(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2010-205020
(P2010-205020A)
(43)公開日　平成22年9月16日(2010.9.16)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/22	(2006.01)	G06F	9/06	660E	5B017
G06F 21/20	(2006.01)	G06F	15/00	330E	5B276
G06F 21/24	(2006.01)	G06F	12/14	530P	5B285

審査請求 未請求　請求項の数 15　ＯＬ　（全 12 頁）

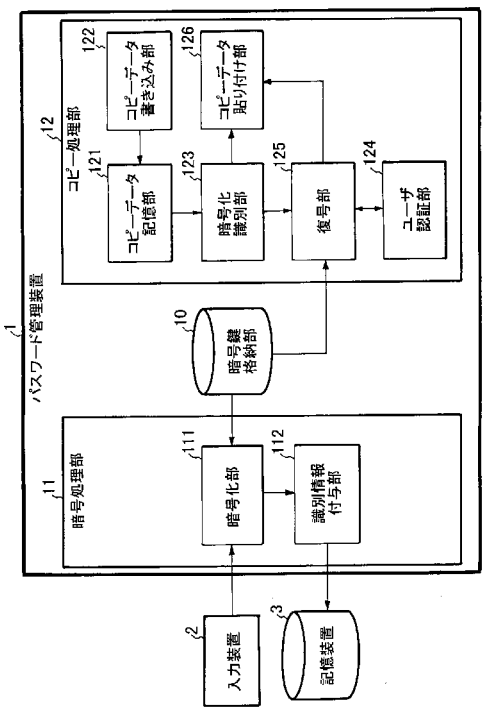
(21)出願番号　特願2009-50459(P2009-50459)
(22)出願日　平成21年3月4日(2009.3.4)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(74)代理人　100065385
弁理士　山下　穣平
(74)代理人　100130029
弁理士　永井　道雄
(72)発明者　久保山　拓
東京都港区芝五丁目７番１号　日本電気株式会社内

Ｆターム(参考)　5B017 AA03 BA05 BA07 CA16
5B276 FA01 FB05
5B285 AA01 AA04 BA08 BA11 CA41 CA42 CA43 CB03 CB52 CB63 CB74

(54)【発明の名称】パスワード管理装置、パスワード管理方法およびパスワード管理用プログラム

(57)【要約】
【課題】アプリケーションにパスワードを入力する際に、画面上にパスワードが表示されず、さらにメモリ上にパスワードが記憶されている期間を短くすることのできるパスワード管理装置を提供する。
【解決手段】暗号鍵でアプリケーション毎のアプリケーション用パスワードを暗号化する暗号化手段、暗号化されたアプリケーション用パスワードをアプリケーション毎に格納する第１記憶手段、或るアプリケーションに対応した暗号化されたアプリケーション用パスワードが第１の記憶手段から読み出された時に、読み出された、暗号化されたアプリケーション用パスワードを記憶する第２の記憶手段、第２の記憶手段に記憶された、暗号化されたアプリケーション用パスワードを暗号鍵に対応した復号鍵で復号する復号手段、復号されたアプリケーション用パスワードを或るアプリケーションの入力領域に貼り付ける貼り付け手段を備える。
【選択図】図１



【特許請求の範囲】
【請求項１】
暗号鍵を用いてアプリケーション毎のアプリケーション用パスワードを暗号化する暗号化手段と、
暗号化されたアプリケーション用パスワードをアプリケーション毎に格納する第１の記憶手段と、
或るアプリケーションに対応した暗号化されたアプリケーション用パスワードが前記第１の記憶手段から読み出された時に、読み出された、暗号化されたアプリケーション用パスワードを記憶する第２の記憶手段と、
前記第２の記憶手段に記憶された、暗号化されたアプリケーション用パスワードを前記暗号鍵に対応した復号鍵で復号する復号手段と、
復号されたアプリケーション用パスワードを前記或るアプリケーションの入力領域に貼り付ける貼り付け手段と、
を備えることを特徴とするパスワード管理装置。
【請求項２】
請求項１に記載のパスワード管理装置において、
暗号化されたアプリケーション用パスワードから、そのハッシュ値を生成するハッシュ生成手段と、
前記ハッシュ値をアプリケーション毎に格納するハッシュ値格納手段と、
ユーザから管理用パスワードを入力し、入力した管理用パスワードから、そのハッシュ値を生成し、入力した管理用パスワードのハッシュ値と前記ハッシュ値格納手段に格納されている何れかのアプリケーションのハッシュ値とが一致しているかどうかを確認することにより、ユーザ認証をするユーザ認証手段を更に備え、
ユーザ認証ができた場合にのみ前記復号手段と前記貼り付け手段は動作することを特徴とするパスワード管理装置。
【請求項３】
請求項２に記載のパスワード管理装置において、
前記管理用パスワードは、何れかのアプリケーション用パスワードと同一であることを特徴とするパスワード管理装置。
【請求項４】
請求項１に記載のパスワード管理装置において、
ユーザから管理用パスワードを入力し、入力した管理用パスワードと予め保持している管理パスワードの対応データとの対応関係を確認することにより、ユーザ認証をするユーザ認証手段を更に備え、
ユーザ認証ができた場合にのみ前記復号手段と前記貼り付け手段は動作することを特徴とするパスワード管理装置。
【請求項５】
請求項２乃至４の何れか１項に記載のパスワード管理装置において、
一部のアプリケーションに対しては、アプリケーション用パスワードを前記暗号化手段により暗号化せず、
暗号化されたアプリケーション用パスワードと暗号化されなかったアプリケーション用パスワードとを識別するための識別情報を、暗号化されたアプリケーション用パスワード、暗号化されなかったアプリケーション用パスワード又はその双方に付与する識別情報付与手段と、
前記第２の記憶手段に記憶された、アプリケーション用パスワードが暗号化されているか否かを前記識別情報を調べることにより識別する暗号化識別手段と、
を更に備え、
前記復号手段及び前記ユーザ認証手段は、前記暗号化識別手段が、アプリケーション用パスワードが暗号化されていると判断した場合にのみ、動作することを特徴とするパスワード管理装置。

【請求項６】
暗号鍵を用いてアプリケーション毎のアプリケーション用パスワードを暗号化する暗号化ステップと、
暗号化されたアプリケーション用パスワードをアプリケーション毎に第１の記憶手段に格納するパスワード格納ステップと、
或るアプリケーションに対応した暗号化されたアプリケーション用パスワードが前記第１の記憶手段から読み出された時に、読み出された、暗号化されたアプリケーション用パスワードを第２の記憶手段に記憶させる記憶ステップと、
前記第２の記憶手段に記憶された、暗号化されたアプリケーション用パスワードを前記暗号鍵に対応した復号鍵で復号する復号ステップと、
復号されたアプリケーション用パスワードを前記或るアプリケーションの入力領域に貼り付ける貼り付けステップと、
を備えることを特徴とするパスワード管理方法。
【請求項７】
請求項６に記載のパスワード管理方法において、
暗号化されたアプリケーション用パスワードから、そのハッシュ値を生成するハッシュ生成ステップと、
前記ハッシュ値をアプリケーション毎にハッシュ値格納手段に格納するハッシュ値格納ステップと、
ユーザから管理用パスワードを入力し、入力した管理用パスワードから、そのハッシュ値を生成し、入力した管理用パスワードのハッシュ値と前記ハッシュ値格納手段に格納されている何れかのアプリケーションのハッシュ値とが一致しているかどうかを確認することにより、ユーザ認証をするユーザ認証ステップを更に備え、
ユーザ認証ができた場合にのみ復号ステップ及び貼り付けステップを行うことを特徴とするパスワード管理方法。
【請求項８】
請求項７に記載のパスワード管理方法において、
前記管理用パスワードは、何れかのアプリケーション用パスワードと同一であることを特徴とするパスワード管理方法。
【請求項９】
請求項６に記載のパスワード管理方法において、
ユーザから管理用パスワードを入力し、入力した管理用パスワードと予め保持している管理パスワードの対応データとの対応関係を確認することにより、ユーザ認証をするユーザ認証ステップを更に備え、
ユーザ認証ができた場合にのみ復号ステップ及び貼り付けステップを行うことを特徴とするパスワード管理方法。
【請求項１０】
請求項７乃至９の何れか１項に記載のパスワード管理方法において、
一部のアプリケーションに対しては、アプリケーション用パスワードを前記暗号化ステップにより暗号化せず、
暗号化されたアプリケーション用パスワードと暗号化されなかったアプリケーション用パスワードとを識別するための識別情報を、暗号化されたアプリケーション用パスワード、暗号化されなかったアプリケーション用パスワード又はその双方に付与する識別情報付与ステップと、
前記第２の記憶手段に記憶された、アプリケーション用パスワードが暗号化されているか否かを前記識別情報を調べることにより識別する暗号化識別ステップと、
を更に備え、
前記復号ステップ及び前記ユーザ認証ステップは、前記暗号化識別ステップで、アプリケーション用パスワードが暗号化されていると判断した場合にのみ、行うことを特徴とするパスワード管理方法。

【請求項１１】
暗号鍵を用いてアプリケーション毎のアプリケーション用パスワードを暗号化する暗号化手段と、
暗号化されたアプリケーション用パスワードをアプリケーション毎に格納する第１の記憶手段と、
或るアプリケーションに対応した暗号化されたアプリケーション用パスワードが前記第１の記憶手段から読み出された時に、読み出された、暗号化されたアプリケーション用パスワードを記憶する第２の記憶手段と、
前記第２の記憶手段に記憶された、暗号化されたアプリケーション用パスワードを前記暗号鍵に対応した復号鍵で復号する復号手段と、
復号されたアプリケーション用パスワードを前記或るアプリケーションの入力領域に貼り付ける貼り付け手段と、
を備えることを特徴とするパスワード管理装置としてコンピュータを機能させるためのパスワード管理用プログラム。
【請求項１２】
請求項１１に記載のパスワード管理用プログラムにおいて、
前記パスワード管理装置は、
暗号化されたアプリケーション用パスワードから、そのハッシュ値を生成するハッシュ生成手段と、
前記ハッシュ値をアプリケーション毎に格納するハッシュ値格納手段と、
ユーザから管理用パスワードを入力し、入力した管理用パスワードから、そのハッシュ値を生成し、入力した管理用パスワードのハッシュ値と前記ハッシュ値格納手段に格納されている何れかのアプリケーションのハッシュ値とが一致しているかどうかを確認することにより、ユーザ認証をするユーザ認証手段を更に備え、
ユーザ認証ができた場合にのみ前記復号手段と前記貼り付け手段は動作することを特徴とするパスワード管理用プログラム。
【請求項１３】
請求項１２に記載のパスワード管理用プログラムにおいて、
前記管理用パスワードは、何れかのアプリケーション用パスワードと同一であることを特徴とするパスワード管理用プログラム。
【請求項１４】
請求項１１に記載のパスワード管理用プログラムにおいて、
前記パスワード管理装置は、
ユーザから管理用パスワードを入力し、入力した管理用パスワードと予め保持している管理パスワードの対応データとの対応関係を確認することにより、ユーザ認証をするユーザ認証手段を更に備え、
前記パスワード管理装置では、ユーザ認証ができた場合にのみ前記復号手段と前記貼り付け手段は動作することを特徴とするパスワード管理用プログラム。
【請求項１５】
請求項１２乃至１４の何れか１項に記載のパスワード管理用プログラムにおいて、
前記パスワード管理装置は、
一部のアプリケーションに対しては、アプリケーション用パスワードを前記暗号化手段により暗号化せず、
暗号化されたアプリケーション用パスワードと暗号化されなかったアプリケーション用パスワードとを識別するための識別情報を、暗号化されたアプリケーション用パスワード、暗号化されなかったアプリケーション用パスワード又はその双方に付与する識別情報付与手段と、
前記第２の記憶手段に記憶された、アプリケーション用パスワードが暗号化されているか否かを前記識別情報を調べることにより識別する暗号化識別手段と、
を更に備え、

前記パスワード管理装置では、前記復号手段及び前記ユーザ認証手段は、前記暗号化識別手段が、アプリケーション用パスワードが暗号化されていると判断した場合にのみ、動作することを特徴とするパスワード管理用プログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明はパスワード管理装置、パスワード管理方法およびパスワード管理用プログラムに関し、特にログイン画面等へのアプリケーション用パスワードのコピーを安全に行なうことのできるパスワード管理装置、パスワード管理方法およびパスワード管理用プログラムに関する。

【背景技術】

【０００２】

近年、インターネット上で提供されるアプリケーション（サービスを含む。）等の普及に伴い、ユーザが認証のためにパスワードを入力する機会が増大している。しかし、安全性への配慮から複雑なパスワードの設定や、同一のパスワードを複数アプリケーションで使用しないことが要求されるため、ユーザは全てのアプリケーションのパスワードの記憶が困難になっている。

【０００３】

そこで、ユーザの利便性を確保しつつ、複数のパスワードを安全に管理することが重要となっている。従来のパスワード管理装置の一例が、特許文献１に記載されている。

【０００４】

特許文献１に記載されたパスワード管理装置は、ユーザはまず、管理用パスワードと、あらかじめ定めた装置を特定する固有情報と、アプリケーション用パスワードを格納するための格納用デバイスのＩＤを用いて生成した暗号鍵を使用してアプリケーション用パスワードを暗号化して、格納用デバイスに格納する。

【先行技術文献】

【特許文献】

【０００５】

【特許文献１】特開２００７－１０８８３３号公報

【特許文献２】特開２００６－０７４５２６号公報

【発明の概要】

【発明が解決しようとする課題】

【０００６】

しかしながら、特許文献１に記載されたパスワード管理装置では、暗号化されたパスワードはパスワード管理装置内で復号されて出力され、ユーザが直接入力するか、またはクリップボード等を介してアプリケーションのパスワード入力欄に入力される。そのため、アプリケーションに入力されるまでの間、画面上やメモリ上にパスワードが露呈される時間が長くなってしまい、可視的に、または不正ソフト等によりパスワードが盗み見られる危険性が高くなる。

【０００７】

また、パスワードを保管する場所を指定する必要があり、さらにパスワードを利用する際にわざわざ復号するためのプログラムを明示的に起動する必要があるなど、パスワードのコピーペースト処理を行なう際に、通常のデータのコピーペースト処理と別の操作が必要となり、ユーザフレンドリーでない。

【０００８】

なお、特許文献１に記載された発明と特許文献２に記載された発明とを組み合わせた場合、外部入力に暗号化データが含まれているかどうかをキーワードテーブルを使って検索することにより知り、暗号化データが含まれていれば認証し、復号して出力するという処理が得られるが、この処理では、暗号化データが全て復号されてしまうので、暗号化されたままデータを出力させることができない。

【０００９】
そこで本発明の目的は、アプリケーションにパスワードを入力する際に、画面上にパスワードが表示されず、さらにメモリ上にパスワードが記憶されている期間を短くすることのできるパスワード管理装置、パスワード管理方法及びパスワード管理用プログラムを提供することにある。
【課題を解決するための手段】
【００１０】
本発明によれば、暗号鍵を用いてアプリケーション毎のアプリケーション用パスワードを暗号化する暗号化手段と、暗号化されたアプリケーション用パスワードをアプリケーション毎に格納する第１の記憶手段と、或るアプリケーションに対応した暗号化されたアプリケーション用パスワードが前記第１の記憶手段から読み出された時に、読み出された、暗号化されたアプリケーション用パスワードを記憶する第２の記憶手段と、前記第２の記憶手段に記憶された、暗号化されたアプリケーション用パスワードを前記暗号鍵に対応した復号鍵で復号する復号手段と、復号されたアプリケーション用パスワードを前記或るアプリケーションの入力領域に貼り付ける貼り付け手段と、を備えることを特徴とするパスワード管理装置が提供される。
【００１１】
また、本発明によれば、暗号鍵を用いてアプリケーション毎のアプリケーション用パスワードを暗号化する暗号化ステップと、暗号化されたアプリケーション用パスワードをアプリケーション毎に第１の記憶手段に格納するパスワード格納ステップと、或るアプリケーションに対応した暗号化されたアプリケーション用パスワードが前記第１の記憶手段から読み出された時に、読み出された、暗号化されたアプリケーション用パスワードを第２の記憶手段に記憶させる記憶ステップと、前記第２の記憶手段に記憶された、暗号化されたアプリケーション用パスワードを前記暗号鍵に対応した復号鍵で復号する復号ステップと、復号されたアプリケーション用パスワードを前記或るアプリケーションの入力領域に貼り付ける貼り付けステップと、を備えることを特徴とするパスワード管理方法が提供される。
【００１２】
更に、本発明によれば、暗号鍵を用いてアプリケーション毎のアプリケーション用パスワードを暗号化する暗号化手段と、暗号化されたアプリケーション用パスワードをアプリケーション毎に格納する第１の記憶手段と、或るアプリケーションに対応した暗号化されたアプリケーション用パスワードが前記第１の記憶手段から読み出された時に、読み出された、暗号化されたアプリケーション用パスワードを記憶する第２の記憶手段と、前記第２の記憶手段に記憶された、暗号化されたアプリケーション用パスワードを前記暗号鍵に対応した復号鍵で復号する復号手段と、復号されたアプリケーション用パスワードを前記或るアプリケーションの入力領域に貼り付ける貼り付け手段と、を備えることを特徴とするパスワード管理装置としてコンピュータを機能させるためのパスワード管理用プログラムが提供される。
【発明の効果】
【００１３】
本発明によれば、アプリケーションにパスワードを入力する際に、画面上にパスワードが表示されず、さらにメモリ上にパスワードが記憶されている期間を短くすることができる。
【図面の簡単な説明】
【００１４】
【図１】本発明の第１の実施形態の構成を示すブロック図である。
【図２】本発明の第１の実施形態の動作を示す流れ図である。
【図３】本発明の第２の実施形態の構成を示すブロック図である。
【図４】本発明の第２の実施形態の動作を示す流れ図である。
【発明を実施するための形態】

【００１５】
以下、図面を参照して本発明を実施するための形態について詳細に説明する。
【００１６】
本実施形態では、アプリケーション用パスワードを使用する際は、格納用デバイスに格納されている全てのアプリケーション用パスワードを復号し、ユーザはその中から必要なアプリケーション用パスワードを選択し、出力する。
【００１７】
以上の動作により、管理用パスワードさえ覚えれば、アプリケーションごとに異なるアプリケーション用パスワードをそれぞれ覚えることなく、各アプリケーションを利用することができる。
【００１８】
図１は、本発明を実施するための第１の実施の形態の構成を示すブロック図である。
【００１９】
図１を参照すると、本発明の第１の実施の形態は、パスワード管理装置１と、キーボード等の入力装置２と、ＨＤＤ等の記憶装置３とを含む。なお、パスワード管理装置１は、コンピュータをパスワード管理装置１として機能させるためのプログラムをコンピュータが読み込んで実行することによっても実現することができる。
【００２０】
パスワード管理装置１は、アプリケーション用パスワードを暗号化するための暗号化鍵と復号するための復号鍵を格納するための暗号鍵格納部１０と、アプリケーション用パスワードを暗号化して記憶装置３へ格納する暗号化処理部１１と、暗号化されたアプリケーション用パスワードのコピーペースト処理を行なうコピー処理部１２とを含む。
【００２１】
暗号鍵格納部１０は、ＨＤＤといった内部記憶装置のほか、ＩＣカードといった外部記憶装置を利用してもかまわない。
【００２２】
暗号化処理部１１は、入力装置２から入力されたアプリケーション毎のアプリケーション用パスワードを暗号化する暗号化部１１１と、暗号化されたアプリケーション用パスワードにパスワード管理装置１によって暗号化されたことを示す識別情報を付与し、アプリケーション毎に、記憶装置３に格納する識別情報付与装置１１２とを含む。この結果、記憶装置３には、アプリケーション毎のアプリケーション用パスワードが、暗号化され、且つ、暗号化されたことを示す識別情報が付与された状態で格納されることとなる。また、アプリケーション毎のアプリケーション用パスワードは、記憶装置３の内部でアプリケーションとの対応が付けられることとなる。
【００２３】
暗号化部１１１は、暗号鍵格納部１０から暗号化鍵を取得し、入力装置２から入力されたアプリケーション用パスワードを暗号化する。アプリケーション用パスワードとしては文字列以外にも、画像、音声等コンピュータ上で扱われるデータも利用可能である。また、暗号化鍵はＲＳＡ暗号のような非対称鍵暗号方式の暗号鍵でも、ＤＥＳ暗号のような対称鍵暗号方式の暗号鍵でもどちらでもかまわない。
【００２４】
識別情報付与部１１２は、暗号化部１１１で暗号化されたアプリケーション用パスワードにパスワード管理装置１によって暗号化されたことを識別するための識別情報を付与し、記憶装置３に格納する。識別情報は、例えば暗号化されたアプリケーション用パスワードが"HIMITSU"の場合に、識別情報"ENC"を文字列の前に付与し、"ENCHIMITSU"のようにして記憶装置３に格納する。識別情報がパスワード管理装置１によって暗号化されたことを識別可能とするものであれば、その付与の方法は問わない。
【００２５】
コピー処理部１２は、コピー用データを記憶するコピーデータ記憶部１２１と、コピーデータをコピーデータ記憶部１２１に書き込むコピーデータ書き込み部１２２と、コピー

データが暗号化されているかを識別する暗号化識別部１２３と、暗号化されたコピーデータから暗号化されたアプリケーション用パスワードのみに識別情報を削除した後に、コピーデータを復号する復号部１２５と、復号する際にユーザに管理用パスワードの入力を要求し、入力された管理用パスワードと予め保持している管理パスワードの対応データとの対応関係を確認することにより、ユーザ認証をするユーザ認証部１２４と、復号されたデータをアプリケーションが提供する入力領域（例えば、パスワード入力のためのテキストボックス）にペーストするコピーデータ貼り付け部１２６とを含む。

【００２６】

コピーデータ記憶部１２１は、コピーされたデータを記憶する。コピーデータ記憶部１２１は通常メモリ上に実装され、通常、クリップボードと呼ばれている機能と同様の機能を有する。コピーデータ記憶部１２１は、オペレーティングシステムや通常のアプリケーションがアクセスできない領域（例えば、メインメモリやハードディスクとは別のメモリ）に設けてもよい。

【００２７】

コピーデータ書き込み部１２２は、ユーザがキーボードやマウス等でコピーコマンドを実行した時に、コピーされたデータをコピーデータ記憶部１２１に書き込む。ここで、コピーされたデータとは、記憶部３に格納されていたアプリケーション用パスワードである。アプリケーション用パスワードが暗号化されていても、ユーザが利用しようとするアプリケーションに対応するアプリケーション用パスワードを利用者が識別してコピーできるようにするためには、例えば、画面にアプリケーションの名称とアプリケーション用パスワードとが組になったテーブルを画面に表示し、そのテーブルからユーザがアプリケーション用パスワードをコピーできるようにする。

【００２８】

暗号化識別部１２３は、ユーザがキーボードやマウス等でペーストコマンドを実行した時に、コピーデータ記憶部１２１に記憶されているコピー用データに、暗号化処理部１１１によって識別情報が付与されているかをチェックする。暗号化処理部１１１によって識別情報が付与されていることを検出したならば、コピー用データは暗号化されていると判断する。

【００２９】

ユーザ認証部１２４は、暗号化されたコピーデータがユーザが作成したデータであることを確認するために、画面にダイアログを出すなどして、ユーザに管理用パスワードの入力を要求する。

【００３０】

復号部１２５は、ユーザ認証部１２４によってユーザの確認が出来たら、暗号鍵格納部１０から暗号化部１１１が利用した暗号鍵に対応した復号鍵を取得し、暗号化されたコピーデータを復号する。

【００３１】

コピーデータ貼り付け部１２６は、復号されたコピーデータを、ペースト先であるアプリケーションが提供する入力領域に貼り付ける。

【００３２】

次に、図１及び図２を参照して本実施の形態の全体の動作について詳細に説明する。

【００３３】

暗号化部１１１は入力装置２から入力されたアプリケーション用パスワードを、暗号化鍵格納部１０から取得した暗号鍵で暗号化する（ステップＳ１０１）。次に識別情報付与部１１２は、暗号化された文字列にパスワード管理装置１によって暗号化されたことを識別するための識別情報を付与する（ステップＳ１０２）。

【００３４】

続いて、ユーザがコピー操作を行なった時、コピーデータ書き込み部１２２は、コピーデータをコピーデータ記憶部１２１に格納する（ステップＳ２０１）。

【００３５】

続いて、ユーザがペースト操作を行なった場合、暗号化識別部１２３はコピーデータ記憶部１２１から取得したコピーデータに識別情報付与部１１２で付与した識別情報があるか判別する（ステップＳ３０１、Ｓ３０２）。暗号化されている場合、ユーザ認証部１２４はユーザに対して管理用パスワードを要求しユーザ認証を行なう（ステップＳ３０３）。ユーザ認証が完了したら復号部１２５は、暗号鍵格納部１０から復号鍵を取得してコピーデータ記憶部１２１から取得したコピーデータの復号を行う（ステップＳ３０４）。コピーデータ貼り付け部１２６は復号されたデータをアプリケーションにペーストする（ステップＳ３０５）。

【００３６】

次に、発明を実施するための第２の形態について図面を参照して詳細に説明する。

【００３７】

図３を参照すると、本発明の第２の発明を実施するための形態は、図１に示された第１の実施の形態の構成に加え、パスワード管理装置４が、ハッシュ値格納部４３と、ハッシュ生成部４１３と、を有する点で異なる。なお、パスワード管理装置４は、コンピュータをパスワード管理装置４として機能させるためのプログラムをコンピュータが読み込んで実行することによっても実現することができる。

【００３８】

ハッシュ値格納部４３は、暗号化されたアプリケーション用パスワードのハッシュ値をアプリケーション毎に格納する。

【００３９】

ハッシュ生成部４１３は、暗号化部１１１で暗号化されたアプリケーション用パスワードのハッシュ値を生成し、ハッシュ値格納部４３に格納する。ハッシュ値の生成にはＭＤ５やＳＨＡ－１や、その他ハッシュ関数を用いる。

【００４０】

また、ユーザ認証部４２４は、ユーザから入力された管理用パスワードを暗号化し、さらにハッシュ値を生成し、ハッシュ値格納部４３に同値のハッシュ値があるかを検索する。同値のハッシュ値が存在する場合、ユーザをアプリケーション用パスワードの所有者であると認証する。

【００４１】

これにより、ユーザは唯一の管理用パスワードを記憶しなくても、複数のアプリケーション用パスワードのうちの一つを管理用パスワードとして記憶していれば、記憶していない他のアプリケーション用パスワードを安全にパスワード入力欄にコピーペーストすることができる。

【００４２】

次に、図３及び図４を参照して本実施の形態の全体の動作について詳細に説明する。

【００４３】

暗号化部１１１は入力装置２から入力されたアプリケーション用パスワードを、暗号化鍵格納部４０から取得した暗号鍵で暗号化する（ステップＳ４０１）。次に、ハッシュ生成部４１３は、Ｓ４０１にて暗号化されたアプリケーション用パスワードのハッシュを生成し、ハッシュ値格納部４３に格納する（ステップＳ４０２）。次に、識別情報付与部１１２は、暗号化された文字列に装置固有の識別文字列を付与する（ステップＳ４０３）。

【００４４】

データのコピー処理は、図２のステップＳ２０１と同一であるため、説明を省略する。

【００４５】

また、データのペースト処理は図２のステップＳ３０１からＳ３０５までと同一のため、説明を省略する。

【００４６】

また、識別情報付与部１１２は、暗号化されたアプリケーション用パスワードのみに識別情報を付与する代わりに、暗号化されなかったアプリケーション用パスワードのみに識別情報を付与してもよい。この場合、暗号化識別部１２３は、暗号化処理部１１１によっ

て識別情報が付与されていないことを検出したならば、コピー用データは暗号化されていると判断する。

【００４７】

更に、識別情報付与部１１２は、暗号化されたアプリケーション用パスワードのみに識別情報を付与する代わりに、暗号化されたか、されなかったを示す識別情報を暗号化されたアプリケーション用パスワード及び暗号化されなかったアプリケーション用パスワードに付与しても良い。この場合、暗号化識別部１２３は、暗号化処理部１１１によって識別情報の内容を検査することにより、コピー用データが暗号化されているか否かを判断する。

【００４８】

なお、全てのアプリケーション用パスワードが暗号化されるのであれば、識別情報付与部１１２は、暗号化されたアプリケーション用パスワードに識別情報を付加する必要はなく、また、暗号化識別部１２３により、アプリケーション用パスワードが暗号化されているかどうかを識別する必要はなく、ステップＳ１０１、Ｓ３０１、Ｓ３０２は省略される。

【００４９】

以上説明したように、本実施形態の第１のパスワード管理装置は、アプリケーション用パスワードを暗号化する暗号処理部と、アプリケーション用パスワードのコピーペースト処理を行なうコピー処理部とを含む。

【００５０】

暗号処理部は、アプリケーション用パスワードを暗号化する暗号化部と、暗号化されたアプリケーション用パスワードに装置固有の識別情報を付与する識別情報付与部とを含む。

【００５１】

コピー処理部は、コピーデータを記憶するコピーデータ記憶部と、コピーデータに本発明のパスワード管理装置固有の識別情報が付与されているかを判別する暗号化識別部と、暗号化されているアプリケーション用パスワードを復号する復号部とを含む。

【００５２】

このような構成を採用し、ユーザは普段利用するアプリケーションを利用するためのアプリケーション用パスワードを暗号処理部で暗号化、識別情報付与をして、記憶装置に記憶する。

【００５３】

続いて、アプリケーション利用時にアプリケーション用パスワードを入力する際には、記憶装置に記憶されている暗号化されたアプリケーション用パスワードに対してコピー操作を実行し、アプリケーション上の貼り付けを行ないたい箇所でペースト操作を実行する。コピー処理部は、ペースト処理実行時に暗号化されたアプリケーション用パスワードかどうかの判別を行い、暗号化されたアプリケーション用パスワードであれば復号し、ユーザの指定する箇所に復号したアプリケーション用パスワードを貼り付ける。

【００５４】

すなわち、暗号化されたままデータをクリップボードへ格納し、ペースト処理がユーザによって要求されてから、復号を行なってアプリケーションに貼り付ける。また、暗号化データを格納するための専用の記憶装置を必要とせず、復号を開始するためのトリガーを貼り付け処理にしている。

【００５５】

従って、アプリケーションにアプリケーション用パスワードを入力する際に、画面上にアプリケーション用パスワードが表示されず、さらにメモリ上にアプリケーション用パスワードが記憶されている期間を短くすることができるという効果（暗号化されたデータを復号して貼り付ける際に復号されたデータがコンピュータ上のメモリと記憶装置に記憶されている時間を短くできるという効果）、及び、従来のコピーペーストを行なう際と同様のユーザ操作によって暗号化されたアプリケーション用パスワードを復号してペーストす

ることができるという効果（通常のデータをコピーペーストするのとほとんど同様の動作で暗号化データをコピーペーストすることができるという効果）が得られる。

【００５６】

また、本実施形態の第２のパスワード管理装置は、第１のパスワード管理装置の構成に加え、ハッシュ値を格納するハッシュ値格納部を備え、暗号処理部は、暗号化処理部が暗号化したアプリケーション用パスワードのハッシュ値をハッシュ値格納部に格納するハッシュ生成部とを含む。

【００５７】

また、ユーザ認証部は、ユーザから入力された管理用パスワードを暗号化し、ハッシュを生成して、ハッシュ値格納部に同値のハッシュ値が存在するかを検索する。

【００５８】

すなわち、暗号化したアプリケーション用パスワードのハッシュ値を保存しておき、コピーデータのペースト時に入力されたアプリケーション用パスワードを暗号化し、ハッシュ生成した値がいずれかに一致するかによってユーザ認証を行なう。

【００５９】

従って、ユーザの保有するアプリケーション用パスワードのうちのいずれかを覚えていれば、アプリケーション用パスワードのコピーペーストを安全に行なうことができるという効果（ユーザの保有するアプリケーション用パスワードのうちのいずれかを覚えていれば、アプリケーション用パスワードのコピーペーストを安全に行なうことができるという効果）が得られる。

【産業上の利用可能性】

【００６０】

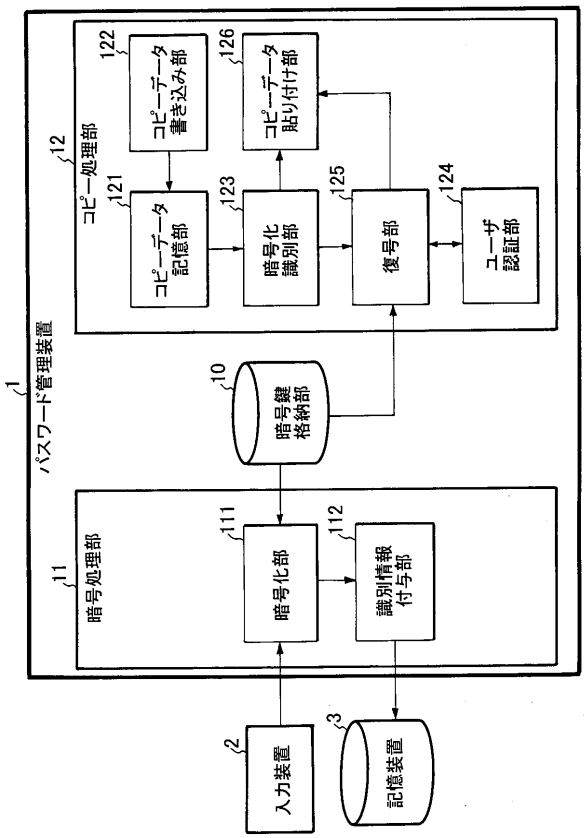
本発明は、アプリケーション用パスワードを安全にコピーペーストするパスワード管理装置や、パスワード管理装置をコンピュータに実現するためのプログラムといった用途に適用できる。

【符号の説明】

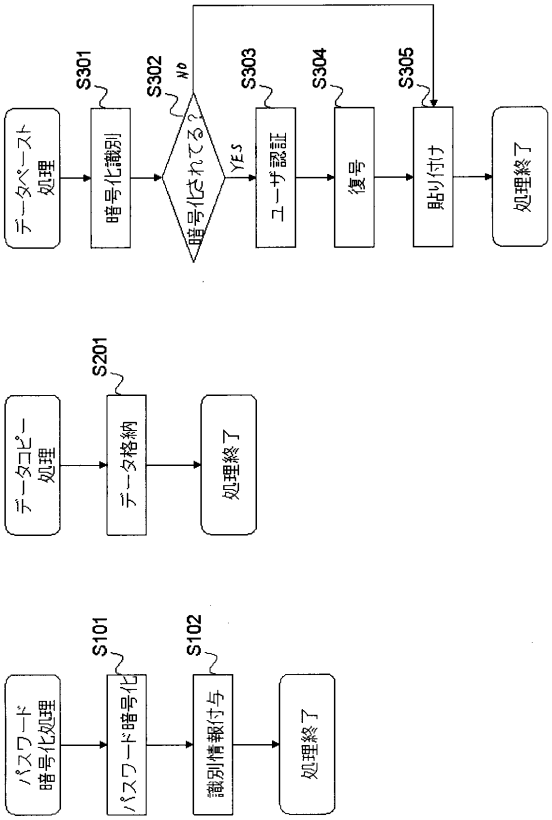
【００６１】

１　パスワード管理装置
１０　暗号鍵格納部
１１　暗号処理部
１１１　暗号化部
１１２　識別情報付与部
１２　コピー処理部
１２１　コピーデータ記憶部
１２２　コピーデータ書き込み部
１２３　暗号化識別部
１２４　ユーザ認証部
１２５　復号部
１２６　コピーデータ貼り付け部
２　入力装置
３　記憶装置
４　パスワード管理装置
４０　暗号鍵格納部
４１　暗号処理部
４１３　ハッシュ生成部
４２　コピー処理部
４２４　ユーザ認証部
４３　ハッシュ値格納部

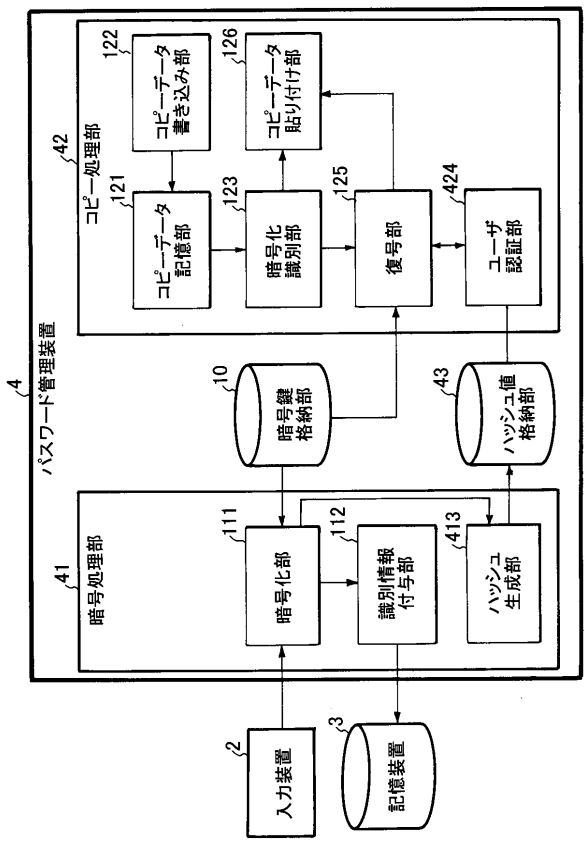
【図１】


1
パスワード管理装置
11
暗号処理部
111
暗号化部
112
識別情報付与部
12
コピー処理部
121
コピーデータ記憶部
122
コピーデータ書き込み部
123
暗号化識別部
124
ユーザ認証部
125
復号部
126
コピーデータ貼り付け部
10
暗号鍵格納部
2
入力装置
3
記憶装置

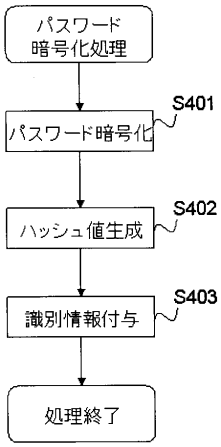
【図２】


データベース処理
S301
暗号化識別
S302
No
暗号化されてる？
YES
S303
ユーザ認証
S304
復号
S305
貼り付け
処理終了
データコピー処理
S201
データ格納
処理終了
パスワード暗号化処理
S101
パスワード暗号化
S102
識別情報付与
処理終了

【図３】


4
パスワード管理装置
41
暗号処理部
111
暗号化部
112
識別情報付与部
413
ハッシュ生成部
42
コピー処理部
121
コピーデータ記憶部
122
コピーデータ書き込み部
123
暗号化識別部
125
復号部
424
ユーザ認証部
126
コピーデータ貼り付け部
10
暗号鍵格納部
43
ハッシュ値格納部
2
入力装置
3
記憶装置

【図４】


パスワード暗号化処理
パスワード暗号化
S401
ハッシュ値生成
S402
識別情報付与
S403
処理終了