(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 107077559 B
(45)授权公告日 2019.09.03

(21)申请号 201580056707.7

(22)申请日 2015.09.08

(65)同一申请的已公布的文献号
申请公布号 CN 107077559 A

(43)申请公布日 2017.08.18

(30)优先权数据
PCT/JP2014/073704 2014.09.08 JP

(85)PCT国际申请进入国家阶段日
2017.04.19

(86)PCT国际申请的申请数据
PCT/JP2015/075391 2015.09.08

(87)PCT国际申请的公布数据
WO2016/039309 JA 2016.03.17

(73)专利权人 帕斯罗基株式会社
地址 日本东京

(72)发明人 小川秀治

(74)专利代理机构 北京市浩天知识产权代理事务所(普通合伙) 11276
代理人 刘云贵

(51)Int.Cl.
*G06F 21/45*(2006.01)

(56)对比文件
US 2013170638 A1,2013.07.04,
JP 2002366517 A,2002.12.20,
CN 103270732 A,2013.08.28,
JP 2009301446 A,2009.12.24,
CN 103270732 A,2013.08.28,
WO 2013070124 A1,2013.05.16,
US 2010107229 A1,2010.04.29,

审查员 罗捷

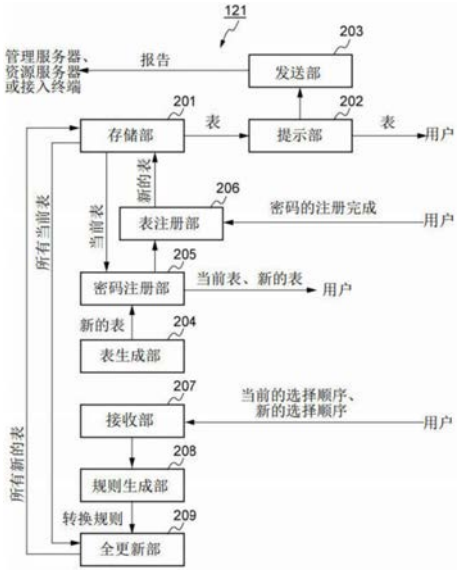
权利要求书3页 说明书28页 附图20页

(54)发明名称

# 认证系统、提醒终端、以及信息记录介质

(57)摘要

在提醒终端(121)中,表生成部(204)生成具有在各要素中包括的随机的字符串的表。密码注册部(205)促使用户辨识表,将注册用字符串作为密码并将其注册在资源服务器中,该注册用字符串是将以用户用的选择顺序从表提取的要素中包括的字符串进行排列而得到的。存储部(201)存储表。提示部(202)通过来自用户的指示将表提示给用户,且促使将认证用字符串作为利用资源服务器的资源的请求的密码,该认证用字符串是将以用户用的选择顺序从表中提取的要素中包括的字符串进行排列而得到的。利用发送部(203)也可以发送表已被提示给用户的消息的报告。如果将报告的目的地设为与资源服务器进行协作的管理服务器,则可以将对用户提示了表的情况加入到利用资源服务器的资源的条件中。




CN 107077559 B

1.一种认证系统,包括提醒终端、资源服务器、管理服务器以及接入终端,其中,

(A)所述提醒终端包括:

表生成部,生成具有在各要素中包括的字符串的表,所述字符串是随机生成的;

密码注册部,使用户辨识所述生成的表,以及促使所述用户进行下述动作,

(1)按对所述用户预先分配的选择顺序从所辨识的表中提取要素,以及将所提取的要素中包括的字符串进行排列,以得到注册用字符串,

(2)将所得到的注册用字符串更新或注册或新近注册为所述用户的用户名在所述资源服务器的密码;

存储部,将所述资源服务器具有的资源服务器名及所述用户名的组合与所述辨识的表相关联地进行存储;

提示部,当通过来自所述用户的指示选择所述组合时,将与所述组合相关联地存储的所述表提示给所述用户,以及促使所述用户进行下述动作,

(a)按预先对所述用户分配的选择顺序从所提示的表中提取要素,以及将所提取的要素中包括的字符串进行排列,以得到认证用字符串,

(b)将得到的认证用字符串用于通过所述用户名利用所述资源服务器的资源的请求的密码;

发送部,发送与所述组合相关联地存储的所述表已提示给所述用户的消息的报告,

(B)所述管理服务器,

当由所述管理服务器接收从所述提醒终端发送的所述报告时,设定与所述报告相关的组合对应的有效时间段,所述有效时间段包含所述管理服务器接收所述报告的时间点,

(C)所述资源服务器,

当通过所述用户名利用所述资源服务器的资源的请求被从所述接入终端发送到所述资源服务器且与所述请求相关的密码与在所述资源服务器中对于所述用户名注册的密码一致时,向所述管理服务器发送与所述用户名相关的询问,

(D)所述管理服务器,

当所述询问被所述管理服务器接收时,判定许可条件“在对于作为所述询问的发起者的资源服务器的服务器名及所述询问相关的用户名的组合设定的有效时间段内,所述管理服务器接收到所述询问”是否成立,并将指示了所述判定的结果的回答发送给所述资源服务器,

(E)所述资源服务器,

如果所述回答被所述资源服务器接收,以及所接收到的回答指示所述许可条件成立,则将用于利用所述资源服务器的资源的响应发送到所述接入终端。

2.根据权利要求1所述的认证系统,其特征在于,

如果所述接入终端和所述提醒终端通过在规定的距离内建立的有线连接或无线连接可通信地连接,则所述报告经由所述有线连接或所述无线连接被发送到所述接入终端,

如果用于从所述接入终端输入与利用所述资源服务器的资源的请求有关的用户名及密码的登录框显示在所述接入终端的画面上,并且与在所述提醒终端选择的组合有关的服务器名是所述资源服务器的服务器名,则所述接入终端将与所述选择的组合相关的用户名输入所述登录框的用户名栏,

所述提醒终端使所述用户从所述提示的表中选择要素，

所述提醒终端通过将在所述选择的要素中包括的字符串进行排列，得到传递用字符串，

所述提醒终端将所得到的传递用字符串经由所述有线连接或所述无线连接传递到所述接入终端，

所述接入终端将从所述提醒终端传递的传递用字符串输入所述登录框的密码栏。

3.根据权利要求2所述的认证系统，其特征在于，

所述提醒终端以所述表的各要素中包括的字符串被隐藏的方式来提示所述表，

所述提醒终端通过与所述资源服务器时间同步的加密方式，对所述选择的要素中包括的字符串进行加密，以获得所述传递用字符串，

所述资源服务器，如果通过所述加密方式将与所述请求相关的认证用字符串进行解密后所得的已解密字符串和对所述用户名注册的密码一致，则确定与所述请求相关的密码与对所述用户名注册的密码一致。

4.根据权利要求3所述的认证系统，其特征在于，

每次所述用户从所述提示的表中选择所述要素时，所述提醒终端将所选择的要素中包括的字符串通过所述加密方式加密后传递给所述接入终端，

每次从所述提醒终端传递了所述加密了的字符串时，所述接入终端在所述登录框的密码栏附加地输入所传递来的所述加密了的字符串。

5.根据权利要求4所述的认证系统，其特征在于，

所述提醒终端，

生成所述表，并且以与在所述表的各要素中包括的字符串的类型不同的类型随机地生成包括在附加要素中的字符，

对用户呈现所生成的表以及所生成的附加要素以使所述用户辨识所述表，

所述注册用字符串以及所述认证用字符串是通过将所述提取的要素以及所述附加要素中包括的字符串进行排列而分别得到的。

6.根据权利要求4所述的认证系统，其特征在于，

在与所述组合相关联地存储了所述表之后，经过了与所述组合相关的资源服务器相关联的更新时间段时，

所述表生成部生成新的表，

所述密码注册部使所述用户辨识所述生成的新的表，并使所述用户进行下述动作，

(1)按对所述用户预先分配的选择顺序从所辨识的新的表中提取要素，将所提取的要素中包括的字符串进行排列，以得到新的注册用字符串，

(2)更新以及注册所得到的新的注册用字符串作为针对与所述组合相关的用户名在所述资源服务器的密码，

所述提醒终端还包括表注册部，所述表注册部在与所述组合相关联的存储部中存储所述新的表。

7.根据权利要求4所述的认证系统，其特征在于，还包括：

接收部，从所述用户接收对所述用户预先分配的选择顺序的输入和要对所述用户新分配的选择顺序的输入；

规则生成部,当接收到所述输入时,生成如下转换规则,

(s)将按所述预先分配的选择顺序提取的要素的内容移动到要按所述新分配的选择顺序提取的要素,

(t)将按所述预先分配的选择顺序提取的要素以外的要素的内容随机移动到要按所述新分配的选择顺序提取的要素以外的要素;

全更新部,通过所述生成的转换规则转换存储于所述存储部的表,更新存储于所述存储部的所有的表。

8.根据权利要求7所述的认证系统,其中,

所述提醒终端,

在通过所述接收部进行接收之前,生成具有与所述选择顺序的长度相同长度并且不含重复的字符的引导字符串,

所述接收部,

(u)通过由所述用户从表中选择要素,接收对所述用户预先分配的选择顺序的输入,每次所述要素被选择时,在该要素显示与所述生成的引导字符串内的选择顺序相关联的字符,

(v)通过由所述用户从表中选择要素,接收要对所述用户新分配的选择顺序的输入,每次所述要素被选择时,在该要素显示与所述生成的引导字符串内的选择顺序相关联的字符,

所述全更新部通过在所述表内的位置中进行下列(x)和(y)处理来对所述表内的各位置分配引导字符:

(x)向要按对所述用户新分配的选择顺序选择的位置分配与所述引导字符串内的选择顺序相关联的字符,

(y)在按对所述用户新分配的选择顺序选择的位置以外的位置随机而不重复地分配字符,

所述提示部在将与多个资源服务器相关联的表中的任一个表提示给所述用户时,将对该表内的各位置分配的引导字符以及各位置的要素提示给所述用户。

9.根据权利要求1所述的认证系统,其中,

所述资源服务器和所述管理服务器通过单个服务器计算机实现。

10.一种存储有程序的非易失性计算机可读信息记录介质,其中,

所述程序使计算机用作权利要求4所述的提醒终端的各部分。

# 认证系统、提醒终端、以及信息记录介质

## 技术领域

[0001] 本发明涉及适于通过提醒终端来管理用于决定针对利用资源服务器的资源的请求的可否的密码的认证系统、该提醒终端、以及使计算机作为该提醒终端起作用的存储有程序的非临时性计算机可读信息记录介质。

## 背景技术

[0002] 目前，为了决定资源服务器提供的资源可否使用，利用用户输入密码的系统。作为这里提供的资源，可以有各种文件的收发及保存、邮件、新闻、静态图像、视频、音乐等的阅览及视听、各种应用的使用等各种形态。

[0003] 在此，资源服务器为了决定可否使用资源而存储密码自身、或对密码应用单向哈希函数而随机化的字符串。此外，也使用在对密码附加了为每一被称作盐(ソルト)的用户决定的字符串后应用哈希函数的方法。在利用单向哈希函数的情况下，不对比密码字符串自身而将用户输入的密码的哈希值和存储于资源服务器内的哈希值进行对比，由此确认密码的一致，进行认证。

[0004] 通常，资源服务器由各种服务提供商运营，因此，有时资源服务器的结构或设定不同，基于该差异，产生安全性上的差异。因此，有时某一资源服务器会受到攻击、或员工泄漏安全性信息、或因用户自身的不注意而泄漏信息，致使密码泄漏。

[0005] 在此，在多个资源服务器中利用同一密码的情况下，当其中的一个资源服务器的密码泄漏时，其它资源服务器也可能会被不正当访问。因此，期望密码在每个资源服务器中不同。

[0006] 另外，已知有将装载于词典的字符串等作为密码按顺序输入，尝试向资源服务器登录的暴力攻击。因此，期望密码由随机生成的字符串构成。但是，这种字符串对于人们来说难以记忆。

[0007] 在此，作为管理对于每一资源服务器都不同的多个难以记忆的密码的技术，提案有下述文献中公开的技术。

[0008] 现有技术文献

[0009] 专利文献

[0010] 专利文献1:日本特开2007-108833号公报

[0011] 专利文献2:国际公开第WO2012/029776号

[0012] 发明所要解决的课题

[0013] 这些技术中，用户在管理密码的提醒用设备中输入一个主密码或密钥，由此得到各资源服务器用的密码。但是，目前期望不直接输入主密码或密钥而得到各资源服务器用的密码，维持各资源服务器用的密码的随机性的技术。

## 发明内容

[0014] 本发明是用于解决上述那种课题的发明，其目的在于，提供适于通过提醒终端来

管理用于决定针对利用资源服务器的资源的请求的可否的密码的认证系统、该提醒终端、以及使计算机作为该提醒终端起作用的存储有程序的非临时性计算机可读信息记录介质。

[0015] 用于解决课题的技术方案

[0016] 本发明的认证系统包括提醒终端、资源服务器、管理服务器以及接入终端，

[0017] (A)上述提醒终端包括：

[0018] 表生成部，生成具有在各要素中包括的字符串的表，上述字符串是随机生成的；

[0019] 密码注册部，使用户辨识上述生成的表，以及促使上述用户进行下述动作，

[0020] (1)按对上述用户预先分配的选择顺序从上述辨识的表中提取要素，以及将上述提取的要素中包括的字符串进行排列，由此得到注册用字符串，

[0021] (2)将所得到的注册用字符串更新或注册或新近注册为所述用户的用户名在所述资源服务器的密码；

[0022] 存储部，将上述资源服务器具有的资源服务器名及上述用户名的组合与上述辨识的表相关联地进行存储；

[0023] 提示部，当通过来自上述用户的指示选择上述组合时，将与上述组合相关联地存储的上述表提示给上述用户，以及促使上述用户进行下述动作，

[0024] (a)按预先对上述用户分配的选择顺序从所提示的表中提取要素，以及将所提取的要素中包括的字符串进行排列，以得到认证用字符串，

[0025] (b)将得到的认证用字符串用于通过上述用户名利用上述资源服务器的资源的请求的密码；

[0026] 发送部，发送与上述组合相关联地存储的上述表已提示给上述用户的消息的报告，

[0027] (B)上述管理服务器，

[0028] 当由上述管理服务器接收从上述提醒终端发送的上述报告时，设定与上述报告相关的组合对应的的有效时间段，上述有效时间段包含上述管理服务器接收上述报告的时间点，

[0029] (C)上述资源服务器，

[0030] 当通过上述用户名利用上述资源服务器的资源的请求被从上述接入终端发送到上述资源服务器且与上述请求相关的密码与在上述资源服务器中对于上述用户名注册的密码一致时，向上述管理服务器发送与上述用户名有关的询问，

[0031] (D)上述管理服务器，

[0032] 当上述询问被上述管理服务器接收时，判定许可条件“在对于上述询问的发起者的资源服务器的服务器名及上述询问相关的用户名的组合设定的有效时间段内，上述管理服务器接收到上述询问”是否成立，并将指示了上述判定的结果的回答发送给上述资源服务器，

[0033] (E)上述资源服务器，

[0034] 如果上述回答被上述资源服务器接收，以及所接收到的回答指示上述许可条件成立，则将用于利用上述资源服务器的资源的响应发送到上述接入终端。

[0035] 本发明的提醒终端是满足上述认证系统的上述的要件(A)的提醒终端。本提醒终端将表示与基于用户的选择而提示的表相关联的资源服务器名和用户名的组合的报告发

送给其它设备，因此，可以在认证时参照该组合。本提醒终端例如可以作为安全令牌利用。

[0036] 发明效果

[0037] 根据本发明，可以提供适于通过提醒终端来管理用于决定针对利用资源服务器的资源的请求的可否的密码的认证系统、该提醒终端、以及使计算机作为该提醒终端起作用的存储有程序的非易失性计算机可读信息记录介质。

## 附图说明

[0038] 图1是表示本发明实施例的认证系统的概要的说明图；

[0039] 图2是表示本发明实施例的提醒终端的概要的说明图；

[0040] 图3A是表示在本发明实施例的提醒终端显示表的情况的说明图；

[0041] 图3B是表示在本发明实施例的提醒终端显示表的情况的说明图；

[0042] 图4是表示本发明实施例的选择顺序的例子的说明图；

[0043] 图5是说明本发明实施例的认证系统的信息交换的情况的说明图；

[0044] 图6是表示本发明实施例的登录框的浏览器的情况的说明图；

[0045] 图7是表示在本发明实施例的用于更新密码而显示的表的情况的说明图；

[0046] 图8A是表示由用户选择当前使用的选择顺序的情况的说明图；

[0047] 图8B是表示由用户选择当前使用的选择顺序的情况的说明图；

[0048] 图8C是表示由用户选择当前使用的选择顺序的情况的说明图；

[0049] 图8D是表示由用户选择当前使用的选择顺序的情况的说明图；

[0050] 图8E是表示由用户选择当前使用的选择顺序的情况的说明图；

[0051] 图9A是表示由用户选择新的选择顺序的情况的说明图；

[0052] 图9B是表示由用户选择新的选择顺序的第一个的情况的说明图；

[0053] 图9C是表示由用户选择新的选择顺序的第二个的情况的说明图；

[0054] 图9D是表示由用户选择新的选择顺序的第三个的情况的说明图；

[0055] 图9E是表示由用户选择新的选择顺序的第四个的情况的说明图；

[0056] 图10是表示由新的选择顺序更新的表的情况的说明图；

[0057] 图11是表示由新的选择顺序更新其它表的前后的情况的说明图。

## 具体实施方式

[0058] 以下，说明本发明的实施方式。此外，本实施方式是用于说明的实施方式，不限定本申请发明的范围。因此，只要是本领域技术人员，则可以采用将这些要素或所有要素置换为等同物的实施方式，这些实施方式也包含在本发明的范围内。

[0059] 实施例1

[0060] 图1是表示本发明的实施例的认证系统的概要的说明图。以下，参照本图进行说明。

[0061] 本实施例的认证系统101包括提醒终端121、接入终端141、资源服务器161、管理服务器181。典型地，相对于多个资源服务器161准备1台管理服务器181。但是，各资源服务器161也可以构成为同时实现管理服务器181的功能，而省略独立的管理服务器181。另外，作为资源服务器161，可以仅采用基于现有的用户名及密码的合法认证，也可以省略管理服务

器181自身。

[0062] 这些设备可经由因特网、移动电话通信网络、Wi-Fi(Wireless Fidelity)等无线LAN(Local Area Network)等计算机通信网络191相互通信。此外，资源服务器161和管理服务器181之间的通信也可以利用专用线路。另外，也可以对通信实施各种加密。

[0063] 提醒终端121将实现用户利用各资源服务器161的资源的密码以仅该用户可知的即第三者仅偷看而不能马上窃取密码的方式提醒给该用户的功能。典型地，作为提醒终端121，可以利用各种便携终端、例如手机、智能手机、平板电脑、PDA(Personal Data Assistant)、可穿戴终端等。

[0064] 接入终端141是用于用户利用资源服务器161的资源的终端。典型地，用户为了利用资源服务器161的资源而从在接入终端141上动作的浏览器访问资源服务器161。作为接入终端141，可以利用各种台式电脑或X终端虚拟终端。另外，作为接入终端141，也可以利用与提醒终端121相同的设备。

[0065] 资源服务器161对用户提供资源的利用服务。资源服务器161通过从接入终端141取得用户在接入终端141输入的密码并进行是否具有利用权限的认证而决定用户可否进行资源的利用。此外，认证也可以利用在接入终端141输入的用户名，但也可以使用接入终端141自身的识别信息(例如通信用的MAC(Media Access Control)地址、CPU(Central Processing Unit)的制造编号、预先保存于接入终端141的cookie中所含的会话ID等)来代替用户名。

[0066] 对资源服务器161分配资源服务器名。资源服务器名通过作为资源服务器161起作用的计算机的服务器ID(IDentifier)、例如主机名、IP(Internet Protocol)地址、域名、成为提供资源的窗口的URL(Universal Resource Locator)等表现。

[0067] 管理服务器181在资源服务器161进行的认证中，可以参照提醒终端121的利用状况。

[0068] (概要)

[0069] 以下，说明本发明的典型的方式的概要。提醒终端121对应于各资源服务器161的服务器名及用户在该各资源服务器161中使用的用户名的组合，生成具有在各要素中包括的随机的字符串的表并存储。

[0070] 该表在用户于各资源服务器161中进行帐户的新注册时、或用户更新各资源服务器161中的已有帐户的密码时由提醒终端生成，提醒终端121使用户辨识所生成的表。

[0071] 另外，在用户要利用各资源服务器161的资源时(要登录或进入时)，提醒终端121也根据用户所选择的资源服务器名和用户名的组合来对用户提示存储于提醒终端121内的表。

[0072] 该表的基本方式是，仅在提醒终端121内被管理，其内容本身不被各资源服务器161或管理服务器181知道。虽然可以相对于各资源服务器161或管理服务器181进行表的备份，但在该情况下，期望在将表适宜加密后进行备份。

[0073] 用户开始使用提醒终端121时，决定一个自己用的选择顺序。该选择顺序在被提醒终端121管理的全组合中被共通使用。该选择顺序自身的基本方式也是其内容自身不被各资源服务器161或管理服务器181知道。

[0074] 用户在某一资源服务器161中要以某一用户名进行新注册时，在提醒终端121输入

该资源服务器161的服务器名及该用户使用的用户名的组合。于是，提醒终端121生成表，使用户辨识该表。

[0075] 用户从所辨识的表中通过自身决定的选择顺序提取要素，将所提取的要素中包括的字符串进行排列。在此得到的字符串为相对于该资源服务器的新注册时输入的注册用密码。

[0076] 用户从接入终端141接入资源服务器161，输入通过辨识用户名和提醒终端121而得到的注册用密码，进行帐户的新注册。

[0077] 由此，因为帐户的新注册完成，所以将与资源服务器名和用户名的组合对应的表存储在提醒终端121内的非易失性存储介质中，今后在要利用资源服务器161的资源时，可以确认其内容。

[0078] 在用户要利用资源服务器161的资源时，相对于提醒终端121选择资源服务器161的资源服务器名和用户名的组合。于是，提醒终端121向用户提示与该组合相关联地存储的表。

[0079] 用户通过从所提示的表中以自身决定的选择顺序提取要素，并将所提取的要素中包括的字符串进行排列，以得知认证用字符串。

[0080] 然后，用户经由接入终端141访问资源服务器161的登录框，将用户名及认证用字符串作为密码输入，对资源服务器161进行登录的请求。

[0081] 资源服务器161判定请求的用户名和密码的组合是否合适。该判定可以采用通常的密码认证的技术。

[0082] 另外，本实施例中，提醒终端121具有在对用户提示了与该组合对应的表后，将该消息报告给外部的设备的特征。由此，外部的设备可以得知提醒终端121的所有者以也包含该组合的用户名在具有该组合的资源服务器名的资源服务器161中进行了登录。

[0083] 在将该报告发送给管理服务器181的方式中，可以将提醒终端121作为安全令牌利用。

[0084] 管理服务器181接收到报告时，对该报告的资源服务器名及用户名的组合设定包含接收到报告的时间点的有效时间段。该有效时间段为例如从报告接收时起至报告接收后5分钟的时间段等极短的时间段。

[0085] 另一方面，在接收到来自接入终端141的登录请求的资源服务器161判定为请求的用户名和密码的组合为合适时，资源服务器161对管理服务器181发送指示自身的资源服务器名和要登录的用户名的询问。

[0086] 管理服务器181在接收到询问时，判定许可条件是否成立。本方式中，作为许可条件，采用“在对于该询问相关的资源服务器名以及用户名的组合设定的有效时间段内由管理服务器181接收到该询问”。这意味着，许可条件成立实质上意味着：在用户向资源服务器161发出请求时，通过提醒终端121观看了资源服务器161用的表。而且，管理服务器181将指示将许可条件的成立与否的回答发送给资源服务器161。

[0087] 资源服务器161基于从管理服务器181接收到的回答的合适与否而判定可否利用登录请求的资源。即，在用户名和密码的组合是合适的组合、最近在提醒终端121上显示了分散地嵌入有密码的表的这两个条件成立的情况下，资源服务器161允许利用资源。因此，在该方式中，可以将提醒终端121作为安全令牌利用。

[0088] 该方式中，期望将提醒终端121的设备信息以及使用提醒终端121的用户自身的个人信息预先注册在管理服务器181中。如果保证附带于提醒终端121的用户的个人信息被管理服务器181管理，则在向资源服务器161新注册时，不需要将用户的个人信息交接给资源服务器161。即，可以进行下述运用，个人信息被管理服务器181管理，只要在资源服务器161中不产生任何事故，就不从管理服务器181向资源服务器161公开个人信息。该运用有助于隐私的保护，因此，提高用户登录的可能性。

[0089] 这样，因为在表的各要素中包括有随机的字符串，所以将要得到的注册用字符串或认证用字符串也是随机的，并且针对资源服务器名及用户名的每一组合生成表，因此，注册用字符串或认证用字符串在资源服务器彼此之间很少重复。

[0090] 因此，用户如果仅存储自身的选择顺序，则可以将随机的密码在多个资源服务器161中不重复地利用。

[0091] 相反，即使提醒终端121被盗、或者存储于提醒终端121的表被偷看，只要不知道用户的选择顺序，就不会泄漏针对各资源服务器161的密码。因此，可以安全地管理密码。

[0092] 此外，也可以采用使插件程序在接入终端141的浏览器中动作，由接入终端141接收来自根据无线通信或有线通信的状况被确认到存在于接入终端141的附近的提醒终端121的报告这种方式。该方式也可以适用于省略了管理服务器181的结构，即资源服务器161也可以适用于仅通过用户名和密码来决定可否请求的方式。后述该方式。

[0093] 以下，详细说明本实施例的各部的动作。

[0094] (提醒终端)

[0095] 图2是表示本发明实施例的提醒终端的概要的说明图。以下，参照本图进行说明。

[0096] 提醒终端121包括存储部201、提示部202。另外，作为可省略的要素，也可以包括发送部203、表生成部204、密码注册部205、表注册部206、接收部207、规则生成部208、全更新部209。此外，通过缓和表共享上的制约，省略的要素的功能也可以由管理服务器181接管。

[0097] 在存储部201与资源服务器161所具有的资源服务器名、及用于对该资源服务器161访问的用户名的组合相关联地存储表。在各表的各要素中存储随机生成的信息(各种字符、数字、记号、图形、它们的列等。)。另外，各表中，还在栏外设置附加要素。附加要素中可以包括随机生成的信息，也可以在首次注册时由用户自己决定，也可以省略。

[0098] 存储于存储部201的表由提示部202基于用户的选择显示于提醒终端121的画面上。为了使安全性最高，该表仅存储于提醒终端121，优选完全不与资源服务器161和管理服务器181共享。该情况下，如果对资源服务器161或管理服务器181备份存储于提醒终端121的表，则被适宜实施加密，即使是资源服务器161或管理服务器181，只要未从用户明确得到用于从备份恢复表的许可以及恢复所需的加密密钥等，就不能知道表。

[0099] 另一方面，如后述，虽然说是最高的安全性，但为了考虑用户的便利性并确保妥当的安全性的高度，也可以放松表的共享限制，由提醒终端121和管理服务器181协作进行表的备份或密码的自动更新等作业。

[0100] (表)

[0101] 图3A是表示在本发明实施例的提醒终端显示表的情况的说明图。图3B是表示在本发明实施例的提醒终端显示表的情况的说明图。以下，参照这些图进行说明。

[0102] 与各资源服务器161的服务器名及在该资源服务器161中使用的用户名的组合相

关联地存储于存储部201的表301由规定行数及列数的要素构成，如上述，在各要素中存储有通过提醒终端121随机生成的字符串的信息。

[0103] 在提醒终端121中，与表301一同，在画面上显示通过资源服务器161的IP地址或URL等表现的服务器ID 303(这些图中示例有“xxx.yyy.com”，服务器ID 303相当于资源服务器名。)、该用户访问该资源服务器161时利用的用户名304(这些图中示例有“john2014”。)、可省略的附加要素305。这些信息在存储部201被相互关联地存储。

[0104] 此外，在以下的说明中，为了使文言简洁且容易理解，以资源服务器名或服务器ID为代表适宜说明资源服务器名和用户名的组合。

[0105] 这些图所示的例子中，表301以5行5列构成。图3A中，在表301的各要素中包括随机生成的小写字母2字符。图3B中，在表301的各要素中包括随机生成的平假名1字符、和将其用小写字母表示的罗马字母拼音。此外，罗马字母拼音的显示可以省略。

[0106] 如上述概要中所说明，在本实施例中，代替现有技术中的主密码而利用对表301的各要素进行选择的选择顺序。

[0107] (选择顺序)

[0108] 图4是表示本发明实施例的选择顺序的例子的说明图。以下，参照本图进行说明。

[0109] 本图中，表示以在表301的右下部沿着粗黑箭头描绘对钩的方式选择四个要素的选择顺序。本图所示的选择顺序中，按4行2列的要素、5行3列的要素、4行4列的要素、3行5列的要素的顺序提取四个要素。按哪一顺序提取几个要素可以根据请求的安全性的等级或用户的熟练度等适宜变更。

[0110] 在相对于图3A所示的例子应用图4所示的选择顺序提取要素时，成为“bp”“pp”“js”“ld”。如果将它们排列则成为“bpppjsld”。在没有附加要素305的情况下，该“bpppjsld”成为通过服务器ID 303识别的资源服务器161用的密码。在图3A所示的例子中，因为存在“#X5”这种附加要素305，所以“bpppjsld”之后连结有附加要素的“bpppjsld#X5”成为密码。

[0111] 在图3A所示的例子中，在表301的各要素中均包括有小写字母的字符串。但是，根据资源服务器161的策略，有时也禁止使用仅由小写字母构成的密码。

[0112] 附加要素305用于与可作为密码利用的字符种类的限制对应。例如，相对于采用均包含大写字母、小写字母、数字、记号的这种策略的资源服务器161，作为附加要素305，通过准备大写字母、数字、记号来进行对应。如上述，也可以不利用附加要素305。

[0113] 在相对于图3B所示的例子应用图4所示的选择顺序时，密码成为“ちたごわ”。作为密码可利用平假名的资源服务器161中，只要将该字符串直接作为密码输入即可，但可作为密码利用的字符的种类多被限定在可通过ASCII码32-126表现的字母、数字、记号。该情况下，通过将附注示于各要素的罗马字母拼音排列，得到密码“titagowa”。进而，在本图中，因为有附加要素305“#X5”，所以密码成为“titagowa#X5”。

[0114] 此外，表301的各要素不限于小写字母的字符串，例如可以利用大写字母、小写字母、数字、记号等、任意的信息。

[0115] 本实施例中，用户为了容易记忆用户的选择顺序，以对于被提醒终端121管理的所有表301共通的方式，不与各要素的位置重复地分配引导字符。引导字符可以省略。在图3A及图3B所示的例子中，引导字符在各要素的右上角以大写字母缩小显示。

[0116] 引导字符可以在显示表301时必须显示，也可以基于用户的指示进行显示。例如，当用户通过摇动提醒终端121等而赋予指示时，使引导字符显示数秒～数十秒。

[0117] 图3A及图3B所示的例子中，对5行5列的25个要素不重复地分配大写字母。对4行2列的要素、5行3列的要素、4行4列的要素、3行5列的要素分别分配“D”“I”“C”“E”，用户也可以将自己的选择顺序首先通过英文单词“DICE”进行存储。在充分掌握了选择顺序后，不显示引导字符，仅通过浏览表301，用户即可按照自己的选择顺序扫描表301内的要素。

[0118] 排列相对于对用户分配的选择顺序的引导字符而得到的引导字符串优选为一定程度上容易存储的字符串。例如，在开始使用提醒终端121时，提醒终端121将空白的表提示给用户并按照用户决定的选择顺序选择要素。而且，提醒终端121从词典中适当选出、或者由用户决定以所选择的要素的数为长度的单词，并对按选择顺序提取的要素按顺序分配该单词中所含的字符。对于其它的要素，只要随机不重复地分配其它的字符即可。

[0119] 另外，从安全性的观点出发，针对每一资源服务器使密码不同，该密码优选未载入词典中的字符串，但用户难以记住如此大量的密码。因此，如上述，在本方式中，用户存储自己的选择顺序。

[0120] 而且，将各资源服务器161用的表301在画面上显示后，用户浏览该表，按对用户分配的选择顺序提取要素，将所提取的要素的内容进行排列、以及适宜追加附加要素305，由此，得到密码。表301的各要素是随机的，因此，得到的密码在安全性上是优选的随机的字符串。

[0121] 本方式中，各资源服务器161用的密码被分割并包括在基于该用户的选择顺序从表301选择的要素中，且根据需要包括在附加要素305中。即，提醒终端121将随机的秘密信息打乱存储于其它随机的伪信息中。因此，仅偷看显示于提醒终端121的画面上的表301，不能窃取密码。因此，可以安全地管理随机的密码。

[0122] 此外，在图3A、及图3B所示的例子中，显示有用于选择资源服务器161的服务器名的导航311、用于检索表的历史的导航312、用于切换用户名的导航313，通过用户操作导航311、312，可以切换资源服务器名与用户名的组合而对其它资源服务器161用的信息切换显示、或者在该资源服务器161检索以前利用的表的历史。它们的UI(User Interface)可以适宜变更。

[0123] 在本图的例子中，导航311、313是服务器ID 303或用户名304的显示栏的列表框，当选择该显示栏时，显示注册于提醒终端121的服务器ID或该资源服务器中的用户名的一览。用于打开列表框的导航311在有其它候补的情况下，用黑色的三角形表示(服务器ID 303)，在没有其它候补的情况下，用白色的三角形表示(用户名304)。用户从其中选择所希望的导航。导航312在显示用于表示表被利用的时间段的条并点击或单击该条时，切换在该时间段利用的表的显示/非显示。在显示中的条上，在开头显示十字标记，在关闭的条上，在开头显示白四角。另外，通过对画面进行点击操作或拖动操作，可以进行滚动，也可以观看在第一视图上未显示的历史。

[0124] 可省略的要素即发送部203将对用户提示了表301的消息的报告发送给外部的设备。通过该结构，作为用于用户访问某一资源服务器161的必要条件，可以采用将该资源服务器161用的表301通过提醒终端121提示给该用户。该结构中，提醒终端121除实现管理密码的作用外，还作为认证用令牌起作用。

[0125] 各资源服务器161用的密码、以及对用户分配的选择顺序在适宜的时机或基于用户的意思进行更新。后述它们的方式。

[0126] (信息的交换)

[0127] 图5是表示本发明实施例的认证系统的信息的交换的情况的说明图。以下,参照本图进行说明。

[0128] 用户在接入终端141的浏览器等中指定资源服务器161的识别信息(例如URL)时(350),从接入终端141向资源服务器161发送访问请求(351)。

[0129] 接收到访问请求的资源服务器161,作为针对该访问请求的响应,向接入终端141发送登录框(352)。

[0130] 由接入终端141接收到的登录框在接入终端141的浏览器等中显示(353)。

[0131] 图6是表示显示本发明实施例的登录框的浏览器的情况的说明图。以下,参照本图进行说明。在接入终端141的浏览器501中,在URL栏502显示资源服务器161的URL,在内容栏503显示登录框511。在登录框511上配置有用户名栏512、密码栏513、及登录按钮514。另外,在浏览器501还显示有用于执行所安装的插件进行的处理的插件图标521。

[0132] 在此,用户为了得到资源服务器161用的密码而在便携终端等启动提醒应用。于是,该便携终端等开始作为提醒终端121起作用。提醒终端121基于用户的选择(354)在提醒终端121的画面上提示(355)对资源服务器161的服务器名及用户名的组合分配的表301等。

[0133] 而且,提醒终端121将对用户提示了表301等消息的报告发送(356)给管理服务器181。管理服务器181相对于该用户及该资源服务器161,对该报告的资源服务器名及用户名的组合设定包含接收到该报告的时间点的有效时间段。作为有效时间段,例如考虑“接收报告后5分钟以内”等。

[0134] 用户将自己的用户名输入登录框511的用户名栏512,进而浏览显示于提醒终端121的表301等,基于自己的选择顺序取得认证用字符串,将得到的认证用字符串输入登录框511的密码栏513,点击或单击(357)登录按钮514。

[0135] 于是,将伴有用户名以及密码的登录请求从接入终端141发送(358)到资源服务器161。

[0136] 接收到登录请求的资源服务器161进行基于用户名及密码的合法认证,如果该合法认证成功,则向管理服务器181询问(359)当前日期相对于该用户及该资源服务器161是否满足许可条件。

[0137] 在此,如上述,如果采用许可条件“在相对于询问的资源服务器名和用户名的组合决定的有效时间段内询问被管理服务器接收”,则可以判定用户是否具有作为安全令牌起作用的提醒终端121。管理服务器181向资源服务器161返回对询问的回答(360)。

[0138] 如果满足许可条件,则判定为该用户具有通过该用户名利用该资源服务器161的资源的权限,资源服务器161将认证成功的消息发送(361)给接入终端141,用户经由接入终端141利用(362)资源服务器161的资源。

[0139] 在有不满足许可条件的消息的回答的情况时、或用户名和密码的合法认证失败的情况下,资源服务器161向接入终端141发送有效时间段外的消息。另外,在前者的情况下,请求用户启动提醒终端121。该情况下,用户在启动了提醒终端121后,从显示于接入终端141的登录框511再次尝试登录(未图示)

[0140] 在用户名和密码的合法认证失败了的情况下,资源服务器161向接入终端141发送认证失败的消息。用户需要在显示于接入终端141的登录框511中再次输入用户名或密码后,再次尝试登录(未图示)。

[0141] 此外,也可以在资源服务器161中的用户名及密码的合法认证之前进行许可条件的询问/回答。在采用许可条件的成立作为事先认证的情况下,如后述,也可以为:只要事先认证不成功,则不能够在接入终端141输入密码。

[0142] 在上述的说明中,从资源服务器161向管理服务器181询问许可条件“当前日期包含于相对于该用户及该资源服务器161决定的有效时间段”是否成立,但也可以询问有效时间段或其自身。该情况下,管理服务器181回答最新设定的有效时间段、或未设定最近有效时间段。另外,也可以从资源服务器161向管理服务器181询问报告的接收日期。该情况下,管理服务器181回答最新接收到的报告的接收时刻、或未接收最近报告,资源服务器161设定对该用户的有效时间段。

[0143] 这样,在本方式中,将提醒终端121作为安全令牌利用,但该功能也可以省略。该情况下,不进行有效时间段的决定或判定,而仅用户名和密码进行的合法认证在资源服务器161进行。

[0144] (脚本的利用)

[0145] 此外,在显示于接入终端141的浏览器501等中的登录框511上,也可以使用基于JavaScript(注册商标)的非同步XML通信技术即AJAX等得到的脚本,由如下构成。

[0146] 即,

[0147] (1)就脚本而言,每次向用户名栏512输入字符时,接入终端141都向资源服务器161或管理服务器181询问当前日期是否在相对于具有已输入用户名栏512的由字符串构成的用户名的用户设定的有效时间段内。

[0148] (2)询问目的地回答来自接入终端141的询问。如果询问目的地是资源服务器161,则资源服务器161向管理服务器181适宜进行有效时间段的询问,并基于该内容对接入终端141进行回答。

[0149] (3a)如果在有效时间段内,则脚本将密码栏513设定为可编辑以及可见状态。

[0150] (3b)如果在有效时间段外,则脚本将密码栏513设定为不能编辑或不可见状态。

[0151] (4)脚本将登录按钮514设定为不可操作或不可见状态,直至将字符串输入密码栏513且在输入了字符串后,脚本将登录按钮514设定为可操作以及可见状态。

[0152] 该方式中,如果未启动提醒终端121,则用户不能输入密码,因此,能够有效抑制第三者的非法访问。

[0153] (提醒终端的自动启动)

[0154] 在上述说明中,要访问资源服务器161的用户自发启动提醒终端121,但通过利用在接入终端141进行动作的浏览器501的插件、及便携终端等所具备的通知的接收功能,可以简单地启动提醒终端121。

[0155] 即,浏览器501的插件监视所显示的URL的内容中是否含有用于隐藏字符地输入的字段。该字段例如可通过内容是否包含由HTML(HyperText Markup Language)中的<input type＝"password">标签表现的要素来识别。

[0156] 如果包含上述字段,则插件自动或以用户进行的插件图标521的点击等为契机,执

行用于向实现提醒终端121的便携终端发送通知的处理。典型地，进行如下的处理。

[0157] 插件对提供便携终端等的OS(Operating System)的供应商等所准备的通知服务器，发送指定了通知的目的用户、目的应用及通知内容的委托。此外，也可以采用插件对管理服务器181发出委托，接收到委托的管理服务器181访问通知服务器的方式。另外，与便携终端等绑定的目的用户的信息在进行插件的安装时由用户设定。

[0158] 接收到委托的通知服务器识别委托中指定的目的用户的便携终端等，并通知对该便携终端等的应用指定的通知内容。

[0159] 接收到通知的便携终端等将通知内容弹出显示或者汇总在通知中心等中显示。当用户通过单击等选择该通知内容时，通知的应用启动，开始与通知内容相对应的处理。

[0160] 通知内容中包含显示于浏览器的内容的URL。因此，如果注册有与该URL匹配的服务器ID绑定的表301，则提醒终端121将其提示给用户。最简单地说，如果URL内所示的域名和作为服务器ID使用的域名一致，则判定为URL匹配，但也可以根据URL整体一致、或者URL中除可选参数以外的部分一致等，判定可否匹配。

[0161] 如果未注册，则提醒终端121可以显示为未注册的消息的警告，也可以请求用户注册针对该资源服务器161的表301。请求注册的处理后述。

[0162] 在组合了上述方式的情况下，如果在浏览器显示针对所希望的资源服务器161的登录框511，则自动或手动地在提醒终端121显示针对该资源服务器161的表301。因为资源服务器161为未注册，所以在提醒终端121未能显示表301的情况下，用户可以得知该消息，并且不能进行向密码栏513的输入以及登录按钮514的操作。因此，能够有效抑制例如向假冒网站的登录。

[0163] 此外，如后述，在用户于提醒终端121注册了包含针对资源服务器161的当前的密码的表301的情况、或更新资源服务器161中的密码并进行了用于开始提醒终端121上的管理的操作的情况下，从提醒终端121进行该消息的报告，且可以进行向密码栏513的输入以及登录按钮514的操作。

[0164] 除此之外，对便携终端的通知也可以不经由通知服务器而利用以下说明的近距离通信。即，在接入终端141动作的浏览器501的插件与便携终端等进行近距离通信，根据需要赋予通过便携终端等启动程序的时机，使便携终端等作为提醒终端121起作用。

[0165] (基于近距离通信的密码输入)

[0166] 如果利用提醒终端121和接入终端141可近距离通信这一情况，则也可以构成为用户不通过手动作业输入认证用字符串，而仅从对提醒终端121提示的表按顺序选择要素，在显示于接入终端141的登录框511的用户名栏512和密码栏513输入认证用字符串。

[0167] 首先，在接入终端141，插件进行动作。该插件是对浏览器提供扩展功能的程序、或监视浏览器的动作的常驻程序。

[0168] 插件始终、间歇、或者基于插件图标521的点击等的用户的指示操作来监视接入终端141的附近是否有可进行近距离通信的提醒终端121。在此，近距离通信可以采用在规定的距离内建立的有线连接或无线连接。例如，在同一WIFI接入点无线连接了接入终端141和提醒终端121的情况、接入终端141和提醒终端121通过Bluetooth(注册商标)或NFC可无线通信的情况、接入终端141和提醒终端121通过USB线缆等直接有线连接的等情况下，建立近距离通信。

[0169] 提醒终端121在对用户提示表时，对建立了近距离通信的接入终端141发送该消息的报告。

[0170] 接收到报告的接入终端141的插件判定接入终端141的浏览器上显示的登录框511的URL与报告的资源服务器名是否匹配，并将其结果发送给提醒终端121。进而，接入终端141的插件进行匹配，将报告的用户名输入登录框511的用户名栏512。

[0171] 提醒终端121基于从接入终端141接收到的结果，如果接入终端141的浏览器上显示的登录框511用的表通过提醒终端121提示给用户，则用户每次进行选择该表的各要素或附加要素305的操作(例如单击或点击表的要素的操作等)时，都将该选择的要素中包括的字符串发送给接入终端141。

[0172] 接入终端141的插件将从提醒终端121送来的字符串输入登录框511的密码栏513。因此，提醒终端121作为针对接入终端141的特殊的键盘起作用。

[0173] 如果基于自己的选择顺序进行的要素选择完成，则用户通过接入终端141的登录框511操作登录按钮514。

[0174] 该方式中，用户不需要浏览表并提取随机的字符串，而且不需要向登录框511的密码栏513直接输入认证用字符串。因此，在提醒终端121和接入终端141建立了近距离通信的时间段，只要显示可选择操作表301的各要素以及附加要素305的按钮或标签即可，不需要显示这些要素中包括的字符串。该情况下，为了容易确认表301的各要素的方格的位置，也可以显示引导字符，也可以省略引导字符的显示。

[0175] 为了将表301的各要素以及附加要素305中包括的字符串在提醒终端121进行显示，也需要在规定的提醒终端121进行其它提醒终端121所准备的辅助认证(例如，通过构成提醒终端121的手机等的OS安装的个人识别号的认证或指纹认证等。)。

[0176] 除此之外，提醒终端121在与接入终端141的插件建立了近距离通信的时间段，显示表301，但也可以是，如果切断近距离通信，则只要在提醒终端121辅助认证不成功，就不显示表301。

[0177] 这些方式中，即使在提醒终端121被盗的情况下，也难以偷看表本身。

[0178] 此外，在利用接入终端141和提醒终端121的近距离通信使提醒终端121作为特殊键盘起作用的方式中，也可以从认证系统101省略管理服务器181的要素。

[0179] 如以上说明，根据这些方式，能够通过提醒终端121安全地管理人们不易记忆的大量的随机密码。

[0180] 另外，如果采用将在提醒终端121分割密码并将其混入并嵌入于其它要素中的表提示给了用户这种情况，来作为针对密码本身的测验的事先认证的要件，则可以有效抑制密码的暴力攻击。

[0181] 进而，因为直至通过提醒终端121将表提示给用户为止，不能进行密码输入等，从而用户可以确认提醒终端121作为认证用令牌起作用。

[0182] 除此之外，通过将接入终端141的浏览器等的插件和提醒终端121组合利用，可以有效防止假冒URL等导致的伤害。

[0183] (变形例)

[0184] 在上述方式中，访问请求被从接入终端141送入资源服务器161，登录框511被从资源服务器161送入接入终端141，用户将密码输入接入终端141，但密码的输入也可以由接入

终端141以外的认证终端进行。认证终端可以是与提醒终端121相同的设备，也可以是不同的设备。

[0185] 例如，如果将访问请求从接入终端141送入资源服务器161，则资源服务器161识别对被访问请求指定的用户名预先分配的智能手机等的认证终端，并向在该认证终端上动作的应用发送通知。进而，在接入终端141的浏览器上，进行待认证的画面显示。

[0186] 当用户在认证终端对该通知进行反应时，在认证终端启动应用，显示登录框511。当用户在认证终端的登录框511中输入密码等时，将这些信息送入资源服务器161，进行登录认证。如果认证成功，则接入终端141的浏览器从待认证的画面显示移至访问表的画面显示。而且，用户可以经由接入终端141利用资源服务器161的资源。

[0187] 如上述，在该方式中，认证终端和提醒终端121可以在同一终端上实现。即，如果将有关访问请求的通知送入提醒终端121，则相对于该资源服务器161注册的用户名、与该资源服务器161对应的表301以及用于输入密码的输入栏在画面上显示。

[0188] 用户一边用提醒终端121观看表301，一边在输入栏输入密码。输入完成后，用户名和密码从提醒终端121被送入资源服务器161。如果在资源服务器161的认证成功，则用户可以经由接入终端141利用资源服务器161的资源。

[0189] 在利用了浏览器插件的情况下，也可以为如下的方式。即，在通过接入终端141显示登录框511的阶段，如果启动插件，则向提醒终端121发送通知。

[0190] 如果用户对该通知进行反应，则相对于该资源服务器161注册的用户名、与该资源服务器161对应的表301、用于输入密码的输入栏在提醒终端121的画面上显示。

[0191] 用户一边观看表301一边在输入栏输入密码。输入完成后，用户名和密码被送入接入终端141的浏览器插件。

[0192] 浏览器插件将接收到的用户名和密码输入登录框511，使登录按钮514动作(也可以由用户操作)。于是，从接入终端141向资源服务器161发送登录请求。以下与上述相同。

[0193] 在该方式中，即使是不以提醒终端121或管理服务器181的存在为前提而提供服务的资源服务器161，仅向接入终端141导入浏览器插件，即可进行利用了提醒终端121的密码管理。

[0194] 此外，关于用户名和密码的认证，也可以采用资源服务器161委托给管理服务器181的方式。该情况下，用户名和密码被适宜发送给管理服务器181，资源服务器161在管理服务器181询问认证的成败。

[0195] (利用已有密码)

[0196] 在上述说明中，在提醒终端121中注册的表301的各要素以随机生成为前提，但在不变更密码地将已有的资源服务器161注册到提醒终端121时，例如只要采用以下的步骤即可。

[0197] 即，

[0198] (1)提醒终端121对用户提示空白的表。

[0199] (2)用户自己分割已有的资源服务器161的密码，根据自己的选择顺序手动写入空白的表。

[0200] (3)被分割的密码的写入完成后，提醒终端121在其它的要素中嵌入随机生成的字符串。

[0201] (4)将完成的表与已有的资源服务器161的服务器ID相关联地存储于提醒终端121的存储部201。

[0202] 通过该步骤,即使在有已设定了密码的资源服务器161的情况下,也能够不变更密码而将该密码的管理委托给提醒终端121。在该方式中,通过省略经由管理服务器181的许可条件进行的认证,可以对应任意的资源服务器161。

[0203] 此外,提醒终端121也可以检查完成的表是否是充分随机的。在随机性低的情况下,期望使用户变更密码。另外,在用户完成所分割的密码的写入的阶段,将进行了写入的要素与已注册于提醒终端121的其它表的相同场所的要素进行对比,在重复的情况下,不将已有的密码直接使用,而期望促使用户变更密码。

[0204] (密码的注册、更新)

[0205] 首先,在提醒终端121开始资源服务器161用的密码的管理时,需要重新生成相对于资源服务器161的资源服务器名及用户名的组合的表,并将从该表取得的注册用字符串作为密码注册到资源服务器161中。

[0206] 另外,一旦在提醒终端121开始资源服务器161用的密码的管理后,则期望定期变更密码。目前,在向服务器登录时,当在上次更新了密码后经过一定时间段(例如90天)时,采用以变更密码的方式进行警告的对策,但在变更密码时,存在再次考虑新的密码的烦恼。

[0207] 因此,在本方式中,提醒终端121辅助密码的注册及更新。

[0208] 即,提醒终端121的表生成部204在相对于资源服务器名和用户名的各组合的新注册的情况下、或已经注册且将表存储于存储部201后,在经过与该组合对应的更新时间段时,生成新的表。

[0209] 更新时间段的典型是从上次的表的生成至经过一定时间段为止,但也可以设定更新的时期,例如根据表的提示频率。

[0210] 在新的表中,包括在各要素的信息也随机生成。另外,附加要素可以由用户指定,也可以随机生成与当前利用的表相同的字符类型的信息,也可以仍旧继续使用当前的附加要素。

[0211] 以对用户分配的选择顺序提取要素,如果根据需要追加附加要素,则得到该资源服务器161用的注册用字符串。

[0212] 而且,在新注册的情况下,密码注册部205提示所生成的表,在更新注册的情况下,密码注册部205提示该资源服务器161用的当前的表和该新的表,并促使新注册或更新注册该资源服务器161中的密码。

[0213] 图7是表示本发明实施例的用于更新密码而显示的表的情况的说明图。以下,参照本图进行说明。

[0214] 在资源服务器161的密码更新时,多请求输入当前使用的密码和新的密码这两方。在提醒终端121,期望构成为能够阅览用于各资源服务器161的表的历史。在进行密码更新时,若能够同时阅览新旧表,则可减少用户的麻烦。

[0215] 本图表示用于基于图3A所示的表更新密码的提醒终端上的显示例,在表301内的各要素及附加要素305上,在上段显示当前的要素,在下段显示新的要素。

[0216] 此外,在新注册的情况下,因为“当前的要素”不存在,所以仅显示新的要素即可。

[0217] 另外,在资源服务器161中用户手动完成密码的新注册或更新注册时,如果点击或

单击完成按钮321，则表注册部206将该新的表对应于该资源服务器161存储到存储部201中。另外，在更新注册的情况下，将以前的表作为历史信息进行存储。此时，也可以进行将提醒终端121管理的表的信息在管理服务器181中加密备份的处理。如果点击或单击取消按钮322，则取消更新。

[0218] 在上述说明中，用户手动进行密码的更新，但用户的选择顺序自身通过提醒终端121或管理服务器181进行管理，如果根据需要可以参照，则提醒终端121或管理服务器181访问资源服务器161，由此也可以定期、自动地更新密码。

[0219] 另外，在要更新密码时，也可以采用下述方式：提醒终端121使用户通过该用户的选择顺序单击图7表示的表301，由此，取得新旧两密码，提醒终端121利用该取得的新旧的密码访问资源服务器161，自动地更新密码。

[0220] 该情况下，因为在提醒终端121的RAM(Random Access Memory)暂时存储所取得的选择顺序或新旧的密码，所以期望在更新了密码后，将该暂时存储的区域删除。

[0221] 根据本方式，作为资源服务器161用的密码，可以使用未装载于词典中的随机的字符串，且定期更新密码也可以容易进行。

[0222] (选择顺序的更新)

[0223] 根据本实施例，不仅可以个别更新各资源服务器用的密码，还可以更新对用户分配的选择顺序。这相当于现有技术中所说的主密码的更新。

[0224] 首先，用户要更新选择顺序时，提醒终端121生成用户用的新的引导字符串。在上述例子中，表301由5行5列构成，对各要素分配1字符的大写字母的引导字符。本实施例中，采用从表301内按顺序选择四个要素的选择顺序。因此，作为用户用的新的引导字符串，由大写字母4字符构成，生成各字符相互不重复的字符串。

[0225] 优选引导字符串在每次更新选择顺序时变更。例如，引导字符串可以随机生成。也可以利用词典等采用容易记忆的拼写。例如，可以采用由4字符的拼写构成的单词(例如“SNOW”“MAZE”)，也可以采用5字符以上的单词的前缀部分(例如“TABLE”的前缀“TABL”、“SCHOOL”的前缀“SCHO”)。

[0226] 进而，也可以在将上述那种容易记忆的拼写的候补随机对用户提供一些后，使用户选择任一个。除此之外，还有在每次进行选择顺序的更新时，使用户创造引导字符串的方法。以下，为了容易理解，对作为新的引导字符串生成“SCHO”的情况进行说明。

[0227] 而且，提醒终端121的接收部207将由提醒终端121管理的与各资源服务器161用的表相同的行数、列数的试行表提示给用户。图8A是表示由用户选择当前使用的选择顺序的情况的说明图。以下，参照本图进行说明。

[0228] 本图所示的例子中，试行表551由5行5列构成，各要素中，为了给用户参考而显示与最后使用的资源服务器161用的表的要素相同的信息。

[0229] 另外，如本图所示，提醒终端121的接收部207请求该用户以对用户分配的选择顺序单击或点击等来选择该试行表551的要素。以下，对用户当前使用图4所示的选择顺序(4行2列、5行3列、4行4列、3行5列)的情况进行说明。

[0230] 图8B是表示由用户选择当前使用的选择顺序的情况的说明图。如本图所示，如果用户在试行表551内选择最初的要素(4行2列)，则对该要素内的引导字符追加所生成的新的引导字符串的最初的字符“S”。

[0231] 图8C是表示由用户选择当前使用的选择顺序的情况的说明图。如本图所示，如果在试行表551内选择第二要素(5行3列)，则对该要素内的引导字符追加所生成的新的引导字符串的最初的字符“C”。

[0232] 图8D是表示由用户选择当前说明的选择顺序的情况的说明图。如本图所示，如果在试行表551内选择第三要素(4行4列)，则对该要素内的引导字符追加所生成的新的引导字符串的最初的字符“H”。

[0233] 图8E是表示由用户选择当前使用的选择顺序的情况的说明图。以下，参照这些图进行说明。如本图所示，如果在试行表551内选择第四要素(3行5列)，则对该要素内的引导字符追加所生成的新的引导字符串的最初的字符“0”。

[0234] 这样，如果根据当前的选择顺序选择试行表551内的要素，则在所选择的要素内明示所生成的新的引导字符串中的与该要素的时序对应的字符。因此，用户可知为新的选择顺序而准备的新的引导字符串为“SCH0”。

[0235] 当前的选择顺序的输入完成，用户单击或点击前进按钮552时，接收部207对用户提示与试行表551相同的行数、列数的迁移表。图9A是表示由用户选择新的选择顺序的情况的说明图。如本图所示，接收部207在提醒终端121的画面上显示迁移表561。

[0236] 迁移表561为5行5列的空白的表，提醒终端121请求用户以用户要新利用的选择顺序单击或点击等选择该试行表561的要素。

[0237] 图9B是表示由用户选择新的选择顺序的第一个的情况的说明图。图9C是表示由用户选择新的选择顺序的第二个的情况的说明图。图9D是表示由用户选择新的选择顺序的第三个的情况的说明图。图9E是表示由用户选择新的选择顺序的第四个的情况的说明图。以下，参照这些图进行说明。

[0238] 用户选择1行1列的位置的要素作为新的选择顺序的第一个。于是，如图9B所示，在迁移表561的1行1列的要素上转印在试行表551中用户第一选择的要素(4行2列)的内容。另外，还明示新的引导字符串的最初的字符“S”。

[0239] 接着，选择2行2列的位置的要素作为新的选择顺序的第二个。于是，如图9C所示，在迁移表561的2行2列的要素上转印在试行表551中用户第二选择的要素(5行3列)的内容。另外，还明示新的引导字符串的第二字符“C”。

[0240] 接着，选择5行5列的位置的要素作为新的选择顺序的第三个。于是，如图9D所示，在迁移表561的5行5列的要素上转印在试行表551中用户第三选择的要素(4行4列)的内容。另外，还明示新的引导字符串的第三字符“H”。

[0241] 最后，选择3行5列的位置的要素作为新的选择顺序的第四个。于是如图9E所示，在迁移表561的3行5列的要素上转印在试行表551中用户最后选择的要素(3行5列)的内容。另外，还明示新的引导字符串的最后的字符“0”。

[0242] 此外，在本例中，第四个选择顺序的场所未变化，但第一～第三选择顺序的场所变化。这样，在更新选择顺序时，仅使选择顺序的一部分变化即可，也可以使全部变化。

[0243] 这样，如果通过新的选择顺序在迁移表561内选择要素，则在迁移表561内依次显示最后参照的密码，并且依次显示新的引导字符串。因此，用户可以确认当前的选择顺序的输入有无错误，并且可以确认成为用于存储新的选择顺序的辅助的新的引导字符串。

[0244] 之后，提醒终端121向用户询问是否可以更新选择顺序。在用户希望进行选择顺序

的更新的情况下，用户选择更新按钮562。于是，提醒终端121的规则生成部208生成一个表的转换规则。该转换规则满足如下条件。

[0245] (s)将按在采样的表中用户采用的选择顺序提取的要素的内容移动到按在空白的表中用户采用的选择顺序提取的要素，

[0246] (t)将按上述预先分配的选择顺序提取的要素以外的要素的内容移动到按上述应新分配的选择顺序提取的要素以外的要素。

[0247] 规则(s)基于用户的指示。在上述的例子中，根据规则(s)，要素如下移动：

[0248] 4行2列→1行1列；

[0249] 5行3列→2行2列；

[0250] 4行4列→5行5列；

[0251] 3行5列→3行5列。

[0252] 规则(t)使剩余的要素(用户的当前的选择顺序中所含的要素以外的要素)随机移动。

[0253] 提醒终端121的全更新部209将与各资源服务器相关联地存储的表通过该生成的转换规则进行更新。即，相对于已注册的资源服务器的服务器名及用户名的所有的组合的表也包含过去的历史中所含的表，通过共通的转换规则一并进行更新。更新了所有的表后，将更新后的信息备份到管理服务器181。

[0254] 根据本方式，可以容易地更新用户的选择顺序。

[0255] 此外，在方格的角部在一定时间段较小地显示字母或平假名，通过根据显示表的次数、更新选择顺序后的经过时间而逐渐难以看到角部的显示等，在更新最初也可以依靠角部的字符取得密码，随着习惯而不依赖于角部的字符按照自己的选择顺序从表中提取密码。

[0256] 此外，当按照选择顺序将显示于方格的角部的字符排列时，也可以按照使其成为容易记忆的单词等的方式，配置角部的字符。该情况下，提醒终端121从词典等选择与新的选择顺序的长度相同的字符数的单词、即所含的字符互不相同的单词，按照该新的选择顺序在各要素的角部按顺序排列该单词的拼写字符，且在其它要素上以相互不重复的方式随机配置所选择的单词中未出现的字符。

[0257] 图10是表示由新的选择顺序更新的表的情况的说明图。本图是以上述的步骤对图3A所示的表更新选择顺序的图。

[0258] 图11是表示由新的选择顺序更新其它表的前后的情况的说明图。本图表示对于通过上述的步骤相对于存储于相同提醒终端121中的其它资源服务器名及用户名的组合而存储的表也一并更新选择顺序的情况，本图所示的表管理4位数的个人识别号。

[0259] 如这些图所示，表的各要素的位置在更新前后通过在表彼此之间相互共通的转换规则进行切换。另外，与转换规则的切换独立开，引导字符也在更新前后进行变化，但引导字符的配置在更新前的表彼此之间共通，且更新后的表彼此之间也共通。即，在相对于任一资源服务器161的表，在哪一位置显示哪一引导字符是共通的。

[0260] 例如，相对于选择规则的更新前的图3A所示的表，基于引导字符“DICE”得到密码“bpppjsld#X5”，相对于选择规则的更新后的图10所示的表，基于引导字符“SCHO”得到密码“bpppjsld#X5”。

[0261] 与此相同，关于图11所示的资源服务器161的服务器名“www.zzz.com”及用户名“paul”的组合，因为没有附加要素，所以更新前基于引导字符“DICE”得到4位数的个人识别号“6441”，更新后基于引导字符“SCHO”得到相同的个人识别号“6441”。

[0262] 此外，如果相对于选择顺序的引导字符串以在进行选择顺序的更新时在提醒终端121被暂时保持，之后从存储器中消除的方式构成，则即使提醒终端121被盗取，选择顺序也不会马上泄漏。

[0263] 该方式中，在用户不习惯新的选择顺序的时间段，用户可以依赖于方格内的角部的字符取得密码。基于从更新起经过一定时间段、或显示表301时不显示引导字符的情况连续产生一定次数等，判断为用户充分记住了新的选择顺序的情况下，也可以将引导字符完全去除。该情况下，在进行下次的选择顺序的更新时，不显示当前使用的引导字符。该方式中，可以进一步提高安全性。

[0264] (对其它资源服务器的依赖)

[0265] 上述的方式包含下述方式：作为用于利用资源服务器161的资源的事先认证，以利用该资源服务器161用的表在提醒终端121上显示的情况，通过与管理服务器181协动而事先认证成功为条件，在资源服务器161上进行基于用户名和密码的合法认证的方式、即确认到许可条件成立后进行合法认证的方式。该方式中，资源服务器161向管理服务器181询问事先认证是否成功。

[0266] 以下，对该方式的扩展例进行说明。首先，在该方式中，以下述方式为前提，即，在资源服务器161中的合法认证之前，询问从资源服务器161向管理服务器181的事先认证是否成功，在回答了从管理服务器181向资源服务器161的事先认证成功后，从资源服务器161向管理服务器181联系合法认证是否成功。

[0267] 之后，作为资源服务器X中的事先认证的判断基准，除“用户在提醒终端121上阅览了该资源服务器X用的表”之外，或者与其组合，还采用“在该资源服务器X依赖的资源服务器Y上，合法认证成功，当前处于根据该成功的日期决定的依赖时间段内”。依赖时间段可以适宜决定。

[0268] 典型地，在依赖于资源服务器Y的资源服务器X中的事先认证成功后再进行基于资源服务器X用的密码的合法认证，但也可以省略该动作。例如，如果在资源服务器Y中合法认证成功后的规定的短时间段内，则为资源服务器X中的合法认证省略等的方式。

[0269] 另外，也可以对事先认证设定等级。例如，如果在资源服务器Y中合法认证成功后的规定的短时间段内，则用户仅在提醒终端121阅览资源服务器X用的表，合法认证即成功，但如果在资源服务器Y中合法认证成功后经过相当时间段，则为请求基于资源服务器X用的密码的输入的合法认证等的方式。

[0270] 依赖时间段可以适宜决定。例如，在资源服务器Y为学生阅览来自大学的通知、或用于提出报告的校内系统，资源服务器X为校外企业相对于某大学的学生提供的公告板系统的情况下，资源服务器X的依赖时间段为从“资源服务器Y中某学生成功进行了合法认证的时间点”至”包含该合法认证成功的时间点的年度的最后一天”。

[0271] 此外，也可以将合法认证后进行许可条件的判定的方式和事先认证后进行合法认证的方式组合。在合法认证后进行许可条件的判定的方式中，如果在资源服务器161合法认证不成功，则不进行向管理服务器181的询问。因此，不需要从资源服务器161向管理服务器

181联络合法认证成功与否。

[0272] (时间同步的加密)

[0273] 在将提醒终端121设定为专用键盘的方式中，为了提高安全性，也可以共享在提醒终端121和资源服务器161之间进行时间同步的加密方式。可以对某资源服务器161管理的每一用户名赋予不同的种子，通过不同的加密方式进行时间同步，资源服务器161的用户整体也可以共享基于一个种子进行时间同步的加密方式。

[0274] 即，提醒终端121和资源服务器161共享时间同步的加密方式。

[0275] 在提醒终端121中，将表301提示给用户。此时，包括在各要素的字符串可以显示也可以隐藏。当用户基于自己的选择顺序全部选择表301的要素的方格，且最后选择附加要素305的方格时，提醒终端121将所选择的要素中包括的字符串和附加要素(也可以是空字符串)连结，得到字符串。

[0276] 而且，连结结果的字符串通过上述的时间同步加密方式进行加密，并将其作为认证用字符串送入接入终端141。

[0277] 因此，在本方式中，每次选择要素时，不充填密码栏513，而在选择附加要素305的方格时才开始进行至此选择的表301内的要素的字符串和附加要素的连结及加密。

[0278] 该用户接口可以变更。例如，在可以与接入终端141进行近距离通信的情况下，也可以如下构成。即，在提醒终端121中，准备“发送”按钮等表示输入完成的对象。当用户选择了表301内的各要素的方格后再选择“发送”按钮等时，进行表301内的要素的字符串和附加要素的连结及加密。

[0279] 另外，当从提醒终端121将认证用字符串送入接入终端141时，接入终端141在密码栏513输入该字符串。以后的处理可以与上述的例子相同，也可以在输入后立即将登录框送入资源服务器161。

[0280] 资源服务器161在从接入终端141接收请求时，基于时间同步的加密方式将对请求指定的认证用字符串解密。

[0281] 在解密成功的情况下，将被解密的字符串作为密码，进行认证。

[0282] 另一方面，在解密失败的情况下，尝试从接入终端141发送未处理的密码，进行认证。

[0283] 或者，提醒终端121也可以与上述的方式相同，在用户每次选择表301的各要素或附加要素时，将该要素加密送入接入终端141，接入终端141将送来的各已加密字符串充填到密码栏513。

[0284] 就资源服务器161的解密而言，将从接入终端141发送的请求指定的认证用字符串分配给已加密字符串，分别尝试解密，全部解密成功后，将它们连结，作为密码。

[0285] 最简单的方式是，以已加密字符串不含特定的分隔符(例如空白)的方式进行加密，且将认证用字符串分割以分隔符分割后，将分割结果分别解密。

[0286] 作为时间同步的加密技术，最简单的加密技术如下。

[0287] 首先，提醒终端121和资源服务器161将随机数的种子时间同步并共享。该种子例如每隔几分钟等、每隔一定时间，基于规定的种子随机数更新算法进行更新。但是，因为两者在时刻上存在一定的误差、用户的输入耗费时间，所以在提醒终端121取得提示了表的时间点的最新及最近的种子v。在资源服务器161，取得登录请求到达的时间点的最新及最近

的种子u[1],u[2],…,u[N]。N的大小也可以考虑共享的种子的更新间隔、用户的输入时间的分布、各种设备的时间误差等通过实验决定。时间同步是指1以上N以下的整数q中满足v＝u[q]的数存在一个。

[0288] 提醒终端121和资源服务器161也共享随机数序列生成算法。随机数序列生成算法可以与上述的种子随机数更新算法相同也可以不同。如果赋予种子p,则可通过种子随机数更新算法来计算随机数序列g(p,1),g(p,2),…。

[0289] 另外,用户选择表301的要素或附加要素并将包括在所选择的要素的字符串连结,由此,得到由字符s[1],s[2],…构成的字符串。

[0290] 提醒终端121相对于已连结字符串的第k个字符s[k]计算字符

[0291] e(g(v,k),s[k])。

[0292] 在此,运算e(x,y)相对于后述的运算c(x,z)满足如下的关系。

[0293] y＝c(x,e(x,y))

[0294] 例如对于e(x,y)和c(x,z)的任一个,如果设为自变量的位异或,则上述成立。除此之外,如e(x,y)＝y+x,c(x,z)＝z-x等,也可以利用和与差。另外,在资源服务器161作为密码可接收的字符集合中,也可以进行使字符代码巡回的加密。例如,在仅容许26字母字符作为密码用字符的资源服务器161中,只要使用以ROT13为基准的加密设为e(x,y)＝ROTx(y),c(x,z)＝ROT-x(z)即可。

[0295] 另外,通过用户的选择而得到的已连结字符串S为由M个字符构成的字符串

[0296] S＝〔s[1],s[2],…,s[M]〕。

[0297] 于是,已加密字符串E可以如下表现。

[0298] E＝〔E[1],E[2],…,E[M]〕＝〔e(g(v,1),s[1]),e(g(v,2),s[2]),…,e(g(v,M),s[M])〕

[0299] 资源服务器161经由接入终端141接收认证用字符串E时,在资源服务器中,相对于认证用字符串E计算N+1个字符串r[1],r[2],…,r[N]。

[0300] r[1]＝〔c(g(u[1],1),E[1]),c(g(u[1],2),E[2]),…,c(g(u[1],M),E[M])〕;

[0301] r[2]＝〔c(g(u[2],1),E[1]),c(g(u[2],2),E[2]),…,c(g(u[2],M),E[M])〕;

[0302] …;

[0303] r[N]＝〔c(g(u[N],1),E[1]),c(g(u[N],2),E[2]),…,c(g(u[N],M),E[M])〕;

[0304] 而且,采用N个字符串r[1],r[2],…,r[N]及认证用字符串E分别作为密码的候补进行密码认证。如果通过任意的字符串r[q]成功进行密码认证,则基于用户名和密码的合法认证成功。关于N个字符串r[1],r[2],…,r[N]及认证用字符串E的任一个,如果密码认证失败,则合法认证也失败。

[0305] 此外,通过认证用字符串E成功进行密码认证的情况认为是用户通过手输入直接将认证用字符串E输入密码栏513的情况。包含本方式在内,通常在判定为用户通过手输入而输入密码的情况下,资源服务器161将例如邮件或短消息发送到用户预先注册的手机,促使其确认等适宜的2阶段认证,也可以提高安全性。

[0306] 在该加密方法中,每次得到1字符的字符s[1],s[2],…时,进行加密,直至最后加密完成后(最后的加密可以通过选择附加要素而决定,也可以通过选择“发送”按钮等决定。),将k的值重新设定为1,进行加密方式的初始化。

[0307] 除此之外，关于加密方式可以采用通过拖拽来切换字符串的顺序、或者可以判定是否附加检验和等信息来加密等各种方式。

[0308] 该方式中，通过尽可能避免原始密码的通信，可以提高安全性，例如也适合于省略了管理服务器181的认证系统101的结构。

[0309] (省略报告)

[0310] 上述方式中，提醒终端121向外部设备报告如下情况：利用提醒终端121将与接下来要访问的资源服务器161的服务器名以及用于访问的用户名的组合相关联的表301提示给用户，由此，可以使提醒终端121作为安全令牌或专用键盘起作用。

[0311] 但是，也可以采用从提醒终端121省略发送部203而完全不向外部的设备进行报告的方式。也可以对每一个资源服务器161设定是否通过发送部203进行报告的发送。

[0312] 在未进行报告的发送的方式中，仅将提醒终端121作为用于管理用户不能记忆的随机的密码的设备利用。

[0313] 即使在此时，因为提醒终端121显示的表301未显示用于在资源服务器161登录的密码自身，所以即使表301被第三者看到，密码也不会马上泄漏。

[0314] 因此，在该方式中，也可以基于用户的指示从提醒终端121附加将表301印刷于纸上的功能。如果利用印刷有表301的纸，则即使在切断了提醒终端121的电源的情况下，也能够进行向资源服务器161的登录。另外，在使用印刷有表301的纸对资源服务器161进行了登录后，即使该纸被忘在桌子上等并被第三者看到表301，密码也不能马上泄漏。

[0315] 这样，通过根据用户的用途所需的安全性等级设定可否发送报告、或可否印刷表301，可以灵活地对应用户的用途。

[0316] (与程序的关系)

[0317] 上述各实施例的提醒终端121、接入终端141、资源服务器161、管理服务器181可通过在各种计算机的硬件上执行各种程序而实现。

[0318] 通常，计算机将记录于非易失性(non-transitory)信息记录介质的程序读出到作为临时性(temporary)存储装置的RAM(Random Access Memory)后，CPU(Central Processing Unit)或处理器执行读出的程序中所含的指令。但是，在可以将ROM和RAM在一个存储空间映射并执行的构架中，CPU直接读出存储于ROM的程序中所含的指令并执行。CPU或处理器等与RAM等协动，控制该硬件包括的NIC(Network Interface Card)或显示器、话筒、扬声器等设备。

[0319] 在此，各程序可以记录于压缩盘、软盘、硬盘、光磁盘、数字视频盘、磁带、ROM(Read Only Memory)、EEPROM(Electrically Erasable Programmable ROM)、闪存、半导体存储器等计算机可读非临时性(non-transitory)信息记录介质。该信息记录介质可以与各硬件独立地发布、销售。

[0320] 进而，上述的程序也可以与执行程序的计算机相独立地经由计算机通信网络等易失性(transitory)传输介质从发布装置等发布给各硬件。

[0321] 此外，也可以通过电路的行为级描述用的程序设计语言来描述上述的程序。该情况下，从上述的程序生成电路的布线图或时间图等各种设计图，基于该设计图可以创建构成上述图像处理装置的电路。例如，除可以根据上述程序通过FPGA(Field Programmable Gate Array)技术在可再编程的硬件上构成上述图像处理装置外，还可以通过ASIC

(Application Specific Integrated Circuit)技术构成特定用途专用的电路。

[0322] 该情况下,提醒终端121、接入终端141、资源服务器161、管理服务器181的各部以执行对其分配的处理的方式构成(configure)。

[0323] (总结)

[0324] 如以上所说明,本认证系统包括提醒终端、资源服务器、管理服务器以及接入终端,

[0325] (A)上述提醒终端包括:

[0326] 表生成部,生成具有在各要素中包括的字符串的表,所述字符串是随机生成的;

[0327] 密码注册部,使用户辨识上述生成的表,以及促使上述用户进行下述动作,

[0328] (1)按对上述用户预先分配的选择顺序从上述辨识的表中提取要素,以及将所提取的要素中包括的字符串排列,由此得到注册用字符串,

[0329] (2)将所得到的注册用字符串更新或注册或新近注册为上述用户的用户名在上述资源服务器的密码;

[0330] 存储部,将上述资源服务器具有的资源服务器名及上述用户名的组合与上述辨识的表相关联地进行存储;

[0331] 提示部,当通过来自上述用户的指示选择上述组合时,将与上述组合相关联地存储的上述表提示给上述用户,以及促使上述用户进行下述动作,

[0332] (a)按预先对上述用户分配的选择顺序从上述提示的表中提取要素,以及将所提取的要素中包括的字符串进行排列,以得到认证用字符串,

[0333] (b)将得到的认证用字符串用于由上述用户名利用上述资源服务器的资源的请求的密码;

[0334] 发送部,发送与上述组合相关联地存储的上述表已提示给上述用户的消息的报告,

[0335] (B)上述管理服务器,

[0336] 当由上述管理服务器接收从上述提醒终端发送的上述报告时,设定与上述报告相关的组合对应的有效时间段,所述有效时间段包含上述管理服务器接收上述报告的时间点,

[0337] (C)上述资源服务器,

[0338] 当通过上述用户名利用上述资源服务器的资源的请求被从上述接入终端发送到上述资源服务器且与上述请求相关的密码与在上述资源服务器中对于上述用户名注册的密码一致时,向上述管理服务器发送上述用户名相关的询问,

[0339] (D)上述管理服务器,

[0340] 当上述询问被上述管理服务器接收时,判定许可条件“在对于作为上述询问的发起者的资源服务器的服务器名及上述询问相关的用户名的组合设定的有效时间段内,上述管理服务器接收到上述询问”是否成立,并将指示了上述判定的结果的回答发送给上述资源服务器,

[0341] (E)上述资源服务器,

[0342] 如果上述回答被上述资源服务器接收,上述接收到的回答指示上述许可条件成立,则将用于利用上述资源服务器的资源的响应发送到上述接入终端。

[0343] 另外，本认证系统中，可以如下构成，

[0344] 如果上述接入终端和上述提醒终端通过在规定的距离内建立的有线连接或无线连接可通信地连接，则上述报告经由上述有线连接或上述无线连接被发送到上述接入终端，

[0345] 如果用于从上述接入终端输入利用上述资源服务器的资源的请求的用户名及密码的登录框在上述接入终端的画面上显示，且在上述提醒终端选择的组合的服务器名是上述资源服务器的服务器名，则

[0346] 上述接入终端将上述选择的组合的用户名输入上述登录框的用户名栏，

[0347] 上述提醒终端使上述用户从上述提示的表中选择要素，

[0348] 上述提醒终端通过将上述选择的要素中包括的字符串进行排列得到传递用字符串，

[0349] 上述提醒终端将上述得到的传递用字符串经由上述有线连接或上述无线连接传递到上述接入终端，

[0350] 上述接入终端将从上述提醒终端传递的传递用字符串输入上述登录框的密码栏。

[0351] 另外，本认证系统中，可以如下构成，

[0352] 上述提醒终端将上述表的各要素中包括的字符串隐藏而提示上述表，

[0353] 上述提醒终端通过与上述资源服务器时间同步的加密方式，对上述选择的要素中包括的字符串进行加密，形成上述传递用字符串，

[0354] 上述资源服务器，如果通过上述加密方式将上述请求的认证用字符串进行解密后所得的已解密字符串与相对于上述用户名注册的密码一致，则看作上述请求的密码与相对于上述用户名注册的密码一致。

[0355] 另外，本提醒终端为上述认证系统中的提醒终端，其可以如下构成，

[0356] 上述用户每次从上述提示的表中选择上述要素时，将上述选择的要素中包括的字符串通过上述加密方式加密后传递给上述接入终端，

[0357] 每次从上述提醒终端传递上述加密了的字符串时，上述接入终端在上述登录框的密码栏追加输入上述传递来的上述加密了的字符串。

[0358] 另外，本提醒终端可以如下构成，

[0359] 生成上述表，并且以与在上述表的各要素中包括的字符串的类型不同的类型随机地生成包括在附加要素中的字符，

[0360] 对用户呈现所生成的表以及所生成的附加要素以使上述用户辨识所述表，

[0361] 上述注册用字符串以及上述认证用字符串是通过将上述提取的要素以及所述附加要素中包括的字符串进行排列而分别得到的。

[0362] 本提醒终端中，可以如下构成，

[0363] 在与上述组合相关联地存储了上述表之后，经过了与上述组合相关的资源服务器相关联的更新时间段时，

[0364] 上述表生成部生成新的表，

[0365] 上述密码注册部使上述用户辨识上述生成的新的表，并促使上述用户进行下述动作，

[0366] (1)按对上述用户预先分配的选择顺序从所辨识的新的表中提取要素，将上述提

取的要素中包括的字符串进行排列，以得到新的注册用字符串，

[0367] (2)更新以及注册所得到的新的注册用字符串作为针对与上述组合相关的用户名在所述资源服务器的密码，

[0368] 所述提醒终端还包括表注册部，所述表注册部在与所述组合相关联的存储部中存储上述新的表。

[0369] 另外，本提醒终端可以如下构成，还包括：

[0370] 接收部，从上述用户接收对上述用户预先分配的选择顺序的输入和要对上述用户新分配的选择顺序的输入；

[0371] 规则生成部，当接收到上述输入时，生成如下转换规则，

[0372] (s)将按上述预先分配的选择顺序提取的要素的内容移动到按上述应新分配的选择顺序提取的要素，

[0373] (t)将按上述预先分配的选择顺序提取的要素以外的要素的内容随机移动到按上述应新分配的选择顺序提取的要素以外的要素；

[0374] 全更新部，通过上述生成的转换规则转换存储于上述存储部的表，由此更新存储于上述存储部的所有的表。

[0375] 另外，本提醒终端可以如下构成，

[0376] 在通过上述接收部进行接收之前，生成具有与上述选择顺序的长度相同长度并且不含重复的字符的引导字符串，

[0377] 上述接收部，

[0378] (u)通过由上述用户从表选择要素，接收对上述用户预先分配的选择顺序的输入，每次上述要素被选择时，在该要素显示与上述生成的引导字符串内的选择顺序相关联的字符，

[0379] (v)通过由上述用户从表选择要素，接收要对上述用户新分配的选择顺序的输入，每次上述要素被选择时，在该要素显示与上述生成的引导字符串内的选择顺序相关联的字符，

[0380] 上述全更新部通过在所述表内的位置进行下列(x)和(y)处理来对上述表内的各位置分配引导字符：

[0381] (x)向要按对上述用户新分配的选择顺序选择的位置分配与上述引导字符串内的选择顺序相关联的字符，

[0382] (y)在对上述用户新分配的选择顺序选择的位置以外的位置随机而不重复地分配字符，

[0383] 上述提示部在将与上述多个资源服务器相关联的表中的任一个提示给上述用户时，将对该表内的各位置分配的引导字符以及该各位置的要素提示给上述用户。

[0384] 另外，本认证系统包括提醒终端、接入终端、资源服务器，

[0385] (a)上述接入终端

[0386] 将来自要利用上述资源服务器的资源的用户的请求发送到上述资源服务器，

[0387] (b)上述资源服务器在接收到上述发送来的请求时，

[0388] 向上述接入终端发送登录框，

[0389] (c)上述接入终端在接收到上述发送来的登录框时，

[0390] 将上述接收到的登录框提示给上述用户，

[0391] (d)上述提醒终端

[0392] 将与上述资源服务器相关联地存储的表提示给上述用户，

[0393] 将对上述用户提示了上述表的消息的报告发送到管理服务器或上述资源服务器，

[0394] (e)上述接入终端，

[0395] 在上述提示的登录框中包含的输入栏，从上述用户接收通过按对上述用户预先分配的选择顺序提取上述提示的表的要素并将其排列而得到的密码，

[0396] 将上述接收到的密码发送到上述资源服务器，

[0397] (f)上述管理服务器或上述资源服务器，

[0398] 在接收到上述报告时，决定包含接收到该报告的时间点的有效时间段，

[0399] (g)上述资源服务器，

[0400] 如果接收到上述密码的时间点包含在上述决定的有效时间段内，则基于上述接收到的密码来决定针对来自上述用户的上述请求的可否。

[0401] 另外，本认证系统中，可以如下构成，

[0402] 上述提醒终端将上述报告发送到上述管理服务器，

[0403] 上述资源服务器向上述管理服务器询问上述有效时间段、或者询问接收到上述密码的时间点是否包含在上述决定的有效时间段。

[0404] 另外，本认证系统中，可以如下构成，

[0405] 上述提醒终端将上述报告向上述管理服务器发送，

[0406] 上述接入终端向上述管理服务器询问上述有效时间段、或询问当前时间点是否在上述决定的有效时间段内，

[0407] (i)如果当前时间点在上述决定的有效时间段内，则以可以从上述用户接收上述密码的方式设定上述输入栏，

[0408] (j)如果未决定上述有效时间段、或者当前时间点在上述决定的有效时间段外，则以不从上述用户接收上述密码的方式设定上述输入栏。

[0409] 另外，在本认证系统中，可以如下构成，

[0410] 上述接入终端当从被提示了上述登录框的上述用户接收到与上述资源服务器相关的提醒显示的指示时，使上述管理服务器向上述提醒终端发送通知，

[0411] 上述提醒终端以接收到上述通知为契机，对上述用户提示与上述资源服务器相关联地存储的上述表。

[0412] 另外，本认证系统中，可以如下构成，

[0413] 对上述用户提示了上述表的提醒终端从上述用户接收密码的输入，且将上述输入的密码传递给上述接入终端，

[0414] 上述接入终端将上述传递来的密码输入上述登录框。

[0415] 另外，本认证系统中，可以如下构成，

[0416] 上述提醒终端，

[0417] 在与上述资源服务器相关联地存储了上述表后，经过了与上述资源服务器相关联的更新时间段时，随机生成新的表，

[0418] 促使上述用户进行下述动作，将相对于上述资源服务器的密码更新为通过按对上

述用户预先分配的上述选择顺序提取上述生成的表的要素并进行排列而得到的新的密码，

[0419] 当将相对于上述资源服务器的密码更新为上述新的密码时，与上述资源服务器相关联地存储上述新的表。

[0420] 另外，本认证系统中，可以如下构成，

[0421] 上述提示的表在栏外包含附加要素，

[0422] 上述密码通过按对上述用户预先分配的选择顺序提取上述提示的表的要素，并将其与上述提示的表的栏外所包含的附加要素一同排列而得到。

[0423] 另外，本认证系统中，可以如下构成，

[0424] 上述认证系统包含其它资源服务器，

[0425] 上述其它资源服务器在从上述接入终端接收来自要利用上述其它资源服务器的资源的上述用户的其它请求时，基于相对于对上述资源服务器的上述请求决定的可否以及该决定的时期，决定相对于来自上述用户的上述其它请求的可否。

[0426] 本提醒终端包括：

[0427] 存储部，存储与多个资源服务器的各资源服务器相关联的表；

[0428] 提示部，根据从上述多个资源服务器选择任一个的用户的指示，将与上述选择的资源服务器相关联地存储于上述存储部的表提示给上述用户，

[0429] 在与上述各资源服务器相关联的表的各要素中包括随机生成的信息，

[0430] 通过从与上述各资源服务器相关联的表中按对上述用户预先分配的选择顺序提取要素并排列，得到用于决定上述各资源服务器的资源可否利用的密码。

[0431] 另外，本提醒终端可以如下构成，

[0432] 还包括发送部，其向管理服务器或与上述提示的表相关联的上述各资源服务器发送上述表已提示给上述用户的消息的报告。

[0433] 另外，本提醒终端可以如下构成，还包括：

[0434] 表生成部，将与上述多个资源服务器的各资源服务器相关联的上述表与上述各资源服务器相关联地存储后，经过与上述各资源服务器相关联的更新时间段后，生成新的表；

[0435] 密码更新部，促使上述用户或命令上述管理服务器进行如下动作，将用于决定上述用户可否利用上述资源服务器的资源的密码更新为通过按对上述用户预先分配的上述选择顺序提取上述生成的表的要素并将其排列而得到的新的密码；

[0436] 表注册部，在将用于决定上述用户可否利用上述资源服务器的资源的密码更新为上述新的密码时，与上述资源服务器相关联地存储上述新的表。

[0437] 另外，本提醒终端可以如下构成，还包括：

[0438] 接收部，从所述用户接收对上述用户预先分配的选择顺序和应对上述用户新分配的选择顺序的输入；

[0439] 规则生成部，在接收到上述输入时，

[0440] (s)将按上述预先分配的选择顺序提取的要素的内容移动到按上述应新分配的选择顺序提取的要素，

[0441] (t)将按上述预先分配的选择顺序提取的要素以外的要素的内容随机移动到按上述应新分配的选择顺序提取的要素以外的要素；

[0442] 全更新部，通过上述生成的转换规则转换与上述多个资源服务器的各资源服务器

相关联地存储于上述存储部的表，由此更新应存储于上述存储部的所有的表。

[0443] 另外，本提醒终端可以如下构成，

[0444] 上述存储的表在栏外包含附加要素，

[0445] 上述密码通过按对上述用户预先分配的选择顺序提取上述提示的表的要素，并将其与上述存储的表的栏外所包含的附加要素一同排列而得到。

[0446] 另外，本提醒终端可以如下构成，

[0447] 在通过上述接收部进行接收之前，生成具有与上述选择顺序的长度相同长度并且不含重复的字符的引导字符串，

[0448] 上述接收部，

[0449] (u)通过由上述用户从表选择要素，接收对上述用户预先分配的选择顺序的输入，每次上述要素被选择时，在该要素显示与上述生成的引导字符串内的选择顺序相关联的字符，

[0450] (v)通过由上述用户从表选择要素，接收要对上述用户新分配的选择顺序的输入，每次上述要素被选择时，在该要素显示与上述生成的引导字符串内的选择顺序相关联的字符，

[0451] 上述全更新部通过在所述表内的位置进行下列(x)和(y)处理来对上述表内的各位置分配引导字符：，

[0452] (x)向要按对上述用户新分配的选择顺序选择的位置分配与上述引导字符串内的选择顺序相关联的字符，

[0453] (y)在按对上述用户新分配的选择顺序选择的位置以外的位置随机而不重复地分配字符

[0454] 另外，本提醒终端中，可以如下构成，

[0455] 上述提示部在将与上述多个资源服务器相关联的表的任一个提示给上述用户时，也将对该表内的各位置分配的引导字符与该各位置的要素一同提示给上述用户。

[0456] 本发明不脱离本发明的广义上的精神和范围而可以进行各种实施方式及变形。另外，上述的实施方式用于说明本发明，不限定本发明的范围。即，本发明的范围不通过实施方式表示，而通过权利要求的范围表示。而且，权利要求的范围内及与其同等的发明的意义的范围内实施的各种变形可以看作在本发明的范围内。

[0457] 在本申请中，针对世界知识产权组织主张以平成26年(2014年)9月8日(月)申请的国际申请PCT/JP2014/073704为基础的优先权，只要指定国的法令许可，则将该基础申请的内容编入本申请中。

[0458] 工业可利用性

[0459] 根据本发明，可以提供适于通过提醒终端来管理用于决定针对利用资源服务器的资源的请求的可否的密码的认证系统、该提醒终端、以及使计算机作为该提醒终端起作用的存储有程序的非临时性计算机可读信息记录介质。

[0460] 符号说明

[0461] 101 认证系统

[0462] 121 提醒终端

[0463] 141 接入终端

[0464] 161 资源服务器

[0465] 181 管理服务器

[0466] 191 计算机通信网络

[0467] 201 存储部

[0468] 202 提示部

[0469] 203 发送部

[0470] 204 表生成部

[0471] 205 密码注册部

[0472] 206 表注册部

[0473] 207 接收部

[0474] 208 规则生成部

[0475] 209 全更新部

[0476] 301 表

[0477] 303 服务器ID

[0478] 304 用户名

[0479] 305 附加要素

[0480] 311 导航

[0481] 312 导航

[0482] 313 导航

[0483] 321 完成按钮

[0484] 322 取消按钮

[0485] 501 浏览器

[0486] 502 URL栏

[0487] 503 内容栏

[0488] 511 登录框

[0489] 512 用户名栏

[0490] 513 密码栏

[0491] 514 登录按钮

[0492] 521 插件图标

[0493] 551 试行表

[0494] 552 前进按钮

[0495] 561 迁移表

[0496] 562 更新按钮

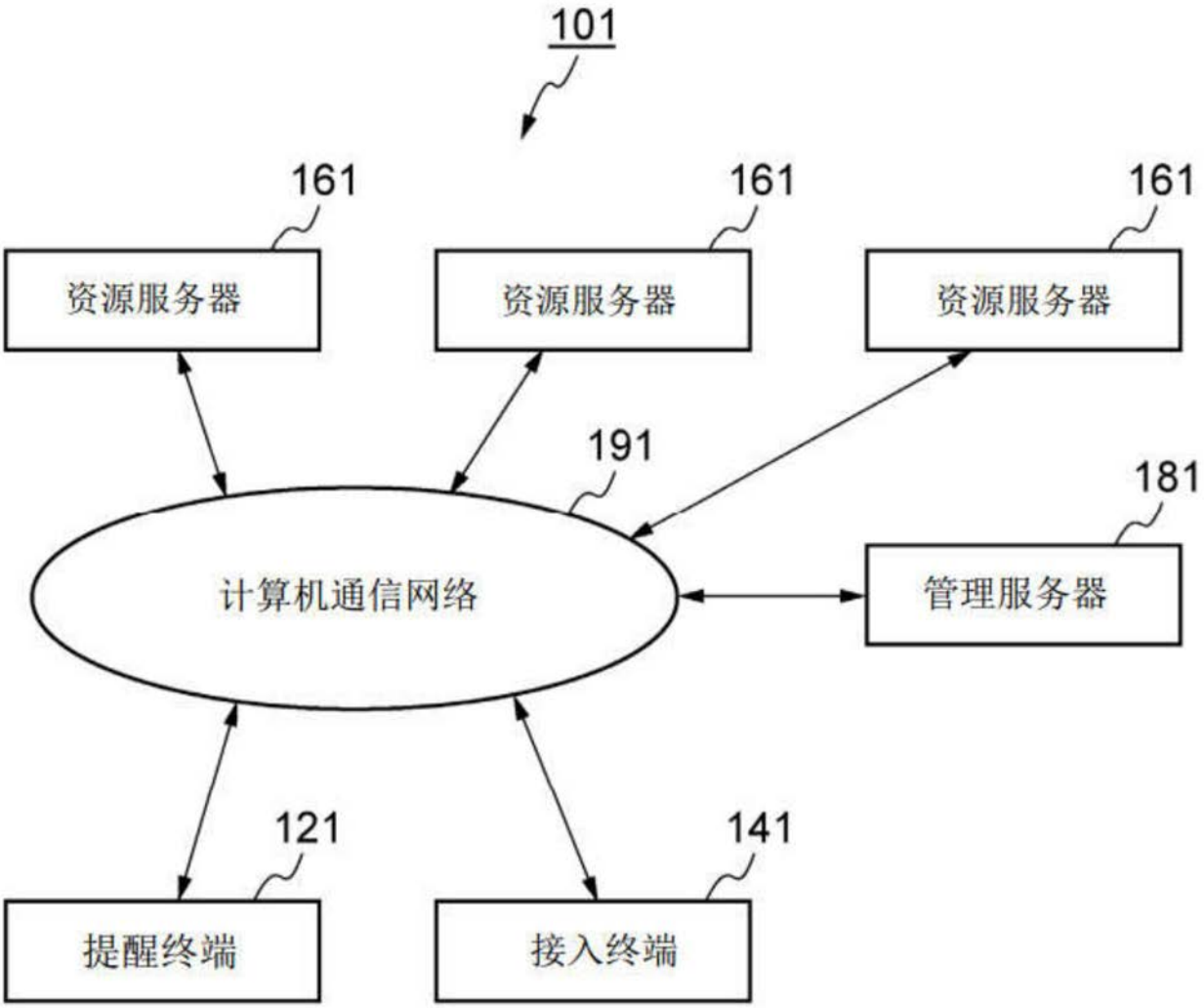

101
161
资源服务器
161
资源服务器
161
资源服务器
191
计算机通信网络
181
管理服务器
121
提醒终端
141
接入终端

图1

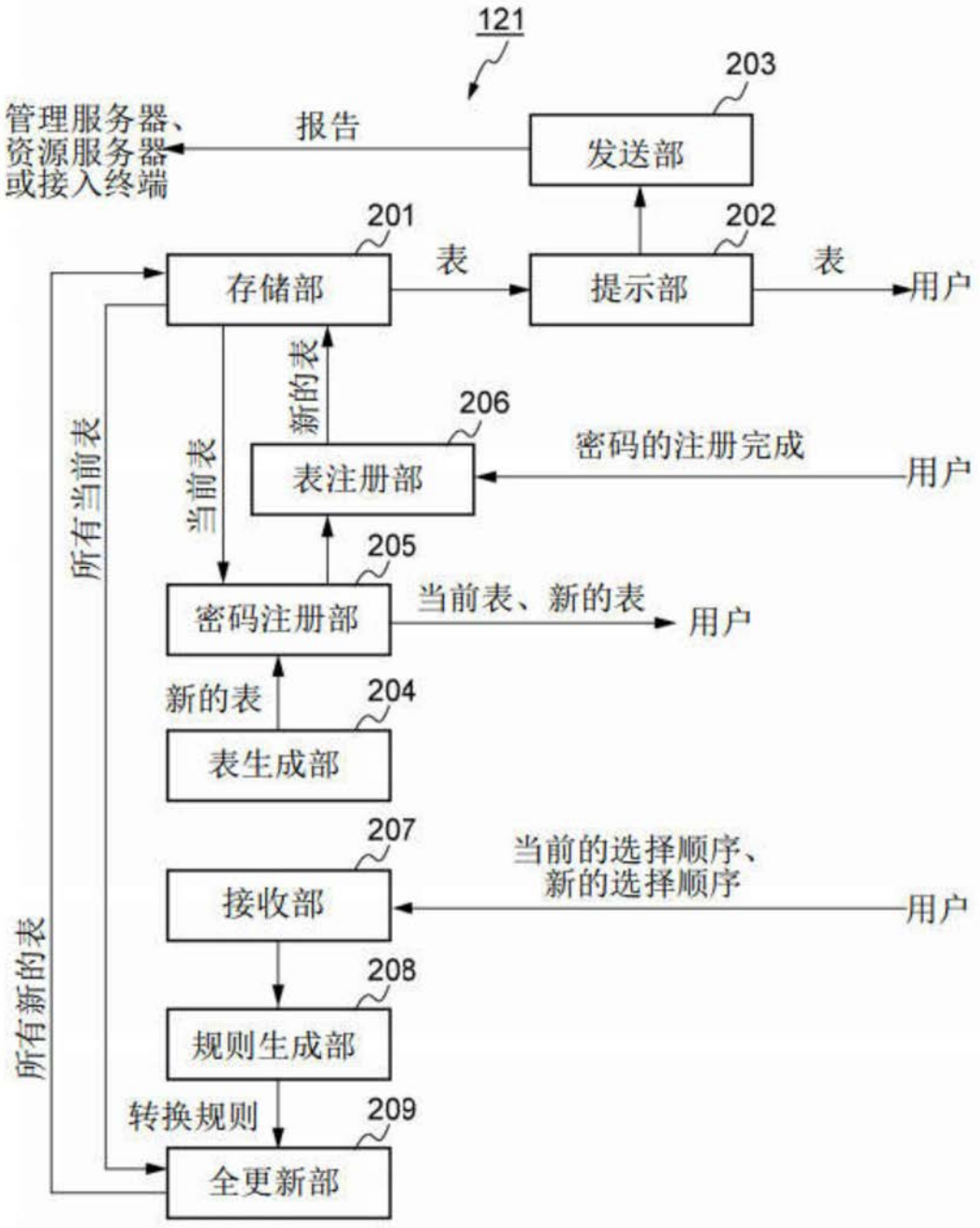

121
203
管理服务器、
资源服务器
或接入终端
报告
发送部
201
202
表
表
存储部
提示部
用户
新的表
206
密码的注册完成
表注册部
用户
当前表
所有当前表
205
密码注册部
当前表、新的表
用户
新的表
204
表生成部
207
当前的选择顺序、
新的选择顺序
接收部
用户
208
规则生成部
转换规则
209
所有新的表
全更新部

图2

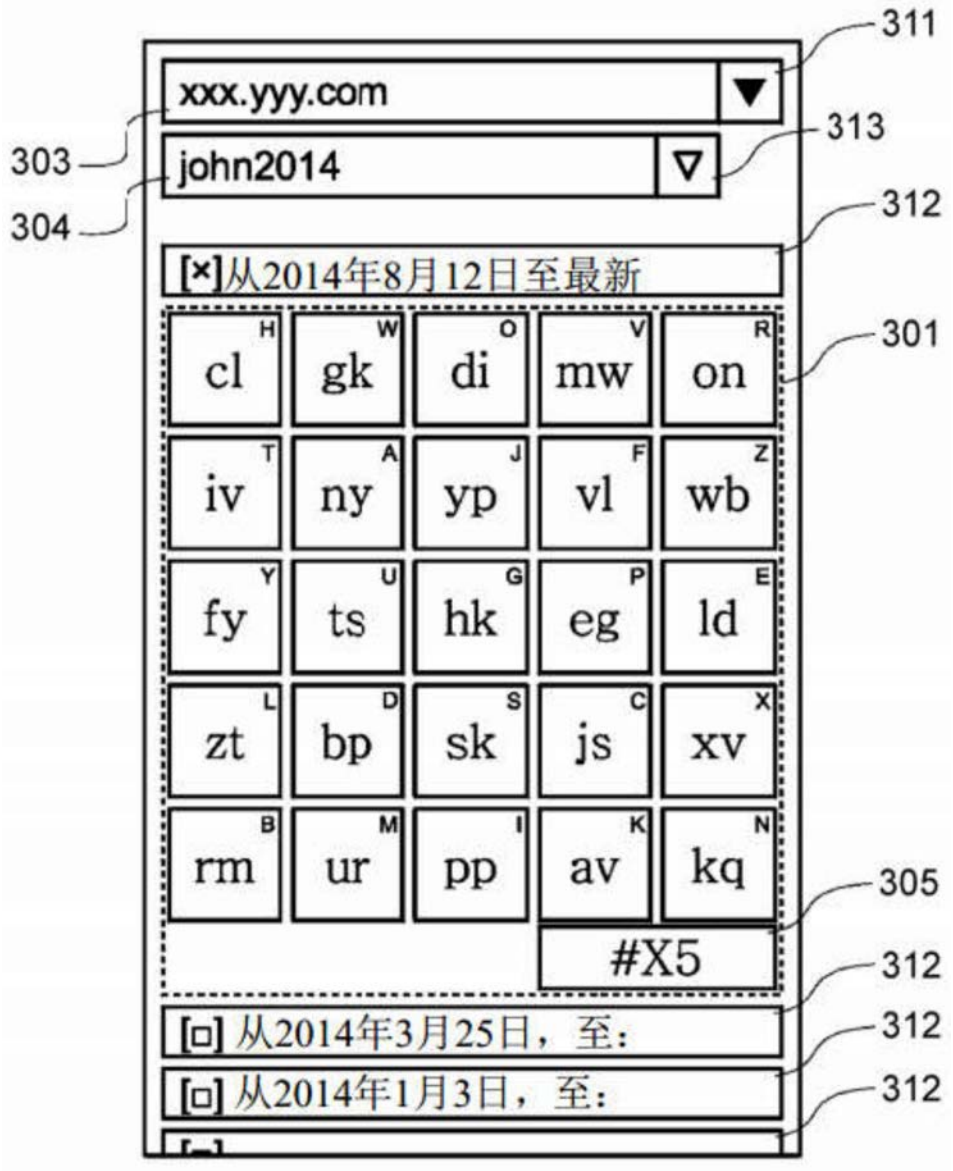

311
xxx.yyy.com
303
313
john2014
304
312
[×]从2014年8月12日至最新
301
H cl
W gk
O di
V mw
R on
T iv
A ny
J yp
F vl
Z wb
Y fy
U ts
G hk
P eg
E ld
L zt
D bp
S sk
C js
X xv
B rm
M ur
I pp
K av
N kq
305
#X5
312
[□] 从2014年3月25日，至：
312
[□] 从2014年1月3日，至：
312

图3A

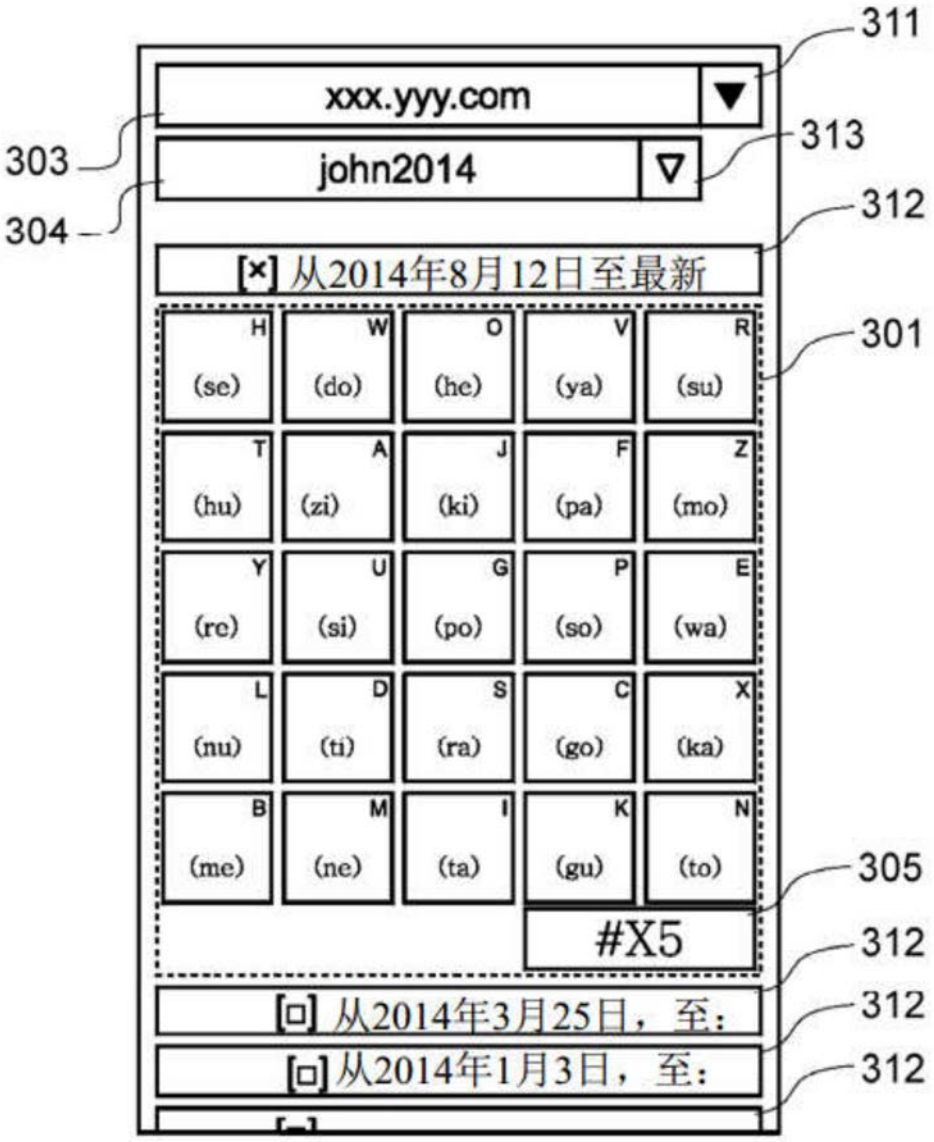

311
xxx.yyy.com
303
313
john2014
304
312
[×] 从2014年8月12日至最新
301
H (se)
W (do)
O (he)
V (ya)
R (su)
T (hu)
A (zi)
J (ki)
F (pa)
Z (mo)
Y (re)
U (si)
G (po)
P (so)
E (wa)
L (nu)
D (ti)
S (ra)
C (go)
X (ka)
B (me)
M (ne)
I (ta)
K (gu)
N (to)
305
#X5
312
[□] 从2014年3月25日，至：
312
[□] 从2014年1月3日，至：
312

图3B

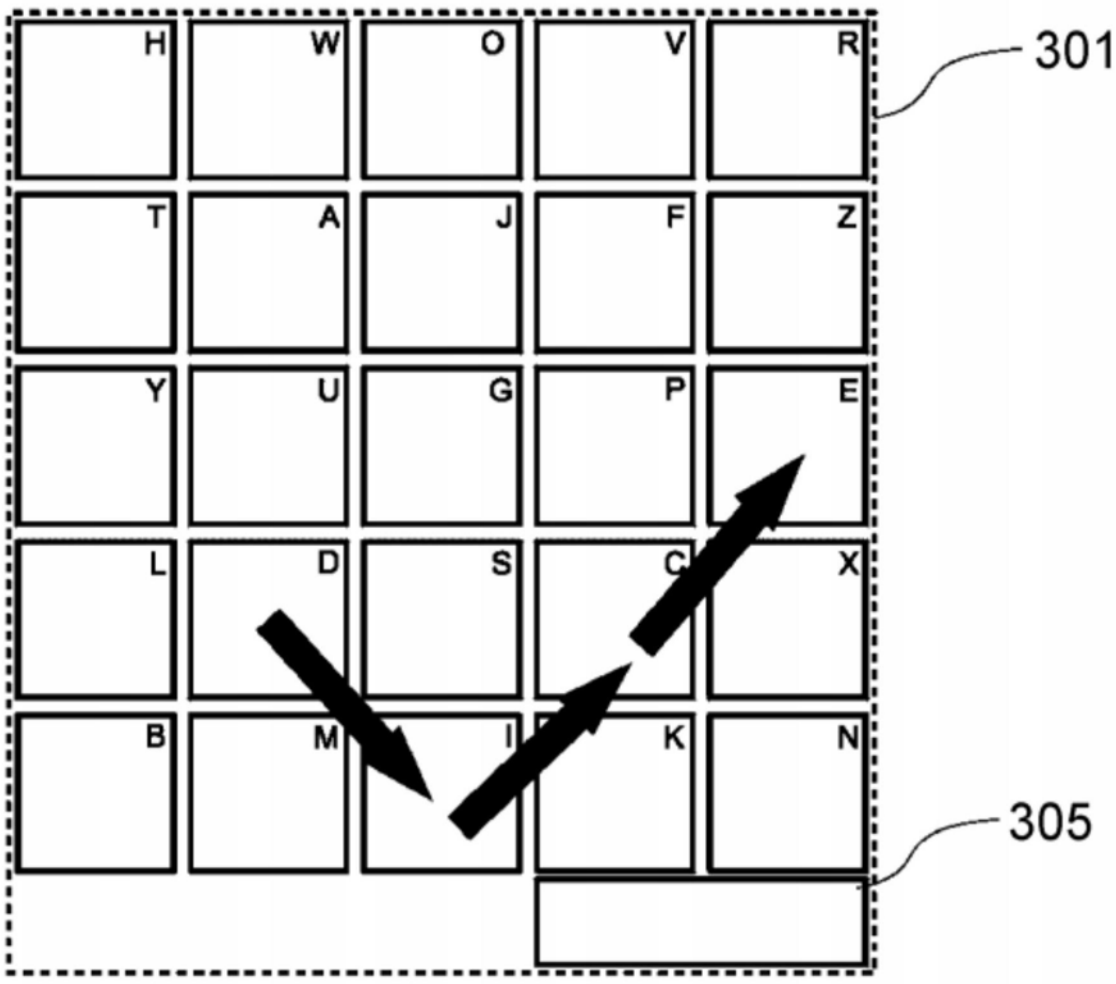



图4

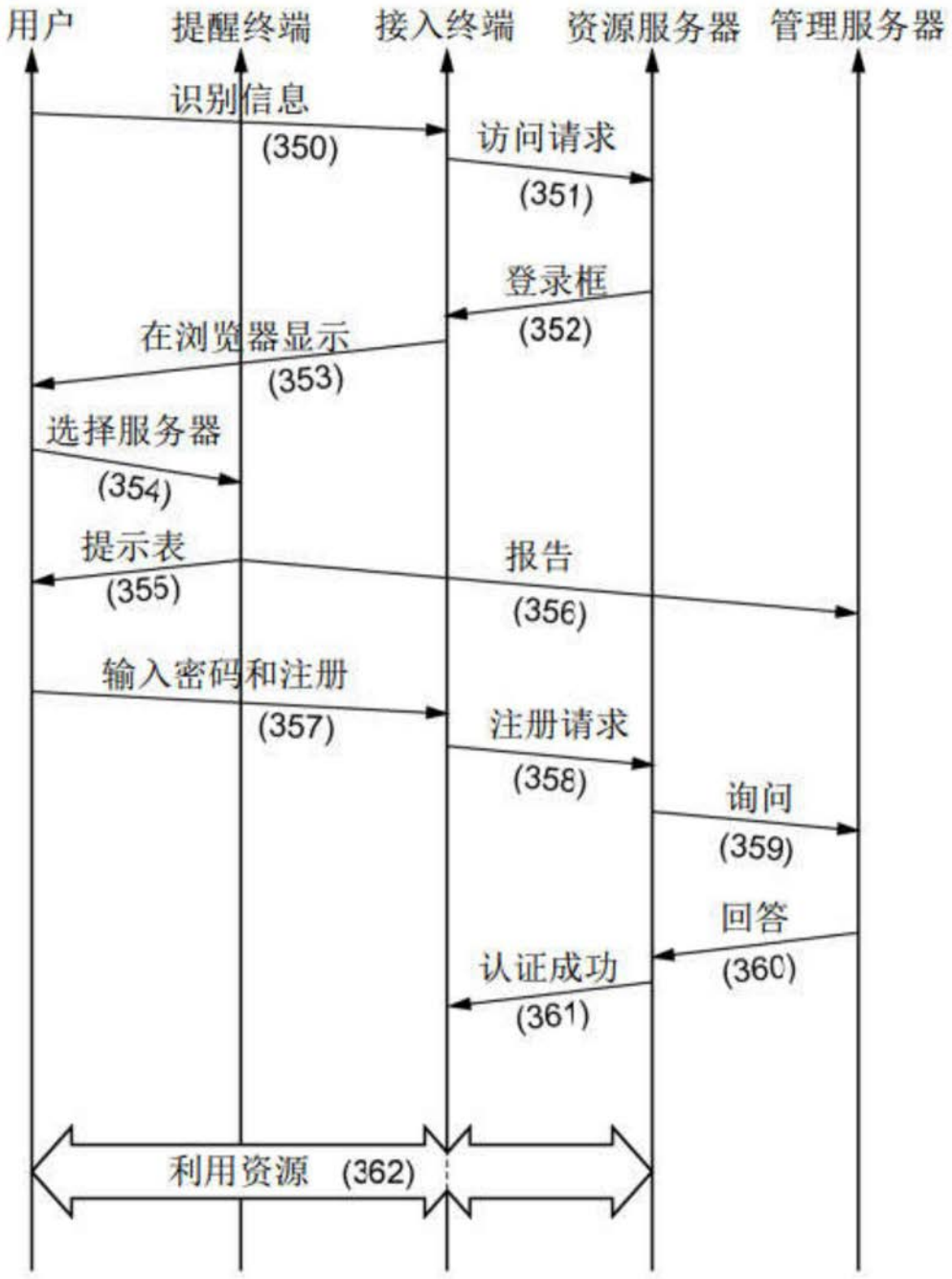

用户
提醒终端
接入终端
资源服务器
管理服务器
识别信息
(350)
访问请求
(351)
登录框
(352)
在浏览器显示
(353)
选择服务器
(354)
提示表
(355)
报告
(356)
输入密码和注册
(357)
注册请求
(358)
询问
(359)
回答
(360)
认证成功
(361)
利用资源 (362)

图5

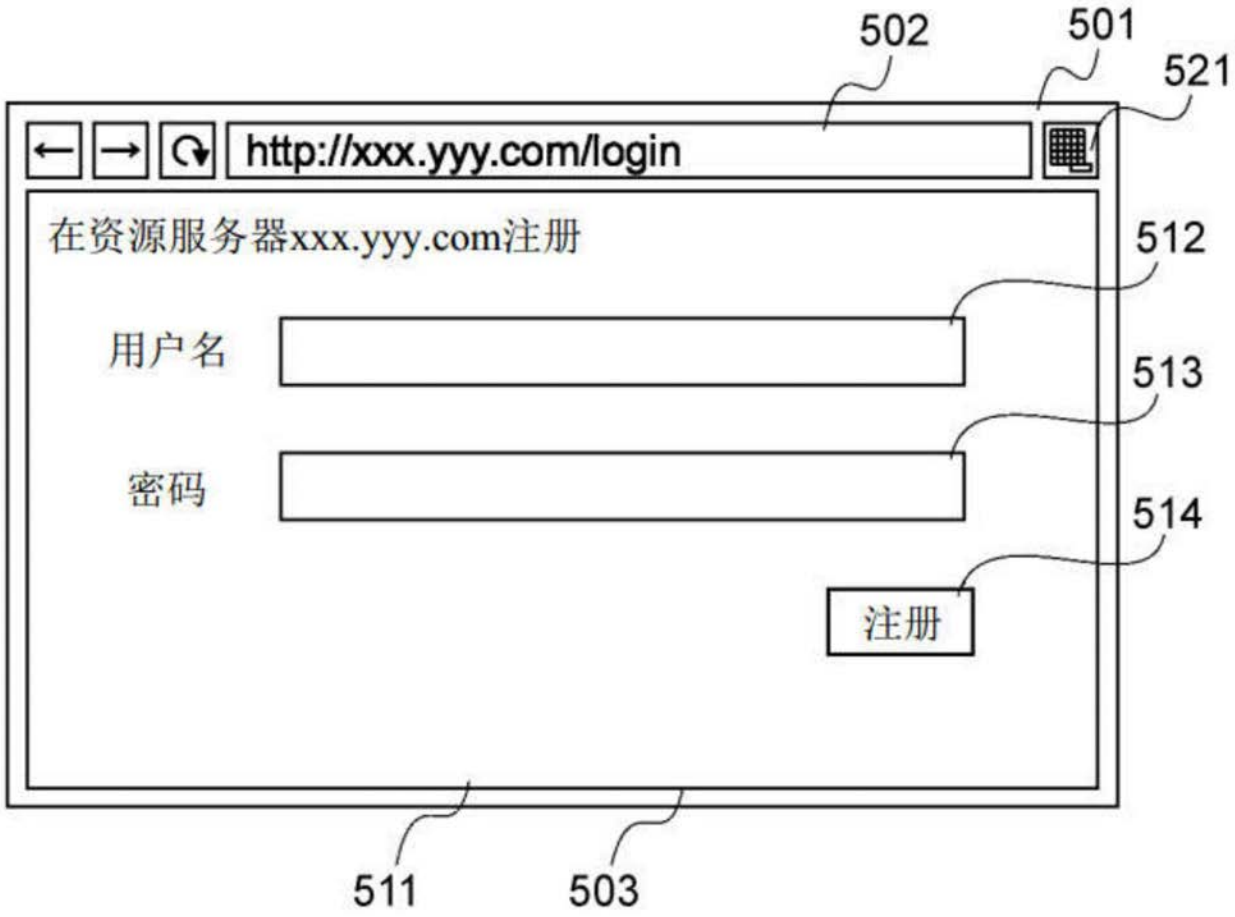

502
501
521
http://xxx.yyy.com/login
在资源服务器xxx.yyy.com注册
512
用户名
513
密码
514
注册
511
503

图6

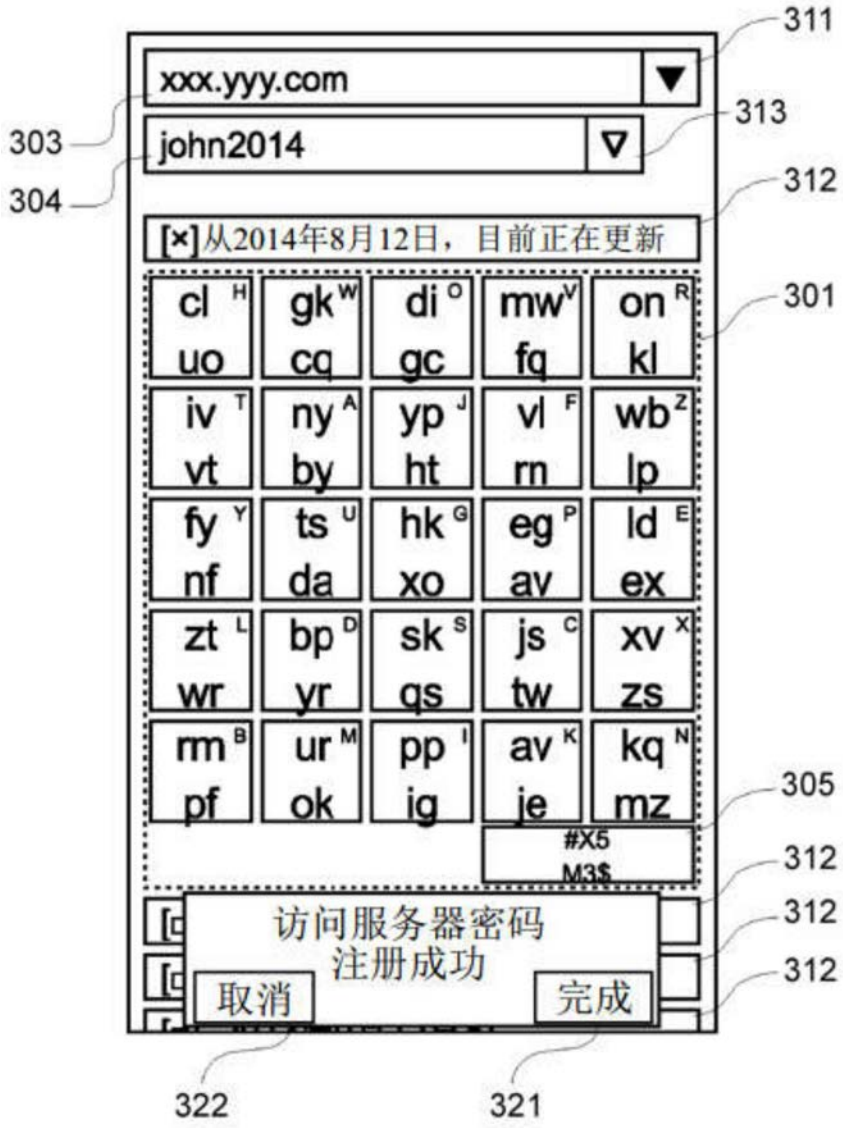

311
xxx.yyy.com
303
john2014
313
304
312
[×]从2014年8月12日，目前正在更新
301
cl H uo
gk W cq
di O gc
mw V fq
on R kl
iv T vt
ny A by
yp J ht
vl F rn
wb Z lp
fy Y nf
ts U da
hk G xo
eg P av
ld E ex
zt L wr
bp D yr
sk S qs
js C tw
xv X zs
rm B pf
ur M ok
pp I ig
av K je
kq N mz
305
#X5
M3$
312
访问服务器密码
注册成功
312
取消
完成
312
322
321

图7

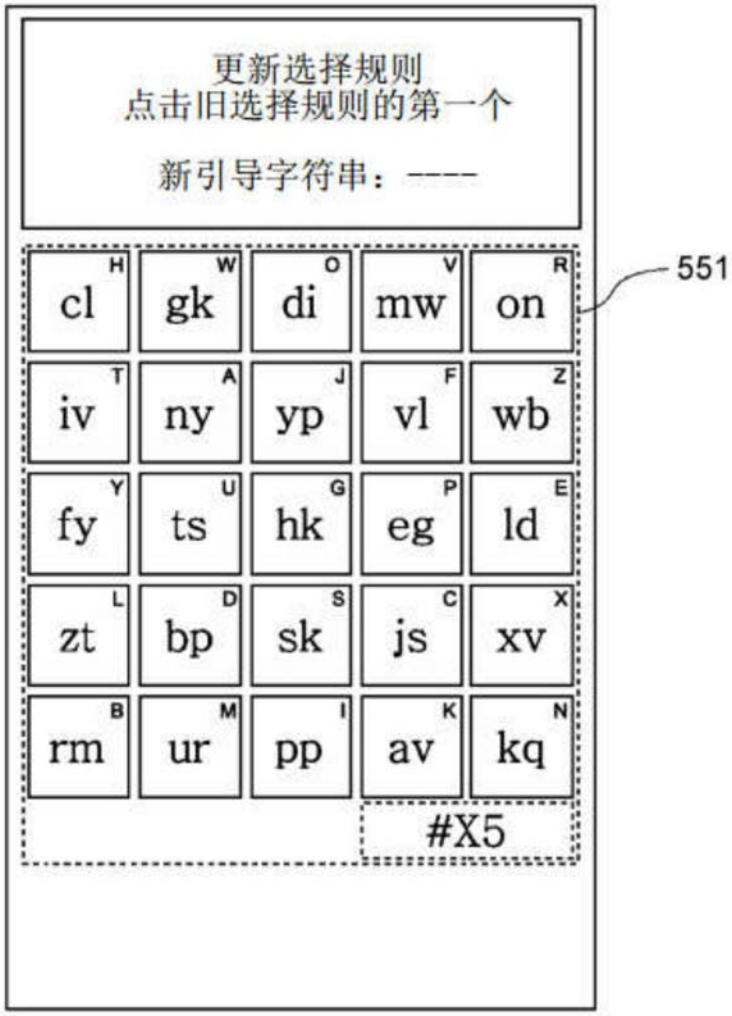

更新选择规则
点击旧选择规则的第一个
新引导字符串：----
H cl
W gk
O di
V mw
R on
T iv
A ny
J yp
F vl
Z wb
Y fy
U ts
G hk
P eg
E ld
L zt
D bp
S sk
C js
X xv
B rm
M ur
I pp
K av
N kq
#X5
551

图8A

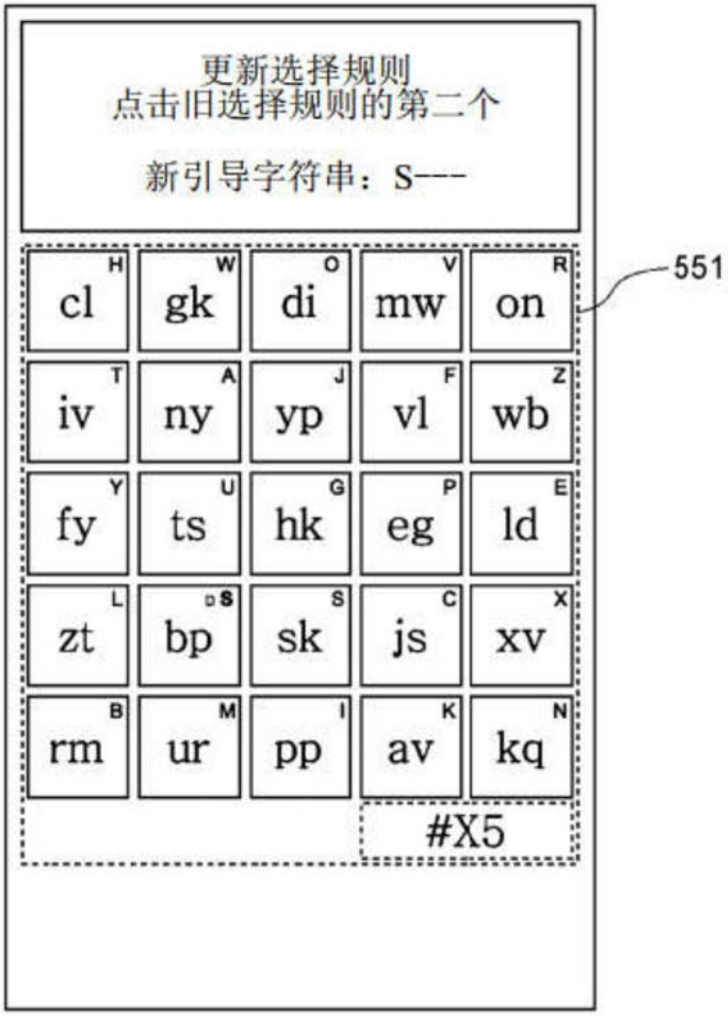

更新选择规则
点击旧选择规则的第二个
新引导字符串：S---
cl
gk
di
mw
on
iv
ny
yp
vl
wb
fy
ts
hk
eg
ld
zt
bp
sk
js
xv
rm
ur
pp
av
kq
#X5
551

图8B

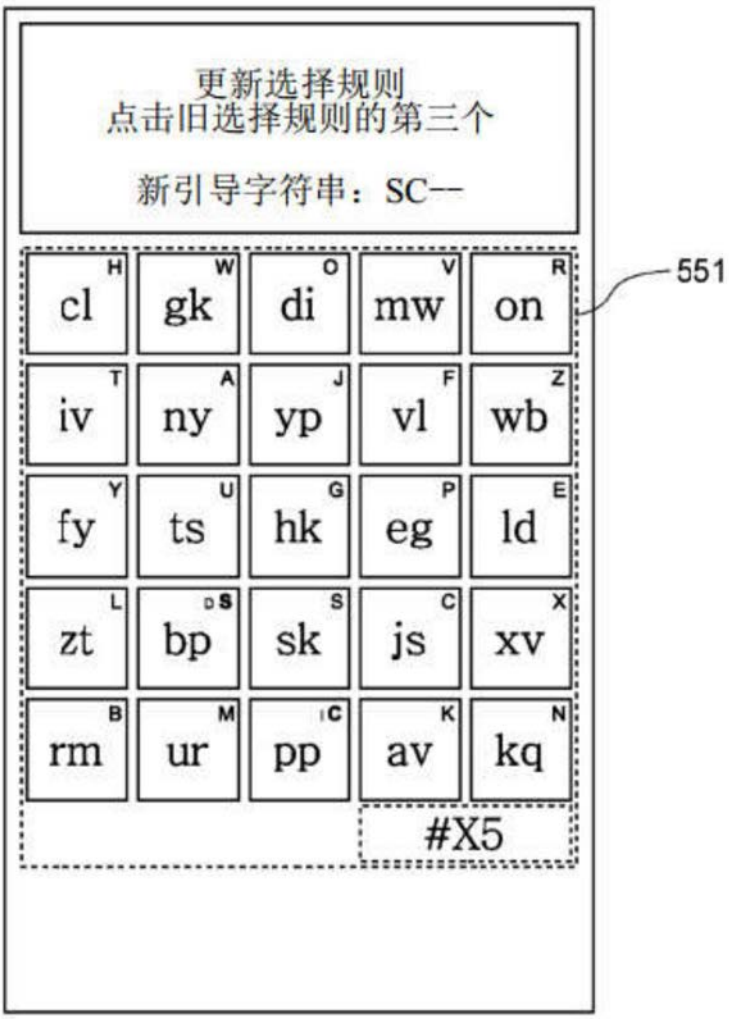

更新选择规则
点击旧选择规则的第三个
新引导字符串：SC—
551
cl
gk
di
mw
on
iv
ny
yp
vl
wb
fy
ts
hk
eg
ld
zt
bp
sk
js
xv
rm
ur
pp
av
kq
#X5

图8C

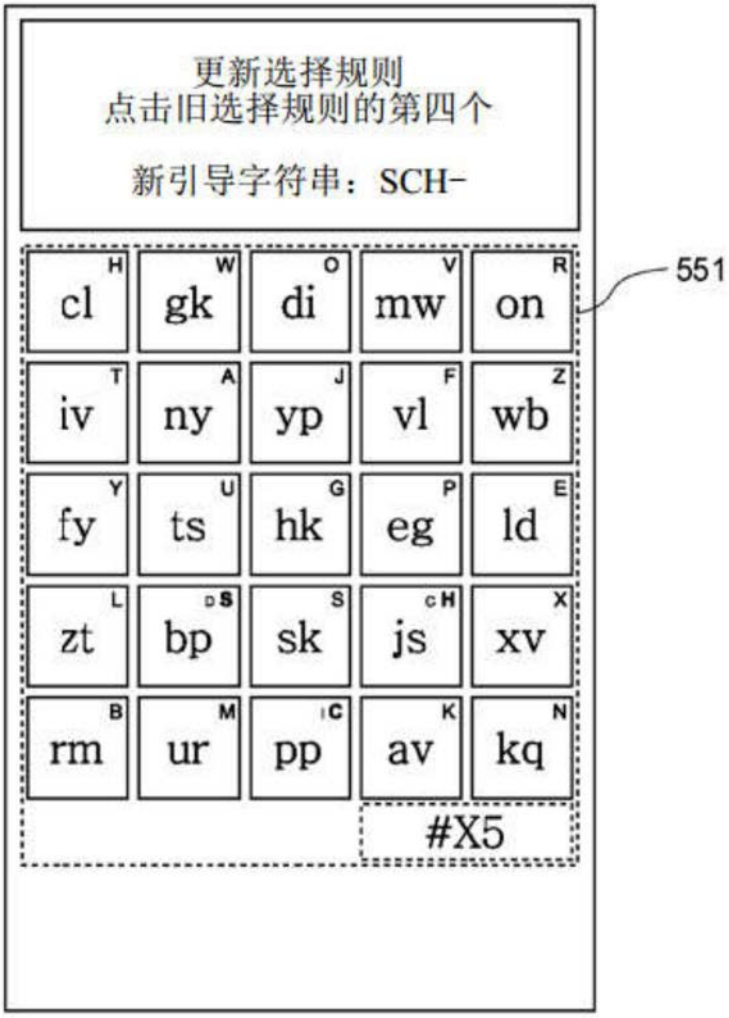

更新选择规则
点击旧选择规则的第四个
新引导字符串：SCH-
551
cl
gk
di
mw
on
iv
ny
yp
vl
wb
fy
ts
hk
eg
ld
zt
bp
sk
js
xv
rm
ur
pp
av
kq
#X5

图8D

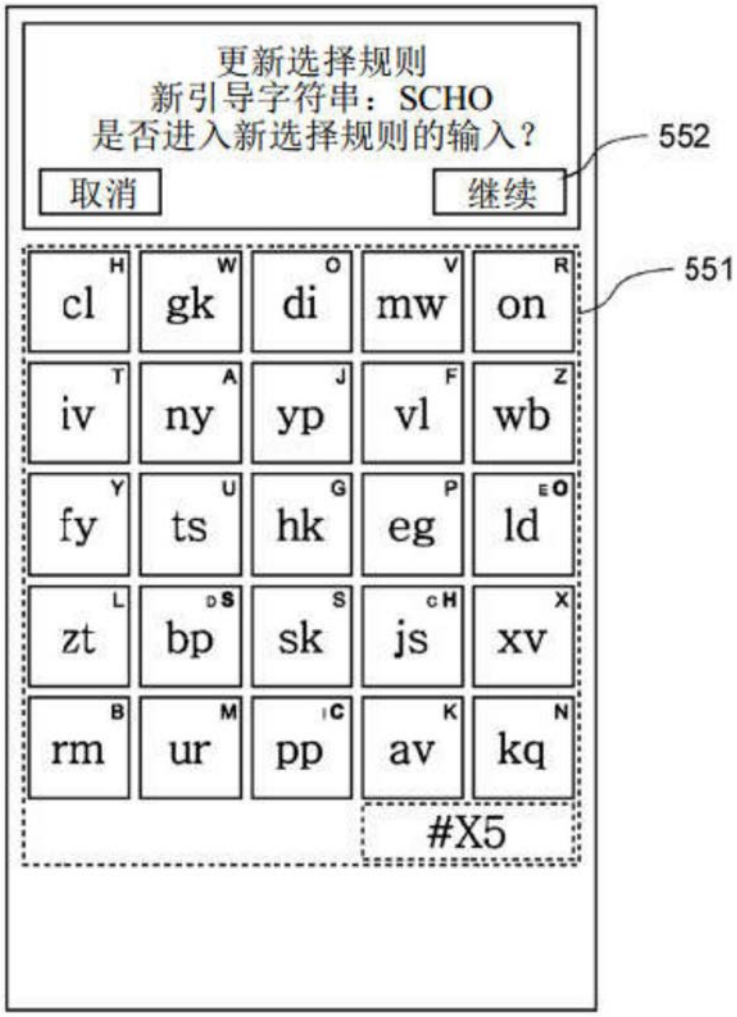

更新选择规则
新引导字符串：SCHO
是否进入新选择规则的输入？
取消
继续
552
551
cl
gk
di
mw
on
iv
ny
yp
vl
wb
fy
ts
hk
eg
ld
zt
bp
sk
js
xv
rm
ur
pp
av
kq
#X5

图8E

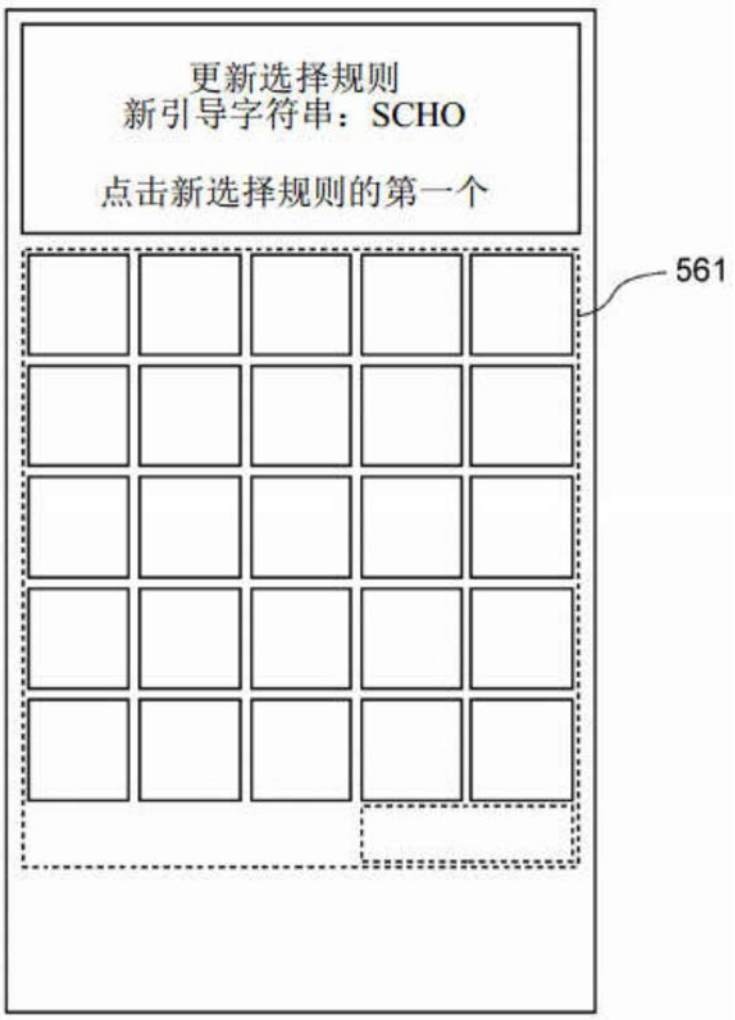



图9A

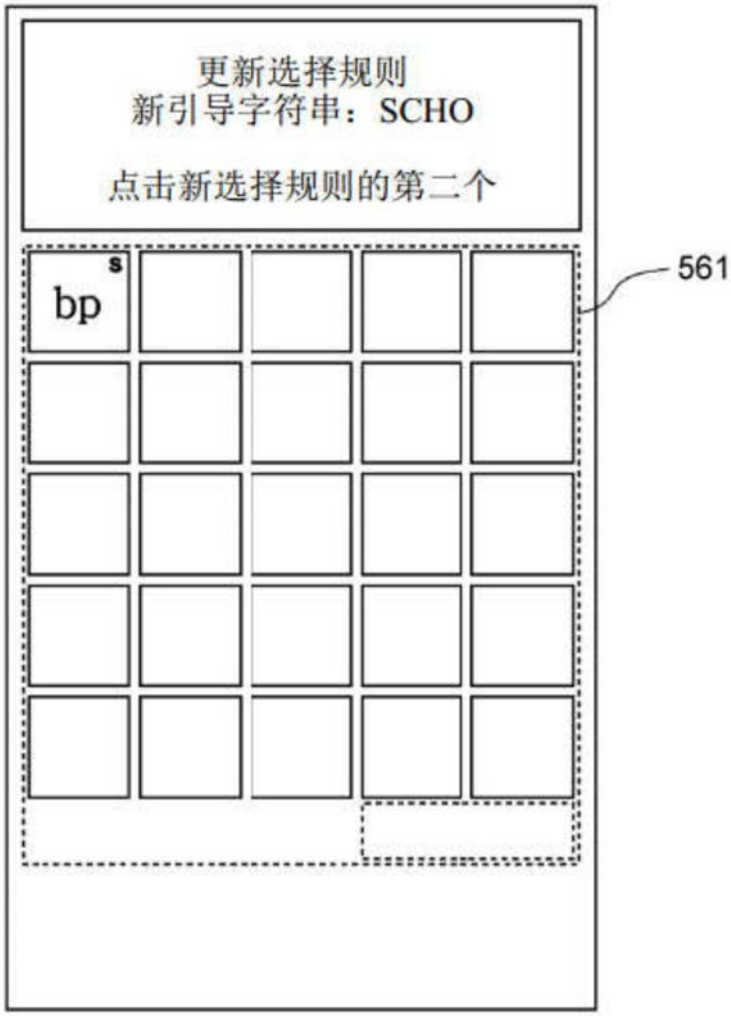



图9B

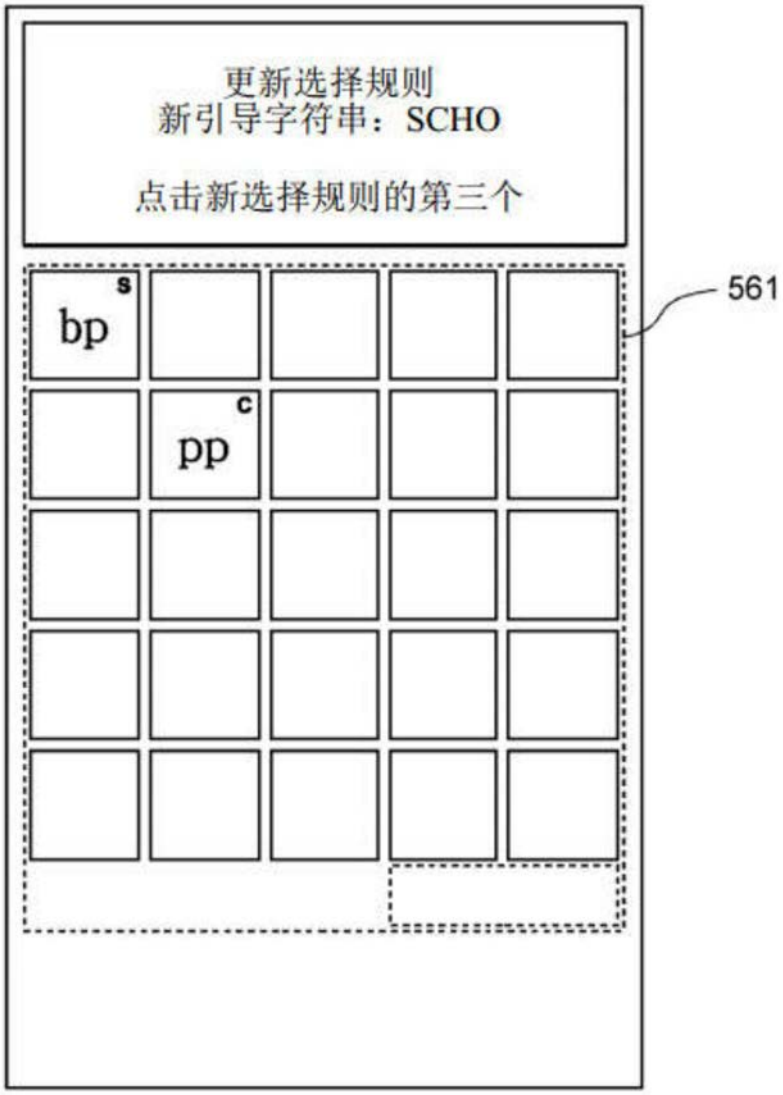



图9C

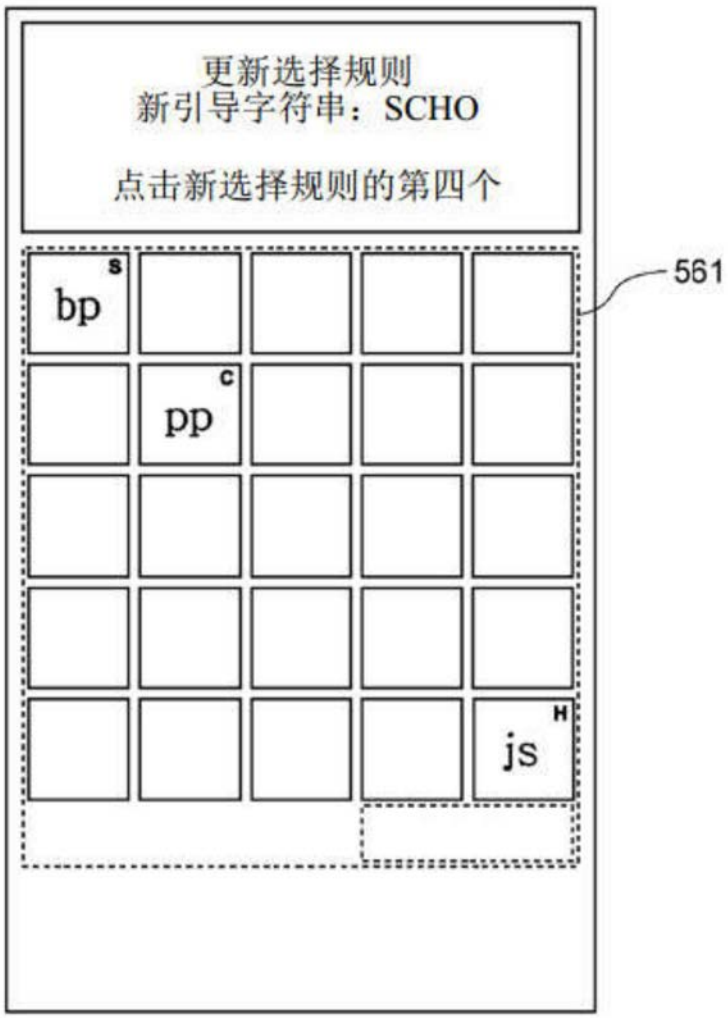



图9D

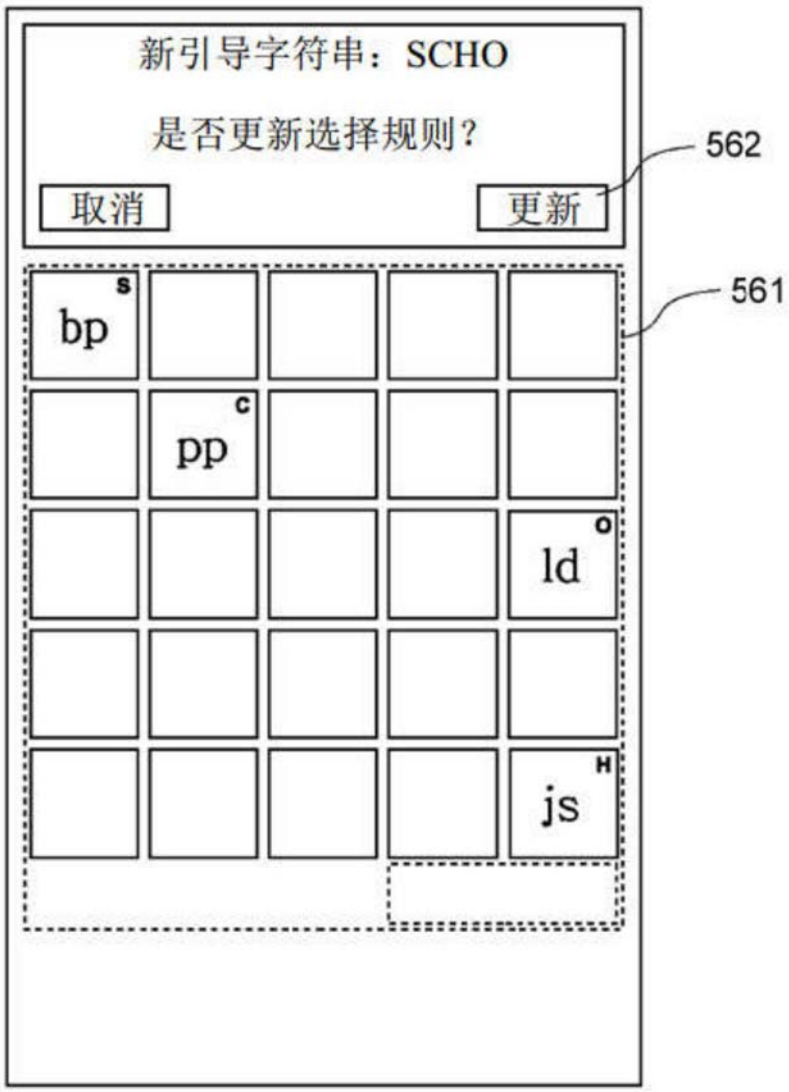



图9E

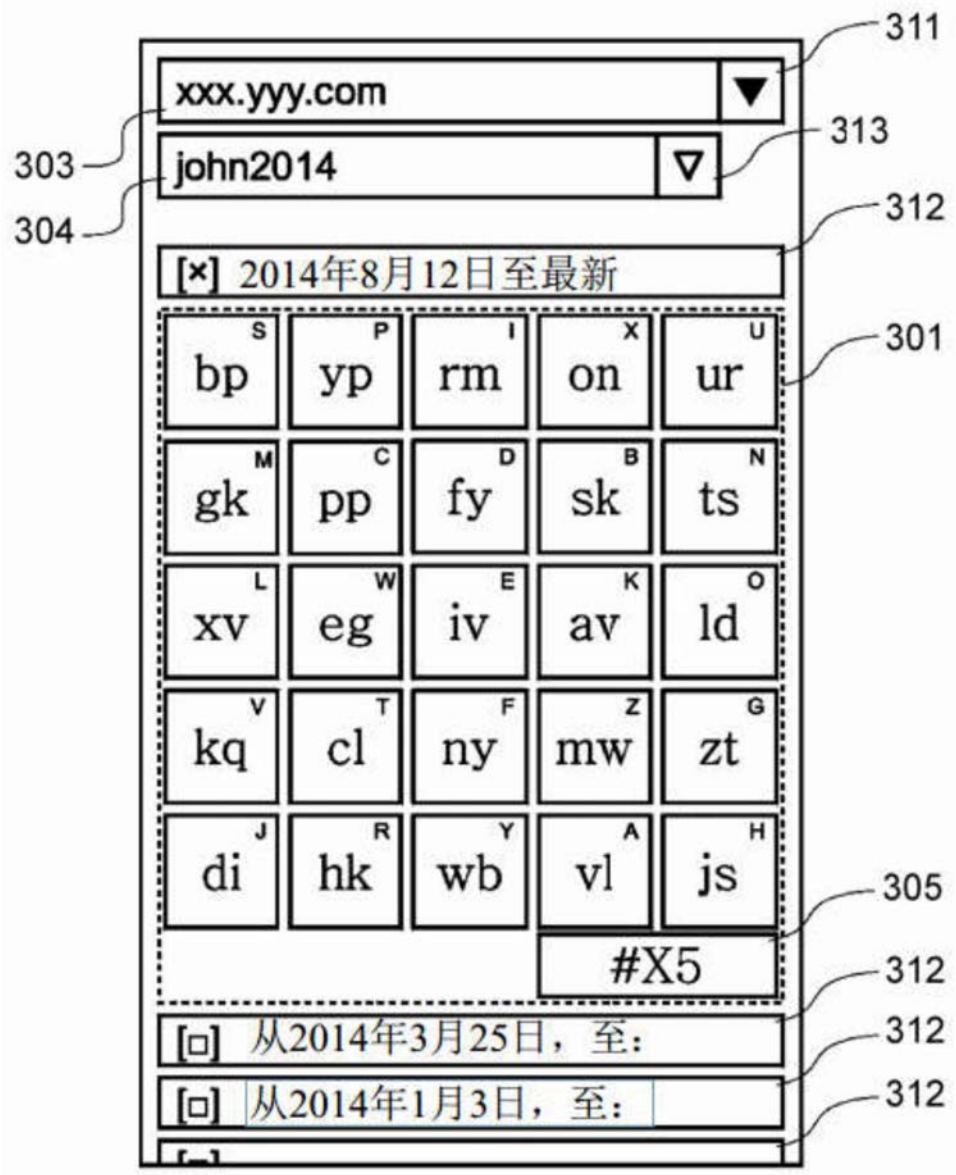

311
xxx.yyy.com
303
313
john2014
304
312
[×] 2014年8月12日至最新
301
S bp
P yp
I rm
X on
U ur
M gk
C pp
D fy
B sk
N ts
L xv
W eg
E iv
K av
O ld
V kq
T cl
F ny
Z mw
G zt
J di
R hk
Y wb
A vl
H js
305
#X5
312
[□] 从2014年3月25日，至：
312
[□] 从2014年1月3日，至：
312

图10

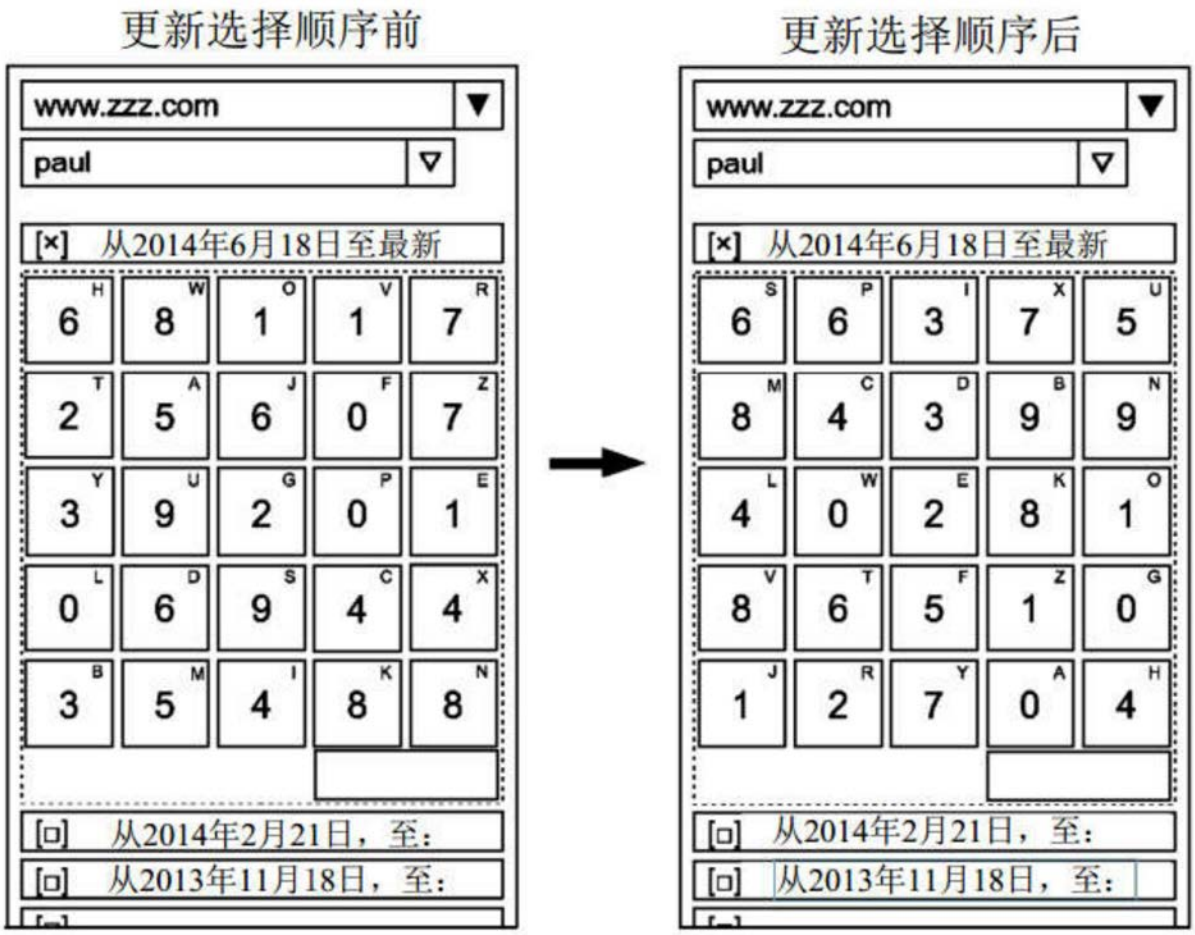

更新选择顺序前
www.zzz.com
paul
[×] 从2014年6月18日至最新
[□] 从2014年2月21日，至：
[□] 从2013年11月18日，至：
更新选择顺序后
www.zzz.com
paul
[×] 从2014年6月18日至最新
[□] 从2014年2月21日，至：
[□] 从2013年11月18日，至：

图11