



(12)发明专利申请

(10)申请公布号 CN 106716919 A

(43)申请公布日 2017. 05. 24

(21)申请号 201580051935.5

(22)申请日 2015.09.11

(30)优先权数据

2014-196994 2014.09.26 JP

(85)PCT国际申请进入国家阶段日

2017.03.24

(86)PCT国际申请的申请数据

PCT/JP2015/075814 2015.09.11

(87)PCT国际申请的公布数据

W02016/047462 JA 2016.03.31

(71)申请人 国立大学法人名古屋大学

地址 日本爱知县

申请人 株式会社自动网络技术研究所

住友电装株式会社

住友电气工业株式会社

(72)发明人 高田广章 高仓弘喜 足立直树

宫下之宏 堀端启史 冈田宏

(74)专利代理机构 中原信达知识产权代理有限

责任公司 11219

代理人 权太白 谢丽娜

(51)Int.Cl.

H04L 9/32(2006.01)

G06F 21/64(2006.01)

G09C 1/00(2006.01)

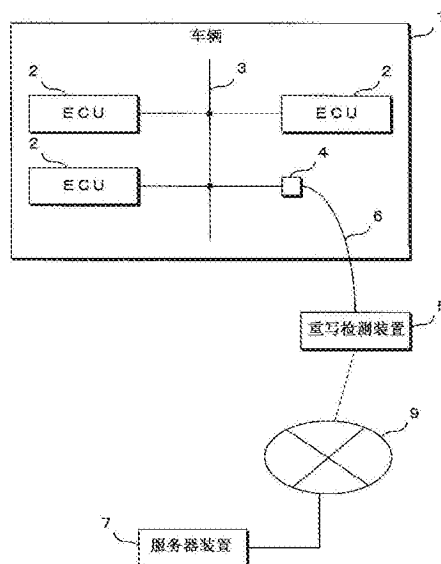
权利要求书2页 说明书16页 附图15页

(54)发明名称

重写检测系统及信息处理装置

(57)摘要

提供一种重写检测系统及信息处理装置,在利用散列值来检测非法重写的系统中,能够实现装置间的通信量的减少或各装置中的处理时间的缩短等。重写检测装置(5)生成随机种子并向ECU(2)发送,ECU(2)根据接收到的随机种子和存储部的存储内容,利用预定的散列函数来计算散列值并向重写检测装置(5)发送。此时,ECU(2)确定存储部的存储区域中的作为散列值计算的处理对象的存储区域,并进行散列值的计算。重写检测装置(5)判定从ECU(2)接收到的散列值是否正确,判定是否进行了针对程序或数据的非法重写。ECU(2)将相对于作为上一次散列值计算的对象的存储区域隔开了预定地址的存储区域设为作为本次处理对象的存储区域。



1. 一种重写检测系统, 针对具备存储有程序或数据的存储部、处理部和通信部的信息处理装置检测所述存储部所存储的程序或数据的重写, 所述处理部进行基于该存储部所存储的程序或数据的处理, 所述通信部通过网络进行与其他装置的通信,

所述重写检测系统的特征在于,

具备重写检测装置, 该重写检测装置具有:

种子信息发送单元, 通过所述网络向所述信息处理装置发送用于散列值计算的种子信息;

散列值接收单元, 接收与该种子信息发送单元发送的种子信息对应地从所述信息处理装置发送的散列值; 以及

散列值判定单元, 判定该散列值接收单元接收到的散列值是否正确,

所述重写检测装置根据该散列值判定单元的判定结果来检测重写,

所述信息处理装置具有:

存储区域确定单元, 从所述存储部确定应作为处理对象的存储区域; 以及

散列值计算单元, 计算基于所述种子信息发送单元发送的种子信息和存储在所述存储区域确定单元所确定的存储区域中的程序或数据的散列值,

所述信息处理装置将该散列值计算单元计算出的散列值向所述重写检测装置发送。

2. 根据权利要求1所述的重写检测系统, 其特征在于,

所述重写检测装置反复执行由所述种子信息发送单元进行的种子信息的发送来重复进行重写检测,

所述信息处理装置的所述存储区域确定单元将相对于作为上一次散列值计算的处理对象的存储区域隔开预定地址的存储区域确定为处理对象。

3. 根据权利要求1所述的重写检测系统, 其特征在于,

所述重写检测装置重复进行由所述种子信息发送单元进行的种子信息的发送来重复进行重写检测,

所述信息处理装置的所述存储区域确定单元将把所述存储部分成两部分而得到的第1存储区域和第2存储区域交替地确定为作为处理对象的存储区域。

4. 根据权利要求1所述的重写检测系统, 其特征在于,

所述重写检测装置重复进行由所述种子信息发送单元进行的种子信息的发送来重复进行重写检测,

所述重写检测装置具有信息发送单元, 在所述散列值接收单元接收到来自所述信息处理装置的散列值之后, 所述信息发送单元将指定应作为下一次散列值计算的处理对象的存储区域的存储区域指定信息向所述信息处理装置发送,

所述信息处理装置具有存储从所述重写检测装置接收到的所述存储区域指定信息的存储区域指定信息存储单元,

所述信息处理装置的所述存储区域确定单元根据所述存储区域指定信息存储单元所存储的所述存储区域指定信息来确定存储区域。

5. 根据权利要求2至4中的任一项所述的重写检测系统, 其特征在于,

所述重写检测装置具有信息发送单元, 该信息发送单元将指定应作为散列值计算的处理对象的第一次的存储区域的存储区域指定信息向所述信息处理装置发送,

所述信息处理装置的所述存储区域确定单元根据从所述重写检测装置接收到的所述存储区域指定信息,确定应作为处理对象的第一次的存储区域。

6.一种重写检测系统,针对具备存储有程序或数据的存储部、处理部和通信部的信息处理装置检测所述存储部所存储的程序或数据的重写,所述处理部进行基于该存储部所存储的程序或数据的处理,所述通信部通过网络进行与其他装置的通信,

所述重写检测系统的特征在于,

具备重写检测装置,该重写检测装置具有:

种子信息发送单元,通过所述网络向所述信息处理装置发送用于散列值计算的种子信息;

散列值接收单元,接收与该种子信息发送单元发送的种子信息对应地从所述信息处理装置发送的散列值;

散列值判定单元,判定该散列值接收单元接收到的散列值是否正确;以及

信息发送单元,在所述散列值接收单元接收到来自所述信息处理装置的散列值之后,将指定应作为下一次散列值计算的处理对象的存储区域的存储区域指定信息向所述信息处理装置发送,

所述重写检测装置根据所述散列值判定单元的判定结果来检测重写,

所述信息处理装置具有:

存储区域指定信息存储单元,存储从所述重写检测装置接收到的所述存储区域指定信息;以及

散列值计算单元,计算基于所述种子信息发送单元发送的种子信息和存储在由所述存储区域指定信息存储单元存储的存储区域指定信息指定的存储区域中的程序或数据的散列值,

所述信息处理装置将该散列值计算单元计算出的散列值向所述重写检测装置发送。

7.一种信息处理装置,其特征在于,具备:

存储部,存储有程序或数据;

处理部,进行基于该存储部所存储的程序或数据的处理;

通信部,通过网络进行与其他装置的通信;

存储区域确定单元,从所述存储部确定应作为处理对象的存储区域;以及

散列值计算单元,计算基于从其他装置发送的种子信息和存储在所述存储区域确定单元所确定的存储区域中的程序或数据的散列值,

所述信息处理装置将该散列值计算单元计算出的散列值向所述其他装置发送。

重写检测系统及信息处理装置

技术领域

[0001] 本发明涉及检测针对搭载在车辆中的ECU(Electronic Control Unit:电子控制单元)等信息处理装置的程序或数据的非法重写的重写检测系统以及构成该系统的信息处理装置。

背景技术

[0002] 在搭载于车辆的ECU等信息处理装置中,根据存储在ROM(Read Only Memory:只读存储器)等存储部中的程序和数据,由CPU(Central Processing Unit:中央处理单元)等处理部进行各种处理。在近年来的车辆中,通过CAN(Controller Area Network:控制器局域网)等车内网络来进行对存储在信息处理装置的存储部中的程序和数据的重写的功能得到应用。由此,能够使信息处理装置的软件版本升级等变得容易,易于实现信息处理装置的高功能化。

[0003] 在专利文献1中,提出了如下的车载网络系统:具备对车载控制装置进行认证的构成管理装置,该构成管理装置通过与车载网络连接的登记装置将用于实施构成证明的构成证明数据传送到车载控制装置。

[0004] 现有技术文献

[0005] 专利文献

[0006] 专利文献1:日本特开2013-17140号公报

发明内容

[0007] 发明要解决的课题

[0008] 由于是能够对存储在信息处理装置的存储部中的程序和数据进行重写的构成,存在进行非法的程序和数据重写的可能性。例如在如拼车或租车等数目不确定的用户利用车辆的情况下,存在由恶意的用户进行非法重写的可能性。另外,例如用户也有可能对自己拥有的车辆进行非法的改造。

[0009] 例如可以考虑通过在信息处理装置中搭载先进的认证功能或加密功能等,防止存储部的程序或数据的非法重写。但是,由于将这种功能搭载到信息处理装置,存在会导致信息处理装置的高成本化的问题。另外,难以完全防止非法重写。专利文献1中记载的车载网络系统也具有相同的问题。

[0010] 为了解决该问题,本申请的发明人提出了如下的系统:对信息处理装置发送种子信息,接收到该种子信息的信息处理装置使用种子信息和存储在存储部中的程序或数据来进行散列值的计算,根据由信息处理装置计算出的散列值是否与期望值一致来检测非法重写。

[0011] 本发明是鉴于如上所述的情况而完成的,其目的在于,提供一种重写检测系统及信息处理装置,在利用上述的散列值来检测非法重写的系统中,能够实现装置间的通信量的减少或各装置中的处理时间的缩短等。

[0012] 用于解决课题的技术方案

[0013] 本发明的重写检测系统,针对具备存储有程序或数据的存储部、处理部和通信部的信息处理装置检测所述存储部所存储的程序或数据的重写,所述处理部进行基于该存储部所存储的程序或数据的处理,所述通信部通过网络进行与其他装置的通信,所述重写检测系统的特征在于,具备重写检测装置,该重写检测装置具有:种子信息发送单元,通过所述网络向所述信息处理装置发送用于散列值计算的种子信息;散列值接收单元,接收与该种子信息发送单元发送的种子信息对应地从所述信息处理装置发送的散列值;以及散列值判定单元,判定该散列值接收单元接收到的散列值是否正确,所述重写检测装置根据该散列值判定单元的判定结果来检测重写,所述信息处理装置具有:存储区域确定单元,从所述存储部确定应作为处理对象的存储区域;以及散列值计算单元,计算基于所述种子信息发送单元发送的种子信息和存储在所述存储区域确定单元所确定的存储区域中的程序或数据的散列值,所述信息处理装置将该散列值计算单元计算出的散列值向所述重写检测装置发送。

[0014] 另外,在本发明的重写检测系统中,其特征在于,所述重写检测装置反复执行由所述种子信息发送单元进行的种子信息的发送来重复进行重写检测,所述信息处理装置的所述存储区域确定单元将相对于作为上一次散列值计算的处理对象的存储区域隔开预定地址的存储区域确定为处理对象。

[0015] 另外,在本发明的重写检测系统中,其特征在于,所述重写检测装置重复进行由所述种子信息发送单元进行的种子信息的发送来重复进行重写检测,所述信息处理装置的所述存储区域确定单元将把所述存储部分成两部分而得到的第1存储区域和第2存储区域交替地确定为作为处理对象的存储区域。

[0016] 另外,在本发明的重写检测系统中,其特征在于,所述重写检测装置重复进行由所述种子信息发送单元进行的种子信息的发送来重复进行重写检测,所述重写检测装置具有信息发送单元,在所述散列值接收单元接收到来自所述信息处理装置的散列值之后,所述信息发送单元将指定应作为下一次散列值计算的处理对象的存储区域的存储区域指定信息向所述信息处理装置发送,所述信息处理装置具有存储从所述重写检测装置接收到的所述存储区域指定信息的存储区域指定信息存储单元,所述信息处理装置的所述存储区域确定单元根据所述存储区域指定信息存储单元所存储的所述存储区域指定信息来确定存储区域。

[0017] 另外,在本发明的重写检测系统中,其特征在于,所述重写检测装置具有信息发送单元,该信息发送单元将指定应作为散列值计算的处理对象的第一次的存储区域的存储区域指定信息向所述信息处理装置发送,所述信息处理装置的所述存储区域确定单元根据从所述重写检测装置接收到的所述存储区域指定信息,确定应作为处理对象的第一次的存储区域。

[0018] 另外,本发明的重写检测系统,针对具备存储有程序或数据的存储部、处理部和通信部的信息处理装置检测所述存储部所存储的程序或数据的重写,所述处理部进行基于该存储部所存储的程序或数据的处理,所述通信部通过网络进行与其他装置的通信,所述重写检测系统的特征在于,具备重写检测装置,该重写检测装置具有:种子信息发送单元,通过所述网络向所述信息处理装置发送用于散列值计算的种子信息;散列值接收单元,接收

与该种子信息发送单元发送的种子信息对应地从所述信息处理装置发送的散列值;散列值判定单元,判定该散列值接收单元接收到的散列值是否正确;以及信息发送单元,在所述散列值接收单元接收到来自所述信息处理装置的散列值之后,将指定应作为下一次散列值计算的处理对象的存储区域的存储区域指定信息向所述信息处理装置发送,所述重写检测装置根据所述散列值判定单元的判定结果来检测重写,所述信息处理装置具有:存储区域指定信息存储单元,存储从所述重写检测装置接收到的所述存储区域指定信息;以及散列值计算单元,计算基于所述种子信息发送单元发送的种子信息和存储在由所述存储区域指定信息存储单元存储的存储区域指定信息指定的存储区域中的程序或数据的散列值,所述信息处理装置将该散列值计算单元计算出的散列值向所述重写检测装置发送。

[0019] 另外,本发明的信息处理装置,其特征在于,具备:存储部,存储有程序或数据;处理部,进行基于该存储部所存储的程序或数据的处理;通信部,通过网络进行与其他装置的通信;存储区域确定单元,从所述存储部确定应作为处理对象的存储区域;以及散列值计算单元,计算基于从其他装置发送的种子信息和存储在所述存储区域确定单元所确定的存储区域中的程序或数据的散列值,所述信息处理装置将该散列值计算单元计算出的散列值向所述其他装置发送。

[0020] 在本发明中,重写检测装置生成种子信息并向信息处理装置发送,根据信息处理装置接收到的种子信息和存储在存储部中的程序或数据来计算散列值并向重写检测装置发送。此时,信息处理装置自行确定存储部的存储区域中的作为散列值计算的处理对象的存储区域,并进行散列值的计算。另外,对于种子信息,例如能够生成预定位数的随机的值来利用。重写检测装置判定从信息处理装置接收到的散列值是否正确,判定是否进行了针对程序或数据的非法重写。即,重写检测装置能够在散列值正确时判断为未进行非法重写,在散列值不正确时判断为进行了非法重写。

[0021] 由此,能够检测针对信息处理装置的程序或数据的非法重写,能够适当地进行对进行了非法重写的信息处理装置的动作停止、修理或更换等处理。由于信息处理装置自行确定应作为处理对象的存储区域,重写检测装置无需将指定存储区域的信息等向信息处理装置发送,能够减少重写检测装置和信息处理装置之间的通信量。另外,信息处理装置通过种子信息的接收,不用等待指定存储区域的信息的接收等就能够开始散列值计算的处理,因此能够缩短处理时间。

[0022] 另外,在本发明中,信息处理装置将相对于作为上一次散列值计算对象的存储区域隔开预定地址的存储区域设为作为本次处理对象的存储区域。即,在上一次的存储区域为例如从A0地址到A1地址时,信息处理装置能够将本次的存储区域确定为例如从A0+ α 地址到A1+ α 地址。另外,重写检测装置也存储相同的预定地址 α ,掌握信息处理装置是使用哪个存储区域进行了散列值的计算。由此,信息处理装置能够容易且切实地确定应作为处理对象的存储区域。

[0023] 另外,在本发明中,信息处理装置将存储区域分成两部分来利用,例如将前半部分作为第1存储区域且将后半部分作为第2存储区域来交替地切换散列值计算的处理对象。由此,信息处理装置能够容易且切实地确定应作为处理对象的存储区域。

[0024] 另外,在本发明中,重写检测装置在从信息处理装置接收到散列值之后,将指定应作为下一次散列值计算的处理对象的存储区域的信息向信息处理装置发送。信息处理装置

从重写检测装置接收存储区域的指定信息并存储,将由进行下一次散列值计算时存储的信息指定的存储区域作为处理对象。该结构虽然需要每次都从重写检测装置向信息处理装置发送指定存储区域的信息,但是信息发送能够在到进行下一次的检测处理为止的任意的时刻进行,因此例如也能够选择网络的负载少的情况等来进行信息发送。另外,信息处理装置在从重写检测装置接收到种子信息时,不用等待指定存储区域的信息的接收就能够根据所存储的信息来确定存储区域并进行散列值的计算,因此能够缩短处理时间。

[0025] 另外,在本发明中,在重复进行的检测处理的第一次中,重写检测装置将指定应作为处理对象的第一次的存储区域的信息发送到信息处理装置。信息处理装置在从重写检测装置接收到指定存储区域的信息时,将所指定的存储区域作为处理对象来进行散列值的计算,在除此以外的情况下通过上述的方法进行散列值的计算。由此,在重复进行的检测处理的第一次中,信息处理装置能够切实地进行散列值的计算。

[0026] 另外,也可以构成为,重写检测装置不指定第一次的存储区域,而是将例如存储部的最前头区域等预先确定的存储区域作为第一次的存储区域来进行散列值的计算。

[0027] 发明效果

[0028] 在本发明的情况下,通过构成为由信息处理装置确定应作为散列值计算的处理对象的存储区域,能够实现重写检测装置和信息处理装置间的通信量的减少或重写检测的处理所需的各装置中的处理时间的缩短等。

附图说明

[0029] 图1是示出本实施方式的重写检测系统的结构的示意图。

[0030] 图2是示出ECU的结构的框图。

[0031] 图3是示出ECU的存储部的结构的示意图。

[0032] 图4是示出重写检测装置的结构的框图。

[0033] 图5是示出服务器装置的结构的框图。

[0034] 图6是示出重写检测数据库的第1构成例的示意图。

[0035] 图7是示出重写检测数据库的第2构成例的示意图。

[0036] 图8是用于说明基于重写检测装置的重写检测处理的示意图。

[0037] 图9是用于说明实施方式1的ECU的存储区域确定方法的示意图。

[0038] 图10是示出重写检测装置进行的重写检测处理的步骤的流程图。

[0039] 图11是示出ECU所进行的重写检测处理的步骤的流程图。

[0040] 图12是示出服务器装置所进行的重写检测处理的步骤的流程图。

[0041] 图13是用于说明实施方式2的ECU的存储区域确定方法的示意图。

[0042] 图14是用于说明实施方式3的基于重写检测系统的存储区域确定方法的示意图。

[0043] 图15是示出实施方式3的重写检测装置所进行的重写检测处理的步骤的流程图。

[0044] 图16是示出实施方式3的ECU所进行的重写检测处理的步骤的流程图。

具体实施方式

[0045] (实施方式1)

[0046] <系统结构>

[0047] 以下,对于本发明,根据示出其实施方式的附图来具体地进行说明。图1是示出本实施方式的重写检测系统的结构的示意图。在附图中,1为车辆,在车辆1中例如搭载有车身ECU和发动机ECU等各种ECU2。搭载于车辆1的多个ECU2经由CAN等车内网络3连接,能够彼此进行信息的收发。另外,在车辆1中设置有用对车内网络3连接其他装置的连接器4。

[0048] 本实施方式的重写检测系统具备重写检测装置5,该重写检测装置5对进行了针对搭载于车辆1的ECU2的程序或数据的非法重写的情况进行检测。重写检测装置5为可移动式装置,例如保管在车辆1的经销商或修理厂等中。重写检测装置5经由通信线缆6与设置在车辆1中的连接器4连接,从而能够通过车内网络3进行与ECU2的通信。重写检测装置5在连接器4连接有通信线缆6的状态下进行针对ECU2的程序或数据的非法重写的检测处理。

[0049] 另外,重写检测装置5具有进行利用了无线LAN(Local Area Network:局域网)或移动电话网络等的无线通信的功能。在本实施方式中,重写检测装置5利用该无线通信功能,通过因特网等网络9进行与服务器装置7的通信。服务器装置7是由例如车辆1的制造公司或销售公司等管理、运营的装置。服务器装置7存储重写检测装置5的重写检测处理所需的信息,并根据进行重写检测处理时提供的来自重写检测装置5的请求,将所需的信息发送到重写检测装置5。

[0050] 图2是示出ECU2的结构的框图。ECU2构成为具备处理部21、存储部22以及通信部23等。处理部21利用CPU(Central Processing Unit:中央处理单元)等运算处理装置构成。处理部21通过读取并执行存储部22所存储的程序,进行车辆1的各种信息处理。

[0051] 存储部22利用闪存或EEPROM(Electrically Erasable Programmable Read Only Memory:电可擦除可编程只读存储器)等能够非易失性地重写数据的存储器元件构成。存储部22存储处理部21所执行的程序和由此进行的处理中所需的各种数据。在本实施方式中,存储部22作为ROM来使用,而存储在存储部22中的程序或数据不会通过处理部21的处理而被重写。但是,能够进行基于程序的版本升级等的重写。

[0052] 通信部23例如依照CAN等的通信协议,进行经由车内网络3的与其他ECU2的通信。通信部23将从处理部21提供的发送用信息转换为依照通信协议的发送信号,并通过向构成车内网络3的通信线输出转换后的信号来进行向其他ECU2的信息发送。通信部23对车内网络3的通信线的电位进行采样,从而获取其他ECU2输出的信号,通过将该信号依照通信协议转换为二进制的信息来进行信息的接收,并将接收到的信息提供给处理部21。

[0053] 另外,在本实施方式中,ECU2的处理部21具有根据来自重写检测装置5的指示来计算散列值的散列值计算部24。散列值计算部24根据从重写检测装置5提供的随机种子(种子信息)和存储在存储部22中的程序或数据,通过预定的散列计算算法(散列函数)计算散列值。散列值计算部24可以实现为软件,也可以实现为硬件。对于散列值的计算方法的详细内容,将在后文中详细叙述。

[0054] 图3是示出ECU2的存储部22的结构的示意图。在图示的例子中,存储部22具有地址(地址)以0000h~FFFFh表示的存储区域。在存储部22中存储有由处理部21执行的两个程序(程序1和程序2)、在各程序的执行中各自所需的两种数据(数据1和数据2)。在存储部22中,从地址的最前头侧起按顺序存储有程序1、程序2、数据1、数据2,在它们之间的存储区域和地址的末尾侧的存储区域中存储有虚拟数据。

[0055] 虚拟数据可以是任意的值,例如能够存储随机确定的值。虚拟数据写入到存储部

22的全部的剩余区域。即,在存储部22中,在其全部的存储区域中存储有某种数据。由此,能够防止在存储部22的剩余区域中存储非法的程序而进行非法的处理的情况。另外,能够使存储在存储部22中的程序和数据难以压缩。

[0056] 图4是示出重写检测装置5的结构框图。重写检测装置5具备处理部51、存储部52、操作部53、显示部54、有线通信部55以及无线通信部56等构成。处理部51利用CPU等运算处理装置构成。处理部51通过读取存储在存储部52中的程序并执行,进行针对搭载于车辆1的ECU2的程序或数据的非法重写的检测处理。存储部52利用闪存等非易失性的存储器元件构成,存储有处理部51所执行的程序和执行中所需的各种数据。重写检测装置5可以将处理部51的处理过程中产生的临时的信息存储到存储部52,也可以具备存储临时的信息的RAM(Random Access Memory:随机存取存储器)。

[0057] 操作部53利用按钮开关或触摸面板等构成,受理用户的操作并通知到处理部51。显示部54利用液晶面板等构成,根据来自处理部51的指示,显示针对用户的各种图像和消息等。有线通信部55例如依照CAN等的通信协议,进行经由通信线缆6的与其他装置的通信。在通信线缆6连接到车辆1的连接器4时,有线通信部55能够通过车辆1的车内网络3进行与ECU2的通信。无线通信部56进行利用无线LAN或移动电话网络等的无线通信,从而通过因特网等网络9进行与服务器装置7的通信。

[0058] 图5是示出服务器装置7的结构框图。服务器装置7具备处理部71、存储部72以及通信部73等而构成。处理部71利用CPU等运算处理装置构成。处理部71通过读取并执行在存储部72中存储的程序,进行发送在重写检测装置5的重写检测处理中所需的信息的处理。通信部73通过因特网等网络9进行与其他装置的通信。在本实施方式中,通信部73在与重写检测装置51之间进行通信,将从重写检测装置51接收到的信息提供给处理部71,并且将从处理部71提供的发送用的信息向重写检测装置51发送。

[0059] 存储部72利用硬盘等大容量的存储装置构成。在本实施方式中,在存储部72中构建有重写检测数据库75。重写检测数据库75是存储有在重写检测装置5的重写检测处理中所需的信息的数据库。关于重写检测数据库75,可以考虑几种结构,以下示出两个构成例。

[0060] 图6是示出重写检测数据库75的第1构成例的示意图。在第1构成例的重写检测数据库75中建立对应地存储有“车型”、“ECU类型”以及“存储内容”。在重写检测数据库75的“车型”中存储有用于识别车辆1的种类的识别信息等。即使车辆1的车名和外观等相同,在级别等不同而所搭载的ECU2的结构不同时,在本实施方式中也将这些车辆处理为不同的车型。在图示的例子中,在重写检测数据库75中存储有车型A、车型B…的信息以作为“车型”。在重写检测数据库75的“ECU类型”中存储有例如用于识别车身ECU或发动机ECU等ECU20的种类的识别信息等。在图示的例子中,在重写检测数据库75中存储有ECUa、ECUb…的信息以作为“ECU类型”。重写检测数据库75的“存储内容”是对应的ECU2的存储部22的存储内容的拷贝。

[0061] 重写检测装置5指定“车型”、“ECU类型”、“存储区域”以及“随机种子”并向服务器装置7询问期望值。与询问有关的“存储区域”是用于指定ECU2的存储部22的存储区域的一部分的信息,例如通过开始地址X和结束地址Y的组合或开始地址X和区域尺寸Z的组合等来指定存储区域。与询问有关的“随机种子”是重写检测装置5生成的信息,在本实施方式中是16进制且4位的数值。

[0062] 服务器装置7从与该询问有关的车型和ECU类型对应的存储内容中读取通过询问来指定的存储区域的存储内容。服务器装置7根据与询问有关的随机种子和所读取的存储内容来进行散列值的计算,并将计算出的散列值作为期望值向重写检测装置5发送。由此,服务器装置7存储与ECU2的散列值计算部24所使用的散列函数相同的函数。

[0063] 图7是示出重写检测数据库75的第2构成例的示意图。在第2构成例的重写检测数据库75中建立对应地存储有“车型”、“ECU类型”、“存储区域”、“随机种子”以及“期望值”。其中“车型”和“ECU类型”与第1构成例相同。第2构成例的重写检测数据库75的“存储区域”是指定ECU2的存储部22的存储区域的一部分的信息。在图示的例子中,将存储部22划分为多个存储区域以作为第1区域、第2区域…。各区域可以不是相同的尺寸,也可以具有重复的部分。

[0064] 重写检测数据库75的“随机种子”是重写检测装置5所生成的随机种子,在本实施方式中为16进制且4位的数值。在图示的例子中,关于“随机种子”,针对每个“ECU类型”设定有如0000h~FFFFh的65536这样的值。重写检测数据库75的“期望值”是应该由ECU3针对“存储区域”和“随机种子”计算的散列值,在本实施方式中为16进制且4位的数值。“期望值”是关于ECU2的存储部22的存储内容(程序、数据和虚拟数据)的针对存储在对应的“存储区域”中的存储内容使用对应的“随机种子”预先计算散列值并存储的值。另外,图示的“期望值”为一例。

[0065] 重写检测装置5指定“车型”、“ECU类型”、“存储区域”以及“随机种子”并向服务器装置7询问期望值。服务器装置7根据该询问而从重写检测数据库75读取对应的期望值并向重写检测装置5发送。

[0066] 另外,在本实施方式中,如果车型和ECU类型相同,则存储在ECU2的存储部22中的程序和数据相同。不过,根据车辆1的目的地或程序的版本差异等,可能存在即使车型和ECU类型相同,所存储的程序和数据也不同的情况。在这种情况下,例如在重写检测数据库75中设置有程序的版本等项目,针对每个版本存储有存储部22的存储内容,或者,针对每个版本存储有期望值。重写检测装置5从该ECU2获取作为重写检测处理的对象的ECU2的程序的版本,在向服务器装置7进行期望值的询问时将程序的版本信息与车型和随机种子等的信息一起发送。服务器装置7能够根据来自重写检测装置5的程序的版本信息,从重写检测数据库75读取适当的信息,并向重写检测装置5发送期望值。

[0067] <散列值计算方法>

[0068] ECU2的散列值计算部24能够构成为,例如利用MD(Message Digest:消息摘要)4、MD5、SHA-1、SHA-256、SHA-384、SHA-512、EIPMD-160或SHA-3等现有的散列函数来进行散列值的计算。这些是所谓的单向散列函数,是针对所输入的信息输出一个散列值的函数。输入到散列函数的信息在本实施方式中是存储在ECU2的存储部22中的程序或数据的一部分或全部。即使输入到散列函数中的信息为程序或数据中的任一种或者是程序和数据这双方,散列函数也能够将所输入的信息简单地处理为二进制的信息,并计算散列值。散列值计算部24存储预先确定的散列函数,利用该散列函数进行散列值的计算。

[0069] 以下,简单地对散列值计算部24利用SHA-1的散列函数来计算散列值的情况进行说明。另外,关于SHA-1的散列函数的详细的处理以及散列值计算部24利用其他散列函数的情况,由于这些散列函数为现有的技术,因此省略说明。

[0070] 在利用SHA-1的散列函数时,散列值计算部24首先进行填充处理。在填充处理中,散列值计算部24通过在输入信息之后附加额外的数据,以使处理对象的信息的大小成为预定值(512位)的整数倍的方式进行调整。接着,散列值计算部24将被填充处理的信息按照每512位的块进行分割,进行对各块计算80个值的第1处理。

[0071] 接着,散列值计算部24针对预定大小(160位)的初始值进行如下的第二处理:进行了通过第1处理计算出的值的运算,并将运算后的160位的值作为散列值。在第2处理中,首先,散列值计算部24使用针对一个块计算出的80个值,对160位的初始值进行80步骤的运算。通过该80步骤的运算,能够对160位的初始值混入块的信息,作为输出而得到160位的值。散列值计算部24将所得到的160位的值作为初始值,使用针对下一个块计算的80个值同样地进行80步骤的运算。散列值计算部24针对全部的块进行同样的80步骤的处理,将最终得到的160位的值作为散列值。

[0072] 另外,在本实施方式中,散列值计算部24需要利用从重写检测装置5提供的随机种子来进行散列值的计算。例如散列值计算部24在上述的填充处理中,能够对附加到输入信息的数据使用随机种子。另外,例如散列值计算部24在上述的第2处理中,能够对160位的初始值使用随机种子。在本实施方式中,对第2处理的初始值使用随机种子。

[0073] 另外,基于散列值计算部24的随机种子的利用方法不限于上述的方法。例如散列值计算部24能够将作为散列值计算的对象的存储部22的信息与随机种子的逻辑运算值(异或等)作为向散列函数的输入信息。另外,例如散列值计算部24能够使对作为散列值计算的对象的存储部22的信息的最前头部分或末尾部分等预定位置附加了随机种子而得到的信息作为向散列函数的输入信息。

[0074] <重写检测处理>

[0075] 例如在车辆1的车检、定期检查或修理等时,经销商或修理厂等的作业人员将重写检测装置5的通信线缆6连接到车辆1的连接部4,将重写检测装置5连接到车辆1的车内网络3。作业人员进行针对重写检测装置5的操作部53的操作,将开始针对车辆1的ECU2的非法重写的检测处理的指示提供给重写检测装置5。

[0076] 重写检测装置5在由操作部53受理了非法重写检测处理的开始指示时,通过有线通信部55开始与车辆1的ECU2的通信。在本实施方式中,重写检测装置5从搭载于车辆1的多个ECU2中适当地选择一个,进行所选择的存储在ECU2的存储部22中的程序和数据的非法重写的检测处理。在对一个ECU2结束了检测处理之后,重写检测装置5进行针对未处理的ECU2的检测处理。重写检测装置5通过重复这些处理来对多个ECU2依次进行检测处理,对搭载于车辆1的能够作为检测对象的全部的ECU2进行非法重写的检测处理。

[0077] 另外,重写检测装置5也可以构成为,针对连接到车内网络3的多个ECU2同时进行非法重写的检测处理。但是,在本实施方式中,如上所述重写检测装置5针对多个ECU2依次进行非法重写的检测处理。另外,在下文中,为了简化说明,对重写检测装置5进行针对一个ECU2的非法重写的检测处理的情况进行说明。对多个ECU2重复进行同样的处理即可。

[0078] 图8是用于说明基于重写检测装置5的重写检测处理的示意图。连接到车辆2的车内网络3的重写检测装置5针对作为重写检测处理的对象的ECU2通知开始重写检测处理等。与此对应地,作为对象的ECU2例如中断其他处理而进行散列值计算部24的处理的准备等(但是,无需一定中断其他处理,也可以构成为散列值计算部24能够与其他处理并行地进行

处理)。

[0079] 重写检测装置5根据适当的随机数生成算法来生成随机的值,将该值作为随机种子发送到ECU2。随机种子可以是例如64位以上的随机的值。在散列值计算部24使用SHA-1作为散列函数时,随机种子可以是例如160位。接收到来自重写检测装置5的随机种子的ECU2进行确定存储部22的存储区域中的作为散列值计算的处理对象的存储区域的处理,并读取所确定的存储区域的存储内容。ECU2根据接收到的随机种子和所读取的存储内容,利用预先确定的散列函数来计算散列值。ECU2将计算出的散列值向重写检测装置5发送。

[0080] 另外,重写检测装置5将所生成的随机种子向服务器装置7发送,询问针对该随机种子的散列值的期望值。此时,重写检测装置5以与ECU2相同的方法确定作为散列值计算的处理对象的存储部22的存储区域。重写检测装置5将进行重写检测处理的车辆1的车辆ID(Identifier:标识符)或车型等车辆信息、识别处理对象的ECU2的ID等ECU识别信息以及指定作为散列值计算的处理对象的存储区域的信息与随机种子一起向服务器装置7发送。

[0081] 接收到这些信息的服务器装置7参照存储部72的重写检测数据库75。例如在重写检测数据库75为图6所示的结构时,服务器装置7从根据与来自重写检测装置5的询问有关的车型和ECU类型存储的ECU2的存储内容中读取与通过询问指定的存储区域对应的存储内容。服务器装置7根据从重写检测数据库75读取的存储内容以及与来自重写检测装置5的询问有关的随机种子来计算散列值,将所计算出的散列值作为期望值向重写检测装置5发送。

[0082] 重写检测装置5对从ECU2接收到的散列值与从服务器装置7接收到的期望值进行比较。在散列值和期望值一致时,重写检测装置5判定为未进行针对存储在ECU2的存储部22中的程序和数据的非法重写。与此相对地,在散列值和期望值不一致时,重写检测装置5判定为进行了针对ECU2的程序和数据的非法重写。作为重写检测处理的处理结果,重写检测装置5在显示部54中显示是否进行了非法重写。

[0083] 另外,重写检测装置5也可以对从向ECU2发送随机种子起到接收散列值为止的时间进行计测,并进行基于所计测到的时间的重写的有无。此时,重写检测装置5判定所计测到的时间是否超过阈值,在计测时间超过阈值时,判定为进行了针对ECU2的程序和数据的非法重写。另外,关于在判定中使用的阈值,考虑重写检测装置5和ECU2的通信速度和ECU2的处理能力等,在本系统的设计阶段等中预先确定。

[0084] <存储区域确定方法>

[0085] ECU2的散列值计算部24在根据来自重写检测装置5的随机种子来计算散列值时,进行确定应作为计算处理对象的存储部22的存储区域的处理。图9是用于说明实施方式1的ECU2的存储区域确定方法的示意图。基于散列值计算部24的存储区域的确定方法在首次计算散列值的情况下和第二次以后计算散列值的情况下不同。在本实施方式中,重写检测装置5确定作为散列值计算对象的第一次的存储区域并通知给ECU2。ECU2的散列值计算部24在首次进行散列值的计算的情况(例如,未存储与上一次散列值计算有关的信息的情况下)下,从重写检测装置5接收随机种子和指定作为散列值计算的处理对象的存储区域的信息,将所指定的存储区域作为散列值计算处理的对象。在图9中,重写检测装置5例如像“从X地址到Y地址为止以Z地址间隔”这样将不连续的多个区域指定为第一次的存储区域。因此,ECU2的散列值计算部24将存储部22的X地址~Y地址、X+Z地址~Y+Z地址、X+2Z地址~Y+2Z地址、…、作为散列值计算的处理对象的存储区域。另外,X、Y、Z的值可以是预先确定的值,

也可以每次由重写检测装置5随机确定。ECU2的散列值计算部24根据所指定的存储区域的存储内容和接收到的随机种子来计算散列值,并且存储与在散列值计算中使用的存储区域有关的信息(本例中为X、Y、Z的值等)。

[0086] ECU2的散列值计算部24能够根据是否存储有与在上一次散列值计算中使用的存储区域有关的信息,判断本次的处理为第一次还是第二次之后。散列值计算部24在第二次之后计算散列值的情况下,根据在上一次散列值计算中使用的存储区域来确定在本次的散列值计算处理中使用的存储区域。散列值计算部24预先存储在确定存储区域时使用的预定值 α 。散列值计算部24将对表示上一次的存储区域的地址加上 α 地址而得到的地址作为本次的散列值计算的处理对象的存储区域。在图9所示的例子中,散列值计算部24将存储部22的 $X+\alpha \sim Y+\alpha$ 、 $X+\alpha+Z \sim Y+\alpha+Z$ 、 $X+\alpha+2Z \sim Y+\alpha+2Z$ 、 $\cdots$ 、作为第二次的散列值计算的处理对象的存储区域。散列值计算部24存储与第二次的存储区域有关的信息,同样地,第三次将存储部22的 $X+2\alpha \sim Y+2\alpha$ 、 $X+2\alpha+Z \sim Y+2\alpha+Z$ 、 $X+2\alpha+2Z \sim Y+2\alpha+2Z$ 、 $\cdots$ 、作为散列值计算的处理对象的存储区域。

[0087] 另外,重写检测装置5针对在第二次以后计算出的散列值向服务器装置7询问期望值,因此需要知晓第二次以后的散列值是根据哪个存储区域计算出的散列值。因此,重写检测装置5存储ECU2的预定值 α 和对于该ECU2来说是第几次散列值计算的信息。预定值 α 例如可以由重写检测装置5预先存储,或者也可以例如在第一次散列值计算时等从ECU2获取,或者也可以例如由重写检测装置5确定预定值 α 并与第一次的存储区域指定信息一起发送到ECU2。重写检测装置5根据所存储的预定值 α 和是第几次的散列值计算的信息,特定作为本次散列值计算的处理对象的存储区域,将表示该存储区域的信息和随机种子等发送到服务器装置7来询问期望值。

[0088] <流程图>

[0089] 接着,使用流程图对本实施方式的重写检测系统所进行的重写检测处理进行说明。另外,在本说明中,采用图6所示的结构作为重写检测数据库。图10是示出重写检测装置5所进行的重写检测处理的步骤的流程图。重写检测装置5的处理部51根据随机数生成算法来生成随机种子(步骤S1)。处理部51判定发送随机种子的ECU2的散列值计算的处理是否为第一次(步骤S2)。在是第一次处理时(S2:是),处理部51将指定应作为散列值计算的处理对象的存储区域的信息与在步骤S1中生成的随机种子一起通过有线通信部55向作为对象的ECU2发送(步骤S3),使处理推进到步骤S6。

[0090] 在本次散列值计算处理不是第一次而是第二次以后的处理时(S2:否),处理部51将在步骤S1中生成的随机种子向作为对象的ECU2发送(步骤S4)。另外,处理部51获取针对该ECU2存储的预定值 α 和进行了散列值计算处理的次数,根据预定值 α 和次数来特定作为本次散列值计算的处理对象的ECU2的存储部22的存储区域(步骤S5),使处理推进到步骤S6。

[0091] 处理部51判定是否由有线通信部55接收了从作为处理对象的ECU2针对随机种子发送的散列值(步骤S6),在未接收时(S6:否),待机直到接收到散列值为止。在接收到散列值时(S6:是),处理部51将车辆信息和ECU2的识别信息、在步骤S1中生成的随机种子以及在步骤S3中指定的存储区域或在步骤S5中特定的存储区域发送到服务器装置7,询问针对从ECU2接收到的散列值的期望值(步骤S7)。处理部51判定是否接收到从服务器装置7针对询问而发送的期望值(步骤S8),在未接收期望值时(S8:否),待机直到接收到期望值为止。

[0092] 在从服务器装置7接收到期望值时(S8:是),处理部51判定在步骤S6中接收到的散列值与在步骤S8中接收到的期望值是否一致(步骤S9)。在散列值和期望值一致时(S9:是),处理部51判定为未进行非法重写(步骤S10),通过显示部54通知该内容并结束处理。在散列值和期望值不一致时(S9:否),处理部51判定为进行了非法重写(步骤S11),通过显示部54通知该内容并结束处理。

[0093] 图11是示出ECU2所进行的重写检测处理的步骤的流程图。ECU2的处理部21判定是否由通信部23接收到重写检测装置5发送的随机种子(步骤S21),在未接收随机种子时(S21:否),待机直到接收到随机种子为止。在接收到随机种子时(S21:是),处理部21的散列值计算部24根据是否存储有与上一次散列值计算处理有关的信息等,判定散列值计算处理是否为第一次(步骤S22)。在是第一次处理时(S22:是),散列值计算部24获取与随机种子一起从重写检测装置5发送的存储区域的指定信息(步骤S23),使处理推进到步骤S25。在不是第一次处理时(S22:否),散列值计算部24根据与在上一次散列值计算处理中使用的存储区域有关的信息和预定值 α ,确定作为本次散列值计算的处理对象的存储区域(步骤S24),使处理推进到步骤S25。

[0094] 处理部21的散列值计算部24根据从重写检测装置5接收到的随机种子以及通过在步骤S23中获取的信息指定的存储区域或在步骤S24中确定的存储区域的存储内容,使用预定的散列函数来进行散列值的计算(步骤S25)。处理部21将散列值计算部24计算出的散列值通过通信部23发送到重写检测装置5(步骤S26),并结束处理。

[0095] 图12是示出服务器装置7所进行的重写检测处理的步骤的流程图。服务器装置7的处理部71判定是否由通信部73接收到来自重写检测装置5的期望值的询问(步骤S31),在未接收时(S31:否),待机直到接收到询问为止。在接收到来自重写检测装置5的询问时(S31:是),处理部71根据询问所包含的车辆信息、ECU类型信息以及存储区域的指定信息等,从存储部72的重写检测数据库75获取所指定的存储区域的存储内容(步骤S32)。接着,处理部71根据来自重写检测装置5的询问所包含的随机种子和在步骤S32中获取的存储内容,进行散列值的计算(步骤S33)。处理部71将计算出的散列值作为期望值发送到重写检测装置5(步骤S34),并结束处理。

[0096] <总结>

[0097] 在以上结构的实施方式1的重写检测系统中,重写检测装置5生成随机种子并发送到ECU2,ECU2根据接收到的随机种子和存储部52的存储内容(程序或数据),使用预定的散列函数来计算散列值并发送到重写检测装置5。此时,ECU2自行确定存储部22的存储区域中的作为散列值计算的处理对象的存储区域,并进行散列值的计算。重写检测装置5判定从ECU2接收到的散列值是否正确,判定是否进行了针对程序或数据的非法重写。即,重写检测装置5能够在散列值正确时判断为未进行非法重写,在散列值不正确时判断为进行了非法重写。

[0098] 由此,重写检测装置5检测针对ECU2的程序或数据的非法重写,能够适当地进行对进行了非法重写的ECU2的动作停止、修理或更换等处理。关于第二次以后的处理,ECU2自行确定作为散列值计算的处理对象的存储区域,从而重写检测装置5不需要将指定存储区域的信息向ECU2发送,能够减少重写检测装置5和ECU2之间的通信量。另外,ECU2通过随机种子的接收,不用等待指定存储区域的信息的接收就能够开始散列值计算的处理,因此能够

缩短处理时间。

[0099] 另外,ECU2的散列值计算部24将相对于作为上一次散列值计算的对象的存储区域隔开了预定地址值 α 的存储区域设为作为本次处理对象的存储区域。重写检测装置5也存储相同的预定地址值 α ,特定ECU2将哪个存储区域作为对象计算了散列值。由此,ECU2能够容易且切实地确定应作为散列值计算的处理对象的存储区域。

[0100] 另外,重写检测装置5的重写检测例如是在车辆1的车检时等定期地重复进行。在首次进行ECU2的重写检测时,重写检测装置5将指定应作为散列值计算的处理对象的第一次的存储区域的信息向ECU2发送。ECU2在从重写检测装置5接收到指定存储区域的信息时,将被指定的存储区域作为处理对象来进行散列值的计算,在除此以外的情况下进行基于预定地址值 α 的散列值的计算。由此,在首次计算散列值时,ECU2能够切实地确定作为处理对象的存储区域,能够切实地进行散列值的计算。

[0101] 另外,服务器装置7根据来自重写检测装置5的询问而发送期望值,根据重写检测装置5从服务器装置7接收到的期望值与从ECU2接收到的散列值是否一致来进行重写的检测。例如,在构成为重写检测装置5存储有散列值的期望值时,存在重写检测装置5的期望值被非法重写的可能性,但是通过构成为从服务器装置7获取期望值而能够防止这种期望值的非法重写。

[0102] 另外,重写检测装置5是能够经由通信线缆6相对于车辆1的车内网络3的连接器4装卸的结构。将这种重写检测装置5例如设置在车辆1的经销商或维修车间等,能够在车辆1的车检、定期检查或修理等时进行ECU2的程序或数据的非法重写检测。另外,例如在租车或拼车等的车辆1的情况下,能够在车辆返还后通过重写检测装置5进行非法重写检测。

[0103] 另外,在本实施方式中,虽然构成为由重写检测装置5将与作为第一次散列值计算的处理对象的存储区域有关的信息发送到ECU2,但是并不限于此。例如ECU2也可以构成为,第一次散列值计算处理将存储部22的预定区域(最前头区域等)作为处理对象,重写检测装置5不指定存储区域。另外,虽然构成为重写检测装置5存储用于确定存储区域的预定地址值 α 和进行了散列值计算处理的次数并根据这些信息来特定作为本次处理对象的存储区域,但是并不限于此。例如也可以构成为,将与作为处理对象的存储区域有关的信息与ECU2计算出的散列值一起发送到重写检测装置5。

[0104] 另外,虽然构成为通过经由通信线缆6的有线通信来进行重写检测装置5与车辆1之间的通信,但是并不限于此,也可以构成为进行无线LAN等的无线通信。另外,虽然重写检测装置5构成为通过无线通信部56进行与服务器装置7的通信,但是并不限于此,也可以构成为通过有线通信进行与服务器装置7的通信。另外,虽然构成为将重写检测装置5连接到车辆1的车内网络3的连接器4,但是并不限于此,也可以构成为例如在搭载于车辆1中的网关等装置连接重写检测装置5,重写检测装置5通过网关进行与连接到车内网络3的ECU2的通信。

[0105] 另外,虽然重写检测装置5构成为在从ECU2获取了散列值之后从服务器装置7获取期望值,但是并不限于此,也可以在获取期望值之后获取散列值,也可以并行地获取散列值和期望值。另外,虽然重写检测装置5构成为针对搭载在车辆1上的多个ECU2逐个地按顺序进行非法重写的检测,但是并不限于此。重写检测装置5也可以例如将随机种子通过广播一起发送到多个ECU2,并从多个ECU2获取散列值,同时进行针对多个ECU2的重写检测处

理。

[0106] 另外,也可以构成为,服务器装置7不具备重写检测数据库75而重写检测装置5具备重写检测数据库75。即,也可以构成为,重写检测系统不具备服务器装置7,由重写检测装置5存储或计算针对散列值的期望值。另外,在本实施方式中,虽然以进行针对搭载于车辆1中的ECU2的程序或数据的重写检测的重写检测系统为例进行了说明,但是并不限于此,例如也可以构成为,进行针对搭载于飞机或船舶等其他移动体中的信息处理装置的程序或数据的重写检测。

[0107] 另外,图9所示的存储区域为一例,并不限于此。在图示的例子中,虽然像“从X地址到Y地址以Z地址间隔”那样将不连续的多个区域指定为第一次的存储区域,但是也可以例如像“从X地址到Y地址”那样采用指定一个连续区域的方法。另外,也可以例如像“从X1地址到Y1地址、从X2地址到Y2地址、…、从Xn地址到Yn地址”那样采用指定多个最前头位置和末尾位置来指定不连续的多个区域的方法。无论在任何情况下,ECU2都能够将对第一次的存储区域加上预定地址值 α 而得到的存储区域确定为第二次的存储区域。

[0108] 另外,重写检测装置5也可以进行一次与这种ECU2的存储部22的一部分对应的散列值的获取,并根据一个散列值进行重写检测。但是,重写检测装置5也可以通过多次进行向ECU2的随机种子的发送来获取将存储部22的多个存储区域作为对象的多个散列值,并根据多个散列值进行重写检测。通过以这种方式进行多次散列值的获取,重写检测装置5能够更高精度地进行重写检测。即使在这种情况下,重写检测装置5也无需在第一次以外的散列值获取时发送指定存储区域的信息。

[0109] 另外,虽然构成为由重写检测装置5生成随机种子,但是并不限于此。例如也可以构成为由服务器装置7生成随机种子。在该结构的情况下,重写检测装置5对服务器装置7委托随机种子和期望值的发送。根据该委托,服务器装置7制作随机种子,根据重写检测数据库75获取或计算对应的期望值,将随机种子和期望值向重写检测装置5发送。重写检测装置5将从服务器装置7接收到的随机种子向ECU2发送,并从ECU2接收根据该随机种子计算出的散列值,将来自服务器装置7的期望值与来自ECU2的散列值进行比较来检测非法重写。另外,也可以构成为服务器装置7还生成指定第一次的存储区域的信息。

[0110] 另外,虽然构成为将重写检测装置5能够相对于车辆1的车内网络3装卸,但是并不限于此。例如也可以在搭载于车辆1中的网关或汽车导航装置等设备中设置进行重写检测处理的功能。另外,也可以构成为例如搭载于车辆1中的多个ECU2中的一个或多个具有进行重写检测处理的功能。

[0111] (实施方式2)

[0112] 在实施方式2的重写检测系统中,作为ECU2的散列值计算的处理对象的存储区域的确定方法不同。图13是用于说明实施方式2的ECU2的存储区域确定方法的示意图。实施方式2的ECU2将存储部22的存储区域分为前半部分和后半部分,交替地作为散列值计算的处理对象。例如,在首次从重写检测装置5接收到随机种子时,ECU2将存储部22的前半部分作为散列值计算的处理对象。在下次从重写检测装置5接收到随机种子时,ECU2将存储部22的后半部分作为散列值计算的处理对象。这样一来,ECU2在每次从重写检测装置5接收随机种子时都将散列值计算的处理对象在存储部22的前半部分和后半部分之间切换。

[0113] 另外,在实施方式2的重写检测系统中,也可以构成为重写检测装置5选择前半部

分或后半部分中的任一个来指定应作为第一次散列值计算的处理对象的存储区域,还可以是第一次预先确定为前半部分等,重写检测装置5不进行指定。无论是哪一种结构,重写检测装置5都需要存储散列值的计算为第几次的信息。另外,服务器装置7在存储部72中存储的重写检测数据库75优选为图7所示的结构。

[0114] 以上结构的实施方式2的重写检测系统构成为ECU2将存储部22的存储区域分成两部分并交替地作为散列值计算的处理对象,从而能够容易且切实地进行存储区域的确定。另外,在本实施方式中,虽然构成为将存储部22的存储区域分成两部分,但是并不限定于此,也可以构成为将存储部22分为三部分以上,按顺序将分割而得到的存储区域作为处理对象。

[0115] 另外,实施方式2的重写检测系统的其他结构与实施方式1的重写检测系统的结构相同,因此对于相同的部位标上相同标号并省略详细的说明。

[0116] (实施方式3)

[0117] 上述的实施方式1、2的重写检测系统具有如下结构:由重写检测装置5指定第一次的存储区域,由ECU2确定第二次以后的存储区域。与此相对地,实施方式3的重写检测系统是由重写检测装置5指定作为每次散列值计算的处理对象的存储区域的结构。图14是用于说明实施方式3的重写检测系统的存储区域确定方法的示意图。另外,实施方式3的重写检测系统的第一次的存储区域的确定方法与实施方式1的重写检测系统相同。即,实施方式3的重写检测装置5在首次进行针对ECU2的重写检测的处理时将指定作为处理对象的存储区域的信息与随机种子一起向ECU2发送。ECU2将由与随机种子一起接收到的信息指定的存储区域作为对象来计算散列值,将计算出的散列值向重写检测装置5发送。

[0118] 从ECU2接收到散列值的重写检测装置5进行针对服务器装置7的询问来获取期望值,并判定ECU2的散列值与服务器装置7的期望值是否一致,从而进行ECU2的重写检测。实施方式3的重写检测装置5在接收到来自ECU2的散列值之后,例如与期望值的获取并行或前后地确定应作为ECU2下一次散列值计算的处理对象的存储区域,并将指定下一次的存储区域的信息向ECU2发送。从重写检测装置5接收到下一次的存储区域指定信息的ECU2对接收到的信息进行存储。另外,ECU2可以将下一次的存储区域指定信息存储到图2中未图示的存储器等中。另外,ECU2也可以构成为将下一次的存储区域指定信息存储到存储部22,但是此时需要将存储下一次的存储区域指定信息的存储区域排除在重写检测处理的对象之外。

[0119] 在第二次以后的重写检测处理中,实施方式3的重写检测装置5生成随机种子并向ECU2发送,此时不发送指定存储区域的信息。接收到来自重写检测装置5的随机种子的ECU2读取在上一次处理中存储的存储区域指定信息,将由所读取的信息指定的存储区域作为散列值计算的处理对象。ECU2将计算出的散列值发送到重写检测装置5,之后接收并存储从重写检测装置5发送的下一次的存储区域指定信息。另外,重写检测装置5也存储向ECU2发送的下一次的存储区域指定信息,在下次检测处理中在向服务器装置7的询问中使用。

[0120] 图15是示出实施方式3的重写检测装置5所进行的重写检测处理的步骤的流程图。另外,在本流程图中,省略关于第一次检测处理的步骤。实施方式3的重写检测装置5的处理部51生成随机种子(步骤S51),将所生成的随机种子向作为对象的ECU2发送(步骤S52)。另外,处理部51读取在上一次重写检测处理中存储的存储区域指定信息(步骤S53),根据读取出的信息来特定作为本次散列值计算的处理对象的ECU2的存储部22的存储区域(步骤

S54)。

[0121] 处理部51判定有线通信部55是否接收到从作为处理对象的ECU2发送的散列值(步骤S55),在未接收时(S55:否),待机直到接收到散列值为止。在接收到散列值时(S55:是),处理部51向服务器装置7询问针对接收到的散列值的期望值(步骤S56)。处理部51判定是否接受到针对询问从服务器装置7发送的期望值(步骤S57),在未接收到期望值时(S57:否),待机直到接收到期望值为止。

[0122] 在从服务器装置7接收到期望值时(S57:是),处理部51判定在步骤S55中接收到的散列值与在步骤S57中接收到的期望值是否一致(步骤S58)。在散列值和期望值一致时(S58:是),处理部51判定为未进行非法重写(步骤S59),并使处理推进到步骤S61。在散列值和期望值不一致时(S58:否),处理部51判定为进行了非法重写(步骤S60),并使处理推进到步骤S61。

[0123] 接着,处理部51生成指定在下一次重写检测处理中应作为散列值计算的处理对象的ECU2的存储部22的存储区域的信息,将所生成的下一次的存储区域指定信息向ECU2发送(步骤S61)。另外,处理部51将所生成的下一次的存储区域指定信息存储到存储部52(步骤S62),并结束写入检测处理。

[0124] 图16是示出实施方式3的ECU2所进行的重写检测处理的步骤的流程图。实施方式3的ECU2的处理部21判定通信部23是否接收到重写检测装置5发送的随机种子(步骤S71),在未接收到随机种子时(S71:否),待机直到接收到随机种子为止。在接收到随机种子时(S71:是),处理部21的散列值计算部24根据是否存储有在上一次重写检测处理中从重写检测装置5接收到的下一次的存储区域指定信息,判定散列值计算处理是否为第一次(步骤S72)。在是第一次的处理时(S72:是),散列值计算部24获取与随机种子一起从重写检测装置5发送的存储区域的指定信息(步骤S73),使处理推进到步骤S75。在不是第一次的处理时(S72:否),散列值计算部24读取所存储的存储区域指定信息(步骤S74),使处理推进到步骤S75。

[0125] 处理部21的散列值计算部24根据从重写检测装置5接收到的随机种子以及由在步骤S73中获取的信息或在步骤S74中读取的信息指定的存储区域的存储内容,利用预定的散列函数来进行散列值的计算(步骤S75)。处理部21将散列值计算部24计算出的散列值通过通信部23向重写检测装置5发送(步骤S76)。

[0126] 接着,处理部21判定是否接收到从接收了散列值的重写检测装置5发送的下一次的存储区域指定信息(步骤S77)。在未接收到下一次的存储区域指定信息时(S77:否),处理部21待机直到接收该信息为止。在接收到下一次的存储区域指定信息时(S77:是),处理部21存储所接收到的下一次的存储区域指定信息(步骤S78),并结束处理。

[0127] 以上结构的实施方式3的重写检测系统在重写检测装置5从ECU2接收到散列值之后,将指定应作为下一次散列值计算的处理对象的存储区域的信息向ECU2发送。ECU2接收并存储来自重写检测装置5的存储区域指定信息,将由在进行下一次散列值计算时存储的存储区域指定信息指定的存储区域作为处理对象来进行计算。在该结构中,虽然需要每次都从重写检测装置5向ECU2发送指定存储区域的信息,但是下一次的存储区域指定信息的发送能够在从来自ECU2的散列值的接收后到进行下一次检测处理为止的任意的时刻进行。由此,例如能够选择网络负载少的情况等来进行存储区域指定信息的发送。另外,ECU2在从重写检测装置5接收到随机种子时,不用等待指定存储区域的信息的接收就能够根据所存

储的存储区域指定信息来确定作为处理对象的存储区域并计算散列值,因此能够缩短处理时间。

[0128] 另外,在本实施方式中构成为,在图15的流程图中,在进行了与散列值和期望值的一致/不一致相应的重写检测之后,从重写检测装置5向ECU2发送下一次的存储区域指定信息,但是信息发送的时刻并不限定于此。重写检测装置5的下一次的存储区域指定信息的发送可以在从ECU2接收到本次的散列值之后到下一次重写检测处理开始为止的任意时刻进行。

[0129] 另外,实施方式3的重写检测系统的其他结构与实施方式1的重写检测系统的结构相同,因此对于相同的部位标上相同的标号并省略详细的说明。

[0130] 标号说明

[0131] 1 车辆

[0132] 2 ECU(信息处理装置)

[0133] 3 车内网络(网络)

[0134] 4 连接器

[0135] 5 重写检测装置

[0136] 6 通信线缆

[0137] 7 服务器装置

[0138] 9 网络

[0139] 21 处理部(存储区域确定单元、散列值计算单元、存储区域指定信息存储单元)

[0140] 22 存储部

[0141] 23 通信部

[0142] 24 散列值计算部(散列值计算单元)

[0143] 51 处理部(种子信息发送单元、散列值接收单元、散列值判定单元、信息发送单元)

[0144] 52 存储部

[0145] 53 操作部

[0146] 54 显示部

[0147] 55 有线通信部

[0148] 56 无线通信部

[0149] 71 处理部

[0150] 72 存储部

[0151] 73 通信部

[0152] 75 重写检测数据库。

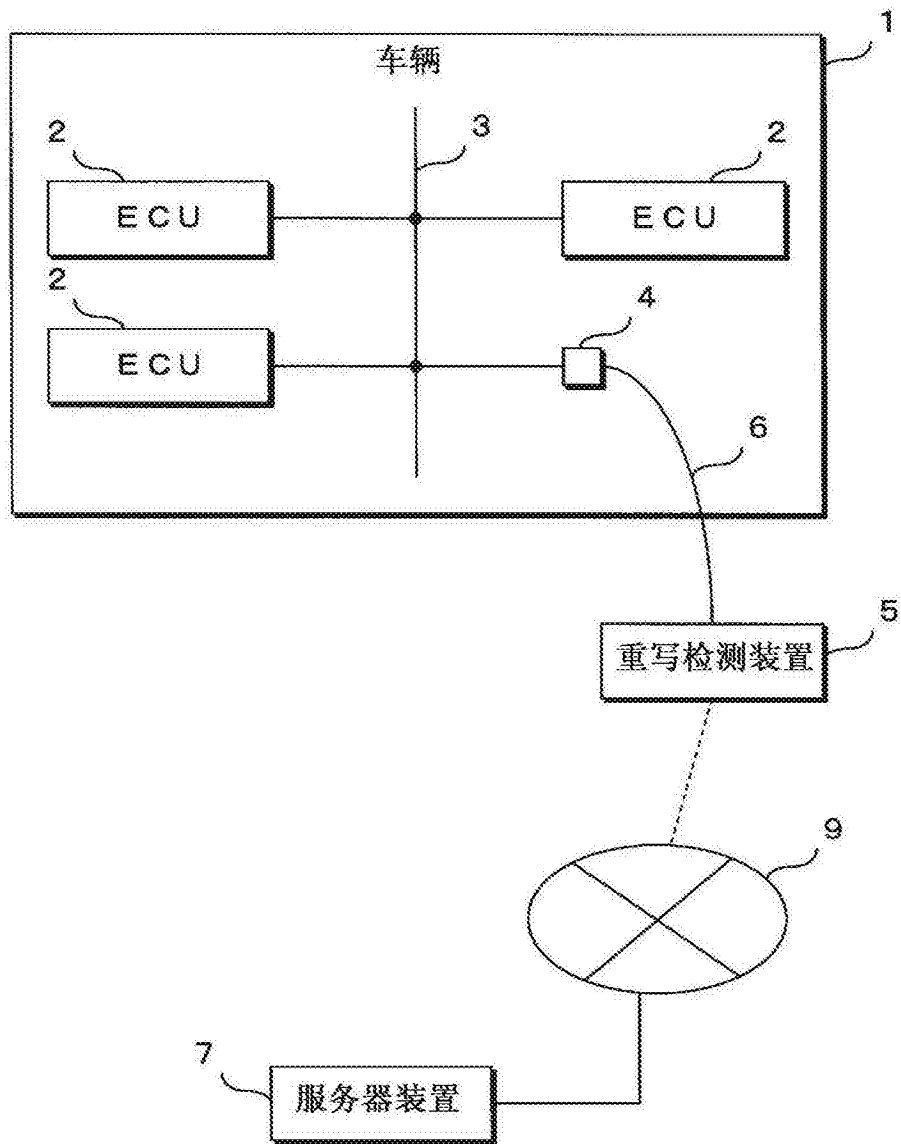


图1

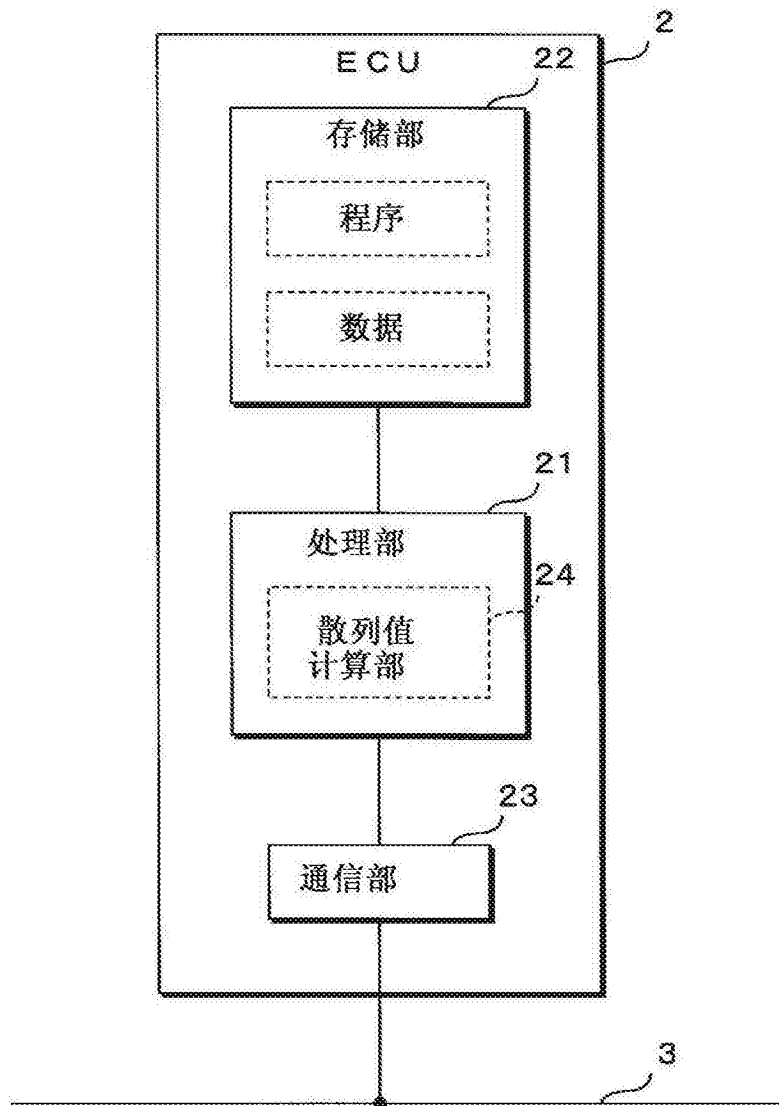


图2



图3

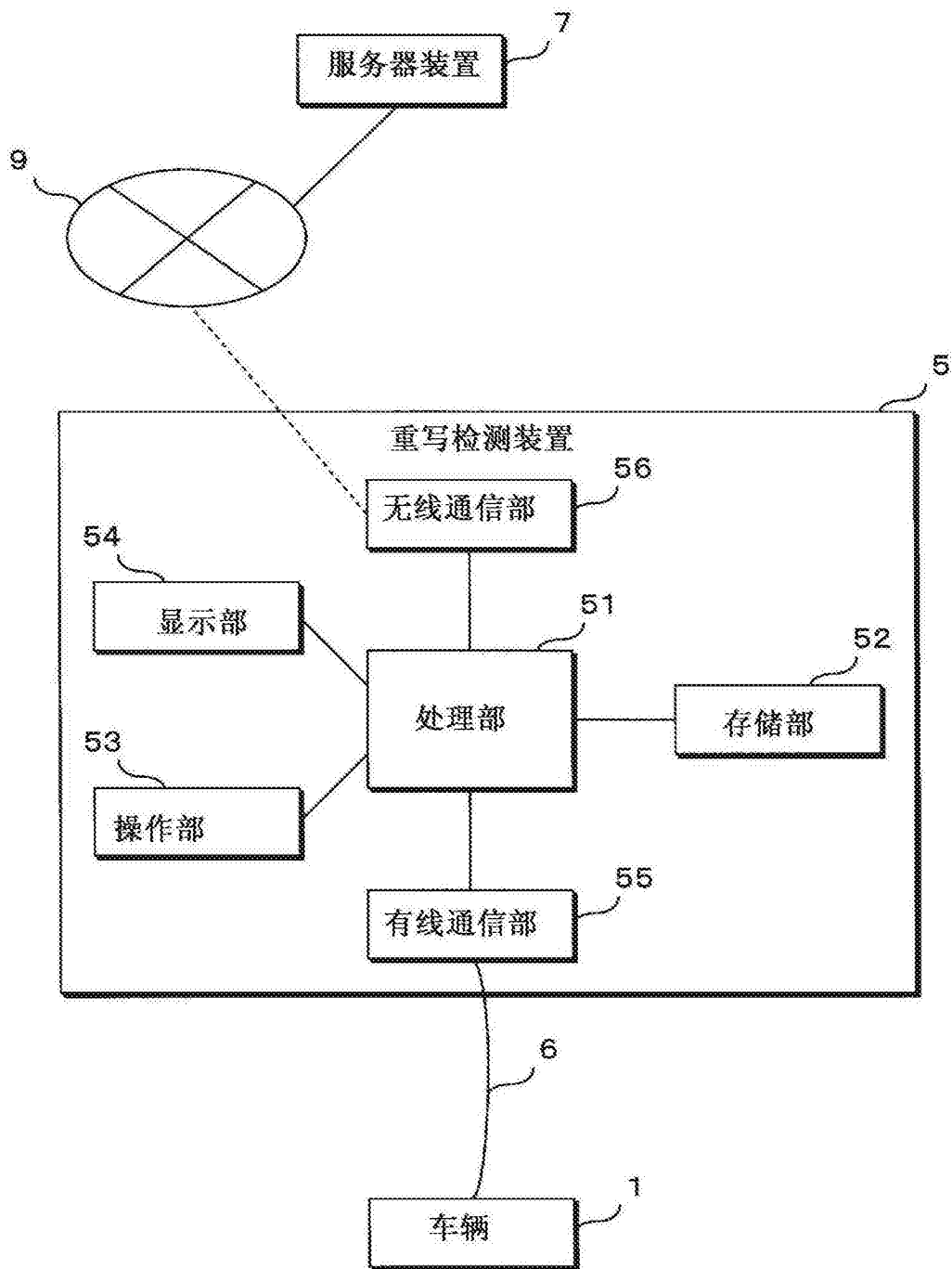


图4

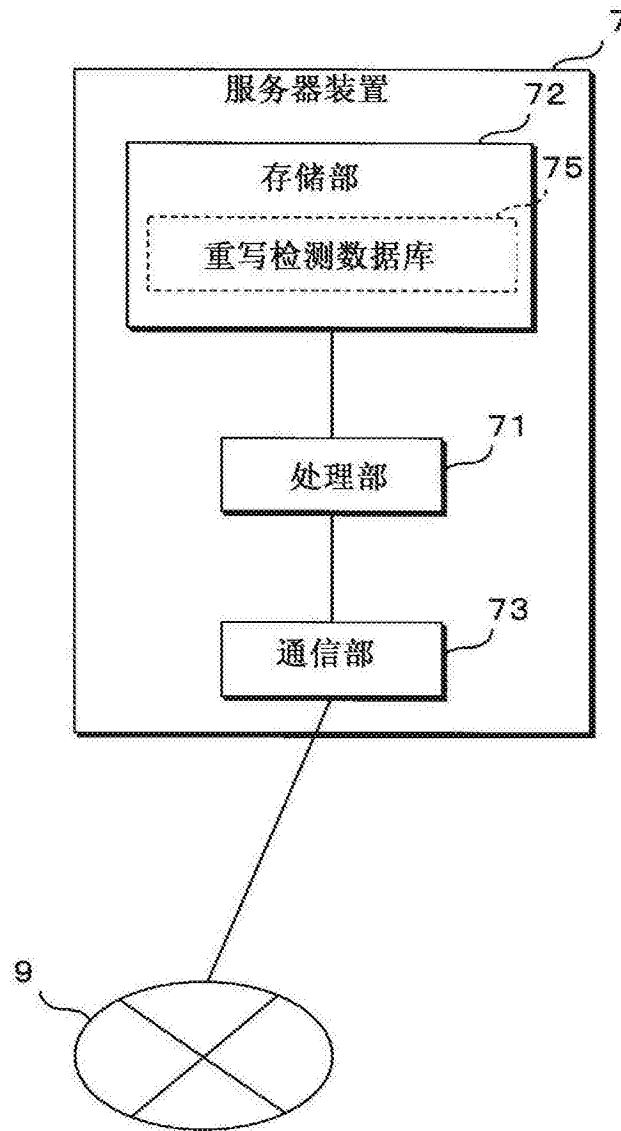


图5

重写检测数据库

车型	ECU类型	存储内容
车型A	ECU a	
	ECU b	
	⋮	⋮
车型B		
⋮	⋮	⋮

图6

重写检测数据库

车型	ECU类型	存储区域	随机种子	期望值
车型A	ECU a	第1区域	0 0 0 0 h	1 3 A 8 h
			⋮	⋮
			F F F F h	7 E 1 1 h
		第2区域	0 0 0 0 h	B 4 4 C h
			⋮	⋮
			F F F F h	9 2 6 6 h
		⋮	⋮	⋮
	ECU b	*****	*****	*****
	⋮	⋮	⋮	⋮
	⋮	⋮	⋮	⋮
车型B	*****	*****	*****	*****
⋮	⋮	⋮	⋮	⋮

图7

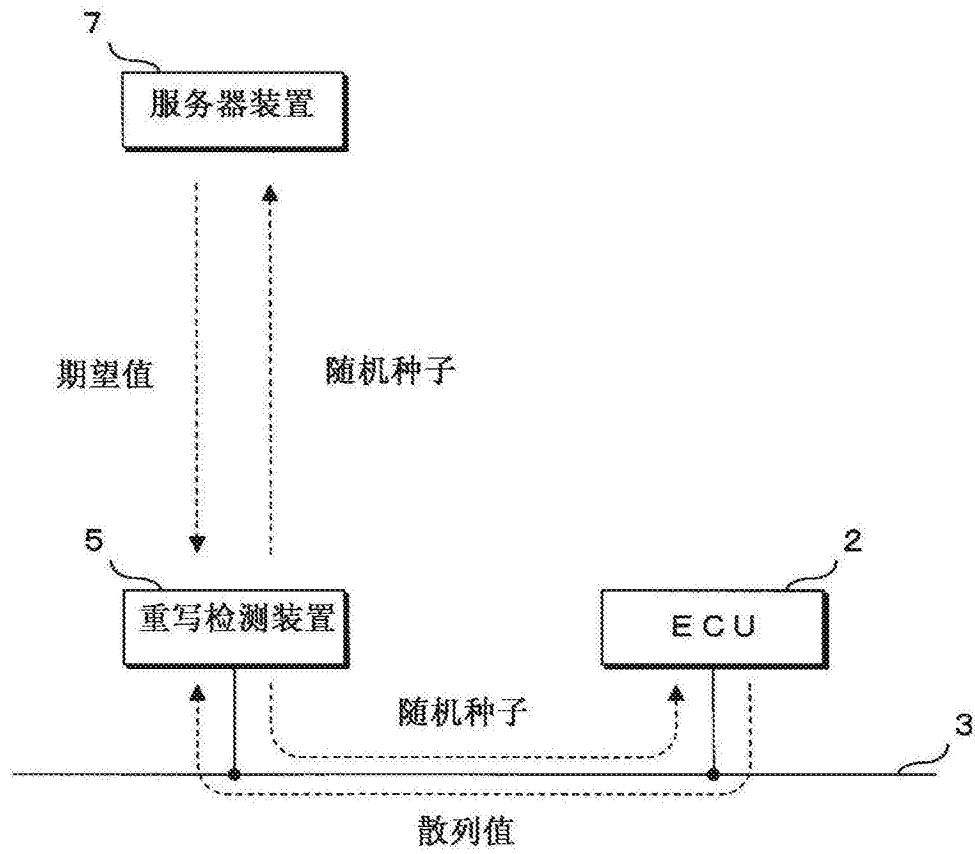


图8

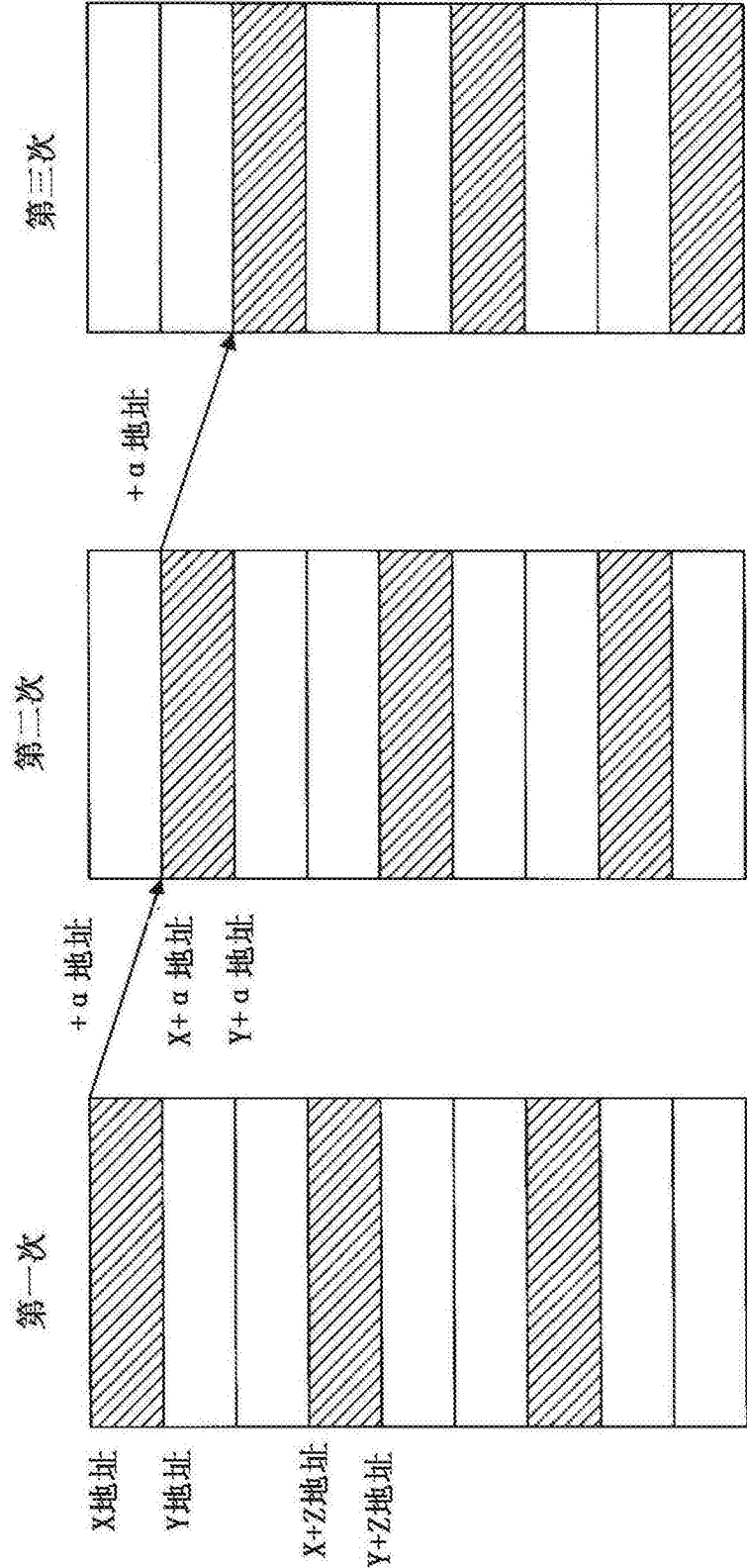


图9

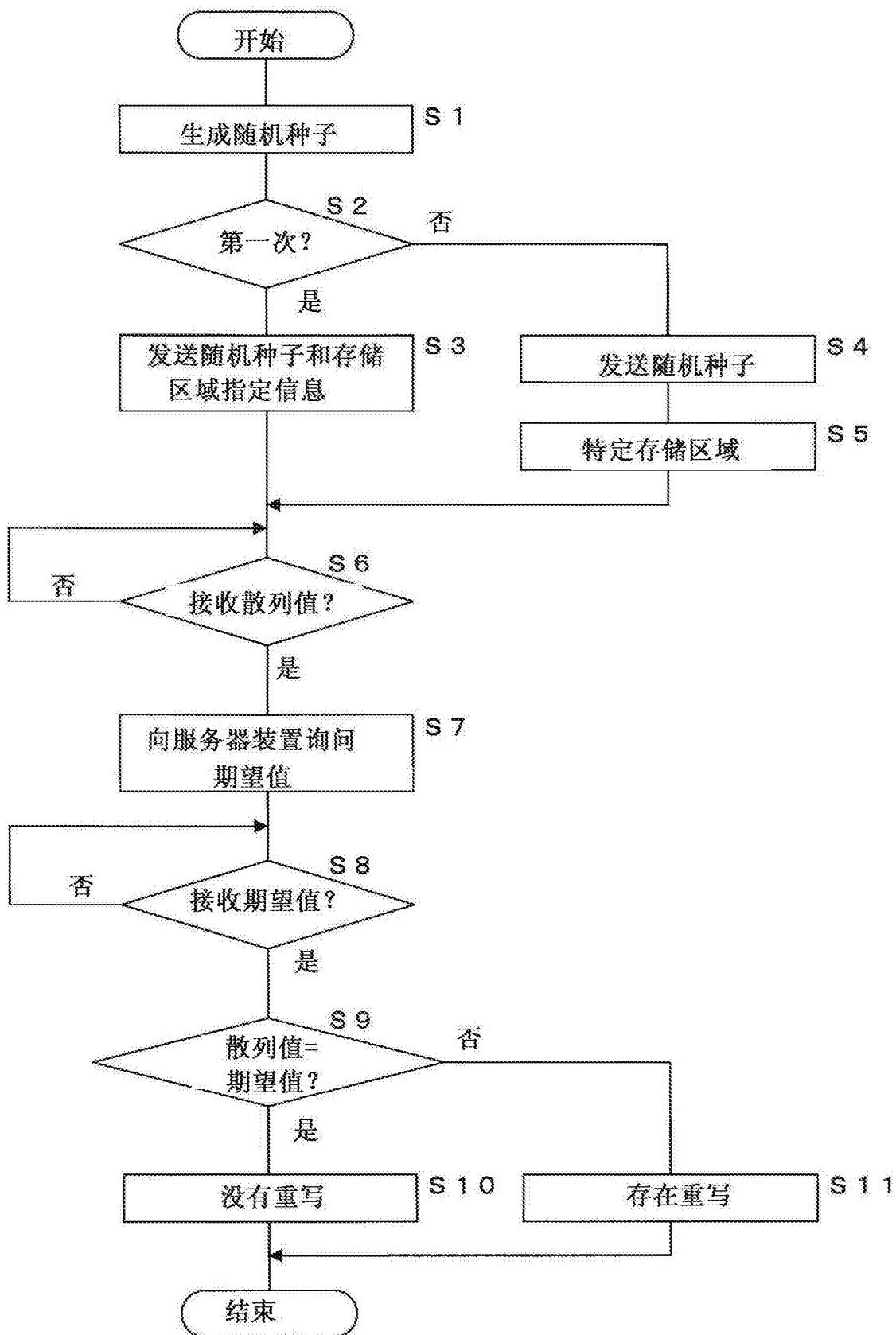


图10

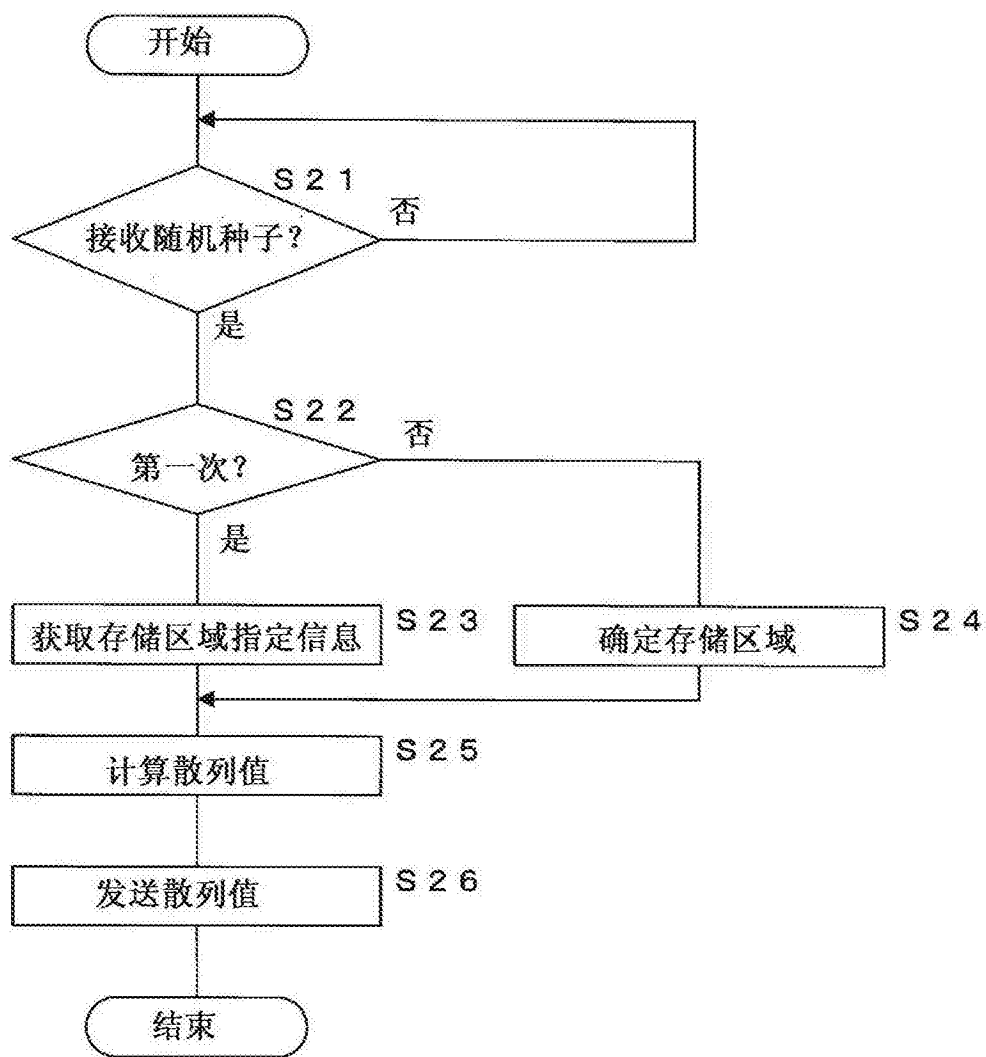


图11

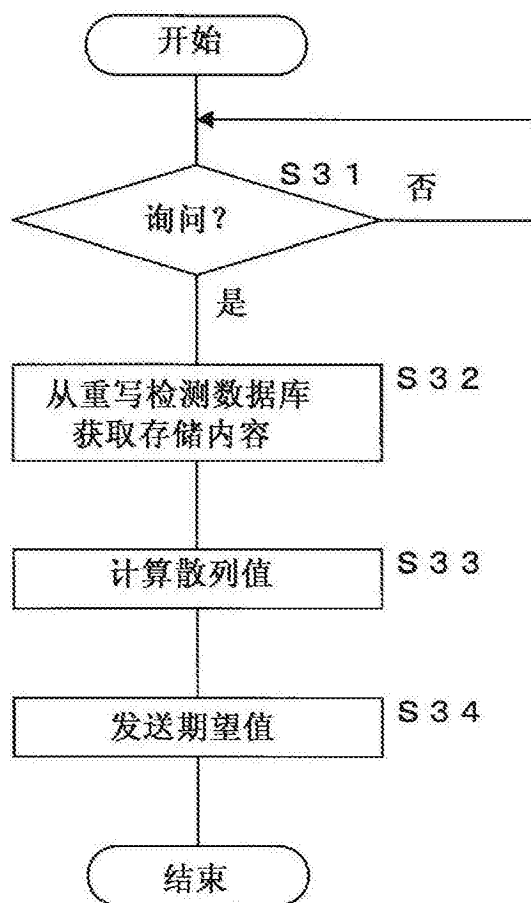


图12

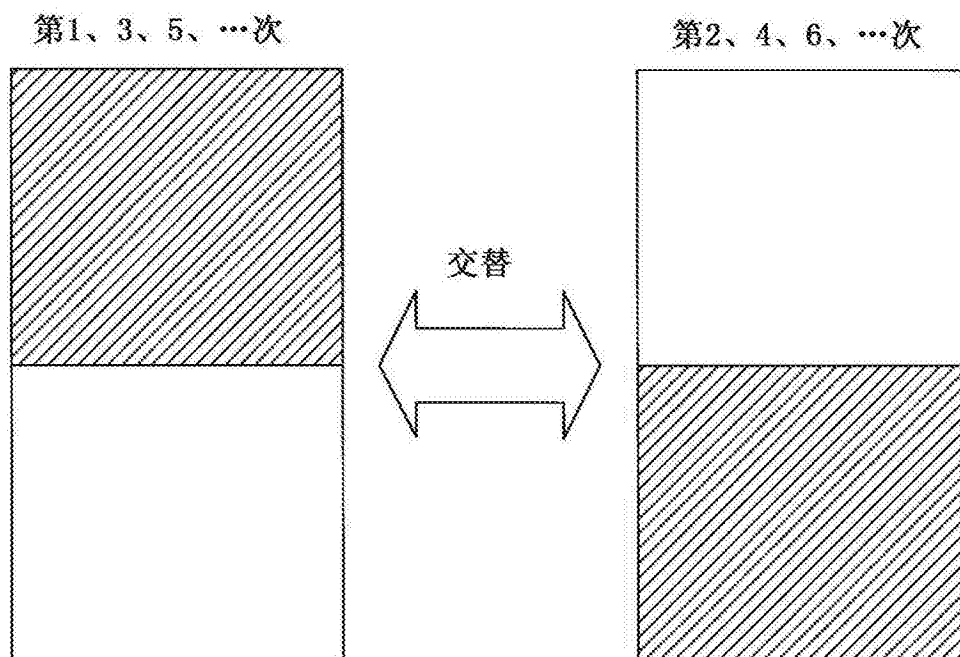


图13

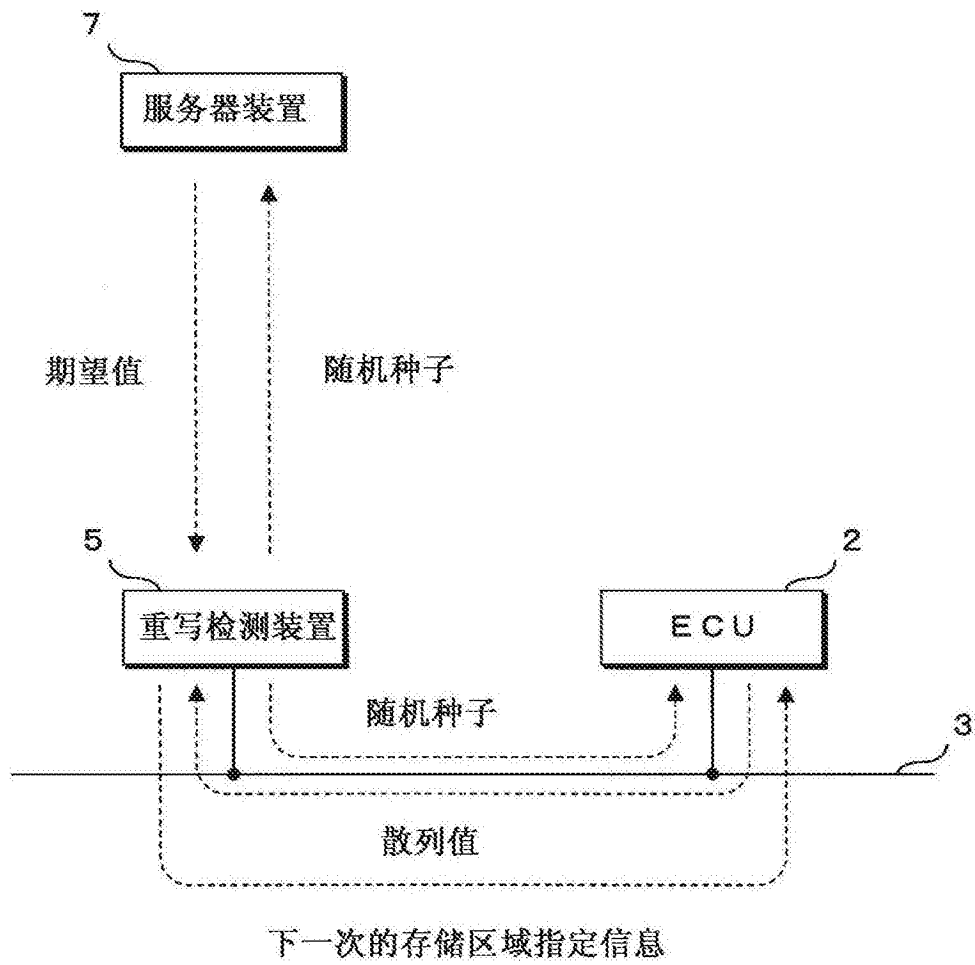


图14

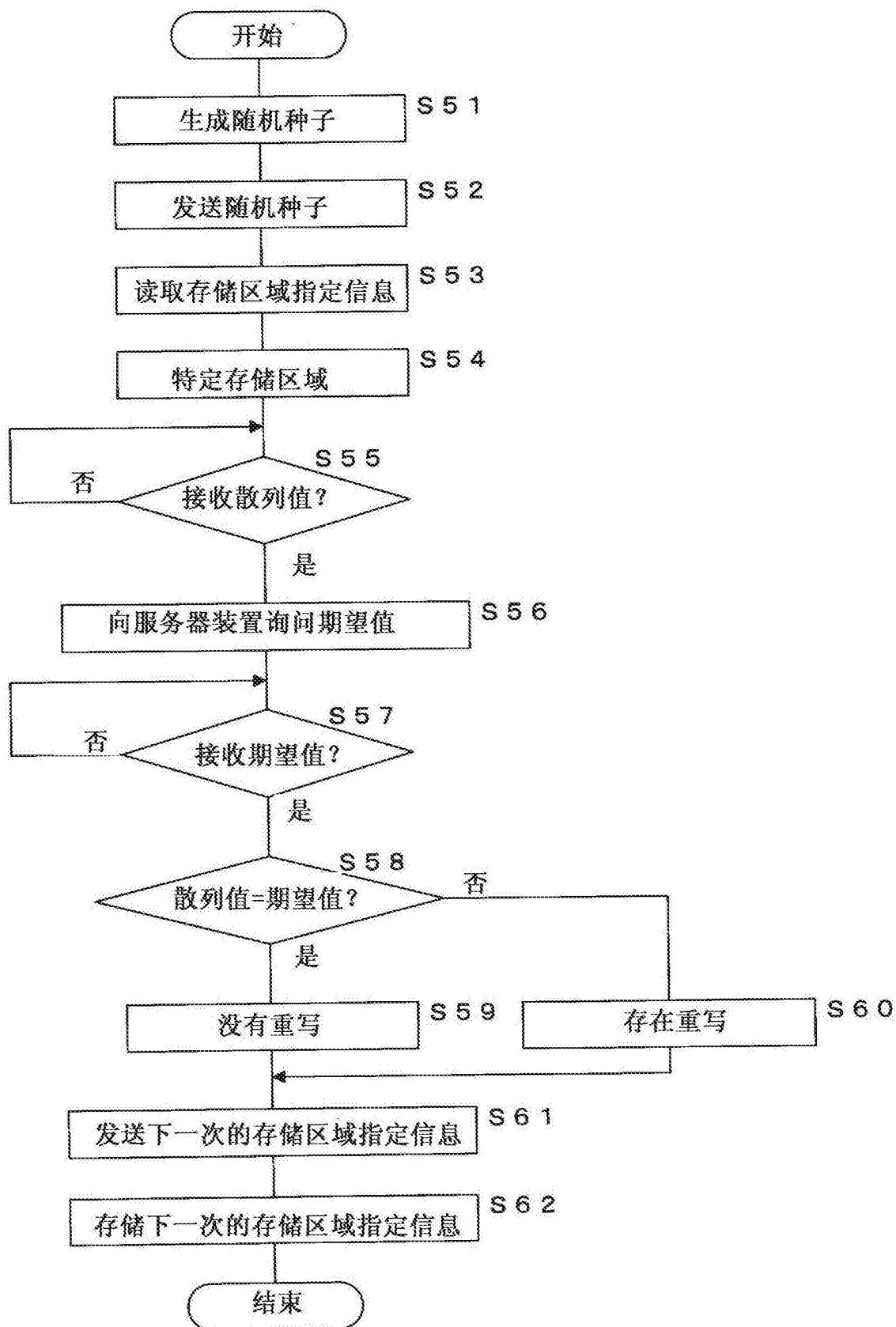


图15

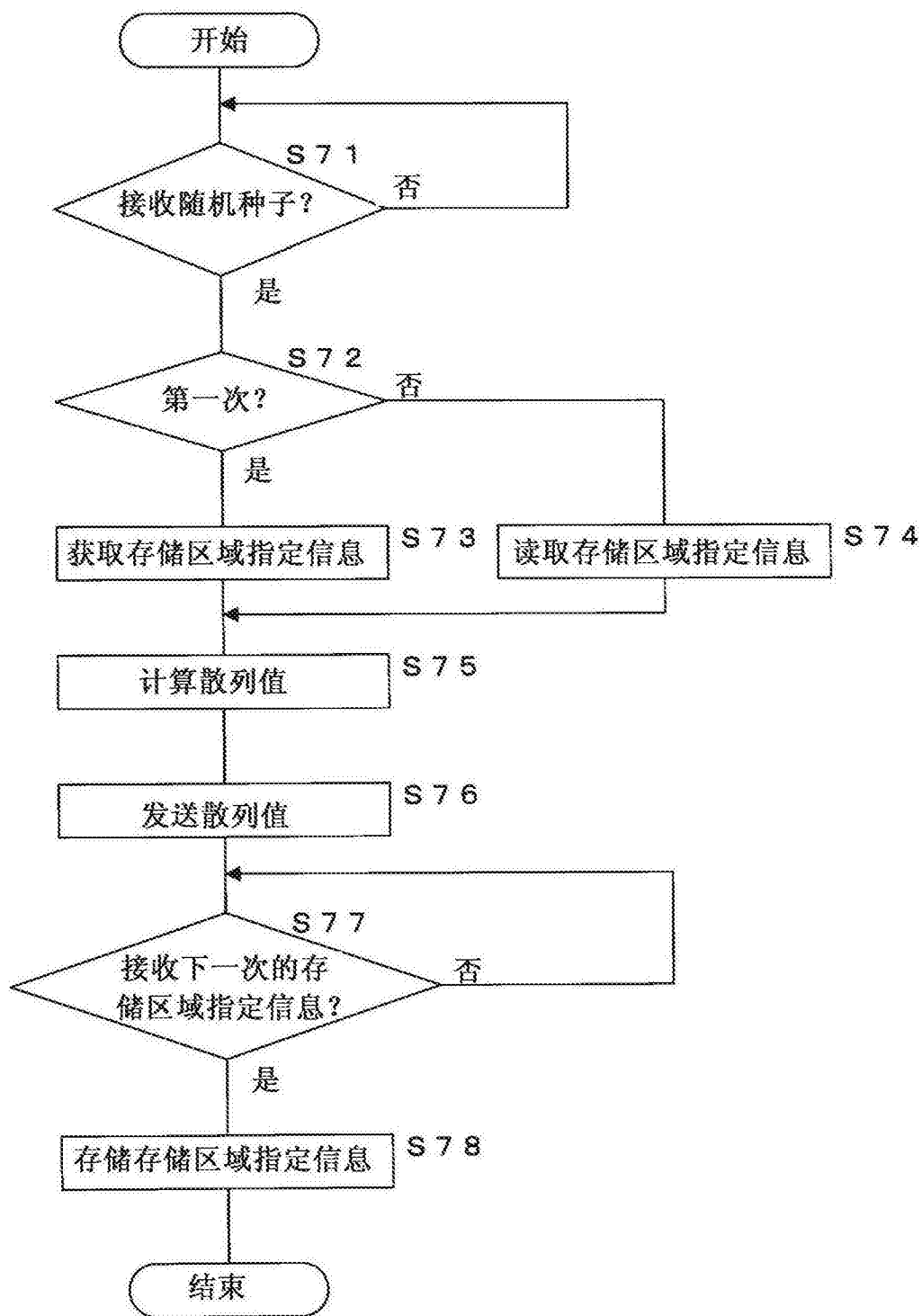


图16