(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第3781874号
(P3781874)

(45)発行日　平成18年5月31日(2006.5.31)　(24)登録日　平成18年3月17日(2006.3.17)

| (51)Int.Cl. | | F I | | |
|---|---|---|---|---|
| G06F 21/24 | (2006.01) | G06F | 12/14 | 530B |
| G06F 21/20 | (2006.01) | G06F | 12/14 | 530C |
| H04L 9/08 | (2006.01) | G06F | 12/14 | 540A |
| H04L 9/32 | (2006.01) | G06F | 15/00 | 330E |
| | | H04L | 9/00 | 601E |

請求項の数 13　(全 21 頁)　最終頁に続く

(21)出願番号　特願平9-241408
(22)出願日　平成9年9月5日(1997.9.5)
(65)公開番号　特開平11-88324
(43)公開日　平成11年3月30日(1999.3.30)
審査請求日　平成12年7月7日(2000.7.7)
審判番号　不服2003-21155(P2003-21155/J1)
審判請求日　平成15年10月30日(2003.10.30)

(73)特許権者　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(74)代理人　100070150
弁理士　伊東　忠彦
(72)発明者　鹿島　一紀
東京都品川区東五反田一丁目２２番１号　株式会社富士通ソーシアルシステムエンジニアリング内
(72)発明者　松浦　正卓
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

最終頁に続く

(54)【発明の名称】画像指示による電子情報管理装置、秘密鍵管理装置及び方法、並びに、秘密鍵管理プログラムを記録した記録媒体

(57)【特許請求の範囲】

【請求項１】

画像上の位置と順序を指定する画像パスワードを利用して、秘密にされるべき電子情報を管理する電子情報管理装置において、

利用者のパスワード登録のため、画像パスワードを利用する際の複数の画像情報、および、画像上に重畳させる目の細かさが異なる複数のメッシュ情報を、画面上に表示し、その中から利用者によって選択された特定の画像情報および特定のメッシュ情報を利用者ごとに登録する画像メッシュ登録手段と、

上記選択された特定の画像およびメッシュに基づき、マウスにより指定された点列の位置及び順序情報を登録する位置順序登録手段と、

上記選択された画像上で指定された上記点列の位置及び順序の情報を暗号化キー作成式の変数に代入することにより値を算出し、該算出された値によって上記電子情報のデータを並び替えることで上記電子情報を暗号化する暗号化手段と、

上記暗号化された電子情報を記憶する電子情報記憶手段と、

利用者のパスワード利用のため、当該パスワードを利用する利用者を指定させ、指定された利用者に対して登録された前記画像情報及び前記メッシュ情報に基づいて、上記特定の画像および該画像に重畳させて特定のメッシュを表示し、上記位置順序登録手段が登録した上記点列の位置及び順序情報と同じ点列の位置及び順序の情報が指定された場合に上記暗号化された電子情報へのアクセスを許可するアクセス許可手段と、

上記アクセス許可手段によって上記アクセスを許可された暗号化された電子情報を復号

化する復号化手段
とを有することを特徴とする電子情報管理装置。
【請求項２】
上記位置情報登録手段は、画像上にマウスでクリックできる個数を受け付け、該個数分の入力順序の確認を促すボックスを表示し、画面上のクリックと連動して、ボックスを強調表示することを特徴とする請求項１記載の電子情報管理装置。
【請求項３】
上記位置情報登録手段は、上記個数を超えてクリックされた場合、または、個数未満のクリック回数で確定された場合に、警告メッセージを出力することを特徴とする請求項２記載の電子情報管理装置。
【請求項４】
上記電子情報は、電子認証局で発行される電子データである秘密鍵であることを特徴とする請求項１乃至３のうちいずれか１項記載の電子情報管理装置。
【請求項５】
上記画像メッシュ登録手段は、上記秘密鍵が記憶される記憶媒体とは別の媒体からの画像を画面上に表示することを特徴とする請求項４記載の電子情報管理装置。
【請求項６】
上記暗号化手段は、同じ点列の位置及び順序の情報を用いて複数個の秘密鍵を暗号化し、
上記アクセス許可手段は、同じ点列の位置及び順序の情報が指定された場合に、複数個の秘密鍵へのアクセスを許可する、
ことを特徴とする請求項４記載の電子情報管理装置。
【請求項７】
上記利用者から指定された利用者情報及び利用者環境情報を入力する手段を更に有し、
上記電子情報記憶手段は、上記暗号化された秘密鍵を、上記秘密鍵の利用者情報及び利用者環境情報と共に記憶する、
ことを特徴とする請求項４乃至６のうちいずれか１項記載の電子情報管理装置。
【請求項８】
上記アクセス許可手段は、上記秘密鍵へのアクセスの可否を判定する判定手段と、
利用者により指定された秘密鍵の利用者情報及び利用者環境情報を受け、上記アクセスが許可された秘密鍵の中で、上記利用者により指定された利用者情報及び利用者環境情報と共に記憶された秘密鍵を選択する秘密鍵選択手段とを有する、
ことを特徴とする請求項７記載の電子情報管理装置。
【請求項９】
画像上の位置と順序を指定する画像パスワードを利用して、秘密にされるべき電子情報を管理する電子情報管理方法において、コンピュータが、
利用者のパスワード登録のため、画像パスワードを利用する際の複数の画像情報、及び、画像上に重畳させる目の細かさが異なる複数のメッシュの情報を、画面上に表示し、その中から利用者によって選択された特定の画像情報及び特定のメッシュ情報を利用者ごとに登録する画像メッシュ登録ステップと、
上記選択された特定の画像及びメッシュに基づき、マウスにより指定された点列の位置及び順序情報を登録する位置順序登録ステップと、
利用者のパスワード利用のため、上記選択された画像上で指定された上記点列の位置及び順序の情報を暗号化キー作成式の変数に代入することにより値を算出し、該算出された値によって上記電子情報のデータを並び替えることで上記電子情報を暗号化する暗号化ステップと、
上記暗号化された電子情報を記憶する電子情報記憶ステップ
とを備えたことを特徴とする電子情報管理方法。
【請求項１０】
さらに、コンピュータが、前記パスワードを利用する利用者を指定させ、指定された利

用者に対して登録された前記画像情報及び前記メッシュ情報に基づいて、上記特定の画像および該画像に重畳させて特定のメッシュを表示し、上記位置順序登録ステップが登録した上記点列の位置及び順序情報と同じ点列の位置及び順序の情報が指定された場合に上記暗号化された電子情報へのアクセスを許可するアクセス許可ステップと、

上記アクセス許可ステップによって上記アクセスを許可された暗号化された電子情報を復号化する復号化ステップ

とを備えたことを特徴とする請求項９記載の電子情報管理方法。

【請求項１１】

上記電子情報記憶ステップは、上記暗号化された電子情報を利用者から利用環境情報と関連させて格納することを特徴とする請求項９乃至１０のいずれか１項記載の電子情報管理方法。

【請求項１２】

上記電子情報は、電子認証局で発行される電子データである秘密鍵であることを特徴とする請求項９乃至１１のいずれか１項記載の電子情報管理方法。

【請求項１３】

画像上の位置と順序を指定する画像パスワードを利用して、秘密にされるべき電子情報を管理する電子情報管理プログラムを記録したコンピュータ読み取り可能な記録媒体において、

コンピュータに、

利用者のパスワード登録のため、画像パスワードを利用する際の複数の画像情報、および、画像上に重畳させる目の細かさが異なる複数のメッシュ情報を、画面上に表示し、その中から利用者によって選択された特定の画像情報および特定のメッシュ情報を利用者ごとに登録する画像メッシュ登録機能と、

上記選択された特定の画像およびメッシュに基づき、マウスにより指定された点列の位置及び順序情報を登録する位置順序登録機能と、

上記選択された画像上で指定された上記点列の位置及び順序の情報を暗号化キー作成式の変数に代入することにより値を算出し、該算出された値によって上記電子情報のデータを並び替えることで上記電子情報を暗号化する暗号化機能と、

上記暗号化された電子情報を記憶する電子情報記憶機能と、

利用者のパスワード利用のため、当該パスワードを利用する利用者を指定させ、指定された利用者に対して登録された前記画像情報及び前記メッシュ情報に基づいて、上記特定の画像および該画像に重畳させて特定のメッシュを表示し、上記位置順序登録機能が登録した上記点列の位置及び順序情報と同じ点列の位置及び順序の情報が指定された場合に上記暗号化された電子情報へのアクセスを許可するアクセス許可機能と、

上記アクセス許可手段によって上記アクセスを許可された暗号化された電子情報を復号化する復号化機能

とを実現させるための電子情報管理プログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、電子認証局が利用者に発行する電子データである秘密鍵等の機密情報データを管理する方法及び装置に関する。

【０００２】

【従来の技術】

従来、電子的に保持されている秘密鍵を管理する場合、悪意の第三者が利用できないように、一般的に、数桁の英数字によるパスワードで管理で秘密鍵が管理されている。数桁の英数字によるパスワードを利用する場合に、利用分野毎に異なるパスワードを利用することが望ましいが、実際上、利用分野毎にパスワードを記憶しておくことが困難であるため、すべての利用分野で統一したパスワードを利用することが多い。

【０００３】
また、利用者の生年月日若しくは電話番号の様な覚え易いパスワードが入力される場合も多い。このような利用者の身近なデータに基づくパスワードが破られる確率は、数学的に推定されるパスワードが破られる確率よりも高くなる。
更に、インターネットの利用時には、利用者はマウスで作業することが多いため、キーボード、特に、テンキーだけを用いてパスワードを入力している場合に、当該作業時に、パスワードが悪意の第三者に遺漏する可能性がある。
【０００４】
【発明が解決しようとする課題】
上記の如く、数桁の英数字によるパスワードで秘密鍵を管理する場合に、利用者によるパスワードの利用形態によってパスワードが破られる可能性が高くなるという問題がある。
パスワードで管理されるべき秘密鍵のデータは、一般的に、数百桁の数値データとなるため、この数値データを人の記憶だけに頼ることは現実的ではない。そのため、一般的に、秘密鍵はＩＣカード等の記憶媒体に保持される。ＩＣカード等の記憶媒体に保持された秘密鍵の内容を明らかにする際のセキュリティ管理手段としてパスワードを利用する場合、上述のような一般的なパスワード管理の問題が発生するので、ＩＣカード等の記憶媒体自体が悪意の第三者により取得されたときに、同様にパスワードが破られる危険性に晒されることになる。
【０００５】
このように、従来技術によれば、一般的に、秘密鍵が他のパスワードで管理するシステムと同様に英数字キーによるパスワードで管理されるため、本来は他のシステムよりも厳格なセキュリティ管理が要求される秘密鍵のアクセスに対するパスワード管理のセキュリティが、他のシステムのセキュリティ管理と同じ程度の管理下に晒されるという問題がある。
【０００６】
また、英数字によるパスワード管理方法において、他のシステムよりも厳格なセキュリティを施すためには、本人のパスワードであることが推測し難く、かつ、桁数の多いパスワードを使用する必要が生じる。しかし、このような性質のパスワードは、利用者本人が記憶することも難しくなり、人の記憶だけに留めておくことが困難である。従って、秘密鍵の管理に関して、他のシステムよりも厳格なセキュリティ管理を施すことが困難であるという問題がある。
【０００７】
また、英数字によるパスワード管理方法では、本人の名前、愛称、電話番号若しくは生年月日等の本人の属性や趣味などからパスワードを設定していることが多いため、数学的にパスワードが破られる確率よりも高い確率でパスワードが破られるので、このような場合に、秘密鍵が第三者によって取得される可能性が高くなるという問題がある。
【０００８】
更に、秘密鍵をやりとりするシステムは、一般的に、インターネットのブラウザで操作され、コンピュータの操作者は主としてマウスを用いてシステムの操作を行う。そのため、秘密鍵の管理に英数字キーによるパスワードを利用した場合に、秘密鍵にアクセスするためのパスワードを英数字キーで入力する際に、マウスから手を離して操作することになるので、秘密鍵の管理のような厳格、かつ、素早い操作による高度なセキュリティが要求される場面で、英数字キーによるパスワード操作は不向きであるという問題がある。
【０００９】
近年では、人間の生体系の特徴である指紋又は声紋等をセキュリティ管理に利用するシステムも開発されているが、いずれのシステムも専用のハードウェアを必要とするため、システムを構成する機器の価格が高価になると言う問題がある。
本発明は、上記従来技術の問題を解決するため、利用者の電話番号等の個人の属性によらず、単純でありながら高度なパスワード管理のセキュリティが簡単なマウス操作だけで実現された画像指示による電子情報管理装置、特に、電子認証局で発行される電子データで

ある秘密鍵を管理する画像指示による秘密鍵管理装置及び方法、並びに、秘密鍵管理プログラムを記録した記録媒体の提供を目的とする。

【００１０】

【課題を解決するための手段】

上記本発明の目的は、秘密にされるべき電子情報を管理する電子情報管理装置により達成される。図１は本発明の電子情報管理装置の原理構成図である。同図に示す如く、本発明の電子情報管理装置２は、

画面４上に画像を表示する手段１０と、

上記画像上でマウス６により指定された点列の位置及び順序の情報を入力する手段１２と、

上記点列の位置及び順序の情報を用いて上記電子情報を暗号化する手段１４と、

上記暗号化された電子情報を記憶する手段１６と、

上記記憶された電子情報を暗号化する際に用いられた点列の位置及び順序の情報と同じ点列の位置及び順序の情報が指定された場合に上記暗号化され記憶された電子情報へのアクセスを許可する手段１８と、

上記アクセスを許可された暗号化された電子情報を復号化する手段２０とにより構成される。

【００１１】

上記本発明の電子情報管理装置２は、画面に表示された画像上でマウスにより指示された点列の位置及び順序の情報の同一性に基づいて秘密にされるべき電子情報へのアクセスを管理するので、マウス操作によるパスワード管理が実現される。更に、本発明の電子情報管理装置２におけるパスワードの入力は、画面に表示された画像上の点列の位置と順序とにより入力されるので、利用者の電話番号等の個人属性によらないデータがパスワードとして用いられるので、パスワードを破られる確率が英数字キーによるパスワードよりも著しく低下する。

【００１２】

更に、本発明の電子情報管理装置２に記憶される電子情報は、マウスにより指示された点列の位置及び順序の情報に基づく暗号化キーを用いて暗号化されているので、電子情報をそのまま記憶する場合、若しくは、見破られやすい暗号化キーを用いて暗号化された電子情報が記憶される場合と比べて高度なセキュリティが実現される。

【００１３】

上記電子情報を暗号化する手段１４は、上記点列の位置及び順序の情報から暗号化キーを生成する手段と、上記生成された暗号化キーを用いて上記電子情報を暗号化する手段とにより構成することができる。

上記暗号化キーを生成する手段は、上記点列の位置及び順序の情報を暗号化キー作成式の変数に代入することにより値を算出する。上記暗号化キーを用いて上記電子情報を暗号化する手段は、上記算出された値によって上記電子情報のデータを並び換えることを特徴とする。

【００１４】

このように電子情報を暗号化する手段１４を構成することにより、電子情報は利用者により指定された点列の位置及び順序の情報に依存した暗号化キーにより暗号化されるので、暗号化された電子情報が悪意の第三者に解読される可能性が低下する。

更に、上記画面４上に画像を表示する手段１０は、上記表示された画像上に可変サイズの縦横のメッシュを任意の色で表示することを特徴とする。これにより、利用者のマウス操作がより簡単に行える点が有利である。

【００１５】

図２は、電子認証局で発行される電子データである秘密鍵を管理する本発明の秘密鍵管理装置３０の構成図である。同図に示す如く、秘密鍵管理装置３０は、

画面上に画像を表示する手段３２と、

上記画像上でマウスにより指定された点列の位置及び順序の情報を入力する手段４０と、

上記点列の位置及び順序の情報を用いて上記秘密鍵を暗号化する手段４２と、
上記暗号化された秘密鍵を記憶する手段５０と、
上記記憶された秘密鍵を暗号化する際に用いられた点列の位置及び順序の情報と同じ点列の位置及び順序の情報が指定された場合に上記暗号化され記憶された秘密鍵へのアクセスを許可する手段６０と、
上記アクセスを許可された秘密鍵を復号化する手段６６とを備える。

【００１６】

上記秘密鍵を暗号化する手段４２は、上記点列の位置及び順序の情報から暗号化キーを生成する手段４４と、上記生成された暗号化キーを用いて上記秘密鍵を暗号化する手段４６とを含む。
上記暗号化キーを生成する手段４４は、上記点列の位置及び順序の情報を暗号化キー作成式の変数に代入することにより値を算出する。上記暗号化キーを用いて上記秘密鍵を暗号化する手段４６は、上記算出された値によって上記秘密鍵のデータを並び換える。

【００１７】

上記画面上に画像を表示する手段３２は、予め登録された画像３４を表示する。
上記画面上に画像を表示する手段３２は、利用者により選択された画像３６を表示してもよい。また、上記画面上に画像を表示する手段３２は、上記秘密鍵が記憶される記憶媒体５０とは別の媒体からの画像を表示してもよい。これにより、画像による指示の際のセキュリティがより良くなる。

【００１８】

上記秘密鍵管理装置３０は、上記画像が表示された画面上に可変サイズの縦横のメッシュを任意の色で表示する手段３８を更に有する。
上記秘密鍵を暗号化する手段４６は、同じ点列の位置及び順序の情報を用いて複数個の秘密鍵を暗号化してもよい。これにより、上記暗号化され記憶された秘密鍵へのアクセスを許可する手段６０は、同じ点列の位置及び順序の情報が指定された場合に、複数個の秘密鍵へのアクセスを許可することが可能である。

【００１９】

本発明の秘密鍵管理装置３０は、利用者から指定された利用者情報及び利用者環境情報を入力する手段６８を更に有し、上記暗号化された秘密鍵を記憶する手段５０は、上記暗号化された秘密鍵５２を、上記秘密鍵の利用者情報５４及び利用者環境情報５６と共に記憶する。
これにより、上記秘密鍵へのアクセスを許可する手段６０は、上記秘密鍵へのアクセスの可否を判定する手段６２と、利用者により指定された秘密鍵の利用者情報及び利用者環境情報を受け、上記アクセスが許可された秘密鍵の中で、上記利用者により指定された利用者情報及び利用者環境情報と共に記憶された秘密鍵を選択する手段６４とを有する点が有利である。

【００２０】

本発明は、電子認証局で発行される電子データである秘密鍵をパスワードで管理する画像指示による秘密鍵管理方法である。本発明の秘密鍵管理方法における秘密鍵の登録処理は、図３のフローチャートに示される如く、
（ａ）利用者からの利用者情報及び利用環境情報を入力し（ステップ１）、
（ｂ）画面上に表示される画像を設定し（ステップ２）、
（ｃ）上記画面上に上記画像を表示し、上記表示された画像上で利用者により指定された点列の位置及び順序の情報を登録し（ステップ３）、
（ｄ）上記点列の位置及び順序の情報に基づいて暗号化キーを決定し（ステップ４）、
（ｅ）利用者により指定された秘密鍵を上記暗号化キーによって暗号化し（ステップ５）、
（ｆ）上記暗号化された秘密鍵を上記利用環境情報と関連させて格納することにより、秘密鍵を登録する。

【００２１】

本発明の秘密鍵管理方法における秘密鍵へのアクセス管理処理は、図４に示される如く、
（ｇ）利用者からの利用者情報を入力し（ステップ７）、
（ｈ）上記画面上に上記画像を表示し、上記表示された画像上で利用者により指定された点列の位置及び順序の情報を取得し（ステップ８）、
（ｉ）上記取得された点列の位置及び順序の情報が上記登録された点列の位置及び順序の情報と一致するかどうかを判定し（ステップ９）、
（ｊ）一致しないと判定された場合、記憶された秘密鍵へのアクセスを禁止し（ステップ１０）、
一致すると判定された場合、上記段階（ｆ）において記憶された秘密鍵の中で、上記段階（ｇ）において入力された利用者情報と関連した秘密鍵を復号化し、上記復号化された秘密鍵と関連して格納された利用環境情報に従って上記秘密鍵のアクセスを許可する（ステップ１１）。

【００２２】

本発明は、更に、電子認証局で発行される電子データである秘密鍵を管理する秘密鍵管理プログラムを記録した記録媒体であって、
画面上に画像を表示させるプロセスと、
上記画像上でマウスにより指定された点列の位置及び順序の情報を入力させるプロセスと、
上記点列の位置及び順序の情報を用いて上記秘密鍵を暗号化させるプロセスと、
上記暗号化された秘密鍵を記憶させるプロセスと、
上記記憶された秘密鍵を暗号化する際に用いられた点列の位置及び順序の情報と同じ点列の位置及び順序の情報が指定された場合に上記暗号化され記憶された秘密鍵へのアクセスを許可させるプロセスと、
上記アクセスを許可された秘密鍵を復号化させるプロセスとを備えたことを特徴とする画像指示による秘密鍵管理プログラムを記録した記録媒体である。

【００２３】

上記秘密鍵を暗号化させるプロセスは、
上記点列の位置及び順序の情報から暗号化キーを生成させるプロセスと、
上記生成された暗号化キーを用いて上記秘密鍵を暗号化させるプロセスとを含むよう構成される点で有利である。
上記暗号化キーを生成させるプロセスは、上記点列の位置及び順序の情報を暗号化キー作成式の変数に代入することにより値を算出させ、　上記暗号化キーを用いて上記秘密鍵を暗号化させるプロセスは、上記算出された値によって上記秘密鍵のデータを並び換えさせることを特徴とする。

【００２４】

また、上記画面上に画像を表示させるプロセスは、予め登録された画像を表示させ、利用者により選択された画像を表示させ、或いは、上記秘密鍵が記憶される記憶媒体とは別の媒体からの画像を表示させる点で有利である。
本発明の記録媒体は、上記画像が表示された画面上に可変サイズの縦横のメッシュを任意の色で表示させるプロセスを更に有する画像指示による秘密鍵管理プログラムが記録される点で有利である。

【００２５】

上記秘密鍵を暗号化させるプロセスは、同じ点列の位置及び順序の情報を用いて複数個の秘密鍵を暗号化させ、
上記暗号化され記憶された秘密鍵へのアクセスを許可させるプロセスは、同じ点列の位置及び順序の情報が指定された場合に、複数個の秘密鍵へのアクセスを許可させる点で有利である。

【００２６】

本発明の記録媒体は、利用者から指定された利用者情報及び利用者環境情報を入力させるプロセスを更に有し、

上記暗号化された秘密鍵を記憶させるプロセスは、
上記暗号化された秘密鍵を、上記秘密鍵の利用者情報及び利用者環境情報と共に記憶させることを特徴とする。
【００２７】
上記秘密鍵へのアクセスを許可させるプロセスは、
上記秘密鍵へのアクセスの可否を判定させるプロセスと、
利用者により指定された秘密鍵の利用者情報及び利用者環境情報を受け、上記アクセスが許可された秘密鍵の中で、上記利用者により指定された利用者情報及び利用者環境情報と共に記憶された秘密鍵を選択させるプロセスとを有することを特徴とする。
【００２８】
【発明の実施の形態】
以下、添付図面を参照して本発明の実施例を説明する。図５は本発明の第１の実施例の秘密鍵管理システム１００の構成図である。秘密鍵管理システム１００は、画像上にマウスで指示する位置と順序の情報によって暗号化キーを生成し、秘密鍵へのアクセスをパスワード管理するシステムである。
【００２９】
秘密管理システム１００は、処理機能選択モジュール１０２を有し、処理機能選択モジュール１０２は、システムへの入力に応じて、初期登録処理部１０３、画像パスワード利用処理部１０４、追加登録処理部１０５若しくは変更処理部１０６を選択的に起動する。
初期登録処理部１０３は、画像パスワード利用者がパスワードを登録するための一連の処理を行う。初期登録処理部１０３は、利用者環境情報登録モジュール１１１、背景画像選択・登録モジュール１１２、重畳メッシュ選択・登録モジュール１１３、位置・選択順序情報登録モジュール１１４、暗号化キー作成モジュール１１５、秘密鍵登録モジュール１１６、秘密鍵暗号化モジュール１１７、秘密鍵格納モジュール１１８及び利用者環境格納モジュール１１９からなる。
【００３０】
以下、図６の動作フローチャートを参照して初期登録処理部１０３の各モジュールの動作を説明する。
ステップ２１：利用者環境情報登録モジュール１１１は、これから画像パスワードを利用しようとする者のシステム環境をセットアップする。利用者は、この利用者環境情報登録モジュールに登録した名前を、以降の画像パスワードの利用時において、その登録名称をマウスで選択して処理を進めることが可能である。登録名称は、必ずしも利用者の本名である必要はないため、利用者にとって親しみやすい名称としたり、悪意の第三者が利用者を推測できないような名称を登録してもよい。
【００３１】
利用者環境情報登録モジュール１１１に、利用者名の登録機能の他に画像パスワード利用時の利用者自身の各種システム環境を予めセットアップさせておくことにより、利用ブラウザからのマウス操作性を高める利用環境が提供される。
ステップ２２：背景画像選択・登録モジュール１１２は、利用者が画像パスワードを利用する際の背景画像を登録する。
【００３２】
利用者は、本システムに予め登録されている背景画像の中から選択された画像データ、利用者が任意に登録する画像データ、或いは、他の記憶媒体に記憶された画像データを選択的に利用することが可能である。
ステップ２３：重畳メッシュ選択・登録モジュール１１３は、利用者が使用する画像上に任意の目の細かさの縦横の線であるメッシュを重畳させる。
【００３３】
利用者は、マウスで画像の任意の位置をパスワードとして登録する際、画像パスワードの利用時に、本処理で登録されたメッシュを画像上に重畳させることにより、利用者が指示する画像上の曖昧な位置と、システム側での認識範囲を一致させて判断できるため、利用

者のマウス指示位置の再現性が高められる。
ステップ２４：位置・選択順序情報登録モジュール１１４は、利用者が登録した画像と重畳するメッシュ上に、マウスで指示する点列の位置及び順序をパスワードの桁数分登録する。
【００３４】
ステップ２５：暗号化キー作成モジュール１１５は、位置・選択順序情報登録モジュール１１４で登録された位置及び順序等の情報に基づいて、暗号化キーを作成する。暗号化キーは、ある特定の数値であり、この数値は暗号化キー作成式に、位置・選択順序情報登録モジュール１１４で得られた情報を変数として取り込み、算出される。
【００３５】
ステップ２６：秘密鍵登録モジュール１１６は、利用者の秘密鍵データを本管理システムに登録する。ＩＣカードに保持されている利用者の秘密鍵である数値データは、本システムに一度登録すれば、画像パスワードを利用する限りにおいては、常時ＩＣカードを利用する毎にカードを挿入する必要性はなくなる。
ステップ２７：秘密鍵暗号化モジュール１１７は、暗号化キー作成モジュール１１５で算出された暗号化キーである数値に基づいて、秘密鍵のデータを並び換える。本暗号化のアルゴリズムは、公知の技術であるＤＥＳ等を利用することが可能である。
【００３６】
ステップ２８：秘密鍵格納モジュール１１８は、秘密鍵暗号化モジュール１１７で暗号化された秘密鍵のデータを秘密鍵管理データベース１３１に格納する。ステップ２９：利用者環境格納モジュール１１９は、上記のモジュール１１１乃至１１８までの利用者環境に関する情報を連携させて利用者環境データベース１３２に格納する。
【００３７】
図７の（ａ）及び（ｂ）は、本発明の第１の実施例における初期登録処理後の秘密鍵管理データベース１３１及び利用者環境データベース１３２を説明する図である。同図の（ａ）及び（ｂ）における利用者コードは、初期登録を行った利用者を識別するコードであり、特定の利用者には、秘密鍵管理データベース１３１と利用者環境データベース１３２の両方に共通した利用者コードが与えられる。同図の（ｂ）における利用者名はステップ２１で登録された利用者の名前であり、背景画像コードはステップ２２で選択・登録された背景画像を指定する情報である。
【００３８】
図７の（ａ）における秘密鍵Ａは、ステップ２８で登録された秘密鍵であり、秘密鍵データベース１３１に登録される秘密鍵は、ステップ２７において上記暗号化キーを用いて暗号化された秘密鍵である。同図の（ａ）に示された画像暗号解とは、暗号化された秘密鍵を復号化する際に利用される暗号解であり、具体的には、暗号化される前の秘密鍵のデータと、暗号化された後の秘密鍵のデータとの差を表わす情報である。
【００３９】
図７の（ｂ）に示された利用環境コードは、初期登録処理において登録された秘密鍵を利用する環境、例えば、ブラウザの種類を表わす利用環境コードであり、画像パスワード利用処理部１０４で参照される。また、同図の（ａ）に示された前回利用アドレスとは、初期登録処理部１０３で秘密鍵管理データベース１３１に格納された秘密鍵を、画像パスワード利用処理部１０４で実際に利用したときに、その秘密鍵を送信した送信先のアドレスのような利用アドレス情報を表わす。
【００４０】
次に、画像パスワード利用処理部１０４は、利用者名選択モジュール１２１、背景・メッシュ選択モジュール１２２、画像パスワード受付モジュール１２３、画像パスワード判定モジュール１２４及び秘密鍵復号化／送信連携モジュール１２５により構成され、画像パスワード利用者がパスワードを利用する際の処理を行う。以下、図８の動作フローチャートを参照して、画像パスワード処理部１０４の動作を説明する。
【００４１】

ステップ３１：利用者選択モジュール１２１は、初期登録処理部１０３において利用者が登録した利用者名をマウスで選択できるように表示する。
ステップ３２：背景・メッシュ画像表示モジュール１２２は、初期登録処理部１０３において、利用者選択モジュール１２１で選択された利用者名に対応した利用者が登録した背景画像及びメッシュ情報を表示する。
【００４２】
ステップ３３：画像パスワード受付モジュール１２３は、利用者がマウスで画像上を指示する位置・選択順序を画像パスワードとして受け付ける。
利用者が画像上をクリックすると、対応した位置の升目の色若しくは模様が変化するので、クリックした数が可視化され、利用者が画像上をチェックした状況が確認できる。
【００４３】
ステップ３４：画像パスワード判定モジュール１２４は、画像パスワード受付モジュール１２３で受け付けたパスワードが、利用者が予め初期登録部１０３で登録したパスワードと合致しているかどうか、即ち、マウスで指定した位置と順序が合致しているかどうかを判定する。利用者がマウスで指示した位置及び順序が合致しているときステップ３５に進む。
【００４４】
ステップ３５：秘密鍵復号化／送信連携モジュール１２５は、ステップ３４で利用者がマウスで指示した位置及び順序が合致していると判定された場合、即ち、画像パスワードが解かれた場合に限り起動され、画像パスワードで暗号化されていた秘密鍵のデータを復号化し、予め登録されていた利用者の秘密鍵を表示し、或いは、送信時のブラウザとの連携を実施する。このとき、図７の（ｂ）に格納された利用環境コードを参照して連携させるべきブラウザを設定し、図７の（ａ）に格納された前回利用アドレスを参照して秘密鍵を送信すべきアドレスを設定することが可能である。
【００４５】
図９は本発明の第１の実施例における追加登録処理部１０５の動作を説明するフローチャートである。以下、既登録の画像パスワードについて秘密鍵を追加登録する追加登録処理部１０５の動作を説明する。
追加登録処理部１０５は、初期登録処理部１０３において利用者が登録した利用者名をマウスで選択できるように表示する（ステップ４１）。
【００４６】
次に、追加登録処理部１０５は、初期登録処理部１０３において、利用者選択モジュール１２１で選択された利用者名に対応した利用者が登録した背景画像及びメッシュ情報を表示する（ステップ４２）。これらの情報は、図７の（ｂ）に示された利用者環境データベース１３２に格納されている。
追加登録処理部１０５は、利用者がマウスで画像上を指示する位置・選択順序を画像パスワードとして受け付ける（ステップ４３）。利用者が画像上をクリックすると、対応した位置の枡目の色若しくは模様が変化するので、クリックした数が可視化され、利用者が画像上をチェックした状況が確認できる。
【００４７】
追加登録処理部１０５は、ステップ４３で受け付けたパスワードが、利用者が予め初期登録部１０３で登録したパスワードと合致しているかどうか、即ち、マウスで指定した位置と順序が合致しているかどうかを判定する（ステップ４４）。この合致は、位置及び順序の情報を直接比較して判定してもよいが、位置と順序の情報から作成された暗号化キーを比較することにより判定することが可能である。利用者がマウスで指示した位置及び順序が合致しているときステップ４５に進む。
【００４８】
追加登録処理部１０５は、既存の画像パスワード処理（復号化）を実施する（ステップ４５）。
追加登録処理部１０５は、利用者の秘密鍵データを本管理システムに追加登録する（ステ

ップ４６）。
追加登録処理部１０５は、既存の画像パスワードに対し算出された暗号化キーである数値に基づいて、秘密鍵のデータを並び換える（ステップ４７）。
【００４９】
追加登録処理部１０５は、ステップ４７で暗号化された秘密鍵のデータを秘密鍵管理データベース１３１に格納する（ステップ４８）。
追加登録処理部１０５は、上記のステップ４１乃至４８までの利用者環境に関する情報を連携させて利用者環境データベース１３２に格納する（ステップ４９）。
【００５０】
図１０は本発明の第１の実施例における追加登録処理後の秘密鍵管理データベースの内容を説明する図である。同図に示す如く、追加登録処理により、既に登録されている秘密鍵Ａと同一の利用者コード及び画像暗号解と関連した別の秘密鍵Ｂが秘密鍵管理データベース１３１に格納される。これにより、一つの画像パスワードに対し複数の秘密鍵を登録することが可能であり、更に、複数の秘密鍵毎に前回利用アドレスを記憶することにより、秘密鍵の利用時に秘密鍵の利用目的に応じた秘密鍵の提供サービスを実現することが可能である。更に、秘密鍵管理データベース１３１及び利用者環境データベース１３２に、秘密鍵管理のための他の付加的な情報を格納することにより、利用者に種々のサービスを提供し得るようになる。
【００５１】
図１１は本発明の第１の実施例における変更処理部１０６の動作を説明するフローチャートである。以下、同図を参照して画像パスワードの変更を行う変更処理部１０６の動作を説明する。
変更処理部１０６は、初期登録処理部１０３において利用者が登録した利用者名をマウスで選択できるように表示する（ステップ５１）。
【００５２】
次に、変更処理部１０６は、初期登録処理部１０３において、利用者選択モジュール１２１で選択された利用者名に対応した利用者が登録した背景画像及びメッシュ情報を表示する（ステップ５２）。
変更処理部１０６は、利用者がマウスで画像上を指示する位置・選択順序を画像パスワードとして受け付ける（ステップ５３）。利用者が画像上をクリックすると、対応した位置の枡目の色若しくは模様が変化するので、クリックした数が可視化され、利用者が画像上をチェックした状況が確認できる。
【００５３】
変更処理部１０６は、ステップ４３で受け付けたパスワードが、利用者が予め初期登録部１０３で登録したパスワードと合致しているかどうか、即ち、マウスで指定した位置と順序が合致しているかどうかを判定する（ステップ５４）。利用者がマウスで指示した位置及び順序が合致しているときステップ５５に進む。
変更処理部１０６は、既存の画像パスワード処理（復号化）を実施する（ステップ５５）。画像パスワードを実施した利用者だけが次のステップ５６へ進む。
【００５４】
以下、変更処理部１０６は、初期登録処理部１０３のステップ２１乃至２９と同様の処理を行い（ステップ５６乃至６４）、既登録の秘密鍵に対する画像パスワードを変更する。
【００５５】
【実施例】
以下、図１２乃至２２を参照して本発明の第２の実施例を説明する。
図１２は、図６のステップ１１に対応して利用者名や利用ブラウザ等の利用環境情報を入力する利用画面例である。入力画面から以下の項目を入力する。
（１）利用者名
（２）利用ブラウザ
（３）秘密鍵連携情報（秘密鍵を登録ブラウザを介して送信するか、或いは、画面に表示

するか等を表わす情報）
上記（１）乃至（３）の情報は、図１２の入力画面上から入力するか、或いは、選択入力する。
【００５６】
図１３は、図６のステップ１２に対応して背景の画像を選択する処理の利用画面例である。入力画面から以下の項目を入力する。
（１）背景画像の選択
（２）利用者背景の登録
（１）又は（２）においては、図１３の入力画面上から選択或いは入力する。（１）又は（２）のいずれか一方の処理を実施すれば、他方の処理を行う必要がないので、両方を選択することはできない仕組みとなっている。
【００５７】
図１３において、（１）の背景画像の選択を実施した場合に、選択した画像の種類によっては、分類項目が細分化されて選択できる。また、（２）の利用者背景の登録を選択した場合には、登録元のファイル名や種別を入力する。選択又は登録された画像は、一般に、随時画面上に表示され、利用者の確認が図られる。尚、（２）の利用者背景には、別媒体に記憶された画像を指定することも可能である。この場合、画像の登録は行われず、背景画像を画面上に表示するためには、毎回、当該別媒体から画像イメージを読み出して表示する必要がある。
【００５８】
図１４は、図６のステップ２３に対応して、選択した画像に重畳させるメッシュを選択する処理の利用画面例である。入力画面から以下の項目を入力する。
（１）メッシュの選択
（２）メッシュ表示色の選択
（１）又は（２）においては、図１４の入力画面上から選択入力する。選択メッシュ情報は、画面上で当該画像イメージを随時表示し、利用者の確認が図れるようになっている。
【００５９】
図１５は、図６のステップ２４に対応して、画像パスワードを入力する処理の利用画面例である。入力画面から以下の項目を入力する。
（１）パスワード桁数の選択
（２）位置／順序登録
（１）又は（２）については、図１５の入力画面から選択、入力する。（１）おいてパスワードの桁数を選択することで、自動的に画像上にマウスでクリックできる個数が確定され、指定桁数の個数を超えてクリックされた場合には、その旨のメッセージが出力される。また、指定桁数の個数未満のクリック回数で確定の意味を表わすＯＫボタンをクリックした場合には、その桁数に満たない旨のエラーメッセージが出力される。
【００６０】
（２）の位置／順序登録は、（１）で選択されたパスワードの桁数に連動して入力順序の確認を促すボックスをパスワード桁数の個数分、表示する。このとき、画像上のクリックと連動して、ボックス内の色と表示画像の位置が反転されるなどにより、画像位置及び順番、並びに、パスワードの個数を確認することができる。
【００６１】
図１６は、図１５に示した処理に対応したシステム内部の構造を説明する図である。同図の例では、パスワードの桁数として４個が選択されている。また、同図に示される如く、メッシュの座標を左から右、上から下の順に定義すると、左上隅の座標は（１，１）、右上隅の座標は（１０，１）のように表される。同図に番号１乃至４がつけられた模様の順序にクリックされたとすると、クリックされた位置情報を表わす座標の系列は、（１，２）、（３，８）、（７，８）、（１０，２）のようになる。
【００６２】
これらの座標の系列をＤＥＳの計算式に代入することにより秘密鍵データが暗号化される

。暗号化は、座標データ（ｘ，ｙ）の各値ｘ及びｙに基づいて、最初にｘはｙと入れ換え、次には、ｙはｘと入れ換えるというようにデータを入れ換えることにより、座標の位置情報及び順序情報から元の秘密鍵が暗号化される。例えば、元の秘密鍵データを：１２３４とすると、暗号化は以下の通り行われる。

(1) 元の秘密鍵データ：　１２３４
(2) （１，２）　：１は２と入れ換える　２２３４
(3) （３，８）　：８は３と入れ換える（該当する入れ換え無し）　２２３４
(4) （７，８）　：７は８と入れ換える（該当する入れ換え無し）　２２３４
(5) （１０，２）：２は０と入れ換える　００３４

上記の暗号化によれば、元のデータを入れ換えているだけであるため、データ量は暗号化しても暗号化前と変わらない。

【００６３】

復号化は暗号解を加えることにより実現される。ここで、

暗号解＝元の秘密鍵データ　－　暗号化された秘密鍵データ

により表され、上記数値例の場合、

１２００＝１２３４　－　００３４

である。秘密鍵の復号化は、暗号化された秘密鍵データに暗号解を加えることにより実現される。

【００６４】

図１７は、図６のステップ２５に対応して秘密鍵を暗号化するキーを作成する処理の実施画面例である。この画面は、図６のステップ２１乃至２４の処理が正常に実施され、利用者固有の暗号化キーが生成されたことが通知する。

図１８は、図６のステップ２６に対応して秘密鍵データを入力する処理の利用画面例である。入力画面から以下の項目を選択入力及び入力する。

（１）ＩＣカードから入力
（２）ファイルから入力
（３）キーボードから入力

（１）乃至（３）において、いずれかを選択入力した場合には、各選択に応じた入力画面が表示され、秘密鍵を登録することができる。

【００６５】

図１９乃至２２は、図８に示された画像パスワード利用処理の処理画面例である。利用時の処理の場合、何れの画面でも利用者はマウス指示だけで処理を実施し得る点が有利である。

図１９は、図８のステップ３１に対応して事前に登録された利用者名を入力画面から選択入力する処理の処理画面である。

【００６６】

図２０は、図８のステップ３２及び３３に対応して事前に登録した背景及びメッシュが表示され、画像パスワードを入力し得る状態の画面を表わす。尚、メッシュ情報は、利用者の好みに応じて表示（ＯＮ）／非表示（ＯＦＦ）が選択される。

図２１は、図８のステップ３４に対応してパスワードが受け付けられた場合の利用画面例である。この表示は、利用登録者及び入力した画像パスワードが登録された利用者及び画像パスワードと一致した場合に表示される。秘密鍵の時処理への連携は、事前に登録してもよく、或いは、この画面上で連携方法の変更を実施することが可能である。

【００６７】

図２２は、本発明の第２の実施例におけるブラウザ連携サービス画面例を示す図である。同図の（ａ）には、ブラウザの画面が示される。デジタル署名ボタンをクリックすると、秘密鍵データの格納先が要求される。

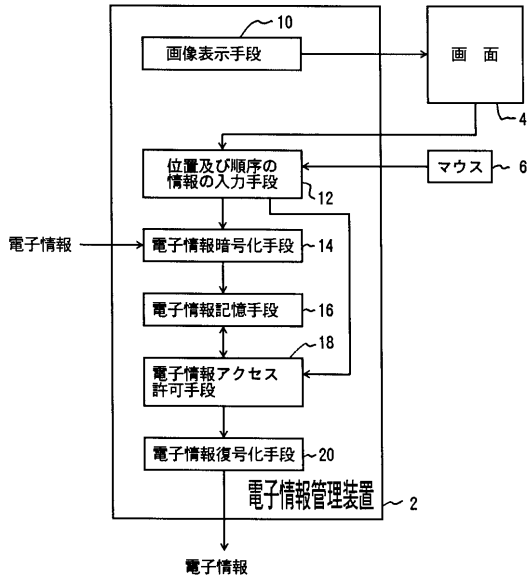
指定された秘密鍵が未使用の場合には、画面上でアイコン化されている上記の画像パスワード処理が起動され、必要な認証局の秘密鍵データの指定が行われる。同図の（ｂ）は、必要な認証局の秘密鍵データを指定する画面例である。

【００６８】
尚、一旦、同図の（ｂ）に示される如く、秘密鍵が指定され、秘密鍵が必要な相手先に送信されたとき、秘密鍵の情報と、利用サイトのアドレス情報とが連携し、更に前回利用時の認証局にチェックマークがつけられるので、利用サイト毎に必要な認証局を記憶する必要がない。
また、上記の実施例では、秘密鍵管理システムの構成要件に基づいて説明しているが、この例に限定されることなく、秘密鍵管理システムの各々の構成要件をソフトウェア（プログラム）で構築し、ディスク装置等に格納しておき、必要に応じて秘密鍵管理システムのコンピュータにインストールして秘密鍵管理を行うことも可能である。さらに、構築されたプログラムをフロッピーディスクやＣＤ－ＲＯＭ等の可搬記憶媒体に格納し、このようなシステムを用いる場面で汎用的に使用することも可能である。
【００６９】
本発明は、上記の実施例に限定されることなく、特許請求の範囲内で種々変更・応用が可能である。
【００７０】
【発明の効果】
以上説明したように、本発明によれば、利用者の任意に選択した画面上に、マウス操作で登録した画像位置及び順序を指示するという形の画像指示によるパスワード方式が実現され、従来の一般的な数桁の英数字によるパスワード管理方式から解放されるので、以下の利点が得られる。
【００７１】
第１に、英数字キーによるパスワードで管理することが一般的である他のパスワードで管理するシステムとは異なり画像位置及び順序によりパスワードが指定されるので、他のシステムよりも厳格な管理が要求される秘密鍵のアクセスに対するパスワード管理のセキュリティを他のシステムのセキュリティよりも高度な管理レベルに高めることが可能になる。
【００７２】
第２に、従来の英数字によるパスワード管理方法では、多くの場合に、本人の名前や愛称、電話番号、或いは、生年月日等の本人の属性や趣味からパスワードが設定されていたため、パスワードが、数学的に予測される確率よりも高い確率で破られる可能性が在るが、本発明によれば、本人の属性とは無関係の画像情報によるパスワード管理が行われるため、パスワードが数学的に予測される確率よりも高い確率で破られる危険性が回避される。
【００７３】
第３に、秘密鍵のやりとりを行うシステムは、インターネットのブラウザで操作される場合が多く、コンピュータの操作者はマウス主体の操作を行う。そのため、従来、秘密鍵にアクセスするためのパスワードを英数字キーで入力する方法は、マウスから手を離してキーを操作することとなり、厳格で、かつ素早い操作による高度なセキュリティが要求される場合には不向きであったが、本発明によれば、マウスだけで操作することが可能になるので、厳格で、かつ素早い操作による高度なセキュリティを実現し得るようになる。
【００７４】
第４に、従来、人間の生体系の特徴である指紋や声帯等をセキュリティ管理に利用するために高価な機器を用いる必要が在るのに対し、本発明によれば、専用のハードウェアを用いることなく画像指示による秘密鍵管理システムを実現することが可能である。また、本発明はソフトウェアだけで実現してもよく、ハードウェアへの追加投資が不要なシステム構築が可能である。
【図面の簡単な説明】
【図１】本発明の原理説明図である。
【図２】本発明の秘密鍵管理装置の構成図である。
【図３】本発明の秘密鍵管理方法における秘密鍵登録の動作フローチャートである。
【図４】本発明の秘密鍵管理方法法における秘密鍵へのアクセス管理処理の動作フローチ

ャートである。
【図５】本発明の第１の実施例による秘密鍵管理システムの構成図である。
【図６】本発明の第１の実施例における初期登録部の動作説明フローチャートである。
【図７】本発明の第１の実施例における初期登録後のデータベースの説明図である。
【図８】本発明の第１の実施例における画像パスワード利用処理部の動作説明フローチャートである
【図９】本発明の第１の実施例における追加登録処理部の動作説明フローチャートである。
【図１０】本発明の第１の実施例における追加登録処理後の秘密鍵管理データベースの説明図である。
【図１１】本発明の第１の実施例における変更処理部の動作説明フローチャートである。
【図１２】本発明の第２の実施例における処理画面例－１である。
【図１３】本発明の第２の実施例における処理画面例－２である。
【図１４】本発明の第２の実施例における処理画面例－３である。
【図１５】本発明の第２の実施例における処理画面例－４である。
【図１６】本発明の第２の実施例における内部処理構造の説明図である。
【図１７】本発明の第２の実施例における処理画面例－５である。
【図１８】本発明の第２の実施例における処理画面例－６である。
【図１９】本発明の第２の実施例における処理画面例－７である。
【図２０】本発明の第２の実施例における処理画面例－８である。
【図２１】本発明の第２の実施例における処理画面例－９である。
【図２２】本発明の第２の実施例におけるブラウザ連携サービス画面例である。
【符号の説明】
２　電子情報管理装置
４　画面
６　マウス
１０　画像表示手段
１２　位置及び順序の情報の入力手段
１４　電子情報暗号化手段
１６　電子情報記憶手段
１８　電子情報アクセス許可手段
２０　電子情報復号化手段

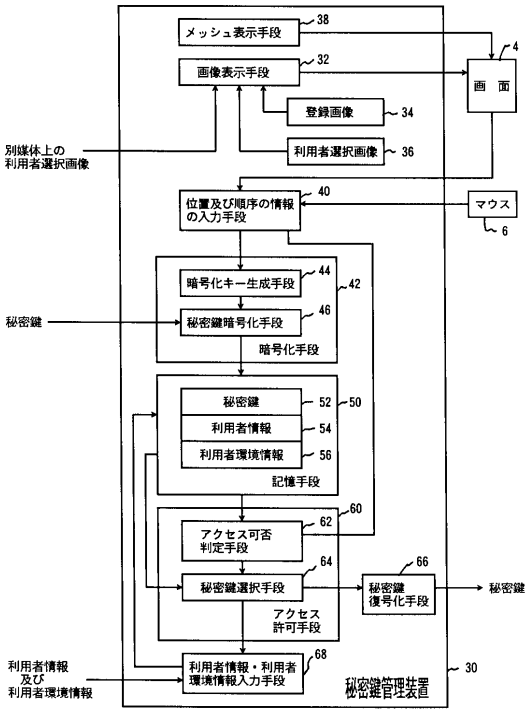
【図１】

本発明の原理構成図



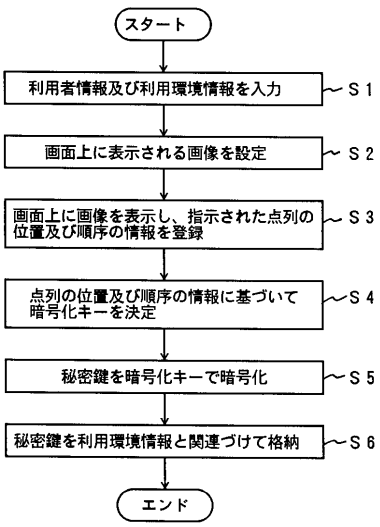

【図２】

本発明の秘密鍵管理装置の構成図



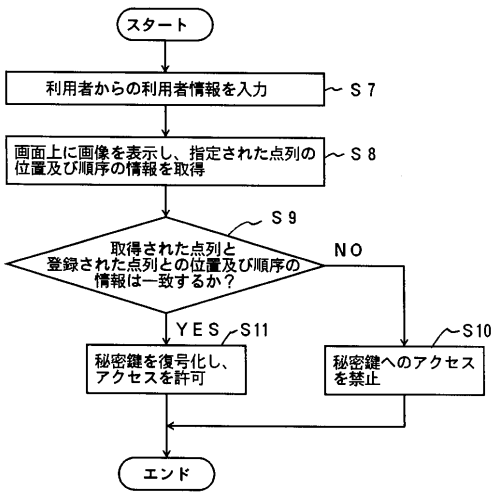

【図３】

本発明の秘密鍵管理方法における
秘密鍵登録の動作フローチャート



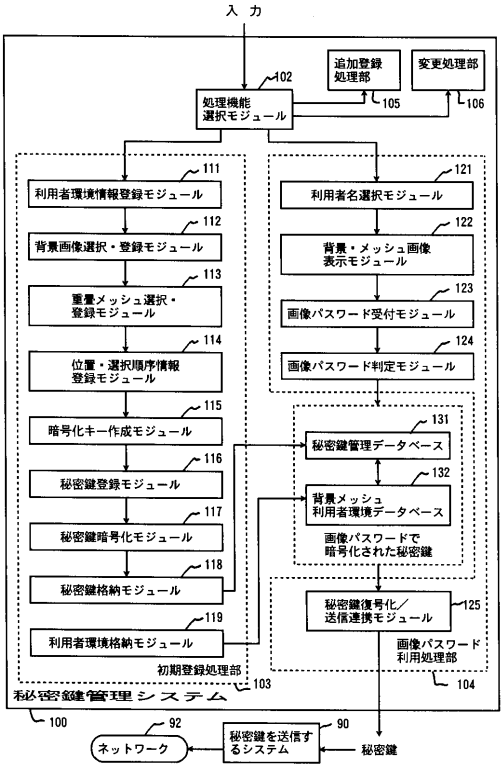

【図４】

本発明の秘密鍵管理方法における秘密鍵への
アクセス管理処理の動作フローチャート



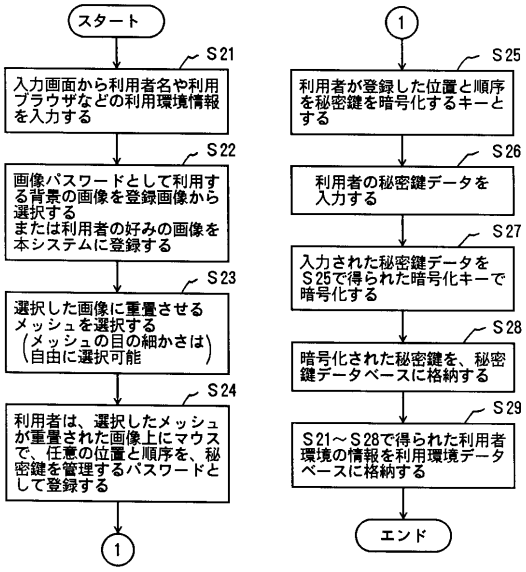
【図５】

本発明の第１の実施例による秘密鍵管理システムの構成図




【図６】

本発明の第１の実施例における
初期登録部の動作説明フローチャート




【図７】

本発明の第１の実施例における
初期登録後のデータベースの説明図

| 利用者コード | 画像暗号解 | 秘密鍵A | 前回利用アドレス | ・・・ |
|---|---|---|---|---|

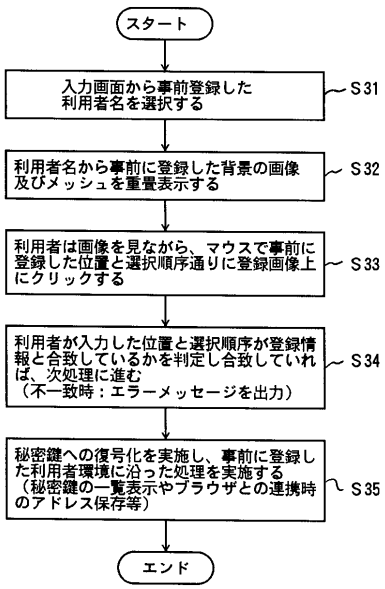
（ａ）秘密鍵管理データベース

| 利用者コード | 利用者名 | 背景画像コード | 利用環境コード | ・・・ |
|---|---|---|---|---|

（ｂ）利用者環境データベース

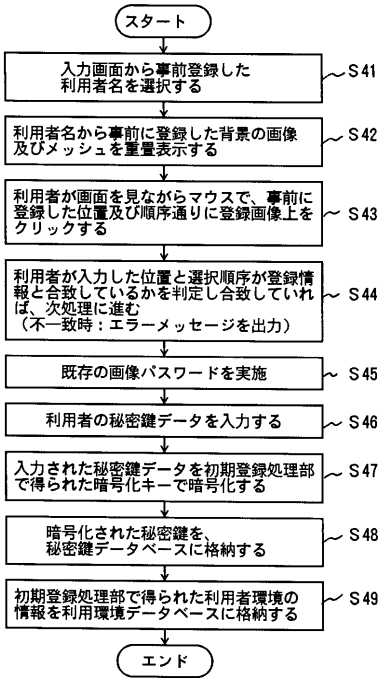
【図８】

本発明の第１の実施例における画像パスワード
利用処理部の動作説明フローチャート



【図９】

本発明の第１の実施例における追加登録処理部の
動作説明フローチャート



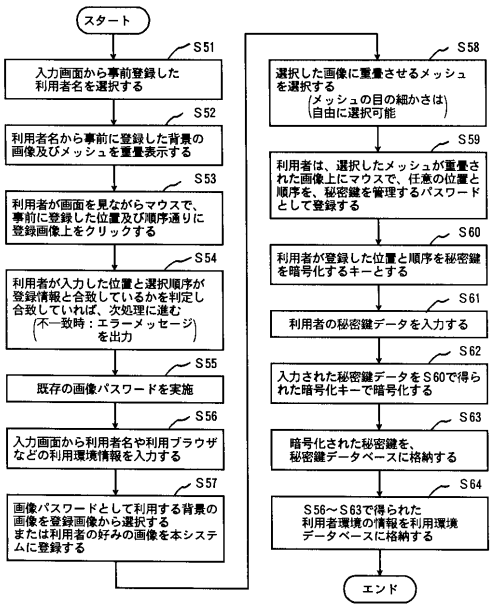

【図１０】

本発明の第１の実施例における追加登録処理後の
秘密鍵管理データベースの説明図

| 利用者コード | 画像暗号解 | 秘密鍵A | 前回利用アドレス | ・・・ |
|---|---|---|---|---|
| | | 秘密鍵B | 前回利用アドレス | |

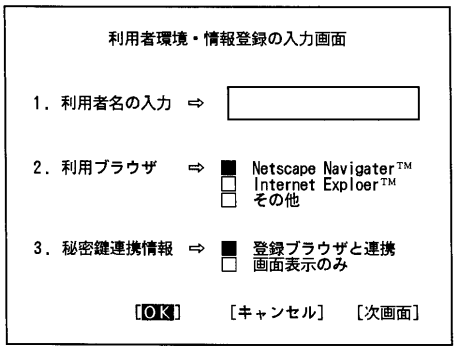
【図１１】

本発明の第１の実施例における
変更処理部の動作説明フローチャート



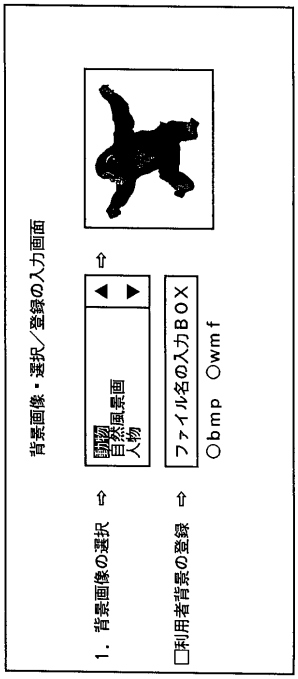

【図１２】

本発明の第２の実施例における処理画面例－１



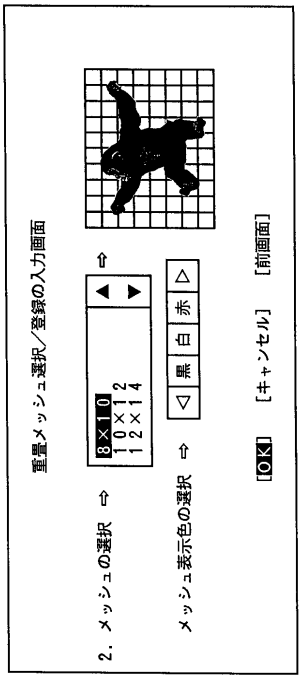
【図１３】

本発明の第２の実施例における処理画面例－２



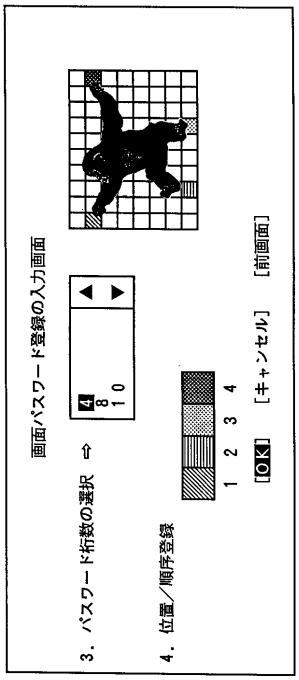

【図１４】

本発明の第２の実施例における処理画面例－３



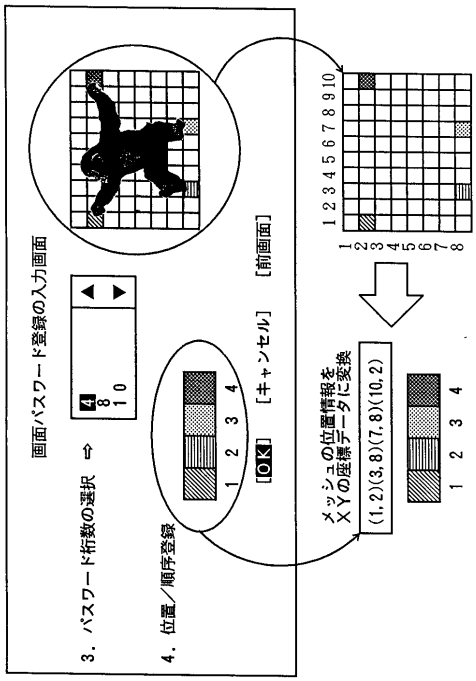

【図１５】

本発明の第２の実施例における処理画面例－４



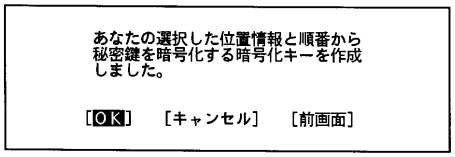

【図１６】

本発明の第２の実施例における内部処理構造の説明図



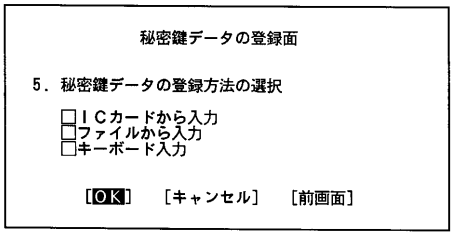
【図１７】

本発明の第２の実施例における処理画面例－５



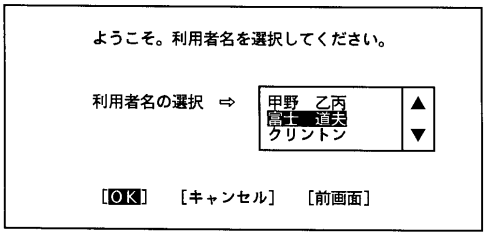

【図１８】

本発明の第２の実施例の処理画面例－６



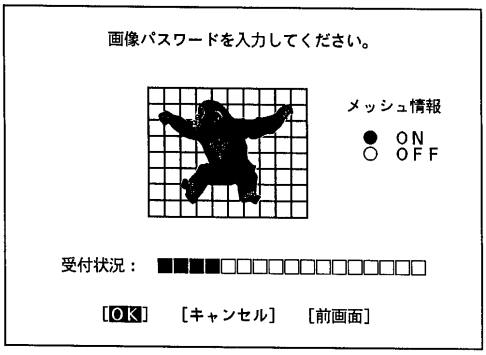

【図１９】

本発明の第２の実施例における処理画面例－７



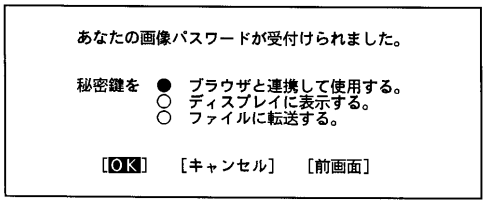

【図２０】

本発明の第２の実施例における処理画面例－８



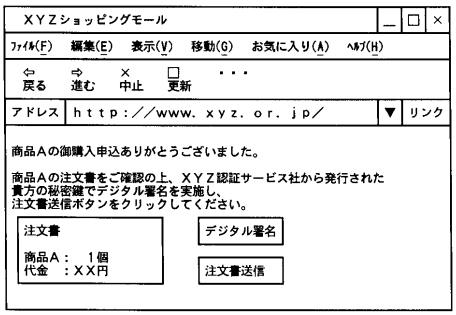

【図２１】

本発明の第２の実施例における処理画面例－９

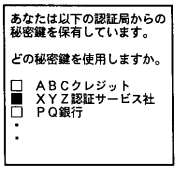



【図２２】

本発明の第２の実施例におけるブラウザ連携サービス画面例




(a)




(b)

フロントページの続き

(51)Int.Cl. FI
H04L 9/00 673D

合議体
審判長 吉岡 浩
審判官 成瀬 博之
審判官 堀江 義隆

(56)参考文献 特開平09－204330（JP，A）
特開平07－254955（JP，A）
特開平01－214976（JP，A）
特開平01－158548（JP，A）
インターネットセキュリティシステム，NEC技報，Vol．49 No．37，p．127－132，1996年7月30日
ECOM通信10 ワーキンググループの紹介－8，Card Wave，Vol．10 No．5，p48－49，1997年4月10日
ネットワーク・セキュリティ，日経マグロウヒル社，p．37－39

(58)調査した分野(Int.Cl.，DB名)
G06F12/14,G06F15/00,H04L9/00