(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2009-163384
(P2009-163384A)
(43)公開日　平成21年7月23日(2009.7.23)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/20	(2006.01)	G06F	15/00	330G	5B285
H04L 9/32	(2006.01)	H04L	9/00	673E	5J104

審査請求 未請求　請求項の数 5　ＯＬ　（全 16 頁）

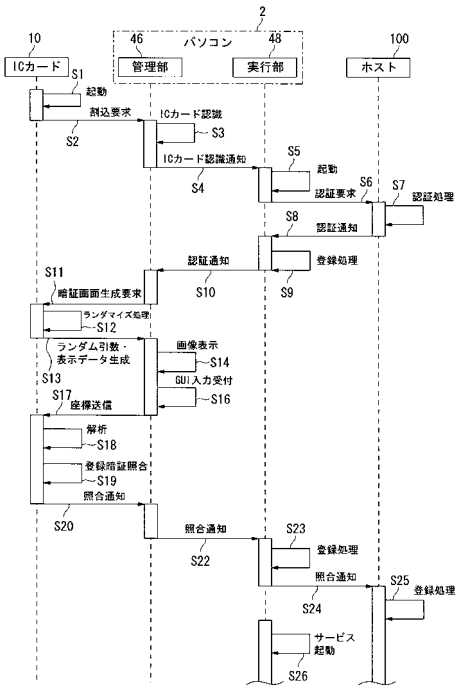
(21)出願番号　特願2007-340684 (P2007-340684)
(22)出願日　平成19年12月28日 (2007.12.28)

(71)出願人　000162113
共同印刷株式会社
東京都文京区小石川４丁目１４番１２号
(74)代理人　100120592
弁理士　山崎　崇裕
(74)代理人　100131037
弁理士　坪井　健児
(72)発明者　茂田井　省三
東京都文京区小石川４丁目１４番１２号
共同印刷株式会社内

Ｆターム(参考)　5B285 AA01 BA03 CA41 CB02 CB04
CB07 CB64 CB75 CB76
5J104 AA07 KA01 NA36 NA38 PA07

(54)【発明の名称】データ入力システム及びデータ入力方法

(57)【要約】
【課題】インターネットバンキング等のサービスにおいて、セキュリティ情報の入力操作に関する安全性を向上する。
【解決手段】ユーザログイン時に、ＩＣカード１０に予め記憶された暗証番号の入力用の画像をランダマイズして表示用データを生成する（ステップＳ１２，Ｓ１３）パソコン２の表示画面には、表示用データに基づいて入力用の画像が表示される（ステップＳ１４）。パソコン２において、画像が表示された表示画面を通じてユーザによる入力情報の入力を受け付ける（ステップＳ１６）。パソコン２から入力情報をＩＣカード１０に送信し（ステップＳ１７）、ＩＣカード１０でこれを解析する（ステップＳ１８）。ＩＣカード１０で登録暗証との照合を行い（ステップＳ１９）、照合が成立した場合、照合通知をＩＣカード１０からパソコン２に通知する（ステップＳ２２）。
【選択図】図４



【特許請求の範囲】
【請求項１】
画像を表示する表示画面を有し、この表示画面を通じて利用者の操作入力を受け付ける機能を有した情報処理端末と、この情報処理端末とローカルに接続された状態で前記情報処理端末とは個別に機能するＩＣカードとを備えたデータ入力システムにおいて、
前記ＩＣカードは、
真正な利用者に関するセキュリティ情報を記憶する記憶部と、
前記情報処理端末の表示画面に前記セキュリティ情報の入力用の画像を表示させる表示用データを生成する生成部と、
前記情報処理端末の表示画面に表示された入力用の画像を用いて利用者により入力された入力情報を前記情報処理端末から受け取り、その入力情報を前記セキュリティ情報と照合する照合処理部と、
前記照合処理部にて前記入力情報と前記セキュリティ情報との照合が成立した場合、その旨を前記情報処理端末に通知する通知処理部と
を有することを特徴とするデータ入力システム。
【請求項２】
請求項１に記載のデータ入力システムにおいて、
前記情報処理端末は、
ネットワークを通じて所定のホストと通信可能に接続されており、前記ＩＣカードの通知処理部から前記セキュリティ情報との照合が成立した旨の通知を前記ホストに送信し、
前記ホストは、
前記ＩＣカードから前記情報処理端末を通じて前記セキュリティ情報との照合が成立した旨の通知を受けた場合、前記情報処理端末を通じて利用者からの操作入力の受け付けを開始することを特徴とするデータ入力システム。
【請求項３】
画像を表示する表示画面を有し、この表示画面を通じて利用者の操作入力を受け付ける機能を有した情報処理端末と、この情報処理端末とローカルに接続された状態で前記情報処理端末とは個別に機能するＩＣカードとを用いてデータを入力するデータ入力方法において、
前記ＩＣカードに予め記憶された真正な利用者に関するセキュリティ情報の入力用の画像を、前記情報処理端末の表示画面に表示させるための表示用データを生成するステップと、
前記表示用データに基づいて前記情報処理端末の表示画面に入力用の画像を表示するステップと、
前記情報処理端末にて、前記入力用の画像が表示された表示画面を通じて利用者による入力情報の入力を受け付けるステップと、
前記情報処理端末にて受け付けた入力情報を前記ＩＣカードに送信し、前記ＩＣカードにて前記入力情報を前記セキュリティ情報と照合するステップと、
前記入力情報と前記セキュリティ情報との照合が成立した場合、その旨を前記ＩＣカードから前記情報処理端末に通知するステップと
を有するデータ入力方法。
【請求項４】
請求項３に記載のデータ入力方法において、
前記情報処理端末にネットワークを通じて通信可能に接続されたホストに対して、前記ＩＣカードから前記セキュリティ情報との照合が成立した旨の通知を送信するステップと、
前記ＩＣカードから前記情報処理端末を通じて前記セキュリティ情報との照合が成立した旨の通知を受けると、前記ホストから前記情報処理端末を通じて利用者からの操作入力に基づく入力情報の受け付けを開始するステップと
をさらに有するデータ入力方法。

【請求項５】
請求項４に記載のデータ入力方法において、
前記ホストからネットワークを通じて提供されるサービスで使用されるサービス情報を前記ＩＣカードに予め記憶させた状態で、前記ホストから前記情報処理端末を通じて利用者からの操作入力に基づく入力情報の受け付けが開始されると、前記ＩＣカードにて、前記サービス情報に基づいて前記サービスを利用するための画像を前記情報処理端末の表示画面に表示させる表示用データを生成するステップと、
前記情報処理端末にて、前記サービスを利用するための画像を表示させた表示画面を通じて利用者による操作入力を受け付け、その入力結果を前記ＩＣカードに通知するステップと、
前記ＩＣカードに通知された入力結果に基づき、前記ＩＣカードから前記情報処理端末を通じて前記サービスを利用するためのサービス利用情報を前記ホストに送信するステップとをさらに有するデータ入力方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、例えばインターネットを通じてサービスを利用する際のセキュリティを向上したデータ入力システム及びデータ入力方法に関するものである。
【背景技術】
【０００２】
従来、インターネットを利用した銀行取引（以下では「インターネットバンキング」と呼称する。）やクレジットカード等を用いた電子商取引等において、パスワードや暗証番号等のセキュリティ情報を予めサービスの利用者に付与しておき、利用者がサービスを利用する度に、パスワードや暗証番号の入力を求めることで、利用者の真正を担保する手法が一般的に用いられている。
【０００３】
ところが近年、こうしたインターネットを通じたサービスの安全性が問題視されており、例えば、入力したセキュリティ情報がインターネット上で余所へ漏洩したり、偽造されたウェブサイトに利用者が誘導され、そこからセキュリティ情報が悪意の第三者に盗み取られたりすることで、不正にサービスを利用される被害が発生している。また、利用者がキーボード等を通じてセキュリティ情報を入力する際、そのキーストロークが不正に監視されたり、入力中の画面を不正にキャプチャされたりすることで、セキュリティ情報を盗み取られる被害も発生している。
【０００４】
このため従来、セキュリティ情報の入力操作に画像を使用するとともに、画像の配置をランダムに変更するソフトウェアキーボードを用いた先行技術が知られている（例えば、特許文献１参照。）。この先行技術の手法は、ユーザＩＤやパスワードを入力する際、ランダムに配置されたボタンイメージ（画像）をポインティングデバイスで選択して入力操作を行うものであり、ボタンイメージの配置は１つ選択される毎にランダムに変更される。また、具体的なイメージはサーバに保管されており、端末からユーザＩＤやパスワードの文字列がそのままサーバに送信されるのではなく、マウスでクリックした座標だけが送信されるものとなっている。
【０００５】
上記の先行技術によれば、第三者にキーストロークを盗まれたり、画面上の操作位置からセキュリティ情報が推測されたりすることを防止することができるし、また、たとえネットワーク経由で情報が漏れたとしても、送信情報には座標しか含まれていないため、直ちにセキュリティ情報が盗み取られることはないと考えられる。
【特許文献１】特開２００４－１０２４６０号公報
【発明の開示】
【発明が解決しようとする課題】

【０００６】
しかしながら、先行技術の手法では依然としてセキュリティ情報の入力操作を反映した情報（座標）がネットワーク上に送信されていることに変わりはなく、座標を解析することでセキュリティ情報が割り出されてしまう危険性がある。また、膨大な数の利用者のセキュリティ情報をサーバで登録しているため、サーバの管理負担が過度に大きくなるという問題もある。
【０００７】
そこで本発明はセキュリティ情報の入力操作に関して、より安全性を向上することができる技術の提供を課題としている。
【課題を解決するための手段】
【０００８】
第１に本発明は、セキュリティ情報をネットワーク上でやりとりすることなく、セキュアな入力環境を構築することができるデータ入力システムを提供する。また第２に本発明は、セキュアな入力環境の下でサービスを提供することができるデータ入力方法を提供する。
【０００９】
本発明のデータ入力システムは、情報処理端末及びＩＣカードを備えた構成である。情報処理端末は画像を表示する表示画面を有しており、この表示画面を通じて利用者の操作入力を受け付ける機能を有している。またＩＣカードは、情報処理端末とローカルに接続された状態で情報処理端末とは個別に機能する。
【００１０】
その上でＩＣカードは、その機能要素として記憶部、生成部、照合処理部及び通知処理部を有する。このうち記憶部は、真正な利用者に関するセキュリティ情報を予め記憶する。また生成部は、情報処理端末の表示画面にセキュリティ情報の入力用の画像を表示させる表示用データを生成する機能を有している。照合処理部は、情報処理端末の表示画面に表示された入力用の画像を用いて利用者により入力された入力情報を情報処理端末から受け取り、その入力情報をセキュリティ情報と照合する機能を有する。そして通知処理部は、照合処理部にて入力情報とセキュリティ情報との照合が成立した場合、その旨を情報処理端末に通知するものである。
【００１１】
上記のように本発明のデータ入力システムは、真正な利用者に関するセキュリティ情報を予めＩＣカードに記憶させておき、その照合をＩＣカードの内部で行う構成である。システムにおいて情報処理端末は、ＩＣカードで生成された表示用データに基づいて入力用の画像を表示したり、その表示画面を通じて受け付けた入力情報をＩＣカードに提供するツールとして機能する。情報処理端末とＩＣカードとはローカルに接続されており、両者のやりとりがネットワーク上を通ることはない。またＩＣカードは、照合を行う際にも終始セキュリティ情報を内部で保持しており、これを情報処理端末に通知することはない。このため、セキュリティ情報はもとより、利用者が行った入力情報がネットワーク上に流出することはない。
【００１２】
本発明のデータ入力システムによれば、ＩＣカードにおいて照合が成立すると、それによって入力操作を行ったシステムの利用者の真正を担保することができる。すなわち、セキュリティ情報は利用者のみが知り得るもの（ＩＤ、パスワード、暗証番号等）であるから、これを知り得ない第三者がシステムを利用しようとしても、ＩＣカードにおいて照合が成立しない。この場合、ＩＣカードから情報処理端末に対して照合の成立が通知されず、それ以上システムは稼働しない。
【００１３】
一方、ＩＣカードにおいて照合が成立した場合、それによってシステムの利用者が真正であることを確認できているため、システムはその後のサービスの利用を可能とする。すなわち、情報処理端末は、ネットワークを通じて所定のホストと通信可能に接続されてお

り、ＩＣカードの通知処理部からセキュリティ情報との照合が成立した旨の通知をホストに送信する。そして、システムにおいてサービスを提供するホストは、ＩＣカードから情報処理端末を通じてセキュリティ情報との照合が成立した旨の通知を受けた場合、情報処理端末を通じて利用者からの操作入力に基づく入力情報の受け付けを開始する。これにより、利用者はホストから提供される各種のサービス（例えば、インターネットを通じた金融取引、電子商取引等）を利用することができる。

【００１４】

システムの稼働に際し、ホストは膨大なセキュリティ情報を保有しておく必要がなく、セキュリティ情報は利用者が管理（所持）するＩＣカード内に保存されている。このため、膨大な数の利用者を相手にするサービスに本発明のシステムを適用した場合であっても、ホストの管理負担が過大になることはない。また、１箇所のホストから膨大なセキュリティ情報が流出するおそれがないので、金融取引や電子商取引等の秘匿性の高いサービスの提供に極めて好適である。

【００１５】

本発明のデータ入力方法は、上記のシステムの動作により実現されるセキュアなデータ入力方法である。特にＩＣカードにおいて照合が成立した場合、以下の手順を実行することで利用者の利便性を向上することができる。

【００１６】

（１）ホストからネットワークを通じて提供されるサービスにおいて使用されるサービス情報をＩＣカードに予め記憶させておく。そして、ホストから情報処理端末を通じて利用者からの操作入力に基づく入力情報の受け付けが開始されると、ＩＣカードがサービス情報に基づいてサービスを利用するための画像を情報処理端末の表示画面に表示させる表示用データを生成する。

【００１７】

（２）情報処理端末は、生成された表示用データを用いて表示画面にサービスを利用するための画像を表示し、この表示画面を通じて利用者による操作入力を受け付け、その入力結果をＩＣカードに通知する。

【００１８】

（３）ＩＣカードは、情報処理端末から通知された入力結果に基づき、情報処理端末を通じてサービスを利用するためのサービス利用情報をホストに送信する。これを受けてホストがサービスメニューを実行し、その利用結果を情報処理端末に通知する。

【００１９】

本発明のデータ入力方法によれば、サービス情報が予めＩＣカードに記憶されているため、これをホストからネットワーク経由で送信する必要がない。サービス情報は例えば、金融取引における振込先の口座情報であったり、振込先の金融機関やその支店名（番号）、預金種目、口座番号、口座名義等を指定するための文字列情報であったり、振込金額を指定するための数字情報であったりする。

【００２０】

このようなサービス情報は予めＩＣカードに記憶されているが、ＩＣカードはそのソースを外部に流出させることはない。すなわち、情報処理端末にはサービスを利用するための画像が表示されるだけであり、ＩＣカードはその画像を表示するための表示用データを情報処理端末に提供するだけである。表示用データはサービス情報に基づいて生成されたものであるが、あくまで画像を表示するためのデータであり、そこにはサービス情報のソースとなるデータは何も含まれていない。

【００２１】

また情報処理端末では、表示画面上に表示された画像を用いた操作入力が受け付けられる。この操作入力はあくまで画像を通じて行われるものであり、そこでキーコード等を発生させる操作（キーボードの押下）が求められることはない。これにより、キーストロークの監視（キーロガー）によるサービス情報の盗み取り行為を確実に防止することができる。

【００２２】
ＩＣカードは、情報処理端末から入力結果の通知を受け取ると、自身が保有するサービス情報に照らして利用者の操作を解析し、実際にサービスを利用するためのサービス利用情報をホストに送信することができる。例えば、画像を通じて指定された振込先の情報や振込金額、実行日時等の情報を、情報処理端末を通じてホストに通知する。このときサービス利用情報がネットワーク上を通過するが、そこでのセキュリティは暗号化等の技術手段によって担保すればよい。
【発明の効果】
【００２３】
以上のように本発明によれば、一度ＩＣカードに登録したセキュリティ情報を外部に流出させることなく、真正な利用者であることの認証を行うことができるので、きわめてセキュアなデータ入力環境を実現することができる。また、本発明のデータ入力方法を実行することで、ホストからネットワークを通じて提供されるサービスを利用する際にさらなるセキュリティ環境を実現することができる。
【発明を実施するための最良の形態】
【００２４】
以下、本発明のデータ入力システム及びこれを用いて実施されるデータ入力方法の実施形態について説明する。
【００２５】
図１は、データ入力方法を実施するためのハードウェア資源となるデータ入力システムを概略的に示した図である。このデータ入力システムは、例えば各種の情報処理端末としてパーソナルコンピュータ（以下、「パソコン」と略称する。）２や携帯電話機４、携帯情報端末６の他、ＩＣカードユニット８、ネットワーク１０２及びホスト（サーバ）コンピュータ１００から構成されている。
【００２６】
〔情報処理端末〕
パソコン２や携帯電話機４、携帯情報端末６は、いずれもネットワーク１０２に接続する機能を有しており、この例ではパソコン２が有線による接続であり、その他の携帯電話機４及び携帯情報端末６はそれぞれ無線による接続が可能である。なお携帯電話機４や携帯情報端末６は、図示しない基地局を通じてネットワーク１０２に接続することができる。また、携帯電話機４や携帯情報端末６は、パソコン２と同様にマイクロコンピュータとしての機能をも有しており、それぞれ内蔵する記憶装置（メモリ）等に記憶されたアプリケーションプログラムを読み出し、これを解釈及び実行するハードウェアリソースを備えている。
【００２７】
〔ＩＣカード〕
ＩＣカードユニット８は、ＩＣカード１０及びカードソケット１２から構成されている。ＩＣカード１０は、例えばカード型の樹脂基板に半導体集積回路を埋設してパッケージした形態である。この例ではＩＣカード１０が接触式を採用しているため、その外面には接点（電極板）が露出しているが、ＩＣカード１０は非接触式であってもよい。
【００２８】
カードソケット１２は、ＩＣカード１０をパソコン２や携帯電話機４、携帯情報端末６に接続するためのアダプタである。カードソケット１２はＩＣカード１０の挿入口を有しており、この挿入口内にＩＣカード１０を挿入した状態で、内蔵したコンタクトピンをＩＣカード１０の接点に接触させることができる。カードソケット１２にはＩＣカード１０とパソコン２等との間の通信を中継する中継回路が実装されており、パソコン２等はカードソケット１２を介してＩＣカード１０との通信を行うことができる。この例では、カードソケット１２に汎用の規格（例えばＵＳＢ）に合致したコネクタを採用している。なお、パソコン２や携帯電話機４、携帯情報端末６にＩＣカード１０そのものの規格に合致した挿入口が予め内蔵されている場合、特にカードソケット１２を用いる必要はない。この

場合、ＩＣカード１０を直接パソコン２等に接続して通信を行うことができる。
【００２９】
〔ネットワーク〕
ネットワーク１０２は一般的な電気通信回線であり、本実施形態では例えばインターネットを想定している。ただしネットワーク１０２は、電話回線や長距離間にわたって敷設された専用ネットワーク等であってもよい。
【００３０】
〔ホスト〕
またネットワーク１０２には、ホストコンピュータ（以下「ホスト」と呼称する。）１００が接続されている。ホスト１００はネットワーク１０２を経由して、パソコン２や携帯電話機４、携帯情報端末６等との間でデータ通信を行う機能を有するほか、サーバコンピュータとして利用者にサービスを提供する機能をも有する。
【００３１】
図２は、ＩＣカード１０、パソコン２等のハードウェア上の構成を概略的に示す図である。以下、それぞれについて説明する。
【００３２】
ＩＣカード１０は、例えば中央処理装置であるＣＰＵ１４をはじめ、ＲＡＭ１６やＥＥＰＲＯＭ１８の半導体メモリ、Ｉ／Ｏ（入出力ドライバ）２０等を高密度に集積した構造である。なおＩＣカード１０は、接続先のパソコン２等から電力の供給を受けて動作することができる。
【００３３】
図２には、各種の情報処理端末のうちパソコン２のハードウェア構成が例として示されている。パソコン２もまた中央処理装置であるＣＰＵ３０をはじめ、ＲＯＭ３２やＲＡＭ３４等のメモリデバイス、Ｉ／Ｏ３６等を有している。なおパソコン２の場合、これらリソースは例えばチップの形態でマザーボード上に実装されている。またパソコン２には、例えば液晶ディスプレイのような表示装置５０が接続されている。表示装置５０の表示画面には、パソコン２による各種のプログラム（ＯＳ、アプリケーション）の実行に伴う出力結果が表示される。
【００３４】
またパソコン２はＧＵＩ（グラフィカルユーザインタフェース）３８を有しており、合わせてパソコン２にはポインティングデバイス５２が接続（又は内蔵）されている。ポインティングデバイス５２を用いた使用者の操作入力は、ＧＵＩ３８によって受け付けられる。ポインティングデバイス５２は、例えばマウス、タッチパッド、トラックボール、ポインティングスティック等である。携帯電話機４や携帯情報端末６にＧＵＩ３８が搭載されていない場合、その機能は例えば方向キー、タッチパネル等の入力デバイスによって代用することができる。
【００３５】
〔ＩＣカードの機能〕
図３は、ＩＣカード１０において動作するプログラムや記憶情報等の構成例を示すブロック図である。ＩＣカード１０の内蔵メモリ（ＥＥＰＲＯＭ１８）には、データ入力システムにおいて動作するためのプログラム４２が組み込まれている。プログラム４２は各種のプログラムモジュール（サブルーチン）から構成されており、この例では各種のプログラムモジュールとして、画像データ生成部４２ａ、座標解析部４２ｂ、照合処理部４２ｃ、通知処理部４２ｄ等が含まれている。個々のプログラムモジュールは、ＩＣカード１０のＣＰＵ１４がプログラム４２を実行する中で、必要に応じて実行される。なお、具体的な処理シーケンスについては後述する。
【００３６】
また内蔵メモリには、プログラム４２の実行に伴う読み出し用のデータ４４が格納されている。データ４４には使用目的に応じて区分された各種のデータモジュールが含まれており、この例では各種のデータモジュールとして、発行データ部４４ａ、登録暗証記憶部

４４ｂ、コマンド登録部４４ｃ、サービス情報記憶部４４ｄ等が含まれている。なお、各種のデータモジュールの利用形態については処理シーケンスとともに後述する。

【００３７】

次に、データ入力システムにおいて実行される処理シーケンスの詳細について説明する。また以下の説明により、データ入力システムを用いて行われるデータ入力方法の使用例が明らかとなる。

【００３８】

図４は、データ入力システムの稼働に伴う各種処理の流れを示すシーケンス図である。以下の処理シーケンスは、例えばユーザ（利用者）が個人用のパソコン２とＩＣカード１０を使用してデータ入力システムを利用する場面を想定している。なお図４では説明の便宜上、パソコン２の構成を管理部４６と実行部４８に分けて示している。このうち管理部４６は、例えばＯＳ（オペレーティングシステム）等の基本プログラムによりサポートされる機能である。また実行部４８は、ＯＳ上で動作するアプリケーション（例えばＪａｖａ（登録商標）アプリケーション）によりサポートされる機能である。その他のＩＣカード１０及びホスト１００については、それぞれ単一の構成として図示されている。以下、処理の流れに沿って説明する。

【００３９】

〔ＩＣカードの処理〕

ステップＳ１：例えば、ユーザがＩＣカード１０をパソコン２に接続すると、ＩＣカード１０に給電が開始され、ＣＰＵ１４がブート処理を行ってプログラム４２を起動する。

ステップＳ２：次に、ＩＣカード１０のＣＰＵ１４は起動後のシーケンスに従い、パソコン２に対して割込要求を発行する。

【００４０】

〔パソコンの処理〕

ステップＳ３：パソコン２は、管理部４６においてＩＣカード１０からの割込要求を受け付けると、ＩＣカード１０の認識処理を行う。

ステップＳ４：続いて管理部４６は、実行部４８に対してＩＣカード１０の認識通知を発行する。

【００４１】

ステップＳ５：認識通知が発行されると、パソコン２は実行部４８を起動する。

ステップＳ６：実行部４８が起動すると、パソコン２はホスト１００に対して認証要求を発行する。なお認証要求の発行は、ネットワーク１０２を用いた通信によって行われ、発行される電文は暗号化処理（例えばＲＳＡ）によって保護されている。

【００４２】

〔ホストの処理〕

ステップＳ７：パソコン２からの認証要求を受けると、ホスト１００は認証処理を実行する。具体的には、ホスト１００は受け取った電文を復号化し、データ入力システム上の正規の認証要求であることを確認する。

ステップＳ８：認証に成功すると、ホスト１００はユーザのパソコン２に対して認証通知を送信する。このときの送信電文もまた、暗号化処理によって保護されている。

【００４３】

〔パソコンの処理〕

ステップＳ９：パソコン２の実行部４８は、ホスト１００からの認証通知を受け取ると、これを復号化し、正規のホスト１００から発行された認証通知を登録する。これにより、パソコン２とホスト１００との間で相互認証が成立する。

ステップＳ１０：また相互認証が成立すると、実行部４８から管理部４６に認証通知を発行する。この認証通知には、ＩＣカード１０に対する要求電文のコードが含まれている。

【００４４】

ステップＳ１１：そしてパソコン２の管理部４６は、実行部４８が発行した認証通知に

含まれる要求電文コードに基づき、ＩＣカード１０に対して暗証画面生成要求を発行する。この例では、管理部４６がＩＣカード１０との通信をサポートし、実行部４８がホスト１００との通信をサポートする構成であるが、特にこのような構成に限るものではない。

【００４５】

〔ＩＣカードの処理〕

ステップＳ１２：ＩＣカード１０のＣＰＵ１４は暗証画面生成要求を受け取ると、これに応じてランダマイズ処理を実行する。ランダマイズ処理では例えば、ＣＰＵ１４において一定の割込周期で複数種類のソフトウェア乱数を発生させておき、そこからいくつか（例えば３つ）の乱数を取得する。

【００４６】

ステップＳ１３：そしてＣＰＵ１４は、取得した乱数を連結してランダム引数を生成する。またＣＰＵ１４は、上記の画像データ生成部４２ａの処理を通じてランダム引数から表示用データを生成する。生成を終えると、ＣＰＵ１４はランダム引数及び表示用データをパソコン２に通知する。なお、ランダム引数や表示用データの例については別の図面を参照しながら後述する。

【００４７】

〔パソコンの処理〕

ステップＳ１４：パソコン２の管理部４６は、受け取ったランダム引数及び表示用データに基づき、表示装置５０に入力用の画像を表示する。これによりユーザは、ポインティングデバイス５２を用いた操作入力が可能な状態となる。

【００４８】

ステップＳ１６：そしてパソコン２の管理部４６は、ＧＵＩ３８にてユーザの操作入力を受け付ける。この間、ユーザが例えばマウスのクリック操作によって表示画面上で画像（暗証番号の入力用画像）を指定すると、その指定した座標データがＲＡＭ３４に保存される。なお、画像の指定や座標データの例についても別の図面を参照しながら後述する。

【００４９】

ステップＳ１７：ユーザの操作入力が完了すると、パソコン２の管理部４６は、保存した座標データをＩＣカード１０に送信する。

【００５０】

〔ＩＣカードの処理〕

ステップＳ１８：ＩＣカード１０のＣＰＵ１４は、上記の座標解析部４２ｂの処理を通じて受け取った座標データを解析する。座標データを解析することで、ユーザが指定した暗証番号を特定することができる。

【００５１】

ステップＳ１９：ユーザが指定した暗証番号を特定すると、ＩＣカード１０のＣＰＵ１４は上記の照合処理部４２ｃの処理を通じて、登録暗証記憶部４４ｂに登録されている暗証番号との照合処理を行う。例えば２つの暗証番号を減算し、その結果が０であったか否かを確認する。

【００５２】

ステップＳ２０：照合が成立すると、ＩＣカード１０のＣＰＵ１４は通知処理部４２ｄでの処理を通じて、パソコン２に照合が成立した旨を表す照合通知を発行する。なお照合通知の電文内容は、例えば上記の発行データ部４４ａに予め登録されている。

【００５３】

〔パソコンの処理〕

ステップＳ２２：ＩＣカード１０から照合通知を受け取ると、パソコン２の管理部４６はこれを実行部４８に転送する。

ステップＳ２３：パソコン２の実行部４８は照合通知の登録処理を行う。この登録処理では、例えば現在のユーザが真正であることを表すステータスフラグがＲＡＭ３４に保存される。

【００５４】

ステップＳ２４：登録処理が完了すると、パソコン２の実行部４８はＩＣカード１０から受け取った照合通知をホスト１００に送信する。この送信電文には、照合が成立した旨のステータスを表すコードのみが含まれており、暗証番号や座標データを表すコードは一切含まれていない。なお、ここでも送信電文は暗号化処理によって保護されている。

【００５５】

〔ホストの処理〕

ステップＳ２５：照合通知を受け取ると、ホスト１００は照合通知の登録処理を実行する。この登録処理により、現在のユーザが真正であることを表すステータスがホスト１００においても登録される。またこれ以降、ホスト１００においてパソコン２を用いたユーザの操作入力に基づく入力情報の受け付けが開始される。

【００５６】

〔パソコンの処理〕

ステップＳ２６：パソコン２の実行部４８は、データ入力システムにおいて利用可能なサービス（サービス用アプリケーション）を起動する。これにより、以降はユーザが実際にホスト１００が提供しているサービスをパソコン２上で利用可能となる。

【００５７】

図５は、上記の処理シーケンスにおいて生成されるランダム引数、表示用データ、及び実際に表示される画像の例をそれぞれ示す図である。

【００５８】

〔ランダム引数〕

図５中（Ａ）：暗証照合時のランダム引数は、例えば３次元データ（ｘ，ｙ，ｚ）の形式で生成することができる。ランダム引数を例えば３バイトで記述する場合、先頭から上位２バイトの引数（ｘ，ｙ）は表示画面上での座標を表している。また下位１バイトの引数（ｚ）は、例えば０から９までのサイクリック数列のうち、先頭に位置する値（先頭値）に対応している。

【００５９】

〔表示用データ〕

図５中（Ｂ）：上記のランダム引数から生成された表示用データの構造例である。表示用データは、引数（ｚ）で表される先頭値に対応する画像（「６」の画像）を配列の先頭に位置付け、そこに続けて「７」，「８」，「９」，「０」，「１」，「２」，「３」，「４」，「５」の画像を順番に配列したものである。個々の画像（例えば「６」の画像）は、表示画面を座標で分割したときの単位領域（１コマ）に相当するサイズを有している。

【００６０】

〔入力用の画像〕

図５中（Ｃ）：上記の表示用データに基づいて、パソコン２の表示画面に表示される入力用の画像例である。この例では、表示画面（ウィンドウ等の表示領域）を縦方向に１１個、横方向に１６個の単位領域（１１×１６コマ）に分割し、画像の表示位置を縦方向に０～１０、横方向に１～１６の座標値で表している。上記のランダム引数（３，５，６）及び表示用データに基づいて画像を表示した場合、座標（３，５）の位置を先頭として、図５中（Ｂ）に示される表示用データが画面内に表示される（図４中のステップＳ１４）。

【００６１】

その他に、この例では操作入力の利便のため、例えば表示画面の右下位置に入力行の画像が表示されており、さらに表示画面の下部領域に「ＯＫ」や「キャンセル」等のボタン画像が表示されている。

【００６２】

〔ユーザの操作入力例〕

このような画像を用いてユーザが暗証番号を入力する場合、ユーザはポインティングデバイスのカーソル（図中の矢印マーク）を数字画像に合わせた状態でクリック操作を行う

。１回クリック操作を行うと、右下の入力行に「●」（又は「＊」）マークが表示されて、番号の指定が行われたことを表示する。このときパソコン２の管理部４６は、上記のように１回ごとのクリック操作に対応した座標データをＲＡＭ３４に保存する（図４中のステップＳ１６）。

【００６３】

ユーザが自己の暗証番号を全て入力すると、上記の「ＯＫ」ボタンをマウスでクリックし、操作入力を確定する。これにより、パソコン２の管理部４６から座標データがＩＣカード１０に送信される（図４中のステップＳ１７）。

【００６４】

ここで、暗証番号が例えば４桁で記述されている場合を想定する。この場合、表示画面を通じてユーザが指定した４桁の番号は、パソコン２上ではあくまで４つの座標データとして認識される。このとき４つの座標データを例えば（８，５）（４，５）（１０，５）（１２，５）とすると、これら座標データがパソコン２からＩＣカード１０に送信される。

【００６５】

〔座標の解析と照合〕

ＩＣカード１０のＣＰＵ１４は、座標解析部４２ｂの処理を通じて座標データ（８，５）（４，５）（１０，５）（１２，５）を解析し、そこから例えば「１７３５」の数列を抽出する。ＣＰＵ１４はこの数列を暗証番号として、登録されている暗証番号との照合処理を行うことができる。

【００６６】

〔サービスの利用例〕

以上の処理は、ユーザが最初にデータ入力システムの利用を開始する際の認証（ログイン）までを扱ったものである。認証完了後は、例えば以下のようにユーザによるサービスの利用が可能となる。

【００６７】

〔データ入力システムを用いた銀行振込〕

図６は、一実施形態のデータ入力システムを用いた銀行振込サービスで用いられるサービス情報、表示用データ及び表示画面の例を示す図である。

【００６８】

図６中（Ａ）：ＩＣカード１０のサービス情報記憶部４４ｄには、予めユーザが指定した振込先の口座に関するサービス情報が登録されている。サービス情報には、例えば振込先の（１）銀行番号、（２）統一店番号、（３）預金種目、（４）口座番号をそれぞれ表すコードが含まれている。ただし画面に表示する際は、これら（１）～（３）がそれぞれ銀行名、支店名、種目（普通／当座等）の画像に変換される。また（４）の口座番号は、振込先名義の画像に変換される。図示の例は、例えば５つのサービス情報を簡易的に通し番号（１～５）と口座名（Ａ口座～Ｅ口座）として示したものである。

【００６９】

図６中（Ｂ）：銀行振込サービスの処理シーケンスでは、ＩＣカード１０がランダマイズ処理において１個のランダム引数（例えば「３」）を生成する。そしてＣＰＵ１４は、生成した引数に基づいて３番目の口座名「Ｃ口座」を先頭に並べ替えた表示用データを生成する。生成された表示用データでは、通し番号が上から３，４，５，１，２の順番に変換されている。

【００７０】

図６中（Ｃ）：上記の表示用データに基づいて、パソコン２の表示画面に表示される入力用の画像例である。この例では、座標（２，４）の位置を先頭として、図６中（Ｂ）に示される表示用データに基づいて振込先の口座一覧を表す画像が表示されている。表示用データでは通し番号と口座名で表されていたが、実際の画像は支店名（ａ支店～ｄ支店）とそれぞれの口座名義を表すものとなっている。また、合わせて口座一覧の上方には銀行名を表すの画像が表示されており、さらに表示画面の下部領域に「ＯＫ」や「キャンセル

」等のボタン画像が表示されている。
【００７１】
〔ユーザの操作入力例〕
このような画像を用いてユーザが銀行振込サービスを利用する場合、ユーザはポインティングデバイスのカーソル（図中の矢印マーク）を振込先の口座名の行に合わせた状態でクリック操作を行う。クリック操作を行うと、指定された口座名の画像が反転表示（又は強調表示）されて、振込先の指定が行われたことを表示する。このときパソコン２の管理部４６は、クリック操作に対応した座標データをＲＡＭ３４に保存する。
【００７２】
ユーザが振込先の指定を確認すると、「ＯＫ」ボタンをマウスでクリックし、操作入力を確定する。これにより、パソコン２の管理部４６から座標データがＩＣカード１０に送信される。
【００７３】
ここでもユーザが指定した振込先は、パソコン２上ではあくまで座標データとして認識される。このときの座標データを例えば（２，５）とすると、この座標データがパソコン２からＩＣカード１０に送信される。
【００７４】
〔座標の解析と振込先の特定〕
ＩＣカード１０のＣＰＵ１４は、座標解析部４２ｂの処理を通じて座標データ（２，５）を解析し、そこから通し番号「４」を抽出する。ＣＰＵ１４はこの通し番号に対応するサービス情報を検索し、登録されている（１）銀行番号、（２）統一店番号、（３）預金種目、（４）口座番号のコードを特定することができる。
【００７５】
〔振込金額の指定〕
次に図７は、振込金額を入力する処理シーケンスで生成されるランダム引数、表示用データ、及び実際に表示される画像の例をそれぞれ示す図である。
【００７６】
〔ランダム引数〕
図７中（Ａ）：振込金額入力時のランダム引数もまた、例えば３次元データ（ｘ，ｙ，ｚ）の形式で生成することができる。ランダム引数の生成ロジックは、暗証照合時に説明したものと同様である。
【００７７】
〔表示用データ〕
図７中（Ｂ）：ランダム引数から生成された表示用データの構造例である。この例ではランダム引数（４，４，３）に基づき、表示用データは引数（ｚ）に対応する「３」の画像を先頭にして、そこから「４」，「５」，「６」，「７」，「８」，「９」，「０」，「１」，「２」の画像が順番に配列された構造となっている。
【００７８】
〔入力用の画像〕
図７中（Ｃ）：上記の表示用データに基づいて、パソコン２の表示画面に表示される入力用の画像例である。画像の表示形態は上記の暗証照合時と同じである。
【００７９】
〔ユーザの操作入力例〕
このような画像を用いてユーザが振込金額を入力する場合、ユーザはポインティングデバイスのカーソル（図中の矢印マーク）を数字画像に合わせた状態でクリック操作を行う。１回クリック操作を行うと、右下の入力行に対応する数値が表示される。なおパソコン２の管理部４６は、数値の表示と合わせて１回ごとのクリック操作に対応した座標データをＲＡＭ３４に保存する。
【００８０】
ユーザが振込金額を正しく入力すると、「ＯＫ」ボタンをマウスでクリックし、操作入

力を確定する。これにより、パソコン２の管理部４６から座標データがＩＣカード１０に送信される。

【００８１】

〔座標の解析と照合〕

座標データを例えば（１２，４）（１１，４）（１１，４）（１１，４）（１１，４）とすると、ＩＣカード１０のＣＰＵ１４は、座標解析部４２ｂの処理を通じて座標データを解析し、そこから例えば「１００００」の数値を抽出する。ＣＰＵ１４はこの数値を振込金額として、上記の振込先の口座情報と合わせて振込電文を生成する。生成した振込電文は、ＩＣカード１０からパソコン２を通じてホスト１００に送信される。なお、ここでも振込電文が暗号化処理により保護されている。

【００８２】

〔サービスの実行〕

ホスト１００は、受信した振込電文を解析し、ユーザの指定した入力情報を正規に受け付ける。これを受けて、ホスト１００は実際に銀行振込サービスの実行処理を行う。

【００８３】

〔その他の表示例〕

図８は、その他の表示例として、暗証番号を照合する処理シーケンスにおいて生成されるランダム引数、表示用データ、及び実際に表示される画像の別例をそれぞれ示す図である。

【００８４】

〔ランダム引数〕

図８中（Ａ）：この場合のランダム引数は、例えば４次データ（ｘ，ｙ，ｚ，α）の形式で生成することができる。ランダム引数（ｘ，ｙ，ｚ）は上記と同様であるが、最下位１バイトの引数（α）は、例えばマトリクス配列形式を表すパラメータに対応している。すなわち、引数（α）に「１」が記述されていた場合、それは表示用データ（数字の画像）をマトリクス状に配列することを意味する。

【００８５】

〔表示用データ〕

図８中（Ｂ）：上記のランダム引数から生成された表示用データの構造例である。表示用データは、引数（ｚ）で表される先頭値に対応する画像（「６」の画像）を配列の先頭に位置付け、そこに続けて「７」，「８」，「９」，「０」，「１」，「２」，「３」，「４」，「５」の画像を順番に配列したものである。ただし図５の例と違って、画像の配列が３列×４行のマトリクス状に変換されている。

【００８６】

〔入力用の画像〕

図８中（Ｃ）：上記の表示用データに基づいて、パソコン２の表示画面に表示される入力用の画像例である。ランダム引数（３，５，６，１）及び表示用データに基づいて画像を表示した場合、座標（３，５）の位置を先頭として、図６中（Ｂ）に示されるマトリクス配列の表示用データが画面内に表示される。なお、この後のユーザの操作入力例や座標の解析、登録暗証との照合については上記と同様である。

【００８７】

以上のように本実施形態のデータ入力システムによれば、サービス提供者と契約した真正なユーザのみが知り得るセキュリティ情報が全てＩＣカード１０の内部に登録されており、そこから外部にセキュリティ情報が流出することがない。このため、ネットワーク１０２上でセキュリティ情報が漏洩する心配は皆無であり、極めてセキュアな環境を構築することができる。また、データ入力システムを用いて実現されるデータ入力方法を適用することで、ホスト１００からのサービスをセキュアな環境の下で提供することができる。

【００８８】

本発明は上述した実施形態に制約されることなく、種々に変形して実施することができる。一実施形態では金融機関が提供するインターネットバンキングを例に挙げているが、

本発明のデータ入力システム及びデータ入力方法は、例えばクレジットカードの発行主体が提供する電子商取引（インターネット決済）にも適用することができる。

【００８９】

また、一実施形態では小型のＩＣカードを一例として挙げているが、ＩＣカードはクレジットカードや銀行キャッシュカード等と同じサイズの形態であってもよい。

【図面の簡単な説明】

【００９０】

【図１】データ入力方法を実施するためのハードウェア資源となるデータ入力システムを概略的に示した図である。

【図２】ＩＣカード、パソコン等のハードウェア上の構成を概略的に示す図である。

【図３】ＩＣカードにおいて動作するプログラムや記憶情報等の構成例を示すブロック図である。

【図４】データ入力システムの稼働に伴う各種処理の流れを示すシーケンス図である。

【図５】図４の処理シーケンスにおいて生成されるランダム引数、表示用データ、及び実際に表示される画像の例をそれぞれ示す図である。

【図６】データ入力システムを用いた銀行振込サービスで用いられるサービス情報、表示用データ及び表示画面の例を示す図である。

【図７】振込金額を入力する処理シーケンスで生成されるランダム引数、表示用データ、及び実際に表示される画像の例をそれぞれ示す図である。

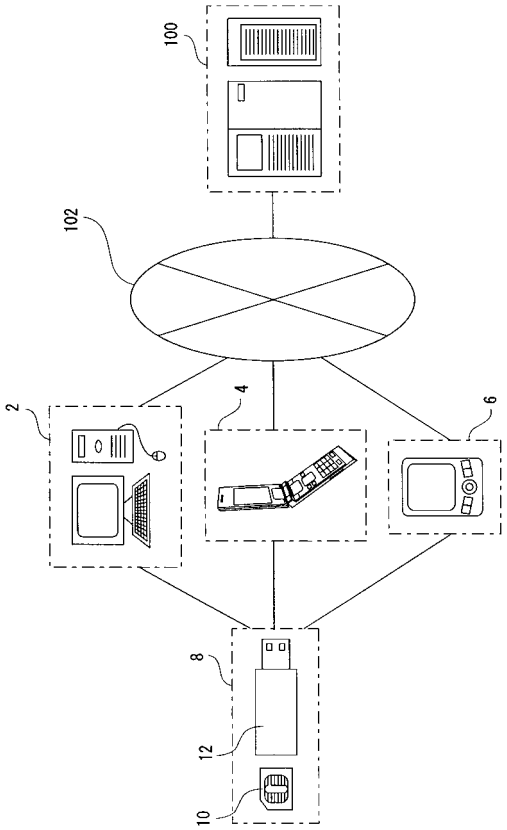
【図８】その他の表示例として、暗証番号を照合する処理シーケンスにおいて生成されるランダム引数、表示用データ、及び実際に表示される画像の別例をそれぞれ示す図である。

【符号の説明】

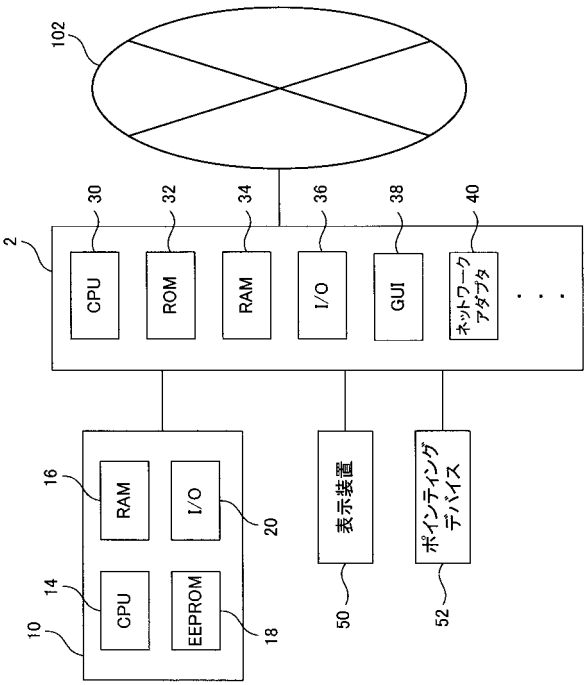
【００９１】

２　パソコン
４　携帯電話機
６　携帯情報端末
１０　ＩＣカード
１２　カードソケット
１４　ＣＰＵ
１６　ＲＡＭ
１８　ＥＥＰＲＯＭ
３８　ＧＵＩ
４２　プログラム
４２ａ　画像データ生成部
４２ｂ　座標解析部
４２ｃ　照合処理部
４２ｄ　通知処理部
４４　データ
４４ａ　発行データ部
４４ｂ　登録暗証記憶部
４４ｃ　コマンド登録部
４４ｄ　サービス情報登録部
５０　表示装置
５２　ポインティングデバイス
１００　ホスト
１０２　ネットワーク

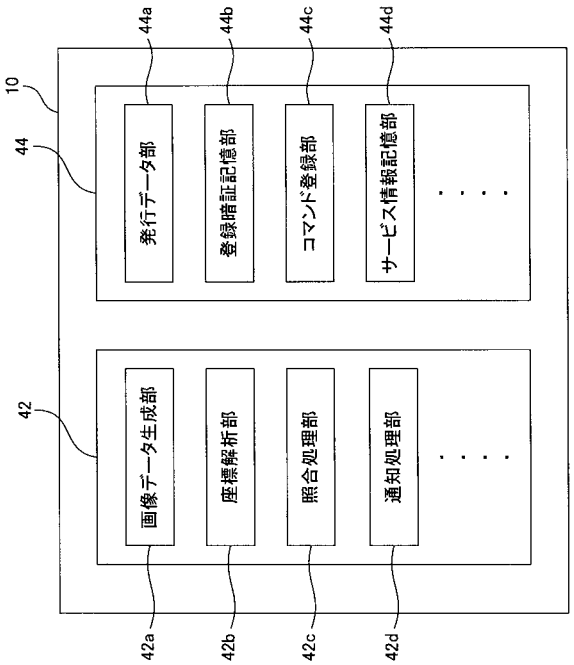
【図１】


100
102
2
4
6
8
12
10

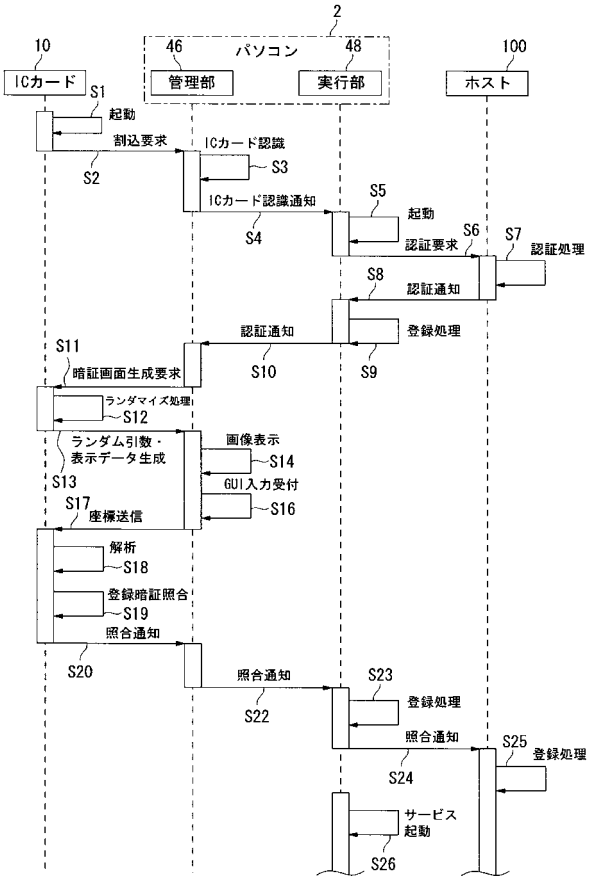
【図２】


102
30
32
34
36
38
40
2
CPU
ROM
RAM
I/O
GUI
ネットワークアダプタ
16
RAM
I/O
20
14
CPU
EEPROM
18
10
表示装置
50
ポインティングデバイス
52

【図３】


44a
44b
44c
44d
10
44
発行データ部
登録暗証記憶部
コマンド登録部
サービス情報記憶部
42
画像データ生成部
座標解析部
照合処理部
通知処理部
42a
42b
42c
42d

【図４】


2
10
ICカード
46
管理部
パソコン
48
実行部
100
ホスト
S1
起動
割込要求
S2
ICカード認識
S3
ICカード認識通知
S4
S5
起動
認証要求
S6
S7
認証処理
S8
認証通知
登録処理
S9
認証通知
S10
S11
暗証画面生成要求
ランダマイズ処理
S12
ランダム引数・
表示データ生成
S13
画像表示
S14
GUI入力受付
S16
S17
座標送信
解析
S18
登録暗証照合
S19
照合通知
S20
照合通知
S22
S23
登録処理
照合通知
S24
S25
登録処理
サービス
起動
S26

【図５】

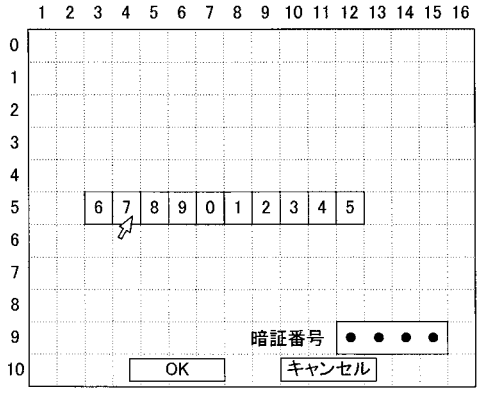
(A)

x	3
y	5
z	6

(B)

6	7	8	9	0	1	2	3	4	5

(C)



【図６】

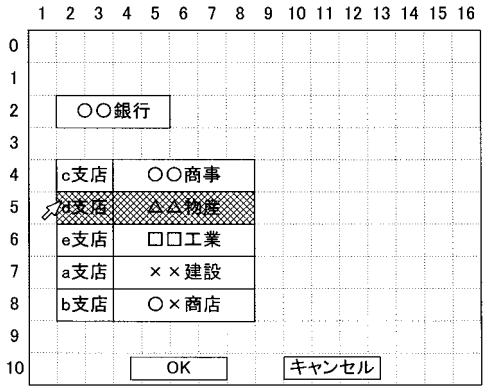
(A)

1	A口座
2	B口座
3	C口座
4	D口座
5	E口座

(B)

3	C口座
4	D口座
5	E口座
1	A口座
2	B口座

(C)



【図７】

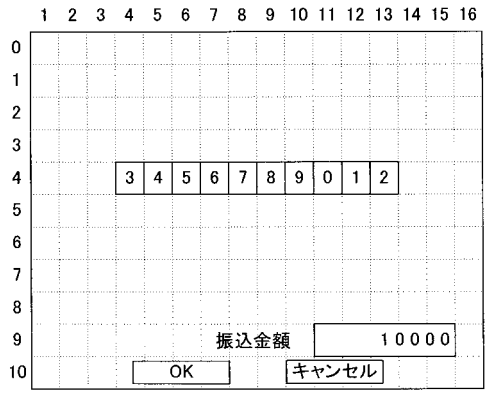
(D)

x	4
y	4
z	3

(E)

3	4	5	6	7	8	9	0	1	2

(F)



【図８】

(A)

x	3
y	5
z	6
α	β

(B)

6	7	8
9	0	1
2	3	4
5		

(C)