(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6498413号
(P6498413)
(45)発行日　平成31年4月10日(2019.4.10)　(24)登録日　平成31年3月22日(2019.3.22)

(51)Int.Cl.　　F I
G06F 21/55 (2013.01)　　G06F 21/55
G06F 11/34 (2006.01)　　G06F 11/34　166

請求項の数 11　(全 14 頁)

(21)出願番号　特願2014-213038(P2014-213038)
(22)出願日　平成26年10月17日(2014.10.17)
(65)公開番号　特開2016-81348(P2016-81348A)
(43)公開日　平成28年5月16日(2016.5.16)
審査請求日　平成29年9月5日(2017.9.5)

(73)特許権者　399035766
エヌ・ティ・ティ・コミュニケーションズ株式会社
東京都千代田区大手町二丁目３番１号
(73)特許権者　507351506
株式会社ＦＦＲＩ
東京都渋谷区恵比寿１丁目１８番１８号
(74)代理人　100107766
弁理士　伊東　忠重
(74)代理人　100070150
弁理士　伊東　忠彦
(74)代理人　100192636
弁理士　加藤　隆夫
(74)代理人　100124844
弁理士　石原　隆治

最終頁に続く

(54)【発明の名称】情報処理システム、情報処理装置、制御サーバ、生成サーバ、動作制御方法及び動作制御プログラム

(57)【特許請求の範囲】
【請求項１】
一以上の情報処理装置を有し、一以上の装置と通信する情報処理システムであって、
プログラムの動作の異常を検出する異常検出手段と、
前記異常検出手段により異常が検出された際に、メモリの記憶内容をメモリダンプ情報に出力する出力手段と、
前記メモリダンプ情報に基づいて、前記異常の要因となる攻撃の特徴を示す特徴情報を抽出する解析手段と、
特徴情報に基づきブロックリストを生成する生成手段と、
前記ブロックリストに基づいて、当該情報処理システムの動作を制御する制御手段と、
を有する情報処理システム。
【請求項２】
前記装置と通信を行う通信手段を有し、
前記制御手段は、前記ブロックリストに含まれる特徴情報と前記通信手段が通信するパケットとを比較し、前記装置が攻撃元の装置であると判断する場合に、前記装置との通信を遮断する、
請求項１に記載の情報処理システム。
【請求項３】
複数の前記情報処理装置で前記ブロックリストを共有するために、前記ブロックリストを配信する配信手段を有する、請求項１又は２に記載の情報処理システム。

【請求項４】
特徴情報の入力を受け付ける入力手段を有し、
前記生成手段は、前記入力手段により受け付けた特徴情報に基づき前記ブロックリストを生成する、請求項１乃至３のいずれか一項に記載の情報処理システム。
【請求項５】
メモリの動作又は通信を監視することでプログラムに対する攻撃を検出する攻撃検出手段と、
前記攻撃検出手段により攻撃が検出された場合に、プログラムの動作の異常を発生させる異常発生手段を有する、請求項１乃至４のいずれか一項に記載の情報処理システム。
【請求項６】
一以上の情報処理装置を有し、一以上の装置と通信する情報処理システムであって、
プログラムの動作の異常を検出する異常検出手段と、
前記異常検出手段により異常が検出された際に、メモリの記憶内容をメモリダンプ情報に出力する出力手段と、
前記メモリダンプ情報を解析することで得られる、前記異常の要因となる攻撃の特徴を示す特徴情報の入力を受け付ける入力手段と、
前記特徴情報に基づきブロックリストを生成する生成手段と、
前記ブロックリストに基づいて、当該情報処理システムの動作を制御する制御手段と、
を有する情報処理システム。
【請求項７】
一以上の装置と通信する情報処理装置であって、
プログラムの動作の異常を検出する異常検出手段と、
前記異常検出手段により異常が検出された際に、メモリの記憶内容をメモリダンプ情報に出力する出力手段と、
前記メモリダンプ情報を送信する送信手段と、
前記異常の要因となる攻撃の特徴を示す特徴情報であって、前記メモリダンプ情報に基づいて抽出される特徴情報を含むブロックリストを受信する受信手段と、
受信した前記ブロックリストに基づいて、当該情報処理装置の動作を制御する制御手段と、
を有する情報処理装置。
【請求項８】
一以上の装置と通信する情報処理装置と生成サーバとに接続される解析サーバであって、
前記情報処理装置から、前記情報処理装置のメモリの記憶内容が出力されたメモリダンプ情報を受信する受信手段と、
前記メモリダンプ情報に基づいて、前記情報処理装置が有するプログラムの動作の異常の要因となる攻撃の特徴を示す特徴情報を抽出する解析手段と、
前記特徴情報を、前記生成サーバに送信する送信手段と、
を有する解析サーバ。
【請求項９】
情報処理装置と解析サーバとに接続される生成サーバであって、
前記解析サーバから、プログラムの動作の異常の要因となる攻撃の特徴を示す特徴情報であって、前記情報処理装置のメモリの記憶内容が出力されたメモリダンプ情報に基づき抽出された特徴情報を受信する受信手段と、
前記特徴情報に基づきブロックリストを生成する生成手段と、
前記ブロックリストを前記情報処理装置に送信する送信手段と、
を有する生成サーバ。
【請求項１０】
一以上の装置と通信し、一以上の情報処理装置を有する情報処理システムの動作制御方法であって、

プログラムの動作の異常を検出する異常検出ステップと、
前記異常検出ステップにより異常が検出された際に、メモリの記憶内容をメモリダンプ情報に出力する出力ステップと、
前記メモリダンプ情報に基づいて、前記異常の要因となる攻撃の特徴を示す特徴情報を抽出する解析ステップと、
前記特徴情報に基づきブロックリストを生成する生成ステップと、
前記ブロックリストに基づいて、当該情報処理システムの動作を制御する制御ステップと、
を有する動作制御方法。
【請求項１１】
一以上の装置と通信する情報処理装置の動作制御プログラムであって、
情報処理装置に、
メモリの動作又は通信を監視することでプログラムに対する攻撃を検出する攻撃検出ステップと、
前記攻撃検出ステップにより攻撃が検出された場合、当該情報処理装置にメモリダンプ情報を生成させるために、プログラムの動作の異常を発生させる異常発生ステップと、
前記メモリダンプ情報を解析することで得られる、前記異常の要因となる攻撃の特徴を示す特徴情報の入力を受け付ける入力ステップと、
前記特徴情報に基づきブロックリストを生成する生成ステップと、
前記ブロックリストに基づいて、当該情報処理装置の動作を制御する制御ステップと、
を実行させるための動作制御プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、情報処理システム、情報処理装置、制御サーバ、生成サーバ、動作制御方法及び動作制御プログラムに関するものである。
【背景技術】
【０００２】
プログラムの実行中に異常動作（クラッシュ）が発生した際、メモリに記憶されている情報を出力することでメモリダンプを収集し、収集したメモリダンプを解析することで、プログラムに潜むバグや脆弱性などの不具合を特定することが一般的に行われている。これにより、特定された不具合の情報を基にプログラムを改修し、修正プログラム（パッチプログラム）を配布することが可能になり、より信頼性の高いプログラムにアップデートすることができる。
【０００３】
ここで、コンピュータに侵入して不正に情報を取得するといった行為や、コンピュータを停止させる等の、いわゆるサイバー攻撃が行われる場合、このようなプログラムの不具合を狙われることが多い。したがって、プログラムのアップデートは、プログラムの異常動作の防止のみならず、コンピュータに対する攻撃の防御策としても有効である。
【０００４】
このようなコンピュータに対する攻撃を検出する技術として、例えば、バッファオーバーフロー攻撃に関する不正アクセスを検出する技術が開示されている（例えば、特許文献１）。
【先行技術文献】
【特許文献】
【０００５】
【特許文献１】特許第４５７２２５９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、修正プログラムを配布するまでには、攻撃により発生したプログラムの不具合を特定、特定した不具合を修正するための修正プログラムを作成、及び不具合が正しく解消されているかの検証に至る一連の工程を踏む必要がある。従って、攻撃が検出されてから修正プログラムが配布及び適用されるまでに一定の時間を要するため、その間はコンピュータに対する攻撃を防止することができず、攻撃対象が拡大してしまうという問題がある。

【０００７】

本発明は、上記に鑑みてなされたもので、修正プログラムを適用することなく、コンピュータに対する攻撃を防御する技術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】

【０００８】

本発明の実施の形態に係る情報処理システムは、一以上の情報処理装置を有し、一以上の装置と通信する情報処理システムであって、プログラムの動作の異常を検出する異常検出手段と、前記異常検出手段により異常が検出された際に、メモリの記憶内容をメモリダンプ情報に出力する出力手段と、前記メモリダンプ情報に基づいて、前記異常の要因となる攻撃の特徴を示す特徴情報を抽出する解析手段と、特徴情報に基づきブロックリストを生成する生成手段と、前記ブロックリストに基づいて、当該情報処理システムの動作を制御する制御手段と、を有する。

【発明の効果】

【０００９】

本発明に係る実施の形態によれば、修正プログラムを適用することなく、コンピュータに対する攻撃を防御することが可能になる。

【図面の簡単な説明】

【００１０】

【図１】第一の実施の形態に係る情報処理システムの概要を示す図である。

【図２】第一の実施の形態に係る情報処理システムの動作手順の概要を示す図である。

【図３】第一の実施の形態に係る情報処理装置のハードウェア構成の一例を示す図である。

【図４】第一の実施の形態に係る情報処理システムの機能構成の一例を示す図である。

【図５】ブロックリストの一例及び制御手段の動作の一例を示す図である。

【図６】第二の実施の形態に係る情報処理システムの動作手順の概要を示す図である。

【図７】第二の実施の形態に係る情報処理システムの機能構成の一例を示す図である。

【発明を実施するための形態】

【００１１】

以下、図面を参照して実施の形態について説明する。各図面において、同一構成部分には同一符号を付し、重複した説明を省略する場合がある。なお、以下で説明する実施の形態は一例に過ぎず、本発明が適用される実施の形態は、以下の実施の形態に限られるわけではない。

＜＜第一の実施の形態＞＞

（概要）

図１は、第一の実施の形態に係る情報処理システムの概要を示す図である。第一の実施の形態に係る情報処理システム１０は、外部ネットワークと接続されており、外部ネットワークの先に存在する装置（図示せず）から要求を受け付けることで処理を行う情報処理装置２０ａ及び情報処理装置２０ｂと、プログラムに発生する異常を解析する解析サーバ３０と、情報処理装置２０に対する攻撃を検出するための情報が含まれるブロックリストを生成するブロックリスト生成サーバ４０と、から構成されている。

【００１２】

また、情報処理システム１０において、情報処理装置２０ａと、情報処理装置２０ｂと、解析サーバ３０と、ブロックリスト生成サーバ４０とは、相互に通信可能なように構成されている。情報処理システム１０に含まれる情報処理装置２０は１台であってもよく、

３台以上であってもよい。以下、「情報処理装置２０ａ」及び「情報処理装置２０ｂ」のうち任意の情報処理装置２０は、「情報処理装置２０」と表す。

【００１３】

図２は、第一の実施の形態に係る情報処理システムの動作手順の概要を示す図である。図１及び図２を参照しながら第一の実施の形態に係る情報処理システム１０の動作の概要を説明する。情報処理装置２０ａが、外部ネットワークの先に存在する装置（以下、「外部装置」という）と通信することで所定の処理を行っている前提で、動作の概要を説明する。

【００１４】

まず、情報処理装置２０ａがバッファオーバーフローを引き起こすような不正パケットが、外部装置から情報処理装置２０ａに対して送信されたとする。情報処理装置２０ａがこの不正パケットに対する脆弱性を含んでいる場合、情報処理装置２０ａにインストールされたプログラムが異常処理を引き起こしてクラッシュ（動作停止）することがある。

【００１５】

情報処理装置２０ａは、プログラムがクラッシュしたことを検出すると（Ｓ１０１）、クラッシュした際のメモリの内容をファイル化したメモリダンプ情報を出力し（Ｓ１０２）、解析サーバ３０に送信する。

【００１６】

解析サーバ３０は、メモリダンプ情報を解析することで、メモリダンプ情報にプログラムがクラッシュした原因となる攻撃コードや、不正パケットの送信元である外部装置のＵＲＬといった、プログラムがクラッシュする要因となる攻撃の特徴を示す特徴情報（以下「特徴情報」という）が含まれていないかを特定する（Ｓ１０３）。

【００１７】

解析サーバ３０は、特定された特徴情報をブロックリスト生成サーバ４０に送信する。ブロックリスト生成サーバ４０は、受信した特徴情報に基づいてブロックリストを生成し（Ｓ１０４）、情報処理装置２０ａに送信する。

【００１８】

情報処理装置２０ａは、外部装置との通信パケットとブロックリストに含まれる特徴情報とを比較し、外部装置との通信パケットが不正パケットであると判断する場合、外部装置との通信を遮断するように動作する（Ｓ１０５）。これにより、情報処理装置２０ａは、アプリケーションプログラムに対して修正プログラムを適用することなく、再度同様の不正パケットを受信した場合でも、プログラムのクラッシュを免れることができる。

【００１９】

なお、ブロックリスト生成サーバ４０は、ブロックリストを、情報処理装置２０ａに加えて、情報処理装置２０ｂにも送信するようにしてもよい。これにより、情報処理装置２０ｂは、上記不正パケットによる攻撃を防御することが可能になる。すなわち、情報処理装置２０ａに対する攻撃により得られた知見を、多数のコンピュータに活用することができる。

【００２０】

なお、情報処理装置２０は、プログラムに従って動作する装置であれば種類を問わない。例えば、情報処理装置２０は、ＰＣ（Personal Computer）、サーバ、携帯端末、又はタブレット端末等であってもよいし、L2/L3スイッチ、又はルータ等のネットワーク機器であってもよい。

（ハードウェア構成）

図３は、第一の実施の形態に係る情報処理装置のハードウェア構成の一例を示す図である。情報処理装置２０は、ＣＰＵ２０１と、ＲＯＭ２０２と、ＲＡＭ２０３と、ＨＤＤ２０４と、操作部２０５と、表示部２０６と、ドライブ装置２０７と、ＮＩＣ（Network Interface card）２０８とを有する。

【００２１】

ＣＰＵ２０１は、情報処理装置２０の全体制御を行うプロセッサである。ＣＰＵ２０１

、ＨＤＤ２０４等に記憶されたオペレーティングシステム、アプリケーション、各種サービス等のプログラムを実行し、情報処理装置２０の各機能を実現する。ＲＯＭ２０２には、各種のプログラムやプログラムによって利用されるデータ等が記憶される。ＲＡＭ２０３は、プログラムをロードするための記憶領域や、ロードされたプログラムのワーク領域等として用いられる。ＨＤＤ２０４には、各種情報及びプログラム等が記憶される。

【００２２】

操作部２０５は、ユーザからの入力操作を受け付けるためのハードウェアであり、例えばキーボード又はマウスである。表示部２０６は、ユーザに向けた表示を行うハードウェアである。

【００２３】

ドライブ装置２０７は、プログラムを記録した記憶媒体２０９からプログラムを読み取る。ドライブ装置２０７によって読み取られたプログラムは、例えば、ＨＤＤ２０４にインストールされる。ＮＩＣ２０８は、情報処理装置２０をネットワークに接続し、データの送受信を行うための通信インタフェースである。

【００２４】

なお、記憶媒体２０９とは、非一時的（non-transitory）な記憶媒体を言う。記憶媒体２０９の例としては、磁気記憶媒体、光ディスク、光磁気記憶媒体、不揮発性メモリなどがある。

【００２５】

解析サーバ３０及びブロックリスト生成サーバ４０のハードウェア構成は、図３と同一であるため説明は省略する。

（機能構成）

図４は、第一の実施の形態に係る情報処理システムの機能構成の一例を示す図である。まず、図４を用いて、情報処理装置２０の機能構成について説明する。図４に示すように、第一の実施の形態に係る情報処理装置２０は、通信手段３０１、異常検出手段３０２、出力手段３０３、制御手段３０４、及びブロックリスト管理手段３０５を備える。なお、図４は、第一の実施の形態に特に関係する機能を示すものであり、例えばＷｅｂクライアント機能のように、本願発明に係る実施の形態とは関係が低い機能については図示していない。

【００２６】

これらの各手段は、各手段の処理内容を記述したプログラムを情報処理装置２０に実行させることにより実現可能である。すなわち、これらの各手段は、情報処理装置２０に内蔵されるＣＰＵ２０１、ＲＯＭ２０２、ＲＡＭ２０３、及びＨＤＤ２０４などのハードウェア資源を用いて、各手段で実施される処理に対応するプログラムを実行することにより実現することが可能である。上記プログラムは、コンピュータが読取り可能な記憶媒体２０９等に記録して、保存したり、配布したりすることが可能である。また、上記プログラムをインターネットなど、ネットワークを通じて提供することも可能である。

【００２７】

通信手段３０１は、外部装置、解析サーバ３０、及びブロックリスト生成サーバ４０との間でパケットを送受信する。

【００２８】

異常検出手段３０２は、情報処理装置２０で動作しているプログラムを監視し、プログラムに発生する異常を検出する。プログラムに発生する異常としては、例えば、動作中のプログラムが、アクセスが許可されていないメモリ領域を参照しようとした場合、動作中のプログラムが０で割算をしようとした場合など、プログラムがそれ以上動作を継続することが出来ない状態があげられる。またプログラムは動作しているものの、無限ループやデッドロック状態に陥っている状態などがあげられる。

【００２９】

このような状態に至る要因は様々であるが、異常検出手段３０２は、特定の要因に限らず、プログラムに発生する異常を検出する。また、異常検出手段３０２が異常を検出する

手段は問わない。例えば、ＣＰＵ２０１が備えるエラー検出機能を利用することで異常を検出するようにしてもよいし、ＯＳ（Operating System）のカーネルが備えるエラー検出機能を利用することで異常を検出するようにしてもよい。

【００３０】

出力手段３０３は、異常検出手段３０２からの指示により、ＲＡＭ２０３に記憶されている内容をファイルに書き出すことで、メモリダンプ情報を出力する。出力手段３０３は、出力したメモリダンプ情報を、通信手段３０１を介して解析サーバ３０に送信する。メモリダンプ情報とは、ある瞬間のメインメモリに記憶されている内容をファイルに書き出したものであり、主に、プログラムの不具合を解析する目的で使用される。

【００３１】

なお、出力手段３０３は、メインメモリに記憶されている内容全てをファイルに書き出すようにしてもよいし、メインメモリの特定領域の内容に限定してファイルに書き出すようにしてもよい。また、メインメモリに記憶されている内容そのものに限らず、問題解析に役立つ情報である、メモリの内容を間接的に示す情報（プログラムに異常が発生したメモリの番地、メモリに記憶された値のハッシュ値など）をファイルに書き出すようにしてもよい。また、出力手段３０３は、メインメモリに限らず、例えば、仮想メモリとして利用しているＨＤＤ２０４の領域や、その他プログラムが利用している外部記憶装置に記憶されている内容をファイルに書き出すようにしてもよい。

【００３２】

また、出力手段３０３は、ＯＳに予め実装されている、メモリダンプ情報を出力する機能を利用するようにしてもよい。

【００３３】

ブロックリスト管理手段３０５は、ブロックリスト管理サーバから受信したブロックリストを、ＲＡＭ２０３又はＨＤＤ２０４に保存すると共に、必要に応じて読出し及び更新を行う。

【００３４】

制御手段３０４は、ブロックリストを用いることで、外部装置からの攻撃を防御する。

【００３５】

図５は、ブロックリストの一例及び制御手段３０４の動作の一例を示す図である。ここで、図５を用いて、制御手段３０４の動作例（その１）について説明する。

【００３６】

図５（ａ）は、ブロックリストに格納されている情報の一例である。ブロックリストには、攻撃元である外部装置のＵＲＬを示す文字列、及び、攻撃コード（exploit code）のバイト列が格納されている。攻撃コードとは、ソフトウェアの脆弱性を攻撃するように作成された、スクリプトやプログラムである。

【００３７】

図５（ｂ）は、情報処理装置２０にインストールされたウェブブラウザが、インターネットを介してウェブサーバにアクセスする様子を表している。制御手段３０４は、情報処理装置２０の中に、ソフトウェアで実現される仮想的なＰｒｏｘｙを設置し、ウェブブラウザがウェブサーバにアクセスする際、仮想的なＰｒｏｘｙを経由してアクセスさせるようにする。仮想的なＰｒｏｘｙは、ウェブブラウザとウェブサーバとの間で送受信されるパケットを監視し、送受信されるパケットと、ブロックリストに格納されているＵＲＬ又は攻撃コードとを比較する。ウェブブラウザのアクセス先が、ブロックリストに格納されているＵＲＬが示すアクセス先と一致する場合、Ｐｒｏｘｙは、例えばパケットを破棄することで、ウェブブラウザに当該アクセス先にアクセスさせないようにする。これにより、ウェブブラウザが、不正な外部装置にアクセスするのを防止することができる。また、ウェブサーバから受信したパケットのバイト列と、ブロックリストに格納されている攻撃コードのバイト列が一致した場合、Ｐｒｏｘｙは、例えばパケットを破棄する。これにより、攻撃パケットが情報処理装置２０の内部に侵入するのを防止することができる。

【００３８】

制御手段３０４の動作例（その２）について説明する。例えば、指定されたＵＲＬからファイルをダウンロードするようなアプリケーションプログラムにおいて、ＯＳ等が提供しているファイルダウンロード用のＡＰＩが使用される場合がある。そこで、アプリケーションプログラムが当該ＡＰＩをコールすると、当該ＡＰＩの代わりに予め用意した別のＡＰＩが動作するようにＡＰＩをフックする。予め用意した別のＡＰＩは、アプリケーションプログラムがアクセスしようとしているＵＲＬと、ブロックリストに格納されているＵＲＬが一致するかを比較し、一致する場合はファイルをダウンロードしないように動作する。これにより、アプリケーションプログラムが不正なサーバからファイルをダウンロードするのを未然に防止することができる。

【００３９】

なお、制御手段３０４は、上記動作例に示す機能に限定されるものではない。ブロックリストを用いて、外部装置からの攻撃を防御することができれば、他の機能も適用できる。また、外部装置からの攻撃の防御に限らず、バグ等に起因する情報処理装置２０の誤作動を防止する機能を含むようにしてもよい。

【００４０】

次に、図４を用いて、解析サーバ３０の機能構成について説明する。図４に示すように、第一の実施の形態に係る解析サーバ３０は、通信手段３１１、解析手段３１２、及び表示手段３１３を備える。

【００４１】

これらの各手段は、各手段の処理内容を記述したプログラムを解析サーバ３０に実行させることにより実現可能である。すなわち、これらの各手段は、解析サーバ３０に内蔵されるＣＰＵ２０１、ＲＯＭ２０２、ＲＡＭ２０３、及びＨＤＤ２０４などのハードウェア資源を用いて、各手段で実施される処理に対応するプログラムを実行することにより実現することが可能である。上記プログラムは、コンピュータが読取り可能な記憶媒体２０９等に記録して、保存したり、配布したりすることが可能である。また、上記プログラムをインターネットなど、ネットワークを通じて提供することも可能である。

【００４２】

通信手段３１１は、情報処理装置２０、及びブロックリスト生成サーバ４０との間でパケットを送受信する。

【００４３】

解析手段３１２は、メモリダンプ情報を解析することで、特徴情報が含まれていないかを特定する。例えば、悪意のあるコードを含むソフトウェアであるマルウェア（malicious software）は、搾取した情報の送信先サーバのＵＲＬをプログラムコード内に含むことがある。このようなマルウェアの動作によりアプリケーションプログラム等で異常が発生した場合、当該ＵＲＬがメモリダンプ情報に含まれる。従って、メモリダンプ情報を解析することで、当該ＵＲＬを抽出することができる。また、メモリダンプ情報から、異常を引き起こすきっかけになった攻撃コード（exploit code）を抽出するようにしてもよい。解析手段３１２は、上記手段により得られたＵＲＬ又は攻撃コードを、特徴情報として扱う。なお、解析手段３１２は、上記の方法により実現される機能に限定されるものではない。特徴情報を抽出する方法であれば、他の機能も適用できる。

【００４４】

解析手段３１２は、特徴情報を、通信手段３１１を介してブロックリスト生成サーバ４０に送信する。

【００４５】

表示手段３１３は、表示部２０６を介して、メモリダンプ情報又は特徴情報をユーザが視認できるように表示する。また、メモリダンプ情報の一部を抽出して表示するようにしてもよい。また、解析手段３１２により一部が解析されたメモリダンプ情報を表示するようにしてもよい。メモリダンプ情報から特徴情報を抽出する際、専門スキルを有するユーザによる詳細な分析により特徴情報が特定される場合もある。従って、表示手段３１３を備えることで、専門スキルを有するユーザが、メモリダンプ情報を用いて詳細な分析を行

うことが出来る。
【００４６】
次に、図４を用いて、ブロックリスト生成サーバ４０の機能構成について説明する。図４に示すように、第一の実施の形態に係るブロックリスト生成サーバ４０は、通信手段３２１、入力手段３２２、及び生成手段３２３を備える。
【００４７】
これらの各手段は、各手段の処理内容を記述したプログラムをブロックリスト生成サーバ４０に実行させることにより実現可能である。すなわち、これらの各手段は、ブロックリスト生成サーバ４０に内蔵されるＣＰＵ２０１、ＲＯＭ２０２、ＲＡＭ２０３、及びＨＤＤ２０４などのハードウェア資源を用いて、各手段で実施される処理に対応するプログラムを実行することにより実現することが可能である。上記プログラムは、コンピュータが読取り可能な記憶媒体２０９等に記録して、保存したり、配布したりすることが可能である。また、上記プログラムをインターネットなど、ネットワークを通じて提供することも可能である。
【００４８】
通信手段３２１は、解析サーバ３０、及び情報処理装置２０との間でパケットを送受信する。
【００４９】
入力手段３２２は、操作部２０５を介して、特徴情報の入力を受け付ける。専門スキルを有するユーザがメモリダンプ情報を解析することで得られた特徴情報を、ブロックリストに反映させることができる。
【００５０】
生成手段３２３は、一以上の特徴情報をまとめてファイル化することで、ブロックリストを生成する。また、生成手段３２３は、生成したブロックリストを、通信手段３２１を介して情報処理装置２０に送信する。
（効果）
以上、第一の実施の形態によれば、情報処理装置２０に修正プログラムを適用することなく、コンピュータに対する攻撃を防御することが可能になる。すなわち、修正プログラムの作成及び検証の完了を待つ必要がないため、コンピュータに対する攻撃を迅速に防御することが可能になる。
＜＜第二の実施の形態＞＞
次に、第二の実施の形態について図面に基づいて説明する。なお、第一の実施の形態と同一構成部分についての説明は省略する。また、特に言及しない点については、第一の実施の形態と同様でよい。
（概要）
図６は、第二の実施の形態に係る情報処理システムの動作手順の概要を示す図である。図６を参照しながら第一の実施の形態に係る情報処理システム１０の動作の概要を説明する。
【００５１】
第二の実施の形態に係る情報処理システム１０は、第一の実施の形態に係る情報処理システム１０が有する機能に加え、情報処理装置２０にインストールされたプログラムに対する攻撃を監視し（Ｓ１１１）、具体的な攻撃が検出された場合や、具体的な攻撃に至らないまでも不審な挙動が発見された場合に、意図的な例外処理（以下、「疑似クラッシュ」という）を発生させる機能を有する（Ｓ１１２）。このように、疑似クラッシュを発生させることで、第一の実施の形態に係る処理手順（Ｓ１０２乃至Ｓ１０５）を強制的に実行させる。これにより、プログラムのクラッシュを誘発しない攻撃に対しても、メモリダンプ情報を収集することによる情報解析を行うことが出来ると共に、ブロックリストによる防御を行うことが出来る。
（ハードウェア構成）
情報処理装置２０、解析サーバ３０、及びブロックリスト生成サーバ４０のハードウェ

ア構成は、図３と同一であるため説明は省略する。
（機能構成）
図７は、第二の実施の形態に係る情報処理システムの機能構成の一例を示す図である。図７を用いて、情報処理装置２０の機能構成について説明する。図７に示すように、第二の実施の形態に係る情報処理装置２０は、通信手段３０１、異常検出手段３０２、出力手段３０３、制御手段３０４、ブロックリスト管理手段３０５、攻撃検出手段、及び異常発生手段３０７を備える。なお、図７は、第二の実施の形態に特に関係する機能を示すものであり、例えば、Ｗｅｂクライアント機能のように、本願発明に係る実施の形態とは関係が低い機能については図示していない。
【００５２】
攻撃検出手段３０６は、外部装置との間で行われる通信又はメモリの動作を監視することで、情報処理装置２０に対する不審な挙動を検出する。例えば、下記（１）～（２）の手段又はこれらの手段の組み合わせにより、不審な挙動を検出することができる。なお、攻撃検出手段３０６は、下記の手段に限らない。情報処理装置２０に対する不審な挙動を検出することができる手段であれは、他の手段も適用できる。
【００５３】
また、例えば、電子商取引の不正注文等が発覚したような場合など、攻撃検出手段３０６は、ユーザの指示により、不審な挙動を検出したと判断するようにしてもよい。
【００５４】
（１）マルウェアである可能性が高いと判断できるような特徴的な文字列又はバイト列を、予めマルウェアを解析することで抽出しておき、これらの特徴的な文字列又はバイト列を含むファイル等が検出された場合、攻撃検出手段３０６は、情報処理装置２０にマルウェアが侵入していると判断することができる。
【００５５】
（２）実行中のプログラムが、自分自身のプログラムをファイルとして出力し、さらに出力したファイルを実行しようとした場合、そのプログラムはマルウェアであると考えられる。従って、このような動作を検出した場合、攻撃検出手段３０６は、情報処理装置２０にマルウェアが侵入していると判断することができる。
【００５６】
異常発生手段３０７は、情報処理装置２０の内部にて意図的な例外処理（疑似クラッシュ）を発生させる。例えば、異常発生手段３０７は、ゼロの割算を行うプログラムを起動させることで、強制的に例外処理を発生させることができる。また、異常発生手段３０７は、プログラムからはアクセス不可能なメモリ領域に値を書き込むことで、強制的に例外処理を発生させることができる。なお、例外処理を発生させる手段は上記の手段に限らない。意図的な例外処理を発生させることができれば、他の手段も適用できる。
（効果）
以上、第二の実施の形態によれば、情報処理装置２０に修正プログラムを適用することなく、コンピュータに対する攻撃を防御することが可能になる。すなわち、修正プログラムの作成及び検証の完了を待つ必要がないため、コンピュータに対する攻撃を迅速に防御することが可能になる。
【００５７】
また、一般的なＯＳは、例外発生を検出したタイミングでメモリダンプ情報を生成する機能を予め備えていることが多い。従って、第二の実施の形態によれば、ＯＳが備えている機能を用いてメモリダンプ情報を生成及び収集することができる。
【００５８】
また、第二の実施の形態によれば、アプリケーションプログラムのクラッシュを誘発しない攻撃に対しても、メモリダンプ情報を収集することによる解析を行うことが出来ると共に、ブロックリストによる防御を行うことが出来る。さらに、収集したメモリダンプ情報を解析することで、検出された不審な挙動に関する詳細な情報を収集することができ、未知の攻撃手法の発見に役立てることができる。

（実施の形態の補足）
なお、本発明の各実施の形態において、情報処理システム１０は、必ずしも情報処理装置２０、解析サーバ３０及びブロックリスト生成サーバ４０に分けて構成される必要は無い。例えば、解析サーバ３０及びブロックリスト生成サーバ４０が有する機能の一部を、情報処理装置２０に実装するようにしてもよい。また、情報処理装置２０に全ての機能を実装するようにしてもよい。

【００５９】
なお、本発明の各実施の形態において、情報処理装置２０、解析サーバ３０及びブロックリスト生成サーバ４０の一部又は全部を、クラウドサーバ上に実装するようにしてもよい。

【００６０】
なお、本発明の各実施の形態において、必ずしも解析サーバ３０が備える表示手段３１３、解析手段３１２、及び通信手段３１１を備えている必要は無い。例えば、解析サーバ３０が備える表示手段３１３、解析手段３１２、及び通信手段３１１を除いた情報処理システム１０を構築するようにしてもよい。メモリダンプ情報の解析及び特徴情報の抽出については、ＯＳのベンダ等が提供するサービスを利用するようにして、当該特徴情報に基づいた攻撃防御を行う情報処理システム１０を構築することができる。

【００６１】
以上、本発明は各実施の形態に限定されるものではなく、本発明の範囲内で種々の変形及び改良が可能である。

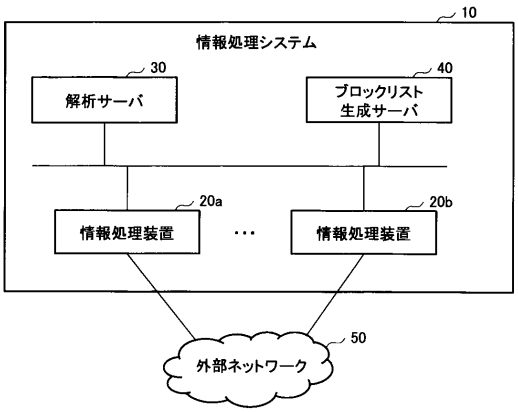
【００６２】
なお、各実施の形態において、通信手段３２１は、配信手段の一例である。攻撃元である外部装置のＵＲＬ及び攻撃コードは、特徴情報の一例である。ブロックリスト生成サーバは、生成サーバの一例である。

【符号の説明】

【００６３】
１０　情報処理システム
２０　情報処理装置
３０　解析サーバ
４０　ブロックリスト生成サーバ
５０　外部ネットワーク
３０１、３１１、３２１　通信手段
３０２　異常検出手段
３０３　出力手段
３０４　制御手段
３０５　ブロックリスト管理手段
３０６　攻撃検出手段
３０７　異常発生手段
３１２　解析手段
３１３　表示手段
３２２　入力手段
３２３　生成手段

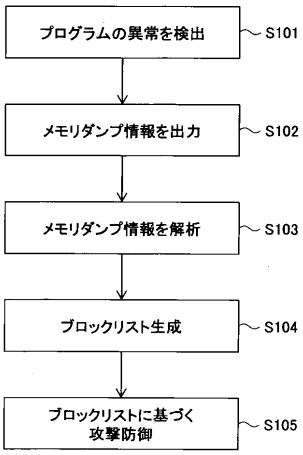
【図１】

第一の実施の形態に係る情報処理システムの概要を示す図



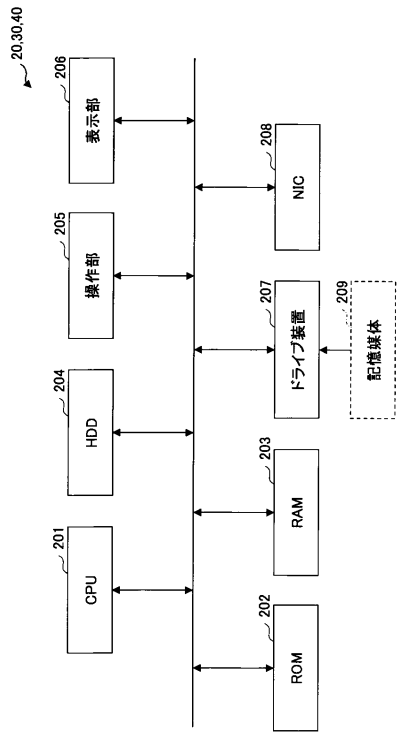
【図２】

第一の実施の形態に係る情報処理システムの動作手順の概要を示す図



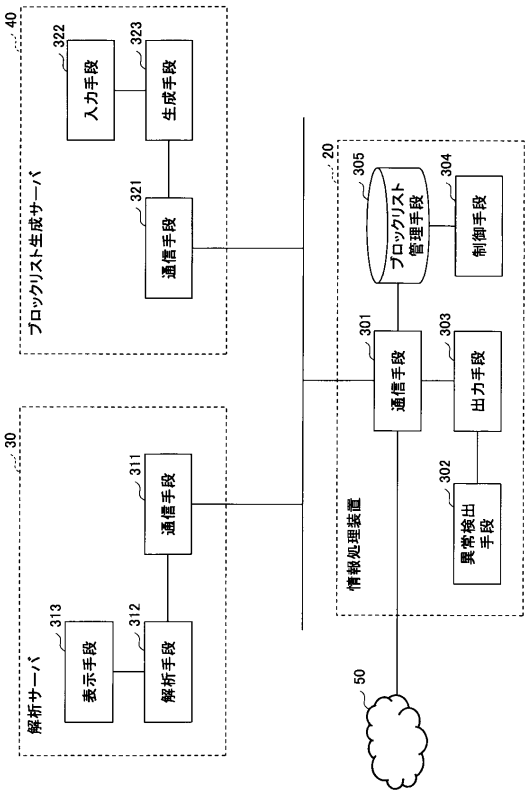
【図３】

第一の実施の形態に係る情報処理装置のハードウェア構成の一例を示す図



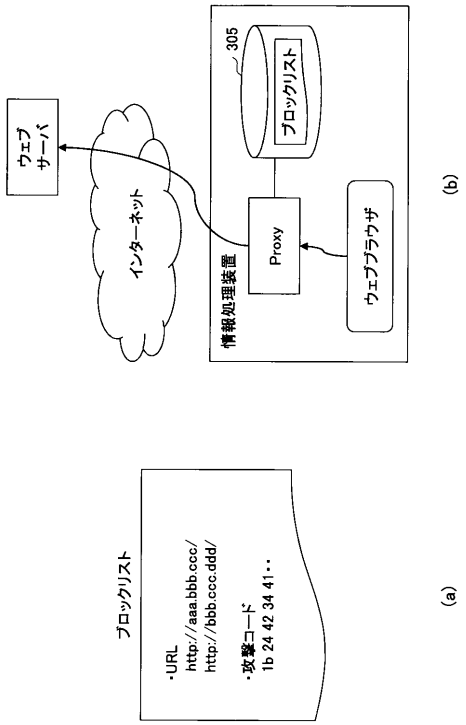
【図４】

第一の実施の形態に係る情報処理システムの機能構成の一例を示す図



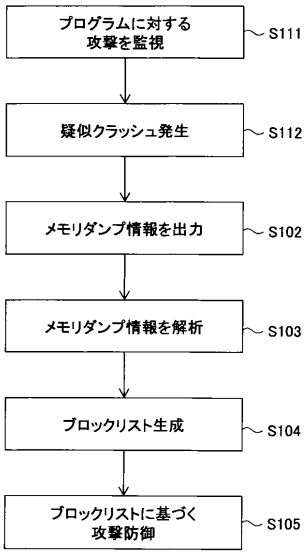
【図５】

ブロックリストの一例及び制御手段の動作の一例を示す図



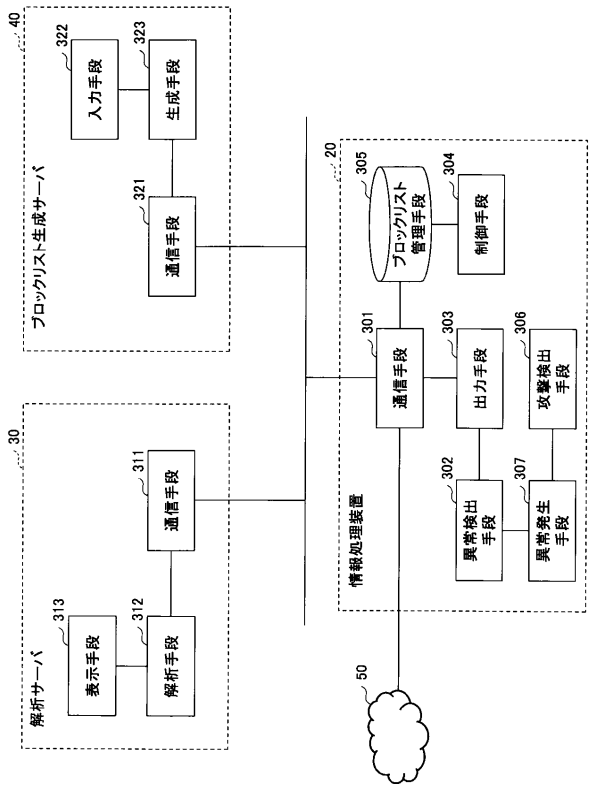
【図６】

第二の実施の形態に係る情報処理システムの動作手順の概要を示す図



【図７】

第二の実施の形態に係る情報処理システムの機能構成の一例を示す図



フロントページの続き

(72)発明者　小山　覚
東京都千代田区内幸町一丁目１番６号　エヌ・ティ・ティ・コミュニケーションズ株式会社内
(72)発明者　金居　良治
東京都渋谷区恵比寿１丁目１８番１８号　株式会社ＦＦＲＩ内

審査官　宮司　卓佳

(56)参考文献　特開２０１３－０１１９４９（ＪＰ，Ａ）
特開２００２－１８２９５１（ＪＰ，Ａ）
特開２０１０－１３４５３６（ＪＰ，Ａ）
特開２００６－２４３８７８（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／５５
Ｇ０６Ｆ　１１／３４