(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 115668189 A
(43)申请公布日 2023.01.31

(21)申请号 202080101079.0
(22)申请日 2020.06.05
(85)PCT国际申请进入国家阶段日
2022.11.18
(86)PCT国际申请的申请数据
PCT/JP2020/022422 2020.06.05
(87)PCT国际申请的公布数据
WO2021/245944 JA 2021.12.09
(71)申请人 富士通株式会社
地址 日本神奈川县川崎市
(72)发明人 乾真季 藤鳥由纪 及川孝德
(74)专利代理机构 北京三友知识产权代理有限公司 11127
专利代理师 朱丽娟
(51)Int.Cl.
G06F 21/55(2006.01)
G06F 21/56(2006.01)

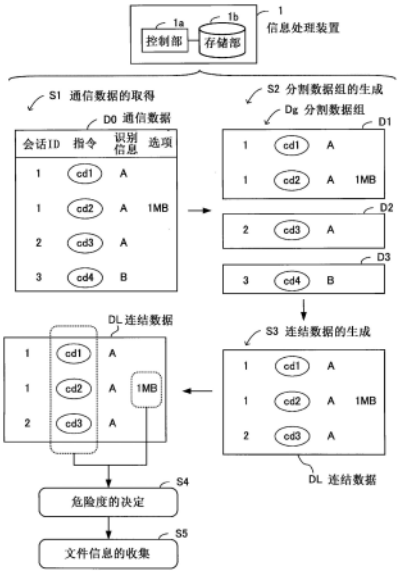
权利要求书2页 说明书13页 附图16页

(54)发明名称

信息处理程序、信息处理方法和信息处理装置

(57)摘要

高效地提取与通信的危险度对应的数据。控制部(11)决定伪会话数据(dp)以及分割会话数据(d3)的危险度等级，从伪会话数据(dp)以及分割会话数据(d3)中收集文件信息。在该情况下，在分割会话数据(d3)中不包含文件，在伪会话数据(dp)中包含文件，因此从伪会话数据(dp)中包含的文件收集文件信息。另外，在伪会话数据(dp)中包含a.exe文件，另外，a.exe文件与危险度等级为3的schtasks指令相关联。因此，控制部(11)从a.exe文件收集元信息、文件散列值以及文件主体作为文件信息。



CN 115668189 A

1.一种信息处理程序,其中,所述信息处理程序使计算机执行如下处理:

按每个会话将通信数据进行分割而生成分割数据组;

从所述分割数据组中提取具有相同的识别信息且会话间隔为阈值以下的分割数据;

将提取出的所述分割数据连结而生成连结数据;

基于所述连结数据中包含的特定信息来决定通信的危险度;以及

从所述连结数据中包含的文件收集基于所述危险度的文件信息。

2.根据权利要求1所述的信息处理程序,其中,所述特定信息是所述连结数据中包含的指令和所述连结数据中包含的所述文件的文件大小。

3.根据权利要求1所述的信息处理程序,其中,所述文件信息是所述文件的元信息、文件散列值以及文件主体中的至少一个。

4.根据权利要求2所述的信息处理程序,其中,所述指令用于远程管理操作。

5.根据权利要求2所述的信息处理程序,其中,在所述处理中,

在所述指令是用于进行信息的参照的参照类指令的情况下,将所述连结数据的所述危险度决定为最低的第一危险度,

在所述指令是用于连接到共享资源的连接类指令的情况下,将所述连结数据的所述危险度决定为比所述第一危险度高的第二危险度,

在所述指令是用于进行数据处理的更新的更新类指令且所述文件的文件大小为阈值以上的情况下,将所述连结数据的所述危险度决定为所述第二危险度,

在所述指令是所述更新类指令且所述文件的文件大小小于阈值的情况下,将所述连结数据的所述危险度决定为比所述第二危险度高的第三危险度。

6.根据权利要求5所述的信息处理程序,其中,在所述处理中,

从被决定为所述第一危险度的所述连结数据中包含的所述文件收集元信息作为所述文件信息,

从被决定为所述第二危险度的所述连结数据中包含的所述文件收集所述元信息以及文件散列值作为所述文件信息,

从被决定为所述第三危险度的所述连结数据中包含的所述文件收集所述元信息、所述文件散列值以及文件主体作为所述文件信息。

7.根据权利要求2所述的信息处理程序,其中,在所述处理中,

在所述指令是用于进行信息的参照的参照类指令的情况下,将所述连结数据的所述危险度决定为最低的第一危险度,

在所述指令是用于与共享资源连接的连接类指令的情况下,将所述连结数据的所述危险度决定为比所述第一危险度高的第二危险度,

在所述指令是用于进行数据处理的更新的更新类指令的情况下,将所述连结数据的所述危险度决定为比所述第二危险度高的第三危险度,

从被决定为所述第一危险度的所述连结数据中包含的所述文件收集元信息作为所述文件信息,

从被决定为所述第二危险度的所述连结数据中包含的所述文件收集所述元信息以及文件散列值作为所述文件信息,

从被决定为所述第三危险度的所述连结数据中包含的所述文件收集所述元信息、所述

文件散列值以及文件主体作为所述文件信息，在所述文件的文件大小为阈值以上的情况下，去除收集到的所述文件主体。

8.根据权利要求1所述的信息处理程序，其中，在所述处理中，将所述会话间隔的阈值设为观测所述通信数据的环境中的所述会话间隔的平均值。

9.根据权利要求5或7所述的信息处理程序，其中，在所述处理中，根据文件种类与在观测所述通信数据的环境中过去利用的扩展名不同的所述文件的大小、或者根据执行形式的所述文件的大小来计算平均，将对所述平均加上标准偏差而得到的值作为文件大小的阈值。

10.一种信息处理方法，其中，计算机进行如下处理：

按每个会话将通信数据进行分割而生成分割数据组；

从所述分割数据组中提取具有相同的识别信息且会话间隔为阈值以下的分割数据；

将提取出的所述分割数据连结而生成连结数据；

基于所述连结数据中包含的特定信息来决定通信的危险度；以及

从所述连结数据中包含的文件收集基于所述危险度的文件信息。

11.一种信息处理装置，其中，所述信息处理装置具有：

存储部，其存储通信数据；以及

控制部，其按每个会话将所述通信数据进行分割而生成分割数据组，从所述分割数据组中提取具有相同的识别信息且会话间隔为阈值以下的分割数据，将提取出的所述分割数据连结而生成连结数据，基于所述连结数据中包含的特定信息来决定通信的危险度，从所述连结数据中包含的文件收集基于所述危险度的文件信息。

信息处理程序、信息处理方法和信息处理装置

技术领域

[0001] 本发明涉及信息处理程序、信息处理方法以及信息处理装置。

背景技术

[0002] 在由于以因特网为代表的网络的普及而使各种信息被电子化并通过网络进行通信的状况下，针对网络威胁的安全性的重要性提高。

[0003] 作为安全相关的技术，例如提出了基于由能够记录通信日志的应用程序输出的分析对象日志文件来判断有无非法访问的技术。另外，提出了推导出表示访问的重要度的指标值以及表示访问不正当的可能性的高低的指标值来判定访问的危险度的技术。

[0004] 现有技术文献

[0005] 专利文献

[0006] 专利文献1：日本特开2002-318734号公报

[0007] 专利文献2：日本特开2018-041316号公报

发明内容

[0008] 发明所要解决的问题

[0009] 在网络安全中，例如在受到网络攻击的情况下，为了使损失为最小限度，迅速掌握攻击全貌是重要的。如果能够在早期阶段明确攻击者所使用的恶意软件(为了非法且有害地进行动作而生成的恶意软件)，则能够迅速地应对攻击。因此，期望能够高效地提取与通信的危险度对应的、和恶意软件关联的数据的技术。

[0010] 在一个方面，本发明的目的在于提供一种能够高效地提取与通信的危险度对应的数据的信息处理程序、信息处理方法以及信息处理装置。

[0011] 用于解决问题的手段

[0012] 为了解决上述问题，提供一种信息处理程序。信息处理程序使计算机执行如下处理：按每个会话将通信数据进行分割而生成分割数据组；从分割数据组中提取具有相同的识别信息且会话间隔为阈值以下的分割数据；将提取出的分割数据连结而生成连结数据；基于连结数据中包含的特定信息来决定通信的危险度；以及从连结数据中包含的文件收集基于危险度的文件信息。

[0013] 另外，为了解决上述问题，提供一种计算机执行与上述信息处理程序同样的控制的信息处理方法。

[0014] 进而，为了解决上述问题，提供一种执行与上述信息处理程序同样的控制的信息处理装置。

[0015] 发明效果

[0016] 根据一个方面，能够高效地提取与通信的危险度对应的数据。

[0017] 通过与作为本发明的例子而表示优选的实施方式的附图相关联的以下的说明，本发明的上述以及其他目的、特征以及优点将变得明确。

附图说明

[0018] 图1是用于说明第一实施方式的信息处理装置的一例的图。

[0019] 图2是表示第二实施方式的信息处理系统的一例的图。

[0020] 图3是表示服务器装置的功能块的一例的图。

[0021] 图4是表示服务器装置的硬件结构的一例的图。

[0022] 图5是表示表信息的一例的图，该表信息表示指令与危险度等级的对应关系。

[0023] 图6是表示表信息的一例的图，该表表示危险度等级与文件信息的对应关系。

[0024] 图7是用于说明从对通信日志进行会话分割到收集文件信息为止的动作的一例的图。

[0025] 图8是用于说明从对通信日志进行会话分割到收集文件信息为止的动作的一例的图。

[0026] 图9是表示通信日志的一例的图。

[0027] 图10是表示分割会话数据的一例的图。

[0028] 图11是用于说明会话间隔的一例的图。

[0029] 图12是表示伪会话数据的生成的一例的图。

[0030] 图13是表示指令-危险度等级对应表的一例的图。

[0031] 图14是表示危险度等级-文件信息对应表的一例的图。

[0032] 图15是表示危险度等级的决定的一例的图。

[0033] 图16是表示文件信息的收集的一例的图。

[0034] 图17是表示伪会话数据的生成动作的一例的流程图。

[0035] 图18是表示基于危险度等级的文件信息收集的动作的一例的流程图。

[0036] 图19是表示基于危险度等级的文件信息收集的动作的一例的流程图。

具体实施方式

[0037] 以下，参照附图说明本实施方式。

[0038] [第一实施方式]

[0039] 使用图1对第一实施方式进行说明。图1是用于说明第一实施方式的信息处理装置的一例的图。信息处理装置1具备控制部1a以及存储部1b。

[0040] 控制部1a按每个会话来分割通信数据而生成分割数据组，从分割数据组中提取具有相同的识别信息且会话间隔为阈值以下的分割数据。另外，控制部1a将提取出的分割数据连结而生成连结数据，基于连结数据所包含的特定信息来决定通信的危险度。然后，控制部1a从连结数据所包含的文件收集基于危险度的文件信息。

[0041] 存储部1b存储通信数据、特定信息与危险度的对应关系、以及收集到的文件信息等。此外，控制部1a的功能通过由信息处理装置1所具备的未图示的处理器执行规定的程序来实现。

[0042] 使用图1所示的例子对动作进行说明。

[0043] (步骤S1)控制部1a取得通信数据D0。通信数据D0具有会话ID(Identity)、指令、识别信息以及选项。识别信息相当于例如账户信息、用于用户认证的证书信息(用户ID、密码等)。

[0044] 在通信数据D0中，基于指令cd1、cd2的会话的会话ID为1，基于指令cd3的会话的会话ID为2，基于指令cd4的会话的会话ID为3。另外，会话ID为1、2的会话的识别信息为A，表示通过指令cd2进行了1MB的文件写入。会话ID为3的会话的识别信息为B。

[0045] 〔步骤S2〕控制部1a按每个会话来分割通信数据D0，生成包含分割数据D1、D2、D3的分割数据组Dg。

[0046] 〔步骤S3〕控制部1a从分割数据组Dg中提取具有相同的识别信息且会话间隔为阈值以下的分割数据。分割数据D1、D2的识别信息为A且相同。另外，分割数据D1、D2的会话间隔为阈值以下(关于会话间隔在后面叙述)。在这种情况下，从分割数据组Dg中提取分割数据D1和D2。然后，控制部1a将提取出的分割数据D1、D2连结而生成连结数据DL。

[0047] 〔步骤S4〕控制部1a基于连结数据DL所包含的特定信息来决定通信的危险度。特定信息是包含在连接数据DL中的指令和包含在连接数据DL中的文件的大小。

[0048] 因此，控制部1a基于指令以及文件的大小来决定危险度。例如，若设在指令cd1、・・・、cd4中，基于指令cd3的操作的危险度最高，设文件大小的阈值为3MB，则在连结数据DL中包含指令cd3，另外，连结数据DL中包含的文件的大小1MB为阈值以下。因此，在该情况下，连结数据DL被决定为具有危险度最高的值。

[0049] 〔步骤S5〕控制部1a基于在步骤S4中决定的危险度，从连结数据所包含的文件收集文件信息。作为文件信息，有文件的元信息、文件散列值以及文件主体。

[0050] 控制部1a基于危险度的等级，从连结数据所包含的文件中自适应地收集元信息、文件散列值以及文件主体中的至少一个。例如，从被决定为具有危险度最高的值的连结数据DL中，收集元信息、文件散列值以及文件主体作为文件信息。

[0051] 这样，在信息处理装置1中，按每个会话分割通信数据，连结具有相同识别信息且会话间隔为阈值以下的分割会话，根据通信的危险度从连结会话收集文件信息。由此，能够高效地提取与危险度对应的数据。

[0052] [第二实施方式]

[0053] 接着，对第二实施方式进行说明。图2是表示第二实施方式的信息处理系统的一例的图。信息处理系统1-1包括服务器装置10、开关sw1和sw2以及用户终端3a、3b、3c、4a、4b和4c。服务器装置10实现图1的信息处理装置1的功能。

[0054] A据点包括服务器装置10、开关sw1以及用户终端3a、3b、3c，B据点包括开关sw2以及用户终端4a、4b、4c。此外，A据点以及B据点通过未图示的网络连接。

[0055] 服务器装置10针对从用户终端3a、3b、3c向用户终端4a、4b、4c进行的通信数据决定通信的危险度等级，从通信数据所包含的文件收集规定的文件信息。或者，服务器装置10针对从用户终端4a、4b、4c向用户终端3a、3b、3c进行的通信数据决定通信的危险度等级，从通信数据所包含的文件收集规定的文件信息。

[0056] ＜功能块＞

[0057] 图3是表示服务器装置的功能块的一例的图。服务器装置10具备控制部11以及存储部12。控制部11实现图1的控制部1a的功能，存储部12实现图1的存储部1b的功能。

[0058] 控制部11包括通信接口部11a、通信日志生成部11b、会话分割部11c、伪会话生成部11d、危险度等级决定部11e以及文件信息收集部11f。

[0059] 通信接口部11a进行经由与服务器装置10连接的网络的通信接口处理，通过网络

接收通信数据(包)。通信日志生成部11b对接收到的通信数据进行解析,根据执行操作的指令、文件访问,由通信数据而生成(重构)通信日志。

[0060] 会话分割部11c在远程管理操作协议(设计为能够将保存于远程计算设备中的文件显示于用户终端来进行访问的协议)的会话中分割通信日志,生成分割会话数据。另外,作为远程管理操作协议,例如有SMB(Server Message Block:服务器消息块)。

[0061] 伪会话生成部11d针对分割会话数据,提取指令的执行账户为相同账户且会话间隔为预先决定的阈值以下的多个分割会话数据。然后,伪会话生成部11d将提取出的分割会话数据连结而生成伪会话数据(相当于图1的连结数据)。

[0062] 危险度等级决定部11e基于伪会话数据所包含的指令以及伪会话数据所包含的文件的大小,决定危险度等级。文件信息收集部11f从伪会话数据所包含的文件中收集基于危险度等级的文件信息。

[0063] 存储部12存储通信数据(通信日志)、表信息以及收集到的文件信息等。另外,存储部12存储与服务器装置10的运用相关的控制信息等。另外,作为表信息,例如有表示指令与危险度等级的对应关系的指令-危险度等级对应表T1、以及表示危险度等级与应收集的文件信息的对应关系的危险度等级-文件信息对应表T2(在图13、图14中后述)。

[0064] ＜硬件＞

[0065] 图4是表示服务器装置的硬件结构的一例的图。服务器装置10由处理器(计算机)100整体控制。处理器100实现控制部11的功能。

[0066] 存储器101、输入输出接口102和网络接口104经由总线103连接到处理器100。

[0067] 处理器100可以是多处理器。处理器100例如是CPU(Central Processing Unit:中央处理单元)、MPU(Micro Processing Unit:微处理单元)、DSP(Digital Signal Processor:数字信号处理器)、ASIC(Application Specific Integrated Circuit:专用集成电路)或PLD(Programmable Logic Device:可编程逻辑器件)。此外,处理器100也可以是CPU、MPU、DSP、ASIC、PLD中的2个以上的要素的组合。

[0068] 存储器101实现存储部12的功能,作为服务器装置10的主存储装置使用。在存储器101中暂时存储有使处理器100执行的OS(Operating System:操作系统)的程序、应用程序的至少一部分。另外,在存储器101中存储处理器100的处理所需的各种数据。

[0069] 另外,存储器101也被用作服务器装置10的辅助存储装置,存储OS的程序、应用程序以及各种数据。存储器101也可以包括闪存、SSD(Solid State Drive:固态硬盘)等半导体存储装置、HDD(Hard Disk Drive:硬盘驱动器)等磁记录介质作为辅助存储装置。

[0070] 作为连接到总线103的外围设备包括输入输出接口102和网络接口104。输入输出接口102能够连接键盘、鼠标等信息输入装置,将从信息输入装置发送来的信号发送到处理器100。

[0071] 此外,输入输出接口102还作为用于连接外围设备的通信接口起作用。例如,输入输出接口102可以连接光学驱动装置,该光学驱动装置使用激光等读取记录在光盘上的数据。光盘有Blu-ray Disc(注册商标)、CD-ROM(Compact Disc Read Only Memory:只读光盘存储器)、CD-R(Recordable:可记录)/RW(Rewritable:可重写)等。

[0072] 另外,输入输出接口102能够连接存储器装置、存储器读写器。存储器装置是安装有与输入输出接口102之间的通信功能的记录介质。存储器读写器是进行向存储卡的数据

的写入、或者从存储卡读出数据的装置。存储卡是卡型记录介质。

[0073] 网络接口104与网络连接而进行网络接口控制。网络接口104例如也能够使用NIC(Network Interface Card:网络接口卡)、无线LAN(Local Area Network:局域网)卡等。由网络接口104接收到的数据被输出到存储器101或处理器100。

[0074] 通过以上那样的硬件结构,能够实现服务器装置10的处理功能。例如,服务器装置10能够通过由处理器100分别执行规定的程序来进行本发明的处理。

[0075] 服务器装置10例如通过执行记录在计算机可读取的记录介质中的程序来实现本发明的处理功能。记述了使服务器装置10执行的处理内容的程序能够记录在各种记录介质中。

[0076] 例如,能够将使服务器装置10执行的程序存储在辅助存储装置中。处理器100将辅助存储装置内的程序的至少一部分加载到主存储装置,来执行程序。

[0077] 另外,也可以记录在光盘、存储装置、存储卡等可移动型记录介质中。存储在可移动型记录介质中的程序例如能够在通过来自处理器100的控制而安装到辅助存储装置之后执行。处理器111也可以直接从可移动型记录介质中读取程序来执行所述程序。

[0078] <文件信息的收集(不生成伪会话数据的情况)>

[0079] 接着,在说明第二实施方式的详细情况之前,使用图5至图8对不生成伪会话数据而收集文件信息的情况下的服务器装置(称为服务器装置20)的动作及其问题进行说明。

[0080] 图5是表示表信息的一例的图,该表表示指令与危险度等级的对应关系。表T11具有作为项目的指令以及危险度等级。在表T11中登记有通信日志所包含的指令的危险度等级。

[0081] 在图5的例子中,登记为(指令,危险度等级)=(net group,1)、(net use,2)、(schtasks,3)(危险度等级的数值越高则危险度越高)。

[0082] 在此,net group是将被远程管理操作侧的装置(远程管理操作源装置)所属的账户信息等一览显示在进行远程管理操作侧的装置(远程管理操作目的地装置)中的参照类的指令。

[0083] net use是用于远程管理操作目的地装置与远程管理操作源装置的共享资源(共享文件夹)连接的连接类的指令。schtasks是远程管理操作目的地装置控制远程管理操作源装置中的任务调度器的任务处理的更新类的指令。

[0084] 在通过远程管理操作目的地装置受到攻击的情况下,对于上述的指令而言,危险度最高的指令(进行感染扩大的可能性最高的指令)是schtasks,将危险度等级设为3。危险度其次高的指令是net use,将危险度等级设为2。并且,3个指令中危险度最低的指令是net group,将危险度等级设为1。

[0085] 图6是示出表示危险度等级与文件信息的对应关系的表信息的一例的图。表T12具有作为项目的危险度等级以及文件信息。在表T12中登记有根据危险度等级应该收集的文件信息。

[0086] 在图6的例子中,登记为(危险度等级,文件信息)=(1,元信息)、(2,元信息/文件散列值)、(3,元信息/文件散列值/文件主体)。

[0087] 即,在危险度等级为1的情况下,应该从文件收集的文件信息仅被设定为该文件的元信息。在危险度等级为2的情况下,应该从文件收集的文件信息被设定为该文件的元信息

以及该文件的文件散列值。在危险度等级为3的情况下，应该从文件收集的文件信息被设定为该文件的元信息、该文件的文件散列值以及该文件的主体。

[0088] 图7、图8是用于说明从对通信日志进行会话分割到收集文件信息为止的动作的一例的图。

[0089] 在图7中，服务器装置20接收被远程管理操作的通信数据，根据接收到的通信数据生成通信日志L2。作为项目，通信日志L2具有日期、时刻、会话ID、指令以及选项。

[0090] 在通信日志L2中，在日志L2a的(2019-12-26,10:40,1,net use,ipc$)中，记录了在2019-12-26的10:40通过net use指令对共享资源ipc$有连接请求。

[0091] 在日志L2b的(2019-12-26,10:42,1,net use,admin$)中，记录了在2019-12-26的10:42通过net use指令对共享文件夹admin$有连接请求。

[0092] 在日志L2c的(2019-12-26,10:45,1,WRITE,a.exe)中，记录了在2019-12-26的10:45通过WRITE指令在共享文件夹admin$进行了a.exe的文件的写入。

[0093] 在日志L2d的(2019-12-26,10:47,2,schtasks,create)中，记录了在2019-12-26的10:47通过schtasks指令在任务调度器中进行了任务登记(create)。

[0094] 在日志L2e的(2019-12-26,10:47,2,schtasks,start)中，记录了在2019-12-26的10:47通过schtasks指令进行了登记的任务的执行的开始(start)。

[0095] 在日志L2f的(2019-12-26,10:57,3,net group,admin)中，记录了在2019-12-26的10:57通过net group指令进行了admin组的一览显示。

[0096] 另外，日志L2a是向共享资源的连接，L2b、L2c是向共享文件夹的文件写入关联的远程管理操作，这些远程管理操作的会话ID为1。另外，日志L2d、L2e是任务处理关联的远程管理操作，该远程管理操作的会话ID为2。进而，日志L2f是账户信息的显示关联的远程管理操作，该远程管理操作的会话ID为3。

[0097] 对于这样的通信日志L2，在服务器装置20中，将通信日志L2按每个会话进行分割。即，将通信日志L2分割为会话ID为1的分割会话数据d11、会话ID为2的分割会话数据d12、以及会话ID为3的分割会话数据d13。

[0098] 在图8中，服务器装置20基于图5所示的表T11，决定分割会话数据d11、d12、d13各自的危险度等级。由于分割会话数据d11包含net use指令，所以危险度等级被决定为2，由于分割会话数据d12包含schtasks指令，所以危险度等级被决定为3。进而，由于分割会话数据d13包含net group指令，所以危险度等级被决定为1。

[0099] 服务器装置20在决定了危险度等级之后，从分割会话数据d11、d12、d13中收集文件信息。在该情况下，由于在分割会话数据d12、d13中不包含文件，在分割会话数据d11中包含文件，所以从分割会话数据d11中包含的文件收集文件信息。

[0100] 在分割会话数据d11中包含a.exe文件，另外，a.exe文件与危险度等级为2的net use指令相关联。

[0101] 因此，服务器装置20基于图6所示的表T12，从a.exe文件收集元信息以及文件散列值作为文件信息。因此，从通信日志L2收集元信息和文件散列值作为文件信息，并将它们存储在存储设备中。

[0102] 但是，在上述那样的服务器装置20的控制中，文件信息的收集精度低，应收集的文件信息不充分。这是因为，在通信日志L2中包含schtasks这样的危险度等级为3的指令，所

以本来希望从通信日志L2收集的文件信息应该是元信息、文件散列值以及文件主体，但只能收集元信息以及文件散列值。

[0103] 产生这样的问题是因为a.exe文件未与危险度等级为3的schtasks指令相关联。如果进行将a.exe文件与危险度等级为3的schtasks指令相关联的通信日志L2的分割控制，则能够收集包括文件主体在内的信息作为文件信息。

[0104] 在此，对根据危险度等级而应收集的文件信息不同的理由进行说明。上述的net use、schtasks等指令是由服务器的运用管理者在正常业务中通常使用的指令。

[0105] 因此，如果针对任何指令都从通过远程管理操作写入的文件全部收集文件主体并存储到存储设备中，则会产生存储设备容量急缺的问题。

[0106] 另外，若进行这样的文件信息的收集控制，则在实际进行了攻击的情况下，非法文件会被埋没在大量的文件中，难以从正常文件中检测非法文件。

[0107] 根据这样的理由，根据危险度等级来收集不同的文件信息。如果从攻击者使用的可能性高的文件收集文件主体，则能够进一步提高文件信息的收集精度。本发明是鉴于这样的点而完成的，提高文件信息的收集精度，高效地提取与危险度高的通信有关的数据。

[0108] ＜本发明的文件信息的收集(生成伪会话数据的情况)＞

[0109] 接着，对第二实施方式的动作进行详细说明。在第二实施方式的服务器装置10中，例如进行与危险度等级为3的schtasks指令相关联的通信日志的分割控制(伪会话数据的生成)。进而，还进行文件大小的判定处理，能够从危险度等级高的文件高精度地收集包括文件主体在内的信息。

[0110] (通信日志的生成)

[0111] 图9是表示通信日志的一例的图。服务器装置10内的控制部11接收被远程管理操作的通信数据，根据接收到的通信数据生成通信日志L1。通信日志L1具有日期、时刻、会话ID、指令以及选项作为项目。

[0112] 在通信日志L1中，在日志L1a的(2019-12-26,10:40,1,net use,ipc$,acccount:A)中，记录了在2019-12-26的10:40由账户A通过net use指令对共享资源ipc$有连接请求。

[0113] 在日志L1b的(2019-12-26,10:42,1,net use,admin$,acccount:A)中，记录了在2019-12-26的10:42由账户A通过net use指令对共享文件夹admin$有连接请求。

[0114] 在日志L1c的(2019-12-26,10:45,1,WRITE,a.exe,acccount:A,1MB)中，记录了在2019-12-26的10:45由账户A通过WRITE指令在共享文件夹admin$中进行了a.exe的文件的写入。另外，文件大小被记录为1MB。

[0115] 在日志L1d的(2019-12-26,10:47,2,schtasks,create,acccount:A)中，记录了在2019-12-26的10:47由账户A通过schtasks指令在任务调度器中进行了任务登记(create)。

[0116] 在日志L1e的(2019-12-26,10:47,2,schtasks,start,acccount:A)中，记录了在2019-12-26的10:47由账户A通过schtasks指令进行了登记的任务的执行的开始(start)。

[0117] 在日志L1f的(2019-12-26,10:57,3,net group,admin,acccount:B)中，记录了在2019-12-26的10:57由账户B通过net group指令进行了admin组的一览显示。

[0118] 另外，日志L1a是向共享资源的连接，L1b、L1c是向共享文件夹的文件写入相关的远程管理操作，该远程管理操作的会话ID为1。另外，日志L1d、L1e是任务处理关联的远程管理操作，该远程管理操作的会话ID为2。进而，日志L1f是账户信息的显示关联的远程管理操

作，该远程管理操作的会话ID为3。

[0119] (分割会话数据的生成)

[0120] 图10是表示分割会话数据的一例的图。控制部11针对通信日志L1，按每个会话分割通信日志L1。即，将通信日志L1分割为会话ID为1的分割会话数据d1、会话ID为2的分割会话数据d2、以及会话ID为3的分割会话数据d3。

[0121] (会话间隔)

[0122] 接着，对为了生成伪会话数据而使用的会话间隔进行说明。图11是用于说明会话间隔的一例的图。横轴是时间。假设会话se1、se2和se3如图11所示连续执行。

[0123] 当会话se1的结束时刻为t1、会话se2的开始时刻为t2(＞t1)时，时刻t1、t2的时间间隔成为会话se1、se2的会话间隔ta(在该情况下为正值)。

[0124] 另外，当会话se2的结束时刻为t4，会话se3的开始时刻为t3(＜t4)时，时刻t3、t4的时间间隔成为会话se2、se3的会话间隔tb(在该情况下为负值)。

[0125] (会话间隔的阈值)

[0126] 会话间隔的阈值例如是在应用服务器装置10的控制的环境中观测到的会话间隔的平均值。这里，将在相同发送源、发送目的地观测的会话的开始时刻设为t_s，将会话的结束时刻设为t_e，将会话间隔t_{int}设为$t_{int}=t_e-t_s$。

[0127] 此时，如果将在环境内观测的会话间隔设为$T=\{t_{int,1},t_{int,2},t_{int,3},\cdots,t_{int,n}\}$，则会话间隔$S_{th}$根据以下的式(1)计算。另外，n是数据的总数。

[0128] [数式1]

[0129] $$S_{th}=\frac{1}{n}\sum_{i=1}^{n}\left|t_{int,i}\right| \quad \cdots(1)$$

[0130] (伪会话数据的生成)

[0131] 图12是表示伪会话数据的生成的一例的图。在生成如图10所示的分割会话数据后，控制部11生成伪会话数据。控制部11将多个分割会话数据中的相同账户(或者相同证书)的分割会话数据、且该分割会话数据的会话间隔为阈值以下的分割会话数据连结而生成伪会话数据。

[0132] 控制部11首先提取分割会话数据d1、d2、d3中的具有相同账户的分割会话数据。这里，由于分割会话数据d1、d2是账户A，分割会话数据d3是账户B，所以提取具有相同账户A的分割会话数据d1、d2。

[0133] 接着，控制部11判定分割会话数据d1、d2的会话间隔是否为阈值以下。分割会话数据d1的结束时刻、即日志L1c的时刻为10:45，分割会话数据d2的开始时刻、即日志L1d的时刻为10:47。

[0134] 因此，如果分割会话数据d1、d2的会话间隔为2分钟，将会话间隔的阈值设为5分钟，则分割会话数据d1、d2为会话间隔的阈值以下，满足条件。

[0135] 因此，控制部11将具有相同的账户且会话间隔为阈值以下的分割会话数据d1、d2连结而生成伪会话数据dp。

[0136] (表结构)

[0137] 图13是表示指令-危险度等级对应表的一例的图。指令-危险度等级对应表T1具有

指令以及危险度等级作为项目，预先登记有通信日志所包含的指令的危险度等级。

[0138] 在图13的例子中，登记为(指令，危险度等级)＝(net group，1)、(net use，2)、(schtasks(文件大小为阈值以上)，2)、(schtasks(文件大小小于阈值)，3)。

[0139] net group是用于进行信息的参照的参照类指令的1个，net use是用于连接到共享资源的连接类指令的1个。此外，schtasks是用于进行数据处理的更新的更新类指令的1个。

[0140] 在此，net group指令的危险度等级为1，net use指令的危险度等级为2这一点与图5相同，但schtasks的危险度等级的设定不同。

[0141] 在服务器装置10中，即使是相同的schtasks指令，在与schtasks指令相关联的文件的大小为阈值以上的情况下，将危险度等级设为2，在与schtasks指令相关联的文件的大小小于阈值的情况下，将危险度等级设为3。

[0142] 图14是示出危险度等级-文件信息对应表的一例的图。危险度等级-文件信息对应表T2具有危险度等级以及文件信息作为项目，登记有根据危险度等级应该收集的文件信息。

[0143] 在图14的例子中，登记为(危险度等级，文件信息)＝(1，元信息)、(2，元信息/文件散列值)、(3，元信息/文件散列值/文件主体)。

[0144] 即，在危险度等级为1的情况下，应该从文件收集的文件信息仅为该文件的元信息。元信息中例如有文件名、文件的扩展名及时间戳(表示进行文件的变更、修正的时期的信息)。

[0145] 另外，在危险度等级为2的情况下，应该从文件收集的文件信息成为该文件的元信息以及该文件的文件散列值。并且，在危险度等级为3的情况下，应该从文件收集的文件信息成为该文件的元信息、该文件的文件散列值以及该文件的主体。这样，设定为危险度等级越高，则应该从提取出的文件收集的文件信息的种类越多。

[0146] ＜文件大小的阈值＞

[0147] 文件大小的阈值(上限值)是对平均加上标准偏差而得到的，该平均是根据实际的文件种类与在应用服务器装置20的控制的环境中过去观测到的扩展名不同的文件的大小、或者根据执行形式的文件的大小而计算出的。

[0148] 这里，如果将实际的文件种类与在环境中过去观测到的扩展名不同的文件、或者执行形式的文件的大小S设为$S=\{S_1,S_2,S_3,\cdots,S_n\}$，则平均μ用以下的式(2)表示(n是数据的总数)。因此，文件大小的阈值F_{th}通过以下的式(3)计算。另外，x_i是各个数值。

[0149] [数式2]

[0150] $$\mu=\frac{1}{n}\sum_{i=1}^{n}S_i \quad \cdots(2)$$

[0151] [数式3]

[0152] $$F_{th}=\mu+\sqrt{\sum_{i=1}^{n}\frac{1}{n}(x_i-\mu)^2} \quad \cdots(3)$$

[0153] 另外，在通常的应用程序中使用的执行文件的大小大多为5MB至10MB左右，但恶意软件的文件大多为例如数百KB至小于5MB。因此，如上述那样决定文件大小的阈值(上限值)，实现非法文件的确定。

[0154] (危险度等级的决定)

[0155] 图15是表示危险度等级的决定的一例的图。控制部11基于图13所示的指令-危险度等级对应表T1，决定伪会话数据dp以及分割会话数据d3的危险度等级。

[0156] 将文件大小的阈值设为3MB。在伪会话数据dp中包含schtasks指令和文件，该文件的大小为1MB。

[0157] 因此，伪会话数据dp具有与文件大小小于阈值的文件相关联的schtasks指令，因此基于指令-危险度等级对应表T1，将危险度等级决定为3。另外，由于在分割会话数据d3中包含net group指令，所以将危险度等级决定为1。

[0158] (文件信息的收集)

[0159] 图16是表示文件信息的收集的一例的图。控制部11在决定了危险度等级之后，从伪会话数据dp以及分割会话数据d3中收集文件信息。

[0160] 在该情况下，在分割会话数据d3中不包含文件，在伪会话数据dp中包含文件，因此从伪会话数据dp中包含的文件收集文件信息。

[0161] 在伪会话数据dp中包含a.exe文件，另外，a.exe文件与危险度等级为3的schtasks指令相关联。

[0162] 因此，控制部11基于图14所示的危险度等级-文件信息对应表T2，从a.exe文件收集元信息、文件散列值以及文件主体作为文件信息。因此，从通信日志L1收集元信息、文件散列值以及文件主体作为非法文件的文件信息，并保存到存储部12(存储设备)。

[0163] 这样，在控制部11中，进行根据通信日志L1生成上述那样的伪会话数据的分割控制，进而进行文件大小的判定。由此，a.exe文件与用于收集包含文件主体的信息的危险度等级建立对应，因此能够收集包含文件主体的信息作为文件信息。

[0164] (流程图)

[0165] 图17是表示伪会话数据的生成动作的一例的流程图。

[0166] 〔步骤S11〕控制部11分割通信数据，生成分割会话数据。

[0167] 〔步骤S12〕控制部11计算以相同账户(或者相同证书)执行的分割会话数据的会话间隔。

[0168] 〔步骤S13〕控制部11判定会话间隔是否为阈值以下。在阈值以下的情况下，处理进入步骤S14，在超过阈值的情况下，处理进入步骤S16。

[0169] 〔步骤S14〕控制部11进行会话连结的处理，连结分割会话数据。

[0170] 〔步骤S15〕控制部11判定在阈值的时间内是否存在后续的分割会话数据。在存在分割会话数据的情况下，处理返回步骤S13，在不存在分割会话数据的情况下，处理进入步骤S16

[0171] 〔步骤S16〕控制部11结束会话连结的处理。

[0172] 〔步骤S17〕控制部11将连结的分割会话数据作为伪会话数据。

[0173] 图18是表示基于危险度等级的文件信息收集的动作的一例的流程图。

[0174] 〔步骤S21〕控制部11进行伪会话数据内的指令的分析。

[0175] 〔步骤S22〕控制部11判定伪会话数据内是否包含更新类指令(例如schtasks)。在包含更新类指令的情况下,处理进入步骤S23,在不包含更新类指令的情况下,处理进入步骤S24。

[0176] 〔步骤S23〕控制部11判定伪会话数据内的文件的大小是否小于阈值。在小于阈值的情况下,处理进入步骤S25a,在阈值以上的情况下,处理进入步骤S25b。

[0177] 〔步骤S24〕控制部11判定伪会话数据内的指令是连接类(例如,net use)还是参照类(例如,net group)。在连接类指令的情况下,处理进入步骤S25b,在参照类指令的情况下,处理进入步骤S25c。

[0178] 〔步骤S25a〕控制部11将伪会话数据的危险度等级决定为3。

[0179] 〔步骤S25b〕控制部11将伪会话数据的危险度等级决定为2。

[0180] 〔步骤S25c〕控制部11将伪会话数据的危险度等级决定为1。

[0181] 〔步骤S26a〕控制部11从伪会话数据内的文件收集元信息、文件散列值以及文件主体作为文件信息。

[0182] 〔步骤S26b〕控制部11从伪会话数据内的文件收集元信息以及文件散列值作为文件信息。

[0183] 〔步骤S26c〕控制部11从伪会话数据内的文件收集元信息作为文件信息。

[0184] 〔步骤S27〕控制部11将收集到的文件信息存储于存储部12。

[0185] 图19是表示基于危险度等级的文件信息收集的动作的一例的流程图。在图19的动作中,如果在危险度等级为3时在伪会话数据内有文件,则与大小无关地暂时收集包括文件主体的信息。然后,在判定为文件大小为阈值以上的情况下,去除收集到的文件,如果小于阈值,则直接进行收集。

[0186] 〔步骤S31〕控制部11判定通过远程管理操作写入到伪会话数据内的文件的大小是否小于阈值。在小于阈值的情况下,处理进入步骤S32,在阈值以上的情况下,处理进入步骤S33。

[0187] 〔步骤S32〕控制部11将用于取得文件主体的文件主体取得开关打开。

[0188] 〔步骤S33〕控制部11将文件主体取得开关关闭。

[0189] 〔步骤S34〕控制部11决定伪会话数据的危险度等级。

[0190] 〔步骤S35〕控制部11判定所决定的危险度等级是否为1。在危险度等级为1的情况下,处理进入步骤S36,在不是1的情况下,处理进入步骤S37。

[0191] 〔步骤S36〕控制部11收集危险度等级为1的文件信息(元信息)。处理进入步骤S40。

[0192] 〔步骤S37〕控制部11判定所决定的危险度等级是否为2。在危险度等级为2的情况下,处理进入步骤S38,在不是2的情况下,处理进入步骤S39。

[0193] 〔步骤S38〕控制部11收集危险度等级为2的文件信息(元信息以及文件散列值)。处理进入步骤S40。

[0194] 〔步骤S39〕控制部11识别为危险度等级是3,收集危险度等级为3的文件信息(元信息、文件散列值以及文件主体)。

[0195] 〔步骤S40〕控制部11判定文件主体取得开关的状态(打开还是关闭)。在关闭的情况下,处理进入步骤S41,在打开的情况下,处理进入步骤S42。

[0196] 〔步骤S41〕控制部11从收集到的文件信息中除去文件主体。

[0197] 〔步骤S42〕控制部11将收集到的文件信息存储于存储部12。

[0198] (效果)

[0199] 接下来,对应用了本发明的情况下的效果进行说明。作为前提,恶意软件的文件大小大多为3MB以下,想要收集这样的文件。

[0200] 作为设想状况,将写入1件文件、在5分钟以内执行更新类操作的操作设为100次/日,将在与文件写入不同的会话中执行的更新类操作的比例设为80%。另外,3MB以下的文件的写入在整体上均匀分布,按40%(40件/天)发生。

[0201] 此时,能够取得的3MB以下的文件件数(连结会话间隔为5分钟以内的会话的情况)在应用本发明前是8件(=100次×(1-0.8)×0.4)。与此相对,在应用了本发明的情况下为40件(=100件×0.4),文件取得率变为5倍,能够高效地取得恶意软件的文件。

[0202] 如以上说明的那样,根据本发明,按每个会话分割通信数据,连结具有相同识别信息且会话间隔为阈值以下的分割会话,根据通信的危险度从连结会话收集文件信息。由此,文件信息的收集精度提高,并且能够高效地提取与危险度高的通信有关的数据。另外,能够迅速地进行攻击全貌调查,能够迅速地应对,因此能够使由攻击引起的损失为最小限度。

[0203] 上述说明的本发明的信息处理装置1以及服务器装置10能够通过计算机来实现。在该情况下,提供记述了信息处理装置1和服务器装置10应具有的功能的处理内容的程序。通过由计算机执行该程序,由此在计算机上实现上述处理功能。

[0204] 记述有该处理的程序可以存储在计算机可读介质中。计算机可读记录介质的例子包括磁存储部、光盘、磁光记录介质、和半导体存储器。磁存储部包括硬盘装置(HDD)、软盘(FD)、磁带等。光盘有CD-ROM/RW等。光磁记录介质有MO(Magneto Optical disk:磁光盘)等。

[0205] 在使程序流通的情况下,例如,销售记录有该程序的CD-ROM等可移动型记录介质。另外,还可以将程序预先存储到服务器计算机的存储部内,并经由网络从服务器计算机向其它计算机转发该程序。

[0206] 执行程序的计算机将例如记录在可移动型记录介质中的程序或从服务器计算机转发的程序存储在自己的存储部中。然后,计算机从自己的存储部读取程序,执行基于程序的处理。另外,计算机可以从可移动型记录介质直接读取程序来执行基于该程序的处理。

[0207] 此外,计算机可以在每次从通过网络连接的服务器计算机转发程序时,依次执行基于所接收的程序的处理。另外,也能够通过DSP、ASIC、PLD等电子电路来实现上述的处理功能的至少一部分。

[0208] 以上例示了实施方式,能够将实施方式中表示的各部分的结构置换为具有相同功能的其他结构。此外,也可以附加其他任意的结构物和步骤。进而,也可以组合前述的实施方式中的任意2个以上的结构(特征)。

[0209] 关于上述内容,仅表示本发明的原理。并且,本领域技术人员能够进行多个变形、变更,本发明并不限定于上述所示和所说明的准确的结构和应用例,对应的所有变形例和等同物被视为基于附加的权利要求及其等同物的本发明的范围。

[0210] 附图标记说明

[0211] 1 信息处理装置

[0212] 1a 控制部

[0213] 1b 存储部

[0214] cd1、cd2、cd3、cd4 指令

[0215] A、B 识别信息

[0216] D0 通信数据

[0217] Dg 分割数据组

[0218] D1、D2、D3 分割数据

[0219] DL 连结数据

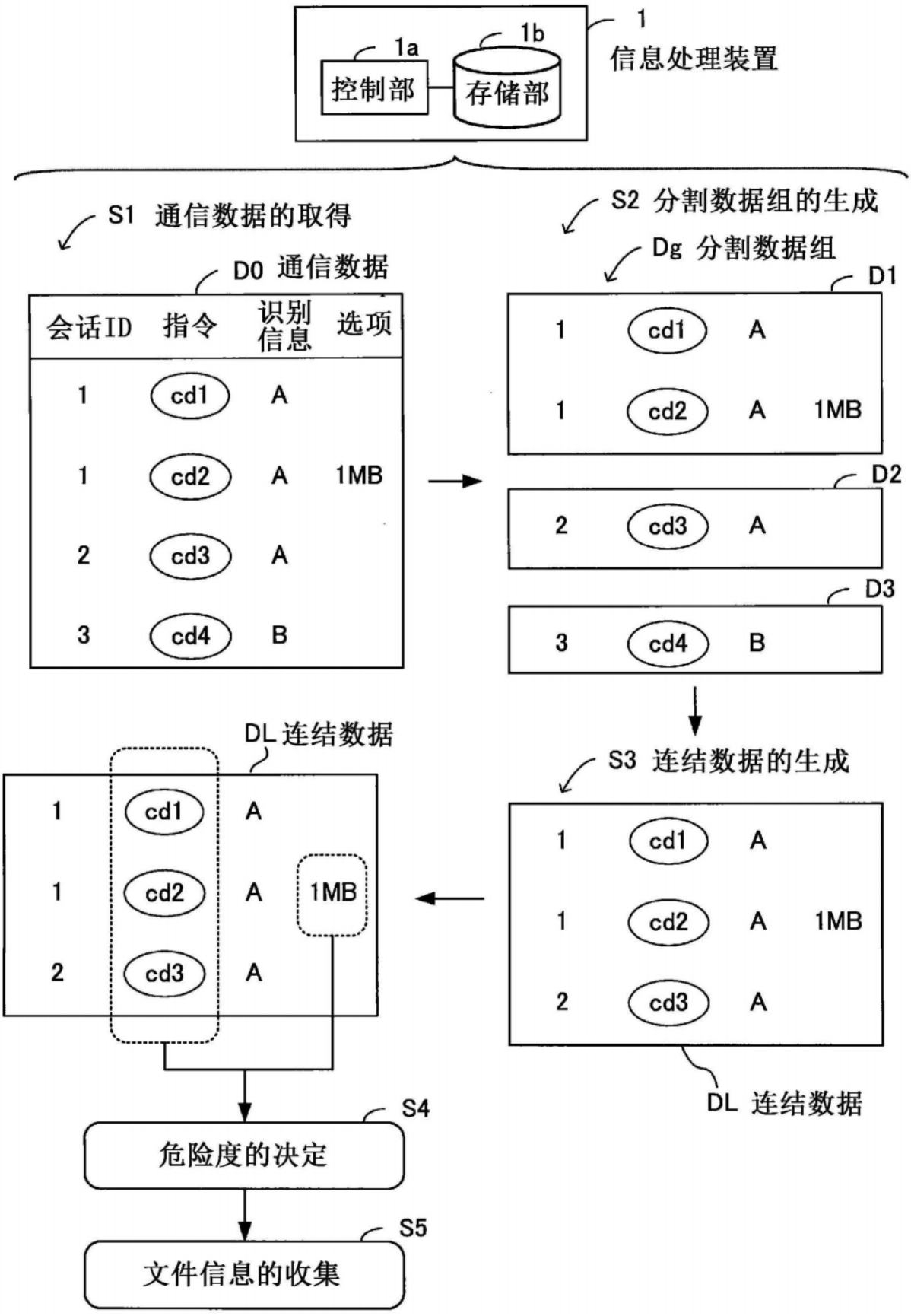

1
信息处理装置
1a
控制部
1b
存储部
S1 通信数据的取得
D0 通信数据
会话ID 指令 识别信息 选项
1 cd1 A
1 cd2 A 1MB
2 cd3 A
3 cd4 B
S2 分割数据组的生成
Dg 分割数据组
D1
1 cd1 A
1 cd2 A 1MB
D2
2 cd3 A
D3
3 cd4 B
S3 连结数据的生成
DL 连结数据
1 cd1 A
1 cd2 A 1MB
2 cd3 A
DL 连结数据
S4
危险度的决定
S5
文件信息的收集

图1

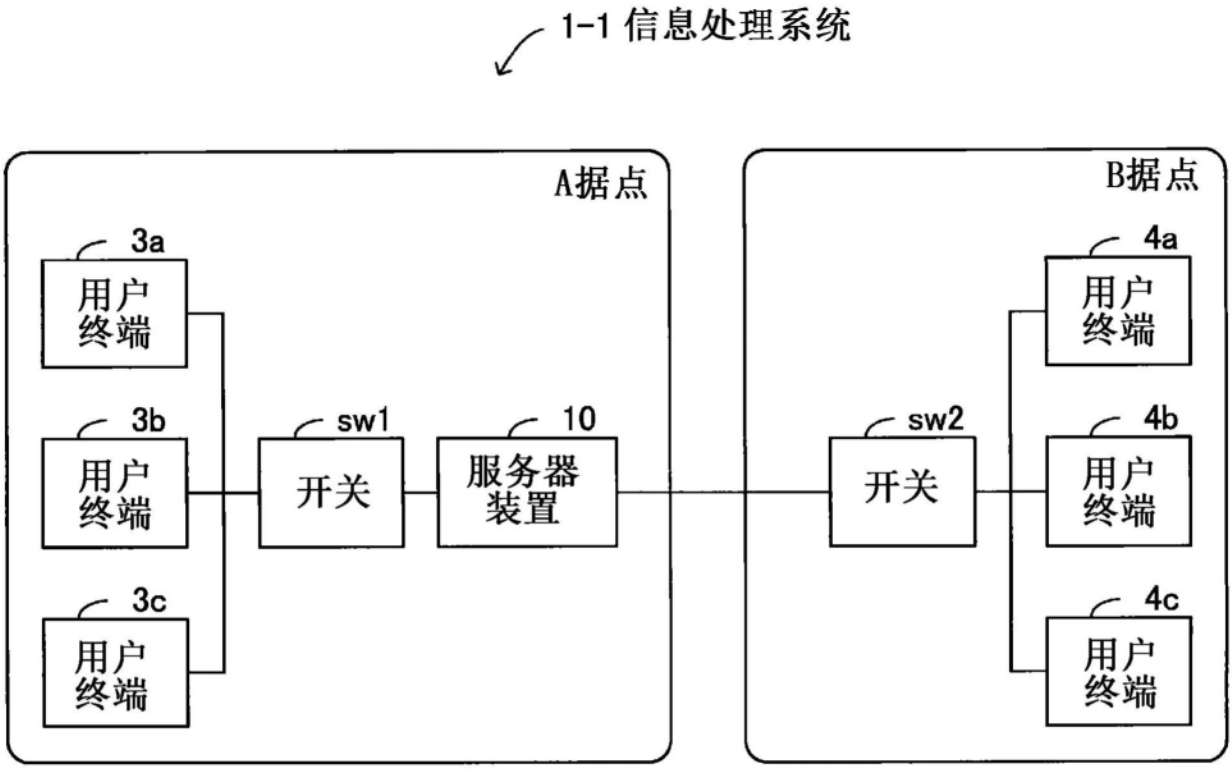

1-1 信息处理系统
A据点
B据点
3a
用户终端
3b
用户终端
3c
用户终端
sw1
开关
10
服务器装置
sw2
开关
4a
用户终端
4b
用户终端
4c
用户终端

图2

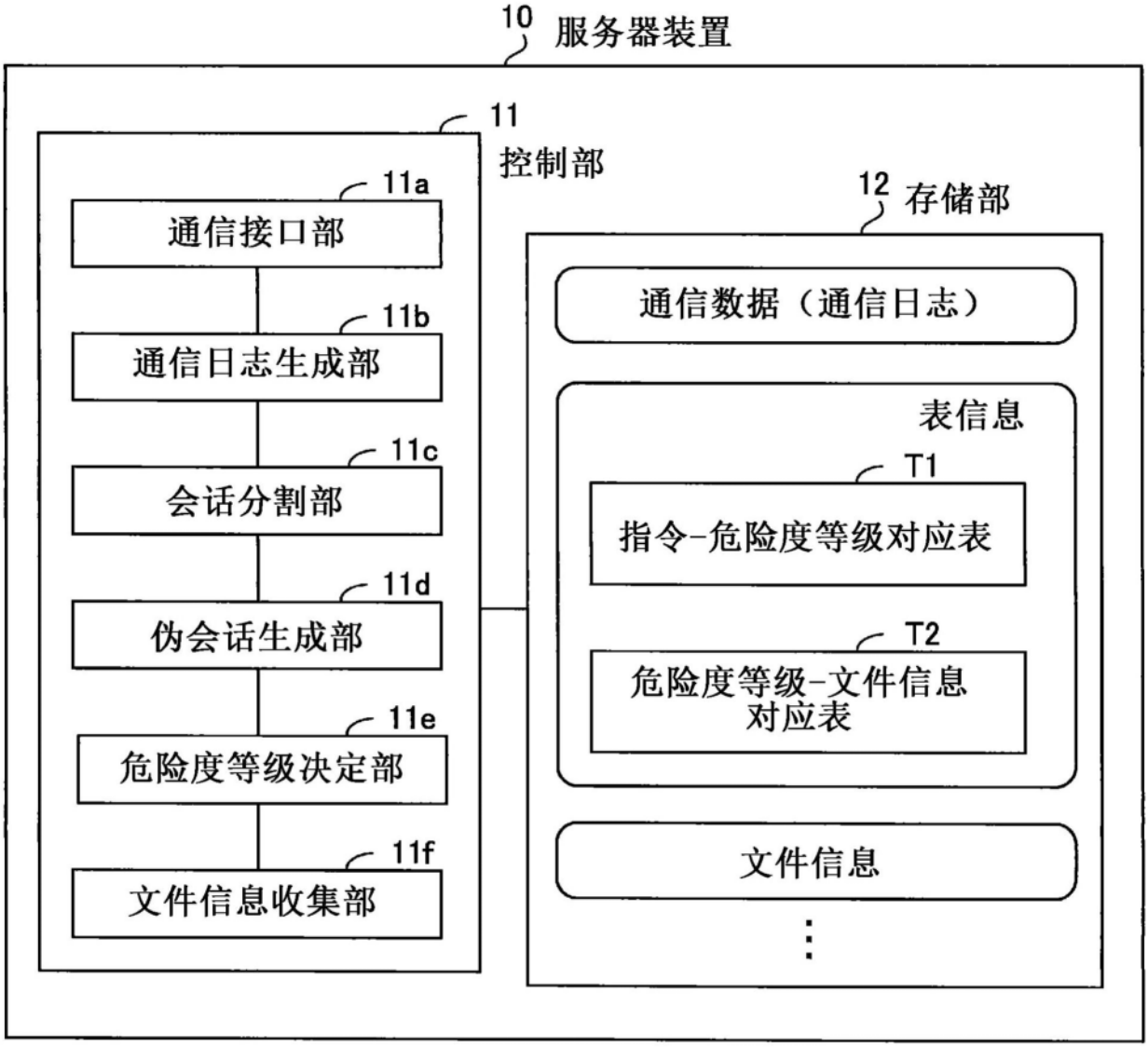

10
服务器装置
11
控制部
11a
通信接口部
11b
通信日志生成部
11c
会话分割部
11d
伪会话生成部
11e
危险度等级决定部
11f
文件信息收集部
12
存储部
通信数据（通信日志）
表信息
T1
指令-危险度等级对应表
T2
危险度等级-文件信息
对应表
文件信息

图3

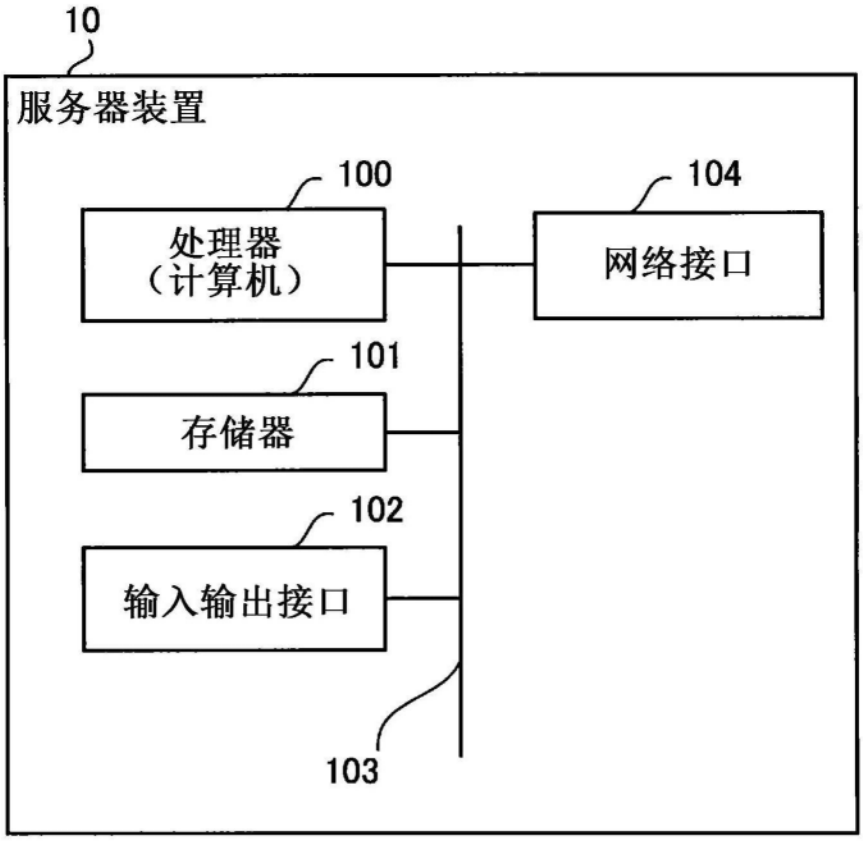


图4

T11

指令	危险度等级
net group	1
net use	2
schtasks	3

图5

T12

危险度等级	文件信息
1	元信息
2	元信息/文件散列值
3	元信息/文件散列值/文件主体

图6

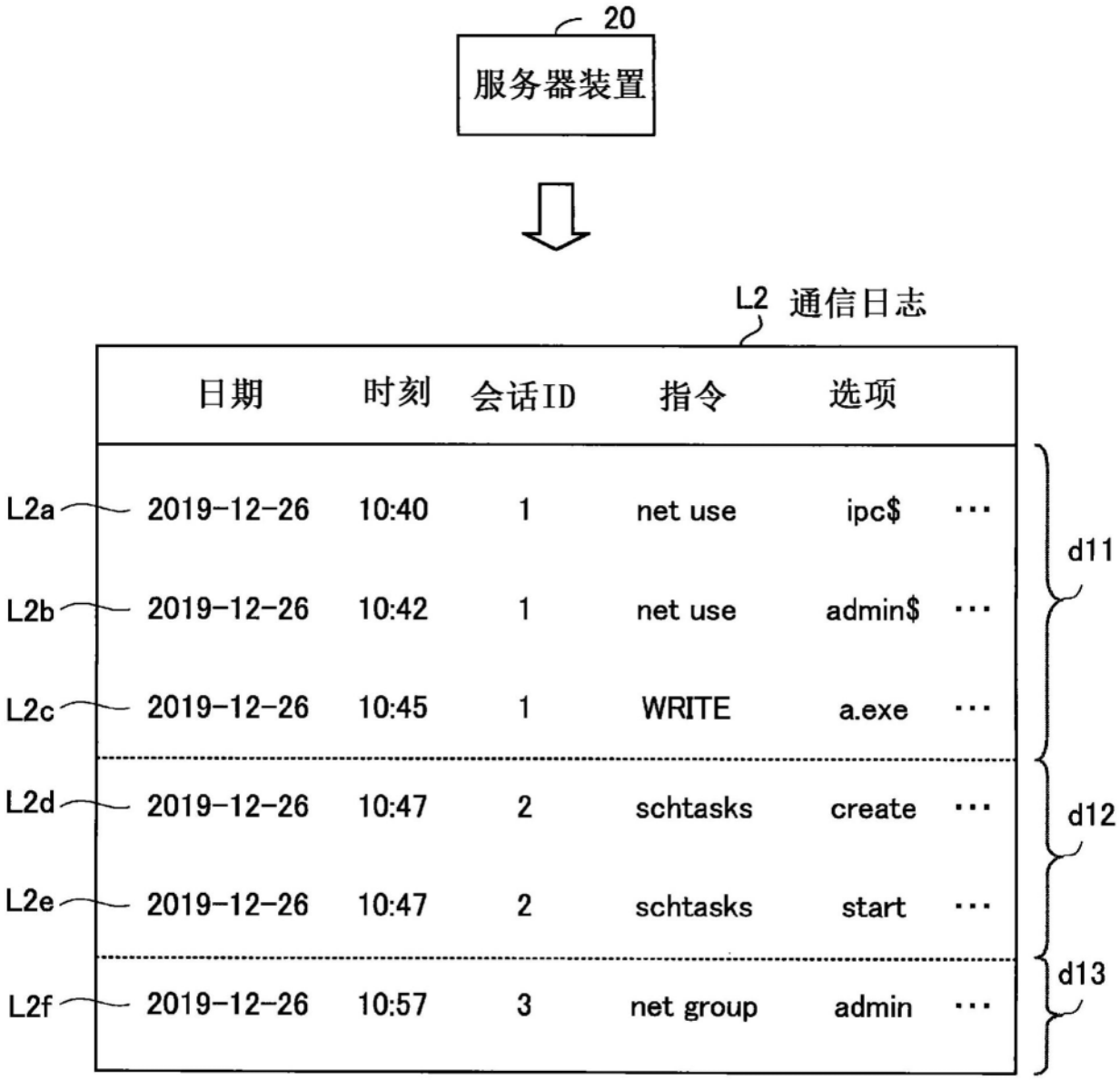

20
服务器装置
L2 通信日志
日期 时刻 会话ID 指令 选项
L2a 2019-12-26 10:40 1 net use ipc$ ···
L2b 2019-12-26 10:42 1 net use admin$ ···
L2c 2019-12-26 10:45 1 WRITE a.exe ···
L2d 2019-12-26 10:47 2 schtasks create ···
L2e 2019-12-26 10:47 2 schtasks start ···
L2f 2019-12-26 10:57 3 net group admin ···
d11
d12
d13

图7

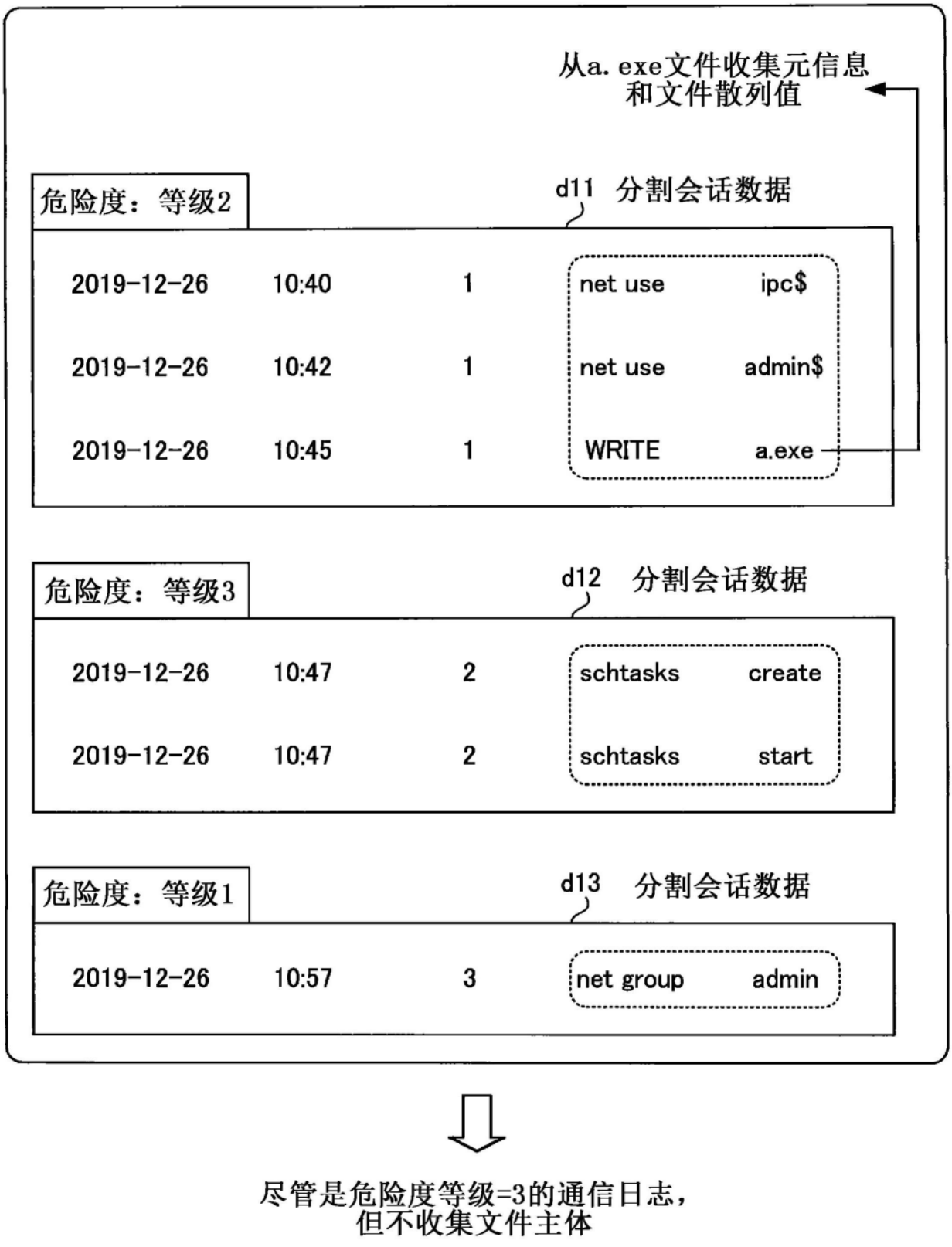

从a. exe文件收集元信息
和文件散列值
危险度：等级2
d11 分割会话数据
2019-12-26 10:40 1 net use ipc$
2019-12-26 10:42 1 net use admin$
2019-12-26 10:45 1 WRITE a.exe
危险度：等级3
d12 分割会话数据
2019-12-26 10:47 2 schtasks create
2019-12-26 10:47 2 schtasks start
危险度：等级1
d13 分割会话数据
2019-12-26 10:57 3 net group admin
尽管是危险度等级=3的通信日志，
但不收集文件主体

图8

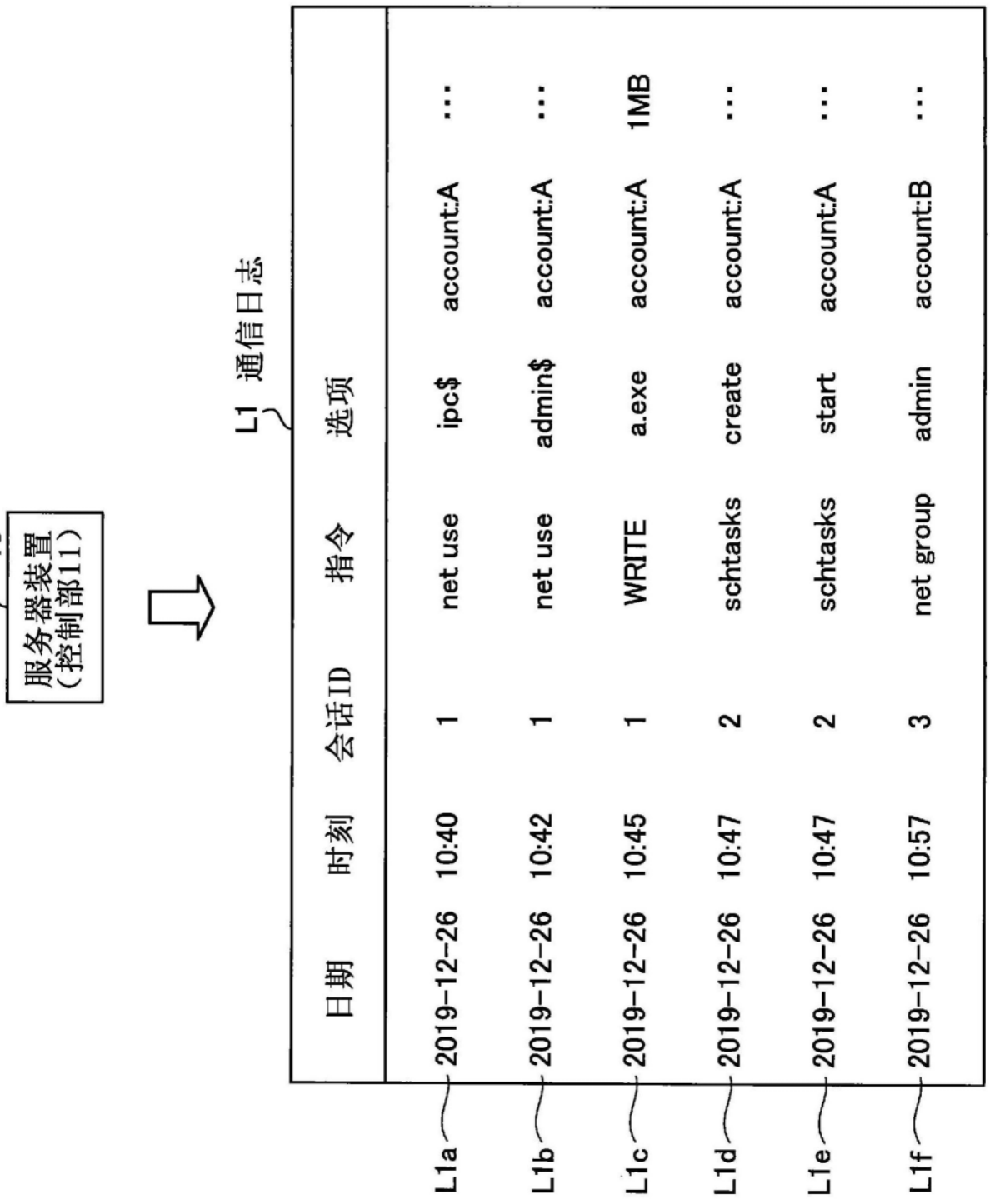

10
服务器装置
(控制部11)
L1 通信日志
日期 时刻 会话ID 指令 选项
L1a 2019-12-26 10:40 1 net use ipc$ account:A ...
L1b 2019-12-26 10:42 1 net use admin$ account:A ...
L1c 2019-12-26 10:45 1 WRITE a.exe account:A 1MB
L1d 2019-12-26 10:47 2 schtasks create account:A ...
L1e 2019-12-26 10:47 2 schtasks start account:A ...
L1f 2019-12-26 10:57 3 net group admin account:B ...

图9

d1 分割会话数据

10:40	1	net use	ipc$	account:A	···
10:42	1	net use	admin$	account:A	···
10:45	1	WRITE	a.exe	account:A	1MB

d2 分割会话数据

10:47	2	schtasks	create	account:A	···
10:47	2	schtasks	start	account:A	···

d3 分割会话数据

10:57	3	net group	admin	account:B	···

图10

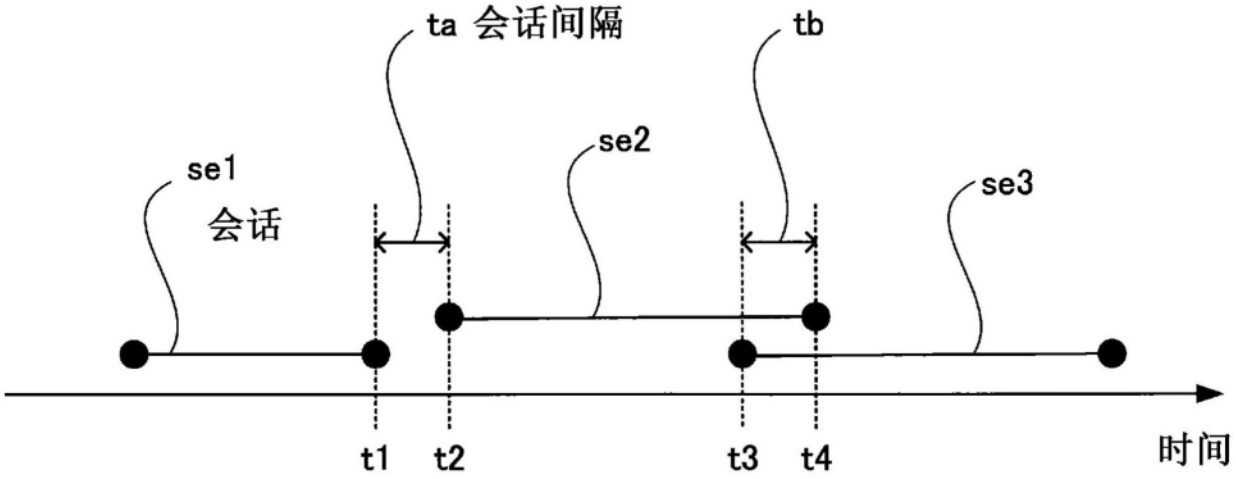

ta 会话间隔
tb
se1
会话
se2
se3
t1
t2
t3
t4
时间

图11

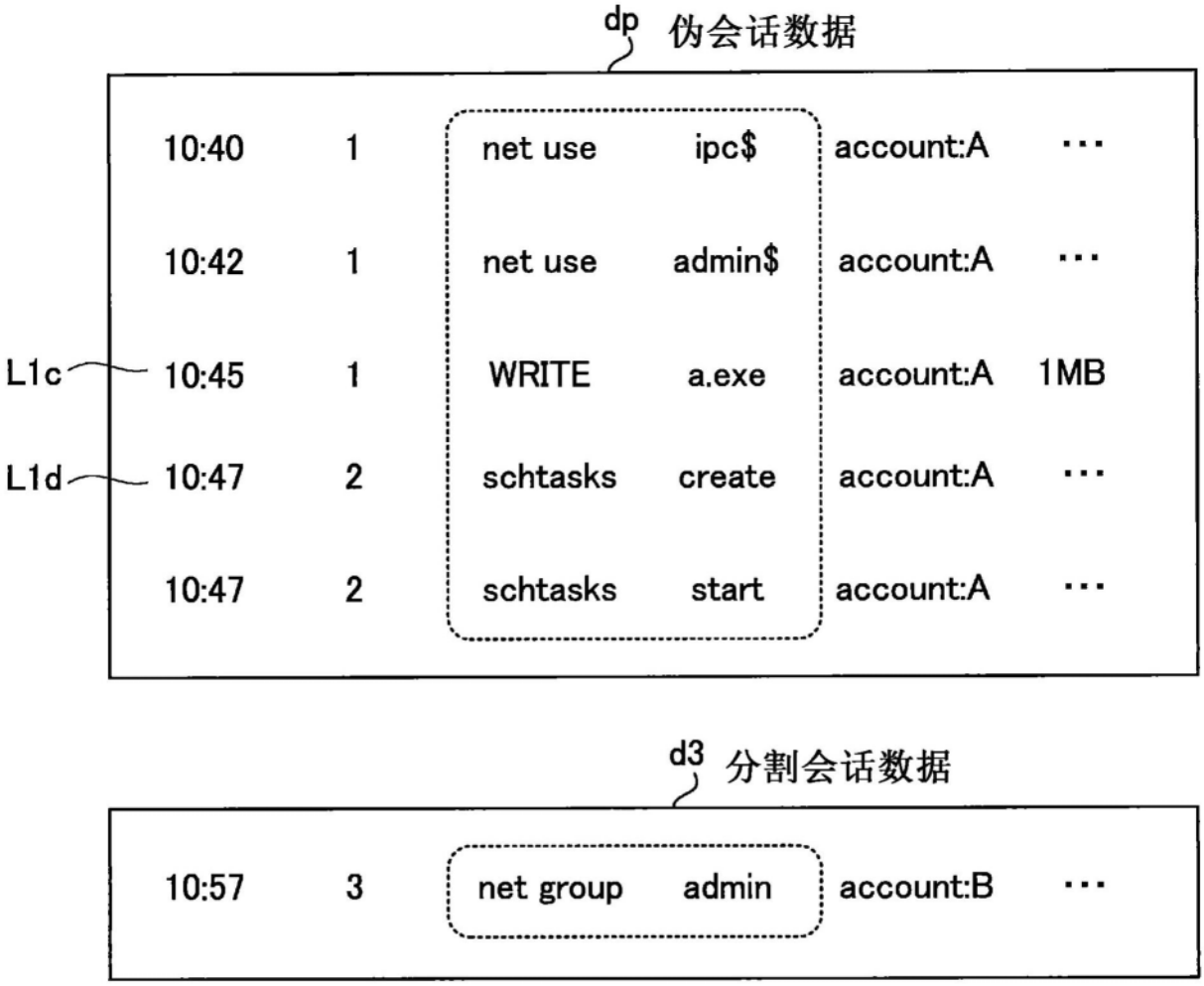

dp 伪会话数据
10:40 1 net use ipc$ account:A ···
10:42 1 net use admin$ account:A ···
L1c
10:45 1 WRITE a.exe account:A 1MB
L1d
10:47 2 schtasks create account:A ···
10:47 2 schtasks start account:A ···
d3 分割会话数据
10:57 3 net group admin account:B ···

图12

T1 指令-危险度等级对应表

指令	危险度等级
net group	1
net use	2
schtasks （文件大小为阈值以上）	
schtasks （文件大小小于阈值）	3

图13

T2 危险度等级-文件信息对应表

危险度等级	文件信息
1	元信息
2	元信息/文件散列值
3	元信息/文件散列值/文件主体

图14

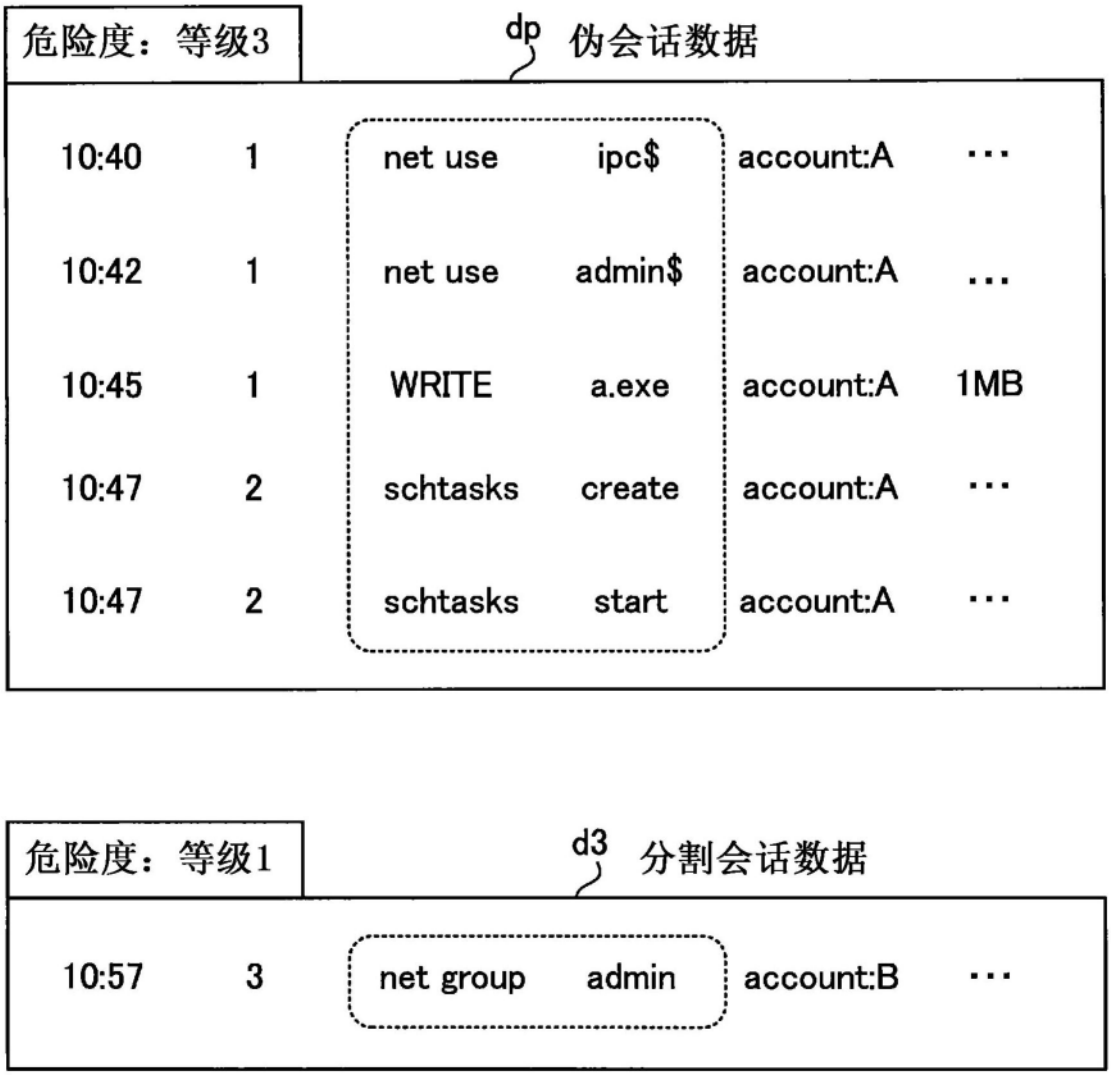

危险度：等级3
dp
伪会话数据
10:40 1 net use ipc$ account:A ···
10:42 1 net use admin$ account:A ···
10:45 1 WRITE a.exe account:A 1MB
10:47 2 schtasks create account:A ···
10:47 2 schtasks start account:A ···
危险度：等级1
d3
分割会话数据
10:57 3 net group admin account:B ···

图15

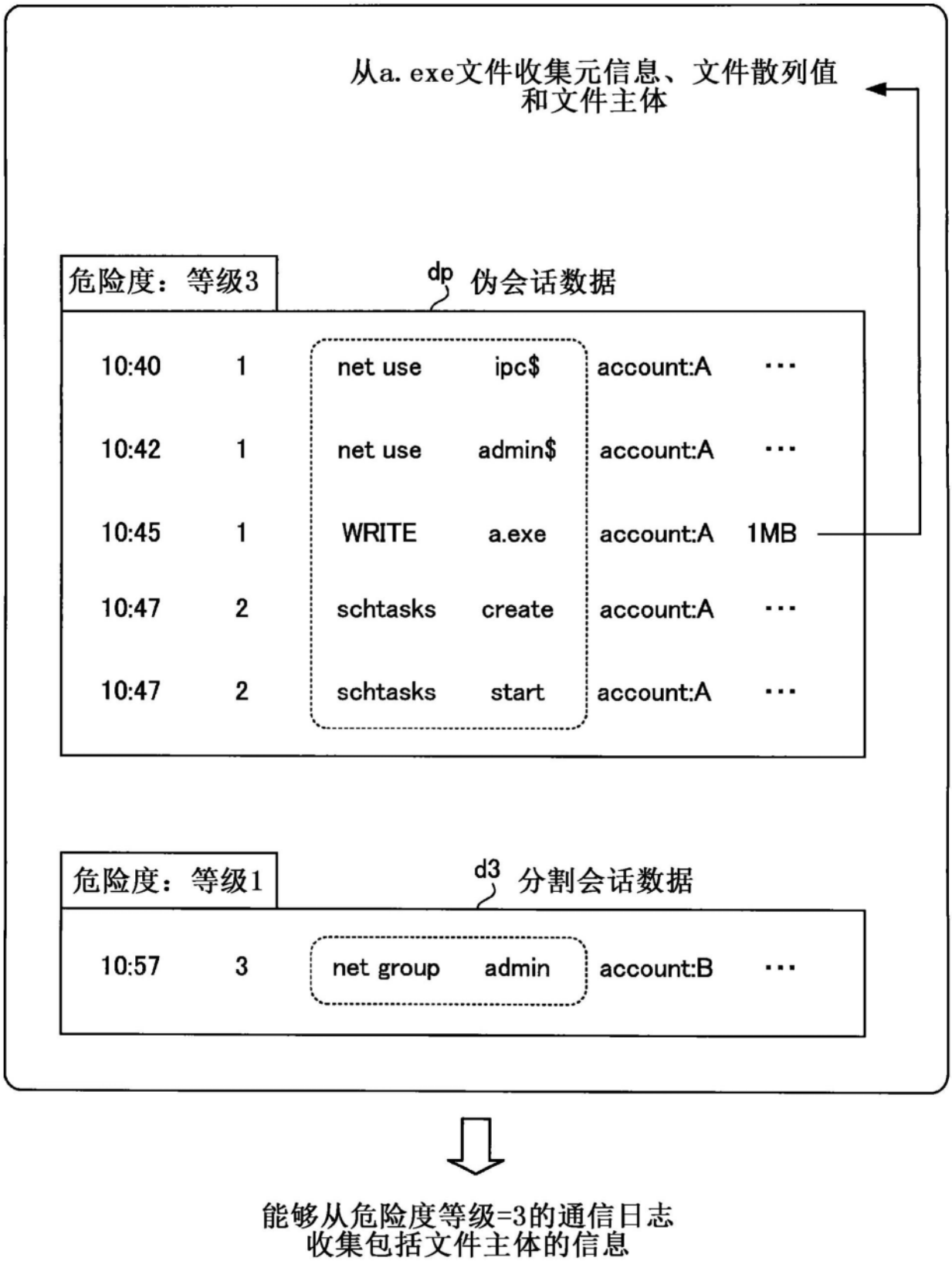

从a. exe文件收集元信息、文件散列值
和文件主体
危险度：等级3
dp 伪会话数据
10:40 1 net use ipc$ account:A ···
10:42 1 net use admin$ account:A ···
10:45 1 WRITE a.exe account:A 1MB
10:47 2 schtasks create account:A ···
10:47 2 schtasks start account:A ···
危险度：等级1
d3 分割会话数据
10:57 3 net group admin account:B ···
能够从危险度等级=3的通信日志
收集包括文件主体的信息

图16

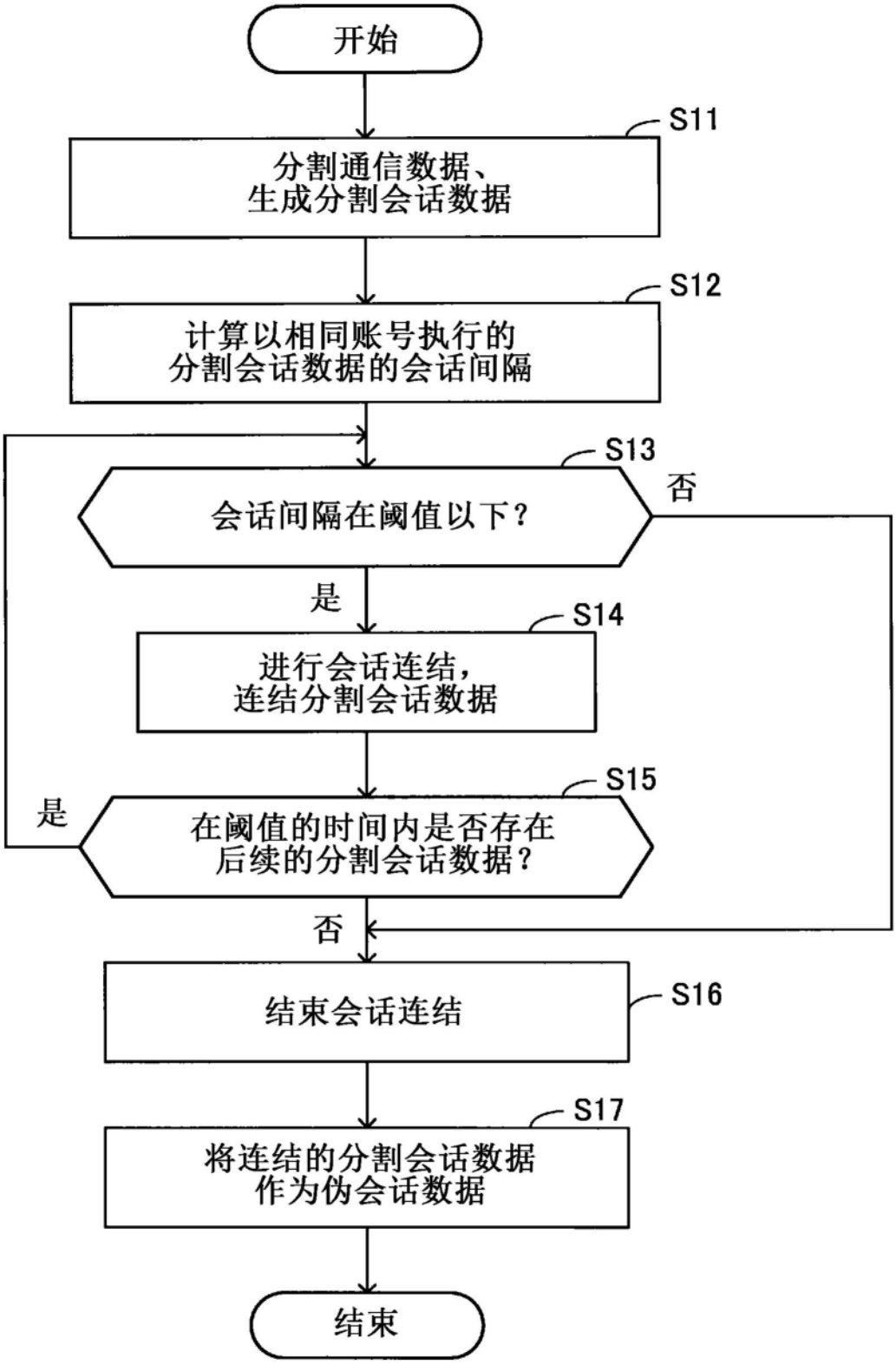

开始
S11
分割通信数据、
生成分割会话数据
S12
计算以相同账号执行的
分割会话数据的会话间隔
S13
会话间隔在阈值以下？
否
是
S14
进行会话连结，
连结分割会话数据
S15
是
在阈值的时间内是否存在
后续的分割会话数据？
否
结束会话连结
S16
S17
将连结的分割会话数据
作为伪会话数据
结束

图17

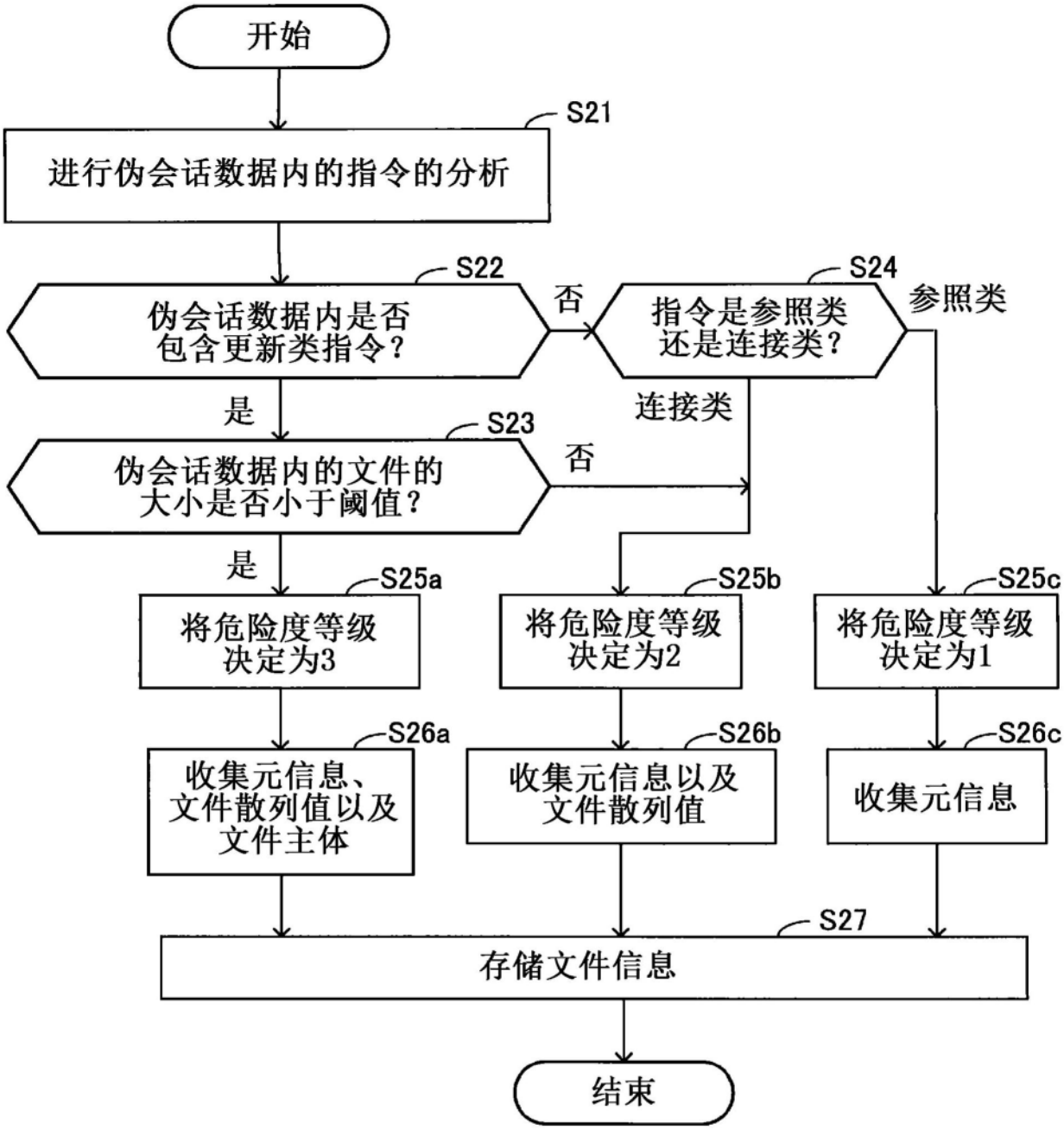

开始
S21
进行伪会话数据内的指令的分析
S22
伪会话数据内是否包含更新类指令？
否
S24
指令是参照类还是连接类？
参照类
是
连接类
S23
伪会话数据内的文件的大小是否小于阈值？
否
是
S25a
将危险度等级决定为3
S25b
将危险度等级决定为2
S25c
将危险度等级决定为1
S26a
收集元信息、文件散列值以及文件主体
S26b
收集元信息以及文件散列值
S26c
收集元信息
S27
存储文件信息
结束

图18

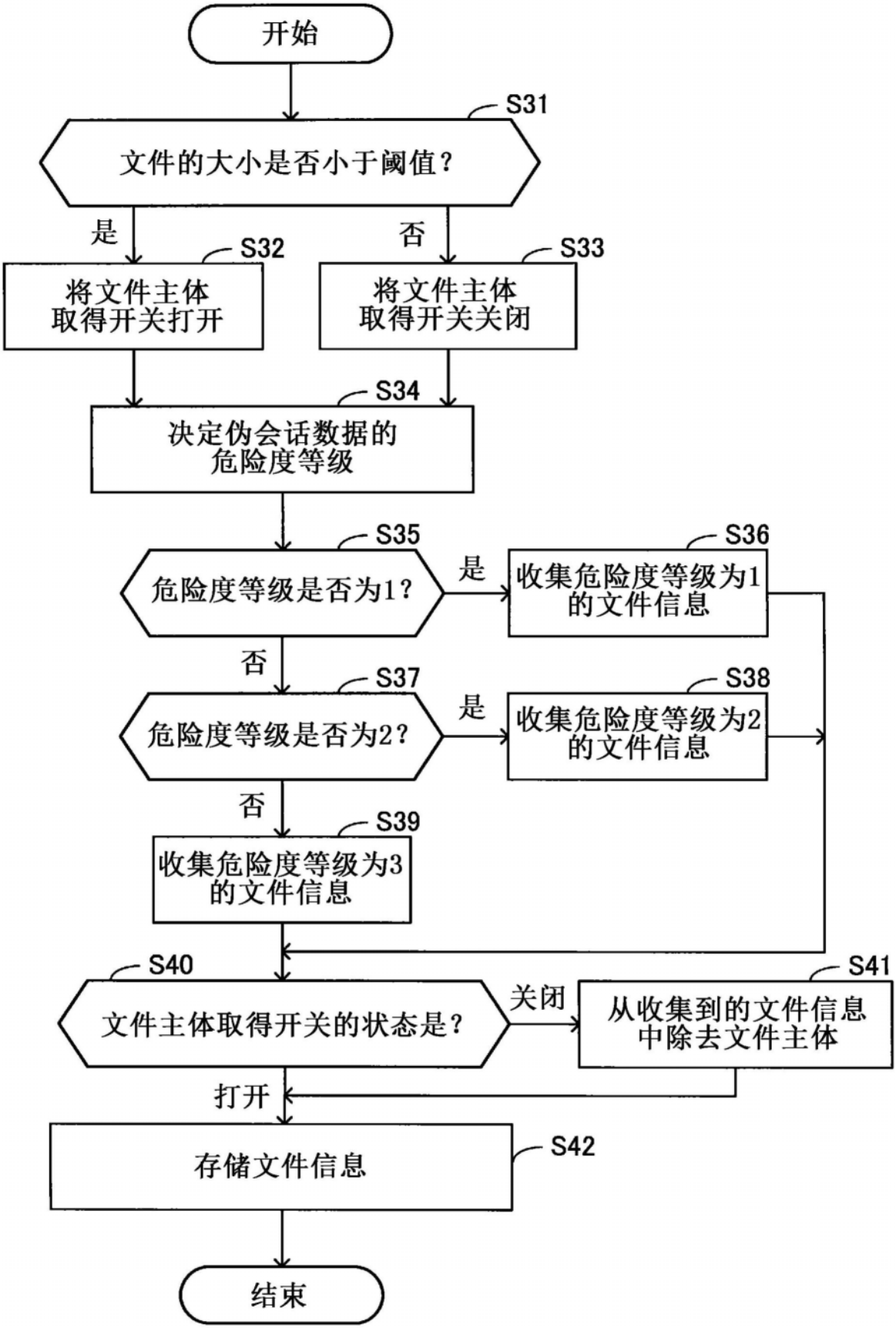

开始
S31
文件的大小是否小于阈值？
是
否
S32
将文件主体
取得开关打开
S33
将文件主体
取得开关关闭
S34
决定伪会话数据的
危险度等级
S35
危险度等级是否为1？
是
S36
收集危险度等级为1
的文件信息
否
S37
危险度等级是否为2？
是
S38
收集危险度等级为2
的文件信息
否
S39
收集危险度等级为3
的文件信息
S40
文件主体取得开关的状态是？
关闭
S41
从收集到的文件信息
中除去文件主体
打开
存储文件信息
S42
结束

图19