

(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2015 年 11 月 19 日(19.11.2015)



(10) 国際公開番号
WO 2015/174512 A1

- (51) 国際特許分類:
G06F 11/30 (2006.01)
- (21) 国際出願番号: PCT/JP2015/063975
- (22) 国際出願日: 2015 年 5 月 15 日(15.05.2015)
- (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:
特願 2014-102114 2014 年 5 月 16 日(16.05.2014) JP
- (72) 発明者: および
- (71) 出願人: 杉中順子(SUGINAKA Junko) [JP/JP]; 〒1050001 東京都港区虎ノ門 3 丁目 1 0 番 4 号 虎ノ門ガーデン 4 0 8 号 Tokyo (JP).
- (74) 代理人: 特許業務法人 楓国際特許事務所 (KAEDE PATENT ATTORNEYS' OFFICE); 〒5400011 大阪府大阪市中央区農人橋 1 丁目 4 番 3 4 号 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, AO, AT, AU, AZ, BA,

BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

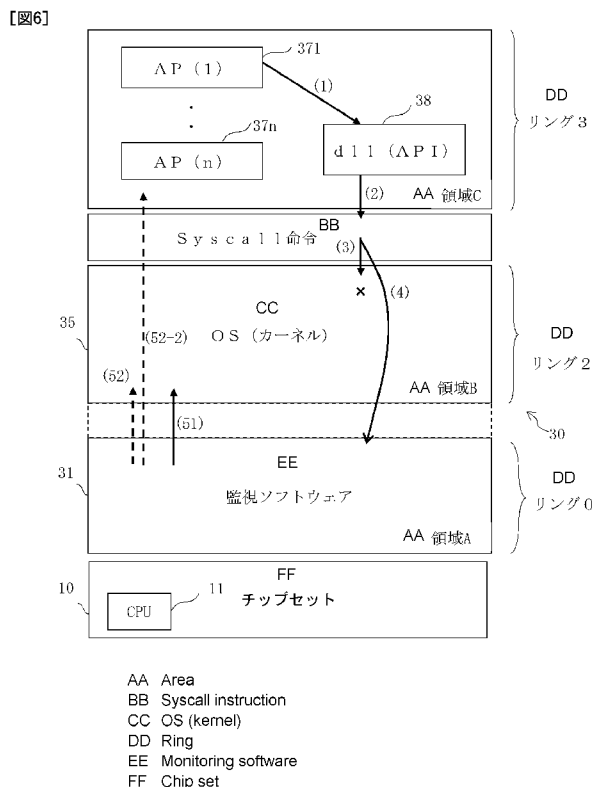
- (84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ユーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類:

- 国際調査報告 (条約第 21 条(3))

(54) Title: INFORMATION-PROCESSING DEVICE, INFORMATION-PROCESSING MONITORING METHOD, PROGRAM, AND RECORDING MEDIUM

(54) 発明の名称: 情報処理装置、情報処理監視方法、プログラム、及び記録媒体



(57) Abstract: An information-processing device (1) is provided with a Syscall-instruction-monitoring unit (313) for monitoring an instruction for passing on at least a process to a kernel (35) of an OS among instructions issued to a CPU (11), and a dedicated loader (201) for loading monitoring software (31) functioning as the Syscall-instruction-monitoring unit (313) into an area (A) of RAM (30) with ring (0) higher than a ring (2) set to the kernel (35) of the OS. Whereby, even when a resource is accessed by execution of an illegal program, the access is detected and intrusion of the illegal program into the kernel is blocked.

(57) 要約: 情報処理装置 (1) は、CPU (11) に対して発行される命令のうち、少なくとも処理をOSのカーネル (35) に引き渡すための命令に対する監視を行う Syscall 命令監視部 (313) と、Syscall 命令監視部 (313) として機能する監視ソフトウェア (31) を、OSのカーネル (35) に設定されるリング (2) より高いリング0でRAM (30) の領域Aにロードする専用ローダ (201) とを備える。これによって、不正なプログラムの実行によってリソースがアクセスされる場合であっても当該アクセスを検知して不正プログラムのカーネルへの侵入を阻止する。

明 細 書

発明の名称：

情報処理装置、情報処理監視方法、プログラム、及び記録媒体

技術分野

[0001] 本発明は、プロセッサが実行する情報処理動作を監視する技術に関する。

背景技術

[0002] 昨今、不正かつ有害な動作を行う意図で作成された悪意のあるプログラム（以下、不正プログラム）によるファイルの書き換えやシステムの設定変更等によってコンピュータのセキュリティが大きく損なわれている。不正プログラムの挙動は、外部からコンピュータ内のメモリに侵入した後、アプリケーションプログラム（ＡＰ）の実行に伴うユーザモードからカーネル空間のリソースへのアクセスに便乗して特権レベル（リング０）を取得し、以後、リソースの制御を支配することで、意図した不正行為を実行可能にする。今日、不正プログラムの実行を監視し、不正動作を規制する各種の対応ソフトウェアが提案されている。

[0003] 特許文献１には、ＡＰＩの利用制限を図るべく、アプリケーションの起動を検出するステップと、起動されたアプリケーションから発行されたリソースに対する処理要求を一時保留するステップと、起動されたアプリケーションが正規のアプリケーションであるか否かを認証するステップと、起動されたアプリケーションの認証結果が成功の場合にのみ、前記一時保留した処理要求による処理を許可するステップとを備えて、リソースの情報漏洩防止を図るアプリケーションの監視方法が記載されている。

[0004] 特許文献２には、コンピュータ上で実行されるアプリケーションがハードディスクＨＤＤ等の記憶装置に記憶された情報にアクセスする時点で、オペレーティングシステム（ＯＳ）のフック機能を利用してこのアプリケーションをフックし、予め設定されたアクセス許容条件を満たすかどうかを判定部によって判定し、ウイルス等の不正なアクセスと判定された場合には前記記

憶装置に記憶された情報のアプリケーションへの受け渡しを禁止するコンピュータの情報漏洩防止システムが記載されている。

- [0005] 特許文献3には、予め専用ローダ及び管理ファイルを格納した外部デバイスを装着してコンピュータの電源を投入することで、外部デバイスから主メモリ（RAM）ロードされる専用ローダを用いて管理ファイルが、更にHDDからOSがロードされる領域をそれぞれ制御し、かつ領域間で特権レベルに差を設けることでRAMの所定領域に管理ファイルによるセキュア領域を確保し得る外部ブート技術が記載されている。

先行技術文献

特許文献

- [0006] 特許文献1：特開2003-108253号公報
特許文献2：特開2007-140798号公報
特許文献3：特開2013-101550号公報

発明の概要

発明が解決しようとする課題

- [0007] 特許文献1に記載された、リソースの情報漏洩防止を図るためのアプリケーション監視方法では、フックを行うフィルタモジュール及び認証モジュールがアプリケーションと同一プロセス空間に設けられた構成であるため、これらモジュールによるフック動作及び認証動作の両信頼性に大きな問題がある。また、フックされたアプリケーションと予め登録されているアプリケーションとのハッシュ値同士を照合によって認証し、この認証が不成功の場合、当該アプリケーションを強制終了又は管理者に通知するようにしているため、コンピュータの動作が停止してしまう場合があるという問題がある。
- [0008] 特許文献2に記載された情報漏洩防止システムは、ファイルシステムの入出力に関する機能を対象とするもので、アクセス許容条件として、コンピュータのユーザインタフェースを介して入力される、ファイルデータの書き込みなどの操作を表すIOタイプ、アプリケーション名、データ・ファイル名

、実行プログラムの実行制約条件（日時、範囲等）などの所定のチェック項目を活用し、これによってユーザの設定によりファイルシステム自身にウイルスに対する監視機能と判断機能を保持させるものである。従って、ファイルデータの読み出しと関連せず、ユーザ空間からカーネル空間のリソースへアクセスするプロセス全般に対して適切な監視を行うには限界がある。

[0009] また、特許文献3に記載された発明は、外部デバイスを必須とし、OSからの不当なアクセスを無効化して、起動時に構築した主メモリ内のセキュア領域を立ち上げ後も維持するようにした技術であり、リソースに対する処理要求のためのカーネルへのアクセス命令に対する監視を行うものではない。

[0010] 本発明は、上記に鑑みてなされたもので、リソースに対する処理要求のためのOSのカーネルへの命令を監視することのできる情報処理装置、情報処理監視方法、プログラム、及び記録媒体を提供することにある。

課題を解決するための手段

[0011] 本発明に係る情報処理装置は、プロセッサに対して発行される命令のうち、少なくとも処理をOSのカーネルに引き渡すための命令に対する監視を行う監視手段と、前記監視手段として機能する監視ソフトウェアを、前記OSのカーネルに設定される特権レベルより高い特権レベルで主メモリの所定領域にロードするロード手段とを含むものである。

[0012] また、本発明に係る情報処理監視方法は、プロセッサに対して発行される命令のうち、少なくとも処理をOSのカーネルに引き渡すための命令に対する監視を行う監視ステップと、前記監視ステップとして機能する監視ソフトウェアを前記OSのカーネルに設定される特権レベルより高い特権レベルを設定して主メモリの所定領域にロードするロードステップとを備えたものである。

[0013] また、本発明に係るプログラムは、プロセッサに対して発行される命令のうち、少なくとも処理をOSのカーネルに引き渡すための命令に対する監視を行う監視手段、前記監視手段として機能する監視ソフトウェアを前記OSのカーネルに設定される特権レベルより高い特権レベルを設定して主メモリ

の所定領域にロードするロード手段として前記プロセッサを機能させるものである。

[0014] また、本発明に係るコンピュータ読み取り可能な記録媒体は、プロセッサに対して発行される命令のうち、少なくとも処理をOSのカーネルに引き渡すための命令に対する監視を行う監視手段、前記監視手段として機能する監視ソフトウェアを前記OSのカーネルに設定される特権レベルより高い特権レベルを設定して主メモリの所定領域にロードするロード手段として前記プロセッサを機能させるプログラムを記録したものである。

[0015] これらの発明によれば、監視ソフトウェアがOSのカーネルに設定される特権レベル（リング）よりも高い特権レベルに設定されるため、プロセッサに対して発行される命令のうち、少なくとも処理をOSのカーネルに引き渡すための命令の発行を常にフック可能な監視状況が確保し得る。従って、かかる命令に不当なプログラムが含まれ、その不正なプログラムの実行によってリソースがアクセスされる場合であっても、当該アクセスを検知して不正プログラムのカーネルへの侵入が阻止される。

発明の効果

[0016] 本発明によれば、不正なプログラムの実行によってリソースがアクセスされる場合であっても当該アクセスを検知して不正プログラムのカーネルへの侵入を阻止することができる。

図面の簡単な説明

- [0017] [図1]本発明に係る情報処理装置の一実施形態を示す構成図である。
[図2]起動後における情報処理装置の主メモリのプログラムマップの一例を示す図である。
[図3]起動処理の一例を示すフローチャートである。
[図4]監視ソフトウェアの一例を示す機能構成図である。
[図5]MSR監視処理の一例を示すフローチャートである。
[図6]監視処理の手順を示す説明図である。
[図7]Syscall監視処理の一例を示すフローチャートである。

[図8]ログ処理の一例を示すフローチャートである。

発明を実施するための形態

[0018] 図1は、本発明に係る情報処理装置の一実施形態を示す構成図である。本発明が適用される情報処理装置1としては、コンピュータを内蔵するサーバ装置、汎用パーソナルコンピュータ、携行用の情報処理端末等、更にはネットワークを介して通信する機能を備えた各種の情報処理装置を含む。

[0019] 情報処理装置1は、マイクロコンピュータで構成され、プロセッサとしてのCPU (Central Processing Unit) 11を含むチップセット10を備える。CPU 10は、バスBAを介してフラッシュROM (Read Only Memory) 21とハードディスクドライブ (HDD) 22とを含む補助記憶装置20、主メモリとしてのRAM (Random Access Memory) 30、入力部40、出力部50、及び必要に応じて設けられるログ記憶部60と接続されている。

[0020] フラッシュROM 21は、BIOS (Basic Input/ Output System) を格納する。HDD 22は、OS (Operation System) の他、各種アプリケーションプログラム及び必要なデータ類の情報を格納する。HDD 22に格納されている情報は、図2に示すように、主に起動時にRAM 30に読み出 (ロード) される。詳細は図2において説明する。

[0021] RAM 30は、主メモリとして機能し、情報処理装置1が起動する際に補助記憶装置20に格納されているプログラム等がロードされると共に、処理途中の情報が一時的に格納される。情報処理装置1は、補助記憶装置20に格納されているプログラム等がRAM 30にロードされ、CPU 11によって実行されることで、公知の各種の情報処理に加えて、本発明に係る図4に示すような処理実行部として機能する。

[0022] 入力部40は、テンキー等を備えたキーボードやマウス、タッチパネル等を含み、所要の情報の入力や処理の指示を行うものである。出力部50は、画像を表示する表示部を想定している。なお、出力部50としては、プリンタ部やインターネット等のネットワークに接続して情報の授受を行う通信部等でもよく、更にこれらが併設されたものでもよい。ログ記憶部60は、後

述するように、情報処理装置 1 の動作中において発生する、リソースに対する処理要求である特権命令によるアクセス（Syscall、Sysenter、コールゲート等）の履歴（プログラム）及び、かかる命令に関する処理内容のログを経時的に記録する。

[0023] 図 2 は、起動後における情報処理装置 1 の RAM 30 のプログラムマップの一例を示す図で、CPU 11 を含むチップセット 10 と共に示している。

[0024] チップセット 10 は、プロセッサとしての CPU 11 の他、現在の CPU 11 の状態を表すフラグレジスタや MSR（Model Specific Register）12、データ格納用の汎用レジスタ 13 の他、メモリのアドレス指定等に関するインデックスレジスタや特殊レジスタ、メモリ管理方式に関するセグメントレジスタ等を備えたレジスタ群を有する。MSR 12 中のレジスタ 121 は、Syscall 命令の発行に対して無効オペコード例外を発生（フック）させる所定のレジスタである。このレジスタ 121 が Disable（=0）のフック条件に設定されている場合、Syscall 命令の発行は無効オペコード違反としてフックされる。

[0025] 図 3 は、起動処理の一例を示すフローチャートである。まず、図 2 に示す RAM 30 のプログラムマップを説明し、次いで、図 3 に示す起動処理のフローチャートについて説明する。

[0026] RAM 30 は、領域 A、B、C に区分け領域を有する。領域 A には特権レベルである DPL（Description Privilege Level）に値 0（いわゆるリング 0）が設定されている。また、領域 B にはリング 2 が、領域 C にはリング 3 が設定されている。領域 A に対して、リング 0 を設定することによって、例えば監視ソフトウェア 31 を最も高い特権レベルでロード可能にしている他、この領域 A 内に設定される情報に対して全てリング 0 でのロードを実現している。DPL（リング）とは、公知のように、メモリ空間の特権レベルを記述するもので、DPL “0” から DPL “3”（リング 0～リング 3）までの 4 ランクがある。DPL 値が相対的に小さい程、特権のレベルが上位となる。例えば、DPL 値の相対的に大きい値として記述された空間で動作す

るプログラムはDPL値がそれより小さい値で記述された空間側にアクセスすることはできない。すなわち、この場合は特権レベル違反として、後述する一般保護例外（#GP）が発行され、当該アクセスは無効とされる。一方、DPL値の相対的に小さい値として記述された空間で動作するプログラムはDPL値がそれより大きい値で記述された空間側にアクセスしたり閲覧したりすることができる。これによって、不適当なアクセスか否かの判断が事前に可能となる。

[0027] 領域Aには、HDD22からロードされる監視ソフトウェア31と、監視ソフトウェア31によって形成されるシステムテーブル34及び割込ハンドラ32と、HDD22からロードされる後述の参照情報部33とが含まれる。なお、参照情報部33は、後述するように監視ソフトウェア31の実行に際して使用されることから、監視ソフトウェア31と一体的に機能する。

[0028] システムテーブル34は、監視ソフトウェア31を動作させるためのGDT (Global Descriptor Table) 341、IDT (InterruptDescriptor Table) 342、TSS (Task State Segment) 343、及びGDT341からのリニアアドレスを物理アドレスに変換するPTE (Page Table Entry) 344等を含む。

[0029] GDT341は、公知のように情報の格納箇所を示すテーブルである。より詳細には、GDT341は、例えば8バイト単位で各情報の格納箇所を管理するセグメントディスクリプタのリストである。各セグメントディスクリプタは、4つの属性を有している。属性は、情報の「種別」（プログラムコード、データ、スタック）と、「ベースアドレス」と、「リミット」と、「DPL」とである。「ベースアドレス」は、情報のRAM30内における格納基準（スタート）アドレスを示している。「リミット」は、情報のアクセス範囲を示す。DPLは、前述した特権レベルを示す。アドレッシングにおいて採用されるセグメントディスクリプタは、リニアアドレスからの変換に際して使用されるセグメントセクタの情報を介して選択される。また、タスクのアクセスが許可されるものか否かは、アクセス要求時に、チップセッ

ト 10 内のレジスタ群内のレジスタ CS, DS, SS のいずれかに書き込まれた CPL (Current Privilege Level) 及び RPL (Requested Privilege Level) と、GDT 341 の対応するセグメントディスクリプタとを照合することで決定される。

[0030] IDT 342 は、例外割込としての一般保護例外 (#GP) に対応して実行される、監視ソフトウェア 31 内の割込ハンドラ 32 の格納箇所を示すテーブルである。

[0031] TSS 343 は、監視ソフトウェア 31 内の各プログラム (タスク) の各々に対応付けて作成されている。すなわち、TSS 343 は、動作状態に応じたプログラムを稼働させるべく、タスクスイッチによって必要なプログラムに実行状態を移し、かつ直前のプログラムの処理内容に対応する個々の TSS にコンテキストすることで、現状復帰を可能にしている。

[0032] PTE 344 は、GDT 341 で作成されたリニアアドレスを物理アドレスに変換するためのもので、各情報 (各プログラムコード、各データ、各スタック) について対応して設けられている。より詳細には、PTE 344 はページを有し、各ページは所定のデータ量、例えば 4 KB 毎に分割されている。各ページデータには、物理アドレスとアクセス属性とが設定されている。各ページデータには、プログラムコード、データ、スタックの種類が含まれる。物理アドレスは、リニアアドレスを RAM 30 内の所定の位置に移動させるためのものである。アクセス属性は、特権レベルに相当するもので、「スーパーバイザー」と「ユーザ」とを有する。なお、「スーパーバイザー」はカーネル空間での処理 (カーネルモード) をいい、リング 0 ~ リング 2 に該当し、「ユーザ」はリング 3 に該当する。なお、波線で示す専用ローダ 201 は、監視ソフトウェア 31 をロードするためのプログラムである。

[0033] 領域 B には、OS であるカーネル (kernel) 35 と、カーネル 35 が自己の挙動を記述するために作成するシステムテーブル 36 とが含まれる。

[0034] 領域 C には、カーネル 35 の環境下で動作する各種のアプリケーションプログラムである AP (1) 371 ~ AP (n) 37n を含む。領域 C には、

AP (1) 371 ~ AP (n) 37n から OS (カーネル) 35 へのアクセスを実行するための関数である API (Application Programming Interface) の動的なリストであるダイナミックリンクライブラリ dli (dynamic link library) (API) 38 が含まれる。dli (API) 38 で作成された、リソースへの処理要求の際の特権レベル 0 でのカーネル 35 に対して発行される API 構造を Syscall 命令という。なお、API とは、複数のプログラムが共通に利用できる種々の機能 (ソフトウェア) の呼び出し時の手順やデータ形式などを定めた仕様をいう。dli (API) とは、モジュール化して実装された API を、動的なリンクによって実行時にプログラムの結合を行うようにした共有ライブラリをいう。

[0035] 図 3 において、まず装置の電源が投入されると、フラッシュ ROM 21 から BIOS (プログラム) が RAM 30 にロードされ (ステップ S1)、続いて BIOS が起動されて利用可能な周辺機器の初期化を行う POST (Power On Self Test) 処理が実行される (ステップ S3)。

[0036] 次いで、監視ソフトウェア 31 のロード処理が実行される (ステップ S5)。監視ソフトウェア 31 のロード処理は、例えば以下の手順で行うことができる。すなわち、BIOS によって HDD 22 の先頭セクタから MBR (Master Boot Record) が RAM 30 にロードされ、次いで CPU 11 の制御が MBR に渡されて、HDD 22 のアクティブなパーティションテーブルに予め格納されている専用ローダ 201 (図 2 参照) が RAM 30 にロードされる。次いで、専用ローダ 201 によって一時的な GDT が作成され、この GDT によって領域 A に対して特権レベルがリング 0 に設定され、この状態で監視ソフトウェア 31 が領域 A にロードされることで行われる。

[0037] 監視ソフトウェア 31 のロード処理が終了すると (ステップ S7 で Yes)、CPU 11 の制御が監視ソフトウェア 31 に渡される (ステップ S9)。続いて、監視ソフトウェア 31 により、監視環境の設定処理、すなわちシステムテーブル 34 の作成、割込ハンドラ 32 の作成が行われる。次いで、OS ロータ 310 (図 2 参照) が起動されて、領域 B の指定、特権レベルと

してリング2の設定を行って、カーネル35を領域Bにロードする（ステップS11）。なお、その後、公知のように、カーネル35内のAPロードによって、AP371～AP(n)37n、dll(AP1)38が、領域Cに特権レベルとしてリング3でロードされる。

[0038] 図4は、監視ソフトウェアの一例を示す機能構成図である。CPU11は、RAM30にロードされた監視ソフトウェア31を実行する。監視ソフトウェア31は、割込ハンドラ32を作成する割込ハンドラ作成部311、フック条件監視部312、Syscall命令に関する監視を行うSyscall命令監視部313、及び必要に応じて採用されるログ処理部314、環境監視部315を備え、それぞれCPU11の処理実行部として機能する。なお、Syscall命令監視部313は、フック条件監視部312とは個別に実行される態様でもよい。また、ログ処理部314、環境監視部315は、フック条件監視部312及びSyscall命令監視部313とは個別に実行される態様でもよい。

[0039] 割込ハンドラ作成部311は、フック条件監視部312、Syscall命令監視部313でそれぞれ検出されたアクセスに対して発行される各例外に対する一連の監視処理をそれぞれ実行させる割込ハンドラ32を作成する。

[0040] フック条件監視部312は、割込ハンドラ32の内、アクセス検出部3121、及びフック条件を監視するプログラムであるフック条件更正部3122を含む。

[0041] MSR12の内容を読み書きするための命令は特権モード（リング0）で許可される。一方、本実施形態では、カーネル35をリング2として動作させるため、特権命令であるMSR12へのアクセス命令（rdmsr、wrmsr）は、CPU11の一般保護例外となる。この時のCPU11による例外割込みは、予め設定しているIDT342を介して割込ハンドラ32に移行する。

[0042] そこで、割込ハンドラ32のアクセス検出部3121は、この一般保護例外をの発行を受けて、CPU11がスタック（stack）にプッシュ（push）した命令ポインタEIP（例外が発生した命令の実行アドレス）を参照してwrmsr命令か否かを判断する。アクセス検出部3121は、アクセス命令がwrmsr命令

であると判断した場合、その書き込み先がMSR 12内の、Syscall命令に関するレジスタ121か否かを判断する。

[0043] フック条件更正部3122は、アクセス検出部3121によって書き込み先がSyscallに関するレジスタ121であると判断された場合、レジスタ121内のDisable bitを値0にする書き込みを行う。フック条件更正部3122は、その後、カーネル35に制御を戻すため、スタックのEIPにwrmsr命令のバイト数分を足し算してiret命令（割り込みでの呼び出しには、スタック上にフラグ（eflags）も積み上げられるために、専用の復帰命令iretを使用）を発行することにより、カーネル35のwrmsr命令に続く次の命令に制御を戻す。かかるフック条件監視処理を行うことで、レジスタ121の不当な書き換え要求（アクセス）に対して、常にそのDisable bitに対して、当該ビットが書き換えられているか否かに関わらず、一律に値0に更正するようにすることで、後述する例外に対する監視可能状態を維持している。なお、値1に書き換えられている場合にのみ、値0に更正するようにしてもよい。

[0044] 図5は、MSR監視処理の一例を示すフローチャートである。なお、図5において、ステップS21、S23は一般保護例外のステップであるが、理解を助ける意味で本フローチャートに含めて説明している。まず、MSR 12へのアクセス命令による一般保護例外が発生したか否かが判断される（ステップS21）。MSRレジスタ12へのアクセス命令による一般保護例外でなければ、本フローをスルーし、MSR 12へのアクセス命令による一般保護例外であれば、処理が割込ハンドラ32に移行される（ステップS23）。

[0045] そして、割込ハンドラ32で、一般保護例外の内容が検査され、書き込み（wrmsr）命令か否かが判断される（ステップS25）。一般保護例外の内容が書き込み（wrmsr）命令でなければ、本フローを抜け、一方、一般保護例外の内容が書き込み（wrmsr）命令であれば、続いて、書き込み先がMSRレジスタ12内の、Syscall命令に関するレジスタ121か否かが判断される（ステップS27）。Syscall命令に関するレジスタ121でなければ、発生した

一般保護例外の内容に対応した処理が実行される（ステップS 2 9）。一方、Syscall命令に関するレジスタ1 2 1であれば、当該レジスタ1 2 1内のDisable bitに値0が書き込まれる（ステップS 3 1）。次いで、カーネル3 5に制御を戻すためのiret命令が発行され、カーネル3 5の（wrmsr）命令に続く次の命令に制御が戻される（ステップS 3 3）。

[0046] 図4に戻って、Syscall命令監視部3 1 3は、割込ハンドラ3 2の内、Syscall命令に対する監視を行うプログラムで、検出部3 1 3 1、正否評価部3 1 3 2、及び代理処理部3 1 3 3を含む。

[0047] MSRレジスタ1 2内のSyscall命令に関するレジスタ1 2 1がDisable（= 0）の場合、Syscall命令の発行に対し、CPU 1 1は無効オペコード例外を発生する。すなわち、本実施形態では、リソースへの処理要求を発行するリング0でのアクセス、ここではSyscall命令は、無効オペコード違反（Invalid Opcode Fault）として設定している。無効オペコード違反とは、例えば正当なコンピュータ命令が存在しない場合とかプロセッサが無効なオペランドを含む命令を実行しようとした場合をいい、無効オペコード違反の種類によっては、この違反から回復できず、すなわちシステムの再起動又はシャットダウンを強いられる。リソースへの処理要求のためのアクセス手段がSyscall命令であることから、Syscall命令中に不正プログラムが関与（潜伏など）する可能性を考慮して、本実施形態では、Syscall命令を一律に無効オペコード違反とするフック対象としている。

[0048] 割込ハンドラ3 2としての検出部3 1 3 1は、CPU 1 1による例外割込の発生によって、処理が割込ハンドラ3 2に移行すると、スタックに保存（プッシュ）した命令ポインタEIP（例外が発生した命令の実行アドレス）を参照して、アクセスがSyscall命令であるか否かを判断する。

[0049] 割込ハンドラ3 2としての正否評価部3 1 3 2は、アクセスがSyscall命令であった場合、その時点での汎用レジスタ1 3内のeax, ebx, ecx, edxの各レジスタ等や直前の処理内容を退避保存しているスタックの内容（Syscall命令のコード等）から、カーネル3 5への呼び出し機能とそのパラメータの正

否を、下記のように評価する。

[0050] 正否評価部 3132 による、カーネル 35 の呼び出し機能とそのパラメータの正否の評価は、予め設定された、領域 A 内の参照情報部 33 を利用して、例えば照合によって行われる。参照情報部 33 には、Syscall 命令を構成する API のコードの内、不当性が高い候補が設定されている。不当性が高い API 候補としては、例えば、(a) 現状では未使用乃至は非公開の API、(b) C:¥ WINDOWS (登録商標) や C:¥ Program Files 配下のファイルへの読み書き (改竄や新たな作成など)、(c) カーネル 35 から付与される権限 (Token) の制御 (例えば、ユーザ権限から管理者権限への昇格要求など) がある。また、参照情報部 33 に、AP (1) 371 ~ AP (n) 37n について、スレッドやプロセスの関連を記述する PCR (Processor Control Region) を参照して、(a) 動作を許可されている AP かどうか (例えば、AP のパス (フォルダ) がインストールの許可がなされているフォルダであるかどうか)、(b) データの書込先のフォルダが書込許可されているフォルダであるかどうかを含めてもよい。さらに、(c) API がどのプロセス (アプリケーションプログラム) から発行されたかを含めて区別する、例えば通信する筈のないプロセスが通信の API を発行したかどうか、(d) 通信の API を発行したプロセスが人が操作するプロセスによって生成されたプロセスであったかどうかを区別する内容を含めることで、入力部 40 を経由しての人為的な操作に依拠するものか、プログラムに依拠する (一般的には不正プログラム) ものかの区別を可能にすることが好ましい。

[0051] また、割込ハンドラ 32 としての代理処理部 3133 は、正当と評価された場合、カーネル 35 に制御を移行し、一方、不当と評価された場合、不当と評価された Syscall 命令を無効とした上で、次の命令を、当該 Syscall 命令を発行した AP に戻すか、あるいはカーネル 35 にプログラムの終了機能进行处理させる。

[0052] なお、カーネル 35 に制御を移行する場合、スタックの EIP をカーネル 35

のエントリポイントに書き換えることで、スタックの内容を、リング2に設定されているカーネル35に戻すことが可能となる。なお、リング2に設定されているカーネル35はスーパーバイザ（カーネルモード）で、代理処理部3133で作成された内容を実行する。また、アプリケーションに制御を戻す場合、Syscall命令のバイト数分を足し算して、iret命令を発行することにより制御が移行される。

[0053] 情報処理装置1の動作中に、図6に示すように、例えばAP(1)371が、所定のリソースへの処理要求を発する場合、d11(AP1)38に対してアクセスし（図6、工程(1)参照）、APIを構築してSyscall命令を作成する（図6、工程(2)参照）。次いで、Syscall命令はリング0でカーネル35にアクセスされる（図6、工程(3)参照）。このとき、Syscall命令に対して無効オペコード違反が発行され、この無効オペコード違反が監視ソフトウェア31でフックされる（図6、工程(4)参照）。

[0054] ところで、無効オペコード違反となる対象は、Syscall命令以外にもあることから、無効オペコード違反を発行した命令の内容の分析が行われる。すなわち、Syscall命令に関しては無効処理とする一方、その正否（正当性）の評価結果に応じて代理処理部3133が処置を行うようにしている（図6、工程(51)、(52)参照）。

[0055] より詳細には、代理処理部3133は、評価結果が正当であると判断された場合、カーネル35へ制御を移行する代行処理を行う（図6、工程(51)参照）。代理処理部3133は、カーネル35への制御のための命令として、無効オペコード違反として無効にしたSyscall命令と同一内容を発行する。

[0056] 一方、代理処理部3133は、不当であると判断した場合、カーネル35へ制御を移行するか（図6、工程(52)参照）、あるいはSyscall命令に続く次の命令を発行元のAPに戻す（図6、工程(52-2)参照）処置を行う。カーネル35へ制御を移行する処置は、正当の場合と同様な手順で行う。なお、代理処理部3133によって作成されるSyscall命令は、プログラム

の強制終了を指示するもの、すなわち何らの処理を行うことなく（スルーさせて）、リターンさせるものである。また、Syscall命令に続く次の命令を発行元のAPに戻す処理は、Syscall命令のバイト数分だけ加算することでSyscall命令をスキップしたと同様に、続きの命令に制御を戻すようにしたものである。

[0057] 図7は、Syscall監視処理の一例を示すフローチャートである。なお、図7において、ステップS41、S43は無効オペコード例外の発生ステップであるが、理解を助ける意味で本フローチャートに含めて説明している。まず、図7において、無効オペコード例外の発生か否かが判断される（ステップS41）。無効オペコード例外の発生であると、制御が割込ハンドラ32に移行される（ステップS43）。

[0058] そして、割込ハンドラ32では、無効オペコード例外を発行した命令がSyscall命令であったか否かの分析が行われる（ステップS45）。Syscall命令でなければ、当該命令に応じた他の無効オペコードに対応する処理が実行される（ステップS47）。一方、Syscall命令であれば、正否評価の処理が実行され（ステップS49）、評価の結果が正当であれば（ステップS51でYes）、カーネル35に制御が移行される。（ステップS53）。一方、評価の結果が不当であれば（ステップS51でNo）、Syscall命令に続く次の命令を発行元のAPに戻す処理（iret）、又はカーネル35に対するプログラムの終了機能の処理が施される（ステップS53）。従って、監視ソフトウェア31によれば、リソース（ハードウェア資源）の保護の他、カーネル35及びAPの動作をリアルタイムで監視可能となることから、外部からの不正プログラムの侵入、逆に外部への情報の漏洩が効果的に防止できる。

[0059] また、ログ処理部314は、参照情報部33と一致した、あるいは不当と評価されたアクセスのプログラム内容を全てログ記憶部60に経時方向に格納する。好ましくは発生時刻情報を含めて格納する。ログ記憶部60がインターネット等のネットワークを介してデータサーバ装置としての位置づけである場合、送信元IPアドレスを付して送信し格納させる。外部のデータサ

ーバ装置の場合には、IPアドレス毎にソートすることで、情報処理装置毎のログ管理が可能となる。なお、ログ情報としては無効オペコード違反のSyscall命令が少なくとも含まれていればよい。本実施形態によれば、後に、ログ記憶部60のセーブ内容を分析することで、異常動作や処理があった場合に対する確実かつ適正な事後解析に供することが可能となる。また、解析を通して、以後の教訓材料とすることができ、不正の抑止効果にもつながる。

[0060] なお、本実施形態におけるログ対象情報としては、プロセス一覧、ファイルI/Oログ、ネットワーク送受信ログ、環境設定値アクセスログ、及び監視及びロギング内容の少なくとも1つ乃至は全てが含まれる。プロセス一覧は、実行されたプログラムはプロセスとしてOSに管理され、PCRに格納される。実行されたプロセスは、必ずSyscallを経てカーネル35とのやり取りが発生するため、実行されたプロセスの一覧が取得できる。取得情報としては、例えば、プログラムファイル名とそのパス、プロセスID、起動時間を含む。これらを取得することで、不知もしくはは不要なプログラムの実行の有無が把握できる。また、取得情報から異常なプログラムか否かが判断できる。

[0061] ファイルI/Oログは、Syscall時点でのAPI機能番号（レジスタeax）より、ファイルI/Oの要求を取得し、そのパラメータ値（汎用レジスタ13の内容やスタック内のデータ）からファイルパス及びその操作（読み書き）として取得される。取得情報としては、例えば、ファイルパス、操作方法（書き込みもしくは読み込み）、プロセスIDを含む。これらを取得することで、プログラムファイルの書き込みやシステムフォルダもしくはユーザ指定の特定フォルダに対する操作から不正の有無が判断できる。

[0062] ネットワーク送受信ログは、Syscall及びSysret時点でのAPI機能番号（レジスタeax）より送受信要求を取得し、そのパラメータ値（汎用レジスタ13の内容やスタック内のデータ）から送受信データ及びその操作（connect、send、receive、accept）として取得される。取得情報としては、例えば、操作方法（connect、send、receive、accept）、送受信データ、送受信ポート

、送受信 I P アドレス (IPV4 及び IPV6) を含む。これらを取得することで、情報漏洩の基本となる送受信操作が監視できる。また、送信先 I P アドレス及び受信元 I P アドレスを元に不正アクセスが追跡できる。さらに送受信データの解析に基づく保護を可能とする。

[0063] 環境設定値アクセスログは、カーネルモードからの不正操作が Syscall 命令を介さないため、環境設定値へのアクセスが監視されており、その監視内容として取得される。取得情報としては、例えば、MSR 12 へのアクセスとその内容、コントロールレジスタ (CR0, CR2, CR4) へのアクセスとその内容、デバッグレジスタへのアクセスとその内容、キャッシュ制御命令の実行、C P U I D 命令の実行、ページテーブル PML4 へのアクセス、ソフトウェア割込み命令の実行、C P U システムテーブル (GDT、IDT、LDT、TSS) へのアクセスとロード命令、実行 EIP とそのモジュール名 (カーネルプログラムやカーネルドライバ)、及び未使用割込みベクタへの割込みと割込み先実行コードを含む。

[0064] 監視及びロギング内容には、物理アドレス 1 Mbyte 以下へのアクセスを含む。これは、O S 起動後、使用されない領域であるため、不正利用と見なすことができる。物理アドレス ACPI 管理テーブルへのアクセスは、端末情報の不正取得と見なすことができる。全ページテーブルに対するデバイスアクセス (MMIO) 物理アドレスの設定は、カーネル以外からの直接デバイスアクセスは不正と判断できる。カーネルプログラム領域の比較は、カーネルプログラムの改ざんをチェックできる。

[0065] 図 8 は、ログ処理の一例を示すフローチャートである。まず、Syscall 命令がフックされたかどうか判断され (ステップ S 61)、フックされていないければ、本フローを抜ける。一方、フックされた場合、ログ記憶部 60 に記録される (ステップ S 63)。かかる処理が、シャットダウン (ステップ S 65 で Y e s) まで継続して行われる。なお、ここでは、Syscall 命令をログ対象としたが、特定のフック理由、例えば無効オペコード違反に該当する命令をログ対象とする場合も同様となる。

[0066] ところで、CPU 11の稼働中は、MSR 12や他のレジスタ内の特定のレジスタ等の内容が悪意のプログラムによって書き替えられる可能性がある。環境監視部315は、かかる特定のレジスタ等への書き込みのアクセスが発行されると、このアクセスをフックする機能を備える。ここに、特定のレジスタ等とは、CPU 11の動作に必要とされる根本的な環境設定値が設定されるレジスタである。なお、根本的な環境設定値は、下記のものを含む。環境監視部315は、これらの環境設定値が設定される特定のレジスタ等へのアクセス、特に書込アクセスを、一般保護例外あるいは無効オペコード違反等としてフックし、このアクセスを阻止（無効、禁止、元に戻すなど）した後、次の命令に戻すようにしている。あるいは、書き換えられたか否かを問わず、元の内容に書き直す処理を施して、戻すようにしてもよい。

[0067] 根本的な環境設定値は、以下のように複数種類存在する。まず、プロセス管理情報（Windows（登録商標）OSのPCR, PRCB, ETHREAD, EPROCESS等）を指すOS（カーネル）の環境設定値がある。この設定値へのアクセスはAPIを通じてカーネルに依頼して行わなければならない。そこで、その際、プロセスはOSが管理する管理者権限（CPU 11の権限である、前述のリングとは異なる）が必要となるため、個々のプロセスの権限を監視する。また、他の根本的な環境設定値として、コントロールレジスタ（CR0, CR4, CR3）、デバッグレジスタ（DR0～DR7）、MSR（IA32E_EFERなど）、及びGDTR、IDTR、LDTRに格納されるCPUの環境設定値、MSRの環境設定値があり、これらへのアクセスをリング2にして、監視する。また、他の根本的な環境設定値として、カーネルに依頼する直前とカーネルからの戻り直後のパラメータ値やデータを監視するAPIの環境設定値がある。監視に際しては、「OSの環境設定値」との組み合わせも加味して、正否を判断する。なお、パラメータの監視に関する例としては、指定されたファイルパス（c:\windows\system32\ntoskrnl.exe）に書込みを依頼しようとしたかどうかがあり、また、データの監視に関する例としては、送受信バッファの内容にバイナリが含まれるかどうかがある。また、他の根本的な環境設定値として、コンピュータの電源制御と

ハードウェア構成要素を規格化したACPIの環境設定値（Advanced Configuration and Power Interface）がある。監視ソフトウェア31が構成する物理メモリマップがOSのカーネル35から分からなくするため、カーネル35が物理メモリに関する情報にアクセスした際、その情報を変更する。また、他の根本的な環境設定値として、OSがリアルモードの時、ソフトウェア割込みを使用してBIOS Functionを使用するBIOSジャンプ命令の環境設定値がある。このBIOS Functionの改ざんや不正使用の防止のため、リアルモードの割込みベクタをフックする。また、他の根本的な環境設定値として、KernelDriverの環境設定値がある。ドライバにより「CPU11の環境設定値」を変更しようとした場合、その命令を無視してアンロードする。また、アプリケーションからドライバのロードを禁止する。

[0068] なお、本実施形態では、Syscall命令を無効オペコード違反としてフックするようにしたが、無効オペコード違反に限定されず、他の例外を適用してフックするようにしてもよい。

[0069] 以上説明したように、本発明は、プロセッサに対して発行される命令のうち、少なくとも処理をOSのカーネルに引き渡すための命令に対する監視を行う監視手段と、前記監視手段として機能する監視ソフトウェアを、前記OSのカーネルに設定される特権レベルより高い特権レベルで主メモリの所定領域にロードするロード手段とを含む情報処理装置である。また、本発明は、情報処理監視方法、プログラム、及び記録媒体に適用される。

[0070] 本発明によれば、監視ソフトウェアがOSのカーネルに設定される特権レベル（リング）よりも高い特権レベルに設定されるため、プロセッサに対して発行される命令のうち、少なくとも処理をOSのカーネルに引き渡すための命令の発行を常にフック可能な監視状況が確保し得る。従って、かかる命令に不当なプログラムが含まれ、その不正なプログラムの実行によってリソースがアクセスされる場合であっても、当該アクセスを検知して不正プログラムのカーネルへの侵入が阻止される。

[0071] また、前記監視手段は、前記プロセッサに対して発行される命令のうち、

少なくとも処理を前記OSのカーネルに引き渡すための命令の発行を検出する検出手段と、検出された前記命令の正否を評価する評価手段と、評価結果に応じて前記命令を代理して実行する代理処理手段とを備えることが好ましい。この構成によれば、検出手段によって検知された命令は、評価手段によって正否が評価される。評価は、不正プログラムの可能性に関連する方法で行われる。そして、代理処理手段によって、評価結果に応じた命令が発行される。評価結果とは、評価が正当な場合と不当な場合とを想定しており、いずれの場合にも、代理処理手段によって新たに命令を発行するようにし、発行元からの元の命令は直接使用されない。従って、不正プログラムのカーネルを介してのリソースへの侵入、さらに潜伏が阻止される。

[0072] また、前記検出手段は、前記命令を無効オペコード違反として検出することが好ましい。この構成によれば、問題となるアクセス命令が確実に検知可能となる。

[0073] また、前記命令は、シスコール命令であり、前記評価手段は、前記シスコール命令を構成するAPIに関する情報との照合に基づいて正否を評価することが好ましい。この構成によれば、アプリケーションプログラムからリソースへのアクセスを可能にするシスコール (Syscall) 命令に注目して検知し、シスコールを構成するAPI (Application Programming Interface) に関する情報、例えば属性、格納場所、出典等を参照情報等と照合することで正否評価するので、不正なプログラムか否かが適正に評価される。

[0074] また、前記代理処理手段は、前記評価手段が前記命令を正当と判断した場合、前記命令と同一の内容を前記カーネルへ移行し、前記評価手段が前記命令を不当と判断した場合、前記命令を終了する命令を前記カーネルへ戻すことが好ましい。この構成によれば、アクセス命令が正当、不当いずれの場合であっても、代理処理手段によって新たに命令が発行されるので、不正プログラムの感染の危険が抑止される。

[0075] また、前記代理処理手段は、前記評価手段が前記命令を正当と判断した場合、前記命令と同一の内容を前記カーネルへ移行し、前記評価手段が前記命

令を不当と判断した場合、前記命令をスキップする命令を前記カーネルに戻すことが好ましい。この構成によれば、アクセス命令が正当、不当いずれの場合であっても、代理処理手段によって新たに命令が発行されるので、不正プログラムの感染の危険が抑止される。

[0076] また、前記監視手段に監視のためのフック条件を設定するフック条件設定手段を備え、前記監視手段は、前記フック条件設定手段で設定された前記フック条件に基づいて前記プロセッサに対して発行される命令のうち、少なくとも処理を前記OSのカーネルに引き渡すための命令の発行を検出することが好ましい。この構成によれば、監視手段は、フック条件設定手段によって設定されたフック条件に従って前記前記OSのカーネルに引き渡すための命令の発行を検出する。

[0077] また、前記フック条件設定手段は、前記フック条件に対する書き換えアクセスを監視するフック条件監視手段と、前記フック条件に対する書き換えアクセスの発行の検出毎に、前記フック条件を書き直すフック条件更正手段とを備えることが好ましい。この構成によれば、フック条件監視手段によって前記フック条件に対する書き換えアクセスが監視され、前記フック条件に対する書き換えアクセスの発行の検出毎に、フック条件更正手段によって前記フック条件が正しく書き直される。

[0078] また、前記ロード手段は、前記監視手段として機能する監視ソフトウェアのロードを行う第1のロード手段と、前記第1のロード手段によってロードされた前記監視ソフトウェアに含まれ、前記OSのカーネルのロードを行う第2のロード手段とを含むものであることが好ましい。この構成によれば、監視ソフトウェアのロードを行う第1のロード手段によってロードされた前記監視ソフトウェアに含まれる第2のロード手段によって、前記OSのカーネルのロードが行われるので、前記OSのカーネルにより低い特権レベルが設定される。

[0079] また、前記第1のロード手段は、前記監視手段として機能する監視ソフトウェアを特権レベル0でロードし、前記第2のロード手段は、前記OSのカーネル

ーネルを特権レベル 1 及び 2 のいずれか一方でロードするものであることが好ましい。この構成によれば、監視ソフトウェアは最高権限の特権レベルを有することで、特権レベル 1 か 2 の、カーネルモードで動作可能な前記 OS のカーネル側の挙動を監視することが可能となる。

符号の説明

- [0080] 1 情報処理装置
 - 1 1 CPU (プロセッサ)
 - 1 2 1 Syscall 命令に関するレジスタ
 - 2 0 1 専用ローダ (ロード手段)
 - 3 0 RAM (主メモリ)
 - 3 1 監視ソフトウェア (監視手段)
 - 3 2 割込ハンドラ
 - 3 3 参照情報部
 - 3 5 カーネル
 - 3 8 d l l (A P I)
 - 3 1 2 フック条件監視部 (フック条件設定手段)
 - 3 1 2 1 アクセス検出部 (フック条件監視手段)
 - 3 1 2 2 フック条件更正部 (フック条件更正手段)
 - 3 1 3 Syscall 命令監視部 (監視手段)
 - 3 1 3 1 検出部 (検出手段)
 - 3 1 3 2 正否評価部 (評価手段)
 - 3 1 3 3 代理処理部 (代理処理手段)

請求の範囲

- [請求項1] プロセッサに対して発行される命令のうち、少なくとも処理をOSのカーネルに引き渡すための命令に対する監視を行う監視手段と、
- 前記監視手段として機能する監視ソフトウェアを、前記OSのカーネルに設定される特権レベルより高い特権レベルで主メモリの所定領域にロードするロード手段とを含む情報処理装置。
- [請求項2] 前記監視手段は、
- 前記プロセッサに対して発行される命令のうち、少なくとも処理を前記OSのカーネルに引き渡すための命令の発行を検出する検出手段と、
- 検出された前記命令の正否を評価する評価手段と、
- 評価結果に応じて前記命令を代理して実行する代理処理手段とを備えたことを特徴とする請求項1に記載の情報処理装置。
- [請求項3] 前記検出手段は、前記命令を無効オペコード違反として検出することを特徴とする請求項2に記載の情報処理装置。
- [請求項4] 前記命令は、シスコール命令であり、
- 前記評価手段は、前記シスコール命令を構成するAPIに関する情報との照合に基づいて正否を評価することを特徴とする請求項2又は3に記載の情報処理装置。
- [請求項5] 前記代理処理手段は、前記評価手段が前記命令を正当と判断した場合、前記命令と同一の内容を前記カーネルへ移行し、前記評価手段が前記命令を不当と判断した場合、前記命令を終了する命令を前記カーネルへ戻すことを特徴とする請求項2～4のいずれかに記載の情報処理装置。
- [請求項6] 前記代理処理手段は、前記評価手段が前記命令を正当と判断した場合、前記命令と同一の内容を前記カーネルへ移行し、前記評価手段が前記命令を不当と判断した場合、前記命令をスキップする命令を前記カーネルに戻すことを特徴とする請求項2～4のいずれかに記載の情

報処理装置。

[請求項7] 前記監視手段に監視のためのフック条件を設定するフック条件設定手段を備え、

前記監視手段は、前記フック条件設定手段で設定された前記フック条件に基づいて前記プロセッサに対して発行される命令のうち、少なくとも処理を前記OSのカーネルに引き渡すための命令の発行を検出することを特徴とする請求項1～6のいずれかに記載の情報処理装置。

[請求項8] 前記フック条件設定手段は、前記フック条件に対する書き換えアクセスを監視するフック条件監視手段と、前記フック条件に対する書き換えアクセスの発行の検出毎に、前記フック条件を書き直すフック条件更正手段とを備えたことを特徴とする請求項7に記載の情報処理装置。

[請求項9] 前記ロード手段は、前記監視手段として機能する監視ソフトウェアのロードを行う第1のロード手段と、前記第1のロード手段によってロードされた前記監視ソフトウェアに含まれ、前記OSのカーネルのロードを行う第2のロード手段とを含む請求項1～8のいずれかに記載の情報処理装置。

[請求項10] 前記第1のロード手段は、前記監視手段として機能する監視ソフトウェアを特権レベル0でロードし、前記第2のロード手段は、前記OSのカーネルを特権レベル1及び2のいずれか一方でロードする請求項9に記載の情報処理装置。

[請求項11] プロセッサに対して発行される命令のうち、少なくとも処理をOSのカーネルに引き渡すための命令に対する監視を行う監視ステップと、

前記監視ステップとして機能する監視ソフトウェアを前記OSのカーネルに設定される特権レベルより高い特権レベルを設定して主メモリの所定領域にロードするロードステップとを備えた情報処理監視方

法。

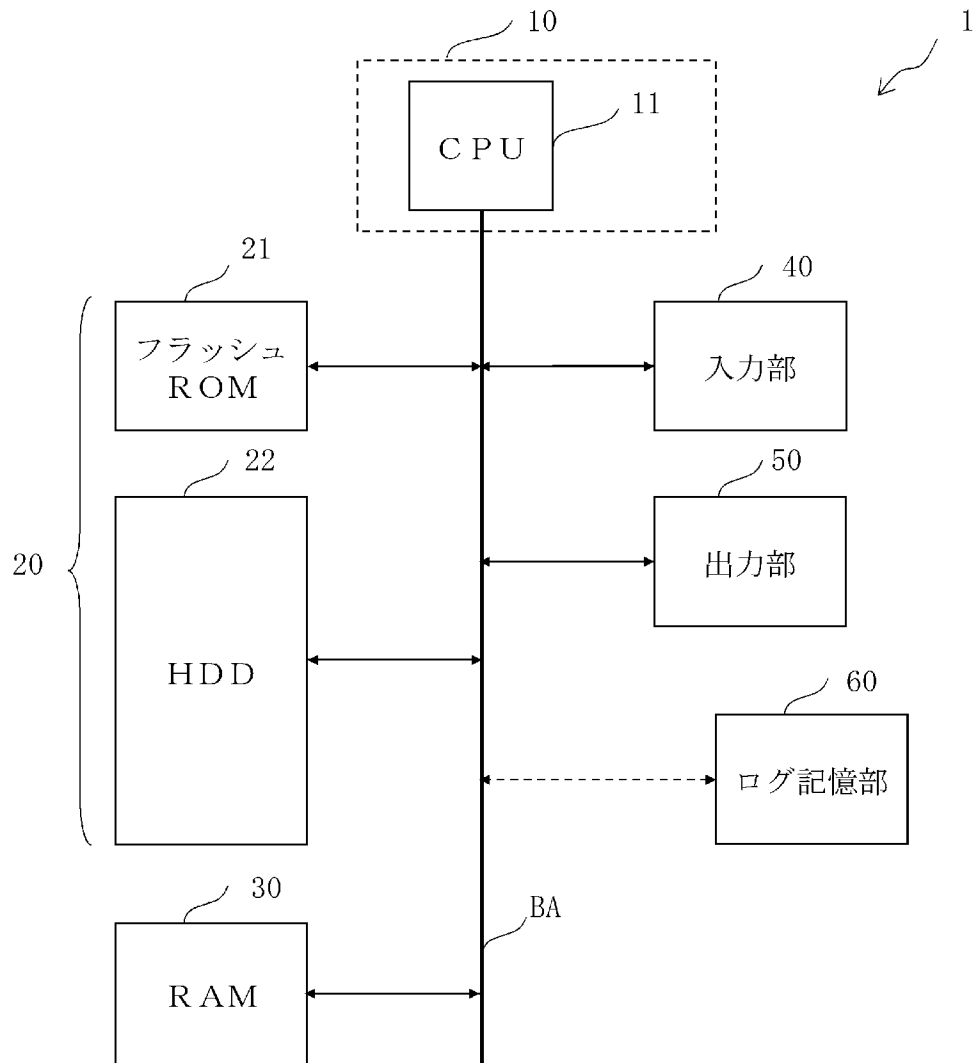
[請求項12] プロセッサに対して発行される命令のうち、少なくとも処理をOSのカーネルに引き渡すための命令に対する監視を行う監視手段、

前記監視手段として機能する監視ソフトウェアを前記OSのカーネルに設定される特権レベルより高い特権レベルを設定して主メモリの所定領域にロードするロード手段として前記プロセッサを機能させるプログラム。

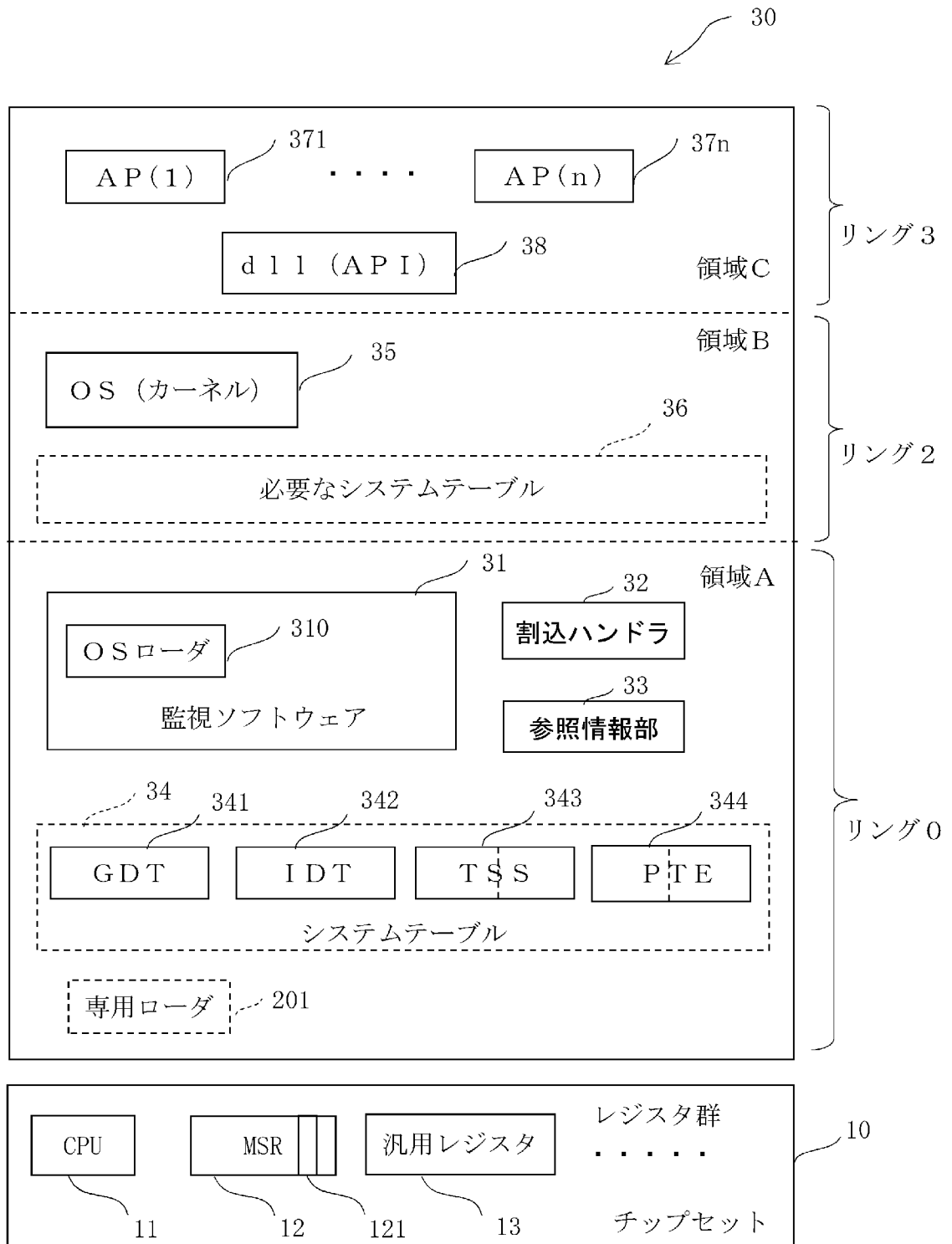
[請求項13] プロセッサに対して発行される命令のうち、少なくとも処理をOSのカーネルに引き渡すための命令に対する監視を行う監視手段、

前記監視手段として機能する監視ソフトウェアを前記OSのカーネルに設定される特権レベルより高い特権レベルを設定して主メモリの所定領域にロードするロード手段として前記プロセッサを機能させ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。

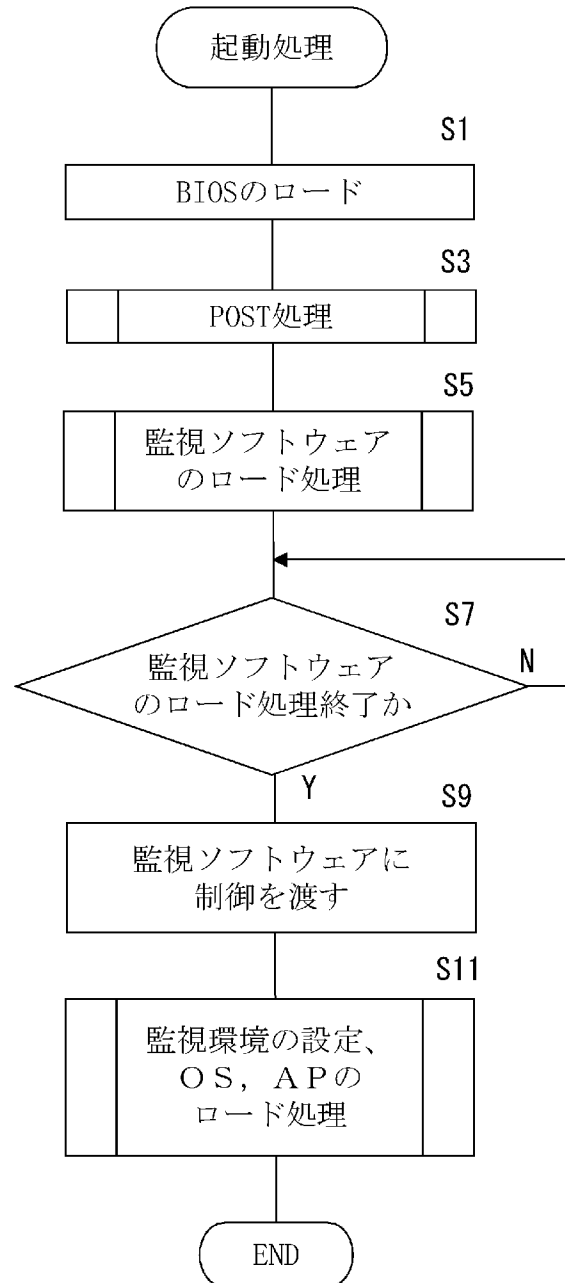
[図1]



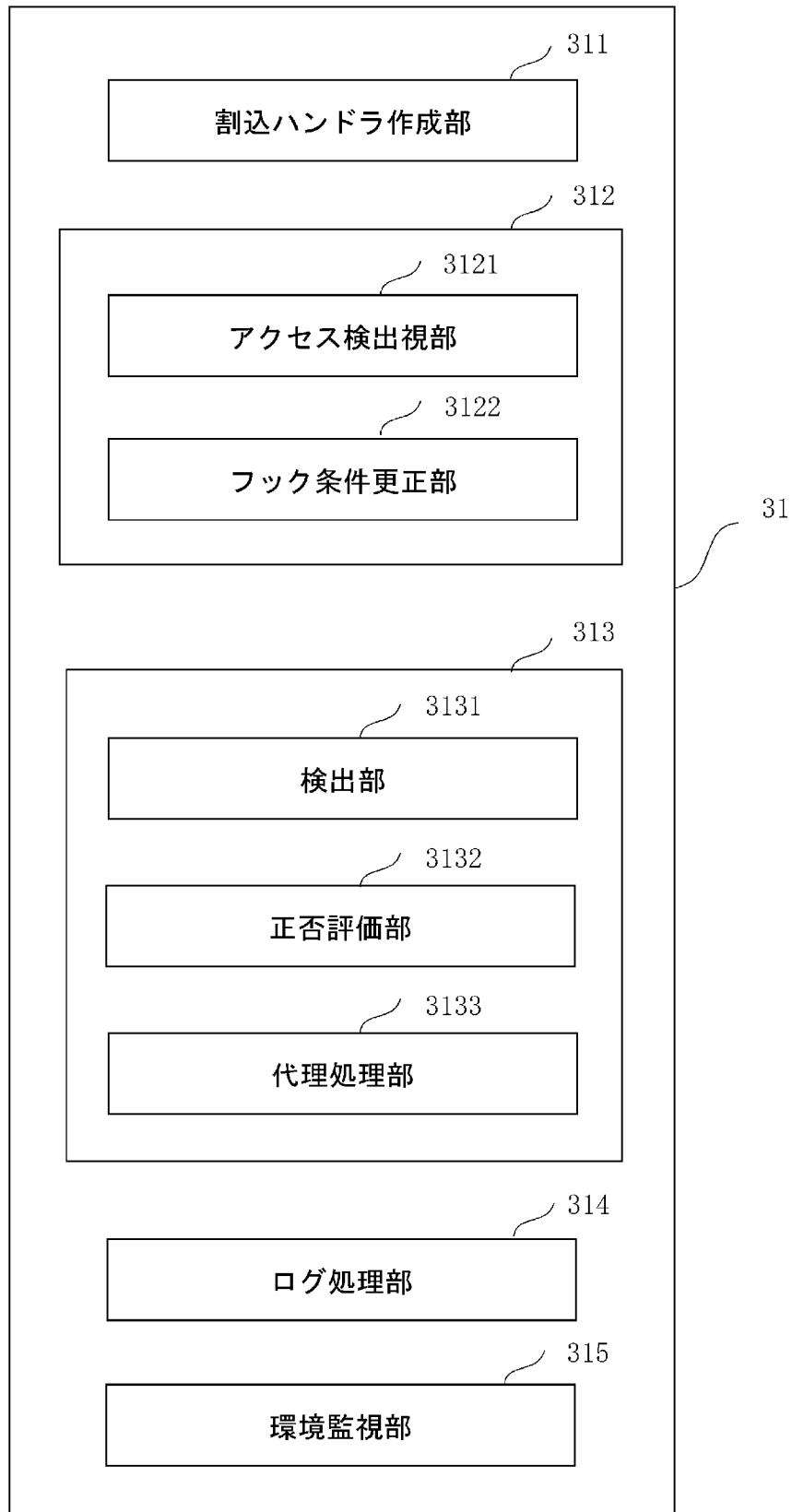
[図2]



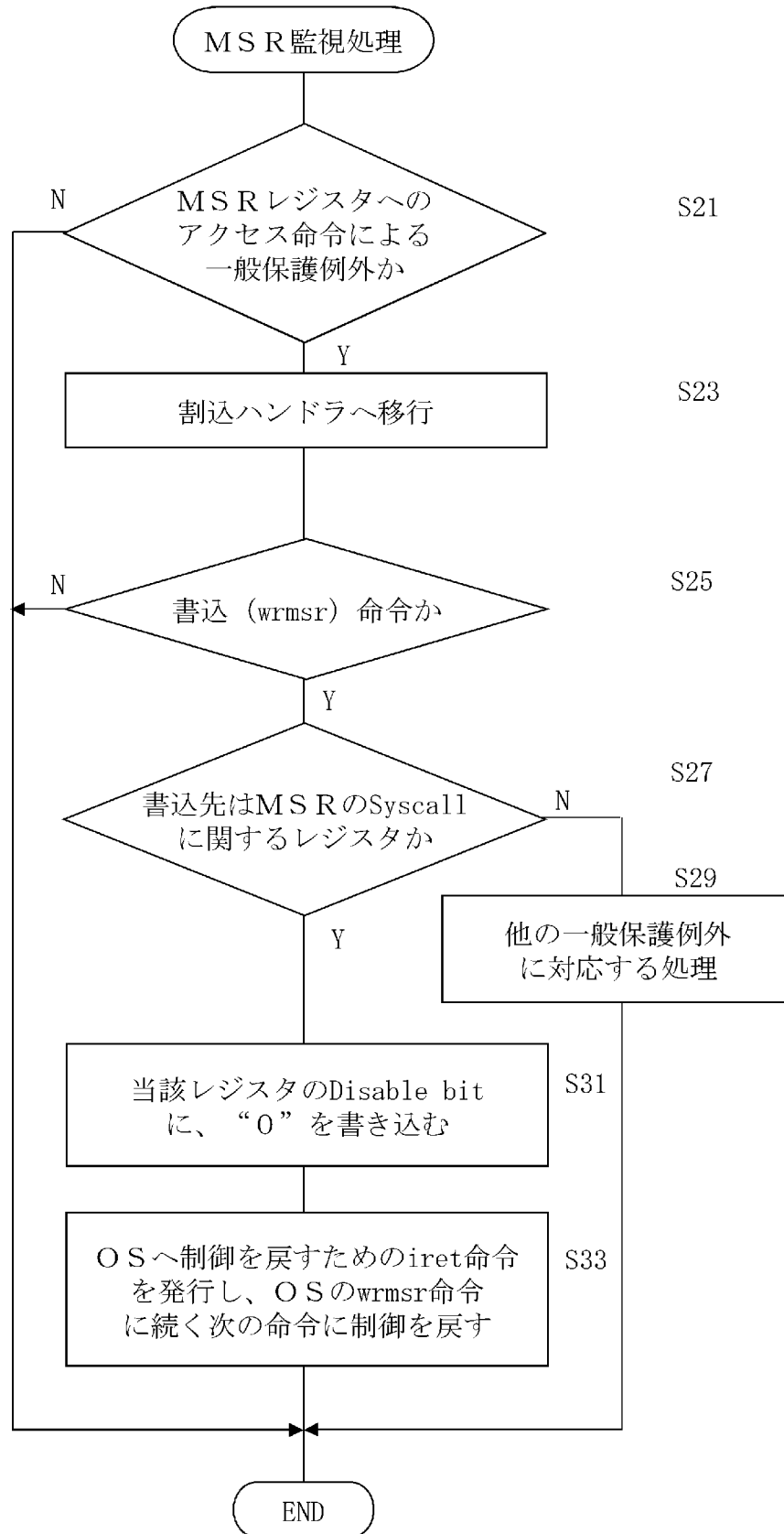
[図3]

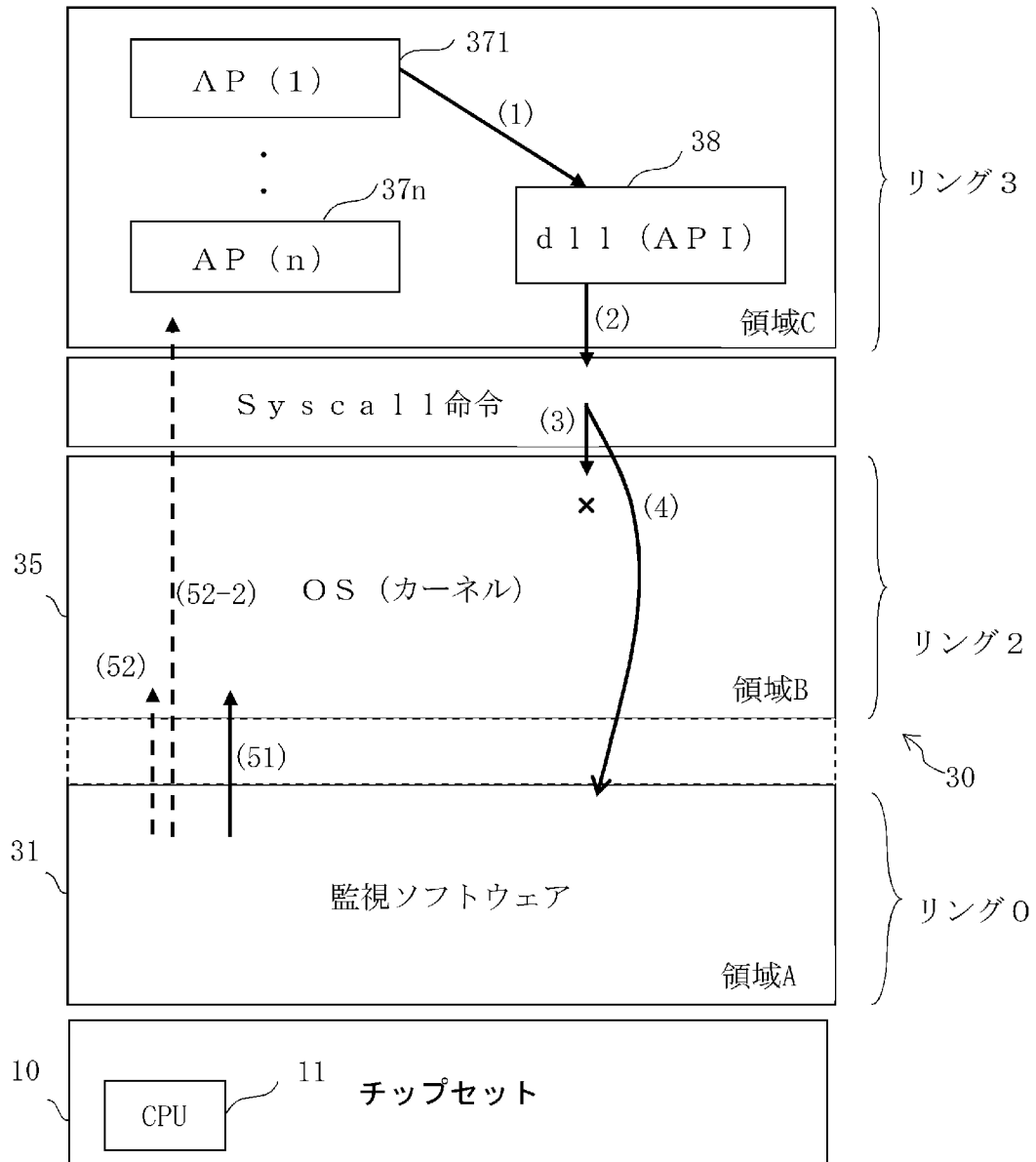


[図4]

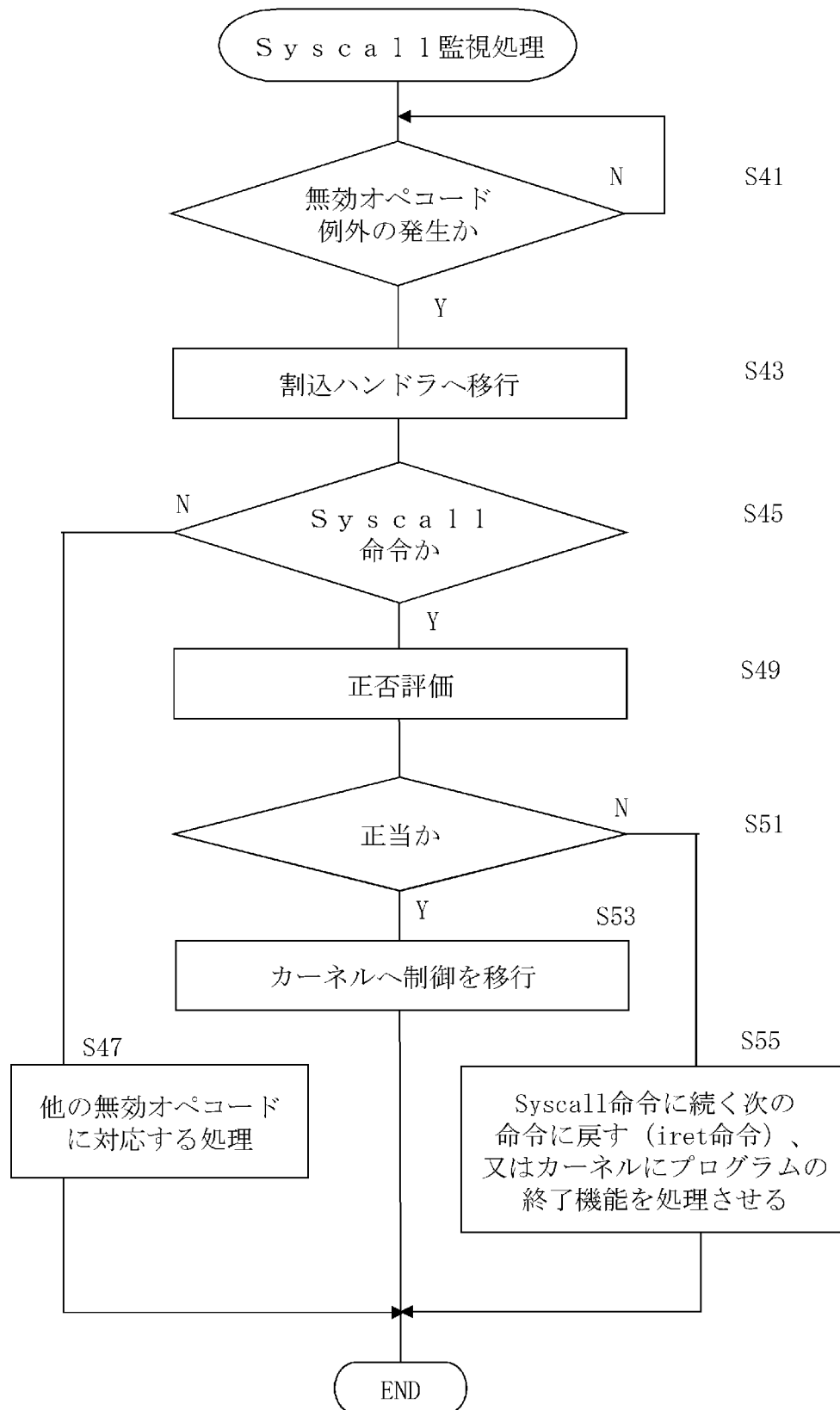


[図5]

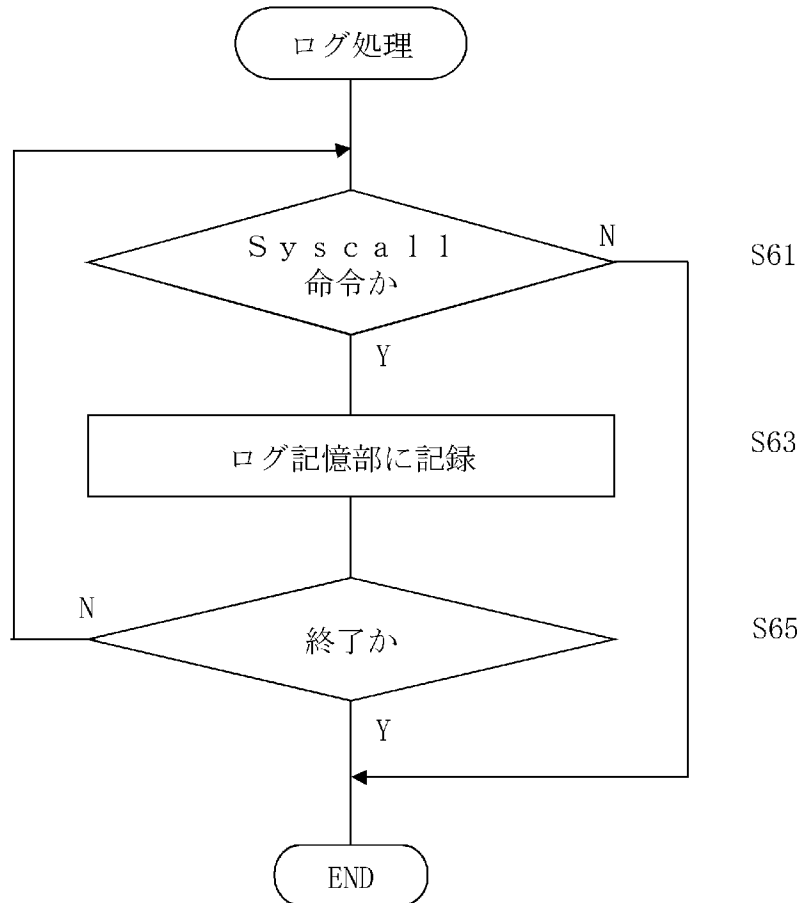




[図7]



[図8]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2015/063975

A. CLASSIFICATION OF SUBJECT MATTER

G06F11/30(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)

G06F11/30

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	1996-2015
Kokai Jitsuyo Shinan Koho	1971-2015	Toroku Jitsuyo Shinan Koho	1994-2015

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.
X	US 7996836 B1 (SYMANTEC CORP.), 09 August 2011 (09.08.2011), column 3, line 38 to column 4, line 26; column 6, lines 29 to 43; column 7, line 59 to column 8, line 36 (Family: none)	1-2, 5-6, 11-13 3-4, 7-10
Y	Tatsuya TAKEHISA, "AES-NI Meirei ni Taisuru Reigai Shori Kogeki no Malware Kaiseki eno Oyo", 2014 Nen Symposium on Cryptography and Information Security Gaiyoshu, The Institute of Electronics, Information and Communication Engineers, 24 January 2014 (24.01.2014), pages 1 to 8	3

☒ 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 August 2015 (06.08.15)

Date of mailing of the international search report
18 August 2015 (18.08.15)

Name and mailing address of the ISA/
Japan Patent Office
3-4-3, Kasumigaseki, Chiyoda-ku,
Tokyo 100-8915, Japan

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2015/063975

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	Koichi ONOUE, "VMM-based Architecture for Protecting Application Data", Symposium on Advanced Computing Systems and Infrastructures SACSIS2009 Ronbunshu, vol.2009, no.5, Information Processing Society of Japan, 21 May 2009 (21.05.2009), pages 189 to 197	4
Y	Takuya YOSHIMURA, "System call hook method for analyzing behavior of malware by virtual machine monitor", Dai 72 Kai (Heisei 22 Nen) Zenkoku Taikai Koen Ronbunshu (3) Network Security, Information Processing Society of Japan, 08 March 2010 (08.03.2010), 3-609 to 3-610	7-8
Y	Shin'etsu IZAWA, "Kasoka no Standard wa Cloud e Keiryo Secure na Hypervisor Xen", ASCII. technologies, 24 March 2010 (24.03.2010), vol.15, no.5, pages 48 to 57	9-10

A. 発明の属する分野の分類（国際特許分類（I P C））

Int.Cl. G06F11/30(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. G06F11/30

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	1 9 2 2 - 1 9 9 6 年
日本国公開実用新案公報	1 9 7 1 - 2 0 1 5 年
日本国実用新案登録公報	1 9 9 6 - 2 0 1 5 年
日本国登録実用新案公報	1 9 9 4 - 2 0 1 5 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 請求項の番号
X	US 7996836 B1 (SYMANTEC CORPORATION)	1-2, 5-6,
Y	2011.08.09, 第3欄第38-第4欄第26行、第6欄第29-43 行、第7欄第59行-第8欄第36行（ファミリーなし）	11-13
Y	竹久 達也, AES-NI 命令に対する例外処理攻撃のマルウェア 解析への応用, 2014年 暗号と情報セキュリティシンポジウム 概要集, 電子情報通信学会, 2014.01.24, 第1-8頁	3-4, 7-10
		3

☒ 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

0 6 . 0 8 . 2 0 1 5

国際調査報告の発送日

1 8 . 0 8 . 2 0 1 5

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 1 0 0 - 8 9 1 5

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）

衣川 裕史

5 B

9 5 5 7

電話番号 0 3 - 3 5 8 1 - 1 1 0 1 内線 3 5 4 5

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 請求項の番号
Y	尾上 浩一, アプリケーションデータを保護するためのVMMに基づくアーキテクチャ, 先進的計算基盤システムシンポジウム SACSIS 2009 論文集, 第2009巻 第5号, 社団法人情報処理学会, 2009.05.21, 第189-197頁	4
Y	吉村 拓也, マルウェア解析のための仮想計算機モニタを用いたシステムコールフック手法, 第72回(平成22年)全国大会講演論文集(3) ネットワーク セキュリティ, 社団法人情報処理学会, 2010.03.08, 3-609-3-610	7-8
Y	井澤 信悦, 仮想化のスタンダードはクラウドへ 軽量・セキュアなハイパーバイザー Xen, 月刊アスキーdotテクノロジーズ, 2010.03.24, 第15巻 第5号, 第48-57頁	9-10