

(19) 世界知的所有権機関
国際事務局(43) 国際公開日
2007年1月4日 (04.01.2007)

PCT

(10) 国際公開番号
WO 2007/000993 A1

- (51) 国際特許分類:
G06F 21/22 (2006.01)
- (21) 国際出願番号: PCT/JP2006/312797
- (22) 国際出願日: 2006年6月27日 (27.06.2006)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
60/694,258 2005年6月28日 (28.06.2005) US
- (71) 出願人 (米国を除く全ての指定国について): 松下電器産業株式会社 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) [JP/JP]; 〒5718501 大阪府門真市大字門真1006番地 Osaka (JP). ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒1410001 東京都品川区北品川6丁目7番35号 Tokyo (JP).
- (72) 発明者; および
- (75) 発明者/出願人 (米国についてのみ): 小野田 仙一 (ONODA, Senichi). 山本 雅哉 (YAMAMOTO, Masaya). 中野 稔久 (NAKANO, Toshihisa). 村瀬 薫 (MURASE,

Kaoru). 小塚 雅之 (KOZUKA, Masayuki). 山西 隆志 (YAMANISHI, Takashi). 大澤 義知 (OHSAWA, Yoshitomo). 大石 丈於 (OHISHI, Tateo). 米満 潤 (YONEMITSU, Jun). 村松 克美 (MURAMATSU, Katsumi).

- (74) 代理人: 中島 司朗, 外 (NAKAJIMA, Shiro et al.); 〒5310072 大阪府大阪市北区豊崎三丁目2番1号淀川5番館6F Osaka (JP).

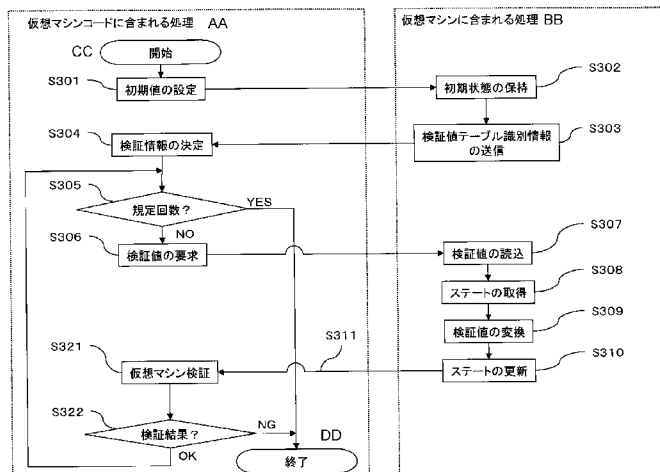
- (81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

- (84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD,

[続葉有]

(54) Title: VERIFICATION METHOD, INFORMATION PROCESSING DEVICE, RECORDING MEDIUM, VERIFICATION SYSTEM, CERTIFICATION PROGRAM, AND VERIFICATION PROGRAM

(54) 発明の名称: 検証方法、情報処理装置、記録媒体、検証システム、証明プログラム及び検証プログラム



AA PROCESSES CONTAINED IN VIRTUAL MACHINE CODE
BB PROCESSED CONTAINED IN VIRTUAL MACHINE
CC START
S301 SET INITIAL VALUE
S302 HOLD INITIAL STATE
S303 SEND VERIFICATION VALUE TABLE IDENTIFIER
S304 DECIDED VERIFICATION INFORMATION
S305 PREDETERMINED NUMBER OF TIMES?
S306 REQUEST FOR VERIFICATION VALUE
S307 READ VERIFICATION VALUE
S308 ACQUIRE STATE
S309 CONVERT VERIFICATION VALUE
S310 UPDATE STATE
S321 VERIFY VIRTUAL MACHINE
S322 VERIFICATION RESULT?
DD END

(57) Abstract: Anyone can mount a virtual machine since information required for mounting such as interface is disclosed. This causes a problem that a virtual machine is mounted in an unauthorized way and a program operating on it is made to execute an unauthorized operation. A program compares the secret information owned by a virtual machine to verification information of the program itself so as to verify whether the virtual machine operating the program has been mounted in an authorized way, thereby excluding an unauthorized virtual machine.

(57) 要約: 仮想マシンは、インタフェース等、実装に必要な情報が公開されているため、誰でも仮想マシンを実装することができる。そのため、仮想マシンを不正に実装することで、その上で稼動するプログラムに正規の動作ではなく、不正な動作をさせることが可能となるという問題がある。本発明は、プログラムが、仮想マシンが持つ秘密情報と、プログラム自身が持つ検証用情報を比較することで、自身を稼動させる仮想マシンが正規に実装されたものであることを検証することで、不正な仮想マシンを排除する。

WO 2007/000993 A1



SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:

— 国際調査報告書

2文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

明 細 書

検証方法、情報処理装置、記録媒体、検証システム、証明プログラム及び検証プログラム

技術分野

[0001] 本発明は、プログラムの実行に仮想マシンを用いる機器に関連し、特に、仮想マシンが実装されるプラットフォームの正当性を判断し、該プラットフォームが不正な場合に、排除する技術に関する。

背景技術

[0002] 近年、プログラムをOSやCPU等のプラットフォームに依存させずに稼動させるため、仮想マシンが利用されている。一般的に、仮想マシンはソフトウェア実装されており、インタフェース等、実装に必要な情報が公開されているため、誰でも仮想マシンを実装することができる。

特許文献1：特開2005－244695号公報

発明の開示

発明が解決しようとする課題

[0003] そのため、仮想マシンを不正に実装することで、その上で稼動するプログラムに正規の動作ではなく、不正な動作をさせることが可能となる。そのプログラムが、例えば、映画等のコンテンツの著作権を保護するプログラムである場合、不正にコンテンツを再生されることにつながる。

本発明は、上記の問題点に鑑み、プログラムが、自身を稼動させる仮想マシンが正規に実装されたものであることを検証できる検証方法、情報処理装置、記録媒体、検証システム、証明プログラム及び検証プログラムを提供することを目的とする。

課題を解決するための手段

[0004] 上記の課題を解決するために、本発明は、内部に含んだ仮想マシンによりコンテンツの再生に係る処理を実行する情報処理装置において用いられる検証方法であって、前記コンテンツと共に記録媒体に記録されている検証プログラムを読み込む読込ステップと、前記検証プログラムを前記仮想マシンが実行することにより、前記仮想マ

シンを含む前記情報処理装置の正当性を検証する検証ステップとを含むことを特徴とする。

発明の効果

[0005] 上記の構成によると、前記仮想マシン上で動作する前記検証プログラムが、自身を実行する前記仮想マシンを含む前記情報処理装置の正当性を検証することができる。

また、前記検証方法は、前記検証ステップにおいて、タイミングによって変動する証明用情報を用いて、前記検証を行うことを特徴とするとしてもよい。

この構成によると、前記検証ステップで用いられる証明用情報は、タイミングによって変動するので、不正な第三者が、前記証明用情報を取得するには、当該検証方法を実装したプログラム等を詳細に解析し、その動作を追いかけていかなければならず、その取得は非常に困難である。従って、証明書や識別番号といった静的なデータにより、正当性を証明する場合に比べ、正当な仮想マシンを偽装しにくいという優れた効果を生じる。

[0006] また、前記検証方法に含まれる前記検証ステップは、前記情報処理装置が保持する秘密情報に基づいた前記証明用情報を要求する要求ステップと、前記証明用情報と、前記記録媒体に記録された検証情報とを比較する比較ステップと、比較結果に基づき、正当であるか否かを判断する判断ステップとを含み、前記検証方法は、さらに、前記要求に応じて、前記仮想マシンにより、前記証明用情報を生成し、生成した前記証明用情報を前記検証プログラムに提供する提供ステップを含むことを特徴とするとしてもよい。

[0007] この構成によると、前記仮想マシンにより生成された前記証明用情報を用いて、正当性の検証を行う。正当な仮想マシンでなければ、正しい証明用情報を生成できないので、確実に、前記情報処理装置の備える仮想マシンの正当性を判断することができる。

また、前記検証方法において、前記判断ステップは、タイミングによって前記証明用情報が増減する毎に、前記比較ステップを繰り返させる繰返しステップと、前記繰返しの結果、所定回数連続して、前記検証情報と前記証明用情報が一致しなけれ

ば、前記情報処理装置は不正であると決定する決定ステップとを含むことを特徴とする構成であつてもよい。

[0008] この構成では、所定回数連続して、前記検証情報と前記証明用情報とが一致した場合に限り、前記仮想マシンを含む情報処理装置が正当であるとする。そのため、何らかの方法で、不正な第三者に、1個の前記検証情報を知られたとしても、前記検証で、正当であると判断されることはない。

また、前記検証方法において、前記提供ステップは、前記秘密情報の読み出し順序に応じて一意的に決定する値により、前記証明用情報が生成される過程において用いられる演算情報を、変更する更新ステップと、生成した前記証明用情報を、前記検証用プログラムへ出力する出力ステップとを含むとしてもよい。

[0009] この構成によると、前記更新ステップにおいて、前記演算情報を更新する。つまり、前記証明用情報の生成に用いられるデータも、前記証明用情報の生成の度に異なるので、正しい証明用情報を予測されにくいという優れた効果を奏する。

また、本発明において、前記記録媒体には、複数の検証候補情報が記録されており、前記情報処理装置は、1以上の秘密情報を保持しており、前記検証ステップは、1の検証候補情報を検証情報として選択する選択ステップと、選択された前記検証情報と対応する秘密情報に基づいて生成された前記証明用情報を要求する要求ステップと、前記検証情報と前記証明用情報とを比較する比較ステップと、比較結果を基に、前記情報処理装置の正当性を判断する判断ステップとを含み、前記検証方法は、さらに、前記要求を受けると、前記仮想マシンにより、前記検証情報と対応する前記秘密情報を用いて前記証明用情報を生成し、生成した前記証明用情報を前記検証用プログラムへ提供する提供ステップとを含むことを特徴とする構成であつてもよい。

[0010] さらに、本発明は、前記判断ステップは、前記比較ステップにより前記検証情報と証明用情報とが一致する場合に、前記選択ステップ、前記要求ステップ及び前記比較ステップを繰り返させる繰り返しステップと、前記繰り返しにより、所定回数連続して前記検証情報と証明用情報とが一致する場合に、前記情報処理装置が正当であると決定し、それ以外の場合に、前記情報処理装置が不正であると決定する決定ステップ

を含むことを特徴とする検証方法でもある。

- [0011] この構成では、繰り返しにおいて、所定回数連続して検証情報と証明用情報とが一致した場合に限り、前記情報処理装置が正当であると、決定するので、より確実に不正な情報処理装置を検出し、不正な情報処理装置によるコンテンツの利用を抑制することができる。

また、本発明は、前記検証ステップの繰り返しにおいて、前記選択ステップでは、繰り返しの回数に応じて異なる検証候補情報を、前記検証情報として選択し、前記提供ステップでは、繰り返しの回数に応じて変動する前記証明用情報を生成することを特徴とする検証方法でもある。

- [0012] この構成によると、前記選択手段は、繰り返しの度に異なる証明用情報を選択するので、不正な第三者に、前記比較に用いられる検証情報を予測されにくいという優れた効果を奏する。

また、前記検証方法は、前記選択ステップでは、ランダムに前記検証情報を選択し、前記比較ステップでは、前記検証情報に対応して、ランダムに変動する前記証明用情報を用いて、前記比較を行うことを特徴とする構成であってもよい。

- [0013] この構成によると、前記選択手段は、証明用情報をランダムに選択するので、不正な第三者に、前記比較に用いられる検証情報を予測されにくいという優れた効果を奏する。

また、本発明の検証方法において、前記複数の検証候補情報のうち少なくとも一つは、前記仮想マシンを一意に識別する識別子と対応しており、前記選択ステップでは、前記識別子と対応する検証候補情報を前記検証情報として選択するとしてもよい。

- [0014] このような、構成にすることで、前記記録媒体に記録されている前記検証プログラムは、それぞれ異なる秘密情報を有する複数の情報処理装置の正当性を検証することができる。

前記記録媒体は、さらに、前記仮想マシン上で実行され、前記コンテンツの再生に係る処理手順を含む再生関連プログラムを記録しており、前記検証方法は、さらに、検証の結果、前記情報処理装置が不正である場合、前記コンテンツの再生に係る処理手順の実行を抑制する抑制ステップを含むことを特徴とする構成であってもよい。

[0015] この構成によると、前記仮想マシンを含む前記情報処理装置が不正であると判定されると、前記抑制ステップにおいて、前記コンテンツの再生に係る処理手順の実行を抑制する。従って、本発明の前記検証方法は、不正に実装された仮想マシンを含む情報処理装置によるコンテンツの再生を抑制することができるという優れた効果を奏する。

図面の簡単な説明

[0016] [図1]記録媒体102及び情報処理装置101の構成を示す図

[図2]仮想マシンコード実行処理のフロー図

[図3]仮想マシンを含む実行環境の正当性検証処理のフロー図

[図4]検証値テーブル116のデータ構造例

[図5]仮想マシンコード121が持つ検証情報のデータ構造例

[図6]仮想マシンコード121が持つ検証情報のデータ構造別例

符号の説明

- [0017] 101 情報処理装置
102 記録媒体
111 ディスク読込部
112 ユーザ操作受付部
113 仮想マシン実行部
114 情報保持部
115 仮想マシン実行コード
116 検証値テーブル
117 検証値テーブル識別情報
121 仮想マシンコード
1151 検証値取得モジュール
1152 検証値変換モジュール
1153 ステート保持モジュール
1154 仮想マシンコード実行モジュール
1121 仮想マシン検証モジュール

1122 検証情報モジュール

1123 コード依存処理モジュール

401 アドレス

402 値

501 検証順序

502 検証値

発明を実施するための最良の形態

[0018] 以下、発明を実施するための最良の形態を、図面を参照しながら説明する。

図1を使って、本発明の一実施形態に係る記録媒体、及び情報処理装置について説明する。

記録媒体102には、仮想マシン上で動作するプログラムである、仮想マシンコード121が記録されている。記録媒体102の一実装例としては、BD(Blu-ray Disc)であるが、それに限るものではない。さらに、仮想マシンコード121は、仮想マシン検証モジュール1121、検証情報保持モジュール1122、コード依存処理モジュール1123から構成される。各モジュールの詳細は後述する。

[0019] 情報処理装置101は、仮想マシンを使って、仮想マシンコード121を実行する装置であり、図1に示すように、ディスク読込部111、ユーザ操作受付部112、仮想マシン実行部113、情報保持部114から構成される。仮想マシンとは、CPUやOS等のプラットフォームに依存せずに、プログラムを動作させるために、仮想マシンコード121として実装されたプログラムを、プラットフォーム用のネイティブコードに変換して実行するソフトウェアである。具体的には、例えば仮想マシンはJava(登録商標)仮想マシンであり、仮想マシンコード121はJavaバイトコードであるが、これに限るものではない。

[0020] 情報処理装置101の一実装例としては、CPU、ワークメモリ、フラッシュメモリ、BDドライブ、リモートコントローラとから構成されるコンピュータシステムであり、ディスク読込部111はBD(Blu-ray Disc)ドライブであり、情報保持部114はフラッシュメモリであり、ユーザ操作受付部112はリモートコントローラであり、仮想マシン実行部113は、CPUとワークメモリを用いて動作するソフトウェアで構成する方法が挙げられるが、他にも、ハードウェアでの実装など、ソフトウェアによる構成に限定されるものではない。

い。その他の実装形態についても、これに限定されるものではない。

[0021] また、情報保持部114には、仮想マシン実行コード115と、検証値テーブル116と、検証値テーブル識別情報117が保持されている。仮想マシン実行コード115は、ソフトウェアであり、検証値取得モジュール1151、検証値変換モジュール1152、ステート保持モジュール1153、仮想マシンコード実行モジュール1154から構成される。各モジュールの詳細は後述する。

[0022] 検証値テーブル116は、情報処理装置の実行環境に関する値を保持しているメモリテーブルであり、仮想マシンコード121が仮想マシンを含む実行環境の正当性を検証するために利用する値を記録したものである。例えば、下記のようにファームウェアのバイナリデータ等であって情報処理装置101固有のものであるため、情報処理装置毎に異なる値をとるデータである。図4に、具体的なデータ構成を示す。検証値テーブル116は、アドレス401と値402で構成されている。例えば、アドレス0x00ff0000に対応する値は、0x00であることを意味している。また、検証値テーブル116は固定的なものではなく、検証値を要求された時点で必ず固定的な値を返すことができれば、検証値テーブル116の全部もしくは一部が、処理を実行する中で動的に変更されても構わない。

[0023] 検証値テーブル識別情報117は、検証値テーブル116を識別するための情報であり、例えば、「情報処理装置メーカID＋情報処理装置のモデル番号＋検証値テーブルのバージョン番号」で構成される8バイトのデータであるが、検証値テーブル116を一意に特定できる情報であれば、これに限るものではない。

ここで、検証情報の作成について説明する。正規の仮想マシン実行コード115の提供者は、仮想マシンの検証値テーブル116と検証値テーブル識別情報117を仮想マシン管理機関に提出する。仮想マシン管理機関は、仮想マシンコードの実装者に対し、正規の仮想マシンの検証値テーブル116と検証値テーブル識別情報117を提供する。仮想マシンコードの実装者は、これを基に検証情報を作成する。

[0024] なお、本実施の形態では、記録媒体102として、BDを想定し、そこに記録された仮想マシンコード121をディスク読込部111にて情報処理装置101に取り込んでいるが、これに限るものではなく、例えば、ディスク読込部111をインターネット接続部に置

き換え、仮想マシンコード121をインターネット経由で情報処理装置101に取り込む等、他の方法で仮想マシンコード121を情報処理装置101に取り込んでもよい。

[0025] 以上で、本発明の一実施形態に係る記録媒体、及び情報処理装置についての説明を終わる。

(仮想マシンコードの実行)

次に、図2を使って、情報処理装置101での仮想マシンコードの実行について説明する。

[0026] まず、情報処理装置101はユーザ操作受付部112を通じて、記録媒体102上の仮想マシンコード121を実行するよう指示を受けることで処理が開始される。

仮想マシンコード121の実行が指示されると、仮想マシン実行部113は、情報保持部114から、仮想マシン実行コード115と検証値テーブル116をロードし、仮想マシンを起動する(S201)。

[0027] 次に、ディスク読込部111を通じて記録媒体102から、仮想マシンコード121を読み出し、仮想マシン実行部113が仮想マシン上で仮想マシンコード121を起動する(S202)。

仮想マシン上で起動された仮想マシンコード121は、仮想マシン検証モジュール1121、及び検証情報保持モジュール1122を用いて、自身を実行している仮想マシンを含む実行環境の正当性の検証を行う(S203)。この処理の詳細については、後述する。

[0028] S203の検証結果がNGの場合、仮想マシンコード121は自身の実行を終了するように実装されているため、その実行を終了する(S204)。

S203の検証結果がOKの場合、仮想マシンコード121中のコード依存処理モジュール1123で定義されたコード依存処理を実行する(S205)。コード依存処理モジュール1123には、仮想マシンコード121毎に異なる処理が定義されており、例えば、記録媒体102に別途記録された映画等のコンテンツデータの著作権保護処理として、コンテンツの復号処理を行うが、これに限るものではない。

[0029] コード依存処理が終了した時点で、仮想マシンコード121の実行を終了する。

以上で、情報処理装置101での仮想マシンコード121の実行についての説明を終

わる。

(仮想マシンを含む実行環境の正当性検証)

仮想マシンを含む実行環境の正当性検証処理の詳細について説明する。この処理は、仮想マシンコード121によって、自身を実行する仮想マシンが正規のものがどうかを検証する処理である。

[0030] 仮想マシン実行コード115は、インタフェースや処理内容等の実装に必要な情報が公開されているため、誰でも実装することができる。このため、正規の仮想マシン実行コード115でなければ、仮想マシンコード121の実行時に不正な動作を行い、仮想マシンコード121の処理が正しく行われなくなる可能性がある。仮想マシンコード121が、例えば、記録媒体102に別途記録されている映画等のコンテンツの著作権を保護するプログラムである場合には、不正にコンテンツを再生され、著作権を保護できなくなるため、仮想マシンを含む実行環境の検証処理が必要になる。

[0031] 仮想マシンコード121を構成するモジュールについて説明する。仮想マシン検証モジュール1121は、自身を実行する仮想マシンが正規のものかどうかを検証するモジュールであり、検証情報保持モジュール1122は、仮想マシンを含む実行環境の正当性を検証するための情報である。具体的には、仮想マシンから検証値テーブル識別情報117と検証値を取得し、その値が検証情報保持モジュール1122で保持する検証情報と一致するかどうかで、仮想マシンを含む実行環境の正当性を検証する。これにより、異なる再生装置にプレーヤモデル番号、メーカー名等を含むデータをコピーしたエミュレータを作成し、例えばコンピュータ上で仮想マシン及び該エミュレータを搭載したとしても、検証値テーブル116に保持された機器固有の値が異なるものとなるため、かかる不当なエミュレータ上における再生を阻止することができる。検証処理の詳細については、後述する。

[0032] 次に、仮想マシン実行コード115を構成するモジュールについて説明する。検証値取得モジュール1151は、仮想マシンコード121中の仮想マシン検証モジュール1121が指定したアドレスに該当する値を、検証値テーブル116中から検索し、その値を取得するモジュールである。検証値変換モジュール1152は、検証値テーブル116から取得した値を演算により変換するモジュールである。仮想マシンはステートを持

っており、検証値テーブル116から読み込んだ値を、ステートに応じて一意的に変換する特徴を持つ。また、ステートは、変換処理が終了した後、これまでの読み出された検証値の読み出し順序によって一意的に決定される値に、更新される。このステートを保持するのが、ステート保持モジュール1153である。

- [0033] 仮想マシンコード実行モジュール1154は、仮想マシンコード121中のコード依存処理モジュール1123で定義される処理をプラットフォームに依存するネイティブコードに変換しながら、実行するモジュールである。

検証値テーブル116は、アドレス401と、値402から構成されるデータであり、値402に対し、一意のアドレス401が対応しているテーブルである。なお、検証値テーブル116の値402を一意に特定することができれば、アドレス401は、物理／論理アドレス、実／仮想アドレスを問わない。また、フォントファイルやファームウェアのバイナリデータ等、情報処理装置101が他の用途のために保持しているバイナリデータの一部を検証値テーブル116として流用しても構わない。

- [0034] 続いて、図3を使って、仮想マシンを含む実行環境の正当性検証処理フローについて説明する。

最初に、仮想マシンコード121は、例えば、0x12などの初期値を仮想マシンに与える(S301)。初期値は予め決定しておいた値であれば、他の値を用いても構わない。

- [0035] 仮想マシンは、与えられた初期値をステート保持モジュール1153に保持する(S302)。続いて、仮想マシンは、検証値テーブル識別情報117を仮想マシンコード121に送信する(S303)。次に、仮想マシンコード121は、仮想マシン検証モジュール1121を使って、S303で受信した検証値テーブル識別情報117に該当する検証情報を検証情報保持モジュール1122から取得する(S304)。続いて、仮想マシン検証モジュール1121を使って、検証回数を確認する。検証回数が、仮想マシン検証モジュール1121内で設定された規定回数に達した場合、処理を終了し、規定回数に満たない場合、検証処理を継続する(S305)。

- [0036] 次に、仮想マシン検証モジュール1121は、検証情報保持モジュール1122が保持する検証情報に定義された順序に従って、仮想マシンに対して検証値を要求する(S

306)。検証情報保持モジュール1122が保持する検証情報のデータ構造を図5に示す。検証情報は、検証値テーブル識別情報117、検証順序501、アドレス401、検証値502から構成され、各情報処理装置101が保持する検証値テーブル116に対応する検証情報を持つ。例えば、図5では、検証値テーブル識別情報117が0x0011ff0000011001の検証情報と、同じく検証値テーブル識別情報117が0x0022ee0000050003の検証情報と、他の検証情報が記述されていることを示している。仮想マシン検証モジュール1121は、S303で受信する検証値テーブル識別情報117と合致するレコードを参照し、検証順序501の順に、アドレス401を使って検証値を仮想マシンに要求する。仮想マシンが返すアドレスの対応する値と、検証値502が一致するかを確認することで、仮想マシンを含む実行環境の正当性を検証する。

[0037] S306では、仮想マシン検証モジュール1121は、検証情報に従い、現在までの検証回数に応じたアドレス401を指定して検証値を仮想マシンに要求するが、具体的に図5の検証値テーブル識別情報117が0x0011ff0000011001の検証情報を用いた場合では、現在までの検証回数が0回の時は、アドレス0x00ff0001を指定して、また、現在までの検証回数が2回の時は、アドレス0x00ff0002を指定して検証値を要求する。

[0038] 検証値の要求を受けた仮想マシンは、検証値取得モジュール1151を使って、検証値テーブル116から指定されたアドレスに対応する値を取得する(S307)。例えば、仮想マシン検証モジュール1121からアドレス0x00ff0001に対応する値を要求された場合、図4の検証値テーブル116から、該当するアドレス401に対応する値0xffを取得する。

[0039] 続いて、仮想マシン中の検証値変換モジュール1152はステート保持モジュール1153からステートを取得する(S308)。例えば、初期状態の場合には、S301、S302で保持したステート0x12を取得する。

次に、検証値変換モジュール1152が検証値テーブル116から取得した値に演算を施し、変換する(S309)。例えば、検証値変換モジュール1152は、ステート保持モジュール1153から取得したステートと、検証値テーブル116から読み込んだ値のXORを行い、変換する。具体的には、取得したステートが0x12、検証値テーブル116

から読み込んだ値が0xffの場合、0xedに変換する。

- [0040] 次に、検証値変換モジュール1152は、S309で利用した値を使って、ステート保持モジュール1153のステートを更新する(S310)。例えば、指定されたアドレスの最下位1バイトの値と、ステート保持モジュール1153が保持する値をXORした値で更新する。

次に、仮想マシンは、S309で算出した検証値を仮想マシンコード121に返す(S311)。仮想マシンコード中の仮想マシン検証モジュール1121が、その値と、検証情報中の値が一致するかを確認し、一致する場合は検証結果をOK、一致しない場合は検証結果をNGと判断する(S321)。

- [0041] 検証結果がOKの場合、S305に戻り、規定回数分の検証を実施する。検証結果がNGの場合、処理を終了する(S322)。

以上で、仮想マシンを含む実行環境の正当性検証処理の説明を終わる。

なお、本実施の形態のS301で、仮想マシンに設定する初期値は、仮想マシンコード121が保持しているとしたが、これに限るものではなく、仮想マシン実行コード115が保持しても構わない。この場合、S301では、仮想マシンコード121が仮想マシンに対して、初期値を設定するのではなく、初期化要求のみを行う。この初期化要求は、ステート保持モジュール1153が仮想マシン検証モジュール1121実行時に初期値を読み込む構成としても良いし、仮想マシン検証モジュール1121が明示的に実行を指示するコードを含む構成としても良い。他にも、検証値テーブル116内の特定の値を初期値として用いても構わない。

- [0042] また、本実施の形態のS309では、検証値の変換演算として、ステート保持モジュール1153から取得したステートと、指定されたアドレスに対応する値のXORを用いているが、これに限るものではなく、ステート保持モジュール1153から取得したステートと、検証値テーブル116から読み込んだ値を使って、一意な値を算出できれば、SHA等の一方向性関数、AES等の暗号関数等の他の演算を用いても構わない。

- [0043] また、本実施の形態では、仮想マシンが要求された検証値をS309で変換した上で仮想マシンコード121に返しているが、検証値テーブル116の値を変換せずにそのまま返しても構わない。この場合、図1における、検証値変換モジュール1152、ステ

ート保持モジュール1153、及び図3におけるS301、S302、S308、S309、S310のステップは不要となる。

[0044] また、本実施の形態のS310では、ステート更新において、更新する値の算出方法として、指定されたアドレスの最下位1バイトの値と、ステート保持モジュール1153が保持する値をXORしているが、これに限るものではなく、検証値を呼び出す順序に応じて異なる値を算出でき、且つ再現性のある算出方法であれば、他の方法を用いても構わない。このようにして算出するステートを検証値の変換に用いていることで、仮想マシンコード121から見た場合、同じアドレスを指定して検証値を要求しても、その要求順序が異なれば、異なる値が返ってくるため、例えば検証値テーブル116が暴露された場合でも、S309の変換演算が暴露されなければ、仮想マシンコード121による検証をパスすることができず、セキュリティレベルを向上させる効果がある。

[0045] なお、本実施の形態では、S305において、検証値の確認を規定された複数回数行うことを前提としているが、どの装置に対しても検証値の確認する回数を1回と規定しておき、S305、S322の処理を省略しても構わない。また、この場合、図6に示す検証情報を用いて、1つの検証値テーブル116に該当する検証情報に複数の検証値を用意しておき、検証時にランダムに1つを選択して仮想マシンに検証値を要求しても構わない。このように、検証値を1回しか確認しない場合に検証値をランダムに要求することで、検証値テーブル116の特定アドレスの値が暴露された際に「不正仮想マシンが暴露された固定値を返す」という不正攻撃に対応することができる。

[0046] また、本実施の形態では、検証値変換モジュール1152は、仮想マシン実行コード115に含まれる構成であるが、これに限るものではなく、仮想マシン実行コード115とは、個別に記憶されているとしても良い。

また、本実施の形態では、検証値のデータ長として、1バイトのデータ長を用いているが、これに限るものではない。

[0047] (その他変形例)

なお、本発明を上記実施の形態に基づいて説明してきたが、本発明は、上記の実施の形態に限定されないのはもちろんである。以下のような場合も本発明に含まれる。

(1) 上記の情報処理装置は、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニット、ディスプレイユニット、キーボード、マウスなどから構成されるコンピュータシステムである。前記RAMまたはハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムにしたがって動作することにより、情報処理装置は、その機能を達成する。ここでコンピュータプログラムは、所定の機能を達成するために、コンピュータに対する指令を示す命令コードが複数個組み合わせられて構成されたものである。

[0048] (2) 上記の情報処理装置を構成する構成要素の一部または全部は、1個のシステムLSI(Large Scale Integration:大規模集積回路)から構成されているとしてもよい。システムLSIは、複数の構成部を1個のチップ上に集積して製造された超多機能LSIであり、具体的には、マイクロプロセッサ、ROM、RAMなどを含んで構成されるコンピュータシステムである。前記RAMには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムにしたがって動作することにより、システムLSIは、その機能を達成する。

[0049] (3) 上記の情報処理装置を構成する構成要素の一部または全部は、情報処理装置に脱着可能なICカードまたは単体のモジュールから構成されているとしてもよい。前記ICカードまたは前記モジュールは、マイクロプロセッサ、ROM、RAMなどから構成されるコンピュータシステムである。前記ICカードまたは前記モジュールは、上記の超多機能LSIを含むとしてもよい。マイクロプロセッサが、コンピュータプログラムにしたがって動作することにより、前記ICカードまたは前記モジュールは、その機能を達成する。このICカードまたはこのモジュールは、耐タンパ性を有するとしてもよい。

[0050] (4) 本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。

また、本発明は、前記コンピュータプログラムまたは前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、CD-ROM、MO、DVD、DVD-ROM、DVD-RAM、BD(Blu-ray Disc)、半導体

メモリなどに記録したものとしてもよい。また、これらの記録媒体に記録されている前記デジタル信号であるとしてもよい。

[0051] また、本発明は、前記コンピュータプログラムまたは前記デジタル信号を、電気通信回線、無線または有線通信回線、インターネットを代表とするネットワーク、データ放送等を経由して伝送するものとしてもよい。

また、本発明は、マイクロプロセッサとメモリを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサは、前記コンピュータプログラムにしたがって動作するものとしてもよい。

[0052] また、前記プログラムまたは前記デジタル信号を前記記録媒体に記録して移送することにより、または前記プログラムまたは前記デジタル信号を前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するものとしてもよい。

(5) 本発明は、内部に含んだ仮想マシンによりコンテンツの再生に係る処理を実行する情報処理装置において用いられる検証方法であって、前記コンテンツと共に記録媒体に記録されている検証プログラムを読み込む読込ステップと、前記検証プログラムを前記仮想マシンが実行することにより、前記仮想マシンを含む前記情報処理装置の正当性を検証する検証ステップとを含むことを特徴とする。

[0053] ここで、「読込ステップ」は、実施の形態において説明したS202の処理に含まれる。また、「検証ステップ」は、実施の形態において説明した、S203の処理(図2参照)と、それぞれ対応している。

(6) また、上記の変形例(5)の検証方法であって、前記検証ステップにおいて、タイミングによって変動する証明用情報を用いて、前記検証を行うものとしてもよい。

[0054] ここで、「証明用情報」とは、実施の形態では、図3のS309の処理によって生成された値である。

(7) また、変形例(6)において、前記検証ステップは、前記情報処理装置が保持する秘密情報に基づいた前記証明用情報を要求する要求ステップと、前記証明用情報と、前記記録媒体に記録された検証情報とを比較する比較ステップと、比較結果に基づき、正当であるか否かを判断する判断ステップとを含み、前記検証方法は、さ

らに、前記要求に応じて、前記仮想マシンにより、前記証明用情報を生成し、生成した前記証明用情報を前記検証プログラムに提供する提供ステップを含むとしてもよい。

[0055] この「要求ステップ」、「比較ステップ」及び「判断ステップ」は、上記の実施の形態で説明した、S306、S321及びS322の処理(図3参照)と、それぞれ対応している。「提供ステップ」は、S307～S311の処理と対応している。「秘密情報」は、検証値テーブル116に含まれる値が該当し、「検証情報」は、図5に示す検証値が該当する。

[0056] (8)また、変形例(7)において、前記判断ステップは、タイミングによって前記証明用情報が変動する毎に、前記比較ステップを繰り返させる繰返しステップと、前記繰返しの結果、所定回数連続して、前記検証情報と前記証明用情報が一致しなければ、前記情報処理装置は不正であると決定する決定ステップとを含むとしてもよい。

ここで、「繰返しステップ」は、上記の実施の形態において説明したS322のOK(図3参照)の場合の処理と対応する。「決定ステップ」は、S305の処理及びS322のNGの場合の処理が該当する。

[0057] (9)また、上記の変形例(7)の検証方法において、前記提供ステップは、前記秘密情報の読み出し順序に応じて一意的に決定する値により、前記証明用情報が生成される過程において用いられる演算情報を、変更する更新ステップと、生成した前記証明用情報を、前記検証用プログラムへ出力する出力ステップとを含むとしてもよい。

ここで、「更新ステップ」及び「出力ステップ」は、上記の実施の形態において説明したS310及びS311の処理と、それぞれ、対応している。また、「演算情報」は、実施の形態において説明したステートと対応する。

[0058] (10)また、上記の変形例(6)において、前記記録媒体には、複数の検証候補情報が記録されており、前記情報処理装置は、1以上の秘密情報を保持しており、前記検証ステップは、1の検証候補情報を検証情報として選択する選択ステップと、選択された前記検証情報と対応する秘密情報に基づいて生成された前記証明用情報を要求する要求ステップと、前記検証情報と前記証明用情報とを比較する比較ステップと、比較結果を基に、前記情報処理装置の正当性を判断する判断ステップとを含み、前記検証方法は、さらに、前記要求を受けると、前記仮想マシンにより、前記検

証情報と対応する前記秘密情報を用いて前記証明用情報を生成し、生成した前記証明用情報を前記検証用プログラムへ提供する提供ステップとを含むとしてもよい。

[0059] ここで、「選択ステップ」、「要求ステップ」及び「比較ステップ」は、上記の実施の形態の、S304、S306及び321(図3)参照の処理とそれぞれ対応している。「判断ステップ」は、S322及びS305の処理を含む。「提供ステップ」は、実施の形態のS307～S311の処理が該当する。また、「検証候補情報」は、図5及び図6に示す検証値502が該当する。「検証情報」は、検証値502の中で、S306の処理により、検証順序501に従って選択された1の検証値と対応する。

[0060] (11)また、上記の変形例(10)において、前記判断ステップは、前記比較ステップにより前記検証情報と証明用情報とが一致する場合に、前記選択ステップ、前記要求ステップ及び前記比較ステップを繰り返させる繰返しステップと、前記繰返しにより、所定回数連続して前記検証情報と証明用情報とが一致する場合に、前記情報処理装置が正当であると決定し、それ以外の場合に、前記情報処理装置が不正であると決定する決定ステップを含むとしてもよい。

[0061] ここで、「繰返しステップ」は、実施の形態1では、S322のOKの場合の処理と対応する。「決定ステップ」は、S322のNGの場合の処理及びS305の処理と対応する。

(12)また、上記の変形例(11)において、前記検証ステップの繰返しにおいて、前記選択ステップでは、繰返しの回数に応じて異なる検証候補情報を、前記検証情報として選択し、前記提供ステップでは、繰返しの回数に応じて変動する前記証明用情報を生成するとしてもよいし、同じく変形例(11)において、前記複数の検証候補情報のうち少なくとも一つは、前記仮想マシンを一意に識別する識別子と対応しており、前記選択ステップでは、前記識別子と対応する検証候補情報を前記検証情報として選択するとしてもよい。

[0062] (13)また、上記の変形例(10)において、前記選択ステップでは、ランダムに前記検証情報を選択し、前記比較ステップでは、前記検証情報に対応して、ランダムに変動する前記証明用情報を用いて、前記比較を行うとしてもよいし、同じく変形例(10)において、前記複数の検証候補情報のうち、少なくとも一つは、前記仮想マシンを一意に識別する識別子と対応しており、前記選択ステップでは、前記識別子と対応する

検証候補情報の中から、前記検証情報を選択するとしてもよい。

[0063] ここで、「識別子」は、上記の実施の形態において説明した検証値テーブル識別情報117と対応する。

(14)また、上記の変形例(5)において、前記記録媒体は、さらに、前記仮想マシン上で実行され、前記コンテンツの再生に係る処理手順を含む再生関連プログラムを記録しており、前記検証方法は、さらに、検証の結果、前記情報処理装置が不正である場合、前記コンテンツの再生に係る処理手順の実行を抑制する抑制ステップを含むとしてもよいし、同じく変形例(5)において、前記コンテンツは、デジタル著作物を暗号化して生成されており、前記コンテンツの再生に係る処理手順は、前記コンテンツを復号する手順を含むとしてもよい。

[0064] ここで、「抑制ステップ」は、実施の形態において説明した、S204のNGの処理(図2参照)と対応している。

(15)また、本発明は、仮想マシンを含み、記録媒体に記録されているコンテンツの再生に係る処理を実行する情報処理装置であって、前記記録媒体には、前記仮想マシン上で実行されることにより、前記情報処理装置の正当性を検証する検証プログラムが記録されており、前記情報処理装置は、自身に固有の秘密情報を1以上記憶している記憶手段と、前記検証プログラムを読み込む読込手段と、前記検証プログラムから、タイミングに応じて変動し、前記検証に用いられる検証情報と対応する秘密情報に基づいて生成された証明用情報に対する要求を受付ける受付手段と、前記要求を受け付けると、前記検証情報と対応する秘密情報を用いて、前記証明用情報を生成し、生成した前記証明用情報を、前記検証用プログラムへ提供する提供手段とを備えることを特徴とする情報処理装置でもある。

[0065] また、本発明は、仮想マシンを含み、記録媒体に記録されているコンテンツの再生に係る処理を実行する情報処理装置に搭載される集積回路であって、前記記録媒体には、前記仮想マシン上で実行されることにより、前記情報処理装置の正当性を検証する検証プログラムが記録されており、前記集積回路は、自身に固有の秘密情報を1以上記憶している記憶手段と、前記検証プログラムを読み込む読込手段と、前記検証プログラムから、タイミングに応じて変動し、前記検証に用いられる検証情報と

対応する秘密情報に基づいて生成された証明用情報に対する要求を受付ける受付手段と、前記要求を受け付けると、前記検証情報と対応する秘密情報を用いて、前記証明用情報を生成し、生成した前記証明用情報を、前記検証用プログラムへ提供する提供手段とを備えることを特徴とする集積回路でもある。

[0066] また、本発明は、仮想マシンを含み、コンテンツの再生に係る処理を実行する情報処理装置の正当性を検証する検証プログラムを記録している記録媒体であって、前記検証プログラムと共に、前記検証に用いられる1以上の検証候補情報を記録しており、前記検証プログラムは、前記検証候補情報から、1の検証候補情報を検証情報として選択する選択ステップと、タイミングに応じて変動し、前記検証情報と対応する秘密情報に基づいて生成された証明用情報を、前記仮想マシンに要求する要求ステップと、前記証明用情報を取得し、取得した前記証明用情報と、前記検証情報とを比較する比較ステップと、比較結果に応じて、前記情報処理装置が正当であるか否かを判断する判断ステップとを含むことを特徴とする記録媒体であってもよい。

[0067] また、本発明は、仮想マシンを含み、コンテンツの再生に係る処理を実行する情報処理装置と、前記仮想マシン上で実行されることにより、前記情報処理装置の正当性を検証する検証プログラムを記録している記録媒体から構成される検証システムであって、前記記録媒体は、前記検証プログラムと、前記検証に用いられる1以上の検証候補情報とを記録しており、前記検証プログラムは、前記複数の検証候補情報から、1の検証候補情報を検証情報として選択する選択ステップと、タイミングに応じて変動し、前記検証情報と対応する秘密情報に基づいて生成された証明用情報を、前記記録装置に要求する要求ステップと、前記情報処理装置から、前記証明用情報を取得し、取得した前記証明用情報と、前記検証情報とを比較する比較ステップと、比較結果に応じて、前記情報処理装置が正当であるか否かを判断する判断ステップとを含み、前記情報処理装置は、前記情報処理装置に固有の秘密情報を1以上記憶している記憶手段と、前記検証プログラムを読み込む読込手段と、前記検証プログラムから、前記要求を受け付ける受付手段と、前記要求を受け付けると、前記検証情報と対応する秘密情報を用いて、前記証明用情報を生成し、生成した前記証明用情報を、前記検証用プログラムへ提供する提供手段とを備えることを特徴とする検証シス

テムでもある。

[0068] ここで、上記の「検証プログラム」は、図1に示す仮想マシン検証モジュール1121と対応しており、「検証候補情報」は、図5及び6に示す検証値502と対応する。

本変形例の「検証プログラム」に含まれる、「選択ステップ」、「要求ステップ」及び「比較ステップ」は、上記の実施の形態の、S304、S306及び321(図3)参照の処理とそれぞれ対応している。「判断ステップ」は、S322及びS305の処理を含む。

[0069] 「情報処理装置」を構成する「記憶手段」は、情報保持部114と対応している。「読み込み手段」は、ディスク読込部111と対応する。「受付手段」及び「提供手段」は、仮想マシン実行部113が、仮想マシン実行コード115に含まれる命令コードを読み出し、解読し、実行することにより実現される。また、「秘密情報」は、図4を用いて説明した値402がこれに該当し、「証明用情報」は、S309の処理により生成される値である。

[0070] (16)また、本発明は、仮想マシンを含み、コンテンツの再生に係る処理を実行する情報処理装置の正当性を検証する検証プログラムであって、前記複数の検証候補情報から、1の検証候補情報を検証情報として選択する選択ステップと、タイミングに応じて変動し、前記検証情報と対応する秘密情報に基づいて生成された証明用情報を、前記記録装置に要求する要求ステップと、前記情報処理装置から、前記証明用情報を取得し、取得した前記証明用情報と、前記検証情報とを比較する比較ステップと、比較結果に応じて、前記情報処理装置が正当であるか否かを判断する判断ステップとを含むことを特徴とする検証プログラムでもある。

[0071] ここで、上記の「検証プログラム」は、図1に示す仮想マシン検証モジュール1121と対応しており、「検証候補情報」は、図5及び6に示す検証値502と対応する。「検証プログラム」に含まれる、「選択ステップ」、「要求ステップ」及び「比較ステップ」は、上記の実施の形態の、S304、S306及び321(図3)参照の処理とそれぞれ対応している。「判断ステップ」は、S322及びS305の処理を含む。また、「秘密情報」は、図4を用いて説明した値402がこれに該当し、「証明用情報」は、S309の処理により生成される値である。

[0072] (17)また、本発明は、仮想マシンを含み、記録媒体に記録されているコンテンツの

再生に係る処理を実行する情報処理装置において用いられる証明プログラムであって、前記記録媒体には、前記仮想マシン上で実行されることにより、前記情報処理装置の正当性を検証する検証プログラムが記録されており、前記情報処理装置は、前記情報処理装置に固有の秘密情報を1以上記憶している記憶手段を備え、前記証明プログラムは、前記検証プログラムから、タイミングに応じて変動し、前記検証に用いられる検証情報と対応する秘密情報に基づいて生成された証明用情報に対する要求を受付ける受付ステップと、前記要求を受け付けると、前記検証情報と対応する秘密情報を用いて、前記証明用情報を生成し、生成した前記証明用情報を、前記検証プログラムへ提供する提供ステップとを備えることを特徴とする証明プログラムでもある。

[0073] ここで、上記の「検証プログラム」及び「証明プログラム」は、実施の形態において説明した仮想マシン検証モジュール1121及び仮想マシン実行コード115とそれぞれ対応する。

「証明プログラム」に含まれる「受付ステップ」は、実施の形態において説明したS307の処理に含まれる、「提供ステップ」は、S307～S311の処理と対応している。

[0074] (18)また、本発明は以下のような構成であってもよい。

(18-1) 本発明は、仮想マシンを使って仮想マシンコードを実行する情報処理方法であって、仮想マシンコードが仮想マシンを含む実行環境の正当性を検証するステップと、検証の結果、前記仮想マシンを含む実行環境が不正であると判定した場合、前記仮想マシンコードの処理を停止するステップと、含むことを特徴とする。

[0075] (18-2) 上記の変形例(18-1)の情報処理方法において、前記検証ステップはさらに、前記仮想マシンが保持する秘密情報に基づいた特定の値を要求するステップと、前記仮想マシンが、前記特定の値を前記仮想マシンコードに提供するステップと、前記特定の値と、前記仮想マシンコードが保持する検証情報を比較し、一致することで正当性を検証するステップとを含むとしてもよい。

[0076] (18-3) また、上記の変形例(18-2)の情報処理方法は、さらに、前記検証ステップを複数回、繰り返して行うステップを含んでもよい。

(18-4) 上記の変形例(18-2)の情報処理方法において、前記仮想マシンが

前記特定の値を前記仮想マシンコードに提供するステップが、前記仮想マシンが、前記特定の値に対し、その読み出し順序に応じて、一意的に決定する値に変換するステップを含むとしてもよい。

[0077] (18-5) また、本発明は、上記の変形例(18-1)～(18-4)の何れかの情報処理方法に含まれるステップをコンピュータに実行させることを特徴とするプログラムでもある。

(18-6) また、本発明は、上記の変形例(18-1)～(18-4)のいずれかに記載された情報処理方法に含まれるステップをコンピュータに実行させることを特徴とするプログラムを記録したコンピュータ読み取り可能な記録媒体でもある。

[0078] (19) 上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

産業上の利用可能性

[0079] 本発明にかかる、仮想マシンを使い、プラットフォームに依存しないプログラムを実行する情報処理装置は、著作権保護用プログラムなど、仮想マシン上で動作するプログラムにセキュリティを要求される場合に有用である。

請求の範囲

- [1] 内部に含んだ仮想マシンによりコンテンツの再生に係る処理を実行する情報処理装置において用いられる検証方法であって、
前記コンテンツと共に記録媒体に記録されている検証プログラムを読み込む読込ステップと、
前記検証プログラムを前記仮想マシンが実行することにより、前記仮想マシンを含む前記情報処理装置の正当性を検証する検証ステップと
を含むことを特徴とする検証方法。
- [2] 前記検証ステップにおいて、タイミングによって変動する証明用情報を用いて、前記検証を行う
ことを特徴とする請求項1に記載の検証方法。
- [3] 前記検証ステップは、
前記情報処理装置が保持する秘密情報に基づいた前記証明用情報を要求する要求ステップと、
前記証明用情報と、前記記録媒体に記録された検証情報とを比較する比較ステップと、
比較結果に基づき、正当であるか否かを判断する判断ステップとを含み、
前記検証方法は、さらに、
前記要求に応じて、前記仮想マシンにより、前記証明用情報を生成し、生成した前記証明用情報を前記検証プログラムに提供する提供ステップを含む
ことを特徴とする請求項2に記載の検証方法。
- [4] 前記判断ステップは、
タイミングによって前記証明用情報の変動する毎に、前記比較ステップを繰り返させる繰返しステップと、
前記繰返しの結果、所定回数連続して、前記検証情報と前記証明用情報が一致しなければ、前記情報処理装置は不正であると決定する決定ステップとを含む
ことを特徴とする請求項3に記載の検証方法。
- [5] 前記提供ステップは、

前記秘密情報の読み出し順序に応じて一意的に決定する値により、前記証明用情報が生成される過程において用いられる演算情報を、変更する更新ステップと、

生成した前記証明用情報を、前記検証用プログラムへ出力する出力ステップとを含む

ことを特徴とする請求項3に記載の検証方法。

[6] 前記記録媒体には、複数の検証候補情報が記録されており、

前記情報処理装置は、1以上の秘密情報を保持しており、

前記検証ステップは、

1の検証候補情報を検証情報として選択する選択ステップと、

選択された前記検証情報と対応する秘密情報に基づいて生成された前記証明用情報を要求する要求ステップと、

前記検証情報と前記証明用情報とを比較する比較ステップと、

比較結果を基に、前記情報処理装置の正当性を判断する判断ステップとを含み、

前記検証方法は、さらに、

前記要求を受けると、前記仮想マシンにより、前記検証情報と対応する前記秘密情報を用いて前記証明用情報を生成し、生成した前記証明用情報を前記検証用プログラムへ提供する提供ステップとを含む

ことを特徴とする請求項2に記載の検証方法。

[7] 前記判断ステップは、前記比較ステップにより前記検証情報と証明用情報とが一致する場合に、前記選択ステップ、前記要求ステップ及び前記比較ステップを繰り返させる繰り返しステップと、

前記繰り返しにより、所定回数連続して前記検証情報と証明用情報とが一致する場合に、前記情報処理装置が正当であると決定し、それ以外の場合に、前記情報処理装置が不正であると決定する決定ステップを含む

ことを特徴とする請求項6に記載の検証方法。

[8] 前記検証ステップの繰り返しにおいて、

前記選択ステップでは、繰り返しの回数に応じて異なる検証候補情報を、前記検証情報として選択し、

前記提供ステップでは、繰返しの回数に応じて変動する前記証明用情報を生成する

ことを特徴とする請求項7に記載の検証方法。

- [9] 前記複数の検証候補情報のうち少なくとも一つは、前記仮想マシンを一意に識別する識別子と対応しており、

前記選択ステップでは、前記識別子と対応する検証候補情報を前記検証情報として選択する

ことを特徴とする請求項8に記載の検証方法。

- [10] 前記選択ステップでは、ランダムに前記検証情報を選択し、
前記比較ステップでは、前記検証情報に対応して、ランダムに変動する前記証明用情報を用いて、前記比較を行う

ことを特徴とする請求項6に記載の検証方法。

- [11] 前記複数の検証候補情報のうち、少なくとも1つは、前記仮想マシンを一意に識別する識別子と対応しており、

前記選択ステップでは、前記識別子と対応する検証候補情報の中から、前記検証情報を選択する

ことを特徴とする請求項10に記載の検証方法。

- [12] 前記記録媒体は、さらに、前記仮想マシン上で実行され、前記コンテンツの再生に係る処理手順を含む再生関連プログラムを記録しており、

前記検証方法は、さらに、検証の結果、前記情報処理装置が不正である場合、前記コンテンツの再生に係る処理手順の実行を抑制する抑制ステップ

を含むことを特徴とする請求項1に記載の検証方法。

- [13] 前記コンテンツは、デジタル著作物を暗号化して生成されており、
前記コンテンツの再生に係る処理手順は、前記コンテンツを復号する手順を含む
ことを特徴とする請求項12に記載の検証方法。

- [14] 仮想マシンを含み、記録媒体に記録されているコンテンツの再生に係る処理を実行する情報処理装置であって、

前記記録媒体には、

前記仮想マシン上で実行されることにより、前記情報処理装置の正当性を検証する検証プログラムが記録されており、

前記情報処理装置は、

自身に固有の秘密情報を1以上記憶している記憶手段と、

前記検証プログラムを読み込む読込手段と、

前記検証プログラムから、タイミングに応じて変動し、前記検証に用いられる検証情報と対応する秘密情報に基づいて生成された証明用情報に対する要求を受付ける受付手段と、

前記要求を受け付けると、前記検証情報と対応する秘密情報を用いて、前記証明用情報を生成し、生成した前記証明用情報を、前記検証用プログラムへ提供する提供手段と

を備えることを特徴とする情報処理装置。

- [15] 仮想マシンを含み、記録媒体に記録されているコンテンツの再生に係る処理を実行する情報処理装置に搭載される集積回路であって、

前記記録媒体には、

前記仮想マシン上で実行されることにより、前記情報処理装置の正当性を検証する検証プログラムが記録されており、

前記集積回路は、

自身に固有の秘密情報を1以上記憶している記憶手段と、

前記検証プログラムを読み込む読込手段と、

前記検証プログラムから、タイミングに応じて変動し、前記検証に用いられる検証情報と対応する秘密情報に基づいて生成された証明用情報に対する要求を受付ける受付手段と、

前記要求を受け付けると、前記検証情報と対応する秘密情報を用いて、前記証明用情報を生成し、生成した前記証明用情報を、前記検証用プログラムへ提供する提供手段と

を備えることを特徴とする集積回路。

- [16] 仮想マシンを含み、コンテンツの再生に係る処理を実行する情報処理装置の正当

性を検証する検証プログラムを記録している記録媒体であって、

前記検証プログラムと共に、前記検証に用いられる1以上の検証候補情報を記録しており、

前記検証プログラムは、

前記検証候補情報から、1の検証候補情報を検証情報として選択する選択ステップと、

タイミングに応じて変動し、前記検証情報と対応する秘密情報に基づいて生成された証明用情報を、前記仮想マシンに要求する要求ステップと、

前記証明用情報を取得し、取得した前記証明用情報と、前記検証情報とを比較する比較ステップと、

比較結果に応じて、前記情報処理装置が正当であるか否かを判断する判断ステップとを含む

ことを特徴とする記録媒体。

- [17] 仮想マシンを含み、コンテンツの再生に係る処理を実行する情報処理装置と、前記仮想マシン上で実行されることにより、前記情報処理装置の正当性を検証する検証プログラムを記録している記録媒体から構成される検証システムであって、

前記記録媒体は、

前記検証プログラムと、前記検証に用いられる1以上の検証候補情報とを記録しており、

前記検証プログラムは、

前記複数の検証候補情報から、1の検証候補情報を検証情報として選択する選択ステップと、

タイミングに応じて変動し、前記検証情報と対応する秘密情報に基づいて生成された証明用情報を、前記記録装置に要求する要求ステップと、

前記情報処理装置から、前記証明用情報を取得し、取得した前記証明用情報と、前記検証情報とを比較する比較ステップと、

比較結果に応じて、前記情報処理装置が正当であるか否かを判断する判断ステップとを含む、

前記情報処理装置は、
前記情報処理装置に固有の秘密情報を1以上記憶している記憶手段と、
前記検証プログラムを読み込む読込手段と、
前記検証プログラムから、前記要求を受け付ける受付手段と、
前記要求を受け付けると、前記検証情報と対応する秘密情報を用いて、前記証明用情報を生成し、生成した前記証明用情報を、前記検証用プログラムへ提供する提供手段とを備える
ことを特徴とする検証システム。

- [18] 仮想マシンを含み、コンテンツの再生に係る処理を実行する情報処理装置の正当性を検証する検証プログラムであって、
前記複数の検証候補情報から、1の検証候補情報を検証情報として選択する選択ステップと、
タイミングに応じて変動し、前記検証情報と対応する秘密情報に基づいて生成された証明用情報を、前記記録装置に要求する要求ステップと、
前記情報処理装置から、前記証明用情報を取得し、取得した前記証明用情報と、前記検証情報とを比較する比較ステップと、
比較結果に応じて、前記情報処理装置が正当であるか否かを判断する判断ステップとを含む
ことを特徴とする検証プログラム。

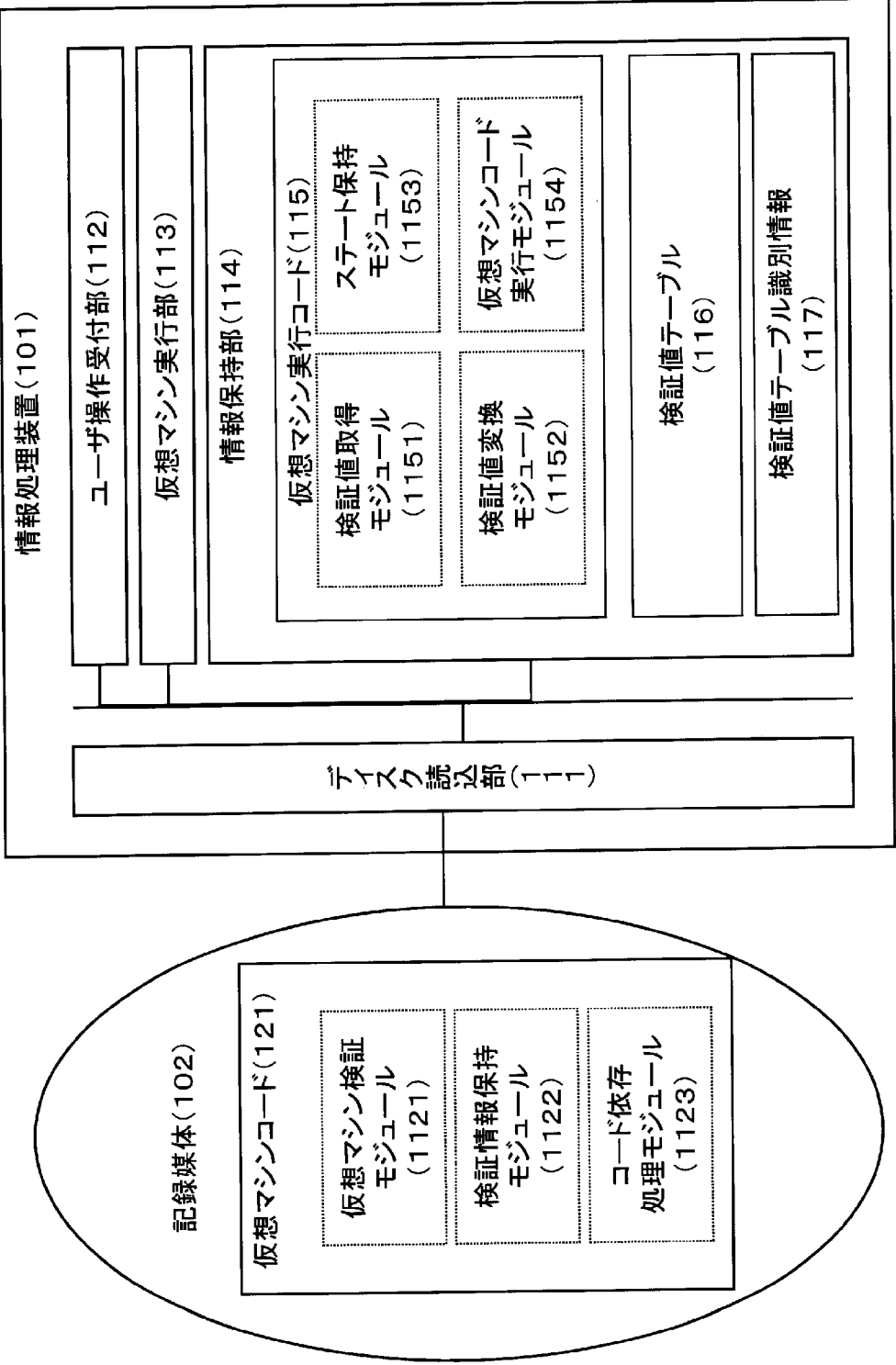
- [19] 仮想マシンを含み、記録媒体に記録されているコンテンツの再生に係る処理を実行する情報処理装置において用いられる証明プログラムであって、
前記記録媒体には、
前記仮想マシン上で実行されることにより、前記情報処理装置の正当性を検証する検証プログラムが記録されており、
前記情報処理装置は、
前記情報処理装置に固有の秘密情報を1以上記憶している記憶手段を備え、
前記証明プログラムは、
前記検証プログラムから、タイミングに応じて変動し、前記検証に用いられる検証情

報と対応する秘密情報に基づいて生成された証明用情報に対する要求を受付ける受付ステップと、

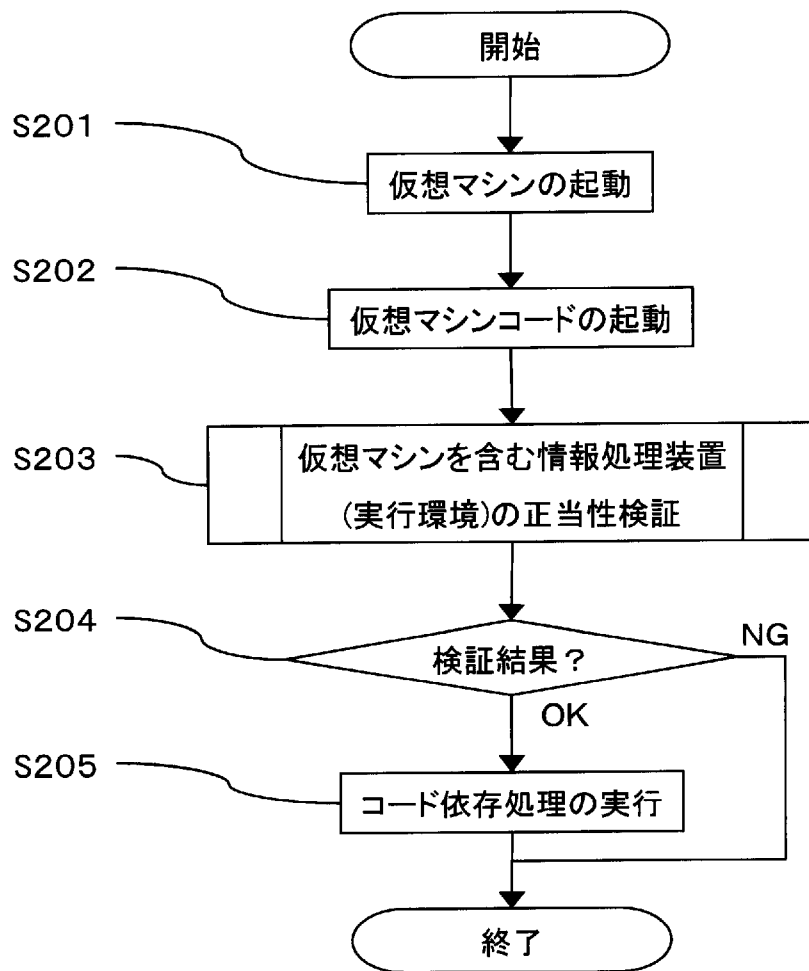
前記要求を受け付けると、前記検証情報と対応する秘密情報を用いて、前記証明用情報を生成し、生成した前記証明用情報を、前記検証用プログラムへ提供する提供ステップと

を備えることを特徴とする証明プログラム。

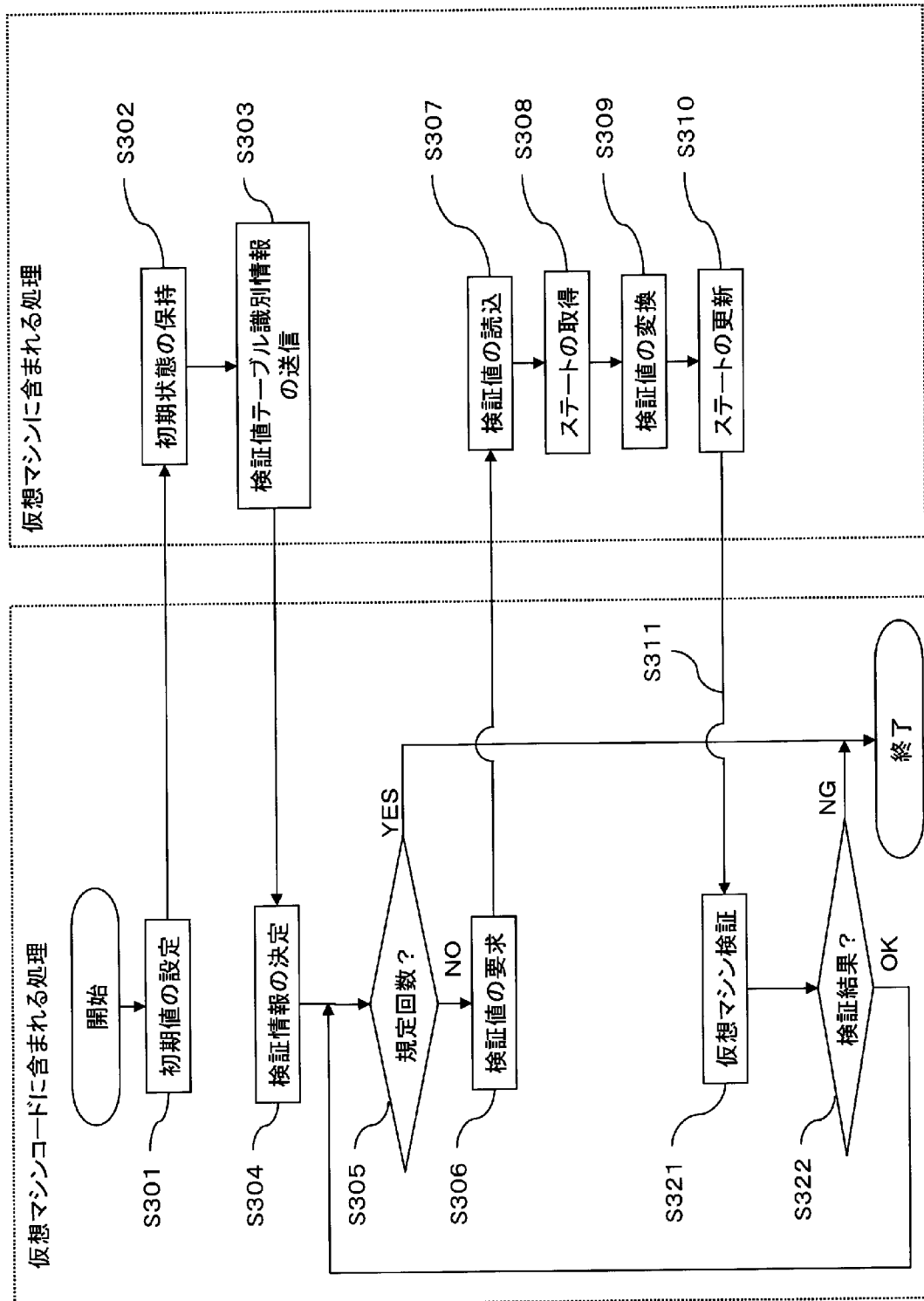
[図1]



[図2]



[図3]



[図4]

アドレス (401)	値 (402)
0x00ff0000	0x00
0x00ff0001	0xff
0x00ff0002	0x04
0x00ff0003	0x04
0x00ff0004	0x26
0x00ff0005	0x25
0x00ff0006	0x80
0x00ff0007	0x71
0x00ff0008	0x15
0x00ff0009	0x21
0x00ff000a	0x91
0x00ff000b	0x12
0x00ff000c	0x12

[図5]

検証値テーブル識別情報 (117)	検証順序 (501)	アドレス (401)	検証値 (502)
0x0011ff0000011001	1	0x00ff0001	0xed
	2	0x00ff0005	0x36
	3	0x00ff0002	0x15
	4	0x00ff0007	0x67
	5	0x00ff0004	0x34
0x0022ee0000050003	1	0x00ee0010	0x1234
	2	0x00ee004a	0x5678
	3	0x00ee0076	0xabcd
⋮			

[図6]

検証値テーブル識別情報 (117)	アドレス (401)	検証値 (502)
0x0011ff0000011001	0x00ff0001	0xed
	0x00ff0002	0x16
	0x00ff0004	0x34
	0x00ff0005	0x37
	0x00ff0007	0x63
0x0022ee0000050003	0x00ee0010	0x4321
	0x00ee004a	0x8765
	0x00ee0076	0xdcba
⋮		

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2006/312797

A. CLASSIFICATION OF SUBJECT MATTER

G06F21/22(2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F21/22

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2006
Kokai Jitsuyo Shinan Koho	1971-2006	Toroku Jitsuyo Shinan Koho	1994-2006

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	Shin HASEGAWA, Noriki AMANO, Kokichi FUTATSUGI, "Fusei na Host no Kogeki ni Taisho suru Mobile Agent no Security Kiko", Information Processing Society of Japan, Dai 63 Kai (Heisei 13 Nen Koki) Zenkoku Taikai Koen Ronbunshu (3), 26 September, 2001 (26.09.01), pages 3-549, 3-550	1 2-19
Y A	JP 2000-295354 A (Siemens Information and Communication Networks Inc.), 20 October, 2000 (20.10.00), Par. No. [0007] & EP 0987846 A2 & US 6526041 B1	1 2-19

☒ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
06 September, 2006 (06.09.06)

Date of mailing of the international search report
19 September, 2006 (19.09.06)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2006/312797

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P,A	WO 2005/096121 A1 (Matsushita Electric Industrial Co., Ltd.), 13 October, 2005 (13.10.05), Full text; all drawings (Family: none)	1-19
P,A	JP 2006-18825 A (Microsoft Corp.), 19 January, 2006 (19.01.06), Full text; all drawings (Family: none)	1-19

A. 発明の属する分野の分類（国際特許分類（I P C））

Int.Cl. G06F21/22(2006.01)i

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（I P C））

Int.Cl. G06F21/22

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922-1996年
日本国公開実用新案公報	1971-2006年
日本国実用新案登録公報	1996-2006年
日本国登録実用新案公報	1994-2006年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y A	長谷川 信, 天野 憲樹, 二木 厚吉, 不正なホストの攻撃に対処するモバイルエージェントのセキュリティ機構, 社団法人情報処理学会、第63回（平成13年後期）全国大会講演論文集（3）, 2001.09.26, p.3-549, p.3-550	1 2-19
Y A	JP 2000-295354 A（シーメンス インフォメーション アンド コミュニケーション ネットワークス インコーポレイテッド） 2000.10.20, 段落【0007】 & EP 0987846 A2 & US 6526041 B1	1 2-19

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日

06.09.2006

国際調査報告の発送日

19.09.2006

国際調査機関の名称及びあて先

日本国特許庁（I S A / J P）
郵便番号100-8915
東京都千代田区霞が関三丁目4番3号

特許庁審査官（権限のある職員）

本郷 彰

5 S

4 2 2 5

電話番号 03-3581-1101 内線 3546

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
P, A	W0 2005/096121 A1 (松下電器産業株式会社) 2005. 10. 13, 全文, 全図 (ファミリーなし)	1-19
P, A	JP 2006-18825 A (マイクロソフトコーポレーション) 2006. 01. 19, 全文, 全図 (ファミリーなし)	1-19