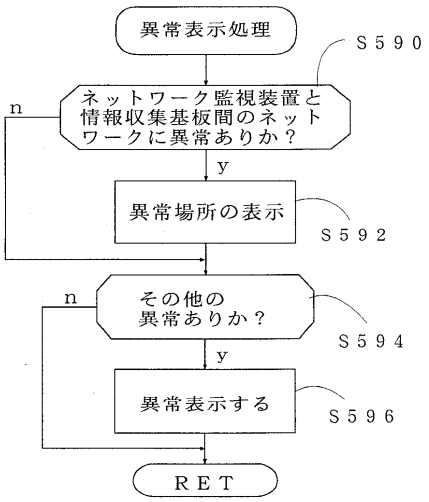
【図４４】



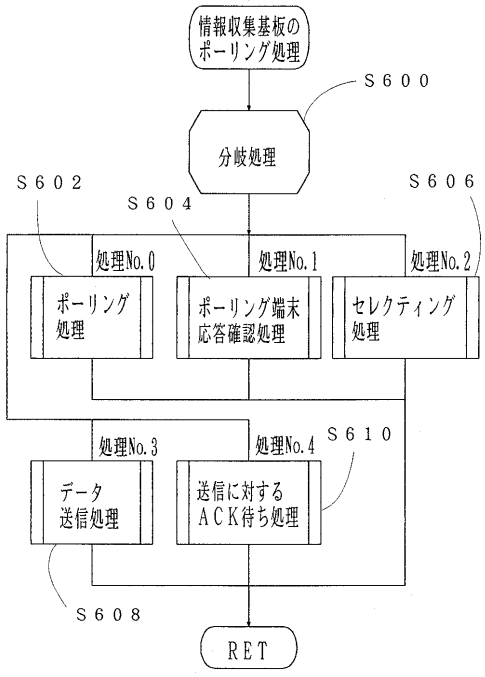
【図４５】



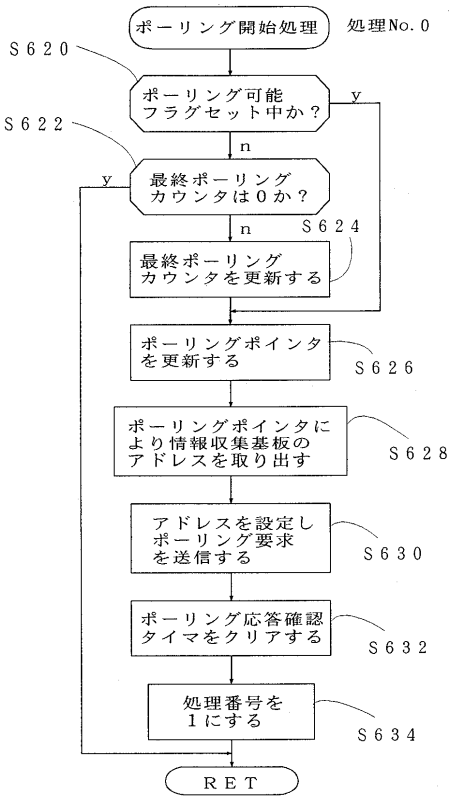
【図４６】



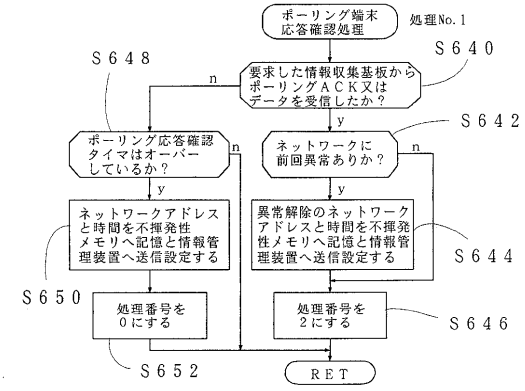
【図４７】



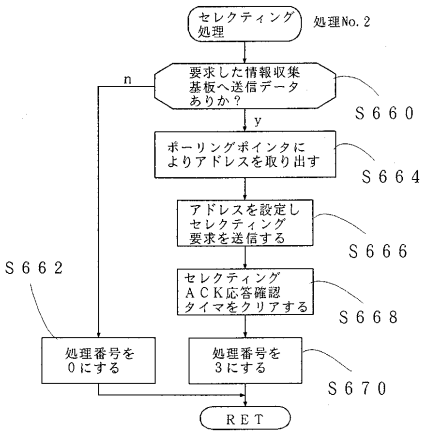
【図４８】



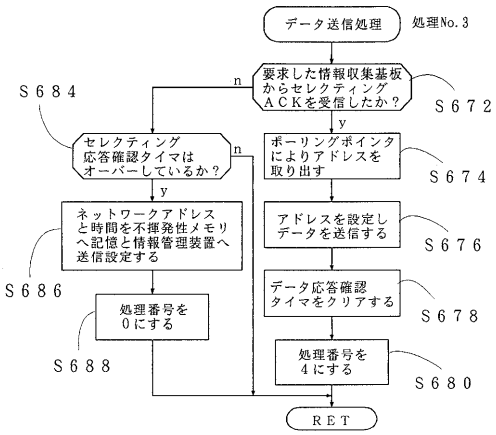
【図４９】



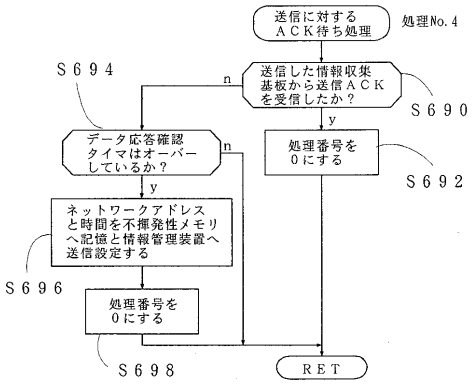
【図５０】



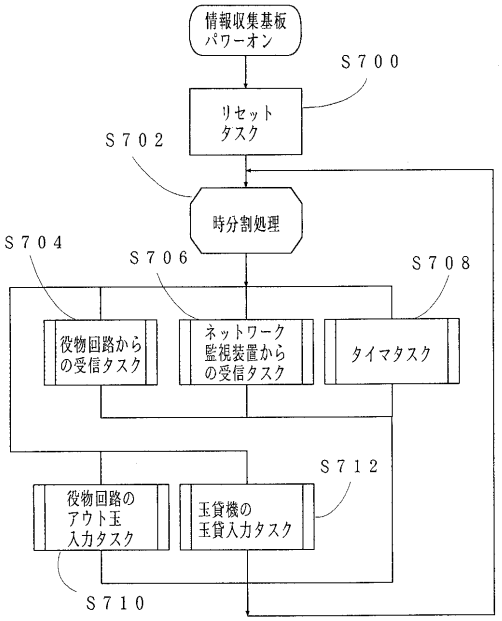
【図５１】



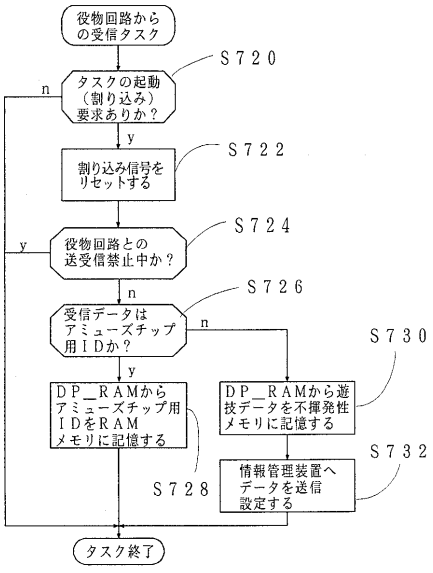
【図５２】



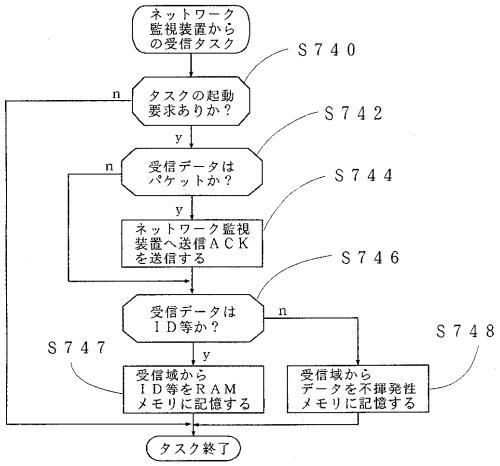
【図５３】



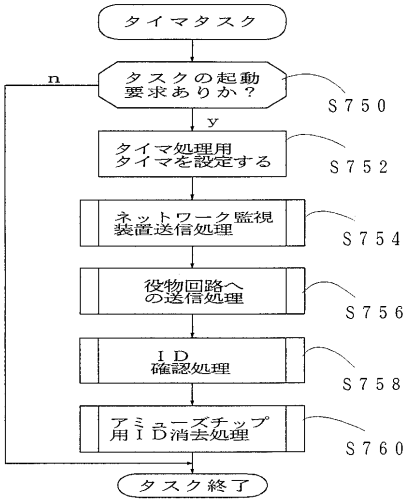
【図５４】



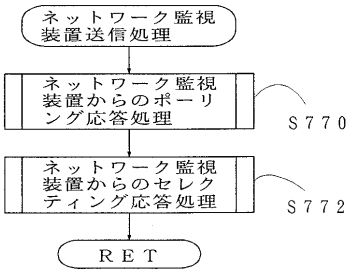
【図５５】



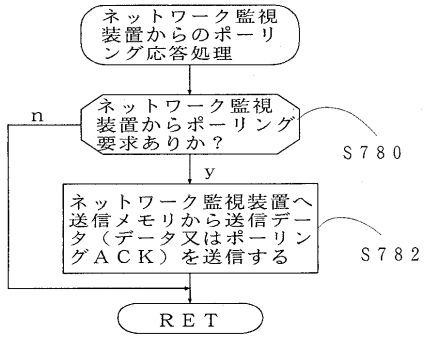
【図５６】



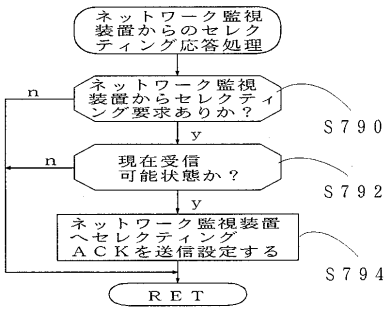
【図５７】



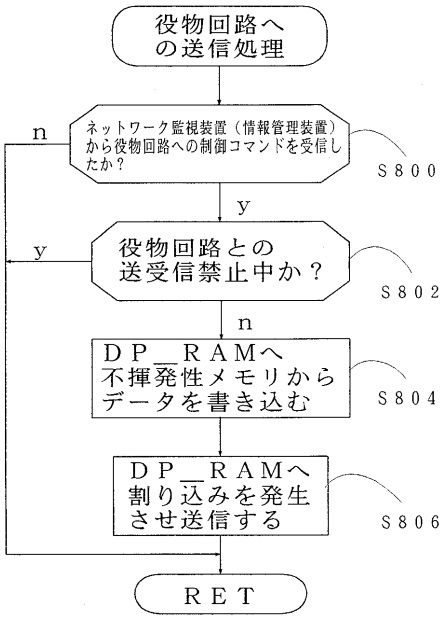
【図５８】



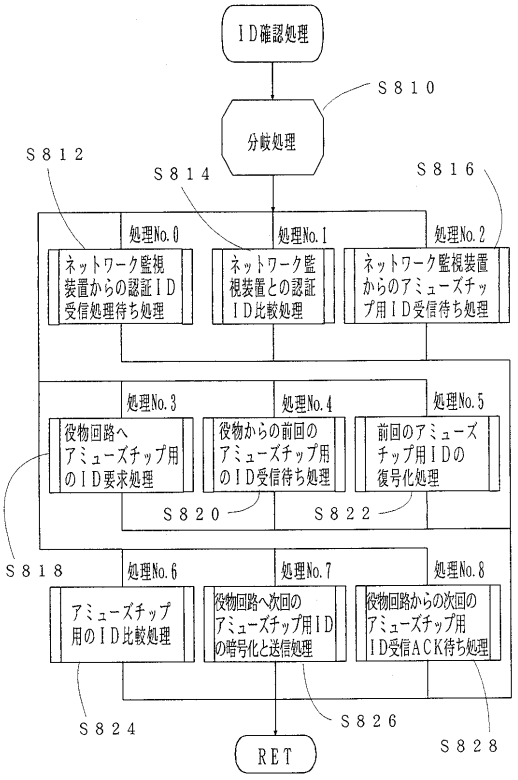
【図５９】



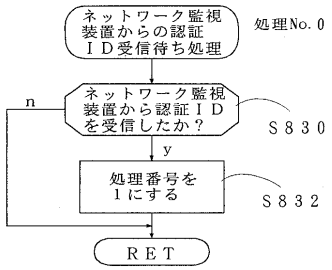
【図６０】



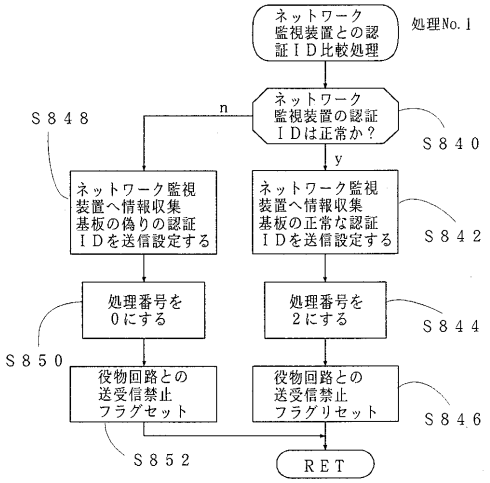
【図６１】



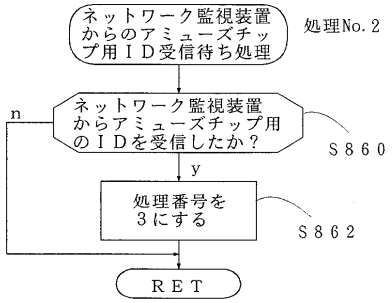
【図６２】



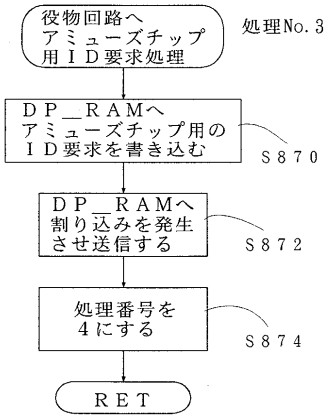
【図６３】



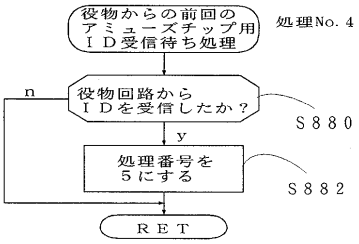
【図６４】



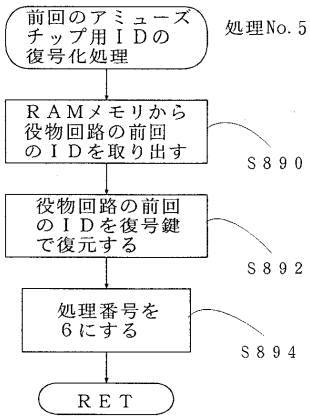
【図６５】



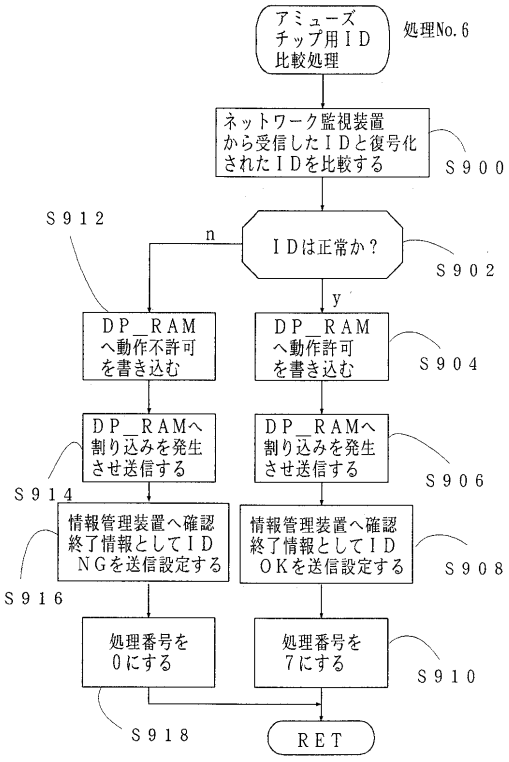
【図６６】



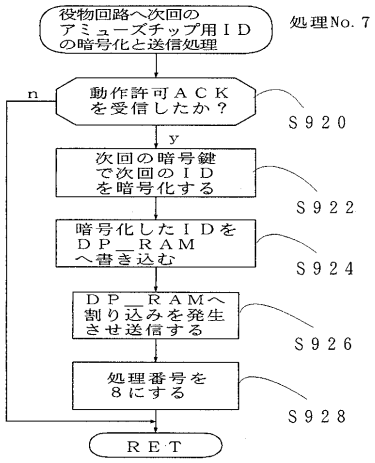
【図６７】



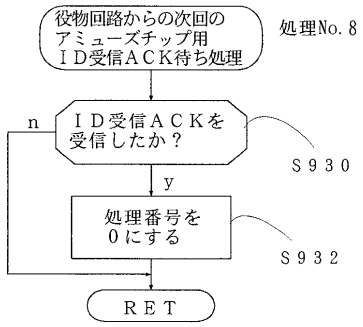
【図６８】



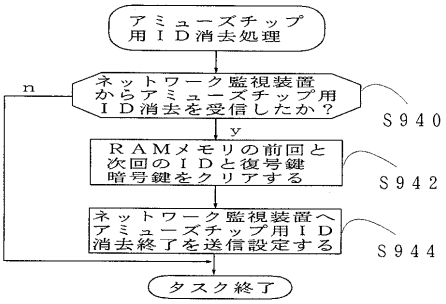
【図６９】



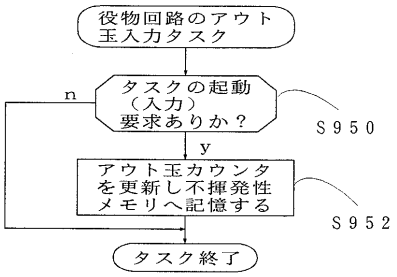
【図７０】



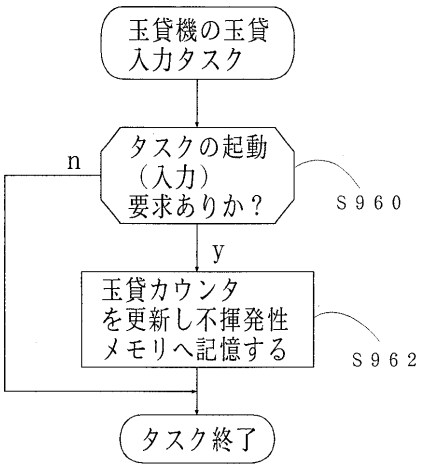
【図７１】



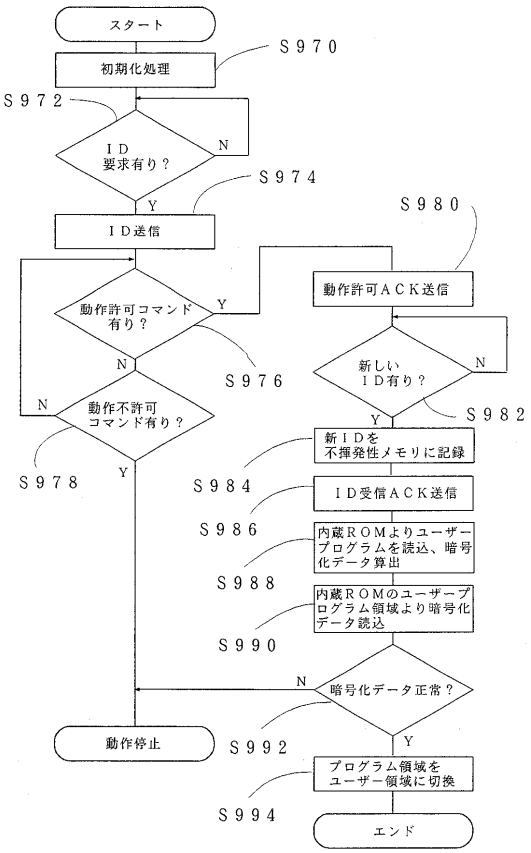
【図７２】



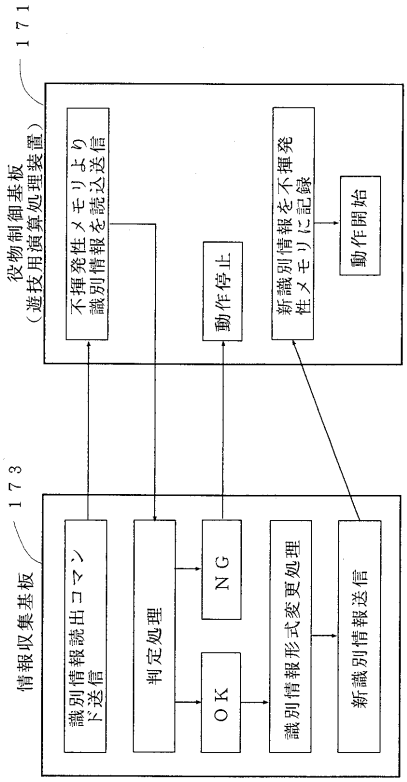
【図７３】



【図７４】



【図７５】


役物制御基板
（遊技用演算処理装置）
１７１
不揮発性メモリより識別情報を読込送信
動作停止
新識別情報を不揮発性メモリに記録
動作開始
情報収集基板
１７３
識別情報読出コマンド送信
判定処理
ＮＧ
ＯＫ
識別情報形式変更処理
新識別情報送信

フロントページの続き

(56)参考文献 特開平０７－０３１７３７（ＪＰ，Ａ）
特開平０６－１４９７３７（ＪＰ，Ａ）
特開平０６－３５０５９８（ＪＰ，Ａ）
特開平０８－１９６７２８（ＪＰ，Ａ）
特開平０５－０９１１１７（ＪＰ，Ａ）
特開平０４－３３２５８２（ＪＰ，Ａ）
特開平０６－１６５８５７（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
A63F 7/02