

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.  
G06F 21/20 (2006.01)  
H04L 9/32 (2006.01)



# [12] 发明专利说明书

专利号 ZL 200680005905.1

[45] 授权公告日 2009年9月30日

[11] 授权公告号 CN 100545852C

[22] 申请日 2006.11.28

[21] 申请号 200680005905.1

[30] 优先权

[32] 2005.12.9 [33] JP [31] 356336/2005

[86] 国际申请 PCT/JP2006/323728 2006.11.28

[87] 国际公布 WO2007/066542 日 2007.6.14

[85] 进入国家阶段日期 2007.8.23

[73] 专利权人 日立软件株式会社

地址 日本神奈川县

[72] 发明人 石田夏树

[56] 参考文献

CN 1427609A 2003.7.2

CN 1329418A 2002.1.2

JP2003-30146A 2003.1.31

JP2001-184310A 2001.7.6

JP2002-259344A 2002.9.13

审查员 沈乐平

[74] 专利代理机构 北京银龙知识产权代理有限公司

代理人 许静

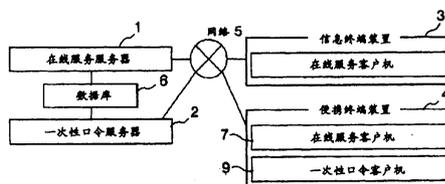
权利要求书6页 说明书24页 附图4页

[54] 发明名称

认证系统以及认证方法

[57] 摘要

本发明的目的是谋求：提高利用一次性口令的认证系统的安全性，或者使从利用固定口令的认证系统容易迁移容易，或者扩大使用范围。一种一次性口令与时间同步的认证系统或者一次性口令与在线服务认证请求的次数同步的认证系统，在一次性口令客户机9从一次性口令服务器2下载在线服务认证用一次性口令时，在客户机服务器之间使现在的时刻信息或者在线服务认证请求次数的现在值一致，仅在被下载的在线服务认证用一次性口令有效期间，认证在线服务认证请求。也能够使一次性口令与在在线服务认证请求中包含的服务利用内容同步。



1. 一种认证系统，其为通过网络连接在线服务服务器和一次性口令服务器和在线服务客户机和一次性口令客户机、且在数据库上连接在线服务服务器和一次性口令服务器构成的客户机服务器系统中的认证系统，其特征在于，

认证系统的初始状态，是在所述数据库中存储的在线服务认证用口令中设定了在线服务认证用固定口令的状态；

所述一次性口令服务器，在认证来自所述一次性口令客户机的初始化请求后在在所述数据库中存储的在线服务认证用口令中设定伪一次性口令，同时，在认证在线服务认证用一次性口令下载请求后，在在所述数据库中存储的在线服务认证用口令中设定在线服务认证用一次性口令；

所述一次性口令服务器和所述一次性口令客户机共有用于获得所述在线服务认证用一次性口令的共有秘密信息；

所述一次性口令客户机通过所述共有秘密信息与所述一次性口令服务器共有所述在线服务认证用一次性口令；

所述在线服务服务器，通过在所述数据库中存储的在线服务认证用口令认证从所述在线服务客户机接收到的在线服务认证请求；

所述在线服务服务器或者所述一次性口令服务器，在认证在线服务认证用一次性口令下载请求后，在不把和一次性口令客户机共有的在线服务认证用一次性口令作为在线服务认证请求的认证条件的场合，在在所述数据库中存储的在线服务认证用口令中设定伪一次性口令。

2. 一种认证系统，其为通过网络连接在线服务服务器和一次性口令服务器和在线服务客户机和一次性口令客户机构成的客户机服务器系统中的认证系统，其特征在于，

所述一次性口令服务器和所述一次性口令客户机共有用于获得在线服务认证用一次性口令的共有秘密信息；

所述一次性口令服务器，在认证在线服务认证用一次性口令下载请求后，和所述一次性口令客户机共有多个在线服务认证用一次性口令；

所述一次性口令客户机，在和所述一次性口令服务器共有在线服务认证

用一次性口令后,以一定时间间隔顺序显示成为显示对象的多个在线服务认证用一次性口令的任何一个;

所述在线服务服务器,对从所述在线服务客户机接收到的在线服务认证请求,如果在共有在线服务认证用一次性口令后经过一定时间后则作为认证失败,在共有在线服务认证用一次性口令后以一定时间间隔顺序通过成为认证条件的多个在线服务认证用一次性口令的任何一个来进行认证。

3. 一种认证系统,其为通过网络连接在线服务服务器和一次性口令服务器和在线服务客户机和一次性口令客户机构成的客户机服务器系统中的认证系统,其特征在于,

所述一次性口令服务器和所述一次性口令客户机共有用于获得在线服务认证用一次性口令的共有秘密信息;

所述一次性口令服务器,在认证在线服务认证用一次性口令下载请求后,和所述一次性口令客户机共有多个在线服务认证用一次性口令;

所述一次性口令客户机,显示在线服务认证请求次数和在线服务认证用一次性口令的组;

所述在线服务服务器,对从所述在线服务客户机接收到的在线服务认证请求,如果在共有在线服务认证用一次性口令以后的在线服务认证请求次数超过了共有的在线服务认证用一次性口令的个数则作为认证失败,通过和在共有在线服务认证用一次性口令以后的在线服务认证请求次数成组的在线服务认证用一次性口令来进行认证。

4. 根据权利要求2或3所述的认证系统,其特征在于,所述在线服务服务器,用字符数是在线服务认证用一次性口令强度的现在值的在线服务认证用一次性口令,认证从在线服务客户机接收到的在线服务认证请求,如果认证失败则增大在线服务认证用一次性口令强度的现在值。

5. 一种认证系统,其为通过网络连接在线服务服务器和一次性口令服务器和在线服务客户机、且由在线服务服务器和一次性口令服务器和在线服务客户机和一次性口令客户机构成的客户机服务器系统中的认证系统,其特征在于,

所述一次性口令服务器和所述一次性口令客户机共有用于获得在线服务

认证用一次性口令的共有秘密信息;

所述一次性口令客户机通过所述共有秘密信息与所述一次性口令服务器共有所述在线服务认证用一次性口令;

所述一次性口令服务器,对于包含从在线服务客户机接收到的服务利用内容的在线服务认证准备请求,和所述一次性口令客户机共有服务利用内容以及用于用所述共有秘密信息认证服务利用内容的信息以及用于用所述共有秘密信息计算在线服务认证用一次性口令的信息;

所述一次性口令客户机,对于用于用共有秘密信息认证服务利用内容的信息如果通过共有秘密信息认证成功,则对于用于通过共有秘密信息计算在线服务认证用一次性口令的信息用所述共有秘密信息计算在线服务认证用一次性口令,显示服务利用内容和在线服务认证用一次性口令;

所述在线服务服务器,通过在线服务认证用一次性口令认证从所述在线服务客户机接收到的在线服务认证请求。

6. 一种认证系统,其为通过网络连接在线服务服务器和一次性口令服务器和在线服务客户机、且由在线服务服务器和一次性口令服务器和在线服务客户机和一次性口令客户机构成的客户机服务器系统中的认证系统,其特征在于,

所述一次性口令服务器,对于包含从在线服务客户机接收到的服务利用内容的在线服务认证准备请求,存储服务利用内容;

所述一次性口令服务器和所述一次性口令客户机共有用于获得在线服务认证用一次性口令的共有秘密信息;

所述一次性口令客户机通过所述共有秘密信息与所述一次性口令服务器共有所述在线服务认证用一次性口令;

所述一次性口令服务器,在认证在线服务认证用一次性口令下载请求后和所述一次性口令客户机共有加密服务利用内容和在线服务认证用一次性口令的组的共同密钥;

所述一次性口令客户机,通过所述共同密钥解密服务利用内容和在线服务认证用一次性口令的组后并进行显示;

所述在线服务服务器,通过在线服务认证用一次性口令认证从所述在线

服务客户机接收到的在线服务认证请求。

7. 根据权利要求 5 或者 6 所述的认证系统，其特征在于，

所述一次性口令服务器，对于包含从所述在线服务客户机接收到的服务利用内容的在线服务认证准备请求，把在线服务认证用一次性口令的字符数作为在线服务认证用一次性口令强度的现在值，增大在线服务认证用一次性口令的强度的现在值；

所述在线服务服务器，如果从所述在线服务客户机接收到的在线服务请求的认证成功，则减小在线服务认证用一次性口令强度的现在值。

8. 根据权利要求 6 所述的认证系统，其特征在于，

所述在线服务服务器，从所述一次性口令服务器接收加密过的所述服务利用内容和在线服务认证用一次性口令的组，编码为 QR 代码后向所述在线服务客户机发送；

所述在线服务客户机，显示所述 QR 代码；

所述一次性口令客户机，输入所述 QR 代码并解码后通过所述共同密钥进行解密。

9. 一种 认证方法，其为通过网络连接在线服务服务器和一次性口令服务器和在线服务客户机和一次性口令客户机、且在数据库上连接在线服务服务器和一次性口令服务器构成的客户机服务器系统中的认证方法，其特征在于，

认证系统的初始状态，是在在所述数据库中存储的在线服务认证用口令中设定了在线服务认证用固定口令的状态；

所述一次性口令服务器，在认证来自所述一次性口令客户机的初始化请求后，在在所述数据库中存储的在线服务认证用口令中设定伪一次性口令，同时，在认证在线服务认证用一次性口令下载请求后，在在所述数据库中存储的在线服务认证用口令中设定在线服务认证用一次性口令；

所述在线服务服务器，通过在所述数据库中存储的在线服务认证用口令认证从所述在线服务客户机接收到的在线服务认证请求；

所述在线服务服务器或者所述一次性口令服务器，在认证在线服务认证用一次性口令下载请求后，在不把和一次性口令客户机共有的在线服务认证用一次性口令作为在线服务认证请求的认证条件的场合，在在所述数据库中存储

的在线服务认证用口令中设定伪一次性口令。

10. 一种认证方法, 其为通过网络连接在线服务服务器和一次性口令服务器和在线服务客户机和一次性口令客户机构成的客户机服务器系统中的认证方法, 其特征在于,

所述一次性口令服务器和所述一次性口令客户机共有用于获得在线服务认证用一次性口令的共有秘密信息;

所述一次性口令服务器, 在认证在线服务认证用一次性口令下载请求后, 和所述一次性口令客户机共有多个在线服务认证用一次性口令;

所述一次性口令客户机, 在和所述一次性口令服务器共有在线服务认证用一次性口令后, 以一定时间间隔顺序显示成为显示对象的多个在线服务认证用一次性口令的任何一个;

所述在线服务服务器, 对从所述在线服务客户机接收到的在线服务认证请求, 如果在共有在线服务认证用一次性口令后经过一定时间后则作为认证失败, 在共有在线服务认证用一次性口令后以一定时间间隔顺序通过成为认证条件的多个在线服务认证用一次性口令的任何一个来进行认证。

11. 一种认证方法, 其为通过网络连接在线服务服务器和一次性口令服务器和在线服务客户机和一次性口令客户机构成的客户机服务器系统中的认证方法, 其特征在于,

所述一次性口令服务器和所述一次性口令客户机共有用于获得在线服务认证用一次性口令的共有秘密信息;

所述一次性口令服务器, 在认证在线服务认证用一次性口令下载请求后和所述一次性口令客户机共有多个在线服务认证用一次性口令;

所述一次性口令客户机, 显示在线服务认证请求次数和在线服务认证用一次性口令的组;

所述在线服务服务器, 对从所述在线服务客户机接收到的在线服务认证请求, 如果在共有在线服务认证用一次性口令以后的在线服务认证请求次数超过共有的在线服务认证用一次性口令的个数则作为认证失败, 通过和在共有在线服务认证用一次性口令以后的在线服务认证请求次数成组的在线服务认证用一次性口令来进行认证。

12. 一种认证方法, 其为通过网络连接在线服务服务器和一次性口令服务器和在线服务客户机、且由在线服务服务器和一次性口令服务器和在线服务客户机和一次性口令客户机构成的客户机服务器系统中的认证方法, 其特征在于,

所述一次性口令服务器, 对于包含从在线服务客户机接收到的服务利用内容的在线服务认证准备请求, 存储服务利用内容;

所述一次性口令服务器和所述一次性口令客户机共有用于获得在线服务认证用一次性口令的共有秘密信息;

所述一次性口令客户机通过所述共有秘密信息与所述一次性口令服务器共有所述在线服务认证用一次性口令;

所述一次性口令服务器, 在认证在线服务认证用一次性口令下载请求后, 和所述一次性口令客户机共有加密服务利用内容和在线服务认证用一次性口令的组的共同密钥;

所述一次性口令客户机, 通过所述共同密钥解密服务利用内容和在线服务认证用一次性口令的组后进行显示;

所述在线服务服务器, 通过在线服务认证用一次性口令认证从所述在线服务客户机接收到的在线服务认证请求。

13. 根据权利要求 12 所述的认证方法, 其特征在于,

所述在线服务服务器, 从所述一次性口令服务器接收加密过的所述服务利用内容和在线服务认证用一次性口令的组, 编码为 QR 代码后向所述在线服务客户机发送;

所述在线服务客户机, 显示所述 QR 代码;

所述一次性口令客户机, 输入所述 QR 代码并解码后通过所述共同密钥解密。

## 认证系统以及认证方法

## 技术领域

本发明涉及认证系统以及认证方法，特别涉及在客户机服务器系统中的客户机的认证以及邮件的认证中使用的合适的认证系统以及认证方法。

## 背景技术

作为进行客户机服务器系统中的客户机的认证的技术，公知使用固定口令的认证系统。

图 1 是表示基于利用固定口令的现有技术的认证系统的构成例的框图。在图 1 中，1 是在线服务服务器，3 是信息终端装置，5 是网络，6 是数据库，7 是在线服务客户机。

通基于利用固定口令的现有技术的认证系统，通过网络 5 连接在线服务服务器 1 和信息终端装置 3 构成。在线服务服务器 1 连接数据库 6，信息终端装置 3 具有在线服务客户机 7。在上述中，在线服务服务器 1 和数据库 6，为在线服务提供者所有。另外，信息终端装置 3，由在线服务利用者所有。例如，在线服务服务器 1 是 WWW 服务器，信息终端装置 3 是个人计算机，在线服务客户机 7 是 WWW 浏览器。

下面说明如上述构成的利用固定口令的认证系统的初始状态。

数据库 6，对于每一个在线服务利用者存储在线服务利用者 ID、以及在线服务认证用口令的各数据。另外，在线服务利用者，自身存储在线服务利用者 ID、以及在线服务认证用固定口令的各数据。但是，作为在线服务认证用口令，设定为在线服务认证用固定口令。

图 2 是说明利用固定口令的认证系统的在线服务认证处理的处理动作的流程图，下面说明该流程图。

(1) 在线服务利用者，向信息终端装置 3 的在线服务客户机 7，把在线服务认证用固定口令作为在线服务认证用口令，输入在线服务利用者 ID 和在线服务认证用口令和服务利用内容。这里，所谓服务利用内容，例如是在线服务

登录等的操作内容、或者商品买卖或者银行存入等交易内容（步骤 101）。

(2) 信息终端装置 3 的在线服务客户机 7，把包含输入的在线服务利用者 ID 和在线服务认证用口令和服务利用内容的在线服务认证请求，向在线服务服务器 1 发送（步骤 102）。

(3) 在线服务服务器 1，通过在在线服务认证请求中包含的在线服务利用者 ID 和在线服务认证用口令的组检索数据库 6，在有与在数据库中存储的在线服务利用者 ID 和在线服务认证用口令的组一致的、而且在包含在接收到的在线服务认证请求中包含的在线服务利用者 ID 的在线服务认证请求在一定时间以内仅在一定次数以下认证失败（账户未被锁定），亦即认证成功场合，遵照接收到的服务利用内容提供在线服务（步骤 103）。

利用固定口令的认证系统，因为不能频繁变更在线服务认证用固定口令，所以当在利用者使用的信息终端装置内设置键记录器（key logger）泄漏在线服务利用者 ID 和在线服务认证用固定口令时，不正当再利用这些口令的危险性高。

作为对于上述的利用固定口令的认证系统的危险性施行对策的客户机服务器系统中的客户机的认证技术，公知利用一次性口令的认证系统。利用一次性口令的认证系统，一次性口令服务器和一次性口令客户机共有在线服务认证用一次性口令，一次性口令客户机显示在线服务认证用一次性口令，把在线服务认证用一次性口令作为在线服务认证用口令，执行在线服务认证处理。

在利用一次性口令的认证系统中，从一次性口令服务器下载一次性口令的认证系统，在线服务利用者向一次性口令客户机输入在线服务利用者 ID 和一次性口令下载用固定口令，一次性口令客户机向一次性口令服务器发送包含在线服务利用者 ID 和一次性口令下载用固定口令的组的在线服务认证用一次性口令下载请求，在认证在一次性口令服务器接收的在线服务认证用一次性口令下载请求中包含的在线服务利用者 ID 和一次性口令下载用固定口令的组后向一次性口令客户机发送在线服务认证用一次性口令并共有。

另外，在利用一次性口令的认证系统中，专利文献 1 记载的一次性口令与时间同步的认证系统，在线服务服务器和一次性口令客户机独立地、把在线服务利用者 ID 和固定口令和现在的时刻信息作为安全散列函数的参数计算在

线服务认证用一次性口令并共有。

再有，在利用一次性口令的认证系统中，一次性口令与在线服务认证请求的次数同步的认证系统，在线服务服务器和一次性口令客户机独立地、把在线服务利用者 ID 和固定口令和在线服务认证请求次数的现在值作为安全散列函数的参数计算在线服务认证用一次性口令并共有。

上述中说明的利用一次性口令的认证系统，因为在线服务认证用一次性口令，对于每一现在的时刻信息或者每一在线服务认证请求次数而不同，所以具有即使在通过键记录器等泄漏了在线服务利用者 ID 和在线服务认证用一次性口令的场合，也能降低不正当再利用的危险性的特征。

专利文献 1：特开 2002-259344 号公报

发明内容

但是，根据上述的现有技术的利用一次性口令的认证系统，其任何一种都具有以下说明那样的问题。

作为第一问题，在从一次性口令服务器下载一次性口令的认证系统的场合，因为使用在线服务利用者输入的一次性口令下载用固定口令认证在线服务认证用一次性口令下载请求，所以存在一次性口令的安全性经常依赖于通过在线服务利用者输入的固定口令的安全性的问题。

作为第二问题，仅设想了新构建利用一次性口令的认证系统的场合，而未设想从利用固定口令的认证系统转移到利用一次性口令的认证系统的场合，所以存在需要变更进行在线服务认证请求的认证的通过图 2 说明的步骤 103 的处理的问题。

作为第三问题，在现有技术的一次性口令与时间同步的认证系统以及一次性口令与在线服务认证请求的次数同步的认证系统的场合，因为必须设想在线服务服务器和一次性口令客户机的现在的时刻信息或者在线服务认证请求的次数的现在值不一致的情况，所以存在也把前后几分钟的时刻信息或者几次前的认证请求次数作为参数计算的在线服务认证用一次性口令认证成功的问题。

作为第四问题，在现有技术的一次性口令与时间同步的认证系统以及一次性口令与在线服务认证请求的次数同步的认证系统的场合，因为在线服务服

务器和一次性口令客户机独立地计算在线服务认证用一次性口令,所以存在攻击者能够不限制时间或者次数地进行攻击的问题。

作为第五问题,因为在线服务认证用一次性口令的强度总是恒定的,所以在特定的在线服务利用者 ID 被攻击的场合,存在在线服务认证用一次性口令的强度变得不强的问题。

作为第六问题,因为一次性口令不与在在线服务认证请求中包含的服务利用内容同步,所以存在即使篡改了在在线服务认证请求中包含的服务利用内容认证也能成功这样的问题。

作为第七问题,因为未设想便携终端装置由在线服务客户机和一次性口令客户机构成的场合,所以存在在便携终端装置的在线服务客户机使用时的在线服务认证处理中不能使用一次性口令的问题。

作为第八问题,因为仅设想了在客户机的认证中使用一次性口令的场合,而未设想在邮件的认证中使用一次性口令,所以存在在钓鱼邮件对策中不能使用一次性口令的问题。

作为第九问题,虽然能够提高口令的安全性,但是不能提高 ID 的安全性,而且因为在线服务利用这 ID 容易用连续序号分配,所以存在攻击者能够推测有效的在线服务利用者 ID 来锁定账户的问题。

本发明的目的是提供一种认证系统以及认证方法,其能够解决上述使用一次性口令的现有技术的问题,提高利用一次性口令的认证系统的安全性,使系统转移容易,扩大使用范围。

根据本发明上述目的这样实现:提供一种认证系统,其为在通过网络连接在线服务服务器和一次性口令服务器和在线服务客户机和一次性口令客户机而构成的客户机服务器系统中的认证系统,其特征在于,所述一次性口令服务器,在通过一次性口令客户机初始化用固定口令认证来自所述一次性口令客户机的初始化请求后、和所述一次性口令客户机共有一次性口令下载用固定口令,同时,在通过一次性口令下载用固定口令认证在线服务认证用一次性口令下载请求后、和所述一次性口令客户机共有在线服务认证用一次性口令,所述在线服务服务器,通过在线服务认证用一次性口令认证从所述在线服务客户机接收到的在线服务认证请求。

另外，上述目的这样实现：提供一种认证系统，其为在通过网络连接在线服务服务器和一次性口令服务器和在线服务客户机和一次性口令客户机、并在数据库上连接在线服务服务器和一次性口令服务器而构成的客户机服务器系统中的认证系统，其特征在于，认证系统的初始状态，是在所述数据库中存储的在线服务认证用口令中设定了在线服务认证用固定口令的状态，所述一次性口令服务器，在认证了来自所述一次性口令客户机的初始化请求后、在在所述数据库中存储的在线服务认证用口令中设定伪一次性口令，同时，在认证了在线服务认证用一次性口令下载请求后、在在所述数据库中存储的在线服务认证用口令中设定在线服务认证用一次性口令，所述在线服务服务器，通过在所述数据库中存储的在线服务认证用口令认证从所述在线服务客户机接收到的在线服务认证请求，所述在线服务服务器或者所述一次性口令服务器，在认证了在线服务认证用一次性口令下载请求后，在不把和一次性口令客户机共有的在线服务认证用一次性口令作为在线服务认证请求的认证条件的场合，在在所述数据库中存储的在线服务认证用口令中设定伪一次性口令。

另外，本发明的目的这样实现：提供一种认证系统，其为在通过网络连接在线服务服务器和一次性口令服务器和在线服务客户机和一次性口令客户机构成的客户机服务器系统中的认证系统，其特征在于，所述一次性口令服务器，在认证了在线服务认证用一次性口令下载请求后、和所述一次性口令客户机共有多个在线服务认证用一次性口令，所述一次性口令客户机，在和所述一次性口令服务器共有在线服务认证用一次性口令后、以一定时间间隔顺序显示成为显示对象的多个在线服务认证用一次性口令的任何一个，所述在线服务服务器，对从所述在线服务客户机接收到的在线服务认证请求，如果在共有在线服务认证用一次性口令后经过一定时间后作为认证失败，在共有在线服务认证用一次性口令后以一定时间间隔顺序通过成为认证条件的多个在线服务认证用一次性口令的任何一个来进行认证。

另外，本发明的目的这样实现：提供一种认证系统，其为在通过网络连接在线服务服务器和一次性口令服务器和在线服务客户机和一次性口令客户机构成的客户机服务器系统中的认证系统，其特征在于，所述一次性口令服务器，在认证在线服务认证用一次性口令下载请求后、和所述一次性口令客户机

共有多个在线服务认证用一次性口令,所述一次性口令客户机,显示在线服务认证请求次数和在线服务认证用一次性口令的组,所述在线服务服务器,对从所述在线服务客户机接收到的在线服务认证请求,如果在共有在线服务认证用一次性口令以后的在线服务认证请求次数超过共有的在线服务认证用一次性口令的个数作为认证失败,通过和在共有在线服务认证用一次性口令以后的在线服务认证请求次数成组的在线服务认证用一次性口令进行认证。

另外,本发明的目的这样实现:提供一种认证系统,其为在通过网络连接在线服务服务器和在线服务客户机、并且由在线服务服务器和一次性口令服务器和在线服务客户机和一次性口令客户机构成的客户机服务器系统中的认证系统,其特征在于,所述在线服务服务器,用字符数是在线服务认证用一次性口令强度的现在值的在线服务认证用一次性口令,认证从在线服务客户机接收到的在线服务认证请求,如果认证失败则增大在线服务认证用一次性口令强度的现在值。

另外,上述目的这样实现:,提供一种认证系统,其为在通过网络连接在线服务服务器和一次性口令服务器和在线服务客户机、并由在线服务服务器和一次性口令服务器和在线服务客户机和一次性口令客户机构成的客户机服务器系统中的认证系统,其特征在于,所述一次性口令服务器和所述一次性口令客户机共有共有秘密信息,所述一次性口令服务器,对于包含从在线服务客户机接收到的服务利用内容的在线服务认证准备请求,和所述一次性口令客户机共有服务利用内容以及为用所述共有秘密信息认证服务利用内容的信息以及为用所述共有秘密信息计算在线服务认证用一次性口令的信息,所述一次性口令客户机,对于为用共有秘密信息认证服务利用内容的信息如果通过共有秘密信息认证成功,则对于为通过共有秘密信息计算在线服务认证用一次性口令的信息用所述共有信息计算在线服务认证用一次性口令,并显示服务利用内容和在线服务认证用一次性口令,所述在线服务服务器,通过在线服务认证用一次性口令认证从所述在线服务客户机接收到的在线服务认证请求。

另外,上述目的这样实现:提供一种认证系统,其为在通过网络连接在线服务服务器和一次性口令服务器和在线服务客户机、并由在线服务服务器和一次性口令服务器和在线服务客户机和一次性口令客户机构成的客户机服务

器系统中的认证系统，其特征在于，所述一次性口令服务器，对于包含从在线服务客户机接收到的服务利用内容的在线服务认证准备请求，存储服务利用内容，所述一次性口令服务器，在认证在线服务认证用一次性口令下载请求后、和所述一次性口令客户机共有服务利用内容和在线服务认证用一次性口令的组，所述一次性口令客户机，显示服务利用内容和在线服务认证用一次性口令的组，所述在线服务服务器，通过在线服务认证用一次性口令认证从所述在线服务客户机接收到的在线服务认证请求。

另外，上述目的这样实现：在上述中，所述一次性口令服务器，对于包含从所述在线服务客户机接收到的服务利用内容的在线服务认证准备请求，把在线服务认证用一次性口令的字符数作为在线服务认证用一次性口令的强度的现在值，增大在线服务认证用一次性口令的强度的现在值，所述在线服务服务器，如果从所述在线服务客户机接收到的在线服务认证请求认证成功，则减小在线服务认证用一次性口令的强度的现在值。

另外，上述目的这样实现：提供一种认证系统，其为在通过网络连接在线服务服务器和便携终端装置、且便携终端装置由在线服务客户机和一次性口令客户机构成的客户机服务器系统中的认证系统，其特征在于，所述便携终端装置的一次性口令客户机，把在线服务登录用一次性口令作为参数，起动便携终端装置的在线服务客户机，所述在线服务服务器，通过在线服务登录用一次性口令认证从便携终端装置的在线服务客户机接收到的在线服务登录请求。

另外，上述目的这样实现：提供一种认证系统，其为在通过网络连接在线服务服务器和一次性口令服务器和便携终端装置、且便携终端装置由在线服务客户机和一次性口令客户机构成的客户机服务器系统中的认证系统，其特征在于，所述一次性口令服务器，在通过一次性口令客户机初始化用固定口令认证一次性口令客户机初始化请求后，和所述便携终端装置的一次性口令客户机共有一次性口令下载用固定口令，同时，在通过一次性口令下载用固定口令认证在线服务登录用一次性口令下载请求后，和便携终端装置的一次性口令客户机共有在线服务登录用一次性口令，所述便携终端装置的一次性口令客户机，把在线服务登录用一次性口令作为参数，起动便携终端装置的在线服务客户机，所述在线服务服务器，通过在线服务登录用一次性口令认证从便携终端装

置的在线服务客户机接收到的在线服务登录请求。

另外，上述目的这样实现：提供一种认证系统，其为在通过网络连接一次性口令服务器和一次性口令客户机构成的客户机服务器系统中的认证系统，一次性口令服务器在邮件中记载邮件认证用一次性口令，一次性口令客户机显示邮件认证用一次性口令。

另外，上述目的这样实现：提供一种认证系统，其为在通过网络连接一次性口令服务器和一次性口令客户机构成的客户机服务器系统中的认证系统，其特征在于，所述一次性口令服务器，在用一次性口令客户机初始化用固定口令认证一次性口令客户机初始化请求后，和一次性口令客户机共有一次性口令下载用固定口令，同时，在邮件中记载邮件认证用一次性口令，在通过一次性口令下载用固定口令认证邮件认证用一次性口令下载请求后，和所述一次性口令客户机共有邮件认证用一次性口令，所述一次性口令客户机显示邮件认证用一次性口令。

另外，上述目的这样实现：提供一种认证系统，其为在通过网络连接在线服务服务器和一次性口令服务器和在线服务客户机和一次性口令客户机构成的客户机服务器系统中的认证系统，其特征在于，所述一次性口令服务器和一次性口令客户机，共有在线服务利用者子 ID，所述一次性口令客户机显示在线服务利用者子 ID，所述在线服务服务器，通过在线服务利用者子 ID 认证从在线服务客户机接收到的在线服务认证请求。

另外，上述目的这样实现：，在上述中，所述在线服务服务器，从所述一次性口令服务器接收加密的所述服务利用内容和在线服务认证用一次性口令的组，编码为 QR 代码后向所述在线服务客户机发送，所述在线服务客户机，显示所述 QR 代码，所述一次性口令客户机，输入所述 QR 代码并解码后通过所述共同密钥进行解密。

另外，上述目的这样实现：提供一种认证系统，其为在通过网络连接在线服务服务器和一次性口令服务器和在线服务客户机和一次性口令客户机构成的客户机服务器系统中的认证方法，其特征在于，所述一次性口令服务器，在通过一次性口令客户机初始化用固定口令认证来自所述一次性口令客户机的初始化请求后，和所述一次性口令客户机共有一次性口令下载用固定口令，

同时,在通过一次性口令下载用固定口令认证在线服务认证用一次性口令下载请求后,和所述一次性口令客户机共有在线服务认证用一次性口令,所述在线服务服务器,通过在线服务认证用一次性口令认证从所述在线服务客户机接收到的在线服务认证请求。

另外,上述目的这样实现:提供一种认证系统,其为在通过网络连接在线服务服务器和一次性口令服务器和在线服务客户机和一次性口令客户机、且在数据库上连接在线服务服务器和一次性口令服务器构成的客户机服务器系统中的认证方法,其特征在于,认证系统的初始状态,是在在所述数据库中存储的在线服务认证用口令中设定了在线服务认证用固定口令的状态,所述一次性口令服务器,在认证来自所述一次性口令客户机的初始化请求后,在在所述数据库中存储的在线服务认证用口令中设定伪一次性口令,同时,在认证在线服务认证用一次性口令下载请求后,在在所述数据库中存储的在线服务认证用口令中设定在线服务认证用一次性口令,所述在线服务服务器,通过在所述数据库中存储的在线服务认证用口令认证从所述在线服务客户机接收到的在线服务认证请求,所述在线服务服务器或者所述一次性口令服务器,在认证在线服务认证用一次性口令下载请求后,在不把和一次性口令客户机共有的在线服务认证用一次性口令作为在线服务认证请求的认证条件的场合,在在所述数据库中存储的在线服务认证用口令中设定伪一次性口令。

另外,上述目的这样实现:提供一种认证系统,其为在通过网络连接在线服务服务器和一次性口令服务器和在线服务客户机和一次性口令客户机构成的客户机服务器系统中的认证方法,其特征在于,所述一次性口令服务器,在认证在线服务认证用一次性口令下载请求后,和所述一次性口令客户机共有多个在线服务认证用一次性口令,所述一次性口令客户机,在和所述一次性口令服务器共有在线服务认证用一次性口令后,以一定时间间隔顺序显示成为显示对象的多个在线服务认证用一次性口令的任何一个,所述在线服务服务器,对从所述在线服务客户机接收到的在线服务认证请求,如果在共有在线服务认证用一次性口令后经过一定时间后作为认证失败、在共有在线服务认证用一次性口令后以一定时间间隔顺序通过成为认证条件的多个在线服务认证用一次性口令的任何一个来进行认证。

另外，上述目的这样实现：提供一种认证系统，其为在通过网络连接在线服务服务器和一次性口令服务器和在线服务客户机和一次性口令客户机构成的客户机服务器系统中的认证方法，其特征在于，所述一次性口令服务器，在认证在线服务认证用一次性口令下载请求后，和所述一次性口令客户机共有多个在线服务认证用一次性口令，所述一次性口令客户机，显示在线服务认证请求次数和在线服务认证用一次性口令的组，所述在线服务服务器，对从所述在线服务客户机接收到的在线服务认证请求，如果在共有在线服务认证用一次性口令以后的在线服务认证请求次数超过共有的在线服务认证用一次性口令的个数作为认证失败，通过和在共有在线服务认证用一次性口令以后的在线服务认证请求次数成组的在线服务认证用一次性口令进行认证。

另外，上述目的这样实现：提供一种认证系统，其为在通过网络连接在线服务服务器和一次性口令服务器和在线服务客户机、且由在线服务服务器和一次性口令服务器和在线服务客户机和一次性口令客户机构成的客户机服务器系统中的认证方法，其特征在于，所述一次性口令服务器，对于包含从在线服务客户机接收到的服务利用内容的在线服务认证准备请求，存储服务利用内容，所述一次性口令服务器，在认证在线服务认证用一次性口令下载请求后，和所述一次性口令客户机共有加密服务利用内容和在线服务认证用一次性口令的组的共同密钥，所述一次性口令客户机，通过所述共同密钥解密显示服务利用内容和在线服务认证用一次性口令的组，所述在线服务服务器，通过在线服务认证用一次性口令认证从所述在线服务客户机接收到的在线服务认证请求。

另外，上述目的这样实现：在上述中，所述在线服务服务器，从所述一次性口令服务器接收加密的所述服务利用内容和在线服务认证用一次性口令的组，编码为QR代码后向所述在线服务客户机发送，所述在线服务客户机，显示所述QR代码，所述一次性口令客户机，输入并解码所述QR代码后通过所述共同密钥进行解密。

根据本发明，能够谋求客户机服务器系统中的、利用一次性口令的认证系统的安全性的提高或者从利用固定口令的认证系统的转移容易化或者范围的扩大。

## 附图说明

图 1 是表示利用固定口令的基于现有技术的认证系统的构成例的框图。

图 2 是说明利用固定口令的认证系统的在线服务认证处理的处理动作的流程图。

图 3 是表示根据本发明的一个实施形态的认证系统的结构的框图。

图 4 是说明信息终端装置的在线服务客户机使用时的在线服务认证处理（一次性口令与时间同步的场合）的处理动作的流程图。

图 5 是说明信息终端装置的在线服务客户机使用时的在线服务认证处理（一次性口令与在线服务认证请求的次数同步的场合）的处理动作的流程图。

图 6 是说明信息终端装置的在线服务客户机使用时的在线服务认证处理（一次性口令与在在线服务认证请求的中包含的利用内容同步的场合）的处理动作的流程图。

## 具体实施方式

下面根据附图更详细地说明本发明的认证系统以及认证方法的实施形态。

图 3 是表示根据本发明的一个实施形态的认证系统的结构的框图。下面说明的本发明的实施形态，是利用一次性口令的认证系统。在图 3 中，2 是一次性口令服务器，4 是便携终端装置，8 是在线服务客户机，9 是一次性口令客户机，其他的符号和图 1 的场合相同。

根据图 3 所示的本发明的实施形态的认证系统，通过网络 5 连接在线服务服务器 1 和一次性口令服务器 2 和信息终端装置 3 和便携终端装置 4 构成。在线服务服务器 1 和一次性口令服务器 2 连接数据库 6。信息终端装置 3 由在线服务客户机 7 构成，便携终端装置 4 由在线服务客户机 8 和一次性口令客户机 9 构成。

在上述中，在线服务服务器 1 和一次性口令服务器 2 和数据库 6，为在线服务提供者所有，信息终端装置 3 和便携终端装置 4，为在线服务利用者所有。另外，便携终端装置 4 可以是便携电话等。

下面说明如上述构成的根据本发明的实施形态的利用一次性口令的认证系统的初始状态。

数据库 6, 对于每个在线服务利用者, 存储在线服务利用者 ID、在线服务认证用口令、以及一次性口令客户机初始化用固定口令的各数据。另外, 在线服务利用者, 存储在线服务利用者 ID 以及一次性口令客户机初始化用固定口令的各数据。

但是, 在从利用固定口令的认证系统迁移到本发明的认证系统的场合, 在在线服务认证用口令中设定在线服务认证用固定口令。另外, 在新构建本发明的认证系统的场合, 在在线服务认证用口令中设定一次性口令服务器 2 随机生成的伪一次性口令。在以下的说明中, 对于数据库 6 的数据操作, 把与在线服务利用者 ID 成组的数据作为对象。

下面说明本发明的实施形态的认证系统中的一次性口令客户机的初始化处理的处理动作。但是, 假定在一次性口令客户机的初始化处理以前, 在线服务利用者随机生成并存储有一次性口令客户机起动用固定口令。此外, 未表示这里的处理动作的流程。

(处理 201)

在线服务利用者, 向一次性口令客户机 9 输入在线服务利用者 ID 和一次性口令客户机初始化用固定口令和一次性口令客户机起动用固定口令。

(处理 202)

一次性口令客户机 9, 向一次性口令服务器 2 发送包含在线服务利用者 ID 和一次性口令客户机初始化用固定口令的组的一次性口令客户机初始化请求。

(处理 203)

一次性口令服务器 2, 通过在接收到的一次性口令客户机初始化请求中包含的在线服务利用者 ID 和一次性口令客户机初始化用固定口令的组检索数据库 6, 在数据库 6 中存储有与在线服务利用者 ID 和一次性口令客户机初始化用固定口令的组一致的记录、而且包含在接收到的一次性口令客户机初始化请求中包含的在线服务利用者 ID 的一次性口令客户机初始化请求在一定时间以内仅一定次数以下认证失败的场合(未锁定账户), 随机生成伪一次性口令, 在数据库 6 中存储的在线服务认证用口令中设定伪一次性口令, 随机生成共有秘密信息, 在数据库 6 中存储该共有秘密信息, 向一次性口令客户机 9 发送共有秘密信息。这里, 所谓共有秘密信息, 是一次性口令服务器 2 和一次性口令

客户机 9 共有的固定口令或者加密系统的密钥。

(处理 204)

一次性口令客户机 9, 当接收发送来的共有秘密信息时, 存储在线服务利用者 ID 和一次性口令客户机起动用固定口令和共有秘密信息。

通过执行以上的处理, 结束一次性口令客户机的初始化处理。

下面说明本发明的实施形态中的一次性口令客户机的起动用处理。但是假定在一次性口令客户机的起动用处理以前, 已经结束了上述中说明的一次性口令客户机的初始化处理的执行。此外, 未表示这里的处理动作的流程。

(处理 301)

在线服务利用者, 向一次性口令客户机 9 输入一次性口令客户机起动用固定口令。

(处理 302)

一次性口令客户机 9, 在输入的一次性口令客户机起动用固定口令和在一次性口令客户机 9 中存储的一次性口令客户机起动用固定口令相等的场合, 使能够执行根据图 4 后述的步骤 401 的处理以后的一次性口令客户机 9 中的处理。

(处理 303)

一次性口令客户机 9, 在一定次数连续输入的一次性口令客户机起动用固定口令和在一次性口令客户机 9 中存储的一次性口令客户机起动用固定口令不相等的场合, 删除在一次性口令客户机 9 中存储的在线服务利用者 ID 和一次性口令客户机起动用固定口令和共有秘密信息。

图 4 是说明在本发明的认证系统中信息终端装置的在线服务客户机使用时的在线服务认证处理(一次性口令与时间同步的场合)的处理动作的流程图, 下面就此加以说明。假定在这里的处理中使用的共有秘密信息是一次性口令下载用固定口令。

(1) 便携终端装置 4 的一次性口令客户机 9, 向一次性口令服务器 2 发送包含在线服务利用者 ID 和一次性口令下载用固定口令的组的在线服务认证用一次性口令下载请求(步骤 401)。

(2) 一次性口令服务器 2, 通过在接收到的在线服务认证用一次性口令下

载请求中包含的在线服务利用者 ID 和一次性口令下载用固定口令的组检索数据库 6, 在数据库 6 中存储有与在线服务利用者 ID 和一次性口令下载用固定口令的组一致的记录的场合, 随机生成  $N$  个在线服务认证用一次性口令 (OTP[0]~OTP[N-1]), 在数据库 6 中存储的在线服务认证用口令中设定 OTP[0], 向一次性口令客户机 9 发送 OTP[0]~OTP[N-1] (步骤 402)。

(3) 一次性口令客户机 9, 显示在线服务利用者 ID 和接收到的在线服务认证用一次性口令之一的 OTP[0] (步骤 403)。

(4) 一次性口令服务器 2, 在执行步骤 402 的处理后, 经过一定时间 ( $T_i$  秒,  $1 \leq i \leq N-1$ ) 后, 在数据库 6 中存储的在线服务认证用口令中设定 OTP[i]。另外, 一次性口令服务器 2, 在执行步骤 402 的处理后, 经过一定时间 ( $T_N$  秒) 后, 随机生成伪一次性口令, 在数据库 6 中存储的在线服务认证用口令中设定伪一次性口令 (步骤 404)。

(5) 一次性口令客户机 9, 在执行步骤 403 的处理后, 经过一定时间 ( $T_i$  秒,  $1 \leq i \leq N-1$ ) 后, 显示在线服务利用者 ID 和在线服务认证用一次性口令之一的 OTP[i]。另外, 一次性口令客户机 9, 在执行步骤 403 的处理后, 经过一定时间 ( $T_N$  秒) 后, 结束在线服务利用者 ID 和在线服务认证用一次性口令的显示 (步骤 405)。

(6) 在线服务利用者, 向信息终端装置 3 的在线服务客户机 7, 把在一次性口令客户机 9 上显示的在线服务认证用一次性口令作为在线服务认证用口令, 输入在线服务利用者 ID 和在线服务认证用口令和服务利用内容 (步骤 406)。

(7) 信息终端装置 3 的在线服务客户机 7, 给在线服务服务器 1, 发送包含在线服务利用者 ID 和在线服务认证用口令和服务利用内容的组的在线服务认证请求 (步骤 407)。

(8) 在线服务服务器 1, 当接收在步骤 407 的处理中发送来的在线服务认证请求时, 执行和根据图 2 说明的现有技术中的步骤 103 的处理同样的处理 (步骤 408)。

图 5 是说明在本发明的认证系统中, 信息终端装置的在线服务客户机使用时的在线服务认证处理 (一次性口令与在线服务认证请求的次数同步的场

合)的处理动作的流程图,下面就此加以说明。把在这里的处理中使用的共有秘密信息作为一次性口令下载用固定口令。另外,假定在本发明的认证系统的初始状态下,数据库6,对于每一在线服务利用者,存储作为在线服务认证请求次数的最大值设定N的在线服务认证请求次数的现在值。

(1) 便携终端装置4的一次性口令客户机9,向一次性口令服务器2发送包含在线服务利用者ID和一次性口令下载用固定口令的组的在线服务认证用一次性口令下载请求(步骤501)。

(2) 一次性口令服务器2,通过在接收到的在线服务认证用一次性口令下载请求中包含的在线服务利用者ID和一次性口令下载用固定口令的组检索数据库6,在数据库6中存储有与在线服务利用者ID和一次性口令下载用固定口令的组一致的记录的场合,随机生成N个在线服务认证用一次性口令(OTP[1]~OTP[N]),在数据库6中存储的在线服务认证用口令中设定OTP[1],在数据库6中存储的在线服务认证请求次数的现在值中设定在线服务认证请求次数初始值1,在数据库6中存储OTP[2]~OTP[N],向一次性口令客户机9发送在线服务认证用一次性口令OTP[1]~OTP[N](步骤502)。

(3) 一次性口令客户机9,接收发送来的在线服务认证用一次性口令OTP[1]~OTP[N]后进行存储(步骤503)。

(4) 一次性口令客户机9,显示在线服务利用者ID和在线服务认证请求次数i和在线服务认证用一次性口令OTP[i]的组( $1 \leq i \leq N$ )(步骤504)。

(5) 在线服务利用者,对于信息终端装置3的在线服务客户机7,把和在线服务认证请求次数的现在值x成组的在一次性口令客户机上显示的在线服务认证用一次性口令OTP[x]作为在线服务认证用口令,输入在线服务利用者ID和在线服务认证用口令和服务利用内容(步骤505)。

(6) 信息终端装置3的在线服务客户机7,对于在线服务服务器1,发送包含在线服务利用者ID和在线服务认证用口令和服务利用内容的组的在线服务认证请求(步骤506)。

(7) 在线服务服务器1,当接收在步骤506的处理中发送来的在线服务认证请求时,执行和根据图2说明的现有技术中的步骤103的处理相同的处理(步骤507)。

(8) 其后, 在线服务服务器 1, 在数据库 6 中存储的在线服务认证请求次数的现在值  $x$  等于在线服务认证请求次数的最大值  $N$  的场合, 随机生成伪一次性口令, 在数据库 6 中存储的在线服务认证用口令中设定伪一次性口令, 向信息终端装置 3 的在线服务客户机 7 发送催促在线服务认证用一次性口令下载的画面。另外, 在线服务服务器 1, 如果在数据库 6 中存储的在线服务认证请求次数的现在值  $x$  不到在线服务认证请求次数最大值  $N$ , 则在数据库 6 中存储的在线服务认证用口令中设定  $OTP[x+1]$ , 在数据库 6 中存储的在线服务认证请求次数的现在值中设定  $x+1$ , 向信息终端装置 3 的在线服务客户机 7 发送显示在线服务认证请求次数的现在值  $x+1$  的画面 (步骤 508)。

下面, 说明在本发明的认证系统中, 即使在攻击特定的在线服务利用者 ID 的场合, 也难于猜中一次性口令, 能够提高安全性的应对处理。该处理可以通过变更在上述中说明的图 4、图 5 的流程中的一部分来实施。此外, 假定在本发明的认证系统的初始状态下, 数据库 6 对于每一在线服务利用者, 存储设定了在线服务认证用一次性口令强度的初始值的在线服务认证用一次性口令强度现在值。

在图 4 中的步骤 408 的处理或者图 5 中的步骤 507 的处理中, 在线服务服务器 1, 取得在数据库 6 中存储的在线服务认证用一次性口令强度现在值  $x$ , 通过在接收到的在线服务认证请求中包含的在线服务认证用口令和在数据库 6 中存储的在线服务认证用口令从开头起  $x$  个字符是否相等来进行认证, 如果认证成功, 则在数据库 6 中存储的在线服务认证用一次性口令强度现在值中设定在线服务认证用一次性口令强度初始值, 如果认证失败, 则在数据库 6 中存储的在线服务认证用一次性口令强度现在值中设定  $x+1$ , 向信息终端装置 3 的在线服务客户机 7 发送显示在线服务认证用一次性口令强度现在值的画面。

图 6 是说明在本发明的认证系统中, 信息终端装置的在线服务客户机使用时的在线服务认证处理(一次性口令与在在线服务认证请求中包含的服务里通内容同步)的处理动作的流程图, 下面就此加以说明。但是, 把在这里的处理中使用的共有秘密信息作为共同密钥加密系统的共同密钥。另外, 假定在本发明的认证系统的初始状态下, 数据库 6 对于每一在线服务利用者存储设定了在线服务认证用一次性口令强度的初始值的在线服务认证用一次性口令强度

现在值。

(1) 在线服务利用者,对于信息终端装置3的在线服务客户机7输入在线服务利用者ID和服务利用内容(步骤601)。

(2) 信息终端装置3的在线服务客户机7,向在线服务服务器1发送包含输入的在线服务利用者ID和服务利用内容的组的在线服务认证准备请求(步骤602)。

(3) 在线服务服务器1,向一次性口令服务器2发送包含在线服务利用者ID和服务利用内容的组的在线服务认证准备请求(步骤603)。

(4) 一次性口令服务器2,根据接收到的在线服务利用者ID检索数据库6,在在线服务利用者ID在数据库6中存储的场合,取得在数据库6中存储的共同密钥K和在线服务认证用一次性口令强度现在值 $x$ ,随机生成在线服务认证准备ID和强度是 $x$ 个字符的在线服务认证用一次性口令,在数据库6中存储的在线服务认证用一次性口令强度现在值中设定 $x+1$ ,在数据库6中存储在线服务认证准备ID和服务利用内容和在线服务认证用一次性口令的组。另外,一次性口令服务器2,在接收到的在线服务利用者ID未存储在数据库6中的场合,随机生成共同密钥K和在线服务认证准备ID和在线服务认证用一次性口令。然后,一次性口令服务器2,把服务利用内容和在线服务认证用一次性口令的连结位列作为明文,用共同密钥加密,而且,附加MAC(Message Authentication Code)后将其作为在线服务认证准备信息,向在线服务服务器1发送在线服务认证准备ID和在线服务认证准备信息(步骤604)。

(5) 在线服务服务器1,把接收到的在线服务认证准备信息编码为QR代码,向信息终端装置3的在线服务客户机7发送在线服务认证准备ID和QR代码(步骤605)。

(6) 信息终端装置3的在线服务客户机7显示接收到的QR代码(步骤606)。

(7) 一次性口令客户机9,从QR代码解码在线服务认证准备信息,用共同密钥K解密在线服务认证准备信息,而且,如果通过MAC的认证成功,则显示服务利用内容和在线服务认证用一次性口令(步骤607)。

(8) 在线服务利用者,确认在一次性口令客户机上显示的服务利用内容是

否等于在步骤 601 的处理中输入的服务利用内容，如果等于，则对于信息终端装置 3 的在线服务服务器 7 输入在一次性口令客户机上显示的在线服务认证用一次性口令（步骤 608）。

(9) 信息终端装置 3 的在线服务服务器 7，向在线服务服务器 1，发送包含在线服务利用者 ID 和在线服务认证准备 ID 和在线服务认证用一次性口令的组的在线服务认证请求（步骤 609）。

(10) 在线服务服务器 1，通过在接收到的在线服务认证请求中包含的在线服务利用者 ID 和在线服务认证准备 ID 和在线服务认证用一次性口令的组检索数据库 6，在数据库 6 中存储有与在线服务利用者 ID 和在线服务认证准备 ID 和在线服务认证用一次性口令的组一致的记录的场合，作为认证成功，在数据库 6 中存储的在线服务认证用一次性口令强度现在值中设定在线服务认证用一次性口令强度初始值，取得在接收到的在线服务认证请求中包含的成为在线服务利用者 ID 和在线服务认证准备 ID 的组的在数据库 6 中存储的服务利用内容，遵照该服务利用内容提供在线服务。另外，在线服务服务器 1，在认证失败的场合，删除在接收到的在线服务认证请求中包含的成为在线服务利用者 ID 和在线服务认证准备 ID 的组的在数据库 6 中存储的在线服务认证准备 ID 和服务利用内容和在线服务认证用一次性口令的组（步骤 610）。

上述的、信息终端装置的在线服务客户机使用时的在线服务认证处理（一次性口令与在在线服务认证请求中包含的服务利用内容同步的场合）的处理动作，把共有秘密信息变更为一次性口令下载用固定口令、即使把上述的步骤 604~607 变更为以下的步骤 611~615 也可以实施。此外，未表示这里的处理动作的流程。

(11) 一次性口令服务器 2，根据接收到的在线服务利用者 ID 检索数据库 6，在在线服务利用者 ID 存储在检索数据库 6 中的场合，取得在数据库 6 中存储的在线服务认证用一次性口令强度现在值  $x$ ，随机生成在线服务认证准备 ID 和强度是  $x$  个字符的在线服务认证用一次性口令，在数据库 6 中存储的在线服务认证用一次性口令强度现在值中设定  $x+1$ ，在数据库 6 中存储在线服务认证准备 ID 和服务利用内容和在线服务认证用一次性口令的组。另外，一次性口令服务器 2，在接收到的在线服务利用者 ID 不在数据库 6 中存储的场合，随

机生成在线服务认证准备 ID。然后，一次性口令服务器 2，向在线服务服务器 1 发送在线服务认证准备 ID（步骤 611）。

(12) 在线服务服务器 1，向信息终端装置 3 的在线服务客户机 7 发送在线服务认证准备 ID（步骤 612）。

(13) 便携终端装置 3 的一次性口令客户机 9，向一次性口令服务器 2，发送包含在线服务利用者 ID 和一次性口令下载用固定口令的组的在线服务认证用一次性口令下载请求（步骤 613）。

(14) 一次性口令服务器 2，根据接收到的在在线服务认证用一次性口令下载请求中包含的在线服务利用者 ID 和一次性口令下载用固定口令的组检索数据库 6，在数据库 6 中存储有与在线服务利用者 ID 和一次性口令下载用固定口令的组一致的记录的场合，向一次性口令客户机 9 发送在数据库 6 中存储的服务利用内容和在线服务认证用一次性口令的组（步骤 614）。

(15) 一次性口令客户机 9，显示接收到的服务利用内容和在线服务认证用一次性口令的组（步骤 615）。

下面说明在本发明的认证系统中便携终端装置的在线服务客户机使用时的在线服务认证处理的处理动作。但是把这里的处理中使用的共有秘密信息作为一次性口令下载用固定口令。此外未表示这里的处理动作的流程。

（处理 701）

便携终端装置 4 的一次性口令客户机 9，向一次性口令服务器 2，发送包含在线服务利用者 ID 和一次性口令下载用固定口令的组的在线服务登录用一次性口令下载请求。

（处理 702）

一次性口令服务器 2，根据在接收到的在线服务登录用一次性口令下载请求中包含的在线服务利用者 ID 和一次性口令下载用固定口令的组检索数据库 6，在数据库 6 中存储有与在线服务利用者 ID 和一次性口令下载用固定口令的组一致的记录的场合，随机生成在线服务登录用一次性口令，在数据库 6 中存储在线服务登录用一次性口令，向一次性口令客户机 9 发送在线服务登录用一次性口令。

（处理 703）

一次性口令客户机 9, 把在线服务利用者 ID 和在线服务登录用一次性口令作为参数, 起动便携终端装置 4 的在线服务客户机 8。

(处理 704)

便携终端装置 4 的在线服务客户机 8, 向在线服务服务器 1 发送包含在线服务利用者 ID 和在线服务登录用一次性口令的组的在线服务登录请求。

(处理 705)

在线服务服务器 1, 根据在接收到的在线服务登录请求中包含的包含在线服务利用者 ID 和在线服务登录用一次性口令的组检索数据库 6, 在数据库 6 中存储有与在线服务利用者 ID 和在线服务登录用一次性口令的组一致的记录的场合, 向便携终端装置 4 的在线服务客户机 8 发送在线服务登录成功画面。

下面说明本发明的认证系统中的邮件认证处理的处理动作。但是, 把在这里的处理中使用的共有秘密信息作为一次性口令下载用口令。此外, 未表示这里的处理动作的流程。

(处理 801)

一次性口令服务器 2, 在接收发送目的地是在线服务利用者的邮件和发送目的地的在线服务利用者的在线服务利用者 ID 的场合, 随机生成邮件认证用一次性口令, 在数据库 6 中存储邮件认证用一次性口令, 在邮件中记载邮件认证用一次性口令后向发送目的地发送。

(处理 802)

一次性口令客户机 9, 向一次性口令服务器 2, 发送包含在线服务利用者 ID 和一次性口令下载用固定口令的组的邮件认证用一次性口令下载请求。

(处理 803)

一次性口令服务器 2, 根据在接收到的邮件认证用一次性口令下载请求中包含的在线服务利用者 ID 和一次性口令下载用固定口令的组检索数据库 6, 在数据库 6 中存储有与在线服务利用者 ID 和一次性口令下载用固定口令的组一致的记录的场合, 取得数据库 6 中存储的邮件认证用一次性口令, 向一次性口令客户机 9 发送邮件认证用一次性口令。

(处理 804)

一次性口令客户机 9 显示接收到的邮件认证用一次性口令。

在线服务利用者，在执行处理 804 后，比较在邮件中记载的邮件认证用一次性口令和在一次性口令客户机 9 上显示的邮件认证用一次性口令，如果一致，则可以知道邮件的发送源是在线服务提供者，如果不一致则可以知道邮件的发送源不是在线服务提供者。

上述的处理 801，是设想作为邮件是电子邮件的场合，但是即使在设想作为邮件是明信片等寄送物的场合，也可以通过在寄送物中记载邮件认证用一次性口令，能够认证邮件的发送源。

下面说明在本发明的认证系统中攻击者不能推测有效的 ID 那样的应对处理。该处理，通过变更在上述中说明的处理 203 以及处理 204 以后的处理能够实施。

在上述中说明的处理 203 中的处理中，一次性口令服务器 2，随机生成在线服务利用者 ID，在数据库 6 中存储在线服务利用者 ID，向一次性口令客户机 9 发送在线服务利用者 ID。

在处理 204 中的处理以后的处理中，代替在线服务利用者 ID 使用在线服务利用者子 ID。但是，在线服务利用者子 ID 可取的值的总数，需要比在线服务利用者的总数大许多，例如大 1 万倍左右。

下面，说明在上述本发明的实施形态中使用的各口令的强度。口令的强度，一般通过构成口令的英文数字符号的字符数决定，考虑系统的安全性和在线服务里通者的便利性来决定，但是在本发明的实施形态中，作为伪一次性口令、一次性口令下载用固定口令、以及在线服务登录用一次性口令，使用英文数字符号 32 个字符左右的口令，另外，作为一次性口令客户机初始化用固定口令以及在线服务认证用固定口令，使用英文数字符号 8 个字符左右的口令，再有，作为一次性口令客户机起动用固定口令、在线服务认证用一次性口令、以及邮件认证用一次性口令，使用数字 8 个字符左右的口令。另外，在线服务认证用一次性口令强度的初始值是 8 个左右。

构成上述的本发明的实施形态的在线服务服务器 1、在线服务服务器 2 以及信息终端装置 3，可以通过具有 CPU、存储器、硬盘装置、显示装置、输入输出装置的信息处理装置构成。另外，便携终端装置 4，作为便携电话进行了说明，但是作为便携终端装置 4，可以使用可携带的如上述构成的信息处理

装置。

另外，上述本发明的各实施形态中的处理，可以通过程序构成，使计算机具有的 CPU 执行，另外，这些程序可以存储在 FD、CDROM、DVD 等记录介质上来提供，另外，可以通过网络通过数字信息提供。

根据上述本发明的实施形态，在一次性口令客户机初始化请求的认证中，因为当一次性口令客户机初始化固定口令的强度减弱为英文数字 8 个字符左右，所以包含有账户被锁定的条件，但是在在线服务认证用一次性口令下载请求的认证中，因为当将一次性口令下载用固定口令的强度加强为英文数字符号 32 个字符左右，所以不包含账户被锁定的条件，故此能够做到使攻击者不能够妨害正当的在线服务利用者的在线服务认证用一次性口令下载请求，由此，能够解决一次性口令的安全性总是依赖于通过在线服务利用者输入的固定口令的安全性这样的、利用基于现有技术的一次性口令的认证系统的第一个问题。

另外，根据本发明的实施形态，因为根据一次性口令客户机初始化的有无以及成为在线服务认证请求的认证条件的在线服务认证用一次性口令的有无，在数据库中存储的在线服务认证用口令中，设定在线服务认证用固定口令、伪一次性口令或者在线服务认证用一次性口令，所以能够解决必须变更执行在线服务认证请求的认证的步骤 103 中的处理这样的、利用现有技术的一次性口令的认证系统的第二个问题。

另外，根据本发明的实施形态，因为在共有在线服务认证用一次性口令时，使在线服务服务器和一次性口令客户机的现在的时刻信息或者在线服务认证请求次数的现在值一致，如果在共有后经过一定时间后或者共有以后的在线服务认证请求次数超过一定次数后，把在线服务认证请求作为认证失败，所以能够解决把前后数分钟之间的时刻信息或者数次前的在线服务认证请求次数作为参数计算的在线服务认证用一次性口令也认证成功这样的、使用现有技术的一次性口令的认证系统的第三个问题，和攻击者可以无时间或者次数限制地进行攻击这样的第四个问题。

另外，根据本发明的实施形态，因为使用字符数是在线服务认证用一次性口令强度的现在值的在线服务认证用一次性口令认证在线服务服务器从在

线服务客户机接收的在线服务认证请求,如果认证失败则加大在线服务认证用一次性口令的强度的现在值,所以能够解决即使攻击特定的在线服务利用者ID 在线服务认证用一次性口令的强度也不变强这样的、使用现有技术的一次性口令的认证系统的第五个问题。

另外,根据本发明的实施形态,因为对于包含一次性口令服务器从在线服务客户机接收到的服务利用内容的在线服务认证准备请求,使服务利用内容和在线服务认证用一次性口令同步,确认一次性口令客户机和正当的一次性口令服务器共有服务利用内容和在线服务认证用一次性口令后,显示服务利用内容和在线服务认证用一次性口令,在线服务利用者能够确认在一次性口令客户机上显示的在服务利用内容和在线服务认证准备请求中包含的服务利用内容是否相等,所以能够解决即使篡改了在线服务认证准备请求中包含的服务利用内容也认证成功的、使用现有技术的一次性口令的认证系统的第六个问题。

另外,根据本发明的实施形态,因为便携终端装置的一次性口令客户机把在线服务登录用一次性口令作为参数起动车携终端装置的在线服务客户机,在线服务服务器根据在线服务登录用一次性口令认证从便携终端装置的在线服务客户机接收到的在线服务登录请求,所以能够解决便携终端装置的在线服务客户机使用时的在线服务认证处理中不能使用一次性口令这样的、使用现有技术的一次性口令的认证系统的第七个问题。

另外,根据本发明的实施形态,因为一次性口令服务器在邮件中记载邮件认证用一次性口令,一次性口令客户机显示邮件认证用一次性口令,所以能够解决钓鱼邮件对策中不能使用一次性口令这样的、使用现有技术的一次性口令的认证系统的第八个问题。

再有,根据本发明的实施形态,因为根据无效的ID比有效的ID远多且随机分配的在线服务利用者子ID认证在线服务认证请求,所以能够解决攻击者能够推测有效的在线服务利用者ID锁定账户的、使用现有技术的一次性口令的认证系统的第九个问题。

#### 符号说明

- 1 在线服务服务器
- 2 一次性口令服务器

- 3 信息终端装置
- 4 便携终端装置
- 5 网络
- 6 数据库
- 7 在线服务客户机
- 8 在线服务客户机
- 9 一次性口令客户机

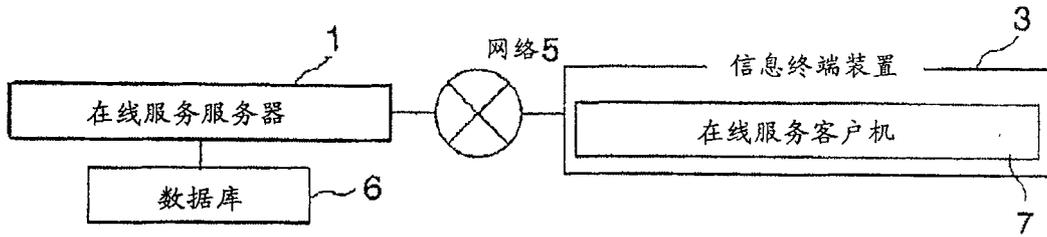


图 1

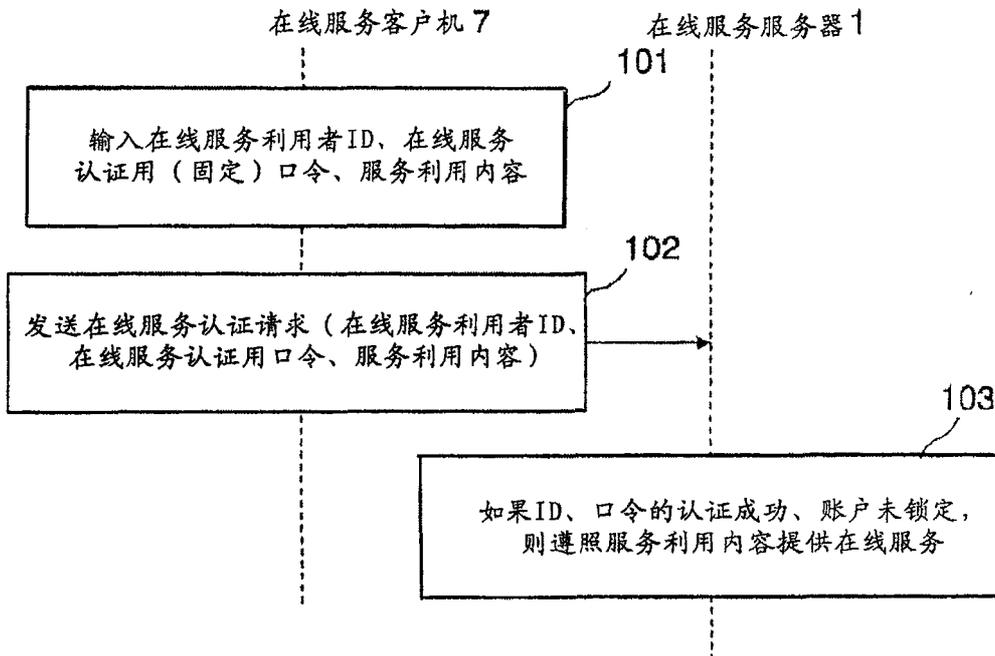


图 2

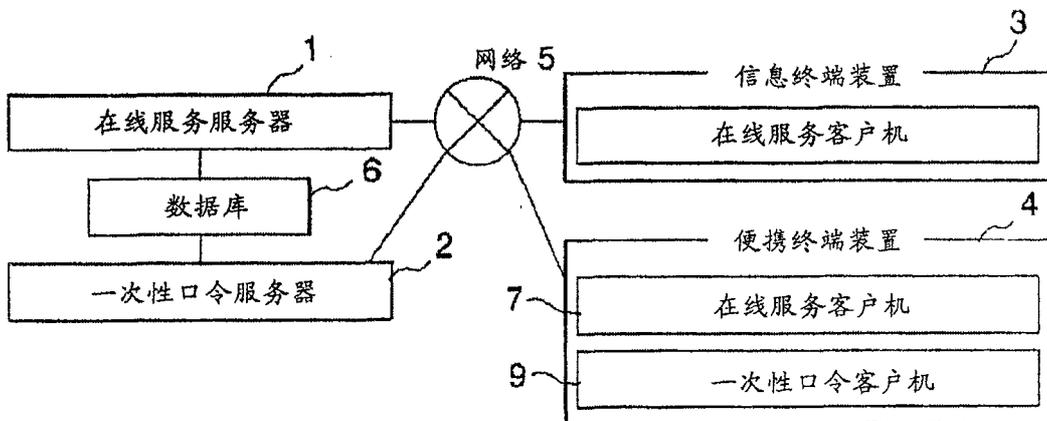


图 3

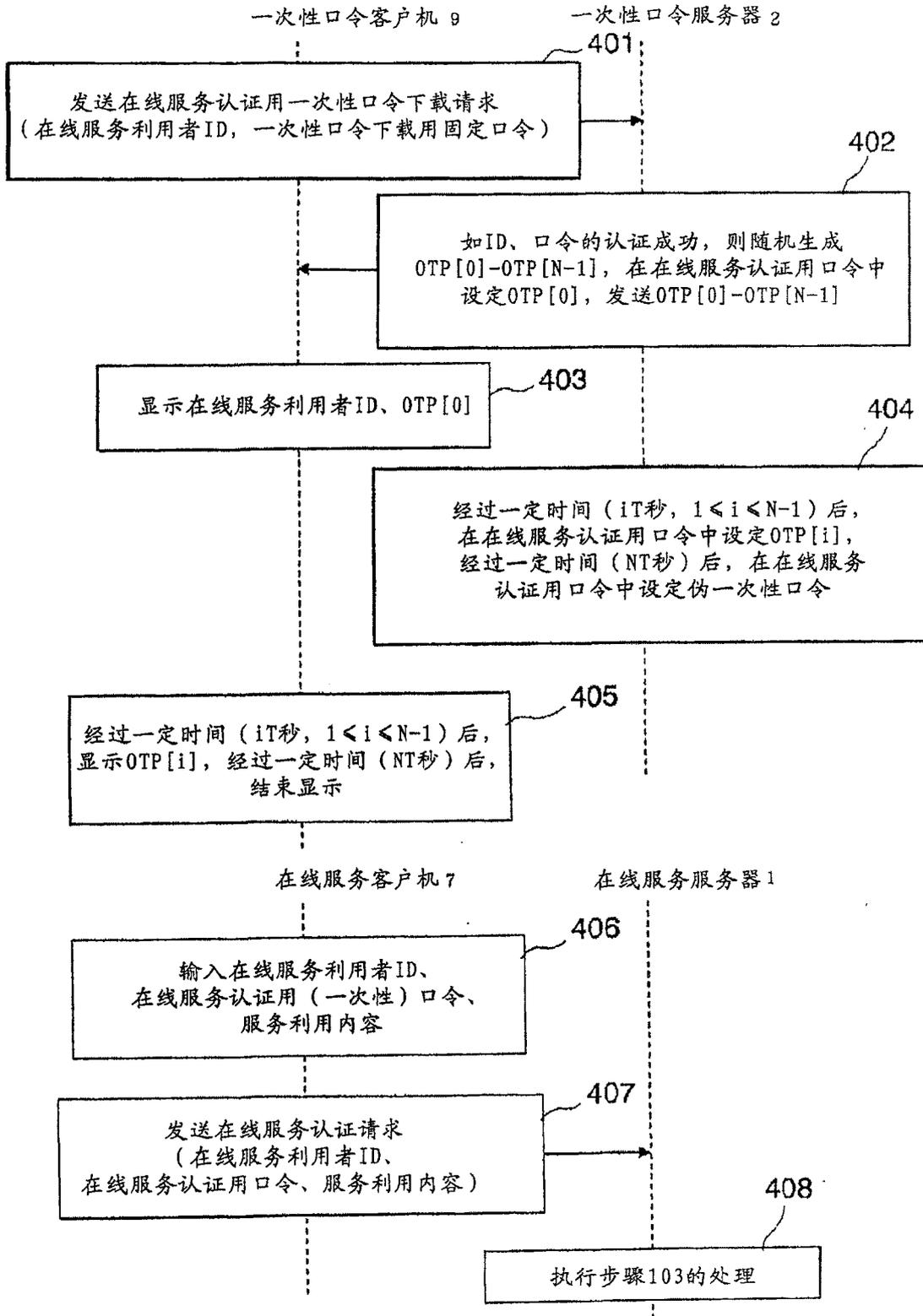


图 4

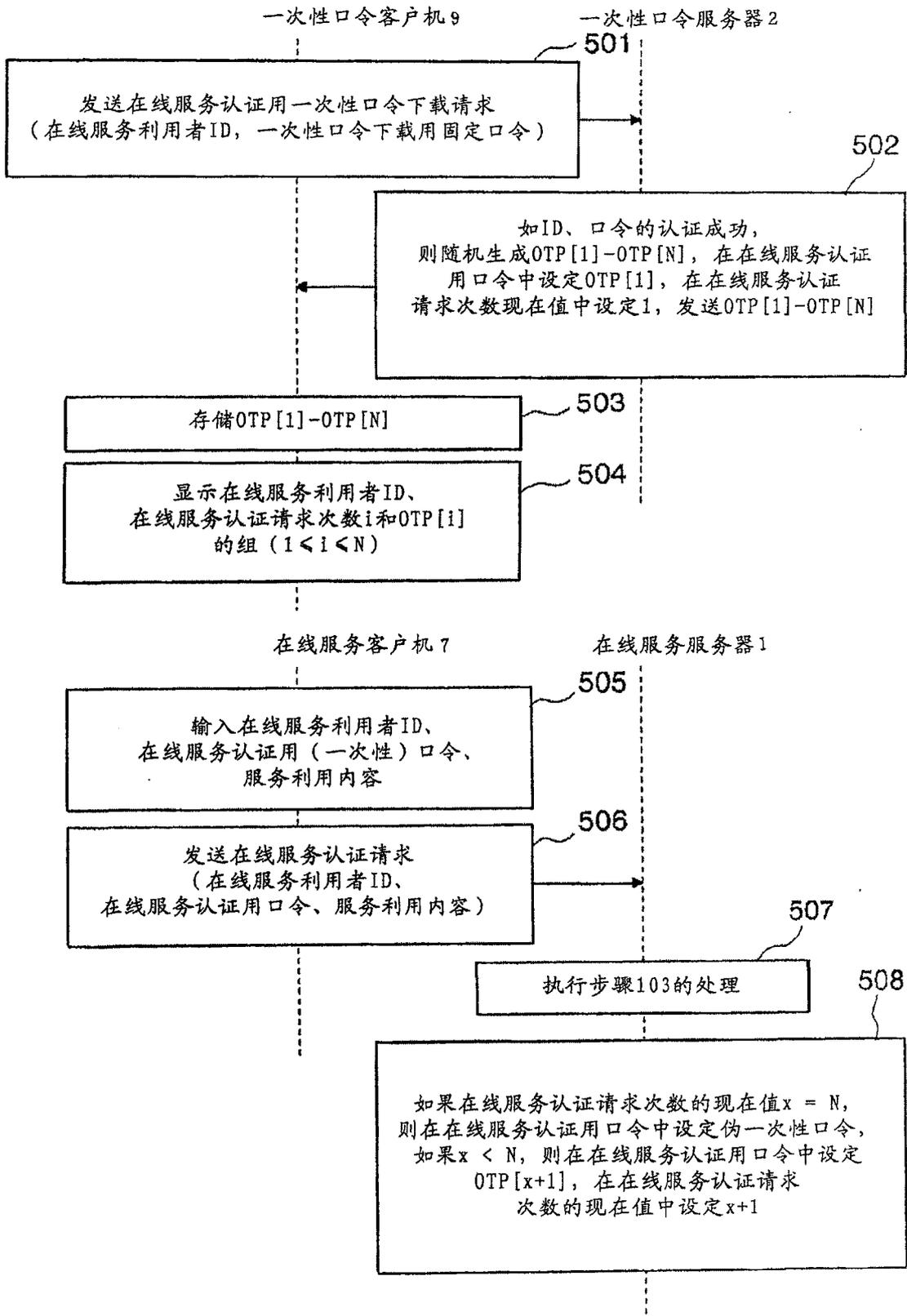


图 5

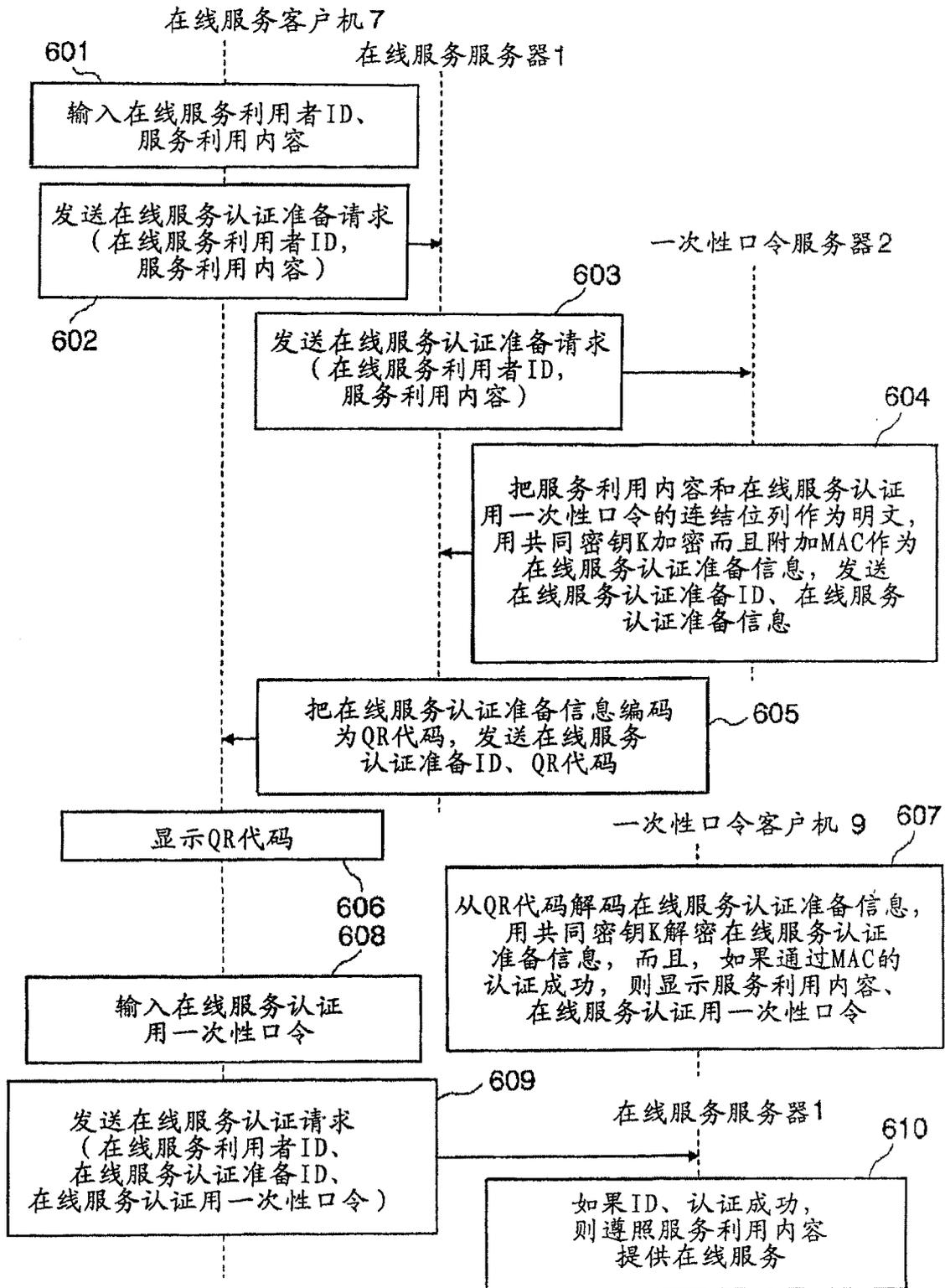


图 6