(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2013-232716
(P2013-232716A)
(43)公開日　平成25年11月14日(2013.11.14)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 12/66	(2006.01)	H04L	12/66	B	5K030
G06F 21/55	(2013.01)	G06F	21/00	155C	

審査請求 未請求　請求項の数 6　ＯＬ　（全 19 頁）

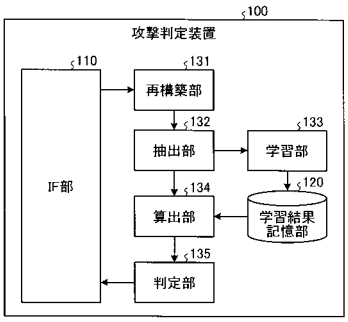
(21)出願番号　特願2012-102602 (P2012-102602)
(22)出願日　平成24年4月27日 (2012.4.27)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(74)代理人　100089118
弁理士　酒井　宏明
(74)代理人　100112656
弁理士　宮田　英毅
(72)発明者　朝倉　浩志
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

Ｆターム(参考)　5K030 GA15　HA08　HC01　HD03　JA10　LC13

(54)【発明の名称】攻撃判定装置、攻撃判定方法及び攻撃判定プログラム

(57)【要約】
【課題】未知の攻撃を検知すること。
【解決手段】攻撃判定装置は、正常であることが既知である正常アクセス要求が情報処理装置に送信された場合に、正常アクセス要求に設定されている設定情報を正常情報として学習する。また、攻撃判定装置は、学習した正常情報の集合を記憶する。また、攻撃判定装置は、正常であることが既知でない未知アクセス要求が情報処理装置に送信された場合に、未知アクセス要求に設定されている設定情報が正常情報の集合に分類される度合いを示す指標値を算出する。また、攻撃判定装置は、算出した指標値に基づいて、未知アクセス要求が情報処理装置に対する攻撃であるか否かを判定する。
【選択図】図３



【特許請求の範囲】
【請求項１】
正常であることが既知である正常アクセス要求が情報処理装置に送信された場合に、当該正常アクセス要求に設定されている設定情報を正常情報として学習する学習部と、
前記学習部によって学習された正常情報の集合を記憶する学習結果記憶部と、
正常であることが既知でない未知アクセス要求が前記情報処理装置に送信された場合に、当該未知アクセス要求に設定されている設定情報が前記正常情報の集合に分類される度合いを示す指標値を算出する算出部と、
前記算出部によって算出された指標値に基づいて、前記未知アクセス要求が前記情報処理装置に対する攻撃であるか否かを判定する判定部と
を備えたことを特徴とする攻撃判定装置。
【請求項２】
前記学習部は、
前記正常アクセス要求に設定されている設定情報の属性毎に、当該設定情報を前記正常情報として学習し、
前記学習結果記憶部は、
前記学習部によって学習された正常情報の集合を前記属性毎に記憶し、
前記算出部は、
前記未知アクセス要求に設定されている設定情報が当該設定情報の属性に対応する前記正常情報の集合に分類されるか否かを示す指標値を算出する
ことを特徴とする請求項１に記載の攻撃判定装置。
【請求項３】
前記学習部は、
前記正常アクセス要求に設定されている設定情報のサイズが所定のサイズ閾値よりも大きい場合に、当該設定情報を分解した部分設定情報を前記正常情報として学習し、
前記算出部は、
前記未知アクセス要求に設定されている設定情報のサイズが前記サイズ閾値よりも大きい場合に、当該設定情報を分解した部分設定情報が前記正常情報の集合に分類されるか否かを示す指標値を算出する
ことを特徴とする請求項２に記載の攻撃判定装置。
【請求項４】
前記学習部は、
前記未知アクセス要求に設定されている設定情報を分解した部分設定情報を当該設定情報の属性に対応する線形識別器に訓練例データとして入力することにより、当該部分設定情報を前記正常情報として学習し、
前記算出部は、
前記未知アクセス要求に設定されている設定情報のサイズが前記サイズ閾値以下である場合に、当該設定情報と前記正常情報の集合との類似度を前記指標値として算出し、前記未知アクセス要求に設定されている設定情報のサイズが前記サイズ閾値よりも大きい場合に、当該設定情報を分解した各部分設定情報を当該設定情報の属性に対応する線形識別器に判定対象データとして入力することにより、当該各部分設定情報が前記正常情報の集合に分類される尤度を前記指標値として算出し、
前記判定部は、
前記類似度が所定の類似度閾値よりも低い設定情報の数、又は、前記尤度が所定の尤度閾値よりも低い部分設定情報の数が所定数よりも多い場合に、前記未知アクセス要求が攻撃であると判定する
ことを特徴とする請求項３に記載の攻撃判定装置。
【請求項５】
攻撃判定装置が実行する攻撃判定方法であって、
正常であることが既知である正常アクセス要求が情報処理装置に送信された場合に、当

該正常アクセス要求に設定されている設定情報を正常情報として学習する学習ステップと、
前記学習ステップにおいて学習された正常情報の集合を学習結果記憶部に格納する格納ステップと、
正常であることが既知でない未知アクセス要求が前記情報処理装置に送信された場合に、当該未知アクセス要求に設定されている設定情報が前記正常情報の集合に分類される度合いを示す指標値を算出する算出ステップと、
前記算出ステップにおいて算出された指標値に基づいて、前記未知アクセス要求が前記情報処理装置に対する攻撃であるか否かを判定する判定ステップと
を含んだことを特徴とする攻撃判定方法。

【請求項６】
コンピュータを請求項１～４のいずれか一つに記載の攻撃判定装置として機能させるための攻撃判定プログラム。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明の実施形態は、攻撃判定装置、攻撃判定方法及び攻撃判定プログラムに関する。

【背景技術】
【０００２】
従来、インターネットの普及に伴い、アプリケーションの配信を実施するサーバに対するサイバー攻撃が急増している。サイバー攻撃の代表例としては、Ｗｅｂアプリケーションの脆弱性を狙った不正なＨＴＴＰ（HyperText Transfer Protocol）リクエスト、ＳＱＬ（Structured Query Language）インジェクション、クロスサイトスクリプティング攻撃などが挙げられる。
【０００３】
このような攻撃への対策として、ＩＤＳ（Intrusion Detection System）、ＩＰＳ（Intrusion Prevention System）、ＷＡＦ（Web Application Firewall）などと呼ばれるネットワークへの不正侵入検知・防御システムが知られている。これらのシステムでは、様々な攻撃手法をパターン化した「ブラックリスト」や「シグネチャファイル」を用いて、パターンに合致する攻撃を検知及び防御することが行われる。

【先行技術文献】
【非特許文献】
【０００４】
【非特許文献１】山田明、三宅優、竹森敬祐、田中俊昭著　「学習データを自動生成する未知攻撃検知システム」　情報処理学会論文誌、ｖｏｌ．４６、Ｎｏ．８　２００５年８月

【発明の概要】
【発明が解決しようとする課題】
【０００５】
しかしながら、上記の従来技術では、未知の攻撃を検知することが困難であった。具体的には、攻撃は日々進化するので、既知の攻撃を予めパターン化しておく手法の場合には、攻撃が既知となってから検知対象及び防御対象の攻撃をパターン化することを要し、未知の攻撃に対応することが困難であった。さらに、攻撃をパターン化する手法の場合には、新たな攻撃が発見されるたびに、専門家等が攻撃を解析してパターン化したデータを作成することを要するので、攻撃に対する対応コストがかかるという問題も招く。
【０００６】
本願の開示する技術は、上記に鑑みてなされたものであって、未知の攻撃を検知することができる攻撃判定装置、攻撃判定方法及び攻撃判定プログラムを提供することを目的とする。

【課題を解決するための手段】

【０００７】
実施形態に係る攻撃判定装置は、正常であることが既知である正常アクセス要求が情報処理装置に送信された場合に、当該正常アクセス要求に設定されている設定情報を正常情報として学習する学習部と、前記学習部によって学習された正常情報の集合を記憶する学習結果記憶部と、正常であることが既知でない未知アクセス要求が前記情報処理装置に送信された場合に、当該未知アクセス要求に設定されている設定情報が前記正常情報の集合に分類される度合いを示す指標値を算出する算出部と、前記算出部によって算出された指標値に基づいて、前記未知アクセス要求が前記情報処理装置に対する攻撃であるか否かを判定する判定部とを備えることを特徴とする。
【発明の効果】
【０００８】
実施形態に係る攻撃判定装置、攻撃判定方法及び攻撃判定プログラムは、未知の攻撃を検知することができるという効果を奏する。
【図面の簡単な説明】
【０００９】
【図１】図１は、第１の実施形態に係るネットワークシステムの構成例を示す図である。
【図２】図２は、第１の実施形態に係る攻撃判定装置によって検知される攻撃の一例を示す説明図である。
【図３】図３は、第１の実施形態に係る攻撃判定装置の構成例を示す図である。
【図４】図４は、第１の実施形態に係る再構築部及び抽出部による処理例を示す説明図である。
【図５】図５は、第１の実施形態に係る攻撃判定装置による学習処理手順を示すフローチャートである。
【図６】図６は、第１の実施形態に係る攻撃判定装置による攻撃判定処理手順を示すフローチャートである。
【図７】図７は、攻撃判定プログラムを実行するコンピュータを示す図である。
【発明を実施するための形態】
【００１０】
以下に、本願に係る攻撃判定装置、攻撃判定方法及び攻撃判定プログラムの実施形態を図面に基づいて詳細に説明する。なお、この実施形態により本願に係る攻撃判定装置、攻撃判定方法及び攻撃判定プログラムが限定されるものではない。
【００１１】
（第１の実施形態）
［ネットワークシステムの構成］
まず、図１を用いて、第１の実施形態に係るネットワークシステムについて説明する。図１は、第１の実施形態に係るネットワークシステム１の構成例を示す図である。図１に例示したネットワークシステム１には、ユーザ端末１１及び１２と、ネットワーク２０と、ネットワーク機器３０と、サーバ装置４０と、プローブ５０と、攻撃判定装置１００とを含まれる。ユーザ端末１１及び１２とサーバ装置４０は、ネットワーク２０及びネットワーク機器３０を介して、互いに通信可能に接続される。
【００１２】
なお、ネットワークシステム１に含まれる各装置の台数は、図１に示した例に限られない。例えば、ネットワークシステム１には、２台以上のユーザ端末１１、ユーザ端末１２、ネットワーク機器３０、サーバ装置４０、プローブ５０、攻撃判定装置１００が含まれてもよい。
【００１３】
ユーザ端末１１及び１２は、ユーザによって利用される情報処理装置であり、例えば、ＰＣ（Personal Computer）や携帯端末装置などである。かかるユーザ端末１１及び１２は、利用者による操作に従って、サーバ装置４０にアクセスする。ここで、第１の実施形態において、ユーザ端末１１は、悪意のない利用者（例えば、攻撃判定装置１００の管理

者等）によって利用され、サーバ装置４０に対して正常なアクセスを行うものとする。一方、ユーザ端末１２は、悪意のある攻撃者によって利用され、サーバ装置４０に対して攻撃（不正アクセス等のサイバー攻撃）を行う場合があるものとする。

【００１４】

ネットワーク２０は、例えば、ＷＡＮ（Wide Area Network）やＬＡＮ（Local Area Network）であり、通信網を形成する。なお、ネットワーク２０は、有線ネットワークを形成してもよいし、無線ネットワークを形成してもよい。

【００１５】

ネットワーク機器３０は、サーバ装置４０とネットワーク２０との間を仲介する装置であり、例えば、スイッチやルータである。

【００１６】

サーバ装置４０は、各種サービスを提供する情報処理装置である。例えば、サーバ装置４０は、Ｗｅｂアプリケーションがインストールされており、ユーザ端末１１又は１２からの要求に応答して、各種Ｗｅｂサービスを提供する。なお、サーバ装置４０は、サーバ装置だけでなく、各種データを記憶するストレージ装置等を具備してもよい。

【００１７】

プローブ５０は、ネットワーク機器３０を流通する各種通信パケットを取得（キャプチャ）し、取得した通信パケットを攻撃判定装置１００に出力する。第１の実施形態に係るプローブ５０は、ユーザ端末１１又は１２からサーバ装置４０に対する通信パケット（例えば、ＨＴＴＰリクエスト等のアクセス要求）を取得する。なお、プローブ５０は、ネットワーク機器３０と一体化されてもよい。

【００１８】

攻撃判定装置１００は、プローブ５０から出力される通信パケットを用いて、サーバ装置４０に対して攻撃が行われているか否かを判定する。具体的には、第１の実施形態に係るネットワークシステム１では、まず、管理者等によって利用されるユーザ端末１１のみがサーバ装置４０に対してアクセス可能であり、ユーザ端末１２等の外部からサーバ装置４０に対してアクセスできない学習用の通信環境を形成する。そして、ユーザ端末１１は、学習用の通信環境において、サーバ装置４０に対して繰り返しアクセスを行うことで、正常であることが既知であるアクセス要求をサーバ装置４０に送信する。このとき、攻撃判定装置１００は、サーバ装置４０に送信された正常であることが既知であるアクセス要求に設定されている設定情報（後述するクエリ）を学習し、学習した設定情報を正常情報の集合として保持しておく。

【００１９】

そして、攻撃判定装置１００は、学習用の通信環境ではなく通常運用の通信環境において、正常であることが既知でないアクセス要求がサーバ装置４０に送信された場合に、かかるアクセス要求に設定されている設定情報が、前述した正常情報の集合に分類される度合いを示す指標値を算出する。そして、攻撃判定装置１００は、算出した指標値に基づいて、かかるアクセス要求がサーバ装置４０に対する攻撃であるか否かを判定する。

【００２０】

このように、第１の実施形態に係る攻撃判定装置１００は、設定情報が正常情報の集合に分類される指標値を用いて攻撃判定を行うので、予めパターン化された攻撃のシグネチャファイルやブラックリストを要することなく、サーバ装置４０に対する未知の攻撃を検知することができる。すなわち、攻撃判定装置１００は、専門家等によるパターン化データの作成に要するコストを低減することができるとともに、未知の攻撃を検知することができる。

【００２１】

ここで、図２を用いて、第１の実施形態に係る攻撃判定装置１００によって検知される攻撃について説明する。図２は、第１の実施形態に係る攻撃判定装置１００によって検知される攻撃の一例を示す説明図である。

【００２２】

図２（１）に示した例のように、アノーマリ型のＩＰＳは、「ネットワーク攻撃やＤｏＳ攻撃（SYN flood攻撃など）」、「システムやアプリケーションの探索」、「異常な形式のパケットやコンテンツを利用した攻撃」などを検知する。また、図２（２）に示した例のように、アプリケーション型のＦＷは、「管理者が許可していないアクセス」、「不正なＰ２Ｐ（Peer to Peer）アプリケーションの利用」などを検知する。

【００２３】

また、図２（３）に示した例のように、シグネチャ型のＩＰＳは、「ＯＳ（Operating System）やサービスの脆弱性を狙った攻撃や侵入」、「Ｗｅｂアプリケーションの脆弱性の一部」などを検知する。また、図２（４）に示した例のように、アンチウィルスは、「ウィルスやワームやトロイの木馬などの有害なコンテンツ」、「スパムメールやフィッシング」などを検知する。

【００２４】

また、図２（５）に示した例のように、ＷＡＦは、Ｗｅｂアプリケーションの脆弱性を狙った「不正なＨＴＴＰリクエスト」や「ＳＱＬインジェクション」や「クロスサイトスクリプティング攻撃」などを検知する。この種のＷｅｂアプリケーションの脆弱性を狙った各種攻撃は、常に未知の攻撃が開発されている。また、大々的なニュースとなるサイバー攻撃は、主にこの種のＷｅｂアプリケーションの脆弱性を狙った攻撃であり、このような攻撃を受けた場合には、企業経営に大きな打撃を与える。しかし、一般的なＷＡＦは、予め攻撃手法をパターン化したシグネチャファイル等を用いて、攻撃を検知するので、未知の攻撃を検知することが困難であった。

【００２５】

そこで、第１の実施形態に係る攻撃判定装置１００は、図２に示した各種攻撃のうち、主にＷｅｂアプリケーションの脆弱性を狙った攻撃（図２（５））を検知する。これにより、第１の実施形態に係る攻撃判定装置１００は、常に未知の攻撃が開発されている攻撃を検知することができるので、サイバー攻撃により大々的なニュースとなることを防止するとともに、企業経営に大きな打撃を与えることを防止することを可能にする。

【００２６】

［攻撃判定装置の構成］

次に、図３を用いて、第１の実施形態に係る攻撃判定装置１００について説明する。図３は、第１の実施形態に係る攻撃判定装置１００の構成例を示す図である。なお、以下では、サーバ装置４０がＷｅｂサーバとして動作しており、ユーザ端末１１及び１２がサーバ装置４０に対してＨＴＴＰリクエストを送信する場合を例に挙げて説明する。

【００２７】

図３に例示するように、第１の実施形態に係る攻撃判定装置１００は、ＩＦ（interface）部１１０と、学習結果記憶部１２０と、再構築部１３１と、抽出部１３２と、学習部１３３と、算出部１３４と、判定部１３５とを有する。

【００２８】

ＩＦ部１１０は、例えば、ＮＩＣ（Network Interface Card）等であり、外部装置との間で各種データを送受信する。例えば、ＩＦ部１１０は、プローブ５０から通信パケットを受信する。

【００２９】

学習結果記憶部１２０は、サーバ装置４０に送信された正常なＨＴＴＰリクエストに含まれる各種情報のうち、ＨＴＴＰリクエストの送信者によって任意に設定可能な設定情報（後述するクエリ）の集合を学習結果（上述した正常情報）として記憶する。第１の実施形態において、「正常なＨＴＴＰリクエスト」とは、ユーザ端末１１からサーバ装置４０に送信されるＨＴＴＰリクエストを示す。

【００３０】

具体的には、ＨＴＴＰリクエストには、送信者によって任意に設定可能な設定情報が、属性名（attribute）と属性値（value）との組合せによって形成されるクエリとして設定される。上記の学習結果記憶部１２０は、正常なＨＴＴＰリクエストに設定される属性名

（attribute）毎に、かかる属性名に対応する正常な属性値（value）を記憶する。

【００３１】

また、後述する学習部１３３は、ソフトウェア等によって実現される線形識別器（例えば、ベイズフィルタ等であり、「線形分類器」等とも呼ばれる）を属性名毎に具備する。この属性名毎の線形識別器は、属性名に対応する正常な属性値が訓練例データとして入力されることにより、かかる正常な属性値を学習する。すなわち、第１の実施形態に係る線形識別器は、所定の属性値が判定対象データとして入力された場合に、かかる属性値が正常である尤度（「スコア」とも呼ばれる）を出力することとなる。上記の学習結果記憶部１２０は、このような線形識別器によって学習される正常な属性値の集合を線形識別器毎（すなわち、属性名毎）に記憶する。

【００３２】

なお、学習結果記憶部１２０は、属性値のサイズに応じて、属性名毎に正常な属性値を記憶するか、属性名毎の線形識別器によって学習された正常な属性値を属性名毎に記憶するかが決定される。この点については、後に学習部１３３とともに説明する。

【００３３】

このような学習結果記憶部１２０は、例えば、ＲＡＭ（Random Access Memory)、フラッシュメモリ（Flash Memory）等の半導体メモリ素子、又は、ハードディスク、光ディスク等によって実現される。

【００３４】

続いて、再構築部１３１、抽出部１３２、学習部１３３、算出部１３４及び判定部１３５について説明するが、再構築部１３１及び抽出部１３２は、正常であることが既知であるＨＴＴＰリクエストのみがサーバ装置４０に送信される学習用の通信環境下と、正常であることが既知でないＨＴＴＰリクエストがサーバ装置４０に送信される通常運用の通信環境下との双方において動作する。一方、学習部１３３は、学習用の通信環境下において動作し、通常運用の通信環境下においては動作しない。また、算出部１３４及び判定部１３５は、通常運用の通信環境下において動作し、学習用の通信環境下においては動作しない。

【００３５】

このような再構築部１３１、抽出部１３２、学習部１３３、算出部１３４及び判定部１３５は、例えば、ＡＳＩＣ（Application Specific Integrated Circuit）やＦＰＧＡ（Field Programmable Gate Array）等の集積回路により実現される。また、再構築部１３１、抽出部１３２、学習部１３３、算出部１３４及び判定部１３５は、例えば、ＣＰＵ（Central Processing Unit）やＭＰＵ（Micro Processing Unit）等によって、図示しない記憶装置に記憶されているプログラムがＲＡＭを作業領域として実行されることにより実現される。

【００３６】

再構築部１３１は、ＩＦ部１１０を介してプローブ５０から受信した通信パケットから、サーバ装置４０に対するＨＴＴＰリクエストを再構築する。具体的には、プローブ５０によって取得された通信パケットは、ビット列である。再構築部１３１は、このようなビット列からＨＴＴＰリクエストを再構築する。

【００３７】

抽出部１３２は、再構築部１３１によって再構築されたＨＴＴＰリクエストからクエリ（Query）を抽出する。そして、抽出部１３２は、ＨＴＴＰリクエストから抽出したクエリを属性名及び属性値の組合せ毎に分解することにより、属性名及び属性値の組合せを抽出する。具体的には、ＨＴＴＰリクエストのクエリは、「属性名＝属性値」の形式で記述される。さらに、ＨＴＴＰリクエストのクエリは、属性名及び属性値の組合せが複数含まれる場合には、「属性名＝属性値」との間に区切り文字列として「＆」が記述される。抽出部１３２は、このような記述形式を解析することにより、クエリから属性名及び属性値の組合せを抽出する。

【００３８】

抽出部１３２がクエリを抽出する理由について説明する。ユーザ端末１２等の利用者である攻撃者は、正常なアクセスを装ってサーバ装置４０に対して攻撃を行う。ただし、攻撃時のＨＴＴＰリクエストに含まれるクエリは、正常なアクセスとは一般的に異なる。そこで、第１の実施形態では、正常なアクセス又は異常なアクセスであるかを判定するために、ＨＴＴＰリクエストからクエリを抽出する。

【００３９】

ここで、図４を用いて、上記の再構築部１３１及び抽出部１３２による処理について説明する。図４は、第１の実施形態に係る再構築部１３１及び抽出部１３２による処理例を示す説明図である。なお、図４では、サーバ装置４０に対して、リクエストＵＲＩ（Uniform Resource Identifier）がＨＴＴＰリクエストとして送信される例を示す。

【００４０】

図４に示した例において、プローブ５０は、ネットワーク機器３０から通信パケットＰ１１を取得したものとする。かかる場合に、攻撃判定装置１００の再構築部１３１は、通信パケットＰ１１からＨＴＴＰリクエストＰ１２を再構築する。なお、図４では、再構築部１３１によって再構築されたＨＴＴＰリクエストＰ１２のうち、ＨＴＴＰヘッダの部分のみを例示している。

【００４１】

そして、抽出部１３２は、図４のＨＴＴＰリクエストＰ１２から、クエリ部分ｑ１２である「/redirect.php?test=a%0d%0aLocation:%20http://attack.example.com/」を抽出する。そして、抽出部１３２は、かかるクエリ部分ｑ１２から、属性名「test」と属性値「a%0d%0aLocation:%20http://attack.example.com/」との組合せを抽出する。

【００４２】

また、図４の例では、クエリ部分ｑ１２に１組の属性名及び属性値が含まれる例を示した。しかし、抽出部１３２は、ＨＴＴＰリクエストから、例えば、「name=%91%BE%98Y&OS=win&submit=%91%97%90M%91%97%90M・・・%91」といったクエリを抽出する場合もある。抽出部１３２は、ＨＴＴＰリクエストのメソッドがＰＯＳＴやＰＵＴである場合に、このようなクエリを抽出する場合がある。この例の場合、クエリに３組の属性名及び属性値が含まれる。すなわち、抽出部１３２は、かかるクエリから、属性名「name」及び属性値「%91%BE%98Y」の組合せと、属性名「OS」及び属性値「win」の組合せと、属性名「submit」及び属性値「%91%97%90M%91%97%90M・・・%91」の組合せとを抽出することとなる。

【００４３】

学習部１３３は、抽出部１３２によって抽出された属性名及び属性値の組合せを用いて、正常なアクセスに含まれる属性名及び属性値の組合せを学習し、正常なアクセスにおける属性名毎に、属性値の集合を学習結果記憶部１２０に格納する。また、学習部１３３は、上記の通り、属性名毎に、ソフトウェア等によって実現される線形識別器を具備する。

【００４４】

学習部１３３による処理について具体的に説明する。学習部１３３は、抽出部１３２によって正常なＨＴＴＰリクエストから抽出された属性名及び属性値の組合せ毎に以下の処理を行う。まず、学習部１３３は、抽出部１３２によって抽出された属性値のサイズ（バイト数）が所定の閾値（以下、「サイズ閾値Ｔ１」とする）よりも大きいか否かを判定する。そして、学習部１３３は、属性値のサイズがサイズ閾値Ｔ１よりも大きい場合には、かかる属性値をデコードする。そして、学習部１３３は、デコード後の属性値を形態素解析することにより、素性（feature）に分解する。そして、学習部１３３は、抽出部１３２によって抽出された属性名に対応する線形識別器に対して、分解後の素性を訓練例データとして入力する。これにより、各線形識別器は、分解後の素性を学習し、学習した素性を学習結果記憶部１２０に格納する。

【００４５】

なお、以下では、学習結果記憶部１２０に記憶される線形識別器による学習結果を「learn（attribute、［素性（集合）］）」と表記する場合がある。すなわち、属性名「submit」に対応する線形識別器によって、素性Ｘ１、素性Ｘ２及び素性Ｘ３が学習された場合

、かかる線形識別器による学習結果は、「lern（submit、［素性Ｘ１、素性Ｘ２、素性Ｘ３］）」となる。

【００４６】

例えば、上記例のように、抽出部１３２によって、属性名「submit」と属性値「%91%97%90M%91%97%90M・・・%91」との組合せが抽出されたものとする。また、この属性値のサイズがサイズ閾値Ｔ１よりも大きいものとする。かかる場合に、学習部１３３は、属性値「%91%97%90M%91%97%90M・・・%91」をデコードする。ここでは、学習部１３３は、デコード結果として、「ＡＡＡＢＢＢＣＣＣ」を取得したものとする。そして、学習部１３３は、属性値「ＡＡＡＢＢＢＣＣＣ」を形態素解析することで、例えば、素性「ＡＡＡ」、「ＢＢＢ」及び「ＣＣＣ」を得る。このような場合に、学習部１３３は、属性名「submit」に対応する線形識別器に対して、正常な属性値の集合として、素性「ＡＡＡ」、「ＢＢＢ」及び「ＣＣＣ」を学習させる。この結果、学習結果記憶部１２０は、属性名「submit」に対応する線形識別器の学習結果として、素性「ＡＡＡ」、「ＢＢＢ」及び「ＣＣＣ」を記憶する。すなわち、学習結果記憶部１２０は、「lern（submit、［ＡＡＡ、ＢＢＢ、ＣＣＣ］）」を記憶する。

【００４７】

また、この後に、抽出部１３２によって、属性名「submit」と所定の属性値との組合せが新たに抽出されたものとする。また、所定の属性値は、サイズがサイズ閾値Ｔ１よりも大きく、学習部１３３によるデコード結果が「ＤＤＤＥＥＥＦＦＦ」であり、形態素解析の結果が素性「ＤＤＤ」、「ＥＥＥ」及び「ＦＦＦ」であったものとする。かかる場合に、学習部１３３は、属性名「submit」に対応する線形識別器に対して、正常な属性値の集合として、素性「ＤＤＤ」、「ＥＥＥ」及び「ＦＦＦ」を学習させる。この結果、学習結果記憶部１２０は、属性名「submit」に対応する線形識別器の学習結果として、素性「ＡＡＡ」、「ＢＢＢ」及び「ＣＣＣ」に加えて、「ＤＤＤ」、「ＥＥＥ」及び「ＦＦＦ」を記憶する。すなわち、学習結果記憶部１２０は、「lern（submit、［ＡＡＡ、ＢＢＢ、ＣＣＣ、ＤＤＤ、ＥＥＥ、ＦＦＦ］）」を記憶する。

【００４８】

一方、学習部１３３は、抽出部１３２によって抽出された属性値のサイズがサイズ閾値Ｔ１以下である場合には、かかる属性値を線形識別器に学習させることが困難である可能性があるので、正常なＨＴＴＰリクエストに含まれる属性名に対応する正常な属性値集合として、かかる属性値を学習結果記憶部１２０に格納する。

【００４９】

なお、以下では、学習結果記憶部１２０に記憶される属性名（attribute）に対応する正常な属性値集合を「Correct（attribute）」と表記する場合がある。すなわち、属性名「submit」に対応する正常な属性値集合は、「Correct（submit）」となる。

【００５０】

例えば、抽出部１３２によって、属性名「test」と属性値「%91%97%90M」との組合せが抽出されたものとする。また、この属性値のサイズがサイズ閾値Ｔ１以下であるものとする。かかる場合に、学習部１３３は、属性名「test」の学習結果として、属性値「%91%97%90M」を学習結果記憶部１２０に格納する。また、この後に、抽出部１３２によって、属性名「test」と属性値「%91%91%91M」との組合せが新たに抽出されたものとする。また、属性値「%91%91%91M」のサイズはサイズ閾値Ｔ１以下であるものとする。かかる場合に、学習部１３３は、属性名「test」の学習結果として、属性値「%91%97%90M」に加えて、属性値「%91%91%91M」を学習結果記憶部１２０に格納する。すなわち、学習結果記憶部１２０は、属性値集合「Correct（test）=（%91%97%90M、%91%91%91M）」を記憶することとなる。

【００５１】

このように、学習部１３３は、抽出部１３２によって正常なＨＴＴＰリクエストから抽出された属性名及び属性値の組合せを学習し、学習結果を学習結果記憶部１２０に格納する。これにより、学習結果記憶部１２０は、正常なＨＴＴＰリクエストに含まれていた属

性名毎に、かかる属性名に対応する正常な属性値の集合を記憶することとなる。

【００５２】

算出部１３４は、正常であることが既知でないＨＴＴＰリクエストがサーバ装置４０に送信された場合に、抽出部１３２によって抽出された属性値が、学習結果記憶部１２０に記憶されている正常な設定情報（上述した正常情報）の集合に分類される度合いを示す指標値を算出する。

【００５３】

具体的には、算出部１３４は、抽出部１３２によって抽出された属性名と属性値との組合せ毎に以下の処理を行う。まず、算出部１３４は、抽出部１３２によって抽出された属性値のサイズがサイズ閾値Ｔ１よりも大きいか否かを判定する。そして、算出部１３４は、属性値のサイズがサイズ閾値Ｔ１よりも大きい場合には、かかる属性値をデコードし、デコード後の属性値を形態素解析することにより素性に分解する。そして、算出部１３４は、抽出部１３２によって抽出された属性名に対応する線形識別器に対して、分解後の素性を判定対象データとして入力することにより、素性毎に、かかる素性が正常情報の集合に分類される尤度（以下、「分類尤度」と表記する場合がある）を上記指標値として算出する。なお、分類尤度は、線形識別器によって出力される。

【００５４】

また、算出部１３４は、抽出部１３２によって抽出された属性値のサイズがサイズ閾値Ｔ１以下である場合には、学習結果記憶部１２０に記憶されている属性値集合「Correct（attribute）」と、かかる属性値との類似度（言い換えれば、「異なり度合い」）を上記指標値として算出する。

【００５５】

例えば、算出部１３４は、抽出部１３２によって抽出された属性名に対応する属性値集合「Correct（attribute）」を学習結果記憶部１２０から取得する。そして、算出部１３４は、抽出部１３２によって抽出された属性値と、学習結果記憶部１２０から取得した属性値集合「Correct（attribute）」とのレーベンシュタイン距離を算出し、算出したレーベンシュタイン距離のうち、最小のレーベンシュタイン距離を上記類似度（すなわち、指標値）として選択する。

【００５６】

この点についてより具体的に説明すると、算出部１３４は、例えば、レーベンシュタイン距離を算出するための関数「Ｆ（ｘ、ｙ）」を用いる。かかる関数「Ｆ（ｘ、ｙ）」のうち、「ｘ」は、抽出部１３２によって抽出された判定対象データの属性値である。また、「ｙ」は、抽出部１３２によって抽出された属性名に対応する属性値集合「Correct（attribute）」である。そして、算出部１３４は、かかる関数「Ｆ（ｘ、ｙ）」を用いて、「ｘ」と「ｙ」とのレーベンシュタイン距離を算出する。このとき、「ｙ」は、属性値集合「Correct（attribute）」であるので、複数の属性値が存在する場合がある。複数の属性値が存在する場合、算出部１３４は、属性値集合「Correct（attribute）」に含まれる各属性値と「ｘ」とのレーベンシュタイン距離のうち、最小のレーベンシュタイン距離を上記指標値として算出する。

【００５７】

そして、算出部１３４は、抽出部１３２によってＨＴＴＰリクエストから抽出された全ての属性名及び属性値の組合せについて、上述した線形識別器を用いた算出処理、又は、類似度（例えば、レーベンシュタイン距離）を用いた算出処理を行う。

【００５８】

判定部１３５は、算出部１３４によって算出された指標値（「分類尤度」や「類似度」）に基づいて、サーバ装置４０に送信されたＨＴＴＰリクエストが攻撃であるか否かを判定する。

【００５９】

具体的には、判定部１３５は、算出部１３４によって算出された各素性の分類尤度が所定の閾値（以下、「尤度閾値Ｔ２」とする）よりも低い場合には、かかる素性が異常であ

ると判定し、素性の分類尤度が尤度閾値Ｔ２以上である場合には、かかる素性が正常であると判定する。

【００６０】

また、判定部１３５は、算出部１３４によって算出された属性値の類似度が所定の閾値（以下、「類似度閾値Ｔ３」とする）よりも低い場合には、かかる属性値が異常であると判定し、属性値の類似度が類似度閾値Ｔ３以上である場合には、かかる属性値が正常であると判定する。なお、判定部１３５は、算出部１３４によってレーベンシュタイン距離が類似度として算出された場合には、かかるレーベンシュタイン距離が類似度閾値Ｔ３よりも大きい場合には、異常であると判定し、レーベンシュタイン距離が類似度閾値Ｔ３以下である場合には、正常であると判定する。

【００６１】

そして、判定部１３５は、抽出部１３２によってＨＴＴＰリクエストから抽出された全ての属性名及び属性値の組合せについて、分類尤度を用いた判定処理、及び、類似度（例えば、レーベンシュタイン距離）を用いた判定処理を行う。そして、判定部１３５は、異常であると判定した素性の数と属性値の数との総和が所定の閾値（以下、「異常数閾値Ｔ４」とする）よりも多い場合に、プローブ５０から入力されたＨＴＴＰリクエストがサーバ装置４０に対する攻撃であると判定する。一方、判定部１３５は、異常であると判定した素性及び属性値の数が異常数閾値Ｔ４以下である場合に、プローブ５０から入力されたＨＴＴＰリクエストがサーバ装置４０に対する攻撃でないと判定する。

【００６２】

なお、判定部１３５は、ＨＴＴＰリクエストが攻撃であると判定した場合には、図示しない記憶部にログとして記憶してもよいし、ＩＦ部１１０を介して、管理者等が利用する管理者端末に警告を通知してもよい。

【００６３】

また、上記例では、算出部１３４が、属性値を分解した各素性を判定対象データとして線形識別器に入力し、素性毎の分類尤度を線形識別器から得る例について示した。このとき、算出部１３４は、線形識別器から得られた各素性の分類尤度と尤度閾値Ｔ２とを比較することにより、分解前の属性値が正常又は異常であるかを判定してもよい。例えば、算出部１３４は、分解した各素性のうち、尤度閾値Ｔ２よりも低い素性の数が所定数よりも多い場合には、分解前の属性値が異常であると判定し、尤度閾値Ｔ２よりも低い素性の数が所定数以下である場合には、分解前の属性値が正常であると判定する。そして、判定部１３５は、抽出部１３２によってＨＴＴＰリクエストから抽出された全ての属性名及び属性値の組合せについて、分類尤度を用いた判定処理、及び、類似度（例えば、レーベンシュタイン距離）を用いた判定処理を行い、異常であると判定した属性値の数が異常数閾値Ｔ４よりも多い場合に、プローブ５０から入力されたＨＴＴＰリクエストがサーバ装置４０に対する攻撃であると判定する。一方、判定部１３５は、異常であると判定した属性値の数が異常数閾値Ｔ４以下である場合に、プローブ５０から入力されたＨＴＴＰリクエストがサーバ装置４０に対する攻撃でないと判定する。このように、算出部１３４は、属性値毎に、かかる属性値が正常又は異常であるかを判定してもよい。

【００６４】

また、線形識別器によっては、複数の素性が入力された場合に、かかる複数の素性によって形成される分解前の属性値の分類尤度を出力するものもある。かかる場合には、算出部１３４は、分解後の複数の素性を線形識別器に入力し、かかる線形識別器から出力される分解前の分類尤度と尤度閾値Ｔ２とを比較することにより、分解前の属性値が正常又は異常であるかを判定してもよい。

【００６５】

［攻撃判定装置による学習処理］

次に、図５を用いて、上述した攻撃判定装置１００による学習処理の手順について説明する。図５は、第１の実施形態に係る攻撃判定装置１００による学習処理手順を示すフローチャートである。なお、攻撃判定装置１００は、学習処理を行う場合には、学習部１３

３による処理を行うが、算出部１３４及び判定部１３５による処理を停止する。
【００６６】
図５に示すように、攻撃判定装置１００は、学習用の通信環境においてユーザ端末１１からサーバ装置４０に対して正常なアクセスが行われた場合に（ステップＳ１０１肯定）、ユーザ端末１１により送信された通信パケットをプローブ５０から受信する（ステップＳ１０２）。
【００６７】
続いて、再構築部１３１は、プローブ５０から受信した通信パケットから、ＨＴＴＰリクエストを再構築する（ステップＳ１０３）。そして、抽出部１３２は、再構築部１３１によって再構築されたＨＴＴＰリクエストのクエリに設定されている属性値及び属性名の組合せを抽出する（ステップＳ１０４）。なお、抽出部１３２は、属性値及び属性名の組合せを複数抽出する場合がある。
【００６８】
続いて、学習部１３３は、抽出部１３２によって抽出された属性値及び属性名の組合せ毎に、下記のステップＳ１０５～Ｓ１０９における処理を行う。具体的には、学習部１３３は、抽出部１３２によって抽出された属性値のサイズがサイズ閾値Ｔ１よりも大きいか否かを判定する（ステップＳ１０５）。
【００６９】
そして、学習部１３３は、属性値のサイズがサイズ閾値Ｔ１よりも大きい場合には（ステップＳ１０５肯定）、かかる属性値をデコードする（ステップＳ１０６）。続いて、学習部１３３は、デコード後の属性値を形態素解析することにより素性に分解する（ステップＳ１０７）。そして、学習部１３３は、抽出部１３２によって抽出された属性名に対応する線形識別器に対して、分解後の素性を訓練例データとして入力することにより、各素性を正常情報として学習する（ステップＳ１０８）。
【００７０】
一方、学習部１３３は、属性値のサイズがサイズ閾値Ｔ１以下である場合には（ステップＳ１０５否定）、抽出部１３２によって抽出された属性名に対応付けて、かかる属性値を学習結果記憶部１２０に格納する（ステップＳ１０９）。
【００７１】
そして、学習部１３３は、抽出部１３２によって抽出された全ての属性値及び属性名の組合せについて処理を行ったか否かを判定する（ステップＳ１１０）。このとき、学習部１３３は、全ての属性値及び属性名の組合せについて処理を行っていない場合には（ステップＳ１１０否定）、未処理の属性値及び属性名の組合せについて、上記ステップＳ１０５～Ｓ１０９における処理を行う。一方、学習部１３３は、全ての属性値及び属性名の組合せについて処理済みである場合には（ステップＳ１１０肯定）、学習処理を終了する。
【００７２】
［攻撃判定装置による攻撃判定処理］
次に、図６を用いて、上述した攻撃判定装置１００による攻撃判定処理の手順について説明する。図６は、第１の実施形態に係る攻撃判定装置１００による攻撃判定処理手順を示すフローチャートである。なお、攻撃判定装置１００は、攻撃判定処理を行う場合には、算出部１３４及び判定部１３５による処理を行うが、学習部１３３による処理を停止する。
【００７３】
図６に示すように、攻撃判定装置１００は、通常運用の通信環境においてユーザ端末１２等からサーバ装置４０に対してアクセスが行われた場合に（ステップＳ２０１肯定）、プローブ５０から通信パケットを受信する（ステップＳ２０２）。続いて、再構築部１３１は、通信パケットからＨＴＴＰリクエストを再構築する（ステップＳ２０３）。そして、抽出部１３２は、ＨＴＴＰリクエストから属性値及び属性名の組合せを抽出する（ステップＳ２０４）。
【００７４】

続いて、算出部１３４及び判定部１３５は、抽出部１３２によって抽出された属性値及び属性名の組合せ毎に、下記のステップＳ２０５～Ｓ２１１における処理を行う。具体的には、算出部１３４は、抽出部１３２によって抽出された属性値のサイズがサイズ閾値Ｔ１よりも大きいか否かを判定する（ステップＳ２０５）。

【００７５】

そして、算出部１３４は、属性値のサイズがサイズ閾値Ｔ１よりも大きい場合には（ステップＳ２０５肯定）、かかる属性値をデコードする（ステップＳ２０６）。続いて、算出部１３４は、デコード後の属性値を形態素解析することにより素性に分解する（ステップＳ２０７）。

【００７６】

続いて、算出部１３４は、抽出部１３２によって抽出された属性名に対応する線形識別器に対して、分解後の素性のそれぞれを判定対象データとして入力することにより、素性の分類尤度を算出する（ステップＳ２０８）。

【００７７】

続いて、判定部１３５は、算出部１３４によって算出された分類尤度に基づいて、素性が異常であるか否かを判定し、異常であると判定した素性の数を計数する（ステップＳ２０９）。例えば、判定部１３５は、分類尤度が尤度閾値Ｔ２よりも低い場合に、異常である素性の数を「１」だけ加算する。判定部１３５は、ステップＳ２０７において得られた各素性について異常であるか否かを判定し、異常である素性の数を計数する。

【００７８】

一方、算出部１３４は、属性値のサイズがサイズ閾値Ｔ１以下である場合には（ステップＳ２０５否定）、上述した関数Ｆ（ｘ、ｙ）を用いるなどして、抽出部１３２によって抽出された属性名に対応付けて学習結果記憶部１２０に記憶されている属性値集合（「Correct（attribute）」）と、かかる属性値との類似度（例えば、レーベンシュタイン距離）を算出する（ステップＳ２１０）。

【００７９】

続いて、判定部１３５は、算出部１３４によって算出された類似度に基づいて、異常である属性値の数を計数する（ステップＳ２１１）。例えば、判定部１３５は、レーベンシュタイン距離が類似度閾値Ｔ３よりも大きい場合に、異常である属性値の数を「１」だけ加算する。

【００８０】

そして、算出部１３４及び判定部１３５は、抽出部１３２によって抽出された全ての属性値及び属性名の組合せについて処理を行ったか否かを判定する（ステップＳ２１２）。このとき、全ての属性値及び属性名の組合せについて処理を行っていない場合には（ステップＳ２１２否定）、算出部１３４及び判定部１３５は、未処理の属性値及び属性名の組合せについて、上記ステップＳ２０５～Ｓ２１１における処理を行う。

【００８１】

一方、全ての属性値及び属性名の組合せについて処理済みである場合には（ステップＳ２１２肯定）、判定部１３５は、ステップＳ２０９及びＳ２１１において計数した数が異常数閾値Ｔ４よりも多いか否かを判定する（ステップＳ２１３）。

【００８２】

そして、判定部１３５は、計数した数が異常数閾値Ｔ４よりも多い場合には（ステップＳ２１３肯定）、ステップＳ２０１において行われたアクセスがサーバ装置４０に対する攻撃であると判定する（ステップＳ２１４）。一方、判定部１３５は、計数した数が異常数閾値Ｔ４以下である場合には（ステップＳ２１３否定）、ステップＳ２０１において行われたアクセスがサーバ装置４０に対する攻撃でなく、正常なアクセスであると判定する（ステップＳ２１５）。

【００８３】

［第１の実施形態の効果］

上述してきたように、第１の実施形態に係る攻撃判定装置１００において、学習部１３

３は、正常であることが既知であるＨＴＴＰリクエスト（正常アクセス要求の一例に相当）がサーバ装置４０（情報処理装置の一例に相当）に送信された場合に、かかる正常なＨＴＴＰリクエストに設定されている属性値（設定情報の一例に相当）を正常情報として学習する。また、学習結果記憶部１２０は、学習部１３３によって学習された正常情報の集合を記憶する。また、算出部１３４は、正常であることが既知でないＨＴＴＰリクエスト（未知アクセス要求の一例に相当）がサーバ装置４０に送信された場合に、かかる未知のＨＴＴＰリクエストに設定されている設定情報が正常情報の集合に分類される度合いを示す指標値を算出する。また、判定部１３５は、算出部１３４によって算出された指標値に基づいて、前述した未知のＨＴＴＰリクエストがサーバ装置４０に対する攻撃であるか否かを判定する。

【００８４】

これにより、第１の実施形態に係る攻撃判定装置１００は、予めパターン化された攻撃のシグネチャファイルやブラックリストを要することなく、サーバ装置４０に対する未知の攻撃を検知することができる。すなわち、攻撃判定装置１００は、専門家等によるパターン化データの作成に要するコストを低減することができるとともに、未知の攻撃を検知することができる。

【００８５】

また、第１の実施形態に係る攻撃判定装置１００において、学習部１３３は、正常なＨＴＴＰリクエストに設定されている属性値の属性名毎に、かかる属性値を正常情報として学習する。また、学習結果記憶部１２０は、学習部１３３によって学習された正常情報の集合を属性名毎に記憶する。また、算出部１３４は、未知のＨＴＴＰリクエストに設定されている属性値が、かかる属性値の属性名に対応する正常情報の集合に分類されるか否かを示す指標値を算出する。

【００８６】

これにより、第１の実施形態に係る攻撃判定装置１００は、ＨＴＴＰリクエストに設定される属性名毎に、属性値が異常であるか否かを判定することが可能となるので、サーバ装置４０に対する未知の攻撃を高精度に検知することができる。

【００８７】

また、第１の実施形態に係る攻撃判定装置１００において、学習部１３３は、正常なＨＴＴＰリクエストに設定されている属性値のサイズがサイズ閾値Ｔ１よりも大きい場合に、かかる属性値を分解した素性（部分設定情報の一例に相当）を正常情報として学習する。また、算出部１３４は、未知のＨＴＴＰリクエストに設定されている属性値のサイズがサイズ閾値Ｔ１よりも大きい場合に、かかる属性値を分解した素性が正常情報の集合に分類されるか否かを示す指標値を算出する。

【００８８】

これにより、第１の実施形態に係る攻撃判定装置１００は、ＨＴＴＰリクエストに設定される属性値を細分化した上で指標値を算出するので、属性値が異常であるか否かを高精度に判定することができ、この結果、サーバ装置４０に対する未知の攻撃を高精度に検知することができる。

【００８９】

また、第１の実施形態に係る攻撃判定装置１００において、学習部１３３は、未知のＨＴＴＰリクエストに設定されている属性値を分解した素性を、かかる属性値の属性名に対応する線形識別器に訓練例データとして入力することにより、素性を正常情報として学習する。また、算出部１３４は、未知のＨＴＴＰリクエストに設定されている属性値のサイズがサイズ閾値Ｔ１以下である場合に、かかる属性値と正常情報の集合との類似度を前述の指標値として算出する。また、算出部１３４は、未知のアクセス要求に設定されている属性値のサイズがサイズ閾値Ｔ１よりも大きい場合に、かかる属性値を分解した各素性を、かかる属性値の属性名に対応する線形識別器に判定対象データとして入力することにより、各素性が正常情報の集合に分類される尤度である分類尤度を前述の指標値として算出する。また、判定部１３５は、類似度が類似度閾値Ｔ３よりも低い属性値の数、又は、分

類尤度が尤度閾値Ｔ２よりも低い素性の数が異常数閾値Ｔ４よりも多い場合に、未知のアクセス要求が攻撃であると判定する。

【００９０】

これにより、第１の実施形態に係る攻撃判定装置１００は、異常である可能性が高い属性値が設定されているＨＴＴＰリクエストを攻撃であると判定することができる。

【００９１】

（第２の実施形態）

上述した攻撃判定装置１００は、上記実施形態以外にも種々の異なる形態にて実施されてよい。そこで、第２の実施形態では、上記の攻撃判定装置１００の他の実施形態について説明する。

【００９２】

［判定処理］

上記実施形態では、判定部１３５が、異常であると判定した素性の数と属性値の数との総和が異常数閾値Ｔ４よりも多い場合に、攻撃であると判定する例を示した。しかし、判定部１３５による判定処理はこの例に限られない。

【００９３】

例えば、判定部１３５は、分類尤度を用いて異常であると判定した素性が１個でも存在すれば、プローブ５０から入力されたＨＴＴＰリクエストが攻撃であると判定してもよい。また、例えば、判定部１３５は、類似度を用いて異常であると判定した属性値が１個でも存在すれば、ＨＴＴＰリクエストが攻撃であると判定してもよい。また、例えば、判定部１３５は、全ての素性及び全ての属性値が異常でない場合に、ＨＴＴＰリクエストが攻撃でないと判定してもよい。

【００９４】

また、例えば、判定部１３５は、算出部１３４によって算出された各分類尤度の平均と、各類似度の平均とを算出し、分類尤度の平均が尤度閾値Ｔ２よりも低く、かつ、類似度の平均が類似度閾値Ｔ３よりも低い場合に、ＨＴＴＰリクエストが攻撃であると判定してもよい。また、例えば、判定部１３５は、分類尤度の平均が尤度閾値Ｔ２よりも低いか、又は、類似度の平均が類似度閾値Ｔ３よりも低い場合に、ＨＴＴＰリクエストが攻撃であると判定してもよい。

【００９５】

［アクセス要求］

また、上記実施形態では、アクセス要求として、ＨＴＴＰリクエストを例に挙げて説明したが、攻撃判定装置１００によって攻撃判定処理が行われるアクセス要求は、ＨＴＴＰリクエストに限られない。具体的には、攻撃判定装置１００は、サーバ装置４０にアクセスする利用者によって任意の設定情報（パラメータ）が設定され得る各種アクセス要求に対して攻撃判定処理を行うことができる。

【００９６】

［システム構成］

また、上記実施形態において説明した各処理のうち、自動的に行われるものとして説明した処理の全部または一部を手動的に行うこともでき、あるいは、手動的に行われるものとして説明した処理の全部または一部を公知の方法で自動的に行うこともできる。この他、上記文書中や図面中で示した処理手順、具体的名称、各種のデータやパラメータを含む情報については、特記する場合を除いて任意に変更することができる。

【００９７】

例えば、攻撃判定装置１００は、学習用の通信環境であることが指定された場合に、算出部１３４及び判定部１３５を停止させてもよいが、手動によって算出部１３４及び判定部１３５が停止されてもよい。同様に、攻撃判定装置１００は、通常運用の通信環境であることが指定された場合に、学習部１３３を停止させてもよいが、手動によって学習部１３３が停止されてもよい。

【００９８】

また、図示した各装置の各構成要素は機能概念的なものであり、必ずしも物理的に図示の如く構成されていることを要しない。すなわち、各装置の分散・統合の具体的形態は図示のものに限られず、その全部または一部を、各種の負荷や使用状況などに応じて、任意の単位で機能的または物理的に分散・統合して構成することができる。

【００９９】

例えば、図３に示した算出部１３４と判定部１３５とは統合されてもよい。また、学習結果記憶部１２０は、「Correct（attribute）」を記憶する第１記憶部と、「lern（attribute、［素性（集合）］）」を記憶する第２記憶部とに分離されてもよい。

【０１００】

また、再構築部１３１及び抽出部１３２は、攻撃判定装置１００に具備されなくてもよい。例えば、プローブ５０が再構築部１３１及び抽出部１３２を具備してもよい。また、上記第１の実施形態では、学習部１３３及び算出部１３４の双方が、属性値をデコードし、デコード後の属性値を形態素解析する処理を行う例を示した。しかし、攻撃判定装置１００は、属性値をデコードするデコード部と、属性値を形態素解析する解析部とを、学習部１３３及び算出部１３４とは別に具備してもよい。かかる場合には、学習部１３３及び算出部１３４は、デコード部にデコード処理を行わせ、解析部に形態素解析処理を行わせる。

【０１０１】

［プログラム］

また、上記実施形態において説明した攻撃判定装置１００が実行する処理をコンピュータが実行可能な言語で記述したプログラムを作成することもできる。例えば、攻撃判定装置１００が実行する処理をコンピュータが実行可能な言語で記述した攻撃判定プログラムを作成することもできる。この場合、コンピュータが攻撃判定プログラムを実行することにより、上記実施形態と同様の効果を得ることができる。さらに、かかる攻撃判定プログラムをコンピュータ読み取り可能な記録媒体に記録して、この記録媒体に記録された攻撃判定プログラムをコンピュータに読み込ませて実行することにより上記実施形態と同様の処理を実現してもよい。以下に、一例として、図３に示した攻撃判定装置１００と同様の機能を実現する攻撃判定プログラムを実行するコンピュータの一例を説明する。

【０１０２】

図７は、攻撃判定プログラムを実行するコンピュータ１０００を示す図である。図７に例示するように、コンピュータ１０００は、例えば、メモリ１０１０と、ＣＰＵ１０２０と、ハードディスクドライブインタフェース１０３０と、ディスクドライブインタフェース１０４０と、シリアルポートインタフェース１０５０と、ビデオアダプタ１０６０と、ネットワークインタフェース１０７０とを有し、これらの各部はバス１０８０によって接続される。

【０１０３】

メモリ１０１０は、図７に例示するように、ＲＯＭ（Read Only Memory）１０１１及びＲＡＭ１０１２を含む。ＲＯＭ１０１１は、例えば、ＢＩＯＳ（Basic Input Output System）等のブートプログラムを記憶する。ハードディスクドライブインタフェース１０３０は、図７に例示するように、ハードディスクドライブ１０３１に接続される。ディスクドライブインタフェース１０４０は、図７に例示するように、ディスクドライブ１０４１に接続される。例えば磁気ディスクや光ディスク等の着脱可能な記憶媒体が、ディスクドライブに挿入される。シリアルポートインタフェース１０５０は、図７に例示するように、例えばマウス１０５１、キーボード１０５２に接続される。ビデオアダプタ１０６０は、図７に例示するように、例えばディスプレイ１０６１に接続される。

【０１０４】

ここで、図７に例示するように、ハードディスクドライブ１０３１は、例えば、ＯＳ１０９１、アプリケーションプログラム１０９２、プログラムモジュール１０９３、プログラムデータ１０９４を記憶する。すなわち、上記の攻撃判定プログラムは、コンピュータ１０００によって実行される指令が記述されたプログラムモジュールとして、例えばハー

ドディスクドライブ１０３１に記憶される。例えば、図３に例示した再構築部１３１と同様の情報処理を実行する再構築手順と、抽出部１３２と同様の情報処理を実行する抽出手順と、学習部１３３と同様の情報処理を実行する学習手順と、算出部１３４と同様の情報処理を実行する算出手順と、判定部１３５と同様の情報処理を実行する判定手順とが記述されたプログラムモジュール１０９３が、ハードディスクドライブ１０３１に記憶される。

【０１０５】

また、上記実施形態で説明した学習結果記憶部１２０が保持する各種データは、プログラムデータとして、例えばメモリ１０１０やハードディスクドライブ１０３１に記憶される。そして、ＣＰＵ１０２０が、メモリ１０１０やハードディスクドライブ１０３１に記憶されたプログラムモジュール１０９３やプログラムデータ１０９４を必要に応じてＲＡＭ１０１２に読み出し、再構築手順、抽出手順、学習手順、算出手順、判定手順を実行する。

【０１０６】

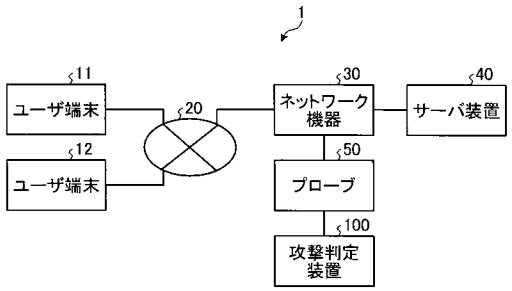
なお、攻撃判定プログラムに係るプログラムモジュール１０９３やプログラムデータ１０９４は、ハードディスクドライブ１０３１に記憶される場合に限られず、例えば着脱可能な記憶媒体に記憶され、ディスクドライブ等を介してＣＰＵ１０２０によって読み出されてもよい。あるいは、攻撃判定プログラムに係るプログラムモジュール１０９３やプログラムデータ１０９４は、ネットワーク（ＬＡＮ（Local Area Network）、ＷＡＮ（Wide Area Network）等）を介して接続された他のコンピュータに記憶され、ネットワークインタフェース１０７０を介してＣＰＵ１０２０によって読み出されてもよい。

【符号の説明】

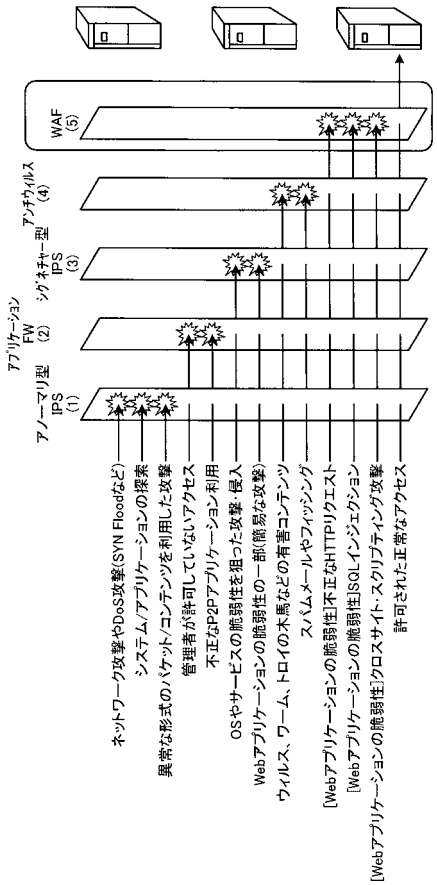
【０１０７】

１　ネットワークシステム
４０　サーバ装置
１００　攻撃判定装置
１２０　学習結果記憶部
１３１　再構築部
１３２　抽出部
１３３　学習部
１３４　算出部
１３５　判定部

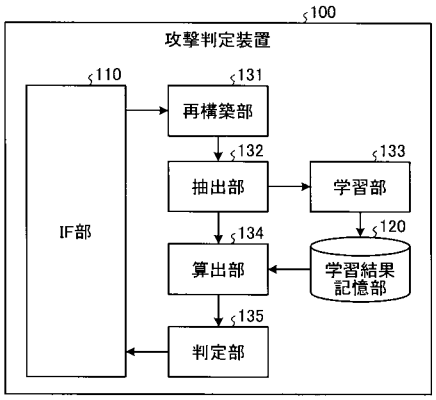
【図１】


1
11
ユーザ端末
12
ユーザ端末
20
30
ネットワーク機器
40
サーバ装置
50
プローブ
100
攻撃判定装置

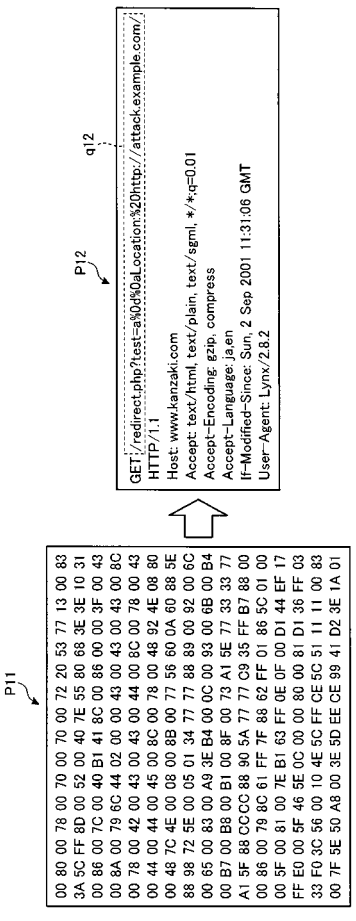
【図２】


WAF (5)
アンチウイルス (4)
シグネチャー型 IPS (3)
アプリケーション FW (2)
アノーマリ型 IPS (1)
ネットワーク攻撃やDoS攻撃(SYN Floodなど)
システム/アプリケーションの探索
異常な形式のパケット/コンテンツを利用した攻撃
管理者が許可していないアクセス
不正なP2Pアプリケーション利用
OSやサービスの脆弱性を狙った攻撃・侵入
Webアプリケーションの脆弱性の一部(簡易な攻撃)
ウィルス、ワーム、トロイの木馬などの有害コンテンツ
スパムメールやフィッシング
[Webアプリケーションの脆弱性]不正なHTTPリクエスト
[Webアプリケーションの脆弱性]SQLインジェクション
[Webアプリケーションの脆弱性]クロスサイト・スクリプティング攻撃
許可された正常なアクセス

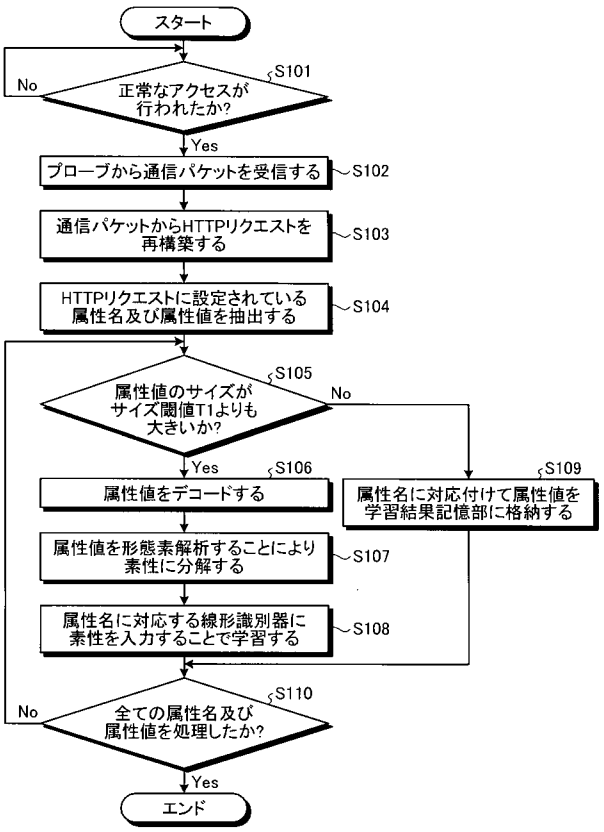
【図３】


100
攻撃判定装置
110
IF部
131
再構築部
132
抽出部
133
学習部
120
学習結果記憶部
134
算出部
135
判定部

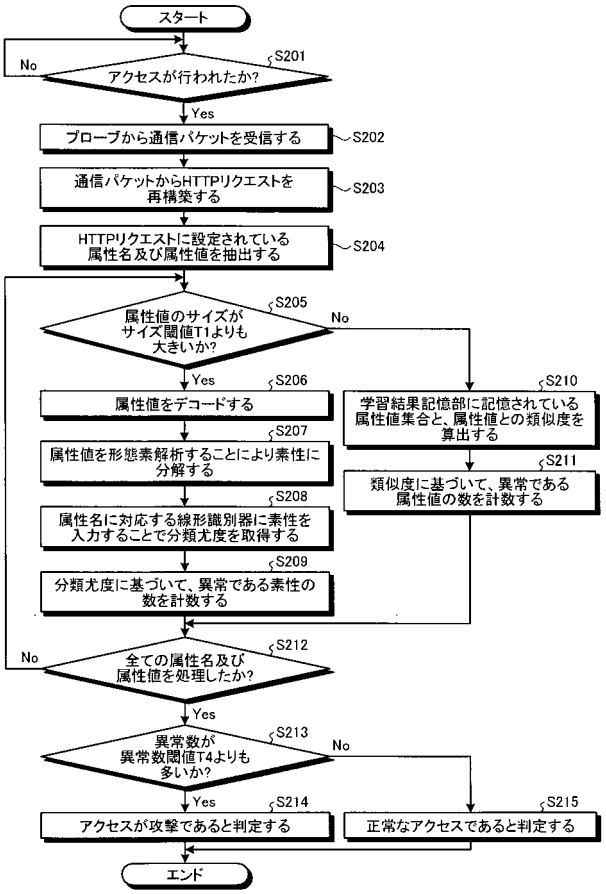
【図４】


P12
q12
GET /redirect.php?test=a%0d%0aLocation:%20http://attack.example.com/
HTTP/1.1
Host: www.kanzaki.com
Accept: text/html, text/plain, text/sgml, */*;q=0.01
Accept-Encoding: gzip, compress
Accept-Language: ja,en
If-Modified-Since: Sun, 2 Sep 2001 11:31:06 GMT
User-Agent: Lynx/2.8.2
P11
00 80 00 78 00 70 00 72 20 53 77 13 00 83
3A 5C FF 8D 00 52 00 40 7E 55 80 68 3E 3E 10 31
00 86 00 7C 00 40 B1 41 8C 00 86 00 00 3F 00 43
00 8A 00 79 6C 44 02 00 00 43 00 43 00 8C 00 8C
00 78 00 42 00 43 00 44 00 8C 00 78 00 43 00 43
00 44 00 44 00 45 00 8C 00 78 00 48 92 4E 08 80
00 48 7C 4E 00 08 00 8B 00 77 56 60 0A 60 88 5E
88 98 72 5E 00 05 01 34 77 77 88 89 00 92 00 6C
00 65 00 83 00 A9 3E B4 00 0C 00 93 00 6B 00 B4
00 B7 00 B8 00 B1 00 8F 00 73 A1 5E 77 33 33 77
A1 5F 88 CC CC 88 90 5A 77 77 C9 35 FF B7 88 00
00 86 00 79 8C 61 FF 7F 88 62 FF 01 86 5C 01 00
00 5F 00 81 00 7E B1 63 FF 0E 0F 00 D1 44 EF 17
FF E0 00 5F 46 5E 0C 00 00 80 00 81 D1 36 FF 03
33 F0 3C 56 00 10 4E 5C FF CE 5C 51 11 11 00 83
00 7F 5E 50 A8 00 3E 5D EE CE 99 41 D2 3E 1A 01

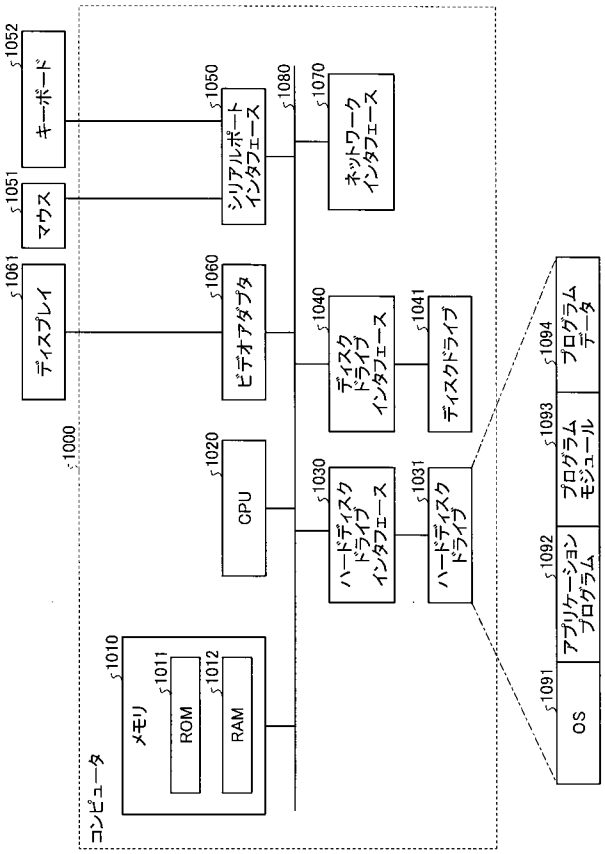
【図５】


スタート
S101
正常なアクセスが行われたか?
No
Yes
プローブから通信パケットを受信する
S102
通信パケットからHTTPリクエストを再構築する
S103
HTTPリクエストに設定されている属性名及び属性値を抽出する
S104
S105
属性値のサイズがサイズ閾値T1よりも大きいか?
No
Yes
S106
属性値をデコードする
S107
属性値を形態素解析することにより素性に分解する
S108
属性名に対応する線形識別器に素性を入力することで学習する
S109
属性名に対応付けて属性値を学習結果記憶部に格納する
S110
全ての属性名及び属性値を処理したか?
No
Yes
エンド

【図６】


スタート
S201
アクセスが行われたか?
No
Yes
プローブから通信パケットを受信する
S202
通信パケットからHTTPリクエストを再構築する
S203
HTTPリクエストに設定されている属性名及び属性値を抽出する
S204
S205
属性値のサイズがサイズ閾値T1よりも大きいか?
No
Yes
S206
属性値をデコードする
S207
属性値を形態素解析することにより素性に分解する
S208
属性名に対応する線形識別器に素性を入力することで分類尤度を取得する
S209
分類尤度に基づいて、異常である素性の数を計数する
S210
学習結果記憶部に記憶されている属性値集合と、属性値との類似度を算出する
S211
類似度に基づいて、異常である属性値の数を計数する
S212
全ての属性名及び属性値を処理したか?
No
Yes
S213
異常数が異常数閾値T4よりも多いか?
No
Yes
S214
アクセスが攻撃であると判定する
S215
正常なアクセスであると判定する
エンド

【図７】


1000
コンピュータ
1010
メモリ
1011
ROM
1012
RAM
1020
CPU
1030
ハードディスクドライブインタフェース
1031
ハードディスクドライブ
1040
ディスクドライブインタフェース
1041
ディスクドライブ
1050
シリアルポートインタフェース
1051
マウス
1052
キーボード
1060
ビデオアダプタ
1061
ディスプレイ
1070
ネットワークインタフェース
1080
1091
OS
1092
アプリケーションプログラム
1093
プログラムモジュール
1094
プログラムデータ