(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 101375286 B
(45)授权公告日 2012.06.27

(21)申请号 200780002907.X

(22)申请日 2007.01.24

(30)优先权数据
016365/2006 2006.01.25 JP

(85)PCT申请进入国家阶段日
2008.07.23

(86)PCT申请的申请数据
PCT/JP2007/051099 2007.01.24

(87)PCT申请的公布数据
WO2007/086435 JA 2007.08.02

(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 冈本隆一 东吾纪男 庭野智
村上弘规

(74)专利代理机构 永新专利商标代理有限公司
72002
代理人 黄剑峰

(51)Int.Cl.
G06F 21/00(2006.01)
G06F 21/24(2006.01)
G06F 13/00(2006.01)

(56)对比文件
CN 1325207 A,2001.12.05, 全文.

审查员 董鑫

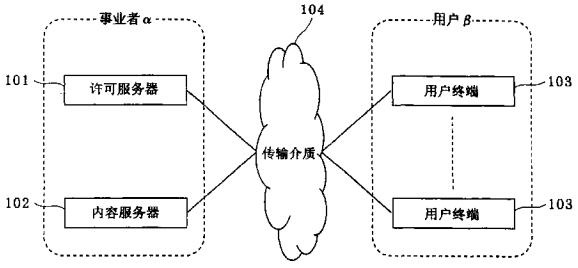
权利要求书 4 页 说明书 23 页 附图 29 页

(54)发明名称

终端装置、服务器装置及事务处理方法以及数字内容分发系统

(57)摘要

减少通信截断对策用的通信管理信息的记录频度。一种数字内容分发系统，包括：许可服务器(101)，发行许可；用户终端(103)，根据被发行的许可来控制内容的利用，并且，许可服务器(101)，按照所发行的许可的细节，判断是否需要记录通信截断对策用的通信管理信息，并将其通知给用户终端。据此，在用户终端(103)可以减少通信管理信息的记录频度。



CN 101375286 B

1. 一种终端装置，将内容密钥请求消息发送给服务器装置，接收来自所述服务器装置的针对所述内容密钥请求消息的应答消息并利用内容，所述终端装置，其特征在于，

所述内容密钥请求消息，包含事务标记，该事务标记和正在执行中的内容密钥请求处理相关联、且取 0 或 1 的值，

所述应答消息，包含内容密钥和事务标记记忆与否标记，该事务标记记忆与否标记表示所述事务标记的记忆与否，

所述终端装置，包括 ：

消息收发单元，与所述服务器装置进行消息的收发 ；

事务标记记忆单元，记忆所述事务标记 ；以及

事务标记写入单元，在

(1) 所述消息收发单元，接收所述应答消息，并且，

(2) 所述应答消息中包含的所述事务标记记忆与否标记被设定为要记忆的情况下，

将所述事务标记写入到所述事务标记记忆单元。

2. 如权利要求 1 所述的终端装置，其特征在于，

所述消息收发单元，将提交消息发送给所述服务器装置，该提交消息是通知成功地接收了所述应答消息的消息，

所述事务标记写入单元，在

(1) 所述消息收发单元，接收来自所述服务器装置的针对所述提交消息的 ACK 消息，并且，

(2) 所述事务标记记忆单元记忆所述事务标记的情况下，

从所述事务标记记忆单元中删除所述事务标记。

3. 如权利要求 2 所述的终端装置，其特征在于，

所述提交消息包含所述事务标记，

所述消息收发单元，在发送所述内容密钥请求消息之前，确认所述事务标记是否被记忆在所述事务记忆单元，在被记忆的情况下，将所记忆的所述事务标记的值，设定在所述提交消息中包含的所述事务标记，将所述提交消息发送给所述服务器装置，

所述事务标记写入单元，

在所述消息收发单元，接收来自所述服务器装置的针对所述提交消息的 ACK 消息的情况下，

从所述事务标记记忆单元中删除所述事务标记。

4. 如权利要求 2 所述的终端装置，其特征在于，

所述消息收发单元，在所述应答消息中包含的所述事务标记记忆与否标记被设定为不要记忆的情况下，不进行所述提交消息的发送。

5. 如权利要求 1 所述的终端装置，其特征在于，

所述应答消息，包含所述事务标记的记忆期限，

所述事务标记写入单元，在将所述事务标记写入到所述事务标记记忆单元时，和所述记忆期限相关联地写入，

在检测到超过所述记忆期限的情况下，以规定的定时，从所述事务标记记忆单元中删除所述事务标记。

6. 一种服务器装置，针对来自终端装置的内容密钥请求消息回送应答消息，所述服务器装置，其特征在于，

所述内容密钥请求消息，包含事务标记，该事务标记和正在执行中的内容密钥请求处理相关联、且取 0 或 1 的值，

所述应答消息，包含内容密钥和事务标记记忆与否标记，该事务标记记忆与否标记表示所述事务标记的记忆与否，

所述服务器装置，包括：

消息收发单元，与所述终端装置进行消息的收发；以及

事务标记记忆与否设定单元，对所述应答消息中的所述事务标记记忆与否标记进行值的设定，

所述事务标记记忆与否设定单元，在所述终端装置不要记忆所述事务标记的情况下，将所述事务标记记忆与否标记设定为不要记忆，在所述终端装置需要记忆所述事务标记的情况下，将所述事务标记记忆与否标记设定为要记忆。

7. 如权利要求 6 所述的服务器装置，其特征在于，

所述服务器装置，还具有，内容密钥发送可能次数管理单元，管理所述内容密钥的向所述终端装置的发送可能次数，

所述事务标记记忆与否设定单元，在所述内容密钥发送可能次数管理单元管理的所述发送可能次数为有限次数的情况下，判断为需要记忆所述事务标记，并将该判断结果设定在所述事务标记记忆与否标记。

8. 如权利要求 6 所述的服务器装置，其特征在于，

所述服务器装置，还具有，内容密钥发送履历管理单元，管理向所述终端装置发送了所述内容密钥的履历，

所述事务标记记忆与否设定单元，在内容密钥发送履历管理单元管理向所述终端装置发送所述内容密钥的发送履历的情况下，判断为需要记忆所述事务标记，并将该判断结果设定在所述事务标记记忆与否标记。

9. 如权利要求 6 所述的服务器装置，其特征在于，

所述应答消息，包含所述事务标记的记忆期限，

所述消息收发单元，在所述事务标记记忆与否设定单元对所述事务标记设定为要记忆的情况下，在所述事务标记的记忆期限设定规定的期限。

10. 如权利要求 6 所述的服务器装置，其特征在于，

所述服务器装置，还具有，提交处理单元，

在所述消息收发单元，从所述终端装置接收到提交消息的情况下，执行所述规定的提交处理，该提交消息是通知所述终端装置成功地接收了所述应答消息的消息。

11. 如权利要求 10 所述的服务器装置，其特征在于，

所述服务器装置，还具有，回退处理单元，在所述终端装置接收所述应答消息失败了的情况下，执行规定的回退处理。

12. 如权利要求 10 所述的服务器装置，其特征在于，

所述服务器装置，还具有，回退处理单元，

在所述消息收发单元，发送所述应答消息后、从所述终端装置接收所述提交消息之前

重新接收了所述内容密钥请求消息的情况下，执行所述规定的回退处理。

13. 一种数字内容分发系统，包括：服务器装置，分发内容密钥；以及终端装置，获得所述内容密钥并利用内容，

所述终端装置，将内容密钥请求消息发送给服务器装置，

所述服务器装置，将针对所述内容密钥请求消息的应答消息发送给终端装置，

所述内容密钥请求消息，包含事务标记，该事务标记和正在执行中的内容密钥请求处理相关联、且取 0 或 1 的值，

所述应答消息，包含内容密钥和事务标记记忆与否标记，该事务标记记忆与否标记表示所述事务标记的记忆与否，

所述终端装置，包括：

第一消息收发单元，与所述服务器装置进行消息的收发；

事务标记记忆单元，记忆所述事务标记；以及

事务标记写入单元，在

(1) 所述第一消息收发单元，接收所述应答消息，并且，

(2) 所述应答消息中包含的所述事务标记记忆与否标记被设定为要记忆的情况下，

将所述事务标记写入到所述事务标记记忆单元，

所述服务器装置，包括：

第二消息收发单元，与所述终端装置进行消息的收发；以及

事务标记记忆与否设定单元，对所述应答消息中的所述事务标记记忆与否标记进行值的设定，

所述事务标记记忆与否设定单元，在所述终端装置不要记忆所述事务标记的情况下，将所述事务标记记忆与否标记设定为不要记忆，在所述终端装置需要记忆所述事务标记的情况下，将所述事务标记记忆与否标记设定为要记忆。

14. 一种终端装置中的事务处理方法，该终端装置：将内容密钥请求消息发送给服务器装置，接收来自所述服务器装置的针对所述内容密钥请求消息的应答消息并利用内容，所述事务处理方法，其特征在于，

所述内容密钥请求消息，包含事务标记，该事务标记和正在执行中的内容密钥请求处理相关联、且取 0 或 1 的值，

所述应答消息，包含内容密钥和事务标记记忆与否标记，该事务标记记忆与否标记表示所述事务标记的记忆与否，

所述事务处理方法，具有：

与所述服务器装置进行消息的收发的步骤；以及

事务标记写入步骤，在

(1) 所述消息收发步骤，接收所述应答消息，并且，

(2) 所述应答消息中包含的所述事务标记记忆与否标记被设定为要记忆的情况下，

将所述事务标记写入到所述事务标记记忆单元。

15. 一种服务器装置中的事务处理方法，该服务器装置：针对来自终端装置的内容密钥请求消息回送应答消息，所述事务处理方法，其特征在于，

所述内容密钥请求消息，包含事务标记，该事务标记和正在执行中的内容密钥请求处

理相关联、且取 0 或 1 的值，

所述应答消息，包含内容密钥和事务标记记忆与否标记，该事务标记记忆与否标记表示所述事务标记的记忆与否，

所述事务处理方法，具有：

与所述终端装置进行消息的收发的步骤；以及

事务标记记忆与否设定步骤，对所述应答消息中的所述事务标记记忆与否标记进行值的设定，

所述事务标记记忆与否设定步骤，在所述终端装置不要记忆所述事务标记的情况下，将所述事务标记记忆与否标记设定为不要记忆；在所述终端装置需要记忆所述事务标记的情况下，将所述事务标记记忆与否标记设定为要记忆。

终端装置、服务器装置及事务处理方法以及数字内容分发系统

技术领域

[0001] 本发明涉及一种系统，利用网络，从服务器装置分发影像及音乐等数字内容、以及允许利用数字内容的许可，用户通过终端装置利用数字内容；尤其涉及一种系统以及装置，在所述服务器装置和所述终端装置间的通信中，防止不正当地进行许可的复制或窜改，并且，在发生通信截断时也防止许可的消失或重复分发。

[0002] 背景技术

[0003] 近年来，被称为内容分发系统的系统已进入实用化阶段，该内容分发系统中，通过互联网等通信或数字广播等，将音乐、影像、游戏等数字内容（以下，描述为内容）从服务器装置分发给终端装置，并且，可以在终端装置利用内容。在一般的内容分发系统中，为了保护内容的著作权、防止由恶意用户等不正当地利用内容，采用著作权保护技术。具体而言，著作权保护技术是一种技术，使用加解密技术等来安全地控制内容的利用。

[0004] 例如，作为内容分发系统的一个例子，在专利文献 1 中记载一种系统：终端装置，从服务器装置接收加密后的内容、利用条件以及内容解密密钥，确认窜改的有无后进行利用条件的符合性验证，只在满足所有的验证的情况下进行内容的解密。

[0005] 如上所述，在以往的内容分发系统中，从服务器装置向终端装置分发许可（是指包含利用条件和内容解密密钥的数据总称。也称为利用权利），而且，一般而言，对于该分发途径使用互联网等公众电路，因此需要防止许可的窃听以及窜改。即，应该防止利用条件的不正当的窜改或内容密钥的流出。再者，服务器装置需要进行接受许可分发方的认证。即，服务器装置还需要防止向不期望的终端装置分发许可。进行窃听、窜改防止和通信对方的认证的协议被称为 SAC(Secure Authenticated Channel) 协议，例如 SSL(Secure Socket Layer) 为一般所知（例如，参照非专利文献 1）。

[0006] 而且，在正在分发许可中因通信装置、通信电路的故障或电源断开等而发生通信截断的情况下，有可能消失该许可。在这些情况下，对于用户产生不能再生已购买的内容的损失。例如，在专利文献 2 以及专利文献 3 中记载一种协议：通过重新发送数据从而回避因通信截断而引起的通信数据的消失。

[0007] 专利文献 1：（日本）特许第 3276021 号公报

[0008] 专利文献 2：（日本）特开 2002-251524 号公报

[0009] 专利文献 3：（日本）特开 2003-16041 号公报

[0010] 非专利文献 1：A.Frier, P.Karlton, and P.Kocher,“The SSL 3.0Protocol”, [online], NetScape Communications Corp., Nov.18,1996, 互联网 <URL:http://wp.netscape.com/eng/ssl3/draft302.txt>, [平成 18 年 1 月 23 日检索]

[0011] 然而，对于 SAC 协议或通信截断对策协议，为了扩大该适用范围而重视通用性，且被定义为相互独立。据此，为了通过利用双方的协议，从而实现许可的窃听及窜改的防止、通信对方的认证、通信截断对策的全部功能，需要双方的协议所需要的通信往复次数。

[0012] 而且，在连续进行许可获得或许可返还等事务 (transaction) 的情况下，若按每

个事务单纯地反复 SAC 协议和通信截断对策协议，则以一次事务处理所需要的通信往复次数的倍数增加通信往复次数。例如，在一次事务处理所需要的通信往复次数是四次的情况下，在处理 n 个事务时需要的通信往复次数是四 n 次。

[0013] 因此，存在的课题是，到终端装置完了事务处理为止发生通信延迟，并从用户发出请求到获得应答为止发生等待时间。

[0014] 而且，如图 26 所示，在许可服务器 101 中，针对来自用户终端 103 的许可获得请求消息，从发送应答消息到接收提交 (commit) 消息为止，为了管理许可的发行需要进行日志记录 2601 以及日志清除 2603 ；在用户终端 103 中，从接收应答消息到接收 ACK 消息为止的期间，为了管理许可需要进行日志记录 2602 以及日志清除 2604。因此，存在的问题是，在许可服务器 101 以及用户终端 103 中需要在每次进行日志记录时蓄积数据，为了应对电源截断等地写入到作为非易失性存储器的闪存等、从而进行日志记录的情 况下，影响到写入次数有限的存储器的寿命。

[0015] 发明内容

[0016] 为了解决所述以往的问题，本发明的目的在于提出一种可以实现协议的系统以及装置，该协议中，在通过使用日志记录来进行服务器装置和终端装置间的许可管理的情况下，在服务器装置和终端装置间要记录的信息的大小较小，且记录日志的频度较少。

[0017] 而且，目的在于提出可实现一种协议的系统以及装置，该协议中，可以实现防止许可的窃听及窜改、通信对方的认证、通信截断对策的全部功能，并且，在多次进行事务处理的情况下，可以减少服务器装置和终端装置间的通信往复次数。

[0018] 为了解决所述以往的课题，本发明的终端装置，将内容密钥请求消息发送给服务器装置，接收来自所述服务器装置的针对所述内容密钥请求消息的应答消息并利用内容，所述终端装置，其特征在于，

[0019] 所述内容密钥请求消息，包含事务标记，该事务标记和正在执行中的内容密钥请求处理相关联、且取 0 或 1 的值，

[0020] 所述应答消息，包含内容密钥和事务标记记忆与否标记，该事务标记记忆与否标记表示所述事务标记的记忆与否，

[0021] 所述终端装置，包括 ：消息收发单元，与所述服务器装置进行消息的收发 ；事务标记记忆单元，记忆所述事务标记 ；以及事务标记写入单元，在 (1) 所述消息收发单元，接收所述应答消息，并且，(2) 所述应答消息中包含的所述事务标记记忆与否标记被设定为要记忆的情况下，将所述事务标记写入到所述事务标记记忆单元。

[0022] 并且，本发明的终端装置的特点是 ：所述消息收发单元，将提交消息发送给所述服务器装置，该提交消息是通知成功地接收了所述应答消息的消息，所述事务标记写入单元，在 (1) 所述消息收发单元，接收来自所述服务器装置的针对所述提交消息的 ACK 消息，并且 (2) 所述事务标记记忆单元记忆所述事务标记的情况下，从所述事务标记记忆单元中删除所述事务标记。

[0023] 根据该结构，在终端装置侧，按照发行可能次数或利用条件，在事务 标记记忆与否标记不需要记忆的情况下，不需要进行用于许可管理的日志记录，通过利用事务标记记忆与否标记，可以使服务器装置和终端装置所记忆的信息大小变小，并且使终端装置记录日志的频度变少。

[0024] 所述的终端装置，其特征在于，所述提交消息包含所述事务标记，所述消息收发单元，在发送所述内容密钥请求消息之前，确认所述事务标记是否被记忆在所述事务记忆单元，在被记忆的情况下，将所记忆的所述事务标记的值，设定在所述提交消息中包含的所述事务标记，将所述提交消息发送给所述服务器装置，所述事务标记写入单元，在所述消息收发单元，接收来自所述服务器装置的针对所述提交消息的 ACK 消息的情况下，

[0025] 从所述事务标记记忆单元中删除所述事务标记。

[0026] 所述的终端装置，其特征在于，所述消息收发单元，在所述应答消息中包含的所述事务标记记忆与否标记被设定为不要记忆的情况下，不进行所述提交消息的发送。

[0027] 所述的终端装置，其特征在于，所述应答消息，包含所述事务标记的记忆期限，所述事务标记写入单元，在将所述事务标记写入到所述事务标记记忆单元时，和所述记忆期限相关联地写入，在检测到超过所述记忆期限的情况下，以规定的定时，从所述事务标记记忆单元中删除所述事务标记。

[0028] 并且，本发明的终端装置的特点是：

[0029] 所述消息收发单元，在所述应答消息中包含的所述事务标记记忆与否标记被设定为不要记忆的情况下，省略所述提交消息的发送。

[0030] 根据该结构，在事务标记记忆与否标记被设定为不要记、而不进行日志记录的情况下，不需要从终端装置向服务器装置发送许可接收的提交消息，并且，服务器装置不需要发送针对提交消息的 ACK 消息，因此可以减少服务器装置和终端装置间的通信往复次数。

[0031] 并且，本发明的服务器装置，针对来自终端装置的内容密钥请求消息回送应答消息，所述服务器装置，其特征在于，

[0032] 所述内容密钥请求消息，包含事务标记，该事务标记和正在执行中的内容密钥请求处理相关联、且取 0 或 1 的值，所述应答消息，包含内容密钥和事务标记记忆与否标记，该事务标记记忆与否标记表示所述事务标记 的记忆与否，所述服务器装置，包括：

[0033] 消息收发单元，与所述终端装置进行消息的收发；以及事务标记记忆与否设定单元，对所述应答消息中的所述事务标记记忆与否标记进行值的设定，

[0034] 所述事务标记记忆与否设定单元，在所述终端装置不要记忆所述事务标记的情况下，将所述事务标记记忆与否标记设定为不要记忆，在所述终端装置需要记忆所述事务标记的情况下，将所述事务标记记忆与否标记设定为要记忆。

[0035] 根据该结构可以实现一种协议，即，服务器装置，在管理许可的发行数的情况下，或在按照利用条件将事务标记记忆与否标记通知给终端装置且在服务器装置以及终端装置不要记录的情况下，不需要进行为了管理许可的事务标记等的日志记录，并且，通过使用事务标记记忆与否标记，从而可以使在服务器装置以及终端装置记录的信息的大小变小，且记录日志的频度少。

[0036] 所述的服务器装置，其特征在于，所述服务器装置，还具有，内容密钥发送可能次数管理单元，管理所述内容密钥的向所述终端装置的发送可能次数，

[0037] 所述事务标记记忆与否设定单元，在所述内容密钥发送可能次数管理单元管理的所述发送可能次数为有限次数的情况下，判断为需要记忆所述事务标记，并将该判断结果设定在所述事务标记记忆与否标记。

[0038] 所述的服务器装置，其特征在于，

[0039] 所述服务器装置，还具有，内容密钥发送履历管理单元，管理向所述终端装置发送了所述内容密钥的履历，

[0040] 所述事务标记记忆与否设定单元，在内容密钥发送履历管理单元管理向所述终端装置发送所述内容密钥的发送履历的情况下，判断为需要记忆所述事务标记，并将该判断结果设定在所述事务标记记忆与否标记。

[0041] 所述的服务器装置，其特征在于，所述应答消息，包含所述事务标记的记忆期限，所述消息收发单元，在所述事务标记记忆与否设定单元对所述事务标记设定为要记忆的情况下，在所述事务标记的记忆期限设定规定的期限。

[0042] 所述的服务器装置，其特征在于，所述服务器装置，还具有，提交处理单元，在所述消息收发单元，从所述终端装置接收到提交消息的情况下，执行所述规定的提交处理，该提交消息是通知所述终端装置成功地接收了所述应答消息的消息。

[0043] 所述的服务器装置，其特征在于，所述服务器装置，还具有，回退处理单元，在所述终端装置接收所述应答消息失败了的情况下，执行规定的回退处理。

[0044] 所述的服务器装置，其特征在于，所述服务器装置，还具有，回退处理单元，在所述消息收发单元，发送所述应答消息后、从所述终端装置接收所述提交消息之前重新接收了所述内容密钥请求消息的情况下，执行所述规定的回退处理。

[0045] 一种数字内容分发系统，包括：服务器装置，分发内容密钥；以及终端装置，获得所述内容密钥并利用内容，所述终端装置，将内容密钥请求消息发送给服务器装置，

[0046] 所述服务器装置，将针对所述内容密钥请求消息的应答消息发送给终端装置，

[0047] 所述内容密钥请求消息，包含事务标记，该事务标记和正在执行中的内容密钥请求处理相关联、且取 0 或 1 的值，

[0048] 所述应答消息，包含内容密钥和事务标记记忆与否标记，该事务标记记忆与否标记表示所述事务标记的记忆与否，

[0049] 所述终端装置，包括：第一消息收发单元，与所述服务器装置进行消息的收发；事务标记记忆单元，记忆所述事务标记；以及事务标记写入单元，在 (1) 所述第一消息收发单元，接收所述应答消息，并且 (2) 所述应答消息中包含的所述事务标记记忆与否标记被设定为要记忆的情况下，将所述事务标记写入到所述事务标记记忆单元，所述服务器装置，包括：第二消息收发单元，与所述终端装置进行消息的收发；以及事务标记记忆与否设定单元，对所述应答消息中的所述事务标记记忆与否标记进行值的设定，

[0050] 所述事务标记记忆与否设定单元，在所述终端装置不要记忆所述事务标记的情况下，将所述事务标记记忆与否标记设定为不要记忆，在所述终端装置需要记忆所述事务标记的情况下，将所述事务标记记忆与否标记设 定为要记忆。

[0051] 一种终端装置中的事务处理方法，该终端装置：将内容密钥请求消息发送给服务器装置，接收来自所述服务器装置的针对所述内容密钥请求消息的应答消息并利用内容，所述事务处理方法，其特征在于，

[0052] 所述内容密钥请求消息，包含事务标记，该事务标记和正在执行中的内容密钥请求处理相关联、且取 0 或 1 的值，

[0053] 所述应答消息，包含内容密钥和事务标记记忆与否标记，该事务标记记忆与否标记表示所述事务标记的记忆与否，

[0054] 所述事务处理方法，具有：与所述服务器装置进行消息的收发的步骤；以及事务标记写入步骤，在 (1) 所述消息收发步骤，接收所述应答消息，并且 (2) 所述应答消息中包含的所述事务标记记忆与否标记被设定为要记忆的情况下，将所述事务标记写入到所述事务标记记忆单元。

[0055] 一种服务器装置中的事务处理方法，该服务器装置：针对来自终端装置的内容密钥请求消息回送应答消息，所述事务处理方法，其特征在于，

[0056] 所述内容密钥请求消息，包含事务标记，该事务标记和正在执行中的内容密钥请求处理相关联、且取 0 或 1 的值，所述应答消息，包含内容密钥和事务标记记忆与否标记，该事务标记记忆与否标记表示所述事务标记的记忆与否，所述事务处理方法，具有：与所述终端装置进行消息的收发的步骤；以及事务标记记忆与否设定步骤，对所述应答消息中的所述事务标记记忆与否标记进行值的设定，

[0057] 所述事务标记记忆与否设定步骤，在所述终端装置不要记忆所述事务标记的情况下，将所述事务标记记忆与否标记设定为不要记忆；在所述终端装置需要记忆所述事务标记的情况下，将所述事务标记记忆与否标记设定为要记忆。

[0058] 而且，为了实现所述目的，本发明可以作为事务处理方法或程序来实现，在所述事务处理方法中，将由所述终端装置以及所述服务器装置构成的数字内容分发系统、所述终端装置以及所述服务器装置的特征性构成单元作为步骤，并且，所述程序中包含所述的全部步骤。并且，不仅可以将所述程序存储在 ROM 等，也可以将所述程序通过 CD-ROM 等记录介质或通信网络来流通。

[0059] 根据本发明，在许可分发处理中从服务器装置侧向终端装置侧通知日志记录与否，从而可以在不要记录日志时不进行日志记录，因此可以减少存储器的写入频度。

[0060] 而且，由于按照许可中包含的利用条件的类别切换许可蓄积时或转发时等的处理，因此可以获得一种效果，即，可以实现一种许可管理，该许可管理中，防止在超过允许范围的情况下内容被利用，并且不进行不必要的 SAC 建立等处理。

[0061] 可以提供一种可以实现协议的系统以及装置，该协议中，可以实现防止许可的窃听及窜改、通信对方的认证、通信截断对策的全部功能，并且，在多次进行事务处理的情况下，也可以减少服务器装置和终端装置间的通信往复次数，再者，为了实现所述功能在服务器装置以及终端装置管理、保持的信息的大小小，且记录频度少。

附图说明

[0062] 图 1 是本发明的实施例的数字分发系统的结构框图。

[0063] 图 2 是示出本发明的实施例的许可 200 的一个例子的图。

[0064] 图 3 是本发明的实施例的许可服务器 101 的结构框图。

[0065] 图 4 是示出本发明的实施例的许可数据库 301 的一个例子的图。

[0066] 图 5 是本发明的实施例的安全通信部 302 的结构框图。

[0067] 图 6 是示出本发明的实施例的事务日志 600 的一个例子的图。

[0068] 图 7 是示出本发明的实施例的事务日志数据库 502 的一个例子的图。

[0069] 图 8 是本发明的实施例的用户终端 103 的结构框图。

[0070] 图 9 是本发明的实施例的安全通信部 803 的结构框图。

[0071] 图 10 是示出本发明的实施例的事务日志 1000 的一个例子的图。

[0072] 图 11 是示出本发明的实施例的事务日志数据库 902 的一个例子的图。

[0073] 图 12 是本发明的实施例的许可获得处理（在用户终端 103 和许可服务器 101 间开始通信时在事务日志数据库 902 没有记录日志的情况下）的许可获得处理的概要的说明图。

[0074] 图 13 是本发明的实施例的许可获得处理（在用户终端 103 和许可服务器 101 间开始通信时在事务日志数据库 902 记录日志的情况下）的许可获得 处理的概要的说明图。

[0075] 图 14 是说明在本发明的实施例的认证相位 P1 中进行的处理的流程图。

[0076] 图 15 是说明在本发明的实施例的认证、请求相位 P2 中进行的处理的流程图。

[0077] 图 16 是说明本发明的实施例的取消处理的流程图。

[0078] 图 17 是说明在本发明的实施例的应答消息生成、发送处理的流程图。

[0079] 图 18 是说明在本发明的实施例的应答消息接收时处理的流程图。

[0080] 图 19 是说明在本发明的实施例的请求相位 P3 中进行的处理的流程图。

[0081] 图 20 是说明在本发明的实施例的提交处理的流程图。

[0082] 图 21 是说明在本发明的实施例的应答消息生成、发送处理（重新发送）的流程图。

[0083] 图 22 是说明在本发明的实施例的提交相位 P4 中进行的处理的流程图。

[0084] 图 23 是说明在本发明的实施例的 ACK 消息接收时处理的流程图。

[0085] 图 24 是说明在本发明的实施例的认证、提交相位 P5 中进行的处理的流程图。

[0086] 图 25 是说明在本发明的实施例的许可服务器 101 检测到通信截断时的处理的流程图。

[0087] 图 26 是以往的数字分发系统的通信序列图。

[0088] 图 27 是本发明涉及的由许可服务器以及用户终端构成的数字分发系统的通信序列图。

[0089] 图 28 是示出向许可服务器的事务日志以及事务日志数据库还赋予了保持期限的情况下的数据结构的一个例子的图。

[0090] 图 29 是示出向用户终端的事务日志以及事务日志数据库还赋予了保持期限的情况下的数据结构的一个例子的图。

[0091] 图 30 是本发明涉及的数字分发系统的其它会话的通信序列图。

[0092] 图 31 是本发明涉及的数字分发系统的其它会话的通信序列图。

[0093] 符号说明

[0094] 101 许可服务器

[0095] 102 内容服务器

[0096] 103 用户终端

[0097] 104 传输介质

[0098] 200 许可

[0099] 201 许可 ID

[0100] 202 内容 ID

[0101] 203 利用条件类别

[0102] 204 利用条件

[0103] 205 内容密钥

[0104] 301 许可数据库

[0105] 302 安全通信部

[0106] 303 许可发行部

[0107] 401 终端 ID

[0108] 402 发行可能次数

[0109] 403 待提交标记

[0110] 501 安全通信控制部

[0111] 502 事务日志数据库

[0112] 503 特有信息记忆部

[0113] 504 随机数发生部

[0114] 505 加解密处理部

[0115] 506 通信部

[0116] 600 事务日志

[0117] 601 正在处理中事务有无

[0118] 602 正在处理中事务识别标记

[0119] 603 回退与否

[0120] 801 许可蓄积部

[0121] 802 内容蓄积部

[0122] 803 安全通信部

[0123] 804 许可获得部

[0124] 805 内容获得部

[0125] 806 内容输出控制部

[0126] 807 内容输出部

[0127] 901 安全通信部

[0128] 902 事务日志数据库

[0129] 903 特有信息记忆部

[0130] 904 随机数发生部

[0131] 905 加解密处理部

[0132] 906 通信部

[0133] 1000 事务日志

[0134] 1001 服务器 ID

具体实施方式

[0135] (实施例 1)

[0136] 说明本发明的实施例的数字内容分发系统。

[0137] 图 1 是本实施例的数字内容分发系统的整体结构图。并且，在本实施例涉及的数字内容分发系统中，如图 27 所示，在从用户终端 103 向许可服务器 101 发送了请求消息

(2701) 的情况下，在许可服务器 101 侧判断为了管理许可是否需要进行事务识别标记的日志记录，向用户终端 103 发送包含日志记录与否的应答消息 (2702)。于是，其特点是，用户终端 103，在需要日志记录的情况下，进行日志记录，在不需要日志记录的情况下，不进行日志记录。

[0138] 在图 1 中，数字内容分发系统包括许可服务器 101、内容服务器 102、多个用户终端 103 和传输介质 104。下面，说明数字内容分发系统的各个构成要素。

[0139] 许可服务器 101 是一种服务器，被设置在事业者 α 侧，管理对用户 β 的内容的利用权利，向用户终端 103 分发用图 2 后述的许可 200。

[0140] 内容服务器 102 是一种服务器，被设置在事业者 α 侧，向用户终端 103 分发内容。并且，假设，内容被加密成使用许可 200 来可以解密的状态后 被分发。

[0141] 用户终端 103，被设置在用户 β 侧，管理从许可服务器 101 分发来的许可 200，并使用许可 200 来再生从内容服务器 102 分发来的内容。

[0142] 传输介质 104 是互联网、CATV(Cable Television)、广播电波等有线传输介质、或有线传输介质以及移动式记录介质，在许可服务器 101、内容服务器 102 和用户终端 103 之间、在用户终端 103 和其它的用户终端 103 之间进行连接，以便可以交换数据。

[0143] 到上述为止，结束关于实施例的数字内容分发系统的整体结构的说明。

[0144] 图 2 是表示许可 200 的一个例子的图。在图 2 中，许可 200 包括许可 ID201、内容 ID202、利用条件类别 203、利用条件 204 和内容密钥 205。

[0145] 在许可 ID201 中描述唯一地确定许可 200 的 ID。在内容 ID202 中描述使用许可 200 来利用的内容的 ID。在利用条件类别 203 中描述表示利用条件 204 的类别的信息。在本实施例中假设，描述表示利用条件 204 是需要更新的利用条件（例如，“可以再生一次”等）、或是不需要更新的利用条件（例如，“到 2007 年 3 月为止可以再生”等）的信息。在利用条件 204 中描述允许利用内容的条件。在内容密钥 205 中描述解密内容的解密密钥。

[0146] 图 3 是本实施例的许可服务器 101 的整体结构图。在图 3 中，许可服务器 101 由许可数据库 301、安全通信部 302 和许可发行部 303 构成。下面，说明各个构成要素。

[0147] 许可数据库 301 是一种数据库，如在图 4 表示该一个例子，管理向各个用户终端 103 可以发行的许可 200。在图 4 中，许可数据库 301 由终端 ID401、向依据终端 ID401 确定的用户终端 103 可以发行的许可 200、发行可能次数 402 和待提交标记 403 构成。终端 ID401 是一种 ID，在数字内容分发系统中唯一地确定用户终端 103。发行可能次数 402 是向用户终端 103 可以发行许可 200 的次数。发行可能次数 402，在向用户终端 103 发送许可 200 后每次接收作为该回信的许可接收完了通知（以后，称为提交消息）时被减去 1，在发行可能次数 402 为 0 的时刻不能发行许可 200。在本实施例中假设，在发行可能次数 402 为 0 的情况下，该许可 200 从许可数据库 301 中被删除。待提交标记 403 是一种信息，表示是否处于等待来自用户终端 103 的提交消息的状态。在本实施例中，待提交标记 403，取“0”或“1”的任一个的值，在是“1”的情况下，表示处于等待提交消息的状态，在是“0”的情况下，表示不处于等待提交消息的状态。在本实施例中假设，在向用户终端 103 发送发行可能次数 402 是有限的许可 200 的情况下，将待提交标记 403 设定为“1”后发送。并且，假设，在待提交标记 403 是“1”的状态下接收提交消息的情况下，作为提交处理进行以下处理，即，从发行可能次数 402 中减去“1”，并将待提交标记 403 变更为“0”。

[0148] 在图 4 中表示，向终端 ID401 为“0001”的用户终端 103，可以发行许可 ID201 为“0011”或“0012”的二个许可 200，向终端 ID401 为“0002”的用户终端 103，可以发行许可 ID201 为“0021”的许可 200。而且表示，例如，向终端 ID401 为“0001”的用户终端 103 可以发行的、许可 ID201 为“0011”的许可 200，只一次可以发行、且正在等待提交。

[0149] 返回图 3，安全通信部 302 进行用户终端 103 的认证、许可服务器 101 和用户终端 103 间的隐藏通信（进行窃听、窜改的防止和通信对方的认证的通信）以及事务中断对策。对于安全通信部 302 的结构，用图 5 在后面进行说明。

[0150] 许可发行部 303 是一种处理部，按照来自用户终端 103 的请求进行许可 200 的发行处理。

[0151] 到上述为止，结束关于许可服务器 101 的整体结构的说明。

[0152] 其次，用图 5 说明许可服务器 101 中的安全通信部 302 的结构。在图 5 中，安全通信部 302 由安全通信控制部 501、事务日志数据库 502、特有信息记忆部 503、随机数发生部 504、加解密处理部 505 和通信部 506 构成。下面，说明安全通信部 302 的各个构成要素。

[0153] 安全通信控制部 501 是进行安全通信部 302 整体的控制的单元，安全通信控制部 501 进行用户终端 103 的认证处理、与用户终端 103 收发的数据的加密 / 解密处理、窜改检查处理等的控制。再者，安全通信控制部 501，在易失性处理器上管理图 6 中表示该一个例子的事务日志 600，而且，根据需要，进行将其记录到事务日志数据库 502 的处理。在因通信截断等而正在执行中的事务被中断的情况下，根据该记录在事务日志数据库 502 的信息进行规定的处理，从而可以使被中断的事务完了、或可以将被中断的事务回复到执行前的状态。

[0154] 在图 6 中，事务日志 600 由终端 ID401、正在处理中事务有无 601、正在处理中事务识别标记 602 和回退与否 603 构成。在终端 ID401 中，描述许可服务器 101 正在通信中的用户终端 103 的 ID。在正在处理中事务有无 601 中，描述是否有正在处理中的事务。在正在处理中事务识别标记 602 中，描述分配给正在处理中的事务的“0”或“1”的值。在本实施例中假设，各个事务被交替赋予“0”或“1”。在回退与否 603 中描述一种信息，该信息表示，在正在处理中的事务以未完了的状态下结束时，是否需要将许可数据库 301 回退。在此，回退 (Roll Back) 是指，在数据库发生障碍时，将数据回退到所记录的检查点，从而重新开始处理。在图 6 中表示，许可服务器 101，与终端 ID401 为“0001”的用户终端 103 正在通信中，而且表示，有正在处理中的事务 ；分配给该事务的正在处理中事务识别标记 602 的值是“0”；在该事务以未完了的状态下结束时，也不需要将许可数据库 301 回退。

[0155] 事务日志数据库 502 是一种数据库，以非易失性记录介质被实现，如图 7 中表示该一个例子，记录终端 ID401 和正在处理中事务识别标记 602 的组。

[0156] 特有信息记忆部 503 记忆，包含以公开密钥加解密方式的许可服务器 101 特有的公开密钥 KDs 的服务器公开密钥证书、许可服务器 101 特有的秘密密钥 KEs 和认证局公开密钥证书。服务器公开密钥证书是在许可服务器 101 的公开密钥 KDs 上施加了认证局的签名的。在本实施例中假设，对于公开密钥证书的格式，采用一般的 X.509 证书格式。并且，对于公开密钥加解密方式以及 X.509 证书格式，在 ITU-T 文件 X.509 “TheDirecrory : Public-key and attribute certificate frameworks”中有详细描述。

[0157] 随机数发生部 504，生成随机数。

[0158] 加解密处理部505进行数据的加密、解密、签名生成、签名验证、会话(session)密钥生成用参数的生成、会话密钥的生成。对于数据的加密以及解密算法，使用AES(Advanced Encryption Standard)，对于签名生成以及签名验证算法，使用EC-DSA(Elliptic Curve Digital SignatureAlgorithm)。对于AES，在National Institute Standard and Technology(NIST)，FIPS Publication 197中有详细描述，对于EC-DSA，在IEEE 1363Standard中有详细描述。

[0159] 加解密处理部505，在进行数据的加密/解密的情况下，将AES密钥和明文/加密数据分别输入，而将用AES密钥来进行加密/解密后的数据分别输出。而且，在进行签名生成/验证的情况下，将签名对象数据/签名验证数据和秘密密钥/公开密钥分别输入，而将签名数据/验证结果分别输出。再者，在进行会话密钥生成用参数的生成的情况下，将随机数输入，而将Diffie-Hellman参数输出。而且，在进行会话密钥的生成的情况下，将随机数和Diffie-Hellman参数输入，而将会话密钥输出。在此，对于会话密钥的生成，使用EC-DH(Elliptic Curve Diffie-Hellman)。对于EC-DH的算法，在所述的IEEE 1363Standard中有详细描述。

[0160] 通信部506是一种单元，与用户终端103进行通信。

[0161] 到上述为止，结束关于许可服务器101中的安全通信部302的结构的说明。

[0162] 其次，用图8说明本实施例的用户终端103的结构。在图8中，用户终端103由许可蓄积部801、内容蓄积部802、安全通信部803、许可获得部804、内容获得部805、内容输出控制部806和内容输出部807构成。下面，说明各个构成要素。

[0163] 许可蓄积部801是一种单元，蓄积从许可服务器101获得的许可200。假设，许可蓄积部801，将许可200安全地蓄积到被反窜改化后的存储器内等。

[0164] 内容蓄积部802是一种单元，蓄积从内容服务器102获得的加密内容。

[0165] 安全通信部803进行许可服务器101的认证、许可服务器101和用户终端103间的隐藏通信（进行窃听、窜改的防止和通信对方的认证的通信）以及事务中断对策。对于安全通信部803的结构，用图9在后面进行说明。

[0166] 许可获得部804是一种单元，进行对许可服务器101的许可200的发行请求处理。

[0167] 内容获得部805是一种单元，从内容服务器102获得内容。

[0168] 内容输出控制部806是一种单元，根据许可200控制内容的输出。

[0169] 内容输出部807是一种单元，根据内容输出控制部806的指示，使用 内容密钥205来解密并输出内容。

[0170] 到上述为止，结束关于用户终端103的整体结构的说明。

[0171] 其次，用图9说明用户终端103中的安全通信部803的结构。在图9中，安全通信部803由安全通信控制部901、事务日志数据库902、特有信息记忆部903、随机数发生部904、加解密处理部905和通信部906构成。下面，说明安全通信部803的各个构成要素。

[0172] 安全通信控制部901是进行安全通信部803整体的控制的单元，安全通信控制部901进行许可服务器101的认证处理、与许可服务器101收发的数据的加密/解密处理、窜改检查处理等的控制。再者，安全通信控制部901，在易失性处理器上管理图10中表示该一个例子的事务日志1000，而且，根据需要，进行将事务日志1000记录到事务日志数据库902的处理。在因通信截断等而正在执行中的事务被中断的情况下，根据该记录在事务日志数

据库 902 的信息进行规定的处理，从而可以使被中断的事务完了、或可以将被中断的事务回复到执行前的状态。

[0173] 在图 10 中，事务日志 1000 由服务器 ID1001、正在处理中事务识别标记 602 构成。在服务器 ID1001 中，描述用户终端 103 正在通信中的许可服务器 101 的 ID。在正在处理中事务识别标记 602 中，与事务日志 600 相同，描述分配给正在处理中的事务的“0”或“1”的值。在图 10 中表示，用户终端 103，与服务器 ID1001 为“0001”的许可服务器 101 正在通信中，而且表示，分配给正在处理中事务的正在处理中事务识别标记 602 的值是“0”。

[0174] 事务日志数据库 902 是一种数据库，以非易失性记录介质被实现，如图 11 中表示该一个例子，记录服务器 ID1001 和正在处理中事务识别标记 602 的组。

[0175] 特有信息记忆部 903 记忆，包含以公开密钥加解密方式的用户终端 103 特有的公开密钥 KDc 的终端公开密钥证书、用户终端 103 特有的秘密密钥 KEc 和认证局公开密钥证书。终端公开密钥证书是在用户终端 103 的公开密钥 KDc 上施加了认证局的签名的。对于公开密钥证书的格式，与许可服务器 101 相同，采用 X.509 证书格式。

[0176] 随机数发生部 904，生成随机数。

[0177] 加解密处理部 905 进行数据的加密、解密、签名生成、签名验证、会话密钥生成用参数的生成、会话密钥的生成。加解密处理部 905 的输入、输出，与许可服务器 101 的加解密处理部 505 相同。

[0178] 通信部 906 是一种单元，与许可服务器 101 进行通信。

[0179] 到上述为止，结束关于用户终端 103 中的安全通信部 803 的结构的说明。

[0180] 到上述为止，结束关于本实施例的数字内容分发系统的说明。

[0181] 其次，参照流程图说明本发明的数字内容系统的处理。

[0182] 首先，参照图 12 以及图 13 说明本实施例的用户终端 103 从许可服务器 101 获得许可 200 的处理的概要。

[0183] 图 12 是，在用户终端 103 和许可服务器 101 间开始通信时在事务日志数据库 902 没有记录日志的情况下的许可获得处理的概要的说明图。

[0184] 图 13 是，在用户终端 103 和许可服务器 101 间开始通信时在事务日志数据库 902 记录日志的情况下的许可获得处理的概要的说明图。

[0185] 用户终端 103 和许可服务器 101 间的通信，均由从用户终端 103 开始的请求消息、和应对请求消息而从许可服务器 101 回信的应答消息构成。请求和应答的对被称为相位，如图 12、图 13 所示由五种相位构成。下面，说明各个相位的概要。

[0186] 首先，说明认证相位 P1。认证相位 P1 是相互认证用的相位，在用户终端 103 和许可服务器 101 间建立会话后，只在最初进行一次。在认证相位 P1 中，用户终端 103，向许可服务器 101 发送作为初次请求消息的认证信息 A，该认证信息 A 是为了由许可服务器 101 认证用户终端 103 所需要的信息。许可服务器 101，验证认证信息 A 后发送认证信息 B，该认证信息 B 是为了由用户终端 103 认证许可服务器 101 所需要的信息。用户终端 103 验证认证信息 B。到上述为止，结束认证相位 P1 的说明。

[0187] 其次，说明认证、请求相位 P2。认证、请求相位 P2 是一种相位，在开始认证相位 P1 时在事务日志数据库 902 没有记录日志的情况下，认证相位 P1 后只进行一次。在认证、请求相位 P2 中，用户终端 103，在向许可服务器 101 发送许可请求消息的同时，发送认证信息

C 以及事务识别标记 T，该认证信息 C 是为了确定相互认证所需要的信息。在此，所发送的事务识别标记 T 中设定初始值（在本实施例中为“0”）。许可服务器 101，在判断为开始新的事务、而有上次中断了的事务的情况下，进行将许可数据库 301 或事务日志数据库 502 的状态，回复到该事务开始前的状态的处理（以后，称为取消处理），然后，向用户终端 103 发送包含许可 200 的应答消息，以作为对请求消息的应答。接收了应答消息的用户终端 103，在不连续进行事务处理的情况下，通过发送提交消息，从而移向提交相位 P4。而且，在连续进行事务处理的情况下，不发送提交消息而移向请求相位 P3。

[0188] 请求相位 P3 是在同一会话内处理二个以上的事务的情况下发生的相位。即，在多次进行许可请求的情况下，使用请求相位 P3。请求相位 P3，按照需要的事务数被反复进行。在该请求相位 P3 中，提交消息不被发送，取代提交消息而将值反转后的事务识别标记 T，与下一个请求相位 P3 中的许可请求消息一起被发送。假设，许可服务器 101，在请求相位 P3 中，在接收了针对在上次的请求相位 P3 接收了的事务识别标记 T、将值反转后的事务识别标记 T 的情况下，进行对上次的事务的提交处理。在最后的请求相位 P3 完了后，移向提交相位 P4。

[0189] 提交相位 P4 是一种相位，在全部事务处理结束后，在许可服务器 101 中用于确定事务处理的完了。在提交相位 P4 中，用户终端 103 向许可服务器 101 发送提交消息。接收了提交消息的许可服务器 101 进行提交处理。

[0190] 其次，说明认证、提交相位 P5。认证、提交相位 P5 是一种相位，在开始认证相位 P1 时在事务日志数据库 902 记录日志的情况下，认证相位 P1 后只进行一次。在认证、提交相位 P5 中，用户终端 103，在向许可服务器 101 发送提交消息的同时，发送认证信息 C 以及事务识别标记 T，该认证信息 C 是为了确定相互认证所需要的信息。许可服务器 101，按照事务识别标记 T 的值，进行提交处理或取消处理。

[0191] 到上述为止，结束本实施例的用户终端 103，从许可服务器 101 获得许可 200 时的五种相位中的处理的概要说明。

[0192] 下面，详细说明在 P1 ～ P5 的各个通信相位中进行的处理。

[0193] 首先，参照图 14 所示的流程图说明在认证相位 P1 中进行的处理。

[0194] S1401：在被用户 β 指示从许可服务器 101 获得许可 200 的情况下，安全通信部 803 中包含的安全通信控制部 901，参照事务日志数据库 902，确认是否有与所指定的许可服务器 101 对应的日志。在有对应的日志的情况下，将其作为事务日志 1000 读出到由自身管理的易失性存储器上。

[0195] S1402：安全通信控制部 901，生成询问消息，并通过通信部 906 向许可服务器 101 发送该询问消息，该询问消息包含随机数发生部 904 所生成的随机数 Rc、和特有信息记忆部 903 所记忆的终端公开密钥证书。

[0196] S1403：许可服务器 101 的安全通信部 302 中包含的安全通信控制部 501，在通过通信部 506 从用户终端 103 接收了包含随机数 Rc 和终端公开密钥证书的询问消息的情况下，首先，通过将特有信息记忆部 503 所记忆的认证局公开密钥证书和所述终端公开密钥证书提供给加解密处理部 505，从而进行所述终端公开密钥证书的签名验证。

[0197] S1404：在 S1403 中的签名验证的结果为验证失败的情况下，进入 S1409 的处理。在 S1403 中的签名验证的结果为验证成功的情况下，进入 S1405 的处理。

[0198] S1405：安全通信控制部501，在随机数生成部504生成随机数Rs、Rs2，在加解密处理部505输入随机数Rs2，并生成Diffie-Hellman参数DHs。

[0199] S1406：安全通信控制部501，在加解密处理部505生成使从用户终端103接收的随机数Rc和在S1405所生成的DHs连接的数据（公式1）的、依据许可服务器101特有的秘密密钥KEs的签名（公式2）。

[0200] Rc||DHs （公式1）

[0201] S(KEs，Rc||DHs) （公式2）

[0202] 在此，符号“||”表示数据的连接。而且，S(A，B)表示，使用生成签名的算法S的、依据秘密密钥A的、针对数据B的签名的生成。

[0203] S1407：安全通信控制部501，参照事务日志数据库502，确认是否有与正在通信中的用户终端103对应的日志。在有对应的日志的情况下，将其作为事务日志600读出到由自身管理的易失性存储器上，并删除从事务日志数据库502读出的日志。并且，此时假设，在正在处理中事务有无601中设定“有”；在回退与否603中设定“要”。另一方面，在没有与事务日志数据库502对应的日志的情况下，在由自身管理的易失性存储器上生成事务日志600。在该情况下，假设，在终端ID401中设定正在通信中的用 户终端103的ID；在正在处理中事务有无601中设定“无”；在正在处理中事务识别标记602中设定“0”；在回退与否603中设定“不要”。

[0204] S1408：安全通信控制部501生成响应－询问消息，并通过通信部506向用户终端103发送该响应－询问消息，该响应－询问消息中包含在S1405所生成的随机数Rs以及Diffie-Hellman参数DHs、特有信息记忆部503所记忆的服务器公开密钥证书和在S1406所生成的签名（公式2）。

[0205] S1409：安全通信控制部501生成错误消息，并通过通信部506向用户终端103发送该错误消息。

[0206] S1410：安全通信控制部901确认从许可服务器101接收的消息是否是响应－询问消息。在从许可服务器101接收的消息是响应－询问消息的情况下，进入S1411的处理。在从许可服务器101接收的消息不是响应－询问消息的情况下，就结束处理。

[0207] S1411：安全通信控制部901，通过将特有信息记忆部903所记忆的认证局公开密钥证书、和响应－询问消息中包含的服务器公开密钥证书提供给加解密处理部905，从而进行所述服务器公开密钥证书的签名验证。

[0208] S1412：在S1411中的签名验证的结果为验证失败的情况下，就结束处理。在S1411中的签名验证的结果为验证成功的情况下，进入S1413的处理。

[0209] S1413：安全通信控制部901，生成将在S1402所制作的随机数Rc和响应－询问消息中包含的DHs结合的数据（公式3），向加解密处理部905输入所述数据（公式3）、响应－询问消息中包含的签名数据（公式2）以及服务器公开密钥证书，进行签名数据（公式2）的验证。

[0210] Rc||DHs （公式3）

[0211] S1414：在S1413中的签名验证的结果为验证失败的情况下，就结束处理。在S1413中的签名验证的结果为验证成功的情况下，用户终端103确实知道通信对方是许可服务器101（通信对方的认证）。在此情况下，进入S1415的处理。

[0212] S1415：安全通信控制部 901，在随机数发生部 904 生成随机数 Rc2，在加解密处理部 905 输入所生成的随机数 Rc2，并生成 Diffie-Hellman 参数 DHc。

[0213] S1416：安全通信控制部 901，根据响应－询问消息中包含的 DHs、和在 S1415 所生成的 Rc2，在加解密处理部 905 生成会话密钥 KS。

[0214] S1417：安全通信控制部 901，在加解密处理部 905 生成使从响应－询问消息中包含的的随机数 Rs 和在 S1415 所生成的 DHc 连接的数据（公式 4）的、依据用户终端 103 特有的秘密密钥 KEc 的签名（公式 5）。

[0215] Rs||DHc （公式 4）

[0216] S(KEc，Rs||DHc) （公式 5）

[0217] S1418：安全通信控制部 901，参照事务日志数据库 902，确认是否有与正在通信中的许可服务器 101 对应的日志。在有与正在通信中的许可服务器 101 对应的日志的情况下，进入认证、提交相位 P5 的处理。在没有与正在通信中的许可服务器 101 对应的日志的情况下，进入认证、请求相位 P2 的处理。

[0218] 到上述为止，结束关于认证相位 P1 中进行的处理的说明。

[0219] 其次，参照图 15 所示的流程图说明在认证、请求相位 P2 中进行的处理。

[0220] S1501：安全通信控制部 901，在自身管理的易失性存储器上生成事务日志 1000。在该情况下，假设，在服务器 ID1001 中设定正在通信中的许可服务器 101 的 ID；正在处理中事务识别标记 602 中设定初始值（在本实施例中为“0”）。

[0221] S1502：许可获得部 804 生成许可获得请求消息 Mreq。假设，在许可获得请求消息 Mreq 中包含希望获得的许可 200 的许可 ID201。

[0222] S1503：安全通信控制部 901，使序号 Seq、事务识别标记 T、在 S1502 所生成的许可获得请求消息 Mreq 和与它们对应的散列值 h 连接，用会话密钥 KS 来将其加密，从而生成加密数据（公式 6）。

[0223] E(KS，Seq||T||Mreq||h) （公式 6）

[0224] 并且，E(X，Y) 表示，使用加密算法 E 的、依据加密密钥 X 的、数据 Y 的加密。

[0225] 在此，假设，在序号 Seq 中设定“0”。假设，序号 Seq，以后，在同一会话中每次发送以及接收消息时，都加上 1。而且假设，在事务识别标记 T 中设定事务日志 1000 的正在处理中事务识别标记 602 的值。

[0226] S1504：安全通信控制部 901，生成响应－询问消息，并通过通信部 906 向许可服务器 101 发送该响应－询问消息，该响应－询问消息中包含在 S1415 所生成的 DHc、在 S1417 所生成的签名（公式 5）和在 S1503 所生成的加密数据（公式 6）。

[0227] S1505：许可服务器 101 的安全通信部 302 中包含的安全通信控制部 501，在通过通信部 506 从用户终端 103 接收包含 Diffie-Hellman 参数 DHc、签名数据以及加密数据的响应－询问消息的情况下，生成将在 S1405 所制作的随机数 Rs 和所述 DHc 结合的数据（公式 7），向加解密处理部 505 输入所述生成数据（公式 7）、所述签名数据以及终端公开密钥证书，进行签名数据的验证。

[0228] Rs||DHc （公式 7）

[0229] S1506：S1505 中的签名验证的结果为验证失败的情况下，进入 S1513 的处理。在 S1505 中的签名验证的结果为验证成功的情况下，进入 S1507 的处理。

[0230] S1507：安全通信控制部 501，根据响应－询问消息中包含的 DHc、和在 S1405 所生成的 Rs2，在加解密处理部 505 生成会话密钥 KS。然后，向加解密处理部 505 输入响应－询问消息中包含的加密数据和所生成的会话密钥 KS，进行加密数据的解密。

[0231] S1508：安全通信控制部 501，进行序号 Seq 和散列值 h 的验证。

[0232] S1509：S1508 中的验证的结果为验证失败的情况下，进入 S1513 的处理。在 S1508 中的验证的结果为验证成功的情况下，进入 S1510 的处理。

[0233] S1510：安全通信控制部 501，确认事务日志 600 的正在处理中事务有无 601 的值。在确认结果是正在处理中事务有无 601 的值为“有”的情况下，进入 S1511 的处理。在正在处理中事务有无 601 的值为“无”的情况下，进入 S1512 的处理。

[0234] S1511：安全通信控制部 501，执行后述的取消处理。

[0235] S1512：安全通信控制部 501，执行后述的应答消息生成、发送处理。

[0236] S1513：安全通信控制部 501，生成错误消息，通过通信部 506 向用户终端 103 发送该错误消息。

[0237] S1514：安全通信控制部 901，确认从许可服务器 101 接收的消息是 否是应答消息。在从许可服务器 101 接收的消息是应答消息的情况下，进入 S1515 的处理。从许可服务器 101 接收的消息不是应答消息的情况下，就结束处理。

[0238] S1515：安全通信控制部 901，执行后述的应答消息接收时处理。

[0239] S1516：在 S1515 的应答消息接收时处理中成功了序号 Seq、散列值 h 的验证的情况下，进入 S1517 的处理。另一方面，在序号 Seq、散列值 h 的验证失败了的情况下，就结束处理。

[0240] S1517：安全通信控制部 901，在继续进行许可请求的情况下，进入请求相位 P3 的处理。另一方面，在不继续进行许可请求的情况下，进入提交相位 P4 的处理。

[0241] 到上述为止，结束关于认证、请求相位 P2 中进行的处理的说明。

[0242] 其次，参照图 16 所示的流程图详细说明在图 15 中的 S1511 的取消处理。

[0243] S1601：安全通信控制部 501，指示许可发行部 303 进行许可数据库 301 的回退处理。假设，该回退指示中包含正在通信中的用户终端 103 的终端 ID401。接收了指示的许可发行部 303，参照许可数据库 301，从和回退指示中包含的终端 ID401 相关联的信息中检索待提交标记 403 的值为“1”的信息，并将该值变更为“0”。

[0244] S1602：安全通信控制部 501，将事务日志 600 的正在处理中事务有无 601 的值设定为“无”。

[0245] 并且，对于取消处理，说明了进行许可数据库 301 的回退处理，但是，不仅限于此，在另外管理、更新需要回退的信息的情况下，可以回退该信息。

[0246] 到上述为止，结束关于取消处理的说明。

[0247] 其次，参照图 17 所示的流程图详细说明在图 15 中的 S1512 的应答消息生成、发送处理。

[0248] S1701：安全通信控制部 501，向许可发行部 303 发送解密后的许可获得请求消息 Mreq，来通知接收了新的许可获得请求。接受了通知的许可发行部 303，参照许可数据库 301，判断能否发行许可 200。假设，许可发行部 303，在依据许可获得请求消息 Mreq 请求发行的许可 200 的发行 可能次数 402 为 1 以上、且待提交标记 403 为“0”的情况下，判断为

可以发行许可 200。在判断结果是可以发行许可的情况下，进入 S1702 的处理。另一方面，在不能发行许可的情况下，进入 S1705 的处理。

[0249] S1702：许可发行部 303，确认发行可能次数 402 是否有限。在判断结果是发行可能次数 402 有限的情况下，进入 S1703 的处理。在发行可能次数 402 无限的情况下，进入 S1705 的处理。

[0250] S1703：许可发行部 303，在用户终端 103 没有接收要发行的许可 200 的情况下，判断为需要许可数据库 301 的回退处理。

[0251] S1704：许可发行部 303，将要发行的许可 200 的待提交标记 403 的值变更为“1”。

[0252] S1705：许可发行部 303，在用户终端 103 没有接收要发行的许可 200 的情况下，也判断为不需要许可数据库 301 的回退处理。

[0253] S1706：许可发行部 303，生成许可请求响应 Mres。并且假设，许可发行部 303，在 S1701 判断为可以发行许可的情况下，生成包含许可 200 的许可请求响应消息 Mres，在 S1701 判断为不能发行许可的情况下，生成通知不能发行许可的许可请求响应 Mres。许可发行部 303，向安全通信控制部 501 发送，所生成的许可请求响应 Mres、和在 S1703 以及 S1705 所判断的回退与否。

[0254] S1707：安全通信控制部 501，将事务日志 600 的正在处理中事务有无 601 的值设定为“有”；将正在处理中事务识别标记 602 的值设定为从用户终端 103 发送来的事务识别标记 T 的值；将回退与否 603 设定为在 S1706 所通知的值。

[0255] S1708：安全通信控制部 501，使序号 Seq、事务识别标记记忆指示 TR、在 S1706 所生成的许可获得请求响应消息 Mres 和与它们对应的散列值 h 连接，用会话密钥 KS 来将其加密，从而生成加密数据（公式 8）。事务识别标记记忆指示 TR 是一种信息，表示在用户终端 103 中是否需要将事务日志 1000 记录到事务日志数据库 902。假设，安全通信控制部 501，在事务日志 600 的回退与否 603 为“要”的情况下，在事务识别标记记忆指示 TR 设定“要记录”；在回退与否 603 为“不要”的情况下，在事务识别标记记忆指示 TR 设定“不要记录”。通过事务识别标记记忆指示 TR，通 知向事务日志数据库 902 的记录与否，从而可以抑制向事务日志数据库 902 的不必要的记录。

[0256] $E(KS, Seq||TR||Mres||h)$ （公式 8）

[0257] 然后，安全通信控制部 501，生成包含所生成的加密数据（公式 8）的应答消息，通过通信部 506 向用户终端 103 发送该应答消息。

[0258] 并且，也可以使从许可服务器 101 发送的应答消息包含事务识别标记的保持期限。

[0259] 在图 28 以及 29 中表示向事务日志 600 还赋予了保持期限的情况下的参考图。

[0260] 许可服务器所管理的事务日志 600 被附加保持期限 2801，事务日志数据库 502 被附加保持期限 2802，并且，用户终端所管理的事务日志 1000 被附加保持期限 2901，事务日志数据库 902 被附加保持期限 2902。作为该保持期限的设定例可以设想，系统特有的长度（记录日志后一个月等），按照利用条件赋予（在到三月为止可以发行许可的情况下，设定为三月末）等。据此，以往存在的问题是，许可服务器 101 或用户终端 103，在即使有中断了的处理也停止运行等的情况下，不能清除事务日志等，但是，通过赋予保持期限，许可服务器 101 以及用户终端 103，由于在事务日志超过保持期限的情况下，可以删除事务日志，因

此可以适当地防止在许可服务器 101 以及用户终端 103 一直留下事务日志的情况。

[0261] 而且，许可服务器 101，判断在用户终端 103 是否需要将事务日志 1000 记录到事务日志数据库 902，通过应答消息中的事务识别标记记忆指示 TR 向用户终端 103 通知所述判断结果，但是，也可以按照所发送的许可 200 中包含的利用条件 204 的细节、或许可服务器 101 所管理的信息的更新的有无等进行所述的记录与否判断。例如，可以设想，在所发送的许可 200 的利用条件 204 为有状态的情况下，判断为“要记录”，在利用条件为无状态的情况下，判断为“不要”。而且，可以设想，在许可服务器 101 中，在随着许可 200 的发行更新所管理的信息的情况下，为“要记录”，在不更新的情况下，为“不要”。可以设想，作为许可服务器 101 所管理的、随着许可 200 的发行而更新的信息有，许可 200 的发行数、或许可 200 的发行履历等。

[0262] 而且，许可服务器 101，判断在用户终端 103 是否需要将事务日志 1000 记录到事务日志数据库 902，但是，也可以在许可服务器 101 不进行记录与否判断，而例如根据许可 200 的利用条件 204 的细节等，在用户终端 103 侧进行判断。

[0263] 到上述为止，结束关于应答消息生成、发送处理的说明。

[0264] 其次，参照图 18 所示的流程图详细说明在图 15 中的 S1515 的应答消息接收时处理。

[0265] S1801 ：安全通信控制部 901，向加解密处理部 905 输入应答消息中包含的加密数据和会话密钥 KS，并进行加密数据的解密。

[0266] S1802 ：安全通信控制部 901，进行序号 Seq 和散列值 h 的验证。

[0267] S1803 ：在 S1802 的验证结果为验证失败的情况下，就结束处理。在 S1802 的验证结果为验证成功的情况下，进入 S1804 的处理。

[0268] S1804 ：安全通信控制部 901，在事务日志数据库 902 中有与正在通信中的许可服务器 101 对应的日志的情况下，删除该日志。

[0269] S1805 ：安全通信控制部 901，参照在 S1801 所解密的数据中包含的事务识别标记记忆指示 TR，确认是否需要将事务日志 1000 记录到事务日志数据库 902。在确认结果为需要记录的情况下，进入 S1806 的处理。在不需要记录的情况下，进入 S1807 的处理。

[0270] S1806 ：安全通信控制部 901，将事务日志 1000 记录到事务日志数据库 902。

[0271] S1807 ：安全通信控制部 901，向许可获得部 804 发送在 S1801 所解密的加密数据中包含的许可获得请求响应消息 Mres。许可获得部 804，参照许可获得请求响应消息 Mres，确认是否获得了许可 200。在确认结果为获得了许可 200 的情况下，进入 S1808 的处理。以后，在用户终端 103 可以使用获得了的许可 200。另一方面，在没有获得许可 200 的情况下，就结束处理。

[0272] S1808 ：许可获得部 804，将许可 200 蓄积在许可蓄积部 801。

[0273] 到上述为止，结束关于应答消息接收时处理的说明。

[0274] 其次，参照图 19 所示的流程图说明在请求相位 P3 中进行的处理。

[0275] S1901 ：安全通信控制部 901，将易失性存储器上管理的事务识别标 记 T 中设定事务日志 1000 的正在处理中事务识别标记 602 的值反转。

[0276] S1902 ：许可获得部 804，生成许可获得请求消息 Mreq。假设，许可获得请求消息 Mreq 中包含希望获得的许可 200 的许可 ID201。

[0277] S1903：安全通信控制部901，使序号Seq、事务识别标记T、在S1902所生成的许可获得请求消息Mreq和与它们对应的散列值h连接，用会话密钥KS来将其加密，从而生成加密数据（公式6）。假设，在事务识别标记T中设定事务日志1000的正在处理中事务识别标记602的值。

[0278] S1904：安全通信控制部901，生成包含在S1903所生成的加密数据（公式6）的请求消息，通过通信部906向许可服务器101发送该请求消息。

[0279] S1905：安全通信控制部501，在接收请求消息的情况下，向加解密处理部505输入请求消息中包含的加密数据和会话密钥KS，并进行加密数据的解密。

[0280] S1906：安全通信控制部501，进行序号Seq和散列值h的验证。

[0281] S1907：在S1906的验证结果为验证失败的情况下，进入S1912的处理。在S1906的验证结果为验证成功的情况下，进入S1908的处理。

[0282] S1908：安全通信控制部501，确认事务日志600的正在处理中事务识别标记602的值、和在S1905所解密的加密数据中包含的事务识别标记T的值。在确认结果是事务识别标记T的值、和正在处理中事务识别标记602的值一致的情况下，进入S1911的处理。在事务识别标记T的值、和正在处理中事务识别标记602的值不一致的情况下，进入S1909的处理。

[0283] S1909：安全通信控制部501，执行后述的提交处理。

[0284] S1910：安全通信控制部501，执行所述的应答消息生成、发送处理。

[0285] S1911：安全通信控制部501，执行后述的应答消息生成、发送处理（重新发送）。

[0286] S1912：安全通信控制部501，生成错误消息，通过通信部506向用户终端103发送该错误消息。

[0287] S1913：安全通信控制部901，确认从许可服务器101接收的消息是否是应答消息。在从许可服务器101接收的消息是应答消息的情况下，进入S1914的处理。从许可服务器101接收的消息不是应答消息的情况下，就结束处理。

[0288] S1914：安全通信控制部901，执行所述的应答消息接收时处理。

[0289] S1915：在S1914的应答消息接收时处理中成功了序号Seq、散列值h的验证的情况下，进入S1916的处理。另一方面，在序号Seq、散列值h的验证失败了的情况下，就结束处理。

[0290] S1916：安全通信控制部901，在继续进行许可请求的情况下，再次执行请求相位P3的处理。另一方面，在不继续进行许可请求的情况下，进入提交相位P4的处理。

[0291] 到上述为止，结束关于请求相位P3中进行的处理的说明。

[0292] 其次，参照图20所示的流程图详细说明在图19中的S1909的提交处理。

[0293] S2001：安全通信控制部501，指示许可发行部303进行提交处理。假设，该提交指示中包含正在通信中的用户终端103的终端ID401。接收了指示的许可发行部303，参照许可数据库301，检索和提交指示中包含的终端ID401相关联的信息中是否有待提交标记403的值为“1”的许可200。在检索结果为检出待提交标记403的值为“1”的许可200的情况下，进入S2002的处理。在未检出待提交标记403的值为“1”的许可200的情况下，进入S2003的处理。

[0294] S2002：许可发行部303，将在S2001检出的许可200的待提交标记403的值变更

为“0”，并从发行可能次数 402 中减去 1。

[0295] S2003：安全通信控制部 501，将事务日志 600 的正在处理中事务有无 601 的值设定为“无”。

[0296] 并且，在 S2002 说明了更新许可数据库 301 中包含的信息，但是，不仅限于此，在另外管理随着许可 200 的发行而需要更新的信息的情况下，可以更新该信息。

[0297] 到上述为止，结束关于提交处理的说明。

[0298] 其次，参照图 21 所示的流程图详细说明在图 19 中的 S1911 的应答消息生成、发送处理（重新发送）。

[0299] S2101：安全通信控制部 501，向许可发行部 303 发送解密后的许可获得请求消息 Mreq，来通知接收了重新发送了的许可获得请求。接受了通知的许可发行部 303，参照许可数据库 301，判断能否发行许可 200。假 设，许可发行部 303，在通过许可获得请求消息 Mreq 请求发行的许可 200 的发行可能次数 402 为 1 以上的情况下，判断为可以发行许可 200。

[0300] S2102：许可发行部 303，生成许可请求响应 Mres。并且假设，许可发行部 303，在 S2101 判断为可以发行许可的情况下，生成包含许可 200 的许可请求响应消息 Mres，在 S2101 判断为不能发行许可的情况下，生成通知不能发行许可的许可请求响应 Mres。许可发行部 303，向安全通信控制部 501 发送，所生成的许可请求响应 Mres。

[0301] S2103：安全通信控制部 501，使序号 Seq、事务识别标记记忆指示 TR、在 S2102 所生成的许可获得请求响应消息 Mres 和与它们对应的散列值 h 连接，用会话密钥 KS 来将其加密，从而生成加密数据（公式 8）。假设，安全通信控制部 501，在事务日志 600 的回退与否 603 为“要”的情况下，在事务识别标记记忆指示 TR 设定“要记录”；在回退与否 603 为“不要”的情况下，在事务识别标记记忆指示 TR 设定“不要记录”。然后，安全通信控制部 501，生成包含所生成的加密数据（公式 8）的应答消息，通过通信部 506 向用户终端 103 发送该应答消息。

[0302] 到上述为止，结束关于应答消息生成、发送处理（重新发送）的说明。

[0303] 其次，参照图 22 所示的流程图说明在提交相位 P4 中进行的处理。

[0304] S2201：安全通信控制部 901，使序号 Seq、事务识别标记 T、提交命令 C 和与它们对应的散列值 h 连接，用会话密钥 KS 来将其加密，从而生成加密数据（公式 9）。假设，在事务识别标记 T 中设定事务日志 1000 的正在处理中事务识别标记 602 的值。

[0305] E(KS, Seq||T||C||h) （公式 9）

[0306] S2202：安全通信控制部 901，生成包含在 S2201 所生成的加密数据（公式 9）的提交消息，通过通信部 906 向许可服务器 101 发送该提交消息。

[0307] S2203：安全通信控制部 501，在接收提交消息的情况下，向加解密处理部 505 输入提交消息中包含的加密数据和会话密钥 KS，并进行加密数据的解密。

[0308] S2204：安全通信控制部 501，进行序号 Seq 和散列值 h 的验证。

[0309] S2205：在 S2204 的验证结果为验证失败的情况下，进入 S2208 的处理。在 S2204 的验证结果为验证成功的情况下，进入 S2206 的处理。

[0310] S2206：安全通信控制部 501，执行所述的提交处理。

[0311] S2207：安全通信控制部 501，使序号 Seq、事务识别标记 T、ACK 命令 A 和与它们对应的散列值 h 连接，用会话密钥 KS 来将其加密，从而生成加密数据（公式 10），生成包含所

生成的数据（公式 10）的 ACK 消息，通过通信部 506 向用户终端 103 发送该 ACK 消息。假设，在事务识别标记 T 中设定事务日志 600 的正在处理中事务识别标记 602 的值。

[0312] E(KS, Seq||T||A||h) （公式 10）

[0313] S2208：安全通信控制部 501，生成错误消息，通过通信部 506 向用户终端 103 发送该错误消息。

[0314] S2209：安全通信控制部 901，确认从许可服务器 101 接收的消息是否是 ACK 消息。在从许可服务器 101 接收的消息是 ACK 消息的情况下，进入 S2210 的处理。在从许可服务器 101 接收的消息不是 ACK 消息的情况下，就结束处理。

[0315] S2210：安全通信控制部 901，进行后述的 ACK 消息接收时处理。

[0316] 到上述为止，结束关于在提交相位 P4 中进行的处理的说明。

[0317] 其次，参照图 23 所示的流程图详细说明在图 22 中的 S2210 的 ACK 消息接收时处理。

[0318] S2301：安全通信控制部 901，向加解密处理部 905 输入 ACK 消息中包含的加密数据和会话密钥 KS，并进行加密数据的解密。

[0319] S2302：安全通信控制部 901，进行序号 Seq 和散列值 h 的验证。

[0320] S2303：在 S2302 的验证结果为验证失败的情况下，就结束处理。在 S2302 的验证结果为验证成功的情况下，进入 S2304 的处理。

[0321] S2304：安全通信控制部 901，从事务日志数据库 902 中删除关于正在处理中的事务的信息。

[0322] 到上述为止，结束关于 ACK 消息接收时处理的说明。

[0323] 其次，参照图 24 所示的流程图说明在认证、提交相位 P5 中进行的处理。

[0324] S2401：安全通信控制部 901，比较从正在通信中的许可服务器 101 接收的服务器公开密钥证书中包含的服务器 ID1001、和事务日志 1000 的服务器 ID1001，确认正在通信中的许可服务器 101 是否是应该发送提交 - 响应消息的许可服务器 101。在确认结果是从正在通信中的许可服务器 101 接收的服务器公开密钥证书中包含的服务器 ID1001、和事务日志 1000 的服务器 ID1001 一致的情况下，进入 S2402 的处理。另一方面，在从正在通信中的许可服务器 101 接收的服务器公开密钥证书中包含的服务器 ID1001、和事务日志 1000 的服务器 ID1001 不一致的情况下，就结束处理。

[0325] S2402：安全通信控制部 901，使序号 Seq、事务识别标记 T 和与它们对应的散列值 h 连接，用会话密钥 KS 来将其加密，从而生成加密数据（公式 11）。

[0326] E(KS, Seq||T||h) （公式 11）

[0327] 在此，假设，在序号 Seq 中设定“0”。假设，序号 Seq，以后，在同一会话中每次发送以及接收消息时，都加上 1。而且假设，在事务识别标记 T 中设定事务日志 1000 的正在处理中事务识别标记 602 的值。

[0328] S2403：安全通信控制部 901，生成提交 - 响应消息，通过通信部 906 向许可服务器 101 发送该提交 - 响应消息，该提交 - 响应消息中包含在 S1415 所生成的 DHc、在 S1417 所生成的签名（公式 5）和在 S2402 所生成的加密数据（公式 11）。

[0329] S2404：许可服务器 101 的安全通信部 302 中包含的安全通信控制部 501，在通过通信部 506 从用户终端 103 接收包含 Diffie-Hellman 参数 DHc、签名数据以及加密数据的

提交－响应消息的情况下，生成将在 S1405 所制作的随机数 Rs 和所述 DHc 结合的数据（公式 7），向加解密处理部 505 输入所述生成数据（公式 7）、所述签名数据以及终端公开密钥证书，进行签名数据的验证。

[0330] S2405：S2404 中的签名验证的结果为验证失败的情况下，进入 S2414 的处理。在 S2404 中的签名验证的结果为验证成功的情况下，进入 S2406 的处理。

[0331] S2406：安全通信控制部 501，根据提交－响应消息中包含的 DHc、和在 S1405 所生成的 Rs2，在加解密处理部 505 生成会话密钥 KS。然后，向加解密处理部 505 输入响应－询问消息中包含的加密数据和所生成的会话密钥 KS，进行加密数据的解密。

[0332] S2407：安全通信控制部 501，进行序号 Seq 和散列值 h 的验证。

[0333] S2408：S2407 中的验证的结果为验证失败的情况下，进入 S2414 的处理。在 S2407 中的验证的结果为验证成功的情况下，进入 S2409 的处理。

[0334] S2409：安全通信控制部 501，确认事务日志 600 的正在处理中事务有无 601 的值。在确认结果是正在处理中事务有无 601 的值为“有”的情况下，进入 S2410 的处理。在正在处理中事务有无 601 的值为“无”的情况下，进入 S2413 的处理。

[0335] S2410：安全通信控制部 501，确认事务日志 600 的正在处理中事务识别标记 602 的值、和在 S2404 所解密的加密数据中包含的事务识别标记 T 的值。在确认结果是事务识别标记 T 的值、和正在处理中事务识别标记 602 的值一致的情况下，进入 S2412 的处理。在事务识别标记 T 的值、和正在处理中事务识别标记 602 的值不一致的情况下，进入 S2411 的处理。

[0336] S2411 安全通信控制部 501，执行所述的取消处理。

[0337] S2412：安全通信控制部 501，执行所述的提交处理。

[0338] S2413：安全通信控制部 501，使序号 Seq、事务识别标记 T、ACK 命令 A 和与它们对应的散列值 h 连接，用会话密钥 KS 来将其加密，从而生成加密数据（公式 10），生成包含所生成的数据（公式 10）的 ACK 消息，通过通信部 506 向用户终端 103 发送该 ACK 消息。假设，在事务识别标记 T 中设定事务日志 600 的正在处理中事务识别标记 602 的值。

[0339] S2414：安全通信控制部 501，生成错误消息，通过通信部 506 向用户终端 103 发送该错误消息。

[0340] S2415：安全通信控制部 901，确认从许可服务器 101 接收的消息是否是 ACK 消息。在从许可服务器 101 接收的消息是 ACK 消息的情况下，进入 S2416 的处理。在从许可服务器 101 接收的消息不是 ACK 消息的情况下，就结束处理。

[0341] S2416：安全通信控制部 901，执行所述的 ACK 消息接收时处理。

[0342] 到上述为止，结束关于在认证、提交相位 P5 中进行的处理的说明。

[0343] 其次，参照图 25 所示的流程图说明在许可服务器 101 检测到通信截断时的处理。

[0344] S2501：安全通信控制部 501，确认事务日志 600 的正在处理中事务 有无 601 的值，来确认在通信截断了的用户终端 103 间是否有正在处理中的事务。在确认结果是有正在处理中的事务的情况下，进入 S2502 的处理。另一方面，在没有正在处理中的事务的情况下，就结束处理。

[0345] S2502：安全通信控制部 501，确认事务日志 600 的回退与否 603 的值，来确认在通信截断了的用户终端 103 间正在处理中的事务是否是需要回退的事务。在确认结果是为需

要回退的事务的情况下，进入 S2503 的处理。在为不需要回退的事务的情况下，就结束处理。

[0346] S2503 ：安全通信控制部 501，将通信截断了的用户终端 103 的终端 ID401、和正在处理中事务识别标记 602 的组，记录在事务日志数据库 502。

[0347] 到上述为止，结束关于许可服务器 101 检测到通信截断时的处理的说明。

[0348] 并且，在本实施例的说明中，在发行可能次数 402 为无期限的情况下，不需要回退、且在中事务识别标记记忆指示 TR 设定“不要记录”，但是，不仅限于此，可以按照其它的规定的规则来设定。例如，可以设想，在要发行的许可 200 的利用条件类别 203 为“无状态”的情况下，不需要回退、且在中事务识别标记记忆指示 TR 设定“不要记录”等。

[0349] 而且，安全通信控制部 501 也可以，在对应来自用户终端 103 的消息而发送了消息的情况下，记忆该消息，并且，在判断为下次接收了的消息是重新发送了的前一个消息的情况下，重新发送所记忆的消息。

[0350] 并且，虽然说明了，在许可数据库 301 中，许可 200，和终端 ID401 相关联而被管理，但是，不仅限于此，可以和将用户 β 或用户终端 103 成组的域相关联。

[0351] 而且，从用户终端 103 向许可服务器 101 发送的许可获得请求消息 Mreq，也可以是为规定的工作（例如，再生请求或输出请求）的允许请求。具体而言，可以设想，许可服务器 101 作为对许可获得请求消息 Mreq 的响应，向用户终端发送内容密钥、可保持内容密钥的期限、控制信息等。可以设想，在来自用户终端 103 的允许请求是再生请求的情况下，所述控制信息是向各个端子的输出的信息 (CCI(Copy Control Information) 或 Macrovision 信号的 ON/OFF 的控制等），在来自用户终端 103 的允许请求是许可或内容的向记录介质等的输出请求的情况下，所述控制信息是接 受输出方的利用条件（在写在 DVD 的情况下，向 DVD 上的 CCI 设定的值等）。

[0352] 而且，许可服务器 101，可以按照被用户终端 103 请求允许的工作的细节，来进行事务日志的记录与否判断。可以设想，例如，在再生请求的情况下，将事务日志的记录变为“不要”，在输出请求的情况下，将事务日志的记录变为“要”。

[0353] 而且，如图 30 所示，用户终端 103，在从许可服务器 101 接受不需要记录事务日志的通知的情况下，可以省略提交消息的发送。在该情况下，在分发在许可服务器 101 或用户终端 103 不需要记录事务日志的许可 200 的情况下，除了省略事务日志的重写次数以外，还可以省略提交消息以后的通信处理，从而可以减少通信次数。

[0354] 并且，虽然说明了，在用户终端 103 中，可以使用从许可服务器 101 获得的许可 200 的定时是接收许可 200 的时刻，但是，不仅限于此，也可以在接收 ACK 消息的时刻可以使用。而且，也可以是，按照事务识别标记记忆指示 TR 的值来变更可以使用的定时。可以设想，例如，在事务识别标记记忆指示 TR 的值为“不要记录”的情况下，处于在接收许可 200 的时刻可以使用的状态，在事务识别标记记忆指示 TR 的值为“要记录”的情况下，如图 31 所示，在接收许可 200(3102) 时使许可 200 和事务日志相关联而处于锁定状态（不可使用的状态），在接收对提交消息 (3103) 的 ACK 消息 (3104) 后使许可 200 处于解锁状态（可以使用的状态）。在该情况下，在用户终端 103 侧，由于处于到接收 ACK 消息为止不可使用许可 200 的状态，因此即使从事务日志数据库 902 清除事务日志，许可 200 也不会被重复获得。因此，即使没有由安全命令的事务日志清除指示，也可以根据非安全的信息，并依据用户 β 的意

思，从事务日志数据库 902 中清除事务日志。

[0355] 而且，再者，在用户终端 103 中，作为从从事务日志数据库 902 中删除事务日志的其它方法的例子，可以设想，(1) 以 SAC 上的命令，被规定的服务器指示后删除，(2) 以 SAC 以外的通信（例如，HTTP 等），得到对删除命令由规定的事业者签名的数据后删除等。在该情况下，可以设想，跟着事务日志的删除，被相关联而锁定的许可 200 也被删除。

[0356] 而且，虽然说明了，对于各个消息中包含的散列值 h，只将消息的一部分作为计算对象，但是，不仅限于此，也可以将消息全体作为计算对象。而且，在该情况下，也可以是，在用户终端 103 以及许可服务器 101 中，在确认接收了的消息是哪种消息时，预先进行散列值 h 的验证。

[0357] （其它变形例）

[0358] 并且，虽然，根据所述实施例说明了本发明，但是，当然本发明不仅限于所述的实施例。本发明也包含如下情况。

[0359] (1) 具体而言，所述的各个装置是由微型处理器、ROM、RAM、硬盘器件、显示器件、键盘、鼠标等构成的计算机系统。所述 RAM 或硬盘器件，记忆计算机程序。通过所述微型处理器根据所述计算机程序进行工作，从而各个装置实现其功能。在此，为了实现所述的功能，计算机程序是使多个指令码组合而构成的，所述多个指令码表示对计算机的指示。

[0360] (2) 构成所述的各个装置的构成要素的一部分或全部，可以由一个系统 LSI(Large Scale Integration：大规模集成电路）构成。系统 LSI 是一种超多功能 LSI，将多个构成部集成在一个芯片上而被制造，具体而言，是包含微型处理器、ROM、RAM 等而构成的计算机系统。所述 RAM，记忆计算机程序。通过所述微型处理器根据所述计算机程序进行工作，从而系统 LSI 实现其功能。

[0361] (3) 构成所述的各个装置的构成要素的一部分或全部，也可以由对各个装置可装卸的 IC 卡或单体的模块。所述 IC 卡或所述模块是，由微型处理器、ROM、RAM 等构成的计算机系统。所述 IC 卡或所述模块，可以包含所述的超多功能 LSI。通过所述微型处理器根据所述计算机程序进行工作，从而所述 IC 卡或所述模块实现其功能。该 IC 卡或该模块，可以具有反窜改性。

[0362] (4) 本发明，也可以是如上所示的方法。而且，可以是由计算机实现这些方法的计算机程序，也可以是由所述计算机程序而成的数字信号。

[0363] 而且，本发明，可以将所述计算机程序或所述数字信号记录到计算机可读的记录介质，例如是软盘、硬盘、CD-ROM、MO、DVD、DVD-RAM、BD(Blu-ray Disc)、半导体存储器等。而且，也可以是记录在这些记录介质的所述数字信号。

[0364] 而且，本发明，可以将所述计算机程序或所述数字信号，通过以电信电路、无线或有线通信电路、互联网为代表的网络、数据广播等来传输。

[0365] 而且，本发明可以是具备微型处理器和存储器的计算机系统，所述存储器记忆所述计算机程序，所述微型处理器根据所述计算机程序进行工作。

[0366] 而且，本发明也可以，将所述程序或所述数字信号记录到所述记录介质而迁移，或者，将所述程序或所述数字信号通过所述网络等迁移，从而由独立的其它计算机系统实施。

[0367] (5) 也可以将所述实施例以及所述变形例分别组合。

[0368] 本发明涉及的许可管理装置以及方法，有用于由数字广播、CATV、互联网等的内容分发服务接收终端、或由 DVD 等包装媒体的内容分发服务接收终端等。

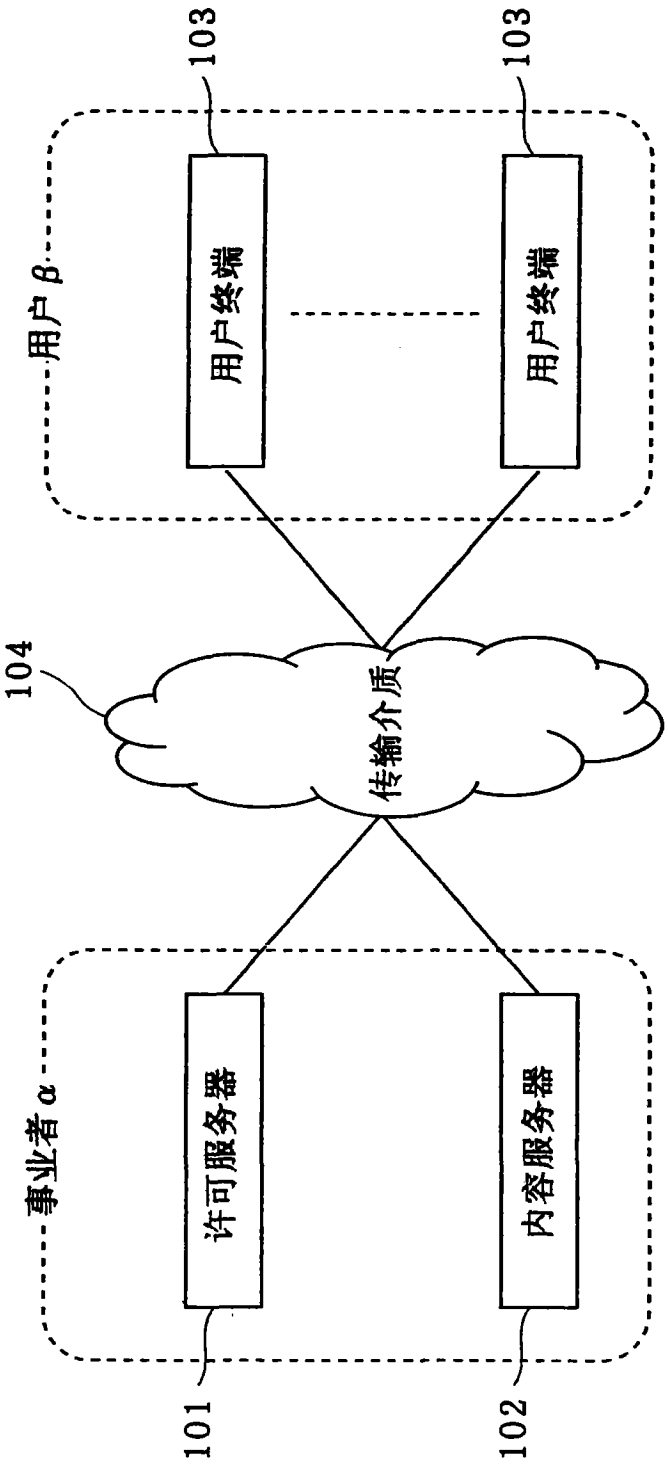


图 1

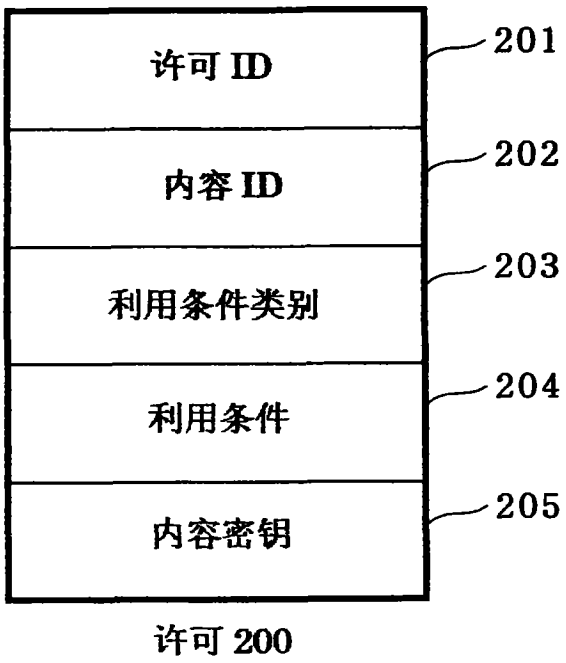


图 2

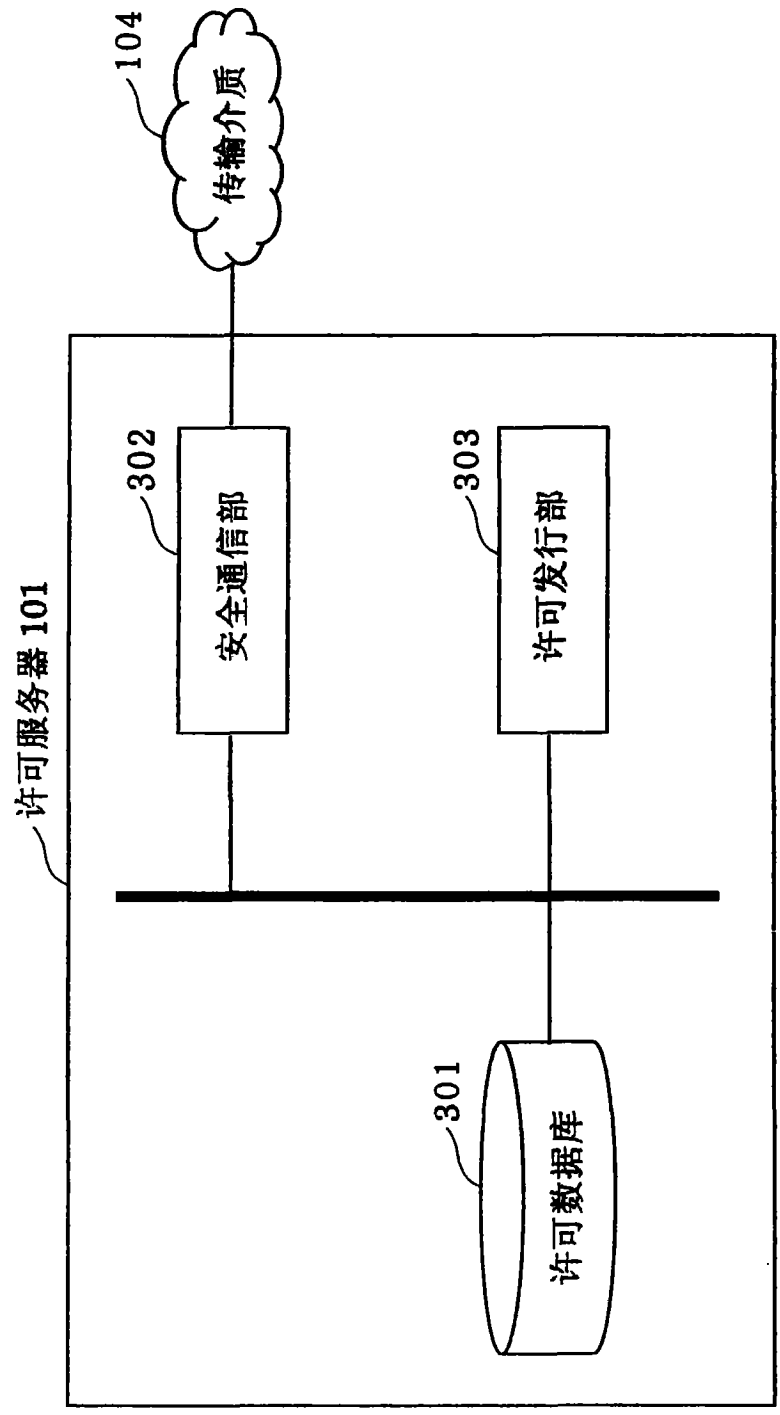


图 3

许可 200

401	201	202	203	204	205	402	403
终端 ID	许可 ID	内容 ID	利用条件类别	利用条件	内容密钥	发行可能次数	待提交标记
0001	0011	0001	无状态	到 2007 年 3 月末为止可以再生	111111	1	1
	0012	0002	有状态	可以再生一次	222222	1	0
0002	0021	0003	无状态	到 2007 年 1 月末为止可以再生	333333	无限制	0
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

许可数据库 301

图 4

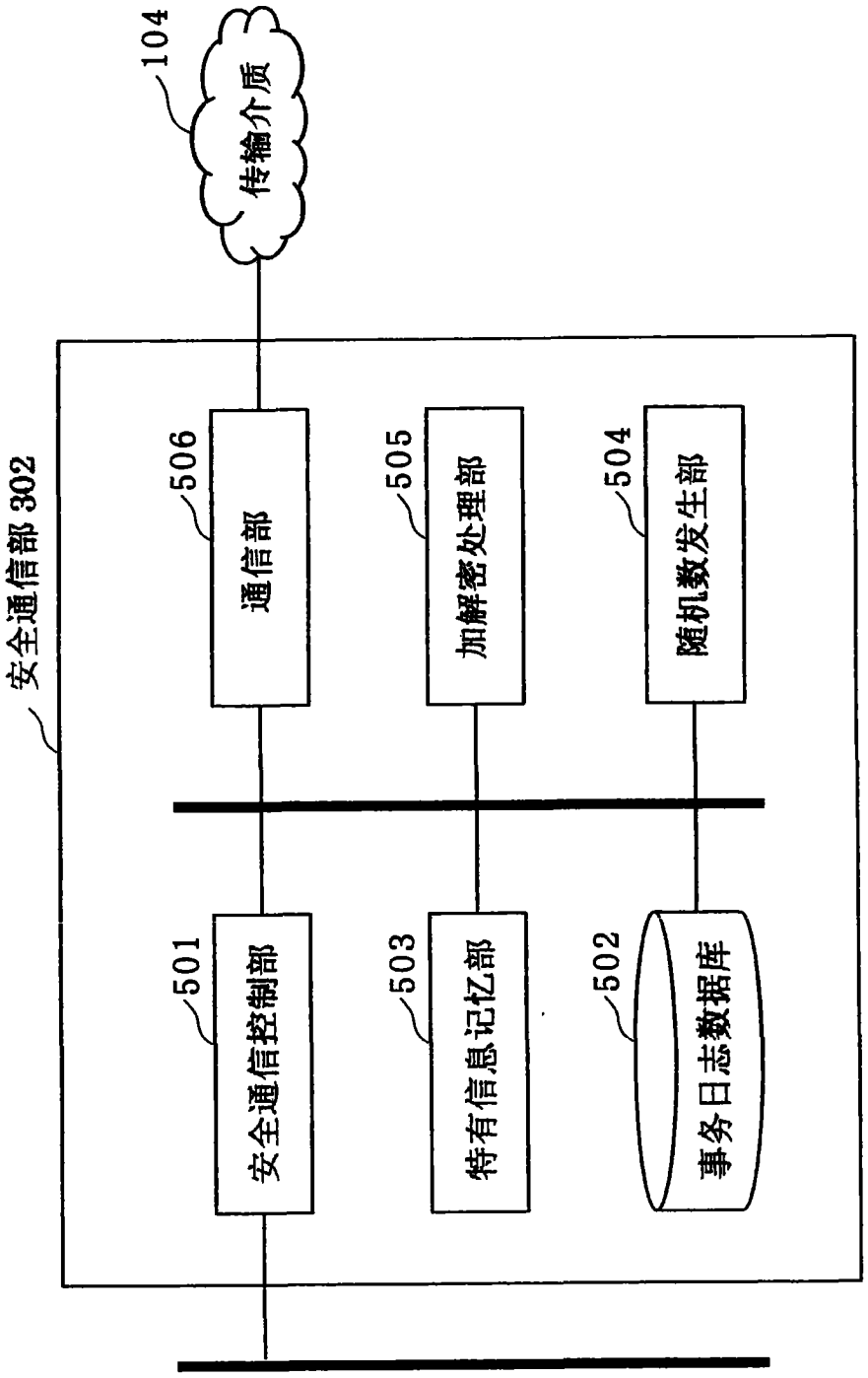

104
传输介质
安全通信部 302
506
通信部
505
加解密处理部
504
随机数发生部
501
安全通信控制部
503
特有信息记忆部
502
事务日志数据库

图 5

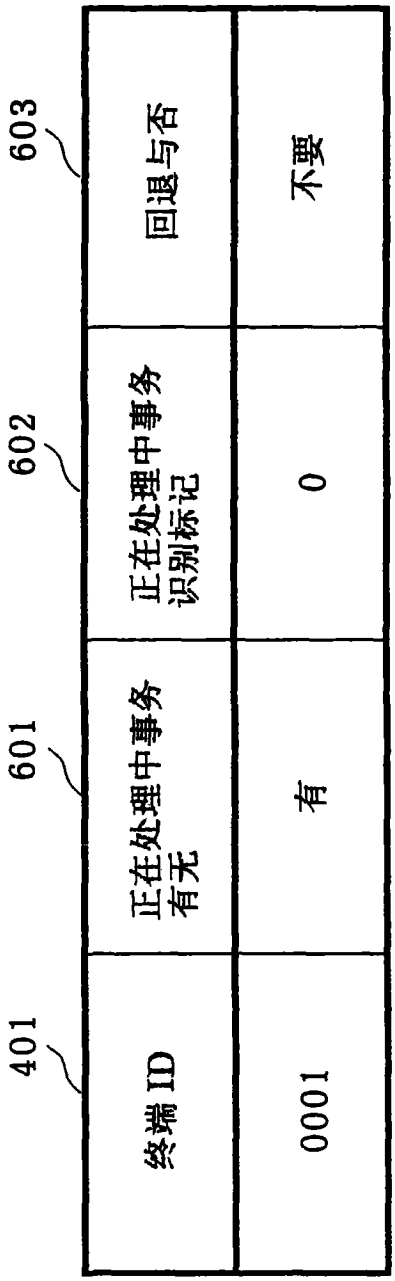

401
601
602
603
终端 ID
正在处理中事务有无
正在处理中事务识别标记
回退与否
0001
有
0
不要
事务日志 600

图 6

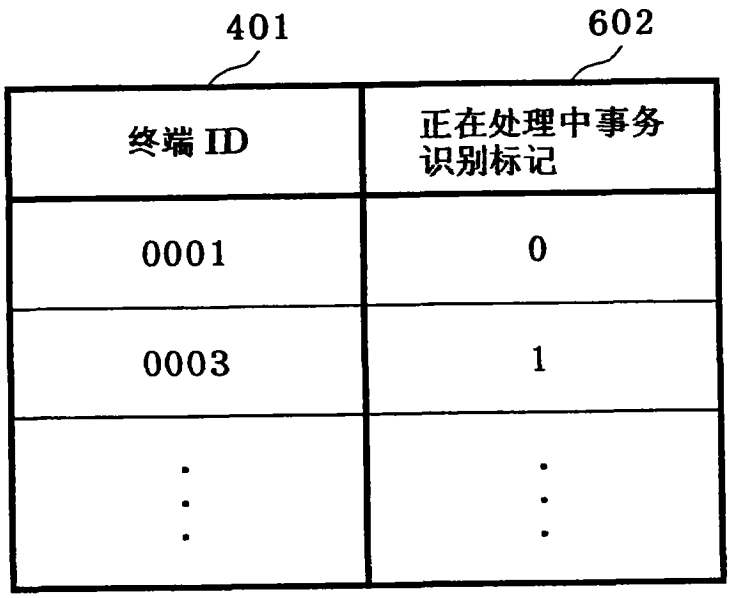


图 7

事务日志数据库 502

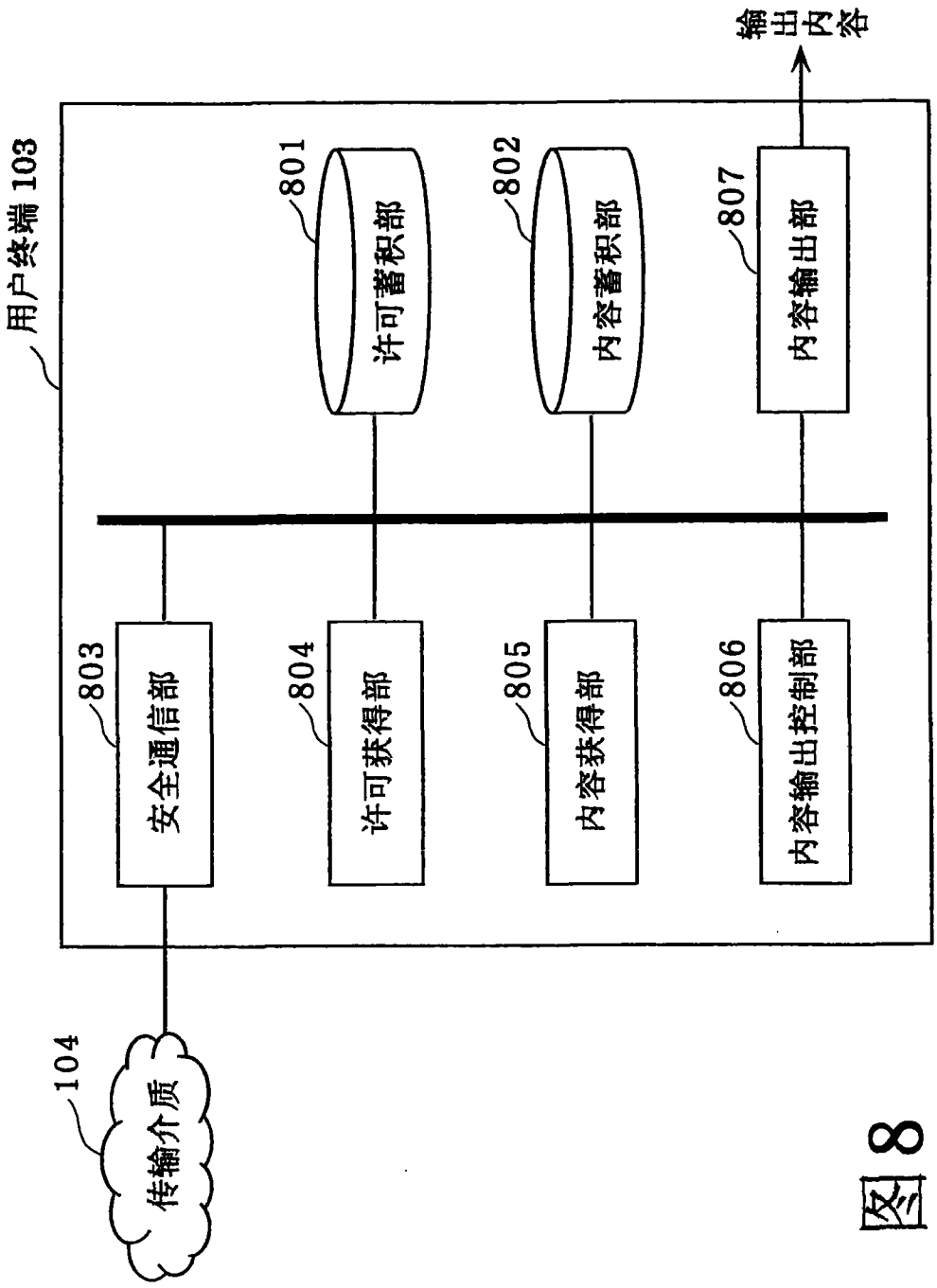

输出内容
用户终端 103
801
许可蓄积部
802
内容蓄积部
807
内容输出部
803
安全通信部
804
许可获得部
805
内容获得部
806
内容输出控制部
104
传输介质

图 8

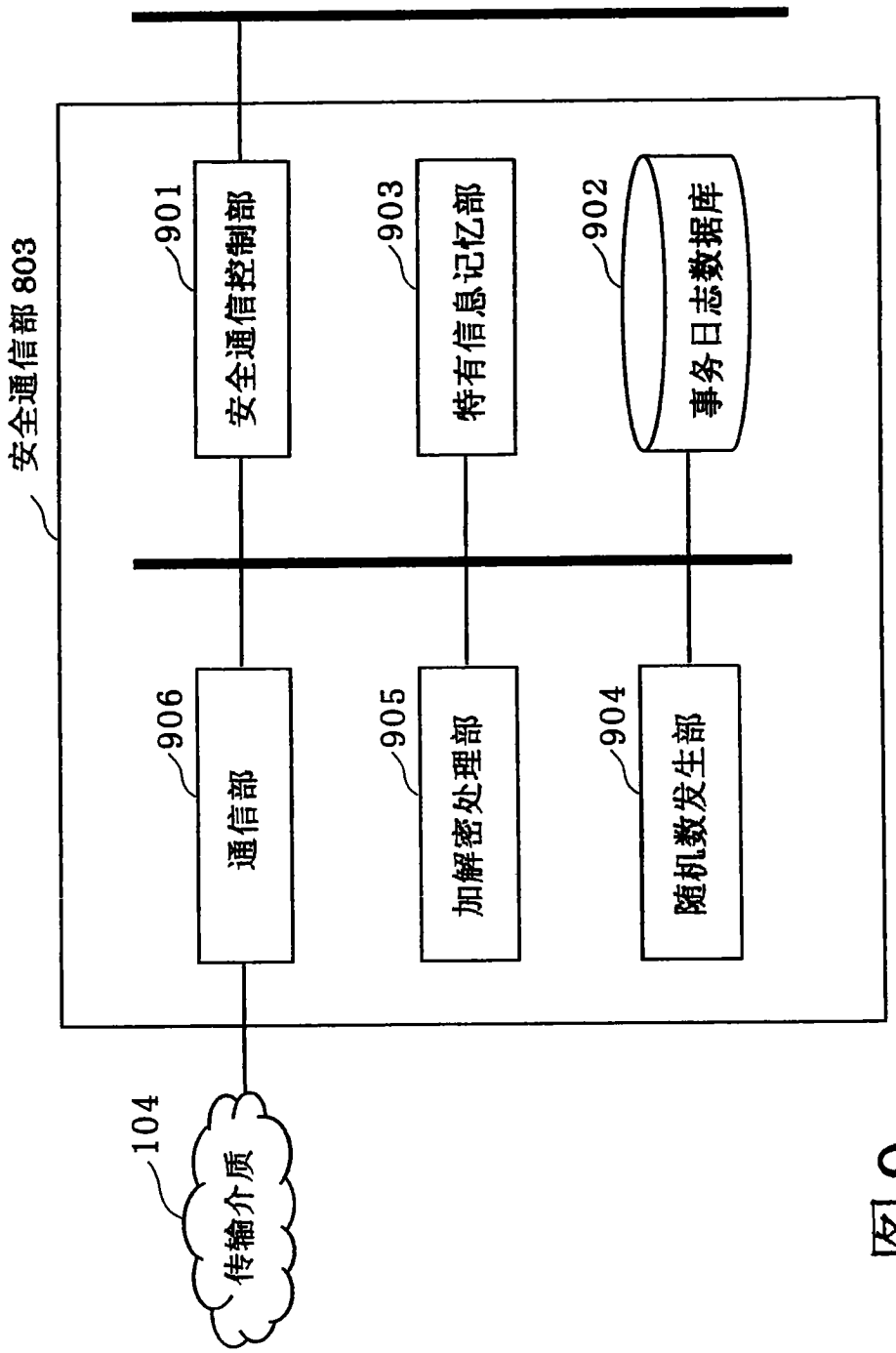

安全通信部 803
901
安全通信控制部
903
特有信息记忆部
902
事务日志数据库
906
通信部
905
加解密处理部
904
随机数发生部
104
传输介质

图 9

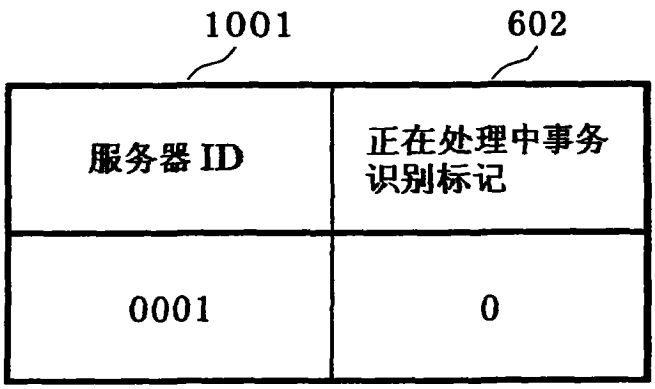


图 10

事务日志 1000

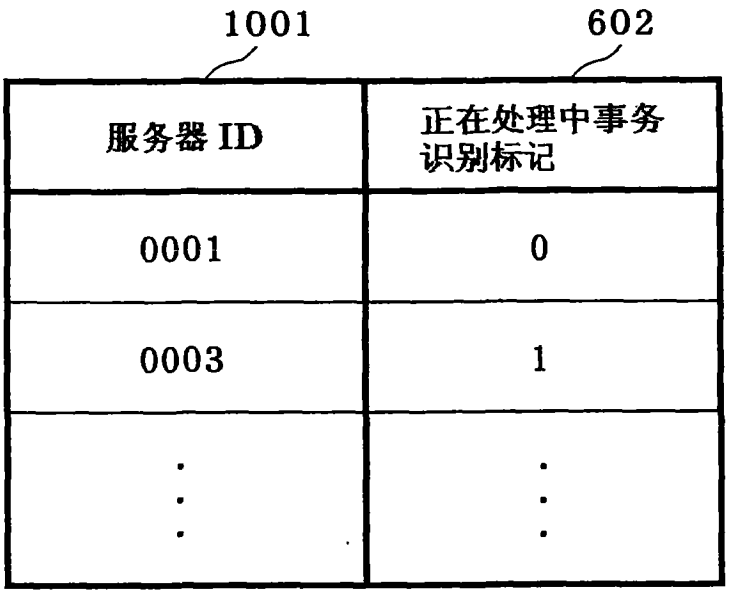


图 11

事务日志数据库 902

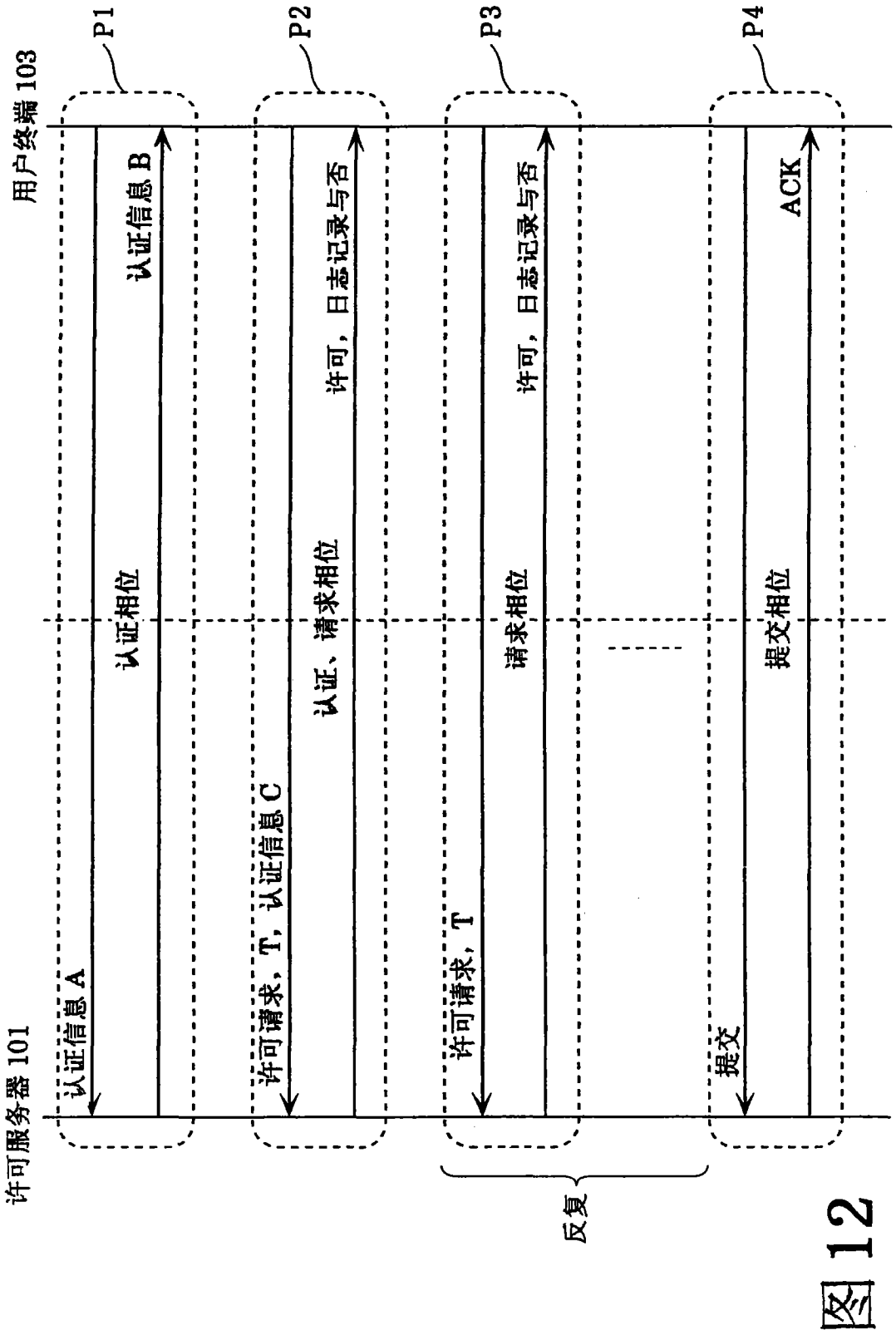

用户终端 103
许可服务器 101
P1
P2
P3
P4
认证信息 A
认证信息 B
认证相位
许可请求，T，认证信息 C
认证、请求相位
许可，日志记录与否
许可请求，T
请求相位
许可，日志记录与否
提交
ACK
提交相位
反复

图 12

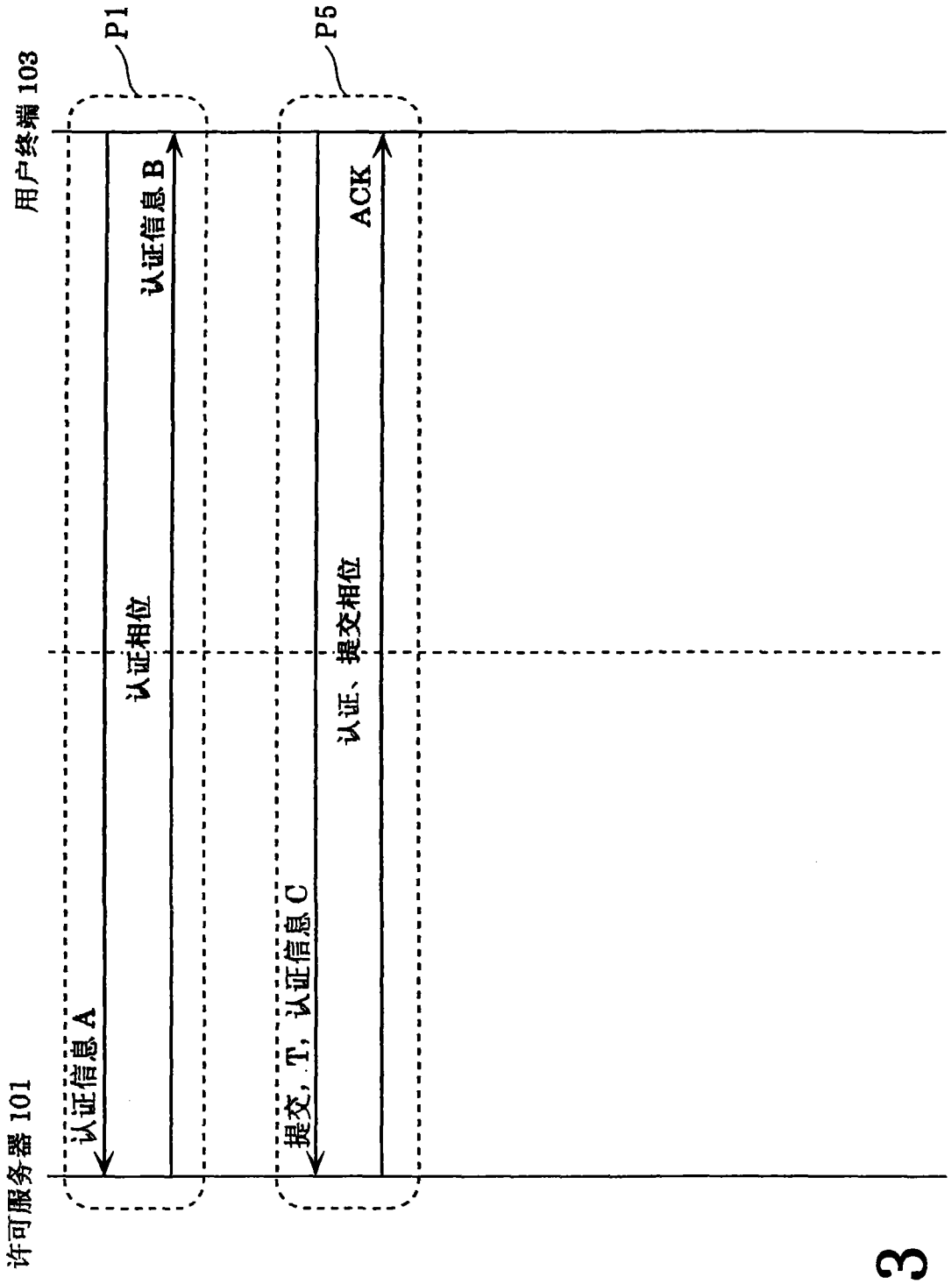

用户终端 103
许可服务器 101
P1
P5
认证信息 A
认证信息 B
认证相位
提交，T，认证信息 C
ACK
认证、提交相位

图 13

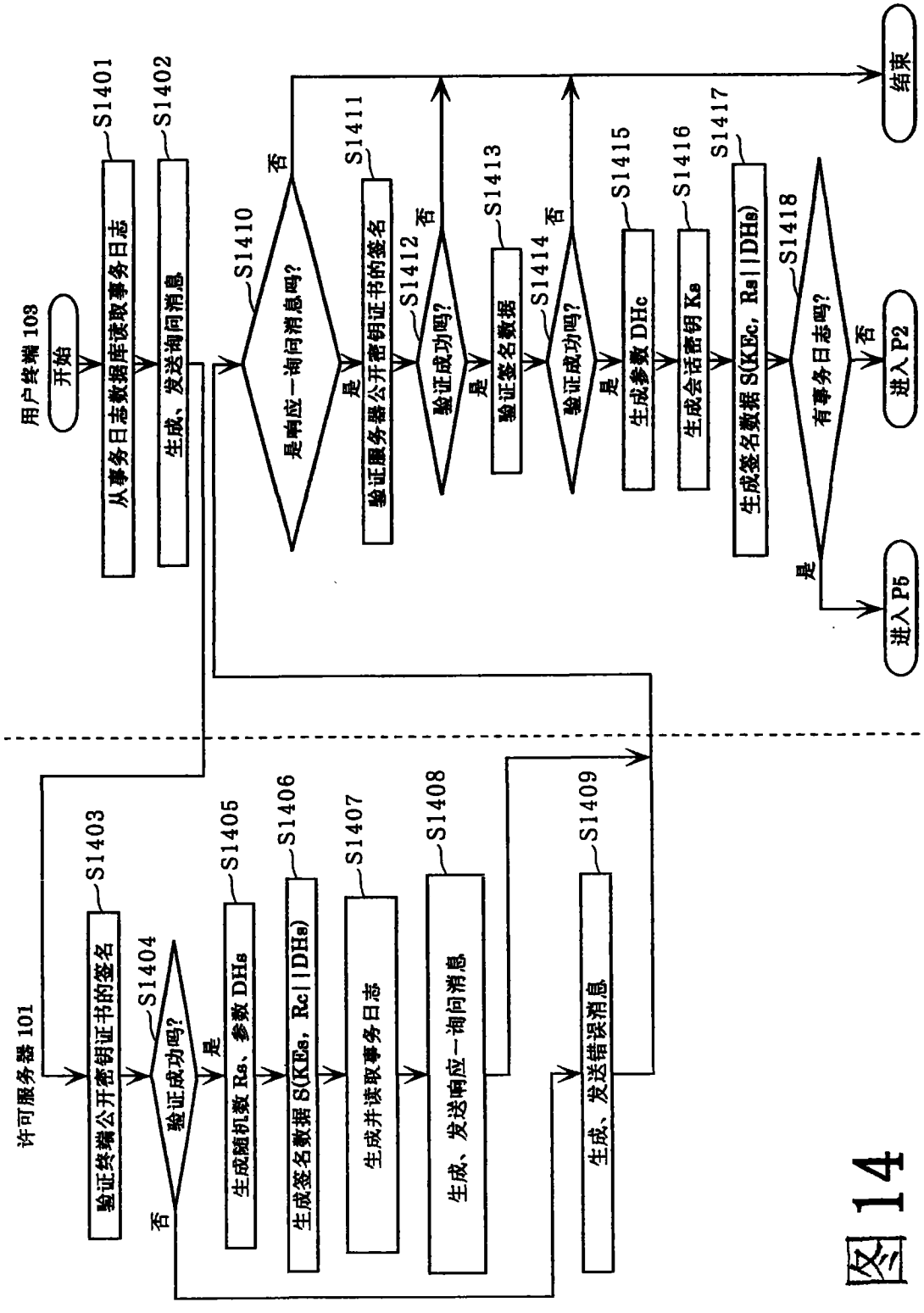

用户终端 103
开始
S1401
从事务日志数据库读取事务日志
S1402
生成、发送询问消息
S1410
是响应一询问消息吗?
否
结束
是
S1411
验证服务器公开密钥证书的签名
S1412
验证成功吗?
否
进入 P2
是
S1413
验证签名数据
S1414
验证成功吗?
否
S1415
生成参数 DHc
S1416
生成会话密钥 Ks
S1417
生成签名数据 S(KEc, Rs||DHs)
S1418
有事务日志吗?
否
进入 P5
是
许可服务器 101
S1403
验证终端公开密钥证书的签名
S1404
验证成功吗?
否
是
S1405
生成随机数 Rs、参数 DHs
S1406
生成签名数据 S(KEs, Rc||DHs)
S1407
生成并读取事务日志
S1408
生成、发送响应一询问消息
S1409
生成、发送错误消息

图 14

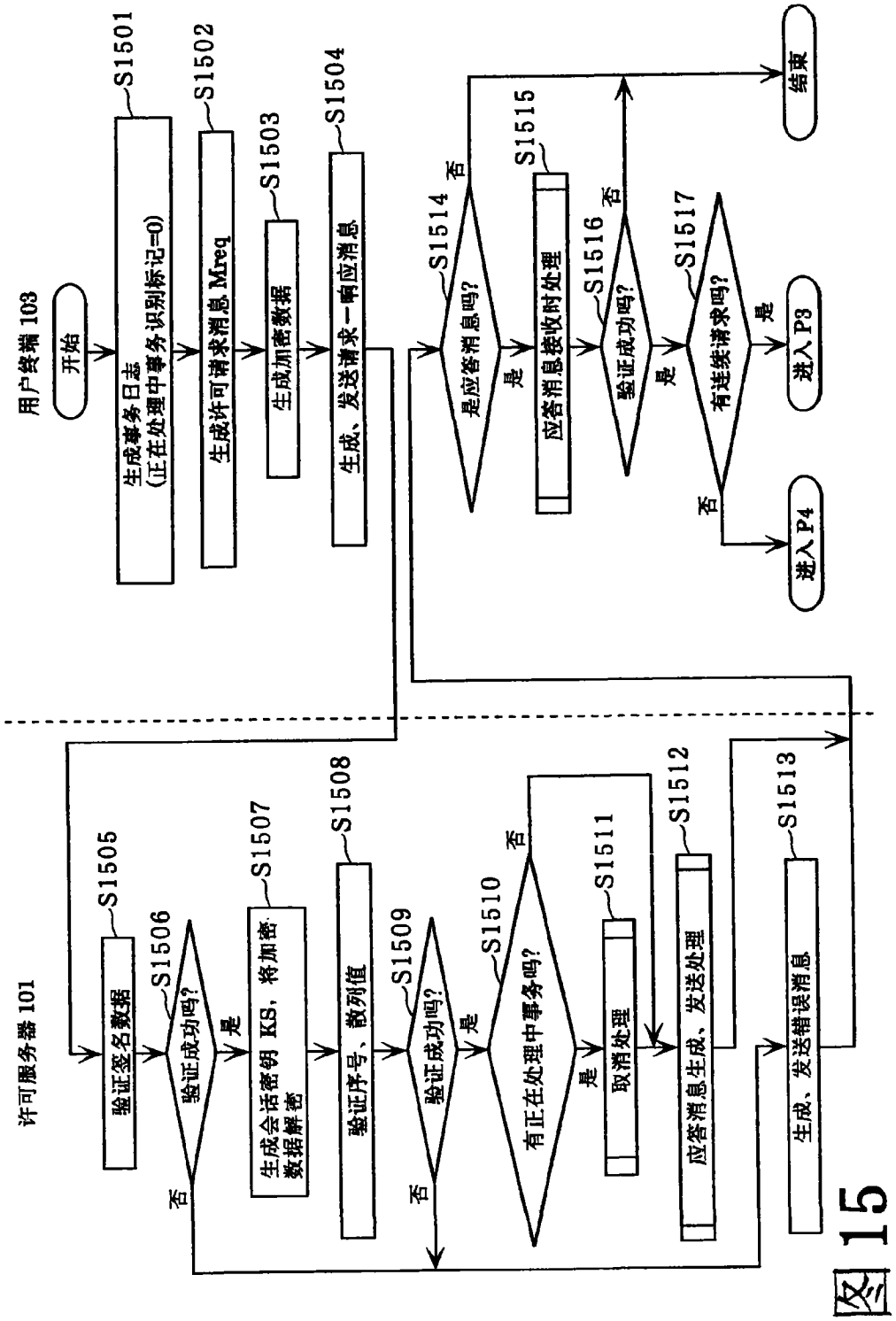

用户终端 103
开始
S1501
生成事务日志
(正在处理中事务识别标记=0)
S1502
生成许可请求消息 Mreq
S1503
生成加密数据
S1504
生成、发送请求一响应消息
S1514
是应答消息吗?
否
是
S1515
应答消息接收时处理
S1516
验证成功吗?
否
是
S1517
有连续请求吗?
否
是
结束
进入P3
进入P4
许可服务器 101
S1505
验证签名数据
S1506
验证成功吗?
否
是
S1507
生成会话密钥 KS，将加密数据解密
S1508
验证序号、散列值
S1509
验证成功吗?
否
是
S1510
有正在处理中事务吗?
否
是
S1511
取消处理
S1512
应答消息生成、发送处理
S1513
生成、发送错误消息

图 15

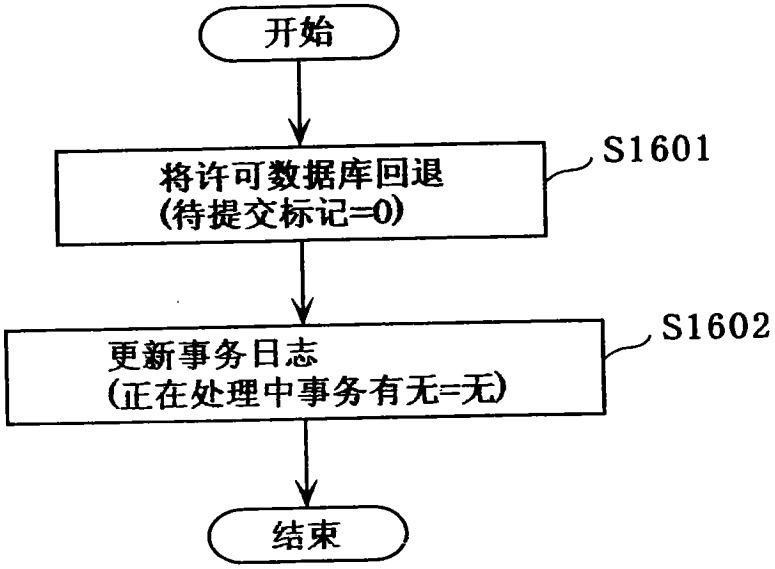


图 16

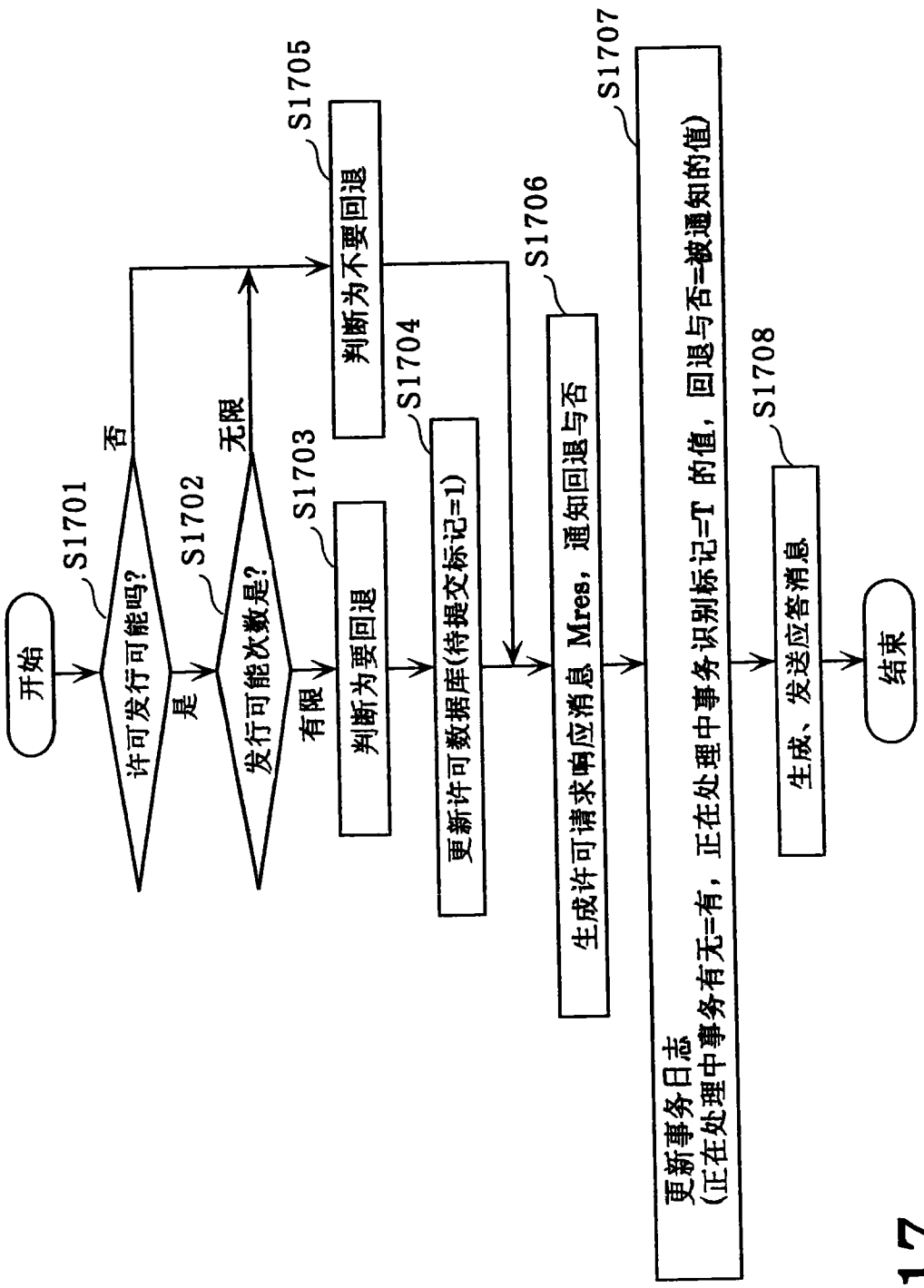

开始
S1701
许可发行可能吗?
否
是
S1702
发行可能次数是?
无限
有限
S1703
判断为要回退
S1705
判断为不要回退
S1704
更新许可数据库(待提交标记=1)
S1706
生成许可请求响应消息 Mres，通知回退与否
S1707
更新事务日志
(正在处理中事务有无=有，正在处理中事务识别标记=T 的值，回退与否=被通知的值)
S1708
生成、发送应答消息
结束

图 17

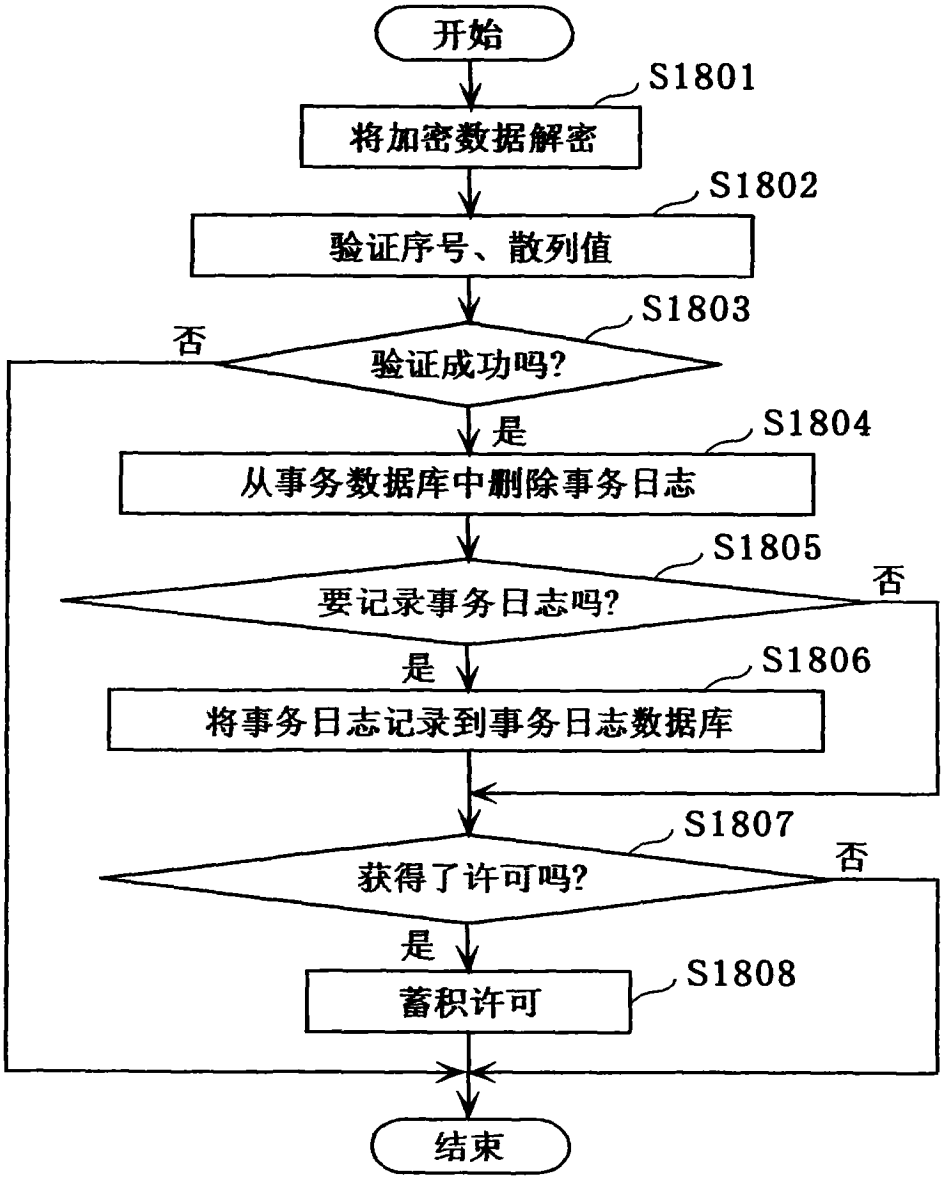

开始
S1801
将加密数据解密
S1802
验证序号、散列值
S1803
否
验证成功吗?
是
S1804
从事务数据库中删除事务日志
S1805
要记录事务日志吗?
否
是
S1806
将事务日志记录到事务日志数据库
S1807
获得了许可吗?
否
是
S1808
蓄积许可
结束

图 18

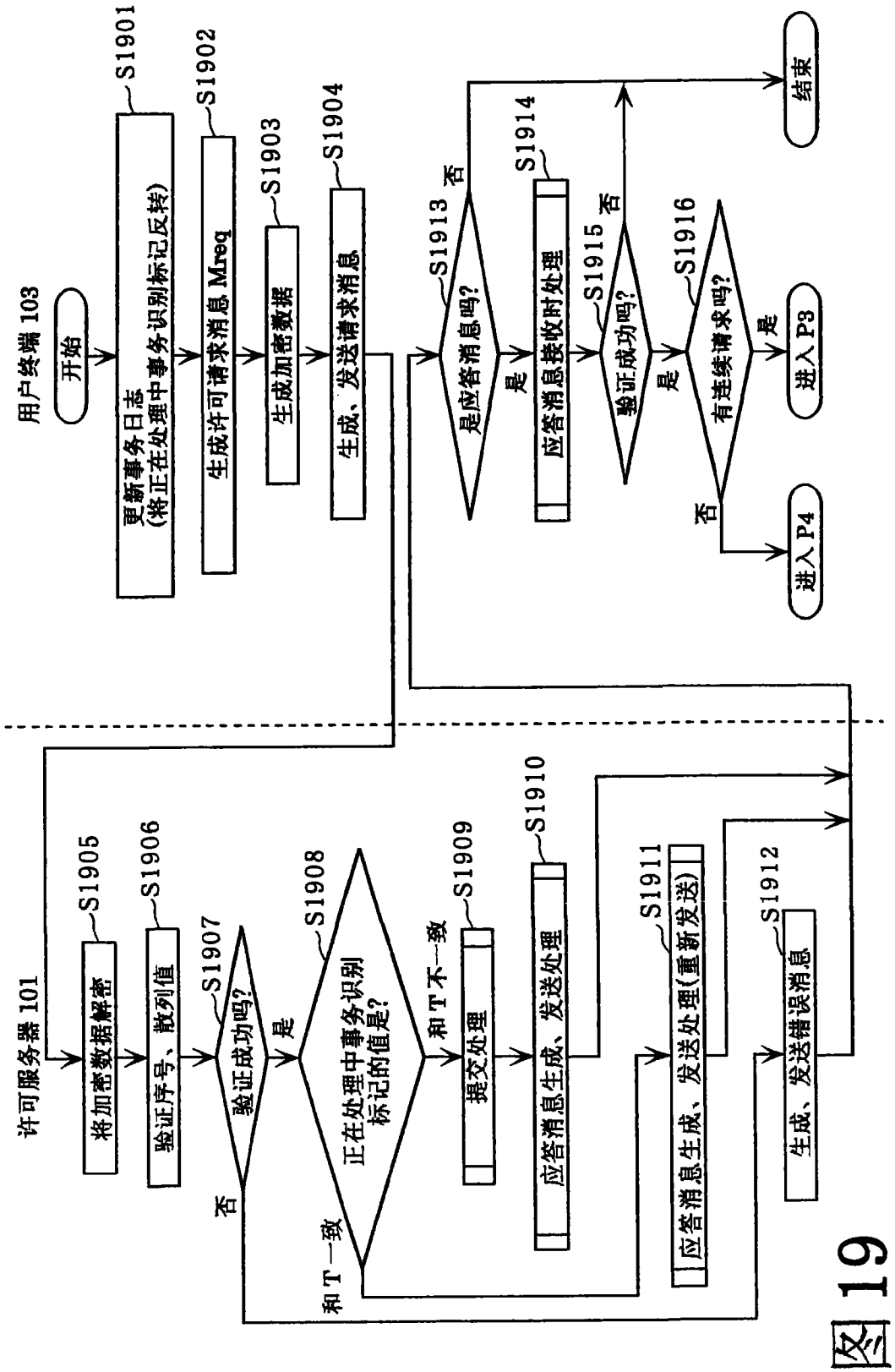

用户终端 103
开始
S1901
更新事务日志
(将正在处理中事务识别标记反转)
S1902
生成许可请求消息 Mreq
S1903
生成加密数据
S1904
生成、发送请求消息
S1913
是应答消息吗?
否
是
S1914
应答消息接收时处理
S1915
验证成功吗?
否
是
S1916
有连续请求吗?
否
是
结束
进入 P3
进入 P4
许可服务器 101
S1905
将加密数据解密
S1906
验证序号、散列值
S1907
验证成功吗?
否
是
S1908
正在处理中事务识别
标记的值是?
和 T 一致
和 T 不一致
S1909
提交处理
S1910
应答消息生成、发送处理
S1911
应答消息生成、发送处理(重新发送)
S1912
生成、发送错误消息

图 19

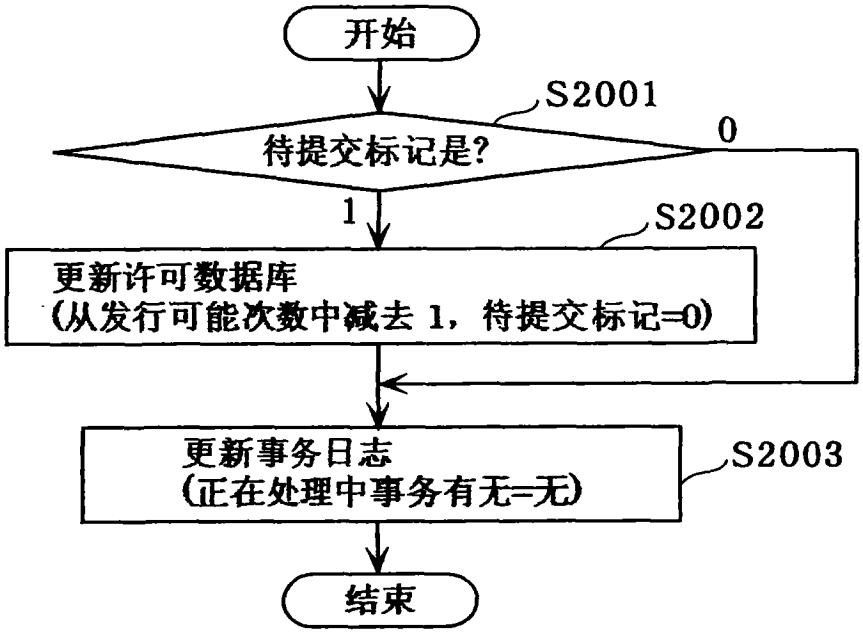

开始
S2001
待提交标记是?
0
1
S2002
更新许可数据库
(从发行可能次数中减去 1，待提交标记=0)
更新事务日志
(正在处理中事务有无=无)
S2003
结束

图 20

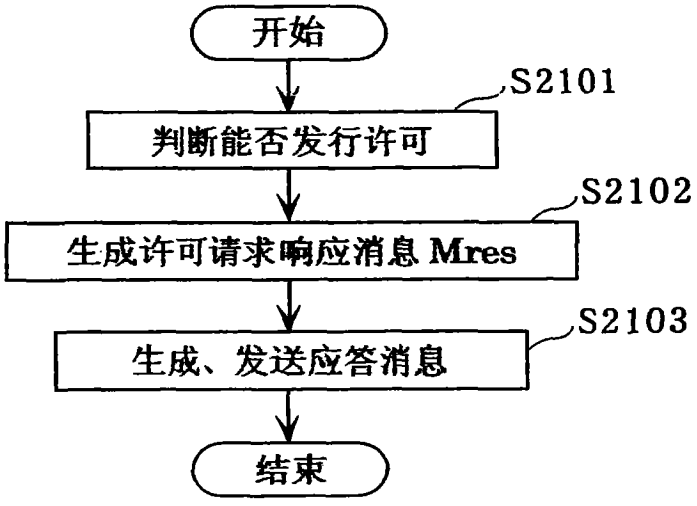

开始
S2101
判断能否发行许可
S2102
生成许可请求响应消息 Mres
S2103
生成、发送应答消息
结束

图 21

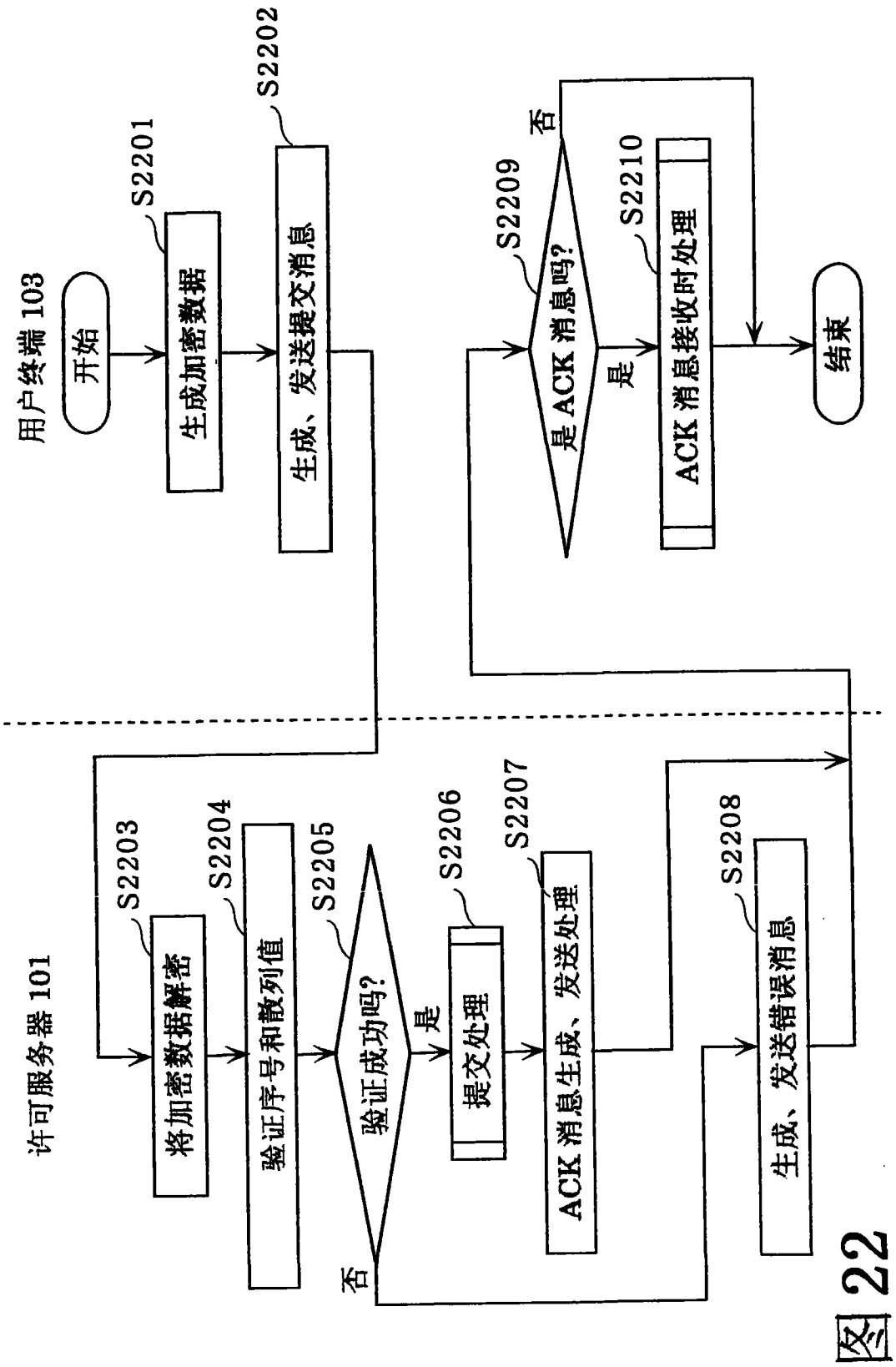

用户终端 103
开始
S2201
生成加密数据
S2202
生成、发送提交消息
S2209
是 ACK 消息吗?
否
是
S2210
ACK 消息接收时处理
结束
许可服务器 101
S2203
将加密数据解密
S2204
验证序号和散列值
S2205
验证成功吗?
否
是
S2206
提交处理
S2207
ACK 消息生成、发送处理
S2208
生成、发送错误消息

图 22

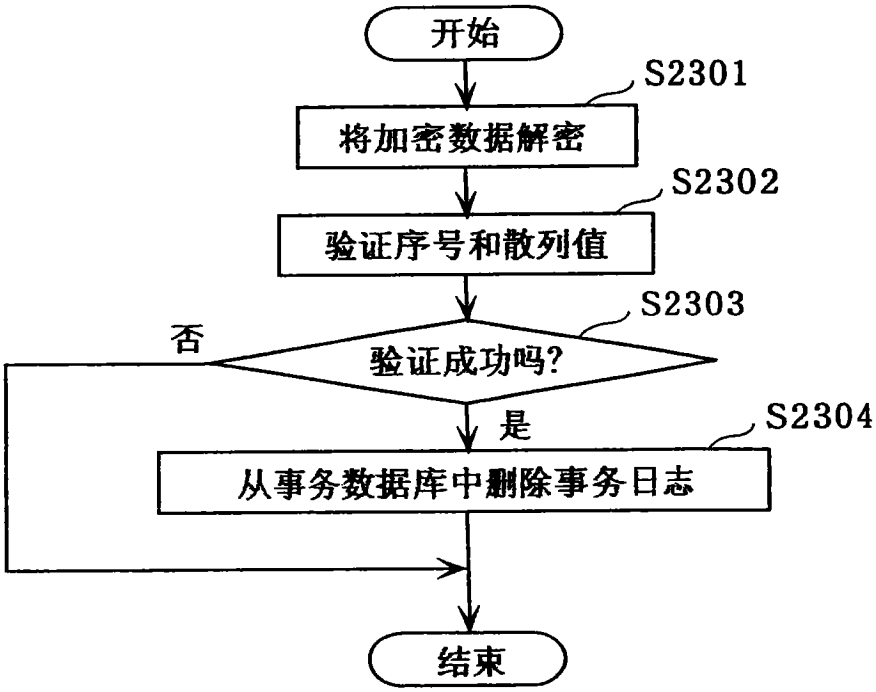

开始
S2301
将加密数据解密
S2302
验证序号和散列值
S2303
否
验证成功吗?
是
S2304
从事务数据库中删除事务日志
结束

图 23

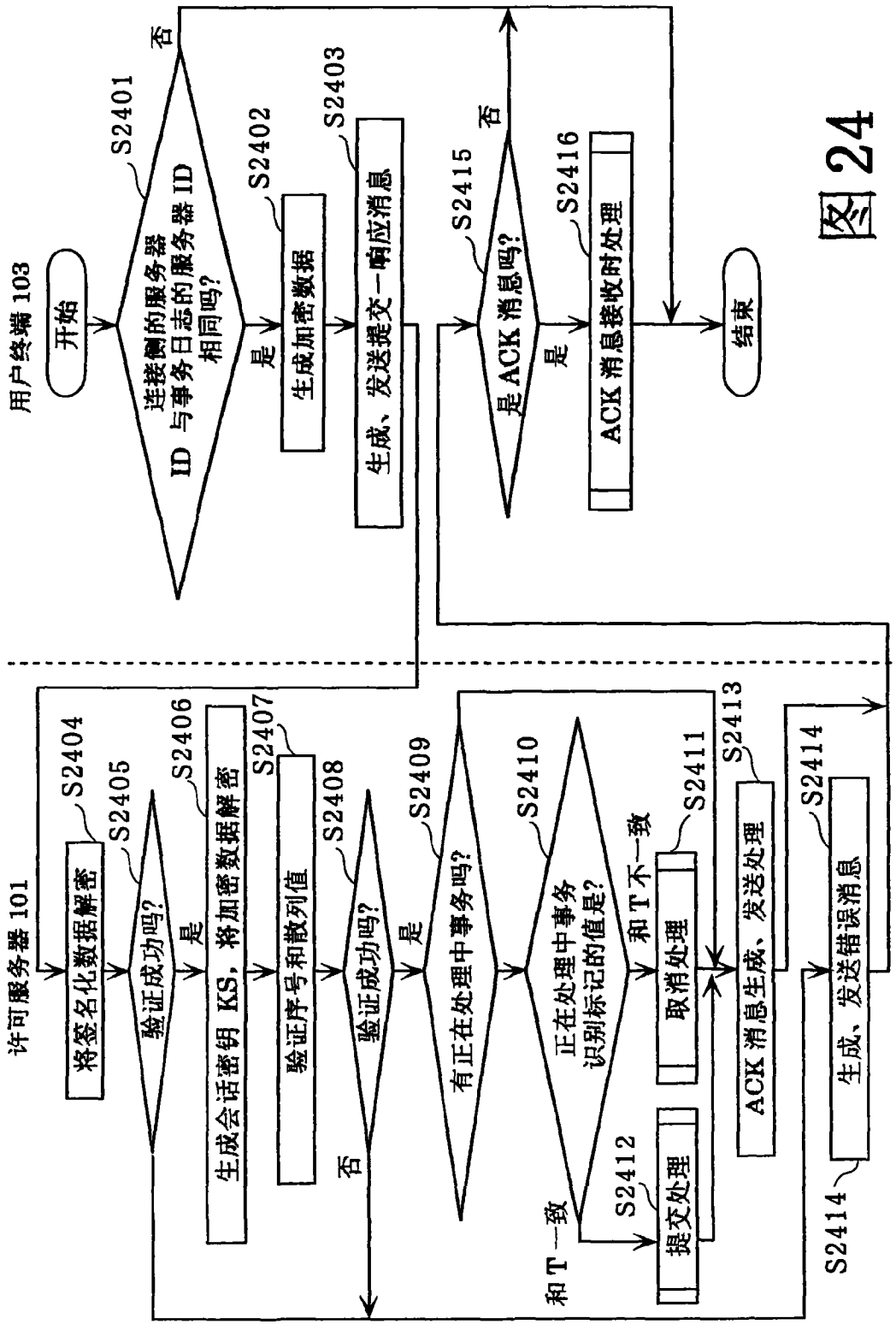

用户终端 103
开始
S2401
连接侧的服务器 ID 与事务日志的服务器 ID 相同吗?
否
是
S2402
生成加密数据
S2403
生成、发送提交一响应消息
S2415
是 ACK 消息吗?
否
是
S2416
ACK 消息接收时处理
结束
许可服务器 101
S2404
将签名化数据解密
S2405
验证成功吗?
是
S2406
生成会话密钥 KS，将加密数据解密
S2407
验证序号和散列值
S2408
验证成功吗?
否
是
S2409
有正在处理中事务吗?
S2410
正在处理中事务识别标记的值是?
和 T 一致
和 T 不一致
S2411
取消处理
S2412
提交处理
S2413
ACK 消息生成、发送处理
S2414
生成、发送错误消息
S2414

图 24

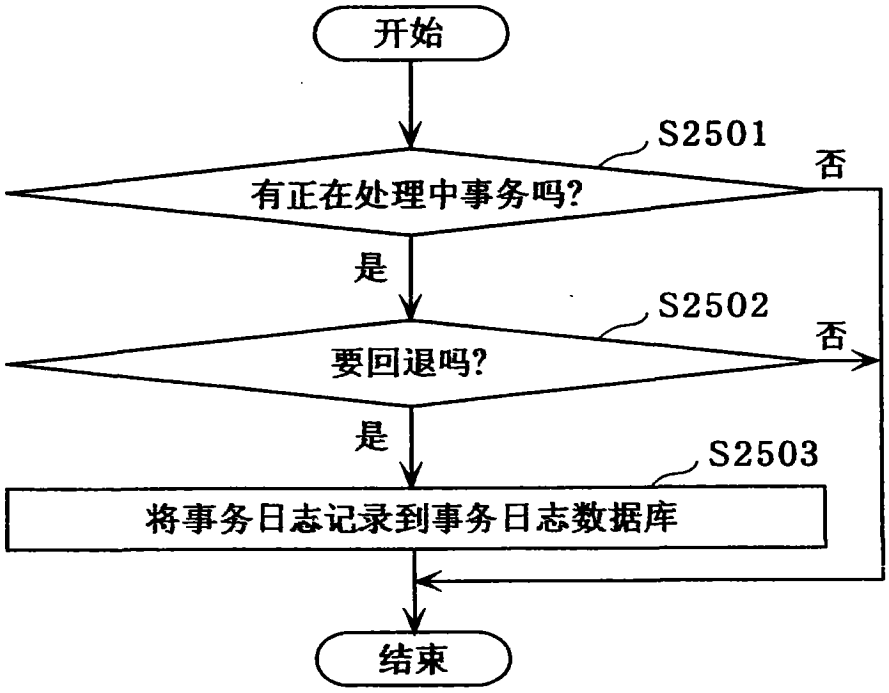

开始
S2501
有正在处理中事务吗?
否
是
S2502
要回退吗?
否
是
S2503
将事务日志记录到事务日志数据库
结束

图 25

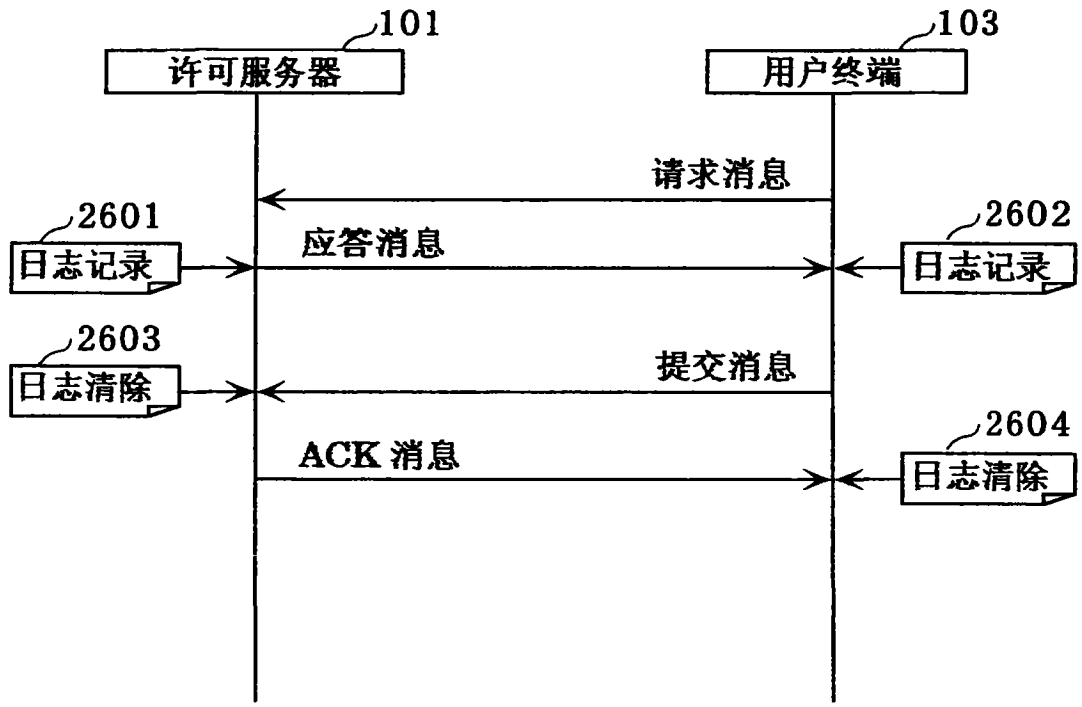

101
许可服务器
103
用户终端
请求消息
2601
日志记录
应答消息
2602
日志记录
2603
日志清除
提交消息
2604
ACK 消息
日志清除

图 26

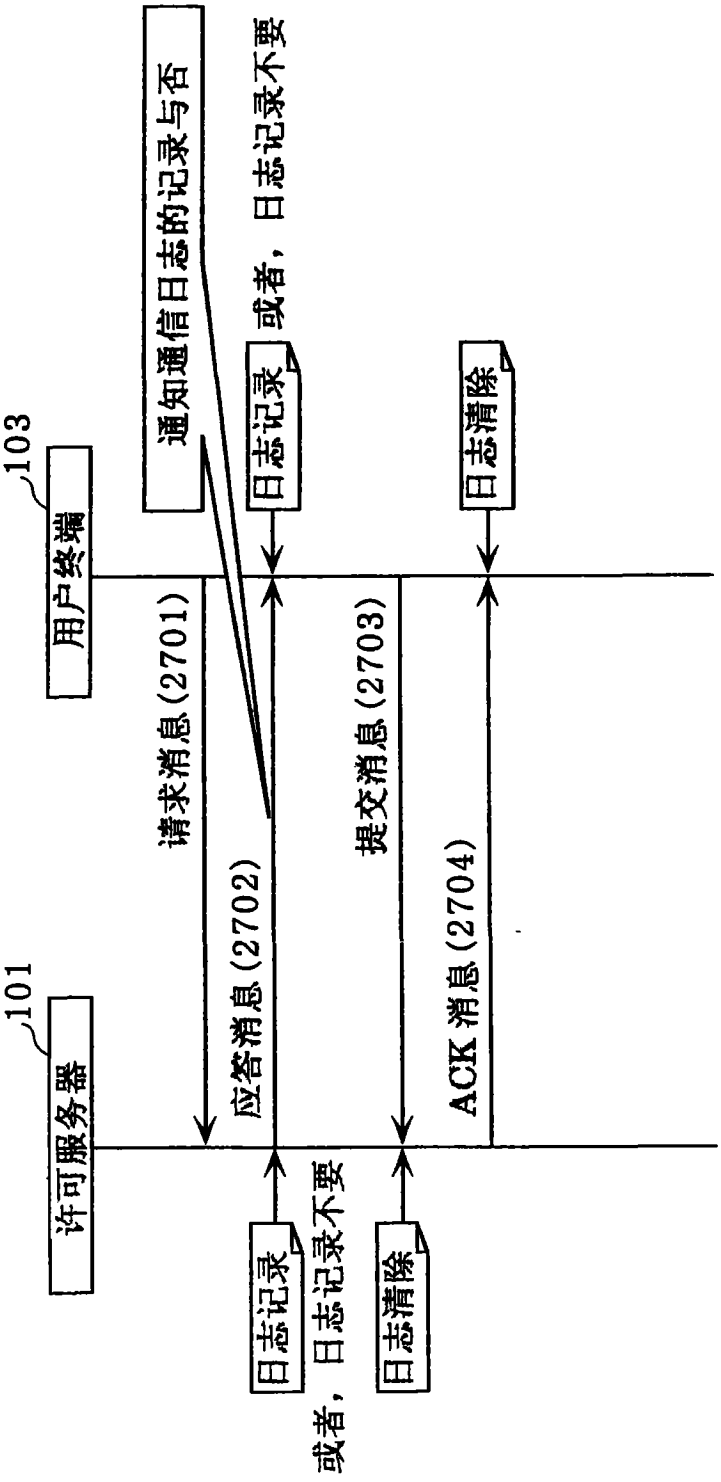

103
用户终端
101
许可服务器
通知通信日志的记录与否
日志记录
或者，日志记录不要
日志清除
请求消息(2701)
应答消息(2702)
提交消息(2703)
ACK 消息(2704)
日志记录
或者，日志记录不要
日志清除

图 27

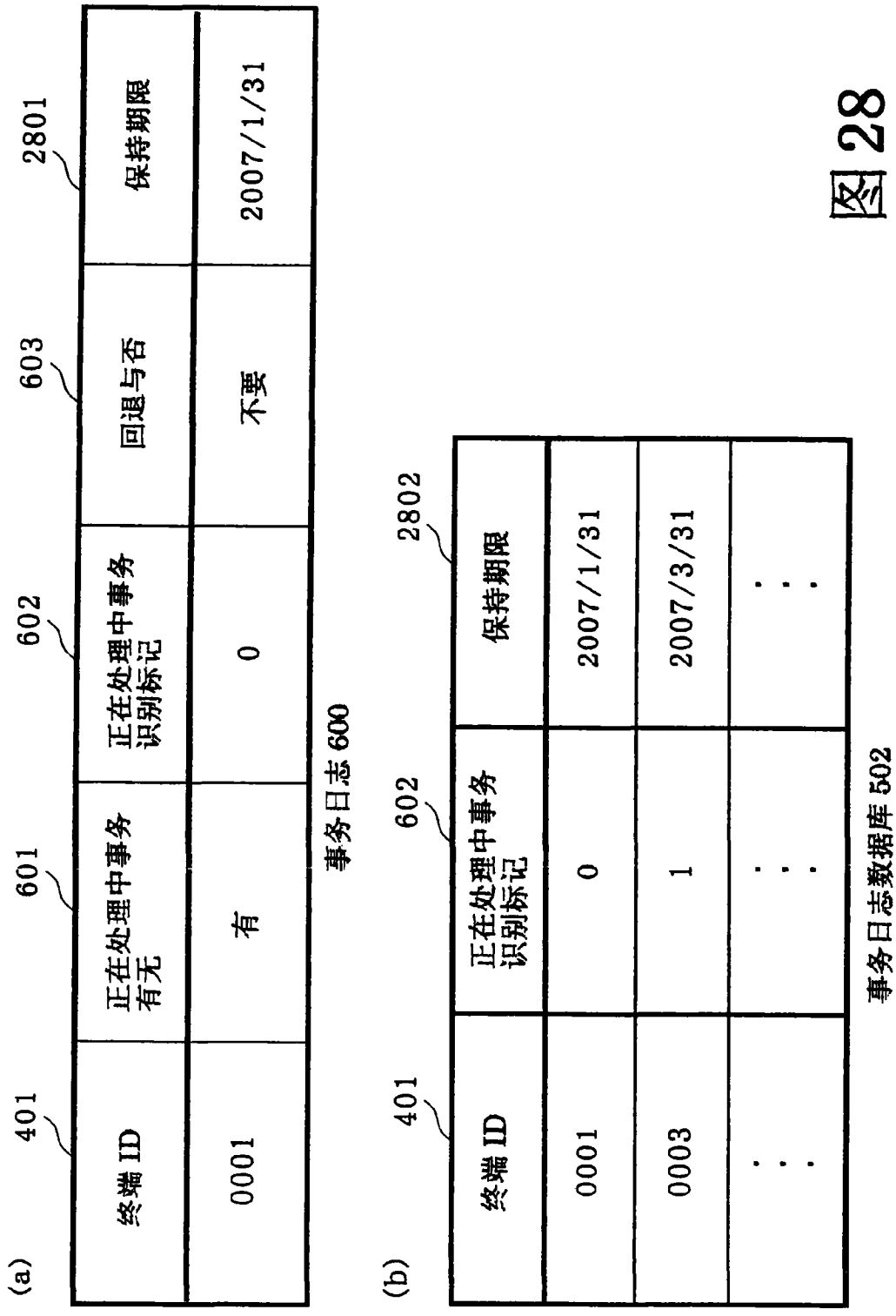

(a)
401
601
602
603
2801
终端 ID
正在处理中事务有无
正在处理中事务识别标记
回退与否
保持期限
0001
有
0
不要
2007/1/31
事务日志 600
(b)
401
602
2802
终端 ID
正在处理中事务识别标记
保持期限
0001
0
2007/1/31
0003
1
2007/3/31
事务日志数据库 502

图 28

(a)

1001 602 2901

服务器 ID	正在处理中事务识别标记	保持期限
0001	0	2007/1/31

事务日志 1000

(b)

1001 602 2902

服务器 ID	正在处理中事务识别标记	保持期限
0001	0	2007/1/31
0003	1	2007/3/31
⋮	⋮	⋮

事务日志数据库 902

图 29

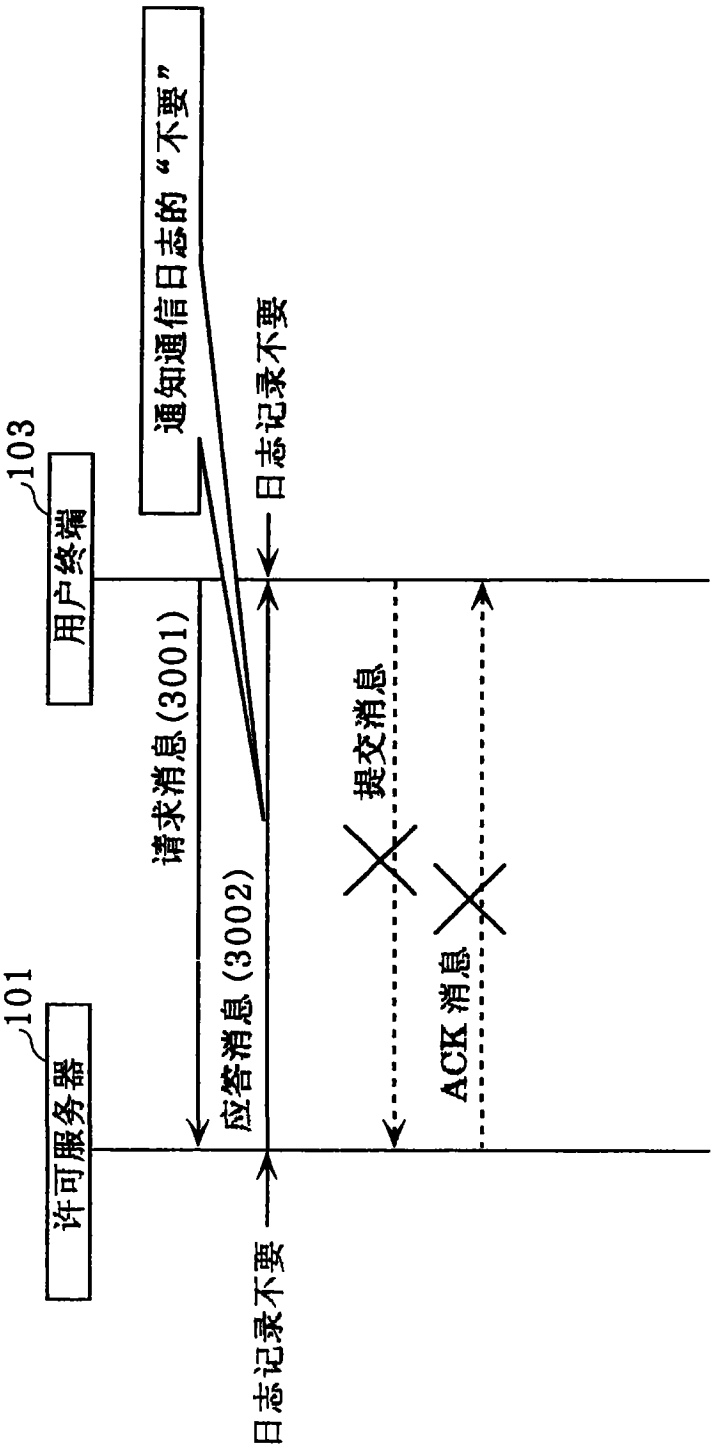

103
用户终端
101
许可服务器
通知通信日志的“不要”
日志记录不要
请求消息(3001)
应答消息(3002)
提交消息
ACK 消息
日志记录不要

图 30

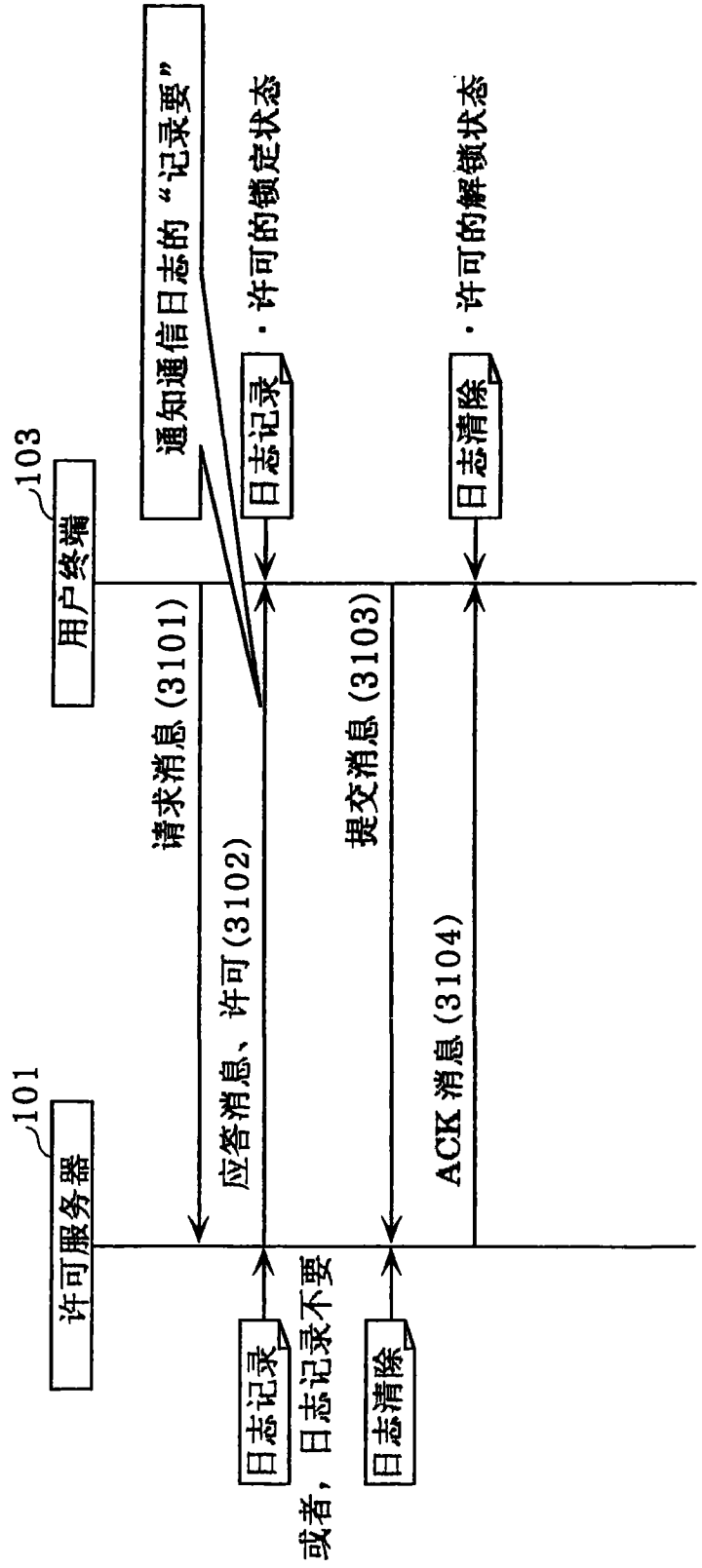

103
用户终端
通知通信日志的“记录要”
日志记录
·许可的锁定状态
日志清除
·许可的解锁状态
请求消息 (3101)
应答消息、许可(3102)
提交消息 (3103)
ACK 消息 (3104)
101
许可服务器
日志记录
日志清除
或者，日志记录不要

图 31