(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2006-343875
(P2006-343875A)
(43)公開日　平成18年12月21日(2006.12.21)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/24	(2006.01)	G06F	12/14	530D	5B017
G06F 12/00	(2006.01)	G06F	12/00	537D	5B082

審査請求 未請求　請求項の数 10　ＯＬ　（全 17 頁）

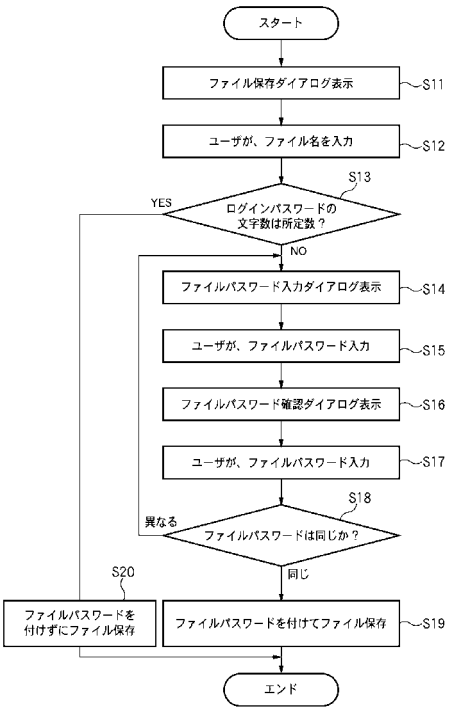
(21)出願番号　特願2005-167371 (P2005-167371)
(22)出願日　平成17年6月7日 (2005.6.7)

(71)出願人　000001007
キヤノン株式会社
東京都大田区下丸子３丁目３０番２号
(74)代理人　100076428
弁理士　大塚　康徳
(74)代理人　100112508
弁理士　高柳　司郎
(74)代理人　100115071
弁理士　大塚　康弘
(74)代理人　100116894
弁理士　木村　秀二
(72)発明者　木村　裕行
東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内

Ｆターム(参考)　5B017 AA03　BA05　CA16
5B082 GA13　HA08

(54)【発明の名称】情報処理装置及びその制御方法、並びにコンピュータプログラム及びコンピュータ可読記憶媒体

(57)【要約】
【課題】　ログイン時に入力するログインパスワードの文字数に応じて、セキュリティに関する動作環境を切り替える。
【解決手段】　装置には、ユーザＩＤと所定数を越える文字のログインパスワードを登録しておく。そして、ログインする際には、登録されたログインパスワードの全文字を入力してログインしたのか、その一部の所定数の文字で構成されるログインパスワードでログインしたのかを判定するため、ログイン時に入力したログインパスワードの文字数を記憶する。ログイン後、アプリケーションを利用したファイルを保存する場合、ログインパスワードの文字数を判定する（Ｓ１３）。所定数の文字数でログインした場合には、そのまま保存する（Ｓ２０）。一方、所定数を越えるログインパスワードでログインした場合には、保存するファイルに対してファイルパスワードを設定するためのダイアログ表示を行い（Ｓ１４）、ファイルパスワード付きで保存する（Ｓ１９）。
【選択図】　図９



【特許請求の範囲】
【請求項１】
ユーザにユーザＩＤ及びログインパスワードを入力させて、処理を行うことが可能な情報処理装置であって、
ログイン時に入力したログインパスワードの文字列を構成する文字数を記憶する記憶手段と、
記憶された文字数に応じて、ログイン後のセキュリティに関する動作環境を切り替える切り替え手段と
を備えることを特徴とする情報処理装置。
【請求項２】
前記切り替え手段は、前記ログインパスワードの文字数が所定数を越える場合には、ファイル保存処理時に、ファイルパスワードの設定を促すダイアログ表示を自動表示するモードに切り替え、前記ログインパスワードの文字数が前記所定数以下である場合にはファイルパスワードの設定を促すダイアログ表示を行わないで保存するモードに切り替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】
前記切り替え手段は、前記ログインパスワードの文字数が所定数を越える場合には、ファイル保存処理時に、暗号化処理を行うモードに切り替え、前記ログインパスワードの文字数が前記所定数以下である場合には暗号化しないで保存するモードに切り替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４】
更に、スクリーンセーバを実行するスクリーンセーバ手段を備え、
前記切り替え手段は、前記ログインパスワードの文字数が所定数以下である場合にはスクリーンセーバが起動開始するまでの時間として第１の期間を設定するモードに切り替え、前記ログインパスワードの文字数が前記所定数を越える場合には前記第１の期間よりも短い第２の期間を設定するモードに切り替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５】
更に、スパイウェアを駆除する処理を実行するスパイウェア駆除手段を備え、
前記切り替え手段は、前記ログインパスワードの文字数が所定数を越える場合には前記スパイウェア駆除手段をログイン直後に実行するモードに切り替え、前記ログインパスワードの文字数が前記所定数以下である場合には前記スパイウェア駆除手段を実行しないモードに切り替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６】
更に、外部記憶メディアへの書き込みを禁止する書き込み禁止手段を備え、
前記切り替え手段は、前記ログインパスワードの文字数が所定数を越える場合には前記書き込み禁止手段をログイン直後に実行するモードに切り替え、前記ログインパスワードの文字数が前記所定数以下である場合には、前記書き込み禁止手段を実行しないモードに切り替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７】
更に、所定の記憶装置に、操作履歴のログを生成するログ記録手段を備え、
前記切り替え手段は、前記ログインパスワードの文字数が所定数を越える場合には前記ログ記録手段をログイン直後に開始するモードに切り替え、前記ログインパスワードの文字数が前記所定数以下である場合には、前記ログ記録手段を実行しないモードに切り替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８】
ユーザにユーザＩＤ及びログインパスワードを入力させて、処理を行うことが可能な情報処理装置の制御方法であって、
ログイン時に入力したログインパスワードの文字列を構成する文字数を記憶する記憶工程と、

記憶された文字数に応じて、ログイン後のセキュリティに関する動作環境を切り替える切り替え工程と
を備えることを特徴とする情報処理装置の制御方法。
【請求項９】
ユーザにユーザＩＤ及びログインパスワードを入力させて、処理を行うことが可能な情報処理装置として機能するコンピュータプログラムであって、
ログイン時に入力したログインパスワードの文字列を構成する文字数を記憶する記憶手段と、
記憶された文字数に応じて、ログイン後のセキュリティに関する動作環境を切り替える切り替え手段
が機能することを特徴とするコンピュータプログラム。
【請求項１０】
請求項９に記載のコンピュータプログラムを格納したことを特徴とするコンピュータ可読記憶媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、コンピュータシステムにおけるファイルを管理する技術に関するものである。
【背景技術】
【０００２】
通常、パーソナルコンピュータ（以下、単にコンピュータ）が有するハードディスク装置等の記憶装置には、様々なファイルが格納されている。このファイルには、そのユーザにとって機密度が高いファイル、あまり機密度が高くないファイルがある。従って、ユーザが機密度が高いファイルを自分のコンピュータに保存する場合には、そのファイルの安全性を高める為にファイルに対してパスワードを付けることを行っていた（例えば特許文献１参照）。
【０００３】
以下、従来行われていた所定のアプリケーションプログラム上で、ユーザが作成したファイルにパスワードを付けてコンピュータに保存する方法を説明する。
【０００４】
図１は、ユーザが作成したファイルの保存を行おうとした際に、アプリケーションプログラムで表示されるファイル保存のダイアログである。なお、このファイル保存ダイアログの一般的な機能に関しては公知であるので、ここでは簡単に説明する。
【０００５】
図１のファイル保存ダイアログには、パスワード保存チェックボックスボックス１が設けられている。ユーザはファイルを保存する際にパスワードを付けたい場合は、このパスワード保存チェックボックス１をチェックする。具体的には、マウス等のポインティングデバイスに連動するカーソルをこのチェックボックス１に移動し、ポインティングデバイスに設けられたボタンを押下する操作する（これ以降、この操作を単に「クリック」あるいは「クリックする」と表現する）。
【０００６】
この後、保存ボタンをクリックすると、図２に示したパスワード設定ダイアログが表示される。パスワード設定ダイアログの中にはパスワード入力エリア２があり、ユーザはここに設定したいパスワードを入力する。入力したパスワードは、通常「＊」で表示され、他人に盗み見されても内容が判らない様になっている。パスワードの入力が終わったら、ユーザは「ＯＫ」ボタン３を押す。すると今度は、図３に示したパスワード確認ダイアログが表示されて、パスワードの再入力が求められる。これは、パスワード設定ダイアログ内のパスワード入力エリア２に入力したパスワードが「＊」で表示されていてユーザ本人にも読めない為、再度パスワードを入力して入力の正しさを確認する目的で行われる。こ

の為、ユーザはパスワード入力エリア６に再度パスワードを入力して、「OK」ボタン７を押すことになる。

【０００７】

この結果、最初に入力したパスワードと、確認するために入力されたパスワードが一致していれば、保存対象のファイルをそのパスワードでないとオープンできないようにする処理を行ない、保存することになる。

【０００８】

なお、保存するファイルの機密度がそれほど高くなく、ユーザがパスワードを付ける必要がないと考えた場合は、図１のファイル保存のダイアログで、パスワード保存チェックボックス１にチェックを入れずに通常の保存ボタンをクリックすれば良い。この場合には、パスワードの入力が求められることなく、保存処理を行うことになる。

【特許文献１】特開２００４－１６４６０４公報

【発明の開示】

【発明が解決しようとする課題】

【０００９】

さて、上記の従来の方法では、ユーザがパスワードを付けてファイルを保存したい場合に、最初のファイル保存ダイアログでユーザがパスワード保存チェックボックス１にチェックを入れる操作が必要なので、余計な手間がかかってしまう。また、ユーザがパスワード保存チェックボックス１にチェックを入れるのを忘れて、ファイル保存の操作を行ってしまうと、パスワードを付けていない安全性の低いファイルが保存されてしまう問題がある。

【００１０】

また、図４に示す様に、図１のファイル保存ダイアログにあるパスワード保存チェックボックス１を付けない様に構成して、ユーザがファイル保存の操作を行った際、必ず図２のパスワード設定ダイアログを出す方法も考えられる。この場合、パスワードを付けて保存したいユーザにとっては、パスワード保存チェックボックス１にチェックを入れる手間から開放されるし、パスワードを付けずにファイルが保存されることもなくなる。しかし、逆に、機密度が高くない為パスワードを付けずにファイルを保存したい場合には、図２のパスワード設定ダイアログの中の「キャンセル」ボタン４、または図３のパスワード確認ダイアログの中の「キャンセル」ボタン８を押して、ファイルにパスワードを付けないことを指示する必要が生じ、これが手間になってしまう問題点があった。

【００１１】

本発明はかかる問題点に鑑みなされたものであり、コンピュータの動作環境を、ログインする際に入力するパスワードの文字数に応じて決定する技術を提供しようとするものである。

【課題を解決するための手段】

【００１２】

この課題を解決するため、例えば本発明の情報処理装置は以下の構成を備える。すなわち、

ユーザにユーザＩＤ及びログインパスワードを入力させて、処理を行うことが可能な情報処理装置であって、

ログイン時に入力したログインパスワードの文字列を構成する文字数を記憶する記憶手段と、

記憶された文字数に応じて、ログイン後のセキュリティに関する動作環境を切り替える切り替え手段とを備える。

【発明の効果】

【００１３】

本発明によれば、ログイン時に入力するログインパスワードの文字数に応じて、動作環境が切り替えることが可能になる。

【発明を実施するための最良の形態】

【００１４】
以下、添付図面に従って本発明に係る実施形態を詳細に説明する。
【００１５】
＜第１の実施形態＞
先ず、以下の説明では、パスワードには、ＰＣにログインする際に入力するパスワードと、ファイルに付けるパスワードの記載がでてくる。混乱を防ぐ為に、前者をログインパスワード、後者をファイルパスワードと呼ぶことにする。
【００１６】
図５は実施形態におけるＰＣのブロック構成図である。図中、１０１は装置全体の制御を司るＣＰＵであり、１０２はＢＩＯＳやブートプログラムを格納しているＲＯＭ、１０３はＣＰＵ１０１のワークメモリとして使用されるＲＡＭである。１０４はハードディスク装置（ＨＤＤ）であり、ここにはＯＳ１０４ａ、各種アプリケーション１０４ｂ、本装置を利用するユーザのユーザＩＤとそのログインパスワードを格納しているログインパスワードファイル１０４ｃ、並びに、ログインに成功した際に入力したログインパスワードの文字数を格納するためのログインパスワード文字数ファイル１０４ｄが格納されている。なお、各アプリケーションで作成されたファイルもこのＨＤＤ１０４に格納されることになる。
【００１７】
１０５はキーボード、１０６はマウス等のポインティングデバイスである。１０７は表示制御部であって、ＣＰＵ１０１からの制御に基づいて内部にあるビデオメモリに描画し、ビデオメモリのデータを読出し表示装置１０８にビデオ信号として出力する。表示装置１０８はＣＲＴ、液晶等の表示装置である。１０９はネットワークインターフェースである。
【００１８】
上記構成において、本装置に電源が投入されると、ＣＰＵ１０１はＲＯＭ１０２に格納されたブートプログラムを実行し、ＨＤＤ１０４からＲＡＭ１０３にＯＳをロードし、ユーザログイン画面を表示し、ユーザＩＤとログインパスワードの入力画面を表示制御部１０７を介して表示装置１０８に表示することになる。正規なユーザがログインすると、各種アプリケーションを利用した作業に移ることが可能になる。
【００１９】
ここで、ログインパスワードファイル１０４ｃの一例を図６に示す。図示のように、ログインパスワードファイルは、ユーザＩＤ２１とログインパスワード２２が対になって登録されている。なお、ユーザＩＤはユニークである必要がある。また、実施形態では、一人のユーザを登録する際のログインパスワードは必ず１０文字以上の長さで登録するものとする（それ以下では登録できないものとする）。なお、詳細は後述するが、登録したログインパスワードは、その全ての文字列を用いてログインする場合と、先頭から所定数の文字数（実施形態では７文字とする）でログインする場合の２通りが存在する。
【００２０】
図７は、実施形態におけるＰＣのＯＳが起動した際の、コンピュータログイン処理を示すフローチャートである。
【００２１】
先ず、ステップＳ１において、表示装置１０８にログインダイアログを表示する。このログインダイアログは、例えば図８に示す通りであり、ユーザＩＤ入力欄３１、ログインパスワード入力欄３２、及びＯＫボタン３３等で構成される。
【００２２】
次いで、ステップＳ２において、ユーザからキーボード１０５を用いて、ユーザＩＤ、ログインパスワードが入力され、ＯＫボタン３３が押下されるのを待つ。ＯＫボタン３３が押下されると、ステップＳ３に進んで、ログインパスワード入力欄３２に入力されたログインパスワードを構成する文字数Ｎを、ＨＤＤ１０４のログインパスワード文字数ファイル１０４ｄに格納する。

【００２３】
次いで、ステップＳ４に進んで、ログインパスワードファイル１０４ｃ内から、ログインダイアログのユーザＩＤ欄３１に入力されたユーザＩＤと一致するユーザＩＤのログインパスワードを読出す。そして、読出したログインパスワードと、ログインダイアログのログインパスワード入力欄３２で入力されたパスワードが一致するか否かを判断する。ここで、ログインパスワードが一致するか否かの判断であるが、入力したログインパスワードの文字列が、登録されたログインパスワードと一致する場合は勿論、入力されたログインパスワードの先頭から７文字が、登録ログインパスワードの先頭から７文字と一致している場合には、正規ユーザのログインであると判定する。それ以外のパスワード不一致の場合、及び、ログインダイアログのユーザＩＤ欄３１に入力されたユーザＩＤが、ログインパスワードファイル１０４ｃ内に存在しない未登録ユーザの場合には、正規ユーザのログインではないと判断する。

【００２４】
正規ユーザのログインではないと判断した場合には、ステップＳ５に進んで認証が失敗した旨のエラー表示を行ない、ステップＳ１に戻る。

【００２５】
また、正規ユーザのログインと判断した場合には、ステップＳ６に進んで、コンピュータの利用できる状態に移行する。

【００２６】
上記ログイン操作において、アプリケーションを利用して、機密性の高いファイルを作成・編集する場合には、所定文字数（閾値＝７文字）よりも長いログインパスワードの全文字とユーザＩＤを使ってログインする。また、機密性が問われないようなファイルを作成・編集する場合には、７文字のログインパスワードとユーザＩＤを使ってログインする。いずれの場合であっても、先に説明したように、ステップＳ３にて、パスワードの文字数ＮがＨＤＤ１０４の所定エリアに格納されるので、実施形態で説明するアプリケーションと同等の機能を持つアプリケーションであれば、ファイルを保存する際、ログインパスワード文字数ファイル１０４ｄを調べて、機密性の高いファイルを保存するのか、機密性を問わないファイルを保存するのかを判定可能とし、それに応じたＧＵＩを使ったファイルを保存する。

【００２７】
実施形態におけるアプリケーションは、文書編集、画像編集等の種類を問わないので、その詳細については省略する。ここでは、そのアプリケーションで作成した、或いは、編集したファイルを保存指示した際の処理を、図９のフローチャートに従って説明する。

【００２８】
先ず、ステップＳ１１でファイル保存ダイアログを表示装置１０８に表示する。この場合に表示されるファイル保存ダイアログは図４に示すもので良い。

【００２９】
次に、ステップＳ１２では、ユーザがファイル保存ダイアログに保存するフォルダを選択して保存するファイル名を入力し、保存ボタンをクリックする。ただし、既存のファイルを編集した場合には、デフォルトでそのファイル名が、そのパス位置に保存するものとして設定された上で表示する。従って、この場合には単に保存ボタンをクリックすればよい。ファイル名を変えたければ、その名前を変更して、保存ボタンをクリックする。

【００３０】
いずれにしても、保存ボタンがクリックされ、保存するファイル名（及び格納位置）が決定すると、処理はステップＳ１３に進み、ＨＤＤ１０４内のログインパスワード文字数ファイル１０４ｄを調べて、ユーザが本装置にログインした際のログインパスワードの文字数Ｎを取得し、その文字数と閾値（実施形態では７文字）とを比較する。

【００３１】
この比較により、文字数Ｎが閾値と同じであると判断した場合には、ステップＳ２０に進み、ファイルパスワードを付けずにファイルの保存を実行して終了する。

【００３２】
また、ステップＳ１３で、ログインパスワードの文字数が閾値を越えると判断した場合（ログインパスワードとして登録した全文字を用いてログインした場合）には、以下のステップＳ１４以降の処理を行う。
【００３３】
先ず、ステップＳ１４では、図２に示す様なファイルパスワードの入力ダイアログを表示する。次いで、ステップＳ１５では、ユーザによるファイルパスワードの入力と、ＯＫボタンの押下を待つ。ファイルパスワードが入力されると（ＯＫボタンの押下を検出すると）、処理はステップＳ１６に進んで、図３で示す様なファイルパスワードの確認ダイアログを表示する。ステップＳ１７において、ユーザが再度ファイルパスワードを入力を待つ。
【００３４】
ステップＳ１８では、ステップＳ１５、Ｓ１７で入力された２つのファイルパスワードが一致するかどうかを判断する。不一致であると判断した場合には、ステップＳ１４に戻り、再度ファイルパスワードを入力させる。また、２つのファイルパスワードが同じだった場合は、ステップＳ１９に進んで、ファイルパスワードを付けた状態でファイルの保存処理を実行し、本処理を終える。なお、ここで言う「パスワードを付ける」というのは、そのファイルを編集するためにオープンする際、パスワードが一致しない限り、アプリケーションで編集可能状態に読み込めないようにすることを意味する。
【００３５】
なお、上記処理では、ログインパスワード数が閾値と同じ場合には、無条件にファイルパスワードを入力を必要とせず保存処理するものとしたが、ログインパスワード数が閾値以下であっても、ユーザが明示的にファイルパスワードを入力することを指示した場合には、ステップＳ１４以降の処理を実行するようにしてもよい。逆に、ログインパスワード数が閾値を越える場合であっても、ファイルパスワードを設定しないことを明示的に指示した場合には、ステップＳ１４ではなく、ステップＳ２０に進むようにしても良い。つまり、デフォルトとしてファイルパスワードを入力するのか、しないのかをログインパスワードの文字数で決定するようにしても構わない。
【００３６】
次に、上記のようにして保存したファイルに対するアクセスの実際を、具体的に説明する。
【００３７】
なお、ログインパスワードの文字数の判定を行う際、予め定められた所定値が必要となるが、以下の説明では、その所定値を「７」としている。
【００３８】
またログインするユーザは、図３のログインパスワードファイルにあるユーザＩＤ「suzuki-tarou」とし、長いログインパスワードを使う場合は１０文字全てを使ったログインパスワード「abcde12345」を入力し、短いログインパスワードを使う場合は７文字分のログインパスワード、つまり「abcde12」を入力するものとする。
【００３９】
ユーザは、コンピュータにログインしようとすると、図７のステップＳ１で、図８に示されるログインダイアログが表示される。次のステップＳ２で、ユーザは図８のログインダイアログのユーザＩＤ入力エリア３１にユーザＩＤ「suzuki-tarou」を入力する。また、ログインパスワード入力エリア３２にはログインパスワードを入力するが、もしユーザは機密度の高いファイルを作成して保存しようと考えているのであれば、登録されたログインパスワードの全文字「abcde12345」を入力することになる。また、さほど機密性を問わないファイルを作成する場合は、７文字のパスワード「abcde12」を入力する。
【００４０】
次にステップＳ３で、ログインパスワードの文字数すなわち、「１０」または「７」がログインパスワード文字数ファイル１０４ｄに保存される。

【００４１】
次に、ステップＳ４で、入力されたユーザＩＤとログインパスワードが登録されたものと一致するかが判断され、ユーザのコンピュータ利用が可能になるのである。
【００４２】
この後、ユーザはこのコンピュータのアプリケーションを使って、データファイルを作成したり、編集したりすることが可能になる。そして、そのアプリケーションでファイルとして保存しようとした場合、図９のステップＳ１１で、図４に示されるファイル保存ダイアログが表示される。次にステップＳ１２で、ユーザは図４のファイル保存ダイアログに保存したいフォルダを選択して、保存したいファイル名を入力する。次にステップＳ１３で、ログインパスワード文字数ファイル１０４ｄに保存されたログインパスワードの文字数が「７」であるか否かを判断する。７文字のログインパスワードを用いてログインしたと判断した場合には、ステップＳ２０でそのままファイルの保存処理を行う。つまり、さほど機密性を問わないファイルを作成するためにログインした場合には、無条件に保存処理を行う。
【００４３】
一方、ログインパスワード文字数ファイル１０４ｄに格納された文字数Ｎが７を越えていると判断した場合には、機密性の高いファイルを作成するためにログインしたことになるので、処理はステップＳ１４に進むことになる。ステップＳ１４では、図２に示されるファイルパスワード入力ダイアログが表示され、ステップＳ１５で、ユーザは設定したいファイルパスワードを入力することになる。次のステップＳ１６では、図３に示されるファイルパスワード確認ダイアログが表示され、ステップＳ１７で、ユーザは設定したいファイルパスワードを再度入力することになる。次のステップＳ１８では、ステップＳ１５で入力されたファイルパスワードとステップＳ１７で再入力されたファイルパスワードとが一致するか比較され、一致した場合は、このファイルパスワードを設定したファイルが、図５のＨＤＤ１０４内に保存される。
【００４４】
以上説明した様に、実施形態によれば、ユーザが機密度の高いファイルを作成するのか否かを、ログインパスワードの文字数の数から判定しているので、ユーザがファイルパスワードの必要性を指示する手順が不要になり、作業性が向上する。また、機密性の高いファイルについて、パスワードを付けるのを忘れて保存してしまう、という問題もなくなる。
【００４５】
＜第２の実施形態＞
次に第２の実施形態を説明する。
【００４６】
本第２の実施形態では、ファイルを保存する際に、その保存対象のファイルについて暗号化するか否かを、ログインパスワードの文字数によって決定することを特徴とする。
【００４７】
なお、本第２の実施形態における装置構成は上記第１の実施形態と同じであるものとする。また、ログイン処理についても第１の実施形態と同じとし、以下では、第２の実施形態のアプリケーションプログラムにおけるファイル保存時の処理を図１０のフローチャートに従って説明する。
【００４８】
先ず、ステップＳ２１でファイル保存ダイアログを表示装置１０８に表示する。この場合に表示されるファイル保存ダイアログは図４に示すもので良い。
【００４９】
次に、ステップＳ２２では、ユーザがファイル保存ダイアログに保存するフォルダを選択して保存するファイル名を入力し、保存ボタンをクリックする。ただし、既存のファイルを編集した場合には、デフォルトでそのファイル名が、そのパス位置に保存するものとして設定された上で表示する。従って、この場合には単に保存ボタンをクリックすればよ

い。ファイル名を変えたければ、その名前を変更して、保存ボタンをクリックする。

【００５０】

いずれにしても、保存ボタンがクリックされ、保存するファイル名（及び格納位置）が決定すると、処理はステップＳ２３に進み、ＨＤＤ１０４内のログインパスワード文字数ファイル１０４ｄを調べて、ユーザが本装置にログインした際のログインパスワードの文字数Ｎを取得し、その文字数が閾値（実施形態では７文字）と比較する。

【００５１】

この比較により、文字数Ｎが閾値と同じであると判断した場合には、ステップＳ２５に進み、そのままファイルを保存する。

【００５２】

また、ステップＳ２３で、ログインパスワードの文字数Ｎが閾値を越えると判断した場合（ログインパスワードとして登録した全文字を用いてログインした場合）には、以下のステップＳ２４以降の処理を行う。

【００５３】

保存すべきデータを暗号化するための暗号化キーを入力するダイアログを表示し、ユーザに暗号化キーを２回入力させる。２回入力するのは、キー入力ミスを除外するためである。２回入力したキーが一致する場合には、入力された暗号化キーに基づいて、保存対象のデータを暗号化し、ファイルとして保存する。

【００５４】

この暗号化されたファイルを、次回、読込む場合には、暗号を解除するためのキー（暗号化する際に用いたキーと同じ）を入力させるダイアログを表示し、正しいキーでない限り暗号復号が行えないようにする。

【００５５】

以上説明したように本第２の実施形態によれば、ユーザが機密度の高いファイルを作成するのか否かを、ログインパスワードの文字数から判定しているので、ユーザが暗号化するか否かを指示する手順が不要になり、作業性が向上する。また、機密性の高いファイルについて、暗号化するのを忘れて保存してしまう、という問題もなくなる。

【００５６】

＜第３の実施形態＞

次に第３の実施形態を説明する。

【００５７】

一般に、パーソナルコンピュータ（ＰＣ）が有するＣＲＴ等の表示装置の焼きつきを防止するため、スクリーンセーバを稼動させることが行われる。このスクリーンセーバは、キーボードやポインティングデバイス等の外部からの指示入力が所定時間経過しても無い場合に実行される（以下、未入力期間という）。

【００５８】

最近では、パスワード付きスクリーンセーバが存在する。これは、スクリーンセーバが一旦その稼動を開始した後は、正しいパスワードを入力しない限り、スクリーンセーバが稼動しつづけるものである。この活用は、ユーザが席を外した場合、他人に作業中であったＰＣの画面をのぞき見されることを防ぐために利用されている。

【００５９】

未入力期間はユーザが自由に設定できることが多いが、余り短くしすぎると、ユーザが思考している最中にスクリーンセーバが稼動を開始してしまい、パスワードの入力作業が必要になってしまい、煩雑になる。それ故、未入力期間は長めに設定することになる。しかしながら、未入力期間を長くする、或いは、スクリーンセーバを起動しないように設定してしまうと、一度、ユーザが席を外した場合に、第３者が作業中の画面をのぞき見できる可能性が高くなり、セキュリティ上の問題がある。

【００６０】

そこで、本第３の実施形態では、かかる問題点を解決するため、ログインした際のログインパスワードの文字数に応じて、未入力期間を設定する例を説明する。

【００６１】
装置構成、並びに、ＰＣへのログイン処理は第１の実施形態と同様であるものとし、以下では、実施形態におけるスクリーンセーバプログラムの処理手順を図１１のフローチャートに従って説明する。
【００６２】
先ず、正常にログインが行われると、ステップＳ３１にて、ＨＤＤ１０４内のログインパスワード文字数ファイル１０４ｄを調べて、ユーザが本装置にログインした際のログインパスワードの文字数Ｎを取得し、その文字数が閾値（実施形態では７文字）と比較する。つまり、短いログインパスワードでログインしたのか、長いログインパスワード（登録したパスワード全文字）でログインしたのかを判断する。長いログインパスワードでログインしたと判断した場合には、ステップＳ３２に進んで、スクリーンセーバ起動時間（未入力期間）Ｔとして１分を設定する。また、短いログインパスワードでログインしたと判断した場合には、ステップＳ３３において、スクリーンセーバ起動時間Ｔとして１０分を設定する。なお、ログインパスワードの文字数と、起動時間Ｔは逆の関係にあれば良く、ここで示した１分、１０分に限るものではない。また、場合によっては、上記条件を満たす限り、ユーザが設定できるようにしても勿論構わない。
【００６３】
処理はいずれの場合にもステップＳ３４に進み、０秒から計時を開始する。そして、次のステップＳ３５で、ＰＣのキーボードやポインティングデバイスからの何らかの入力があったか否かを判定し、何らかの入力があると判断される度にステップＳ３４の処理を行うことで、計時がリセットされる。
【００６４】
また、ステップＳ３５でユーザから何らの指示入力が無いと判断した場合には、ステップＳ３６に進んで、ステップＳ３２、或いは、Ｓ３３で設定された未入力期間Ｔが経過したか否かを判断する。未入力期間Ｔが経過したと判断した場合には、ステップＳ３７に進んで、スクリーンセーバ処理を開始する。なお、スクリーンセーバ処理の解除処理は、公知であるので説明については省略する。ただし、短いログインパスワードでログインした場合には、パスワード無しのスクリーンセーバを稼動し、長いログインパスワードでログインした場合にはパスワード有り（ここでのパスワードとは、スクリーンセーバ用のパスワードのこと。これは、ログインパスワードと同じであることが多い)のスクリーンセーバを稼動するようにしても良い。
【００６５】
以上説明したように本第３の実施形態によれば、ユーザが機密度の高いファイルを作成するため、長いログインパスワードを利用してログインした場合、そのユーザが席を外す等を行った場合には比較的短い期間を経てスクリーンセーバが稼動することになり、第３者にのぞき見される危険性を低くすることが可能になる。
【００６６】
＜第４の実施形態＞
第４の実施形態を説明する。
【００６７】
インターネット接続が容易になってきて、便利になってきているが、その反面、スパイウエアと言われる悪意を持ったソフトが、コンピュータ内に仕組まれると言う事件が発生している。スパイウエアとは、コンピュータに仕込まれて、ユーザの個人情報を盗んでしまうソフトウエアのことで、例えば、スパイウエアの１種であるキー・ロガーと言われるソフトは、ユーザがキーボードから入力する全ての情報を収集し、定期的に特定のサイトに送ってしまう動作を行うので、ユーザが入力する重要なパスワードが盗まれてしまう問題点があった。これに対して、コンピュータ内のスパイウエアを検索して駆除してくれるソフトが開発されたので、これを使用すれば、安心してコンピュータを使える様になっていた。なお、スパイウエア駆除ソフトの詳細に関しては、既に公知であるので、ここでの詳細な説明は省略する。

【００６８】
ところが、この様なスパイウエア駆除ソフトをコンピュータ内に常駐させておくと、常にプロセスとして動作するので、コンピュータのリソースが使われ、他のプロセスの動作性能が落ちてしまう問題点があった。また、常駐を行わせず、必要なときにだけ、コンピュータ内を検索させて駆除させる方法も可能であるが、ユーザがうっかりその操作を忘れて重要なパスワードを入力してしまうと、その情報が盗まれてしまう問題があった。また、ユーザがログインした直後に、検索と駆除を行わせる方法も可能であるが、ユーザが重要な情報にアクセスしない場合でも、検索が行われる間待たされることになり、時間が無駄になってしまう問題がある。
【００６９】
そこで、本第４の実施形態では、特にログイン時にスパイウェア駆除プログラムを自動実行するか否かを、ログインパスワードの文字数に応じて決定する例を説明する。
【００７０】
装置構成は第１の実施形態と同様であるものとし、以下では、本第４の実施形態におけるログイン処理を図１２のフローチャートに従って説明する。なお、第１の実施形態における図７と同じ処理は、同符号を付した。従って以下では、異なる点について説明することとする。
【００７１】
ユーザが正しいユーザＩＤとログインパスワードを入力する（登録したログインパスワード全文字を用いるか、登録された先頭の７文字を利用してログインするかの何れか）と、処理はステップＳ４１に進む。
【００７２】
ステップＳ４１では、ステップＳ３で記憶したログインパスワードの文字数Ｎが所定値（実施形態では「７」）より大きいか否かを判断する。つまり、ユーザが機密度の高いファイルを作成する等を意図してログインしたのか否かを判断する。
【００７３】
登録したログインパスワードの全文字（第１の実施形態で説明したように１０文字）でログインしたと判断した場合には、ステップＳ４２に進んで、スパイウェア駆除ソフトを実行する。
【００７４】
以上の結果、本第４の実施形態によれば、ユーザは機密性の高い作業を行うためにログインした場合には、スパイウェア駆除処理が必ず行われ、システムの安全性が保証された上で作業を行うことが可能になる。また、機密性を問わない作業を行うためにログインした場合には、スパイウェア駆除処理が行われないことになり、その処理が完了するのを待たないで作業を開始できる。
【００７５】
＜第５の実施形態＞
第５の実施形態を説明する。
【００７６】
コンピュータを使用する際、他人に重要なファイルを、ＭＯやメモリーカード、フレキシブルディスク等の外部メディアにコピーされて持去られる危険性をなくす為に、ファイルの外部メディアへのコピーを禁止することが行われている。
【００７７】
この機能は、コンピュータ内に常駐するプロセスを起動させておき、このプロセスが外部メディアが接続され得るＵＳＢ、IEEE1394、SCSI、フレキシブルディスク等のインターフェースを監視し、これらのインターフェースを介して外部メディアへの書込み操作が行われた場合は、これを検知して禁止することで実現されている。
【００７８】
また、コンピュータの正規のユーザが使用する際も、書出し禁止の重要ファイルを誤って外部メディアにコピーしてしまう危険性がなくなるので、有効である。

【００７９】
ところが、コンピュータの正規のユーザが、機密度が高くないファイルを外部メディアにコピーしようとした際にも、このコピー禁止が働いてコピーできないと言う問題点があった。
【００８０】
そこで、本第５の実施形態では、特に外部メディアへの書き込み禁止モジュールを常駐する否かを、ログインパスワードの文字数に応じて決定する例を説明する。
【００８１】
装置構成は第１の実施形態と同様であるものとし、以下では、本第５の実施形態におけるログイン処理を図１３のフローチャートに従って説明する。なお、第１の実施形態における図７と同じ処理は、同符号を付した。従って以下では、異なる点について説明することとする。
【００８２】
ユーザが正しいユーザＩＤとログインパスワードを入力する（登録したログインパスワード全文字を用いるか、登録された先頭の７文字を利用してログインするかの何れか）と、処理はステップＳ５１に進む。
【００８３】
ステップＳ５１では、ステップＳ３で記憶したログインパスワードの文字数Ｎが所定値（実施形態では「７」）より大きいか否かを判断する。つまり、ユーザが機密度の高いファイルを作成する等を意図してログインしたのか否かを判断する。
【００８４】
登録したログインパスワードの全文字（第１の実施形態で説明したように１０文字）でログインしたと判断した場合には、ステップＳ５２に進んで、外部メディアへの書き出し禁止モジュールのメモリ常駐を開始する。
【００８５】
以上の結果、本第５の実施形態によれば、ユーザは機密性の高い作業を行うためにログインした場合には、外部メディアへの書き出しが禁止されることになる。従って、ログインユーザは勿論、ログインユーザが席を外しいる場合においても、第３者が外部メディアへの書き出しは行えない。また、機密性を問わない作業を行うためにログインした場合（７文字のログインパスワードでログインした場合）には、外部メディアへの書き出しを禁止するモジュールがメモリに常駐することが無くなるので、必要なファイルを外部メディアに書き出すことが可能になる。
【００８６】
＜第６の実施形態＞
第６の実施形態を説明する。
【００８７】
コンピュータ（ＰＣ）を使用する際、不正なアクセスを監視する為に、コンピュータに対して行った操作のログを記録することが行われている。この機能は、コンピュータ内に常駐するプロセスを起動させておき、ユーザがファイルの読み込みや書出し等の操作を行った際、このプロセスが、そのユーザ名、時間、操作した内容をログファイルに書出す事で実現されていた。なお、ログ記録に関する技術内容は、既に公知であるので、ここでの詳細な説明は省略する。
【００８８】
このログ記録は、不正なユーザが不正にコンピュータを操作した痕跡を記録する意味だけでなく、正当なユーザが正当にコンピュータを操作したことを証明する意味からも重要である。
【００８９】
ところが、コンピュータの正規のユーザが、機密度が高くないファイルを操作する場合でも、ログ記録の機能が動作してしまうので、コンピュータの動作が遅くなってしまう問題点がある。また、この様な場合、価値のないログ記録が残されるので、コンピュータの

記憶装置の領域を無駄に使ってしまう問題も発生する。更に、価値のないログが残ることで、後でログを検索する際、必要以上に時間を費やしてしまう問題点も発生する。

【００９０】

そこで、本第６の実施形態では、特にログ記録モジュールを常駐する否かを、ログインパスワードの文字数に応じて決定する例を説明する。

【００９１】

装置構成は第１の実施形態と同様であるものとし、以下では、本第６の実施形態におけるログイン処理を図１４のフローチャートに従って説明する。なお、第１の実施形態における図７と同じ処理は、同符号を付した。従って以下では、異なる点について説明することとする。

【００９２】

ユーザが正しいユーザＩＤとログインパスワードを入力する（登録したログインパスワード全文字を用いるか、登録された先頭の７文字を利用してログインするかの何れか）と、処理はステップＳ６１に進む。

【００９３】

ステップＳ６１では、ステップＳ３で記憶したログインパスワードの文字数Ｎが所定値（実施形態では「７」）より大きいか否かを判断する。つまり、ユーザが機密度の高いファイルを作成する等を意図してログインしたのか否かを判断する。

【００９４】

登録したログインパスワードの全文字（第１の実施形態で説明したように１０文字）でログインしたと判断した場合には、ステップＳ６２に進んで、ログ記録モジュールのメモリ常駐を開始する。

【００９５】

以上の結果、本第６の実施形態によれば、ユーザが機密度の高くないファイルにしかアクセスしないことを、ログインパスワードの文字数が短いことで判定しているので、ログ記録モジュールが動作して無駄にコンピュータが遅くなる問題を解決することができる。また、不要なログを記録しないですみ、コンピュータの記憶領域を無駄に使用する問題点も解決される。更に、後のログ検索で無駄に時間がかかってしまう問題点も解決できる。

【００９６】

以上、第１乃至第６の実施形態を説明したが、各実施形態は、必要に応じて組み合わせても構わない。

【００９７】

また、実施形態では、短いログインパスワードの文字数を「７」とする例を説明したが、これは一例であり、この数値に限るものではない。また、ファイルの保存先として、ローカルコンピュータの記憶装置を例にしたが、ネットワーク装置上のファイルサーバ等に保存する構成の場合でもかまわない。

【００９８】

また、上記実施形態では、１つのログインパスワードの全文字と、その先頭から７文字を利用する例を説明したが、文字列の長さの異なる独立した２つのパスワードを登録し、それを用いてもよい。

【００９９】

更には、本実施形態では、長さの違うログインパスワードでユーザ認証を行ったが、異なる複数の認証方法を用い、認証の安全性に応じて、セキュリティに関する動作環境を切り替える方法であってもかまわない。例えば、ログインパスワードによる認証とＩＣカードによる認証と、指紋による認証の３つの認証を行える様にしておき、ユーザが、ログインパスワードで認証した場合は、ファイルパスワードを付けずにファイル保存を行い、ＩＣカードによる認証か指紋による認証を行った場合は、ファイルパスワードを付けてファイル保存を行う様にすることが、この例に相当する。

【０１００】

また、上記実施形態からも容易に理解できるように、各実施形態に係る処理はコンピュ

ータプログラムによるものである。通常、コンピュータプログラムはＣＤ－ＲＯＭ等のコンピュータ可読記憶媒体に格納されていて、コンピュータの読取り装置（ＣＤ－ＲＯＭドライブ等）にセットしてシステムにコピーもしくはインストールすることで実行可能になるから、当然、そのようなコンピュータ可読記憶媒体も本発明の範疇に入る。

【図面の簡単な説明】

【０１０１】

【図１】パスワード入力付きファイル保存ダイアログの一例を示す図である。

【図２】ファイルパスワード入力ダイアログの一例を示す図である。

【図３】ファイルパスワード確認ダイアログの一例を示す図である。

【図４】ファイル保存ダイアログの一例を示す図である。

【図５】実施形態におけるシステム構成図である。

【図６】ログインパスワードファイルの内容の一例を示す図である。

【図７】第１の実施形態におけるログイン時の処理手順を示すフローチャートである。

【図８】第１の実施形態におけるログインダイアログの一例を示す図である。

【図９】第１の実施形態におけるファイル保存時の処理を示すフローチャートである。

【図１０】第２の実施形態におけるファイル保存時の処理を示すフローチャートである。

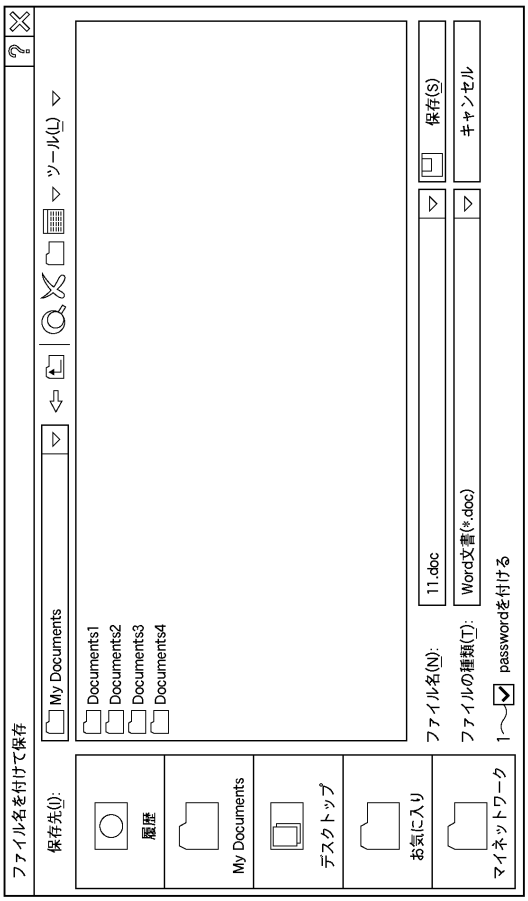
【図１１】第３の実施形態におけるスクリーンセーバの起動処理手順を示すフローチャートである。

【図１２】第４の実施形態におけるログイン時の処理手順を示すフローチャートである。

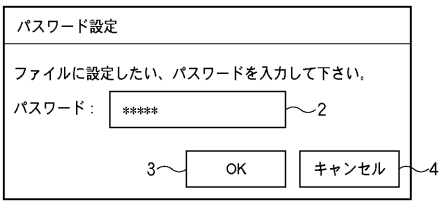
【図１３】第５の実施形態におけるログイン時の処理手順を示すフローチャートである。

【図１４】第６の実施形態におけるログイン時の処理手順を示すフローチャートである。

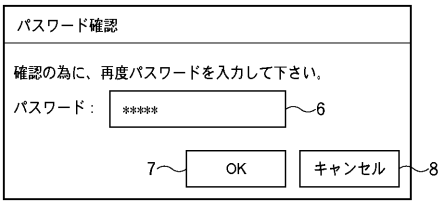
【図１】



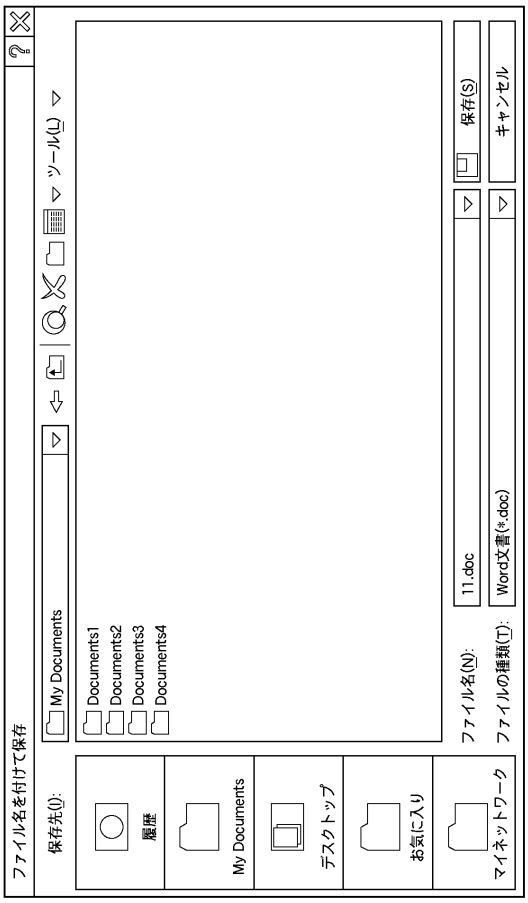
【図２】



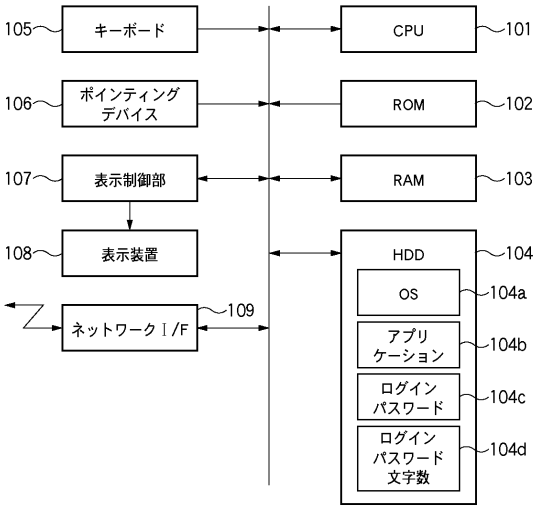
【図３】



【図４】



【図５】

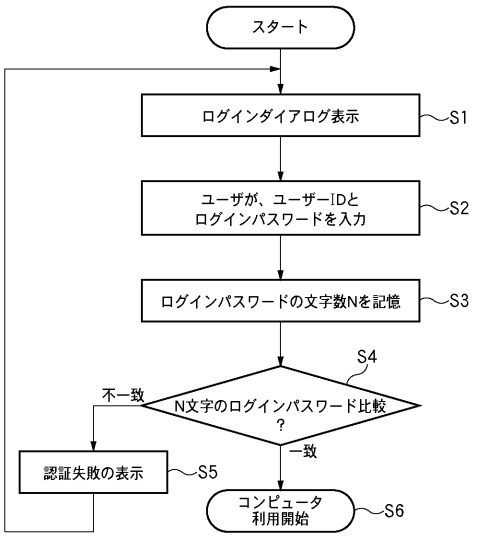


【図６】

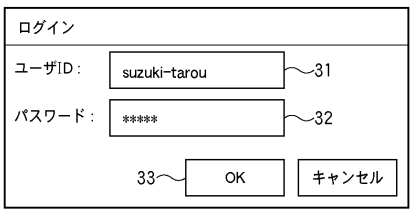
suzuki-tarou	abcde12345
satou-hanako	fghijk678901
yamada-ichirou	lmnopqr2345678
…	…

21 22

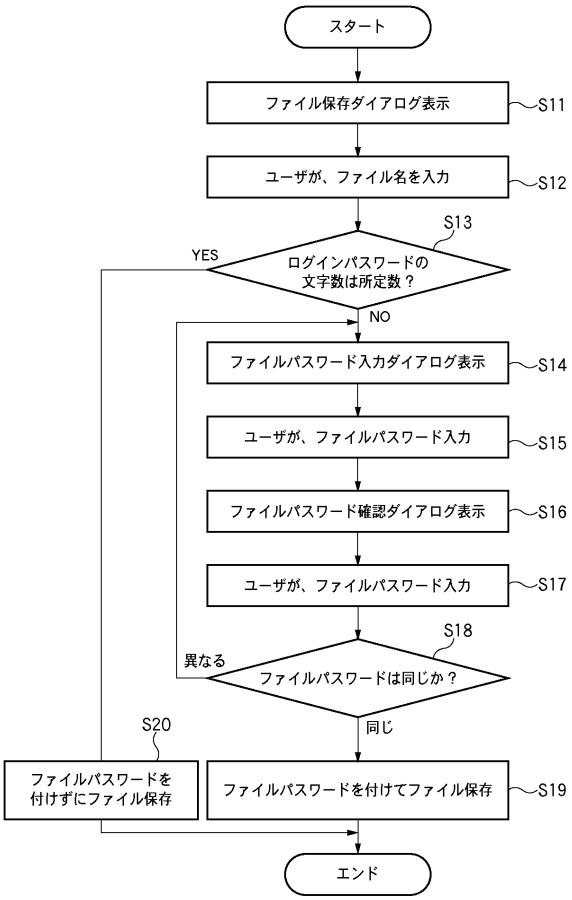
【図７】



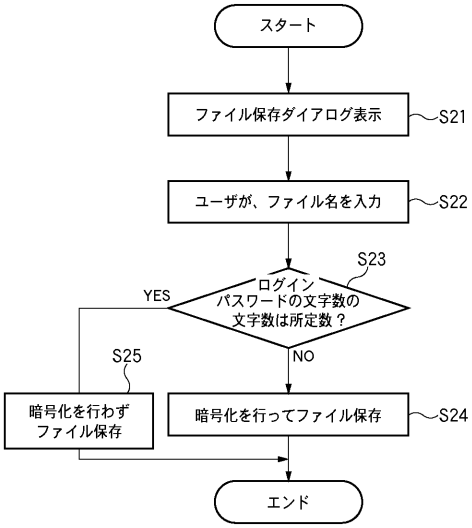
【図８】



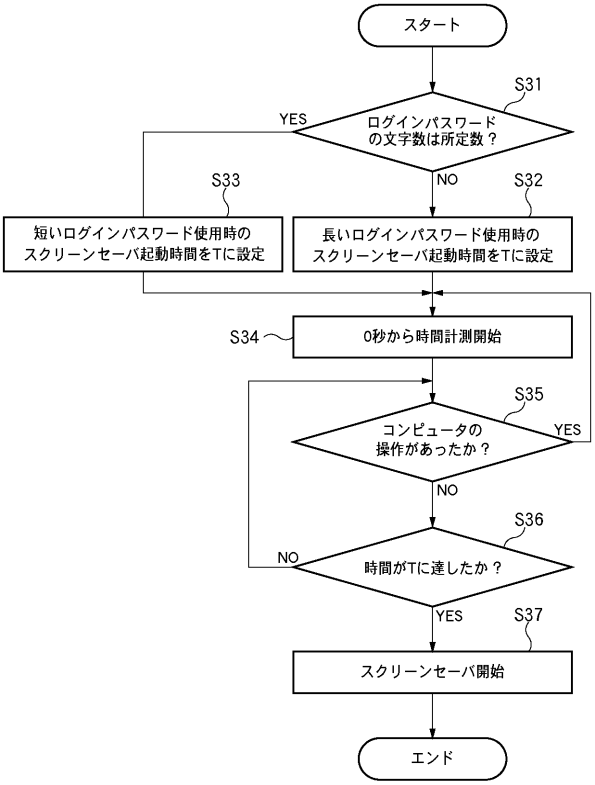
【図９】



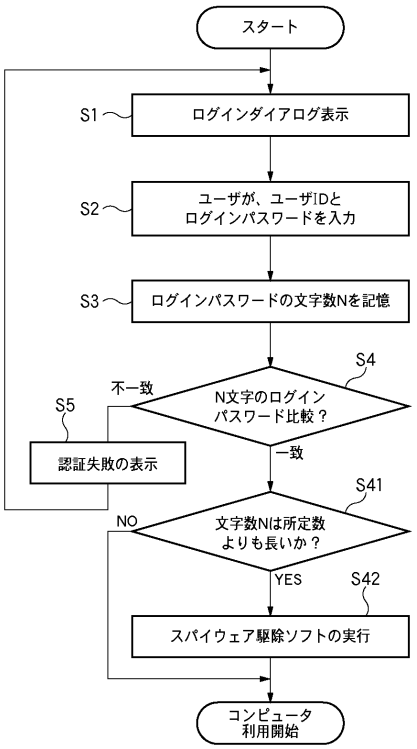
【図１０】



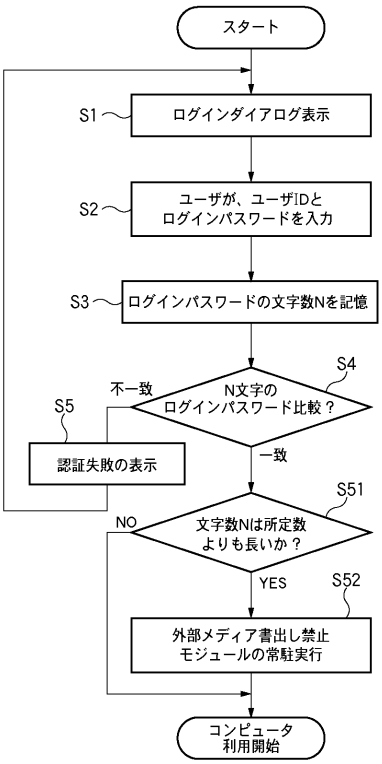
【図１１】



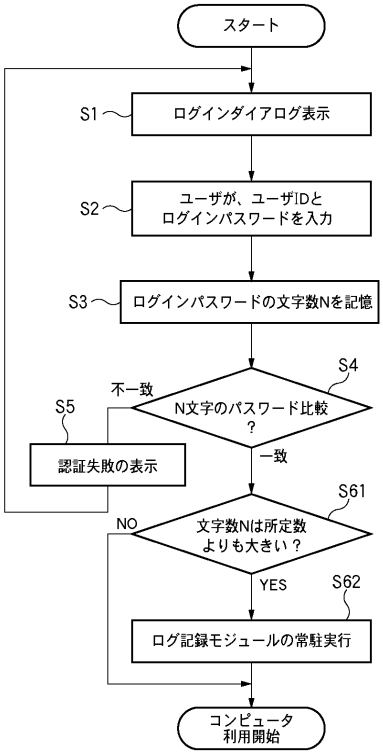
【図１２】



【図１３】



【図１４】


スタート
S1
ログインダイアログ表示
S2
ユーザが、ユーザIDと
ログインパスワードを入力
S3
ログインパスワードの文字数Nを記憶
S4
不一致
N文字のパスワード比較
？
S5
認証失敗の表示
一致
S61
NO
文字数Nは所定数
よりも大きい？
YES
S62
ログ記録モジュールの常駐実行
コンピュータ
利用開始