

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第6281560号  
(P6281560)

(45) 発行日 平成30年2月21日 (2018. 2. 21)

(24) 登録日 平成30年2月2日 (2018. 2. 2)

(51) Int. Cl.	F I
<b>G 0 6 F 21/60 (2013.01)</b>	G O 6 F 21/60 3 2 0
<b>G 0 6 F 21/62 (2013.01)</b>	G O 6 F 21/62 3 4 5
<b>G 0 9 C 1/00 (2006.01)</b>	G O 9 C 1/00 6 6 0 D

請求項の数 9 (全 24 頁)

(21) 出願番号	特願2015-241559 (P2015-241559)	(73) 特許権者	390002761 キヤノンマーケティングジャパン株式会社 東京都港区港南2丁目16番6号
(22) 出願日	平成27年12月10日 (2015. 12. 10)		
(65) 公開番号	特開2016-122441 (P2016-122441A)	(73) 特許権者	592135203 キヤノンITソリューションズ株式会社 東京都品川区東品川2丁目4番11号
(43) 公開日	平成28年7月7日 (2016. 7. 7)		
審査請求日	平成28年6月2日 (2016. 6. 2)	(74) 代理人	100189751 弁理士 木村 友輔
(31) 優先権主張番号	特願2014-262697 (P2014-262697)	(74) 代理人	100208904 弁理士 伊藤 秀起
(32) 優先日	平成26年12月25日 (2014. 12. 25)	(72) 発明者	中村 俊文 東京都品川区東品川2丁目4番11号 キ ヤノンITソリューションズ株式会社内
(33) 優先権主張国	日本国 (JP)		
		審査官	平井 誠
			最終頁に続く

(54) 【発明の名称】 情報処理装置、処理方法、およびプログラム

(57) 【特許請求の範囲】

【請求項 1】

ユーザによる情報の入力を受け付ける情報処理装置であって、  
 前記情報の入力を受け付ける画面を出力する画面出力手段と、  
 前記画面出力手段により出力された画面に入力された情報を暗号化する暗号化手段と、  
 前記ユーザの操作又は所定時間の経過に従って、前記入力された情報を前記暗号化手段  
 により暗号化した形態で出力するか暗号化しない形態で出力するかを制御する出力制御手  
 段と

を備えることを特徴とする情報処理装置。

【請求項 2】

前記画面出力手段により出力された画面に入力された情報の暗号化に用いる暗号キーの  
 入力を受け付ける暗号キー受付手段  
 を更に備え、

前記暗号化手段は、前記暗号キー受付手段により受け付けた暗号キーを用いて、前記入  
 力された情報を暗号化し、

前記暗号化手段により暗号化された情報を、暗号化された状態で記憶すべく、サーバに  
 送信する暗号化情報送信手段

を更に備えることを特徴とする請求項 1 に記載の情報処理装置。

【請求項 3】

前記暗号化情報送信手段により送信され、既に記憶されている前記暗号化された情報を

10

20

、サーバに対して要求する暗号化情報要求手段と、

前記暗号化情報要求手段による要求に応じてサーバから受信した前記暗号化された情報の復号化に用いる復号キーの入力を受け付ける復号キー受付手段と、

前記復号キー受付手段により受け付けた復号キーを用いて、前記暗号化された情報を復号化する復号化手段と、

前記復号化手段により復号化された情報を表示する表示手段と  
を更に備えることを特徴とする請求項 2 に記載の情報処理装置。

【請求項 4】

前記出力制御手段により、前記暗号化した形態で出力している場合は、前記暗号化情報送信手段による暗号化された情報のサーバへの送信を可能に制御し、一方、前記出力制御手段により、前記暗号化しない形態で出力している場合は、前記暗号化情報送信手段による暗号化された情報のサーバへの送信を不可能に制御する送信制御手段  
を更に備えることを特徴とする請求項 2 に記載の情報処理装置。

10

【請求項 5】

前記画面に入力された情報のうち、暗号化する情報を前記ユーザの操作に従って決定する決定手段を更に備え、

前記暗号化手段は、前記決定手段により暗号化すると決定した情報を暗号化すること  
を特徴とする請求項 1 乃至 4 のいずれか 1 項に記載の情報処理装置。

【請求項 6】

前記画面に入力された情報のうち、暗号化する情報の項目の定義をサーバから取得する定義取得手段を更に備え、

前記暗号化手段は、前記定義取得手段により取得された暗号化する情報の項目の定義に従って、前記入力された情報を暗号化すること  
を特徴とする請求項 1 乃至 5 のいずれか 1 項に記載の情報処理装置。

20

【請求項 7】

前記暗号化手段による暗号化に用いる暗号方式を前記ユーザの操作に従って決定する暗号方式決定手段を更に備え、

前記暗号化手段は、前記暗号方式決定手段により決定した暗号化方式を用いて、前記入力された情報を暗号化すること  
を特徴とする請求項 1 乃至 6 に記載の情報処理装置。

30

【請求項 8】

ユーザによる情報の入力を受け付ける情報処理装置における処理方法であって、  
前記情報処理装置が、

前記情報の入力を受け付ける画面を出力する画面出力ステップと、

前記画面出力ステップにより出力された画面に入力された情報を暗号化する暗号化ステップと、

前記ユーザの操作又は所定時間の経過に従って、前記入力された情報を前記暗号化ステップにより暗号化した形態で出力するか暗号化しない形態で出力するかを制御する出力制御ステップと

を実行することを特徴とする処理方法。

40

【請求項 9】

ユーザによる情報の入力を受け付ける情報処理装置で実行可能なプログラムであって、  
前記情報処理装置を、

前記情報の入力を受け付ける画面を出力する画面出力手段と、

前記画面出力手段により出力された画面に入力された情報を暗号化する暗号化手段と、

前記ユーザの操作又は所定時間の経過に従って、前記入力された情報を前記暗号化手段により暗号化した形態で出力するか暗号化しない形態で出力するかを制御する出力制御手段

として機能させるためのプログラム。

50

## 【発明の詳細な説明】

## 【技術分野】

## 【0001】

本発明は、情報登録をするための情報処理装置、処理方法、およびプログラムに関する。

## 【背景技術】

## 【0002】

近年、インターネットを利用して商品やサービスを手軽に購入することができる。通常、商品やサービスの購入を希望する顧客は、商品の製造元やサービスを提供元の企業サイトや、百貨店のように複数企業の商品やサービスを取り扱う総合サイトにアクセスして購入する。

10

## 【0003】

いずれにしても、購入時には、購入者自身の氏名、住所、電話番号、性別、年齢、クレジットカード番号等のユーザ情報、および購入を希望する商品やサービスの番号、サイズ等の購入仕様、購入個数等の注文情報をサイト等の運営者に対して、通知提供しなければならない。

## 【0004】

なお、上記のユーザ情報はサイトに登録しておき、繰り返し商品やサービスを購入する場合、再度入力する手間を省くことができるため、顧客にとってユーザ情報を登録するメリットがある。一方、サイト運営者にとっても、ユーザ情報を再度入力する手間を省くことは、マウスのクリックだけで購入完了まで到達させることができるため、購入に対する心理的なハードルを下げる、顧客情報と購入履歴情報を基にマーケティング分析を行う、といったメリットがある。

20

## 【0005】

しかしながら、サイト運営者からの顧客情報流出事故は後を絶たず、外部からの不正アクセスによる犯行だけでなく、内部関係者による犯行も存在するため、インターネットを利用した商品やサービスの購入を躊躇するというユーザも少なくない。

## 【0006】

つまり、顧客がインターネットを利用した商品やサービスの購入に躊躇することの背景には、顧客の個人情報サイト運営者の管理下に半永久的に存在し、その個人情報が流出したり、不正利用されたりするリスクが常に潜んでいることが原因と考えられる。

30

## 【0007】

特許文献1には、顧客が購入を申込む際に、希望物品名並びに顧客の氏名、住所等の個人情報を暗号して申込を行い、インターネット送信途中における情報漏洩を防止可能なシステムが記載されている。

## 【先行技術文献】

## 【特許文献】

## 【0008】

【特許文献1】特開2002-334245号公報

## 【発明の概要】

40

## 【発明が解決しようとする課題】

## 【0009】

しかしながら、特許文献1のシステムでは、サイト運営者の限定的な担当者のみが暗号化された顧客情報を解読することができるとしており、万が一、この担当者が不正を犯した場合には、クレジットカード番号等の個人情報の流出してしまうという問題が生じる。

## 【0010】

また、特許文献1のシステムでは、商品やサービスを繰り返し購入する場合、ユーザ情報を再入力する手間を省くといった顧客にとってのメリットや、顧客情報と購入履歴情報を基にマーケティング分析を行うといったサイト運営者にとってのメリットが損なわれてしまうという問題もある。

50

また、近年では、ユーザが登録した情報がビッグデータとして２次利用されることが多いが、ユーザが登録した情報のうちビッグデータへの利用可能・利用不可の項目をユーザ自身が指定できないという課題もある。

【００１１】

そこで、本発明は、情報の漏洩リスクを低減しつつ、ユーザの利便性を損なわない仕組みを提供することを目的とする。

【課題を解決するための手段】

【００１２】

ユーザによる情報の入力を受け付ける情報処理装置であって、前記情報の入力を受け付ける画面を出力する画面出力手段と、前記画面出力手段により出力された画面に入力された情報を暗号化する暗号化手段と、前記ユーザの操作又は所定時間の経過に従って、前記入力された情報を前記暗号化手段により暗号化した形態で出力するか暗号化しない形態で出力するかを制御する出力制御手段とを備えることを特徴とする情報処理装置。

10

【発明の効果】

【００１３】

本発明によれば、情報の漏洩リスクを低減しつつ、ユーザの利便性を損なわない仕組みを提供することができる。

20

【図面の簡単な説明】

【００１４】

【図１】本実施形態の情報処理システム１００の構成の一例を示す図

【図２】本実施形態の情報処理装置１０１およびサーバ１０２のハードウェア構成の一例を示す図

【図３】本実施形態の情報処理装置１０１およびサーバ１０２の機能構成の一例を示すブロック図

【図４】本実施形態のユーザ登録処理の一例を示すフローチャート

【図５】本実施形態の情報処理装置１０１に出力されるユーザ登録画面５０１およびユーザ登録確認画面５２０の一例を示す図

30

【図６】本実施形態の認証処理の一例を示すフローチャート

【図７】本実施形態の商品注文処理の一例を示すフローチャート

【図８】本実施形態の情報処理装置１０１に出力される商品注文画面８０１の一例を示す図

【図９】本実施形態のユーザ情報復号処理の一例を示すフローチャート

【図１０】本実施形態の情報処理装置１０１に出力されるユーザ情報復号画面１００１の一例を示す図

【図１１】本実施形態のサーバ１０２におけるテーブルの一例

【図１２】第２の実施形態に係るユーザ登録画面表示処理の一例を示すフローチャート

【図１３】第２の実施形態に係るユーザ登録確認画面表示処理の一例を示すフローチャート

40

【図１４】第２の実施形態に係る情報処理装置１０１に出力されるユーザ登録画面およびユーザ登録確認画面の一例を示す図

【図１５】第２の実施形態に係るサーバ１０２におけるテーブルの一例

【発明を実施するための形態】

【００１５】

〔第１の実施形態〕

以下、図面を参照して本発明の実施形態を詳細に説明する。

図１は、本実施形態の情報処理システム１００の構成の一例を示す図である。

【００１６】

50

図 1 に示すように、情報処理システム 100 は、情報処理装置 101 およびサーバ 102 が、ネットワーク 103 により通信可能に接続された構成をとる。情報処理装置 101 は、デスクトップ PC、携帯電話、スマートフォン、タブレット端末、ノート PC、および PDA 端末などの端末であって、ブラウザがインストールされており、ネットワーク 103 を介して、サーバ 102 と通信可能である。

【0017】

情報処理システム 100 のユーザは、情報処理装置 101 にインストールされたウェブブラウザやクライアントソフトウェアなどを介し、サーバ 102 に対して情報の登録、サーバ 102 に登録されている情報の取得、取得した情報を用いた処理などを行う。

【0018】

サーバ 102 は、情報処理装置 101 からの要求に応じて、情報の登録、登録された情報の取得、取得した情報の送信などを行う。情報処理装置 101 とサーバ 102 間の通信は、HTTP のリクエスト・レスポンスでもよいし、SOAP などを利用したウェブサービスに用いられるリクエスト・レスポンスでもよい。

【0019】

なお、この実施形態においては、情報処理システム 100 はインターネットを利用して商品やサービスを購入するネットショッピングシステムとしたが、これに限定するものではなく、サーバ 102 が情報処理装置 101 から送信された情報を登録するシステムであればよい。

以下、図 2 を用いて、図 1 に示した情報処理装置 101 およびサーバ 102 に適用可能なハードウェア構成の一例について説明する。

【0020】

図 2 において、201 は CPU で、システムバス 204 に接続される各デバイスやコントローラを統括的に制御する。また、ROM 203 あるいは外部メモリ 211 には、CPU 201 の制御プログラムである BIOS (Basic Input / Output System) やオペレーティングシステムプログラム (以下、OS) や、各サーバあるいは各 PC の実行する機能を実現するために必要な各種プログラム等が記憶されている。

【0021】

202 は RAM で、CPU 201 の主メモリ、ワークエリア等として機能する。CPU 201 は、処理の実行に際して必要なプログラム等を ROM 203 あるいは外部メモリ 211 から RAM 202 にロードして、該ロードしたプログラムを実行することで各種動作を実現するものである。

【0022】

また、205 は入力コントローラで、入力装置 209 等からの入力を制御する。206 はビデオコントローラで、液晶ディスプレイ等のディスプレイ装置 210 への表示を制御する。なお、ディスプレイ装置は、液晶ディスプレイに限られず、CRT ディスプレイなどであっても良い。これらは必要に応じてクライアントが使用するものである。

【0023】

207 はメモリコントローラで、ブートプログラム、各種のアプリケーション、フォントデータ、ユーザファイル、編集ファイル、各種データ等を記憶するハードディスク (HD) や、フレキシブルディスク (FD)、或いは PCMCIA カードスロットにアダプタを介して接続されるコンパクトフラッシュ (登録商標) メモリ等の外部メモリ 211 へのアクセスを制御する。

【0024】

208 は通信 I/F コントローラで、ネットワーク 103 を介して外部機器と接続・通信するものであり、ネットワークでの通信制御処理を実行する。例えば、TCP/IP を用いた通信等が可能である。

【0025】

なお、CPU 201 は、例えば RAM 202 内の表示情報用領域へアウトラインフォントの展開 (ラスターライズ) 処理を実行することにより、ディスプレイ装置 210 上での表

10

20

30

40

50

示を可能としている。また、CPU 201は、ディスプレイ装置210上の不図示のマウスカーソル等でのユーザ指示を可能とする。

【0026】

ハードウェア上で動作する各種プログラムは、外部メモリ211に記録されており、必要に応じてRAM 202にロードされることによりCPU 201によって実行されるものである。

なお、全ての装置がこれらの構成を備えているわけではなく、必要なものを夫々備えていればよい。

【0027】

図3は、情報処理装置101の機能構成の一例を示すブロック図である。

10

登録画面出力部301は、ユーザ情報の登録を受け付ける登録画面を出力する機能部である。

決定部302は、登録画面出力部301により出力された登録画面に登録されたユーザ情報のうち、ユーザ情報の登録後にデータ分析に利用可能なデータと、利用不可とするデータをユーザの操作に従って決定する機能部である。

【0028】

決定部302は、登録画面出力部301により出力された登録画面に登録されたユーザ情報のうち、暗号化するユーザ情報をユーザの操作に従って決定する機能部である。

暗号キー受付部303は、登録画面に登録されたユーザ情報の暗号化に用いる暗号キーの入力を受け付ける機能部である。

20

暗号化部304は、暗号キー受付部303により受け付けた暗号キーを用いて、利用不可とするデータを暗号化する機能部である。

暗号化部304は、暗号キー受付部303により受け付けた暗号キーを用いて、ユーザ情報を暗号化する機能部である。

【0029】

暗号化部304は、決定部302により暗号化すると決定したユーザ情報を暗号化し、決定部302により暗号化すると決定したユーザ情報以外のユーザ情報を暗号化しない機能部である。

ユーザ情報送信部305は、データ分析に利用可能なデータと暗号化部304により暗号化されたデータとをサーバに送信する機能部である。

30

ユーザ情報送信部305は、暗号化されたユーザ情報を前記サーバに送信する機能部である。

形態出力部306は、決定部302により決定した利用可能なデータの利用可能な形態と、利用不可とするデータの利用不可な形態とを出力する機能部である。

【0030】

形態出力部306は、決定部302により暗号化すると決定したユーザ情報を暗号化した形態で出力し、決定部302により暗号化すると決定したユーザ情報以外のユーザ情報を暗号化しない形態で出力する機能部である。

形態出力部306は、ユーザ操作または所定時間の経過に従って、利用不可とするデータの出力を利用不可な形態から利用可能な形態へ変える機能部である。

40

【0031】

形態出力部306は、ユーザ操作または所定時間の経過に従って、決定部302により暗号化すると決定したユーザ情報の出力を、暗号化した形態から暗号化しない形態へ変える機能部である。

復号キー受付部307は、暗号化部304により暗号化されたデータの復号化に用いる復号キーの入力を受け付ける機能部である。

復号化部308は、復号キー受付部307により受け付けた復号キーを用いて、暗号化されたデータを復号化する機能部である。

暗号方式決定部309は、暗号化部304による暗号化に用いる暗号方式をユーザの操作に従って決定する機能部である。

50

暗号化部 304 は、暗号方式決定部 309 により決定した暗号化方式により利用不可とするデータを暗号化する機能部である。

【0032】

暗号化部 304 は、暗号方式決定部 309 により決定した暗号化方式を用いて、決定部 302 により暗号化すると決定したユーザ情報を暗号化する機能部である。

暗号化ユーザ情報送信部 310 は、暗号化部 304 により暗号化されたユーザ情報を、暗号化された状態でユーザマスタに記憶すべく、サーバに送信する機能部である。

暗号化ユーザ情報要求部 311 は、暗号化ユーザ情報送信部 310 により送信され、既にユーザマスタに記憶されている暗号化されたユーザ情報を、サーバに対して要求する機能部である。

10

復号キー受付部 307 は、暗号化ユーザ情報要求部 311 による要求に応じてサーバから受信した暗号化されたユーザ情報の復号化に用いる復号キーの入力を受け付ける機能部である。

表示部 312 は、復号化部 308 により復号化されたユーザ情報を用いて、前記サーバへ前記サービスの利用要求を行うために、当該復号化されたユーザ情報を表示する機能部である。

送信制御部 313 は、形態出力部 306 により、暗号化した形態で出力している場合は、暗号化ユーザ情報送信部 310 による暗号化されたユーザ情報のサーバへの送信を可能に制御し、一方、形態出力部 306 により、暗号化しない形態で出力している場合は、暗号化ユーザ情報送信部 310 による暗号化されたユーザ情報のサーバへの送信を不可能に制御する機能部である。

20

定義取得部 314 は、登録画面に登録されたユーザ情報のうち、暗号化するユーザ情報の項目の定義をサーバから取得する機能部である。

暗号化部 304 は、定義取得部 314 により取得された暗号化するユーザ情報の項目の定義に従って、ユーザ情報を暗号化する機能部である。

【0033】

図 4 は、本実施形態のユーザ登録処理の一例を示すフローチャートである。図 4 のユーザ登録処理とは、情報処理システム 100 が、情報処理システム 100 を利用するユーザによるユーザ情報の登録を受け付ける処理である。また、図 5 は、本実施形態の情報処理装置 101 に出力されるユーザ登録画面 501 およびユーザ登録確認画面 520 の一例を示す図である。また、図 10 は、本実施形態のサーバ 102 におけるテーブルの一例である。

30

ステップ S401 において、情報処理装置 101 の CPU 201 は、サーバ 102 にユーザ登録画面の画面情報の要求を送信する。

ステップ S402 において、サーバ 102 の CPU 201 は、情報処理装置 101 からユーザ登録画面の画面情報の要求を受信する。

ステップ S403 において、サーバ 102 の CPU 201 は、RAM 202 または外部メモリ 211 からユーザ登録画面情報を取得する。

ステップ S404 において、サーバ 102 の CPU 201 は、情報処理装置 101 に取得したユーザ登録画面情報を送信する。

40

ステップ S405 において、情報処理装置 101 の CPU 201 は、サーバ 102 からユーザ登録画面情報を受信する。

【0034】

ステップ S406 において、情報処理装置 101 の CPU 201 は、受信したユーザ登録画面情報を用いて、ディスプレイ装置 210 にユーザ登録画面 501 (図 5) を表示する。すなわち、ステップ S406 は、ユーザ情報の登録を受け付ける登録画面を出力する処理の一例を示すステップである。

【0035】

ステップ S407 において、情報処理装置 101 の CPU 201 は、ログイン用パスワード 502、ユーザ情報項目 503 ~ 509、および暗号化選択チェックボックス 510

50

～ 5 1 6 の入力を受け付ける。

【 0 0 3 6 】

すなわち、ステップ S 4 0 7 は、出力された登録画面に登録されたユーザ情報のうち、ユーザ情報の登録後にデータ分析に利用可能なデータと、利用不可とするデータをユーザの操作に従って決定する処理の一例を示すステップである。また、ステップ S 4 0 7 は、登録画面に登録されたユーザ情報のうち、暗号化するユーザ情報をユーザの操作に従って決定する処理の一例を示すステップである。

【 0 0 3 7 】

ステップ S 4 0 8 において、情報処理装置 1 0 1 の C P U 2 0 1 は、暗号方式 5 1 7 と暗号キー 5 1 8 の入力を受け付ける。すなわち、ステップ S 4 0 8 は、登録画面に登録されたユーザ情報の暗号化に用いる暗号キーの入力を受け付ける処理の一例を示すステップである。また、ステップ S 4 0 8 は、暗号化に用いる暗号方式をユーザの操作に従って決定する処理の一例を示すステップである。

【 0 0 3 8 】

ステップ S 4 0 9 において、情報処理装置 1 0 1 の C P U 2 0 1 は、ステップ S 4 0 7 にて選択された暗号化選択チェックボックス 5 1 0 ～ 5 1 6 に対応するユーザ情報項目 5 0 3 ～ 5 0 9 の値を、ステップ S 4 0 8 にて選択された暗号方式 5 1 7 と入力された暗号キー 5 1 8 を用いて暗号化し、R A M 2 0 2 に記憶する。

【 0 0 3 9 】

すなわち、ステップ S 4 0 9 は、受け付けた暗号キーを用いて、前記利用不可とするデータを暗号化する処理の一例を示すステップである。また、ステップ S 4 0 9 は、決定した暗号化方式により前記利用不可とするデータを暗号化する処理の一例を示すステップである。

すなわち、ステップ S 4 0 9 は、受け付けた暗号キーを用いて、ユーザ情報を暗号化する処理の一例を示すステップである。

【 0 0 4 0 】

また、ステップ S 4 0 9 は、暗号化すると決定したユーザ情報を暗号化し、暗号化すると決定したユーザ情報以外のユーザ情報を暗号化しない処理の一例を示すステップである。また、ステップ S 4 0 9 は、決定した暗号化方式を用いて、暗号化すると決定したユーザ情報を暗号化する処理の一例を示すステップである。

【 0 0 4 1 】

また、ステップ S 4 0 7 にて選択された暗号化選択チェックボックス 5 1 0 ～ 5 1 6 に対応する項目名、具体的には、図 5 の場合、チェックボックスがチェックされている「氏名」「住所」「電話番号」「クレジットカード番号」を暗号化した項目として、R A M 2 0 2 に項目名を記憶する。

【 0 0 4 2 】

なお、ステップ S 4 0 9 における暗号化処理は、J a v a S c r i p t (登録商標)ライブラリ等を用いて情報処理装置 1 0 1 の C P U 2 0 1 が行う。これにより、ユーザ情報の登録後にデータ分析に利用不可とユーザが所望したデータ(暗号化選択チェックボックス 5 1 0 ～ 5 1 6 でチェックした項目への入力値)は、情報処理装置 1 0 1 において暗号化されるため、暗号化されていない状態でネットワーク 1 0 3 を通じて外部に漏洩することがない。

【 0 0 4 3 】

ステップ S 4 1 0 において、情報処理装置 1 0 1 の C P U 2 0 1 は、ステップ S 4 0 9 にて暗号化したユーザ情報(以下、「暗号化済情報」と記す)と、暗号化していないユーザ情報(以下、「非暗号化情報」と記す)を用いて、ディスプレイ装置 2 1 0 にユーザ登録確認画面 5 2 0 (図 5)を表示する。なお、ユーザが暗号化済情報と非暗号化情報とを容易に識別できるよう、フォント、色、文字背景を変える等によって識別して表示する。

【 0 0 4 4 】

すなわち、ステップ S 4 1 0 は、利用可能なデータの利用可能な形態と、利用不可とす

10

20

30

40

50



るデータの利用不可な形態とを出力する処理の一例を示すステップである。また、ステップS 4 1 0は、暗号化すると決定したユーザ情報を暗号化した形態で出力し、暗号化すると決定したユーザ情報以外のユーザ情報を暗号化しない形態で出力する処理の一例を示すステップである。

#### 【 0 0 4 5 】

具体的には、ユーザ登録確認画面5 2 0 (図5)では、「氏名」「住所」「電話番号」が暗号化済情報であり、「性別」「生年月日」「メール」が非暗号化情報である。なお、「暗号化済情報」と「非暗号化情報」を合わせたユーザ情報全体を「部分暗号化済ユーザ情報」と呼ぶ。これにより、ユーザによって入力された個人情報のうち、データ分析に利用可能なデータと利用不可とするデータを識別して表示することができるため、ユーザは自身の個人情報が流出したり、不正利用されたりする恐れを低減することができる。

10

#### 【 0 0 4 6 】

なお、ユーザ登録確認画面5 2 0 (図5)では、「暗号化済情報」は暗号化された状態で表示し、データ分析に利用不可とするデータを識別して表示することとしたが、その場合、ユーザ登録画面5 0 1 (図5)で入力した値を確認することができない。よって、ユーザ登録確認画面5 2 0において、「暗号化済情報」にマウスをかざされたこと(オンマウス操作)を受け付けると、暗号化していない値を確認することができるようにする(不図示)。

#### 【 0 0 4 7 】

なお、「暗号化済情報」の暗号化していない値を確認する方法として、オンマウス操作を例に挙げたが、この方法に限定するものではなく、ボタン押下を受け付けて暗号化状態/非暗号化状態を切り替えたり、ユーザの操作とは無関係に(所定時間が経過した等により)アニメーション効果によって暗号化状態から非暗号化状態へ表示を変えたりする等、「暗号化済情報」の暗号化していない値をユーザが確認できれば他の方法であってもよい。

20

#### 【 0 0 4 8 】

すなわち、ステップS 4 1 0は、ユーザ操作または所定時間の経過に従って、利用不可とするデータの出力を利用不可な形態から利用可能な形態へ変える処理の一例を示すステップである。また、ステップS 4 1 0は、ユーザ操作または所定時間の経過に従って、暗号化すると決定したユーザ情報の出力を、暗号化した形態から暗号化しない形態へ変える処理の一例を示すステップである。

30

#### 【 0 0 4 9 】

なお、この実施形態においては、情報処理装置1 0 1は、ユーザ登録確認画面5 2 0の画面情報の「暗号化済情報」と「非暗号化情報」、つまり「部分暗号化済ユーザ情報」をサーバ1 0 2に送信することなく、情報処理装置1 0 1にて生成することとしたが、この方法に限定するものではなく、「部分暗号化済ユーザ情報」をサーバ1 0 2に送信し、サーバ1 0 2にて生成されたユーザ登録確認画面5 2 0の画面情報を受信し、情報処理装置1 0 1で表示するとしてもよい。ただし、その場合も、ステップS 4 0 9の説明で述べたように、ユーザ情報の登録後にデータ分析に利用不可とユーザが所望したデータ(暗号化済情報)は、暗号化された状態でサーバ1 0 2に送信されるため、暗号化されていない状態でネットワーク1 0 3を通じて外部に漏洩することはない。

40

#### 【 0 0 5 0 】

ステップS 4 1 1において、情報処理装置1 0 1のCPU 2 0 1は、サーバ1 0 2に部分暗号化済ユーザ情報を送信する。また、ステップS 4 0 9にて、RAM 2 0 2に記憶した暗号化した項目名も併せて送信する。すなわち、ステップS 4 1 1は、データ分析に利用可能なデータと暗号化されたデータとをサーバに送信する処理の一例を示すステップである。また、ステップS 4 1 1は、暗号化されたユーザ情報を、暗号化された状態でユーザマスタに記憶すべく、サーバに送信する処理の一例を示すステップである。

ステップS 4 1 2において、サーバ1 0 2のCPU 2 0 1は、情報処理装置1 0 1から部分暗号化済ユーザ情報と暗号化した項目名を受信する。

50

## 【 0 0 5 1 】

ステップ S 4 1 3 において、サーバ 1 0 2 の C P U 2 0 1 は、部分暗号化済ユーザマスタ 1 1 1 0 ( 図 1 1 ) に、受信した部分暗号化済ユーザ情報と暗号化した項目名を登録する。

ステップ S 4 1 4 において、サーバ 1 0 2 の C P U 2 0 1 は、情報処理装置 1 0 1 に部分暗号化済ユーザ情報の登録完了通知を送信する。

ステップ S 4 1 5 において、情報処理装置 1 0 1 の C P U 2 0 1 は、サーバ 1 0 2 から部分暗号化済ユーザ情報の登録完了通知を受信する。

## 【 0 0 5 2 】

ステップ S 4 1 6 において、情報処理装置 1 0 1 の C P U 2 0 1 は、非暗号化情報の値を抽象化し、データ分析に利用可能なマーケティング情報を生成する。具体的には、図 5 において、暗号化選択チェックボックス 5 1 0 ~ 5 1 6 のうち、チェックされなかった項目「性別」「生年月日」「メール」への入力値から、データ分析に利用可能なマーケティング情報を生成する。例えば、マーケティング情報の例として、生年月日の値 ( 1 9 8 2 / 0 1 / 0 2 ) から、「30代前半」のようにデータ分析に利用可能な値に変換することでマーケティング情報を生成する。

ステップ S 4 1 7 において、情報処理装置 1 0 1 の C P U 2 0 1 は、サーバ 1 0 2 に生成したマーケティング情報を送信する。

ステップ S 4 1 8 において、サーバ 1 0 2 の C P U 2 0 1 は、情報処理装置 1 0 1 からマーケティング情報を受信する。

## 【 0 0 5 3 】

ステップ S 4 1 9 において、サーバ 1 0 2 の C P U 2 0 1 は、受信したマーケティング情報をマーケティング情報マスタ 1 1 2 0 ( 図 1 1 ) に登録する。なお、この実施形態においては、ステップ S 4 1 1 にて部分暗号化済ユーザ情報の送信、ステップ S 4 1 7 にてマーケティング情報を送信のようにサーバ 1 0 2 への送信処理を 2 回に分けたが、この送信方法に限定するものではなく、1 度にまとめて送信したり、「暗号化済情報」「非暗号化情報」「マーケティング情報」のように 3 回に分けたり、入力項目毎に分けたりしてもよい。

## 【 0 0 5 4 】

なお、部分暗号化済ユーザマスタ 1 1 1 0 とマーケティング情報マスタ 1 1 2 0 とは、ほぼ同じカラムを持つが、部分暗号化済ユーザマスタ 1 1 1 0 に存在するカラムで明らかにマーケティング情報としては利用しない項目 ( 例えば、「パスワード」「クレジットカード番号」) はマーケティング情報マスタ 1 1 2 0 には持たない。

## 【 0 0 5 5 】

また、マーケティング情報マスタ 1 1 2 0 には、データ分析に利用不可とユーザが所望したデータ ( 暗号化済情報 ) は登録しない。データ分析の際には、部分暗号化済ユーザマスタ 1 1 1 0 ではなく、マーケティング情報マスタ 1 1 2 0 を利用することで、データ分析に利用可能であるとユーザが所望したデータ ( 非暗号化情報 ) を用いてデータ分析することが可能になる。

ステップ S 4 2 0 において、サーバ 1 0 2 の C P U 2 0 1 は、情報処理装置 1 0 1 にマーケティング情報の登録完了通知を送信する。

ステップ S 4 2 1 において、情報処理装置 1 0 1 の C P U 2 0 1 は、サーバ 1 0 2 からマーケティング情報の登録完了通知を受信する。

ステップ S 4 2 2 において、情報処理装置 1 0 1 の C P U 2 0 1 は、ディスプレイ装置 2 1 0 に処理完了画面を表示する。

以上で、図 4 のユーザ登録処理の説明を終了する。

## 【 0 0 5 6 】

図 6 は、本実施形態の認証処理の一例を示すフローチャートである。図 6 の認証処理とは、図 4 でユーザ情報の登録処理を行ったユーザによって、情報処理システム 1 0 0 へのログイン要求に伴う認証処理である。

ステップS 6 0 1において、情報処理装置1 0 1のCPU 2 0 1は、ユーザの操作に従って、サーバ1 0 2にユーザ認証画面の要求を送信する。

ステップS 6 0 2において、サーバ1 0 2のCPU 2 0 1は、情報処理装置1 0 1からユーザ認証画面の要求を受信する。

ステップS 6 0 3において、サーバ1 0 2のCPU 2 0 1は、RAM 2 0 2または外部メモリ2 1 1からユーザ認証画面情報を取得する。

ステップS 6 0 4において、サーバ1 0 2のCPU 2 0 1は、情報処理装置1 0 1に取得したユーザ認証画面情報を送信する。

ステップS 6 0 5において、情報処理装置1 0 1のCPU 2 0 1は、サーバ1 0 2からユーザ認証画面情報を受信する。

10

#### 【0 0 5 7】

ステップS 6 0 6において、情報処理装置1 0 1のCPU 2 0 1は、受信したユーザ認証画面情報を用いて、ディスプレイ装置2 1 0にユーザ認証画面（不図示）を表示する。ユーザ認証画面は、いわゆるログイン画面であり、ユーザIDとパスワードの入力を受け付ける画面である。

ステップS 6 0 7において、情報処理装置1 0 1のCPU 2 0 1は、認証情報としてユーザIDとパスワードの入力を受け付ける。

ステップS 6 0 8において、情報処理装置1 0 1のCPU 2 0 1は、サーバ1 0 2に認証情報（ユーザIDとパスワード）を送信する。

ステップS 6 0 9において、サーバ1 0 2のCPU 2 0 1は、情報処理装置1 0 1から認証情報を受信する。

20

ステップS 6 1 0において、サーバ1 0 2のCPU 2 0 1は、受信した認証情報を検索キーとして、部分暗号化済ユーザマスタ1 1 1 0を検索する。

#### 【0 0 5 8】

ステップS 6 1 1において、サーバ1 0 2のCPU 2 0 1は、ステップS 6 1 0にてユーザ情報がヒットした場合、RAM 2 0 2または外部メモリ2 1 1から認証完了画面情報を取得する。

ステップS 6 1 2において、サーバ1 0 2のCPU 2 0 1は、情報処理装置1 0 1に取得した認証完了画面情報を送信する。

ステップS 6 1 3において、情報処理装置1 0 1のCPU 2 0 1は、サーバ1 0 2から認証完了画面情報を受信する。

30

#### 【0 0 5 9】

ステップS 6 1 4において、情報処理装置1 0 1のCPU 2 0 1は、受信した認証完了画面情報を用いて、ディスプレイ装置2 1 0に認証完了画面（不図示）を表示する。認証完了画面とは、いわゆるログイン成功画面であって、ログインが成功したことをユーザに通知する画面や、ログイン直後に表示されるメニュー画面などを指す。

以上で、図6の認証処理の説明を終了する。

#### 【0 0 6 0】

図7は、本実施形態の商品注文処理の一例を示すフローチャートである。図7の商品注文処理とは、図6で情報処理システム1 0 0へログインしたユーザによる図4で登録したユーザ情報の利用を受け付ける処理である。また、図8は、本実施形態の情報処理装置1 0 1に出力される商品注文画面8 0 1の一例を示す図である。

40

ステップS 7 0 1において、情報処理装置1 0 1のCPU 2 0 1は、サーバ1 0 2に商品注文開始の要求を送信する。

ステップS 7 0 2において、サーバ1 0 2のCPU 2 0 1は、情報処理装置1 0 1から商品注文開始の要求を受信する。

ステップS 7 0 3において、サーバ1 0 2のCPU 2 0 1は、RAM 2 0 2または外部メモリ2 1 1から商品注文画面情報を取得する。

ステップS 7 0 4において、サーバ1 0 2のCPU 2 0 1は、情報処理装置1 0 1に取得した商品注文画面情報を送信する。

50

ステップS705において、情報処理装置101のCPU201は、サーバ102から商品注文画面情報を受信する。

【0061】

ステップS706において、情報処理装置101のCPU201は、受信した商品注文画面情報を用いて、ディスプレイ装置210に商品注文画面801（図8）を表示する。

【0062】

ステップS707において、情報処理装置101のCPU201は、購入する商品807～808の情報の入力を受け付ける。この情報は、ユーザによって値が入力されるとしてもよいし、商品紹介ページ（不図示）においてユーザが選択した商品の情報が購入する商品807～808に設定されるとしてもよい。

10

ステップS708において、情報処理装置101のCPU201は、ユーザによる自動入力ボタン802の押下を受け付ける。

【0063】

自動入力ボタン802の押下を受け付けなかった場合、ステップS709において、情報処理装置101のCPU201は、商品配送先情報803～805の入力を受け付ける。

【0064】

自動入力ボタン802の押下を受け付けた場合、ステップS710において、情報処理装置101のCPU201は、サーバ102からユーザ情報取得済みか否かを判定する。ユーザ情報取得済みか否かの判定は、RAM202にユーザ情報が記憶されているか否かで判定する。つまり、ユーザが図7の商品注文処理を繰り返し行った場合、後述するステップS715の処理によって、RAM202にユーザ情報が記憶されているため、ユーザ情報取得済みと判定する。

20

【0065】

ユーザ情報未取得と判定した場合、ステップS711において、情報処理装置101のCPU201は、サーバ102に対してユーザIDとともに部分暗号化済ユーザ情報の要求を送信する。すなわち、ステップS711は、送信され、既にユーザマスタに記憶されている暗号化されたユーザ情報をサーバに対して要求する処理の一例を示すステップである。

ステップS712において、サーバ102のCPU201は、情報処理装置101からユーザIDと部分暗号化済ユーザ情報の要求を受信する。

30

【0066】

ステップS713において、サーバ102のCPU201は、ユーザIDを検索キーとして、部分暗号化済ユーザマスタ1110から部分暗号化済ユーザ情報を取得する。また、サーバ102のCPU201は、RAM202または外部メモリ211からユーザ情報復号画面情報を取得する。

【0067】

ステップS714において、サーバ102のCPU201は、情報処理装置101に取得した部分暗号化済ユーザ情報およびユーザ情報復号画面情報を送信する。

【0068】

40

ステップS715において、情報処理装置101のCPU201は、サーバ102から部分暗号化済ユーザ情報およびユーザ情報復号画面情報を受信する。すなわち、ステップS715は、サーバから送信された前記暗号化されたユーザ情報を受信する処理の一例を示すステップである。

ステップS716において、情報処理装置101のCPU201は、部分暗号化済ユーザ情報の復号処理（図9）を実行する。

【0069】

ステップS717において、情報処理装置101のCPU201は、復号化されたユーザ情報を用いて、商品配送先と支払方法の値として出力することによって自動入力する。すなわち、ステップS717は、復号化されたユーザ情報を用いて、サーバへサービスの

50

利用要求を行うために、復号化されたユーザ情報を表示する処理の一例を示すステップである。具体的には、復号化された「氏名」「住所」「電話」「クレジットカード番号」の値を、商品注文画面 801 の氏名 803、住所 804、電話 805、およびクレジットカード番号 806 の値として出力する（図 10 の 1005）。

【0070】

ステップ S718 において、情報処理装置 101 の CPU 201 は、注文ボタン 809 の押下を受け付け、サーバ 102 に商品配送先、支払方法、購入する商品の情報を含む商品注文要求を送信する。

ステップ S719 において、サーバ 102 の CPU 201 は、情報処理装置 101 から商品注文要求を受信する。

10

【0071】

ステップ S720 において、サーバ 102 の CPU 201 は、商品注文要求から商品配送先、支払方法、購入する商品の情報を取得し、注文トランザクション 1130 と配送トランザクション 1140 に登録する。具体的には、新たに発番した配送番号、商品配送先の「氏名」「住所」「電話」を用いて配送レコードを生成し、配送トランザクション 1140 に登録する。配送番号、購入する商品の情報を用いて、注文レコードを生成し、注文トランザクション 1130 に登録する。

【0072】

なお、支払方法の「クレジットカード番号」は決済が完了した時点で RAM 202 から消去し、注文トランザクション 1130 などのテーブルには記憶しない。なお、配送トランザクション 1140 には、「氏名」「住所」「電話」といった個人情報が含まれており、部分暗号化済ユーザマスタ 1110 および注文トランザクション 1130 とテーブル結合させることで、部分暗号化済ユーザマスタ 1110 に登録されているユーザの個人情報が明らかになってしまう。そのため、部分暗号化済ユーザマスタ 1110 および注文トランザクション 1130 は別筐体のデータベースに保管したり、別のデータベースユーザの所有テーブルとしたりすることで、外部からの不正アクセスだけでなく、サイト運営の内部関係者による操作であっても部分暗号化済ユーザマスタ 1110 と配送トランザクション 1140 はテーブル結合ができないように管理する。

20

【0073】

これにより、外部からの不正アクセスやサイト運営の内部関係者による犯行によって、情報処理システム 100 を利用するユーザの個人情報が流出したり、不正利用されたりするリスクを低減することができる。

30

ステップ S721 において、サーバ 102 の CPU 201 は、RAM 202 または外部メモリ 211 から商品注文完了画面情報を取得する。

ステップ S722 において、サーバ 102 の CPU 201 は、情報処理装置 101 に取得した商品注文完了画面情報を送信する。

ステップ S723 において、情報処理装置 101 の CPU 201 は、サーバ 102 から商品注文完了画面情報を受信する。

【0074】

ステップ S724 において、情報処理装置 101 の CPU 201 は、受信した商品注文完了画面情報を用いて、ディスプレイ装置 210 に商品注文完了画面（不図示）を表示する。

40

以上で、図 7 の商品注文処理の説明を終了する。

【0075】

図 9 は、本実施形態のユーザ情報復号処理の一例を示すフローチャートである。図 9 のユーザ情報復号処理とは、図 7 でユーザ情報を利用しようとするユーザに係る部分暗号化済ユーザ情報の復号化を行う処理である。また、図 10 は、本実施形態の情報処理装置 101 に出力されるユーザ情報復号画面 1001 の一例を示す図である。

【0076】

ステップ S901 において、情報処理装置 101 の CPU 201 は、ステップ S715

50

にて受信したユーザ情報復号画面情報を用いて、ディスプレイ装置 210 にユーザ情報復号画面 1001 (図 10) を表示する。

【0077】

ステップ S902 において、情報処理装置 101 の CPU 201 は、復号処理に用いる暗号方式 1002 と暗号キー 1003 の入力を受け付ける。すなわち、ステップ S902 は、サーバから受信した暗号化されたデータの復号化に用いる復号キーの入力を受け付ける処理の一例を示すステップである。

【0078】

ステップ S903 において、情報処理装置 101 の CPU 201 は、復号化ボタン 1004 が押下を受け付けると、ステップ S715 にて受信した部分暗号化済ユーザ情報から「暗号化項目」を取得し、部分暗号化済ユーザ情報のうち、「暗号化項目」に対応する項目を、ステップ S902 にて受け付けた暗号方式 1002 と暗号キー 1003 を用いて復号化する。

【0079】

すなわち、ステップ S903 は、復号キーを用いて、暗号化されたユーザ情報を復号化する処理の一例を示すステップである。具体的には、「暗号化項目」= { 氏名 / 住所 / 電話 / クレジットカード番号 } の場合、部分暗号化済ユーザ情報のうち、{ 氏名 / 住所 / 電話 / クレジットカード番号 } の項目の値を復号化する。

以上で、図 9 のユーザ情報復号処理の説明を終了する。

【0080】

以上により、ユーザが所望する態様で、情報漏洩リスクを低減する仕組みを提供することができる。つまり、ユーザが所望する情報が暗号化された状態でシステムにおいて管理されるため、顧客が入力した情報が不正利用されるリスクを低減することができる。

【0081】

また、以上により、暗号化した情報 (暗号化済情報) は、再利用する際にユーザによって復号化されるため、商品やサービスを繰り返し購入する場合にユーザ情報を再入力する手間を省くといったユーザにとってのメリットは損なわれない。つまり、ユーザ情報の漏洩リスクを低減しつつ、ユーザの利便性を損なわないようにすることができる。

また、以上により、暗号化していない情報 (非暗号化情報) は、マーケティング情報として利用することが可能であるため、顧客情報と購入履歴情報を基にマーケティング分析を行うといったサイト運営者にとってのメリットは損なわれない。

【0082】

なお、この実施形態においては、ユーザが登録する情報はユーザの個人情報としたが、個人情報に限定するものではなく、ユーザが登録する情報であれば、個人情報でなくてもよい。つまり、システムに登録する情報のうち、情報登録後のデータ分析に利用可能・利用不可な情報を、ユーザの操作に従って決定することができる。これにより、システムに登録する情報のうち、ビッグデータ等のデータ分析に利用可能・利用不可な情報をユーザ自身が決定することができる。

【0083】

また、本発明は、クライアント端末のブラウザからサーバにおける通信データの暗号化技術である SSL (Secure Sockets Layer) とは異なり、クライアント端末で暗号化された情報を暗号化された状態のまま、サーバに記憶するため、サーバにおいて復号化処理を行わない。そして、本発明は、ユーザがこの暗号化された情報を用いて購入処理などのサービスを利用する際に、暗号化された情報をクライアント端末に受信し、クライアント端末において復号化を行う。これにより、外部からの不正アクセスや、サイト運営者など内部関係者の犯行による、ユーザ情報の漏洩リスクを低減しつつ、ユーザの利便性を損なわないようにすることができる。

【0084】

〔第 2 の実施形態〕

第 1 の実施形態は、暗号化するデータと暗号化しないデータをユーザの操作に従って決

10

20

30

40

50

定する仕組みであり、第2の実施形態は、ユーザの操作による決定だけでなく、暗号化するデータと暗号化しないデータをシステムとして定義しておき、その定義に従って決定する仕組みである。

【0085】

また、第1の実施形態は、ユーザ登録確認画面において、暗号化した状態と暗号化しない状態を切り替えて表示する仕組みであり、第2の実施形態は、その表示の切り替えに従って、サーバへの送信ボタンを押下の可否を制御する仕組みである。

【0086】

図12は、第2の実施形態に係るユーザ登録画面表示処理の一例を示すフローチャートであり、第1の実施形態における図4のステップS406（ユーザ登録画面表示）を置き換えたものである。

10

【0087】

図13は、第2の実施形態に係るユーザ登録確認画面表示処理の一例を示すフローチャートであり、第1の実施形態における図4のステップS410（ユーザ登録確認画面表示）を置き換えたものである。

図14は、第2の実施形態に係る情報処理装置101に出力されるユーザ登録画面およびユーザ登録確認画面の一例を示す図であ

【0088】

り、1401は第1の実施形態における図5の501（ユーザ登録画面）を置き換えた画面であり、1420および1430は第1の実施形態における図5の520（ユーザ登録確認画面）を置き換えた画面である。図14において、図5と同じ箇所については、説明を省略する。

20

図15は、第2の実施形態に係るサーバ102におけるテーブルの一例である。

【0089】

図12を用いて、第2の実施形態に係るユーザ登録画面表示処理について説明する。

ステップS1201において、情報処理装置101のCPU201は、ステップS405にて受信したユーザ登録画面情報を用いて、ディスプレイ装置210にユーザ登録画面1401（図14）を表示する。すなわち、ステップS1201は、ユーザ情報の登録を受け付ける登録画面を出力する処理の一例を示すステップである。

ステップS1202において、情報処理装置101のCPU201は、入力項目の数だけ、ステップS1203～ステップS1207を繰り返す。

30

【0090】

ステップS1203において、情報処理装置101のCPU201は、入力項目のデフォルト暗号マスタの値を判定する。なお、第2の実施形態においては、サーバ102は、ステップS403にてデフォルト暗号マスタ1500の値を取得し、ステップS403にてデフォルト暗号マスタ1500の値をユーザ登録画面情報に含めて送信する。よって、情報処理装置101は、ステップS405にてユーザ登録画面情報に含まれるデフォルト暗号マスタ1500の値を受信する。すなわち、ステップS405は、登録画面に登録されたユーザ情報のうち、暗号化するユーザ情報の項目の定義をサーバから取得する処理の一例を示すステップである。

40

【0091】

ここで、図15のデフォルト暗号マスタ1500について説明しておく。デフォルト暗号マスタ1500は、ユーザ登録画面1401における入力項目の暗号化する／しないのデフォルト値を定義し、また暗号化する／しないをユーザが変更できる／できないを定義するテーブルである。

【0092】

入力項目ごとの設定値について説明する。 は、デフォルトで暗号化する、かつ暗号化する／しないをユーザが変更できる。 は、デフォルトで暗号化しない、かつ暗号化する／しないをユーザが変更できる。 は、デフォルトで暗号化する、かつ暗号化する／しないをユーザが変更できない。 は、デフォルトで暗号化しない、かつ暗号化する／しない

50

をユーザが変更できない。という意味である。

【0093】

よって、図15のデフォルト暗号マスタ1500の場合、「性別」「生年月日」は(マーケティング分析に利用するため)必ず暗号化しない。「氏名」「クレジットカード番号」は(マーケティング分析に利用しないため)必ず暗号化する、という意味である。これにより、ユーザの操作による決定だけでなく、暗号化するデータと暗号化しないデータをシステムとして定義しておき、その定義に従って決定することができるため、顧客情報を基にマーケティング分析を行うといったサイト運営者にとってのメリットは損なわれない。また、以上により、暗号化していない情報(非暗号化情報)は、マーケティング情報として利用することが可能であるため、顧客情報と購入履歴情報を基にマーケティング分析を行うといったサイト運営者にとってのメリットは損なわれない。

10

【0094】

なお、本実施形態においては、デフォルト暗号マスタ1500には1レコードしか登録していないが、1件に限定するものではなく、例えば、ユーザIDのカラムにロールなどの権限を設定して、権限毎にレコードを登録し、権限によって暗号化可否の範囲を変えらるゝとしてもよい。また、ユーザの年齢、性別などによって、暗号化可否の範囲を変えらるゝとしてもよい。

図12の説明に戻る。

【0095】

ステップS1203における入力項目のデフォルト暗号マスタの値の判定結果が、 の場合はステップS1204に進み、 の場合はステップS1202に戻り、 の場合はステップS1206に進み、 の場合はステップS1207に進む。

20

【0096】

ステップS1204において、情報処理装置101のCPU201は、対象の入力項目のチェックボックスを表示するHTMLタグにchecked属性を追加する。これにより、ユーザ登録画面情報が表示された時点(デフォルト)で、チェックボックス=ONの状態であり、ユーザはON/OFFを変更できる(図14の1412、1413)。

【0097】

ステップS1205において、情報処理装置101のCPU201は、対象の入力項目のチェックボックスを表示するHTMLタグにdisabled属性を追加する。ステップS1206において、情報処理装置101のCPU201は、対象の入力項目のチェックボックスを表示するHTMLタグにchecked属性を追加する。これにより、ユーザ登録画面情報が表示された時点(デフォルト)で、チェックボックス=ONの状態であり、ユーザはONの状態を変更できない(図14の1410、1416)。

30

【0098】

ステップS1207において、情報処理装置101のCPU201は、対象の入力項目のチェックボックスを表示するHTMLタグにdisabled属性を追加する。これにより、ユーザ登録画面情報が表示された時点(デフォルト)で、チェックボックス=OFFの状態であり、ユーザはOFFの状態を変更できない(図14の1411、1414)。

40

【0099】

なお、図14の1401および図15においては、図面および設定値をわかりやすくするため、 と記したが、これに限定するものではなく、その他の表示方法や設定値であってもよい。

以上で、図12のユーザ登録画面表示処理の説明を終了する。

【0100】

よって、この後、ステップS409では、受け付けた暗号キーを用いて、ユーザ情報を暗号化するが、ステップS1203にて取得したデフォルト暗号マスタ1500の値に従って、ユーザ情報を暗号化するため、ステップS409は、取得された暗号化するユーザ情報の項目の定義に従って、ユーザ情報を暗号化する処理の一例を示すステップである。

50



## 【 0 1 0 1 】

次に、図 1 3 を用いて、第 2 の実施形態に係るユーザ登録確認画面表示処理について説明する。

ステップ S 1 3 0 1 において、情報処理装置 1 0 1 の C P U 2 0 1 は、ステップ S 4 0 9 にて暗号化したユーザ情報（対応するチェックボックスが O N 状態の情報）を用いて、ディスプレイ装置 2 1 0 にユーザ登録確認画面 1 4 2 0（図 1 4）を表示する。すなわち、ステップ S 1 3 0 1 は、利用可能なデータの利用可能な形態と、利用不可とするデータの利用不可な形態とを出力する処理の一例を示すステップである。

## 【 0 1 0 2 】

ステップ S 1 3 0 1 において、情報処理装置 1 0 1 の C P U 2 0 1 は、暗号化スイッチの切り替えを受け付け、暗号化スイッチの値を判定する。具体的には、暗号化スイッチには、「入力値」と「暗号化」の状態があり、暗号化スイッチをクリックする等のユーザ操作によって、この状態を切り替えることができる。なお、図 1 4 の 1 4 2 1 が「暗号化」の状態、図 1 4 の 1 4 3 1 が「入力値」の状態である。

## 【 0 1 0 3 】

ステップ S 1 3 0 1 における暗号化スイッチの値の判定結果が、「入力値」の場合はステップ S 1 3 0 3 に進み、「暗号化」の場合はステップ S 1 3 0 5 に進む。

## 【 0 1 0 4 】

ステップ S 1 3 0 3 において、情報処理装置 1 0 1 の C P U 2 0 1 は、チェックボックスが O N 状態のユーザ情報の入力値を復号化して表示する（図 1 4 の 1 4 3 2）。また、ステップ S 1 3 0 3 は、ユーザ操作または所定時間の経過に従って、暗号化すると決定したユーザ情報の出力を、暗号化した形態から暗号化しない形態へ変える処理の一例を示すステップである。例えば、図 1 4 のユーザ登録画面 1 4 0 1 において、O N 状態のチェックボックスは、1 4 1 0、1 4 1 2、1 4 1 3、1 4 1 6 であり、それぞれに対応する氏名 1 4 0 3、住所 1 4 0 5、電話番号 1 4 0 6、クレジットカード番号 1 4 0 9 の入力値を復号化し、1 4 3 2 のように表示する。

## 【 0 1 0 5 】

ステップ S 1 3 0 4 において、情報処理装置 1 0 1 の C P U 2 0 1 は、送信ボタンを表示する H T M L タグに d i s a b l e d 属性を追加する。これにより、図 1 4 のユーザ登録確認画面 1 4 3 0 では、ユーザは送信ボタン 1 4 3 3 を押下できないようになる。すなわち、ステップ S 1 3 0 4 は、暗号化しない形態で出力している場合は、暗号化されたユーザ情報のサーバへの送信を不可能に制御する処理の一例を示すステップである。

## 【 0 1 0 6 】

ステップ S 1 3 0 5 において、情報処理装置 1 0 1 の C P U 2 0 1 は、チェックボックスが O N 状態のユーザ情報の入力値を暗号化して表示する（図 1 4 の 1 4 2 2）。すなわち、ステップ S 4 1 0 は、暗号化すると決定したユーザ情報を暗号化した形態で出力し、暗号化すると決定したユーザ情報以外のユーザ情報を暗号化しない形態で出力する処理の一例を示すステップである。例えば、図 1 4 のユーザ登録画面 1 4 0 1 において、O N 状態のチェックボックスは、1 4 1 0、1 4 1 2、1 4 1 3、1 4 1 6 であり、それぞれに対応する氏名 1 4 0 3、住所 1 4 0 5、電話番号 1 4 0 6、クレジットカード番号 1 4 0 9 の入力値を暗号化し、1 4 2 2 のように表示する。

## 【 0 1 0 7 】

ステップ S 1 3 0 6 において、情報処理装置 1 0 1 の C P U 2 0 1 は、送信ボタンを表示する H T M L タグから d i s a b l e d 属性を削除する。これにより、図 1 4 のユーザ登録確認画面 1 4 2 0 では、ユーザは送信ボタン 1 4 2 3 を押下できるようになる。すなわち、ステップ S 1 3 0 6 は、暗号化した形態で出力している場合は、暗号化されたユーザ情報のサーバへの送信を可能に制御する処理の一例を示すステップである。

## 【 0 1 0 8 】

ステップ S 1 3 0 7 において、情報処理装置 1 0 1 の C P U 2 0 1 は、送信ボタンの押下を受け付け、押下されたと判定した場合は図 1 3 のユーザ登録確認画面表示処理を終了

10

20

30

40

50

し、ステップS 4 1 1にてサーバ1 0 2に部分暗号化済ユーザ情報を送信する。押下されていないと判定した場合はステップS 1 3 0 2に戻る。

【0 1 0 9】

なお、本実施形態においては、画面に表示するスクリプト言語の例としてHTMLを挙げたが、これに限定するものではなく、その他の表示言語、表示方法を用いてもよい。

以上で、図1 3のユーザ登録確認画面表示処理の説明を終了する。

【0 1 1 0】

これにより、サーバ1 0 2に部分暗号化済ユーザ情報を送信する時点で、チェックボックスがON状態のユーザ情報の入力値を暗号化してユーザ登録確認画面に表示しているため、ユーザ情報が暗号化された状態でサーバに送信されたことをユーザが識別できるため、安心してユーザ情報の登録を行うことができる。つまり、システムを利用する心理的なハードルを下げることができる、

【0 1 1 1】

以上のように、前述した実施形態の機能を実現するプログラムを記録した記録媒体を、システムあるいは装置に供給し、そのシステムあるいは装置のコンピュータ（またはCPUやMPU）が記録媒体に格納されたプログラムを読み出し、実行することによっても本発明の目的が達成されることは言うまでもない。

【0 1 1 2】

この場合、記録媒体から読み出されたプログラム自体が本発明の新規な機能を実現することになり、そのプログラムを記録した記録媒体は本発明を構成することになる。

【0 1 1 3】

プログラムを供給するための記録媒体としては、例えば、フレキシブルディスク、ハードディスク、光ディスク、光磁気ディスク、CD-ROM、CD-R、DVD-ROM、磁気テープ、不揮発性のメモ리카ード、ROM、EEPROM、シリコンディスク等を用いることが出来る。

【0 1 1 4】

また、コンピュータが読み出したプログラムを実行することにより、前述した実施形態の機能が実現されるだけでなく、そのプログラムの指示に基づき、コンピュータ上で稼働しているOS（オペレーティングシステム）等が実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【0 1 1 5】

さらに、記録媒体から読み出されたプログラムが、コンピュータに挿入された機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに書き込まれた後、そのプログラムコードの指示に基づき、その機能拡張ボードや機能拡張ユニットに備わるCPU等が実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【0 1 1 6】

また、本発明は、複数の機器から構成されるシステムに適用しても、ひとつの機器から成る装置に適用しても良い。また、本発明は、システムあるいは装置にプログラムを供給することによって達成される場合にも適用できることは言うまでもない。この場合、本発明を達成するためのプログラムを格納した記録媒体を該システムあるいは装置に読み出すことによって、そのシステムあるいは装置が、本発明の効果を享受することが可能となる。

【0 1 1 7】

上記プログラムの形態は、オブジェクトコード、インタプリタにより実行されるプログラムコード、OS（オペレーティングシステム）に供給されるスクリプトデータ等の形態から成ってもよい。

【0 1 1 8】

さらに、本発明を達成するためのプログラムをネットワーク上のサーバ、データベース

10

20

30

40

50

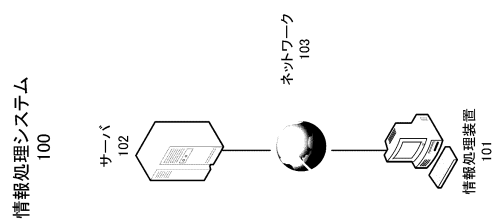
等から通信プログラムによりダウンロードして読み出すことによって、そのシステムあるいは装置が、本発明の効果を享受することが可能となる。なお、上述した各実施形態およびその変形例を組み合わせた構成も全て本発明に含まれるものである。

【符号の説明】

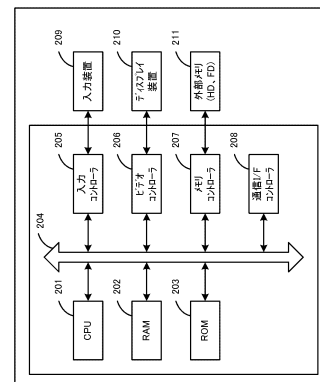
【 0 1 1 9 】

- 1 0 0 情報処理システム
- 1 0 1 情報処理装置
- 1 0 2 サーバ
- 1 0 3 ネットワーク

【 図 1 】

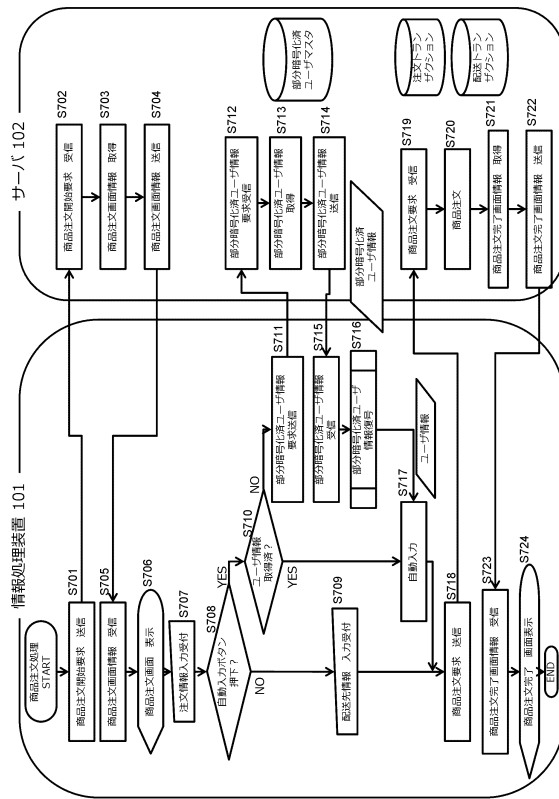


【 図 2 】

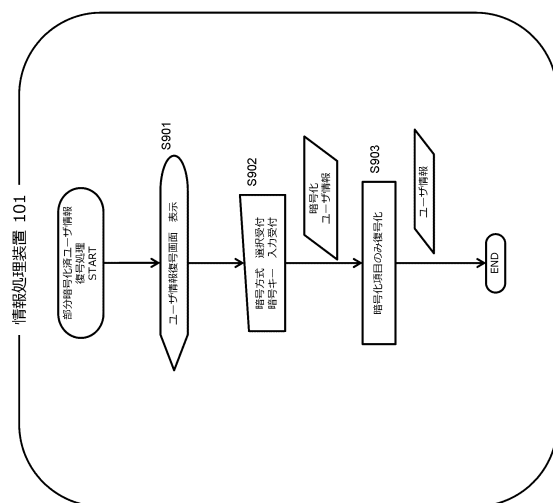




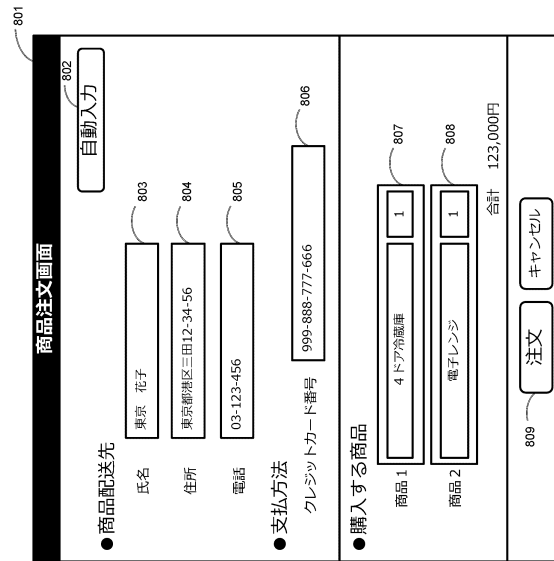
【 図 7 】



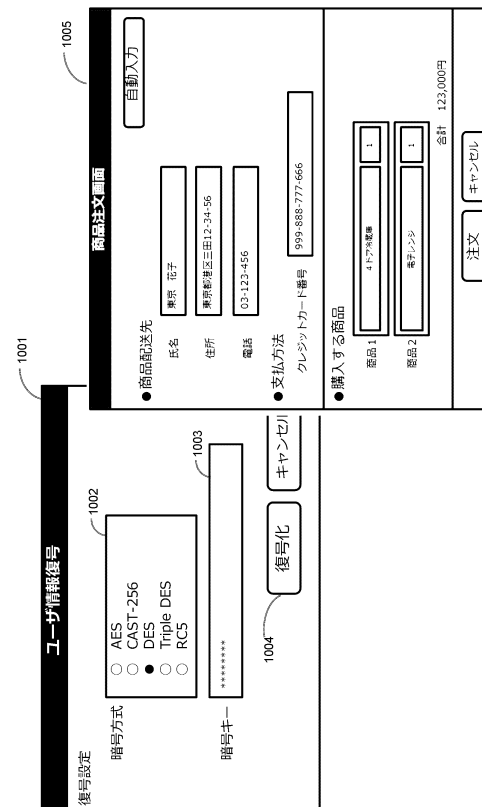
【 図 9 】



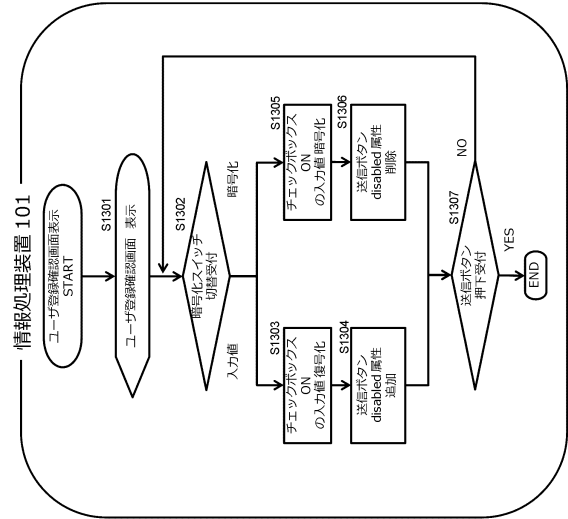
【 図 8 】



【 図 1 0 】



【図 1 3】



【図 1 1】

部分暗号化済ユーザマスタ 1110					
ユーザID	パスワード	氏名	性別	生年月日	住所
user123	*****	Odsgew8807#09J	女	1982/01/02	Popewf9((r2#dwiswec7c4faf
		SXW'dscs			Far
		w5			
クレジットカード 暗号化項目					
				電話番号	メール
				8902#4221(E")	tokkyo@test.co.jp
				Hjidsjdsa#(8	

マスケディング情報マスタ 1120

ユーザID	氏名	性別	生年月日	住所	電話番号	メール
user123		女	30代前半			tokkyo@test.co.jp

注文ランザクション 1130

注文ID	商品コード	ユーザID	注文日時	支払	配送番号
200356	H001	user123	2012/01/05/02:30:12	済	0085
301023	X8/C1	user123	2012/03/21/01:10:12	済	0111
301023	H0K03T	user123	2012/03/21/01:10:12	済	0111

配送ランザクション 1140

配送番号	配送先氏名	配送先住所	配送先電話番号
0111	東京 花子	東京都港区三田12-34-56	03-123-456

【図 1 4】

ユーザ登録画面 1401

ユーザID user123

パスワード \*\*\*\*\*

氏名 東京 花子

性別 男

住所 東京都港区三田12-34-56

生年月日 1982/01/02

電話番号 03-123-456

メール tokkyo@test.co.jp

クレジットカード番号 99988877666

暗号化 1402

ユーザ登録確認画面 1420

ユーザID user123

入力値

ユーザ情報は以下の状態で登録されます。

氏名 Odsgew8807#409SXW'dscsW5

性別 女

住所 Popewf9((r2#dwiswec7c4faf

電話番号 584'g9hUD'g"

生年月日 1982/01/02

メール tokkyo@test.co.jp

クレジットカード番号 8902#4221(E")Hjidsjdsa#(8

送信 1423

ユーザ登録確認画面 1430

ユーザID user123

入力値

ユーザ情報は以下の状態で入力されました。

氏名 東京 花子

性別 女

住所 東京都港区三田12-34-56

電話番号 03-123-456

生年月日 1982/01/02

メール tokkyo@test.co.jp

クレジットカード番号 99988877666

送信 1433

暗号方式

AFS

CST-256

D5S

Triple DES

RCS

暗号キー \*\*\*\*\*

登録 キャンセル

【 図 1 5 】

デフォルト暗号マスク 1500

ユーザID		氏名	性別	生年月日	住所	電話番号	メール	クレジットカード番号
—		▲	△	△	■	■	□	▲

---

フロントページの続き

(56)参考文献 特開2003-324430(JP,A)  
特開2005-151030(JP,A)  
特開2005-111083(JP,A)  
特開2002-351995(JP,A)  
米国特許出願公開第2014/0208418(US,A1)  
特開2001-147978(JP,A)  
特開2014-081744(JP,A)

(58)調査した分野(Int.Cl., DB名)  
G06F 21/60-62