(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)公表番号
特表2024-542621
(P2024-542621A)
(43)公表日　令和6年11月15日(2024.11.15)

(51)国際特許分類　FI
G06F 21/55 (2013.01)　G06F 21/55
G06F 21/53 (2013.01)　G06F 21/53

審査請求　未請求　予備審査請求　未請求　（全30頁）

(21)出願番号　特願2024-531643(P2024-531643)
(86)(22)出願日　令和4年11月9日(2022.11.9)
(85)翻訳文提出日　令和6年5月28日(2024.5.28)
(86)国際出願番号　PCT/EP2022/081209
(87)国際公開番号　WO2023/099135
(87)国際公開日　令和5年6月8日(2023.6.8)
(31)優先権主張番号　17/457,467
(32)優先日　令和3年12月3日(2021.12.3)
(33)優先権主張国・地域又は機関
米国(US)
(81)指定国・地域　AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA,RW,SD,SL,ST,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(AL,AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,
最終頁に続く

(71)出願人　390009531
インターナショナル・ビジネス・マシーンズ・コーポレーション
ＩＮＴＥＲＮＡＴＩＯＮＡＬ ＢＵＳＩＮＥＳＳ ＭＡＣＨＩＮＥＳ ＣＯＲＰＯＲＡＴＩＯＮ
アメリカ合衆国１０５０４ ニューヨーク州 アーモンク ニュー オーチャード ロード
Ｎｅｗ Ｏｒｃｈａｒｄ Ｒｏａｄ， Ａｒｍｏｎｋ， Ｎｅｗ Ｙｏｒｋ １０５０４， Ｕｎｉｔｅｄ Ｓｔａｔｅｓ ｏｆ Ａｍｅｒｉｃａ
(74)代理人　100112690
弁理士　太佐 種一
最終頁に続く

(54)【発明の名称】　外部コンピュータ・システムに関する情報を取得する方法、システム、プログラム

(57)【要約】
外部コンピュータ・システムに関する情報を取得する方法が提供される。前記方法は外部コンピュータ・システムからリクエストを受信し、リクエストに応じて外部コンピュータ・システムを潜在的な脅威として分類したことに応答して、リクエストに応じたコンピュータ・ファイルが生成される。前記コンピュータ・ファイルは、外部コンピュータ・システムのプロセッサ上で実行された場合に、外部コンピュータ・システムに関する情報を取得するように設計された命令を含み、リクエストに応じてデータを用意し、前記データはコンピュータ・ファイルとともに外部コンピュータ・システムに送られ、コンピュータ・ファイルの命令に応じて生成される情報を受信し、コンピュータ・システムを保護する手段の開発向けに前記情報を提供するためにデータベースに記憶するように構成される。
（図５）

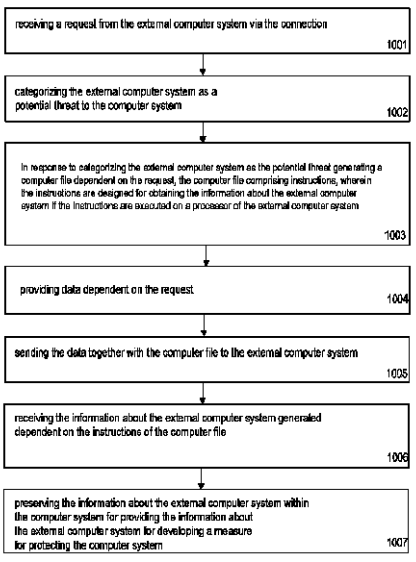


Fig. 5

【特許請求の範囲】
【請求項１】
コンピュータ・システムへの接続を有する外部コンピュータ・システムに関する情報を取得するためのコンピュータ実装方法であって、前記方法が、
－　前記接続を介して前記外部コンピュータ・システムからリクエストを受信することと、
－　前記外部コンピュータ・システムを、前記コンピュータ・システムに対する潜在的な脅威として分類することと、
－　前記外部コンピュータ・システムを前記潜在的な脅威として分類したことに応答して、前記リクエストに応じたコンピュータ・ファイルを生成することであって、前記コンピュータ・ファイルは命令を含み、前記命令は、前記外部コンピュータ・システムのプロセッサ上で実行された場合に前記外部コンピュータ・システムに関する前記情報を取得するように設計されている、前記生成することと、
－　前記リクエストに応じたデータを用意することと、
－　前記データを前記コンピュータ・ファイルとともに、前記外部コンピュータ・システムに送信することと、
－　前記コンピュータ・ファイルの前記命令に応じて生成された前記外部コンピュータ・システムに関する前記情報を受信することと、
－　前記コンピュータ・システムを保護するための手段の開発向けに、前記外部コンピュータ・システムに関する前記情報を提供するために前記外部コンピュータ・システムに関する前記情報を前記コンピュータ・システム内に保存することと、
を含む、コンピュータ実装方法。
【請求項２】
前記コンピュータ・システムが、前記データを提供するデータ・サーバを含み、前記接続がプロキシ・サーバによって確立され、前記方法が、
－　前記プロキシ・サーバによって前記リクエストを受信することと、
－　前記プロキシ・サーバによって前記リクエストを前記データ・サーバに方向付けることと、
－　前記リクエストに応じて、前記データ・サーバから前記プロキシ・サーバに前記データを送信することと、
－　前記プロキシ・サーバによって前記コンピュータ・ファイルを生成することと、
－　前記プロキシ・サーバから前記外部コンピュータ・システムへ、前記コンピュータ・ファイルとともに前記データを送信することと、
をさらに含む、請求項１に記載の方法。
【請求項３】
前記コンピュータ・システムがデータ・サービスを含み、前記リクエストに応じて前記データを前記用意することが、おとりモジュールによって前記データ・サービスを模倣することを含む、請求項１または２に記載の方法。
【請求項４】
前記方法が、
－　プロキシ・サーバによって前記接続を確立することと、
－　前記プロキシ・サーバによって前記リクエストを受信することと、
－　前記データおよび前記コンピュータ・ファイルをともに、前記プロキシ・サーバから前記外部コンピュータ・システムに送信することと
をさらに含む、請求項３に記載の方法。
【請求項５】
前記コンピュータ・ファイルが、前記プロキシ・サーバによって生成される、請求項４に記載の方法。
【請求項６】
前記方法が、おとりサーバを用意することをさらに含み、前記おとりサーバが、前記お

とりモジュールを含み、前記方法が、プロキシ・サーバから前記おとりサーバに前記リクエストを方向付けることと、前記プロキシ・サーバによって前記おとりサーバから前記データを受信することとをさらに含む、請求項２ないし５のいずれかに記載の方法。
【請求項７】
前記方法が、前記外部システムから一連のリクエストを受信することをさらに含み、前記リクエストが、前記一連のリクエストのうち最新のリクエストである、請求項１ないし６のいずれかに記載の方法。
【請求項８】
前記リクエストが前記外部コンピュータ・システムに関する初期情報を含み、前記コンピュータ・ファイルが前記外部コンピュータ・システムに関する前記初期情報に応じて生成される、請求項１ないし７のいずれかに記載の方法。
【請求項９】
前記方法が、前記外部コンピュータ・システムの分類を実行することをさらに含み、前記データを前記用意することが、前記外部コンピュータ・システムの前記分類の結果に応じて前記データを生成することを含む、請求項１ないし８に記載の方法。
【請求項１０】
前記方法が、前記外部コンピュータ・システムの分類を実行することをさらに含み、前記命令が前記外部コンピュータ・システムの前記分類の結果に応じて生成される、請求項１ないし９のいずれかに記載の方法。
【請求項１１】
前記外部コンピュータ・システムを前記潜在的な脅威として前記分類することが、人工知能モジュール（ＡＩモジュール）によって実行される、請求項１ないし１０のいずれかに記載の方法。
【請求項１２】
前記ＡＩモジュールが、ニューロン・ネットワークから構成される、請求項１１に記載の方法。
【請求項１３】
前記ＡＩモジュールが、規則ベースの決定モジュールから構成される、請求項１１に記載の方法。
【請求項１４】
前記外部コンピュータ・システムに関する前記情報が、前記外部コンピュータ・システムのブラウザ設定に関する情報を含む、請求項１ないし１３のいずれかに記載の方法。
【請求項１５】
前記外部コンピュータ・システムに関する前記情報が、前記外部コンピュータ・システムの中央処理装置に関する情報を含む、請求項１ないし１４のいずれかに記載の方法。
【請求項１６】
前記外部コンピュータ・システムに関する前記情報が、前記外部コンピュータ・システムのグラフィックス処理装置に関する情報を含む、請求項１ないし１５に記載の方法。
【請求項１７】
前記外部コンピュータ・システムに関する前記情報が、前記外部コンピュータ・システムのデータベースのデータを含む、請求項１ないし１６のいずれかに記載の方法。
【請求項１８】
前記方法が、前記外部コンピュータ・システムに関する前記情報に応じて、前記コンピュータ・システムを保護するための手段を開発し、実行することをさらに含む、請求項１ないし１７に記載の方法。
【請求項１９】
コンピュータ・システムへの接続を有する外部コンピュータ・システムに関する情報を取得するためのコンピュータ・プログラム製品であって、前記コンピュータ・プログラム製品が、１つまたは複数のコンピュータ可読記憶媒体と、前記１つまたは複数のコンピュータ可読記憶媒体に集合的に記憶されたプログラム命令とを含み、前記プログラム命令が

、
－　前記接続を介して前記外部コンピュータ・システムからリクエストを受信するためのプログラム命令と、
－　前記リクエストに応じて、前記外部コンピュータ・システムを前記コンピュータ・システムに対する潜在的な脅威として分類するためのプログラム命令と、
－　前記外部コンピュータ・システムを前記潜在的な脅威として分類したことに応答して、前記リクエストに応じたコンピュータ・ファイルを生成するためのプログラム命令であって、前記コンピュータ・ファイルは命令を含み、前記命令は、前記外部コンピュータ・システムのプロセッサ上で実行された場合に前記外部コンピュータ・システムに関する情報を取得するように設計されている、前記生成するためのプログラム命令と、
－　前記リクエストに応じたデータを用意するためのプログラム命令と、
－　前記データを前記コンピュータ・ファイルとともに、前記外部コンピュータ・システムに送信するためのプログラム命令と、
－　前記コンピュータ・ファイルの前記命令に応じて生成された前記外部コンピュータ・システムに関する前記情報を受信するためのプログラム命令と、
－　前記コンピュータ・システムを保護するための手段の開発向けに、前記外部コンピュータ・システムに関する前記情報を提供するために前記外部コンピュータ・システムに関する前記情報をデータベースに記憶するためのプログラム命令と、を含む、
コンピュータ・プログラム製品。
【請求項２０】
コンピュータ・システムへの接続を有する外部コンピュータ・システムに関する情報を取得するためのコンピュータ・システムであって、前記コンピュータ・システムが、
－　前記接続を介して前記外部コンピュータ・システムからリクエストを受信することと、
－　前記リクエストに応じて、前記外部コンピュータ・システムを前記コンピュータ・システムに対する潜在的な脅威として分類することと、
－　前記外部コンピュータ・システムを前記潜在的な脅威として分類したことに応答して、前記リクエストに応じたコンピュータ・ファイルを生成することであって、前記コンピュータ・ファイルが命令を含み、前記命令が、前記外部コンピュータ・システムのプロセッサ上で実行された場合に前記外部コンピュータ・システムに関する前記情報を取得するように設計されている、前記生成することと、
－　前記リクエストに応じたデータを用意することと、
－　前記データを前記コンピュータ・ファイルとともに、前記外部コンピュータ・システムに送信することと、
－　前記コンピュータ・ファイルの前記命令に応じて生成された前記外部コンピュータ・システムに関する前記情報を受信することと、
－　前記コンピュータ・システムを保護するための手段の開発向けに、前記外部コンピュータ・システムに関する前記情報を提供するために前記外部コンピュータ・システムに関する情報をデータベースに記憶することと、
を行うように構成されている、コンピュータ・システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本開示は、一般的には侵入検出システムの分野に関し、詳細には、外部コンピュータ・システムをコンピュータ・システムに対する脅威として分類した後に、その外部コンピュータ・システムに関する情報を取得するための方法に関する。
【０００２】
侵入検出システムは、保護されたシステムに向けられた攻撃者の実際のリクエストをリクエスト・データベースと比較することによって、潜在的な攻撃者を検出しようとすることがある。リクエスト・データベースは、保護されたシステムに向けられた他の攻撃者の

リクエストに関する情報を含むことがある。そうした他の攻撃者は、実際の攻撃者よりも先に保護されたシステムに侵入している可能性がある。

【発明の概要】

【０００３】

様々な実施形態は、独立請求項の主題によって説明されるように、外部コンピュータ・システムに関する情報を取得するためのコンピュータ・システムおよび方法を提供する。有利な実施形態は従属請求項に説明される。本開示の実施形態は、相互に排他的でなければ、自由に組み合わせることができる。

【０００４】

一態様において、本開示は、コンピュータ・システムへの接続を有する外部コンピュータ・システムに関する情報を取得するためのコンピュータ実装方法を含み、方法は以下を含む：

－　接続を介して外部コンピュータ・システムからリクエストを受信すること、

－　外部コンピュータ・システムを、コンピュータ・システムに対する潜在的な脅威として分類すること、

－　外部コンピュータ・システムを潜在的な脅威として分類したことに応答して、リクエストに応じたコンピュータ・ファイルを生成することであって、コンピュータ・ファイルは命令を含み、命令は、外部コンピュータ・システムのプロセッサ上で実行された場合に外部コンピュータ・システムに関する情報を取得するように設計されている、生成すること、

－　リクエストに応じたデータを用意すること、

－　データをコンピュータ・ファイルとともに、外部コンピュータ・システムに送信すること、

－　コンピュータ・ファイルの命令に応じて生成された外部コンピュータ・システムに関する情報を受信すること、

－　コンピュータ・システムを保護するための手段の開発向けに、外部コンピュータ・システムに関する情報を提供するために外部コンピュータ・システムに関する情報をコンピュータ・システム内に保存すること。

【０００５】

別の態様において、本開示は、コンピュータ・システムへの接続を有する外部コンピュータ・システムに関する情報を取得するためのコンピュータ・プログラム製品を含み、コンピュータ・プログラム製品は、１つまたは複数のコンピュータ可読記憶媒体と、１つまたは複数のコンピュータ可読記憶媒体に集合的に記憶されたプログラム命令とを含み、プログラム命令は、以下を含む：

－　接続を介して外部コンピュータ・システムからリクエストを受信するためのプログラム命令、

－　リクエストに応じて、外部コンピュータ・システムをコンピュータ・システムに対する潜在的な脅威として分類するためのプログラム命令、

－　外部コンピュータ・システムを潜在的な脅威として分類したことに応答して、リクエストに応じたコンピュータ・ファイルを生成するためのプログラム命令であって、コンピュータ・ファイルは命令を含み、命令は、外部コンピュータ・システムのプロセッサ上で実行された場合に外部コンピュータ・システムに関する情報を取得するように設計されている、生成するためのプログラム命令、

－　リクエストに応じたデータを用意するためのプログラム命令、

－　データをコンピュータ・ファイルとともに、外部コンピュータ・システムに送信するためのプログラム命令、

－　コンピュータ・ファイルの命令に応じて生成された外部コンピュータ・システムに関する情報を受信するためのプログラム命令、

－　コンピュータ・システムを保護するための手段の開発向けに、外部コンピュータ・システムに関する情報を提供するために外部コンピュータ・システムに関する情報をデー

タベースに記憶するためのプログラム命令。
【０００６】
別の態様では、本開示は、コンピュータ・システムへの接続を有する外部コンピュータ・システムに関する情報を取得するためのコンピュータ・システムを含み、コンピュータ・システムは以下を行うように構成される：
－　接続を介して外部コンピュータ・システムからリクエストを受信すること、
－　リクエストに応じて、外部コンピュータ・システムをコンピュータ・システムに対する潜在的な脅威として分類すること、
－外部コンピュータ・システムを潜在的な脅威として分類したことに応答して、リクエストに応じたコンピュータ・ファイルを生成することであって、コンピュータ・ファイルは命令を含み、命令は、外部コンピュータ・システムのプロセッサ上で実行された場合に外部コンピュータ・システムに関する情報を取得するように設計されている、生成すること、
－　リクエストに応じたデータを用意することと、
－　データをコンピュータ・ファイルとともに、外部コンピュータ・システムに送信すること、
－　コンピュータ・ファイルの命令に応じて生成された外部コンピュータ・システムに関する情報を受信すること、
－　コンピュータ・システムを保護するための手段の開発向けに、外部コンピュータ・システムに関する情報を提供するために外部コンピュータ・システムに関する情報をデータベースに記憶すること。
【図面の簡単な説明】
【０００７】
以下では、本開示の実施形態について、図面を参照しながら単なる例として、より詳細に説明する。
【０００８】
【図１】本発明の主題の一例による、コンピュータ・システムのプロキシ・サーバとコントローラ・サーバを概略的に示すブロック図である。
【０００９】
【図２】図１に示すコントローラ・サーバの構成要素を概略的に示すブロック図である。
【００１０】
【図３】図１に示すプロキシ・サーバの構成要素を概略的に示すブロック図である。
【００１１】
【図４】図１に示すコンピュータ・システムとネットワークとの接続を示すブロック図である。
【００１２】
【図５】外部システムに関する情報を取得するための方法のフローチャートである。
【発明を実施するための形態】
【００１３】
本開示の様々な実施形態の説明は、説明目的で提示されるが、網羅的であること、または開示される実施形態に限定されることを意図するものではない。説明される実施形態の範囲および趣旨から逸脱することなく、当業者には多くの修正および変形が明らかであろう。本明細書で使用される用語は、実施形態の原理、実用的な応用、もしくは市場で見られる技術に対する技術的改善を最良に説明するために、または本明細書で開示される実施形態を当分野の他の当業者が理解できるように選択された。
【００１４】
いくつかの実施形態におけるコンピュータ・システムは、パーソナル・コンピュータ・システム、サーバ・コンピュータ・システム、マイクロプロセッサベースのシステム、または、例えば携帯電話やネットワークＰＣのようなプログラマブル家電であってもよい。一例では、コンピュータ・システムは、複数のサーバなど、複数のコンピューティング・

デバイスのネットワークであってもよい。さらなる例によれば、コンピュータ・システムは、外部コンピュータ・システムに接続されているだけのスタンドアロンのコンピュータであってもよい。

【００１５】

リクエストは、外部コンピュータ・システム（以降、外部システムとも称する）によって生成され得る。リクエストは、ＨＴＴＰリクエスト「ＧＥＴ」または「ＨＥＡＤ」などの、ＨＴＴＰリクエストであり得る。例えば、外部コンピュータ・システムは、外部コンピュータ・システムのユーザ向けにウェブページを表示するためのウェブ・ブラウザ・ソフトウェアを実行することができる。ウェブページは、コンピュータ・システムのウェブサーバ上でホストされることもある。ＨＴＴＰリクエストは、ユーザが作成した入力データに応じて生成され得る。

【００１６】

入力データは、ユーザのアクションを記述し、それに応答して作り出すことができる。ユーザのアクションは、ウェブページのボックスをチェックすること、ウェブページのテキスト・フィールドにテキストを入力することなどを含むことがある。したがって、入力データは、外部システムのキーボードまたはマウスによって生成された電子信号の形態で受け取ることができる。一例によると、外部システムは、ユーザを模倣することで入力データを自動的に生成することができる自動化スクリプトを実行することができる。

【００１７】

リクエストは、例えばファイル名、ハイパーリンク、リクエストされたテーブルの名前、テーブルの列番号またはテーブルの行番号あるいはその両方など、データを指定するための情報を含むことができる。

【００１８】

外部システムは、ウェブ・ブラウザを実行するなどして、コンピュータ・ファイルとともに送信されたデータに応じたウェブページの更新版を表示することができる。データはリクエストに応じて用意されるため、このリクエストはそのデータ用のリクエストと説明することができる。データは、例えばログイン画面を表示するためのグラフィックを表示するためのデータを含むことができる。さらに、データは、機密データ（例えば、コンピュータ・システムの給与システムのデータ）または非機密データ（例えば、機密データの誤ったバージョン）あるいはその両方を含む場合がある。いくつかの実施形態では、データは、ウェブページの更新版がデータに応じて表示されるように設計されることがある。いくつかの実施形態では、ウェブページの更新版はデータを含むことがある。

【００１９】

コンピュータ・システムは、データを指定するための情報に応じたデータを用意することができる。例えば、コンピュータ・システムのプロセッサは、コンピュータ・システムのストレージからデータを読み込み、コンピュータ・システムのインターフェースにデータを送信することができる。ストレージは、データベース・サーバまたはおとりサーバのストレージであってもよい。一例によると、コンピュータ・システムは、リクエストに応じたデータを生成することができる。

【００２０】

外部システムとコンピュータ・システム間の接続は、インターネット、コンピュータ・システムのインターフェース、および外部システムのインターフェースを介して提供されることがある。一例では、コンピュータ・システムのインターフェースは、プロキシ・サーバを介して外部システムのインターフェースに間接的に接続されることがある。

【００２１】

コンピュータ・システムは、外部システムとコンピュータ・システム間の記録されたデータ・トラフィックに応じて、外部システムを潜在的な脅威として分類することができる。記録されたデータ・トラフィックは、リクエストを含むことがある。一例では、コンピュータ・システムは、リクエスト・データベースを使用して、外部システムをリクエストに応じて潜在的な脅威として分類することができる。リクエスト・データベースは、過去

にコンピュータ・システムに対する攻撃と分類されたリクエストのプロファイルを記憶することができる。一例では、コンピュータ・システムは、外部システムによって実行されたリクエストの履歴に応じて、外部システムを潜在的な脅威として分類することができる。リクエストの履歴には、過去の複数のリクエストおよび前述のリクエストが含まれることがある。リクエストの履歴には、ログイン・ページを表示するための数回、例えば１０回のリクエストが含まれることがある。同様に、リクエストの履歴は、コンピュータ・システムのウェブ・サービスの保護されたセクションへのログインを何度か試みることを含み得る。

【００２２】

いくつかの実施形態では、コンピュータ・システムは、コンピュータ・ファイルがリクエストに応答して要求されるデータから構成されるように、リクエストに応じたコンピュータ・ファイルを生成することができる。したがって、いくつかの実施形態では、コンピュータ・ファイルとともにデータを外部システムに送信することは、ファイルを外部システムに送信することによって実行され得る。したがって、このコンピュータ・ファイルは、リクエストに対するレスポンス・ファイルと考えることができる。

【００２３】

コンピュータ・ファイルは、外部システムのプロセッサが読み取り可能なファイルであってもよい。例えば、外部システムのプロセッサは、ウェブ・ブラウザを使用してウェブページを更新するためのコンピュータ・ファイルの一部としてデータを読み取ることができる。一例では、コンピュータ・ファイルはＨＴＭＬ文書であってもよい。ＨＴＭＬ文書は、データと命令から構成することができる。この命令は、スクリプト言語「Ｊａｖａ（Ｒ）Ｓｃｒｉｐｔ」のコマンドで構成されることもある。一例では、命令は、外部システムで実行されているアクションの追跡またはプロファイリングあるいはその両方に役立つことがある。一例では、命令は、外部システムの中央処理装置および／もしくはグラフィックス処理装置、および／もしくは外部システムのウェブ・ブラウザのブラウザ設定、またはその組合せについての情報を取得するための命令のセット、または外部システムのデータベースのデータを読み取るための命令のセット、あるいはその組合せのための命令セットを形成することができる。後者の場合、外部システムに関する情報は、外部システムのデータベースのデータを含むことがある。その結果、外部コンピュータ・システムに関する情報は、外部システムの中央処理装置および／またはグラフィック処理装置、および／または外部システムのウェブ・ブラウザのブラウザ設定、および／または外部システムのデータベースのデータ、あるいはその組合せに関する情報から構成される可能性がある。中央処理装置に関する情報は、外部システムが複数セットのプロセッサのラックから構成される高性能コンピューティング・マシンであることを示すことがある。この情報は、外部システムを不審なシステムとして識別するために使用される可能性がある。さらに、外部システムのウェブ・ブラウザのブラウザ設定に関する情報は、不審なウェブ・ブラウザのプラグインの使用を示すことがある。外部コンピュータ・システムに関する情報は、外部システムの指紋を含むこともある。指紋は、外部システムの識別に使用される一組の特性であることができる。一組の特性は、外部システムのブラウザのユーザ・エージェント識別情報、クッキー、ＩＰアドレス、またはユーザ・タイム・ゾーンあるいはその組合せを含むことがある。

【００２４】

命令のセットには、以下のようなコマンドが関与することがある：「ｎａｖｉｇａｔｏｒ．ｕｓｅｒＡｇｅｎｔ」、「ｗｉｎｄｏｗ．ｎａｖｉｇａｔｏｒ．ｈａｒｄｗａｒｅＣｏｎｃｕｒｒｅｎｃｙ」、「ｎａｖｉｇａｔｏｒ．ｂｕｉｌｄＩＤ」、「ｎａｖｉｇａｔｏｒ．ｃｌｉｐｂｏａｒｄ」、「ｎａｖｉｇａｔｏｒ．ｌａｎｇｕａｇｅ」、および「ｎａｖｉｇａｔｏｒ．ｍｅｄｉａＤｅｖｉｃｅｓ」。このように、外部システムに関する情報は、外部システムのプロセッサ上で命令のセットが実行されることによって生成される場合がある。

【００２５】

命令のセットは、外部システムからコンピュータ・システムまたはプロキシ・サーバへの外部システムに関する情報の送信を初期化するための命令を含むことができ、これは以降では「ｓｅｎｄ　ｂａｃｋ　ｉｎｓｔｒｕｃｔｉｏｎ」とも称される。このような命令は、以下のようなコマンドで構成され得る：例えば、「ＸＭＬＨｔｔｐＲｅｑｕｅｓｔ」、「ｎａｖｉｇａｔｏｒ．ｓｅｎｄＢｅａｃｏｎ」、「ｄｏｃｕｍｅｎｔ．ｂｏｄｙ．ａｐｐｅｎｄＣｈｉｌｄ（ｍｙＦｏｒｍ）」、「ｍｙＦｏｒｍ．ｓｕｂｍｉｔ（）」、「ｉｍｇ．ｓｒｃ」、および「ｉｆｒａｍｅ．ｓｒｃ」。

【００２６】

言い換えれば、命令は、命令のセットの実行が、外部システムに関する情報を取得し、外部システムに関する情報をコンピュータ・システムまたはプロキシ・サーバに送信することを引き起こすように設計することができる。

【００２７】

外部コンピュータ・システムに関する情報をコンピュータ・システム内に保存することは、この情報をデータベース、例えば侵入者データベースに記憶することによって行うことができる。侵入者データベースは、過去にコンピュータ・システムに対して攻撃を行った以前の外部コンピュータ・システム（以降、以前の外部システムとも称する）のプロファイルを含むことができる。

【００２８】

一例によれば、コンピュータ・システムに外部コンピュータ・システムに関する情報を保存することは、外部コンピュータ・システムに関する情報に応じて人工知能モジュール（ＡＩ－Ｍｏｄｕｌｅ）を訓練することによって実行することができる。訓練には、ＡＩモジュールのパラメータ値を外部コンピュータ・システムに関する情報に適合させることを含むことができる。この例によれば、外部コンピュータ・システムに関する情報は、ＡＩモジュールのパラメータの適合値の形態で保存され得る。この場合、外部コンピュータ・システムに関する情報は、ＡＩモジュールの入力データセットおよびＡＩモジュールのパラメータの適合値に応じて、ＡＩモジュールの出力データセットを生成することによって提供することができる。

【００２９】

いくつかの実施形態の１つの特徴および利点は、外部システムに関する情報が、コンピュータ・システムの外部、すなわち外部システム上で実行されるアクションによって取得できることである。このようなアクションは、外部システムに関する情報を取得するための命令のセットを実行することを含む。一般に、命令は外部システムのプロセッサによって実行され得る。これにより、外部システムからコンピュータ・システムに送信されたリクエストに基づいてのみ外部システムに関する情報を取得する方法に比べて、コンピュータ・システムが外部システムから攻撃されるリスクを低減できる可能性がある。さらに、コンピュータ・ファイルとともにデータを送信することで、外部システムによってこの命令をマルウェアとして発見することができない状況を作ることができる。この効果は、コンピュータ・ファイルが命令を含む場合、より高まる可能性がある。

【００３０】

外部コンピュータ・システムを潜在的な脅威として分類することに応答してコンピュータ・ファイルを生成することは、外部コンピュータ・システムが潜在的な脅威として分類されない場合、コンピュータ・ファイルが生成されず、外部システムに送信されないことを意味し得る。その結果、コンピュータ・システムと、コンピュータ・システムに対する潜在的な脅威として各々分類されないさらなる外部システムとの間のデータ・トラフィックの量は、一般には分類を行うことによって減少する可能性がある。分類が実行されなかった場合、命令を含むコンピュータ・ファイルは通常、さらなる外部システムに関する情報を得るために、コンピュータ・システムからの情報を要求するさらなる外部システムにデフォルトで送信される。これは、コンピュータ・システムとさらなる外部システムとの間のデータ・トラフィックを増大させることになる。それに加えて、さらなる外部システムに関する情報は、コンピュータ・システムを保護することに関連性がないかも知れない

。さらなる外部システムは、コンピュータ・システムの既知のユーザのコンピュータ・システムであってもよい。

【００３１】

一実施形態によれば、方法は、外部コンピュータ・システムに関する情報に応じて、コンピュータ・システムを保護するための手段を開発し、実行することをさらに含むことができる。この手段は、外部システムに関する情報の分析を実行することに応答して、外部システムをコンピュータ・システムから切り離すことを含むことができる。コンピュータ・システムのコントローラ・ノードは、外部システムに関する情報の分析を実行することができる。分析を実行することは、外部コンピュータ・システムに関する情報と、侵入者データベースによって与えられた情報との比較を実行することを含む場合がある。

【００３２】

さらなる例によれば、訓練されたＡＩモジュールは、将来的な外部コンピュータ・システムを潜在的な脅威として認識するために使用することができる。代替的に、または追加的に、将来的な外部コンピュータ・システムの情報は、将来的な外部コンピュータ・システムを潜在的な脅威として認識するために、侵入者データベースによって与えられた情報と比較されることがある。将来的な外部コンピュータ・システムの１つを潜在的な脅威として認識することに応答して、コンピュータ・システムはその将来的な外部コンピュータ・システムを切り離すことができる。このことは、外部コンピュータ・システムに関する情報に依存してコンピュータ・システムを保護するための手段の一例であろう。

【００３３】

一実施形態によれば、方法は、外部システムから一連のリクエストを受信することをさらに含み得、リクエストは一連のリクエストのうち最新のリクエストである。この実施形態には、一連のリクエストの数をカウントすること、およびリクエストの数が所定の閾値に達した場合に、コンピュータ・ファイルとともにデータを送信することを初期化することを伴うことがある。これは、外部システムからコンピュータ・システムに送信される最初のリクエストと、コンピュータ・ファイルの外部システムへの送信との間に遅延を引き起こすことがある。

【００３４】

いくつかの実施形態では、外部システムは最初のレスポンス・ファイルの検査を実行することができる。最初のレスポンス・ファイルは、最初のリクエストに対するレスポンスの形でコンピュータ・システムから送信されることがある。最初のリクエストは、外部システムからコンピュータ・システムに送信され、一連のリクエストの最初のリクエストとなる可能性がある。最初のレスポンス・ファイルは、前述の命令のいずれも含んでいない可能性がある。そのため、外部システムはコンピュータ・システムを攻撃的でないと分類し、前述のリクエストを含め、さらなるリクエストをコンピュータ・システムに送り続ける可能性がある。コンピュータ・システムは、さらなるリクエストを受信したことに応答して、前述のレスポンス・ファイル、すなわちコンピュータ・ファイルを含む、さらなるレスポンス・ファイルを送信することができる。多くの適用例では、外部システムは、さらなるレスポンス・ファイル次第で、コンピュータ・システムが攻撃的でないかどうかをチェックしないことがある。これにより、外部システムのプロセッサ上で命令の実行を開始することができ、この実行が外部システムによって検出されないようにすることができる。

【００３５】

一実施形態によれば、コンピュータ・システムは、データを提供するデータ・サーバから構成されることがある。接続は、プロキシ・サーバを使用して確立してもよい。この実施形態によれば、方法はさらに以下を含むことができる：

－　プロキシ・サーバを使用してリクエストを受信すること、

－　プロキシ・サーバを使用してリクエストをデータ・サーバに方向付けること、

－　リクエストに応じて、データ・サーバからプロキシ・サーバにデータを送信すること、

－　プロキシ・サーバを使用してコンピュータ・ファイルを生成すること、
－　プロキシ・サーバから外部コンピュータ・システムへ、コンピュータ・ファイルとともにデータを送信すること。

【００３６】

プロキシ・サーバは、サーバ・アプリケーションの形態で設計することができ、外部システムとコンピュータ・システムの少なくとも一部、例えばデータ・サーバまたはおとりサーバとの仲介として機能することができる。一例では、コンピュータ・システムはプロキシ・サーバを含むことができる。プロキシ・サーバはリクエストの評価を実行し、リクエストの評価結果次第で、リクエストをデータ・サーバまたはおとりサーバに方向付けることができる。例えば、プロキシ・サーバがリクエストを完全に未知のリクエストと評価する場合、プロキシ・サーバはデータ・サーバまたはおとりサーバへのリクエストの送信をブロックすることができる。したがって、プロキシ・サーバは、コンピュータ・システムの少なくとも一部、例えばデータ・サーバまたはおとりサーバあるいはその両方を、外部システムからカプセル化することができる。さらに、プロキシ・サーバは、外部システムに送信されるデータの出所をマスクすることができる。

【００３７】

プロキシ・サーバを使用したコンピュータ・ファイルの生成は、コンピュータ・ファイルの生成を実行するためにプロキシ・サーバだけを適合させればよいという利点がある。この場合、コンピュータ・システムの保護された部分を適合させる必要がないことがある。

【００３８】

一実施形態によれば、コンピュータ・システムは、データ・サービスから構成されることがある。この実施形態によれば、リクエストに応じたデータを用意することは、おとりモジュールを使用してデータ・サービスを模倣することを含むことがある。いくつかの実施形態では、データ・サービスは、リクエストによって要求されたデータを提供するように設計されている場合がある。しかし、このリクエストは、機密データ、例えば給与システムのデータに対するリクエストを含むこともある。おとりモジュールは、データが機密データのフォーマットを含むことができるように、また機密データの誤った値を含むことができるように、データを生成するように設計することができる。そうすることで、データが外部システムから「偽のデータ」として検出されるリスクを減らすことができる。フォーマットは、一例として給与テーブルなどのテーブルの行数または列数あるいはその両方を規定することができる。

【００３９】

いくつかの実施形態では、データは、おとりモジュールによって提供される場合があり、方法は、プロキシ・サーバを使用して接続を確立することと、プロキシ・サーバを使用してリクエストを受信することと、上述のように、データおよびコンピュータ・ファイルをともにプロキシ・サーバから外部コンピュータ・システムに送信することとをさらに含む場合がある。この実施形態の一変形例によると、コンピュータ・ファイルはプロキシ・サーバを使用して生成されることがある。さらに、プロキシ・サーバは、おとりモジュールを構成することができる。したがって、「偽のデータ」の形態でデータを生成するためには、プロキシ・サーバだけを適合させればよい。一例では、プロキシ・サーバはフォーマット・データベースで構成されてもよい。さらに、プロキシ・サーバは、過去のリクエストの訓練セット、およびデータ・フォーマットを構成する過去のデータファイルの訓練セットに応じて、フォーマット・データベースを作成するように設計することができる。過去のリクエストの訓練セットの各リクエストは、過去のデータファイルの訓練セットのデータ・フォーマットのうちの１つに対応することができる。

【００４０】

一実施形態によれば、方法は、おとりサーバを用意することをさらに含み得、おとりサーバはおとりモジュールを含むことができる。この実施形態によれば、この方法は、プロキシ・サーバからのリクエストをおとりサーバに方向付けることと、プロキシ・サーバを

使用しておとりサーバからデータを受信することとをさらに含むことができる。おとりサーバまたはおとりモジュールあるいはその両方は、セキュリティ上の欠陥を含むように設計することができる。例えば、おとりサーバは更新されていないシステム・ソフトウェアを含むことができる。セキュリティ上の欠陥は、おとりモジュールまたはおとりサーバあるいはその両方に方向付けられるようにリクエストを設計することを引き起こすことができる。そうすることで、機密データを記憶している可能性のあるデータ・サーバにリクエストが方向付けられるのを防ぐことができる。

【００４１】

一実施形態によれば、方法は、外部コンピュータ・システムの分類を実行することをさらに含むことができる。分類は、外部システムとコンピュータ・システム間の記録されたデータ・トラフィックに応じて、例えば、リクエストまたはリクエストの履歴あるいはその両方に応じて実施することができる。この実施形態の変形例によれば、データを用意することは、外部コンピュータ・システムの分類の結果に応じてデータを生成することを含むことができる。この実施形態のさらなる変形例によれば、外部コンピュータ・システムの分類の結果に応じて命令を生成することができる。したがって、データまたは命令あるいはその両方は、それぞれカスタマイズされたデータおよびカスタマイズされた命令と考えることができ、データまたは命令あるいはその両方は外部システムに対して適合される。これにより、外部システムはコンピュータ・システムへの接続を維持するようになり、外部システムに関する情報を受信する機会が増える可能性がある。外部コンピュータ・システムの分類には、その地域、リクエストの送信パターン、またはリクエストの履歴によって外部システムを分類することが伴うことがある。

【００４２】

一実施形態によれば、リクエストは、外部システムに関する初期情報を含むことができる。この実施形態によれば、コンピュータ・システムは、外部システムに関する初期情報に応じて、コンピュータ・ファイル、例えばデータまたは命令あるいはその両方を生成することができる。代替的に、または追加的に、コンピュータ・システムは、記録されたデータ・トラフィックに応じて、データまたは命令あるいはその両方を生成することができる。外部システムまたは記録されたデータ・トラフィックあるいはその両方に関する初期情報は、外部システムから送信されたＩＰアドレスまたはジオロケーション・データあるいはその両方を含むことがある。リクエストは、ブラウザのユーザ・エージェントに関する情報、または外部システムのブラウザに関する追加的な情報あるいはその両方、例えば許容可能な言語、クッキー、またはリファラあるいはその組合せを含み得るヘッダを含んでいてもよい。

【００４３】

したがって、いくつかの実施形態では、データまたは命令あるいはその両方は、それぞれカスタマイズされたデータおよびカスタマイズされたコンピュータ・ファイルと考えることができ、データまたはコンピュータ・ファイルあるいはその両方は、初期情報に基づいて外部システムに対して適合される。これは、外部システムがコンピュータ・システムとの接続を維持するよう促す可能性がある。

【００４４】

一実施形態によれば、外部コンピュータ・システムを潜在的な脅威として分類することは、さらなる人工知能モジュール（以下、さらなるＡＩモジュールとも称する）を使用して実施することができる。外部システムとコンピュータ・システムの間で記録されたトラフィック・データに関する情報は、さらなるＡＩモジュールに入力信号の形態で送ることができる。さらなるＡＩモジュールは、トラフィック・データに関する情報に応じて、外部コンピュータ・システムを潜在的な脅威として分類することができる。ＡＩモジュールは、ニューロン・ネットワークまたは規則ベースの決定モジュールあるいはその両方を含むことができる。

【００４５】

一実施形態によれば、方法は、外部コンピュータ・システムに関する情報に応じてレポ

ートを生成することをさらに含むことができる。レポートは、コンピュータ・システムのセキュリティ・マネージャに送られることもある。

【００４６】

本開示の実施形態は、コンピュータ・システム、クライアント、またはサーバとも呼ばれるコンピューティング・デバイスを使用して実装され得る。次に図１を参照すると、コンピュータ・システム１０の一例の概略図が示されている。コンピュータ・システム１０は、好適なコンピュータ・システムの一例に過ぎず、本明細書で説明される実施形態の使用範囲または機能に関する制限を示唆することは意図されていない。それにもかかわらず、コンピュータ・システム１０は、本明細書で上述した機能のいずれかを実装すること、または実行すること、あるいはその両方が可能である。

【００４７】

コンピュータ・システム１０は、図２に示すような第１のコンピュータ・システム／サーバ１２の形態のコントローラ・サーバと、図３に示すような第２のコンピュータ・システム／サーバ２１２の形態のプロキシ・サーバとを含むことができる。

【００４８】

第１のコンピュータ・システム／サーバ１２および第２のコンピュータ・システム／サーバ２１２は、それぞれ、多数の他の汎用または特殊目的のコンピューティング・システム環境または構成で動作可能である。第１のコンピュータ・システム／サーバ１２および第２のコンピュータ・システム／サーバ２１２とともに使用するのに適したコンピューティング・システム、環境、または構成あるいはその組合せの例としては、パーソナル・コンピュータ・システム、サーバ・コンピュータ・システム、シン・クライアント、シック・クライアント、ハンドヘルドまたはラップトップ・デバイス、マルチプロセッサ・システム、マイクロプロセッサベース・システム、セット・トップ・ボックス、プログラマブル家電、ネットワークＰＣ、ミニコンピュータ・システム、メインフレーム・コンピュータ・システム、および上記のシステムまたはデバイスのいずれかを含む分散コンピューティング環境などが挙げられるが、これらに限定されない。

【００４９】

第１のコンピュータ・システム／サーバ１２および第２のコンピュータ・システム／サーバ２１２は、コンピュータ・システムによって実行されるプログラム・モジュールなどのコンピュータ・システム実行可能命令の一般的なコンテキストで説明することができる。一般に、プログラム・モジュールには、特定のタスクを実行する、または特定の抽象データ型を実装するルーチン、プログラム、オブジェクト、構成要素、ロジック、データ構造などが含まれる。第１のコンピュータ・システム／サーバ１２および第２のコンピュータ・システム／サーバ２１２は、通信ネットワークを介してリンクされたリモート処理デバイスによってタスクが実行される可能性のある分散コンピューティング環境で実用化することができる。分散コンピューティング環境では、プログラム・モジュールは、メモリ記憶装置を含むローカルおよびリモート両方のコンピュータ・システム記憶媒体に配置される可能性がある。

【００５０】

図２に示すように、コンピュータ・システム１０における第１のコンピュータ・システム／サーバ１２は、汎用コンピューティング・デバイスであってもよい。第１のコンピュータ・システム／サーバ１２の構成要素には、１つまたは複数のプロセッサまたは処理装置１６、システム・メモリ２８、およびシステム・メモリ２８を含む様々なシステム構成要素を処理装置１６に結合するバス１８が含まれるが、これらに限定されない。バス１８は、メモリ・バスまたはメモリ・コントローラ、周辺機器バス、アクセラレーテッド・グラフィックス・ポート、および様々なバス・アーキテクチャのいずれかを使用するプロセッサまたはローカル・バスを含む、いくつかのタイプのバス構造のいずれか１つまたは複数を表すことができる。例として、また限定はしないが、このようなアーキテクチャには以下のものを挙げることができる：Ｉｎｄｕｓｔｒｙ Ｓｔａｎｄａｒｄ Ａｒｃｈｉｔｅｃｔｕｒｅ（ＩＳＡ）バス、Ｍｉｃｒｏ Ｃｈａｎｎｅｌ Ａｒｃｈｉｔｅｃｔｕｒｅ

（ＭＣＡ）バス、Ｅｎｈａｎｃｅｄ　ＩＳＡ（ＥＩＳＡ）バス、Ｖｉｄｅｏ　Ｅｌｅｃｔｒｏｎｉｃｓ　Ｓｔａｎｄａｒｄｓ　Ａｓｓｏｃｉａｔｉｏｎ（ＶＥＳＡ）ローカル・バス、およびＰｅｒｉｐｈｅｒａｌ　Ｃｏｍｐｏｎｅｎｔ　Ｉｎｔｅｒｃｏｎｎｅｃｔ（ＰＣＩ）バス。

【００５１】

第１のコンピュータ・システム／サーバ１２は、様々なコンピュータ・システム可読媒体を含むことができる。このような媒体は、第１のコンピュータ・システム／サーバ１２がアクセス可能な利用可能な媒体であれば何でもよく、揮発性媒体と不揮発性媒体、リムーバブル媒体と非リムーバブル媒体の両方を含むことができる。

【００５２】

システム・メモリ２８は、ランダム・アクセス・メモリ（ＲＡＭ）３０またはキャッシュ・メモリ３２あるいはその両方などの揮発性メモリの形態のコンピュータ・システム可読媒体を含むことができる。第１のコンピュータ・システム／サーバ１２は、他のリムーバブル／非リムーバブルの、揮発性／不揮発性のコンピュータ・システム記憶媒体をさらに含むことができる。単なる一例として、ストレージ・システム３４は、非リムーバブルの不揮発性の磁気媒体（図示せず、一般に「ハード・ドライブ」と呼ばれる）からの読み取りおよび磁気媒体への書き込みのために設けられることがある。図示していないが、リムーバブルの不揮発性磁気ディスク（例えば、「フロッピ・ディスク」）から読み取りおよびそれに書き込みするための磁気ディスク・ドライブ、およびリムーバブルの不揮発性の光ディスク（例えば、ＣＤ－ＲＯＭ、ＤＶＤ－ＲＯＭまたは他の光媒体）から読み取りまたはそれに書き込みするための光ディスク・ドライブを設けることができる。このような場合、一部またはすべてが、１つまたは複数のデータ媒体インターフェースによってバス１８に接続される。以下にさらに図示し説明するように、メモリ２８は、いくつかの実施形態の機能を遂行するように構成されたプログラム・モジュールのセット（例えば、少なくとも１つ）を有する少なくとも１つのプログラム製品を含むことができる。

【００５３】

プログラム・モジュール５０のセット（少なくとも１つ）を有するプログラム／ユーティリティ４０は、オペレーティング・システム、１つまたは複数のアプリケーション・プログラム、他のプログラム・モジュール、およびプログラム・データと同様に、例として、また限定はしないが、メモリ２８に記憶することができる。オペレーティング・システム、１つまたは複数のアプリケーション・プログラム、その他のプログラム・モジュール、およびプログラム・データ、またはそれらの組合せの各々は、ネットワーキング環境の実装形態を含むことができる。プログラム・モジュール５０は、本明細書で説明されるいくつかの実施形態の機能または方法論あるいはその両方を遂行することができる。

【００５４】

第１のコンピュータ・システム／サーバ１２は、キーボード、ポインティング・デバイス、ディスプレイ２４などの１つもしくは複数の外部デバイス１４、ユーザが第１のコンピュータ・システム／サーバ１２と対話することを可能にする１つもしくは複数のデバイス、または第１のコンピュータ・システム／サーバ１２が１つもしくは複数の他のコンピューティング・デバイスと通信することを可能にする任意のデバイス（例えば、ネットワーク・カード、モデムなど）あるいはその組合せと通信することもできる。このような通信は、入力／出力（Ｉ／Ｏ）インターフェース２２を介して行われることがある。さらになお、第１のコンピュータ・システム／サーバ１２は、ネットワーク・アダプタ２０を介して、ローカル・エリア・ネットワーク（ＬＡＮ）、一般的なワイド・エリア・ネットワーク（ＷＡＮ）、またはパブリック・ネットワーク（例えば、インターネット）あるいはその組合せなどの、１つまたは複数のネットワークと通信することができる。描かれているように、ネットワーク・アダプタ２０は、バス１８を介して第１のコンピュータ・システム／サーバ１２の他の構成要素と通信することができる。図示していないが、他のハードウェアまたはソフトウェアあるいはその両方の構成要素も、第１のコンピュータ・システム／サーバ１２と組み合わせて使用できることを理解されたい。例として、マイクロコ

ード、デバイス・ドライバ、冗長処理装置、外付けディスク・ドライブ・アレイ、ＲＡＩＤシステム、テープ・ドライブ、データ・アーカイバル・ストレージ・システムなどが挙げられるが、これらに限定されるものではない。

【００５５】

図３に示すように、コンピュータ・システム１０における第２のコンピュータ・システム／サーバ２１２は、汎用コンピューティング・デバイスであってもよい。第２のコンピュータ・システム／サーバ２１２の構成要素には、１つまたは複数のプロセッサまたは処理装置２１６、システム・メモリ２２８、およびシステム・メモリ２２８を含む様々なシステム構成要素を処理装置２１６に結合するバス２１８が含まれ得るが、これらに限定されない。バス２１８は、メモリ・バスまたはメモリ・コントローラ、周辺機器バス、アクセラレーテッド・グラフィックス・ポート、および様々なバス・アーキテクチャのいずれかを使用するプロセッサまたはローカル・バスを含む、いくつかのタイプのバス構造のいずれか１つまたは複数を表すことができる。例として、また限定はしないが、このようなアーキテクチャには以下のものを挙げることができる：Ｉｎｄｕｓｔｒｙ Ｓｔａｎｄａｒｄ Ａｒｃｈｉｔｅｃｔｕｒｅ（ＩＳＡ）バス、Ｍｉｃｒｏ Ｃｈａｎｎｅｌ Ａｒｃｈｉｔｅｃｔｕｒｅ（ＭＣＡ）バス、Ｅｎｈａｎｃｅｄ ＩＳＡ（ＥＩＳＡ）バス、Ｖｉｄｅｏ Ｅｌｅｃｔｒｏｎｉｃｓ Ｓｔａｎｄａｒｄｓ Ａｓｓｏｃｉａｔｉｏｎ（ＶＥＳＡ）ローカル・バス、およびＰｅｒｉｐｈｅｒａｌ Ｃｏｍｐｏｎｅｎｔ Ｉｎｔｅｒｃｏｎｎｅｃｔ（ＰＣＩ）バス。

【００５６】

第２のコンピュータ・システム／サーバ２１２は、様々なコンピュータ・システム可読媒体を含むことができる。このような媒体は、第２のコンピュータ・システム／サーバ２１２がアクセス可能な利用可能な媒体であれば何でもよく、揮発性媒体と不揮発性媒体、リムーバブル媒体と非リムーバブル媒体の両方を含むことができる。

【００５７】

システム・メモリ２２８は、ランダム・アクセス・メモリ（ＲＡＭ）２３０またはキャッシュ２３２あるいはその両方などの揮発性メモリの形態のコンピュータ・システム可読媒体を含むことができる。第２のコンピュータ・システム／サーバ２１２は、他のリムーバブル／非リムーバブルの、揮発性／不揮発性のコンピュータ・システム記憶媒体をさらに含むことができる。単なる一例として、ストレージ・システム２３４は、非リムーバブルの不揮発性の磁気媒体またはソリッドステート記憶媒体（例えば、図示しないが「ハード・ドライブ」）からの読み取りおよび磁気媒体への書き込みのために設けられることがある。図示していないが、リムーバブルの不揮発性磁気ディスク（例えば、「フロッピ・ディスク」）から読み取りおよびそれに書き込みするための磁気ディスク・ドライブ、およびＣＤ－ＲＯＭ、ＤＶＤ－ＲＯＭまたは他の光媒体などのリムーバブルの不揮発性の光ディスクから読み取りまたはそれに書き込みするための光ディスク・ドライブを設けることができる。このような場合、各々が、１つまたは複数のデータ媒体インターフェースによってバス２１８に接続され得る。以下にさらに図示し説明するように、メモリ２２８は、本開示の実施形態の機能を遂行するように構成されたプログラム・モジュールのセット（例えば、少なくとも１つ）を有する少なくとも１つのプログラム製品を含むことができる。

【００５８】

プログラム・モジュール２５０のセット（少なくとも１つ）を有するプログラム／ユーティリティ２４０は、オペレーティング・システム、１つまたは複数のアプリケーション・プログラム、他のプログラム・モジュール、およびプログラム・データと同様に、例として、また限定はしないが、メモリ２２８に記憶することができる。オペレーティング・システム、１つまたは複数のアプリケーション・プログラム、その他のプログラム・モジュール、およびプログラム・データ、またはそれらの組合せの各々は、ネットワーキング環境の実装形態を含むことができる。プログラム・モジュール２５０は一般に、本明細書で説明されるいくつかの実施形態の機能または方法論あるいはその両方を遂行することが

できる。

【００５９】

第２のコンピュータ・システム／サーバ２１２は、キーボード、ポインティング・デバイス、ディスプレイ２２４などの１つもしくは複数の外部デバイス２１４、ユーザが第２のコンピュータ・システム／サーバ２１２と対話することを可能にする１つもしくは複数のデバイス、または第２のコンピュータ・システム／サーバ２１２が１つもしくは複数の他のコンピューティング・デバイスと通信することを可能にする任意のデバイス（例えば、ネットワーク・カード、モデムなど）あるいはその組合せと通信することもできる。このような通信は、入力／出力（Ｉ／Ｏ）インターフェース２２２を介して行われることがある。さらになお、第２のコンピュータ・システム／サーバ２１２は、ネットワーク・アダプタ２２０を介して、ローカル・エリア・ネットワーク（ＬＡＮ）、一般的なワイド・エリア・ネットワーク（ＷＡＮ）、またはパブリック・ネットワーク（例えば、インターネット）あるいはその組合せなどの、１つまたは複数のネットワークと通信することができる。描かれているように、ネットワーク・アダプタ２２０は、バス２１８を介して第２のコンピュータ・システム／サーバ２１２の他の構成要素と通信することができる。図示していないが、他のハードウェアまたはソフトウェアあるいはその両方の構成要素も、第２のコンピュータ・システム／サーバ２１２と組み合わせて使用できることを理解されたい。例として、マイクロコード、デバイス・ドライバ、冗長処理装置、外付けディスク・ドライブ・アレイ、ＲＡＩＤシステム、テープ・ドライブ、データ・アーカイバル・ストレージ・システムなどが挙げられるが、これらに限定されるものではない。

【００６０】

図１に示されるコンピュータ・システム１０などのコンピュータ・システムは、コンピュータ・システム１０と外部コンピュータ・システム２との間の接続を介して外部コンピュータ・システム２からＨＴＴＰ－リクエスト１を受信すること（以降では第１の受信動作とも称する）、外部コンピュータ・システム２をコンピュータ・システム１０に対する潜在的な脅威として検出すること（以降では検出動作とも称する）、リクエスト１に応じてコンピュータ・ファイル３を生成すること（以降ではファイル生成動作とも称する）、リクエスト１に応じてデータ４を提供すること（以降ではデータ生成とも称する）、データ４をコンピュータ・ファイル３とともに外部コンピュータ・システム２に送信すること（以降ではレスポンス動作とも称する）、コンピュータ・ファイル３の命令５に応じて生成された外部コンピュータ・システム２に関する情報６を受信すること（以降では第２の受信動作とも称する）、および外部コンピュータ・システム２に関する情報６をコンピュータ・システム１０に保存すること（以降では保存動作とも称する）など、本明細書において開示される動作を実行するように構成することができる。

【００６１】

命令５は、外部コンピュータ・システム２のプロセッサ７で実行される場合、情報６を取得するように設計することができる。

【００６２】

図４は、コンピュータ・システム１０などのコンピュータ・システムが、例えばネットワーク・アダプタ２２０を使用して、ネットワーク２００に接続されている例示のコンピューティング環境を示している。限定するものではないが、ネットワーク２００は、インターネット、ローカル・エリア・ネットワーク（ＬＡＮ）、移動体通信ネットワークなどの無線ネットワークなどの通信ネットワークとすることができる。ネットワーク２００は、クラウド・コンピューティング・ネットワークのようなコンピューティング・ネットワークを含んでもよい。コンピュータ・システム１０は、ネットワーク２００を介して外部コンピュータ・システム２と接続することができる。コンピュータ・システム１０は、外部コンピュータ・システム２とコンピュータ・システム１０との間の接続を構築するための通信データおよびリクエスト１など、処理すべきデータをネットワーク２００から受信することができる。さらに、コンピュータ・システム１０は、コンピュータ・ファイル３などの計算結果を、外部コンピュータ・システム２など、ネットワーク２００を介してコ

ンピュータ・システム１０に接続された別の計算装置に提供することができる。
【００６３】
コンピュータ・システム１０は、ネットワーク２００を介して受信したリクエスト１に応答して、本明細書で説明される動作を、全体的にまたは部分的に実行することができる。特に、コンピュータ・システム１０は、ネットワーク２００を介してコンピュータ・システム１０に接続される１つまたは複数のさらなるコンピュータ・システムとともに、分散コンピューテーションでそのような演算を実行することができる。そのために、コンピューティング・システム１０またはさらに関与するコンピュータ・システムあるいはその両方は、ネットワーク２００を使用して、専用メモリまたは共有メモリなどのさらなるコンピューティング・リソースにアクセスすることができる。
【００６４】
プロキシ・サーバ２１２は、第１の受信プログラム・モジュール２５１、レスポンス・プログラム・モジュール２５２および第２の受信プログラム・モジュール２５３をそれぞれ処理装置２１６で実行することにより、第１の受信動作、レスポンス動作および第２の受信動作を行うことができる。処理装置２１６上で第１の受信プログラム・モジュール２５１を実行することにより、ネットワーク・アダプタ２２０からメモリ２２８への、例えばキャッシュ２３２への、電子信号の形態のリクエスト１を含む第１のデータ・パッケージ１０１の送信を引き起こす可能性がある。外部コンピュータ・システム２は、ネットワーク２００を介して、第１のデータ・パッケージ１０１の形態でリクエスト１をプロキシ・サーバ２１２に送信することができる。第１のデータ・パッケージ１０１またはリクエスト１あるいはその両方は、外部コンピュータ・システム２に関する初期情報、例えば、外部コンピュータ・システム２のジオロケーション情報またはＩＰアドレスあるいはその両方を含むことができる。さらに、処理装置２１６上で第１の受信プログラム・モジュール２５１を実行することにより、Ｉ／Ｏインターフェース２２２を介してＩ／Ｏインターフェース２２に初期情報とともにリクエスト１の送信を引き起こす可能性がある。したがって、プロキシ・サーバは、初期情報とともに、リクエスト１をコントローラ・サーバ１２に方向付けることができる。
【００６５】
同様に、処理装置２１６上で第２の受信プログラム・モジュール２５３を実行することは、第１のさらなる電子信号の形態の情報６を含む第３のデータ・パッケージ１０３の、ネットワーク・アダプタ２２０からメモリ２２８への、例えばキャッシュ２３２への送信、およびＩ／Ｏインターフェース２２２を介したＩ／Ｏインターフェース２２への情報６の送信を引き起こす可能性がある。したがって、プロキシ・サーバは、情報６をコントローラ・サーバ１２に方向付けることができる。処理装置２１６は、第１のデータ・パッケージ１０３および第３のデータ・パッケージ１０３が、メモリ２２８に記憶された規定されたセキュリティ規則に準拠し得るかどうかをチェックすることができる。
【００６６】
処理装置２１６上でレスポンス・プログラム・モジュール２５３を実行することは、外部コンピュータ・システム２のアドレスとコンピュータ・ファイル３とを含む第２のデータ・パッケージを使用して、メモリ２２８から、例えばキャッシュ２３２から、ネットワーク・アダプタ２２０を介してネットワーク２００にコンピュータ・ファイル３を送信することを引き起こす可能性がある。
【００６７】
コントローラ・サーバ１２は、検出プログラム・モジュール５１、ファイル生成プログラム・モジュール５２、データ生成プログラム・モジュール５３および保存プログラム・モジュール５４をそれぞれ処理装置１６で実行することにより、検出動作、ファイル生成動作、データ生成動作および保存動作を実行することができる。
【００６８】
検出プログラム・モジュール５１を実行することにより、例えば初期情報を含むリクエスト１のデータに応じて、プログラム・モジュール５１のＡＩモジュール６１の出力値を

計算することを引き起こすことができる。一例では、検出プログラム・モジュール５１を実行することは、過去のリクエストとリクエスト１のデータに応じてＡＩモジュール６１の出力値を計算することからなる。この場合、過去のリクエストとリクエスト１のデータは、ＡＩモジュール１の入力データとして使用することができる。過去のリクエストは、外部コンピュータ・システム２またはさらなる外部システムからプロキシ・サーバ２１２に送信される可能性がある。ＡＩモジュール６１の出力値は、外部コンピュータ・システム２（以下、外部システム２とも称される）が潜在的な脅威として分類されるかどうかを示すことができる。例えば、出力値「１」は、ＡＩモジュールが外部システム２を潜在的な脅威と評価していることを示すことができる。外部システム２が潜在的な脅威と評価されない場合、ＡＩモジュール６１の出力値は「０」であってもよい。

【００６９】

検出プログラム・モジュール５１またはＡＩモジュール６１あるいはその両方は、過去のリクエストとリクエスト１の共通パターンまたは過去のリクエストとリクエスト１によって与えられる全体パターンあるいはその両方を検出することにより、外部システム２を潜在的な脅威として評価するように設計され得る。共通パターンが初期情報を構成することもある。この場合、過去のリクエストがそれぞれ初期情報を構成することがある。一例では、共通パターンは、過去のリクエストおよびリクエスト１が類似のデータを含むようなものであってもよい。過去のリクエストおよびリクエスト１は、それぞれあるフレーズ、例えばパスワード・フレーズを含むことがある。類似のデータは、類似の文字のセットを含むことがある。例えば、類似のデータを含む過去のリクエストおよびリクエスト１では、過去のリクエストのフレーズとリクエスト１のフレーズがそれぞれ１文字または２文字だけ互いに異なっている場合を含んでもよい。

【００７０】

全体的なパターンは、過去のリクエストとリクエスト１が、所与の時間閾値よりも小さいサイズを持つ時間間隔内にプロキシ・サーバ２１２によって受信される、という形であってもよい。

【００７１】

ＡＩモジュール６１は訓練された状態であってもよい。ＡＩモジュール６１は、以前のＨＴＴＰリクエストの訓練データセットを提示することによって訓練されている可能性がある。以前のＨＴＴＰリクエストは、コンピュータ・システム１０に対する脅威として既知の第２のさらなる外部システムから送信される可能性がある。

【００７２】

リクエスト１のデータは、コンピュータ・システム１０の保護されたデータベース・サーバ８にログインするためのアクセス・データで構成される場合がある。一例では、データベース・サーバ８は給与データベースを提供することができる。

【００７３】

データ生成プログラム・モジュール５３を実行することは、おとりモジュール６３を使用してデータ４を生成することを含むことがある。おとりモジュール６３は、保護されたデータベース・サーバ８の修正された機密データの形態でデータ４を生成するように構成されることがある。おとりモジュール６３は、データ４が保護されたデータベース・サーバ８の機密情報を含まないように、データ４を生成することができる。データ４は、一例では、未分類の公開情報を含んでもよい。

【００７４】

一例では、おとりモジュール６３は、データベース・サーバ８の機能を模倣することでデータ４を生成することができる。例えば、おとりモジュール６３は、データ４がデータベース・サーバ８のオペレーティング・システムに関する情報を含むように、データ４を生成することができる。

【００７５】

一例では、おとりモジュール６３は、データ４がおとり情報を含むように、データ４を生成することができる。おとり情報は、データベース・サーバ８のオペレーティング・シ

ステムに関する情報が、データベース・サーバ８のオペレーティング・システムの期限切れバージョンを示すように設計することができる。

【００７６】

コントローラ・サーバ１２は、データ生成プログラム・モジュール５３の実行時に機密データを読み取るために、Ｉ／Ｏインターフェース２２を介してデータベース・サーバ８に接続することができる。

【００７７】

おとりモジュール６３は、コントローラ・サーバ１２の構成要素として図２に示されている。図示しない例では、おとりモジュール６３は、Ｉ／Ｏインターフェース２２を介してコントローラ・サーバ１２に接続されるおとりサーバの構成要素であってもよい。データ生成プログラム・モジュール５３の実行は、この場合、コントローラ・サーバ１２とおとりサーバとの間で通信セッションを確立することを含むことができる。

【００７８】

ファイル生成プログラム・モジュール５２を実行することは、データ４および命令５をコンピュータ・ファイル３に書き込むことを含み得る。ファイル生成プログラム・モジュール５２は、初期情報、リクエスト１のデータ、または外部システム２の分類の結果あるいはその組合せに応じて、命令５を生成することができる。ファイル生成プログラム・モジュール５２の分類モジュール６２は、初期情報に応じて、またはリクエスト１のデータに応じて、あるいはその両方に応じて外部システム２の分類を実行することができる。例えば、命令５は、外部システム２のオペレーション・システムのタイプに適合させることができる。ファイル生成プログラム・モジュール５２は、外部システム２の分類の結果に応じて、外部システム２のオペレーション・システムのタイプを決定することができる。

【００７９】

命令５は、追跡スクリプト、プロファイリング・スクリプト、または外部システム２のデータベースにアクセスするためのスクリプトあるいはその組合せを含むことができる。追跡スクリプトは、外部システム２におけるデータ４の処理など、外部システム２上で実行されたアクションに関する情報を記録することができる。データ４の処理には、データ４を１回または数回コピーすること、データ分析ツールを使用してデータ４を分析すること、および外部システム２の永続記憶装置にデータ４を記憶することが含まれる。外部システム２上でプロファイリング・スクリプトを実行することは、外部システム２上で実行されたアクションを分類することを含み得る。一例では、プロファイリング・スクリプトを実行することは、外部システム２のオペレーション・システムに関する情報を収集することを含むことがある。プロファイリング・スクリプトをコンピュータ・ファイル３とともに送信することは、外部システム２のプロファイリングが外部システム２のプロセッサによって実行されるという利点を有し得る。これにより、コンピュータ・システム１０の計算作業を削減することができる。外部システム２のデータベースにアクセスするためのスクリプトは、外部システム２のデータベースのデータを読み取るための命令で構成することができる。命令５は、ＨＴＭＬまたはＪａｖａ（Ｒ）Ｓｃｒｉｐｔあるいはその両方の言語の形式であってもよい。

【００８０】

一例では、命令５はメッセージ生成スクリプトを含んでもよい。メッセージ生成スクリプトは、情報６を含むメッセージを作成することができる。情報６は、追跡スクリプト、プロファイリング・スクリプト、または外部システム２のデータベースにアクセスするためのスクリプトあるいはその組合せを、外部システム２のプロセッサ上で実行することによって得られる情報を含むことができる。メッセージ生成スクリプトは、第３のデータ・パッケージ１０３の一部としてメッセージを生成することができる。第３のデータ・パッケージ１０３は、外部システム２によって生成されるさらなるＨＴＴＰリクエストを含むことができる。外部システム２は、おとり情報を読み取ったことに応答して、さらなるＨＴＴＰリクエストを生成することができる。

【００８１】

ファイル生成プログラム・モジュール５２は、コントローラ・サーバ１２の構成要素として図２に示されている。図に示されない一例では、ファイル生成プログラム・モジュール５２は、プロキシ・サーバ２１２の構成要素であってもよく、このプロキシ・サーバ２１２はＩ／Ｏインターフェース２２２を介してデータベース・サーバ８に接続されていてもよい。ファイル生成プログラム・モジュール５２を実行することは、この場合、プロキシ・サーバ２１２とデータベース・サーバ８との間に通信セッションを確立することを含み得る。この例によると、プロキシ・サーバ２１２はコンピュータ・ファイル３を生成することができる。

【００８２】

コントローラ・サーバ１２、例えば処理装置１６は、プロキシ・サーバ２１２から情報６を受信したことに応答して、外部システム２に関する情報６の分析を実行することができる。情報６の分析を実行することは、情報６を侵入者データベース３５の情報と比較することを含むことがある。侵入者データベース３５は、様々な侵入者プロファイルを記憶することができる。情報６は初期情報よりも多くのデータを含む可能性があるため、情報６は侵入者データベース３５に記憶されている侵入者プロファイルの１つと一致する可能性がある。この場合、処理装置１６は、コンピュータ・システム１０を保護するための保護手段を開始することができる。処理装置１６は、情報６に一致する侵入者プロファイルに応じて、保護手段のセットからある保護手段を選択することができる。

【００８３】

処理装置１６は、情報６の一部、例えば、外部システム２によって使用されるウェブ・ブラウザのブラウザ・プラグインのタイプまたは外部システム２のＩＰアドレスあるいはその両方に応じて、保護手段を選択することができる。

【００８４】

一例では、処理装置１６は、情報６に応じて、さらなる侵入者プロファイルを生成することができる。情報６が侵入者データベース３５のどの侵入者プロファイルにも一致しない場合、さらなる侵入者プロファイルを作成することができる。

【００８５】

一例では、侵入者データベース３５は、侵入者プロファイルに基づいて訓練された、さらなるＡＩモジュールであってもよい。侵入者プロファイルは各々、情報６の構造と類似した構造を有するデータを含むことができる。情報６の構造は、異なるヘッダと、それぞれがヘッダの１つに対応する異なるテキスト本文から構成され得る。情報６が侵入者プロファイルのいずれとも一致しない場合、処理装置１６は、侵入者データベース３５を更新し、例えば、情報６またはさらなる侵入者プロファイルを使用して、さらなるＡＩモジュールを訓練することができる。情報６に応じて侵入者データベース３５を更新することは、プロセッサ（処理装置）１６上で保存プログラム・モジュール５４を実行することによって行うことができる。

【００８６】

図５は、情報６を取得するためのコンピュータ実装方法のフローチャートを示す。

【００８７】

動作１００１において、プロキシ・サーバ２１２は、外部システム２から、例えば上述したような第１のデータ・パッケージ１０１の形態で、リクエスト１を受信することができる。

【００８８】

動作１００２において、コントローラ・サーバ１２は、例えば、上述の検出プログラム・モジュール５１を実行することにより、外部コンピュータ・システム２をコンピュータ・システム１０に対する潜在的な脅威として分類することができる。

【００８９】

動作１００３において、コントローラ・サーバ１２またはプロキシ・サーバ２１２は、例えば、上述のファイル生成プログラム・モジュール５２を実行することにより、コンピュータ・ファイル３を生成することができる。

【００９０】
動作１００４では、例えば上述のようにデータ生成プログラム・モジュール５３を実行することにより、データ４を用意することができる。
【００９１】
動作１００５において、プロキシ・サーバ２１２は、データ４をコンピュータ・ファイル３とともに、外部システム２に送信することができる。
【００９２】
動作１００６において、プロキシ・サーバ２１２は、コンピュータ・ファイル６の命令５に応じて生成された外部コンピュータ・システム２に関する情報６を受信することができる。外部システム２のプロセッサは、外部システム２のウェブ・ブラウザを実行しながら、命令５を実行することができる。
【００９３】
動作１００７において、コントローラ・サーバ１２は、外部システム２または第３のさらなる外部システムに対してコンピュータ・システム１０を保護するための保護手段を開発するための情報６を提供するために、外部コンピュータ・システム２に関する情報６をコンピュータ・システム１０内に保存することができる。
【００９４】
動作番号１００１、１００２、１００３、１００４、１００５、１００６、１００７は、これらの動作の実行順序を規定するものではない。例えば、いくつかの実施形態では、データ４は、コンピュータ・ファイル３が生成される前に用意されてもよい。
【００９５】
様々な実施形態は、以下の番号付けされた請求項において規定される：
【００９６】
１．コンピュータ・システムへの接続を有する外部コンピュータ・システムに関する情報を取得するためのコンピュータ実装方法であって、前記方法が、
前記接続を介して前記外部コンピュータ・システムからリクエストを受信することと、
前記外部コンピュータ・システムを、前記コンピュータ・システムに対する潜在的な脅威として分類することと、
前記外部コンピュータ・システムを前記潜在的な脅威として分類したことに応答して、前記リクエストに応じたコンピュータ・ファイルを生成することであって、前記コンピュータ・ファイルは命令を含み、前記命令は、前記外部コンピュータ・システムのプロセッサ上で実行された場合に前記外部コンピュータ・システムに関する前記情報を取得するように設計されている、前記生成することと、
前記リクエストに応じたデータを用意することと、
前記データを前記コンピュータ・ファイルとともに、前記外部コンピュータ・システムに送信することと、
前記コンピュータ・ファイルの前記命令に応じて生成された前記外部コンピュータ・システムに関する前記情報を受信することと、
前記コンピュータ・システムを保護するための手段の開発向けに、前記外部コンピュータ・システムに関する前記情報を提供するために前記外部コンピュータ・システムに関する前記情報を前記コンピュータ・システム内に保存することと、
を含む、コンピュータ実装方法。
【００９７】
２．前記コンピュータ・システムが、前記データを提供するデータ・サーバを含み、前記接続がプロキシ・サーバによって確立され、前記方法が、
前記プロキシ・サーバによって前記リクエストを受信することと、
前記プロキシ・サーバによって前記リクエストを前記データ・サーバに方向付けることと、
前記リクエストに応じて、前記データ・サーバから前記プロキシ・サーバに前記デー

タを送信することと、
前記プロキシ・サーバによって前記コンピュータ・ファイルを生成することと、
前記プロキシ・サーバから前記外部コンピュータ・システムへ、前記コンピュータ・ファイルとともに前記データを送信することと、
をさらに含む、請求項１に記載の方法。
【００９８】
３．前記コンピュータ・システムがデータ・サービスを含み、前記リクエストに応じて前記データを前記用意することが、おとりモジュールによって前記データ・サービスを模倣することを含む、請求項１または２に記載の方法。
【００９９】
４．前記方法が、
プロキシ・サーバによって前記接続を確立することと、
前記プロキシ・サーバによって前記リクエストを受信することと、
前記データおよび前記コンピュータ・ファイルをともに、前記プロキシ・サーバから前記外部コンピュータ・システムに送信することと
をさらに含む、請求項３に記載の方法。
【０１００】
５．前記コンピュータ・ファイルが、前記プロキシ・サーバによって生成される、請求項４に記載の方法。
【０１０１】
６．前記方法が、おとりサーバを用意することをさらに含み、前記おとりサーバが、おとりモジュールを含み、前記方法が、プロキシ・サーバから前記おとりサーバに前記リクエストを方向付けることと、前記プロキシ・サーバによって前記おとりサーバから前記データを受信することとをさらに含む、請求項２ないし５のいずれかに記載の方法。
【０１０２】
７．前記方法が、前記外部システムから一連のリクエストを受信することをさらに含み、前記リクエストが、前記一連のリクエストのうち最新のリクエストである、請求項１ないし６のいずれかに記載の方法。
【０１０３】
８．前記リクエストが前記外部コンピュータ・システムに関する初期情報を含み、前記コンピュータ・ファイルが前記外部コンピュータ・システムに関する前記初期情報に応じて生成される、請求項１ないし７のいずれかに記載の方法。
【０１０４】
９．前記方法が、前記外部コンピュータ・システムの分類を実行することをさらに含み、前記データを前記用意することが、前記外部コンピュータ・システムの前記分類の結果に応じて前記データを生成することを含む、請求項１ないし８のいずれかに記載の方法。
【０１０５】
１０．前記方法が、前記外部コンピュータ・システムの分類を実行することをさらに含み、前記命令が前記外部コンピュータ・システムの前記分類の結果に応じて生成される、請求項１ないし９のいずれかに記載の方法。
【０１０６】
１１．前記外部コンピュータ・システムを前記潜在的な脅威として前記分類することが、人工知能モジュール（ＡＩモジュール）によって実行される、請求項１ないし１０のいずれかに記載の方法。
【０１０７】
１２．前記ＡＩモジュールが、ニューロン・ネットワークから構成される、請求項１１に記載の方法。
【０１０８】
１３．前記ＡＩモジュールが、規則ベースの決定モジュールから構成される、請求項１１に記載の方法。

【０１０９】
１４．前記外部コンピュータ・システムに関する前記情報が、前記外部コンピュータ・システムのブラウザ設定に関する情報を含む、請求項１ないし１３のいずれかに記載の方法。
【０１１０】
１５．前記外部コンピュータ・システムに関する前記情報が、前記外部コンピュータ・システムの中央処理装置に関する情報を含む、請求項１ないし１４のいずれかに記載の方法。
【０１１１】
１６．前記外部コンピュータ・システムに関する前記情報が、前記外部コンピュータ・システムのグラフィックス処理装置に関する情報を含む、請求項１ないし１５に記載の方法。
【０１１２】
１７．前記外部コンピュータ・システムに関する前記情報が、前記外部コンピュータ・システムのデータベースのデータを含む、請求項１ないし１６のいずれかに記載の方法。
【０１１３】
１８．前記方法が、前記外部コンピュータ・システムに関する前記情報に応じて、前記コンピュータ・システムを保護するための手段を開発し、実行することをさらに含む、請求項１ないし１７に記載の方法。
【０１１４】
１９．コンピュータ・システムへの接続を有する外部コンピュータ・システムに関する情報を取得するためのコンピュータ・プログラム製品であって、前記コンピュータ・プログラム製品は、１つまたは複数のコンピュータ可読記憶媒体と、前記１つまたは複数のコンピュータ可読記憶媒体に集合的に記憶されたプログラム命令とを含み、前記プログラム命令が、
前記接続を介して前記外部コンピュータ・システムからリクエストを受信するためのプログラム命令と、
前記リクエストに応じて、前記外部コンピュータ・システムを前記コンピュータ・システムに対する潜在的な脅威として分類するためのプログラム命令と、
前記外部コンピュータ・システムを前記潜在的な脅威として分類したことに応答して、前記リクエストに応じたコンピュータ・ファイルを生成するためのプログラム命令であって、前記コンピュータ・ファイルは命令を含み、前記命令は、前記外部コンピュータ・システムのプロセッサ上で実行された場合に前記外部コンピュータ・システムに関する情報を取得するように設計されている、前記生成するためのプログラム命令と、
前記リクエストに応じたデータを用意するためのプログラム命令と、
前記データを前記コンピュータ・ファイルとともに、前記外部コンピュータ・システムに送信するためのプログラム命令と、
前記コンピュータ・ファイルの前記命令に応じて生成された前記外部コンピュータ・システムに関する前記情報を受信するためのプログラム命令と、
前記コンピュータ・システムを保護するための手段の開発向けに、前記外部コンピュータ・システムに関する前記情報を提供するために前記外部コンピュータ・システムに関する前記情報をデータベースに記憶するためのプログラム命令と、を含む、
コンピュータ・プログラム製品。
【０１１５】
２０．コンピュータ・システムへの接続を有する外部コンピュータ・システムに関する情報を取得するためのコンピュータ・システムであって、前記コンピュータ・システムが、
前記接続を介して前記外部コンピュータ・システムからリクエストを受信すること、
前記リクエストに応じて、前記外部コンピュータ・システムを前記コンピュータ・システムに対する潜在的な脅威として分類すること、

前記外部コンピュータ・システムを前記潜在的な脅威として分類したことに応答して、前記リクエストに応じたコンピュータ・ファイルを生成することであって、前記コンピュータ・ファイルが命令を含み、前記命令が、前記外部コンピュータ・システムのプロセッサ上で実行された場合に前記外部コンピュータ・システムに関する前記情報を取得するように設計されている、前記生成すること、

前記リクエストに応じたデータを用意すること、

前記データを前記コンピュータ・ファイルとともに、前記外部コンピュータ・システムに送信することと、

前記コンピュータ・ファイルの前記命令に応じて生成された前記外部コンピュータ・システムに関する前記情報を受信すること、

前記コンピュータ・システムを保護するための手段の開発向けに、前記外部コンピュータ・システムに関する前記情報を提供するために前記外部コンピュータ・システムに関する情報をデータベースに記憶すること、

を行うように構成されている、コンピュータ・システム。

【０１１６】

本開示の実施形態は、システム、方法、またはコンピュータ・プログラム製品あるいはその組合せとすることができる。コンピュータ・プログラム製品は、プロセッサに本開示の態様を遂行させるためのコンピュータ可読プログラム命令をその上に有する１つまたは複数のコンピュータ可読記憶媒体を含み得る。

【０１１７】

コンピュータ可読記憶媒体は、命令実行デバイスによって使用される命令を保持および記憶できる有形のデバイスとすることができる。コンピュータ可読記憶媒体は、例えば、電子記憶装置、磁気記憶装置、光学記憶装置、電磁気記憶装置、半導体記憶装置、またはこれらの任意の適切な組合せとすることができるが、これらに限定されるものではない。コンピュータ可読記憶媒体のより具体的な例の非網羅的な列挙としては、以下が挙げられる：ポータブル・コンピュータ・ディスケット、ハード・ディスク、ランダム・アクセス・メモリ（ＲＡＭ）、読み取り専用メモリ（ＲＯＭ）、消去可能プログラマブル読み取り専用メモリ（ＥＰＲＯＭまたはフラッシュ・メモリ）、静的ランダム・アクセス・メモリ（ＳＲＡＭ）、ポータブル・コンパクト・ディスク読み取り専用メモリ（ＣＤ－ＲＯＭ）、デジタル・バーサタイル・ディスク（ＤＶＤ）、メモリ・スティック、フロッピ・ディスク、命令が記録されたパンチカードまたは溝に刻まれた構造などの機械的にエンコードされたデバイス、および前述のあらゆる好適な組合せ。本明細書において使用される場合、コンピュータ可読記憶媒体は、電波もしくは他の自由に伝搬する電磁波、導波路もしくは他の伝送媒体を介して伝搬する電磁波（例えば、光ファイバ・ケーブルを通過する光パルス）、または電線を介して伝送される電気的信号など、一過性の信号そのものであると解釈されてはならない。

【０１１８】

本明細書において説明されるコンピュータ可読プログラム命令は、コンピュータ可読記憶媒体から個別のコンピューティング／処理デバイスに、あるいは、例えばインターネット、ローカル・エリア・ネットワーク、ワイド・エリア・ネットワークもしくは無線ネットワークまたはその組合せなどのネットワークを介して、外部のコンピュータまたは外部のストレージ・デバイスに、ダウンロードすることができる。ネットワークは、銅の伝送ケーブル、光学伝送ファイバ、無線伝送、ルータ、ファイヤウォール、スイッチ、ゲートウェイ・コンピュータまたはエッジ・サーバあるいはその組合せを備えることができる。それぞれのコンピューティング／処理デバイスのネットワーク・アダプタ・カードまたはネットワーク・インターフェースは、ネットワークからコンピュータ可読プログラム命令を受信し、個別のコンピューティング／処理デバイス内のコンピュータ可読記憶媒体に記憶するためにコンピュータ可読プログラム命令を転送する。

【０１１９】

一部の実施形態におけるいくつかの動作を遂行するためのコンピュータ可読プログラム

命令は、アセンブラ命令、命令セットアーキテクチャ（ＩＳＡ）命令、機械命令、機械依存命令、マイクロコード、ファームウェア命令、状態設定データ、あるいはスモールトーク（Ｒ）、Ｃ＋＋などのオブジェクト指向プログラミング言語、および「Ｃ」プログラミング言語など従来型の手続き型プログラミング言語もしくは類似するプログラミング言語、を含む１つまたは複数のプログラミング言語の任意の組合せで記述された、ソース・コードまたはオブジェクト・コードのいずれかであってもよい。コンピュータ可読プログラム命令は、すべてユーザのコンピュータ上で、一部はユーザのコンピュータ上でスタンドアロンのソフトウェア・パッケージとして、一部はユーザのコンピュータ上で一部はリモート・コンピュータ上で、またはすべてリモート・コンピュータ上もしくはサーバ上で、実行することができる。後者のシナリオでは、リモート・コンピュータは、ローカル・エリア・ネットワーク（ＬＡＮ）もしくはワイド・エリア・ネットワーク（ＷＡＮ）を含む任意のタイプのネットワークを介してユーザのコンピュータに接続することができ、または接続は（例えば、インターネット・サービス・プロバイダを使用してインターネットを介して）外部のコンピュータに対してなされてもよい。いくつかの実施形態において、例えば、プログラマブル・ロジック回路、フィールド・プログラマブル・ゲート・アレイ（ＦＰＧＡ）、またはプログラマブル・ロジック・アレイ（ＰＬＡ）を含む電子回路は、いくつかの実施形態の態様を実行するために、コンピュータ可読プログラム命令の状態情報を利用することによって、コンピュータ可読プログラム命令を実行して電子回路を個別化することができる。

【０１２０】

本開示の態様は、本明細書では、いくつかの実施形態による方法、装置（システム）、およびコンピュータ・プログラム製品のフローチャート図またはブロック図あるいはその両方を参照しながら説明される。フローチャート図またはブロック図あるいはその両方のそれぞれのブロック、およびフローチャート図またはブロック図あるいはその両方におけるブロックの組合せは、コンピュータ可読プログラム命令によって実装されることが理解されよう。

【０１２１】

これらのコンピュータ可読プログラム命令は、コンピュータまたは他のプログラマブル・データ処理装置のプロセッサを介して実行することができる命令が、フローチャートまたはブロック図あるいはその両方の１つまたは複数のブロックに指定される機能／作用／動作を実装するべく、汎用コンピュータ、特殊目的コンピュータ、または他のプログラマブル・データ処理装置のプロセッサに提供されて機械を作るものであってよい。これらのコンピュータ可読プログラム命令はまた、命令を記憶して有するコンピュータ可読記憶媒体が、フローチャートまたはブロック図あるいはその両方の１つまたは複数のブロックに指定される機能／作用の態様を実装する命令を含む製造物品を備えるべく、コンピュータ可読記憶媒体に記憶され、コンピュータ、プログラマブル・データ処理装置、または他のデバイスあるいはその組合せに特定のやり方で機能するように指示できるものであってもよい。

【０１２２】

コンピュータ可読プログラム命令はまた、コンピュータ、他のプログラマブル装置、または他のデバイスで実行する命令が、フローチャートまたはブロック図あるいはその両方の１つまたは複数のブロックに指定される機能／作用を実装するように、コンピュータ実装処理を作るべく、コンピュータ、他のプログラマブル・データ処理装置、または他のデバイス上にロードされ、コンピュータ、他のプログラマブル装置、または他のデバイス上で一連の動作を実行させるものであってもよい。

【０１２３】

図面中のフローチャートおよびブロック図は、本開示の様々な実施形態にしたがって、システム、方法、およびコンピュータ・プログラム製品の可能な実装形態の、アーキテクチャ、機能、および動作を図示している。この点において、フローチャートまたはブロック図のそれぞれのブロックは、指定される論理機能を実装するための１つまたは複数の実

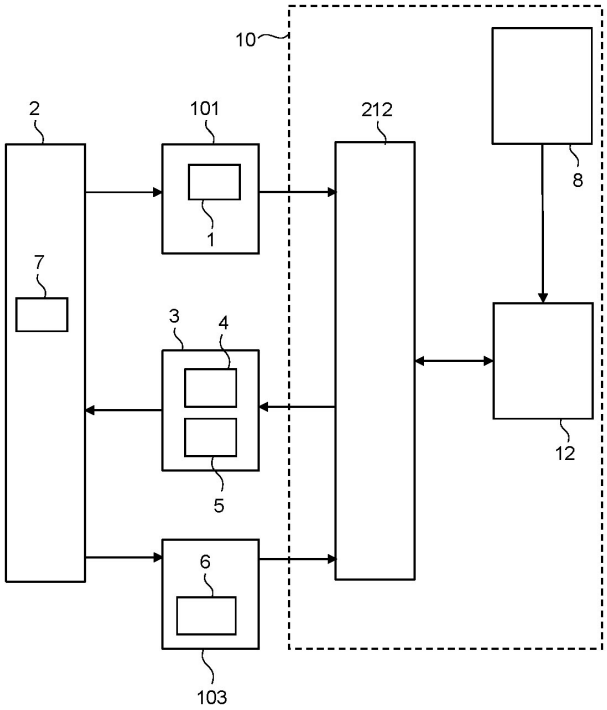
行可能な命令を含む、命令のモジュール、セグメント、または部分を表現することができる。一部の代替的な実装形態において、ブロックで示される機能は図面で示した順とは異なって発生してもよい。例えば、連続して示される２つのブロックは、実際には実質的に同時に実行されてもよく、またはブロックは関与する機能によっては、時に逆の順で実行されてもよい。ブロック図またはフローチャート図あるいはその両方のそれぞれのブロック、およびブロック図またはフローチャート図あるいはその両方のブロックの組合せは、指定される機能もしくは作用を実施する、または特殊目的ハードウェアとコンピュータ命令との組合せを実行する、特殊目的ハードウェア・ベースのシステムによって実装されることにも留意されたい。

【０１２４】

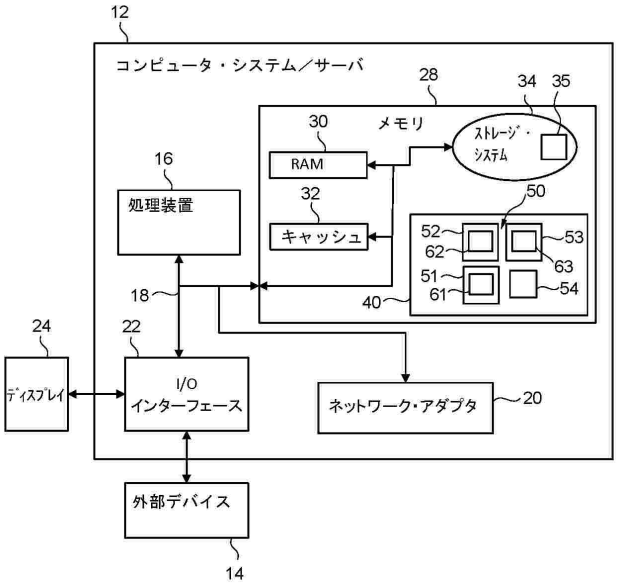
したがって、本明細書で説明される実施形態は、あらゆる点で制限的ではなく例示的なものと考えられ、本発明の範囲を判断するために添付の特許請求の範囲を参照することが望まれる。

【図面】

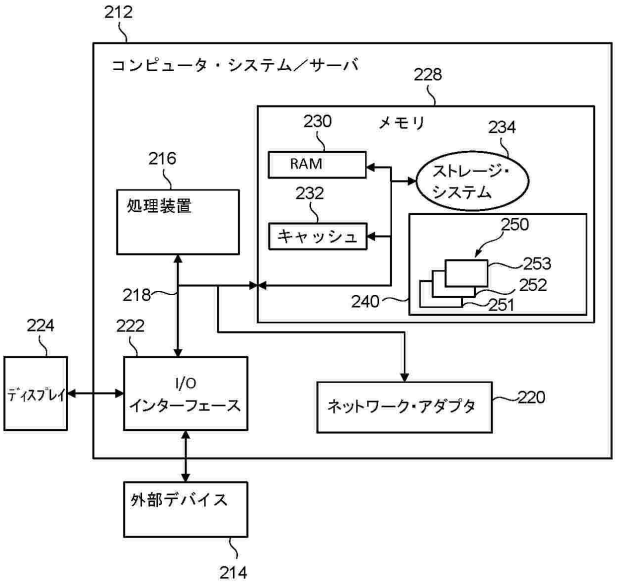
【図１】



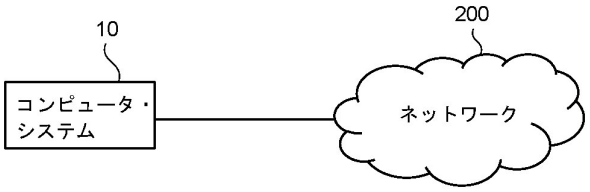
【図２】



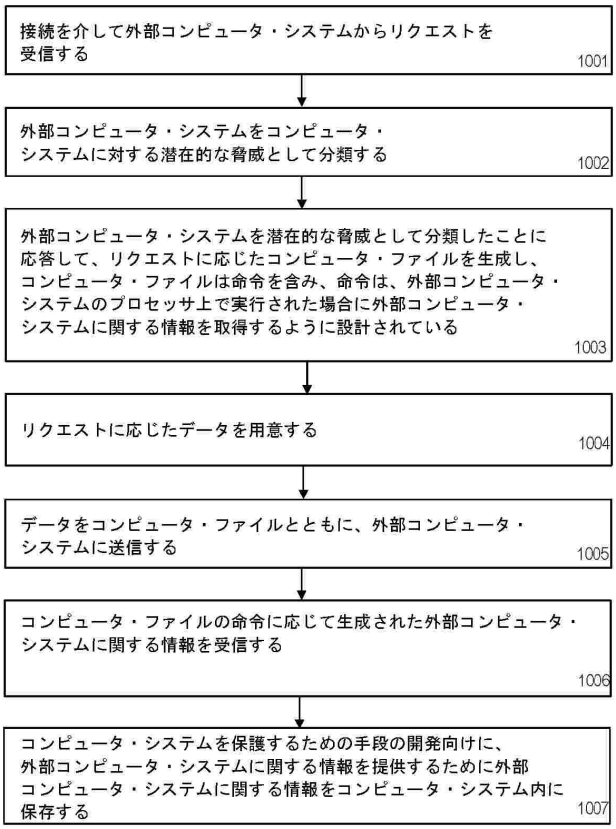
【図３】


212
コンピュータ・システム／サーバ
228
230
メモリ
234
RAM
ストレージ・システム
216
処理装置
232
キャッシュ
250
253
252
251
218
240
224
222
ディスプレイ
I/O インターフェース
ネットワーク・アダプタ
220
外部デバイス
214

【図４】


10
コンピュータ・システム
200
ネットワーク

【図５】


接続を介して外部コンピュータ・システムからリクエストを受信する
1001
外部コンピュータ・システムをコンピュータ・システムに対する潜在的な脅威として分類する
1002
外部コンピュータ・システムを潜在的な脅威として分類したことに応答して、リクエストに応じたコンピュータ・ファイルを生成し、コンピュータ・ファイルは命令を含み、命令は、外部コンピュータ・システムのプロセッサ上で実行された場合に外部コンピュータ・システムに関する情報を取得するように設計されている
1003
リクエストに応じたデータを用意する
1004
データをコンピュータ・ファイルとともに、外部コンピュータ・システムに送信する
1005
コンピュータ・ファイルの命令に応じて生成された外部コンピュータ・システムに関する情報を受信する
1006
コンピュータ・システムを保護するための手段の開発向けに、外部コンピュータ・システムに関する情報を提供するために外部コンピュータ・システムに関する情報をコンピュータ・システム内に保存する
1007

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2022/081209

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/55 H04L9/40 G06N3/00
ADD.

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)
G06F H04L G06N

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

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 2 779 574 A1 (JUNIPER NETWORKS INC [US]) 17 September 2014 (2014-09-17)	1,2,4,5, 7-10, 14-20
Y	paragraph [0012] - paragraph [0062]; figures 1-5	3,6, 11-13
Y	US 2021/067553 A1 (RIES CHRISTOPHER JAMES [US] ET AL) 4 March 2021 (2021-03-04) paragraph [0029] - paragraph [0042]	3,6, 11-13
A	WO 2009/032379 A1 (UNIV COLUMBIA [US]; STOLFO SALVATORE J [US]; KEROMYTIS ANGELOS D [US]) 12 March 2009 (2009-03-12) paragraph [0068]; figure 3	1-20

☐ 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	Date of mailing of the international search report
16 February 2023	27/02/2023

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Jascau, Adrian

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2022/081209

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 2779574 A1	17-09-2014	CN 104052734 A	17-09-2014
		EP 2779574 A1	17-09-2014
		US 2014283061 A1	18-09-2014
US 2021067553 A1	04-03-2021	CN 114342319 A	12-04-2022
		EP 4026297 A1	13-07-2022
		JP 2022547485 A	14-11-2022
		US 2021067553 A1	04-03-2021
		WO 2021046094 A1	11-03-2021
WO 2009032379 A1	12-03-2009	NONE	

Form PCT/ISA/210 (patent family annex) (April 2005)

フロントページの続き

MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,KM,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BN,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,CV,CV,CZ,DE,DJ,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IQ,IR,IS,IT,JM,JO,JP,KE,KG,KH,KN,KP,KR,KW,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,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,WS,ZA,ZM,ZW

(74)代理人　100120710
弁理士　片岡 忠彦
(72)発明者　パルーチ、ミハル
ポーランド３０－１５０ クラクフ アレヤ・アルミイ・クラヨベイ１８
(72)発明者　コヴァルチク、シモン
ポーランド３０－１５０ クラクフ アレヤ・アルミイ・クラヨベイ１８
(72)発明者　グリュンセイゼン、イリー
チェコ ブルノ６１６００ テクニカ２９９５／２１
(72)発明者　ブトゥーチア パナイト、マーセル
チェコ ブルノ６１６００ テクニカ２９９５／２１