

【公報種別】特許法第 17 条の 2 の規定による補正の掲載
 【部門区分】第 1 部門第 2 区分
 【発行日】平成26年12月4日(2014.12.4)

【公開番号】特開2014-100535(P2014-100535A)
 【公開日】平成26年6月5日(2014.6.5)
 【年通号数】公開・登録公報2014-029
 【出願番号】特願2013-218359(P2013-218359)
 【国際特許分類】

A 6 3 F 7/02 (2006.01)

【F I】

A 6 3 F 7/02 3 2 6 Z

A 6 3 F 7/02 3 3 4

A 6 3 F 7/02 3 5 2 F

A 6 3 F 7/02 3 5 2 L

A 6 3 F 7/02 3 5 2 N

【手続補正書】

【提出日】平成26年10月20日(2014.10.20)

【手続補正 1】

【補正対象書類名】特許請求の範囲

【補正対象項目名】全文

【補正方法】変更

【補正の内容】

【特許請求の範囲】

【請求項 1】

遊技媒体を循環させる循環経路を有する封入式遊技機と、互いに通信可能な第 1 の制御手段と第 2 の制御手段とを備えた遊技用システムであって、

前記第 1 の制御手段と前記第 2 の制御手段とで互いに認証方式の異なる複数種類の相互認証を行なう相互認証手段と、

前記相互認証手段による各相互認証の単独での認証結果が不適正な場合に該単独での認証結果を認証相手の制御手段に通知せず、前記複数種類の相互認証すべてを実行した結果の異常を総括して、認証相手の制御手段に通知する総括通知手段と、

該相互認証手段による認証結果が適正なことを条件として、前記第 1 の制御手段と前記第 2 の制御手段との間での暗号通信に用いる通信鍵を生成する通信鍵生成手段とを備え、

前記第 1 の制御手段と前記第 2 の制御手段とは、前記通信鍵生成手段により生成された通信鍵を用いて暗号通信を行なう、遊技用システム。

【請求項 2】

遊技場に設置され、遊技媒体を循環させる循環経路を有する封入式遊技機と通信可能に接続された遊技用装置であって、

互いに通信可能に接続された第 1 の制御手段と第 2 の制御手段と、

前記第 1 の制御手段と前記第 2 の制御手段とで互いに認証方式の異なる複数種類の相互認証を行なう相互認証手段と、

前記相互認証手段による各相互認証の単独での認証結果が不適正な場合に該単独での認証結果を認証相手の制御手段に通知せず、前記複数種類の相互認証すべてを実行した結果の異常を総括して、認証相手の制御手段に通知する総括通知手段と、

該相互認証手段による認証結果が適正なことを条件として、前記第 1 の制御手段と前記第 2 の制御手段との間での暗号通信に用いる通信鍵を生成する通信鍵生成手段とを備え、

前記第 1 の制御手段と前記第 2 の制御手段とは、前記通信鍵生成手段により生成された通信鍵を用いて暗号通信を行なう、遊技用装置。

【手続補正２】

【補正対象書類名】明細書

【補正対象項目名】０００６

【補正方法】変更

【補正の内容】

【０００６】

（１）本発明は、遊技媒体を循環させる循環経路を有する封入式遊技機と、互いに通信可能な第１の制御手段（メイン制御部３２３、またはＣＵ３、Ｐ台２、Ｚカウンタ、ＰＯＳ端末等）と第２の制御手段（ＣＵ通信制御部８０、またはＣＵ３、Ｐ台２、Ｚカウンタ、ＰＯＳ端末等）とを備えた遊技用システムであって、

前記第１の制御手段と前記第２の制御手段とで互いに認証方式の異なる複数種類の相互認証を行なう相互認証手段（図８３、図８４のＣＵ通信制御部認証シーケンス）と、

前記相互認証手段による各相互認証の単独での認証結果が不適正な場合に該単独での認証結果を認証相手の制御手段に通知せず、前記複数種類の相互認証すべてを実行した結果の異常を総括して、認証相手の制御手段に通知する総括通知手段と、

該相互認証手段による認証結果が適正なことを条件として、前記第１の制御手段と前記第２の制御手段との間での暗号通信に用いる通信鍵を生成する通信鍵生成手段（図７、図２０のセッション鍵を本認証鍵と乱数とから生成する）とを備え、

前記第１の制御手段と前記第２の制御手段とは、前記通信鍵生成手段により生成された通信鍵を用いて暗号通信を行なう（図７、図２０のセッション鍵を使用して通信する）。

【手続補正３】

【補正対象書類名】明細書

【補正対象項目名】００１０

【補正方法】変更

【補正の内容】

【００１０】

（３）本発明の他の態様は、遊技場に設置され、遊技媒体を循環させる循環経路を有する封入式遊技機と通信可能に接続された遊技用装置（カードユニット３）であって、

互いに通信可能に接続された第１の制御手段（メイン制御部３２３）と第２の制御手段（ＣＵ通信制御部８０）と、

前記第１の制御手段と前記第２の制御手段とで互いに認証方式の異なる複数種類の相互認証を行なう相互認証手段（図８３、図８４のＣＵ通信制御部認証シーケンス）と、

前記相互認証手段による各相互認証の単独での認証結果が不適正な場合に該単独での認証結果を認証相手の制御手段に通知せず、前記複数種類の相互認証すべてを実行した結果の異常を総括して、認証相手の制御手段に通知する総括通知手段と、

該相互認証手段による認証結果が適正なことを条件として、前記第１の制御手段と前記第２の制御手段との間での暗号通信に用いる通信鍵を生成する通信鍵生成手段（図７、図２０のセッション鍵を本認証鍵と乱数とから生成する）とを備え、

前記第１の制御手段と前記第２の制御手段とは、前記通信鍵生成手段により生成された通信鍵を用いて暗号通信を行なう（図７、図２０のセッション鍵を使用して通信する）。