(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 101989998 B
(45)授权公告日 2013.10.30

(21)申请号 201010237426.0
(22)申请日 2010.07.22
(30)优先权数据
2009-176573 2009.07.29 JP
(73)专利权人 索尼公司
地址 日本东京
(72)发明人 宫林直树 相马功 阿部野尚
米田好博 末吉正弘
(74)专利代理机构 中国国际贸易促进委员会专利商标事务所 11038
代理人 张荣海
(51)Int.Cl.
H04L 29/08(2006.01)
H04L 29/06(2006.01)
G06Q 30/00(2012.01)
G06Q 20/00(2012.01)

(56)对比文件
WO 2007107868 A2,2007.09.27,
WO 2009001197 A2,2008.12.31,
US 2005105734 A1,2005.05.19,
US 2008072061 A1,2008.03.20,
CN 1802647 A,2006.07.12,
CN 101258507 A,2008.09.03,
CN 101171604 A,2008.04.30,

审查员 胡锐先

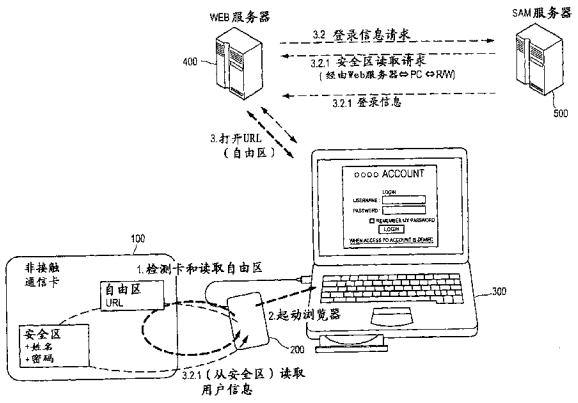
权利要求书3页 说明书15页 附图17页

(54)发明名称

信息处理设备、信息提供服务器和登录信息提供服务器

(57)摘要

本发明涉及信息处理设备、信息提供服务器和登录信息提供服务器。在一个例证实施例中，公开的通信系统包括从具有包括地址信息的第一区域和包括账户信息的第二区域的存储装置获得地址信息的信息处理设备。信息处理设备利用获得的地址信息与服务器的资源连接。信息处理设备使安全服务器从存储装置获得账户信息，并把获得的账户信息传给服务器，以致服务器使用户能够利用账户信息访问服务器的资源。



CN 101989998 B

1. 一种信息处理设备，包括：

处理器；

与处理器耦接的通信单元；和

与处理器耦接的存储装置，

其中与通信单元和存储装置合作的处理器响应非接触通信而：

(a) 从第二存储装置获得地址信息，第二存储装置具有：

(i) 包括所述地址信息的自由区；和

(ii) 包括账户信息的安全区；

(b) 利用所述获得的地址信息与服务器的资源连接；和

(c) 使安全服务器：

(i) 建立安全的通信路径；

(ii) 从所述第二存储装置获得所述账户信息；和

(iii) 把所述获得的账户信息传送给所述服务器，以致所述服务器使用户能够利用所述账户信息访问所述服务器的资源。

2. 按照权利要求 1 所述的信息处理设备，其中响应使与所述信息处理设备分离的通信卡接触或接近卡读 / 写器，发生所述非接触通信。

3. 按照权利要求 1 所述的信息处理设备，其中所述处理器向所述服务器请求用于确认对所述服务器的资源的访问的会话编号。

4. 按照权利要求 1 所述的信息处理设备，其中所述第二存储装置包括在与所述信息处理设备分离的非接触通信卡中。

5. 按照权利要求 1 所述的信息处理设备，其中所述地址信息包括 URL。

6. 按照权利要求 1 所述的信息处理设备，其中所述账户信息包括登录信息。

7. 按照权利要求 1 所述的信息处理设备，该信息处理设备包括操作上与所述处理器耦接的显示装置，其中所述处理器操作所述显示装置，以显示登录画面。

8. 一种操作信息处理设备的方法，所述方法包括：

响应非接触通信：

(a) 处理器从第二存储装置获得地址信息，所述第二存储装置具有：

(i) 包括所述地址信息的自由区；和

(ii) 包括账户信息的安全区；

(b) 所述处理器利用所述获得的地址信息与服务器的资源连接；和

(c) 所述处理器使安全服务器：

(i) 建立安全的通信路径；

(ii) 从所述第二存储装置获得所述账户信息；和

(iii) 把所述获得的账户信息传送给所述服务器，以致所述服务器使用户能够利用所述账户信息访问所述服务器的资源。

9. 一种服务器，包括：

处理器；

操作上与所述处理器耦接的通信单元；和

操作上与所述处理器耦接的存储装置，

其中与所述通信单元和所述存储装置合作的所述处理器响应非接触通信而：

(a) 与信息处理设备连接，所述信息处理设备被配置成利用从第二存储装置获得的地址信息与所述服务器连接，该第二存储装置具有

(i) 包括所述地址信息的自由区；和

(ii) 包括账户信息的安全区；

(b) 从安全服务器获得所述账户信息，所述安全服务器被配置成从所述第二存储装置的安全区获得所述账户信息；和

(c) 使用户能够利用所述从所述安全服务器获得的账户信息来访问所述服务器的资源。

10. 按照权利要求 9 所述的服务器，其中响应使与所述信息处理设备分离的通信卡接触或接近卡读 / 写器，发生所述非接触通信。

11. 按照权利要求 9 所述的服务器，其中所述处理器向所述信息处理设备发出会话编号，所述会话编号用于确认对所述服务器的资源的访问。

12. 按照权利要求 9 所述的服务器，其中所述地址信息包括 URL。

13. 按照权利要求 9 所述的服务器，其中所述账户信息包括登录信息。

14. 按照权利要求 9 所述的服务器，其中所述信息处理设备包括所述第二存储装置。

15. 一种操作服务器的方法，所述方法包括：

响应非接触通信：

(a) 处理器操作通信单元，从而与信息处理设备连接，所述信息处理设备被配置成利用从第二存储装置获得的地址信息与所述服务器连接，所述第二存储装置具有：

(i) 包括所述地址信息的自由区；和

(ii) 包括账户信息的安全区；

(b) 所述处理器从安全服务器获得所述账户信息，所述安全服务器被配置成从所述第二存储装置的安全区获得所述账户信息；和

(c) 所述处理器使用户能够利用所述从所述安全服务器获得的账户信息访问所述服务器的资源。

16. 一种信息处理设备，包括：

处理器；

操作上与所述处理器耦接的通信单元；和

操作上与所述处理器耦接的第一存储装置，

其中与所述通信单元和所述第一存储装置合作的所述处理器响应非接触通信而：

(a) 使显示装置起动安全服务器的浏览器；

(b) 从第二存储装置获得地址信息，该第二存储装置具有：

(i) 包括所述地址信息的自由区；和

(ii) 包括账户信息的安全区；

(c) 借助所述安全服务器的浏览器，利用所述获得的地址信息访问服务器；和

(d) 使所述安全服务器：

(i) 建立安全的通信路径；

(ii) 使用户能够选择第一访问目的地或第二访问目的地；

(iii) 响应选择了所述第一访问目的地，访问所述信息处理设备；和

(iv) 响应选择了所述第二访问目的地，访问所述第二存储装置的安全区。

17. 按照权利要求 16 所述的信息处理设备，其中响应使与所述信息处理设备分离的通信卡接触或接近卡读 / 写器，发生所述非接触通信。

18. 按照权利要求 16 所述的信息处理设备，所述信息处理设备包括操作上与所述处理器耦接的读 / 写器。

19. 按照权利要求 18 所述的信息处理设备，其中所述处理器操作所述读 / 写器，从而获得所述地址信息。

20. 按照权利要求 19 所述的信息处理设备，其中所述第二存储装置包括在与所述信息处理设备分离的非接触通信卡中。

21. 按照权利要求 16 所述的信息处理设备，其中所述地址信息包括 URL。

22. 按照权利要求 16 所述的信息处理设备，其中所述账户信息包括登录信息。

23. 一种操作信息处理设备的方法，所述方法包括：

响应非接触通信：

(a) 处理器使显示装置起动安全服务器的浏览器；

(b) 所述处理器从第二存储装置获得地址信息，该第二存储装置具有：

(i) 包括所述地址信息的自由区；和

(ii) 包括账户信息的安全区；

(c) 所述处理器借助所述安全服务器的浏览器，利用所述获得的地址信息访问服务器；和

(d) 所述安全服务器：

(i) 建立安全的通信路径；

(ii) 使用户能够选择第一访问目的地或第二访问目的地；

(iii) 响应选择了所述第一访问目的地，访问所述信息处理设备；和

(iv) 响应选择了所述第二访问目的地，访问所述第二存储装置的安全区。

信息处理设备、信息提供服务器和登录信息提供服务器

技术领域

[0001] 本发明提供一种信息处理设备，信息提供服务器，程序，通信系统和登录信息提供服务器。

背景技术

[0002] JP-A-2002-366868 公开一种能够与通信网络上的虚拟商店的电子商务服务器连接，购买商品的现有系统。该专利文献公开一种配有电子商务支持服务器的系统，所述服务器请求具有信用卡功能的 IC 卡中的唯一编号数据，并向电子商务服务器传送通过转换接收的唯一编号而生成的信誉数据。

[0003] 另外，JP-A-2002-366859 公开一种把诸如信用卡号之类的信息从加盟店传给发卡机构，并提交信贷请求的中间系统。

[0004] 不过，按照上面说明的现有技术，借贷和身份认证都由代理服务器完成，并进行向作为实际商业实体的电子商务服务器和加盟店终端返回结果的处理。这种方法存在代理服务器的结构变得复杂，并且系统规模增大，从而构成系统需要巨大成本的缺点。

发明内容

[0005] 鉴于上面所述，理想的是提供一种新颖的、改进的能够用安全的结构实现身份认证的信息处理设备，信息提供服务器，程序，通信系统和登录信息提供服务器。

[0006] 在例证实施例中，信息处理设备包括 ：处理器 ；操作上与处理器耦接的通信单元 ；和操作上与处理器耦接的存储装置，存储装置保存指令，所述指令使与通信单元和存储装置合作的处理器响应非接触通信 ：(a) 从具有 (i) 包括地址信息的自由区 ；和 (ii) 包括账户信息的安全区的第二存储装置获得地址信息 ；(b) 利用获得的地址信息与服务器的资源连接 ；和 (c) 使安全服务器 ：(i) 建立安全的通信路径 ；(ii) 从第二存储装置获得账户信息 ；和 (iii) 把获得的账户信息传送给服务器，以致服务器使用户能够利用账户信息访问服务器的资源。

[0007] 在例证实施例中，响应使通信卡接触或接近卡读 / 写器，发生非接触通信。

[0008] 在例证实施例中，指令使处理器向服务器请求用于确认对服务器资源的访问的会话编号。

[0009] 在例证实施例中，信息处理设备包括操作上与处理器耦接的卡读 / 写器。在例证实施例中，指令使处理器操作卡读 / 写器，从而获得地址信息。

[0010] 在例证实施例中，第二存储装置包括在信息处理设备中。在例证实施例中，第二存储装置包括在与信息处理设备分离的非接触通信卡中。

[0011] 在例证实施例中，地址信息包括 URL。在例证实施例中，账户信息包括登录信息。在例证实施例中，服务器包括 Web 服务器。

[0012] 在例证实施例中，信息处理设备包括操作上与处理器耦接的显示装置。在例证实施例中，方法包括使处理器执行操作显示装置，以显示登录画面的指令。

[0013] 在例证实施例中，一种操作包括指令的信息处理设备的方法，包括：响应非接触通信：(a) 使处理器执行指令，从而从具有 (i) 包括地址信息的自由区；和 (ii) 包括账户信息的安全区的第二存储装置获得地址信息；(b) 使处理器执行指令，以利用获得的地址信息与服务器的资源连接；和 (c) 使处理器执行指令，以使安全服务器：(i) 建立安全的通信路径；(ii) 从第二存储装置获得账户信息；和 (iii) 把获得的账户信息传送给服务器，以致服务器使用户能够利用账户信息访问服务器的资源。

[0014] 在例证实施例中，响应使通信卡接触或接近卡读 / 写器，发生非接触通信。

[0015] 在例证实施例中，所述方法包括使处理器执行指令，以向服务器请求用于确认对服务器资源的访问的会话编号。

[0016] 在例证实施例中，信息处理设备包括读 / 写器。在例证实施例中，所述方法包括使处理器执行指令，从而操作读 / 写器，以获得地址信息。

[0017] 在例证实施例中，信息处理设备包括第二存储装置。在例证实施例中，第二存储装置包括在与信息处理设备分离的非接触通信卡中。在例证实施例中，地址信息包括 URL。在例证实施例中，账户信息包括登录信息。在例证实施例中，服务器包括 Web 服务器。

[0018] 在例证实施例中，信息处理设备包括显示装置。在例证实施例中，所述方法包括使处理器执行操作显示装置，以显示登录画面。

[0019] 在例证实施例中，服务器包括：处理器；操作上与处理器耦接的通信单元；和操作上与处理器耦接的存储装置，所述存储装置保存指令，所述指令使与通信单元和存储装置合作的处理器响应非接触通信：(a) 与信息处理设备连接，信息处理设备被配置成利用从具有 (i) 包括地址信息的自由区；和 (ii) 包括账户信息的安全区的第二存储装置获得的地址信息与服务器连接；(b) 从安全服务器获得账户信息，安全服务器被配置成从第二存储装置的安全区获得账户信息；和 (c) 使用户能够利用从安全服务器获得的账户信息访问服务器的资源。

[0020] 在例证实施例中，响应使通信卡接触或接近卡读 / 写器，发生非接触通信。

[0021] 在例证实施例中，所述指令使处理器向信息处理设备发给会话编号，所述会话编号用于确认对服务器资源的访问。

[0022] 在例证实施例中，地址信息包括 URL。在例证实施例中，账户信息包括登录信息。在例证实施例中，服务器是 Web 服务器。在例证实施例中，信息处理设备包括第二存储装置。

[0023] 在例证实施例中，响应使通信卡接触或接近卡读 / 写器，发生非接触通信。

[0024] 在例证实施例中，操作包括指令的服务器的方法包括：响应非接触通信：(a) 使处理器执行指令，以操作通信单元，从而与信息处理设备连接，所述信息处理设备被配置成利用从具有 (i) 包括地址信息的自由区；和 (ii) 包括账户信息的安全区的第二存储装置获得的地址信息与服务器连接；(b) 使处理器执行指令，以从安全服务器获得账户信息，安全服务器被配置成从第二存储装置的安全区获得账户信息；和 (c) 使处理器执行指令，从而使用户能够利用从安全服务器获得的账户信息访问服务器的资源。

[0025] 在例证实施例中，响应使通信卡接触或接近卡读 / 写器，发生非接触通信。

[0026] 在例证实施例中，所述方法包括使处理器执行指令，从而向信息处理设备发给会话编号，所述会话编号用于确认对服务器资源的访问。

[0027] 在例证实施例中，地址信息包括 URL。在例证实施例中，账户信息包括登录信息。

在例证实施例中，服务器是 Web 服务器。

[0028] 在例证实施例中，信息处理设备包括第二存储装置。

[0029] 在例证实施例中，信息处理设备包括：处理器；操作上与处理器耦接的通信单元；和操作上与处理器耦接的第一存储装置，第一存储装置保存指令，所述指令使与通信单元和第一存储装置合作的处理器响应非接触通信：(a) 使显示装置起动安全服务器的浏览器；(b) 从具有 (i) 包括地址信息的自由区；和 (ii) 包括账户信息的安全区的第二存储装置获得地址信息；(c) 借助安全服务器的浏览器，利用获得的地址信息访问服务器；和 (d) 使安全服务器：(i) 建立安全的通信路径；(ii) 使用户选择第一访问目的地或第二访问目的地；(iii) 响应选择了第一访问目的地，访问信息处理设备；和 (iv) 响应选择了第二访问目的地，访问第二存储装置的安全区。

[0030] 在例证实施例中，响应使通信卡接触或接近卡读 / 写器，发生非接触通信。在例证实施例中，信息处理设备包括操作上与处理器耦接的读 / 写器。在例证实施例中，指令使处理器操作读 / 写器，从而获得地址信息。

[0031] 在例证实施例中，第二存储装置包括在信息处理设备中。在例证实施例中，第二存储装置包括在与信息处理设备分离的非接触通信卡中。

[0032] 在例证实施例中，地址信息包括 URL。在例证实施例中，账户信息包括登录信息。在例证实施例中，服务器包括 Web 服务器。

[0033] 在例证实施例中，操作包括指令的信息处理设备的方法包括：响应非接触通信：(a) 使处理器执行指令，从而使显示装置起动安全服务器的浏览器；(b) 使处理器执行指令，以从具有 (i) 包括地址信息的自由区；和 (ii) 包括账户信息的安全区的第二存储装置获得地址信息；(c) 使处理器执行指令，从而借助安全服务器的浏览器，利用获得的地址信息访问服务器；和 (d) 使安全服务器：(i) 建立安全的通信路径；(ii) 使用户选择第一访问目的地或第二访问目的地；(iii) 响应选择了第一访问目的地，访问信息处理设备；和 (iv) 响应选择了第二访问目的地，访问第二存储装置的安全区。

[0034] 在例证实施例中，响应使通信卡接触或接近卡读 / 写器，发生非接触通信。

[0035] 在例证实施例中，信息处理设备包括读 / 写器。在例证实施例中，所述方法包括使处理器执行指令，从而操作读 / 写器，以获得地址信息。

[0036] 在例证实施例中，信息处理设备包括第二存储装置。在例证实施例中，第二存储装置包括在与信息处理设备分离的非接触通信卡中。

[0037] 在例证实施例中，地址信息包括 URL。在例证实施例中，账户信息包括登录信息。在例证实施例中，服务器包括 Web 服务器。

[0038] 按照上面说明的本发明的实施例，能够提供一种能够用安全的结构进行身份认证的信息处理设备，信息提供服务器，程序，通信系统和登录信息提供服务器。

[0039] 另外的特征和优点在这里说明，并且根据下面的详细说明和附图将是显而易见的。

附图说明

[0040] 图 1 是示意表示按照第一实施例的系统结构，和信息交换的概念图；

[0041] 图 2 是表示按照本发明的第一实施例的系统的结构的示意图；

[0042] 图 3 是描述由第一实施例的系统执行的处理的序列图；

[0043] 图 4 是表示 SAM 服务器和非接触通信卡之间，图 3 中的步骤 S28 的登录信息获取过程的细节的序列图；

[0044] 图 5 是表示按照第一实施例的个人计算机的结构的功能方框图；

[0045] 图 6 是表示按照第一实施例的 Web 服务器的结构的功能方框图；

[0046] 图 7 是示意表示按照第二实施例的系统结构，和信息交换的概念图；

[0047] 图 8 是表示由第二实施例的系统执行的处理的序列图；

[0048] 图 9 是表示步骤 S88 的处理的序列图；

[0049] 图 10 是表示按照第二实施例的个人计算机的结构的功能方框图；

[0050] 图 11 是示意表示按照第三实施例的系统结构，和信息交换的概念图；

[0051] 图 12 是示意表示按照第三实施例的系统结构，和信息交换的概念图；

[0052] 图 13 是表示第三实施例的处理的序列图；

[0053] 图 14 是表示图 13 中的步骤 S158 的本地访问处理的细节的序列图；

[0054] 图 15 是说明 SAM 服务器的本地访问处理（步骤 S228 和后面的步骤）的流程图；

[0055] 图 16 是表示按照第三实施例的个人计算机的结构的功能方框图；以及

[0056] 图 17 是表示按照第三实施例的 SAM 服务器的结构的功能方框图。

具体实施方式

[0057] 下面参考附图，详细说明本发明的优选实施例。注意，在说明书和附图中，具有实质相同的功能和结构的结构元件用相同的附图标记表示，这些结构元件的重复说明被省略。

[0058] 另外，将按照下述顺序进行说明：

[0059] 1. 第一实施例（从 SAM 服务器获得登录信息的结构例子）

[0060] 2. 第二实施例（为登录标识分配会话编号的例子）

[0061] 3. 第三实施例（连接到 SAM 服务器的虚拟 Web 上的访问 URL 的例子）

[0062] 1. 第一实施例

[0063] 图 1 是示意表示按照第一实施例的系统结构和信息交换的概念图。如图 1 的概念图中所示，按照本实施例的系统包括非接触通信卡 100，卡读 / 写器 200，个人计算机 300，Web 服务器 400 和 SAM（安全应用模块）服务器 500。

[0064] 在根据图 1 说明本实施例的信息交换的概念时，非接触通信卡 100 在其存储器内包括自由区和安全区。诸如 URL 之类的信息保存在自由区中，诸如用户名和密码之类的登录信息保存在安全区中。当使非接触通信卡 100 与卡读 / 写器 200 接触或者接近卡读 / 写器 200 时，启动个人计算机 300 的浏览器，借助与 Web 服务器 400 的通信打开保存在非接触通信卡 100 的自由区中的 URL。

[0065] 当 Web 服务器 400 的 URL 被打开时，请求诸如用户名和密码之类的登录信息。Web 服务器 400 向 SAM 服务器 500 请求这些登录信息。SAM 服务器 500 经由 Web 服务器 400，个人计算机 (PC)300 和卡读 / 写器 200 向非接触通信卡 100 请求从非接触通信卡 100 的安全区读出，并获得登录信息。随后，SAM 服务器 500 把获得的登录信息传送给 Web 服务器 400。Web 服务器 400 利用接收的登录信息登录到该 URL。这使用户通过仅仅使非接触通信卡 100

接触或者接近卡读 / 写器 200，就能够访问 Web 服务器 400 的 URL。

[0066] 下面根据图 2-4，具体说明本实施例的系统。图 2 是表示按照本发明的第一实施例的系统的结构的示意图。如图 2 中所示，本实施例的系统包括非接触通信卡 100，卡读 / 写器 (R/W)200，个人计算机 (PC)300，Web 服务器 400，SAM(安全应用模块) 服务器 500。个人计算机 300，Web 服务器 400 和 SAM 服务器 500 按照经因特网 800 能够相互通信的方式被连接。

[0067] 非接触通信卡 100 包括 RF 单元 102，CPU 104 和存储器 106。RF 单元 102 从由卡读 / 写器 200 生成的 13.56MHz 频带的载波 (RF 信号) 中提取已用 Manchester 方案叠加的基带信号，并接收数据。另外，RF 单元 102 通过把非接触通信卡 100 的基带信号重叠在载波上，把数据传送给卡读 / 写器 200。CPU 104 执行这些通信控制，对卡中的存储器 106 的访问控制，和数据的加密 / 解密处理。存储器 106 为每种服务分割其区域，每个区域被设以可读 / 可写的属性。具体地说，主要为存储器 106 的区域确定两种属性 :需要通过验证和加密才能访问的区域 (下面称为安全区域)，和没有任何访问限制的区域 (下面称为自由区域)。

[0068] 卡读 / 写器 200 包括 RF 单元 202 和 CPU 204。RF 单元 202 生成 13.56MHz 频带的载波，并通过把基带信号叠加在传送的波上和从接收的波中提取基带信号，与非接触通信卡 100 通信。CPU 204 把从个人计算机 300 接收的通信控制命令转换成基带信号，并把基带信号传送给 RF 单元 202。另外，CPU 204 把从 RF 单元 202 接收的基带信号变换成 PC 的通信控制命令格式，并把基带信号传送给个人计算机 300。

[0069] 个人计算机 300 包括卡控制单元 302，通信单元 304，用户接口 (UI) 单元 306 和 CPU 308。卡控制单元 302 发出卡控制命令，并与卡读 / 写器 200 进行传输 / 接收。通信单元 304 与因特网 800 上的服务器，比如 SAM 服务器 500，Web 服务器 400 等通信。用户接口单元 306 具有用户的通过键盘、鼠标等输入指令的装置的功能，或者用户的输出装置，比如显示器、声音输出单元等的功能。CPU 308 根据从服务器获得的 html 信息显示和控制 Web 浏览器。此外，CPU 308 根据与服务器共用的加密设定信息，对因特网通信路径加密，并转换从 SAM 服务器 500 到卡读 / 写器 200 的控制信号。

[0070] 下面根据图 3 的序列图，说明由第一实施例的系统执行的处理。首先，说明卡的读取。个人计算机 300 向卡读 / 写器 200 传送读取控制信号，以读取非接触通信卡 100 的自由区中的信息 (步骤 S10)。

[0071] 随后，卡读 / 写器 200 进行轮询 (步骤 S12)。这里，卡读 / 写器 200 通过发送载波检测卡。当非接触通信卡 100 的天线收到载波，并且用电力激活 CPU 104 时，非接触通信卡 100 返回唯一的标识符 (IDm) 和卡的种类 (系统代码)。

[0072] 1.2) 自由区读取

[0073] 成功地检测到卡的卡读 / 写器 200 访问非接触通信卡 100 中的自由访问区。卡读 / 写器 200 读取将在个人计算机 300 的 Web 浏览器与因特网连接时使用的目的地 URL(起动 URL)，和配备 SAM(安全应用模块) 的 SAM 服务器 500 的 URL(步骤 S14)。这使 Web 浏览器的目的地 URL 和 SAM 服务器 500 的 URL 被发送给卡读 / 写器 200(步骤 S16)，并进一步被发送给个人计算机 300(步骤 S18)。

[0074] 2)Web 浏览器起动

[0075] 个人计算机 300 起动 Web 浏览器，以便显示从 Web 服务器 400 接收的 html 文件（步骤 S20）。另外例如，Internet Explorer，Firefox 等可被用作 Web 浏览器。

[0076] 3)http_get(Start URL，SAM_URL) 命令传输

[0077] 个人计算机 300 的 Web 浏览器传送 http_get 命令（包括起动 URL 和 SAM 服务器 500 的 URL)（步骤 S22)，并借助 http_get 命令经因特网 800 与 Web 服务器 400 的 URL 连接。个人计算机 300 的 Web 浏览器把 SAM 服务器 500 的 URL 传送给 Web 服务器 400。随后，个人计算机 300 的 Web 浏览器分析借助 http_get 命令获得的 http 格式的接收数据，并显示登录画面。这里，SAM 服务器 500 的地址 (URL) 作为参数被添加到 http_get 命令中。例如可实现 SAM 服务器的地址 (URL) 到 http_get 命令中的添加，比如 https://www.sample_web_server.co.jp/sam_login.cgi ? URL = https://www.sam_server.co.jp。

[0078] 3.1) 通信路径加密

[0079] 当从个人计算机 300 收到 http_get 命令时，Web 服务器 400 操作 CGI，并用 SSL 等加密到 SAM 服务器 500 的通信路径（步骤 S24）。随后，Web 服务器 400 通过利用从个人计算机 300 获得的 SAM 服务器 500 的 URL，访问 SAM 服务器 500。

[0080] 3.2) 登录信息请求

[0081] Web 服务器 400 向 SAM 服务器 500 请求登录信息（步骤 S26）。SAM 服务器 500 从非接触通信卡 100 的安全区获得登录信息（用户名和密码）（步骤 S28)，并登录到 Web 服务器 400。步骤 S28 的处理将在下面详细说明。

[0082] 3.2.1) 登录信息获取的细节

[0083] 图 4 是表示 SAM 服务器 500 和非接触通信卡 100 之间图 3 中的步骤 S28 的登录信息获取过程的细节的序列图。

[0084] 安全客户端起动请求

[0085] SAM 服务器 500 向 Web 服务器 400 传送对个人计算机 300 的安全客户端请求命令（步骤 S40）。

[0086] 1.1) 传送（安全客户端起动请求）

[0087] 首先，SAM 服务器 500 通过传输 http_get 命令等，向 Web 服务器 400 发出安全客户端起动请求（步骤 S40）。安全客户端是保存在个人计算机 300 中的程序。Web 服务器 400 把对安全客户端的请求命令传送给通过利用 http_get 命令连接的个人计算机 300（步骤 S42）。

[0088] 1.1.1) 安全客户端起动

[0089] 收到安全客户端起动命令的个人计算机 300 内的 CPU 308 起动安全客户端（步骤 S44）。该客户端程序加密 SAM 服务器 500 和个人计算机 300 之间的通信路径。另外，该客户端程序把从 SAM 服务器 500 接收的卡控制命令转换成卡读 / 写器 200 的控制命令，并进行对非接触通信卡 100 的卡控制。这导致从个人计算机 300 经由 Web 服务器 400 到 SAM 服务器 500 的路径被加密，并导致将在 SAM 服务器 500，Web 服务器 400 和个人计算机 300 之间传输 / 接收的分组被加密。因此，能够隐藏哪种命令被传送给非接触通信卡 100。

[0090] 2) 验证请求（公开信息 1)

[0091] 建立加密通信路径的 SAM 服务器 500 向个人计算机 300 传送验证请求命令，以向非接触通信卡 100 请求加密验证（步骤 S46）。利用随机数 N1 和私有密钥 A 生成的公开信

息（公开密钥）1 包括在该命令中。在 SAM 服务器 500，Web 服务器 400 和个人计算机 300 之间的加密传输路径中进行验证请求。另外，假定非接触通信卡 100 此时接近或接触卡读 / 写器 200，并且能够与卡读 / 写器 200 通信。

[0092] 1) 传送（验证请求）

[0093] 从 SAM 服务器 500 收到验证请求命令的 Web 服务器 400 把该命令原样传送给个人计算机 300（步骤 S48）。

[0094] 2.1.1) 验证请求（公开信息 1）

[0095] 在把验证请求命令转换成给卡读 / 写器 200 的验证请求命令之后，个人计算机 300 把该验证请求命令传送给卡读 / 写器 200（步骤 50）。

[0096] 2.1.1.1) 验证请求（公开信息 1）

[0097] 在把验证请求命令转换成 RF 信号之后，卡读 / 写器 200 把 RF 信号传送给非接触通信卡 100（步骤 S52）。私有密钥 A 被保存在非接触通信卡 100 中，从而非接触通信卡 100 利用密钥 A 和随机数 N2 生成公开信息（公开密钥）2。公开信息 2 经卡读 / 写器 200、个人计算机 300 和 Web 服务器 400 被返回给 SAM 服务器 500。

[0098] 3)，4) 共用密钥生成

[0099] 通过传输 / 接收和交换公开信息 1 和 2，非接触通信卡 100 和 SAM 服务器 500 均生成对非接触通信卡 100 和 SAM 服务器 500 来说是相同密钥的共用密钥（私有密钥）（步骤 S54，S56），共用密钥被共用。在生成共用密钥之后，在用该共用密钥加密的情况下，非接触通信卡 100 的安全区中的必要区域的读取值被传送。另外，可用通常称为“Diffie-Hellman 密钥交换”的方法实现从步骤 S46 到步骤 S56 的共用密钥的生成。按照这种方式形成从 SAM 服务器 500 到非接触通信卡 100 的加密通信路径，SAM 服务器 500 和非接触通信卡 100 将处于能够实现安全通信的状态。

[0100] 5) 安全区读取请求

[0101] 为了获得写入非接触通信卡 100 的安全区中的登录信息（用户名、密码等），SAM 服务器 500 利用加密通信路径，经 Web 服务器 400 向个人计算机 300 传送对非接触通信卡 100 的安全区的读取请求（步骤 S58）。关于非接触通信卡 100 的存储器 106 上的待访问区域（服务区）的信息被包括在对安全区的读取请求中。

[0102] 5.1) 传送（安全区读取请求）

[0103] 从 SAM 服务器 500 收到对安全区的读取请求的 Web 服务器 400 把该命令原样传送给个人计算机 300（步骤 S60）。

[0104] 5.1.1) 安全区读取请求

[0105] 当收到对安全区的读取请求时，个人计算机 300 上的安全客户端把对安全区的读取请求转换成卡读 / 写器 200 的命令格式，并将其传送给卡读 / 写器 200（步骤 S62）。

[0106] 5.1.1.1) 安全区访问

[0107] 收到对安全区的读取请求的卡读 / 写器 200 访问非接触通信卡 100 的安全区（步骤 S64）。非接触通信卡 100 用共用密钥加密保存在安全区中的登录信息（用户名和密码），并经由加密通信路径把其返回给 SAM 服务器 500（步骤 S66）。

[0108] 6) 登录信息解密

[0109] 当从加密传输路径收到非接触通信卡 100 的登录信息时，SAM 服务器 500 利用共

用密钥，对加密的登录信息解密（步骤 S68）。

[0110] 按照上面说明的图 4 中的序列，SAM 服务器 500 能够在图 3 中的步骤 S28 中从非接触通信卡 100 获得登录信息。

[0111] SAM 服务器 500 把解密的登录信息发送给 Web 服务器 400（图 3 中的步骤 S30）。Web 服务器 400 利用接收的解密登录信息进行登录。从而完成到 Web 服务器 400 的登录（步骤 S30），在个人计算机 300 的屏幕上显示登录后的画面。因此，用户能够检查他 / 她已登录的个人计算机 300 的 Web 浏览器画面。

[0112] 因此，由于非接触通信卡 100 的安全区的登录信息从 SAM 服务器 500 被传送给 Web 服务器 400，因此用户能够在不在登录画面上输入用户名、密码等的情况下自动登录到 Web 服务器 400。

[0113] 图 5 是表示按照第一实施例的个人计算机 300 的结构的功能方框图。如图 5 中所示，个人计算机 300 包括访问目的地信息传输单元 310，登录信息传输单元 312，和接收处理单元 314。每个功能块可用设置在个人计算机 300 中的硬件、CPU 308 和使 CPU 308 运行的软件（程序）构成。程序可被保存在设置于个人计算机 300 中的硬盘中，或者保存在诸如在外部与个人计算机 300 连接的存储器之类的记录介质中。

[0114] 此外，图 6 是表示按照第一实施例的 Web 服务器 400 的结构的功能方框图。如图 6 中所示，Web 服务器 400 包括访问目的地信息获取单元 410，登录信息获取单元 412，登录执行单元 414 和传输处理单元 416。每个功能块可由设置在 Web 服务器 400 中的硬件、CPU 402 和使 CPU 402 运行的软件（程序）构成。程序可被保存在设置于 Web 服务器 400 中的硬盘中，或者保存在诸如在外部与 Web 服务器 400 连接的存储器之类的记录介质中。

[0115] 如上所述，按照第一实施例，SAM 服务器 500 把已从加密传输路径发送给 SAM 服务器 500 的登录信息发送给 Web 服务器 400，并登录到 Web 服务器 400。这使用户仅仅通过把非接触通信卡 100 保持在卡读 / 写器 200 上方，就能够容易地实现登录。

[0116] 2. 第二实施例

[0117] 下面，说明本发明的第二实施例。第二实施例涉及利用会话编号，经由 SAM 服务器 500 的登录。

[0118] 图 7 是示意表示按照第二实施例的系统结构，和信息交换的概念图。如图 7 的概念图中所示，本实施例的系统还包括非接触通信卡 100，卡读 / 写器 200，个人计算机 300，Web 服务器 400 和 SAM（安全应用模块）服务器 500。

[0119] 在根据图 7 说明本实施例的信息交换的概念时，非接触通信卡 100 在其存储器内包括自由区和安全区。诸如 URL 之类的登录信息被保存在自由区中，诸如用户名和密码之类的信息被保存在安全区中。当使非接触通信卡 100 接触或接近卡读 / 写器 200 时，起动个人计算机 300 的浏览器，保存在非接触通信卡 100 的自由区中的 URL 由与 Web 服务器 400 的通信打开。

[0120] 当 Web 服务器 400 的 URL 被打开时，请求诸如用户名和密码之类的登录信息。个人计算机 300 向 SAM 服务器 500 请求这些登录信息。SAM 服务器 500 经由个人计算机 (PC) 300 和卡读 / 写器 200 向非接触通信卡 100 请求从非接触通信卡 100 的安全区读出，并获得登录信息。随后，SAM 服务器 500 把获得的登录信息传送给 Web 服务器 400。Web 服务器 400 利用接收的登录信息登录到该 URL。这使用户通过仅仅使非接触通信卡 100 接触或者接近

卡读 / 写器 200，就能够访问 Web 服务器 400 的 URL。

[0121] 下面根据图 8 和 9，详细说明本实施例的系统。按照第二实施例的系统结构和非接触通信卡 100、卡读 / 写器 200、个人计算机 300、Web 服务器 400 和 SAM 服务器 500 的结构与图 2 中的相同。

[0122] 图 8 是表示由第二实施例的系统进行的处理的序列图。首先，个人计算机 300 读取非接触通信卡（步骤 S70-S78）。随后，个人计算机 300 起动 Web 浏览器（步骤 S80）。步骤 S70-S80 的处理和图 3 中的步骤 S10-S20 的处理相同。

[0123] 3)http_get（起动 URL）命令传输

[0124] 个人计算机 300 的 Web 浏览器传送 http_get 命令（包括起动 URL）（步骤 S82）。随后，Web 浏览器依据 http_get 命令，经由因特网 800 与 Web 服务器 400 的 URL 连接，分析由 http_get 命令获得的 http 格式的接收数据，并显示登录画面。

[0125] 4)https_get（会话编号请求）

[0126] 在利用 SSL 加密到 Web 服务器 400 的通信路径之后，个人计算机 300 访问 Web 服务器 400，请求该服务器发给会话编号（步骤 S84）。这里，通过利用随机数等，由 Web 服务器 400 发给的会话编号能够与另一用户的登录会话编号区分开，或者当达到某一有效期时，由 Web 服务器 400 发给的会话编号会失效。如后所述，会话编号是用于确认用户的登录的编号，将是唯一的编号。

[0127] 例如，个人计算机 300 利用 https_get 命令传送“https://www.web_server.co.jp/login.html+get_session_number.cgi”。Web 服务器 400 按 html 格式描述由执行代码（CGI 脚本等）生成的会话编号，并将其返回给 https_get（步骤 S85）。

[0128] 5)https_get(SAM_URL，login_URL，会话编号）

[0129] 在利用 SSL 对到 SAM 服务器 500 的通信路径加密之后，个人计算机 300 访问 SAM 服务器 500，并向 SAM 服务器 500 传送对 Web 服务器 400 的登录请求命令（步骤 S86）。此时，作为登录目的地的 Web 服务器 400 的 URL，SAM 服务器 500 的 URL，和在步骤 S85 中从 Web 服务器 400 获得的会话编号信息作为参数被添加到该请求命令中。另外，登录目的地的 URL 和 SAM 服务器 500 的 URL 读取自非接触通信卡 100 的存储器。

[0130] 例如，个人计算机 300 利用 https_get 命令传送“https://www.sam_server.co.jp/remote_login.cgi ？ URL ＝ www.web_server.co.jp ？ session ＝ XXX”，SAM 服务器 500 激活用于获取登录信息的执行代码（CGI 脚本等）。

[0131] 5.1) 登录信息获取

[0132] 随后，SAM 服务器 500 从非接触通信卡 100 的安全区获得登录信息（步骤 S88）。这里的获取方法和第一实施例的用图 4 说明的处理相同，不过 Web 服务器 400 不在 SAM 服务器 500 和个人计算机 300 之间充当中介。第二实施例和第一实施例的不同之处在于 SAM 服务器 500 和个人计算机 300 直接相互通信。

[0133] 图 9 是表示步骤 S88 的处理的序列图。

[0134] 1) 安全客户端起动请求

[0135] 首先，SAM 服务器 500 通过传送 http_get 命令等，向个人计算机 300 发出安全客户端起动请求（步骤 S100）。安全客户端是保存在个人计算机 300 中的程序。

[0136] 1.1.1) 安全客户端起动

[0137] 收到安全客户端起动命令的个人计算机 300 内的 CPU 308 起动安全客户端（步骤 S102）。该客户端程序是加密 SAM 服务器 500 和个人计算机 300 之间的通信路径，另外还把从 SAM 服务器 500 接收的卡控制命令转换成卡读 / 写器 200 的控制命令，并对非接触通信卡 100 进行卡控制的程序。这使从个人计算机 300 到 SAM 服务器 500 的路径被加密，并且使在 SAM 服务器 500，Web 服务器 400 和个人计算机 300 之间传输 / 接收的分组被加密。因此，能够隐藏哪种命令被传送给非接触通信卡 100。

[0138] 2) 验证请求（公开信息 1）

[0139] 建立加密通信路径的 SAM 服务器 500 向个人计算机 300 传送验证请求命令，以向非接触通信卡 100 要求加密验证（步骤 S104）。利用随机数 N1 和私有密钥 A 生成的公开信息（公开密钥）1 包括在该命令中。在 SAM 服务器 500，Web 服务器 400 和个人计算机 300 之间的加密传输路径中进行验证请求。另外，假定非接触通信卡 100 此时接近或接触卡读 / 写器 200，并且能够与卡读 / 写器 200 通信。

[0140] 2.1) 验证请求（公开信息 1）

[0141] 在把验证请求命令转换成给卡读 / 写器 200 的验证请求命令之后，个人计算机 300 把该验证请求命令传送给卡读 / 写器 200（步骤 106）。

[0142] 2.1.1) 验证请求（公开信息 1）

[0143] 在把验证请求命令转换成 RF 信号之后，卡读 / 写器 200 把 RF 信号传送给非接触通信卡 100（步骤 S108）。私有密钥 A 被保存在非接触通信卡 100 中，从而非接触通信卡 100 利用密钥 A 和随机数 N2 生成公开信息（公开密钥）2。公开信息 2 经卡读 / 写器 200 和个人计算机 300 被返回给 SAM 服务器 500（步骤 S109）。

[0144] 3)，4) 共用密钥生成

[0145] 通过传输 / 接收和交换公开信息 1 和 2，非接触通信卡 100 和 SAM 服务器 500 均生成对非接触通信卡 100 和 SAM 服务器 500 来说是相同密钥的共用密钥（私有密钥）（步骤 S110，S112），共用密钥被共用。在生成共用密钥之后，在用该共用密钥加密的情况下，非接触通信卡 100 的安全区中的必要区域的读取值被传送。另外，和第一实施例一样，可用通常称为“Diffie-Hellman 密钥交换”的方法实现从步骤 S104 到步骤 S112 的共用密钥的生成。按照这种方式形成从 SAM 服务器 500 到非接触通信卡 100 的加密通信路径，SAM 服务器 500 和非接触通信卡 100 将处于能够实现安全通信的状态。

[0146] 5) 安全区读取请求

[0147] SAM 服务器 500 获得写入非接触通信卡 100 的安全区中的登录信息（用户名、密码等）。为此，SAM 服务器 500 利用加密通信路径，向个人计算机 300 传送对非接触通信卡 100 的安全区的读取请求（步骤 S114）。关于非接触通信卡 100 的存储器 106 上的待访问区域（服务区）的信息被包括在对安全区的读取请求中。

[0148] 5.1) 安全区读取请求

[0149] 当收到对安全区的读取请求时，个人计算机 300 上的安全客户端把对安全区的读取请求转换成卡读 / 写器 200 的命令格式。随后，安全客户端把呈转换后的命令格式的读取命令传送给卡读 / 写器 200（步骤 S116）。

[0150] 5.1.1) 安全区访问

[0151] 收到对安全区的读取请求的卡读 / 写器 200 访问非接触通信卡 100 的安全区（步

骤 S118)。非接触通信卡 100 用共用密钥加密保存在安全区中的登录信息（用户名和密码），并经由加密传输路径把其返回给 SAM 服务器 500（步骤 S120)。

[0152] 6) 登录信息解密

[0153] 当从加密传输路径收到非接触通信卡 100 的登录信息时，SAM 服务器 500 利用共用密钥，对加密的登录信息解密（步骤 S122)。

[0154] 按照上面说明的图 9 中的序列，SAM 服务器 500 能够在图 8 中的步骤 S88 中从非接触通信卡 100 获得登录信息。

[0155] 5.2) 通信路径加密

[0156] 获得登录信息的 SAM 服务器 500 与由在图 8 的步骤 S86 中获得的登录 URL 中指定的 Web 服务器 400 连接，并利用 SSL 之类的处理对通信路径加密（图 8 中的步骤 S90)。

[0157] 5.3) 登录请求（登录信息，会话编号）

[0158] SAM 服务器 500 向 Web 服务器 400 传送包括登录信息（用户名，密码，会话编号等）的命令（步骤 S92)。通过接收会话编号，Web 服务器 400 能够识别源自 SAM 服务器 500 的登录被指定给哪个会话。Web 服务器 400 检查登录信息的真 / 假，随后，在登录信息为真的情况下，进行登录，并向 SAM 服务器 500 传送登录完成通知（步骤 S94)。收到登录完成通知的 SAM 服务器 500 类似地向个人计算机 300 返回登录完成通知（步骤 S95)。

[0159] 6)http_get（登录确认，会话编号）

[0160] 当收到登录完成通知时，个人计算机 300 把会话编号传送给 Web 服务器 400（步骤 S96)，并确认源自 SAM 服务器 500 的登录已完成。例如，个人计算机 300 利用 http_get 命令传送“https://www.sample_web_server.co.jp/sam_login_cfm.cgi？ session ＝ YYY”，Web 服务器 400 返回登录结果。这导致登录后的画面被显示在个人计算机 300 的屏幕上。因此，用户能够检查他 / 她已登录到的个人计算机 300 的 Web 浏览器画面。

[0161] 图 10 是表示按照第二实施例的个人计算机 300 的结构的功能方框图。如图 10 中所示，个人计算机 300 包括访问目的地信息传输单元 320，标识信息获取单元 322，登录信息传输单元 324，和接收处理单元 326。每个功能块可用设置在个人计算机 300 中的硬件、CPU 308 和使 CPU 308 运行的软件（程序）构成。程序可被保存在设置于个人计算机 300 中的硬盘中，或者保存在诸如在外部与个人计算机 300 连接的存储器之类的记录介质中。

[0162] 如上所述，按照第二实施例，通过使用当在个人计算机 300 的 Web 浏览器上显示 Web 服务器 400 的 URL 时的会话编号，能够使 Web 服务器 400 和 SAM 服务器 500 并行工作。于是，能够在 Web 服务器 400 和 SAM 服务器 500 相互并行工作的状态下，在个人计算机 300 上显示基于会话编码对其进行登录的访问目的地的信息。

[0163] 3. 第三实施例

[0164] 下面，说明本发明的第三实施例。第三实施例涉及作为本地化 (localized) 安全区的虚拟浏览器。

[0165] 图 11 和 12 是示意表示按照第三实施例的系统结构，和信息交换的概念图。本实施例的系统还包括非接触通信卡 100，卡读 / 写器 200，个人计算机 300，Web 服务器 400 和 SAM（安全应用模块）服务器 500。

[0166] 在根据图 11 和 12 描述本实施例的信息交换的概念时，非接触通信卡 100 在其存储器内包括自由区和安全区。诸如 URL 之类的信息被保存在自由区中，诸如用户名和密码

之类的登录信息被保存在安全区中。当使非接触通信卡 100 接触或接近卡读 / 写器 200 时，起动 SAM 服务器 500 的浏览器。此外，借助与 Web 服务器 400 通信的 SAM 服务器 500，其上显示 Web 服务器 400 的 URL 的 SAM 服务器 500 的浏览器（虚拟浏览器）被显示在个人计算机 300 上。

[0167] 在 Web 服务器 400 的 URL 要求诸如用户名和密码之类的登录信息的情况下，SAM 服务器 500 通过加密的通信路径，从非接触通信卡 100 获得登录信息，如图 12 中所示。

[0168] 此外，当 Web 服务器 400 发出本地 (local) 访问请求时，SAM 服务器 500 访问本地信息。此时，SAM 服务器 500 根据用户的选择，访问诸如设置在个人计算机 300 中的硬盘驱动器之类的存储介质，或者非接触通信卡 100 的安全区，并写入或读出高速缓存信息等，如图 12 中所示。这使用户仅仅通过使非接触通信卡 100 接触或接近卡读 / 写器 200，就能够经由 SAM 服务器 500 上的虚拟浏览器访问 Web 服务器 400 的 URL。

[0169] 下面根据图 13-15，详细说明本实施例的系统。按照第三实施例的系统结构和非接触通信卡 100、卡读 / 写器 200、个人计算机 300、Web 服务器 400 和 SAM 服务器 500 的结构与图 2 中的相同。图 13 是表示第三实施例的处理的序列图。

[0170] 1) 非接触通信卡 100 读取

[0171] 首先，个人计算机 300 读取非接触通信卡（步骤 S130-S138）。随后，个人计算机 300 起动 Web 浏览器（步骤 S140）。步骤 S130-S138 的处理和图 3 中的步骤 S10-S20 的处理相同。

[0172] 3) 虚拟浏览器起动

[0173] 个人计算机 300 的 Web 浏览器经由因特网 800 与 SAM 服务器 500 的目的地 URL 连接，并利用 http_get 命令把关于虚拟浏览器的起动请求传送给 SAM 服务器 500（步骤 S142）。这导致在 SAM 服务器 500 运行 Web 浏览器（虚拟浏览器）。之后，虚拟浏览器从 Web 服务器 400 接收的 html 数据被正常传送给个人计算机 300，个人计算机 300 的 Web 浏览器将分析接收的数据，并把接收的数据显示在屏幕上。因此，如图 11 中所示，在个人计算机 300 的显示屏幕上，SAM 服务器 500 的虚拟浏览器被显示在个人计算机 300 的 Web 浏览器上，由 Web 服务器 400 的 URL 指定的信息被显示在虚拟浏览器上。

[0174] 4)Web 访问请求

[0175] 在添加在步骤 S138 中从卡获得的目的地的 URL 信息之后，个人计算机 300 把 Web 访问请求命令传送给 SAM 服务器 500（步骤 S144）。

[0176] 4.1)http_get（起动 URL）

[0177] SAM 服务器 500 把包括接收的 URL 的 http_get 命令传送给 Web 服务器（步骤 S146），并把接收的 http 数据传递给个人计算机 300。这使 Web 服务器 400 的 URL 被显示在个人计算机 300 的显示屏幕上。

[0178] 5) 登录请求

[0179] 这里，当待起动的 Web 服务器 400 显示登录画面时，个人计算机 300 向 SAM 服务器 500 传送登录请求命令（步骤 S148）。

[0180] 5.1) 登录信息（用户名，密码）获取

[0181] 当收到登录请求命令时，SAM 服务器 500 进行获取登录信息的处理（步骤 S150）。利用与关于图 9 说明的第二实施例相似的过程，从非接触通信卡 100 的安全区获得登录信

息。

[0182] 5.2) 登录请求

[0183] SAM 服务器 500 通过利用在步骤 S150 中获得的登录信息，对在步骤 S130-S138 中从非接触通信卡 100 读取的 URL 处 Web 服务器 400 进行登录请求（步骤 S152）。

[0184] 6) 本地访问请求

[0185] 取决于Web服务器400，在登录时，除了登录信息的匹配之外，可以进行对Web服务器400的登录历史和保存在用户的个人计算机300的本地存储介质中的登录历史（登录历史保存在Cookie中）之间的匹配，以进行用户（登录）验证。这种情况下，Web服务器400发出本地（个人计算机300）访问请求（步骤S156）。另外，用户能够从保存在个人计算机300的本地硬盘驱动器（HDD）中的“收藏夹”中选择待显示的URL。从Web服务器400经由SAM服务器500的虚拟浏览器把这些信息通知个人计算机300。另外，本地访问目的地并不局限于上面提及的Cookie和收藏夹，可以是浏览器保存在个人计算机300的本地HDD中的所有信息任意之一，比如历史。

[0186] 6.1) 本地访问处理

[0187] 当收到本地访问请求时，SAM服务器500进行本地访问处理（步骤S158）。本地信息的读取来源/写入目的地可以选自包括在个人计算机300本身中的存储介质，比如硬盘，和具有安全区的外部非接触通信卡100。

[0188] 图14是表示步骤S158的本地访问处理的细节的序列图。

[0189] 1) 本地访问请求

[0190] 首先，SAM服务器500向个人计算机300发出本地访问请求（步骤S170）。

[0191] 2) 用户确认

[0192] 从Web服务器400收到本地访问请求的个人计算机300创建能够访问的存储介质（包括非接触通信卡100）的列表。另外，收到本地访问请求的个人计算机300向用户显示确认画面，所述确认画面显示“允许或拒绝本地访问”。当选择“允许”时，显示用于使用户选择“个人计算机300的本地HDD和非接触通信卡100（安全区）”之一，作为访问目的地的候选者的画面（步骤S172）。随后，用户的访问目的地选择结果被传送给SAM服务器500。参见图14，当在步骤S172中选择HDD时，HDD被设为Web服务器400所请求的本地信息的访问目的地，之后在HDD上进行读取/写入。另外，个人计算机300的本地访问目的地并不局限于HDD，它可以是包含在个人计算机300中的任何存储介质，比如闪速存储器（NVM），或者与个人计算机300连接的任何存储介质。

[0193] 4) 安全客户端起动请求

[0194] 另一方面，当在步骤S172中选择非接触通信卡100时，SAM服务器500向个人计算机300传送安全客户端起动请求命令（步骤S176）。

[0195] 4.1) 安全客户端起动

[0196] 收到安全客户端起动命令的个人计算机300中的CPU 308起动安全客户端（步骤S178）。该客户端程序加密SAM服务器500和个人计算机300之间的通信路径。另外，该客户端程序把从SAM服务器500接收的卡控制命令转换成卡读/写器200的控制命令，并进行非接触通信卡100的卡控制。

[0197] 5) 验证请求（公开信息1）

[0198] 建立加密的通信路径的 SAM 服务器 500 向个人计算机 300 传送验证请求命令（步骤 S182）。该命令包括用随机数 N1 和私有密钥 A 生成的公开信息 1。

[0199] 5.1) 验证请求（公开信息 1）

[0200] 在把验证请求命令转换成卡读 / 写器 200 的验证请求命令之后，个人计算机 300 将其传送给卡读 / 写器 200（步骤 S184）。

[0201] 5.1.1) 验证请求（公开信息 1）

[0202] 在把验证请求命令转换成 RF 信号之后，卡读 / 写器 200 把 RF 信号传送给非接触通信卡 100。私有密钥 A 被保存在非接触通信卡 100 中，从而非接触通信卡 100 利用密钥 A 和随机数 N2 生成公开信息 2，并经个人计算机 300 把公开信息 2 返回给 SAM 服务器 500（步骤 S188）。

[0203] 6)，7) 共用密钥生成

[0204] 根据传输 / 接收的公开信息 1 和 2，非接触通信卡 100 和 SAM 服务器 500 生成对非接触通信卡 100 和 SAM 服务器 500 来说是相同密钥的共用密钥（步骤 S190，S192）。之后，在用该共用密钥加密的情况下，为非接触通信卡 100 的安全设定区所必需的区域的读取值被传送。类似于第一和第二实施例，可用通常称为“Diffie-Hellman 密钥交换”的方法实现共用密钥的生成。

[0205] 8) 写入信息加密（共用密钥）

[0206] 当来自 Web 服务器 400 的对非接触通信卡 100 的访问种类是写入时，SAM 服务器 500 利用共用密钥对写入数据加密（步骤 S194）。

[0207] 9) 安全区 R/W 请求

[0208] SAM 服务器 500 向个人计算机 300 传送对安全区的读取请求或写入请求（步骤 S196）。关于待访问区域（服务区）的信息被包括在对安全区的读取请求或写入请求中。

[0209] 9.1) 安全区读取 / 写入请求

[0210] 个人计算机 300 上的安全客户端把对安全区的读取请求或写入请求转换成卡读 / 写器 200 的命令格式。安全客户端把格式转换后的读取请求或写入请求传送给卡读 / 写器 200（步骤 S198）。

[0211] 9.1.1) 安全区访问

[0212] 卡读 / 写器 200 访问非接触通信卡 100 的安全区（步骤 S200）。对安全区的访问的种类被分成读取或写入。在用共用密钥解密之后，写入信息被写入到适当的服务区。另外，用共用密钥加密从指定的服务区读取的读取信息，并返回给 SAM 服务器 500（步骤 S202）。

[0213] 10) 读取信息解密（共用密钥）

[0214] 当来自 Web 服务器 400 的对非接触通信卡 100 的访问种类是读取时，SAM 服务器 500 用共用密钥对在步骤 S202 中接收的读取数据解密。

[0215] 图 15 是描述在关于图 13 和 14 说明的处理中，SAM 服务器 500 的本地访问处理（步骤 S228 和后面的步骤）的流程图。在根据图 15 说明该处理时，非接触通信卡 100 和卡读 / 写器 200 在步骤 S220 开始通信。随后，在步骤 S222 中起动个人计算机 300 的 Web 浏览器，在下一步骤 S224 中在 Web 浏览器中起动虚拟浏览器。在下一步骤 S226 中从 Web 浏览器发出本地访问请求。

[0216] 在步骤 S228 和后面的步骤中，SAM 服务器 500 进行本地访问处理。在步骤 S228

中，确定用户是否允许对本地信息的访问，当允许所述访问时，处理进入步骤 S230。在步骤 S230 中，用户选择访问目的地。另一方面，当在步骤 S228 中拒绝所述访问时，返回访问失败。

[0217] 当访问目的地是非接触通信卡 100 时，处理进入步骤 S232，使非接触通信卡 100 的安全区成为虚拟本地 HDD。随后，在步骤 S234 中，诸如 Cookie 之类的信息被写入非接触通信卡 100 中。这里的处理对应于图 14 中的步骤 S194-S204。例如，在用户使用位于上网咖啡馆等中的个人计算机 300 的情况下，把个人信息写入个人计算机 300 的 HDD 中并不可取。从而，通过使非接触通信卡 100 成为访问目的地，个人信息能够被写入卡 100 的安全区中。此时，由于在非接触通信卡 100 和 SAM 服务器 500 之间构成加密的传输路径，因此信息能够安全地写入卡 100 中。

[0218] 另一方面，当在步骤 S230 中选择 HDD 时，诸如 Cookie 之类的信息被写入个人计算机 300 的 HDD 中。这里的处理对应于图 14 中的步骤 S174。在步骤 S234 和 S236 之后，处理进入步骤 S238，返回访问信息。

[0219] 图 16 是表示按照第三实施例的个人计算机 300 的结构的功能方框图。如图 16 中所示，个人计算机 300 包括访问目的地信息传输单元 330，登录信息传输单元 332，和接收处理单元 334。每个功能块可用设置在个人计算机 300 中的硬件、CPU 308 和使 CPU 308 运行的软件（程序）构成。程序可被保存在设置于个人计算机 300 中的硬盘中，或者保存在诸如在外部与个人计算机 300 连接的存储器之类的记录介质中。

[0220] 图 17 是表示按照第三实施例的 SAM 服务器 500 的结构的功能方框图。如图 17 中所示，SAM 服务器 500 包括访问目的地信息获取单元 520，登录信息接收单元 522，登录执行单元 524，访问目的地信息传输单元 526，和本地访问单元 528。每个功能块可用设置在 SAM 服务器 500 中的硬件、CPU 502 和使 CPU 502 运行的软件（程序）构成。程序可被保存在设置于 SAM 服务器 500 中的硬盘中，或者保存在诸如在外部与 SAM 服务器 500 连接的存储器之类的记录介质中。

[0221] 如上所述，在第三实施例中，个人计算机 300 基本上具有显示 SAM 服务器 500 的虚拟浏览器的功能，和把用户的选择通知 SAM 服务器 500 的功能。即，在用户查看 SAM 服务器 500 的虚拟浏览器时，个人计算机 300 起中介的作用。当在虚拟浏览器的查看期间，必须读取用户的个人信息或者保存 Cookie 信息等时，能够根据用户的选择，访问个人计算机 300 的存储介质或者非接触通信卡 100 的安全区。

[0222] 应明白对本领域的技术人员来说，对目前优选的实施例的各种变化和修改将是显而易见的。在不脱离本发明的精神和范围，并且不灭失其预期优点的情况下，能够做出这样的变化和修改。于是，这样的变化和修改被附加的权利要求覆盖。

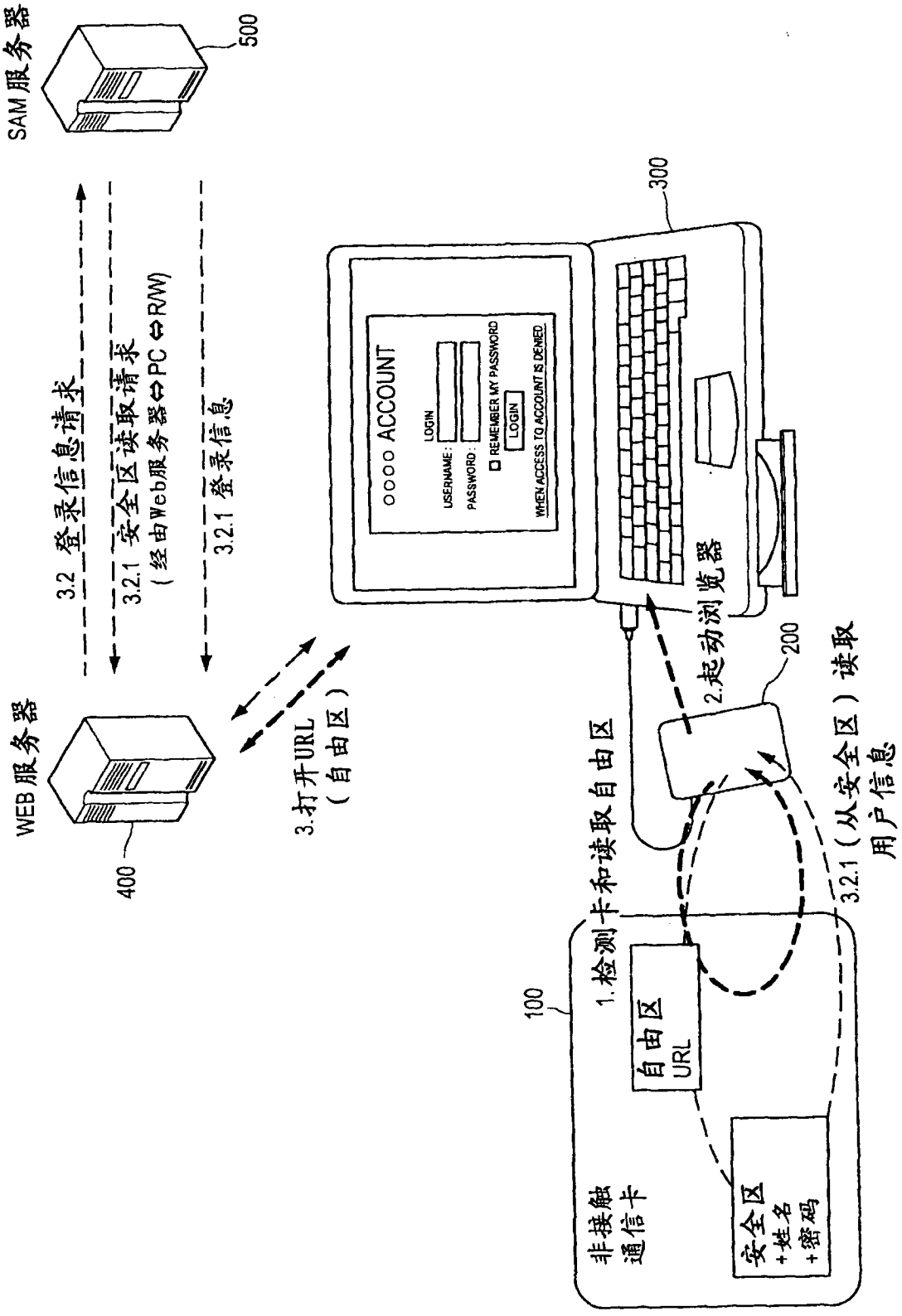

SAM服务器
500
3.2 登录信息请求
3.2.1 安全区读取请求
(经由Web服务器⇔PC ⇔R/W)
3.2.1 登录信息
WEB服务器
400
3.打开URL
(自由区)
300
OOOO ACCOUNT
LOGIN
USERNAME:
PASSWORD:
REMEMBER MY PASSWORD
LOGIN
WHEN ACCESS TO ACCOUNT IS DENIED
2.起动浏览器
200
1.检测卡和读取自由区
3.2.1(从安全区)读取
用户信息
100
自由区
URL
非接触
通信卡
安全区
+姓名
+密码

图 1

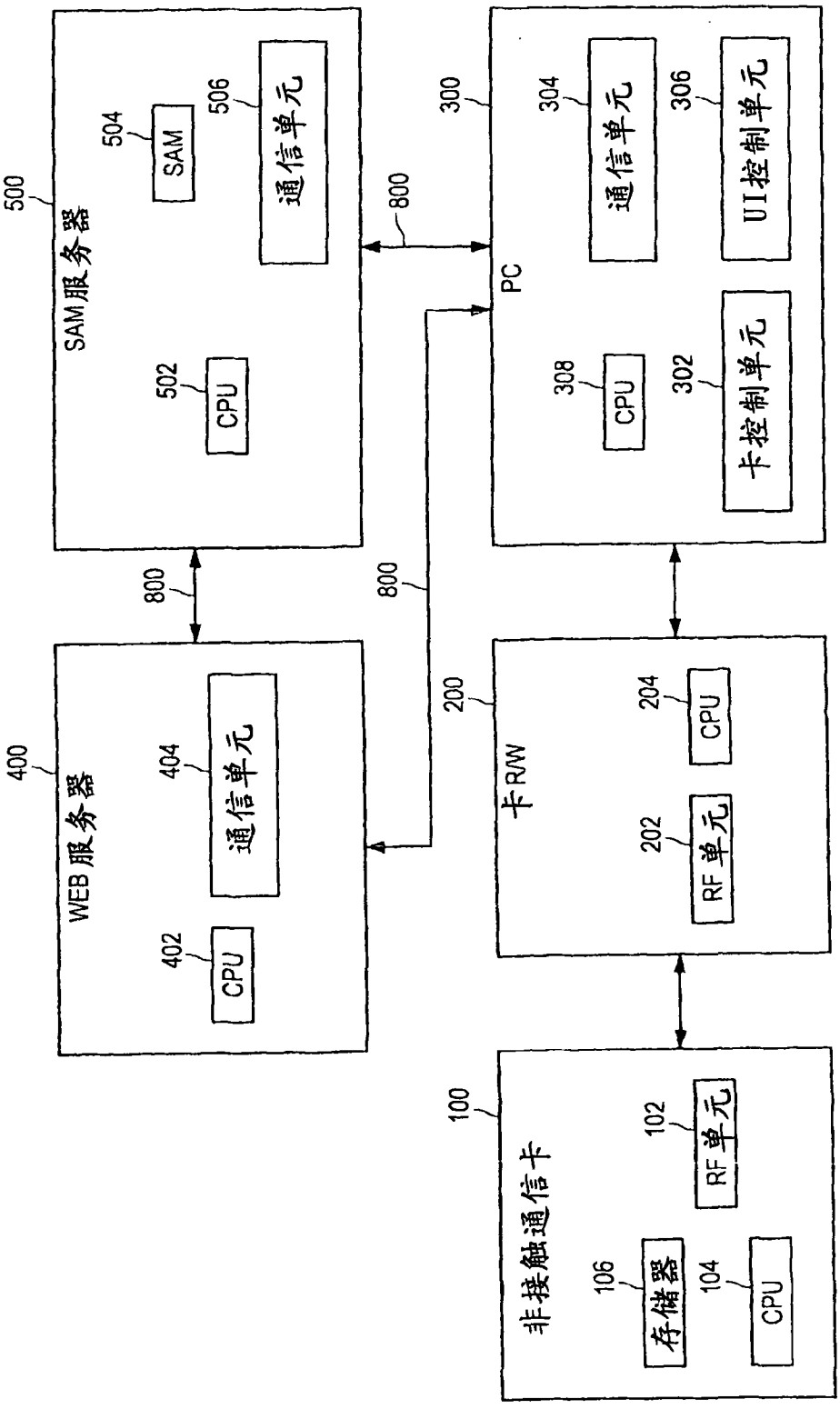

500
SAM服务器
504
SAM
506
通信单元
502
CPU
800
300
PC
304
通信单元
306
UI控制单元
308
CPU
302
卡控制单元
800
800
400
WEB服务器
404
通信单元
402
CPU
200
卡R/W
204
CPU
202
RF单元
100
非接触通信卡
102
RF单元
106
存储器
104
CPU

图 2

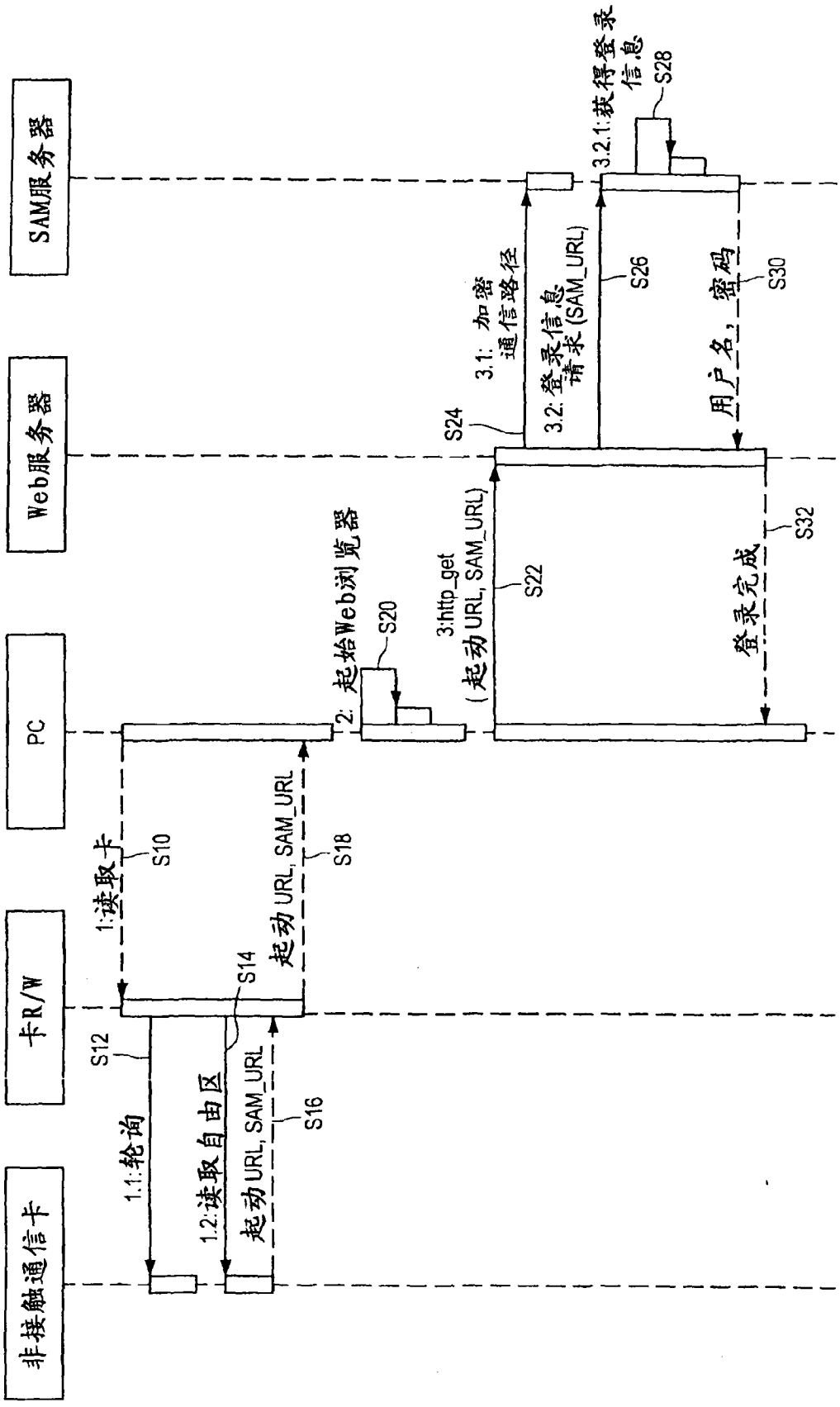

非接触通信卡
卡R/W
PC
Web服务器
SAM服务器
1.1:轮询
1.2:读取自由区
1:读取卡
起动URL, SAM_URL
起动URL, SAM_URL
2: 起始Web浏览器
3:http_get
(起动URL, SAM_URL)
3.1: 加密通信路径
3.2: 登录信息请求(SAM_URL)
3.2.1:获得登录信息
用户名，密码
登录完成
S10
S12
S14
S16
S18
S20
S22
S24
S26
S28
S30
S32

图 3

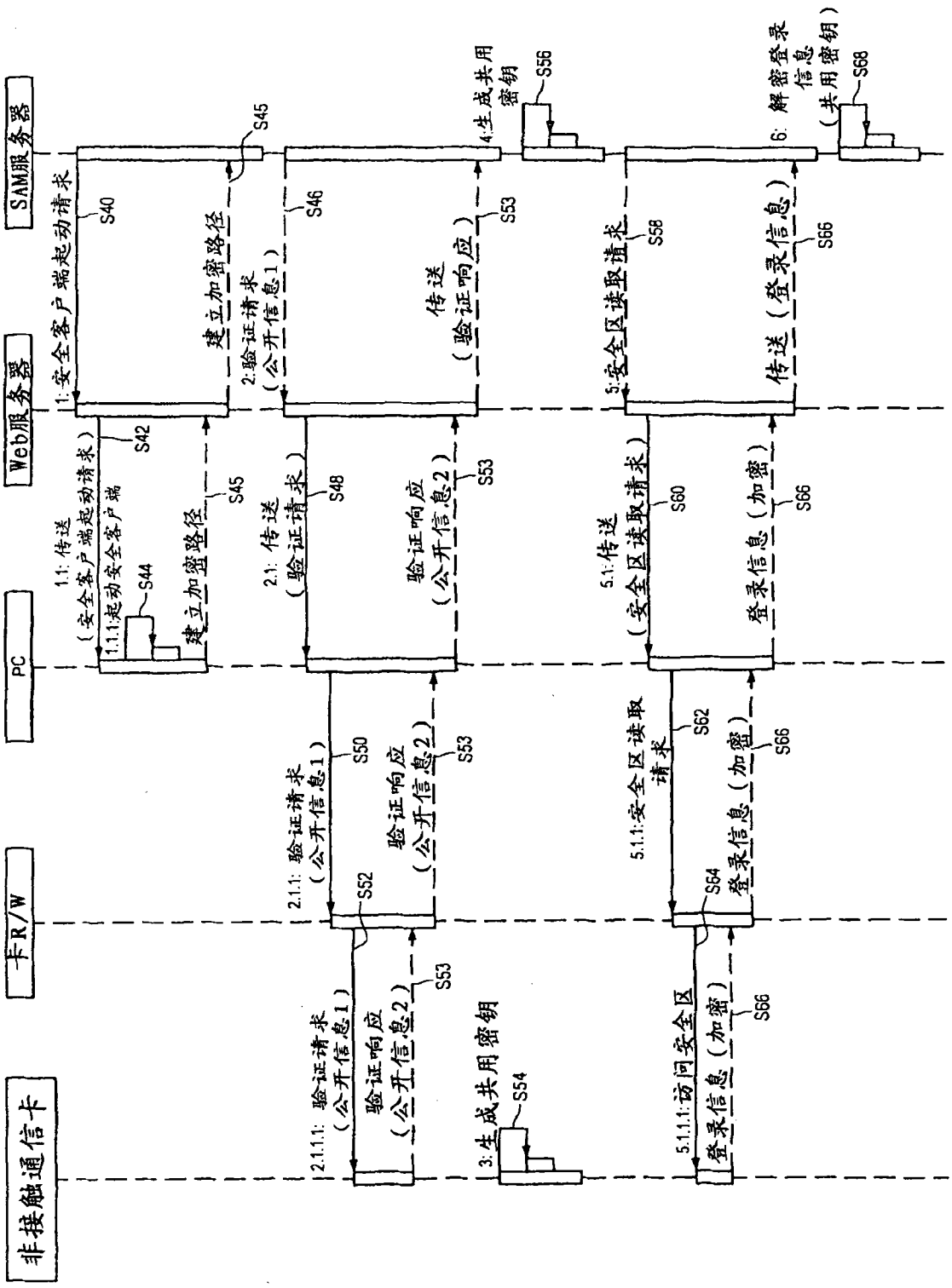

非接触通信卡
卡R/W
PC
Web服务器
SAM服务器
1:安全客户端起动请求
S40
1.1: 传送
（安全客户端起动请求）
S42
1.1.1:起动安全客户端
S44
建立加密路径
S45
建立加密路径
S45
2:验证请求
（公开信息1）
S46
2.1: 传送
（验证请求）
S48
2.1.1: 验证请求
（公开信息1）
S50
S52
2.1.1.1: 验证请求
（公开信息1）
验证响应
（公开信息2）
S53
验证响应
（公开信息2）
S53
传送
（验证响应）
S53
3:生成共用密钥
S54
4:生成共用密钥
S56
5:安全区读取请求
S58
5.1:传送
（安全区读取请求）
S60
5.1.1:安全区读取请求
S62
S64
5.1.1.1:访问安全区
登录信息（加密）
S66
登录信息（加密）
S66
传送（登录信息）
S66
6: 解密登录信息（共用密钥）
S68

图 4

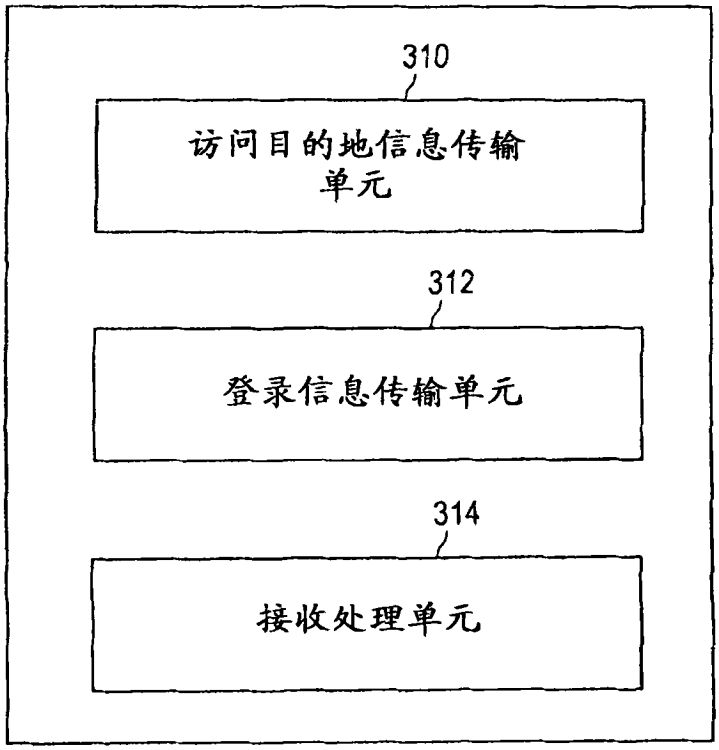


图 5

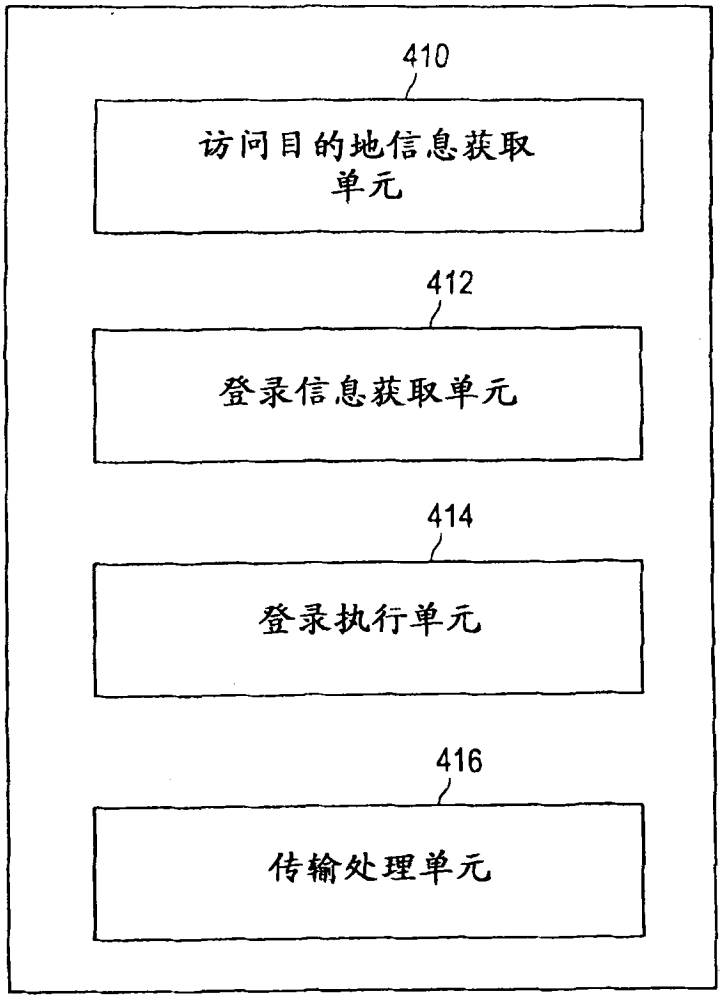


图 6

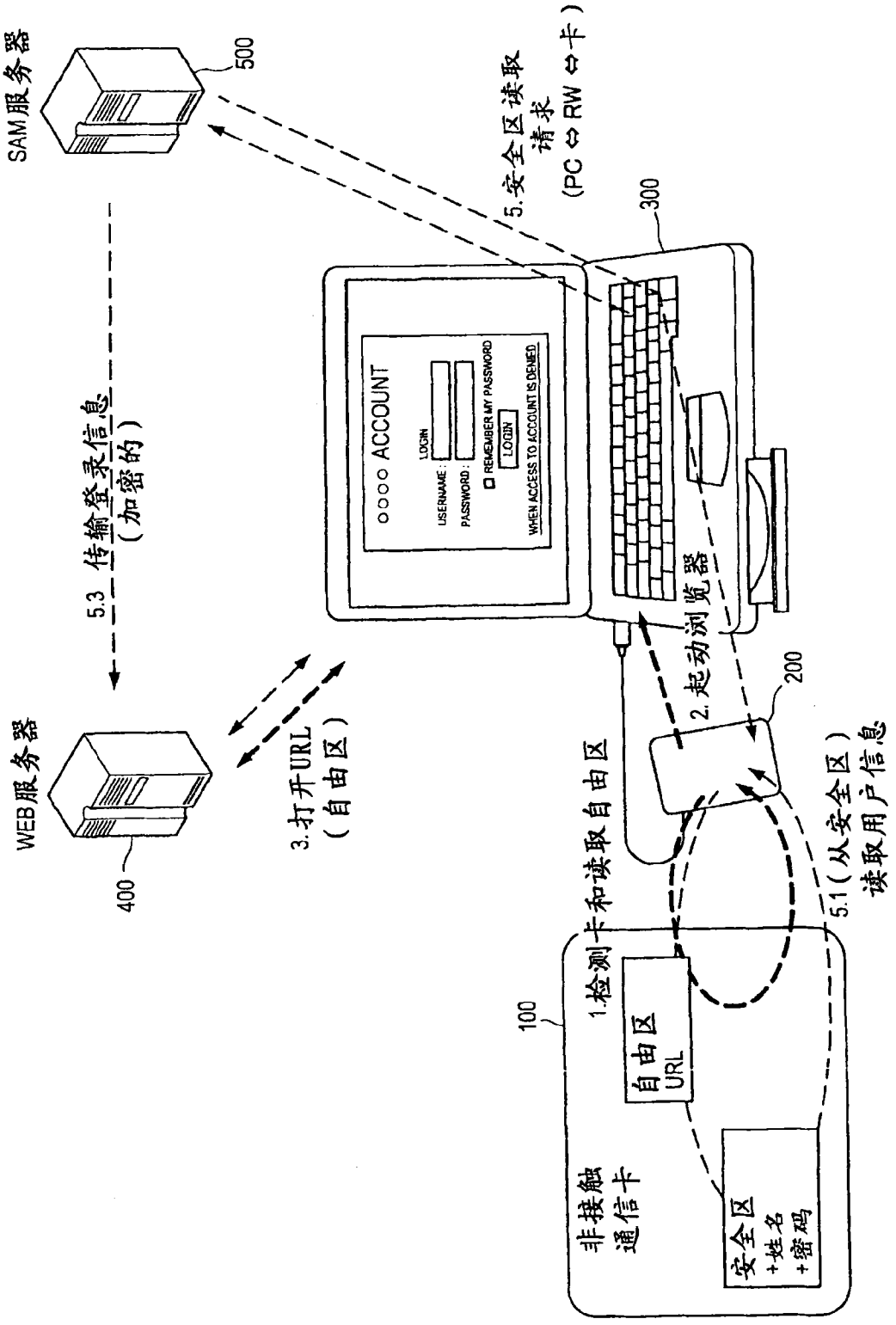

SAM服务器
500
5.安全区读取
请求
(PC ⇔ RW ⇔卡)
300
5.3 传输登录信息
(加密的)
ACCOUNT
LOGIN
USERNAME:
PASSWORD:
REMEMBER MY PASSWORD
LOGIN
WHEN ACCESS TO ACCOUNT IS DENIED
WEB服务器
400
3.打开URL
(自由区)
2.起动浏览器
200
1.检测卡和读取自由区
5.1(从安全区)
读取用户信息
100
自由区
URL
非接触
通信卡
安全区
+姓名
+密码

图 7

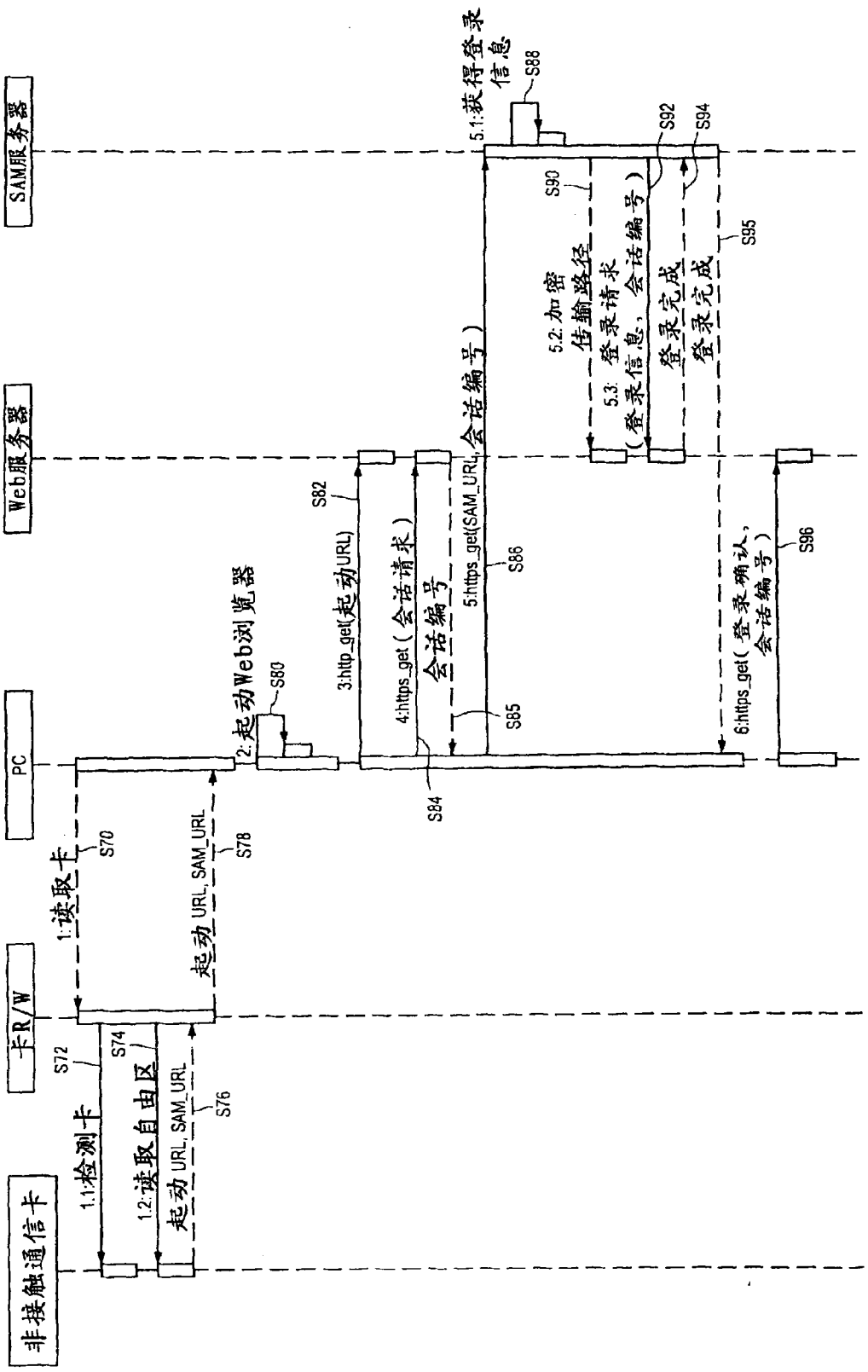

非接触通信卡
卡R/W
PC
Web服务器
SAM服务器
1:读取卡
S70
1.1:检测卡
S72
1.2:读取自由区
S74
起动 URL, SAM_URL
S76
起动 URL, SAM_URL
S78
2:起动Web浏览器
S80
3:http_get(起动URL)
S82
4:https_get(会话请求)
会话编号
S84
5:https_get(SAM_URL, 会话编号)
S85
S86
5.1:获得登录信息
S88
S90
5.2:加密传输路径
5.3:登录请求(登录信息, 会话编号)
S92
登录完成
S94
登录完成
S95
6:https_get(登录确认, 会话编号)
S96

图 8

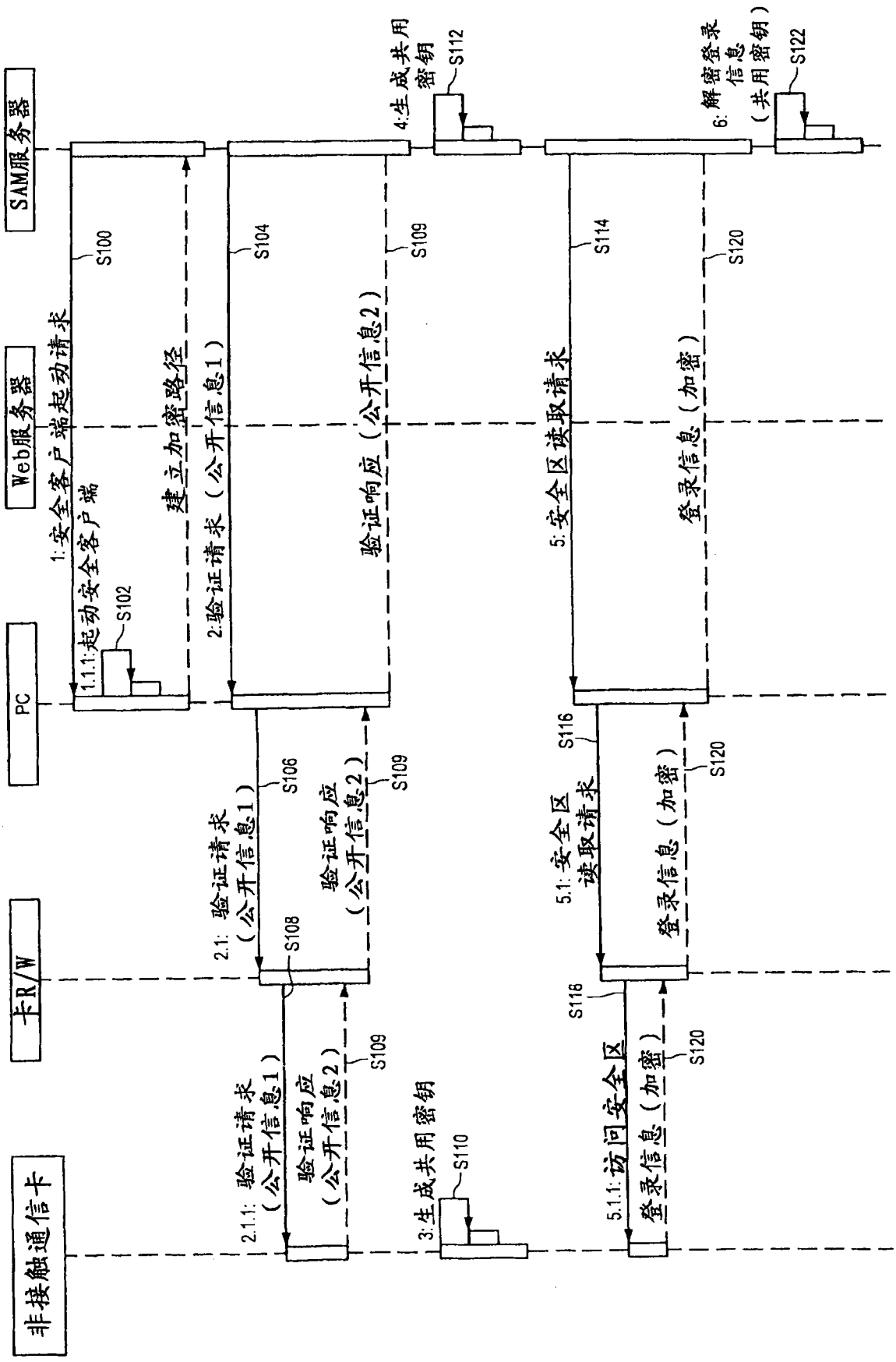

SAM服务器
Web服务器
PC
卡R/W
非接触通信卡
1:安全客户端起动请求
1.1.1:起动安全客户端
S100
S102
建立加密路径
2:验证请求（公开信息1）
S104
2.1: 验证请求（公开信息1）
S106
2.1.1: 验证请求（公开信息1）
S108
验证响应（公开信息2）
S109
4:生成共用密钥
S112
3:生成共用密钥
S110
验证响应（公开信息2）
S109
验证响应（公开信息2）
S109
5: 安全区读取请求
S114
5.1: 安全区读取请求
S116
5.1.1: 访问安全区
S118
登录信息（加密）
S120
登录信息（加密）
S120
登录信息（加密）
S120
6: 解密登录信息（共用密钥）
S122

图 9

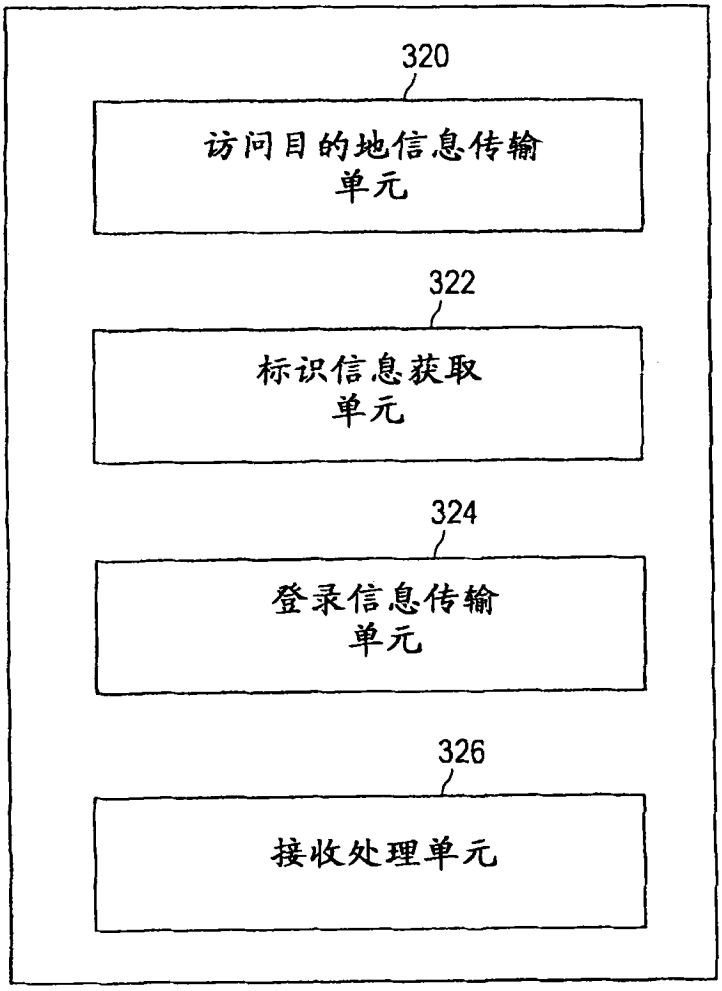


图 10

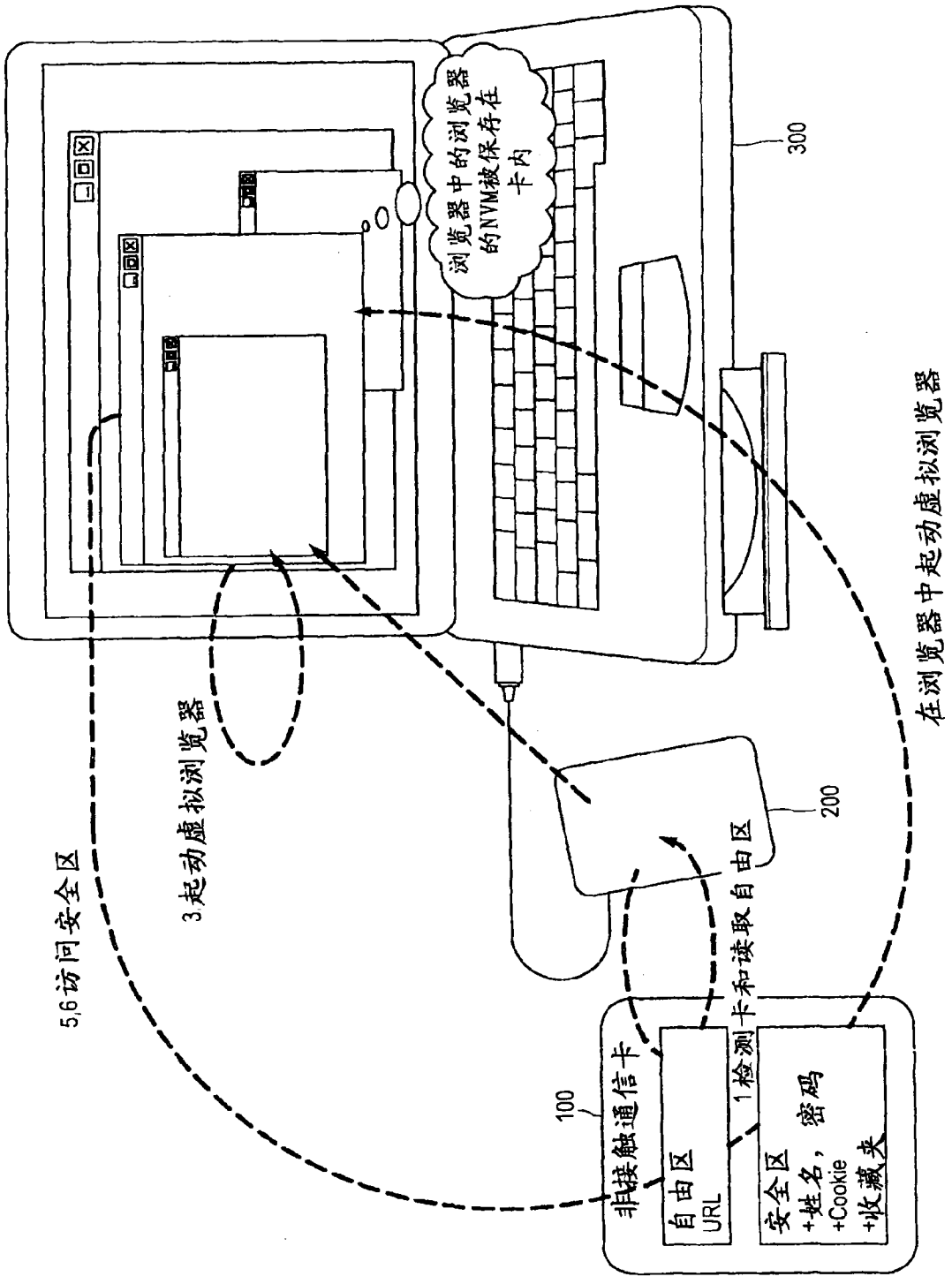

浏览器中的浏览器的NVM被保存在卡内
300
3.起动虚拟浏览器
5,6访问安全区
在浏览器中起动虚拟浏览器
200
100
非接触通信卡
自由区
URL
1检测卡和读取自由区
安全区
+姓名，密码
+Cookie
+收藏夹

图 11

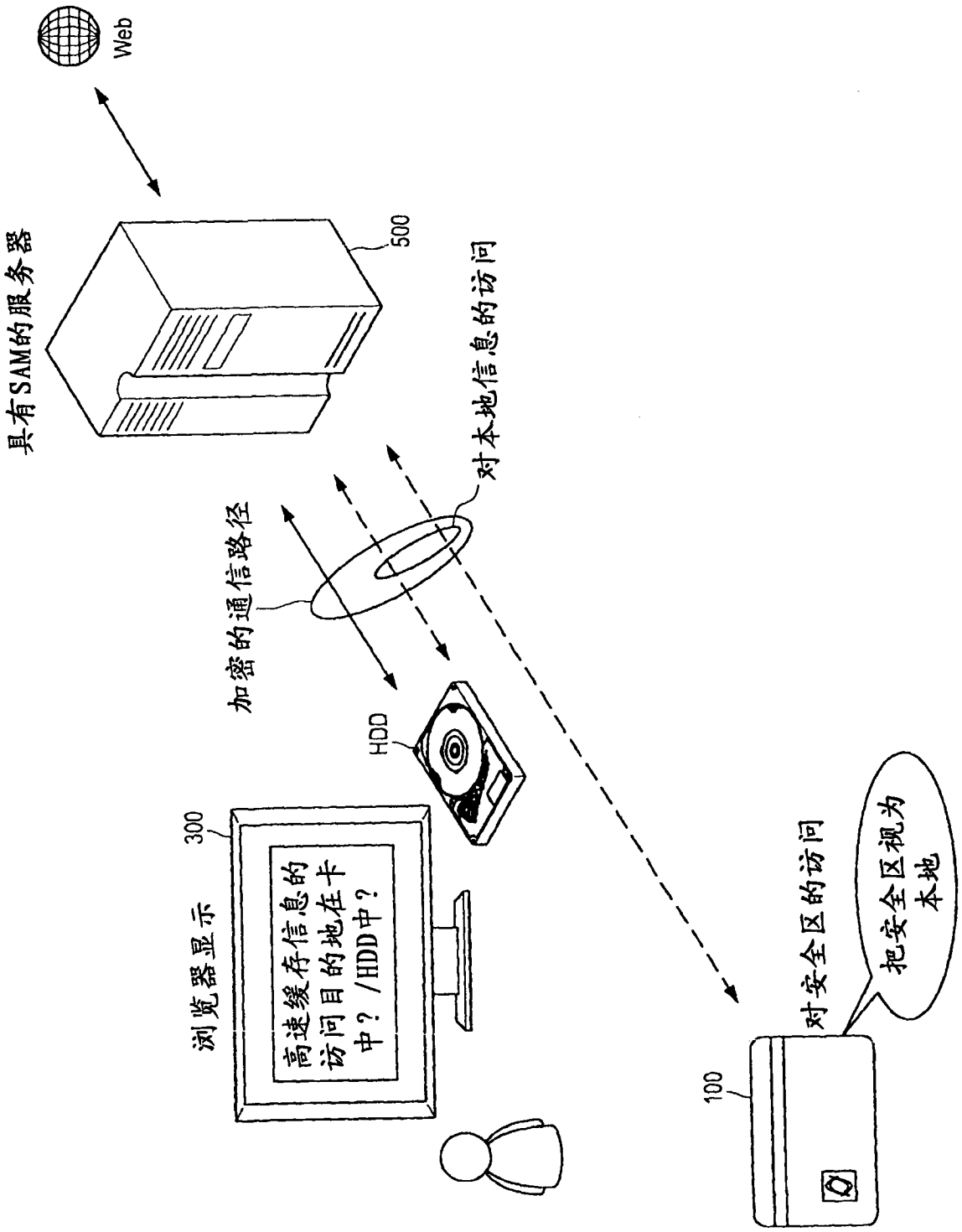

Web
具有SAM的服务器
500
对本地信息的访问
加密的通信路径
HDD
300
浏览器显示
高速缓存信息的访问目的地在卡中？/HDD中？
对安全区的访问
把安全区视为本地
100

图 12

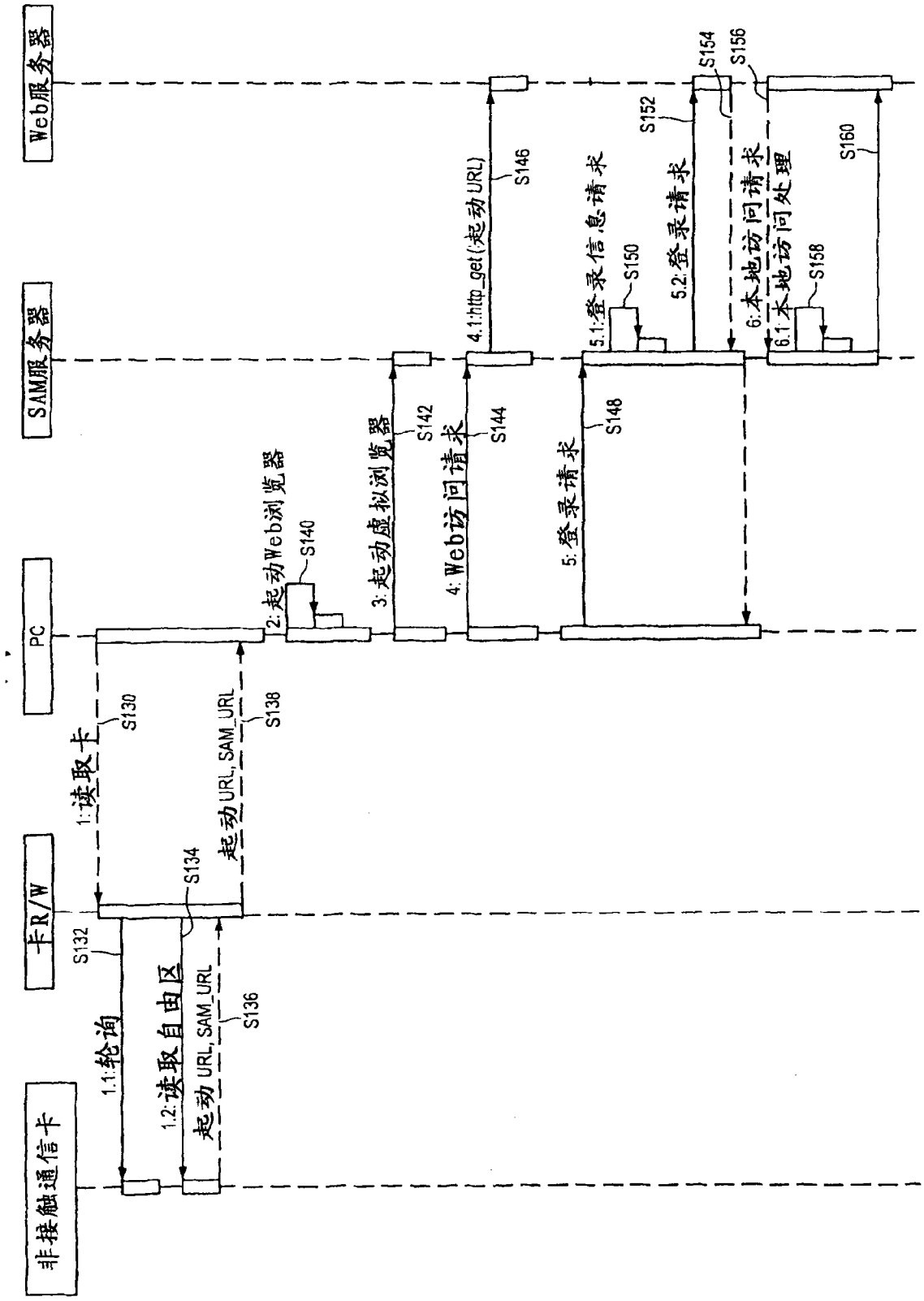

非接触通信卡
卡R/W
PC
SAM服务器
Web服务器
1.1:轮询
S132
1.2:读取自由区
S134
起动URL,SAM_URL
S136
1:读取卡
S130
起动URL,SAM_URL
S138
2:起动Web浏览器
S140
3:起动虚拟浏览器
S142
4:Web访问请求
S144
4.1:http_get(起动URL)
S146
5:登录请求
S148
5.1:登录信息请求
S150
5.2:登录请求
S152
S154
6:本地访问请求
S156
6.1:本地访问处理
S158
S160

图 13

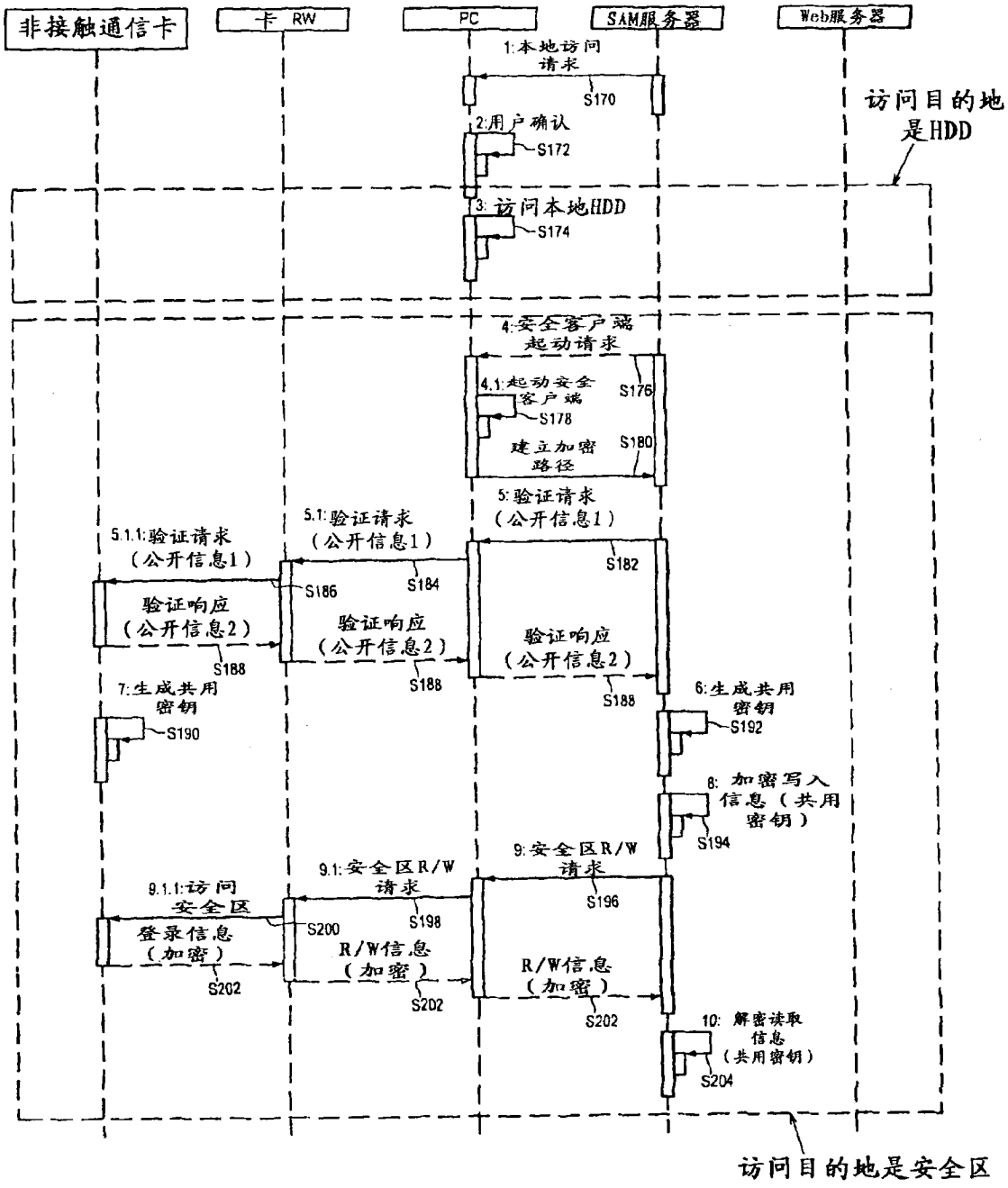

非接触通信卡
卡 RW
PC
SAM服务器
Web服务器
1:本地访问请求
S170
2:用户确认
S172
访问目的地是HDD
3: 访问本地HDD
S174
4:安全客户端起动请求
4.1:起动安全客户端
S176
S178
建立加密路径
S180
5:验证请求（公开信息1）
S182
5.1:验证请求（公开信息1）
S184
5.1.1:验证请求（公开信息1）
S186
验证响应（公开信息2）
S188
验证响应（公开信息2）
S188
验证响应（公开信息2）
S188
6:生成共用密钥
S192
7:生成共用密钥
S190
8: 加密写入信息（共用密钥）
S194
9:安全区R/W请求
S196
9.1:安全区R/W请求
S198
9.1.1:访问安全区
S200
登录信息（加密）
S202
R/W信息（加密）
S202
R/W信息（加密）
S202
10: 解密读取信息（共用密钥）
S204
访问目的地是安全区

图 14

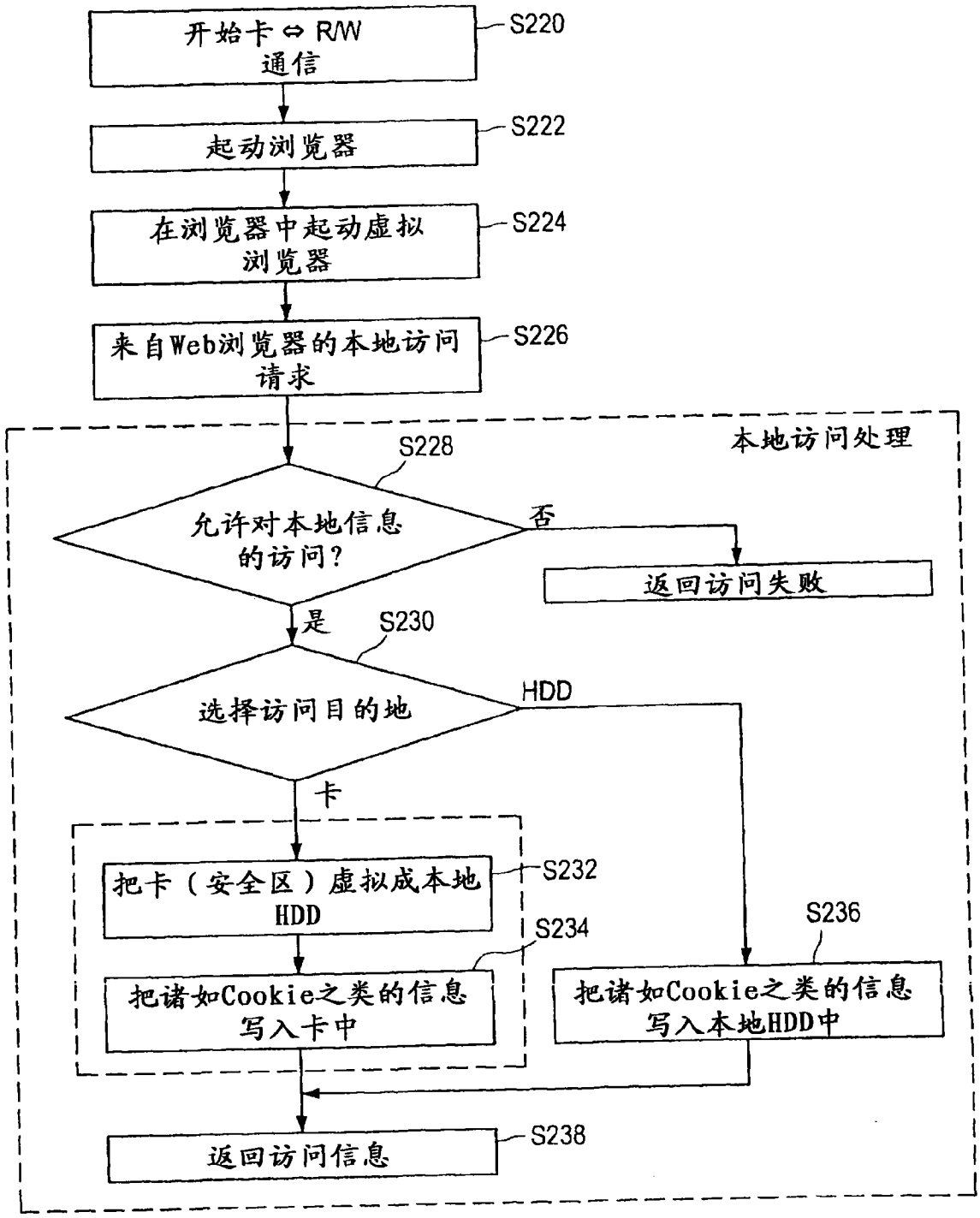

开始卡 ⇔ R/W 通信
S220
起动浏览器
S222
在浏览器中起动虚拟浏览器
S224
来自Web浏览器的本地访问请求
S226
本地访问处理
S228
允许对本地信息的访问?
否
返回访问失败
是
S230
选择访问目的地
HDD
卡
把卡（安全区）虚拟成本地HDD
S232
S234
把诸如Cookie之类的信息写入卡中
S236
把诸如Cookie之类的信息写入本地HDD中
返回访问信息
S238

图 15

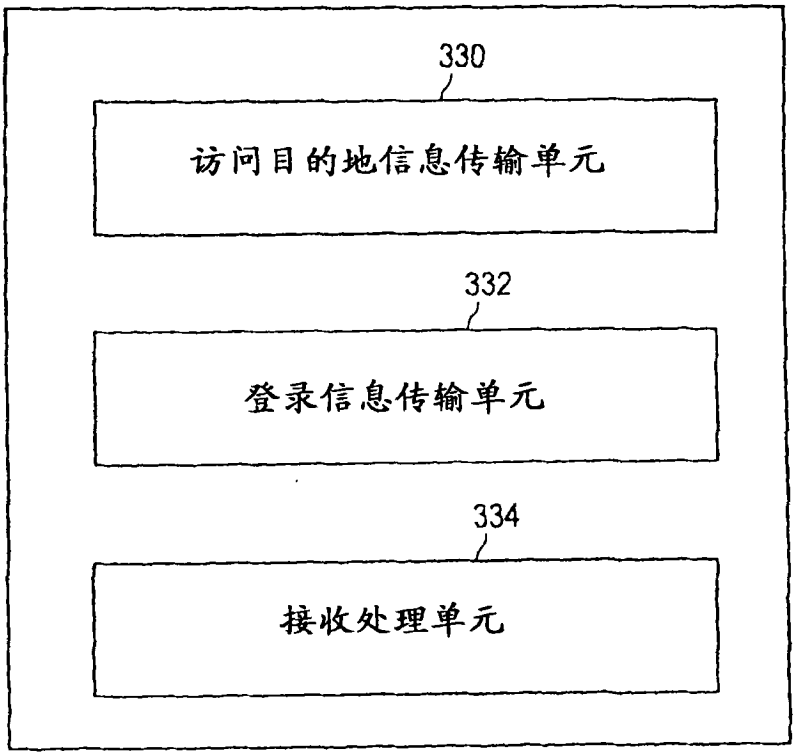


图 16

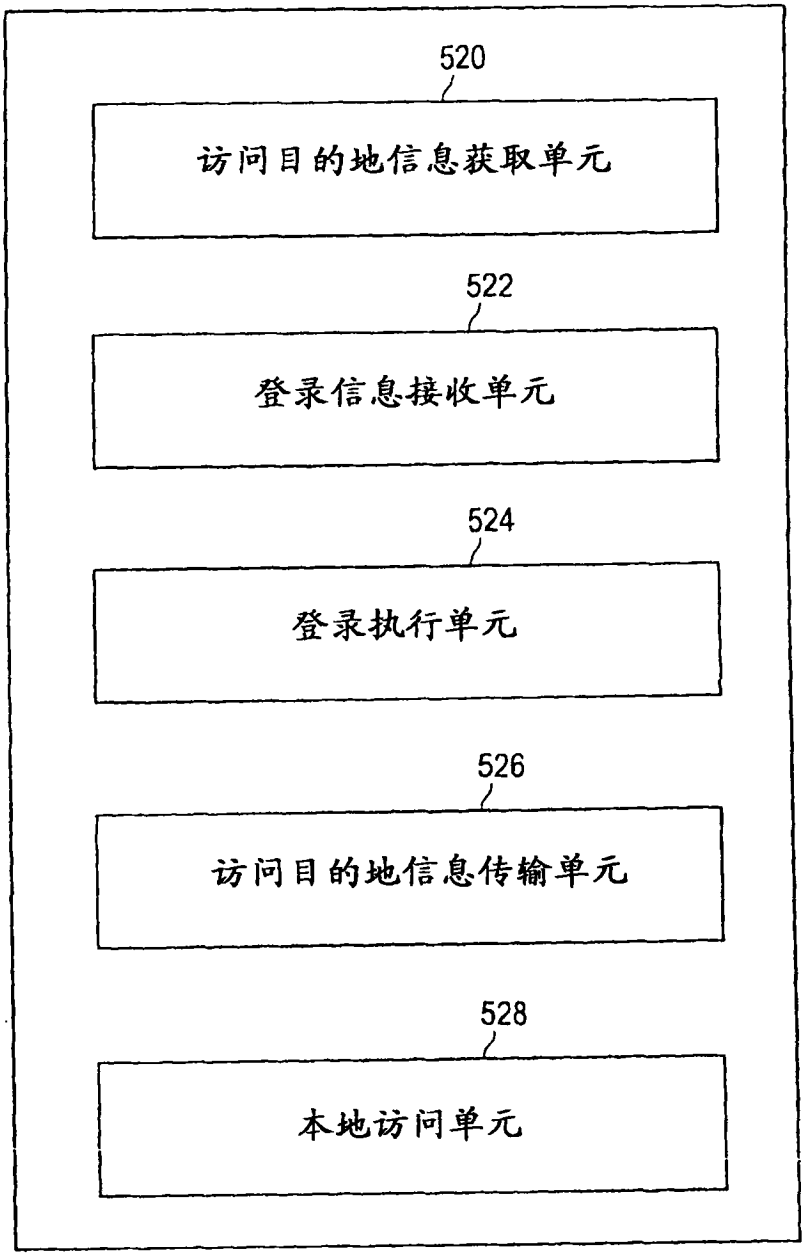

520
访问目的地信息获取单元
522
登录信息接收单元
524
登录执行单元
526
访问目的地信息传输单元
528
本地访问单元
500

图 17