

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.

G06F 1/00 (2006.01)

G06F 12/14 (2006.01)



[12] 发明专利说明书

专利号 ZL 200410094192.3

[45] 授权公告日 2008 年 2 月 13 日

[11] 授权公告号 CN 100368952C

[22] 申请日 2001. 12. 20

[21] 申请号 200410094192.3

分案原申请号 01140394.2

[30] 优先权

[32] 2000. 12. 20 [33] JP [31] 387833/2000

[73] 专利权人 世嘉股份有限公司

地址 日本东京都

[72] 发明人 见吉隆夫 节政晓生

[56] 参考文献

CN1249873A 2000. 4. 5

US5341429A 1994. 8. 23

EP1016960A1 2000. 7. 5

审查员 刘 栩

[74] 专利代理机构 中原信达知识产权代理有限责
任公司

代理人 谷惠敏 袁炳泽

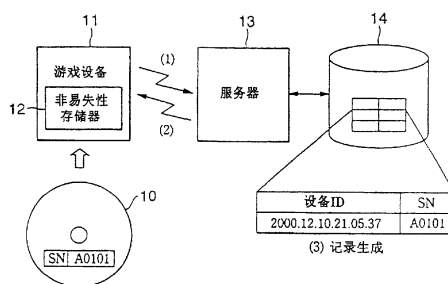
权利要求书 1 页 说明书 14 页 附图 7 页

[54] 发明名称

安全系统

[57] 摘要

本发明提供一种安全系统，用于管理预先不具有识别信息的游戏设备中使用的 CD-ROM 在哪个游戏设备被使用。游戏设备(11)通过通信网络访问服务器(13)时，将由服务器(13)分配的设备 ID 存储在非易失性存储器(12)中。根据游戏设备(11)通过通信网络访问服务器(13)的时间(例如 2000 年 12 月 10 日 21 时 5 分 37 秒)生成该设备 ID。服务器(13)将在游戏设备(11)中使用的 CD-ROM(10)的序列号(SN)与游戏设备(10)的设备 ID 相关联并登录在数据库(14)中。据此，可以管理哪一个 CD-ROM(10)在哪个游戏设备(11)中使用。



1. 一种安全系统，包括：将设有备份存储器的数据处理装置连接至通信网络的次数登录在数据库、同时又将上述次数记录在备份存储器或者数据处理装置中的装置；以及在设有备份存储器的数据处理装置连接至通信网络时，在由数据处理装置取得的上述次数与数据库中登录的次数一致的情况下，才允许对备份存储器内的数据进行处理装置。

2. 根据权利要求1所述的安全系统，其中，使用具有备份存储器的数据处理装置连接至通信网络的时间或者利用该时间的信息，作为上述备份存储器中固有的识别信息。

3. 一种保存数据的管理方法，包括以下各步骤：将具有备份存储器的数据处理装置连接至通信网络的次数登录在数据库、同时又将上述次数记录在备份存储器或者数据处理装置中；以及在具有备份存储器的数据处理装置连接至通信网络时，在由数据处理装置取得的上述次数与数据库中登录的次数一致的情况下，才允许对备份存储器内的数据进行处理。

4. 根据权利要求3所述的保存数据的管理方法，其中，使用具有备份存储器的数据处理装置连接至通信网络的时间或者利用该时间的信息，作为上述备份存储器中固有的识别信息。

安全系统

本申请本申请是申请日为 2001 年 12 月 20 日、申请号为 01140394.2、发明名称为“安全系统”的中国专利申请的分案申请。

技术领域

本发明涉及把多个游戏设备连接到网络进行的通信游戏的改进技术。

背景技术

有人曾提出一种把多个游戏设备连接到电话线路、ISDN 网等通信网络进行通信游戏方案。对于上述通信游戏，为了防止第三者非法使用记录有游戏软件的记录媒介，在特开平 2000-35885 号中提出记录媒介的安全技术方案。

上述公报记载的技术为，服务器对记录游戏软件的记录媒介中的固有识别信息和游戏设备中的固有识别信息进行一元化管理，通过把握哪一个游戏设备使用哪一个记录媒介，把游戏设备连接到通信网络时，当服务器判断那一个游戏设备中装着的记录媒介为以前其他游戏设备中使用的记录媒介时，对游戏处理设置限制，当服务器判断为只在该游戏设备中使用的记录媒介时进行通常的游戏处理。

但是，由于游戏设备中的固有识别信息不一定是游戏设备开发阶段预先装入的，所以也存在不具有这样的识别信息的游戏设备。

此外，在通信游戏中，虽然通过使游戏的进行状况和游戏者获得的各种项目等数据躲避保存在从游戏设备主体或者操作用控制器上可以装卸的备份存储器中，可以从游戏结束前的状态再一次进行游戏，

但由于通过复制备份存储器的内容，可以将自己的保存数据（例如项目）提供给第三者，该第三者就可以利用他人的保存数据享受游戏。象这样，如果很容易地复制备份存储器的内容，就会产生游戏者无法体验游戏乐趣的缺点。

这样的问题也会在将从游戏设备主体或者操作用控制器上可以装卸的备份存储器装入他人的游戏设备主体或者操作用控制器中进行游戏的情况下发生。

此外，也会有以下被非法使用的担心，即虽然躲避保存在备份存储器中的保存数据可以通过通信网络由游戏设备向其他游戏设备传送，但由备份存储器向游戏设备传送数据时，如果在备份存储器内残留着保存的数据，通过将备份存储器从游戏设备中强制拔出，就可以将自己的备份存储器中的保存数据原封不动地提供给他人。

此外，在现有的通信游戏中，由于没有对可以参加游戏的级别设置限制，例如初学者与高级别游戏者同时参加通信游戏的情况下，初学者即使什么也不做，只跟在高级别游戏者的后面就可以亦步亦趋地跟到游戏的结尾，结果使游戏的乐趣减半。

同样，多个游戏者参加通信游戏的情况下，如果躲避保存有关游戏进行状况的保存数据，初学者就可以通过与高级别游戏者共同参加游戏，从高级别游戏者的一局的中途参加游戏。如果在初学者的备份存储器中保存有关游戏进行状况的保存数据，下次游戏就可以从该中途开始进行，由于这样使游戏的一部分不能进行，因而，这是所不希望的。

此外，在通信游戏的情况下，由于只要连接电话线路，就要缴纳作为连接费的电话费，还要向互联网服务提供商缴纳互联网连接费，所以如果在游戏者不需要操作的游戏结束上花费不必要的过长时间，

结果就会导致尽管游戏者没有进行游戏，也会被强制承担过大的经济负担。

因此，本发明提出防止第三者非法使用记录媒介的安全系统、数据处理装置、记录媒介管理方法以及记录用于执行该方法的程序的计算机可读的记录媒介的方案。此外，本发明还提出防止非法使用备份存储器的数据处理装置、数据处理方法、安全系统、保存数据的管理方法以及记录用于执行该方法的程序的计算机可读的记录媒介的方案。此外，本发明还提出为使通信游戏更有趣的游戏服务器、游戏处理方法以及记录用于执行该方法的程序的计算机可读的记录媒介的方案。

发明内容

为了解决上述问题，在本发明中为连接通信网络的数据处理装置分配固有识别信息，使该数据处理装置中固有的识别信息与记录由该数据处理装置所处理的数据的记录媒介中固有的识别信息相关联并进行存储，通过参照该关联来管理哪一个记录媒介在哪一个数据处理装置被使用。由于服务器通过通信网络分配数据处理装置的识别信息，即使是预先没有固有识别信息的数据处理装置，也可以确保记录媒介的安全性。

此外，本发明还可以提供一种计算机可读的记录媒介，记录使计算机系统执行上述方法的程序。作为计算机可读的记录媒介，除了例如光盘（CD-ROM、DVD-ROM、DVD-RAM、DVD-R、PD 盘、MD 盘、MO 盘等具有固有物理格式的盘）和软磁盘（FD）的可移动记录媒介之外，还可以为 RAM 和 ROM 等计算机内的内部存储装置，或者如硬盘的外部存储装置等。

此外，在本发明中，将数据处理装置中固有的识别信息作为密钥，对备份存储器的保存数据进行加密处理。据此，由于备份存储器内的

保存数据在其他的数据处理装置中无法使用，可以防止非法使用保存数据。

此外，在本发明中，把由数据处理装置中进行数据处理的保存数据传送到数据处理装置后，消去备份存储器内非易失性存储器中存储的保存数据。据此，可以有效地防止将残留在该备份存储器内的保存数据原封不动地传送到其他的数据处理装置中的非法使用。

此外，在本发明中，将具有备份存储器的数据处理装置连接到通信网络的次数登录在数据库中，同时又将上述次数记录在备份存储器或者数据处理装置中。在具有备份存储器的数据处理装置连接到通信网络时，由数据处理装置取得的上述次数与数据库中登录的次数一致的情况下，才允许对备份存储器内的数据进行处理。因此，可以有效地防止非法复制备份存储器内的保存数据。

此外，在本发明中，对应于游戏的难易度，预先设定可参加通信游戏的级别，只有对于满足对应游戏难易度的要求级别的游戏者才被允许参加通信游戏。据此，可以克服初学者通过与高级别游戏者共同参加游戏，借助高级别游戏者的力量进行游戏的上述缺点。

此外，在本发明中，连接通信网络进行通信游戏时，不将游戏的进行状况作为保存数据保存。此外，即使是在游戏设备保存游戏进行状况的情况下，也可以禁止在不连接通信网络进行游戏时，参照该进行状况从一局的中途参加游戏。据此，可以克服上述缺点。

此外，在本发明中，连接通信网络进行通信游戏时缩短了游戏结束画面的显示时间。据此，抑制了通信网络的连接费和连接到游戏服务器的互联网连接费的增长。

附图说明

图 1 为记录媒介的安全系统的说明图。

图 2 为游戏设备和控制器的说明图。

图 3 为游戏设备和控制器的外观说明图。

图 4 为表示游戏设备和通信网络的连接结构的说明图。

图 5 为表示保存数据移动的说明图。

图 6 为备份存储器的安全系统的说明图。

图 7 为备份存储器的非法复制对策的说明图。

图 8 为通信游戏的说明图。

图 9 为可参加通信游戏级别的说明图。

图 10 为游戏展开的剧情的说明图。

图 11 为关于游戏进行的标记数据的保存的流程图。

图 12 为游戏结束画面的说明图。

具体实施方式

〈发明实施例 1〉

图 1 为防止第三者非法使用记录媒介的服务器和游戏设备的说明图。本图中，标号 10 为 CD-ROM 等记录游戏软件的可移动记录媒介，标号 11 为家庭用游戏设备。游戏设备 11 读取记录在记录媒介 10 上的游戏程序，通过电话线路、ISDN 网等各种公共线路或专用线等通信网络与其他游戏设备共同进行通信游戏，具有预期的通信功能。服务器 13 管理与通信网络连接的各个游戏设备的通信游戏处理。

记录媒介 10 上被标有被称为序列号 (SN) 的各记录媒介的固有识别信息。本图示例中记录媒介的 SN 为 A0101。SN 可以作为数据记录在记录媒介 10 上，也可以记载在记录媒介或者其收藏容器、说明书上。游戏设备 11 如果通过通信网络访问服务器 13 (本图 (1))，服务器 13 就会要求游戏设备 11 传送游戏设备 11 的设备 ID 和记录媒介 10 的 SN。所谓的设备 ID 是由服务器 13 分配的对于各游戏设备不重复的识别信息。

游戏设备 11 第一次访问服务器 13 的情况下, 由于游戏设备 11 未被分配设备 ID, 服务器 13 会为游戏设备 11 分配一个设备 ID (本图 (2))。可以利用游戏设备 11 访问服务器的时间作为设备 ID。时间中包括公历年、月、日、时、分、秒。例如, 访问服务器的时间为 2000 年 12 月 10 日 21 时 5 分 37 秒的情况下, 设备 ID 为 2000.12.10.21.05.37。游戏设备 11 将由服务器 13 分配的设备 ID 存入闪速存储器等非易失性存储器中。此外, 也可以将该时间加密后的数据作为设备 ID 存入非易失性存储器 12。

在数据库 14 中, 设备 ID 作为密钥与游戏设备中使用的记录媒介的 SN 相关联, 作为一个记录单位来管理。服务器 13 生成一个将为游戏设备 11 分配的设备 ID (2000.12.10.21.05.37) 与 SN (A0101) 相关联的记录 (图 (3))。

根据上述结构, 由于服务器 13 将游戏设备 11 的设备 ID 和记录媒介 10 的 SN 相关联进行一元化管理, 第三者将其他游戏设备上使用的记录媒介插入自己的游戏设备内使用时, 由于该记录媒介的 SN 与游戏设备的设备 ID 不一致, 服务器就会限制该第三者使用记录媒介。

此外, 考虑到几乎没有 2 人以上的游戏者包含秒单位同时访问服务器的情况, 利用游戏设备 11 访问服务器 13 包含秒单位的时间作为设备 ID, 实际上就能将各个游戏设备固有的设备 ID 区分开来。当然, 不仅游戏设备访问服务器的时间, 也可以利用预先准备的不重复的 ID 作为设备 ID。

上述的说明是以 CD-ROM 作为记录媒介的例子来说明的, 但本发明不限于此, 也适用于 DVD-ROM、DVD-RAM、DVD-R、PD 盘、MD 盘、MO 盘等各种光盘、软磁盘 (FD)、存储游戏程序的装卸式盒式磁带、存储器卡等。

〈发明实施例 2〉

图 3 为游戏设备和操作用控制器的说明图。为了可以在操作用控制器 20 中躲避存储保存数据而设置有可以自由装卸的备份存储器 22, 还设有配置有模拟键和各种开关的操作部件 21。备份存储器 22 具有非易失性存储器。操作用控制器 20 通过连接软线 28 以及连接器 29 与游戏设备 23 连接。此外, 也可以设置为把备份存储器 22 直接自由装卸地安装在游戏设备 23 上的结构。

图 2 为游戏设备和操作用控制器的功能框图。游戏设备 23 由游戏处理单元 24、加密处理单元 25、CD-ROM 驱动器 26、设备 ID 存储器 27 构成。上述各个模块由 CPU、ROM、RAM 等硬件实现。游戏处理单元 24 通过 CD-ROM 驱动器 26 读取由 CD-ROM 提供的游戏程序, 根据由操作部件 21 输出的模拟键和各种开关的控制信号展开游戏, 生成躲避保存到备份存储器 22 的保存数据。

游戏者是否向游戏设备 23 发出将保存数据躲避存入备份存储器 22 的指示, 如果在游戏程序进行程序处理的过程中向游戏设备 23 发出将保存数据躲避存入备份存储器 22 的指示, 则加密处理单元 25 将存储在设备 ID 存储器 27 内的游戏设备 23 的固有信息 (例如制造编号) 作为密钥, 对保存数据进行加密处理, 并躲避存入备份存储器 22 中。加密处理可以利用公知的加密处理方法。另一方面, 游戏设备 23 读取备份存储器 22 内存储的保存数据时, 通过加密处理单元 25 将设备 ID 作为密钥对保存数据进行解码处理, 然后由游戏处理单元 24 输出。

根据上述结构, 由于将游戏设备 23 的固有信息作为密钥对备份存储器 22 内保存的数据进行加密处理, 所以在其他的游戏设备中无法使用。因此, 可以有效地防止利用他人的备份存储器在自己的游戏设备上玩游戏等的备份存储器的非法使用。

〈发明实施例 3〉

图 4 为多个游戏设备与通信网络连接进行游戏的说明图。在本图中，标号 32、34 为家庭用游戏设备，35 为控制通信游戏的服务器。标号 36 为公共线路等通信网络。游戏设备 32 与具有用于躲避存储保存数据的备份存储器 310 的操作用控制器 31 连接。同样，游戏设备 34 也与具有备份存储器 330 的操作用控制器 33 连接。通信网络 36 的通信协议使用与开放网络相适应的 TCP/IP。

游戏设备 32 随着游戏的进行，将游戏者获得的项目、分数、游戏进行状况等适当地写入 RAM320。写入 RAM320 的数据可以作为保存数据传送给备份存储器 310。此外，游戏者获得的项目等可以通过通信网络 36 传送给游戏设备 34 的 RAM340。

图 5 为表示利用躲避存入备份存储器的保存数据，进行通信游戏时的备份存储器的状态的说明图。备份存储器 310 中躲避存储有项目等保存数据。游戏设备 23 与通信网络连接时，备份存储器 310 内的保存数据就会传送（移动）给游戏设备 23 的 RAM320，然后消去备份存储器 310 内的保存数据。因此，游戏设备 23 与通信网络 36 连接期间，备份存储器 310 内的保存数据处于空的状态。游戏结束时，RAM320 内的保存数据躲避存入备份存储器 310 时，保存数据由 RAM320 向备份存储器 310 传送。

过去，由于备份存储器 310 的保存数据传送到 RAM320 时，是将保存数据复制然后传送，所以即使将保存数据传送到 RAM320 后，备份存储器 310 内仍躲避存储有保存数据。因此，即使在游戏者向其他游戏者提供保存数据中的参数的一部分或全部的情况下，其后通过将备份存储器 310 从操作用控制器 31 中强制抽取，也可以将他人提供的保存数据存入自己的备份存储器 310 内。

但是，通过本实施例，由于备份存储器 310 内的保存数据不是向

RAM320 内复制，而是移动到 RAM320 内，所以可以有效地防止上述备份存储器的非法使用。

〈发明实施例 4〉

图 6 为控制通信游戏的服务器和游戏设备的说明图。本图中，标号 41 为家庭用游戏设备，通过访问服务器 44 可以进行通信游戏。游戏设备 41 根据由操作用控制器 42 提供的游戏者的操作信号展开游戏。操作用控制器 42 具有用于躲避存储保存数据的备份存储器 43，备份存储器 43 由非易失性存储器构成。

服务器 44 具有数据库 45，游戏设备 41 访问网络的次数和访问时间（以下称为访问信息）作为密钥，以一个记录单位记录。设备 ID 为游戏设备 41 的固有识别信息，例如制造编号和游戏设备 41 第一次连接网络的时间（包含秒单位）等。本图示例中，游戏设备 41 的设备 ID 为 B1011，访问次数为 72 次，访问时间为 2000 年 10 月 2 日 19 时 14 分 32 秒、2000 年 10 月 4 日 21 时 25 分 11 秒、2000 年 10 月 9 日 11 时 7 分 52 秒、……。将游戏设备 41 的访问信息登录在数据库 45，同时也将同样的内容写入备份存储器 43。

本图中，游戏设备 41 通过通信网络访问服务器 44 时（本图（1）），服务器 44 从游戏设备 41 中取得设备 ID 和备份存储器 43 内的访问信息。接下来，参照数据库 45（本图（2）），检查设备 ID 与访问信息是否匹配。考虑到几乎不会有多个游戏设备在包含秒单位的同一时间访问服务器，所以可以认为访问信息为备份存储器 43 内的固有信息。因此，游戏设备的访问信息具有可以作为用于将备份存储器 43 识别为其它的备份存储器的识别信息的功能。

在设备 ID 与访问信息一致的情况下，只增加一次访问次数，服务器 44 通过追加记录访问时间，更新记录内容。同时，更新备份存储器 43 的访问信息（本图（3））。另一方面，设备 ID 与访问信息不

一致的情况下，由于怀疑非法使用备份存储器 43，所以限制备份存储器 43 的使用。

设备 ID 与访问信息不一致的情况为，①将保存数据存入他人的备份存储器而使用的情况，②怀疑非法复制保存数据情况。①的情况下，由于设备 ID 和访问次数以及访问时间完全不一致，就可以知道使用了在游戏设备 41 中未被使用的其他保存数据。②的情况下，虽然由于是在游戏设备 41 中被使用的保存数据，访问时间部分一致，但由于访问次数不同，所以有非法复制之嫌。

关于②的情况，参照图 7 详细进行说明。如本图所示，欲将备份存储器 43 中记录的保存数据向备份存储器 46 中非法复制（本图（1））。如果备份存储器 43 中记录的访问次数为 72 次，则备份存储器 46 中记录的访问次数变为 72 次。当游戏者使用备份存储器 43 时，备份存储器 43 中记录的访问次数被更新为 73 次（本图（2））。此外，数据库内的记录也被更新为 73 次（本图（3））。此时，游戏者从控制器 42 中抽取备份存储器 43，将备份存储器 46 重新装入，然后访问服务器 44 时，由于备份存储器 46 中的访问次数与数据库 45 中记录的访问次数不同，所以被怀疑为非法复制（本图（4））。此外，如果预先将保存数据复制到其他记录媒介中，然后进行游戏，更新保存数据，再次返回到更新前的保存数据，则与像进行游戏那样的使用同一备份存储器的情况相同。

根据以上所说明的实施例，由于服务器 44 对游戏设备 41 的设备 ID 和访问信息进行一元化的管理，通过核对设备 ID 和访问信息，就可以有效地防止备份存储器 43 的非法使用以及非法复制。

〈发明实施例 5〉

图 8 为将多个游戏设备连接到通信网络，进行通信游戏的情况的说明图。本图中，标号 51~53 为连接到通信网络 54 的游戏设备，标

号 55 为控制通信游戏的服务器。本实施例中，如图 9 所示，对应于通信游戏的级别，设定可以参加的级别。例如，游戏参加条件为，所有人都可以参加普通级别，级别 20 以上的可以参加较难级别，级别 40 以上可以参加极难级别。此处所谓的级别为，随着游戏的进行，给予游戏者角色的参数，主要是根据在游戏中打倒敌人角色的种类和数量给予。

图 8 中记述了进行较难级别的通信游戏的情况下的各个游戏者的级别，由于游戏设备 51 的游戏者的级别为 25，游戏设备 52 的游戏者的级别为 30，游戏设备 53 的游戏者的级别为 45，所以这三个游戏者可以进行较难级别的通信游戏。

过去，在多人进行这种通信游戏的情况下，由于不管游戏者的级别高低都可以参加，例如熟悉通信游戏的高级别游戏者与刚刚开始通信游戏的初学者可以一起进行游戏，初学者通过跟随在高级别游戏者的后面，就可以亦步亦趋地跟到游戏的结尾。这种不管级别高低都可以自由参加通信游戏的形式，使游戏的趣味减半。但是，通过本实施例，由于是根据通信游戏的级别设定可以参加的游戏者的级别，可以克服上述缺点。

〈发明实施例 6〉

图 10 为记述游戏展开的剧情的说明图。如本图所示，游戏由进程 1～进程 3 的各进程构成。进程具有森林地带、地下洞窟、采掘场、古代宇宙飞船等场景。各个进程中配合游戏的进行设定有场景 1、场景 2，随场景展开进行变化。各个进程最后设有决战场景，在此处将出场的敌人角色打倒就可以进入下一个进程。

游戏者在不连接通信网络，离线进行游戏的情况下，一般是将游戏的进行状况作为标记数据保存，为下次游戏作准备。但是，在连接通信网络在线进行游戏的情况下，由于是多个游戏角色展开游戏，例

如即使初学者什么也不做，只跟在高级别游戏者的后面也可以进行游戏。

由于这个原因，本实施例中如图 11 所示，在进行在线游戏的情况下（步骤 S1：YES），不保存游戏进行的标记数据（步骤 S2）；在不进行在线游戏的情况下（步骤 S1：NO），保存游戏进行的标记数据（步骤 S3）。通过上述结构，可以消除上述缺点。此外，也可以具有以下结构，即即使在游戏设备保存游戏进行的标记数据的情况下，在不连接通至讯网络进行游戏时，禁止参照该标记数据从一局的中途参加游戏。

在通信游戏的情况下，作为控制保存游戏进行的标记数据的装置，可以在游戏设备的一侧设置保存控制装置，也可以通过游戏服务器控制保存游戏进行的标记数据。

〈发明实施例 7〉

图 12 表示游戏的结束画面的画面转换。本图中，(A1)～(A3)为游戏者不连接通信网络离线进行游戏，游戏结束时的结束画面的画面转换图。游戏者角色 61 将敌人角色 62 打倒，游戏结束时（本图 (A1)），在几分钟的时间内打出游戏制作职员表（本图 (A2)），然后显示出结束画面（本图 (A3)）。

另一方面，(B1)～(B2)为多人连接到通信网络在线进行游戏，游戏结束时的结束画面的画面转换图。游戏者角色 71～74 将敌人角色 75 打倒，游戏结束时（本图 (B1)），立刻就表示出结束画面（本图 (B2)），然后返回原来的游戏画面。

这样，游戏者在线进行通信游戏的情况下，由于只要连接电话线路，除了缴纳作为电话线路的连接费的电话费之外，还要缴纳连接服务器的互联网连接费，游戏的结束画面在很短时间内结束，就可以减

轻游戏者的经济负担。

在通信游戏的情况下，作为控制缩短游戏结束画面显示时间的装置，可以在游戏设备一侧设置该控制装置，也可以通过游戏服务器控制缩短游戏结束画面显示时间。

根据本发明的安全系统、记录媒介管理方法以及记录使计算机系统执行该方法的程序的计算机可以读取的记录媒介，由于通过通信网络由服务器分配给数据处理装置识别信息，即使预先不给予数据处理装置识别信息的情况下，也可以管理哪一个记录媒介在哪一个数据处理装置中的使用。

根据本发明的数据处理装置、数据处理方法以及记录使计算机系统执行该方法的程序的计算机可以读取的记录媒介，由于可以将数据处理装置中固有识别信息作为密钥，对备份存储器的保存数据进行加密处理以及解码处理，所以是有效的保存数据的安全对策。

根据本发明的数据处理装置以及保存数据的管理方法，由于把被数据处理装置进行数据处理的保存数据传送到数据处理装置后，消去了备份存储器内的非易失性存储器记录的保存数据，所以可以有效地防止非法使用保存数据。

根据本发明的安全系统、保存数据的管理方法以及记录使计算机系统执行该方法的程序的计算机可以读取的记录媒介，由于服务器管理具有备份存储器的数据处理装置连接至通信网络的次数，所以可以有效地防止非法使用备份存储器内的保存数据。

根据本发明的游戏服务器，由于对应于游戏的难易度，预先设定可以参加的通信游戏的级别，只有对于满足对应游戏难易度的要求级别的游戏者才被允许参加通信游戏，所以可以使通信游戏更加有趣。

根据本发明的游戏处理方法以及记录使游戏设备执行该方法的程序的计算机可以读取的记录媒介，由于不将连接通信网络进行通信游戏时游戏的进行状况作为保存数据保存，所以可以使通信游戏更加有趣。

根据本发明的游戏处理方法以及记录使游戏设备执行该方法的程序的计算机可以读取的记录媒介，由于连接通信网络进行通信游戏时，缩短了游戏的结束画面的显示时间，所以可以减轻通信网络的连接费的负担。

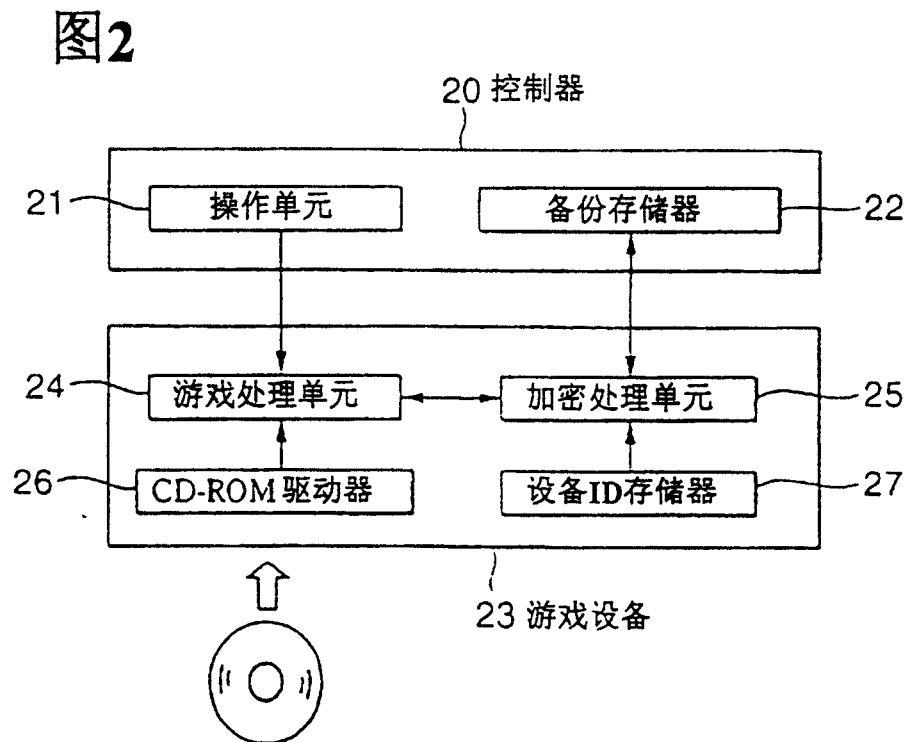
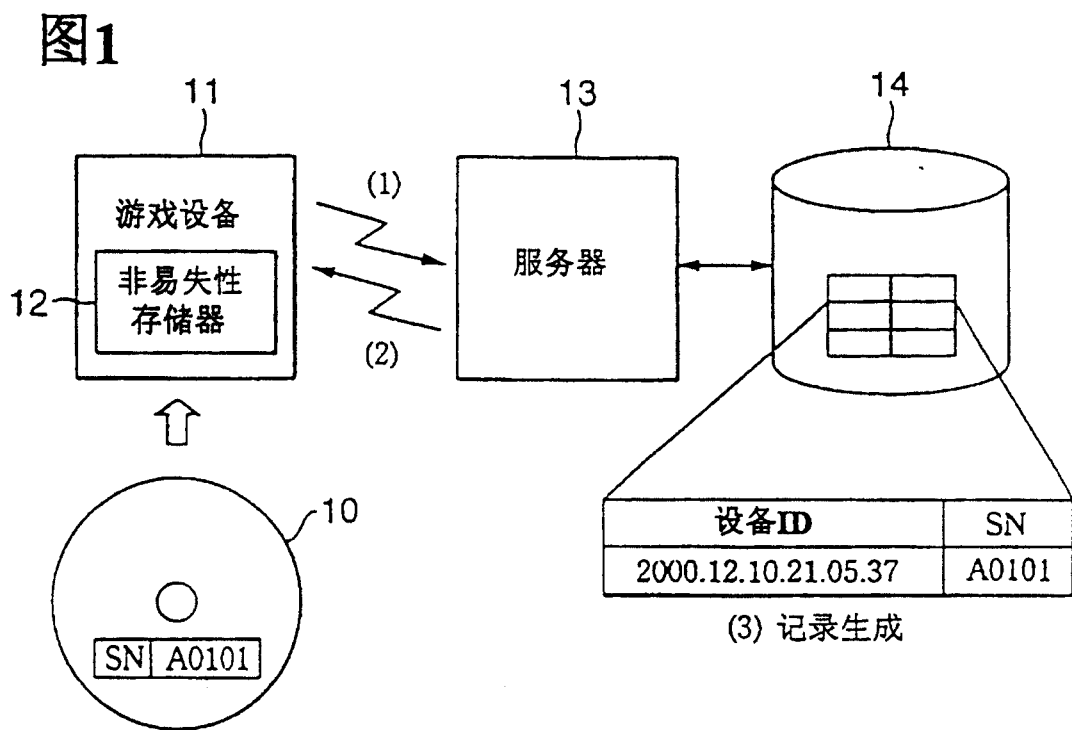


图3

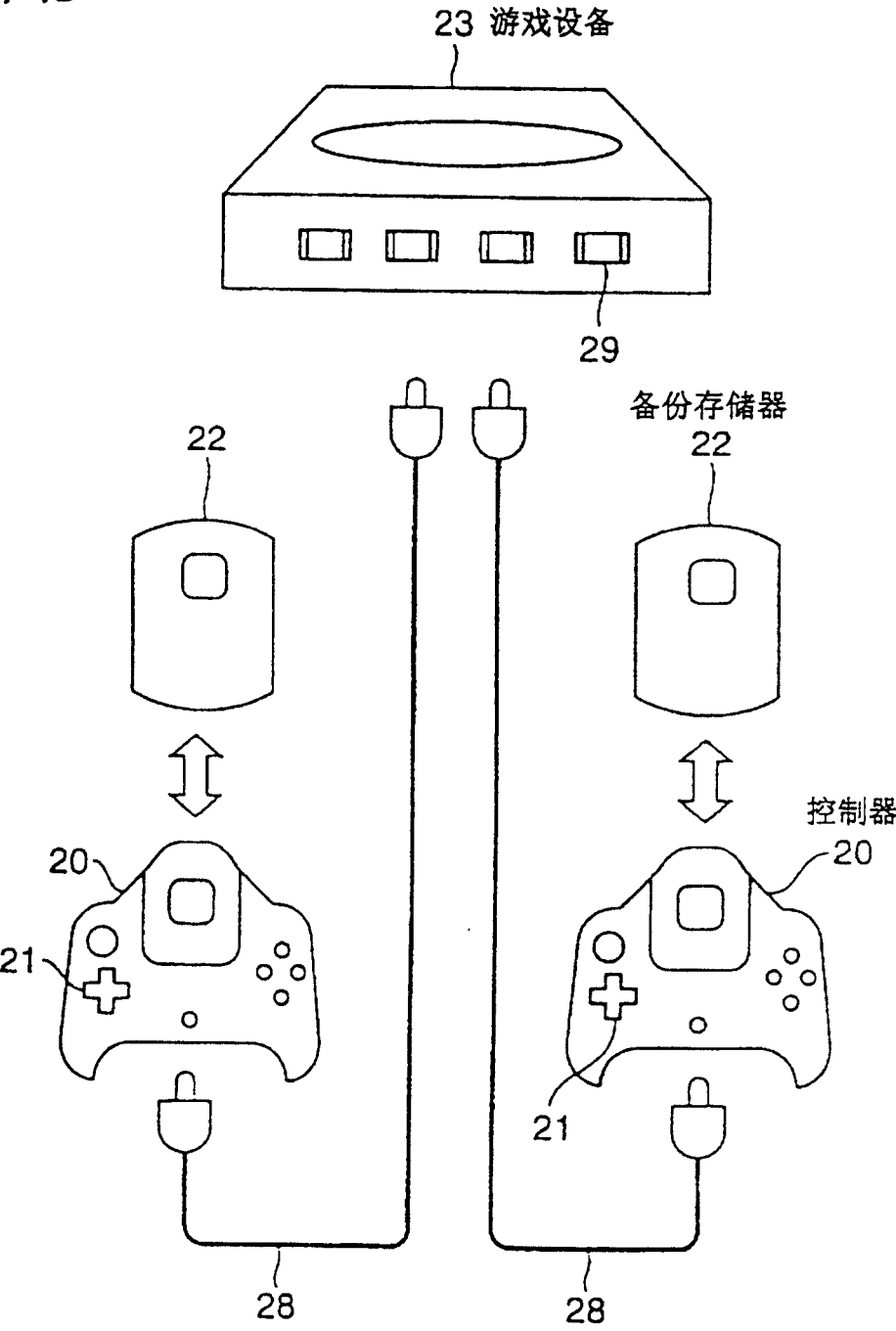


图4

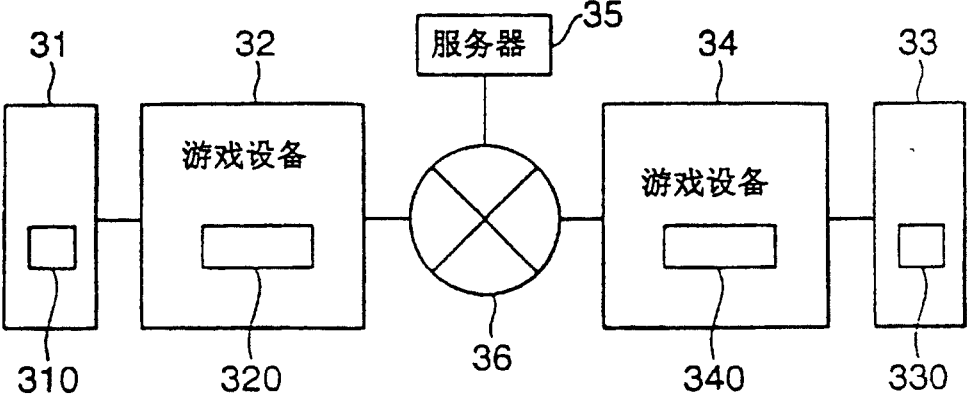


图5

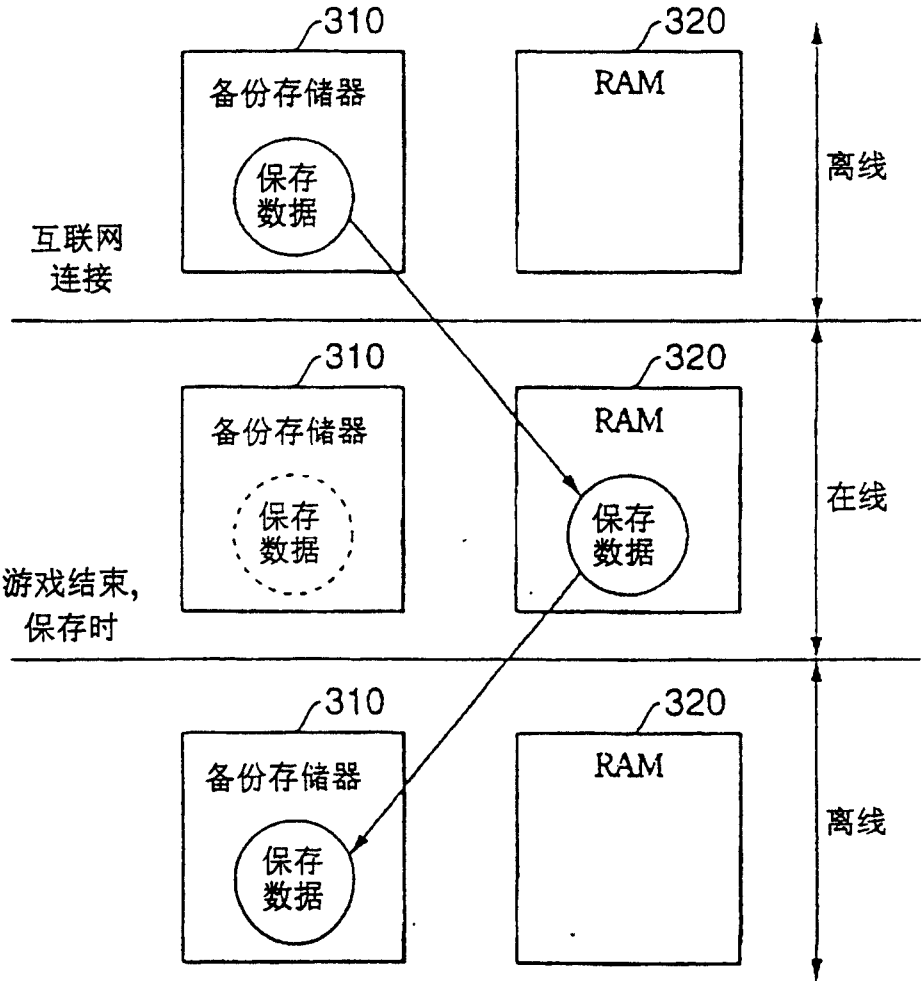


图6

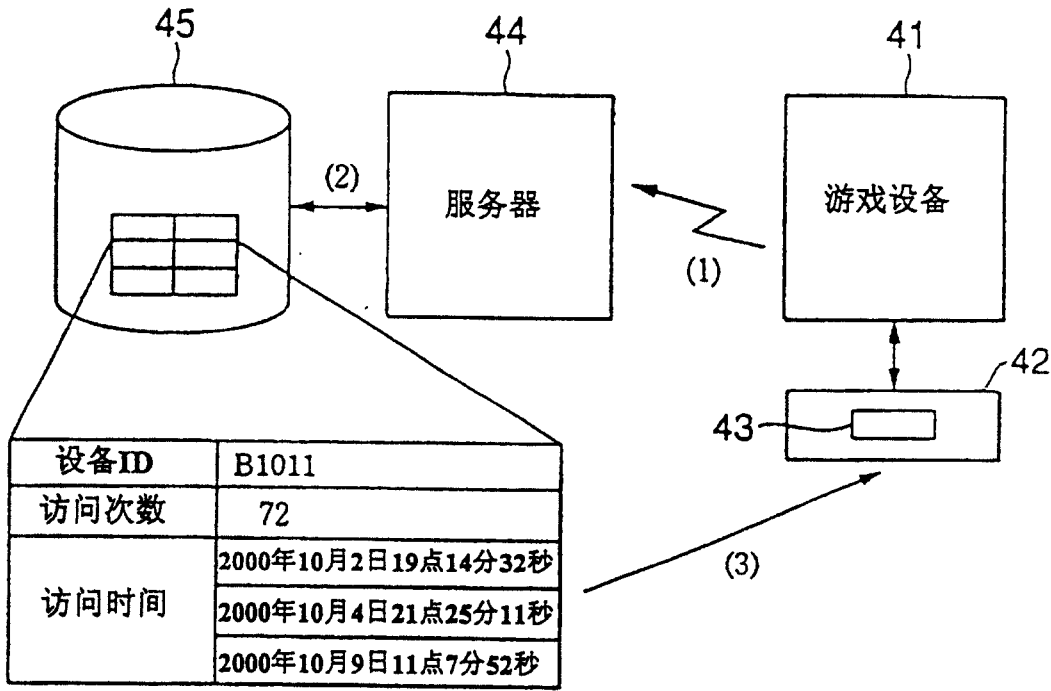


图7

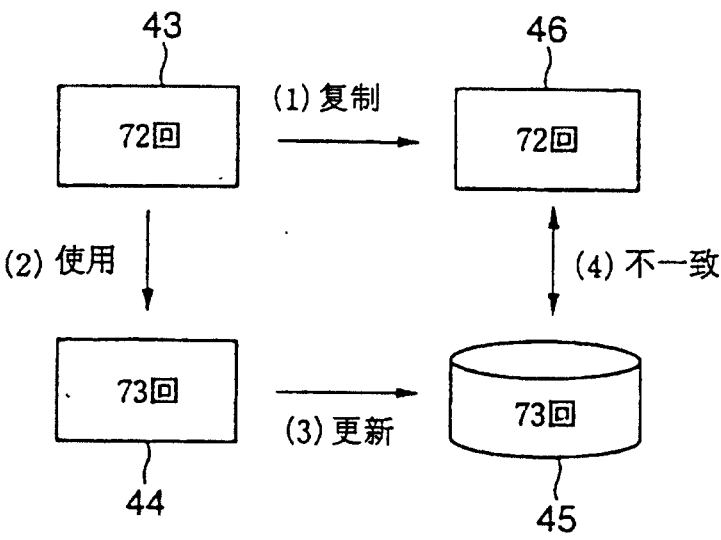


图8

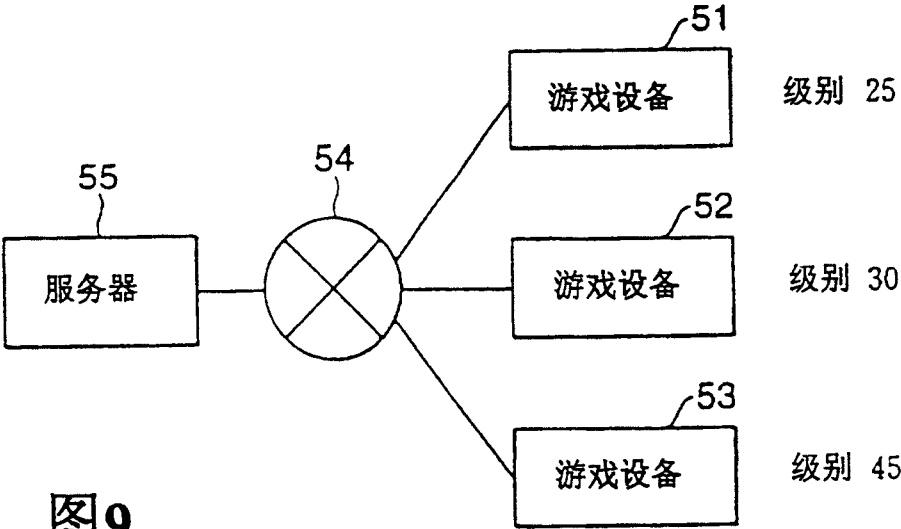


图9

模式	要求级别
普通	所有人均可
较难	20以上
极难	40以上

图10

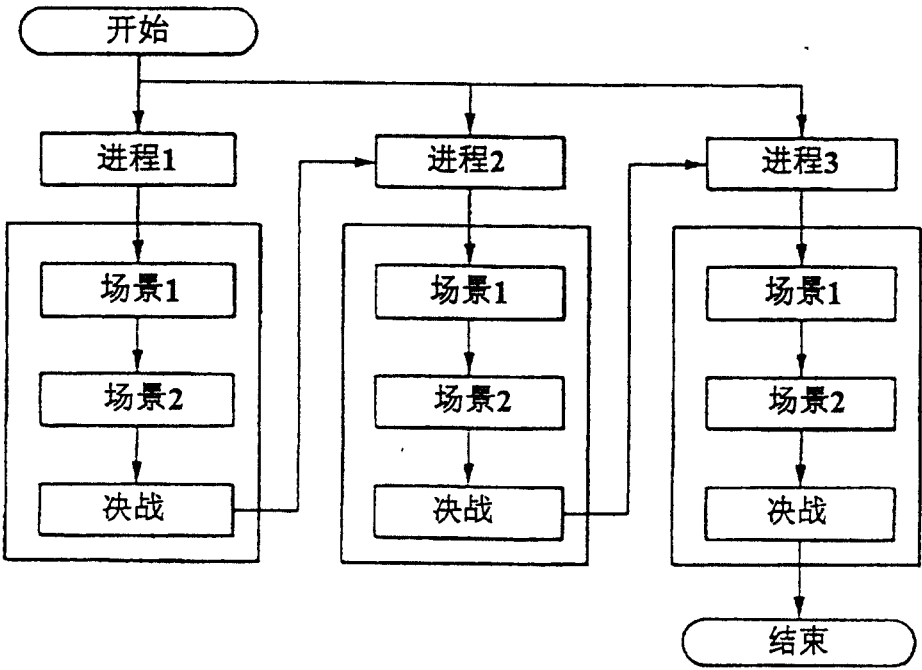


图11

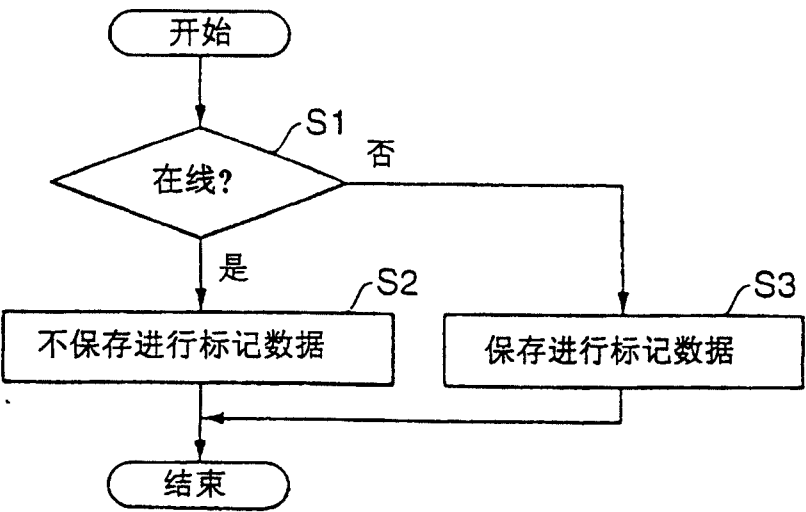


图12

