[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 9/10 (2006.01)
G06F 12/14 (2006.01)
G10K 15/02 (2006.01)
G06F 13/00 (2006.01)

[12] 发明专利说明书

专利号 ZL 00818755.X

[45] 授权公告日 2006 年 9 月 27 日

[11] 授权公告号 CN 1277364C

[22] 申请日 2000.12.1 [21] 申请号 00818755.X
[30] 优先权
[32] 1999.12.2 [33] JP [31] 343389/99
[86] 国际申请 PCT/JP2000/008544 2000.12.1
[87] 国际公布 WO2001/041356 日 2001.6.7
[85] 进入国家阶段日期 2002.8.1
[71] 专利权人 三洋电机株式会社
地址 日本大阪府
共同专利权人 富士通株式会社
株式会社日立制作所
[72] 发明人 堀吉宏 日置敏昭 金森美和
吉川隆敏 武村浩司 高桥政孝
长谷部高行 古田茂树 畠山卓久
利根川忠明 穴泽健明
审查员 刘欣科

[74] 专利代理机构 中国专利代理(香港)有限公司
代理人 刘宗杰 叶恺东

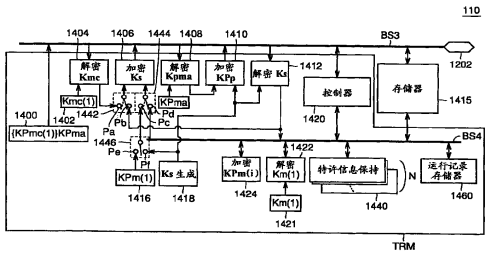
权利要求书 6 页 说明书 33 页 附图 24 页

[54] 发明名称

数据记录装置、数据供给装置及数据传送系统

[57] 摘要

存储卡(110)，根据保持在认证数据保持部(1400)内的数据与服务器之间进行认证处理。存储卡(110)，通过进行解密处理而从供给到数据总线(BS3)上的数据提取来自服务器的第 1 对话密钥(Ks1)及事务 ID。进一步，存储卡(110)，由对话密钥发生部(1418)生成第 2 对话密钥(Ks2)，并用第 1 对话密钥(Ks1)将第 2 对话密钥(Ks2)及存储卡(110)所固有的密钥(KPm(1)加密后发送到服务器，在内容密钥受到解密时作为对内容密钥进行加密的密钥。保持在运行记录存储器(1460)内的事务 ID 及第 2 对话密钥(Ks2)，在再次传送处理中使用。



1. 一种数据记录装置，用于通过通信路径接收和记录包含着与加密内容数据的再生相关且用于对上述加密内容数据进行解密而使其成为明文的内容密钥的再生信息，该数据记录装置（110）备有：数据通信部，用于建立与再生信息的发送源之间可以发送接收加密后的信息的加密通信路径，接收与加密内容数据分别供给上述数据记录装置、且加密后而被传送的上述再生信息；第 1 存储部（1415、1440），用于保持从上述数据通信部供给的与上述再生信息有关的数据；信息提取部，用于进行将来自上述数据通信部的与上述再生信息有关的数据存储到上述第 1 存储部的处理，并根据存储在上述第 1 存储部内的数据提取上述再生信息；第 2 存储部（1460），用于存储表示接收上述再生信息并记录到上述第 1 存储部的接收处理中的处理状态的接收运行记录信息；上述接收运行记录信息，具有在每次进行上述再生信息的传送处理时由上述再生信息的发送源生成后发送到上述数据记录装置并用于特定上述再生信息的传送处理的通信特定信息，还备有用于控制上述数据记录装置的动作的接收控制部（1420），上述接收控制部，根据请求通过上述数据通信部发送记录在上述第 2 存储部内的上述接收运行记录信息。

2. 根据权利要求 1 所述的数据记录装置，其特征在于：上述数据通信部，包括：第 1 密钥保持部（1402），保持用于对由对应于上述数据记录装置而预先设定的第 1 公开加密密钥加密后的数据进行解密的第 1 保密解密密钥；第 1 解密处理部（1404），用于接收在上述再生信息的每次通信中更新后从上述再生信息的发送源发送且由上述第 1 公开加密密钥加密后的第 1 共用密钥，并进行解密处理；第 2 密钥保持部（1416），用于保持上述每个数据记录装置所固有的第 2 公开加密密钥；密钥生成部（1418），在上述再生信息的每次通信中更新而生成第 2 共用密钥；第 1 加密处理部（1406），用于根据上述第 1 共用密钥对上述第 2 公开加密密钥及上述第 2 共用密钥进行加密并输出；第 2 解密处理部（1412），用于接收由上述第 2 公开加密密钥加密、进一步再由上述第 2 共用密钥加密后的上述再生信息并根据上述第 2 共用密钥进行解密，上述信息提取部，包括保持用于对由上述第 2 公开加密密钥加密后的数据进行解密的第 2 保密解密密钥的第 3 密钥保持部（1421）、及在从与上述再生信息有关的数据对上述第 1 存

储部的存储处理到提取上述再生信息的处理的过程中对上述第 2 保密解密密钥进行解密处理的第 3 解密处理部（1422），上述第 1 存储部，保持上述第 2 解密处理部的输出或基于上述第 2 解密处理部的输出的上述再生信息，上述接收运行记录信息，还具有上述第 2 共用密钥。

3.根据权利要求 2 所述的数据记录装置，其特征在于：上述第 1 存储部，包括用于以明文状态存储上述再生信息中的除上述内容密钥外的上述再生信息的一部分即第 1 数据的第 3 存储部（1440），及用于以加密后的状态存储上述再生信息中的包含除上述第 1 数据以外的全部第二数据的上述再生信息的一部分或上述再生信息的全部的第 4 存储部（1415）；上述信息提取部，包括再次加密处理部，用于将上述第 3 解密处理部对上述第 2 解密处理部的输出进行解密处理后的结果中的上述第 2 数据存储在上述第 3 存储部内，并利用上述第 2 公开加密密钥将上述第 3 解密处理部对上述第 2 解密处理部的输出进行解密处理后的结果中的一部分再次加密而生成应存储在上述第 4 存储部内的上述第 1 数据。

4. 根据权利要求 3 所述的数据记录装置，其特征在于：上述第 3 存储部，接收和存储可以根据上述内容密钥进行解密的上述加密内容数据。

5. 根据权利要求 2 所述的数据记录装置，其特征在于：上述信息提取部，将上述第 3 解密处理部对上述第 2 解密处理部的输出进行解密处理后的结果以明文状态存储在上述第 1 存储部内。

6. 根据权利要求 5 所述的数据记录装置，其特征在于：上述第 1 存储部，包括用于接收和存储可以根据上述内容密钥进行解密的上述加密内容数据的第 3 存储部（1415）及以明文状态存储上述再生信息的第 4 存储部（1440）。

7. 根据权利要求 2 所述的数据记录装置，其特征在于：上述接收运行记录信息，具有在每次进行上述再生信息的接收处理时由上述发送源生成的用于特定上述接收处理的通信特定信息、及上述第 2 共用密钥。

8. 根据权利要求 7 所述的数据记录装置，其特征在于：上述接收运行记录信息，还具有表示上述接收处理中的已完成上述再生信息对上述第 1 存储部的存储的状态的状态信息。

9.根据权利要求 1 所述的数据记录装置，其特征在于：上述接收运行记录信息，在上述接收处理中每次将上述再生信息记录在上述第 1 存储部时从上述第 2 存储部删除。

10.根据权利要求 9 所述的数据记录装置，其特征在于：上述状态信息，是在上述接收处理中每次对上述发送源请求发送上述再生信息时变为接通状态而每次将上述再生信息存储在上述第 1 存储部内时变为断开状态的标志信息。

11.根据权利要求 2 所述的数据记录装置，其特征在于：上述数据记录装置，还备有保持在接收上述再生信息之前由上述再生信息的发送源进行认证处理用的认证数据的第 5 存储部（1400）。

12.根据权利要求 11 所述的数据记录装置，其特征在于：上述认证数据，包含上述第 1 公开加密密钥。

13.根据权利要求 12 所述的数据记录装置，其特征在于：上述第 1 加密处理部，根据上述第 1 共用密钥分别对上述接收运行记录信息和上述署名信息进行加密，上述数据记录装置，将由上述第 1 加密处理部分别加密后的上述接收运行记录信息和上述署名信息送回上述发送源。

14.根据权利要求 1 所述的数据记录装置，其特征在于：上述数据记录装置，还备有根据上述接收运行记录信息的全部或一部分生成署名信息的装置，当输出上述接收运行记录信息时，生成与上述接收运行记录信息对应的上述署名信息，并与上述接收运行记录信息一起输出。

15.根据权利要求 1 所述的数据记录装置，其特征在于：上述数据记录装置，是存储插卡，上述第 1 记录部，是非易失性半导体存储器。

16.一种数据传送系统，备有数据供给装置，用于分别单独供给加密内容数据及包含着与上述加密内容数据的再生相关且用于对上述加密内容数据进行解密而使其成为明文的解密密钥即内容密钥的再生信息，上述数据供给装置（10），包括：传送控制部，用于控制上述数据供给装置；传送信息保持部（304），用于保持上述加密内容数据及上述再生信息；第 1 接口部（350），用于与外部之间进行数据的发送接收；第 1 对话密钥发生部（316），生成在上述再生信息对上述终端的每次传送中更新的第 1 共用密钥；对话密钥加密部（318），用于由

对应于上述用户的终端而预先设定的第 1 公开加密密钥对上述第 1 共用密钥进行加密并供给上述第 1 接口部；对话密钥解密部（320），用于对由上述第 1 共用密钥加密后送回的第 2 公开加密密钥及第 2 共用密钥进行解密；第 1 特许数据加密处理部（326），利用由上述对话密钥解密部解密后的上述第 2 公开加密密钥对用于再生上述加密内容数据的再生信息进行加密；第 2 特许数据加密处理部（328），利用上述第 2 共用密钥进一步对上述第 1 特许数据加密处理部的输出进行加密，并传送给上述第 1 接口部；传送运行记录信息保持部（306），用于记录表示上述传送处理中的处理状态的传送运行记录信息；上述传送运行记录信息，具有在每次进行上述再生信息的传送处理时由上述数据供给装置生成并用于特定上述再生信息的传送处理的通信特定信息；还备有为通过通信路径从上述数据供给装置接收传送而分别与多个用户对应的多个终端（100）；各上述终端，包括用于与外部之间进行数据的发送接收的第 2 接口部（1104）及接收和存储上述加密内容数据及上述再生信息的数据存储部（110）；上述数据存储部，具有：第 1 密钥保持部（1402），保持用于对由对应于上述数据存储部而预先设定的第 1 公开加密密钥加密后的数据进行解密的第 1 保密解密密钥；第 1 解密处理部（1404），用于接收在上述再生信息的每次通信中更新后传送且由上述第 1 公开加密密钥加密后的第 1 共用密钥，并进行解密处理；第 2 密钥保持部（1416），用于保持对上述每个数据存储部都不相同的第 2 公开加密密钥；密钥生成部（1418），在上述再生信息的每次通信中更新而生成第 2 共用密钥；第 1 加密处理部（1406），用于根据上述第 1 共用密钥对上述第 2 公开加密密钥及上述第 2 共用密钥进行加密并输出；第 2 解密处理部（1412），用于接收由上述第 2 公开加密密钥加密、进一步再由上述第 2 共用密钥加密后的再生信息，并根据上述第 2 共用密钥进行解密；第 1 存储部（1415、1440），保持基于上述第 2 解密处理部的上述再生信息；第 3 密钥保持部（1421），保持用于对由上述第 2 公开加密密钥加密后的数据进行解密的第 2 保密解密密钥；第 3 解密处理部（1422），在从与上述再生信息有关的数据对上述第 1 存储部的存储处理到提取上述再生信息的处理的过程中，对上述第 2 保密解密密钥进行解密处理；第 2 存储部（1460），用于存储表示再生信息的传送处理中的处理状态且包

含从上述数据供给装置发送来的上述通信特定信息的接收运行记录信息；接收控制部（1420），对与外部之间的数据发送接收进行控制；上述接收控制部，当上述传送处理过程中上述通信路径被切断时，向上述数据供给装置发送上述接收运行记录信息，上述传送控制部，当上述传送处理过程中上述通信路径被切断时，根据上述接收运行记录信息和上述传送运行记录信息控制重新传送处理。

17.根据权利要求 16 所述的数据传送系统，其特征在于：上述数据存储部，是可在上述终端上进行插卸的存储插卡。

18.根据权利要求 16 所述的数据传送系统，其特征在于：上述数据存储部，还备有保持在接收上述再生信息之前由上述再生信息的发送源进行认证处理用的认证数据的第 5 存储部（1400）；上述数据供给装置，还备有在传送上述再生信息之前根据由上述数据存储部保持和发送的认证数据对上述存储插卡进行认证的装置（312）；上述数据供给装置，当在上述认证处理中认证了上述数据存储部时，向装有上述数据存储部的上述终端发送上述再生信息。

19.根据权利要求 16 所述的数据传送系统，其特征在于：上述传送运行记录信息，还具有用于特定要传送的上述传送信息的再生信息特定信息及上述第 2 共用密钥，上述接收运行记录信息，还具有上述第 2 共用密钥。

20.根据权利要求 16 所述的数据传送系统，其特征在于：上述接收运行记录信息，在每次将再生信息存储在上述第 1 存储部时从上述第 2 存储部删除。

21.根据权利要求 16 所述的数据传送系统，其特征在于：上述接收运行记录信息，包含每次对上述数据供给装置请求传送上述再生信息时变为接通状态而每次将上述再生信息存储在上述第 1 存储部内时变为断开状态的接收状态标志。

22.根据权利要求 16 所述的数据传送系统，其特征在于：上述接收运行记录信息，至少具有上述通信特定信息及上述第 2 共用密钥。

23.一种数据供给装置，备有数据存储部并用于向与多个用户分别对应的多个终端（100）供给再生信息，该数据存储部，用于记录包含着与加密内容数据的再生相关且用于对上述加密内容数据进行解密而使其成为明文的解密密钥即内容密钥并与上述加密内容数据

分别供给的再生信息、及在接收和记录上述再生信息的传送处理中表示上述传送处理的处理状态且包含通信特定信息的接收运行记录信息；该数据供给装置，备有：传送信息保持部（304），用于保持上述内容数据及上述再生信息；第 1 接口部（350），用于与外部之间进行数据的发送接收；第 1 对话密钥发生部（316），生成在上述再生信息对上述终端的每次传送中更新的第 1 共用密钥；对话密钥加密部（318），用于由对应于上述用户的终端而预先设定的第 1 公开加密密钥对上述第 1 共用密钥进行加密并供给上述第 1 接口部；对话密钥解密部（320），用于对由上述第 1 共用密钥加密后送回的第 2 公开加密密钥及第 2 共用密钥进行解密；第 1 特许数据加密处理部（326），利用由上述对话密钥解密部解密后的上述第 2 公开加密密钥对用于再生上述加密内容数据的再生信息进行加密；第 2 特许数据加密处理部（328），利用上述第 2 共用密钥进一步对上述第 1 特许数据加密处理部的输出进行加密，并传送给上述第 1 接口部；传送运行记录信息保持部（306），用于记录表示上述传送处理中的处理状态且包含上述通信特定信息的传送运行记录信息；传送控制部，控制上述数据供给装置的动作，在每次进行上述再生信息的传送处理时生成用于特定上述再生信息的传送处理的上述通信特定信息并发送到上述终端；上述传送控制部，当上述传送处理过程中上述通信路径被切断时，根据由上述数据存储部记录且从上述终端发送来的上述接收运行记录信息和上述传送运行记录信息，确认是来自切断前相互通信着的上述终端的重新传送请求，从而控制重新传送处理。

24.根据权利要求 23 所述的数据供给装置，其特征在于：上述数据供给装置，还备有在传送上述再生信息之前根据从上述数据存储部发送的认证数据对上述数据存储部进行认证的装置（312），当在上述认证处理中认证了上述数据存储部时，发送上述再生信息。

25.根据权利要求 23 所述的数据供给装置，其特征在于：上述传送运行记录信息，还具有用于特定要传送的上述传送信息的再生信息特定信息及上述第 2 共用密钥，上述接收运行记录信息，还具有上述第 2 共用密钥。

数据记录装置、数据供给装置及数据传送系统

技术领域

本发明涉及在用于对携带式电话机等终端传送信息的信息传送系统中可以对所复制的信息的著作权加以保护的存储卡及采用该插卡的数据传送系统。

背景技术

近年来，随着因特网等信息通信网等的进展，使各用户可以很方便地利用采用了携带式电话等的面向个人的终端访问因特网的信息。

在这种信息通信中，用数字信号传输信息。因此，即使当各个人用户对例如由如上所述的信息通信网传输的音乐或视频数据进行了复制时，也几乎不会因这种复制而使音质或画质恶化，因而可以进行数据的复制。

就是说，当在这种信息通信网上传送音乐信息或图象数据等存在着著作者的权利的内容数据时，如不采取适当的用于著作权保护的对策，则显然将有可能使著作者的权利受到侵害。

另一方面，假如不能将著作权保护的目的放在最优先的位置就通过急速扩大的数字信息通信网进行内容数据的传送，则尽管基本上在复制数据时可以征收一定的著作权费用但对著作权者来说这反而是不利的。

可是，当通过如上所述的数字信息通信网进行音乐数据等内容数据的传送时，各用户可以将按如上述方式传送的数据记录在任何记录装置上，然后用再生装置进行再生。

作为这种记录装置，例如，可以采用存储卡之类的能以电气方式进行数据的写入和删除的媒体。

进一步，作为对所传送的音乐数据进行再生的装置，在采用用于接收这种数据的传送的携带式电话本身的情况下、或记录装置为存储卡等可以从接收传送的装置上插卸的情况下，也可以采用专用的再生装置。

无论在哪种情况下，当通过数字信息通信网、特别是无线方式的通信网接收音乐数据等内容数据的传送时，在音乐数据等的全部传送

结束之前，都可能由于通信线路的状态等而存在着通信中断的情况。例如，当作为将内容数据加密后的加密内容数据和必需解密和再生的再生信息进行传送时，如在加密内容数据的传送过程中发生通信的中断，则只需在重新接通后继续进行数据的接收即可，但在再生信息的传送过程中，由于还要同时对用户进行计费处理，所以当发生这种通信中断时用户在重新接通后就要请求重新进行再生信息的发送。但是，从著作权者的权利保护的观点考虑，不允许一有请求就随意地进行再生信息的重新发送。反过来说，假如不进行重新发送，则可能存在着虽已进行了计费处理但用户不能取得再生信息的问题。

发明内容

本发明的另一目的在于，提供一种即使在再生信息的传送结束之前发生了通信中断也可以在保护了著作权者的权利后通过重新开始通信而完成再生信息的传送的数据传送系统及用于该系统的存储插卡等数据记录装置。

为达到本发明的目的，本发明的一种数据记录装置，用于通过通信路径接收和记录包含着与加密内容数据的再生相关且用于对上述加密内容数据进行解密而使其成为明文的内容密钥的再生信息，该数据记录装置备有：数据通信部，用于建立与再生信息的发送源之间可以发送接收加密后的信息的加密通信路径，接收与加密内容数据分别供给数据记录装置且加密后而被传送的上述再生信息；第 1 存储部，用于保持从上述数据通信部供给的与上述再生信息有关的数据；信息提取部，用于进行将来自上述数据通信部的与上述再生信息有关的数据存储到上述第 1 存储部的处理，并根据存储在上述第 1 存储部内的数据提取上述再生信息；第 2 存储部，用于存储表示接收上述再生信息并记录到上述第 1 存储部的接收处理中的处理状态的接收运行记录信息；上述接收运行记录信息，具有在每次进行上述再生信息的传送处理时由上述再生信息的发送源生成后发送到上述数据记录装置并用于特定上述再生信息的传送处理的通信特定信息，还备有用于控制上述数据记录装置的动作的接收控制部，上述接收控制部，根据请求通过上述数据通信部发送记录在上述第 2 存储部内的上述接收运行记录信息。

数据通信部，最好包括第 1 密钥保持部、第 1 解密处理部、第 2 密钥保持部、密钥生成部、第 1 加密处理部、第 2 解密处理部。第 1

密钥保持部，保持用于对由对应于数据记录装置而预先设定的第 1 公开加密密钥加密后的数据进行解密的第 1 保密解密密钥。第 1 解密处理部，接收在再生信息的每次通信中更新后从再生信息发送源发送且由第 1 公开加密密钥加密后的第 1 共用密钥，并进行解密处理。第 2 密钥保持部，保持每个数据记录装置所固有的第 2 公开加密密钥。密钥生成部，在再生信息的每次通信中更新而生成第 2 共用密钥。第 1 加密处理部，根据第 1 共用密钥对第 2 公开加密密钥及第 2 共用密钥进行加密并输出。第 2 解密处理部，接收由第 2 公开加密密钥加密、进一步再由第 2 共用密钥加密后的再生信息，并根据第 2 共用密钥进行解密。信息提取部，包括第 3 密钥保持部和第 3 解密处理部。第 3 密钥保持部，保持用于对由第 2 公开加密密钥加密后的数据进行解密的第 2 保密解密密钥。第 3 解密处理部，在从与再生信息有关的数据对第 1 存储部的存储处理到提取再生信息的处理的过程中，对第 2 保密解密密钥进行解密处理。第 1 存储部，保持基于第 2 解密处理部的输出或第 2 复合处理部的输出的再生信息。

按照本发明的另一方面，提供一种数据传送系统，该数据传送系统，备有内容数据供给装置及多个终端。

数据供给装置，分别单独供给加密内容数据及包含着与加密内容数据的再生相关且用于对加密内容数据进行解密而使其成为明文的解密密钥即内容密钥的再生信息。数据供给装置，包括传送控制部、传送信息保持部、第 1 接口部、第 1 对话密钥发生部、对话密钥加密部、对话密钥解密部、第 1 特许数据加密处理部、第 2 特许数据加密处理部、传送运行记录信息保持部。传送控制部，控制数据供给装置。传送信息保持部，保持加密内容数据及再生信息。第 1 接口部，与外部之间进行数据的发送接收。第 1 对话密钥发生部，生成在再生信息对终端的每次传送中更新的第 1 共用密钥。对话密钥加密部，由对应于用户的终端而预先设定的第 1 公开加密密钥对第 1 共用密钥进行加密并供给第 1 接口部。对话密钥解密部，对由第 1 共用密钥加密后送回的第 2 公开加密密钥及第 2 共用密钥进行解密。第 1 特许数据加密处理部，利用由对话密钥解密部解密后的第 2 公开加密密钥对用于再生加密内容数据的再生信息进行加密。第 2 特许数据加密处理部，用第 2 共用密钥进一步对第 1 特许数据

加密处理部的输出进行加密，并传送给第 1 接口部。传送运行记录信息保持部，保持表示传送处理中的处理状态的传送运行记录。传送运行记录信息，具有在每次进行再生信息的传送处理时由数据供给装置生成并用于特定再生信息的传送处理的通信特定信息。多个终端，通过通信路径从内容数据供给装置接收传送，并分别与多个用户相对应。各终端，包括第 2 接口部、接收控制部、数据存储部。第 2 接口部，与外部之间进行数据的发送接收。接收控制部，对与外部之间的数据发送接收进行控制。数据存储部，接收和存储加密内容数据及再生信息。数据存储部，具有第 1 密钥保持部、第 1 解密处理部、第 2 密钥保持部、密钥生成部、第 1 加密处理部、第 2 解密处理部、第 1 存储部、第 3 密钥保持部、第 3 解密处理部、第 2 存储部。第 1 密钥保持部，保持用于对由对应于数据存储部而预先设定的第 1 公开加密密钥加密后的数据进行解密的第 1 保密解密密钥。第 1 解密处理部，接收在再生信息的每次通信中更新后传送且由第 1 公开加密密钥加密后的第 1 共用密钥，并进行解密处理。第 2 密钥保持部，保持对每个数据存储部都不相同的第 2 公开加密密钥。密钥生成部，在再生信息的每次通信中更新而生成第 2 共用密钥。第 1 加密处理部，根据第 1 共用密钥对第 2 公开加密密钥及第 2 共用密钥进行加密并输出。第 2 解密处理部，接收由第 2 公开加密密钥加密、进一步再由第 2 共用密钥加密后的再生信息，并根据第 2 共用密钥进行解密。第 1 存储部，保持基于第 2 解密处理部的输出的数据，第 3 密钥保持部，保持用于对由第 2 公开加密密钥加密后的数据进行解密的第 2 保密解密密钥。第 3 解密处理部，在从与再生信息有关的数据对第 1 存储部的存储处理到提取再生信息的处理的过程中，对第 2 保密解密密钥进行解密处理。第 2 存储部，存储表示再生信息的传送处理中的处理状态且包含通信特定信息的接收运行记录。接收控制部，当传送处理过程中通信路径被切断时，根据接收运行记录控制重新传送处理。第 1 存储部，保持基于第 2 解密处理部的输出或第 2 复合处理部的输出的再生信息。接收控制部，当传送处理过程中通信路径被切断时，向数据供给装置发送接收运行记录信息，传送控制部，当传送处理过程中通信路径被切断时，根据接收运行记录信息和传送运行记录信息控制重新传送处理。

进一步，按照本发明的另一方面，提供一种备有数据存储部的向与多个用户分别对应的多个终端供给再生信息的数据供给装置，该数据存储部，用于记录包含着与加密内容数据的再生相关且用于对加密内容数据进行解密而使其成为明文的解密密钥即内容密钥并与加密内容数据分别供给的再生信息及在接收和记录再生信息的传送处理中表示传送处理的处理状态且包含通信特定信息的接收运行记录信息，该数据供给装置，备有传送信息保持部、第 1 接口部、第 1 对话密钥发生部、对话密钥加密部、对话密钥解密部、第 1 特许数据加密处理部、第 2 特许数据加密处理部、传送运行记录信息保持部、传送控制部。

传送信息保持部，保持加密内容数据及再生信息。第 1 接口部，与外部之间进行数据的发送接收。第 1 对话密钥发生部，生成在再生信息对终端的每次传送中更新的第 1 共用密钥。对话密钥加密部，由对应于用户的终端而预先设定的第 1 公开加密密钥对第 1 共用密钥进行加密并供给第 1 接口部。对话密钥解密部，对由第 1 共用密钥加密后送回的第 2 公开加密密钥及第 2 共用密钥进行解密。

第 1 特许数据加密处理部，利用由对话密钥解密部解密后的第 2 公开加密密钥对用于再生加密内容数据的再生信息进行加密。第 2 特许数据加密处理部，用第 2 共用密钥进一步对第 1 特许数据加密处理部的输出进行加密，并传送给第 1 接口部。传送运行记录信息保持部，保持表示传送处理中的处理状态且包含通信特定信息的传送运行记录信息。传送控制部，控制数据供给装置的动作，在每次进行再生信息的传送处理时生成用于特定再生信息的传送处理的通信特定信息并发送到终端，传送控制部，当传送处理过程中通信路径被切断时，根据由数据存储部记录且从终端发送来的接收运行记录信息和传送运行记录信息，确认是来自切断前相互通信着的终端的重新传送请求，从而控制重新传送处理。

因此，在本发明的采用了数据再生装置的传送系统及用于该系统的存储插卡中，服务器及存储插卡都保持着传送的历史记录和传送的状态，所以，即使在传送过程中发生了通信的中断时，也可以通过重新开始通信而重新发送信息，因而可以提高传送处理的可靠性。

附图的简单说明:

图 1 是用于简略地说明本发明的数据传送系统的总体结构的概念图。

图 2 是说明图 1 示出的数据传送系统中所使用的用于通信的数据、信息等的特性的图。

图 3 是表示特许服务器 10 的结构的简略框图。

图 4 是表示携带式电话机 100 的结构的简略框图。

图 5 是表示存储卡 110 的结构的简略框图。

图 6 是用于说明实施例 1 的数据传送系统中的传送动作的第 1 流程图。

图 7 是用于说明实施例 1 的数据传送系统中的传送动作的第 2 流程图。

图 8 是用于说明实施例 1 的数据传送系统中的传送动作的第 3 流程图。

图 9 是用于说明重新接通处理的流程图。

图 10 是用于说明实施例 1 的数据传送系统中的第 2 重新接通动作的第 1 流程图。

图 11 是用于说明实施例 1 的数据传送系统中的第 2 重新接通动作的第 2 流程图。

图 12 是用于说明实施例 1 的数据传送系统中的第 2 重新接通动作的第 3 流程图。

图 13 是用于说明实施例 1 的数据传送系统中的第 3 重新接通动作的流程图。

图 14 是用于说明重新接通处理的流程图。

图 15 是用于说明实施例 2 的数据传送系统中的内容购入时发生的传送动作的第 1 流程图。

图 16 是用于说明实施例 2 的数据传送系统中的内容购入时发生的传送动作的第 2 流程图。

图 17 是用于说明实施例 2 的数据传送系统中的内容购入时发生的传送动作的第 3 流程图。

图 18 是用于说明实施例 2 的数据传送系统中的第 2 重新接通动作的第 1 流程图。

图 19 是用于说明实施例 2 的数据传送系统中的第 2 重新接通动作的第 2 流程图。

图 20 是用于说明实施例 2 的数据传送系统中的第 2 重新接通动作的第 3 流程图。

图 21 是用于说明实施例 3 的数据传送系统中的第 2 重新接通动作的第 1 流程图。

图 22 是用于说明实施例 3 的数据传送系统中的第 2 重新接通动作的第 2 流程图。

图 23 是用于说明实施例 3 的数据传送系统中的第 2 重新接通动作的第 3 流程图。

图 24 是用于说明实施例 3 的数据传送系统中的第 2 重新接通动作的第 4 流程图。

用于实施发明的最佳形态

以下，参照附图说明本发明的实施例。

[实施例 1]

图 1 是用于简略地说明本发明的数据传送系统的总体结构的概念图。

另外，在下文中，以通过携带式电话网将音乐数据传送给用户的数据传送系统的结构为例进行说明，但从以下的说明中可以看出，本发明并不限定于这种情况，在通过其他信息通信网传送其他的内容数据、朗读数据、图象数据、视频数据、教材数据等情况下，也可以应用。

参照图 1，对存在着著作权的音乐数据进行管理的特许服务器 10，在按规定的加密方式将音乐数据（以下，也称作内容数据）加密后，将这种加密数据传送给作为用于传送信息的传送载体 20 的携带式电话公司。另一方面，认证服务器 12，对请求传送内容数据而进行了访问的用户是否用合法的设备进行了访问的情况进行认证。

携带式电话公司 20，通过自己的携带式电话网将来自各用户的传送要求（传送请求）转接到特许服务器 10。特许服务器 10，当接收到传送请求时，由认证服务器 12 确认用户从合法的设备进行着访问，并在将所请求的音乐数据进一步加密后通过携带式电话公司 20 的携带式电话网向各用户的携带式电话机传送内容数据。

在图 1 中，例如，构成为将可插卸的存储卡 110 插装在携带式电话用户 1 的携带式电话机 100 内。存储卡 110，接收由携带式电话机 100 接收到的加密内容数据，并对在上述发送时所执行的加密进行解密，然后供给到携带式电话机 100 中的音乐再生电路（图中未示出）。

进一步，例如，用户 1，可以通过与携带式电话机 100 连接的耳机 130 等将上述音乐数据「再生」后进行收听。

在下文中，假定将上述特许服务器 10、认证服务器 12 及传送载体（携带式电话公司）20 合在一起总称为传送服务器 30。

另外，还假定将从上述传送服务器 30 向各携带式电话机等传输内容数据的处理称为「传送」。

在按如上方式构成的情况下，首先，从结构上就使不具备存储卡 110 的用户不能接收和再生来自传送服务器 30 的传送数据。

而且，如果每当传送例如一首乐曲的内容数据时由传送载体 20 对其次数进行计数从而由传送载体 20 按携带式电话的通话费用征收用户每次接收（下载）内容数据时产生的著作权费用，则使著作权者很容易确保著作权费用。

而且，这种内容数据的传送，通过携带式电话网这种封闭型的系统进行，所以，与因特网等开放型的系统相比，具有易于采取著作权保护对策的优点。

这时，例如，可以由具有存储卡 112 的用户 2 用自己的携带式电话机 102 从传送服务器 30 直接接收内容数据的传送。但是，假如用户 2 从传送服务器 30 直接接收数据量相当大的内容数据等时，则为进行这种接收有时将需要很长的时间。在这种情况下，如果可以从已经接收了该内容数据的传送的用户 1 复制该内容数据，则对用户来说将带来很大的方便。

但是，从著作权者的权利保护的观点考虑，在系统的结构上不容许对内容数据的复制放任自流。

如图 1 所示，将用户 1 接收到的内容数据与内容数据本身及为能再生该内容数据所需的再生信息一起复制到用户 2 的情况，称为音乐数据的「移动」。在这种情况下，通过携带式电话机 100 和 102 而在存储卡 110 和 112 之间移动加密后的内容数据及为进行再生所需的再生信息。这里，「再生信息」，如后文所述，具有可以对按规定加密方

式加密后的内容数据进行解密的特许密钥、与访问再生有关的限制信息及内容 ID（标识符）等特许信息。

与此不同，将只复制内容数据而不同时进行再生信息的移动的情况，称为「复制」。由于在复制过程中不同时移动再生信息，所以接受了复制的用户只需向传送服务器 30 请求再生信息的传送即可变成可以再生的状态。在这种情况下，可以省去传送内容数据时的数据量相当大的传送。

通过采用如上所述的结构，在接收者一侧可以灵活地使用已从传送服务器 30 接收传送后的内容数据。

另外，当携带式电话机 100 和 102 是 PHS(Personal Handy Phone: 个人手持式电话机）时，可以进行所谓的收发两用模式的通话，所以，可以利用这种功能进行用户 1 和用户 2 之间的信息移动。

在如图 1 所示的结构中，为了可以在用户侧对加密后传送的内容数据进行再生，在系统的构成上，第 1，必须是用于传送通信中的加密密钥的方式，第 2，必须是对传送数据进行加密的方式，进一步，第 3，必须实现数据保护，以防擅自复制按上述方式传送的数据。

在本发明的实施例中，特别是，说明一种在信息的发送侧及接收侧双方记录保持传送中的状态和历史记录信息从而即使在传送过程中发生了通信的中断时也可以通过重新开始通信而重新发送信息因而可以提高传送处理的可靠性的系统。

[系统的密钥及数据的构成]

图 2 是说明图 1 示出的数据传送系统中所使用的用于通信的数据、信息等的特性的图。

首先，由传送服务器 30 传送的数据 Data，是音乐数据等内容数据。内容数据 Data，如后文所述，以进行了至少可以用特许密钥 Kc 解密的加密后的加密内容数据{Data}Kc 的形式，由传送服务器 30 分别向用户发送。

另外，在下文中，{Y}X 这样的符号，表示将数据 Y 变换为可以用密钥数据 X 解密的密码后的信息。

进一步，与内容数据一起从传送服务器发送与内容数据有关的或与服务器访问相关的明文信息形式的附加信息 Data-inf。即，在附加信息 Data-inf 中，包含着用于特定内容数据的乐曲名或艺术家姓名等

内容数据的信息及用于特定传送服务器30是哪一个服务器的信息。

其次，作为与内容数据的加密或解密及再生处理、以及再生电路即携带式电话机或记录媒体即存储卡的认证有关的密钥，有以下的几种。

即，如上所述，分别设定用于对加密内容数据进行解密的特许密钥Kc、内容再生电路（携带式电话机100）所固有的公开加密密钥KPp（n）、存储卡所固有的公开加密密钥KPmc（m）。

由公开加密密钥KPp（n）及KPmc（m）加密后的数据，可以分别由内容再生电路（携带式电话机100）所固有的保密解密密钥Kp（n）及存储卡所固有的保密解密密钥Kmc（m）进行解密。这些固有的保密解密密钥，具有对每种类型的携带式电话机及每种类型的存储卡都不相同的内容。这里，所谓携带式电话机或存储卡的类型，根据其制造厂商、产品的类型和制造日期（制造批号）的不同等规定。该公开加密密钥及保密解密密钥的赋予单位，称为密级。自然数m、n，分别表示用于区分各存储卡及内容再生电路（携带式电话机）的密级的编号。

进一步，作为由整个传送系统共同使用的密钥，主要有特许密钥Kc或为取得如后文所述的对再生电路的限制信息等而使用的保密共用密钥Kcom、及认证密钥Kpma。保密共用密钥Kcom，由传送服务器和携带式电话机双方保持。

另外，上述的按每个存储卡及内容再生电路设定的公开加密密钥KPmc（m）及KPp（n），可以通过用认证密钥Kpma进行解密而确认其合法性。即在出厂时时分别以作为认证处理的对象的认证数据{KPmc（m）}Kpma及{KPp（n）}Kpma的形式记录在存储卡及携带式电话机内。

此外，保密共用密钥Kcom，并不限定于共用密钥方式，也可以置换为公开密钥方式的保密解密密钥和公开加密密钥Kpcom后使用。在这种情况下，在携带式电话机100内保持保密解密密钥Kcom，但将公开加密密钥Kpcom作为加密密钥保持在传送服务器30内。

进一步，作为用于对构成系统的设备、即用作内容再生电路的携带式电话机100和存储卡110的动作进行控制的信息，包括当使用者购入特许密钥等时为指定其购入条件而从携带式电话机100向传送服

务器 30 发送的购入条件 AC、根据购入条件 AC 从传送服务器 30 向存储卡 110 传送的表示为再生而访问特许密钥 Kc 的次数（允许再生次数）或特许密钥 Kc 的复制和移动次数及对复制和移动的限制的访问限制信息 AC1、从传送服务器 30 向携带式电话机 100 传送的表示再生电路的再生条件的限制的再生电路限制信息 AC2。所谓再生电路的再生条件，例如意味着在为新乐曲的促销而以廉价或免费的方式传送样品等情况下只允许再生各内容数据的开头的规定时间或再生期限等条件。

另外，作为用于管理存储卡 100 内的数据处理的密钥，有按每个存储卡这样的媒体分别设定的各存储卡所固有的公开加密密钥 KPm（i）（i 为自然数）、可以对由公开加密密钥 KPm（i）加密后的数据进行解密的各存储卡所固有的保密解密密钥 Km（i）。这里，自然数 i，表示用于区别各存储卡的编号。

进一步，在图 1 所示的数据传送系统中，作为在数据通信时使用的密钥等，有以下几种。

即，作为用于对存储卡的外部与存储卡之间的数据发送接收进行保密的密钥，采用每当进行内容数据的传送、再生及移动时由服务器 30、携带式电话机 100 或 102、存储卡 110 或 112 生成的共用密钥 Ks1～Ks4。

这里，共用密钥 Ks1～Ks4，是按服务器、携带式电话机或存储卡之间的通信单位或访问单位即在每次「对话」中产生的固有共用密钥，在下文中，也将这些共用密钥 Ks1～Ks4 称为「对话密钥」。

这些对话密钥 Ks1～Ks4，由于在每次通信对话中具有固有值，所以由传送服务器、携带式电话机及存储卡管理。

具体地说，对话密钥 Ks1，由传送服务器 30 在每次传送对话时产生。对话密钥 Ks2，由存储卡在每次传送对话及移动（接收侧）对话时产生，对话密钥 Ks3，同样由存储卡在每次再生对话及移动（发送侧）对话时产生，对话密钥 Ks4，由携带式电话机在每次再生对话时产生。在各对话中，发送接收这些对话密钥，并接收由其他设备生成的对话密钥，在以该对话密钥执行了加密后进行特许密钥等的发送，从而可以提高对话中的安全强度。

进一步，作为与传送服务器之间发送接收的数据，有用于由系统

对内容数据进行识别的内容 ID、用于特定何时和对谁进行再生信息的发送并在每次传送对话时生成的特定各传送对话的代码即事务 ID 等。此外，特许 ID 与事务 ID 也可以兼用。

特许 ID、内容 ID 及访问限制信息 AC1，总称为特许信息，该特许信息、特许密钥 Kc 及再生电路限制信息 AC2，总称为再生信息。

[特许服务器 10 的结构]

图 3 是表示图 1 示出的特许服务器 10 的结构的简略框图。

特许服务器 10，备有用于保持按规定方式将内容数据加密后的数据及内容 ID 等传送信息的信息数据库 304、用于按每个用户保持随着对内容数据的访问开始的计费信息的计费数据库 302、用于保持特许服务器的运行记录信息的运行记录管理数据库 306、用于通过数据总线 BS1 接收来自信息数据库 304、计费数据库 302 及运行记录管理数据库 306 的数据并进行规定的处理的数据处理部 310、在传送载体 20 和数据处理部 310 之间通过通信网进行数据发送接收的通信装置 350。

这里，作为表示由运行记录管理数据库 306 保持的特许信息的传送历史记录的「特许传送运行记录」，有事务 ID、内容 ID、公开加密密钥 KPmc（m）及 KPp（n）、访问限制信息 AC1、再生电路限制信息 AC2、公开加密密钥 KPm（i）、对话密钥 Ks2、计费状态标志等信息。计费状态标志，是表示对传送中的内容数据的计费处理是否已经结束的标志。

数据处理部 310，包括用于根据数据总线 BS1 上的数据控制数据处理部 310 的动作的传送控制部 315、由传送控制部 315 控制并用于在传送对话时产生对话密钥 Ks1 的对话密钥发生部 316、通过通信装置 350 及数据总线 BS1 接收从存储卡及携带式电话机传送来的用于认证的认证数据{KPmc（m）} Kpma 及{KPp（n）} Kpma 并进行与认证密钥 Kpma 对应的解密处理的解密处理部 312、利用由解密处理部 312 取得的公开加密密钥 KPmc（m）将由对话密钥发生部 316 生成的对话密钥 Ks1 加密后输出到数据总线 BS1 上用的加密处理部 318、从数据总线 BS1 接收由各用户利用对话密钥 Ks1 加密后发送的数据并进行解密处理的解密处理部 320。

数据处理部 310，还包括保持保密共用密钥 Kcom 的 Kcom 保持部 322、利用保密共用密钥 Kcom 对从传送控制部 315 供给的特许密

钥 Kc 及再生电路限制信息 AC2 进行加密的加密处理部 324、利用由解密处理部 320 取得的存储卡所固有的公开加密密钥 KPm（i）对从加密处理部 324 输出的数据进行加密用的加密处理部 326、利用从解密处理部 320 供给的对话密钥 Ks2 进一步将加密处理部 326 的输出加密后输出到数据总线 BS1 用的加密处理部 328。

另外，在使保密共用密钥 Kcom 为非对称的公开密钥密码系统的密钥的情况下，保持密钥数据的保持部 322，保持作为公开密钥方式的加密密钥的公开加密密钥 Kpcom，而不是共用密钥方式的保密共用密钥 Kcom。

[携带式电话机 100 的结构]

图 4 是表示图 1 示出的携带式电话机 100 的结构的简略框图。

在携带式电话机 100 中，假定表示密级的自然数 n 为 n=1。

携带式电话机 100，包括用于接收由携带式电话网以无线方式传输的信号的天线 1102、用于接收来自天线 1102 的信号并变换为基带信号或对来自携带式电话机的数据进行调制后供给天线 1102 的发送接收部 1104、用于进行携带式电话机 100 的各部的数据发送接收的数据总线 BS2、用于通过数据总线 BS2 控制携带式电话机 100 的动作的控制器 1106。

携带式电话机 100，还包括将来自外部的指示供给携带式电话机 100 的键盘 1108、用于将从控制器 1106 等输出的信息作为视觉信息供给用户的显示器 1110、用于在通常的通话动作中根据通过数据总线 BS2 供给的接收数据对语音进行再生的语音再生部 1112、用于与外部之间进行数据的发送接收的连接器 1120、用于将来自连接器 1120 的数据变换为可以供给数据总线 BS2 的信号或将来自数据总线 BS2 的数据变换为可以供给连接器 1120 的信号的外部接口部 1122。

携带式电话机 100，还包括用于存储来自传送服务器 30 的内容数据（音乐数据）并进行解密处理的可插卸的存储卡 110、用于控制存储卡 110 与数据总线 BS2 之间的数据的发送接收的存储接口 1200、保持加密到可以通过用认证密钥 Kpma 将按每个携带式电话机的密级设定的公开加密密钥 KPp（1）解密而进行认证的状态的数据的认证数据保持部 1500。

进一步，携带式电话机 100，还包括保持携带式电话机（内容再

生电路）的密级所固有的解密密钥即保密解密密钥 Kp（n）（n=1）的 Kp 保持部 1502、利用保密解密密钥 Kp（1）对从数据总线 BS2 接收到的数据进行解密并取得由存储卡产生的对话密钥 Ks3 的解密处理部 1504、在对存储卡 110 所存储的内容数据进行再生的再生对话中由随机数等生成用于将在数据总线 BS2 上与存储卡之间交换的数据加密的对话密钥 Ks4 的对话密钥发生部 1508、利用由解密处理部 1504 取得的对话密钥 Ks3 将所生成的对话密钥 Ks4 加密并输出到数据总线 BS2 上的加密处理部 1506、利用对话密钥 Ks4 将数据总线 BS2 上的数据解密后输出数据{Kc‖AC2}Kcom 的解密处理部 1510。

携带式电话机 100，还包括保持保密共用密钥 Kcom 的 Kcom 保持部 1512、利用保密共用密钥 Kcom 对解密处理部 1510 输出的数据{Kc‖AC2}Kcom 进行解密并输出特许密钥 Kc 及再生电路限制信息 AC2 的解密处理部 1514、从数据总线 BS2 接收加密后的加密内容数据{Data}Kc 并由从解密处理部 1514 取得的特许密钥 Kc 将其解密后输出内容数据 Data 的解密处理部 1516、用于接收解密处理部 1516 的输出即内容数据 Data 并对音乐进行再生的音乐再生部 1518、用于接收音乐再生部 1518 和语音再生部 1112 的输出并根据动作模式而进行有选择的输出的切换部 1525、用于接收切换部 1525 的输出并与耳机 130 连接的连接端子 1530。

这里，从解密处理部 1514 输出的再生电路限制信息 AC2，通过数据总线 BS2 供给控制器 1106。

另外，在图 4 中，为简化说明，只给出了携带式电话机中与本发明的音乐数据的传送有关的部件，而省略了携带式电话机本来备有的与通话功能有关的一部分部件。

[存储卡 110 的结构]

图 5 是表示图 1 示出的存储卡 110 的结构的简略框图。

如上所述，公开加密密钥 KPm（i）及与其对应的保密解密密钥 Km(i)，对每个存储卡为固有值，但在存储卡 110 中假定该自然数 i=1。此外，作为存储卡的密级所固有的公开加密密钥及保密解密密钥，设有 KPmc（m）及 Kmc（m），但在存储卡 110 中，自然数 m，假定用 m=1 表示。

存储卡 110，包括保持认证数据{KPmc（m）} Kpma 的认证数据

保持部 1400、保持作为按每个存储卡的密级设定的固有解密密钥的 Kmc（1）的 Kmc 保持部 1402、保持按每个存储卡固有地设定的公开加密密钥 KPm（1）的 KPm（1）保持部 1416、保持可以用公开加密密钥 KPm（1）解密的非对称保密解密密钥 Km（1）的 Km（1）保持部 1421。其中，认证数据保持部 1400，对按每个存储卡的密级设定的公开加密密钥 KPmc（1）进行可以通过用认证密钥 Kpma 解密而认证其合法性的加密后加以保持。

存储卡 110，还包括通过端子 1202 与存储接口 1200 之间进行信号的发送接收的数据总线 BS3、根据由存储接口 1200 供给数据总线 BS3 的数据从 Kmc（1）保持部 1402 接收每个存储卡的密级所固有的保密解密密钥 Kmc（1）并将传送服务器在传送对话中生成的对话密钥 Ks3 输出到接点 Pa 的解密处理部 1404、从 KPma 保持部 1443 接收认证密钥 Kpma 后用认证密钥 Kpma 从供给到数据总线 BS3 的数据执行解密处理并将解密结果输出到加密处理部 1410 的解密处理部 1408、利用由切换开关 1442 有选择地供给的密钥数据对由切换开关 1444 有选择地供给的数据进行加密并输出到数据总线 BS3 的加密处理部 1406。

存储卡 110，还包括在传送、再生及移动的各对话中产生对话密钥的对话密钥发生部 1418、利用由解密处理部 1408 取得的公开加密密钥 KPp（n）将对话密钥发生部 1418 输出的对话密钥加密后输出到数据总线 BS3 的加密处理部 1410、从 BS3 接收加密后的数据而由从对话密钥发生部 1418 取得的对话密钥 Ks3 进行解密并将解密结果输出到数据总线 BS4 的解密处理部 1412。

存储卡 110，还包括在传送或移动对话等的过程中利用存储卡固有的公开加密密钥 KPm（i）（i 也可以为 1 或其他的存储卡的编号 j）对数据总线 BS4 上的数据进行加密的加密处理部 1424、利用与公开加密密钥 KPm（1）构成一对的存储卡 110 所固有的保密解密密钥 Km（1）对数据总线 BS4 上的数据进行解密用的解密处理部 1422、用于从数据总线 BS4 接收和存储用公开加密密钥 KPm（1）加密的再生信息（特许密钥 Kc、内容 ID、事务 ID、访问限制信息 AC1、再生电路限制信息 AC2）的一部分并从数据总线 BS3 接收和存储加密内容数据{Data}Kc 的存储器 1415。

携带式电话机 110，还包括用于保持由解密处理部 1422 取得的特许信息（事务 ID、内容 ID 及访问限制信息 AC1）的特许信息保持部 1440、用于保持与存储卡中的再生信息的发送接收有关的运行记录的运行记录存储器 1460、通过数据总线 BS3 与外部之间进行数据的发送接收并与数据总线 BS4 之间进行再生信息等的接收从而对存储卡 110 的动作进行控制的控制器 1420。

作为表示保持在运行记录存储器 1460 内的再生信息的接收状态的「接收运行记录」，有事务 ID 和对话密钥 Ks2 等。在实施例 1 中，这些接收运行记录信息，是进行特许信息的接收时生成的数据，在存储卡 110 对再生信息的接收和保持结束的时刻将其删除。

另外，在图 5 中，用实线围出的区域 TRM，组装成一个 TRM 模块，当从外部进行了非法的开封处理等时，在存储卡 110 内，通过删除内部数据并使内部电路损坏，即可使第三者不能读出存在于该区域中的电路内的数据等。这种模块，就是一般的防窜改模块（Tamper Resistance Module）。

当然，在结构上也可以包含存储器 1415 而将其组装在 TRM 模块内。但是，在如图 5 所示的结构中，保持在存储器 1415 内的数据，都是进行了加密的数据，所以第三者只用该存储器 1415 内的数据不可能从内容数据再生音乐，而且，由于没有必要将存储器 1415 设在高价的防窜改模块内，所以具有降低制造成本的优点。

[传送动作]

以下，参照流程图详细说明本发明实施例的数据传送系统的各对话中的动作。

图 6、图 7 和图 8，是用于说明实施例 1 的数据传送系统中的购入内容数据时发生的传送动作（以下，也称为传送对话）的第 1、第 2 和第 3 流程图。

在图 6～图 8 中，说明用户 1 在使用存储卡 110 的情况下通过携带式电话机 100 从传送服务器 30 接收音乐数据的传送时的动作。

首先，用户 1，通过携带式电话机 100 的键盘 1108 的按键操作等发出传送请求（步骤 S100）。

在存储卡 110 中，响应该传送请求，从认证数据保持部 1400 输出认证数据{KPmc（1）}Kpma（步骤 S102）。

携带式电话机 100，除了从存储卡 110 受理的用于认证的认证数据{KPmc（1）} Kpma 外，还将用于携带式电话机 100 本身的认证的认证数据{KP（1）} Kpma、内容 ID、特许购入条件 AC 发送到传送服务器 30（步骤 S104）。

在传送服务器 30 中，从携带式电话机 100 接收内容 ID、认证数据{KPmc（1）} Kpma 、{KP（1）} Kpma、特许购入条件 AC（步骤 S106），并由解密处理部 312 用认证密钥 Kpma 执行解密处理，从而受理作为存储卡 110 的公开加密密钥的 KPmc（1）及作为携带式电话机 100 的公开加密密钥的 KP（1）（步骤 S108）。

传送控制部 315，根据所受理的公开加密密钥 KPmc（1）及 KP（1）向认证服务器 12 进行查询（步骤 S110），当这些公开加密密钥有效时进入随后的处理（步骤 S112），当这些公开加密密钥无效时，结束处理（步骤 S170）。

这里，在利用认证密钥 Kpma 的解密处理中，当进行公开加密密钥 KP（1）或 KPmc（1）的合法性的认证时，向认证服务器 12 进行了查询，但由于公开加密密钥 KP（1）或 KPmc（1）分别进行了可以通过用认证密钥 Kpma 进行解密而判断其合法性的加密，所以在结构上也可以由特许服务器 10 的传送控制部 315 根据利用认证密钥 Kpma 的解密结果独自进行认证。

当从查询的结果识别出是向合法的存储卡进行传送时，传送控制部 315，接着生成用于特定传送对话的事务 ID（步骤 S112）。

当从查询的结果确认是向合法的存储卡进行传送时，进一步，传送控制部 315，将事务 ID、内容 ID、公开加密密钥 KPmc（1）及 KPp（1）与尚未计费的信息（计费状态标志）一起作为特许传送运行记录存储在管理数据库 306 内（步骤 S113）

接着，在传送服务器 30 中，对话密钥发生部 316，生成用于传送的对话密钥 Ks1。对话密钥 Ks1，由加密处理部 318 利用由解密处理部 312 取得的与存储卡 110 对应的公开加密密钥 KPmc（1）进行加密（步骤 S114）。

将事务 ID 与加密后的对话密钥{Ks1}Kmc（1）通过数据总线 BS1 及通信装置 350 输出到外部（步骤 S116）。

携带式电话机 100，当接收到事务 ID 及加密后的对话密钥

{Ks1}Kmc（1）时（步骤 S118），在存储卡 110 中，将接收数据通过存储接口 1200 供给数据总线 BS3。解密处理部 1404，通过由保持部 1402 所保持的存储卡 110 所固有的保密解密密钥 Kmc(1)对{Ks1}Kmc（1）进行解密处理，解密并提取对话密钥 Ks1，因此，受理事务 ID 及对话密钥 Ks1（步骤 S120）。

将到此为止的直到步骤 S120 的处理，称为「事务 ID 取得步骤」。

参照图 7，控制器 1420，当确认受理了由传送服务器 30 生成的对话密钥 Ks1 时，指示对话密钥发生部 1418 生成由存储卡 110 在进行传送动作时生成的对话密钥 Ks2。进一步，控制器 1420，将对话密钥 Ks2 与接收到的事务 ID 一起作为接收运行记录存储在运行记录存储器 1460 内（步骤 S121）。

加密处理部 1406，利用由解密处理部 1404 通过切换开关 1442 的接点 Pa 供给的对话密钥 Ks1 对通过将切换开关 1444 及 1446 的接点依次切换而供给的对话密钥 Ks2 及公开加密密钥 KPm（1）进行加密，并将{Ks2‖KPm（1）}Ks1 输出到数据总线 BS3（步骤 S122）。

输出到数据总线 BS3 的加密数据{Ks2‖KPm（1）}Ks1，从数据总线 BS3 通过端子 1202 及存储接口 1200 发送到携带式电话机 100，并从携带式电话机 100 发送到传送服务器 30（步骤 S124）。

传送服务器 30，接收到加密数据{Ks2‖KPm（1）}Ks1 后，由解密处理部 320 利用对话密钥 Ks1 执行解密处理，并受理由存储卡 110 生成的对话密钥 Ks2 及存储卡 110 所固有的公开加密密钥 KPm（1）（步骤 S126）。

然后，传送控制部 315，根据在步骤 S106 中取得的内容 ID 及特许购入条件 AC，生成访问限制信息 AC1 及再生电路限制信息 AC2(步骤 S130)。进一步，从信息数据库 304 取得用于对加密内容数据进行解密的特许密钥 Kc（步骤 S132）。

传送控制部 315，将所取得的特许密钥 Kc 及再生电路限制信息 AC2 供给加密处理部 324。加密处理部 324，利用从 Kcom 保持部 322 取得的保密共用密钥 Kcom 将特许密钥 Kc 及再生电路限制信息 AC2 加密（步骤 S134）。

由加密处理部 326 利用由解密处理部 320 取得的公开加密密钥 KPm（1）对加密处理部 324 输出的加密数据{Kc‖AC2}Kcom 及传送

控制部 315 输出的事务 ID、内容 ID 及访问限制信息 AC1 进行加密(步骤 S136)。

加密处理部 328，接收加密处理部 326 的输出，并利用由存储卡 110 生成的对话密钥 Ks2 将其加密（步骤 S137)。

传送控制部 315，将访问限制信息 AC1、再生电路限制信息 AC2、公开加密密钥 KPm（1)、对话密钥 Ks2 与已计费的信息（计费状态标志）一起存储在运行记录管理数据库 306 内（步骤 S138)。

由加密处理部 328 输出的加密数据{{{Kc‖AC2}Kcom‖事务 ID‖内容 ID‖AC1}Km（1）}Ks2，通过数据总线 BS1 及通信装置 350 发送到携带式电话机 100（步骤 S139)。

按照如上方式，通过交换由发送服务器及存储卡分别生成的对话密钥并由双方利用接收到的加密密钥执行加密后将该加密数据发送到对方，在各自的加密数据的发送接收中都可以进行实际上的相互认证，因而可以提高数据传送系统的安全性。进一步，还可以在传送服务器 30 内记录保持与计费状态、传送的历史记录有关的信息。

携带式电话机 100，接收发送到的加密数据{{{Kc‖AC2}Kcom‖事务 ID‖内容 ID‖AC1}Km（1）}Ks2（步骤 S140)，并在存储卡 110 内由解密处理部 1412 对通过存储接口 1200 供给数据总线 BS3 的接收数据进行解密。即，解密处理部 1412，利用从对话密钥发生部 1418 供给的对话密钥 Ks2 将数据总线 BS3 的接收数据解密并输出到数据总线 BS4（步骤 S144)。

参照图 8，在步骤 S144 的阶段中，将可以用 Km（1）保持部 1421 所保持的保密解密密钥 Km（1）解密的数据{{Kc‖AC2}Kcom‖事务 ID‖内容 ID‖AC1}Km（1）输出到数据总线 BS4。该数据{{Kc‖AC2}Kcom‖事务 ID‖内容 ID‖AC1}Km（1)，首先由保密解密密钥 Km（1）解密，并受理作为再生信息的数据{Kc‖AC2}Kcom、事务 ID、内容 ID、访问限制信息 AC1（步骤 S146)。

将事务 ID、内容 ID、访问限制信息 AC1 记录在特许信息保持部 1440 内。数据{Kc‖AC2}Kcom，再次由公开加密密钥 KPm（1）进行加密，并作为数据{{Kc‖AC2}Kcom} Km（1）存储在存储器 1415 内（步骤)。

进一步，将运行记录存储器 1460 中的接收运行记录删除（步骤

S150)。

将从步骤 S121 到步骤 S150 的处理称为「再生信息取得步骤」。在该「再生信息取得步骤」中，进行计费对象的处理。

在直到步骤 S150 的处理正常完成的阶段，从携带式电话机 100 向传送服务器 30 发出内容数据的传送请求（步骤 S152)。

传送服务器 30，接收内容数据传送请求后，从信息数据库 304 取得加密内容数据{Data}Kc 及附加信息 DATA-inf，并将这些数据通过数据总线 BS1 及通信装置 350 输出（步骤 S154)。

携带式电话机 100，接收{Data}Kc‖DATA-inf，并受理加密内容数据{Data}Kc 及附加信息 DATA-inf（步骤 S156)。加密内容数据{Data}Kc 及附加信息 DATA-inf，通过存储接口 1200 及端子 1202 传送到存储卡 110 的数据总线 BS3。在存储卡 110 中，将接收到的加密内容数据{Data}Kc 及附加信息 DATA-inf 直接存储在存储器 1415 内（步骤 S158)。

将从步骤 S152 到步骤 S158 的处理称为「内容数据取得步骤」。在该「内容数据取得步骤」中，进行计费对象以外的处理。

进一步，从存储卡 110 向传送服务器 30 发送传送受理的通知（步骤 S162)，并在进行对计费数据库 302 的计费数据存储等的同时，执行结束传送的处理（步骤 S164)，从而结束传送服务器的处理（步骤 S170)。

[重新接通动作]

以下，说明在如上所述的传送动作的任何处理步骤的阶段中发生了通信线路的中断时为再次接收传送而进行重新接通时的处理。图 9 是用于说明重新接通处理的流程图。

首先，例如，用户 1，通过携带式电话机 100 的键盘 1108 的按键操作等发出重新接通的请求并开始重新接通处理（步骤 S200)。

接着，携带式电话机 100 的控制器 1106，判断发生通信切断的步骤是在哪一步处理中（步骤 S202)，如果该步骤是事务 ID 取得步骤，则由于不作为计费的对象所以重新进行图 6～图 8 的基本传送处理(第 1 重新接通处理)(步骤 S204)，并结束重新接通处理（步骤 S206)。

另一方面，如果通信切断的步骤是特许信息取得步骤（步骤 S202)，则控制器 1106 根据接收运行记录执行后文所述的第 2 重新接

通处理（步骤 S206），或者，如果是内容数据取得步骤（步骤 S2020，则执行后文所述的用于继续进行通信切断时的通信的第 3 重新接通处理（步骤 S206），并结束重新接通处理（步骤 S210）。

[第 2 重新接通处理]

图 10、图 11 和图 12 是用于说明实施例 1 的数据传送系统中的上述第 2 重新接通动作的第 1、第 2 和第 3 流程图。通过对比特许服务器 10 的特许传送运行记录和存储卡 110 的接收运行记录，确认通信切断时的再生信息的传送状态，可以在保护著作者的权利的同时实现对用户的保证。

首先，参照图 10，用户 1，通过携带式电话机 100 的键盘 1108 的按键操作等发出重新接通请求，根据该请求开始第 2 重新接通处理（步骤 S300）。

在存储卡 110 中，响应该重新接通请求，输出保持在运行记录存储器 1460 内的事务 ID（步骤 S302）。

携带式电话机 100，将从存储卡 110 受理的事务 ID 发送到传送服务器 30（步骤 S304）。

在传送服务器 30 中，接收事务 ID（步骤 S306），并由传送控制部 315 检索运行记录管理数据库 306 中的特许传送运行记录（步骤 S308）。

传送控制部 315，当根据事务 ID 确认已经对发出重新接通请求的终端（携带式电话机 100 及存储卡 110）进行了计费处理时（步骤 S308），从特许传送运行记录取得公开加密密钥 KPmc（1）（步骤 S310）。

对话密钥发生部 316，生成用于传送的对话密钥 Ks1。对话密钥 Ks1，由加密处理部 318 利用公开加密密钥 KPmc（1）进行加密（步骤 S312）。

将事务 ID 与加密后的对话密钥{Ks1}Kmc（1）通过数据总线 BS1 及通信装置 350 输出到外部（步骤 S314）。

携带式电话机 100，当接收到事务 ID 及加密后的对话密钥{Ks1}Kmc（1）时（步骤 S316），在存储卡 110 中，由解密处理部 1404 利用保持在保持部 1402 内的存储卡 110 所固有的保密解密密钥 Kmc（1）对通过存储接口 1200 供给数据总线 BS3 的接收数据进行解密处

理，从而解密并提取对话密钥 Ks1（步骤 S318）。

在这之后，进行与图 7 所示的步骤 S121 以后的处理即特许信息取得步骤以后的处理相同的处理。

另一方面，当在步骤 S308 中传送控制部 315 根据对运行记录管理数据库 306 中的特许传送运行记录的检索结果判断为计费处理尚未结束时，从特许传送运行记录取得公开加密密钥 KPmc（1）（步骤 S330）。

接着，在传送服务器 30 中，对话密钥发生部 316，生成用于传送的对话密钥 Ks1。对话密钥 Ks1，由加密处理部 318 利用公开加密密钥 KPmc（1）进行加密（步骤 S332）。

将事务 ID 与加密后的对话密钥{Ks1}Kmc（1）通过数据总线 BS1 及通信装置 350 输出到外部（步骤 S334）。

携带式电话机 100，当接收到事务 ID 及加密后的对话密钥{Ks1}Kmc（1）时（步骤 S336），在存储卡 110 中，由解密处理部 1404 利用保持在保持部 1402 内的存储卡 110 所固有的保密解密密钥 Kmc（1）对通过存储接口 1200 供给数据总线 BS3 的接收数据进行解密处理，从而解密并提取对话密钥 Ks1（步骤 S338）。

加密处理部 1406，利用对话密钥 Ks1 对接收运行记录进行加密，并生成{接收运行记录}Ks1（步骤 S340）。

参照图 11，控制器 1420，指示对话密钥发生部 1418 生成由存储卡 110 在进行传送动作时生成的对话密钥 Ks2 （步骤 S342）。

加密处理部 1406，利用由解密处理部 1404 通过切换开关 1442 的接点 Pa 供给的对话密钥 Ks1 对通过切换开关 1444 及 1446 的接点供给的对话密钥 Ks2 进行加密而生成{Ks2 }Ks1。从存储卡 110 输出按如上所述的方式生成的数据{接收运行记录}Ks1 及{Ks2 }Ks1（步骤 S344）。

输出到数据总线 BS3 的加密数据{接收运行记录}Ks1 及{Ks2 }Ks1，从数据总线 BS3 通过端子 1202 及存储接口 1200 发送到携带式电话机 100，并从携带式电话机 100 发送到传送服务器 30（步骤 S346）。

传送服务器 30，接收到加密数据{接收运行记录}Ks1 及{Ks2 }Ks1 后，由解密处理部 320 利用对话密钥 Ks1 执行解密处理，并受理接收

运行记录及由存储卡 110 生成的对话密钥 Ks2 （步骤 S348）。

然后，传送控制部 315，对所受理的接收运行记录的合法性进行检查（步骤 S350）。

当判定接收运行记录不合法时，结束第 2 重新接通处理（步骤 S390）。

另一方面，当判定接收运行记录合法时，传送控制部 315，从特许传送运行记录取得内容 ID、访问限制信息 AC1、再生电路限制信息 AC2 及公开加密密钥 KPm（1）（步骤 S352）。进一步，从信息数据库 304 取得用于对加密内容数据进行解密的特许密钥 Kc（步骤 S354）。

传送控制部 315，将所取得的特许密钥 Kc 及再生电路限制信息 AC2 供给加密处理部 324。加密处理部 324，利用从 Kcom 保持部 322 取得的保密共用密钥 Kcom 将特许密钥 Kc 及再生电路限制信息 AC2 加密（步骤 S356）。

由加密处理部 326 利用在步骤 S352 中得到的存储卡 110 所固有的公开加密密钥 KPm（1）对加密处理部 324 输出的加密数据{Kc ‖ AC2}Kcom 及传送控制部 315 输出的事务 ID、内容 ID 及访问限制信息 AC1 进行加密（步骤 S358）。

加密处理部 328，接收加密处理部 326 的输出，并利用由存储卡 110 生成的对话密钥 Ks2 进行加密（步骤 S360）。

由加密处理部 328 输出的加密数据{{{Kc ‖ AC2}Kcom ‖ 事务 ID ‖ 内容 ID ‖ AC1}Km（1）}Ks2 ，通过数据总线 BS1 及通信装置 350 发送到携带式电话机 100（步骤 S362）。

携带式电话机 100，接收发送到的加密数据{{{Kc ‖ AC2}Kcom ‖ 事务 ID ‖ 内容 ID ‖ AC1}Km（1）}Ks2 （步骤 S364）。

参照图 12，在存储卡 110 中，由解密处理部 1412 对通过存储接口 1200 供给数据总线 BS3 供给的接收数据进行解密。即，解密处理部 1412，利用从对话密钥发生部 1418 供给的对话密钥 Ks2 将数据总线 BS3 的接收数据解密并输出到数据总线 BS4（步骤 S366）。

在这一阶段，将可以用 Km（1）保持部 1421 所保持的保密解密密钥 Km（1）解密的数据{{Kc ‖ AC2}Kcom ‖ 特许 ID ‖ 内容 ID ‖ AC1}Km（1）输出到数据总线 BS4。该数据{{Kc ‖ AC2}Kcom ‖ 事务

ID‖内容 ID‖AC1}Km（1），首先用保密解密密钥 Km（1）解密，然后受理作为再生信息的数据{Kc‖AC2}Kcom、事务 ID、内容 ID、访问限制信息 AC1（步骤 S368）。

将事务 ID、内容 ID、访问限制信息 AC1 记录在特许信息保持部 1440 内。数据{Kc‖AC2}Kcom，再次由公开加密密钥 KPm（1）进行加密，并作为数据{{Kc‖AC2}Kcom} Km（1）存储在存储器 1415 内（步骤 S370）。

进一步，将运行记录存储器 1460 中的接收运行记录删除（步骤 S372）。

在直到步骤 S372 的处理正常完成的阶段，从携带式电话机 100 向传送服务器 30 发出内容数据的传送请求（步骤 S374）。

传送服务器 30，接收内容数据传送请求后，从信息数据库 304 取得加密内容数据{Data}Kc 及附加信息 DATA-inf，并将这些数据通过数据总线 BS1 及通信装置 350 输出（步骤 S376）。

携带式电话机 100，接收{Data}Kc‖DATA-inf，并受理加密内容数据{Data}Kc 及附加信息 DATA-inf（步骤 S378）。加密内容数据{Data}Kc 及附加信息 DATA-inf，通过存储接口 1200 及端子 1202 传送到存储卡 110 的数据总线 BS3。在存储卡 110 中，将接收到的加密内容数据{Data}Kc 及附加信息 DATA-inf 直接存储在存储器 1415 内（步骤 S380）。

进一步，从存储卡 110 向传送服务器 30 发送传送受理的通知（步骤 S382），并当传送服务器 30 接收到传送受理时（步骤 S384），执行结束传送的处理（步骤 S386），从而结束传送服务器的处理（步骤 S390）。

[第 3 重新接通动作]

图 13 是用于说明实施例 1 的数据传送系统中的上述第 3 重新接通动作的流程图。

参照图 13，用户 1，通过携带式电话机 100 的键盘 1108 的按键操作等发出重新接通请求，根据该请求开始第 3 重新接通处理（步骤 S400）。

在携带式电话机 100 中，响应该重新接通请求，向传送服务器 30 发出内容数据的传送请求（步骤 S402）。

传送服务器 30，接收内容数据传送请求后，从信息数据库 304 取得加密内容数据{Data}Kc 及附加信息 DATA-inf，并将这些数据通过数据总线 BS1 及通信装置 350 输出（步骤 S404）。

携带式电话机 100，接收{Data}Kc // DATA-inf，并受理加密内容数据{Data}Kc 及附加信息 DATA-inf（步骤 S406）。加密内容数据{Data}Kc 及附加信息 DATA-inf，通过存储接口 1200 及端子 1202 传送到存储卡 110 的数据总线 BS3。在存储卡 110 中，将接收到的加密内容数据{Data}Kc 及附加信息 DATA-inf 直接存储在存储器 1415 内（步骤 S408）。

进一步，从存储卡 110 向传送服务器 30 发送传送受理的通知（步骤 S410），并当传送服务器 30 接收到传送受理时（步骤 S412），执行结束传送的处理（步骤 S414），从而结束传送服务器的处理（步骤 S416）。

[重新接通动作中线路切断时的重新接通动作]

以下，说明在如上所述的重新接通动作的任何处理步骤的阶段中发生了通信线路的中断时为进一步再次接收传送而进行重新接通时的处理。图 14 是用于说明这种重新接通处理的流程图。

首先，例如，用户 1，通过携带式电话机 100 的键盘 1108 的按键操作等发出重新接通的请求并开始重新接通处理（步骤 S500）。

接着，控制器 1106，根据保持在存储卡 110 内的特许接收等待运行记录判断发生通信切断的步骤是在哪一步处理中（步骤 S502），如果该步骤是特许信息取得步骤或特许信息重新取得步骤，则再次重新进行第 2 重新接通处理（步骤 S504），并结束重新接通处理（步骤 S508）。

另一方面，如果发生了通信切断的步骤是内容取得步骤（步骤 S502），则控制器 1106 进行后文所述的第 3 重新接通处理（步骤 S506），并结束重新接通处理（步骤 S508）。

通过采用如上所述的结构，无论在哪个处理步骤中发生了通信线路的中断时都可以进行重新接通，因而进一步强化了系统的可靠性。

[实施例 2]

在实施例 2 的数据传送系统中，如下文所述，与实施例 1 的数据传送系统的结构不同，其特征在于，不删除保持在存储卡 110 的运行

记录存储器 1460 内的特许接收等待运行记录。进行这种变更的结果是，除实施例 1 的结构外，在接收运行记录内还附加了接收状态标志。

因此，如下文所述，在实施例 2 的数据传送系统的结构中，存储卡 110 内的控制器 1420 的动作及保持在运行记录存储器 1460 内的数据，与实施例 1 的情况不同。

图 15、图 16 和图 17 是用于说明实施例 2 的数据传送系统中的内容购入时发生的传送动作的第 1、第 2 和第 3 流程图，是与实施例 1 的图 6～图 8 对应的图。

在图 15～图 17 中，也是说明用户 1 在使用存储卡 110 的情况下通过携带式电话机 100 从传送服务器 30 接收音乐数据的传送时的动作。

与实施例 1 的不同点在于，在事务 ID 取得步骤之后，在图 16 所示的步骤 S121 中，控制器 1420，当确认受理了由传送服务器 30 生成的对话密钥 Ks1 时，指示对话密钥发生部 1418 生成由存储卡 110 在进行传送动作时生成的对话密钥 Ks2。进一步，控制器 1420，将指示等待接收的变为接通状态的接收状态标志与对话密钥 Ks 及接收到的事务 ID 一起作为接收运行记录存储在运行记录存储器 1460 内（步骤 S121 ）。

另外，参照图 17，在步骤 S148 中，将事务 ID、内容 ID、访问限制信息 AC1 记录在特许信息保持部 1440 内。数据{Kc‖AC2}Kcom，再次由公开加密密钥 KPm(1)进行加密，并作为数据{{Kc‖AC2}Kcom}Km（1）存储在存储器 1415 内，然后，将运行记录存储器 1460 内的接收运行记录中的接收状态标志变为指示已完成接收的断开状态（步骤 S150 ）。

其他处理与实施例 1 相同，所以，对同一处理标以相同的符号，其说明不再重复。

[重新接通动作]

在实施例 2 中，也与实施例 1 的图 9 一样，当在如上所述的传送动作的任何处理步骤的阶段中发生了通信线路的中断时，为再次接收传送而进行重新接通处理。

但是，对实施例 1 的第 2 重新接通处理的一部分进行了变更。

[第 2 重新接通处理]

图 18、图 19 和图 20 是用于说明实施例 2 的数据传送系统中的上述第 2 重新接通动作的第 1、第 2 和第 3 流程图，是与实施例 1 的图 10～图 12 对应的图。

与实施例 1 的不同点在于，在图 18 内，在步骤 S318 中受理了对话密钥 Ks1 之后，将处理转移到图 16 所示的步骤 S121 ，在图 20 内，在步骤 S370 中，将事务 ID、内容 ID、访问限制信息 AC1 记录在特许信息保持部 1440 内。数据{Kc‖AC2}Kcom，再次由公开加密密钥 KPm（1）进行加密，并作为数据{{Kc‖AC2}Kcom} Km（1）存储在存储器 1415 内，然后，在步骤 S372 中，将接收运行记录中的接收状态标志变为指示已完成接收的断开状态。

其他处理与实施例 1 相同，所以，对同一处理标以相同的符号，其说明不再重复。

进一步，关于第 3 重新接通处理及重新接通动作中发生线路切断时的重新接通动作，与实施例 1 的处理相同。

通过采用如上所述的结构，无论在哪个处理步骤中发生了通信线路的中断时也都可以进行重新接通，因而进一步强化了系统的可靠性。

[实施例 3]

在实施例 3 的数据传送系统中，如下文所述，与实施例 2 的数据传送系统的结构不同点在于，将在存储卡 110 中的运行记录存储器 1460 所保持的接收运行记录内增加了状态标志后的状态信息发送到服务器。

状态信息，包括作为接收运行记录的事务 ID、对话密钥 Ks2、接收状态标志及状态标志等信息。

这里，特许状态标志，是具有 3 种状态的标志变量，当在存储卡 110 的特许信息保持部 1440 内存在着记录于接收运行记录中的事务 ID 并存在着对应的再生信息且不禁止用保持在特许信息保持部 1440 内的访问限制信息 AC1 进行再生、即可以再生时，取「01h」这样的值，当在特许信息保持部 1440 内存在着事务 ID 但不存在对应的再生信息或禁止用保持在特许信息保持部 1440 内的访问限制信息 AC1 进行再生、即不能再生时，取「00h」这样的值，当事务 ID 不存在时，取「FFh」这样的值。

因此，如下文所述，在实施例 3 的数据传送系统的结构中，存储卡 110 内的控制器 1420 的动作及保持在运行记录存储器 1460 内的数据，与实施例 2 的情况不同。

实施例 3 的传送动作及重新接通动作，除以下说明的第 2 重新接通处理外，与实施例 2 的处理相同，因此其说明不再重复。

[第 2 重新接通处理]

图 21、图 22、图 23 和图 24 是用于说明实施例 3 的数据传送系统中的第 2 重新接通动作的第 1、第 2、第 3 和第 4 流程图。

首先，参照图 21，从步骤 S300 到步骤 S338，与实施例 2 的第 2 重新接通动作相同。

在步骤 S338 中，在存储卡 110 内，由解密处理部 1404 利用保持在保持部 1402 内的存储卡 110 所固有的保密解密密钥 Kmc（1）对通过存储接口 1200 供给数据总线 BS3 的接收数据进行解密处理，从而解密并提取对话密钥 Ks1，然后，存储卡 110 中的控制器 1420，根据保持在运行记录存储器 1460 内的接收运行记录中的事务 ID，检索存储在特许信息保持部 1440 内的数据（步骤 S640）。

控制器 1420，首先，检查特许信息保持部 1440 中是否存在着事务 ID（步骤 S642）。

当事务 ID 不存在时，将特许状态标志设定为「FFh」（步骤 S644），并使处理进入步骤 S652。

另一方面，当在步骤 S642 中判定存在着事务 ID 时，控制器 1420，进一步确认保持在特许信息保持部 1440 内的访问限制信息 AC1 的状态及在存储器 1415 内是否记录着对应的特许密钥 Kc（步骤 S646）。当可以再生时，将特许状态标志设定为「01h」（步骤 S648）。而当不能再生时，将特许状态标志设定为「00h」（步骤 S650）。在此之后，使处理进入步骤 S652。

接着，生成在运行记录存储器 1460 所保持的接收运行记录内附加了状态标志后的状态信息（步骤 S652）。

控制器 1420，指示对话密钥发生部 1418 生成由存储卡 110 在进行传送动作时生成的对话密钥 Ks2 （步骤 S654）。

加密处理部 1406，利用对话密钥 Ks1 对状态信息和对话密钥 Ks2 进行加密，并生成加密数据{状态信息‖Ks2 }Ks1（步骤 S656）。

控制器 1420，求取以与加密数据{状态信息‖Ks2 }Ks1 对应的散列函数为依据的散列值，并生成与加密数据{状态信息‖Ks2 }Ks1 对应的署名数据 hash（步骤 S658）。

加密处理部 1406，利用由解密处理部 1404 通过切换开关 1442 的接点 Pa 供给的对话密钥 Ks1 对在控制器 1420 的控制下提供的署名数据 hash 进行加密，并生成加密署名数据{hash}Ks1（步骤 S660）。

从存储卡 110 输出按如上方式生成的数据{状态信息‖Ks2 }Ks1 及加密署名数据{hash}Ks1（步骤 S662）。

输出到数据总线 BS3 上的加密数据{状态信息‖Ks2 }Ks1 及加密署名数据{hash}Ks1，从数据总线 BS3 通过端子 1202 及存储接口 1200 发送到携带式电话机 100，并从携带式电话机 100 发送到传送服务器 30（步骤 S664）。

传送服务器 30，接收加密数据{状态信息‖Ks2 }Ks1 及加密署名数据{hash}Ks1（步骤 S666）。

参照图 23，由传送服务器 30 的解密处理部 320 利用对话密钥 Ks1 对加密署名数据{hash}Ks1 执行解密处理，并求得与加密数据{状态信息‖Ks2 }Ks1 对应的署名数据 hash。然后，根据加密数据{状态信息‖Ks2 }Ks1 和署名数据检查状态信息的合法性（步骤 S668）。

如状态信息不合法，则结束处理（步骤 S712），如确认状态信息合法，则利用对话密钥 Ks1 执行解密处理，并受理状态信息及由存储卡生成的对话密钥 Ks2 （步骤 S670）。

接着，传送控制部 315，根据所受理的状态信息和特许传送运行记录，检查再生信息的再生请求的合法性（步骤 S672）。

当判定再生信息的再生请求不合法时，结束第 2 重新接通处理（步骤 S712）。

另一方面，当判定再生信息的再生请求合法时，传送控制部 315，从特许传送运行记录取得内容 ID、访问限制信息 AC1、再生电路限制信息 AC2 及公开加密密钥 KPm（1）（步骤 S674）。进一步，从信息数据库 304 取得用于对加密内容数据进行解密的特许密钥 Kc（步骤 S676）。

传送控制部 315，将所取得的特许密钥 Kc 及再生电路限制信息 AC2 供给加密处理部 324。加密处理部 324，利用从 Kcom 保持部 322

取得的保密共用密钥 Kcom 将特许密钥 Kc 及再生电路限制信息 AC2 加密（步骤 S678）。

由加密处理部 326 利用在步骤 S674 中求得的存储卡 110 所固有的公开加密密钥 KPm（1）对加密处理部 324 输出的加密数据{Kc ‖ AC2}Kcom 及传送控制部 315 输出的事务 ID、内容 ID 及访问限制信息 AC1 进行加密（步骤 S680）。

加密处理部 328，接收加密处理部 326 的输出，并利用由存储卡 110 生成的对话密钥 Ks2 进行加密（步骤 S682）。

由加密处理部 328 输出的加密数据{{{Kc ‖ AC2}Kcom ‖ 事务 ID ‖ 内容 ID ‖ AC1}Km（1）}Ks2 ，通过数据总线 BS1 及通信装置 350 发送到携带式电话机 100（步骤 S684）。

携带式电话机 100，接收发送到的加密数据{{{Kc ‖ AC2}Kcom ‖ 事务 ID ‖ 内容 ID ‖ AC1}Km（1）}Ks2 （步骤 S686）。

参照图 24，在存储卡 110 中，由解密处理部 1412 对通过存储接口 1200 供给数据总线 BS3 供给的接收数据进行解密。即，解密处理部 1412，利用从对话密钥发生部 1418 供给的对话密钥 Ks2 将数据总线 BS3 的接收数据解密后输出到数据总线 BS4（步骤 S690）。

在这一阶段，将可以用 Km（1）保持部 1421 所保持的保密解密密钥 Km（1）解密的数据{{Kc ‖ AC2}Kcom ‖ 特许 ID ‖ 内容 ID ‖ AC1}Km（1）输出到数据总线 BS4。该数据{{Kc ‖ AC2}Kcom ‖ 事务 ID ‖ 内容 ID ‖ AC1}Km（1），首先用公开加密密钥 Km（1）解密，然后受理数据{Kc ‖ AC2}Kcom、事务 ID、内容 ID、访问限制信息 AC1（步骤 S692）。

将事务 ID、内容 ID、访问限制信息 AC1，记录在特许信息保持部 1440 内。数据{Kc ‖ AC2}Kcom，再次由公开加密密钥 KPm（1）进行加密，并作为数据{{Kc ‖ AC2}Kcom} Km（1）存储在存储器 1415 内（步骤 S694）。

进一步，将运行记录存储器 1460 内的接收运行记录中的接收状态标志变为指示已完成接收的断开状态（步骤 S696）。

在直到步骤 S372 的处理正常完成的阶段，从携带式电话机 100 向传送服务器 30 发出内容数据的传送请求（步骤 S698）。

传送服务器 30，接收内容数据传送请求后，从信息数据库 304 取

得加密内容数据{Data}Kc 及附加信息 DATA-inf，并将这些数据通过数据总线 BS1 及通信装置 350 输出（步骤 S700）。

携带式电话机 100，接收{Data}Kc ‖ DATA-inf，并受理加密内容数据{Data}Kc 及附加信息 DATA-inf（步骤 S702）。加密内容数据{Data}Kc 及附加信息 DATA-inf，通过存储接口 1200 及端子 1202 传送到存储卡 110 的数据总线 BS3。在存储卡 110 中，将接收到的加密内容数据{Data}Kc 及附加信息 DATA-inf 直接存储在存储器 1415 内（步骤 S704）。

进一步，从存储卡 110 向传送服务器 30 发送传送受理的通知（步骤 S706），并当传送服务器 30 接收到传送受理时（步骤 S708），执行结束传送的处理（步骤 S710），从而结束传送服务器的处理（步骤 S712）。

另外，在以上的说明中，在步骤 S654 中用对话密钥 Ks1 对状态信息的所有信息进行加密后，将加密数据{状态信息 ‖ Ks2 }Ks1 通过步骤 S622 及 S624 发送到传送服务器 30。

但是，对于状态信息中的事务 ID，与考虑其机密性相比，如能指明其来源则是更适用的信息。因此，用加密署名数据{hash}Ks1 指明其来源，所以，也可以构成为不对事务 ID 进行加密而以原来的明文形式将其发送到传送服务器 30。在这种情况下，状态信息，以事务 ID ‖ {除事务 ID 外的状态信息 ‖ Ks2 }Ks1 的形式发送，并与其对应地生成署名数据 hash。

通过采用如上所述的结构，无论在哪个处理步骤中发生了通信线路的中断时也都可以进行重新接通，因而进一步强化了系统的可靠性。

进一步，在实施例 1～3 的数据传送系统中，构成为由传送服务器 30 和携带式电话机 100 利用保密共用密钥 Kcom 执行加密和解密处理，但也可以构成为不进行利用该保密共用密钥 Kcom 的加密和解密处理。

即，在用图 3 说明过的实施 1 的数据传送系统所具备的传送服务器 30 中，在结构上可以不具备 Kcom 保持部 322 及加密处理部 324。即，在这种传送服务器 30 中，将传送控制部 315 输出的特许密钥 Kc 及再生电路限制信息 AC2 直接传送到加密处理部 326。

进一步，与图 4 中说明过的实施例 1 的携带式电话机 100 的结构相比，也可以构成为不具备保持保密共用密钥 Kcom 的 Kcom 保持部 1512 及利用保密共用密钥 Kcom 的解密处理部 1514。

即，在这种结构的携带式电话机 101 中，与在传送服务器 30 中不进行将保密共用密钥作为对称的加密密钥的加密处理的情况相对应，由利用对话密钥 Ks4 执行解密处理的解密处理部 1510 直接取得特许密钥 Kc，所以在结构上可以将其直接供给解密处理部 1510。

另外，在这种不进行利用该保密共用密钥 Kcom 的加密和解密处理的结构中，也可以直接使用存储卡 110。

在这时的传送处理等情况下，不用保密共用密钥 Kcom 将内容密钥 Kc 及再生电路限制信息 AC2 加密而进行传送和保持，此外，除了不需要利用保密共用密钥 Kcom 的加密处理和对应的解密处理这一点外，与实施例 1～3 的相同。

通过采用如上所述的结构，即使在结构上不进行与保密共用密钥 Kcom 有关的加密处理，也可以构成享受与实施例 1～3 的数据传送系统相同的效果的数据传送系统。

进一步，在如上所述的实施例 1～3 中，也可以进行如下的变更。

首先，在实施例 1～3 中，可以构成为用公开加密密钥 KPm（1）再次将数据{Kc‖AC2}Kcom（在如上所述的省略了密钥 Kcom 的结构中，为数据 Kc‖AC2）加密后记录在特许信息保持部 1440 内。但是，如果是存储于设在 TRM（防窜改模块）内的特许信息保持部 1440，则不一定需要利用公开加密密钥 KPm（1）的再次加密，即使将所有再生信息都记录在特许信息保持部 1440 内，也可以取得与实施例 1～3 相同的效果。在这种情况下，在实施例 1 中，只需将图 8 中的步骤 S148、图 12 中的步骤 S370 变更为「将事务 ID、内容 ID、AC1、{Kc‖AC2}Kcom 记录在特许信息保持部内」即可。此外，与实施例 1 一样，在实施例 2 中只需将图 17 中的步骤 S148、图 20 中的步骤 S370 而在实施例 3 中只需将图 24 中的步骤 S694 变更为「将事务 ID、内容 ID、AC1、{Kc‖AC2}Kcom 记录在特许信息保持部内」即可。进一步，与上述实施例 1～3 的任何一种变更相对应，如果在结构上省略了密钥 Kcom，则也只需变更为「将事务 ID、内容 ID、AC1、Kc‖AC2 记录在特许信息保持部内」即可。

进一步，在所有实施例 1～3 的数据传送系统中，说明了当从传送服务器接收再生信息的传送时将存储卡及携带式电话机（内容再生电路）的认证数据{KPm（1）} Kpma 及{KPp（1）} Kpma 发送到传送服务器（步骤 S104）而传送服务器在接收（步骤 S106）并用认证密钥 Kpma 进行解密（步骤 S108）后根据解密结果对存储卡和携带式电话机（内容再生电路）的双方进行认证处理。但是，从以下 2 点来看，也可以构成为不进行传送服务器中的内容再生电路的认证数据{KPpm（1）} Kpma 的认证处理，即，　）存储卡是可插卸的，所以用于再生音乐的内容再生电路也不一定必然是接收到传送的携带式电话机，　）当再生时，在输出再生信息的一部分（特许密钥 Kc 及再生电路限制信息 AC2）的时候，在存储卡内，也进行输出目的端的内容再生电路的认证数据{KPm（1）} Kpma 的认证处理，因而即使在传送服务器中不进行内容再生电路的认证数据{KPm（1）} Kpma 的认证处理也不会使安全性降低。

在这种情况下，携带式电话机，在步骤 S104 中，发送内容 ID、存储卡的认证数据{KPmc（1）} Kpma 及特许购入条件 AC，传送服务器，在步骤 S106 中，发送内容 ID、存储卡的认证数据{KPmc（1）} Kpma 及特许购入条件 AC，在步骤 S108 中，用认证密钥 Kpma 对认证数据{KPmc（1）} Kpma 进行解密，从而受理公开加密密钥的 KPmc（1）。接着，在步骤 S110 中，根据解密结果、或向认证服务器查询，进行判断公开加密密钥 KPmc（1）是否是从合法的设备输出的认证处理，并只需变更为根据存储卡的认证数据{KPmc（1）} Kpma 的认证结果进行以后的处理即可，而再生处理没有任何变更。

另外，在以上的说明中，所传送的信息的存储，由存储卡进行，但本发明并不限定于这种情况。即，只要是具有与如上所述的存储卡相同的记录及加密等功能，也可以采用更为一般的记录装置。这时，记录装置，不一定限定于存储卡这样的可以在携带式电话机之类的通信装置上插卸的结构，也可以是组装在通信装置内的结构。

以上对本发明给出了详细的说明，但这只是用于示例而没有任何限定，应该清楚地知道，发明的精神和范围只由所附加的权利要求范围限定。

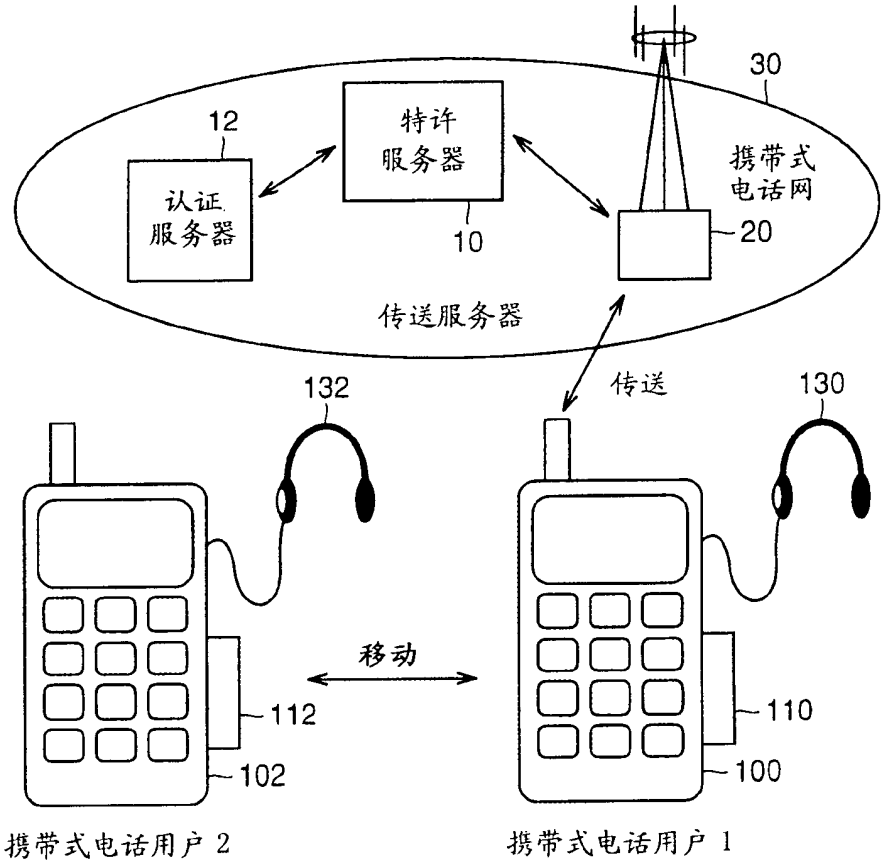

30
12
特许
服务器
携带式
电话网
认证
服务器
10
20
传送服务器
传送
132
130
移动
112
110
102
100
携带式电话用户 2
携带式电话用户 1

图 1

名称	功能特征	保持、生成部位、
Data	内容数据，作为进行了可以用 Kc 解密的加密后的内容数据以（Data）Kc 的形式发送	传送服务器
Data-inf	附加信息，与内容数据的著作相关或与服务器访问相关的明文信息	传送服务器
Kc	内容解密密钥	传送服务器
Kp(n)/Kmc(n)	内容再生/依据媒体的密级（类型）的解密密钥	携带式电话机存储卡
KPp(n)/KPmc(n)	可以用 Kp/Kmc 解密的非对称加密密钥，具有认证功能。出厂时以{KPp} Kpma/ {KPp} Kpma 的形式记录	携带式电话机存储卡
Kcom	再生电路共用的保密解密密钥，用于对加密后的 Kc、AC2 的解密(也可以是非对称的传送服务器 Kpcom/再生电路 Kcom)	携带式电话机传送服务器
KPma	系统的共用认证密钥（公开）	传送服务器
AC	来自使用者侧的对特许内容购入条件（功能限定、特许内容数等）	携带式电话机
AC1	对存储器的访问限制信息	传送服务器
AC2	再生电路的限制信息	传送服务器
Km(i)	每个存储卡固有的解密密钥（i 为识别卡的标识符）	存储卡
KPm(i)	可以用 Km（i）解密的非对称公开加密密钥	存储卡
Ks1	在每次传送对话时产生的对话固有共用密钥	传送服务器
Ks2	在每次传送/移动（接收）对话时产生的对话固有共用密钥	存储卡
Ks3	在每次再生对话时产生的对话固有共用密钥	存储卡
Ks4	在每次再生对话时产生的对话固有共用密钥	携带式电话机
内容 ID	识别内容数据 Data 的代码	传送服务器
事务 ID	可以特定特许内容发送的管理代码（也可以考虑将内容 ID 也包括在内进行识别）	传送服务器

图 2

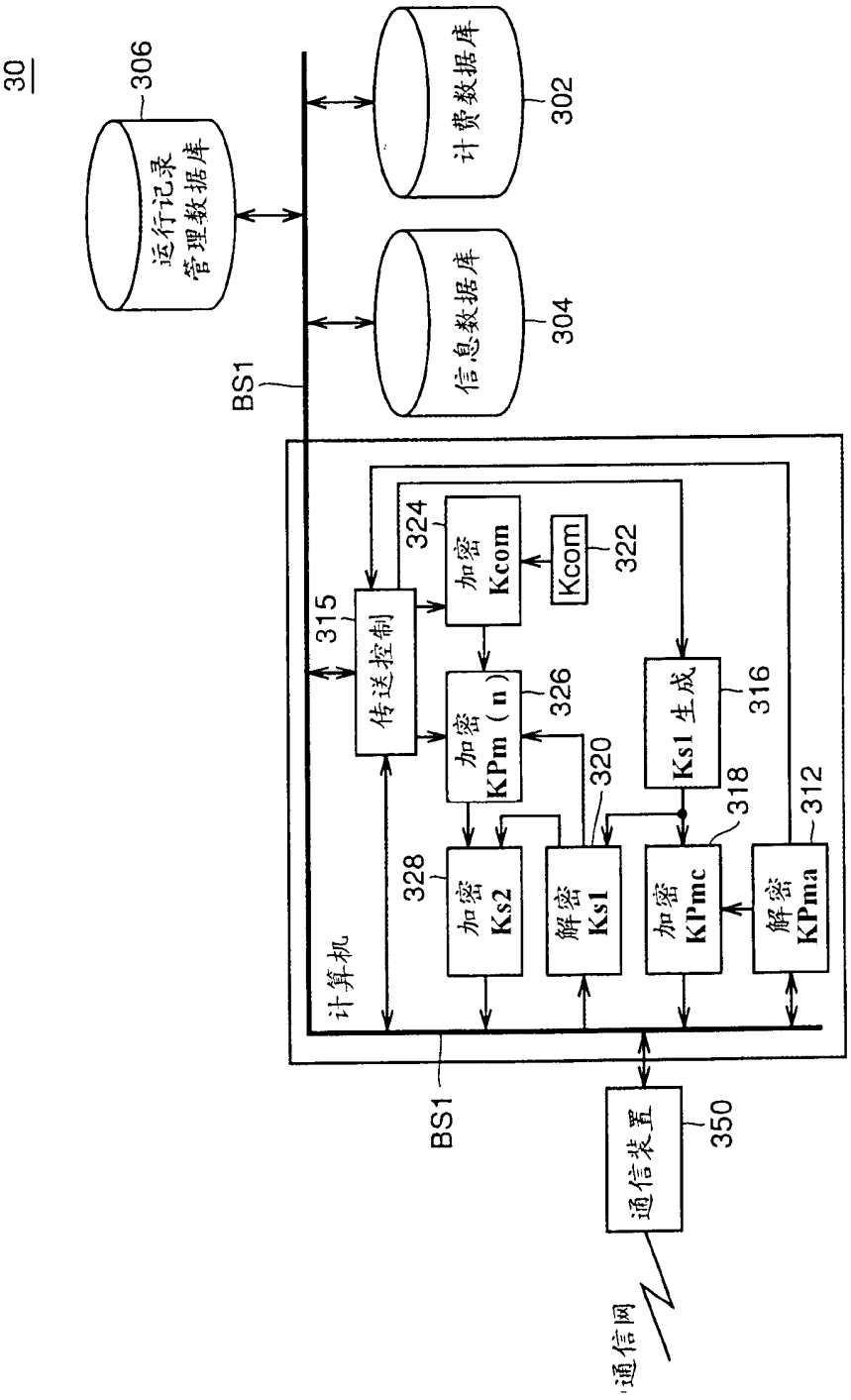

30
306
运行记录管理数据库
计费数据库
302
BS1
信息数据库
304
计算机
315
传送控制
324
加密 Kcom
Kcom
322
加密 KPm（n）
326
Ks1 生成
316
320
318
312
328
加密 Ks2
解密 Ks1
加密 KPmc
解密 KPma
BS1
通信装置
350
通信网

图 3

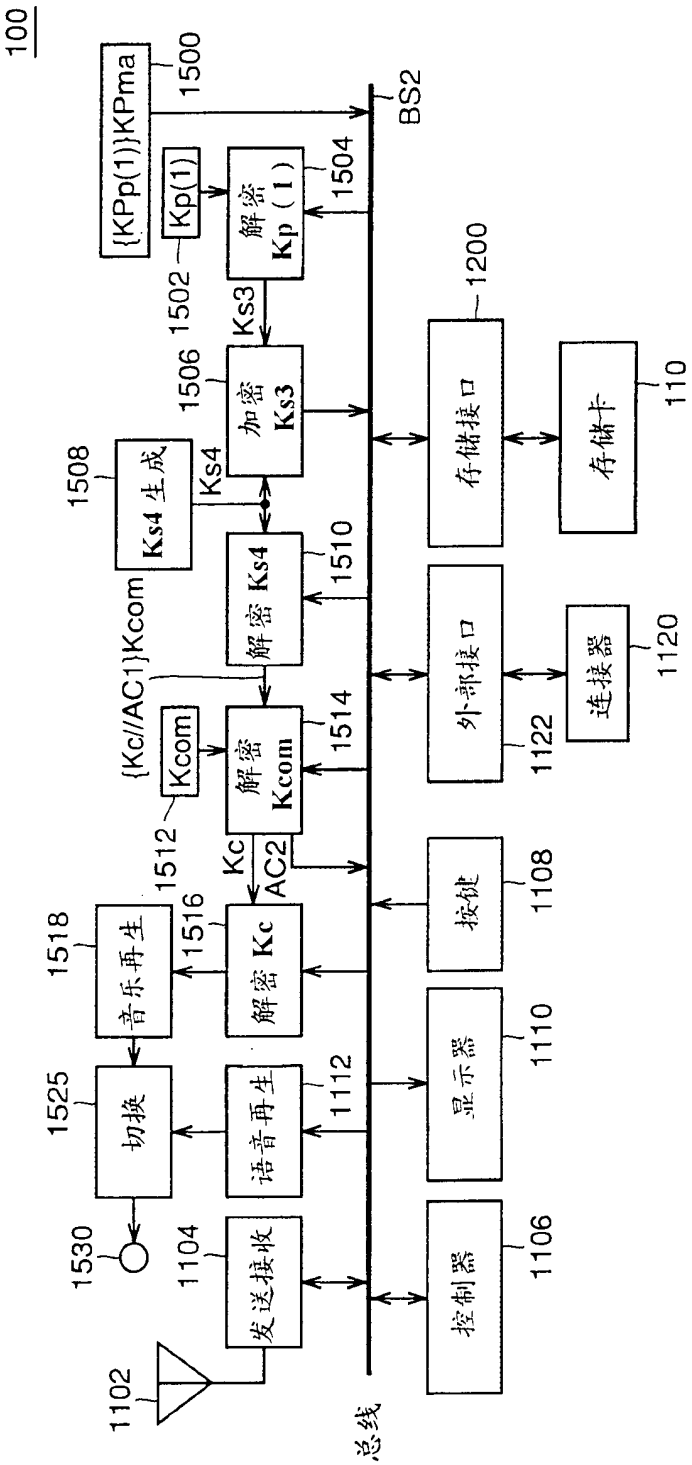

100
{KPp(1)}KPma
1500
BS2
Kp(1)
1502
解密 Kp(1)
1504
Ks3
1506
加密 Ks3
Ks4
1508
Ks4 生成
解密 Ks4
1510
{Kc//AC1}Kcom
Kcom
解密 Kcom
1514
Kc
AC2
1512
1516
解密 Kc
音乐再生
1518
切换
1525
语音再生
1112
发送接收
1104
1530
1102
总线
控制器
1106
显示器
1110
按键
1108
外部接口
1122
存储接口
1200
连接器
1120
存储卡
110

图 4

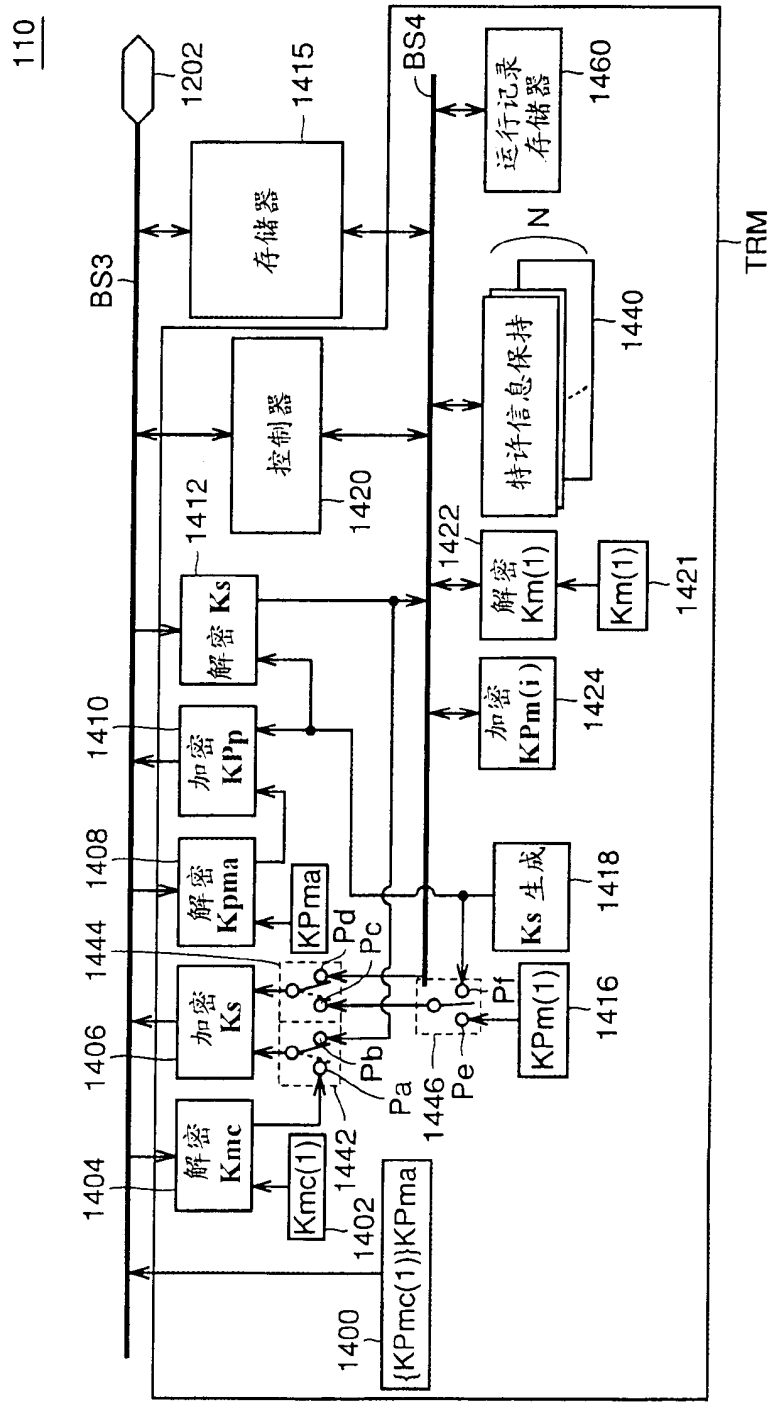

110
1202
1415
BS4
1460
运行记录存储器
BS3
存储器
TRM
N
1440
特许信息保持
控制器
1420
1412
1422
1421
解密 Ks
解密 Km(1)
Km(1)
1410
加密 KPp
加密 KPm(i)
1424
1408
解密 Kpma
KPma
Pd
Pc
1444
Ks 生成
1418
1406
加密 Ks
Pf
KPm(1)
1416
Pb
Pa
1446
Pe
1404
解密 Kmc
Kmc(1)
1442
1402
{KPmc(1)}KPma
1400

图 5

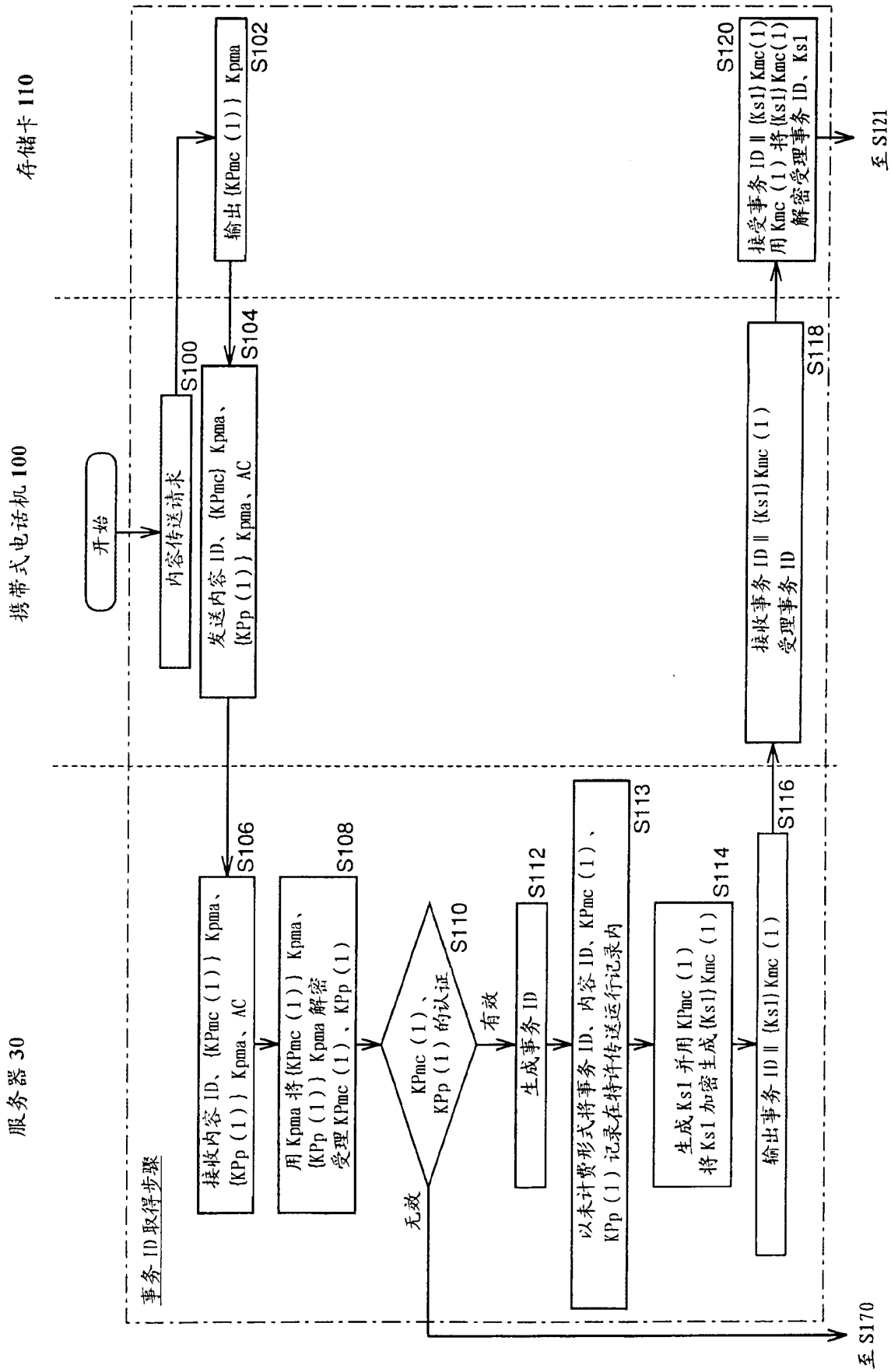

服务器 30
携带式电话机 100
存储卡 110
事务 ID 取得步骤
开始
内容传送请求
S100
输出 {KPmc（1）} Kpma
S102
发送内容 ID、{KPmc} Kpma、{KPp（1）} Kpma、AC
S104
接收内容 ID、{KPmc（1）} Kpma、{KPp（1）} Kpma、AC
S106
用 Kpma 将 {KPmc（1）} Kpma、{KPp（1）} Kpma 解密
受理 KPmc（1）、KPp（1）
S108
KPmc（1）、KPp（1）的认证
S110
无效
有效
生成事务 ID
S112
以未计费形式将事务 ID、内容 ID、KPmc（1）、KPp（1）记录在特许传送运行记录内
S113
生成 Ks1 并用 KPmc（1）将 Ks1 加密生成 {Ks1} Kmc（1）
S114
输出事务 ID ‖ {Ks1} Kmc（1）
S116
接收事务 ID ‖ {Ks1} Kmc（1）
受理事务 ID
S118
接受事务 ID ‖ {Ks1} Kmc（1）
用 Kmc（1）将 {Ks1} Kmc（1）解密受理事务 ID、Ks1
S120
至 S121
至 S170

图 6

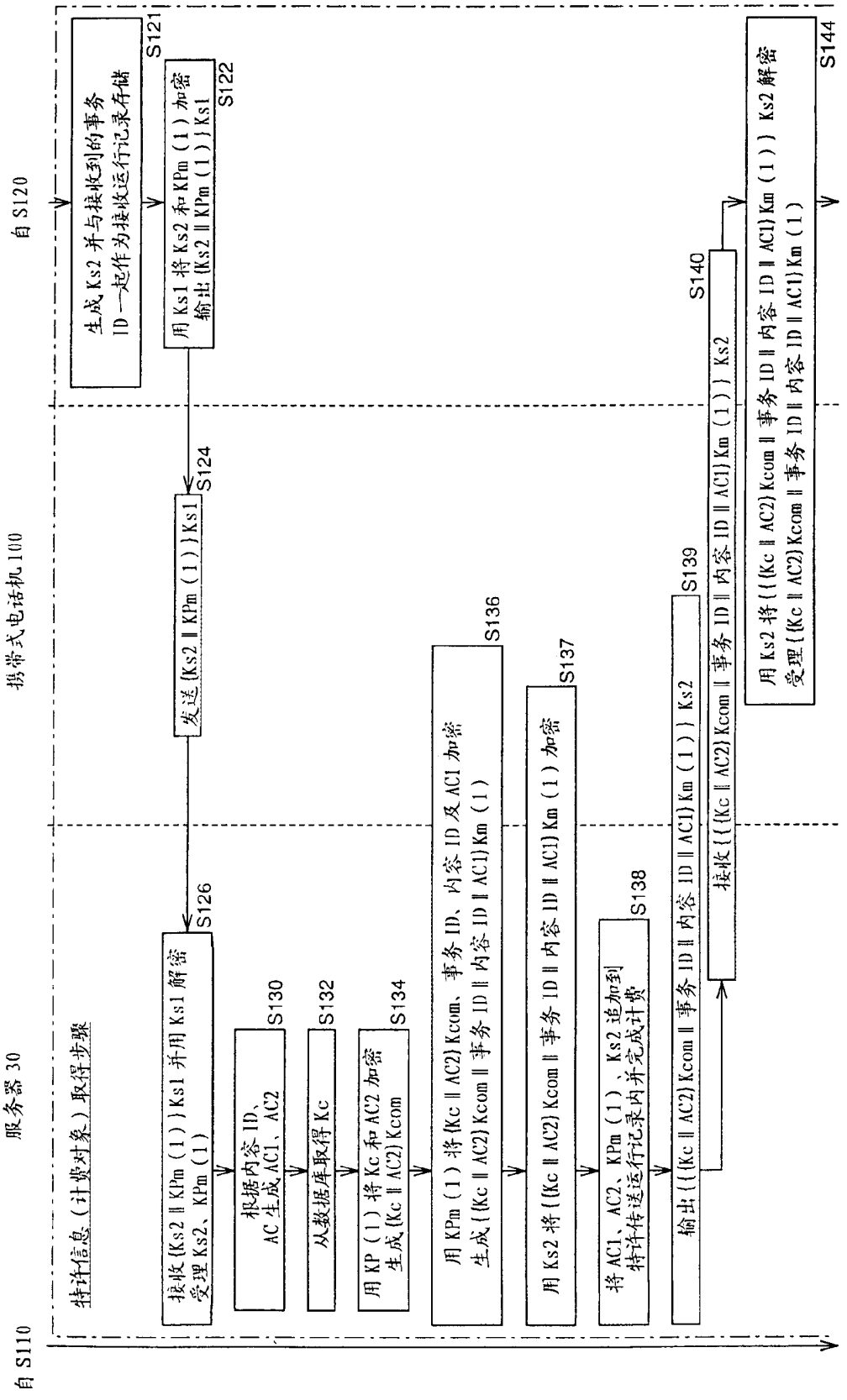

存储卡 110
服务器 30
携带式电话机 100
自 S110
自 S120
特许信息（计费对象）取得步骤
生成 Ks2 并与接收到的事务 ID 一起作为接收运行记录存储
S121
用 Ks1 将 Ks2 和 KPm（1）加密输出 {Ks2 ‖ KPm（1）} Ks1
S122
发送 {Ks2 ‖ KPm（1）} Ks1
S124
接收 {Ks2 ‖ KPm（1）} Ks1 并用 Ks1 解密受理 Ks2、KPm（1）
S126
根据内容 ID、AC 生成 AC1、AC2
S130
从数据库取得 Kc
S132
用 KP（1）将 Kc 和 AC2 加密生成 {Kc ‖ AC2} Kcom
S134
用 KPm（1）将 {Kc ‖ AC2} Kcom、事务 ID、内容 ID 及 AC1 加密生成 {{Kc ‖ AC2} Kcom ‖ 事务 ID ‖ 内容 ID ‖ AC1} Km（1）
S136
用 Ks2 将 {{Kc ‖ AC2} Kcom ‖ 事务 ID ‖ 内容 ID ‖ AC1} Km（1）加密
S137
将 AC1、AC2、KPm（1）、Ks2 追加到特许传送运行记录内并完成计费
S138
输出 {{{Kc ‖ AC2} Kcom ‖ 事务 ID ‖ 内容 ID ‖ AC1} Km（1）} Ks2
S139
接收 {{{Kc ‖ AC2} Kcom ‖ 事务 ID ‖ 内容 ID ‖ AC1} Km（1）} Ks2
S140
用 Ks2 将 {{{Kc ‖ AC2} Kcom ‖ 事务 ID ‖ 内容 ID ‖ AC1} Km（1）} Ks2 解密受理 {{Kc ‖ AC2} Kcom ‖ 事务 ID ‖ 内容 ID ‖ AC1} Km（1）
S144
至 S146
至 S170

图 7

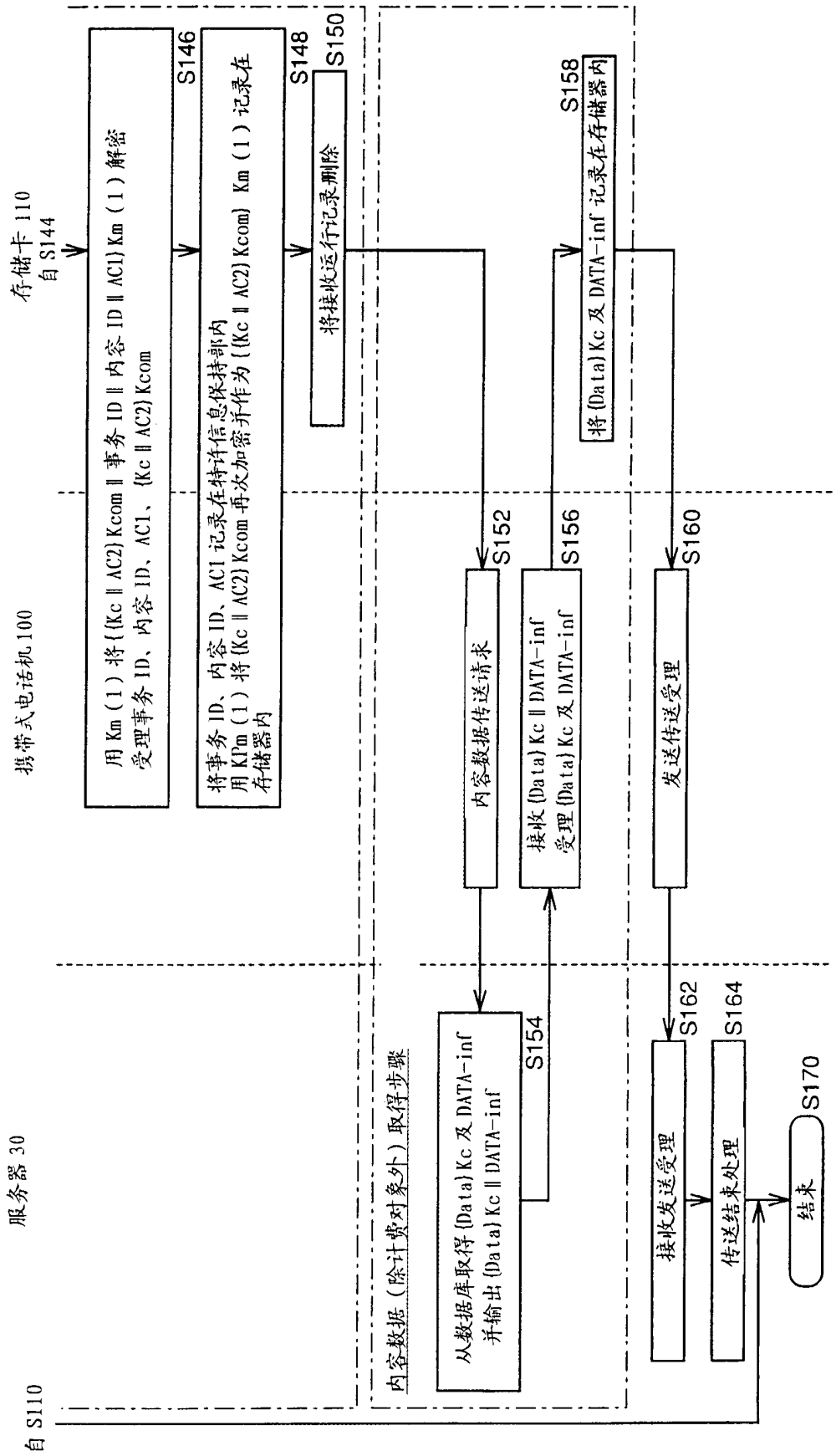

服务器 30
携带式电话机 100
存储卡 110
自 S110
自 S144
用 Km（1）将{{Kc ‖ AC2} Kcom ‖ 事务 ID ‖ 内容 ID ‖ AC1} Km（1）解密
受理事务 ID、内容 ID、AC1、{Kc ‖ AC2} Kcom
S146
将事务 ID、内容 ID、AC1 记录在特许信息保持部内
用 KPm（1）将{Kc ‖ AC2} Kcom 再次加密并作为{{Kc ‖ AC2} Kcom} Km（1）记录在存储器内
S148
将接收运行记录删除
S150
内容数据（除计费对象外）取得步骤
内容数据传送请求
S152
从数据库取得{Data} Kc 及 DATA-inf
并输出{Data} Kc ‖ DATA-inf
S154
接收{Data} Kc ‖ DATA-inf
受理{Data} Kc 及 DATA-inf
S156
将{Data} Kc 及 DATA-inf 记录在存储器内
S158
发送传送受理
S160
接收发送受理
S162
传送结束处理
S164
结束
S170

图 8

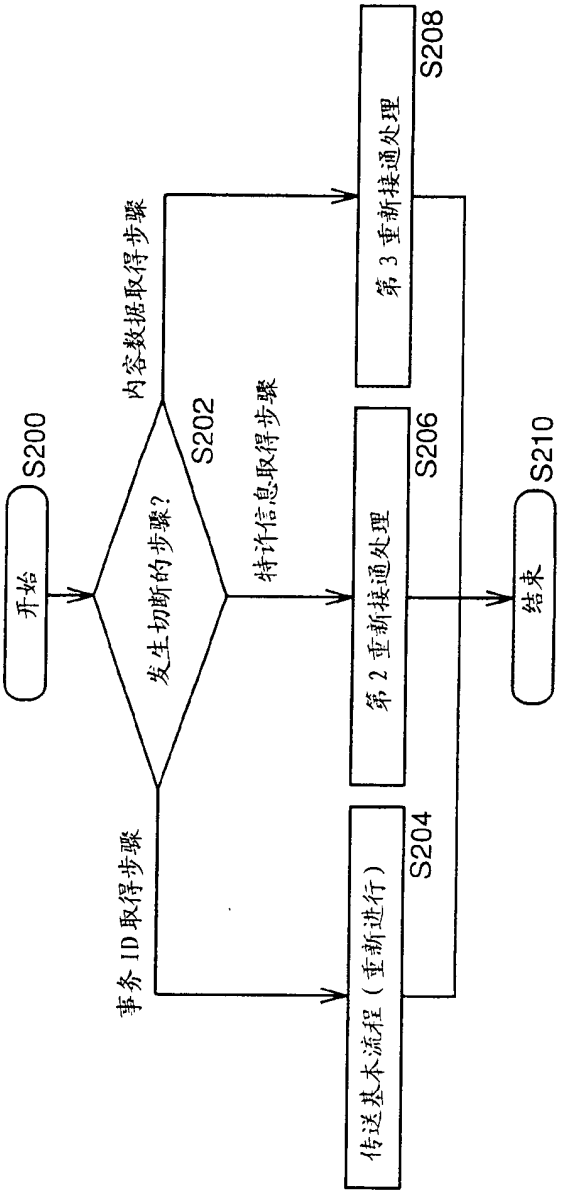

开始
S200
发生切断的步骤?
S202
内容数据取得步骤
特许信息取得步骤
事务 ID 取得步骤
第 3 重新接通处理
S208
第 2 重新接通处理
S206
传送基本流程（重新进行）
S204
结束
S210

图 9

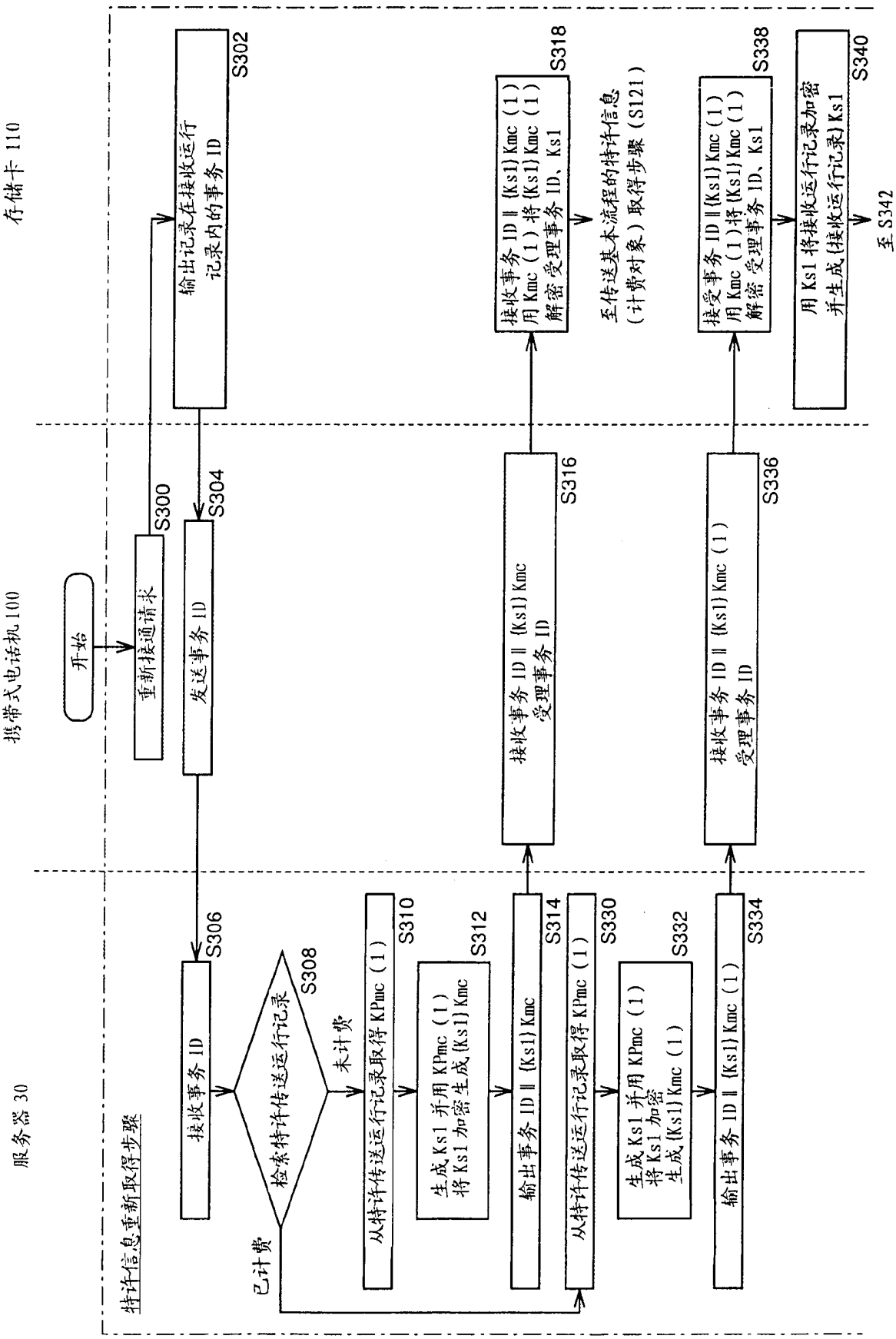

存储卡 110
携带式电话机 100
服务器 30
特许信息重新取得步骤
开始
重新接通请求
S300
发送事务 ID
S304
输出记录在接收运行记录内的事务 ID
S302
接收事务 ID
S306
检索特许传送运行记录
S308
已计费
未计费
从特许传送运行记录取得 KPmc（1）
S310
生成 Ks1 并用 KPmc（1）
将 Ks1 加密生成{Ks1}Kmc
S312
输出事务 ID‖{Ks1}Kmc
S314
接收事务 ID‖{Ks1}Kmc
受理事务 ID
S316
接收事务 ID‖{Ks1}Kmc（1）
用 Kmc（1）将{Ks1}Kmc（1）
解密受理事务 ID、Ks1
S318
至传送基本流程的特许信息
（计费对象）取得步骤（S121）
从特许传送运行记录取得 KPmc（1）
S330
生成 Ks1 并用 KPmc（1）
将 Ks1 加密
生成{Ks1}Kmc（1）
S332
输出事务 ID‖{Ks1}Kmc（1）
S334
接收事务 ID‖{Ks1}Kmc（1）
受理事务 ID
S336
接受事务 ID‖{Ks1}Kmc（1）
用 Kmc（1）将{Ks1}Kmc（1）
解密受理事务 ID、Ks1
S338
用 Ks1 将接收运行记录加密
并生成{接收运行记录}Ks1
S340
至 S342

图 10

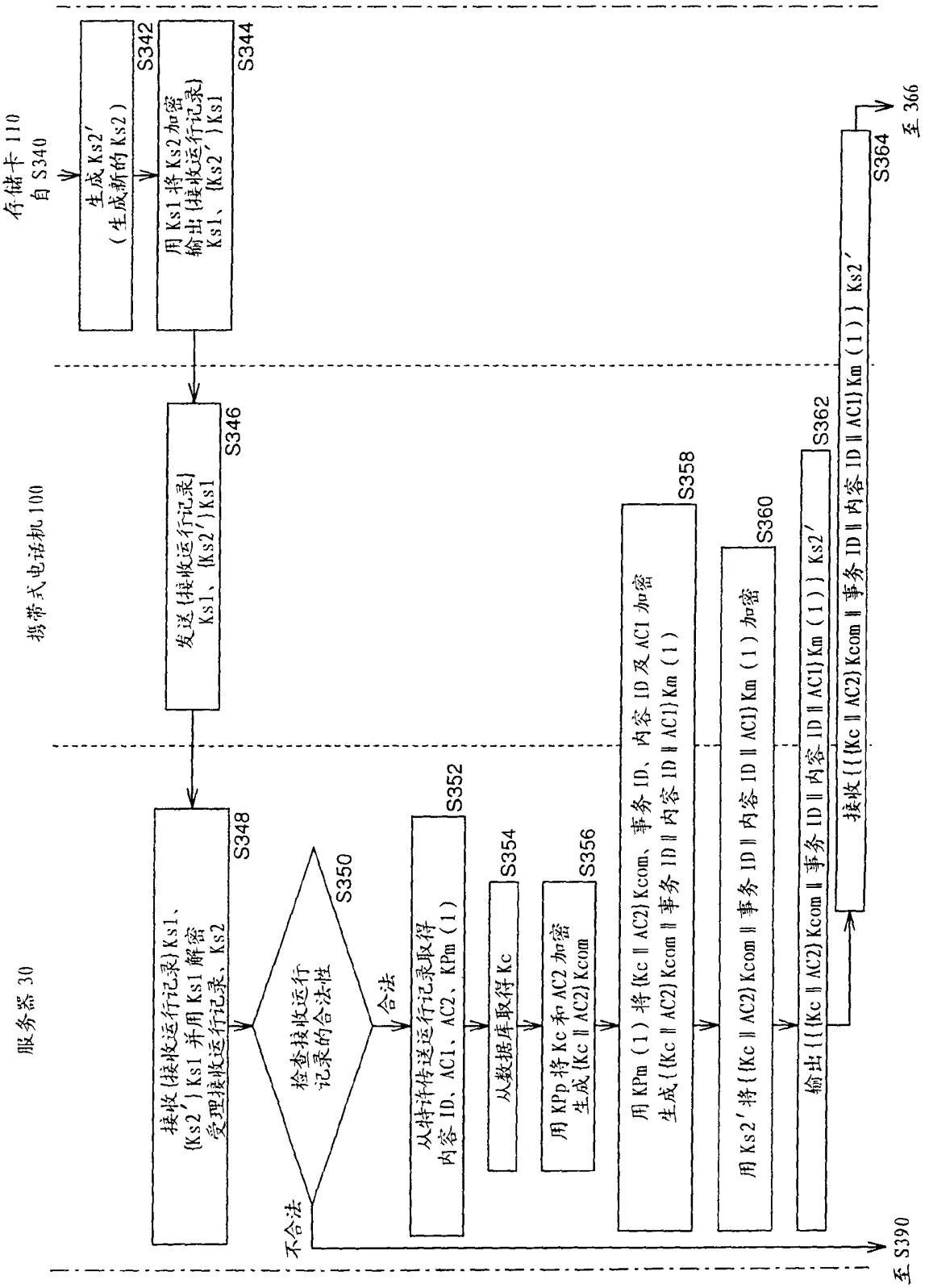

存储卡 110
自 S340
携带式电话机 100
服务器 30
生成 Ks2′
（生成新的 Ks2）
S342
用 Ks1 将 Ks2 加密
输出 {接收运行记录}
Ks1、{Ks2′} Ks1
S344
发送 {接收运行记录}
Ks1、{Ks2′} Ks1
S346
接收 {接收运行记录} Ks1、
{Ks2′} Ks1 并用 Ks1 解密
受理接收运行记录、Ks2
S348
检查接收运行
记录的合法性
S350
不合法
合法
从特许传送运行记录取得
内容 ID、AC1、AC2、KPm（1）
S352
从数据库取得 Kc
S354
用 KPp 将 Kc 和 AC2 加密
生成 {Kc ‖ AC2} Kcom
S356
用 KPm（1）将 {Kc ‖ AC2} Kcom、事务 ID、内容 ID 及 AC1 加密
生成 {{Kc ‖ AC2} Kcom ‖ 事务 ID ‖ 内容 ID ‖ AC1} Km（1）
S358
用 Ks2′将 {{Kc ‖ AC2} Kcom ‖ 事务 ID ‖ 内容 ID ‖ AC1} Km（1）加密
S360
输出 {{{Kc ‖ AC2} Kcom ‖ 事务 ID ‖ 内容 ID ‖ AC1} Km（1）} Ks2′
S362
接收 {{{Kc ‖ AC2} Kcom ‖ 事务 ID ‖ 内容 ID ‖ AC1} Km（1）} Ks2′
S364
至 366
至 S390

图 11

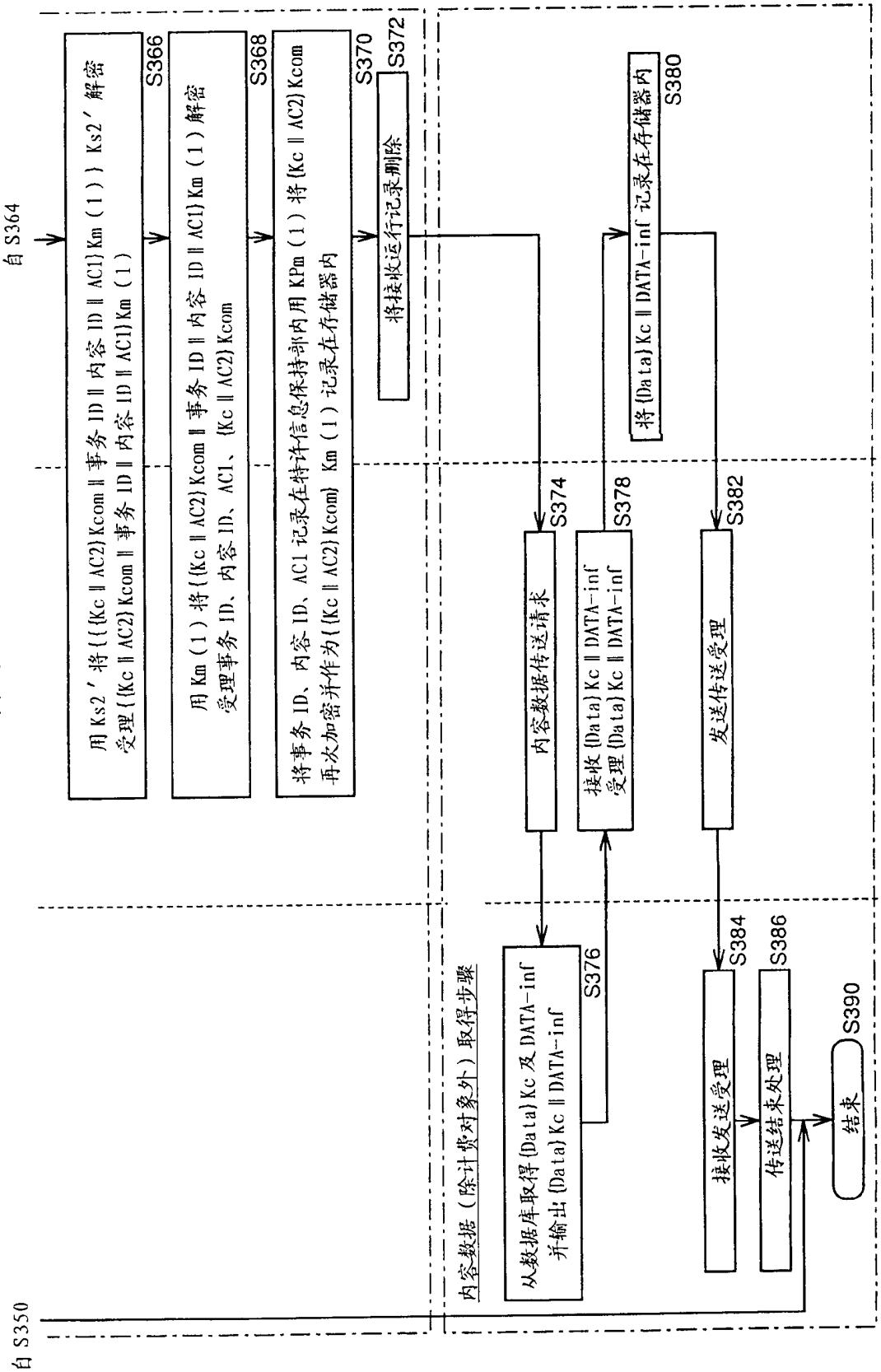

服务器 30
携带式电话机 100
存储卡 110
自 S350
自 S364
用 Ks2′ 将{{{Kc ‖ AC2} Kcom ‖ 事务 ID ‖ 内容 ID ‖ AC1} Km（1）} Ks2′ 解密
受理{{Kc ‖ AC2} Kcom ‖ 事务 ID ‖ 内容 ID ‖ AC1} Km（1）
S366
用 Km（1）将{{Kc ‖ AC2} Kcom ‖ 事务 ID ‖ 内容 ID ‖ AC1} Km（1）解密
受理事务 ID、内容 ID、AC1、{Kc ‖ AC2} Kcom
S368
将事务 ID、内容 ID、AC1 记录在特许信息保持部内用 KPm（1）将{Kc ‖ AC2} Kcom
再次加密并作为{{Kc ‖ AC2} Kcom} Km（1）记录在存储器内
S370
将接收运行记录删除
S372
内容数据（除计费对象外）取得步骤
内容数据传送请求
S374
从数据库取得{Data} Kc 及 DATA-inf
并输出{Data} Kc ‖ DATA-inf
S376
接收{Data} Kc ‖ DATA-inf
受理{Data} Kc ‖ DATA-inf
S378
将{Data} Kc ‖ DATA-inf 记录在存储器内
S380
发送传送受理
S382
接收发送受理
S384
传送结束处理
S386
结束
S390

图 12

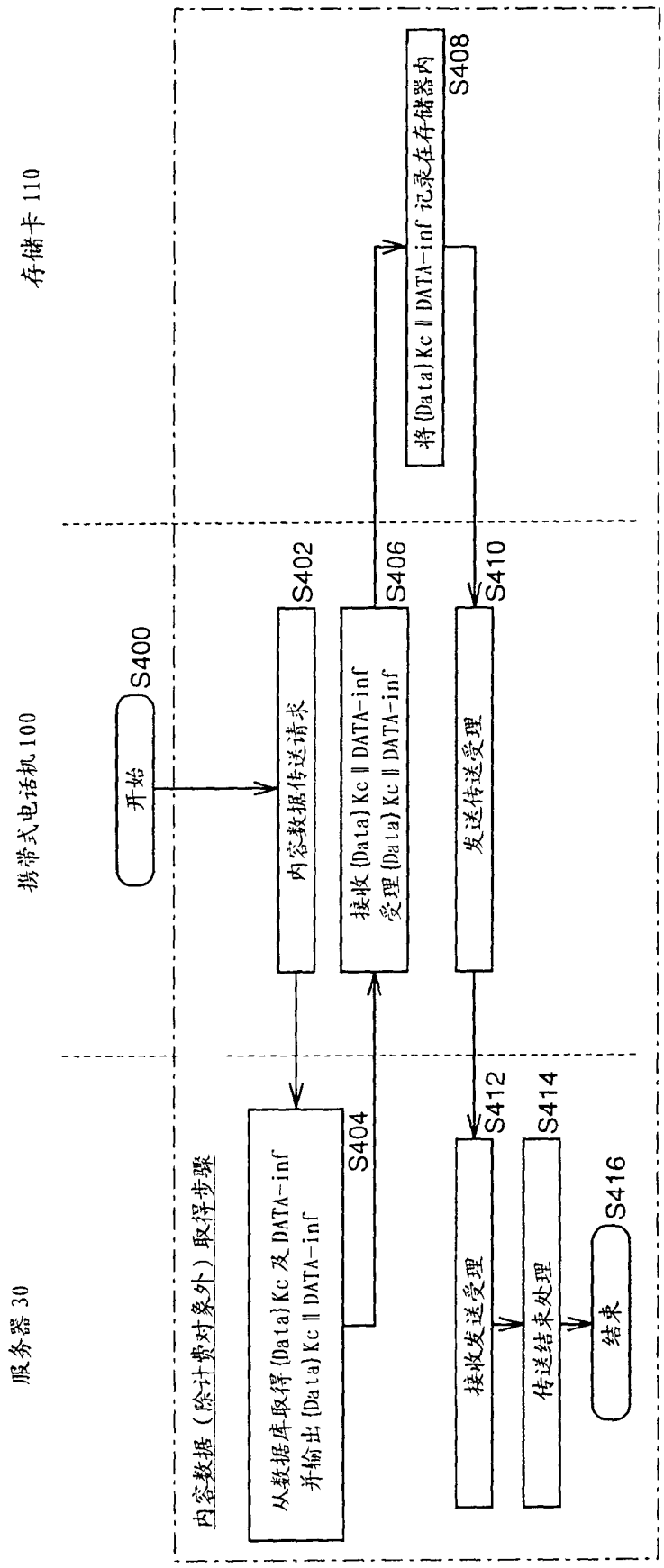

服务器 30
携带式电话机 100
存储卡 110
内容数据（除计费对象外）取得步骤
开始
S400
内容数据传送请求
S402
从数据库取得{Data}Kc及DATA-inf
并输出{Data}Kc‖DATA-inf
S404
接收{Data}Kc‖DATA-inf
受理{Data}Kc‖DATA-inf
S406
将{Data}Kc‖DATA-inf记录在存储器内
S408
发送传送受理
S410
接收发送受理
S412
传送结束处理
S414
结束
S416

图 13

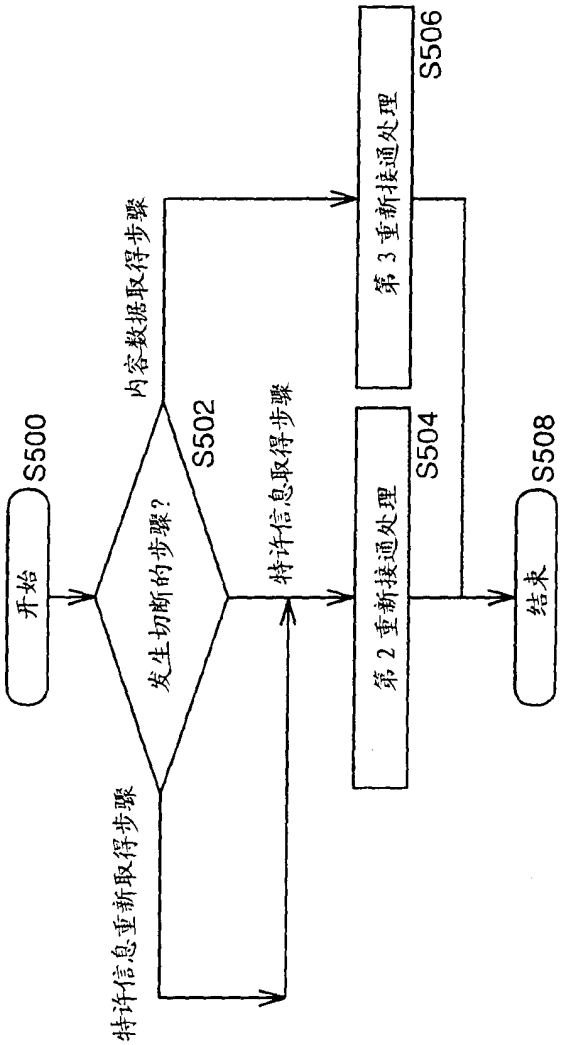

开始
S500
发生切断的步骤?
S502
内容数据取得步骤
特许信息取得步骤
特许信息重新取得步骤
第 2 重新接通处理
S504
第 3 重新接通处理
S506
结束
S508

图 14

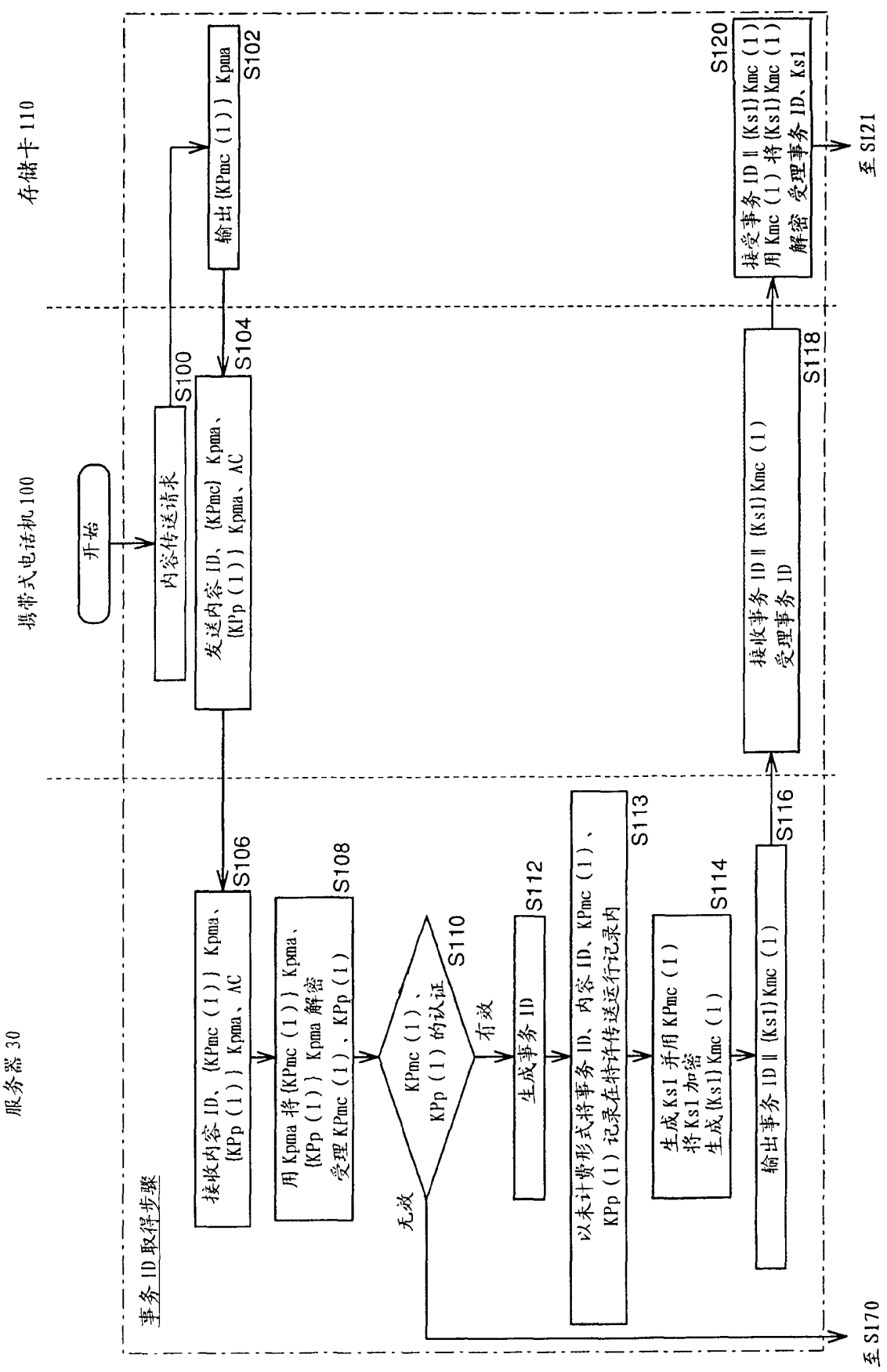

服务器 30
携带式电话机 100
存储卡 110
事务 ID 取得步骤
开始
内容传送请求
S100
发送内容 ID、{KPmc} Kpma、{KPp (1)} Kpma、AC
S104
输出 {KPmc (1)} Kpma
S102
接收内容 ID、{KPmc (1)} Kpma、{KPp (1)} Kpma、AC
S106
用 Kpma 将 {KPmc (1)} Kpma 解密
受理 KPmc (1)、KPp (1)
S108
KPmc (1)、KPp (1) 的认证
S110
无效
有效
生成事务 ID
S112
以未计费形式将事务 ID、内容 ID、KPmc (1)、KPp (1) 记录在特许传送运行记录内
S113
生成 Ks1 并用 KPmc (1) 将 Ks1 加密
生成 {Ks1} Kmc (1)
S114
输出事务 ID ‖ {Ks1} Kmc (1)
S116
接收事务 ID ‖ {Ks1} Kmc (1)
受理事务 ID
S118
接受事务 ID ‖ {Ks1} Kmc (1)
用 Kmc (1) 将 {Ks1} Kmc (1) 解密
受理事务 ID、Ks1
S120
至 S121
至 S170

图 15

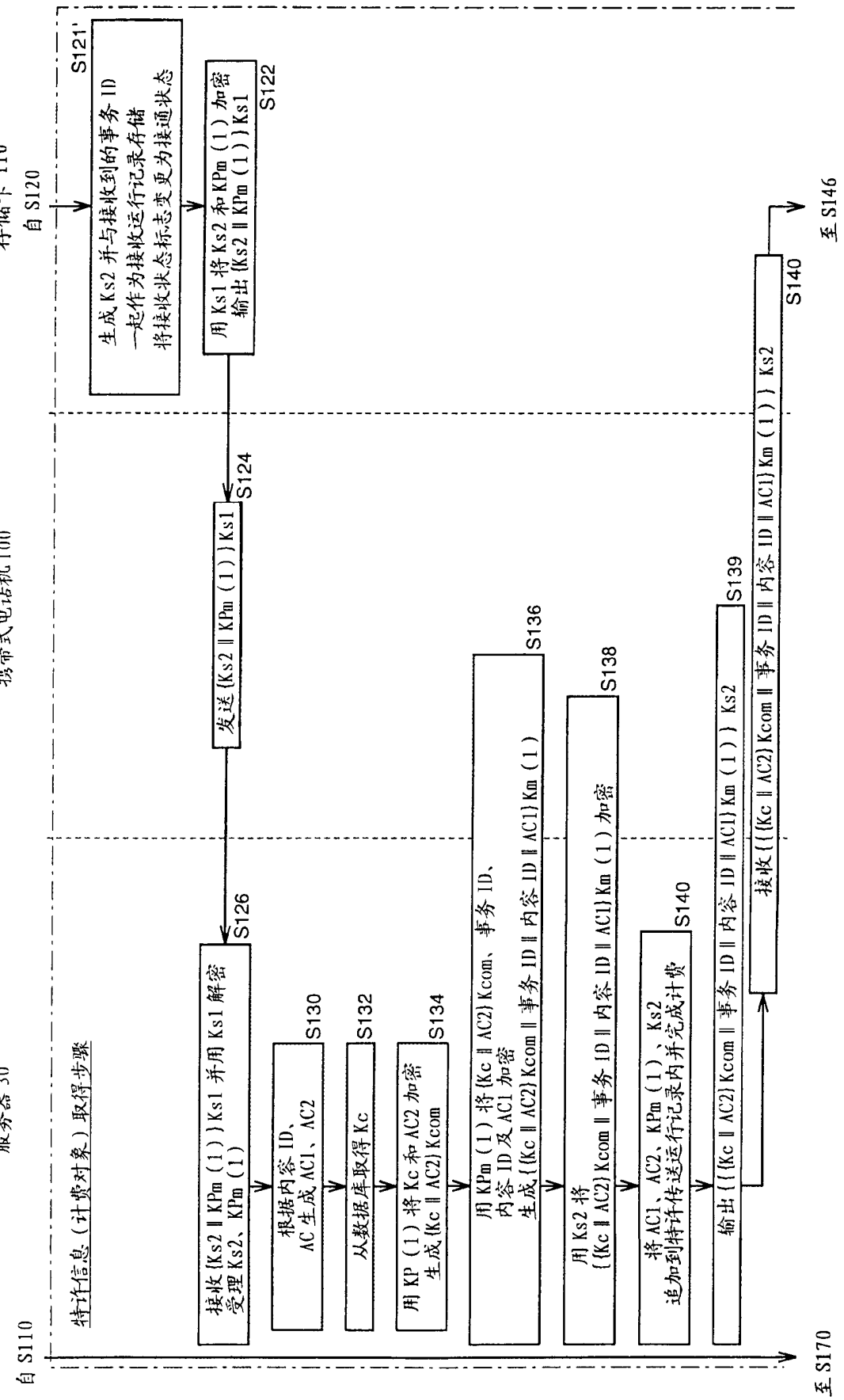

服务器 30
携带式电话机 100
存储卡 110
自 S110
特许信息（计费对象）取得步骤
自 S120
S121'
生成 Ks2 并与接收到的事务 ID
一起作为接收运行记录存储
将接收状态标志变更为接通状态
S122
用 Ks1 将 Ks2 和 KPm（1）加密
输出 {Ks2 ‖ KPm（1）} Ks1
S124
发送 {Ks2 ‖ KPm（1）} Ks1
S126
接收 {Ks2 ‖ KPm（1）} Ks1 并用 Ks1 解密
受理 Ks2、KPm（1）
S130
根据内容 ID、
AC 生成 AC1、AC2
S132
从数据库取得 Kc
S134
用 KP（1）将 Kc 和 AC2 加密
生成 {Kc ‖ AC2} Kcom
S136
用 KPm（1）将 {Kc ‖ AC2} Kcom、事务 ID、
内容 ID 及 AC1 加密
生成 {{Kc ‖ AC2} Kcom ‖ 事务 ID ‖ 内容 ID ‖ AC1} Km（1）
S138
用 Ks2 将
{{Kc ‖ AC2} Kcom ‖ 事务 ID ‖ 内容 ID ‖ AC1} Km（1）加密
S140
将 AC1、AC2、KPm（1）、Ks2
追加到特许传送运行记录内并完成计费
S139
输出 {{{Kc ‖ AC2} Kcom ‖ 事务 ID ‖ 内容 ID ‖ AC1} Km（1）} Ks2
S140
接收 {{{Kc ‖ AC2} Kcom ‖ 事务 ID ‖ 内容 ID ‖ AC1} Km（1）} Ks2
至 S146
至 S170

图 16

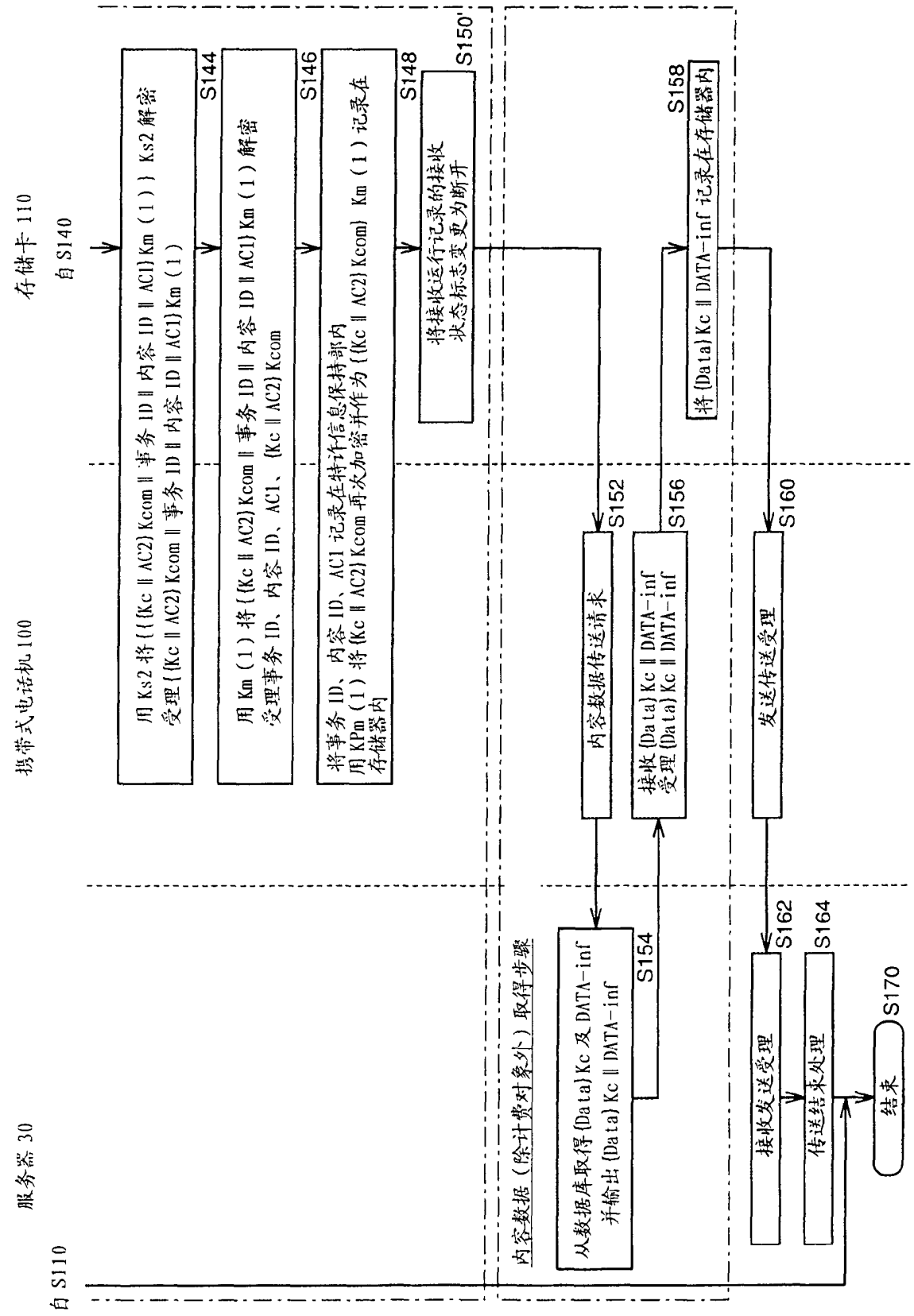

服务器 30
携带式电话机 100
存储卡 110
自 S110
自 S140
用 Ks2 将 {{{Kc ‖ AC2} Kcom ‖ 事务 ID ‖ 内容 ID ‖ AC1} Km（1）} Ks2 解密
受理 {{Kc ‖ AC2} Kcom ‖ 事务 ID ‖ 内容 ID ‖ AC1} Km（1）
S144
用 Km（1）将 {{Kc ‖ AC2} Kcom ‖ 事务 ID ‖ 内容 ID ‖ AC1} Km（1）解密
受理事务 ID、内容 ID、AC1、{Kc ‖ AC2} Kcom
S146
将事务 ID、内容 ID、AC1 记录在特许信息保持部内
用 KPm（1）将 {Kc ‖ AC2} Kcom 再次加密并作为 {{Kc ‖ AC2} Kcom} Km（1）记录在
存储器内
S148
将接收运行记录的接收
状态标志变更为断开
S150'
内容数据（除计费对象外）取得步骤
从数据库取得 {Data} Kc 及 DATA-inf
并输出 {Data} Kc ‖ DATA-inf
S154
内容数据传送请求
S152
接收 {Data} Kc ‖ DATA-inf
受理 {Data} Kc ‖ DATA-inf
S156
将 {Data} Kc ‖ DATA-inf 记录在存储器内
S158
发送传送受理
S160
接收发送受理
S162
传送结束处理
S164
结束
S170

图 17

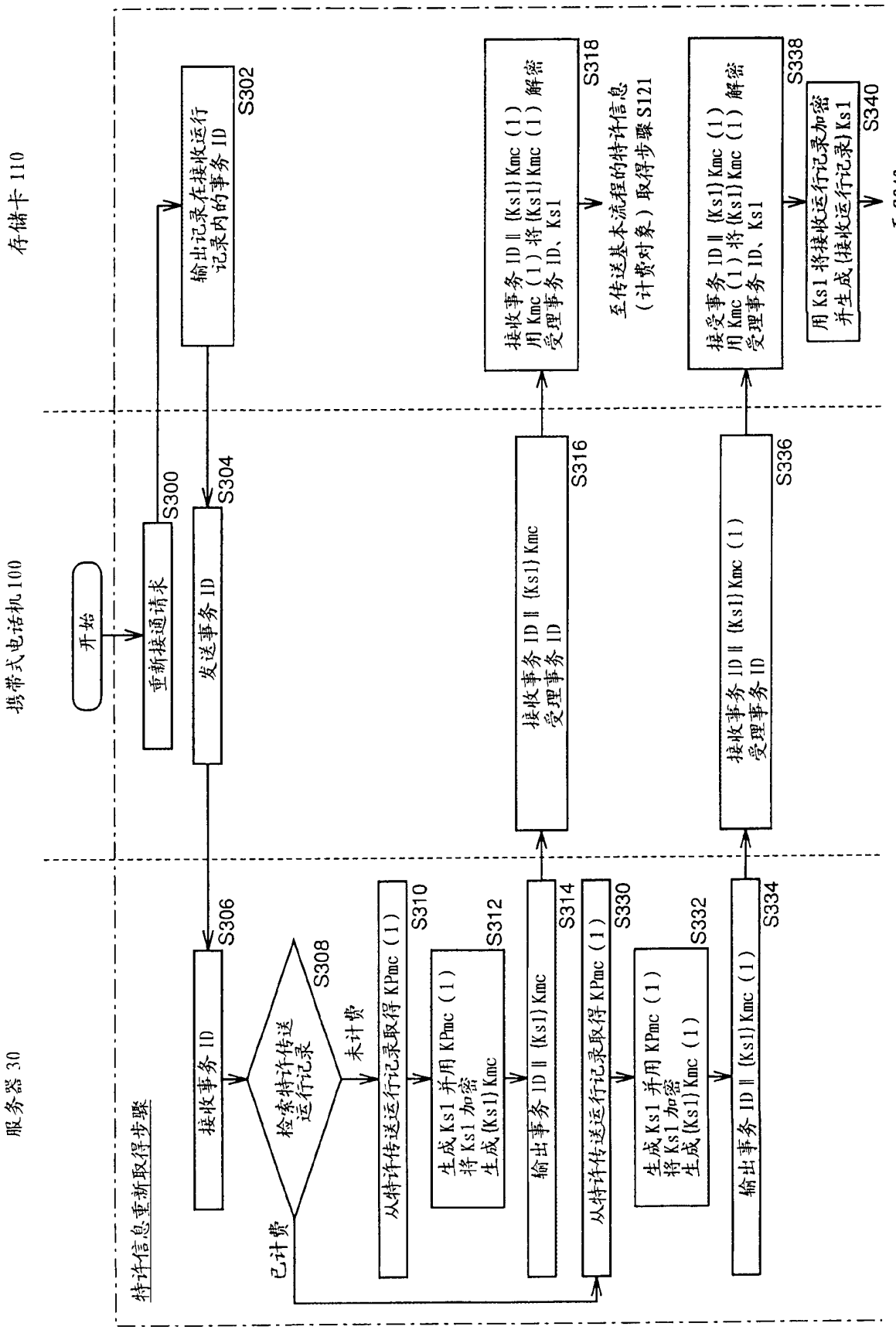

服务器 30
携带式电话机 100
存储卡 110
特许信息重新取得步骤
开始
重新接通请求
S300
输出记录在接收运行记录内的事务 ID
S302
发送事务 ID
S304
接收事务 ID
S306
检索特许传送运行记录
S308
已计费
未计费
从特许传送运行记录取得 KPmc（1）
S310
生成 Ks1 并用 KPmc（1）
将 Ks1 加密
生成{Ks1}Kmc
S312
输出事务 ID ‖ {Ks1}Kmc
S314
接收事务 ID ‖ {Ks1}Kmc
受理事务 ID
S316
接收事务 ID ‖ {Ks1}Kmc（1）
用 Kmc（1）将{Ks1}Kmc（1）解密
受理事务 ID、Ks1
S318
至传送基本流程的特许信息
（计费对象）取得步骤 S121
从特许传送运行记录取得 KPmc（1）
S330
生成 Ks1 并用 KPmc（1）
将 Ks1 加密
生成{Ks1}Kmc（1）
S332
输出事务 ID ‖ {Ks1}Kmc（1）
S334
接收事务 ID ‖ {Ks1}Kmc（1）
受理事务 ID
S336
接受事务 ID ‖ {Ks1}Kmc（1）
用 Kmc（1）将{Ks1}Kmc（1）解密
受理事务 ID、Ks1
S338
用 Ks1 将接收运行记录加密
并生成{接收运行记录}Ks1
S340
至 S342

图 18

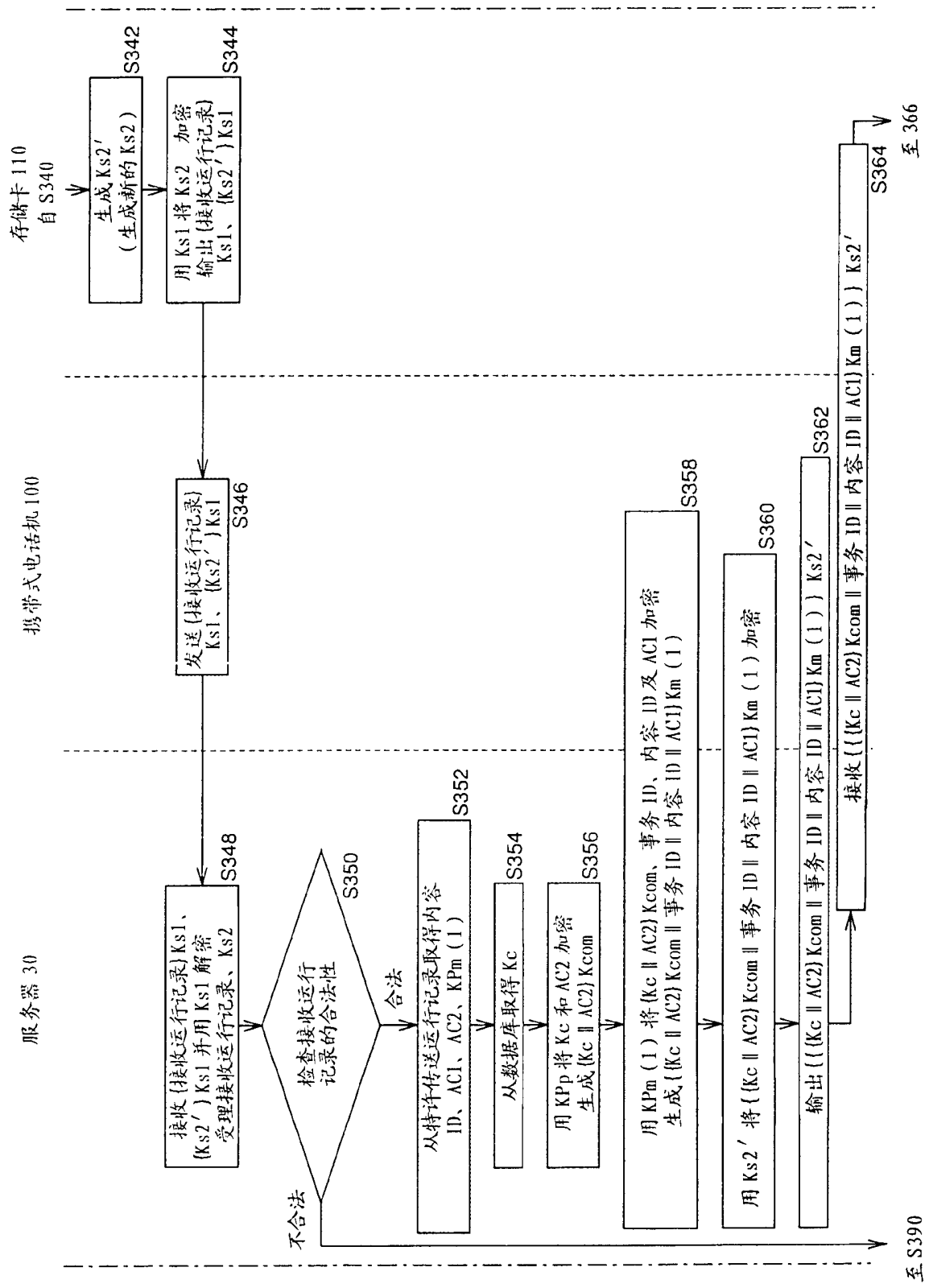

存储卡 110
自 S340
携带式电话机 100
服务器 30
生成 Ks2′
（生成新的 Ks2）
S342
用 Ks1 将 Ks2 加密
输出{接收运行记录}
Ks1、{Ks2′}Ks1
S344
发送{接收运行记录}
Ks1、{Ks2′}Ks1
S346
接收{接收运行记录}Ks1、
{Ks2′}Ks1 并用 Ks1 解密
受理接收运行记录、Ks2
S348
检查接收运行
记录的合法性
S350
不合法
合法
从特许传送运行记录取得内容
ID、AC1、AC2、KPm（1）
S352
从数据库取得 Kc
S354
用 KPp 将 Kc 和 AC2 加密
生成{Kc ‖ AC2}Kcom
S356
用 KPm（1）将{Kc ‖ AC2}Kcom、事务 ID、内容 ID 及 AC1 加密
生成{{Kc ‖ AC2}Kcom ‖ 事务 ID ‖ 内容 ID ‖ AC1}Km（1）
S358
用 Ks2′将{Kc ‖ AC2}Kcom ‖ 事务 ID ‖ 内容 ID ‖ AC1}Km（1）加密
S360
输出{{Kc ‖ AC2}Kcom ‖ 事务 ID ‖ 内容 ID ‖ AC1}Km（1）} Ks2′
S362
接收{{{Kc ‖ AC2}Kcom ‖ 事务 ID ‖ 内容 ID ‖ AC1}Km（1）} Ks2′
S364
至 366
至 S390

图 19

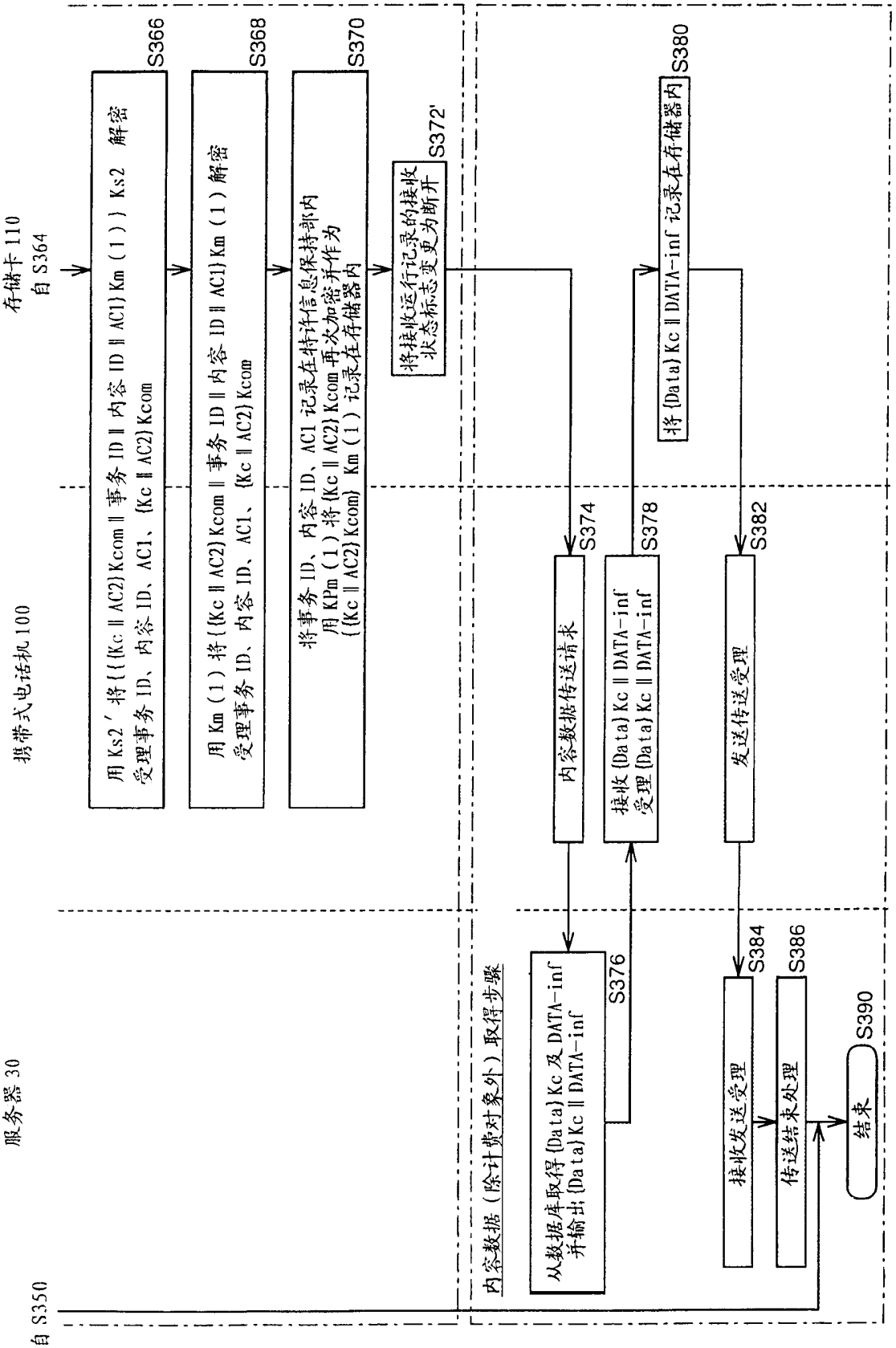

服务器 30
携带式电话机 100
存储卡 110
自 S350
自 S364
用 Ks2′ 将{{{Kc ‖ AC2}Kcom ‖ 事务 ID ‖ 内容 ID ‖ AC1}Km（1）} Ks2 解密
受理事务 ID、内容 ID、AC1、{Kc ‖ AC2}Kcom
S366
用 Km（1）将{{Kc ‖ AC2}Kcom ‖ 事务 ID ‖ 内容 ID ‖ AC1}Km（1）解密
受理事务 ID、内容 ID、AC1、{Kc ‖ AC2}Kcom
S368
将事务 ID、内容 ID、AC1 记录在特许信息保持部内
用 KPm（1）将{Kc ‖ AC2}Kcom 再次加密并作为
{{Kc ‖ AC2}Kcom} Km（1）记录在存储器内
S370
将接收运行记录的接收
状态标志变更为断开
S372′
内容数据（除计费对象外）取得步骤
从数据库取得{Data}Kc 及 DATA-inf
并输出{Data}Kc ‖ DATA-inf
S376
内容数据传送请求
S374
接收{Data}Kc ‖ DATA-inf
受理{Data}Kc ‖ DATA-inf
S378
将{Data}Kc ‖ DATA-inf 记录在存储器内
S380
发送传送受理
S382
接收发送受理
S384
传送结束处理
S386
结束
S390

图 20

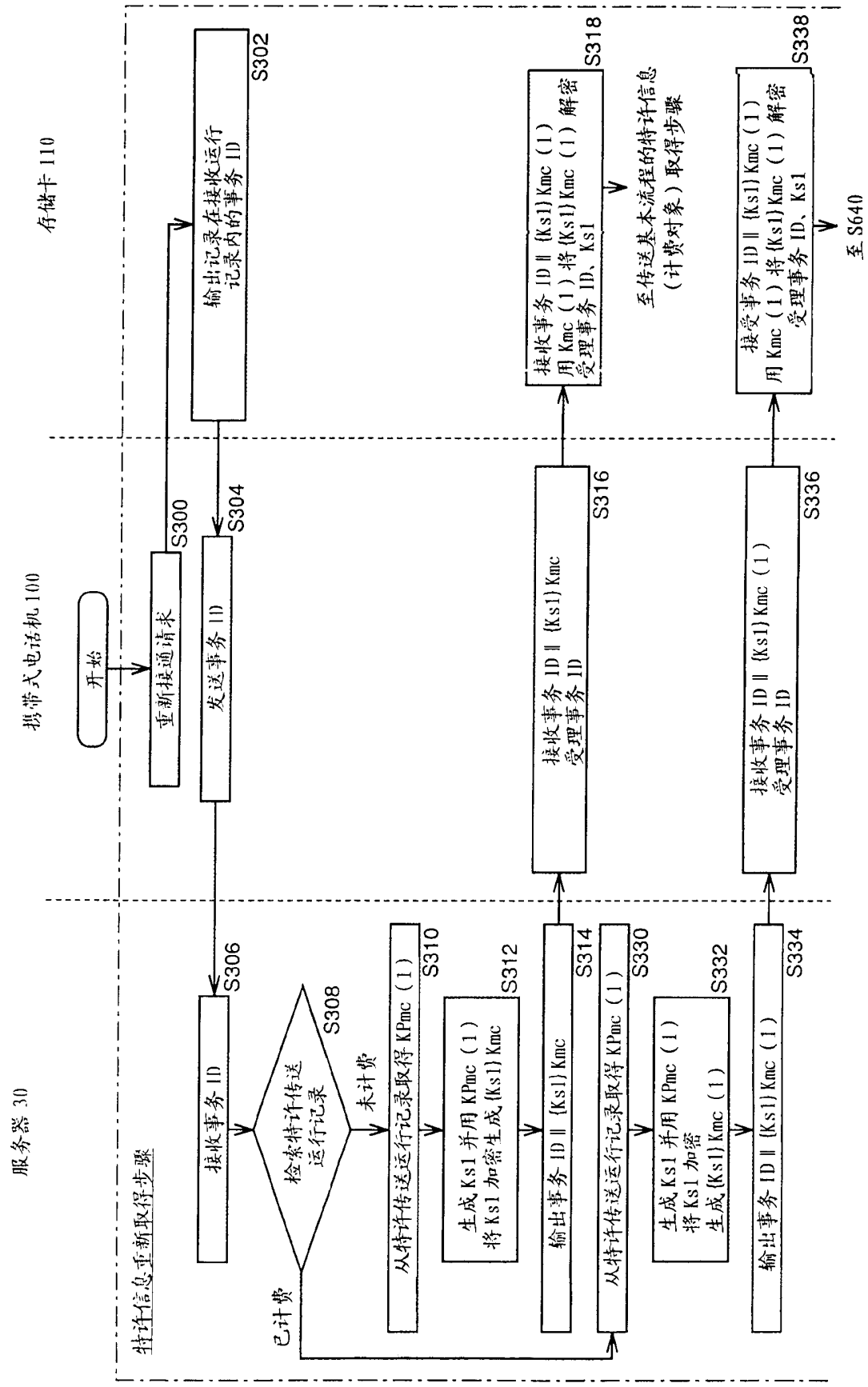

服务器 30
携带式电话机 100
存储卡 110
特许信息重新取得步骤
开始
重新接通请求
S300
发送事务 ID
S304
接收事务 ID
S306
检索特许传送运行记录
S308
已计费
未计费
从特许传送运行记录取得 KPmc（1）
S310
生成 Ks1 并用 KPmc（1）将 Ks1 加密生成 {Ks1} Kmc
S312
输出事务 ID ‖ {Ks1} Kmc
S314
接收事务 ID ‖ {Ks1} Kmc 受理事务 ID
S316
接收事务 ID ‖ {Ks1} Kmc（1）用 Kmc（1）将 {Ks1} Kmc（1）解密 受理事务 ID、Ks1
S318
至传送基本流程的特许信息（计费对象）取得步骤
从特许传送运行记录取得 KPmc（1）
S330
生成 Ks1 并用 KPmc（1）将 Ks1 加密生成 {Ks1} Kmc（1）
S332
输出事务 ID ‖ {Ks1} Kmc（1）
S334
接收事务 ID ‖ {Ks1} Kmc（1）受理事务 ID
S336
接受事务 ID ‖ {Ks1} Kmc（1）用 Kmc（1）将 {Ks1} Kmc（1）解密 受理事务 ID、Ks1
S338
至 S640
输出记录在接收运行记录内的事务 ID
S302

图 21

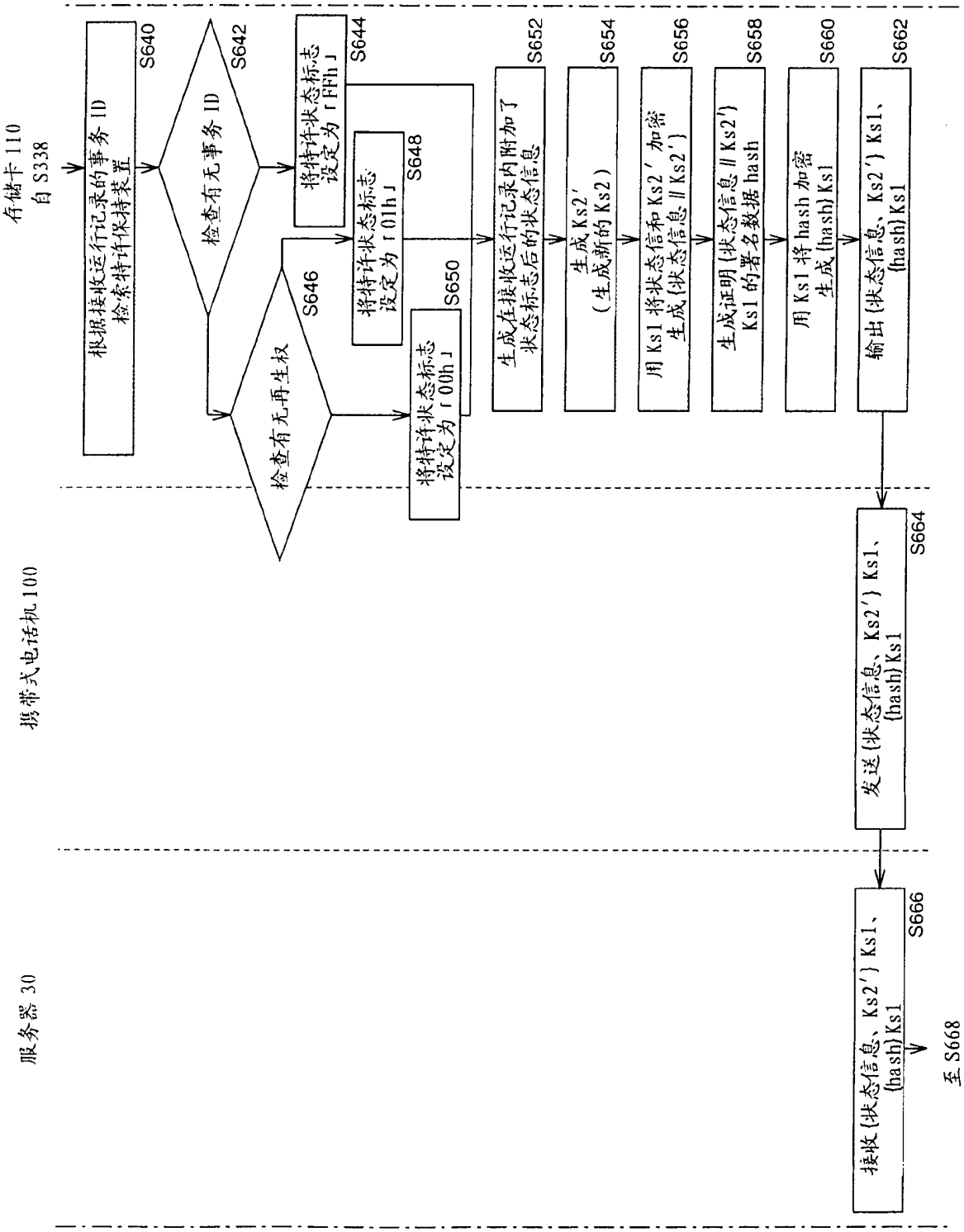

存储卡 110
自 S338
携带式电话机 100
服务器 30
根据接收运行记录的事务 ID
检索特许保持装置
S640
检查有无事务 ID
S642
将特许状态标志
设定为「FFh」
S644
检查有无再生权
S646
将特许状态标志
设定为「01h」
S648
将特许状态标志
设定为「00h」
S650
生成在接收运行记录内附加了
状态标志后的状态信息
S652
生成 Ks2′
（生成新的 Ks2）
S654
用 Ks1 将状态信和 Ks2′ 加密
生成{状态信息 // Ks2′}
S656
生成证明{状态信息 // Ks2′}
Ks1 的署名数据 hash
S658
用 Ks1 将 hash 加密
生成{hash}Ks1
S660
输出{状态信息、Ks2′} Ks1、
{hash}Ks1
S662
发送{状态信息、Ks2′} Ks1、
{hash}Ks1
S664
接收{状态信息、Ks2′} Ks1、
{hash}Ks1
S666
至 S668

图 22

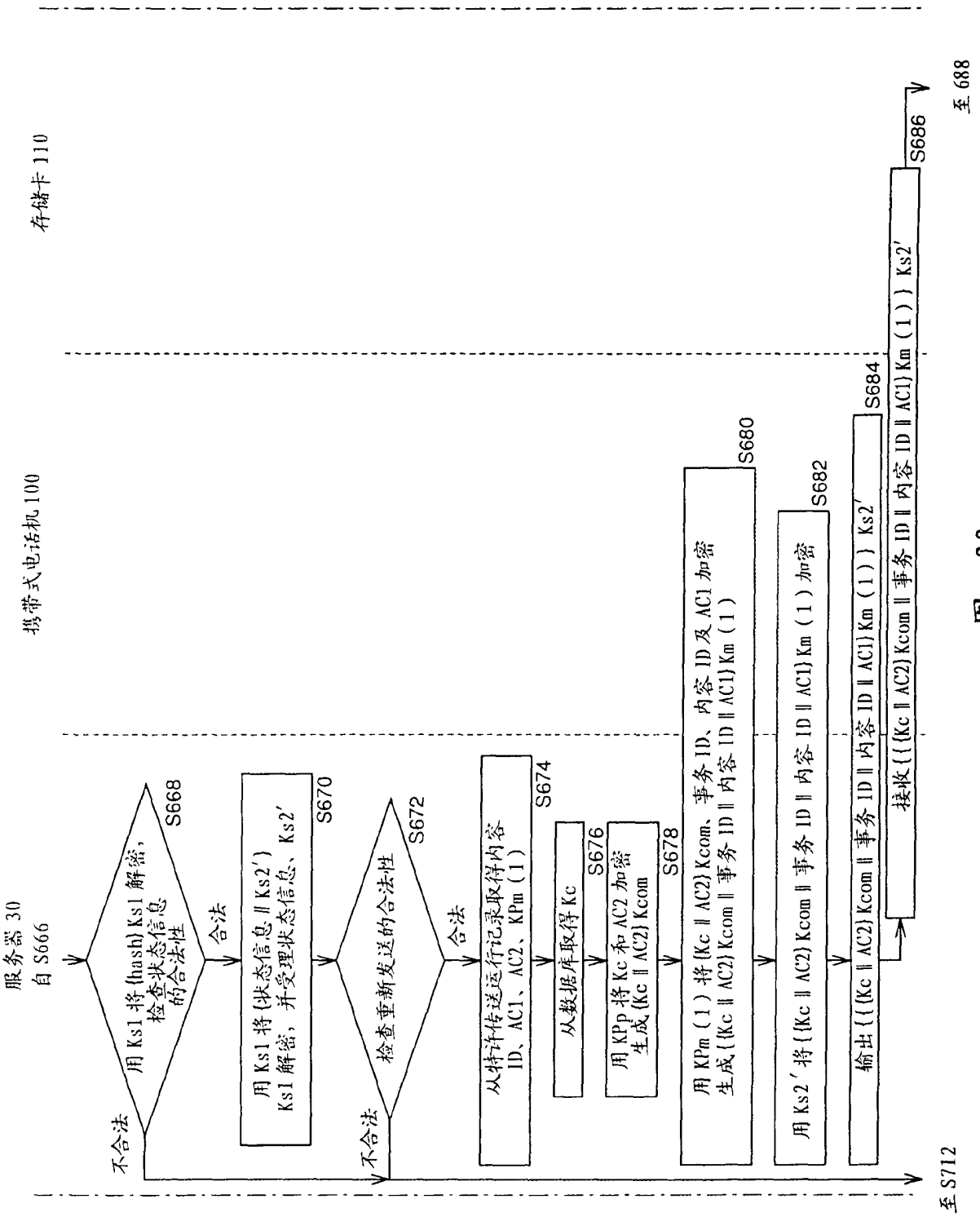

服务器 30
自 S666
携带式电话机 100
存储卡 110
用 Ks1 将 {hash} Ks1 解密，检查状态信息的合法性
S668
不合法
合法
用 Ks1 将 {状态信息 ‖ Ks2'} Ks1 解密，并受理状态信息、Ks2'
S670
检查重新发送的合法性
S672
不合法
合法
从特许传送运行记录取得内容 ID、AC1、AC2、KPm (1)
S674
从数据库取得 Kc
S676
用 KPp 将 Kc 和 AC2 加密生成 {Kc ‖ AC2} Kcom
S678
用 KPm (1) 将 {Kc ‖ AC2} Kcom、事务 ID、内容 ID 及 AC1 加密生成 {{Kc ‖ AC2} Kcom ‖ 事务 ID ‖ 内容 ID ‖ AC1} Km (1)
S680
用 Ks2' 将 {{Kc ‖ AC2} Kcom ‖ 事务 ID ‖ 内容 ID ‖ AC1} Km (1) 加密
S682
输出 {{{Kc ‖ AC2} Kcom ‖ 事务 ID ‖ 内容 ID ‖ AC1} Km (1)} Ks2'
S684
接收 {{{Kc ‖ AC2} Kcom ‖ 事务 ID ‖ 内容 ID ‖ AC1} Km (1)} Ks2'
S686
至 S712
至 688

图 23

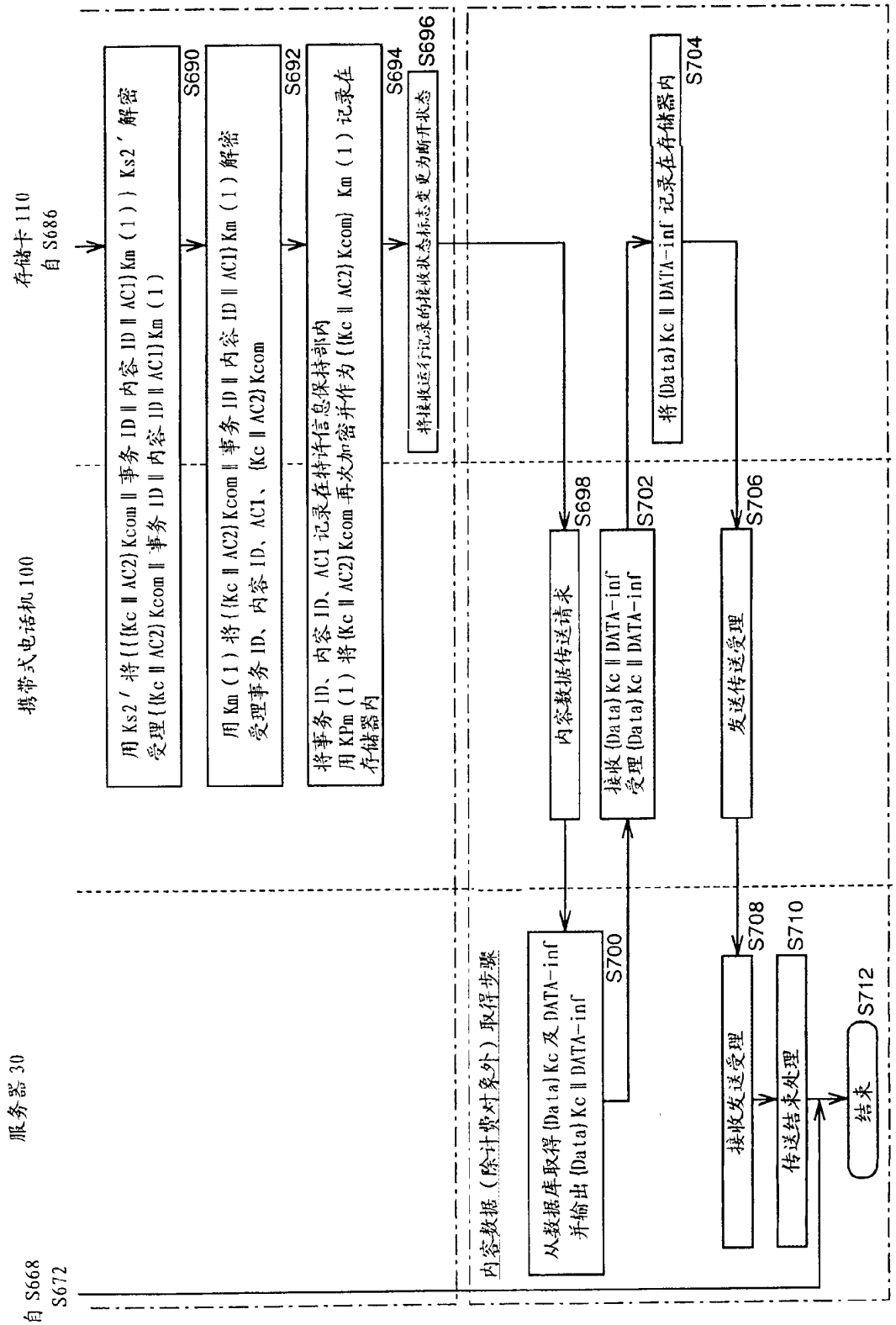

服务器 30
携带式电话机 100
存储卡 110
自 S668
S672
自 S686
用 Ks2′ 将{{{Kc ‖ AC2} Kcom ‖ 事务 ID ‖ 内容 ID ‖ AC1} Km (1)} Ks2′ 解密
受理{{Kc ‖ AC2} Kcom ‖ 事务 ID ‖ 内容 ID ‖ AC1} Km (1)
S690
用 Km (1) 将{{Kc ‖ AC2} Kcom ‖ 事务 ID ‖ 内容 ID ‖ AC1} Km (1) 解密
受理事务 ID、内容 ID、AC1、{Kc ‖ AC2} Kcom
S692
将事务 ID、内容 ID、AC1 记录在特许信息保持部内
用 KPm (1) 将{Kc ‖ AC2} Kcom 再次加密并作为{{Kc ‖ AC2} Kcom} Km (1) 记录在存储器内
S694
将接收许可记录的接收状态标志变更为断开状态
S696
内容数据（除计费对象外）取得步骤
从数据库取得{Data} Kc 及 DATA-inf
并输出{Data} Kc ‖ DATA-inf
S700
内容数据传送请求
S698
接收{Data} Kc ‖ DATA-inf
受理{Data} Kc ‖ DATA-inf
S702
将{Data} Kc ‖ DATA-inf 记录在存储器内
S704
发送传送受理
S706
接收发送受理
S708
传送结束处理
S710
结束
S712

图 24