(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2017-199250
(P2017-199250A)
(43)公開日　平成29年11月2日(2017.11.2)

| (51)Int.Cl. | F I | テーマコード（参考） |
|---|---|---|
| G06F 21/55 (2013.01) | G06F 21/55 | |

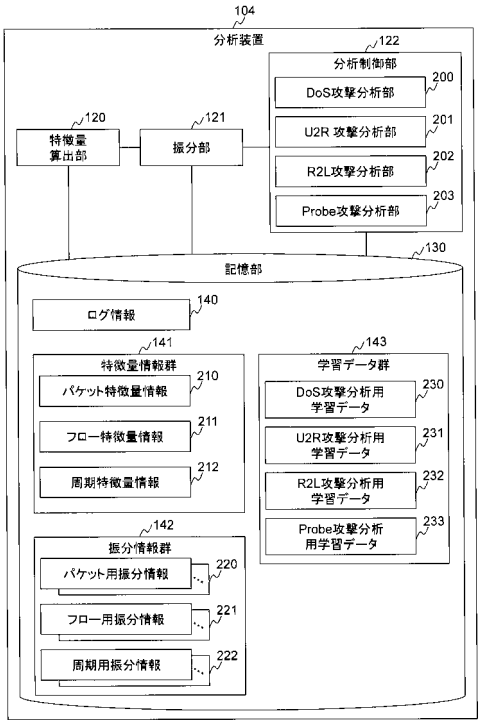
審査請求 未請求　請求項の数 15　ＯＬ　（全 18 頁）

(21)出願番号　特願2016-90661(P2016-90661)
(22)出願日　平成28年4月28日(2016.4.28)

(71)出願人　000005108
株式会社日立製作所
東京都千代田区丸の内一丁目６番６号
(74)代理人　110001678
特許業務法人藤央特許事務所
(72)発明者　増田　千絵
東京都千代田区丸の内一丁目６番６号　株式会社日立製作所内
(72)発明者　松原　大典
東京都千代田区丸の内一丁目６番６号　株式会社日立製作所内

(54)【発明の名称】計算機システム、データの分析方法、及び計算機

(57)【要約】
【課題】複数の分析器を備えるシステムにおいて、使用する計算機リソース量の削減及び分析精度の向上を目的とする。
【解決手段】複数の計算機を備える計算機システムであって、複数の計算機は、分析処理を実行する分析部を複数含む分析制御部を有する計算機と、分析部が使用する特徴量を算出する特徴量算出部、及び使用する分析部を選択する振分部を有する計算機と、を含み、振分部は、特徴量、分析処理の種別、及び分析処理の結果を含むエントリを複数含む振分情報を管理し、振分情報を参照して、データから算出された特徴量に類似する特徴量を含むエントリを検索し、検索されたエントリに含まれる分析処理の結果に基づいて、実行する分析処理を選択し、分析処理の結果を受信した場合、データから算出された特徴量、分析処理の種別、及び分析処理の結果を含むエントリを振分情報に追加する。
【選択図】図２



【特許請求の範囲】
【請求項１】
複数の計算機を備える計算機システムであって、
前記複数の計算機の各々は、プロセッサ、前記プロセッサに接続されるメモリ、前記プロセッサに接続され、他の装置と接続するためのインタフェースを有し、
前記複数の計算機は、
ネットワークを介して送受信されるデータを用いた分析処理を実行する分析部を複数含む分析制御部を有する計算機と、
前記データを用いて前記複数の分析部の各々が使用する特徴量を算出する特徴量算出部、及び使用する前記分析部を選択する振分部を有する計算機と、を含み、
前記振分部は、前記複数の分析部の各々が使用する前記特徴量、前記分析処理の種別、及び分析処理の結果を含むエントリを複数含む振分情報を管理し、
前記分析処理の結果は、前記分析処理が必要であるか否かを示す値であり、
前記振分部は、
前記振分情報を参照して、前記データから算出された特徴量に類似する特徴量を含む類似エントリを検索し、
前記類似エントリに含まれる前記分析処理の結果に基づいて、実行する前記分析処理を選択し、
前記振分部によって選択された分析処理を実行する前記分析部は、前記データから算出された特徴量を用いた分析処理を実行し、前記分析処理の結果を前記振分部に送信し、
前記振分部は、前記分析処理の結果を受信した場合、前記データから算出された特徴量、前記分析処理の種別、及び前記分析処理の結果を含むエントリを前記振分情報に追加することを特徴とする計算機システム。
【請求項２】
請求項１に記載の計算機システムであって、
前記特徴量算出部は、前記複数の分析部の各々が使用する種別が異なる複数の特徴量を算出し、
前記振分情報に含まれるエントリは、前記複数の特徴量を含み、
前記振分部は、
一つ種別の特徴量を一つの成分とする特徴量空間における、前記複数のエントリに含まれる前記複数の特徴量と、前記データから算出された前記複数の特徴量との間の距離を算出し、
前記距離が所定の閾値以下となるエントリの中から、前記距離が最も小さいエントリを、前記類似エントリとして特定することを特徴とする計算機システム。
【請求項３】
請求項２に記載の計算機システムであって、
前記振分部は、前記距離が前記所定の閾値以下となるエントリが存在しない場合、全ての前記分析処理を選択することを特徴とする計算機システム。
【請求項４】
請求項２に記載の計算機システムであって、
前記振分部は、
前記分析処理の結果が前記分析処理が不要であることを示す値を含むエントリの中から、前記距離が最小となる第１エントリを特定し、
前記分析処理の結果が前記分析処理が必要であることを示す値を含むエントリの中から、前記距離が最小となる第２エントリを特定し、
前記第１エントリに含まれる複数の特徴量と前記データから算出された複数の特徴量との間の第１距離が第１閾値以下、かつ、前記第２エントリに含まれる複数の特徴量と前記データから算出された複数の特徴量との間の第２距離が第２閾値より大きい場合、前記第１エントリを、前記類似エントリとして特定し、
前記第１距離が前記第１閾値より大きく、かつ、前記第２距離が前記第２閾値以下の場

合、前記第２エントリを、前記類似エントリとして特定し、
　前記第１距離が前記第１閾値以下、かつ、前記第２距離が前記第２閾値以下の場合、前記第２エントリを、前記類似エントリとして特定することを特徴とする計算機システム。
【請求項５】
　請求項４に記載の計算機システムであって、
　前記第１閾値は、前記第２閾値より小さいことを特徴とする計算機システム。
【請求項６】
　複数の計算機を備える計算機システムにおけるデータの分析方法であって、
　前記複数の計算機の各々は、プロセッサ、前記プロセッサに接続されるメモリ、前記プロセッサに接続され、他の装置と接続するためのインタフェースを有し、
　前記複数の計算機は、
　ネットワークを介して送受信されるデータを用いた分析処理を実行する分析部を複数含む分析制御部を有する計算機と、
　特徴量を算出する特徴量算出部、及び使用する前記分析部を選択する振分部を有する計算機と、を含み、
　前記振分部は、前記複数の分析部の各々が使用する前記特徴量、前記分析処理の種別、及び分析処理の結果を含むエントリを複数含む振分情報を管理し、
　前記分析処理の結果は、前記分析処理が必要であるか否かを示す値であり、
　前記データの分析処理方法は、
　前記特徴量算出部が、前記データを用いて、前記複数の分析部の各々が使用する特徴量を算出する第１のステップと、
　前記振分部が、前記振分情報を参照して、前記データから算出された特徴量に類似する特徴量を含む類似エントリを検索する第２のステップと、
　前記振分部が、前記類似エントリに含まれる前記分析処理の結果に基づいて、実行する前記分析処理を選択する第３のステップと、
　前記振分部によって選択された分析処理を実行する前記分析部が、前記データから算出された特徴量を用いた分析処理を実行し、前記分析処理の結果を前記振分部に送信する第４のステップと、
　前記振分部が、前記分析処理の結果を受信した場合、前記データから算出された特徴量、前記分析処理の種別、及び前記分析処理の結果を含むエントリを前記振分情報に追加する第５のステップと、を含むことを特徴とするデータの分析方法。
【請求項７】
　請求項６に記載のデータの分析方法であって、
　前記振分情報に含まれるエントリは、種別が異なる複数の特徴量を含み、
　前記第１のステップは、前記特徴量算出部が、前記複数の分析部の各々が使用する前記複数の特徴量を算出するステップを含み、
　前記第２のステップは、
　前記振分部が、一つの種別の特徴量を一つの成分とする特徴量空間における、前記複数のエントリに含まれる前記複数の特徴量と、前記データから算出された前記複数の特徴量との間の距離を算出する第６のステップと、
　前記振分部が、前記距離が所定の閾値以下となるエントリの中から、前記距離が最も小さいエントリを、前記類似エントリとして特定する第７のステップと、を含むことを特徴とするデータの分析方法。
【請求項８】
　請求項７に記載のデータの分析方法であって、
　前記第２のステップは、前記振分部が、前記距離が前記所定の閾値以下となるエントリが存在しない場合、全ての前記分析処理を選択するステップを含むことを特徴とするデータの分析方法。
【請求項９】
　請求項７に記載のデータの分析方法であって、

前記第７のステップは、
前記振分部が、前記分析処理の結果が前記分析処理が不要であることを示す値を含むエントリの中から、前記距離が最小となる第１エントリを特定するステップと、
前記振分部が、前記分析処理の結果が前記分析処理が必要であることを示す値を含むエントリの中から、前記距離が最小となる第２エントリを特定するステップと、
前記第１エントリに含まれる複数の特徴量と前記データから算出された複数の特徴量との間の第１距離が第１閾値以下、かつ、前記第２エントリに含まれる複数の特徴量と前記データから算出された複数の特徴量との間の第２距離が第２閾値より大きい場合、前記振分部が、前記第１エントリを、前記類似エントリとして特定するステップと、
前記第１距離が前記第１閾値より大きく、かつ、前記第２距離が前記第２閾値以下の場合、前記振分部が、前記第２エントリを、前記類似エントリとして特定するステップと、
前記第１距離が前記第１閾値以下、かつ、前記第２距離が前記第２閾値以下の場合、前記振分部が、前記第２エントリを、前記類似エントリとして特定するステップと、を含むことを特徴とするデータの分析方法。
【請求項１０】
請求項９に記載のデータの分析方法であって、
前記第１閾値は、前記第２閾値より小さいことを特徴とするデータの分析方法。
【請求項１１】
プロセッサ、前記プロセッサに接続されるメモリ、前記プロセッサに接続され、他の装置と接続するためのインタフェースを備える計算機であって、
前記計算機は、
ネットワークを介して送受信されるデータを用いた分析処理を実行する分析部を複数含む分析制御部と、
前記データを用いて前記分析部が使用する特徴量を算出する特徴量算出部と、
使用する前記分析部を選択する振分部と、を有し、
前記複数の分析部の各々が使用する前記特徴量、前記分析処理の種別、及び分析処理の結果を含むエントリを複数含む振分情報を保持し、
前記分析処理の結果は、前記分析処理が必要であるか否かを示す値であり、
前記振分部は、
前記振分情報を参照して、前記データから算出された特徴量に類似する特徴量を含む類似エントリを検索し、
前記類似エントリに含まれる前記分析処理の結果に基づいて、実行する前記分析処理を選択し、
前記振分部によって選択された分析処理を実行する前記分析部が、前記データから算出された特徴量を用いた分析処理を実行し、前記分析処理の結果を前記振分部に出力し、
前記振分部は、前記分析処理の結果を受信した場合、前記データから算出された特徴量、前記分析処理の種別、及び前記分析処理の結果を含むエントリを前記振分情報に追加することを特徴とする計算機。
【請求項１２】
請求項１１に記載の計算機であって、
前記特徴量算出部は、前記複数の分析部の各々が使用する種別が異なる複数の特徴量を算出し、
前記振分情報に含まれるエントリは、前記複数の特徴量を含み、
前記振分部は、
一つの種別の特徴量を一つの成分とする特徴量空間における、前記複数のエントリに含まれる前記複数の特徴量と、前記データから算出された前記複数の特徴量との間の距離を算出し、
前記距離が所定の閾値以下となるエントリの中から、前記距離が最も小さいエントリを、前記類似エントリとして特定することを特徴とする計算機。
【請求項１３】

請求項１２に記載の計算機であって、
前記振分部は、前記距離が前記所定の閾値以下となるエントリが存在しない場合、全ての前記分析処理を選択することを特徴とする計算機。
【請求項１４】
請求項１２に記載の計算機であって、
前記振分部は、
前記分析処理の結果が前記分析処理が不要であることを示す値を含むエントリの中から、前記距離が最小となる第１エントリを特定し、
前記分析処理の結果が前記分析処理が必要であることを示す値を含むエントリの中から、前記距離が最小となる第２エントリを特定し、
前記第１エントリに含まれる複数の特徴量と前記データから算出された複数の特徴量との間の第１距離が第１閾値以下、かつ、前記第２エントリに含まれる複数の特徴量と前記データから算出された複数の特徴量との間の第２距離が第２閾値より大きい場合、前記第１エントリを、前記類似エントリとして特定し、
前記第１距離が前記第１閾値より大きく、かつ、前記第２距離が前記第２閾値以下の場合、前記第２エントリを、前記類似エントリとして特定し、
前記第１距離が前記第１閾値以下、かつ、前記第２距離が前記第２閾値以下の場合、前記第２エントリを、前記類似エントリとして特定することを特徴とする計算機。
【請求項１５】
請求項１４に記載の計算機であって、
前記第１閾値は、前記第２閾値より小さいことを特徴とする計算機。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ネットワークを介して送受信されるデータを用いた分析処理を実行する分析器を複数備えるシステムの管理方法に関する。
【背景技術】
【０００２】
近年、ビッグデータといわれる大量の情報を収集し、収集した大量の情報を利用するソリューションが期待されている。このような大量の情報を利用したソリューションの１つとしてネットワーク運用管理がある。
【０００３】
ビッグデータを利用したネットワーク運用管理技術では、ネットワーク装置を流れる情報がパケットレベルで分析される。この技術は、侵入検知システム（ＩＤＳ：Ｉｎｔｒｕｓｉｏｎ　Ｄｅｔｅｃｔｉｏｎ　Ｓｙｓｔｅｍ）等の分野で使われている。
【０００４】
ＩＤＳには、シグネチャ型ＩＤＳ及びアノマリ型ＩＤＳが存在する。シグネチャ型ＩＤＳは、通過する情報が登録されたパターンと一致するか否かを判定することによって、不正アクセスを検知する。一方、アノマリ型ＩＤＳは、通過する情報を分析することによってパターンに登録されていない未知の不正アクセスを検知する。より具体的には、アノマリ型ＩＤＳは、正常なトラフィックを用いた機械学習に基づいて学習モデルを生成し、通過する情報と学習モデルとを比較することによって、正常なトラフィックであるか否かを判定する。
【０００５】
前述したような機械学習に基づく分析は、不正アクセスの検知だけでなく、複数の装置が分散配置されたシステムにおいて各装置の動作品質の保証及び装置管理等、様々な分野での応用が期待されている。
【０００６】
アノマリ型ＩＤＳは、検知率が低く、また、誤検知率が高いといった問題がある。前述の問題の解決方法として、不正アクセスの種類毎に専門の分析器を用いることによって検

知精度（分析精度）を向上させる方法が考えられる。別の解決方法としては、複数の分析器を統合することによって性能の高い一つの分析器を構成するアンサンブル学習法が考えられる（例えば、特許文献１参照）。

【０００７】

特許文献１には、「不正アクセスによって引き起こされる異常を、トラヒック量や通信範囲の異常、通信手順の異常、送受信データの異常の３種類として定義した複数グループに分類し、グループ毎の検出に特化した特徴量を用いた検出モジュールを備えたシステムを構成して不正アクセスの検出を行う。タイムスロット型、フロー・カウント型、フロー・ペイロード型の各グループの検出に特化した特徴量を用いた検出モジュールを備え、各検出モジュールの検出結果の論理和を最終的な出力結果とするシステムを構成し、いずれかの検出モジュールが異常と判断するとシステムがアラートを警告することにより不正アクセスの検出を行う」ことが記載されている。

【０００８】

しかし、特許文献１に記載の方法では、複数の分析器が並列的に動作するため、処理負荷が大きくなり、また、処理時間が長くなるという問題がある。したがって、特許文献１に記載の方法ではシステム性能が低下する。そのため、分析精度を向上させるとともに、分析処理に用いられる計算機リソース量を削減する技術が求められている。

【０００９】

分析処理に用いられる計算機リソース量を削減する方法として、特許文献２に記載された技術が知られている。特許文献２には、「ゲートウェイ装置は、第１ネットワーク上の１ないし複数の機器の動作情報を取得して解析装置に送信する動作情報取得部を備え、解析装置は、動作情報を用いて機器の障害解析を行う障害解析部を備え、動作情報取得部は、取得した動作情報のうち重要度の高いものをあらかじめ定められた重要度にしたがって絞り込んだ上で解析装置３００に送信する」ことが記載されている。

【先行技術文献】

【特許文献】

【００１０】

【特許文献１】特開２００６－１１５１２９号公報

【特許文献２】特開２０１３－３４２４３号公報

【発明の概要】

【発明が解決しようとする課題】

【００１１】

特許文献２の技術では予めルールを定義する必要があるため、未知の情報については、従来と同様に全ての分析器が分析を行う必要がある。そのため、分析処理に使用する計算機リソース量を削減することができない。

【００１２】

本発明は、複数の機械学習に基づく分析を行うシステムにおいて、分析精度の向上及び分析処理に使用する計算機リソース量の削減を目的とする。

【課題を解決するための手段】

【００１３】

本願において開示される発明の代表的な一例を示せば以下の通りである。すなわち、複数の計算機を備える計算機システムであって、前記複数の計算機の各々は、プロセッサ、前記プロセッサに接続されるメモリ、前記プロセッサに接続され、他の装置と接続するためのインタフェースを有し、前記複数の計算機は、ネットワークを介して送受信されるデータを用いた分析処理を実行する分析部を複数含む分析制御部を有する計算機と、前記データを用いて前記複数の分析部の各々が使用する特徴量を算出する特徴量算出部、及び使用する前記分析部を選択する振分部を有する計算機と、を含み、前記振分部は、前記複数の分析部の各々が使用する前記特徴量、前記分析処理の種別、及び分析処理の結果を含むエントリを複数含む振分情報を管理し、前記分析処理の結果は、前記分析処理が必要であるか否かを示す値であり、前記振分部は、前記振分情報を参照して、前記データから算出

された特徴量に類似する特徴量を含む類似エントリを検索し、前記類似エントリに含まれる前記分析処理の結果に基づいて、実行する前記分析処理を選択し、前記振分部によって選択された分析処理を実行する前記分析部は、前記データから算出された特徴量を用いた分析処理を実行し、前記分析処理の結果を前記振分部に送信し、前記振分部は、前記分析処理の結果を受信した場合、前記データから算出された特徴量、前記分析処理の種別、及び前記分析処理の結果を含むエントリを前記振分情報に追加することを特徴とする。

【発明の効果】

【００１４】

本発明によれば、振分情報に基づいて分析部が選択されるため、分析処理に使用する計算機リソース量を削減できる。また、分析部の分析結果を振分情報に反映することによって、分析精度を向上させることができる。前述した以外の課題、構成及び効果は、以下の実施例の説明によって明らかにされる。

【図面の簡単な説明】

【００１５】

【図１】実施例１の計算機システムの構成例を示す図である。

【図２】実施例１の分析装置のソフトウェア構成の詳細を説明する図である。

【図３】実施例１の振分情報群に含まれる振分情報の一例を示す図である。

【図４】実施例１の振分部が実行する処理を説明するフローチャートである。

【図５】実施例１の特徴量空間の一例を示す図である。

【図６】実施例２の計算機システムの構成例を示す図である。

【発明を実施するための形態】

【００１６】

以下、本発明の実施例を、図面を用いて説明する。なお、以下で説明する実施例は一例にすぎず、本発明が適用される実施例は、以下の実施例に限られるわけではない。さらに、以下に示した実施例は単独で適用してもよいし、複数又は全ての実施例を組み合わせて適用しても構わない。

【実施例１】

【００１７】

図１は、実施例１の計算機システムの構成例を示す図である。

【００１８】

計算機システムは、データセンタ１００及び複数の端末１０１から構成される。データセンタ１００及び複数の端末１０１は外部ＮＷ１０５を介して接続される。

【００１９】

データセンタ１００は、ＮＷ装置１０２、計算機１０３、及び分析装置１０４を含む。なお、各装置は二つ以上存在してもよい。計算機１０３及び分析装置１０４は、ＮＷ装置１０２に接続する。

【００２０】

ＮＷ装置１０２は、ネットワークを介して外部の装置及び内部装置を接続する装置である。ＮＷ装置１０２は、例えば、スイッチ、ルータ、及びゲートウェイ等が考えられる。ＮＷ装置１０２は、端末１０１及び計算機１０３との間で送受信されるデータをミラーリングし、ミラーリングされたデータを分析装置１０４に送信する。

【００２１】

計算機１０３は、端末１０１からの処理要求に基づいて各種処理を実行する。例えば、計算機１０３は、Ｗｅｂサーバ及びデータベースサーバ等として、端末１０１にサービスを提供する。なお、本実施例は、計算機１０３の構成、及び計算機１０３が提供するサービスの種別等に限定されない。

【００２２】

分析装置１０４は、ＮＷ装置１０２を通過するデータ（パケット）又は当該データのログをＮＷ装置１０２から取得し、当該データを分析することによってデータの搾取、データの破壊、データの改ざん、及び計算機１０３に機能不全等を目的とした不正アクセスを

検知する。以下の説明では、ＮＷ装置１０２を通過するデータ又は当該データのログを観測データとも記載する。

【００２３】

不正アクセスとしては、ＤｏＳ（Ｄｅｎｉａｌ　ｏｆ　Ｓｅｒｖｉｃｅ）攻撃、Ｕ２Ｒ（Ｕｓｅｒ　ｔｏ　Ｒｏｏｔ）攻撃、Ｒ２Ｌ（Ｒｅｍｏｔｅ　ｔｏ　Ｌｏｃａｌ）攻撃、及びＰｒｏｂｅ攻撃等が知られている。

【００２４】

ＤｏＳ攻撃は、大量のデータ又は異常データを送信することによって、データを受信したシステムを稼働できない状態にする攻撃である。Ｕ２Ｒ攻撃及びＲ２Ｌ攻撃は、異常データを送信することによって、システムに不正に侵入する攻撃である。また、Ｐｒｏｂｅ攻撃は、システムのサービス及びプロトコル等を調査する攻撃である。

【００２５】

分析装置１０４は、ハードウェアとして、ＣＰＵ１１０、メモリ１１１、記憶装置１１２、及びＩ／Ｆ１１３を有する。各構成は内部バス等を介して互いに接続される。なお、端末１０１、ＮＷ装置１０２、及び計算機１０３のハードウェアは分析装置１０４と同一であるものとする。

【００２６】

ＣＰＵ１１０は、メモリ１１１に格納されるプログラムを実行する。ＣＰＵ１１０がプログラムを実行することによって、分析装置１０４が有する機能を実現できる。以下の説明では、機能部を主語に処理を説明する場合、ＣＰＵ１１０が当該機能部を実現するプログラムを実行していることを示す。

【００２７】

メモリ１１１は、ＣＰＵ１１０が実行するプログラムを格納する。また、メモリ１１１は、プログラムが処理に使用するワークエリアを含む。メモリ１１１に格納されるプログラムについては後述する。

【００２８】

記憶装置１１２は、情報を永続的に格納する。記憶装置１１２は、ＨＤＤ（Ｈａｒｄ　Ｄｉｓｋ　Ｄｒｉｖｅ）及びＳＳＤ（Ｓｏｌｉｄ　Ｓｔａｔｅ　Ｄｒｉｖｅ）等が考えられる。記憶装置１１２は、各種情報を格納する記憶部１３０として使用される。記憶装置１１２に格納される情報については後述する。

【００２９】

Ｉ／Ｆ１１３は、他の装置と接続するためのインタフェースである。Ｉ／Ｆ１１３は、例えば、ネットワークインタフェースが考えられる。

【００３０】

メモリ１１１に格納されるプログラムについて説明する。メモリ１１１は、特徴量算出部１２０、振分部１２１、及び分析制御部１２２を実現するプログラムを格納する。

【００３１】

特徴量算出部１２０は、観測データを用いて、分析処理に使用する各種特徴量を算出する。

【００３２】

分析制御部１２２は、複数の分析処理を実行する。本実施例の分析制御部１２２は、ＤｏＳ攻撃、Ｕ２Ｒ攻撃、Ｒ２Ｌ攻撃、及びＰｒｏｂｅ攻撃のそれぞれを検知するための分析部（分析器）を有する。各分析部は、それぞれの攻撃を検知するための分析処理を実行する。

【００３３】

各分析部が分析処理に使用する特徴量は異なる場合がある。本実施例では、以下のような特徴量が用いられる。

【００３４】

Ｕ２Ｒ攻撃分析部２０１（図２参照）及びＲ２Ｌ攻撃分析部２０２（図２参照）は、一つのパケットから算出される特徴量を用いて分析処理を実行する。Ｕ２Ｒ攻撃及びＲ２Ｌ

攻撃は、パケットに含まれる異常データに起因するためである。

【００３５】

ＤｏＳ攻撃分析部２００（図２参照）は、複数のパケットを集約したフローから算出される特徴量を用いて分析処理を実行する。ＤｏＳ攻撃は、通信量及び通信範囲の異常に起因するためである。

【００３６】

Ｐｒｏｂｅ攻撃分析部２０３（図２参照）は、フローから算出された特徴量又は一定期間に取得した複数のパケットから算出された特徴量を用いて分析処理を実行する。Ｐｒｏｂｅ攻撃は、通信量及び通信範囲の異常に起因する場合、又は、通信手順の異常に起因する場合があるためである。

【００３７】

Ｐｒｏｂｅ攻撃の一つである「ＩＰｓｗｅｅｐ」は、不特定のＩＰアドレスに対してｐｉｎｇを実行し、稼働しているシステムを特定する攻撃である。「ＩＰｓｗｅｅｐ」を検知するためには、例えば、同一の送信元から送信されるパケットの数を特徴量として用いればよい。

【００３８】

分析部が分析処理に使用する特徴量の種別は、一つでもよいし、また、複数でもよい。本発明は、分析処理に使用する特徴量に限定されない。

【００３９】

振分部１２１は、特徴量算出部１２０によって算出された各種特徴量に基づいて、分析処理の実行を指示する分析部を選択する。

【００４０】

記憶装置１１２によって実現される記憶部１３０に格納される情報について説明する。記憶部１３０は、ログ情報１４０、特徴量情報群１４１、振分情報群１４２、及び学習データ群１４３を格納する。なお、記憶部１３０に格納される情報は、メモリ１１１に格納されてもよい。

【００４１】

ログ情報１４０は、ＮＷ装置１０２から取得した観測データをログとして管理する情報である。ログ情報１４０には、タイムスタンプ、送信元のＩＰアドレス、パケットサイズ等を含むエントリが複数含まれる。

【００４２】

特徴量情報群１４１は、各分析部が使用する特徴量を管理する情報である。振分情報群１４２は、分析部を選択するための情報である。学習データ群１４３は、各分析部が機械学習に使用する学習データを管理する情報である。

【００４３】

図２は、実施例１の分析装置１０４のソフトウェア構成の詳細を説明する図である。なお、各機能部を接続する線は、論理的な接続関係を示す。

【００４４】

まず、分析制御部１２２、特徴量情報群１４１、振分情報群１４２、及び学習データ群１４３の詳細について説明する。

【００４５】

分析制御部１２２は、ＤｏＳ攻撃分析部２００、Ｕ２Ｒ攻撃分析部２０１、Ｒ２Ｌ攻撃分析部２０２、及びＰｒｏｂｅ攻撃分析部２０３を含む。各分析部は、特徴量情報群１４１を参照して、受信した観測データに関連する分析処理を実行する。

【００４６】

特徴量情報群１４１は、パケット特徴量情報２１０、フロー特徴量情報２１１、及び周期特徴量情報２１２を含む。

【００４７】

パケット特徴量情報２１０は、パケット単位の特徴量を管理する情報である。フロー特徴量情報２１１は、フロー単位の特徴量を管理する情報である。周期特徴量情報２１２は

、任意の時間範囲の観測データを用いて算出される特徴量を管理する情報である。
【００４８】
振分情報群１４２は、パケット用振分情報２２０、フロー用振分情報２２１、及び周期用振分情報２２２を含む。
【００４９】
パケット用振分情報２２０は、パケット単位の特徴量に基づいて、分析部を選択するための情報である。フロー用振分情報２２１は、フロー単位の特徴量に基づいて、分析部を選択するための情報である。周期用振分情報２２２は、任意の時間範囲の観測データを用いて算出される特徴量に基づいて、分析部を選択するための情報である。
【００５０】
なお、分析に使用する特徴量の組合せが複数存在するため、パケット用振分情報２２０、フロー用振分情報２２１、及び周期用振分情報２２２は複数存在する。
【００５１】
学習データ群１４３は、ＤｏＳ攻撃分析用学習データ２３０、Ｕ２Ｒ攻撃分析用学習データ２３１、Ｒ２Ｌ攻撃分析用学習データ２３２、Ｐｒｏｂｅ攻撃分析用学習データ２３３を含む。各学習データには、正常な通信の特徴量を含むデータが含まれる。
【００５２】
ＤｏＳ攻撃分析用学習データ２３０は、ＤｏＳ攻撃分析部２００が使用する学習データである。Ｕ２Ｒ攻撃分析用学習データ２３１は、Ｕ２Ｒ攻撃分析部２０１が使用する学習データである。Ｒ２Ｌ攻撃分析用学習データ２３２は、Ｒ２Ｌ攻撃分析部２０２が使用する学習データである。Ｐｒｏｂｅ攻撃分析用学習データ２３３は、Ｐｒｏｂｅ攻撃分析部２０３が使用する学習データである。
【００５３】
次に、分析装置１０４の処理の流れについて説明する。
【００５４】
分析制御部１２２に含まれる分析部は、学習データ群１４３に格納される学習データを用いて機械学習を実行する。なお、機械学習は、周期的に実行されてもよいし、ユーザからの指示を受け付けた場合に実行されてもよい。
【００５５】
特徴量算出部１２０は、ＮＷ装置１０２から受信した観測データをログ情報１４０に格納し、ログ情報１４０を用いて各種特徴量を算出する。例えば、特徴量算出部１２０は、パケット単位の特徴量、フロー単位の特徴量、及び任意の時間範囲の観測データの特徴量を算出する。
【００５６】
特徴量算出部１２０は、算出された特徴量を特徴量情報群１４１に格納し、その後、振分部１２１に処理の開始を指示する。
【００５７】
振分部１２１は、特徴量情報群１４１及び振分情報群１４２に基づいて、異常を示す特徴量であるか否かを判定する。異常を示す特徴量であると判定された場合、振分部１２１は、特徴量情報群１４１及び振分情報群１４２に基づいて、受信した観測データに関連する分析処理を実行する分析部を選択する。
【００５８】
振分部１２１は、分析制御部１２２に選択された分析部の実行を指示する。具体的には、振分部１２１は、選択された分析部に対応する分析関数を呼び出し、算出された特徴量を引数として分析制御部１２２に入力する。
【００５９】
なお、振分部１２１が実行する処理の詳細は、図４を用いて説明する。
【００６０】
分析制御部１２２は、呼び出された分析関数に対応する分析部に分析処理の実行を指示する。分析部は、引数として入力された特徴量に基づいて、不正アクセスを検知するため

の分析処理を実行する。分析制御部１２２は、分析部によって実行された分析処理の結果を振分部１２１に出力する。

【００６１】

振分部１２１は、分析処理の結果に基づいて振分情報群１４２を更新する。

【００６２】

以上で説明したように、振分部１２１は、異常を示す特徴量を検知した場合、特徴量情報群１４１及び振分情報群１４２に基づいて分析処理を実行する分析部を選択する。これによって、必要な分析処理のみが実行されるため、分析装置１０４が使用する計算機リソース量を削減できる。また、分析処理の結果に基づいて振分情報群１４２が更新されるため、分析装置１０４における不正アクセスの検知精度が向上する。

【００６３】

図３は、実施例１の振分情報群１４２に含まれる振分情報の一例を示す図である。図３では、フロー用振分情報２２１の一例を示す。

【００６４】

フロー用振分情報２２１は、特徴量３０１、分析種別３０２、及び分析結果３０３を含むエントリを複数含む。

【００６５】

特徴量３０１は、分析部を選択するための指標となる特徴量である。図３の特徴量３０１は、送信パケット数３１１及びコネクション割合３１２を含む。

【００６６】

送信パケット数３１１は、任意のフローを介して端末１０１から計算機１０３に送信されたパケットの数である。所定の期間（例えば、パケットが送信された時間から５秒前の間）に生成されたコネクションのうち、パケットの送信元の端末１０１と計算機１０３との間に生成されたコネクションの割合である。

【００６７】

分析種別３０２は、分析処理の種別である。分析結果３０３は、分析処理の結果である。分析結果３０３には、正常な通信であることを示す「正常」及び異常な通信であることを示す「異常」のいずれかが格納される。本実施例では、分析処理を実行するか否かを示す情報として分析結果３０３を用いる。すなわち、分析結果３０３が「正常」の場合には、分析処理が不要であると判定され、分析結果３０３が「異常」の場合には、分析処理が必要であると判定される。

【００６８】

図４は、実施例１の振分部１２１が実行する処理を説明するフローチャートである。図５は、実施例１の特徴量空間の一例を示す図である。

【００６９】

振分部１２１は、特徴量算出部１２０から処理の開始指示を受け付けた場合、以下で説明する処理を開始する。なお、特徴量算出部１２０は、観測データの受信に伴って更新された特徴量情報の識別情報、及び特徴量情報のエントリの識別情報を振分部１２１に入力するものとする。

【００７０】

振分部１２１は、振分情報群１４２の中から振分情報を一つ選択する（ステップＳ４０１）。

【００７１】

具体的には、振分部１２１は、更新された特徴量を含む振分情報を検索し、検索された振分情報のリストを生成する。振分部１２１は、振分情報のリストを参照して、振分情報を一つ選択する。このとき、振分部１２１は、特徴量情報群１４１の更新された特徴量情報から選択された振分情報の特徴量３０１に対応する特徴量を取得する。

【００７２】

次に、振分部１２１は、選択された振分情報を参照して、特徴量３０１が取得されたエントリの特徴量と類似するエントリが存在するか否かを判定する（ステップＳ４０２）。

具体的には、以下のような処理が実行される。

【００７３】

振分部１２１は、選択された振分情報の特徴量３０１を軸とする特徴量空間に各エントリの特徴量をプロットする。図３に示すフロー用振分情報２２１が選択された場合、図５に示すような特徴量空間に各エントリの特徴量がプロットされる。図３に示すフロー用振分情報２２１は、二つの特徴量を含むため特徴量空間は二次元となる。したがって、ｎ個の特徴量を含む振分情報の場合、特徴量空間はｎ次元となる。

【００７４】

また、白丸及び黒丸は、フロー用振分情報２２１のエントリの特徴量を示す。白丸は任意の分析処理の分析結果３０３が「正常」であるエントリの特徴量を示す。黒丸は任意の分析処理の分析結果３０３が「異常」であるエントリの特徴量を示す。ここでは、Ｐｒｏｂｅ攻撃の分析処理の分析結果３０３を想定する。なお、白丸及び黒丸の区別は説明のために区別したものである。

【００７５】

振分部１２１は、更新された特徴量情報から更新された特徴量を含むエントリを取得し、更新されたエントリの特徴量を特徴量空間にプロットする。図５に示す特徴量空間のバツ印が取得されたエントリの特徴量の点を示す。

【００７６】

振分部１２１は、特徴量空間における各エントリの特徴量と取得されたエントリの特徴量との間の距離を算出する。振分部１２１は、分析結果３０３が「正常」であるエントリなかで最も距離が短いエントリ（第１エントリ）を特定し、分析結果３０３が「異常」であるエントリのなかで最も距離が短いエントリ（第２エントリ）を特定する。

【００７７】

図５に示す例では、点（α２，β２）に対応するエントリが第１エントリとなり、点（α３，β３）に対応するエントリが第２エントリとなる。

【００７８】

振分部１２１は、第１エントリの特徴量と取得されたエントリの特徴量との間の距離ｒ１、第２エントリの特徴量と取得されたエントリの特徴量との間の距離ｒ２に基づいて、類似するエントリを特定する。具体的には、振分部１２１は、以下に示す四つの条件に基づいて、類似するエントリを特定する。

【００７９】

（条件１）　ｒ１≦Ｒ１　かつ　ｒ２＞Ｒ
（条件２）　ｒ１＞Ｒ１　かつ　ｒ２≦Ｒ
（条件３）　ｒ１≦Ｒ１　かつ　ｒ２≦Ｒ
（条件４）　ｒ１＞Ｒ１　かつ　ｒ２＞Ｒ２

【００８０】

Ｒ１は分析結果３０３が「正常」であるエントリに類似と判定する基準距離を表す。Ｒ２は分析結果３０３が「異常」であるエントリと類似と判定する基準距離を表す。ただし、Ｒ２はＲ１より大きいものとする。

【００８１】

通常、トラフィックの大部分が正常な通信内容であり、異常な通信内容を含むトラフィックは少ない。そのため、分析結果３０３が「異常」であるエントリは、分析結果３０３が「正常」であるエントリが分布するエリアとは異なるエリアに存在する。また、一般的に分析結果３０３が「異常」であるエントリの周辺には、分析結果３０３が「正常」であるエントリは存在しない。そこで、Ｒ２を十分大きくすることによって、異常を示す特徴量を検知する精度を高める効果がある。

【００８２】

（条件１）は、第１エントリを中心とする円の領域に取得されたエントリの特徴量が含まれることを示す。（条件２）は、第２エントリを中心とする円の領域に取得されたエントリの特徴量が含まれることを示す。（条件３）は、第１エントリを中心とする円の領域

及び第２エントリを中心とする円の領域の両方に取得されたエントリの特徴量が含まれることを示す。（条件４）は、第１エントリを中心とする円の領域及び第２エントリを中心とする円の領域のいずれにも取得されたエントリの特徴量が含まれないことを示す。

【００８３】

（条件１）を満たす場合、振分部１２１は、取得されたエントリの特徴量が第１エントリの特徴量３０１に類似すると判定する。（条件２）を満たす場合、振分部１２１は、取得されたエントリの特徴量が第２エントリの特徴量３０１に類似すると判定する。（条件３）を満たす場合、振分部１２１は、取得されたエントリの特徴量が第２エントリの特徴量３０１に類似すると判定する。（条件４）を満たす場合、振分部１２１は、特徴量３０１が類似するエントリは存在しないと判定する。以上がステップＳ４０２の処理の説明である。

【００８４】

特徴量３０１が取得されたエントリの特徴量と類似するエントリが存在しないと判定された場合、振分部１２１は、全ての分析部を選択し、全ての分析部に対して分析処理の実行を指示する（ステップＳ４０９）。その後、振分部１２１は、ステップＳ４０６に進む。

【００８５】

なお、振分部１２１は、分析制御部１２２から分析結果を受信した場合、選択された振分情報の識別情報、取得されたエントリの特徴量、分析種別、及び分析結果を対応付けたエントリをメモリ１１１に一時的に格納する。

【００８６】

特徴量３０１が取得されたエントリの特徴量と類似するエントリが存在すると判定された場合、振分部１２１は、類似するエントリの分析種別３０２に基づいて分析処理を一つ選択し（ステップＳ４０３）、当該分析処理に対応する分析結果３０３が「正常」であるか否かを判定する（ステップＳ４０４）。

【００８７】

選択された分析処理に対応する分析結果３０３が「正常」であると判定された場合、振分部１２１は、ステップＳ４０５に進む。

【００８８】

選択された分析処理に対応する分析結果３０３が「異常」であると判定された場合、振分部１２１は、当該分析処理に対応する分析部を選択し、選択された分析部に対して分析処理の実行を指示する（ステップＳ４１０）。その後、振分部１２１は、ステップＳ４０５に進む。

【００８９】

なお、振分部１２１は、分析制御部１２２から分析結果を受信した場合、選択された振分情報の識別情報、取得されたエントリの特徴量、分析種別、及び分析結果を対応付けたエントリをメモリ１１１に一時的に格納する。

【００９０】

ステップＳ４０５では、振分部１２１は、類似するエントリの全ての分析種別３０２について処理が完了したか否かを判定する（ステップＳ４０５）。

【００９１】

類似するエントリの全ての分析種別３０２について処理が完了していないと判定された場合、振分部１２１は、ステップＳ４０３に戻り、同様の処理を実行する。

【００９２】

類似するエントリの全ての分析種別３０２について処理が完了したと判定された場合、振分部１２１は、全ての振分情報について処理が完了したか否かを判定する（ステップＳ４０６）。

【００９３】

具体的には、振分部１２１は、振分情報のリストに含まれる全ての振分情報について処理が完了したか否かを判定する。

【００９４】
全ての振分情報について処理が完了していないと判定された場合、振分部１２１は、ステップＳ４０１に戻り、同様の処理を実行する。
【００９５】
全ての振分情報について処理が完了したと判定された場合、振分部１２１は、一回以上分析部が選択されたか否かを判定する（ステップＳ４０７）。すなわち、ステップＳ４０９又はステップＳ４１０の処理が一回以上実行されたか否かが判定される。
【００９６】
分析部が選択されていないと判定された場合、振分部１２１は、処理を終了する。
【００９７】
一回以上分析部が選択されたと判定された場合、振分部１２１は、分析制御部１２２から分析処理の結果を全て受信した後、振分情報群１４２を更新し（ステップＳ４０８）、その後、処理を終了する。
【００９８】
具体的には、振分部１２１は、メモリ１１１に格納されるエントリを参照して、更新する振分情報を特定し、特定された振分情報にエントリを一つ追加する。振分部１２１は、追加されたエントリの特徴量３０１に取得されたエントリの特徴量を設定し、分析種別３０２に全ての分析種別の行を生成し、各行の分析結果３０３に分析結果を設定する。なお、実行が指示されていない分析処理の分析結果３０３には、「正常」が設定されるものとする。
【００９９】
なお、図３では、振分情報の分析種別３０２には全ての分析処理の行が含まれるが、本発明はこれに限定されない。例えば、特徴量３０１を用いる分析処理の行のみを含んでもよい。
【０１００】
なお、実施例１では、パケットの特徴量を用いた分析処理を行うシステムを例に説明したが、本発明はこれに限定されない。パケット以外のデータを分析する分析部を複数有するシステムでも同様の効果を奏する。
【０１０１】
実施例１によれば、分析装置１０４は、振分情報に基づいて、任意の分析結果が異常を示す特徴量に類似する特徴量の有無を判定し、異常を示す特徴量に類似する特徴量が検知された場合、当該特徴量を用いた分析処理を実行する分析部を選択し、分析処理の実行を指示する。これによって、分析装置１０４が分析処理に使用する計算機リソース量を削減できる。
【０１０２】
また、分析部の分析結果に基づいて振分情報を更新することによって、特徴量の類否判断に使用するデータ量が増加するため、適切に分析部を選択できる。これによって、システム全体の分析精度を向上させることができる。
【実施例２】
【０１０３】
実施例２では、振分部１２１及び分析制御部１２２が別々の装置に実装される点が実施例１と異なる。以下実施例１との差異を中心に実施例２について説明する。
【０１０４】
図６は、実施例２の計算機システムの構成例を示す図である。
【０１０５】
実施例２ではデータセンタ１００内の構成が実施例１のデータセンタ１００と異なる。具体的には、データセンタ１００は、ＮＷ装置１０２、計算機１０３、振分装置６００、及び分析装置６０１を含む。なお、各装置は二つ以上存在してもよい。計算機１０３及び振分装置６００は、ＮＷ装置１０２に接続する。
【０１０６】

実施例２のデータセンタ１００は、分析処理を選択する振分装置６００及び分析処理を実行する分析装置６０１を別々の装置として含む点が実施例１と異なる。

【０１０７】

振分装置６００のメモリ１１１は、特徴量算出部１２０及び振分部１２１を実現するプログラムを格納する。振分装置６００の記憶部１３０は、ログ情報１４０、特徴量情報群１４１、及び振分情報群１４２を格納する。

【０１０８】

分析装置６０１のメモリ１１１は、分析制御部１２２を実現するプログラムを格納する。分析装置６０１の記憶部１３０は、学習データ群１４３を格納する。

【０１０９】

特徴量算出部１２０及び分析制御部１２２が実行する処理は、実施例１と同一である。また、ログ情報１４０、特徴量情報群１４１、振分情報群１４２、及び学習データ群１４３の内容は、実施例１と同一である。

【０１１０】

振分部１２１が実行する処理は、実施例１と一部処理が異なる。具体的には、分析処理の実行を指示する方法が実施例１と異なる。

【０１１１】

例えば、ステップＳ４１０において、振分部１２１は、分析処理の種別、算出された特徴量を引数として含む分析処理の実行指示を分析装置６０１に送信する。

【０１１２】

また、分析処理毎に分析装置６０１を有する構成であってもよい。この場合、振分部１２１は、分析装置６０１の識別情報、及び分析処理の種別を含む情報を保持する。振分部１２１は、分析処理の実行を指示する場合、当該情報に基づいて、選択された分析処理を実行する分析装置６０１を特定し、特定された分析装置６０１に算出された特徴量を引数として含む分析処理の実行指示を送信する。

【０１１３】

実施例２は、実施例１と同一の効果を奏する。また、振分装置６００及び分析装置６０１を別々の装置にすることによって、分析装置６０１の追加及び削除の制約がないため、システムの構成を柔軟に変更することができる。また、既存の計算機システムに振分装置６００を追加することによって、本発明の効果を有する計算機システムを実現できる。

【０１１４】

なお、本発明は上記した実施例に限定されるものではなく、様々な変形例が含まれる。また、例えば、上記した実施例は本発明を分かりやすく説明するために構成を詳細に説明したものであり、必ずしも説明した全ての構成を備えるものに限定されるものではない。また、実施例の構成の一部について、他の構成に追加、削除、置換することが可能である。

【０１１５】

また、上記の各構成、機能、処理部、処理手段等は、それらの一部又は全部を、例えば集積回路で設計する等によりハードウェアで実現してもよい。また、本発明は、実施例の機能を実現するソフトウェアのプログラムコードによっても実現できる。この場合、プログラムコードを記録した記憶媒体をコンピュータに提供し、そのコンピュータが備えるＣＰＵが記憶媒体に格納されたプログラムコードを読み出す。この場合、記憶媒体から読み出されたプログラムコード自体が前述した実施例の機能を実現することになり、そのプログラムコード自体、及びそれを記憶した記憶媒体は本発明を構成することになる。このようなプログラムコードを供給するための記憶媒体としては、例えば、フレキシブルディスク、ＣＤ－ＲＯＭ、ＤＶＤ－ＲＯＭ、ハードディスク、ＳＳＤ（Ｓｏｌｉｄ Ｓｔａｔｅ Ｄｒｉｖｅ）、光ディスク、光磁気ディスク、ＣＤ－Ｒ、磁気テープ、不揮発性のメモリカード、ＲＯＭなどが用いられる。

【０１１６】

また、本実施例に記載の機能を実現するプログラムコードは、例えば、アセンブラ、Ｃ

／Ｃ＋＋、ｐｅｒｌ、Ｓｈｅｌｌ、ＰＨＰ、Ｊａｖａ（登録商標）等の広範囲のプログラム又はスクリプト言語で実装できる。

【０１１７】

さらに、実施例の機能を実現するソフトウェアのプログラムコードを、ネットワークを介して配信することによって、それをコンピュータのハードディスクやメモリ等の記憶手段又はＣＤ－ＲＷ、ＣＤ－Ｒ等の記憶媒体に格納し、コンピュータが備えるＣＰＵが当該記憶手段や当該記憶媒体に格納されたプログラムコードを読み出して実行するようにしてもよい。

【０１１８】

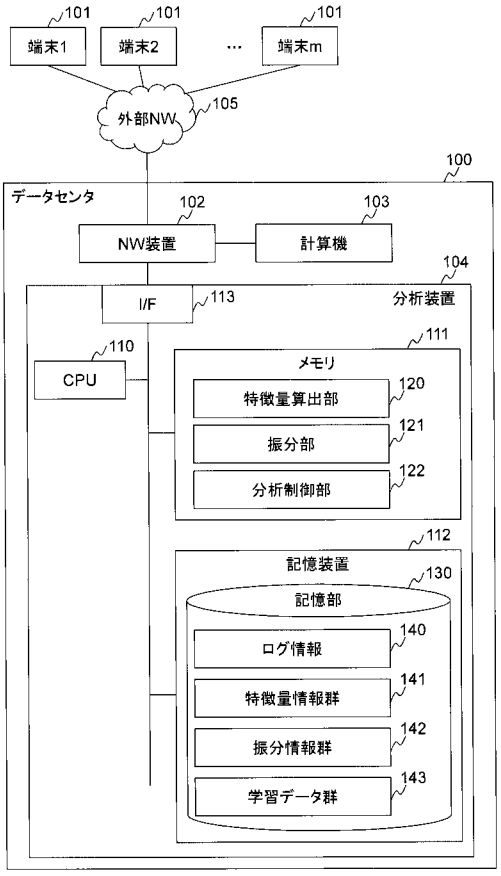
上述の実施例において、制御線や情報線は、説明上必要と考えられるものを示しており、製品上必ずしも全ての制御線や情報線を示しているとは限らない。全ての構成が相互に接続されていてもよい。

【符号の説明】

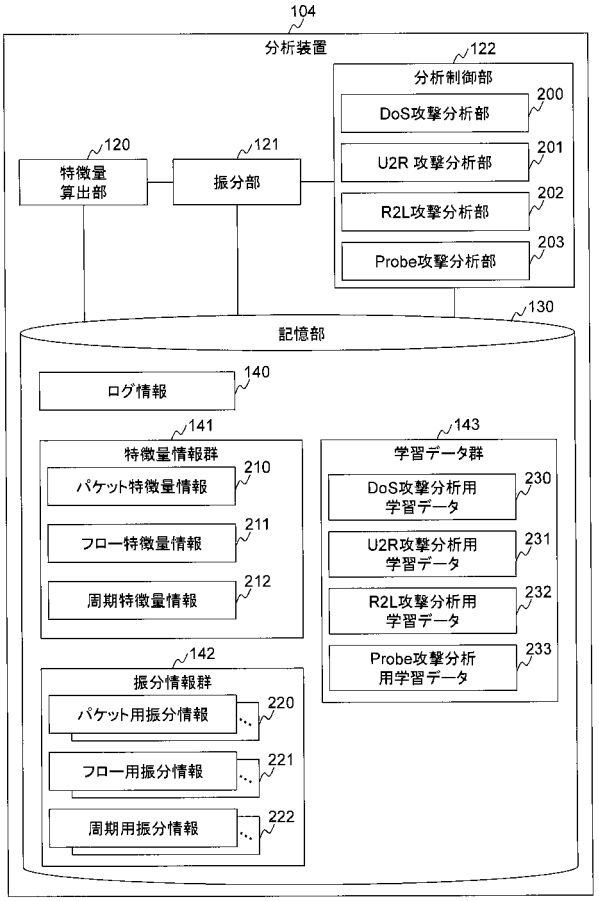
【０１１９】

１００　データセンタ
１０１　端末
１０２　ＮＷ装置
１０３　計算機
１０４　分析装置
１０５　外部ＮＷ
１１０　ＣＰＵ
１１１　メモリ
１１２　記憶装置
１１３　Ｉ／Ｆ
１２０　特徴量算出部
１２１　振分部
１２２　分析制御部
１３０　記憶部
１４０　ログ情報
１４１　特徴量情報群
１４２　振分情報群
１４３　学習データ群
２００　ＤｏＳ攻撃分析部
２０１　Ｕ２Ｒ攻撃分析部
２０２　Ｒ２Ｌ攻撃分析部
２０３　Ｐｒｏｂｅ攻撃分析部
２１０　パケット特徴量情報
２１１　フロー特徴量情報
２１２　周期特徴量情報
２２０　パケット用振分情報
２２１　フロー用振分情報
２２２　周期用振分情報
２３０　ＤｏＳ攻撃分析用学習データ
２３１　Ｕ２Ｒ攻撃分析用学習データ
２３２　Ｒ２Ｌ攻撃分析用学習データ
２３３　Ｐｒｏｂｅ攻撃分析用学習データ
６００　振分装置
６０１　分析装置

【図１】




【図２】

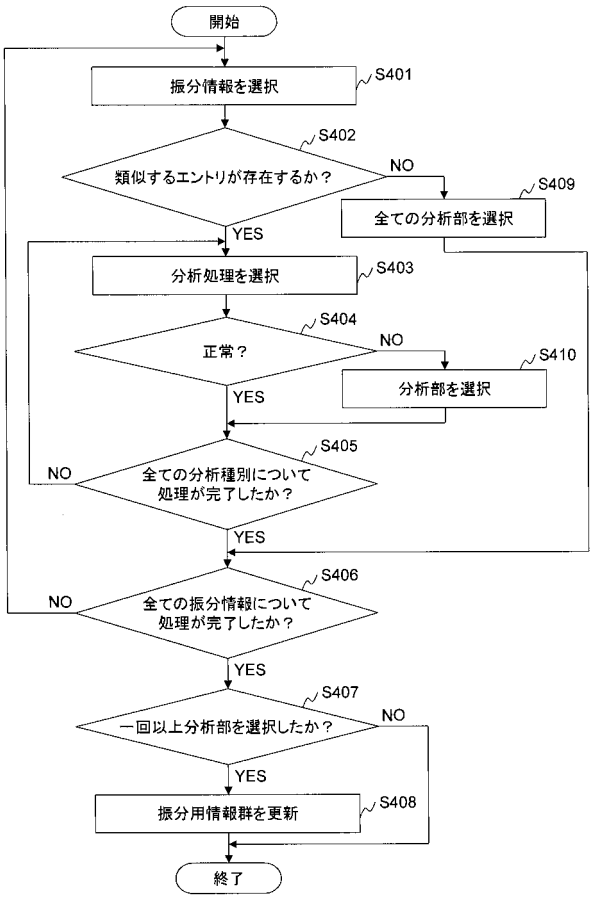



【図３】

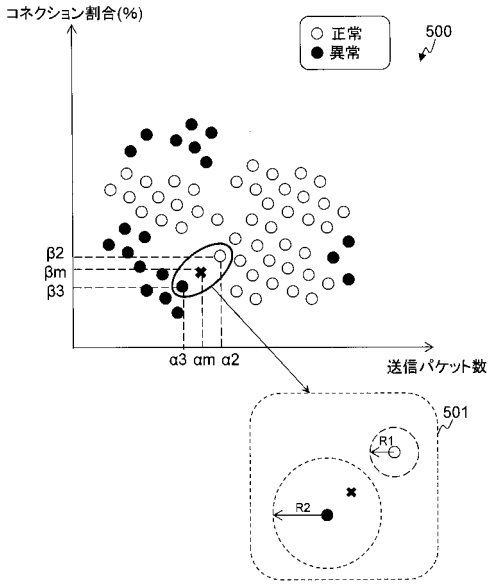
221

| 301 特徴量 311 送信パケット数 | 301 特徴量 312 コネクション割合（%） | 302 分析種別 | 303 分析結果 |
|---|---|---|---|
| α1 | β1 | DoS攻撃分析 | 異常 |
| | | U2R攻撃分析 | 正常 |
| | | R2L攻撃分析 | 異常 |
| | | Probe攻撃分析 | 異常 |
| α2 | β2 | DoS攻撃分析 | 正常 |
| | | U2R攻撃分析 | 正常 |
| | | R2L攻撃分析 | 正常 |
| | | Probe攻撃分析 | 正常 |
| α3 | β3 | DoS攻撃分析 | 正常 |
| | | U2R攻撃分析 | 正常 |
| | | R2L攻撃分析 | 異常 |
| | | Probe攻撃分析 | 異常 |
| ⋮ | ⋮ | ⋮ | ⋮ |
| αn | βn | DoS攻撃分析 | 異常 |
| | | U2R攻撃分析 | 正常 |
| | | R2L攻撃分析 | 正常 |
| | | Probe攻撃分析 | 正常 |

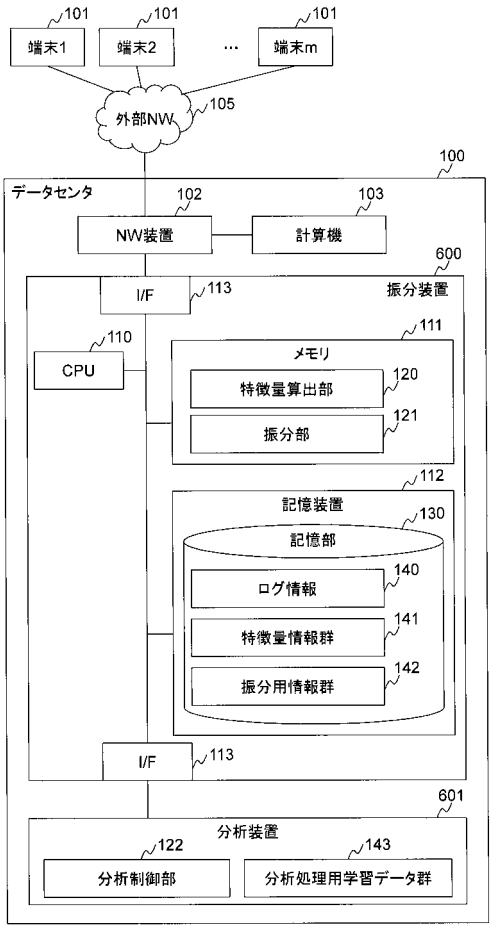
【図４】



【図５】


コネクション割合(%)
○ 正常
● 異常
500
β2
βm
β3
α3 αm α2
送信パケット数
501
R1
R2

【図６】


101
端末1
101
端末2
…
101
端末m
外部NW
105
100
データセンタ
102
NW装置
103
計算機
600
振分装置
I/F
113
111
メモリ
110
CPU
特徴量算出部
120
振分部
121
112
記憶装置
130
記憶部
ログ情報
140
特徴量情報群
141
振分用情報群
142
I/F
113
601
分析装置
122
分析制御部
143
分析処理用学習データ群