



(12) 发明专利

(10) 授权公告号 CN 113348111 B

(45) 授权公告日 2024. 09. 06

(21) 申请号 202080010092.5	(73) 专利权人 NTT通信公司
(22) 申请日 2020.01.08	地址 日本东京
(65) 同一申请的已公布的文献号 申请公布号 CN 113348111 A	(72) 发明人 上野哲 小田春树 若杉厚司
(43) 申请公布日 2021.09.03	(74) 专利代理机构 北京天昊联合知识产权代理有限公司 11112
(30) 优先权数据 2019-007916 2019.01.21 JP	专利代理师 何立波 张天舒
(85) PCT国际申请进入国家阶段日 2021.07.20	(51) Int.Cl. B60R 16/02 (2006.01) G06F 21/55 (2006.01)
(86) PCT国际申请的申请数据 PCT/JP2020/000285 2020.01.08	(56) 对比文件 JP 2017111796 A, 2017.06.22 JP 2018032254 A, 2018.03.01
(87) PCT国际申请的公布数据 W02020/153122 JA 2020.07.30	审查员 陈巧玲

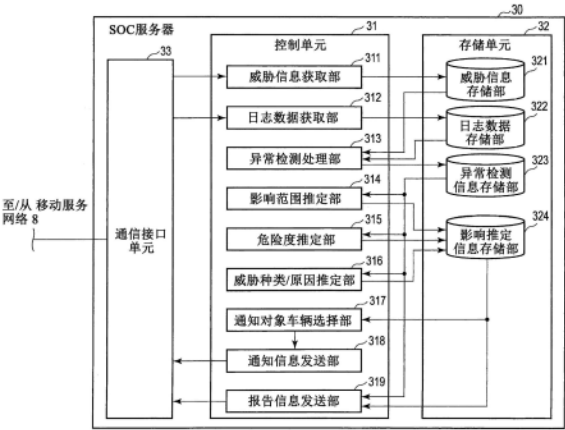
权利要求书2页 说明书10页 附图6页

(54) 发明名称

车辆安全监视装置、方法以及程序记录介质

(57) 摘要

本发明的一个方式是能够与具有发送与车载装置的动作状态相关的日志数据的功能的车载网络之间进行通信的车辆安全监视装置,其中,获取所述日志数据,基于获取到的所述日志数据而检测所述车载网络的异常状态。而且,对检测到的所述异常状态造成的影响的范围进行推定,对表示推定出的所述影响的范围的信息进行管理。



1. 一种车辆安全监视装置,其能够与具有发送与车载装置的动作状态相关的日志数据的功能的车载网络之间进行通信,其中,

所述车辆安全监视装置具有:

日志数据获取部,其获取所述日志数据;

异常状态检测部,其基于所述获取到的日志数据而检测所述车载网络的异常状态;

第1推定部,其对所述检测到的异常状态造成的影响的范围进行推定;

第2推定部,其对所述检测到的异常状态造成的危险的程度进行推定;

第3推定部,其对所述检测到的异常状态的威胁种类以及产生要因中的至少一者进行推定;

推定信息管理部,其对表示所述推定出的影响的范围的信息、表示所述推定出的危险的程度的信息、表示所述推定出的威胁种类以及产生要因中的至少一者的信息进行管理,对所述威胁种类和所述危险的程度的尺度的组合进行了定义的信息进行存储;以及

发送控制部,

所述发送控制部具有:

基于由所述异常状态检测部检测到的异常状态、以及由所述推定信息管理部管理的表示所述影响的范围、所述危险的程度、所述威胁种类以及产生要因中的至少一者的各信息,生成包含针对所述异常状态的应对内容在内的应对指示信息的处理部;

参照由所述推定信息管理部存储的对所述威胁种类和所述危险的程度的尺度的组合进行了定义的信息,而决定所述应对指示信息的通知对象的处理部;以及

将所述生成的应对指示信息发送至所述决定的通知对象的处理部。

2. 根据权利要求1所述的车辆安全监视装置,其中,

作为与所述影响的范围相关的对策的通知对象,所述发送控制部选择搭载有所述车载网络或能够进行所述车载网络和外部网络的各种数据的收发的系统的车辆的制造者或销售商、车型、年份、使用地域符合条件的车辆或其车载网络,对该选择的车辆或其车载网络发送所述生成的应对指示信息。

3. 一种车辆安全监视方法,其由能够与具有发送与车载装置的动作状态相关的日志数据的功能的车载网络之间进行通信的车辆安全监视装置执行,其中,

所述车辆安全监视方法具有:

获取所述日志数据的过程;

基于所述获取到的日志数据而检测所述车载网络的异常状态的检测过程;

对所述检测到的异常状态造成的影响的范围进行推定的过程;

对所述检测到的异常状态造成的危险的程度进行推定的过程;

对所述检测到的异常状态的威胁种类以及产生要因中的至少一者进行推定的过程;

对表示所述推定出的影响的范围的信息、表示所述推定出的危险的程度的信息、表示所述推定出的威胁种类以及产生要因中的至少一者的信息进行管理的管理过程、对所述威胁种类和所述危险的程度的尺度的组合进行了定义的信息进行存储的存储过程;以及

发送控制过程,

所述发送控制过程具有:

基于由所述检测过程检测到的异常状态、以及由所述管理过程管理的表示所述影响的

范围、所述危险的程度、所述威胁种类以及产生要因中的至少一者的各信息,生成包含针对所述异常状态的应对内容在内的应对指示信息的过程;

参照所述存储的对所述威胁种类和所述危险的程度的尺度的组合进行了定义的信息,而决定针对所述异常状态的应对指示信息的通知对象的过程;以及

将所述生成的应对指示信息发送至所述决定的通知对象的过程。

4. 一种程序记录介质,其记录有程序,其中,

所述程序使计算机执行由权利要求1或2所述的车辆安全监视装置的各部进行的处理。

车辆安全监视装置、方法以及程序记录介质

技术领域

[0001] 本发明的一个方式涉及用于监视例如在车辆内构建的车载网络的安全状态的车辆安全监视装置、方法以及程序。

背景技术

[0002] 近年来的汽车等车辆搭载有以构成导航系统的车载控制装置为代表的对发动机、制动器等各种车载仪器进行电子控制的车载控制装置、对显示车辆的各种状态的仪表等仪器进行控制的车载控制装置等多种车载控制装置。而且,在车辆内,利用通信线将上述各车载控制装置电连接而形成车载网络,经由该车载网络而在各车载控制装置之间进行各种数据的收发。

[0003] 关于车载网络,与该网络连接的各车载控制装置负责搭载于车辆的发动机、制动器等各种车载仪器的控制,因此要求极高的安全。然而,通常这种车载网络与外部的网络隔离。因此,例如以控制·区域·网络(CAN)等为代表的车载网络,以通过该车载网络收发的数据是从标准的车载控制装置发送的标准数据为前提而设计的。

[0004] 另一方面,最近推进了能够进行这种车载网络和外部网络的各种数据的收发、与连接于在车辆设置的数据·链接·连接器(DLC)的外部仪器的各种数据的收发的系统的开发。搭载有这种系统的车辆通常称为联网汽车,例如用于实现导航系统的地图数据的更新、自动驾驶等高级的服务。

[0005] 然而,在联网汽车中,车载网络能够与外部网络连接,因此指出了从外部网络利用恶意软件、病毒等的网络攻击的威胁。如果受到网络攻击,则有可能车辆例如执行非法的控制命令而进行误动作、或者车载控制装置的软件或控制数据被篡改。

[0006] 因此,研究了各种检测车载控制装置的软件或控制数据等车内系统的篡改、由此引发的故障的技术(例如参照专利文献1)。

[0007] 专利文献1:日本特开2018-081349号公报

发明内容

[0008] 但是,当前研究的技术通常针对每台车辆而检测由网络攻击引起的系统篡改、故障,仅对检测到该系统篡改、故障的车辆通知障碍的产生等。

[0009] 本发明就是着眼于上述情形而提出的,其一个方面要提供能够基于从车载网络发送的日志数据而执行更有效的安全对策。

[0010] 为了解决上述问题,本发明所涉及的车辆安全监视装置的一个方式能够与具有发送与车载装置的动作状态相关的日志数据的功能的车载网络之间进行通信,具有:日志数据获取部,其获取所述日志数据;异常状态检测部,其基于所述获取到的日志数据而检测所述车载网络的异常状态;第1推定部,其对所述检测到的异常状态造成的影响的范围进行推定;以及推定信息管理部,其对表示所述推定出的影响的范围的信息进行管理。

[0011] 发明的效果

[0012] 根据本发明的第1方式,基于从车辆的车载网络发送的日志数据而检测异常状态,对该异常状态造成的影响的范围进行推定。因此,不仅是检测到异常状态的车辆,还能够将对策的对象扩大至该异常状态造成影响的范围。其结果,例如在因网络攻击而篡改了车辆的车载网络的程序的情况下,对于与该车辆或车载网络关联的其他车辆或车载网络也能够统一采取应对措施。

[0013] 即,根据本发明的各方式,能够提供如下技术,即,能够基于从车载网络发送的日志数据而执行更有效的安全对策。

附图说明

[0014] 图1是表示包含本发明的一个实施方式所涉及的车辆安全监视装置在内的车辆信息通信系统的整体结构的框图。

[0015] 图2是表示作为本发明的一个实施方式所涉及的车辆安全监视装置而执行动作的SOC服务器的硬件结构的框图。

[0016] 图3是表示作为本发明的一个实施方式所涉及的车辆安全监视装置而执行动作的SOC服务器的软件结构的框图。

[0017] 图4是表示图2及图3所示的SOC服务器的控制次序和控制内容的流程图。

[0018] 图5是表示作为威胁信息而定义的威胁的种类(事件的攻击种类)和危险度的尺度(事件的危险度)的组合的一个例子的图。

[0019] 图6是表示分析报告的一个例子的图。

具体实施方式

[0020] 下面,参照附图对本发明所涉及的实施方式进行说明。

[0021] [一个实施方式]

[0022] (结构)

[0023] (1) 系统

[0024] 图1是表示具有本发明的一个实施方式所涉及的车辆安全监视装置的系统的整体结构的图。

[0025] 一个实施方式所涉及的车辆安全管理系统例如作为核心而具有移动服务网络8。移动服务服务器20、安全操作中心(Security Operation Center:SOC)服务器30以及PSIRT(Product Security Incident Response Team)服务器40与移动服务网络8连接。

[0026] 另外,移动服务网络8能够与搭载于车辆1的车载网络2之间经由移动通信网络7而通信。并且,移动服务网络8与外部服务器50之间也能够经由互联网9而通信。

[0027] 此外,移动通信网络7与移动服务网络8之间、以及移动服务网络8与互联网9之间分别经由作为网络间连接装置的例如网关81、82而连接。另外,作为移动通信网络7,例如使用蜂窝移动通信网络、无线LAN(Local Area Network)。

[0028] 车载网络2例如称为CAN(Control Area Network),具有多个车载电子控制装置(Electric Control Unit:ECU)。ECU构成为,分别使处理器执行程序而实现规定的控制功能。例如,ECU用作对发动机、变速器、转向角、加速器、制动器等进行控制的装置、对信号灯、车灯、雨刷进行控制的装置、对门锁及车窗的开闭进行控制的装置、对空调进行控制的装置

等。

[0029] 另外,在车辆1设置有监视以速度传感器、温度传感器、振动传感器等涉及车辆的动作状态的各种车辆传感器的测量数据为代表的驾驶员的状态的车内传感器、监视车外的状况的车外传感器等多种传感器。ECU还用作取入从上述传感器输出的传感数据的装置。ECU还用作自动驾驶控制装置、监视驾驶员的状态的装置。

[0030] 另外,通信控制单元(TCU)3及导航装置4与车载网络2连接。TCU 3用于在车载网络2与移动通信网络7之间进行数据的收发。例如,TCU 3用于收发驾驶员的通话数据、从Web网站接收导航数据、或者将表示上述ECU的动作状态的日志数据向SOC服务器30发送。

[0031] 导航装置4具有USB端口以及无线接口。而且,具有如下功能,即,经由USB端口与USB存储器5之间进行数据的写入及读出,并且经由无线接口而进行与智能手机等便携终端6之间的数据的收发、与外部之间的数据的收发。此外,作为无线接口,例如使用Bluetooth(注册商标)或WiFi(注册商标)。

[0032] 此外,车载网络2具有外部接口端口(OBD-2)。测试装置、个人计算机能够与该OBD-2连接。测试装置、个人计算机例如用于进行ECU的测试、或者针对ECU而安装更新程序、控制数据。

[0033] 外部服务器50例如由Auto-ISAC(Automotive Information Sharing and Analysis Center)运用管理。外部服务器50例如具有对与联网汽车相关的网络威胁、与潜在的脆弱性相关的威胁信息进行积蓄的数据库。而且,对SOC服务器30提供积蓄于该数据库的信息。

[0034] PSIRT服务器40例如由车辆制造商或用于通过车载装置的开发生命周期而实施所需的安全管理、支援、事件应对的组织(PSIRT)运用。PSIRT服务器40例如具有对该制造商固有的网络威胁信息进行存储的威胁信息数据库。而且,根据来自SOC服务器30的请求而将威胁信息向SOC服务器30发送。另外,PSIRT服务器40具有如下功能,即,例如,在由PSIRT的管理者输入了按各制造商确定的应对方针等的情况下,向该车辆发送包含该应对方针等在内的召回指示。上述应对方针等基于从SOC服务器30提供的针对安全的分析报告而输入。此外,威胁信息例如由威胁的种类和危险度的尺度的组合而定义。分析报告例如也利用上述威胁的种类和危险度的尺度的组合进行记述。

[0035] (2) SOC服务器

[0036] 图2及图3是分别表示上述SOC服务器30的硬件结构及软件结构的框图。

[0037] SOC服务器30例如作为车辆安全监视装置而执行动作,由云服务器、Web服务器构成。SOC服务器30具有控制单元31、存储单元32以及通信I/F(通信I/F) 33。上述部件经由总线34而彼此连接。

[0038] 通信I/F 33根据移动服务网络8及互联网9中使用的通信协议,在车载网络2、外部服务器50以及PSIRT服务器40之间分别进行各种数据的传送。

[0039] 存储单元32例如具有HDD(Hard Disk Drive)或Solid State Drive(SSD)等能够随时写入及读出的非易失性存储器、ROM(Read Only Memory)以及RAM(Random Access Memory)组合而构成的存储介质,具有程序存储区域以及数据存储区域。此外,存储介质的结构并不局限于上述结构。除了OS(Operating System)等中间件以外,程序存储区域中还储存有本发明的一个实施方式所涉及的为了执行各种控制处理所需的程序。

[0040] 数据存储区域中设置有威胁信息存储部321、日志数据存储部322、异常检测信息存储部323以及影响推定信息存储部324。

[0041] 威胁信息存储部321用于积蓄从外部服务器50及PSIRT服务器40获取的威胁信息。日志数据存储部322用于积蓄从车载网络2发送的日志数据。异常检测信息存储部323用于存储通过控制单元31的异常检测处理而获得的车载网络2的异常检测信息。影响推定信息存储部324用于存储通过控制单元31获得的表示与上述异常的影响相关的多种推定结果的信息。

[0042] 控制单元31例如具有CPU(Central Processing Unit)等硬件处理器。作为用于实现本发明的一个实施方式的控制功能,控制单元31具有威胁信息获取部311、日志数据获取部312、异常检测处理部313、影响范围推定部314、危险度推定部315、威胁种类/原因推定部316、通知对象车辆选择部317、通知信息发送部318以及报告信息发送部319。上述控制功能部均通过使上述硬件处理器执行上述存储单元32的程序存储区域中储存的程序而实现。

[0043] 威胁信息获取部311从外部服务器50及PSIRT服务器40经由移动服务网络8而获取针对车载网络2的威胁信息。而且,进行将获取到的威胁信息存储于威胁信息存储部321的处理。威胁信息中例如包含表示相对于网络攻击的车载网络2的脆弱性的种类以及脆弱程度的信息、表示有可能引发事故的异常动作的种类及其重要度的信息。此外,可以不经由移动服务网络8,而是经由互联网9等其他网络进行威胁信息的获取。

[0044] 日志数据获取部312经由移动通信网络7及移动服务网络8而获取从车载网络2发送的日志数据。而且,进行将获取到的日志数据存储于日志数据存储部322的处理。另外,关于日志数据的获取,也可以不经由移动服务网络8而是经由互联网9等其他网络进行。

[0045] 日志数据中例如包含车载网络2内的ECU的程序、控制数据的变更履历、各ECU对车载仪器及车载装置的动作履历、表示从外部网络接收到各种控制数据或内容数据时的该接收数据的通信路径的信息。另外,向日志数据赋予识别发送源的信息、作为日志数据产生源的ECU、车辆仪器或车载装置的识别编号、预先分配给车辆1的网络地址、表示日志数据的产生日期时间的时间戳以及表示车辆1的当前位置的位置信息,作为报头。位置信息例如可以由车辆导航系统所具有的GPS(Global Positioning System)接收器获取。

[0046] 异常检测处理部313求出由上述日志数据获取部312获取的日志数据与威胁信息存储部321中存储的威胁信息的关联性,由此判定日志数据的内容是否相当于威胁。而且,在判定为相当于威胁的情况下,进行如下处理,即,将表示与该威胁对应的异常的种类以及上述关联的程度的信息和成为上述对象的日志数据一起,作为异常检测信息而存储于异常检测信息存储部323。

[0047] 影响范围推定部314进行如下处理,即,基于上述异常检测信息存储部323中存储的异常检测信息的内容,推定异常状态造成的影响的范围,将表示其推定结果的信息存储于影响推定信息存储部324。作为影响范围的推定对象,例如设想为车辆的制造商、车型、年份、地域、ECU以及车载网络2内的部位。

[0048] 危险度推定部315通过获取存储于上述异常检测信息存储部323的异常检测信息中包含的异常动作的种类与威胁信息的关联性,从而推定异常动作造成的危险的程度(危险度)。而且,进行如下处理,即,将表示其推定结果的信息存储于影响推定信息存储部324。危险度例如表示异常动作对车辆或驾驶员造成的危险的程度,例如可以分为

“Information”、“Medium”、“Serious”、“Critical”这4个等级来判定。

[0049] 威胁种类/原因推定部316基于向检测到上述异常状态的日志数据赋予的信息而推定异常状态(事件)的攻击种类。另外,威胁种类/原因推定部316在受到恶意软件、病毒等的网络攻击的情况下,根据此时接收到的传送数据的通信路径信息而推定发送路径以及发送源。而且,进行如下处理,即,基于上述推定结果而生成表示异常状态的威胁种类或产生要因或这两者的信息,并存储于影响推定信息存储部324。

[0050] 通知对象车辆选择部317基于上述影响推定信息存储部324中存储的表示影响范围、危险度以及威胁种类或产生要因或这两者的推定结果的信息,选择成为异常应对的对象的车辆组。而且,针对所选择的车辆组而进行发送异常应对通知信息的处理。作为成为异常应对的对象的车辆组,例如能举出制造商、车型、形式中的任一者符合条件的车辆、或者在特定地域使用的车辆等。

[0051] 通知信息发送部318进行如下处理,即,以由上述通知对象车辆选择部317选择的车辆组为目的地从通信I/F 33向移动服务网络8发送上述异常应对通知信息。

[0052] 报告信息发送部319制作包含上述影响推定信息存储部324中存储的表示影响范围、危险度以及威胁种类或产生要因各自的推定结果的信息、以及异常检测信息存储部323中存储的异常检测信息在内的车辆安全用的分析报告。而且,进行如下处理,即,从通信I/F 33向PSIRT服务器40发送所制作的分析报告的信息。

[0053] (动作)

[0054] 接下来,与车载网络2的动作例一起对以上述方式构成的SOC服务器30的动作例进行说明。图4是表示其控制次序及控制内容的一个例子的流程图。

[0055] (1) 威胁信息的获取

[0056] 在威胁信息获取部311的控制下,在步骤S20中,SOC服务器30从外部服务器50及PSIRT服务器40定期地或在任意定时,获取对联网汽车相关的网络威胁、潜在的脆弱性进行了定义的信息。具体而言,获取由威胁种类和危险度的尺度定义的信息。而且,将获取到的信息作为威胁信息而存储于威胁信息存储部321。此外,上述威胁信息的获取处理可以从SOC服务器30访问外部服务器50等而获取的方式,也可以是SOC服务器30接收由外部服务器50等定期地或不定期地以推送(push)方式发送的威胁信息的方式。

[0057] (2) 日志数据的获取

[0058] 关于各车辆1的车载网络2,各ECU以及车辆仪器或装置始终或定期地监视自身的动作状态等。而且,基于其监视结果而生成表示动作履历的日志数据。另外,即使在车载网络2接收到从外部网络发送的传送数据的情况下,也生成表示该传送数据的接收履历的日志数据。

[0059] 另外,车载网络2通过步骤S10收集上述生成的日志数据并临时存储于内部存储器。而且,车载网络2在步骤S11中每当经过一定期间而读出上述存储的日志数据。而且,在步骤S12中从TCU 3向SOC服务器30发送所读出的日志数据。此外,对于上述日志数据,可以不以一定时间为单位集中发送,而是每当生成时就实时地发送。

[0060] 与此相对,SOC服务器30在日志数据获取部312的控制下通过步骤S21而监视日志数据的接收。在该状态下,如果利用通信I/F31接收日志数据,则日志数据获取部312通过步骤S22取入上述接收到的日志数据并存储于日志数据存储部322。日志数据获取部312每当

接收到日志数据时反复执行上述处理。

[0061] (3) 异常检测处理

[0062] 每当获取到新日志数据时, SOC服务器30在异常检测处理部313的控制下在步骤S22中从日志数据存储部322读入上述新获取的日志数据。而且, 分别对表示该日志数据中包含的动作内容等的信息、与威胁信息存储部321中存储的多种威胁信息的关联性值进行运算。而且, 将关联性值大于或等于阈值的日志数据作为异常检测信息而存储于异常检测信息存储部323。

[0063] 例如, 作为对基于网络攻击对程序或控制数据的篡改、基于程序的漏洞等而产生的不自然的动作进行定义的威胁信息, 定义了“晴天时的雨刷的连续动作”、“车头灯的连续闪烁”、“发动机的异常的高速旋转动作”之类的检测逻辑。如果从车载网络2发送的日志数据的内容与上述检测逻辑中的任一者一致, 则异常检测处理部313提取上述日志数据作为包含异常状态在内的日志数据, 将其作为异常检测信息而存储于异常检测信息存储部323。

[0064] (4) 异常状态造成的影响范围的推定

[0065] 如果SOC服务器30在步骤S24中判定为检测出包含异常状态在内的日志数据, 则首先在影响范围推定部314的控制下通过步骤S25对上述异常动作造成的影响范围进行推定。

[0066] 例如, 异常状态判定为“晴天时的雨刷的连续动作”、“车头灯的连续闪烁”、“发动机的异常的高速旋转动作”, 在一定期间中从多台车辆通知了该异常状态。在该情况下, 影响范围推定部314从日志数据提取出检测到的上述多台车辆的车辆识别编号或底盘编号, 对例如车辆的制造商名、车型、年份的共通性进行判定。而且, 基于其判定结果而推定上述异常动作的影响范围是特定的“制造商”、或者特定的“车型”、或者特定的“年份”, 将其推定结果与对象日志数据一起存储于影响推定信息存储部324。此外, 除了上述车辆制造商以外, 可以将车辆的销售商、车载网络2的制造商或销售商推定为影响范围。

[0067] 另外, 例如, 在“寒冷地域规格的车载装置”产生了异常状态的情况下, 将影响范围推定为“寒冷地域”。而且, 将其推定结果与对象日志数据一起存储于影响推定信息存储部324。

[0068] 并且, 例如, 将与产生了表示动作异常的日志数据的ECU、车载仪器或装置连接在同一总线上的其他ECU、车载仪器或装置推定为上述异常动作造成的影响范围。而且, 将其推定结果与对象日志数据一起存储于影响推定信息存储部324。

[0069] (5) 异常状态造成的危险的程度

[0070] 接下来, SOC服务器30在危险度推定部315的控制下, 在步骤S26中对上述异常动作造成的危险的程度(危险度)进行推定。该危险度的推定是基于异常检测信息中包含的异常动作的种类、以及该异常动作与威胁信息的关联性值而进行推定的。

[0071] 例如, 在异常状态的种类涉及发动机、变速器等动力单元的情况下、怀疑基于恶意软件、病毒等网络攻击的车载网络2的强占的情况下, 推定为对车辆1或驾驶员造成的危险的程度较高。另一方面, 在异常状态的种类涉及空调装置的情况下, 推定为对车辆1或驾驶员造成的危险的程度较低。具体而言, 如图5举例所示, 分为“信息(Information)”、“中等(Medium)”、“严重(Serious)”、“危急(Critical)”这4个等级判定事件的危险度。

[0072] 而且, 危险度推定部315将表示以上述方式推定的上述危险度的推定结果的信息与成为推定的对象的日志数据一起存储于影响推定信息存储部324。

[0073] (6) 异常状态的威胁种类/产生要因的推定

[0074] 接下来,SOC服务器30进行如下处理,即,在威胁种类/原因推定部316的控制下,在步骤S27中,对异常状态的威胁种类或产生要因或这两者进行推定。例如,基于表示向检测到异常状态的日志数据赋予的日志产生源的信息,推定异常状态的产生场所为ECU、车载仪器、车载装置中的哪一个。另外,例如在受到基于恶意软件、病毒等的网络攻击的情况下,通过解析该网络攻击所涉及的传送数据的通信路径信息而对表示攻击源及其通信路径的信息、例如地域、ID、域(domain)进行推定。而且,基于上述推定结果而生成表示异常状态的威胁种类(事件的攻击种类)或产生要因或这两者的信息,并存储于影响推定信息存储部324。作为事件的攻击种类,例如图4举例所示,定义了“非法访问”、“DOS攻击”、“恶意软件”、“不自然的通信”、“调查行为”以及“其他”这6个种类。

[0075] 此外,作为威胁种类/原因推定部316的处理内容,不仅可以对异常产生场所或网络攻击源进行推定,还可以对日志数据的内容进行解析而推定异常状态的威胁种类或产生要因。例如,提取由振动传感器检测出的波形的特征、由温度传感器检测出的温度变化的特征,将提取出的特征数据输入至学习模型,由此对异常状态的威胁种类或产生要因或这两者进行推定。

[0076] (7) 通知对象车辆的选择及应对信息的通知

[0077] 如果上述影响范围、危险度以及威胁种类/原因的各推定处理结束,则SOC服务器30在通知对象车辆选择部317的控制下,在步骤S28中基于表示上述影响推定信息存储部324中存储的影响范围、危险度以及威胁种类或产生要因的各推定结果的信息,选择应对信息的通知对象车辆。

[0078] 例如,在影响范围的推定结果为“制造商”、“车型”、“年份”的情况下,从PSIRT服务器40或外部服务器50获取制造商类别、车辆种类、年份类别的车辆所有者的登记信息,基于获取到的登记信息而提取“制造商”、“车型”、“年份”符合条件的车辆的所有者。而且,在通知信息发送部318的控制下,在步骤S29中基于上述危险度以及威胁种类或产生要因或这两者的推定结果而生成针对异常的应对指示。而且,基于上述提取出的所有者的列表,将包含所生成的上述应对指示在内的通知信息向该各所有者的车辆分别发送。

[0079] 另外,在影响范围的推定结果为“地域”的情况下,通知信息发送部318基于对日志数据赋予的车辆的位置信息,提取该地域存在的车辆。而且,基于上述危险度以及威胁种类或产生要因或这两者的推定结果,生成针对异常状态的应对指示,将包含该应对指示在内的通知信息向上述地域内存在的车辆发送。

[0080] 并且,通知信息发送部318根据危险度而设定发送应对指示时的优先顺序。例如,在同一时间带在多个车载网络2中分别检测到异常状态的情况下,从各异常状态造成的危险度较高的开始按顺序设定优先级,根据该优先级而发送包含应对指示在内的通知信息。其结果,例如,针对产生了动力单元的异常、怀疑车载网络2的强占的异常的车辆,与产生了空调机、电动车窗的异常、导航系统的异常的车辆相比,以更高的优先级发送包含应对指示在内的通知信息。包含上述应对指示在内的通知信息经由移动服务网络8及移动通信网络7分别向通知对象的各车辆传送。

[0081] 如果接收到上述通知信息的车辆的车载网络2通过图4所示的步骤S13而检测出接收到上述通知信息,则在步骤S14中根据上述通知信息中包含的应对指示而执行车载网络2

的复原处理。例如,根据应对指示对检测到动作异常的ECU的程序、控制数据进行修复、或对车载仪器或装置的动作状态进行重置。

[0082] (8) 分析报告的制作及发送

[0083] 并且,在报告信息发送部319的控制下,在步骤S30中,SOC服务器30制作包含上述影响推定信息存储部324中存储的表示影响范围、危险度以及威胁种类或产生要因或这两者各自的推定结果的信息、以及异常检测信息存储部323中存储的异常检测信息在内的分析报告。而且,将制作的分析报告向符合条件的制造商的PSIRT服务器40发送。

[0084] 分析报告中例如记载有表示推定出的威胁种类(事件的攻击种类)或产生要因或这两者、事件的危险度以及推荐的应对内容的消息。图5是表示威胁种类(事件的攻击种类)和危险度的尺度(事件的危险度)的组合的一个例子的图,在该例子中定义了12种组合。图6是表示分析报告的一个例子的图,“Severity”一栏中记载事件的危险度,“Category”一栏中记载事件的攻击种类。另外,“Recommendation/Action”一栏中记载针对攻击而推荐的应对消息。

[0085] 制造商能够基于上述分析报告而研究例如针对该车辆的长久的恢复方法并将其对策指示发送至该车辆、或者根据情况而研究召回。另外,还能够反映到搭载于此后开发的车辆的车载网络2的设计。

[0086] (效果)

[0087] 如以上详细所述,在一个实施方式中,在SOC服务器30中,获取从车载网络2发送的日志数据,求出获取到的日志数据和威胁信息的关联性,由此检测表示异常动作的日志数据。而且,基于上述异常的检测信息而分别对上述异常造成的影响范围、危险的程度以及异常的威胁种类或产生要因或这两者进行推定,基于上述推定结果而选择成为应对指示的通知对象的车辆,对选择的车辆发送应对指示。

[0088] 因此,基于从车辆的车载网络2发送的日志数据,对由该日志数据表示的异常状态造成的影响范围进行推定,选择与该影响范围对应的车辆组并通知应对指示。因此,不仅是检测到异常状态的车辆,例如对于同一制造商、车型、年份的其他车辆也能够同时通知应对指示。其结果,例如在因网络攻击而篡改了特定的制造商、车型或年份的车辆的ECU的程序或控制数据的情况下,也能够远程地对符合条件的车辆的程序或控制数据进行统一修复。

[0089] 另外,基于异常状态造成的影响范围而选择成为应对指示的通知目标的车辆,将通知指示仅通知给上述车辆。因此,对于需要应对的车辆能够无遗漏地通知应对指示,另一方面,对其他毫无关联的车辆不通知应对指示,因此能够不对其他车辆造成不良影响。

[0090] 并且,在发送应对指示时,能够基于异常状态造成的危险的程度以及异常的威胁种类或产生要因或这两者的推定结果而生成并发送适当的应对指示。因此,能够更可靠地使得车载网络2内的ECU、车载仪器或装置的程序、动作状态复原。

[0091] 并且,基于异常状态造成的危险程度,针对应对指示的通知目标设定优先级。因此,对于检测到例如动力单元的异常、基于网络攻击的车载网络2的强占等之类对车辆的行驶本身造成影响的重要度较高的异常的车载网络2,与检测到与其相比重要度低的异常的车载网络2相比,能够优先通知对策指示。

[0092] [其他实施方式]

[0093] (1) 作为根据日志数据而检测异常的方法,例如,为了对异常的影响范围、危险度

以及威胁种类或产生要因或这两者进行推定,可以使用利用神经网络等的学习模型。在该情况下,SOC服务器30从日志数据提取表示异常动作的特征的多个参数,将上述参数输入至学习模型,由此能够获得异常动作造成的影响范围、危险度以及异常的威胁种类或产生要因或这两者的推定结果。作为表示异常动作的特征的参数,例如可以考虑振动、温度、转速、速度、照度、周围的气候等。

[0094] (2) 在一个实施方式中,以对SOC服务器30设置车辆安全监视装置的所有功能的情况为例进行了说明。然而,并不限于此,例如,可以将车辆安全监视装置的功能分散设置于SOC服务器30和PSIRT服务器40或外部服务器50。

[0095] (3) 除此以外,关于成为检测对象的异常的种类及其检测方法、异常状态的影响范围、危险度以及威胁种类或产生要因或这两者各自的推定手法、车辆安全监视装置以及车载网络的结构、车辆安全监视处理的处理次序及处理内容等,也可以在不脱离本发明的主旨的范围内进行各种变形。

[0096] (4) 在所述一个实施方式中,以在地上行驶的轿车、货车、二轮车等通常的车辆为对象进行了说明。然而,本发明作为车辆可以将巴士、出租车等乘坐用的运营车辆、工程用车辆、农业用车辆、救护车辆等特殊用途车辆等设为对象,并且还可以应用于飞机、直升机、无人机等飞行体、在水上行驶的渔船、客船、货船、拖船等船舶、路面电车、在单轨等轨道上行驶的铁路车辆等。

[0097] (5) 可以尽量适当地对各实施方式进行组合实施,在该情况下能够获得组合效果。并且,上述实施方式中包含各种阶段的发明,能够通过公开的多个技术特征的适当的组合而提炼出各种发明。例如,即使从实施方式所示的所有技术特征删除多个技术特征,也能够解决发明要解决的问题一栏中记述的问题,在能够获得发明的效果一栏中记述的效果的情况下,作为发明能够提炼出删除了该技术特征的结构。

[0098] 标号的说明

[0099] 1…车辆

[0100] 2…车载网络

[0101] 3…通信控制单元(TCU)

[0102] 4…导航装置

[0103] 5…USB存储器

[0104] 6…便携终端

[0105] 7…移动通信网络

[0106] 8…移动服务网络

[0107] 81、82…网关

[0108] 9…互联网

[0109] 20…移动服务服务器

[0110] 30…SOC服务器

[0111] 31…控制单元

[0112] 32…存储单元

[0113] 33…通信I/F

[0114] 311…威胁信息获取部

- [0115] 312...日志数据获取部
- [0116] 313...异常检测处理部
- [0117] 314...影响范围推定部
- [0118] 315...危险度推定部
- [0119] 316...威胁种类/原因推定部
- [0120] 317...通知对象车辆选择部
- [0121] 318...通知信息发送部
- [0122] 319...报告信息发送部
- [0123] 321...威胁信息存储部
- [0124] 322...日志数据存储部
- [0125] 323...异常检测信息存储部
- [0126] 324...影响推定信息存储部
- [0127] 40...PSIRT服务器
- [0128] 50...外部服务器

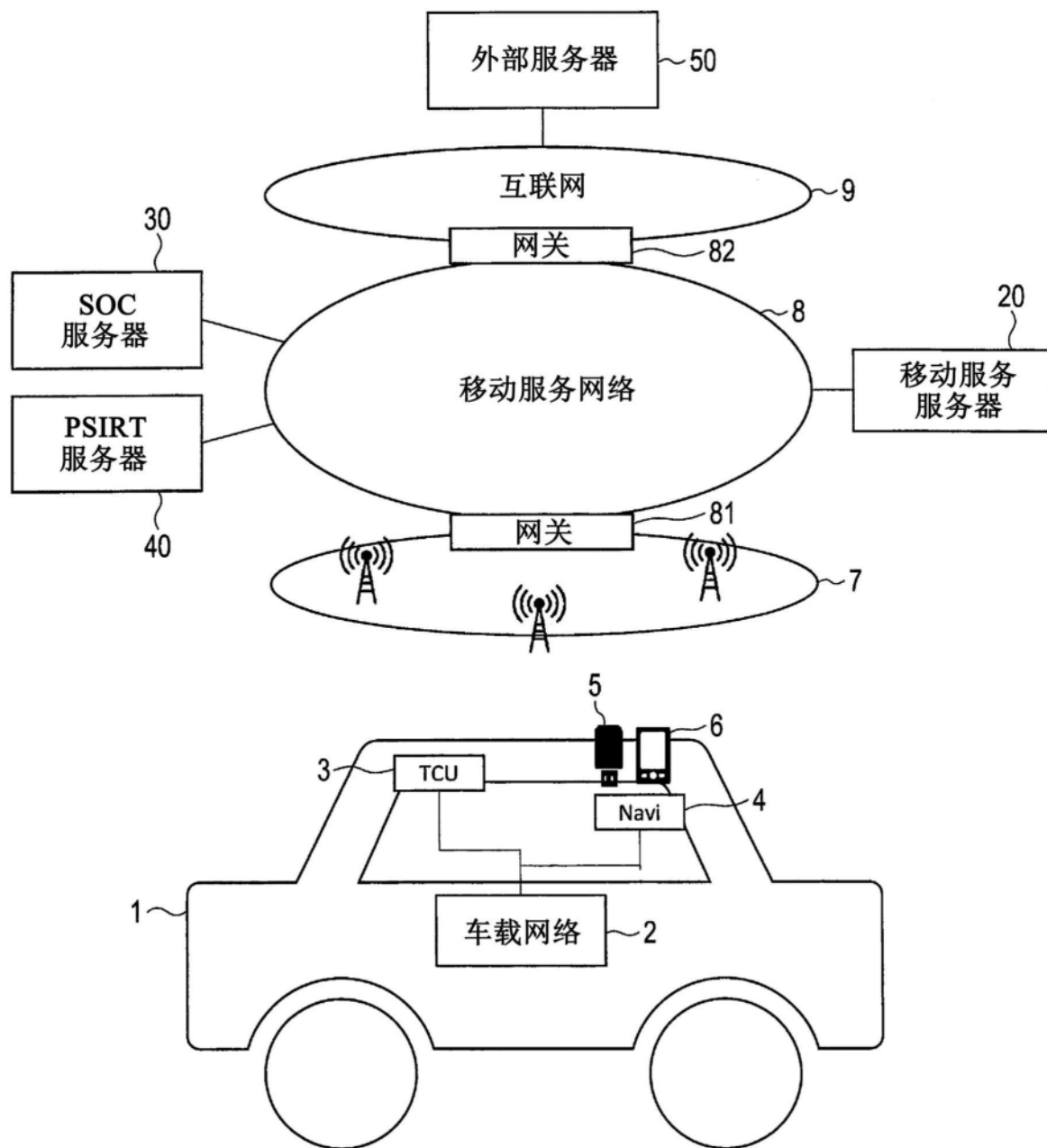


图1

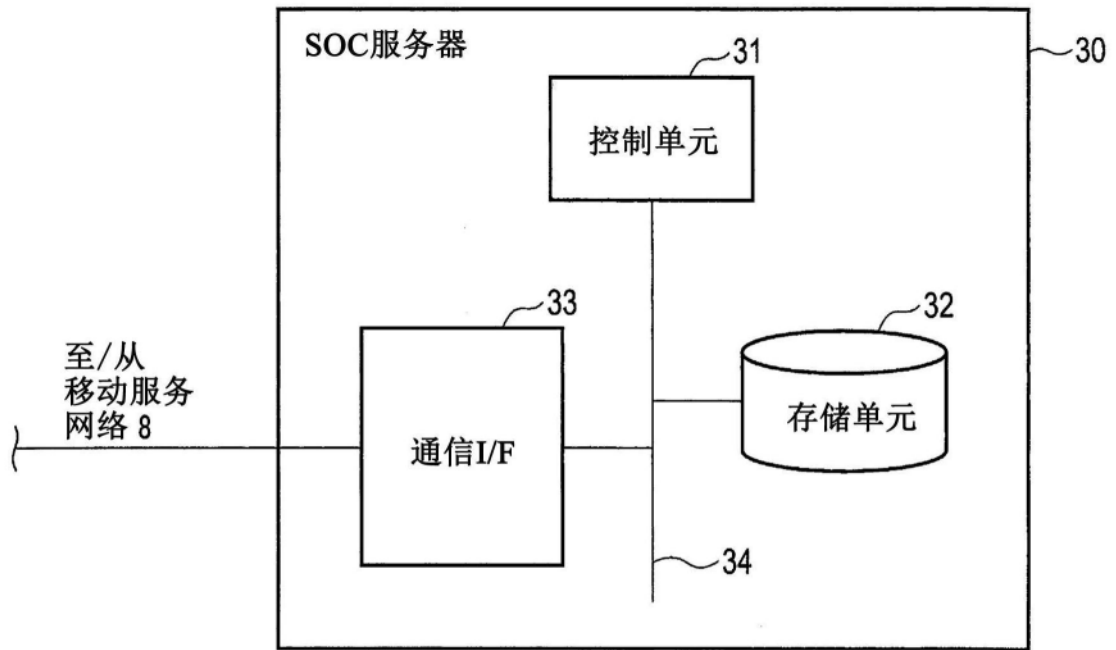


图2

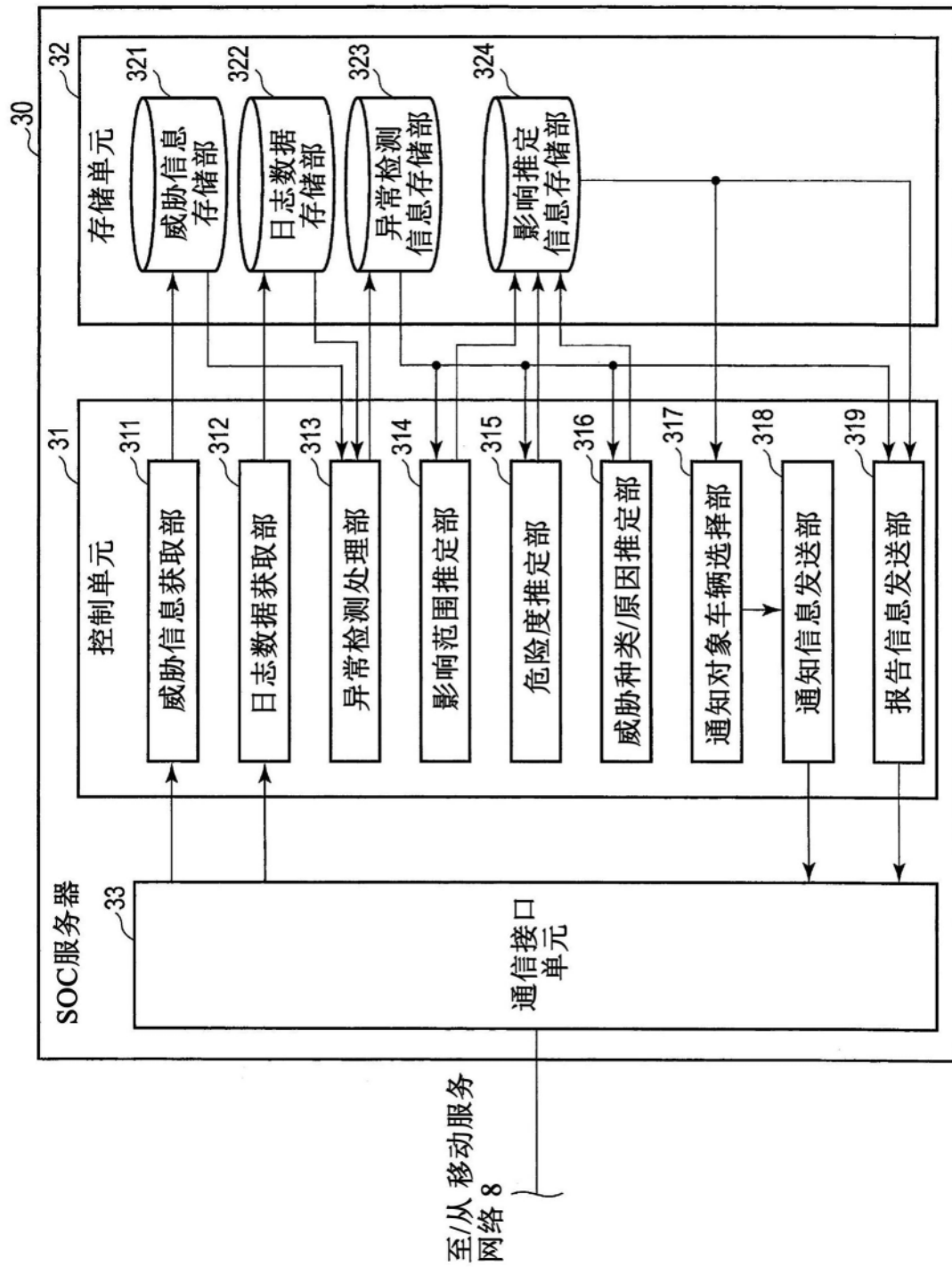


图3

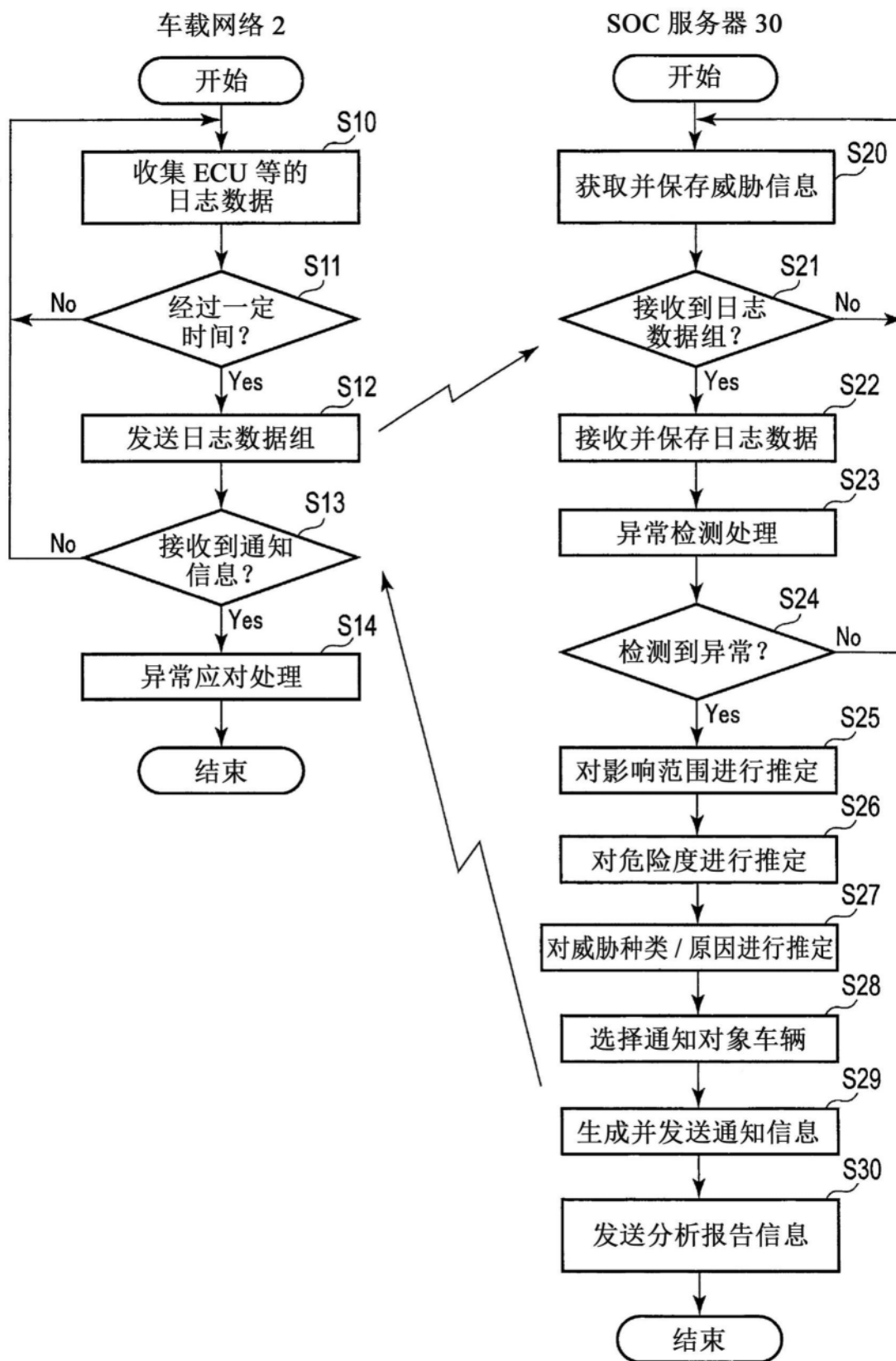


图4

事件的攻击 种类	事件的危险度				
	描述	信息	中等	严重	危急
非法访问	击中脆弱性的 攻击、尝试突破 认证的访问			攻击成功的 可能性较高的 情况	明显攻击 成功的情况
DoS攻击	陷入无法服务 状态之类的事件		未发现影响 但产生了 DoS 攻击的情况		确认到无法服务 状态的情况
恶意软件	恶意软件的下载 以及感染后的动作		确认到广告软件 等讨厌的程序 动作的情况	确认到恶意 软件的下载 成功的情况	确认到感染了 恶意软件的情况
不自然的通信	违反通常的策略的 通信、怀疑设定 有缺陷之类的通信	确认到不自然的 通信的情况		发现了导致 安全侵害之类的 设定缺陷的情况	
调查行为	网络扫描、 脆弱性扫描等 调查行为		产生了连续的 扫描行为的情况		
其他	未归类为上述 种类的攻击	其他		调查过程中 发现了安全 缺陷的情况	

图5

分析报告	
※Analysts name	
向非法站点的访问 (NUCLEAR Exploit Kit)	
※Customer	
○○有限公司	
※Device	Reference #
test_device_ids01	277622
Data and Time	
2018-07-01 15:06:1	
※Severity	
Medium	
※Category	
×300恶意软件	
※Description	
Dst侧主机存在有可能访问了设置有钓鱼工具包的页面。	
Time:2015-06-27 15:41:19	
Src:203.xx.yy.zz:8080	
Dst:203.zz.yy.zz:49612	
Signature:NUCLEAR Exploit Kit Detection	
对于通常的通过下载进行的驱动，	
在用户访问了设置有钓鱼工具包的页面之后，	
利用应用等的脆弱性而执行恶意软件的下载。	
根据本次获取的PCAP，确认到了被认为是由NUCLEAR ExploitKit生成的	
JavaScript的一部分。	
由于未获取URL日志，因此通过SOC无法掌握具体的访问目标，	
未能进行更进一步的调查。	
在当前时间点，没有确认到被认为是恶意软件感染的通信	
※Recommendation/Actions	
推荐实施下述项目。	
(1) 请确认Proxy日志等，请确认相关主机的访问目标是否为业务上意图访问的目标。	
(2) 在万一向非法的站点进行了访问的情况下，请使用防病毒软件实施相关主机的	
扫描，并且确认周边的NW仪器没有发生非法的通信。	

图6