(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 102132521 B
(45)授权公告日 2014.09.24

(21)申请号 201080002410.X
(22)申请日 2010.06.23
(30)优先权数据
2009-154959 2009.06.30 JP
(85)PCT国际申请进入国家阶段日
2011.02.23
(86)PCT国际申请的申请数据
PCT/JP2010/004169 2010.06.23
(87)PCT国际申请的公布数据
WO2011/001630 JA 2011.01.06
(73)专利权人 松下电器产业株式会社
地址 日本大阪府
(72)发明人 山口胜久 野村和博
(74)专利代理机构 永新专利商标代理有限公司 72002
代理人 王成坤 胡建新
(51)Int.Cl.
H04L 9/08(2006.01)
(56)对比文件
CN 101188731 A,2008.05.28,
CN 101227204 A,2008.07.23,
CN 1780468 A,2006.05.31,
审查员 汪辉

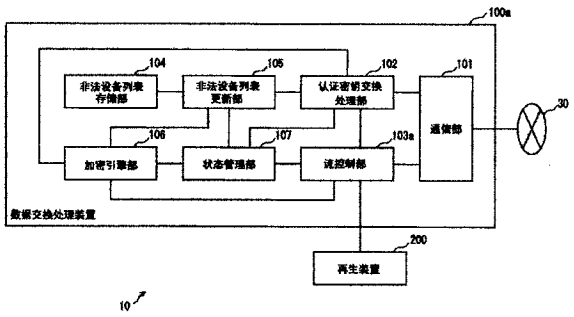
权利要求书2页 说明书16页 附图10页

(54)发明名称

数据交换处理装置及数据交换处理方法

(57)摘要

本发明的数据交换处理装置其特征为，具备：加密引擎部，进行加密处理及验证处理；流控制机构，利用上述加密引擎部进行内容的加密处理，并输出内容；非法设备列表更新机构，利用上述加密引擎部进行非法设备列表的验证处理；状态管理机构，使用与上述内容有关的元信息和由上述流控制机构得到的处理位置，检测到相比其他区间上述加密引擎部的加密处理的负荷小的区间时，向上述非法设备列表更新机构输出许可通知；上述非法设备列表更新机构从上述状态管理机构接收到上述许可通知时，开始利用了上述加密引擎部的非法设备列表的验证处理。



CN 102132521 B

1. 一种数据交换处理装置，利用非法设备列表来清除非法的设备，并收发内容，其特征为，

具备：

加密引擎部，进行加密处理及验证处理；

流控制机构，利用上述加密引擎部进行内容的加密处理，并输出内容；

非法设备列表更新机构，利用上述加密引擎部进行非法设备列表的验证处理；

元信息取得机构，对于构成上述内容的多个部分内容分别取得表示上述内容中的位置和加密处理的负荷的元信息；以及

状态管理机构，以规定的时间间隔，从上述流控制机构取得该流控制机构正在处理的上述内容的位置，在上述流控制机构接下来处理的部分内容是由上述元信息表示的加密处理的负荷少的部分内容的情况下，向上述非法设备列表更新机构输出许可通知；

当从上述状态管理机构接收到上述许可通知时，上述非法设备列表更新机构开始利用了上述加密引擎部进行的非法设备列表的验证处理。

2. 如权利要求 1 所述的数据交换处理装置，其特征为，

上述元信息包含复制控制信息，该复制控制信息表示对于构成上述内容的多个部分内容有无著作权保护，

在上述流控制机构接下来处理的部分内容是不需要著作权保护的部分内容的情况下，上述状态管理机构向上述非法设备列表更新机构输出许可通知。

3. 如权利要求 1 所述的数据交换处理装置，其特征为，

上述元信息包含关于构成上述内容的多个部分内容的区间信息，

在上述流控制机构接下来处理的部分内容不存在的情况下，上述状态管理机构向上述非法设备列表更新机构输出许可通知。

4. 如权利要求 1 所述的数据交换处理装置，其特征为，

上述状态管理机构，

在未由上述流控制机构使用上述加密引擎部的情况下，向上述非法设备列表更新机构输出上述许可通知，

当受理了上述流控制机构对上述加密引擎部的使用请求时，使上述非法设备列表更新机构对上述加密引擎部的使用中断，使上述流控制机构进行的处理优先。

5. 如权利要求 1 所述的数据交换处理装置，其特征为，

上述数据交换处理装置具备保持非法设备列表的保持机构；

上述非法设备列表更新机构，包括：

判断部，根据从其他的数据交换处理装置所取得的由该其他的数据交换处理装置当前保持的非法设备列表的版本信息及世代信息，来判断是否更新由上述保持机构保持的上述非法设备列表；

取得部，在判断为进行更新的情况下，从上述其他的数据交换处理装置取得更新用的非法设备列表；

验证部，当从上述状态管理机构接收到上述许可通知时，委托利用上述加密引擎部来判断上述更新用的非法设备列表的合法性的上述验证处理；以及

更新部，当认定了上述更新用的非法设备列表的合法性时，将保持在上述保持机构中

的上述非法设备列表，置换为上述更新用的非法设备列表。

6. 一种在数据交换处理装置中使用的数据交换处理方法，该数据交换处理装置利用非法设备列表来清除非法的设备并收发内容，其特征为，

上述数据交换处理装置，具备：

加密引擎部，进行加密处理及验证处理；

上述数据交换处理方法，具备：

元信息取得步骤，对于构成内容的多个部分内容分别取得表示上述内容中的位置和加密处理的负荷的元信息；

流控制步骤，利用上述加密引擎部进行内容的加密处理，并输出内容；

状态管理步骤，以规定的时间间隔，取得在上述流控制步骤正在处理的上述内容的位置，在上述流控制步骤中接下来处理的部分内容是由上述元信息表示的加密处理的负荷少的部分内容的情况下，输出许可通知；以及

非法设备列表更新步骤，在从上述状态管理步骤接收到上述许可通知时，开始利用了上述加密引擎部进行的非法设备列表的验证处理。

数据交换处理装置及数据交换处理方法

技术领域

[0001] 本发明涉及在设备间交换数字设备具有的非法设备列表的技术。

背景技术

[0002] 近年来，正在实现通过网络连接家庭内的数字设备，在设备间共享各种数字内容（下面记述为“内容”。）的家庭内网络。

[0003] 在另一方面，在内容之中，还包括新创作的电影或付费广播的电视节目等需要著作权保护的内容。作为著作权保护的有力方法，一般实施将内容加密后在网络上进行传输的方法。该技术已经按照 DTCP-IP(DigitalTransmission Content Protection over Internet Protocol/ 因特网上的数字传输内容保护）进行了标准化。

[0004] DTCP-IP 具备 AKE(Authentication and Key Exchange/ 认证密钥交换）认证密钥交换功能及密钥无效化功能。因此，可以保证接收对象的数字设备安全地接收内容，并且防止由此外的设备做出的内容盗用。

[0005] 另外，在 DTCP 中，为了实现更为安全的著作权保护，规定了通过由各数字设备保持已登录非法设备的列表（下面记述为“非法设备列表”。），来抑制由非法的设备收发内容的技术。

[0006] 非法设备列表被从 DTLA(Digital Transmission Licensing Administrator/ 数字传输许可管理员），发放给各数字设备。由于若新发现了非法设备，则 DTLA 更新非法设备列表，因而新制造出的数字设备有时已经保持更新后的新的非法设备列表。

[0007] 因此，各数字设备当进行内容的收发时，相互交换由本机保持着的非法设备列表的信息，从保持着较新的非法设备列表的数字设备，接收该新的非法设备列表，更新由本机保持的旧的非法设备列表。

[0008] 作为进行非法设备列表的收发之技术，在专利文献 1 中公示出，一种利用拓扑连接信息，将拓扑整体的非法设备列表总是更新为最新的信息的技术。

[0009] 先行技术文献

[0010] 专利文献 1 ：日本特开 2004-96637 号公报

发明内容

[0011] 发明的概要

[0012] 发明要解决的课题

[0013] 但是，以往的数字设备若在流处理中还取得了新的非法设备列表，则开始非法设备列表的更新处理。

[0014] 由于流处理和非法设备列表更新处理使用一个加密引擎部，并进行处理，因而若在流处理中开始了非法设备列表更新处理，则在再现侧的设备中再现处理变慢，存在使再现品质下降这样的问题。具体而言，给用户带来“被迫等待再现”这样的印象。

[0015] 本发明是鉴于上述的问题所在而做出的，其目的为，提供通过控制非法设备列表

的更新定时，而在不妨碍流处理的状况下进行非法设备列表的更新处理的数据交换处理装置及数据交换处理方法。

[0016] 解决课题的手段

[0017] 为了达到上述目的，本发明是一种数据交换处理装置，使用非法设备列表来清除非法的设备，并收发内容，其特征为，具备：加密引擎部，进行加密处理及验证处理；流控制机构，利用上述加密引擎部进行内容的加密处理，并输出内容；非法设备列表更新机构，利用上述加密引擎部进行非法设备列表的验证处理；以及状态管理机构，当利用与上述内容有关的元信息和由上述流控制机构得到的处理位置，检测到相比其他区间上述加密引擎部的加密处理的负荷小的区间时，向上述非法设备列表更新机构输出许可通知；当从上述状态管理机构接收到上述许可通知时，上述非法设备列表更新机构开始利用了上述加密引擎部进行的非法设备列表的验证处理。

[0018] 发明效果

[0019] 本发明由于具备上述的结构，因而把加密引擎部的加密处理的负荷小的区间作为目的来开始非法设备列表的验证处理，因此，即便在流处理中发生了非法设备列表的更新处理时，也可以在不妨碍流处理的状况下，保证较高的再现品质。

附图说明

[0020] 图 1 是表示网络 1 结构的附图。

[0021] 图 2 是表示客户机装置 10 结构的功能框图。

[0022] 图 3 是表示非法设备列表格式的附图。

[0023] 图 4 是表示加密引擎部 107 结构的附图。

[0024] 图 5 是表示硬件资源管理信息具体例的附图。

[0025] 图 6 是表示非法设备列表更新部 105 动作的流程图。

[0026] 图 7 是表示状态管理部 107 动作的流程图。

[0027] 图 8 是流控制部 103a、非法设备列表更新部 105 及状态管理部 107 的状态转移图。

[0028] 图 9 是表示元信息具体例的附图。

[0029] 图 10 是表示元信息进展信息具体例的附图。

[0030] 图 11 是表示服务器装置 20 结构的功能框图。

[0031] 图 12 是使用具体例来说明由客户机装置 10 及服务器装置 20 做出的流处理及非法设备列表更新处理的时序图，下接图 13。

[0032] 图 13 是使用具体例来说明由客户机装置 10 及服务器装置 20 做出的流处理及非法设备列表更新处理的时序图，上接图 12。

具体实施方式

[0033] 作为本发明第 1 方式的数据交换处理装置使用非法设备列表来清除非法的设备，并收发内容，其特征为，具备：加密引擎部，进行加密处理及验证处理；流控制机构，利用上述加密引擎部进行内容的加密处理，并输出内容；非法设备列表更新机构，利用上述加密引擎部进行非法设备列表的验证处理；以及状态管理机构，当利用与上述内容有关的元信息和由上述流控制机构得到的处理位置，检测到相比其他区间上述加密引擎部的加密处理的

负载小的区间时，对上述非法设备列表更新机构输出许可通知；上述非法设备列表更新机构从上述状态管理机构接收到上述许可通知时，开始利用了上述加密引擎部的非法设备列表的验证处理。

[0034] 这里，在本发明的数据交换处理装置具备在接收加密内容的客户机装置中时，由上述加密引擎部进行的加密处理是指加密内容的解密处理。在另一方面，在本发明的数据交换处理装置具备到发送加密内容的服务器装置中时，由上述加密引擎部进行的加密处理是指内容的加密处理。

[0035] 在作为本发明第 2 方式的数据交换处理装置中其特征为，上述元信息包含复制控制信息，该复制控制信息表示对于构成上述内容的多个部分内容有无著作权保护；当利用上述复制控制信息和由上述流控制机构得到的处理位置，上述状态管理机构检测到不需要著作权保护的部分内容作为相比其他区间上述加密引擎部的加密处理的负载小的区间时，向上述非法设备列表更新机构输出许可通知。

[0036] 这里，被著作权保护的部分内容需要在服务器装置侧进行加密，在客户机装置侧进行解密。也就是说，需要由加密引擎部做出的加密处理。在另一方面，不需要著作权保护的部分内容不需要在服务器装置侧进行加密，也不需要在客户机装置侧进行解密。也就是说，不需要由加密引擎部做出的加密处理。

[0037] 因此，通过在流控制机构不使用加密引擎部时，使之执行非法设备列表的验证处理，即便在流处理中发生非法设备列表的更新处理时，也可以在不妨碍流处理的状况下，保证较高的再现品质，并进行非法设备列表的更新处理。

[0038] 还有，所谓的“流处理”在服务器装置的场合，是指将部分内容依次加密而发送给客户机装置的处理，在客户机装置的场合，是指依次接收部分内容，进行解密并再现的处理。

[0039] 在作为本发明第 3 方式的数据交换处理装置中其特征为，上述元信息包含有关构成上述内容的多个部分内容的区间信息，当利用上述区间信息和由上述流控制机构得到的处理位置，上述状态管理机构检测到上述内容的结束时刻作为相比其他区间上述加密引擎部的加密处理的负载小的区间时，向上述非法设备列表更新机构输出许可通知。

[0040] 这里，上述区间信息是表示各部分内容中包含的数据的数据量、帧数或者各部分内容的处理时间、再现时间等的信息。因此，只要使用上述区间信息和上述处理位置，就可以识别流处理的结束时刻。

[0041] 因此，由于只要在由流控制机构做出的最后部分内容的处理结束时对非法设备列表更新机构通知使用许可，就可以在流控制机构不使用加密引擎部时，使之执行非法设备列表的验证处理，因而可以在不妨碍流处理的状况下，保证较高的再现品质，并进行非法设备列表的更新处理。

[0042] 在作为本发明第 4 方式的数据交换处理装置中其特征为，上述状态管理机构在未由上述流控制机构使用上述加密引擎部时，对上述非法设备列表更新机构输出上述许可通知，在受理了上述流控制机构对上述加密引擎部的使用请求时，使上述非法设备列表更新机构做出的上述加密引擎部的使用中断，使由上述流控制机构做出的处理优先。

[0043] 根据该结构，由于使流控制机构优先使用加密引擎部，因而可以在不妨碍流处理的状况下，保证较高的再现品质，并进行非法设备列表的更新处理。

[0044] 作为本发明第 5 方式的数据交换处理装置其特征为，具备保持非法设备列表的保持机构；上述非法设备列表更新机构包括：判断部，根据从其他的数据交换处理装置所取得的由该其他的数据交换处理装置当前保持的非法设备列表的版本信息及世代信息，来判断是否更新由上述保持机构保持的上述非法设备列表；取得部，在判断为进行更新的情况下，从上述其他的数据交换处理装置取得更新用的非法设备列表；验证部，当从上述状态管理机构接收到上述许可通知时，委托利用上述加密引擎部来判断上述更新用非法设备列表的合法性的上述验证处理；更新部，当认定了上述更新用非法设备列表的合法性时，将保持在上述保持机构中的上述非法设备列表，置换为上述更新用的非法设备列表。

[0045] 根据该结构，由于使用版本信息及世代信息来判断非法设备列表的新旧，因而能够导入版本及世代都新的非法设备列表。

[0046] 另外，通过取得对方装置的世代信息，就能够按照由非易失性存储器构成的上述保持机构的大小，来变换非法设备列表的大小。借此，可以降低作为非法设备列表传输通路的网络频带的负荷，使非法设备列表的收发进一步高效化。另外，还可以降低非法设备列表更新处理占用的 CPU 处理时间。

[0047] 在下面，对于本发明的实施方式一边参照附图一边进行说明。

[0048] < 系统的概要 >

[0049] 图 1 是表示本发明实施方式中的网络系统 1 结构的附图。如同图所示，网络系统 1 包括多个客户机装置 10、11、…、12 和多个服务器装置 20、21、…、22，来构成。各客户机装置及各服务器装置是具有通信功能的装置，能够通过网络 30 相互连接。

[0050] 各服务器装置保持着 1 个以上的内容。各客户机装置若对服务器装置，请求了内容的取得，则服务器装置对所请求的内容进行流发送，客户机装置对内容进行流再现。

[0051] 作为各客户机装置及各服务器装置的具体例，是电视机、影像再现机、录像设备等的 AV 家电设备、个人计算机、工作站等的信息处理装置以及数字摄像机、视频摄像机、移动电话机、移动影像再现机等的移动信息终端。

[0052] 网络 30 使用有线线路、无线线路、IEEE1394、USB 或者它们的组合。通信协议使用 TCP、RTP、HTTP 及 FTP 等。在各客户机装置及各服务器装置中，作为表示网络上的位置的地址信息分配了 IP 地址。地址信息不限于 IP 地址，也可以使用电话号码等其他的信息。

[0053] 还有，关于网络系统 1 中包含的客户机装置的数目及服务器装置的数目，不需要进行限定。

[0054] 另外，客户机装置及服务器装置不限于各自总是作为客户机装置进行动作，总是作为服务器装置进行动作的情形，而根据执行的功能，既可以由客户机装置作为服务器装置进行动作，也可以由服务器装置作为客户机装置进行动作。

[0055] < 流再现的概要 >

[0056] 这里，简单说明由客户机装置 10 对服务器装置 20 保持的内容进行流再现，并更新非法设备列表时的过程。

[0057] 客户机装置 10 从服务器装置 20，取得包括与内容有关的复制控制信息在内的管理信息（下面记述为“元信息”。）。

[0058] 接着，客户机装置 10 及服务器装置 20 执行认证密钥交换处理。另外，在认证密钥交换处理的期间，客户机装置 10 和服务器装置 20 将本机当前保持的非法设备列表的世代

及版本号发送至对方装置。

[0059] 客户机装置 10 及服务器装置 20 比较本机当前保持的非法设备列表的世代及版本号和对方装置当前保持的非法设备列表的世代及版本号，由保持着新的非法设备列表的装置向保持着旧的非法设备列表的装置，发送非法设备列表。

[0060] 这里，假定为客户机装置 10 从服务器装置 20 接收到新的非法设备列表。在本实施方式中，客户机装置 10 即便接收到新的非法设备列表，也不立刻开始非法设备列表更新处理。

[0061] 客户机装置 10 若取得了交换密钥，则开始流再现，依次接收从服务器装置 20 发送的流数据（分组数据），进行解密及再现。

[0062] 客户机装置 10 使用元信息和再现位置，找到不妨碍流处理的定时，进行非法设备列表更新处理。

[0063] 这里，记述在元信息中的复制控制信息已被设定成“不许复制”及“自由复制”的某一个。

[0064] 由于设定了“不许复制”的分组数据是需要著作权保护的数据，在由服务器装置 20 加密之后进行发送，因而在客户机装置 10 中需要解密处理。

[0065] 由于设定了“自由复制”的分组数据是不需要著作权保护的数据，不用加密就进行发送，因而在客户机装置 10 中不需要解密处理。

[0066] 〈客户机装置 10〉

[0067] 图 2 是表示客户机装置 10 结构的框图。

[0068] 如同图所示，客户机装置 10 包括本发明所涉及的数据交换处理装置 100a 及再现装置 200。

[0069] 数据交换处理装置 100a 包括通信部 101、认证密钥交换处理部 102、流控制部 103a、非法设备列表存储部 104、非法设备列表更新部 105、加密引擎部 106 及状态管理部 107。

[0070] 再现装置 200 包含显示单元等，将从流控制部 103a 输出的 AV 数据显示于显示单元上。

[0071] 在下面，对于数据交换处理装置 100a 的详细情况进行说明。

[0072] (1) 通信部 101

[0073] 通信部 101 在和通过网络 30 所连接的服务器装置之间实施数据的收发。具体而言，通信部 101 对与所指定的端口对应的作为网络应用的认证密钥交换处理部 102 及流控制部 103a 通知接收数据。另外，通信部 101 还从认证密钥交换处理部 102 及流控制部 103a 受理数据发送请求，通过网络 30 发送发往服务器装置的数据。

[0074] (2) 认证密钥交换处理部 102

[0075] 认证密钥交换处理部 102 通过对通信部 101 通知认证密钥交换执行请求，经由通信部 101 给服务器装置发送认证密钥交换的数据，来开始认证密钥交换处理。认证密钥交换处理部 102 经由通信部 101 从服务器装置接收认证密钥交换的数据。

[0076] 还有，认证密钥交换处理部 102 在开始认证密钥交换处理之前，对状态管理部 107 通知针对加密引擎部 106 之硬件资源的使用请求。随后，认证密钥交换处理部 102 从状态管理部 10 接收包括识别加密引擎部 106 之硬件资源的信息在内的使用许可通知，开始认证

密钥交换处理。

[0077] 认证密钥交换处理部 102 通过经由通信部 101，和服务器装置交换询问命令、响应命令及交换密钥命令，来实施认证密钥交换。若认证密钥交换处理完成，则对流控制部 103a 通知认证密钥交换完成。

[0078] 认证密钥交换处理部 102 在认证密钥交换处理完成后，将包括询问命令及响应命令中含有的非法设备列表的世代及版本号和能识别认证密钥交换处理的识别信息在内的非法设备列表比较请求，通知给非法设备列表更新部 105。随后，认证密钥交换处理部 102 通过从非法设备列表更新部 105 取得比较结果，来判定是否需要非法设备列表的更新处理。

[0079] 认证密钥交换处理部 102 从非法设备列表更新部 105 接收的比较结果是不需要收发（同值）、发送非法设备列表（新）及接收非法设备列表（旧）的某一个。

[0080] 在比较结果为“不需要收发”的场合，不进行非法设备列表的更新处理。

[0081] 在比较结果为“发送非法设备列表”的场合，认证密钥交换处理部 102 从非法设备列表更新部 105 取得非法设备列表存储部 104 中所存储的非法设备列表，经由通信部 101 发送非法设备列表。

[0082] 在比较结果为“接收非法设备列表”的场合，认证密钥交换处理部 102 经由通信部 101 接收包括非法设备列表的数据在内的交换命令。认证密钥交换处理部 102 若接收到交换命令，则对非法设备列表更新部 105，通知包括接收到的非法设备列表的数据和识别认证密钥交换的识别信息在内的非法设备列表更新请求。

[0083] 另外，认证密钥交换处理部 102 若接收到认证密钥交换结束请求，则对状态管理部 107 通知废弃请求，释放硬件资源。

[0084] (3) 流控制部 103a

[0085] 流控制部 103a 若从认证密钥交换处理部 102 接收到包括交换密钥信息在内的交换密钥交换完成通知，则将内容及与该内容对应的元信息的取得请求委托给通信部 101。随后，流控制部 103a 接收内容及元信息。流控制部 103a 在开始内容的再现处理之前，对状态管理部 107 通知针对加密引擎部 106 之硬件资源的使用请求。流控制部 103a 使用下述的加密引擎部 106 中所具备的作为硬件资源的 AES128.CBC 部 113，进行已加密的分组数据的解密处理。

[0086] 另外，流控制部 103a 还将接收到的元信息登录于状态管理部 107 中。

[0087] 流控制部 103a 若从状态管理部 107 接收到包括硬件资源识别信息在内的使用许可通知，则开始内容再现处理。

[0088] 流控制部 103a 从由通信部 101 接收到的内容的头信息取得密钥信息。然后，使用该密钥信息和从认证密钥交换处理部 102 接收到的交换密钥信息，生成用来将内容解密的解密密钥（内容密钥）。

[0089] 流控制部 103a 使用解密密钥将从服务器装置传送出的内容依次解密，输出给再现装置 200。流控制部 103a 一边再现内容，一边按一定的时间间隔，将包括硬件资源识别信息和内容的再现位置在内的位置信息发送给状态管理部 107，通知内容的再现状况。

[0090] 若内容的再现结束，则流控制部 103a 对状态管理部 107 通知废弃请求，释放硬件资源。

[0091] (4) 非法设备列表存储部 104

[0092] 非法设备列表存储部 104 包括存储器管理部及非易失性存储器。在非易失性存储器中，存储着非法设备列表。非法设备列表存储部 104 若从非法设备列表更新部 105 发出了请求，则经由存储器管理部，从非易失性存储器读出非法设备列表。另外，非法设备列表存储部 104 若从非法设备列表更新部 105 接收到新的非法设备列表的数据，则经由存储器管理部，向指定地址存储数据。

[0093] 这里，使用图 3，对于非法设备列表进行说明。

[0094] 非法设备列表 150 如图 3 所示，作为头信息，具备类别 151(4 位)、世代 152(4 位)、保留区域 153(8 位)、版本号 154(16 位) 及大小 156(16 位)，作为主体信息，具备记述了非法设备的 ID 后的列表 157 及 DTLA 签名 158(320 位)。

[0095] 与 DTCP 标准相应的非法设备列表的格式变更由世代 152 中所记述的信息进行管理。如果世代 152 的数字大，则是较新的格式的非法设备列表。例如，第 1 世代非法设备列表的场合，在世代 152 中记述“0”，第 2 世代非法设备列表的场合，在世代 152 中记述“1”。另外，世代 152 和非易失性存储器的大小相对应。只要查看世代 152 中所记述的信息，就可以判定当前保持该非法设备列表的数字设备的非易失性存储器的大小。

[0096] 版本号 154 是 DTLA 发放非法设备列表的每次都进行增量的信息。还有，版本号 154 作为比世代 152 更靠下位的信息来使用。

[0097] 列表 157 记述着由 DTLA 所认定的非法设备的设备 ID，是非法设备列表 150 的主要内容。各服务器装置及各客户机装置在认证密钥交换处理中，检查认证密钥交换请求源的装置的 ID 是否记述在列表 157 中。

[0098] DTLA 签名 158 是为了证明非法设备列表 150 是由 DTLA 正式发放的信息，所使用的。

[0099] (5) 非法设备列表更新部 105

[0100] 非法设备列表更新部 105 由认证密钥交换处理部 102 进行启动。非法设备列表更新部 105 利用后述的加密引擎部 106 中所具备的作为硬件资源的椭圆运算部 114，进行非法设备列表中包含的 DTLA 签名的验证处理。

[0101] 这里，使用图 6 所示的流程图，按照处理的过程说明由非法设备列表更新 105 执行的处理。

[0102] 非法设备列表更新部 105 从认证密钥交换处理部 102，取得包括服务器装置保持的非法设备列表的世代及版本号和认证密钥交换的识别信息在内的非法设备列表比较请求 (步骤 S1)。

[0103] 非法设备列表更新部 105 若接收到非法设备列表比较请求，则从非法设备列表存储部 104 取得非法设备列表的世代和版本号，判断自己的非法设备列表和服务器装置的非法设备列表进行比较，是新、是旧、还是同值。具体而言，比较双方的世代及版本号 (步骤 S2)。然后，非法设备列表更新部 105 将比较结果通知给认证密钥交换处理部 102。在本实施方式中，在自己的非法设备列表的世代及版本号至少一个较旧的情况下，需要更新非法设备列表。

[0104] 非法设备列表更新部 105 在比较结果为同值的场合 (步骤 S2 中的“相同”)，将从认证密钥交换处理部 102 接收到的信息废弃。

[0105] 在比较结果为新的场合（步骤 S2 中的“新”），非法设备列表更新部 105 从非法设备列表存储部 104 读出非法设备列表（步骤 S3）。然后，非法设备列表更新部 105 对状态管理部 107 通知硬件资源的使用请求（步骤 S4）。随后，进行由状态管理部 107 做出的处理（步骤 S5），若从状态管理部 107 接收到包括硬件资源识别信息在内的使用许可通知，则非法设备列表更新部 105 将非法设备列表和硬件资源识别信息通知给加密引擎部 106，执行 DTLA 签名的签名验证处理（步骤 S6）。

[0106] 若由加密引擎部 106 做出的签名验证处理成功（步骤 S7 中的 OK），则非法设备列表更新部 105 根据服务器装置的非法设备列表的世代及版本号，实施非法设备列表的变换。

[0107] 再者，非法设备列表更新部 105 对变换后的非法设备列表，进行与服务器装置的非易失性存储器的大小相符的大小变换处理（步骤 S8）。随后，非法设备列表更新部 105 对认证密钥交换处理部 102 通知非法设备列表，经由认证密钥交换处理部 102 发送非法设备列表（步骤 S9）。

[0108] 若由加密引擎部 106 做出的签名验证处理失败（步骤 S7 中的 NG），则非法设备列表更新部 105 结束非法设备列表更新处理。

[0109] 在比较结果为旧的场合（步骤 S2 中的“旧”），非法设备列表更新部 105 经由认证密钥交换处理部 102 接收服务器装置的非法设备列表（步骤 S10）。

[0110] 然后，非法设备列表更新部 105 对状态管理部 107 通知硬件资源的使用请求（步骤 S11）。随后，进行由状态管理部 107 做出的处理（步骤 S12），若从状态管理部 107 接收到包括硬件资源识别信息在内的使用许可通知，则非法设备列表更新部 105 将非法设备列表和硬件资源识别信息通知给加密引擎部 106，进行 DTLA 签名的签名验证处理（步骤 S13）。

[0111] 若由加密引擎部 106 做出的签名验证处理成功（步骤 S14 中的 OK），则非法设备列表更新部 105 在非法设备列表存储部 104 中写入验证完成的非法设备列表（步骤 S15）。

[0112] 若由加密引擎部 106 做出的签名验证处理失败（步骤 S14 中的 NG），则非法设备列表更新部 105 将从服务器装置接收到的非法设备列表废弃（步骤 S16），结束非法设备列表更新处理。

[0113] 若非法设备列表的更新处理完成，则非法设备列表更新部 105 对状态管理部 107 通知废弃请求，释放硬件资源。

[0114] 还有，步骤 S5 及步骤 S12 的“由状态管理部做出的处理”将在下述状态管理部 107 的说明中进行详细阐述。

[0115] (6) 加密引擎部 106

[0116] 加密引擎部 106 是被防篡改化后的由芯片构成的安全单元。加密引擎部 106 如图 4 所示，包括安全 I/F111、控制部 112、AES128・CBC 部 113 及椭圆运算部 114。

[0117] AES128・CBC 部 113 是赋予识别信息 0001 后的硬件资源，进行使用 AES128・CBC 算法的加密处理及解密处理。具体而言，进行已加密的分组数据的解密处理。

[0118] 椭圆运算部 114 是赋予识别信息 0002 后的硬件资源，进行使用 EC-DSA 算法的签名生成处理及签名验证处理。具体而言，进行非法设备列表中包含的 DTLA 签名的验证处理。

[0119] 控制部 112 若通过安全 I/F111，从状态管理部 107 接收到硬件资源使用请求，则通

知与各硬件资源对应的识别信息。另外，控制部 112 若从状态管理部 107 接收到硬件资源废弃请求，则释放对应的硬件资源。再者，控制部 112 还对状态管理部 107 通知各硬件资源的处理状况。

[0120] 加密引擎部 106 具备在解密处理及签名验证处理中使用的隐匿信息，因为需要确保牢固的安全性，所以和外部之间的数据收发只可以通过安全 I/F111 进行。在外部和安全 I/F111 之间的传输通路上以分时的形式收发数据，若在由流控制部 103a 做出的流数据的解密处理中发生了由非法设备列表更新部 105 做出的 DTLA 签名的验证处理，则流数据的解密处理发生延迟，对再现装置 200 的 AV 数据的传送变慢。

[0121] 因此，通过后述的状态管理部 107 进行控制，以便判断由非法设备列表更新部 105 做出的椭圆运算部 114 的使用可否，按流数据的解密处理不延迟的定时，对非法设备列表更新部 105 通知椭圆运算部 114 的使用许可。

[0122] (7) 状态管理部 107

[0123] 状态管理部 107 管理由认证密钥交换处理部 102、流控制部 103a 及非法设备列表更新部 105 而来的加密引擎部 106 的硬件资源使用状态。

[0124] 具体而言，状态管理部 107 若从认证密钥交换处理部 102、流控制部 103a 及非法设备列表更新部 105 接收到针对加密引擎部 106 之硬件资源的使用请求通知，则生成硬件资源管理信息。

[0125] 在图 5 中表示硬件资源管理信息的具体例。硬件资源管理信息 160 的第 1 行是从流控制部 103a 接收到使用请求通知时所生成的信息，第 2 行是从非法设备列表更新部 105 接收到使用请求通知时所生成的信息。各信息包含 ID、硬件资源 ID、功能及状态。

[0126] 若状态管理部 107 从认证密钥交换处理部 102、流控制部 103a 及非法设备列表更新部 105 接收到使用请求通知，则 ID 是由状态管理部 107 自身生成的信息。

[0127] 硬件资源 ID 是若获得加密引擎部 106 的硬件资源则能得到的该硬件资源的识别信息。

[0128] 功能是在该硬件资源中使用的功能。功能的类别有 AES128 •CBC 加密、AES128 •CBC 解密、椭圆运算验证及椭圆运算签名等。

[0129] 状态表示该硬件资源的功能的使用状态。状态的种类有 ACTIVE、WAIT 和 TERMINATE 等。

[0130] 若从加密引擎部 106 接收到包括硬件资源识别信息在内的处理状况信息，则状态管理部 107 更新对应的硬件资源管理信息的“状态”栏。

[0131] 若从认证密钥交换处理部 102、流控制部 103a 及非法设备列表更新部 105 接收到废弃请求的通知，则状态管理部 107 实施从加密引擎部 106 所获得的硬件资源的释放，删除对应的硬件资源管理信息。

[0132] 若硬件资源的释放处理完成，则状态管理部 107 对通知过废弃请求的认证密钥交换处理部 102、流控制部 103a 及非法设备列表更新部 105，通知硬件资源的废弃完成。

[0133] 状态管理部 107 若从认证密钥交换处理部 102、流控制部 103a 及非法设备列表更新部 105 接收到使用请求通知，则参照硬件资源管理信息，判定所请求的硬件资源的使用许可。在所请求的硬件资源为可使用的状态时，状态管理部 107 对通知过使用请求的认证密钥交换处理部 102、流控制部 103a 及非法设备列表更新部 105，发出许可通知。

[0134] 另外，状态管理部 107 还从流控制部 103a 接收元信息，将其存储于内部。再者，状态管理部 107 还接收由流控制部 103a 根据内容包含内容再现位置的位置信息。使用存储在内部的元信息和接收到的位置信息，来生成元信息进展信息。元信息进展信息包含流控制部 103a 接下来处理的预定分组数据的复制控制信息。

[0135] 状态管理部 107 若从非法设备列表更新部 105 接收到硬件资源使用请求，则使用硬件资源管理信息及元信息进展信息，来决定对非法设备列表更新部 105 通知硬件资源使用许可的定时。

[0136] 这里，使用图 7 的流程图，来说明流控制部 103a 执行内容流处理的过程中，状态管理部 107 从非法设备列表更新部 105 通知了针对加密引擎部 106 之硬件资源的使用请求时的动作。还有，这里说明的动作是图 6 的步骤 S5 及步骤 S12 的细节。

[0137] 状态管理部 107 若受理了使用请求通知（步骤 S21），则生成与非法设备列表更新部 105 对应的硬件资源管理信息（步骤 S22）。然后，状态管理部 107 确认加密引擎部 106 的硬件资源使用状况（步骤 S23）。

[0138] 在此，由于假定为已经开始由流控制部 103a 做出的内容再现处理，因而状态管理部 107 管理着与流控制部 103a 对应的硬件资源管理信息。因此，在步骤 S23 中，要判断在与流控制部 103a 对应的硬件资源管理信息的“状态”栏中是否记述有 ACTIVE。

[0139] 在不是 ACTIVE 的场合（步骤 S24 中 :否），状态管理部 107 前进到步骤 S30。

[0140] 在 ACTIVE 的场合（步骤 S24 中 :是），状态管理部 107 取得从流控制部 103a 发送的位置信息（步骤 S25），根据元信息和位置信息，生成元信息进展信息（步骤 S26）。

[0141] 状态管理部 107 判断在步骤 S26 中所生成的元信息进展信息内所记述的再现位置区间状态是否是“自由复制”。

[0142] 在自由复制的场合（步骤 S27 中 :是），前进到步骤 S30。在不是自由复制的场合（步骤 S27 中 :否），判断内容的再现是否是结束。具体而言，判断在步骤 S26 中所生成的元信息进展信息内所记述的再现位置区间状态是否是“0”。

[0143] 在内容的再现为结束的场合（步骤 S28 中 :是），前进到步骤 S30。在内容的再现不是结束的场合（步骤 S28 中 :否），返回到步骤 S25，继续处理。

[0144] 在流控制部 103a 的硬件资源使用状态不是“ACTIVE”的场合，流控制部 103a 不使用加密引擎部 106 的硬件资源。另外，在元信息进展信息的再现位置区间状态为“自由复制”的场合，因为不需要分组数据的解密，所以流控制部 103a 不使用加密引擎部 106 的硬件资源。另外，在内容的再现已结束时，流控制部 103a 也不使用加密引擎部 106 的硬件资源。

[0145] 因此，状态管理部 107 对非法设备列表更新部 105 通知硬件资源的使用许可（步骤 S29）。

[0146] < 由状态管理部 107 做出的硬件资源管理 >

[0147] 下面，对于由状态管理部 107 做出的硬件资源管理，使用图 8 ～图 10 进行说明。

[0148] 图 8 是表示流控制部 103a、状态管理部 107 及非法设备列表更新部 105 的状态转移的附图。

[0149] 若从流控制部 103a 对状态管理部 107 通知了硬件资源的使用请求，则状态管理部 107 生成硬件资源管理信息（设为 ID = 0001）。随后，若从状态管理部 107 对流控制部 103a 通知了硬件资源的使用许可，则流控制部 103a 开始流处理。

[0150] 在此，假设进行再现处理的分组数据的复制控制信息从内容的起始按顺序，是NMC、NMC、NMC、CF、NMC 及 NMC。“NMC”表示不许复制，“CF”表示自由复制。

[0151] 若开始了再现处理，则流控制部 103a 按预定的时间间隔，对状态管理部 107 通知包括再现位置在内的位置信息 1 ～ 6。

[0152] 状态管理部 107 每次接收位置信息 1 ～ 6，都使用存储在内部的元信息和接收到的位置信息，来生成元信息进展信息。

[0153] 具体来说，假设存储着图 9 所示的元信息 170，则在受理了位置信息 1、位置信息 2 及位置信息 5 时，状态管理部 107 生成图 10(a) 所示的元信息进展信息 180。元信息进展信息 180 表示，因为再现位置区间信息是 NMC，所以接下来再现的分组数据的复制控制信息被设定成 NMC。

[0154] 另外，在受理了位置信息 3 时，状态管理部 107 生成图 10(b) 所示的元信息进展信息 190。元信息进展信息 190 表示，因为再现位置区间信息是 CF，所以接下来再现的分组数据的复制信息被设定成 CF。

[0155] 另外，在受理了位置信息 6 时，状态管理部 107 生成图 10(c) 所示的元信息进展信息 210。元信息进展信息 210 表示，因为再现区间位置信息是 0，所以接下来再现的分组数据不存在，内容的再现处理结束。

[0156] 还有，由于位置信息 1 ～ 6 包含再现位置，因而状态管理部 107 只要查看再现位置和元信息 170 中所记述的区间信息，就可以识别流控制部 103a 当前在处理第几个分组数据。然后，状态管理部 107 从元信息 170 取得接下来处理的预定分组数据的复制控制信息，将其设定于元信息进展信息的再现区间位置信息中。

[0157] 例如，在位置信息 3 中包含再现位置＝ 1420 时，状态管理部 107 判明流控制部 103a 当前在处理第 3 个分组数据。而且，因为接下来处理的第 4 个分组数据的复制控制信息是 CF，所以状态管理部 107 将元信息进展信息的再现区间位置信息设定为“CF”。

[0158] 另外，在位置信息 6 中包含再现位置＝ 2700 时，状态管理部 107 判明流控制部 103a 当前在处理第 6 个分组数据。而且，由于接下来处理的分组数据不存在，因而状态管理部 107 将元信息进展信息的再现区间位置信息设定为“0”。

[0159] 返回图 8 的说明。若从非法设备列表更新部 105 对状态管理部 107 通知了硬件资源的使用请求，则状态管理部 107 生成硬件资源管理信息（设为 ID ＝ 0002）。随后，状态管理部 107 一边生成元信息进展信息，一边等待再现位置区间信息变为 CF。由于在通知位置信息 3 之后，元信息进展信息的再现位置区间信息变为 CF，因而状态管理部 107 对非法设备列表更新部 105 通知硬件资源的使用许可。

[0160] 非法设备列表更新部 105 若接收到使用许可的通知，则进行 DTLA 签名的验证处理。

[0161] 非法设备列表更新部 105 若 DTLA 签名的验证处理结束，则对状态管理部 107 通知硬件资源的废弃请求。流控制部 103a 若再现处理结束，则对状态管理部 107 通知硬件资源的废弃请求。

[0162] ＜服务器装置 20 的结构＞

[0163] 图 11 是表示服务器装置 20 结构的框图。

[0164] 如同图所示，服务器装置 20 包括本发明所涉及的数据交换处理装置 100b 及内容

存储部 300。

[0165] 数据交换处理部 100b 包括通信部 101、认证密钥交换处理部 102、流控制部 103b、非法设备列表存储部 104、非法设备列表更新部 105、加密引擎部 106 及状态管理部 107。

[0166] 内容存储部 300 由硬盘驱动器等构成，存储着 1 个以上的内容和与各内容对应的元信息。这里，内容是电影、音乐、计算机程序、计算机游戏、相片及文本数据等。

[0167] 在图 11 中，对于数据交换处理装置 100b 的结构要素之中，具有和客户机装置 10 的数据交换处理装置 100a 的结构要件相同的功能的部分，使用了和图 2 相同的符号。在此，对于具有相同符号的结构要素省略其说明，只说明流控制部 103b。

[0168] 流控制部 103b 若经由通信部 101 从客户机装置请求了元信息，则从内容存储部 300 取得与内容对应的元信息，经由通信部 101 给客户机装置发送元信息。

[0169] 另外，流控制部 103b 若经由通信部 101 从客户机装置请求了内容，则从认证密钥交换处理部 102 取得交换密钥信息，对状态管理部 107，通知针对加密引擎部 106 之硬件资源的使用请求。

[0170] 随后，流控制部 103b 若从状态管理部 107 接收到包括硬件资源识别信息在内的使用许可通知，则从内容存储部 300 读出内容。

[0171] 流控制部 103b 从内容的头信息取得密钥信息。然后，使用该密钥信息和从认证密钥交换处理部 102 接收到的交换密钥信息，生成用来将内容加密的加密密钥（内容密钥）。然后，流控制部 103b 将内容分割为分组数据进行加密，经由通信部 101 依次发送给客户机装置。

[0172] 此时，流控制部 103b 对于复制控制信息被设定成 CF 的分组数据，不需要进行加密，按明文的原状发送给客户机装置 10。对于复制控制信息被设定成 NMC 的部分内容，则进行加密来发送给客户机装置 10。

[0173] 另外，流控制部 103b 若内容的加密处理及发送处理结束，则对状态管理部 107 通知硬件资源的废弃请求。

[0174] 客户机装置 10 接收内容的分组数据进行再现，与之相对，服务器装置 20 将内容分组数据加密并进行发送。因此，服务器装置 20 的状态管理部 107 在流控制部 103b 一边使用加密引擎部 106 一边进行流处理时，使用元信息和处理位置来生成元信息进展信息。然后，在使用元信息进展信息，由流控制部 103b 处理复制控制信息被设定成 CF（自由复制）的分组数据时，对非法设备列表更新部 105 通知硬件资源的使用许可。

[0175] ＜系统的时序图＞

[0176] 图 12 及图 13 是客户机装置 10 及服务器装置 20 中与非法设备列表更新处理有关的时序图。

[0177] 在此，使用客户机装置 10 一边从服务器装置 20 取得内容进行再现，一边更新非法设备列表的具体例，进行说明。

[0178] 首先，用户操作客户机装置 10 的操作部（未图示），指示内容的再现。客户机装置 10 执行具有内容再现功能的应用。

[0179] 客户机装置 10 通过网络 30，对保持内容的服务器装置 20，请求认证密钥交换。服务器装置 20 若接收到认证密钥交换请求，则在客户机装置 10 的认证密钥交换处理部 102 和服务器装置 20 的认证密钥交换处理部 102 之间，进行认证密钥交换处理（步骤 S101）。

还有，客户机装置 10 在认证密钥交换处理中取得交换密钥信息，对流控制部 103a 通知交换密钥信息。另外，客户机装置 10 和服务器装置 20 在认证密钥交换处理中，相互交换非法设备列表的世代和版本号。

[0180] 客户机装置 10 通过网络 30，向服务器装置 20 请求元信息。服务器装置 20 若受理了元信息的请求，则将元信息发送给客户机装置 10（步骤 S102）。客户机装置 10 若取得了元信息，则在状态管理部 107 中登录元信息（步骤 S103）。

[0181] 客户机装置 10 的流控制部 103a 通过网络 30，给服务器装置 20 发送流请求，服务器装置 20 的流控制部 103b 接收流请求（步骤 S104）。

[0182] 流控制部 103b 将与流请求对应的内容的分组数据 (DATA1)，发送给流控制部 103a，流控制部 103a 接收 DATA1（步骤 S105）。在步骤 S105 中收发的 DATA1 其复制控制信息被设定成 NMC，并且已加密。因此，流控制部 103a 一边将接收到的 DATA1 解密，一边进行 AV 数据的再现（步骤 S106）。

[0183] 在另一方面，客户机装置 10 的非法设备列表更新部 105 和服务器装置 20 的非法设备列表更新部 105 进行本机当前保持的非法设备列表的新旧判定处理（步骤 S107 及步骤 S108）。在此，设为服务器装置 20 的非法设备列表较新。还有，步骤 S107 及步骤 S108 的处理因为和流请求（步骤 S104）并行进行动作，所以有时执行顺序要变换。

[0184] 服务器装置 20 若在步骤 S108 中判定出是非法设备列表发送方，则从非法设备列表存储部 104 读出非法设备列表，根据在认证密钥交换处理中所取得的客户机装置 10 的非法设备列表的世代，变换非法设备列表的大小（步骤 S109）。然后，经由认证密钥交换处理部 102，将非法设备列表发送给客户机装置 10，客户机装置 10 接收非法设备列表（步骤 S110）。

[0185] 客户机装置 10 的认证密钥交换处理部 102 若接收到非法设备列表，则对非法设备列表更新部 105 通知非法设备列表更新请求（步骤 S111），非法设备列表更新部 105 对状态管理部 107 通知硬件资源使用请求。

[0186] 在客户机装置 10 中，非法设备列表的更新处理和流处理并行进行动作。

[0187] 步骤 S106 之后，流处理继续。服务器装置 20 将接于 DATA1 后的分组数据 (DATA2)，发送给客户机装置 10，客户机装置 10 接收 DATA2（步骤 S112）。由于 DATA2 已经加密，因而流控制部 103a 一边将接收到的 DATA2 解密，一边进行 AV 数据的再现（步骤 S113）。

[0188] 服务器装置 20 将接于 DATA2 后的分组数据 (DATA3)，发送给客户机装置 10，客户机装置 10 接收 DATA3（步骤 S114）。由于 DATA3 已经加密，因而流控制部 103a 一边将接收到的 DATA3 解密，一边进行 AV 数据的再现（步骤 S114）。

[0189] 客户机装置 10 的状态管理部 107 每次从流控制部 103a 接收位置信息，都使用在步骤 S103 中所登录的元信息和位置信息来生成元信息进展信息。

[0190] 这里，接下来取得的分组数据 (DATA4) 其复制控制信息被设定成 CF（自由复制），并且判明是不需要解密处理的区间。因此，状态管理部 107 判断出非法设备列表更新处理中包含的 DTLA 签名的验证处理比 DATA4 的处理短，而对非法设备列表更新部 105 通知硬件资源的使用许可（步骤 S116）。

[0191] 服务器装置 20 将接于 DATA3 后的分组数据 (DATA4)，发送给客户机装置 10，客户机装置 10 接收 DATA4（步骤 S117）。由于 DATA4 未加密，因而流控制部 103a 进行接收到的

AV 数据的再现（步骤 S118）。

[0192] 在此期间，非法设备列表更新部 105 执行非法设备列表更新处理（步骤 S119），在非法设备列表存储部 104 中写入非法设备列表（步骤 S120）。

[0193] 步骤 S118 之后，流处理仍继续。服务器装置 20 将接于 DATA4 后的分组数据 (DATA5)，发送给客户机装置 10，客户机装置 10 接收 DATA5（步骤 S121）。流控制部 103a 一边将接收到的 DATA5 解密，一边进行 AV 数据的再现（步骤 S122）。

[0194] 服务器装置 20 将接于 DATA5 后的分组数据 (DATA6)，发送给客户机装置 10，客户机装置 10 接收 DATA6（步骤 S123）。流控制部 103a 一边将接收到的 DATA6 解密，一边进行 AV 数据的再现（步骤 S124）。

[0195] ＜其他的异例＞

[0196] 虽然根据上述的实施方式说明了本发明，但是不言而喻，本发明不能限定为上述的实施方式，如下的情形也包含于本发明中。

[0197] (1) 在上述的实施方式中，加密引擎部 106 作为硬件资源，搭载了 AES128・CBC 部 113 及椭圆运算部 114 的 2 个。但是，本发明的加密引擎部不限定于此，也可以再搭载与其他加密算法对应的硬件资源。

[0198] (2) 在上述的实施方式中，例如在图 12 中所记述的那样，在开始了由服务器装置和客户机装置做出的流处理之后，已经开始非法设备列表的更新处理。

[0199] 但是，本发明不限定于此，在本发明中还包括，在开始流处理之前，取得了更新用的非法设备列表时，在流处理之前开始非法设备列表的更新处理的情形。

[0200] 状态管理部 107 通过参照当前在内部管理的硬件资源管理信息，判明加密引擎部 106 未由流控制部 103a、103b 使用。因此，那种情况下，也可以对通知过硬件资源使用请求的非法设备列表更新部 105，通知硬件资源使用许可。

[0201] 还有，在非法设备列表更新部 105 正在使用加密引擎部 106 时，开始了由流控制部 103a、103b 做出的流处理的情况下，也可以通过状态管理部 107 进行控制，以使加密引擎部 106 优先使用于流控制部 103a、103b。

[0202] 状态管理部 107 若从流控制部 103a、103b 通知了硬件资源的使用请求，则使用硬件资源管理信息来确认当前的加密引擎部 106 的使用状态。在非法设备列表更新部 105 正在使用加密引擎部 106 时，对非法设备列表更新部 105，请求签名验证处理的中断。

[0203] 这里，在加密引擎部 106 的 AES128・CBC 部 133 和椭圆运算部 114 正在共用一个寄存器（未图示）的情况下，在寄存器中保持着由椭圆运算部 114 得到的中间的计算结果等。因此，椭圆运算部 114 也可以使保持在寄存器中的计算结果暂时保存于存储器（未图示）中。

[0204] 非法设备列表更新部 105 若请求中断签名验证处理，则暂时中断签名验证处理。随后，状态管理部 107 对流控制部 103a、103b 通知硬件资源的使用许可。

[0205] 若由流控制部 103a、103b 做出的流处理开始，则随后象上述实施方式所述的那样，实施由状态管理部 107 做出的控制就可以。

[0206] 也就是说，状态管理部 107 根据元信息和位置信息生成元信息进展信息，流控制部 103a、103b 进行控制，以便按处理自由复制的分组数据的定时，使由非法设备列表更新部 105 做出的签名验证处理再次开始。另外，在没有自由复制的分组数据时，其控制为，在

流处理结束的时候，使由非法设备列表更新部 105 做出的签名验证处理再次开始。

[0207] (3) 在上述的实施方式中，使用元信息进展信息，来控制对非法设备列表更新部 105 通知使用许可的定时。另外，在上述的异例 (2) 中，使用硬件资源管理信息及元信息进展信息，来控制对非法设备列表更新部通知使用许可的定时。

[0208] 在任何的情况下，虽然都排除了由加密引擎部 106 的 AES128・CBC 部 113 和椭圆运算部 114 同时进行处理的情形，但是本发明不限定于此。

[0209] 在本发明中，加密引擎部 106 的 AES128・CBC 部 113 和椭圆运算部 114 也可以同时进行处理。那种情况下，状态管理部 107 也可以除了元信息进展信息及硬件资源管理信息之外，还使用硬件资源同时处理数及硬件资源带宽信息等，来判定硬件资源的使用许可。

[0210] 例如，状态管理部 107 预先存储包括流处理所需要的带宽和 DTLA 签名的验证处理所需要的带宽在内的硬件资源带宽信息。再者，状态管理部 107 管理着当前使用中的带宽。而且，在从非法设备列表管理部 105 通知了使用请求时，状态管理部 107 使用硬件资源带宽信息和当前使用中的带宽，对于非法设备列表更新部 105，判定是否许可椭圆运算部 114 的使用。

[0211] 状态管理部 107 在如果使用椭圆运算部 114，则在流处理中发生延迟的那种情况下，不对非法设备列表更新部 105 通知使用许可，在即使使用椭圆运算部 114，也不在流处理中发生延迟的情况下，才对非法设备列表更新部 105 通知使用许可。

[0212] (4) 上述的实施方式说明了在作为家庭网络的网络 30 上所连接的客户机装置和服务器装置之间，进行非法设备列表的收发的具体例。

[0213] 本发明不限定为在客户机装置和服务器装置之间，进行非法设备列表的收发的情形，例如还包含如下的情形。

[0214] (a) 在因特网等的网络上设置由 DTLA 管理的 DTLA 运用服务器。DTLA 运用服务器管理着由 DTLA 发布的新的非法设备列表。各数字设备（实施方式中的客户机装置及服务器装置）通过网络从 DTLA 运用服务器接收新的非法设备列表，进行更新。

[0215] (b) 另外，也可以由 DTLA 将新的非法设备列表存储于移动式的媒体中，进行发布。例如，也可以在存储有电影内容的作为民用媒体的 DVD-ROM 或 BD-ROM 中，存储新的非法设备列表，进行销售。而且，各数字设备若插入了该媒体，则判定本机当前保持的非法设备列表和存储在媒体中的非法设备列表的新旧，在本机保持的非法设备列表较旧时，也可以从媒体读出新的非法设备列表，进行更新。

[0216] (5) 上述实施方式中的客户机装置及服务器装置是具备微处理器、ROM、RAM 及 HDD 等的计算机系统。在 HDD 或者 ROM 中，记录着计算机程序，通过由微处理器使用工作用的 RAM 执行计算机程序，客户机装置及服务器装置实现各种的功能。这里，计算机程序是为了实现预定的功能，组合多个表示针对计算机的指令的命令代码来构成的。

[0217] 另外，客户机装置及服务器装置的结构要件一部分或者全部也可以由 1 个系统 LSI(Large Scale Integration：大规模集成电路）构成。系统 LSI 是将多个结构部集成在 1 个芯片上制造出的超多功能 LSI，具体而言，是包含微处理器、ROM、RAM 等来构成的计算机系统。

[0218] 另外，构成客户机装置及服务器装置的结构要件各单元既可以分别进行单芯片化，也可以以包含一部分或者全部的形式进行单芯片化。

[0219] 另外，本发明也可以是上面所示的方法。另外，既可以是由计算机实现这些方法的计算机程序，也可以是将上述计算机程序记录到计算机可读取的记录媒体例如软盘、硬盘、CD-ROM、MO、DVD、DVD-ROM、DVD-RAM、BD(Blu-ray Disc)及半导体存储器等中的方式。

[0220] (6)也可以分别组合上述的实施方式及上述异例。

[0221] 产业上的可利用性

[0222] 本发明可以在制造及销售依照DTCP-IP标准的数据交换处理装置的产业中，作为一面在流处理中保证较高的再现品质，一面执行非法设备列表的更新处理的规格，加以利用。

[0223] 符号说明

[0224] 1 网络系统

[0225] 10、11、12 客户机装置

[0226] 20、21、22 服务器装置

[0227] 30 网络

[0228] 100a 数据交换处理装置

[0229] 100b 数据交换处理装置

[0230] 101 通信部

[0231] 102 密钥交换处理部

[0232] 103a 流控制部

[0233] 103b 流控制部

[0234] 104 非法设备列表存储部

[0235] 105 非法设备列表更新部

[0236] 106 加密引擎部

[0237] 107 状态管理部

[0238] 200 再现装置

[0239] 300 内容存储部

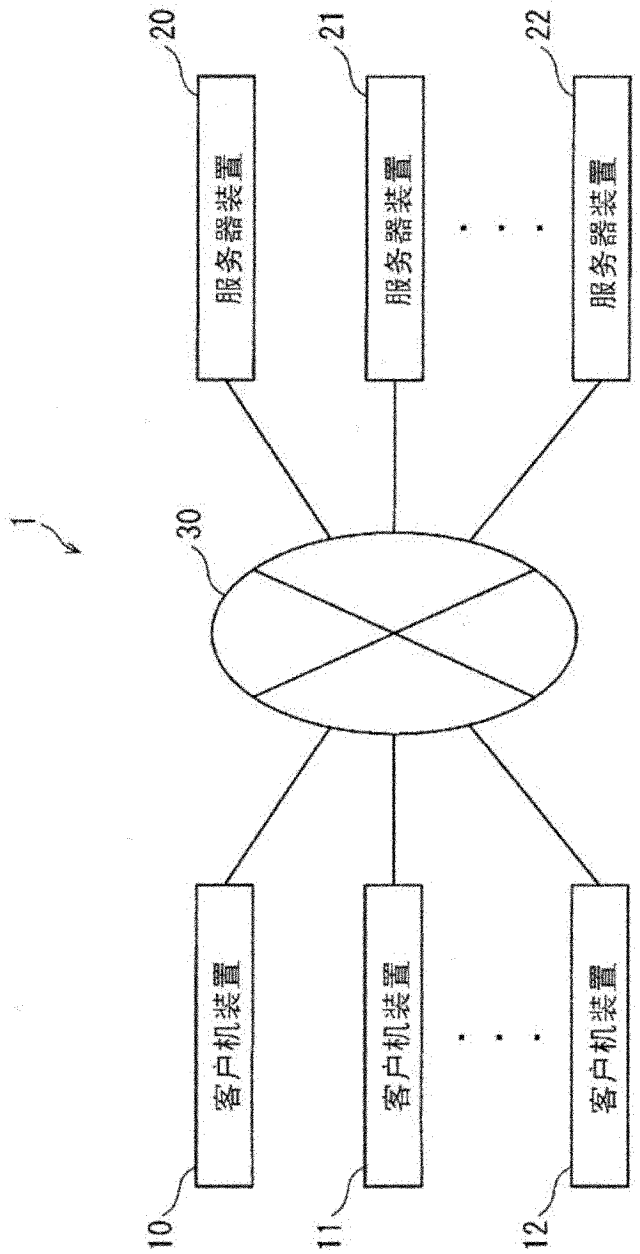


图 1

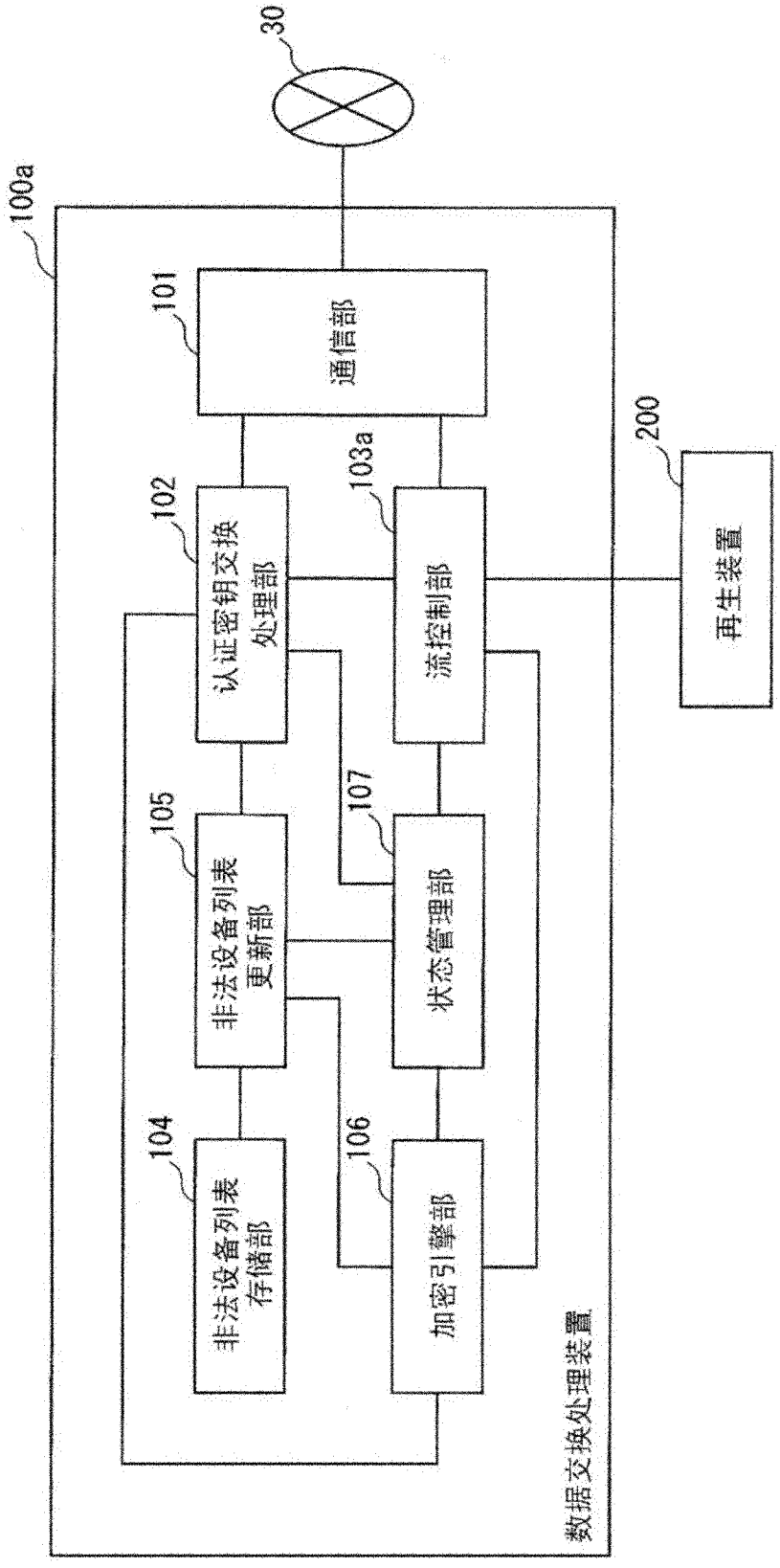

30
100a
101
通信部
200
102
认证密钥交换处理部
103a
流控制部
再生装置
105
非法设备列表更新部
107
状态管理部
104
非法设备列表存储部
106
加密引擎部
数据交换处理装置
10

图 2

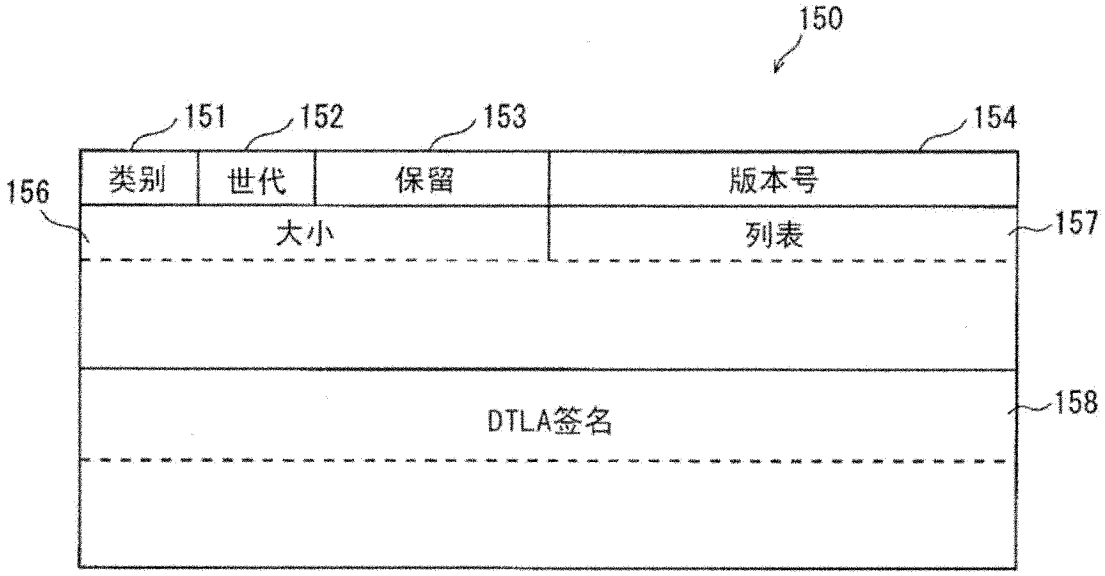


图 3

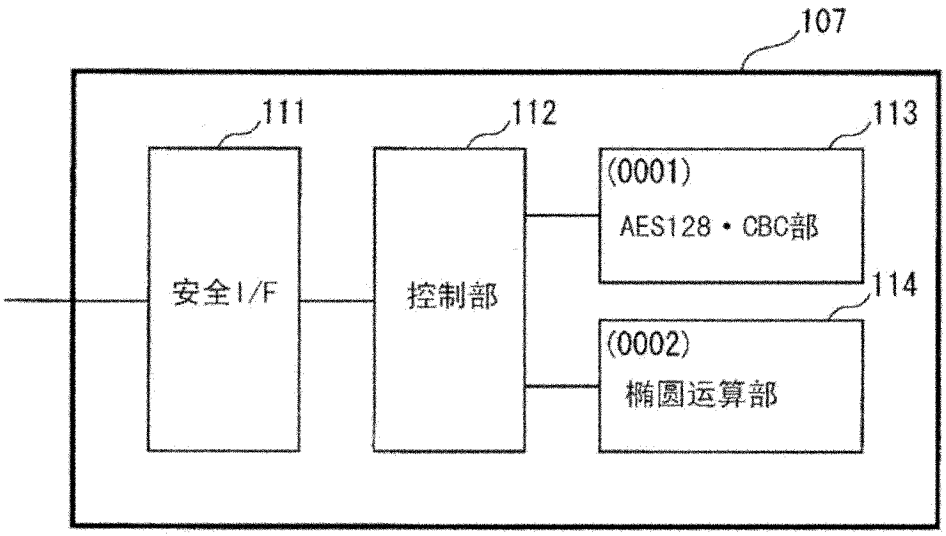


图 4

160

ID	硬件资源ID	功能	状态
0001	0001	AES128・CBC加密	ACTIVE
0002	0002	椭圆运算　验证	WAIT

图 5

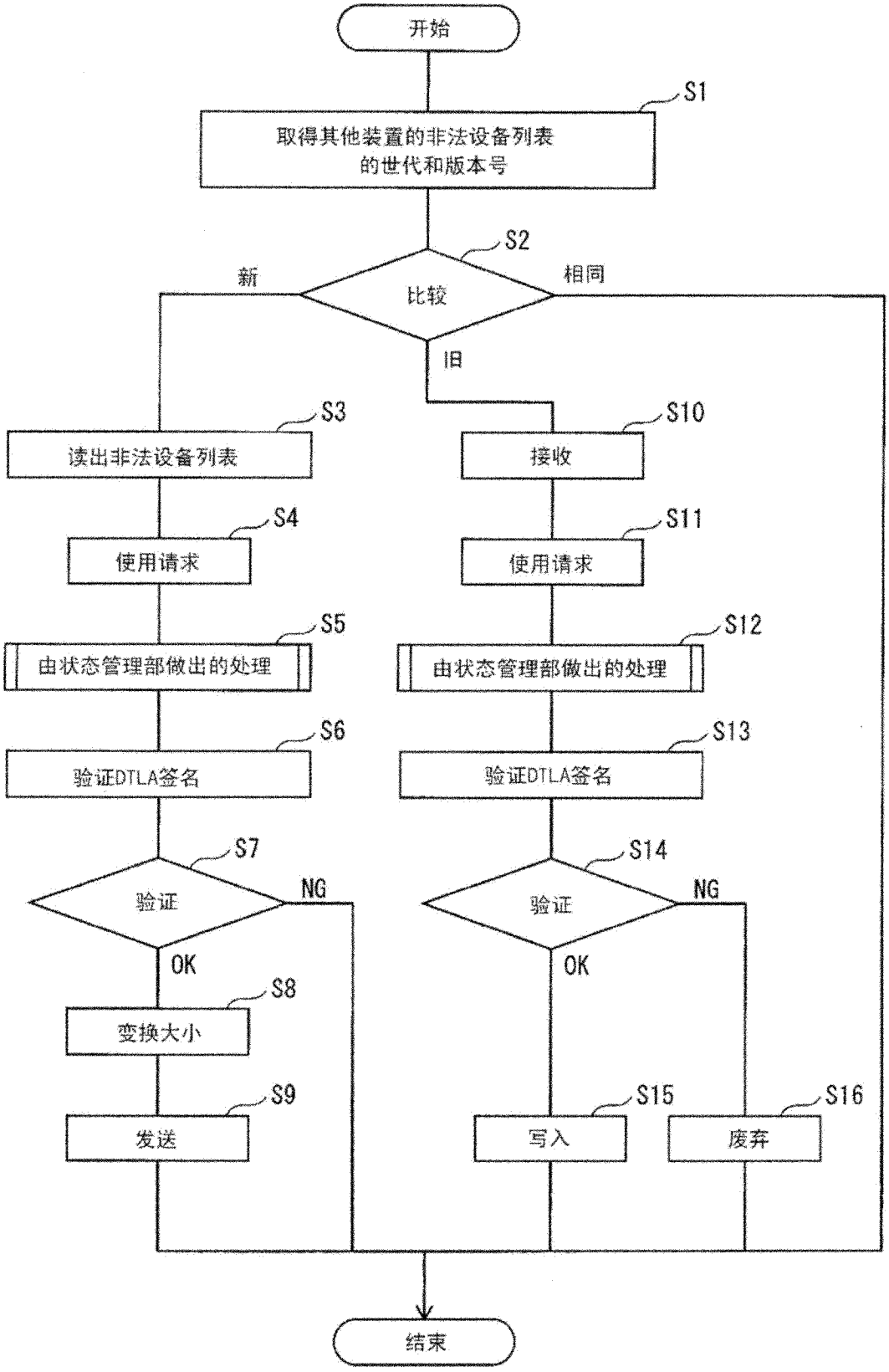

开始
S1
取得其他装置的非法设备列表
的世代和版本号
S2
比较
新
相同
旧
S3
读出非法设备列表
S4
使用请求
S5
由状态管理部做出的处理
S6
验证DTLA签名
S7
验证
NG
OK
S8
变换大小
S9
发送
S10
接收
S11
使用请求
S12
由状态管理部做出的处理
S13
验证DTLA签名
S14
验证
NG
OK
S15
写入
S16
废弃
结束

图 6

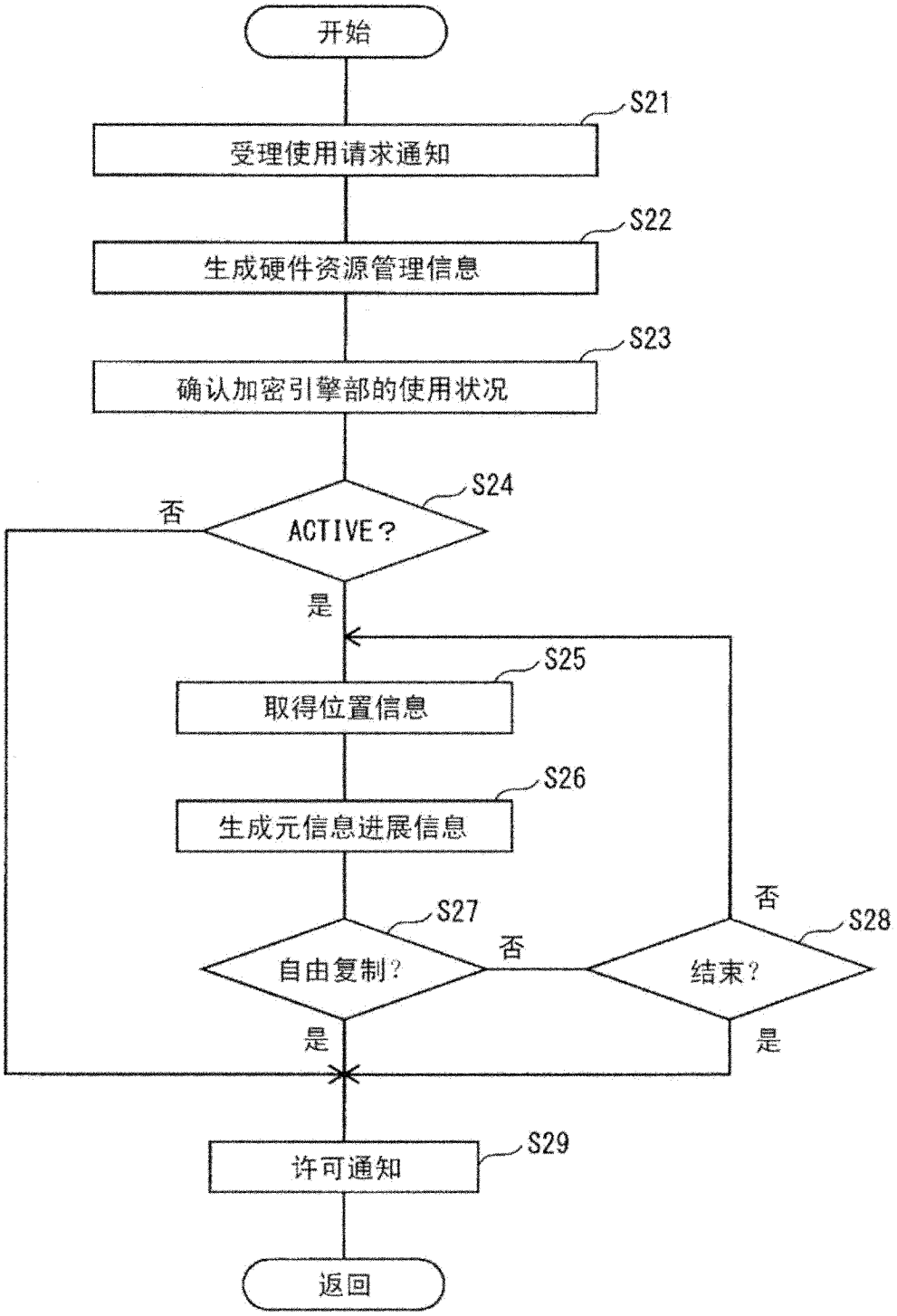

开始
S21
受理使用请求通知
S22
生成硬件资源管理信息
S23
确认加密引擎部的使用状况
S24
ACTIVE？
否
是
S25
取得位置信息
S26
生成元信息进展信息
S27
自由复制？
否
是
S28
结束？
否
是
S29
许可通知
返回

图 7

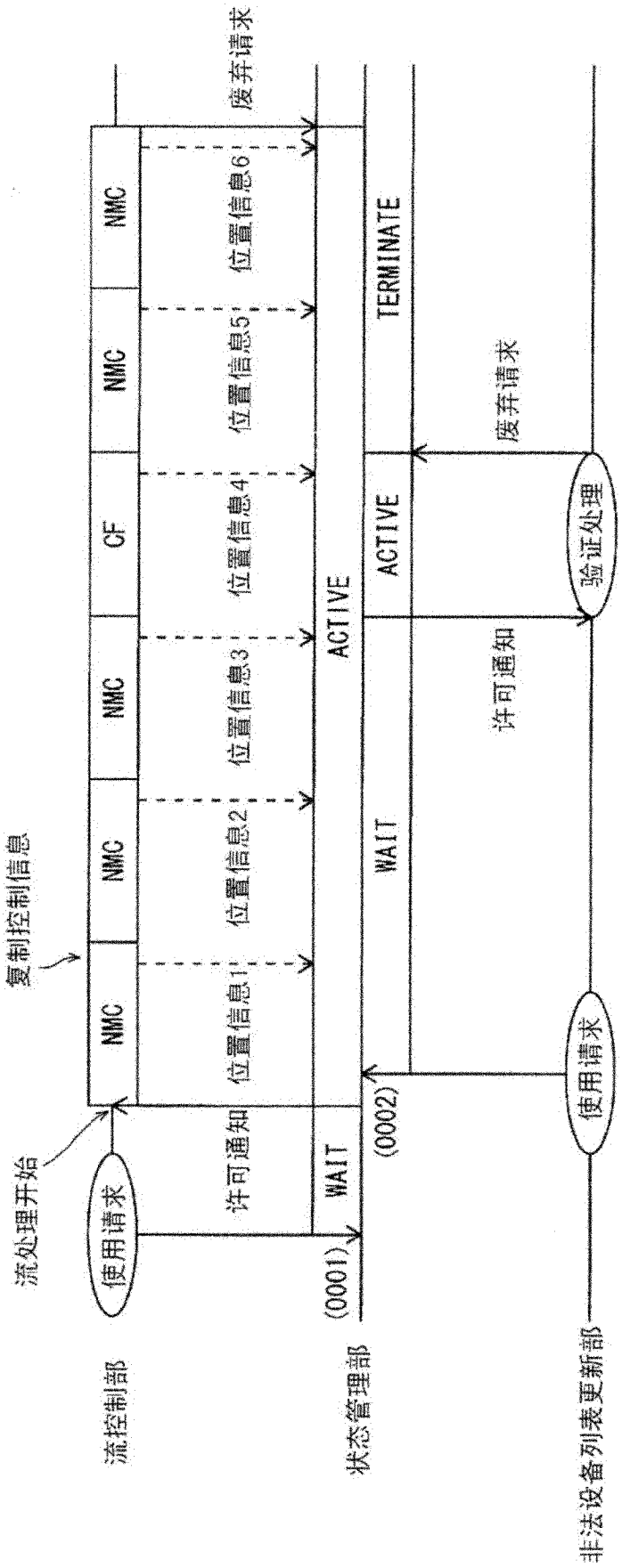

流处理开始
复制控制信息
使用请求
许可通知
位置信息1
位置信息2
位置信息3
位置信息4
位置信息5
位置信息6
废弃请求
NMC
NMC
NMC
CF
NMC
NMC
WAIT
(0001)
ACTIVE
(0002)
WAIT
ACTIVE
TERMINATE
许可通知
废弃请求
验证处理
使用请求
流控制部
状态管理部
非法设备列表更新部

图 8

170

0001		
编号	区间信息	复制控制信息
1	0 ～ 120	NMC
2	121 ～ 1000	NMC
3	1001 ～ 1500	NMC
4	1501 ～ 1800	CF
5	1801 ～ 2400	NMC
6	2401 ～ 2800	NMC

图 9

(a)

180

ID	元文件名	再生位置区间状态
0001	navi0001	NMC

(b)

190

ID	元文件名	再生位置区间状态
0001	navi0001	CF

(c)

210

ID	元文件名	再生位置区间状态
0001	navi0001	0

图 10

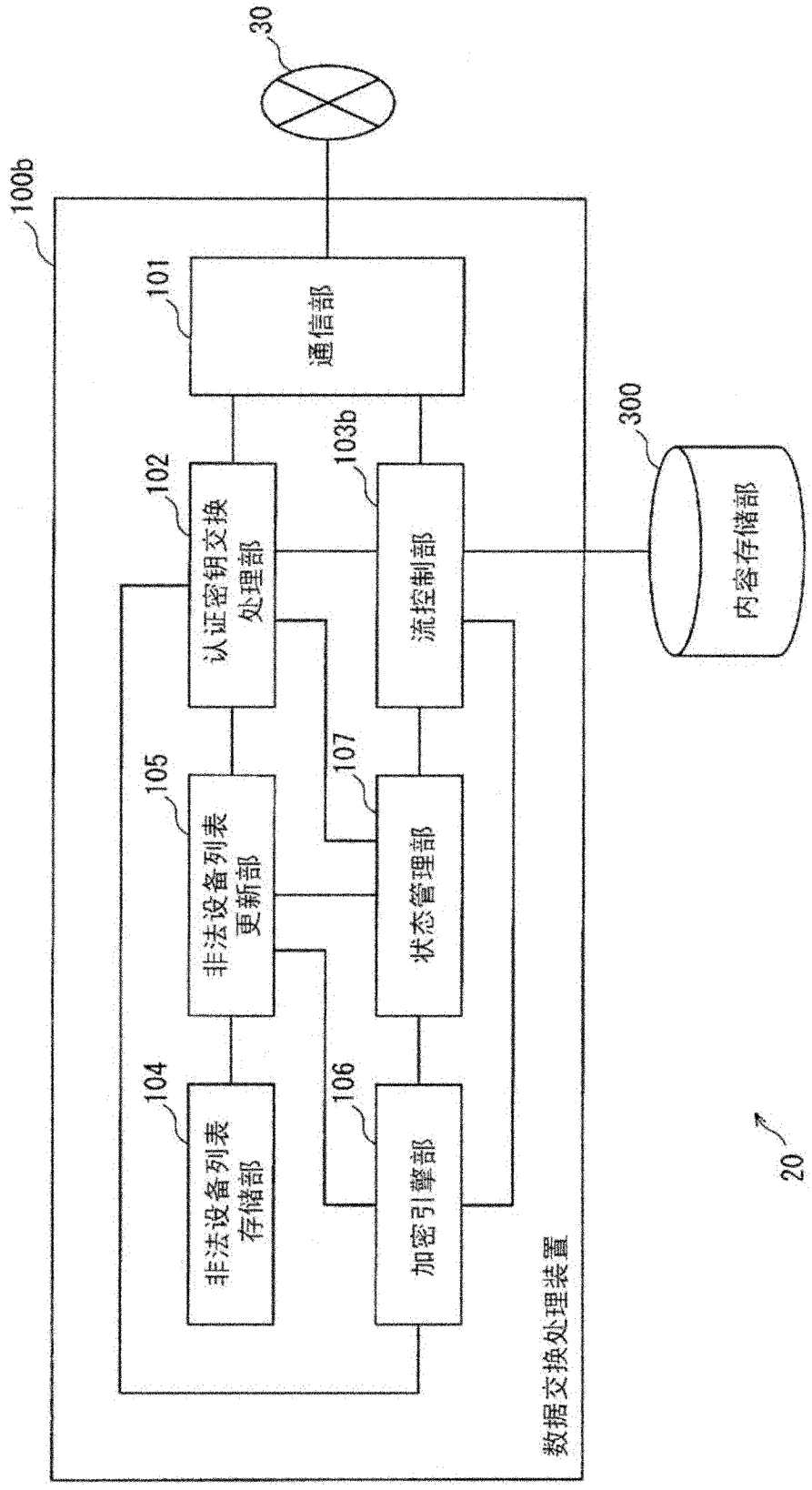

30
100b
101
通信部
102
认证密钥交换处理部
103b
流控制部
300
内容存储部
105
非法设备列表更新部
107
状态管理部
104
非法设备列表存储部
106
加密引擎部
数据交换处理装置
20

图 11

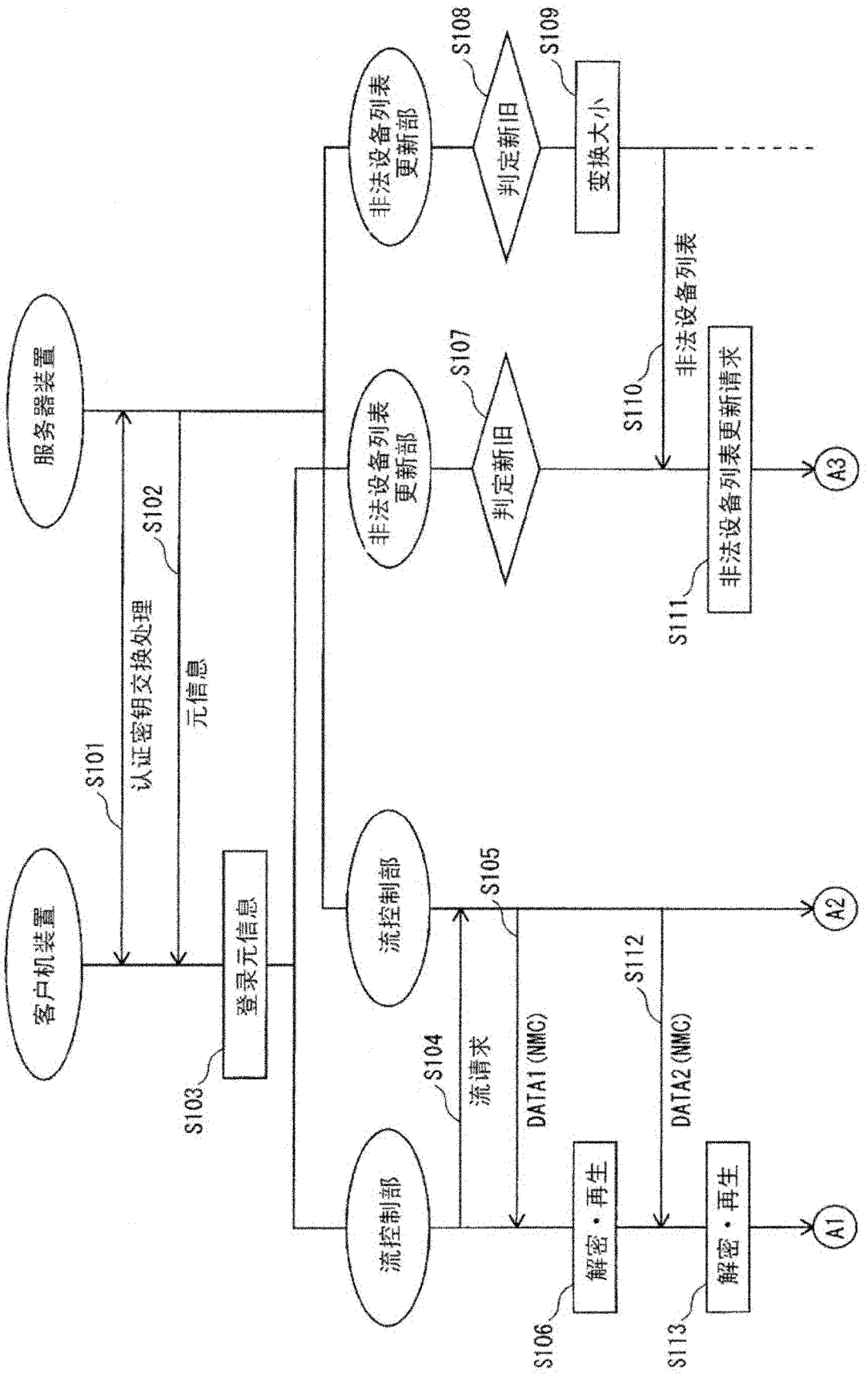

服务器装置
客户机装置
S101
认证密钥交换处理
S102
元信息
登录元信息
S103
非法设备列表更新部
S107
判定新旧
非法设备列表更新部
S108
判定新旧
S109
变换大小
S110
非法设备列表
非法设备列表更新请求
S111
A3
流控制部
S105
A2
S104
流请求
DATA1 (NMC)
S112
DATA2 (NMC)
流控制部
解密・再生
S106
解密・再生
S113
A1

图 12

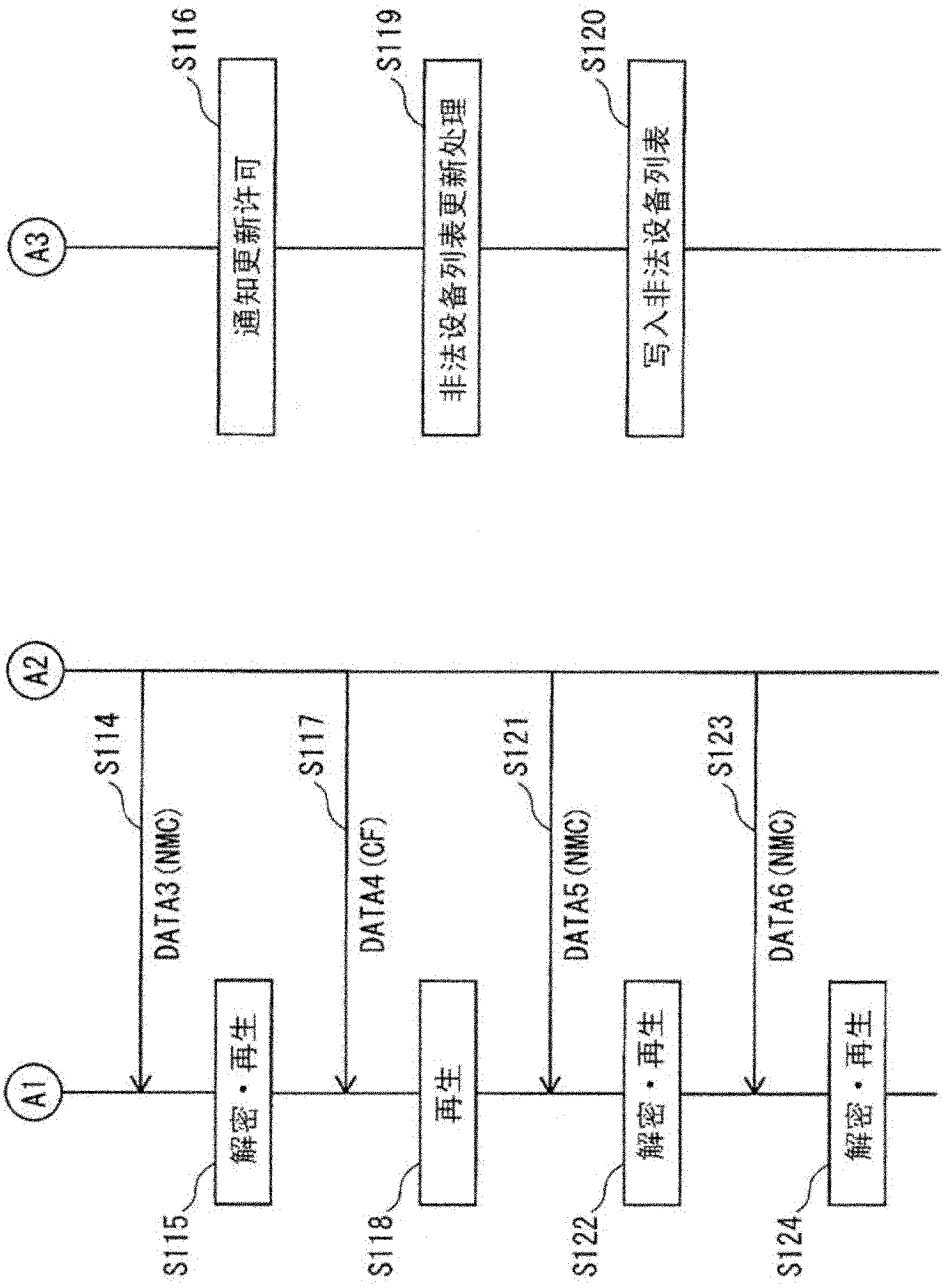

A3
S116
通知更新许可
S119
非法设备列表更新处理
S120
写入非法设备列表
A2
S114
DATA3 (NMC)
S117
DATA4 (CF)
S121
DATA5 (NMC)
S123
DATA6 (NMC)
A1
解密・再生
再生
解密・再生
解密・再生
S115
S118
S122
S124

图 13