(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2004-234331
(P2004-234331A)
(43)公開日　平成16年8月19日(2004.8.19)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G06F 1/00	G06F 1/00	370E	5B058
G06K 17/00	G06K 17/00	T	

審査請求 有　請求項の数 18　ＯＬ　（全 20 頁）

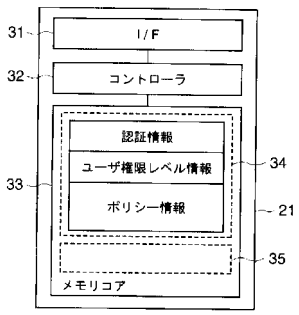
(21)出願番号　特願2003-22156(P2003-22156)
(22)出願日　平成15年1月30日(2003.1.30)

(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(74)代理人　100058479
弁理士　鈴江　武彦
(74)代理人　100091351
弁理士　河野　哲
(74)代理人　100088683
弁理士　中村　誠
(74)代理人　100108855
弁理士　蔵田　昌俊
(74)代理人　100084618
弁理士　村松　貞男
(74)代理人　100092196
弁理士　橋本　良郎

最終頁に続く

(54)【発明の名称】情報処理装置および同装置で使用されるユーザ操作制限方法

(57)【要約】
【課題】操作制限情報の設定操作無しで各ユーザが実行可能な操作を制限することが可能な情報処理装置を実現する。
【解決手段】ＳＤカード２１は、認証のためのトークンデバイスとして使用される。ＳＤカード２１には、認証情報のみならずポリシー情報も併せて記憶されている。ポリシー情報は、ユーザ操作を制限する情報である。コンピュータがパワーオンされたとき、ＳＤカード２１に格納された認証情報に基づいて、コンピュータの使用を許可するか否かを判別するための認証処理が行われる。コンピュータの使用を許可すべきことが判別された場合、今度は、ＳＤカード２１に格納されたポリシー情報に基づいて、コンピュータを使用するユーザが使用可能なコンピュータの機能が制限される。
【選択図】　図２



【特許請求の範囲】
【請求項１】
トークンデバイスが取り外し自在に接続可能な情報処理装置であって、
前記情報処理装置の使用を許可するための認証情報と前記情報処理装置を使用するユーザの操作を制限するためのポリシー情報とを含むトークンデータを、前記情報処理装置に接続されたトークンデバイスに格納する格納手段と、
前記情報処理装置の電源投入に応答して、前記情報処理装置に接続されたトークンデバイスに格納された前記認証情報に基づき、前記情報処理装置の使用を許可すべきか否かを判別する判別手段と、
前記判別手段によって前記情報処理装置の使用を許可すべきことが判別された場合、前記情報処理装置に接続されたトークンデバイスに格納された前記ポリシー情報に基づいて、前記情報処理装置を使用するユーザが使用可能な前記情報処理装置の機能を制限する制限手段とを具備することを特徴とする情報処理装置。
【請求項２】
前記ポリシー情報は、前記情報処理装置が有する予め決められた複数の機能の各々についてその使用をユーザに許可するか否かを示す情報を含むことを特徴とする請求項１記載の情報処理装置。
【請求項３】
前記ポリシー情報は、前記情報処理装置の動作環境の設定を変更する機能の使用を許可するか否かを示す情報を少なくとも含むことを特徴とする請求項１記載の情報処理装置。
【請求項４】
前記トークンデータは、さらに、前記情報処理装置を使用するユーザの権限レベルを示す権限レベル情報を含み、
前記制限手段は、前記情報処理装置に接続されたトークンデバイスに格納された前記権限レベル情報および前記ポリシー情報に基づき、前記情報処理装置を使用するユーザが使用可能な前記情報処理装置の機能を制限する手段を含むことを特徴とする請求項１記載の情報処理装置。
【請求項５】
ユーザの操作に応じて、前記トークンデバイスに書き込むべき前記ポリシー情報の内容を変更するポリシー変更処理を実行する手段をさらに具備し、
前記トークンデータは、前記情報処理装置を使用するユーザの権限レベルを示す権限レベル情報を含み、
前記制限手段は、
前記情報処理装置に接続されたトークンデバイスに格納された前記権限レベル情報に基づいて、前記情報処理装置を使用するユーザの権限レベルがスーパバイザユーザに対応する所定の権限レベルであるか否かを判別する手段と、
前記情報処理装置を使用するユーザの権限レベルが前記所定の権限レベルではない場合、前記ポリシー変更処理の実行を禁止する手段とを含むことを特徴とする請求項１記載の情報処理装置。
【請求項６】
前記ポリシー変更処理を実行する手段は、
前記ポリシー情報の内容を設定するための画面を前記情報処理装置の表示装置に表示する手段と、
前記画面上の操作に従って、前記トークンデバイスに格納すべき前記ポリシー情報の内容を決定する手段とを含むことを特徴とする請求項５記載の情報処理装置。
【請求項７】
前記判別手段は、
前記情報処理装置の電源投入に応答して、前記情報処理装置にパスワードが登録されているか否かを判別する手段と、
前記情報処理装置にパスワードが登録されている場合、前記情報処理装置にトークンデバ

イスが接続されているか否かを判別する手段と、
前記情報処理装置にトークンデバイスが接続されている場合、前記情報処理装置に接続されたトークンデバイスに格納された前記認証情報に基づき、前記情報処理装置の使用を許可すべきか否かを判別する手段と、
前記情報処理装置にトークンデバイスが接続されていない場合、ユーザが前記情報処理装置のキーボードを操作することによって入力したパスワードと前記登録されているパスワードとに基づいて、前記情報処理装置の使用を許可すべきか否かを判別する手段とを含むことを特徴とする請求項１記載の情報処理装置。
【請求項８】
前記トークンデバイスは、前記情報処理装置のファイルシステムからのアクセスが禁止されたエリアを有し、
前記格納手段は、前記トークンデータを前記トークンデバイスの前記エリアに格納する手段を含むことを特徴とする請求項１記載の情報処理装置。
【請求項９】
前記トークンデバイスは、前記情報処理装置のファイルシステムからのアクセスが禁止された第１エリアと前記ファイルシステムからのアクセスが可能な第２エリアとを有し、
前記格納手段は、前記トークンデータを前記トークンデバイスの前記第１エリアに格納する手段を含むことを特徴とする請求項１記載の情報処理装置。
【請求項１０】
トークンデバイスが取り外し自在に接続可能な情報処理装置のユーザの操作を制限するユーザ操作制限方法であって、
前記情報処理装置の使用を許可するための認証情報と前記情報処理装置を使用するユーザの操作を制限するためのポリシー情報とを含むトークンデータを、前記情報処理装置に接続されたトークンデバイスに格納する格納ステップと、
前記情報処理装置の電源投入に応答して、前記情報処理装置に接続されたトークンデバイスに格納された前記認証情報に基づき、前記情報処理装置の使用を許可すべきか否かを判別する判別ステップと、
前記判別ステップによって前記情報処理装置の使用を許可すべきことが判別された場合、前記情報処理装置に接続されたトークンデバイスに格納された前記ポリシー情報に基づいて、前記情報処理装置を使用するユーザが使用可能な前記情報処理装置の機能を制限する制限ステップとを具備することを特徴とするユーザ操作制限方法。
【請求項１１】
前記ポリシー情報は、前記情報処理装置が有する予め決められた複数の機能の各々についてその使用をユーザに許可するか否かを示す情報を含むことを特徴とする請求項１０記載のユーザ操作制限方法。
【請求項１２】
前記ポリシー情報は、前記情報処理装置の動作環境の設定を変更する機能の使用をユーザに許可するか否かを示す情報を少なくとも含むことを特徴とする請求項１０記載のユーザ操作制限方法。
【請求項１３】
前記トークンデータは、さらに、前記情報処理装置を使用するユーザの権限レベルを示す権限レベル情報を含み、
前記制限ステップは、前記情報処理装置に接続されたトークンデバイスに格納された前記権限レベル情報および前記ポリシー情報に基づき、前記情報処理装置を使用するユーザが使用可能な前記情報処理装置の機能を制限するステップを含むことを特徴とする請求項１０記載のユーザ操作制限方法。
【請求項１４】
ユーザの操作に応じて、前記トークンデバイスに書き込むべき前記ポリシー情報の内容を変更するポリシー変更処理を実行するステップをさらに具備し、
前記トークンデータは、前記情報処理装置を使用するユーザの権限レベルを示す権限レベ

ル情報を含み、
前記制限ステップは、
前記情報処理装置に接続されたトークンデバイスに格納された前記権限レベル情報に基づいて、前記情報処理装置を使用するユーザの権限レベルがスーパバイザユーザに対応する所定の権限レベルであるか否かを判別するステップと、
前記情報処理装置を使用するユーザの権限レベルが前記所定の権限レベルではない場合、前記ポリシー変更処理の実行を禁止するステップとを含むことを特徴とする請求項１０記載のユーザ操作制限方法。
【請求項１５】
前記ポリシー変更処理を実行するステップは、
前記ポリシー情報の内容を設定するための画面を前記情報処理装置の表示装置に表示するステップと、
前記画面上の操作に従って、前記トークンデバイスに格納すべき前記ポリシー情報の内容を決定するステップとを含むことを特徴とする請求項１４記載のユーザ操作制限方法。
【請求項１６】
前記判別ステップは、
前記情報処理装置の電源投入に応答して、前記情報処理装置にパスワードが登録されているか否かを判別するステップと、
前記情報処理装置にパスワードが登録されている場合、前記情報処理装置にトークンデバイスが接続されているか否かを判別するステップと、
前記情報処理装置にトークンデバイスが接続されている場合、前記情報処理装置に接続されたトークンデバイスに格納された前記認証情報に基づき、前記情報処理装置の使用を許可すべきか否かを判別するステップと、
前記情報処理装置にトークンデバイスが接続されていない場合、ユーザが前記情報処理装置のキーボードを操作することによって入力したパスワードと前記登録されているパスワードとに基づいて、前記情報処理装置の使用を許可すべきか否かを判別するステップとを含むことを特徴とする請求項１０記載のユーザ操作制限方法。
【請求項１７】
前記トークンデバイスは、前記情報処理装置のファイルシステムからのアクセスが禁止されたエリアを有し、
前記格納ステップは、前記トークンデータを前記トークンデバイスの前記エリアに格納するステップを含むことを特徴とする請求項１０記載のユーザ操作制限方法。
【請求項１８】
前記トークンデバイスは、前記情報処理装置のファイルシステムからのアクセスが禁止された第１エリアと前記ファイルシステムからのアクセスが可能な第２エリアとを有し、
前記格納ステップは、前記トークンデータを前記トークンデバイスの前記第１エリアに格納するステップを含むことを特徴とする請求項１０記載のユーザ操作制限方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は例えばパーソナルコンピュータのような情報処理装置および同装置で使用されるユーザ操作制限方法に関する。
【０００２】
【従来の技術】
一般に、パーソナルコンピュータのような情報処理装置においては、セキュリティ機能が設けられている。
【０００３】
代表的なセキュリティ機能の一つとして、パスワードを用いたユーザ認証機能が知られている。パーソナルコンピュータに予め登録されたパスワードと同一のパスワードがユーザによるキーボード操作によって入力された場合のみ、パーソナルコンピュータの使用が許

可される。
【０００４】
また、外部記憶装置から読み込んだパスワードを用いてユーザ認証を行うシステムも開発されている（例えば、特許文献１参照。）。このシステムにおいては、ユーザによるパスワード入力の代わりに外部記憶装置に記憶されたパスワードが用いられる。外部記憶装置から読み込まれたパスワードがコンピュータに予め登録されたパスワードと一致した場合、システムの起動が許可される。これにより、パスワード忘れやパスワード入力操作のミスに起因するトラブルの発生を未然に防止することができる。
【０００５】
【特許文献１】
特開２００２－２６８７６６号公報（第２頁、図１）
【０００６】
【発明が解決しようとする課題】
しかし、特許文献１のシステムでは、外部記憶装置に記憶されるデータはパスワードだけである。このため、外部記憶装置を用いて実行可能な認証処理は、システムの起動を許可するか否かを判別するための処理のみとなり、ユーザの操作を制限することは出来ない。
【０００７】
あるコンピュータを複数人で使用するマルチユーザ環境においては、各ユーザのユーザ権限レベル等に応じて、各ユーザが実行可能な操作を制限する機能が要求される。この機能を実現するためには、複数のユーザそれぞれに対応する操作制限情報をコンピュータに設定する操作を予め行うことが必要となる。
【０００８】
最近では、複数台のコンピュータを複数人によって共有する環境が増え始めている。この場合、個々のコンピュータ毎に全てのユーザそれぞれに対応する操作制限情報を設定するという煩雑な操作を行うことが必要となり、これによって管理コストの増大が引き起こされる。
【０００９】
本発明は上述の事情を考慮してなされたものであり、操作制限情報の設定操作無しで各ユーザが実行可能な操作を制限することが可能な情報処理装置およびユーザ操作制限方法を提供することを目的とする。
【００１０】
【課題を解決するための手段】
上述の課題を解決するため、本発明は、トークンデバイスが取り外し自在に接続可能な情報処理装置であって、前記情報処理装置の使用を許可するための認証情報と前記情報処理装置を使用するユーザの操作を制限するためのポリシー情報とを含むトークンデータを、前記情報処理装置に接続されたトークンデバイスに格納する格納手段と、前記情報処理装置の電源投入に応答して、前記情報処理装置に接続されたトークンデバイスに格納された前記認証情報に基づき、前記情報処理装置の使用を許可すべきか否かを判別する判別手段と、前記判別手段によって前記情報処理装置の使用を許可すべきことが判別された場合、前記情報処理装置に接続されたトークンデバイスに格納された前記ポリシー情報に基づいて、前記情報処理装置を使用するユーザが使用可能な前記情報処理装置の機能を制限する制限手段とを具備することを特徴とする。
【００１１】
この情報処理装置によれば、その情報処理装置の使用を許可するための認証情報とユーザの操作を制限するためのポリシー情報とがトークンデータとしてトークンデバイスに格納される。トークンデバイスに格納された認証情報によって情報処理装置の使用を許可すべきことが判別された場合、さらに、情報処理装置に接続されたトークンデバイスに格納されたポリシー情報に基づいて、情報処理装置を使用するユーザが使用可能な情報処理装置の機能が制限される。よって、情報処理装置に操作制限情報を設定する操作を行うことなく、ユーザが実行可能な操作をトークンデバイスを用いて制限することが可能となる。

【００１２】
【発明の実施の形態】
以下、図面を参照して本発明の実施形態を説明する。まず、本発明の一実施形態に係る情報処理装置の外観について説明する。ここでは、ノートブック型パーソナルコンピュータとして実現した場合を想定する。
【００１３】
図１は本コンピュータのディスプレイユニットを開いた状態における正面図である。本コンピュータ１は、コンピュータ本体１１と、ディスプレイユニット１２とから構成されている。ディスプレイユニット１２にはＬＣＤ（Ｌｉｑｕｉｄ　Ｃｒｙｓｔａｌ　Ｄｉｓｐｌａｙ）からなる表示装置１２１が組み込まれており、そのＬＣＤ１２１はディスプレイユニット１２のほぼ中央に位置されている。
【００１４】
ディスプレイユニット１２は、コンピュータ本体１１に対して解放位置と閉塞位置との間を回動自在に取り付けられている。コンピュータ本体１１は薄い箱形の筐体を有しており、その上面にはキーボード１３、本コンピュータ１を電源オン／オフするためのパワーボタン１４、およびタッチパッド１５などが配置されている。
【００１５】
さらに、コンピュータ本体１１の側面には、トークンデバイスを取り外し自在に装着するためのスロット１６が設けられている。トークンデバイスは認証用のトークンデータを記憶する外部記憶装置であり、例えばメモリカードなどのリムーバブル記憶装置から構成される。以下では、トークンデバイスとして、ＳＤ（Ｓｅｃｕｒｅ　Ｄｉｇｉｔａｌ）カード２１を使用する場合を想定する。
【００１６】
ＳＤカード２１は認証のためのトークンデータを記憶した小型メモリカードデバイス（ＳＤトークン）である。スロット１６は、ＳＤカード２１が取り外し自在に装着可能に構成されている。各ユーザは、キーボード１３からパスワードをタイピングする代わりに、そのユーザに対応するＳＤカード２１を使用することが出来る。
【００１７】
図２には、ＳＤカード２１の構成が示されている。ＳＤカード２１は、図示のように、ＳＤインタフェース３１、コントローラ３２、およびメモリコア３３とから構成されている。ＳＤインタフェース３１は、コンピュータ１との通信を行うためのインターフェース回路である。コンピュータ１は、ＳＤカード２１のホスト装置として機能する。コントローラ３２は、ＳＤインタフェース３１を介してホストから入力されるコマンドに応じて、メモリコア３３に対するアクセスを実行する。メモリコア３３は、フラッシュＥＥＰＲＯＭなどの不揮発性メモリから構成されている。
【００１８】
メモリコア３３には、第１記憶エリア３４と第２記憶エリア３５とが割り当てられている。第１記憶エリア３４は、コンピュータで実行されるファイルシステムからはアクセスすることが出来ない記憶エリアである。第１記憶エリア３４に対するアクセスは、ＳＤカード２１のセキュリティ機能に対応した専用のカード認証機能を持つソフトウェアのみが可能である。第２記憶エリア３５は、ファイルシステムから自由にアクセスすることができるデータ記憶エリアである。このため、ＳＤカード２１は、通常のデータ記憶装置としても機能する。ファイルシステムは、ＳＤカード２１をディスクドライブとして認識する。
【００１９】
第１記憶エリア３４は、トークンデータの記憶のために利用される。トークンデータは、認証情報、ユーザ権限レベル情報、およびポリシー情報を含む。
【００２０】
ＳＤカード２１に記憶された認証情報は、本コンピュータ１の使用を許可するか否かを判別するための認証用の情報であり、本コンピュータ１の使用権を示す。本コンピュータを使用可能な複数のユーザそれぞれは、それぞれ自分用のＳＤカード２１を所有する。本コ

ンピュータを使用する各ユーザは、ＳＤカード２１に記憶された認証情報によって認証される。

【００２１】

ＳＤカード２１に記憶された認証情報を用いた認証処理は、本コンピュータ１の電源投入に応答して実行される。この認証処理によりコンピュータ１の使用を許可すべきか否かが判別され、その判別結果に応じて、コンピュータ１の起動（ブートまたはレジューム）が許可または禁止される。

【００２２】

ＳＤカード２１に記憶されたユーザ権限レベル情報は、そのＳＤカード２１を所有するユーザの権限レベルを示す。権限レベルとしては、例えば、

１．　スーパバイザ

２．　パワーユーザ

３．　ユーザ

等の種類がある。以下では、“スーパバイザ”および“ユーザ”の２種類の権限レベルを利用する場合を想定する。

【００２３】

この場合、使用されるＳＤトークンの種類は、大別して“スーパバイザ”トークンおよび“ユーザ”トークンの２種類となる。

【００２４】

ＳＤカード２１に記憶されたポリシー情報は、そのＳＤカード２１を所有するユーザが実行可能な操作を制限するための情報であり、実行可能な操作を規定する。すなわち、ポリシー情報は、コンピュータ１が有する予め決められた複数の機能の各々についてその使用をユーザに許可するか否かを示す。

【００２５】

権限レベルが“スーパバイザ”であるユーザは本コンピュータ１の管理者であるので、そのポリシー情報によって本コンピュータ１が有する全ての機能を使用することが許可される。一方、権限レベルが“ユーザ”である各ユーザについては、そのポリシー情報によって、使用可能な操作は制限される。“スーパバイザ”は、ＳＤカード２１に格納すべきポリシー情報の内容を“ユーザ”毎に設定／変更することができる。すなわち、権限レベルが“ユーザ”である各ユーザが使用可能な本コンピュータ１の機能は、その“ユーザ”が所有するＳＤカード２１に記憶されたポリシー情報によって決定される。

【００２６】

次に、図２を参照して、本コンピュータ１のシステム構成について説明する。

【００２７】

本コンピュータ１には、図示のように、ＣＰＵ１０１、ホストブリッジ１０２、主メモリ１０３、表示コントローラ１０４、システムコントローラ１０５、ハードディスクドライブ（ＨＤＤ）１０６、カードコントローラ１０７、ＢＩＯＳ－ＲＯＭ１０８、およびエンベデッドコントローラ／キーボードコントローラＩＣ（ＥＣ／ＫＢＣ）１０９等が設けられている。

【００２８】

ＣＰＵ１０１は本コンピュータ１の動作を制御するために設けられたプロセッサであり、ハードディスクドライブ（ＨＤＤ）１０６から主メモリ１０３にロードされたオペレーティングシステム（ＯＳ）および各種アプリケーション／ユーティリティプログラムを実行する。また、ＣＰＵ１０１は、ＢＩＯＳ－ＲＯＭ１０８に格納されたＢＩＯＳ（Ｂａｓｉｃ　Ｉｎｐｕｔ　Ｏｕｔｐｕｔ　Ｓｙｓｔｅｍ）も実行する。

【００２９】

ＢＩＯＳはコンピュータ１を構成するハードウェアを制御するためのプログラムである。ＢＩＯＳは、コンピュータ１の動作環境の設定を変更するためのハードウェアセットアップ機能（ＢＩＯＳセットアップ機能とも云う）を有している。ポリシー情報によってハードウェアセットアップ機能を利用することが許されたユーザは、例えば、コンピュータ１

を構成する各デバイスのイネーブル／ディエーブルの設定、コンピュータ１のパワーオンモード（ブートモード／レジュームモード）の設定、ＣＰＵ１０１の省電力モードの設定、等を行うことが出来る。

【００３０】

コンピュータ１においては、ユーティリティプログラムの一つとして、パスワードユーティリティプログラムが予めインストールされている。このパスワードユーティリティプログラムは、ＳＤトークンを利用した認証を実現するためのプログラムである。このパスワードユーティリティプログラムは、１）“スーパバイザ”／“ユーザ”パスワードの登録機能、２）ポリシー情報を設定／変更する機能、３）ＳＤトークンを作成する機能、４）ユーザ認証およびユーザ操作制限機能、等を有する。ユーザ認証およびユーザ操作制限機能はＢＩＯＳと共同して実行される。もし“スーパバイザ”ユーザのパスワードがコンピュータ１に登録されているならば、ポリシー情報を設定／変更する機能は“スーパバイザ”として認証されたユーザにのみ許可される。

【００３１】

ホストブリッジ１０２はＣＰＵ１０１のローカルバスとシステムコントローラ１０５との間を接続するブリッジデバイスである。ホストブリッジ１０２には、主メモリ１０３をアクセス制御するメモリコントローラが内蔵されている。表示コントローラ１０４は本コンピュータ１のディスプレイモニタとして使用されるＬＣＤ１２１を制御する。

【００３２】

システムコントローラ１０５は、ＰＣＩバス上の各デバイスおよびＩＳＡバス上の各デバイスを制御する。また、システムコントローラ１０５には、ＨＤＤ１０６を制御するためのＩＤＥコントローラも内蔵されている。

【００３３】

カードコントローラ１０７は、カードスロット１６に装着されたＳＤカード２１を制御するように構成されたＳＤホストコントローラである。ＢＩＯＳ－ＲＯＭ１０８にはＢＩＯＳが格納されている。ＢＩＯＳ－ＲＯＭ１０８はフラッシュＥＥＰＲＯＭから構成されている。コンピュータ１に登録された“スーパバイザ”パスワード／“ユーザ”パスワードは、例えば、ＢＩＯＳ－ＲＯＭ１０８内に記憶される。また、“スーパバイザ”／“ユーザ”トークンが作成された時、その作成されたトークンを識別するためのトークン識別情報が、“スーパバイザ”／“ユーザ”パスワードに対応付けてＢＩＯＳ－ＲＯＭ１０８内に記憶される。

【００３４】

ＢＩＯＳ－ＲＯＭ１０８には、さらに、ユーザ権限レベル情報およびポリシー情報も、“スーパバイザ”／“ユーザ”パスワードに対応付けて記憶されている。ユーザ権限レベル情報は、登録された各パスワードが“スーパバイザ”パスワードおよび“ユーザ”パスワードのいずれであるかを示す。ポリシー情報は、登録された各“ユーザ”パスワード毎に、そのパスワードをタイプすることによって認証されたユーザが操作可能な機能を制限するために使用される。ＢＩＯＳ－ＲＯＭ１０８内に記憶されるユーザ権限レベル情報およびポリシー情報は、パスワードをタイプすることによって認証されたユーザが実行可能な操作を制限するために用いられる。

【００３５】

なお、これら“スーパバイザ”／“ユーザ”パスワード、トークン識別情報、ユーザ権限レベル情報およびポリシー情報は、ＢＩＯＳ－ＲＯＭ１０８ではなく、ＨＤＤ１０６内の特定の一部の記憶領域に記憶してもよい。

【００３６】

エンベデッドコントローラ／キーボードコントローラＩＣ（ＥＣ／ＫＢＣ）１０９は、電力管理のためのエンベデッドコントローラと、キーボード１３を制御するためのキーボードコントローラとが集積された１チップマイクロコンピュータである。このエンベデッドコントローラ／キーボードコントローラＩＣ（ＥＣ／ＫＢＣ）１０９は、ユーザによるパワーボタン１４の操作に応じて本コンピュータ１をパワーオン／パワーオフする機能を有

している。
【００３７】
次に、図４乃至図１０を参照して、パスワードユーティリティプログラムの各機能について説明する。
【００３８】
図４は、パスワードユーティリティプログラムによってＬＣＤ１２１に表示される認証ダイアログ２０１を示している。パスワードユーティリティプログラムがユーザによって起動された時、パスワードユーティリティプログラムは、最初に、認証ダイアログ２０１を表示する。認証ダイアログ２０１は、パスワードユーティリティプログラムを使用するユーザを認証する画面である。
【００３９】
認証ダイアログ２０１は、ユーザ認証の２種類の方法を提供する。一つはパスワード入力を使用する方法であり、もう一つはＳＤトークンを使用する方法である。認証ダイアログ２０１には、トークン認証エリア２０２とパスワード認証エリア２０３が配置されている。トークン認証エリア２０２およびパスワード認証エリア２０３にはそれぞれラジオボタンが設けられており、ユーザによってクリックされたラジオボタンに対応する認証方法が有効となる。
【００４０】
トークン認証エリア２０２には、ＳＤカード２１が装着されているディスクドライブ番号をユーザに指定させるためのプルダウンメニュー２０４が設けられている。トークン認証が有効な場合においては、認証ダイアログ２０１上の［認証］ボタン２０６がユーザによってクリックされた時、パスワードユーティリティプログラムは、プルダウンメニュー２０４で指定されたドライブ番号のディスクドライブをアクセスする。これにより、ＳＤカード２１からトークンデータが読み込まれる。このトークンデータの内容により、パスワードユーティリティプログラムは、そのプログラムを起動したユーザが“スーパバイザ”／“ユーザ”のいずれであるかを判別することができる。
【００４１】
パスワード認証エリア２０３には、パスワード入力フィールド２０５が設けられている。パスワード認証を行う場合、ユーザは、キーボード１３を用いたタイピングによってパスワードを入力した後、［認証］ボタン２０６をクリックする。パスワードユーティリティプログラムは、入力されたパスワードがコンピュータ１に登録された“スーパバイザ”パスワード／“ユーザ”パスワードのいずれに一致するかをチェックすることにより、そのプログラムを起動したユーザが“スーパバイザ”／“ユーザ”のいずれであるかを判別することができる。
【００４２】
認証ダイアログ２０１を用いたユーザ認証が実行された後、図５のメインダイアログ３０１がパスワードユーティリティプログラムによって最初に表示される。
【００４３】
図５のメインダイアログ３０１は、２つのタブ、［ユーザパスワード］タブ３０２および［スーパバイザパスワード］タブ３０３を含む。［ユーザパスワード］タブ３０２は、“ユーザ”パスワードの設定、削除、変更を行うためのユーザパスワード機能と、“ユーザ”トークンの作成、無効化に関するユーザトークン機能を提供する。
【００４４】
［ユーザパスワード］タブ３０２上の［ユーザパスワード］には、［Ｓｅｔ］ボタン３０６、［Ｄｅｌｅｔｅ］ボタン３０７、および［Ｃｈａｎｇｅ］ボタン３０８が配置されている。［Ｓｅｔ］ボタン３０６は、“ユーザ”パスワードをコンピュータ１に登録するための操作ボタンである。［Ｄｅｌｅｔｅ］ボタン３０７は、コンピュータ１に登録された“ユーザ”パスワードを削除するための操作ボタンである。［Ｃｈａｎｇｅ］ボタン３０８は、コンピュータ１に登録された“ユーザ”パスワードを変更するための操作ボタンである。

【００４５】
［ユーザパスワード］タブ３０２上の［ユーザトークン］には、［Ｃｒｅａｔｅ］ボタン３０９、および［Ｄｉｓａｂｌｅ］ボタン３１０が配置されている。［Ｃｒｅａｔｅ］ボタン３０９は、“ユーザ”トークンを作成するための操作ボタンである。［Ｄｉｓａｂｌｅ］ボタン３１０は、既に作成された“ユーザ”トークンを無効化するための操作ボタンである。［Ｄｉｓａｂｌｅ］ボタン３１０がクリックされたとき、パスワードユーティリティプログラムは、コンピュータ１に“ユーザ”パスワードと一緒に登録されているトークン識別情報を削除する。
【００４６】
次に、図６を参照して、［スーパバイザパスワード］タブ３０３の構成を説明する。
【００４７】
［スーパバイザパスワード］タブ３０３は、“スーパバイザ”パスワードの設定、削除、変更を行うためのスーパバイザパスワード機能と、“スーパバイザ”トークンの作成、無効化に関するスーパバイザトークン機能と、ユーザポリシーの設定／変更機能を提供する。これら各機能は、“スーパバイザ”として認証されたユーザにのみ許可される。
【００４８】
［スーパバイザパスワード］タブ３０３上の［スーパバイザパスワード］には、［Ｓｅｔ］ボタン４０４、［Ｄｅｌｅｔｅ］ボタン４０５、および［Ｃｈａｎｇｅ］ボタン４０６が配置されている。［Ｓｅｔ］ボタン４０４は、“スーパバイザ”パスワードをコンピュータ１に登録するための操作ボタンである。［Ｄｅｌｅｔｅ］ボタン４０５は、コンピュータ１に登録された“スーパバイザ”パスワードを削除するための操作ボタンである。［Ｃｈａｎｇｅ］ボタン４０６は、コンピュータ１に登録された“スーパバイザ”パスワードを変更するための操作ボタンである。
【００４９】
［スーパバイザパスワード］タブ３０３上の［スーパバイザトークン］には、［Ｃｒｅａｔｅ］ボタン４０７、および［Ｄｉｓａｂｌｅ］ボタン４０８が配置されている。［Ｃｒｅａｔｅ］ボタン４０７は、“スーパバイザ”トークンを作成するための操作ボタンである。［Ｄｉｓａｂｌｅ］ボタン４０８は、既に作成された“スーパバイザ”トークンを無効化するための操作ボタンである。［Ｄｉｓａｂｌｅ］ボタン４０８がクリックされたとき、パスワードユーティリティプログラムは、コンピュータ１に“スーパバイザ”パスワードと一緒に登録されているトークン識別情報を削除する。
【００５０】
［スーパバイザパスワード］タブ３０３上の［ユーザポリシー］には、［Ｓｅｔ］ボタン４０９が配置されている。［Ｓｅｔ］ボタン４０９は、“ユーザ”トークンに格納すべきポリシー情報の内容を設定／変更するための操作ボタンである。“ユーザ”トークンに格納すべきポリシー情報のデフォルトは予め決められている。“スーパバイザ”は、ポリシー情報を任意の内容に変更することが出来る。
【００５１】
図７は、トークン作成ダイアログ６０１を示している。メインダイアログ３０１上の［ユーザ／スーパバイザトークン］の［Ｃｒｅａｔｅ］ボタン３０９または４０７がクリックされた時、パスワードユーティリティプログラムは、トークン作成ダイアログ６０１を表示する。
【００５２】
“スーパバイザ”は、“ユーザ”トークンおよび“スーパバイザ”トークンの両方を作成することができる。“ユーザ”が作成できるのは、“ユーザ”トークンのみである。
【００５３】
トークン作成ダイアログ６０１には、ＳＤカード２１が装着されているディスクドライブ番号をユーザに指定させるためのプルダウンメニュー６０２が設けられている。ＳＤカード２１は、ＳＤトークンの作成前にフォーマットされなければならない。トークン作成ダイアログ６０１上の［Ｃｒｅａｔｅ］ボタン６０３がクリックされた時、パスワードユー

ティリティプログラムは、トークンデータをＳＤカード２１に格納することによって、ＳＤトークン（“ユーザ”トークンまたは“スーパバイザ”トークン）を作成する。

【００５４】

図８には、ユーザポリシー設定ダイアログ８０１が示されている。ユーザポリシー設定ダイアログ８０１は、“ユーザ”トークンに書き込むべきポリシー情報の内容を設定／変更するための画面である。

【００５５】

メインダイアログ３０１上の［ユーザポリシー］の［Ｓｅｔ］ボタン４０９がクリックされた時、パスワードユーティリティプログラムは、ユーザポリシー設定ダイアログ８０１を表示する。ユーザポリシー設定ダイアログ８０１上には、コンピュータ１が有する複数の機能それぞれについてその実行を許可／禁止するための複数の設定項目が配置されている。各設定項目には、その設定項目に対応する操作の実行を許可するためのチェックボックスが設けられている。各設定項目の意味は次の通りである。

【００５６】

［Ｐｅｒｍｉｔ ｔｏ ｓｅｔ Ｕｓｅｒ Ｐａｓｓｗｏｒｄ］：この設定項目は、ユーザが“ユーザ”パスワードの登録操作をメインダイアログ３０１上で行うことを許可するか否かを指定する。

【００５７】

［Ｐｅｒｍｉｔ ｔｏ ｄｅｌｅｔｅ Ｕｓｅｒ Ｐａｓｓｗｏｒｄ］：この設定項目は、ユーザが“ユーザ”パスワードの削除操作をメインダイアログ３０１上で行うことを許可するか否かを指定する。

【００５８】

［Ｐｅｒｍｉｔ ｔｏ ｃｈａｎｇｅ Ｕｓｅｒ Ｐａｓｓｗｏｒｄ］：この設定項目は、ユーザが“ユーザ”パスワードの変更操作をメインダイアログ３０１上で行うことを許可するか否かを指定する。

【００５９】

［Ｐｅｒｍｉｔ ｔｏ ｃｒｅａｔｅ Ｕｓｅｒ Ｔｏｋｅｎ］：この設定項目は、ユーザが“ユーザ”トークンの作成操作をメインダイアログ３０１上で行うことを許可するか否かを指定する。

【００６０】

［Ｐｅｒｍｉｔ ｔｏ ｃｒｅａｔｅ Ｕｓｅｒ Ｔｏｋｅｎ］：この設定項目は、ユーザが“ユーザ”トークンの無効化操作をメインダイアログ３０１上で行うことを許可するか否かを指定する。

【００６１】

［Ｐｅｒｍｉｔ ｔｏ ｂｏｏｔ ｏｒ ｒｅｓｕｍｅ ｂｙ Ｕｓｅｒ Ｐａｓｓｗｏｒｄ］：この設定項目は、コンピュータ１のブートまたはレジューム時における認証を“ユーザ”パスワードを用いて行うことを許可するか否かを指定する。もしこの設定項目がチェックされないならば、ブートまたはレジューム時における認証のために使用可能なパスワードは“スーパバイザ”パスワードのみとなる。

【００６２】

［Ｐｅｒｍｉｔ ｔｏ ｕｓｅ ＨＷ Ｓｅｔｕｐ ｏｒ ＢＩＯＳ Ｓｅｔｕｐ］：この設定項目は、ユーザがコンピュータ１のハードウェアセットアップ機能（またはＢＩＯＳセットアップ機能）を使用することを許可するか否かを指定する。もしこの設定項目がチェックされないならば、ハードウェアセットアップ機能（またはＢＩＯＳセットアップ機能）を用いたコンピュータ１の動作環境の変更操作は、“スーパバイザ”のみに許可される。

【００６３】

［Ｐｅｒｍｉｔ ｔｏ ｕｐｄａｔｅ ＢＩＯＳ］：この設定項目は、ユーザがコンピュータ１のＢＩＯＳを更新するためのＢＩＯＳ更新機能を使用することを許可するか否かを指定する。もしこの設定項目がチェックされないならば、ＢＩＯＳ更新機能は、“スー

パバイザ”のみに許可される。

【００６４】

このように、ポリシー情報は、“ユーザ”の操作を制限する複数のルールの集合である。“スーパバイザ”だけが、ユーザポリシー設定ダイアログ８０１上でポリシー情報の内容を設定／変更することができる。

【００６５】

ユーザポリシー設定ダイアログ８０１上の［ＯＫ］ボタン８０５がクリックされた時、パスワードユーティリティプログラムは、ユーザポリシー設定ダイアログ８０１上の各チェックボックスの状態に応じて、新たなポリシー情報を生成する。このポリシー情報は、ＢＩＯＳ－ＲＯＭ１０８内に格納される。そして、“ユーザ”トークンの作成時に、ＢＩＯＳ－ＲＯＭ１０８内に格納されているポリシー情報がＳＤカード２１に書き込まれる。

【００６６】

次に、図９のフローチャートを参照して、パスワードユーティリティプログラムによって実行されるＳＤトークン作成処理の手順を説明する。以下では、例えば図４の［認証］ダイアログ２０１によって、現在のユーザが“ユーザ”／“スーパバイザ”のいずれであるかがパスワードユーティリティプログラムによって既に認証されているものとする。

【００６７】

パスワードユーティリティプログラムは、まず、ＬＣＤ１２１にメインダイアログ３０１を表示する（ステップＳ１０１）。メインダイアログ３０１上の［ユーザ／スーパバイザトークン］の［Ｃｒｅａｔｅ］ボタン３０９または４０７がクリックされた時（ステップＳ１０２のＹＥＳ）、パスワードユーティリティプログラムは、ＳＤカード２１がコンピュータ１に装着（接続）されているか否かを判別する（ステップＳ１０３，Ｓ１０５）。もしＳＤカード２１が未装着であれば（ステップＳ１０４のＮＯ）、ＳＤカードを装着すべきことを示すエラーメッセージがＬＣＤ１２１に表示される（ステップＳ１０５）。

【００６８】

ＳＤカードが装着されているならば（ステップＳ１０４のＹＥＳ）、パスワードユーティリティプログラムは、ＳＤカード２１が正しくフォーマットされているかどうかを判別する（ステップＳ１０６，Ｓ１０７）。もしＳＤカード２１が正しくフォーマットされていないならば（ステップＳ１０７のＮＯ）、フォーマットされたＳＤカードを装着すべきことを示すエラーメッセージがＬＣＤ１２１に表示される（ステップＳ１０８）。

【００６９】

ＳＤカード２１が正しくフォーマットされているならば（ステップＳ１０７のＹＥＳ）、パスワードユーティリティプログラムは、ＳＤトークンの作成処理を開始する。

【００７０】

まず、パスワードユーティリティプログラムは、ステップＳ１０２でクリックされたボタンが［スーパバイザトークン］の［Ｃｒｅａｔｅ］ボタン４０７および［ユーザトークン］の［Ｃｒｅａｔｅ］ボタン３０９のいずれであるかを判別することによって、作成要求されたＳＤトークンが“スーパバイザ”トークンおよび“ユーザ”トークンのいずれであるかを決定する（ステップＳ１０９）。“スーパバイザ”トークンの作成は、“スーパバイザ”として認証されたユーザにのみ許可される。

【００７１】

作成要求されたＳＤトークンが“スーパバイザ”トークンであるならば、パスワードユーティリティプログラムは、スーパバイザ用トークンデータを作成する（ステップＳ１１０）。このステップＳ１１０においては、まず、“スーパバイザ”トークン用の認証情報が生成される。この“スーパバイザ”トークン用の認証情報は、例えば、コンピュータ１に登録されている“スーパバイザ”パスワードに基づいて生成される。また、ユーザ権限レベルが“スーパバイザ”であることを示すユーザ権限レベル情報と、全ての機能を使用可能であることを示すポリシー情報とが準備される。この後、パスワードユーティリティプログラムは、認証情報、ユーザ権限レベル情報、およびポリシー情報を含むトークンデータを、ＳＤカード２１の第１記憶エリア３４に書き込む（ステップＳ１１１）。このステ

ップＳ１１１においては、作成した“スーパバイザ”トークンに対応するトークン識別情報を、“スーパバイザ”パスワードに対応付けてＢＩＯＳ－ＲＯＭ１０８に書き込む処理も行われる。

【００７２】

作成要求されたＳＤトークンが“ユーザ”トークンであるならば、パスワードユーティリティプログラムは、まず、“ユーザ”トークン用の現在のポリシー情報の内容をＢＩＯＳ－ＲＯＭ１０８からリードする（ステップＳ１１２）。そして、パスワードユーティリティプログラムは、ユーザ用トークンデータを作成する（ステップＳ１１３）。このステップＳ１１３においては、“ユーザ”トークン用の認証情報が生成される。“ユーザ”トークン用の認証情報は、例えば、コンピュータ１に登録されている“ユーザ”パスワードに基づいて生成される。また、ユーザ権限レベルが“ユーザ”であることを示すユーザ権限レベル情報と、ポリシー情報とが準備される。このポリシー情報は、ＢＩＯＳ－ＲＯＭ１０８からリードされたものである。この後、パスワードユーティリティプログラムは、認証情報、ユーザ権限レベル情報、およびポリシー情報を含むトークンデータを、ＳＤカード２１の第１記憶エリア３４に書き込む（ステップＳ１１１）。このステップＳ１１１においては、作成した“ユーザ”トークンに対応するトークン識別情報を、“ユーザ”パスワードに対応付けてＢＩＯＳ－ＲＯＭ１０８に書き込む処理も行われる。

【００７３】

次に、図１０のフローチャートを参照して、パスワードユーティリティプログラムによって実行されるユーザポリシー設定／変更処理の手順を説明する。以下では、例えば図４の［認証］ダイアログ２０１によって現在のユーザが“ユーザ”／“スーパバイザ”のいずれであるかが既に認証されているものとする。

【００７４】

パスワードユーティリティプログラムは、まず、ＬＣＤ１２１にメインダイアログ３０１を表示する（ステップＳ２０１）。メインダイアログ３０１上の［スーパバイザパスワード］タブ３０３がクリックされた時（ステップＳ２０２のＹＥＳ）、パスワードユーティリティプログラムは、現在のユーザが“スーパバイザ”および“ユーザ”のどちらとして認証されているかを判別する（ステップＳ２０３）。

【００７５】

もし現在のユーザが“ユーザ”として認証されているならば（ステップＳ２０３のＮＯ）、パスワードユーティリティプログラムは、［スーパバイザパスワード］タブ３０３上のスーパバイザパスワード機能、スーパバイザトークン機能、及びユーザポリシー設定／変更機能を全て無効化する（ステップＳ２０４）。この場合、［スーパバイザパスワード］タブ３０３上の全てのボタンは非表示となる。

【００７６】

もし現在のユーザが“スーパバイザ”として認証されているならば（ステップＳ２０３のＹＥＳ）、パスワードユーティリティプログラムは、［スーパバイザパスワード］タブ３０３上のスーパバイザパスワード機能、スーパバイザトークン機能、及びユーザポリシー設定／変更機能を全て有効にする（ステップＳ２０５）。この場合、［スーパバイザパスワード］タブ３０３上の全てのボタンが表示される。

【００７７】

［スーパバイザパスワード］タブ３０３上の［ユーザポリシー］の［Ｓｅｔ］ボタン４０９がクリックされたならば（ステップＳ２０６のＹＥＳ）、パスワードユーティリティプログラムは、図８のユーザポリシー設定ダイアログ８０１を表示する（ステップＳ２０６）。“スーパバイザ”は、ユーザポリシー設定ダイアログ８０１上で複数の機能それぞれについて“ユーザ”に許可すべきか否かを指定することができる。

【００７８】

ユーザポリシー設定ダイアログ８０１上の［ＯＫ］ボタン８０５がクリックされたならば（ステップＳ２０７のＹＥＳ）、パスワードユーティリティプログラムは、ユーザポリシー設定ダイアログ８０１上の各チェックボックスの状態に応じて、“ユーザ”トークンに

格納すべきポリシー情報の内容を変更する（ステップＳ２０８）。そして、パスワードユーティリティプログラムは、変更したポリシー情報の内容を新たなポリシー情報としてＢＩＯＳ－ＲＯＭ１０８にセーブする（ステップＳ２０９）。これにより、“ユーザ”パスワードに対応付けてＢＩＯＳ－ＲＯＭ１０８に格納されているポリシー情報の内容が更新される。

【００７９】

次に、図１１のフローチャートを参照して、コンピュータ１の電源投入時にＢＩＯＳによって実行されるユーザ認証処理について説明する。

【００８０】

パワーボタン１４がオンされた時、ＥＣ／ＫＢＣ１０９によってコンピュータ１がパワーオンされる。ＣＰＵ１０１は、最初に、ＢＩＯＳを実行する。ＢＩＯＳは、“ユーザ”／“スーパバイザ”パスワードがコンピュータ１に登録されているかどうかを判断する（ステップＳ３０１）。“ユーザ”／“スーパバイザ”パスワードが登録されていないならば（ステップＳ３０１のＮＯ）、ＢＩＯＳは、ユーザによるコンピュータ１の使用を直ちに許可し、コンピュータ１を起動する（ステップＳ３１５）。このステップＳ３１５では、レジューム処理またはオペレーティングシステムのブートストラップ処理が実行される。

【００８１】

コンピュータ１に“ユーザ”／“スーパバイザ”パスワードが登録されているならば（ステップＳ３０１のＹＥＳ）、ＢＩＯＳは、ユーザ認証処理を行う。ＢＩＯＳは、ユーザ認証の２種類の方法を提供する。一つはパスワード入力を使用する方法であり、もう一つはＳＤトークンを使用する方法である。

【００８２】

ＢＩＯＳは、まず、ＳＤカード２１（ＳＤトークン）がコンピュータ１に装着されているかどうかを判断する（ステップＳ３０２）。ＳＤカード２１が装着されているならば（ステップＳ３０２のＹＥＳ）、ＢＩＯＳは、ＳＤカード２１に格納されている認証情報をリードし（ステップＳ３０３）、そのリードした認証情報を使用して、現在のユーザにコンピュータ１の使用を許可するか否かを判別するための認証処理を実行する（ステップＳ３０４）。このステップＳ３０４では、リードした認証情報に基づいて、ＳＤカード２１が正当なＳＤトークンであるか否かが判別される。具体的には、ステップＳ３０４においては、例えば、リードした認証情報に対応するトークン識別情報がＢＩＯＳ－ＲＯＭ１０８に存在するかどうかを判別する処理、あるいはリードした認証情報がＢＩＯＳ－ＲＯＭ１０８に登録されている“ユーザ”／“スーパバイザ”パスワードに一致するかどうかを判別する処理、等が実行される。

【００８３】

ＳＤカード２１が正当なＳＤトークンであることが判別されたならば（ステップＳ３０５のＹＥＳ）、ユーザによるコンピュータ１の使用が許可される。この場合、ＢＩＯＳは、現在のユーザが実行可能な機能を決定するために、ＳＤカード２１に格納されているポリシー情報およびユーザ権限レベル情報をリードし（ステップＳ３０６）、その後にコンピュータ１を起動する（ステップＳ３０７）。このステップＳ３０７では、レジューム処理またはオペレーティングシステムのブートストラップ処理が実行される。コンピュータ１が起動された後は、ＳＤカード２１からリードされたポリシー情報およびユーザ権限レベル情報に基づいてユーザの操作を制限する処理が、ＢＩＯＳまたはパスワードユーティリティプログラムによって実行される（ステップＳ３０８）。

【００８４】

すなわち、ユーザ権限レベル情報で指定される現在のユーザの権限レベルが“ユーザ”である場合には、その“ユーザ”が実行可能な機能は、ＳＤカード２１からリードされたポリシー情報によって制限される。

【００８５】

ここで、複数のコンピュータを複数人で共用する環境を考える。どのコンピュータにも、上述のＢＩＯＳおよびパスワードユーティリティプログラムが実装されているとする。各

ユーザは、自分が所有するＳＤトークンを使用することにより、複数のコンピュータの各々を使用することができる。この場合、権限レベルが“ユーザ”である各ユーザは、どのコンピュータを利用する場合においても、自身のＳＤトークンに格納されているポリシー情報によって規定された、同一のユーザ操作制限を受ける。よって、個々のコンピュータに各“ユーザ”に対応する操作制限情報を個別に設定するという操作を行うことなく、複数のコンピュータを統一的に管理することが可能となる。

【００８６】

ユーザ権限レベル情報で指定される現在のユーザの権限レベルが“スーパバイザ”である場合には、基本的には、実行可能な機能は制限されない。

【００８７】

ＳＤカード２１（ＳＤトークン）がコンピュータ１に装着されていない場合には（ステップＳ３０２のＮＯ）、ＢＩＯＳは、ユーザによるパスワード入力を受け付ける。ユーザがキーボード１３によってパスワードをタイプ入力した場合（ステップＳ３０９のＹＥＳ）、ＢＩＯＳは、入力されたパスワードとコンピュータ１に登録されている“ユーザ”／“スーパバイザ”パスワードとを比較することにより、現在のユーザにコンピュータ１の使用を許可するか否かを判別するための認証処理を実行する（ステップＳ３１０）。この認証処理によって、入力されたパスワードがコンピュータ１に登録されている“ユーザ”または“スーパバイザ”パスワードに一致した場合、現在のユーザに対してコンピュータ１の使用が許可される。

【００８８】

この場合、ＢＩＯＳは、現在のユーザが実行可能な機能を決定するために、入力されたパスワードと一致した登録パスワードに対応するポリシー情報およびユーザ権限レベル情報をＢＩＯＳ－ＲＯＭ１０８からリードし（ステップＳ３１２）、その後にコンピュータ１を起動する（ステップＳ３１３）。このステップＳ３１３では、レジューム処理またはオペレーティングシステムのブートストラップ処理が実行される。コンピュータ１が起動された後は、ＢＩＯＳ－ＲＯＭ１０８からリードされたポリシー情報およびユーザ権限レベル情報に基づいてユーザの操作を制限する処理が、ＢＩＯＳまたはパスワードユーティリティプログラムによって実行される（ステップＳ３１４）。

【００８９】

すなわち、ユーザ権限レベル情報で指定される現在のユーザの権限レベルが“ユーザ”である場合には、その“ユーザ”が実行可能な機能は、ＢＩＯＳ－ＲＯＭ１０８に格納されているポリシー情報によって制限される。

【００９０】

以上のように、本実施形態によれば、ＳＤトークンに認証情報のみならずポリシー情報も併せて記憶することにより、認証に使用されるＳＤトークン毎に、そのＳＤトークンに対応したユーザ操作制限を行うことが可能となる。よって、複数のコンピュータを複数人で使用する環境であっても、個々のコンピュータに個別に操作制限情報を設定するという操作を行うことなく、複数のコンピュータを統一的に管理することが可能となる。

【００９１】

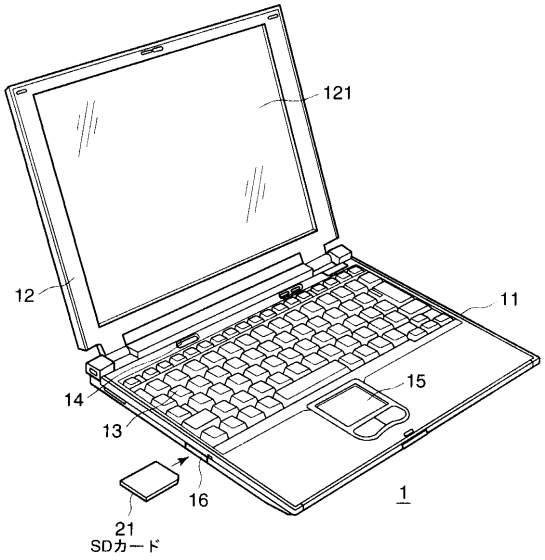
またトークンデバイスとして、ファイルシステムからのアクセスが禁止された記憶エリアを持つＳＤカードを利用しているので、トークンデバイス内に格納されたトークンデータの不正な書き換えを防止することもできる。

【００９２】

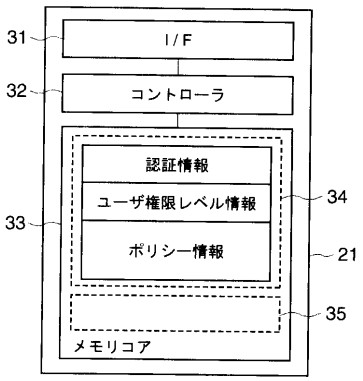
なお、本発明は、上記実施形態に限定されるものではなく、実施段階ではその要旨を逸脱しない範囲で種々に変形することが可能である。更に、上記実施形態には種々の段階の発明が含まれており、開示される複数の構成要件における適宜な組み合わせにより種々の発明が抽出され得る。例えば、実施形態に示される全構成要件から幾つかの構成要件が削除されても、発明が解決しようとする課題の欄で述べた課題が解決でき、発明の効果の欄で述べられている効果が得られる場合には、この構成要件が削除された構成が発明として抽出され得る。

【００９３】
【発明の効果】
以上のように本発明によれば、操作制限情報の設定操作無しで各ユーザが実行可能な操作を制限することが可能となる。
【図面の簡単な説明】
【図１】本発明の一実施形態に係るコンピュータのディスプレイ開放状態における外観を示す図。
【図２】同実施形態のコンピュータで使用されるＳＤトークンを説明するための図。
【図３】同実施形態のコンピュータのシステム構成を示すブロック図。
【図４】同実施形態のコンピュータで使用される認証ダイアログ画面の例を示す図。
【図５】同実施形態のコンピュータで使用されるメインダイアログ画面上のユーザパスワードタブの例を示す図。
【図６】同実施形態のコンピュータで使用されるメインダイアログ画面上のスーパバイザパスワードタブの例を示す図。
【図７】同実施形態のコンピュータで使用されるトークン作成ダイアログ画面の例を示す図。
【図８】同実施形態のコンピュータで使用されるユーザポリシー設定ダイアログ画面の例を示す図。
【図９】同実施形態のコンピュータによって実行されるＳＤトークン作成処理の手順を示すフローチャート。
【図１０】同実施形態のコンピュータによって実行されるユーザポリシー設定／変更処理の手順を示すフローチャート。
【図１１】同実施形態のコンピュータによって実行されるユーザ認証処理の手順を示すフローチャート。
【符号の説明】
１…コンピュータ、１１…コンピュータ本体、１２…ディスプレイユニット、１６…カードスロット、２１…ＳＤカード、３４…第１エリア、３５…第２エリア、１０１…ＣＰＵ、１０７…カードコントローラ、１０８…ＢＩＯＳ－ＲＯＭ、２０１…認証ダイアログ、３０１…メインダイアログ、８０１…ユーザポリシー設定ダイアログ。

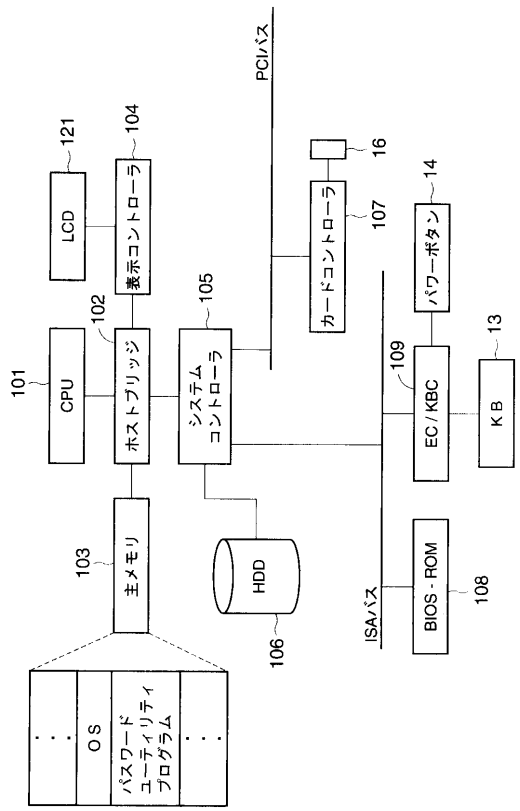
【図１】


121
12
11
15
14
13
16
1
21
SDカード

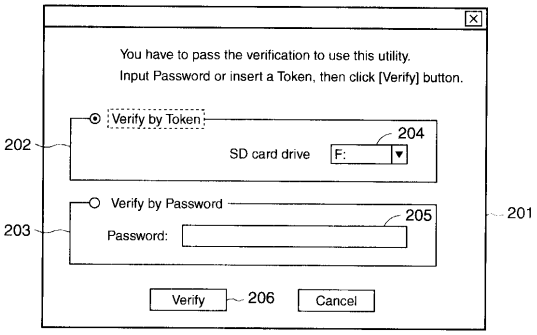
【図２】


31
I/F
32
コントローラ
認証情報
ユーザ権限レベル情報
ポリシー情報
33
34
21
35
メモリコア

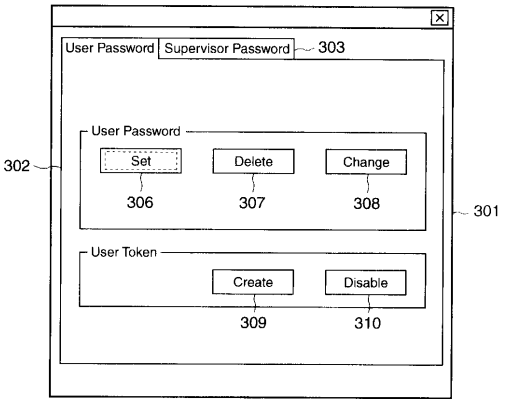
【図３】


PCIバス
121
LCD
104
表示コントローラ
16
107
カードコントローラ
14
パワーボタン
102
105
101
CPU
ホストブリッジ
システムコントローラ
109
EC / KBC
13
KB
103
主メモリ
HDD
106
ISAバス
BIOS - ROM
108
OS
パスワードユーティリティプログラム

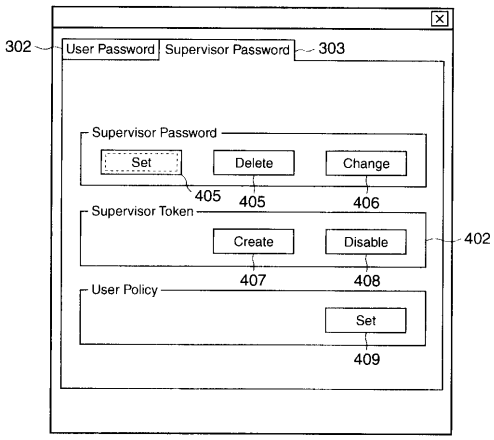
【図４】


You have to pass the verification to use this utility.
Input Password or insert a Token, then click [Verify] button.
Verify by Token
204
202
SD card drive
F:
Verify by Password
205
203
Password:
201
Verify
206
Cancel

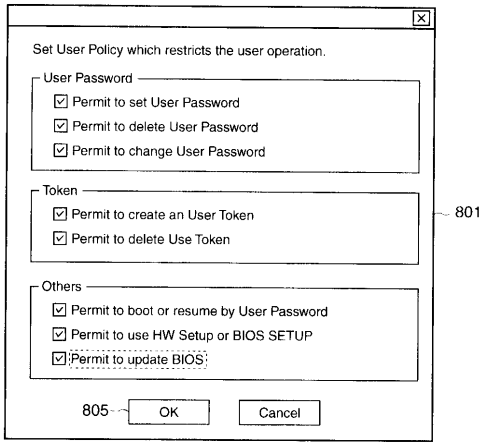
【図５】


User Password
Supervisor Password
303
User Password
302
Set
Delete
Change
306
307
308
301
User Token
Create
Disable
309
310

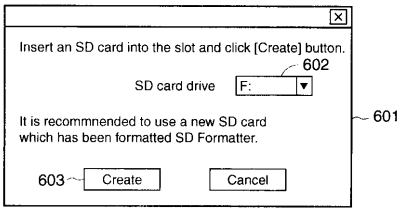
【図６】



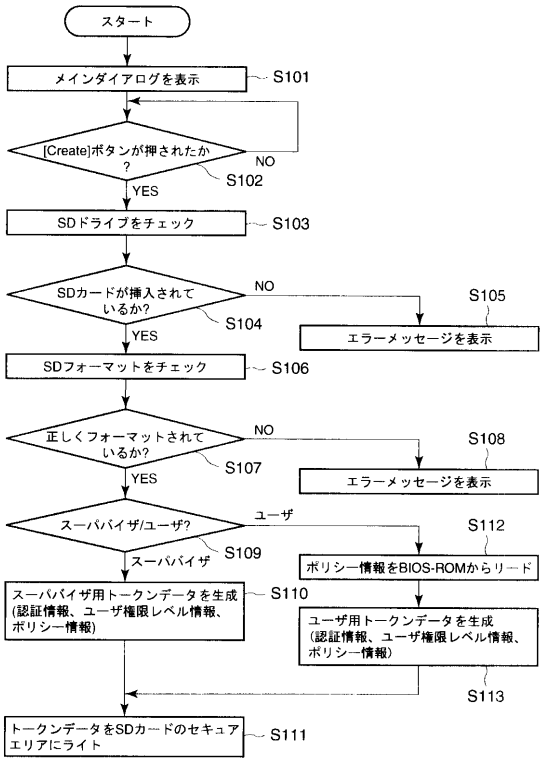
【図８】



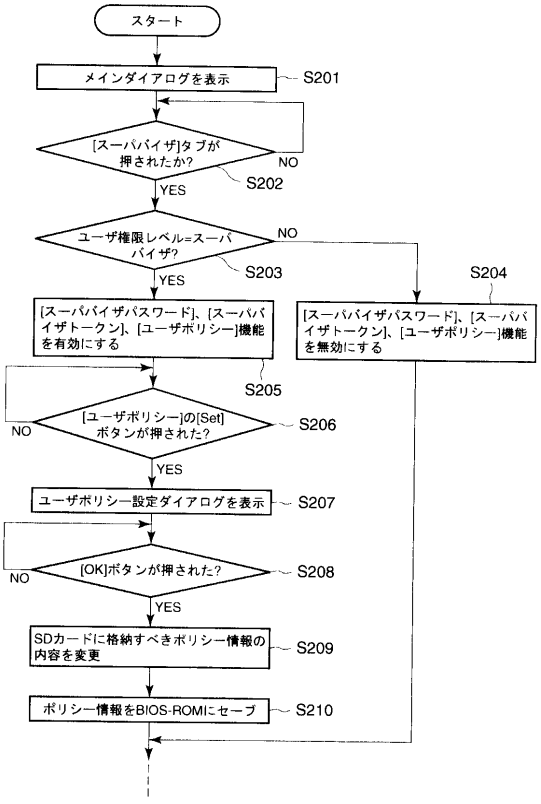
【図７】



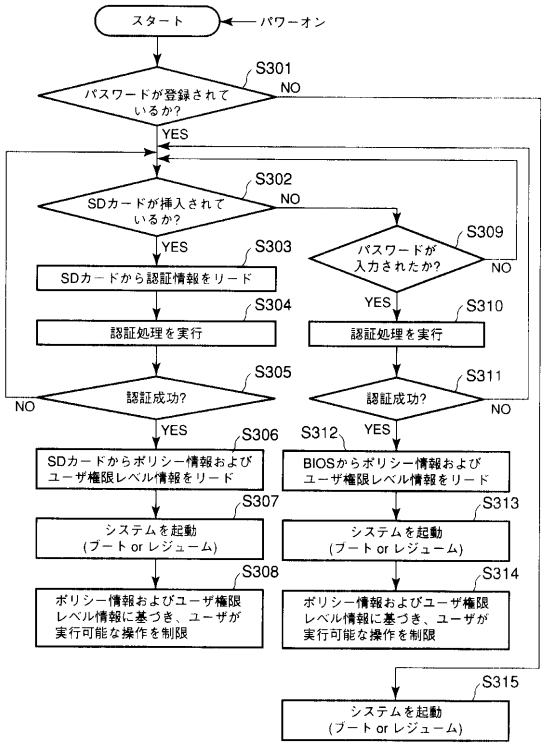
【図９】



【図１０】



【図１１】


スタート
パワーオン
S301
パスワードが登録されているか?
NO
YES
S302
SDカードが挿入されているか?
NO
YES
S303
SDカードから認証情報をリード
S304
認証処理を実行
S305
認証成功?
NO
YES
S306
SDカードからポリシー情報およびユーザ権限レベル情報をリード
S307
システムを起動
(ブート or レジューム)
S308
ポリシー情報およびユーザ権限レベル情報に基づき、ユーザが実行可能な操作を制限
S309
パスワードが入力されたか?
NO
YES
S310
認証処理を実行
S311
認証成功?
NO
YES
S312
BIOSからポリシー情報およびユーザ権限レベル情報をリード
S313
システムを起動
(ブート or レジューム)
S314
ポリシー情報およびユーザ権限レベル情報に基づき、ユーザが実行可能な操作を制限
S315
システムを起動
(ブート or レジューム)

フロントページの続き

(72)発明者　川上　智之
東京都青梅市末広町２丁目９番地　株式会社東芝青梅事業所内

Ｆターム(参考) 5B058 CA02　KA02　KA40