(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5934142号
(P5934142)
(45)発行日　平成28年6月15日(2016.6.15)　(24)登録日　平成28年5月13日(2016.5.13)

(51)Int.Cl.　F I
A63F 7/02 (2006.01)　A63F 7/02 352N
A63F 7/02 334
A63F 7/02 326Z

請求項の数 3　(全 65 頁)

(21)出願番号　特願2013-118234(P2013-118234)
(22)出願日　平成25年6月4日(2013.6.4)
(62)分割の表示　特願2011-218767(P2011-218767)の分割
原出願日　平成23年9月30日(2011.9.30)
(65)公開番号　特開2013-166052(P2013-166052A)
(43)公開日　平成25年8月29日(2013.8.29)
審査請求日　平成26年9月26日(2014.9.26)

(73)特許権者　000144153
株式会社三共
東京都渋谷区渋谷三丁目２９番１４号
(73)特許権者　591085972
日本ゲームカード株式会社
東京都渋谷区渋谷３丁目２８番１３号
(74)代理人　100095407
弁理士　木村　満
(72)発明者　小倉　敏男
東京都渋谷区渋谷三丁目２９番１４号　株式会社三共内
(72)発明者　柳　漢呉
東京都渋谷区渋谷三丁目２８番１３号　渋谷新南口ビル　日本ゲームカード株式会社内

最終頁に続く

(54)【発明の名称】書込システム及び書込装置

(57)【特許請求の範囲】
【請求項１】
遊技用装置に搭載される、所定の処理を行う第１の制御装置と、前記所定の処理とは異なる処理を行う第２の制御装置と、のそれぞれに情報を書き込む書込システムであって、
前記第１の制御装置に情報を書き込む第１の書込装置と、
前記第２の制御装置に情報を書き込む第２の書込装置と、を備え、
前記第１の書込装置は、前記第１の制御装置に予め記録されている所定情報を読み取る読取手段と、前記読取手段により読み取られた前記所定情報を前記第２の書込装置に送信する送信手段と、を備え、
前記第２の書込装置は、前記送信手段により送信された前記所定情報を前記第２の制御装置に書き込む書込手段を備え、
前記第２の制御装置は、前記第１の制御装置から前記所定情報を取得する取得手段を備え、
前記書込手段により書き込まれる前記所定情報と、前記取得手段により取得される前記所定情報とは、前記第２の制御装置による前記第１の制御装置の認証で比較される認証用情報である、
ことを特徴とする書込システム。
【請求項２】
遊技用装置に搭載される、所定の処理を行う第１の制御装置に情報を書き込む書込装置であって、

前記第１の制御装置に予め記録されている所定情報を読み取る読取手段と、
前記読取手段により読み取られた前記所定情報を、前記所定の処理とは異なる処理を行う第２の制御装置に情報を書き込む他の書込装置に送信する送信手段と、を備え、
前記第２の制御装置は、前記第１の制御装置から前記所定情報を取得する取得手段を備え、
前記送信手段により送信されて前記他の書込装置により書き込まれる前記所定情報と、前記取得手段により取得される前記所定情報とは、前記第２の制御装置による前記第１の制御装置の認証で比較される認証用情報である、
ことを特徴とする書込装置。
【請求項３】
遊技用装置に搭載される、所定の処理を行う第２の制御装置に情報を書き込む書込装置であって、
前記所定の処理とは異なる処理を行う第１の制御装置に情報を書き込む他の書込装置が前記第１の制御装置から読み取って送信する、前記第１の制御装置に予め記録されている所定情報を取得する第１取得手段と、
前記第１取得手段により取得された前記所定情報を前記第２の制御装置に書き込む書込手段と、を備え、
前記第２の制御装置は、前記第１の制御装置から前記所定情報を取得する第２取得手段を備え、
前記書込手段により書き込まれる前記所定情報と、前記第２取得手段により取得される前記所定情報とは、前記第２の制御装置による前記第１の制御装置の認証で比較される認証用情報である、
ことを特徴とする書込装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、遊技用装置の制御装置のための書込システム及び書込装置に関する。
【背景技術】
【０００２】
このような遊技用装置としては、例えば、パチンコ機、パチスロ機、カードゲーム機等の遊技機や、この遊技機とともに設置されて使用される周辺装置（カードユニット等）等がある。そして、このような遊技用装置には、一般的に所定の処理を行う制御装置（例えば、ＩＣチップなど）が搭載されている。各制御装置には、所定の情報を所定の装置によって読み書きすることが一般的である。
【０００３】
ここで、特許文献１に、１つの装置によって２つのＲＦＩＤタグから情報を読み取る技術が開示されているように、２つの制御装置それぞれから情報を読み取る場合（書き込む場合も含む）には、１つの装置によってそれを行うことが一般的である。
【先行技術文献】
【特許文献】
【０００４】
【特許文献１】特開２０１０－２０１０２２号公報
【発明の概要】
【発明が解決しようとする課題】
【０００５】
しかし、上記のように、１つの装置によって２つの制御装置に情報を読み書きする場合、１つの装置に２つの制御装置に対して情報を読み書きする機能が搭載されてしまう。ここで、例えば、２つの制御装置が異なるメーカーによって製造される場合には、一方の制御装置を製造するメーカーによって、両方の制御装置に対して情報を読み書きする装置が製造されることがある。このような場合、例えば、他方の制御装置に情報を読み書きする

内容などが、前記一方の制御装置を製造するメーカーに知られてしまう恐れがあり、情報漏洩のリスクがあった。このように、１つの装置によって２つの制御装置に情報を読み書きする場合には、情報漏洩のリスクがある。

【０００６】

本発明は、このような背景のもとになされたものであり、その目的とするところは、２つの制御装置それぞれに情報を読み書きする場合の情報漏洩のリスクを低減した書込システム及び書込装置を提供することにある。

【課題を解決するための手段】

【０００７】

（１）上記目的を達成するため、本発明に係る書込システムは、

遊技用装置（例えば、カードユニット２０など）に搭載される、所定の処理（例えば、パチンコ機１０との通信処理（ステップＣ２７）など）を行う第１の制御装置（例えば、通信制御ＩＣ２３など）と、前記所定の処理とは異なる処理（例えば、パチンコ機１０に搭載された主制御チップ１３などの認証要求を行う処理（ステップＣ３１）など）を行う第２の制御装置（例えば、セキュリティチップ２２など）と、のそれぞれに情報を書き込む書込システム（例えば、遊技用システム１など）であって、

前記第１の制御装置に情報を書き込む第１の書込装置（例えば、通信制御ＩＣ用ライター６１０など）と、

前記第２の制御装置に情報を書き込む第２の書込装置（例えば、セキュリティチップ用ライター６５０など）と、を備え、

前記第１の書込装置は、前記第１の制御装置に予め記録されている所定情報（例えば、認証用情報Ａ２など）を読み取る読取手段（例えば、ステップＡ１０で認証用情報Ａ２を読み取る制御部６１１など）と、前記読取手段により読み取られた前記所定情報を前記第２の書込装置に送信する送信手段（例えば、ステップＡ１１で認証用情報Ａ２を送信する制御部６１１など）と、を備え、

前記第２の書込装置は、前記送信手段により送信された前記所定情報を前記第２の制御装置に書き込む書込手段（例えば、ステップＡ１６で認証用情報Ａ２を書き込む制御部６５１など）を備え、

前記第２の制御装置は、前記第１の制御装置から前記所定情報を取得する取得手段（例えば、ステップＣ２１において認証用情報Ａ２を取得する処理部２２ａなど）を備え、

前記書込手段により書き込まれる前記所定情報と、前記取得手段により取得される前記所定情報とは、前記第２の制御装置による前記第１の制御装置の認証で比較される認証用情報である（例えば、ステップＣ２１において認証用情報Ａ２の照合参照）、

ことを特徴とする。

【０００８】

上記構成によれば、１つの装置によって２つの制御装置に情報を読み書きする必要がないので、情報漏洩のリスクを低減できる。

【０００９】

（２）上記目的を達成するため、本発明に係る書込装置は、

遊技用装置（例えば、カードユニット２０など）に搭載される、所定の処理（例えば、パチンコ機１０との通信処理（ステップＣ２７）など）を行う第１の制御装置（例えば、通信制御ＩＣ２３など）に情報を書き込む書込装置（例えば、通信制御ＩＣ用ライター６１０など）であって、

前記第１の制御装置に予め記録されている所定情報（例えば、認証用情報Ａ２など）を読み取る読取手段（例えば、ステップＡ１０で認証用情報Ａ２を読み取る制御部６１１など）と、

前記読取手段により読み取られた前記所定情報を、前記所定の処理とは異なる処理（例えば、パチンコ機１０に搭載された主制御チップ１３などの認証要求を行う処理（ステップＣ３１）など）を行う第２の制御装置（例えば、セキュリティチップ２２など）に情報を書き込む他の書込装置（例えば、セキュリティチップ用ライター６５０など）に送信す

る送信手段（例えば、ステップＡ１１で認証用情報Ａ２を送信する制御部６１１など）と、を備え、
前記第２の制御装置は、前記第１の制御装置から前記所定情報を取得する取得手段（例えば、ステップＣ２１において認証用情報Ａ２を取得する処理部２２ａなど）を備え、
前記送信手段により送信されて前記他の書込装置により書き込まれる前記所定情報と、前記取得手段により取得される前記所定情報とは、前記第２の制御装置による前記第１の制御装置の認証で比較される認証用情報である（例えば、ステップＣ２１において認証用情報Ａ２の照合参照）、
ことを特徴とする。
【００１０】
上記構成によれば、１つの装置によって２つの制御装置に情報を読み書きする必要がないので、情報漏洩のリスクを低減できる。
【００１１】
（３）上記目的を達成するため、本発明に係る書込装置は、
遊技用装置（例えば、カードユニット２０など）に搭載される、所定の処理（例えば、パチンコ機１０に搭載された主制御チップ１３などの認証要求を行う処理（ステップＣ３１）など）を行う第２の制御装置（例えば、セキュリティチップ２２など）に情報を書き込む書込装置（例えば、セキュリティチップ用ライター６５０など）であって、
前記所定の処理とは異なる処理（例えば、パチンコ機１０との通信処理（ステップＣ２７）など）を行う第１の制御装置（例えば、通信制御ＩＣ２３など）に情報を書き込む他の書込装置（例えば、通信制御ＩＣ用ライター６１０など）が前記第１の制御装置から読み取って送信する、前記第１の制御装置に予め記録されている所定情報（例えば、認証用情報Ａ２など）を取得する第１取得手段（例えば、ステップＡ１１で認証用情報Ａ２を受信する制御部６５１など）と、
前記第１取得手段により取得された前記所定情報を前記第２の制御装置に書き込む書込手段（例えば、ステップＡ１６で認証用情報Ａ２を書き込む制御部６５１など）と、を備え、
前記第２の制御装置は、前記第１の制御装置から前記所定情報を取得する第２取得手段（例えば、ステップＣ２１において認証用情報Ａ２を取得する処理部２２ａなど）を備え、
前記書込手段により書き込まれる前記所定情報と、前記第２取得手段により取得される前記所定情報とは、前記第２の制御装置による前記第１の制御装置の認証で比較される認証用情報である（例えば、ステップＣ２１において認証用情報Ａ２の照合参照）、
ことを特徴とする。
【００１２】
上記構成によれば、１つの装置によって２つの制御装置に情報を読み書きする必要がないので、情報漏洩のリスクを低減できる。
【００１３】
（４）上記（１）から（３）いずれかの書込システム又は書込装置において、
前記所定の情報は、前記第１の制御装置を認証するための第１の認証用情報（例えば、認証用情報A２など）であり、
前記第２の制御装置は、前記第１の制御装置から前記第１の認証用情報を取得する取得手段（例えば、ステップＣ２１において認証用情報A２を取得する処理部２２ａなど）と、前記取得手段が取得した前記第１の認証用情報と前記第２の書込装置の前記書込手段によって書き込まれた前記第１の認証用情報とに基づいて前記第１の制御装置を認証する第１認証手段（例えば、ステップＣ２１において認証用情報A２の照合を行う処理部２２ａなど）と、を備える、
ようにしてもよい。
【００１４】
上記構成によれば、第１の制御装置を認証するための第１の認証用情報が第２の書込装

置が読み取る必要が無くなり、認証用情報という重要な情報の漏洩リスクを低減できる。
【００１５】
（５）上記（１）の書込システムにおいて、
前記第１の書込装置から第２の認証用情報（例えば、認証用情報Ａ１など）を取得し、取得した前記第２の認証用情報に基づいて前記第１の書込装置を認証する第２認証手段（例えば、ステップＡ５において照合を行う制御部３１１など）と、前記第２の書込装置から第３の認証用情報（例えば、認証用情報Ｂ１など）を取得し、取得した前記第３の認証用情報に基づいて前記第２の書込装置を認証する第３認証手段（例えば、ステップＡ７において照合を行う制御部３１１など）と、を備える認証装置をさらに備える、
ようにしてもよい。
【００１６】
上記認証によって、第１の書込装置や第２の書込装置のすり替えなどを検出できるので、情報漏洩のリスクを低減できる。
【００１７】
（６）上記（１）から（５）のいずれか１つの書込システム又は書込装置において、
前記第１の書込装置と前記第２の書込装置とは、互いに通信を行って所定の認証用情報（例えば、認証用情報Ａ１や認証用情報Ｂ１など）を用いて相互認証が可能である（変形例参照）、
ようにしてもよい。
【００１８】
上記認証によって、第１の書込装置や第２の書込装置のすり替えなどを検出できるので、情報漏洩のリスクを低減できる。
【００１９】
（７）上記（１）から（６）のいずれか１つの書込システム又は書込装置において、
前記第１の制御装置と前記第２の制御装置とは、異なるメーカーで製造され、
前記第１の書込装置と前記第１の制御装置とは、同じメーカーで製造される、
ようにしてもよい。
【００２０】
上記構成によれば、第１の書込装置と第１の制御装置とが同じメーカーで製造されるので、第１の書込装置が第１の制御装置から情報を読み取る機能や書き込む機能を他者に開示する必要がなく、情報漏洩のリスクを低減できる。
【図面の簡単な説明】
【００２１】
【図１】本発明の一実施形態に係る遊技用システムの構成を示すブロック図である。
【図２】本発明の一実施形態におけるカードユニットとパチンコ機の構成を示すブロック図である。
【図３】図１の遊技用システムを構成する鍵管理センターサーバの構成を示すブロック図である。
【図４】図１の遊技用システムを構成するチップメーカーコンピュータの構成を示すブロック図である。
【図５】図１の遊技用システムを構成する通信制御ＩＣ用ライターの構成を示すブロック図である。
【図６】図１の遊技用システムを構成するセキュリティチップ用ライターの構成を示すブロック図である。
【図７】図１の遊技用システムを構成する上位サーバの構成を示すブロック図である。
【図８】カードユニットの製造時における各装置の動作フローの一例を示す図である。
【図９】カードユニットの製造時における各装置の動作フローの一例を示す図である。
【図１０】カードユニットの製造時における各装置の動作フローの一例を示す図である。
【図１１】カードユニットの製造時における各装置の動作フローの一例を示す図である。
【図１２】カードユニットの動作確認時における各装置の動作フローの一例を示す図であ

る。
【図１３】パチンコ機及びカードユニットの遊技場設置時における各装置の動作フローの一例を示す図である。
【図１４】パチンコ機及びカードユニットの遊技場設置時における各装置の動作フローの一例を示す図である。
【図１５】パチンコ機及びカードユニットの遊技場設置時における各装置の動作フローの一例を示す図である。
【図１６】パチンコ機及びカードユニットの遊技場設置時における各装置の動作フローの一例を示す図である。
【図１７】通常時における各装置の動作フローの一例を示す図である。
【図１８】セキュリティチップのモードの条件と、行われる処理との関係の一例を示す図である。
【図１９】チップ情報の問い合わせ先を説明するための動作フローの一例を示す図である。
【図２０】チップ情報の問い合わせ先を説明するための動作フローの一例を示す図である。
【図２１】チップ情報の問い合わせ先を説明するための動作フローの一例を示す図である。
【図２２】チップ情報の問い合わせ先を説明するための動作フローの一例を示す図である。
【図２３】制御情報の配信を説明するための動作フローの一例を示す図である。
【発明を実施するための形態】
【００２２】
この発明の実施形態について、図面を参照して詳細に説明する。
【００２３】
（実施形態）
（遊技用システム１の構成）
図１に示すように、本実施形態に係る遊技用システム１は、パチンコ機１０と、カードユニット２０と、鍵管理センターサーバ３１０と、チップメーカーコンピュータ１１０と、通信制御ＩＣ用ライター６１０と、セキュリティチップ（ＳＣ）用ライター６５０（以下、ＳＣ用ライター６５０という。）と、上位サーバ５１０と、を備えている。パチンコ機１０及びカードユニット２０は、遊技用装置の一例である。
【００２４】
鍵管理センターサーバ３１０と、チップメーカーコンピュータ１１０と、通信制御ＩＣ用ライター６１０と、ＳＣ用ライター６５０と、上位サーバ５１０と、は、インターネット等のネットワークＮと接続され、これらのうちの所定の装置同士が通信可能となっている。なお、情報の漏洩を防止するため、上記各装置の少なくとも一部は、通信相手となる所定の装置と専用回線に接続されて、当該所定の装置と専用回線を介して通信してもよい。
【００２５】
上位サーバ５１０とカードユニット２０とは、遊技場５００（パチンコ店等）に設置され、遊技場５００内のローカルネットワーク等を介して、互いに通信可能に接続される。上位サーバ５１０は、遊技場５００に、例えば、一台設置される。カードユニット２０は、パチンコ機１０と通信可能に接続されて遊技場５００に複数設置される。カードユニット２０とパチンコ機１０とは、それぞれが一対一の関係で、互いに通信可能に接続され、遊技場５００に複数設置される。
【００２６】
通信制御ＩＣ用ライター６１０とＳＣ用ライター６５０とは、カードユニットメーカー６００内のローカルネットワーク等を介して、互いに通信可能に接続される。
【００２７】

（パチンコ機１０）
パチンコ機１０は、パチンコ店（遊技場５００）における遊技島において機種等毎に所定の位置に配置される。パチンコ機１０は、本実施形態では、いわゆるＣＲ式のパチンコ機（所謂封入式のパチンコ機であってもよい。）である。遊技者は、パチンコ機１０で遊技を行う。遊技者は、パチンコ機１０で行う遊技において、遊技媒体であるパチンコ玉をパチンコ機１０の遊技領域に打ち込んで遊技を行う。
【００２８】
封入式パチンコ機とは、パチンコ機１０内に封入されたパチンコ球を循環使用して遊技を行う遊技機であり、パチンコ球による賞球の払い出しを行わないパチンコ機のことをいう。封入式パチンコ機では、遊技者は、パチンコ球貸出し可能金額等の有価情報を記録したプリペイド式の記録媒体、例えば磁気カード等のカード状記録媒体（以下、単にカードともいう。）を、パチンコ機１０の外枠に沿って配設されるカードユニット２０に挿入し、必要なパチンコ球数をカードから度数を減算して（持ち球数情報に変換して）貸し出し遊技を行う。封入式パチンコ機は、パチンコ球の入賞口への入賞やアウト口への入球等に応じて持ち球数情報が示す持ち球数を増減させる。この増減の基本的なルールは一般的なパチンコ機の球の増減と同様である。遊技終了時には、遊技者は、精算ボタンを操作し、その時点において獲得している持ち球数を示す持ち玉数情報をカードに記録させ（このとき、この持ち玉数情報をカードの度数に変換してもよい。）、このカードをカードユニット２０外に排出させる。なお、持ち玉数情報は、上位サーバ５１０で管理してもよい。この場合、カードユニット２０は、例えば、持ち玉数情報をカードに記録させる代わりに、上位サーバ５１０に持ち玉数情報と、カードを識別するカード識別情報とを送信する。上位サーバ５１０は、例えば、持ち玉数情報と、カードを識別するカード識別情報とを対応付けて記憶して、各カード毎に持ち玉数を管理してもよい。なお、カードユニット２０は、プリペイド式のカードだけでなく、現金、又は現金とプリペイド式のカードを併用してもよい。
【００２９】
パチンコ機１０は、遊技釘、入賞口、表示装置等が取り付けられて前記遊技領域を構成する遊技盤と、遊技盤を収納する筐体と、を含んで構成されるとともに（図示省略）、図１に示すように、払出制御チップ１１と主制御チップ１３とを備える。
【００３０】
主制御チップ１３は、パチンコ機１０の遊技盤側の制御基板に搭載され、主に遊技の進行の制御を行う。払出制御チップ１１は、パチンコ機１０の筐体側の制御基板に搭載され、主に賞球の払い出しの制御（封入式の場合には、持ち玉数の加減算など）を行う。
【００３１】
払出制御チップ１１は、図２に示すように、ＣＰＵ（Central Processing Unit）及びＲＡＭ（Random Access Memory）等からなる処理部１１ａと、ＲＯＭ（Read Only Memory）等の不揮発性の記憶装置等からなる記憶部１１ｂと、入出力ポート等からなる通信部１１ｃと、を備えた、例えば、ワンチップマイコン等によって構成されている。なお、ＲＯＭは、ＥＰＲＯＭ等の書込可能なＲＯＭであってもよい（以下、ＲＯＭについて同じ）。なお、ＲＡＭは、基本的に揮発性のものとするが、適宜、不揮発性のものを含んでもよい（以下、ＲＡＭについて同じ）。
【００３２】
記憶部１１ｂは、プログラムの他、所定の情報を記憶する。通信部１１ｃは、処理部１１ａが払出制御チップ１１外部と通信（情報の送信又は受信）を行うときに使用される。処理部１１ａは、記憶部１１ｂが記憶するプログラムに従って、所定の処理を行う部分である。例えば、処理部１１ａは、カードユニット２０（通信制御ＩＣ２３）との間でパチンコ玉の貸与に関する情報のやり取り（特に封入式でない場合）、又は、持ち球数情報の増減に関する情報のやり取り（特に封入式の場合）を、通信部１１ｃを介して行うことによって玉貸処理（ビジタ玉貸処理，会員単位玉貸処理，及び会員端数玉貸処理等）等を行う。また、処理部１１ａは、後述の処理を行う。なお、処理部１１ａは、記憶部１１ｂが

記憶する情報や、通信部１１ｃを介して受信する情報を用いて処理を行う。
【００３３】
主制御チップ１３は、図２に示すように、ＣＰＵ及びＲＡＭ等からなる処理部１３ａと、ＲＯＭ等の不揮発性の記憶装置等からなる記憶部１３ｂと、入出力ポート等からなる通信部１３ｃと、を備えた、例えば、ワンチップマイコン等によって構成されている。
【００３４】
記憶部１３ｂは、プログラムの他、所定の情報を記憶する。通信部１３ｃは、処理部１３ａが主制御チップ１３外部と通信（情報の送信又は受信）を行うときに使用される。処理部１３ａは、記憶部１３ｂが記憶するプログラムに従って、所定の処理を行う部分である。例えば、処理部１３ａは、パチンコ機１０の各部に、パチンコ機１０が行う遊技に関する演出動作（例えば、遊技盤の入賞口の開閉、及び、表示装置への画像の表示）を行わせる。また、処理部１３ａは、例えば、払出制御チップ１１と通信部１３ｃを介して通信して、入賞が発生した場合に持ち球数情報を増やす処理（特に封入式の場合）、払出制御チップ１１にパチンコ球をいくつ払い出すかの処理（特に封入式でない場合）や、後述の処理を行う。なお、処理部１３ａは、記憶部１３ｂが記憶する情報や、通信部１３ｃを介して受信する情報を用いて、処理を行う。
【００３５】
（カードユニット２０）
カードユニット２０は、パチンコ機１０に対応して（例えば、パチンコ機１０の、向かって左側に隣接して）配置され、両者は通信可能に接続される。カードユニット２０は、玉貸しの管理（特に、パチンコ機１０が封入式でない場合）、カード残高の管理、カードに記録された持ち球数情報（特に、パチンコ機１０が封入式の場合）の管理等を行う。カードユニット２０は、使用可能状態であるか否かを示す使用可能表示ランプ等の各種ランプ、カード挿入口、カード挿入口に挿入されたカードを読み取るためのカードリーダライター等（いずれも図示せず。）を備える。また、カードユニット２０は、図２に示すように、ＣＵ制御部２１と、セキュリティチップ２２と、通信制御ＩＣ２３と、セキュリティ基板２４と、を備える。 セキュリティチップ２２と通信制御ＩＣ２３とは、セキュリティ基板２４に実装される。
【００３６】
通信制御ＩＣ２３は、図２に示すように、ＣＰＵ及びＲＡＭ等からなる処理部２３ａと、ＲＯＭ等の不揮発性の記憶装置等からなる記憶部２３ｂと、入出力ポート等からなる通信部２３ｃと、を備えた、例えば、ワンチップマイコン等によって構成されている。
【００３７】
記憶部２３ｂは、プログラムの他、所定の情報を記憶する。通信部２３ｃは、処理部２３ａが通信制御ＩＣ２３外部と通信（情報の送信又は受信）を行うときに使用される。処理部２３ａは、記憶部２３ｂが記憶するプログラムに従って、後述の所定の処理などを行う。なお、処理部２３ａは、記憶部２３ｂが記憶する情報や、通信部２３ｃを介して受信する情報を用いて処理を行う。
【００３８】
セキュリティチップ２２は、図２に示すように、ＣＰＵ及びＲＡＭ等からなる処理部２２ａと、ＲＯＭ等の不揮発性の記憶装置等からなる記憶部２２ｂと、入出力ポート等からなる通信部２２ｃと、を備えた、例えば、ワンチップマイコン等によって構成されている。
【００３９】
記憶部２２ｂは、プログラムの他、所定の情報を記憶する。通信部２２ｃは、処理部２２ａがセキュリティチップ２２外部と通信を行うときに使用される。処理部２２ａは、記憶部２２ｂが記憶するプログラムに従って、所定の処理を行う。例えば、処理部２２ａは、後述の処理を行う。また、処理部２２ａは、例えば、パチンコ機１０から送信される情報を用いてベース異常チェックを行う。 なお、処理部２２ａは、記憶部２２ｂが記憶する情報や、通信部２２ｃを介して受信する情報を用いて処理を行う。

【００４０】
ここで、ベース異常について説明する。パチンコ業界ではベースと称されている通常遊技状態における出玉率がある。このベースＢは、例えば、Ｂ＝（ＯＵＴ－特賞中ＯＵＴ）／（ＩＮ－特賞中ＩＮ）×１００という数式で算出される。
【００４１】
ここで、ＩＮとは、パチンコ機１０に打込んだ球数の集計結果であり、島設備に設けられ、パチンコ機１０毎に設置される打込球タンクに取り付けられた打込球カウンタの計数結果に基づいて集計される。ＯＵＴとは、払い出された賞球数の集計結果であり、パチンコ機１０から出力される賞球信号に基づいて集計される。特賞中ＩＮとは、特賞（大当り）中における打込球数の集計結果であり、パチンコ機１０から出力される大当り信号の出力中における打込球検出スイッチの検出結果に基づいて集計される。特賞中ＯＵＴとは、特賞中における賞球数の集計結果であり、パチンコ機１０から出力される大当り信号の出力中における賞球信号に基づいて集計される。本実施形態におけるパチンコ機１０が所謂封入式パチンコ機である場合、ＩＮや特賞中ＩＮは、打込みより消費される持ち球数情報を示し、ＯＵＴや特賞中ＯＵＴは、入賞等により獲得する持ち球数情報を示す。
【００４２】
ベースＢの値が高いということは、通常遊技において入賞しやすい、言い換えれば球持ちがよいということである。このようにベースＢは、パチンコ機１０の稼働状況を知る上で有用な値であり、遊技場５００の管理者はベースＢの値を参考にしながら釘調整を行うことが多い。例えば、ベースＢの値が高いから遊技釘を渋めに調整し、あるいは、ベースＢの値が低いから遊技釘を少し甘めに調整する、というような調整が可能になる。さらに、ベースＢの値は、大当り遊技終了直後といった場合を除けば、ほぼ一定の範囲内の値となる。このように、ベースＢの値は突然高くなるということがないことから、仮に、ベースＢの値が突然高くなった場合には、パチンコ機１０自体に問題が発生したかあるいは不正行為（ベース異常）が行われた可能性があると判断することができる。
【００４３】
セキュリティ基板２４には、通信制御ＩＣ２３、セキュリティチップ２２などが実装されるとともに、特に、通信制御ＩＣ２３、セキュリティチップ２２が後述の処理を実行できるような所定の電子回路が設けられている。例えば、セキュリティ基板２４には、通信制御ＩＣ２３とセキュリティチップ２２とを通信可能にしたり、通信制御ＩＣ２３とパチンコ機１０とを通信可能にしたり、セキュリティチップ２２とＣＵ制御部２１とを通信可能にしたりする、適宜の電子回路が設けられている。
【００４４】
ＣＵ制御部２１は、図２に示すように、ＣＰＵ及びＲＡＭ等からなる処理部２１ａと、ＲＯＭ等の不揮発性の記憶装置等からなる記憶部２１ｂと、入出力ポート等からなる通信部２１ｃと、を備えた、例えば、所定の制御基板などによって構成される。なお、処理部２１ａと、記憶部２１ｂと、通信部２１ｃと、のうちの少なくとも一部は、適宜、ワンチップマイコンで構成されてもよい。
【００４５】
記憶部２１ｂは、プログラムの他、所定の情報を記憶する。通信部２１ｃは、処理部２１ａがＣＵ制御部２１外部と通信を行うときに使用される。処理部２１ａは、記憶部２１ｂが記憶するプログラムに従って、所定の処理を行う。例えば、処理部２１ａは、パチンコ機１０（払出制御チップ１１）との間でパチンコ玉の貸与に関する情報のやり取りを、通信部２１ｃ、セキュリティチップ２２、通信制御ＩＣ２３を介して行うことによって前記の玉貸処理等（遊技に係る動作）を行う。また、処理部２１ａは、カードリーダライター等を制御して、カードに対して情報の読み書きを行ったり、ランプを点灯等させたり、通信部２１ｃを介して後述の上位サーバ５１０に玉貸処理で得られる売り上げ情報等を送信したりして遊技に係る処理を適宜行い、また、後述の処理を行う。具体的には、処理部２１ａは、例えば、カード残高、貯留されているパチンコ球を示す貯球の情報、遊技者を識別する会員ＩＤ等の読み取りや書込み等を行う。本実施形態におけるパチンコ機１０が

所謂封入式パチンコ機である場合、処理部２１ａは、上記の読み取りや書込みの他、カード状記録媒体の度数の読み取りや書込み（持ち球数情報の増減に関する情報への変換も含む）等を行う。なお、処理部２１ａは、記憶部２１ｂが記憶する情報や、通信部２１ｃを介して受信する情報を用いて、処理を行う。

【００４６】

（鍵管理センターサーバ３１０）

鍵管理センターサーバ３１０は、例えば、一般的なサーバコンピュータであり、遊技場５００外（パチンコ店外）に設置され、鍵管理センター３００（例えば、所定のカードユニットメーカー６００によって運営される。）によって管理されている（図１参照）。

【００４７】

鍵管理センターサーバ３１０は、図３に示すように、記憶部３１２と、制御部３１１と、入出力部３１３と、前記各部を相互に接続するシステムバス３１４とを備えている。

【００４８】

記憶部３１２は、ＲＯＭ、磁気ディスク（ハードディスクなど）、半導体メモリ等の不揮発性の記憶装置から構成されている。この記憶部３１２は、制御部３１１が処理を行うために必要な情報、プログラム等を記憶する。

【００４９】

入出力部３１３は、ネットワークＮなどの外部と接続されるシリアルインタフェース等から構成される通信部を有している。また、入出力部３１３は、制御部３１１に制御されて所定の画面を表示するモニター等から構成される表示部や、制御部３１１に制御されて所定の情報を音声出力するブザーなどの音声出力部、鍵管理センター３００に所属する従業員等からの入力操作を受け付け、受け付けた操作に応じた操作信号を制御部３１１に供給するキーボードやマウス等から構成される操作入力部等を備えても良い。

【００５０】

制御部３１１は、ＣＰＵ及びＲＡＭ等から構成される。制御部３１１は、記憶部３１２が記憶するプログラムに従って、また、記憶部３１２が記憶する情報や、通信部を介して受信する情報などを用いて後述の処理を行う。また、制御部３１１は、表示部、音声出力部などを制御するとともに、操作部から供給される操作信号（つまり、従業員等による操作）に応じた処理を行う。

【００５１】

（チップメーカーコンピュータ１１０）

チップメーカーコンピュータ１１０は、例えば、一般的なコンピュータであり、遊技場５００外に設置され、チップメーカー１００によって管理されている（図１参照）。

【００５２】

チップメーカーコンピュータ１１０は、図４に示すように、記憶部１１２と、制御部１１１と、入出力部１１３と、前記各部を相互に接続するシステムバス１１４とを備えている。

【００５３】

記憶部１１２は、ＲＯＭ、磁気ディスク（ハードディスクなど）、半導体メモリ等の不揮発性の記憶装置から構成されている。この記憶部１１２は、制御部１１１が処理を行うために必要な情報、プログラム等を記憶する。

【００５４】

入出力部１１３は、ネットワークＮなどの外部と接続されるシリアルインタフェース等から構成される通信部を有している。また、入出力部１１３は、制御部１１１に制御されて所定の画面を表示するモニター等から構成される表示部や、制御部１１１に制御されて所定の情報を音声出力するブザーなどの音声出力部、チップメーカー１００に所属する従業員等からの入力操作を受け付け、受け付けた操作に応じた操作信号を制御部１１１に供給するキーボードやマウス等から構成される操作入力部等を備えても良い。

【００５５】

制御部１１１は、ＣＰＵ及びＲＡＭ等から構成される。制御部１１１は、記憶部１１２

が記憶するプログラムに従って、また、記憶部１１２が記憶する情報や、通信部を介して受信する情報などを用いて後述の処理を行う。また、制御部１１１は、表示部、音声出力部などを制御するとともに、操作部から供給される操作信号（つまり、従業員等による操作）に応じた処理を行う。

【００５６】

（通信制御ＩＣ用ライター６１０）

通信制御ＩＣ用ライター６１０は、例えば、情報の読み取り／書き込みをするリーダー／ライターであり、チップメーカー１００から出荷され、遊技場５００外のカードユニットメーカー６００内に納入、設置される（図１参照）。通信制御ＩＣ用ライター６１０は、各種情報を通信制御ＩＣ２３の記憶部（ＲＯＭなど）に書き込む処理等を行う。

【００５７】

通信制御ＩＣ用ライター６１０は、図５に示すように、記憶部６１２と、制御部６１１と、入出力部６１３と、書込読取部６１５と、前記各部を相互に接続するシステムバス６１４とを備えている。

【００５８】

記憶部６１２は、ＲＯＭ、磁気ディスク（ハードディスクなど）、半導体メモリ等の不揮発性の記憶装置から構成されている。この記憶部６１２は、制御部６１１が処理を行うために必要な情報、プログラム等を記憶する。

【００５９】

入出力部６１３は、ネットワークＮ、ローカルネットワークなどの外部と接続されるシリアルインタフェース等から構成される通信部を有している。また、入出力部６１３は、制御部６１１に制御されて所定の画面を表示するモニター等から構成される表示部や、制御部６１１に制御されて所定の情報を音声出力するブザーなどの音声出力部、チップメーカー１００、カードユニットメーカー６００に所属する従業員等からの入力操作を受け付け、受け付けた操作に応じた操作信号を制御部６１１に供給するキーボードやマウス等から構成される操作入力部等を備えても良い。

【００６０】

書込読取部６１５は、制御部６１１のもと、通信制御ＩＣ２３（記憶部２３ｂ（ＲＯＭなど））との間で情報の読み取り／書き込みをする。

【００６１】

制御部６１１は、ＣＰＵ及びＲＡＭ等から構成される。制御部６１１は、記憶部６１２が記憶するプログラムに従って、また、記憶部６１２が記憶する情報や、通信部を介して受信する情報などを用いて後述の処理を行う。また、制御部６１１は、表示部、音声出力部などを制御するとともに、操作部から供給される操作信号（つまり、従業員等による操作）に応じた処理を行う。また制御部６１１は、書込読取部６１５を介して通信制御ＩＣ２３に対して各種情報の読み書きを行う。

【００６２】

（ＳＣ用ライター６５０）

ＳＣ用ライター６５０は、例えば、情報の読み取り／書き込みをするリーダー／ライターであり、カードユニットメーカー６００で製造されるか、他のメーカーから出荷され、遊技場５００外のカードユニットメーカー６００内に納入、設置される（図１参照）。ＳＣ用ライター６５０は、各種情報をセキュリティチップ２２の記憶部（ＲＯＭなど）に書き込む処理等を行う。

【００６３】

ＳＣ用ライター６５０は、図５に示すように、記憶部６５２と、制御部６５１と、入出力部６５３と、書込読取部６５５と、前記各部を相互に接続するシステムバス６５４とを備えている。

【００６４】

記憶部６５２は、ＲＯＭ、磁気ディスク（ハードディスクなど）、半導体メモリ等の不揮発性の記憶装置から構成されている。この記憶部６５２は、制御部６５１が処理を行う

ために必要な情報、プログラム等を記憶する。
【００６５】
入出力部６５３は、ネットワークＮ、ローカルネットワークなどの外部と接続されるシリアルインタフェース等から構成される通信部を有している。また、入出力部６５３は、制御部６５１に制御されて所定の画面を表示するモニター等から構成される表示部や、制御部６５１に制御されて所定の情報を音声出力するブザーなどの音声出力部、カードユニットメーカー６００や他のメーカーに所属する従業員等からの入力操作を受け付け、受け付けた操作に応じた操作信号を制御部６５１に供給するキーボードやマウス等から構成される操作入力部等を備えても良い。
【００６６】
書込読取部６５５は、制御部６５１のもと、通信制御ＩＣ２３（記憶部２３ｂ（ＲＯＭなど））との間で情報の読み取り／書き込みをする。
【００６７】
制御部６５１は、ＣＰＵ及びＲＡＭ等から構成される。制御部６５１は、記憶部６５２が記憶するプログラムに従って、また、記憶部６５２が記憶する情報や、通信部を介して受信する情報などを用いて後述の処理を行う。また、制御部６５１は、表示部、音声出力部などを制御するとともに、操作部から供給される操作信号（つまり、従業員等による操作）に応じた処理を行う。また制御部６５１は、書込読取部６５５を介してセキュリティチップ２２に対して各種情報の読み書きを行う。
【００６８】
（上位サーバ５１０）
上位サーバ５１０は、例えば、一般的なサーバコンピュータであり、遊技場５００の所定箇所（例えば管理事務所等）に設置され、遊技場５００内に設置されている複数のカードユニット２０と複数のパチンコ機１０をそれぞれ管理する場内管理装置である（図１参照）。上位サーバ５１０は、鍵管理センターサーバ３１０と遊技場５００内に設置されている複数のカードユニット２０と相互に通信可能に接続されている。上位サーバ５１０は、例えば、各カードユニット２０から送信される売り上げ情報等を集計する他、カードユニット２０を制御する。上位サーバ５１０は、例えば、パチンコ店毎（遊技場５００毎）に設置される。
【００６９】
上位サーバ５１０は、図７に示すように、記憶部５１２と、制御部５１１と、入出力部５１３と、上記各部を相互に接続するシステムバス５１４とを備えている。
【００７０】
記憶部５１２は、ＲＯＭ、磁気ディスク（ハードディスクなど）、半導体メモリ等の不揮発性の記憶装置から構成されている。この記憶部５１２は、制御部５１１が処理を行うために必要な情報、プログラム等を記憶する。
【００７１】
入出力部５１３は、ネットワークＮ、ローカルネットワークなどの外部と接続されるシリアルインタフェース等から構成される通信部を有している。また、入出力部５１３は、制御部５１１に制御されて所定の画面を表示するモニター等から構成される表示部や、制御部５１１に制御されて所定の情報を音声出力するブザーなどの音声出力部、遊技場５００で働く従業員等からの入力操作を受け付け、受け付けた操作に応じた操作信号を制御部５１１に供給するキーボードやマウス等から構成される操作入力部等を備えても良い。
【００７２】
制御部５１１は、ＣＰＵ及びＲＡＭ等から構成される。制御部５１１は、記憶部５１２が記憶するプログラムに従って、また、記憶部５１２が記憶する情報や、通信部を介して受信する情報などを用いて後述の処理や上記処理を行う。また、制御部５１１は、表示部、音声出力部などを制御するとともに、操作部から供給される操作信号（つまり、従業員等による操作）に応じた処理を行う。
【００７３】

（遊技用システム１の動作など）
次に、カードユニット２０の製造時における各装置の動作、カードユニット２０の動作確認における各装置の動作、パチンコ機１０及びカードユニット２０の遊技場５００設置時における各装置の動作、パチンコ機１０及びカードユニット２０の遊技場５００設置後における各装置の動作などについて、図面を参照して説明する。なお、後述の暗号鍵Ａ１及びＡ２、暗号鍵Ｃ１からＣ３、秘匿鍵Ａ及びＢ、配送鍵Ａ及びＢなどの等の各種の暗号通信用の鍵を用いて行われる暗号通信のアルゴリズムは、任意である。例えば、ＤＥＳ（Data Encryption Standard）方式や、ＡＥＳ（Advanced Encryption Standard）方式などの共通鍵暗号方式等が用いられる。

【００７４】
また、下記での照合（認証の一例）では、照合対象の両情報が、同じ内容を示している場合（例えば、両情報が同じ情報である（例えば、数値が一致している）等して同じものを識別している場合）には、照合結果を照合ＯＫ（単にＯＫともいう。また、照合の成功などともいう。）とし（認証成功の一例）、同じ内容を示していない場合（例えば、両情報が異なる情報である（例えば、数値が一致していない）等して同じものを識別していない場合）には、照合結果を照合ＮＧ（単にＮＧともいう。また、照合の失敗などともいう。）とする（認証失敗の一例）。

【００７５】
また、下記での各装置（ＣＵ制御部２１、セキュリティチップ２２、通信制御ＩＣ２３、払出制御チップ１１、主制御チップ１３なども含む。）間での情報の送受信（各種通知、各種要求なども含む）は、各装置が備える通信部を介して行われるものとする。さらに、下記での各ステップは、例えば、各装置を操作する従業員等のユーザが操作入力部を操作する等の適宜の方法及びタイミングで行われる場合がある。また、各装置が記憶部等に記憶する情報等も、操作入力部への操作等、適宜の方法で、記憶部へ格納されているものとする。

【００７６】
なお、下記で参照される図面中、実線で囲まれた情報は予め格納されている情報を示し、破線で囲まれた情報は新たに格納される情報を示す。また、下線を付した情報は所定の暗号鍵によって暗号化されている情報を示す。また、矢印は、情報の供給方向を示すものである。また、矢印の線が情報まで延びている場合には、その情報が供給先の装置の記憶部に正式に格納されること（例えば、その後の処理で使用可能に格納されることをいい、ＲＡＭに一時記憶されることも含む。）を示し、矢印の線が装置で止まっている場合には、その時点において、その情報が正式に記憶部に格納されないこと（ＲＡＭに一時記憶されることはある。）を示す。

【００７７】
また、各ステップの順序は、各ステップが実行できない事態が生じない限り適宜変更可能である。また、複数の情報を同じ鍵で暗号化する場合、基本的に、それぞれの情報を個別に暗号化するものとするが、適宜、複数の情報をまとめて暗号化することも出来る。

【００７８】
（カードユニット２０の製造時）
カードユニット２０の製造時における各装置の動作等を、図８～１１等を参照して説明する。カードユニット２０は、下記の遊技用システム１の動作などによって、製造されることになる。なお、カードユニット２０は、カードユニットメーカー６００で製造されるが、通信制御ＩＣ２３はチップメーカー１００で製造され、カードユニットメーカー６００に出荷される。セキュリティチップ２２はチップメーカー１００又は他のメーカーで製造され、カードユニットメーカー６００で使用される。カードユニットメーカー６００は、セキュリティ基板２４を製造し、通信制御ＩＣ２３及びセキュリティチップ２２を実装するとともに、ＣＵ制御部２１を製造し、これらを搭載したカードユニット２０を製造する。

【００７９】

図８に示すように、チップメーカー１００は、通信制御ＩＣ用ライター６１０を製造し、カードユニットメーカー６００に出荷する（ステップＡ１）。チップメーカーコンピュータ１１０は、ステップＡ１で出荷された通信制御ＩＣ用ライター６１０についての各種情報を鍵管理センターサーバ３１０に登録する（ステップＡ２）。チップメーカー１００は、ステップＡ１で出荷した通信制御ＩＣ用ライター６１０が情報を書き込む対象である通信制御ＩＣ２３をカードユニットメーカー６００に出荷する（ステップＡ３）。チップメーカーコンピュータ１１０は、ステップＡ３で出荷された通信制御ＩＣ用ライター６１０についての情報を鍵管理センターサーバ３１０に登録する（ステップＡ４）。

【００８０】

ここで、通信制御ＩＣ用ライター６１０の記憶部６１２、チップメーカーコンピュータ１１０の記憶部１１２、通信制御ＩＣ２３の記憶部２３ｂに記憶される情報について説明する。このような情報としては、メーカー情報Ａ、認証用情報Ａ１、配送鍵Ａ、書込鍵、許可情報Ｂ、許可情報Ａ、動作制御情報、バージョン情報Ａ２、暗号鍵Ａ１、バージョン情報Ａ１、秘匿鍵Ａ、認証用情報Ａ２などがある。なお、図示しないが、通信制御ＩＣ用ライター６１０の記憶部６１２、チップメーカーコンピュータ１１０の記憶部１１２、通信制御ＩＣ２３の記憶部２３ｂには、処理を実行するための必要なプログラム、情報なども、適宜記憶されているものとする。

【００８１】

メーカー情報Ａは、通信制御ＩＣ用ライター６１０を製造するチップメーカー１００毎に付された所定の数値などからなる。メーカー情報Ａは、通信制御ＩＣ用ライター６１０の記憶部６１２、チップメーカーコンピュータ１１０の記憶部１１２及び通信制御ＩＣ２３の記憶部２３ｂのそれぞれに格納される。

【００８２】

認証用情報Ａ１は、通信制御ＩＣ用ライター６１０を認証するための情報であり、例えば、通信制御ＩＣ用ライター６１０を識別する識別情報（例えば、通信制御ＩＣ用ライター６１０毎にユニークな識別情報）である。認証用情報Ａ１は、所定の数値などからなる。認証用情報Ａ１は、通信制御ＩＣ用ライター６１０の記憶部６１２及びチップメーカーコンピュータ１１０の記憶部１１２のそれぞれに格納される。

【００８３】

配送鍵Ａは、暗号通信において送受信される情報を暗号化又は復号化するときに使用される、暗号通信用の鍵となるものである。配送鍵Ａは、通信制御ＩＣ用ライター６１０の記憶部６１２及びチップメーカーコンピュータ１１０の記憶部１１２のそれぞれに格納される。

【００８４】

書込鍵は、暗号通信において送受信される情報を暗号化又は復号化するときに使用される、暗号通信用の鍵となるものである。書込鍵は、通信制御ＩＣ２３の記憶部２３ｂ及び通信制御ＩＣ用ライター６１０の記憶部６１２のそれぞれに格納される。

【００８５】

許可情報Ｂ及び許可情報Ａは、それぞれ、所定のタイミングで通信制御ＩＣ２３に設定されることによって、通信制御ＩＣ２３に所定の処理を行わせることを許可する情報（例えば、数値などからなる。）である。許可情報Ｂは、カードユニット２０が遊技場５００に設置された後に、通信制御ＩＣ２３に設定される。許可情報Ａは、カードユニット２０がカードユニットメーカー６００から出荷される前（動作確認時）において、通信制御ＩＣ２３に設定される。許可情報Ｂ及び許可情報Ａは、チップメーカーコンピュータ１１０の記憶部１１２に格納される。

【００８６】

動作制御情報は、通信制御ＩＣ用ライター６１０が所定の動作（例えば、通信制御ＩＣ２３への情報の書き込み）を行うことができる条件を特定するものである。例えば、動作制御情報が第１の内容（例えば、「１」）である場合には、通信制御ＩＣ用ライター６１０は、鍵管理センターサーバ３１０と通信出来ても出来なくても、所定の動作ができる。

一方、例えば、動作制御情報が第２の内容（例えば、「２」）である場合には、通信制御ＩＣ用ライター６１０は、鍵管理センターサーバ３１０と通信出来る場合にのみ所定の動作が出来る。動作制御情報は、チップメーカーコンピュータ１１０の記憶部１１２に格納される。本実施形態では、動作制御情報が第２の内容であり、通信制御ＩＣ用ライター６１０は、鍵管理センターサーバ３１０と通信出来る場合にのみ所定の動作が出来る。

【００８７】

バージョン情報Ａ２は、後に生成される暗号鍵Ａ２のバージョンの情報（第１版、第２版・・・などの版数）として記録されるものである。バージョン情報Ａ２は、その時点（ステップＡ２の時点）において、暗号鍵Ａ２についての最新のバージョンの情報として記録される。バージョン情報Ａ２は、チップメーカーコンピュータ１１０の記憶部１１２に格納される。

【００８８】

暗号鍵Ａ１は、暗号通信において送受信される情報を暗号化又は復号化するときに使用される、暗号通信用の鍵となるものである。暗号鍵Ａ１は、チップメーカーコンピュータ１１０の記憶部１１２に格納される。

【００８９】

バージョン情報Ａ１は、暗号鍵Ａ１のバージョンを表す情報（第１版、第２版・・・などの版数）である。バージョン情報Ａ１は、チップメーカーコンピュータ１１０の記憶部１１２に格納される。

【００９０】

秘匿鍵Ａは、暗号通信において送受信される情報を暗号化又は復号化するときに使用される、暗号通信用の鍵となるものである。秘匿鍵Ａは、通信制御ＩＣ２３の記憶部２３ｂ及びチップメーカーコンピュータ１１０の記憶部１１２に格納される。

【００９１】

認証用情報Ａ２は、通信制御ＩＣ２３を認証するための情報であり、例えば、通信制御ＩＣ２３を識別する識別情報（例えば、１つの通信制御ＩＣ用ライター６１０で情報が書き込まれる複数の通信制御ＩＣ２３（ステップＡ３で出荷される複数の通信制御ＩＣ２３）毎にユニークな識別情報）である。認証用情報Ａ２は、所定の数値などからなる。認証用情報Ａ２は、通信制御ＩＣ用ライター６１０の記憶部６１２及びチップメーカーコンピュータ１１０の記憶部１１２のそれぞれに格納される。

【００９２】

チップメーカーコンピュータ１１０の記憶部１１２に格納される、許可情報Ｂ、許可情報Ａ、動作制御情報、配送鍵Ａ、バージョン情報Ａ２、暗号鍵Ａ１、バージョン情報Ａ１、メーカー情報Ａ、認証用情報Ａ１、認証用情報Ａ２、及び、秘匿鍵Ａは、通信制御ＩＣ用ライター６１０毎に互いに対応付けられて格納される。

【００９３】

ステップＡ２で登録される各種情報は、許可情報Ｂ、許可情報Ａ、動作制御情報、配送鍵Ａ、バージョン情報Ａ２、暗号鍵Ａ１、バージョン情報Ａ１、メーカー情報Ａ、及び、認証用情報Ａ１である。ステップＡ２では、制御部１１１は、ステップＡ１で出荷された通信制御ＩＣ用ライター６１０の認証用情報Ａ１を含む各種情報を鍵管理センターサーバ３１０に送信し、鍵管理センターサーバ３１０の制御部３１１は、制御部１１１が送信した情報を受信すると、受信した各情報を対応付けて記憶部３１２に格納する。上記の送信は、例えば、チップメーカー１００の従業員によるチップメーカーコンピュータ１１０への操作（上記の各種情報の送信を指示する操作）に基づいて行われる。なお、上記の送信において、許可情報Ｂは、秘匿鍵Ａで暗号化され、鍵管理センターサーバ３１０の記憶部３１２には、暗号化されたままで登録される。なお、適宜、チップメーカーコンピュータ１１０と鍵管理センターサーバ３１０とで鍵を持ち、上記各種情報を暗号化して、鍵管理センターサーバ３１０に送信し、鍵管理センターサーバ３１０で復号するようにしてもよい。

【００９４】

ステップＡ４で登録される通信制御ＩＣ２３についての情報は、認証用情報Ａ２である。ステップＡ４において、制御部１１１は、ステップＡ３で出荷された通信制御ＩＣ２３の認証用情報Ａ２を、認証用情報Ａ２に対応づけられた認証用情報Ａ１とともに、鍵管理センターサーバ３１０に送信し、鍵管理センターサーバ３１０の制御部３１１は、制御部３１１が送信した認証用情報Ａ１及び認証用情報Ａ２を受信し、ステップＡ２で記憶部３１２に格納した認証用情報Ａ１を含む各種情報に対応付けて受信した認証用情報Ａ２を記憶部３１２に格納する。上記の送信は、例えば、チップメーカー１００の従業員によるチップメーカーコンピュータ１１０への操作（上記の各種情報の送信を指示する操作）に基づいて行われる。なお、適宜、チップメーカーコンピュータ１１０と鍵管理センターサーバ３１０とで鍵を持ち、上記各情報を暗号化して、鍵管理センターサーバ３１０に送信し、鍵管理センターサーバ３１０で復号するようにしてもよい。

【００９５】

ステップＡ２及びＡ４で登録された各情報は、鍵管理センターサーバ３１０の記憶部３１２に格納されている他の情報にも、対応付けられて記憶部３１２に格納される。前記の他の情報としては、暗号鍵Ｃ１、出荷情報、日時、更新情報、配送鍵Ｂ、メーカー情報Ｂ、認証用情報Ｂ１、バージョン情報Ｃ、暗号鍵Ｃ３、動作モードがある。これら情報は、適宜のタイミングで、例えば、カードユニットメーカー６００の依頼などに基づく鍵管理センター３００の従業員による鍵管理センターサーバ３１０への操作（上記の情報を登録する操作）に基づいて行われる。

【００９６】

暗号鍵Ｃ１は、暗号通信において送受信される情報を暗号化又は復号化するときに使用される、暗号通信用の鍵となるものである。

【００９７】

出荷情報は、ステップＡ１での通信制御ＩＣ用ライター６１０の出荷先、ステップＡ３での通信制御ＩＣ２３の出荷先、つまり、この出荷情報に対応付けられて格納される認証用情報Ａ１を格納している通信制御ＩＣ用ライター６１０及び認証用情報Ａ２を格納している通信制御ＩＣ２３の出荷先のカードユニットメーカー６００を識別する情報であり、例えば、所定の数値などからなる。

【００９８】

日時は、現在の日時（日付までであってもよく、時刻は含まなくてもよい。）を表す情報である。例えば、制御部１１１は、制御部１１１が含むカレンダ部（図示せず）を参照し、現在の日時を取得し、取得した日時を日時としてリアルタイムで更新していく。

【００９９】

更新情報は、暗号鍵Ａ２を生成するときのもとになる情報である。更新情報は、例えば、所定の数値などからなる。この更新情報の内容は、バージョン情報Ａ２の内容（例えば、版数）と対応する。このため、バージョン情報Ａ２は、その後に生成される暗号鍵Ａ２（及び更新情報）のバージョン（例えば、版数）を示す情報になる。更新情報は、例えば、鍵管理センター３００の従業員による鍵管理センターサーバ３１０への操作（更新情報を更新する操作）などに基づいて、適宜のタイミングで更新される。この場合、バージョン情報Ａ２が示すバージョンも更新され、例えば、新たな更新情報の版数にバージョン情報Ａ２が更新されるものとする。

【０１００】

配送鍵Ｂは、暗号通信において送受信される情報を暗号化又は復号化するときに使用される、暗号通信用の鍵となるものである。

【０１０１】

メーカー情報Ｂは、セキュリティ基板２４を製造するメーカーを識別する情報であり、例えば、所定の数値などからなる。なお、本実施形態では、セキュリティ基板２４を製造するのは、カードユニットメーカー６００なので、メーカー情報Ｂは、カードユニットメーカー６００を識別する情報である。

【０１０２】

認証用情報Ｂ１は、ＳＣ用ライター６５０の認証に使用するための情報であり、例えば、ＳＣ用ライター６５０を識別する識別情報（例えば、ＳＣ用ライター６５０毎にユニークな識別情報）である。認証用情報Ｂ１は、所定の数値などからなる。

【０１０３】

バージョン情報Ｃは、セキュリティチップ２２や、セキュリティ基板２４のバージョンを表す情報（第１版、第２版・・・などの版数）である。

【０１０４】

暗号鍵Ｃ３は、暗号通信において送受信される情報を暗号化又は復号化するときに使用される、暗号通信用の鍵となるものである。

【０１０５】

動作モードは、セキュリティチップ２２の動作（処理部２２ａの処理内容）を規定する情報である。セキュリティチップ２２の処理部２２ａは、動作モードが記憶部２２ｂに格納されていると、この動作モードに応じた処理（つまり、後述の各種処理）を行う。

【０１０６】

なお、鍵管理センターサーバ３１０の制御部３１１は、記憶部３１２に格納された、許可情報Ｂ（暗号化されたままの情報）及び暗号鍵Ｃ１を、所定のタイミング（例えば、鍵管理センター３００の従業員による鍵管理センターサーバ３１０への操作（更新情報を更新する操作）などのタイミング）で、上位サーバ５１０に送信し、上位サーバ５１０の制御部３１１は、鍵管理センターサーバ３１０から送信される許可情報Ｂ（暗号化されたままの情報）及び暗号鍵Ｃ１を記憶部３１２に格納する（ステップＡ９９）。許可情報Ｂは、引き続き暗号化されたままの状態で、記憶部３１２に格納される。なお、許可情報Ｂ（暗号化されたままの情報）及び暗号鍵Ｃ１の上位サーバ５１０の記憶部５１２への格納は、情報記憶媒体（例えば、ＣＤ－ＲＯＭ（Compact Disc Read Only Memory）など）を上位サーバ５１０の読み取り装置（例えば、ＣＤドライブなどであり、入出力部５１３が備えているものとする。）に挿入等して、情報記憶媒体から許可情報Ｂ（暗号化されたままの情報）及び暗号鍵Ｃ１を読み取らせて、記憶部５１２に格納するなど、適宜の方法によって行っても良い。許可情報Ｂが格納される上位サーバ３１０は、ステップＡ３によって出荷された各通信制御ＩＣ２３が搭載されて製造された各カードユニット２０の出荷先の遊技場５００に設置される上位サーバである。本実施形態では、１つの通信制御ＩＣ用ライター６１０が用いられて製造される各通信制御ＩＣ２３をそれぞれ搭載した各カードユニット２０すべては、１つの遊技場５００に設置されるものとする。

【０１０７】

また、図９のように、ＳＣ用ライター６５０及びセキュリティチップ２２は、他メーカーによって製造されてカードユニットメーカー６００に納入されるか、カードユニットメーカー６００自身によって製造される。ＳＣ用ライター６５０の記憶部６５２には、認証用情報Ｂ１（鍵管理センターサーバ３１０に登録されている認証用情報Ｂ１に対応している。）、配送鍵Ｂ（鍵管理センターサーバ３１０に登録されている配送鍵Ｂに対応している。）が格納されている。カードユニットメーカー６００において、セキュリティ基板２４が製造され、セキュリティチップ２２と通信制御ＩＣ２３とがセキュリティ基板２４に実装されると、ステップＡ５以降の処理が行われる。なお、通信制御ＩＣ用ライター６１０とＳＣ用ライター６５０とは、互いに通信可能に接続されている。なお、図示しないが、ＳＣ用ライター６５０の記憶部６５２、セキュリティチップ２２の記憶部２２ｂには、処理を実行するための必要なプログラム、情報なども、適宜記憶されているものとする。

【０１０８】

ステップＡ５において、通信制御ＩＣ用ライター６１０の制御部６１１は、記憶部６１２に格納されている、認証用情報Ａ１とメーカー情報Aとを、照合要求とともに、鍵管理センターサーバ３１０に送信する。鍵管理センターサーバ３１０の制御部３１１は、認証用情報Ａ１とメーカー情報Ａとを照合要求とともに受信すると、記憶部３１２に格納されている認証用情報Ａ１及びメーカー情報Ａと、受信した認証用情報Ａ１及びメーカー情報Ａと、を照合する。この照合がＮＧの場合（少なくともいずれか１つの情報についての照

合がＮＧだった場合）には、制御部３１１は、照合ＮＧの旨を通信制御ＩＣ用ライター６１０に通知するとともに、入出力部３１３等を介して、所定の報知処理（例えば入出力部３１３に含まれる表示部への照合ＮＧの旨の表示、入出力部３１３に含まれるブザーを鳴らす等。以下制御部３１１が行う所定の報知処理について同じ。）を行う。上記の通知を受け取った制御部６１１は、入出力部６１３等を介して、所定の報知処理（例えば入出力部６１３に含まれる表示部への照合ＮＧの旨の表示、入出力部６１３に含まれるブザーを鳴らす等。以下制御部６１１が行う所定の報知処理について同じ。）を行う。

【０１０９】

ステップＡ５の照合がＯＫの場合（全ての照合がＯＫだった場合）には、ステップＡ６において、鍵管理センターサーバ３１０の制御部３１１は、記憶部３１２に格納されている、暗号鍵Ａ１、バージョン情報Ａ１、出荷情報、動作制御情報、日時を通信制御ＩＣ用ライター６１０に送信し、通信制御ＩＣ用ライター６１０の制御部６１１は、鍵管理センターサーバ３１０から送信される前記各情報を受信し、記憶部６１２に格納する（情報登録）。なお、通信制御ＩＣ用ライター６１０の制御部６１１は、ステップＡ６での情報登録が終了すると、適宜、ＳＣ用ライター６５０に、その旨を送信する。なお、日時は、ステップＡ６が行われた時点で固定される。

【０１１０】

なお、ステップＡ５において、通信制御ＩＣ用ライター６１０の制御部６１１は、認証用情報Ａ１とメーカー情報Aとを、配送鍵Ａによって暗号化して送っても良い。この場合、鍵管理センターサーバ３１０は、例えば、通信制御ＩＣ用ライター６１０の通信アドレス毎に、記憶部３１２に格納する情報を管理しておき、制御部３１１は、通信アドレスに基づいて、どの配送鍵Ａで情報を復号化するかを決定し、決定した配送鍵Ａで復号化し、復号化に使用した配送鍵Ａに対応する認証用情報Ａ１とメーカー情報Aとに基づいて、上記照合を行う。または、制御部３１１は、記憶部３１２に格納された全ての配送鍵Ａで復号化を試みて、復号化が出来た配送鍵Ａに対応する認証用情報Ａ１とメーカー情報Aとに基づいて、上記照合を行っても良い。

【０１１１】

また、ステップＡ６において、鍵管理センターサーバ３１０の制御部３１１は、暗号鍵Ａ１、バージョン情報Ａ１、出荷情報、動作制御情報、日時を、記憶部３１２に格納する配送鍵Ａによって暗号化して送っても良い。この場合、通信制御ＩＣ用ライター６１０の制御部６１１は、鍵管理センターサーバ３１０から受信した前記各情報を記憶部６１２に格納する配送鍵Ａで復号化してから記憶部６１２に格納する（情報登録）。

【０１１２】

ステップＡ７において、通信制御ＩＣ用ライター６１０から情報登録の終了を受信したＳＣ用ライター６５０の制御部６５１は、記憶部６５２に格納されている、認証用情報Ｂ１を、照合要求とともに、鍵管理センターサーバ３１０に送信する。鍵管理センターサーバ３１０の制御部３１１は、認証用情報Ｂ１を照合要求とともに受信すると、記憶部３１２に格納されている認証用情報Ｂ１と、受信した認証用情報Ｂ１と、を照合する。この照合がＮＧの場合には、制御部３１１は、照合ＮＧの旨をＳＣ用ライター６５０に通知するとともに、入出力部３１３等を介して、所定の報知処理を行う。上記の通知を受け取った制御部６５１は、入出力部６５３等を介して、所定の報知処理（例えば入出力部６５３に含まれる表示部への照合ＮＧの旨の表示、入出力部６５３に含まれるブザーを鳴らす等。以下制御部６５１が行う所定の報知処理について同じ。）を行う。

【０１１３】

ステップＡ７の照合がＯＫの場合には、ステップＡ８において、鍵管理センターサーバ３１０の制御部３１１は、記憶部３１２に格納されている、暗号鍵Ｃ１、日時、メーカー情報Ｂ、バージョン情報Ｃ、許可情報Ａ、暗号鍵Ｃ３、動作モードをＳＣ用ライター６５０に送信し、ＳＣ用ライター６５０の制御部６５１は、鍵管理センターサーバ３１０から送信される前記各情報を受信し、記憶部６５２に格納する（情報登録）。なお、ＳＣ用ライター６５０の制御部６５１は、ステップＡ８での情報登録が終了すると、適宜、通信制

御ＩＣ用ライター６１０に、その旨を送信する。

【０１１４】

なお、ステップＡ７において、ＳＣ用ライター６５０の制御部６５１は、認証用情報Ｂ１を、配送鍵Ｂによって暗号化して送っても良い。この場合、鍵管理センターサーバ３１０は、例えば、ＳＣ用ライター６５０の通信アドレス毎にも、記憶部３１２に格納する情報を管理しておき、制御部３１１は、通信アドレスに基づいて、どの配送鍵Ｂで情報を復号化するかを決定し、決定した配送鍵Ｂで復号化し、復号化に使用した配送鍵Ｂに対応する認証用情報Ｂ１に基づいて、上記照合を行う。または、制御部３１１は、記憶部３１２に格納された全ての配送鍵Ｂで復号化を試みて、復号化が出来た配送鍵Ｂに対応する認証用情報Ｂ１に基づいて、上記照合を行っても良い。

【０１１５】

また、ステップＡ８において、鍵管理センターサーバ３１０の制御部３１１は、暗号鍵Ｃ１、暗号鍵Ａ１、バージョン情報Ａ１、出荷情報、日時、メーカー情報Ｂ、バージョン情報Ｃ、許可情報Ａ、暗号鍵Ｃ３、動作モードを、記憶部３１２に格納する配送鍵Ｂによって暗号化して送っても良い。この場合、ＳＣ用ライター６５０の制御部６５１は、鍵管理センターサーバ３１０から受信した前記各情報を記憶部６５２に格納する配送鍵Ｂで復号化してから記憶部６５２に格納する（情報登録）。

【０１１６】

ステップＡ９において、ＳＣ用ライター６５０から情報登録の終了を受信した通信制御ＩＣ用ライター６１０の制御部６１１は、書込読取部６１５を介して、通信制御ＩＣ２３からメーカー情報Ａを読み取り、読み取ったメーカー情報Ａと、記憶部６１２に格納されているメーカー情報Ａとを照合する。なお、このとき、メーカー情報Ａは、通信制御ＩＣ２３の処理部２３ａによって、記憶部２３ｂに格納された書込鍵で暗号化されて送信され、通信制御ＩＣ用ライター６１０の制御部６１１は、受信したメーカー情報Ａを記憶部６１２の書込鍵で復号化し、前記照合を行っても良い。この照合がＮＧの場合には、制御部６１１は、入出力部６１３等を介して、所定の報知処理を行う。この照合がＯＫだった場合には、通信制御ＩＣ用ライター６１０の制御部６１１は、書込読取部６１５を介して、通信制御ＩＣ２３から認証用情報Ａ２を読み取り、読み取った認証用情報Ａ２を記憶部６１２に格納する。このようにして、認証用情報Ａ２の情報登録が行われる（ステップＡ１０）。なお、このとき、認証用情報Ａ２は、通信制御ＩＣ２３の処理部２３ａによって、記憶部２３ｂに格納された書込鍵で暗号化されて送信され、通信制御ＩＣ用ライター６１０の制御部６１１は、受信したメーカー情報Ａを記憶部６１２の書込鍵で復号化し、記憶部６１２に格納してもよい。

【０１１７】

ステップＡ１０が終わると、ステップＡ１１において、通信制御ＩＣ用ライター６１０の制御部６１１は、記憶部６１２に格納されている認証用情報Ａ１、暗号鍵Ａ１、バージョン情報Ａ１、出荷情報、認証用情報Ａ２をＳＣ用ライター６５０に送信する。ＳＣ用ライター６５０の制御部６５１は、通信制御ＩＣ用ライター６１０から送信された認証用情報Ａ１、暗号鍵Ａ１、バージョン情報Ａ１、出荷情報、認証用情報Ａ２を受信すると、記憶部６５２に格納する（情報登録）。

【０１１８】

ステップＡ１１が終わると、ステップＡ１２において、ＳＣ用ライター６５０の制御部６５１は、記憶部６１２に格納されているメーカー情報Ｂ、日時、認証用情報Ａ１に基づいて、認証用情報Ｃ１を自動生成する。例えば、制御部６５１は、メーカー情報Ｂと、日時と、認証用情報Ａ１とを論理演算するなどして、認証用情報Ｃ１を生成する。また、制御部６５１は、乱数生成回路を備え、乱数生成回路が生成した乱数と、メーカー情報Ｂと、日時と、認証用情報Ａ１とを論理演算し、認証用情報Ｃ１を生成してもよい。

【０１１９】

ここで、認証用情報Ｃ１は、セキュリティ基板２４を認証するための情報であり、例えば、セキュリティ基板２４を識別する識別情報（例えば、ステップＡ３で出荷される複数

の通信制御ＩＣ２３がそれぞれ実装される複数のセキュリティ基板２４毎にユニークな識別情報）である。同じカードユニット２０内には、セキュリティ基板２４と、セキュリティチップ２２と、ＣＵ制御部２１とが搭載されているため、例えば、セキュリティ基板２４を識別する識別情報は、セキュリティチップ２２と、ＣＵ制御部２１とを識別する識別情報でもある。このように、認証用情報Ｃ１は、セキュリティチップ２２やＣＵ制御部２１を認証するための情報でもある。認証用情報Ｃ１は、所定の数値などからなる。

【０１２０】

ステップＡ１２が終わると、ステップＡ１３において、ＳＣ用ライター６５０の制御部６５１は、ステップＡ１２で生成した認証用情報Ｃ１に基づいて、認証用情報Ｂ２、認証用情報Ｃ２を自動生成する。例えば、制御部６５１は、乱数生成回路を備え、乱数生成回路が生成した乱数と、認証用情報Ｃ１とを論理演算し、認証用情報Ｂ２、認証用情報Ｃ２をそれぞれ別個に生成する。

【０１２１】

ここで、認証用情報Ｂ２は、セキュリティチップ２２を認証するための情報であり、例えば、セキュリティチップ２２を識別する識別情報（例えば、１つのＳＣ用ライター６５０で情報が書き込まれる複数のセキュリティチップ２２（ステップＡ３で出荷される複数の通信制御ＩＣ２３とそれぞれ対をなす（同じセキュリティ基板２４に実装される）セキュリティチップ２２）毎にユニークな識別情報）である。認証用情報Ｂ２は、所定の数値などからなる。

【０１２２】

ここで、認証用情報Ｃ２は、セキュリティ基板２４を認証するための情報であり、例えば、セキュリティ基板２４を識別する識別情報（例えば、ステップＡ３で出荷される複数の通信制御ＩＣ２３がそれぞれ実装される複数のセキュリティ基板２４毎にユニークな識別情報）である。同じカードユニット２０内には、セキュリティ基板２４と、セキュリティチップ２２と、ＣＵ制御部２１とが搭載されているため、例えば、セキュリティ基板２４を識別する識別情報は、セキュリティチップ２２と、ＣＵ制御部２１とを識別する識別情報でもある。このように、認証用情報Ｃ２は、セキュリティチップ２２やＣＵ制御部２１を認証するための情報でもある。認証用情報Ｃ２は、所定の数値などからなる（認証用情報Ｃ１とは数値が異なる）。

【０１２３】

ステップＡ１３が終わると、ステップＡ１４において、ＳＣ用ライター６５０の制御部６５１は、記憶部６５２に格納されている認証用情報Ｂ２を通信制御ＩＣ用ライター６１０に送信する。通信制御ＩＣ用ライター６１０の制御部６１１は、ＳＣ用ライター６５０から送信された認証用情報Ｂ２を受信すると、記憶部６１２に格納する（情報登録）。

【０１２４】

なお、ステップＡ１１及びＡ１４では、適宜、通信制御ＩＣ用ライター６１０とＳＣ用ライター６５０とで鍵を持ち、通信制御ＩＣ用ライター６１０（又はＳＣ用ライター６５０）が送信する情報をこの鍵で暗号化し、ＳＣ用ライター６５０（又は通信制御ＩＣ用ライター６１０）は受信した情報を前記鍵で復号化し記憶部６５２（又は記憶部６１２）に格納してもよい。

【０１２５】

ステップＡ１４が終わると、ステップＡ１５において、通信制御ＩＣ用ライター６１０の制御部６１１は、書込読取部６１５を介して、認証用情報Ａ１と、暗号鍵Ａ１と、バージョン情報Ａ１と、出荷情報と、認証用情報Ｂ２と、を通信制御ＩＣ２３に書き込む（情報登録）。通信制御ＩＣ用ライター６１０の制御部６１１は、記憶部に格納されている書込鍵で、前記各情報を暗号化し、通信制御ＩＣ２３に供給する。通信制御ＩＣ２３の処理部２３ａは、供給された各情報を記憶部２３ｂが格納する書込鍵で復号化し、復号化した、認証用情報Ａ１と、暗号鍵Ａ１と、バージョン情報Ａ１と、出荷情報と、認証用情報Ｂ２とを、記憶部２３ｂに格納する。これによって前記の書き込みが行われる。なお、この書込時において、通信制御ＩＣ用ライター６１０の制御部６１１は、上記情報とともに、

後述の処理を実行させるプログラムなど（この場合、カードユニットメーカー６００の従業員の操作などによって、記憶部６５２にこれら情報が格納されるものとする。）をセキュリティチップ２２に書き込んでも良い（上記暗号化も適宜行う）。

【０１２６】

一方、ＳＣ用ライター６５０の制御部６５１は、ステップＡ１４の処理を行うと、秘匿鍵Ｂを生成する（ステップＡ１６）。秘匿鍵Ｂは、例えば、自動生成される。例えば、制御部６５１は、乱数生成回路を備え、乱数生成回路が生成した乱数に基づく論理演算を行い、秘匿鍵Ｂを生成する。秘匿鍵Ｂは、例えば、カードユニットメーカー６００の従業員によるＳＣ用ライター６５０への操作（秘匿鍵Ｂを登録する操作）などに基づいて、適宜のタイミングで生成されてもよい。また、制御部６５１は、記憶部６５２が記憶する情報（例えば、日時）と乱数生成回路が生成した乱数とで論理演算を行い、秘匿鍵Ｂを生成してもよい。

【０１２７】

秘匿鍵Ｂは、暗号通信において送受信される情報を暗号化又は復号化するときに使用される、暗号通信用の鍵となるものである。

【０１２８】

ＳＣ用ライター６５０の制御部６５１は、ステップＡ１６の処理を行うと、ステップＡ１６．５として、書込読取部６５５を介して、許可情報Ａと、メーカー情報Ｂと、認証用情報Ａ１と、暗号鍵Ａ１と、バージョン情報Ａ１と、出荷情報と、認証用情報Ａ２と、認証用情報Ｂ２と、暗号鍵Ｃ３と、認証用情報Ｃ１と、認証用情報Ｃ２と、暗号鍵Ｃ１と、バージョン情報Ｃと、日時と、動作モードと、秘匿鍵Ｂと、をセキュリティチップ２２に書き込む（情報登録）。この書込時において、ＳＣ用ライター６５０の制御部６５１は、上記情報とともに、後述の処理を実行させるプログラムなど（この場合、カードユニットメーカー６００の従業員の操作などによって、記憶部６５２にこれら情報が格納されるものとする。）をセキュリティチップ２２に書き込んでも良い。なお、ＳＣ用ライター６５０とセキュリティチップ２２とで共通の鍵を設定しておき（例えば、製造時に記憶部６５２及び記憶部２２ｂに共通して格納する。）、この書込時において、ＳＣ用ライター６５０の制御部６５１は、設定された前記鍵で、前記各情報などを暗号化し、セキュリティチップ２２に供給し、セキュリティチップ２２の処理部２２ａは、供給された各情報を記憶部２２ｂが格納する前記鍵で復号化し、復号化した、許可情報Ａ、メーカー情報Ｂ、認証用情報Ａ１、暗号鍵Ａ１、バージョン情報Ａ１、出荷情報、認証用情報Ａ２、認証用情報Ｂ２、暗号鍵Ｃ３、認証用情報Ｃ１、認証用情報Ｃ２、暗号鍵Ｃ１、バージョン情報Ｃ、日時、動作モード、秘匿鍵Ｂなどを、記憶部２２ｂに格納してもよい。

【０１２９】

ステップＡ１５のあと、通信制御ＩＣ用ライター６１０の制御部６１１は、書込読取部６１５を介して、認証用情報Ａ１と、暗号鍵Ａ１と、バージョン情報Ａ１と、出荷情報と、認証用情報Ｂ２と、を通信制御ＩＣ２３に書き込む（情報登録）。通信制御ＩＣ用ライター６１０の制御部６１１は、記憶部に格納されている書込鍵で、前記各情報を暗号化し、通信制御ＩＣ２３に供給する。通信制御ＩＣ２３の処理部２３ａは、供給された各情報を記憶部２３ｂが格納する書込鍵で復号化し、復号化した、認証用情報Ａ１と、暗号鍵Ａ１と、バージョン情報Ａ１と、出荷情報と、認証用情報Ｂ２とを、記憶部２３ｂに格納する。これによって前記の書き込みが行われる。

【０１３０】

ステップＡ１５が終了すると、ステップＡ１７において、通信制御ＩＣ用ライター６１０の制御部６１１は、記憶部６１２に格納されている、認証用情報Ａ１と、認証用情報Ａ２と、認証用情報Ｂ２と、を、鍵管理センターサーバ３１０に送信する。

【０１３１】

ステップＡ１６．５が終了すると、ステップＡ１８において、ＳＣ用ライター６５０の制御部６５１は、記憶部６５２に格納されている、認証用情報Ｂ２と、認証用情報Ｃ２と、認証用情報Ｃ１と、暗号鍵Ｃ２と、秘匿鍵Ｂと、を、鍵管理センターサーバ３１０に送

信する。

【０１３２】

ステップ１８．５において、鍵管理センターサーバ３１０の制御部３１１は、ステップＡ１７で通信制御ＩＣ用ライター６１０から送信された認証用情報Ａ１と、認証用情報Ａ２と、認証用情報Ｂ２と、を受信し、ステップＡ１８でＳＣ用ライター６５０から送信された認証用情報Ｂ２と、認証用情報Ｃ２と、認証用情報Ｃ１と、暗号鍵Ｃ２と、秘匿鍵Ｂと、を受信すると、記憶部３１２に格納されている認証用情報Ａ２と、通信制御ＩＣ用ライター６１０から送信された認証用情報Ａ２と、を照合し、照合ＯＫであれば、記憶部３１２に格納されている認証用情報Ａ２（照合ＯＫの認証用情報Ａ２）に対応付けて、認証用情報Ａ１と、認証用情報Ｂ２と、認証用情報Ｃ２と、認証用情報Ｃ１と、暗号鍵Ｃ２と、秘匿鍵Ｂと、を正式登録する（後述の処理で使用可能なように記憶部３１２に正式に格納する。）。なお、鍵管理センターサーバ３１０の制御部３１１は、通信制御ＩＣ用ライター６１０から送信された認証用情報Ｂ２と同じ認証用情報Ｂ２を送信したＳＣ用ライター６５０から送信された認証用情報Ｂ２と、認証用情報Ｃ２と、認証用情報Ｃ１と、暗号鍵Ｃ２と、秘匿鍵Ｂと、を正式登録する。つまり、認証用情報Ｂ２によって、対となる通信制御ＩＣ用ライター６１０とＳＣ用ライター６５０が特定され、各情報が正式登録されることになる。

【０１３３】

鍵管理センターサーバ３１０の制御部３１１は、上記正式登録終了後に、通信制御ＩＣ用ライター６１０及びＳＣ用ライター６５０に対して、正式登録完了を通知する。通信制御ＩＣ用ライター６１０の制御部６１１及びＳＣ用ライター６５０の制御部６５１は、正式登録完了を受信すると、それぞれが、ステップＡ１５、ステップＡ１６及び１６．５を、複数のセキュリティ基板２４（ステップＡ３で出荷された通信制御ＩＣ２３分のセキュリティ基板２４）のうちの残りのセキュリティ基板２４それぞれの通信制御ＩＣ２３及びセキュリティ２２に対して行うことが可能になるように設定されている。ステップＡ１６及び１６．５がセキュリティ基板２４それぞれの通信制御ＩＣ２３及びセキュリティ２２に対して行われると、上記情報が書き込まれた通信制御ＩＣ２３及びセキュリティ２２が実装されたセキュリティ基板２４が量産されることになる。なお、各セキュリティ基板２４それぞれの通信制御ＩＣ２３及びセキュリティ２２について、ステップＡ９以降の処理を繰り返し行うことによって、上記情報が書き込まれた通信制御ＩＣ２３及びセキュリティ２２が実装されたセキュリティ基板２４を量産してもよい。この場合、ステップＡ１８で正式登録される情報は、同じ情報で随時更新されることになる。

【０１３４】

なお、ステップＡ１８．５で、照合がＮＧだった場合、照合ＮＧの旨を通信制御ＩＣ用ライター６１０及びＳＣ用ライター６５０（通信制御ＩＣ用ライター６１０が送信した認証用情報Ｂ２と同じ認証用情報Ｂ２を送信するＳＣ用ライター６５０）に通知するとともに、入出力部３１３等を介して、所定の報知処理を行う。上記の通知を受け取った通信制御ＩＣ用ライター６１０の制御部６１１及びＳＣ用ライター６５０の制御部６５１は、それぞれ、入出力部等を介して、所定の報知処理を行う。

【０１３５】

なお、ステップＡ１５において、通信制御ＩＣ用ライター６１０の制御部６１１は、認証用情報Ａ１と、認証用情報Ａ２と、認証用情報Ｂ２と、を、記憶部６１２に格納された配送鍵Ａによって暗号化して送っても良い。この場合、鍵管理センターサーバ３１０は、例えば、通信制御ＩＣ用ライター６１０の通信アドレス毎に、記憶部３１２に格納する情報を管理しておき、制御部３１１は、ステップＡ１８．５において、通信アドレスに基づいて、どの配送鍵Ａで情報を復号化するかを決定し、決定した配送鍵Ａで、認証用情報Ａ１と、認証用情報Ａ２と、認証用情報Ｂ２と、を復号化し、上記照合や正式登録を行う。または、制御部３１１は、ステップＡ１８．５において、記憶部３１２に格納された全ての配送鍵Ａで復号化を試みて、復号化が出来た配送鍵Ａに対応する認証用情報Ａ２について上記照合を行い、復号化した情報について上記正式登録を行っても良い。

【０１３６】
なお、ステップＡ１６．５において、ＳＣ用ライター６５０の制御部６５１は、認証用情報Ｂ２と、認証用情報Ｃ２と、認証用情報Ｃ１と、暗号鍵Ｃ２と、秘匿鍵Ｂと、を、記憶部６５２に格納された配送鍵Ｂによって暗号化して送っても良い。この場合、鍵管理センターサーバ３１０は、例えば、ＳＣ用ライター６５０の通信アドレス毎に、記憶部３１２に格納する情報を管理しておき、制御部３１１は、ステップＡ１８．５において、通信アドレスに基づいて、どの配送鍵Ｂで情報を復号化するかを決定し、決定した配送鍵Ｂで、認証用情報Ｂ２と、認証用情報Ｃ２と、認証用情報Ｃ１と、暗号鍵Ｃ２と、秘匿鍵Ｂと、を復号化し、上記正式登録などを行ってもよい。または、制御部３１１は、ステップＡ１８．５において、記憶部３１２に格納された全ての配送鍵Ｂで復号化を試みて、復号化が出来た配送鍵Ｂに対応する認証用情報Ａ２に対応付けて、復号化した情報について上記正式登録を行っても良い。
【０１３７】
なお、ステップＡ１８において、ＳＣ用ライター６５０の制御部６５１は、記憶部６５２に格納されている、認証用情報Ａ２を、認証用情報Ｂ２などともに鍵管理センターサーバ３１０に送信してもよい。この場合、鍵管理センターサーバ３１０の制御部３１１は、記憶部３１２に格納されている認証用情報Ａ２と、通信制御ＩＣ用ライター６１０から送信された認証用情報Ａ２と、を照合し、照合ＯＫであれば、記憶部３１２に格納されている認証用情報Ａ２（照合ＯＫの認証用情報Ａ２）に対応付けて、認証用情報Ａ１と、認証用情報Ｂ２と、を正式登録し、鍵管理センターサーバ３１０の制御部３１１は、記憶部３１２に格納されている認証用情報Ａ２と、ＳＣ用ライター６５０から送信された認証用情報Ａ２と、を照合し、照合ＯＫであれば、記憶部３１２に格納されている認証用情報Ａ２（照合ＯＫの認証用情報Ａ２）に対応付けて、認証用情報Ｃ２と、認証用情報Ｃ１と、暗号鍵Ｃ２と、秘匿鍵Ｂと、を正式登録してもよい。
【０１３８】
なお、上記ステップＡ１１で登録される情報のうちの一部（例えば、暗号鍵Ａ１、バージョン情報Ａ１、出荷情報）は、ステップＡ８で登録されてもよい。つまり、通信制御ＩＣライター６１０経由ではなく、鍵管理センターサーバ３１０から直接ＳＣ用ライター６５０に情報（例えば、暗号鍵Ａ１、バージョン情報Ａ１、出荷情報）を送信し、情報登録を行ってもよい。
【０１３９】
また、上記ステップＡ８で登録される情報のうちの少なくとも一部（例えば、日時）は、ステップＡ１１で登録されてもよい。つまり、鍵管理センターサーバ３１０から直接ＳＣ用ライター６５０に情報（例えば、日時）を送信し、情報登録を行うのではなく、通信制御ＩＣライター６１０から情報（例えば、日時）を送信し、情報登録を行うことで、通信制御ＩＣライター６１０経由で情報登録を行っても良い。
【０１４０】
なお、カードユニットメーカー６００は、これら処理とは別にカードユニット２０の筐体やＣＵ制御部２１等のカードユニット２０を構成する各部を製造し、製造した筐体、ＣＵ制御部２１等の各部と、前記処理によって情報が書き込まれた通信制御ＩＣ２３及びセキュリティチップ２２を実装したセキュリティ基板２４と、を組み合わせて、カードユニット２０を製造する。
【０１４１】
上記のように、本実施形態では、通信制御ＩＣ２３及び通信制御ＩＣ用ライター６１０がチップメーカー１００で製造されて、カードユニットメーカー６００に出荷、納入される。また、セキュリティチップ２２及びＳＣ用ライター６５０は、カードユニットメーカー６００又は他のメーカー（特にチップメーカー１００以外）によって製造され、カードユニットメーカー６００で使用される。つまり、通信制御ＩＣ２３及び通信制御ＩＣ用ライター６１０の製造元と、セキュリティチップ２２及びＳＣ用ライター６５０の製造元とが異なる。一方、後述するように、セキュリティチップ２２と通信制御ＩＣ２３とは、お

互いの認証用情報を用いて認証が行われるので、相互に認証用情報を持つ必要がある。仮に、ライターを一台として、ＳＣ用ライター６５０によって、通信制御ＩＣ２３の認証に用いられる認証用情報Ａ２を通信制御ＩＣ２３から読み取り、セキュリティチップ２２に書き込む場合を考えると、通信制御ＩＣ２３の製造元（チップメーカー１００）は、ＳＣ用ライター６５０の製造元（カードユニットメーカー６００又は他のメーカー）である他の製造元に対して、通信制御ＩＣ２３に対する情報の読み書きの仕様などを開示する必要が生じ、他の製造元に仕様を開示することは、情報漏洩の観点から問題が生じる。また、通信制御ＩＣ用ライター６１０によって、セキュリティチップ２２の認証に用いられる認証用情報Ｂ２をＳＣ用ライター６５０の代わりに生成し、セキュリティチップ２２及びＳＣ用ライター６５０に書き込む場合を考えると、セキュリティチップ２２の製造元（カードユニットメーカー６００又は他のメーカー）は、通信制御ＩＣ用ライター６１０の製造元（チップメーカー１００）である他の製造元に対して、セキュリティチップ２２に対する情報の書込の仕様、認証用情報Ｂ２の生成ロジックなどを開示する必要が生じ、他の製造元に仕様を開示することは、情報漏洩の観点から問題が生じる。そこで上記実施形態では、２つのライター（通信制御ＩＣ用ライター６１０及びＳＣ用ライター６５０）を用意し、通信制御ＩＣ用ライター６１０は、セキュリティチップ２２に対して情報を読み書きすることが出来ず、ＳＣ用ライター６５０は、通信制御ＩＣ２３に対して情報を読み書き出来ないようにした。具体的には、認証用情報Ａ２については、通信制御ＩＣ用ライター６１０で読み取り（ステップＡ１０）、通信制御ＩＣ用ライター６１０がＳＣ用ライター６５０に送信し（ステップＡ１１）、ＳＣ用ライター６５０がセキュリティチップ２２に書き込むようにした（ステップＡ１６．５）。また、認証用情報Ｂ２については、ＳＣ用ライター６５０が生成を行い（ステップＡ１３）、通信制御ＩＣ用ライター６１０に送信し（ステップＡ１４）、通信制御ＩＣ用ライター６１０が通信制御ＩＣ２３に書き込むようにした（ステップＡ１５）。このような構成によって、上記の開示は必要なくなり、本実施形態では、情報漏洩のリスクを低減又は無くすことができる。

【０１４２】

また、通信制御ＩＣ用ライター６１０とＳＣ用ライター６５０とは、それぞれ、鍵管理センターサーバ３１０による認証（ステップＡ５やステップＡ７）の成功後に、通信制御ＩＣ２３とセキュリティチップ２２とに書き込む情報の一部を鍵管理センターサーバ３１０から取得している（ステップＡ６やステップＡ８）。つまり、通信制御ＩＣ用ライター６１０とＳＣ用ライター６５０とは、それぞれ、外部で認証が行われた後に、書き込む情報を取得し、取得した情報を通信制御ＩＣ２３やセキュリティチップ２２に書き込むので、通信制御ＩＣ用ライター６１０とＳＣ用ライター６５０とは、それぞれ、正当なものであるときに、書き込む情報が供給されて前記の書き込みが許可されることになる。このため、通信制御ＩＣ用ライター６１０とＳＣ用ライター６５０とのいずれかについてすり替えが起こったとしても、情報の漏洩のリスクを低減又は無くすことができる。特に、外部での認証の成功後に、書き込む情報が初めて通信制御ＩＣ用ライター６１０やＳＣ用ライター６５０に供給されるので、すり替えられた通信制御ＩＣ用ライター６１０やＳＣ用ライター６５０に書き込む情報が供給されることが防止されたり、チップメーカー６００に納入される前に通信制御ＩＣ用ライター６１０やＳＣ用ライター６５０から、書き込む情報が読み取られることが防止されるので、情報の漏洩のリスクを低減又は無くすことができる。

【０１４３】

なお、変形例として、通信制御ＩＣ用ライター６１０とＳＣ用ライター６５０とは互いに認証を行っても良い。例えば、通信制御ＩＣ用ライター６１０の記憶部６１２及びＳＣ用ライター６５０の記憶部６５２には、認証用情報（例えば、共通の情報であり、認証用情報Ａ１やＢ１を利用してもよい）が格納され、この認証用情報の照合などによって、お互いの認証し、認証成功の場合（照合ＯＫの場合）に、ステップＡ１１の処理を行っても良い。これによって、通信制御ＩＣ用ライター６１０やＳＣ用ライター６５０のすり替えによる情報漏洩などのリスクをさらに低減又は無くすことができる。

【０１４４】
（カードユニット２０の動作確認）
次に、カードユニット２０の動作確認における各装置の動作について図１２を参照して説明する。カードユニットメーカー６００では、カードユニット２０の製造後など、カードユニット２０の製造における所定の段階において、カードユニット２０での処理が正常に行われるか否かを確認する動作確認が行われる。 ここで、カードユニット２０（通信制御ＩＣ２３）は、テスト用のパチンコ機１０（構成は、図２参照）と接続され、動作確認がなされる。
【０１４５】
例えば、カードユニット２０（製造途中のものも含む）の電源を最初に投入した場合、テスト用のパチンコ機１０と接続された場合、カードユニット２０に通常動作用のカードが挿入されていない場合などにおいて、ＣＵ制御部２１などは、動作確認用の動作を行う。なお、ＣＵ制御部２１の記憶部２１ｂには、メーカー情報Ｂ（セキュリティチップ２２に格納されているメーカー情報Ｂと同じ内容である。）、及び、統一店舗コードが予め格納されている（製造時に格納される）。
【０１４６】
統一店舗コードとは、カードユニット２０が出荷される遊技場５００を識別する識別情報（例えば、遊技場５００毎にユニークな情報）などからなるが、この情報は適宜の情報であればよい。
【０１４７】
カードユニット２０の動作確認では、まず、ＣＵ制御部２１は、セキュリティチップ２２と通信を行い、メーカー情報Ｂを相互に照合する（ステップＢ１）。例えば、ＣＵ制御部２１の処理部２１ａは、記憶部２１ｂに格納したメーカー情報Ｂをセキュリティチップ２２に送信する。セキュリティチップ２２の処理部２２ａは、ＣＵ制御部２１から送信されたメーカー情報Ｂを受信し、受信したメーカー情報Ｂと記憶部２２ｂに格納されたメーカー情報Ｂとを照合する。この照合がＮＧであれば、セキュリティチップ２２の処理部２２ａは、その後の処理を中止する。この照合がＯＫであれば、セキュリティチップ２２の処理部２２ａは、記憶部２２ｂに格納されたメーカー情報ＢをＣＵ制御部２１に送信する。ＣＵ制御部２１の処理部２１ａは、セキュリティチップ２２から送信されたメーカー情報Ｂを受信し、受信したメーカー情報Ｂと記憶部２１ｂに格納されたメーカー情報Ｂとを照合する。この照合がＮＧであれば、ＣＵ制御部２１の処理部２１ａは、その後の処理を中止する。この照合がＯＫであれば、相互の認証が成功となり、ＣＵ制御部２１の処理部２１ａは、セキュリティチップ２２に対して接続要求（記憶部２１ｂに格納された統一店舗コードの送信）を行う（ステップＢ２）。
【０１４８】
セキュリティチップ２２の処理部２２ａは、統一店舗コードをＣＵ制御部２１の処理部２１ａから受信すると、この統一店舗コードを保持し、記憶部２２ｂに格納された暗号鍵Ｃ１に基づく相互認証（暗号認証）を行うように試みるが、ＣＵ制御部２１の記憶部２１ｂには暗号鍵Ｃ１が格納されていないので、相互認証は失敗する（ステップＢ３）。この相互認証では、例えば、処理部２２ａと処理部２１ａとが、暗号鍵Ｃ１を用いて正常に暗号通信を行えるかで認証の成功及び失敗が判断される。暗号通信を行うことができれば、認証は成功になり、暗号通信を行うことができなければ、認証は失敗になる。このような認証では、例えば、ＭＡＣ（Message Authentication Code）が用いられる。なお、ＨＭＡＣ(Keyed-Hashing for Message Authentication code)などが用いられても良い。
【０１４９】
セキュリティチップ２２の処理部２２ａは、ステップＢ３で認証が失敗すると、記憶部２２ｂに格納している暗号鍵Ｃ３をＣＵ制御部２１に送信し、ＣＵ制御部２１の処理部２１ａは、受信した暗号鍵Ｃ３を保持（例えば、ＲＡＭに一時記憶されることをいう。以下同じ。）する。（ステップＢ４）。
【０１５０】

ステップＢ４の後、ＣＵ制御部２１の処理部２１ａと、セキュリティチップ２２の処理部２２ａとは、保持している又は記憶部２２ｂに格納しているそれぞれの暗号鍵Ｃ３を用いて、暗号鍵Ｃ３に基づく相互認証（暗号認証）を行う（ステップＢ５）。この相互認証では、例えば、処理部２２ａと処理部２１ａとが、暗号鍵Ｃ３を用いて暗号通信を行えるかで認証の成功及び失敗が判断される。つまり、この相互認証は、暗号鍵Ｃ１に基づく相互認証と同様のものであるので、詳細な説明は上記に準じる。

【０１５１】

上記相互認証が失敗した場合には、処理部２１ａや処理部２２ａは、その後の処理を中止する。上記相互認証が成功した場合、セキュリティチップ２２の処理部２２ａは、ステップＢ６の処理を行う。

【０１５２】

ステップＢ６において、セキュリティチップ２２の処理部２２ａは、認証用情報Ａ２の要求を通信制御ＩＣ２３に送信し、通信制御ＩＣ２３の処理部２３ａは、セキュリティチップ２２からの要求を受信すると、記憶部２３ｂに格納している認証用情報Ａ２をセキュリティチップ２２に送信する。セキュリティチップ２２の処理部２２ａは、通信制御ＩＣ２３から送信された認証用情報Ａ２を受信すると、受信した認証用情報Ａ２と、記憶部２２ｂに格納している認証用情報Ａ２とを照合する。

【０１５３】

認証用情報Ａ２の照合が失敗した場合（認証用情報Ａ２のセキュリティチップ２２への送信が一定時間無い場合なども含む。以下、照合について適宜同じ。）、セキュリティチップ２２の処理部２２ａは、その後の処理を中止する。

【０１５４】

一方、認証用情報Ａ２の照合が成功した場合、ステップＢ７の処理が行われる。ステップＢ７の処理において、セキュリティチップ２２の処理部２２ａは、記憶部２２ｂに格納している認証用情報Ｂ２を照合要求とともに通信制御ＩＣ２３に送信し、通信制御ＩＣ２３の処理部２３ａは、セキュリティチップ２２からの認証用情報Ｂ２及び照合要求を受信すると、記憶部２３ｂに格納している認証用情報Ｂ２と受信した認証用情報Ｂ２とを照合し、照合がＮＧの場合には、その後の処理を中止する。一方で、照合がＯＫの場合には、通信制御ＩＣ２３の処理部２３ａは、その旨をセキュリティチップ２２に通知する。

【０１５５】

通信制御ＩＣ２３の処理部２３ａによる照合ＯＫの通知が行われると、ステップＢ８の処理が行われる。セキュリティチップ２２の処理部２２ａは、通信制御ＩＣ２３から照合ＯＫの通知を受信すると、記憶部２２ｂに格納している認証用情報Ａ１、出荷情報、バージョン情報Ａ１を照合要求とともに通信制御ＩＣ２３に送信し、通信制御ＩＣ２３の処理部２３ａは、セキュリティチップ２２からの認証用情報Ａ１、出荷情報、バージョン情報Ａ１を受信すると、記憶部２３ｂに格納している認証用情報Ａ１、出荷情報、バージョン情報Ａ１と受信した認証用情報Ａ１、出荷情報、バージョン情報Ａ１とをそれぞれ照合し、照合がＮＧの場合（上記情報のうちの１つでも照合がＮＧの場合）には、その後の処理を中止する。一方で、照合がＯＫの場合（上記情報のうちの全ての照合がＯＫの場合）には、通信制御ＩＣ２３の処理部２３ａは、その旨をセキュリティチップ２２に通知する。

【０１５６】

通信制御ＩＣ２３の処理部２３ａによる照合ＯＫの通知が行われると、ステップＢ９の処理が行われる。つまり、セキュリティチップ２２の処理部２２ａと通信制御ＩＣ２３の処理部２３ａとは、各々の記憶部に格納された暗号鍵Ａ１での暗号通信を開始する。

【０１５７】

上記暗号通信を開始すると、セキュリティチップ２２の処理部２２ａは、記憶部２２ｂに格納されている許可情報Ａを暗号鍵Ａ１（記憶部２２ｂに格納されている。）で暗号化し、通信制御ＩＣ２３に送信し、通信制御ＩＣ２３の処理部２３ａは、許可情報Ａを暗号鍵Ａ１（記憶部２２ｂに格納されている。）で復号化し、保持する。この保持によって許可情報Ａが通信制御ＩＣ２３に設定されたことになる（ステップＢ１０）。この設定によ

って、通信制御ＩＣ２３は、初めてステップＢ１１以降の処理を行うことができる。なお、ステップＢ１０において、通信制御ＩＣ２３の処理部２３ａは、許可情報Ａを保持したことを通信制御ＩＣ２３に通知する。

【０１５８】

セキュリティチップ２２の処理部２２ａは、通信制御ＩＣ２３から、許可情報Ａを保持したことの通知を受信すると、通信制御ＩＣ２３に対してチップ情報の要求を行う（ステップＢ１１）。このチップ情報の要求も、許可情報Ａと同様に、暗号鍵Ａ１によって暗号化及び復号化してもよい。

【０１５９】

チップ情報は、本実施形態では、払出制御チップ１１のチップ情報、主制御チップ１３のチップ情報を含む。 払出制御チップ１１のチップ情報は、払出制御チップ１１を識別する識別情報であり、本実施形態では、払出制御チップ１１毎にユニークな数値等からなる。主制御チップ１３のチップ情報は、主制御チップ１３を識別する識別情報であり、本実施形態では、主制御チップ１３毎にユニークな数値等からなる。払出制御チップ１１のチップ情報は、払出制御チップ１１の記憶部１１ｂに予め格納され、主制御チップ１３のチップ情報は、主制御チップ１３の記憶部１１ｂに予め格納されているものとする。

【０１６０】

通信制御ＩＣ２３の処理部２３ａは、セキュリティチップ２２からのチップ情報の要求を受信すると、チップ情報を取得する（ステップＢ１２）。例えば、通信制御ＩＣ２３の処理部２３ａは、テスト用のパチンコ機１０の払出制御チップ１１と通信を行い、チップ情報の要求を送信する。払出制御チップ１１の処理部１１ａは、この要求を受信すると、テスト用のパチンコ機１０の主制御チップ１３に対してチップ情報の送信要求を行う。主制御チップ１３の処理部１３ａは、この要求を受信すると、記憶部１３ｂに格納されている主制御チップ１３１のチップ情報を払出制御チップ１１に送信する。払出制御チップ１１の処理部１１ａは、主制御チップ１３のチップ情報を受信すると、記憶部１１ｂに格納されている払出制御チップ１１のチップ情報を、受信した主制御チップ１３のチップ情報とともに、通信制御ＩＣ２３に返信する。これによって、通信制御ＩＣ２３の処理部２３ａは、チップ情報を受信することで、チップ情報を取得する。チップ情報は、処理部２３ａに保持される。

【０１６１】

通信制御ＩＣ２３の処理部２３ａは、ステップＢ１２で取得したチップ情報からチップ番号を生成する（ステップＢ１３）。例えば、処理部２３ａは、チップ情報と、予め設定された所定の値や記憶部２３ｂに格納されている所定の情報などと、を論理演算して、チップ番号を生成する。 チップ番号は、例えば、払出制御チップ１１のチップ情報、主制御チップ１３のチップ情報毎に生成される。チップ番号及びチップ情報は、処理部２３ａに保持される。

【０１６２】

通信制御ＩＣ２３の処理部２３ａは、保持しているチップ情報及びチップ番号を記憶部２３ｂに格納されている暗号鍵Ａ１で暗号化して、セキュリティチップ２２に送信し、セキュリティチップ２２の処理部２２ａは、チップ情報及びチップ番号を受信すると、記憶部２２ｂに格納されている暗号鍵Ａ１で復号化し保持する（ステップＢ１４）。

【０１６３】

次に、セキュリティチップ２２の処理部２２ａは、保持するチップ番号などからチップ問合せ番号を自動生成し、保持する（ステップＢ１４．５）。チップ問合せ番号は例えば、チップ番号と、現在の日時（例えば、処理部２２ａは図示しないカレンダ部を参照して現在の日時を特定する。）などと、を論理演算することによって生成される（必要に応じて、認証用情報Ｃ２などが用いられてもよい）。

【０１６４】

次に、セキュリティチップ２２の処理部２２ａは、保持するチップ情報とチップ問合わせ番号とを記憶部２２ｂに格納されている秘匿鍵Ｂで暗号化し、暗号化されたチップ情報

とチップ問合わせ番号とをさらに、処理部２２ａが保持するチップ番号とともに、記憶部２２ｂに格納されている暗号鍵Ｃ３で暗号化し、ＣＵ制御部２１に送信する（ステップＢ１５）。

【０１６５】

ＣＵ制御部２１の処理部２１ａは、セキュリティチップ２２からのチップ情報とチップ問合わせ番号とチップ番号とを記憶部２１ｂに格納されている暗号鍵Ｃ３で復号化し、復号化した情報を保持するとともに（チップ情報とチップ問合わせ番号とは、秘匿鍵Ｂで暗号化されたままである。）、チップ情報がない旨の通知をセキュリティチップ２２に返信する（ステップＢ１６）。

【０１６６】

次に、セキュリティチップ２２の処理部２２ａは、ＣＵ制御部２１からのチップ情報がない旨の通知を受信すると、以降の処理を続けるために、認証ＯＫの情報を通信制御ＩＣ２３に送信し、通信制御ＩＣ２３の処理部２３ａは、認証ＯＫの情報をセキュリティチップ２２から受信すると、この情報を保持する（ステップＢ１７）。この保持によって、処理部２３ａは、下記のセッション鍵を生成できる。

【０１６７】

次に、セキュリティチップ２２の処理部２２ａは、セッション鍵の要求を通信制御ＩＣ２３に送信し（ステップＢ１８）、通信制御ＩＣ２３の処理部２３ａは、セッション鍵の要求をセキュリティチップ２２から受信すると、セッション鍵を自動生成する（ステップＢ１８．５）。例えば、処理部２２ａは、乱数生成回路を備え、乱数生成回路が生成した乱数に基づいてセッション鍵を生成する。例えば、前記乱数と所定の情報（例えば、記憶部２３ｂに格納されている情報）とを論理演算し、セッション鍵を生成してもよい。

【０１６８】

通信制御ＩＣ２３の処理部２３ａは、生成したセッション鍵を保持するとともに、生成したセッション鍵をセキュリティチップ２２に通知する（ステップＢ１９）。セキュリティチップ２２の処理部２２ａは、通信制御ＩＣ２３からのセッション鍵を受信すると、処理部２２ａと処理部２３ａとは、遊技に係る処理を行うための情報（業務電文等）の送受信を行うが、この送受信のときに、送受信する情報をセッション鍵で暗号化及び復号化することで、処理部２２ａと処理部２３ａとは、暗号通信を行う（ステップＢ２０）。

【０１６９】

以上のような一連の処理によって、カードユニット２０の動作確認を効率良く行うことができる。なお、照合ＮＧや、相互認証の失敗などによって、処理が中止されることなどによって、カードユニット２０の動作確認開始から一定時間経過してもカードユニット２０が通常の動作（遊技に係る処理を行うための情報（業務電文等）の送受信）に移行しない場合には、カードユニット２０は動作不良であることが分かる。なお、上記で各処理部に保持されている情報は、動作確認後の電源ＯＦＦにともなって、失われるか（クリアされるか）適宜消去される。また、ＣＵ制御部２１に格納されている統一店舗コードも失われる又は消去される。

【０１７０】

（パチンコ機１０及びカードユニット２０の遊技場５００新規設置時）

カードユニットメーカー６００が製造したカードユニット２０と、遊技機メーカーが製造したパチンコ機１０とは、出荷先の遊技場５００に新規設置されることになる。このとき、遊技用システム１は、カードユニット２０のＣＵ制御部２１、セキュリティチップ２２（セキュリティ基板２４）、通信制御ＩＣ２３の認証、パチンコ機１０の払出制御チップ１１、主制御チップ１３の認証を行うための動作を行う。この動作について、図１３から図１６を参照して説明する。なお、下記の処理は、新規設置された、複数のカードユニット２０及び複数のパチンコ機１０それぞれについて行われる。

【０１７１】

ＣＵ制御部２１の処理部２１ａは、カードユニット２０に通常動作用のカードが挿入され、カードユニット２０の電源が投入されたことを契機として（この時、パチンコ機１０

の電源も投入されるものとする。）、図１３に示すように、上位サーバ５１０との接続を要求する接続要求を上位サーバ５１０へ送信する（ステップＣ１）。

【０１７２】

上位サーバ５１０の制御部５１１は、処理部２１ａからの接続要求を受信すると、記憶部５１２に格納されている許可情報Ｂ（秘匿鍵Ａで暗号化されたままである。）と統一店舗コード（適宜のタイミングで記憶部５１２に格納される。）と暗号鍵Ｃ１とをＣＵ制御部２１に送信し、ＣＵ制御部２１の処理部２１ａは受信したこれら情報を保持する（ステップＣ２）。このように、ＣＵ制御部２１は、上位サーバ５１０と通信を確立することにより許可情報Ｂを取得するため、許可情報Ｂは、適したタイミングでＣＵ制御部２１に送信されるので、セキュリティが確保されている。

【０１７３】

なお、ステップＣ２の許可情報Ｂ等の送信前において、ＣＵ制御部２１と制御部５１１とは相互認証を行っても良い。この場合、例えば、記憶部２１ｂ及び記憶部５１２には、予め、認証用の情報が格納されており、ＣＵ制御部２１と制御部５１１とは、それぞれ、記憶部２１ａと記憶部５１２とのそれぞれに格納されている認証用の情報をやり取りして照合することによって相互認証を行う。相互認証が成功した場合にのみ、前記送信を行うことによって、特に、有効鍵（商用）の送信について、セキュリティが確保される。

【０１７４】

ステップＣ２の後、ＣＵ制御部２１の処理部２１ａは、セキュリティチップ２２の処理部２２ａと通信を行い、メーカー情報Ｂを相互に照合する（ステップＣ３）。例えば、ＣＵ制御部２１の処理部２１ａは、記憶部２１ｂに格納したメーカー情報Ｂをセキュリティチップ２２に送信する。セキュリティチップ２２の処理部２２ａは、ＣＵ制御部２１から送信されたメーカー情報Ｂを受信し、受信したメーカー情報Ｂと記憶部２２ｂに格納されたメーカー情報Ｂとを照合する。この照合がＮＧであれば、セキュリティチップ２２の処理部２２ａは、その後の処理を中止する。この照合がＯＫであれば、セキュリティチップ２２の処理部２２ａは、記憶部２２ｂに格納されたメーカー情報ＢをＣＵ制御部２１に送信する。ＣＵ制御部２１の処理部２１ａは、セキュリティチップ２２から送信されたメーカー情報Ｂを受信し、受信したメーカー情報Ｂと記憶部２１ｂに格納されたメーカー情報Ｂとを照合する。この照合がＮＧであれば、ＣＵ制御部２１の処理部２１ａは、その後の処理を中止する。この照合がＯＫであれば、ＣＵ制御部２１とセキュリティチップ２２とは、相互に認証が成功したことになるので、ＣＵ制御部２１の処理部２１ａは、セキュリティチップ２２に対して接続要求（保持されている統一店舗コードの送信）を行う（ステップＣ４）。

【０１７５】

セキュリティチップ２２の処理部２２ａは、統一店舗コードをＣＵ制御部２１から受信すると、記憶部２２ｂに格納された暗号鍵Ｃ１に基づく相互認証（暗号認証）を行う（ステップＣ５）。この相互認証では、例えば、処理部２２ａと処理部２１ａとが、暗号鍵Ｃ１を用いて暗号通信を正常に行えるかで認証の成功及び失敗が判断される。処理部２２ａは、記憶部２２ｂに格納されている暗号鍵Ｃ１を用い、処理部２１ａは、保持している暗号鍵Ｃ１を用いて処理を行う。暗号鍵Ｃ１を用いて暗号通信を行うことができれば、認証は成功になり、暗号通信を行うことができなければ、認証は失敗になる。このような認証では、例えば、ＭＡＣが用いられる。なお、ＨＭＡＣなどが用いられても良い。

【０１７６】

相互認証が失敗だった場合には、セキュリティチップ２２の処理部２２ａは、処理を中止する。相互認証が成功だった場合には、セキュリティチップ２２の処理部２２ａは、保持している統一店舗コードと、記憶部２２ｂに格納された日時及び認証用情報Ｃ２と、に基づいて、基板問合せ番号を生成し、保持する（ステップＣ６）。例えば、処理部２２ａは、乱数生成回路を備え、乱数生成回路が生成した乱数と、統一店舗コードと、日時と、認証用情報Ｃ２とを論理演算し、基板問合せ番号を生成するか、統一店舗コードと、日時と、認証用情報Ｃ２とを論理演算して基板問合せ番号を生成する。

【０１７７】
セキュリティチップ２２の処理部２２ａは、ステップＣ６に続いて、基板問合せ番号を記憶部２２ｂに格納されている秘匿鍵Ｂで暗号化し、暗号化した基板問合せ番号を認証用情報Ｃ１とともに記憶部２２ｂに格納されている暗号鍵Ｃ１でさらに暗号化し、暗号化した情報をＣＵ制御部２１に送信する（ステップＣ７）。また、ステップＣ７において、ＣＵ制御部２１の処理部２１ａは、前記暗号化した情報を受信すると、記憶部２１ｂに格納した暗号鍵Ｃ１で、受信した情報を復号し、復号した基板問合せ番号（秘匿鍵Ｂで暗号化されたままである。）と認証用情報Ｃ１とを保持する。
【０１７８】
続いて、ＣＵ制御部２１の処理部２１ａは、情報要求とともに、基板問合せ番号（秘匿鍵Ｂで暗号化されたままである。）と認証用情報Ｃ１とを上位サーバ５１０に送信し、上位サーバ５１０の制御部５１１は、情報要求とともに、基板問合せ番号（秘匿鍵Ｂで暗号化されたままである。）と認証用情報Ｃ１とを受信すると、これら情報を保持する（ステップＣ８）。
【０１７９】
続いて、上位サーバ５１０の制御部５１１は、情報要求とともに、基板問合せ番号（秘匿鍵Ｂで暗号化されたままである。）と認証用情報Ｃ１とを鍵管理センターサーバ３１０に送信し、鍵管理センターサーバ３１０の制御部５１１は、情報要求とともに、基板問合せ番号（秘匿鍵Ｂで暗号化されたままである。）と認証用情報Ｃ１とを受信すると、基板問合せ番号を記憶部３１２に格納された秘匿鍵Ｂで復号し、これら情報を保持する（ステップＣ９）。
【０１８０】
続いて、鍵管理センターサーバ３１０の制御部５１１は、保持している認証用情報Ｃ１と同じ情報が記憶部５１２に格納されているかを検索し、同じ情報が格納されていない場合には、その旨を上位サーバ５１０に送信する。上位サーバ５１０の処理部５１１は、格納されていない旨の情報を受信すると、入出力部５１３等を介して、所定の報知処理（例えば入出力部５１３に含まれる表示部への照合ＮＧの旨の表示、入出力部５１３に含まれるブザーを鳴らす等。以下制御部５１１が行う所定の報知処理について同じ。）を行う。同じ情報が格納されている場合には、鍵管理センターサーバ３１０の制御部３１１は、適宜、検索された認証用情報Ｃ１に対応付けて、復号化した基板問合せ番号を記憶部３１２に格納するとともに、検索された認証用情報Ｃ１と、この認証用情報Ｃ１に対応付けられて記憶部３１２に格納されている、基板問合せ番号と、認証用情報Ｃ２と、バージョン情報Ｃと、暗号鍵Ｃ２と、認証用情報Ａ１と、出荷情報と、バージョン情報Ａ２と、更新情報と、を上位サーバ５１０に送信する（ステップＣ１０）。なお、このとき、制御部３１１は、基板問合せ番号と、認証用情報Ａ１と、出荷情報と、バージョン情報Ａ２と、更新情報と、を、記憶部３１２で格納された秘匿鍵Ｂでそれぞれ暗号化して送信する。
【０１８１】
上位サーバ５１０の制御部５１１は、鍵管理センターサーバ３１０からの情報を受信すると、これら情報を保持して、そのまま（秘匿鍵Ｂで暗号化されたものは、暗号化されたまま）、ＣＵ制御部２１に送信する（ステップＣ１１）。
【０１８２】
ＣＵ制御部２１の処理部２１ａは、上位サーバ５１０からの情報を受信すると、これら情報を保持し、セキュリティチップ２２の処理部２２ａと通信を行い、認証用情報Ｃ２を相互に照合する（ステップＣ１２）。例えば、ＣＵ制御部２１の処理部２１ａは、保持している認証用情報Ｃ２をセキュリティチップ２２に送信する。セキュリティチップ２２の処理部２２ａは、ＣＵ制御部２１から送信された認証用情報Ｃ２を受信し、受信した認証用情報Ｃ２と記憶部２２ｂに格納された認証用情報Ｃ２とを照合する。この照合がＮＧの場合は処理が中止される。この照合がＯＫであれば、セキュリティチップ２２の処理部２２ａは、記憶部２２ｂに格納された認証用情報Ｃ２をＣＵ制御部２１に送信する。ＣＵ制御部２１の処理部２１ａは、セキュリティチップ２２から送信された認証用情報Ｃ２を受

信し、受信した認証用情報Ｃ２と保持している認証用情報Ｃ２とを照合する。この照合がＮＧの場合は処理が中止される。

【０１８３】

前記照合がＯＫであれば、相互認証が成功したことになるので、ＣＵ制御部２１の処理部２１ａは、セキュリティチップ２２の処理部２２ａと再度通信を行い、バージョン情報Ｃを相互に照合する（ステップＣ１３）。例えば、ＣＵ制御部２１の処理部２１ａは、保持しているバージョン情報Ｃをセキュリティチップ２２に送信する。セキュリティチップ２２の処理部２２ａは、ＣＵ制御部２１から送信されたバージョン情報Ｃを受信し、受信したバージョン情報Ｃと記憶部２２ｂに格納されたバージョン情報Ｃとを照合する。この照合がＮＧの場合は処理が中止される。この照合がＯＫであれば、セキュリティチップ２２の処理部２２ａは、記憶部２２ｂに格納されたバージョン情報ＣをＣＵ制御部２１に送信する。ＣＵ制御部２１の処理部２１ａは、セキュリティチップ２２から送信されたバージョン情報Ｃを受信し、受信したバージョン情報Ｃと保持しているバージョン情報Ｃとを照合する。この照合がＮＧの場合は処理が中止される。

【０１８４】

前記照合がＯＫであれば、ＣＵ制御部２１の処理部２１ａは、保持している暗号鍵Ｃ２を保持している暗号鍵Ｃ１で暗号化し、セキュリティチップ２２に送信し、セキュリティチップ２２の処理部２２ａは、暗号鍵Ｃ２を受信すると、受信した暗号鍵Ｃ２を記憶部２２ｂに格納されている暗号鍵Ｃ１で復号化し、保持する。これ以降、処理部２１ａと処理部２２ａとは、暗号鍵Ｃ２を用いた暗号通信を開始する（ステップＣ１４）。

【０１８５】

続いて、ＣＵ制御部２１の処理部２１ａは、保持している、暗号化されたままの状態の、基板問合せ番号と、認証用情報Ａ１と、出荷情報と、バージョン情報Ａ２と、更新情報と、許可情報Ｂと、を、さらに、暗号鍵Ｃ２で暗号化してセキュリティチップ２２に送信する（ステップＣ１５）。

【０１８６】

セキュリティチップ２２の処理部２２ａは、前記情報をＣＵ制御部２１から受信すると、まず、記憶部２２ｂに格納された暗号鍵Ｃ２で復号化し、さらに、基板問合せ番号と、認証用情報Ａ１と、出荷情報と、バージョン情報Ａ２と、更新情報と、を記憶部２２ｂに格納された秘匿鍵Ｂで復号化し、保持する。そして、処理部２２ａは、復号化した基板問合せ番号と、保持している基板問合せ番号とを比較し、両者が同じなら、さらに、復号化した認証用情報Ａ１及び出荷情報と、記憶部２２ｂに格納された認証用情報Ａ１及び出荷情報とを照合し、全て照合ＯＫなら、復号化した更新情報に基づいて、暗号鍵Ａ２を生成し、保持する（ステップＣ１６）。例えば、更新情報に現在の日付（所定のカレンダ部を参照して得られる。）を論理演算し、暗号鍵Ａ２を生成する。基板問合せ番号が同じでない（基板問合せ番号とともに送信された情報が真性の情報でない可能性がある）、又は、前記の照合がすべてＯＫでない場合には、処理部２２ａは、は処理を中止する。

【０１８７】

次に、セキュリティチップ２２の処理部２２ａは、通信制御ＩＣ２３に対して、バージョン情報Ａ２を要求する。通信制御ＩＣ２３の処理部２３ａは、バージョン情報Ａ２を保持又は記憶部２３ｂに格納していれば、そのバージョン情報Ａ２をセキュリティチップ２２に送信し、保持又は格納されていなければ、その旨をセキュリティチップ２２に送信する。ここでは、保持又は格納されていない旨が送信される。セキュリティチップ２２の処理部２２ａは、通信制御ＩＣ２３から送信された、保持又は格納されていない旨を受信すると、暗号情報Ａ２が更新されていない（最新の暗号情報Ａ２が保持又は格納されていない）と判定する。また、セキュリティチップ２２の処理部２２ａは、通信制御ＩＣ２３から送信されたバージョン情報Ａ２を受信すると、受信したバージョン情報Ａ２と復号化したバージョン情報Ａ２とを比較して異なっていれば、暗号情報Ａ２が更新されていないと判定する。このように、セキュリティチップ２２の処理部２２ａは、バージョン情報Ａ２の更新確認を行う（ステップＣ１７）。なお、両者が同じであれば、暗号情報Ａ２が更新

されている（つまり、通信制御ＩＣ２３には最新の暗号情報Ａ２が設定されている）と判定し、セキュリティチップ２２の処理部２２ａは、ステップＣ２１からの処理を行う。なお、ステップＣ１７からステップＣ２４までの間、セキュリティチップ２２の処理部２２ａと通信制御ＩＣ２３の処理部２３ａとは、適宜、それぞれの記憶部２２ｂ、２３ｂに格納された暗号鍵Ａ１でやり取りする情報を暗号化及び復号化するものとする。

【０１８８】

ステップＣ１７で、暗号情報Ａ２が更新されていないと判定した場合、セキュリティチップ２２の処理部２２ａは、復号化した更新情報及びバージョン情報Ａ２を通信制御ＩＣ２３に送信する（ステップＣ１８）。

【０１８９】

通信制御ＩＣ２３の処理部２３ａは、セキュリティチップ２２から送信された更新情報及びバージョン情報Ａ２を受信すると、受信した更新情報に基づいて、暗号鍵Ａ２を生成し、保持する（ステップＣ１９）。例えば、暗号鍵Ａ２は、ステップＣ１６での生成と同じロジックで生成される。これによって、通信制御ＩＣ２３とセキュリティチップ２２とで同じ暗号鍵Ａ２が生成されるので、暗号鍵Ａ２に基づく暗号通信が実現される。また、暗号鍵Ａ２のバージョンを表すバージョン情報Ａ２も通信制御ＩＣ２３とセキュリティチップ２２とで共通になる。暗号鍵Ａ２は、例えば、上記同様、更新情報と、現在の日付（所定のカレンダ部を参照して得られる。）と、を論理演算して生成される。

【０１９０】

通信制御ＩＣ２３の処理部２３ａは、上記暗号情報Ａ２を生成すると、暗号情報Ａ２の更新完了をセキュリティチップ２２に通知する（ステップＣ２０）。セキュリティチップ２２の処理部２２ａは、通信制御ＩＣ２３から更新完了の通知を受信すると、セキュリティチップ２２の処理部２２ａは、認証用情報Ａ２の要求を通信制御ＩＣ２３に送信し、通信制御ＩＣ２３の処理部２３ａは、セキュリティチップ２２からの要求を受信すると、記憶部２３ｂに格納している認証用情報Ａ２をセキュリティチップ２２に送信する。セキュリティチップ２２の処理部２２ａは、通信制御ＩＣ２３から送信された認証用情報Ａ２を受信すると、受信した認証用情報Ａ２と、記憶部２２ｂに格納している認証用情報Ａ２とを照合する（ステップＣ２１）。

【０１９１】

認証用情報Ａ２の照合が失敗した場合（認証用情報Ａ２のセキュリティチップ２２への送信が一定時間無い場合なども含む。）、セキュリティチップ２２の処理部２２ａは、その後の処理を中止する。

【０１９２】

一方、認証用情報Ａ２の照合が成功した場合、ステップＣ２２の処理が行われる。ステップＣ２２の処理において、セキュリティチップ２２の処理部２２ａは、記憶部２２ｂに格納している認証用情報Ｂ２を照合要求とともに通信制御ＩＣ２３に送信し、通信制御ＩＣ２３の処理部２３ａは、セキュリティチップ２２からの認証用情報Ｂ２及び照合要求を受信すると、記憶部２３ｂに格納している認証用情報Ｂ２と受信した認証用情報Ｂ２とを照合し、照合がＮＧの場合には、その後の処理を中止する。一方で、照合がＯＫの場合には、通信制御ＩＣ２３の処理部２３ａは、その旨をセキュリティチップ２２に通知する。

【０１９３】

通信制御ＩＣ２３の処理部２３ａによる照合ＯＫの通知が行われると、ステップＣ２３の処理が行われる。セキュリティチップ２２の処理部２２ａは、通信制御ＩＣ２３から照合ＯＫの通知を受信すると、記憶部２２ｂに格納している認証用情報Ａ１、出荷情報、保持しているバージョン情報Ａ２を照合要求とともに通信制御ＩＣ２３に送信し、通信制御ＩＣ２３の処理部２３ａは、セキュリティチップ２２からの認証用情報Ａ１、出荷情報、バージョン情報Ａ２を受信すると、記憶部２３ｂに格納している認証用情報Ａ１、出荷情報、保持しているバージョン情報Ａ１と受信した認証用情報Ａ１、出荷情報、バージョン情報Ａ１とをそれぞれ照合し、照合がＮＧの場合（上記情報のうちの１つでも照合がＮＧの場合）には、その後の処理を中止する。一方で、照合がＯＫの場合（上記情報のうちに

ついての全ての照合がＯＫの場合）には、通信制御ＩＣ２３の処理部２３ａは、その旨をセキュリティチップ２２に通知する。

【０１９４】

通信制御ＩＣ２３の処理部２３ａによる照合ＯＫの通知が行われると、ステップＣ２４の処理が行われる。つまり、セキュリティチップ２２の処理部２２ａと通信制御ＩＣ２３の処理部２３ａとは、各々で保持する暗号鍵Ａ２での暗号通信を開始する。

【０１９５】

上記暗号通信を開始すると、セキュリティチップ２２の処理部２２ａは、保持している許可情報Ｂを、保持している暗号鍵Ａ２で暗号化し、通信制御ＩＣ２３に送信し、通信制御ＩＣ２３の処理部２３ａは、受信した許可情報Ｂを、保持している暗号鍵Ａ２で復号化し、さらに、記憶部２３ｂに格納されている秘匿鍵Ａで復号化され、保持される。この保持によって許可情報Ｂが通信制御ＩＣ２３に設定されたことになる（ステップＣ２５）。この設定によって、通信制御ＩＣ２３は、初めてステップＣ２６以降の処理を行うことができる。なお、ステップＣ２５において、通信制御ＩＣ２３の処理部２３ａは、許可情報Ａを保持したことを通信制御ＩＣ２３に通知する。ここで、許可情報Ｂは、通信制御ＩＣ２３で初めて復号化される。つまり、途中の装置では復号化されない。これによって、許可情報Ｂの秘匿性が担保されることになる。また、このような許可情報Ｂの設定によって、初めてステップＣ２６以降の処理が行われるので、例えば、通信制御ＩＣ２３を不用意に不正使用されることが抑制される。

【０１９６】

セキュリティチップ２２の処理部２２ａは、通信制御ＩＣ２３から許可情報Ｂを保持したことの通知を受信すると、通信制御ＩＣ２３に対してチップ情報の要求を行う（ステップＣ２６）。このチップ情報の要求も、許可情報Ａと同様に、暗号鍵Ａ２によって暗号化及び復号化してもよい。

【０１９７】

チップ情報は、上記同様、払出制御チップ１１のチップ情報、主制御チップ１３のチップ情報を含む。 払出制御チップ１１のチップ情報は、払出制御チップ１１を識別する識別情報であり、本実施形態では、払出制御チップ１１毎にユニークな数値等からなる。主制御チップ１３のチップ情報は、主制御チップ１３を識別する識別情報であり、本実施形態では、主制御チップ１３毎にユニークな数値等からなる。払出制御チップ１１のチップ情報は、払出制御チップ１１の記憶部１１ｂに予め格納され、主制御チップ１３のチップ情報は、主制御チップ１３の記憶部１１ｂに予め格納されているものとする。

【０１９８】

通信制御ＩＣ２３の処理部２３ａは、セキュリティチップ２２からのチップ情報の要求を受信すると、チップ情報を取得する（ステップＣ２７）。例えば、通信制御ＩＣ２３の処理部２３ａは、パチンコ機１０の払出制御チップ１１と通信を行い、チップ情報の要求を送信する。払出制御チップ１１の処理部１１ａは、この要求を受信すると、パチンコ機１０の主制御チップ１３に対してチップ情報の送信要求を行う。主制御チップ１３の処理部１３ａは、この要求を受信すると、記憶部１３ｂに格納されている主制御チップ１３１のチップ情報を払出制御チップ１１に送信する。払出制御チップ１１の処理部１１ａは、主制御チップ１３のチップ情報を受信すると、記憶部１１ｂに格納されている払出制御チップ１１のチップ情報を、受信した主制御チップ１３のチップ情報とともに、通信制御ＩＣ２３に返信する。これによって、通信制御ＩＣ２３の処理部２３ａは、チップ情報を受信することで、チップ情報を取得する。チップ情報は、処理部２３ａに保持される。

【０１９９】

通信制御ＩＣ２３の処理部２３ａは、ステップＢ１２で取得したチップ情報からチップ番号を生成する（ステップＣ２８）。例えば、処理部２３ａは、チップ情報と、所定の情報（例えば、認証用情報Ｃ２）などと、を論理演算して、チップ番号を生成する。 チップ番号は、例えば、払出制御チップ１１のチップ情報、主制御チップ１３のチップ情報毎に生成される。チップ番号及びチップ情報は、処理部２３ａに保持される。

【０２００】
なお、チップ情報（ステップＣ２６で取得されるチップ情報と同じチップ情報）は、予め適宜のタイミングで、チップ番号とともに、両者が対応付けられて（払出制御チップ１１のチップ情報、主制御チップ１３のチップ情報毎に対応付けられて）、鍵管理センターサーバ３１０の記憶部３１２に格納されているものとする。チップ番号は、ステップＣ２７と同じロジックで生成される。例えば、制御部３１１は、上記と同様に、チップ情報と、所定の情報（例えば、認証用情報Ｃ２）などと、を論理演算して、チップ番号を生成する。従って、チップ情報が同じであれば、チップ番号も同じになる。
【０２０１】
通信制御ＩＣ２３の処理部２３ａは、保持しているチップ情報及びチップ番号を暗号鍵Ａ２で暗号化して、セキュリティチップ２２に送信し、セキュリティチップ２２の処理部２２ａは、チップ情報及びチップ番号を受信すると暗号鍵Ａ２で復号化し保持する（ステップＣ２９）。
【０２０２】
次に、セキュリティチップ２２の処理部２２ａは、保持するチップ番号などからチップ問合せ番号を自動生成し、保持する（ステップＣ３０）。チップ問合せ番号は例えば、チップ番号と、現在の日時（例えば、処理部２２ａは図示しないカレンダ部を参照して現在の日時を特定する。）などと、を論理演算することによって生成される（必要に応じて、認証用情報Ｃ２などが用いられてもよい）。
【０２０３】
次に、セキュリティチップ２２の処理部２２ａは、保持するチップ情報とチップ問合わせ番号とを記憶部２２ｂに格納されている秘匿鍵Ｂでそれぞれ暗号化し、暗号化されたチップ情報とチップ問合わせ番号とをさらに、処理部２２ａが保持するチップ番号とともに、保持している暗号鍵Ｃ２で暗号化し、ＣＵ制御部２１に送信する（ステップＣ３１）。
【０２０４】
ＣＵ制御部２１の処理部２１ａは、セキュリティチップ２２からのチップ情報とチップ問合わせ番号とチップ番号とを保持している暗号鍵Ｃ２で復号化し、復号化した情報を保持するとともに（チップ情報とチップ問合わせ番号とは、秘匿鍵Ｂで暗号化されたままである。）、復号化した各情報を上位サーバ５１０に送信する（ステップＣ３２）。
【０２０５】
上位サーバ５１０の制御部５１１は、ＣＵ制御部２１から送信された各情報（チップ情報とチップ問合わせ番号とは、秘匿鍵Ｂで暗号化されたままである。）を受信すると、受信した各情報をそのまま、対応付けて保持するとともに、鍵管理センターサーバ３１０に送信する（ステップＣ３３）。
【０２０６】
鍵管理センターサーバ３１０の制御部３１１は、上位サーバ５１０から送信された各情報（チップ情報とチップ問合わせ番号とは、秘匿鍵Ｂで暗号化されたままである。）を受信すると、チップ情報とチップ問合わせ番号とを、記憶部３１２に格納された秘匿鍵Ｂ（鍵管理センターサーバ３１０の制御部３１１は、上位サーバ５１０との情報の送受信の際に、一度、秘匿鍵Ｂを用いると、その上位サーバ５１０から送られてきた情報については、その秘匿鍵Ｂで復号化を行うものとする。）で復号するとともに、前記各情報のうちのチップ番号と同じチップ番号を記憶部３１２から検索し、検索したチップ番号に対応付けられたチップ情報と、復号したチップ情報とを照合し、照合結果を生成する（ステップＣ３４）。なお、同じチップ番号が１つでも検索出来なかった場合であっても照合結果はＮＧとなる。また、チップ情報に含まれる少なくとも１つが照合ＮＧであれば、照合結果はＮＧになる。同じチップ番号が全て検索出来て、チップ情報が全て照合ＯＫであれば、照合結果はＯＫになる。
【０２０７】
鍵管理センターサーバ３１０の制御部３１１は、照合結果とチップ問合わせ番号とを、検索されたチップ番号及び照合されたチップ情報に対応付けて記憶部３１２に格納すると

ともに（パチンコ機１０毎に格納されることになる。）、照合結果とチップ問合せ番号とチップ番号とを上位サーバ５１０に送信する（ステップＣ３５）。このとき、制御部３１１は、照合結果とチップ問合せ番号とを秘匿鍵Ｂで暗号化して送信する。

【０２０８】

上位サーバ５１０の制御部５１１は、鍵管理センターサーバ３１０から送信された各情報と、ステップＣ３３で保持したチップ情報とを対応付けて、記憶部５１２に格納するとともに（パチンコ機１０毎に格納されることになる。）、鍵管理センターサーバ３１０から送信された各情報をそのまま、ＣＵ制御部２１に送信する（ステップＣ３６）。なお、記憶部５１２に格納される情報のうち、照合結果とチップ問合せ番号とチップ情報とは、秘匿鍵Ｂで暗号化されたままである。

【０２０９】

ＣＵ制御部２１の処理部２１ａは、上位サーバ５１０から送信された各情報と、ステップＣ３２で保持したチップ情報とを対応付けて、保持するとともに、上位サーバ５１０から送信された各情報を保持している暗号鍵Ｃ２で暗号化し、セキュリティチップ２２に送信する（ステップＣ３７）。なお、処理部２１ａで保持される情報のうち、照合結果とチップ問合せ番号とチップ情報とは、秘匿鍵Ｂで暗号化されたままである。

【０２１０】

セキュリティチップ２２の処理部２２ａは、ＣＵ制御部２１から送信された各情報をまず、保持している暗号鍵Ｃ２で復号するとともに、復号した各情報のうち、照合結果とチップ問合せ番号とチップ情報とを記憶部２２ｂに格納されている秘匿鍵Ｂで復号化する。そして、ステップＳ３０で生成し保持しているチップ問合せ番号と、復号化したチップ問合せ番号とを比較し、同じである場合に、照合結果を取り込む（保持する）。これにより、セキュリティチップ２２の処理部２２ａは、照合結果とチップ問合せ番号とチップ情報とチップ番号とを保持する。両チップ問合せ番号が異なる場合には、照合結果が不正に操作されている可能性があるので、その後の処理を中止する。

【０２１１】

セキュリティチップ２２の処理部２２ａは、照合結果がＮＧであれば、その後の処理を中止し、照合結果がＯＫであれば、パチンコ機１０の各チップの認証ＯＫの旨の認証結果を通信制御ＩＣ２３に送信する（ステップＣ３８）。この認証結果は、通信制御ＩＣ２３の処理部２３ａで保持される。通信制御ＩＣ２３は、認証ＯＫの旨の認証結果を保持することで、下記のセッション鍵の生成が可能になる。

【０２１２】

次に、セキュリティチップ２２の処理部２２ａは、セッション鍵の要求を通信制御ＩＣ２３に送信し（ステップＣ３９）、通信制御ＩＣ２３の処理部２３ａは、セッション鍵の要求をセキュリティチップ２２から受信すると、セッション鍵を自動生成する（ステップＣ４０）。例えば、処理部２２ａは、乱数生成回路を備え、乱数生成回路が生成した乱数に基づいてセッション鍵を生成する。例えば、前記乱数と所定の情報（例えば、記憶部２３ｂに格納されている情報）とを論理演算し、セッション鍵を生成してもよい。

【０２１３】

通信制御ＩＣ２３の処理部２３ａは、生成したセッション鍵を保持するとともに、生成したセッション鍵をセキュリティチップ２２に通知する（ステップＣ４１）。セキュリティチップ２２の処理部２２ａは、通信制御ＩＣ２３からのセッション鍵を受信すると、処理部２２ａと処理部２３ａとは、遊技に係る処理を行うための情報（業務電文等）の送受信（例えば、ＣＵ制御部２１とパチンコ機の払出制御チップ１１とが行う玉貸処理における業務電文のやりとりの中継での情報の送受信）を行うが、この送受信のときに、送受信する情報をセッション鍵で暗号化及び復号化することで、処理部２２ａと処理部２３ａとは、暗号通信を行う（ステップＣ４２）。

【０２１４】

上記処理では、照合ＮＧ（認証の失敗）や、相互認証の失敗などによって、処理が中止されるなどするので、カードユニット２０の動作確認開始から一定時間経過してもカード

ユニット２０が通常の動作（遊技に係る処理を行うための情報（業務電文等）の送受信など）に移行しない場合には、パチンコ機１０の主制御チップ１３や払出制御チップ１１、カードユニット２０のセキュリティチップ２２、通信制御ＩＣ２３、ＣＵ制御部２１などについて、すり替えなどがあった可能性があり、カードユニット２０が通常の動作に移行しないことによって、すり替えの可能性を報知出来る。なお、ＣＵ制御部２１などは、照合ＮＧだった場合に、カードユニット２０のランプを点灯させるなどして、照合ＮＧの旨を報知するようにしても良い。ステップＣ３、Ｃ５、Ｃ１２、Ｃ１３、Ｃ１４などでの照合ＮＧの場合には、カードユニット２０のＣＵ制御部２１の認証に失敗したことになり、ステップＣ３、Ｃ５、Ｃ１２、Ｃ１３、Ｃ１４、Ｃ２２、Ｃ２３などでの照合ＮＧの場合には、セキュリティチップ２２（セキュリティ基板２４）の認証に失敗したことになり、ステップＣ２１などでの照合ＮＧの場合には、通信制御ＩＣ２３の認証に失敗したことになり、ステップＣ３４などで照合がＮＧの場合には、パチンコ機１０の払出制御チップ１１、主制御チップ１３の少なくともいずれかの認証が失敗したことになる。まお、本実施形態では、払出制御チップ１１、主制御チップ１３など、複数の装置（基板なども含む）について、認証を行う場合には、いずれかの認証失敗（照合ＮＧ）のよって、全体の認証を失敗にしている（全体の照合ＮＧ）。これによって、認証結果が読み取られても、どの装置についての認証が失敗したか分からなくなっており、認証結果の悪用が防止される。

【０２１５】

なお、上記処理において、ＣＵ制御部２１と上位サーバ５１０との間の情報のやり取り（ステップＣ１１、Ｃ３２など）についても暗号化通信を行っても良い。この場合、例えば、ＣＵ制御部２１と上位サーバ５１０とに共通の暗号鍵を設定して、この暗号鍵で暗号化通信を行う。

【０２１６】

なお、上記処理において、上位サーバ５１０と鍵管理センターサーバ３１０との間の情報のやり取り（ステップＣ１０、ステップＣ３３など）についても暗号化通信を行っても良い。この場合、例えば、上位サーバ５１０と鍵管理センターサーバ３１０とに共通の暗号鍵を設定して、この暗号鍵で暗号化通信を行う。

【０２１７】

上記処理では、許可情報Ｂは、通信制御ＩＣ２３が秘匿鍵Ａで復号できるのみであるので（ステップＣ２５）、許可情報Ｂを中継する上位サーバ５１０、ＣＵ制御部２１、セキュリティチップ２２では、許可情報Ｂを復号化できず、許可情報Ｂの漏洩のリスクが低減又は防止されている。

【０２１８】

上記処理では、基板問合せ番号、チップ問合せ番号、チップ情報、更新情報などは、上位サーバ５１０、ＣＵ制御部２１では復号できない秘匿鍵Ｂによって暗号化され、上位サーバ５１０、ＣＵ制御部２１を介して、セキュリティチップ２２と鍵管理センターサーバ３１０とでやり取りされるので（ステップＣ１０からＣ１１、ステップＣ３１からＣ３３など）、上位サーバ５１０、ＣＵ制御部２１で不用意に復号化が行われることを防止でき、情報漏洩のリスクが低減又は防止されている。特に、セキュリティチップ２２が、ＣＵ制御部２１により復号してもよい情報（チップ番号など）を送信する場合には、暗号鍵Ｃ２で暗号化が行われ、セキュリティチップ２２から最終的に鍵管理センターサーバ３１０に対して情報（基板問合せ番号、チップ問合せ番号など）を送信する場合には、その情報の一部について秘匿鍵Ｂで暗号化が行われる。このように、情報の最終的な行き先（情報の重要度）に応じて暗号鍵を使い分けることによって、不用意に復号化が行われることを防止でき、情報漏洩のリスクが低減又は防止されている。また、チップ問合せ番号や基板問合せ番号などの、認証の問い合わせを行うときの問合せ情報を、問い合わせ（認証用情報Ｃ１やチップ番号の送信）の際に付加し、照合結果などの返信の際にもこの問合せ情報が付加され、返信された問合せ情報と送信した問合せ情報とが同じであって場合に、照合結果など（問合せ情報とともに送信された情報）を真性（正当）のものとして扱い、その後の処理（例えば、照合結果などを用いる処理、照合結果などに従った処理）を行うので

、例えば、問い合わせの途中で、照合結果などが入れ替わった場合には、問合せ情報が異なるので、その入れ替わりを検出でき、照合結果の不正な操作を検出できる。また、問合せ情報を上位サーバ５１０、ＣＵ制御部２１では復号できないようにしていることによって、問合せ情報を悪用した照合結果の操作（問合せ情報を盗み、盗んだ問合せ情報と不正な照合結果などとをともに送信することで、セキュリティチップ２２に照合結果などを真性のものと認識させる操作）も検出できる。なお、チップ問合せ番号は、チップ番号から生成され（ステップＣ３０）、チップ番号は、チップ情報から生成されるので（ステップＣ２７）、チップ問合せ番号は、チップ情報から生成されるものでもある。チップ問合せ番号は、チップ情報から直接生成されてもよい。

【０２１９】

上記処理では、セキュリティチップ２２と、通信制御ＩＣ２３との暗号通信において使用される暗号鍵Ａ２が、更新情報から生成される。更新情報は、セキュリティチップ２２から通信制御ＩＣ２３に送信され、両者で暗号鍵Ａ２を別個に生成する（ステップＣ１６、スＣ１９）。これによって、暗号鍵Ａ２をそのまま送信しないので、例えば、セキュリティチップ２２と通信制御ＩＣ２３とを接続する信号線から情報を読み取ったとしても、暗号鍵Ａ２が直接読み取られることはないので、暗号鍵Ａ２の漏洩のリスクが低減又は防止されている。さらに、更新情報は、鍵管理センターサーバ３１０から送信されてくるので（ステップＣ１０、Ｃ１１、Ｃ１５）、更新情報は、外部で管理され、セキュリティチップ２２自身で更新情報を管理するよりも、情報漏洩のリスクが低減又は防止されている。つまり、セキュリティチップ２２を解析しただけでは、どのような暗号鍵Ａ２が生成されるか解析しにくいので、暗号鍵Ａ２の漏洩のリスクを低減できる。

【０２２０】

また、主制御チップ１３、払出制御チップ１１、セキュリティ基板２４（セキュリティチップ２２などと同義）は、外部の鍵管理センターサーバ３１０で認証が行われるため（ステップＣ３４の照合、ステップＣ１０の検索など）、認証の正確性が一定以上担保される。

【０２２１】

（パチンコ機１０及びカードユニット２０の遊技場５００への新規設置後）

上記では、パチンコ機１０とカードユニット２０とをともに新規設置する場合について説明したが、新規設置後、上記処理が終了すると、上位サーバ５１０、カードユニット２０、パチンコ機１０は、電源が落とされる（電源ＯＦＦ）。

【０２２２】

この電源ＯＦＦによって、上位サーバ５００が保持する基板問合せ番号、認証用情報Ｃ１、認証用情報Ｃ２、バージョン情報Ｃ、暗号鍵Ｃ２、認証用情報Ａ１、出荷情報、バージョン情報Ａ２、更新情報は、失われる。これら情報は、消去されてもよい。

【０２２３】

また、電源ＯＦＦによって、ＣＵ制御部２１の処理部２１ａに保持されているチップ番号、チップ情報、チップ問合せ番号も失われる。これら情報は、消去されてもよい。

【０２２４】

一方で、ＣＵ制御部２１の処理部２１ａは、許可情報Ｂ、統一店舗コード、暗号鍵Ｃ１、基板問合せ番号、認証用情報Ｃ１、認証用情報Ｃ２、バージョン情報Ｃ、暗号鍵Ｃ２、認証用情報Ａ１、出荷情報、バージョン情報Ａ２、更新情報を保持するときに、不揮発性のＲＡＭに保持することによって、電源ＯＦＦになっても、これら情報は失われず、保持されたままになる。これら情報は、電源ＯＦＦになっても失われないように記憶部２１ｂに格納されてもよい。以下では、これら情報は、記憶部２１ｂに格納されたものとして説明する。

【０２２５】

また、電源ＯＦＦによって、セキュリティチップ２２の処理部２２ａが保持する統一店舗コード、基板問合せ番号、セッション鍵は、失われる。これら情報は、消去されてもよい。

【０２２６】
一方で、セキュリティチップ２２の処理部２２ａは、許可情報Ｂ、バージョン情報Ａ２、更新情報、暗号鍵Ａ２、チップ番号、チップ情報、チップ問合せ番号、照合結果を保持するときに、不揮発性のＲＡＭに保持することによって、電源ＯＦＦになっても、これら情報は失われず、保持されたままになる。これら情報は、電源ＯＦＦになっても失われないように記憶部２２ｂに格納されてもよい。以下では、これら情報は、記憶部２２ｂに格納されたものとして説明する。
【０２２７】
また、電源ＯＦＦによって、通信制御ＩＣ２３の処理部２３ａが保持する許可情報Ｂ、チップ番号、チップ情報、認証結果、セッション鍵は、失われる。これら情報は、消去されてもよい。
【０２２８】
一方で、通信制御ＩＣ２３の処理部２３ａは、バージョン情報Ａ２、更新情報、暗号鍵Ａ２を保持するときに、不揮発性のＲＡＭに保持することによって、電源ＯＦＦになっても、これら情報は失われず、保持されたままになる。これら情報は、電源ＯＦＦになっても失われないように記憶部２３ｂに格納されてもよい。以下では、これら情報は、記憶部２３ｂに格納されたものとして説明する。
【０２２９】
なお、上記の電源ＯＦＦによって失われる各情報は、制御部や処理部それぞれにおいて、バックアップなどの目的で、不揮発性のＲＡＭに保持されるか、記憶部に格納するようにしてもよい。なお、この場合であっても、制御部や処理部それぞれにおいて所定の情報を元に生成される情報（基板問合せ番号など）は、電源ＯＦＦによって、失われるように又は消去するようにしてもよい。
【０２３０】
上記で説明したカードユニット２０、パチンコ機１０の新規設置後、遊技場５００の通常の開店時において、カードユニット２０、パチンコ機１０、上位サーバ５００は、電源が投入され、その直後に、カードユニット２０のＣＵ制御部２１、セキュリティチップ２２（セキュリティ基板２４）、通信制御ＩＣ２３の認証、パチンコ機１０の払出制御チップ１１、主制御チップ１３の認証を行うための処理が行われる。この処理は、上記の情報が残った状態でスタートするために、新規設置時の動作とは異なる動作が各装置において行われる。以下では、このときの動作（通常営業時の動作）について説明する。
【０２３１】
なお、ＣＵ制御部２１の記憶部２１ｂに格納されている暗号鍵Ｃ２及びバージョン情報Ｃは、適宜更新される。この更新は、例えば、鍵管理センターサーバ３１０から行われる。具体的には、例えば、鍵管理センターサーバ３１０に新たな暗号鍵Ｃ２及びバージョン情報Ｃが記録されると、これら情報が上位サーバ５１０を介してＣＵ制御部２１に供給される記憶部２１ｂに格納される（例えば、上位サーバ５１０及びカードユニット２０が電源投入されたあとのタイミングで行われる）。なお、先にバージョン情報Ｃのみを記憶部２１ｂに格納し、後述の処理において暗号鍵Ｃ２を記憶部２１ｂに格納させてもよい。
【０２３２】
まず、カードユニット２０の情報を扱う通常動作（ＣＵ制御部２１、セキュリティチップ２２（セキュリティ基板２４）、通信制御ＩＣ２３の認証）を行うための処理について図１７を参照して説明する。
【０２３３】
まず、ＣＵ制御部２１の処理部２１ａは、カードユニット２０に通常動作用のカードが挿入された状態で、上記の新規設置時と同様にカードユニット２０の電源が投入されたことを契機として（この時、パチンコ機１０の電源も投入されるものとする。）、上位サーバ５１０との接続を要求する接続要求を上位サーバ５１０へ送信する（ステップＤ１）。
なお、ステップＣ１のときと異なり、この時点では、ＣＵ制御部２１の記憶部２１ｂに許可情報Ｂと統一店舗コードと暗号鍵Ｃ１とが格納されているので、ＣＵ制御部２１の処

理部２１ａは、そのことを示す接続要求を送信する。
【０２３４】
上位サーバ５１０の制御部５１１は、処理部２１ａからの前記接続要求を受信すると、ＣＵ制御部２１との通信を確立する（ステップＤ２）。
【０２３５】
ステップＤ２の後、ＣＵ制御部２１の処理部２１ａは、セキュリティチップ２２の処理部２２ａと通信を行い、メーカー情報Ｂを相互に照合する（ステップＤ３）。このステップの処理は、ステップＣ３と同じであるので説明を省略する。相互の照合の少なくとも１つがＮＧであれば、その後の処理は中止される。一方、相互の照合がＯＫであれば、ＣＵ制御部２１の処理部２１ａは、セキュリティチップ２２に対して接続要求（保持されている統一店舗コードの送信）を行う（ステップＤ４）。
【０２３６】
セキュリティチップ２２の処理部２２ａは、統一店舗コードをＣＵ制御部２１から受信すると、保持している統一店舗コードと、記憶部２２ｂに格納された日時及び認証用情報Ｃ２と、に基づいて、基板問合せ番号を生成し、保持する（ステップＤ５）。この処理は、ステップＣ６と同じであるので、説明を省略する
【０２３７】
セキュリティチップ２２の処理部２２ａは、ステップＤ５に続いて、基板問合せ番号を記憶部２２ｂに格納されている秘匿鍵Ｂで暗号化し、暗号化した基板問合せ番号を認証用情報Ｃ１とともに記憶部２２ｂに格納されている暗号鍵Ｃ１でさらに暗号化し、暗号化した情報をＣＵ制御部２１に送信する（ステップＤ６）。また、ステップＤ６において、ＣＵ制御部２１の処理部２１ａは、前記暗号化した情報を受信すると、記憶部２１ｂに格納した暗号鍵Ｃ１で、受信した情報を復号し、復号した基板問合せ番号（秘匿鍵Ｂで暗号化されたままである。）と認証用情報Ｃ１とを保持する。
【０２３８】
ここで、新規設置時においては、この後に情報要求（ステップＣ８）が行われるが、ＣＵ制御部２１の記憶部２１ｂには、以前に鍵管理センターサーバ３１０から送信された認証用情報Ｃ１、認証用情報Ｃ２、バージョン情報Ｃ、暗号鍵Ｃ２が格納されているため、ＣＵ制御部２１の処理部２１ａは、このような格納がある場合には、セキュリティチップ２２の処理部２２ａと通信を行い、認証用情報Ｃ２を相互に照合する（ステップＤ７）。このステップＤ７は、ステップＣ１２と同じであるので、説明を省略する。
【０２３９】
ステップＤ７での照合がすべてＯＫでなかった場合には、処理が中止されるが、全てＯＫであった場合には、ＣＵ制御部２１の処理部２１ａは、セキュリティチップ２２の処理部２２ａと再度通信を行い、バージョン情報Ｃを相互に照合する（ステップＤ８）。このステップＤ８は、ステップＣ１３の処理と同じであるので説明を省略する。
【０２４０】
ステップＤ８の照合がＯＫであれば、これ以降、処理部２１ａと処理部２２ａとは、各記憶部に格納されている暗号鍵Ｃ２を用いた暗号通信を開始する（ステップＤ９）。ステップＤ８での照合がすべてＯＫでなかった場合には、処理が中止される。
【０２４１】
ステップＤ９の後は、ステップＤ１０からＤ１４が行われるが、これら処理は、それぞれ、ステップＣ２１からＣ２５と同じ処理であるので、説明を省略する。
【０２４２】
上記のような処理では、鍵管理センターサーバ３１０への問い合わせが一度行われたことを条件として、通常時の処理では、鍵管理センターサーバ３１０への情報要求などが行われないので、鍵管理センターサーバ３１０への処理負荷などが軽減される。また、情報が遊技場５００の外部に漏れる可能性も少ないので、情報漏洩のリスクを回避出来る。
【０２４３】
なお、セキュリティチップ２２の処理部２２ａには、第１モードと第２モードとがあっ

てもよい（図１８参照）。例えば、処理部２２ａは、記憶部２２ｂに暗号鍵Ｃ２が格納されていない場合（新規設置時もこれにあたる。）、ステップＤ８での照合がすべてＯＫでなかった場合（いずれかの照合がＯＫでない場合、処理部２２ａと処理部２１ａは、お互いにその旨を通知するとよい。）、ステップＤ９で暗号通信が出来ない場合（この場合であっても、認証が失敗したと捉えることができる。）には、暗号鍵Ｃ２が更新されていたり、何らかの理由で暗号鍵Ｃ２が消去されてしまっていたりする可能性があるので、ＣＵ制御部２１の処理部２１ａ及びセキュリティチップ２２の処理部２２ａは、第１モードで動作し、ステップＣ４の後や、ステップＤ８、Ｄ９の後に、ステップＣ５からＣ２５の処理を行う。セキュリティチップ２２の処理部２２ａは、一方で、処理部２２ａは、記憶部２２ｂに暗号鍵Ｃ２が格納されている場合には、暗号鍵Ｃ２での暗号通信が可能であるので（つまり、一度鍵管理センターサーバ３１０での認証（セキュリティ基板２４の認証）が行われているので）、ステップＤ４の後にステップＤ５の処理を行う。このように、一度、鍵管理センターサーバ３１０への情報要求が行われたあとであっても、暗号鍵Ｃ２の更新等の例外的な場面に対して適切な対処が可能になっている。このようなモードによって、セキュリティチップ２２の処理部２２ａは、結果的に、認証用情報Ｃ２などを用いた認証について、鍵管理センターサーバ３１０から取得した認証用情報Ｃ２について認証を行うか、ＣＵ制御部２１に格納された認証用情報Ｃ２について認証を行うかなど、認証の問い合わせを変更できることになる。これによって、状況に応じた適宜の認証が可能になっている。なお、別の観点から見ると、ＣＵ制御部２１は、自身が記憶（保持する場合も含む）する認証用情報Ｃ２などを用い、セキュリティチップ２２の認証を行い（ステップＤ７での、セキュリティチップ２２から認証用情報Ｃ２を取得しての照合を行い）、認証が成功なら、上位サーバ５１０を介した鍵管理センターサーバ３１０への問い合わせを行わず、認証が失敗なら、上位サーバ５１０を介した鍵管理センターサーバ３１０への問い合わせを行うことになる。なお、セキュリティチップ２２の処理部２２ｂが、認証結果に応じて、上位サーバ５１０を介した鍵管理センターサーバ３１０への問い合わせの必要性の有無をＣＵ制御部２１に指示してもよい。鍵管理センターサーバ３１０への問い合わせ有りが指示された場合、ＣＵ制御部２１は、認証用情報Ｃ１、認証用情報Ｃ２、バージョン情報Ｃ、暗号鍵Ｃ２などの格納に関わらず、鍵管理センターサーバ３１０への問い合わせを行う。

【０２４４】

次に、パチンコ機１０の情報を扱う通常動作（主制御チップ１３、払出制御チップ１１の認証）を行うための処理について図１９を参照して説明する。

【０２４５】

セキュリティチップ２２の処理部２２ａは、通信制御ＩＣ２３に対してチップ情報の要求を行う（ステップＥ１）。通信制御ＩＣ２３の処理部２３ａは、セキュリティチップ２２からのチップ情報の要求を受信すると、チップ情報を取得する（ステップＥ２）。通信制御ＩＣ２３の処理部２３ａは、ステップＥ２で取得したチップ情報からチップ番号を生成する（ステップＥ３）。ステップＥ１からＥ３の処理は、それぞれ、ステップＣ２６からＣ２８の処理と同じであるので説明を省略する。

【０２４６】

通信制御ＩＣ２３の処理部２３ａは、チップ情報及びチップ番号を暗号鍵Ａ２で暗号化して、セキュリティチップ２２に送信し、セキュリティチップ２２の処理部２２ａは、チップ情報及びチップ番号を受信すると暗号鍵Ａ２で復号化するが、チップ番号及びチップ情報は照合結果とともにすでに記憶部２３ｂに格納されているので、処理部２２ａは、記憶部２２ｂに格納されているチップ情報と復号化されたチップ情報とを照合し、照合ＯＫ（全てのチップについての照合ＯＫの場合）であるかを判定する。また、記憶部２２ｂに格納されている照合結果がＯＫであるかを判定する。照合結果がＯＫである場合、この照合結果と一緒に記憶されているチップ情報は、パチンコ機１０の新規設置時に鍵管理センターサーバ３１０で照合ＯＫの結果が出ている情報である（つまり、正当なチップ情報である）ので、チップ情報の照合もＯＫである場合には、パチンコ機１０から取得されたチ

ップ情報は正当である、つまり、主制御チップ１３や払出制御部１１は正当である可能性が高い。この場合には、処理部２２ａは、チップ情報を記憶部２２ｂに格納されている秘匿鍵Ｂで暗号化し、暗号化されたチップ情報をさらに、チップ番号とともに、暗号鍵Ｃ２で暗号化し、ＣＵ制御部２１に送信する。このとき、処理部２２ａは、チップ情報の照合について、外部に問い合わせる必要がないので、問い合わせの必要がない旨を暗号化した情報とともに送信する（ステップＥ６）。ＣＵ制御部２１の処理部２１ａは、受信した情報暗号鍵Ｃ２で復号化し、保持する。また、ＣＵ制御部２１の処理部２１ａは、問い合わせの必要がない旨を情報を受信しているので、上位サーバ５１０への情報送信は行わない。

【０２４７】

セキュリティチップ２２の処理部２２ａは、ステップＥ６のあと、認証ＯＫの認証結果を通信制御ＩＣ２３に送信し、通信制御ＩＣ２３の処理部２３ａは認証結果を保持する（ステップＥ７）。この後は、適宜、ステップＣ３９以降の処理が行われる。

【０２４８】

上記のような処理によれば、鍵管理センターサーバ３１０において、チップ情報の照合が行われ、照合ＯＫだった場合には、その後は、カードユニット２０内で、チップ情報の照合が行われるので、状況に応じて適切な場所での認証が実現される。また、上位サーバ５１０や鍵管理センター３１０にチップ情報が送信されないので、これらの処理負担が軽減される。

【０２４９】

なお、通信制御ＩＣ２３の処理部２３ａは、チップの認証の問い合わせのレベル（チップ情報をどこまで送信するかのレベル）を状況に応じて変更できる。この点について、図２０から２２を参照して説明する。なお、上記図１９の場合には、問い合わせが結果的に無いので、問い合わせのレベルが最も低いことになる。

【０２５０】

図２０は、セキュリティチップ２２の記憶部２２ｂにチップ情報が格納されていない場合についての処理の流れを詳細に説明するものである。

【０２５１】

セキュリティチップ２２の処理部２２ａは、通信制御ＩＣ２３に対してチップ情報の要求を行う（ステップＦ１）。通信制御ＩＣ２３の処理部２３ａは、セキュリティチップ２２からのチップ情報の要求を受信すると、チップ情報を取得する（ステップＦ２）。通信制御ＩＣ２３の処理部２３ａは、取得したチップ情報からチップ番号を生成する（ステップＦ３）。通信制御ＩＣ２３の処理部２３ａは、チップ情報及びチップ番号を暗号鍵Ａ２で暗号化して、セキュリティチップ２２に送信し、セキュリティチップ２２の処理部２２ａは、チップ情報及びチップ番号を受信すると暗号鍵Ａ２で復号化し、また、記憶部２２ｂにチップ情報などが格納されていないので（つまり、上記新規設置時と同じ状態であるので）、チップ情報などを保持する（ステップＦ４）。次に、セキュリティチップ２２の処理部２２ａは、保持するチップ番号などからチップ問合せ番号を自動生成し、保持する（ステップＦ５）。

【０２５２】

次に、セキュリティチップ２２の処理部２２ａは、保持するチップ情報とチップ問合わせ番号とを記憶部２２ｂに格納されている秘匿鍵Ｂで暗号化し、暗号化されたチップ情報とチップ問合わせ番号とをさらに、処理部２２ａが保持するチップ番号とともに、暗号鍵Ｃ２で暗号化し、ＣＵ制御部２１に送信する（ステップＦ６）。なお、このとき、記憶部２２ｂにチップ情報などが格納されていないので、処理部２２ａは、上記のように自身での照合が行えないので、上位サーバ５１０に問い合わせを要求する情報も送信する。ＣＵ制御部２１の処理部２１ａは、セキュリティチップ２２からのチップ情報とチップ問合わせ番号とチップ番号とを暗号鍵Ｃ２で復号化し、復号化した情報を保持するとともに（チップ情報とチップ問合わせ番号とは、秘匿鍵Ｂでそれぞれ暗号化されたままである。）、上位サーバ５１０に問い合わせを要求する情報を受信しているので、前記で復号化した各

情報を照合要求とともに上位サーバ５１０に送信する（ステップＦ７）。なお、ステップＦ１からＦ７は、ステップＣ２６からＣ３２までと基本的に同じ処理であるので、詳細な説明は省略する。

【０２５３】

ステップＦ８において、上位サーバ５１０は、記憶部５１２に、送信されたチップ番号と同じチップ番号（及び／又は認証結果）を格納しているか否かでその動作が異なる。前記のように、セキュリティチップ２２の記憶部２２ｂにチップ情報などが格納されておらず、上位サーバ５１０の記憶部５１２にも対応するチップ番号が格納されていない場合には、パチンコ機１０は上記のように新規設置されたことになる。この場合に、これ以降、ステップＣ３３以降の処理が行われる。一方、前記のように、セキュリティチップ２２の記憶部２２ｂにチップ情報などが格納されておらず、上位サーバ５１０の記憶部５１２に対応するチップ番号が格納されている場合には、以前、そのパチンコ機１０の各チップについて認証が行われていることになる。つまり、この場合、カードユニット２０のみが新規に設置された状況である。このような場合には、これ以降、ステップＦ９以降の処理（図２１参照）が行われる。

【０２５４】

ステップＦ９において、上位サーバ５１０の制御部５１１は、記憶部５１２に格納されている、ステップＦ７で送信されたチップ番号と同じチップ番号とこのチップ番号とともに格納されているチップ情報、チップ問合せ番号、照合結果をＣＵ制御部２１に送信する（ステップＦ９）。ＣＵ制御部２１の処理部２１ａは、チップ番号、チップ情報、チップ問合せ番号、照合結果を受信すると、そのままセキュリティチップ２２に送信する（ステップＦ１０）。セキュリティチップ２２の処理部２２ａは、チップ番号、チップ情報、チップ問合せ番号、照合結果を受信すると、記憶部２２ｂに格納された秘匿鍵Ｂを用いてチップ情報、チップ問合せ番号、照合結果を復号化し、復号化し、復号化したチップ問合せ番号が、ステップＦ５で生成したチップ問合せ番号と同じであれば、復号化した照合結果を取り込む。処理部２２ａは、照合結果が照合ＯＫの場合には（照合結果が照合ＮＧの場合には、例えば、処理を中止する。）、認証ＯＫの認証結果を通信制御ＩＣ２３に送信する。この後は、適宜、ステップＣ３９以降の処理が行われる。処理部２２ａは、復号化したチップ情報と、ステップＦ４で送信されたチップ情報とを照合してもよい。しかし、チップ番号は、チップ情報に基づいて生成されるものであり、上位サーバ５１０で同じチップ情報があったと言うことは、チップ情報の照合も照合ＯＫで有る可能性が高い。このように、上位サーバ５１０は、実質的には、チップ番号で、パチンコ機１０のチップの認証を行うことになる。

【０２５５】

図２１は、セキュリティチップ２２の記憶部２２ｂに格納された照合結果が照合ＮＧの場合についての処理の流れを詳細に説明するものである。

【０２５６】

セキュリティチップ２２の処理部２２ａは、通信制御ＩＣ２３に対してチップ情報の要求を行う（ステップＧ１）。通信制御ＩＣ２３の処理部２３ａは、セキュリティチップ２２からのチップ情報の要求を受信すると、チップ情報を取得する（ステップＧ２）。通信制御ＩＣ２３の処理部２３ａは、取得したチップ情報からチップ番号を生成する（ステップＧ３）。通信制御ＩＣ２３の処理部２３ａは、チップ情報及びチップ番号を暗号鍵Ａ２で暗号化して、セキュリティチップ２２に送信し、セキュリティチップ２２の処理部２２ａは、チップ情報及びチップ番号を受信すると暗号鍵Ａ２で復号化し、ステップＥ６などと同様に、記憶部２２ｂに格納されている照合結果がＯＫであるか、記憶部２２ｂに格納されているチップ情報と復号化されたチップ情報とを照合し、照合ＯＫ（全てのチップについての照合ＯＫの場合）であるかを判定する（ステップＧ５）。ここでは、照合結果がＮＧであるので、ステップＧ５でチップ情報を照合した結果にかかわらず、以前の照合時において、パチンコ機１０の主制御チップ１３や払出制御チップ１１についてすり替えなどが発生していた可能性があるので、処理部２２ａは、このチップの認証について、鍵管

理センターサーバ３１０に問い合わせを行う。具体的には、セキュリティチップ２２の処理部２２ａは、保持するチップ番号などからチップ問合せ番号を自動生成し、保持する（ステップＧ５）。次に、セキュリティチップ２２の処理部２２ａは、保持するチップ情報とチップ問合わせ番号とを記憶部２２ｂに格納されている秘匿鍵Ｂで暗号化し、暗号化されたチップ情報とチップ問合わせ番号とをさらに、処理部２２ａが保持するチップ番号とともに、暗号鍵Ｃ２で暗号化し、ＣＵ制御部２１に送信する（ステップＧ６）。なお、このとき、前記の照合がＮＧだったため、鍵管理センターサーバ３１０に問い合わせを要求する情報も送信する。ＣＵ制御部２１の処理部２１ａは、セキュリティチップ２２からのチップ情報とチップ問合わせ番号とチップ番号とを暗号鍵Ｃ２で復号化し、復号化した情報を保持するとともに（チップ情報とチップ問合わせ番号とは、秘匿鍵Ｂで暗号化されたままである。）、鍵管理センターサーバ３１０に問い合わせを要求する情報を受信しているので、前記で復号化した各情報を鍵管理センターサーバ３１０に問い合わせを要求する照合要求とともに上位サーバ５１０に送信する（ステップＧ７）。

【０２５７】

上位サーバ５１０の制御部５１１は、鍵管理センターサーバ３１０に問い合わせを要求する照合要求を受信しているので、ＣＵ制御部２１から送信された前記各情報をそのまま、照合要求とともに、鍵管理センターサーバ３１０に送信する。これにより、セキュリティチップ２２の処理部２２ａは、鍵管理センターサーバ３１０に対してチップ情報などを送信したことになり、認証の問い合わせが行われたことになる。その後、鍵管理センターサーバ３１０では照合が行われ、ステップＣ３４以降の処理が行われる。なお、鍵管理センターサーバ３１０でも照合結果がＮＧの場合には、主制御チップ１３と払出制御チップ１１とのうちの少なくともいずれかにすり替えなどの不正が行われた可能性が高い。一方で、照合結果がＯＫの場合には、パチンコ機１０が新規に設置されたか、カードユニット２０とのペアが変更された可能性がある。

【０２５８】

上記をまとめると、例えば、記憶部２２ｂに格納された照合結果がＮＧの場合（鍵管理センターサーバ３１０での以前の認証の結果が失敗だった場合）には、処理部２２ａでの照合結果（送信されたチップ情報を用いた照合の結果）にかかわらず（チップ情報を用いたパチンコ機１０の各種チップの認証の正否に関わらず）、鍵管理センターサーバ３１０が問い合わせ先になる。また、記憶部２２ｂに格納された照合結果がＯＫで（鍵管理センターサーバ３１０での以前の認証の結果が成功だった場合）、処理部２２ａでの照合結果もＯＫの場合（チップ情報を用いたパチンコ機１０の各種チップの認証が成功だった場合）には、問い合わせ先は無しになる。一方、照合結果やチップ情報が格納されていない場合には、上位サーバ５１０が問い合わせ先になる。なお、記憶部２２ｂに格納された照合結果がＯＫで、処理部２２ａでの照合結果がＮＧの場合（チップ情報を用いたパチンコ機１０の各種チップの認証が失敗だった場合）には、パチンコ機１０の台移動があったなどの可能性があるので、上位サーバ５１０にチップ情報などが格納されている可能性があるので、上位サーバ５１０を問い合わせにするとよい。なお、念のため、鍵管理センターサーバ３１０への問い合わせを行っても良い。

【０２５９】

図１９から図２２を参照して説明したように、セキュリティチップ２２は、記憶部２２ｂにチップ情報が格納されているか否かなどの状況（つまり、パチンコ機１０が送信するチップ情報の照合結果）に応じて、チップ情報の問い合わせを、どこまで行うか決定し、問い合わせを行うことになるので（つまり、決定した問い合わせ先に対してチップ情報を送信し、問い合わせが行われることになるので）、状況に応じた適切な認証が行われる。特に、過去に認証がＯＫだった場合には、その後の認証がカードユニット２０内や遊技場５００内で完結するので、その他の装置や遊技場５００外部へ情報を送信する必要が無く、セキュリティの面からも望ましい。

【０２６０】

上記のように説明したように、本実施形態では、パチンコ機１０やカードユニット２０

の新規設置後であっても、適切な認証処理を行うことが出来る。通常の営業時においては、ステップＤ１からＤ１４までの処理、ステップＥ１からＥ７、ステップＣ３９からの処理が行われることになる。また、パチンコ機１０のみが新規に設置された直後には、ステップＤ１からＤ１４までの処理、ステップＧ１からＧ８間での処理、ステップＣ３４以降の処理が行われることになる。また、カードユニット２０のみが新規に設置された直後には、ステップＣ１からＣ２５までの処理、ステップＦ１からＦ１１、ステップＣ３９からの処理が行われることになる。このように、本実施形態の遊技用システム１は、様々な状況にあわせて適切な動作が行われるようになっている。

【０２６１】

また、上記問い合わせのレベルは、制御情報などによって、外部から指定することもできる。例えば、鍵管理センターサーバ３１０の記憶部３１２には、制御情報が格納される（例えば、鍵管理センター３００の従業員による鍵管理センターサーバ３１０への操作（制御情報を格納する操作）に基づいて行われる。）。この制御情報は、例えば、セキュリティチップ２２における認証レベルを指定する情報である。

【０２６２】

例えば、チップ情報がパチンコ機１０の主制御チップ１３及び払出制御チップ１１を認証するために様々な情報（識別情報の他、チップのバージョン、チップのメーカーコードなど）を含む場合、この制御情報は、例えば、チップ情報の照合において、チップ情報に含まれるどの情報を照合に用いるかを指定する情報である。全ての情報を照合に用いれば、認証レベルは高まり、照合に用いる情報が少なければ認証レベルは低くなる。また、この制御情報は、照合ＯＫとする場合の、照合されるチップ情報の一致度を指定するものであってもよい。例えば、この制御情報は、チップ情報に含まれる所定の情報が一致している場合（一部一致している場合）に照合結果をＯＫとすることを指定したり、チップ情報に含まれる全ての情報が一致している場合（前記の一部一致よりも認証レベルは高くなる。）にのみ照合結果をＯＫとすることを指定したりする情報であってもよい。状況によっては、それほど高度な認証レベルが必要でない場合もあり（例えば、新規設置時には一度も認証が行われていないので、認証レベルを高める必要があるが、一度認証が成功すれば、その後は認証レベルが低くても一定のセキュリティは確保出来る。）、認証レベルを設定することで、適切な認証が行われる。なお、認証レベルの高低によって、照合結果が変わることもあり得る。そして、照合結果が変わると、上記図１９乃至図２２で説明した処理などでは、問い合わせ先が異なることになる。つまり、制御情報は、問い合わせ先を間接的に指定する情報でもある。

【０２６３】

図２３を参照して、制御情報の配信について説明する。例えば、鍵管理センター３００の従業員による鍵管理センターサーバ３１０への操作（制御情報の内容を指定する操作及び制御情報を送信する上位サーバ５１０（つまり、制御情報で認証レベルを変更したいカードユニット２０）を指定する操作）に基づいて、鍵管理センターサーバ３１０の記憶部３１２には、制御情報が格納され、制御部３１１は、制御情報を秘匿鍵Ｂで暗号化し、上位サーバ５１０に送信する（ステップＨ１）。上位サーバ５１０の制御部５１１は、制御情報を暗号化されたまま、ＣＵ制御部２１に送信する（ステップＨ２）。ＣＵ制御部２１の処理部２１ａは、制御情報を受信すると、制御情報を暗号化されたまま、セキュリティチップ２２に送信する（ステップＨ３）。セキュリティチップ２２の処理部２２ａは、制御情報を受信すると、記憶部２２ｂに格納されている秘匿鍵Ｂで制御情報を復号化して保持する。これによって、例えば、上記認証レベルが変更される（例えば、認証レベルが引き上げられ、チップ情報に含まれる全ての情報について照合が行われるようになる）。このように、外部から問い合わせのレベルなどを変更することによって、状況に応じた適切な問い合わせレベルで、問い合わせを行うことが出来る。

【０２６４】

なお、制御情報は、問い合わせのレベルを直接指定する情報であってもよい。例えば、制御情報がセキュリティチップ２２に供給されることで、セキュリティチップ２２の処理

部２２ａは、鍵管理センターサーバ３１０までの問い合わせを必ず行うようにしたり、制御情報が「１」である場合には鍵管理センターサーバ３１０までの問い合わせを必ず行い、制御情報が「２」である場合には上記のような通常通りの問い合わせを行うようにしたりしてもよい。

【０２６５】

（変形例）

本発明は、上記で説明した実施形態に限定されず、種々の変形及び応用が可能である。下記にその変形例を例示する。下記の変形例は、上記で説明した実施形態に個別又は複数組み合わせて、適用される。

【０２６６】

（変形例１）

遊技場５００は、パチンコ店に限らず、カジノや、ゲームセンター等であってもよい。また、遊技用装置は、パチンコ機１０だけでなく、例えば、スロットマシンやゲーム機、又はこれらの周辺機器等、１以上の集積回路を搭載した遊技用の装置であればよい。

【０２６７】

スロットマシンとは、例えば、所定の遊技媒体を１ゲームに対して所定数の賭数を設定した後、遊技者がスタートレバーを操作することにより可変表示装置による識別情報の可変表示を開始し、遊技者が各可変表示装置に対応して設けられた停止ボタンを操作することにより、その操作タイミングから予め定められた最大遅延時間の範囲内で識別情報の可変表示を停止し、全ての可変表示装置の可変表示を停止したときに導出表示された表示結果に従って入賞が発生し、入賞に応じて予め定められた所定の遊技媒体が払い出され、特定入賞が発生した場合に、遊技状態として所定の遊技価値を遊技者に与える状態にするように構成した遊技機である。

【０２６８】

スロットマシンは、遊技場５００における遊技島において機種等毎に所定の位置に配置される。スロットマシンも、パチンコ機１０と同様に、払出制御チップ１１（遊技媒体を払い出す処理等を行うチップ）と主制御チップ１３（可変表示装置の制御、遊技状態の演出の制御等を行うチップ）とを備える場合がある。この場合、上記実施形態と同様に本発明を適用可能である。また、スロットマシンにおいては、演出制御のチップが主制御チップ１３のように認証対象であってもよい。

【０２６９】

（変形例２）

払出制御チップ１１、主制御チップ１３は１つにパッケージ化されてパチンコ機１０に搭載されてもよい。

【０２７０】

（変形例３）

また、上記実施形態では、暗号通信を共通鍵で行っていたが、暗号通信は公開鍵と秘密鍵を用いた通信であってもよい。この場合には、適宜、暗号通信を行う構成要素間で、公開鍵と秘密鍵とが設定される。その他暗号化方式は任意であり、様々な方式で暗号化が行われる。

【０２７１】

（変形例４）

なお、遊技用システム１を構成する各装置の記憶部に格納されたプログラムは、ネットワークＮを介してダウンロード等されたものであってもよい。

【０２７２】

（変形例５）

なお、遊技用システム１を構成する各装置の制御部や処理部は、その少なくとも一部が上述の処理の少なくとも一部を行うための専用回路によって構成されてもよい。

【０２７３】

（変形例６）

なお、鍵管理センターサーバ３１０は、遊技場５００毎に設置されている遊技用装置の種類とそれに対応する台数を集計するようにしてもよい。

【０２７４】

（変形例７）

上記実施形態では、カードユニット２０と鍵管理センターサーバ３１０との間には、上位サーバ５１０が介在し、カードユニット２０と鍵管理センターサーバ３１０との間で送受信される情報は、上位サーバ５１０を介して送受信されている。しかし、カードユニット２０と鍵管理センターサーバ３１０との間には、上位サーバ５１０に加え、上位サーバ５１０に接続された他のサーバが介在してもよい。上位サーバと他のサーバとによって、中継システムが構成される。カードユニット２０と鍵管理センターサーバ３１０との間で送受信される情報は、中継システムを介して送受信される。なお、上位サーバ５１０のみでも、上記中継システムを構成するものとする。

【０２７５】

（変形例８）

上記日時は、各装置における制御部や処理部が、所定のカレンダ部（図示せず）を参照し、現在の日時を取得し、取得した日時を日時としてリアルタイムで更新していく情報であってもよい。例えば、ステップＡ６やステップＡ８において、日時は、通信制御ＩＣ用ライター６１０やＳＣ用ライター６５０に登録されているが、通信制御ＩＣ用ライター６１０やＳＣ用ライター６５０がリアルタイムで日時を更新してもよい。なお、日時は、時単位であってもよく、日単位であってもよい。

【０２７６】

（変形例９）

暗号鍵Ｃ２や秘匿鍵Ｂは、適宜のタイミングで鍵管理センターサーバ３１０に登録されればよい。

【０２７７】

（変形例１０）

上記実施形態では、認証用情報Ｃ２は、鍵管理センターサーバ３１０から上位サーバ５１０を介してＣＵ制御部２１に送信され、ＣＵ制御部２１において照合に使用されていたが、チップ情報と同様に、セキュリティチップ２２（又はＣＵ制御部２１）が認証用情報Ｃ２などを鍵管理センターサーバ３１０に対して送信し、鍵管理センターサーバ３１０で認証用情報Ｃ２などの照合を行わせても良い。この場合、チップ情報の場合と同様に、照合結果や認証用情報Ｃ２などが、上位サーバ５１０で記憶され、上位サーバ５１０は、認証の問い合わせのときに、照合結果や認証用情報Ｃ２などを格納していたら、これらをセキュリティチップ２２に返信し、格納していなかったら認証用情報Ｃ２を鍵管理センターサーバ３１０に送信してもよい。さらに、チップ情報のときと同様に、セキュリティチップ２２（又はＣＵ制御部２１）は、鍵管理センターサーバ３１０における照合の照合結果やそのときに使用された認証用情報Ｃ２などを記憶し、新たに認証される認証用情報Ｃ２などを取得し、取得した認証用情報Ｃ２などと、記憶している認証用情報Ｃ２との照合についての結果や、記憶している照合結果に基づいて、問い合わせ先を決定してもよい。また、チップ情報を、認証用情報Ｃ２と同様に、鍵管理センターサーバ３１０から上位サーバ５１０及びＣＵ制御部２１を介してセキュリティチップ２２に送信し、セキュリティチップ２２で照合に使用してもよい。また、認証用情報Ｂ２などについても、鍵管理センターサーバ３１０から上位サーバ５１０及びＣＵ制御部２１を介してセキュリティチップ２２に送信してもよいし、セキュリティチップ２２が認証用情報Ｃ２を鍵管理センターサーバ３１０に対して送信し、鍵管理センターサーバ３１０で認証用情報Ｂ２の照合を行わせても良い。このような場合、以前に鍵管理センターサーバ３１０で照合された照合結果を用いなくてもよい。

【０２７８】

（変形例１１）

また、セキュリティチップ２２と主制御チップ１１や払出制御チップ１３とは、通信制

御ＩＣ２３などを介して、例えば、所定の暗号通信を行うことによる暗号認証を行い、これによって、セキュリティチップ２２と主制御チップ１１や払出制御チップ１３とが相互認証を行うようにしてもよい。

【０２７９】

（変形例１２）

認証用情報Ａ２は、通信制御ＩＣ２３ごとにユニークな情報であってもよい。認証用情報Ｂ２は、セキュリティチップ２２ごとにユニークな情報であってもよい。認証用情報Ｃ１、認証用情報Ｃ２は、それぞれ、基板２４ごとにユニークな情報であってもよい。このような場合、通信制御ＩＣライター６１０ごと、ＳＣ用ライター６５０ごとに、複数の認証用情報が管理されることになる。

【０２８０】

（変形例１３）

セキュリティチップ２２、通信制御ＩＣ２３、ＳＣ用ライター６５０、通信制御ＩＣ用ライター６１０などは、同じメーカー（例えば、チップメーカー６００）で製造され、カードユニットメーカー６００に出荷されてもよい。

【０２８１】

（変形例１４）

許可情報Bは、鍵管理センターサーバ３１０の記憶部３１２に格納される時点では秘匿鍵Ａで暗号化されず、上位サーバ５１０に送信されるときに暗号化されてもよい。例えば、チップメーカーコンピュータ１１０の制御部１１１は、ステップＡ２で、記憶部１１２に格納されている秘匿鍵Ａを他の情報（暗号化されていない許可情報Ｂも含む。）とともに送信し、鍵管理センターサーバ３１０の制御部３１１は、受信した秘匿鍵Ａを他の情報とともに記憶部３１２に格納し、制御部３１１は、ステップＡ９９で上位サーバ５１０に許可情報Ｂを送信するときに、許可情報Ｂを対応する秘匿鍵Ａで暗号化して送信してもよい。

【０２８２】

（変形例１５）

ステップＡ９以降の処理は、鍵管理センターサーバ３１０から通信制御ＩＣライター６１０及びＳＣ用ライター６５０に、その後の処理を行うことを許可する情報が供給されたことを条件として行われるようにしてもよい。この場合、例えば、通信制御ＩＣ用ライター６１０の制御部６１１は、ステップＡ６での情報登録が終了すると、鍵管理センターサーバ３１０にもその旨を送信する。また、ＳＣ用ライター６５０の制御部６５１は、ステップＡ８での情報登録が終了すると、鍵管理センターサーバ３１０にその旨を送信する。鍵管理センターサーバ３１０の処理部３１１は、通信制御ＩＣライター６１０及びＳＣ用ライター６５０の両者から、情報登録の終了の情報を受信すると、通信制御ＩＣライター６１０及びＳＣ用ライター６５０のそれぞれに、処理の許可を通知する。通信制御ＩＣライター６１０及びＳＣ用ライター６５０は、この許可の通知を条件として、ステップＡ９以降の処理を行うことができるようにしてもよい。特に、通信制御ＩＣライター６１０は、この許可の通知によって、ステップＡ９の処理を行うことを開始する。このように、鍵管理センターサーバ３１０の方で通信制御ＩＣライター６１０及びＳＣ用ライター６５０の認証が成功しない限り、情報の書き込みなどのステップＡ９以降の処理が許可されないことによって、例えば、ＳＣ用ライター６５０のなりすましがあり、情報登録の終了の情報が偽のＳＣ用ライター６５０から通信制御ＩＣライター６１０に送信され、通信制御ＩＣライター６１０がステップＡ９の処理を開始してしまうといったことなどを防ぐことができる。つまり、セキュリティが向上する。

【０２８３】

（変形例１６）

秘匿鍵Ｂは、鍵管理センターサーバ３１０に登録されてもよい。この場合、例えば、ステップＡ７の前に秘匿鍵Ｂが登録され、ステップＡ７で他の情報とともにＳＣ用ライター６５０に情報登録する。また、例えば、秘匿鍵Ｂは、ステップＡ１８で送信されないよう

にする。秘匿鍵Ｂは、上記と同様の方法（自動生成など）で生成される。なお、秘匿鍵Ｂは、例えば、鍵管理センター３００の従業員による鍵管理センターサーバ３１０への操作（秘匿鍵Ｂを登録する操作）などに基づいて、適宜のタイミングで生成されてもよい。

【０２８４】

（変形例１７）

通信制御ＩＣ２３の処理部２３ａによるチップ情報の取得（ステップＢ１２、ステップＣ２７など）は、電源投入による通信制御ＩＣ２３の動作開始時（カードユニット２０の電源投入時）に行っても良い。

【０２８５】

（変形例１８）

鍵管理センターサーバ３１０は、ステップＣ３４で照合結果がＯＫだった場合にのみ、ステップＣ３５以降の処理を行ってもよい。鍵管理センターサーバ３１０は、ステップＣ３４で照合結果がＯＫだった場合にのみ、ステップＣ３５以降の処理を行ってもよい。セキュリティチップ２２の処理部２２ａに供給される照合結果は、ＯＫ（全てＯＫ）の場合にのみ、電源ＯＦＦがあっても失われないようにしてもよい。これらの場合には、記憶部２２ｂに照合結果が格納されていることによって、記憶部２２ｂが格納する照合結果（例えば、以前の鍵管理センターサーバ３１０での照合）がＯＫであるということになる。

【０２８６】

（その他）

上記実施形態や変形例で把握され得る構成例等を、以下に記載する。なお、以下に記載された各構成は、適宜他の構成と組み合わせることが出来る。また、下記の発明は、上記実施形態や変形例を一例とするものであり、実施態様は適宜変更可能である。

【０２８７】

（その他１）

（１）所定の遊技用装置（例えば、カードユニット２０など）に搭載される、所定の処理（例えば、パチンコ機１０との通信処理（ステップＣ２７）など）を行う第１の制御装置（例えば、通信制御IC２３など）と、前記所定の処理とは異なる処理（例えば、パチンコ機１０に搭載された主制御チップ１３などの認証要求を行う処理（ステップＣ３１）など）を行う第２の制御装置（例えば、セキュリティチップ２２など）と、のそれぞれに情報を書き込む書込システム（例えば、遊技用システム１など）であって、

前記第１の制御装置に対して情報を書き込む第１の書込装置（例えば、通信制御IC用ライター６１０など）と、

前記第２の制御装置に対して情報を書き込む第２の書込装置（例えば、セキュリティチップ用ライター６５０など）と、を備え、

前記第１の書込装置は、前記第１の制御装置に予め記録されている所定情報（例えば、認証用情報A２など）を読み取る読取手段（例えば、ステップＡ１０で認証用情報A２を読み取る制御部６１１など）と、前記読取手段が読み取った前記所定情報を前記第２の書込装置に送信する送信手段（例えば、ステップＡ１１で認証用情報A２を送信する制御部６１１など）と、を備え、

前記第２の書込装置は、前記送信手段から送信された前記所定情報を前記第２の制御装置に対して書き込む書込手段（例えば、ステップＡ１６で認証用情報A２を書き込む制御部６５１など）を備える、

ことを特徴とする書込システム。

【０２８８】

上記構成によれば、１つの装置によって２つの制御装置に情報を読み書きする必要がないので、情報漏洩のリスクを低減できる。

【０２８９】

（２）所定の遊技用装置（例えば、カードユニット２０など）に搭載される、所定の処理（例えば、パチンコ機１０との通信処理（ステップＣ２７）など）を行う第１の制御装置（例えば、通信制御IC２３など）に情報を書き込む書込装置（例えば、通信制御IC用ライ

ター６１０など）であって、
前記第１の制御装置に予め記録されている所定情報（例えば、認証用情報A２など）を読み取る読取手段（例えば、ステップＡ１０で認証用情報A２を読み取る制御部６１１など）と、
前記読取手段が読み取った前記所定情報を、前記所定の処理とは異なる処理（例えば、パチンコ機１０に搭載された主制御チップ１３などの認証要求を行う処理（ステップＣ３１）など）を行う第２の制御装置（例えば、セキュリティチップ２２など）に対して情報を書き込む他の書込装置（例えば、セキュリティチップ用ライター６５０など）に送信する送信手段（例えば、ステップＡ１１で認証用情報A２を送信する制御部６１１など）と、を備える、
ことを特徴とする書込装置。
【０２９０】
上記構成によれば、１つの装置によって２つの制御装置に情報を読み書きする必要がないので、情報漏洩のリスクを低減できる。
【０２９１】
（３）所定の遊技用装置（例えば、カードユニット２０など）に搭載される、所定の処理（例えば、パチンコ機１０に搭載された主制御チップ１３などの認証要求を行う処理（ステップＣ３１）など）を行う第２の制御装置（例えば、セキュリティチップ２２など）に情報を書き込む書込装置（例えば、セキュリティチップ用ライター６５０など）であって、
前記所定の処理とは異なる処理（例えば、パチンコ機１０との通信処理（ステップＣ２７）など）を行う第１の制御装置（例えば、通信制御IC２３など）に情報を書き込む他の書込装置（例えば、通信制御IC用ライター６１０など）が前記第１の制御装置から読み取って送信する、前記第１の制御装置に予め記録されている所定情報（例えば、認証用情報A２など）を取得する取得手段（例えば、ステップＡ１１で認証用情報A２を受信する制御部６５１など）と、
前取得手段が取得した前記所定情報を前記第２の制御装置に対して情報を書き込む書込手段（例えば、ステップＡ１６で認証用情報A２を書き込む制御部６５１など）と、を備える、
ことを特徴とする書込装置。
【０２９２】
上記構成によれば、１つの装置によって２つの制御装置に情報を読み書きする必要がないので、情報漏洩のリスクを低減できる。
【０２９３】
（４）上記（１）から（３）いずれかの書込システム又は書込装置において、
前記所定の情報は、前記第１の制御装置を認証するための第１の認証用情報（例えば、認証用情報A２など）であり、
前記第２の制御装置は、前記第１の制御装置から前記第１の認証用情報を取得する取得手段（例えば、ステップＣ２１において認証用情報A２を取得する処理部２２ａなど）と、前記取得手段が取得した前記第１の認証用情報と前記第２の書込装置の前記書込手段によって書き込まれた前記第１の認証用情報とに基づいて前記第１の制御装置を認証する第１認証手段（例えば、ステップＣ２１において認証用情報A２の照合を行う処理部２２ａなど）と、を備える、
ようにしてもよい。
【０２９４】
上記構成によれば、第１の制御装置を認証するための第１の認証用情報が第２の書込装置が読み取る必要が無くなり、認証用情報という重要な情報の漏洩リスクを低減できる。

【０２９５】
（５）上記（１）の書込システムにおいて、

前記第１の書込装置から第２の認証用情報（例えば、認証用情報Ａ１など）を取得し、取得した前記第２の認証用情報に基づいて前記第１の書込装置を認証する第２認証手段（例えば、ステップＡ５において照合を行う制御部３１１など）と、前記第２の書込装置から第３の認証用情報（例えば、認証用情報Ｂ１など）を取得し、取得した前記第３の認証用情報に基づいて前記第２の書込装置を認証する第３認証手段（例えば、ステップＡ７において照合を行う制御部３１１など）と、を備える認証装置をさらに備える、
ようにしてもよい。
【０２９６】
上記認証によって、第１の書込装置や第２の書込装置のすり替えなどを検出できるので、情報漏洩のリスクを低減できる。
【０２９７】
（６）上記（１）から（５）のいずれか１つの書込システム又は書込装置において、
前記第１の書込装置と前記第２の書込装置とは、互いに通信を行って所定の認証用情報（例えば、認証用情報Ａ１や認証用情報Ｂ１など）を用いて相互認証が可能である（変形例参照）、
ようにしてもよい。
【０２９８】
上記認証によって、第１の書込装置や第２の書込装置のすり替えなどを検出できるので、情報漏洩のリスクを低減できる。
【０２９９】
（７）上記（１）から（６）のいずれか１つの書込システム又は書込装置において、
前記第１の制御装置と前記第２の制御装置とは、異なるメーカーで製造され、
前記第１の書込装置と前記第１の制御装置とは、同じメーカーで製造される、
【０３００】
上記構成によれば、第１の書込装置と第１の制御装置とが同じメーカーで製造されるので、第１の書込装置が第１の制御装置から情報を読み取る機能や書き込む機能を他者に開示する必要がなく、情報漏洩のリスクを低減できる。
【０３０１】
（その他２）
（１）所定の処理を行う第１の制御部（例えば、セキュリティチップ２２など）と、前記第１の制御部と暗号通信可能な第２の制御部（例えば、ステップＣ２４以降で暗号通信する通信制御ＩＣ２３など）と、のうちの少なくとも前記第１の制御部を備える遊技用装置（例えば、カードユニットなど）であって、
前記第１の制御部は、所定の情報（例えば、更新情報など）に基づいて前記暗号通信で使用する鍵を生成する第１の生成手段（例えば、ステップＣ１６で更新情報から暗号情報Ａ２を生成する処理部２２ａ）と、前記第２の制御部において前記暗号通信で使用する鍵（例えば、暗号鍵Ａ２など）を生成させる（例えば、ステップＣ１９で更新情報から暗号情報Ａ２を生成するなど）ために前記所定の情報を前記第２の制御部に送信する送信手段（例えば、ステップＣ１８で更新情報を送信する処理部２２ａ）と、を備え、
前記所定の情報は、前記第１の制御部の外部（例えば、鍵管理センターサーバ３１０など）から前記第１の制御部に供給される情報である（例えば、ステップＣ１０、Ｃ１１、Ｃ１５で送信される更新情報など）、
ことを特徴とする遊技用装置。
【０３０２】
上記構成によれば、鍵の生成の基となる所定の情報が外部から供給されるので、第１の制御部や第２の制御部を解析しただけでは、どのような鍵が生成されるか解析しにくいので、暗号通信で使用される鍵の漏洩のリスクを低減できる。
【０３０３】
（２）遊技用システムは、
上記（１）の遊技用装置と、

前記所定の情報を前記遊技用装置の外部から供給する供給装置（例えば、鍵管理センターサーバ３１０など）と、
を備えることを特徴とする。
【０３０４】
上記構成によれば、鍵の生成の基となる所定の情報が供給装置によって外部から供給されるので、第１の制御部や第２の制御部を解析しただけでは、どのような鍵が生成されるか解析しにくいので、暗号通信で使用される鍵の漏洩のリスクを低減できる。
【０３０５】
（３）上記（１）又は（２）の遊技用装置又は遊技用システムにおいて、
前記所定の情報は、前記外部から、暗号化されたままの状態で所定の装置（例えば、ＣＵ制御部２１や上位サーバ５１０など）に中継されて前記第１の制御部に供給され（例えば、ＣＵ制御部２１や上位サーバ５１０は更新情報を復号できないなど）、
前記第１の制御部は、予め記憶している復号鍵を用いて前記所定の情報を復号化する復号化手段（例えば、ステップＣ１６で更新情報を復号化する処理部２２ａなど）を備える、
ようにしてもよい。
【０３０６】
上記構成によれば、所定の情報を中継する所定の装置では所定の情報が復号化されないので、この所定の情報が漏洩することによる、暗号通信で使用される鍵の漏洩のリスクを低減できる。
【０３０７】
（その他３）
（１）所定の装置（例えば、払出制御チップ１１など）を認証する認証制御部（例えば、セキュリティチップ２２など）を備える遊技用装置（例えば、カードユニット２０など）であって、
前記所定の装置は、前記遊技用装置又は他の遊技用装置（パチンコ機１０）に搭載されたものであり、
前記認証制御部は、
前記所定の装置の識別情報を記憶する記憶手段（例えば、チップ情報を記憶する記憶部２２ｂ）と、
前記所定の装置が送信する前記所定の装置の識別情報を取得し、取得した識別情報と、前記記憶手段が記憶する識別情報と、に基づいて前記所定の装置の認証を行う認証手段（例えば、ステップＣ２９で送信されたチップ情報を照合する処理部２２ａ）と、
前記認証手段による認証が失敗だった場合には、前記所定の装置が送信する前記識別情報を前記所定の装置を認証する認証装置（例えば、上位サーバ５１０、鍵管理センターサーバ３１０など）に対して送信し、前記認証装置に対して前記識別情報に基づく前記所定の装置の認証の問い合わせを行い、前記認証手段による認証が成功だった場合には、前記問い合わせを行わない、問い合わせ手段（例えば、照合結果に応じて、ステップＥ６の処理又はステップＧ５、Ｇ６の処理を行う処理部２２ａ）と、を有する、
ことを特徴とする遊技用装置。
【０３０８】
上記構成によれば、認証手段による認証が成功した場合には認証の問い合わせを行わず、認証が失敗した場合には認証装置への認証の問い合わせを行うので、認証手段による認証が成功したような認証装置への問い合わせが不要な場合における認証装置への問い合わせが防止されるので、状況に応じた適切な問い合わせを行うことが出来る。
【０３０９】
（２）所定の装置（例えば、ＣＵ制御部２１など。セキュリティチップ２２であってもよい。）を認証する認証制御部（例えば、セキュリティチップ２２など。ＣＵ制御部２１であってもよい。）を備える遊技用装置（例えば、カードユニット２０など）であって、
前記所定の装置は、前記遊技用装置又は他の遊技用装置（パチンコ機１０）に搭載され

たものであり、
前記認証制御部は、
前記所定の装置の識別情報（例えば、認証用情報Ｃ１など）と、前記所定の装置を認証するための認証用情報（例えば、暗号鍵Ｃ２など）と、を記憶する記憶手段（保持される場合も含む。）と、
前記所定の装置と前記認証用情報を用いた通信を行い、通信状況（暗号通信が出来るか否か）に基づいて前記所定の装置の認証を行う認証手段（例えば、ステップＤ９において暗号鍵Ｃ２を用いて暗号通信を行えない場合を特定する処理部２２ａなど。処理部２１ａであってもよい。）と、
前記認証手段による認証が失敗だった場合には、前記記憶手段が記憶する前記識別情報を前記所定の装置を認証する認証装置（例えば、上位サーバ５１０、鍵管理センターサーバ３１０など）に対して送信し、前記認証装置に対して前記識別情報に基づく前記所定の装置の認証の問い合わせを行い、前記認証手段による認証が成功だった場合には、前記問い合わせを行わない、問い合わせ手段（例えば、暗号鍵Ｃ２を用いて暗号通信を行えない場合に、第１のモードに移行する処理部２２ａなど。ステップＣ８などで鍵管理センターサーバ３１０に対して認証用情報Ｃ１などを送信する処理部２１ａであってもよい。）と、を有する、
ことを特徴とする遊技用装置。
【０３１０】
上記構成によれば、認証手段による認証が成功した場合には認証の問い合わせを行わず、認証が失敗した場合には認証装置への認証の問い合わせを行うので、認証手段による認証が成功したような認証装置への問い合わせが不要な場合における認証装置への問い合わせが防止されるので、状況に応じた適切な問い合わせを行うことが出来る。
【０３１１】
（３）遊技用システムは、
上記（１）又は（２）に記載された遊技用装置と、
認証装置と、を備える遊技用システムであって、
前記遊技用装置は、前記認証装置に前記識別情報を送信し、前記認証装置に対して前記識別情報に基づく前記所定の装置の認証の問い合わせを行う、
ことを特徴とする。
【０３１２】
上記構成によれば、認証手段による認証が成功した場合には認証の問い合わせを行わず、認証が失敗した場合には認証装置への認証の問い合わせを行うので、認証手段による認証が成功したような認証装置への問い合わせが不要な場合における認証装置への問い合わせが防止されるので、状況に応じた適切な問い合わせを行うことが出来る。
【０３１３】
（４）上記（１）から（３）のいずれか遊技用装置又は遊技用システムにおいて、
前記認証装置に送信される前記識別情報は、所定の中間装置（例えば、上位サーバ５１０など）を介して前記認証装置に送信され、
前記問い合わせ手段は、前記認証手段による認証が、前記記憶手段に前記識別情報が記憶されていなかったことによる失敗だった場合には、前記所定の中間装置に対して前記所定の装置の認証（例えば、チップ情報が記憶されているか否かの判別、ステップＦ８参照）の問い合わせを行う（例えば、ステップＦ５及びＦ６などを参照）、
ようにしてもよい。
【０３１４】
上記の構成によれば、さらに、認証の失敗の内容に応じて、中間装置に対しても認証の問い合わせが可能になっているため、状況に応じた適切な問い合わせを行うことが出来る。
【０３１５】
（５）上記（１）から（４）のいずれかの遊技用装置又は遊技用システムにおいて、

前記問い合わせ手段は、前記認証装置から前記認証手段による認証のレベルを指定するレベル指定情報（例えば、制御情報など）が供給された場合には、前記認証のレベルに応じた前記認証手段による認証の結果に基づいて特定される問い合わせ先に対して前記識別情報を送信して、前記識別情報に基づく前記所定の装置の認証の問い合わせを行う（例えば、ステップＨ１からＨ３などを参照）、

ようにしてもよい。

【０３１６】

上記の構成によれば、さらに、問い合わせ先を外部からの指定によって調整できるため、状況に応じて適切な問い合わせが行われる。

【０３１７】

（６）上記（１）から（５）のいずれかの遊技用装置又は遊技用システムにおいて、

前記認証装置に送信される前記識別情報は、前記問い合わせ手段によって暗号化され、暗号化された状態のまま所定の中間装置を介して前記認証装置に送信され、前記認証装置で復号化される（例えば、ステップＣ３１からＣ３３を参照）、

ようにしてもよい。

【０３１８】

上記構成によれば、識別情報は中間装置では暗号化されたままの状態なので、識別情報の漏洩のリスクを低減することが出来る。

【０３１９】

（７）上記（１）から（６）のいずれかの遊技用装置又は遊技用システムにおいて、

前記記憶手段が記憶する前記識別情報は、前記認証装置が記憶する識別情報と同じ内容である（ステップＣ３７で照合ＯＫの場合にチップ情報が記憶されるなど）、

ようにしてもよい。

【０３２０】

上記構成によれば、記憶手段が記憶する識別情報は、正当なものであることが担保されるので、この識別情報を用いた認証の正確性を担保できる。

【０３２１】

（その他４）

（１）所定の装置（例えば、払出制御チップ１１など）を認証する認証制御部（例えば、セキュリティチップ２２など）を備える、遊技場（例えば、遊技場５００など）内に設置された遊技用装置（例えば、カードユニット２０など）と、

前記所定の装置を認証する、前記遊技場外に設置された認証装置（例えば、鍵管理センターサーバ３１０など）と、

を備える遊技用システム（例えば、遊技用システム１など）であって、

前記所定の装置は、前記遊技用装置又は他の遊技用装置（パチンコ機１０）に搭載されたものであり、

前記認証制御部は、前記所定の装置を識別する識別情報を記憶する記憶手段（例えば、チップ情報を記憶する記憶部２２ｂ）と、前記所定の装置が送信する前記所定の装置の識別情報を取得し、取得した識別情報と前記記憶手段が記憶する識別情報とに基づいて前記所定の装置の認証を行う認証手段（例えば、ステップＣ２９で送信されたチップ情報を照合する処理部２２ａ）と、前記所定の装置が送信する前記識別情報を前記認証装置に対して送信し、前記認証装置に対して前記識別情報に基づく前記所定の装置の認証の問い合わせを行う問い合わせ手段（例えば、照合結果に応じて、ステップＧ５、Ｇ６の処理を行う処理部２２ａ）と、を有し、

前記認証装置は、前記認証制御部に前記問い合わせ手段を制御するための制御情報（例えば、制御情報など）を供給する供給手段（例えば、ステップＨ１からＨ３参照）を備え、

前記問い合わせ手段は、前記制御情報の内容に応じて、前記問い合わせを行うか否かを決定する（例えば、ステップＨ３などを参照）、

ことを特徴とする遊技用装置。

【０３２２】
上記構成によれば、問い合わせの有無が認証装置からの制御情報の内容に応じて決定されるので、状況に応じた適切な問い合わせを行うことできる。
【０３２３】
（２）所定の装置（例えば、ＣＵ制御部２１など。セキュリティチップ２２であってもよい。）を認証する認証制御部（例えば、セキュリティチップ２２など。ＣＵ制御部２１であってもよい。）を備える、遊技場（例えば、遊技場５００など）内に設置された遊技用装置（例えば、カードユニット２０など）と、
前記所定の装置を認証する、前記遊技場外に設置された認証装置（例えば、鍵管理センターサーバ３１０など）と、
を備える遊技用システム（例えば、遊技用システム１など）であって、
前記所定の装置は、前記遊技用装置又は他の遊技用装置（パチンコ機１０）に搭載されたものであり、
前記認証制御部は、前記所定の装置を識別する識別情報（例えば、認証用情報Ｃ１）と、前記所定の装置を認証するための認証用情報（例えば、暗号鍵Ｃ２）と、を記憶する記憶手段（例えば、記憶部２２ｂ又は処理部２２ｂなど。記憶部２１ａ、記憶部１２ｂであってもよい。）と、前記所定の装置と前記認証用情報を用いた通信を行い、通信状況に基づいて前記所定の装置の認証を行う認証手段（例えば、ステップＤ９において暗号鍵Ｃ２を用いて暗号通信を行えない場合を特定する処理部２２ａなど。処理部２１ａであってもよい。）と、前記記憶手段が記憶する前記識別情報を前記認証装置に対して送信し、前記認証装置に対して前記識別情報に基づく前記所定の装置の認証の問い合わせを行う問い合わせ手段（例えば、暗号鍵Ｃ２を用いて暗号通信を行えない場合に、第１のモードに移行する処理部２２ａなど。ステップＣ８などで鍵管理センターサーバ３１０に対して認証用情報Ｃ１などを送信する処理部２１ａであってもよい。）と、を有し、
前記認証装置は、前記認証制御部に前記問い合わせ手段を制御するための制御情報（例えば、制御情報など）を供給する供給手段（例えば、ステップＨ１からＨ３参照）を備え、
前記問い合わせ手段は、前記制御情報の内容に応じて、前記問い合わせを行うか否かを決定する（例えば、ステップＨ３参照）、
ことを特徴とする遊技用システム。
【０３２４】
上記構成によれば、問い合わせの有無が認証装置からの制御情報の内容に応じて決定されるので、状況に応じた適切な問い合わせを行うことできる。
【０３２５】
（３）所定の装置（例えば、払出制御チップ１１など）を認証する認証制御部（例えば、セキュリティチップ２２など）を備える、遊技場（例えば、遊技場５００など）内に設置された遊技用装置（例えば、カードユニット２０など）であって、
前記所定の装置は、前記遊技用装置又は他の遊技用装置（パチンコ機１０）に搭載されたものであり、
前記認証制御部は、前記所定の装置を識別する識別情報を記憶する記憶手段（例えば、チップ情報を記憶する記憶部２２ｂ）と、前記所定の装置が送信する前記所定の装置の識別情報を取得し、取得した識別情報と前記記憶手段が記憶する識別情報とに基づいて前記所定の装置の認証を行う認証手段（例えば、ステップＣ２９で送信されたチップ情報を照合する処理部２２ａ）と、前記所定の装置が送信する前記識別情報を、前記所定の装置を認証する、前記遊技場外に設置された認証装置（例えば、鍵管理センターサーバ３１０など）に対して送信し、前記認証装置に対して前記識別情報に基づく前記所定の装置の認証の問い合わせを行う問い合わせ手段（例えば、照合結果に応じて、ステップＧ５、Ｇ６の処理を行う処理部２２ａ）と、を有し、
前記認証装置は、前記認証制御部に前記問い合わせ手段を制御するための制御情報（例えば、制御情報など）を供給する供給手段（例えば、ステップＨ１からＨ３参照）を備え

、
前記問い合わせ手段は、前記制御情報の内容に応じて、前記問い合わせを行うか否かを決定する（例えば、ステップＨ３などを参照）、
ことを特徴とする遊技用装置。
【０３２６】
上記構成によれば、問い合わせの有無が認証装置からの制御情報の内容に応じて決定されるので、状況に応じた適切な問い合わせを行うことできる。
【０３２７】
（４）所定の装置（例えば、ＣＵ制御部２１など）を認証する認証制御部（例えば、セキュリティチップ２２など）を備える、遊技場（例えば、遊技場５００など）内に設置された遊技用装置（例えば、カードユニット２０など）であって、
前記所定の装置は、前記遊技用装置又は他の遊技用装置（パチンコ機１０）に搭載されたものであり、
前記認証制御部は、前記所定の装置を識別する識別情報（例えば、認証用情報Ｃ１）と、前記所定の装置を認証するための認証用情報（例えば、暗号鍵Ｃ２）と、を記憶する記憶手段（記憶部２２ｂ）と、前記所定の装置と前記認証用情報を用いた通信を行い、通信状況に基づいて前記所定の装置の認証を行う認証手段（例えば、ステップＤ９において暗号鍵Ｃ２を用いて暗号通信を行えない場合を特定する処理部２２ａ）と、前記記憶手段が記憶する前記識別情報を、前記所定の装置を認証する、前記遊技場外に設置された認証装置（例えば、鍵管理センターサーバ３１０など）に対して送信し、前記認証装置に対して前記識別情報に基づく前記所定の装置の認証の問い合わせを行う問い合わせ手段（例えば、暗号鍵Ｃ２を用いて暗号通信を行えない場合に、第１のモードに移行する処理部２２ａ）と、を有し、
前記認証装置は、前記認証制御部に前記問い合わせ手段を制御するための制御情報（例えば、制御情報など）を供給する供給手段（例えば、ステップＨ１からＨ３参照）を備え、
前記問い合わせ手段は、前記制御情報の内容に応じて、前記問い合わせを行うか否かを決定する（例えば、ステップＨ３参照）、
ことを特徴とする遊技用装置。
【０３２８】
上記構成によれば、問い合わせの有無が認証装置からの制御情報の内容に応じて決定されるので、状況に応じた適切な問い合わせを行うことできる。
【０３２９】
（５）上記（１）から（４）のいずれかの遊技用システム又は遊技用装置において、
前記問い合わせ手段は、前記制御情報の内容と前記認証手段による認証の結果とに基づいて、前記問い合わせを行うかを特定する（例えば、ステップＨ３参照）、
ようにしてもよい。
【０３３０】
上記構成によれば、前記制御情報の内容と前記認証手段による認証の結果とに基づいて、前記問い合わせを行うので、より状況に応じた適切な問い合わせを行うことできる。
【０３３１】
（６）上記（１）から（５）のいずれかの遊技用システム又は遊技用装置において、
前記外部の装置に送信される前記識別情報は、前記問い合わせ手段によって暗号化され、暗号化された状態のまま所定の中間装置を介して前記外部の装置に送信され、前記外部の装置で復号化される、
ようにしてもよい。
【０３３２】
上記構成によれば、識別情報は中間装置では暗号化されたままの状態なので、識別情報の漏洩のリスクを低減することが出来る。
【０３３３】

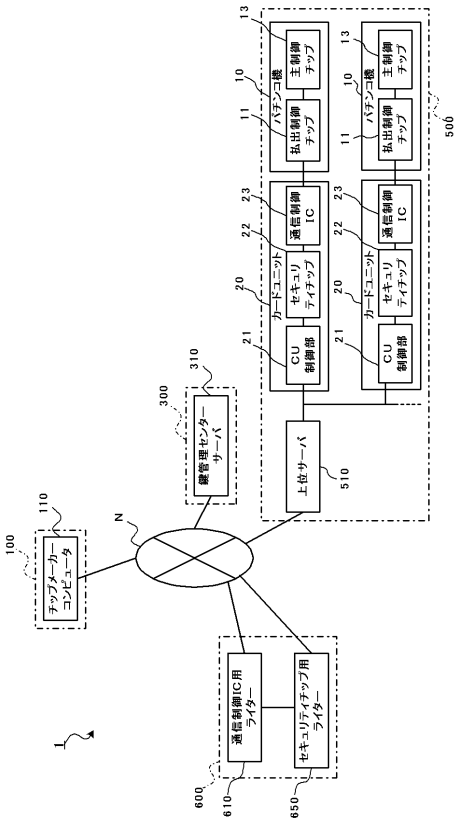
（その他５）
（１）所定の装置（例えば、払出制御チップ１１など）を認証する認証制御部（例えば、セキュリティチップ２２など）を備える、遊技場（例えば、遊技場５００など）内に設置された遊技用装置（例えば、カードユニット２０など）と、
前記遊技場内に設置された場内装置（例えば、上位サーバ５１０など）と、
前記遊技場外に設置された認証装置（例えば、鍵管理センターサーバ３１０など）と、
を備える遊技用システム（例えば、遊技用システム１など）であって、
前記認証制御部は、前記所定の装置を識別する識別情報を記憶する第１の記憶手段（例えば、チップ情報を記憶する記憶部２２ｂ）と、前記所定の装置が送信する前記所定の装置の識別情報を取得する取得手段（例えば、ステップＣ２９でチップ情報を取得する処理部２２ａ）と、前記取得手段が取得した前記識別情報と前記記憶手段が記憶する前記識別情報とに基づいて前記所定の装置の認証を行う第１の認証手段（例えば、ステップＣ２９で取得したチップ情報を用いた照合を行う処理部２２ａなど）と、前記第１の記憶手段が前記識別情報を記憶していない場合に前記取得手段が取得した識別情報を送信する第１の送信手段（例えば、ステップＣ３１でチップ情報を送信する処理部２２ａなど）と、を有し、
前記場内装置は、前記第１の送信手段から送信された前記識別情報を送信する第２の送信手段（例えば、ステップＣ３３でチップ情報を送信する制御部５１１など）を備え、
前記認証装置は、前記所定の装置の識別情報を予め記憶する記憶手段（例えば、記憶部３１２など）と、前記記憶手段が記憶する前記識別情報と前記第２の送信手段が送信した前記識別情報とに基づいて前記所定の装置の認証を行う第２の認証手段（例えば、ステップＣ３４で照合を行う制御部３１１など）と、前記第２の認証手段による認証結果を前記場内装置に供給する供給手段（例えば、ステップＣ３５で照合結果を送信する制御部３１１など）と、を備え、
前記場内装置は、前記供給手段から供給される前記認証結果を前記識別情報とともに記憶する第２の記憶手段（例えば、記憶部５１２など）を備え、
前記第２の送信手段は、前記第１の送信手段が送信した前記識別情報に対応する前記認証結果を前記第２の記憶手段が記憶している場合には、前記識別情報を前記認証装置に送信せずに、前記認証結果を前記認証制御部に送信する（例えば、ステップＦ８以降の処理などを参照）、
ことを特徴とする遊技用システム。
【０３３４】
上記構成によれば、照合結果やチップ情報の記憶状況によって、認証場所を遊技場内外に分けることが出来るため、例えば、他の遊技用装置が他の場所へ移動した場合などであっても、遊技場内での認証によって、前記所定の装置の認証を行うことができ、状況に応じた適切な認証を行うことできる。
【０３３５】
（２）　所定の装置（例えば、払出制御チップ１１など）を認証する認証制御部（例えば、セキュリティチップ２２など）を備える、遊技場（例えば、遊技場５００など）内に設置された遊技用装置（例えば、カードユニット２０など）であって、
前記認証制御部は、
前記所定の装置を識別する識別情報を記憶する記憶手段（例えば、チップ情報を記憶する記憶部２２ｂ）と、
前記所定の装置が送信する前記所定の装置の識別情報を取得する取得手段（例えば、ステップＣ２９でチップ情報を取得する処理部２２ａ）と、
前記取得手段が取得した前記識別情報と前記記憶手段が記憶する前記識別情報とに基づいて前記所定の装置の認証を行う認証手段（例えば、ステップＣ２９で取得したチップ情報を用いた照合を行う処理部２２ａなど）と、
前記記憶手段が前記識別情報を記憶していない場合に前記取得手段が取得した識別情報を送信する送信手段（例えば、ステップＣ３１でチップ情報を送信する処理部２２ａなど

）と、
前記送信手段が送信した前記識別情報に基づく認証の認証結果（例えば、照合結果など）を、前記認証を行う前記遊技場外に設置された認証用装置から前記遊技場内に設置された場内装置（例えば、上位サーバ５１０）を介して受信するか（ステップＣ３５からＣ３７ｂなど）、前記認証結果を前記場内装置が記憶している場合には前記場内装置から受信する（ステップＦ９からＦ１０など）受信手段（例えば、処理部２２ａなど）と、を備える、
ことを特徴とする遊技用装置。
【０３３６】
上記構成によれば、照合結果やチップ情報の記憶状況によって、認証場所を遊技場内外に分けることが出来るため、例えば、他の遊技用装置が他の場所へ移動した場合などであっても、遊技場内での認証によって、前記所定の装置の認証を行うことができ、状況に応じた適切な認証を行うことできる。
【０３３７】
（３）上記（１）又は（２）の遊技用システム又は遊技用装置において、
前記第１の送信手段は、前記識別情報を暗号化して送信し（例えば、ステップＣ３１でチップ情報は暗号化されて送信されるなど）、
前記第２の送信手段は、暗号化されたままの状態で前記識別情報を送信し（例えば、ステップＣ３３で送信されるチップ情報は暗号化されたままなど）、
前記第２の認証手段は、前記第２の送信手段から送信された前記識別情報を復号化してから前記認証を行い（例えば、ステップＣ３３で送信されるチップ情報は暗号化されたままなど）、
前記供給手段は、前記認証結果を暗号化して供給し（例えば、ステップＣ３４での照合などを参照）、
前記第２の記憶手段は、前記認証結果を暗号化したまま記憶し（例えば、ステップＣ３５で送信された照合結果は暗号化されたまま記憶されるなど）、
前記第２の送信手段は、前記認証結果を暗号化したままで送信し（例えば、ステップＣ３６で送信される照合結果は暗号化されたままなど）、
前記認証制御部は、前記第２送信手段が送信した前記認証結果を復号して取得する第２の取得手段を備える（例えば、ステップＣ３７で送信された照合結果を復号化するなど）、
ようにしてもよい。
【０３３８】
上記構成によれば、識別情報は場内装置では暗号化されたままの状態なので、識別情報の漏洩のリスクを低減することが出来る。
【０３３９】
（４）上記（１）から（３）のいずれかの遊技用システム又は遊技用装置において、
前記第１の送信手段は、前記第１の記憶手段に前記識別情報が記憶されており、かつ、前記第１の認証手段による認証が失敗した場合には、前記識別情報を前記認証装置に送信する指示とともに送信し（例えば、ステップＧ５及びＧ６参照）、
前記第２の送信手段は、前記第１の送信手段が前記識別情報を前記指示とともに送信した場合には、前記第２の記憶手段に前記認証結果が記憶されているか否かにかかわらず前記識別情報を前記認証装置に対して送信し（例えば、ステップＧ８参照）、
前記第２の認証手段は、前記第２の送信手段が送信した前記識別情報に基づいて前記認証を行う（例えば、ステップＣ３４参照）、
ようにしてもよい。
【０３４０】
上記構成によれば、第１の記憶手段に前記識別情報が記憶されており、かつ、第１の認証手段による認証が失敗した場合には、遊技場外の認証装置で認証を行うため、状況に応じた適切な認証を行うことが出来る。

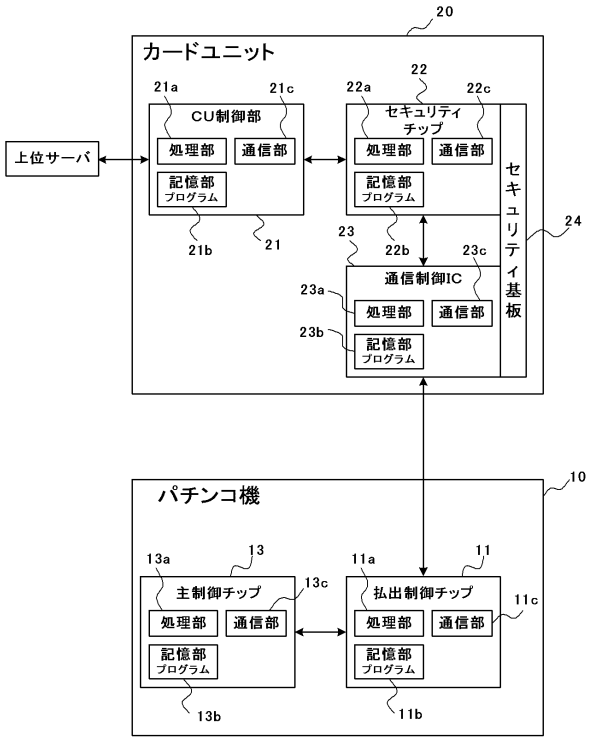
【符号の説明】
【０３４１】
１　遊技用システム
１０　パチンコ機
１１　払出制御チップ
１１ａ　処理部
１１ｂ　記憶部
１１ｃ　通信部
１３　主制御チップ
１３ａ　処理部
１３ｂ　記憶部
１３ｃ　通信部
２０　カードユニット
２１　ＣＵ制御部
２１ａ　処理部
２１ｂ　記憶部
２１ｃ　通信部
２２　セキュリティチップ
２２ａ　処理部
２２ｂ　記憶部
２２ｃ　通信部
２３　通信制御ＩＣ
２３ａ　処理部
２３ｂ　記憶部
２３ｃ　通信部
１００　チップメーカー
１１０　チップメーカーコンピュータ
１１１　制御部
１１２　記憶部
１１３　入出力部
１１４　システムバス
３００　鍵管理センター
３１０　鍵管理センターサーバ
３１１　制御部
３１２　記憶部
３１３　入出力部
３１４　システムバス
５００　遊技場
５１０　上位サーバ
５１１　制御部
５１２　記憶部
５１３　入出力部
５１４　システムバス
６００　カードユニットメーカー
６１０　通信制御ＩＣ用ライター
６１１　制御部
６１２　記憶部
６１３　入出力部
６１４　システムバス
６１５　書込読取部

６５０　セキュリティチップ用ライター
６５１　制御部
６５２　記憶部
６５３　入出力部
６５４　システムバス
６５５　書込読取部

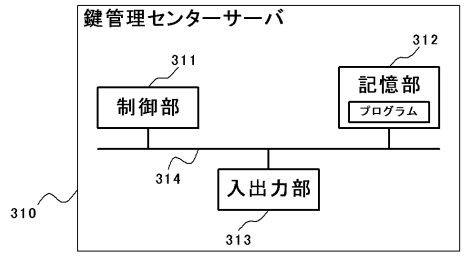
【図１】



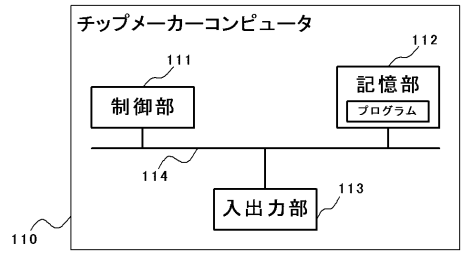
【図２】



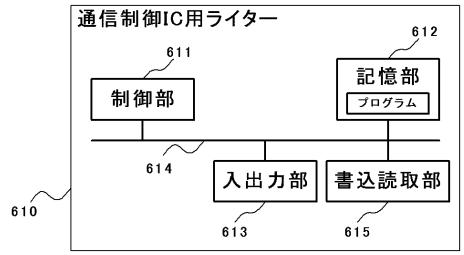
【図３】



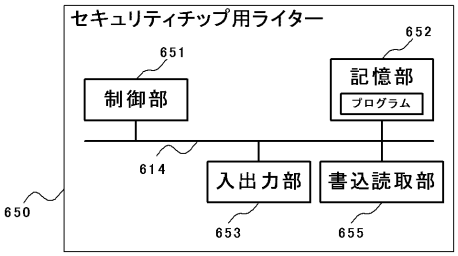
【図４】



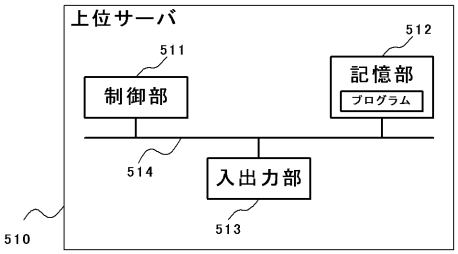
【図５】



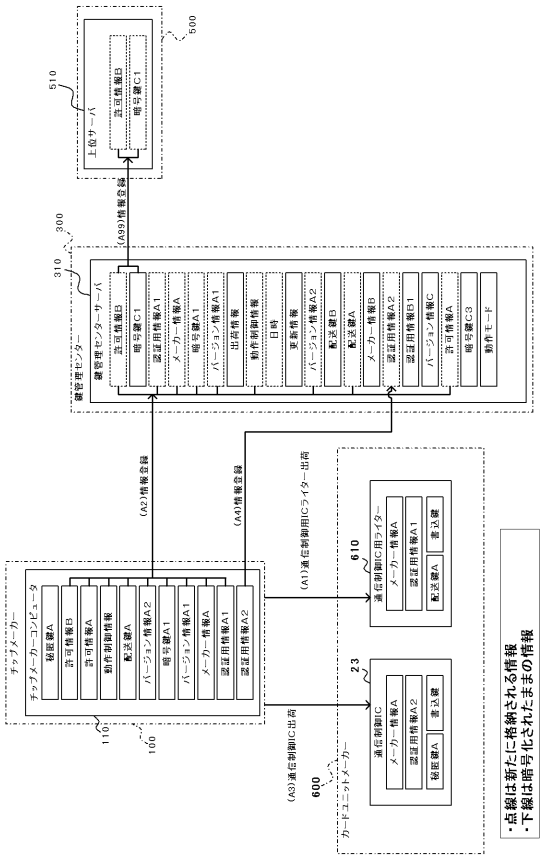
【図６】



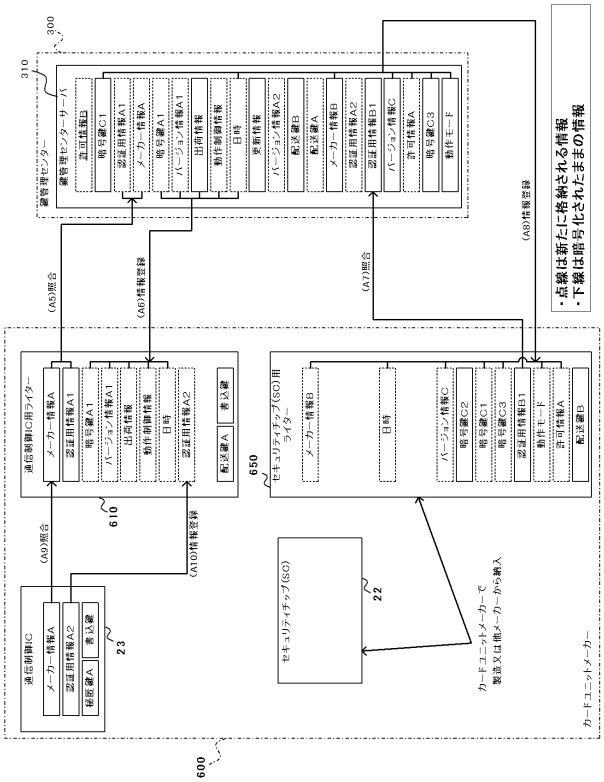
【図７】



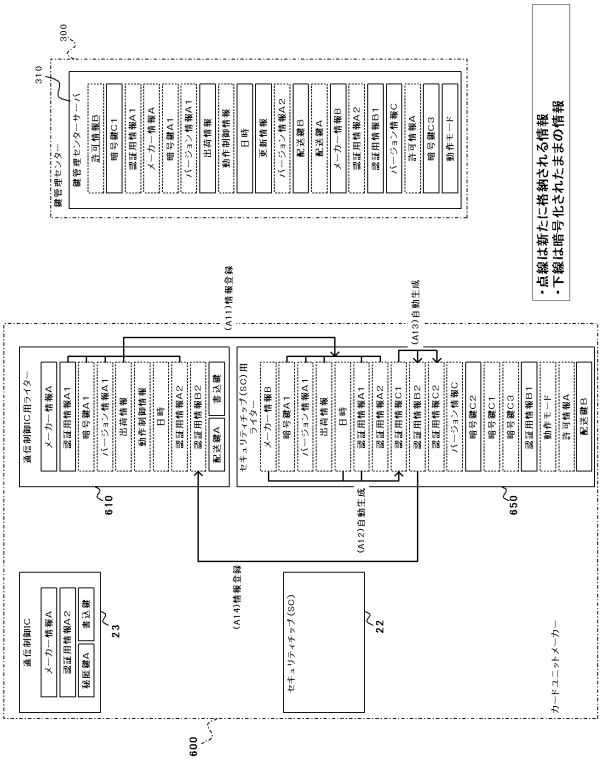
【図８】



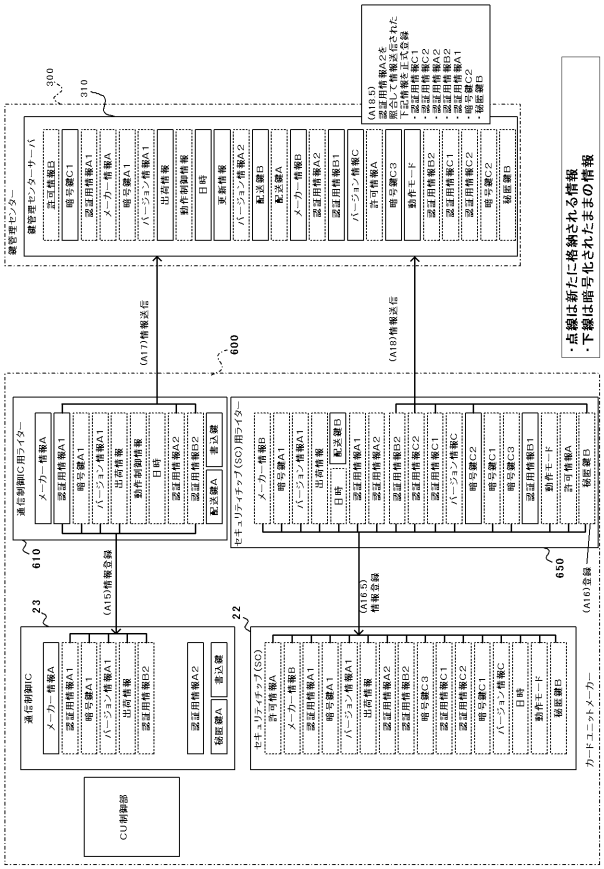
【図９】



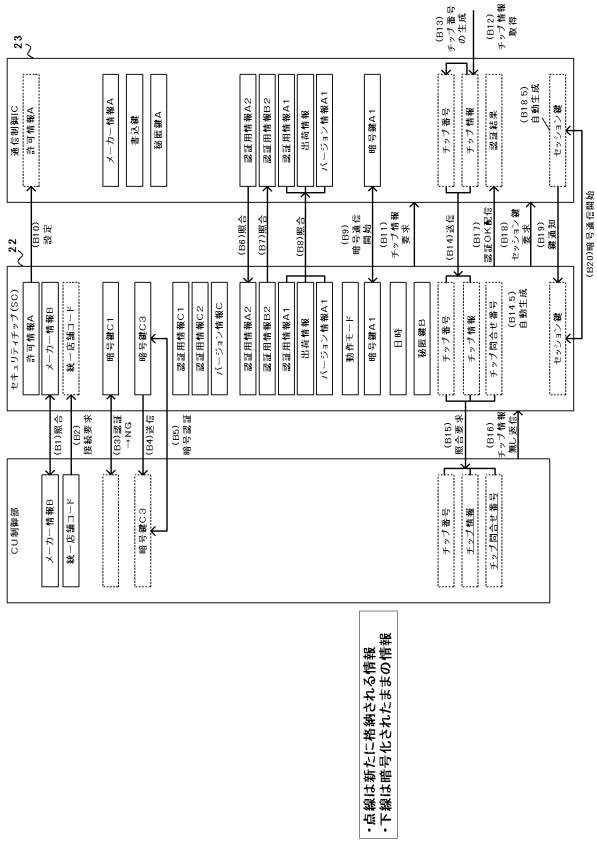
【図１０】



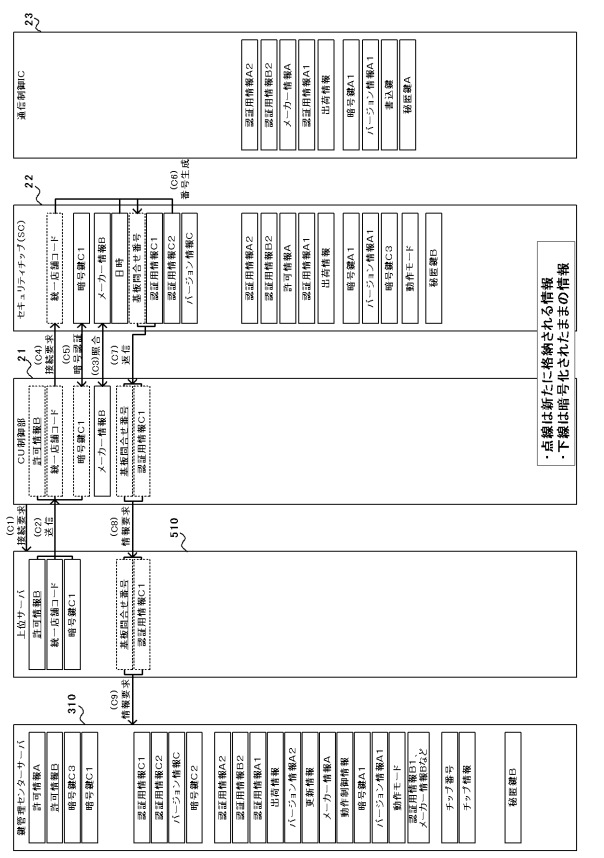
【図１１】



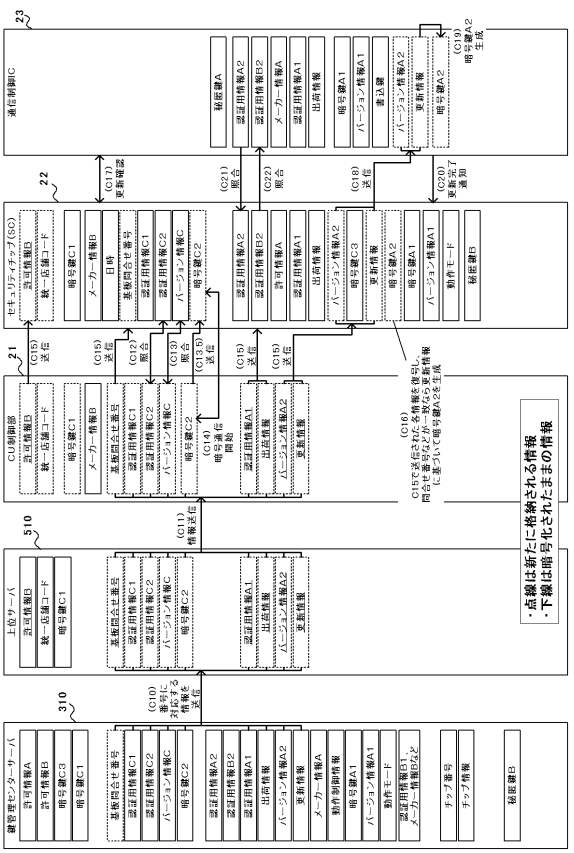
【図１２】



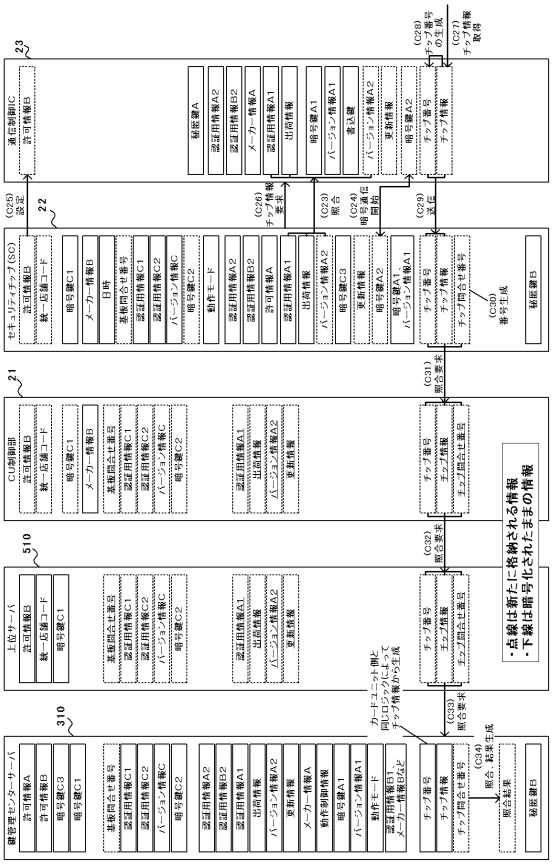
【図１３】



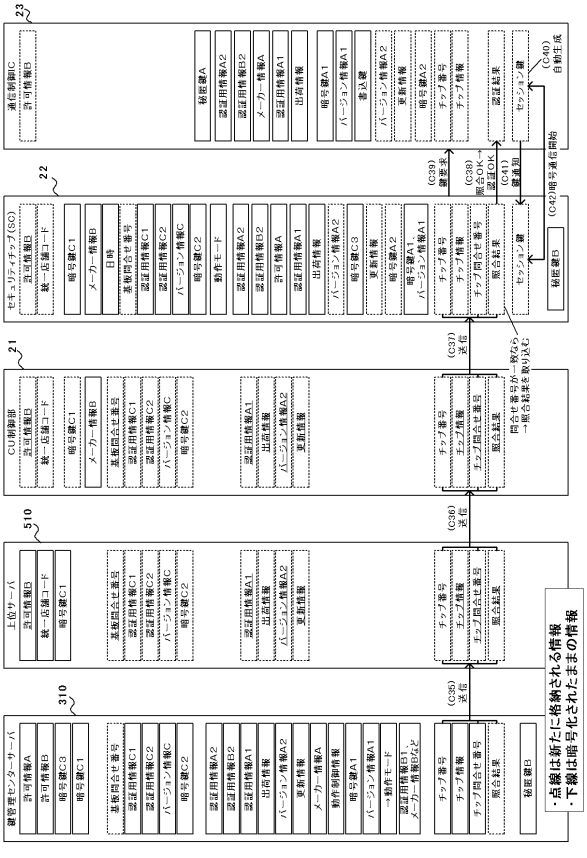
【図１４】



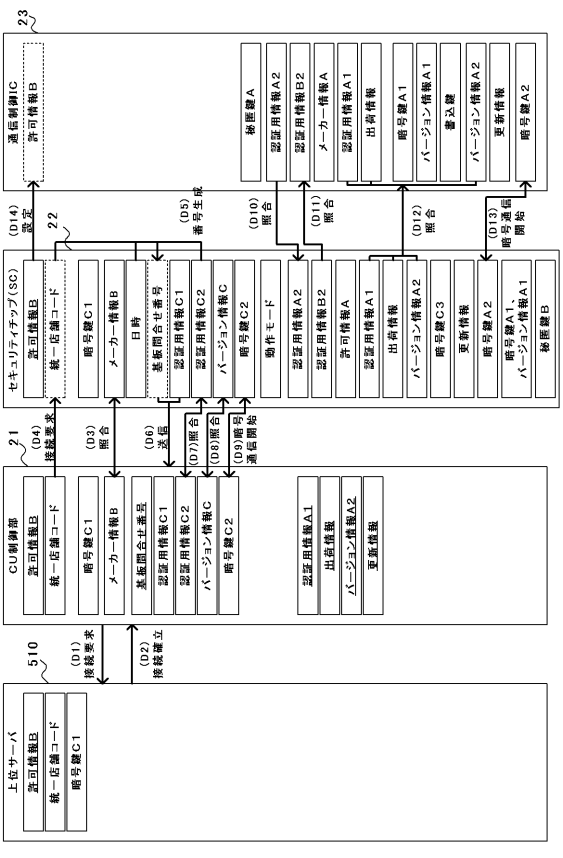
【図１５】



【図１６】



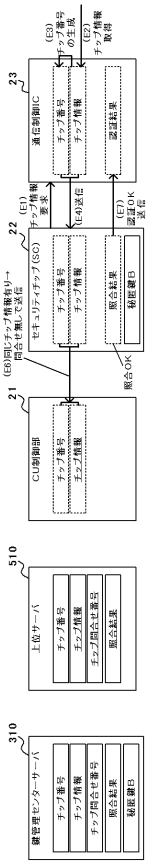
【図１７】



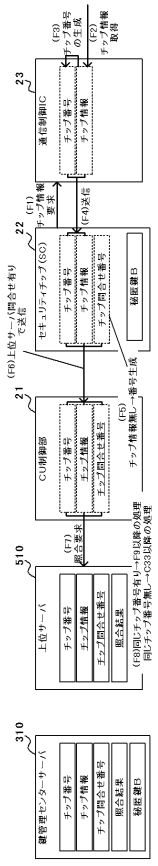
【図１８】

モード名	条件等	行われる処理
第1モード	暗号鍵C2が記録されていない D8又はD9がNGの場合	C5～C25の処理
第2モード	上記以外の場合で、 暗号鍵C2が記録されている	D5～D14の処理

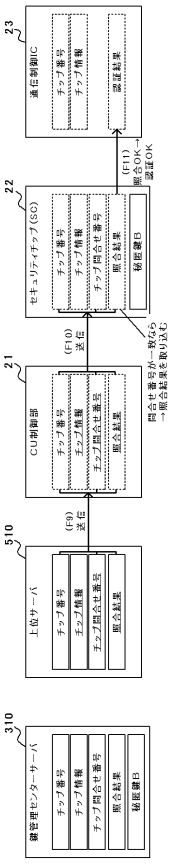
【図１９】



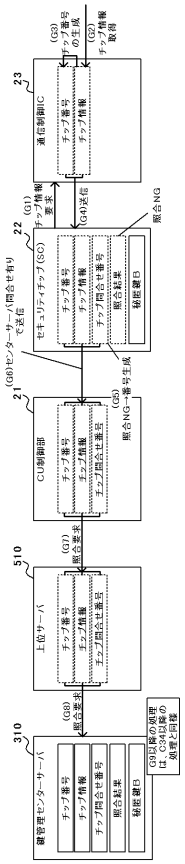
【図２０】



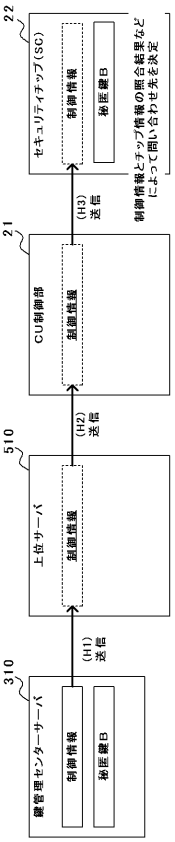
【図２１】



【図２２】


鍵管理センターサーバ
チップ番号
チップ情報
チップ問合せ番号
照合結果
秘匿鍵B
秘匿鍵B
(G5)照合要求
(G6)センターサーバ(問合せ有り)で送信
上位サーバ
(G7)照合要求
CU制御部
(G5)NG→番号生成
通信制御IC
(G1)チップ情報要求
(G4)送信
セキュリティチップ(SC)
照合NG
(G2)チップ情報取得
(G3)チップ番号の送信

【図２３】


鍵管理センターサーバ
制御情報
秘匿鍵B
(H1)送信
上位サーバ
(H2)送信
CU制御部
(H3)送信
セキュリティチップ(SC)
制御情報
秘匿鍵B
制御情報とチップ情報の照合結果などによって問い合わせ先を決定

フロントページの続き

審査官　小河　俊弥

(56)参考文献　特開２０１０－２０１０２２（ＪＰ，Ａ）
特開２００４－１９９８２７（ＪＰ，Ａ）
特開２００３－１８６５６０（ＪＰ，Ａ）
特開平０５－００３９５７（ＪＰ，Ａ）
特許第５２９０３７５（ＪＰ，Ｂ２）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ａ６３Ｆ　　７／０２
Ａ６３Ｆ　　５／０４