(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5878560号
(P5878560)
(45)発行日　平成28年3月8日(2016.3.8)　(24)登録日　平成28年2月5日(2016.2.5)

(51)Int.Cl.　　F I
G06F 21/56 (2013.01)　　G06F 21/56 360
G06F 21/53 (2013.01)　　G06F 21/53

請求項の数 5　(全 27 頁)

(21)出願番号　特願2013-550585 (P2013-550585)
(86)(22)出願日　平成24年1月19日 (2012.1.19)
(65)公表番号　特表2014-504765 (P2014-504765A)
(43)公表日　平成26年2月24日 (2014.2.24)
(86)国際出願番号　PCT/US2012/021916
(87)国際公開番号　WO2012/100088
(87)国際公開日　平成24年7月26日 (2012.7.26)
審査請求日　平成27年1月16日 (2015.1.16)
(31)優先権主張番号　13/011,344
(32)優先日　平成23年1月21日 (2011.1.21)
(33)優先権主張国　米国(US)

早期審査対象出願

(73)特許権者　513180200
ファイヤアイ　インク
アメリカ合衆国，カリフォルニア州　９５０３５，ミルピタス，１３９０　マッカーシー　ブールバード
(74)代理人　110001416
特許業務法人　信栄特許事務所
(72)発明者　スタニフォード　ステュアート　グレスリー
アメリカ合衆国，カリフォルニア州　９５０３５，ミルピタス，１３９０　マッカーシー　ブールバード

最終頁に続く

(54)【発明の名称】悪意あるＰＤＦネットワークコンテンツを検出するシステムおよび方法

(57)【特許請求の範囲】
【請求項１】
ネットワークを通じてデジタル装置によって受信された悪意あるポータブルドキュメントフォーマット（ＰＤＦ）文書を検出する方法であって、
前記デジタル装置内のＰＤＦパーサによって、少なくともヘッダを含む前記ＰＤＦ文書の一部に悪意あるネットワークコンテンツを示す少なくとも１つの不審性が含まれているかを判断すべく、当該ＰＤＦ文書の当該一部の検査を行ない、
前記ＰＤＦ文書の前記一部に悪意あるネットワークコンテンツを示す少なくとも１つの不審性が含まれていると判断された場合、当該ＰＤＦ文書を、前記デジタル装置内で動作する少なくとも１つの仮想マシンに提供し、
前記少なくとも１つの仮想マシンによって、ＰＤＦリーダアプリケーションを用いて前記ＰＤＦ文書の前記一部の処理を行ない、当該ＰＤＦ文書の当該一部が前記悪意あるネットワークコンテンツを含んでいるかを検証する、方法。
【請求項２】
前記ＰＤＦ文書の前記一部が悪意あるネットワークコンテンツを示す少なくとも１つの不審性を含んでいると判断されると、少なくとも当該ＰＤＦ文書に関連付けられたデータに基づいて前記デジタル装置に関連付けられた前記少なくとも１つの仮想マシンを構成する、請求項１に記載の方法。
【請求項３】
ネットワークを通じて受信した悪意あるポータブルドキュメントフォーマット（ＰＤＦ

）文書を検出するシステムであって、
少なくともヘッダを含む前記ＰＤＦ文書の一部が悪意あるネットワークコンテンツを示す少なくとも１つの不審性を含んでいるかを判断するために、当該ＰＤＦ文書の当該一部を検査するように構成されたパーサと、
前記パーサと通信可能に結合され、（ｉ）前記パーサによって前記ＰＤＦ文書の前記一部が悪意あるネットワークコンテンツを示す少なくとも１つの不審性を含んでいると判断されると、当該ＰＤＦ文書の少なくとも当該一部を受信し、（ｉｉ）ＰＤＦリーダアプリケーションを用いて当該ＰＤＦ文書の当該一部を処理し、当該ＰＤＦ文書の当該一部が当該悪意あるネットワークコンテンツを含んでいるかを検証するように構成された少なくとも１つの仮想マシンと、
を備えている、システム。
【請求項４】
前記ＰＤＦ文書の前記一部が検査され、当該ＰＤＦ文書の当該一部が悪意あるネットワークコンテンツを示す少なくとも１つの不審性を含むと判断されると、少なくとも当該ＰＤＦ文書に関連付けられたデータに基づいて前記少なくとも１つの仮想マシンが構成される、請求項３に記載のシステム。
【請求項５】
前記少なくとも１つの仮想マシンは、前記パーサにより検査される前記ＰＤＦ文書の前記ヘッダに含まれるＰＤＦ仕様バージョン番号に一部基づいて構成される、請求項３に記載のシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
本出願は、「悪意あるネットワークコンテンツを検出するシステムおよび方法」を発明の名称とし、２００８年１１月３日に提出された米国特許出願１２／２６３，９７１号の一部継続出願である。
本出願は、「仮想マシン上でのリプレイによる経験則ベースのキャプチャ」を発明の名称とし、２００６年４月２０日に提出された同時係属中の米国特許出願１１／４０９，３５５号にも関連する。当該関連出願は、「コンピュータウイルス防御システムおよび方法」を発明の名称とし、２００５年６月１３日に提出された米国特許出願１１／１５２，２８６号の一部継続出願である。当該一部継続出願は、「コンピュータウイルス防御システムおよび方法」を発明の名称とし、２００４年６月１４日に提出された米国特許仮出願６０／５７９，９１０の優先権の利益を主張するものである。
米国特許出願１１／４０９，３５５号は、「コンピュータウイルスを検出するシステムおよび方法」を発明の名称とし、２００５年３月３１日に提出された米国特許出願１１／０９６，２８７号の一部継続出願でもある。当該一部継続出願は、「コンピュータウイルスを検出するシステムおよび方法」を発明の名称とし、２００４年４月１日に提出された米国特許仮出願６０／５５９，１９８の優先権の利益を主張するものである。
米国特許出願１１／４０９，３５５号は、「コンピュータウイルスをインターセプトするシステムおよび方法」を発明の名称とし、２００５年６月１３日に提出された米国特許出願１１／１５１，８１２号の一部継続出願でもある。当該一部継続出願は、「コンピュータウイルスをインターセプトするシステムおよび方法」を発明の名称とし、２００４年６月１４日に提出された米国特許仮出願６０／５７９，９５３の優先権の利益を主張するものである。
上記各特許出願の内容は、ここに参照として取り込まれる。
【０００２】
本出願は、主にネットワークセキュリティに関連し、より具体的には、悪意あるネットワークコンテンツの検出に関連する。
【背景技術】
【０００３】

現在、悪意あるネットワークコンテンツ（悪意あるソフトウェア、マルウェアなど）が通信ネットワークを経由して様々な装置を攻撃可能である。例えば、マルウェアは、コンピュータユーザにとって有害なプログラムやファイルを含みうる。例えば、ボット、コンピュータウイルス、ワーム、トロイの木馬、アドウェア、スパイウェア、コンピュータユーザの情報を収集したり、当該ユーザの許可なく動作したりするプログラミングが挙げられる。

【０００４】

アドウェアは、コンピュータや特定のユーザに広告を宛てるプログラムである。一例として、アドウェアは、様々なウェブサイトをブラウザで訪問したコンピュータとユーザの少なくとも一方を特定する。するとウェブサイトは、ポップアップ広告を生成したり、特定の広告をユーザのブラウザに宛てるべく、アドウェアを使用しうる。

スパイウェアは、ユーザ、コンピュータ、およびユーザのネットワーク習慣の少なくとも１つに係る情報を収集するプログラムである。一例として、スパイウェアは、ユーザが閲覧したウェブサイトの名称と種別に係る情報を収集し、当該情報を別のコンピュータに送信しうる。

アドウェアとスパイウェアは、これらをホストするウェブサイトをユーザが閲覧した後に当該ユーザのコンピュータに追加されることが多い。ユーザはこれらのプログラムが追加されたことに気づかないことが多い。アドウェアやスパイウェアの機能についても同様である。

【０００５】

悪意あるネットワークコンテンツが引き起こしうる問題を防ぐために、様々な処理や装置が用いられている。例えば、コンピュータは、アンチウイルススキャンソフトを内蔵することが多い。当該ソフトは、特定のクライアント装置におけるウイルスをスキャンする。またコンピュータは、スパイウェアとアドウェアの少なくとも一方をスキャンするソフトウェアを内蔵しうる。スキャンは手動で実行されてもよいし、そのコンピュータに関わるユーザやシステム管理者などによって指定されたスケジュールに基づいて実行されてもよい。残念なことに、そのスキャンソフトによってウイルスやスパイウェアが検出されるまでは、そのコンピュータにおけるダメージや、プライバシーの損失がすでに生じているおそれがある。

【０００６】

悪意あるソフトウェアコンテンツは、ボットを備えている場合がある。ボットは、デジタル装置（コンピュータなど）の少なくとも一部を、当該デジタル装置に係る正規所有者の許可なく遠隔制御するように構成されたソフトウェアロボットである。ボットに関わる動作としては、ボットの伝搬や、ネットワーク上における他のコンピュータの攻撃が含まれる。ボットは、ネットワーク上で動作しているノード（例えばコンピュータやその他のデジタル装置）をスキャンし、脆弱なターゲットを探すことにより、広く伝搬する。脆弱なコンピュータが見つかると、ボットは自身のコピーを当該コンピュータにインストールしうる。インストールが済むと、新たなボットは、感染させるネットワーク上の他のコンピュータの探索を継続しうる。ボットは、悪意あるウェブサイトからも伝搬しうる。当該サイトは、そのウェブページを訪れた脆弱なコンピュータにつけこむように構成されている。

【０００７】

ボットは、感染したコンピュータユーザの許可なく、コマンドを生成し、命令を受信する通信チャネルを制御しうる。またボットは、コマンドを受信し、中央ボットサーバや他の感染したコンピュータからの通信を制御しうる。当該通信は、例えば、感染したコンピュータ上のボットにより形成されたピアツーピア（Ｐ２Ｐ）ネットワークを経由して行なわれる。複数のボット（いわゆるボットネット）がともに動作すると、感染したコンピュータ（いわゆるゾンビ）は、ネットワーク上の少なくとも１つのコンピュータに対して組織化された攻撃を行なったり、犯罪活動に関与したりすることがある。少なくとも１つのボットが、命令を受信すると感染したコンピュータに宛ててスパムを送信しうる例もある

。認可されていない医薬品を販売する医薬品ウェブサイトのような不法ビジネスを、ボットがホストしうる例もある。

【０００８】

悪意あるネットワークコンテンツは、例えばウェブサイトやＨＴＴＰ標準に基づいて動作するサーバを経由してネットワークに広がりうる。このようにして広がった悪意あるネットワークコンテンツは、これをホストするウェブサイトにアクセスするだけで、ユーザの承諾や認識を伴うことなく積極的にダウンロードされ、当該ユーザのコンピュータにインストールされうる。悪意あるネットワークコンテンツをホストするウェブサイトは、悪意あるウェブサイトと称されることがある。

悪意あるネットワークコンテンツは、悪意あるウェブサイトにホストされたウェブページに付随するデータに埋め込まれうる。例えば、ウェブページはジャバスクリプト（ＪａｖａＳｃｒｉｐｔ：登録商標）コードを含みうる。そして悪意あるネットワークコンテンツは、当該ジャバスクリプトコードに埋め込まれうる。本例において、ジャバスクリプトコードに埋め込まれた悪意あるネットワークコンテンツは見つかりにくくされうる。当該ジャバスクリプトコードが実行されるまで、それが悪意あるネットワークコンテンツを含んでいることが判らないようにするためである。したがって、悪意あるネットワークコンテンツは、アンチウイルスソフト、ファイヤーウォール、侵入検知システムなどにより検出される前に、ユーザのコンピュータを攻撃したり感染させたりしうる。

【先行技術文献】

【非特許文献】

【０００９】

【非特許文献１】N. Provos, P, Mavrommatis, M. A. Rajab, and F. Monrose, "All your iFRAMEs Point to Us," Google Technical Report Provos-2008a, February 4, 2008

【発明の概要】

【発明が解決しようとする課題】

【００１０】

２００９年の始まり頃、ボットの作者の間では、ウェブ媒介攻撃を伝搬させるためにアドビシステム社のポータブルドキュメントフォーマット（ＰＤＦ）形式の悪意ある文書を用いることが広く知られていた。悪意あるＰＤＦ文書は、犯罪者によって制御されたウェブサーバによってホストされ、当該ウェブサーバへのリンクが他の多くのウェブサイトによって作成された。よって不慣れなユーザは、悪意あるＰＤＦをブラウザおよびＰＤＦリーダにロードさせるウェブサイトを、偶然かつ無認識のうちに閲覧してしまい、ユーザのコンピュータアカウントやコンピュータ全体が支配下に置かれる可能性があった。これにより、悪意あるボットソフトがインストールされうる状況となる。

【課題を解決するための手段】

【００１１】

幾つかの実施形態によれば、本発明は、悪意あるポータブルドキュメントフォーマット（ＰＤＦ）形式のネットワークコンテンツを検出する方法に係る。当該方法は、少なくとも以下のステップを含みうる。

（ａ）受信したＰＤＦネットワークコンテンツの少なくとも一部を検査し、当該ＰＤＦネットワークコンテンツの少なくとも一部に悪意あるネットワークコンテンツが含まれていることを示す少なくとも１つの不審性があるかを判断する。

（ｂ）当該ＰＤＦネットワークコンテンツの少なくとも一部に悪意あるネットワークコンテンツが含まれていると判断された場合、当該ＰＤＦネットワークコンテンツの少なくとも一部を少なくとも１つの仮想マシンに提供し、当該ＰＤＦネットワークコンテンツの少なくとも一部に悪意あるネットワークコンテンツが含まれているかを検証する。

【図面の簡単な説明】

【００１２】

【図１】悪意あるネットワークコンテンツの検出環境１００の例を示す図である。

【図２】分析環境の例を示す図である。

【図３】悪意あるネットワークコンテンツを検出する方法の例を示す図である。
【図４】悪意あるネットワークコンテンツを検出する方法の別例を示す図である。
【図５】コントローラの例を示す図である。
【図６】悪意あるＰＤＦネットワークコンテンツの検出環境の例を示す図である。
【図７】悪意あるネットワークコンテンツを検出する方法の例を示す図である。
【発明を実施するための形態】
【００１３】
ネットワークコンテンツは、ネットワークを通じて送信されるデータ（すなわちネットワークデータ）を含みうる。ネットワークデータは、テキスト、ソフトウェア、画像、音声、その他のデジタルデータを含みうる。
一例として、ネットワークコンテンツは、ウェブコンテンツや、ＨＴＴＰ（HyperTextTransfer Protocol）、ＨＴＴＰ（HyperText Markup Language Protocol）、あるいはウェブブラウザソフトウェアアプリケーション上での表示に適した手法を用いて転送されうるネットワークデータを含みうる。
別例として、ネットワークコンテンツは、電子メールプロトコルを用いて転送されうる電子メールメッセージを含みうる。電子メールプロトコルとしては、ＳＭＴＰ（Simple Mail Transfer Protocol）、ＰＯＰ３（Post Office Protocol version 3）、ＩＭＡＰ４（Internet Message Access Protocol）が挙げられる。
さらに別例として、ネットワークコンテンツは、インスタントメッセージングプロトコルを用いて転送されうるインスタントメッセージを含みうる。インスタントメッセージングプロトコルとしては、ＳＩＰ（Session Initiation Protocol）、ＸＭＰＰ（eXtensible Messaging and Presence Protocol）などが挙げられる。
さらにネットワークコンテンツは、ＦＴＰ（File Transfer Protocol）のような他のデータ転送プロトコルを用いて転送されうるネットワークデータを含みうる。
ここではネットワークコンテンツを、ネットワークプロトコルヘッダ情報と区別する。ネットワークプロトコルヘッダ情報は、ネットワークコンテンツの宛先を指定し、送信経路を決定し、送り届けるために用いられる。
【００１４】
通信ネットワークを通じて演算装置に転送される悪意あるネットワークコンテンツ（悪意あるウェブコンテンツなど）を検出するために、受信システム上におけるネットワークコンテンツの受信と処理をシミュレーションする仮想マシンが用いられうる。当該ネットワークコンテンツが悪意あるものかの判断は、仮想マシンの当該ネットワークコンテンツに対する応答に基づいてなされうる。不審なネットワークコンテンツが悪意なしと判断されることもある。仮想マシンにおける不審なネットワークコンテンツの処理は、当該不審なネットワークコンテンツが実際に悪意あるものかを判断し、誤って悪意ありとみなされることを防止するために重要なステップである。悪意あるネットワークコンテンツの検出時における誤判定は、不審なネットワークコンテンツを仮想マシン内で処理し、当該不審なネットワークコンテンツに対する当該仮想マシンの応答を分析して悪意あるネットワークコンテンツを検出することにより、回避されうる。
【００１５】
従来は、悪意あるネットワークコンテンツをホストするウェブサーバと演算装置間のネットワークにおいてプロキシが用いられうる。プロキシは、当該演算装置上で動作するウェブブラウザにより発行されるネットワークコンテンツの要求をインターセプトしうる。そしてプロキシは、演算装置の代理としてウェブサーバに要求を発行しうる。プロキシは、当該要求に対する応答をウェブサーバより受信しうる。そしてプロキシは、悪意あるネットワークコンテンツを検出するために、当該要求と応答を含むデータ交換を仮想マシン上で処理し、当該データ交換に対する仮想マシンの応答を評価しうる。悪意あるネットワークコンテンツが検出されない場合、プロキシは、要求されたネットワークコンテンツを要求元の演算装置に提供しうる。
【００１６】

各データ交換は仮想マシンを用いて処理されるため、この手法は非常に演算負荷が高く、ネットワーク上の多くの演算装置に対して拡張可能ではない。また要求されたネットワークコンテンツは、それが悪意あるネットワークコンテンツを含んでいないと判断されるまでは演算装置に届けられないため、ネットワークコンテンツを要求してから届けられるまでの間に顕著な遅れが発生する。

【００１７】

非特許文献１は、大型のウェブリポジトリおよび不審なＵＲＬのコーパスを用いたウェブマルウェアの分析について報告している。非特許文献１においては、ウェブリポジトリ内のウェブページから特徴を抽出し、当該特徴を尤度スコアに変換するために、まず分析用のデータが前処理フェーズにおいて機械学習フレームワークを用いて収集される。次に、機械学習フレームワークにより特定された候補を検証する検証フェーズにおいて、仮想マシンが用いられる。ウェブリポジトリ内のウェブページの約０．１％が、検証フェーズにおいて仮想マシンにより処理される。非特許文献１は、リポジトリ内の各ＵＲＬを余すところなく検査することは、法外なコストを伴うとしている。非特許文献１において用いられているシステムは、クローラに依存している。クローラは、リポジトリ内のデータを検査のために収集すべく、ウェブ内を徐々に進んでいく。仮想マシン内での検査のために進行中のネットワーク上におけるウェブページを検査・選択することはできない。

【００１８】

図１は、悪意あるネットワークコンテンツの検出環境１００の例を示す図である。悪意あるネットワークコンテンツの検出環境１００は、サーバ装置１０５、クライアント装置１１０、およびタップ１１５（データアクセスコンポーネントとしても知られる）を備える。これらの各々は通信ネットワーク１２０と結合されている。

様々な実施形態において、サーバ装置１０５とクライアント装置１１０はそれぞれ複数であってもよい。

タップ１１５は、さらに悪意あるネットワークコンテンツの検出システム１２５と結合されている。悪意あるネットワークコンテンツの検出システム１２５は、ネットワークコンテンツ（ウェブコンテンツなど）が悪意あるネットワークコンテンツを含むと判定されるまで、これをインターセプトあるいは保持するのではなく、ネットワークコンテンツの流通を監視しうる。悪意あるネットワークコンテンツの検出システム１２５は、通信ネットワーク１２０を通じて流通するネットワークコンテンツを検査し、不審なネットワークコンテンツを特定し、当該不審なネットワークコンテンツを仮想マシンで分析することにより悪意あるネットワークコンテンツを検出するように構成されうる。

このように、悪意あるネットワークコンテンツの検出システム１２５は、演算効率が高く、データトラフィック量と通信ネットワークを通じて通信を行なう演算装置の数の増加に対してスケーラブルでありうる。したがって、悪意あるネットワークコンテンツの検出システム１２５は、悪意あるネットワークコンテンツの検出環境１００におけるボトルネックとはなりえない。

【００１９】

通信ネットワーク１２０は、インターネットのような公衆コンピュータネットワークや、無線電話ネットワーク、広域ネットワーク、ローカルエリアネットワーク、あるいはこれらの組合せのような私的コンピュータネットワークを含みうる。通信ネットワーク１２０は、あらゆる種類のネットワークを含み、異なる種類のデータ通信に用いられうるが、例示の目的で、ウェブデータの通信について以下述べることとする。

【００２０】

サーバ装置１０５とクライアント装置１１０は、デジタル装置を含みうる。デジタル装置の例としては、コンピュータ、サーバ、ラップトップ、個人用携帯情報端末、携帯電話などが挙げられる。サーバ装置１０５は、通信ネットワーク１２０を通じてネットワークデータをクライアント装置１１０に送信するように構成されうる。クライアント装置１１０は、サーバ装置１０５からのネットワークデータを受信するように構成されうる。ネットワークデータは、ネットワーク通信プロトコル（ＨＴＴＰなど）を用いて送信されたウ

ェブページのような、ネットワークコンテンツを含みうる。
様々な実施形態において、サーバ装置１０５は、ネットワークコンテンツを提供するように構成されたウェブサーバを含みうる。クライアント装置１１０は、ネットワークコンテンツの読出しと表示の少なくとも一方を行なうように構成されたウェブラウザを含みうる。

【００２１】
タップ１１５は、ネットワークデータを監視し、当該ネットワークデータのコピーを悪意ネットワークコンテンツの検出システム１２５に提供するように構成されたデジタルデータタップを含みうる。ネットワークデータは、通信ネットワーク１２０を通じて送信され、サーバ装置１０５からクライアント装置１１０へのデータフローを含む信号およびデータを備えうる。一例として、タップ１１５は、ネットワークデータの監視およびコピーを、サーバ装置１０５、クライアント装置１１０、通信ネットワーク１２０の性能低下が認識されることなく実行する。タップ１１５は、ネットワークデータの任意の部分をコピーしうる。例えば、タップ１１５は、ネットワークデータから任意の数のデータパケットを受信し、コピーしうる。

【００２２】
幾つかの実施形態においては、ネットワークデータが、少なくとも１つのデータフローにまとめられ、悪意あるネットワークコンテンツの検出システム１２５に提供されうる。
様々な実施形態において、タップ１１５は、サンプリングスキームに基づいてネットワークデータをサンプリングしうる。データフローは、当該サンプリングされたネットワークデータに再構成されうる。

【００２３】
またタップ１１５は、ネットワークデータからメタデータを保存しうる。メタデータは、サーバ装置１０５とクライアント装置１１０の少なくとも一方と関連付けられうる。例えば、メタデータは、サーバ装置１０５とクライアント装置１１０の少なくとも一方を特定しうる。
別の実施形態においては、後述するヒューリスティックモジュール１３０が、メタデータを生成するためにネットワークデータ中のデータパケットを分析することにより、サーバ装置１０５とクライアント装置１１０を特定しうる。

【００２４】
悪意ネットワークコンテンツの検出システム１２５は、タップ１１５からネットワークデータを受信するデジタル装置、ソフトウェア、あるいはこれらの組合せを含みうる。悪意ネットワークコンテンツの検出システム１２５は、ヒューリスティックモジュール１３０、経験則データベース１３５、スケジューラ１４０、仮想マシンプール１４５、および分析環境１５０を含む。
幾つかの実施形態においては、タップ１１５が、悪意ネットワークコンテンツの検出システム１２５に含まれうる。

【００２５】
ヒューリスティックモジュール１３０は、タップ１１５からネットワークデータのコピーを受信し、当該データに経験則を適用してネットワークデータが不審なネットワークコンテンツを含んでいるかを判定する。ヒューリスティックモジュール１３０により適用される経験則は、経験則データベース１３５に保存されているデータと規則の少なくとも一方に基づきうる。一例として、ヒューリスティックモジュール１３０は、経験則分析を適用した後、ネットワークデータが不審であるとのフラグを立てうる。そのネットワークデータは次いでバッファされ、データフローにまとめられうる。そのデータフローは、次いでスケジューラ１４０に提供されうる。
幾つかの実施形態においては、不審なネットワークデータが、バッファされたりデータフローにまとめられたりすることなく、スケジューラ１４０に直接提供されうる。
その他の実施形態において、仮想マシンによる後の読出しのために、データフローグループ（関連するウェブページ要求と応答のセットなど）の通知が、スケジューラ１４０に

対してなされうる。

【００２６】

ヒューリスティックモジュール１３０は、少なくとも１つの経験則分析をネットワークデータに対して行ないうる。ヒューリスティックモジュール１３０は、タップ１１５により過去にコピーされた特定のデータフローに所属するデータパケットを保持しうる。一例として、ヒューリスティックモジュール１３０は、タップ１１５からデータパケットを受信し、当該データパケットをバッファあるいは他のメモリに保存する。ヒューリスティックモジュール１３０が所定数のデータパケットを特定のデータフローから受信すると、ヒューリスティックモジュール１３０は、経験則分析と確率分析の少なくとも一方を実行しうる。

【００２７】

幾つかの実施形態においては、ヒューリスティックモジュール１３０が、データフローに所属するデータパケットのセットに対して経験則分析を行ない、当該データパケットをバッファあるいは他のメモリに保存する。そしてヒューリスティックモジュール１３０は、同じデータフローに所属する新たなデータパケットの読み出しを継続しうる。同じデータフローに所属する所定数の新たなデータパケットが読み出されると、不審なネットワークコンテンツの尤度を特定するために、バッファされたデータパケットと新たなデータパケットの組合せに対して経験則分析が行なわれうる。

【００２８】

幾つかの実施形態においては、任意のバッファが、フラグの立てられたネットワークデータをヒューリスティックモジュール１３０から受信する。当該バッファは、フラグの立てられたネットワークデータを保存し、少なくとも１つのデータフローにまとめるために用いられうる。その後、当該少なくとも１つのデータフローが、スケジューラ１４０に提供される。一例として、当該バッファは、ネットワークデータを保存することにより、悪意ネットワークコンテンツの検出システム１２５における他のコンポーネントが機能の遂行や、データ渋滞の解消を可能にする。

【００２９】

幾つかの実施形態においては、ヒューリスティックモジュール１３０が、仮想マシンの処理対象となりうるネットワークコンテンツデータのコピーを維持し、要求に応じて提供しうる（例えば、後に仮想マシン内でウェブブラウザ実行され、それ以前にネットワーク上に送信されたエンティティを要求したとき）。ヒューリスティックモジュール１３０がこのデータをメモリ内に保持する時間の長さは、そのデータの不審さ、システムにかかる負荷の程度、および他の要因の少なくとも１つに基づきうる。

【００３０】

スケジューラ１４０は、クライアント装置１１０を特定し、当該クライアント装置１１０に関連付けられた仮想マシンを読み出しうる。仮想マシンは、装置（クライアント装置１１０など）の動作を模倣するように構成されたソフトウェアである。仮想マシンは、仮想マシンプール１４５から読み出されうる。さらに、スケジューラ１４０は、クライアント装置１１０上で動作するウェブブラウザを特定し、当該ウェブブラウザに関連付けられた仮想マシンを読み出しうる。

【００３１】

幾つかの実施形態においては、ヒューリスティックモジュール１３０が、クライアント装置１１０を特定するメタデータをスケジューラ１４０に送信する。

別の実施形態においては、スケジューラ１４０が、ネットワークデータにおける少なくとも１つのデータパケットを、ヒューリスティックモジュール１３０から受信し、クライアント装置１１０を特定するために当該少なくとも１つのデータパケットを分析する。

さらに別の実施形態においては、メタデータがタップ１１５から受信されうる。

【００３２】

スケジューラ１４０は、仮想マシンを読み出し、クライアント装置１１０の関連する動作特性を模倣するように当該仮想マシンを構成しうる。一例として、スケジューラ１４０

は、タップ１１５によりコピーされたネットワークデータにより影響を受けるクライアント装置１１０の特徴のみを模倣するように、仮想マシンの特性を構成する。スケジューラ１４０は、ネットワークデータにより影響を受けるクライアント装置１１０の特徴を、タップ１１５からの当該ネットワークデータを受信および分析することにより、決定しうる。そのようなクライアント装置１１０の特徴としては、ネットワークデータを受信するためのポート、ネットワークデータに応答するためにデバイスドライバ、およびネットワークデータに応答可能かつクライアント装置１１０に結合あるいは装備された他の装置の選択が含まれうる。

他の実施形態においては、ヒューリスティックモジュール１３０が、ネットワークデータにより影響を受けるクライアント装置１１０の特徴を、タップ１１５からの当該ネットワークデータを受信および分析することにより、決定しうる。ヒューリスティックモジュール１３０は、当該クライアント装置の特徴を、スケジューラ１４０に送信しうる。

【００３３】

仮想マシンプール１４５は、少なくとも１つの仮想マシンを保存するように構成されうる。仮想マシンプール１４５は、ソフトウェアと、ソフトウェアを保存可能な記憶媒体の少なくとも一方を含みうる。一例として、仮想マシンプール１４５は、単一の仮想マシンを保存する。当該単一の仮想マシンは、スケジューラ１４０によって、通信ネットワーク１２０上のクライアント装置１１０の動作を模倣するように構成されうる。仮想マシンプール１４５は、様々なクライアント装置１１０の動作をシミュレートするように構成されうる任意の数の独立した仮想マシンを保存しうる。

【００３４】

分析環境１５０は、ネットワークコンテンツをクライアント装置１１０から受信した後に、当該ネットワークコンテンツがクライアント装置１１０に与える影響を分析するために、サーバ装置１０５からのネットワークデータの受信と表示の少なくとも一方をシミュレートする。分析環境１５０は、仮想マシンにより実行されたネットワークコンテンツがクライアント装置１１０に与える影響のシミュレーションを分析することにより、マルウェアや悪意あるネットワークコンテンツの影響を特定しうる。ネットワークコンテンツの複数のフローをシミュレートするために、複数の分析環境１５０が設けられてもよい。分析環境１５０については、図２を参照しつつ、さらに説明する。

【００３５】

図１は、サーバ装置１０５からクライアント装置１１０へ送信されるデータを示しているが、どちらの装置も相互にデータの送受信が可能である。同様に、２つの装置のみが示されているが、任意の数の装置が通信ネットワーク１２０を通じてデータの送受信を行ないうる。さらに、タップ１１５は、通信ネットワーク１２０や、これに接続された装置の性能に目に見える影響を与えることなく、複数の装置から送信されるデータの監視とコピーを行なうことが可能である。

【００３６】

図２は、分析環境１５０の例を示す。分析環境１５０は、レプレイヤ２０５、仮想スイッチ２１０、および仮想マシン２１５を含む。リプレイヤ２０５は、ヒューリスティックモジュール１３０によってフラグが立てられたネットワークコンテンツを受信し、当該ネットワークコンテンツを、仮想スイッチ２１０を介して仮想マシン２１５に提供する（すなわち、ネットワークコンテンツをリプレイする）。

幾つかの実施形態においては、リプレイヤ２０５は、フラグが立てられたネットワークコンテンツの送信時におけるサーバ装置１０５の挙動を模倣する。サーバ装置１０５とクライアント装置１１０間におけるネットワークコンテンツの送信をシミュレートする任意の数のリプレイヤ２０５が設けられうる。

別の実施形態においては、リプレイヤ２０５が、リプレイされるプロトコルシーケンスにおける「現実の」クライアントやサーバをエミュレートするために、必要に応じてセッション変数を直接変更しうる。一例として、直接置き換えられる動的変数は、直接割り当てられたポート、トランザクションＩＤ、および各プロトコルセッションについて動的で

ある他の変数を含む。

【００３７】

仮想スイッチ２１０は、フラグを立てられたネットワークコンテンツのパケットを仮想マシン２１５に送ることができるソフトウェアを含みうる。一例として、リプレイヤ２０５は、サーバ装置１０５によるデータフローの送信をシミュレートする。仮想スイッチ２１０は通信ネットワーク１２０をシミュレートし、仮想マシン２１５はクライアント装置１１０をシミュレートする。仮想スイッチ２１０は、データフローのパケットを仮想マシン２１５の正しいポートへ送りうる。

【００３８】

幾つかの実施形態においては、仮想マシン２１５におけるクライアントソフトウェア（ウェブブラウザなど）からデータがキャッシュされているヒューリスティックモジュール１３０へのデータ要求が、リプレイヤによってプロキシされうる。ヒューリスティックモジュール１３０から仮想マシン２１５上で動作しているクライアントソフトウェアへの応答も、リプレイヤによってプロキシされうる。

【００３９】

仮想マシン２１５は、スケジューラ１４０によって分析環境１５０に提供されうるクライアント装置１１０のリプレゼンテーションを含む。一例として、スケジューラ１４０は、仮想マシン２１５のインスタンスを仮想マシンプール１４５から読み出し、クライアント装置１１０を模倣するように仮想マシン２１５を構成する。そうして構成された仮想マシン２１５は、分析環境１５０に提供され、フラグが立てられたネットワークコンテンツを仮想スイッチ２１０から受信しうる。

【００４０】

分析環境１５０がネットワークコンテンツの送受信をシミュレートすることにより、仮想マシン２１５の無権限活動に係る挙動が厳重に監視されうる。仮想マシン２１５がクラッシュしたり、不法な動作を行なったり、異常動作をしたり、無権限エンティティ（無権限のコンピュータユーザやボットなど）へのデータアクセスを許可したりすると、分析環境１５０が反応しうる。一例として、分析環境１５０は、コマンドをクライアント装置１１０に送信し、サーバ装置１０５からのネットワークコンテンツやデータフローの受け入れを停止する。

【００４１】

幾つかの実施形態においては、特定種のマルウェアや悪意あるネットワークコンテンツを判断するために、分析環境１５０が、仮想マシン２１５の挙動を監視・分析する。また分析環境１５０は、新種のウイルス、ワーム、ボッツ、アドウェア、スパイウェア、その他のマルウェアや悪意あるネットワークコンテンツを排除するように構成されたコンピュータコードを生成しうる。

様々な実施形態において、分析環境１５０は、マルウェアや悪意あるネットワークコンテンツにより与えられたダメージを修復するように構成されたコンピュータコードを生成する。不審なネットワークコンテンツの送受信をシミュレーションし、かつ仮想マシン２１５の応答を分析することにより、分析環境１５０は、コンピュータシステムがダメージを与えられたり、危険に晒されたりする前に、既知あるいは未特定のマルウェアおよび悪意あるネットワークコンテンツを特定しうる。

【００４２】

図３は、悪意あるネットワークコンテンツを検出する方法３００の例を示す。

ステップ３０５においては、ネットワークコンテンツのパケットがインターセプトあるいはコピーされる。パケットは、サーバ装置１０５と宛先（クライアント装置１１０など）の間のネットワークデータ転送において、例えばタップ１１５などによって、インターセプトとコピーの少なくとも一方が行なわれうる。パケットは、ネットワークコンテンツのようなデータの要求や、要求に応答して提供されるデータを含みうる。

【００４３】

ステップ３１０においては、ネットワークコンテンツのパケットが検査される。ヒュー

リスティックモジュール１３０は、ネットワークコンテンツのパケットが不審なものであるかを検査するために、少なくとも１つの経験則を利用しうる。不審なネットワークコンテンツは、パケット内に悪意あるネットワークコンテンツやマルウェアが存在する可能性を示す。

【００４４】

ネットワークコンテンツのパケットは、別のネットワークコンテンツのパケットを含むデータフローの一部でありうる。例えば、ネットワークコンテンツのパケットは、ウェブページの一部を表現しうる。一方、データフローにおいて関連する他のパケットは、ウェブページの別の一部を表現しうる。ネットワークコンテンツのパケットは、データフローに含まれるネットワークコンテンツのパケット群が連続あるいは並行して検査されうるように、当該関連する他のパケットとともに保存されうる。悪意あるネットワークコンテンツの検出システムは、ネットワークコンテンツのパケット群、およびデータフローの少なくとも一部を保存しうる。データフローとデータパケット群は、検査のために任意のタイミングで任意の期間（数秒から数分、数十分よりも長く）保存されうる。

【００４５】

高いデータ転送速度の通信ネットワークを通じてのデータフローをより長い時間保存することを容易にするため、多数のデータパケットに含まれる大容量のデータオブジェクトが切り捨てられて、代表的なデータパケットの小容量のサブセットとされうる。データオブジェクトの切捨ては、ネットワーク通信帯域幅の大半が大容量のデータオブジェクトのごく一部によって利用される場合（動画の場合など）において、とりわけ有用である。例えば、動画データは、少数のデータパケット（最初の数パケットなど）に切り捨てられうる。大容量のデータパケットが切り捨てられる程度は、利用可能なメモリ量、データ帯域幅、データオブジェクトの種別、その他の因子に依存しうる。

データフローを保存するために割り当てられたメモリ量は、データ種別のようなデータフローの特性にも依存しうる。一例として、８ビットのストリーム、テキストストリーム、ＨＴＭＬストリーム、および様々なバイナリストリームには、１メガバイト（ＭＢ）が割り当てられうる。動画、音声、その他ほとんどのデータ種には、１２８キロバイト（ｋＢ）が割り当てられうる。悪意あるネットワークコンテンツの検出精度を維持し、メモリの制限内で動作しつつ、分析スループットを向上させるために、各データフロー種の保存に割り当てられるメモリ量は、動的にあるいは定期的に調整されうる。

【００４６】

ステップ３１５においては、ネットワークコンテンツの不審性が特定される。ヒューリスティックモジュール１３０は、ステップ３１０におけるネットワークコンテンツ検査の結果として、ネットワークコンテンツの不審性を特定しうる。文字列やキーワードといったパケットの特性が、ステップ３１０において用いられた経験則の条件に合致すると判断されると、ネットワークコンテンツの不審性あるいは「特徴」が特定される。特定された特徴は、参照および分析のために保存されうる。

幾つかの実施形態においては、パケット全体が検査に供され、次のステップに進む前に複数の特徴が特定されうる。

幾つかの実施形態においては、ネットワークコンテンツを含む複数のパケットにわたる分析の結果として、特徴が特定されうる。

【００４７】

経験則に用いられるキーワードは、近似ベイズ確率論的分析を行なうことにより選択されうる。当該分析は、ＨＴＭＬ仕様における全てのキーワードに対して、悪意あるネットワークコンテンツのコーパスおよび悪意なきネットワークコンテンツのコーパスを用いて行なわれる。近似ベイズ確率論的分析は、ベイズ理論と単純ベイズ分類法の少なくとも一方の原理に基づきうる。例えば、悪意あるネットワークコンテンツにキーワードが出現する確率Ｐｍは、悪意あるネットワークコンテンツのコーパスを用いて計算されうる。一方、悪意なきネットワークコンテンツにキーワードが出現する確率Ｐｎは、悪意なきネットワークコンテンツのコーパスを用いて計算されうる。あるキーワードは、計算された比Ｐ

ｍ／Ｐｎに基づくスコアが不審度閾値を上回る場合に、悪意あるネットワークコンテンツと関連付けられる不審性を有するものとして特定されうる。不審度閾値は、１、１０、３０、６０、１００以上の値、あるいは、不審性がどの程度であるかを示す他の値とされうる。すなわち、ネットワークコンテンツが悪意なきものであるよりは、悪意あるものであろうことを示しうる値とされうる。

【００４８】

ステップ３２０においては、ステップ３１５で特定された不審性が悪意あるネットワークコンテンツを示す確率に係るスコアが決定される。近似ベイズ確率論的分析は、リアルタイムで実行されうる。あるいは、過去に行なわれた近似ベイズ確率論的分析に基づくルックアップテーブルを用いて実行されうる。

【００４９】

例えば、特定の特徴がパケット中の悪意あるネットワークコンテンツの存在に関連付けられる相対確率スコアを決定するために、近似ベイズ確率論的分析が、悪意あるネットワークコンテンツのコーパスと通常あるいは悪意なきネットワークコンテンツのコーパスを比較することにより行なわれうる。特徴は、ステップ３１０で用いられた経験則の条件に合致するパケットの特性（文字列やキーワード列など）を含みうる。また特徴は、順次あるいは並列に検査された少なくとも１つのパケットに関連する特性を含みうる。一例として、特徴は、文字列「eval(unescape(」を含みうる。当該文字列は、ジャバスクリプトの「eval」コマンド引数内にネストされたジャバスクリプトの「unescape」コマンドを示す。特徴の別例は、方法４００におけるステップ４４５を参照して後述する。

悪意あるネットワークコンテンツのパケット中に特徴が存在する確率$P_{f|m}$は、悪意なきネットワークコンテンツのコーパスを分析することにより計算される。悪意なきネットワークコンテンツのパケット中に特徴が存在する確率$P_{f|n}$は、悪意なきネットワークコンテンツのコーパスを分析することにより計算される。悪意あり確率スコアは、特徴が悪意あるネットワークコンテンツに関連付けられる相対確率因子$P_{f|m}$の２を底とする対数として計算される。悪意あり確率スコアは、悪意あるネットワークコンテンツのパケット中に特徴が存在する確率の２を底とする対数と、悪意なきネットワークコンテンツのパケット中に特徴が存在する確率の２を底とする対数の比を計算することにより求められる。相対確率因子は、次式で表される。

【００５０】

$$\log_2(P_{m|f}) = \log_2(P_{f|m}) / \log_2(P_{f|n}) \qquad (式１)$$

【００５１】

$\log_2(P_{m|f})$の値の大きさ（すなわち悪意あり確率スコア）は、不審なネットワークコンテンツが悪意あるネットワークコンテンツを含む確率を示しうる。例えば、１１という計算結果は、悪意あるネットワークコンテンツ内における特徴の現れやすさが、悪意なきネットワークコンテンツ内の場合よりも約２０００倍大きいことを示しうる。同様に、１２という計算結果は、悪意あるネットワークコンテンツ内における特徴の現れやすさが約４０００倍であることを示しうる。

【００５２】

幾つかの実施形態においては、悪意ありコーパスと悪意なしコーパスの少なくとも一方が、モニタされるネットワークデータ通信量に応じて連続的に更新されうる。また特徴に関連付けられた悪意あり確率スコアが、コーパスの更新に応じて連続的に更新されうる。

他の実施形態においては、特徴が特定される際に参照するためのルックアップテーブルに予め計算された悪意あり確率スコアが保存される前に、コーパスが生成および使用されうる。悪意あるネットワークコンテンツの顕著な確率に関連付けられた特徴は、コーパスの変更に伴って変更しうる。

【００５３】

ステップ３２５においては、ステップ３２０で計算された特徴の悪意あり確率スコアが分析閾値に達した場合、悪意あるネットワークコンテンツが特定あるいはフラグ立てされうる。分析閾値は、１、１０、３０、６０、１００、１０００、２０００、あるいはより

大きな数を上回る値とされうる。分析閾値は、予め設定されうる。あるいは悪意あるネットワークコンテンツの検出システム１２５の動作条件に基づいて可変とされうる。悪意あり確率スコアが分析閾値に達しなかった場合、悪意あり確率スコアに関連付けられた特徴に対して何も行なわれなくともよい。あるいは、分析が次のステップに進行しうる。例えば、仮想マシン（例えば仮想マシン２１５）による処理を通じた分析を行なうステップ３３０に進行しうる。

幾つかの実施形態においては、優先度を各特徴とパケット全体の少なくとも一方に割り当てるために、ステップ３２０で計算された全ての悪意あり確率スコアが、分析閾値と比較されうる。優先度は、様々な因子に基づいて計算されうる。因子の例としては、パケット内で特定された特徴の数や、パケット中の特徴に係る悪意あり確率スコアの最大値、平均値、中間値などが挙げられる。

【００５４】

分析閾値は、悪意あるネットワークコンテンツの検出システム１２５の動作条件に基づいて適応可能とされうる。あるいは当該動作条件に基づいて頻繁に更新されうる。

例えば、閾値は、検査されるネットワークコンテンツのパケット量に応じて動的に更新されうる。ステップ３１０においてネットワークデータ送信からインターセプトやコピーがされるデータパケット量が増えると、検査されるデータパケットの量も増える。これにより演算負荷が増加し、データパケットのより詳細な分析のために利用可能な演算帯域幅を大きくできない。したがって、より詳細な分析のために利用可能な演算帯域幅の減少を補うために、閾値が大きくされうる。

別例として、閾値は、より詳細な分析に用いられる少なくとも１つの仮想マシンの利用可能性に応じて動的に更新されうる。閾値は、悪意あるネットワークコンテンツを示す顕著な可能性を有する特徴のみが仮想マシンを用いて処理されるように、設定されうる。例えば、１０００を超える特徴のうち、５０未満が顕著とみなされうる。

【００５５】

複数の動的適応性のある閾値が用いられうる。それらは相互に同期されうる。例えば、スケジューラ１４０は、待ち行列に入れられた不審なネットワークコンテンツを処理するために割り当てられるべき仮想マシンを決定するために、閾値を用いうる。スケジューラ１４０の閾値は、仮想マシンを実行することによる分析環境１５０用に利用可能な演算リソースの不足によって大きくなりうる。ヒューリスティックモジュール１３０は、特定された特徴に経験則が適用可能かを判断するために、別の閾値を用いうる。ヒューリスティックモジュール１３０の閾値は、特定された特徴の悪意あり確率スコアに基づきうる。スケジューラ１４０の閾値が大きくなると、ヒューリスティックモジュール１３０の閾値も大きくなりうる。これは、特定された特徴に対して運用中の経験則に基づいて不審なネットワークコンテンツにフラグを立てることが適切でないためである。また、スケジューラ１４０の演算リソースの非効率的な使用は、スケジューラ１４０内の閾値が増すことにより、仮想マシンにおける不審なネットワークコンテンツを処理しない。

【００５６】

ステップ３２５において、さらなる分析のために不審なネットワークコンテンツにフラグが立てられた後、当該不審なネットワークコンテンツを含む保存されたデータフロー全体が再分析されうる。データフロー内の特徴が閾値よりも大きな悪意あり確率スコアを有することが見出されることにより、各特徴は、より高い悪意あり確率スコアを与えられうる。

データフロー中に見出された各特徴の優先度は、高められうる。不審なネットワークコンテンツに関わるドメインに関連付けられた全てのデータパケットおよびデータフローは、キャッシュされ、そうでない場合よりも高い優先度と悪意あり確率スコアが与えられうる。

スケジューラ１４０は、データフローにおいてフラグが立てられた不審なネットワークコンテンツの各々を処理するために、仮想マシンを実行しうる。当該処理は、個別に、優先度の順に、元の登場順に、あるいはその他の順序にしたがって行なわれうる。仮想マシ

ンは、より優先度の高いものに割り込まれるまでは、目前の不審なネットワークコンテンツを処理しうる。

【００５７】

ステップ３３０においては、不審なネットワークコンテンツを処理するために仮想マシンが実行される。仮想マシンは、当該マシン上で動作するウェブブラウザにおける不審なネットワークコンテンツを、効果的にリプレイしうる。

ヒューリスティックモジュール１３０は、当該不審なネットワークコンテンツを含むパケットを、当該パケット中に存在する特徴のリストおよび各特徴に対応付けられた悪意あり確率スコアとともに、スケジューラ１４０に提供しうる。

あるいは、ヒューリスティックモジュール１３０は、当該不振なネットワークコンテンツを含むパケットを示すポインタを、スケジューラ１４０に提供しうる。これによりスケジューラ１４０は、ヒューリスティックモジュール１３０と共有するメモリを経由して当該パケットにアクセスしうる。

別の実施形態においては、ヒューリスティックモジュール１３０が、パケットに係る識別情報をスケジューラ１４０に提供しうる。これによりスケジューラ１４０、リプレイヤ２０５や仮想マシンが、必要に応じて当該パケットに係るデータについて、ヒューリスティックモジュール１３０にクエリを行ないうる。

【００５８】

またヒューリスティックモジュール１３０は、パケットの優先度と当該パケット中に存在する特徴の少なくとも一方を提供しうる。次いでスケジューラ１４０は、仮想マシンを仮想マシンプール１４５からロードして構成を行ない、不審なネットワークコンテンツを処理するために当該仮想マシンを分析環境１５０に割り当てうる。仮想マシンは、最小限の量の処理を実行するように、あるいは最小限の時間（４５秒など）だけ動作するように構成されうる。当該最小限の時間が経過すると、仮想マシンは、別の仮想マシンを割り当てるためのスケジューラ１４０による割り込みを受けうる。複数の仮想マシンが同時に動作しうる。

【００５９】

スケジューラ１４０は、ヒューリスティックモジュール１３０により提供された優先度に応じて、どの特徴を最初に処理するかを選択しうる。スケジューラ１４０は、分析環境１５０において既に別の特徴、パケット、あるいはパケット群のセットを処理あるいは分析している別の仮想マシンを、ロードされた仮想マシンの割り当てに先立って終了させうる。例えば、別の特徴を処理している別の仮想マシンにより演算リソースが占有され、ロードされた仮想マシンを実行できないことがある。スケジューラ１４０は、仮想マシンに処理されている特徴の優先度、仮想マシンが既にどれくらいの時間を処理に費やしているか、あるいはその他の理由に基づいて、終了させる仮想マシン（群）を選択しうる。

【００６０】

スケジューラ１４０は、新たに特定された不審なネットワークコンテンツに基づいて、仮想マシンに処理されるべく既に待ち行列にある不審なネットワークコンテンツの優先順位を変更しうる。例えば、新たに特定された不審なネットワークコンテンツと共通に特定されたドメインが存在する場合、既に待ち行列に入れられた不審なネットワークコンテンツの優先順位が変更されうる。多くの不審なネットワークコンテンツが単一のドメインに関連付けられている場合、当該ドメインに関連付けられている全てのネットワークコンテンツの優先度を高くできる。

【００６１】

分析環境１５０におけるリプレイヤ２０５は、仮想マシンにより要求されたネットワークコンテンツの記録をとりうる。既にスケジューラ１４０の待ち行列にある不審なネットワークコンテンツが要求され、先に割り当てられた他の不審なネットワークコンテンツを処理しつつ、当該順番待ちの不審なネットワークコンテンツが処理される場合、および順番待ちの不審なネットワークコンテンツが悪意ありとみなされなかった場合、スケジューラ１４０は、当該順番待ちの不審なネットワークコンテンツを待ち行列から削除しうる。

このようにして、演算要求が削減されうる。ある不審なネットワークコンテンツは、別の不審なネットワークコンテンツにその都度参照されるのではなく、一度だけ仮想マシンで処理されるためである。

【００６２】

ステップ３３５においては、不審なネットワークコンテンツが検出される。検出は、当該不審なネットワークコンテンツに対する仮想マシンの応答を分析することにより行なわれる。分析環境１５０は、不審なネットワークコンテンツが実際に悪意あるネットワークコンテンツであるかを識別すべく仮想マシンをモニタするように構成されうる。分析環境１５０は、異常なメモリアクセス、実行可能な処理の異常な生成、異常なネットワーク通信、クラッシュ、異常な動作の変化などについて、仮想マシンをモニタしうる。分析環境１５０は、監視された仮想マシンの挙動に応じて、不審なネットワークコンテンツに悪意あるネットワークコンテンツであることを示すフラグを立てうる。

【００６３】

仮想マシンが悪意あるネットワークコンテンツを検出することなく、不審なネットワークコンテンツの処理時間が所定量を上回った場合、スケジューラ１４０は、演算リソースを解放するために当該仮想マシンを終了させうる。所定量の時間は、仮想マシンによる処理を待つ不審なネットワークコンテンツの待ち行列、不審なネットワークコンテンツが悪意あるネットワークコンテンツである確率、利用可能な演算リソースなどに応じて可変とされうる。所定量の時間の長さとしては、４５秒、２分などが挙げられる。

【００６４】

不審なネットワークコンテンツが悪意あるネットワークコンテンツと判定されると、悪意あるネットワークシステムの検出システム１２５は、当該悪意あるネットワークコンテンツについて、報告と将来参照するための記録の少なくとも一方を行ないうる。例えば、悪意あるネットワークコンテンツの検出システム１２５は、検出されたネットワークコンテンツのパケットが悪意あるネットワークコンテンツを含む旨の警告を生成しうる。悪意あるネットワークコンテンツの検出システム１２５は、悪意あるネットワークコンテンツを、サーバ装置１０５を運用担当する者に報告しうる。

悪意あるネットワークコンテンツがサーバ装置１０５に由来するものであると判断された場合、クライアント装置１１０は、サーバ装置１０５とのネットワーク通信を継続しないように指示されうる。サーバ装置１０５を担当する者が既知の場合、悪意あるネットワーク装置の検出システム１２５は、悪意あるネットワークコンテンツを、当該サーバ装置１０５を担当する者に報告しうる。当該サーバ装置１０５は、悪意あるネットワークコンテンツの提供者リストに加えられ、以降の当該サーバ装置１０５からの宛先を指定されたネットワーク通信がブロックされうる。

【００６５】

図４は、別例として、悪意あるネットワークコンテンツを検出する方法４００を示す。方法４００は、ヒューリスティックモジュール１３０により実行されうる。方法４００においては、ネットワークコンテンツのパケットが、悪意あるネットワークコンテンツの存在を示す特徴を特定すべく検査される。方法４００は、単一パスのパーサと拡張有限オートマトンの少なくとも一方の使用を含みうる。これにより状態のスタックを維持できる。方法４００は、文字列「ＨＴＴＰ」が識別された後の文字で始まるデータパケットの処理を開始しうる。

【００６６】

ステップ４０５においては、データ文字がデータパケットから読み出される。読み出されたデータ文字は、有力なキーワード、方法３００について説明した有力な特徴、あるいは異なる種類のデータ（例えばＨＴＭＬコンテンツに埋め込まれたジャバスクリプトコンテンツ）の始まりを示しうる。そのようなデータ文字は、例えば開き括弧「＜」を含みうる。読み出されたデータ文字がキーワードや特徴の始まりを示す場合、方法４００はステップ４１５に進みうる。それ以外の場合、方法４００はステップ４２０に進みうる。

【００６７】

ステップ４１５においては、方法４００がキーワードや特徴の始まりに遭遇したことを示すべく、新規の状態が状態のスタックに加えられる。新規の状態は、方法４００がキーワード処理の最中であることを示すInKeyword状態とされうる。読み出された文字に応じて、異なる新たな状態がスタックに加えられうる。最後に読み出された文字や次に読み出される文字で始まる文字列が保存されうる。方法４００は、次にステップ４４０に進む。

【００６８】

ステップ４２０においては、ステップ４０５で読み出されたデータ文字が、キーワードあるいは方法３００を参照して説明した特徴の終わりを示すものであるかを判断すべく評価される。そのようなデータ文字は、例えば閉じ括弧「＞」を含みうる。読み出されたデータ文字がキーワードや特徴の終わりを示す場合、方法４００はステップ４２５に進みうる。それ以外の場合、方法４００はステップ４４０に進みうる。

【００６９】

ステップ４２５においては、データパケットに適用される経験則が特定され、読み出された文字列（ステップ４１０で特定されたデータ文字で始まり、ステップ４２０で特定されたデータ文字列で終わるもの）に基づいて適用される。ヒューリスティックモジュール３００は、文字列を保存しうる。文字列は、キーワードに基づいてデータパケットに適用されうる少なくとも１つの経験則を決定すべく、経験則データベース１３５に保存された文字列のデータベースと比較されうる。

幾つかの実施形態においては、経験則の適用結果のリストが作成されうる。結果のリストは、ステップ４４５において参照できるように保存されうる。

【００７０】

パケットに適用されうる経験則は、例えばキーワードマッチングを含みうる。幾つかのキーワードは、悪意なきネットワークコンテンツよりも悪意あるネットワークコンテンツとの関連が高いとされ、ネットワークコンテンツのパケットにおける当該キーワードの存在は、当該パケットが不審なネットワークコンテンツを含む旨を示しうる。

【００７１】

経験則の一例においては、ピリオドに続くオブジェクトファイル名の拡張子が分析されうる。例えば、「．ｉｎｉ」、「．ａｎｒ」や「．ｈｔｍ」の文字で終了するファイル名は不審であるとみなされうる。また、通常はあるファイル形式に関連付けられているが、別のファイル形式を参照するように関連付けられているファイル名は、不審であるとみなされうる。例えば、「．ｊｐｇ」の文字で終わるのに画像ファイルを参照しないファイル名は、不審であるとみなされうる。

【００７２】

経験則の別例においては、ネットワークコンテンツが不審であるかを判断すべく、ウェブページのコンテンツが分析されうる。例えば、幅と高さの少なくとも一方が０か１ピクセルであるような小さなインラインフレームがウェブページ内に存在する場合、不審であるとみなされうる。

【００７３】

さらに別例に係る経験則は、ジャバスクリプトのコードシーケンスに関連付けられうる。「eval(unescape(…))」というジャバスクリプトのコマンドシーケンス（「eval」コマンドの引数内にネストされた「unescape」コマンド）がデータパケット内に検出されると、当該経験則は、不審なネットワークコンテンツを特定すべく、当該コマンドシーケンスを評価しうる。「eval(unescape(…))」というコマンドシーケンスは、悪意あるネットワークコンテンツを見つけにくくするために用いられうる。これにより、ネットワークデータ通信において悪意あるネットワークコンテンツが検出されにくくなる。したがって、「eval(unescape(…))」というコマンドシーケンスは、不審なネットワークコンテンツを示唆しうる。

【００７４】

さらに別例に係る経験則は、「unescape」や他のジャバスクリプト関数の引数の長さ（始めの文字から終わりの文字までの長さ）に係る。「unescape」や他の関数名の後の開き

丸括弧と閉じ丸括弧の間の文字数を数えるか、時間を測定することにより、上記の長さが特定されうる。丸括弧間の文字数が多い場合、難読化されたコマンド本体が用いられていることを示唆しうる。

【００７５】

さらに別例に係る経験則として、バイグラム検出がジャバスクリプトや他のネットワークコンテンツに用いられうる。バイグラム検出においては、ネットワークコンテンツ内における文字遷移が分析される。データの評価に伴い、条件確率テーブルが生成および連続的に更新されうる。条件確率テーブルは、１文字目の後に現れる２文字目の確率を示す。ある１文字目Ｃ１に対する２文字目Ｃ２の確率は、Ｐ（Ｃ２｜Ｃ１）と書き表されうる。経験則は、条件確率テーブルに基づいて、普通でない遷移をする文字列の出現を特定しうる。

普通でない遷移をする文字列の長さに係る閾値が、文字遷移が普通でない旨のフラグを立てる条件確率の値との組合せで予め設定されうる。当該設定は、悪意あるネットワークコンテンツのコーパスおよび悪意なきネットワークコンテンツのコーパスを用いるベイズ確率論分析に基づく。当該閾値は、条件確率テーブルの更新に伴い、ほぼリアルタイムで調節されてもよい。例えば、普通でない遷移をする長い文字列は、ジャバスクリプトの「eval(unescape(…))」節における悪意あるネットワークコンテンツの存在を示唆しうる。

【００７６】

他の経験則よりも誤検出率を下げるために用いられる経験則の別例として、ドメインプロフィールが用いられる。ドメインプロフィール経験則は、悪意あるネットワークコンテンツの検出に係るスループットを向上し、演算負荷を低減するために、他の経験則と連携して用いられうる。監視対象であるネットワークがやり取りされるネットワークドメインの各々は、分類され、当該ネットワークドメインに関連付けられたネットワークコンテンツ内に存在する特徴のリストにより注釈付けがなされうる。

別の経験則によりある特徴が特定されると、当該特徴は、当該ネットワークドメインに関連付けられた特徴のリストが参照されうる。当該特徴が当該ネットワークドメインに関連するものとしてリストされており、当該ドメインに関連付けられたネットワークコンテンツ内の特徴の特定により悪意あるネットワークコンテンツが過去に検出されていない場合、当該ネットワークドメインに関連付けられた特徴を含むネットワークコンテンツを処理するために仮想マシンが実行されなくてもよい。一方、当該特徴が過去に検出されたか当該ネットワークドメインに関連付けられていた場合、当該ネットワークコンテンツは悪意あるものと特定され、仮想マシンにより処理されうる。

【００７７】

悪意あるネットワークコンテンツを含むドメインやウェブサイトのリストは、維持されうる。悪意あるネットワークコンテンツのソースのリストは、コンピュータネットワーク上でホストされ、当該コンピュータネットワーク上のクライアントによりアクセス可能とされる。ヒューリスティックモジュール１３０は、ドメインプロファイル経験則により提供される情報を補うべく、悪意あるネットワークコンテンツを含むドメインやウェブサイトのリストにアクセスできる。

例えば、悪意あるネットワークコンテンツソースのリストにおける、ウェブサイトに関連付けられたネットワークコンテンツに係る閾値は、他のネットワークコンテンツに係る閾値よりも低く設定されうる。これに加えてあるいは代えて、悪意あるネットワークコンテンツの優先度は、他のネットワークコンテンツに係る優先度よりも高く設定されうる。悪意あるネットワークコンテンツが検出されると、他者により参照される情報とともに、ドメインリストが通知あるいは更新されうる。

【００７８】

ステップ４３０においては、ある状態が終了すると、当該終了した状態がスタックから削除される。終了した状態がInKeyword状態である場合、方法４００がもはやキーワード読み取り中でない旨を示すべく、当該InKeyword状態がスタックから削除されうる。ある状態が終了していなければ、その状態はスタックから削除されなくてもよい。

複数の状態がスタックに保存されうる。幾つかの実施形態においては、同時に３２個までの状態がスタックに存在しうる。例えば、ジャバスクリプトはＨＴＭＬに埋め込まれうる。したがって、ネストされた特徴を構成するために複数の状態が同時にアクティブとなりうる。様々な実施形態において、悪意あるネットワークコンテンツについて分析されるデータパケットに関連付けられた６０個を超える状態が存在しうる。

【００７９】

ステップ４３５においては、方法４００が新規の状態の処理中である旨を示すべく、当該新規の状態がスタックに加えられる。当該新規の状態は、最後に読み取られたキーワードによって、あるいは新たな種類のコンテンツを示す文字によって、特定されうる。例えば、方法４００が別キーワードの処理を待機中である旨を示すInBetweenKeyword状態が当該新規の状態でもよい。幾つかの実施形態においては、方法４００がジャバスクリプトセグメントの読み取り中である旨を示すInJavaScript状態が当該新規の状態でもよい。

当該状態は、ステップ４４５においてどの経験則が特定されてウェブデータのパケットに特定されるのかについて影響を与えうる。例えば、第１の状態がアクティブであれば第１の経験則が選択され、第２の状態がアクティブであれば第２の経験則が選択されうる。

【００８０】

ステップ４４０においては、データ文字がパケットの最後にあるかを判断すべく、ステップ４０５で読み取られた文字のカウントが評価される。データ文字がパケットの最後にある場合、方法４００はステップ４４５に進みうる。そうでない場合、方法４００はステップ４０５に進みうる。

【００８１】

ステップ４４５においては、データパケット内のどの特徴が仮想マシンを用いて処理されるかを決定すべく、ステップ４２５において経験則を適用することにより生成されたデータパケット内の特徴に係る結果のリストが参照される。その特徴が不審なネットワークコンテンツを示しているかを判断すべく、各特徴についての悪意あり確率スコアが閾値と比較されうる。データパケットと関連付けられた特徴には、優先順位が付与されうる。特徴は、データパケットおよび関連付けられたコンテンツを仮想マシンに割り当てるかどうかの優先順位をつけるために用いられうる。割り当て順序は、ステップ４２５で特定された順序、悪意あり確率スコアにより定められた優先度に基づく順序、その他の順序とされうる。

【００８２】

図５は、コントローラ５００の例を示す。コントローラ５００は、幾つかの実施形態に係る悪意あるネットワークコンテンツの検出システム１２５を備えうる。コントローラ５００は、少なくともプロセッサ５０５、メモリシステム５１０、ストレージシステム５１５を備えうる。これらの全てはバス５２０と結合されている。コントローラ５００は、通信ネットワークインターフェース５２５、入出力（Ｉ／Ｏ）インターフェース５３０、および表示インターフェース５３５も備えうる。通信ネットワークインターフェース５２５は、通信媒体５４０を介して通信ネットワーク１２０と結合しうる。

幾つかの実施形態においては、コントローラ５００がタップ（例えばタップ１１５）と結合しうる。この場合、当該タップを通じて通信ネットワーク１２０と結合する。

バス５２０は、通信ネットワークインターフェース５２５、プロセッサ５０５、メモリシステム５１０、ストレージシステム５１５、Ｉ／Ｏインターフェース５３０、および表示インターフェース５３５間の通信を提供する。

【００８３】

通信ネットワークインターフェース５２５は、他のデジタル装置（図示なし）と通信媒体５４０を介して通信しうる。プロセッサ５０５は、命令を実行する。メモリシステム５１０は、永続的にあるいは一時的にデータを保存する。メモリシステム５１０の例としては、ＲＡＭとＲＯＭが挙げられる。ストレージシステム５１５もまた、永続的にあるいは一時的にデータを保存する。ストレージシステム５１５の例としては、ハードディスクとディスクドライブが挙げられる。Ｉ／Ｏインターフェース５３０は、入力を受け付け、出

力をユーザに提供可能な任意の装置を含みうる。Ｉ／Ｏインターフェース５３０は、キーボード、マウス、タッチスクリーン、キーパッド、バイオセンサ、コンパクトディスク（ＣＤ）ドライブ、デジタル多用途ディスク（ＤＶＤ）ドライブ、フレキシブルディスクドライブを含みうるが、これらに限定されるものではない。表示インターフェース５３５は、ディスプレイ、モニタ、スクリーンを支持するように構成されたインターフェースを含みうる。幾つかの実施形態においては、コントローラ５００が、モニタを通じてユーザｃに表示されるグラフィカルユーザインターフェースを備えうる。ユーザは、当該グラフィカルユーザインターフェースによりコントローラ５００の制御が可能とされる。

【００８４】

他の実施形態によれば、悪意あるネットワークコンテンツは、悪意あるポータブルドキュメントフォーマット（ＰＤＦ）のネットワークコンテンツも含みうる。「悪意あるＰＤＦネットワークコンテンツ」という語が、ポータブルドキュメントフォーマット（ＰＤＦ）ファイルを含むことは明らかである。当該ＰＤＦファイルは、少なくとも１つのサーバ装置１０５に配置され、通信ネットワーク１２０を介して少なくとも１つのクライアント装置１１０に分配可能とされるものである。

【００８５】

一般的に、タップ１１５は、ＰＤＦネットワークコンテンツの取得要求をインターセプト可能とされうる。当該要求は、クライアント装置１１０に関連付けられたウェブブラウザ、ＰＤＦリーダなどのアプリケーション、そのようなＰＤＦネットワークコンテンツを要求するモジュールやエンジンより受信される。

幾つかの実施形態においては、少なくとも１つのクライアント装置１１０と少なくとも１つのサーバ装置１０５の間にタップ１１５が配置され、ＰＤＦネットワークコンテンツの取得要求を悪意あるネットワークコンテンツの検出システム６００（後に図６を参照して詳述する）へ送りうる。タップ１１５が複数のサーバ装置１０５間に配置され、当該サーバ装置１０５間でやり取りされるＰＤＦネットワークコンテンツをインターセプトする仕組みを提供しうることは明らかである。

【００８６】

背景として、ＰＤＦ文書のようなＰＤＦネットワークコンテンツは、ＰＤＦリーダアプリケーション（図示せず）によりパースされる際に当該ＰＤＦ文書に含まれるデータの視覚的表示を生成するレイアウト固定文書を含みうる。ＰＤＦ文書内のデータは、ヘッダに始まり、少なくとも１つのオブジェクトを示す情報を含む本体部と「ＸＲＥＦ」テーブルとしても知られる相互参照テーブル、およびトレーラを含むように、階層的に配置されている。ヘッダは、文書が貼り付けられるＰＤＦ仕様バージョン番号を示す情報を含む。バージョン番号は、ＰＤＦ文書をパースするために最適化されたＰＤＦ文書リーダのバージョンを特定するために用いられうる。

【００８７】

ＸＲＥＦテーブルは、ＰＤＦ文書中におけるオブジェクトの位置を示すオフセット情報を含む。その場合、ＸＲＥＦテーブルは、ＰＤＦリーダアプリケーションがＰＤＦ文書の各部分（ページなど）をパースやウォークできるようにする。このときＰＤＦリーダアプリケーションは、ＰＤＦ文書全体をパースやウォークする必要はない。最後に、ＰＤＦ文書のトレーラは、ＰＤＦアプリケーションがＸＲＥＦテーブルを他の適当なオブジェクトに対して効率的に配置できるようにする。当該他のオブジェクトは、上記視覚的表示を構成すべくＰＤＦリーダアプリケーションにより利用されうる。

【００８８】

本体部は、ＰＤＦ文書のコンテンツを備える少なくとも１つのオブジェクトを含みうる。一般に、ＰＤＦ文書のオブジェクトは、ブール演算子、数字、名前、文字列、配列、辞書、ストリーム、およびこれらの組合せを含みうるが、これらに限られるものではない。本体部は、メタデータ、セキュリティ機能などのトランスペアレントなオブジェクトも含みうる。

【００８９】

ＰＤＦ文書のオブジェクトは、概ね直接的か間接的のいずれかに分類されうる。直接的オブジェクトが、他のオブジェクトを参照できないことは明らかである。逆に間接的オブジェクトは、少なくとも１つのオブジェクトを参照しうる。当該参照されるオブジェクトは、直接的でも間接的でもよい。ＰＤＦ文書は、AcroForm要素やＸＭＬ形式データフォーマット（ＸＦＤＦ）要素のようなインタラクティブ要素も含みうる。AcroForm要素とＸＦＤＦ要素の双方は、ジャバスクリプトＡＰＩとしても知られるジャバスクリプトコードを含みうる。

【００９０】

ＰＤＦリーダアプリケーションとウェブブラウザアプリケーションの双方に存在する脆弱性を攻撃すべく、マルウェアがジャバスクリプトコードを利用するように構成されていることは明らかである。ＰＤＦリーダアプリケーションとウェブブラウザアプリケーションがプラグインを介して協働可能であることも明らかである。例えば、ウェブブラウザがＰＤＦ文書を要求すると、ＰＤＦリーダアプリケーションは、当該ＰＤＦ文書をパースすべく自動的に起動される。当該ＰＤＦ文書が、ジャバスクリプトコードを参照する少なくとも１つのオブジェクトを含んでいる場合、パース中に呼び出されるジャバスクリプトコードは、自身に関連付けられた機能を実行すべくウェブブラウザ内に仮想ＯＳを構成しうる。

【００９１】

ＰＤＦリーダアプリケーションとウェブブラウザアプリケーションによるプラグイン協働が顕著な利益（クライアント装置１１０のＯＳに依存しないクロスプラットフォーム互換性など）をもたらす一方、ウェブブラウザ内に多くの脆弱性が生成されうる。当該脆弱性は、クライアント装置１１０を異なる種類のマルウェアやウイルスなどに曝しうる。

【００９２】

幾つかの実施形態においては、ＰＤＦリーダアプリケーションの動作に割り当てられたメモリに悪意あるコードをロードする（しばしば「ヒープスプレー」と呼ばれる）ことにより、ジャバスクリプトコードがウェブブラウザアプリケーションにおける少なくとも１つの脆弱性を攻撃しうる。ヒープスプレーは、ＰＤＦリーダアプリケーションに割り当てられたメモリにシェルコードを作成するように構成されている。作成が済むと、脆弱性をトリガすべく脆弱なジャバスクリプトコードが呼び出され、当該シェルコードが実行され、ペイロードがもたらされる。「ペイロード」という語が、悪意あるネットワークコンテンツにより引き起こされるクライアント装置１１０にとって有害な影響を含むことは明らかである。悪意あるネットワークコンテンツにより引き起こされる有害な影響は、個別に記載するにはあまりに多すぎる。しかしながら、当業者であれば本明細書の開示に基づいて容易に理解できると思われる。有害な影響の例としては、メモリの消費、システムやプログラムファイルの上書きや破損などが挙げられるが、これに限られるものではない。

【００９３】

ＨＴＭＬ文書の場合、ＰＤＦ文書に添付された悪意あるネットワークコンテンツを示す不審性は、先に図１を参照して説明したヒューリスティックモジュール１３０を介して特定されうる。その場合、ヒューリスティックモジュール１３０は、経験則データベース１３５内にある経験則的手法のいずれか（あるいは組合せ）を利用しうる。

【００９４】

図６に示すように、幾つかの実施形態においては、ＰＤＦ文書に添付された悪意あるネットワークコンテンツを示す不審性は、悪意あるネットワークコンテンツの検出システム６００を介して特定されうる。悪意あるネットワークコンテンツの検出システム６００は、悪意あるネットワークコンテンツの検出システム１２５（図１参照）の各要素とともに、ＰＤＦパーサ６０５のような少なくとも１つの別モジュールを含みうる。ＰＤＦパーサ６０５は、悪意あるネットワークコンテンツを示す少なくとも１つの不審性がＰＤＦネットワークコンテンツに含まれているかを判断すべく、インターセプトなどを通じて受信したＰＤＦネットワークコンテンツを検査可能とされうる。「検査」という語が、ウォーク、パース、インスペクト、ビュー、コンパイル、リード、エクストラクト、デコードやこ

れらの組合せを含むものと理解されうることは明らかである。

【００９５】

悪意あるネットワークコンテンツの検出システム６００は、ＨＴＭＬファイルについて説明した方法（図４を参照して説明した悪意あるネットワークコンテンツを検出する方法４００など）を用いて悪意あるネットワークコンテンツを示す不審性を特定可能とされうる。またＰＤＦパーサ６０５は、ＰＤＦネットワークコンテンツに固有の悪意あるネットワークコンテンツを示す少なくとも１つの不審性を特定可能とされうる。例えば、ＰＤＦパーサ６０５は、特定種のジャバスクリプトコードを含むオブジェクトを検索すべく、ＰＤＦネットワークコンテンツの本体を検査可能とされうる。ウェブブラウザの脆弱性を攻撃するためによく用いられるジャバスクリプトコードの例としては、eval()、util.printf()、media.newPlayer()が挙げられるが、これに限られるものではない。

【００９６】

ＰＤＦネットワークコンテンツマルウェアの制作者は、マルウェアを参照するジャバスクリプトコードを複数のオブジェクトに分けることによって発見し難くしようと試みる場合がある。当該複数のオブジェクトは、ＰＤＦリーダアプリケーションによって参照されると、悪意あるコードを実行すべく結合されうる。したがって、ＰＤＦパーサ６０５は、getField()機能を利用して複数のオブジェクトにまたがる難読化された悪意あるジャバスクリプトコードを特定可能とされうる。

【００９７】

別の実施形態においては、ＰＤＦパーサ６０５は、ＲＣ４やＡＥＳ暗号化方式のようなソフトウェアストリーム暗号化を利用してＰＤＦネットワークコンテンツ内に暗号化された悪意あるジャバスクリプトコードを特定可能とされうる。

【００９８】

上述の例においては、ジャバスクリプトコードのような不審コンテンツの特定に対するＰＤＦパーサ６０５の適合可能性について考慮したが、ＰＤＦパーサ６０５は、他のオブジェクトに関連付けられた別種のマルウェアを特定可能とされうる。そのようなオブジェクトの例としては埋め込みフラッシュストリームオブジェクトが挙げられるが、これに限られるものではない。例えば、フラッシュファイルは、ActionScript仮想マシン指令を含みうる。当該指令は、ヒープスプレイをシェルコードでセットアップ可能である。別例として、悪意あるコードは、少なくとも１つのＴＩＦＦ（Tagged Image File Format）脆弱性を介してＰＤＦネットワークコンテンツに内蔵されうる。ＴＩＦＦ脆弱性がヒープスプレー機能を利用できないことは明らかである。

【００９９】

全てを列挙しているわけではないが、以下の機能は悪意あるネットワークコンテンツを含むＰＤＦネットワークコンテンツを示すものとされうる。

PDFBadVersion（ＰＤＦネットワークコンテンツに関連付けられたＰＤＦ仕様バージョン番号が正しいかを判断する）

PDFHeader1_0（ＰＤＦネットワーク文書のヘッダ情報のエラー、すなわち不正な形式のヘッダ情報であるかを検査する）

PDFNameJS（ジャバスクリプトコードを示すＪＳという文字を含む名前をＰＤＦオブジェクトが含んでいるかについてＰＤＦ文書を検査する）

PDFNameJavaScript（ジャバスクリプトコードを示すJavaScriptという文字を含む名前をＰＤＦオブジェクトが含んでいるかについてＰＤＦ文書を検査する）

PDFBadFileStart（不適切なファイルスタートシグネチャについてＰＤＦネットワークコンテンツを検査する）

PDFNameOpenAction（ＰＤＦコンテンツの初期ロードに際してジャバスクリプト機能を実行させるＰＤＦコンテンツについてＰＤＦネットワークコンテンツを検査する）

PDFCouldNotParse（ＰＤＦパーサがＰＤＦネットワークコンテンツを適切にパースできないかを判断する）

ＰＤＦパーサ６０５は、ＰＤＦネットワークコンテンツに含まれる少なくとも１つの不

審性を特定すべく、上記の機能やその組合せを利用できる。

【０１００】

ＰＤＦネットワークコンテンツにおける少なくとも１つの部分（ページなど）が、当該ＰＤＦネットワークコンテンツ全体をウォークやパースすることなくアセンブルされうることは明らかであり、ＰＤＦパーサ６０５は、クライアント装置１１０により要求されたＰＤＦネットワークコンテンツの一部のみを評価可能である。

【０１０１】

ＰＤＦパーサ６０５により検索された不審性の種別や量によらず、不審性がＰＤＦネットワークコンテンツの少なくとも一部に含まれると判断された場合、当該ＰＤＦネットワークコンテンツの少なくとも一部は、悪意あるネットワークコンテンツの検証のために少なくとも１つの仮想マシンに提供されうる。

【０１０２】

当該少なくとも１つの仮想マシンは、分析対象であるＰＤＦネットワークコンテンツのヘッダに含まれるＰＤＦ仕様バージョン番号に一部基づいて、仮想マシンプール１４５から選択されうる。

幾つかの実施形態においては、当該少なくとも１つの仮想マシンが、それぞれ拡張有限オートマトンを含みうる。これらの拡張有限オートマトンは、それぞれ異なる構成のコンピュータ読み取り可能な指令（ＯＳ指令、ウェブブラウザ指令、ＰＤＦリーダアプリケーション指令、と少なくとも１つのウェブブラウザをＰＤＦリーダアプリケーションと動作可能に結合させるプラグイン指令など）とともに、ＰＤＦネットワークコンテンツに悪意あるネットワークコンテンツが含まれているかを検証可能な別種のコンピュータ読み取り可能な指令を含みうる。

【０１０３】

幾つかの実施形態においては、複数（２以上）の拡張有限オートマトンの使用により、ＰＤＦネットワークコンテンツが様々なシステム構成にまたがって処理されうる。すなわち、ＯＳ指令、ウェブブラウザ指令、およびＰＤＦリーダアプリケーション指令が置き換えられうる。その場合、ある種のウェブブラウザアプリケーション内の脆弱性を攻撃することはないＰＤＦネットワークコンテンツが、別種のウェブブラウザアプリケーション内の脆弱性を攻撃するかが検証されうる。このような多面的分析は、特定バージョンのプログラムやアプリケーションの脆弱性を攻撃する悪意あるネットワークコンテンツがＰＤＦネットワークコンテンツ内に存在するかを検証しやすくする。

【０１０４】

拡張有限オートマトンの各々は、ＰＤＦネットワークコンテンツのクライアント装置１１０への影響を分析すべく、ＰＤＦネットワークコンテンツの受信、編集、実行、表示の少なくとも１つをシミュレートする分析環境１５０を含んでいる。例えば、分析環境１５０は、ＰＤＦネットワークコンテンツをサーバ装置１０５から要求するウェブブラウザを含みうる。当該ウェブブラウザは、ＰＤＦリーダアプリケーションに当該ＰＤＦネットワークコンテンツをパースさせる。当該ＰＤＦネットワークコンテンツが実際に悪意あるコード（ジャバスクリプト、フラッシュなど）を含んでいる場合、ウェブブラウザアプリケーションまたはＰＤＦリーダアプリケーションにおける少なくとも１つの脆弱性が当該悪意あるコードにより攻撃され、ペイロードがもたらされうる。ペイロードの影響は、直接的あるいは間接的に分析環境１５０内で観察されうる。

【０１０５】

分析環境１５０の例については、先に図２を参照して詳細に説明した通りであり、少なくとも１つの不審性を含むと判断されたＰＤＦネットワークコンテンツのパースの影響を観察可能とされうることは明らかである。

【０１０６】

幾つかの実施形態においては、悪意あるネットワークコンテンツの検出システム６００が、悪意あるネットワークコンテンツを含むと検証されたＰＤＦネットワークコンテンツに対してさらにインデックス付与を可能とされうる。インデックス付与は、当該ＰＤＦネ

ットワークコンテンツに識別子を関連付け、当該関連付けのなされたＰＤＦネットワークコンテンツを記録として少なくとも１つのデータベースに保存することにより行なわれる。当該識別子は、ＰＤＦネットワークコンテンツが取得される少なくとも１つのドメインを示す。当該データベースは、少なくとも１つのサーバ装置１０５と動作可能に結合される。

【０１０７】

データベースは、少なくとも１つの不審性を含むと判断されたＰＤＦネットワークコンテンツを、過去に悪意あるネットワークコンテンツを含むと検証されたＰＤＦネットワークコンテンツのインデックスと比較すべく、悪意あるネットワークコンテンツの検出システム６００により利用されうる。また、悪意あるネットワークコンテンツを含むと検証されたＰＤＦネットワークをホストしたと判断されたドメインに属する全てのＰＤＦネットワーク文書が、自動的にレビューされうる。ＰＤＦネットワークコンテンツの不審性についてさらなる検査は行なわれない。

【０１０８】

図７は、悪意あるネットワークコンテンツを検出する方法７００の例を示す。方法７００は、ＰＤＦネットワークコンテンツの少なくとも一部の要求を、タップ１１５を介してインターセプトするステップ７０５を含みうる。当該ＰＤＦネットワークコンテンツの少なくとも一部がウェブブラウザアプリケーションに受信される前に、タップ１１５がそれをインターセプトしうることは明らかである。

【０１０９】

次に方法７００は、悪意あるネットワークコンテンツを示す少なくとも１つの不審な機能や特性が当該ＰＤＦネットワークコンテンツの少なくとも一部に含まれているか判断すべく、当該ＰＤＦネットワークコンテンツの少なくとも一部を検査するステップ７１０を含みうる。前述のように、検査は、当該ＰＤＦネットワークコンテンツの少なくとも一部に添付された特定の機能や特定の脆弱なジャバスクリプトコードの存在を判断すべく、経験則やＰＤＦパーサを利用することを含みうる。

【０１１０】

方法７００は、ＰＤＦネットワークコンテンツの少なくとも一部を少なくとも１つの仮想マシン（拡張有限オートマトンとしても知られる）に提供するステップ７１５も含みうる。

【０１１１】

次に、当該ＰＤＦネットワークコンテンツの少なくとも一部を当該少なくとも１つの仮想マシンにおいて実行あるいはコンパイルすることにより、当該ＰＤＦネットワークコンテンツの少なくとも一部に悪意あるネットワークコンテンツが含まれるかが検証されうる（ステップ７２０）。当該ＰＤＦネットワークコンテンツの少なくとも一部のコンパイルは、脆弱なジャバスクリプトコードに、それと関連付けられた悪意あるネットワークコンテンツを実行させる。

【０１１２】

次に方法７００は、当該ＰＤＦネットワークコンテンツの少なくとも一部が実際に悪意あるネットワークコンテンツを含むかを判断すべく、少なくとも１つの仮想マシンの挙動を観測するステップ７２５を含みうる。悪意あるネットワークコンテンツの実行を示す挙動が観測される例としては、ＰＤＦリーダアプリケーションに割り当てられたメモリ内におけるヒープスプレーの生成、シェルコードの実行、メモリの消費、システムやプログラムファイルの上書きや破壊などが挙げられるが、これらに限定されるものではない。

【０１１３】

最後に方法７００は、悪意あるネットワークコンテンツを含むと検証されたＰＤＦネットワークコンテンツの少なくとも一部が要求元のクライアント装置に提供されることを阻止するステップ７３０を含みうる。

【０１１４】

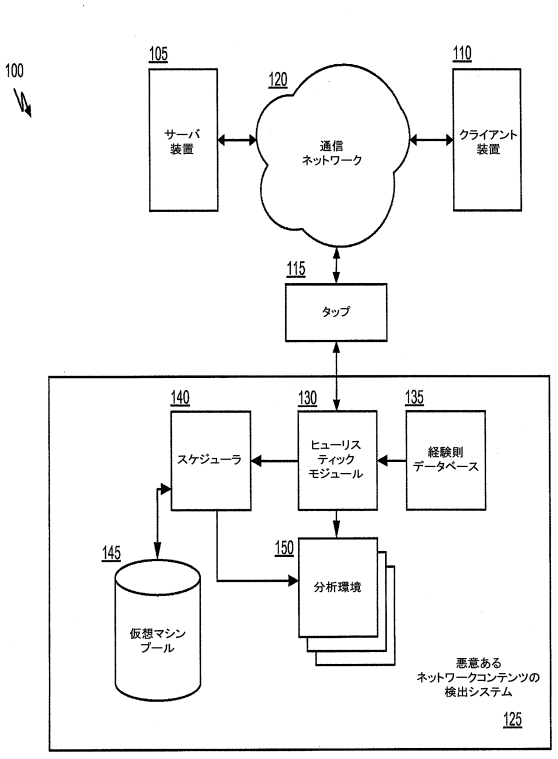
上記のモジュールは、記憶媒体（コンピュータ読み取り可能な媒体など）に保存された

命令群からなる。当該命令群は、プロセッサ（プロセッサ５０５など）により読出しと実行がなされうる。当該命令群の例としては、ソフトウェア、プログラムコード、およびファームウェアが挙げられる。記憶媒体は、例えばメモリ装置および集積回路を備える。当該命令群は、プロセッサにより実行されて利用可能とされ、当該プロセッサを本発明の実施形態に基づいて動作させる。当業者は、命令群、プロセッサ、および記憶媒体について精通している。

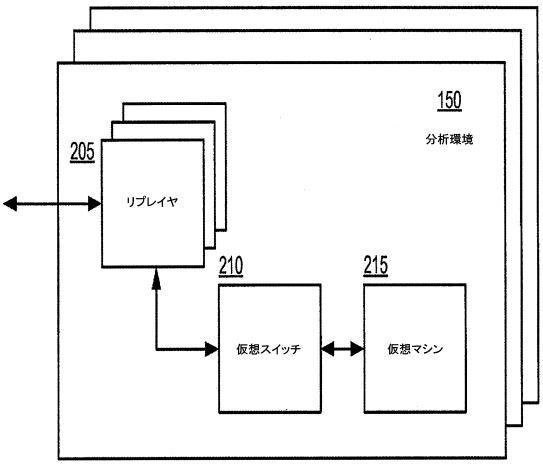
【０１１５】

これまで本明細書において特定の実施形態を参照しつつ本発明について記載したが、本発明がこれに限定されないことは当業者にとって明らかである。上述の発明に係る様々な特徴や態様は、独立してあるいは組み合わせて利用可能である。さらに、本発明は、背景にある思想と明細書の開示範囲を逸脱しない限りにおいて、明細書に記載された数を上回る環境やアプリケーションにおいて利用可能である。したがって、明細書と図面は、例示的なものであって限定的なものではない。ここで用いられている「備える」、「含む」、「有する」という語は、各要素を最低限含むこと（開放形式）を表す専門用語として読まれることを特に意図している。

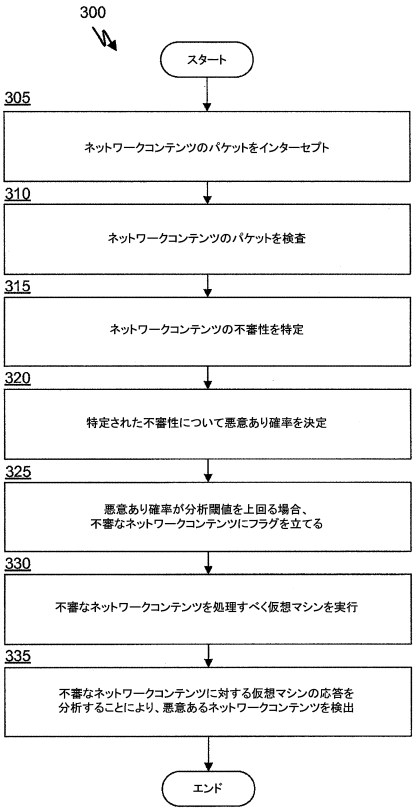
【図１】



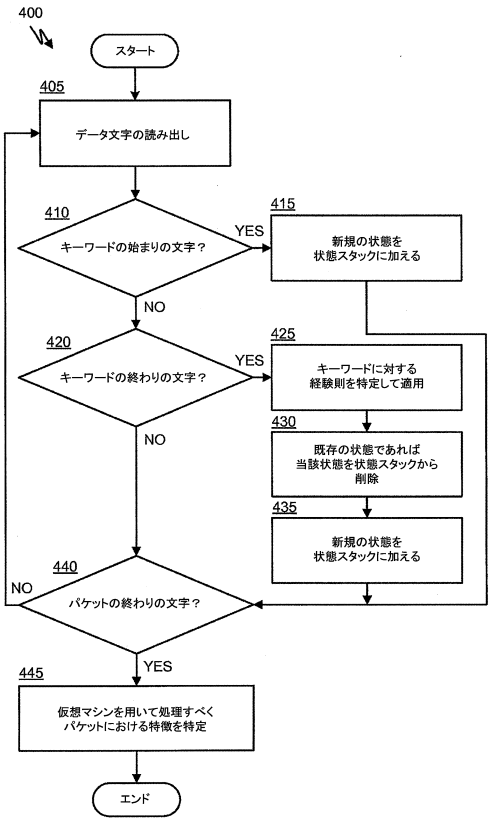
【図２】



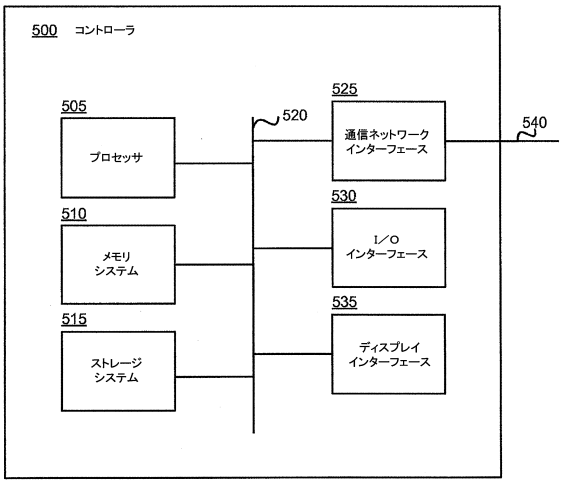
【図３】


300
スタート
305
ネットワークコンテンツのパケットをインターセプト
310
ネットワークコンテンツのパケットを検査
315
ネットワークコンテンツの不審性を特定
320
特定された不審性について悪意あり確率を決定
325
悪意あり確率が分析閾値を上回る場合、
不審なネットワークコンテンツにフラグを立てる
330
不審なネットワークコンテンツを処理すべく仮想マシンを実行
335
不審なネットワークコンテンツに対する仮想マシンの応答を
分析することにより、悪意あるネットワークコンテンツを検出
エンド

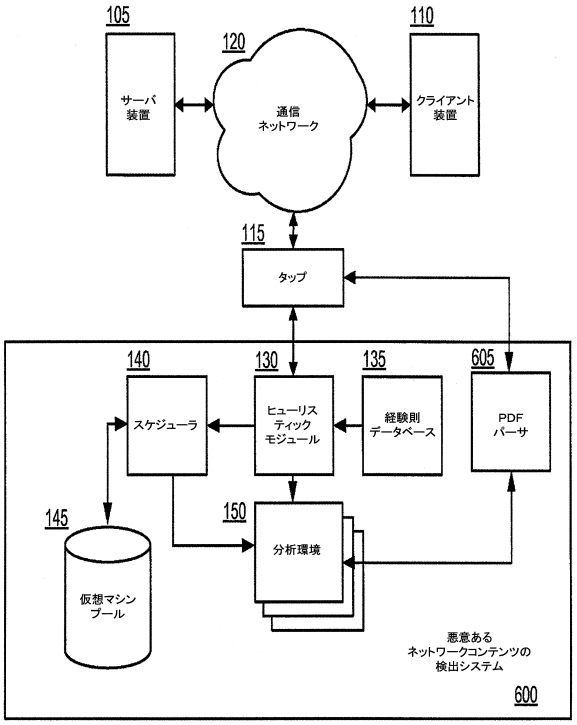
【図４】


400
スタート
405
データ文字の読み出し
410
キーワードの始まりの文字？
YES
415
新規の状態を
状態スタックに加える
NO
420
キーワードの終わりの文字？
YES
425
キーワードに対する
経験則を特定して適用
NO
430
既存の状態であれば
当該状態を状態スタックから
削除
435
新規の状態を
状態スタックに加える
440
NO
パケットの終わりの文字？
YES
445
仮想マシンを用いて処理すべく
パケットにおける特徴を特定
エンド

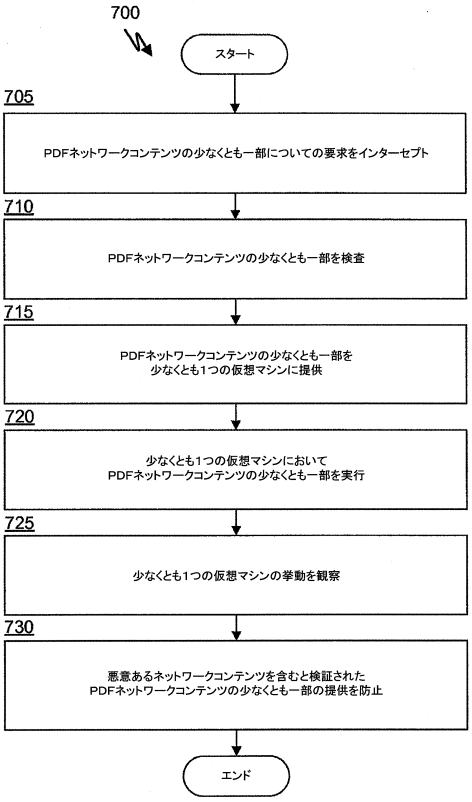
【図５】


500 コントローラ
505
プロセッサ
510
メモリ
システム
515
ストレージ
システム
520
525
通信ネットワーク
インターフェース
530
I／O
インターフェース
535
ディスプレイ
インターフェース
540

【図６】


105
サーバ
装置
120
通信
ネットワーク
110
クライアント
装置
115
タップ
140
スケジューラ
130
ヒューリス
ティック
モジュール
135
経験則
データベース
605
PDF
パーサ
145
仮想マシン
プール
150
分析環境
悪意ある
ネットワークコンテンツの
検出システム
600

【図７】


700
スタート
705
PDFネットワークコンテンツの少なくとも一部についての要求をインターセプト
710
PDFネットワークコンテンツの少なくとも一部を検査
715
PDFネットワークコンテンツの少なくとも一部を
少なくとも1つの仮想マシンに提供
720
少なくとも1つの仮想マシンにおいて
PDFネットワークコンテンツの少なくとも一部を実行
725
少なくとも1つの仮想マシンの挙動を観察
730
悪意あるネットワークコンテンツを含むと検証された
PDFネットワークコンテンツの少なくとも一部の提供を防止
エンド

フロントページの続き

(72)発明者　アジズ　アシャール
アメリカ合衆国，カリフォルニア州　９５０３５，ミルピタス，１３９０　マッカーシー　ブールバード

審査官　岸野　徹

(56)参考文献　米国特許出願公開第２０１０／０１１５６２１（ＵＳ，Ａ１）
特表２００８－５００６５３（ＪＰ，Ａ）
米国特許出願公開第２００６／００２１０２９（ＵＳ，Ａ１）
特開２０１０－２６２６０９（ＪＰ，Ａ）
特開２０１０－１４０２７７（ＪＰ，Ａ）
特開２００２－１０８６１０（ＪＰ，Ａ）
米国特許出願公開第２０１０／００６４３６９（ＵＳ，Ａ１）
米国特許出願公開第２０１１／０１５４４３１（ＵＳ，Ａ１）
鴨狩　裕紀　Yuki　Kamogari，転送ファイルの構造を考慮したアノマリ型侵入検知システムの提案　A Proposal of File Anomaly-based Intrusion Detection System，情報処理学会研究報告　平成２１年度▲６▼　［ＤＶＤ－ＲＯＭ］，日本，社団法人情報処理学会，２０１０年　４月１５日，pp.1-8
末安　泰三，Ｌｉｎｕｘレポート，日経Ｌｉｎｕｘ　第１３巻　第２号　NIKKEI Linux，日本，日経ＢＰ社　Nikkei Business Publications,Inc.，２０１１年　１月　８日，第13巻，pp.8-9
神薗　雅紀　Masaki　KAMIZONO，動的解析を利用したＰＤＦマルウェア解析システムの実装と評価　Development and evaluation of PDF malware analysis system using dynamic analysis，電子情報通信学会技術研究報告　Ｖｏｌ．１１０　Ｎｏ．４７５　IEICE Technical Report，日本，社団法人電子情報通信学会　The Institute of Electronics,Information and Communication Engineers，２０１１年　３月１８日，第110巻，pp.47-52

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／５６
Ｇ０６Ｆ　２１／５３