

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 753 147**

51 Int. Cl.:

G06F 21/31 (2013.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **30.01.2012 PCT/JP2012/052013**

87 Fecha y número de publicación internacional: **06.12.2012 WO12164970**

96 Fecha de presentación y número de la solicitud europea: **30.01.2012 E 12792699 (6)**

97 Fecha y número de publicación de la concesión europea: **28.08.2019 EP 2717183**

54 Título: **Sistema de procesamiento de información, procedimiento de procesamiento de información, dispositivo de procesamiento de información, programa y medio de almacenamiento**

30 Prioridad:

31.05.2011 JP 2011122968

45 Fecha de publicación y mención en BOPI de la traducción de la patente:

07.04.2020

73 Titular/es:

**RAKUTEN, INC. (100.0%)
1-14-1, Tamagawa, Setagaya-ku
Tokyo 158-0094, JP**

72 Inventor/es:

YAMAHARA, HISANORI

74 Agente/Representante:

GARCÍA GONZÁLEZ, Sergio

ES 2 753 147 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Sistema de procesamiento de información, procedimiento de procesamiento de información, dispositivo de procesamiento de información, programa y medio de almacenamiento

5

Campo técnico

La presente invención se refiere a un sistema de procesamiento de información, un procedimiento de procesamiento de información, un dispositivo de procesamiento de información, un programa y un medio de almacenamiento.

10

Técnica antecedente

Existen sitios de compras y otros que están configurados para proporcionar pantallas que se han personalizado para cada usuario en función de un historial de compras, un historial de navegación, sexo, edad y similares.

15

Como una tecnología de protección de la privacidad para dichos sitios web, la Literatura de Patente 1 divulga un dispositivo de procesamiento de información que evalúa si la información se utiliza o su uso está limitado desde el punto de vista de una propiedad de confidencialidad y similares de la información, y es capaz de limitar el uso de la información cuando se juzga que su uso debe ser limitado. Los documentos de solicitud de patente JP2003-203139 A, US2007250920 A1, US2010212002 A1 y US2009247123 A1 divulgan enseñanzas relacionadas con el campo de la invención.

20

Sumario de la invención

25

La invención se define por las reivindicaciones independientes adjuntas.

Problema técnico

Es conveniente si el usuario puede limitar un rango de información que forma la base de una pantalla que se ha personalizado para cada usuario. Sin embargo, cuando se requiere una operación explícita para limitar el rango de la información que forma la base de la pantalla personalizada, otra persona advierte fácilmente dicha operación explícita. Como resultado, existe el temor de que la persona pueda sentir que el usuario tiene alguna información que ocultar.

30

35

La presente invención se ha realizado en vista del problema mencionado anteriormente y, por lo tanto, tiene el objetivo de reducir el temor de que otra persona advierta la limitación del rango de la información que forma la base de la pantalla proporcionada al usuario.

40

Solución al problema

Para resolver el problema mencionado anteriormente, según una realización de la presente invención, se proporciona un sistema de procesamiento de información que incluye: medios de identificación de información de control para identificar información de control, que es información diferente de una contraseña, en base a contenido de una operación realizada en un campo de entrada de contraseña con un dispositivo de entrada; medios de identificación de rango visualizable públicamente para identificar un rango de información visualizable públicamente sobre un usuario en base a la información de control; y medios de limitación para limitar un rango de información que forma una base de una pantalla proporcionada al usuario de modo que el rango de la información se encuentre dentro del rango visualizable públicamente identificado por los medios de identificación de rango visualizable públicamente.

45

50

Además, según una realización de la presente invención, se proporciona un procedimiento de procesamiento de información que incluye: una etapa de identificación de información de control para identificar información de control, que es información diferente de una contraseña, en base al contenido de una operación realizada en un campo de entrada de contraseña con un dispositivo de entrada; una etapa de identificación de rango visualizable públicamente para identificar un rango de información visualizable públicamente sobre un usuario en base a la información de control; y una etapa de limitación de limitar un rango de información que forma una base de una pantalla proporcionada al usuario para que el rango de la información se encuentre dentro del rango visualizable públicamente identificado en la etapa de identificación del rango visualizable públicamente.

55

60

Además, según una realización de la presente invención, se proporciona un dispositivo de procesamiento de información que incluye: medios de identificación de rango visualizable públicamente para identificar un rango de información visualizable públicamente sobre un usuario en base a información de control, que es información diferente de una contraseña y se identifica en base al contenido de una operación realizada en un campo de entrada de contraseña con un dispositivo de entrada; y medios de limitación para limitar un rango de información

65

que forma una base de una pantalla proporcionada al usuario de modo que el rango de la información se encuentre dentro del rango visualizable públicamente identificado por los medios de identificación de rango visualizable públicamente.

5 Además, según una realización de la presente invención, se proporciona un programa para hacer que un ordenador funcione como: medios de identificación de rango visualizable públicamente para identificar un rango de información visualizable públicamente sobre un usuario en base a información de control, que es información diferente de una contraseña y se identifica en base al contenido de una operación realizada en un campo de entrada de contraseña con un dispositivo de entrada; y medios de limitación para limitar un rango de información
10 que forma una base de una pantalla proporcionada al usuario de modo que el rango de la información se encuentre dentro del rango visualizable públicamente identificado por los medios de identificación de rango visualizable públicamente.

15 Además, según una realización de la presente invención, se proporciona un medio de almacenamiento que tiene un programa almacenado en el mismo, el programa hace que un ordenador funcione como: medios de identificación de rango visualizable públicamente para identificar un rango de información visualizable públicamente sobre un usuario en base a información de control, que es información diferente de una contraseña y se identifica en base al contenido de una operación realizada en un campo de entrada de contraseña con un dispositivo de entrada; y medios de limitación para limitar un rango de información que forma una base de una
20 pantalla proporcionada al usuario de modo que el rango de la información se encuentre dentro del rango visualizable públicamente identificado por los medios de identificación de rango visualizable públicamente.

De acuerdo con la presente invención, la información de control se identifica en base al contenido de la operación realizada en el campo de entrada de contraseña con el dispositivo de entrada. Luego, el rango de la
25 información que forma la base de la pantalla proporcionada al usuario se limita al rango visualizable públicamente identificado en base a la información de control. Por lo tanto, de acuerdo con la presente invención, es posible reducir el temor de que otra persona advierta la limitación del rango de la información que forma la base de la pantalla proporcionada al usuario.

30 De acuerdo con un aspecto de la presente invención, los medios de identificación de rango visualizable públicamente identifican al menos un elemento de información entre uno o más elementos de información en el usuario, y los medios de limitación limitan, al menos, un elemento de información identificado, el rango de la información que forma la base de la pantalla proporcionada al usuario.

35 Además, de acuerdo con un aspecto de la presente invención, para cada uno de los elementos de información, se establece un nivel de confidencialidad que representa un grado de confidencialidad de la información, los medios de identificación de información de control identifican el nivel de confidencialidad, y los medios de identificación de rango visualizable públicamente identifican un elemento de información que ha establecido un nivel de confidencialidad que representa una confidencialidad que es inferior a la confidencialidad representada
40 por el nivel de confidencialidad identificado.

Además, de acuerdo con un aspecto de la presente invención, los medios de limitación limitan un rango de información mostrada en la pantalla proporcionada al usuario.

45 Además, de acuerdo con un aspecto de la presente invención, el sistema de procesamiento de información además incluye medios de control para controlar información incluida en la pantalla proporcionada al usuario de modo que se disponga información alternativa en lugar de información limitada para ser excluida de la pantalla.

50 Además, de acuerdo con un aspecto de la presente invención, cuando se cumple una condición de que la entrada de contraseña al dispositivo de entrada incluya una cadena de caracteres establecida de antemano por el usuario, el medio de limitación limita el rango de la información que forma la base de la pantalla.

55 Además, de acuerdo con un aspecto de la presente invención, cuando se ingresa al dispositivo de entrada cualquiera de una pluralidad de contraseñas asociadas con diferentes rangos de información, el medio de limitación limita el rango de la información que forma la base de la pantalla proporcionada al usuario de modo que el rango de la información se encuentre dentro de un rango de información asociado con cualquiera de la pluralidad de contraseñas ingresadas al dispositivo de entrada.

60 Además, de acuerdo con un aspecto de la presente invención, la pluralidad de contraseñas tiene el mismo número de caracteres.

Además, de acuerdo con un aspecto de la presente invención, al menos partes de las teclas utilizadas para ingresar caracteres en las mismas posiciones desde la parte superior de la pluralidad de contraseñas coinciden entre sí.

65

Además, de acuerdo con un aspecto de la presente invención, los medios de identificación de información de control identifican la información de control en base a un intervalo de entrada de caracteres incluidos en la contraseña o un período de tiempo calculado en base a un tiempo en el que se habilita el ingreso de la contraseña y un tiempo en el que se ingresa un carácter incluido en la contraseña.

5

Además, de acuerdo con un aspecto de la presente invención, el sistema de procesamiento de información además incluye medios de autenticación para autenticar al usuario utilizando la contraseña ingresada al dispositivo de entrada, y los medios de limitación limitan un rango de información que forma una base de una pantalla proporcionada cuando el usuario es autenticado de manera satisfactoria por los medios de autenticación de modo que el rango de la información se encuentre dentro del rango visualizable públicamente identificado por los medios de identificación de rango visualizable públicamente.

10

Breve descripción de los dibujos

15

La Figura 1 es un diagrama de configuración general de una red informática según una realización de la presente invención.

La Figura 2 es un diagrama que ilustra un ejemplo de una página de portal en modo privado.

La Figura 3 es un diagrama que ilustra un ejemplo de una página de portal en modo público.

La Figura 4 es un diagrama que ilustra un ejemplo de datos de historial de acceso.

20

La Figura 5 es un diagrama que ilustra un ejemplo de datos de historial de compras.

La Figura 6 es un diagrama de bloques funcional que ilustra un ejemplo de funciones implementadas por un servidor según la realización de la presente invención.

La Figura 7 es un diagrama que ilustra un ejemplo de datos de cuenta.

La Figura 8 es un diagrama que ilustra un ejemplo de datos maestros de artículos.

25

La Figura 9 es un diagrama que ilustra un ejemplo de datos de configuración de nivel de confidencialidad.

La Figura 10 es un diagrama de flujo que ilustra un ejemplo de un flujo de procesamiento realizado por el servidor según la realización de la presente invención.

La Figura 11 es un diagrama que ilustra otro ejemplo de la página de portal en el modo público.

30

Descripción de las realizaciones

A continuación, se describe en detalle una realización de la presente invención con referencia a los dibujos.

35

La Figura 1 es un diagrama de configuración general de un sistema de procesamiento de información 10 según la realización de la presente invención. Como se ilustra en la Figura 1, el sistema de procesamiento de información 10 incluye un servidor 12 y terminales de usuario 14 (14-1 a 14-n), cada una de las cuales está constituida principalmente por un ordenador. El servidor 12 y cada una de las terminales de usuario 14 son comunicables entre sí a través de una red informática 16 tal como Internet.

40

El servidor 12 según esta realización es un dispositivo de procesamiento de información que incluye una unidad de control, que es un dispositivo de control de programa tal como una unidad central de procesamiento (CPU) y opera de acuerdo con los programas instalados en el servidor 12, una unidad de almacenamiento como un elemento de memoria, por ejemplo, una memoria de solo lectura (ROM) y una memoria de acceso aleatorio (RAM), o una unidad de disco duro, y una unidad de comunicación, que es una interfaz de comunicación como una placa de red. Esos elementos están conectados a través de un bus. La unidad de almacenamiento del servidor 12 almacena los programas a ejecutar por la unidad de control del servidor 12. La unidad de almacenamiento del servidor 12 también funciona como memoria de trabajo del servidor 12. El servidor 12 según esta realización es capaz de usar una tecnología web para proporcionar a un usuario un servicio tal como un sitio de compras en el que un artículo o servicio se puede comprar en línea.

50

La terminal de usuario 14 es, por ejemplo, un dispositivo de procesamiento de información tal como un ordenador personal, un teléfono móvil, un asistente digital personal (PDA) y un teléfono inteligente. La terminal de usuario 14 incluye, por ejemplo, una unidad de control como una CPU, una unidad de almacenamiento como un elemento de memoria, por ejemplo, una ROM y una RAM, y una unidad de disco duro, una unidad de salida como una pantalla, una unidad de entrada como un ratón, un teclado, un panel táctil y un botón, y una unidad de comunicación como una placa de red. Además, en la terminal de usuario 14 según esta realización, se preinstala un navegador web y se ejecuta un programa del navegador web. La terminal de usuario 14 recibe el servicio proporcionado por el servidor 12 a través del navegador web.

55

60

En esta realización, cuando la terminal de usuario 14 accede a una página web colocada en el servidor 12 a través del navegador web, la página web se muestra en la pantalla de la terminal de usuario 14. Además, después de que el servidor 12 ejecuta el procesamiento de autenticación del usuario, el servidor 12 puede determinar un identificador del usuario (ID de usuario) que usa la terminal de usuario 14.

65

En esta realización, se muestra, en el monitor de la terminal de usuario 14, a través del navegador web, una

página de inicio de sesión (no mostrada), que es proporcionada por el servidor 12 según esta realización y en la que se disponen un campo de entrada de ID de usuario, un campo de entrada de contraseña y un botón de inicio de sesión, . Luego, el usuario hace clic en el campo de entrada de ID de usuario o realiza otra operación para lograr un estado en el que se muestra un mensaje en el campo de entrada de ID de usuario, y luego usa un dispositivo de entrada como el teclado para ingresar el ID de usuario en el campo de entrada de ID de usuario. Luego, el usuario hace clic en el campo de entrada de contraseña o realiza otra operación para lograr un estado en el que se muestra un mensaje en el campo de entrada de contraseña, y luego usa el dispositivo de entrada como el teclado para ingresar una contraseña en el campo de entrada de contraseña. Luego, cuando el usuario hace clic en el botón de inicio de sesión, el ID de usuario y la contraseña ingresados se transmiten al servidor 12. Luego, el servidor 12 ejecuta el procesamiento de autenticación en base al ID de usuario y la contraseña, que se transmiten desde la terminal de usuario 14. Luego, cuando la autenticación es exitosa, el servidor 12 genera una página de portal del sitio de compras (en esta realización, una página de portal 20 en un modo privado ilustrado en la Figura 2 o una página de portal 22 en un modo público ilustrado en la Figura 3) dependiendo del modo de entrada de la contraseña recibida desde la terminal de usuario 14, y transmite la página de portal a la terminal de usuario 14. Luego, la terminal de usuario 14 emite la página recibida para visualizarla en el monitor a través del navegador web.

Además, en esta realización, cuando el usuario accede a una página que presenta un artículo o servicio vendido en el sitio de compras, el servidor 12 genera datos de historial de acceso 24 ejemplificados en la Figura 4, que incluye el ID de usuario del usuario que accede a la página, un identificador del artículo (ID de artículo) o servicio introducido en la página, información de fecha/hora de acceso que indica la fecha y hora en que se accede a la página, y similares, y almacena los datos de historial de acceso 24 en la unidad de almacenamiento incluida en el servidor 12. Además, cuando el usuario compra un artículo o servicio vendido en el sitio de compras, el servidor 12 genera datos de historial de compras 26 ejemplificados en la Figura 5, que incluye el ID de usuario del usuario que compra el artículo o servicio, el ID de artículo del artículo o servicio, información que indica la fecha y hora de compra del artículo o servicio, y similares, y almacena los datos de historial de compras 26 en la unidad de almacenamiento incluida en el servidor 12.

La Figura 6 es un diagrama de bloques funcional que ilustra un ejemplo de funciones implementadas por el servidor 12 según esta realización. El servidor 12 según esta realización incluye funcionalmente una unidad de almacenamiento de datos 30, una unidad de recepción 32, una unidad de autenticación 34, una unidad de generación de página 36 y una unidad de salida de página 38. La unidad de almacenamiento de datos 30 es implementada principalmente por la unidad de almacenamiento del servidor 12. La unidad receptora 32 y la unidad de salida de página 38 son implementadas principalmente por la unidad de control y la unidad de comunicación del servidor 12. Los otros elementos son implementados principalmente por la unidad de control del servidor 12.

Esos elementos se implementan ejecutando los programas instalados en el servidor 12, que es un ordenador, por la unidad de control del servidor 12. Debe observarse que los programas se suministran al servidor 12 a través de, por ejemplo, un medio de almacenamiento legible por ordenador, como un disco compacto (CD-ROM) y un disco digital versátil (DVD-ROM), o mediante una red de comunicación tal como Internet.

Debe observarse que, el servidor 12 según esta realización también implementa funciones (por ejemplo, funciones relacionadas con la compra en línea) distintas de las ilustradas en la Figura 6.

En esta realización, la unidad de almacenamiento de datos 30 almacena por adelantado los datos de historial de acceso 24 y los datos de historial de compras 26 descritos anteriormente, los datos de cuenta 40 ejemplificados en la Figura 7, datos maestros de artículo 42 ejemplificados en la Figura 8, datos de configuración del nivel de confidencialidad 44 ejemplificados en la Figura 9 y similares.

Los datos de cuenta 40 son datos para gestionar usuarios que usan el sitio de compras e incluyen, por ejemplo, el identificador del usuario (ID de usuario), la contraseña establecida por el usuario y los datos que representan atributos del usuario tales como datos de nombre que representan el nombre del usuario, datos de sexo que indican el sexo, datos de edad que indican la edad y datos de dirección que indican la dirección.

Los datos maestros del artículo 42 son datos para gestionar artículos o servicios vendidos en el sitio de compras implementado por el servidor 12, e incluyen, por ejemplo, el ID de artículo que es el identificador del artículo vendido o servicio, los datos del nombre del artículo indican el nombre del artículo o servicio, los datos del tipo de artículo que indican el tipo del artículo o servicio, los datos de precio que indican el precio del artículo o servicio, y similares.

Los datos de configuración del nivel de confidencialidad 44 son datos para gestionar configuraciones sobre la confidencialidad de elementos en el usuario, tales como un historial de acceso del usuario, un historial de compras del usuario y atributos del usuario, e incluye, por ejemplo, un ID de configuración de nivel de confidencialidad, que es un identificador de los datos de configuración de nivel de confidencialidad 44, datos de

atributo de configuración que indican datos para los que se establece un nivel de confidencialidad y atributos de los datos para los que se establece el nivel de confidencialidad, y datos de nivel de confidencialidad que indican el nivel de confidencialidad que representa un grado de confidencialidad. En esta realización, el nivel de confidencialidad está representado por cualquier número entero de 1 a 5, y a medida que el número aumenta, la confidencialidad aumenta.

El usuario puede establecer arbitrariamente un valor de los datos de nivel de confidencialidad. Alternativamente, el valor de los datos de nivel de confidencialidad se puede establecer en función del nivel de confidencialidad establecido de antemano para cada tipo de artículo, y el tipo de un artículo o servicio introducido en una página recién explorada por el usuario.

Además, se puede establecer de antemano una relación de correspondencia entre una combinación del tipo de artículo, un atributo del usuario y el valor de los datos de nivel de confidencialidad. Luego, el valor de los datos de nivel de confidencialidad se puede establecer en función del tipo de artículo o servicio introducido en la página recién explorada por el usuario y el atributo del usuario. Por ejemplo, se supone que los tipos de artículos de artículos introducidos en una página examinada por el usuario son "cosméticos", "zapatos de hombre" y "agua potable". En este caso, cuando el sexo del usuario que navega por la página es "masculino", los valores de los datos de nivel de confidencialidad se pueden establecer en un orden descendente de "cosméticos", "agua potable" y "zapatos de hombre", y cuando el sexo del usuario que navega por la página es "femenino", los valores de los datos de nivel de confidencialidad se pueden establecer en orden descendente de "zapatos de hombre", "agua potable" y "cosméticos".

Además, por ejemplo, cuando el usuario navega por una nueva página, se puede determinar un artículo o similar que sea igual o relacionado con el artículo o similar introducido en la página. Luego, el valor del conjunto de datos de nivel de confidencialidad para el artículo determinado o similar por el usuario antes de que se explore la nueva página se puede establecer como un valor de los datos de nivel de confidencialidad del artículo o similar introducido en la nueva página explorada por el usuario.

En esta realización, un valor de "4" se establece como el valor de los datos de nivel de confidencialidad para todos los atributos de los datos de historial de acceso 24, y un valor de "5" se establece como el valor de los datos de nivel de confidencialidad para todos los atributos de los datos de historial de compras 26. Además, para los atributos incluidos en los datos de cuenta 40, como los valores de los datos de nivel de confidencialidad, un valor de "1" se establece en el ID de usuario, un valor de "2" se establece en los datos de nombre, los datos de sexo, y los datos de edad, y un valor de "3" se establece en los datos de dirección.

Ahora, se describe un ejemplo de un flujo de procesamiento realizado por el servidor 12 según esta realización con referencia a un diagrama de flujo ilustrado en la Figura 10.

Primero, la unidad receptora 32 recibe de la terminal de usuario 14 un ID de usuario y una contraseña, que el usuario ingresa a la página de inicio de sesión (S101). Entonces, la unidad de autenticación 34 identifica una contraseña asociada con el ID de usuario, que se recibe en el procesamiento indicado por S101, en los datos de cuenta 40 almacenados en la unidad de almacenamiento de datos 30 (S102).

La unidad de autenticación 34 juzga si la autenticación ha tenido éxito o no (S103). En esta realización, la unidad de autenticación 34 juzga que la autenticación ha tenido éxito cuando la contraseña recibida en el procesamiento denotado por S101 es cualquiera de una cadena de caracteres obtenida con el prefijo o sufijo "1" a la contraseña identificada en el procesamiento denotado por S102, una cadena de caracteres obtenida con el prefijo o sufijo "0" a la contraseña identificada en el procesamiento indicado por S102, y una cadena de caracteres de la contraseña identificada en el procesamiento indicado por la propia S102, y juzga que la autenticación ha fallado de otra manera. En lo sucesivo, la cadena de caracteres obtenida con el prefijo o sufijo "1" a la contraseña identificada en el procesamiento indicado por S102 se denomina roja como contraseña privada, y la cadena de caracteres obtenida con el prefijo o sufijo "0" a la contraseña identificada en el procesamiento denotado por S102 o la cadena de caracteres de la contraseña identificada en el procesamiento denotado por el propio S102 se denomina contraseña pública.

Entonces, cuando se juzga en el procesamiento denotado por S103 que la autenticación ha fallado (S103: N), la unidad de autenticación 34 transmite a la terminal de usuario 14 un mensaje de que la autenticación ha fallado (S104), y el procesamiento ilustrado en este ejemplo de procesamiento termina. En este caso, la terminal de usuario 14 emite, por ejemplo, una página de inicio de sesión que incluye el mensaje de que la autenticación no se pudo visualizar en el monitor a través del navegador web.

Por otro lado, cuando se juzga en el procesamiento denotado por S103 que la autenticación ha tenido éxito (S103: Y), la unidad de autenticación 34 juzga si la contraseña recibida en el procesamiento denotado por S101 es la contraseña privada o contraseña pública (S105). Entonces, cuando la contraseña es la contraseña privada, la unidad de generación de página 36 genera la página de portal 20 en el modo privado ilustrado en la Figura 2

(S106) en base a los atributos incluidos en los datos de cuenta 40, los datos de historial de acceso 24 y los datos de historial de compras 26 asociados con el ID de usuario recibido en el procesamiento indicado por S101.

5 Por otro lado, cuando la contraseña es la contraseña pública, la unidad de generación de página 36 identifica información que tiene el valor de los datos de nivel de confidencialidad establecido igual o inferior a un umbral predeterminado (en este ejemplo de procesamiento, "3") entre los atributos incluidos en los datos de cuenta 40, los datos de historial de acceso 24 y los datos de historial de compras 26 asociados con el ID de usuario recibido en el procesamiento indicado por S101, y genera la página de portal 22 en el modo público ilustrado en la Figura 3 en base a la información identificada (S107). Como se describió anteriormente, en este ejemplo de
10 procesamiento, los datos sobre un usuario A sobre la base de los cuales se genera la página de portal 20 en el modo privado no están limitados, pero los datos sobre el usuario A sobre la base de los cuales la página de portal 22 en el modo público es generada se limita a la información que establece un nivel de confidencialidad que representa una confidencialidad inferior a la confidencialidad determinada en función del tipo de contraseña introducida por el usuario.

15 Luego, la unidad de salida de página 38 transmite a la terminal de usuario 14 la página de portal generada en el procesamiento indicado por S106 o S107 (S108), y finaliza el procesamiento ilustrado en este ejemplo de procesamiento. Cuando la terminal de usuario 14 recibe la página de portal transmitida en el procesamiento
20 indicado por S108, la terminal de usuario 14 emite la página de portal recibida para su visualización en el monitor.

Por ejemplo, cuando un usuario (en adelante denominado usuario A) que tiene un ID de usuario de "a001" ingresa una contraseña "a1b2c31" en la página de inicio de sesión, la contraseña es una cadena de caracteres obtenida al poner como sufijo "1" en la contraseña "alb2c3" establecida en los datos de cuenta 40, y por lo tanto
25 la unidad de autenticación 34 juzga que la contraseña de entrada es la contraseña privada. Como resultado, en respuesta a la entrada de la contraseña, la unidad de generación de página 36 genera la página de portal 20 en el modo privado ejemplificado en la Figura 2) Como se describió anteriormente, los datos sobre el usuario A sobre la base de los cuales se genera la página de portal 20 en el modo privado no están limitados.

30 En esta realización, en la página de portal 20 en el modo privado, los enlaces a páginas que presentan artículos o servicios identificados por ID de artículo asociados con el ID de usuario del usuario A en los datos de historial de acceso 24 están dispuestos en una región que muestra "Artículos vistos recientemente". También en la página de portal 20 en el modo privado, los enlaces a páginas que presentan los artículos o servicios identificados por los ID de artículo asociados con el ID de usuario del usuario A en los datos de historial de
35 compras 26 se disponen en una región que muestra "Artículos comprados recientemente". También en la página de portal 20 en el modo privado, los enlaces a páginas que presentan artículos o servicios recomendados para el usuario A se disponen en una región que muestra "Artículos recomendados". Los artículos o servicios recomendados para el usuario A se determinan aquí en base a los ID de artículo asociados con el ID de usuario del usuario A en los datos de historial de acceso 24 y los datos de historial de compras 26 en esta realización. En la región que muestra "Artículos recomendados", por ejemplo, se organizan enlaces a páginas que presentan artículos o servicios que son del mismo tipo de artículo pero que el usuario A no ha comprado. En esta
40 realización, como se ilustra en la Figura 2, en la página de portal 20 en el modo privado, se disponen enlaces a páginas que presentan artículos del tipo de artículo: "Productos de golf".

45 Por otro lado, cuando el usuario A ingresa una contraseña "a1b2c30" en la página de inicio de sesión, la contraseña es una cadena de caracteres obtener al poner como sufijo "0" en la contraseña "alb2c3" establecida en los datos de cuenta 40, y por lo tanto la unidad de autenticación 34 juzga que la contraseña de entrada es la contraseña pública. Como resultado, en respuesta a la entrada de la contraseña, la unidad de generación de página 36 genera la página de portal 22 en el modo público ejemplificado en la Figura 3. Como se describió
50 anteriormente, los datos sobre el usuario A sobre la base de los cuales se genera la página de portal 22 en el modo público se limitan a la información que tiene el valor de los datos de nivel de confidencialidad igual o inferior a "3". Entonces, en esta realización, en la página de portal 22 en el modo público, la región que muestra "Artículos vistos recientemente" y la región que muestra "Artículos comprados recientemente" no están presentes. También en la página de portal 22 en el modo público, en la región que muestra "Artículos recomendados", por ejemplo, enlaces a páginas que presentan artículos o servicios determinados independientemente de un historial de compras y un historial de acceso del usuario A (por ejemplo, grupo de artículos de venta o grupo de servicios más vendido dentro de la última semana) están dispuestos. Debe observarse que, por ejemplo, en la página de portal 22 en el modo público, la información dispuesta en la región que muestra "Artículos vistos recientemente" y la región que muestra "Artículos comprados recientemente" se puede establecer como datos ocultos. En otras palabras, la información dispuesta en la región que muestra "Artículos vistos recientemente" y la región que muestra "Artículos comprados recientemente" se puede transmitir desde el servidor 12 a la terminal de usuario 14 pero no mostrarse en la terminal de usuario 14. Específicamente, por ejemplo, la información dispuesta en la región que muestra "Artículos vistos recientemente" y la región que muestra "Artículos comprados recientemente" en la página de portal 22 en el modo público puede estar
60 encerrada por las etiquetas <div style="visibility:hidden"> y </div>.
65

Como se describió anteriormente, en esta realización, dependiendo de la contraseña introducida por el usuario A, la información sobre el usuario A dispuesta en la página de portal (por ejemplo, información personal) e información sobre el usuario A que forma la base de la información dispuesta en la página de portal (por ejemplo, información personal) se determinan. Además, en el caso de que se ingrese la contraseña pública, el rango de la información que se muestra como la página de portal y el rango de la información que forma la base de la información incluida en la página de portal son más limitadas que en el caso en el que se ingresa la contraseña privada.

Como se describió anteriormente, en esta realización, en base al contenido de una operación realizada en el campo de entrada de contraseña por el usuario con el dispositivo de entrada en un estado en el que se activa el campo de entrada de contraseña (por ejemplo, estado en el que la solicitud se visualiza), se identifica información de control (en el ejemplo mencionado anteriormente, nivel de confidencialidad) que es diferente de la contraseña. Luego, en base a la información de control, se identifica un rango de información pública del usuario que se puede visualizar. Luego, el rango de la información sobre la base de la cual se genera la página de portal se limita al rango visualizable públicamente identificado. Por lo tanto, es posible reducir el temor de que otra persona advierta la limitación del rango de la información que forma la base de la pantalla proporcionada al usuario. En particular, un formulario para ingresar la contraseña en la página de inicio de sesión muestra la cadena de caracteres ingresada como caracteres ocultos y, por lo tanto, incluso en una situación en la que otra persona se asoma mientras el usuario ingresa la contraseña en la página de inicio de sesión, se espera que haya un riesgo bajo porque la persona encuentra que el usuario controla el rango de la información sobre la base de la cual se genera la página de portal. Además, en esta realización, la entrada de contraseña cuando se muestra la página de portal 20 en el modo privado y la entrada de contraseña cuando se muestra la página de portal 22 en el modo público tienen el mismo número de caracteres, y por lo tanto se espera que haya un riesgo aún menor en que otra persona encuentra al usuario controlando el rango de la información sobre la base de la cual se genera la página de portal. Debe observarse que la información de control descrita anteriormente no necesita ser el nivel de confidencialidad.

Debe observarse que la presente invención no se limita a la realización descrita anteriormente.

Por ejemplo, la unidad de generación de página 36 puede generar la página de portal 20 en el modo privado cuando la contraseña incluida en los datos de cuenta 40 y la entrada de contraseña por el usuario coinciden completamente como cadenas de caracteres insensibles a mayúsculas y minúsculas y cuando los caracteres en las cadenas de caracteres también coinciden completamente siendo sensibles a mayúsculas y minúsculas, y pueden generar la página de portal 22 en el modo público cuando la contraseña incluida en los datos de cuenta 40 y la contraseña ingresada por el usuario coinciden completamente como las cadenas de caracteres insensibles a mayúsculas y minúsculas y no coinciden completamente siendo sensibles a mayúsculas y minúsculas. Específicamente, por ejemplo, cuando se ingresa "a1b2c3" como contraseña, la unidad de generación de página 36 genera la página de portal 20 en el modo privado, y cuando las entradas de tecla de la tecla shift más "a", la tecla shift más "b", y la tecla shift más "c" se realizan en lugar de las entradas de tecla de "a", "b" y "c" para ingresar "A1B2C3" como contraseña, la unidad de generación de página 36 puede generar la página de portal 22 en el modo público. De esta manera, se puede establecer una relación entre la entrada de contraseña para generar la página de portal 20 en el modo privado y la entrada de contraseña para generar la página de portal 22 en el modo público en donde al menos parte de las teclas se utilizadas para ingresar caracteres en las mismas posiciones superiores coinciden entre sí.

Además, por ejemplo, en los datos de cuenta 40, se pueden establecer dos contraseñas (por ejemplo, primera contraseña y segunda contraseña) para un usuario. Luego, cuando el usuario ingresa la primera contraseña, la unidad de generación de página 36 puede generar la página de portal 20 en el modo privado, y cuando el usuario ingresa la segunda contraseña, la unidad de generación de página 36 puede generar la página de portal 22 en el modo público.

Además, como se ejemplifica en la Figura 11, cuando la unidad de generación de página 36 genera la página de portal 22 en el modo público, se puede organizar información alternativa en la región que muestra "Artículos vistos recientemente" y la región que muestra "Artículos comprados recientemente". La unidad de generación de página 36 puede disponer en las regiones, por ejemplo, información sobre artículos o servicios ficticios predeterminados o similares en lugar de la información limitada para ser excluida de la página de portal.

Además, por ejemplo, el nivel de confidencialidad se puede establecer en asociación con una combinación de un atributo de un artículo (por ejemplo, tipo de artículo o similar) y un atributo del usuario (por ejemplo, sexo o similar). Específicamente, por ejemplo, para una combinación de un tipo de artículo: "bolso de mujer" y el sexo: "masculino", "5" puede establecerse como el valor del nivel de confidencialidad. Luego, en este caso, cuando el valor de los datos de sexo incluidos en los datos de cuenta 40 del usuario que ha iniciado sesión es "masculino" y los datos de historial de compras 26 del usuario incluyen un ID de artículo correspondiente a un bolso de mujer, un enlace que presenta el artículo no puede disponerse en la página de portal 22 en el modo público.

Además, por ejemplo, la unidad de generación de página 36 puede determinar, en base a un intervalo de entrada de caracteres incluidos en la contraseña o un período de tiempo calculado en función de un tiempo en que se habilita una entrada de la contraseña y un tiempo en que un caracter se incluye en la contraseña se ingresa, ya sea para generar la página de portal 20 en el modo privado o la página de portal 22 en el modo público.

5 Específicamente, por ejemplo, cuando un período de tiempo desde el tiempo en el que se ingresa el primer caracter de la contraseña hasta el tiempo en que se hace clic en el botón de inicio de sesión es más largo que un período de tiempo predeterminado, la unidad de generación de página 36 puede generar la página de portal 20 en el modo privado, de lo contrario la unidad de generación de página 36 puede generar la página de portal 22 en el modo público. Además, por ejemplo, cuando un período de tiempo desde el tiempo en el que se ingresa el primer caracter de la contraseña hasta el tiempo en el que se ingresa el último caracter de la contraseña es más largo que un período de tiempo predeterminado, la unidad de generación de página 36 puede generar la página de portal 20 en el modo privado, de lo contrario la unidad de generación de página 36 puede generar la página de portal 22 en el modo público. Además, por ejemplo, cuando un valor promedio de intervalos de tiempo para ingresar caracteres incluidos en la contraseña es mayor que un período de tiempo predeterminado, la unidad de generación de página 36 puede generar la página de portal 20 en el modo privado, de lo contrario la unidad de generación de página 36 puede generar la página de portal 22 en el modo público. Además, por ejemplo, cuando un período de tiempo desde el tiempo en que se muestra la página de inicio de sesión hasta el tiempo en el que se ingresa el primer caracter de la contraseña es más largo que un período de tiempo predeterminado, la unidad de generación de página 36 puede generar la página de portal 20 en el modo privado, de lo contrario la unidad de generación de página 36 puede generar la página de portal 22 en el modo público. Además, por ejemplo, dependiendo de si un tiempo transcurrido desde el tiempo en que se recibe la página de inicio de sesión desde el servidor 12 (o el tiempo en que se muestra la página de inicio de sesión en la terminal de usuario 14) hasta el tiempo en el que se ingresa la contraseña completa es más largo que un período de tiempo predeterminado, la unidad de generación de página 36 puede determinar si generar la página de portal 20 en el modo privado o la página de portal 22 en el modo público. Además, por ejemplo, un valor estándar de un intervalo de tiempo de entrada puede almacenarse por adelantado para cada usuario en la unidad de almacenamiento de datos 30, y dependiendo de si el valor promedio de los intervalos de tiempo para ingresar los caracteres incluidos en la contraseña es más largo que el valor estándar mencionado anteriormente, la unidad de generación de página 36 puede determinar si generar la página de portal 20 en el modo privado o la página de portal 22 en el modo público.

Debe observarse que, el servidor 12 puede identificar un tiempo en el que se ingresa la contraseña o similar cuando, por ejemplo, la terminal de usuario 14 transmite al servidor 12 información que indica un tiempo de entrada y el servidor 12 recibe la información. Se entiende que el tiempo en el que se ingresa la contraseña o similar puede ser identificado por el servidor 12 también cuando la terminal de usuario 14 transmite una notificación al servidor 12 cada vez que se ingresa la contraseña y el servidor 12 trata un tiempo de recepción de la notificación como el tiempo de entrada de la contraseña. Además, el servidor 12 puede identificar un tiempo en que se muestra la página de inicio de sesión cuando, por ejemplo, el servidor 12 trata un tiempo para transmitir la página de inicio de sesión a la terminal de usuario 14 como el tiempo en que se muestra la página de inicio de sesión. Además, por ejemplo, al igual que con una función de barra de herramientas del navegador web, un programa instalado en la terminal de usuario 14 puede controlar el tiempo en el que se ingresa la contraseña o el tiempo en que se hace clic en el botón de inicio de sesión, y el programa puede transmitir información indicando esos tiempos al servidor 12.

Además, por ejemplo, cuando la unidad receptora 32 recibe como contraseña una cadena de caracteres obtenida agregando un caracter arbitrario o una cadena de caracteres a la contraseña establecida por el usuario, la unidad de autenticación 34 puede juzgar que el usuario ha sido autenticado de manera satisfactoria. Luego, en este caso, dependiendo de la longitud del caracter agregado o la cadena de caracteres, el orden de la secuencia, la posición de la adición (ya sea que el caracter o la cadena de caracteres se agregue al principio o al final de la contraseña establecida por el usuario), o similares, la unidad de generación de página 36 puede determinar si generar la página de portal 20 en el modo privado o la página de portal 22 en el modo público.

Además, por ejemplo, dependiendo de un modo de entrada de la contraseña recibida, la unidad de generación de página 36 puede generar cualquiera de una pluralidad de páginas de portal 22 en el modo público que tiene diferentes criterios para reducir el rango de la información sobre la base de la cual se genera la página de portal (criterios sobre qué rango de información se utiliza como base para generar la página de portal). Por ejemplo, cuando se recibe la primera contraseña, el historial de acceso puede disponerse, pero el historial de compras no puede disponerse en la página de portal, y cuando se recibe la segunda contraseña, el historial de compras puede disponerse, pero el historial de acceso puede no estar dispuesto en la página de portal.

Además, por ejemplo, dependiendo del número de repeticiones de una cadena de caracteres establecida de antemano por el usuario en la entrada de la cadena de caracteres como contraseña, la unidad de generación de página 36 puede determinar si generar la página de portal 20 en el modo privado o la página de portal 22 en el modo público. Específicamente, por ejemplo, cuando la unidad receptora 32 recibe como contraseña la misma cadena de caracteres que la cadena de caracteres establecida de antemano por el usuario, la unidad de

- generación de página 36 puede generar la página de portal 20 en modo privado, y cuando la unidad receptora 32 recibe como contraseña una cadena de caracteres obtenida mediante la concatenación de una pluralidad de cadenas de caracteres establecidas previamente por el usuario, la unidad de generación de página 36 puede generar la página de portal 22 en el modo público. Además, la información sobre la cual se genera la página de portal no se limita a la información mencionada anteriormente, y puede ser, por ejemplo, un número de teléfono del usuario, un marcador establecido por el usuario, un correo electrónico, una libreta de direcciones, datos de horarios, imágenes o un programa. Además, la información sobre la cual se genera la página de portal puede ser información almacenada en el servidor 12 o información almacenada en la terminal de usuario 14.
- 5
- 10 Además, la división de roles entre el servidor 12 y la terminal de usuario 14 no se limita a la realización mencionada anteriormente. Por ejemplo, la terminal de usuario 14 puede identificar la información de control tal como el nivel de confidencialidad en base al contenido de la operación realizada en el campo de entrada de contraseña con el dispositivo de entrada, y transmitir la información de control al servidor 12. Entonces, el servidor 12 puede identificar el rango visualizable públicamente de la información sobre el usuario en base a la información de control recibida desde la terminal de usuario 14. Además, esta realización puede aplicarse a un servidor 12 que proporciona un servicio diferente del sitio de compras. Además, los valores numéricos específicos y las cadenas de caracteres mencionados anteriormente, y los valores numéricos específicos y las cadenas de caracteres en los dibujos son ejemplares, y la presente invención no se limita a esos valores numéricos y cadenas de caracteres.
- 15
- 20

REIVINDICACIONES

1. Un sistema de procesamiento de información, que comprende:
 - 5 medios de autenticación para:
 - recibir un ID de usuario y una entrada de contraseña en una página de inicio de sesión, siendo introducida la contraseña como parte de una operación realizada en un campo de entrada de contraseña de la página de inicio de sesión;
 - 10 identificar una contraseña establecida de antemano por el usuario y asociada con el ID de usuario, en los datos de cuenta almacenados en una unidad de almacenamiento de datos; y autenticar de manera satisfactoria al usuario cuando la contraseña ingresada en la página de inicio de sesión es la misma que la contraseña identificada;
 - 15 medios de identificación de información de control para identificar información de control, que es información diferente de la contraseña establecida de antemano por el usuario, y se basa en el contenido de la operación realizada en el campo de entrada de contraseña con el dispositivo de entrada, y determinar si se debe mostrar información de acuerdo con un modo privado o de acuerdo con un modo público en base a la información de control;
 - 20 medios de identificación de rango visualizable públicamente para identificar, para mostrar en el modo público, un rango de información visualizable públicamente relacionada con el usuario en base a la información de control; y
 - 25 medios de limitación para limitar, en el modo público, un rango de información relacionada con el usuario que forma la base de una pantalla provista al usuario de modo que el rango de la información se encuentre dentro del rango visualizable públicamente identificado por los medios de identificación de rango visualizable públicamente, cuando el usuario es autenticado de manera satisfactoria por los medios de autenticación, tal que:
 - 30 en el modo privado, los enlaces a páginas que presentan artículos o servicios identificados por los ID de artículos asociados con el ID de usuario en datos de historial de acceso y datos de historial de compras se disponen en una región de la pantalla; y
 - 35 en el modo público, los artículos o servicios identificados por los ID de artículos asociados con el ID de usuario en datos de historial de acceso y datos de historial de compras no se muestran en la pantalla.
 2. El sistema de procesamiento de información de acuerdo con la reivindicación 1, en el que los medios de identificación de rango visualizable públicamente identifican al menos un elemento de información entre uno o más elementos de información relacionados con el usuario, y en el que los medios de limitación limitan, al menos a un elemento de información identificado, el rango de la información relacionada con el usuario que forma la base de la pantalla proporcionada al usuario.
 3. El sistema de procesamiento de información de acuerdo con la reivindicación 2, en el que, para cada uno de los uno o más elementos de información, se establece un nivel de confidencialidad representando un grado de confidencialidad de la información, en el que los medios de identificación de información de control identifican el nivel de confidencialidad, y en el que los medios de identificación de rango visualizable públicamente identifican un elemento de información que tiene establecido un nivel de confidencialidad que representa una confidencialidad que es inferior a la confidencialidad representada por el nivel de confidencialidad identificado.
 4. El sistema de procesamiento de información de acuerdo con la reivindicación 3, en el que un valor del nivel de confidencialidad para el uno o más elementos de información se establece en base a un tipo de artículo o servicio introducido en una página recién visitada por el usuario y un atributo del usuario.
 5. El sistema de procesamiento de información de acuerdo con una cualquiera de las reivindicaciones 1 a 3, en el que los medios de limitación limitan un rango de información mostrada en la pantalla proporcionada al usuario.
 6. El sistema de procesamiento de información de acuerdo con la reivindicación 4, que además comprende: medios de control para controlar información incluida en la pantalla proporcionada al usuario de modo que se disponga información alternativa en lugar de información limitada para ser excluida de la pantalla.
 7. El sistema de procesamiento de información de acuerdo con una cualquiera de las reivindicaciones 1 a 6, en el que cuando se cumple una condición de que una entrada de cadena de caracteres al dispositivo de

entrada incluye la contraseña establecida de antemano por el usuario, los medios de limitación limitan el rango de la información que forma la base de la pantalla.

5 8. El sistema de procesamiento de información de acuerdo con una cualquiera de las reivindicaciones 1 a 7, en el que cuando se introduce una cualquiera de una pluralidad de cadenas de caracteres que tiene el mismo número de caracteres en el dispositivo de entrada, los medios de limitación limitan el rango de la información que forma la base de la pantalla proporcionada al usuario de modo que el rango de la información se encuentre dentro de un rango de información asociado con la información de control, siendo la información de control parte de la cadena de caracteres de entrada.

10 9. El sistema de procesamiento de información de acuerdo con una cualquiera de las reivindicaciones 1 a 8, en el que cuando cualquiera de una pluralidad de cadenas de caracteres tiene el mismo número de caracteres, y para el cual al menos parte de las teclas utilizadas para ingresar caracteres en la misma posición desde el principio de la cadena de caracteres coinciden entre sí, se ingresa al dispositivo de entrada, el medio de limitación limita el rango de la información que forma la base de la pantalla proporcionada al usuario de modo que el rango de la información se encuentre dentro del rango de información asociado con la información de control, siendo la información de control una de dichas teclas de entrada al dispositivo de entrada.

15 20 10. El sistema de procesamiento de información de acuerdo con una cualquiera de las reivindicaciones 1 a 9, en el que los medios de identificación de información de control identifican la información de control en base a un intervalo de entrada de caracteres incluidos en la contraseña o un período de tiempo calculado en base a un tiempo en el que el ingreso de la contraseña está habilitado y a un tiempo en el que se ingresa un carácter incluido en la contraseña.

25 11. Un procedimiento de procesamiento de información, que comprende:

una etapa de autenticación, que comprende:

30 recibir un ID de usuario y una entrada de contraseña en una página de inicio de sesión, siendo introducida la contraseña como parte de una operación realizada en un campo de entrada de contraseña de la página de inicio de sesión;
 identificar una contraseña establecida de antemano por el usuario y asociada con el ID de usuario, en los datos de cuenta almacenados en una unidad de almacenamiento de datos; y
 35 autenticar de manera satisfactoria al usuario cuando la contraseña ingresada en la página de inicio de sesión es la misma que la contraseña identificada;

40 una etapa de identificación de información de control para identificar información de control, que es información diferente de la contraseña establecida de antemano por el usuario, y se basa en el contenido de la operación realizada en el campo de entrada de contraseña con el dispositivo de entrada, y determinar si se debe mostrar información de acuerdo con un modo privado o de acuerdo con un modo público en base a la información de control;

45 una etapa de identificación de rango visualizable públicamente para identificar, para mostrar en el modo público, un rango de información visualizable públicamente relacionada con el usuario en base a la información de control; y

una etapa de limitación que limita, en el modo público, un rango de información relacionada con el usuario que forma la base de una pantalla provista al usuario de modo que el rango de la información se encuentre dentro del rango visualizable públicamente identificado en la etapa de identificación de rango visualizable públicamente, cuando el usuario es autenticado de manera satisfactoria en la etapa de autenticación,
 50 tal que:

55 en el modo privado, los enlaces a páginas que presentan artículos o servicios identificados por los ID de artículos asociados con el ID de usuario en datos de historial de acceso y datos de historial de compras se disponen en una región de la pantalla; y

en el modo público, los artículos o servicios identificados por los ID de artículos asociados con el ID de usuario en datos de historial de acceso y datos de historial de compras no se muestran en la pantalla.

12. Un dispositivo de procesamiento de información, que comprende:

60 medios de autenticación para:

recibir un ID de usuario y una entrada de contraseña en una página de inicio de sesión, siendo introducida la contraseña como parte de una operación realizada en un campo de entrada de contraseña de la página de inicio de sesión;
 65 identificar una contraseña establecida de antemano por el usuario y asociada con el ID de usuario, en

los datos de cuenta almacenados en una unidad de almacenamiento de datos; y
autenticar de manera satisfactoria al usuario cuando la contraseña ingresada en la página de inicio de sesión es la misma que la contraseña identificada;

5 medios de identificación de rango visualizable públicamente para identificar, para mostrar en un modo público, un rango de información visualizable públicamente relacionada con el usuario en base a la información de control, que es información diferente de la contraseña establecida de antemano por el usuario, y se identifica en base al contenido de la operación realizada en el campo de entrada de contraseña con el dispositivo de entrada; y

10 medios de limitación para limitar, en el modo público, un rango de información relacionada con el usuario que forma la base de una pantalla provista al usuario de modo que el rango de la información se encuentre dentro del rango visualizable públicamente identificado por los medios de identificación de rango visualizable públicamente, cuando el usuario es autenticado de manera satisfactoria por los medios de autenticación,
15 tal que:

en un modo privado, los enlaces a páginas que presentan artículos o servicios identificados por los ID de artículos asociados con el ID de usuario en datos de historial de acceso y datos de historial de compras se disponen en una región de la pantalla; y

20 en el modo público, los artículos o servicios identificados por los ID de artículos asociados con el ID de usuario en datos de historial de acceso y datos de historial de compras no se muestran en la pantalla.

13. Un programa para hacer que un ordenador funcione como:

25 medios de autenticación para:

recibir un ID de usuario y una entrada de contraseña en una página de inicio de sesión, siendo introducida la contraseña como parte de una operación realizada en un campo de entrada de contraseña de la página de inicio de sesión;

30 identificar una contraseña establecida de antemano por el usuario y asociada con el ID de usuario, en datos de cuenta almacenados en una unidad de almacenamiento de datos; y
autenticar de manera satisfactoria al usuario cuando la contraseña ingresada en la página de inicio de sesión es la misma que la contraseña identificada;

35 medios de identificación de rango visualizable públicamente para identificar, para mostrar en un modo público, un rango de información visualizable públicamente relacionada con el usuario en base a la información de control, que es información diferente de la contraseña establecida de antemano por el usuario, y se identifica en base al contenido de la operación realizada en el campo de entrada de contraseña con el dispositivo de entrada; y

40 medios de limitación para limitar, en el modo público, un rango de información relacionada con el usuario que forma la base de una pantalla provista al usuario de modo que el rango de la información se encuentre dentro del rango visualizable públicamente identificado por los medios de identificación de rango visualizable públicamente, cuando el usuario es autenticado de manera satisfactoria por los medios de autenticación,
45 tal que:

en un modo privado, los enlaces a páginas que presentan artículos o servicios identificados por los ID de artículos asociados con el ID de usuario en datos de historial de acceso y datos de historial de compras se disponen en una región de la pantalla; y

50 en el modo público, los artículos o servicios identificados por los ID de artículos asociados con el ID de usuario en datos de historial de acceso y datos de historial de compras no se muestran en la pantalla.

14. Un medio de almacenamiento que tiene un programa almacenado en el mismo, el programa hace que un ordenador funcione como:

55 medios de autenticación para:

recibir un ID de usuario y una entrada de contraseña en una página de inicio de sesión, siendo introducida la contraseña como parte de una operación realizada en un campo de entrada de contraseña de la página de inicio de sesión;

60 identificar una contraseña establecida de antemano por el usuario y asociada con el ID de usuario, en los datos de cuenta almacenados en una unidad de almacenamiento de datos; y
autenticar de manera satisfactoria al usuario cuando la contraseña ingresada en la página de inicio de sesión es la misma que la contraseña identificada;

65

5 medios de identificación de rango visualizable públicamente para identificar, para mostrar en un modo público, un rango de información visualizable públicamente relacionada con el usuario en base a la información de control, que es información diferente de una contraseña y se identifica en base al contenido de la operación realizada en el campo de entrada de contraseña con el dispositivo de entrada; y
10 medios de limitación para limitar, en el modo público, un rango de información relacionada con el usuario que forma la base de una pantalla provista al usuario de modo que el rango de la información se encuentre dentro del rango visualizable públicamente identificado por los medios de identificación de rango visualizable públicamente, cuando el usuario es autenticado de manera satisfactoria por los medios de autenticación,
15 tal que:

en un modo privado, los enlaces a páginas que presentan artículos o servicios identificados por los ID de artículos asociados con el ID de usuario en datos de historial de acceso y datos de historial de compras se disponen en una región de la pantalla; y
20 en el modo público, los artículos o servicios identificados por los ID de artículos asociados con el ID de usuario en datos de historial de acceso y datos de historial de compras no se muestran en la pantalla.

20

FIG. 1

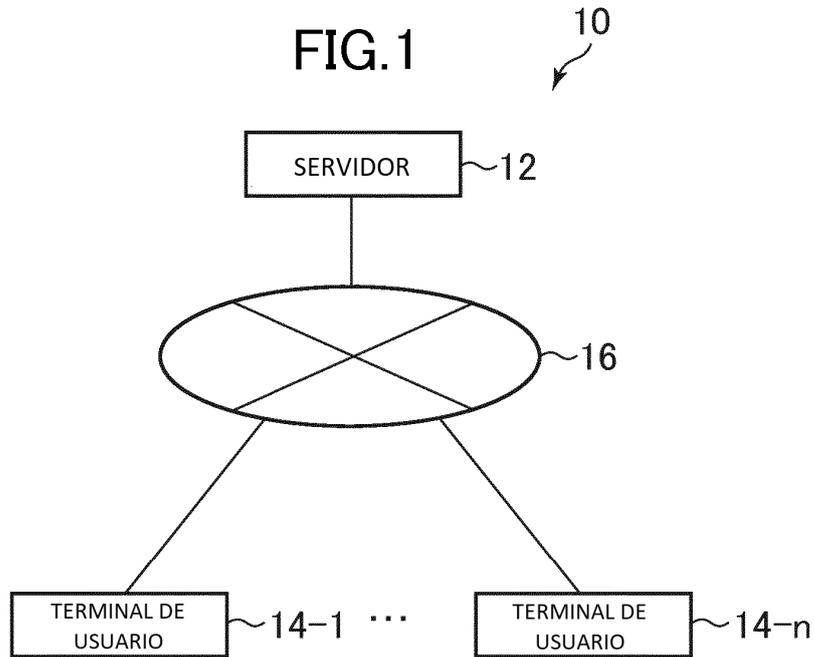


FIG. 2

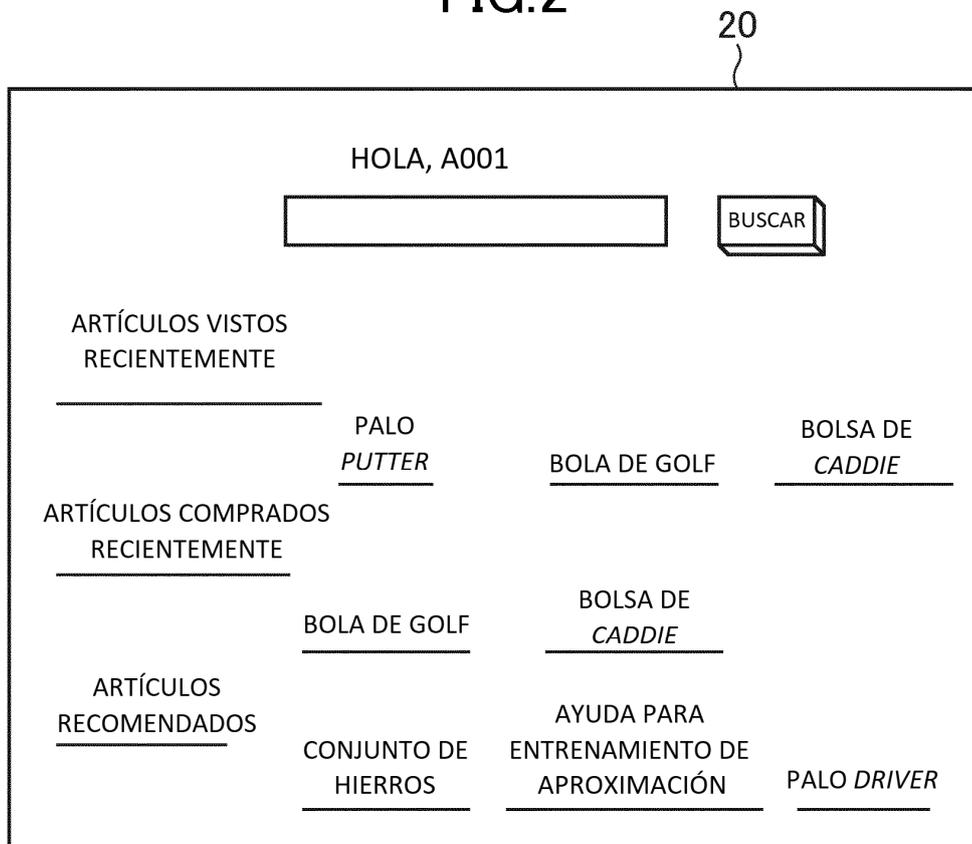


FIG.3

22

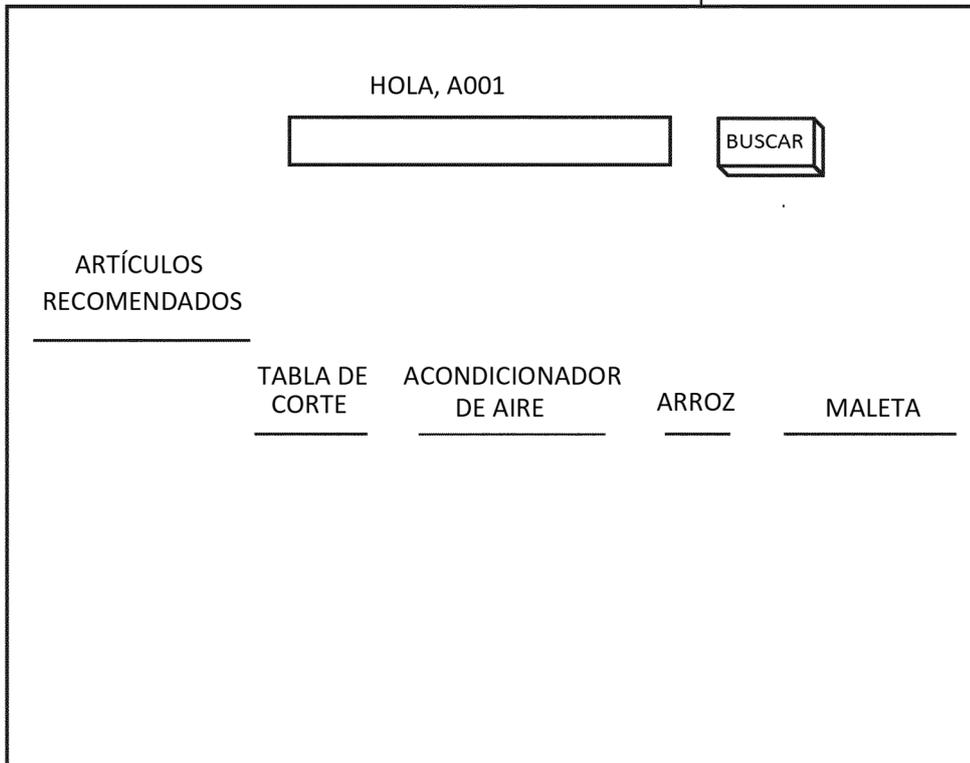


FIG.4

24

ID DE USUARIO	ID DE ARTÍCULO	FECHA DE ACCESO/ INFORMACIÓN DE HORA	
a001	0001	05/01/2011 10:05:25	
a001	0002	05/01/2011 10:10:50	
a001	0003	05/01/2011 10:20:20	

FIG.5

26
↙

ID DE USUARIO	ID DE ARTÍCULO	FECHA DE ACCESO/ INFORMACIÓN DE HORA
a001	0001	05/01/2011 11:05:30
a001	0002	05/01/2011 11:05:30

FIG.6

12
⋮

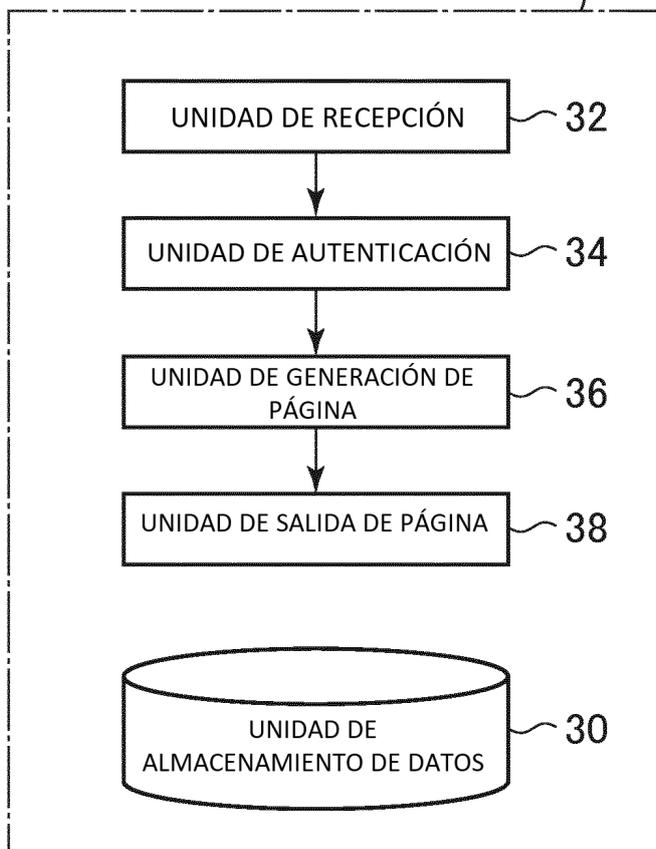


FIG.7

40

ID DE USUARIO	CONTRASEÑA	DATOS DE NOMBRE	DATOS DE SEXO	DATOS DE EDAD	DATOS DE DIRECCIÓN
a001	a1b2c3	MASCULINO	50
b012	x4y5z6	FEMENINO	35

FIG.8

42

ID DE ARTÍCULO	DATOS DE NOMBRE DE ARTÍCULO	DATOS DE TIPO DE ARTÍCULO	DATOS DE PRECIO
0001	BOLSA DE CADDIE	PRODUCTOS DE GOLF	12.000 YEN
0002	BOLSA DE GOLF	PRODUCTOS DE GOLF	700 YEN
0003	PALO PUTTER	PRODUCTOS DE GOLF	10.000 YEN

FIG.9

44
↙

ID DE CONFIGURACIÓN DE NIVEL DE CONFIDENCIALIDAD	DATOS DE ATRIBUTO DE CONFIGURACIÓN	DATOS DE NIVEL DE CONFIDENCIALIDAD
001	DATOS DE CUENTA/ID DE USUARIO	1
002	DATOS DE CUENTA/NOMBRE	2
003	DATOS DE CUENTA/SEXO	2
004	DATOS DE CUENTA/EDAD	2
005	DATOS DE CUENTA/DIRECCIÓN	3
006	DATOS DE HISTORIAL DE ACCESO/TODO	4
007	DATOS DE HISTORIAL DE COMPRAS/TODO	5

FIG.10

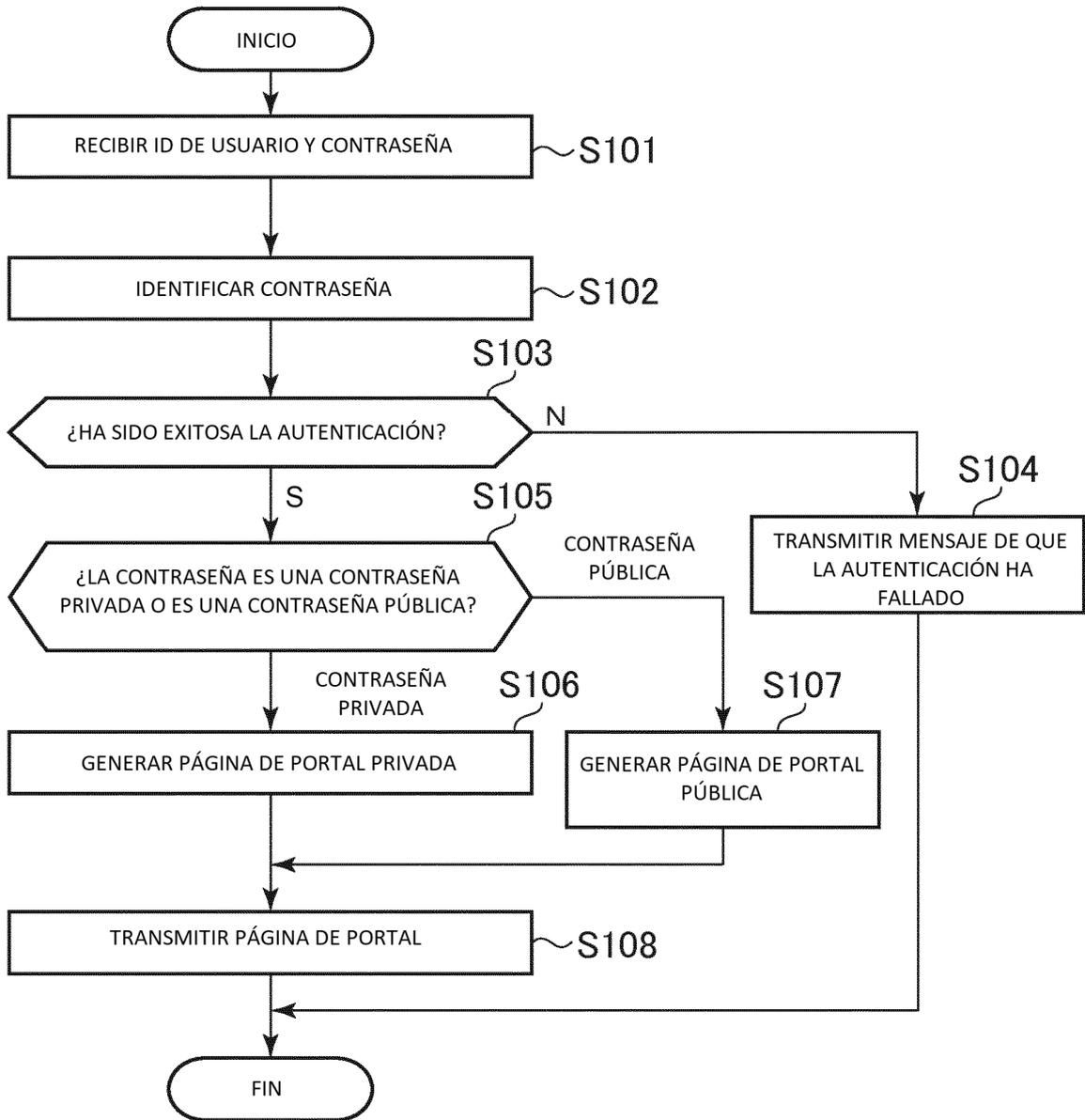


FIG. 11

22

