[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 1/00 (2006.01)

[12] 发明专利说明书

专利号 ZL 200410064167.0

[45] 授权公告日 2006 年 10 月 25 日

[11] 授权公告号 CN 1282052C

[22] 申请日 2004.8.20

[21] 申请号 200410064167.0

[30] 优先权

[32] 2003.8.21 [33] JP [31] 297701/2003

[71] 专利权人 株式会社东芝

地址 日本东京都

[72] 发明人 国分智幸 石垣智 石崎浩

审查员 刘 翎

[74] 专利代理机构 中国国际贸易促进委员会专利商标事务所

代理人 李德山

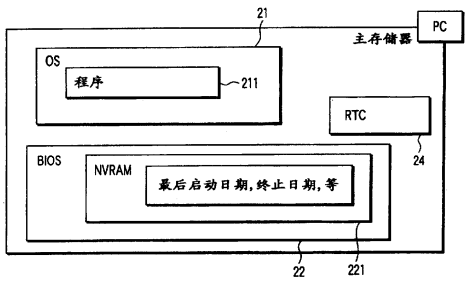
权利要求书 5 页 说明书 10 页 附图 4 页

[54] 发明名称

信息处理设备

[57] 摘要

一种信息处理设备，该设备包含通信单元(21)，被配置与管理所述信息处理设备的管理设备进行通信；管理单元(211)，被配置基于通过通信单元所接收的来自所述管理设备的给定信息来管理所述信息处理设备的可用时间；以及控制单元(22)，被配置基于所述管理单元所管理的可用时间来限制所述信息处理设备的使用。



1. 一种信息处理设备，其特征在于，包含:

通信单元（30，21），被配置成与管理设备进行通信，其中，所述管理设备管理所述信息处理设备;

在所述信息处理设备中的管理单元（211），被配置成，当所述信息处理设备的系统启动时，判断该信息处理设备是否可以通过通信单元（30，21）连接到网络，并且，如果可以连接，则与所述管理设备一起执行验证过程，并从所述管理设备接收日期和时间信息以便基于通过所述通信单元从所述管理设备接收的日期和时间信息来管理所述信息处理设备的可用时间；以及

在所述信息处理设备中的控制单元（22），被配置基于所述管理单元所管理的可用时间来限制所述信息处理设备的使用。

2. 如权利要求 1 所述的信息处理设备，其特征在于，所述控制单元（22）包含处理单元（22），被配置用于管理在一个特定区域内的可用时间。

3. 如权利要求 1 所述的信息处理设备，其特征在于，所述日期和时间信息至少包含当前日期，当前时间，终止日期，以及可用时间段中的一个。

4. 如权利要求 2 所述的信息处理设备，其特征在于，所述控制单元（22）还被配置基于存储于所述特定区域内的日期和时间信息禁止对所述信息处理设备的使用。

5. 如权利要求 4 所述的信息处理设备，其特征在于，所述处理单元（22）包含:

一个单元，被配置在所述特定区域上存储并管理作为最后启动日期的系统启动的最后日期;

一个单元，被配置在所述特定区域上存储并管理用于管理作为终止日期的可用时间的日期和时间信息，

一个单元，被配置比较所述最后启动日期和在所述信息处理系统

中管理的当前日期;

一个单元，被配置比较所述终止日期和所述当前日期;

一个单元，被配置当所述当前日期迟于所述最后启动日期且所述当前日期早于所述终止日期时将最后启动日期更新为当前日期，以及

一个单元，被配置当所述当前日期迟于所述最后启动日期且所述当前日期早于所述终止日期时启动系统。

6. 如权利要求 5 所述的信息处理设备，其特征在于，所述被配置启动系统的单元还被配置当所述当前日期早于所述最后启动日期时禁止启动系统。

7. 如权利要求 5 所述的信息处理设备，其特征在于，所述被配置启动系统的单元还被配置当所述当前日期迟于所述终止日期时禁止启动系统。

8. 如权利要求 2 所述的信息处理设备，其特征在于，所述通信单元（30，21）还被配置与所述管理设备一起执行验证过程，而后从所述管理设备获得日期和时间信息并将该日期和时间信息发送到所述处理单元。

9. 如权利要求 8 所述的信息处理设备，其特征在于，所述通信单元（30，21）还被配置接收至少一部分来自所述管理设备的作为加密信息的日期和时间信息。

10. 如权利要求 8 所述的信息处理设备，其特征在于，所述管理单元（211）包含:

一个单元，被配置在所述信息处理设备中所提供的时钟上设置当前日期;

一个单元，被配置将所述日期和时间信息通知给所述处理单元;以及

一个单元，被配置更新在所述处理单元管理的特定区域上设置的最后启动日期。

11. 如权利要求 4 所述的信息处理设备，其特征在于，所述管理单元（211）还被配置在所述特定区域上设置一个限制所述信息处理

设备的操作时间的限制时间，依据所述设备的操作更新该限制时间，并且在接收到来自所述通信单元的日期和时间信息时，向所述处理单元通知更新后的限制时间。

12. 如权利要求 4 所述的信息处理设备，其特征在于，

所述管理单元（211）还被配置向所述管理设备通知所述管理单元已被验证，并且

所述处理单元（22）还被配置在所述特定区域上记录数字信息，用于基于上述通知来限制对所述信息处理设备的使用，依据完成所述信息处理设备的一项操作更新该数字信息，并且当所述数字信息到达限制使用所述信息处理设备的值时禁止使用所述信息处理设备。

13. 如权利要求 4 所述的信息处理设备，其特征在于，所述处理单元（22）还被配置在所述特定区域上存储唯一标识存储媒介的信息，基于所述唯一标识该存储媒介的信息确定是否验证所述存储媒介，并且当所述存储媒介未被验证时，禁止使用所述信息处理设备，其中所述存储媒介存储所述管理单元的程序。

14. 一种适用于信息处理设备的信息处理方法，其特征在于，包含：

当所述信息处理设备的系统启动时，判断该信息处理设备是否可以通过通信单元连接到网络，并且，如果所述信息处理设备可以连接到所述网络，则与管理设备一起执行验证过程，并从所述管理设备接收日期和时间信息，其中所述管理设备管理所述信息处理设备（S102 至 S104）；

基于通过通信单元从所述管理设备接收的日期和时间信息来管理所述信息处理设备的可用时间（S105 至 S108）；以及

基于所述管理单元所管理的可用时间来限制所述信息处理设备的使用（S11 至 S15，S21 至 S31）。

15. 如权利要求 14 所述的信息处理方法，其特征在于，还包含：

更新并管理所述信息处理设备的最后启动日期（S108）；

比较所述最后启动日期和由所述信息处理设备管理的当前日期（S11；S21）；并且

当所述当前日期早于所述最后启动日期时，限制对所述信息处理设备的使用（S15；S31）。

16. 如权利要求 15 所述的信息处理方法，其特征在于，还包含：

管理限制所述信息处理设备的使用的终止日期，其中所述终止日期由所述信息处理设备管理（S105）；

比较由所述信息处理设备管理的终止日期和由所述信息处理设备管理的当前日期（S12；S22）；并且

当所述当前日期迟于所述终止日期时，限制对所述信息处理设备的使用（S15；S31）。

17. 如权利要求 16 所述的信息处理方法，其特征在于，还包含：

从管理设备获取由该管理设备管理的终止日期，其中所述管理设备管理所述信息处理设备（S104）；并且

将从所述管理设备获取的所述终止日期设置为所述信息处理设备的终止日期（S105）。

18. 如权利要求 17 所述的信息处理方法，其特征在于，还包含：

从所述管理设备获取由该管理设备管理的当前日期（S104）；并且

将从所述管理设备获取的所述当前日期设置为所述信息处理设备的当前日期（S106）。

19. 如权利要求 18 所述的信息处理方法，其特征在于，还包含：

在将从所述管理设备获取的当前日期设置为所述信息处理设备的当前日期后，依据所述信息处理设备的操作更新所述最后启动日期（S108）。

20. 如权利要求 15 所述的信息处理方法，其特征在于，还包含:

管理存储媒介的唯一标识信息，其中所述存储媒介被用于最后启动日期的管理（S23 至 S29）；

当所述信息处理设备工作时，利用所管理的唯一标识信息判断所述存储媒介是否被验证（S26，S29）；以及

当所述存储媒介未被验证时，禁止操作所述信息处理设备（S31）。

21. 如权利要求 16 所述的信息处理方法，其特征在于，还包含:

管理存储媒介的唯一标识信息，其中所述存储媒介被用于终止日期的管理（S23 至 S29）；

当所述信息处理设备工作时，利用所管理的唯一标识信息判断所述存储媒介是否被验证（S26，S29）；以及

当所述存储媒介未被验证时，禁止操作所述信息处理设备（S31）。

信息处理设备

技术领域

本发明涉及一种利于在诸如 LAN 的网络上提供的客户端个人电脑的反盗机制的信息处理设备.

背景技术

保护诸如 LAN 的网络上提供的个人电脑中数据的安全方法有许多种.

Kensington 锁反盗机制是一种客户端的个人电脑（客户端 PC）的主部件的反盗机制. 该 Kensington 锁对于限制外部用户（非特定的第三方）对个人电脑的使用是有效的. 然而, Kensington 锁在正常的使用环境中使用却有困难, 因为它必须伴随一个物理结合体. 如果 Kensington 锁针对一个易于携带的小型设备上应用, 例如移动 PC, 其锁定机制就会很复杂从而导致正常使用上的问题. 另外, 设备自身的防护除了需要考虑外部使用者外内部使用者同样需要考虑. 从这个方面而言, 由于用户通常都被提供有密匙, 因此 Kensington 锁同样不是很有效的.

日本专利申请 KOKAI 公布 No.8-305461 揭示了一种技术, 该技术禁止设备正常操作的技术, 除非通过通信线路该设备由验证中心以一个有规律的时间间隔加以验证, 例如每过一固定时期以及每使用若干次, 一旦设备被盗用, 它将通过向警察报告盗用以阻止设备通过验证中心的验证. 然而, 盗用报告很可能引起人为的错误并使得维持具有可靠性的安全很困难.

如上所述, 通常, 没有一种有效的反盗机制来保护个人电脑的主部件以免在正常使用环境下被盗用.

发明内容

本发明的具体实施例将提供一种保护主部件不被盗用并防止数据通过未经验证的访问而泄漏的信息处理设备。

根据本发明的一个方面，提供一种信息处理设备，包含：通信单元，被配置成与管理设备进行通信，其中，所述管理设备管理所述信息处理设备；在所述信息处理设备中的管理单元，被配置成，当所述信息处理设备的系统启动时，判断该信息处理设备是否可以通过通信单元连接到网络，并且，如果可以连接，则与所述管理设备一起执行验证过程，并从所述管理设备接收日期和时间信息以便基于通过所述通信单元从所述管理设备接收的日期和时间信息来管理所述信息处理设备的可用时间；以及在所述信息处理设备中的控制单元，被配置基于所述管理单元所管理的可用时间来限制所述信息处理设备的使用。

根据本发明的另一个方面，提供一种适用于信息处理设备的信息处理方法，包含：当所述信息处理设备的系统启动时，判断该信息处理设备是否可以通过通信单元连接到网络，并且，如果所述信息处理设备可以连接到所述网络，则与管理设备一起执行验证过程，并从所述管理设备接收日期和时间信息，其中所述管理设备管理所述信息处理设备；基于通过通信单元从所述管理设备接收的日期和时间信息来管理所述信息处理设备的可用时间；以及基于所述管理单元所管理的可用时间来限制所述信息处理设备的使用。

在本发明的一个具体实施例中，提供一种信息处理设备，包含通信单元，被配置与管理所述信息处理设备的管理设备进行通信；管理单元，被配置基于通过通信单元所接收的来自所述管理设备的给定信息来管理所述信息处理设备的可用时间；以及控制单元，被配置基于所述管理单元所管理的可用时间来限制所述信息处理设备的使用。

在本发明的另一个具体实施例中，提供了一种信息处理设备所用的信息处理方法，包含更新并管理所述信息处理设备的最后启动日期；将该最后启动日期与由所述信息处理设备管理的当前日期相比较以确定该当前日期是否早于所述最后启动日期；并且在确定当前日期早于所述最后启动日期时，限制对所述信息处理设备的使用。

在一个具体实施例中，一种信息处理设备，包含通信单元，被配置与一管理设备进行通信，其中所述管理设备管理所述信息处理设备，在所述信息处理设备中的管理单元，被配置基于通过所述通信单元所接收的来自所述管理设备的日期和时间信息来管理所述信息处理设备的可用时间，以及在信息处理设备中的控制单元，被配置基于所述管

理单元所管理的可用时间来限制所述信息处理设备的使用。

在另一具体实施例中，一种信息处理方法，包含与一管理设备通信，其中所述管理设备管理所述信息处理设备，基于通过通信单元所接收的来自所述管理设备的日期和时间信息来管理所述信息处理设备的可用时间，并基于管理单元所管理的可用时间来限制所述信息处理设备的使用。

在另一具体实施例中，一种信息处理设备，包含与管理设备进行通信的装置，其中所述管理设备管理所述信息处理设备，基于通过所述通信装置所接收的来自所述管理设备的日期和时间信息来管理所述信息处理设备的可用时间的装置，以及基于所述管理装置所管理的可用时间来限制所述信息处理设备的使用的装置。

在又一具体实施例中，一种产品包含嵌入计算机可读程序指令的计算机可用媒介。所述计算机可读程序指令包含被配置与一管理设备进行通信的计算机可读程序指令，其中所述管理设备管理所述信息处理设备，被配置基于所接收的来自所述管理设备的日期和时间信息来管理所述信息处理设备的可用时间的计算机可读程序指令，被配置基于所述可用时间来限制信息处理设备的使用的计算机可读程序指令。

出于概括本发明的目的，将在此描述本发明的某些方面，优点以及创新特征。应明确的是，并非根据本发明的任何特定实施例都必然实现所有这些优点。因此本发明能以实现或优化本文所授的一个或一些优点的方式来实施或执行而不必实现本文所授或建议的其它优点。

附图说明

包含于说明书中并作为其组成部分的附图示出了本发明的具体实施方式，并与上文所述发明内容以及下文所述具体实施例一起阐明本发明的原理。

图 1 示出了根据本发明一个具体实施例的系统的配置和主要组件的方框图；

图 2 示出了根据本发明一个具体实施例的客户端 PC 主要组件的方框图；

图 3 示出了根据本发明一个具体实施例的执行 BIOS 启动禁止控制过程的流程图；

图 4 示出了根据本发明一个具体实施例的执行操作系统启动禁止控制程序过程的流程图；

图 5 示出了根据本发明一个具体实施例的执行 BIOS 启动禁止控制过程的流程图。

具体实施方式

在详细描述本发明的具体实施方式之前，需要阐明在实施例中所述的基础概念。

当一台客户端个人电脑（又称客户端 PC）通过诸如 LAN 的网络连接到被验证的服务器上时，它可以正常的被使用。在一个实施例中，当客户端 PC 脱离使用环境时，其系统启动将被禁止。这一启动禁止功能通过在客户端 PC 中的 BIOS(基本输入/输出系统)和由操作系统（OS）管理的程序来实现。BIOS 执行诸如检查终止日期的过程。其他过程，例如通过与服务器间的通信进行信息获取以及日期更新，则由 OS 管理的程序完成。这样，启动禁止功能就能容易的实现。

所述服务器在客户端 PC 中设置一个终止日期。无论何时客户端 PC 连接到服务器上，服务器都向该客户端 PC 发送该终止日期的管理信息。对于客户端 PC 与服务器之间的通信，在一个实施例中，使用诸如 RSA（Rivest Shamir Adleman）的加密方案是被希望的。

客户端 PC 管理诸如由 BIOS 管理的在非易失保密区域上的终止日期和最后更新日期之类的信息。

当系统启动时，BIOS 将比较客户端 PC 的 RTC（实时时钟）上所显示的当前日期信息与上述管理信息来决定启动系统或是禁止启动。如果客户端 PC 落在终止日期以内， OS 启动，以通过与服务器通信来更新管理信息。如果客户端 PC 的使用期满，禁止启动系统。BIOS 在决定启动系统或是禁止启动同时也进行检查以阻止未验证的使用，举例来说，回调 RTC。当系统处于启动禁止状态时，它不能被启动或者响应管理员的密码输入而释放该状态。在任一种情况下，都将准备附加的措施使管理员可以重置或重启系统。

当用户登陆系统时，由 OS 管理的程序将确认服务器的 SSID（服务集标识符）。而后，程序根据一个给定的协议接收终止日期信息并通过一个特定接口向 BIOS 提供该终止日期信息及当前日期。

BIOS 在由其自身管理的保密区域中存储所接收的信息。BIOS 接收由服务器管理的当前日期信息以及终止日期信息并设置 PC 中的

RTC 的信息。在一个实施例中，这一过程被首先执行。然而，如果 RTC 在随后过程中为了未验证的使用被回调，通过对最后启动日期或最后启动日期和时间的检查，系统被置为启动禁止模式。

除了设置 PC 的可用时间（允许 PC 不与服务器连接时被使用的时间）外，将上述日期设置为终止日期也是能够实现的。在这种情况下，所述可用时间（8 小时，40 小时等）由 BIOS 的保密区域管理。当系统启动时或在启动期间，BIOS 确定 PC 是否与一个验证服务器相连接。当 PC 没有连接时，在保密区域上缩短该可用时间。当可用时间变为“0”时 BIOS 禁止系统启动或强行关闭系统。

为了手动的释放上述启动禁止状态，举例来说，管理员启动一个已转变为启动禁止状态的 PC 并且输入密码，该密码在每一台 PC 上为管理员配置且不同于用户密码。所述密码也存储在 BIOS 的保密区域上。为了自动的释放启动禁止状态，BIOS 利用一个用于再验证的最小设备，例如 LAN 适配器或 HDD，来启动已转变为启动禁止状态的 PC（通过禁止使用诸如不必要的显示设备来抑止对 PC 未验证的使用）。当 PC 启动时，如果验证程序能够获得对验证服务器的访问，举例来说，再次设置一个终止日期并重启 PC。由于重启后的终止日期被延长了，因此启动禁止状态被释放以允许 PC 正常使用。

由于第三方可以执行由 OS 管理的所述程序，为了禁止程序被改变并保持其安全性，在 BIOS 的保密区域中将设置一个此程序的安装标志。当该程序在客户端 PC 上被安装时，系统向 BIOS 通知该程序的安装。BIOS 在保密区域中存储表示安装的标志信息。当程序被安装时，它将确认所述标志是否为开。程序被设计为：如果标志为开，它将既不能被安装也不能被卸载。这样，对程序未验证的使用就能被阻止。该标志可以通过管理员对 BIOS 的密码输入被重置。

由 OS 管理的程序被存储在一程序存储区（通常为 HDD）中，其存储的程序可以由第三方改写。这样，启动禁止功能可能通过改写程序或更换 HDD 被无效。为避免这种情况，在 BIOS 的保密区域中设有一个启动限制计数器。程序将在每次启动系统时通知 BIOS 该程

序被正确安装。每当 BIOS 接收上述通知，计数器都被置为初始值。当系统关闭时，BIOS 加/减计数器的值。如果上述通知没有被作出但在重复启动几次后，例如 5 次，计数器的值被固定，BIOS 就能确定 PC 被非法使用并禁止系统后续的启动。因此，由改写程序，更换每个 OS 的 HDD 等类似方式而导致的对 PC 未验证的使用就可以被阻止。

在另一实施例中，作为另一排除由更换 HDD 所导致的未验证的使用的过程，HDD 序列号将被存储于 BIOS 的保密区域中用以确定在系统每次启动时该 HDD 都被验证。BIOS 在保密区域中存储序列号，散列值，或其他与客户端 PC 连接的 HDD 的唯一标识信息。此后，每当系统启动时，BIOS 都将比较 HDD 的序列号和存储在保密区域中的值（HDD 序列号）。如果它们之间是不同的，BIOS 将系统设置到启动禁止状态。相应的，由更换 HDD 而导致的未验证的使用就能够被禁止。

当在 PC 和服务器之间的验证过程失效时，可立即禁止在单机基础上使用 PC，而非还在一固定时间段内允许使用 PC。如果上述程序在系统启动时不能正确验证服务器，程序将通知 BIOS 禁止启动来立即关闭系统。

现在，将参考附图对本发明的具体实施例进行说明。

图 1 示出了根据本发明一个实施例的系统的配置和主要组件的方框图。该系统是 LAN 连接客户端/服务器系统的一个例子。在图 1 中，附图标记 10 表示服务器，20 显示为客户端 PC 并且 30 代表 LAN。图 2 示出了客户端 PC 20 的主部件。

服务器 10 和客户端 PC 20 通过 LAN 30 彼此相互连接。服务器 10 包含通知客户端 PC 终止日期的程序 15。客户端 PC 20 包含操作系统（OS）21，BIOS 22 以及 RTC 24 作为主部件，如图 2 所示。

所述 OS 21 包含用于启动禁止控制的程序 211（又称启动禁止控制程序）。当系统启动来起动客户端 PC 20 时，程序 211 执行一个过程通过 LAN 30 验证客户端 PC 20 与服务器 10，从服务器 10 获得管

理可用时间的信息，向 BIOS 22 发送所获得的信息，并且更新存储在 BIOS 22 的保密区域（NVRAM）221 中的诸如最后启动日期，终止日期．执行 OS 21 的启动禁止控制程序 211 的过程由图 4 示出．

所述保密区域（NVRAM）221 由 BIOS 22 管理的非易失性存储器形成并且具有管理诸如最后启动日期，终止日期的字段．每一字段都由 OS 21 中的启动禁止控制程序 211 控制并更新．图 3 示出了根据一个实施例的执行 BIOS 22 的启动禁止控制的过程，并且图 5 示出了根据另一个实施例的执行 BIOS 22 的启动禁止控制的过程．

RTC 24 具有与通常个人电脑（PC）中提供的 RTC 相同的功能．在一个实施例中，启动禁止控制程序 211 被执行用以设置由服务器 10 获得的当前日期和时间．当系统启动时，BIOS 22 将参考该当前日期和时间．

当客户端 PC 20 请求服务器 10 连接客户端 20 来进行验证时，在服务器 10 中的程序 15 为客户端 PC 20 提供该客户端 PC 20 用来管理其可用时间的信息，或者将该信息分发到每个连接到 LAN 30 的客户端 PC 20．在一个实施例中，每当客户端 PC 20 正常的请求服务器 10 执行验证过程时，服务器 10 都向客户端 PC 20 提供该客户端 PC 20 用来管理可用时间的信息．

上述信息包含由服务器 10 所管理的终止日期以及当前日期和时间（由服务器中的 RTC 所测量）．所述终止日期可以由绝对日期（月和日）以及一个可用时间段（X 天）表示．在一个实施例中，可用时间段被用作终止日期．

当服务器 10 完成与客户端 PC 20 的验证过程时，它将向客户端 PC 20 通知由服务器 10 所管理的当前日期和可用时间（终止日期）信息．

当被连接到 LAN 30 的客户端 PC 20 完成验证过程时，它将接收来自服务器 10 的当前日期和可用时间信息并且基于该信息管理可用时间．每当系统启动时，客户端 PC 20 都确定该启动是否应被限制．

根据本发明的一个实施例，在客户端 PC 20 中提供的 OS 21 中的

启动禁止控制程序 211 在系统启动时(图 4 中的步骤 S101)通知 BIOS 22 所述程序 211 开始执行。而后，BIOS 22 确定客户端 PC 20 是否可被连接到 LAN 30（步骤 S102）。如果它可被连接到 LAN 30（步骤 S102 中的“是”），客户端 PC 20 根据一个给定的协议执行与服务器 10 的验证过程并且确定服务器 10 是否被授权（步骤 S103）。

如果客户端 PC 20 确认服务器 10 得到了验证（步骤 S103 中的“是”），它将与服务器 10 进行通信并获得由服务器 10 管理的定义可用时间的终止日期和当前日期(步骤 S104)。客户端 PC 20 向 BIOS 22 通知该最终日期（步骤 S105）而后为 RTC 24 设置当前日期（步骤 S106）。

在后续的启动之后，最后启动日期由在 BIOS 22 的保密区域（NVRAM）221 中形成的最后启动日期字段上的一个给定的读/写操作来更新（步骤 S107 和 S108）。

BIOS 22 将启动禁止控制程序 211 发送的终止日期设置到保密区域(NVRAM)中形成的终止日期字段中。而后，BIOS 22 将比较 RTC 24 的当前日期和存储于保密区域（NVRAM）221 中的最后启动日期来确 RTC 24 的当前日期是否迟于最后启动日期(图 3 中的步骤 S11)。

如果 RTC 24 的当前日期早于最后启动日期（步骤 S11 中的“否”），BIOS 22 确定该客户端 PC 22 通过 RTC 24 的日期设置操作被非法使用，执行启动禁止过程（步骤 S105），并且设置系统进入启动禁止模式。这样，随后的系统启动变为无效并且客户端 PC 20 不再可用。

如果 RTC 24 的当前日期迟于最后启动日期（步骤 S11 中的“是”)，BIOS 22 确定 RTC 24 没有执行过日期设置操作。而后，BIOS 22 将比较 RTC 24 的当前时间和存储于保密区域（NVRAM）221 中的最后启动日期来确定当前日期是否早于终止日期（步骤 S12）。

如果 RTC 24 的当前日期不早于终止日期(步骤 S12 中的“否”)，BIOS 22 执行启动禁止过程（步骤 S15）并设置系统进入启动禁止模式。随后的系统启动变为无效并且客户端 PC 20 不再可用。

如果 RTC 24 的当前日期早于终止日期（步骤 S12 中的“是”），存储于保密区域（NVRAM）221 中的最后启动日期被更新为 RTC 24 的当前日期（步骤 S13）。此后，BIOS 22 执行一个启动过程（步骤 S14）来启动系统。由此，在 OS 21 控制下的各种应用程序都可被执行。

图 5 示出了根据本发明另一实施例的执行 BIOS 22 启动禁止控制的过程。

图 5 所示的过程与图 4 相比主要区别在于它具有一个确认启动禁止控制程序 211 有效性的功能以及通过 RTC 24 的未验证操作排除使用客户端 PC 20 的功能。换言之，BIOS 22 具有排除由改写程序 211，更换 HDD 等类似方式而导致的未经验证使用客户端 PC 20 的功能。排除由改写程序 211 导致的未验证使用的功能通过图 5 中步骤 S24 至 S26 所示的确定过程来实现。排除由更换 HDD 而导致的未验证使用的功能通过图 5 中步骤 S27 至 S29 所示的确定过程来实现。

在一个实施例中，用于限制启动次数的启动限制计数器的字段和硬盘驱动（HDD）管理编号（HDD 序列号）的字段以及上文所述的字段都在 BIOS 22 中的保密区域（NVRAM）上设置。

每当系统启动时，启动禁止控制程序 211 都向 BIOS 22 通知程序已被正确安装。

每当 BIOS 22 接收到来自启动禁止控制程序 211 的上述通知时，都将重置启动限制计数器为初始值。换言之，启动限制计数器被禁止（步骤 S24 中的“否”）。

每当系统关闭时，BIOS 22 为启动限制计数器的值加 1（+1）（步骤 S25）。

当 BIOS 22 未接收到上述通知并且所述启动限制计数器变为一个固定值时，举例来说，“5”，在重复启动几次后（5 次启动后将不再通知）（步骤 S26 中的“是”），BIOS 22 确定该服务器 PC 未被验证而后禁止随后的启动（步骤 S31）。由此，排除由改写程序 211，更换每个 OS 的 HDD 等类似方式而导致的未验证的使用将成为可能。

在一个实施例中，BIOS 22 在保密区域（NVRAM）221 中存储 HDD 序列号并在系统每次启动时确定该 HDD 是否被验证。

每当系统启动时，BIOS 22 获取 HDD 的序列号并比较该序列号与保密区域（NVRAM）221 中存储 HDD 序列号（步骤 S27 和 S28），如果它们之间是不同的（步骤 S29 中的“否”），BIOS 22 确定 HDD 被非法更换了并禁止系统启动（步骤 S31）。由此，由更换 HDD 而导致的未验证的使用就能够被禁止。

由于其他的过程可以从上述第一实施例中很容易的理解，在此省略对其的描述。

上述实施例所述的程序可以作为诸如，举例来说，代码等的计算机程序被存储于诸如，举例来说，磁盘，光盘，半导体存储器等的计算机可读存储媒介中并被计算机（处理器）读出。这些计算机程序可以通过通信媒体从一个计算机分发到另一个计算机。

如上所述，本发明的实施例可以保护主部件不被盗用并防止数据通过未经验证的访问而泄漏。

附加的优点和修改对本领域的普通技术人员而言是显而易见的。因此，本发明更广泛的方面并不局限于在此示出的并描述的具体细节和典型的实施例。因此，在不背离由附随的权利要求及其等同物所定义的通用发明概念的精神和范围下，可以作出各种修改。

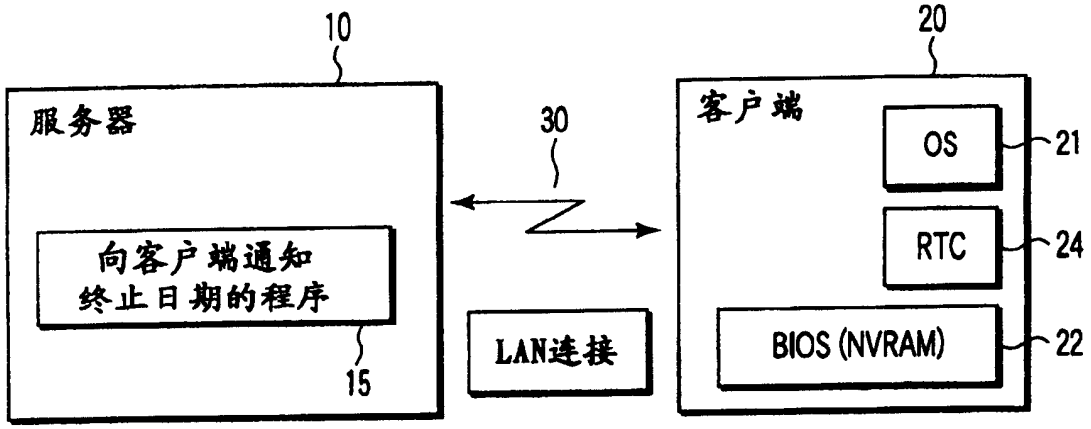

10
服务器
向客户端通知
终止日期的程序
15
30
LAN连接
20
客户端
OS
21
RTC
24
BIOS (NVRAM)
22

图 1

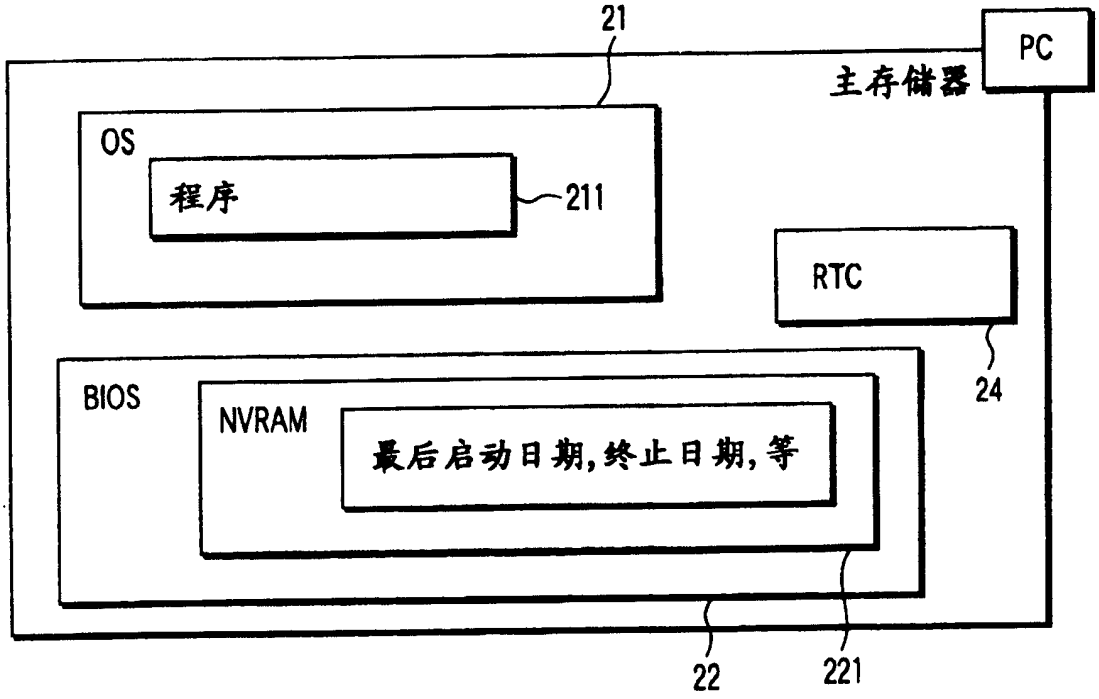

21
PC
主存储器
OS
程序
211
RTC
24
BIOS
NVRAM
最后启动日期,终止日期,等
22
221

图 2

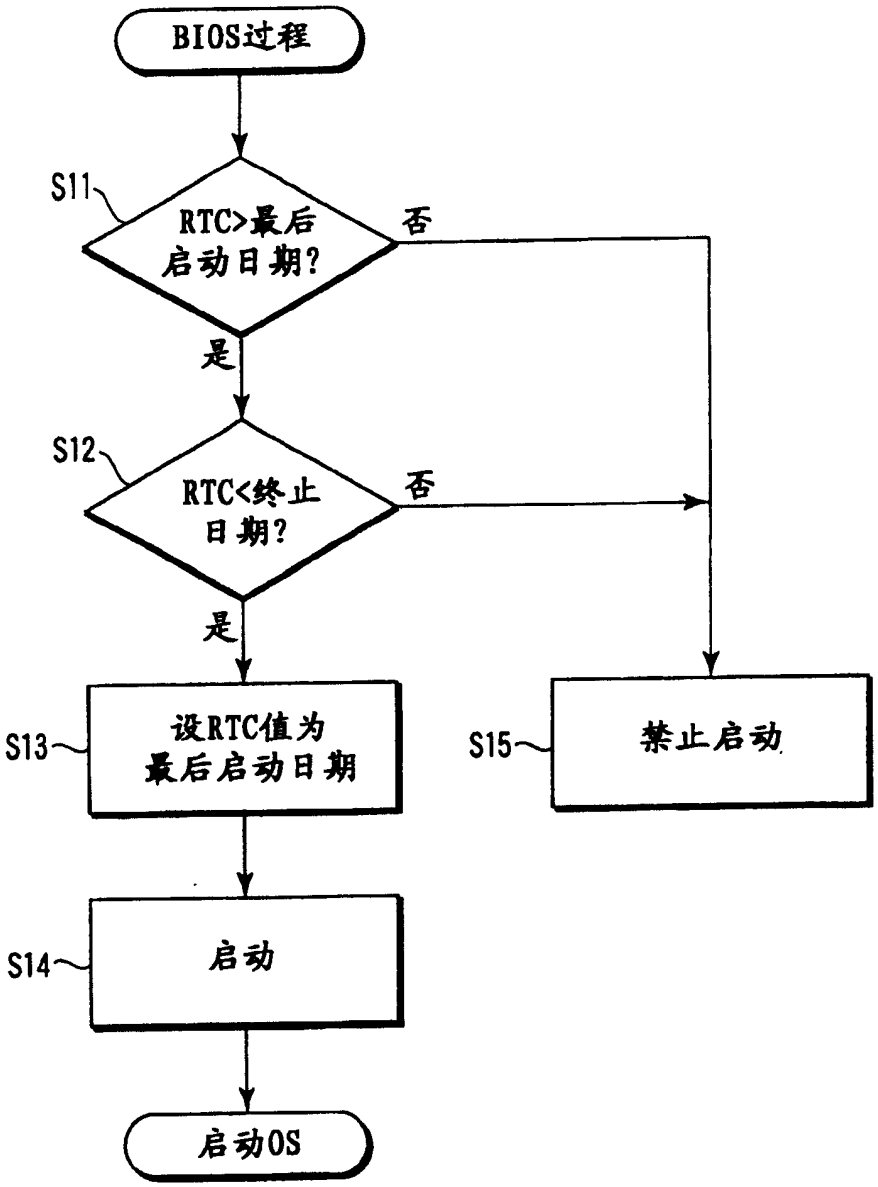

BIOS过程
S11
RTC>最后启动日期?
否
是
S12
RTC<终止日期?
否
是
S13
设RTC值为最后启动日期
S15
禁止启动
S14
启动
启动OS

图 3

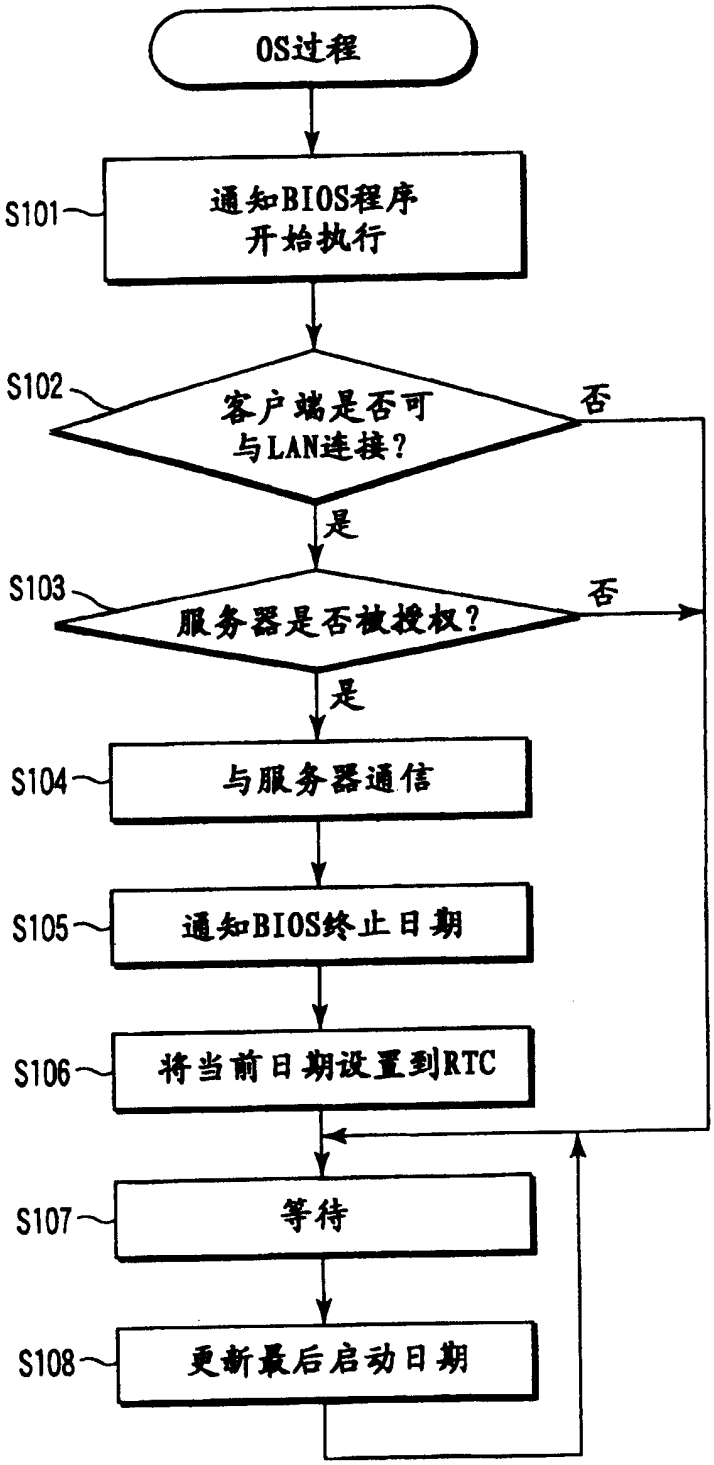

OS过程
S101
通知BIOS程序
开始执行
S102
客户端是否可
与LAN连接?
否
是
S103
服务器是否被授权?
否
是
S104
与服务器通信
S105
通知BIOS终止日期
S106
将当前日期设置到RTC
S107
等待
S108
更新最后启动日期

图 4

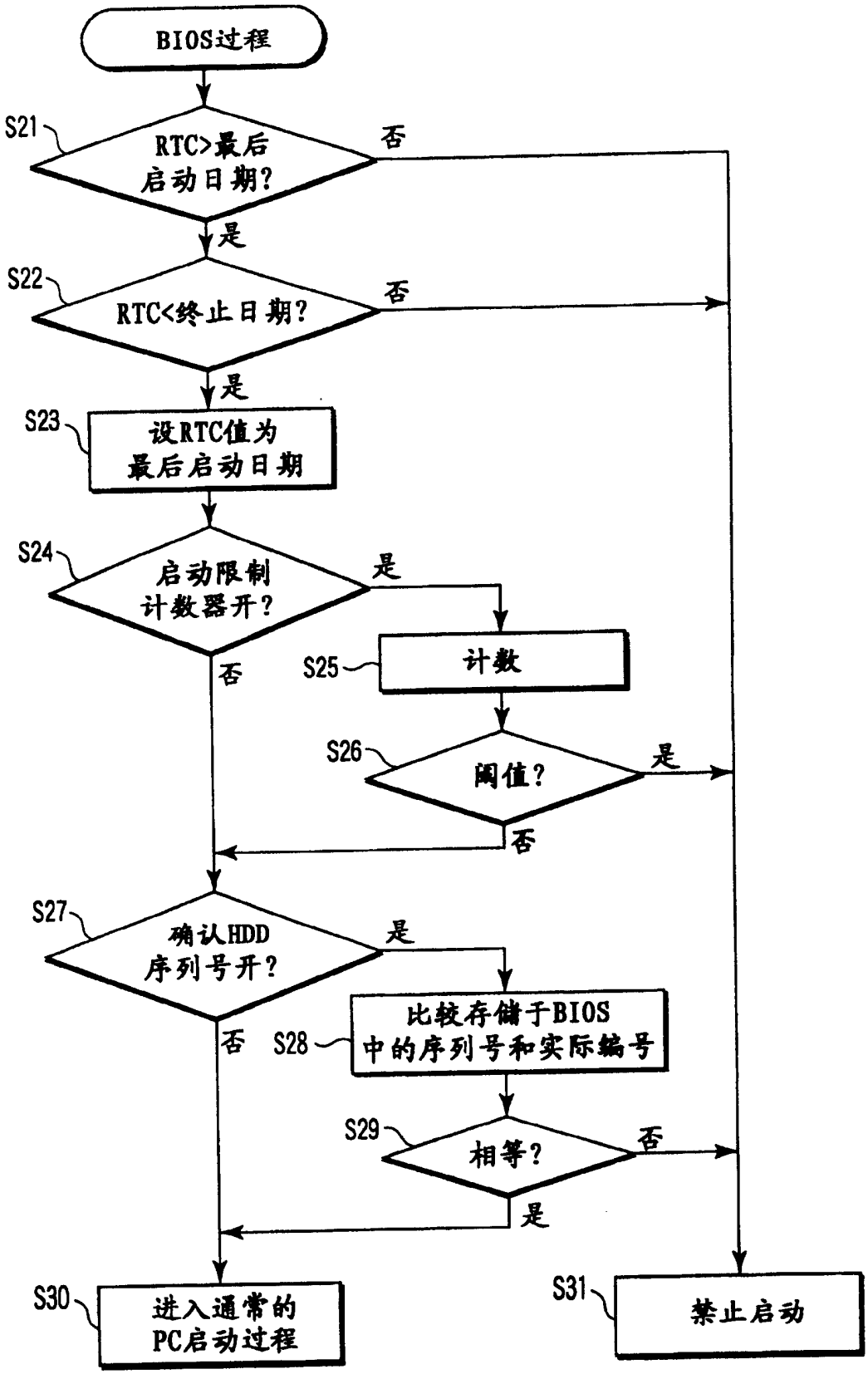

BIOS过程
S21
RTC>最后启动日期?
否
是
S22
RTC<终止日期?
否
是
S23
设RTC值为最后启动日期
S24
启动限制计数器开?
是
否
S25
计数
S26
阈值?
是
否
S27
确认HDD序列号开?
是
否
S28
比较存储于BIOS中的序列号和实际编号
S29
相等?
否
是
S30
进入通常的PC启动过程
S31
禁止启动

图 5