(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5773494号
(P5773494)
(45)発行日　平成27年9月2日(2015.9.2)　(24)登録日　平成27年7月10日(2015.7.10)

(51)Int.Cl.　F I
G06F 21/34 (2013.01)　G06F 21/34

請求項の数 9　(全 15 頁)

(21)出願番号　特願2011-265908(P2011-265908)
(22)出願日　平成23年12月5日(2011.12.5)
(65)公開番号　特開2013-117911(P2013-117911A)
(43)公開日　平成25年6月13日(2013.6.13)
審査請求日　平成26年7月8日(2014.7.8)

(73)特許権者　390009531
インターナショナル・ビジネス・マシーンズ・コーポレーション
ＩＮＴＥＲＮＡＴＩＯＮＡＬ　ＢＵＳＩＮＥＳＳ　ＭＡＣＨＩＮＥＳ　ＣＯＲＰＯＲＡＴＩＯＮ
アメリカ合衆国１０５０４　ニューヨーク州　アーモンク　ニュー　オーチャード　ロード
(74)代理人　100108501
弁理士　上野　剛史
(74)代理人　100112690
弁理士　太佐　種一
(74)代理人　100091568
弁理士　市位　嘉宏

最終頁に続く

(54)【発明の名称】情報処理装置、制御方法及びプログラム

(57)【特許請求の範囲】
【請求項１】
固有の識別情報をセキュアに記憶する認証デバイスが装着されて認証処理を行う情報処理装置において、
前記認証デバイスが装着される装着部と、
第１のプログラムが記憶されている第１の記憶部と、
第２のプログラムが記憶されている第２の記憶部と、
前記認証デバイスの固有の識別情報とカウンタ値とが対応付けられているテーブルが記憶されている第３の記憶部と、
電源が投入された際に、前記第１の記憶部から前記第１のプログラムを読み出して起動し、当該第１のプログラムにしたがって、前記装着部に装着されている前記認証デバイスの識別情報を読み出し、前記テーブルを参照して、前記認証デバイスの識別情報に対応付けられているカウンタ値が所定の値よりも大きいことを条件に、前記認証デバイスとの間で認証処理を行い、当該認証処理が成功した場合に、前記第２の記憶部から前記第２のプログラムを読み出して起動し、当該第２のプログラムの起動中に前記認証デバイスが前記装着部に装着され続けていた場合、前記認証デバイスの固有の識別情報に対応する前記テーブルのカウンタ値を減算する制御部を備える情報処理装置。
【請求項２】
前記制御部は、前記装着部に前記認証デバイスが装着されていない場合、前記テーブルを参照し、前記認証デバイスの識別情報に対応付けられているカウンタ値が所定の値以下

の場合、又は前記装着部に装着されている前記認証デバイスとの間で行った認証処理が失敗した場合には、前記第２のプログラムを起動しないように制御する請求項１記載の情報処理装置。

【請求項３】

前記制御部は、前記第２のプログラムが起動中に、所定のタイミングで前記認証デバイスとの間において再認証を要求して、前記テーブルを参照し、前記認証デバイスの識別情報に対応付けられているカウンタ値が所定の値よりも大きいことを条件に、前記認証デバイスとの間で認証処理を行い、当該認証処理が成功した場合に、当該第２のプログラムの実行を継続する請求項１記載の情報処理装置。

【請求項４】

前記制御部は、前記再認証を要求したときに、前記装着部に前記認証デバイスが装着されなかった場合、前記テーブルを参照し、前記認証デバイスの識別情報に対応付けられているカウンタ値が所定の値以下の場合、又は前記装着部に装着されている前記認証デバイスとの間で行った再認証処理が失敗した場合には、当該第２のプログラムの実行を制限又は停止するように制御する請求項３記載の情報処理装置。

【請求項５】

前記制御部は、前記第２のプログラムが起動中に、前記認証デバイスが前記装着部に装着されていないことを条件に、前記認証デバイスの固有の識別情報に対応する前記テーブルのカウンタ値を加算する請求項１乃至４のいずれか一項に記載の情報処理装置。

【請求項６】

前記制御部は、前記第２のプログラムが起動中に、実行されているアプリケーションプログラムが所定のアプリケーションプログラムであると判断した場合には、前記認証デバイスが前記装着部に装着され続けていても、前記認証デバイスの固有の識別情報に対応する前記テーブルのカウンタ値を減算しないように制御する請求項１記載の情報処理装置。

【請求項７】

前記制御部は、所定のタイミングで前記所定のアプリケーションプログラムの継続使用の有無を問い合わせる確認メッセージを表示部に表示するように制御する請求項６記載の情報処理装置。

【請求項８】

固有の識別情報をセキュアに記憶する認証デバイスを用いて情報処理装置により認証処理を行う認証方法において、

前記情報処理装置の電源が投入された際に、第１のプログラムを読み出して起動する第１の起動ステップと、

当該第１のプログラムにしたがって、前記情報処理装置の装着部に装着されている前記認証デバイスの識別情報を読み出し、前記認証デバイスの固有の識別情報とカウンタ値とが対応付けられているテーブルを参照して、前記認証デバイスの識別情報に対応付けられているカウンタ値が所定の値よりも大きいかどうかを判断する判断ステップと、

前記判断ステップによりカウンタ値が所定の値よりも大きいと判断した場合、前記装着部に装着されている前記認証デバイスとの間で認証処理を行う認証処理ステップと、

前記認証処理が成功した場合には、第２のプログラムを読み出して起動する第２の起動ステップと、

前記第２のプログラムの起動中に前記認証デバイスが前記装着部に装着され続けていたら、前記認証デバイスの固有の識別情報に対応する前記テーブルのカウンタ値を減算する減算ステップを備える制御方法。

【請求項９】

固有の識別情報をセキュアに記憶する認証デバイスを用いた認証処理をコンピュータによって実現するためのプログラムであって、

情報処理装置の電源が投入された際に、第１のプログラムを読み出して起動する第１の起動ステップと、

当該第１のプログラムにしたがって、前記情報処理装置の装着部に装着されている前記

認証デバイスの識別情報を読み出し、前記認証デバイスの固有の識別情報とカウンタ値とが対応付けられているテーブルを参照して、前記認証デバイスの識別情報に対応付けられているカウンタ値が所定の値よりも大きいかどうかを判断する判断ステップと、
前記判断ステップによりカウンタ値が所定の値よりも大きいと判断した場合、前記装着部に装着されている前記認証デバイスとの間で認証処理を行う認証処理ステップと、
前記認証処理が成功した場合には、第２のプログラムを読み出して起動する第２の起動ステップと、
前記第２のプログラムの起動中に前記認証デバイスが前記装着部に装着され続けていたら、前記認証デバイスの固有の識別情報に対応する前記テーブルのカウンタ値を減算する減算ステップをコンピュータによって実現するためのプログラム。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、認証処理の機能を有する情報処理装置、当該情報処理装置の制御方法及びプログラムに関する。
【背景技術】
【０００２】
コンピュータにインストールされているアプリケーションプログラムの起動を制御する技術がある（例えば、特許文献１を参照）。
具体的には、ＵＳＢインターフェースを有するＵＳＢキーやＵＳＢトークンを用いて認証を行うことにより、当該制御を行うシステムがある。
【０００３】
例えば、ＰＣ等のＵＳＢポートにＵＳＢキー等を装着して、認証を行い、ＵＳＢキー等が装着されている間だけ、コンピュータを利用できるシステムがある（以下、第１のシステムという。）。
【０００４】
また、ＰＣのＵＳＢポートにＵＳＢキー等を装着して、ネットワーク経由でユーザ認証を行い、サーバ側で有効期限を管理するシステムもある（以下、第２のシステムという。）。
【先行技術文献】
【特許文献】
【０００５】
【特許文献１】特開２０１０－１４６１２５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、第１のシステムは、パスワードの代替手段という位置づけであり、ＰＣの盗難や紛失対策には一定の効果があるが、ＵＳＢキー等を装着したままＰＣを盗難・紛失されることは考慮されていない。また、ＰＣにＵＳＢキー等が装着されたまま盗難・紛失に合う可能性が高まり、セキュリティリスクがかえって大きくなる。
【０００７】
また、第２のシステムは、ネットワークの接続が必須であり、単体（スタンドアロン）で有効期限を管理できるものではない。
【０００８】
本発明は、ＵＳＢキー等を利用して認証処理を行う機能を有し、セキュリティリスクを最小限に抑えることができる情報処理装置、制御方法及びプログラムを提供することを目的の一つとする。
【課題を解決するための手段】
【０００９】
本発明に係る情報処理装置は、上記課題を解決するために、固有の識別情報をセキュア

に記憶する認証デバイスが装着されて認証処理を行う情報処理装置において、前記認証デバイスが装着される装着部と、第１のプログラムが記憶されている第１の記憶部と、第２のプログラムが記憶されている第２の記憶部と、前記認証デバイスの固有の識別情報とカウンタ値（以下、「カウント値」ともいう）とが対応付けられているテーブルが記憶されている第３の記憶部と、電源が投入された際に、前記第１の記憶部から前記第１のプログラムを読み出して起動し、当該第１のプログラムにしたがって、前記装着部に装着されている前記認証デバイスの識別情報を読み出し、前記テーブルを参照して、前記認証デバイスの識別情報に対応付けられているカウンタ値が所定の値よりも大きいことを条件に、前記認証デバイスとの間で認証処理を行い、当該認証処理が成功した場合に、前記第２の記憶部から前記第２のプログラムを読み出して起動し、当該第２のプログラムの起動中に前記認証デバイスが前記装着部に装着され続けていた場合、前記認証デバイスの固有の識別情報に対応する前記テーブルのカウント値を減算する制御部を備える構成である。

【００１０】
また、情報処理装置では、制御部は、前記装着部に前記認証デバイスが装着されていない場合、前記テーブルを参照し、前記認証デバイスの識別情報に対応付けられているカウンタ値が所定の値以下の場合、又は前記装着部に装着されている前記認証デバイスとの間で行った認証処理が失敗した場合には、前記第２のプログラムを起動しないように制御する構成でも良い。

【００１１】
また、情報処理装置では、制御部は、前記第２のプログラムが起動中に、所定のタイミングで前記認証デバイスとの間において再認証を要求して、前記テーブルを参照し、前記認証デバイスの識別情報に対応付けられているカウンタ値が所定の値よりも大きいことを条件に、前記認証デバイスとの間で認証処理を行い、当該認証処理が成功した場合に、当該第２のプログラムの実行を継続する構成でも良い。

【００１２】
また、情報処理装置では、制御部は、前記再認証を要求したときに、前記装着部に前記認証デバイスが装着されなかった場合、前記テーブルを参照し、前記認証デバイスの識別情報に対応付けられているカウンタ値が所定の値以下の場合、又は前記装着部に装着されている前記認証デバイスとの間で行った再認証処理が失敗した場合には、当該第２のプログラムの実行を制限又は停止するように制御する構成でも良い。

【００１３】
また、情報処理装置では、制御部は、前記第２のプログラムが起動中に、前記認証デバイスが前記装着部に装着されていないことを条件に、前記認証デバイスの固有の識別情報に対応する前記テーブルのカウント値を加算する構成でも良い。

【００１４】
また、情報処理装置では、制御部は、前記第２のプログラムが起動中に、実行されているアプリケーションプログラムが所定のアプリケーションプログラムであると判断した場合には、前記認証デバイスが前記装着部に装着され続けていても、前記認証デバイスの固有の識別情報に対応する前記テーブルのカウント値を減算しないように制御する構成でも良い。

【００１５】
また、情報処理装置では、制御部は、所定のタイミングで前記所定のアプリケーションプログラムの継続使用の有無を問い合わせる確認メッセージを表示部に表示するように制御する構成でも良い。

【００１６】
本発明に係る制御方法は、上記課題を解決するために、固有の識別情報をセキュアに記憶する認証デバイスを用いて情報処理装置により認証処理を行う認証方法において、前記情報処理装置の電源が投入された際に、第１のプログラムを読み出して起動する第１の起動ステップと、当該第１のプログラムにしたがって、前記情報処理装置の装着部に装着さ

れている前記認証デバイスの識別情報を読み出し、前記認証デバイスの固有の識別情報とカウンタ値とが対応付けられているテーブルを参照して、前記認証デバイスの識別情報に対応付けられているカウンタ値が所定の値よりも大きいかどうかを判断する判断ステップと、前記判断ステップによりカウンタ値が所定の値よりも大きいと判断した場合、前記装着部に装着されている前記認証デバイスとの間で認証処理を行う認証処理ステップと、前記認証処理が成功した場合には、第２のプログラムを読み出して起動する第２の起動ステップと、前記第２のプログラムの起動中に前記認証デバイスが前記装着部に装着され続けていたら、前記認証デバイスの固有の識別情報に対応する前記テーブルのカウント値を減算する減算ステップを備える構成である。

【００１７】

本発明に係るプログラムは、上記課題を解決するために、固有の識別情報をセキュアに記憶する認証デバイスを用いた認証処理をコンピュータによって実現するためのプログラムであって、情報処理装置の電源が投入された際に、第１のプログラムを読み出して起動する第１の起動ステップと、当該第１のプログラムにしたがって、前記情報処理装置の装着部に装着されている前記認証デバイスの識別情報を読み出し、前記認証デバイスの固有の識別情報とカウンタ値とが対応付けられているテーブルを参照して、前記認証デバイスの識別情報に対応付けられているカウンタ値が所定の値よりも大きいかどうかを判断する判断ステップと、前記判断ステップによりカウンタ値が所定の値よりも大きいと判断した場合、前記装着部に装着されている前記認証デバイスとの間で認証処理を行う認証処理ステップと、前記認証処理が成功した場合には、第２のプログラムを読み出して起動する第２の起動ステップと、前記第２のプログラムの起動中に前記認証デバイスが前記装着部に装着され続けていたら、前記認証デバイスの固有の識別情報に対応する前記テーブルのカウント値を減算する減算ステップをコンピュータによって実現するためのものである。

【発明の効果】

【００１８】

本発明によれば、セキュリティリスクを最小限に抑えることができる。

【図面の簡単な説明】

【００１９】

【図１】本発明の情報処理装置の構成を示す図である。

【図２】テーブルの構成を模式的に示す図である。

【図３】第１のプログラム起動中の制御部の具体的な構成と、第２のプログラム起動中の制御部の具体的な構成を示す機能ブロック図である。

【図４】本発明の情報処理装置の動作の流れについての説明に供するフローチャートである。

【図５】テーブルの他の構成例を模式的に示す図である。

【発明を実施するための形態】

【００２０】

以下、本発明の実施形態について図を参照しながら説明する。

図１は、情報処理装置１の構成について示す図である。情報処理装置１は、固有の識別情報をセキュアに記憶する認証デバイス２が装着されて認証処理を行う装置である。

本実施例では、認証デバイス２は、ＵＳＢ（ｕｎｉｖｅｒｓａｌ　ｓｅｒｉａｌ　ｂｕｓ）トークンであるとして説明を行うが、これに限られない。認証デバイス２は、固有の識別情報をセキュアに記憶するものであれば良く、例えば、ＵＳＢキー等でも良い。

【００２１】

情報処理装置１は、図１に示すように、装着部１１と、第１の記憶部１２と、第２の記憶部１３と、第３の記憶部１４と、制御部１５、表示部１６を備える。

装着部１１は、所定の規格（例えば、ＵＳＢ）に準拠したインターフェースであり、認証デバイス２が装着される。

【００２２】

第１の記憶部１２は、第１のプログラムが記憶されている。第１の記憶部１２は、ＲＯ

Ｍ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）で構成されている。第１のプログラムとは、ＢＩＯＳ（Ｂａｓｉｃ　Ｉｎｐｕｔ／Ｏｕｔｐｕｔ　Ｓｙｓｔｅｍ）プログラムのことであり、情報処理装置１の初期化を行うプログラムである。

【００２３】

第２の記憶部１３は、第２のプログラムが記憶されている。第２の記憶部１３は、例えば、ＨＤＤ（ｈａｒｄ　ｄｉｓｃ　ｄｒｉｖｅ）で構成されているが、フラッシュメモリで構成されても良い。第２のプログラムは、基本ソフトウェアであるＯＳ（ｏｐｅｒａｔｉｎｇ　ｓｙｓｔｅｍ）プログラムのことである。

【００２４】

第３の記憶部１４は、認証デバイス２の固有の識別情報と、カウンタ値とが対応付けられているテーブルＴが記憶されている。本実施例では、第３の記憶部１４は、独立した記憶部として説明するが、これに限られず、第２の記憶部１３と同一の構成でも良い。

【００２５】

また、図２は、テーブルＴを模式的に示す図である。テーブルＴは、第２のプログラムを制限なく使用するための有効期限を管理するテーブルであり、例えば、認証デバイス２の固有の識別情報と、カウンタ値と、上限値により構成されている。認証デバイス２の固有の識別情報とは、例えば、製造番号である。カウンタ値は、情報処理装置１の継続使用するための時間を規定するものであり、例えば、一カウンタ一秒である。上限値は、カウンタ値の上限を示している。

【００２６】

また、認証デバイス２は、情報処理装置１において予め所定の登録処理を行うことにより、テーブルＴに登録されるものとする。例えば、管理者は、情報処理装置１を起動し、登録用のアプリケーションを実行し、当該登録用のアプリケーションの指示にしたがって操作を行う。このような登録処理により、登録対象となる認証デバイス２がテーブルＴに登録される。

【００２７】

制御部１５は、電源が投入された際に、第１の記憶部１２から第１のプログラムを読み出して起動し、当該第１のプログラムにしたがって、装着部１１に装着されている認証デバイス２の識別情報を読み出し、テーブルＴを参照して、認証デバイス２の識別情報に対応付けられているカウンタ値が所定の値よりも大きいかどうかの判断を行う。

【００２８】

制御部１５は、カウンタ値が所定の値よりも大きいと判断した場合には、認証デバイス２との間で認証処理を行う。制御部１５は、認証処理が成功した場合に、第２の記憶部１３から第２のプログラムを読み出して起動する。認証処理とは、例えば、ＰＫＩを利用した認証処理である。

【００２９】

制御部１５は、当該第２のプログラムの起動中に認証デバイス２が装着部１１に装着され続けていた場合、認証デバイス２の固有の識別情報に対応するテーブルＴのカウント値を減算する。例えば、制御部１５は、認証デバイス２が装着部１１に装着されている時間に基づいて、一定の割合でカウント値を減算してゆく。

【００３０】

このように構成されることにより、情報処理装置１は、電源投入時において、有効な認証デバイス２を装着部１１に装着するように、ユーザに動機付けを行うことができ、かつ、認証デバイス２が装着部１１に装着され続けていると、テーブルＴのカウント値が減算されてゆくので、認証が終わったタイミングで認証デバイス２を装着部１１から取り外すように、ユーザに動機付けを行うことができる。したがって、情報処理装置１は、例えば、認証デバイス２が装着され続けたまま放置されて、他のユーザに持ち去られるような事態を回避することができ、セキュリティリスクを最小限に抑えることができる。

【００３１】

また、上述では、情報処理装置１の構成と動作について説明したが、これに限られず、

各構成要素を備え、セキュリティリスクを最小限に抑えることができる制御方法や、プログラムとして構成されても良い。

【００３２】

制御部１５は、装着部１１に認証デバイス２が装着されていない場合、テーブルＴを参照し、認証デバイス２の識別情報に対応付けられているカウンタ値が所定の値以下の場合、又は装着部１１に装着されている認証デバイス２との間で行った認証処理が失敗した場合には、第２のプログラムを起動しないように制御する構成でも良い。

【００３３】

具体的には、制御部１５は、電源が投入された際に、第１の記憶部１２から第１のプログラムを読み出して起動し、当該第１のプログラムにしたがって、装着部１１に認証デバイス２が装着されているかどうかを確認する。制御部１５は、装着部１１に認証デバイス２が装着されていない場合、第２のプログラムを起動せずに終了する。なお、制御部１５は、装着部１１に認証デバイス２が装着されていない場合には、表示部１６に「認証デバイス２を装着してください」等のメッセージを表示しても良い。

【００３４】

また、制御部１５は、テーブルＴを参照し、認証デバイス２の識別情報に対応付けられているカウンタ値が所定の値以下の場合には、第２のプログラムを起動せずに終了する。なお、本実施例では、所定の値とは、カウンタ値が「０」を想定するが、これ以外でも良い。また、制御部１５は、表示部１６に「認証デバイス２を装着してください」等のメッセージを表示しても良い。

【００３５】

また、制御部１５は、カウンタ値が所定の値よりも大きい場合であっても、装着部１１に装着されている認証デバイス２との間で行った認証処理が失敗した場合には、第２のプログラムを起動せずに終了する。なお、制御部１５は、表示部１６に「認証デバイス２を装着してください」等のメッセージを表示しても良い。

【００３６】

このように構成されることにより、情報処理装置１は、少なくとも、カウンタ値が所定の値以下の場合にも第２のプログラムが起動しなくなるので、認証が終了したタイミングで認証デバイス２を装着部１１から取り外すように、ユーザに動機付けを行うことができる。したがって、情報処理装置１は、例えば、認証デバイス２が装着され続けたまま放置されて、他のユーザに持ち去られるような事態を回避することができ、セキュリティリスクを最小限に抑えることができる。

【００３７】

制御部１５は、第２のプログラムが起動中に、所定のタイミングで認証デバイス２との間において再認証を要求し、テーブルＴを参照して、認証デバイス２の識別情報に対応付けられているカウンタ値が所定の値よりも大きいことを条件に、認証デバイス２との間で認証処理を行い、当該認証処理が成功した場合に、当該第２のプログラムの実行を継続する構成でも良い。

【００３８】

所定のタイミングとしては、定期的な時刻（例えば、１０分、２０分等）、特定のアプリケーションが起動するタイミング等が考えられる。なお、定期的な時刻は、ユーザが自由に設定可能である。

【００３９】

また、制御部１５は、情報処理装置１が配置されている場所によって、再認証の要求を変更しても良い。例えば、制御部１５は、情報処理装置１が社内にあると判断した場合には、再認証の要求を行わず、一方、情報処理装置１が社外にあると判断した場合には、所定のタイミングで再認証の要求を行う。

【００４０】

また、制御部１５は、ネットワークがオンラインの状態であるか、又はオフラインの状態であるかによって、情報処理装置１が社内にあるのか社外にあるのかを判断する構成で

も良い。なお、本構成は一例であって、これに限られず、制御部１５は、内蔵されているＧＰＳの機能を利用して、情報処理装置１が社内にあるのか社外にあるのかを判断する構成でも良い。

【００４１】

このように構成されることにより、情報処理装置１は、所定のタイミングで再認証を要求することによって、セキュリティを向上することができ、かつ、カウンタ値が所定の値よりも大きく、再認証が成功した場合に、第２のプログラムの実行が継続されるので、認証が終了したタイミングで認証デバイス２を装着部１１から取り外すように、ユーザに動機付けを行うことができる。したがって、情報処理装置１は、例えば、認証デバイス２が装着され続けたまま放置されて、他のユーザに持ち去られるような事態を回避することができ、セキュリティリスクを最小限に抑えることができる。

【００４２】

制御部１５は、再認証を要求したときに、装着部１１に認証デバイス２が装着されなかった場合、テーブルＴを参照し、認証デバイス２の識別情報に対応付けられているカウンタ値が所定の値以下の場合、又は装着部１１に装着されている認証デバイス２との間で行った再認証処理が失敗した場合には、第２のプログラムの実行を制限又は停止するように制御する構成でも良い。

【００４３】

第２のプログラムの実行を制限又は停止するとは、例えば、表示部１６に表示されている画面をロックしたり、電源を強制的にシャットダウンすること意味する。なお、制御部１５は、いきなり第２のプログラムの実行を制限又は停止せずに、「あと・・・秒（分）後に使用を制限します」等のメッセージを表示部１６に表示した後に、第２のプログラムの実行を制限又は停止しても良い。

【００４４】

また、制御部１５は、画面のロック中に、認証デバイス２が装着部１１に装着されて、認証デバイス２の識別情報に対応付けられているカウンタ値が所定の値よりも大きく、かつ認証処理に成功した場合には、画面のロックを解除する構成でも良い。

【００４５】

また、制御部１５は、第２のプログラムの起動中に認証デバイス２が装着部１１に装着され続けていた場合、認証デバイス２の固有の識別情報に対応するテーブルＴのカウント値を減算するので、認証デバイス２が装着され続けていると、カウント値が所定の値以下になり、第２のプログラムの実行が制限又は停止することになる。

【００４６】

このように構成されることにより、情報処理装置１は、少なくとも、再認証の要求時に、カウンタ値が所定の値以下の場合には第２のプログラムの実行が制限又は停止してしまうので、認証が終了したタイミングで認証デバイス２を装着部１１から取り外すように、ユーザに動機付けを行うことができる。したがって、情報処理装置１は、例えば、認証デバイス２が装着され続けたまま放置されて、他のユーザに持ち去られるような事態を回避することができ、セキュリティリスクを最小限に抑えることができる。

【００４７】

制御部１５は、第２のプログラムが起動中に、認証デバイス２が装着部１１に装着されていないことを条件に、認証デバイス２の固有の識別情報に対応するテーブルＴのカウント値を加算する構成でも良い。

【００４８】

例えば、制御部１５は、認証デバイス２が装着部１１に装着されていない時間に基づいて、一定の割合でカウント値を加算してゆく。ただし、制御部１５は、テーブルＴに規定されている上限値を超えない範囲で加算を行う。

【００４９】

このように構成されることにより、情報処理装置１は、カウント値が残りわずかであっても、認証デバイス２を装着部１１から取り外しておくことにより、カウント値が回復す

るので、認証が終わったタイミングで認証デバイス２を装着部１１から取り外すように、ユーザに動機付けを行うことができる。また、情報処理装置１は、例えば、認証デバイス２が装着され続けたまま放置されて、他のユーザに持ち去られるような事態を回避することができ、セキュリティリスクを最小限に抑えることができる。

【００５０】

制御部１５は、第２のプログラムが起動中に、実行されているアプリケーションプログラムが所定のアプリケーションプログラムであると判断した場合には、認証デバイス２が装着部１１に装着され続けていても、認証デバイス２の固有の識別情報に対応するテーブルＴのカウント値を減算しないように制御する構成でも良い。

【００５１】

所定のアプリケーションプログラムとは、予め登録されているアプリケーションプログラムであり、例えば、ドングルと呼ばれる不正コピーを防止するために使われるハードウェアキーを所定のポートに接続しないと起動することができないアプリケーションプログラムや、認証デバイス２が装着部１１に装着されていないと使用することができないアプリケーションプログラム等である。

【００５２】

このように構成されることにより、情報処理装置１は、一定条件下においてのみ、認証デバイス２が装着部１１に装着され続けることを許容し、それ以外のときには、認証デバイス２が装着部１１に装着され続けていると、カウント値が減算されてゆく。よって、情報処理装置１は、一定条件下においては、例外処理が行われるので、ユーザの操作性を損なうことがないメリットがある。また、情報処理装置１は、一定条件下以外の場合には、認証デバイス２を装着部１１から取り外すように、ユーザに動機付けを行うことができるので、セキュリティリスクを最小限に抑えることができる。

【００５３】

制御部１５は、所定のタイミングで所定のアプリケーションプログラムの継続使用の有無を問い合わせる確認メッセージを表示部１６に表示するように制御する構成でも良い。

【００５４】

所定のタイミングとしては、定期的な時刻（例えば、１０分、２０分等）等が考えられる。なお、定期的な時刻は、ユーザが自由に設定可能である。

【００５５】

このように構成されることにより、情報処理装置１は、ユーザが所定のアプリケーションプログラムを起動状態のまま、他のアプリケーションプログラムを使用している場合等に、注意喚起を行うことができる。

【００５６】

つぎに、制御部１５の具体的な機能について説明する。

図３は、第１のプログラム起動中の制御部１５の具体的な構成と、第２のプログラム起動中の制御部１５の具体的な構成を示す機能ブロック図である。以下では、第１のプログラム起動中の構成を第１のプログラムサイド１００といい、第２のプログラム起動中の構成を第２のプログラムサイド２００という。なお、以下では、情報処理装置１は、電源が投入されて、第１の記憶部１２から第１のプログラムが読み出され、起動状態にあるものとする。

【００５７】

制御部１５は、図３に示すように、第１のプログラムサイド１００において、認証部１０１と、カウンタ参照部１０２と、第２のプログラム起動制御部（以下、起動制御部という。）１０３を備える。

【００５８】

認証部１０１は、第１のプログラムにしたがって、装着部１１に認証デバイス２が装着されているかどうかの確認を行い、装着されている認証デバイス２の識別情報を読み出す。認証部１０１は、当該識別情報に対応するカウンタ値をテーブルＴから読み出すようにカウンタ参照部１０２に命令を行う。

【００５９】
カウンタ参照部１０２は、命令にしたがって、テーブルＴから識別情報に対応するカウンタ値を読み出して、認証部１０１に送る。
認証部１０１は、認証デバイス２の識別情報に対応付けられているカウンタ値が所定の値よりも大きいかどうかの判断を行う。認証部１０１は、カウンタ値が所定の値によりも大きいと判断した場合には、認証デバイス２との間で認証処理を行う。認証部１０１は、認証処理が成功した場合に、起動制御部１０３にその旨を伝える。
【００６０】
起動制御部１０３は、認証部１０１による認証処理が成功したことを契機として、第２の記憶部１３から第２のプログラムを読み出して起動する。
【００６１】
また、制御部１５は、図３に示すように、第２のプログラムサイド２００において、タイマ部２０１と、認証部２０２と、カウンタ参照部２０３と、操作制限制御部２０４と、監視部２０５と、カウンタ更新部２０６と、アプリケーション監視部２０７と、メッセージ表示制御部２０８を備える。
【００６２】
タイマ部２０１は、システムクロックを利用して、第２のプログラムが起動してからの時間を計る。タイマ部２０１は、第２のプログラムが起動してから設定されている時間（例えば、１０分等）が経過したと判断したときに、認証部２０２とカウンタ参照部２０３に対してタイミング信号を送信する。
【００６３】
認証部２０２は、タイマ部２０１から送信されてきたタイミング信号に応じて、認証デバイス２との間において再認証を要求する。認証部２０２は、認証処理が成功しなかった場合には、認証が失敗したことを示す信号を操作制限制御部２０４に送信する。
【００６４】
カウンタ参照部２０３は、タイマ部２０１から送信されてきたタイミング信号に応じて、テーブルＴを参照して、認証デバイス２の識別情報に対応付けられているカウンタ値が所定の値よりも大きいかどうかを判断する。カウンタ参照部２０３は、カウンタ値が所定の値以下であると判断した場合には、カウンタ値が所定の値以下であることを示す信号を操作制限制御部２０４に送信する。
【００６５】
操作制限制御部２０４は、認証が失敗したことを示す信号、又はカウンタ値が所定の値以下であることを示す信号を受信した場合には、第２のプログラムの実行を制限又は停止する。具体的には、操作制限制御部２０４は、表示部１６に表示されている画面をロックしたり、電源を強制的にシャットダウンする。
【００６６】
監視部２０５は、認証デバイス２の装着部１１に対する装着状態を監視する。具体的には、監視部２０５は、認証処理が完了してから、所定時間（例えば、１分）以上経過後も、認証デバイス２が装着部１１に装着され続けていた場合には、装着時間に基づいて、カウンタ減算信号をカウンタ更新部２０６に送信する。一方、監視部２０５は、装着部１１から認証デバイス２が取り外されている場合には、非装着時間に基づいて、カウンタ加算信号をカウンタ更新部２０６に送信する。
【００６７】
カウンタ更新部２０６は、カウンタ減算信号に基づいて、認証デバイス２の固有の識別情報に対応するテーブルＴのカウント値を減算する。例えば、監視部２０５は、装着時間が１分経過する度にカウンタ減算信号をカウンタ更新部２０６に送信する。カウンタ更新部２０６は、カウンタ減算信号を受信したタイミングで、テーブルＴのカウンタ値を１カウント減算する。したがって、情報処理装置１は、装着部１１に認証デバイス２が６０分間装着され続けると、テーブルＴのカウンタ値が６０カウント減算することになる。
【００６８】

また、カウンタ更新部２０６は、カウンタ加算信号に基づいて、認証デバイス２の固有の識別情報に対応するテーブルＴのカウント値を加算する。例えば、監視部２０５は、非装着時間が１分経過する度にカウンタ加算信号をカウンタ更新部２０６に送信する。カウンタ更新部２０６は、カウンタ加算信号を受信したタイミングで、テーブルＴのカウンタ値を１カウント加算する。したがって、情報処理装置１は、６０分間、装着部１１に認証デバイス２が装着されていない場合、テーブルＴのカウンタ値が６０カウント加算することになる。なお、カウント値は、テーブルＴに規定されている上限値を超えない範囲で加算される。

【００６９】

アプリケーション監視部２０７は、事前登録された所定のアプリケーションプログラムの起動状態を監視し、起動されている場合には、認証デバイス２が装着部１１に装着され続けていても、テーブルＴのカウント値を減算しないようにカウンタ更新部２０６を制御する。

【００７０】

メッセージ表示制御部２０８は、アプリケーション監視部２０７によりカウンタ更新部２０６のカウンタ更新を制御している場合には、定期的に所定のアプリケーションプログラムの継続使用の有無を問い合わせる確認メッセージを表示部１６に表示するように制御する。

【００７１】

このように構成されることにより、情報処理装置１は、電源投入時において、有効な認証デバイス２を装着部１１に装着するように、ユーザに動機付けを行うことができ、かつ、認証デバイス２が装着部１１に装着され続けていると、テーブルＴのカウント値が減算されてゆくので、認証が終わったタイミングで認証デバイス２を装着部１１から取り外すように、ユーザに動機付けを行うことができる。したがって、情報処理装置１は、例えば、認証デバイス２が装着され続けたまま放置されて、他のユーザに持ち去られるような事態を回避することができ、セキュリティリスクを最小限に抑えることができる。

【００７２】

つぎに、情報処理装置１の動作の流れについて、図４に示すフローチャートを参照して説明する。

ステップＳＴ１において、制御部１５は、情報処理装置１の電源が投入された際に、第１のプログラムを読み出して起動する。

【００７３】

ステップＳＴ２において、制御部１５（認証部１０１）は、当該第１のプログラムにしたがって、装着部１１に装着されている認証デバイス２の識別情報を読み出し、テーブルＴを参照して、認証デバイス２の識別情報に対応付けられているカウンタ値が所定の値よりも大きいかどうかを判断する。所定の値よりも大きい場合（Ｙｅｓ）には、ステップＳＴ３に進み、所定の値以下の場合（Ｎｏ）には、一連の処理を終了する。なお、所定の値以下の場合には、一連の処理を終了する前に、例えば、認証処理を数回リトライしたり、認証デバイス２の付け替えを要求したりしても良い。

【００７４】

ステップＳＴ３において、制御部１５（認証部１０１）は、判断ステップＳＴ２によりカウンタ値が所定の値よりも大きいと判断した場合、情報処理装置１の装着部１１に装着されている認証デバイス２との間で認証処理を行う。

【００７５】

ステップＳＴ４において、制御部１５（起動制御部１０３）は、認証処理が成功した場合には、第２のプログラムを読み出して起動する。なお、認証処理が失敗した場合には、第２のプログラムを読み出さず、例えば、認証処理を数回リトライしたり、認証デバイス２の付け替えを要求したり、認証処理が失敗した旨を表示し、シャットダウン等の処理を行う。

【００７６】

ステップＳＴ５において、制御部１５（監視部２０５）は、認証デバイス２が装着中かどうかを判断する。認証デバイス２が装着部１１に装着されていると判断した場合（Ｙｅｓ）には、ステップＳＴ６に進み、認証デバイス２が装着部１１から外されていると判断した場合（Ｎｏ）には、一連の処理を終了する。

【００７７】

ステップＳＴ６において、制御部１５（カウンタ更新部２０６）は、第２のプログラムの起動中に認証デバイス２が装着部１１に装着され続けているので、認証デバイス２の固有の識別情報に対応するテーブルＴのカウント値を減算する。

【００７８】

ステップＳＴ７において、制御部１５（カウンタ参照部２０３）は、テーブルＴのカウンタ値が所定の値が大きいかどうかを判断する。カウンタ値が所定の値よりも大きいと判断した場合（Ｙｅｓ）には、ステップＳＴ５に戻る。また、カウンタ値が所定の値以下であると判断した場合（Ｎｏ）には、一連の処理を終了する。この場合には、制御部１５（カウンタ参照部２０３）は、カウンタ値が所定の値以下であることを示す信号を操作制限制御部２０４に送信する。操作制限制御部２０４は、第２のプログラムの実行を制限又は停止する。具体的には、操作制限制御部２０４は、表示部１６に表示されている画面をロックしたり、電源を強制的にシャットダウンする。

【００７９】

このように構成されることにより、情報処理装置１は、電源投入時において、有効な認証デバイス２を装着部１１に装着するように、ユーザに動機付けを行うことができ、かつ、認証デバイス２が装着部１１に装着され続けていると、テーブルＴのカウント値が減算されてゆくので、認証が終わったタイミングで認証デバイス２を装着部１１から取り外すように、ユーザに動機付けを行うことができる。したがって、情報処理装置１は、例えば、認証デバイス２が装着され続けたまま放置されて、他のユーザに持ち去られるような事態を回避することができ、セキュリティリスクを最小限に抑えることができる。

【００８０】

また、図２に示したテーブルＴの構成は、一例であって、これに限られない。図５は、テーブルＴの他の構成を模式的に示す図である。

テーブルＴは、図５に示すように、アプリケーションプログラムごとに対応するカウンタ値を複数有する構成でも良い。図５に示す例では、識別情報（ＩＢＭ＿１２３４５）の認証デバイス２に対して、第１のアプリケーションプログラム（例えば、作図用のアプリケーションプログラム）に関して、カウンタ値１とその上限値が規定されており、第２のアプリケーションプログラム（例えば、外部のＤＢにアクセスするためのアプリケーションプログラム）に関して、カウンタ値２とその上限値が規定されており、第３のアプリケーションプログラム（例えば、その他のアプリケーションプログラム）に関して、カウンタ値３とその上限値が規定されている。

このような構成によれば、情報処理装置１は、アプリケーションプログラムごとに認証デバイス２の連続した装着時間を異ならせて管理することができる。

また、テーブルＴには、複数台の認証デバイス２を登録することができる。よって、情報処理装置１は、認証デバイス２ごとに利用者を管理することもできる。

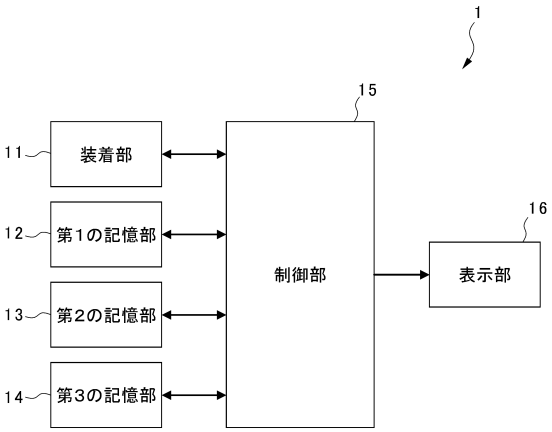
【符号の説明】

【００８１】

１　情報処理装置
２　認証デバイス
１１　装着部
１２　第１の記憶部
１３　第２の記憶部
１４　第３の記憶部
１５　制御部
１６　表示部

１００　第１のプログラムサイド
１０１、２０２　認証部
１０２、２０３　カウンタ参照部
１０３　起動制御部
２００　第２のプログラムサイド
２０１　タイマ部
２０４　操作制限制御部
２０５　監視部
２０６　カウンタ更新部
２０７　アプリケーション監視部
２０８　メッセージ表示制御部

【図１】

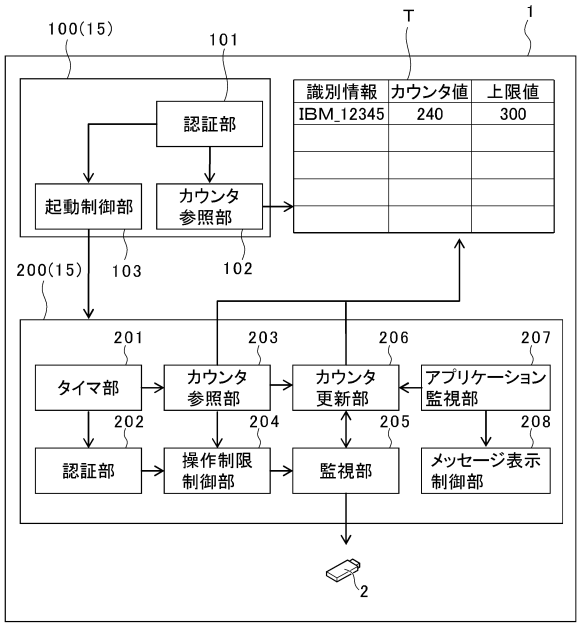


【図２】

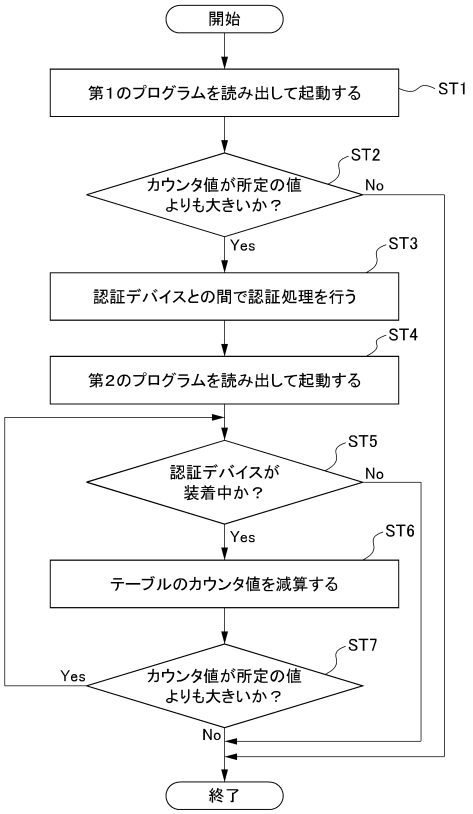
T

識別情報	カウンタ値	上限値
IBM_12345	240	300

【図３】



【図４】



【図５】

T

識別情報	カウンタ値1/上限値	カウンタ値2/上限値	カウンタ値3/上限値
IBM_12345	1000/3000	200/250	240/300

フロントページの続き

(72)発明者　古市　実裕
神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　大和事業所内
(72)発明者　多田　政美
神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　大和事業所内

審査官　岸野　徹

(56)参考文献　特開２０１１－０３４５７７（ＪＰ，Ａ）
特開２００８－１４０１４３（ＪＰ，Ａ）
特開２００６－０４８４４６（ＪＰ，Ａ）
米国特許出願公開第２００３／０１９９２６７（ＵＳ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／３４