(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2023-136601
(P2023-136601A)
(43)公開日　令和5年9月29日(2023.9.29)

(51)Int.Cl.		FI		テーマコード（参考）
G06F 21/12	(2013.01)	G06F 21/12	330	
G06F 21/64	(2013.01)	G06F 21/64		
H04L 9/32	(2006.01)	H04L 9/32	200B	

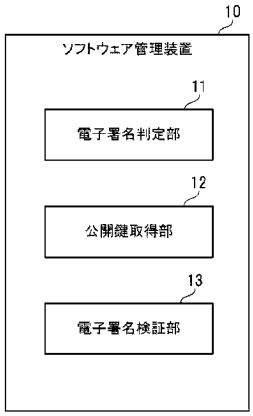
審査請求 未請求　請求項の数 9　ＯＬ　（全 16 頁）

(21)出願番号　特願2022-42365(P2022-42365)
(22)出願日　令和4年3月17日(2022.3.17)

(71)出願人　000232092
ＮＥＣソリューションイノベータ株式会社
東京都江東区新木場一丁目１８番７号
(74)代理人　110002044
弁理士法人ブライタス
(72)発明者　河辺　正仁
東京都江東区新木場一丁目１８番７号　ＮＥＣソリューションイノベータ株式会社内

(54)【発明の名称】ソフトウェア管理装置、ソフトウェア管理方法、及びプログラム

(57)【要約】
【課題】ソフトウェアの使用に用いる鍵の漏洩を抑制して、ソフトウェアの不正使用を阻止する。
【解決手段】ソフトウェア管理装置１０は、コンピュータ上で起動されるソフトウェアに、秘密鍵で署名された電子署名が付与されているかどうかを判定する、電子署名判定部１１と、電子署名が付与されていると判定されると、コンピュータが要件を満たす場合にデータの読み出しが可能となる記憶領域から、秘密鍵に対応する公開鍵を取得する、公開鍵取得部１２と、公開鍵を用いて、ソフトウェアに付与されている電子署名を復号し、電子署名が正当であるかどうかを判定し、電子署名が正当である場合に、ソフトウェアの起動を許可する、電子署名検証部１３と、を備えている。
【選択図】図１



【特許請求の範囲】
【請求項１】
コンピュータ上で起動されるソフトウェアに、秘密鍵で署名された電子署名が付与されているかどうかを判定する、電子署名判定部と、
前記電子署名が付与されていると判定されると、前記コンピュータが要件を満たす場合にデータの読み出しが可能となる記憶領域から、前記秘密鍵に対応する公開鍵を取得する、公開鍵取得部と、
前記公開鍵を用いて、前記ソフトウェアに付与されている前記電子署名を復号し、前記電子署名が正当であるかどうかを判定し、前記電子署名が正当である場合に、前記ソフトウェアの起動を許可する、電子署名検証部と、
を備えている、ことを特徴とするソフトウェア管理装置。
【請求項２】
請求項１に記載のソフトウェア管理装置であって、
前記記憶領域が、前記コンピュータに搭載されたセキュリティチップに設けられており、前記セキュリティチップによって前記コンピュータ上での改ざんが検出されていない場合に、前記記憶領域からのデータの読み出しが可能となる、
ことを特徴とするソフトウェア管理装置。
【請求項３】
請求項１または２に記載のソフトウェア管理装置であって、
前記ソフトウェアには、前記秘密鍵によって暗号化されたハードウェア証明書が組み込まれており、
前記電子署名検証部が、前記公開鍵を用いて、前記ハードウェア証明書を復号し、前記ハードウェア証明書が有効であるかどうかを判定し、
前記ハードウェア証明書が有効である場合に、更に、前記ハードウェア証明書に含まれる情報と前記コンピュータのデバイス情報とが整合しているかどうかを判定し、両者が整合しており、且つ、前記電子署名が正当である場合に、前記ソフトウェアの起動を許可する、
ことを特徴とするソフトウェア管理装置。
【請求項４】
コンピュータ上で起動されるソフトウェアに、秘密鍵で署名された電子署名が付与されているかどうかを判定する、電子署名判定ステップと、
前記電子署名が付与されていると判定されると、前記コンピュータが要件を満たす場合にデータの読み出しが可能となる記憶領域から、前記秘密鍵に対応する公開鍵を取得する、公開鍵取得ステップと、
前記公開鍵を用いて、前記ソフトウェアに付与されている前記電子署名を復号し、前記電子署名が正当であるかどうかを判定し、前記電子署名が正当である場合に、前記ソフトウェアの起動を許可する、電子署名検証ステップと、
を有する、ことを特徴とするソフトウェア管理方法。
【請求項５】
請求項４に記載のソフトウェア管理方法であって、
前記記憶領域が、前記コンピュータに搭載されたセキュリティチップに設けられており、前記セキュリティチップによって前記コンピュータ上での改ざんが検出されていない場合に、前記記憶領域からのデータの読み出しが可能となる、
ことを特徴とするソフトウェア管理方法。
【請求項６】
請求項４または５に記載のソフトウェア管理方法であって、
前記ソフトウェアには、前記秘密鍵によって暗号化されたハードウェア証明書が組み込まれており、
前記電子署名検証ステップにおいて、前記公開鍵を用いて、前記ハードウェア証明書を復号し、前記ハードウェア証明書が有効であるかどうかを判定し、

前記ハードウェア証明書が有効である場合に、更に、前記ハードウェア証明書に含まれる情報と前記コンピュータのデバイス情報とが整合しているかどうかを判定し、両者が整合しており、且つ、前記電子署名が正当である場合に、前記ソフトウェアの起動を許可する、
ことを特徴とするソフトウェア管理方法。
【請求項７】
コンピュータに、
前記コンピュータ上で起動されるソフトウェアに、秘密鍵で署名された電子署名が付与されているかどうかを判定する、電子署名判定ステップと、
前記電子署名が付与されていると判定されると、前記コンピュータが要件を満たす場合にデータの読み出しが可能となる記憶領域から、前記秘密鍵に対応する公開鍵を取得する、公開鍵取得ステップと、
前記公開鍵を用いて、前記ソフトウェアに付与されている前記電子署名を復号し、前記電子署名が正当であるかどうかを判定し、前記電子署名が正当である場合に、前記ソフトウェアの起動を許可する、電子署名検証ステップと、
を実行させる、プログラム。
【請求項８】
請求項７に記載のプログラムであって、
前記記憶領域が、前記コンピュータに搭載されたセキュリティチップに設けられており、前記セキュリティチップによって前記コンピュータ上での改ざんが検出されていない場合に、前記記憶領域からのデータの読み出しが可能となる、
ことを特徴とするプログラム。
【請求項９】
請求項７または８に記載のプログラムであって、
前記ソフトウェアには、前記秘密鍵によって暗号化されたハードウェア証明書が組み込まれており、
前記電子署名検証ステップにおいて、前記公開鍵を用いて、前記ハードウェア証明書を復号し、前記ハードウェア証明書が有効であるかどうかを判定し、
前記ハードウェア証明書が有効である場合に、更に、前記ハードウェア証明書に含まれる情報と前記コンピュータのデバイス情報とが整合しているかどうかを判定し、両者が整合しており、且つ、前記電子署名が正当である場合に、前記ソフトウェアの起動を許可する、
ことを特徴とするプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本開示は、コンピュータに搭載されたソフトウェアを管理するための、ソフトウェア管理装置、及びソフトウェア管理方法に関し、更には、これらを実現するためのプログラムに関する。
【背景技術】
【０００２】
従来から、コンピュータにおいては、正当な権限のない者によるソフトウェアの不正使用を排除することは重要である。このため、例えば、特許文献１は、端末装置のインターフェイスに、ＩＣチップを接続することによって、正当な権限のない者によるソフトウェアの不正使用を阻止する技術を開示している。
【０００３】
具体的には、特許文献１に開示された技術では、ＩＣチップには、データを暗号化するための公開鍵と、データを復号するための開錠鍵とが、記録される。そして、このＩＣチップが端末装置に接続されている間だけ、所定のソフトウェアによるファイルのアクセスが可能となる。この結果、正当な権限のない者によるソフトウェアの不正使用が阻止され

ることになる。
【先行技術文献】
【特許文献】
【０００４】
【特許文献１】特開２００１－１０１０８２号公報
【発明の概要】
【発明が解決しようとする課題】
【０００５】
しかしながら、ＩＣチップに記録されている公開鍵と開錠鍵とを複製することは、悪意のある第三者にとっては簡単であり、特許文献１に開示された技術では、正当な権限のない者によるソフトウェアの不正使用の阻止に限度がある。
【０００６】
本開示の目的の一例は、ソフトウェアの使用に用いる鍵の漏洩を抑制して、ソフトウェアの不正使用を阻止し得る、ソフトウェア管理装置、ソフトウェア管理方法、及び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】
【０００７】
上記目的を達成するため、本開示の一側面におけるソフトウェア管理装置は、
コンピュータ上で起動されるソフトウェアに、秘密鍵で署名された電子署名が付与されているかどうかを判定する、電子署名判定部と、
前記電子署名が付与されていると判定されると、前記コンピュータが要件を満たす場合にデータの読み出しが可能となる記憶領域から、前記秘密鍵に対応する公開鍵を取得する、公開鍵取得部と、
前記公開鍵を用いて、前記ソフトウェアに付与されている前記電子署名を復号し、前記電子署名が正当であるかどうかを判定し、前記電子署名が正当である場合に、前記ソフトウェアの起動を許可する、電子署名検証部と、
を備えている、ことを特徴とする。
【０００８】
また、上記目的を達成するため、本開示の一側面におけるソフトウェア管理方法は、
コンピュータ上で起動されるソフトウェアに、秘密鍵で署名された電子署名が付与されているかどうかを判定する、電子署名判定ステップと、
前記電子署名が付与されていると判定されると、前記コンピュータが要件を満たす場合にデータの読み出しが可能となる記憶領域から、前記秘密鍵に対応する公開鍵を取得する、公開鍵取得ステップと、
前記公開鍵を用いて、前記ソフトウェアに付与されている前記電子署名を復号し、前記電子署名が正当であるかどうかを判定し、前記電子署名が正当である場合に、前記ソフトウェアの起動を許可する、電子署名検証ステップと、
を有する、ことを特徴とする。
【０００９】
更に、上記目的を達成するため、本開示の一側面におけるプログラムは、
コンピュータに、
前記コンピュータ上で起動されるソフトウェアに、秘密鍵で署名された電子署名が付与されているかどうかを判定する、電子署名判定ステップと、
前記電子署名が付与されていると判定されると、前記コンピュータが要件を満たす場合にデータの読み出しが可能となる記憶領域から、前記秘密鍵に対応する公開鍵を取得する、公開鍵取得ステップと、
前記公開鍵を用いて、前記ソフトウェアに付与されている前記電子署名を復号し、前記電子署名が正当であるかどうかを判定し、前記電子署名が正当である場合に、前記ソフトウェアの起動を許可する、電子署名検証ステップと、
を実行させる、ことを特徴とする。

【発明の効果】
【００１０】
以上のように本開示によれば、ソフトウェアの使用に用いる鍵の漏洩を抑制して、ソフトウェアの不正使用を阻止することができる。
【図面の簡単な説明】
【００１１】
【図１】図１は、実施の形態１におけるソフトウェア管理装置の概略構成を示す構成図である。
【図２】図２は、実施の形態１におけるソフトウェア管理装置の構成を具体的に示す構成図である。
【図３】図３は、実施の形態１においてソフトウェア管理装置における処理を説明する図である。
【図４】図４は、実施の形態１におけるソフトウェア管理装置の動作を示すフロー図である。
【図５】図５は、実施の形態２においてソフトウェア管理装置における処理を説明する図である。
【図６】図６は、実施の形態２におけるソフトウェア管理装置の動作を示すフロー図である。
【図７】図７は、実施の形態１及び２におけるソフトウェア管理装置を実現するコンピュータの一例を示すブロック図である。
【発明を実施するための形態】
【００１２】
（実施の形態１）
以下、実施の形態１における、ソフトウェア管理装置、ソフトウェア管理方法、及びプログラムについて、図１～図４を参照しながら説明する。
【００１３】
［装置構成］
最初に、実施の形態１におけるソフトウェア管理装置の概略構成について図１を用いて説明する。図１は、実施の形態１におけるソフトウェア管理装置の概略構成を示す構成図である。
【００１４】
図１に示す実施の形態１におけるソフトウェア管理装置１０は、コンピュータに搭載されたソフトウェアを管理するための装置である。図１に示すように、ソフトウェア管理装置１０は、電子署名判定部１１と、公開鍵取得部１２と、電子署名検証部１３と、を備えている。
【００１５】
電子署名判定部１１は、コンピュータ上で起動されるソフトウェアに、秘密鍵で署名された電子署名が付与されているかどうかを判定する。公開鍵取得部１２は、電子署名判定部１１によって電子署名が付与されていると判定されると、コンピュータが要件を満たす場合にデータの読み出しが可能となる記憶領域から、秘密鍵に対応する公開鍵を取得する。
【００１６】
電子署名検証部１３は、まず、公開鍵取得部１２によって取得された公開鍵を用いて、ソフトウェアに付与されている電子署名を復号する。続いて、電子署名検証部１３は、復号した電子署名が正当であるかどうかを判定し、判定の結果、電子署名が正当である場合に、ソフトウェアの起動を許可する。
【００１７】
このように、ソフトウェア管理装置１０によれば、ソフトウェアは、電子署名が正当でないと起動されず、更に、電子署名は暗号化されており、それを復号するための公開鍵は、セキュリティ性の高い特定の記憶領域に格納されている。このため、ソフトウェア管理

装置１０によれば、ソフトウェアの使用に用いる鍵の漏洩を抑制して、ソフトウェアの不正使用を阻止することができる。

【００１８】

続いて、図２及び図３を用いて、実施の形態１におけるソフトウェア管理装置の構成及び機能について具体的に説明する。図２は、実施の形態１におけるソフトウェア管理装置の構成を具体的に示す構成図である。

【００１９】

図２に示すように、実施の形態１においては、コンピュータ１１０は、オペレーティングシステム（以下「ＯＳ」とも表記する）１００を備えている。ＯＳ１００は、例えば、コンピュータ１１０のオペレータが指示を入力すると、指示に応じて、ソフトウェア２０を起動する。

【００２０】

また、実施の形態１においては、ソフトウェア管理装置１０は、後述するプログラムによって、ＯＳ１００上に構築されている。ソフトウェア管理装置１０は、ＯＳ１００が起動するソフトウェア２０の起動を管理している。ソフトウェア２０は、コンピュータ１１０の記憶装置に格納されており、起動時が指示されると、ＯＳ１００によって、メモリに読み出されて起動される。

【００２１】

実施の形態１では、上述した公開鍵が格納される記憶領域は、コンピュータ１１０に搭載されたセキュリティチップ１０１に設けられている。そして、セキュリティチップ１０１は、コンピュータ１１０上での改ざんが検出されていない場合に、記憶領域からのデータの読み出しを可能にする。

【００２２】

セキュリティチップ１０１の例としては、ＴＰＭ（Trusted Platform Module）が挙げられる。ＴＰＭは、コンピュータ１１０のマザーボードに実装される半導体部品（半導体チップ）であり、セキュリティに関する機能を備えている。セキュリティに関する機能としては、演算、鍵生成、鍵格納、ハッシュ値計算、ハッシュ値格納、乱数生成等が挙げられる。なお、ＴＰＭは、ソフトウェアによって構築されたものであっても良い。

【００２３】

図３は、実施の形態１においてソフトウェア管理装置における処理を説明する図である。図３に示すように、ソフトウェア２０には、予め、例えば、工場出荷時等において、秘密鍵で署名された電子署名が付与されている。

【００２４】

また、図３に示すように、電子署名判定部１１は、コンピュータ１１０のオペレータがソフトウェア２０の起動を指示すると、起動が指示されたソフトウェア２０に、暗号化された電子署名が付与されているかどうかを判定する。

【００２５】

判定の結果、ソフトウェア２０に、暗号化された電子署名が付与されている場合、公開鍵取得部１２は、ＴＰＭであるセキュリティチップ１０１から、暗号化に用いられた秘密鍵に対応する公開鍵を取得する。

【００２６】

電子署名検証部１３は、セキュリティチップ１０１から取得された公開鍵を用いて、ソフトウェア２０に付与されている電子署名を復号し、電子署名が正当であるかどうか判定する。判定の結果、電子署名が正当である場合は、電子署名検証部１３は、ＯＳ１００にソフトウェア２０の起動を許可する。一方、判定の結果、電子署名が正当でない場合は、電子署名検証部１３は、ＯＳ１００にソフトウェア２０の起動を停止させる。

【００２７】

［装置動作］

次に、実施の形態１におけるソフトウェア管理装置１０の動作について図４を用いて説明する。図４は、実施の形態１におけるソフトウェア管理装置の動作を示すフロー図であ

る。以下の説明においては、適宜図１～図３を参照する。また、実施の形態１では、ソフトウェア管理装置１０を動作させることによって、ソフトウェア管理方法が実施される。よって、実施の形態におけるソフトウェア管理方法の説明は、以下のソフトウェア管理装置の動作説明に代える。

【００２８】

図４においては、前提として、高いセキュリティ性が求められるソフトウェア２０には、予め、秘密鍵で署名された電子署名が付与されているとする。また、コンピュータ１１０のオペレータが、いずれかのソフトウェア２０の起動を指示しているとする。

【００２９】

図４に示すように、いずれかのソフトウェア２０の起動が指示されると、電子署名判定部１１は、起動が指示されたソフトウェア２０に、暗号化された電子署名が付与されているかどうかを判定する（ステップＡ１）。

【００３０】

ステップＡ１の判定の結果、ソフトウェア２０に、暗号化された電子署名が付与されていない場合は（ステップＡ１：Ｎｏ）、ソフトウェア管理装置１０における処理は終了する。一方、ステップＡ１の判定の結果、ソフトウェア２０に、暗号化された電子署名が付与されている場合は（ステップＡ１：Ｙｅｓ）、公開鍵取得部１２は、ＴＰＭであるセキュリティチップ１０１から、暗号化に用いられた秘密鍵に対応する公開鍵を取得する（ステップＡ２）。

【００３１】

次に、ステップＡ２が実行されると、電子署名検証部１３は、ステップＡ２で取得された公開鍵を用いて、ソフトウェア２０に付与されている電子署名を復号する（ステップＡ３）。

【００３２】

次に、電子署名検証部１３は、電子署名が正当であるかどうか判定する（ステップＡ４）。具体的には、電子署名検証部１３は、公開鍵によって電子署名を復号できた場合は、電子署名が正当であると判定し、公開鍵によって電子署名を復号できなかった場合は、電子署名が正当でないと判定する。

【００３３】

ステップＡ４の判定の結果、電子署名が正当である場合は（ステップＡ４：Ｙｅｓ）、電子署名検証部１３は、ＯＳ１００にソフトウェア２０の起動を許可する（ステップＡ５）。

【００３４】

一方、ステップＡ４の判定の結果、電子署名が正当でない場合は（ステップＡ４：Ｎｏ）、電子署名検証部１３は、ＯＳ１００にソフトウェア２０の起動停止を指示する（ステップＡ６）。

【００３５】

［実施の形態１における効果］

以上のように、実施の形態１では、ソフトウェア２０は電子署名が正当でない限り起動されることはない。更に、ソフトウェア２０の電子署名を復号するための公開鍵は、対タンパ性の高いＴＰＭといったセキュリティチップ１０１に格納されている。このため、実施の形態１によれば、ソフトウェア２０の使用に用いる鍵の漏洩を抑制して、ソフトウェア２０の不正使用を阻止することができる。

【００３６】

［プログラム］

実施の形態１におけるプログラムは、コンピュータに、図４に示すステップＡ１～Ａ６を実行させるプログラムであれば良い。このプログラムをコンピュータにインストールし、実行することによって、実施の形態１におけるソフトウェア管理装置１０とソフトウェア管理方法とを実現することができる。この場合、コンピュータのプロセッサは、電子署名判定部１１、公開鍵取得部１２、及び電子署名検証部１３として機能し、処理を行なう

。

【００３７】

また、実施の形態１におけるプログラムを実行するコンピュータは、図２に示したように、ソフトウェア２０を実行するコンピュータであっても良いし、これとは別のコンピュータであっても良い。コンピュータとしては、汎用のＰＣの他に、スマートフォン、タブレット型端末装置が挙げられる。

【００３８】

また、実施の形態１におけるプログラムは、複数のコンピュータによって構築されたコンピュータシステムによって実行されても良い。この場合は、例えば、各コンピュータが、それぞれ、電子署名判定部１１、公開鍵取得部１２、及び電子署名検証部１３のいずれかとして機能しても良い。

【００３９】

（実施の形態２）

次に、実施の形態２における、ソフトウェア管理装置、ソフトウェア管理方法、及びプログラムについて、図５及び図６を参照しながら説明する。

【００４０】

［装置構成］

最初に、実施の形態２におけるソフトウェア管理装置の構成について、上述した図１及び図２を参照しながら説明する。まず、実施の形態２におけるソフトウェア管理装置は、図１及び図２に示した実施の形態１におけるソフトウェア管理装置と同様の構成を有している。このため、以下の説明では、図１及び図２を参照する。

【００４１】

但し、実施の形態２においては、実施の形態１と異なり、ソフトウェア２０には、秘密鍵によって暗号化されたハードウェア証明書が組み込まれている。また、このため、電子署名検証部１３における処理も、実施の形態１と異なっている。以下、実施の形態２と実施の形態１との相違点を中心に説明する。

【００４２】

図５は、実施の形態２においてソフトウェア管理装置における処理を説明する図である。図５に示すように、ソフトウェア２０には、予め、例えば、工場出荷時等において、秘密鍵で署名された電子署名が付与されている。また、実施の形態２においては、ソフトウェア２０には、ハードウェア証明書が組み込まれている。

【００４３】

ハードウェア証明書は、それが組み込まれたソフトウェア２０を起動するハードウェアのデバイス情報を含む情報である。デバイス情報としては、ソフトウェアを起動できるコンピュータの識別情報、プロセッサ名、メモリ容量等が挙げられる。

【００４４】

また、ハードウェア証明書も、電子署名と同様に、秘密鍵によって暗号化されている。ハードウェア証明書の暗号化に用いる秘密鍵は、電子署名の暗号化に用いる秘密鍵と同一であっても良いし、異なる鍵であっても良い。

【００４５】

図５に示すように、電子署名判定部１１は、実施の形態２においても、実施の形態１と同様に、コンピュータ１１０のオペレータがソフトウェア２０の起動を指示すると、起動が指示されたソフトウェア２０に、暗号化された電子署名が付与されているかどうかを判定する。

【００４６】

判定の結果、ソフトウェア２０に、暗号化された電子署名が付与されている場合、公開鍵取得部１２は、実施の形態２においても、実施の形態１と同様に、ＴＰＭであるセキュリティチップ１０１から、暗号化に用いられた秘密鍵に対応する公開鍵を取得する。

【００４７】

電子署名検証部１３は、まず、実施の形態１と同様に、セキュリティチップ１０１から

取得された公開鍵を用いて、ソフトウェア２０に付与されている電子署名を復号し、電子署名が正当であるかどうか判定する。

【００４８】

続いて、実施の形態２では、電子署名検証部１３は、セキュリティチップ１０１から取得された公開鍵を用いて、更に、ハードウェア証明書を復号し、ハードウェア証明書が有効であるかどうかを判定する。

【００４９】

また、電子署名検証部１３は、ハードウェア証明書が有効である場合は、ハードウェア証明書に含まれる情報とコンピュータ１１０のデバイス情報とが整合しているかどうかを判定する。なお、コンピュータ１１０のデバイス情報は、電子署名検証部１３によって予め保持されていても良いし、電子署名検証部１３によってＯＳ１００から取得されても良い。

【００５０】

そして、上述の判定の結果、電子署名が正当であり、ハードウェア証明書が有効であり、更に、ハードウェア証明書に含まれる情報とコンピュータ１１０のデバイス情報とが整合している場合は、電子署名検証部１３は、ＯＳ１００にソフトウェア２０の起動を許可する。一方、電子署名が正当でない場合、ハードウェア証明書が有効でない場合、及びハードウェア証明書に含まれる情報とコンピュータ１１０のデバイス情報とが整合していない場合のうち、少なくとも１つに該当する場合は、電子署名検証部１３は、ＯＳ１００にソフトウェア２０の起動を停止させる。

【００５１】

［装置動作］

次に、実施の形態２におけるソフトウェア管理装置の動作について図６を用いて説明する。図６は、実施の形態２におけるソフトウェア管理装置の動作を示すフロー図である。以下の説明においては、適宜図１、２、及び５を参照する。また、実施の形態２では、ソフトウェア管理装置を動作させることによって、ソフトウェア管理方法が実施される。よって、実施の形態におけるソフトウェア管理方法の説明は、以下のソフトウェア管理装置の動作説明に代える。

【００５２】

図６においては、前提として、高いセキュリティ性が求められるソフトウェア２０には、予め、秘密鍵で署名された電子署名が付与され、更に、秘密鍵によって暗号化されたハードウェア証明書が組み込まれているとする。また、コンピュータ１１０のオペレータが、いずれかのソフトウェア２０の起動を指示しているとする。

【００５３】

図６に示すように、いずれかのソフトウェア２０の起動が指示されると、電子署名判定部１１は、起動が指示されたソフトウェア２０に、暗号化された電子署名が付与されているかどうかを判定する（ステップＢ１）。

【００５４】

ステップＢ１の判定の結果、ソフトウェア２０に、暗号化された電子署名が付与されていない場合は（ステップＢ１：Ｎｏ）、ソフトウェア管理装置１０における処理は終了する。一方、ステップＢ１の判定の結果、ソフトウェア２０に、暗号化された電子署名が付与されている場合は（ステップＡ１：Ｙｅｓ）、公開鍵取得部１２は、ＴＰＭであるセキュリティチップ１０１から、暗号化に用いられた秘密鍵に対応する公開鍵を取得する（ステップＢ２）。

【００５５】

次に、ステップＡ２が実行されると、電子署名検証部１３は、ステップＢ２で取得された公開鍵を用いて、ソフトウェア２０に付与されている電子署名を復号する（ステップＡ３）。

【００５６】

次に、電子署名検証部１３は、電子署名が正当であるかどうか判定する（ステップＢ４

）。具体的には、電子署名検証部１３は、公開鍵によって電子署名を復号できた場合は、電子署名が正当であると判定し、公開鍵によって電子署名を復号できなかった場合は、電子署名が正当でないと判定する。

【００５７】

一方、ステップＢ４の判定の結果、電子署名が正当でない場合は（ステップＢ４：Ｎｏ）、電子署名検証部１３は、ＯＳ１００にソフトウェア２０の起動停止を指示する（ステップＢ９）。

【００５８】

ステップＢ４の判定の結果、電子署名が正当である場合は（ステップＢ４：Ｙｅｓ）、電子署名検証部１３は、ステップＢ２で取得された公開鍵を用いて、ハードウェア証明書を復号する（ステップＢ５）。

【００５９】

次に、電子署名検証部１３は、ハードウェア証明書が有効であるかどうかを判定する（ステップＢ６）。具体的には、電子署名検証部１３は、例えば、ハードウェア証明書の有効期限が切れていない場合は、ハードウェア証明書が有効であると判定し、ハードウェア証明書の有効期限が切れている場合は、ハードウェア証明書が有効でないと判定する。

【００６０】

ステップＢ６の判定の結果、ハードウェア証明書が有効でない場合（ステップＢ６：Ｎｏ）は、電子署名検証部１３は、ＯＳ１００にソフトウェア２０の起動停止を指示する（ステップＢ９）。

【００６１】

一方、ステップＢ６の判定の結果、ハードウェア証明書が有効である場合（ステップＢ６：Ｙｅｓ）は、電子署名検証部１３は、ハードウェア証明書に含まれる情報とコンピュータ１１０のデバイス情報とが整合しているかどうかを判定する（ステップＢ７）。

【００６２】

ステップＢ７の判定の結果、ハードウェア証明書に含まれる情報とコンピュータ１１０のデバイス情報とが整合している場合は（ステップＢ７：Ｙｅｓ）、電子署名検証部１３は、ＯＳ１００にソフトウェア２０の起動を許可する（ステップＢ８）。

【００６３】

一方、ステップＢ７の判定の結果、ハードウェア証明書に含まれる情報とコンピュータ１１０のデバイス情報とが整合していない場合は（ステップＢ７：Ｎｏ）、電子署名検証部１３は、ＯＳ１００にソフトウェア２０の起動停止を指示する（ステップＢ９）。

【００６４】

［実施の形態２における効果］

以上のように、実施の形態２では、ソフトウェア２０は、電子署名が正当であり、ハードウェア証明書が有効であり、更に、有効なハードウェア証明書とデバイス情報とが整合する場合にのみ、起動する。更に、ソフトウェア２０の電子署名とハードウェア証明書とを復号するための公開鍵は、対タンパ性の高いＴＰＭといったセキュリティチップ１０１に格納されている。このため、実施の形態２においても、実施の形態１と同様に、ソフトウェア２０の使用に用いる鍵の漏洩を抑制して、ソフトウェア２０の不正使用を阻止することができる。

【００６５】

［プログラム］

実施の形態２におけるプログラムは、コンピュータに、図６に示すステップＢ１～Ｂ９を実行させるプログラムであれば良い。このプログラムをコンピュータにインストールし、実行することによって、実施の形態２におけるソフトウェア管理装置とソフトウェア管理方法とを実現することができる。この場合、コンピュータのプロセッサは、電子署名判定部１１、公開鍵取得部１２、及び電子署名検証部１３として機能し、処理を行なう。

【００６６】

また、実施の形態２におけるプログラムを実行するコンピュータは、図２に示したよう

に、ソフトウェア２０を実行するコンピュータであっても良いし、これとは別のコンピュータであっても良い。コンピュータとしては、汎用のＰＣの他に、スマートフォン、タブレット型端末装置が挙げられる。

【００６７】

また、実施の形態２におけるプログラムは、複数のコンピュータによって構築されたコンピュータシステムによって実行されても良い。この場合は、例えば、各コンピュータが、それぞれ、電子署名判定部１１、公開鍵取得部１２、及び電子署名検証部１３のいずれかとして機能しても良い。

【００６８】

［物理構成］

ここで、実施の形態１及び２におけるプログラムを実行することによって、ソフトウェア管理装置を実現するコンピュータについて図７を用いて説明する。図７は、実施の形態１及び２におけるソフトウェア管理装置を実現するコンピュータの一例を示すブロック図である。

【００６９】

図７に示すように、コンピュータ１１０は、ＣＰＵ（Central Processing Unit）１１１と、メインメモリ１１２と、記憶装置１１３と、入力インターフェイス１１４と、表示コントローラ１１５と、データリーダ／ライタ１１６と、通信インターフェイス１１７と、セキュリティチップ１０１と、を備える。これらの各部は、バス１２１を介して、互いにデータ通信可能に接続される。

【００７０】

図７の例では、セキュリティチップ１０１は、バス１２１に接続されているが、これは一例である。セキュリティチップ１０１は、例えば、バス１２１とは別のバスによってＣＰＵ１１１に接続されていても良いし、ＣＰＵ１１１の内部に構築されていても良い。

【００７１】

また、コンピュータ１１０は、ＣＰＵ１１１に加えて、又はＣＰＵ１１１に代えて、ＧＰＵ（Graphics Processing Unit）、又はＦＰＧＡ（Field-Programmable Gate Array）を備えていても良い。この態様では、ＧＰＵ又はＦＰＧＡが、実施の形態におけるプログラムを実行することができる。

【００７２】

ＣＰＵ１１１は、記憶装置１１３に格納された、コード群で構成された実施の形態におけるプログラムをメインメモリ１１２に展開し、各コードを所定順序で実行することにより、各種の演算を実施する。メインメモリ１１２は、典型的には、ＤＲＡＭ（Dynamic Random Access Memory）等の揮発性の記憶装置である。

【００７３】

また、実施の形態におけるプログラムは、コンピュータ読み取り可能な記録媒体１２０に格納された状態で提供される。なお、本実施の形態におけるプログラムは、通信インターフェイス１１７を介して接続されたインターネット上で流通するものであっても良い。

【００７４】

また、記憶装置１１３の具体例としては、ハードディスクドライブの他、フラッシュメモリ等の半導体記憶装置が挙げられる。入力インターフェイス１１４は、ＣＰＵ１１１と、キーボード及びマウスといった入力機器１１８との間のデータ伝送を仲介する。表示コントローラ１１５は、ディスプレイ装置１１９と接続され、ディスプレイ装置１１９での表示を制御する。

【００７５】

データリーダ／ライタ１１６は、ＣＰＵ１１１と記録媒体１２０との間のデータ伝送を仲介し、記録媒体１２０からのプログラムの読み出し、及びコンピュータ１１０における処理結果の記録媒体１２０への書き込みを実行する。通信インターフェイス１１７は、ＣＰＵ１１１と、他のコンピュータとの間のデータ伝送を仲介する。

【００７６】

また、記録媒体１２０の具体例としては、ＣＦ（Compact Flash（登録商標））及びＳＤ（Secure Digital）等の汎用的な半導体記憶デバイス、フレキシブルディスク（Flexible Disk）等の磁気記録媒体、又はＣＤ－ＲＯＭ（Compact Disk Read Only Memory）などの光学記録媒体が挙げられる。

【００７７】

なお、実施の形態１及び２におけるソフトウェア管理装置は、プログラムがインストールされたコンピュータではなく、各部に対応したハードウェアを用いることによっても実現可能である。更に、ソフトウェア管理装置は、一部がプログラムで実現され、残りの部分がハードウェアで実現されていてもよい。

【００７８】

上述した実施の形態の一部又は全部は、以下に記載する（付記１）～（付記９）によって表現することができるが、以下の記載に限定されるものではない。

【００７９】

（付記１）

コンピュータ上で起動されるソフトウェアに、秘密鍵で署名された電子署名が付与されているかどうかを判定する、電子署名判定部と、

前記電子署名が付与されていると判定されると、前記コンピュータが要件を満たす場合にデータの読み出しが可能となる記憶領域から、前記秘密鍵に対応する公開鍵を取得する、公開鍵取得部と、

前記公開鍵を用いて、前記ソフトウェアに付与されている前記電子署名を復号し、前記電子署名が正当であるかどうかを判定し、前記電子署名が正当である場合に、前記ソフトウェアの起動を許可する、電子署名検証部と、

を備えている、ことを特徴とするソフトウェア管理装置。

【００８０】

（付記２）

付記１に記載のソフトウェア管理装置であって、

前記記憶領域が、前記コンピュータに搭載されたセキュリティチップに設けられており、前記セキュリティチップによって前記コンピュータ上での改ざんが検出されていない場合に、前記記憶領域からのデータの読み出しが可能となる、

ことを特徴とするソフトウェア管理装置。

【００８１】

（付記３）

付記１または２に記載のソフトウェア管理装置であって、

前記ソフトウェアには、前記秘密鍵によって暗号化されたハードウェア証明書が組み込まれており、

前記電子署名検証部が、前記公開鍵を用いて、前記ハードウェア証明書を復号し、前記ハードウェア証明書が有効であるかどうかを判定し、

前記ハードウェア証明書が有効である場合に、更に、前記ハードウェア証明書に含まれる情報と前記コンピュータのデバイス情報とが整合しているかどうかを判定し、両者が整合しており、且つ、前記電子署名が正当である場合に、前記ソフトウェアの起動を許可する、

ことを特徴とするソフトウェア管理装置。

【００８２】

（付記４）

コンピュータ上で起動されるソフトウェアに、秘密鍵で署名された電子署名が付与されているかどうかを判定する、電子署名判定ステップと、

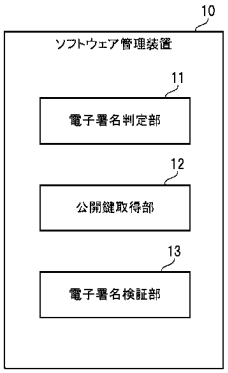
前記電子署名が付与されていると判定されると、前記コンピュータが要件を満たす場合にデータの読み出しが可能となる記憶領域から、前記秘密鍵に対応する公開鍵を取得する、公開鍵取得ステップと、

前記公開鍵を用いて、前記ソフトウェアに付与されている前記電子署名を復号し、前記

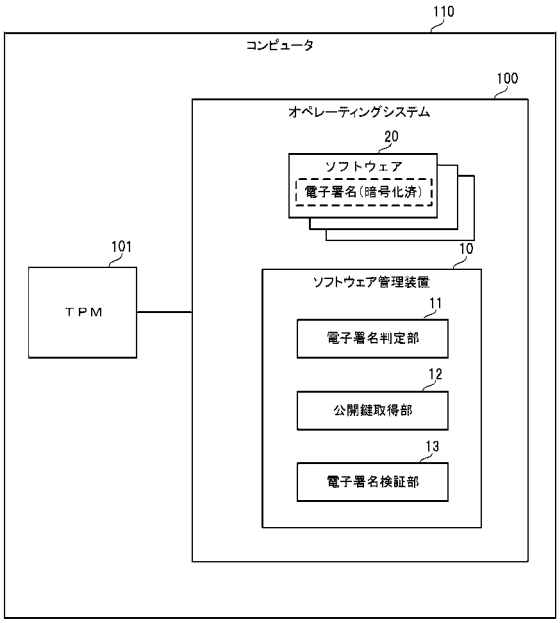
電子署名が正当であるかどうかを判定し、前記電子署名が正当である場合に、前記ソフトウェアの起動を許可する、電子署名検証ステップと、
を有する、ことを特徴とするソフトウェア管理方法。
【００８３】
（付記５）
付記４に記載のソフトウェア管理方法であって、
前記記憶領域が、前記コンピュータに搭載されたセキュリティチップに設けられており、前記セキュリティチップによって前記コンピュータ上での改ざんが検出されていない場合に、前記記憶領域からのデータの読み出しが可能となる、
ことを特徴とするソフトウェア管理方法。
【００８４】
（付記６）
付記４または５に記載のソフトウェア管理方法であって、
前記ソフトウェアには、前記秘密鍵によって暗号化されたハードウェア証明書が組み込まれており、
前記電子署名検証ステップにおいて、前記公開鍵を用いて、前記ハードウェア証明書を復号し、前記ハードウェア証明書が有効であるかどうかを判定し、
前記ハードウェア証明書が有効である場合に、更に、前記ハードウェア証明書に含まれる情報と前記コンピュータのデバイス情報とが整合しているかどうかを判定し、両者が整合しており、且つ、前記電子署名が正当である場合に、前記ソフトウェアの起動を許可する、
ことを特徴とするソフトウェア管理方法。
【００８５】
（付記７）
コンピュータに、
前記コンピュータ上で起動されるソフトウェアに、秘密鍵で署名された電子署名が付与されているかどうかを判定する、電子署名判定ステップと、
前記電子署名が付与されていると判定されると、前記コンピュータが要件を満たす場合にデータの読み出しが可能となる記憶領域から、前記秘密鍵に対応する公開鍵を取得する、公開鍵取得ステップと、
前記公開鍵を用いて、前記ソフトウェアに付与されている前記電子署名を復号し、前記電子署名が正当であるかどうかを判定し、前記電子署名が正当である場合に、前記ソフトウェアの起動を許可する、電子署名検証ステップと、
を実行させる、プログラム。
【００８６】
（付記８）
付記７に記載のプログラムであって、
前記記憶領域が、前記コンピュータに搭載されたセキュリティチップに設けられており、前記セキュリティチップによって前記コンピュータ上での改ざんが検出されていない場合に、前記記憶領域からのデータの読み出しが可能となる、
ことを特徴とするプログラム。
【００８７】
（付記９）
付記７または８に記載のプログラムであって、
前記ソフトウェアには、前記秘密鍵によって暗号化されたハードウェア証明書が組み込まれており、
前記電子署名検証ステップにおいて、前記公開鍵を用いて、前記ハードウェア証明書を復号し、前記ハードウェア証明書が有効であるかどうかを判定し、
前記ハードウェア証明書が有効である場合に、更に、前記ハードウェア証明書に含まれる情報と前記コンピュータのデバイス情報とが整合しているかどうかを判定し、両者が整合

しており、且つ、前記電子署名が正当である場合に、前記ソフトウェアの起動を許可する
、
ことを特徴とするプログラム。
【産業上の利用可能性】
【００８８】
以上のように本開示によれば、ソフトウェアの使用に用いる鍵の漏洩を抑制して、ソフトウェアの不正使用を阻止することができる。本開示は、ソフトウェアの不正使用が求められる種々のシステムに有効である。
【符号の説明】
【００８９】
１０　ソフトウェア管理装置
１１　電子署名判定部
１２　公開鍵取得部
１３　電子署名検証部
２０　ソフトウェア
１００　オペレーティングシステム
１０１　セキュリティチップ
１１０　コンピュータ
１１１　ＣＰＵ
１１２　メインメモリ
１１３　記憶装置
１１４　入力インターフェイス
１１５　表示コントローラ
１１６　データリーダ／ライタ
１１７　通信インターフェイス
１１８　入力機器
１１９　ディスプレイ装置
１２０　記録媒体
１２１　バス

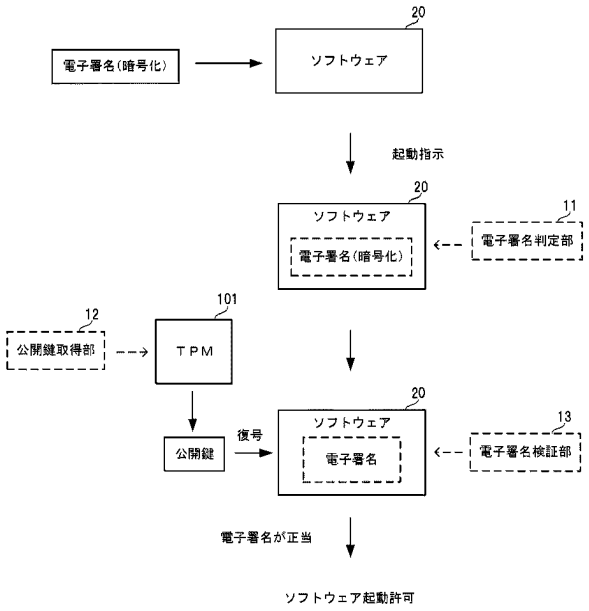
【図１】


10
ソフトウェア管理装置
11
電子署名判定部
12
公開鍵取得部
13
電子署名検証部

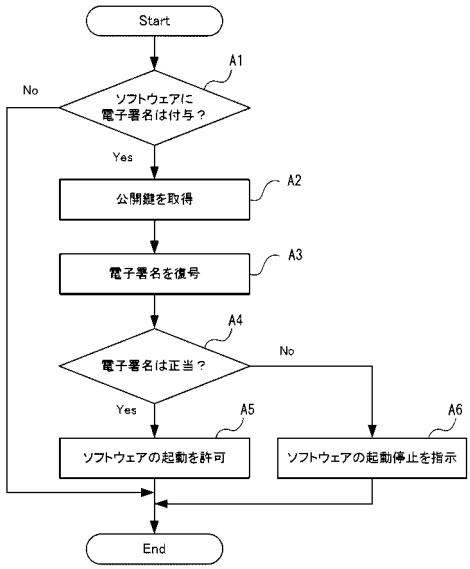
【図２】


110
コンピュータ
100
オペレーティングシステム
20
ソフトウェア
電子署名（暗号化済）
101
ＴＰＭ
10
ソフトウェア管理装置
11
電子署名判定部
12
公開鍵取得部
13
電子署名検証部

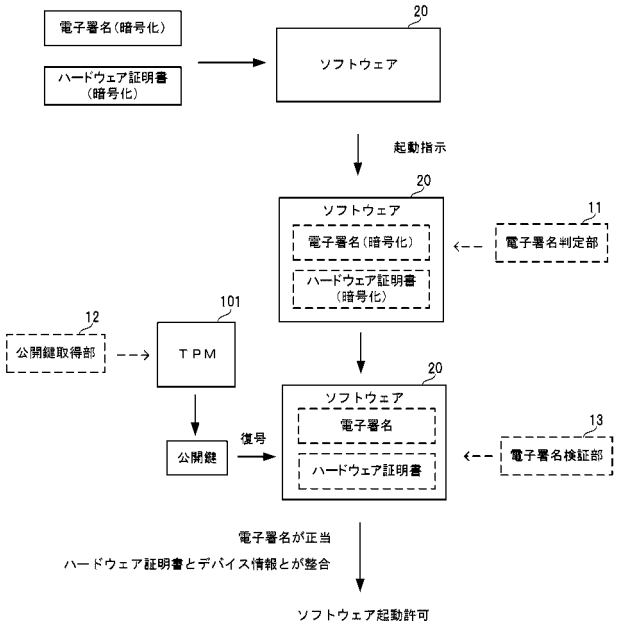
【図３】


電子署名（暗号化）
20
ソフトウェア
起動指示
20
ソフトウェア
電子署名（暗号化）
11
電子署名判定部
12
公開鍵取得部
101
ＴＰＭ
公開鍵
復号
20
ソフトウェア
電子署名
13
電子署名検証部
電子署名が正当
ソフトウェア起動許可

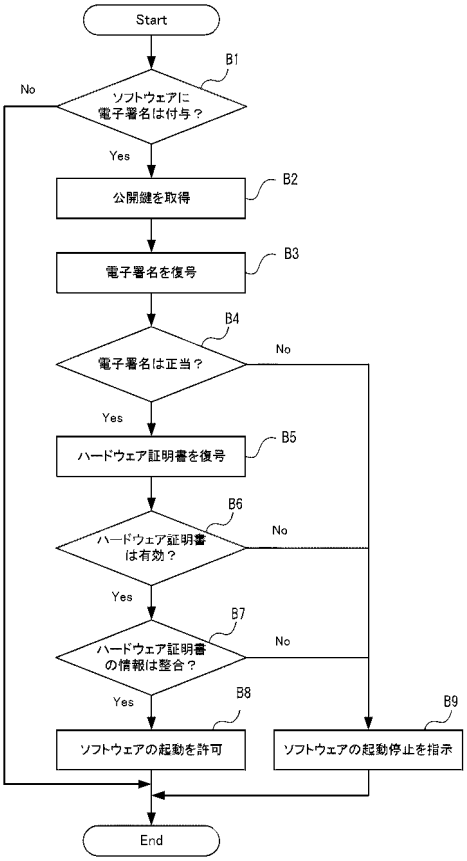
【図４】


Start
A1
ソフトウェアに
電子署名は付与？
No
Yes
A2
公開鍵を取得
A3
電子署名を復号
A4
電子署名は正当？
No
Yes
A5
ソフトウェアの起動を許可
A6
ソフトウェアの起動停止を指示
End

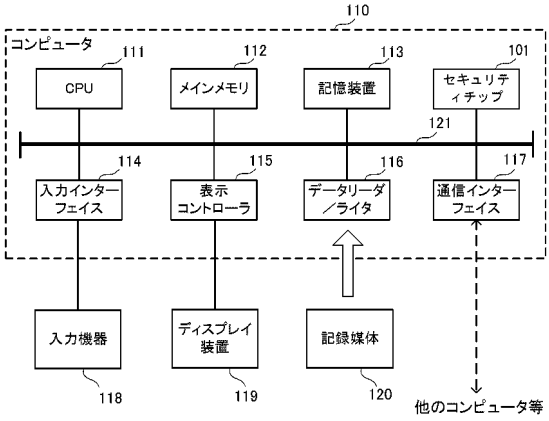
【図５】


電子署名（暗号化）
ハードウェア証明書（暗号化）
20
ソフトウェア
起動指示
20
ソフトウェア
電子署名（暗号化）
ハードウェア証明書（暗号化）
11
電子署名判定部
12
公開鍵取得部
101
ＴＰＭ
20
ソフトウェア
電子署名
ハードウェア証明書
13
電子署名検証部
公開鍵
復号
電子署名が正当
ハードウェア証明書とデバイス情報とが整合
ソフトウェア起動許可

【図６】


Start
B1
ソフトウェアに電子署名は付与？
No
Yes
B2
公開鍵を取得
B3
電子署名を復号
B4
電子署名は正当？
No
Yes
B5
ハードウェア証明書を復号
B6
ハードウェア証明書は有効？
No
Yes
B7
ハードウェア証明書の情報は整合？
No
Yes
B8
ソフトウェアの起動を許可
B9
ソフトウェアの起動停止を指示
End

【図７】


110
コンピュータ
111
CPU
112
メインメモリ
113
記憶装置
101
セキュリティチップ
121
114
入力インターフェイス
115
表示コントローラ
116
データリーダ／ライタ
117
通信インターフェイス
入力機器
118
ディスプレイ装置
119
記録媒体
120
他のコンピュータ等